

SÉCURITÉ ET CRYPTOGRAPHIE

A. EL HIBAOUI

Faculté des Sciences de Tétouan – Université Abdelmalek Essaâdi
Département Informatique

hibaoui.ens@gmail.com

Menaces de sécurité

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 système et généralement préjudiciables.

... Mais pourquoi attaquer ?

- Obtenir l'accès à un système
- Troubler le bon fonctionnement d'un service
- Voler des informations confidentielles
- Utiliser les ressources du système attaqué
- Utiliser le système attaqué comme rebond pour mener une attaque
- ...

Qui attaque ?

Un pirate

Un **pirate** désigne toute personne s'introduisant dans les systèmes informatiques

- **Black Hat Hackers** : Nuire au bon fonctionnement du système informatique.
- **White Hat Hackers** : Améliorer la sécurité des systèmes informatiques (conception de protocoles, outils, etc.)
- **Lamers ou crashers** : Utiliser des programmes dans le but de s'amuser.
- **Phreakers** : Pirates des réseaux téléphoniques commutés
- **Carders** : Pirates des cartes à puce.
- **Crackers** : Casser les protections des logiciels payants.
- **Les Hacktivistes** : de motivation idéologique

Types d'attaques

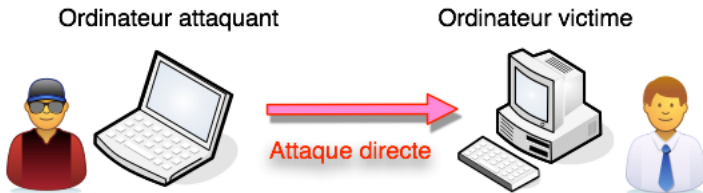
- 1 Attaques directes
- 2 Attaques indirectes par rebond
- 3 Attaques indirectes par réponse

Types d'attaques

Attaques directes

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.

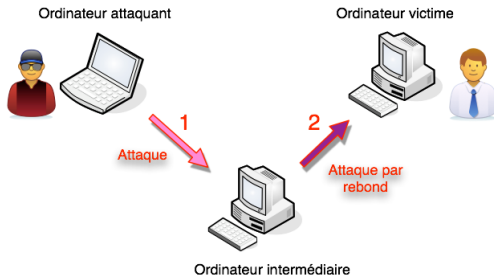


⇒ Facile de remonter à l'origine de l'attaque, identifiant par la même occasion l'identité de l'attaquant.

Types d'attaques

Attaques indirectes par rebond

Le pirate attaque la victime en attaquant une machine intermédiaire \Rightarrow cette attaque sera dirigée vers la victime.



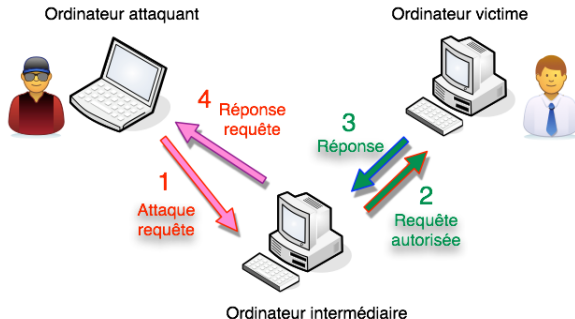
Ce qui implique :

- Une difficulté de remonter à l'origine de l'attaque (Masquer l'identité (l'adresse IP) du hacker)
- Utilisation des ressources de la machine intermédiaires (CPU, bande passante...) pour attaquer.

Types d'attaques

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.



⇒ C'est pas simple de remonter à la source.

Techniques d'attaques

Les attaques les plus répondues

- Attaque par dictionnaire ;
- Injection SQL ;
- Spoofing IP ;
- Denial of Service (DoS) ;
- Sniffing ;
- Bombe Logique ;
- Ingénierie sociale ;
- Cookies ;
- Instant Messaging ;
- Peer to Peer ;
- Phishing ;
- Keylogger ;
- SPAM ;
- Scanning ports ;
- Ping of Death (ping à la mort) ;
- Programme Auto-producteur (virus, ver)
- Programme simple (Chaveaux de troie, Espiogiciel)

Techniques d'attaques

- Attaques des mots de passe
 - ▶ Attaque par force brute
 - ▶ Attaque par dictionnaire
 - ▶ Attaque hybride
 - ▶ Enregistreur de touches
 - ▶ Ingénierie sociale
 - ▶ Espionnage
- Attaque Man In The Middel
 - ▶ Scanning
 - ▶ Spoofing
 - ▶ Routing
 - ▶ Sniffing
 - ▶ par rejeu
- Attaques par déni de service
 - ▶ par saturation
 - ▶ par réflexion
 - ▶ par ping de mort
 - ▶ par fragmentation
 - ▶ attaque LAND
 - ▶ attaque SYN
- Détournement d'une session TCP
 - ▶ Attaque de Mitnick

Attaques des mots de passe – Attaque par force brute

Attaque par force brute

L'outil utilisé pour mener cette attaque teste tous les mots de passe possibles

Test de solidité

Taille du mot de passe	Contenu du mot de passe	Nombre de possibilités
2	Lettres minuscules	$26^2 = 676$
3	Lettres minuscules	$26^3 = 17576$
4	Chiffres	$10^4 = 10000$
4	Minuscules+Majuscules+Chiffres	$(26 + 26 + 10)^4 = 14776336$

- Méthode sûre
- Mais trop lente si le mot de passe est long et contient des
- minuscules, des majuscules, des chiffres et des caractères spéciaux

Exemple

Attaque du mot de passe d'une session Windows.

- Net user : pour afficher la liste des utilisateurs
- Utilisation de l'utilitaire wlpc.exe : wlpc Legolas -b -l (Legolas est le nom de l'utilisateur)

Attaques des mots de passe – Attaque par dictionnaire

Attaque par dictionnaire

L'outil utilisé pour mener cette attaque teste tous les mots de passe d'un dictionnaire

Test de solidité

Nombre des mots du dictionnaire	Nombre de mots de passe maximal à tester
1000	1000
10000	10000
100000	100000

- Méthode non sûre : peut être le mot de passe n'est pas inclus dans le dictionnaire
- Rapide et dépend de la taille du dictionnaire

Exemple

Attaque du mot de passe d'une session Windows

- Net user : pour afficher la liste des utilisateurs
- Recherche ou génération d'un dictionnaire : pouvant contenir le mot de passe (Dans notre exemple, c'est le fichier [passwords.txt](#))
- Utilisation de l'utilitaire wlpc.exe : wlpc Legolas -w passords.txt

Attaques des mots de passe – Attaque hybride

Attaque hybride

- C'est une combinaison d'une attaque par force brute et d'une attaque par dictionnaire.
- Utilisé généralement pour obtenir des mots de passe tels que : admin001, rootadmin, etc.

Attaque par dictionnaire utilisant Burp suite

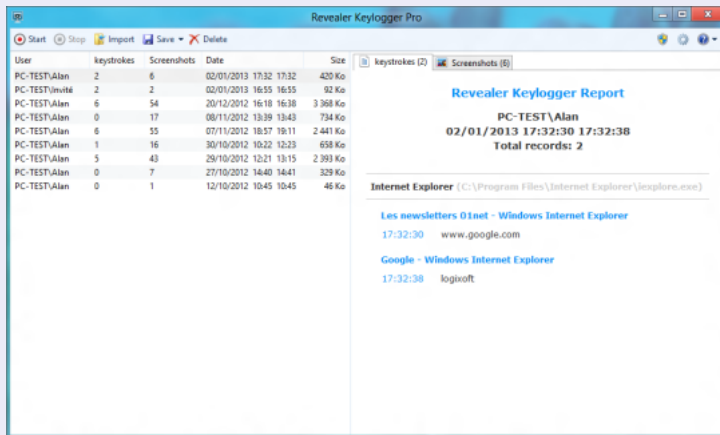
(voir vidéo)

Attaques des mots de passe – Enregistreur de touches

Enregistreur de touches (Keylogger)

Logiciel permettant d'enregistrer les frappes du clavier dans un fichier journal.

Exemple : Revealer keylogger



The screenshot displays the Revealer Keylogger Pro application window. It features a menu bar with options: Start, Stop, Import, Save, and Delete. Below the menu is a table with columns: User, keystrokes, Screenshots, Date, and Size. The table lists several entries for 'PC-TEST\Alan'. To the right of the table, there are tabs for 'keystrokes (2)' and 'Screenshots (6)'. Below the table, a 'Revealer Keylogger Report' is shown for the user 'PC-TEST\Alan' on '02/01/2013 17:32:30 17:32:38', indicating 'Total records: 2'. The report also lists recent activity for 'Internet Explorer' (C:\Program Files\Internet Explorer\iexplore.exe), including 'Les newsletters 01net - Windows Internet Explorer' and 'Google - Windows Internet Explorer'.

User	keystrokes	Screenshots	Date	Size
PC-TEST\Alan	2	6	02/01/2013 17:32 17:32	420 Ko
PC-TEST\invité	2	2	02/01/2013 16:55 16:55	92 Ko
PC-TEST\Alan	6	54	20/12/2012 16:18 16:38	3 368 Ko
PC-TEST\Alan	0	17	08/11/2012 13:39 13:43	734 Ko
PC-TEST\Alan	6	55	07/11/2012 18:57 19:11	2 441 Ko
PC-TEST\Alan	1	16	30/10/2012 10:22 12:23	658 Ko
PC-TEST\Alan	5	43	29/10/2012 12:21 13:15	2 393 Ko
PC-TEST\Alan	0	7	27/10/2012 14:40 14:41	329 Ko
PC-TEST\Alan	0	1	12/10/2012 10:45 10:45	46 Ko

Revealer Keylogger Report

PC-TEST\Alan
02/01/2013 17:32:30 17:32:38
Total records: 2

Internet Explorer (C:\Program Files\Internet Explorer\iexplore.exe)

Les newsletters 01net - Windows Internet Explorer
17:32:30 www.google.com

Google - Windows Internet Explorer
17:32:38 logixoft

Sous linux

Lancer le keylogger

```
sudo logkeys --start --keymap=~/.logkeys-master/keymaps/fr.map --output test.log
```

visualiser les touches capturées

```
sudo tail --follow test.log
```

Mettre fin au programme

```
sudo logkeys --kill
```

Attaques des mots de passe – Ingénierie sociale

Ingénierie sociale

- C'est une technique exploitant la naïveté de la victime.
- Une fois le pirate en possession d'un nombre de données qu'il juge satisfaisantes pour mener son attaque il passe à l'action.

Exemple

- Fouiller les poubelles.
- Voler le matériel ciblé ou des documents importants.
- Hameçonnage avec les fausses pages.

1- LE BON MOT DE PASSE



Attaques des mots de passe – Espionnage :

Espionnage

C'est une technique qui se base sur des renifleurs (sniffer) pour pouvoir trouver un information dans le trafic réseau

Exemple : Espionner une connexion ftp.

Lutte contre les attaques des mots de passe

Attaques	Solutions et recommandations
<ul style="list-style-type: none"> ● Par force brute ● Par dictionnaire ● Hybride 	<p>Éviter :</p> <ul style="list-style-type: none"> ● Identifiant, nom et Prénom ● Date de mariage ● Date de naissance ● un mot à l'envers ● Un mot de dictionnaire ● Exiger une taille minimale ● Utiliser des minuscules, majuscules, caractères spéciaux et des chiffres ● Utiliser des mots de passe multiples
<ul style="list-style-type: none"> ● Keyloggers 	<ul style="list-style-type: none"> ● Accéder à vos comptes sur votre machine seulement.
<ul style="list-style-type: none"> ● Ingénierie sociale 	<ul style="list-style-type: none"> ● Vérifier l'identité de la personne qui vous demande le mot de passe. ● En cas de Phishing, vérifier le lien de la fausse page et activer la protection contre le Phishing sur votre navigateur.
<ul style="list-style-type: none"> ● Espionnage 	<ul style="list-style-type: none"> ● Utiliser un antispyware. ● Utiliser des communication chiffrées.

Attaque Man In the Middel – Scanner

Scanner

Un scanner est un programme qui permet de scanner le réseau pour savoir quels ports sont ouverts sur les machines du réseau.

On utilise un scanner pour avoir une idée sur les machines du réseau local (nmap par exemple)



Man In The Middle



```
root@bt:~# nmap 192.168.0.0/24

Starting Nmap 6.01 ( http://nmap.org ) at 2013-02-25 21:56 WET
Nmap scan report for 192.168.0.1
Host is up (0.0089s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:76:CF:80 (VMware)

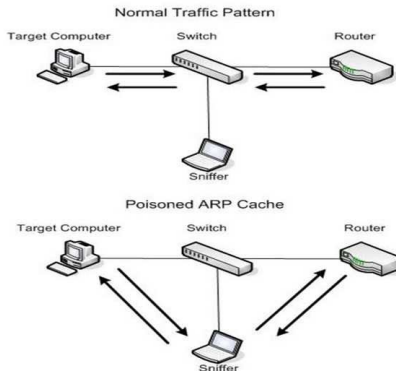
Nmap scan report for 192.168.0.2
Host is up (0.0085s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:32:B1:05 (VMware)
```

Attaque Man In the Middel – Spoofing

Spoofing

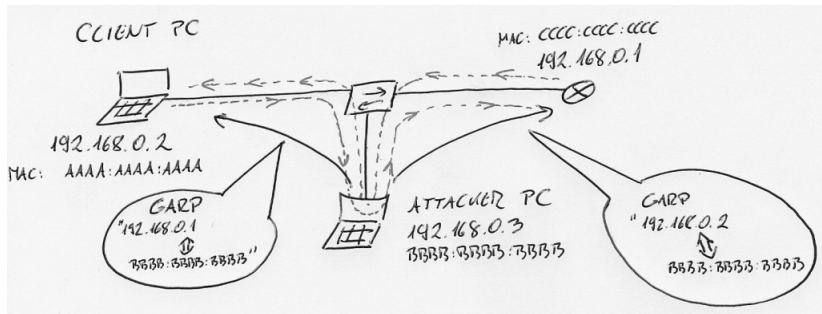
Usurpation d'identité (Technique ARP Spoofing ou ARP poisoning)

ARP Poisoning e ARP Spoofing



Attacker can send gratuitous ARP in which he is telling to some device in the network, let's say a PC that he is default gateway for this LAN. Attacker will be able to convince that PC that the attacker's MAC address is the MAC address of the PC's default gateway. The PC will start to send traffic to the attacker every time he needs to send something out of the LAN. The attacker will try to read packets but enable the communication of that PC with the internet. In this manner the attacker will not cause that the PC don't have a internet connection. The PC user will actually not notice the attack and the attacker will be free to capture the traffic and then forwards the traffic to the appropriate default gateway.

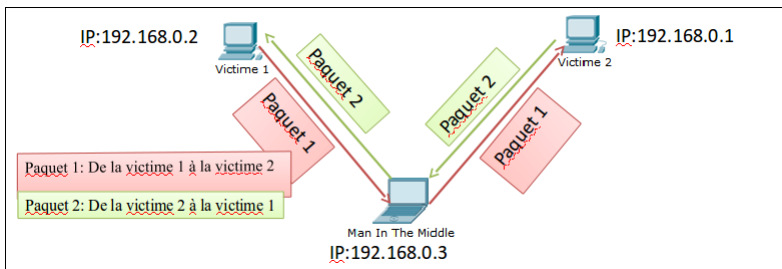
On the picture we have the default gateway with IP address 192.168.0.1. Attacker will sends GARP messages to PC1 with the information that the MAC address corresponding to 192.168.0.1 is on MAC address BBBB.BBBB.BBBB. And that is actually the attacker's MAC address. The attacker will send GARP messages to the default gateway to and he will convince the default gateway router that MAC address corresponding to PC1 is BBBB.BBBB.BBBB. This is called ARP cache poisoning. In this case ARP cache poisoning will enable that PC1 and Router1 can exchange traffic via the attacker's PC without notice it. This is why this type of ARP spoofing attack is considered to be a man in the middle attack.



Attaque Man In the Middel – Routing

Routing

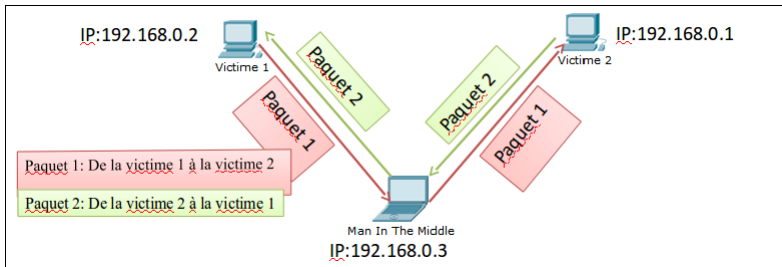
Configurer la machine du pirate comme routeur pour transférer les paquets provenant de la victime 1 à la victime 2 et vice versa.



Attaque Man In the Middel – Sniffing

Sniffing

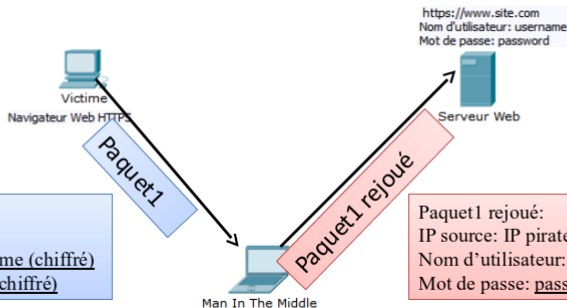
Utiliser un analyseur de paquets pour récupérer les informations importantes vis-à-vis du pirate (Wireshark , dsniff, etc)



Attaque Man In the Middel – Attaque par rejeu

Attaque par rejeu

C'est une attaque MITM dans laquelle le pirate reçoit un paquet d'authentification d'une machine (client = navigateur Web par exemple) et le transmet tel quel est au serveur Web afin de se connecter à ce dernier.



Paquet1:
IP source: IP victime
Nom d'utilisateur: username (chiffré)
Mot de passe: password (chiffré)

Paquet1 rejoué:
IP source: IP pirate
Nom d'utilisateur: username (chiffré)
Mot de passe: password (chiffré)

Attaques par déni de service

Définition

Ce sont des attaques qui rendent une machine ou un réseau indisponible (incapable de répondre aux requêtes)

Types

- **Par saturation** : Bombarder une machine des requêtes afin qu'elle soit incapable de répondre aux requêtes réelles.
- **Par exploitation de vulnérabilités** : Exploiter les failles du système de la Victime en lui envoyant des requêtes incompréhensibles afin de le rendre inutilisable et instable

Attaques par déni de service

Attaque par réflexion

Requête ICMP : (paquet spoofé)

- IP source : IP de la victime
- IP destination : IP du serveur

FIGURE – Add figure

Attaques par déni de service

Ping de la mort

C'est un paquet excédant la taille maximale d'un paquet normal

⇒ Si la pile TCP/IP est vulnérable, ce paquet provoquera un plantage.

Remarque : Aucune machine actuelle n'est vulnérable à ce type d'attaques.

Attaque par fragmentation (TearDrop)

C'est une attaque dont laquelle le on insère des information de décalage erronées dans un paquet fragmenté.

⇒ Des vides ou des recouvrements

Fragment 3	Fragment 1	Fragment 1	Fragment 4
------------	------------	------------	------------

⇒ Une instabilité du système

Fragment 1		Fragment 3	Fragment 4
------------	--	------------	------------

Attaques par déni de service

Attaque LAND

C'est une attaque qui utilise un paquet dont les champs d'adresses IP et de numéros de ports source et destination sont les mêmes.

⇒ Dans une machine vulnérable, ce paquet conduit à un état instable.

Remarque : Aucune machine actuelle n'est vulnérable à ce type d'attaques.

IP source	IP destination	Port source	Port destination	Données
10.0.0.1	10.0.0.1	80	80	GET ...

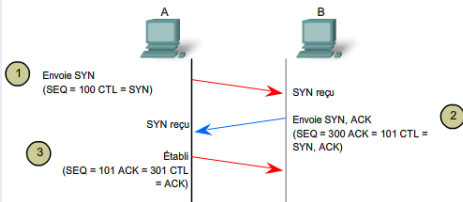
Attaques par déni de service

Attaque SYN

Etablissement d'une connexion TCP :

Principe de l'attaque

- Envoyer un nombre important de paquets SYN avec une adresse IP inexistante à une machine cible.
 - La machine cible essaie de répondre avec un SYN/ACK. Et puisque l'adresse est inexistante, elle ne recevra jamais la réponse ACK.
 - La machine cible met les requêtes de demande de connexions en attente dans sa mémoire tampon
 - Une fois la mémoire est saturée, toute autre demande de connexion sera rejetée.
- ⇒ La machine cible est hors service.



Les attaques de spoofing (usurpation d'adresse IP)

Schéma de l'IP spoofing :

L'IP spoofing est une technique utilisée dans plusieurs attaques telles que le vol ou le détournement d'une session TCP.

192.168.1.1



Client

192.168.1.1 : Autorisée
Autres machines : Bloquées



Serveur



Pirate

