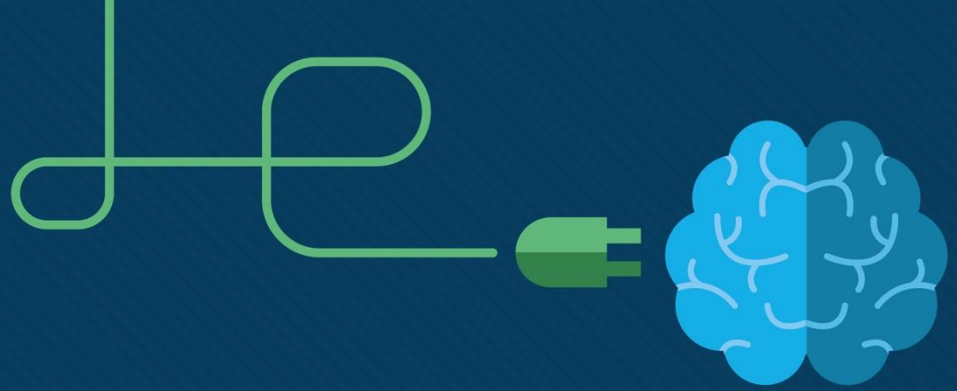


Module 6:Les attaquants et leurs outils

CyberOps Associate v1.0

Objectifs du module

- **Titre du Module:** Les attaquants et leurs outils
- **Objectif du Module:** Expliquer comment les réseaux sont attaqués.

Titre du Rubrique	Objectif du Rubrique
Qui attaque notre réseau?	Expliquer l'évolution des menaces ciblant le réseau.
Outils des acteurs de menace	Décrire les différents types d'outils d'attaque utilisés par les hackers.

6.1 Qui attaque notre réseau ?

Menaces, vulnérabilités et risques

- Les attaquants veulent accéder à nos biens tels que les données et autres propriétés intellectuelles, les serveurs, les ordinateurs, les smartphones, les tablettes, etc.

Menaces, vulnérabilités et risques (suite)

- Pour comprendre les questions liées à la sécurité du réseau, il est important de connaître les termes suivants:

TERM	EXPLICATION
Menace	Un danger potentiel pour une ressource, comme les données ou le réseau lui-même.
Vulnérabilité	Faille dans un système ou sa conception susceptible d'être exploitée par une menace.
Surface d'exposition aux attaques	La surface d'exposition aux attaques est la somme totale des vulnérabilités d'un système donné qu'un attaquant peut exploiter. La surface d'exposition aux attaques correspond aux différents emplacements par lesquels un hacker peut pénétrer dans un système ou extraire des données de ce système.
Exploiter	Le mécanisme utilisé pour exploiter une vulnérabilité pour compromettre une ressource. Un exploit peut être local ou distant. Un exploit distant fonctionne sur le réseau, sans accès préalable au système ciblé. Dans le cadre d'un exploit local, le cyberpirate dispose d'un accès utilisateur ou administrateur lui permettant de s'introduire dans le système ciblé. Il ne signifie pas nécessairement que le hacker dispose d'un accès physique au système ciblé.
Risque	La probabilité pour qu'une menace spécifique exploite une vulnérabilité précise associée à une ressource et que des conséquences indésirables en résultent.

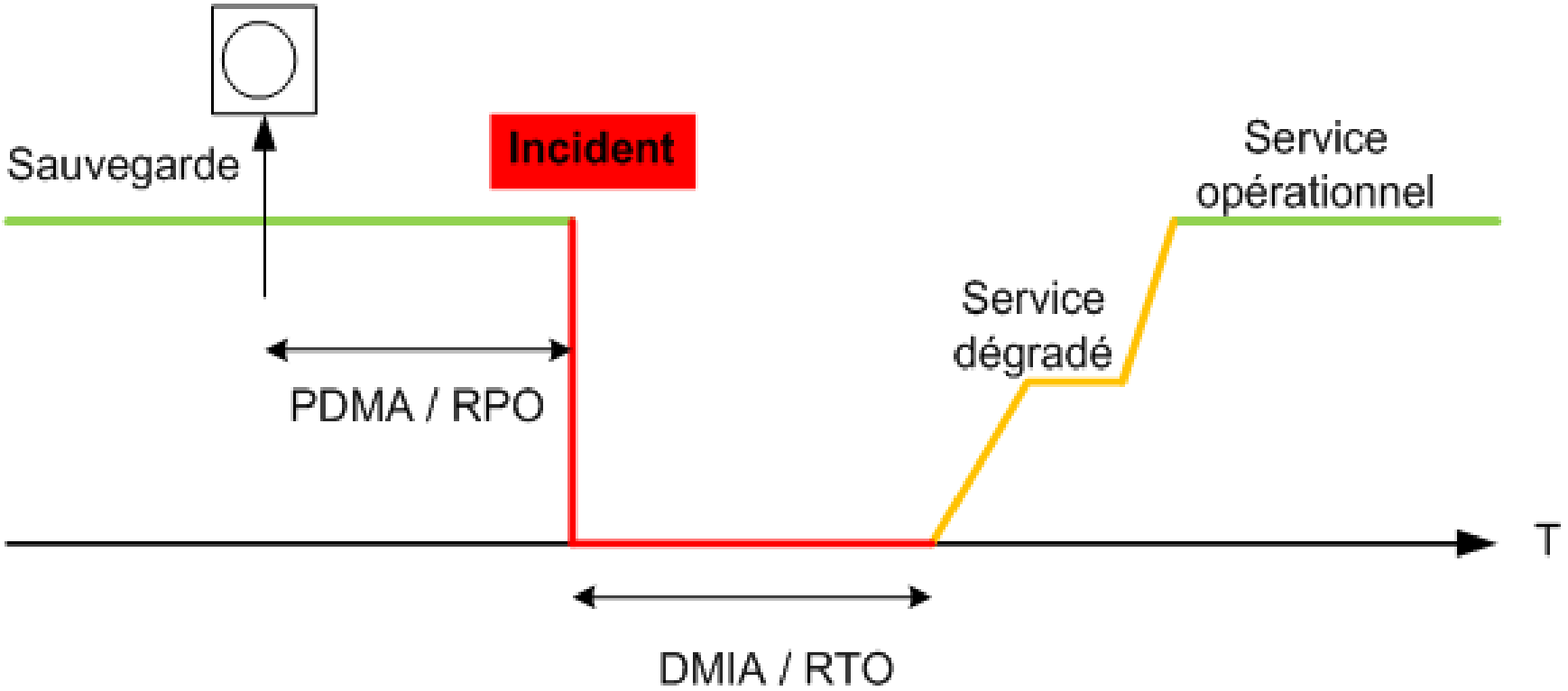
Menaces, vulnérabilités et risques (suite)

- La gestion des risques consiste à trouver un juste équilibre entre les coûts générés par les mesures de protection et les gains résultants de la protection des ressources.

Quatre façons de gérer les risques sont:

Stratégie de gestion des risques	Explication
Acceptation des risques	Lorsque le coût des options de gestion des risques est supérieur au coût représenté par le risque concerné, le risque est accepté, et aucune décision n'est prise.
Évitement des risques	Cela signifie éviter toute exposition au risque en éliminant l'activité, ce qui entraîne la perte des avantages de l'activité.
Réduction des risques	Cela réduit l'exposition au risque. C'est la stratégie de gestion des risques la plus couramment retenue. Cette stratégie exige une évaluation minutieuse des coûts des pertes, de la stratégie d'atténuation et des avantages tirés de l'exploitation ou de l'activité à risque.
Transfert des risques	Tout ou partie du risque est transféré vers un tiers consentant par exemple une compagnie d'assurance.

Menaces, vulnérabilités et risques (suite)



Attaquant contre acteur de menace?

Attaquant est un terme commun utilisé pour décrire un acteur de menace attaquant et peut désigner des profils très différents, comme :

- Un programmeur astucieux capable de développer de nouveaux programmes et de modifier le code de programmes existants pour les optimiser.
- Un professionnel des réseaux utilisant ses compétences avancées en programmation pour s'assurer qu'un réseau ne présente pas de vulnérabilité.
- Personne qui exécute des programmes pour empêcher ou corrompre des données sur les serveurs.

Types d'attaquants:

- Hackers au chapeau blanc
- Hackers au chapeau gris
- Hackers au chapeau noir

Attaquant contre acteur de menace (suite)

Hackers au chapeau blanc:

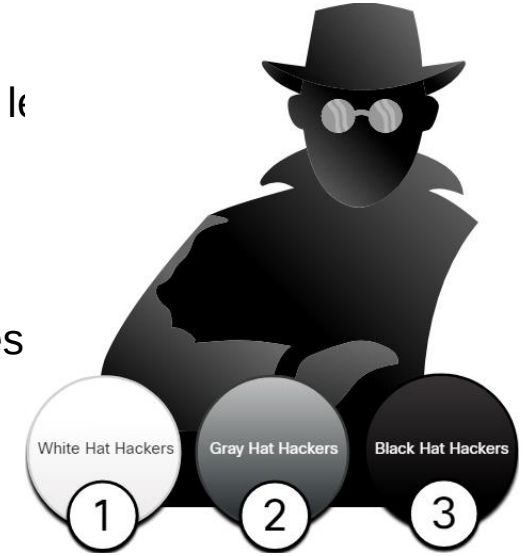
- Les hackers chapeau blanc sont des programmateurs éthiques dont le activités sont bénéfiques, éthiques et légales (formuler des recommandations pour les améliorer).

Hackers au chapeau gris:

- Les hackers au chapeau gris sont des personnes qui commettent des délits ou effectuent des actions non éthiques, mais pas à des fins de profit financier ni pour infliger des dommages.

Hackers au chapeau noir:

- Les hackers chapeau noir sont des criminels qui compromettent la sécurité des systèmes informatiques et des réseaux à des fins de profit personnel (gains financiers)



Évolution d'acteur de menace (suite)

Types d'acteurs de menace:

- **Script kiddies** - Il désigne des adolescents ou des acteurs de menace inexpérimentés exécutant des scripts, des outils ou des exploits afin de provoquer des dommages, mais généralement sans motivation financière.
- **Les courtiers en vulnérabilités** - Il sont généralement des hackers au chapeau gris qui recherchent des exploits pour les signaler aux fournisseurs, parfois en contrepartie d'un prix ou d'une récompense.
- **Hacktivists** - Il sont des hackers au chapeau gris qui se regroupent pour s'opposer aux idées politiques et sociales contraires à leurs propres convictions.
- **Cybercriminels** - Il sont des hackers au chapeau noir qui travaillent à leur compte ou pour de grandes organisations de piratage informatique.
- **Hackers financés par un État** - Il sont des cyberpirates qui volent des secrets d'État, collectent des informations stratégiques et mènent des actions de sabotage visant des réseaux ou des gouvernements étrangers, des groupes terroristes ou des entreprises.

Cybercriminels

- Les cybercriminels sont des acteurs de menace décidés à s'enrichir par tous les moyens.
- Les cybercriminels sont indépendants, mais ils sont généralement financés et soutenus par des organisations criminelles.
- Ils dérobent des milliards de dollars aux particuliers et aux entreprises.
- Ils fonctionnent dans l'économie souterraine et achètent et vendent des informations personnelles et de la propriété intellectuelle qu'ils volent aux victimes.
- Ils s'attaquent aussi bien aux petites entreprises et à leurs clients qu'aux grandes entreprises et autres groupes industriels.

Mesures de cybersécurité

- Les acteurs de menace peuvent aussi bien attaquer les terminaux vulnérables de particuliers que de PME ou d'entreprises plus importantes, qu'elles soient publiques ou privées.
- Par conséquent, la cybersécurité est une responsabilité partagée que tous les utilisateurs doivent pratiquer pour rendre l'Internet et les réseaux plus sûrs.
- Les entreprises doivent prendre les mesures nécessaires pour protéger leurs ressources, leurs utilisateurs et leurs clients. Elles doivent développer et appliquer des actions renforçant la cybersécurité telles que celles qui sont citées dans l'illustration.

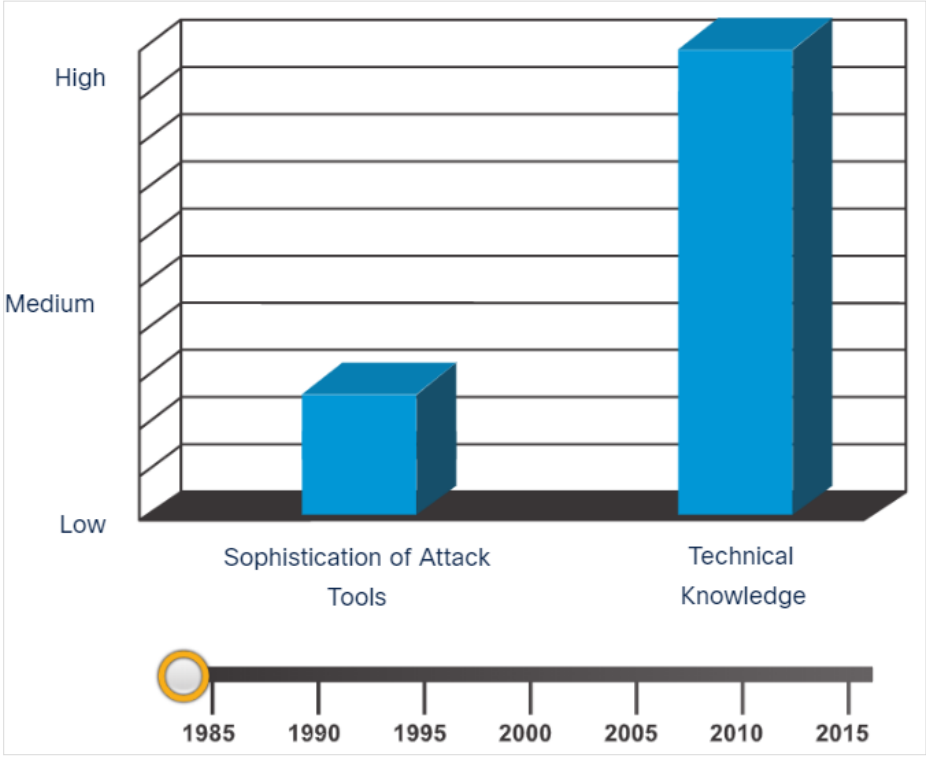
Partage des menaces et sensibilisation à la cybersécurité

- Désormais, la cybersécurité est une priorité pour de nombreux gouvernements dans le monde.
- La CISA (Cybersecurity Infrastructure and Security Agency) des États-Unis dirige les efforts visant à automatiser le partage d'informations sur la cybersécurité avec des organisations publiques et privées sans frais.
- Le système AIS permet au gouvernement américain et aux entreprises privées de s'informer mutuellement sur les indicateurs d'attaque aussitôt qu'une menace est identifiée.
- L’agence européenne pour la cybersécurité (ENISA) fournit des conseils et des solutions pour relever les défis de cybersécurité des États membres de l'EU.
- La CISA et la National Cyber Security Alliance (NCSA) organisent chaque année, en octobre, une campagne annuelle appelée Mois national de sensibilisation à la cybersécurité (NCASM) pour sensibiliser la population à la cybersécurité.

6.2 Outils des acteurs de menace

Présentation des outils utilisés pour les attaques

- Pour exploiter une vulnérabilité, un acteur de menace doit disposer d'une technique ou d'un outil.
- Au fil des ans, les outils d'attaque sont devenus plus sophistiqués et hautement automatisés.
- Ces nouveaux outils nécessitent moins de connaissances techniques pour être implémentés.
- Dans la figure, faites glisser le cercle blanc le long de la frise pour afficher le rapport entre la sophistication des outils d'attaque et les connaissances requises pour les utiliser.



Évolution des outils de sécurité

- Le piratage éthique implique l'utilisation de nombreux types d'outils différents pour tester le réseau et les appareils terminaux.
- Pour valider la sécurité d'un réseau et de ses systèmes, de nombreux outils de test de pénétration des réseaux ont été développés et nombre de ces outils peuvent également être utilisés par les acteurs de menace à des fins d'exploitation.
- Ces derniers ont également créé leurs propres outils de hacking. Les spécialistes de la cybersécurité doivent savoir comment utiliser ces outils pour effectuer des tests d'intrusion sur des réseaux.

Remarque: *une grande partie de ces outils sont basés sur UNIX ou sur Linux; par conséquent, un professionnel de la sécurité doit avoir une solide expérience de ces systèmes.*

Évolution des outils de sécurité (suite)

Le tableau suivant répertorie certaines catégories d'outils communs de test de pénétration de réseau.

Catégories d'outils	Description
Des programmes de piratage de mots de passe	Utilisé pour déchiffrer ou récupérer un mot de passe. Par exemple: Jean l'Éventreur, Ophcrack
Des outils de piratage sans fil	Ils sont utilisés pour pirater intentionnellement un réseau sans fil afin d'en détecter les failles de sécurité. Eg:Aircrack-ng, Kismet
Des outils d'analyse du réseau et de piratage	Les outils d'analyse du réseau recherchent des ports TCP ou UDP ouverts sur les appareils réseau, les serveurs et les hôtes. Par exemple: Nmap, SuperScan
Des créateurs de paquets	Utilisés pour sonder et tester la robustesse d'un pare-feu Par exemple: Hping, Scapy
Des analyseurs de paquets	Utilisés pour capturer et analyser les paquets au sein des réseaux locaux ou WLAN Ethernet traditionnels.Par exemple: Wireshark, Tcpdump
Des détecteurs de rootkit	Il s'agit d'un vérificateur d'intégrité des répertoires et des fichiers utilisé par les chapeaux blancs pour détecter les root kits installés. Par exemple: AIDE, Netfilter
Générateurs de bruits pour rechercher des vulnérabilités	Utilisés par les acteurs de menace qui essaient de détecter des vulnérabilités de sécurité dans un système informatique. Par exemple: Skipfish, Wapiti

Évolution des outils de sécurité (suite)

Catégories d'outils	Description
Des outils d'investigation	Ces outils sont utilisés par les hackers au chapeau blanc pour identifier des preuves d'intrusion dans un système informatique. Par exemple: Sleuth Kit, Helix
Débogueurs	Utilisés par les hackers au chapeau noir pour inverser l'ingénierie des fichiers binaires lors de l'écriture d'exploits et lors de l'analyse de logiciels malveillants. Eg:GDB, WinDBG
Des systèmes d'exploitation conçus pour les hackers	Ce sont préchargés des outils et des technologies optimisés pour le piratage. Par exemple: Kali Linux, SELinux
Des outils de chiffrement	Ces outils utilisent des algorithmes pour encoder les données afin d'empêcher tout accès non autorisé aux données chiffrées. Par exemple: VeraCrypt, CipherShed
Des outils d'exploitation des vulnérabilités	Ces outils déterminent si un hôte distant est vulnérable à une attaque. Par exemple: Metasploit, Impact de base
Des scanners de vulnérabilité	Ces outils analysent un réseau ou un système pour identifier les ports ouverts. Ils peuvent également rechercher des vulnérabilités connues et analyser des machines virtuelles, des appareils BYOD et des bases de données clientes. Eg:Nipper, Securia PSI

Catégories d'attaques

- Les acteurs de menace peuvent utiliser les outils d'attaque mentionnés précédemment, ou une combinaison d'outils pour créer des attaques.
- Il est important de comprendre que les cyberpirates s'appuient sur tout un arsenal d'outils liés à la sécurité en ligne pour livrer leurs attaques.
- Le tableau suivant affiche les types d'attaques courants.

Catégorie d'attaque	Description
Attaque par interception	Une attaque par interception a lieu lorsqu'un acteur de menace capte et peut visualiser le trafic réseau. Cette attaque est aussi appelée «attaque par analyse ou par espionnage du réseau».
Attaque par modification de données	On parle d'attaque par modification de données lorsqu'un acteur de menace capte un trafic d'entreprise et modifie des données de paquets à l'insu de l'expéditeur et du destinataire.
Attaque par usurpation d'adresse IP	Une attaque d'usurpation d'adresse IP est lorsqu'un acteur de menace construit un paquet IP qui semble provenir d'une adresse valide à l'intérieur de l'intranet de l'entreprise.

Catégories d'attaques (suite)

Catégorie d'attaque	Description
Attaques de mot de passe	Une attaque basée sur les mots de basse peut survenir lorsqu'un acteur de menace découvre un compte utilisateur valide.
Attaque par déni de service (DoS)	Une attaque DoS empêche les utilisateurs autorisés à utiliser normalement un ordinateur ou un réseau. Cette attaque DoS peut également bloquer le trafic et donc empêcher les utilisateurs autorisés d'accéder aux ressources du réseau.
Attaques de l'homme-au-milieu (MiTM)	Cette attaque se produit lorsque les acteurs de menace se sont positionnés entre une source et une destination.
Compromission des clés	Une attaque par compromission des clés a lieu lorsqu'un acteur de menace s'approprie une clé secrète, que l'on qualifie alors de compromise. Une clé compromise peut être utilisée pour accéder à une communication sécurisée sans que l'expéditeur ou le destinataire.
Attaque de renifleur	Un analyseur réseau est une application ou un appareil capable de lire, de surveiller et de capturer les échanges de données sur le réseau, et de lire les paquets réseau. Si les paquets ne sont pas chiffrés, l'analyseur offre une visibilité complète sur les données qu'ils contiennent.


CISCO

6.3 Récapitulation des attaquants et leurs outils

Qu'est-ce que j'ai appris dans ce module?

- Pour comprendre la sécurité du réseau, vous devez comprendre les termes suivants: menace, vulnérabilité, surface d'attaque, exploitation et risque.
- La gestion du risque est le processus qui consiste à prendre des mesures de protection en protégeant l'actif.
- Quatre façons communes de gérer les risques sont l'acceptation des risques, l'évitement des risques, la réduction des risques et le transfert des risques.
- Pirate est un terme commun utilisé pour décrire un acteur de menace. Les hackers au chapeau blanc sont des hackers éthiques qui utilisent leurs capacités dont les activités sont bénéfiques, éthiques et légales.
- Les hackers chapeau gris sont des personnes qui commettent des délits ou effectuent des actions non éthiques, mais pas à des fins de profit financier.
- Les hackers au chapeau noir sont des criminels qui compromettent la sécurité des systèmes informatiques et des réseaux à des fins de profit personnel ou avec des intentions malveillantes.

Qu'est-ce que j'ai appris dans ce module? (suite)

- De nombreuses attaques réseau peuvent être évitées en diffusant des informations sur les indicateurs d'attaques (IOC). La CISA et la NCSA sont des exemples d'organisations de promotion de la cybersécurité.
- Les outils d'attaque sont devenus plus sophistiqués et hautement automatisés.
- La plupart des outils sont basés sur Linux ou UNIX et leur connaissance est utile pour un professionnel de la cybersécurité.
- les outils incluent les systèmes de piratage des mots de passe, les outils de piratage sans fil, les outils d'analyse et de piratage du réseau, les outils de création de paquets, les renifleurs de paquets, les détecteurs de rootkits, les générateurs de bruits pour rechercher des vulnérabilités, les outils d'investigation, les débogueurs, les systèmes d'exploitation de piratage, les outils de chiffrement, les outils d'exploitation des vulnérabilités et les analyseurs de vulnérabilités.
- Les catégories d'attaques comprennent les attaques d'écoute, les attaques de modification de données, les attaques d'usurpation d'adresse IP, les attaques basées sur un mot de passe, les attaques par déni de service, les attaques homme au milieu, les attaques clés compromises et les attaques renifleurs.