DZERAHOVIC—BONNETAUD SACHA

ZLATARU FLORIN – CATALIN

RIBARDIÈRE JULIEN

POISSON SIMEON

Projet SAE : Lot C Découverte de machines

- Découvrir les machines du réseau
- Leurs OS (Fingerprint)
- Les services disponibles
- Les logiciels utilisés et leurs versions

Découvrir les machines du réseau

Plan:

- Les machines du réseau : Adresse IP et MAC
- Disponibilité de la machine
- Les chemins parcouru sur notre réseau
- Des services, des programmes ???

Les chemins parcouru sur notre réseau : Arp-Scan


```
user@debian-bullseye:~$ sudo arp-scan --localnet
Interface: enp0s3, type: EN10MB, MAC: 08:00:27:c0:f1:2b, IPv4: 172.21.108.153
Starting arp-scan 1.9.7 with 65536 hosts (https://github.com/royhills/arp-scan)
172.21.0.1      f4:8e:38:4d:7a:33       Dell Inc.
172.21.1.1      84:69:93:07:a2:fa       (Unknown)
172.21.1.2      84:69:93:07:a1:44       (Unknown)
172.21.1.5      84:69:93:07:98:af       (Unknown)
172.21.1.3      84:69:93:07:a3:7d       (Unknown)
172.21.1.6      84:69:93:07:a4:3a       (Unknown)
172.21.1.7      84:69:93:07:a1:5c       (Unknown)
172.21.1.8      84:69:93:07:a4:8a       (Unknown)
172.21.1.9      84:69:93:0e:1e:7f       (Unknown)
172.21.1.11     84:69:93:07:a1:3e       (Unknown)
172.21.1.12     84:69:93:07:a4:ae       (Unknown)
172.21.1.13     84:69:93:07:a1:3c       (Unknown)
```

Les machines du réseau : Adresse IP et MAC : Ping


```
user@debian-bullseye:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=107 time=6.34 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=107 time=6.16 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=107 time=15.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=107 time=6.28 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 6.158/8.601/15.623/4.054 ms
```

Disponibilité de la machine : Traceroute


```
sacha@vbox:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (172.21.0.1)  1.712 ms  2.375 ms  2.375 ms
 2  192.168.0.4 (192.168.0.4)  1.242 ms  1.234 ms  0.963 ms
 3  10.181.76.2 (10.181.76.2)  1.214 ms  1.204 ms  1.193 ms
 4  10.1.2.36 (10.1.2.36)  2.295 ms  2.285 ms  2.275 ms
 5  10.1.243.32 (10.1.243.32)  2.266 ms  2.127 ms  2.115 ms
 6  10.1.243.33 (10.1.243.33)  1.372 ms  1.326 ms  1.598 ms
 7  10.0.180.118 (10.0.180.118)  1.585 ms 10.0.180.120 (10.0.180.120)  1.576 ms 10.0.180.118 (10.0.180.118)  1.505 ms
 8  10.0.180.113 (10.0.180.113)  1.492 ms  1.101 ms  1.077 ms
 9  10.1.243.4 (10.1.243.4)  1.047 ms  1.037 ms  1.010 ms
10  193.48.154.148 (193.48.154.148)  2.956 ms  2.922 ms  2.914 ms
11  * * *
12  * * *
13  vl3201-be1-ren-nr-rouen-rtr-091.noc.renater.fr (193.51.184.130)  3.720 ms  3.713 ms  3.707 ms
14  et-4-4-1-ren-nr-paris1-rtr-131.noc.renater.fr (193.51.177.176)  5.535 ms  5.648 ms  5.640 ms
15  et-5-0-1-ren-nr-paris2-rtr-131.noc.renater.fr (193.55.204.195)  5.747 ms  5.741 ms  5.722 ms
16  192.178.70.144 (192.178.70.144)  5.716 ms  5.767 ms  5.759 ms
17  * * *
18  dns.google (8.8.8.8)  5.568 ms  5.500 ms  5.659 ms
```

Découvrir les OS machines sur le réseau (Fingerprint)

Différents logiciels pour la découverte réseau

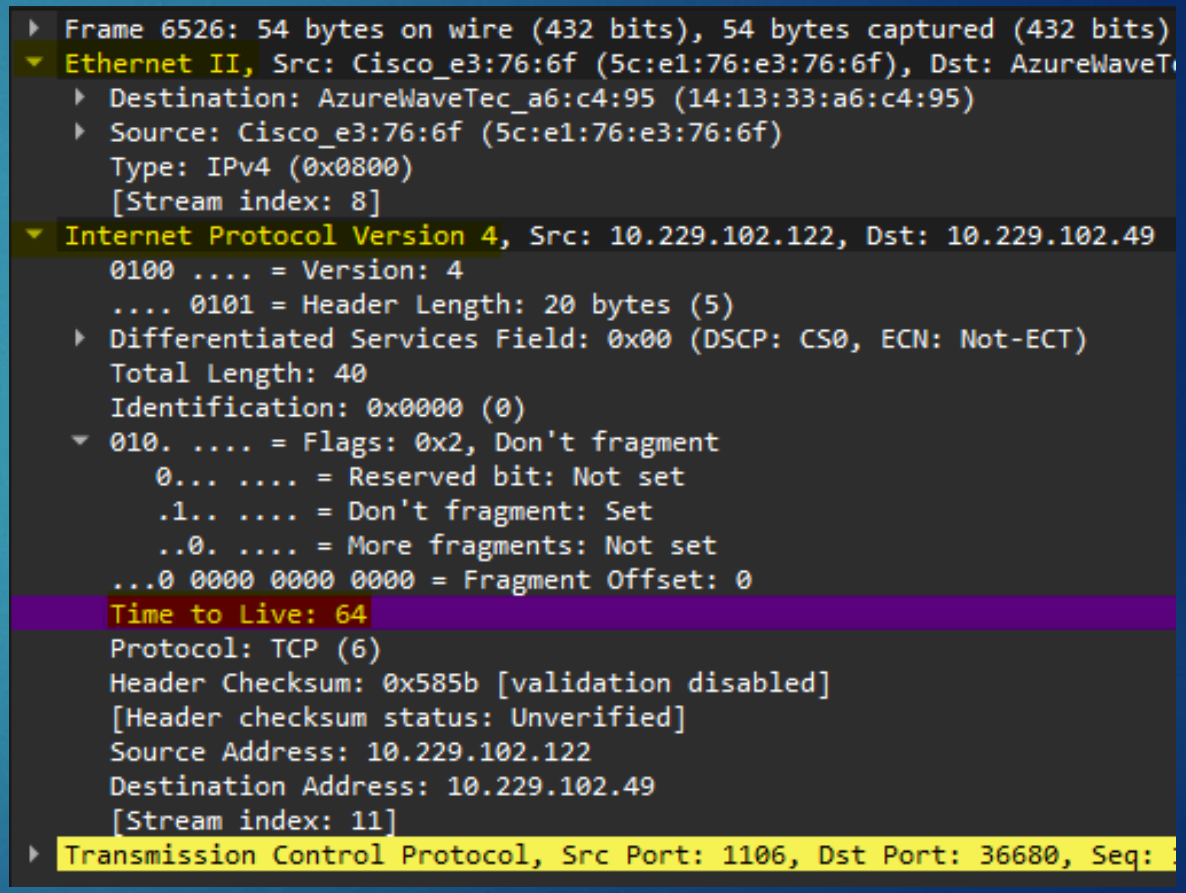
- Wireshark
- Nmap
- Netcat

Les différentes techniques pour déterminer les OS des machines d'un Réseau

- Extraction et analyse du TTL d'un paquet avec Wireshark
- Scan d'OS avec Nmap
- Analyse de Bannière avec Netcat

Extraction et analyse du TTL d'un paquet avec Wireshark


```
C:\Users\Utilisateur>nmap -sS 10.229.102.122
Starting Nmap 7.95 ( https://nmap.org ) at 2024-
10-18 14:08 Romance Daylight Time
Nmap scan report for 10.229.102.122
Host is up (0.011s latency).
All 1000 scanned ports on 10.229.102.122 are in
ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 9A:3C:57:E8:8E:C6 (Unknown)

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



Scan d'OS avec Nmap (normal)


```
C:\Users\Utilisateur>nmap -O 10.229.102.27
Starting Nmap 7.95 ( https://nmap.org ) at 2024-
10-22 10:50 Romance Daylight Time
Nmap scan report for 10.229.102.27
Host is up (0.014s latency).
All 1000 scanned ports on 10.229.102.27 are in
ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 70:3A:51:3A:9E:48 (Xiaomi
Communications)
Too many fingerprints match this host to give
specific OS details
Network Distance: 1 hop
```

```
C:\Users\Utilisateur>nmap -O 10.229.102.49
Starting Nmap 7.95 ( https://nmap.org ) at 2024-
10-22 10:46 Romance Daylight Time
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
1.72 seconds
```

```
C:\Users\Utilisateur>nmap -O 192.168.47.98
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-22 23:55
Romance Daylight Time
Nmap scan report for 192.168.47.98
Host is up (0.020s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
81/tcp   open  hosts2-ns
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1080/tcp open  socks
3306/tcp open  mysql
8081/tcp open  blackice-icecap
MAC Address: C4:17:FE:B8:F2:DF (Hon Hai Precision Ind.)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4),
MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
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 9.24 seconds
```

Scan d'OS avec Nmap (agressif)


```
C:\Users\Utilisateur>nmap -A 10.229.102.49
Starting Nmap 7.95 ( https://nmap.org ) at 2024-
10-18 14:42 Romance Daylight Time
Nmap scan report for 10.229.102.49
Host is up (0.00072s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
135/tcp open  msrpc   Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 21H2
Network Distance: 0 hops
Service Info: OS: Windows; CPE:
cpe:/o:microsoft:windows

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
17.05 seconds
```

```
C:\Users\Utilisateur>nmap -A 192.168.47.98
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-22 23:56 Romance Daylight
Time
Nmap scan report for 192.168.47.98
Host is up (0.014s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 f2:2f:aa:3e:f7:33:86:ab:ba:68:fc:aa:cc:e9:dc:f3 (ECDSA)
|_  256 7f:d7:52:fd:0f:b3:56:8f:9f:c3:04:f3:26:93:99:57 (ED25519)
80/tcp   open  http        Apache httpd 2.4.59 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.59 (Debian)
81/tcp   open  http        Golang net/http server

|_http-title: CasaOS
139/tcp  open  netbios-ssn Samba smbd 4
445/tcp  open  netbios-ssn Samba smbd 4
1080/tcp open  http        nginx 1.25.4
|_http-title: RomM
|_http-server-header: nginx/1.25.4
3306/tcp open  mysql       MariaDB 11.4.2
| mysql-info:

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: DEBIAN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| smb2-time:
|   date: 2024-10-22T21:56:41
|_  start_date: N/A

TRACEROUTE
HOP RTT      ADDRESS
1   13.71 ms 192.168.47.98

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 63.79 seconds
```

Analyse de Bannière avec Netcat


```
C:\Users\Utilisateur>nmap -p- 192.168.47.98
Starting Nmap 7.95 ( https://nmap.org ) at 2024-
10-22 23:36 Romance Daylight Time
Nmap scan report for 192.168.47.98
Host is up (0.012s latency).
Not shown: 65524 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
81/tcp    open  hosts2-ns
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1080/tcp  open  socks
3306/tcp  open  mysql
5216/tcp  open  unknown
8081/tcp  open  blackice-icecap
8444/tcp  open  pcsync-http
19999/tcp open  dnp-sec
MAC Address: C4:17:FE:B8:F2:DF (Hon Hai Precision
Ind.)

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

```
C:\Users\Utilisateur>ncat 192.168.47.98 22
SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u2
```

Découvrir les services disponibles

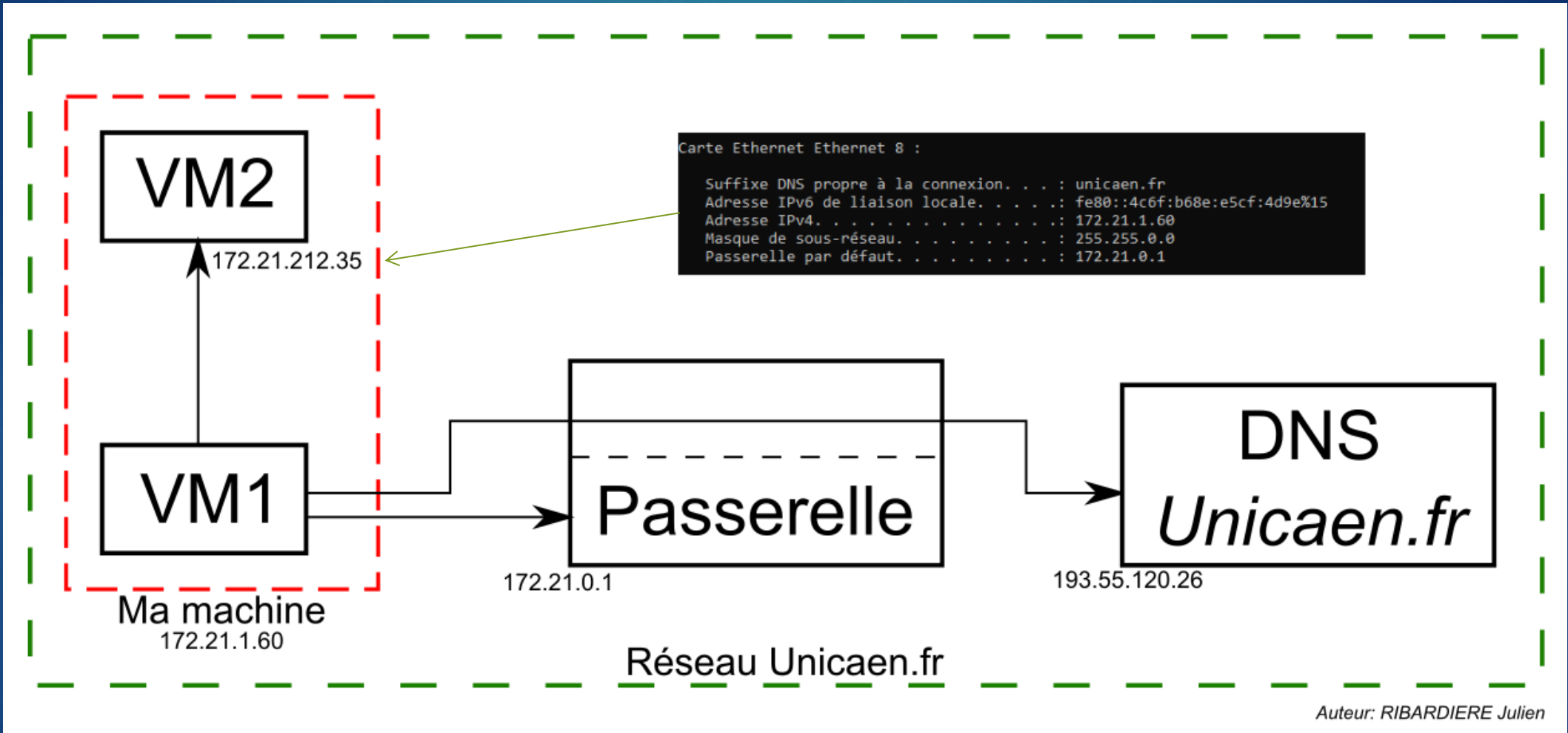
Utilisation de Nmap


```
nmap -sV [adresse ip cible]

et/ou

nmap -sV [adresse ip cible] --version-trace
```

- États possibles des ports :

• Ouvert	• Filtré	• Ouvert | Filtré
• Fermé	• Non-filtré	• Fermé | Filtré

Utilisation de Nmap



Utilisation de Nmap

Cible : Machine virtuelle (VM2)

```
user@debian-bullseye:~$ nmap -sV 172.21.212.35
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-17 11:36 CEST
Nmap scan report for 172.21.212.35
Host is up (0.00026s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

```
Carte Ethernet Ethernet 8 :

   Suffixe DNS propre à la connexion. . . : unicaen.fr
   Adresse IPv6 de liaison locale. . . . .: fe80::4c6f:b68e:e5cf:4d9e%15
   Adresse IPv4. . . . . . . . . . . . . .: 172.21.1.60
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 172.21.0.1
```

Cible : Passerelle

```
user@debian-bullseye:~$ nmap -sV 172.21.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-18 13:26 CEST
Nmap scan report for 172.21.0.1
Host is up (0.028s latency).
Not shown: 998 closed ports
PORT     STATE    SERVICE VERSION
22/tcp   open     ssh     OpenSSH 6.8 (protocol 1.99)
3260/tcp filtered iscsi

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.61 seconds
```

Utilisation de Nmap

Cible : DNS (Unicaen.fr)

```
user@debian-bullseye:~$ nmap -sV unicaen.fr
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-18 13:16 CEST
Nmap scan report for unicaen.fr (193.55.120.26)
Host is up (0.0015s latency).
rDNS record for 193.55.120.26: rp5.unicaen.fr
Not shown: 994 filtered ports
PORT     STATE  SERVICE   VERSION
80/tcp   open   http      nginx
113/tcp  closed ident
443/tcp  open   ssl/http  nginx
444/tcp  closed snpp
843/tcp  closed unknown
8443/tcp closed https-alt

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.12 seconds
```

```
Carte Ethernet Ethernet 8 :

   Suffixe DNS propre à la connexion. . . : unicaen.fr
   Adresse IPv6 de liaison locale. . . . .: fe80::4c6f:b68e:e5cf:4d9e%15
   Adresse IPv4. . . . . . . . . . . . . .: 172.21.1.60
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 172.21.0.1
```

Fonctionnement de Nmap

Cible : Passerelle

```
user@debian-bullseye:~$ nmap -sV 172.21.0.1 --version-trace
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-18 13:28 CEST
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 45 scripts for scanning.
Overall sending rates: 1019.37 packets / s.
mass_rdns: Using DNS server 193.55.120.80
mass_rdns: 0.00s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Overall sending rates: 765.15 packets / s.
NSOCK INFO [1.5450s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [1.5450s] nsock_connect_tcp(): TCP connection requested to 172.21.0.1:22 (IOD #1) EID 8
NSOCK INFO [1.5500s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [172.21.0.1:22]
Service scan sending probe NULL to 172.21.0.1:22 (tcp)
NSOCK INFO [1.5500s] nsock_read(): Read request from IOD #1 [172.21.0.1:22] (timeout: 6000ms) EID 18
NSOCK INFO [1.5510s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [172.21.0.1:22] (21 bytes): SSH-1.99-OpenSSH_6
.8.
Service scan match (Probe NULL matched with NULL line 3537): 172.21.0.1:22 is ssh.  Version: |OpenSSH|6.8|protocol 1.99|
NSOCK INFO [1.5510s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSE: Script scanning 172.21.0.1.
NSE: Starting runlevel 1 (of 2) scan.
NSE: Starting runlevel 2 (of 2) scan.
Nmap scan report for 172.21.0.1
Host is up (0.024s latency).
Scanned at 2024-10-18 13:28:56 CEST for 1s
Not shown: 998 closed ports
PORT     STATE    SERVICE VERSION
22/tcp   open     ssh     OpenSSH 6.8 (protocol 1.99)
3260/tcp filtered iscsi
Final times for host: srtt: 23631 rttvar: 1211  to: 100000

Read from /usr/bin/../share/nmap: nmap-payloads nmap-service-probes nmap-services.
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.56 seconds
```

```
Carte Ethernet Ethernet 8 :

   Suffixe DNS propre à la connexion. . . : unicaen.fr
   Adresse IPv6 de liaison locale. . . . .: fe80::4c6f:b68e:e5cf:4d9e%15
   Adresse IPv4. . . . . . . . . . . . . .: 172.21.1.60
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 172.21.0.1
```

Découvrir les logiciels utilisés et leurs versions

Intérêt ?

SECURITEE

STABILITEE

La banière

- HTTP :

```
http                    Apache httpd 2.4.62 ((Debian))
```

- SSH

```
SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u2
```

Modifier la bannière : « ServerTokens »

HTTP :

/etc/apache2/apache2.conf

On ajoute/modifie :

ServerTokens [option]

Les options :

Prod, Major, Minor, Minimal, OS

Nmap + -sV


```
adminetu@LinuxDebianGUI:~$ nmap -Pn -sV 172.17.239.221
Starting Nmap 7.93 ( https://nmap.org ) at 2024-10-18 12:22 CEST
Nmap scan report for 172.17.239.221
Host is up (0.00028s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT    STATE SERVICE         VERSION
80/tcp  open  http            Apache httpd 2.4.62 ((Debian))
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
```

Nmap + -script=banner


```
adminetu@LinuxDebianGUI:~$ nmap -Pn --script=banner 172.17.239.221
Starting Nmap 7.93 ( https://nmap.org ) at 2024-10-18 12:34 CEST
Nmap scan report for 172.17.239.221
Host is up (0.00020s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT    STATE SERVICE
80/tcp  open  http
902/tcp open  iss-realsecure
| banner: 220 VMware Authentication Daemon Version 1.10: SSL Required, Se
|_rverDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , VMXARGS supported,...
```

NetCat


```
C:\Users\Utilisateur>ncat 192.168.47.98 22
SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u2
```

Merci de votre écoute!