Menaces, vulnérabilités et attaques en matière de cybersécurité 1

Menaces courantes

Définition et exploitation de menaces

Un **domaine de menace** est une zone de contrôle, d'autorité ou de protection que les hackers peuvent exploiter pour accéder à un système.

Les hackers peuvent détecter les vulnérabilités et exploiter les systèmes d'un domaine de plusieurs manières.

ⓘ Les hackers peuvent exploiter les systèmes d'un domaine via :

- Accès physique direct aux systèmes et aux réseaux
- Un réseau sans fil qui s'étend au-delà des limites de l'entreprise
- Dispositifs Bluetooth ou de communication en champ proche (NFC)
- Pièces jointes d'e-mails malveillants
- Éléments moins sécurisés de la chaîne d'approvisionnement d'une entreprise
- Les comptes de réseaux sociaux d'une entreprise
- Les supports amovibles tels que les clés USB
- Applications cloud

Types de cybermenaces

Les cybermenaces peuvent être classées en différentes catégories. Cela permet aux entreprises d'évaluer la probabilité qu'une menace se produise et de comprendre l'impact financier d'une menace afin de hiérarchiser leurs efforts de sécurité.
C'est le montage d'Allan :

1. Attaques logiciel
    - Un déni de service (DDOS)
    - Un virus informatique
2. Erreurs logicielles

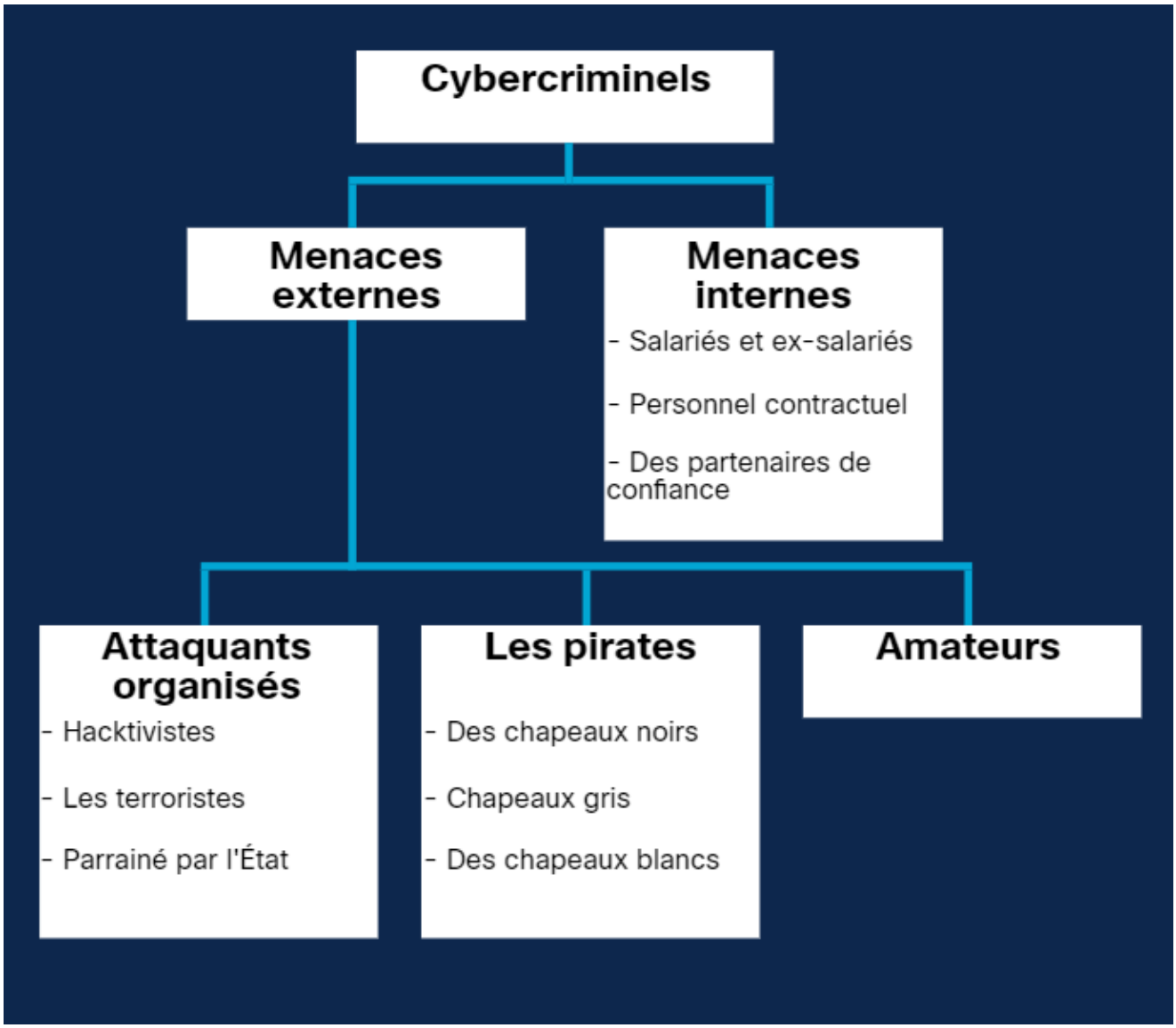
- Un bug logiciel
- Une application qui se déconnecte
- Un script intersite ou un partage illégal de serveur de fichiers

3. Sabotage
    - Un utilisateur autorisé réussit à pénétrer et à compromettre la base de données principale d'une organisation
    - La défiguration du site web d'une entreprise
4. Erreur humaine
    - Erreurs de saisie de données par inadvertance
    - Une mauvaise configuration du pare-feu
5. Vol
    - Vol d'ordinateurs portables ou d'équipements dans une pièce non verrouillée
6. Défaillances matérielles
    - Le disque dur tombe en panne
7. Interruption des services publiques
    - Les pannes d'électricité
    - Dégâts des eaux résultant d'une défaillance du système d'arrosage anti-incendie
8. catastrophes naturelles
    - Tempêtes violentes telles que les ouragans ou les tornades
    - Des tremblements de terre
    - Les inondations
    - Les incendies

Menaces internes et externes

Les menaces internes surviennent souvent lorsque des employés actuels ou passés, ainsi que d'autres partenaires contractuels, utilisent intentionnellement ou par mégarde des données confidentielles. Ils peuvent également menacer le bon fonctionnement des serveurs ou des périphériques du réseau en connectant des supports infectés ou en accédant à des e-mails ou des sites web malveillants.

La source d'une **menace externe** provient généralement d'attaquants pouvant exploiter les vulnérabilités des dispositifs en réseau ou utiliser des techniques d'ingénierie sociale, comme la ruse, pour accéder aux ressources internes d'une organisation.



Menaces et vulnérabilités des utilisateurs

Un **domaine d'utilisateur** comprend toute personne ayant accès au système d'information d'une entreprise, y compris les employés, les clients et les partenaires contractuels.

Les utilisateurs sont souvent considérés comme le maillon faible des systèmes de sécurité de l'information, car ils représentent une menace importante pour la confidentialité, l'intégrité et la disponibilité des données d'une organisation.

ⓘ Voici les menaces les plus courantes liés aux utilisateurs :

- Pas de sensibilisation à la sécurité
- Politiques de sécurité mal appliquées
- Vol de données
- Téléchargement et médias non autorisés
- Réseaux privés virtuels (VPN) non autorisés

- Sites web non autorisés
- Destruction (sabotage) de systèmes, d'applications ou de données

Menaces et vunérabilités des appareils

Les vulnérabilités matérielles sont souvent causées par des défauts de conception du matériel.

Exemple

Le type de mémoire RAM se compose de nombreux condensateurs (composants capables de contenir une charge électrique) installés très près les uns des autres. Cependant, il a été découvert qu'à cause de leur proximité, les modifications continues appliquées à l'un des condensateurs pouvaient affecter les condensateurs environnants.
Sur la base de ce défaut de conception, un exploit appelé Rowhammer a été créé. En accédant à à plusieurs reprises (en martelant) une ligne de mémoire, l'exploit RowHAMMER déclenche des interférences électriques qui finissent par corrompre les données stockées dans la mémoire RAM.

Les cybercriminels exploitent souvent les vulnérabilités des logiciels installés sur les terminaux d'une entreprise pour lancer une attaque.

× Mauvaises pratiques en entreprise :

- Laisser un périphérique sous tension sans surveillance.
  => Risque d'accès non autorisé.
- Télécharger des fichiers, photos, de la musique ou des vidéos à partir de sources non fiables.
  => Risque d'exécution de code malveillant.
- Insérer des clés USB, des CD ou des DVD non autorisés.
  => Risque d'introduire des malwares ou de compromettre les données stockés sur l'appareil.
- Utilisation de matériel ou de logiciels obsolètes.
  => Rend les systèmes et les données d'une entreprise plus vulnérable

aux attaques.

✓ **Bonne pratiques en entreprise :**

- Les équipes de sécurité de l'information d'une organisation doivent essayer de se tenir au courant de la découverte quotidienne de nouveaux virus, vers et autres logiciels malveillants qui constituent une menace pour leurs appareils.
- Suivre les politiques de sécurités en place.

Vulnérabilités logicielles

Buffer overflow (dépassement de tampon)

Les tampons sont des zones de mémoire affectées à une application. Une vulnérabilité se produit lorsque les données sont écrites au-delà des limites d'un tampon.

En modifiant les données au-delà des limites d'une mémoire tampon, l'application accède à la mémoire allouée à d'autres processus. Cela peut provoquer une panne du système, une compromission des données ou permettre une élévation des privilèges.

Entrée non valiée

Les programmes requièrent souvent des données d'entrée, mais ces données entrant dans le programme pourraient avoir un contenu malveillant, conçu pour détraquer les activités du programme.

⁝☰ **Exemple**

Considérons un programme qui reçoit une image à traiter. Un utilisateur malveillant pourrait concevoir un fichier image avec des dimensions d’image non valides. Les dimensions trafiquées de manière malveillante peuvent forcer le programme à répartir des tampons de tailles incorrectes et imprévues.

Situation de compétition

Cette vulnérabilité se produit lorsque la sortie d'un événement dépend de sorties commandées ou planifiées. Une situation de compétition devient une source de vulnérabilité lorsque les événements nécessaires commandés ou planifiés ne se produisent pas dans l'ordre correct ou en temps voulu.

Failles dans les mesures de sécurité

Les données système et les données sensibles peuvent être protégées grâce à des techniques comme l'authentification, l'autorisation et le chiffrement. Les développeurs devraient s'en tenir à l'utilisation de bibliothèques et de techniques de sécurité qui ont déjà été créées, testées et vérifiées et ne devraient pas tenter de créer leurs propres algorithmes de sécurité. Ceux-ci ne feront probablement qu'introduire de nouvelles vulnérabilités.

Problèmes de contrôle d'accès

Le contrôle d'accès est le processus de contrôle des affectations, de la gestion de l'accès physique à l'équipement dictant qui a accès à une ressource, notamment un fichier, et ce qu'il peut réaliser avec ce fichier, comme lire ou modifier celui-ci. De nombreuses vulnérabilités de sécurité sont créées par l'utilisation inappropriée des contrôles d'accès.

Quasiment l'ensemble des contrôles d'accès et des pratiques de sécurité peuvent être surmontés si l'agresseur dispose d'un accès physique à l'équipement cible.

> **Exemple**
>
> Quels que soient les paramètres d'autorisation sur un fichier, un hacker peut contourner le système d'exploitation et lire les données directement sur le disque. Pour protéger la machine et les données qu'elle contient, l'accès physique doit y être limité et des techniques de chiffrement doivent être utilisées pour protéger les données d'un vol ou d'une corruption.

Menaces sur le cloud privé

Le **domaine du cloud privé** comprend tous les serveurs, ressources et infrastructures informatiques privés mis à la disposition des membres d'une même organisation via Internet. Bien que de nombreuses entreprises estiment que leurs

données sont plus en sécurité dans un cloud privé, ce domaine présente toujours d'importantes menaces pour la sécurité, notamment :

- Exploration des ports ouverts et analyse réseau
- Accès non autorisé aux ressources
- Vulnérabilités du système d'exploitation ou du logiciel d'un routeur, d'un pare-feu ou d'un dispositif de réseau
- Erreurs de configuration du routeur, du pare-feu ou du périphérique réseau
- Des utilisateurs distants accèdent à l'infrastructure d'une organisation et téléchargent des données sensibles

Menaces pesant sur les applications

Le **domaine d'application** comprend tous les systèmes, applications et données critiques utilisés par une organisation pour soutenir ses opérations. De plus en plus, les organisations déplacent des applications telles que la messagerie électronique, la surveillance de la sécurité et la gestion des bases de données vers le cloud public.

Les menaces courantes pour les applications sont les suivantes :

- Une personne obtient un accès non autorisé aux centres de données, aux salles informatiques, aux armoires de câblage ou aux systèmes
- Les interruptions du serveur pendant les périodes de maintenance
- Vulnérabilités du logiciel du système d'exploitation réseau
- Perte de données
- Les vulnérabilités du développement d'applications client-serveur ou web

Complexité des menaces

Advanced Persistent Threat

Une **menace persistante avancée (APT)** est une attaque continue qui utilise des tactiques d'espionnage élaborées impliquant plusieurs acteurs et/ou des malwares sophistiqués pour accéder au réseau d'une cible et l'analyser.
Les hackers passent inaperçus et restent longtemps non détectés, avec des conséquences potentiellement dévastatrices. Les programmes APT ciblent généralement les gouvernements et les organisations de haut niveau et sont généralement bien orchestrés et bien financés.

Attaques par algorithme

Comme son nom l'indique, les **attaques par algorithme** tirent parti des algorithmes d'un logiciel légitime pour générer des comportements inattendus. Par exemple, les algorithmes utilisés pour suivre et signaler la consommation d'énergie d'un ordinateur peuvent être utilisés pour sélectionner des cibles ou déclencher de fausses alertes. Ils peuvent également désactiver un ordinateur en le forçant à utiliser toute sa mémoire vive ou en surchargeant son unité centrale de traitement (CPU).

Threat Intelligence et sources de recherche

L'équipe américaine de préparation aux urgences informatiques (US-CERT) et le ministère américain de la sécurité intérieure parrainent une base de données des **vulnérabilités et expositions communes (CVE).** Ces CVE ont été largement adoptées pour décrire et référencer les vulnérabilités connues.

Chaque entrée CVE contient un numéro d'identification standard, une brève description de la vulnérabilité de sécurité et toute référence importante à des rapports de vulnérabilité connexes. La liste CVE est maintenue par un organisme à but non lucratif, la MITRE Corporation, sur son site Web public.

Le dark web

Il s'agit du contenu web chiffré qui n'est pas indexé par les moteurs de recherche classiques et qui nécessite un logiciel, une autorisation ou des configurations

spécifiques pour y accéder. Des chercheurs experts surveillent le dark web à la recherche de nouvelles informations sur les menaces.

Indicateur de compromission (IOC)

Les IOC, tels que les signatures de malwares ou les noms de domaine, fournissent des preuves des failles de sécurité et des informations les concernant.

Automated Indicator Sharing (AIS)

Le partage automatisé d'indicateurs (AIS), une capacité de l'Agence pour la cybersécurité et la sécurité des infrastructures (CISA), permet l'échange en temps réel d'indicateurs de menaces pour la cybersécurité à l'aide d'un langage normalisé et structuré. L'expression structurée des informations sur les menaces (STIX) et l'échange automatisé et fiable d'informations sur le renseignement (TAXII) sont des normes utilisées dans les SIA.

Tromperies

Ingénierie sociale

L'ingénierie sociale est une stratégie non technique qui vise à manipuler les individus pour les amener à effectuer certaines actions ou à divulguer des informations confidentielles.

Plutôt que des vulnérabilités logicielles ou matérielles, l'ingénierie sociale exploite la nature humaine, tirant parti de la volonté des gens d'aider ou de leurs faiblesses, telles que l'appât du gain ou la vanité.

Pretexting

Ce type d'attaque se produit lorsqu'un individu ment pour accéder à des données privilégiées.

> Par exemple, un attaquant prétend avoir besoin de données personnelles ou financières afin de confirmer l'identité d'une personne.

Quiproquo

Les attaques quiproquo impliquent une demande d'informations personnelles en échange de quelque chose, comme un cadeau.

> Par exemple, un e-mail malveillant peut vous demander de fournir vos informations personnelles sensibles en échange de vacances gratuites.

L'usurpation d'identité

Il s'agit de l'utilisation de l'identité volée d'une personne pour obtenir des biens ou des services par la tromperie.

> Par exemple, un cybercriminel se faisant passer pour un employé du fisc a récemment ciblé des contribuables en disant aux victimes qu'elles devaient de l'argent et qu'elles devaient être payées immédiatement par virement bancaire, sous peine d'être arrêtées.
> Les criminels peuvent également utiliser l'usurpation d'identité pour attaquer d'autres personnes. Par exemple, ils peuvent se faire passer pour leur victime en ligne et publier sur des sites web ou des pages de réseaux sociaux pour miner la crédibilité de la victime.

Tactiques d'ingénierie sociale

Les cybercriminels utilisent plusieurs tactiques d'ingénierie sociale pour accéder aux informations sensibles.

- **Autorité**
  Les hackers profitent du fait que les utilisateurs sont plus susceptibles de se conformer aux instructions d'une personne qu'ils considèrent comme une figure d'autorité.

Exemple

Un dirigeant ouvre ce qui ressemble à une pièce jointe à comparaître officielle, mais qui est en réalité un fichier PDF infecté.

- **L'intimidation**
  Les cybercriminels intimident souvent une victime pour qu'elle prenne des mesures qui compromettent la sécurité.

Exemple

Une secrétaire reçoit un appel lui annonçant que son patron est sur le point de faire une présentation importante, mais que les fichiers sont corrompus. Le criminel au téléphone prétend que c'est la faute de la secrétaire et fait pression sur elle pour qu'elle transmette les fichiers immédiatement, sinon elle risque d'être renvoyée.

- **Le consensus**
  Souvent appelées « preuves sociales », les attaques par consensus fonctionnent parce que les gens ont tendance à agir de la même manière que les autres personnes autour d'eux, en pensant que quelque chose doit aller bien si les autres le font.

Exemple

Les cybercriminels peuvent publier un message sur les médias sociaux concernant une fausse opportunité d'affaires et obtenir des dizaines de comptes légitimes ou illégitimes pour commenter sa validité. Cela encourage les victimes peu méfiantes à faire un achat.

- **La rareté**
  Une tactique marketing bien connue, les attaques par pénurie fonctionnent, car les hackers savent que les utilisateurs ont tendance à agir lorsqu'ils pensent qu'il y a une quantité limitée de quelque chose disponible.

Exemple

Quelqu'un reçoit un e-mail au sujet d'un article de luxe vendu pour très peu d'argent, mais il indique qu'il n'y en a qu'une poignée à ce prix, afin d'inciter la

victime sans méfiance à agir.Cela peut inciter la victime sans méfiance à agir de manière impulsive.

- **L'urgence**
  De même, les gens ont également tendance à agit lorsqu'ils pensent que leur temps est limité.

Exemple

Les cybercriminels font la promotion d'une fausse offre d'expédition à durée limitée pour tenter d'inciter les victimes à agir rapidement.

- **La familiarité**
  Les gens sont plus susceptibles de faire ce qu'une autre personne leur demande s'ils l'apprécient.
  Par conséquent, les hackers essaient souvent d'établir une relation avec leur victime afin d'établir une relation. Dans d'autres cas, ils peuvent cloner le profil d'un de vos amis sur les réseaux sociaux pour vous faire croire que vous leur parlez.
- **La confiance**
  L'établissement d'une relation de confiance avec une victime peut nécessiter plus de temps.

Exemple

Un cybercriminel déguisé en expert en sécurité appelle la victime sans méfiance pour lui donner des conseils. En aidant la victime, "l'expert en sécurité" découvre une "erreur grave" qui nécessite une attention immédiate. La solution permet au cybercriminel de violer la sécurité de la victime.

- **Canulars**
  Un canular est un acte destiné à tromper ou à piéger quelqu'un. Les canulars peuvent causer autant de perturbations qu’une faille de sécurité réelle.

Exemple

Un message qui avertit d'une menace de virus (inexistante) sur un périphérique et demande au destinataire de partager cette information avec toutes ses connaissances. Ce canular suscite une réaction des utilisateurs, créant une peur inutile et un comportement irrationnel qui se perpétue par le biais des e-mails et des réseaux sociaux.

- **Arnaque à la facture**
  De fausses factures sont envoyées dans le but de recevoir de l'argent d'une victime en l'invitant à saisir ses informations d'identification dans un faux écran de connexion. La fausse facture peut également inclure des propos urgents ou menaçants.
- **Attaque de points d'eau**
  Une attaque par trou d'eau décrit un exploit dans lequel un hacker observe ou devine les sites web qu'une entreprise utilise le plus souvent, et infecte un ou plusieurs d'entre eux avec un malware.
- **Typo squatting**
  Ce type d'attaque repose sur des erreurs courantes telles que des fautes de frappe commises par des individus lors de la saisie d'une adresse de site web dans leur navigateur. L'URL incorrecte dirigera les individus vers un site web d'apparence légitime appartenant au hacker, dont le but est de recueillir leurs informations personnelles ou financières.
- **Ajout au début**
  Les hackers peuvent supprimer la balise d'e-mail « externe » utilisée par les entreprises pour avertir le destinataire qu'un e-mail provient d'une source externe. Cela incite les utilisateurs à croire qu'un e-mail malveillant a été envoyé depuis l'intérieur de leur entreprise.
- **Campagnes d'influence**
  Souvent utilisées dans le cadre de la cyberguerre, les campagnes d'influence sont généralement très bien coordonnées et combinent diverses méthodes telles que les fake news, les campagnes de désinformation et les messages sur les médias sociaux.

Tactiques d'ingénierie sociale physiques

- **Le Shoulder Surfing**
  C'est une attaque simple qui consiste à observer ou à regarder littéralement par-dessus l'épaule d'une cible pour obtenir des informations précieuses

telles que des codes PIN, des codes d'accès ou des détails de cartes de crédit. Les criminels n'ont pas besoin d'être toujours près de leur victime pour surfer à l'épaule : ils peuvent utiliser des jumelles ou des caméras de sécurité pour obtenir ces informations.

Tip

C'est l'une des raisons pour lesquelles un écran de DAB ne peut être vu que sous certains angles. Ces types de protections rendent cette pratique beaucoup plus difficile.

- **Dumpster Diving (Fouille des poubelles)**
  C'est un processus qui consiste à fouiller les poubelles d'une cible pour voir quelles informations ont été jetées.

Tip

C'est pourquoi les documents contenant des informations sensibles doivent être déchiquetés ou conservés dans des sacs à incinérer jusqu'à ce qu'ils puissent être détruits.

- **Piggybacking et tailgating (talonnage)**
  On parle de piggybacking ou de tailgating lorsqu'un criminel suit une personne autorisée pour pénétrer physiquement dans un lieu sécurisé ou une zone restreinte.
  Les hackers peuvent y parvenir ansi :

1. Donner l'impression d'être escorté dans les locaux par une personne autorisée.
2. Cibler une personne autorisée qui ne respecte pas les règles de l'établissement.
3. Rejoindre et faire semblant de faire partie d'une grande foule qui entre dans les locaux.

Pour éviter cela :

On peut utiliser deux jeux de portes. C'est ce que l'on appelle parfois un piège à homme et cela signifie que les individus entrent par une porte

extérieure, qui doit se fermer avant de pouvoir accéder par une porte intérieure.

Se protéger contre la tromperie

Les organisations doivent promouvoir la sensibilisation aux tactiques d'ingénierie sociale et former correctement les employés aux mesures de prévention. Voici quelques conseils.

- Ne divulguez jamais d'informations confidentielles ou d'identifiants à des tiers inconnus par courrier électronique, par chat, par SMS ou au cours d'une conversation.
- Résistez à l'envie de cliquer sur des courriels et des liens Internet alléchants.
- Méfiez-vous des téléchargements non initiés ou automatiques.
- Établissez et formez vos collaborateurs aux principales politiques de sécurité.
- Encouragez vos collaborateurs à prendre en charge les problèmes de sécurité.
- Ne cédez pas à la pression d'individus inconnus.

Cyber-attaques

Malwares

Les cybercriminels utilisent de nombreux types de logiciels malveillants, ou maliciels, pour mener leurs attaques. Un logiciel malveillant est un code qui peut être utilisé pour voler des données, contourner les contrôles d'accès, endommager ou compromettre un système.

ⓘ Quel que soit le type de malware infectant le système, certains symptômes sont communs aux malwares, notamment :

- Une augmentation de l'utilisation du CPU, ce qui ralentit le périphérique
- L'ordinateur se bloque ou tombe souvent en panne
- Une diminution de la vitesse de navigation sur internet
- Des problèmes inexplicables avec les connexions réseau
- Des fichiers modifiés ou supprimés
- La présence de fichier, de programmes ou d'icônes de bureau inconnus
- L'execution de processus ou de services inconnus

- Des programmes qui s'éteingnet ou se reconfigurent eux-mêmes
- Des e-mails envoyés à votre insu ou sans votre consentement.

Prenons note des principaux malwares existants...

Spywares (logiciel espion)

Conçus pour vous suivre et vous espionner, les logiciels espions surveillent votre activité en ligne et peuvent enregistrer chaque touche de votre clavier sur laquelle vous appuyez. De plus, ils capturent presque toutes vos données, y compris les informations personnelles sensibles telles que vos coordonnées bancaires en ligne. Pour ce faire, les logiciels espions modifient les paramètres de sécurité de vos périphériques.

Le logiciel espion se regroupe souvent avec des logiciels légitimes ou avec des chevaux de Troie.

Journalisation du clavier

Comme son nom l'indique, l'enregistrement au clavier consiste à enregistrer ou à consigner chaque touche du clavier d'un ordinateur.

Les cybercriminels enregistrent les frappes au moyen d'un logiciel installé sur un système informatique ou de dispositifs matériels reliés physiquement à un ordinateur. Ils configurent le logiciel enregistreur de frappe de sorte qu'il envoie le fichier journal par e-mail. Comme il a enregistré toutes les frappes au clavier, ce fichier journal peut révéler les noms d'utilisateur, les mots de passe, les sites Web visités et d'autres informations sensibles.

De nombreuses suites anti logiciels espions peuvent détecter et supprimer les enregistreurs de frappe non autorisés.

adware (publiciel)

Les logiciels publicitaires sont souvent installés avec certaines versions de logiciels et sont conçus pour distribuer automatiquement des publicités à un utilisateur, le plus souvent dans un navigateur web. Vous le savez quand vous le voyez ! Difficile de l'ignorer lorsque des publicités incessantes s'affichent à l'écran.

Les logiciels publicitaires sont souvent accompagnés de logiciels espions.

Backdoor (porte dérobée)

Les programmes de porte dérobée, tels que Netbus et Back Orifice, sont utilisés par les cybercriminels pour obtenir un accès non autorisé à un système en contournant les procédures d'authentification normales.

Les cybercriminels demandent généralement aux utilisateurs autorisés d'exécuter à leur insu un programme d'administration à distance (RAT) sur leur ordinateur, qui installe une porte dérobée. La porte dérobée donne au criminel un contrôle administratif sur un ordinateur cible.

Une porte dérobée fonctionne en arrière-plan et est difficile à détecter. Les portes dérobées permettent aux cybercriminels de continuer à accéder à un système, même si l'organisation a corrigé la vulnérabilité initiale utilisée pour attaquer le système.

> **Exemple**
>
> Abdel a trouvé une Backdoor sur Windows, plus de détail ici

Ransomware (rançongiciel)

Ce malware est conçu pour maintenir captif le système d'un ordinateur ou ses données, jusqu'à ce qu'un paiement soit effectué. Les ransonwares chiffrent généralement vos données pour vous empêcher d'y accéder.

Selon les allégations de rançongiciel, une fois la rançon payée via un système de paiement intraçable, le cybercriminel fournit un programme qui décrypte les fichiers ou envoie un code de déverrouillage. En réalité, de nombreuses victimes n'ont pas accès à leurs données, même après avoir payé.

D'autres versions de rançongiciel peuvent tirer parti de vulnérabilités spécifiques du système pour le verrouiller. Les raçongiciels se propagent souvent par le biais d'e-mails de phishing qui vous encouragent à télécharger une pièce jointe malveillante ou par le biais d'une vulnérabilité logicielle.

Scareware (alarmiciel)

Il s'agit d'un type de malware qui utilise des tactiques de « peur » pour vous inciter à effectuer une action spécifique. Les Scarewares se composent principalement de fenêtres de type système d'exploitation qui s'affichent pour vous avertir que

votre système est menacé et qu'il doit exécuter un programme spécifique pour revenir à un fonctionnement normal.

Si vous acceptez d'exécuter le programme en question, votre système sera infecté par un malware.

Logic bombe (bombes logiques)

Une bombe logique est un programme malveillant qui attend un élément déclencheur, comme une date ou une entrée de base de données spécifiée, pour déclencher le code malveillant. Tant que cet événement déclencheur ne se produit pas, la bombe logique reste inactive.

Une fois activée, une bombe logique met en œuvre un code malveillant qui endommage un ordinateur de diverses manières.

> **Exemple**
>
> Il peut saboter les enregistrements des bases de données, effacer les fichiers et attaquer les systèmes d'exploitation ou les applications.

Les spécialistes de la cybersécurité ont récemment découvert des bombes logiques qui attaquent et détruisent les composants matériels d'un appareil ou d'un serveur, notamment les ventilateurs de refroidissement, l'unité centrale de traitement (UC), la mémoire, les disques durs et les alimentations. La bombe logique surcharge ces composants jusqu'à ce qu'ils surchauffent ou tombent en panne.

Rootkit

Ce malware est conçu pour modifier le système d'exploitation afin de créer une porte dérobée, que les hackers peuvent ensuite utiliser pour accéder à distance à votre ordinateur. La plupart des rootkits profitent des vulnérabilités des logiciels pour effectuer une élévation de privilèges et modifier les fichiers système.

Il est également fréquent que les rootkits modifient les investigations du système et les outils de surveillance, ce qui rend très difficile leur détection. Dans la plupart des cas, un ordinateur infecté par un rootkit doit être nettoyé et tous les logiciels requis réinstallés.

Virus

Un virus est un type de programme informatique qui, une fois exécuté, se réplique et s'attache à d'autres fichiers exécutables, comme un document, en y insérant son propre code. La plupart des virus requièrent une interaction avec l'utilisateur pour s'activer et peuvent s'exécuter à une heure ou une date spécifique.

Les virus peuvent être relativement inoffensifs, comme ceux qui affichent une image amusante. Ils peuvent également être destructeurs, comme ceux qui modifient ou suppriment des données.

Les virus mutent pour éviter d'être détectés.

Comment se propagent-ils ?

La plupart des virus sont actuellement propagés par les lecteurs USB, les disques optiques, les partages réseau ou par e-mail.

Trojan horse

Ce malware effectue des opérations malveillantes en masquant ses véritables intentions. Il peut sembler légitime, mais est en réalité très dangereux. Les chevaux de Troie exploitent vos privilèges d'utilisateur et se trouvent le plus souvent dans des fichiers image, des fichiers audio ou des jeux.

Contrairement aux virus, les chevaux de Troie ne se reproduisent pas automatiquement, mais agissent comme un leurre pour faire circuler des logiciels malveillants sous le nez des utilisateurs peu méfiants.

Worms

Il s'agit d'un type de malware qui se réplique pour se propager d'un ordinateur à un autre. Alors que le virus nécessite un programme hôte pour s'exécuter, les vers fonctionnent de façon autonome. Hormis l'infection initiale de l'hôte, elles ne nécessitent pas la participation de l'utilisateur et peuvent se propager très rapidement sur le réseau.

Les vers partagent des modèles similaires : ils exploitent les vulnérabilités du système, ils ont un moyen de se propager de façon autonome et ils contiennent tous du code malveillant (charge utile) pour endommager les systèmes informatiques ou les réseaux.

Exemple

Les vers sont responsables de certaines des attaques les plus dévastatrices sur Internet. En 2001, le ver Code Red a infecté plus de 300 000 serveurs en seulement 19 heures.

Zero-day exploit (attaque zero-day)

Une attaque ou une menace zero-day exploite les vulnérabilités logicielles avant qu'elles soient connues ou avant qu'elles soient révélées par le fournisseur du logiciel.

Un réseau est extrêmement vulnérable aux attaques entre le moment où un exploit est découvert (zéro heure) et le temps nécessaire pour que le fournisseur de logiciels développe et publie un correctif qui corrige cet exploit.

ⓘ Exploit ?

Un programme écrit pour profiter d'une vulnérabilité de sécurité connue est un exploit.

Pour se défendre contre des attaques aussi rapides, les professionnels de la sécurité des réseaux doivent adopter une vision plus sophistiquée et holistique de toute l'architecture de réseau.

Attaques réseau

Botnet

Un bot est généralement infecté en visitant un site Web, en ouvrant une pièce jointe d'un e-mail ou en ouvrant un fichier média infecté. Un botnet est un réseau de bots (zombies) connecté à Internet.

Un individu ou un groupe malveillant est capable de le contrôler. Il peut avoir des dizaines de milliers, voire des centaines de milliers de bots qui sont généralement contrôlés via un serveur de commande et de contrôle.

Ces bots peuvent être activés pour distribuer un malware, pour lancer des attaques DDoS, pour distribuer un pourriel ou pour exécuter une attaque de mot de passe par force brute. Les cybercriminels loueront souvent des réseaux de zombies à des tiers pour des fins néfastes.

DDOS et DOS

Les attaques par déni de service (DoS) sont faciles à réaliser, même pour un novice. Elles posent un grand risque car elles peuvent interrompre les services réseau, causant des pertes de temps et d'argent considérables.

Même les technologies opérationnelles, comme le matériel et les logiciels qui contrôlent les appareils et les processus dans les bâtiments, les usines et les services publics, sont vulnérables aux attaques DoS. Dans des cas extrêmes, ces attaques peuvent provoquer un arrêt complet.

- **Quantité encombrante de trafic (DOS)**
  C'est lorsqu'un réseau, un hôte ou une application reçoivent une énorme quantité de données à un rythme qu'ils ne peuvent pas gérer. Cela provoque un ralentissement de la transmission ou de la réaction, ou une panne d'un appareil ou d'un service.
- **Paquets formatés de manière malveillante**
  Un paquet est un ensemble de données qui circulent entre un ordinateur source et un ordinateur ou une application de destination sur un réseau, comme Internet. Lorsqu'un paquet formaté de façon malveillante est envoyé à un hôte ou à une application, le récepteur ne pourra pas le gérer.

Exemple

Si un agresseur transmet des paquets contenant des erreurs ou transmet des paquets mal formatés qui ne peuvent être identifiés par l'application, cela va causer le ralentissement de l'appareil, voire le faire planter.

DOS ou DDOS ?

- **Une attaque DoS (déni de service)**
  Interrompt un réseau connecté à Internet en l'encombrant de données ou de paquets formatés de manière malveillante qu'il ne peut pas gérer.

- **Une attaque DDoS (déni de service distribué)**
  Est similaire, mais provient d'un botnet d'hôtes infectés appelés zombies. Lorsqu'il est prêt, l'attaquant donne des instructions aux systèmes de gestion pour que le botnet de zombies mène une attaque DDoS.

Attaques de couche 2

L'adresse MAC identifie le destinataire prévu d'une adresse IP envoyée sur le réseau, et ARP résout les adresses IP en adresses MAC pour la transmission des données.

Les hackers tirent souvent parti des vulnérabilités de ce système de sécurité de couche 2.

- **Empoisonnement ARP**
  Le spoofing, ou empoisonnement, est un type d'attaque par usurpation d'identité qui tire parti d'une relation de confiance entre deux systèmes.
  - L'usurpation d'adresse MAC se produit lorsqu'un hacker déguise son appareil en appareil valide sur le réseau et peut donc contourner le processus d'authentification.
  - L'usurpation d'identité ARP envoie des messages ARP usurpés sur un LAN. Cela lie l'adresse MAC d'un hacker à l'adresse IP d'un périphérique autorisé sur le réseau.
  - L'usurpation d'adresse IP envoie des paquets IP à partir d'une adresse source usurpée afin de la dissimuler.
- **Flooding MAC**
  Les périphériques d'un réseau sont connectés via un commutateur réseau en utilisant la commutation de paquets pour recevoir et transférer les données vers le périphérique de destination. L'inondation MAC compromet les données transmises à un périphérique. Un hacker inonde le réseau de fausses adresses MAC, compromettant ainsi la sécurité du commutateur réseau.

Man in the middle

Les attaquants peuvent intercepter ou modifier les communications entre deux appareils pour voler des informations ou se faire passer pour l'un des appareils.

- **Attaque Man-in-the-Middle MitM (l'homme du milieu)**
  Une attaque MitM se produit lorsqu'un cybercriminel prend le contrôle d'un appareil à l'insu de l'utilisateur. Avec ce niveau d'accès, un hacker peut intercepter, manipuler et transmettre de fausses informations entre l'expéditeur et la destination prévue.
  Les attaques MitM sont souvent utilisées pour dérober des informations

financières. De nombreux types de malwares possèdent des capacités d'attaque MitM.

- **Attaque Man-in-the-Mobile (l'homme du mobile)**
  Variante de l'expression man-in-the-middle, MitMo est un type d'attaque utilisé pour prendre le contrôle de l'appareil mobile d'un utilisateur.
  Après l'infection, l'appareil mobile peut recevoir l'instruction d'exfiltrer des informations sensibles de l'utilisateur et de les envoyer aux agresseurs.

> **Exemple**
>
> ZeuS est un exemple de programme malveillant doté de fonctionnalités MitMo. Il permet aux attaquants de capturer discrètement les SMS de vérification en deux étapes envoyés aux utilisateurs.

Système de noms de domaines

De nombreux services techniques essentiels sont nécessaires au fonctionnement d'un réseau, tels que le routage, l'adressage et l'attribution de noms de domaine. Ce sont des cibles de choix pour les attaques.

- **Réputation du domaine**
  Si un serveur DNS ne connaît pas d'adresse IP, il demandera à un autre serveur DNS.
  Une entreprise doit surveiller la réputation de son domaine, y compris son adresse IP, pour se protéger contre les domaines externes malveillants. La réputation du domaine permet de classer les e-mails comme spams ou menaces potentielles pour la sécurité.
- **Spoofing DNS**
  L'usurpation d'identité (DNS) ou empoisonnement du cache DNS est une attaque par laquelle de fausses données sont introduites dans le cache d'un résolveur DNS, c'est-à-dire la base de données temporaire du système d'exploitation d'un ordinateur qui enregistre les récentes visites sur les sites web et autres domaines Internet.
  Ces attaques par empoisonnement exploitent une faiblesse du logiciel DNS qui amène les serveurs DNS à rediriger le trafic pour un domaine spécifique vers l'ordinateur de l'attaquant.
- **Piratage de domaine**
  Lorsqu'un hacker prend à tort le contrôle des informations DNS d'une cible, il

peut y apporter des modifications non autorisées. C'est ce qu'on appelle le piratage de domaine.
Le moyen le plus courant de détourner un nom de domaine consiste à modifier l'adresse e-mail de contact de l'administrateur via l'ingénierie sociale ou en piratant le compte de messagerie de l'administrateur. L'adresse e-mail de l'administrateur est facilement accessible via l'enregistrement WHOIS du domaine, qui est un dossier public.

- **Redirection d'un localisateur de ressources uniformes (URL)**
  Un URL (Uniform Resource Locator) est un identifiant unique permettant de trouver une ressource spécifique sur Internet. La redirection d'une URL se produit généralement à des fins légitimes.
  Par exemple, vous vous êtes connecté à un portail eLearning pour commencer ce cours. Si vous vous déconnectez du portail et y revenez une autre fois, le portail vous redirige vers la page de connexion.
  C'est ce type de fonctionnalité que les hackers peuvent exploiter. Au lieu de vous rediriger vers la page de connexion de la formation en ligne, ils peuvent vous rediriger vers un site malveillant.

SEO Poisoning (Empoisonnement par SEO)

Les moteurs de recherche tels que Google présentent une liste de pages web aux utilisateurs en fonction de leur requête. Ces pages web sont classées en fonction de la pertinence de leur contenu.

Alors que de nombreuses entreprises légitimes se spécialisent dans l'optimisation de sites web pour un meilleur positionnement, l'empoisonnement par SEO (Search Engine Optimization) utilise la technologie SEO afin de faire apparaître un site web malveillant en tête des résultats de recherche.

Cette technique est appelée empoisonnement par SEO.
L'objectif le plus commun de l'empoisonnement par SEO est d'augmenter le trafic vers des sites malveillants qui peuvent héberger un malware ou effectuer une ingénierie sociale.

Se défendre contre les attaques réseau

Les organisations peuvent prendre plusieurs mesures pour se défendre contre diverses attaques réseau. à savoir :

- Configurez les pare-feu pour supprimer tous les paquets provenant de l'extérieur du réseau et dont les adresses indiquent qu'ils proviennent de

l'intérieur du réseau.
- Assurez-vous que les correctifs et les mises à niveau sont à jour.
- Répartir la charge de travail sur les systèmes de serveurs.
- Les périphériques réseau utilisent des paquets ICMP (Internet Control Message Protocol) pour envoyer des messages d'erreur et contrôler, par exemple, si un périphérique peut ou non communiquer avec un autre sur le réseau. Pour éviter les attaques DoS et DDoS, les entreprises peuvent bloquer les paquets ICMP externes avec leurs pare-feu.

Attaques de mot de passe

Password spraying (diffusion de mot de passe)

Cette technique tente d'accéder à un système en « diffusant » quelques mots de passe couramment utilisés sur un grand nombre de comptes.

> **Exemple**
>
> Un cybercriminel utilise « Password123 » avec de nombreux noms d'utilisateur avant de réessayer avec un deuxième mot de passe couramment utilisé, tel que « azerty ».

Cette technique permet au hacker de passer inaperçu car ils évitent les blocages de compte fréquents.

Dictionary attacks (attaque dictionnaire)

Un hacker essaie systématiquement chaque mot dans un dictionnaire ou une liste de mots couramment utilisés comme mot de passe pour tenter de pénétrer par effraction dans un compte protégé par mot de passe.

Brut-force attacks (Attaques par brut force)

L'attaque par force brute est le moyen le plus simple et le plus couramment utilisé d'accéder à un site protégé par mot de passe : un hacker utilise toutes les combinaisons possibles de lettres, de chiffres et de symboles dans l'espace du mot de passe jusqu'à ce qu'il réussisse.

Rainbow attacks (attaques arc-en-ciel)

Les mots de passe dans un système informatique ne sont pas stockés sous forme de texte brut, mais sous forme de valeurs hachées (valeurs numériques qui identifient de manière unique les données). Une table arc-en-ciel est un grand dictionnaire de hashs précalculés et des mots de passe à partir desquels ils ont été calculés.

Contrairement à une attaque par force brute qui doit calculer chaque hash, une attaque arc-en-ciel compare le hash d'un mot de passe avec ceux stockés dans la table arc-en-ciel. Lorsqu'un hacker trouve une correspondance, il identifie le mot de passe utilisé pour créer le hash.

Trafic interception (Interception du trafic)

Le texte brut ou les mots de passe non chiffrés peuvent être facilement lus par d'autres humains et machines en interceptant les communications.

Si vous stockez un mot de passe en clair et lisible, toute personne ayant accès à votre compte ou à votre appareil, qu'elle y soit autorisée ou non, peut le lire.

Attaques visant les terminaux sans fil et mobile

Graywares et SMiShing

Un Grayware est une application indésirable qui se comporte de manière gênante ou indésirable. Et bien que les graywares ne soient pas porteurs de malwares reconnaissables, ils peuvent néanmoins présenter un risque pour l'utilisateur, par exemple en suivant votre emplacement ou en diffusant des publicités indésirables.
Les auteurs de grayware conservent généralement leur légitimité en incluant ces capacités ‘grises’ dans les petits caractères de l'accord de licence du logiciel. Ce facteur représente une menace croissante pour la sécurité mobile en particulier, car de nombreux utilisateurs de smartphones installent des applications mobiles sans vraiment tenir compte de ces petits caractères.

Le **SMiShing** ou phishing par service de messages courts est une autre tactique utilisée par les hackers pour vous tromper. Les faux messages texte vous incitent à visiter un site web malveillant ou à appeler un numéro de téléphone frauduleux, ce qui peut entraîner le téléchargement de malwares sur votre terminal ou le partage d'informations personnelles.

Points d'accès malveillants

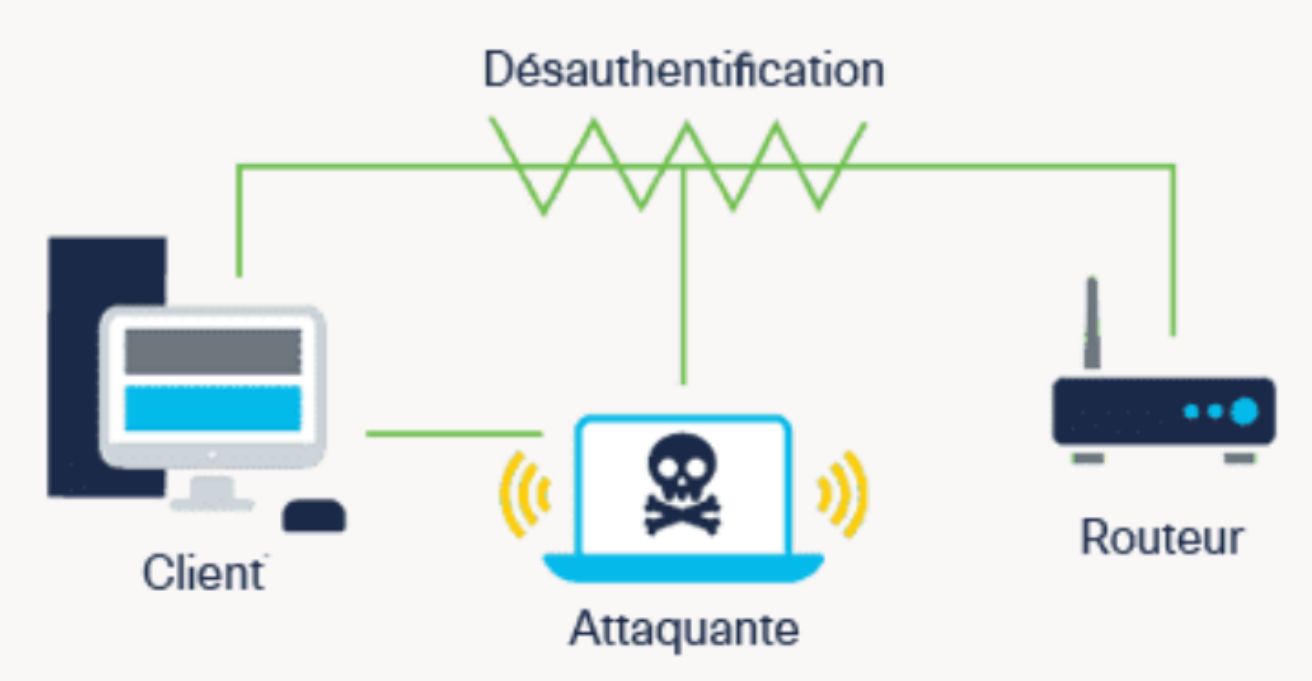
Un point d'accès non autorisé est un point d'accès sans fil installé sur un réseau sécurisé sans autorisation explicite. Bien qu'il puisse être mis en place par un employé bien intentionné à la recherche d'une meilleure connexion sans fil, il présente également une opportunité pour les hackers qui cherchent à accéder au réseau d'une entreprise.

Remarque

Un hacker utilise souvent des tactiques d'ingénierie sociale pour accéder physiquement à l'infrastructure réseau d'une entreprise et installer le **point d'accès non autorisé**.

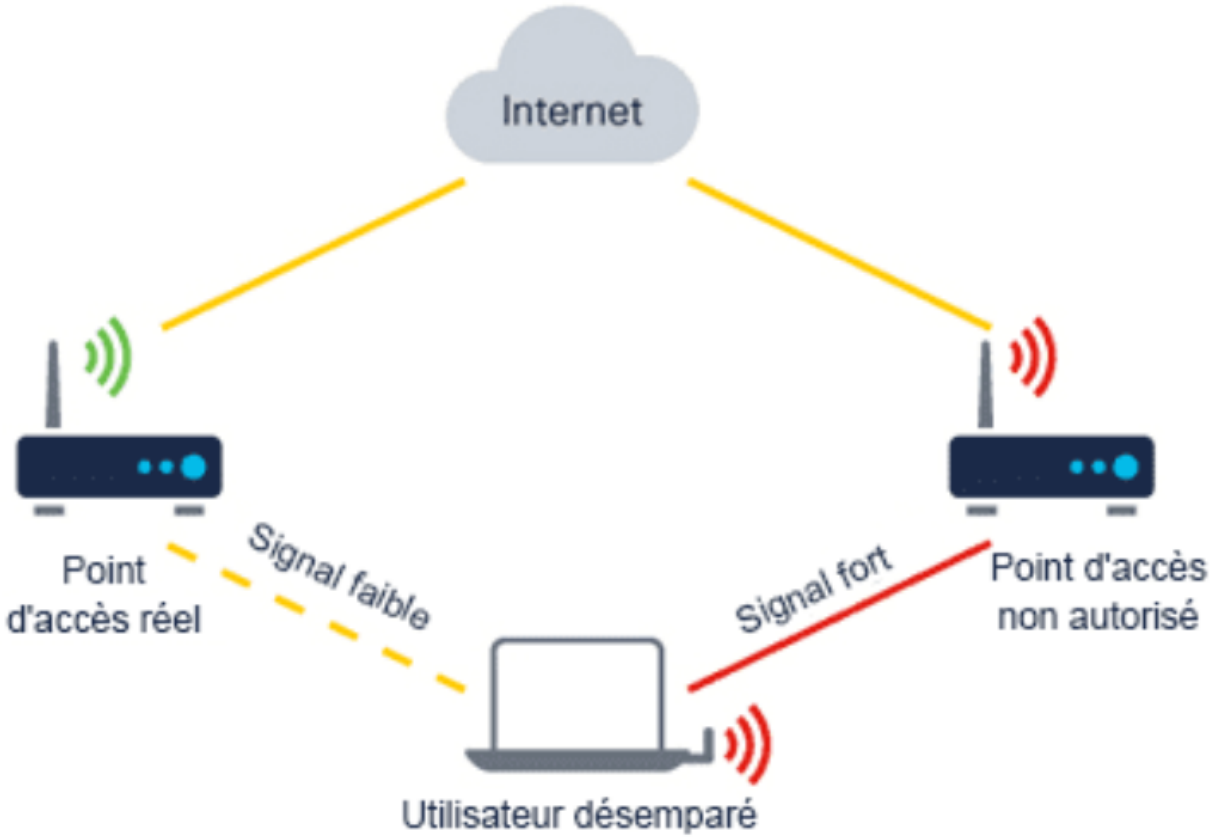
Également connu sous le nom de point d'accès pour criminels, le point d'accès peut être configuré comme un périphérique MitM pour capturer vos informations de connexion.

Cela fonctionne en déconnectant le point d'accès non autorisé, ce qui déclenche l'envoi d'une trame de désauthentification sur le réseau pour dissocier le point d'accès. Ce processus est ensuite exploité en usurpant votre adresse MAC et en envoyant une transmission de données de désauthentification au point d'accès sans fil.



Attaque jumelle malveillante ?

Une attaque jumelle malveillante décrit une situation dans laquelle le point d'accès du hacker est configuré pour ressembler à une meilleure option de connexion. Une fois que vous vous connectez au point d'accès malveillant, l'attaquant peut analyser votre trafic réseau et exécuter des attaques MitM.



Brouillage des fréquences radio

Les signaux sans fil sont sensibles aux interférences électromagnétiques (EMI), aux interférences de fréquence radio (RFI) et même aux coups de foudre ou au bruit des lampes fluorescentes.

Les hackers peuvent en tirer parti en brouillant délibérément la transmission d'une station radio ou satellite pour empêcher un signal sans fil d'atteindre la station réceptrice.

Pour réussir à brouiller le signal, la fréquence, la modulation et la puissance du brouilleur RF doivent être égales à celles de l'appareil que l'attaquant cherche à perturber.

Bluejacking et Bluesnarfing

Bluetooth est un protocole à faible consommation et à courte portée qui transmet les données dans un réseau personnel (PAN) et utilise le jumelage pour établir une relation entre les périphériques tels que les mobiles, les ordinateurs portables et les imprimantes. Les cybercriminels ont découvert des moyens d'exploiter les vulnérabilités entre ces connexions.

En raison de la portée limitée du Bluetooth, un hacker doit se trouver à portée de sa cible. Voici quelques façons d'exploiter le périphérique d'une cible à son insu.

- **Bluejacking**
  Le bluejacking utilise la technologie sans fil Bluetooth pour envoyer des messages non autorisés ou des images choquantes à un autre périphérique Bluetooth.
- **Bluesnarfing**
  Se produit lorsqu'un hacker copie des informations, telles que des e-mails et des listes de contacts, à partir du périphérique d'une cible à l'aide d'une connexion Bluetooth.

Les attaques contre les protocoles Wi-Fi

WEP (Wired Equivalent Privacy) et **WPA (Wireless Protected Access)** sont des protocoles de sécurité conçus pour sécuriser les réseaux sans fil vulnérables aux attaques.

Le protocole WEP a été développé pour fournir aux données transmises sur un réseau local sans fil (WLAN) un niveau de protection comparable à celui généralement attendu d'un réseau filaire classique. Elle a renforcé la sécurité des réseaux sans fil en chiffrant les données.

Le WEP utilisait une clé pour le cryptage. Le problème, cependant, était que le protocole WEP n'avait aucune disposition pour la gestion des clés et que le nombre de personnes partageant la même clé augmentait continuellement, donnant aux hackers l'accès à une grande quantité de données de trafic. En outre, le vecteur d'initialisation WEP (IV), l'un des composants clés de sa clé de chiffrement, était trop petit, lisible et statique.

Pour résoudre ce problème et remplacer le WEP, **WPA**, puis **WPA2** ont été développés en tant que protocoles de sécurité améliorés. Contrairement au protocole WEP, un hacker ne peut pas récupérer la clé de chiffrement WPA2 en observant le trafic réseau. Cependant, ils peuvent toujours utiliser un détecteur de paquets pour analyser les paquets entre un point d'accès et un utilisateur légitime.

Wi-Fi et protection mobile

Les organisations et les utilisateurs doivent prendre plusieurs mesures pour se défendre contre les attaques visant les appareils sans fil et mobiles. à savoir :

- Tirez parti des fonctions de sécurité sans fil de base, telles que l'authentification et le cryptage, en modifiant les paramètres de configuration par défaut.
- Limitez le placement des points d'accès en plaçant ces périphériques à l'extérieur du pare-feu ou dans une zone démilitarisée, c'est-à-dire un réseau de périmètre qui protège le LAN d'une entreprise contre les périphériques non fiables.
- Utilisez des outils WLAN tels que NetStumbler pour détecter les points d'accès pirates ou les postes de travail non autorisés.
- Développez une politique pour l'accès des invités au réseau Wi-Fi d'une entreprise.
- Les collaborateurs d'une entreprise doivent utiliser un VPN d'accès à distance pour l'accès WLAN.

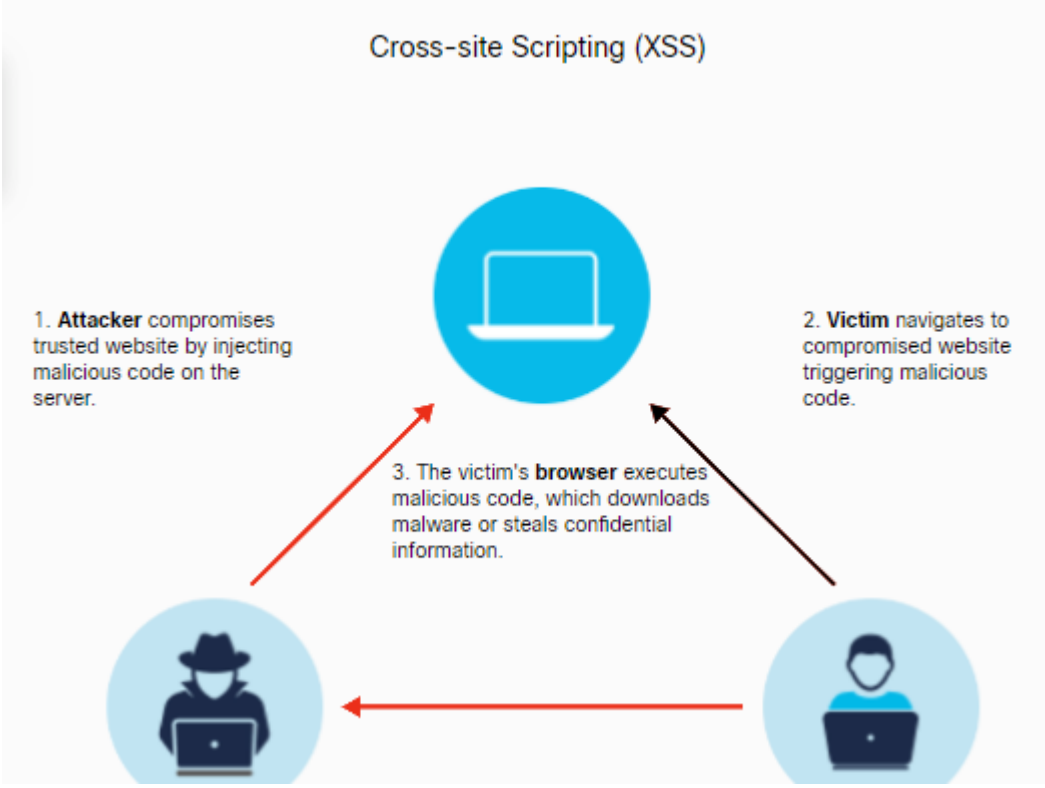
Attaques d'application

Scripts intersites (XSS)

Les attaques menées via des applications web sont de plus en plus courantes. Les cybercriminels tirent parti des vulnérabilités du codage d'une application web pour accéder à une base de données ou à un serveur.

Les scripts intersites (XSS) sont une vulnérabilité courante dans de nombreuses applications web. Voici comment cela fonctionne :

1. Les cybercriminels exploitent la vulnérabilité XSS en injectant des scripts contenant du code malveillant dans une page web.
2. La page web est consultée par la victime et les scripts malveillants sont transmis sans le savoir à son navigateur.
3. Le script malveillant peut accéder à tous les cookies, jetons de session ou autres informations sensibles sur l'utilisateur, qui sont renvoyés au cybercriminel.
4. Armé de ces informations, le cybercriminel peut usurper l'identité de l'utilisateur.



Injection de code

La plupart des sites web modernes utilisent une base de données, comme SQL (Structured Query Language) ou XML (Extensible Markup Language), pour stocker et gérer les données. Les attaques par injection cherchent à exploiter les faiblesses de ces bases de données.

- **Attaque par injection de code**
  Une attaque par injection XML peut corrompre les données de la base de données XML et menacer la sécurité du site web. Il interfère avec le traitement par une application des données XML ou des requêtes saisies par un utilisateur.
  Les cybercriminels peuvent manipuler cette requête en la programmant en fonction de leurs besoins. Cela leur donnera accès à toutes les informations sensibles stockées dans la base de données et leur permettra d'apporter autant de modifications que nécessaire au site web.
- **Attaque par injection SQL**
  Les cybercriminels peuvent lancer une attaque par injection SQL sur des sites web ou toute base de données SQL en insérant une instruction SQL malveillante dans un champ de saisie. Cette attaque tire parti d'une vulnérabilité dans laquelle l'application ne filtre pas correctement les données saisies par un utilisateur pour les caractères dans une instruction SQL.
  En conséquence, le cybercriminel peut obtenir un accès non autorisé aux informations stockées dans la base de données, à partir duquel il peut usurper son identité, modifier des données existantes, détruire des données ou même devenir administrateur du serveur de base de données lui-même.
- **Attaque par injection de DLL**
  Un fichier de bibliothèque de liens dynamiques (DLL) est une bibliothèque qui contient un ensemble de code et de données permettant d'effectuer une activité particulière dans Windows. Les applications utilisent ce type de fichier pour ajouter des fonctionnalités qui ne sont pas intégrées, lorsqu'elles ont besoin d'effectuer cette activité.
  L'injection de DLL permet à un cybercriminel de tromper une application pour qu'elle appelle un fichier DLL malveillant, qui s'exécute dans le cadre du processus cible.
- **Attaque par injection LDAP**
  Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole ouvert permettant d'authentifier l'accès des utilisateurs aux services d'annuaire.

Une attaque par injection LDAP exploite les vulnérabilités de validation des entrées en injectant et en exécutant des requêtes dans les serveurs LDAP, ce qui permet aux cybercriminels d'extraire des informations sensibles de l'annuaire LDAP d'une entreprise.

Débordement de la mémoire tampon

Les tampons sont des zones de mémoire affectées à une application. Un dépassement de tampon se produit lorsque des données sont écrites au-delà des limites d'un tampon. En modifiant les données au-delà des limites d'une mémoire tampon, l'application accède à la mémoire allouée à d'autres processus. Cela peut conduire à une panne du système ou à une compromission des données, ou permettre une escalade des privilèges.

Ces failles de mémoire donnent également aux hackers un contrôle total sur l'équipement d'une cible. Par exemple, un hacker peut modifier les instructions d'une application vulnérable pendant le chargement du programme en mémoire et, par conséquent, installer un malware et accéder au réseau interne à partir du périphérique infecté.

Exécution de code à distance

L'exécution de code à distance permet à un cybercriminel de tirer parti des vulnérabilités d'une application pour exécuter n'importe quelle commande avec les privilèges de l'utilisateur qui exécute l'application sur l'appareil cible.

L'escalade des privilèges exploite un bogue, un défaut de conception ou une mauvaise configuration d'un système d'exploitation ou d'une application pour accéder à des ressources normalement restreintes.

Metasploit ?

Le projet Metasploit est un projet de sécurité informatique qui fournit des informations sur les vulnérabilités de sécurité et facilite les tests de pénétration. Parmi les outils qu'ils ont développés se trouve le cadre Metasploit, qui peut être utilisé pour développer et exécuter un code d'exploitation sur une cible distante.
Meterpreter, en particulier, est une charge utile dans Metasploit qui permet aux utilisateurs de prendre le contrôle du périphérique d'une cible en écrivant leurs propres extensions et en chargeant ces fichiers dans un processus en cours d'exécution sur le périphérique. Ces fichiers sont chargés et exécutés à partir de la mémoire, de sorte qu'ils n'impliquent jamais le disque dur. Cela signifie que ces fichiers passent sous le radar de détection des antivirus.
Meterpreter dispose également d'un module permettant de contrôler la webcam d'un système distant. Une fois que Meterpreter est installé sur un

périphérique cible, l'utilisateur Metasploit peut afficher et capturer des images à partir de la webcam de la cible.