Ethical Hacking

List of Experiments

1. Execute and display the results for the following commands in Kali Linux Operating Systems:

rm command

users command

tree command

```
┌──(kali㉿kali)-[~]
└─$ tree
.
├── Desktop
├── Documents
├── Downloads
├── Music
├── Pictures
└── Public
```

2. Execute and display the results for the following commands in Kali Linux Operating Systems:

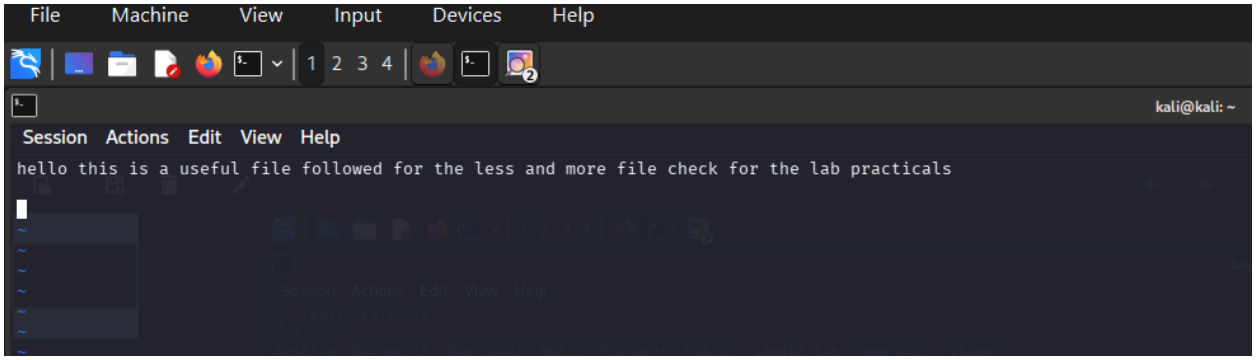
less command

```
┌──(kali㉿kali)-[~]
└─$ less sample.txt
```

more command

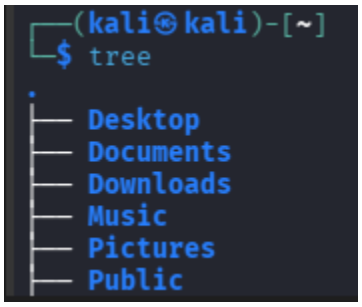
```
┌──(kali㉿kali)-[~]
└─$ more sample.txt
hello this is a useful file followed for the less and more file check for the lab practicals
```

vi command

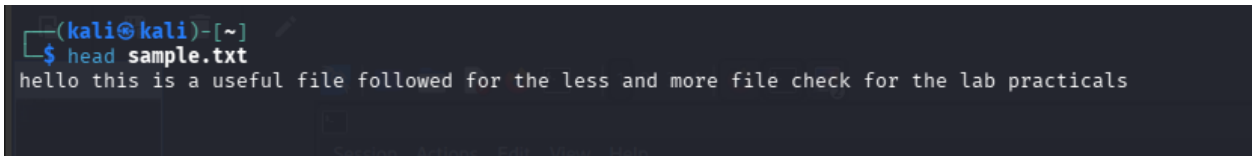


3. Execute and display the results for the following commands in Kali Linux Operating Systems:

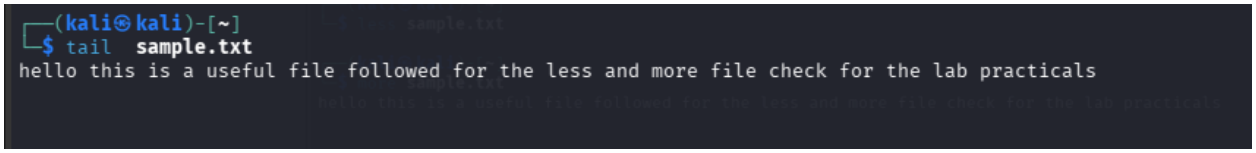
Tree



Head

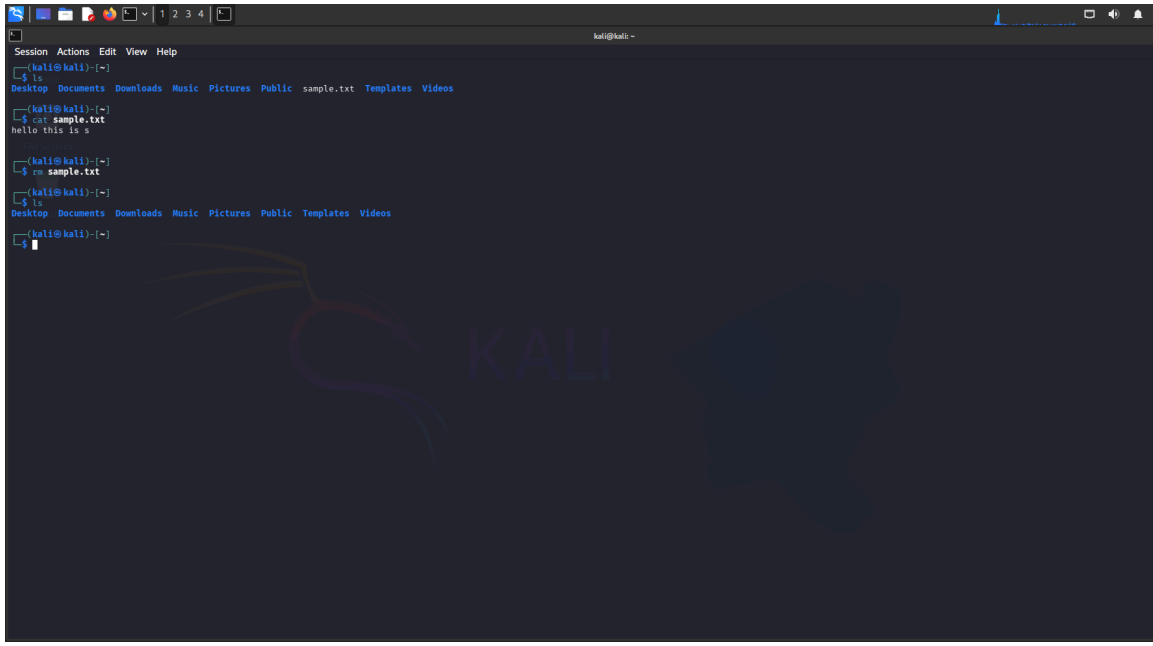


Tail

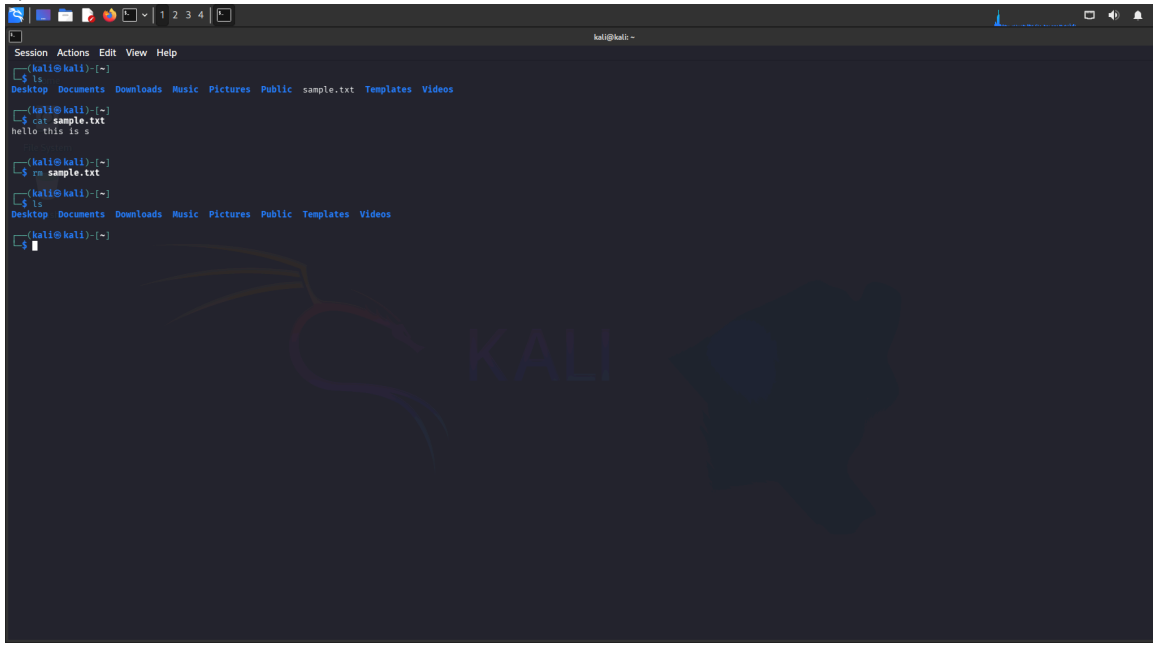


4. Execute and display the results for the following commands in Kali Linux Operating Systems:

i) Ls



ii) Cat



iii) Mkdir

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  sample.txt  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ mkdir practicals

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  practicals  Public  sample.txt  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ cd practicals

┌──(kali㉿kali)-[~/practicals]
└─$
```

5. Execute and display the results for the following commands in Kali Linux Operating Systems:

i) Uptime

```
┌──(kali㉿kali)-[~/practicals]
└─$ uptime
 05:03:30 up  2:04,  1 user,  load average: 0.21, 0.17, 0.11

┌──(kali㉿kali)-[~/practicals]
└─$
```

ii) Date

```
┌──(kali㉿kali)-[~/practicals]
└─$ date
Mon Dec 22 05:04:35 AM EST 2025
```

iii) Mv

```
Desktop  Documents  Downloads  Music  Pictures  practicals  Public  sample.txt  Templates

┌──(kali㉿kali)-[~]
└─$ mv sample.txt practicals

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  practicals  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ cd practicals

┌──(kali㉿kali)-[~/practicals]
└─$ ls
sample.txt

┌──(kali㉿kali)-[~/practicals]
└─$ mv sample.txt practical_sample_file.txt

┌──(kali㉿kali)-[~/practicals]
└─$ ls
practical_sample_file.txt

┌──(kali㉿kali)-[~/practicals]
└─$ pwd
/home/kali/practicals

┌──(kali㉿kali)-[~/practicals]
└─$
```

6. Execute and display the results for the following commands in Kali Linux Operating Systems:

i) Touch

ii) Pwd


```
Desktop  Documents  Downloads  Music  Pictures  practicals  Public  sample.txt  Templates

┌──(kali㉿kali)-[~]
└─$ mv sample.txt practicals

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  practicals  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ cd practicals

┌──(kali㉿kali)-[~/practicals]
└─$ ls
sample.txt

┌──(kali㉿kali)-[~/practicals]
└─$ mv sample.txt practical_sample_file.txt

┌──(kali㉿kali)-[~/practicals]
└─$ ls
practical_sample_file.txt

┌──(kali㉿kali)-[~/practicals]
└─$ pwd
/home/kali/practicals

┌──(kali㉿kali)-[~/practicals]
└─$
```


iii) Wget

```
┌──(kali㉿kali)-[~/practicals]
└─$ wget google.com
Prepended http:// to 'google.com'
--2025-12-22 05:18:52--  http://google.com/
Resolving google.com (google.com)... 142.251.222.142, 2404:6800:4007:82f::200e
Connecting to google.com (google.com)|142.251.222.142|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.google.com/ [following]
--2025-12-22 05:18:52--  http://www.google.com/
Resolving www.google.com (www.google.com)... 172.217.24.132, 2404:6800:4009:814::2004
Connecting to www.google.com (www.google.com)|172.217.24.132|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html.1'

index.html.1                                            [ <=>

2025-12-22 05:18:53 (177 KB/s) - 'index.html.1' saved [20072]


┌──(kali㉿kali)-[~/practicals]
└─$ ls
index.html  index.html.1  practical_sample_file.txt

┌──(kali㉿kali)-[~/practicals]
└─$
```

7. Execute and display the results for the following commands in Kali Linux Operating Systems:

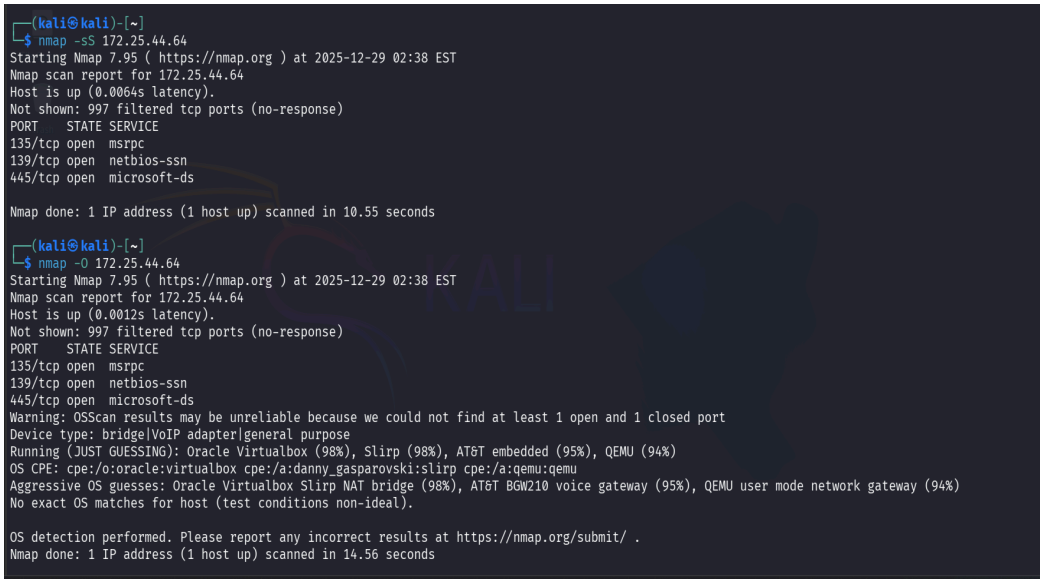
Cd

```
┌──(kali㉿kali)-[~/practicals]
└─$ ls
index.html  index.html.1  practical_sample_file.txt

┌──(kali㉿kali)-[~/practicals]
└─$ mkdir trailofsubfolder

┌──(kali㉿kali)-[~/practicals]
└─$ ls
index.html  index.html.1  practical_sample_file.txt  trailo

┌──(kali㉿kali)-[~/practicals]
└─$ cd trailofsubfolder

┌──(kali㉿kali)-[~/practicals/trailofsubfolder]
└─$ cd

┌──(kali㉿kali)-[~]
└─$ cd practicals

┌──(kali㉿kali)-[~/practicals]
└─$ cd trailofsubfolder

┌──(kali㉿kali)-[~/practicals/trailofsubfolder]
└─$ cd ..

┌──(kali㉿kali)-[~/practicals]
└─$ cd trailofsubfolder

┌──(kali㉿kali)-[~/practicals/trailofsubfolder]
└─$ cd ...
cd: no such file or directory: ...

┌──(kali㉿kali)-[~/practicals/trailofsubfolder]
└─$ cd .

┌──(kali㉿kali)-[~/practicals/trailofsubfolder]
└─$ cd ..
```

Cp
ls

8. Execute and display the results for 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

```
└─$ nmap -A 172.25.44.64
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-29 02:39 EST
Nmap scan report for 172.25.44.64
Host is up (0.00071s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (94%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210 voice gateway (94%), QEMU user mode network gateway (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-12-29T07:40:32
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: 1s

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.81 ms 172.25.44.64

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 35.17 seconds

┌──(kali㉿kali)-[~]
└─$
```

9. Execute and display the results for the following Nmap Timing and performance commands in Kali Linux operating Systems:

(i) polite IDS evasion

(ii) normal IDS evasion

```
┌──(kali㉿kali)-[~]
└─$ nmap -T2 172.25.44.64
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-29 02:57 EST
Nmap scan report for 172.25.44.64
Host is up (0.090s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 28.16 seconds

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ nmap -T3 172.25.44.64
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-29 02:58 EST
Nmap scan report for 172.25.44.64
Host is up (0.0024s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 14.96 seconds
```

10. To execute the following commands in Kali Linux Operating Systems:

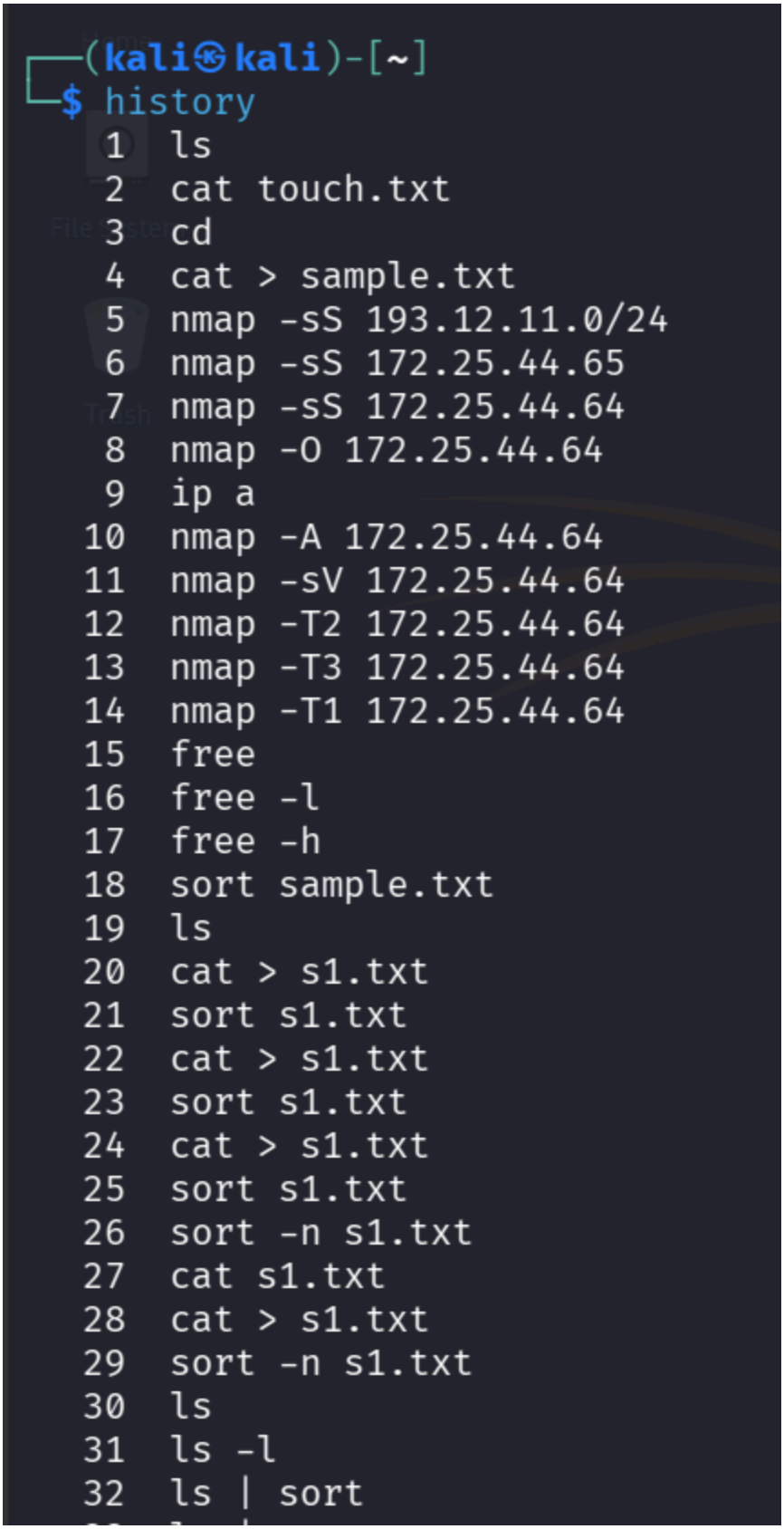
Free command

```
┌──(kali㉿kali)-[~]
└─$ free
               total        used        free      shared  buff/cache   available
Mem:         3033964      910692     1780224       22888      514176     2123272
Swap:         976556           0      976556

┌──(kali㉿kali)-[~]
└─$ free -l
               total        used        free      shared  buff/cache   available
Mem:         3033964      911204     1779624       22888      514188     2122760
Low:         3033964     1254340     1779624
High:              0           0           0
Swap:         976556           0      976556

┌──(kali㉿kali)-[~]
└─$ free -h
               total        used        free      shared  buff/cache   available
Mem:           2.9Gi       890Mi       1.7Gi        22Mi       502Mi       2.0Gi
Swap:          953Mi          0B       953Mi
```

Sort command

```
┌──(kali㉿kali)-[~]
└─$ cat > s1.txt
zat
bar
tar
are
neo

┌──(kali㉿kali)-[~]
└─$ sort -n s1.txt
are
bar
neo
tar
zat
```

History command


┌──(kali㉿kali)-[~]
└─$ history
1 ls
2 cat touch.txt
3 cd
4 cat > sample.txt
5 nmap -sS 193.12.11.0/24
6 nmap -sS 172.25.44.65
7 nmap -sS 172.25.44.64
8 nmap -O 172.25.44.64
9 ip a
10 nmap -A 172.25.44.64
11 nmap -sV 172.25.44.64
12 nmap -T2 172.25.44.64
13 nmap -T3 172.25.44.64
14 nmap -T1 172.25.44.64
15 free
16 free -l
17 free -h
18 sort sample.txt
19 ls
20 cat > s1.txt
21 sort s1.txt
22 cat > s1.txt
23 sort s1.txt
24 cat > s1.txt
25 sort s1.txt
26 sort -n s1.txt
27 cat s1.txt
28 cat > s1.txt
29 sort -n s1.txt
30 ls
31 ls -l
32 ls | sort

11. Execute and display the results for the following Nmap Timing and performance commands in Kali Linux operating Systems:

(i) aggressive speed scan

(ii) insane speed scan

```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 172.25.44.64
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-29 03:14 EST
Nmap scan report for 172.25.44.64
Host is up (0.0024s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 10.73 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -T5 172.25.44.64
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-29 03:14 EST
Nmap scan report for 172.25.44.64
Host is up (0.0011s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 9.08 seconds
```

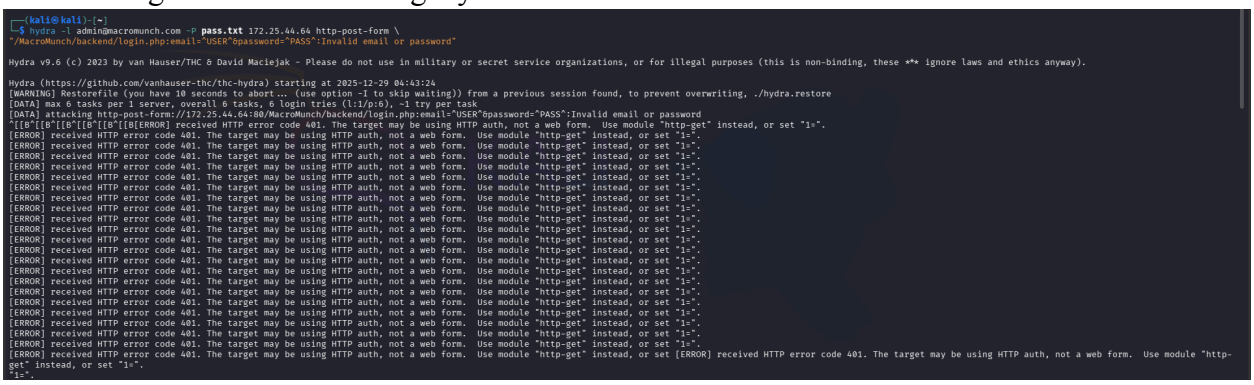
12. Port Scanning Tools

```
┌──(kali㉿kali)-[~]
└─$ nmap -P 172.25.44.64
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-29 03:18 EST
Nmap scan report for 172.25.44.64
Host is up (0.0040s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 10.84 seconds
```

13. Host Discovery

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 172.25.44.64
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-29 03:20 EST
Nmap scan report for 172.25.44.64
Host is up (0.0021s latency).
Nmap done: 1 IP address (1 host up) scanned in 5.62 seconds
```

14. Cracking the Password Using Hydra



15. Information Gathering Using theHarvester

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d saveetha.com -b duckduckgo
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___     /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \   / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/  / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___|  \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.8.2                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: saveetha.com

[*] Searching Duckduckgo.

[*] No IPs found.

[*] Emails found: 17
____________________
admin@saveetha.com
adminofficer@saveetha.com
asso.deanfaculty@saveetha.com
dean.ssm@saveetha.com
enggadmission@saveetha.com
hr.smc@saveetha.com
hr.smch.nts@saveetha.com
hr.smch.ts@saveetha.com
lawdirector@saveetha.com
physiotherapy.smc@saveetha.com
prime@saveetha.com
principal.ahs@saveetha.com
principal.sclas@saveetha.com
principal.scon@saveetha.com
principal.scot@saveetha.com
principalphysiotherapy@saveetha.com
scadadmission@saveetha.com

[*] No people found.

[*] Hosts found: 4
_____________________
360.saveetha.com
sdg.saveetha.com
simatsadmissions.saveetha.com
sspe.saveetha.com

┌──(kali㉿kali)-[~]
```