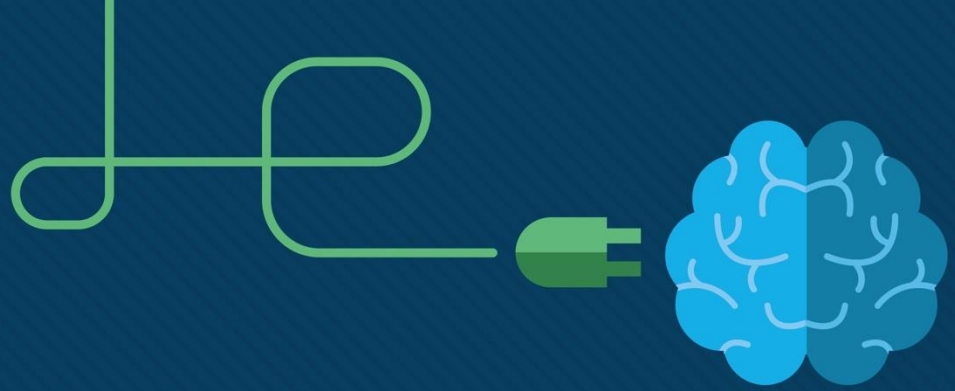
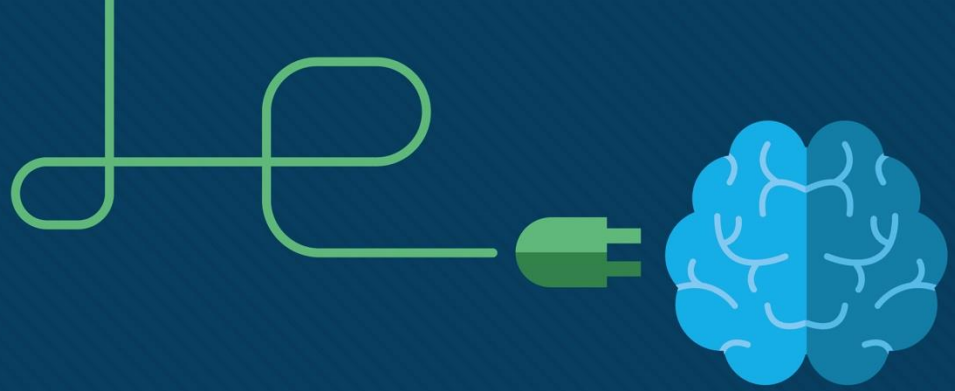


Module 3: Concepts de sécurité des réseaux

Matériel de l'instructeur

Réseau, Sécurité et Automatisation D'entreprise v7.0 (ENSA)



Module 3: Concepts de sécurité des réseaux

Réseau, Sécurité et Automatisation D'entreprise v7.0 (ENSA)

Objectifs du module

Module 3: Concepts de sécurité des réseaux

Objectif du module: Expliquer comment les vulnérabilités, les menaces et les attaques peuvent être atténuer pour renforcer la sécurité du réseau.

Titre du rubrique	Objectif du rubrique
État actuel de la cybersécurité:	Décrire l'état actuel de la cybersécurité et les vecteurs de perte de données.
Acteurs de menace	Décrire les outils utilisés par les acteurs de menace pour attaquer les réseaux.
Logiciel malveillant	Décrire les types des Logiciels malveillants.
Attaques réseau courantes	Décrire les attaques réseau courantes.
Menaces et vulnérabilités liées au protocole IP	Expliquer comment les vulnérabilités liées au protocole IP sont exploitées par les acteurs de menace.
Vulnérabilités liées aux protocoles TCP et UDP	Expliquer comment les vulnérabilités liées aux protocoles TCP et UDP sont exploitées par les acteurs de menace.
Services IP	Expliquer comment les services IP sont exploités par les acteurs de menace.
Meilleures pratiques de sécurité réseau	Décrire les meilleures pratiques de protection d'un réseau.
Cryptographie	Décrire les processus cryptographiques courants utilisés pour protéger les données en transit.

Déclaration de piratage éthique

- Dans ce module, les apprenants peuvent être exposés à des outils et des techniques dans un environnement de machine virtuelle «sandboxed» pour démontrer divers types de cyberattaques. L'expérimentation de ces outils, techniques et ressources est à la discrétion de l'instructeur et de l'institution locale. Si l'apprenant envisage d'utiliser des outils d'attaque à des fins éducatives, il doit contacter son instructeur avant toute expérimentation.
- L'accès non autorisé aux données, aux ordinateurs et aux systèmes de réseau est un crime dans de nombreuses juridictions et s'accompagne souvent de graves conséquences, quelles que soient les motivations de l'auteur. Il est de la responsabilité de l'apprenant, en tant qu'utilisateur de ce matériel, de connaître et de respecter les lois sur l'utilisation des ordinateurs.

3.1 État actuel de la cybersécurité:

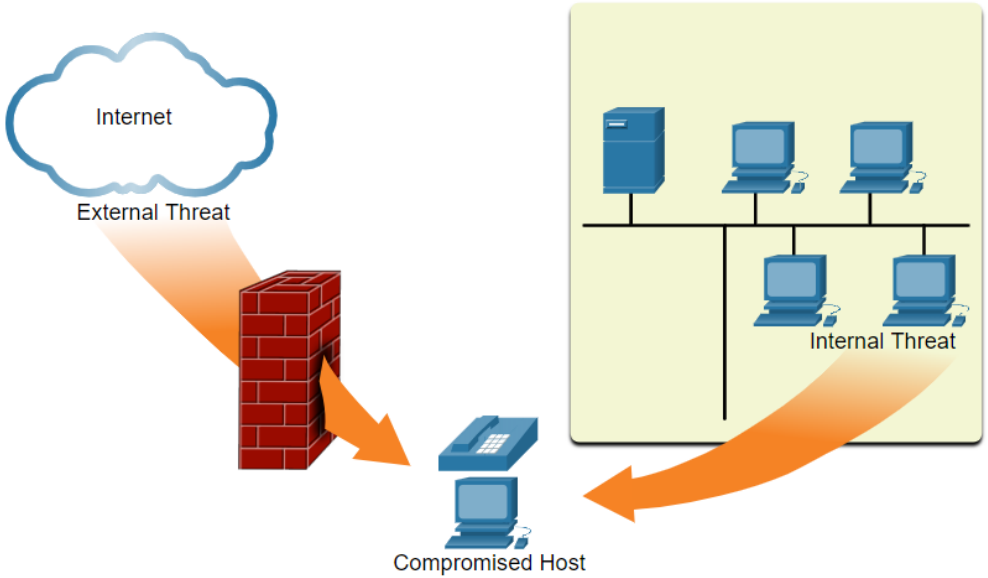
État actuel des affaires

- Les cybercriminels disposent désormais de l'expertise et des outils nécessaires pour éliminer les infrastructures et les systèmes critiques. Leurs outils et techniques continuent d'évoluer.
- Le maintien d'un réseau sécurisé garantit la sécurité des utilisateurs du réseau et protège les intérêts commerciaux. Tous les utilisateurs doivent connaître les termes de sécurité du tableau.

Termes de sécurité	Description
Atouts	Un atout est tout ce qui a de la valeur pour l'organisation. Cela comprend les personnes, l'équipement, les ressources et les données.
Vulnérabilité	Une vulnérabilité est une faiblesse d'un système, ou de sa conception, qui pourrait être exploitée par une menace.
Menace	Une menace est un danger potentiel pour les actifs, les données ou les fonctionnalités réseau d'une entreprise.
Exploiter	Un exploit est un mécanisme qui tire parti d'une vulnérabilité.
Atténuation	L'atténuation est la contre-mesure qui réduit la probabilité ou la gravité d'une menace ou d'un risque potentiel. La sécurité du réseau implique plusieurs techniques d'atténuation.
Risque	Le risque est la probabilité qu'une menace exploite la vulnérabilité d'un actif, dans le but d'affecter négativement une organisation. Le risque est mesuré en utilisant la probabilité de survenance d'un événement et ses conséquences.

Vecteurs d'attaques réseau

- Un vecteur d'attaque est un chemin par lequel un acteur de menace peut accéder à un serveur, un hôte ou un réseau. Les vecteurs d'attaque proviennent de l'intérieur ou de l'extérieur du réseau d'entreprise, comme le montre la figure.
- Les menaces internes ont le potentiel de causer des dommages plus importants que les menaces externes car les utilisateurs internes ont un accès direct au bâtiment et à ses équipements d'infrastructure.



Perte de données

La perte ou l'exfiltration de données se produit lorsque les données sont intentionnellement ou involontairement perdues, volées ou divulguées au monde extérieur. La perte de données peut entraîner:

- Dommages à la marque et perte de réputation
- Perte d'avantage concurrentiel
- Perte de clients
- Perte de revenus
- Litiges/actions en justice entraînant des amendes et des sanctions civiles
- Coûts et efforts importants pour informer les parties concernées et se remettre de la violation

Les professionnels de la sécurité réseau doivent protéger les données de l'organisation. Divers contrôles de prévention des pertes de données (DLP) doivent être mis en œuvre qui combinent des mesures stratégiques, opérationnelles et tactiques.

Perte de données (suite)

Vecteurs de perte de données	Description
Courriel / Réseaux sociaux	Les e-mails ou les messages instantanés interceptés peuvent être capturés et révéler des informations confidentielles.
Appareils non chiffrés	Si les données ne sont pas stockées à l'aide d'un algorithme de cryptage, le voleur peut récupérer des données confidentielles précieuses.
Périphériques de stockage cloud	Les données sensibles peuvent être perdues si l'accès au cloud est compromis en raison de faibles paramètres de sécurité.
Supports amovibles	L'un des risques est qu'un employé puisse effectuer un transfert non autorisé de données vers une clé USB. Un autre risque est la perte d'une clé USB contenant de précieuses données d'entreprise.
Copie conforme	Les données confidentielles doivent être déchiquetées lorsqu'elles ne sont plus nécessaires.
Contrôle d'accès incorrect	Les mots de passe ou les mots de passe faibles qui ont été compromis peuvent fournir à un acteur de la menace un accès facile aux données de l'entreprise.

3.2 Acteurs de menace

Le pirate

Pirate est un terme commun utilisé pour décrire un acteur de menace

Type de pirate	Description
Pirates au chapeau blanc	Il s'agit de pirates éthiques qui utilisent leurs compétences en matière de programmation à des fins bénéfiques, éthiques et légales. Les vulnérabilités de sécurité sont signalées aux développeurs afin qu'ils les corrigent avant qu'elles ne puissent être exploitées.
Pirates au chapeau gris	Il s'agit de personnes qui commettent des délits et dont l'éthique est discutable, mais qui ne le font pas pour leur gain personnel ou pour causer des dommages. Les hackers au chapeau gris peuvent dévoiler une vulnérabilité à l'entreprise affectée après avoir compromis son réseau.
Pirates au chapeau noir	Ce sont des criminels contraires à l'éthique qui compromettent la sécurité des ordinateurs et des réseaux à des fins personnelles ou pour des raisons malveillantes, telles que des attaques de réseaux.

L'évolution des pirates

Le tableau affiche les termes de piratage modernes et une brève description de chacun.

Terme de piratage	Description
Les script kiddies (hackers néophytes)	Ce sont des adolescents ou des pirates informatiques inexpérimentés qui exécutent des scripts, des outils et des exploits existants, pour causer du tort, mais généralement sans but lucratif.
Courtier de vulnérabilité	Ce sont généralement des pirates du chapeau gris qui tentent de découvrir des exploits et de les signaler aux fournisseurs, parfois pour des prix ou des récompenses.
Les hacktivistes	Ce sont des pirates du chapeau gris qui protestent publiquement contre des organisations ou des gouvernements en publiant des articles, des vidéos, des fuites d'informations sensibles et des attaques de réseau.
Cybercriminels	Il s'agit de hackers au chapeau noir qui travaillent à leur compte ou pour de grandes organisations de piratage informatique.
Sponsorisé par l'État	Ils peuvent être vus comme des hackers en chapeau blanc ou en chapeau noir qui volent des secrets du gouvernement, collectent des renseignements et sabotent les réseaux. Ils ciblent généralement les gouvernements étrangers, les groupes terroristes et les grandes entreprises. La plupart des pays du monde participent dans une certaine mesure au piratage parrainé par l'État

Cybercriminels

On estime que les cybercriminels volent des milliards de dollars aux consommateurs et aux entreprises. Les cybercriminels opèrent dans une économie souterraine où ils achètent, vendent et échangent des kits d'outils d'attaque, du code d'exploitation zero day, des services de botnet, des chevaux de Troie bancaires, des enregistreurs de frappe et bien plus encore. Ils achètent et vendent également les informations privées et la propriété intellectuelle qu'ils volent. Les cybercriminels ciblent les petites entreprises et les consommateurs, ainsi que les grandes entreprises et des industries entières.

Les hacktivistes

Anonymous et l'armée syrienne électronique sont deux exemples de groupes hacktivistes. Bien que la plupart des groupes hacktivistes ne soient pas bien organisés, ils peuvent causer des problèmes importants aux gouvernements et aux entreprises. Les hacktivistes ont tendance à s'appuyer sur des outils assez simples et disponibles gratuitement.

Pirates sponsorisés par l'État

Les pirates informatiques sponsorisés par l'État créent un code d'attaque avancé et personnalisé, utilisant souvent des vulnérabilités logicielles non découvertes appelées vulnérabilités zero-day. Un exemple d'attaque parrainée par l'État concerne le malware Stuxnet qui a été créé pour endommager les capacités d'enrichissement nucléaire de l'Iran.

3.3 Outils d'acteur de menace

Vidéo - Outils d'acteur de menace

Cette vidéo couvrira les points suivants:

- Expliquer les outils de test de pénétration
- Expliquez les types d'attaque

Introduction aux outils d'attaque

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.

Évolution des outils de sécurité

Le tableau présente les catégories d'outils de test de pénétration courants. Remarquez comment certains outils sont utilisés par les chapeaux blancs et les chapeaux noirs. Gardez à l'esprit que la liste n'est pas exhaustive car de nouveaux outils sont toujours en développement.

Outil de test de pénétration	Description
Craqueurs de mots de passe	Les outils de piratage de mot de passe sont souvent appelés outils de récupération de mot de passe et peuvent être utilisés pour casser ou récupérer un mot de passe. Les craqueurs de mot de passe font des suppositions à plusieurs reprises afin de casser le mot de passe. Des exemples d'outils de craquage de mot de passe incluent John the Ripper, Ophcrack, L0phtCrack, THC Hydra, Rainbow Crack et Medusa.
Outils de piratage sans fil	Les outils de piratage sans fil sont utilisés pour pirater intentionnellement un réseau sans fil afin de détecter les vulnérabilités de sécurité. Des exemples d'outils de piratage sans fil incluent Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep et ViStumbler.
Analyse du réseau et outils de piratage	Les outils d'analyse réseau sont utilisés pour sonder les périphériques réseau, les serveurs et les hôtes pour les ports TCP ou UDP ouverts. Des exemples d'outils d'analyse incluent Nmap, SuperScan, Angry IP Scanner et NetScanTools.
Outils de fabrication de paquets	Ces outils sont utilisés pour sonder et tester la robustesse d'un pare-feu à l'aide de paquets forgés spécialement conçus. Les exemples incluent Hping, Scapy, Socat, Yersinia, Netcat, Nping et Nemesis.
Renifleurs de paquets	Ces outils sont utilisés pour capturer et analyser les paquets au sein des réseaux locaux ou WLAN Ethernet traditionnels. Les outils incluent Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy et SSLstrip.

Évolution des outils de sécurité (suite)

Outil de test de pénétration	Description
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. Exemples d'outils: AIDE, Netfilter et PF: OpenBSD Packet Filter.
Fuzzers pour rechercher des vulnérabilités	Les fuzzers sont des outils utilisés par les acteurs de menace pour découvrir les vulnérabilités de sécurité d'un ordinateur. Les exemples de fuzzers incluent Skipfish, Wapiti et W3af.
Outils d'investigation	Ces outils sont utilisés par les pirates du chapeau blanc pour flairer toute trace de preuves existant dans un ordinateur. Des exemples d'outils incluent Sleuth Kit, Helix, Maltego et Encase.
Débogueurs	Ces outils sont utilisés par les hackers au chapeau noir pour inverser l'ingénierie des fichiers binaires lors de l'écriture d'exploits. Ils sont également utilisés par les chapeaux blancs lors de l'analyse des logiciels malveillants. Les outils de débogage incluent GDB, WinDbg, IDA Pro et Immunity Debugger.
Piratage de systèmes d'exploitation	Ce sont des systèmes d'exploitation spécialement conçus préchargés avec des outils optimisés pour le piratage. Des exemples de systèmes d'exploitation de piratage spécialement conçus incluent Kali Linux, BackBox Linux.
Outils de chiffrement	Les outils de chiffrement utilisent des schémas d'algorithmes pour coder les données afin d'empêcher tout accès non autorisé aux données chiffrées. Des exemples de ces outils incluent VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN et Stunnel.
Outils d'exploitation des vulnérabilités	Ces outils identifient si un hôte distant est vulnérable à une attaque de sécurité. Des exemples d'outils d'exploitation de vulnérabilité comprennent Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit et Netsparker.
Analyseurs de vulnérabilité	Ces outils analysent un réseau ou un système pour identifier les ports ouverts. Ils peuvent également être utilisés pour rechercher des vulnérabilités connues et analyser les VM, les dispositifs BYOD et les bases de données des clients. Des exemples d'outils incluent Nipper, Core Impact, Nessus, SAINT et OpenVAS

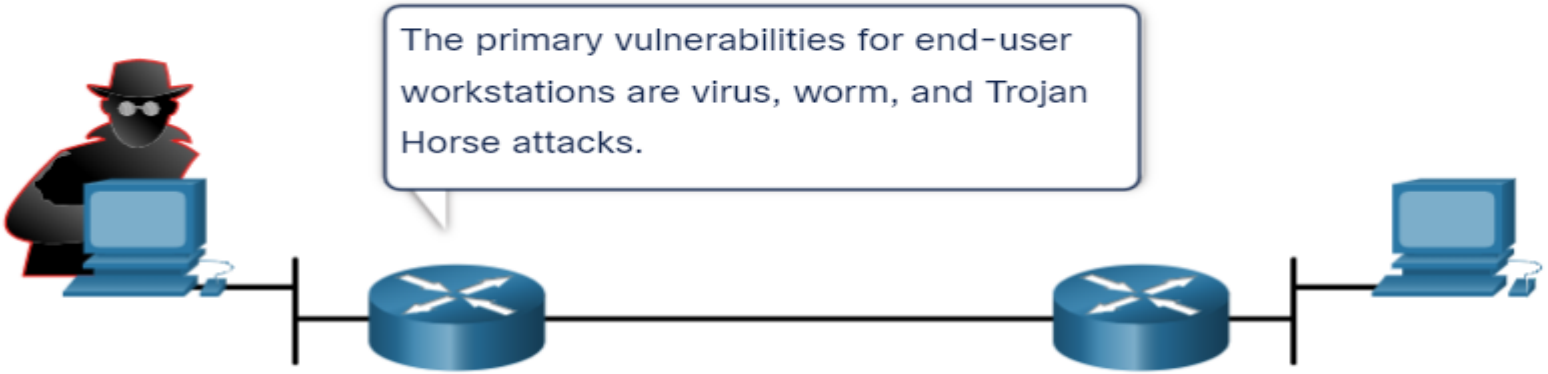
Types d'attaque

Type d'attaque	Description
Attaque d'écoute	C'est à ce moment qu'un acteur de menace capture et «écoute» le trafic réseau. Cette attaque est également appelée reniflement ou surveillance.
Attaque par modification de données	Si les acteurs de menace ont capturé le trafic d'entreprise, ils peuvent modifier les données du paquet à l'insu de l'expéditeur ou du destinataire.
Attaque par usurpation d'adresse IP	Un acteur de menace construit un paquet IP qui semble provenir d'une adresse valide à l'intérieur de l'intranet de l'entreprise.
Attaques basées sur un mot de passe	Si les acteurs de menace découvrent un compte d'utilisateur valide, les acteurs de menace ont les mêmes droits que l'utilisateur réel. Les acteurs de menace peuvent utiliser ce compte valide pour obtenir des listes d'autres utilisateurs, des informations sur le réseau, changer les configurations de serveur et de réseau et modifier, réacheminer ou supprimer des données.
Attaque par déni de service	Une attaque DoS empêche l'utilisation normale d'un ordinateur ou d'un réseau par des utilisateurs valides. Une attaque DoS peut inonder un ordinateur ou l'ensemble du réseau de trafic jusqu'à ce qu'un arrêt se produise en raison de la surcharge. Une attaque DoS peut également bloquer le trafic et donc empêcher les utilisateurs autorisés d'accéder aux ressources du réseau.
Attaque de l'homme-au-milieu	Cette attaque se produit lorsque les acteurs de menace se sont positionnés entre une source et une destination. Ils peuvent désormais surveiller, capturer et contrôler activement la communication de manière transparente.
Attaque à clé compromise	Si un acteur de menace obtient une clé secrète, cette clé est appelée clé compromise. Une clé compromise peut être utilisée pour accéder à une communication sécurisée sans que l'expéditeur ou le destinataire ne soit au courant de l'attaque.
Attaque de renifleur	Un renifleur est une application ou un appareil qui peut lire, surveiller et capturer des échanges de données réseau et lire des paquets réseau. Si les paquets ne sont pas chiffrés, un renifleur fournit une vue complète des données à l'intérieur du paquet

3.4 Logiciel malveillant

Présentation des logiciels malveillants

- Maintenant que vous connaissez les outils utilisés par les pirates, cette rubrique vous présente différents types de logiciels malveillants que les pirates utilisent pour accéder aux terminaux.
- Les terminaux sont particulièrement exposés aux attaques de logiciels malveillants. Il est important de les connaître, car les acteurs de menace comptent sur les utilisateurs pour installer des logiciels malveillants afin d'aider à exploiter les failles de sécurité.



Virus et chevaux de Troie (Trojan Horses)

- Le premier type de programme malveillant, et le plus répandu, est le virus. Les virus nécessitent une action humaine pour se propager et infecter d'autres ordinateurs.
- Le virus se cache en s'attachant au code informatique, aux logiciels ou aux documents sur l'ordinateur. Une fois ouvert, le virus s'exécute et infecte l'ordinateur.
- Les virus peuvent:
  - Modifier, corrompre, supprimer des fichiers ou effacer des disques entiers.
  - Cause des problèmes de démarrage de l'ordinateur et des applications corrompues.
  - Capturer et envoyer des informations sensibles aux acteurs de menace.
  - Accéder et utiliser des comptes de messagerie pour vous propager.
  - Rester en sommeil jusqu'à ce qu'il soit convoqué par l'acteur de menace.

Virus et chevaux de Troie (Trojan Horses) (suite)

Les virus modernes sont développés pour des objectifs spécifiques tels que ceux répertoriés dans le tableau.

Types de virus	Description
Virus du secteur de démarrage	Le virus attaque le secteur de démarrage, la table de partition de fichiers ou le système de fichiers.
Virus de micrologiciel	Le virus attaque le micrologiciel du périphérique.
Virus macro	Le virus utilise la fonctionnalité macro de MS Office de façon malveillante.
Virus de programme	Le virus s'insère dans un autre programme exécutable.
Virus de script	Le virus attaque l'interpréteur du système d'exploitation utilisé pour exécuter des scripts.

Virus et chevaux de Troie (Trojan Horses) (suite)

Les acteurs de menace utilisent des chevaux de Troie pour compromettre les hôtes. Un cheval de Troie est un programme qui semble utile mais qui contient également du code malveillant. Les chevaux de Troie sont souvent fournis avec des programmes en ligne gratuits, tels que des jeux informatiques. Il existe plusieurs types de chevaux de Troie, comme décrit dans le tableau.

Type de cheval de Troie	Description
Accès distant	Le cheval de Troie permet un accès à distance non autorisé.
Envoi de données	Le cheval de Troie fournit à l'acteur de menace des données sensibles, telles que des mots de passe.
Destructeur	Le cheval de Troie corrompt ou supprime des fichiers.
Proxy	Le cheval de Troie utilisera l'ordinateur de la victime comme périphérique source pour lancer des attaques et effectuer d'autres activités illégales.
FTP	Le cheval de Troie permet des services de transfert de fichiers non autorisés sur des dispositifs terminaux.
Désactivation des logiciels de sécurité	Le cheval de Troie empêche les programmes antivirus ou les pare-feu de fonctionner.
Déni de service (DoS)	Le cheval de Troie ralentit ou arrête l'activité du réseau.
Enregistreur de frappe	Le cheval de Troie tente activement de voler des informations confidentielles, telles que les numéros de carte de crédit, en enregistrant les frappes de touches saisies dans un formulaire Web.

Types de Logiciels malveillants

Logiciel malveillant	Description
Logiciel publicitaire (Adware)	•Le logiciel publicitaire est généralement distribué lors du téléchargement de logiciels en ligne. •Les logiciels publicitaires peuvent afficher des publicités non sollicitées à l'aide de fenêtres de navigateur Web contextuelles, de nouvelles barres d'outils ou rediriger de manière inattendue une page Web vers un autre site Web. •Les fenêtres contextuelles sont souvent difficiles à contrôler, car de nouvelles fenêtres contextuelles s'ouvrent plus rapidement que l'utilisateur ne peut les fermer.
Ransomware	•Un ransomware empêche généralement un utilisateur d'accéder à ses fichiers en chiffrant les fichiers, puis en affichant un message demandant une rançon pour la clé de décodage. •Les utilisateurs qui ne disposent pas de sauvegardes à jour doivent payer la rançon pour déchiffrer leurs fichiers. •Le paiement est généralement effectué par virement bancaire ou par des crypto-monnaies telles que Bitcoin.
Rootkit	•Les rootkits sont utilisés par les acteurs de menace pour obtenir un accès administrateur à un ordinateur au niveau du compte. •Ils sont très difficiles à détecter, car ils peuvent modifier le pare-feu, la protection antivirus, les fichiers système et même les commandes du système d'exploitation pour dissimuler leur présence. •Ils peuvent fournir une porte dérobée aux acteurs de menace en leur donnant accès au PC, en leur permettant de télécharger des fichiers et d'installer de nouveaux logiciels à utiliser dans une attaque DDoS. •Des outils spéciaux de suppression de rootkit doivent être utilisés pour les supprimer, ou une réinstallation complète du système d'exploitation peut être nécessaire.
Logiciel espion (Spyware)	•Comme un logiciel de publicité, mais utilisé pour collecter des informations sur l'utilisateur et envoyer aux acteurs de menace sans le consentement de l'utilisateur. •Les logiciels espions peuvent être une menace faible, collectant des données de navigation, ou une menace élevée capturant des informations personnelles et financières.
Ver (Worm)	•Un ver est un programme de réplication automatique qui se propage automatiquement sans intervention de l'utilisateur en exploitant les vulnérabilités des logiciels légitimes. •Il utilise le réseau pour rechercher d'autres victimes ayant la même vulnérabilité. •L'intention d'un ver est généralement de ralentir ou de perturber les opérations réseau.

3.5 Attaques réseau courantes

Présentation des attaques réseau courantes

- Lorsque des logiciels malveillants sont livrés et installés, la charge utile peut être utilisée pour provoquer diverses attaques liées au réseau.
- Pour atténuer les attaques, il est utile de comprendre les types d'attaques. En catégorisant les attaques de réseau, il est possible de traiter des types d'attaques plutôt que des attaques individuelles.
- Les réseaux sont sensibles aux types d'attaques suivants:
  - Attaques de reconnaissance
  - Attaques par accès
  - Attaques DoS

Vidéo sur les attaques réseau courantes - Attaques réseau communes

Cette vidéo expliquera les techniques suivantes utilisées dans une attaque de reconnaissance:

- Effectuer une requête d'informations sur une cible
- Lancer un balayage ping du réseau cible
- Lancer une analyse de port des adresses IP actives
- Exécuter des scanners de vulnérabilité
- Exécuter des outils d'exploitation

Attaques de reconnaissance

- La reconnaissance est la collecte d'informations.
- Les acteurs de menace utilisent des attaques de reconnaissance (ou recon) pour effectuer la découverte et la cartographie non autorisées de systèmes, de services ou de vulnérabilités. Les attaques Recon précèdent les attaques d'accès ou les attaques DoS.

Attaques de reconnaissance (suite)

Certaines des techniques utilisées par les acteurs de menace malveillants pour mener des attaques de reconnaissance sont décrites dans le tableau.

Technique	Description
Exécuter une requête d'information sur une cible	L'acteur de menace recherche les premières informations sur une cible. Divers outils peuvent être utilisés, notamment la recherche Google, le site Web des organisations, le whois, etc.
Lancer un balayage ping du réseau cible	La requête d'informations révèle généralement l'adresse réseau de la cible. L'acteur de menace peut désormais lancer un balayage ping pour déterminer quelles adresses IP sont actives.
Lancer l'analyse des ports des adresses IP actives	Ceci est utilisé pour déterminer quels ports ou services sont disponibles. Exemples d'analyseurs de ports: Nmap, SuperScan, Angry IP Scanner et NetScanTools.
Exécuter des scanners de vulnérabilité	Il s'agit d'interroger les ports identifiés pour déterminer le type et la version de l'application et du système d'exploitation qui s'exécutent sur l'hôte. Des exemples d'outils incluent Nipper, Core Impact, Nessus, SAINT et Open VAS.
Exécuter des outils d'exploitation	L'acteur de menace tente maintenant de découvrir des services vulnérables qui peuvent être exploités. Des exemples d'outils d'exploitation de vulnérabilité comprennent Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit et Netsparker.

Vidéo sur les attaques réseau courantes- Accès et attaques d'ingénierie sociale

Cette vidéo couvrira les points suivants:

- Techniques utilisées dans les attaques d'accès (password attacks, spoofing attacks, trust exploitations, port redirections, man-in-the-middle attacks, buffer overflow attacks)
- Techniques utilisées dans les attaques d'ingénierie sociale (pretesting, phishing, spear phishing, spam, something for something, baiting, impersonation, tailgating, shoulder surfing, dumpster diving)

Attaques d'accès

- Les attaques par accès exploitent les vulnérabilités connues des services d'authentifications, services FTP et services web pour accéder à des comptes web, des bases de données confidentielles ou accéder à d'autres ressources. Le but de ces types d'attaques est d'accéder à des comptes Web, à des bases de données confidentielles et à d'autres informations sensibles.
- Les acteurs de menace utilisent des attaques d'accès sur les périphériques réseau et les ordinateurs pour récupérer des données, y accéder ou pour augmenter les privilèges d'accès au statut d'administrateur.
- **Attaques par mot de passe:** lors d'une attaque par mot de passe, l'acteur de la menace tente de découvrir des mots de passe système critiques en utilisant diverses méthodes. Les attaques par mot de passe sont très courantes et peuvent être lancées à l'aide d'une variété d'outils de craquage de mot de passe.
- **Attaques d'usurpation d'identité:** lors d'attaques d'usurpation d'identité, le dispositif d'acteur de menace tente de se faire passer pour un autre appareil en falsifiant des données. Les attaques d'usurpation d'identité courantes incluent l'usurpation d'adresse IP, l'usurpation d'adresse MAC et l'usurpation d'identité DHCP. Ces attaques d'usurpation seront discutées plus en détail plus loin dans ce module
- Les autres attaques d'accès incluent:
  - Exploiter la confiance
  - Redirection de port
  - Attaques de l'homme-au-milieu
  - Attaques par débordement de la mémoire tampon

Attaques d'ingénierie sociale

- L'ingénierie sociale est une attaque d'accès qui tente de manipuler des individus pour effectuer des actions ou divulguer des informations confidentielles. Certaines techniques d'ingénierie sociale sont réalisées en personne tandis que d'autres peuvent utiliser le téléphone ou Internet.
- Les ingénieurs sociaux comptent souvent sur la volonté des gens d’être utiles. Ils exploitent également les faiblesses des gens.

Attaques d'ingénierie sociale (suite)

Attaque d'ingénierie sociale	Description
Prétexte	Un acteur de menace prétend avoir besoin de données personnelles ou financières pour confirmer l'identité du destinataire.
Hameçonnage (Phishing)	Un acteur de menace envoie un e-mail frauduleux déguisé en une source légitime et fiable pour inciter le destinataire à installer un logiciel malveillant sur son appareil ou pour partager des informations personnelles ou financières.
Hameçonnage ciblé	Un acteur de menace crée une attaque de phishing ciblée adaptée à un individu ou une organisation spécifique.
Courrier indésirable (spam)	Également connu sous le nom de courrier indésirable, il s'agit d'un courrier électronique non sollicité qui contient souvent des liens nuisibles, des logiciels malveillants ou du contenu trompeur.
Contrepartie (Something for Something)	Parfois appelé «Quid pro quo», c'est lorsqu'un acteur de menace demande des informations personnelles à une partie en échange de quelque chose comme un cadeau.
Appâtage	Un acteur de menace laisse un lecteur flash infecté par un logiciel malveillant dans un lieu public. Une victime trouve le lecteur et l'insère sans méfiance dans son ordinateur portable, installant involontairement des logiciels malveillants.
Usurpation d'identité	Ce type d'attaque est l'endroit où un acteur de menace prétend être quelqu'un qu'il ne doit pas gagner la confiance d'une victime.
Accès non autorisé (Tailgating)	C'est là qu'un acteur de menace suit rapidement une personne autorisée dans un endroit sécurisé pour accéder à une zone sécurisée.
Espionnage par-dessus l'épaule (Shoulder Surfing)	C'est là qu'un acteur de menace regarde discrètement par-dessus l'épaule de quelqu'un pour voler ses mots de passe ou d'autres informations.
Fouille de poubelles (Dumpster Diving)	C'est là qu'un acteur de menace fouille dans des poubelles pour découvrir des documents confidentiels

Attaques d'ingénierie sociale (suite)

- Le Social Engineering Toolkit (SET) a été conçu pour aider les pirates informatiques et autres professionnels de la sécurité des réseaux à créer des attaques d'ingénierie sociale pour tester leurs propres réseaux.
- Les entreprises doivent éduquer leurs utilisateurs sur les risques de l'ingénierie sociale et développer des stratégies pour valider les identités par téléphone, par e-mail ou en personne.
- La figure montre les pratiques recommandées qui devraient être suivies par tous les utilisateurs.

Travaux pratiques – Ingénierie sociale

Au cours de ce TP, vous rechercherez des exemples d'ingénierie sociale et identifierez des façons de les reconnaître et de les contrer.

Vidéo –Attaques par déni de service

Cette vidéo couvrira les points suivants:

- Techniques utilisées dans les attaques par déni de service (quantité écrasante de trafic, paquets formatés de manière malveillante)
- Techniques utilisées dans les attaques par déni de service distribué (zombies)

Attaques DoS et DDoS

- Une attaque par déni de service (DoS) crée une sorte d'interruption des services réseau pour les utilisateurs, les appareils ou les applications. Il existe deux principaux types d'attaques DoS:
  - **Quantité écrasante de trafic** - L'acteur de menace envoie une énorme quantité de données à un débit que le réseau, l'hôte ou l'application ne peut pas gérer. Cela ralentit la transmission et le temps de réponse. Il peut également planter un appareil ou un service.
  - **Paquets formatés de manière malveillante** -L'acteur de menace envoie un paquet formaté de manière malveillante à un hôte ou une application et le récepteur n'est pas en mesure de le gérer. Cela provoque un ralentissement de l'appareil récepteur ou une panne.
- Les attaques DoS sont un risque majeur car elles interrompent la communication et provoquent une perte de temps et d'argent importante. Ces attaques sont relativement simples à mener, même par un acteur de menace non qualifié.
- Une attaque DoS distribuée (DDoS) est similaire à une attaque DoS, mais elle provient de plusieurs sources coordonnées.

3.6 Vulnérabilités et menaces IP

Vidéo sur les vulnérabilités et menaces IP - Attaques IP et ICMP courantes

Cette vidéo couvrira les points suivants:

- Techniques utilisées dans les attaques IP (attaques ICMP, attaques d'amplification et de réflexion, attaques d'usurpation d'adresse, attaques homme-au-milieu, détournement de session)
- Techniques utilisées dans les attaques ICMP (demande d'écho ICMP et réponse d'écho, ICMP inaccessible, réponse de masque ICMP, redirections ICMP, découverte de routeur ICMP)

IPv4 et IPv6

- l'IP ne valide pas si l'adresse IP source contenue dans un paquet provient réellement de cette source. Pour cette raison, les acteurs de menace peuvent envoyer des paquets à l'aide d'une adresse IP source usurpée. Les analystes de sécurité doivent comprendre les différents champs des en-têtes IPv4 et IPv6.
- Certaines des attaques liées à l'IP les plus courantes sont présentées dans le tableau

Techniques d'attaque IP	Description
Attaques ICMP	Les acteurs de menace utilisent des paquets d'écho (ping) ICMP (Internet Control Message Protocol) pour découvrir les sous-réseaux et les hôtes sur un réseau protégé, pour générer des attaques par inondation DoS et pour modifier les tables de routage des hôtes.
Amplification et attaques par réflexion	Les acteurs de menace tentent d'empêcher les utilisateurs légitimes d'accéder aux informations ou aux services à l'aide d'attaques DoS et DDoS.
Attaques par usurpation d'adresse	Les acteurs de menace usurpent l'adresse IP source dans un paquet IP pour effectuer une usurpation aveugle ou une usurpation non aveugle.
Attaques de l'homme-au-milieu (MITM)	Les acteurs de menace se positionnent entre une source et une destination pour surveiller, capturer et contrôler de manière transparente la communication. Ils pourraient espionner en inspectant les paquets capturés, ou modifier les paquets et les transmettre à leur destination d'origine.
Détournement de session	Les acteurs de menace accèdent au réseau physique, puis utilisent une attaque MITM pour détourner une session

Attaques ICMP

- Les acteurs de menace utilisent ICMP pour les attaques de reconnaissance et de scan. Ils peuvent lancer des attaques de collecte d'informations pour cartographier une topologie de réseau, découvrir quels hôtes sont actifs (accessibles), identifier le système d'exploitation hôte (empreinte du système d'exploitation) et déterminer l'état d'un pare-feu. Les acteurs de menace utilisent également ICMP pour les attaques DoS.
- **Remarque**: ICMP pour IPv4 (ICMPv4) et ICMP pour IPv6 (ICMPv6) sont sensibles à des types d'attaques similaires.
- Les réseaux doivent avoir un filtrage strict de la liste de contrôle d'accès (ACL) ICMP sur la périphérie du réseau pour éviter les sondages ICMP à partir d'Internet. Dans le cas de grands réseaux, les dispositifs de sécurité tels que les pare-feu et les systèmes de détection d'intrusion (IDS) détectent de telles attaques et génèrent des alertes aux analystes de sécurité.

Attaques ICMP (suite)

Les messages communs d'ICMP qui intéressent les acteurs de menace sont énumérés dans le tableau.

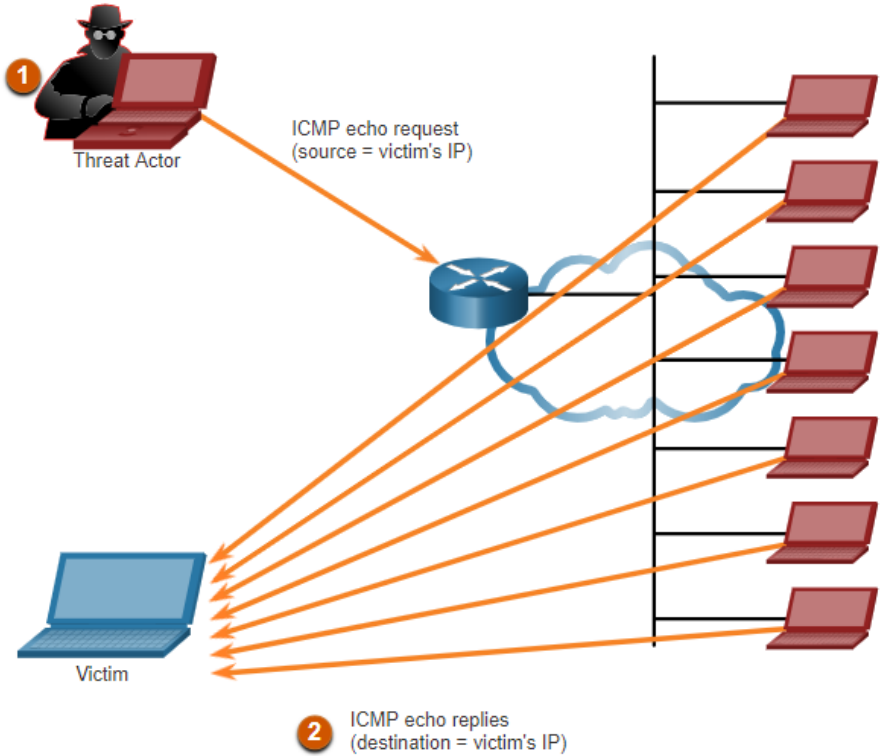
Messages ICMP utilisés par les pirates	Description
Demande d'écho ICMP et réponse d'écho	Ceci est utilisé pour effectuer une vérification de l'hôte et des attaques DoS.
ICMP inaccessible	Il est utilisé pour effectuer des attaques de reconnaissance et de balayage de réseau.
Réponse de masque ICMP	Ceci est utilisé pour mapper un réseau IP interne.
Redirection ICMP	Ceci est utilisé pour attirer un hôte cible dans l'envoi de tout le trafic via un appareil compromis et créer une attaque MITM.
Découverte du routeur ICMP	Ceci est utilisé pour injecter des entrées de route fausses dans la table de routage d'un hôte cible.

Vidéo sur les vulnérabilités et les menaces IP - Attaque d'amplification, de réflexion et d'usurpation

Cette vidéo expliquera l'amplification, la réflexion et l'attaque d'usurpation.

Attaques par amplification et réflexion

- Les acteurs de menace utilisent souvent des techniques d'amplification et de réflexion pour créer des attaques DoS. L'exemple de la figure illustre une attaque Smurf utilisée pour submerger un hôte cible.
  - **Remarque**: De nouvelles formes d'attaques d'amplification et de réflexion telles que les attaques de réflexion et d'amplification basées sur DNS et les attaques d'amplification NTP (Network Time Protocol) sont désormais utilisées.
- Les acteurs de menace utilisent également des attaques d'épuisement des ressources pour planter un hôte cible ou pour consommer les ressources d'un réseau.



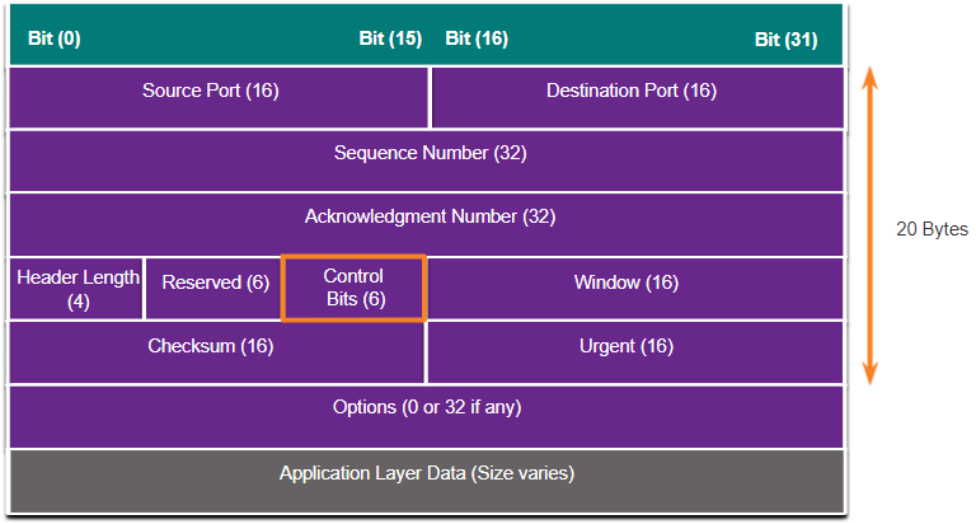
Attaques par usurpation d'adresse

- Les attaques d'usurpation d'adresse IP se produisent lorsqu'un acteur de menace crée des paquets contenant de fausses informations d'adresse IP source pour masquer l'identité de l'expéditeur ou pour se faire passer pour un autre utilisateur légitime. L'usurpation d'identité est généralement intégrée à une autre attaque telle qu'une attaque de Smurf.
- Les attaques d'usurpation d'identité peuvent être non aveugles ou aveugles:
  - **Usurpation d'identité non aveugle** - L'acteur de menace peut voir le trafic qui est envoyé entre l'hôte et la cible. L'usurpation non aveugle détermine l'état d'un pare-feu et la prédiction du numéro de séquence. Il peut également détourner une session autorisée.
  - **Usurpation aveugle** - L'acteur de menace ne peut pas voir le trafic envoyé entre l'hôte et la cible. L'usurpation aveugle est utilisée dans les attaques DoS.
- Les attaques d'usurpation d'adresse MAC sont utilisées lorsque les acteurs de menace ont accès au réseau interne. Les acteurs de menace modifient l'adresse MAC de leur hôte pour correspondre à une autre adresse MAC connue d'un hôte cible.

3.7 Vulnérabilités TCP et UDP

En-tête de segment TCP

- Les informations de segment TCP apparaissent immédiatement après l'en-tête IP. Les champs du segment TCP et les drapeaux du champ Control Bits sont affichés sur la figure.
- Voici les six bits de contrôle du segment TCP:
  - **URG** - Champ de pointeur urgent significatif (Urgent pointer field significant)
  - **ACK** - Champ d'acquittement significatif (Acknowledgment field significant)
  - **PSH** - Fonction push (Push function)
  - **RST**- -Réinitialiser la connexion
  - **SYN** -Synchroniser les numéros de séquence
  - **FIN** - Plus de données de l'expéditeur



Services TCP

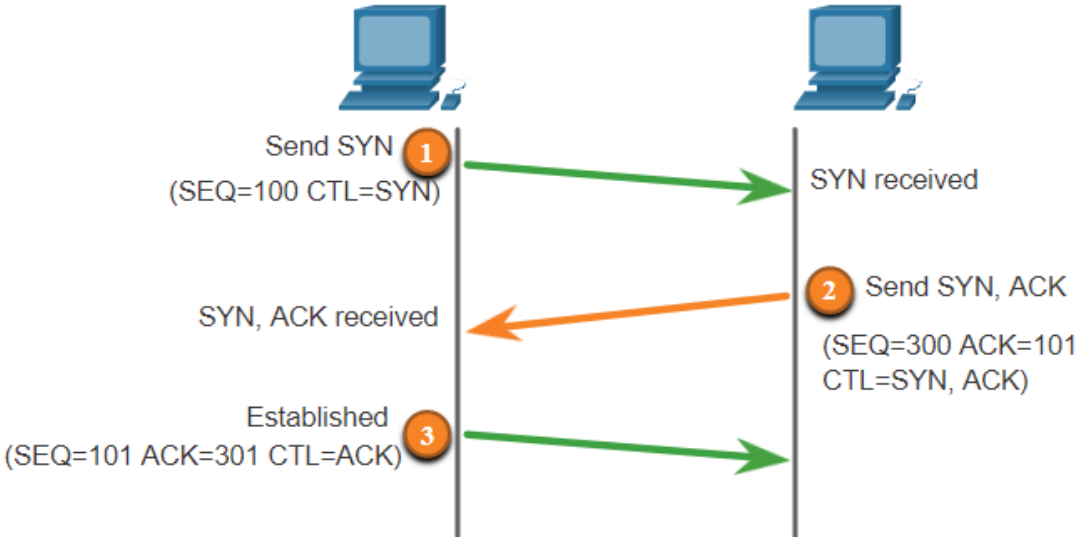
TCP fournit ces services:

- **Livraison fiable** - TCP intègre des remerciements pour garantir la livraison. Si un accusé de réception en temps opportun n'est pas reçu, l'expéditeur retransmet les données. La demande d'accusé de réception des données reçues peut entraîner des retards importants. Des exemples de protocoles de couche d'application qui utilisent la fiabilité TCP incluent HTTP, SSL / TLS, FTP, les transferts de zone DNS et autres.
- **Contrôle de flux** - TCP implémente un contrôle de flux pour résoudre ce problème. Plutôt que d'accuser la réception d'un segment à la fois, plusieurs segments peuvent être acquittés avec un seul segment d'accusé de réception.
- **Communication avec état** - La communication avec état TCP entre deux parties se produit pendant la prise de contact à trois voies TCP.

Services TCP (suite)

Une connexion TCP est établie en trois étapes :

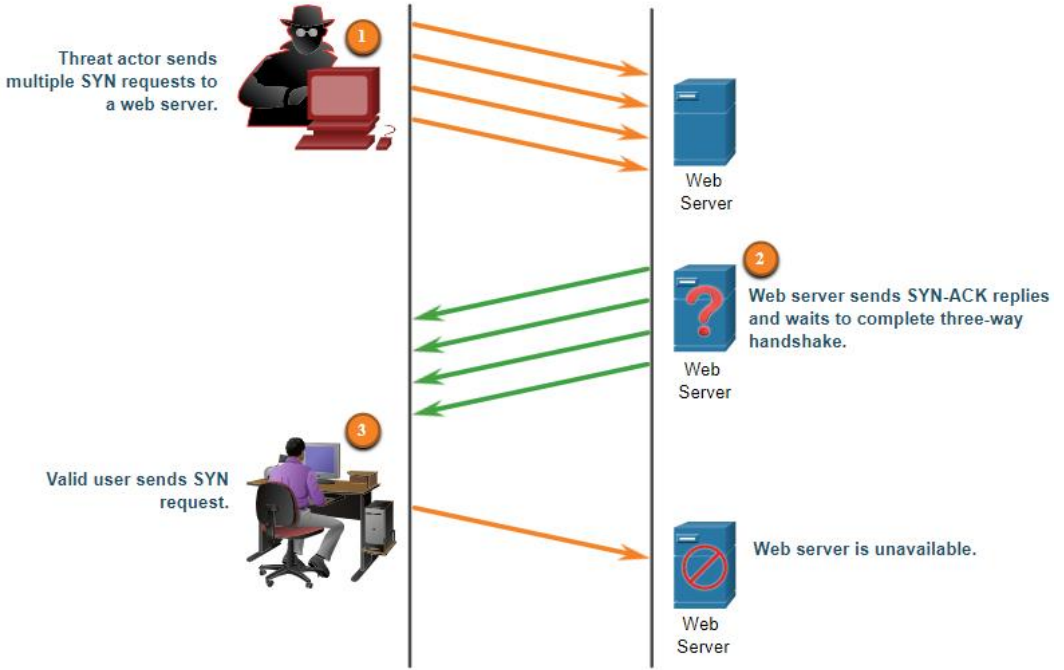
1. Le client demande l'établissement d'une session de communication client-serveur avec le serveur.
2. Le serveur accuse réception de la session de communication client-serveur et demande l'établissement d'une session de communication serveur-client.
3. Le client accuse réception de la session de communication serveur-client.



Attaques TCP

TCP SYN Attaque par inondation

1. L'acteur de menace envoie plusieurs demandes SYN à un serveur Web.
2. Le serveur Web répond avec des SYN-ACK pour chaque demande SYN et attend de terminer la négociation à poignée de main à trois voies. L'acteur de menace ne répond pas aux SYN-ACK.
3. Un utilisateur valide ne peut pas accéder au serveur Web car le serveur Web possède trop de connexions TCP semi-ouvertes.

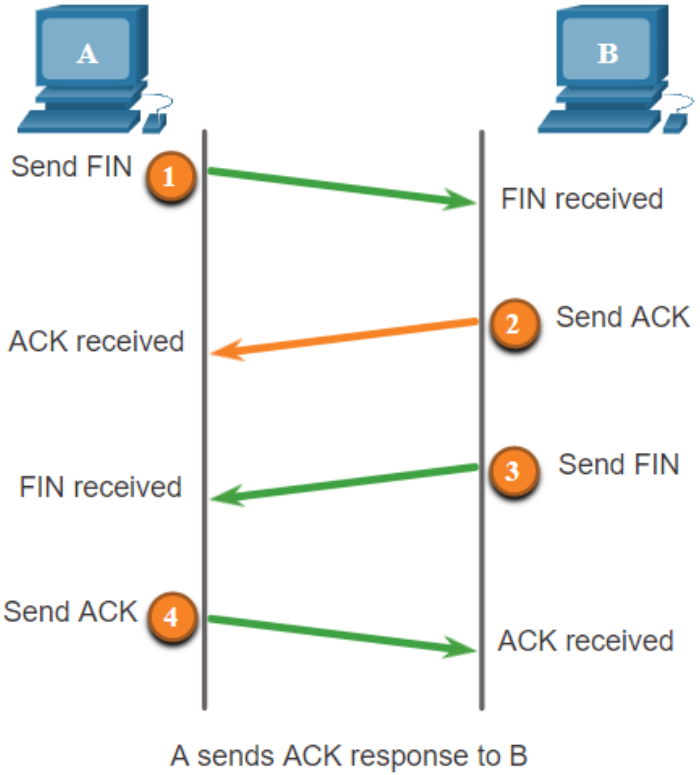


Attaques TCP (suite)

La fin d'une session TCP utilise le processus d'échange à quatre voies suivant:

1. Quand le client n'a plus de données à envoyer dans le flux, il envoie un segment dont l'indicateur FIN est défini.
2. Le serveur envoie un segment ACK pour informer de la bonne réception du segment FIN afin de fermer la session du client au serveur.
3. Le serveur envoie un segment FIN au client pour mettre fin à la session du serveur au client.
4. Le client répond à l'aide d'un segment ACK pour accuser réception du segment FIN envoyé par le serveur.

Un acteur de menace pourrait effectuer une attaque de réinitialisation TCP et envoyer un paquet usurpé contenant un TCP RST à un ou aux deux points de terminaison.

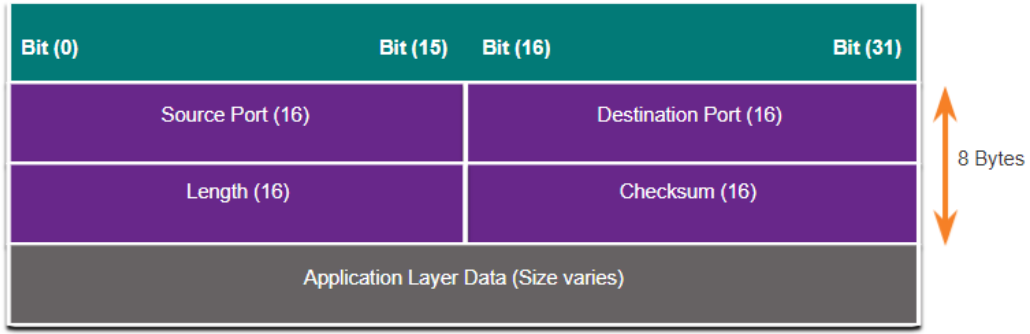


Attaques TCP (suite)

Le détournement de session TCP apparaît comme une autre vulnérabilité TCP. Bien que difficile à mener, un acteur de menace prend le contrôle d'un hôte déjà authentifié lors de sa communication avec la cible. L'acteur de menace doit usurper l'adresse IP d'un hôte, prédire le numéro de séquence suivant et envoyer un ACK à l'autre hôte. En cas de succès, l'acteur de menace pourrait envoyer, mais pas recevoir, des données de l'appareil cible.

En-tête et fonctionnement du segment UDP

- Le protocole UDP est généralement utilisé par les protocoles DNS, TFTP, NFS et SNMP. Il est aussi utilisé par les applications en temps réel comme la diffusion multimédia en flux continu ou les transmissions VoIP. Le protocole UDP s'inscrit comme un protocole de couche transport sans connexion. Il crée beaucoup moins de surcharge que le protocole TCP car il est sans connexion et n'offre pas de mécanismes sophistiqués de fiabilité (retransmission, séquençage et contrôle de flux).
- Ces fonctions de fiabilité ne sont pas fournies par le protocole de couche transport et doivent être implémentées ailleurs si nécessaire.
- La faible surcharge d'UDP le rend très souhaitable pour les protocoles qui effectuent des transactions de demande et de réponse simples.



Attaques UDP

- Le protocole UDP n'est pas protégé par chiffrement. Vous pouvez ajouter un chiffrement à UDP, mais il n'est pas disponible par défaut. L'absence de cryptage signifie que n'importe qui peut voir le trafic, le modifier et l'envoyer à sa destination.
- **UDP Flood Attacks:** L'acteur de menace utilise un outil comme UDP Unicorn ou Low Orbit Ion Cannon. Ces outils envoient un flot de paquets UDP, souvent à partir d'un hôte usurpé, vers un serveur du sous-réseau. Le programme balaye tous les ports connus afin de trouver les ports fermés. Par conséquent, le serveur répond avec un message Port ICMP inaccessible. Étant donné qu'il existe de nombreux ports fermés sur le serveur, cela crée beaucoup de trafic sur le segment, qui utilise la majeure partie de la bande passante. Le résultat est très similaire à celui d'une attaque DoS.

3.8 Services IP

Vulnérabilités ARP

- Les hôtes diffusent une demande ARP à d'autres hôtes sur le segment pour déterminer l'adresse MAC d'un hôte avec une adresse IP particulière. L'hôte dont l'adresse IP correspond à la requête ARP envoie une réponse ARP.
- Tout client peut envoyer une réponse ARP non sollicitée appelée «ARP gratuit». Lorsqu'un hôte envoie un ARP gratuit, les autres hôtes du sous-réseau stockent l'adresse MAC et l'adresse IP contenues dans l'ARP gratuit dans leurs tables ARP.
- Cette fonctionnalité d'ARP signifie également que tout hôte peut prétendre être le propriétaire de n'importe quelle adresse IP ou MAC. Un acteur de menace peut empoisonner le cache ARP des appareils sur le réseau local, créant une attaque MITM pour rediriger le trafic.

Empoisonnement du cache ARP

L'empoisonnement du cache ARP peut être utilisé pour lancer diverses attaques de l'homme-au-milieu.

1. PC-A requiert l'adresse MAC de sa passerelle par défaut (R1); par conséquent, il envoie une demande ARP pour l'adresse MAC de 192.168.10.1.
2. R1 met à jour son cache ARP avec les adresses IP et MAC de PC-A. R1 envoie une réponse ARP à PC-A, qui met ensuite à jour son cache ARP avec les adresses IP et MAC de R1.
3. L'acteur de menace envoie deux réponses ARP usurpées gratuitement en utilisant sa propre adresse MAC pour les adresses IP de destination indiquées. PC-A met à jour son cache ARP avec sa passerelle par défaut qui pointe maintenant vers l'adresse MAC hôte de l'acteur de la menace. R1 met également à jour son cache ARP avec l'adresse IP de PC-A pointant vers l'adresse MAC de l'acteur de menace.

L'attaque d'empoisonnement ARP peut être passive ou active. L'empoisonnement passif par ARP est l'endroit où les acteurs de la menace volent des informations confidentielles. L'empoisonnement ARP actif est l'endroit où les acteurs de menace modifient les données en transit ou injectent des données malveillantes.

Vidéo des services IP - Usurpation ARP

Cette vidéo explique une attaque d'usurpation ARP.

Attaques DNS

- Le protocole DNS (Domain Name Service) définit un service automatisé qui fait correspondre les noms de ressources, tels que www.cisco.com, avec l'adresse réseau numérique requise, telle que l'adresse IPv4 ou IPv6. Il inclut le format des requêtes, des réponses et des données, et utilise les enregistrements de ressource (RR) pour identifier le type de réponse DNS.
- La sécurisation du protocole DNS est souvent négligée. Toutefois, celui-ci est indispensable à l'exploitation d'un réseau et doit être sécurisé en conséquence.
- Les attaques DNS sont les suivantes:
  - Attaques DNS résolveur ouvert
  - Attaques furtives DNS
  - Les attaques de shadowing de domaine DNS
  - Attaques de Tunnellisation (tunneling) DNS

Attaques DNS (suite)

Attaques du résolveur ouvert DNS: un résolveur ouvert DNS répond aux requêtes des clients en dehors de son domaine administratif. Les résolveurs ouverts DNS sont vulnérables à plusieurs activités malveillantes décrites dans le tableau.

Vulnérabilités du résolveur DNS	Description
Attaques d'empoisonnement du cache DNS	Les acteurs de menace envoient des informations de ressource d'enregistrement (RR) falsifiées à un résolveur DNS pour rediriger les utilisateurs de sites légitimes vers des sites malveillants. Les attaques d'empoisonnement du cache DNS peuvent toutes être utilisées pour informer le résolveur DNS d'utiliser un serveur de noms malveillant qui fournit des informations RR pour les activités malveillantes.
Attaques par amplification et réflexion du DNS	Les acteurs de menace utilisent des attaques DoS ou DDoS sur les résolveurs ouverts DNS pour augmenter le volume des attaques et masquer la véritable source d'une attaque. Les acteurs de menace envoient des messages DNS aux résolveurs ouverts en utilisant l'adresse IP d'un hôte cible. Ces attaques sont possibles car le résolveur ouvert répondra aux requêtes de toute personne posant une question.
Attaques d'utilisation des ressources DNS	Une attaque DoS qui consomme les ressources des résolveurs ouverts DNS. Cette attaque DoS consomme toutes les ressources disponibles pour affecter négativement les opérations du résolveur ouvert DNS. L'impact de cette attaque DoS peut nécessiter le redémarrage du résolveur ouvert DNS ou l'arrêt et le redémarrage des services.

Attaques DNS (suite)

Attaques furtives DNS: pour masquer leur identité, les acteurs de menace utilisent également les techniques de furtivité DNS décrites dans le tableau pour mener leurs attaques.

Techniques DNS furtives	Description
Flux rapide	Les auteurs de menace utilisent cette technique pour masquer leurs sites de phishing et de diffusion de logiciels malveillants derrière un réseau en évolution rapide d'hôtes DNS compromis. Les adresses IP du protocole DNS changent continuellement après quelques minutes. Les botnets utilisent souvent des techniques Flux rapide pour cacher efficacement la détection de serveurs malveillants.
Double flux IP	Les acteurs de menace utilisent cette technique pour changer rapidement le nom d'hôte en mappages d'adresses IP et également pour changer le serveur de noms faisant autorité. Cela augmente la difficulté d'identifier la source de l'attaque.
Algorithmes de génération de domaine	Les auteurs de menace utilisent cette technique dans les logiciels malveillants pour générer de manière aléatoire des noms de domaine qui peuvent ensuite être utilisés comme points de rendez-vous vers leurs serveurs de commande et de contrôle (C&C).

Attaques DNS (suite)

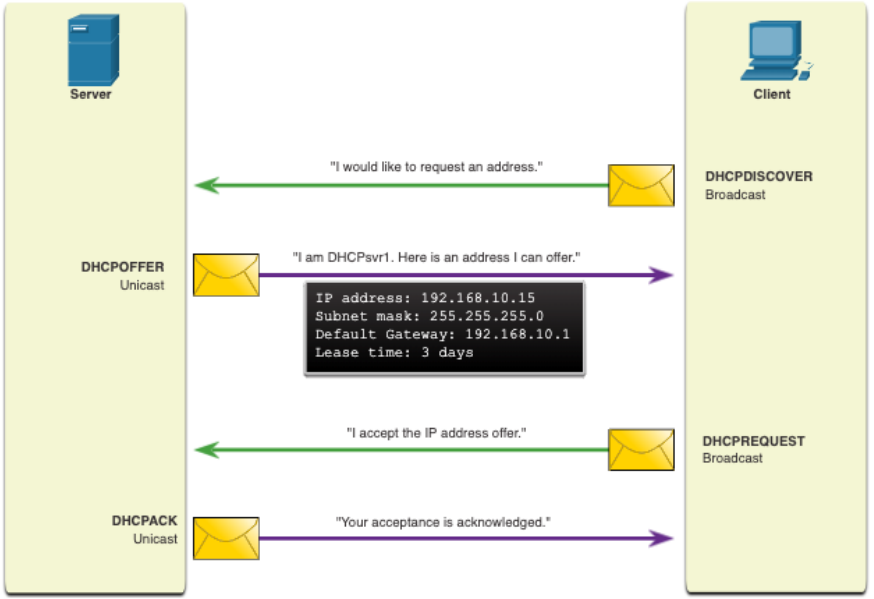
Attaques d'ombrage (shadowing) de domaine DNS : La surveillance de domaine implique que l'acteur de menace recueille des informations sur le compte du domaine afin de créer silencieusement plusieurs sous-domaines à utiliser lors des attaques. Ces sous-domaines pointent généralement vers des serveurs malveillants sans alerter le propriétaire réel du domaine parent.

Tunnellisation (tunneling) DNS

- Les acteurs de menace qui utilisent la tunnellisation DNS placent le trafic non DNS dans le trafic DNS. Cette méthode contourne souvent les solutions de sécurité lorsqu'un acteur de menace souhaite communiquer avec des bots à l'intérieur d'un réseau protégé ou exfiltrer des données de l'organisation. Voici comment fonctionne la tunnelisation DNS pour les commandes CnC envoyées à un botnet:
  1. Les données de commande sont divisées en plusieurs blocs codés.
  2. Chaque bloc est placé sous une étiquette de nom de domaine d'un niveau inférieur à celui de la requête DNS.
  3. Étant donné qu'il n'y a pas de réponse du DNS local ou en réseau pour la requête, la demande est envoyée aux serveurs DNS récursifs du ISP.
  4. Le service DNS récursif transmet la requête au serveur de noms faisant autorité de l'acteur de menace.
  5. Le processus est répété jusqu'à ce que toutes les requêtes contenant les blocs soient envoyées.
  6. Lorsque le serveur de noms faisant autorité de l'acteur de menace reçoit les requêtes DNS des appareils infectés, il envoie des réponses pour chaque requête DNS, qui contiennent les commandes CnC encapsulées et encodées.
  7. Le logiciel malveillant (malware) sur l'hôte compromis recombine les morceaux et exécute les commandes cachées dans l'enregistrement DNS.
- Pour arrêter la tunnellisation DNS, l'administrateur réseau doit utiliser un filtre qui inspecte le trafic DNS. Portez une attention particulière aux requêtes DNS qui sont plus longues que la moyenne, ou celles qui ont un nom de domaine suspect.

DHCP

- Les serveurs DHCP fournissent dynamiquement des informations de configuration IP aux clients.
- Dans la figure, un client diffuse un message de découverte DHCP. Le DHCP répond avec une offre de monodiffusion qui inclut les informations d'adressage que le client peut utiliser. Le client diffuse une requête DHCP pour indiquer au serveur que le client accepte l'offre. Le serveur répond par un accusé de réception monodiffusion acceptant la demande.



Attaques DHCP

- Une **attaque d'usurpation DHCP** se produit lorsqu'un serveur DHCP non autorisé est connecté au réseau et fournit de faux paramètres de configuration IP aux clients légitimes. Un serveur non autorisé peut fournir une variété d'informations trompeuses:
  - **Passerelle par défaut incorrecte** - L'acteur de menace fournit une passerelle non valide ou l'adresse IP de son hôte pour créer une attaque MITM. Cela peut ne pas être détecté car l'intrus intercepte le flux de données à travers le réseau.
  - **Serveur DNS incorrect** - L'acteur de menace fournit une adresse de serveur DNS incorrecte orientant l'utilisateur vers un site Web malveillant.
  - **Adresse IP incorrecte** - L'acteur de menace fournit une adresse IP non valide, une adresse IP de passerelle par défaut non valide, ou les deux. L'acteur de la menace crée ensuite une attaque DoS sur le client DHCP.

Attaques DHCP (suite)

Supposons qu'un acteur de menace ait correctement connecté un serveur DHCP non autorisé à un port de commutateur sur le même sous-réseau que les clients cibles. Le but du serveur non autorisé est de fournir aux clients de fausses informations de configuration IP.

1. Le client diffuse une demande de découverte DHCP à la recherche d'une réponse d'un serveur DHCP. Les deux serveurs reçoivent le message.
2. Les serveurs DHCP légitimes et escrocs répondent chacun avec des paramètres de configuration IP valides. Le client répond à la première offre reçue
3. Le client a d'abord reçu l'offre frauduleuse. Il diffuse une requête DHCP acceptant les paramètres du serveur non autorisé. Le serveur légitime et escroc reçoit chacun la demande.
4. Seul le serveur non autorisé envoie un message de réponse au client pour accuser réception de sa demande. Le serveur légitime cesse de communiquer avec le client car la demande a déjà été acquittée.

Travaux pratiques– Explorer le trafic DNS

Dans ce TP, vous atteindrez les objectifs suivants:

- Capturer le trafic DNS
- Explorer le trafic des requêtes DNS
- Explorer le trafic des réponses DNS

3.9 Meilleures pratiques de sécurité réseau

Confidentialité, disponibilité et intégrité

- La sécurité du réseau consiste à protéger les informations et les systèmes d'information contre tout accès, utilisation, divulgation, interruption, modification ou destruction non autorisés.
- La plupart des organisations suivent la triade de sécurité de l'information de la CIA:
  - **Confidentialité** - Seuls les individus, entités ou processus autorisés peuvent accéder aux informations sensibles. Cela peut nécessiter l'utilisation d'algorithmes de cryptage cryptographiques tels que AES pour crypter et décrypter les données.
  - **Intégrité** -Désigne la protection des données contre toute altération non autorisée. Il nécessite l'utilisation d'algorithmes de hachage cryptographiques tels que SHA.
  - **Disponibilité** - Les utilisateurs autorisés doivent avoir un accès ininterrompu aux ressources et données importantes. Cela nécessite la mise en œuvre de services, de passerelles et de liaisons redondants.

L'approche de défense en profondeur

- Pour garantir des communications sécurisées sur les réseaux publics et privés, vous devez sécuriser les appareils, y compris les routeurs, les commutateurs, les serveurs et les hôtes. La plupart des organisations utilisent une approche de défense en profondeur de la sécurité. Cela nécessite une combinaison de périphériques réseau et de services fonctionnant ensemble.
- Plusieurs dispositifs et services de sécurité sont mis en œuvre.
  - **VPN**
  - **Pare-feu ASA**
  - **IPS**
  - **ESA/WSA**
  - **Serveur AAA**
- Tous les périphériques réseau, y compris le routeur et les commutateurs, sont renforcés.
- Vous devez également sécuriser les données lorsqu'elles transitent par différents liens.

Pare-feu

Un pare-feu est un système ou un groupe de systèmes qui applique une stratégie de contrôle d'accès entre les réseaux.

Allow traffic from any external address to the web server.

Allow traffic to FTP server.

Allow traffic to SMTP server.

Allow traffic to internal IMAP server.

Deny all inbound traffic with network addresses matching internal-registered IP addresses.

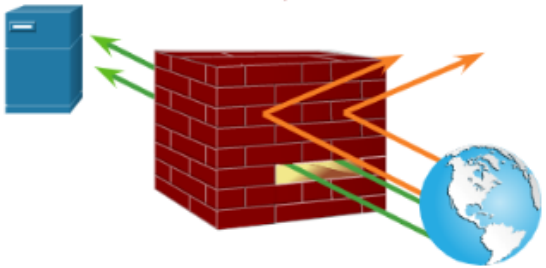
Deny all inbound traffic to server from external addresses.

Deny all inbound ICMP echo request traffic.

Deny all inbound MS Active Directory queries.

Deny all inbound traffic to MS SQL server queries.

Deny all MS Domain Local Broadcasts.



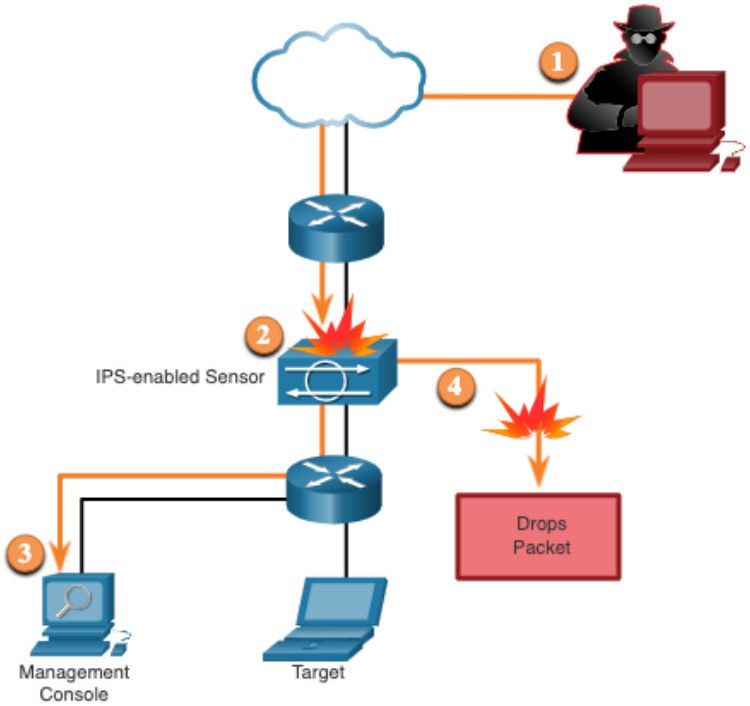
IPS

- Pour vous défendre contre les attaques rapides et évolutives, vous pouvez avoir besoin de systèmes de détection et de prévention économiques intégrés aux points d'entrée et de sortie du réseau.
- Les technologies IDS et IPS partagent plusieurs caractéristiques. Les technologies IDS et IPS sont toutes deux déployées comme des capteurs. Un capteur IDS ou IPS peut se présenter sous la forme de plusieurs appareils différents:
  - Un routeur configuré avec le logiciel Cisco IOS IPS
  - Un appareil spécialement conçu pour fournir des services IDS ou IPS dédiés
  - Un module réseau installé dans un dispositif de sécurité adaptatif ASA (Adaptive Security Appliance), un commutateur ou un routeur
  - Les technologies IDS et IPS détectent les modèles de trafic réseau à l'aide de signatures, qui sont un ensemble de règles utilisées pour détecter les activités malveillantes. Les technologies IDS et IPS peuvent détecter des modèles de signature atomique (mono-paquet) ou des modèles de signature composite (multi-paquet).

IPS (suite)

La figure montre comment un IPS gère le trafic refusé.

1. L'acteur de menace envoie un paquet destiné à l'ordinateur portable cible.
2. L'IPS intercepte le trafic et l'évalue par rapport aux menaces connues et aux stratégies configurées.
3. L'IPS envoie un message de journal à la console de gestion.
4. L'IPS abandonne le paquet.



Appareils de sécurité du contenu

- Appliance de sécurité de messagerie Cisco ESA (Cisco Email Security Appliance) est un appareil spécial conçu pour surveiller le protocole de transfert de courrier simple SMTP (Simple Mail Transfer Protocol). Cisco ESA est constamment mis à jour par des flux en temps réel de Cisco Talos. Ces données de renseignement sur les menaces sont extraites par Cisco ESA toutes les trois à cinq minutes.
- L'appliance de sécurité Web Cisco (WSA) est une technologie d'atténuation des menaces Web. Cisco WSA combine une protection avancée contre les logiciels malveillants, la visibilité et le contrôle des applications, des contrôles de politique d'utilisation acceptable et des rapports.
- Cisco WSA offre un contrôle complet sur la façon dont les utilisateurs accèdent à Internet. Le WSA peut effectuer la mise sur liste noire des URL, le filtrage des URL, l'analyse des logiciels malveillants, la catégorisation des URL, le filtrage des applications Web et le chiffrement et le déchiffrement du trafic Web.

3.10 Cryptographie

Vidéo de cryptographie - Cryptographie

Cette vidéo montrera les données de sécurité à l'aide du hachage et du chiffrement.

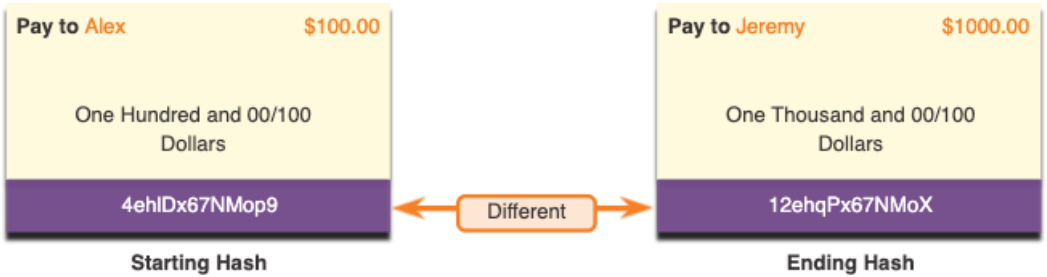
Sécurisant les communications

- Les organisations doivent fournir un support pour sécuriser les données au fur et à mesure qu'elles traversent les liens. Cela peut inclure le trafic interne, mais il est encore plus important de protéger les données qui circulent en dehors de l'organisation.
- Ce sont les quatre éléments des communications sécurisées:
  - **Intégrité des données** -garantit que le message n'a pas été modifié. L'intégrité est assurée par l'implémentation de Message Digest version 5 (MD5) ou des algorithmes de génération de hachage SHA (Secure Hash Algorithm).
  - **Authentification d'origine** - Garantit que le message n'est pas une contrefaçon et qu'il provient du propriétaire. De nombreux réseaux modernes garantissent l'authentification avec des protocoles, par exemple le code HMAC (hash message authentication code).
  - **Confidentialité des données** - Garantit que seuls les utilisateurs autorisés peuvent lire le message. La confidentialité des données est implémentée à l'aide d'algorithmes de chiffrement symétrique et asymétrique.
  - **Non-répudiation des données** - Garantit que l'expéditeur ne peut pas répudier ou réfuter la validité d'un message envoyé. La non-répudiation repose sur le fait que seul l'expéditeur dispose des caractéristiques uniques ou de la signature relative au traitement du message.
- La cryptographie peut être utilisée presque partout où se produit une communication de données. En fait, la tendance est au cryptage de toutes les communications.

Intégrité des données

- Les fonctions de hash sont utilisées pour garantir l'intégrité d'un message. Ils garantissent que les données des messages n'ont pas été modifiées accidentellement ou intentionnellement.
- Sur la figure, l'expéditeur envoie un transfert d'argent de 100 $ à Alex. L'expéditeur souhaite s'assurer que le message n'est pas modifié sur son chemin vers le récepteur.

1. Le périphérique émetteur entre le message dans un algorithme de hachage et calcule son hachage de longueur fixe de 4ehiDx67NMop9.
2. Ce hash est ensuite joint au message et envoyé au récepteur. Le message et le hash sont en texte clair.
3. Le périphérique récepteur supprime le hash du message et saisit celui-ci dans le même algorithme de hash. Si le hash calculé est égal à celui joint au message, c'est que celui-ci n'a pas été modifié pendant l'envoi. Si les hachages ne sont pas égaux, l'intégrité du message ne peut plus être approuvée.

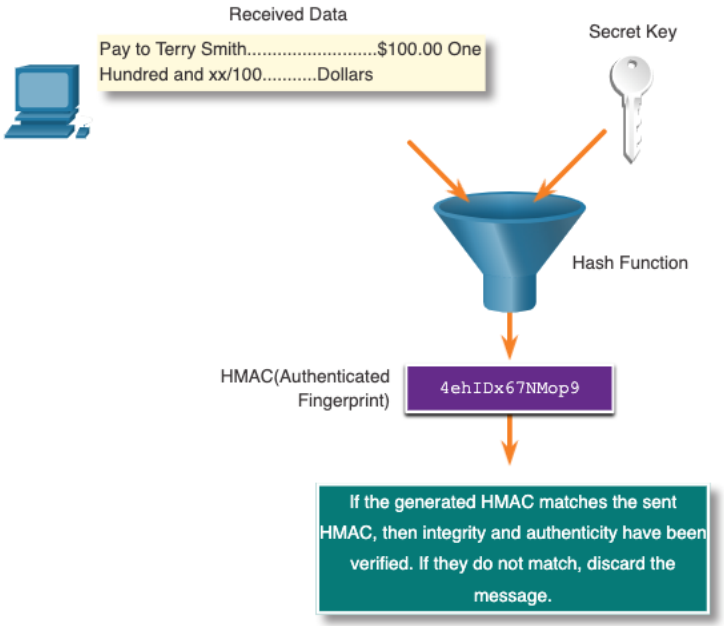


Fonctions de hash

- Il existe trois fonctions de hachage bien connues.
  - **MD5 avec 128 bits Digest:** MD5 est une fonction unidirectionnelle qui produit un message haché de 128 bits. MD5 est un algorithme hérité qui ne devrait être utilisé que lorsqu'aucune meilleure alternative n'est disponible. Utilisez SHA-2 à la place.
  - **Algorithme de hachage SHA:** SHA-1 très similaire aux fonctions de hash MD5. SHA-1 crée un message haché de 160 bits et est légèrement plus lent que MD5. SHA-1 a des défauts connus et c'est un algorithme hérité. Utilisez SHA-2 lorsque cela est possible.
  - **SHA-2:** cela inclut SHA-224 (224 bits), SHA-256 (256 bits), SHA-384 (384 bits) et SHA-512 (512 bits). SHA-256, SHA-384 et SHA-512 sont des algorithmes de nouvelle génération et doivent être utilisés dans la mesure du possible.
- Bien que le hachage puisse être utilisé pour détecter des modifications accidentelles, il ne peut pas être utilisé pour se prémunir contre des modifications délibérées. Cela signifie que n'importe qui peut calculer un hash pour n'importe quelle donnée, à condition de disposer de la fonction de hash correcte.
- Par conséquent, le hachage est vulnérable aux attaques de l'homme-au-milieu et n'assure pas la sécurité des données transmises.

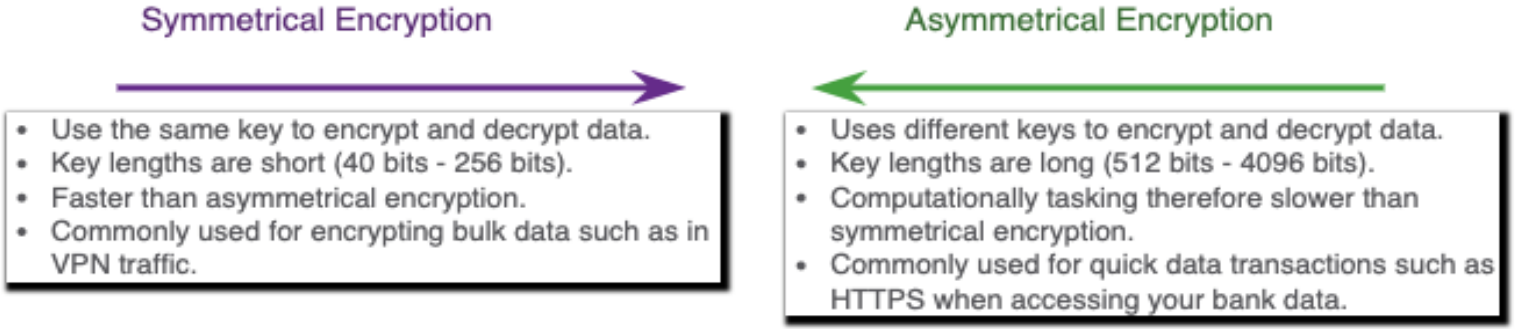
Authentification de l'origine

- Pour ajouter l'authentification à l'assurance d'intégrité, utilisez un code d'authentification de message de hachage à clé (HMAC).
- Un HMAC est calculé à l'aide de tout algorithme cryptographique qui combine une fonction de hachage cryptographique avec une clé secrète.
- Seules les parties qui ont accès à cette clé secrète peuvent calculer le condensé d'une fonction HMAC. Cela permet de vaincre les attaques de type "homme-au-milieu" et d'authentifier l'origine des données.



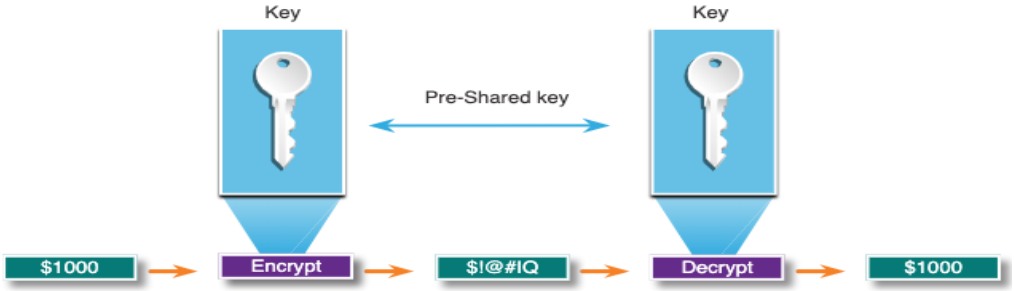
Confidentialité des données

- Il existe deux classes de cryptage utilisées pour assurer la confidentialité des données. Ces deux classes diffèrent dans la façon dont elles utilisent les clés.
- Les algorithmes de chiffrement symétrique tels que (DES), 3DES et Advanced Encryption Standard (AES) sont basés sur l'hypothèse que chaque partie communicante connaît la clé pré-partagée. La confidentialité des données peut également être assurée à l'aide d'algorithmes asymétriques, notamment Rivest, Shamir et Adleman (RSA) et l'infrastructure à clé publique (PKI).
- La figure met en évidence les différences entre chaque méthode d'algorithme de chiffrement.



Chiffrement symétrique

- Les algorithmes symétriques utilisent la même clé pré-partagée, également appelée clé secrète, pour crypter et décrypter les données. L'expéditeur et le destinataire connaissent une clé pré-partagée avant que toute communication chiffrée puisse avoir lieu.
- Les algorithmes de chiffrement symétriques sont couramment utilisés avec le trafic VPN car ils utilisent moins de ressources CPU que les algorithmes de chiffrement asymétriques.
- Lorsque vous utilisez des algorithmes de chiffrement symétriques, plus la clé est longue, plus il faudra du temps à quelqu'un pour découvrir la clé. Pour garantir la sécurité du cryptage, utilisez une longueur de clé minimale de 128 bits.



Chiffrement symétrique (suite)

Algorithmes de chiffrement symétriques	Description
Algorithme de chiffrement des données (DES)	Il s'agit d'un algorithme de chiffrement symétrique hérité. Il peut être utilisé en mode de chiffrement de flux, mais fonctionne habituellement en mode bloc pour chiffrer les données dans une taille de bloc de 64 bits. Un chiffrement de flux chiffre un byte ou un bit à la fois.
3DES (Triple DES)	Il s'agit d'une version plus récente de DES, mais elle répète le processus d'algorithme DES trois fois. Il est considéré comme très fiable lorsqu'il est mis en œuvre en utilisant des durées de vie de clé très courtes.
Norme de cryptage avancée (AES)	AES est un algorithme sécurisé et plus efficace que l'algorithme 3DES. Il s'agit d'un algorithme de chiffrement symétrique populaire et recommandé. Il propose neuf combinaisons de longueur de clé et de bloc en utilisant une longueur de clé variable de 128, 192 ou 256 bits pour crypter des blocs de données de 128, 192 ou 256 bits.
Algorithme de chiffrement optimisé par logiciel (SEAL)	SEAL est un algorithme de chiffrement symétrique alternatif plus rapide que DES, 3DES et AES. Il utilise une clé de cryptage 160 bits et a un impact moindre sur le processeur par rapport aux autres algorithmes logiciels.
Algorithmes de la série Rivest Ciphers (RC)	Cet algorithme a été développé par Ron Rivest. Plusieurs variantes ont été développées, mais le RC4 est le plus utilisé. RC4 est un chiffrement de flux et est utilisé pour sécuriser le trafic Web en SSL et TLS.

Chiffrement symétrique

- Les algorithmes asymétriques, également appelés algorithmes à clé publique, sont conçus pour que la clé utilisée pour le chiffrement soit différente de la clé utilisée pour le déchiffrement.
- Les algorithmes asymétriques utilisent une clé publique et une clé privée. La clé appariée complémentaire est requise pour le déchiffrement. Les données chiffrées avec la clé publique nécessitent la clé privée pour être déchiffrées. Les algorithmes asymétriques assurent la confidentialité, l'authentification et l'intégrité en utilisant ce processus.
- Étant donné qu'aucune des parties n'a un secret partagé, des longueurs de clé très longues doivent être utilisées. Le chiffrement asymétrique peut utiliser des longueurs de clé comprises entre 512 et 4 096 bits. Des longueurs de clé supérieures ou égales à 1024 bits peuvent être approuvées tandis que des longueurs de clé plus courtes sont considérées comme non fiables.

Chiffrement asymétrique (suite)

- Voici des exemples de protocoles qui utilisent des algorithmes à clé asymétrique:
  - **Échange de clés Internet IKE (Internet Key Exchange) -** Il s'agit d'un composant fondamental des VPN IPsec.
  - **SSL (Secure Socket Layer) -** Ceci est maintenant implémenté en tant que TLS (Transport Layer Security) standard de l'IETF.
  - **SSH (Secure Shell) -** protocole qui assure une connexion à distance sécurisée aux appareils réseau.
  - **PGP (Pretty Good Privacy) -** Ce programme informatique fournit une confidentialité cryptographique et une authentification. Il est souvent utilisé pour augmenter la sécurité des communications par e-mail.
- Les algorithmes asymétriques sont sensiblement plus lents que les algorithmes symétriques. Leur conception est basée sur des problèmes de calcul, tels que la factorisation de très grands nombres ou le calcul de logarithmes discrets de très grands nombres.
- Parce qu'ils sont lents, les algorithmes asymétriques sont généralement utilisés dans les mécanismes cryptographiques à faible volume, tels que les signatures numériques et l'échange de clés.

Cryptographie

Chiffrement asymétrique (suite)

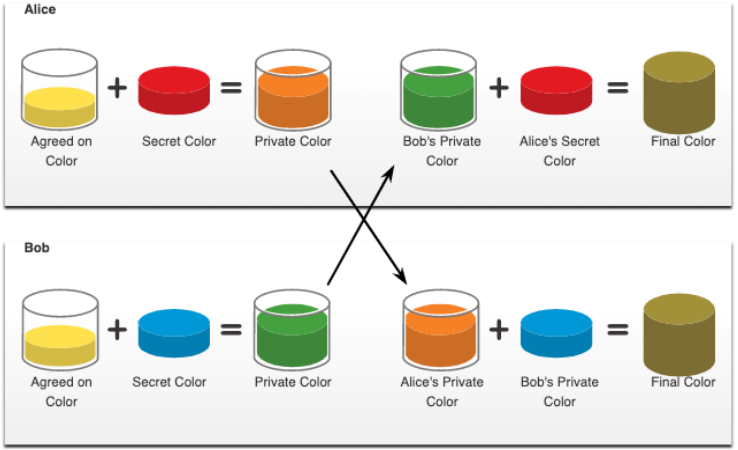
Algorithmes de chiffrement asymétrique	Longueur de clé (Key Length)	Description
Diffie-Hellman (DH)	512, 1024, 2048, 3072, 4096	L'algorithme Diffie-Hellman permet à deux parties de s'entendre sur une clé qu'elles peuvent utiliser pour crypter les messages qu'elles souhaitent s'envoyer l'une à l'autre. La sécurité de cet algorithme dépend de l'hypothèse qu'il est facile d'élever un nombre à une certaine puissance, mais difficile de calculer quelle puissance a été utilisée compte tenu du nombre et du résultat.
Norme de signature numérique (DSS) et algorithme de signature numérique (DSA)	512 - 1024	DSS spécifie DSA comme algorithme pour les signatures numériques. DSA est un algorithme à clé publique basé sur le schéma de signature ElGamal. La vitesse de création de signature est similaire à RSA mais est 10 à 40 fois plus lente pour la vérification.
Algorithmes de chiffrement Rivest, Shamir et Adleman (RSA)	De 512 à 2048	RSA est destiné à la cryptographie à clé publique basée sur la difficulté actuelle de factoriser de très grands nombres. Il s'agit du premier algorithme connu pour être adapté à la signature ainsi qu'au cryptage. Il est largement utilisé dans les protocoles de commerce électronique et est censé être sécurisé étant donné les clés suffisamment longues et l'utilisation d'implémentations à jour.
ElGamal	De 512 à 1024	Un algorithme de chiffrement asymétrique de cryptographie à clé publique qui repose sur l'accord de clé Diffie-Hellman. Un inconvénient du système ElGamal est que le message crypté devient très gros, environ deux fois la taille du message d'origine et pour cette raison, il n'est utilisé que pour les petits messages tels que les clés secrètes.
Techniques de courbe elliptique	160	La cryptographie à courbe elliptique peut être utilisée pour adapter de nombreux algorithmes cryptographiques, tels que Diffie-Hellman ou ElGamal. Le principal avantage de la cryptographie sur les courbes elliptiques est que les clés peuvent être beaucoup plus petites.

Diffie-Hellman

- Diffie-Hellman (DH) est un algorithme mathématique asymétrique où deux ordinateurs génèrent une clé secrète partagée identique sans avoir communiqué auparavant. En réalité, la nouvelle clé partagée n'est pas véritablement échangée entre l'émetteur et le récepteur.
- Voici trois exemples d'instances où DH est couramment utilisé:
  - Les données sont échangées à l'aide d'un VPN IPsec.
  - Les données sont cryptées sur Internet à l'aide de SSL ou TLS.
  - Les données SSH sont échangées.
- La sécurité DH utilise des nombres incroyablement élevés dans ses calculs.
- Malheureusement, les systèmes à clé asymétrique sont extrêmement lents, quel que soit le mode de chiffrement par bloc. Par conséquent, il est courant de chiffrer la majeure partie du trafic à l'aide d'un algorithme symétrique, tel que 3DES ou AES, puis d'utiliser l'algorithme DH pour créer des clés qui seront utilisées par l'algorithme de chiffrement.

Diffie-Hellman (suite)

- Les couleurs de la figure seront utilisées à la place des nombres pour simplifier le processus d'accord de clé DH. L'échange de clés DH commence par Alice et Bob se mettant d'accord sur une couleur commune arbitraire qui n'a pas besoin d'être gardée secrète. La couleur convenue dans notre exemple est le jaune.
- Ensuite, Alice et Bob doivent chacun choisir une couleur secrète. Alice choisit le rouge et Bob le bleu. Ces couleurs secrètes ne doivent jamais être partagées. La couleur secrète représente la clé privée choisie par chacune des parties.
- Alice et Bob mélangent maintenant la couleur commune partagée (le jaune) avec leur propre couleur secrète afin d'obtenir une couleur privée. Par conséquent, Alice mélange le jaune au rouge et obtient ainsi une couleur privée orange. Bob mélange le jaune au bleu et obtient ainsi une couleur privée verte.
- Alice envoie sa couleur privée (l'orange) à Bob et Bob envoie sa couleur privée (le vert) à Alice.
- Alice et Bob mélangent chacun la couleur qu'ils ont reçue avec leur couleur d'origine secrète (rouge pour Alice et bleu pour Bob). Le résultat est un mélange de couleurs marron final identique au mélange de couleurs final de l'autre. La couleur brune représente la clé secrète partagée résultante entre Bob et Alice.



3.11 Module pratique et questionnaire

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

- Les failles de sécurité du réseau peuvent perturber le commerce électronique, entraîner la perte de données commerciales, menacer la confidentialité des personnes et compromettre l'intégrité des informations.
- Les vulnérabilités doivent être traitées avant de devenir une menace et d'être exploitées. Des techniques d'atténuation sont requises avant, pendant et après une attaque.
- Un vecteur d'attaque est un chemin par lequel un acteur de menace peut accéder à un serveur, un hôte ou un réseau. Les vecteurs d'attaque proviennent de l'intérieur ou de l'extérieur du réseau d'entreprise.
- Le terme «acteur de menace» comprend les pirates et tout appareil, personne, groupe ou État-nation qui est, intentionnellement ou non, la source d'une attaque.
- Les outils d'attaque sont devenus plus sophistiqués et hautement automatisés. Ces nouveaux outils nécessitent moins de connaissances techniques pour être implémentés.
- Les types d'attaques les plus courants sont les suivants: écoute clandestine, modification de données, usurpation d'adresse IP, mot de passe, déni de service, homme au milieu, clé compromise et renifleur.
- Les trois types de logiciels malveillants les plus courants sont les vers, les virus et les chevaux de Troie.
- Les réseaux sont sensibles aux types d'attaques suivants: reconnaissance, accès et DoS.
- Les types d'attaques d'accès sont les suivants: mot de passe, usurpation d'identité, exploitations de confiance, redirections de ports, homme-au-milieu et buffer overflow.
- Les techniques d'attaque IP incluent: ICMP, amplification et réflexion, usurpation d'adresse, MITM et détournement de session.

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

- Les acteurs de menace utilisent ICMP pour les attaques de reconnaissance et de scan. Ils lancent des attaques de collecte d'informations pour cartographier une topologie de réseau, découvrir quels hôtes sont actifs (accessibles), identifier le système d'exploitation hôte (empreinte digitale du système d'exploitation) et déterminer l'état d'un pare-feu. Les acteurs de menace utilisent souvent des techniques d'amplification et de réflexion pour créer des attaques DoS.
- Les attaques TCP incluent: l'attaque TCP SYN Flood, l'attaque de réinitialisation TCP et le détournement de session TCP. Les attaques UDP Flood envoient un flot de paquets UDP, souvent à partir d'un hôte usurpé, vers un serveur du sous-réseau. Le résultat est très similaire à une attaque DoS.
- Tout client peut envoyer une réponse ARP non sollicitée appelée «ARP gratuit». Cela signifie que tout hôte peut prétendre être le propriétaire de n'importe quelle adresse IP ou MAC. Un acteur de menace peut empoisonner le cache ARP des appareils sur le réseau local, créant une attaque MITM pour rediriger le trafic.
- Les attaques DNS incluent: les attaques par résolveur ouvert, les attaques furtives, les attaques par suivi de domaine et les attaques par tunnel. Pour arrêter la tunnellisation DNS, l'administrateur réseau doit utiliser un filtre qui inspecte le trafic DNS.
- Une attaque d'usurpation DHCP se produit lorsqu'un serveur DHCP non autorisé est connecté au réseau et fournit de faux paramètres de configuration IP aux clients légitimes.
- La plupart des organisations suivent la triade de sécurité de l'information de la CIA: confidentialité, intégrité et disponibilité.
- Pour garantir des communications sécurisées sur les réseaux publics et privés, vous devez sécuriser les appareils, y compris les routeurs, les commutateurs, les serveurs et les hôtes. C'est ce qu'on appelle la défense en profondeur.

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

- Un pare-feu est un système, ou un groupe de systèmes, qui impose une politique de contrôle d'accès entre des réseaux.
- Pour vous défendre contre les attaques rapides et évolutives, vous pouvez avoir besoin d'un système de détection d'intrusion (IDS) ou des systèmes de prévention des intrusions (IPS) plus évolutifs.
- Les quatre éléments des communications sécurisées sont l'intégrité des données, l'authentification d'origine, la confidentialité des données et la non-répudiation des données.
- Les fonctions de hachage garantissent que les données des messages n'ont pas été modifiées accidentellement ou intentionnellement.
- Trois fonctions de hachage bien connues sont MD5 avec un résumé de 128 bits, l'algorithme de hachage SHA et SHA-2.
- Pour ajouter l'authentification à l'assurance d'intégrité, utilisez un code d'authentification de message de hachage à clé (HMAC). HMAC est calculé à l'aide de tout algorithme cryptographique qui combine une fonction de hachage cryptographique avec une clé secrète.
- Les algorithmes de chiffrement symétrique utilisant DES, 3DES, AES, SEAL et RC sont basés sur l'hypothèse que chaque partie communicante connaît la clé pré-partagée.
- La confidentialité des données peut également être assurée à l'aide d'algorithmes asymétriques, notamment Rivest, Shamir et Adleman (RSA) et l'infrastructure à clé publique (PKI). Diffie-Hellman (DH) est un algorithme mathématique asymétrique où deux ordinateurs génèrent une clé secrète partagée identique sans avoir communiqué auparavant.


CISCO