03 - Réseau — Sécurité

Gaétan Richard
gaetan.richard@info.unicaen.fr

DNR2I - M2

1. Filtrage

Pare-feu

Principe : Contrôle les communications passant par une machine.

Sous Linux : Utilisation du logiciel **iptables** qui permet de configurer le(s) module(s) Netfilter du noyau.

Autres OS : Principe similaire avec des utilitaires différents.

Filtrage

Type de trafic :

- Entrant (`INPUT`) ;
- Sortant (`OUTPUT`) ;
- En transit (`FORWARD`).

Effet :

- Accepter (`ACCEPT`) ;
- Refuser en envoyant un message (`REJECT`) ;
- Ignorer (`DROP`) ;
- Loguer (`LOG`).

Découverte d'iptables

```
# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Note : À faire également pour ipv6 (**ip6tables**).

Politique par défaut

Commande : `iptables -P INPUT DROP`

Résultat :

```
# iptables -L -n
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Règles

Principe : Il est possible d'ajouter des règles plus précises qui prennent le pas sur les politiques par défaut.

Exemple :

```
iptables -A INPUT -p TCP --dport domain -j ACCEPT
```

Résultat :

```
# iptables -L -n
Chain INPUT (policy DROP)
target  prot opt source     destination
ACCEPT  tcp  --  0.0.0.0/0  0.0.0.0/0    tcp dpt :53
...
```

Filtrage avancé

Il est possible de filtrer par :

- l'état de la connection
  `-m state --state NEW,RELATED,ESTABLISHED;`
- protocole utilisé `-p TCP`, `-p UDP`, `-p ICMP;`
- port d'origine / de destination `--sport dns`, `--dport 22;`
- interface utilisée en entrée / sortie `-i eth0`, `-o eth1;`
- adresse ip source / destination `-s 192.168.0.0/16`,
  `-d 10.3.1.134;`
- ...

En savoir plus : Consulter la manuel d'**iptables**.

NAT

Principe : Le NAT s'effectue sous linux à l'aide d'**iptables**.

Commande :

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Remarque : Ne pas oublier d'activer le "forward" ip sur la machine (ligne `net.ipv4.ip_forward = 1` dans */etc/sysctl.conf*).

Transfert de port

Principe : Rediriger le trafic entrant sur un port fixé vers une autre ordinateur.

Utilité : Permettre d'avoir un service accessible sur une machine avec un ip privée.

Commande : `iptables -t nat -A PREROUTING -p tcp -i eth0 -d xxx.xxx.xxx.xxx --dport 8888 -j DNAT --to 192.168.0.2 :80`

2. Les menaces

La sécurité

Principe : on parle souvent de chaîne de sécurité

Note : la sécurité d'un système informatique est déterminée par la résistance de son maillon le plus faible.

Menaces : Sur internet, de nombreuses menaces rôdent.

Principe

Méthode : Prendre physiquement possession de l'ordinateur.

Protections :

- Mettre les machines dans des pièces fermées ;
- Utiliser une protection au démarrage via le BIOS ;
- Crypter le disque.

Accidents

Exemples : Incendie, inondation, surtension, coupure de courant, …

Protections :

- *Prévention* ;
- Sauvegarde des données dans un site distant ;
- Plan de reprise d'activité.

Note : Dans ces cas, il est extrêmement important d'avoir une réflexion globale sur l'importance relative des différentes données et de choisir une politique adaptée.

DOS

Principe : Saturer (“faire tomber”) un serveur à l’aide de demandes complexes (potentiellement à l’aide d’un grand nombre de machines).

Protection :

- Mettre en place des systèmes de limitation de charge ;
- Augmenter la capacité des serveurs ;
- Faire le dos rond.

Note : Ce phénomène peut être causé par une trop grande réussite du service / mauvaise prévision (cf *geoportail.fr*, *france.fr*).

Principe

Méthode : Utiliser une faille dans un logiciel pour prendre le contrôle de la machine.

Protection :

- Maintenir les logiciel à jour ;
- Limiter les accès depuis l'extérieur.

Vulnérabilités

Type :

- Locale (nécessite un compte local) ;
- Élévation de privilège (permet d'outrepasser le système de droit) ;
- Distante (sur un service en écoute).

Les classiques :

- Dépassement de tampon (*buffer overflow*) ;
- Injection SQL ;
- CSS (*Cross Site Scripting*).

Surveillance : Publication sous forme de *CVE* (*Common Vulnerabilities and Exposures*), présence de patchs.

Virus / Cheval de Troie / Keylogger

Virus : Logiciel malveillant cherchant à se répliquer

Cheval de Troie : Logiciel ouvrant une “porte dérobée” (*backdoor*) sur la machine.

Keylogger : Enregistre les mots de passe tapés au clavier.

Entrée :

- De façon automatique (faille distante) ;
- En trompant l’utilisateur *XXX.jpg.exe* ;
- …

Principe

Méthode : Profiter de la faiblesse du maillon humain.

Important : L'utilisateur est un maillon de la chaîne de sécurité.

Prévention : Limiter les possibilité d'action de l'utilisateur pour s'en protéger et le protéger.

Fishing

Méthode : Envoie d'un mail plus ou moins alarmiste dans le but de récupérer les identifiants.

Protection :

- Former l'utilisateur ;
- Mettre en place un anti-spam

Attaques par dictionnaires

Méthode : Tentative d'intrusion dans le réseau de l'entreprise en "devinant" le login / mot de passe d'un utilisateur.

Prévention :

- Politique de mot de passe ;
- Formation des utilisateurs.

Social Engineering

Méthode : Demander les identifiants à l'aide d'informations

Protection :

- Former l'utilisateur.

Actes de malveillances

Méthode : rm -rf / après un licenciement.

Protection :

- Maintenir à jour les droits ;
- Restreindre au stricte nécessaire les droits.

”Oups …”

Méthode : *Je ne comprends pas depuis que j’ai renversé du café sur ma machine, elle ne démarre plus*.

Protection :

- Formation de l’utilisateur ;
- Sauvegarde.

3. Les solutions

Mieux vaut prévenir que guérir

Constat : C'est dans l'urgence qu'on fait le mieux des conneries.

Corollaire : Il vaut prévoir différents scénarios *catastrophes* et définir clairement :

- Des priorités ;
- Des actions à effectuer ;
- Des moyens d'agir.

Politique de protection des données

Politique : Une bonne politique doit déterminer :

- Où sont stockes les données ;
- Quelles sauvegardes sont faites (nombres / lieu / périodicité) ;
- Comment restaurer ces données ;
- Quelles sont les priorités.

CNIL : Tout cela avec l'accord de la CNIL bien sûr.

Politique de mot de passe

La politique de mot de passe sert :

- À imposer une certaine complexité sur les mots de passes ;
- à définir leur durée de validité ;
- …

Attention : Imposer des fortes contraintes ne garantit pas (loin s'en faut) d'avoir de bons mots de passe.

Politique de sécurité

Principe : De manière générale, il faut déterminer précisément :

- Qui a accès a quoi ;
- Quelles sont les autorisations ;
- Quoi faire des clefs usb ;
- Quoi faire des machines ;
- …

Surveillance

Principe : Chaque action donne lieu à une inscription dans des fichiers de logs.

Analyse : Il existe des logiciel qui analysent et envoient des alertes ou rapports (suivant la gravité) aux administrateurs.

Compromission

Si on découvre une intrusion dans le système :

- On isole la (ou les) machines compromises ;
- On analyse l'étendu du problème ;
- On réinstalle **from scratch** la (ou les) machine(s) infectée(s).
- On cherche à déterminer la cause de l'attaque.

Rappel : C'est dans l'urgence qu'on fait les plus belles conneries.