

DÉCOUVERTES DE MACHINES



Presented by : Maxence, Gilles, Remi, Ylan et Simon



MACHINES DU RÉSEAU

```
adminetu@LinuxDebianGUI:~$ sudo nmap -sL 192.168.153.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-10-22 14:44 CEST
Nmap scan report for 192.168.153.0
Nmap scan report for 192.168.153.1
Nmap scan report for 192.168.153.2
Nmap scan report for 192.168.153.3
Nmap scan report for 192.168.153.4
Nmap scan report for 192.168.153.5
Nmap scan report for 192.168.153.6
Nmap scan report for 192.168.153.7
Nmap scan report for 192.168.153.8
Nmap scan report for 192.168.153.9
Nmap scan report for 192.168.153.10
Nmap scan report for 192.168.153.11
Nmap scan report for 192.168.153.12
Nmap scan report for 192.168.153.13
Nmap scan report for 192.168.153.14
Nmap scan report for 192.168.153.15
Nmap scan report for 192.168.153.16
Nmap scan report for 192.168.153.17
Nmap scan report for 192.168.153.18
Nmap scan report for 192.168.153.19
Nmap scan report for 192.168.153.20
Nmap scan report for 192.168.153.21
Nmap scan report for 192.168.153.22
Nmap scan report for 192.168.153.23
Nmap scan report for 192.168.153.24
Nmap scan report for 192.168.153.25
Nmap scan report for 192.168.153.26
Nmap scan report for 192.168.153.27
Nmap scan report for 192.168.153.28
Nmap scan report for 192.168.153.29
Nmap scan report for 192.168.153.30
```

-SL (Liste simplement)

```
Nmap scan report for 192.168.153.219
Nmap scan report for 192.168.153.220
Nmap scan report for 192.168.153.221
Nmap scan report for 192.168.153.222
Nmap scan report for 192.168.153.223
Nmap scan report for 192.168.153.224
Nmap scan report for 192.168.153.225
Nmap scan report for 192.168.153.226
Nmap scan report for 192.168.153.227
Nmap scan report for 192.168.153.228
Nmap scan report for 192.168.153.229
Nmap scan report for 192.168.153.230
Nmap scan report for 192.168.153.231
Nmap scan report for 192.168.153.232
Nmap scan report for 192.168.153.233
Nmap scan report for 192.168.153.234
Nmap scan report for 192.168.153.235
Nmap scan report for 192.168.153.236
Nmap scan report for 192.168.153.237
Nmap scan report for 192.168.153.238
Nmap scan report for 192.168.153.239
Nmap scan report for 192.168.153.240
Nmap scan report for 192.168.153.241
Nmap scan report for 192.168.153.242
Nmap scan report for 192.168.153.243
Nmap scan report for 192.168.153.244
Nmap scan report for 192.168.153.245
Nmap scan report for 192.168.153.246
Nmap scan report for 192.168.153.247
Nmap scan report for 192.168.153.248
Nmap scan report for 192.168.153.249
Nmap scan report for 192.168.153.250
Nmap scan report for 192.168.153.251
Nmap scan report for 192.168.153.252
Nmap scan report for 192.168.153.253
Nmap scan report for 192.168.153.254
Nmap scan report for 192.168.153.255
Nmap done: 256 IP addresses (0 hosts up) scanned in 0.03 seconds
```

02/09



MACHINES DU RÉSEAU

03/09

-sP(Scan ping)

```
adminetu@LinuxDebianGUI:~$ sudo nmap -sP 192.168.153.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-10-22 14:45 CEST
Nmap scan report for 192.168.153.128
Host is up (0.00018s latency).
MAC Address: 08:00:27:2D:94:0B (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.153.254
Host is up (0.000038s latency).
MAC Address: 00:50:56:F7:47:C5 (VMware)
Nmap scan report for 192.168.153.1
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 4.28 seconds
```



OS MACHINES DU RÉSEAU

04/09

-O (Enable OS detection)

--osscan-limit (Limit OS detection to promising targets)

--osscan-guess; --fuzzy (Guess OS detection results)

```
adminetu@LinuxDebianGUI:~$ sudo nmap -O 192.168.153.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-10-22 14:46 CEST
Nmap scan report for 192.168.153.128
Host is up (0.00014s latency).
All 1000 scanned ports on 192.168.153.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:2D:94:0B (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.153.254
Host is up (0.000036s latency).
All 1000 scanned ports on 192.168.153.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F7:47:C5 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.153.1
Host is up (0.000019s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
443/tcp    open  https
902/tcp    open  iss-realsecure
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 12.53 seconds
```

SERVICES DISPONIBLES

- : le service n'est pas en cours d'exécution

+ : le service est en cours d'exécution

? : l'état du service ne peut être déterminé

source : <https://askubuntu.com/questions/407075/how-to-read-service-status-all-results>

```
adminetu@LinuxDebianGUI:~$ sudo service --status-all
[sudo] Mot de passe de adminetu :
[ - ] alsa-utils
[ - ] anacron
[ + ] apparmor
[ - ] bluetooth
[ - ] console-setup.sh
[ + ] cron
[ + ] cups
[ + ] cups-browsed
[ + ] dbus
[ + ] docker
[ + ] exim4
[ - ] hwclock.sh
[ - ] keyboard-setup.sh
[ + ] kmod
[ + ] lightdm
[ + ] lm-sensors
[ - ] mdadm
[ - ] mdadm-waitidle
[ + ] networking
[ - ] plymouth
[ + ] plymouth-log
[ + ] procps
[ - ] pulseaudio-enable-autospawn
[ - ] saned
[ - ] speech-dispatcher
[ - ] sudo
[ + ] udev
[ - ] uuidd
[ + ] vmware
[ ? ] vmware-USBArbitrator
[ + ] vmware-workstation-server
[ - ] x11-common
```

05/09



SERVICES DISPONIBLES

Enabled : Active une unité pour qu'elle démarre au démarrage du système

Disabled : Désactive une unité pour qu'elle n'exécute plus au démarrage.

Alias : L'unité est un alias vers une autre unité. Elle ne peut pas être démarrée indépendamment.

source : <https://blog.stephane-robert.info/docs/admin-serveurs/linux/services/>

UNIT FILE	STATE	PRESET
alsa-restore.service	static	-
alsa-state.service	static	-
alsa-utils.service	masked	enabled
anacron.service	enabled	enabled
apparmor.service	enabled	enabled
apt-daily-upgrade.service	static	-
apt-daily.service	masked	enabled
autovt@.service	alias	-
avahi-daemon.service	enabled	enabled
blk-availability.service	enabled	enabled
bluetooth.service	enabled	enabled
colord.service	static	-
configure-printer@.service	static	-
console-getty.service	disabled	disabled
console-setup.service	enabled	enabled
container-getty@.service	static	-
containerd.service	enabled	enabled
cron.service	enabled	enabled
cryptdisks-early.service	masked	enabled
cryptdisks.service	masked	enabled
cups-browsed.service	enabled	enabled
cups.service	enabled	enabled
dbus-fi.wl.wpa_supplicant1.service	alias	-
dbus-org.bluez.service	alias	-
dbus-org.freedesktop.Avahi.service	alias	-
dbus-org.freedesktop.hostname1.service	alias	-
dbus-org.freedesktop.import1.service	alias	-
dbus-org.freedesktop.locale1.service	alias	-
dbus-org.freedesktop.login1.service	alias	-
dbus-org.freedesktop.machine1.service	alias	-
dbus-org.freedesktop.ModemManager1.service	alias	-
dbus-org.freedesktop.nm-dispatcher.service	alias	-
dbus-org.freedesktop.portable1.service	alias	-
dbus-org.freedesktop.timedate1.service	alias	-
dbus-org.freedesktop.timesync1.service	alias	-
dbus.service	static	-
debug-shell.service	disabled	disabled
display-manager.service	alias	-

06/09



GÉRER LES SERVICE

Systemctl

07/09

sudo systemctl status (service)

sudo systemctl start (service)

```
adminetu@LinuxDebianGUI:~$ sudo systemctl status cups
[sudo] Mot de passe de adminetu :
● cups.service - CUPS Scheduler
    Loaded: loaded (/lib/systemd/system/cups.service; enabled; preset: enabled)
    Active: active (running) since Tue 2024-10-22 14:04:41 CEST; 39min ago
  TriggeredBy: ● cups.socket
                ○ cups.path
      Docs: man:cupsd(8)
     Main PID: 19660 (cupsd)
       Status: "Scheduler is running..."
          Tasks: 1 (limit: 18967)
        Memory: 1.3M
           CPU: 7ms
```



LOGICIELS UTILISÉS ET LEUR VERSION

08/09

- nmap @adresse_ip
- nmap -sV @adresse_ip
- nmap -sV -p 22 @adresse_ip

```
root@debian-10:~# nmap -sV 172.21.1.122
Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-22 13:38 CEST
Nmap scan report for 172.21.1.122
Host is up (-0.017s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1309/tcp   open  tcpwrapped
1947/tcp   open  http         Aladdin/SafeNet HASP license manager 16.00
3580/tcp   open  http         Mbedthis-Appweb 2.5.0
MAC Address: 64:00:6A:59:5A:A0 (Dell)
Service Info: Host: RTN13; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 29.47 seconds
```



MERCI
DE NOUS AVOIR ÉCOUTÉ

