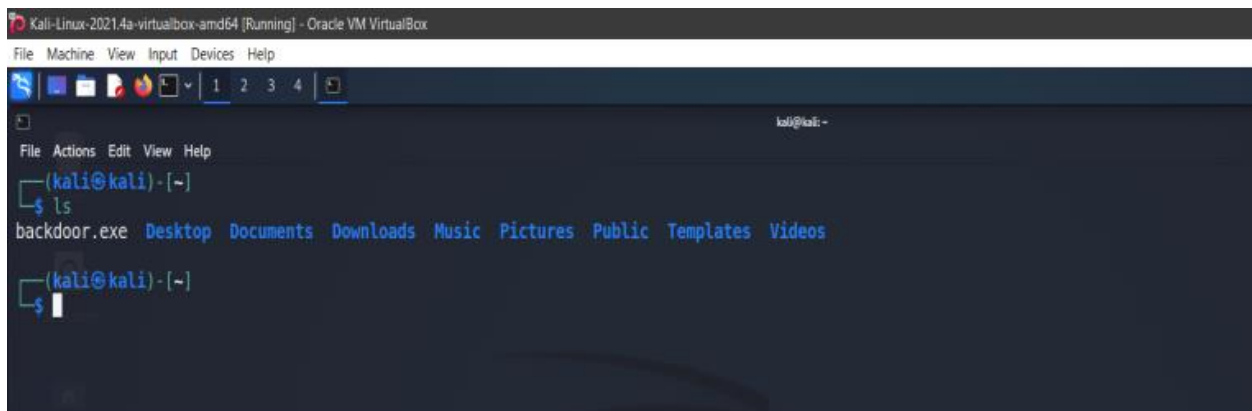


Name: Gaurav Jaiswal
Reg no: 20BKT0028

CYBER SECURITY AND ETHICAL HACKING ASSESSMENT 1

ls

A screenshot of a Kali Linux terminal window. The window title is "Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal shows the prompt "(kali@kali) - [~]" and the command "ls" has been entered. The output of the command is displayed as a list of files and directories: "backdoor.exe Desktop Documents Downloads Music Pictures Public Templates Videos".

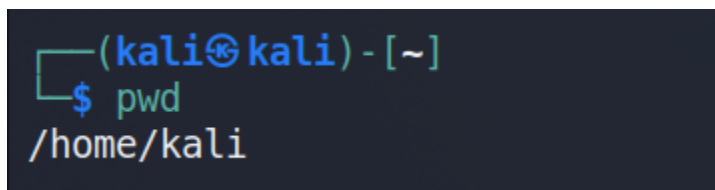
```
(kali@kali) - [~]  
$ ls  
backdoor.exe Desktop Documents Downloads Music Pictures Public Templates Videos  
(kali@kali) - [~]  
$
```

cd

A screenshot of a Kali Linux terminal window. The window title is "Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal shows the prompt "(kali@kali) - [~]" and the command "cd Desktop" has been entered. The output of the command is displayed as "Desktop".

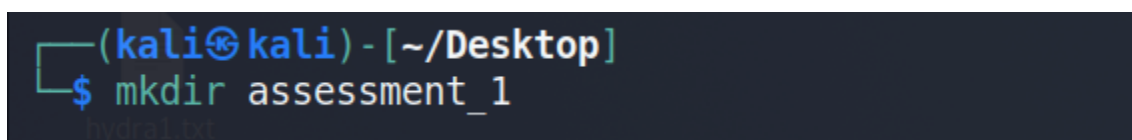
```
(kali@kali) - [~]  
$ cd Desktop  
Desktop  
(kali@kali) - [~/Desktop]  
$
```

pwd

A screenshot of a Kali Linux terminal window. The window title is "Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal shows the prompt "(kali@kali) - [~]" and the command "pwd" has been entered. The output of the command is displayed as "/home/kali".

```
(kali@kali) - [~]  
$ pwd  
/home/kali  
(kali@kali) - [~]  
$
```

mkdir

A screenshot of a Kali Linux terminal window. The window title is "Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal shows the prompt "(kali@kali) - [~/Desktop]" and the command "mkdir assessment_1" has been entered. The output of the command is displayed as "assessment_1".

```
(kali@kali) - [~/Desktop]  
$ mkdir assessment_1  
assessment_1  
(kali@kali) - [~/Desktop]  
$
```

touch

```
(kali㉿kali) - [~/Desktop/assessment_1]
$ touch new.txt

(kali㉿kali) - [~/Desktop/assessment_1]
$ ls
new.txt  smartbridge.txt
```

cp

```
(kali㉿kali) - [~/Desktop]
$ ls
assessment_1  hydra1.txt  hydra.txt  new  password.txt

(kali㉿kali) - [~/Desktop]
$ ls new

(kali㉿kali) - [~/Desktop]
$ cp hydra1.txt hydra.txt new

(kali㉿kali) - [~/Desktop]
$ ls new
hydra1.txt  hydra.txt
```

mv

```
(kali㉿kali) - [~]
$ cd Desktop

(kali㉿kali) - [~/Desktop]
$ mv hydra1.txt /home
mv: cannot move 'hydra1.txt' to '/home/hydra1.txt': Permission denied

(kali㉿kali) - [~/Desktop]
$ sudo mv hydra1.txt /home

(kali㉿kali) - [~/Desktop]
$ ls
assessment_1  new  password.txt
```

find

```
(kali㉿kali) - [~]
$ find ./ -name index.html
./index.html
```

```
(kali㉿kali)-[~/Desktop]
└─$ cat name
Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and composed it to produce a sample book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s by the Letraset team, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum
Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and composed it to produce a sample book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s by the Letraset team, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum
Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and composed it to produce a sample book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s by the Letraset team, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum
```

[illegible]

head

```
(kali@kali)-[~/Desktop]
$ head name
Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, men book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum
Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, men book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum
Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, men book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum
```

tail

```
(kali@kali)-[~/Desktop]
$ tail name
Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, men book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum
Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, men book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum
Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, men book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum
```

nano

```
(kali@kali)-[~/Desktop]
$ nano smartbridge.txt
```

ps

```
(kali@kali)-[~]
$ ps
  PID TTY          TIME CMD
 1187 pts/0        00:00:00 zsh
 1540 pts/0        00:00:00 ps
```

top

```
top 03:47:57 up 4 min, 1 user, load averages: 0.26, 0.20, 0.09
Tasks: 155 total, 1 running, 154 sleeping, 0 stopped, 0 zombie
Mem(s): 0.5 us, 0.7 sy, 0.0 ni, 98.5 id, 0.2 wa, 0.0 hi, 0.2 si, 0.0 st
MiB Mem: 1582.0 total, 1802.8 free, 490.7 used, 488.5 buff/cache
MiB Swap: 975.0 total, 975.0 free, 0.0 used, 1336.1 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR     S    CPU%  MEM%   TIME+  COMMAND
 542 root       20   0 362432 118088 50660 S    0.7  5.8  0:02.04 xorg
 842 kali     20   0 152864 2840   2380 S    0.3  0.1  0:00.26 VBoxClient
 935 kali     20   0 207180 24464 17400 S    0.2  1.2  0:00.05 panel-13-cpugra
 937 kali     20   0 359080 27304 19844 S    0.3  1.3  0:00.55 panel-15-gemmon
2317 kali     20   0 484868 87444 70100 S    0.3  4.3  0:00.13 atermimal
   1 root       20   0 164436 10344 7784 S    0.0  0.5  0:00.26 systemd
   2 root       0   0 0        0        0 S    0.0  0.0  0:00.00 kthreadd
   3 root      -20  0 0        0        0 I    0.0  0.0  0:00.00 rcu_gp
   4 root      -20  0 0        0        0 I    0.0  0.0  0:00.00 rcu_gar_gp
   5 root       0   0 0        0        0 I    0.0  0.0  0:00.00 kworker/0:0-ata_sff
   6 root      -20  0 0        0        0 I    0.0  0.0  0:00.00 kworker/0:0H-events_highpri
   7 root       0   0 0        0        0 I    0.0  0.0  0:00.03 kworker/0:1-events
   8 root       0   0 0        0        0 I    0.0  0.0  0:00.00 kworker/u:0-flush-sio
   9 root      -20  0 0        0        0 I    0.0  0.0  0:00.00 mm_percpu_wq
  10 root      20   0 0        0        0 S    0.0  0.0  0:00.00 rcu_tasks_rude_
  11 root      20   0 0        0        0 S    0.0  0.0  0:00.00 rcu_tasks_trace
  12 root      20   0 0        0        0 S    0.0  0.0  0:00.02 ksoftirqd/0
  13 root      20   0 0        0        0 I    0.0  0.0  0:00.00 rcu_sched
  14 root      rt   0 0        0        0 S    0.0  0.0  0:00.00 migration/0
  15 root      20   0 0        0        0 S    0.0  0.0  0:00.00 cpupd/0
  16 root      20   0 0        0        0 S    0.0  0.0  0:00.00 cpupd/1
  17 root      rt   0 0        0        0 S    0.0  0.0  0:00.13 migration/1
  18 root      20   0 0        0        0 S    0.0  0.0  0:00.01 ksoftirqd/1
  19 root      20   0 0        0        0 I    0.0  0.0  0:00.00 kworker/1:0-events
  20 root      -20  0 0        0        0 I    0.0  0.0  0:00.00 kworker/1:0H-events_highpri
  22 root      20   0 0        0        0 I    0.0  0.0  0:00.06 kworker/u:1H-events_unbound
  23 root      20   0 0        0        0 S    0.0  0.0  0:00.00 kintegrityd
  24 root      -20  0 0        0        0 I    0.0  0.0  0:00.00 netns
  25 root      -20  0 0        0        0 I    0.0  0.0  0:00.00 inet_frag_wq
  26 root      20   0 0        0        0 S    0.0  0.0  0:00.00 kauditd
  27 root      20   0 0        0        0 S    0.0  0.0  0:00.00 khungtaskd
  28 root      20   0 0        0        0 S    0.0  0.0  0:00.00 oom_reaper
  29 root      -20  0 0        0        0 I    0.0  0.0  0:00.00 writeback
  30 root      20   0 0        0        0 S    0.0  0.0  0:00.00 kcompactd0
  31 root      25   5 0        0        0 S    0.0  0.0  0:00.00 ksmd
  32 root      25  10 0        0        0 S    0.0  0.0  0:00.05 khugepaged
  34 root      20   0 0        0        0 I    0.0  0.0  0:00.02 kworker/1:1-ata_sff
  52 root      -20  0 0        0        0 I    0.0  0.0  0:00.00 kintegrityd
  53 root      -20  0 0        0        0 I    0.0  0.0  0:00.00 blklockd
  54 root      -20  0 0        0        0 I    0.0  0.0  0:00.00 blkcg_punt_bio
  55 root      -20  0 0        0        0 I    0.0  0.0  0:00.00 tpm_dev_wq
  56 root      -20  0 0        0        0 I    0.0  0.0  0:00.00 sdac-poller
  57 root      -20  0 0        0        0 I    0.0  0.0  0:00.00 devfreq_wq
  58 root      -20  0 0        0        0 I    0.0  0.0  0:00.04 kworker/0:1H-kblockd
  59 root      20   0 0        0        0 S    0.0  0.0  0:00.00 kswapd0
```

kill

```
(kali㉿kali)-[~]  
$ ps  
  PID TTY          TIME CMD  
 2320 pts/0    00:00:00 zsh  
 3204 pts/0    00:00:00 ps  
  
(kali㉿kali)-[~]  
$ kill 2320
```

bg

```
(kali㉿kali)-[~]  
$ jobs  
  
(kali㉿kali)-[~]  
$ sleep 500  
^Z  
zsh: suspended  sleep 500  
  
(kali㉿kali)-[~]  
$ jobs  
[1] + suspended  sleep 500  
  
(kali㉿kali)-[~]  
$ bg %1  
[1] + continued  sleep 500  
  
(kali㉿kali)-[~]  
$ jobs  
[1] + running    sleep 500
```

fg

```
(kali㉿kali)-[~]  
$ fg %1  
[1] + running    sleep 500  
█
```

uname

```
(kali㉿kali)-[~]  
$ uname  
Linux
```

df

```
(kali㉿kali)-[~]
$ df
Filesystem      1K-blocks      Used Available Use% Mounted on
udev            972456         0    972456   0% /dev
tmpfs           202952        932    202020   1% /run
/dev/sda1       81000912 10012844  66827456  14% /
tmpfs           1014760       23992    990768   3% /dev/shm
tmpfs            5120          0       5120   0% /run/lock
tmpfs           202952         64    202888   1% /run/user/1000
```

free

```
(kali㉿kali)-[~]
$ free
              total        used        free      shared  buff/cache   available
Mem:           2029520      801564      591916         41172        636040       1034744
Swap:           998396           0       998396
```

uptime

```
(kali㉿kali)-[~]
$ uptime
04:08:59 up 25 min,  1 user,  load average: 0.19, 0.22, 0.18
```

who

```
(kali㉿kali)-[~]
$ who
kali          tty7                2023-05-21 03:43 (:0)
```

w

```
(kali㉿kali)-[~]
$ w
04:11:15 up 28 min,  1 user,  load average: 0.21, 0.21, 0.18
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
kali      tty7      :0            03:43    28:12  6.67s  0.15s xfce4-session
```


ifconfig

```
(kali㉿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::a00:27ff:fe50:4c14 prefixlen 64 scopeid 0<link>
    ether 08:00:27:50:4c:14 txqueuelen 1000 (Ethernet)
    RX packets 12540 bytes 16556241 (15.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7419 bytes 522246 (510.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

ping

```
(kali㉿kali)-[~]
$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
 64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.014 ms
 64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.024 ms
 64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.086 ms
 64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.024 ms
 64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.025 ms
 64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.023 ms
 64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.024 ms
 64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.024 ms
 64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=0.026 ms
 64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=0.060 ms
 64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=0.062 ms
^C
--- 10.0.2.15 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10278ms
rtt min/avg/max/mdev = 0.014/0.035/0.086/0.021 ms
```

wget

```
(kali㉿kali)-[~]
$ wget https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/
--2023-05-21 04:29:21-- https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/
Resolving www.checkpoint.com (www.checkpoint.com)... 108.159.15.35, 108.159.15.58, 108.159.15.101, ...
Connecting to www.checkpoint.com (www.checkpoint.com)|108.159.15.35|:443... connected.
HTTP request sent, awaiting response... 202 Accepted
Length: 0 [text/html]
Saving to: 'index.html'

index.html                                     [ ↔ ]
2023-05-21 04:29:21 (0.00 B/s) - 'index.html' saved [0/0]
```

sudo

```
(kali㉿kali)-[~]  
$ sudo apt update  
[sudo] password for kali:  
Hit:1 http://kali.download/kali kali-last-snapshot InRelease  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
1902 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

apt-get

```
(kali㉿kali)-[~]  
$ sudo apt-get upgrade  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
Calculating upgrade... Done  
The following packages were automatically installed and are no longer required:  
dctrl-tools dh-dkms dleyna-server gir1.2-javascriptcoregtk-4.0 gir1.2-soup-2.4 gir1.2-webkit2-4.0  
libdleydna-connector-dbus-1.0-1 libdleydna-core-1.0-5 libhttp-server-simple-perl libnginx-mod-http-geoip  
libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream  
libnginx-mod-stream-geoip libsoup-gnome2.4-1 libwacom-bin libwebkit2gtk-4.0-37 nginx-common nginx-core  
python3-dataclasses-json python3-limiter python3-marshmallow-enum python3-mypy-extensions  
python3-responses python3-spyse python3-token-bucket python3-typing-inspect sphinx-rtd-theme-common  
Use 'sudo apt autoremove' to remove them.
```

systemctl

```
(kali㉿kali)-[~]  
$ systemctl  
UNIT  
proc-sys-fs-binfmt_misc.automount  
sys-devices-pci0000:00-0000:00:01.1-ata2-host1-target1:0:0-1:0:0:0-block-sr0.  
sys-devices-pci0000:00-0000:00:03.0-net-eth0.device  
sys-devices-pci0000:00-0000:00:05.0-sound-card0-controlC0.device  
sys-devices-pci0000:00-0000:00:0d.0-ata3-host2-target2:0:0-2:0:0:0-block-sda.  
sys-devices-pci0000:00-0000:00:0d.0-ata3-host2-target2:0:0-2:0:0:0-block-sda.  
sys-devices-pci0000:00-0000:00:0d.0-ata3-host2-target2:0:0-2:0:0:0-block-sda.  
sys-devices-pci0000:00-0000:00:0d.0-ata3-host2-target2:0:0-2:0:0:0-block-sda.  
sys-devices-platform-serial8250-tty-ttyS0.device  
sys-devices-platform-serial8250-tty-ttyS1.device  
sys-devices-platform-serial8250-tty-ttyS2.device  
sys-devices-platform-serial8250-tty-ttyS3.device  
sys-devices-virtual-misc-rfkill.device  
sys-module-configfs.device  
sys-module-fuse.device  
sys-subsystem-net-devices-eth0.device  
-.mount  
dev-hugepages.mount  
dev-mqueue.mount  
proc-sys-fs-binfmt_misc.mount  
run-credentials-systemd\x2dsysctl.service.mount  
run-credentials-systemd\x2dsysusers.service.mount  
lines 1-23...skipping...
```


crontab

```
(kali㉿kali)-[~]
└─$ crontab -e
no crontab for kali - using an empty one

Select an editor. To change later, run 'select-editor'.
 1. /bin/nano      <---- easiest
 2. /usr/bin/vim.basic
 3. /usr/bin/vim.tiny

Choose 1-3 [1]: /bin/nano
Choose 1-3 [1]: 1
No modification made
```

```
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
```

useradd

```
(kali㉿kali)-[~]
└─$ sudo useradd newuser
[sudo] password for kali:
```

passwd

```
(kali㉿kali)-[~]  
$ sudo passwd newuser  
New password:  
Retype new password:  
passwd: password updated successfully
```