Chapitre 15-17 : Tout savoir sur les attaques réseau

BENJAMIN DESROSIERS-BOSSÉ

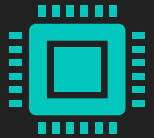
2023

Chapitre 15-17 - Sections et objectifs

Outils de surveillance du réseau

Expliquer la surveillance du trafic réseau.

- Expliquer l'importance de la surveillance du réseau.
- Expliquer comment la surveillance de réseau est effectuée.



Attaques ciblant les fondements du réseau

Expliquer comment les vulnérabilités TCP/IP favorisent les attaques réseau.

- Expliquer comment les vulnérabilités IP favorisent les attaques réseau.
- Expliquer comment les vulnérabilités TCP/UDP favorisent les attaques réseau.

Attaques ciblant les activités

Expliquer pourquoi les applications et les services réseau fréquemment utilisés sont vulnérables aux attaques.

- Expliquer les vulnérabilités IP.
- Expliquer comment les vulnérabilités des applications réseau favorisent les attaques réseau.

Outils de surveillance du réseau

Présentation de la surveillance du réseau
Topologie de la sécurité du réseau

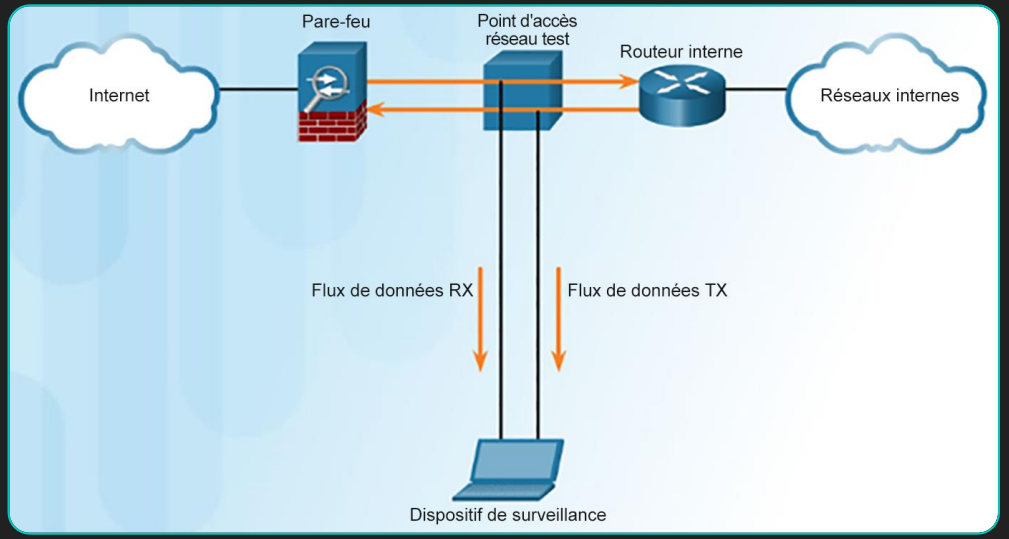
- Tous les réseaux peuvent être ciblés et doivent être protégés à l'aide d'une approche de défense en profondeur.
- Les analystes en charge de la sécurité doivent parfaitement connaître le comportement normal du réseau, car un comportement anormal est généralement synonyme de problème.

Présentation de la surveillance du réseau
Méthodes de surveillance du réseau

- Pour vérifier que le comportement du réseau est normal, ils peuvent notamment utiliser les outils suivants : les systèmes de détection des intrusions (IDS), les analyseurs de paquets, SNMP ou NetFlow.
- Méthodes de capture des informations sur le trafic :
  - **Points d'accès réseau test (TAP)** : points d'accès réseau test qui transmettent l'ensemble du trafic, dont les erreurs de la couche physique, à un appareil d'analyse.
  - **Mise en miroir du port** : permet à un commutateur de copier des trames d'un ou de plusieurs ports vers un port SPAN (Switch Port Analyzer) connecté à un appareil d'analyse.

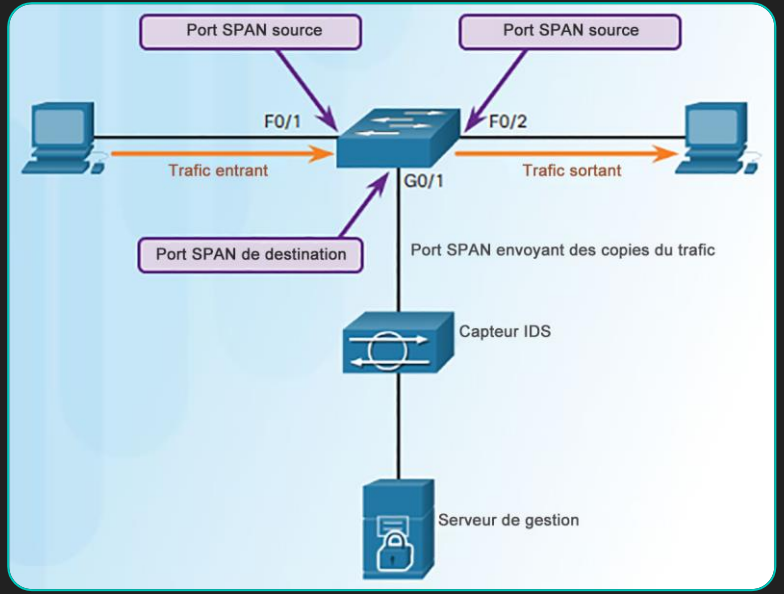
Présentation de la surveillance du réseau
Points d'accès réseau test

- Le point d'accès réseau test est généralement à un appareil de fractionnement passif implémenté en direct entre un appareil d'intérêt et le réseau. Le point d'accès test transfère l'ensemble du trafic (y compris les erreurs de la couche physique) vers un appareil d'analyse.
- Par ailleurs, le point d'accès test est généralement protégé en cas de défaillance : la diminution ou la perte de puissance du point d'accès test n'affecte pas le trafic entre le pare-feu et le routeur interne.



Présentation de la surveillance du réseau
Mise en miroir du trafic et fonction SPAN

- La mise en miroir du port permet à un commutateur de copier des trames d'un ou de plusieurs ports vers un port SPAN (Switch Port Analyzer) connecté à un appareil d'analyse.
- Dans la figure, le commutateur transmet le trafic entrant sur F0/1 et le trafic sortant sur F0/2 vers le port de destination SPAN G0/1 connecté à un système IDS.
- La liaison entre les ports source et le port de destination est appelé « session SPAN ». Une ou plusieurs voies peuvent être surveillées au cours d'une même session.



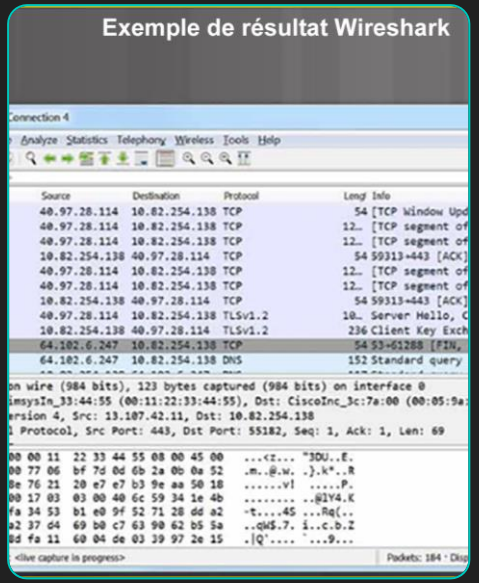
Présentation des outils de surveillance du réseau
Outils de surveillance de la sécurité du réseau

- **Outils de surveillance :**
  - **Analyseurs de protocoles** : programmes utilisés pour capturer le trafic. Ex. Wireshark et Tcpdump.
  - **NetFlow** : fournit une piste d'audit complète des informations de base sur chaque flux IP transmis sur un appareil.
  - **SIEM** : les systèmes de gestion des informations et des événements liés à la sécurité (SIEM) fournissent des rapports en temps réel et des analyses à long terme des événements liés à la sécurité.
  - **SNMP** : le protocole SNMP (Simple Network Management Protocol) permet de demander et de recueillir de manière passive des informations sur tous les appareils réseau.

Fichiers journaux : les fichiers journaux Syslog permettent aux analystes en charge de la sécurité de consulter et d'analyser les événements et les alertes concernant le système.

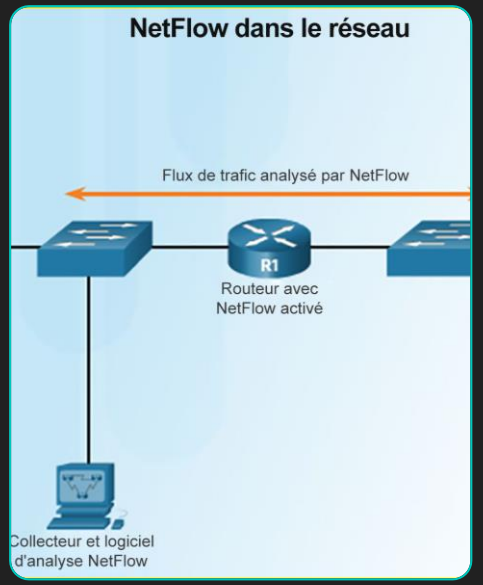
Présentation des outils de surveillance du réseau
Analyseurs de protocoles réseau

- Les analystes peuvent utiliser des analyseurs de protocoles tels que Wireshark et tcpdump pour voir les échanges réseau jusqu'au niveau du paquet.
- Les analyseurs de protocoles réseau se révèlent également utiles pour le dépannage réseau, le développement de logiciels et de protocoles et la formation. Pour mener des recherches, un analyste en sécurité peut tenter de reconstituer un incident à partir des captures de paquets pertinents.



Présentation des outils de surveillance du réseau NetFlow

- La fonctionnalité NetFlow est une technologie Cisco IOS qui fournit 24 h/24, 7 j/7 des statistiques sur les paquets traversant un routeur ou un commutateur multicouche Cisco.
- La fonctionnalité NetFlow peut être utilisée à des fins de surveillance du réseau et de la sécurité, de planification du réseau et d'analyse du trafic. Toutefois, elle ne permet pas de capturer le contenu.
- Les collecteurs NetFlow (Cisco StealthWatch, p. ex.) offrent également des fonctions avancées, notamment :
  - **Convergence des flux** : cette fonction regroupe les entrées individuelles dans les flux.
  - **Déduplication des flux** : cette fonction filtre les entrées entrantes dupliquées de divers clients NetFlow.
  - **Convergence des opérations de traduction d'adresses réseau** : cette fonction simplifie les flux des entrées NAT.



Présentation des outils de surveillance du réseau SIEM

- Les systèmes de gestion des informations et des événements liés à la sécurité (SIEM) fournissent des rapports en temps réel et des analyses à long terme des événements liés à la sécurité.
- Les systèmes SIEM incluent les fonctions de base suivantes :
  - **Investigation** : permet d'explorer les journaux et les enregistrements d'événement issus des sources de l'entreprise. Elle fournit des informations plus complètes à des fins d'investigation.
  - **Corrélation** : permet d'examiner les journaux et les événements de différents systèmes ou applications, d'accélérer la détection et de réagir en cas de menaces pour la sécurité.
  - **Agrégation** : permet de réduire le volume des données d'événement en consolidant les enregistrements d'événement dupliqués.
  - **Reporting** : présente les données d'événement corrélées et agrégées avec la surveillance en temps réel et les résumés à long terme.

Présentation des outils de surveillance du réseau Systèmes SIEM

- Splunk est l'un des systèmes SIEM propriétaires les plus populaires dans les centres opérationnels de sécurité.
- Ce cours utilise la suite ELK pour systèmes SIEM en tant qu'option open source. « ELK » est l'acronyme de trois produits open source d'Elastic :
- **Elasticsearch** : moteur de recherche par texte intégral orienté document
- **Logstash** : système de traitement de pipeline qui relie les « entrées » aux « sorties » à l'aide de « filtres » facultatifs
- **Kibana** : tableau de bord de recherche et d'analytique basé sur un navigateur pour Elasticsearch

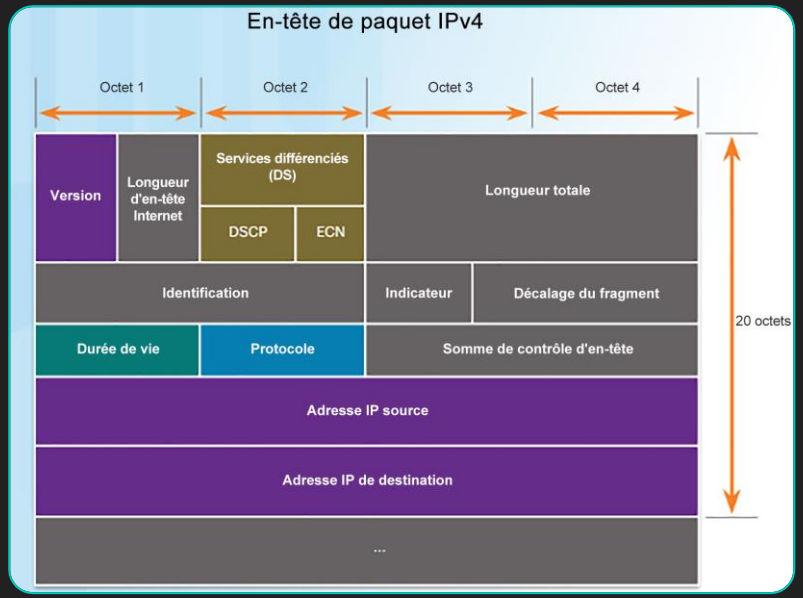

Attaques ciblant les fondements du réseau

Menaces et vulnérabilités IP IPv4 et IPv6

- Les analystes en charge de la sécurité doivent connaître les différents champs des en-têtes IPv4 et IPv6, car les hackers peuvent falsifier les informations des paquets.

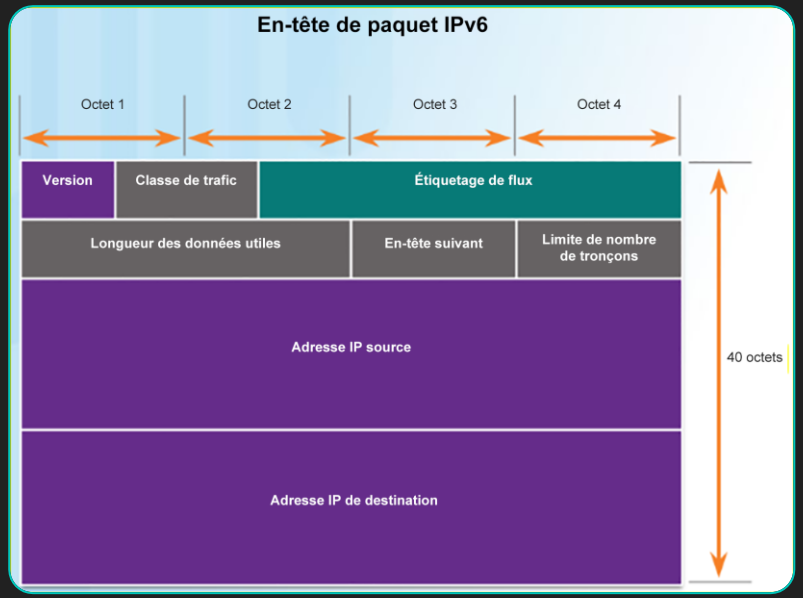
Menaces et vulnérabilités IP
L'en-tête de paquet IPv4

- Un en-tête de paquet IPv4 contient 10 champs :
  - Version
  - Longueur d'en-tête Internet
  - Services différenciés (ou DiffServ/DS)
  - Longueur totale
  - Identification, Indicateur et Décalage du fragment
  - Time-to-Live (TTL)
  - Protocole
  - Somme de contrôle d'en-tête
  - Adresse IPv4 source
  - Adresse IPv4 de destination
  - Options et remplissage



Menaces et vulnérabilités IP
L'en-tête de paquet IPv6

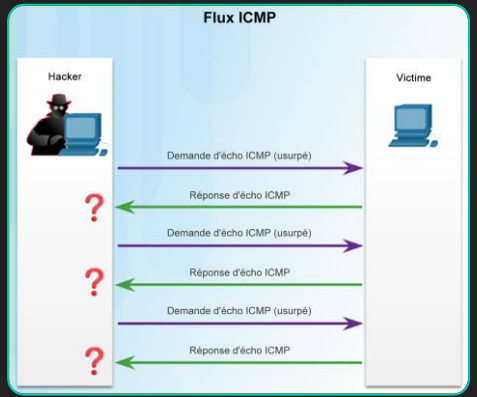
- Un en-tête de paquet IPv4 contient 8 champs :
  - Version
  - Classe de trafic
  - Étiquetage de flux
  - Longueur des données utiles
  - En-tête suivant
  - Limite de nombre de tronçons
  - Adresse IPv6 source
  - Adresse IPv6 de destination



Menaces et vulnérabilités IP
Vulnérabilités IP

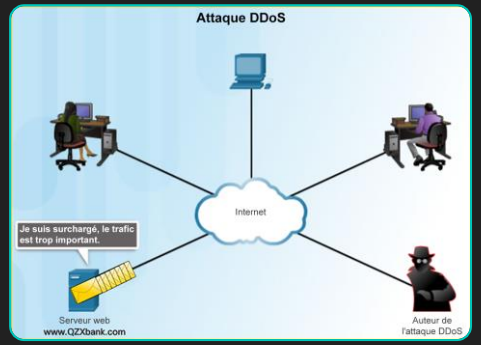
Menaces et vulnérabilités IP
Attaques ICMP

- Le protocole ICMP a été conçu pour transporter des messages de diagnostic et pour signaler des conditions d'erreur lorsque les routes, les hôtes et les ports ne sont pas disponibles. Les messages ICMP sont générés par un appareil en cas d'erreur réseau ou d'interruption.
- Les cyberpirates s'intéressent notamment aux messages ICMP courants suivants :
  - **Requête d'écho et réponse par écho ICMP** : ces messages sont utilisés pour les attaques de vérification de l'hôte et pour les attaques DoS.
  - **ICMP inaccessible** : ce message est utilisé pour les attaques de reconnaissance et d'analyse.
  - **Réponse de masque ICMP** : ce message est utilisé pour cartographier un réseau IP interne.
  - **Redirection ICMP** : ce message est utilisé pour inciter l'hôte cible à envoyer l'ensemble du trafic via un appareil compromis et pour créer une attaque MITM.
  - **Détection de routeur ICMP** : ce message est utilisé pour introduire de fausses entrées de route dans la table de routage d'un hôte cible.



Menaces et vulnérabilités IP
Attaques DoS

- Une attaque DoS vise à empêcher les utilisateurs légitimes d'accéder aux sites web, aux e-mails, aux comptes en ligne et à d'autres services.
- Il existe deux sources majeures d'attaques par déni de service :
  - **Paquets malveillants** : les cyberpirates créent un paquet malveillant et le transmettent à un hôte vulnérable afin de le ralentir ou de le bloquer complètement.
  - **Volume de trafic trop important** : les cyberpirates saturent un réseau, un hôte ou une application cible afin de le ralentir ou de le bloquer complètement.
- Une attaque DoS distribuée (DDoS) combine plusieurs attaques DoS.

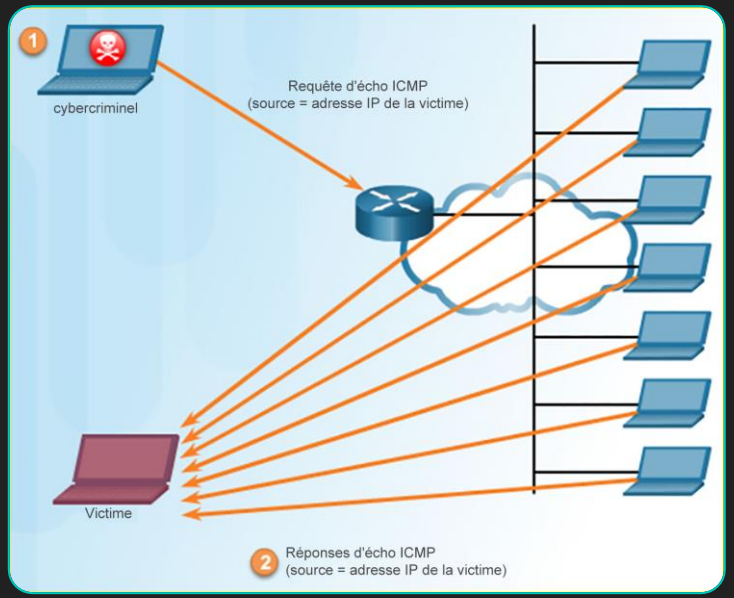


Menaces et vulnérabilités IP
Attaques par amplification et réflexion

- Les cyberpirates utilisent souvent des techniques d'amplification et de réflexion pour créer des attaques DoS. La figure propose un exemple de technique d'amplification et de réflexion (attaque smurf) utilisée pour saturer un hôte cible :

1. **Amplification** : le cyberpirate transmet les messages de requête d'écho ICMP contenant l'adresse IP source de la victime à un grand nombre d'hôtes.

2. **Réflexion** : ces hôtes répondent tous à l'adresse IP usurpée de la victime (et la saturent).



Menaces et vulnérabilités IP
Attaques DDoS

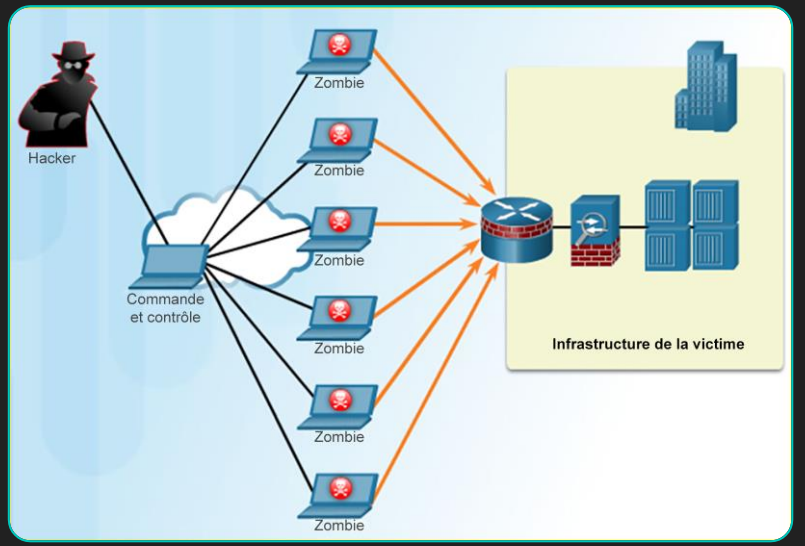
- Les attaques DDoS ont une portée plus importante à celle des attaques DoS, car elles proviennent de sources multiples et coordonnées. Les attaques DDoS introduisent de nouveaux termes (« réseau de zombies », « systèmes de gestionnaire » et « ordinateurs zombies », p. ex.).

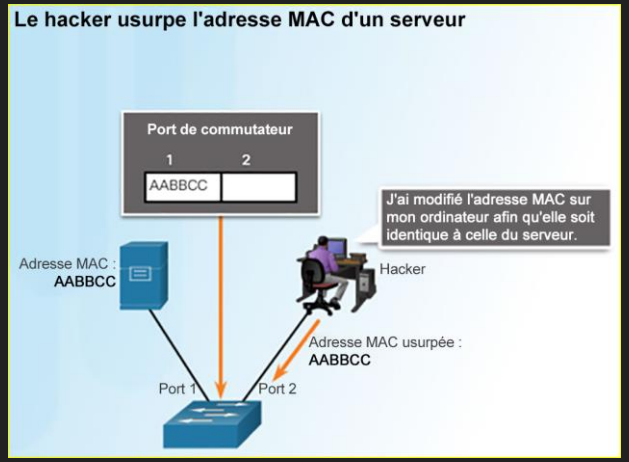
Une attaque DDoS peut se dérouler comme suit :

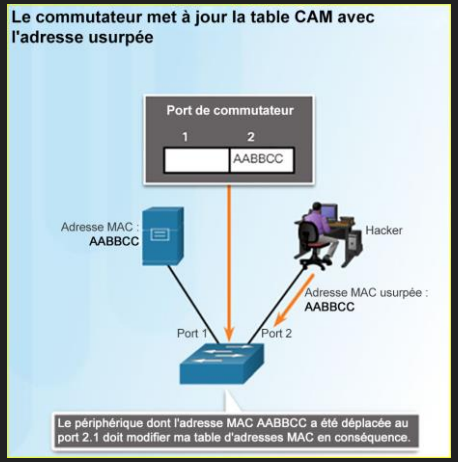
1. Le cyberpirate (botmaster) développe ou acquiert l'utilisation d'un réseau d'hôtes zombies. Le serveur de contrôle-commande (C&C) communique avec des zombies via un canal secret qui utilise un protocole IRC, P2P, DNS, HTTP ou HTTPS.

2. Les ordinateurs « zombies » analysent et infectent toujours plus de cibles afin de créer d'autres zombies.

3. Une fois prêt, le botmaster utilise les systèmes de gestionnaire pour lancer une attaque par déni de service distribuée sur la cible choisie par le biais du réseau de zombies.

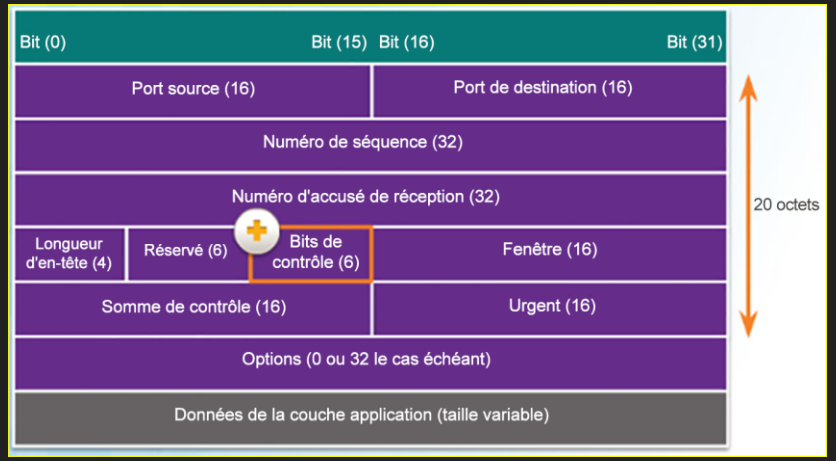


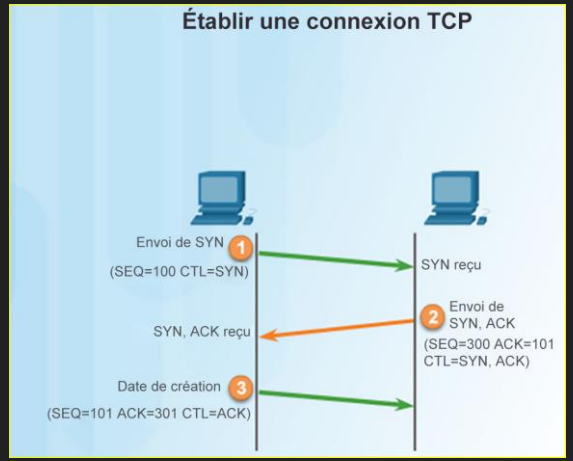




Menaces et vulnérabilités IP
Attaques par usurpation d'adresse

- Les attaques par usurpation d'adresse se produisent lorsqu'un cyberpirate crée des paquets avec de fausses informations sur l'adresse IP source afin de cacher l'identité de l'expéditeur ou de se présenter comme un autre utilisateur légitime. Le hacker peut alors accéder aux données autrement inaccessibles ou contourner les configurations de sécurité.





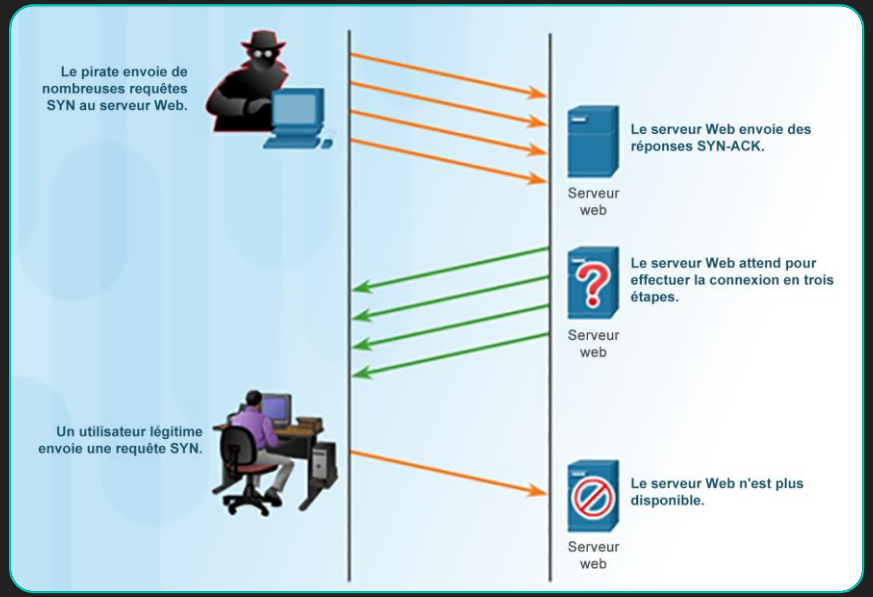
Vulnérabilités TCP et UDP

TCP

- Les informations de segment TCP apparaissent immédiatement après l'en-tête IP.
- Le protocole TCP offre les services suivants :
  - **Acheminement fiable**
  - **Contrôle de flux**
  - **Communication avec état**

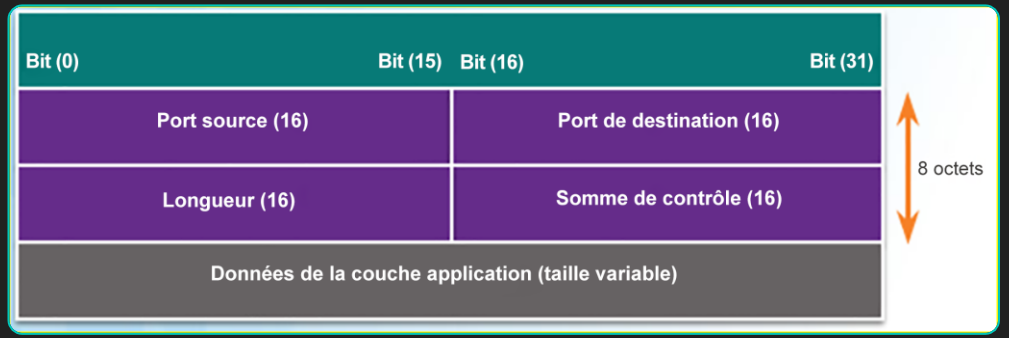
Vulnérabilités TCP et UDP
Attaques TCP

- Même si le protocole TCP est un protocole fiable avec connexion, certaines vulnérabilités peuvent néanmoins être exploitées.
- Les attaques TCP ciblent les comportements attendus du protocole :
  - Attaque par inondation SYN sur TCP
  - Attaque par réinitialisation TCP
  - Piratage de session TCP



Vulnérabilités TCP et UDP
Protocole et attaques UDP

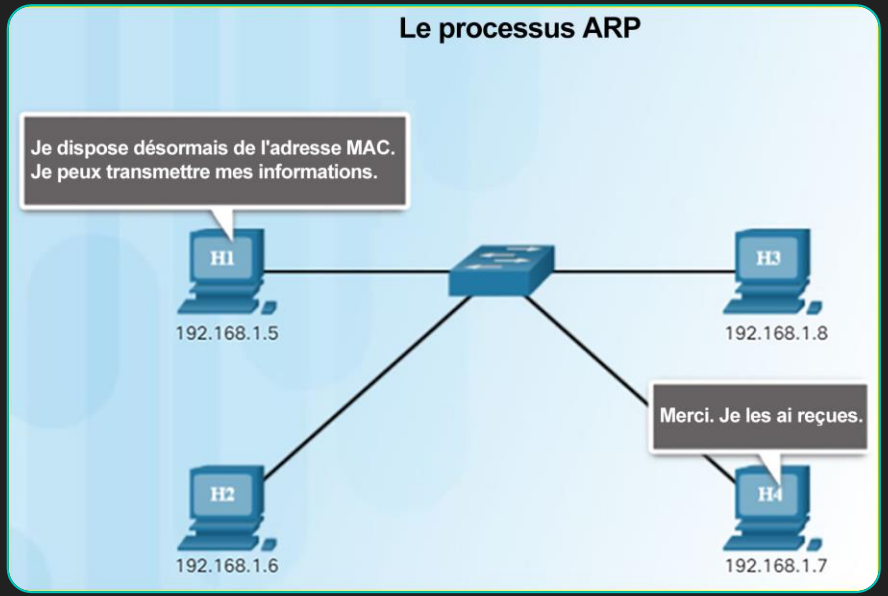
- Le protocole UDP est un protocole simple offrant des fonctions de couche transport de base. Le protocole UDP est généralement utilisé par les protocoles DNS, TFTP, NFS et SNMP. Il est aussi utilisé par les applications en temps réel comme la diffusion multimédia en flux continu ou les transmissions VoIP. Le protocole UDP s'inscrit comme un protocole de couche transport sans connexion.
- Par défaut, le protocole UDP n'est pas protégé par chiffrement. L'absence de chiffrement permet à quiconque de consulter, de modifier et d'envoyer le trafic vers sa propre destination.
- Les attaques de protocole UDP ciblent l'absence de comportements du protocole (UDP) :
  - Attaque contre la somme de contrôle UDP
  - Attaque par inondation UDP
  - Attaques DoS UDP



Attaques ciblant les activités

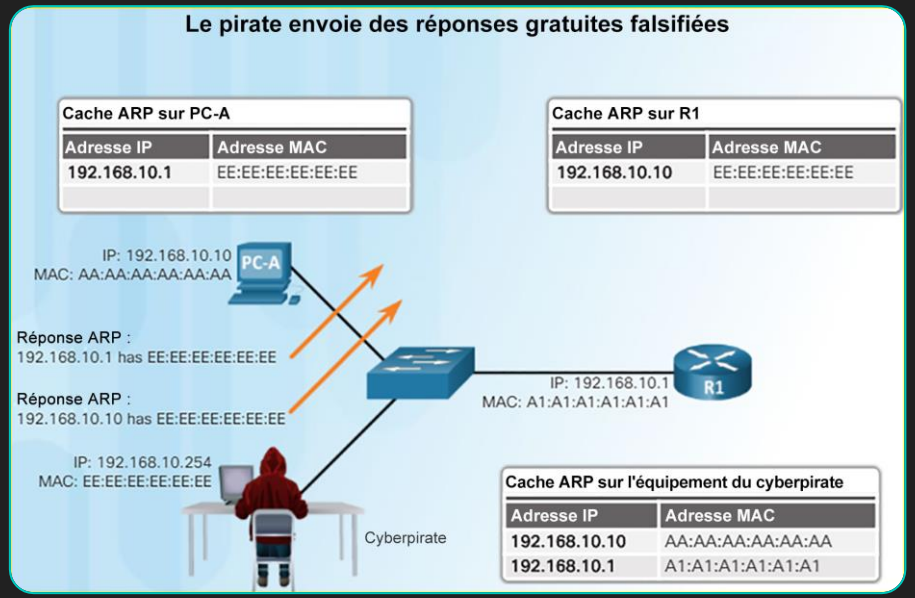
Services IP
Vulnérabilités ARP

- Les hôtes diffusent une requête ARP vers d'autres hôtes sur le segment afin de déterminer l'adresse MAC d'un hôte doté d'une adresse IP spécifique.
- Tous les hôtes du sous-réseau reçoivent et traitent la requête ARP.
- L'hôte dont l'adresse IP correspond à la requête ARP envoie une réponse ARP.



Services IP
Empoisonnement du cache ARP

- Les attaques par empoisonnement du cache ARP empoisonnent délibérément le cache d'un autre ordinateur avec des mappages adresse IP-adresse MAC usurpés.

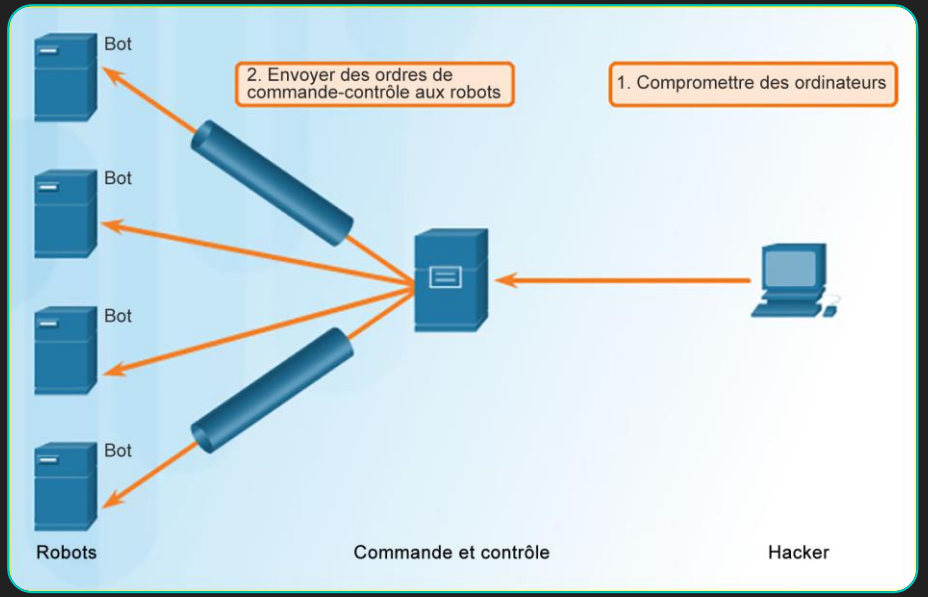


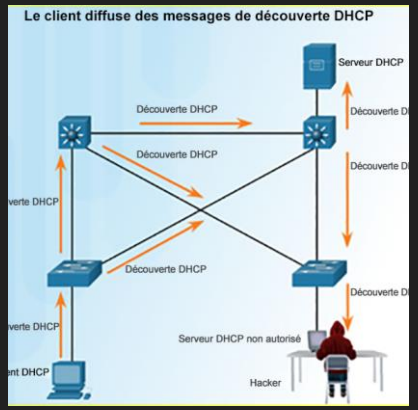
Services IP
Attaques DNS

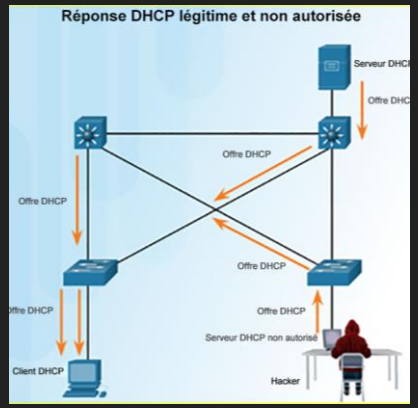
- Les serveurs DNS attribuent un nom à des adresses IP et représentent une cible majeure pour les hackers. Voici quelques exploits DNS :
  - **Programmes de résolution DNS ouverts** (serveurs de noms publics)
  - **Attaques furtives DNS**
  - **Attaques par dissimulation DNS** : des domaines piratés sont utilisés pour créer des sous-domaines chargés de la résolution en sites web malveillants
  - **Attaques par tunnellisation DNS** : elles dissimulent des instructions malveillantes dans des requêtes et des réponses DNS

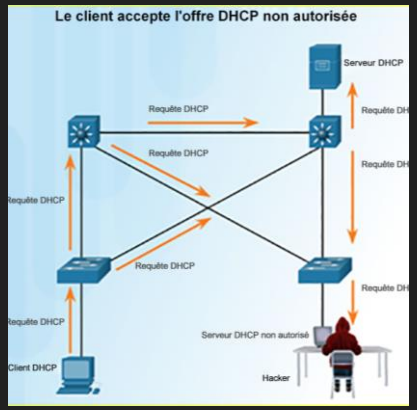
Services IP
Tunnellisation DNS

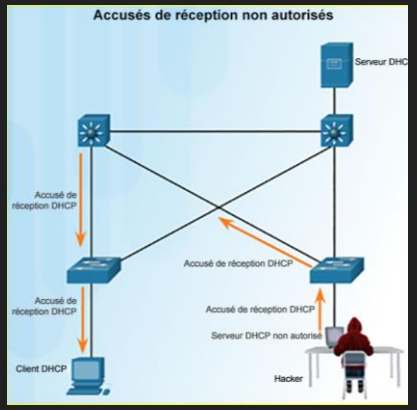
- Les cyberpirates qui utilisent une attaque DNS par tunnellisation introduisent un trafic non DNS dans le trafic DNS. Cette méthode permet généralement de contourner les solutions de sécurité. Lorsque le cyberpirate lance une attaque DNS par tunnellisation, les différents types d'enregistrements DNS (TXT, MX, SRV, NULL, A ou CNAME, p. ex.) sont modifiés.











Services IP DHCP

- Suite à une attaque DHCP, chaque hôte du réseau est susceptible de communiquer avec des passerelles et des serveurs DNS malveillants. Une attaque par surveillance DHCP crée un serveur DHCP non autorisé en direction d'un serveur contenant des informations falsifiées.

Services d'entreprise HTTP et HTTPS

- Internet est sans aucun doute le vecteur d'attaque le plus important. Les analystes en charge de la sécurité doivent avoir une connaissance approfondie du fonctionnement des attaques web.
  - **iFrames malveillants** : un iFrame permet à une page d'un autre domaine d'être ouverte en direct dans la page actuelle. Un iFrame peut servir à lancer du code malveillant.
  - **Amortisseur HTTP 302** : permet à une page web d'effectuer une redirection et d'ouvrir une autre URL. Permet de rediriger le trafic vers un code malveillant.
  - **Domaines miroirs :** des sites web malveillants sont créés à partir de sous-domaines créés dans un domaine piraté.

Services d'entreprise
E-mail

- Les utilisateurs accèdent à des e-mails depuis de nombreux appareils différents qui souvent ne sont pas protégés par le pare-feu de l'entreprise.
  - **Attaques basées sur les pièces jointes** : un e-mail auquel sont joints des fichiers exécutables malveillants.
  - **Attaque par usurpation d'adresse** : attaque de phishing lors de laquelle le message semble provenir d'une source légitime.
  - **Spam** : e-mail non sollicité renfermant des publicités ou du contenu malveillant.
  - **Serveur Open Mail Relay** : des serveurs de messagerie mal configurés envoient d'importantes quantités de spam et de vers.
  - **Homoglyphes** : une méthode de phishing, où les caractères de texte
    (liens hypertextes) ressemblent aux véritables liens et textes.

Services d'entreprise
Bases de données exposées sur le web

- Les applications web se connectent généralement à une base de données relationnelle. Ces bases de données relationnelles contiennent souvent des données sensibles, c'est pourquoi elles sont souvent la cible d'attaques.
  - **Attaques par injection de commandes** : si les applications web et le code ne sont pas protégés, des commandes OS peuvent être injectées dans les champs du formulaire ou la barre d'adresse.
  - **Attaques par scripts intersites** : si un script n'est pas protégé côté serveur sans entrée validée, des commandes de scripts peuvent être insérées dans les champs des formulaires générés par les utilisateurs comme des commentaires sur une page web. Cela se traduit par la redirection des internautes vers un
    site web malveillant avec le code de malware.
  - **Attaques par injection de code SQL** : si un script n'est pas protégé côté serveur, des commandes SQL peuvent être insérées dans les champs de formulaires sans entrée validée.
  - **Attaques par injection de code HTTP** : la manipulation du code HTML permet d'injecter du code exécutable par le biais de balises div HTML, etc.

Récapitulatif

Récapitulatif

- Tous les réseaux peuvent être ciblés et doivent être protégés à l'aide d'une approche de défense en profondeur.
- Pour vérifier que le comportement du réseau est normal, ils peuvent notamment utiliser les outils suivants : les systèmes de détection des intrusions (IDS), les analyseurs de paquets, SNMP ou NetFlow.
- Le point d'accès réseau test transfère l'ensemble du trafic (y compris les erreurs de la couche physique) vers un appareil d'analyse.
- La mise en miroir du port permet à un commutateur de copier des trames d'un ou de plusieurs ports vers un port SPAN (Switch Port Analyzer) connecté à un appareil d'analyse.
- Les analystes peuvent utiliser des analyseurs de protocoles tels que Wireshark et tcpdump pour voir les échanges réseau jusqu'au niveau du paquet.
- La fonctionnalité NetFlow peut être utilisée à des fins de surveillance du réseau et de la sécurité, de planification du réseau et d'analyse du trafic. Toutefois, elle ne permet pas de capturer le contenu.
- Les systèmes de gestion des informations et des événements liés à la sécurité (SIEM) fournissent des rapports en temps réel et des analyses à long terme des événements liés à la sécurité.
- Splunk et ELK sont deux systèmes SIEM propriétaires utilisés dans les centres opérationnels de sécurité.

Récapitulatif (suite)

- Les analystes en charge de la sécurité doivent connaître les différents champs des en-têtes IPv4 et IPv6, car les hackers peuvent falsifier les informations des paquets.
- L'en-tête de paquet IPv4 contient 10 champs : Version, Longueur d'en-tête Internet, Services différenciés ou DiffServ (DS), Durée totale, Identification, Indicateur et Décalage du fragment, Durée de vie (TTL), Protocole, Somme de contrôle d'en-tête, Adresse IPv4 source, Adresse IPv4 de destination, Options et Remplissage.
- L'en-tête de paquet IPv4 contient 8 champs : Version, Classe de trafic, Étiquetage de flux, Longueur des données utiles, Prochain en-tête, Limite du nombre de sauts, Adresse IPv6 source et Adresse IPv6 de destination.
- Les vulnérabilités IP incluent les attaques ICMP, les attaques DoS et DDoS, l'usurpation d'adresse, les attaques MITM et les piratages de session.
- Le protocole ICMP a été conçu pour transporter des messages de diagnostic et pour signaler des conditions d'erreur lorsque les routes, les hôtes et les ports ne sont pas disponibles. Les messages ICMP sont générés par un appareil en cas d'erreur réseau ou d'interruption.

Récapitulatif (suite)

- Une attaque DoS vise à empêcher les utilisateurs légitimes d'accéder aux sites web, aux e-mails, aux comptes en ligne et à d'autres services.
- Les cyberpirates utilisent souvent des techniques d'amplification et de réflexion pour créer des attaques DoS.
- Les attaques DDoS ont une portée plus importante à celle des attaques DoS, car elles proviennent de sources multiples. Les attaques DDoS introduisent les termes « réseau de zombies », « systèmes de gestionnaire » et « ordinateurs zombies ».
- Les attaques par usurpation d'adresse se produisent lorsqu'un cyberpirate crée des paquets avec de fausses informations sur l'adresse IP source afin de cacher l'identité de l'expéditeur ou de se présenter comme un autre utilisateur légitime.
- Le protocole TCP offre les services suivants : acheminement fiable, contrôle de flux, communication avec état.
- Même si le protocole TCP est un protocole fiable avec connexion, certaines vulnérabilités peuvent néanmoins être exploitées.
- Le protocole UDP est un protocole simple offrant des fonctions de couche transport de base. 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.

Récapitulatif (suite)

- Les hôtes diffusent une requête ARP vers d'autres hôtes sur le segment afin de déterminer l'adresse MAC d'un hôte doté d'une adresse IP spécifique.
- Les attaques par empoisonnement du cache ARP empoisonnent délibérément le cache d'un autre ordinateur avec des mappages adresse IP-adresse MAC usurpés.
- Les serveurs DNS attribuent un nom à des adresses IP et représentent une cible majeure pour les hackers.
- Les cyberpirates qui utilisent une attaque DNS par tunnellisation introduisent un trafic non DNS dans le trafic DNS.
- Une attaque par surveillance DHCP crée un serveur DHCP non autorisé en direction d'un serveur contenant des informations falsifiées.
- La navigation Internet est sans aucun doute le vecteur d'attaque le plus important, et ce que le protocole utilisé soit HTTP ou HTTPs. Les analystes en charge de la sécurité doivent avoir une connaissance approfondie du fonctionnement des attaques web.
- Vous accédez à vos e-mails depuis de nombreux appareils différents qui souvent ne sont pas protégés par le pare-feu de l'entreprise.
- Les applications web se connectent généralement à une base de données relationnelle. Ces bases de données relationnelles contiennent souvent des données sensibles, c'est pourquoi elles sont souvent la cible d'attaques.

Chapitre 15-17
Les nouveaux termes

- Technique d'attaque par amplification et par réflexion
- Empoisonnement du cache ARP
- Usurpation aveugle
- Cross-Site Scripting (XSS)
- Tunnellisation DNS
- algorithmes de génération de domaine
- Domaines miroirs
- Double flux IP
- flux rapide
- Homoglyphes
- Redirection HTTP 302
- iFrame
- Système de surveillance du réseau
- Usurpation non aveugle
- Prise d'empreintes du SE
- mise en miroir des ports
- Piratage de session
- Injection SQL
- Analyseur de port commuté (SPAN)