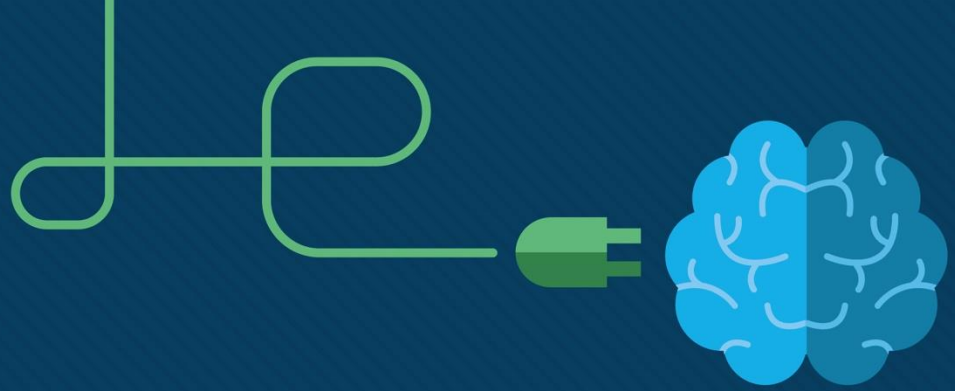


Module : Conception de sécurité LAN

Notions de base sur la commutation, le routage et le sans fil v7.0 (SRWE)

Objectifs de ce module

Titre du module: Conception de sécurité du réseau local LAN

Objectif du module: Expliquez comment les vulnérabilités compromettent la sécurité du réseau local.

Titre du rubrique	Objectif du rubrique
Sécurité des terminaux	Expliquez comment utiliser la sécurité des terminaux pour atténuer les attaques.
Contrôle d'accès	Expliquez comment AAA et 802.1x sont utilisés pour authentifier les périphériques et les terminaux LAN.
Menaces de la sécurité de couche 2	Identifiez les vulnérabilités de couche 2.
Attaque du table d'adresses MAC	Expliquez comment une attaque de table d'adresses MAC compromet la sécurité du réseau LAN.
Les attaques de réseau LAN	Expliquez comment les attaques LAN compromettent la sécurité LAN.

.1 La sécurité des terminaux

Les attaques de réseau au quotidien

Les médias d'information couvrent généralement les attaques contre les réseaux d'entreprise. Recherchez simplement sur Internet les «dernières attaques réseau» pour trouver des informations à jour sur les attaques en cours. Probablement, ces attaques impliqueront un ou plusieurs les éléments suivants:

- **Déni de service distribué (DDoS)** - Il s'agit d'une attaque coordonnée de nombreux périphériques, appelés zombies, dans le but de dégrader ou d'interrompre l'accès du public au site Web et aux ressources d'une organisation.
- **Violation de données** – Il s'agit d'une attaque dans laquelle les serveurs de données ou les hôtes d'une organisation sont compromis pour voler des informations confidentielles.
- **Programme malveillant** – Il s'agit d'une attaque dans laquelle les hôtes d'une organisation sont infectés par des logiciels malveillants qui provoquent des problèmes différentes. Par exemple, un ransomware comme WannaCry chiffre les données sur un hôte et verrouille l'accès jusqu'à ce qu'une rançon soit payée.

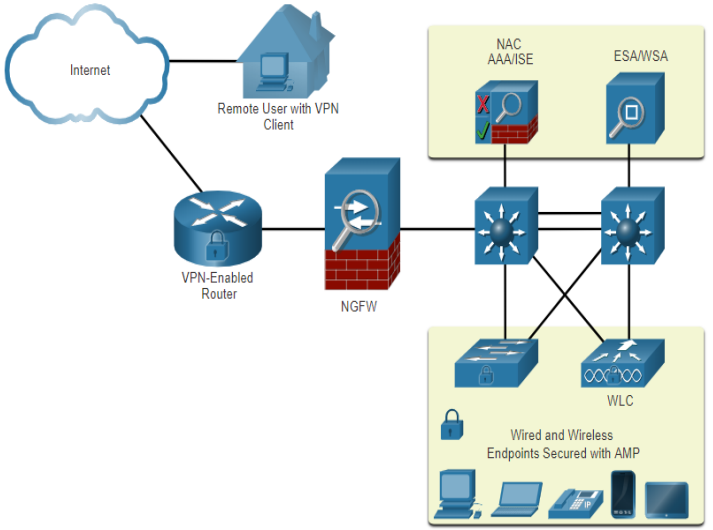
Les attaques de réseau au quotidien

Divers appareils de sécurité du réseau sont nécessaires pour protéger le périmètre du réseau contre tout accès extérieur. Ces appareils peuvent inclure les éléments suivants:

- Un routeur activé VPN fournit une connexion sécurisée aux utilisateurs distants sur un réseau public et sur le réseau d'entreprise. Les services VPN peuvent être intégrés au pare-feu.
- Pare-feu de nouvelle génération (NGFW) - fournit une inspection des paquets avec état, une visibilité et un contrôle des applications, un système de prévention des intrusions de nouvelle génération (NGIPS), une protection avancée contre les logiciels malveillants (AMP) et un filtrage d'URL.
- Contrôle d'accès réseau (NAC) - comprend les services d'authentification, d'autorisation et de comptabilité (AAA). Dans les grandes entreprises, ces services peuvent être intégrés dans une appliance capable de gérer les politiques d'accès sur une grande variété d'utilisateurs et de types d'appareils. Le moteur de services d'identité de Cisco (ISE) est un exemple de périphérique NAC.

Protection des terminaux

- Les terminaux sont des hôtes qui se composent généralement d'ordinateurs portables, d'ordinateurs de bureau, de serveurs et de téléphones IP, ainsi que les appareils appartenant aux employés. Les terminaux sont particulièrement sensibles aux attaques liées aux logiciels malveillants qui proviennent de la messagerie électronique ou de la navigation Web.
- Ces terminaux ont généralement utilisé des fonctionnalités de sécurité traditionnelles basées sur l'hôte, telles que l'antivirus / anti-programme malveillant, les pare-feu basés sur l'hôte et les systèmes de prévention des intrusions (HIPS) basés sur l'hôte.
- les terminaux sont mieux protégés par une combinaison de NAC, d'un logiciel AMP, d'un appliance de sécurité de messagerie (ESA) et d'un appliance de sécurité Web (WSA).



Appliance pour la sécurité de la messagerie électronique Cisco

Cisco ESA est un appareil conçu pour surveiller le protocole SMTP (Simple Mail Transfer Protocol). Cisco ESA est constamment mis à jour par des flux en temps réel de Cisco Talos, qui détecte et corrèle les menaces et les solutions en utilisant un système de surveillance de base de données mondial. Ces données d'intelligence sur les menaces sont tiré par Cisco ESA chaque trois à cinq minutes.

Voici quelques-unes des fonctions de Cisco ESA:

- Bloquer les menaces connues
- Solution contre les logiciels malveillants furtifs qui ont échappé à la détection initiale.
- Annulez les e-mails contenant des liens incorrects
- Bloquer l'accès aux sites nouvellement infectés.
- chiffrez le contenu des e-mails sortants pour éviter la perte de données.

Appliance pour la sécurité de la messagerie électronique Cisco

- L'appliance de sécurité Web Cisco (WSA) est une technologie d'atténuation des menaces Web. Il aide les organisations à relever les défis de la sécurisation et du contrôle du trafic 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. Certaines fonctionnalités et applications, comme le chat, la messagerie, la vidéo et l’audio, peuvent être autorisées, limité avec le temps et de bande passante, ou bloquées, selon les besoins de l’organisation.
- Le WSA peut effectuer la 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.

.2 Le contrôle d'accès

Authentification avec un mot de passe local

De nombreux types d'authentification peuvent être effectués sur des périphériques réseau, et chaque méthode offre différents niveaux de sécurité.

```
R1(config)# line vty 0 4
R1(config-line)# password ci5c0
R1(config-line)# login
```

La méthode d'authentification d'accès à distance la plus simple est de configurer une combinaison d'identifiant et de mot de passe sur la console, les lignes vty et les ports auxiliaires.

```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

SSH est une forme d'accès à distance plus sécurisée:

- Il nécessite un nom d'utilisateur et un mot de passe.
- Le nom d'utilisateur et le mot de passe peuvent être authentifiés locale.

La méthode de la base de données locale a certaines limites :

- Les comptes d'utilisateurs doivent être configurés localement sur chaque périphérique qui n'est pas évolutif.
- La méthode ne fournit aucune méthode d'authentification de secours.

les Composants AAA

AAA signifie Authentification, Autorisation et Comptabilité et fournit le cadre principal pour configurer le contrôle d'accès sur un périphérique réseau.

L'AAA est un moyen de contrôle qui est autorisé à accéder à un réseau (authentifier), ce qu'ils peuvent faire pendant qu'ils sont là (autoriser), et de vérifier les actions effectuées lors de l'accès au réseau (comptabilité).

L'authentification

L'authentification locale et l'authentification par serveur sont deux méthodes courantes de mise en œuvre de l'authentification AAA.

L’authentification AAA locale:

- Est un méthode qui stocke les noms d'utilisateur et les mots de passe localement dans un périphérique réseau (par exemple le routeur Cisco).
- Les utilisateurs s'authentifient contre la base de données locale.
- L'authentification AAA locale est idéale pour les réseaux de petite taille.

L'authentification AAA basée sur le serveur :

- Avec la méthode basée sur le serveur, le routeur accède à un serveur AAA central.
- Le serveur AAA contient les noms d'utilisateur et mot de passe pour tous les utilisateurs.
- Le routeur utilise les protocoles RADIUS (Service utilisateur d'accès à distance par authentification) ou TACACS+ (Contrôleur d'accès aux terminaux Système de contrôle d'accès) pour communiquer avec le serveur AAA.
- Lorsqu'il y a plusieurs routeurs et commutateurs, la méthode AAA basée sur le serveur est plus approprié.

L'autorisation

- L'autorisation AAA est automatique et ne nécessite pas que les utilisateurs effectuent des étapes supplémentaires après l'authentification.
- L'autorisation régit ce que les utilisateurs peuvent et ne peuvent pas faire sur le réseau après leur authentification.
- L'autorisation utilise un ensemble d'attributs qui décrivent l'accès de l'utilisateur au réseau. Ces attributs sont utilisés par le serveur AAA pour déterminer les privilèges et les restrictions pour cet utilisateur.

La comptabilité

La comptabilité AAA collecte et rapporte les données d'utilisation. Ces données peuvent être utilisées à des fins comme l'audit ou la facturation. Les données recueillies peuvent indiquer les heures de début et de fin des connexions, les commandes exécutées, le nombre de paquets et le nombre d'octets.

Une utilisation principale de la comptabilité est de la combiner avec l'authentification AAA.

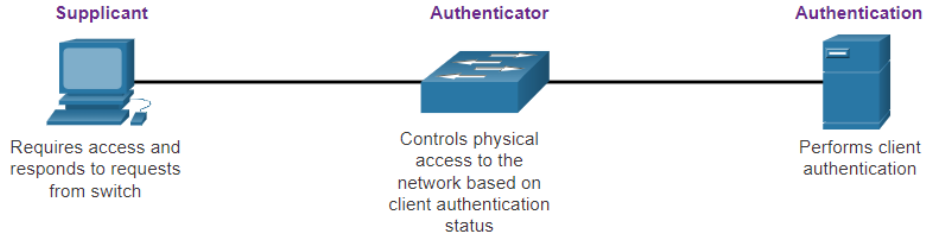
- Le serveur AAA conserve un journal détaillé de ce que l'utilisateur authentifié fait exactement sur le périphérique, comme indiqué sur la figure. Ce journal comprend toutes les commandes EXEC et les commandes de configuration exécutées par l'utilisateur.
- Il contient de nombreux champs de données, à savoir le nom d'utilisateur, la date et l'heure ainsi que les commandes saisies par l'utilisateur. Ces informations sont utiles lors du dépannage des appareils. Il fournit aussi des preuves lorsque des individus commettent des actes malveillants.

Contrôle d'accès
802.1X

La norme IEEE 802.1X est un protocole de contrôle d'accès et d'authentification basé sur les ports. Ce protocole empêche les stations de travail non autorisées de se connecter à un réseau local via des ports de commutation accessibles au public. Avant de mettre à disposition les services offerts par le commutateur ou le LAN, le serveur d'authentification authentifie chaque station de travail connectée à un port de commutation.

Avec une authentification 802.1x basée sur les ports, les périphériques réseau ont des rôles spécifiques.

- **Le client (Demandeur)** - Il s'agit d'un appareil exécutant un logiciel client compatible 802.1X, qui est disponible pour les appareils câblés ou sans fil.
- **Le commutateur (authentificateur)** - Le commutateur peut servir d'intermédiaire entre le client et le serveur d'authentification. Il demande les informations d'identification du client, vérifie ces informations auprès du serveur d'authentification, puis transmet une réponse au client. Un autre périphérique qui pourrait faire office d'authentificateur est un point d'accès sans fil.
- **Le Serveur d'authentification** –Le serveur valide l'identité du client et informe le commutateur ou le point d'accès sans fil que le client est autorisé ou non à accéder au LAN et aux services de commutateur.

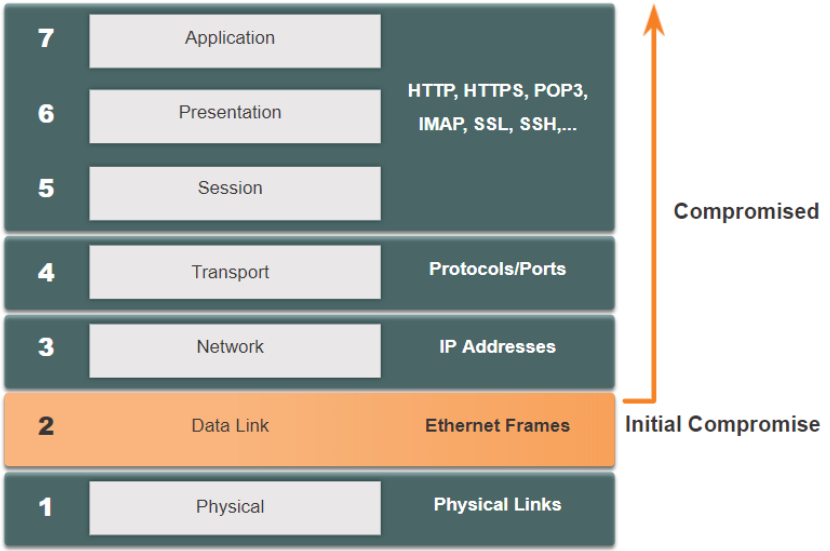


.3 Menaces de sécurité de couche 2

Vulnérabilités de couche 2

Rappelons que le modèle de référence OSI est divisé en sept couches qui fonctionnent indépendamment les unes des autres. La figure montre la fonction de chaque couche et les éléments centraux qui peuvent être exploités.

Les administrateurs du réseau implémentent régulièrement des solutions de sécurité pour protéger les éléments de la couche 3 à la couche 7. Ils utilisent des VPN, des pare-feu et des périphériques IPS pour protéger ces éléments. Cependant, si la couche 2 est compromise, toutes les couches supérieures sont aussi affectées. Par exemple, si un acteur de menace ayant accès au réseau interne a capturé des trames de couche 2, alors toute la sécurité mise en œuvre sur les couches ci-dessus serait inutile. L'acteur de menace pourrait causer de nombreux dommages à l'infrastructure réseau LAN de couche 2.



Les catégories d'attaque de commutateurs

La sécurité n'est aussi solide que le lien le plus faible du système, et la couche 2 est considérée comme ce lien faible. Cela est dû au fait que, les réseaux locaux étaient traditionnellement sous le contrôle administratif d'une seule organisation. Nous faisions intrinsèquement confiance à toutes les personnes et à tous les appareils connectés à notre réseau local. Aujourd'hui, avec le BYOD et des attaques plus sophistiquées, nos réseaux locaux sont devenus plus vulnérables à la pénétration.

Catégorie	Exemples
Les Attaques de table MAC	Il comprend les attaques par inondation de l'adresse MAC.
Attaques de VLAN	Il comprend les attaques par saut et par revérifier VLAN. Il aussi comprend les attaques entre les périphériques sur un VLAN commun.
Attaques DHCP	Il comprend les attaques d'insuffisance DHCP et les attaques d'usurpation DHCP.
Les attaques ARP	Il comprend les attaques d'usurpation ARP et les attaques d'empoisonnement ARP.
Attaques par usurpation d'adresse	Il comprend les attaques d'usurpation d'adresse MAC et d'adresse IP.
Les attaques STP	Il comprend les attaques de manipulation du protocole Spanning Tree.

Les techniques d'atténuation des attaques de commutateur

La solution	Description
Sécurité des ports	Empêche de nombreux types d'attaques, y compris les attaques d'inondation d'adresses MAC et les attaques d'insuffisance DHCP.
Espionnage (snooping) DHCP	Empêche l'insuffisance DHCP et les attaques d'usurpation du DHCP.
Inspection ARP dynamique (DAI)	Empêche l'usurpation d'ARP et les attaques d'empoisonnement d'ARP.
Protection de la source IP (IPSG)	Empêche les attaques d'usurpation d'adresse MAC et IP.

Ces solutions de couche 2 ne seront pas efficaces si les protocoles de gestion ne sont pas sécurisés. Les stratégies suivantes sont recommandées:

- Utilisez toujours des variantes sécurisées de protocoles de gestion telles que SSH, protocole de copie sécurisée (SCP), FTP sécurisé (SFTP) et couche de socket sécurisée / sécurité de la couche de transport (SSL / TLS).
- Considérez d'utiliser un réseau de gestion hors bande pour gérer les périphériques.
- Utilisez un VLAN de gestion dédié où ne réside rien d'autre que le trafic de gestion.
- Utilisez des listes de contrôle d'accès pour filtrer tout accès non indésirable.

.4 Attaque du table d'adresse MAC

Révision du fonctionnement de commutateur

Rappelez-vous cela pour prendre des décisions de transfert, un commutateur LAN de couche 2 construit un tableau basé sur les adresses MAC source dans les trames reçues. Cela s'appelle une table d'adresse MAC. Les tables d'adresses MAC sont stockées en mémoire et sont utilisées pour transmettre plus efficacement les trames.

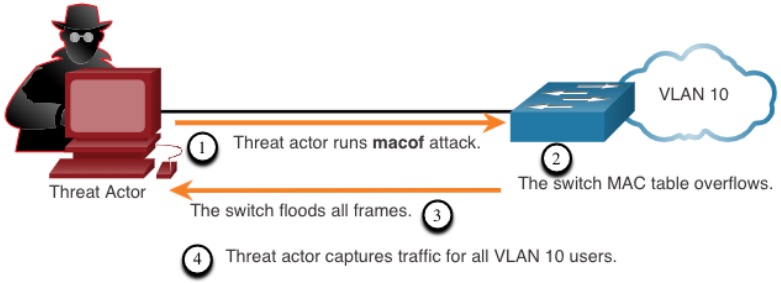
```
S1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
S1#
```

L'inondation (flooding) de table d'adresse MAC

Toutes les tables MAC ont une taille fixe et par conséquent, un commutateur peut manquer de ressources pour stocker les adresses MAC. Les attaques par inondation d'adresses MAC profitent de cette limitation en bombardant le commutateur avec de fausses adresses sources MAC jusqu'à ce que la table d'adresses MAC du commutateur soit pleine.

Lorsque cela se produit, le commutateur traite la trame comme une monodiffusion inconnue et commence à inonder tout le trafic entrant sur tous les ports du même VLAN sans référencer la table MAC. Cette condition permet désormais à un acteur de menace de capturer toutes les trames envoyées d'un hôte à un autre sur le LAN local ou le VLAN local.

Remarque: Le trafic n'est inondé que dans le LAN local ou le VLAN. L'acteur de menace ne peut capturer que le trafic au sein du LAN ou VLAN local auquel il est connecté.



L’atténuation des attaques de table d'adresse MAC

Ce qui rend les outils tels que **macof** si dangereux, c'est qu'un attaquant peut créer une attaque de débordement de table MAC très rapidement. Par exemple, un commutateur Catalyst 6500 peut stocker 132,000 adresses MAC dans sa table d'adresse MAC. Un outil tel que **macof** peut inonder un commutateur avec jusqu'à 8,000 faux trames par seconde ; créant une attaque de débordement de table d'adresse MAC en quelques secondes.

Une autre raison pour laquelle ces outils d'attaque sont dangereux est qu'ils n'affectent pas seulement le commutateur local, ils peuvent aussi affecter les autres commutateurs de couche 2 connectés. Lorsque la table d'adresse MAC d'un commutateur est pleine, il commence à inonder tous les ports, y compris ceux qui sont connectés aux autres commutateurs de couche 2.

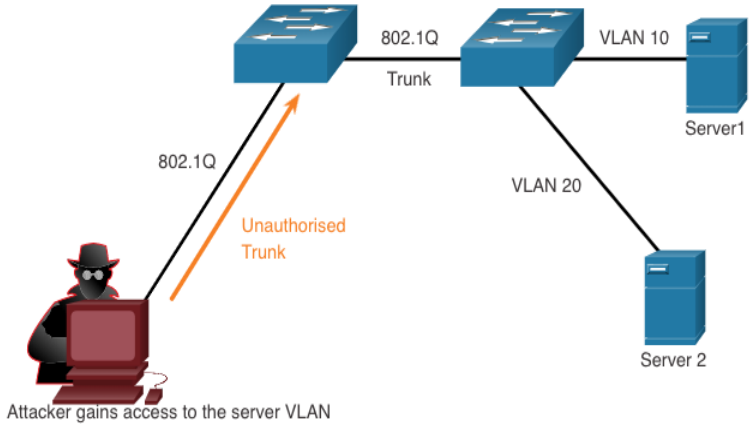
Pour atténuer les attaques de débordement de table d'adresse MAC, les administrateurs réseau doivent implémenter la sécurité des ports. La sécurité des ports ne permettra d'apprendre qu'un nombre spécifié d'adresses MAC sources sur le port. La sécurité des ports est discuté plus en détail dans un autre module.

.5 Les attaques de réseau LAN

Les attaques de saut de VLAN

Une attaque par saut de VLAN permet au trafic d'un VLAN d'être détecté par un autre VLAN sans l'aide d'un routeur. Dans une attaque de base de saut de VLAN, l'acteur de menace configure un hôte pour qu'il agisse comme un commutateur afin de profiter de la fonction de port de trunc automatique activée par défaut sur la plupart des ports de commutateur.

L'acteur de menace configure l'hôte pour usurper la signalisation 802.1Q et la signalisation DTP (Dynamic Trunking Protocol) propriétaire de Cisco pour le trunc avec le commutateur de connexion. En cas de succès, le commutateur établit une liaison de trunc avec l'hôte, comme illustré dans la figure. L'acteur de menace peut accéder tous les VLAN sur le commutateur. L'acteur de menace peut envoyer et recevoir du trafic sur n'importe quel VLAN, sautant efficacement entre les VLAN.



Les Attaques de double étiquetage VLAN

Un acteur de menace est une situation spécifique qui pourrait incorporer une étiquette 802.1Q cachée dans la trame qui a déjà une étiquette 802.1Q. Cette balise permet à la trame d'accéder à un VLAN que l'étiquette 802.1Q d'origine n'a pas spécifié.

- **Étape 1:** L'acteur de menace envoie une trame 802.1Q double étiquetage au commutateur. L'en-tête externe a une étiquette VLAN de l'acteur de menace, qui est identique au VLAN natif du port trunc.
- **Étape 2**: La trame arrive sur le premier commutateur, qui examine la première étiquette 802.1Q de 4 octets Le commutateur voit que la trame est destinée au VLAN natif. Le commutateur transfère le paquet sur tous les ports VLAN natifs après avoir divisé l'étiquette VLAN. La trame n'est pas réétiquetée car elle fait partie du VLAN natif. À ce stade, l'étiquette VLAN interne est toujours intacte et n'a pas été inspectée par le premier commutateur.
- **Étape 3**: La trame arrive au deuxième commutateur qui ne sait pas qu'elle était destinée au VLAN natif. Le trafic VLAN natif n'est pas étiqueté par le commutateur d'envoi selon la spécification 802.1Q. Le deuxième commutateur ne concerne que l'étiquetage 802.1Q interne que l'acteur de menace a insérée et indique que la trame est destinée au VLAN cible. Le deuxième commutateur envoie la trame à la cible ou l'inonde, selon qu'il existe une entrée de table d'adresses MAC existante pour la cible.

Les attaques de double étiquetage VLAN (Cont.)

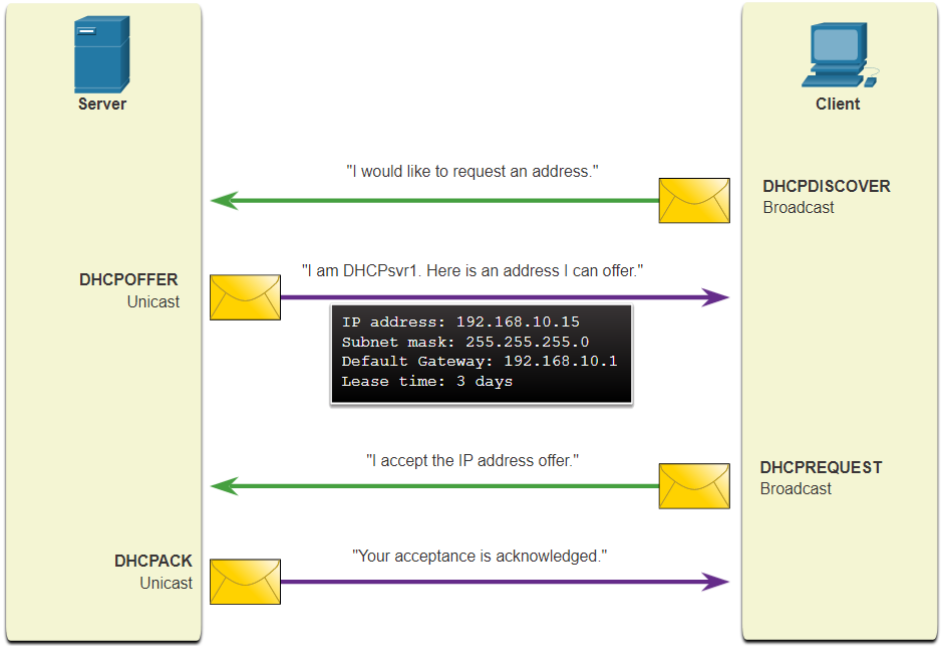
Une attaque de double étiquetage VLAN est unidirectionnelle et ne fonctionne que lorsque l'attaquant est connecté à un port résidant dans le même VLAN que le VLAN natif du port de trunc. L'idée est que le double étiquetage permet à l'attaquant d'envoyer des données à des hôtes ou des serveurs sur un VLAN qui autrement seraient bloqués par un certain type de configuration de contrôle d'accès. Probablement, le trafic de retour sera aussi autorisé, ce qui donnera à l'attaquant la possibilité de communiquer avec des périphériques sur le VLAN normalement bloqué.

L'attaque d'atténuation VLAN - Les attaques de saut de VLAN et de double étiquetage VLAN peuvent être évitées en mettant en œuvre les directives de sécurité de trunc suivantes, comme indiqué dans un module précédent :

- Désactivez trunking sur tous les ports d'accès.
- Désactivez trunking automatique sur les liaisons de trunc afin que les truncs doivent être activées manuellement.
- Assurez-vous que le VLAN natif n'est utilisé que pour les liaisons de trunc.

Les messages DHCP

Les serveurs DHCP fournissent aux clients les informations de configuration IP, notamment l'adresse IP, le masque de sous-réseau, la passerelle par défaut, les serveurs DNS, etc., et ce de manière dynamique. Une révision de la séquence de l'échange de messages DHCP entre le client et le serveur est illustré dans la figure.



les attaques DHCP

Deux types d'attaques DHCP sont l'insuffisance DHCP et l'usurpation DHCP. Les deux attaques sont atténuées en mettant en œuvre l'espionnage DHCP.

- **L'attaque par insuffisance DHCP –** L'objectif d'une attaque par insuffisance DHCP est de créer un déni de service (DoS) pour connecter les clients. Les attaques par épuisement des ressources DHCP reposent sur un outil d'attaque, Gobbler, par exemple. Gobbler a la possibilité d'examiner l'intégralité des adresses IP louables et essaie de toutes les louer. Plus précisément, il crée des messages de découverte DHCP avec de fausses adresses MAC.
- **Attaque d'usurpation DHCP –** Cela se produit lorsqu'un serveur DHCP non autorisé (rogue) se connecte au réseau et fournit des paramètres de configuration IP incorrects aux clients légitimes. Un serveur non autorisé peut fournir des informations différentes trompeuses, y compris les suivantes :
  - **Passerelle par défaut incorrecte** - Le serveur non autorisé fournit une passerelle non valide ou l'adresse IP de son hôte pour créer une attaque d'homme au milieu. Cette approche peut passer totalement inaperçue, car l'intrus intercepte le flux de données via le réseau.
  - **Serveur DNS incorrect** - Le serveur non autorisé fournit une adresse de serveur DNS incorrecte pointant l'utilisateur vers un site Web néfaste.
  - **Adresse IP incorrecte** - Le serveur non autorisé fournit une adresse IP invalide créant efficacement une attaque DoS sur le client DHCP.

les attaques ARP

- Les hôtes diffusent des requêtes ARP pour déterminer l'adresse MAC d'un hôte avec une adresse IP de destination. 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.
- Un client peut envoyer une réponse ARP non sollicitée appelé «ARP gratuite». les autres hôtes du sous-réseau stockent l'adresse MAC et l'adresse IP contenue par l'ARP gratuite dans leurs tables ARP.
- Un attaquant peut envoyer un message ARP gratuit contenant une adresse MAC usurpée à un commutateur, et le commutateur mettrait à jour sa table MAC en conséquence. Dans une attaque typique, un acteur de menace peut envoyer des réponses ARP non sollicitées à d'autres hôtes du sous-réseau avec l'adresse MAC de l'acteur de menace et l'adresse IP de la passerelle par défaut, configurant efficacement une attaque d'homme au milieu.
- Il existe de nombreux outils disponibles sur Internet pour créer des attaques ARP homme-au-milieu.
- IPv6 utilise le protocole de découverte de voisin ICMPv6 pour la résolution d'adresse de couche 2. IPv6 comprend des stratégies pour atténuer l'usurpation de publicité de voisin, de la même manière que IPv6 empêche une réponse ARP usurpée.
- L'usurpation ARP et l'empoisonnement ARP sont atténués par la mise en œuvre de l'inspection ARP dynamique (DAI).

Les Attaques par usurpation d'adresse

- L'usurpation d'adresse IP est lorsqu'un acteur de menace détourne une adresse IP valide d'un autre périphérique sur le sous-réseau ou utilise une adresse IP aléatoire. L'usurpation d'adresse IP est difficile à atténuer, en particulier lorsqu'elle est utilisée à l'intérieur d'un sous-réseau auquel appartient l'IP.
- Les attaques d'usurpation d'adresse MAC se produisent lorsque les acteurs de menace modifient l'adresse MAC de leur hôte pour correspondre à une autre adresse MAC connue d'un hôte cible. Le commutateur remplace l'entrée de table MAC actuelle et attribue l'adresse MAC au nouveau port. Il transfère ensuite par inadvertance des trames destinées à l'hôte cible à l'hôte attaquant.
- Lorsque l'hôte cible envoie du trafic, le commutateur vérifiera l'erreur, en réalignant l'adresse MAC sur le port d'origine. Pour empêcher le commutateur de ramener l'affectation de port à son état correct, l'acteur de menace peut créer un programme ou un script qui enverra constamment des trames au commutateur afin que le commutateur conserve les informations incorrectes ou usurpées.
- Il n'y a pas de mécanisme de sécurité au couche 2 qui permet à un commutateur de vérifier la source des adresses MAC, ce qui le rend très vulnérable à l'usurpation.
- L'usurpation d'adresse IP et MAC peut être atténuée en implémentant IPSG.

les attaques STP

- Les attaquants du réseau peuvent manipuler le protocole STP (Spanning Tree Protocol) pour mener une attaque en usurpant le pont racine et en modifiant la topologie d'un réseau. Les attaquants peuvent alors capturer tout le trafic pour le domaine commuté immédiat.
- Pour mener une attaque de manipulation STP, l'hôte attaquant diffuse des unités de données de protocole de pont STP (BPDU) contenant de configuration et de topologie obligera à réévaluer le spanning-tree. Les BPDU envoyés par l'hôte attaquant annoncent une priorité de pont inférieure pour tenter d'être élu pont racine.
- Cette attaque STP est atténuée par l'implémentation de BPDU Guard sur tous les ports d'accès. BPDU Guard est discuté plus en détail plus tard dans le cours.

Reconnaissance CDP

Le protocole CDP (Cisco Discovery Protocol) est un protocole propriétaire de découverte de liaison de couche 2. Il est activé par défaut sur tous les périphériques Cisco. Les administrateurs réseau utilisent également le protocole CDP pour configurer et dépanner les périphériques réseau. les informations CDP sont envoyées sur les ports activés CDP dans des diffusions périodiques, non chiffrés et non authentifiées. Les données CDP incluent l'adresse IP du périphérique, la version logicielle IOS, la plate-forme, les fonctionnalités et le VLAN natif. Le périphérique qui reçoit le message CDP met à jour sa base de données CDP.

Pour réduire le risque d'attaque de CDP, limitez l'utilisation de ce protocole sur les périphériques et les ports. Par exemple, désactivez CDP sur les ports périphériques qui se connectent aux périphériques non fiables.

- Pour désactiver CDP globalement sur un périphérique, utilisez la commande du mode de configuration globale **no cd run** . Pour activer CDP globalement, utilisez la commande de configuration globale **cdp run**
- Pour désactiver CDP sur un port, utilisez la commande de configuration d'interface **no cdp enable** Pour activer CDP sur un port, utilisez la commande de configuration d'interface **cdp enable**

Remarque: Le protocole LLDP (Link Layer Discovery Protocol) est aussi vulnérable aux attaques de reconnaissance. Configurez **no lldp run** pour désactiver LLDP globalement. Pour désactiver LLDP sur l'interface, configurez **no lldp transmite** et **no lldp receive**.


CISCO