Report scansioni nmap

Metasploitable IP 192.168.50.100

SYN Scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.100
[sudo] password for kali:

Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 11:04 EDT

Nmap scan report for 192.168.50.100

Host is up (0.00066s latency).
Not shown: 977 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
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

Version detection/Banner grabbing

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.100

Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 11:12 EDT

Nmap scan report for 192.168.50.100

Host is up (0.00052s latency).
Not shown: 977 closed tcp ports (conn-refused)

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      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
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        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
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  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
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?
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1

Service Info: Hosts:  metasploitable.localdomain, 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 126.18 seconds
```

Version detection/Banner grabbing with output to file

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -oN file.txt  192.168.50.100

Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 11:29 EDT

Nmap scan report for 192.168.50.100

Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (conn-refused)

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      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
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        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
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  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
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?
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, 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 126.21 seconds
```

File position:

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Esercizi  file.txt
```

Operating System Detection

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.100
[sudo] password for kali:

Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 12:02 EDT

Nmap scan report for 192.168.50.100

Host is up (0.0012s latency).
Not shown: 977 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
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.29
(Gentoo)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 10.68 seconds
```

Verbose UDP Sequential Scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -r -v  192.168.50.100

Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 11:44 EDT

Initiating Ping Scan at 11:44
Scanning 192.168.50.100 [4 ports]
Completed Ping Scan at 11:44, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:44
Completed Parallel DNS resolution of 1 host. at 11:44, 0.00s elapsed
Initiating UDP Scan at 11:44
Scanning 192.168.50.100 [1000 ports]
Discovered open port 53/udp on 192.168.50.100
Discovered open port 111/udp on 192.168.50.100
Increasing send delay for 192.168.50.100 from 0 to 50 due to
max_successful_tryno increase to 4
Discovered open port 137/udp on 192.168.50.100
Increasing send delay for 192.168.50.100 from 50 to 100 due to 11 out of
12 dropped probes since last increase.
Increasing send delay for 192.168.50.100 from 100 to 200 due to
max_successful_tryno increase to 5
Increasing send delay for 192.168.50.100 from 200 to 400 due to
max_successful_tryno increase to 6
Increasing send delay for 192.168.50.100 from 400 to 800 due to
max_successful_tryno increase to 7
UDP Scan Timing: About 5.66% done; ETC: 11:53 (0:08:37 remaining)
Increasing send delay for 192.168.50.100 from 800 to 1000 due to
max_successful_tryno increase to 8
UDP Scan Timing: About 6.75% done; ETC: 11:59 (0:14:03 remaining)
UDP Scan Timing: About 8.35% done; ETC: 12:02 (0:16:38 remaining)
UDP Scan Timing: About 10.05% done; ETC: 12:04 (0:18:02 remaining)
UDP Scan Timing: About 13.64% done; ETC: 12:06 (0:19:06 remaining)
Discovered open port 2049/udp on 192.168.50.100
UDP Scan Timing: About 27.35% done; ETC: 12:09 (0:17:59 remaining)
UDP Scan Timing: About 34.44% done; ETC: 12:09 (0:16:41 remaining)
UDP Scan Timing: About 41.62% done; ETC: 12:10 (0:15:23 remaining)
UDP Scan Timing: About 47.49% done; ETC: 12:11 (0:14:04 remaining)
UDP Scan Timing: About 52.42% done; ETC: 12:11 (0:12:43 remaining)
UDP Scan Timing: About 58.20% done; ETC: 12:11 (0:11:19 remaining)
UDP Scan Timing: About 63.51% done; ETC: 12:11 (0:09:57 remaining)
UDP Scan Timing: About 68.74% done; ETC: 12:11 (0:08:35 remaining)
UDP Scan Timing: About 73.85% done; ETC: 12:12 (0:07:13 remaining)
UDP Scan Timing: About 78.80% done; ETC: 12:11 (0:05:47 remaining)
UDP Scan Timing: About 83.88% done; ETC: 12:11 (0:04:22 remaining)
UDP Scan Timing: About 88.96% done; ETC: 12:11 (0:03:00 remaining)
UDP Scan Timing: About 93.98% done; ETC: 12:11 (0:01:38 remaining)
Completed UDP Scan at 12:13, 1763.05s elapsed (1000 total ports)
```

```
Nmap scan report for 192.168.50.100
Host is up (0.0015s latency).
Not shown: 993 closed udp ports (port-unreach)

PORT     STATE         SERVICE
53/udp   open          domain
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1763.21 seconds
           Raw packets sent: 2068 (92.856KB) | Rcvd: 1160 (84.157KB)
```

TCP SYN Scan for Port 8080

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 8080  192.168.50.100
[sudo] password for kali:

Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 11:39 EDT

Nmap scan report for 192.168.50.100

Host is up (0.0049s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

Host Discovery

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sP 192.168.50.100

Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 12:30 EDT

Nmap scan report for 192.168.50.100

Host is up (0.00085s latency).

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

Fast Scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -F 192.168.50.100
[sudo] password for kali:

Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 12:17 EDT

Nmap scan report for 192.168.50.100

Host is up (0.00066s latency).
Not shown: 82 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
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

ARP Ping Scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -PR 192.168.50.100

Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 12:26 EDT

Nmap scan report for 192.168.50.100

Host is up (0.00054s latency).
Not shown: 977 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
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

No Ping Host Discovery

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn 192.168.50.100

Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 12:35 EDT

Nmap scan report for 192.168.50.100

Host is up (0.0040s latency).
Not shown: 977 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
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

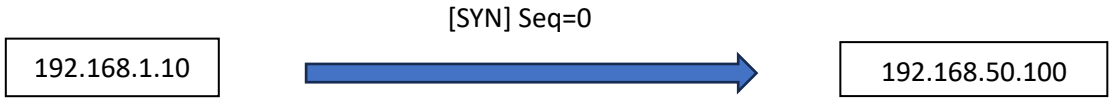
SYN Scan Chart

```
sudo nmap -sS 192.168.50.100
```

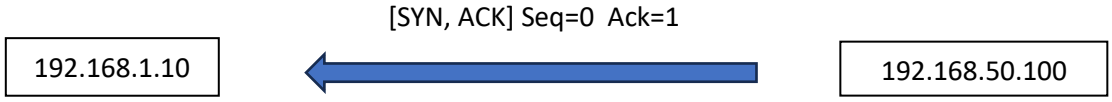
Port 80 Wireshark details

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000036875	192.168.1.10	192.168.50.100	TCP	54	52285 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
35	0.063760174	192.168.1.10	192.168.50.100	TCP	58	52541 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55	0.064699263	192.168.50.100	192.168.1.10	TCP	60	80 → 52541 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
62	0.064712377	192.168.1.10	192.168.50.100	TCP	54	52541 → 80 [RST] Seq=1 Win=0 Len=0

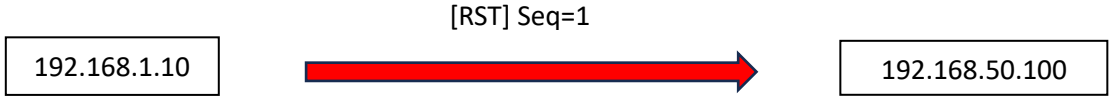
1. SYN: Initiation



2. ACK: Acknowledgment



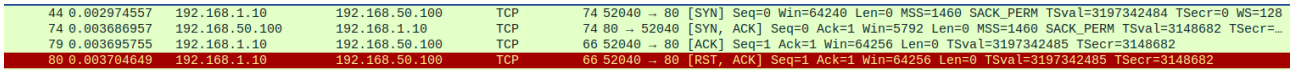
3. RST: Reset



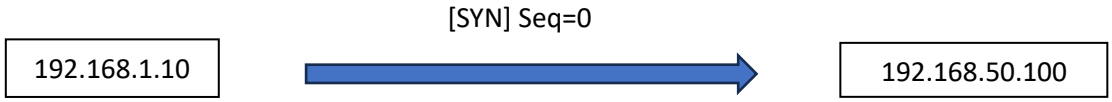
Version detection/Banner grabbing chart

```
nmap -sV 192.168.50.100
```

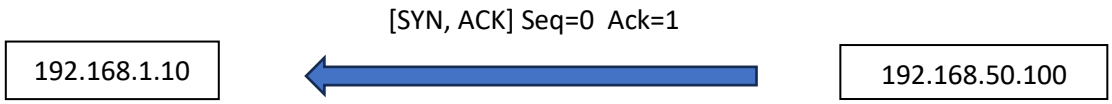
Port 80 Wireshark details



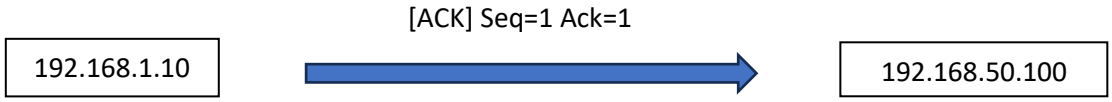
1. SYN: Initiation



2. ACK: Acknowledgment



3. ACK: Acknowledgment



4. RST Reset