ESERCIZIO M3 D6

```
┌──(root㉿kali)-[/home/heskarioth94]
└─# nmap -sS 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 15:29 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0022s latency).
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.60 seconds
```

```
┌──(root㉿kali)-[/home/heskarioth94]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 16:31 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  rpcbind
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  unknown
MAC Address: 08:00:27:A0:26:54 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, 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 62.18 seconds
```

```
┌──(root㉿kali)-[/home/heskarioth94]
└─# nmap -sV -oN file.txt 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 15:32 CEST
Stats: 0:01:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 73.91% done; ETC: 15:35 (0:00:33 remaining)
Stats: 0:02:46 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 15:35 (0:00:00 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.00035s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:A0:26:54 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, 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 180.14 seconds
```

```
┌──(root㉿kali)-[/home/heskarioth94]
└─# nmap -sS -p 8080 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 15:37 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).

PORT     STATE    SERVICE
8080/tcp filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.42 seconds
```

```
┌──(root㉿kali)-[/home/heskarioth94]
└─# nmap -sS -p- 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 15:42 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000066s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
32987/tcp open  unknown
48273/tcp open  unknown
52302/tcp open  unknown
59337/tcp open  unknown
MAC Address: 08:00:27:A0:26:54 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

```
┌──(root㉿kali)-[/home/heskarioth94]
└─# nmap -sU -r -v 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 15:43 CEST
Initiating ARP Ping Scan at 15:43
Scanning 192.168.50.101 [1 port]
Completed ARP Ping Scan at 15:43, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:43
Completed Parallel DNS resolution of 1 host. at 15:43, 0.07s elapsed
```

```
Initiating UDP Scan at 15:43
Scanning 192.168.50.101 [1000 ports]
Discovered open port 111/udp on 192.168.50.101
Discovered open port 53/udp on 192.168.50.101
Increasing send delay for 192.168.50.101 from 0 to 50 due to max_successful_tryno increase to 4
Discovered open port 137/udp on 192.168.50.101
Increasing send delay for 192.168.50.101 from 50 to 100 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 192.168.50.101 from 100 to 200 due to 11 out of 12 dropped probes since last increase.
UDP Scan Timing: About 9.45% done; ETC: 15:48 (0:04:57 remaining)
Increasing send delay for 192.168.50.101 from 200 to 400 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 11.40% done; ETC: 15:52 (0:07:54 remaining)
UDP Scan Timing: About 12.53% done; ETC: 15:55 (0:10:35 remaining)
Increasing send delay for 192.168.50.101 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 13.15% done; ETC: 15:58 (0:13:19 remaining)
UDP Scan Timing: About 13.72% done; ETC: 16:01 (0:15:50 remaining)
UDP Scan Timing: About 14.30% done; ETC: 16:04 (0:18:05 remaining)
Increasing send delay for 192.168.50.101 from 800 to 1000 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 14.78% done; ETC: 16:07 (0:20:16 remaining)
UDP Scan Timing: About 15.23% done; ETC: 16:09 (0:22:21 remaining)
UDP Scan Timing: About 15.68% done; ETC: 16:12 (0:24:17 remaining)
UDP Scan Timing: About 16.13% done; ETC: 16:14 (0:26:05 remaining)
UDP Scan Timing: About 16.60% done; ETC: 16:16 (0:27:43 remaining)
UDP Scan Timing: About 19.25% done; ETC: 16:14 (0:25:14 remaining)
Discovered open port 2049/udp on 192.168.50.101
UDP Scan Timing: About 22.25% done; ETC: 16:12 (0:22:46 remaining)
UDP Scan Timing: About 25.25% done; ETC: 16:11 (0:20:46 remaining)
UDP Scan Timing: About 28.25% done; ETC: 16:09 (0:19:05 remaining)
UDP Scan Timing: About 31.25% done; ETC: 16:08 (0:17:38 remaining)
UDP Scan Timing: About 34.25% done; ETC: 16:08 (0:16:21 remaining)
UDP Scan Timing: About 35.63% done; ETC: 16:10 (0:17:39 remaining)
UDP Scan Timing: About 36.87% done; ETC: 16:13 (0:19:02 remaining)
UDP Scan Timing: About 38.40% done; ETC: 16:16 (0:20:34 remaining)
UDP Scan Timing: About 42.98% done; ETC: 16:16 (0:18:53 remaining)
UDP Scan Timing: About 46.28% done; ETC: 16:15 (0:17:09 remaining)
UDP Scan Timing: About 49.88% done; ETC: 16:14 (0:15:27 remaining)
UDP Scan Timing: About 53.48% done; ETC: 16:13 (0:13:54 remaining)
UDP Scan Timing: About 64.02% done; ETC: 16:17 (0:12:21 remaining)
UDP Scan Timing: About 68.22% done; ETC: 16:16 (0:10:34 remaining)
UDP Scan Timing: About 72.72% done; ETC: 16:15 (0:08:48 remaining)
UDP Scan Timing: About 77.22% done; ETC: 16:14 (0:07:08 remaining)
UDP Scan Timing: About 84.23% done; ETC: 16:18 (0:05:32 remaining)
UDP Scan Timing: About 89.03% done; ETC: 16:17 (0:03:45 remaining)
UDP Scan Timing: About 94.13% done; ETC: 16:16 (0:01:57 remaining)
Completed UDP Scan at 16:15, 1949.50s elapsed (1000 total ports)
Nmap scan report for 192.168.50.101
Host is up (0.0012s latency).
Not shown: 752 closed udp ports (port-unreach), 244 open|filtered udp ports (no-response)
```

```
PORT     STATE SERVICE
53/udp   open  domain
111/udp  open  rpcbind
137/udp  open  netbios-ns
2049/udp open  nfs
MAC Address: 08:00:27:A0:26:54 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1949.69 seconds
           Raw packets sent: 2482 (113.347KB) | Rcvd: 769 (56.851KB)
```

```
┌──(root㉿kali)-[/home/heskarioth94]
└─# nmap -O 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 15:44 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0025s latency).
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.61 seconds
```

```
┌──(root㉿kali)-[/home/heskarioth94]
└─# nmap -F 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 15:45 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00090s latency).
All 100 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 1.92 seconds
```

```
┌──(root㉿kali)-[/home/heskarioth94]
└─# nmap -PR 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 15:46 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.29 seconds
```

```
┌──(root㉿kali)-[/home/heskarioth94]
└─# nmap -sP 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 15:47 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00082s latency).
Nmap done: 1 IP address (1 host up) scanned in 8.17 seconds
```

```
┌──(root㉿kali)-[/home/heskarioth94]
└─# nmap -PN 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 15:47 CEST
Nmap scan report for 192.168.50.101
Host is up.
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 205.48 seconds
```