

# MODEL PRACTICAL EXAMINATION

NAME: BALA MANOHAR JAVVAJI

REG NO: 192124133

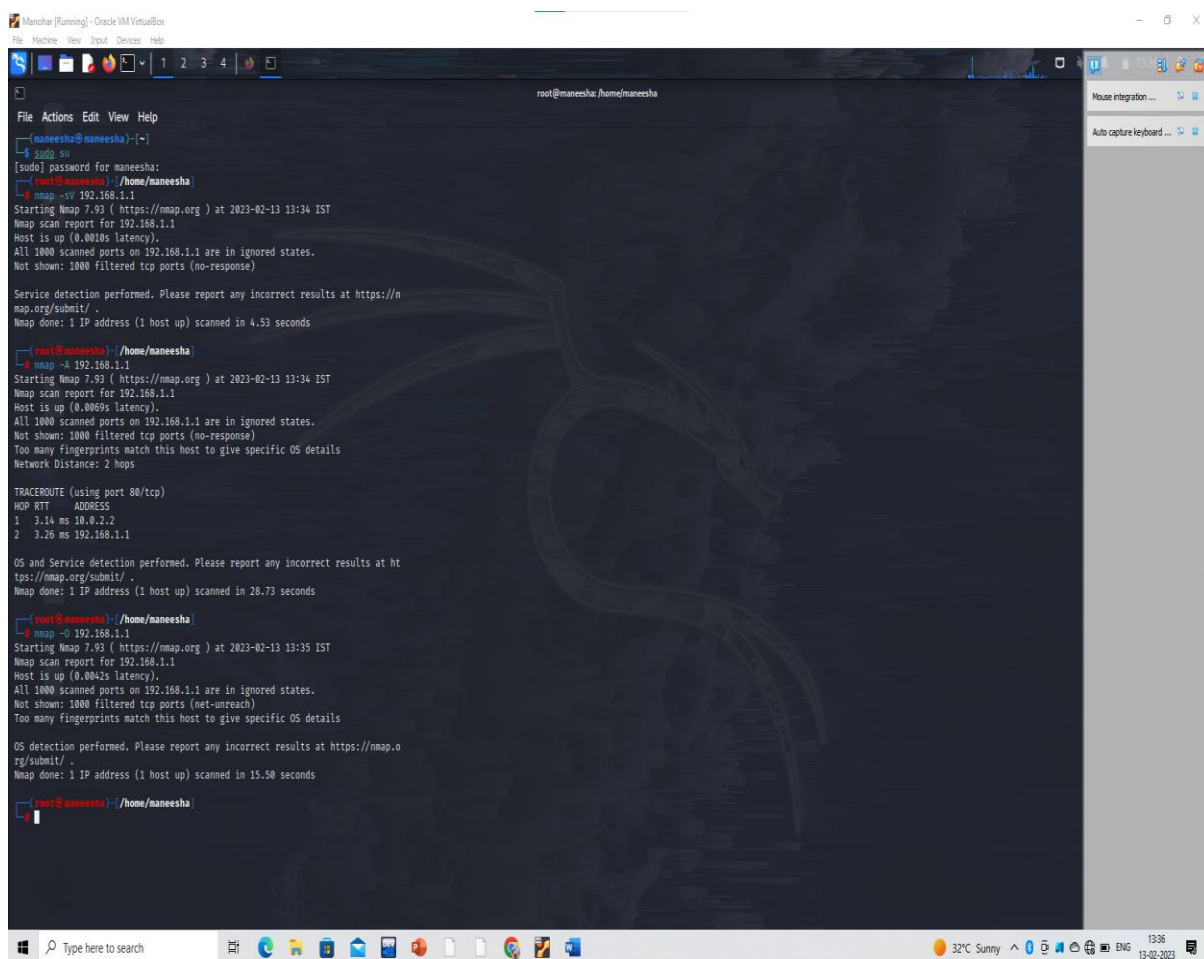
DEPT: AI&DS

COURSE CODE: ITA1443

COURSE: ETHICAL HACKING FOR LEGAL  
PRACTICES

1. To execute the following Nmap service version and OS detection commands in Kali Linux operating Systems.

- (i) detect the version of services running
- (ii) aggressive scan
- (iii) detect operating system of the target



```
Manohar [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@manesha: /home/manesha

manesha@manesha:~$ sudo su
[sudo] password for manesha:
root@manesha:~# nmap -sV 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-13 13:34 IST
Nmap scan report for 192.168.1.1
Host is up (0.0018s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.53 seconds

root@manesha:~# nmap -A 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-13 13:34 IST
Nmap scan report for 192.168.1.1
Host is up (0.0069s 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
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 3.14 ms 10.0.2.2
2 3.26 ms 192.168.1.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.73 seconds

root@manesha:~# nmap -O 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-13 13:35 IST
Nmap scan report for 192.168.1.1
Host is up (0.0042s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (net-unreach)
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 15.50 seconds

root@manesha:~#
```

## 2.To Implement the Boot Sector Virus in The Kali Linux Operating System

```
root@DESKTOP-O109TSU:~  
File Actions Edit View Help  
root@DESKTOP-O109TSU:~  
root@DESKTOP-O109TSU:~# msfvenom  
Error: No options  
MsfVenom - a Metasploit standalone payload generator.  
Also a replacement for msfpayload and msfencode.  
Usage: /usr/bin/msfvenom [options] <var=val>  
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe  
  
Options:  
-l, --list <type> List all modules for [type]. Types are: payloads, encoders, nops, platforms,  
-p, --payload <payload> Payload to use (--list payloads to list, --list-options for arguments). Speci  
--list-options List --payload <value>'s standard, advanced and evasion options  
-f, --format <format> Output format (use --list formats to list)  
-e, --encoder <encoder> The encoder to use (use --list encoders to list)  
--sec-name <value> The new section name to use when generating large Windows binaries. Default:  
--smallest Generate the smallest possible payload using all available encoders  
--encrypt <value> The type of encryption or encoding to apply to the shellcode (use --list encr  
--encrypt-key <value> A key to be used for --encrypt  
--encrypt-iv <value> An initialization vector for --encrypt  
-a, --arch <arch> The architecture to use for --payload and --encoders (use --list archs to lis  
--platform <platform> The platform for --payload (use --list platforms to list)  
-o, --out <path> Save the payload to a file  
-b, --bad-chars <list> Characters to avoid example: '\x00\xff'  
-n, --nopsled <length> Prepend a nopsled of [length] size on to the payload  
--pad-nops Use nopsled size specified by -n <length> as the total payload size, auto-pre  
-s, --space <length> The maximum size of the resulting payload  
--encoder-space <length> The maximum size of the encoded payload (defaults to the -s value)  
-i, --iterations <count> The number of times to encode the payload  
-c, --add-code <path> Specify an additional win32 shellcode file to include  
-x, --template <path> Specify a custom executable file to use as a template  
-k, --keep Preserve the --template behaviour and inject the payload as a new thread  
-v, --var-name <value> Specify a custom variable name to use for certain output formats  
-t, --timeout <second> The number of seconds to wait when reading the payload from STDIN (default 30  
-h, --help Show this message  
root@DESKTOP-O109TSU:~# msfvenom
```

3. Ram is a network administrator for a large enterprise and he have been experiencing some network performance issues. His goal is to analyze the network packet transmission using a packet analyzer tool to identify the cause of the problem.

The screenshot displays a network packet analyzer (Wireshark) interface. The top pane shows a list of captured packets, including HTTP requests and responses. The middle pane shows the details of the selected packet (Frame 12616), which is an HTTP request to the URL `http://ocsp.digicert.com/`. The bottom pane shows the raw packet data in hexadecimal and ASCII. In the background, a web browser window is visible, showing the login page of Saveetha University. The login form has fields for username and password, and a "LOGIN" button. A message below the form states: "The username and password you entered is invalid".

No.	Time	Source	Destination	Protocol	Length	Info
4559	133.190415	180.235.121.242	192.168.31.34	HTTP	1183	HTTP/1.1 200 OK (text/css)
4560	133.191983	192.168.31.34	180.235.121.242	HTTP	568	GET /assets/global/css/components.css HTTP/1.1
4563	133.197297	192.168.31.34	180.235.121.242	HTTP	557	GET /assets/global/css/plugins.css HTTP/1.1
4613	133.927741	192.168.31.34	180.235.121.242	HTTP	562	GET /assets/admin/layout/css/layout.css HTTP/1.1
4650	134.057442	180.235.121.242	192.168.31.34	HTTP	1149	HTTP/1.1 200 OK (text/css)
4651	134.058016	192.168.31.34	180.235.121.242	HTTP	571	GET /assets/admin/layout/css/themes/darkblue.css HTTP/1.1
4867	138.037994	192.168.31.34	180.235.121.242	HTTP	562	GET /assets/admin/layout/css/custom.css HTTP/1.1
4882	138.425196	180.235.121.242	192.168.31.34	HTTP	783	HTTP/1.1 200 OK (text/css)
5358	154.541813	192.168.31.34	180.235.121.242	HTTP	609	GET / HTTP/1.1
5366	154.650294	192.168.31.34	180.235.121.242	HTTP	505	GET /assets/global/css/plugins.css HTTP/1.1
5367	154.659466	192.168.31.34	180.235.121.242	HTTP	510	GET /assets/admin/layout/css/custom.css HTTP/1.1
5373	154.761243	192.168.31.34	180.235.121.242	HTTP	565	GET /assets/admin/layout/css/layout.css HTTP/1.1
5383	155.416102	180.235.121.242	192.168.31.34	HTTP	350	HTTP/1.1 206 Partial Content (text/css)
5384	155.418086	192.168.31.34	180.235.121.242	HTTP	565	GET /assets/admin/layout/css/layout.css HTTP/1.1
5398	155.887859	180.235.121.242	192.168.31.34	HTTP	1144	HTTP/1.1 200 OK (text/html)
5664	167.168391	192.168.31.34	180.235.121.242	HTTP	497	GET /assets/global/plugins/respond.min.js HTTP/1.1
6511	190.756726	180.235.121.242	192.168.31.34	HTTP	354	HTTP/1.1 200 OK (text/css)
12615	589.690682	192.168.31.34	117.18.237.29	OCSP	470	Request
12616	589.691858	192.168.31.34	117.18.237.29	OCSP	470	Request
12618	589.748764	117.18.237.29	192.168.31.34	OCSP	853	Response
12656	592.499295	117.18.237.29	192.168.31.34	OCSP	815	Response
12894	599.209933	192.168.31.34	49.44.116.239	OCSP	469	Request
12895	599.210149	192.168.31.34	49.44.116.239	OCSP	469	Request
12897	599.257955	49.44.116.239	192.168.31.34	OCSP	943	Response
12906	599.524645	49.44.116.239	192.168.31.34	OCSP	943	Response

Frame 12616: 470 bytes on wire (3760 bits), 470 bytes captured (0) on interface 0  
Ethernet II, Src: IntelCor\_ff:fa:8f (2c:8d:bf:fa:8f), Dst: 2e:8b:12:18:23:72  
Internet Protocol Version 4, Src: 192.168.31.34, Dst: 117.18.237.29  
Transmission Control Protocol, Src Port: 63488, Dst Port: 80, Seq: 354884800, Win: 65535, Len: 0  
Hypertext Transfer Protocol  
POST / HTTP/1.1  
Host: ocsp.digicert.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20180307 Firefox/102.0  
Accept: \*/\*  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Content-Type: application/ocsp-request  
Content-Length: 83  
Connection: keep-alive  
Cache-Control: no-cache  
[Full request URI: http://ocsp.digicert.com/]  
[HTTP request 1/1]  
File Data: 83 bytes  
Online Certificate Status Protocol

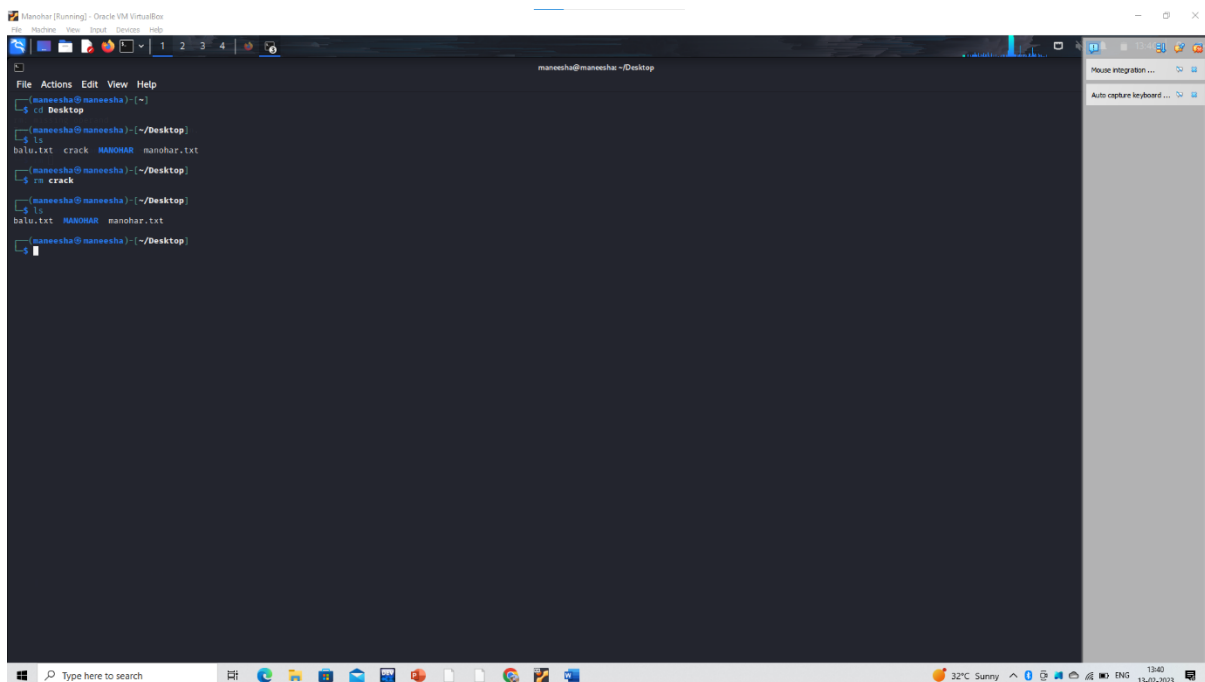
4.To execute the following commands in Kali Linux Operating Systems.

rm command

Users Command

Tree command

(i) rm Command

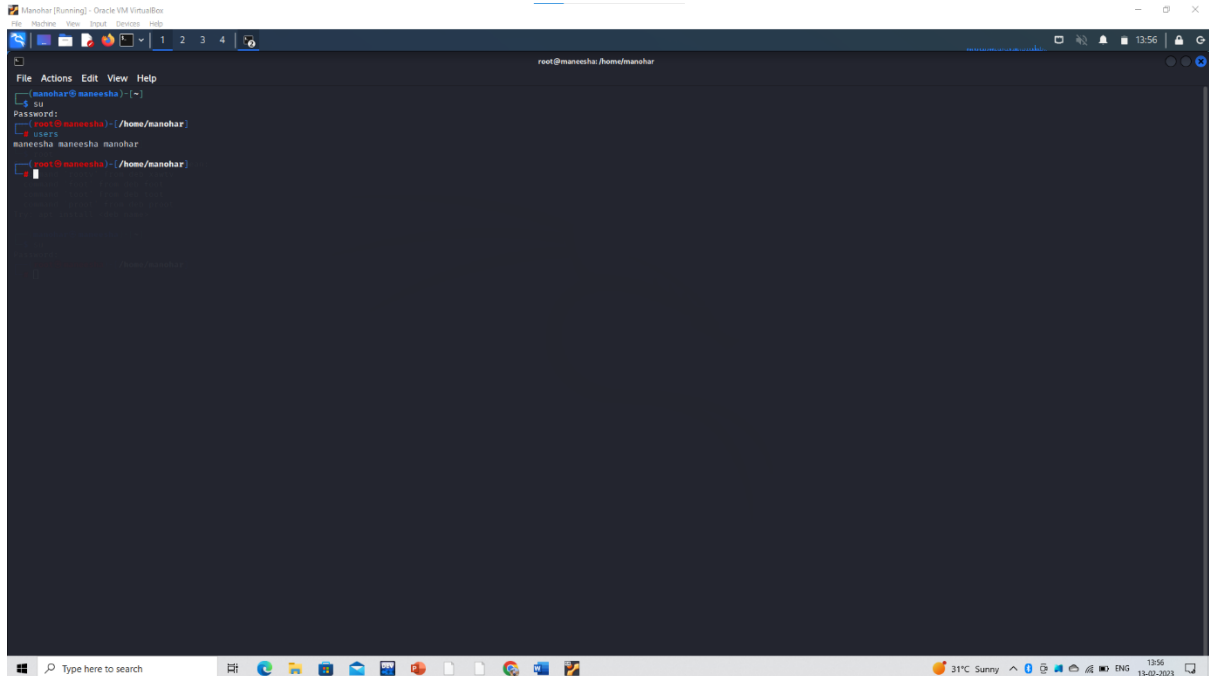


The screenshot shows a terminal window titled "Manohar [Running] - Oracle VM VirtualBox". The terminal output is as follows:

```
maneesha@maneesha:~/Desktop
$ cd Desktop
maneesha@maneesha:~/Desktop
$ ls
balu.txt  crack  MANOHAR  manohar.txt
maneesha@maneesha:~/Desktop
$ rm crack
maneesha@maneesha:~/Desktop
$ ls
balu.txt  MANOHAR  manohar.txt
maneesha@maneesha:~/Desktop
```

The terminal window is running on a Kali Linux virtual machine. The user has navigated to the Desktop directory and listed the files. They then executed the `rm crack` command, which successfully removed the file. The subsequent `ls` command confirms that the file is no longer present.

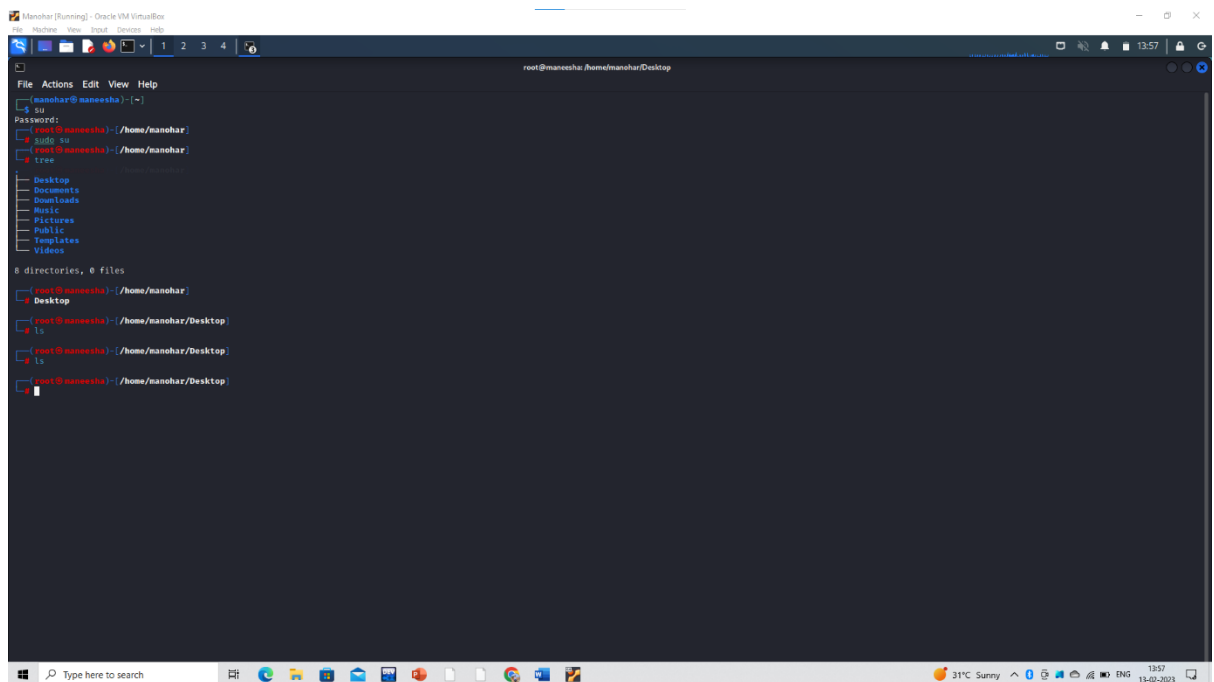
## (ii) users Command



A screenshot of a terminal window titled "Manohar [Running] - Oracle VM VirtualBox". The terminal shows a user named "manohar" at the prompt "manohar@manesha:~". The user enters the command "su", followed by "root@manesha:~/home/manohar". Then, the user enters "users", and the output is "manesha manesha manohar". The terminal window has a menu bar with "File", "Actions", "Edit", "View", and "Help". The status bar at the bottom shows "31°C Sunny" and the date "13-02-2023".

```
manohar@manesha:~$ su
root@manesha:~/home/manohar# users
manesha manesha manohar
root@manesha:~/home/manohar#
```

## (iii) Tree Command



A screenshot of a terminal window titled "Manohar [Running] - Oracle VM VirtualBox". The terminal shows a user named "manohar" at the prompt "manohar@manesha:~". The user enters the command "su", followed by "root@manesha:~/home/manohar". Then, the user enters "tree", and the output is a directory tree structure. The terminal window has a menu bar with "File", "Actions", "Edit", "View", and "Help". The status bar at the bottom shows "31°C Sunny" and the date "13-02-2023".

```
manohar@manesha:~$ su
root@manesha:~/home/manohar# tree
.
├── Desktop
├── Documents
├── Downloads
├── Music
├── Pictures
├── Public
├── Templates
└── Videos

0 directories, 0 files
root@manesha:~/home/manohar# cd Desktop
root@manesha:~/home/manohar/Desktop$ ls
root@manesha:~/home/manohar/Desktop$ ls
root@manesha:~/home/manohar/Desktop$
```