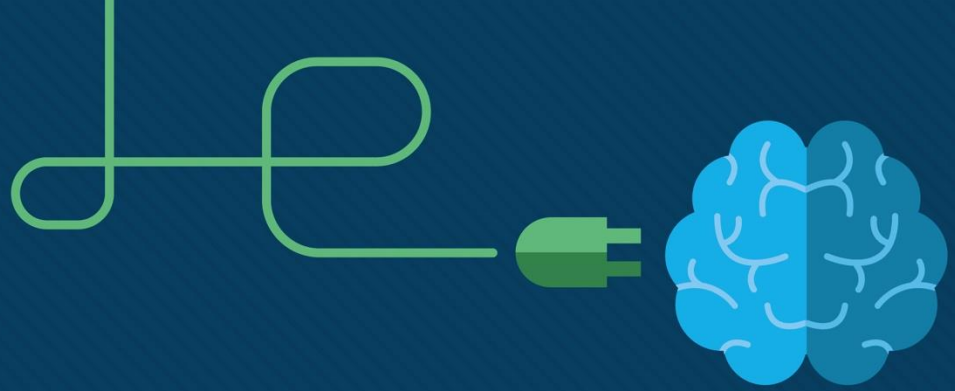


Module 7: les menaces et les attaques communes.

CyberOps Associate v1.0

Objectifs du module

Titre de Module: les menaces et les attaques communes.

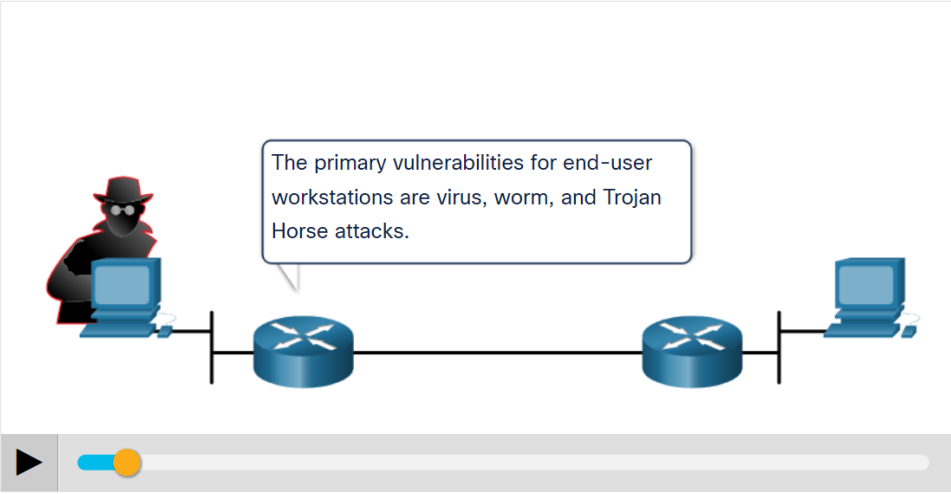
Objectif de Module: Expliquer les divers types de menaces et d'attaques.

Titre du Rubrique	Objectif du Rubrique
Malware	Décrire les types de programmes malveillants.
Les attaques réseau courantes - Reconnaissance, Accès et Ingénierie Sociale	Expliquer les attaques de réseau: reconnaissance, accès et ingénierie sociale.
Les attaques réseau - Déni de Service, Dépassement de La Mémoire Tampon et Contournement	Expliquer les attaques par déni de service, dépassement de la mémoire tampon et contournement.

7.1 Les malwares

Types de Malware

- Il s'agit d'un code ou d'un logiciel spécifiquement conçu pour endommager, perturber, voler ou infliger une action "mauvaise" ou illégitime sur des données, des hôtes ou des réseaux.
- Les trois types de logiciels malveillants les plus courants sont les vers, les virus et les chevaux de Troie.
- Lisez l'animation pour afficher des exemples des différents types de logiciels malveillants.



Virus

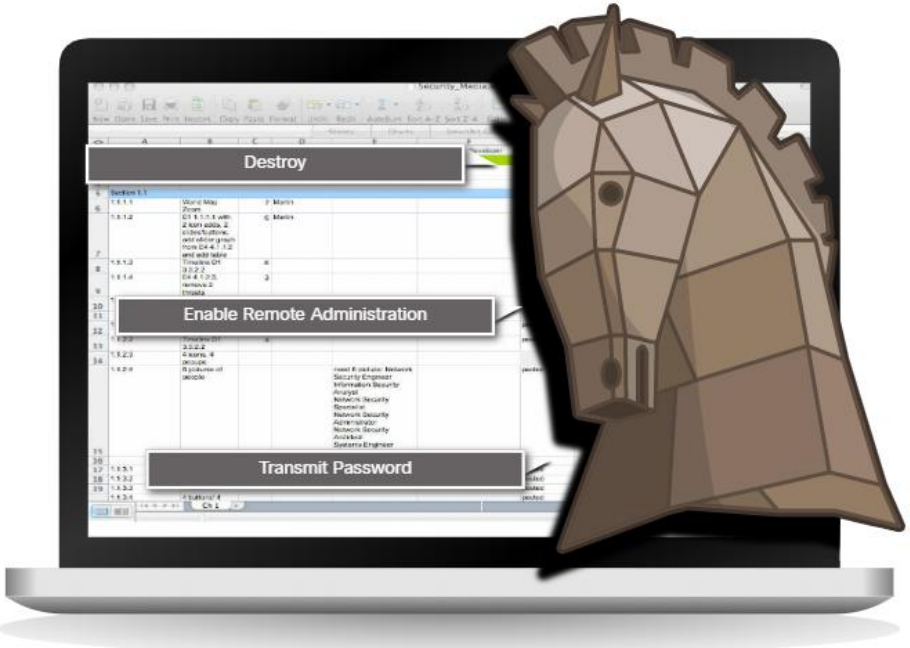
- Un virus est un type de logiciel malveillant qui se propage en insérant une copie de lui-même dans un autre programme.
- Après l'exécution du programme, les virus infectent ensuite une série d'ordinateurs en passant de l'un à l'autre.
- Un virus simple peut s'installer à la première ligne de code d'un fichier exécutable.
- Un virus peut être inoffensif et se contenter d'afficher une image à l'écran, ou être destructeur et modifier ou supprimer des fichiers du disque dur. Ils peuvent également modifier ou supprimer des fichiers sur le disque dur.
- Actuellement, la plupart des virus sont propagés par des lecteurs USB, des CD, des DVD, des partages réseau ou des e-mails. Les virus par e-mail sont actuellement les plus répandus.

Chevaux deTroie

- En cybersécurité, un cheval de Troie est un logiciel qui semble légitime, mais contient du code malveillant qui exploite les autorisations d'accès de l'utilisateur qui l'exécute.
- Ils sont fréquemment associés à des jeux en ligne.
- Les utilisateurs sont régulièrement incités à télécharger et à exécuter ces chevaux de Troie sur leurs systèmes à leur insu.
- Le concept de cheval de Troie est flexible.
- Il peut causer des dommages immédiats, ouvrir un accès distant au système ou y accéder par une porte dérobée.
- Les chevaux de Troie à usage spécifique sont difficiles à détecter, en particulier ceux qui sont créés pour s'attaquer à une cible précise.

Chevaux deTroie Classification

- Les chevaux de Troie sont généralement classés en fonction des dégâts qu'ils provoquent ou de la manière dont ils s'introduisent dans un système, comme illustré dans la figure :



Classification des chevaux deTroie (Cont.)

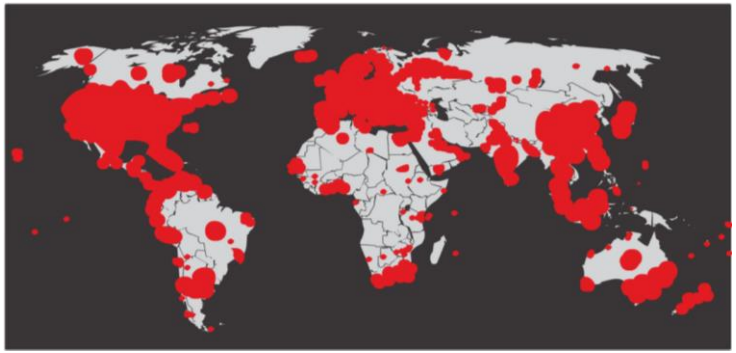
Les types de chevaux de Troie sont les suivants :

Type de cheval de Troie	Description
Accès distant	Permet un accès distant non autorisé.
Envoi de données	Fournit à l'acteur de menace des données sensibles, telles que des mots de passe.
Destructeur	Endommage ou supprime des fichiers.
Proxy	Utilise l'ordinateur de la victime pour lancer des attaques et pratiquer d'autres activités illégales.
FTP	Permet le transfert non autorisé de fichiers sur les périphériques finaux.
Désactivation des logiciels de sécurité	Empêche les logiciels antivirus ou les pare-feu de fonctionner.
Déni de service (DoS)	Ralentit ou interrompt l'activité réseau.
Enregistreur de frappe	Tente activement de dérober des informations confidentielles, telles que des numéros de carte de paiement, en enregistrant des frappes de touches dans un formulaire web.

Vers

- Mais les vers ont la capacité de se répliquer eux-mêmes en exploitant, en toute autonomie, les vulnérabilités des réseaux.
- Ils ralentissent le réseau tout en se propageant d'un système à l'autre.
- Les vers s'exécutent à l'intérieur d'un programme hôte.
- Cependant, une fois que l'hôte est infecté, le ver se propage rapidement sur le réseau.
- En 2001, le ver Code Red avait infecté 658 serveurs. 19 heures plus tard, plus de 300,000 serveurs étaient infectés.

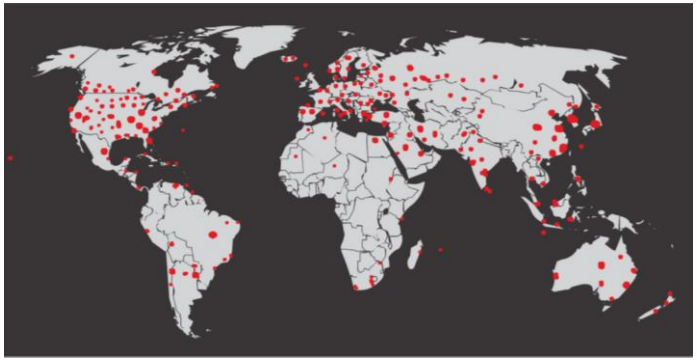
État initial de l’infection par le ver Code Red



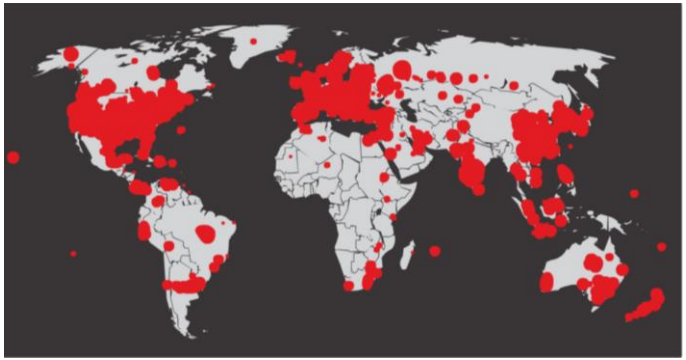
Infection par le Code Red 19 heures plus tard

Vers

- L'infection initiale par le ver SQL Slammer, connu comme le ver qui a mangé Internet.
- SQL Slammer mettait en œuvre une attaque DoS exploitant un bug de dépassement de mémoire tampon « buffer overflow» dans Microsoft SQL Server.
- Au plus fort de son attaque, le nombre de serveurs infectés doublait toutes les 8,5 secondes.
- Mais les serveurs infectés ne l'avaient pas encore appliqué.
- Cet incident a permis de tirer le signal d'alarme dans plusieurs entreprises, qui alors ont mis en place une politique de sécurité exigeant que les mises à jour et les correctifs soient appliqués dans les meilleurs délais.



État initial de l’infection par le ver SQL Slammer



Infection par le ver SQL Slammer 30 minutes plus ta

Ransomware

- Un ransomware est un malware qui bloque l'accès à l'ordinateur infecté ou à ses données jusqu'à ce que le propriétaire accepte de payer une rançon.
- La plupart d'entre eux utilisent un algorithme pour chiffrer les systèmes de fichiers et les données.
- L'e-mail et la publicité malveillante, parfois appelée « malvertising », sont souvent utilisés pour lancer des attaques de ransomware.
- L'ingénierie sociale est également utilisée. Des hackers se font passer pour des techniciens en sécurité et appellent des utilisateurs chez eux pour les persuader de se connecter à un site web qui téléchargera le ransomware sur l'ordinateur ciblé.

Comportements des malwares courants

- Un ordinateur infecté manifestera un ou plusieurs des symptômes suivants :
  - Apparition de fichiers, de programmes ou d'icônes du bureau anormaux
  - Désactivation des programmes antivirus et pare-feu, ou reconfiguration de leurs paramètres
  - Gel de l'écran ou défaillances du système
  - Envoi automatique d'e-mails à des personnes de votre liste de contacts
  - Modification ou suppression de fichiers
  - Utilisation accrue du CPU ou de la mémoire
  - Problèmes de connexion aux réseaux
  - Ordinateur ou navigateur web ralenti
  - Exécution de processus ou de services inconnus
  - Ports TCP ou UDP inconnus ouverts
  - Connexion à des hôtes sur Internet sans action de l'utilisateur
  - Comportement anormal de l'ordinateur
- **remarque:** cette liste n'est pas exhaustive.

7.2 Les attaques réseau courantes - reconnaissance, accès et ingénierie sociale

Types d'attaques reseau

- Un malware est un outil permettant d'acheminer une charge utile.
- Une fois cette charge utile libérée et installée, elle peut être utilisée pour lancer un grand nombre d'attaques provenant de l'intérieur du réseau ciblé.
- Les attaques de réseau peuvent être classées en trois catégories principales:
  - Attaques de reconnaissance
  - Attaques par accès
  - Attaques DoS

Attaque de reconnaissance

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

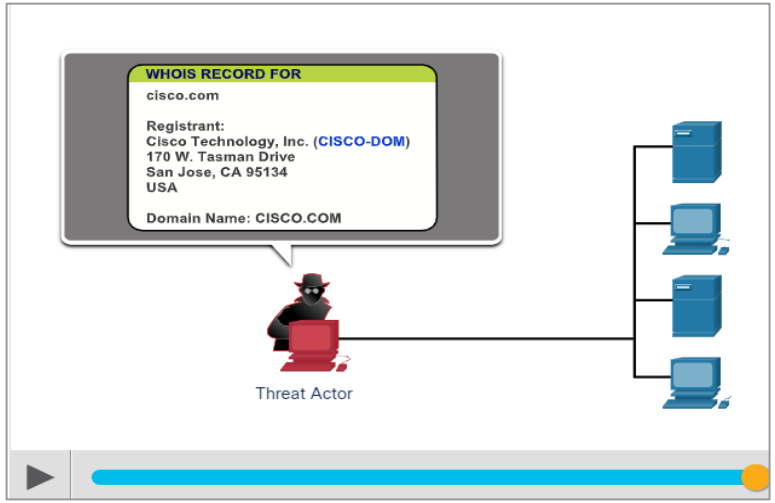
Attaque de reconnaissance (Suite)

Voici quelques-unes des techniques utilisées par les cyberpirates pour lancer des attaques de reconnaissance :

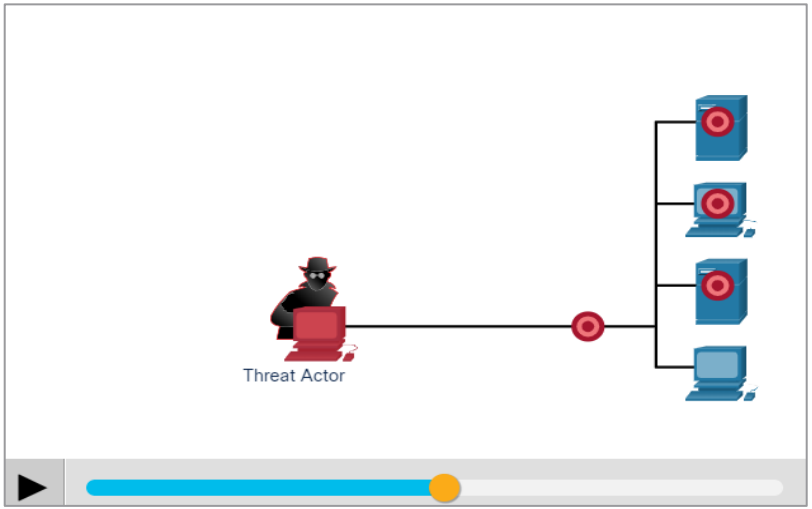
Technique	Description
Exécuter une requête d'information sur une cible	L'acteur de menace recherche les premières informations sur une cible. Divers outils peuvent être utilisés, notamment la recherche Google, le site Web des organisations, le whois, etc.
Lancer un balayage ping du réseau cible	La requête 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. Nipper, Secunia PSI, Core Impact, Nessus v6, SAINT et Open VAS sont quelques exemples de ces outils.
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.

Attaque de reconnaissance (Suite)

Internet Information Queries: Cliquez sur Lecture dans la figure pour afficher une animation d'un acteur de menace à l'aide de la commande whois pour rechercher des informations sur une cible.

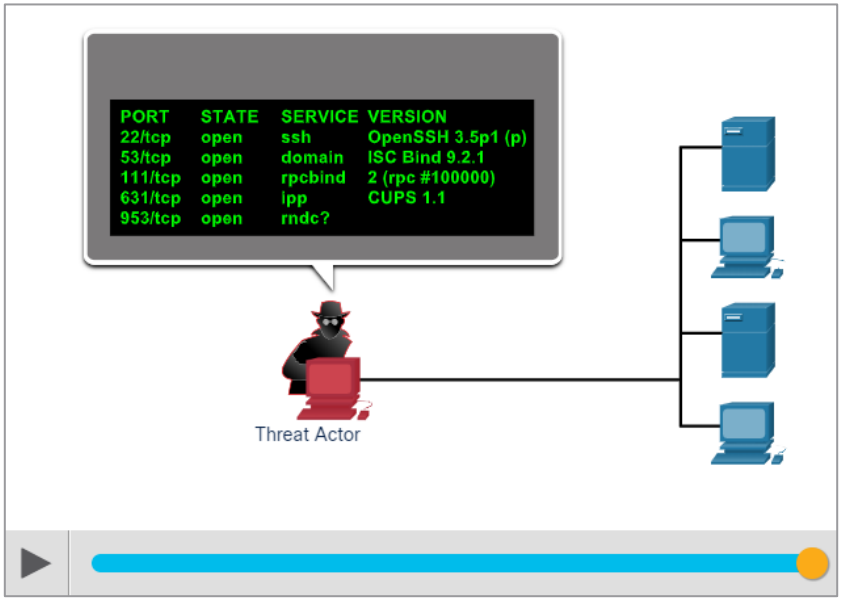


Performing Ping Sweep: Cliquez sur Lecture dans la figure pour afficher une animation d'un acteur de menace effectuant un balayage ping de l'adresse réseau de la cible pour découvrir des adresses IP actives



Attaque de reconnaissance (Suite)

Performing Port Scan: Cliquez sur Lecture dans la figure pour afficher une animation d'un acteur de menace effectuant une analyse de port sur les adresses IP actives découvertes à l'aide de Nmap.



Attaque d’accès (Suite)

- Les attaques par accès exploitent les vulnérabilités connues des services d'authentification, services FTP et services web pour accéder à des comptes web, des bases de données confidentielles et d'autres informations sensibles.

Attaques de mot de passe

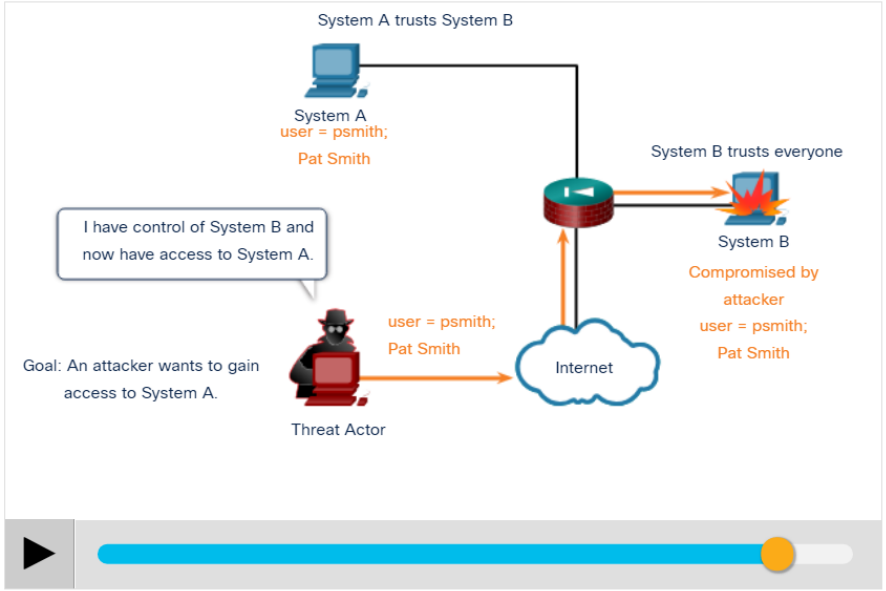
- Dans une attaque par mot de passe, l'acteur de menace tente de découvrir les mots de passe des systèmes critiques en utilisant diverses méthodes.

Attaques par usurpation

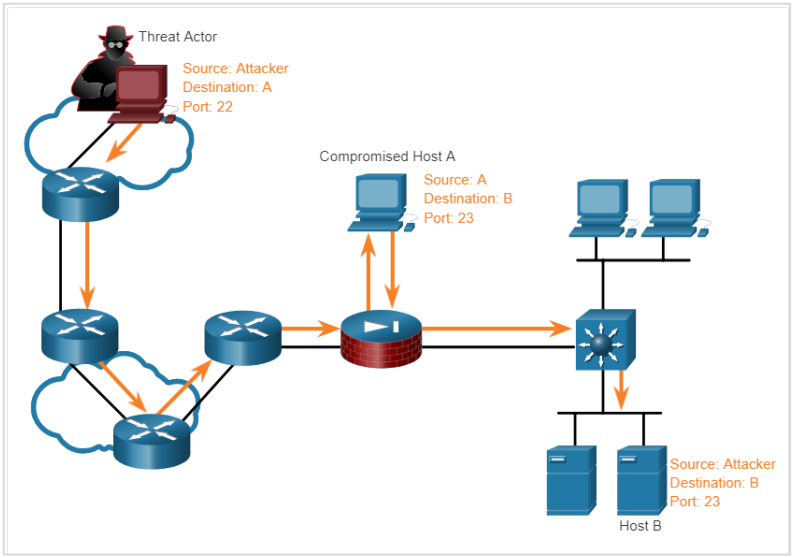
- Dans les attaques d'usurpation d'identité, le dispositif d'acteur de menace tente de se faire passer pour un autre dispositif en falsifiant les données.
- Les attaques d'usurpation d'identité courantes incluent l'usurpation d'adresse IP, l'usurpation d'adresse MAC et l'usurpation d'identité DHCP.
    - Exploiter la confiance
    - Redirection de port
    - Attaques de l'homme-au-milieu
    - Attaques par débordement de la mémoire tampon

Attaque d'accès (Suite)

Trust Exploitation Example: Cliquez sur Lecture dans la figure pour afficher un exemple d'exploitation de confiance.29-04-2020 01:33.

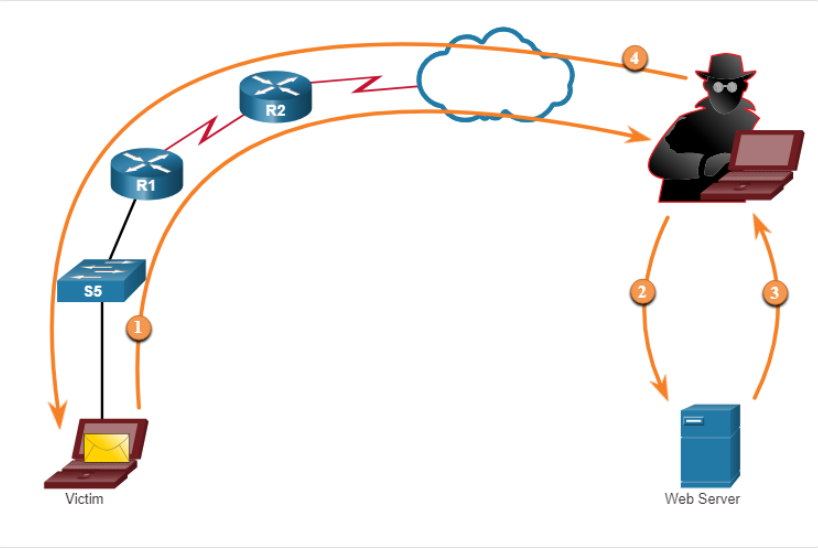


L'exemple de redirection de port présenté sur la figure montre un acteur de menace qui utilise le protocole SSH (port 22) pour se connecter à un hôte compromis A. Hôte A est réputé fiable par l'hôte B. Ainsi, l'acteur de menace utilise Telnet (port 23) pour l'accéder.

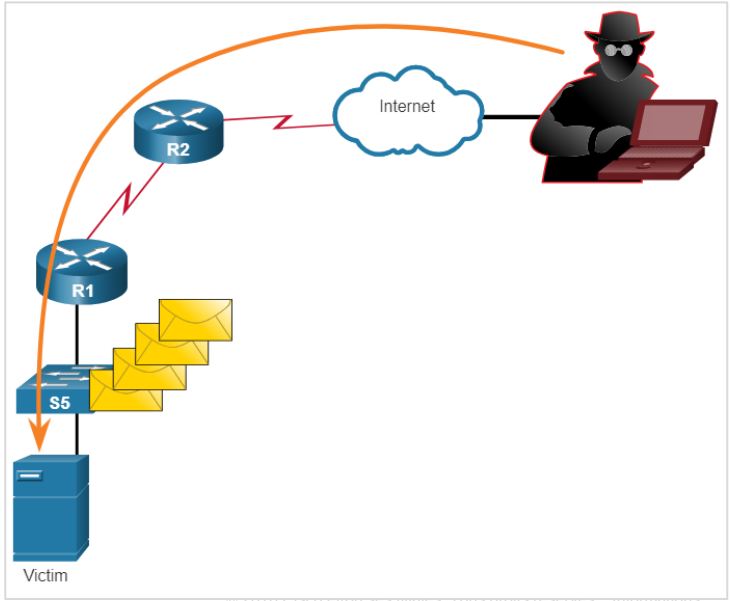


Attaque d'accès (Suite)

La figure présente un exemple d'attaque de l'homme du milieu (man-in-the-middle).



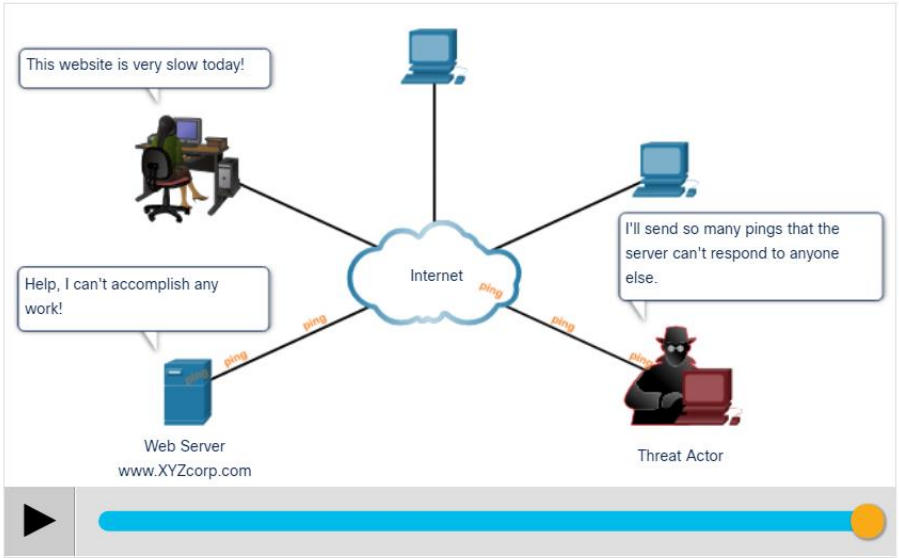
Buffer Overflow Attack: La figure montre que l'acteur de la menace envoie de nombreux paquets à la victime pour tenter de déborder le tampon de la victime.



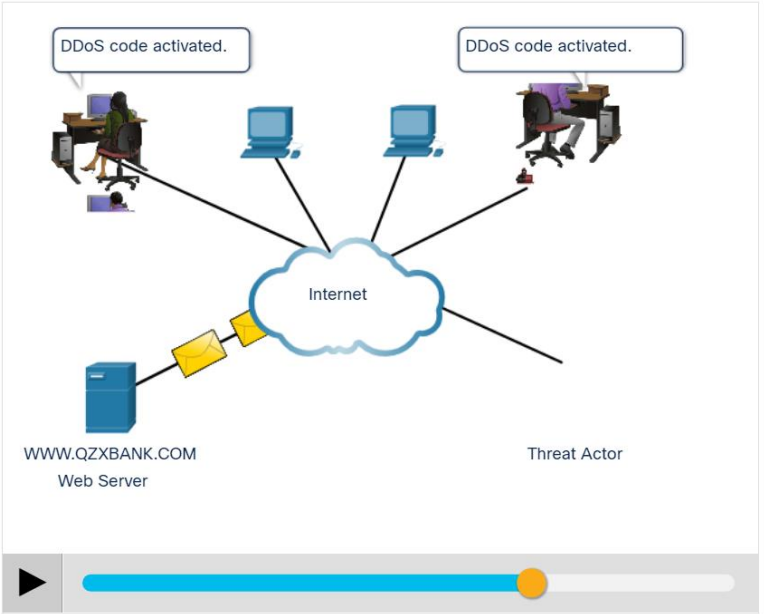
7.3 Les attaques réseau - Déni de Service, Dépassement de La Mémoire Tampon et Contournement

Attaques DoS et DDoS

DoS Attack: Cliquez sur Lecture dans la figure pour afficher l'animation d'une attaque par déni de service (DoS).



DoS Attack: Cliquez sur Lecture dans la figure pour afficher l'animation d'une attaque par déni de service (DoS).



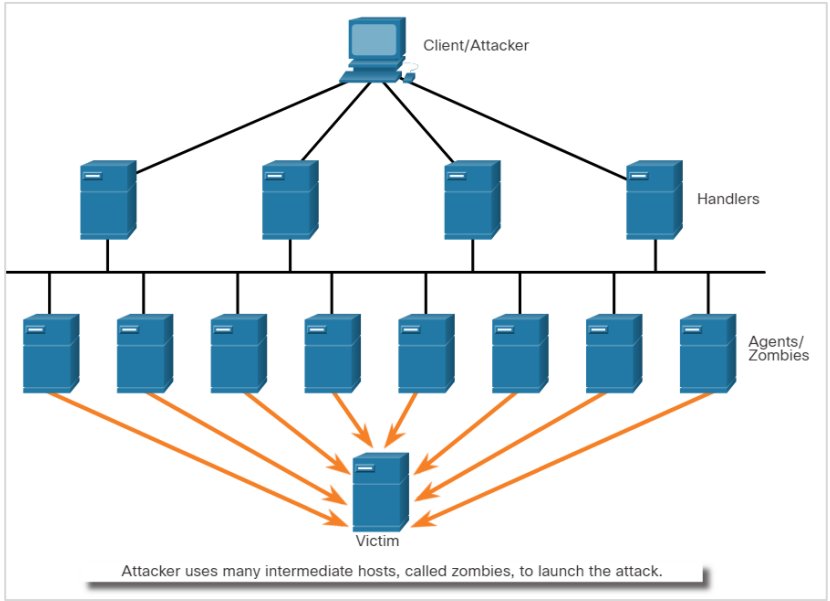
Attaques DoS et DDoS(Suite.)

- 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.
- **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.

Attaques DoS et DDoS(Suite.)

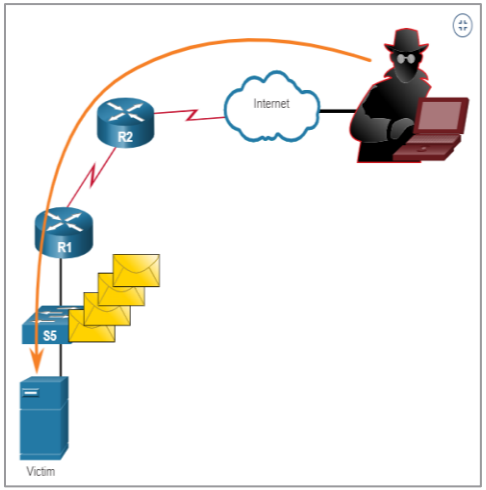
Les termes suivants sont utilisés pour décrire les composants d'une attaque DDoS :

Composant	Description
Zombies	Un groupe d'hôtes compromis. Ces hôtes exécutent du code malveillant.
bots	Les Bots sont des logiciels malveillants conçus pour infecter un hôte et communiquer avec un système gestionnaire.
réseau de zombies	Il s'agit d'un groupe de zombies infectés par un logiciel malveillant à propagation autonome (les bots) et contrôlés par des gestionnaires.
Gestionnaires	il s'agit d'un serveur maître de type commande et contrôle (CnC or C2) contrôlant les groupes de zombies.
Botmaster	Permet le transfert non autorisé de fichiers sur les périphériques finaux.



Dépassement la memoire tampon

- L'objectif d'un cyberpirate lors d'une attaque DoS par dépassement de la mémoire tampon consiste à trouver une faille associée à la mémoire système d'un serveur en vue de l'exploiter.
- Par exemple, une vulnérabilité d'attaque par déni de service à distance a été découverte dans Microsoft Windows 10, où l'acteur de menace a créé du code malveillant pour accéder à la mémoire hors portée.
- Un autre exemple est **ping of death**, où un acteur de menace envoie un ping of death, qui est une requête d'écho dans un paquet IP qui est supérieure à la taille maximale du paquet.
- L'hôte destinataire était incapable de traiter un paquet de cette taille, ce qui le mettait hors service.
- **Remarque :** on estime qu'un tiers des attaques malveillantes résultent de dépassement de la mémoire tampon.




CISCO

7.4 Récapitulation des menaces et attaques communes

Qu'ai-je appris dans ce module ?

- Le mot « malware » est un mot-valise formé à partir des termes « malicious » et « software ».
- Actuellement, la plupart des virus sont propagés par des lecteurs USB, des CD, des DVD, des partages réseau ou des e-mails.
- Les chevaux de Troie se trouvent dans les jeux en ligne.
- Les trois types de logiciels malveillants les plus courants sont les vers, les virus et les chevaux de Troie.
- Il arrive également aux cyberpirates d'attaquer un réseau de l'extérieur.
- Les trois principales catégories sont la reconnaissance, l'accès et les attaques DoS.
- Les attaques Recon précèdent les attaques d'accès ou les attaques DoS.
- 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.
- Les attaques DoS qui créent une sorte d'interruption des services réseau pour les utilisateurs, les appareils ou les applications.

Qu'ai-je appris dans ce module ? (suite)

- Les attaques DDoS suivent la même logique que les attaques DoS, mais ont une ampleur bien plus importante, car elles proviennent de sources multiples et coordonnées.
- Mirai est un programme malveillant qui cible les appareils IoT configurés avec des informations de connexion par défaut.
- L'objectif d'un cyberpirate lors d'une attaque DoS par dépassement de la mémoire tampon consiste à trouver une faille associée à la mémoire système d'un serveur en vue de l'exploiter.