Sécurité informatique

Les attaques

Etude des différents types d'attaques

Depuis l'ère ancienne, il existait des conflits entre les chefs, les tribus, … pour cela chacune des parties essayait d'inventer de nouvelles techniques d'attaques et de protection (sécurité).

Les attaques

- Définition du hacking

Le hacking est un ensemble de techniques informatiques, visant à attaquer un réseau, un site, etc.

Les attaques peuvent être locales (sur le même ordinateur, voire sur le même réseau) ou distantes (sur Internet, par télécommunication).

Les attaques

- Le hacking à des objectifs à satisfaire, selon les hackers on y trouve :
  - La Vérification de la sécurisation d'un système.
  - Le Vol d'informations (fiches de paye...).
  - Le Terrorisme.
  - L’Espionnage "classique ou industriel".
  - Le Chantage.
  - La Manifestation politique.
  - Le simple jeu, le défi.
  - L’apprentissage
  - Etc

Les types d’attaques

Les hackers utilisent plusieurs techniques d'attaques. Ces attaques peuvent être regroupées en trois familles différentes :

- Les attaques directes.
- Les attaques indirectes par rebond.
- Les attaques indirectes par réponse.

Les attaques directes

Ce sont les plus simples des attaques. Le hacker attaque directement sa victime à partir de son ordinateur

Les attaques indirectes par rebond

Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

- Masquer l'identité (l'adresse IP) du hacker.
- Éventuellement, utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante, etc.) pour attaquer.

Le principe en lui-même est simple : les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime. D'où le terme de rebond.

Les attaques indirectes par réponse

Cette attaque est un dérivé de l'attaque par rebond. Elle offre les mêmes avantages, du point de vue du hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime.

Classification des attaques

1. Les attaques de modification
2. Les attaques d‘accès
3. Les attaques de mots de passe
4. Les attaques par saturation

Failles de sécurité sur internet

IP Spoofing

L'IP Spoofing signifie usurpation d'adresse IP. Bien que cette attaque soit ancienne, certaines formes d'IP Spoofing sont encore d'actualité. Effectivement, cette attaque peut être utilisée de deux manières différentes,

- La première utilité de l'IP Spoofing va être de falsifier la source d'une attaque. Par exemple, lors d'une attaque de type déni de service, l'adresse IP source des paquets envoyés sera falsifiée pour éviter de localiser la provenance de l'attaque
- L'autre utilisation de l'IP Spoofing va permettre de profiter d'une relation de confiance entre deux machines pour prendre la main sur l'une des deux.

DNS Spoofing

Le therme "Spoofing" désigne en Français "l'usurpation". C-à-d, se faire passer pour quelqu'un d'autre. le "Spoofing DNS" consiste à usurper l'identité d'un serveur DNS déjà connu.

Le DNS Spoofing est une méthode utilisée pour rediriger des ordinateurs vers une fausse adresse.

DNS Spoofing

Le DNS spoofing, consiste à récupérer le flux réseau pour répondre à votre requête en vous donnant une mauvaise adresse IP. De ce fait, pensant vous connecter à www.dicodunet.com, vous arriveriez sur une autre page ou sur rien du tout.
Cette technique est utilisée pour les attaques réseaux.

Flooding

Flooding est une action généralement malveillante qui consiste à envoyer une grande quantité de données inutiles dans un réseau afin de le rendre inutilisable, par exemple en saturant sa bande passante ou en provoquant le plantage des machines du réseau dont le déni de service est la conséquence possible.

Smurf

C'est un ping flooding un peu particulier. C'est une attaque axée réseaux, faisant partie de la grande famille des Refus De Service (DOS : Denial Of Service). Ce procédé est décomposé en deux étapes:

- La première est de récupérer l'adresse IP de la cible par spoofing.
- La seconde est d'envoyer un flux maximal de packets ICMP ECHO (ping) aux adresses de Broadcast. Chaque ping comportant l'adresse spoofée de l'ordinateur cible.

Hoax

Un Hoax constitue une fausse information, un canular ou une rumeur infondée circulant sur Internet, notamment par le biais du courrier électronique.

Information vraie ou fausse, souvent transmise par messagerie électronique ou dans un forum, et incitant les destinataires à effectuer des opérations ou à prendre des initiatives, souvent dommageables.

Les virus

Le virus informatique s'inspire du fonctionnement biologique des virus organiques. Il fait partie de l'écosystème complexe de la cybersécurité.

Définition

Un **virus** désigne, dans l'univers informatique, un programme malveillant dont l'objectif principal est de perturber le bon fonctionnement d'un ordinateur. Il est conçu pour se propager d'un hôte à un autre, avec la capacité de se répliquer.

Les virus

Déroulement d'une attaque par virus

Une fois qu'un virus parvient à se joindre à un programme, un fichier ou un document, il reste inactif jusqu'à ce que des circonstances particulières provoquent l'exécution de son code sur l'ordinateur ou le périphérique.

Les vers

Un ver informatique est un logiciel malveillant qui se propage sur un réseau pour infecter un maximum de systèmes. Il permet d'espionner l'activité d'un poste, de détruire ou de corrompre des données, d'ouvrir une porte dérobée aux hackers. Le ver est également employé pour réaliser une attaque par déni de service. C'est-à-dire qu'il sature un réseau ou un site Web ciblé afin pour le rendre inaccessible.

Cheval de troie

Un cheval de Troie est un type de programme malveillant se faisant passer bien souvent pour un logiciel authentique. Les chevaux de Troie peuvent être utilisés par des cybercriminels et des pirates informatiques pour accéder aux systèmes des utilisateurs.

Cheval de troie

À quoi ressemble un cheval de Troie

les chevaux de Troie peuvent ressembler à presque tout. Le jeu informatique téléchargé à partir d'un site Web étrange. Une publicité peut essayer d'installer quelque chose sur l’ordinateur.

Déni de service DoS

L'attaque par déni de service, ou DoS (en anglais *Denial of Service*), vise à perturber, ou paralyser totalement, le fonctionnement d'un serveur informatique en le bombardant à outrance de requêtes erronées.

Déni de service DoS

Le but peut être d'affecter un service en ligne ou le réseau d'une entreprise en saturant une des ressources du système : la bande passante, l'espace de stockage, la capacité de traitement d'une base de données, les ressources de calcul des processeurs, la mémoire vive, etc.

Déni de service DoS

Comment fonctionne une attaque DoS

Les ressources réseau, telles que les serveurs Web, ne peuvent simultanément gérer qu'un nombre limité de requêtes. Outre la limite de capacité du serveur, le canal qui relie le serveur à Internet possède lui aussi une bande passante/capacité limitée. Lorsque le nombre de requêtes dépasse la capacité maximale d'un composant de l'infrastructure, le niveau de service peut rencontrer les problèmes suivants :

- La réponse aux requêtes est beaucoup plus lente que la normale.
- Les requêtes de tout ou partie des utilisateurs peuvent être totalement ignorées.

Écoute du réseau (sniffer)

Écoute du réseau consiste à écouter les communications réseau afin de **récupérer** et d'analyser le contenu transmis. Ce contenu peut-être constitué d'informations **très sensibles** lorsque aucun chiffrement n'est utilisé. Parmi ces informations sensibles, on peut trouver le contenu d'une conversation par **mail,** les **cookies** ou encore les fameux **mots de passe**.

Écoute du réseau (sniffer)

Comment se protéger contre le sniffing réseau

La meilleure protection contre ce type d'attaque est d'utiliser un protocole de communication sécurisé comme HTTPS.