Project Rootkit documentation

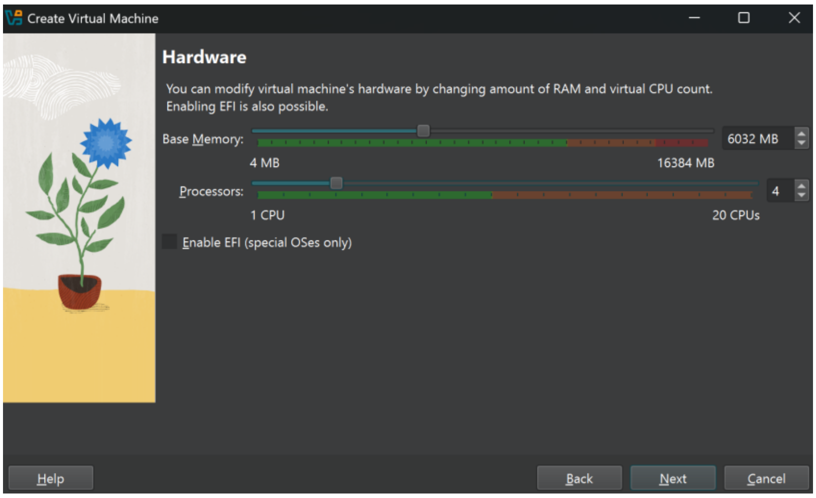
Github link containing code: https://github.com/yousuf865/Project-Rootkit/

Introduction

This is not an exploit. This assumes prior privileged access on a server in order to be inserted in the first place. Instead, it is a sophisticated method to burden the victim's CPU with an unnecessary load through a cryptojacker program, which is covered up with a rootkit. The intention isn't to cause the victim's system to crash, but to slow it down by consuming its CPU in a persistent and subtle manner. As such, the crypto-jacker allows easy manipulation of the amount of CPU it consumes on the victim's machine.

Setup

I installed Ubuntu version 22.04, and launched it through VirtualBox. Assigned 6GB RAM, and 4 CPU cores to the VM, and 30GB of storage.



Create Virtual Machine

Hardware

You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 6032 MB

Processors: 4

□ Enable EFI (special OSes only)

Crypto-jacker

Recall that I assigned 4 CPU's to the VM when I was setting it up. After implementing my cryptojacker in a way such that I allowed one variable to be changed in the program to tweak the CPU usage, I played around with different variable values and used the 'top' command to monitor theCPU usage each time I changed the variable value.

From the two images below, the first is the output of 'top' when I set the variable num_threads, the threads that execute this process, to 1, and the second is when I set it to 2. These images show that each thread that runs occupies approximately a whole logical core, since the cryptojacker process (first line of the processes table) is 100% in the first image – meaning it uses 1 CPU, and is 200% in the second image - meaning it uses 2 CPU's.

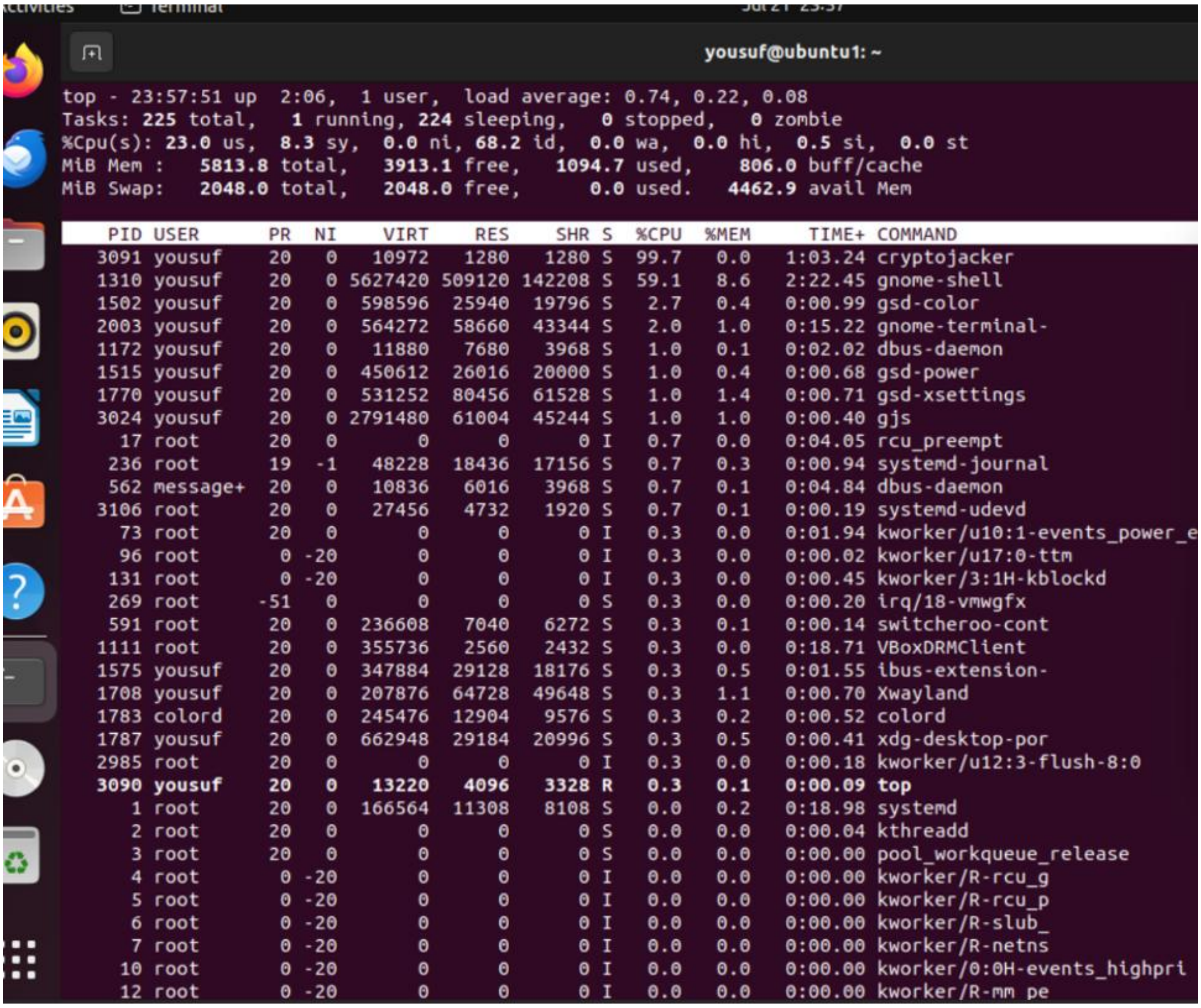
Also notice the '%Cpu(s): 23.0 us' in the first image. This is saying that 23% of the entire CPU available is being dedicated to user processes, which includes the cryptojacker process. Since we have 4 CPU's available here, and we use approximately a quarter with 23%, this again confirms that the one thread running in the cryptojacker program uses up approximately one CPU.

In the second image, we have '%Cpu(s): 46.8 us', which is expected as there are 2 threads running, and it uses approximately 2 whole CPU's.

Using 3 threads in the cryptojacking process resulted in 3 CPU's being used, and from this, we can interpret that there is a linear relationship between the threads running in the cryptojacking program and the amount of CPU's it uses.

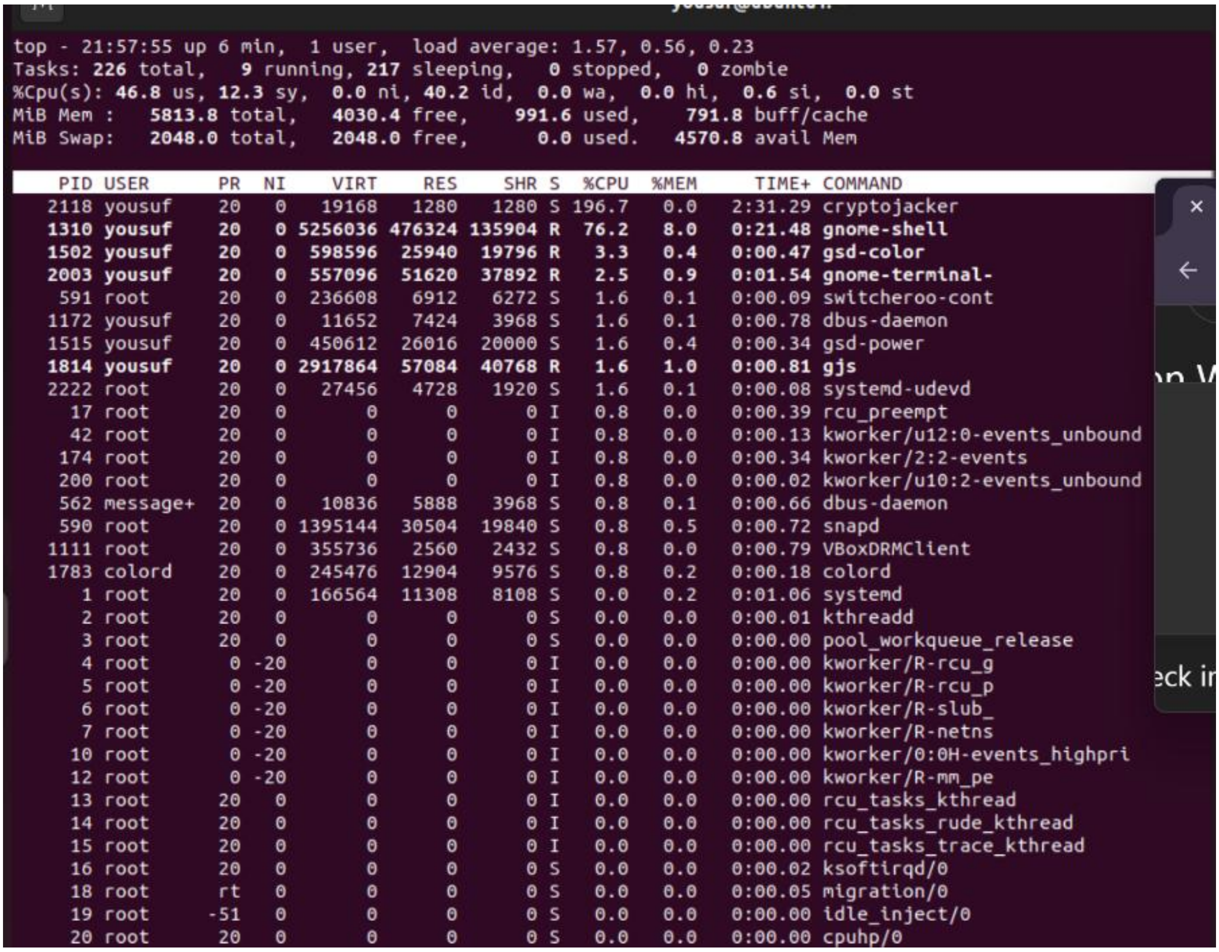
More formally it is CPU % ≈ num_threads × 100

This would be generally consistent with different machines as well, but it may slightly differ due to various factors.



```
top - 23:57:51 up  2:06,  1 user,  load average: 0.74, 0.22, 0.08
Tasks: 225 total,   1 running, 224 sleeping,   0 stopped,   0 zombie
%Cpu(s): 23.0 us,  8.3 sy,  0.0 ni, 68.2 id,  0.0 wa,  0.0 hi,  0.5 si,  0.0 st
MiB Mem :   5813.8 total,   3913.1 free,   1094.7 used,    806.0 buff/cache
MiB Swap:   2048.0 total,   2048.0 free,      0.0 used.   4462.9 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   3091 yousuf    20   0   10972   1280   1280 S  99.7   0.0   1:03.24 cryptojacker
   1310 yousuf    20   0 5627420 509120 142208 S  59.1   8.6   2:22.45 gnome-shell
   1502 yousuf    20   0  598596  25940  19796 S   2.7   0.4   0:00.99 gsd-color
   2003 yousuf    20   0  564272  58660  43344 S   2.0   1.0   0:15.22 gnome-terminal-
   1172 yousuf    20   0   11880   7680   3968 S   1.0   0.1   0:02.02 dbus-daemon
   1515 yousuf    20   0  450612  26016  20000 S   1.0   0.4   0:00.68 gsd-power
   1770 yousuf    20   0  531252  80456  61528 S   1.0   1.4   0:00.71 gsd-xsettings
   3024 yousuf    20   0 2791480  61004  45244 S   1.0   1.0   0:00.40 gjs
     17 root      20   0       0      0      0 I   0.7   0.0   0:04.05 rcu_preempt
    236 root      19  -1   48228  18436  17156 S   0.7   0.3   0:00.94 systemd-journal
    562 message+  20   0   10836   6016   3968 S   0.7   0.1   0:04.84 dbus-daemon
   3106 root      20   0   27456   4732   1920 S   0.7   0.1   0:00.19 systemd-udevd
     73 root      20   0       0      0      0 I   0.3   0.0   0:01.94 kworker/u10:1-events_power_e
     96 root       0 -20       0      0      0 I   0.3   0.0   0:00.02 kworker/u17:0-ttm
    131 root       0 -20       0      0      0 I   0.3   0.0   0:00.45 kworker/3:1H-kblockd
    269 root     -51   0       0      0      0 S   0.3   0.0   0:00.20 irq/18-vmwgfx
    591 root      20   0  236608   7040   6272 S   0.3   0.1   0:00.14 switcheroo-cont
   1111 root      20   0  355736   2560   2432 S   0.3   0.0   0:18.71 VBoxDRMClient
   1575 yousuf    20   0  347884  29128  18176 S   0.3   0.5   0:01.55 ibus-extension-
   1708 yousuf    20   0  207876  64728  49648 S   0.3   1.1   0:00.70 Xwayland
   1783 colord    20   0  245476  12904   9576 S   0.3   0.2   0:00.52 colord
   1787 yousuf    20   0  662948  29184  20996 S   0.3   0.5   0:00.41 xdg-desktop-por
   2985 root      20   0       0      0      0 I   0.3   0.0   0:00.18 kworker/u12:3-flush-8:0
   3090 yousuf    20   0   13220   4096   3328 R   0.3   0.1   0:00.09 top
      1 root      20   0  166564  11308   8108 S   0.0   0.2   0:18.98 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.04 kthreadd
      3 root      20   0       0      0      0 S   0.0   0.0   0:00.00 pool_workqueue_release
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-rcu_g
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-rcu_p
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-slub_
      7 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-netns
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
     12 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-mm_pe
```



```
top - 21:57:55 up 6 min,  1 user,  load average: 1.57, 0.56, 0.23
Tasks: 226 total,   9 running, 217 sleeping,   0 stopped,   0 zombie
%Cpu(s): 46.8 us, 12.3 sy,  0.0 ni, 40.2 id,  0.0 wa,  0.0 hi,  0.6 si,  0.0 st
MiB Mem :   5813.8 total,   4030.4 free,    991.6 used,    791.8 buff/cache
MiB Swap:   2048.0 total,   2048.0 free,      0.0 used.   4570.8 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   2118 yousuf    20   0   19168   1280   1280 S 196.7   0.0   2:31.29 cryptojacker
   1310 yousuf    20   0 5256036 476324 135904 R  76.2   8.0   0:21.48 gnome-shell
   1502 yousuf    20   0  598596  25940  19796 R   3.3   0.4   0:00.47 gsd-color
   2003 yousuf    20   0  557096  51620  37892 R   2.5   0.9   0:01.54 gnome-terminal-
    591 root      20   0  236608   6912   6272 S   1.6   0.1   0:00.09 switcheroo-cont
   1172 yousuf    20   0   11652   7424   3968 S   1.6   0.1   0:00.78 dbus-daemon
   1515 yousuf    20   0  450612  26016  20000 S   1.6   0.4   0:00.34 gsd-power
   1814 yousuf    20   0 2917864  57084  40768 R   1.6   1.0   0:00.81 gjs
   2222 root      20   0   27456   4728   1920 S   1.6   0.1   0:00.08 systemd-udevd
     17 root      20   0       0      0      0 I   0.8   0.0   0:00.39 rcu_preempt
     42 root      20   0       0      0      0 I   0.8   0.0   0:00.13 kworker/u12:0-events_unbound
    174 root      20   0       0      0      0 I   0.8   0.0   0:00.34 kworker/2:2-events
    200 root      20   0       0      0      0 I   0.8   0.0   0:00.02 kworker/u10:2-events_unbound
    562 message+  20   0   10836   5888   3968 S   0.8   0.1   0:00.66 dbus-daemon
    590 root      20   0 1395144  30504  19840 S   0.8   0.5   0:00.72 snapd
   1111 root      20   0  355736   2560   2432 S   0.8   0.0   0:00.79 VBoxDRMClient
   1783 colord    20   0  245476  12904   9576 S   0.8   0.2   0:00.18 colord
      1 root      20   0  166564  11308   8108 S   0.0   0.2   0:01.06 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
      3 root      20   0       0      0      0 S   0.0   0.0   0:00.00 pool_workqueue_release
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-rcu_g
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-rcu_p
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-slub_
      7 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-netns
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
     12 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-mm_pe
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread
     14 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread
     15 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread
     16 root      20   0       0      0      0 S   0.0   0.0   0:00.02 ksoftirqd/0
     18 root      rt   0       0      0      0 S   0.0   0.0   0:00.05 migration/0
     19 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/0
     20 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
```

Initially I was printing logs that said “Crypto mining has started” etc. but I removed these logs as one of the purposes of rootkits is to be stealthy.

I also implemented daemonization to allow the crypto-jacker to run in the background without it occupying a terminal. Then to be able to stop the process, I created a hidden file (in /tmp/.cryptojacker.pid) which contains the process ID of the crypto-jacker, which I can use to kill the process.

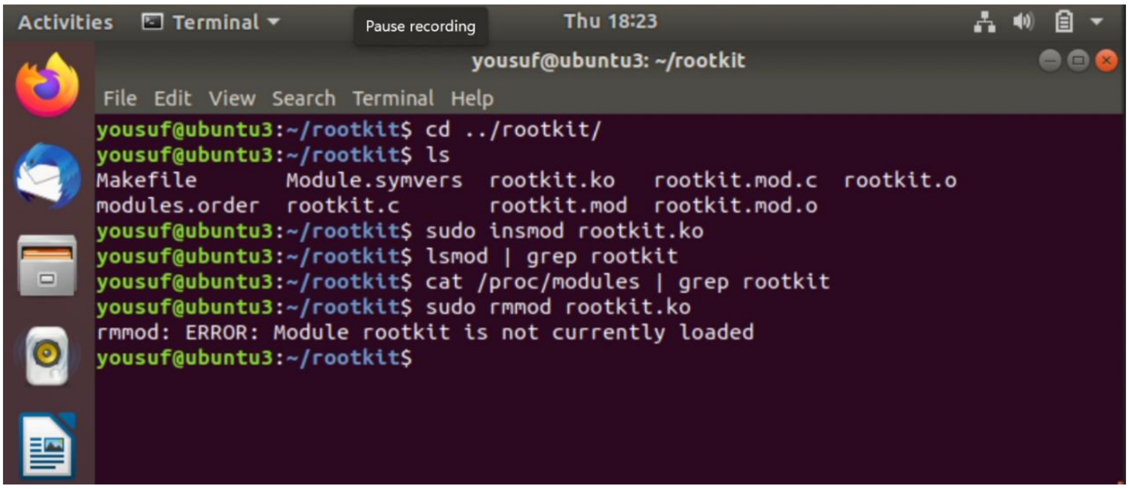
Rootkit

Initially I was trying to hide the files such as cryptojacker.c and rootkit.c. Halfway through this, I realised that there is no need for the files at all, and this fits well within a realistic situation, where once the cryptojacking process is spawned and the rootkit is inserted, there's no need for the files. Also, leaving the files there would be counterproductive as one of the intentions of the malware package is that it should be stealthy, so having these files would broaden the vector from which the malware package can be discovered or compromised. Thus the intended use of the package includes deleting the files once the process is spawned and the kernel module is inserted.

I used to DKOM (Direct Kernel Object Manipulation) as opposed to syscall hooking, initially due to restrictions of the linux version, and directly modified the kernel structures to unlink the crypto-jacking process, which also benefited me as it was also a lot more stealthy.

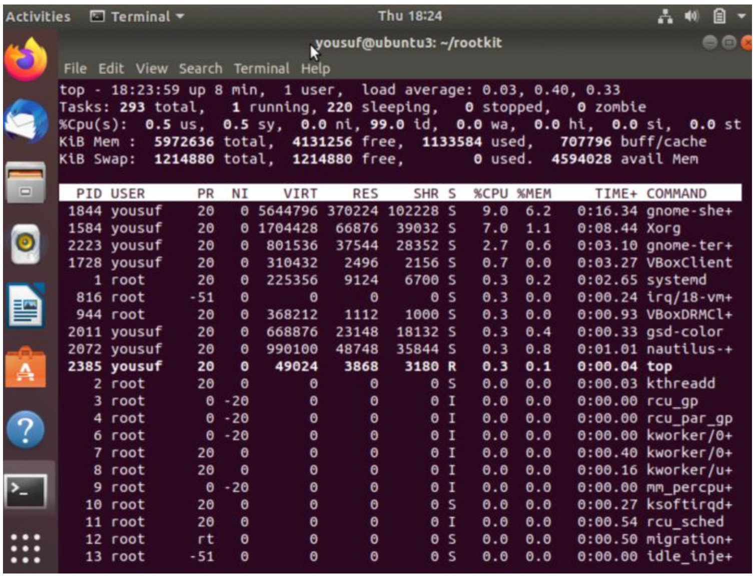
Once more, I had to delete the VM and everything relevant to it, as well as the version of Ubuntu that I was currently using. I then installed version 18.04 of Ubuntu and launched a new VM instance with it. I continued using DKOM and the rootkit worked on this version.

The rootkit's kernel module hides itself, and the traditional 'rmmod (remove module)' command doesn't work


Activities
Terminal
Pause recording
Thu 18:23
yousuf@ubuntu3: ~/rootkit
File Edit View Search Terminal Help

```
yousuf@ubuntu3:~/rootkit$ cd ../rootkit/
yousuf@ubuntu3:~/rootkit$ ls
Makefile       Module.symvers  rootkit.ko   rootkit.mod.c  rootkit.o
modules.order  rootkit.c       rootkit.mod  rootkit.mod.o
yousuf@ubuntu3:~/rootkit$ sudo insmod rootkit.ko
yousuf@ubuntu3:~/rootkit$ lsmod | grep rootkit
yousuf@ubuntu3:~/rootkit$ cat /proc/modules | grep rootkit
yousuf@ubuntu3:~/rootkit$ sudo rmmod rootkit.ko
rmmod: ERROR: Module rootkit is not currently loaded
yousuf@ubuntu3:~/rootkit$
```

The crypto-jacking process doesn’t appear once the rootkit is loaded



Activities
Terminal
Thu 18:24
yousuf@ubuntu3: ~/rootkit
File Edit View Search Terminal Help

```
top - 18:23:59 up 8 min,  1 user,  load average: 0.03, 0.40, 0.33
Tasks: 293 total,   1 running, 220 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.5 us,  0.5 sy,  0.0 ni, 99.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  5972636 total,  4131256 free,  1133584 used,   707796 buff/cache
KiB Swap:  1214880 total,  1214880 free,        0 used.  4594028 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
 1844 yousuf    20   0 5644796 370224 102228 S   9.0  6.2   0:16.34 gnome-she+
 1584 yousuf    20   0 1704428  66876  39032 S   7.0  1.1   0:08.44 Xorg
 2223 yousuf    20   0  801536  37544  28352 S   2.7  0.6   0:03.10 gnome-ter+
 1728 yousuf    20   0  310432   2496   2156 S   0.7  0.0   0:03.27 VBoxClient
    1 root      20   0  225356   9124   6700 S   0.3  0.2   0:02.65 systemd
  816 root     -51   0       0      0      0 S   0.3  0.0   0:00.24 irq/18-vm+
  944 root      20   0  368212   1112   1000 S   0.3  0.0   0:00.93 VBoxDRMCl+
 2011 yousuf    20   0  668876  23148  18132 S   0.3  0.4   0:00.33 gsd-color
 2072 yousuf    20   0  990100  48748  35844 S   0.3  0.8   0:01.01 nautilus-+
 2385 yousuf    20   0   49024   3868   3180 R   0.3  0.1   0:00.04 top
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.03 kthreadd
    3 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 rcu_gp
    4 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 rcu_par_gp
    6 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 kworker/0+
    7 root      20   0       0      0      0 I   0.0  0.0   0:00.40 kworker/0+
    8 root      20   0       0      0      0 I   0.0  0.0   0:00.16 kworker/u+
    9 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 mm_percpu+
   10 root      20   0       0      0      0 S   0.0  0.0   0:00.27 ksoftirqd+
   11 root      20   0       0      0      0 I   0.0  0.0   0:00.54 rcu_sched
   12 root      rt   0       0      0      0 S   0.0  0.0   0:00.50 migration+
   13 root     -51   0       0      0      0 S   0.0  0.0   0:00.00 idle_inje+
```