

Experiment 15

FAMILIARIZATION OF KALI LINUX

15.1 Aim

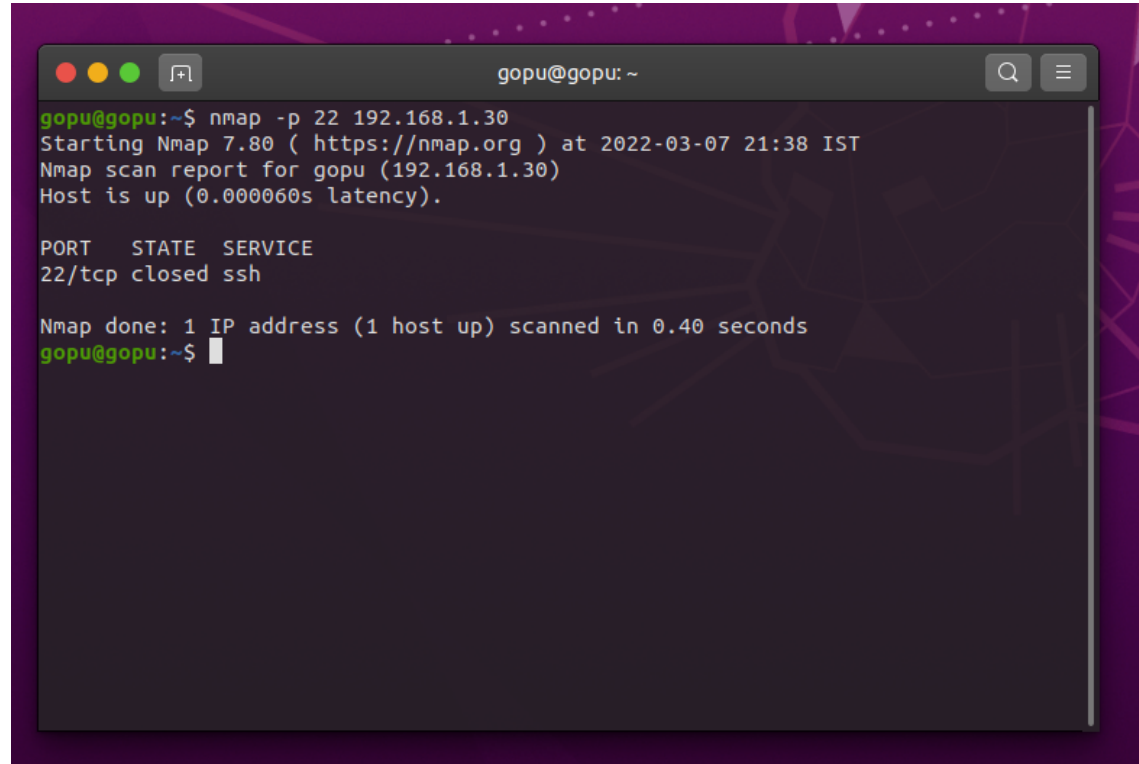
Familiarisation of KALI LINUX .

15.2 Theory

Kali Linux is an open-source, Debian based linux distro, focused on penetration testing , security research and various other computer forensics. It was developed by Mati Aharoni and Devon Kearns. Kali Linux is a specifically built operating system for network analysts, penetration testers, and those that work in the field of cybersecurity and analysis. Kali Linux's official website is Kali.org. It became well-known after appearing in the Mr. Robot television series. It is not intended for public usage; rather, it is intended for experts or individuals who are familiar with Linux/Kali.

Kali Linux has around 600 penetration-testing tools like nmap , wireshark, metasploit, etc.

15.3 Procedure

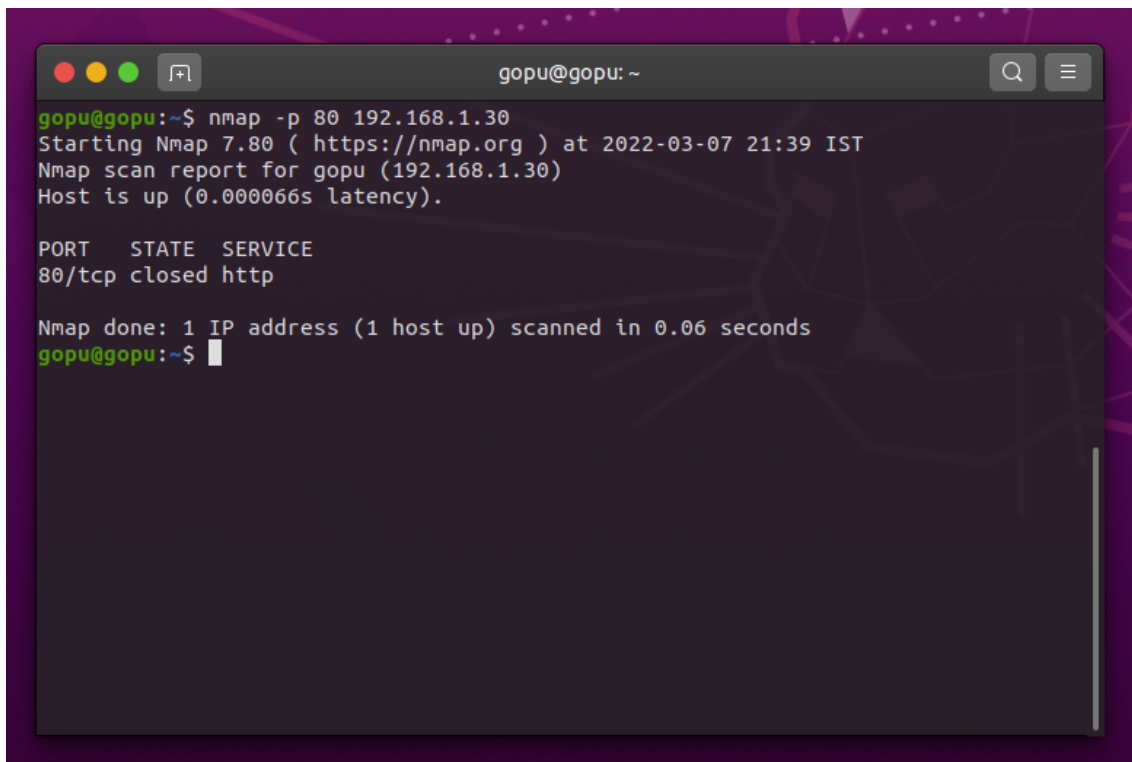
A screenshot of a terminal window in Kali Linux. The window title is 'gopu@gopu: ~'. The terminal shows the command 'nmap -p 22 192.168.1.30' being executed. The output indicates that Nmap 7.80 is starting at 2022-03-07 21:38 IST, and the scan report for 192.168.1.30 shows that port 22/tcp is closed and the service is ssh. The scan is completed in 0.40 seconds.

```
gopu@gopu:~$ nmap -p 22 192.168.1.30
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-07 21:38 IST
Nmap scan report for gopu (192.168.1.30)
Host is up (0.000060s latency).

PORT      STATE SERVICE
22/tcp    closed ssh

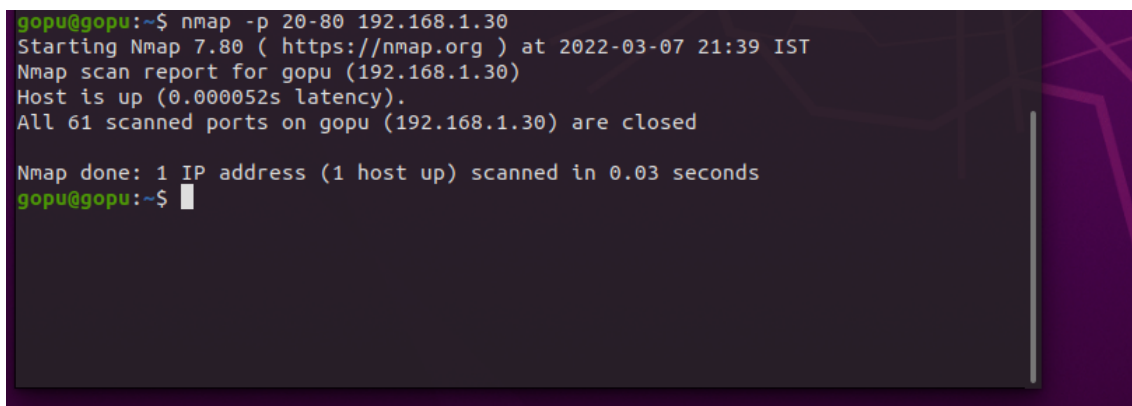
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
gopu@gopu:~$
```

Figure 1: nmap command checking port 22



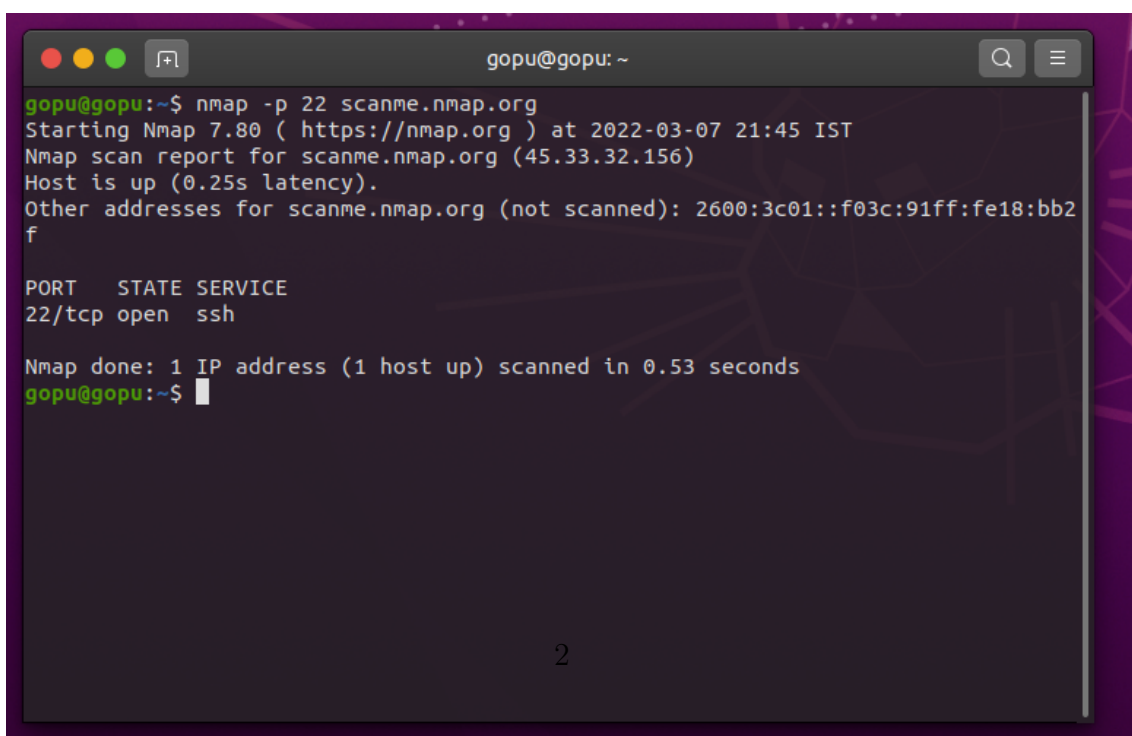
```
gopu@gopu: ~  
gopu@gopu:~$ nmap -p 80 192.168.1.30  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-07 21:39 IST  
Nmap scan report for gopu (192.168.1.30)  
Host is up (0.000066s latency).  
  
PORT      STATE SERVICE  
80/tcp    closed http  
  
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds  
gopu@gopu:~$
```

Figure 2: nmap command checking port 80



```
gopu@gopu:~$ nmap -p 20-80 192.168.1.30  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-07 21:39 IST  
Nmap scan report for gopu (192.168.1.30)  
Host is up (0.000052s latency).  
All 61 scanned ports on gopu (192.168.1.30) are closed  
  
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds  
gopu@gopu:~$
```

Figure 3: nmap command checking the ports ranging from 20 to 80



```
gopu@gopu: ~  
gopu@gopu:~$ nmap -p 22 scanme.nmap.org  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-07 21:45 IST  
Nmap scan report for scanme.nmap.org (45.33.32.156)  
Host is up (0.25s latency).  
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f  
  
PORT      STATE SERVICE  
22/tcp    open  ssh  
  
Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds  
gopu@gopu:~$
```

Figure 4: nmap command to check the port 22 on scanme.nmap.org

```
gopu@gopu: ~  
gopu@gopu:~$ nmap -A 192.168.1.30  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-07 21:41 IST  
Nmap scan report for gopu (192.168.1.30)  
Host is up (0.000070s latency).  
All 1000 scanned ports on gopu (192.168.1.30) are closed  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds  
gopu@gopu:~$
```

Figure 5: nmap -A command on scanme.nmap.org

```
gopu@gopu: ~  
gopu@gopu:~$ nmap -A scanme.nmap.org  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-07 21:46 IST  
Stats: 0:01:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 99.40% done; ETC: 21:48 (0:00:00 remaining)  
Nmap scan report for scanme.nmap.org (45.33.32.156)  
Host is up (0.35s latency).  
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f  
Not shown: 990 closed ports  
PORT      STATE      SERVICE      VERSION  
22/tcp    open      ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; proto  
col 2.0)  
| ssh-hostkey:  
| 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)  
| 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)  
| 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)  
|_ 256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)  
23/tcp    filtered  telnet  
25/tcp    open      tcpwrapped  
|_ smtp-comands: Couldn't establish connection on port 25  
80/tcp    open      http         Apache httpd 2.4.7 ((Ubuntu))  
|_ http-title: Go ahead and ScanMe!  
135/tcp   filtered  msrpc  
139/tcp   filtered  netbios-ssn  
445/tcp   filtered  microsoft-ds  
7007/tcp  filtered  afs3-bos  
9929/tcp  open      nping-echo   Nping echo  
31337/tcp open      tcpwrapped  
Service Info: OS: 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 115.42 seconds  
gopu@gopu:~$
```

Figure 6: nmap -A scanme.nmap.org

15.4 Result

Got Familiarized with Kali linux .