

Université Ziane Achour de Djelfa



Département : Mathématiques et Informatique

Attaques et vulnérabilités des réseaux

Université Ziane Achour de Djelfa



Département : Mathématiques et Informatique

Introduction

Introduction

Hacker et cracker

Hacker

Une communauté de programmeurs expérimentés et des spécialistes des réseaux, ont créé le mot "***hacker***".

Ces informaticiens sont:

- Généralement discrets
 - Motivés par la curiosité.
-

Introduction

Hacker et cracker

cracker

- Personnes qui s'autoproclament des "hackers".
 - Adolescents de sexe masculin
 - S'introduisant à distance dans les systèmes informatiques
 - piratent des systèmes téléphoniques.
 - Utilisent des outils écrits par d'autres personnes (trouvés sur Internet).
-

Introduction

Hacker et cracker

Les vrais hackers appellent ces gens des ***crackers***.

Les vrais hackers pensent que les crackers sont:

- Des gens *paresseux*,
 - *Irresponsables et*
 - *Pas très brillants.*
-

Introduction

Objectifs des attaques

- Désinformer
 - Empêcher l'accès à une ressource
 - Prendre le contrôle d'une ressource
 - Récupérer de l'information présente sur le système
 - Utiliser le système compromis pour rebondir
 - Constituer un réseau de « botnet » (ou réseau de machines zombies)
-

Introduction

Motivations des attaques

- Vol d'informations
 - Modifications d'informations
 - Vengeance/rancune
 - Politique/religion
 - Défis intellectuels
-

Introduction

Cible des pirates

- Les états
 - Serveurs militaires
 - Banques
 - Universités
 - Tout le monde
-



Définitions



Définitions

Nœud malicieux:

- Unité malveillante (écoute puis attaque)

Attaquant actif-n-m:

- Attaquant qui possède m nœuds malicieux et qui compromet n nœuds

Attaques externes :

- Attaques lancées par un nœud qui n'appartient pas au réseau ou bien qui n'est pas autorisé à y accéder
-

Définitions

Attaques internes:

- Attaques lancées par des nœuds internes compromis ou malveillants.
 - C'est le type de menace le plus sévère
 - Les mécanismes proposés pour lutter contre les attaques externes sont inefficaces devant ce type d'attaques
-

Définitions

(Définitions: **Attaques passives**)

- Écoute des lignes
- Analyse de trafic
- Plus facile avec le sans fil
- C'est une préparation d'une attaque active

La Solution doit:

- **Assurer la confidentialité des échanges.**
-

Définitions

(Définitions: **Attaques actives**)

- **Détruire** des messages
- **Injecter** des messages erronés
- **Modifier** des messages et **6 l'identité** d'un nœud.
- ...etc





La Solution doit:

- **Assurer la disponibilité, l'intégrité, l'authentification et la non répudiation**
-

Les outils d'attaque

Pour mener à bien les attaques sur les systèmes informatiques, les pirates utilisent des outils informatiques bien connus du domaine.

Parmi ces outils, nous pouvons citer :

-  Les programmes malveillants (virus, ver, cheval de troie, logiciel espion [spyware])
 -  Les scanners et sniffers
 -  Les backdors (portes dérobées)
 -  Les spams (courriers indésirables)
-

Les programmes malveillants

Virus

C'est un programme malveillant conçu pour se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés « hôtes ».

Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté.

Il peut se répandre à travers tout moyen d'échange de données numériques comme les réseaux informatiques et les CD/DVD, les clefs USB, etc.

▪

Les programmes malveillants

Ver

Un ver informatique est un programme malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet.

Contrairement à un virus informatique, un ver n'a pas besoin d'un programme pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.

Les programmes malveillants

Cheval de troie

Un cheval de Troie est un programme d'apparence légitime conçu pour exécuter de façon cachée des actions à l'insu de l'utilisateur. En général, un cheval de Troie tente d'utiliser les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations, ou encore pour ouvrir une porte dérobée qui permet à un attaquant de prendre, à distance, le contrôle de l'ordinateur.

Les programmes malveillants

Logiciel espion (spyware, mouchard ou espiogiciel)

Un logiciel espion est un programme malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance.

Un logiciel espion est généralement composé de trois mécanismes distincts:

Infection, collecte et transmission

Les programmes malveillants



Rootkit

Un rootkit ("jeu de démarrage" en français) est un programme malveillant dont la principale fonctionnalité est de dissimuler la présence de son activité et celle des autres programmes néfastes aux yeux de l'utilisateur du système et des logiciels de sécurité (antivirus, pare-feu, IDS).

Certains rootkit peuvent installer des backdors (porte dérobée).

Les programmes malveillants

Les rootkits ont deux caractéristiques principales :

-  Ils modifient profondément le fonctionnement du système d'exploitation
 -  Ils se rendent invisibles (difficile à les détecter)
-



Attaques réseaux



Les réseaux peuvent être vulnérables:

- Par une mauvaise implémentation des piles udp/ip et tcp/ip.
 - Par des faiblesses des protocoles
-

IP Spoofing: Introduction (Usurpation d'adresse IP)

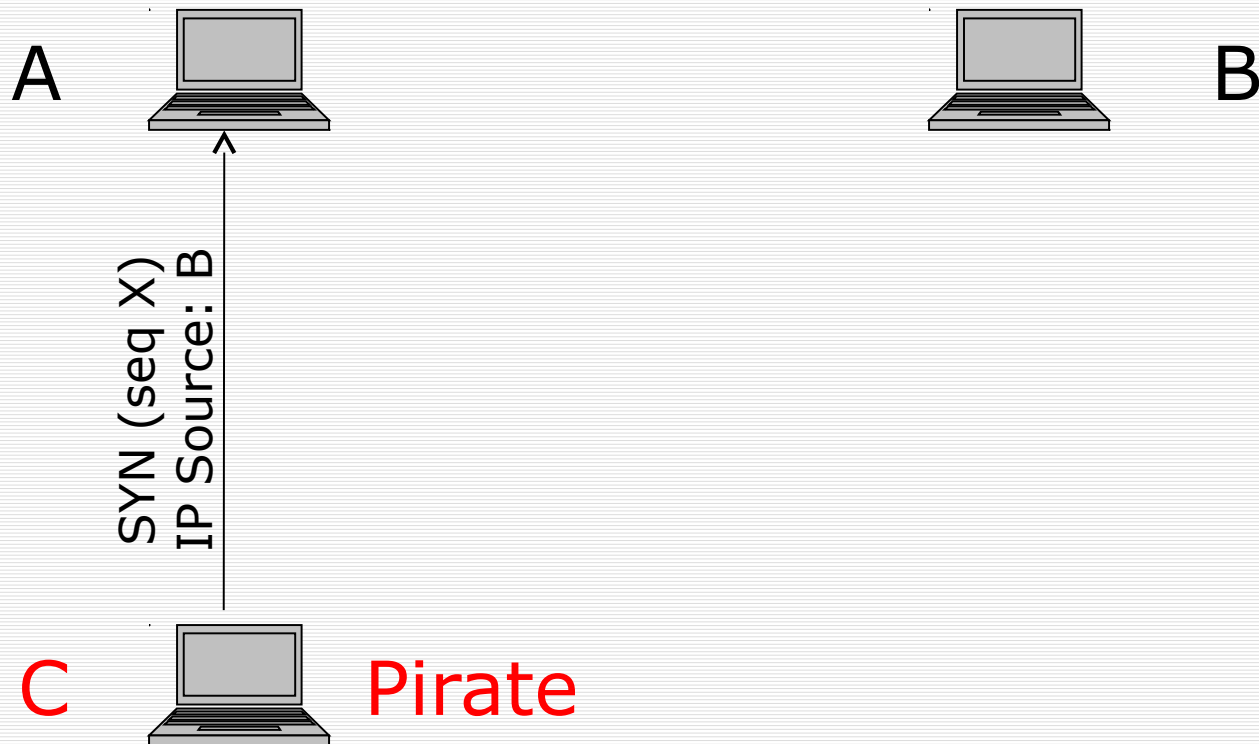
- Dans certains cas, l'adresse IP source est utilisée pour autoriser une connexion (Systèmes sur lesquels l'authentification est fondée sur l'adresse IP).

IP Spoofing: On fait croire que la requête provient d'une machine autorisée.

IP Spoofing: Principe

- **IP Spoofing:** Forger l'adresse source d'un paquet et à abusez de la confiance de cette source.
 - Plus facile à utiliser avec les protocoles basés sur **UDP**.
 - Pour **TCP** ???
-

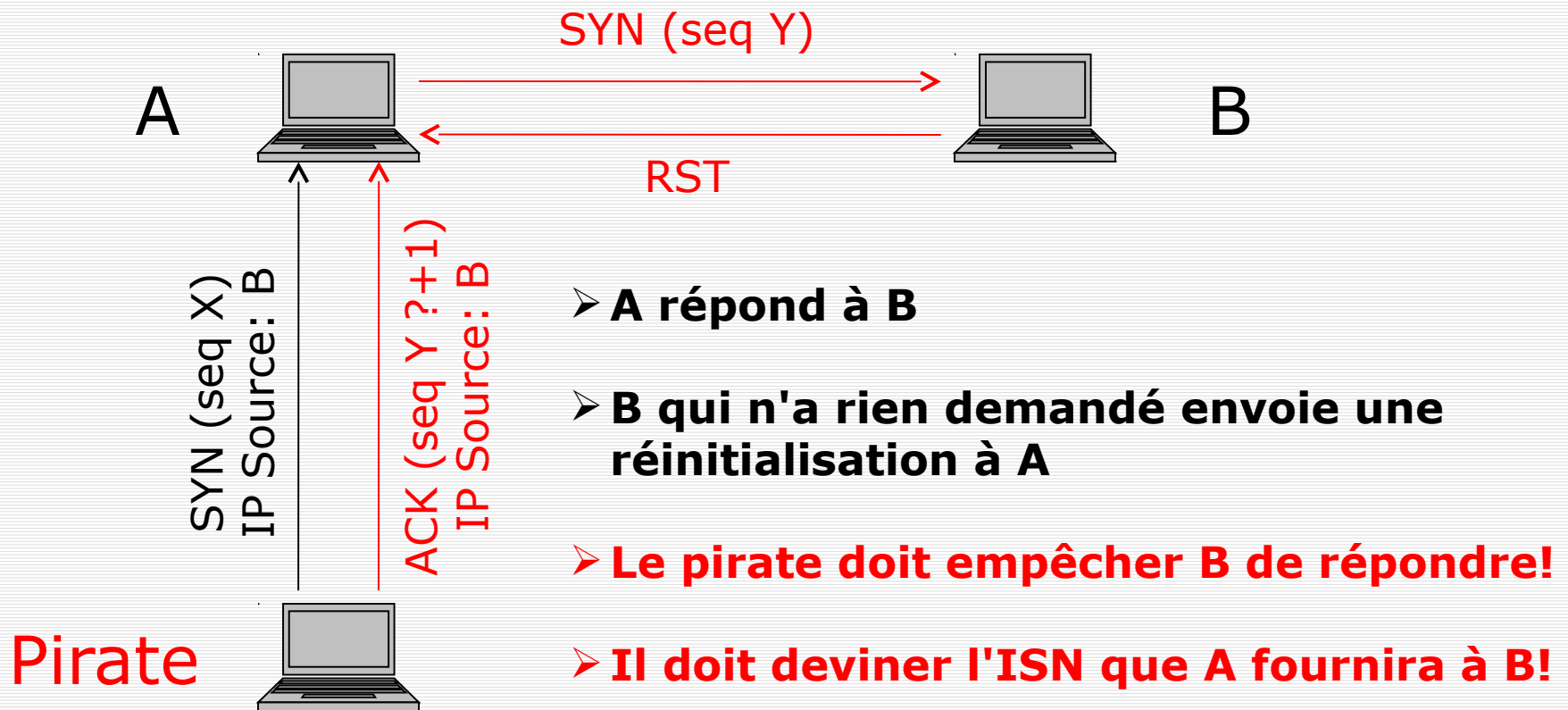
IP Spoofing: Attaques à base de TCP



IP Spoofing: Attaques à base de TCP

- TCP est un protocole en mode connecté, il utilise des acquittements et des numéros de séquence
- Pour éviter d'utiliser les mêmes numéros de séquence, un numéro de séquence initial aléatoire (ISN) est choisi pour chaque nouvelle connexion
- **Exemple d'attaque:** les protocoles **rlogin**, **rsh** sur les machines à numéro de séquence TCP prévisible.

IP Spoofing: Attaque à base de TCP



-
- **Comment deviner l'ISN d'une machine?**
 - **Comment empêcher une machine répondre! ?**

TCP ISN generation

Dans certaines implémentations de pile TCP/IP prochain ISN peut que soit prédit.

Un pirate procède comme suite:

TCP ISN generation

- Il ouvre quelques connexions (par exemple SMTP) pour obtenir les ISN courants et leurs méthodes d'incrémentation.
 - Il lance sa connexion forgée qui utilise le dernier ISN incrémenté selon la méthode détectée.
 - Il peut lancer des connexions forgées multiples avec différentes augmentations en espérant qu'au moins une est correcte.
-

➤ **Comment empêcher une machine de répondre?**

DOS (dédi de service)

- Attaque destinée à empêcher l'utilisation d'une machine ou d'un service.
 - Plus souvent utilisé pour saturer un routeur ou un serveur.
 - Ce type d'attaque peut engendrer des pertes très importantes pour une entreprise.
 - Attaque très simple à mettre en œuvre (outils faciles à trouver) et très difficile à empêcher.
-

DOS

DOS local

- **Epuisement des ressources**
- Saturation de l'espace disque
- répertoires récursifs
- boucle infinie de fork ()
- ...etc

DOS par le réseau

- **Consommation de bande passante**
 - SYN flood
 - *mailbombing.*
 - ...etc
-

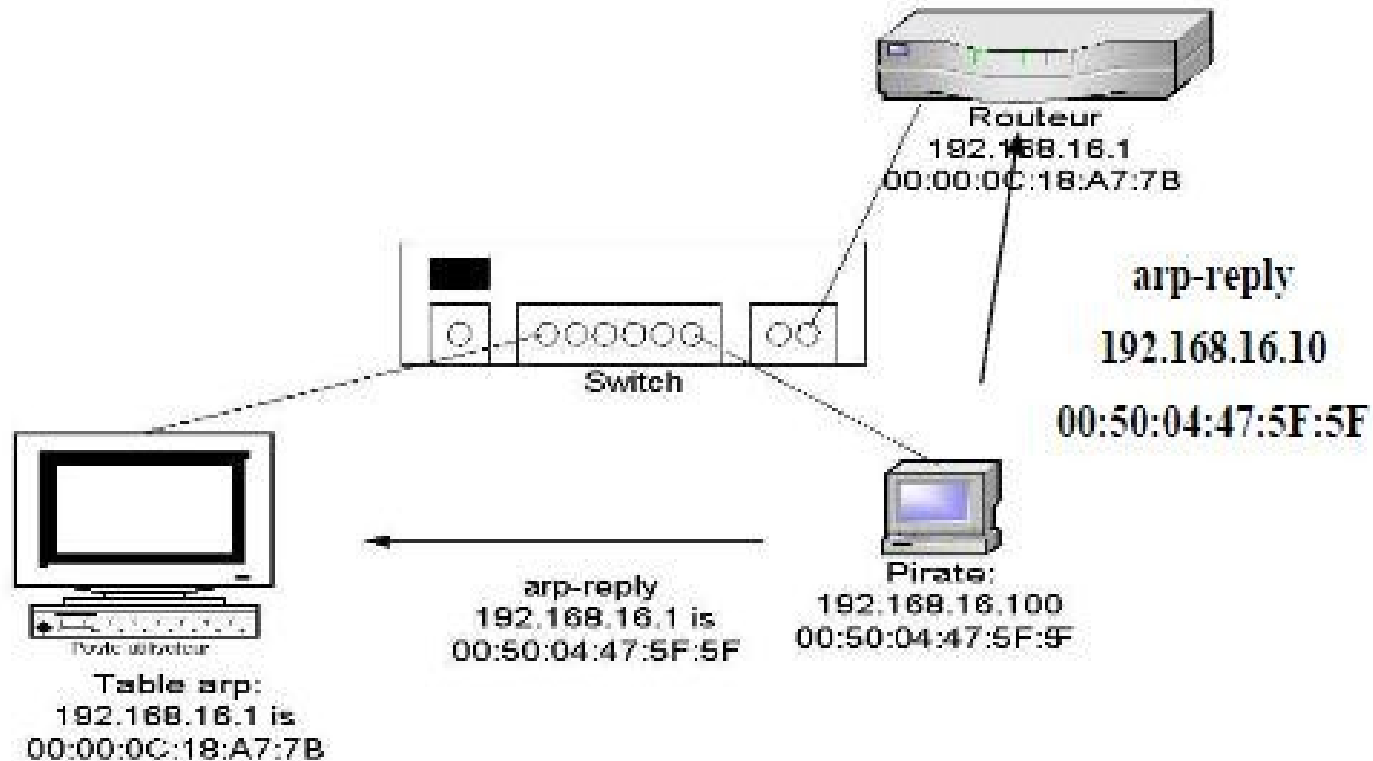
DOS: Exemple SYN Flood

- Attaque par inondation de SYN avec une adresse source usurpée (spoofée) et inaccessible.
- La machine cible doit gérer une liste de connexions dans l'état SYN_RECV .
- Le pirate sature cette liste.
- La machine victime ignore les prochaines connexions
- **Attaque visible si la commande *netstat -an* indique un grand nombre de connexions**

ARP Spoofing

-
- Pollution des caches arp avec de fausses associations adresse mac/adresse IP.
 - Permet des attaques de type "man in the middles."
-

ARP Spoofing



Se protéger contre ARP Spoofing

- Utiliser des associations statiques
 - Surveiller les changements d'association:
-

Sniffer

- De nombreux protocoles utilisent une authentification en texte clair
 - En visualisant la circulation sur un réseau, nous pouvons obtenir les noms d'utilisateurs et les mots de passe == **sniffer**
 - Les sniffers Utilisent des sockets en mode « promiscuous »
-

Sniffing: Examples

Les protocoles d'authentification dont l'échange de données est en text clair:

- telnet
 - rsh, rlogin, rexec
 - ftp
 - http (with basic authentication)
 - pop, imap (with default authentication)
-

Smurf

Envoie d'une trame ICMP "echo request « ping » sur une adresse de diffusion.

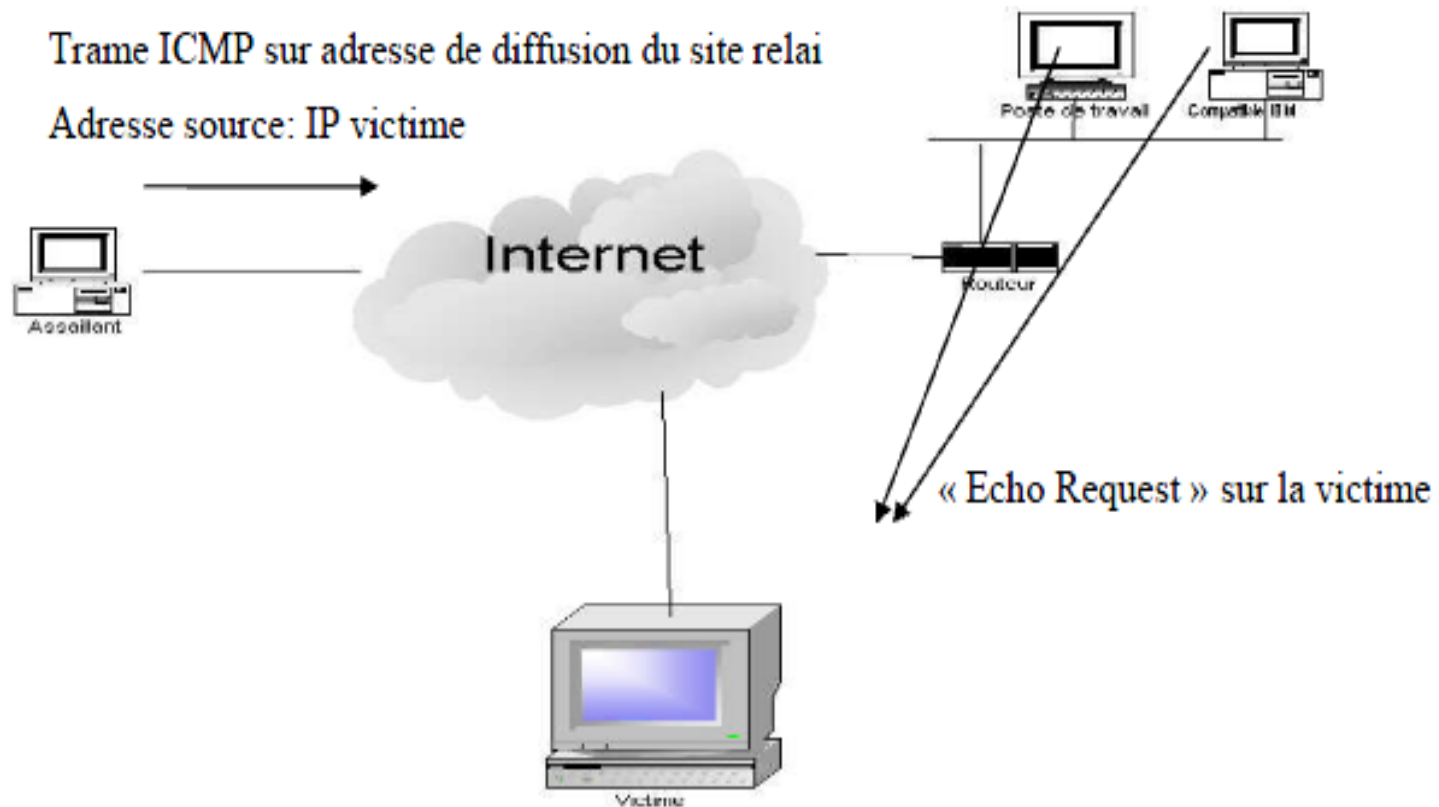
- **Exemple:** *ping 193.49.200.255*

Objectif

- Utilisée pour déterminer les machines actives sur une plage IP donnée.
 - Ecrouler une machine
-

Smurf

Ecrouter une machine



Se protéger Contre Smurf

Interdire la réponse aux trames ICMP sur les adresses de diffusion:

- Au niveau routeur
 - Au niveau machine
-

L'ingénierie sociale

- Il n'y a généralement pas d'attaques réussies sans relations humaines
 - basée sur quatre grands principes:
 - **Le contexte** (l'organigramme de l'entreprise)
 - **L'audace** ou le **bluff** (avoir connaissance et savoir parler)
 - **La chance**
 - **La patience calculée**
-

Réussite de l'attaque ingénierie sociale

- Les personnes ne sont pas formées à la notion de sécurité informatique
 - *Disquettes ou sauvegardes jetées à la poubelle*
 - *Papiers où l'on note ses mots de passe jetés à la poubelle*
-

DDOS

- Distributed Denial Of Service.
 - Type d 'attaque très à la mode.
 - L 'objectif est d 'écrouler une machine et/ou saturer la bande passante de la victime.
 - Nécessite plusieurs machines corrompues.
-

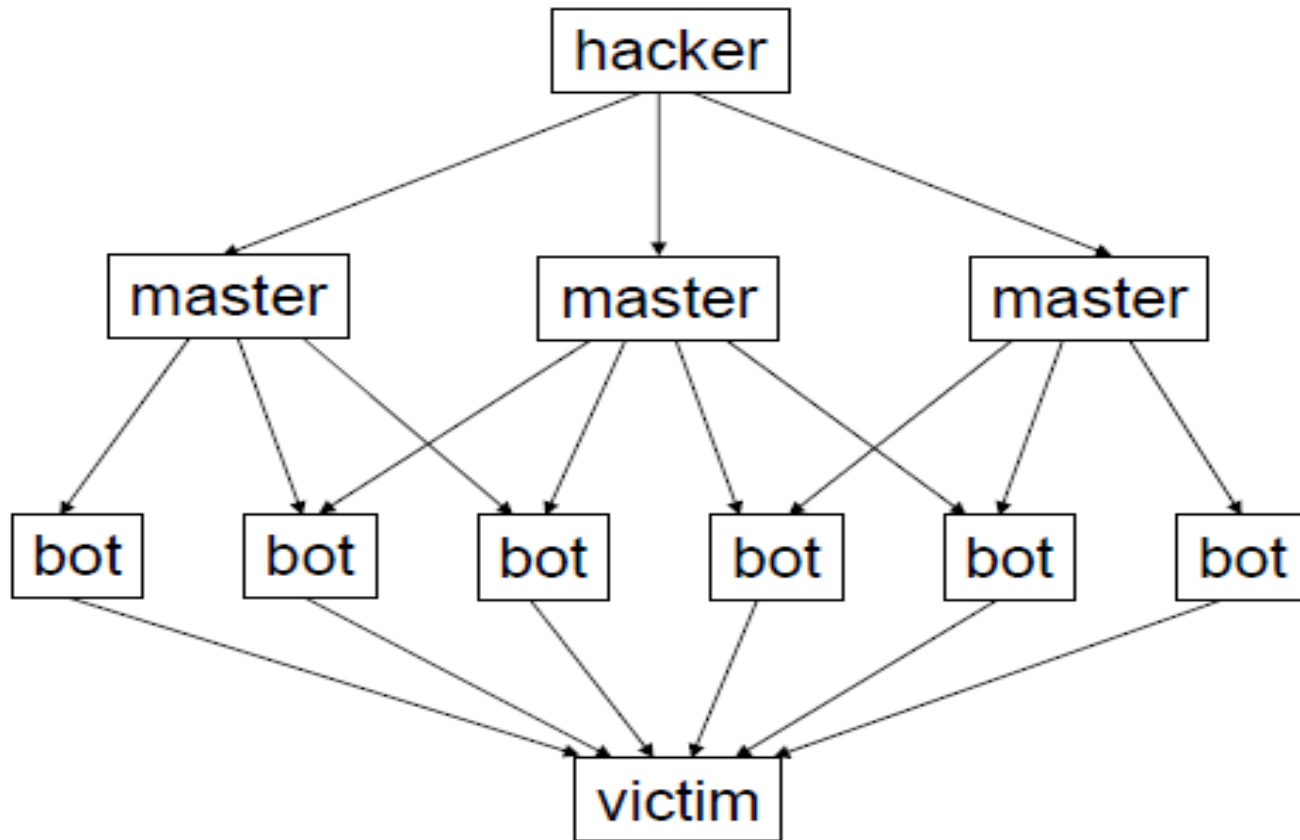
DDOS

Distributed Denial Of Service.

- Attaque popularisée le 14 février 2000 sur quelques sites .com renommés (ebay, cnn, amazon, microsoft, ...). Le coupable « Mafiaboy », 15 ans, est arrêté au Canada le 15 avril et condamné à 8 mois de détention. Il a causé des pertes estimées à 1,2 milliards de dollars en 24 heures.
-

DDOS

Distributed Denial Of Service.



DDOS

Exemples

- Tribe Flood Network (TFN)
- Trinoo
- TFN2K
- Trinity (utilise les serveurs irc)..etc

Se protéger contre DDOS:

- Être attentif aux ports ouverts
-

But d'une attaque DDOS

- Un botnet de 1000 machines peut saturer la bande passante d'une grande entreprise ($1000 * 128\text{Kb/s} = 128\text{ Mb/s}$).
 - Une entreprise peut acheter les services d'un « bot herders » pour attaquer un concurrent.
 - « Ddos extortion »: des pirates peuvent menacer des sites de commerce en ligne (Exemple: la société Canbet en Angleterre).
-

Les « botnets »

- Début des années 1990.
- Réseau de machines contrôlées par un « bot herder » ou « botmaster ».

Selon une estimation: une machine sur quatre fait partie d'un botnet, soit environ 154 millions de machines.

Les « botnets » (Utilisation)

- Envoyer du spam
- Vol d'informations sensibles (keylogger).
- Installer des spywares.
- **Paralyser un réseau en déni de services (ddos)**
- Installer un site web malicieux (phishing)
- Truquer les statistiques de sites webs.

— ...

L'homme du milieu ***man in the middle***

Ce type d'attaque vise à intercepter les communications entre deux parties (personne, ordinateur) sans que ni l'une, ni l'autre ne puisse s'en apercevoir.

DHCP ,ARP,ICMP,RIP,DNS,Proxy HTTP

Intrusion

Attaque :

- Découverte systématique d'informations.
- Tentative d'intrusion ou de déni de service.

Intrusion :

- Prise de contrôle totale ou partielle d'un système distant
-

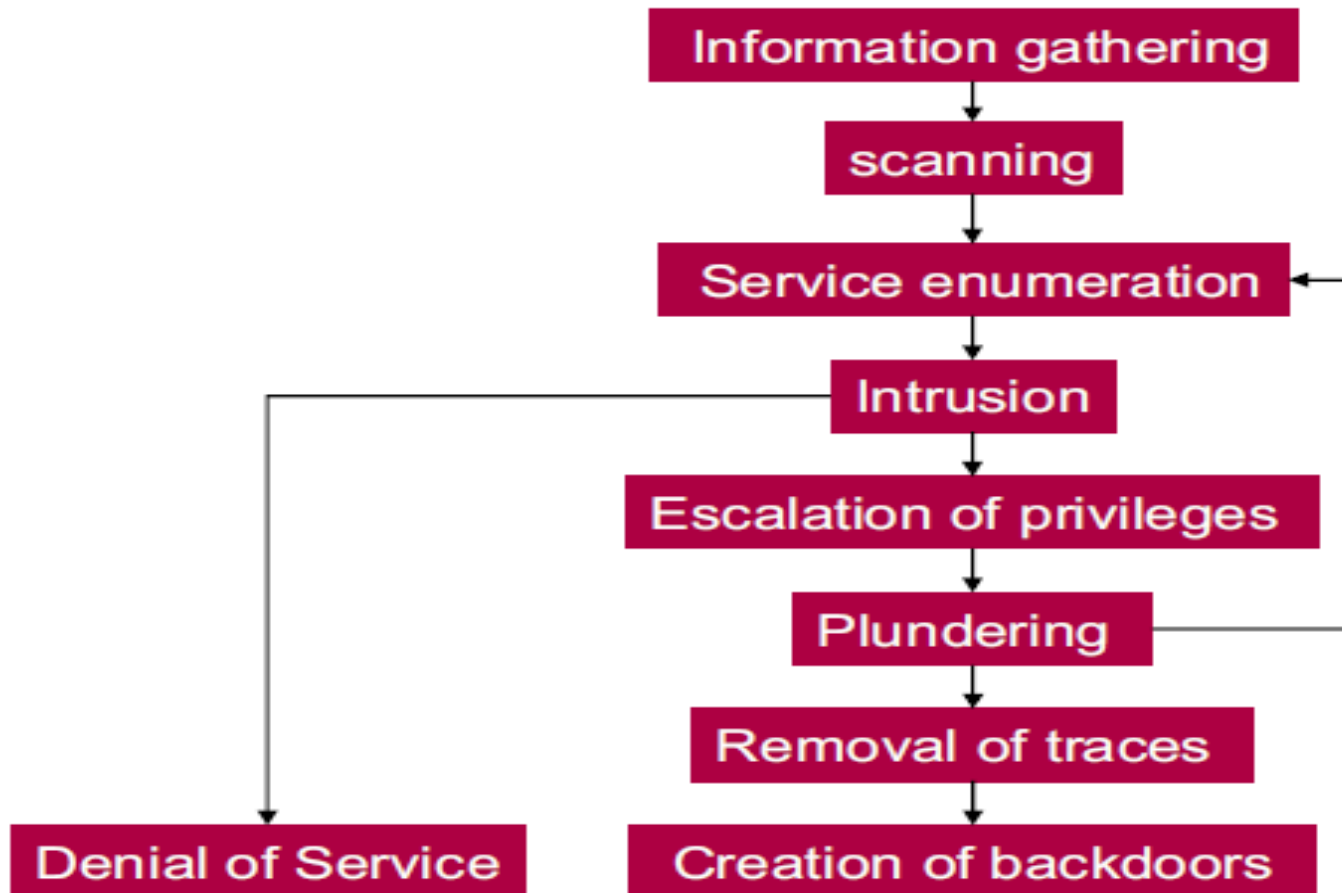
Intrusion

- la réalisation d'une menace (c 'est une attaque).
- Les conséquences peuvent être catastrophiques : vol, fraude, incident diplomatique, chantage...etc

Solution:

- Firewall et systèmes de détection d'intrusion
(étudier dans les prochaines parties)
-

La méthode des hackers



Collecte d'information

Utilitaires utilisés par les pirates pour préparer leurs attaques.

- Détermination des champs d'activités(site web): Téléphone, Implantation Emails, politique de sécurité, liens vers d'autres serveurs WEB, Code source HTML
 - Recensement des éléments du réseau (Identifier les noms de domaines et les réseaux associés d'une organisation: BDD INTERNIC, ARIN,...etc)
-

Collecte d'information

- Interrogation des serveurs DNS
(**outil**: nslookup www.google.fr)
 - Cartographie du réseau (Détermination de la topologie de chaque réseau : **traceroute**)
 - Utiliser aussi les techniques d'**Ingénierie sociale**
-

Balayage systématique

Scanner

Frapper contre tous les murs dans l'espoir de trouver les portes et les fenêtres du réseau cible.

- En connaissant les adresses IP, nous pouvons lancer un scan pour trouver des cibles intéressantes
- Le scanner va essayer de se connecter à tous les services voulu sur toutes les machines appartenant à une plage d'adresses
- **Résultat:** liste des machines accessibles, des ports ouverts sur ces machines (**Outil:** superscan)

Enumération des services

➤ Dans cette phase, il faut trouver des informations sur les services disponibles (TCP et UDP).

➤ Chercher aussi des:

Systemes d'exploitation

Fournisseur d'un logiciel

Version d'un logiciel (ou service)

Outils de scan : *nmap, strobe, udp_scan, netcat,*

Intrusion

- Par la recherche d'une vulnérabilité connue qui n'a pas encore été corrigé (patcher), nous pouvons pénétrer dans un système.
 - Des failles connues peuvent être trouvées sur des sites web: **securityfocus.com**, **secunia.com**
-

Suite des étapes

Escalation (extension) of privileges

- Chercher à augmenter ses privilèges
 - Par exemple l'installation d'un petit script que l'administrateur exécute par erreur .
 - Le pirate peut installer un sniffeur
-

Suite des étapes

Plundering

- Le vol de mots de passe.
- La recherche des informations, des documents ou des emails contenant des mots de passe

Suite des étapes

Effacer la trace

- Correction de logs avec des outils automatiques
- Dissimulation d'intrusion à l'aide de rootkits pour masquer la présence du hacker

Installation d'un backdoor

Conclusion

Après quelques minutes, n'importe qui est capable d'apprendre la manière de hacker votre site

Ce n'est pas parce que vous n'êtes pas connu que vous ne serez pas attaqué

Il faut donc:

- installer les correctifs de sécurité (patches) quand ils sont publiés
 - installer seulement les modules logiciels strictement nécessaires pour vos serveurs.
-

Conclusion

Lorsque les compétences au sein de l'entreprise ne sont pas suffisantes pour mener à bien cette opération, il convient de faire réaliser un audit par une société spécialisée dans la sécurité informatique.



Merci