Sécurité des réseaux

Alexandre Kervadec

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

I. Les attaques

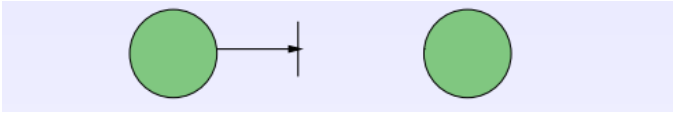
ON peut différencier une attaque d'une intrusion. Une attaque correspond à toute action compromettant la sécurité des informations. Une intrusion est la prise de contrôle partielle ou totale d'un système distant.

A. Description d'une attaque

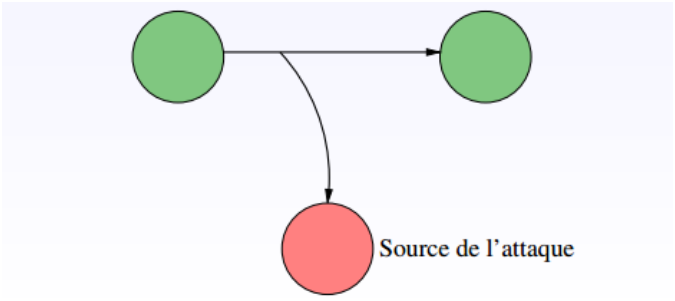
- **Recherche d'informations :** réseau, serveurs, routeurs, ...
- **Recherche de vulnérabilités :** OS, serveurs applicatifs, ...
- **Tentative d'exploitation des vulnérabilités :** à distance puis localement
- **Installation de backdoor**
- **Installation de sniffer**
- **Suppression des traces**
-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

B. But des attaques

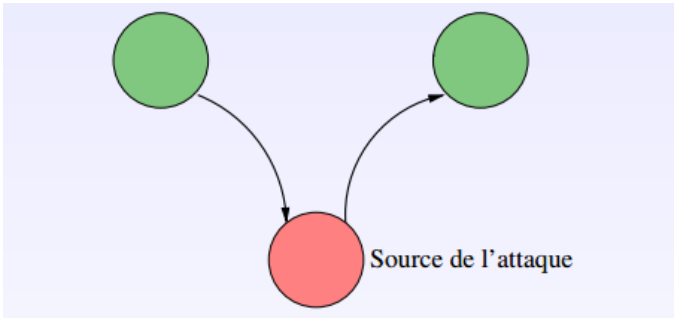
Interruption : vise la disponibilité des informations (DoS, ...).



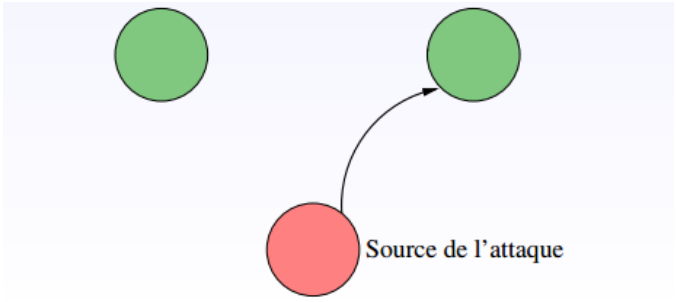
Interception : vise la confidentialité des informations (capture de contenu, analyse de traffic, ...).



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