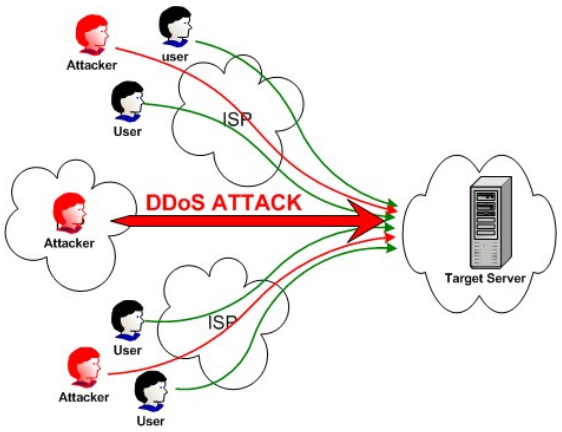
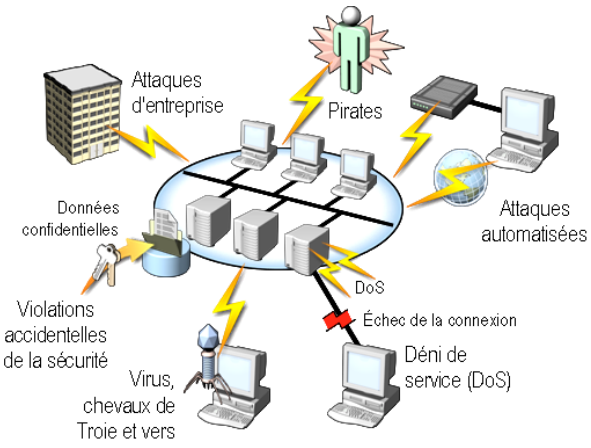
POURQUOI SÉCURISER ?





Objectifs du COURS :

Ce cours traitera essentiellement les points suivants :

- les attaques :
  - les techniques d'intrusion :
    - le sniffing
    - le « craquage » de mot de passe
    - le fishing
    - le spoofing
    - les malwares
  - Déni de service :
    - SYN Flood
    - DDOS

Les attaques visant à pirater un système en réseau dans le but de récupérer des informations sensibles ou d'altérer les services existent à tous les niveaux. La majorité des entreprises a connu une attaque, même mineure. Google a annoncé en janvier 2010 qu'elle a été la victime d'une attaque pirate ciblée. Chez un particulier, un PC non protégé et connecté à l'Internet peut être infecté en moins de 24 heures (la durée dépend du trafic généré et de l'OS). Les points d'entrée les plus vulnérables sont les navigateurs (lien malveillant) et les clients de messagerie (faux lien intégré et pièces jointes). Par ailleurs, ces derniers reçoivent souvent davantage de spam que de vrais courriers !

Les services récents sont également concernés : les nouvelles menaces impliquent les blogs, le partage des fichiers multimédia et les sites des réseaux sociaux (Facebook, Twitter, …).

Quelle que soit leur place ou leur rôle dans une architecture de réseau local ou sur Internet, les systèmes (serveurs, PC, routeurs, systèmes de stockage, …) sont donc tous vulnérables à un certain niveau pour différentes raisons :

- émergence en permanence des nouveaux usages et de nouvelles technologies, et donc de nouvelles vulnérabilités (réseaux sociaux, P2P, messagerie instantanée, réseaux sans fil, smartphones connectés en WiFi ou en 3G, téléphonie sur IP, stockage sur clé USB, …) ;
- les politiques de sécurité sont complexes car elles doivent opérer simultanément sur tous les éléments d'une architecture réseau et pour différents types d'utilisateurs (firewall sur les routeurs d'accès et sur les serveurs d'extrémité, cryptage de certains fichiers, droits accrus pour les administrateurs sur certaines ressources, …) ;
- les politiques de sécurité mises en place sont basées sur des jugements humains qui doivent de plus être révisés en permanence pour s'adapter aux nouvelles attaques ;
- la sécurisation est coûteuse en moyens, en temps et surtout en ressources humaines.

Pour limiter ces vulnérabilités (quelles que soient les solutions, un système reste toujours vulnérable), la sécurité informatique vise généralement trois objectifs principaux :

- l'intégrité consiste à garantir que les données n'ont pas été altérées sur la machine ou durant la communication (sécurité du support et sécurité du transport) ;
- la confidentialité consiste à assurer que seules les personnes autorisées ont accès aux ressources ;
- la disponibilité consiste à garantir à tout moment l'accès à un service ou à des ressources.

Un quatrième objectif peut être rajouté, il s'agit de la non-répudiation qui permet de garantir qu'aucun des correspondants ne pourra nier la transaction. L'authentification est un moyen de garantir la confidentialité. Elle consiste à s'assurer de l'identité d'un utilisateur ; un contrôle d'accès (nom d'utilisateur et mot de passe crypté) permet de limiter l'accès à certaines ressources (lecture seule sur tel dossier, accès interdit à tel fichier, …).

LES ATTAQUES

Les attaques peuvent être classées en deux grandes catégories : les techniques d'intrusion dont l'objectif principal est de s'introduire sur un réseau pour découvrir ou modifier des données et les dénis de service (DoS : Denial of Service attack) qui ont pour but d'empêcher une application ou un service de fonctionner normalement.
Cette deuxième catégorie agit donc sur la disponibilité de l'information tandis que la première concerne essentiellement la confidentialité et l'intégrité.

LES TECHNIQUES D'INTRUSION

Ces techniques peuvent être classées suivant le niveau d'intervention :

- les accès physiques vont du vol de disque dur ou de portable à l'écoute du trafic sur le réseau (sniffing) ;
- l'ingénierie sociale permet de retrouver ou de récupérer directement des couples identifiant/mot de passe en envoyant par exemple des messages falsifiés (phishing) ;
- l'interception de communication permet l'usurpation d'identité, le vol de session (hijacking), le détournement ou l'altération de messages (spoofing) ;

- les intrusions sur le réseau comprennent le balayage de ports (port scan), l'élévation de privilèges (passage du mode utilisateur au mode administrateur) et surtout les logiciels malveillants ou malwares (virus, vers et chevaux de Troie).

LE SNIFFING

Sur la plupart des réseaux, les trames sont diffusées sur tout le support (câble Ethernet, transmission radio WiFi, …). En fonctionnement normal, seul le destinataire reconnaît son adresse et lit le message. La carte Ethernet ou WiFi d'un PC peut être reprogrammée pour lire tous les messages qui traversent le réseau (promiscuous mode).

Exemple d'activation du promiscuous mode (sous GNU/Linux bien entendu !) :
ifconfig eth0 promisc ou **ip link set wlan0 promisc on**

Pour la désactivation :
ifconfig eth0 -promisc ou **ifconfig eth0 promisc off**

La limite dans ce cas est le dispositif d'interconnexion utilisé sur le LAN ou le segment de LAN (switch, routeur). Les hackers utilisent des sniffers ou analyseurs réseau qui scannent tous les messages qui circulent sur le réseau et recherchent ainsi des identités et des mots de passe. La commande « tcpdump » sous GNU/Linux (bien entendu !) et le logiciel « Wireshark », par exemple permettent le sniffing.

LE « CRAQUAGE » DE MOT DE PASSE

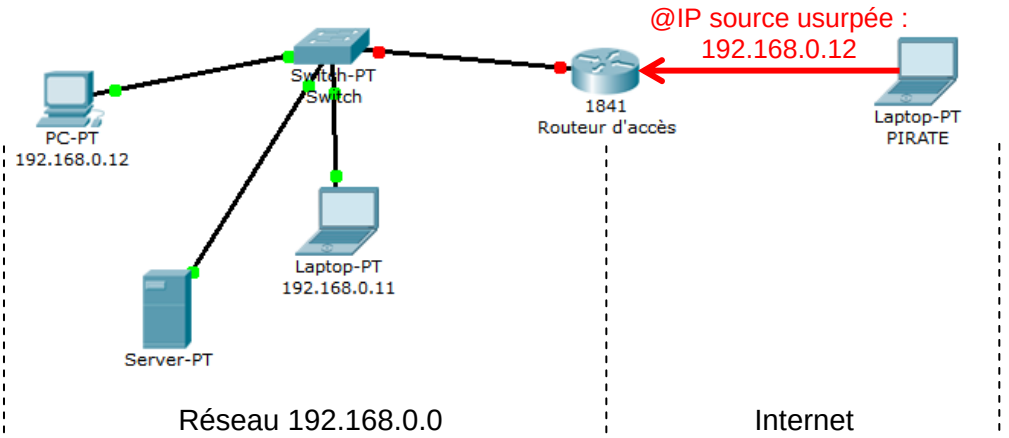
Le hacker utilise un dictionnaire de mots de noms propres construit à partir d'informations personnelles et privées qui ont été collectées (social engineering).
Ces chaînes de caractère sont essayées une à une à l'aide de programmes spécifiques qui peuvent tester des milliers de mots de passe à la seconde (exemple : John the ripper).
Toutes les variations sur les mots peuvent être testées : mots écrits à l'envers, lettres majuscules et minuscules, ajout de chiffres et de symboles. Ce type d'attaque est souvent nommé « attaque par force brute » car le mot de passe est deviné grâce à des milliers d'essais successifs à partir d'un dictionnaire, et non pas retrouvé à l'aide d'un programme capable de décrypter une chaîne de caractère.

LE PHISHING

Ce mot anglais provient de la contraction de fishing (pêcher) et de phreaking (pirater le réseau téléphonique). Il s'agit de conduire des internautes à divulguer des informations confidentielles, notamment bancaires, en usant d'un hameçon fait de mensonge et de contrefaçon électronique (identité visuelle d'un site connu, en-têtes, logo, …). Le cas le plus classique est celui d'un mail usurpant l'identité de votre banque et contenant un lien vers un faux site où l'on vous demandera de confirmer votre numéro de carte bleue par exemple.
Le phishing utilise également des virus qui installent des programmes espions afin d'intercepter la frappe des données confidentielles sur le clavier (keyloggers) pour les transmettre ensuite sur un site où le « phisher » pourra les récupérer.
La parade proposée par la plupart des banques est une saisie à la souris du numéro de compte et de code d'entrée.

LE SPOOFING

L'attaque basique de ce type est la falsification d'adresse IP : l'agresseur prétend provenir d'une machine interne pour pénétrer sur le réseau privé. Cette attaque peut être simplement bloquée avec un firewall au niveau du routeur d'accès qui éliminera les paquets entrants avec une IP source interne.



Le mail spoofing : les courriers électroniques sur Internet sont également exposés à la falsification. Une adresse d'expéditeur peut être falsifiée simplement dans la mesure où elle ne comporte pas de signature numérique. Le protocole d'envoi de messages SMTP n'est pas sécurisé.

Le DNS spoofing : le pirate utilise les faiblesses du protocole DNS et de son implémentation sur les serveurs de noms de domaine pour rediriger les internautes vers des sites falsifiés. Le but du pirate est donc de faire correspondre l'adresse IP d'une machine qu'il contrôle à l'URL réel d'une machine publique. On peut distinguer deux attaques de type DNS spoofing :

- le DNS ID spoofing basé sur la récupération et l'exploitation dans une fausse réponse du numéro d'identification contenu dans une requête DNS ;
- le DNS cache poisoning qui corrompt (empoisonne) avec de fausses adresses le cache des serveurs DNS.

Le web spoofing est une version élaborée de l'IP spoofing : il s'agit de remplacer un site par une version pirate du même site. Cette technique est notamment utilisée dans la dernière étape du phishing. La falsification se déroule en plusieurs temps :

- amener la victime à entrer dans le faux site web (grâce à l'utilisation du DNS spoofing par exemple) ;
- intercepter les requêtes HTTP ;
- récupérer les vraies pages web et modifier ces pages ;
- envoyer de fausses pages aux victimes.

LES MALWARES

Le terme « virus » est souvent employé abusivement pour désigner toutes sortes de logiciels malveillants (les virus ont été historiquement les premiers malwares). Un logiciel antivirus devrait logiquement s'appeler anti-malwares puisqu'il permet aussi de détecter les vers et les chevaux de Troie. Le spam est l'un des vecteurs les plus importants de propagation des malwares.

Un virus est un programme qui se propage à l'aide d'autres programmes ou de fichiers. Il est souvent simple et facile à détecter à partir de son code (signature) mais néanmoins efficace lorsqu'il se propage plus rapidement que la mise à jour des antivirus. Un virus passe le plus souvent par la messagerie et est activé par la sélection d'un lien sur le message ou l'ouverture d'un fichier attaché. Les conséquences de l'exécution du virus peuvent aller de la simple modification des paramètres d'une application (page par défaut du navigateur) ou de la base de registre du système (exécution automatique d'un programme commercial à chaque démarrage) à l'effacement de données ou de fichiers essentiels à l'OS.

Un ver (worm) est un programme plus sophistiqué capable de se propager et de s'auto-reproduire sans l'utilisation d'un programme quelconque, ni d'une action d'une personne. La particularité des vers ne réside pas forcément dans leur capacité immédiate de nuire mais dans leur facilité de se propager grâce par exemple aux listes de contacts présentes sur les PC ou les smartphones. Le premier ver introduit sur l'iPhone change le fond d'écran : en avril 2009, le ver « StalkDaily » a exploité une faille de sécurité sur le site Twitter pour envoyer des milliers de messages de spam en utilisant des comptes de membres Twitter.

Un cheval de Troie (trojan) est un programme caché dans un autre programme qui s'exécute au démarrage du programme. Il permet donc de s'introduire sur le système à l'insu de la victime (ouverture d'une porte dérobée ou backdoor) ; le cheval de Troie devient alors autonome et peut agir comme un virus en infectant des données ou des programmes.

DÉNI DE SERVICE

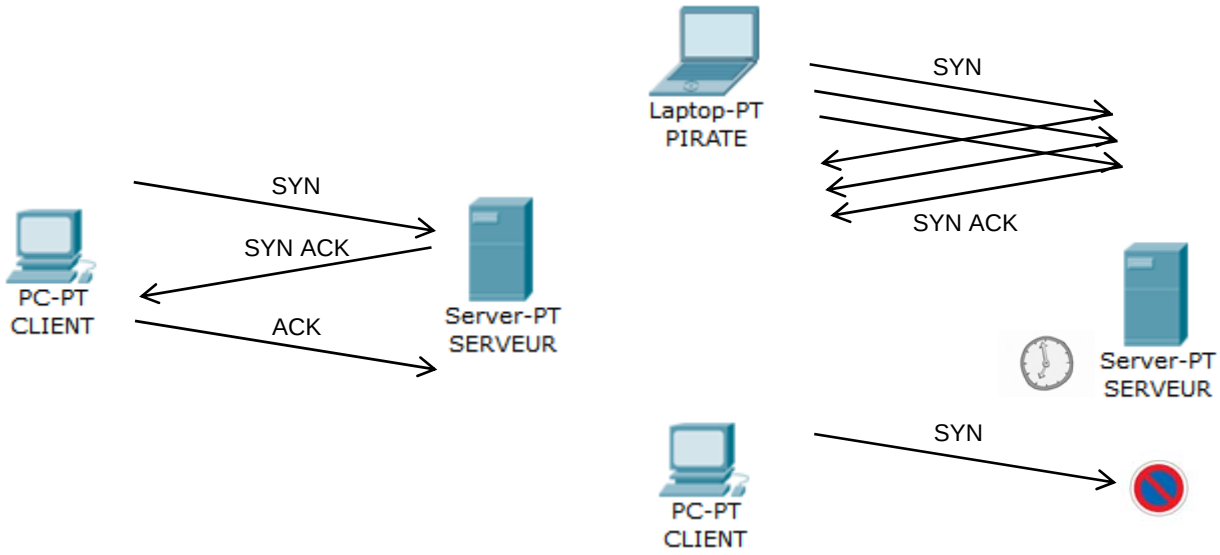
Ce type d'attaque (Denial Of Service ou DOS) empêche par saturation un service de fonctionner correctement sur une machine. Par exemple « Ping of the death » qui est la plus ancienne des attaques de type DOS : un ping continu avec une taille de paquet maximum est lancé vers la machine cible.
Une variante connu sou le nom de « smarfing » est basée sur l'envoi d'un « echo request » ICMP avec comme adresse source celle de la victime et une adresse de destination de broadcast.
Les réponses « echo reply » provenant de toutes les machines du réseau vers la machine de la victime saturent celle-ci.

SYN FLOOD

Cette attaque consiste à inonder (flooding) la cible à l'aide de demandes successives d'ouverture de connexion TCP. Lors d'une ouverture normale :
- le premier segment TCP est transmis par le client avec le bit SYN à 1 pour demander l'ouverture ;
- le serveur répond avec dans son segment TCP les bits SYN et ACK à 1 ;
- le client demandeur conclut la phase avec le bit ACK à 1.

Les abus interviennent au moment où le serveur a renvoyé un accusé de réception (SYN ACK) au client mais n'a pas reçu le « ACK » du client. C'est alors une connexion a semi-ouverte et l'agresseur peut saturer la structure de données du serveur victime en créant un maximum de connexions partiellement ouvertes. Le client autorisé ne pourra plus ouvrir de connexion.

Ouverture normale : **Saturation du serveur :**



Il existe plusieurs méthodes simples pour parer cette attaque :
- la limitation du nombre de connexions depuis la même source ou la même plage d'adresses IP ;
- la libération des connexions semi-ouvertes selon un choix de client et un délai aléatoire ;
- la réorganisation de la gestion des ressources allouées aux clients en évitant d'allouer des ressources tant que la connexion n'est pas complètement établie.

DDOS

Le déni de service distribué ou DDOS (Distributed Denial Of Service) a les mêmes effets que le DOS traditionnel excepté que ce n'est plus une seule machine qui attaque les autres mais une multitude de machines nommées zombies contrôlées par un maître unique. L'attaque se déroule en plusieurs étapes :
- recherche sur Internet d'un maximum de machines vulnérables qui deviendront des complices involontaires, des « zombies ». Les réseaux de zombies (botnet) ainsi formés sont une ressource précieuse pour les hackers ;
- installation sur ces machines de programmes dormants (daemons) et suppression des traces éventuelles. Les daemons sont basés sur les attaques DOS classiques (paquets UDP multiples, SYN Flood, …) ;
- activation du dispositif à l'heure et au jour programmé.

Parmi les attaques DDOS très populaires, on connaît l'attaque sur les sites Yahoo, CNN et eBay qui ont subi une inondation de leur réseau.