Sécurité des réseaux
Les attaques

A. Guermouche

Plan

1. Les attaques?

2. Quelques cas concrets
   - DNS : Failles & dangers

3. *honeypot*

Plan

Techniques d'attaque/d'intrusion

Attaque. n'importe quelle action qui compromet la sécurité des informations.

Intrusion. Prise de contrôle partielle ou totale d'un système distant.

Description d'une attaque :

Recherche d'informations. réseau, serveurs, routeurs, ...

Recherche de vulnérabilités. système d'exploitation, serveurs applicatifs, ...

Tentative d'exploitation des vulnérabilités. à distance puis localement

Installation de backdoor.

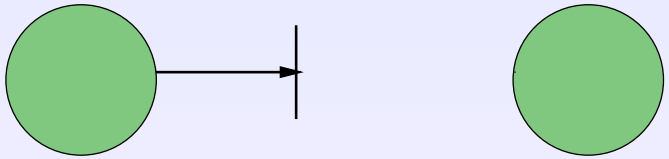
Installaltion de *sniffer*.

Suppression des traces.

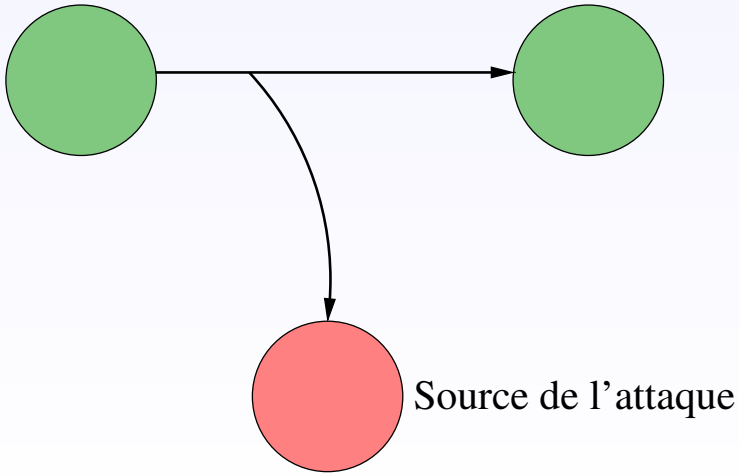
Attaque par déni de service.

Buts des attaques (1/2)

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

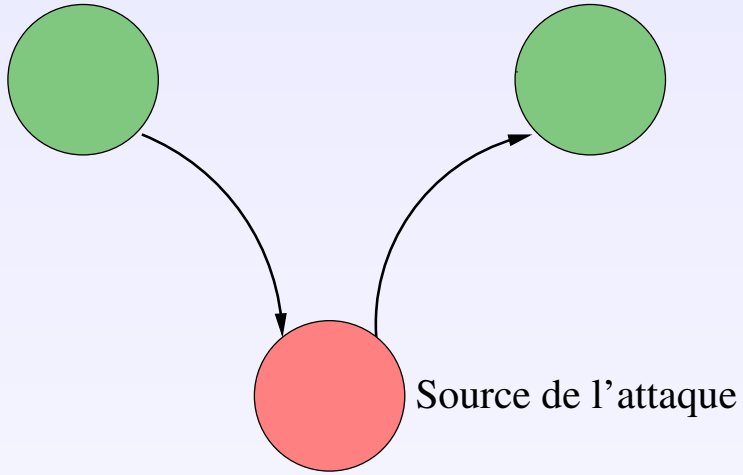


Interception. vise la confidentialité des informations (capture de contenu, analyse de traffic, . . .)

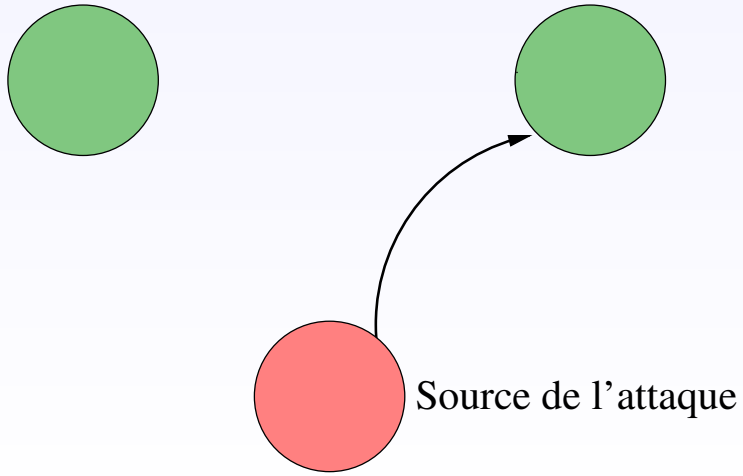


Buts des attaques (2/2)

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



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



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, ...

Exemple : Découverte de machines via DNS

Interrogation du DNS avec dig :

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

```
>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.
...
```

Balayage

Découverte de machines :

But.
- ⋆ découvrir les machines d'un réseau donné.

Principe.
- ⋆ envoyer un paquet à toutes les adresses.
- ⋆ analyser le paquet retour

Outils.
- ⋆ nmap
- ⋆ ...

Découverte de ports ouverts :

But.
- ⋆ découvrir les services/ports ouverts sur une machine donnée.

Principe.
- ⋆ envoyer des paquests.
- ⋆ analyser les paquet retour (ou leur absence)

Outils.
- ⋆ nmap
- ⋆ telnet
- ⋆ netcat
- ⋆ ...

Techinques 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 : nécessitent généralement des privilèges administrateur sur la machine source

- *Half Open SYN scan* (un seul paquet SYN)
- *NULL scan* (paquet sans flags) (réponse uniquement si le port correspondant est fermé)
- *FIN scan* (un seul paquet avec le flag FIN)
- *XMAS scan* (URG + PUSH + FIN)
- ...

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 ...`

Détermination du filtrage IP

Méthode :

- Forger un paquet avec un *ttl* tel que le paquet est arrêté par un filtre IP.
- Essayer de communiquer avec hôte situé derrière le firewall.
- Analyser les réponses.

Outils :

- firewalk, . . .

Défense :

- Interdir aux réponses ICMP de sortir du réseau protégé.
- ...

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.

Attaques sur les réseaux locaux

Écoute 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 adresse IP...

- dsniff
- ...

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

- juggernaut
- hunt
- ...

Usurpation d'adresses (spoofing)

Principe.

- Forger et envoyer des paquets IP avec une fausse adresse source.

Propriété.

- Impossibilité de trouver la véritable source.

Utilisation.

- Technique souvent utilisée dans le cas d'attaque de type DoS.
  Rappel : Une attaque de type DoS vise l'interruption d'un service en saturant la cible de requêtes.

Vol de session (*Connection Hijacking*)

Objectif.

- 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 qu'on veut.

Difficulté.

- Attaque très compliquée (voire impossible) si on n'a pas la possibilité de voir le traffic entre le client et le serveur.

Plan

Pourquoi DNS? (1/2)

DNS :

- Proposé en 1983, très peu d'évolution depuis.
- Mécanisme rapide, précis pour trouver la correspondance entre noms et adresse IP.
- Équivalent des services de renseignement téléphonique pour internet.
  - Service plus critique/sensible que les renseignements téléphoniques.
  - Une personne peut garder son numéro de téléphone pendant des années alors qu'un serveur peut changer d'adresse IP tous les jours.
  - Internet n'a pas de mécanisme d'envoi d'un echec ou une redirection (l'equivalent de *"le numéro que vous demandez n'est pas attribué, le nouveau numéro est ... "*).

Pourquoi DNS? (1/2)

Est-il possible que DNS fasse plus que renvoyer l'adresse IP à partir du nom?
Réponse Simple : Biensur, il peut renvoyer la liste des serveurs mail, des noms à partir d'adresses IP, ...
Meilleure réponse : Pourquoi cette question?

- ★ DNS est le deuxième plus ancien protocole *"incontesté"* dans ce qu'il fait.
  - ▸ Telnet a évolué vers ssh, FTP a été délaissé pour HTTP, ...
  - ▸ Il ne reste que SMTP dans le même cas.
- ★ Il est universellement utilisé et largement déployé.

Mécanismes pouvant poser problème

Proxy DNS. Si un serveur ne sait pas répondre à une requête, il va demander à quelqu'un qui sait (correspond à une recherche récursive).

Cache DNS. Si un serveur sert de proxy pour un autre, les résultats sont stockés (mis en cache) pour un certain temps (au plus une semaine pour la majorité des implémentation).

Route DNS. Si un serveur ne sait pas répondre à une requête et qu'il ne veut pas demander à quelqu'un qui connait la réponse, il peut donner une indication sur le serveur à contacter (correspond à une recherche itérative).

DNS *Cache Poisoning* (1/2)

Cache Poisoning : Attaque consistant à faire en sorte que le cache DNS contienne des correspondances invalides (c'est à dire que l'adresse IP n'est pas celle de la machine demandée mais une autre).

- Théoriquement possible mais attaque dure à mettre en œuvre (dure jusqu'à cet été).
- À l'été 2008, Dan Kaminsky, un chercheur en sécurité, a mis au point une attaque simple pour empoisoner les caches DNS.
- L'attaque se base sur un défaut de presque tous les serveurs DNS (à savoir le port source de la communication est toujours le même).

DNS *Cache Poisoning* (2/2)

Propriétés :

- ⋆ Chaque requête DNS est identifiée par un identifiant unique codé sur 16 bits (2^{16} possibilités).
- ⋆ Le port source est toujours le même sur presque toutes les implémentations de serveur DNS.

description :

1. Récupérer la liste des serveurs ayant l'authorité sur la zone visée.
2. Émettre une requête DNS pour une correspondance qui n'est pas dans le cache.
3. Envoyer plein de réponses *" spoofées"* (au plus 65536), chacune avec un numéro de requête différent, au serveur en se faisant passé pour le serveur d'authorité et en mettant dans la réponse une correspondance erronée.
4. Si l'opération réussit, le cache contient une entrée invalide.

Dangers et Solutions

Dangers :

- Peut tout simplement casser la hiéarchie DNS et donc faire tomber Internet.
- Le cache poisoning peut permettre de rediriger le traffic entre un serveur et un client vers un tier qui peut être malveillant.
- Beaucoup de protocoles, et notamment des protocoles de sécurité, sont sensibles aux résolutions DNS.

Solutions retenues :

- Améliorer la randomisation pour le choix du numéro de requête.
- Utiliser un port source aléatoire (ce qui ferait la taille de l'espace de recherche pour forger une réponse "valide" de 2^{16} à 2^{32}).
- À plus long terme, il faudrait utiliser un protocole à signature électronique tel que DNSSec.

Plan

Honeypot (1/2)

Un *honeypot* est une ressource de sécurité dont le principal

- ⋆ Tout le traffic vers le honeypot est authorisé.
- ⋆ Tout traffic initié par le honeypot est suspect (souvent dû au fait que le système a été compromis).

but est d'être attaqué.
deux types de *honeypot* :

Production. Il s'agît des logiciels classiques. Leur but est d'augmenté la sécurité de l'infrastructure.

Recherche. Il s'agît de mécanisme permettant de récuppérer de l'information sur les pirates et les attaques qu'ils utilisent.

Honeypot (2/2)

Avantages :

- Les informations récupérées à partir de honeypots ont de la valeur (personne d'autre qu'un pirate n'est censé se connecter dessus).
- Pas de problèmes de saturation de la ressource vu que la traffic dirigé vers le *honeypot* est très ciblé. (par opposition à conntrac par ex).
- Permettent de mettre en évidence de l'activité suspecte etc ...

Inconvénients :

- Vision étroite (on ne voit que ce qui est destiné au honeypot).
- Les honeypots laissent souvent une empreinte qui fait qu'on peut les reconnaître.
- On laissant une machine sans défense, le honeypot pause un problème en cas de compromission.