

## Quiz de securite

les hôtes actifs :

nmap -sn -n 192.168.63.0/24

```
(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
└─(root㉿kali)-[/home/kali]
# systemctl restart wg-quick@wg1.service

└─(root㉿kali)-[/home/kali]
# nmap -sn -n 192.168.63.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 06:06 EDT
Nmap scan report for 192.168.63.1
Host is up (0.16s latency).
Nmap scan report for 192.168.63.69
Host is up (0.14s latency).
Nmap scan report for 192.168.63.101
Host is up (0.12s latency).
Nmap scan report for 192.168.63.102
Host is up (0.13s latency).
Nmap scan report for 192.168.63.109
Host is up (0.15s latency).
Nmap scan report for 192.168.63.111
Host is up (0.15s latency).
Nmap done: 256 IP addresses (6 hosts up) scanned in 10.59 seconds

└─(root㉿kali)-[/home/kali]
#
```

nmap -sn -n 192.168.63.0/24 -oG UP.txt

```
(root㉿kali)-[/home/kali]
# nmap -sn -n 192.168.63.0/24 -oG UP.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 06:10 EDT
Nmap scan report for 192.168.63.1
Host is up (0.15s latency).
Nmap scan report for 192.168.63.69
Host is up (0.11s latency).
Nmap scan report for 192.168.63.101
Host is up (0.12s latency).
Nmap scan report for 192.168.63.102
Host is up (0.12s latency).
Nmap scan report for 192.168.63.109
Host is up (0.13s latency).
Nmap scan report for 192.168.63.111
Host is up (0.12s latency).
Nmap done: 256 IP addresses (6 hosts up) scanned in 8.90 seconds

└─(root㉿kali)-[/home/kali]
# cat UP.txt
# Nmap 7.94SVN scan initiated Wed Apr 17 06:10:19 2024 as: nmap -sn -n -oG UP.txt 192.168.63.0/24
Host: 192.168.63.1 ( ) Status: Up
Host: 192.168.63.69 ( ) Status: Up
Host: 192.168.63.101 ( ) Status: Up
Host: 192.168.63.102 ( ) Status: Up
Host: 192.168.63.109 ( ) Status: Up
Host: 192.168.63.111 ( ) Status: Up
# Nmap done at Wed Apr 17 06:10:28 2024 -- 256 IP addresses (6 hosts up) scanned in 8.90 seconds
```

## Quiz de securite

Pour supprimer l'adresse 192.168.63.1 :

```
(root@kali)-[/home/kali]
# cat UP.txt | grep Up | cut -d ' ' -f 2 >les_up.txt

(root@kali)-[/home/kali]
# cat les_up.txt
192.168.63.1
192.168.63.69
192.168.63.101
192.168.63.102
192.168.63.109
192.168.63.111

(root@kali)-[/home/kali]
# nano les_up.txt

(root@kali)-[/home/kali]
# cat les_up.txt
192.168.63.69
192.168.63.101
192.168.63.102
192.168.63.109
192.168.63.111

(root@kali)-[/home/kali]
#
```

les ports ouverts et les versions de services qui s'exécutent sur eux :

```
nmap -vv -n -sV -iL les_up.txt
```

```
[root@kali:~/home/kali]#
# nmap -vv -n -sV -iL les.up.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 06:26 EDT
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 06:26
Scanning 5 hosts [4 ports/host]
Completed Ping Scan at 06:26, 0.23s elapsed (5 total hosts)
Initiating SYN Stealth Scan at 06:26
Scanning 5 hosts [1000 ports/host]
Discovered open port 21/tcp on 192.168.63.101
Discovered open port 80/tcp on 192.168.63.69
Discovered open port 80/tcp on 192.168.63.109
Discovered open port 80/tcp on 192.168.63.111
Discovered open port 80/tcp on 192.168.63.102
Discovered open port 80/tcp on 192.168.63.101
Discovered open port 22/tcp on 192.168.63.69
Discovered open port 22/tcp on 192.168.63.101
Discovered open port 22/tcp on 192.168.63.102
Discovered open port 22/tcp on 192.168.63.111
Discovered open port 5000/tcp on 192.168.63.102
Discovered open port 9001/tcp on 192.168.63.102
Discovered open port 8081/tcp on 192.168.63.102
Completed SYN Stealth Scan against 192.168.63.111 in 20.84s (4 hosts left)
Completed SYN Stealth Scan against 192.168.63.69 in 21.17s (3 hosts left)
Completed SYN Stealth Scan against 192.168.63.102 in 22.46s (2 hosts left)
Completed SYN Stealth Scan against 192.168.63.109 in 22.82s (1 host left)
Completed SYN Stealth Scan at 06:26, 23.10s elapsed (5000 total ports)
Initiating Service scan at 06:26
Scanning 13 services on 5 hosts
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '\sHTTP/1.1 \d\d\d\d(?:[^\r\n]*\r\n(?:\r\n)?)*.*\r\nServer: Virata-EmWeb/R([\d_])\r\nContent-Type: text/html; \?charset=UTF-8\r\nExpires:.*<title>HP (Color )LaserJet ([\w_ -])&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&~'HTTP/1.1 \d\d\d\d(?:[^\r\n]*\r\n(?:\r\n)?)*.*\r\nServer: Virata-EmWeb/R([\d_])\r\nContent-Type: text/html; \?charset=UTF-8\r\nExpires:.*<title>HP (Color )LaserJet ([\w_ -])&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&~'
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '\sHTTP/1.1 \d\d\d\d(?:[^\r\n]*\r\n(?:\r\n)?)*.*\r\nServer: Virata-EmWeb/R([\d_])\r\nContent-Type: text/html; \?charset=UTF-8\r\nExpires:.*<title>HP (Color )LaserJet ([\w_ -])&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&~'
Completed Service scan at 06:26, 11.50s elapsed (13 services on 5 hosts)
NSE: Script scanning 5 hosts.
NSE: Starting runLevel 1 (of 2) scan.
Initiating NSE at 06:26
Completed NSE at 06:26, 0.84s elapsed
```

## Quiz de securite

```
80/tcp open  http      syn-ack ttl 63 nginx 1.22.1
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.63.102
Host is up, received echo-reply ttl 63 (0.11s latency).
Scanned at 2024-04-17 06:26:15 EDT for 36s
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http      syn-ack ttl 63  nginx 1.14.0 (Ubuntu)
5000/tcp  open  http      syn-ack ttl 63  nginx 1.14.0 (Ubuntu)
8081/tcp  open  http      syn-ack ttl 63  nginx 1.14.0 (Ubuntu)
9001/tcp  open  http      syn-ack ttl 63  nginx 1.14.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.63.109
Host is up, received echo-reply ttl 63 (0.12s latency).
Scanned at 2024-04-17 06:26:15 EDT for 36s
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http      syn-ack ttl 63  Apache httpd 2.4.18 ((Ubuntu))

Nmap scan report for 192.168.63.111
Host is up, received echo-reply ttl 63 (0.12s latency).
Scanned at 2024-04-17 06:26:15 EDT for 36s
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
80/tcp    open  http      syn-ack ttl 63  Apache httpd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 5 IP addresses (5 hosts up) scanned in 37.14 seconds
Raw packets sent: 5102 (224.408KB) | Rcvd: 5100 (203.992KB)
```