SCANNER UN RESEAU AVEC NMAP

L'objectif de ce TP est de scanner votre réseau et de voir les appareils qui y sont connectés, les adresses IP et les ports et services utilisés.

1 Taper la commande ***nmap -- help***

2 Taper la commande ***ifconfig***

Quelle est votre adresse IP privée ? Quelle est votre adresse masque ?

Inet 192.168.1.16 netmask 255.255.255.0

3 Taper la commande : ***nmap adresse ip du réseau***

root@Ubuntu:/home/chris# **nmap 192.168.1.0/24**

Starting Nmap 7.80 (https://nmap.org) at 2021-06-08 11:15 CEST
Nmap scan report for lan.home (192.168.1.1)
Host is up (0.0037s latency).
Not shown: 992 filtered ports
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
113/tcp closed ident
135/tcp closed msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
631/tcp open ipp
MAC Address: 78:B2:13:13:8B:D6 (DWnet Technologies(Suzhou))

Nmap scan report for chromecast.home (192.168.1.10)
Host is up (0.0083s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
8008/tcp open http
8009/tcp open ajp13
8443/tcp open https-alt
9000/tcp open cslistener
10001/tcp open scp-config
MAC Address: 88:3D:24:0E:B6:70 (Google)
Nmap scan report for android.home (192.168.1.11)
Host is up (0.0075s latency).
All 1000 scanned ports on android.home (192.168.1.11) are closed
MAC Address: 38:78:62:7A:F9:11 (Sony Mobile Communications)

```
Nmap scan report for chromecast.home (192.168.1.12)
Host is up (0.011s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
8008/tcp open  http
8009/tcp open  ajp13
8443/tcp open  https-alt
9000/tcp open  cslistener
9080/tcp open  glrpc
MAC Address: 64:E0:03:5B:A0:E9 (Unknown)
Nmap scan report for laptop-kb6k56pq.home (192.168.1.15)
Host is up (0.11s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
7070/tcp open  realserver
MAC Address: F8:E4:E3:82:57:35 (Unknown)

Nmap scan report for amandinechambre.home (192.168.1.17)
Host is up (0.015s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
7070/tcp open  realserver
MAC Address: D0:37:45:20:67:0E (Tp-link Technologies)
Nmap scan report for ubuntu.home (192.168.1.16)
Host is up (0.000016s latency).
All 1000 scanned ports on ubuntu.home (192.168.1.16) are closed
```

4 Nmap done: 256 IP addresses (6 hosts up) scanned in 7.64 seconds

a Quelles sont les machines connectées à votre réseau ?

```
chris@Ubuntu:~$ nmap -sP 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-08 11:44 CEST
Nmap scan report for lan.home (192.168.1.1)
Host is up (0.0069s latency).
Nmap scan report for chromecast.home (192.168.1.10)
Host is up (0.015s latency).
Nmap scan report for android.home (192.168.1.11)
Host is up (0.067s latency).
Nmap scan report for chromecast.home (192.168.1.12
Host is up (0.071s latency).
Nmap scan report for ubuntu.home (192.168.1.16)
Host is up (0.00027s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 3.19 seconds
```

Quel est le statut des ports ?

Open, ou closed, tout dépend des ports ou de la machine

Quelle est l'adresse MAC de la machine ?

MAC Address: 88:3D:24:0E:B6:70 (Google)

a Taper la commande nmap -0 adresse ip d'une machine

Nmap scan report for chromecast.home (192.168.1.10)

Quel est le système d'exploitation que cette machine utilise ?

Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10

Quelle est son adresse MAC ?

MAC Address: 88:3D:24:0E:B6:70 (Google)

b Quels sont les ports ouverts sur cette machine ?

Not shown: 995 closed ports
PORT STATE SERVICE
8008/tcp open http
8009/tcp open ajp13
8443/tcp open https-alt
9000/tcp open cslistener
10001/tcp open scp-config

5 Taper la commande *nmap - -script default adresse ip d'une machine*

map - -script default 192.168.1.17

a Quel est le nom de la machine ?

Nmap scan report for amandine-chambre.home (192.168.1.17)

b Quel est le nom de l'utilisateur ?

NetBIOS name: AMANDINECHAMBRE, NetBIOS user: <unknown>

c Quelle est la version du système d'exploitation ?

Running (JUST GUESSING): Microsoft Windows XP|7|2008 (87%)OS CPE:
cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_7
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows XP SP2 (87%), Microsoft Windows 7 (85%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%)

6 Taper la commande *nmap – v - -script vuln adresse ip d'une machine*

6.a Quelles sont les failles, faiblesses et vulnérabilités de cette machine ? (Ports, statut des ports, les services utilisés)

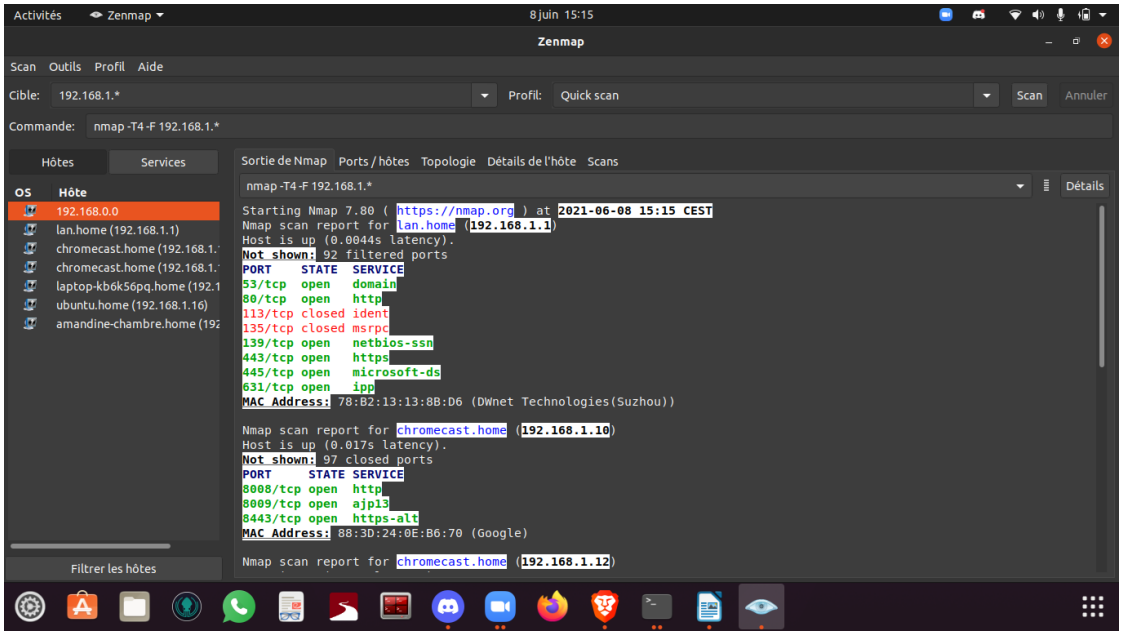
```
Initiating Connect Scan at 14:18
Scanning amandine-chambre.home (192.168.1.17) [1000 ports]
Discovered open port 139/tcp on 192.168.1.17
Discovered open port 445/tcp on 192.168.1.17
Discovered open port 135/tcp on 192.168.1.17
Discovered open port 7070/tcp on 192.168.1.17
Completed Connect Scan at 14:18, 4.92s elapsed (1000 total ports)

PORT     STATE SERVICE
135/tcp  open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp  open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp  open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
7070/tcp open  realserver
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:

Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
```

7 Taper la commande *nmap –v --script dos adresse ip d'une machine*

7.a Peut-on analyser, détecter et mener une attaque Dos ?

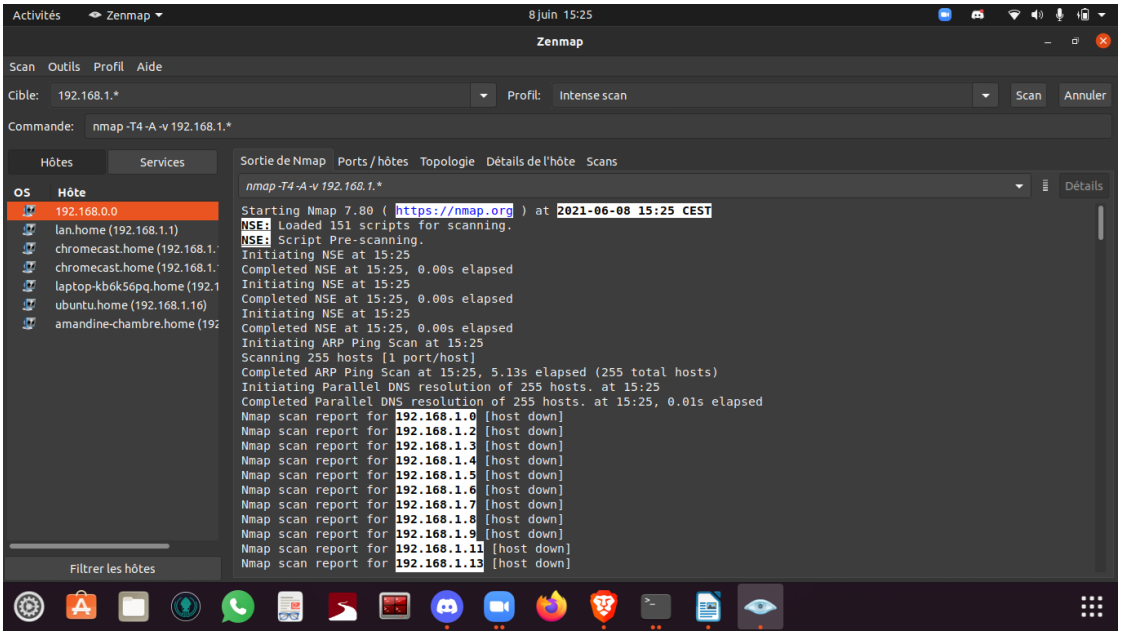
INTERFACE GRAPHIQUE ZENMAP

1 Faites un Quick scan de votre réseau

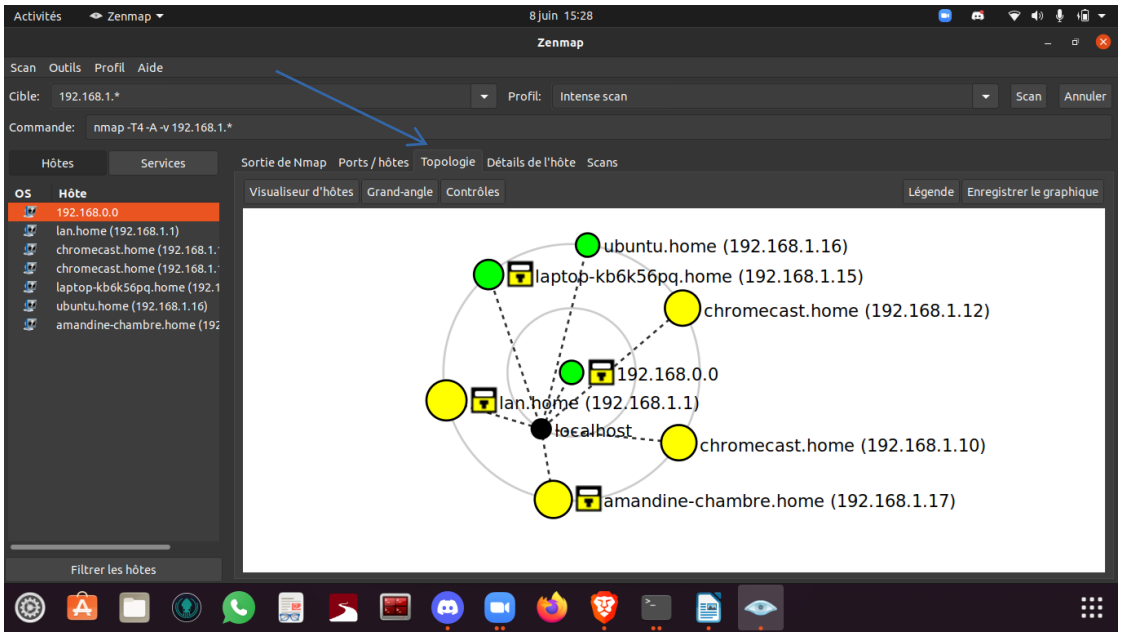


nmap -T4 -F 192.168.1.*

2 Faites également un scan intense



3 Essayer de trouver la topologie de ce réseau



Une fois le scan effectué avec les noms des machines, les adresses IP, les adresses MAC, les services qu'ils utilisent, les systèmes d'exploitation qu'ils utilisent, Qu'êtes-vous capable de faire ?

Infiltrer le/les PC, voler ou modifier des données, faire un botnet en vue d'une attaque DDOS