

COMP 4108 Assignment 2

Rootkits

1)2)

```
student@COMP4108-a2:~$ wget --user comp4108 --password z48QVUanF2wYV49A https://www.cisl.carleton.ca/~hpatel/comp4108/private/code/a2/a2.tar.gz
```

```
student@COMP4108-a2:~$ ls -la
total 60
drwxr-xr-x 7 student student 4096 Sep 27 11:56 .
drwxr-xr-x 4 root     root    4096 Jan 23  2017 ..
-rw-rw-r-- 1 student student 2647 Aug 22 14:54 a2.tar.gz
```

3)

```
root@COMP4108-a2:/home/student# grep "sys_call_table" /proc/kallsyms
fffffffffaae002a0 R x32_sys_call_table
fffffffffaae013c0 R sys_call_table
fffffffffaae02400 R ia32_sys_call_table
```

sys_call_table has the address ffffffff013c0 and is also read only. The other two aren't relevant for the rootkit.c file

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;
}
```

sys_call_table from above used for the kallsyms_lookup_name

5)

```
student@COMP4108-a2:~/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'
```

Make doesn't give any errors. Only warnings

6)

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

Rootkit successfully inserted.

7)

```
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
```

Rootkit ejected, rootkit should appear at top if it was there.

```
root@COMP4108-a2:/home/student/a2# tail /var/log/syslog
Sep 27 12:29:22 COMP4108-a2 systemd[1]: Started Session 8 of user student.
Sep 27 12:30:01 COMP4108-a2 CRON[2930]: (root) CMD ([ -x /etc/init.d/anacron ] && if [ ! -d /
run/systemd/system ]; then /usr/sbin/invoke-rc.d anacron start >/dev/null; fi)
Sep 27 12:34:09 COMP4108-a2 systemd[1]: Started Run anacron jobs.
Sep 27 12:34:09 COMP4108-a2 anacron[4752]: Anacron 2.3 started on 2024-09-27
Sep 27 12:34:09 COMP4108-a2 anacron[4752]: Normal exit (0 jobs run)
Sep 27 12:34:09 COMP4108-a2 systemd[1]: anacron.service: Succeeded.
Sep 27 12:34:20 COMP4108-a2 kernel: [ 3646.647607] Rootkit module initializing.
Sep 27 12:34:20 COMP4108-a2 kernel: [ 3646.664556] Rootkit module is loaded!
Sep 27 12:35:44 COMP4108-a2 kernel: [ 3730.289905] Rootkit module is unloaded!
Sep 27 12:35:44 COMP4108-a2 kernel: [ 3730.289908] Rootkit module cleanup complete.
```

Print messages in rootkit.c are printing indicating the hook is happening while on sudo bash shell

8)

```
root@COMP4108-a2:/home/student/a2# cat benos.txt
benos
```

```
Oct 15 22:21:28 COMP4108-a2 kernel: [1594070.754020] Rootkit module initializing.
Oct 15 22:21:28 COMP4108-a2 kernel: [1594070.769119] Rootkit module is loaded!
Oct 15 22:27:45 COMP4108-a2 kernel: [1594448.008532] openat() called for benos.txt
```

With the module inserted using the “cat” command on a txt file invokes the new_openat() function as seen in the above syslog snippet.

9)

Least privilege is important for the mitigation of rootkits because rootkits rely on access to higher privileged files to get going. Denying the higher privileged files from normal users would mitigate most rootkit delivery.

Datatype validation would also greatly minimize the variables that an attacker to insert into their own custom syscalls using a rootkit.

Part B)