Application Security Lab

Name: Swanand Garge

Div : D(D2)

Roll no :42

SRN: 202201589

Q . ***Explore the variety of different nmap commands.***

1. Basic usage of nmap for *olacabs.com*

```
┌──(kali㉿kali)-[~]
└─$ nmap olacabs.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 02:19 EST
Nmap scan report for olacabs.com (108.159.61.98)
Host is up (0.0076s latency).
Other addresses for olacabs.com (not scanned): 108.159.61.100 108.159.61.22 108.159.61.26
rDNS record for 108.159.61.98: server-108-159-61-98.bom78.r.cloudfront.net
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
2000/tcp open  cisco-sccp
5060/tcp open  sip
8010/tcp open  xmpp

Nmap done: 1 IP address (1 host up) scanned in 4.95 seconds
```

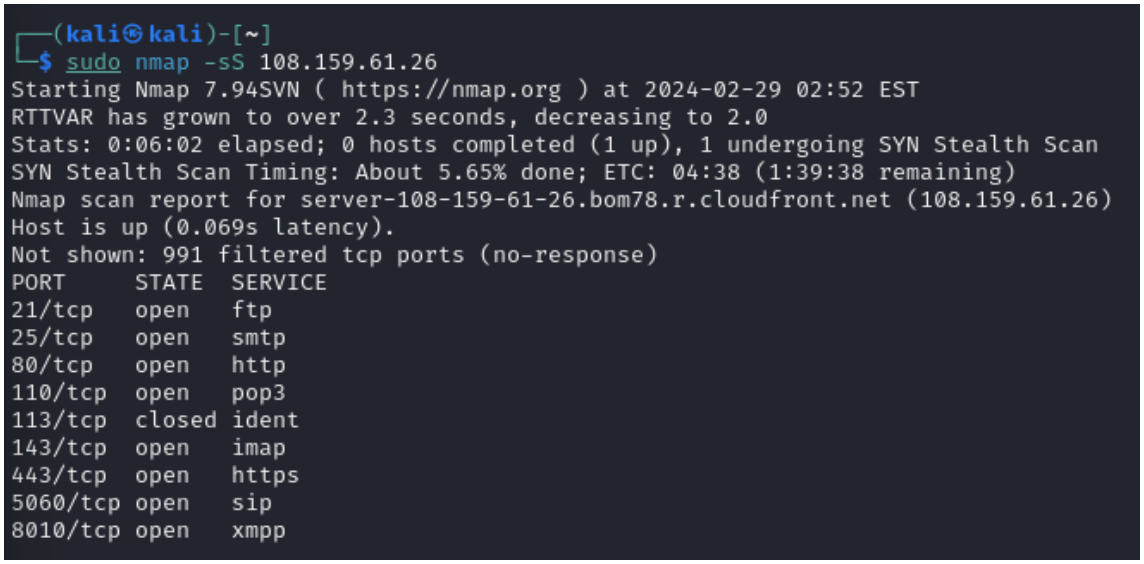
2. Using -sA and -O to get remote firewall setting and operating system information for *olacabs.com*

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sA -O olacabs.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 02:39 EST
Nmap scan report for olacabs.com (108.159.61.22)
Host is up (0.011s latency).
Other addresses for olacabs.com (not scanned): 108.159.61.98 108.159.61.26 108.159.61.100
rDNS record for 108.159.61.22: server-108-159-61-22.bom78.r.cloudfront.net
All 1000 scanned ports on olacabs.com (108.159.61.22) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: print server|webcam
Running: D-Link embedded, Hamlet embedded, TRENDnet embedded
OS CPE: cpe:/h:dlink:dp-300u cpe:/h:dlink:dp-g310 cpe:/h:hamlet:hps01uu cpe:/h:trendnet:tv-ip100
OS details: D-Link DP-300U, DP-G310, or Hamlet HPS01UU print server, TRENDnet TV-IP100 webcam

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.88 seconds
```

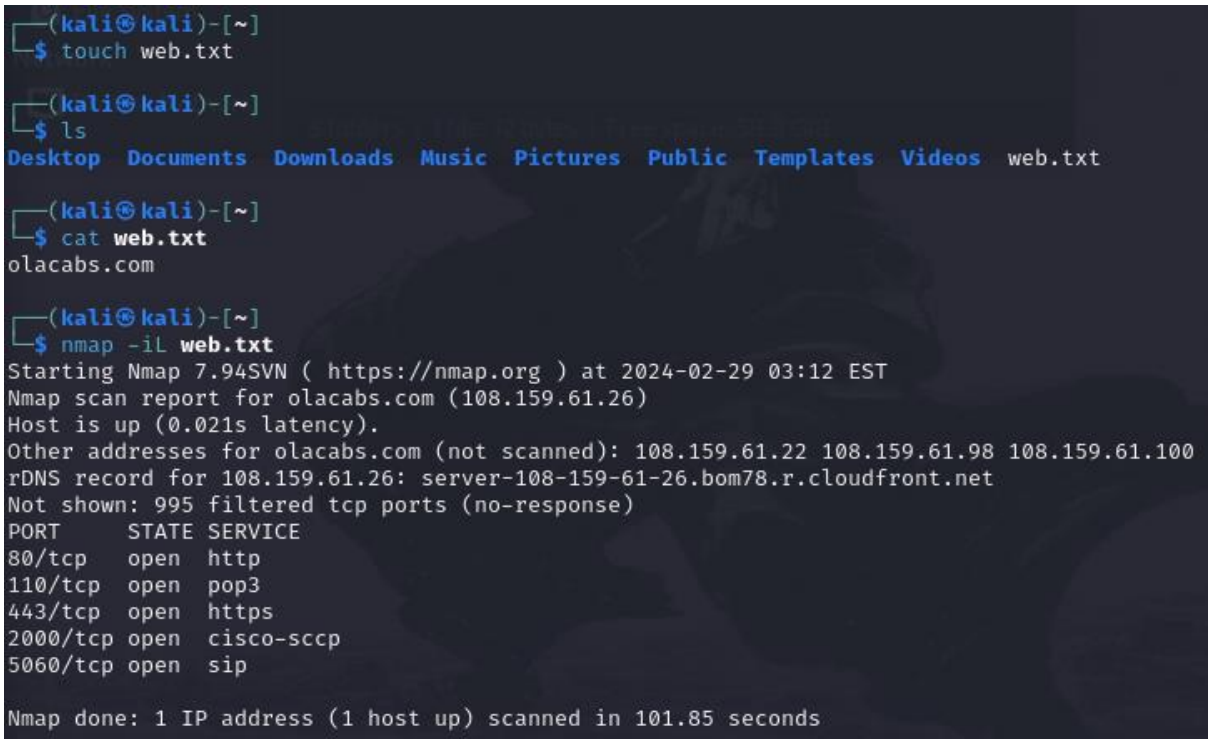
3. Using '-' to scan for range of IP addresses for *olacabs.com*

```
┌──(kali㉿kali)-[~]
└─$ nmap 108.159.61.26-28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 02:31 EST
Nmap scan report for server-108-159-61-26.bom78.r.cloudfront.net (108.159.61.26)
Host is up (0.082s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
110/tcp  open  pop3
443/tcp  open  https
2000/tcp open  cisco-sccp
5060/tcp open  sip
8010/tcp open  xmpp

Nmap scan report for server-108-159-61-27.bom78.r.cloudfront.net (108.159.61.27)
Host is up (0.014s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
110/tcp  open  pop3
443/tcp  open  https
2000/tcp open  cisco-sccp
5060/tcp open  sip
8010/tcp open  xmpp

Nmap scan report for server-108-159-61-28.bom78.r.cloudfront.net (108.159.61.28)
Host is up (0.013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
110/tcp  open  pop3
443/tcp  open  https
8010/tcp open  xmpp

Nmap done: 3 IP addresses (3 hosts up) scanned in 130.36 seconds
```

4. Using ‘-sS’ for stealthily scanning all the TCP SYN requests for *olacabs.com*



5. Using ‘-iL’ to give input via a text file for *olacabs.com*



6. Using ‘-p’ to scan for specific ports or range of ports for *olacabs.com*

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 7000-9000 olacabs.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 03:36 EST
Nmap scan report for olacabs.com (108.159.61.100)
Host is up (0.027s latency).
Other addresses for olacabs.com (not scanned): 108.159.61.22 108.159.61.26 108.159.61.98
rDNS record for 108.159.61.100: server-108-159-61-100.bom78.r.cloudfront.net
Not shown: 1999 filtered tcp ports (no-response)
PORT     STATE SERVICE
8015/tcp open  cfg-cloud
8020/tcp open  intu-ec-svcdisc

Nmap done: 1 IP address (1 host up) scanned in 6.81 seconds
```

7. Using ‘--trace’ to to trace the route to the target i.e for *olacabs.com*

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --trace olacabs.com
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 03:38 EST
Nmap scan report for olacabs.com (108.159.61.100)
Host is up (0.019s latency).
Other addresses for olacabs.com (not scanned): 108.159.61.98 108.159.61.22 108.159.61.26
rDNS record for 108.159.61.100: server-108-159-61-100.bom78.r.cloudfront.net
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
2000/tcp open  cisco-sccp
5060/tcp open  sip
8010/tcp open  xmpp

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   17.07 ms 10.0.2.2
2   17.14 ms server-108-159-61-100.bom78.r.cloudfront.net (108.159.61.100)

Nmap done: 1 IP address (1 host up) scanned in 5.02 seconds
```

8. Using ‘scan report’ to scan for all the hosts the IP i.e for *olacabs.com*

Conclusion:

In summary, various Nmap options were employed to gather information about olacabs.com. These included -sA and -O for firewall settings and OS detection, '-' for scanning a range of IP addresses, -sS for stealthy TCP SYN scanning, -iL for input via a text file, -p for specific or range of ports scanning, - trace for tracing the route to the target, and 'scan report' for scanning all hosts associated with the IP. These methods provide a comprehensive overview of olacabs.com's network and system configurations.