COMP 4108

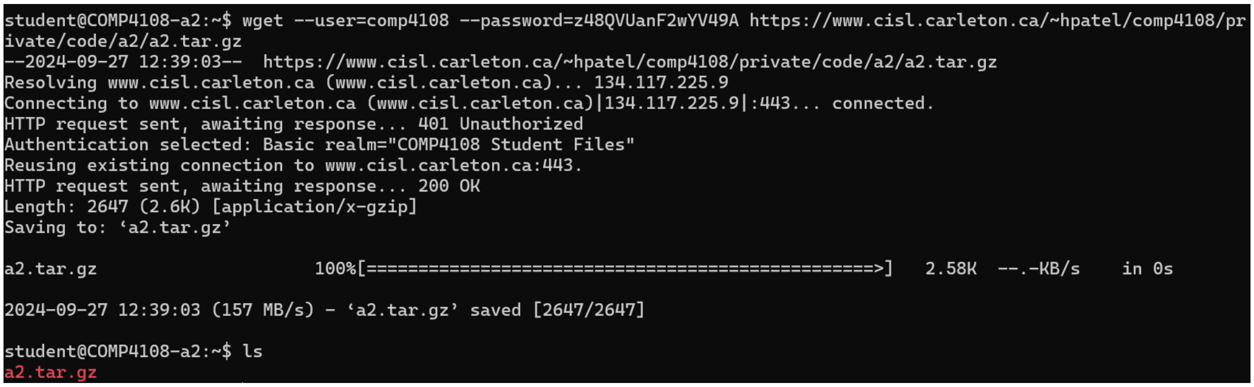
Assignment 2

Yahya Mohamed

101186046

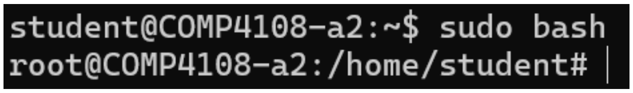
Part A:

1.



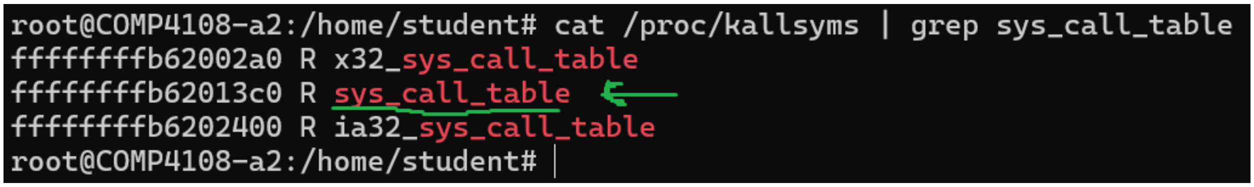
```
student@COMP4108-a2:~$ wget --user=comp4108 --password=z48QVUanF2wYV49A https://www.cisl.carleton.ca/~hpatel/comp4108/pr
ivate/code/a2/a2.tar.gz
--2024-09-27 12:39:03--  https://www.cisl.carleton.ca/~hpatel/comp4108/private/code/a2/a2.tar.gz
Resolving www.cisl.carleton.ca (www.cisl.carleton.ca)... 134.117.225.9
Connecting to www.cisl.carleton.ca (www.cisl.carleton.ca)|134.117.225.9|:443... connected.
HTTP request sent, awaiting response... 401 Unauthorized
Authentication selected: Basic realm="COMP4108 Student Files"
Reusing existing connection to www.cisl.carleton.ca:443.
HTTP request sent, awaiting response... 200 OK
Length: 2647 (2.6K) [application/x-gzip]
Saving to: ‘a2.tar.gz’

a2.tar.gz                     100%[================================================>]   2.58K  --.-KB/s    in 0s

2024-09-27 12:39:03 (157 MB/s) - ‘a2.tar.gz’ saved [2647/2647]

student@COMP4108-a2:~$ ls
a2.tar.gz
```

2.



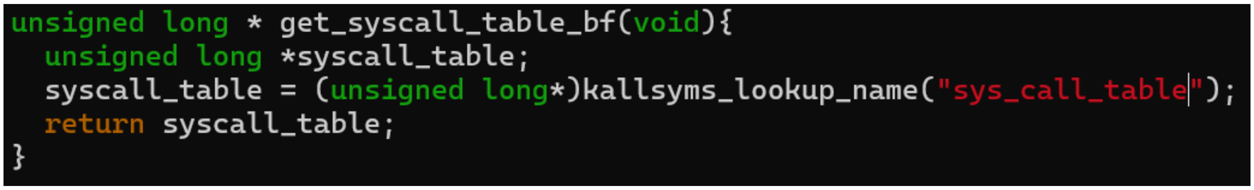
```
student@COMP4108-a2:~$ sudo bash
root@COMP4108-a2:/home/student#
```

3.



```
root@COMP4108-a2:/home/student# cat /proc/kallsyms | grep sys_call_table
ffffffffb62002a0 R x32_sys_call_table
ffffffffb62013c0 R sys_call_table
ffffffffb6202400 R ia32_sys_call_table
root@COMP4108-a2:/home/student#
```

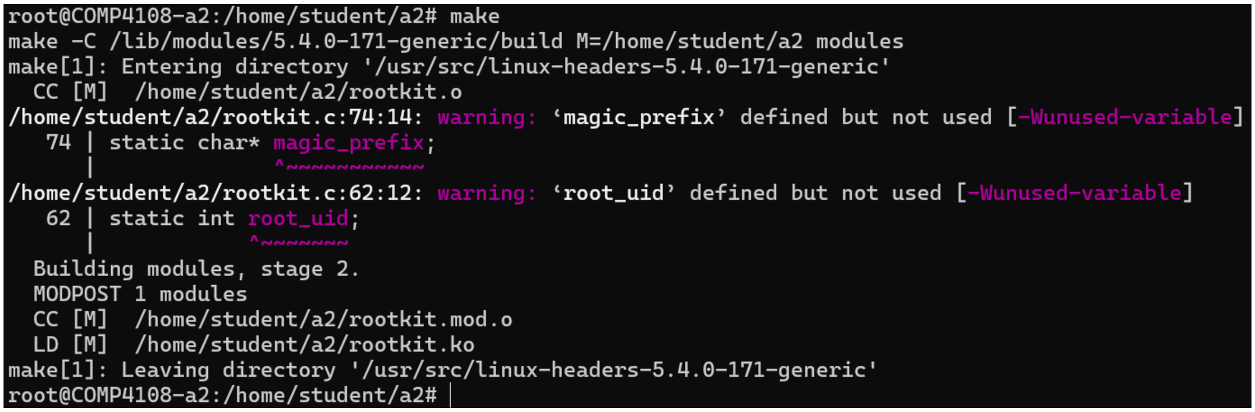
4.



```
unsigned long * get_syscall_table_bf(void){
  unsigned long *syscall_table;
  syscall_table = (unsigned long*)kallsyms_lookup_name("sys_call_table");
  return syscall_table;
}
```

5.

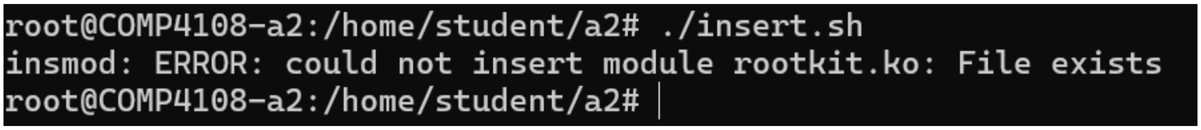
Building rootkit framework by running make:



```
root@COMP4108-a2:/home/student/a2# make
make -C /lib/modules/5.4.0-171-generic/build M=/home/student/a2 modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-171-generic'
  CC [M]  /home/student/a2/rootkit.o
/home/student/a2/rootkit.c:74:14: warning: ‘magic_prefix’ defined but not used [-Wunused-variable]
   74 | static char* magic_prefix;
      |              ^~~~~~~~~~~~
/home/student/a2/rootkit.c:62:12: warning: ‘root_uid’ defined but not used [-Wunused-variable]
   62 | static int root_uid;
      |            ^~~~~~~~
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/student/a2/rootkit.mod.o
  LD [M]  /home/student/a2/rootkit.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-171-generic'
root@COMP4108-a2:/home/student/a2#
```

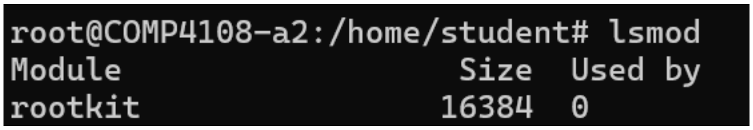
6.

File exists error returned since I already ran it but forgot to add screenshot:



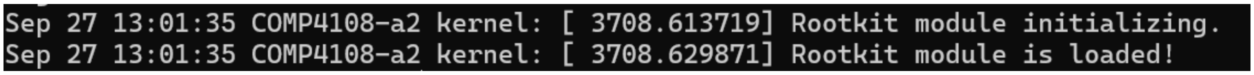
```
root@COMP4108-a2:/home/student/a2# ./insert.sh
insmod: ERROR: could not insert module rootkit.ko: File exists
root@COMP4108-a2:/home/student/a2#
```

Confirmation from lsmod:



```
root@COMP4108-a2:/home/student# lsmod
Module                  Size  Used by
rootkit                16384  0
```

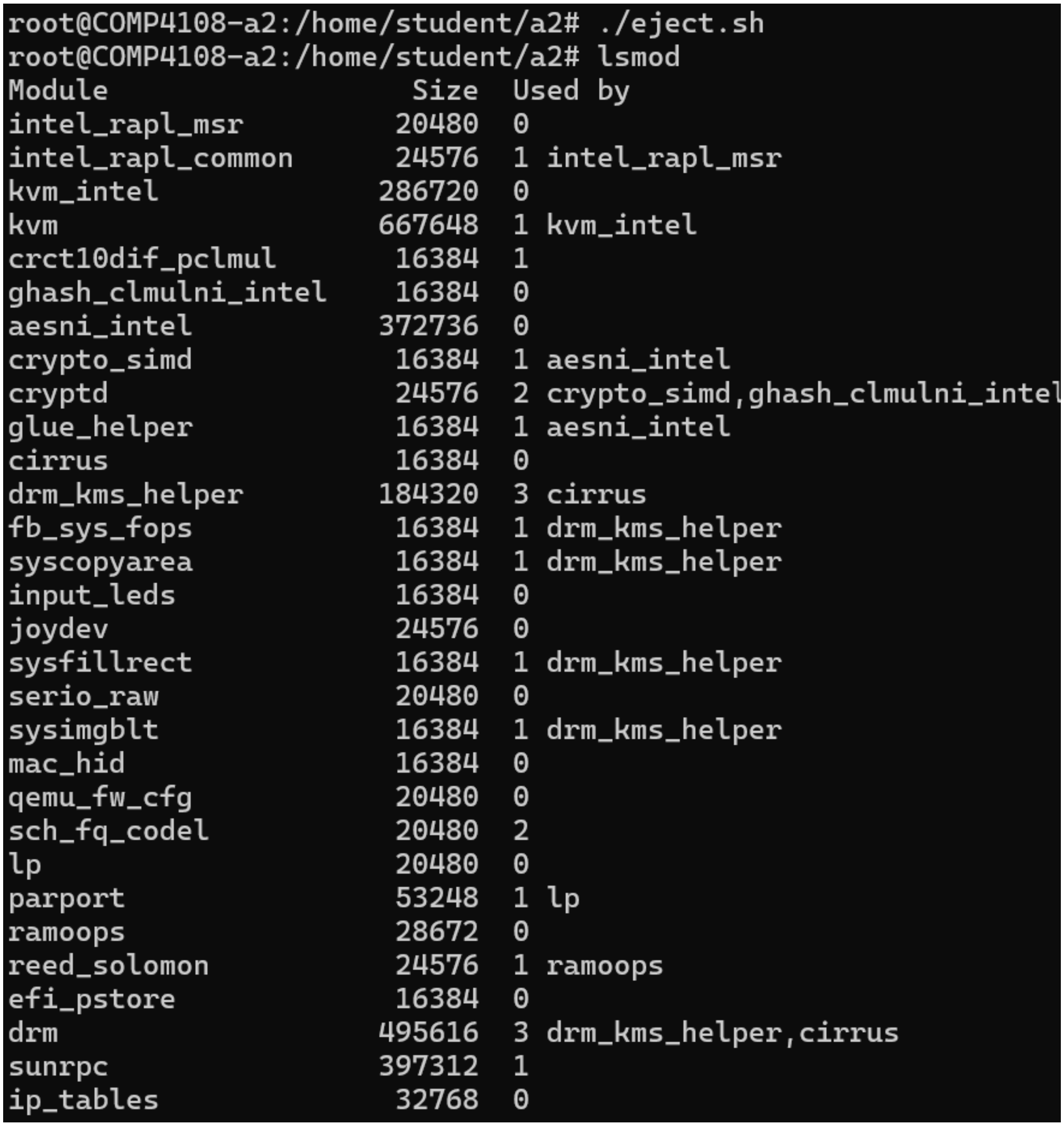
Syslog file confirmation (after running “cat /var/log/syslog”)



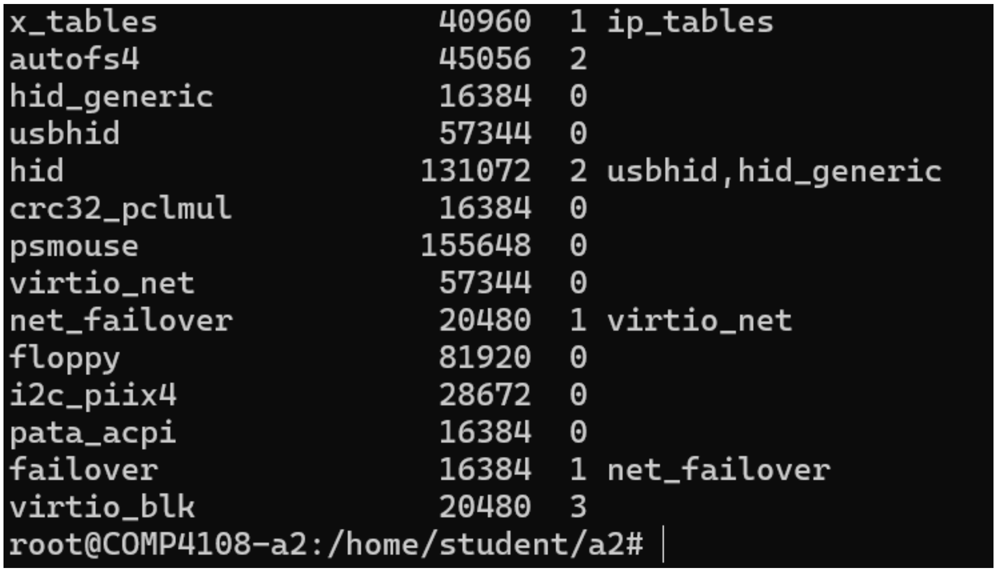
```
Sep 27 13:01:35 COMP4108-a2 kernel: [ 3708.613719] Rootkit module initializing.
Sep 27 13:01:35 COMP4108-a2 kernel: [ 3708.629871] Rootkit module is loaded!
```

7.

After running ./eject.sh, rootkit was ejected, confirmed by running lsmod:

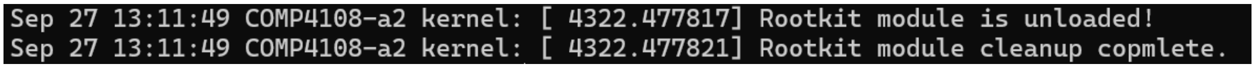


```
root@COMP4108-a2:/home/student/a2# ./eject.sh
root@COMP4108-a2:/home/student/a2# lsmod
Module                  Size  Used by
intel_rapl_msr         20480  0
intel_rapl_common      24576  1 intel_rapl_msr
kvm_intel             286720  0
kvm                   667648  1 kvm_intel
crct10dif_pclmul       16384  1
ghash_clmulni_intel    16384  0
aesni_intel           372736  0
crypto_simd            16384  1 aesni_intel
cryptd                 24576  2 crypto_simd,ghash_clmulni_intel
glue_helper            16384  1 aesni_intel
cirrus                 16384  0
drm_kms_helper        184320  3 cirrus
fb_sys_fops            16384  1 drm_kms_helper
syscopyarea            16384  1 drm_kms_helper
input_leds             16384  0
joydev                 24576  0
sysfillrect            16384  1 drm_kms_helper
serio_raw              20480  0
sysimgblt              16384  1 drm_kms_helper
mac_hid                16384  0
qemu_fw_cfg            20480  0
sch_fq_codel           20480  2
lp                     20480  0
parport                53248  1 lp
ramoops                28672  0
reed_solomon           24576  1 ramoops
efi_pstore             16384  0
drm                   495616  3 drm_kms_helper,cirrus
sunrpc                397312  1
ip_tables              32768  0
```



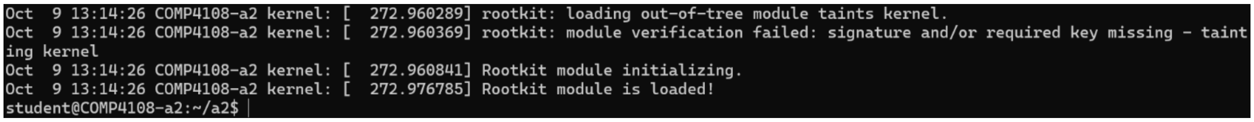
```
x_tables               40960  1 ip_tables
autofs4                45056  2
hid_generic            16384  0
usbhid                 57344  0
hid                   131072  2 usbhid,hid_generic
crc32_pclmul           16384  0
psmouse               155648  0
virtio_net             57344  0
net_failover           20480  1 virtio_net
floppy                 81920  0
i2c_piix4              28672  0
pata_acpi              16384  0
failover               16384  1 net_failover
virtio_blk             20480  3
root@COMP4108-a2:/home/student/a2#
```

Syslog file shows rootkit module is unloaded:



```
Sep 27 13:11:49 COMP4108-a2 kernel: [ 4322.477817] Rootkit module is unloaded!
Sep 27 13:11:49 COMP4108-a2 kernel: [ 4322.477821] Rootkit module cleanup copmlete.
```

8.



```
Oct  9 13:14:26 COMP4108-a2 kernel: [  272.960289] rootkit: loading out-of-tree module taints kernel.
Oct  9 13:14:26 COMP4108-a2 kernel: [  272.960369] rootkit: module verification failed: signature and/or required key missing - taint
ing kernel
Oct  9 13:14:26 COMP4108-a2 kernel: [  272.960841] Rootkit module initializing.
Oct  9 13:14:26 COMP4108-a2 kernel: [  272.976785] Rootkit module is loaded!
student@COMP4108-a2:~/a2$
```

9.

We have execution permissions to run the insmod binary owned by root (insmod is run by the insert.sh bash script), which loads our rootkit module to the kernel. Had we not had that permission enabled, we wouldn't have been able to load that rootkit module to the kernel. Therefore, the Least-Privilege principle would help mitigate this risk. Another principle that would help mitigate rootkit risks is Isolated-Compartments, since we would avoid this scenario where we have a link to the insmod program that has 777 permissions on it (allowing us, non-root users, to run the insmod program that inserts the module). Isolated compartments allows us to isolate the components so that the permissions of one file cannot allow us access to the other file.

Part B:

1.