

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

## Assignment #1 Traffic Tracing and Analysis

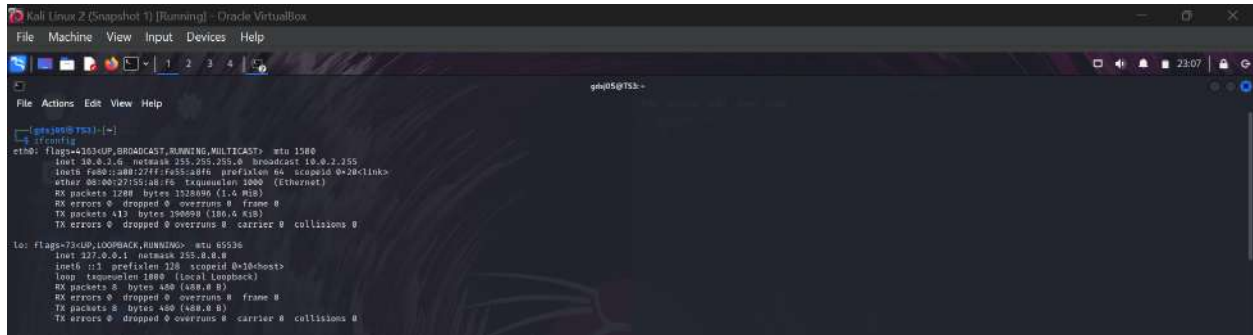
George "Trey" Smith

01249099

# TASK A

## 1. How to find the IP address on Kali Linux

- Ipconfig is a command that shows ipv4 and ipv6

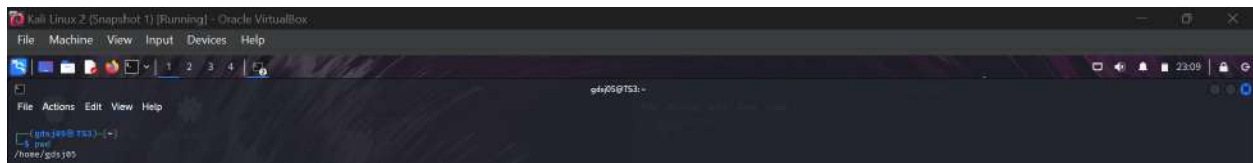


```
gsh@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0  broadcast 10.0.2.255
    inet6 fe80::a88:27ff:fe55:a9f6 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:15:aa:f6 txqueuelen 1000  (Ethernet)
    RX packets 1288  bytes 1528896 (1.4 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 413  bytes 390898 (180.6 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

## 2. Display your current directory in a terminal

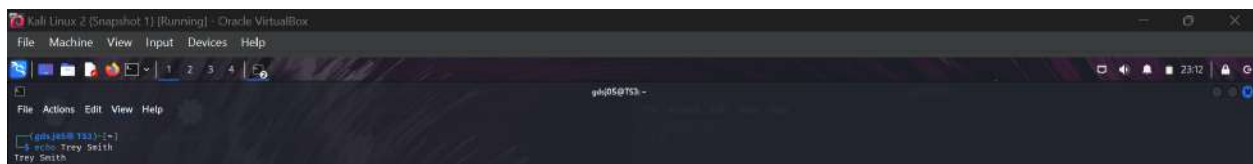
- Print working directory = pwd



```
gsh@kali:~$ pwd
/home/gsh
```

## 3. Use the echo command to print your name to the console.

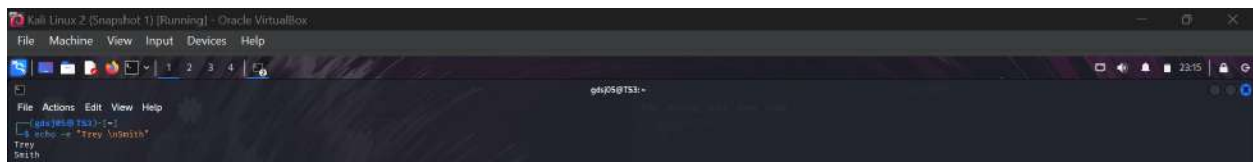
- Echo "words" will print what you typed in the terminal



```
gsh@kali:~$ echo Trey Smith
Trey Smith
```

## 4. Display your first and last names in two separate lines using a single echo command (tip: how to enable the interpretation of escape characters?)

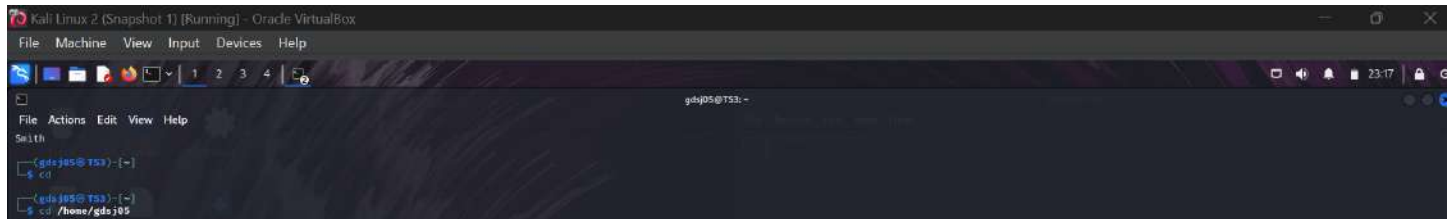
- Adding -e to echo allows it to enable interpretation this way to know to register \n as a break



```
gsh@kali:~$ echo -e "Trey\nSmith"
Trey
Smith
```

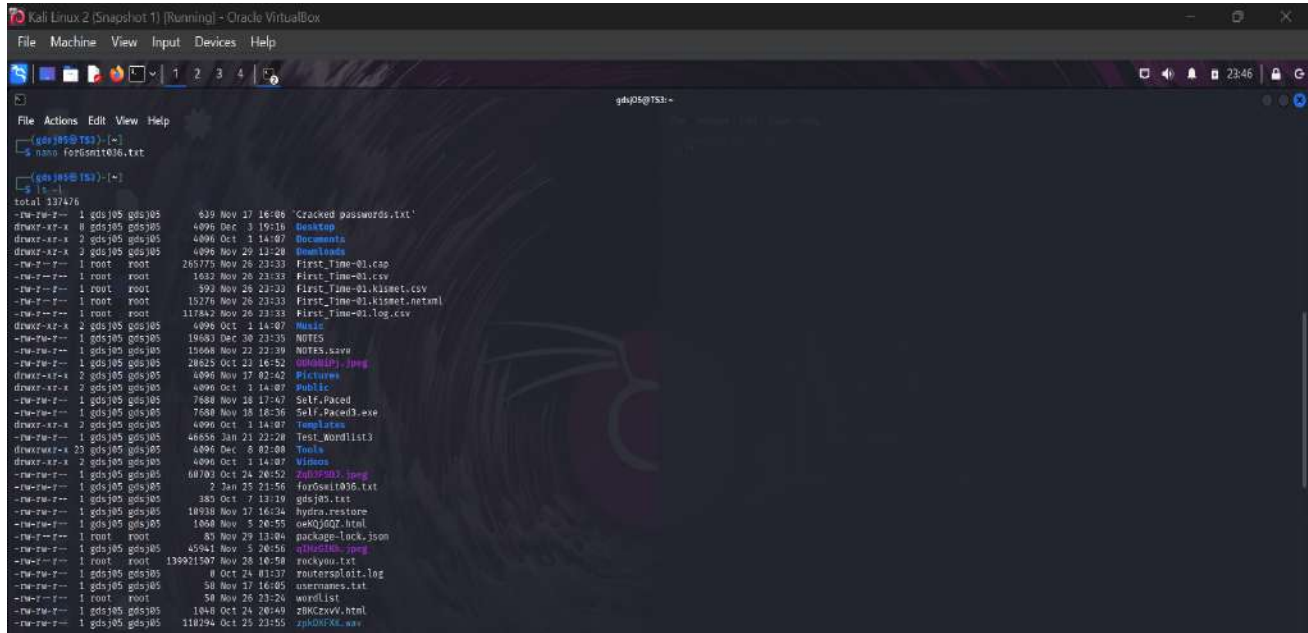
## 5. How to change to home directory using cd command and, absolute pathname.

- CD will automatically take you to your user's home directory but the absolute path for it is /home/"username."



6. Create a new file named "forXXXX.txt" in your home directory (replace "XXXX" with your own MIDAS). Then, use the long listing format to display the contents in your home directory.

- What is the size of the file you just created?
  - 2
- Nano makes a txt file and ls -l creates a long list that gives an abundance of info



7. Create a new directory named "XXXX" in your home directory (replace "XXXX" with your own MIDAS). Then, use the long listing format to display the contents in your home directory.

- What is the size of the file you just created?
  - 4096
- Mkdir makes a directory

```
Kali Linux 2 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

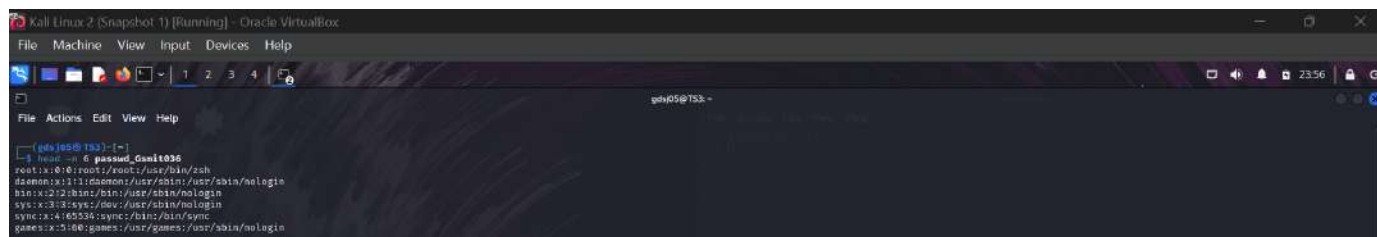
gh@kali:~$ cp /etc/passwd .
gh@kali:~$ mv passwd passwd_G0m1t936
gh@kali:~$ ls -l
total 137480
-rw-r--r-- 1 gh@kali gh@kali 639 Nov 17 16:06 'Cracked passwords.txt'
drwxr-xr-x 8 gh@kali gh@kali 4096 Dec 3 19:16 Desktop
drwxr-xr-x 2 gh@kali gh@kali 4096 Oct 1 14:07 Documents
drwxr-xr-x 3 gh@kali gh@kali 4096 Nov 29 13:08 Downloads
-rw-r--r-- 1 root root 265775 Nov 26 23:33 First_Time-01.cap
-rw-r--r-- 1 root root 1632 Nov 26 23:33 First_Time-01.csv
-rw-r--r-- 1 root root 503 Nov 26 23:33 First_Time-01.kismet.csv
-rw-r--r-- 1 root root 15276 Nov 26 23:33 First_Time-01.kismet.netxml
-rw-r--r-- 1 root root 117862 Nov 26 23:33 First_Time-01.log.csv
drwxr-xr-x 2 gh@kali gh@kali 4096 Jan 25 22:17 G0m1t936
drwxr-xr-x 2 gh@kali gh@kali 4096 Oct 1 14:07 Music
-rw-r--r-- 1 gh@kali gh@kali 19683 Dec 30 23:35 NOTES
-rw-r--r-- 1 gh@kali gh@kali 15608 Nov 22 22:29 NOTES.save
-rw-r--r-- 1 gh@kali gh@kali 28625 Oct 23 16:52 Pictures.jpg
drwxr-xr-x 2 gh@kali gh@kali 4096 Nov 17 02:42 Pictures
drwxr-xr-x 2 gh@kali gh@kali 4096 Oct 1 14:07 Public
-rw-r--r-- 1 gh@kali gh@kali 7088 Nov 18 17:47 Self_Paced
-rw-r--r-- 1 gh@kali gh@kali 7088 Nov 18 16:26 Self_Paced3.exe
drwxr-xr-x 2 gh@kali gh@kali 4096 Oct 1 14:07 Templates
-rw-r--r-- 1 gh@kali gh@kali 46656 Jan 21 22:28 Test_MurfiList3
drwxr-xr-x 23 gh@kali gh@kali 4096 Dec 8 02:48 Tools
drwxr-xr-x 2 gh@kali gh@kali 4096 Oct 1 14:07 Videos
-rw-r--r-- 1 gh@kali gh@kali 60783 Oct 24 20:52 2gh@kali.jpg
-rw-r--r-- 1 gh@kali gh@kali 2 Jan 25 22:26 forG0m1t936.txt
-rw-r--r-- 1 gh@kali gh@kali 385 Oct 7 13:19 gds385.txt
-rw-r--r-- 1 gh@kali gh@kali 18928 Nov 17 16:34 hydra.restore
-rw-r--r-- 1 gh@kali gh@kali 3808 Nov 5 20:53 oeoQ10Q2.html
-rw-r--r-- 1 root root 85 Nov 29 13:04 package-lock.json
-rw-r--r-- 1 gh@kali gh@kali 45041 Nov 5 20:56 2gh@kali.jpg
-rw-r--r-- 1 root root 119921587 Nov 28 18:58 rackyou.txt
-rw-r--r-- 1 gh@kali gh@kali 8 Oct 24 01:37 routersploit.log
-rw-r--r-- 1 gh@kali gh@kali 58 Nov 17 16:05 usernames.txt
-rw-r--r-- 1 root root 58 Nov 26 23:24 wordlist
-rw-r--r-- 1 gh@kali gh@kali 1848 Oct 24 20:49 z8KCzvv.html
-rw-r--r-- 1 gh@kali gh@kali 118204 Oct 25 23:55 2gh@kali.svg
```

8. Copy /etc/passwd file to your home directory. The copy should be named as “passwd\_XXXX” (replace “XXXX” with your own MIDAS) in your home directory. Then, complete the following two subtasks:
- A. Use the proper command to display the first six lines in this file.
    - a. Head = first 10, head -n 6 = specifies a limit on how many I want to show
  - B. Search keyword “www” in this file.
    - a. Grep command allows a search through a file

```
Kali Linux 2 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

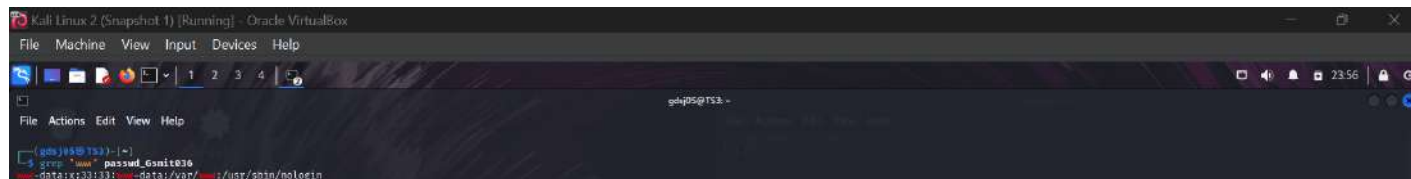
gh@kali:~$ cp /etc/passwd .
gh@kali:~$ mv passwd passwd_G0m1t936
gh@kali:~$ ls -l
total 137480
-rw-r--r-- 1 gh@kali gh@kali 639 Nov 17 16:06 'Cracked passwords.txt'
drwxr-xr-x 8 gh@kali gh@kali 4096 Dec 3 19:16 Desktop
drwxr-xr-x 2 gh@kali gh@kali 4096 Oct 1 14:07 Documents
drwxr-xr-x 3 gh@kali gh@kali 4096 Nov 29 13:08 Downloads
-rw-r--r-- 1 root root 265775 Nov 26 23:33 First_Time-01.cap
-rw-r--r-- 1 root root 1632 Nov 26 23:33 First_Time-01.csv
-rw-r--r-- 1 root root 503 Nov 26 23:33 First_Time-01.kismet.csv
-rw-r--r-- 1 root root 15276 Nov 26 23:33 First_Time-01.kismet.netxml
-rw-r--r-- 1 root root 117862 Nov 26 23:33 First_Time-01.log.csv
drwxr-xr-x 2 gh@kali gh@kali 4096 Jan 25 22:17 G0m1t936
drwxr-xr-x 2 gh@kali gh@kali 4096 Oct 1 14:07 Music
-rw-r--r-- 1 gh@kali gh@kali 19683 Dec 30 23:35 NOTES
-rw-r--r-- 1 gh@kali gh@kali 15608 Nov 22 22:29 NOTES.save
-rw-r--r-- 1 gh@kali gh@kali 28625 Oct 23 16:52 Pictures.jpg
drwxr-xr-x 2 gh@kali gh@kali 4096 Nov 17 02:42 Pictures
drwxr-xr-x 2 gh@kali gh@kali 4096 Oct 1 14:07 Public
-rw-r--r-- 1 gh@kali gh@kali 7088 Nov 18 17:47 Self_Paced
-rw-r--r-- 1 gh@kali gh@kali 7088 Nov 18 16:26 Self_Paced3.exe
drwxr-xr-x 2 gh@kali gh@kali 4096 Oct 1 14:07 Templates
-rw-r--r-- 1 gh@kali gh@kali 46656 Jan 21 22:28 Test_MurfiList3
drwxr-xr-x 23 gh@kali gh@kali 4096 Dec 8 02:48 Tools
drwxr-xr-x 2 gh@kali gh@kali 4096 Oct 1 14:07 Videos
-rw-r--r-- 1 gh@kali gh@kali 60783 Oct 24 20:52 2gh@kali.jpg
-rw-r--r-- 1 gh@kali gh@kali 2 Jan 25 22:26 forG0m1t936.txt
-rw-r--r-- 1 gh@kali gh@kali 385 Oct 7 13:19 gds385.txt
-rw-r--r-- 1 gh@kali gh@kali 18928 Nov 17 16:34 hydra.restore
-rw-r--r-- 1 gh@kali gh@kali 3808 Nov 5 20:53 oeoQ10Q2.html
-rw-r--r-- 1 root root 85 Nov 29 13:04 package-lock.json
-rw-r--r-- 1 gh@kali gh@kali 45041 Nov 5 20:56 2gh@kali.jpg
-rw-r--r-- 1 root root 119921587 Nov 28 18:58 rackyou.txt
-rw-r--r-- 1 gh@kali gh@kali 8 Oct 24 01:37 routersploit.log
-rw-r--r-- 1 gh@kali gh@kali 58 Nov 17 16:05 usernames.txt
-rw-r--r-- 1 root root 58 Nov 26 23:24 wordlist
-rw-r--r-- 1 gh@kali gh@kali 1848 Oct 24 20:49 z8KCzvv.html
-rw-r--r-- 1 gh@kali gh@kali 118204 Oct 25 23:55 2gh@kali.svg
```

A



```
Kali Linux 2 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
gdbp05@TS3: ~
(gdbp05@TS3)~$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

B



```
Kali Linux 2 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
gdbp05@TS3: ~
(gdbp05@TS3)~$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```