Sécurité des réseaux

Alexandre Kervadec

***Résumé*—Notes du cours de sécurité des réseaux de A.Guermouche**

I. Les attaques

ON peut différencier une attaque d'une intrusion. Une attaque correspond à toute action compromettant la sécurité des informations. Une intrusion est la prise de contrôle partielle ou totale d'un système distant.

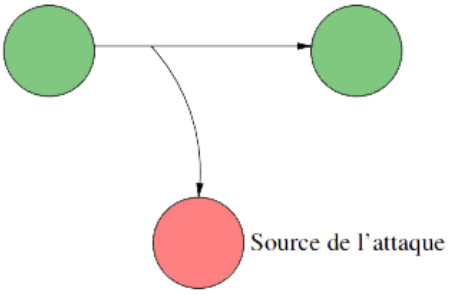
A. Description d'une attaque

- **Recherche d'informations :** réseau, serveurs, routeurs, ...
- **Recherche de vulnérabilités :** OS, serveurs applicatifs, ...
- **Tentative d'exploitation des vulnérabilités :** à distance puis localement
- **Installation de backdoor**
- **Installation de sniffer**
- **Suppression des traces**
- **Attaque par déni de service**

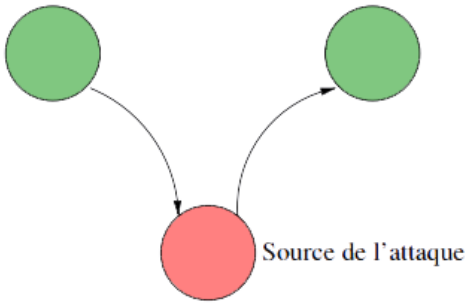
B. But des attaques

Interruption : vise la disponibilité des informations (DoS, ...).

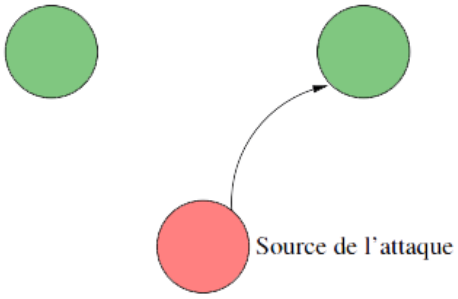
Interception : vise la confidentialité des informations (capture de contenu, analyse de traffic, ...).



Modification : vise l'intégrité des informations (modification, rejeu, ...).



Fabrication : vise l'authenticité des informations (mascarade, ...).



C. Technique de recherche d'information

- Recherche d'informations publiques : DNS, `whois`, ...
- Découverte du réseau et du filtrage IP : `traceroute`, `ping`, `hping`, `netcat`, ...
- Découverte des systèmes d'exploitation : `nessus`, `nmap`, `xprobe`, `queso`, ...
- Découverte de services ouverts : `nmap`, `udp-scan`, `nessus`, ...
- Découverte des versions logicielles : `telnet`, `netcat`, ...

D. Exemple : découverte des machines via DNS

Interrogation du DNS avec `dig` :

- serveur de mail (champ MX), serveur DNS (champ NS)
- résolution inverse sur toutes les adresses (*peu discret*) : `dig -x`
- transfert de zone (*pas toujours autorisé*) : `dig server axfr zone.`

Professeur : A.Guermouche

```
>dig labri.fr. MX
; <<>> DiG 9.4.1-P1 <<>> labri.fr. MX
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status:
NOERROR, id: 22464
...
;; QUESTION SECTION:
;labri.fr. IN MX
;; ANSWER SECTION:
labri.fr. 28800 IN MX 10 iona.labri.fr.
...
```

E. Balayage

1) Découverte de machines:
But : découvrir les machines d'un réseau donné.
Principe : envoyer un paquet à toutes les adresses et analyser le paquet retour.
Outils : `nmap`.

2) Découverte de ports ouverts:
But : découvrir les services/ports ouverts sur une machine donnée.
Principe : envoyer des paquets et analyser les paquet retour (ou leur absence).
Outils : `nmap`, `telnet`, `netcat`, ...

3) Techniques de balayage avec nmap:
ping sweep (balayage avec ping) : `nmap -sP -PI ...`
Principe : envoyer un paquet `ICMP Echo Request` et attendre le paquet `ICMP Echo Reply`.
Inconvénient : méthode très peu discrète.

Techniques plus sophistiquées : nécessite généralement des privilèges administrateur sur la machine source :
- *Half Open SYN scan* (un seul paquet SYN)
- *NULL scan* (paquet sans flags) (réponse uniqueent si le port correspondant est fermé)
- *FIN scan* (un seul paquet avec le flag FIN)
- *XMAS scan* (URG + PUSH + FIN)
- ...

4) Détection de ports ouverts:
scan TCP via HTTP *proxy bounce scan* : utiliser un proxy HTTP comme relai pour faire du scan de ports :
- `GET http://ftp.ens-lyon.fr:21 HTTP/1.0` et attendre la réponse

scan TCP via FTP *FTP Bounce attack* : utiliser un proxy FTP (ayant un disfonctionnement) comme relai pour faire du scan de ports :
- `PORT 10,10,0,2,0,25`
- `nmap -b ...`

scan UDP : `nmap -sU ...`
scan RPC : `nmap -sR ...`

F. Détermination du filtrage IP

Méthode :
- forger un paquet avec un *ttl* tel que le paquet soit arrêté par un filtre IP.
- Essayer d ecommuniquer avc un hôte situé derrière le firewall.
- Analyser les réponses.

Outils : firewalk, ...
Défense : Interdir aux réponses ICMP de sortir du réseau protégé, **etc**.

G. Prise de contrôle d'un serveur distant

En plusieurs étapes :

1) Recherche de services ouverts (SMTP, FTP, ...)
2) Exploitation de vulnérabilités : (CGI, exploit connu, débordement de buffer, injection de code/commande, ...)
3) Pose de sniffer
4) Pose de backdoor

Exemples de backdoor :
rwwwshell : lancer un client HTTP avec un shell associé sur une machine à l'intérieur du réseau et ouvrir une connexion HTTP vers un serveur du pirate.
loki : installer un serveur particulier sur une machine du réseau interne et communiquer avec lui en utilisant le champ données des paquets ICMP.

H. Attaques sur les réseaux locaux

Ecoute du réseau : capturer le contenu des paquets qui ne nous sont pas destinés :
- tcpdump
- sniff
- ...

Usurpation d'adresses (IP et MAC) : Forger et envoyer des paquets avec une fausse @IP :
- dsniff
- ...

Vol de session : Forger des paquets permettant la prise de contrôle d'une connexion déjà établie :
- juggernaut
- hunt
- ...

I. Usurpation d'adresses (Spoofing)

Le principe est de forger et envoyer des paquets IP avec une fausse adresse source. Il est donc impossible de trouver la véritable source.
C'est une technique souvent utilisée dans le cas d'attaque de type DoS [1].

1. Une attaque de type DoS vise l'interruption d'un service en saturant la cible de requêtes

J. Vol de session (Connection Hijacking)

L'objectif est de prendre la main sur une connexion déjà établie.

Principe :

- Attendre l'établissement d'une connexion
- Désynchroniser la connexion entre le client et le serveur (en forgeant un paquet avec un numéro de séquence particulier)
- Profiter de la désynchronisation pour faire faire au serveur ce que l'on veut

C'est une attaques très compliquée, voir impossible si l'on a pas la possibilité de voir le trafic entre le client et le serveur.

II. Quelques cas concrets

A. DNS : failles et dangers

Présentation de DNS

C'est un protocole proposé en 1983, qui n'a pas beaucoup évolué depuis.

C'est un mécanisme rapide et précis qui réalise la correspondance nom/@IP. DNS peut servir à plus que simplement renvoyer l'@IP d'un nom de domaine.

DNS est le deuxième plus ancien protocole *incontesté* dans ce qu'il fait [2], il ne reste que SMTP qui est dans le même cas. Il est donc universellement utilisé et largement déployé.

Fonctionnement

On distingue deux types de fonctionnement lors d'une requête DNS :

- Récursif : si le serveur interrogé ne connaît pas la réponse, il va lui-même lancer une requête vers un autre serveur pour obtenir la réponse, qu'il garde en cache (au maximum 1 semaine en moyenne)
- Itératif : si le serveur interrogé ne connaît pas la réponse, il va simplement indiquer quel serveur interroger au client

La grosse faille des serveurs DNS est le fait qu'ils utilisent majoritairement le même port (53), et qu'il devient donc facile de spammer le cache d'un serveur. Ceci peut par contre avoir des effets collatéraux [3].

Afin de patcher ce problème, il faudrait améliorer la randomisatin de numéro de requête (pour éviter le spamming), utiliser un port source aléatoire et à plus long terme, utiliser un protocole à signature électronique tel que DNSSec.

B. Honeypot

Le *honeypot* est une technique qui laisse volontairement une machine ou plus souvent une partie du réseau (complètement séparé du reste) afin que les attaquants ciblent plus ce dernier. Un honeypot à deux principaux buts :

- Augmenter la sécurité du réseau
- Récupérer des informations sur les méthodes des attaquants

Cependant, cette méthode est assez visible car un honeypot laisse une empreinte qui peut être repérée.

2. telnet a évolué vers ssh, FTP a été délaissé pour HTTP, ...
3. casser la hiérarchie DNS et donc faire tomber internet

III. IPSec

Le besoin de sécurité s'est fait ressentir vers 1994 [4] avec la recrudescence des attaques de type spoofing. IPSec apporte plusieurs applications :

- Sécuriser une connexion de succursale sur internet
- Accès distant sécurisé sur internet
- Authenticité des paquets reçus

De plus, IPSec a les avantages d'être utilisé uniquement sur des communications spécifiques [5], d'être au dessous de la couche de transport (TCP, UDP) ce qui lui permet d'être transparent aux applications, ainsi qu'aux utilisateurs [6].

	AH	ESP (chi)	ESP (chif. + auth.)
Ctrl d'accès	X	X	X
Intégr. hors co.	X		X
Auth. origine datas	X		X
Rejet paquets rejoués	X	X	X
Confidentialité		X	X
Confi. flot trafic		X	X

FIGURE 1. Services d'IPSec

Une association de sécurité [7] est une relation en sens unique entre un émetteur et un destinataire qui garantit les services de sécurité pour le trafic généré.

Des services de sécurité sont alloués à une AS pour utiliser AH ou ESP, mais pas les deux.

Une AS est définie par 3 paramètres :

- Index de paramètre de sécurité (IPS) : une chaîne binare assignée à cette AS et ayant une signification locale
- @IP de destination
- Identification du protocole de sécurité : indique si l'association est AH ou ESP

Plusieurs AS peuvent être combinées.

Les associations entre AS et type de trafic se font pas le biais d'une base de données de politique de sécurité (SPD [8]).

Il y a deux modes d'utilisation d'IPSec :

- Mode transport : sécurité au niveau de la couche transport, ESP chiffre (et optionnellement authentifie) uniquement l'information utile du paquet, AH authentifie l'information utile IP et des parties de l'en-tête
- Mode tunnel : sécurité du paquet tout entier, après l'ajout des champs AH ou ESP, le paquet entier est traité comme l'information utile du paquet IP externe. Au moins une extrémité de l'AS doit être une passerelle de sécurité [9]

4. RFC 1636
5. sans perturber les autres communications
6. une fois mis en place
7. AS
8. Security Policy Database
9. firewall, passerelle inplémentant IPSec, ...