NMAP

inetdoc

Dans ce chapitre, nous allons décrire le fonctionnement des outils permettant de récupérer des informations à distance. Ces utilitaires sont fréquemment utilisés par les pirates pour préparer de futures attaques. C'est pour cette raison qu'il est indispensable de les décrire dès le début. Vous apprendrez également à les utiliser pour votre propre protection.

le scanner

L'objectif du pirate est de repérer les serveurs offrant des services particuliers et de les identifier. Pour obtenir ces informations, le pirate va utiliser un scanner . Le but de ce section est de présenter des méthodes de protections contre le scan (en utilisant des règles de firewalling sous iptables/ipchains par exemple) et de savoir utiliser un scanner pour anticiper les futures attaques. Le scanner décrit dans ce chapitre est nmap , un des scanners les plus utilisés et un des plus performants. nmap est disponible Linux en paquet dans toutes les distributions majeures. La version décrite dans ce chapitre étant celle disponible sous Linux. Je décrirai dans une première partie ce qu'est un scanner. Ensuite, je me focaliserai sur nmap et je le présenterai d'un point de vue un peu plus technique, permettant de comprendre les différentes méthodes de protection.

à noter que

pour une capacité optimale de fonctionnement, nmap doit être utilisé avec les droits du super-utilisateur root

ou son interface graphique nmapfe (gksu nmapfe)

qu'est ce qu'un scanner ?

C'est très simple : lorsqu'un serveur offre un service particulier (web, messagerie, mail), il exécute un programme assurant ce service. Ce programme est en attente de connexions. Les clients devant accéder à ce service doivent connaître l'adresse IP du serveur et le numéro de port associé au service. Ce numéro de port a été attribué suivant le document standard RFC1010 au programme exécutant ce service. Sur les systèmes Linux la liste de ces numéros est disponible dans le fichier `/etc/services`. La plupart des services ont un numéro de port bien défini. Par exemple, un serveur de messagerie utilise le port 25, un serveur web le port 80... Lorsqu'un service est en écoute sur un port, on dit que le numéro de port associé à ce service est ouvert.

L'intérêt du scanner est très simple : il permet de trouver dans un délai très court, tous les ports ouverts sur une machine distante. Il existe différents types de *scanner*, certains se contentent juste de donner : la liste des ports ouverts, le type et la version de l'OS tournant sur le serveur (ces fonctionnalités seront décrites dans ce chapitre avec nmap). D'autres scanners comme nessus permettent de tester différentes failles connues sur ces services.

exemple avec nmap

Utilisons nmap pour connaître les services en écoute sur la machine d'adresse IP `192.168.1.1` :

```
[root@nowhere.net /root]# nmap 192.168.1.1
Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on (192.168.1.1) :
(The 1544 ports scanned but not shown below are in state : closed)
Port State Service
21/tcp open ftp
53/tcp open domain
80/tcp open http
110/tcp open pop-3
111/tcp open sunrpc
113/tcp open auth
631/tcp open cups
845/tcp open unknown
901/tcp open samba-swat
10000/tcp open snet-sensor-mgmt
Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds.
```

Nmap donne un aperçu assez complet des différents services s'exécutant sur la machine dans un temps assez bref.

On peut observer ici que des serveurs FTP, DNS, WEB, POP-3 ... sont en attente de connexions.

comment marche nmap ?

Je présenterai de manière très succinte nmap et me focaliserai principalement sur les fonctions les plus utilisées.

Pour connaître les ports ouverts sur une machine, nmap procède à l'envoi de paquets sur tous les ports de cette machine et analyse les réponses. Bien sûr, il y a différents types de scans, donc différents types d'envois et donc, différents types de réponses.

Nous nous intéresserons aux scans utilisant le protocole TCP (les scans UDP et ICMP étant possibles eux aussi).

le scan *vanilla TCP connect*

Nmap procède à l'appel de la fonction connect() sur tous les ports de la machine. Ce type de scan est facilement repérable.

Le scan en *vanilla TCP connect* est le scan par défaut avec Nmap, la commande est :

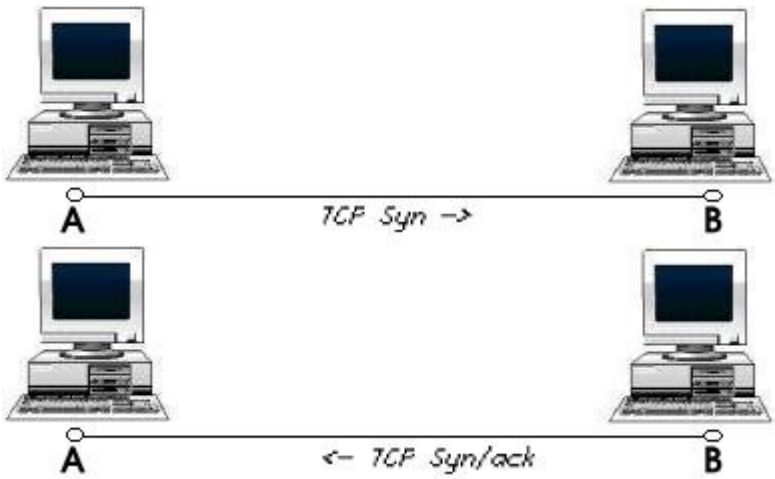
```
[root@nowhere.net /root]# nmap [ip de la machine cible]
  ou
[root@nowhere.net /root]# nmap -sT [ip de la machine cible]
```

les scans furtifs

Nous rentrons maintenant dans une classe de scans plus difficiles à détecter :

Le scan en connexion demi-ouverte ou "Syn-scan"

> Nmap envoie sur chaque port un paquet TCP avec le flag SYN armé ; si un port est ouvert, il renverra un paquet avec les flags SYN et ACK armés. Illustration :



> La commande se fait par l'appel de nmap avec l'option `-sS` :
>
> ```
> [root@nowhere.net /root]# nmap -sS [adresse IP de la machine cible]
> ```

Les scans Xmas, FIN et NULL

Le scan FIN consiste en l'envoi de paquets TCP avec seulement le flag FIN armé. La commande se fait par l'appel de nmap avec l'option `-sF` :

```
[root@nowhere.net /root]# nmap -sF [adresse IP de la machine cible]
```

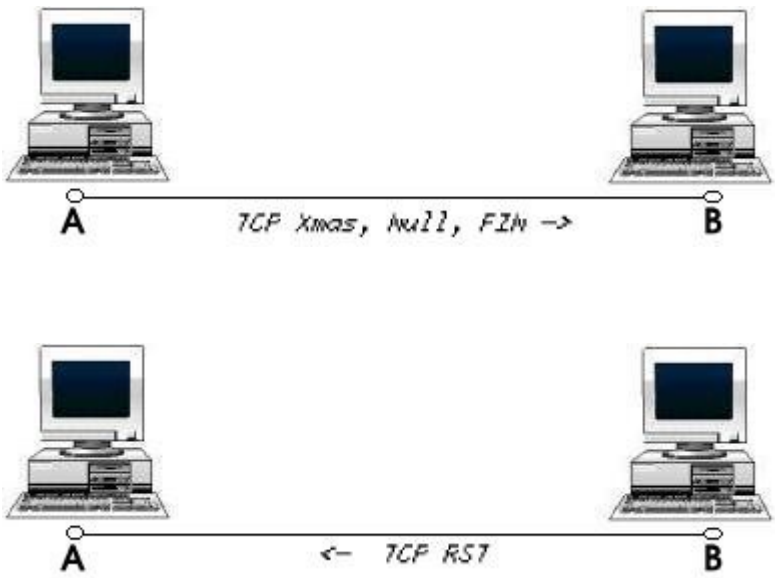
Le scan NULL consiste en l'envoi de paquets TCP avec seulement le flag NULL armé. La commande se fait par l'appel de nmap avec l'option `-sN` :

```
[root@nowhere.net /root]# nmap -sN [adresse IP de la machine cible]
```

Le Xmas scan (traduisez le scan de Noël) consiste en l'envoi de paquets TCP avec les flags FIN/URG/PUSH armés. La commande se fait par l'appel de nmap avec l'option `-sX` :

```
[root@nowhere.net /root]# nmap -sX [adresse IP de la machine cible]
```

Pour ces trois types de scans, les systèmes répondent avec un paquet RST si le port est fermé et ne répondent pas si le port est ouvert. Illustration :



la détermination du système d'exploitation avec Nmap

Si on lance nmap avec l'option -O :

```
[root@nowhere.net /root]# nmap -O 192.168.0.1
Starting nmap 3.48 ( http://www.insecure.org/nmap/ )
Interesting ports on (192.168.0.1):
(The 1647 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
113/tcp open  auth
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
515/tcp open  printer
587/tcp open  submission
901/tcp open  samba-swat
Device type: general purpose
Running: Linux 2.4.X ❶
OS details: Linux 2.4.20 - 2.4.21 w/grsecurity.org patch
Uptime 76.872 days (since Tue Sep  2 15:20:23 2003)
Nmap run completed -- 1 IP address (1 host up) scanned in 7.030 seconds
```

❶ Notez bien cette ligne : `Linux 2.4.X`.

Nmap parvient à déterminer le système d'exploitation tournant sur la machine cible. La machine cible utilise un noyau Linux 2.4.21-grsec. Nmap ne s'est pas trompé.

Il faut savoir que chaque système d'exploitation construit ses paquets d'une manière bien particulière. Certains champs au niveau de la couche IP ou TCP sont propres à chaque système d'exploitation. nmap contient une base de données d'un grand nombre de systèmes. nmap envoie donc des paquets tests à la machine cible et compare les paquets reçus en réponse à ceux de sa base de données et en déduit le type de système.

Cette base de données est mise à jour en fonction des différentes version de nmap.

quel est l'intêret d'utiliser nmap ?

nmap permet de pouvoir prévoir les futures attaques, et aussi de pouvoir connaître quels services tournent sur une machine. Une installation faite un peu trop vite peut laisser des services en écoute (donc des ports ouverts sans que cela ne soit nécessaire) et donc vulnérables à une attaque. N'hésitez pas à utiliser nmap contre vos serveurs pour savoir quels ports sont en écoute.

nmap est un logiciel très complet et très évolutif, et il est une référence dans le domaine du *scanning*.

comment s'en protéger ?

Configurer votre pare-feu pour empêcher les scans :

```
[root@nowhere /root]# iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit
--limit 1/s -j ACCEPT
```

Cette commande permet de détecter l'envoi un grand nombre de paquets TCP avec les flags FIN et/ou SYN et/ou ACK et/ou RST armé(s). Vérifiez que votre pare-feu (si ce n'est pas iptables) supporte la détection de scans.