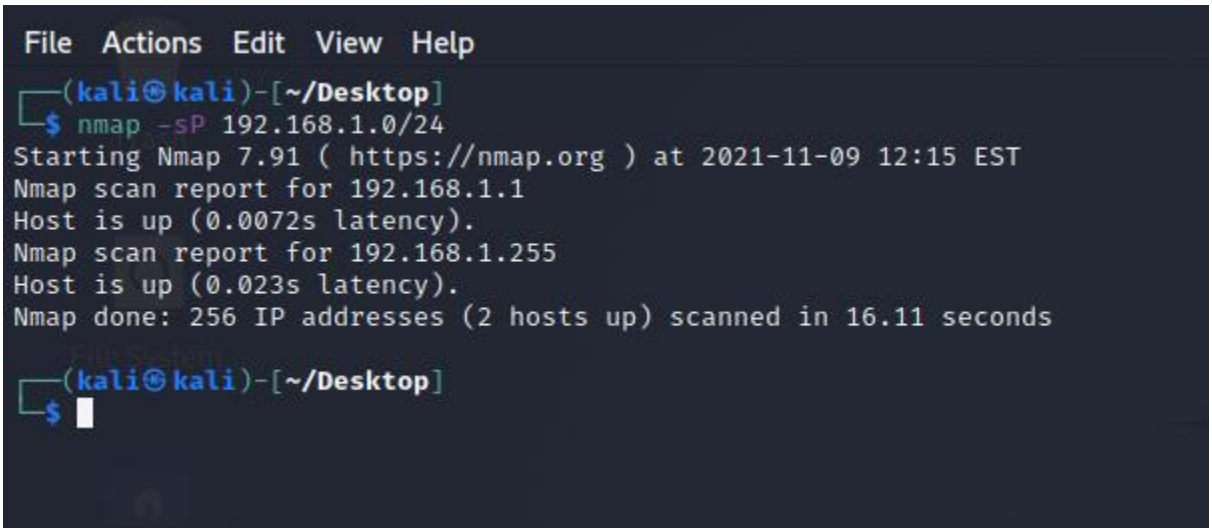
Name: Kulvir Singh
Register Number: 19BCE2074

Information Security and Audit Analysis
Lab DA 5

SNORT

Snort commands output screenshots :--

nmap -sP 192.168.1.0/24



nmap -sP 192.168.1.0/24 –packet-trace

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sP 192.168.1.0/24 --packet-trace
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 12:18 EST
CONN (0.0547s) TCP localhost > 192.168.1.1:80 ⇒ Operation now in progress
CONN (0.0560s) TCP localhost > 192.168.1.2:80 ⇒ Operation now in progress
CONN (0.0562s) TCP localhost > 192.168.1.3:80 ⇒ Operation now in progress
CONN (0.0572s) TCP localhost > 192.168.1.4:80 ⇒ Operation now in progress
CONN (0.0585s) TCP localhost > 192.168.1.5:80 ⇒ Operation now in progress
CONN (0.0588s) TCP localhost > 192.168.1.6:80 ⇒ Operation now in progress
CONN (0.0591s) TCP localhost > 192.168.1.7:80 ⇒ Operation now in progress
CONN (0.0594s) TCP localhost > 192.168.1.8:80 ⇒ Operation now in progress
CONN (0.0596s) TCP localhost > 192.168.1.9:80 ⇒ Operation now in progress
CONN (0.0599s) TCP localhost > 192.168.1.10:80 ⇒ Operation now in progress
CONN (1.0587s) TCP localhost > 192.168.1.13:80 ⇒ Operation now in progress
CONN (1.0593s) TCP localhost > 192.168.1.14:80 ⇒ Operation now in progress
CONN (1.0596s) TCP localhost > 192.168.1.15:80 ⇒ Operation now in progress
CONN (1.0599s) TCP localhost > 192.168.1.16:80 ⇒ Operation now in progress
CONN (1.0602s) TCP localhost > 192.168.1.17:80 ⇒ Operation now in progress
CONN (1.0609s) TCP localhost > 192.168.1.20:80 ⇒ Operation now in progress
CONN (1.0612s) TCP localhost > 192.168.1.21:80 ⇒ Operation now in progress
CONN (1.0615s) TCP localhost > 192.168.1.22:80 ⇒ Operation now in progress
CONN (1.0618s) TCP localhost > 192.168.1.23:80 ⇒ Operation now in progress
CONN (1.0622s) TCP localhost > 192.168.1.24:80 ⇒ Operation now in progress
CONN (2.0655s) TCP localhost > 192.168.1.1:80 ⇒ Operation now in progress
CONN (2.0706s) TCP localhost > 192.168.1.2:80 ⇒ Operation now in progress
CONN (2.0707s) TCP localhost > 192.168.1.3:80 ⇒ Operation now in progress
CONN (2.0708s) TCP localhost > 192.168.1.4:80 ⇒ Operation now in progress
CONN (2.0719s) TCP localhost > 192.168.1.5:80 ⇒ Operation now in progress
CONN (2.0991s) TCP localhost > 192.168.1.6:80 ⇒ Operation now in progress
CONN (2.0992s) TCP localhost > 192.168.1.7:80 ⇒ Operation now in progress
CONN (2.0993s) TCP localhost > 192.168.1.8:80 ⇒ Operation now in progress
CONN (2.0993s) TCP localhost > 192.168.1.9:80 ⇒ Operation now in progress
CONN (2.0994s) TCP localhost > 192.168.1.10:80 ⇒ Operation now in progress
CONN (2.0995s) TCP localhost > 192.168.1.1:80 ⇒ Connected
```

nmap -sP 192.168.1.1/24 –disable-arp-ping

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sP 192.168.1.1/24 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 12:19 EST
Nmap scan report for 192.168.1.1
Host is up (0.010s latency).
Nmap scan report for 192.168.1.255
Host is up (0.017s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 16.05 seconds
```

Sudo nmap -O -osscan-guess 192.168.1.255

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -O -osscan-guess 192.168.1.255
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 12:23 EST
Nmap scan report for 192.168.1.255
Host is up (0.0016s latency).
Not shown: 999 closed ports
PORT    STATE    SERVICE
514/tcp filtered shell
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:4.4
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.03 seconds
```

Sudo nmap -O -PN 192.168.1.255

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -O -PN 192.168.1.255
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 12:27 EST
Nmap scan report for 192.168.1.255
Host is up (0.0029s latency).
Not shown: 999 closed ports
PORT    STATE    SERVICE
514/tcp filtered shell
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:4.4
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.31 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$
```