Types courants de cyberattaques et de contre-mesures – une brève explication

www.eccentrix.ca

Dans le monde d'aujourd'hui, nos précieuses propriétés comprennent majoritairement des informations numériques - comptes de messagerie, services bancaires en ligne, documentation de l'entreprise, données personnelles, etc. Pour cette raison, les cyberattaques ont évolué à un point tel que des efforts sérieux doivent être déployés pour garantir la sécurité de nos informations.

Mais, qu'est-ce qu'une cyberattaque? Il s'agit d'une action lancée par des acteurs de la menace, des cybercriminels, des pirates qui visent à affecter l'intégrité, la confidentialité ou la disponibilité de vos données. Ainsi, l'objectif peut être de perturber, de voler ou d'empêcher l'utilisation d'un système légitime pour ses utilisateurs.

De nos jours, les attaques sont devenues faciles à lancer - toutes les personnes intéressées peuvent y trouver de nombreuses façons, car les outils et la documentation sont également devenus très accessibles en ligne.

Les cyberattaques courantes sont divisées en types :
- Ingénierie sociale
- Applications et services réseau
- Sans fil
- Cryptographique

Explorons-les en comprenant le type et en énumérant les façons dont il est possible de nuire à un système, à des données ou à un actif numérique précieux pour vous ou votre organisation.

Ingénierie sociale

L'ingénierie sociale existe aussi longtemps que ce monde. Il y a toujours eu des gens qui ont essayé d'obtenir des informations précieuses, une fois qu'une confiance entre deux individus a été établie. Cela peut également être fait en trompant quelqu'un d'inexpérimenté. Les attaques de cette catégorie sont les plus réussies, car l'humain est très souvent le maillon le plus faible de la chaîne des événements.

L'ingénierie sociale existe sous plusieurs formes :

Hameçonnage : une technique d'ingénierie sociale dans laquelle l'acteur de la menace ou l'attaquant tente d'obtenir les informations de l'utilisateur en lui envoyant un courriel où l'attaquant prétend à tort provenir d'une source fiable.

Spear phishing : Un hameçonnage ciblé, où l'attaquant envoie un courriel très personnalisé à la victime.

Whaling : Similaire au hammeçonage ciblé, mais la cible est souvent quelqu'un de très connu, par exemple une célébrité, un dirigeant d'une grande entreprise ("baleine"), etc.

Vishing : Une attaque de phishing qui se produit par un appel téléphonique ou VoIP.
Smishing : Une attaque de phishing qui se produit sur les messages SMS.

Pharming : Les pirates utilisent cette attaque pour rediriger les utilisateurs vers de faux sites Web en modifiant le système DNS d'un réseau ou d'un ordinateur.

Tailgaiting : Une forme physique d'ingénierie sociale, où l'attaquant suit de près quelqu'un avec l'autorisation d'entrer dans une zone de sécurité.

Usurpation d'identité : un acteur menaçant se fait passer pour quelqu'un d'autre afin d'atteindre un objectif.

Dumpster diving : les attaquants recherchent souvent des informations précieuses sur l'entreprise dans les poubelles des employés de l'entreprise, où ils pourraient trouver des courriels imprimés, des papiers avec des mots de passe de compte, des diagrammes de réseau, etc.

Shoulder surfing : Un moyen de voir des informations en regardant derrière l'épaule de quelqu'un.

Watering hole : Similaire au spear phishing, mais dans ce type d'attaque, l'acteur de la menace n'utilise pas le courrier, mais attaque un site que l'utilisateur visite régulièrement, pour compromettre la sécurité de l'entreprise.

Contre-mesures

Les contre-mesures contre l'ingénierie sociale sont très différentes des autres formes d'attaques. Étant donné que l'utilisateur est au centre de chaque action, il est peu probable que cela puisse être évité uniquement en utilisant la technologie, par exemple un logiciel ou un matériel.

Ici, l'accent est mis sur la sensibilisation. C'est par nature pour les employés d'aider, ou d'être curieux. Cependant, il doit y avoir un effort continu pour s'assurer que les gens comprennent les implications de telles attaques et la facilité avec laquelle elles peuvent être lancées. L'effort commun par tous dans l'organisation fournira cette force.

Si la formation et la sensibilisation sont au cœur de la solution, ce n'est pas la seule :

- Établir des politiques d'entreprise, des lignes directrices et toute autre forme de documentation pertinente pour contrôler la manière dont l'information est accessible et partagée;
- Utiliser des contre-mesures techniques, telles que des logiciels capables de détecter des activités potentiellement nuisibles;
- Utiliser des contrôles physiques, tels que des portes verrouillées, des sas, ainsi que d'autres mécanismes pour empêcher l'accès facile aux zones contrôlées de votre installation.

Dans l'ensemble, la mise en œuvre d'une culture d'entreprise qui met l'accent sur la responsabilité de chacun est essentielle pour aider à atténuer les attaques d'ingénierie sociale.

Applications et services réseau

Nous utilisons des ressources d'applications et de services disponibles à tout moment et en tout lieu. En raison de leur forte interaction avec eux, les attaques se sont rapidement développées dans ce domaine. Il existe plusieurs types d'attaques d'applications et de services réseau que nous devrions connaître :

Usurpation : Une technique consistant à fournir une fausse identité sur le réseau. Il existe deux attaques d'usurpation d'identité courantes.

- **IP spoofing** : L'attaquant modifie son adresse IP source en essayant de cacher son ordinateur pour accéder à des ressources non autorisées. Il est couramment utilisé dans le but d'établir une connexion entre deux systèmes (man-in-the-middle) ou de lancer un déni de service.
- **MAC spoofing** : L'auteur de la menace altère l'adresse MAC (Media Access Control) de son périphérique réseau en essayant d'accéder au réseau de l'entreprise.

Contre-mesure : Il est important d'effectuer des balayages de réseau afin de détecter des bris d'intégrité dans les informations transmises au niveau des paquets et des trames.

Débordement de mémoire tampon (buffer overflow) : une conception défectueuse dans une application permet à une allocation d'espace de stockage de mémoire d'être dépassée par la demande de stockage de l'application dans la mémoire système. Cela provoque une élévation des privilèges ou un arrêt abrupt de l'application.

Contre-mesure : Lors de la conception d'une application, sa sécurité doit être prise en compte dès le début. De plus, il est important de mettre en œuvre un processus de mise à jour une fois qu'il est prêt à être utilisé. Les améliorations apportées au logiciel réduiront le risque de débordement de la mémoire tampon.

Le système sur lequel le logiciel s'exécute doit également être sécurisé.

Zero day : Exploite les menaces inconnues pour lesquelles un correctif ou un correctif n'existe pas encore.

Contre-mesure : Il est important d'être actif dans les connaissances de la communauté et d'être informé avec des renseignements appropriés sur ces types de menaces. Bien que le fabricant du logiciel travaille sur un correctif, il existe souvent des solutions temporaires ou de contournement qui peuvent également être mises en œuvre, ce qui réduit la possibilité qu'une attaque zero day ait lieu.

Attaque de script intersite (XSS) : Un attaquant falsifie un site Web légitime et injecte un code malveillant. Le code malveillant est ensuite exécuté sur le navigateur lorsque le client visite la page. Des activités d'accès non autorisées, telles que le vol de fichiers témoins contenant des données confidentielles, peuvent se produire.

Contre-mesure : Il est important d'assurer la sécurité du site Web en mettant en œuvre des tests de résistance, des tests de fuzz… tout cela aide à assurer la sécurité du code et réduit le potentiel d'attaque XSS.

Injection SQL : Un attaquant insère un code malveillant dans une base de données relationnelle, qui est ensuite transmise au serveur de base de données. Le résultat peut être des privilèges élevés, une perte d'intégrité des données, le vol d'informations d'identification, etc.

Contre-mesure : Semblable au XSS, il est important d'assurer la sécurité de l'application Web. Bien qu'ici, nous pourrions penser que la principale préoccupation concerne le serveur de base de données. C'est vrai, cependant c'est l'application qui ne filtre pas bien la requête, permettant à la requête malicieuse de modifier les données à l'arrière.

Détournement de session (hijacking) : Une attaque qui se produit lorsqu'un acteur malveillant détourne une session entre un serveur Web et un client de confiance.

Contre-mesure : Cette attaque tire parti des jetons réutilisables ou des identifiants de session. En s'assurant qu'un client a son propre jeton et qu'il n'est pas réutilisable, l'attaque a moins de chances de se produire. Il s'agit également de la sécurité de l'application elle-même, ainsi que du système d'exploitation.

Man-in-the-middle : Un attaquant intercepte la communication entre deux ordinateurs, dans le but de modifier leur conversation et de voler des données précieuses. Cela se fait au niveau du protocole, comme avec ARP.

Contre-mesure : Des sondes sur le réseau peuvent être installées pour surveiller les activités suspectes, telles que les systèmes de détection et de prévention des intrusions. Les antivirus conventionnels ou les outils de pare-feu de base n'aideront pas à atténuer une attaque de ce type.

R**eplay**: L'acteur de la menace réutilise les paquets qui ont déjà été capturés dans une conversation, dans le but de contourner la connexion, généralement.

Contre-mesure : en s'assurant que chaque paquet utilise un horodatage et en protégeant également l'intégrité des paquets avec l'utilisation d'IPsec, par exemple, cette activité ne serait pas possible.

Empoisonnement ARP/DNS : L'ARP (Address Resolution Protocol) associe les adresses MAC aux adresses IP. L'empoisonnement ARP implique la falsification de la table ARP, où se trouvent les relations MAC à IP. Le résultat peut être une attaque man-in-the-middle, un déni de service ou une attaque MAC flodding. Dans l'empoisonnement DNS, l'attaquant modifie l'enregistrement IP d'un domaine spécifique dans le cache DNS et redirige le trafic vers un site illégitime.

Contre-mesure : ARP étant un protocole très peu sécurisé (mais dont nous avons besoin pour que le réseau fonctionne correctement), il existe des outils de sécurité qui suivent la relation des entrées dans la table ARP, située sur les systèmes eux-mêmes. C'est une approche similaire en ce qui concerne le DNS - l'intégrité du cache sur le serveur et le client est importante.

Déni de service : Le but principal d'une attaque DoS (Denial-of service) est de perturber les services de la victime en rendant le système inopérable. Exemples d'attaques DoS : smurf, fraggle, ping flood, SYN flood, teardrop. Cela peut également se produire au niveau de l'ordinateur, avec l'utilisation d'un débordement de tampon.

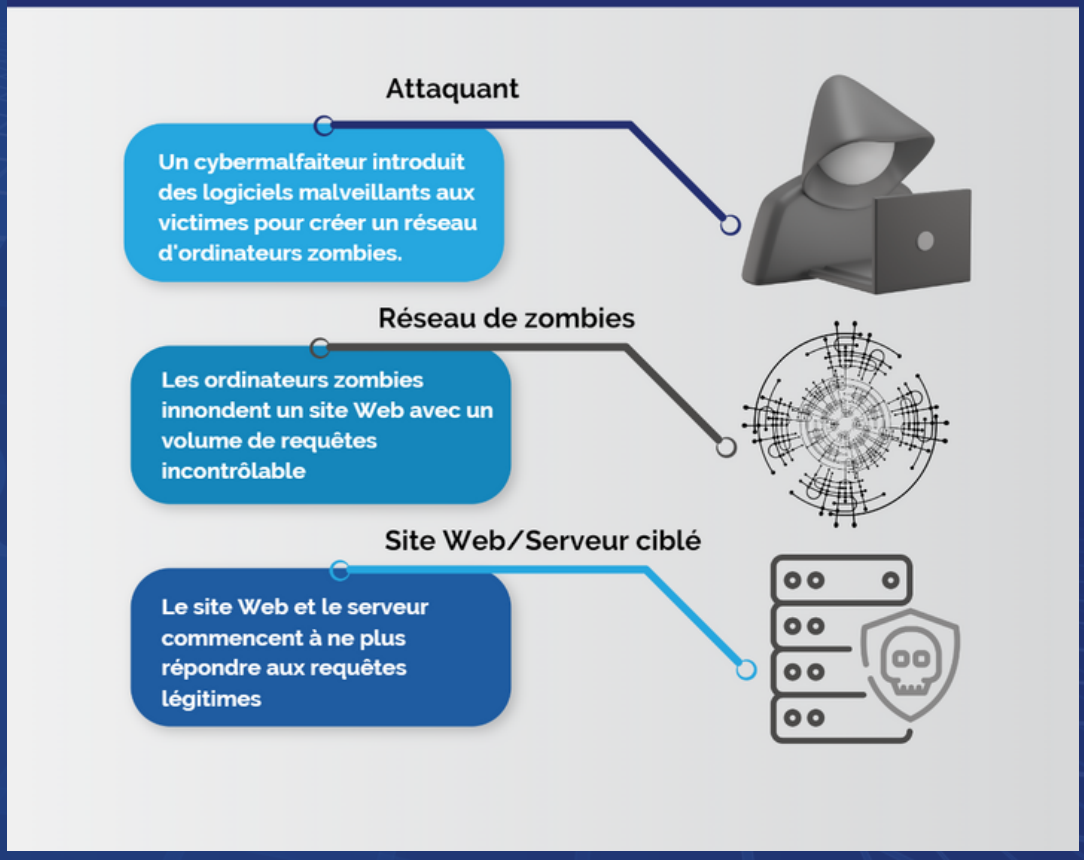
Contre-mesure : Des dispositifs de sécurité réseau et informatique peuvent être utiles, par exemple des pares-feux puissants, des systèmes de détection d'intrusion, mais aussi une stratégie pour minimiser l'exposition d'un système au monde extérieur, limitant la possibilité de trouver une vulnérabilité pour ce type d'attaque.

Déni de service distribué - Un attaquant crée son "armée" d'ordinateurs zombies en y déployant un logiciel malveillant, puis utilise ces systèmes pour attaquer la victime. Une attaque DDoS est plus massive, l'objectif étant de neutraliser le serveur ou le site Web de la victime en le submergeant de fausses requêtes, empêchant ainsi le traitement des requêtes légitimes.

Contre-mesure : Nous pouvons compter sur les fournisseurs de services Internet qui peuvent bloquer certaines adresses IP pour nous atteindre via un processus de liste noire, ou acquérir du matériel spécialisé qui utilisera son intelligence pour bloquer le trafic réseau indésirable. Cependant, c'est souvent une combinaison de plusieurs contre-mesures qui sera globalement la meilleure technique de prévention.

LES ATTAQUES DDOS EXPLIQUÉES

Une attaque DDoS se produit lorsqu'un pirate utilise un réseau zombie pour inonder un site Web/serveur de traffic ou de demandes jusqu'à ce qu'il se bloque.



Attaques sans fil

Les réseaux sans fil sont sujets aux mêmes types d'attaques que ceux qui existent sur les réseaux câblés : attaques de l'intercepteur, déni de service, rejeu des trames. Mais, les réseaux sans fil présentent des problèmes de sécurité supplémentaires qui peuvent empêcher leur utilisation. En général, étant donné que le signal est diffusé dans l'air, la contention des informations qui circulent dans l'air est plus difficile à réaliser.

Brouillage : Il s'agit d'une attaque qui vise la disponibilité du service. Quelqu'un réglera ses appareils pour qu'ils fonctionnent à la même fréquence que les vôtres, ce qui rendra plus difficile l'accès de vos clients à votre antenne et aura un lien fiable. Il s'agit essentiellement d'interférences à son niveau le plus élevé.

Contre-mesure : Assurez-vous d'une inspection physique de la zone où se trouvent vos points d'accès d'entreprise. Vous pouvez également utiliser des outils pour trouver des appareils inconnus.

Point d'accès non autorisé : Un appareil non autorisé utilisé pour se présenter comme un point d'accès légitime, auquel les clients peuvent se connecter. Cela peut être utilisé pour une attaque de l'homme du milieu. Cela contournerait également les politiques de sécurité de l'entreprise et exposerait l'appareil à devenir moins sécurisé.

Contre-mesure : Comme pour le brouillage, il est important d'identifier physiquement les appareils qui ne sont pas gérés par l'entreprise. Il est également possible d'utiliser un appareil pour cartographier les emplacements physiques de ces appareils malveillants et leur envoyer un signal d'arrêt.

Evil twin : En raison d'une force de signal plus élevée, un client peut choisir un point d'accès non autorisé pour se connecter - il devient donc son appareil privilégié. Cet appareil est susceptible de diffuser le même nom de réseau, ce qui rend plus difficile pour l'utilisateur final de voir l'attaque.

Contre-mesure : Une inspection visuelle de la zone est nécessaire, ou l'utilisation d'une étude de site pour détecter ces types d'attaques. De telles attaques peuvent être lancées à partir d'un système conventionnel qui se transforme en point d'accès, ce qui doit donc également être pris en compte lors de l'investigation.

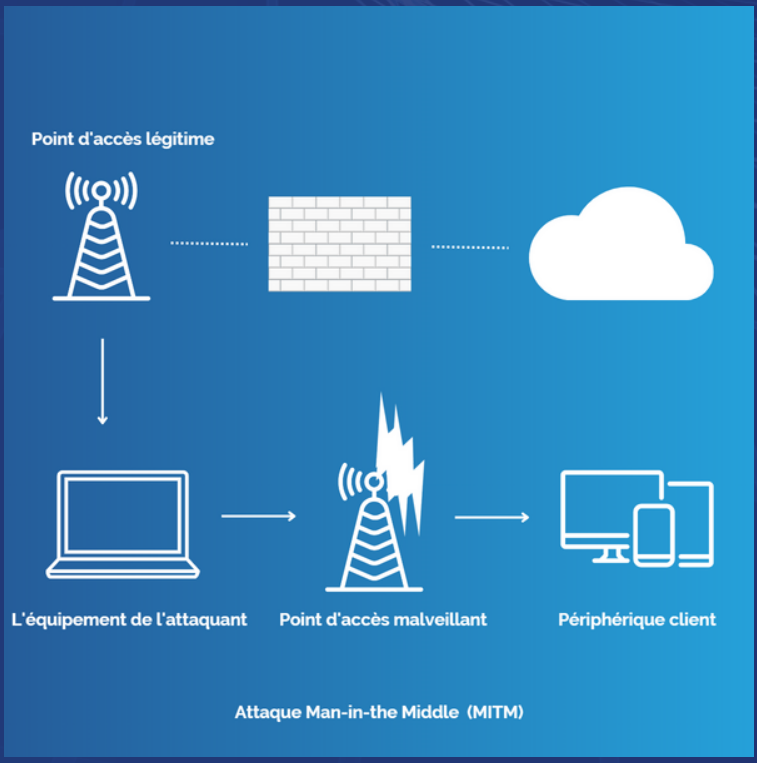
Dissociation ou désauthentification : Ceci vise principalement la disponibilité d'une connexion stable. Le client est continuellement déconnecté et reconnecté à un point d'accès, car un utilisateur malveillant a pu reproduire l'adresse MAC du client légitime, et qu'il utilise pour envoyer de fausses demandes de déconnexion.

Souvent, pour faciliter la connexion par l'utilisateur, une technologie nommée WPS (Wireless Protected Setup) a été introduite. Cependant, des défauts majeurs ont été découverts au fil du temps, donc s'y fier ne serait pas une solution.

Contre-mesure : La mise en place d'un système de détection d'intrusion qui écoute des requêtes spécifiques dans l'air, produites par l'utilisateur malveillant peut aider à détecter l'origine d'une attaque de dissociation ou de désauthentification.

Attaque par relecture ARP (ARP replay) : Une attaque par relecture ARP vise à établir un scénario man-in-the-middle, permettant à l'utilisateur malveillant d'écouter la communication entre les parties. C'est également la base de nombreuses autres attaques sans fil, telles que la découverte d'une clé WEP en corrélation avec des vecteurs d'initialisation (IV).

Contre-mesure : Il est essentiel de mettre en œuvre des systèmes de surveillance et de passer à des algorithmes d'authentification et de cryptage plus performants et plus sécurisés.



Attaques cryptographiques

Avec les attaques cryptographiques, les attaquants tentent de casser des contenus tels que le texte chiffré ou les clés chiffrées. Les mots de passe sont l'un des plus gros problèmes de chaque service informatique d'entreprise. Les utilisateurs ont généralement des mots de passe faciles à mémoriser et même si un service informatique définit des politiques de mots de passe complexes, l'utilisateur écrit ses mots de passe et met les actifs d'une entreprise en danger.

Attaque par dictionnaire : C'est lorsqu'un attaquant utilise un « dictionnaire de mots de passe » pour accéder au système, qui réussit le mieux avec des mots de passe faciles et simples.

Contre-mesure : Implémenter des politiques de mot de passe plus strictes pour vous assurer que le mot de passe n'est pas aussi simple et qu'il est peu probable qu'il se trouve dans un dictionnaire qui peut être obtenu très facilement en ligne.

Attaque par force brute (bruteforce) : Elle utilise la cryptanalyse des algorithmes pour découvrir le mot de passe de l'utilisateur. Pour les mots de passe courts, c'est beaucoup plus rapide que l'attaque par dictionnaire, mais si le mot de passe est très complexe, il faut beaucoup de temps et de puissance de calcul. L'attaque réussit toujours. Cependant, tout est une question de temps - les mots de passe les plus complexes nécessitent des années pour être cassés.

Contre-mesure : Il est important de travailler sur une stratégie pour s'assurer que le mot de passe peut être facilement mémorisé par l'utilisateur, mais comme les caractères spéciaux ou la longueur du mot de passe ont été optimisés, il faudrait beaucoup de temps pour que la force brute réussisse.

Attaque hybride : Il s'agit essentiellement d'une attaque par dictionnaire, mais les lettres sont échangées avec des chiffres pour essayer de déchiffrer les substitutions simples que quelqu'un peut faire en utilisant un mot de passe (S pour 5, 0 pour o, etc.).

Contre-mesure : Assurez-vous que la stratégie de mot de passe protège des mots de passe simples, ainsi que de leurs variantes.

Attaque d'anniversaire : Elle exploite le paradoxe de l'anniversaire - la probabilité de trouver deux entrées avec la même valeur de hachage.

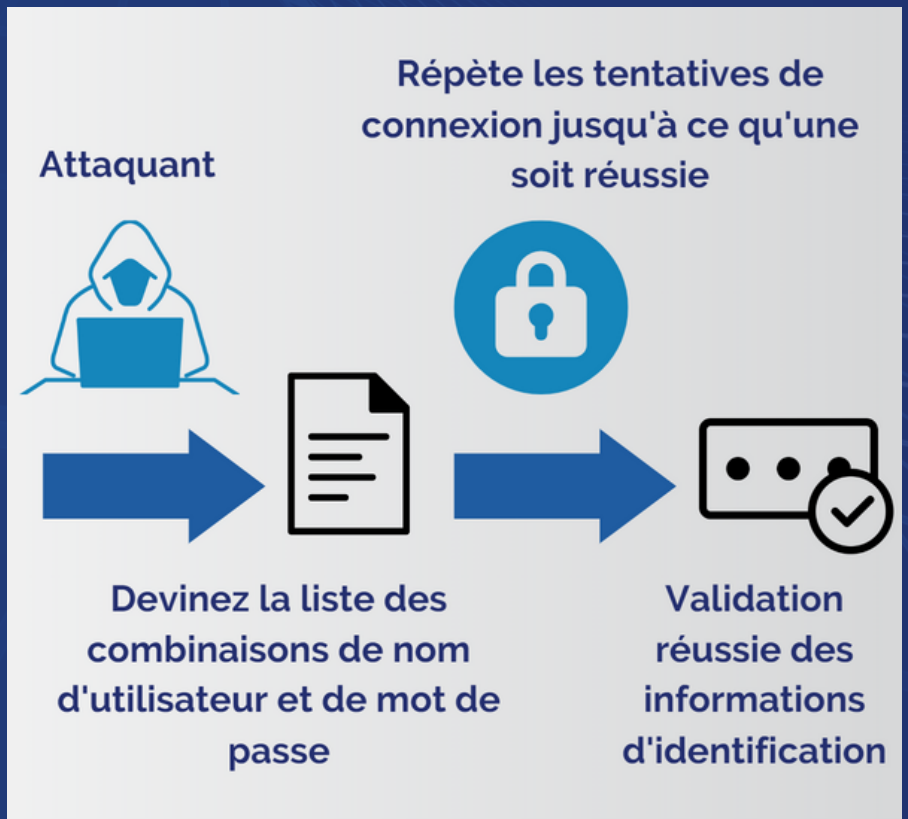
Contre-mesure : Les anciens algorithmes de hachage ou cryptographiques peuvent être plus à risque. Ainsi, les améliorer et les mettre à niveau peut aider à prévenir de telles attaques.

Attaque rainbow table : Une très grande base de données de valeurs de hachage précalculées pour chaque combinaison de caractères existe avec deux colonnes - le mot de passe en clair, ainsi que sa valeur de hachage. Un attaquant saisit la valeur de hachage (volée) et s'attend à ce que l'équivalent sous sa forme de texte en clair soit affiché.

Contre-mesure : La technique du salting fonctionne, car deux valeurs de texte en clair ne seront pas égales au même hachage.

Attaques de rétrogradation : Elles obligent l'ordinateur à abandonner un protocole plus sûr pour un protocole plus ancien et moins sûr (pour maintenir la compatibilité avec les logiciels plus anciens), ce qui permet à l'attaquant d'exploiter les vulnérabilités d'un protocole plus ancien (par exemple, SSL par rapport à TLS).

Contre-mesure : L'utilisation de suites de chiffrement fortes, permettant l'authentification multi facteur (MFA), etc.



ÉTAPES CLÉS D'UNE ATTAQUE PAR FORCE BRUTE

Parcours de formations relatifs à cette écriture:

CompTIA Security+ (CT8742)

CompTIA CySA+ (Cybersecurity Analyst) (CT8742)

Cybersecurity Bootcamp (CS8524)

Certified Ethical Hacker (CEHv12) (EC6154)

ECCENTRIX

CONTACTEZ-NOUS

1-888-718-9732

www.eccentrix.ca

info@eccentrix.ca