Analysez les différents Scans avec Wireshark

Scan UDP

1. Scan avec nmap

Lancez un scan UDP avec nmap grâce à l'option -sU

```
root@kali:~# nmap 192.168.2.1 -sU

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-18 23:15 CEST
```

Le scan UDP pour nmap est particulier car il utilise des profils de scan pour chaque port différent, cela peut donc prendre un certain temps. Il faut donc scanner les ports classiques.

Coupez les scans UDP (Ctrl + C)

Scannez le port DNS à l'aide de l'option -p

```
root@kali:~# nmap 192.168.2.1 -sU -p 53
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-18 23:20 CEST
Nmap scan report for 192.168.2.1
Host is up (0.00011s latency).
PORT   STATE SERVICE
53/udp open  domain
MAC Address: 08:00:27:6B:25:CB (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.07 seconds
```

Le port 53 est ouvert cela indique qu'il y a un service DNS.

Avec l'option -p il est possible de préciser une plage de ports.

```
nmap 192.168.2.1 -sU -p 1-100
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-18 23:25 CEST
Nmap scan report for 192.168.2.1
Host is up (0.00050s latency).
Not shown: 97 closed ports
PORT   STATE         SERVICE
53/udp open          domain
68/udp open|filtered dhcpc
69/udp open|filtered tftp
MAC Address: 08:00:27:6B:25:CB (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 114.75 seconds
```

Il est aussi possible de scanner sur une plage réseau.

```
nmap 192.168.2.1-254 -sU -p 53
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-18 23:28 CEST
Nmap scan report for 192.168.2.1
Host is up (0.00080s latency).
PORT   STATE SERVICE
53/udp open  domain
MAC Address: 08:00:27:6B:25:CB (Cadmus Computer Systems)

Nmap scan report for 192.168.2.10
Host is up (0.00024s latency).
PORT   STATE  SERVICE
53/udp closed domain
MAC Address: 08:00:27:FC:11:32 (Cadmus Computer Systems)

Nmap scan report for 192.168.2.5
Host is up (0.000032s latency).
PORT   STATE  SERVICE
53/udp closed domain

Nmap done: 254 IP addresses (3 hosts up) scanned in 27.98 seconds
```

Optimisation

Il est aussi possible de scanner seulement les ip obtenues dans les fichiers avec l'optimisation des outils lors de la phase de découverte.

```
nmap -iL ipliste.txt -sU -p 53
```

```
Nmap scan report for 192.168.2.1
Host is up (0.000089s latency).
PORT   STATE SERVICE
53/udp open  domain
MAC Address: 08:00:27:6B:25:CB (Cadmus Computer Systems)

Nmap scan report for 192.168.2.10
Host is up (0.00014s latency).
PORT   STATE  SERVICE
53/udp closed domain
MAC Address: 08:00:27:FC:11:32 (Cadmus Computer Systems)

Nmap done: 5 IP addresses (5 hosts up) scanned in 39.06 seconds
```

2. Scan avec metasploit

Lancez Metasploit.

```
msfconsole
```

Chargez le module udp_sweep

```
use auxiliary/scanner/discovery/udp_sweep
```

Listez les options

```
msf auxiliary(udp_sweep) > show options
```

```
Module options (auxiliary/scanner/discovery/udp_sweep):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe in each set
   RHOSTS                      yes       The target address range or CIDR identifier
   THREADS    10               yes       The number of concurrent threads
```

Il faut donc modifier la cible à scanner avec le champ RHOSTS

```
msf auxiliary(udp_sweep) > set rhosts 192.168.2.1
rhosts => 192.168.2.1
```

Vérifiez le changement

```
msf auxiliary(udp_sweep) > show options

Module options (auxiliary/scanner/discovery/udp_sweep):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe in each set
   RHOSTS     192.168.2.1      yes       The target address range or CIDR identifier
   THREADS    10               yes       The number of concurrent threads
```

Lancez le scan

```
msf auxiliary(udp_sweep) > run
```

```
[*] Sending 13 probes to 192.168.2.1->192.168.2.1 (1 hosts)
[*] Discovered NetBIOS on 192.168.2.1:137 (METASPLOITABLE:<00>:U :METASPLOITABLE:<03>:U :METASPLOITABLE:<20>:U :
WORKGROUP:<00>:G :WORKGROUP:<1e>:G :00:00:00:00:00:00)
[*] Discovered DNS on 192.168.2.1:53 (BIND 9.4.2)
[*] Discovered Portmap on 192.168.2.1:111 (100000 v2 TCP(111), 100000 v2 UDP(111), 100024 v1 UDP(44915), 100024
v1 TCP(39262), 100003 v2 UDP(2049), 100003 v3 UDP(2049), 100003 v4 UDP(2049), 100021 v1 UDP(53887), 100021 v3 UD
P(53887), 100021 v4 UDP(53887), 100003 v2 TCP(2049), 100003 v3 TCP(2049), 100003 v4 TCP(2049), 100021 v1 TCP(380
52), 100021 v3 TCP(38052), 100021 v4 TCP(38052), 100005 v1 UDP(44809), 100005 v1 TCP(44586), 100005 v2 UDP(44809
), 100005 v2 TCP(44586), 100005 v3 UDP(44809), 100005 v3 TCP(44586))
[*] Scanned 1 of 1 hosts (100% complete)
```

```
msf auxiliary(udp_sweep) > set rhosts 192.168.2.1-10
rhosts => 192.168.2.1-10
```

Il est possible de préciser une plage ip dans le champ RHOSTS

```
[*] Sending 13 probes to 192.168.2.1->192.168.2.10 (10 hosts)
[*] Discovered NetBIOS on 192.168.2.1:137 (METASPLOITABLE:<00>:U :METASPLOITABLE:<03>:U :METASPLOITABLE:<20>:U :
WORKGROUP:<00>:G :WORKGROUP:<1e>:G :00:00:00:00:00:00)
[*] Discovered DNS on 192.168.2.1:53 (BIND 9.4.2)
[*] Discovered Portmap on 192.168.2.1:111 (100000 v2 TCP(111), 100000 v2 UDP(111), 100024 v1 UDP(44915), 100024
v1 TCP(39262), 100003 v2 UDP(2049), 100003 v3 UDP(2049), 100003 v4 UDP(2049), 100021 v1 UDP(53887), 100021 v3 UD
P(53887), 100021 v4 UDP(53887), 100003 v2 TCP(2049), 100003 v3 TCP(2049), 100003 v4 TCP(2049), 100021 v1 TCP(380
52), 100021 v3 TCP(38052), 100021 v4 TCP(38052), 100005 v1 UDP(44809), 100005 v1 TCP(44586), 100005 v2 UDP(44809
), 100005 v2 TCP(44586), 100005 v3 UDP(44809), 100005 v3 TCP(44586))
[*] Discovered NetBIOS on 192.168.2.10:137 (FORMATION:<00>:U :WORKGROUP:<00>:G :FORMATION:<20>:U :WORKGROUP:<1e>
:G :WORKGROUP:<1d>:U :[illegible] MSBROWSE__[illegible]<01>:G :08:00:27:fc:11:32)
[*] Discovered SNMP on 192.168.2.10:161 (Hardware: x86 Family 6 Model 60 Stepping 3 AT/AT COMPATIBLE - Software:
 Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free))
[*] Discovered NTP on 192.168.2.10:123 (Microsoft NTP)
[*] Scanned 10 of 10 hosts (100% complete)
```

Scan TCP SYN

1.Nmap

Pour lancer un scan TCP – SYN avec nmap rajoutez la fonction -sS

```
nmap -sS 192.168.2.1
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-19 20:43 CEST
Nmap scan report for 192.168.2.1
Host is up (0.000064s 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
MAC Address: 08:00:27:6B:25:CB (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

Pour scannez des ports précis, il faut utiliser l'option -p

```
nmap -sS 192.168.2.1 -p 21,80,443
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-19 20:45 CEST
Nmap scan report for 192.168.2.1
Host is up (0.00042s latency).
PORT    STATE  SERVICE
21/tcp  open   ftp
80/tcp  open   http
443/tcp closed https
MAC Address: 08:00:27:6B:25:CB (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.04 seconds
```

Il est aussi possible de scanner une plage de port.

```
nmap -sS 192.168.2.1 -p 1-100
```

```
Nmap scan report for 192.168.2.1
Host is up (0.000063s latency).
Not shown: 94 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
MAC Address: 08:00:27:6B:25:CB (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
```

Scannez l'intégralité des ports TCP

```
nmap -sS 192.168.2.1 -p 0-65535
```

2.hping3

Lancez hping3 avec l'option –scan pour scanner un port de la machine cible et -S pour SYN.

```
hping3 192.168.2.1 --scan 80 -S
```

```
Scanning 192.168.2.1 (192.168.2.1), port 80
1 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   80 http       : .S..A...  64     0  5840    46
All replies received. Done.
Not responding ports:
```

On remarque que la réponse porte le flag SYN+ACK, le SYN a donc aboutit.

Scannez plusieurs port précis :

```
hping3 192.168.2.1 --scan 21,80,443 -S -V
```

```
3 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   21 ftp         : .S..A...  64     0  5840    46
   80 http        : .S..A...  64     0  5840    46
  443 https       : ..R.A...  64     0     0    46
All replies received. Done.
```

https envoie les flags ACK + RST , il est donc fermé.

Scannez une plage de port :

```
hping3 192.168.2.1 --scan 0-100 -S
```

```
Scanning 192.168.2.1 (192.168.2.1), port 0-100
101 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   21 ftp         : .S..A...  64     0  5840    46
   22 ssh         : .S..A...  64     0  5840    46
   23 telnet      : .S..A...  64     0  5840    46
   25 smtp        : .S..A...  64     0  5840    46
   80 http        : .S..A...  64     0  5840    46
   53 domain      : .S..A...  64     0  5840    46
All replies received. Done.
```

Scan TCP three-way handshake (TCP Connect)

1.Nmap

Lancez un scan TCP connect avec nmap grâce à l'option -sT sur le port 80

```
root@kali:~# nmap -sT 192.168.2.1 -p 80
```

Lancez un scan sur des ports précis et un second sur une plage de ports.

2. Dmitry

Lancez un scan avec dmitry

```
dmitry -p 192.168.2.1
```