# Module 16 : Fondamentaux de la sécurité des réseaux

Introduction aux Réseaux v7.0
(ITN)

# Objectifs de ce module

**Titre du Module:** Fondamentaux de la sécurité des réseaux

**Objectif du module**: Configurer les commutateurs et les routeurs avec des fonctions de durcissement des dispositifs pour renforcer la sécurité.

| Titre du rubrique | Objectif du rubrique |
|---|---|
| **Menaces pour la sécurité et vulnérabilités** | Expliquer pourquoi des mesures de sécurité de base sont nécessaires pour les périphériques réseau. |
| **Attaques du réseau** | Identifier les vulnérabilités. |
| **Maîtrise des attaques du réseau** | Identifier les techniques générales de maîtrise des menaces. |
| **Sécurité des périphériques** | Configurer les périphériques réseau en utilisant des fonctionnalités de sécurisation renforcées pour maîtriser les menaces pour la sécurité. |

# 16.1 Menaces et vulnérabilités de la sécurité

# Types de menaces

Les attaques contre un réseau peuvent être dévastatrices et peuvent entraîner une perte de temps et d'argent en raison des dommages ou du vol d'informations ou de biens importants. Les intrus peuvent accéder à un réseau en exploitant les failles logicielles, en lançant des attaques matérielles ou en devinant l'identifiant et le mot de passe d'un utilisateur. Les intrus qui obtiennent l'accès en modifiant les logiciels ou en exploitant les vulnérabilités des logiciels sont appelés acteurs de menace.

Une fois que l'acteur de menace a accédé au réseau, quatre types de menaces peuvent apparaître :

- Vol d'informations
- Perte et manipulation de données
- Usurpation d'identité
- Interruption de service

# Types de vulnérabilités

La vulnérabilité est le degré de faiblesse inhérent à tout réseau ou périphérique. Un certain degré de vulnérabilité est inhérent aux routeurs, aux commutateurs, aux ordinateurs de bureau, aux serveurs et même aux dispositifs de sécurité. En général, les périphériques réseau attaqués sont des terminaux comme les serveurs et les ordinateurs de bureau.

Vulnérabilités ou faiblesses interviennent principalement à trois niveaux :

- Les vulnérabilités technologiques peuvent inclure des faiblesses du protocole TCP/IP, des faiblesses du système d'exploitation et des faiblesses de l'équipement réseau.
- Les vulnérabilités de configuration peuvent inclure des comptes d'utilisateur non sécurisés, des comptes système avec des mots de passe faciles à deviner, des services internet mal configurés, des paramètres par défaut non sécurisés et un équipement réseau mal configuré.
- Les vulnérabilités de la politique de sécurité peuvent inclure l'absence d'une politique de sécurité écrite, la politique, le manque de continuité de l'authentification, les contrôles d'accès logiques non appliqués, l'installation et les modifications de logiciels et de matériel ne respectant pas la politique, et un plan de reprise après sinistre inexistant.

Ces trois sources de vulnérabilité peuvent laisser un réseau ou un dispositif ouvert à diverses attaques, y compris les attaques par code malveillant et les attaques de réseau.

# Sécurité physique

Si les ressources du réseau peuvent être physiquement compromises, un acteur de menace peut refuser l'utilisation des ressources du réseau. Les quatre catégories de menaces physiques sont les suivantes :

- **Menaces matérielles -** Cela comprend les dommages physiques aux serveurs, routeurs, commutateurs, installations de câblage et postes de travail.
- **Menaces environnementales -** Cela comprend les extrêmes de température (trop chaud ou trop froid) ou les extrêmes d'humidité (trop humide ou trop sec).
- **Menaces électriques -** Cela comprend les pointes de tension, tension d'alimentation insuffisante (chutes de tension), alimentation non contrôlée (bruit) et coupure totale de l'alimentation.
- **Menaces de maintenance -** Cela comprend la mauvaise manipulation des principaux composants électriques (décharge électrostatique), le manque de pièces de rechange essentielles, le mauvais câblage et le mauvais étiquetage.

Un bon plan de sécurité physique doit être élaboré et mis en œuvre pour régler ces problèmes.

# 16.2 Attaques réseau

# Types de logiciels malveillants

Malware est l'abréviation de logiciel malveillant. 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. Voici les types de logiciels malveillants :

- **Virus -** Un virus informatique est un type de logiciel malveillant qui se propage en insérant une copie de lui-même dans un autre programme et en en faisant partie. Il se transmet ainsi d'un ordinateur à un autre.
- **Vers -** Les vers informatiques sont similaires aux virus en ce sens qu'ils reproduisent des copies fonctionnelles d'eux-mêmes et peuvent causer le même type de dommages. Contrairement aux virus, qui nécessitent la diffusion d'un fichier hôte infecté, les vers sont des logiciels autonomes et ne requièrent pas de programme d'accueil ou d'intervention humaine pour se propager.
- **Chevaux de Troie -** Il s'agit d'un logiciel nuisible qui semble légitime. Contrairement aux virus et aux vers, les chevaux de Troie ne se reproduisent pas en infectant d'autres fichiers. Ils se répliquent. Les chevaux de Troie doivent se propager par le biais d'une interaction avec l'utilisateur, par exemple en ouvrant une pièce jointe à un courriel ou en téléchargeant et en exécutant un fichier sur l'internet.

# Attaques de reconnaissance

En plus des attaques de programmes malveillants, les réseaux peuvent également être la proie de différentes attaques de réseau. Les attaques de réseau peuvent être classées en trois catégories principales :

- **Attaques de reconnaissance** - Découverte et cartographie des systèmes, services ou vulnérabilités.
- **Attaques d'accès** - Manipulation non autorisée de données, d'accès au système ou de privilèges d'utilisateur.
- **Déni de service** - Désactivation ou corruption de réseaux, de systèmes ou de services.

Pour les attaques de reconnaissance, les acteurs externes de menace peuvent utiliser des outils Internet, tels que les utilitaires **nslookup** et **whois** , pour déterminer facilement l'espace d'adresse IP attribué à une société ou une entité donnée. Une fois l'espace d'adresses IP déterminé, un acteur de menace peut alors effectuer un ping sur les adresses IP accessibles au public afin d'identifier les adresses qui sont actives.

# Attaques par accèss

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.

Il existe quatre types d'attaques par accès :

- **Attaques par mot de passe -** Implémentation en utilisant la force brute, le cheval de Troie et les renifleurs de paquets
- **Exploitation de la confiance -** Un acteur de menace utilise des privilèges non autorisés pour accéder à un système, ce qui peut compromettre la cible.
- **Redirection de port**: - Un acteur de menace utilise un système compromis comme base pour des attaques contre d'autres cibles. Par exemple, un acteur de menace utilisant SSH (port 22) pour se connecter à un hôte A compromis. L'hôte B fait confiance à l'hôte A et, par conséquent, l'acteur de la menace peut utiliser Telnet (port 23) pour y accéder.
- **Homme-au-milieu -** L'acteur de menace est positionné entre deux entités légitimes afin de lire ou de modifier les données qui passent entre les deux parties.

# Attaques par déni de service

Les attaques par déni de service sont les plus médiatisées, mais constituent également l'une des formes d'attaque les plus difficiles à éliminer. Toutefois, la facilité de mise en œuvre des attaques DoS et leurs dégâts potentiellement importants retiennent toute l'attention des administrateurs de la sécurité.

- Les attaques DoS peuvent prendre de nombreuses formes. Elles empêchent l'utilisation d'un service par les personnes autorisées en épuisant les ressources du système. Afin d'aider à prévenir les attaques DoS, il est important d'installer les dernières mises à jour de sécurité des systèmes d'exploitation et des applications.
- 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 effectuer, même par des cyberpirates peu qualifiés.
- Un DDoS est similaire à une attaque DoS, mais il provient de sources multiples et coordonnées. Par exemple, un acteur de menace construit un réseau d'hôtes infectés, appelés zombies. Un réseau de zombies est appelé un botnet. L'acteur de menace utilise un programme de commande et de contrôle (CNC) pour demander au botnet de zombies de mener une attaque DDoS.

# Travail pratique - Recherche des Menaces de la sécurité des réseaux

Au cours de ces travaux pratiques, vous aborderez les points suivants :

- Partie 1 : Découvrir le site web SANS
- Partie 2 : Identifier les menaces pour la sécurité du réseau les plus récentes
- Partie 3 : Décrire en détail une menace spécifique pour la sécurité du réseau

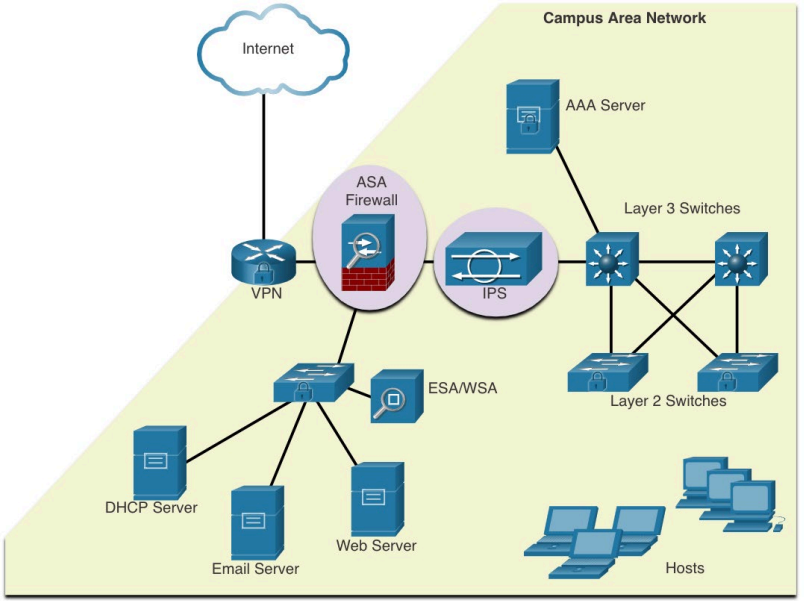
# 16.3 Atténuation des attaques de réseaux

# L'approche de la défense en profondeur

Pour atténuer les attaques réseau, vous devez d'abord sécuriser les périphériques, y compris les routeurs, les commutateurs, les serveurs et les hôtes. La plupart des organisations utilisent une approche de défense en profondeur (également connue sous le nom d'approche par couches) de la sécurité. Pour cela, divers appareils réseau et services doivent fonctionner en tandem.

Plusieurs dispositifs et services de sécurité sont mis en œuvre pour protéger les utilisateurs et les atouts d'une organisation contre les menaces TCP / IP:

- VPN
- Pare-feu ASA
- IPS
- ESA/WSA
- Serveur AAA



# Conserver les sauvegardes

La sauvegarde des données est l'un des moyens de protection les plus efficaces contre la perte de données. La sauvegarde des données doit donc être effectuée régulièrement. Elle doit faire partie de la politique de sécurité. Les sauvegardes sont généralement stockées en dehors des installations, afin de protéger le support de sauvegarde en cas de sinistre dans le bâtiment principal.

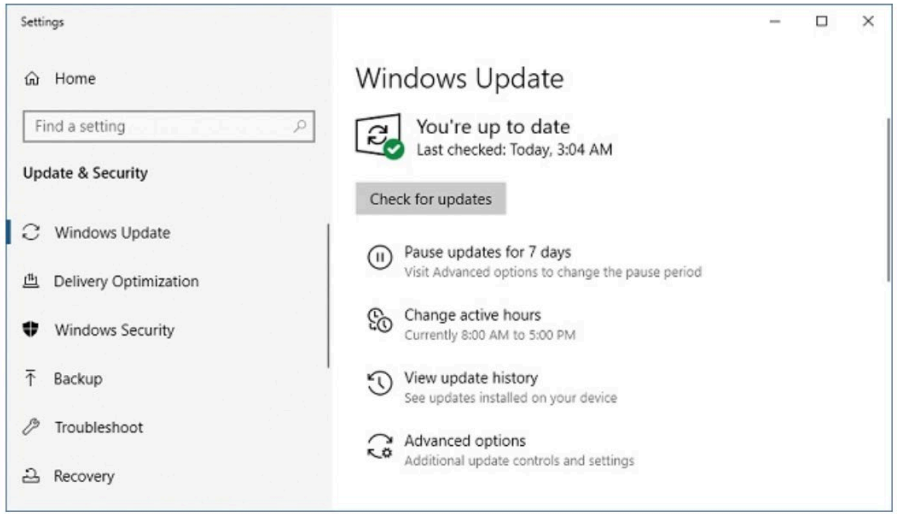
Le tableau présente les considérations relatives à la sauvegarde et la restauration des données.

| Intérêt | Description |
|---|---|
| Fréquence | •Sauvegardez régulièrement les données conformément à la politique de sécurité.<br>•Les sauvegardes complètes peuvent prendre beaucoup de temps, c'est pourquoi il faut effectuer des sauvegardes mensuelles ou hebdomadaires avec des sauvegardes partielles fréquentes des fichiers modifiés. |
| Stockage | •Validez toujours les sauvegardes afin de garantir l'intégrité des données et de valider les procédures de restauration des fichiers. |
| Sécurité | •Les sauvegardes doivent être stockées sur un site dédié et agréé. Le transfert des sauvegardes doit être effectué une fois par jour, par semaine ou par mois, conformément à la stratégie de sécurité. |
| Validation | •Les sauvegardes doivent être protégées à l'aide de mots de passe forts. Le mot de passe est nécessaire pour restaurer les données. |

# Mise à niveau, mise à jour et correctif

Au fur et à mesure que de nouveaux programmes malveillants apparaissent, les entreprises doivent acquérir la version la plus récente de leur logiciel antivirus.

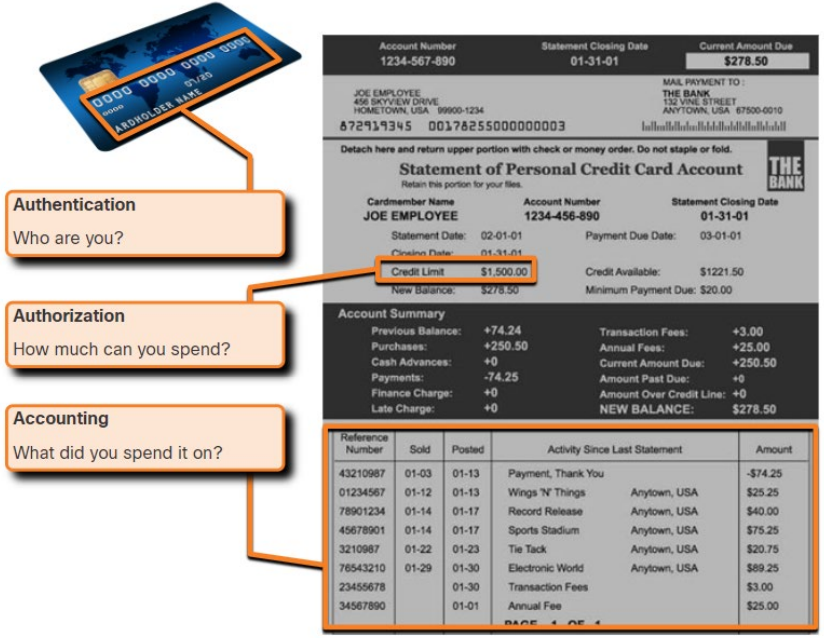
- La meilleure façon de limiter les risques d'attaque de ver est de télécharger les mises à jour de sécurité du fournisseur du système d'exploitation et d'appliquer des correctifs sur tous les systèmes vulnérables.
- Une solution pour la gestion des correctifs de sécurité critiques consiste à s'assurer que tous les systèmes finaux téléchargent automatiquement les mises à jour.



# Authentification, autorisation et comptabilité

Les services de sécurité des réseaux d'authentification, d'autorisation et de comptabilité (AAA, ou "triple A") fournissent le cadre principal pour mettre en place un contrôle d'accès sur les dispositifs de réseau.

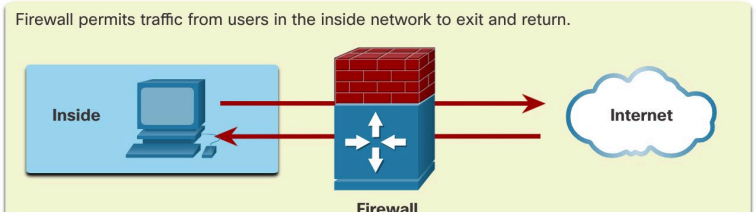
- L'AAA est un moyen de contrôler qui est autorisé à accéder à un réseau (authentification), quelles sont les actions qu'il effectue lors de l'accès au réseau (autorisation), et d'enregistrer ce qui a été fait pendant son séjour (comptabilité).
- Le concept des services d'authentification, d'autorisation et de gestion des comptes est similaire à l'utilisation d'une carte de crédit. La carte bancaire identifie qui est autorisé à l'utiliser, combien cet utilisateur peut dépenser et les achats qu'il a effectués.

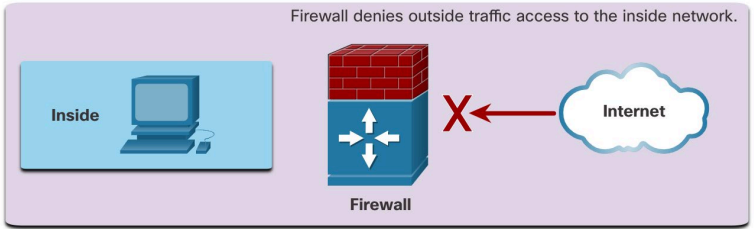


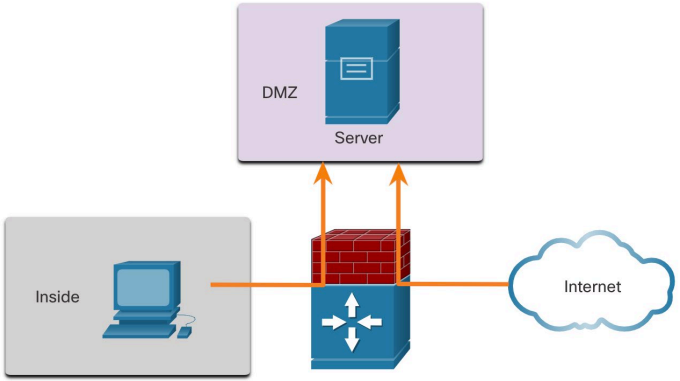
# Pare-feu

Un pare-feu se trouve entre deux réseaux, ou plus, et contrôle le trafic entre eux tout en contribuant à interdire les accès non autorisés.

Un pare-feu permet aux utilisateurs externes de contrôler l'accès à des services spécifiques. Par exemple, les serveurs accessibles aux utilisateurs extérieurs sont généralement situés sur un réseau spécial appelé zone démilitarisée (DMZ). La DMZ permet à un administrateur de réseau d'appliquer des politiques spécifiques pour les hôtes connectés à ce réseau.



# Types de Pare-feu

Les produits pare-feu se présentent sous différentes formes. Ces produits utilisent différentes techniques pour déterminer ce qui sera autorisé ou non à accéder à un réseau. On trouve notamment les produits suivants :

- **Filtrage des paquets** - Empêche ou autorise l'accès sur la base d'adresses IP ou MAC
- **Filtrage des applications** - Empêche ou autorise l'accès à des types d'applications spécifiques en fonction des numéros de port
- **Filtrage des URL** - Empêche ou permet l'accès à des sites web basés sur des URL ou des mots clés spécifiques
- **Inspection minutieuse des paquets (SPI)** - Les paquets entrants doivent être des réponses légitimes aux demandes des hôtes internes. Les paquets non sollicités sont bloqués, sauf s'ils sont expressément autorisés. Le SPI peut également inclure la capacité de reconnaître et de filtrer des types d'attaques spécifiques, comme le déni de service (DoS).

# Sécurité des points d'extrémité

Un point de terminaison, ou hôte, est un système informatique ou un périphérique qui tient lieu de client réseau. Les terminaux les plus courants sont les ordinateurs portables, les ordinateurs de bureau, les serveurs, les smartphones et les tablettes.

La sécurisation des points de terminaison est l'une des tâches les plus difficiles pour un administrateur réseau, car elle implique de prendre en compte le facteur humain. L'entreprise doit mettre en place des stratégies bien documentées et les employés doivent en être informés.

Ils doivent également être formés sur l'utilisation appropriée du réseau. Les stratégies incluent souvent l'utilisation de logiciels antivirus et la prévention des intrusions sur les hôtes. Des solutions plus complètes de sécurisation des terminaux reposent sur le contrôle de l'accès au réseau.

# 16.4 – Sécurité de périphérique

# Cisco AutoSecure

Lorsqu'un nouveau système d'exploitation est installé sur un périphérique, les paramètres de sécurité sont définis à l'aide des valeurs par défaut. Dans la plupart des cas, le niveau de sécurité correspondant n'est pas suffisant. Pour les routeurs Cisco, la fonction AutoSecure de Cisco peut être utilisée pour aider à sécuriser le système.

Voici également quelques étapes simples qu'il convient d'effectuer sur la plupart des systèmes d'exploitation :

- Changement immédiat des noms d'utilisateur et des mots de passe par défaut.
- Accès aux ressources du système limité strictement aux personnes autorisées à utiliser ces ressources.
- Désactivation des services et applications qui ne sont pas nécessaires et désinstallation dans la mesure du possible.
- Souvent, les périphériques expédiés par les fabricants ont été entreposés pendant un certain temps et ne disposent pas des correctifs les plus récents. Il est important de mettre à jour les logiciels et d'installer les correctifs de sécurité avant toute mise en œuvre.

# Mots de passe

Pour protéger les périphériques réseau, il est important d'utiliser des mots de passe forts. Voici quelques recommandations classiques à suivre :

- Utilisez un mot de passe d'une longueur d'au moins huit caractères, de préférence 10 caractères ou plus.
- Choisissez des mots de passe complexes. Utilisez une combinaison de lettres majuscules et minuscules, de chiffres, de symboles et d'espaces si elles sont autorisées.
- Évitez de répéter un même mot, d'utiliser des mots communs du dictionnaire, des lettres ou des chiffres consécutifs, les noms d'utilisateur, les noms des membres de votre famille ou de vos animaux domestiques, des informations biographiques telles que la date de naissance, les numéros d'identification, les noms de vos ascendants ou toute autre information facilement identifiable.
- Faites volontairement des fautes d'orthographe. Par exemple, Smith = Smyth = 5mYth ou Sécurité = 5ecur1te.
- Modifiez régulièrement votre mot de passe. Si un mot de passe est compromis sans le savoir, la possibilité pour l'acteur de menace d'utiliser le mot de passe est limitée.
- Ne notez pas les mots de passe sur des bouts de papier placés en évidence sur votre bureau ou sur votre écran.

Sur les routeurs Cisco, les espaces en début de mot de passe sont ignorés, mais ceux situés après le premier caractère sont pris en compte. Par conséquent, vous pouvez utiliser la barre d'espace pour créer un mot de passe fort composé d'une expression de plusieurs mots. On parle dans ce cas de phrase secrète. Une phrase de passe est souvent plus facile à retenir qu'un simple mot de passe. Elle est également plus longue et plus difficile à deviner.

# Sécurité des mots de passe supplémentaires

Plusieurs mesures peuvent être prises pour garantir que les mots de passe restent secrets sur un routeur et un commutateur Cisco, y compris ceux-ci :

- Cryptez tous les mots de passe en texte clair avec la commande **service password-encryption**
- Définissez une longueur minimale de mot de passe acceptable avec la commande **security password min-length**
- Dissuader les attaques par force brute de deviner le mot de passe avec la commande **login block-for # attempts # within #**
- Désactivez un accès en mode EXEC privilégié inactif après une durée spécifiée à l'aide de la commande **exec-timeout** .

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
Router#
```

# Activation de SSH

Il est possible de configurer un dispositif Cisco pour supporter SSH en suivant les étapes suivantes :

1. **Configurer un nom d'hôte unique pour l'appareil**. Un appareil doit avoir un nom d'hôte unique autre que celui par défaut.
2. **Configurer le nom de domaine IP**. Configurez le nom de domaine IP du réseau en utilisant la commande **ip-domain name**. **du mode de configuration globale.**
3. **Générer une clé pour chiffrer le trafic SSH**. SSH crypte le trafic entre la source et la destination. Cependant, pour ce faire, une clé d'authentification unique doit être générée à l'aide de la commande de configuration globale **crypto key generate rsageneral-keys modulus** *bits*. Le module de *bits* détermine la taille de la clé et peut être configuré de 360 bits à 2048 bits. Plus la valeur du bit est grande, plus la clé est sécurisée. Cependant, les valeurs de bits plus importantes prennent également plus de temps pour chiffrer et déchiffrer les informations. Il est recommandé d'utiliser un module d'au moins 1 024 bits.
4. **Vérifiez ou créez une entrée de base de données locale**. Créez une entrée de nom d'utilisateur dans la base de données locale à l'aide de la commande de configuration globale **username** .
5. **S'authentifier par rapport à la base de données locale**. Utilisez la commande **login local** line configuration pour authentifier la ligne vty par rapport à la base de données locale.
6. **Activer des sessions SSH vty entrantes**. Par défaut, aucune session d'entrée n'est autorisée sur les lignes vty. Vous pouvez spécifier plusieurs protocoles d'entrée, y compris Telnet et SSH, à l'aide de la commande **transport input [ssh | telnet]** .

# Désactiver les services inutilisés

Les routeurs et commutateurs Cisco démarrent avec une liste de services actifs qui peuvent ou non être requis dans votre réseau. Désactivez tous les services inutilisés pour préserver les ressources système, telles que les cycles CPU et la RAM, et empêcher les acteurs de menaces d'exploiter ces services.

- Le type de services activés par défaut varie en fonction de la version d'IOS. Par exemple, IOS-XE n'a généralement que les ports HTTPS et DHCP ouverts. Vous pouvez vérifier cela avec la commande **show ip ports all** .
- Les versions IOS antérieures à IOS-XE utilisent la commande **show control-plane host open-ports** .

# Packet Tracer – Configuration de mots de passe sécurisés et de SSH

Dans ce Packet Tracer, vous allez configurer les mots de passe et SSH:

- L'administrateur réseau vous a demandé de préparer RTA et SW1 pour le déploiement. Avant de le connecter au réseau, il faut mettre en place des mesures de sécurité.

# Travaux pratiques- Configurer les périphériques réseau avec SSH

Au cours de ces travaux pratiques, vous aborderez les points suivants :

- Partie 1 : Configurer les paramètres de base des périphériques
- Partie 2 : Configurer le routeur pour l'accès SSH
- Partie 3 : Configurer le commutateur pour l'accès SSH
- Partie 4 : SSH à partir de l'interface en ligne de commande du commutateur

# 16.5 Module pratique et questionnaire

# Travaux pratiques - Sécurisation des périphériques réseau

Dans cette activité, vous configurerez un routeur et un commutateur selon la liste d'exigences.

# Travaux pratiques - Sécurisation des périphériques réseau

Au cours de ces travaux pratiques, vous aborderez les points suivants :

- Configurer les paramètres de base des appareils
- Configurer les mesures de sécurité de base sur le routeur
- Configurer les mesures de sécurité de base sur le commutateur

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

- Si l'acteur de menace accède au réseau, quatre types de menaces sont possibles : le vol d'informations, l'usurpation d'identité, la perte ou la manipulation de données et l'interruption de service.
- Trois vulnérabilités principales relatives à la technologie, à la configuration et à la politique de sécurité
- Les quatre catégories de menaces physiques sont : le matériel, l'environnement, l'électricité et la maintenance.
- Malware est l'abréviation de logiciel malveillant. 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 virus, les vers et les chevaux de Troie sont des types de logiciels malveillants.
- Les attaques de réseau peuvent être classées en trois grandes catégories : reconnaissance, accès et déni de service.
- Pour atténuer les attaques réseau, vous devez d'abord sécuriser les périphériques, y compris les routeurs, les commutateurs, les serveurs et les hôtes. La plupart des organisations utilisent une approche défensive en matière de sécurité. Cela nécessite une combinaison de périphériques réseau et de services fonctionnant ensemble.
- Plusieurs périphériques et services de sécurité sont mis en œuvre pour protéger les utilisateurs et les ressources d'une organisation contre les menaces TCP/IP : VPN, pare-feu ASA, IPS, ESA/WSA et serveur AAA.

# Qu'est-ce que j'ai appris dans ce module? (Suite)

- Les périphériques d'infrastructure doivent avoir des sauvegardes de fichiers de configuration et d'images IOS sur un serveur FTP ou similaire. Si l'ordinateur ou un matériel de routeur échoue, les données ou la configuration peuvent être restaurées à l'aide de la copie de sauvegarde.
- La meilleure façon de limiter les risques d'attaque de ver est de télécharger les mises à jour de sécurité du fournisseur du système d'exploitation et d'appliquer des correctifs sur tous les systèmes vulnérables. Pour gérer les correctifs de sécurité critiques, assurez-vous que tous les systèmes finaux téléchargent automatiquement les mises à jour.
- Ces services permettent de contrôler les utilisateurs autorisés à accéder à un réseau (authentification), ce que ces derniers peuvent faire lorsqu'ils sont connectés (autorisation) et les actions qu'ils exécutent lors de l'accès au réseau (gestion des comptes).
- Un pare-feu se trouve entre deux réseaux, ou plus, et contrôle le trafic entre eux tout en contribuant à interdire les accès non autorisés.
- La sécurisation des terminaux est essentielle à la sécurité du réseau. Une entreprise doit avoir mis en place des politiques bien documentées, qui peuvent inclure l'utilisation d'un logiciel antivirus et la prévention des intrusions sur l'hôte. Des solutions plus complètes de sécurisation des terminaux reposent sur le contrôle de l'accès au réseau.

# Qu'est-ce que j'ai appris dans ce module? (Suite)

- Pour les routeurs Cisco, la fonction AutoSecure de Cisco peut être utilisée pour aider à sécuriser le système. Pour la plupart des systèmes d'exploitation, les noms d'utilisateur et mots de passe par défaut doivent être modifiés immédiatement, l'accès aux ressources système devrait être limité aux personnes autorisées à utiliser ces ressources, et tous les services et applications inutiles devraient être désactivés et désinstallés si possible.
- Pour protéger les périphériques réseau, il est important d'utiliser des mots de passe forts. Une phrase de passe est souvent plus facile à retenir qu'un simple mot de passe. Elle est également plus longue et plus difficile à deviner.
- Pour les routeurs et les commutateurs, chiffrez tous les mots de passe en texte clair, définissez une longueur de mot de passe minimale acceptable, dissuadez les attaques de deviner par mot de passe par force brute et désactivez un accès en mode EXEC privilégié inactif après une durée spécifiée.
- Configurez les périphériques appropriés pour prendre en charge SSH et désactivez les services inutilisés.


CISCO