Evan Valentin

Rapport de test : machine victime

1) Rédigez un rapport de test complet sur les capacités de sécurisation du pare-feu de Windows, réalisé à partir de vos observations sous nmap. Ces tests viseront la machine victime.

Phase 1 : pare-feu désactivé

- nmap 192.168.1.2

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-09 12:44 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 192.168.1.2
Host is up (0.00066s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:AB:CF:8B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
```

- nmap -O 192.168.1.2

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-09 12:43 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.2
Host is up (0.00052s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:AB:CF:8B (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 21H2
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.76 seconds
```

- nmap -F 192.168.1.2

```
┌──(kali㉿kali)-[~]
└─$ nmap -F 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-09 12:45 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 192.168.1.2
Host is up (0.00061s latency).
Not shown: 97 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:AB:CF:8B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
```

- nmap -T 2 192.168.1.2

```
┌──(kali㉿kali)-[~]
└─$ nmap -T 2 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-09 12:50 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 192.168.1.2
Host is up (0.00069s latency).
Not shown: 627 closed tcp ports (reset), 370 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:AB:CF:8B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 612.17 seconds
```

- nmap -sY 192.168.1.2

```
┌──(kali㉿kali)-[~]
└─$ nmap -sY 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-09 13:07 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
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 1.93 seconds
```

Phase 2 : pare-feu activé

- nmap 192.168.1.2

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-09 13:30 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 192.168.1.2
Host is up (0.00059s latency).
All 1000 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:AB:CF:8B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 26.46 seconds
```

- nmap -O 192.168.1.2

- nmap -F 192.168.1.2

```
┌──(kali㉿kali)-[~]
└─$ nmap -F 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-09 13:32 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 192.168.1.2
Host is up (0.00046s latency).
All 100 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
MAC Address: 08:00:27:AB:CF:8B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.29 seconds

mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 192.168.1.2
Host is up (0.00043s latency).
All 1000 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:AB:CF:8B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.60 seconds
```

- nmap -T 2 192.168.1.2

```
┌──(kali㉿kali)-[~]
└─$ nmap -T 2 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-09 13:35 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 192.168.1.2
Host is up (0.00063s latency).
All 1000 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:AB:CF:8B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 849.59 seconds
```

- nmap -sY 192.168.1.2

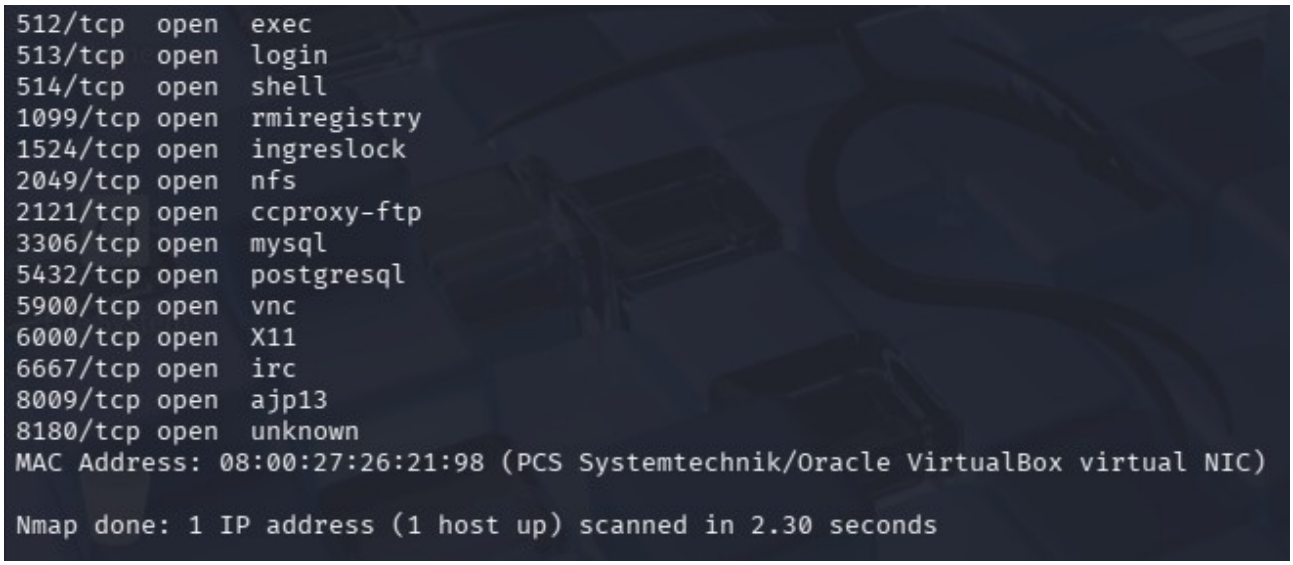
```
┌──(kali㉿kali)-[~]
└─$ nmap -sY 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-09 14:04 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 192.168.1.2
Host is up (0.00056s latency).
All 52 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 52 filtered sctp ports (no-response)
MAC Address: 08:00:27:AB:CF:8B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.43 seconds
```

Lorsque les pare-feux sont désactivés, les ports sont en état de service et 3 d'entre eux sont ouverts (msrpc ; netbios-ssn ; microsft-ds).

Mais lorsque les pare-feux sont désactivés, les ports ne sont plus visibles. Signifiant qu'ils ne sont plus ouverts.

2) A l'aide de nmap, rédigez une rapport permettant de définir la surface d'attaque du serveur victime



La surface d'attaque du serveur victime est « facile d'accès » : 23 ports tcp sont en état d'ouverture, en plus d'être visible par tout le monde.