OFPPT

Office de la Formation Professionnelle et de la Promotion du Travail

مكتب التكوين المهني وإنعاش الشغل

ISTA ROUTE DE SEBTA TÉTOUAN

Les Types D'attaques Informatique

Préparer par le stagiaire :

-***Youssef CHAIKHI DOUAS***

contrôler par le formateur :

-***Yassin EL HADRI***

Sommaire

1.Introduction

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.
Une « **attaque** » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du systèmes et généralement préjudiciables.
Sur internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques.
Afin de contrer ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en oeuvre des dispositions préventives.
Les motivations des attaques peuvent être de différentes sortes :

- obtenir un accès au système ;
- voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- glâner des informations personnelles sur un utilisateur ;
- récupérer des données bancaires ;
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- troubler le bon fonctionnement d'un service ;
- utiliser le système de l'utilisateur comme « rebond » pour une attaque ;
- utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée

2. Typologies de pirates

2.1. Qu'est-ce qu'un hacker ?

Le terme « **hacker** » est souvent utilisé pour désigner un pirate informatique. Les victimes de piratage sur des réseaux informatiques aiment à penser qu'ils ont été attaqués par des pirates chevronnés ayant soigneusement étudié leur système et ayant développé des outils spécifiquement pour en exploiter les failles.
Le terme *hacker* a eu plus d'une signification depuis son apparition à la fin des années 50. A l'origine ce nom désignait d'une façon méliorative les programmeurs émérites, puis il servit au cours des années 70 à décrire les révolutionnaires de l'informatique, qui pour la plupart sont devenus les fondateurs des plus grandes entreprises informatiques.
C'est au cours des années 80 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéos, en désamorçant les protections de ces derniers, puis en en revendant des copies.
Aujourd'hui ce mot est souvent utilisé à tort pour désigner les personnes s'introduisant dans les systèmes informatiques

2.2. Les différents types de pirates

En réalité il existe de nombreux types d'"attaquants" catégorisés selon leur expérience et selon leurs motivations :
Les « white hat hackers », hackers au sens noble du terme, dont le but est d'aider à l'amélioration des systèmes et technologies informatiques, sont généralement à l'origine des principaux protocoles et outils informatiques que nous utilisons aujourd'hui; Le courrier électronique est un des meilleurs exemples ;

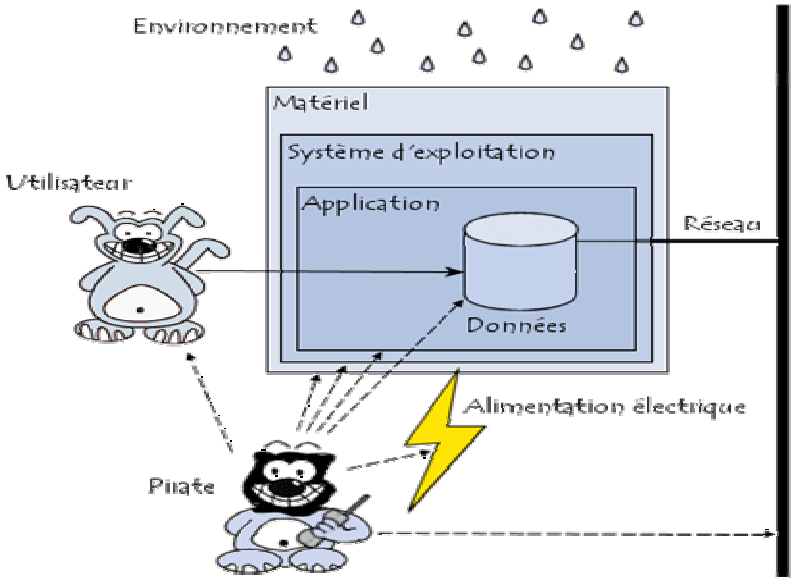
- Les « black hat hackers », plus couramment appelés pirates, c'est-à-dire des personnes s'introduisant dans les systèmes informatiques dans un but nuisible ;
- Les « script kiddies » (traduisez gamins du script, parfois également surnommés crashers, lamers ou encore packet monkeys, soit les singes des paquets réseau) sont de jeunes utilisateurs du réseau utilisant des programmes trouvés sur Internet, généralement de façon maladroite, pour vandaliser des systèmes informatiques afin de s'amuser.
- Les « phreakers » sont des pirates s'intéressant au réseau téléphonique commuté (RTC) afin de téléphoner gratuitement grâce à des circuits électroniques (qualifiées de box, comme la blue box, la violet box, ...) connectés à la ligne téléphonique dans le but d'en falsifier le fonctionnement. On appelle ainsi « phreaking » le piratage de ligne téléphonique.

- Les « carders » s'attaquent principalement aux systèmes de cartes à puces (en particulier les cartes bancaires) pour en comprendre le fonctionnement et en exploiter les failles. Le terme carding désigne le piratage de cartes à puce.
- Les « crackers » ne sont pas des biscuits apéritifs au fromage mais des personnes dont le but est de créer des outils logiciels permettant d'attaquer des systèmes informatiques ou de casser les protections contre la copie des logiciels payants. Un « crack » est ainsi un programme créé exécutable chargé de modifier (patcher) le logiciel original afin d'en supprimer les protections.

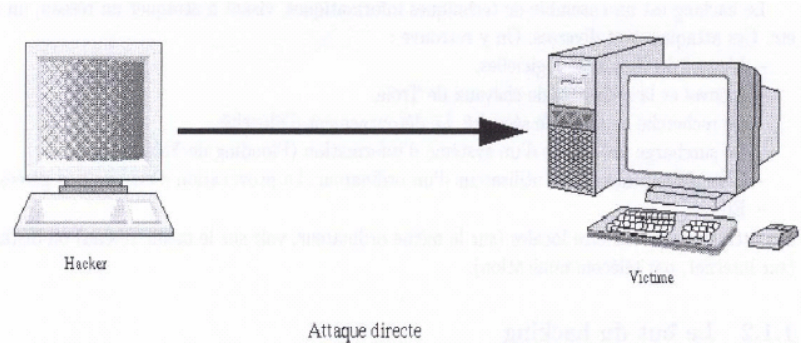
Les « hacktivistes » (contraction de hackers et activistes que l'on peut traduire en cybermilitant ou cyberrésistant), sont des hackers dont la motivation est principalement idéologique. Ce terme a été largement porté par la presse, aimant à véhiculer l'idée d'une communauté parallèle (qualifiée généralement de underground, par analogie aux populations souterraines des films de science-fiction.

3. Types d'attaques

Les systèmes informatiques mettent en oeuvre différentes composantes, allant de l'électricité pour alimenter les machines au logiciel exécuté via le système d'exploitation et utilisant le réseau.
Les attaques peuvent intervenir à chaque maillon de cette chaîne, pour peu qu'il existe une vulnérabilité exploitable. Le schéma ci-dessous rappelle très sommairement les différents niveaux pour lesquels un risque en matière de sécurité existe :



3.1. Attaques direct



C'est la plus simple des attaques à réaliser :

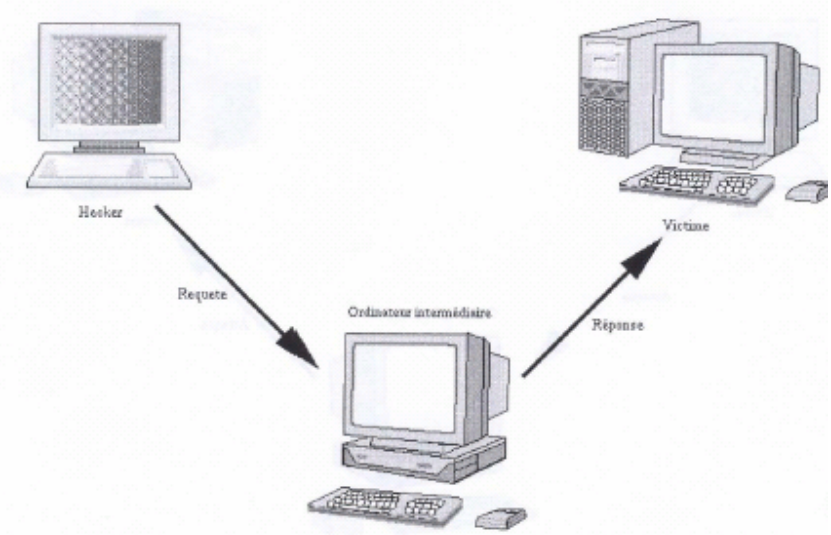
- Le hacker attaque directement sa victime à partir de son ordinateur par des scripts d'attaques faiblement paramétrable
- les programmes de hack qu'ils utilisent envoient directement les packets à la victime.
- Dans ce cas, il est possible en général de remonter à l'origine de l'attaque, identifiant par la même occasion l'identité de l'attaquant.

3.2. Attaques par rebond

Lors d'une attaque, le pirate garde toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle les pirates privilégient habituellement les **attaques par rebond** (par opposition aux **attaques directes**), consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter à lui (telle que son

adresse IP) et dans le but d'utiliser les ressources de la machine servant de rebond.
Cela montre l'intérêt de protéger son réseau ou son ordinateur personnel, il est possible de se retrouver « complice » d'une attaque et en cas de plainte de la victime, la première personne interrogée sera le propriétaire de la machine ayant servi de rebond.
Avec le développement des réseaux sans fils, ce type de scénario risque de devenir de plus en plus courant car lorsque le réseau sans fil est mal sécurisé, un pirate situé à proximité peut l'utiliser pour lancer des attaques !

3.3. Les attaques indirectes par réponse



Cette attaque est un dérivé de l'attaque par rebond.

- Elle offre les même 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.

4. Technique d'attaque

4.1. Protection par mot de passe

4.1.1. Les mots de passe

Lors de la connexion à un système informatique, celui-ci demande la plupart du temps un **identifiant** (en anglais *login* ou *username*) et un **mot de passe** (en anglais *password*) pour y accéder. Ce couple *identifiant/mot de passe* forme ainsi la clé permettant d'obtenir un accès au système.
Si l'identifiant est généralement automatiquement attribué par le système ou son administrateur, le choix du mot de passe est souvent laissé libre à l'utilisateur. Ainsi, la plupart des utilisateurs, estimant qu'ils n'ont rien de vraiment secret à protéger, se contentent d'utiliser un mot de passe facile à retenir (par exemple leur identifiant, le prénom de leur conjoint ou leur date de naissance).
Or, si les données sur le compte de l'utilisateur n'ont pas un caractère stratégique, l'accès au compte de l'utilisateur peut constituer une porte ouverte vers le système tout entier. En effet, dès qu'un pirate obtient un accès à un compte d'une machine, il lui est possible d'élargir son champ d'action en obtenant la liste des utilisateurs autorisés à se connecter à la machine. A l'aide d'outils de génération de mots de passe, le pirate peut essayer un grand nombre de mots de passe générés aléatoirement ou à l'aide d'un dictionnaire (éventuellement une combinaison des deux). S'il trouve par hasard le mot de passe de l'administrateur, il obtient alors toutes les permissions sur la machine !
De plus, à partir d'une machine du réseau, le pirate peut éventuellement obtenir un accès sur le réseau local, ce qui signifie qu'il peut dresser une cartographie des autres serveurs côtoyant celui auquel il a obtenu un accès.
Les mots de passe des utilisateurs représentent donc la première défense contre les attaques envers un système, c'est la raison pour laquelle il est nécessaire de définir une politique en matière de mots de passe afin d'imposer aux utilisateurs le choix d'un mot de passe suffisamment sécurisé.
Méthodes d'attaque
La plupart des systèmes sont configurés de manière à bloquer temporairement le compte d'un utilisateur après un certain nombre de tentatives de connexion infructueuses. Ainsi, un pirate peut difficilement s'infiltrer sur un système de cette façon.
En contrepartie, un pirate peut se servir de se mécanisme d'auto-défense pour bloquer l'ensemble des comptes utilisateurs afin de provoquer un déni de service.
Sur la plupart des systèmes les mots de passe sont stockés de manière chiffrée (« cryptée ») dans un fichier ou une base de données.

Néanmois, lorsqu'un pirate obtient un accès au système et obtient ce fichier, il lui est possible de tenter de casser le mot de passe d'un utilisateur en particulier ou bien de l'ensemble des comptes utilisateurs.

4.1.2. Attaque par force brute

On appelle ainsi « **attaque par force brute** » (en anglais « *brute force cracking* », parfois également *attaque exhaustive*) le cassage d'un mot de passe en testant tous les mots de passe possibles. Il existe un grand nombre d'outils, pour chaque système d'exploitation, permettant de réaliser ce genre d'opération. Ces outils servent aux administrateurs système à éprouver la solidité des mots de passe de leurs utilisateurs mais leur usage est détourné par les pirates informatiques pour s'introduire dans les systèmes informatiques.

4.1.3. Attaque par dictionnaire

Les outils d'attaque par force brute peuvent demander des heures, voire des jours, de calcul même avec des machines équipées de processeurs puissants. Ainsi, une alternative consiste à effectuer une « **attaque par dictionnaire** ». En effet, la plupart du temps les utilisateurs choisissent des mots de passe ayant une signification réelle. Avec ce type d'attaques, un tel mot de passe peut être craqué en quelques minutes.

4.1.4. Attaque hybride

Le dernier type d'attaques de ce type, appelées « **attaques hybrides** », vise particulièrement les mots de passe constitué d'un mot traditionnel et suivi d'une lettre ou d'un chiffre (tel que « marechal6 »). Il s'agit d'une combinaison d'attaque par force brute et d'attaque par dictionnaire.
Il existe enfin des moyens permettant au pirate d'obtenir les mots de passe des utilisateurs :
Les key loggers (littéralement « enregistreurs de touches »), sont des logiciels qui, lorsqu'ils sont installés sur le poste de l'utilisateur, permettent d'enregistrer les frappes de claviers saisies par l'utilisateur. Les systèmes d'exploitation récents possèdent des mémoires tampon protégées permettant de retenir temporairement le mot de passe et accessibles uniquement par le système.
L'ingénierie sociale consiste à exploiter la naïveté des individus pour obtenir des informations. Un pirate peut ainsi obtenir le mot de passe d'un individu en se faisant passer pour un administrateur du réseau ou bien à l'inverse appeler l'équipe de support en demandant de réinitialiser le mot de passe en prétextant un caractère d'urgence ;
L'**espionnage** représente la plus vieille des méthodes. Il suffit en effet parfois à un pirate d'observer les papiers autour de l'écran de l'utilisateur ou sous le clavier afin d'obtenir le mot de passe. Par ailleurs, si le pirate fait partie de l'entourage de la victime, un simple coup d'oeil par dessus son épaule lors de la saisie du mot de passe peut lui permettre de le voir ou de le deviner.

4.1.5. Choix du mot de passe

Il est aisément compréhensible que plus un mot de passe est long, plus il est difficile à casser. D'autre part, un mot de passe constitué uniquement de chiffres sera beaucoup plus simple à casser qu'un mot de passe contenant des lettres :
Un mot de passe de 4 chiffres correspond à 10 000 possibilités (10^4). Si ce chiffre paraît élevé, un ordinateur doté d'une configuration modeste est capable de le casser en quelques minutes.
On lui préfèrera un mot de passe de 4 lettres, pour lequel il existe 456972 possibilités (26^4). Dans le même ordre d'idée, un mot de passe mêlant chiffres et lettres, voire également des majuscules et des caractères spéciaux sera encore plus difficile à casser.
Mots de passe à **éviter** :
votre identifiant
votre nom
votre prénom ou celui d'un proche (conjoint, enfant, etc.) ;
un mot du dictionnaire ;
un mot à l'envers (les outils de cassage de mots de passe prennent en compte cette possibilité) ;
un mot suivi d'un chiffre, de l'année en cours ou d'une année de naissance (par exemple « password1999 »).

4.1.6. Politique en matière de mot de passe

L'accès au compte d'un seul employé d'une entreprise peut compromettre la sécurité globale de toute l'organisation. Ainsi, toute entreprise souhaitant garantir un niveau de sécurité optimal se doit de mettre en place une réelle politique de sécurité de matière de mots de passe. Il s'agit notamment d'imposer aux employés le choix d'un mot de passe conforme à certaines exigences, par exemple :
Une longueur de mot de passe minimale
La présence de caractères particuliers
Un changement de casse (minuscule et majuscules)
Par ailleurs, il est possible de renforcer cette politique de sécurité en imposant une durée d'expiration des mots de passe, afin d'obliger les utilisateurs à modifier régulièrement leur mot de passe. Cela complique ainsi la tâche des pirates essayant de casser des mots de passe sur la durée. Par ailleurs il s'agit d'un excellent moyen de limiter la durée de vie des mots de passe ayant été cassés.
Enfin, il est recommandé aux administrateurs système d'utiliser des logiciels de cassage de mots de passe en interne sur les mots de passe de leurs utilisateurs afin d'en éprouver la solidité. Ceci doit néanmoins se faire dans le cadre de la politique de sécurité et être écrit noir sur blanc, afin d'avoir l'approbation de la direction et des utilisateurs.

4.1.7. Mots de passe multiples

Il n'est pas sain d'avoir un seul mot de passe, au même titre qu'il ne serait pas sain d'avoir comme code de carte bancaire le même code que pour son téléphone portable et que le digicode en bas de l'immeuble.
Il est donc conseillé de posséder plusieurs mots de passe par catégorie d'usage, en fonction de la confidentialité du secret qu'il protège. Le code d'une carte bancaire devra ainsi être utilisé uniquement pour cet usage. Par contre, le code PIN d'un téléphone portable peut correspondre à celui du cadenas d'une valise.

4.2. Attaque man in the middle

L'attaque « **man in the middle** » (littéralement « *attaque de l'homme au milieu* » ou « *attaques de l'intercepteur* »), parfois notée *MITM*, est un scénario d'attaque dans lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties.
La plupart des attaques de type « *man in the middle* » consistent à écouter le réseau à l'aide d'un outil appelé sniffer.

4.3. Attaque par rejeu

Les attaques par « rejeu » (en anglais « replay attaque ») sont des attaques de type « Man in the middle » consistant à intercepter des paquets de données et à les rejouer, c'est-à-dire les retransmettre tels quel (sans aucun déchiffrement) au serveur destinataire.
Ainsi, selon le contexte, le pirate peut bénéficier des droits de l'utilisateur. Imaginons un scénario dans lequel un client transmet un nom d'utilisateur et un mot de passe chiffrés à un serveur afin de s'authentifier. Si un pirate intercepte la communication (grâce à un logiciel d'écoute) et rejoue la séquence, il obtiendra alors les mêmes droits que l'utilisateur. Si le système permet de modifier le mot de passe, il pourra même en mettre un autre, privant ainsi l'utilisateur de son accès

4.4. Introduction aux attaques par déni de service

Une « **attaque par déni de service** » (en anglais « **Denial of Service** », abrégé en *DoS*) est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés.
Les attaques par déni de service sont un fléau pouvant toucher tout serveur d'entreprise ou tout particulier relié à internet. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à la réputation de sociétés ayant une présence sur internet et éventuellement de

nuire à leur fonctionnement si leur activité repose sur un système d'information.
D'un point de vue technique, ces attaques ne sont pas très compliquées, mais ne sont pas moins efficaces contre tout type de machine possédant un système d'exploitation Windows (95, 98, NT, 2000, XP, etc.), Linux (Debian, Mandrake, RedHat, Suse, etc.), Unix commercial (HP-UX, AIX, IRIX, Solaris, etc.) ou tout autre système. La plupart des attaques par déni de service exploitent des failles liées à l'implémentation d'un protocole du modèle TCP/IP.
On distingue habituellement deux types de dénis de service :

- Les dénis de service par saturation, consistant à submerger une machine de requêtes, afin qu'elle ne soit plus capable de répondre aux requêtes réelles ;
- Les dénis de service par exploitation de vulnérabilités, consistant à exploiter une faille du système distant afin de le rendre inutilisable.

Le principe des attaques par déni de service consiste à envoyer des paquets IP ou des données de taille ou de constitution inhabituelle, afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer les services réseau qu'elles proposent.
Lorsqu'un déni de service est provoqué par plusieurs machines, on parle alors de « **déni de service distribué** » (noté *DDOS* pour *Distributed Denial of Service*). Les attaques par déni de service distribué les plus connues sont *Tribal Flood Network* (notée *TFN*) et Trinoo.

4.4.1. Se protéger d'un déni de service

Pour se protéger de ce type d'attaque, il est nécessaire de mener une veille active sur les nouvelles attaques et vulnérabilités et de récupérer sur internet des correctifs logiciels (patchs) conçus par les éditeurs de logiciels ou certains groupes spécialisés :

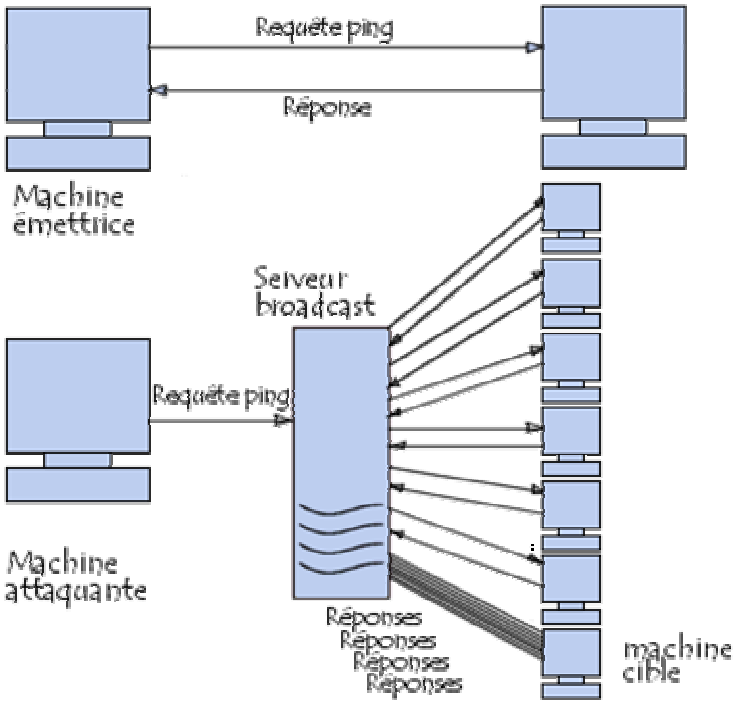
- http://windowsupdate.microsoft.com/
- http://www.securityfocus.com/

4.4.2. Attaque par réflexion (Smurf)

La technique dite « attaque par réflexion » (en anglais « smurf ») est basée sur l'utilisation de serveurs de diffusion (*broadcast*) pour paralyser un réseau. Un serveur broadcast est un serveur capable de dupliquer un message et de l'envoyer à toutes les machines présentes sur le même réseau.
Le scénario d'une telle attaque est le suivant :

- la machine attaquante envoie une requête ping (ping est un outil exploitant le protocole ICMP, permettant de tester les connexions sur un réseau en envoyant un paquet et en attendant la réponse) à un ou plusieurs serveurs de diffusion en falsifiant l'adresse IP source (adresse à laquelle le serveur doit théoriquement répondre) et en fournissant l'adresse IP d'une machine cible.
- le serveur de diffusion répercute la requête sur l'ensemble du réseau ;
- toutes les machines du réseau envoient une réponse au server de diffusion,
- le serveur broadcast redirige les réponses vers la machine cible.

Ainsi, lorsque la machine attaquante adresse une requête à plusieurs serveurs de diffusion situés sur des réseaux différents, l'ensemble des réponses des ordinateurs des différents réseaux vont être routées sur la machine cible.



De cette façon l'essentiel du travail de l'attaquant consiste à trouver une liste de serveurs de diffusion et à falsifier l'adresse de réponse afin de les diriger vers la machine cible.

4.5. Attaque du ping de la mort

L'« **attaque du ping de la mort** » (en anglais « *ping of death* ») est une des plus anciennes attaque réseau.
Le principe du ping de la mort consiste tout simplement à créer un datagramme IP dont la taille totale excède la taille maximum autorisée (65536 octets). Un tel paquet envoyé à un système possédant une pile TCP/IP vulnérable, provoquera un plantage. Plus aucun système récent n'est vulnérable à ce type d'attaque.

4.6. Attaque par fragmentation

Une « attaque par fragmentation » (en anglais fragment attack) est une attaque réseau par saturation (déni de service) exploitant le principe de fragmentation du protocole IP.
En effet, le protocole IP est prévu pour fragmenter les paquets de taille importante en plusieurs paquets IP possédant chacun un numéro de séquence et un numéro d'identification commun. A réception des données, le destinataire réassemble les paquets grâce aux valeurs de décalage (en anglais offset) qu'ils contiennent.
L'attaque par fragmentation la plus célèbre est l'attaque Teardrop. Le principe de l'attaque Teardrop consiste à insérer dans des paquets fragmentés des informations de décalage erronées. Ainsi, lors du réassemblage il existe des vides ou des recoupements (overlapping), pouvant provoquer une instabilité du système.
A ce jour, les systèmes récents ne sont plus vulnérables à cette attaque.

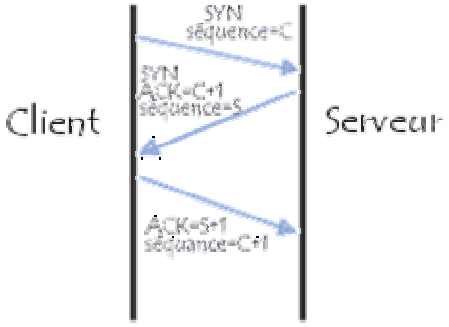
4.7. Attaque LAND

L'« attaque LAND » est une attaque réseau datant de 1997, utilisant l'usurpation d'adresse IP afin d'exploiter une faille de certaines implémentation du protocole TCP/IP dans les systèmes. Le nom de cette attaque provient du nom donné au premier code source (appelé « exploit ») diffusé permettant de mettre en oeuvre cette attaque : land.c.
L'attaque LAND consiste ainsi à envoyer un paquet possédant la même adresse IP et le même numéro de port dans les champs source et destination des paquets IP.
Dirigée contre des systèmes vulnérables, cette attaque avait pour conséquence de faire planter les systèmes ou de les conduire à des états instables.

Les systèmes récents ne sont aujourd'hui plus vulnérables à ce type d'attaque.

4.8. Attaque SYN

L'« **attaque SYN** » (appelée également « *TCP/SYN Flooding* ») est une attaque réseau par saturation (*déni de service*) exploitant le mécanisme de poignéee de main en trois temps (en anglais *Three-ways handshake*) du protocole TCP.
Le mécanisme de poignée de main en trois temps est la manière selon laquelle toute connexion « fiable » à internet (utilisant le protocole TCP) s'effectue.



Lorsqu'un client établit une connexion à un serveur, le client envoie une requête SYN, le serveur répond alors par un paquet *SYN/ACK* et enfin le client valide la connexion par un paquet *ACK* (*acknowledgement*, qui signifie *accord* ou *remerciement*).
Une connexion TCP ne peut s'établir que lorsque ces 3 étapes ont été franchies. L'attaque SYN consiste à envoyer un grand nombre de requêtes SYN à un hôte avec une adresse IP source inexistante ou invalide. Ainsi, il est impossible que la machine cible reçoive un paquet *ACK*.
Les machines vulnérables aux attaques SYN mettent en file d'attente, dans une structure de données en mémoire, les connexions ainsi ouvertes, et attendent de recevoir un paquet *ACK*. Il existe un mécanisme d'expiration permettant de rejeter les paquets au bout d'un certain délai. Néanmoins, avec un nombre de paquets SYN très important, si les ressources utilisées par la machine cible pour stocker les requêtes en attente sont épuisées, elle risque d'entrer dans un état instable pouvant conduire à un plantage ou un redémarrage.

4.9. Vol de session TCP (hijacking)

4.9.1. Le vol de session TCP

Le « **vol de session TCP** » (également appelé *détournement de session TCP* ou en anglais *TCP session hijacking*) est une technique consistant à intercepter une session TCP initiée entre deux machine afin de la détourner.
Dans la mesure où le contrôle d'authentification s'effectue uniquement à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session.

4.9.2. Source-routing

La méthode de détournement initiale consistait à utiliser l'option source routing du protocole IP. Cette option permettait de spécifier le chemin à suivre pour les paquets IP, à l'aide d'une série d'adresses IP indiquant les routeurs à utiliser.
En exploitant cette option, le pirate peut indiquer un chemin de retour pour les paquets vers un routeur sous son contrôle.

4.9.3. Attaque à l'aveugle

Lorsque le source-routing est désactivé, ce qui est le cas de nos jours dans la plupart des équipements, une seconde méthode consiste à envoyer des paquets « à l'aveugle » (en anglais « blind attack »), sans recevoir de réponse, en essayant de prédire les numéros de séquence.

4.9.4. Man in the middle

Enfin, lorsque le pirate est situé sur le même brin réseau que les deux interlocuteurs, il lui est possible d'écouter le réseau et de « faire taire » l'un des participants en faisant planter sa machine ou bien en saturant le réseau afin de prendre sa place.

4.10. Analyseurs réseau (sniffers)

4.10.1. L'analyse de réseau

Un « **analyseur réseau** » (appelé également *analyseur de trames* ou en anglais *sniffer*, traduisez « renifleur ») est un dispositif permettant d'« écouter » le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent.
En effet, dans un réseau non commuté, les données sont envoyées à toutes les machines du réseau. Toutefois, dans une utilisation normale les machines ignorent les paquets qui ne leur sont pas destinés. Ainsi, en utilisant l'interface réseau dans un mode spécifique (appelé généralement *mode promiscuous*) il est possible d'écouter tout le trafic passant par un

adaptateur réseau (une carte réseau ethernet, une carte réseau sans fil, etc.).

4.10.2. Utilisation du sniffer

Un sniffer est un formidable outil permettant d'étudier le trafic d'un réseau. Il sert généralement aux administrateurs pour diagnostiquer les problèmes sur leur réseau ainsi que pour connaître le trafic qui y circule. Ainsi les détecteurs d'intrusion (IDS, pour intrusion detection system) sont basés sur un sniffeur pour la capture des trames, et utilisent une base de données de règles (rules) pour détecter des trames suspectes.
Malheureusement, comme tous les outils d'administration, le sniffer peut également servir à une personne malveillante ayant un accès physique au réseau pour collecter des informations. Ce risque est encore plus important sur les réseaux sans fils car il est difficile de confiner les ondes hertziennes dans un périmètre délimité, si bien que des personnes malveillantes peuvent écouter le trafic en étant simplement dans le voisinage.
La grande majorité des protocoles Internet font transiter les informations en clair, c'est-à-dire de manière non chiffrée. Ainsi, lorsqu'un utilisateur du réseau consulte sa messagerie via le protocole POP ou IMAP, ou bien surfe sur internet sur des sites dont l'adresse ne commence pas par HTTPS, toutes les informations envoyées ou reçues peuvent être interceptées. C'est comme cela que des sniffers spécifiques ont été mis au point par des pirates afin de récupérer les mots de passe circulant dans le flux réseau.

4.10.3. Les parades

Il existe plusieurs façons de se prémunir des désagréments que pourrait provoquer l'utilisation d'un sniffer sur votre réseau :

- Utiliser des protocoles chiffrés pour toutes les communications dont le contenu possède un niveau de confidentialité élevé.
- Segmenter le réseau afin de limiter la diffusion des informations. Il est notamment recommandé de préférer l'utilisation de switchs (commutateurs) à celle des hubs (concentrateurs) car ils commutent les communications, c'est-à-dire que les informations sont délivrées uniquement aux machines destinataires.
- Utiliser un détecteur de sniffer. Il s'agit d'un outil sondant le réseau à la recherche de matériels utilisant le mode promiscuous.
- Pour les réseaux sans fils il est conseillé de réduire la puissance des matériels de telle façon à ne couvrir que la surface nécessaire. Cela n'empêche pas les éventuels pirates d'écouter le réseau mais réduit le périmètre géographique dans lequel ils ont la possibilité de le faire.
-

4.11. Phishing (hameçonnage)

4.11.1. Introduction au phishing

Le **phishing** (contraction des mots anglais « *fishing* », en français *pêche*, et « *phreaking* », désignant le *piratage de lignes téléphoniques*), traduit parfois en « **hameçonnage** », est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes.
La technique du phishing est une technique d'« ingénierie sociale » c'est-à-dire consistant à exploiter non pas une faille informatique mais la « faille humaine » en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de commerce.
Le mail envoyé par ces pirates usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et les invite à se connecter en ligne par le biais d'un lien hypertexte et de metre à jour des informations les concernant dans un formulaire d'une page web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, etc.
Dans la mesure où les adresses électroniques sont collectées au hasard sur Internet, le message a généralement peu de sens puisque l'internaute n'est pas client de la banque de laquelle le courrier semble provenir. Mais sur la quantité des messages envoyés il arrive que le destinataire soit effectivement client de la banque.
Ainsi, par le biais du formulaire, les pirates réussissent à obtenir les identifiants et mots de passe des internautes ou bien des données personnelles ou bancaires (numéro de client, numéro de compte en banque, etc.).
Grâce à ces données les pirates sont capables de transférer directement l'argent sur un autre compte ou bien d'obtenir ultérieurement les données nécessaires en utilisant intelligemment les données personnelles ainsi collectées.

4.11.2. Comment se protéger du phishing ?

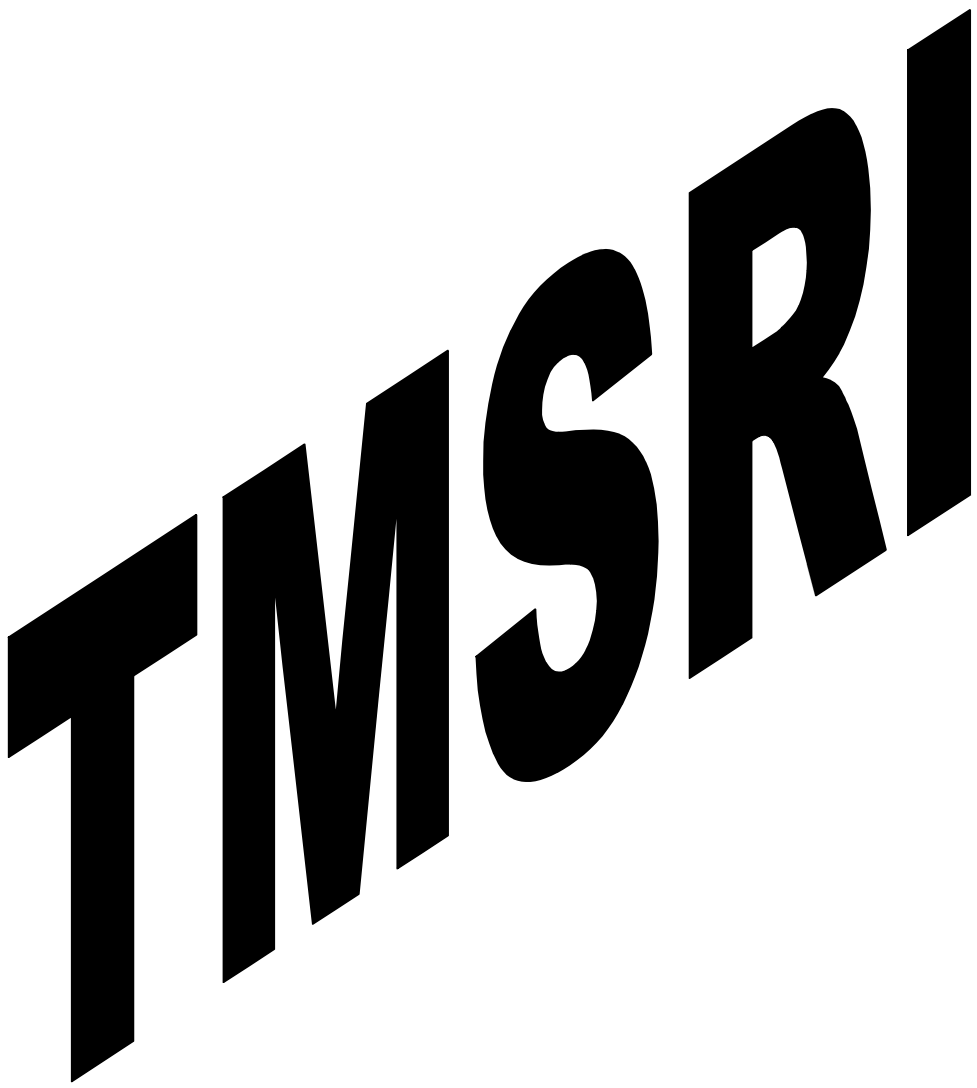
Lorsque vous recevez un message provenant a priori d'un établissement bancaire ou d'un site de commerce électronique il est nécessaire de vous poser les questions suivantes :

- Ai-je communiqué à cet établissement mon adresse de messagerie ?
- Le courrier reçu possède-t-il des éléments personnalisés permettant d'identifier sa véracité (numéro de client, nom de l'agence, etc.) ?

Par ailleurs il est conseillé de suivre les conseils suivants :

- Ne cliquez pas directement sur le lien contenu dans le mail, mais ouvrez votre navigateur et saisissez vous-même l'URL d'accès au service.

- Méfiez-vous des formulaires demandant des informations bancaires. Il est en effet rare (voire impossible) qu'une banque vous demande des renseignements aussi importants par un simple courrier électronique. Dans le doute contactez directement votre agence par téléphone !
- Assurez-vous, lorsque vous saisissez des informations sensibles, que le navigateur est en mode sécurisé, c'est-à-dire que l'adresse dans la barre du navigateur commence par https et qu'un petit cadenas est affiché dans la barre d'état au bas de votre navigateur, et que le domaine du site dans l'adresse correspond bien à celui annoncé (gare à l'orthographe du domaine)


TMSRI