TP test d’intrusion

Reconnaissance avec Nmap et utilisation de Metasploit

Olivier LASNE

2020-11-29

Introduction

Dans ce TP, nous allons voir comment utiliser Nmap pour découvrir services présents sur une machine, et récupérer leur version.

Nous verrons aussi comment vérifier si il existe un exploit pour la version utiliser, et comment exploiter une vulnérabilité avec le framework Metasploit.

Nmap

Nmap est un scanner réseau, il peut être utiliser à la fois pour découvrir les machines présentes sur un réseau, et pour lister les services (et leur version) d'une machine.

Nmap a de nombreuses options, nous ne les détaillerons pas toutes ici.

Scan basique

Si on lui donne une IP en paramètre, nmap va simplement effectuer un scan de port TCP, et lister les ports ouverts.

Exemple avec Metasploitable :

```
$ nmap 192.168.56.101

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-29 15:06 CET
Nmap scan report for 192.168.56.101
Host is up (0.00018s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
```

```
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

Découvrir les machines présentes sur un réseau

Ping scan

Pour découvrir rapidement les machines présentes sur le réseau, on peut faire simplement un ping scan :

```
nmap -sn 10.11.1.1-254
```

Top ports

Néanmoins, un certain nombre de machines sont configurés pour ne pas répondre aux ping. On peut choisir de scanner uniquement les ports les plus communs

```
nmap 10.11.1.1/24 -Pn --top-ports 10 --open -sS
```

-Pn : scan les ports même si la machine ne réponds pas aux pings.
--top-ports xx : scan uniquement les **xx** ports les plus communs.
--open : dans la sortie indique uniquement les ports ouverts.
-sS : **syn** scan, effectue seulement la 1ère partie du handshake TCP et est donc plus rapide. Peut-être également plus discret, mais est généralement détecté aujourd'hui.

Enregister les résultats

Nmap support 3 formats d'enregistrement

-oN : format texte classique. Identique à la sortie de la console.
-oG : *grepable nmap*, optimisé pour une recherche dans les résultats avec `grep`
-oX : format xml. Peut permettre de **reprendre un scan interrompu**, et l'importation des résultats dans certains outils comme **Metasploit**.

Scanner une machine

Une fois notre cible définie, on va généralement chercher à avoir le maximum d'information.

Options communes

Avant d'attaquer une machine, on va généralement effectuer un scan TCP complet avec les options suivantes :

```
1 nmap -sV -sC -O -p- 192.168.56.102 -oN full.nmap
```

-p- va indiquer que l'on liste absolument tous les ports
-sV indique que l'on veut récupérer les informations de version
-sC indique que l'on lance les *scripts nmap* de récupération d'information qui n'ont pas d'effet de bord
-O signifie que nmap va essayer de détecter la version du système d'exploitation présent en face.
-oN écrit les résultats dans le fichier `full.nmap`

On réalise généralement un 1er scan de port sans l'option **-p-** de façon à avoir uniquement les 1000 ports les plus fréquents. Et dans un second temps un scan avec tous les ports.

Scan UDP

Un scan UDP peut être (très) long. Néanmoins, il est généralement intéressant d'effectuer un scan au moins sur les ports les plus fréquents.

```
1 nmap -sU 192.168.56.102 -oN udp.nmap
```