

Nom:Zeinebou/Saleh

Matricule :22065

1. nmap -sn 192.168.63.0/24

```
(root@kali)~[/home/kali]
# nmap -sn 192.168.63.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 06:01 EDT
Nmap scan report for 192.168.63.1
Host is up (0.083s latency).
Nmap scan report for 192.168.63.69
Host is up (0.17s latency).
Nmap scan report for 192.168.63.101
Host is up (0.22s latency).
Nmap scan report for 192.168.63.102
Host is up (0.22s latency).
Nmap scan report for 192.168.63.109
Host is up (0.22s latency).
Nmap scan report for 192.168.63.111
Host is up (0.14s latency).
Nmap done: 256 IP addresses (6 hosts up) scanned in 24.92 seconds

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

2. nmap -sn 192.168.63.0/24 -oG fileName.txt

cat 22065.txt | grep Up | cut -d ' ' -f 2 > up.txt

nmap -vv -n -sV -iL up.txt

```
(root@kali)-[/home/kali]
# nmap -vv -n -sV -iL up.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 06:40 EDT
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 06:40
Scanning 6 hosts [4 ports/host]
Completed Ping Scan at 06:40, 0.18s elapsed (6 total hosts)
Initiating SYN Stealth Scan at 06:40
Scanning 6 hosts [1000 ports/host]
Discovered open port 8080/tcp on 192.168.63.1
Discovered open port 80/tcp on 192.168.63.69
Discovered open port 80/tcp on 192.168.63.101
Discovered open port 80/tcp on 192.168.63.102
Discovered open port 80/tcp on 192.168.63.109
Discovered open port 80/tcp on 192.168.63.111
Discovered open port 21/tcp on 192.168.63.101
Discovered open port 22/tcp on 192.168.63.102
Discovered open port 22/tcp on 192.168.63.101
Discovered open port 22/tcp on 192.168.63.111
Discovered open port 22/tcp on 192.168.63.69
Discovered open port 2222/tcp on 192.168.63.1
Discovered open port 5000/tcp on 192.168.63.102
Discovered open port 8081/tcp on 192.168.63.102
Discovered open port 9001/tcp on 192.168.63.102
Completed SYN Stealth Scan against 192.168.63.101 in 41.05s (5 hosts left)
Completed SYN Stealth Scan against 192.168.63.111 in 42.20s (4 hosts left)
Completed SYN Stealth Scan against 192.168.63.102 in 43.16s (3 hosts left)
Completed SYN Stealth Scan against 192.168.63.69 in 43.79s (2 hosts left)
Completed SYN Stealth Scan against 192.168.63.109 in 43.79s (1 host left)
Completed SYN Stealth Scan at 06:41, 44.75s elapsed (6000 total ports)
Initiating Service scan at 06:41
Scanning 15 services on 6 hosts
```

```
nmap scan report for 192.168.63.69
Host is up, received echo-reply ttl 63 (0.15s latency).
Scanned at 2024-04-17 06:40:41 EDT for 58s
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
80/tcp    open  http     syn-ack ttl 63 nginx 1.22.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

File System
nmap scan report for 192.168.63.101
Host is up, received echo-reply ttl 63 (0.15s latency).
Scanned at 2024-04-17 06:40:41 EDT for 58s
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 63 vsftpd 3.0.3
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
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 (0.16s latency).
Scanned at 2024-04-17 06:40:41 EDT for 58s
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)
8000/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)
8001/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 (0.17s latency).
Scanned at 2024-04-17 06:40:41 EDT for 58s
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 (0.16s latency).
Scanned at 2024-04-17 06:40:41 EDT for 58s
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: 6 IP addresses (6 hosts up) scanned in 58.86 seconds
Raw packets sent: 6250 (274.888KB) | Rcvd: 6217 (248.668KB)

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