

ITA1443-Ethical Hacking For Legal Systems

Name: R.Surya

Reg.No:192011244

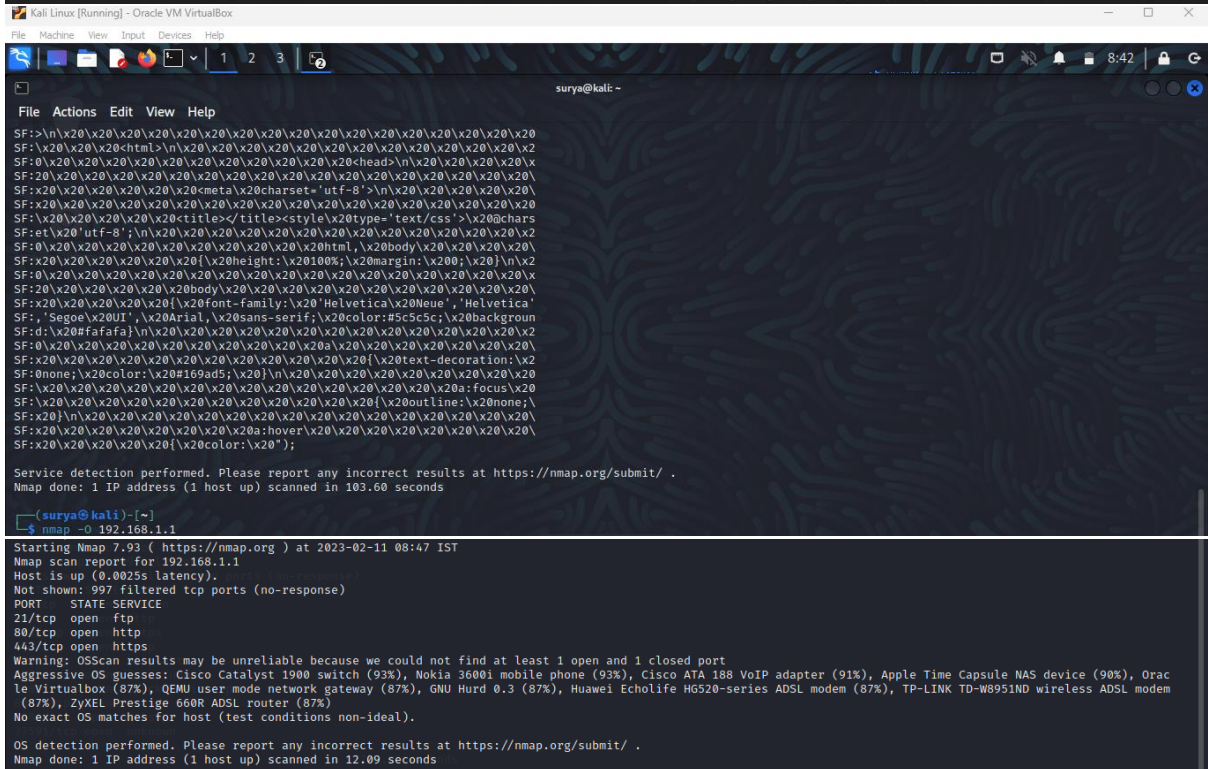
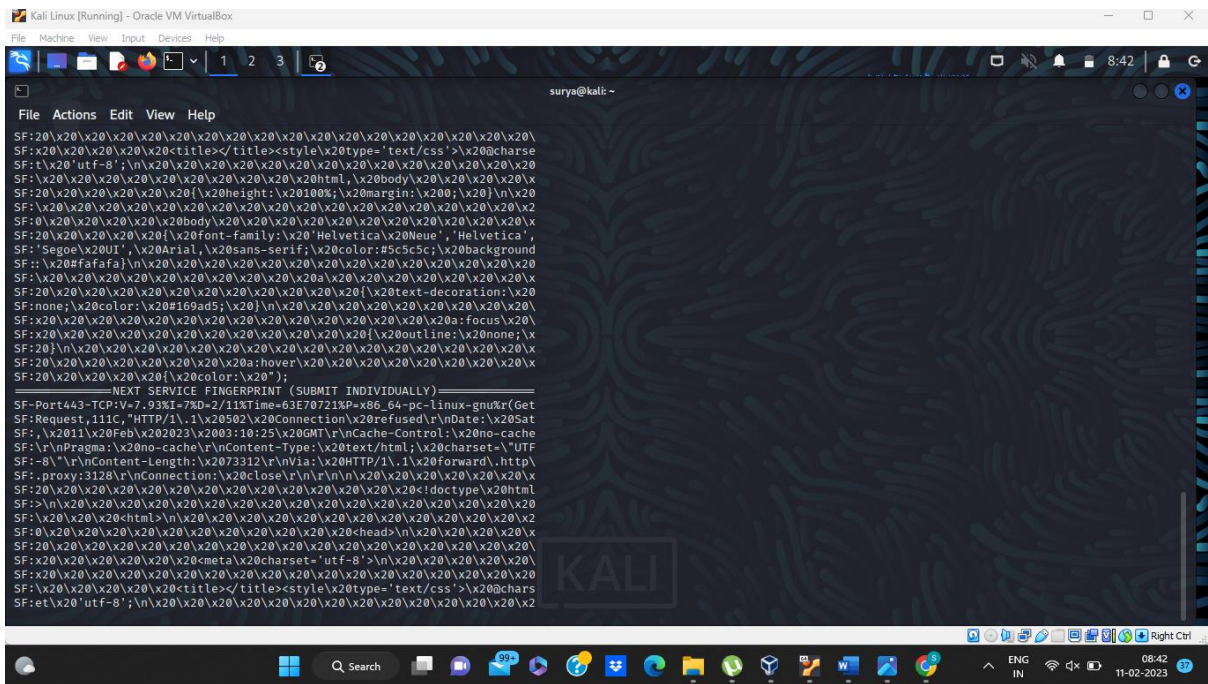
Slot: D

Exercise No 1: Nmap Scan

```
surya@kali: ~  
File Actions Edit View Help  
[surya@kali]~  
$ nmap -Pn 192.168.1.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 11:35 IST  
Nmap scan report for 192.168.1.1  
Host is up (0.12s latency).  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 99.86 seconds  
[surya@kali]~  
$ nmap -sn 192.168.1.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 11:38 IST  
Nmap scan report for 192.168.1.1  
Host is up (0.027s latency).  
Nmap done: 1 IP address (1 host up) scanned in 15.08 seconds  
[surya@kali]~  
$ nmap -PR 192.168.1.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 11:38 IST  
Nmap scan report for 192.168.1.1  
Host is up (0.040s latency).  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 61.00 seconds  
[surya@kali]~
```

```
[surya@kali]~  
$ nmap -n 192.168.1.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 11:42 IST  
Nmap scan report for 192.168.1.1  
Host is up (0.037s latency).  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 47.19 seconds
```

```
[surya@kali]~  
$ nmap -sV 192.168.1.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-10 13:42 IST  
Nmap scan report for 192.168.1.1  
Host is up (0.39s latency).  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE VERSION  
21/tcp    open  tcpwrapped  
80/tcp    open  tcpwrapped  
443/tcp   open  tcpwrapped  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 234.87 seconds  
[surya@kali]~  
$ nmap -p 1-30 192.168.1.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-10 13:55 IST  
Nmap scan report for 192.168.1.1  
Host is up (0.0056s latency).  
Not shown: 29 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
  
Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
```


```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
surya@kali: ~
File Actions Edit View Help
(surya@kali)-[~]
$ nmap -p- 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-10 18:29 IST
Nmap scan report for 192.168.1.1
Host is up (0.0097s latency).
Not shown: 65525 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
8000/tcp  open  http-alt
8001/tcp  open  vcom-tunnel
8081/tcp  open  blackice-icecap
8083/tcp  open  us-srv
8084/tcp  open  websnp
37591/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13748.34 seconds

(surya@kali)-[~]
$ nmap -F 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 08:30 IST
Nmap scan report for 192.168.1.1
Host is up (0.020s latency).
Not shown: 97 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 2.06 seconds
```

```
(surya@kali)-[~]
$ nmap -sT 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-10 14:11 IST
Nmap scan report for 192.168.1.1
Host is up (0.0089s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 70.02 seconds
```

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
surya@kali: ~
File Actions Edit View Help
(surya@kali)-[~]
$ nmap -T3 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 08:58 IST
Nmap scan report for 192.168.1.1
Host is up (0.0070s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 41.13 seconds

(surya@kali)-[~]
$ nmap -T4 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 08:59 IST
Nmap scan report for 192.168.1.1
Host is up (0.0066s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https

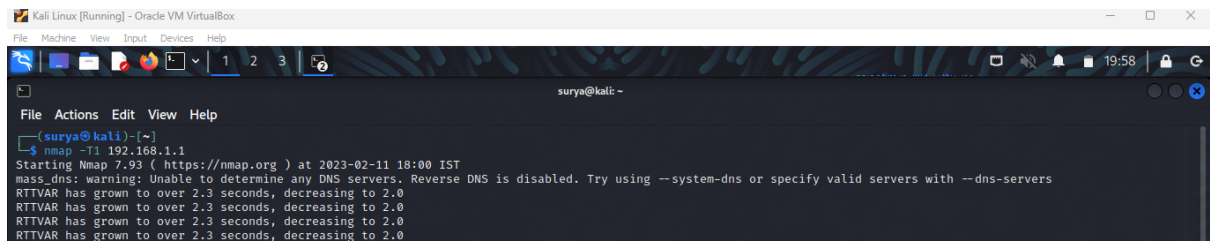
Nmap done: 1 IP address (1 host up) scanned in 36.03 seconds

(surya@kali)-[~]
$ nmap -T5 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 08:59 IST
Nmap scan report for 192.168.1.1
Host is up (0.0062s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 2192.69 seconds
```

```
(surya@kali)-[~]
$ nmap -T2 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 08:56 IST
Nmap scan report for 192.168.1.1
Host is up (0.010s latency).
Not shown: 997 filtered tcp ports (no-response), 2 filtered tcp ports (net-unreach)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 2192.69 seconds
```



The image shows a terminal window titled "Kali Linux [Running] - Oracle VM VirtualBox". The terminal displays the output of the command `nmap -T1 192.168.1.1`. The output includes the Nmap version (7.93), the start time (2023-02-11 18:00 IST), and a warning about DNS servers. It also shows three instances of the message "RTTVar has grown to over 2.3 seconds, decreasing to 2.0".

```
(surya@kali)-[~]  
$ nmap -T1 192.168.1.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 18:00 IST  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers  
RTTVar has grown to over 2.3 seconds, decreasing to 2.0  
RTTVar has grown to over 2.3 seconds, decreasing to 2.0  
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
```