Remise du rapport de test

1./ Résumer des commandes nmap utilisées

```
┌──(root💀kali)-[~]
└─# nmap 192.168.1.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 13:33 UTC
Nmap scan report for 192.168.1.254
Host is up (0.00059s latency).
All 1000 scanned ports on 192.168.1.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.14 seconds
```

1) nmap 192.168.1.254 :

Un scan des ports de la machine 192.168.1.254 est effectué avec cette commande.

```
┌──(root💀kali)-[~]
└─# nmap -O 192.168.1.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 13:34 UTC
Nmap scan report for 192.168.1.254
Host is up (0.00068s latency).
All 1000 scanned ports on 192.168.1.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.98 seconds
```

2) nmap –O 192.168.1.254 :

Cette commande permet de connaître le système d'exploitation de la machine 192.168.1.254.

```
┌──(root💀kali)-[~]
└─# nmap -sn 192.168.1.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 13:35 UTC
Nmap scan report for 192.168.1.254
Host is up (0.00067s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

3) nmap –sn 192.168.1.254 :

Ici nous avons utilisé cette commande afin de savoir si la cible est fonctionnelle, nous avons donc « Host is up ».

```
┌──(root💀kali)-[~]
└─# nmap -sV 192.168.1.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 13:35 UTC
Nmap scan report for 192.168.1.254
Host is up (0.00074s latency).
All 1000 scanned ports on 192.168.1.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.45 seconds
```

4) nmap –sV 192.168.1.254 :

Permet de prendre connaissance des versions des services via les ports ouverts.

```
┌──(root💀kali)-[~]
└─# nmap -A 192.168.1.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 13:36 UTC
Nmap scan report for 192.168.1.254
Host is up (0.00085s latency).
All 1000 scanned ports on 192.168.1.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.99 ms 192.168.1.254

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.40 seconds
```

5) nmap –A 192.168.1.254 :

Ici nous effectuons un check-up des ports les plus souvent mis en avant.

```
┌──(root💀kali)-[~]
└─# nmap -F 192.168.1.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 14:17 UTC
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.51 seconds
```

6) nmap –F 192.168.1.254 :

Procédure similaire mais simplifié et rapide.

```
┌──(root💀kali)-[~]
└─# nmap -v 192.168.1.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 14:19 UTC
Initiating ARP Ping Scan at 14:19
Scanning 192.168.1.254 [1 port]
Completed ARP Ping Scan at 14:19, 1.41s elapsed (1 total hosts)
Nmap scan report for 192.168.1.254 [host down]
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.47 seconds
           Raw packets sent: 2 (56B) | Rcvd: 0 (0B)
```

7) nmap –v 192.168.1.254 :

Cette fois-ci nous voulons une liste d'information plus détaillée.

```
┌──(root💀kali)-[~]
└─# nmap -sU 192.168.1.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 14:21 UTC
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.46 seconds
```

8) nmap –sU 192.168.1.254 :

Toujours une procédure de scan mais pour les protocoles UDP.

```
┌──(root💀kali)-[~]
└─# nmap -T5 192.168.1.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 14:24 UTC
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.48 seconds
```

9) nmap –Tx 192.168.1.254 :

La valeur x permet de préciser lors du scan le taux de requêtes de nmap.

```
┌──(root💀kali)-[~]
└─# nmap -p22 192.168.1.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 14:26 UTC
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.47 seconds
```

10) nmap –px 192.168.1.254 :

Dans ce cas présent p définit le mot port et x le numéro de celui-ci.

```
┌──(root💀kali)-[~]
└─# nmap -sS 192.168.1.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 14:33 UTC
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.47 seconds
```

11) nmap –sS 192.168.1.254 :

Cette commande synchronise ou établit une connexion TCP.

```
┌──(root💀kali)-[~]
└─# nmap -sf 192.168.1.254
Nmap 7.92 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
```

12) nmap –sf 192.168.1.254 :

Finalisations de la connexion TCP effectuer précédemment.

```
┌──(root💀kali)-[~]
└─# nmap -sN 192.168.1.254                                          255 ✕
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 14:37 UTC
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.47 seconds
```

13) nmap –sN 192.168.1.254 :

Trame TCP envoyé sans identifiant.

```
┌──(root💀kali)-[~]
└─# nmap -sX 192.168.1.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 14:39 UTC
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.47 seconds
```

14) nmap –sX 192.168.1.254 :

En cas d'attaque soudaine et rapide, une trame TCP est envoyé avec un niveau d'urgence élevé.

Toutes ces commandes permettent de cibler un domaine bien précis, pour les tester nous pouvons utiliser le domaine « scanme.nmap.org ». Ce domaine offre donc un exemple complet des utilisations de ces commande nmap. Pour expliquer et montrer l'exemple, les commandes ont été saisies sur Kali.

2./ Rapport sur les ports découverts avec et sans pare-feu.

Sans pare-feu :

Port Http : 80 Port SSH : 22

Port ftp : 21 Port telnet : 23

Avec pare-feu :

Avec le pare-feu activé la sécurité concernant le service des ports est sécurisé et donc leurs accès inaccessible.

3./ Conclusion sur les éléments à sécuriser.

Afin de sécuriser un maximum et de se protéger de toutes attaques éventuelles, il est important de veiller à activer toutes les défenses et sécurisations proposer par la pare-feu. Celui-ci évitera de donner des informations quelconques sur les ports les plus souvent utilisés et solliciter, comme le port http, le pot ssh, ect…

Nous avons remarqué grâce à Metasploitable que de nombreuses informations peuvent-être récupérer en peu de temps s'il y a un défaut de sécurisation.