Blocs de cours

# CFA-23-24 -MD-01 - Initiation aux réseaux informatiques



## 16.1.1 - Menaces et failles de sécurité

### Types de menaces

les filaires ou sans fil réseaux informatiques jouent un rôle essentiel dans la vie quotidienne. Les particuliers comme les entreprises se servent constamment de leurs ordinateurs et de leurs réseaux. Une intrusion par une personne non autorisée peut causer des pannes de réseau et des pertes de productivité coûteuses. 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.


### Types de vulnérabilité

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

Trois vulnérabilités principales relatives à la technologie, à la configuration et à la politique de sécurité. Ces trois sources de vulnérabilité peuvent laisser un réseau ou un périphérique ouvert à diverses attaques, y compris les attaques par code malveillant et les attaques de réseau.

**Vulnérabilités Technologiques**

| Vulnérabilité | Description |
|---|---|
| Faiblesse des protocoles TCP/IP | • Protocole HTTP (Hypertext Transfer Protocol), Protocole FTP (File Transfer Protocol) et protocole ICMP (Internet Control Message Protocol) sont intrinsèquement non sécurisés.<br>• Protocole SNMP (Simple Network Management Protocol) et le protocole SMTP (Simple Mail Transfer Protocol) Protocole (SMTP) sont liés à la structure intrinsèquement non sécurisée sur lequel TCP a été conçu. |
| Faiblesses du système d'exploitation | • Chaque système d'exploitation présente des problèmes de sécurité qui doivent être résolus.<br>• UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8<br>• Ils sont documentés dans les archives de la CERT (Computer Emergency Response Team) archives à http://www.cert.org |
| Faiblesse des équipements réseau | Différents types d'équipements réseau, tels que les routeurs, les pare-feu et les commutateures présentent des faiblesses de sécurité qui doivent être reconnues et protégées. Leurs faiblesses comprennent la protection par mot de passe, le manque de l'authentification, les protocoles de routage et des failles de pare-feu. |

**Vulnérabilités de Configuration**

| Vulnérabilité | Description |
|---|---|
| Comptes utilisateurs non sécurisés | Les informations relatives au compte d'utilisateur peuvent être transmises de manière non sécurisée sur le réseau, exposant ainsi les noms d'utilisateur et les mots de passe aux acteurs de menaces. |
| Comptes système avec mots de passe faciles à deviner | Ce problème fréquent résulte de mots de passe utilisateur mal choisis. |
| Services Internet mal configurés | L'activation de JavaScript dans les navigateurs Web permet d'activer les attaques par le biais de JavaScript contrôlé par les acteurs de menaces lors l'accès à des sites non fiables. D'autres sources potentielles de faiblesses comprennent un terminal mal configuré services, FTP ou serveurs Web (par exemple, Microsoft Internet Information Services (IIS) et serveur HTTP Apache) |
| Paramètres par défaut non sécurisés dans les produits logiciels | Un grand nombre de produits logiciels ont des paramètres de configuration par défaut qui génèrent des failles de sécurité. |
| Équipement réseau mal configuré | Les erreurs de configuration du matériel peuvent entraîner d'importants problèmes en matière de sécurité. Par exemple, des listes d'accès mal configurées, des protocoles de routage ou les chaînes de communauté SNMP peuvent créer ou activer des failles de sécurité. |

**Vulnérabilités de Stratégie**

| Vulnérabilité | Description |
|---|---|
| Absence de stratégie de sécurité écrite | Une stratégie de sécurité ne peut pas être appliquée ni respectée de manière cohérente si elle n'est pas écrite. |
| Politique | Les batailles politiques et les conflits entre départements peuvent rendre difficile la mise en œuvre d' une stratégie de sécurité cohérente. |
| Manque de continuité de l'authentification | Des mots de passe mal choisis, faciles à trouver ou établis par défaut peuvent conduire à des accès non autorisés au réseau. |
| Contrôle des accès logiques non appliqué | La surveillance et le contrôle insuffisants du réseau permettent aux attaques et aux utilisations non autorisée d'entraîner un gaspillage des ressources de l'entreprise. Cela pourrait résulter une action légale ou la résiliation des techniciens informatiques, le département de gestion informatique ou même l'entreprise qui permet à ces conditions dangereuses de persister. |
| Installation de logiciels et de matériels et modifications non conformes à la stratégie de sécurité | Des modifications non autorisées de la topologie du réseau ou l'installation d'applications logicielles non approuvées engendrent des vulnérabilités. |
| Absence d'un plan de reprise après sinistre | L'absence d'un plan de reprise après sinistre entraîne le chaos, la panique et la confusion lorsqu'un acteur de menace s'attaque l'entreprise. |

Modifié le: mardi 5 mars 2024, 14:10

◄ Cliquez ici pour être redirigé vers le module 12

Aller à...

16.1.2 - Sécurité physiq