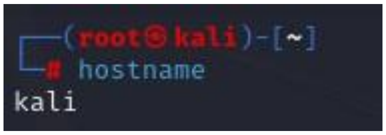
OVERVIEW:

The objective of this lab is to explore using Linux and how it can be useful for pen testers.

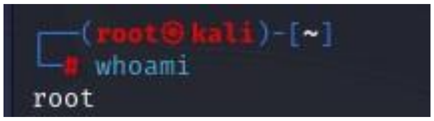
ANALYSIS:

Task 1

1. 

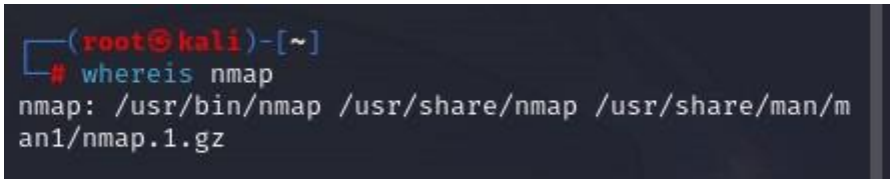
```
┌──(root㉿kali)-[~]
└─# hostname
kali
```

The hostname command is useful because it can be used to obtain the DNS name. It is the name given to a computer attached to the network.

2. 

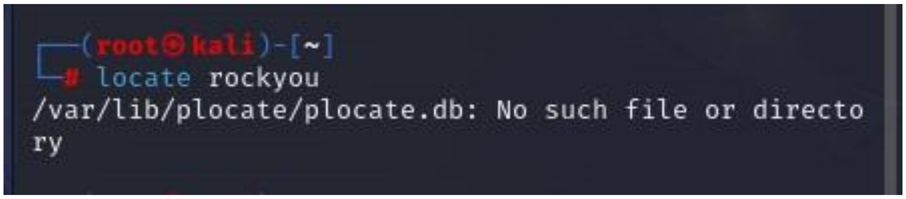
```
┌──(root㉿kali)-[~]
└─# whoami
root
```

The whoami command is useful because it will display the username of the effective user associated with the current shell session. It can be used to see who is running a script, or if you have root privileges.

3. 

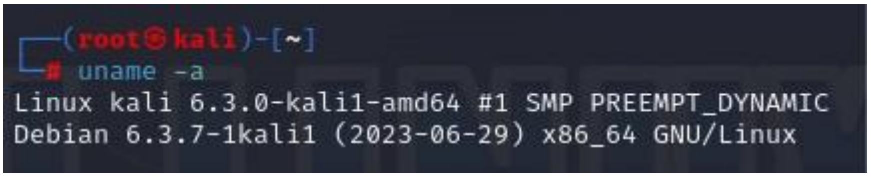
```
┌──(root㉿kali)-[~]
└─# whereis nmap
nmap: /usr/bin/nmap /usr/share/nmap /usr/share/man/m
an1/nmap.1.gz
```

The whereis command is useful for locating where specific files are stored within a linux system.

4. 

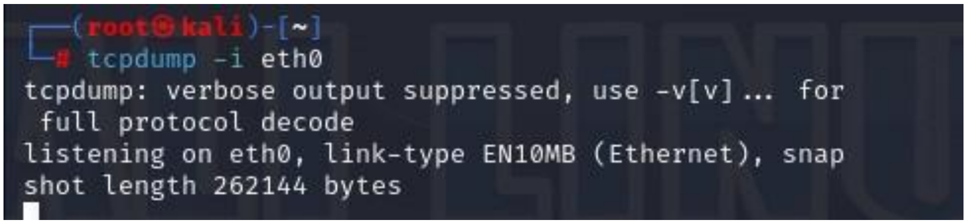
```
┌──(root㉿kali)-[~]
└─# locate rockyou
/var/lib/plocate/plocate.db: No such file or directo
ry
```

The locate command is useful to find files on the filesystems. It will search through a prebuilt database.

5. 

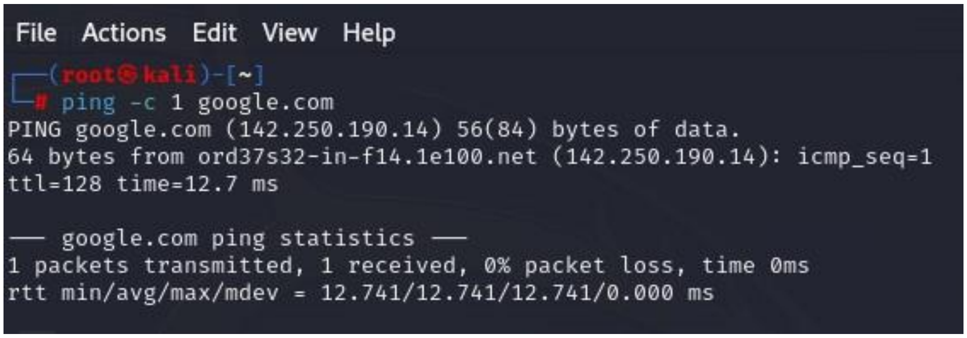
```
┌──(root㉿kali)-[~]
└─# uname -a
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC
Debian 6.3.7-1kali1 (2023-06-29) x86_64 GNU/Linux
```

The uname command is used to retrieve essential information about the systems. Such as kernel name, version, machine hardware name, OS.

6. 

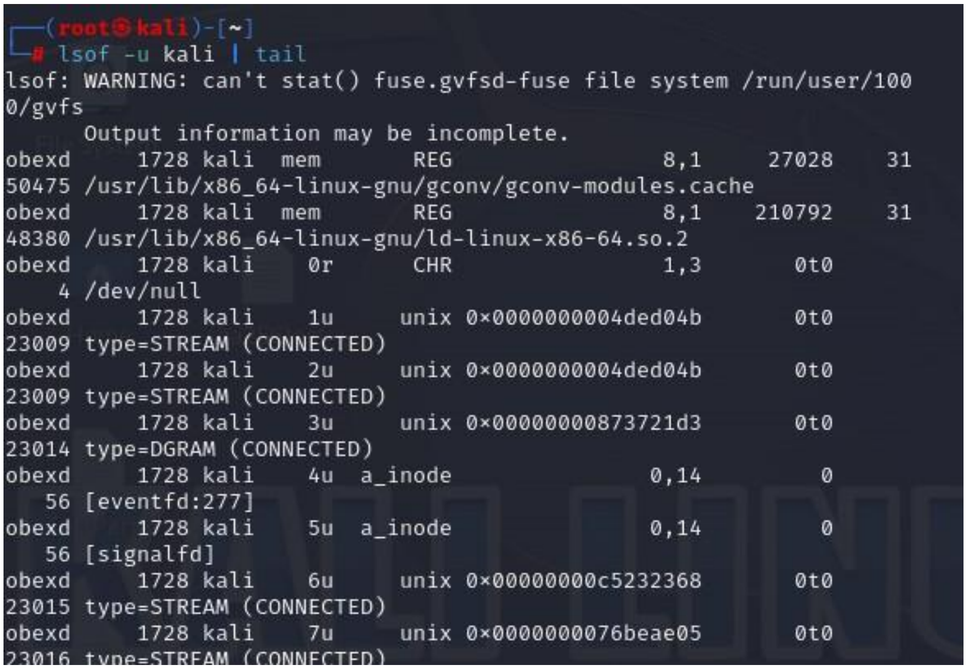
```
┌──(root㉿kali)-[~]
└─# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v[v]... for
 full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snap
shot length 262144 bytes
```

Tcpdump is a packet analyzer that can be used to analyze network traffic by intercepting and displaying packets.

7. 

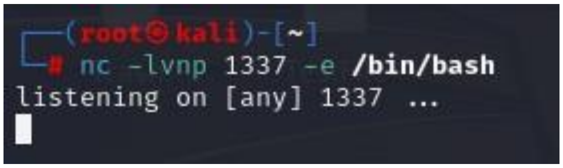
```
┌──(root㉿kali)-[~]
└─# ping -c 1 google.com
PING google.com (142.250.190.14) 56(84) bytes of data.
64 bytes from ord37s32-in-f14.1e100.net (142.250.190.14): icmp_seq=1
ttl=128 time=12.7 ms

—— google.com ping statistics ——
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 12.741/12.741/12.741/0.000 ms
```

The ping command can be useful for diagnosing connectivity issues, monitoring network performance, and checking availability.

8. 

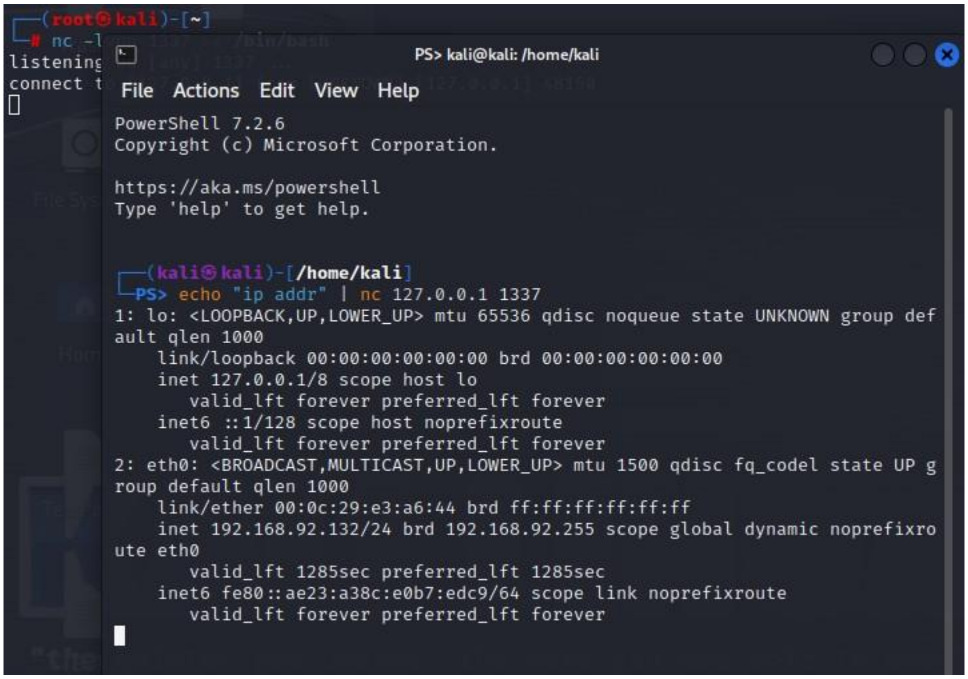
```
┌──(root㉿kali)-[~]
└─# lsof -u kali | tail
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/100
0/gvfs
      Output information may be incomplete.
obexd     1728 kali  mem       REG                8,1     27028    31
50475 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
obexd     1728 kali  mem       REG                8,1    210792    31
48380 /usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2
obexd     1728 kali    0r      CHR                1,3       0t0
    4 /dev/null
obexd     1728 kali    1u     unix 0×0000000004ded04b       0t0
23009 type=STREAM (CONNECTED)
obexd     1728 kali    2u     unix 0×0000000004ded04b       0t0
23009 type=STREAM (CONNECTED)
obexd     1728 kali    3u     unix 0×00000000873721d3       0t0
23014 type=DGRAM (CONNECTED)
obexd     1728 kali    4u  a_inode               0,14         0
   56 [eventfd:277]
obexd     1728 kali    5u  a_inode               0,14         0
   56 [signalfd]
obexd     1728 kali    6u     unix 0×00000000c5232368       0t0
23015 type=STREAM (CONNECTED)
obexd     1728 kali    7u     unix 0×0000000076beae05       0t0
23016 type=STREAM (CONNECTED)
```

The lsof command is useful because it can help you understand which files are being used by what processes on the system.

9. 

```
┌──(root㉿kali)-[~]
└─# nc -lvnp 1337 -e /bin/bash
listening on [any] 1337 ...
█
```

Netcat is useful for port scanning and listening.

10. 

```
┌──(root㉿kali)-[~]
└─# nc -l
listening
connect t
▯
```

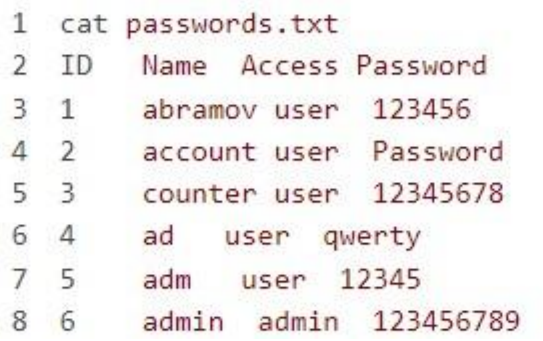
```
PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

┌──(kali㉿kali)-[/home/kali]
└─PS> echo "ip addr" | nc 127.0.0.1 1337
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:0c:29:e3:a6:44 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.132/24 brd 192.168.92.255 scope global dynamic noprefixro
ute eth0
       valid_lft 1285sec preferred_lft 1285sec
    inet6 fe80::ae23:a38c:e0b7:edc9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
█
```

The echo command is useful to display text. IT is commonly used in scripts and batch files to output status.

Task 2

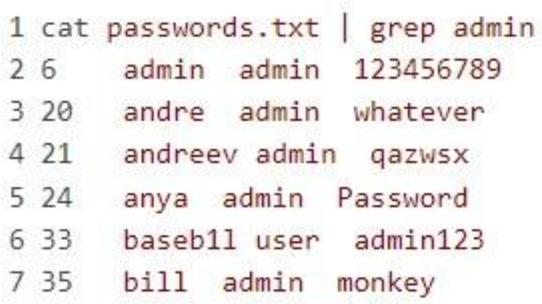
Additional commands that may be useful for pentesters in linux are

CAT – this is shor for concatenate, the command is useful because it can look to see whats inside a file.



```
cat passwords.txt
ID   Name  Access Password
1    abramov user  123456
2    account user  Password
3    counter user  12345678
4    ad   user  qwerty
5    adm   user  12345
6    admin  admin  123456789
```

GREP – This command is useful because it can be used to search for certain criteria



```
cat passwords.txt | grep admin
6    admin  admin  123456789
20   andre  admin  whatever
21   andreev admin  qazwsx
24   anya  admin  Password
33   baseb1l user  admin123
35   bill  admin  monkey
```

MAN – This command is very useful because it is used to display the user manual of any command that we can run on the terminal. This is great if you want more information on how to use a command.