Sécurité des réseaux

Alexandre Kervadec

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

I. Les attaques

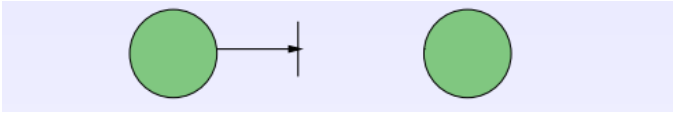
ON peut différencier une attaque d'une intrusion. Une attaque correspond à toute action compromettant la sécurité des informations. Une intrusion est la prise de contrôle partielle ou totale d'un système distant.

A. Description d'une attaque

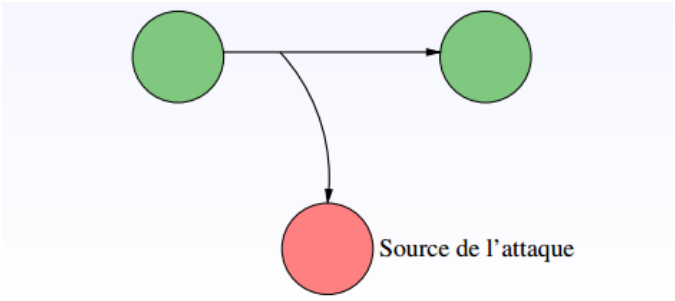
- **Recherche d'informations :** réseau, serveurs, routeurs, ...
- **Recherche de vulnérabilités :** OS, serveurs applicatifs, ...
- **Tentative d'exploitation des vulnérabilités :** à distance puis localement
- **Installation de backdoor**
- **Installation de sniffer**
- **Suppression des traces**
-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

B. But des attaques

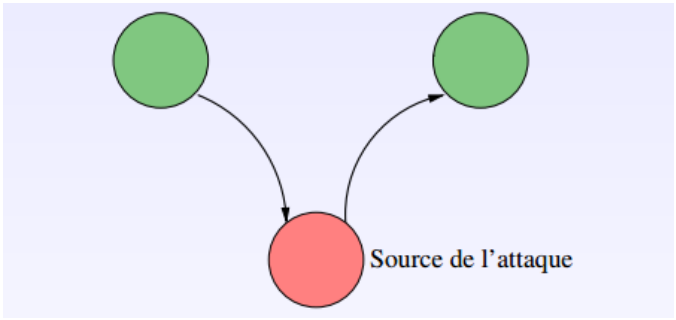
Interruption : vise la disponibilité des informations (DoS, ...).



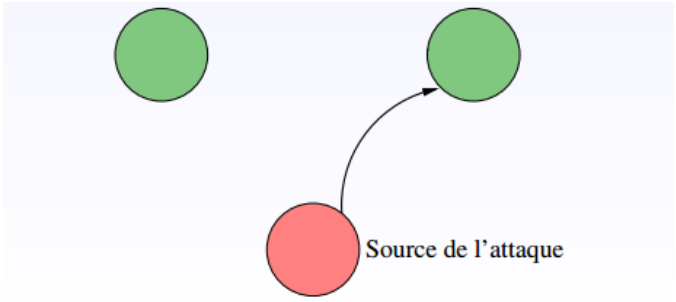
Interception : vise la confidentialité des informations (capture de contenu, analyse de traffic, ...).



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.
...
```