

# ITA1443-Ethical Hacking For Legal Systems

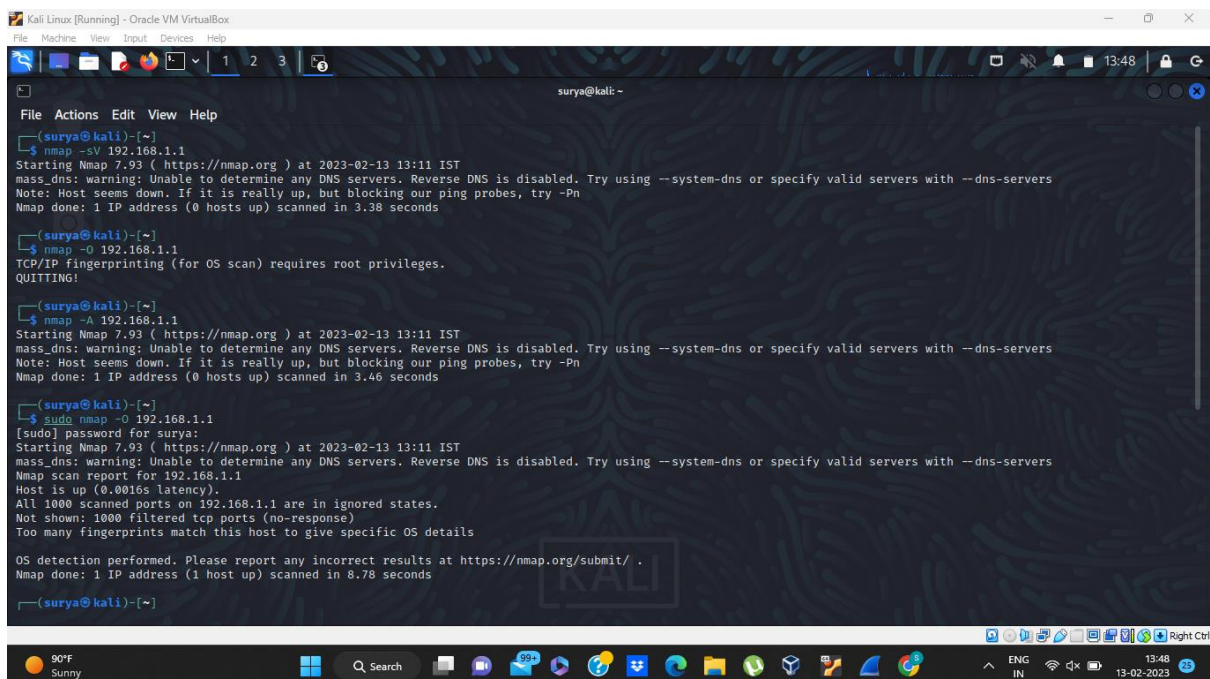
## Model Practical Examination

Name:R.Surya

RegNo:192011244

Slot:D

QUS1:



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

surya@kali: ~
File Actions Edit View Help

(surya@kali)-[~]
$ nmap -sV 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-13 13:11 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
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.38 seconds

(surya@kali)-[~]
$ nmap -O 192.168.1.1
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!

(surya@kali)-[~]
$ nmap -A 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-13 13:11 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
Note: Host seems down. If it is up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.46 seconds

(surya@kali)-[~]
$ sudo nmap -O 192.168.1.1
[sudo] password for surya:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-13 13:11 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
Nmap scan report for 192.168.1.1
Host is up (0.0016s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.78 seconds

(surya@kali)-[~]
```