

# Lab 2.2

By: Nathan Metens ([metens@pdx.edu](mailto:metens@pdx.edu))

<b>Task 1: Accounts - useradd, passwd, id</b>	<b>1</b>
<b>Task 1.1: Duplicate UIDs</b>	<b>2</b>
<b>Task 2: umask</b>	<b>3</b>
<b>Task 3: chmod</b>	<b>4</b>
<b>Task 4: groups, newgrp, chgrp</b>	<b>4</b>
<b>Task 5: setuid bit, sudo</b>	<b>5</b>
<b>Task 6: Using sudo, chown</b>	<b>5</b>
<b>Task 7: Process - w, tty, /proc</b>	<b>9</b>
<b>Task 8: pstree, killall</b>	<b>11</b>
<b>Task 9: Configuration issues - PATH hijacking</b>	<b>12</b>
<b>Task 10: sshd</b>	<b>15</b>
<b>Task 11: TryHackMe Linux process analysis</b>	<b>16</b>

## Task 1: Accounts - useradd, passwd, id

The screenshot shows a terminal window titled "myuser@cs591-metens-kali-1: ~". The terminal history is as follows:

```
(metens㉿cs591-metens-kali-1)~]$ id
uid=1000(metens) gid=1000(metens) groups=1000(metens),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),103(scanner),116(bluetooth),121(lpadmin),124(wireshark),133(kaboxer)

(metens㉿cs591-metens-kali-1)~]$ sudo useradd -m -d /home/myuser -s /bin/bash myuser
[sudo] password for metens:

(metens㉿cs591-metens-kali-1)~]$ sudo passwd myuser
New password:
Retype new password:
passwd: password updated successfully

(metens㉿cs591-metens-kali-1)~]$ su - myuser
Password:
(myuser㉿cs591-metens-kali-1)~]$ id
uid=1001(myuser) gid=1001(myuser) groups=1001(myuser)

(myuser㉿cs591-metens-kali-1)~]$
```

The uid and gid of my account (metens) are 1000 and 1000, respectively.

The uid and gid of the new account (myuser) are 1001 and 1001, respectively.

## Task 1.1: Duplicate UIDs

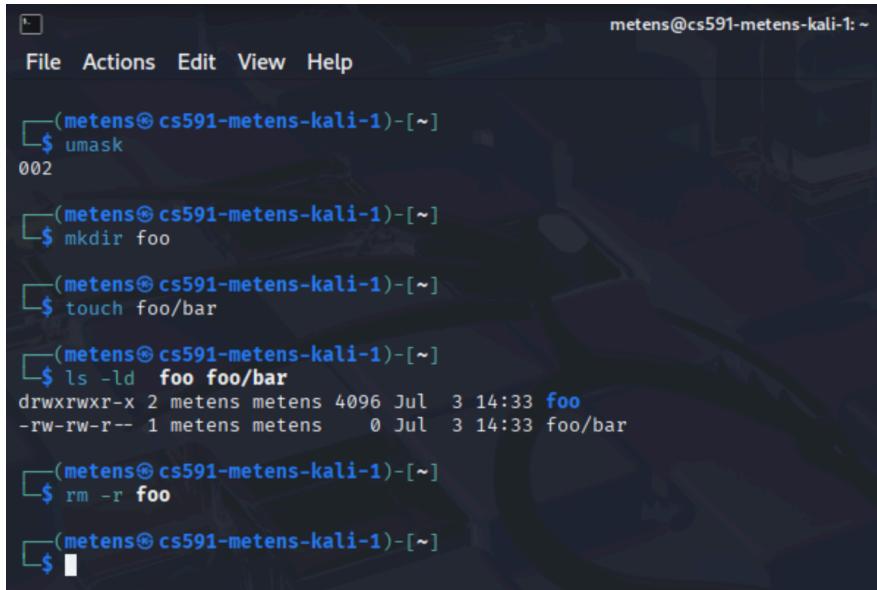
```
metens:x:1000:1000:metens,,,,:/home/metens:/usr/bin/zsh
myuser:x:1001:1001::/home/myuser:/bin/bash
hacker:x:0:0::/root:/bin/bash
~
"/etc/passwd" 57L, 3226B written
```

```
metens:$y$j9T$17.y20WF BwU V93.0TH7dN.$Y0aq2pn3LRps oQujArVGsxdgp06rS0QCaIg8KXz.IY6:20265:0:99999:7 :::
myuser:$y$j9T$R57.tR1L1cKSGXz0poxDK0$Cg2ytP810gyI4J6HbE0uX3rMVbmP5TLP/6sTyE0dzI8:20270:0:99999:7 :::
hacker:$y$j9T$8xG5XibWEPE3YQkw1Q4.N1$T65mXEYJonvPndC/A72fxpXllx2p4bquzlA6eCiufx9:20270:0:99999:7 :::
```

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "cs491-metens-kali-1 (Snapshot 3 - lab 2.1) [Running]". The terminal session shows the following steps:

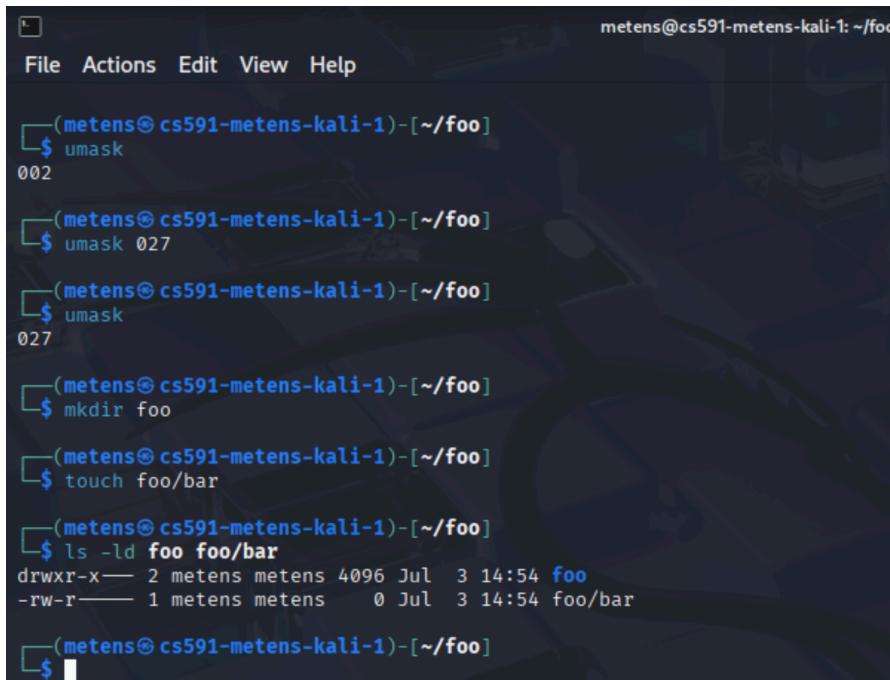
- \$ sudo useradd -m -d /home/hacker -s /bin/bash hacker
- \$ sudo passwd hacker
- New password: (user enters a password)
- Retype new password: (user re-enters the password)
- passwd: password updated successfully
- \$ sudo vim /etc/passwd
- (metens@cs591-metens-kali-1:~)
- \$ su - hacker
- Password: (user enters the password)
- # vim /etc/shadow
- shadow shadow- shells
- (root@cs591-metens-kali-1:~)
- # vim /etc/shadow
- (root@cs591-metens-kali-1:~)
- # id
- uid=0(root) gid=0(root) groups=0(root)
- (root@cs591-metens-kali-1:~)
- # tail -n 2 /etc/passwd
- myuser:x:1001:1001::/home/myuser:/bin/bash
- hacker:x:0:0::/root:/bin/bash
- (root@cs591-metens-kali-1:~)
- # tail -n 2 /etc/shadow
- myuser:\$y\$j9T\$R57.tR1L1cKSGXz0poxDK0\$Cg2ytP810gyI4J6HbE0uX3rMVbmP5TLP/6sTyE0dzI8:20270:0:99999:7 :::
- hacker:\$y\$j9T\$8xG5XibWEPE3YQkw1Q4.N1\$T65mXEYJonvPndC/A72fxpXllx2p4bquzlA6eCiufx9:20270:0:99999:7 :::
- (root@cs591-metens-kali-1:~)
- # id
- uid=0(root) gid=0(root) groups=0(root)
- (root@cs591-metens-kali-1:~)
- #

## Task 2: umask



```
metens@cs591-metens-kali-1: ~
File Actions Edit View Help
└──(metens@cs591-metens-kali-1)-[~]
    $ umask
002
└──(metens@cs591-metens-kali-1)-[~]
    $ mkdir foo
└──(metens@cs591-metens-kali-1)-[~]
    $ touch foo/bar
└──(metens@cs591-metens-kali-1)-[~]
    $ ls -ld foo foo/bar
drwxrwxr-x 2 metens metens 4096 Jul  3 14:33 foo
-rw-rw-r-- 1 metens metens     0 Jul  3 14:33 foo/bar
└──(metens@cs591-metens-kali-1)-[~]
    $ rm -r foo
└──(metens@cs591-metens-kali-1)-[~]
    $ ┌─
```

Since file permissions are organized in an owner-group-others fashion, and each group can have a bit for read, write, and execute, this means that for full access, rwx -> 111, the first value in the umask (owner) must be 7. Then, for read and execute permissions on the group, r-x -> 101, the second umask value will be 5. Finally, no access to others would be 0. So we have 750 as our file permissions. To get the umask value, we subtract out permissions from the maximum value for full permissions, which would be 777. So we get a umask of  $777-750 = 027$ . Now we can change to that umask value in the shell:



```
metens@cs591-metens-kali-1: ~/foo
File Actions Edit View Help
└──(metens@cs591-metens-kali-1)-[~/foo]
    $ umask
002
└──(metens@cs591-metens-kali-1)-[~/foo]
    $ umask 027
└──(metens@cs591-metens-kali-1)-[~/foo]
    $ umask
027
└──(metens@cs591-metens-kali-1)-[~/foo]
    $ mkdir foo
└──(metens@cs591-metens-kali-1)-[~/foo]
    $ touch foo/bar
└──(metens@cs591-metens-kali-1)-[~/foo]
    $ ls -ld foo foo/bar
drwxr-x--- 2 metens metens 4096 Jul  3 14:54 foo
-rw-r----- 1 metens metens     0 Jul  3 14:54 foo/bar
└──(metens@cs591-metens-kali-1)-[~/foo]
    $ ┌─
```

## Task 3: chmod

```
└─(metens@cs591-metens-kali-1)─[~/foo]
  └─$ ls -ld foo/bar foo
  drwxr-x— 2 metens metens 4096 Jul  3 14:54 foo
  -rw-r— 1 metens metens     0 Jul  3 14:54 foo/bar

└─(metens@cs591-metens-kali-1)─[~/foo]
  └─$ chmod -R o+rX foo

└─(metens@cs591-metens-kali-1)─[~/foo]
  └─$ ls -ld foo/bar foo
  drwxr-xr-x 2 metens metens 4096 Jul  3 14:54 foo
  -rw-r--r-- 1 metens metens     0 Jul  3 14:54 foo/bar
```

I used `‐R` for the recursive flag, ‘o’ for others, and a ‘+rX’ for updating the permissions. The lowercase r for reading the foo/bar file, and the uppercase X for executing the dir foo.

## Task 4: groups, newgrp, chgrp

```
metens@cs591-metens-kali-1: ~/foo
File Actions Edit View Help

└─(metens@cs591-metens-kali-1)─[~/foo]
  └─$ groups
  metens adm dialout cdrom floppy sudo audio dip video plugdev users netdev scanner bluetooth lpadmin wireshark kaboxer

└─(metens@cs591-metens-kali-1)─[~/foo]
  └─$ newgrp adm
└─(metens@cs591-metens-kali-1)─[~/foo]
  └─$ groups
  adm dialout cdrom floppy sudo audio dip video plugdev users netdev scanner bluetooth lpadmin wireshark kaboxer metens

└─(metens@cs591-metens-kali-1)─[~/foo]
  └─$ mkdir foo; touch foo/bar

└─(metens@cs591-metens-kali-1)─[~/foo]
  └─$ ls -ld foo foo/bar
  drwxr-x— 2 metens adm 4096 Jul  3 15:15 foo
  -rw-r— 1 metens adm     0 Jul  3 15:15 foo/bar

└─(metens@cs591-metens-kali-1)─[~/foo]
  └─$ chgrp -R metens foo

└─(metens@cs591-metens-kali-1)─[~/foo]
  └─$ ls -ld foo foo/bar
  drwxr-x— 2 metens metens 4096 Jul  3 15:15 foo
  -rw-r— 1 metens metens     0 Jul  3 15:15 foo/bar

└─(metens@cs591-metens-kali-1)─[~/foo]
  └─$ █
```

## Task 5: setuid bit, sudo

```
metens@cs591-metens-kali-1: ~/foo
File Actions Edit View Help

└─(metens@cs591-metens-kali-1)-[~/foo]
└─$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 142424 Apr 19 03:20 /usr/bin/passwd

└─(metens@cs591-metens-kali-1)-[~/foo]
└─$ touch sudo1; sudo touch sudo2
[sudo] password for metens:

└─(metens@cs591-metens-kali-1)-[~/foo]
└─$ ls -l sudo*
-rw-r-- 1 metens adm 0 Jul 3 15:24 sudo1
-rw-r-- 1 root root 0 Jul 3 15:24 sudo2

└─(metens@cs591-metens-kali-1)-[~/foo]
```

It appears that both files have equal permissions for the owner. However, for one, the owner is metens, and the other's owner is root. I, metens, will be able to read and write the contents of the file, and so will root, but others can't do anything to it, and groups can only read the file.

## Task 6: Using sudo, chown

```
metens@cs591-metens-kali-1: ~/foo
File Actions Edit View Help

└─(metens@cs591-metens-kali-1)-[~/foo]
└─$ ls -l /etc/shadow
-rw-r-- 1 root shadow 1601 Jul 1 12:54 /etc/shadow

└─(metens@cs591-metens-kali-1)-[~/foo]
└─$ cat /etc/shadow
cat: /etc/shadow: Permission denied

└─(metens@cs591-metens-kali-1)-[~/foo]
└─$ █
```

Since the shadow file has no read, write, or execute permissions for the others group, this means I am unable to cat the data inside the file.

```
[metens@cs591-metens-kali-1] ~/foo
$ sudo cat /etc/shadow | egrep "myuser"
myuser:$y$j9T$R57.tR1IcKSGXzOpoxDK0$Cg2ytP810gyI4J6HbE0uX3rMVbmP5TLP/6sTyE0dzI8:20270:0:99999:7 :::
```

```
[metens@cs591-metens-kali-1] ~/foo
$ mkdir foo; touch foo/bar

[metens@cs591-metens-kali-1] ~/foo
$ sudo chown -R myuser foo

[metens@cs591-metens-kali-1] ~/foo
$ ls -ld foo foo/bar
drwxr-x— 2 myuser adm 4096 Jul 3 16:16 foo
-rw-r— 1 myuser adm 0 Jul 3 16:16 foo/bar

[metens@cs591-metens-kali-1] ~/foo
$ 
```

To remove the file and dir, I was not the owner, so I changed to the myuser. However, the contents weren't in myuser's dir. So I tried to delete them from myuser by accessing metens dir structure. This was not possible:

```
[metens@cs591-metens-kali-1] ~/foo
$ ls -ld foo foo/bar
drwxr-x— 2 myuser adm 4096 Jul 3 16:16 foo
-rw-r— 1 myuser adm 0 Jul 3 16:16 foo/bar

[metens@cs591-metens-kali-1] ~/foo
$ rm -r *
zsh: sure you want to delete the only file in /home/metens/foo [yn]? y
rm: descend into write-protected directory 'foo'? y
rm: remove write-protected regular empty file 'foo/bar'? y
rm: cannot remove 'foo/bar': Permission denied

[metens@cs591-metens-kali-1] ~/foo
$ su - myuser
Password:
[myuser@cs591-metens-kali-1] ~
$ rm -rf /home/metens/foo
rm: cannot remove '/home/metens/foo': Permission denied

[myuser@cs591-metens-kali-1] ~
$ 
```

So, I changed back to metens, changed the permissions of the foo dir to be executable by all, and tried to delete from myuser. This also didn't work:

```
(metens㉿cs591-metens-kali-1) [~/foo]
$ chmod +x /home/metens/foo/
```

```
(metens㉿cs591-metens-kali-1) [~/foo]
$ su - myuser
Password:
(myuser㉿cs591-metens-kali-1) [~]
$ rm -rf /home/metens/foo/
rm: cannot remove '/home/metens/foo/': Permission denied
$ exit
```

```
(myuser㉿cs591-metens-kali-1) [~]
$ logout
```

```
(metens㉿cs591-metens-kali-1) [~/foo]
$ chmod -R +x /home/metens/foo/
```

chmod: changing permissions of '/home/metens/foo/foo': Operation not permitted  
chmod: changing permissions of '/home/metens/foo/foo/bar': Operation not permitted

Frustratingly, I couldn't seem to figure this out in less than 30 minutes, which is too long, so I took a break and then searched the web for some guidance... After trying again, I set everything up the same way as before:

```
(metens㉿cs591-metens-kali-1) [~/foo]
$ ls -ld foo foo/bar
drwxr-x--- 2 myuser metens 4096 Jul  3 16:50 foo
-rw-r----- 1 myuser metens     0 Jul  3 16:50 foo/bar
```

Now you can finally:

```
(metens㉿cs591-metens-kali-1) [~/foo]
$ rm foo/bar
rm: remove write-protected regular empty file 'foo/bar'? y
rm: cannot remove 'foo/bar': Permission denied
```

```
(metens㉿cs591-metens-kali-1) [~/foo]
$ rm foo
rm: cannot remove 'foo': Is a directory
```

```
(metens㉿cs591-metens-kali-1) [~/foo]
$ rm -r foo
rm: descend into write-protected directory 'foo'? y
rm: remove write-protected regular empty file 'foo/bar'? y
rm: cannot remove 'foo/bar': Permission denied
```

```
(metens㉿cs591-metens-kali-1) [~/foo]
$ ls -ld foo foo/bar
drwxr-x--- 2 myuser metens 4096 Jul  3 16:50 foo
-rw-r----- 1 myuser metens     0 Jul  3 16:50 foo/bar
```

Here is what I did to be able to delete the bar file:

```
File Actions Edit View Help
[metens@cs591-metens-kali-1] ~ /foo
$ ls -ld foo foo/bar
drwxr-x--- 2 myuser metens 4096 Jul 3 18:19 foo
-rw-r----- 1 myuser metens 0 Jul 3 18:19 foo/bar

[metens@cs591-metens-kali-1] ~ /home/metens
$ chmod +x /home/metens
[metens@cs591-metens-kali-1] ~ /foo
$ chmod +x /home/metens/foo

[metens@cs591-metens-kali-1] ~ /foo
$ chmod +x /home/metens/foo/foo
chmod: changing permissions of '/home/metens/foo/foo': Operation not permitted

[metens@cs591-metens-kali-1] ~ /foo
$ chmod +x /home/metens/foo/foo/bar
chmod: changing permissions of '/home/metens/foo/foo/bar': Operation not permitted

[metens@cs591-metens-kali-1] ~ /foo
$ su - myuser
Password: Now you can finally...
[myuser@cs591-metens-kali-1] ~
$ rm -rf /home/metens/foo/
rm: cannot remove '/home/metens/foo/foo': Permission denied

[myuser@cs591-metens-kali-1] ~
$ rm -rf /home/metens/foo/
rm: cannot remove '/home/metens/foo/foo': Permission denied

[myuser@cs591-metens-kali-1] ~
$ rm -rf /home/metens/foo/foo/bar
[myuser@cs591-metens-kali-1] ~
$ rm -rf /home/metens/foo/foo/
rm: cannot remove '/home/metens/foo/foo': Permission denied

[myuser@cs591-metens-kali-1] ~
$ exit
logout

[metens@cs591-metens-kali-1] ~ /foo
$ ls -ld foo
drwxr-x--- 2 myuser metens 4096 Jul 3 18:21 foo
```

After another 20 minutes of testing and changing mods around, I did this, and it magically worked:

```
File Actions Edit View Help
[myuser@cs591-metens-kali-1] ~
$ chmod u+rxw /home/metens/foo
chmod: changing permissions of '/home/metens/foo': Operation not permitted

[myuser@cs591-metens-kali-1] ~
$ exit
logout

[metens@cs591-metens-kali-1] ~ /foo
$ chmod u+rwx /home/metens/foo

[metens@cs591-metens-kali-1] ~ /foo
ls -ld /home/metens /home/metens/foo /home/metens/foo/foo
drwxr-xr-x 17 metens metens 4096 Jul 3 16:38 /home/metens
drwxr-xr-x 3 metens metens 4096 Jul 3 18:19 /home/metens/foo
drwxr-xr-x 2 myuser metens 4096 Jul 3 18:21 /home/metens/foo/foo

[metens@cs591-metens-kali-1] ~ /foo
$ su - myuser
Password: Finally gone. If not, we rename the machine to "haunt"
[myuser@cs591-metens-kali-1] ~
$ rm -rf /home/metens/foo
rm: cannot remove '/home/metens/foo/foo': Permission denied

[myuser@cs591-metens-kali-1] ~
$ exit
logout

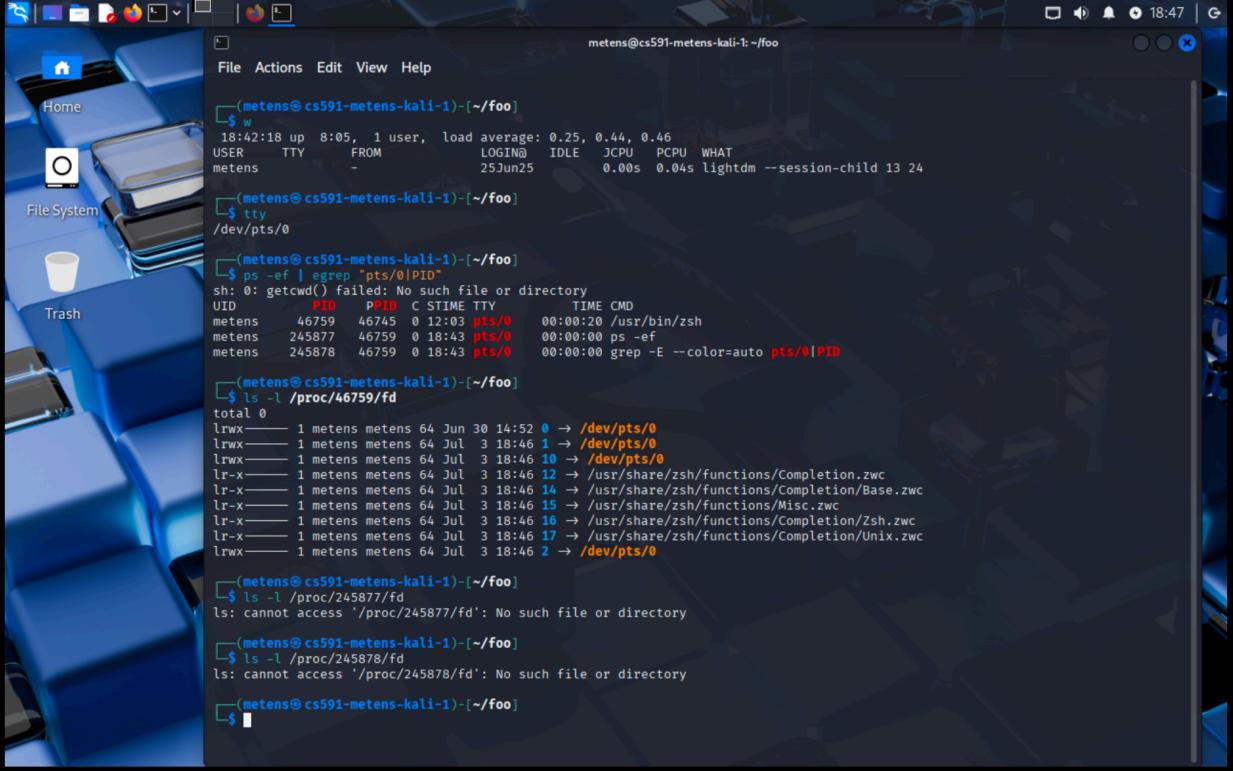
[metens@cs591-metens-kali-1] ~ /foo
$ rm -rf /home/metens/foo

[metens@cs591-metens-kali-1] ~ /foo
$ ls
[metens@cs591-metens-kali-1] ~ /foo
$ ls -ld *
ls: cannot access '*': No such file or directory

[metens@cs591-metens-kali-1] ~ /foo
$ ls -ld .
drwxr-xr-x 0 metens metens 0 Jul 3 18:32 .

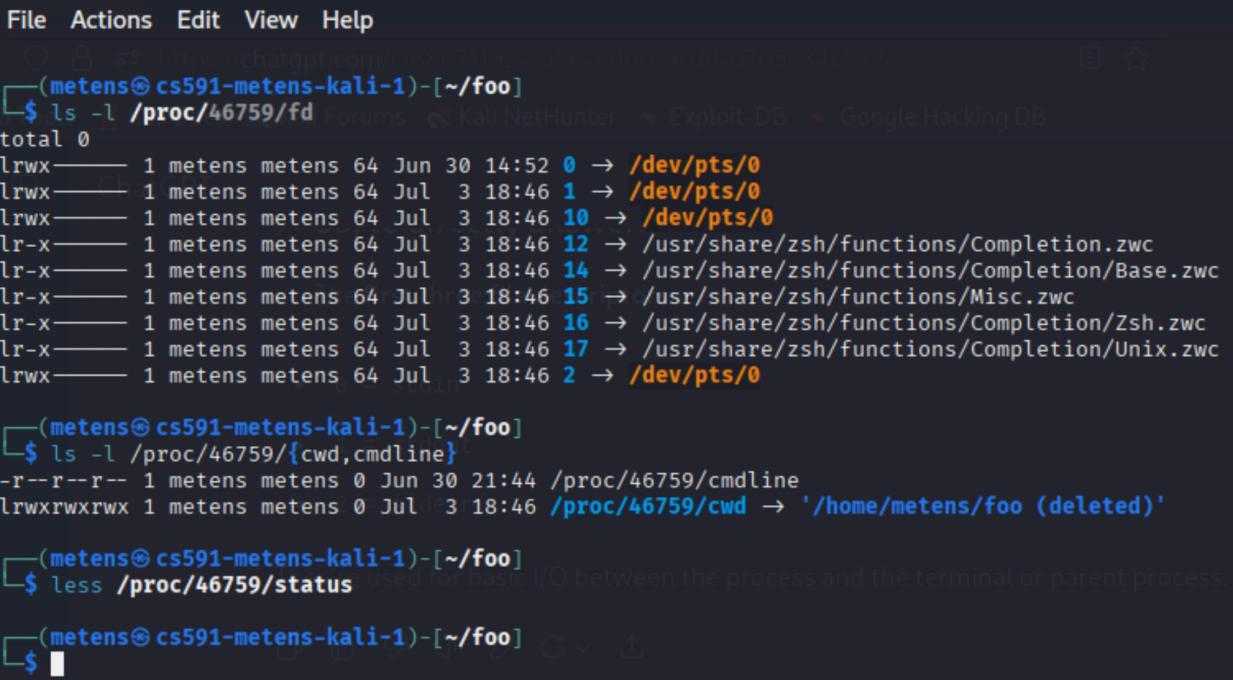
[metens@cs591-metens-kali-1] ~ /foo
$
```

## Task 7: Process - w, tty, /proc

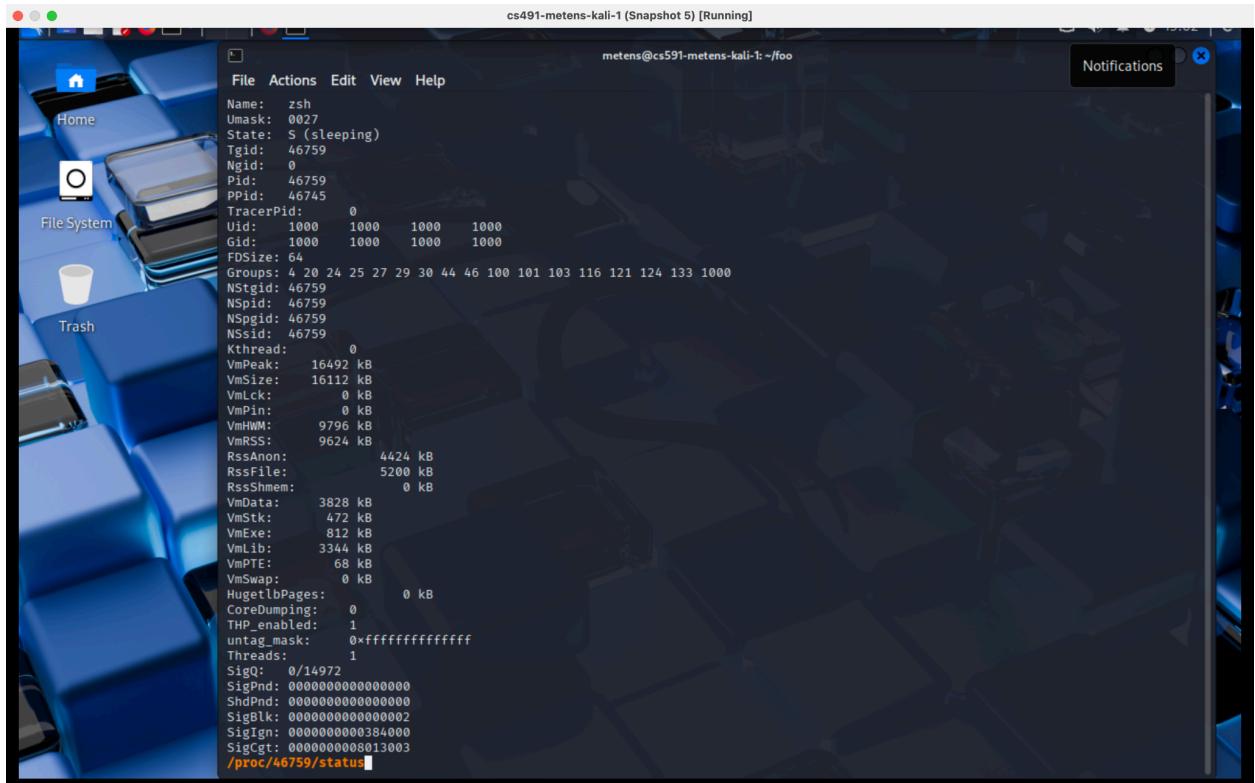


```
metens@cs591-metens-kali-1: ~/foo
File Actions Edit View Help
└── (metens@cs591-metens-kali-1)-[~/foo]
    $ w
    18:42:18 up 8:05, 1 user, load average: 0.25, 0.44, 0.46
    USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
    metens -          25Jun25      0.00s 0.04s lightdm --session-child 13 24
    └── (metens@cs591-metens-kali-1)-[~/foo]
        $ tty
        /dev/pts/0
    └── (metens@cs591-metens-kali-1)-[~/foo]
        $ ps -ef | grep pts/0|PID
        sh: 0: getcwd(): failed: No such file or directory
        UID PID PPID C STIME TTY TIME CMD
        metens 46759 46745 0 12:03 pts/0 00:00:20 /usr/bin/zsh
        metens 245877 46759 0 18:43 pts/0 00:00:00 ps -ef
        metens 245878 46759 0 18:43 pts/0 00:00:00 grep -E --color=auto pts/0|PID
    └── (metens@cs591-metens-kali-1)-[~/foo]
        $ ls -l /proc/46759/fd
        total 0
        lrwx--- 1 metens metens 64 Jun 30 14:52 0 → /dev/pts/0
        lrwx--- 1 metens metens 64 Jul 3 18:46 1 → /dev/pts/0
        lrwx--- 1 metens metens 64 Jul 3 18:46 10 → /dev/pts/0
        lr-x--- 1 metens metens 64 Jul 3 18:46 12 → /usr/share/zsh/functions/Completion.zwc
        lr-x--- 1 metens metens 64 Jul 3 18:46 14 → /usr/share/zsh/functions/Completion/Base.zwc
        lr-x--- 1 metens metens 64 Jul 3 18:46 15 → /usr/share/zsh/functions/Misc.zwc
        lr-x--- 1 metens metens 64 Jul 3 18:46 16 → /usr/share/zsh/functions/Completion/Zsh.zwc
        lr-x--- 1 metens metens 64 Jul 3 18:46 17 → /usr/share/zsh/functions/Completion/Unix.zwc
        lrwx--- 1 metens metens 64 Jul 3 18:46 2 → /dev/pts/0
    └── (metens@cs591-metens-kali-1)-[~/foo]
        $ ls -l /proc/245877/fd
        ls: cannot access '/proc/245877/fd': No such file or directory
    └── (metens@cs591-metens-kali-1)-[~/foo]
        $ ls -l /proc/245878/fd
        ls: cannot access '/proc/245878/fd': No such file or directory
    └── (metens@cs591-metens-kali-1)-[~/foo]
```

After doing some research, the 0 -> /dev/pts/0, 1 -> /dev/pts/0, and 2 -> /dev/pts/0 are linux processes. The 0 references stdin (read), 1 references stdout (write), and 2 references stderr (write and errors). These processes are used for input and output operations on the terminal.



```
File Actions Edit View Help
└── (metens@cs591-metens-kali-1)-[~/foo]
    $ ls -l /proc/46759/fd
    total 0
    lrwx--- 1 metens metens 64 Jun 30 14:52 0 → /dev/pts/0
    lrwx--- 1 metens metens 64 Jul 3 18:46 1 → /dev/pts/0
    lrwx--- 1 metens metens 64 Jul 3 18:46 10 → /dev/pts/0
    lr-x--- 1 metens metens 64 Jul 3 18:46 12 → /usr/share/zsh/functions/Completion.zwc
    lr-x--- 1 metens metens 64 Jul 3 18:46 14 → /usr/share/zsh/functions/Completion/Base.zwc
    lr-x--- 1 metens metens 64 Jul 3 18:46 15 → /usr/share/zsh/functions/Misc.zwc
    lr-x--- 1 metens metens 64 Jul 3 18:46 16 → /usr/share/zsh/functions/Completion/Zsh.zwc
    lr-x--- 1 metens metens 64 Jul 3 18:46 17 → /usr/share/zsh/functions/Completion/Unix.zwc
    lrwx--- 1 metens metens 64 Jul 3 18:46 2 → /dev/pts/0
    └── (metens@cs591-metens-kali-1)-[~/foo]
        $ ls -l /proc/46759/{ cwd, cmdline }
        -r--r--r-- 1 metens metens 0 Jun 30 21:44 /proc/46759/cmdline
        lrwxrwxrwx 1 metens metens 0 Jul 3 18:46 /proc/46759/cwd → '/home/metens/foo (deleted)'
    └── (metens@cs591-metens-kali-1)-[~/foo]
        $ less /proc/46759/status
        used for basic I/O between the process and the terminal or parent process.
    └── (metens@cs591-metens-kali-1)-[~/foo]
```



```
File Actions Edit View Help
Name: zsh
Umask: 0027
State: S (sleeping)
Tgid: 46759
Ngid: 0
Pid: 46759
PPid: 46745
TracerPid: 0
Uid: 1000 1000 1000 1000
Gid: 1000 1000 1000 1000
FDSize: 64
Groups: 4 20 24 25 27 29 30 44 46 100 101 103 116 121 124 133 1000
NSTgid: 46759
NSpid: 46759
NSpgid: 46759
NSsuid: 46759
KThread: 0
VmPeak: 16492 kB
VmSize: 16112 kB
VmLck: 0 kB
VmPin: 0 kB
VmHWM: 9796 kB
VmRSS: 9624 kB
RssAnon: 4424 kB
RssFile: 5200 kB
RssShmem: 0 kB
VmData: 3828 kB
VmStk: 472 kB
VmExe: 812 kB
VmLib: 3344 kB
VmPTE: 68 kB
VmSwap: 0 kB
HugeTlbPages: 0 kB
CoreDumping: 0
THP_enabled: 1
untag_mask: 0xffffffffffff
Threads: 1
SigQ: 0/14972
SigPnd: 0000000000000000
ShdPnd: 0000000000000000
SigBlk: 0000000000000002
SigIgn: 0000000000384000
SigCgt: 0000000008013003
/proc/46759/status
```

The line in the status output that tells us that any file created will be readable by anyone is the line containing “Umask: 0027”. If we do 777-27, we get 750, which means that the owner can rwx, the groups can r-x, but the others cannot do anything 0 -> —.

## Task 8: pstree, killall

```
File Actions Edit View Help
(chatgpt.com) 2023-09-24 15:58:30 UTC - ID: d705c44e949d
[metens@cs591-metens-kali-1:~]
$ vim sleep.bash
[metens@cs591-metens-kali-1:~]
$ chmod +x sleep.bash
[metens@cs591-metens-kali-1:~]
$ ./sleep.bash &          Directories you create will be accessible by you and your group, but not accessible by others.
[1] 269114
[metens@cs591-metens-kali-1:~]
$ ps -ef | grep 269114
metens 269114 46759 0 19:30 pts/0    00:00:00 /bin/bash ./sleep.bash
metens 269116 269114 0 19:30 pts/0    00:00:00 sleep 1000
metens 269117 269114 0 19:30 pts/0    00:00:00 sleep 2000
metens 269118 269114 0 19:30 pts/0    00:00:00 sleep 3000
metens 269119 269114 0 19:30 pts/0    00:00:00 sleep 4000
metens 269245 46759 0 19:30 pts/0    00:00:00 grep -E --color=auto 269114
[metens@cs591-metens-kali-1:~]
$ [redacted]          Files created will NOT be readable by anyone (others) except owner and group.
[metens@cs591-metens-kali-1:~]
$ [redacted]          This is a stricter default than 0022 , which allows others to read files.
```

The 4 sleep commands pop up in the ps listing because each process is independent of the others. The first process (running the bash script in the background), 269114, is the parent process to all the other processes. Each process is run in the background, “hence the & in the script”. The parent id 269114 corresponds to the `./sleep.bash` process that is also in the background because we performed a `./sleep.bash &` to put it in the background as well.

After killing the `./sleep.bash` parent process by its PID, each other sleep process built off of the first one. I did this twice, so there are duplicate processes. However, the first process of sleep 1000 has a PID of 269116, and the other 3 have one count higher than that PID each time. All of them seem to be running independently of each other, so there is no parent process in this case. So, their PPIDs correspond to themselves.

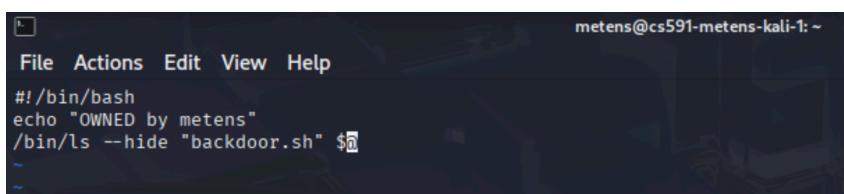
```
(metens@cs591-metens-kali-1) [~]
$ killall sleep
(metens@cs591-metens-kali-1) [~]
$ ps -ef | egrep sleep
metens    278550   46759  0 19:49 pts/0    00:00:00 grep -E --color=auto sleep
(metens@cs591-metens-kali-1) [~]
```

## Task 9: Configuration issues - PATH hijacking

```
(metens@cs591-metens-kali-1) [~]
$ echo $PATH
/home/metens/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
(metens@cs591-metens-kali-1) [~]
$ which ls
ls: aliased to ls --color=auto
(metens@cs591-metens-kali-1) [~]
$ type -a ls
ls is an alias for ls --color=auto
ls is /usr/bin/ls
ls is /bin/ls
(metens@cs591-metens-kali-1) [~]
$ file /bin/ls
/bin/ls: ELF 64-bit LSB pie executable, ARM aarch64, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux-aarch64.so.1, BuildID[sha1]=fe571522db0132bb133f557b075eeb4e9ba76dab, for GNU/Linux 3.7.0, stripped
(metens@cs591-metens-kali-1) [~]
$ touch /etc/cron.daily/backdoor.sh
touch: cannot touch '/etc/cron.daily/backdoor.sh': Permission denied
(metens@cs591-metens-kali-1) [~]
$ ls /etc/cron.daily
apache2 apt-compat backdoor.sh dpkg logrotate man-db plocate sysstat
(metens@cs591-metens-kali-1) [~]
$
```

Since the `'\$PATH` is `/home/metens/.local/bin:/usr/local/sbin:...` and it searches each dir in order from left to right, it will come across the `/bin/ls` directory first before the `/usr/bin/ls` directory to find the correct ls for listing stuff.

As we can see from the `file /bin/ls` command, the ls command is an “ELF executable” binary file type.



The screenshot shows a terminal window with a black background and white text. At the top, it says "metens@cs591-metens-kali-1: ~". Below that is a menu bar with "File", "Actions", "Edit", "View", and "Help". The main area of the terminal contains the following code:

```
#!/bin/bash
echo "OWNED by metens"
/bin/ls --hide "backdoor.sh" $@
```

This part brought me a bunch of issues. I was having trouble with alias and my backdoor ls just wasn't working no matter what I tried:

```
metens@cs591-metens-kali-1:~  
File Actions Edit View Help  
[metens@cs591-metens-kali-1:~]  
$ echo $PATH  
/home/metens/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/usr/local/games:/usr/games  
  
[metens@cs591-metens-kali-1:~]  
$ which ls  
/usr/bin/ls  
  
[metens@cs591-metens-kali-1:~]  
$ type -a ls  
ls is /usr/bin/ls  
ls is /bin/ls  
  
[metens@cs591-metens-kali-1:~]  
$ hash -r  
  
[metens@cs591-metens-kali-1:~]  
$ type -a ls  
ls is /usr/bin/ls  
ls is /bin/ls  
  
[metens@cs591-metens-kali-1:~]  
$ which ls  
/usr/bin/ls  
  
[metens@cs591-metens-kali-1:~]  
$ ls /etc/cron.daily  
apache2 apt-compat backdoor.sh dpkg logrotate man-db plocate sysstat  
  
[metens@cs591-metens-kali-1:~]  
$ \ls  
Desktop Documents Downloads Music Pictures polyglot.pdf Public sleep.bash Templates Videos  
  
[metens@cs591-metens-kali-1:~]  
$ \ls /etc/cron.daily  
apache2 apt-compat backdoor.sh dpkg logrotate man-db plocate sysstat
```

```
metens@cs591-metens-kali-1:~  
File Actions Edit View Help  
[metens@cs591-metens-kali-1:~]  
$ sudo vim /usr/local/sbin/ls  
  
[metens@cs591-metens-kali-1:~]  
$ chmod +x /usr/local/sbin/ls  
chmod: changing permissions of '/usr/local/sbin/ls': Operation not permitted  
  
[metens@cs591-metens-kali-1:~]  
$ sudo chmod +x /usr/local/sbin/ls  
  
[metens@cs591-metens-kali-1:~]  
$ which ls  
ls: aliased to ls --color=auto  
  
[metens@cs591-metens-kali-1:~]  
$ type -a ls  
ls is an alias for ls --color=auto  
          ls is /usr/bin/ls  
          ls is /bin/ls  
  
[metens@cs591-metens-kali-1:~]  
$ hash -r  
  
[metens@cs591-metens-kali-1:~]  
$ ls /etc/cron.daily  
apache2 apt-compat backdoor.sh dpkg logrotate man-db plocate sysstat  
  
[metens@cs591-metens-kali-1:~]  
$ cat /etc/cron.daily/backdoor.sh  
  
[metens@cs591-metens-kali-1:~]  
$ unalias ls  
  
[metens@cs591-metens-kali-1:~]  
$ which ls  
/usr/bin/ls
```

Here are the steps I followed to resolve the issue. I just rechecked my steps, and somehow it worked after that:

```
metens@cs591-metens-kali-1:~  
File Actions Edit View Help  
Volume 40%  
Built-in Audio A  
└──(metens@cs591-metens-kali-1)~  
$ sudo vim /usr/local/sbin/ls  
└──(metens@cs591-metens-kali-1)~  
$ sudo chmod +x /usr/local/sbin/ls  
└──(metens@cs591-metens-kali-1)~  
$ which ls  
/usr/local/sbin/ls  
└──(metens@cs591-metens-kali-1)~  
$ hash -r  
└──(metens@cs591-metens-kali-1)~  
$ ls /etc/cron.daily  
/bin/bash: /usr/local/sbin/ls: Permission denied  
└──(metens@cs591-metens-kali-1)~  
$ sudo ls /etc/cron.daily  
OWNED by metens  
apache2 apt-compat dpkg logrotate man-db plocate sysstat  
└──(metens@cs591-metens-kali-1)~  
$ sudo echo $PATH  
/home/metens/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/b  
/local/games:/usr/games  
└──(metens@cs591-metens-kali-1)~  
$ ls /etc/cron.daily  
/bin/bash: /usr/local/sbin/ls: Permission denied  
└──(metens@cs591-metens-kali-1)~  
$ ls -l /usr/local/sbin/ls  
/bin/bash: /usr/local/sbin/ls: Permission denied  
└──(metens@cs591-metens-kali-1)~  
$ sudo -l /usr/local/sbin/ls  
/usr/local/sbin/ls  
└──(metens@cs591-metens-kali-1)~  
$ sudo chmod 755 /usr/local/sbin/ls
```

```
(metens@cs591-metens-kali-1)~  
└──(metens@cs591-metens-kali-1)~  
$ sudo -l /usr/local/sbin/ls  
/usr/local/sbin/ls  
└──(metens@cs591-metens-kali-1)~  
$ sudo ls -l /usr/local/sbin/ls  
OWNED by metens  
-rwxr-xr-x 1 root root 69 Jul 4 00:04 /usr/local/sbin/ls  
└──(metens@cs591-metens-kali-1)~  
$ ls /etc/cron.daily  
OWNED by metens  
apache2 apt-compat dpkg logrotate man-db plocate sysstat  
└──(metens@cs591-metens-kali-1)~  
$ t
```

# Task 10: sshd

```
metens@cs591-metens-kali-1: ~
File Actions Edit View Help
      daemon. This allows easy monitoring of sshd.

-d      Debug mode. The server sends verbose debug output to standard error, and
       does not put itself in the background. The server also will not fork(2)
       and will only process one connection. This option is only intended for
       debugging for the server. Multiple -d options increase the debugging
       level. Maximum is 3.

-E log_file
      Append debug logs to log_file instead of the system log.

-e      Write debug logs to standard error instead of the system log.

-f config_file
      Specifies the name of the configuration file. The default is
      /etc/ssh/sshd_config. sshd refuses to start if there is no configuration
      file.

-g      Parse and print configuration file. Check the validity of the configura-
      tion file, output the effective configuration to stdout and then exit.
      Optionally, Match rules may be applied by specifying the connection para-
      meters using one or more -C options.
```

```
metens@cs591-metens-kali-1: ~
File Actions Edit View Help
      daemon. This allows easy monitoring of sshd.

-d      Debug mode. The server sends verbose debug output to standar
       d error, and
       does not put itself in the background. The server also will
       not fork(2)
       and will only process one connection. This option is only i
       ntended for
       debugging for the server. Multiple -d options increase t
       he debugging
       level. Maximum is 3.

-E log_file
      Append debug logs to log_file instead of the system log.

-e      Write debug logs to standard error instead of the system log.

-f config_file
      Specifies the name of the configuration file. The
      default is
      /etc/ssh/sshd_config. sshd refuses to start if there is no c
      onfiguration
      file.

-g      Parse and print configuration file. Check the validity of th
      e configura
      tion file, output the effective configuration to stdout an
      then exit.
      Optionally, Match rules may be applied by specifying the conn
      ection para
      meters using one or more -C options.

-g login_grace_time
      Gives the grace time for clients to authenticate themselves (
      default 120
      seconds). If the client fails to authenticate the user with
      in this many
      seconds, the server disconnects and exits. A value of zero i
      ndicates no
      limit.

-h host_key_file
      Manual page sshd(8) line 51 (press h for help or q to quit)[]
```

```
metens@cs591-metens-kali-1: ~
File Actions Edit View Help
      51 # HostbasedAuthentication
      52 #IgnoreUserKnownHosts no
      53 # Don't read the user's ~/.rhosts and ~/.shosts files
      54 #IgnoreRhosts yes
      55
      56 # To disable tunneled clear text passwords, change to "no" here!
      57 #PasswordAuthentication yes
      58 #PermitEmptyPasswords no
      59 New chat
```

The name of the option that allows one to log in as root is on line 33 of the `sshd_config` file. It is called “`PermitRootLogin`”. The value can be changed to “`yes`”. Similarly, the name of the option that permits authentication via password is on line 57 and is called “`PasswordAuthentication`”; it is set to “`yes`”.

## Task 11: TryHackMe Linux process analysis

One of the cool things I did in this task was to list the ``pspy64`` command, and every 15 seconds, the system outputted this:

```
e/abzk083o4jakxld.sh
2025/07/06 03:00:01 CMD: UID=0      PID=1507    | /bin/bash /etc
urly/beacon
2025/07/06 03:00:01 CMD: UID=0      PID=1508    | /bin/bash /var
kup
2025/07/06 03:00:01 CMD: UID=0      PID=1509    | tail -n 1 /var
n.log
2025/07/06 03:00:01 CMD: UID=0      PID=1510    | tar -czf web_b
r.gz /var/www/html
2025/07/06 03:00:01 CMD: UID=0      PID=1511    | /bin/sh -c gzi
2025/07/06 03:00:01 CMD: UID=0      PID=1513    | /etc/badr/badr
g /etc/badr/rules.yaml --config /etc/badr/room.config.yaml > /
badr.log 2>&1
2025/07/06 03:00:01 CMD: UID=0      PID=1514    | /etc/badr/badr
g /etc/badr/rules.yaml --config /etc/badr/room.config.yaml > /
badr.log 2>&1
2025/07/06 03:00:01 CMD: UID=0      PID=1515    | /etc/badr/badr
g /etc/badr/rules.yaml --config /etc/badr/room.config.yaml > /
badr.log 2>&1
Metens
2025/07/06 03:00:14 CMD: UID=0      PID=1516    |
2025/07/06 03:00:14 CMD: UID=0      PID=1517    | /bin/sh -c /bi
e 'VEhNezg1MWE50DE0NDVkyMzi0TQ4NWmZnzcXNTEwYTUzNTY4fQ=='
2025/07/06 03:00:14 CMD: UID=0      PID=1518    | /bin/echo -e V
WE50DE0NDVkyMzi0TQ4NWmZnzcXNTEwYTUzNTY4fQ==
2025/07/06 03:00:14 CMD: UID=0      PID=1519    | sleep 15
2025/07/06 03:00:29 CMD: UID=0      PID=1520    |
2025/07/06 03:00:29 CMD: UID=0      PID=1521    |
2025/07/06 03:00:29 CMD: UID=0      PID=1522    | ???
2025/07/06 03:00:29 CMD: UID=0      PID=1523    | sleep 15
2025/07/06 03:00:44 CMD: UID=0      PID=1524    | /bin/bash /va
4.sh
2025/07/06 03:00:44 CMD: UID=0      PID=1525    | /bin/bash /var
.sh
2025/07/06 03:00:44 CMD: UID=0      PID=1526    | /bin/echo -e V
WE50DE0NDVkyMzi0TQ4NWmZnzcXNTEwYTUzNTY4fQ==
2025/07/06 03:00:44 CMD: UID=0      PID=1527    |
```

This was an encoded message. To decode the flag, I ran this in my terminal:

```
(base) nathanmetens@Nathans-MacBook-Air ~ % echo VEhNezg1MWE50DE0NDVkyMzi0TQ4NWmZnzcXNTEwYTUzNTY4fQ== | base64 -d
THM{851a981445dbfb9485c3771510a53568}%
(base) nathanmetens@Nathans-MacBook-Air ~ %
```

The rest of this TryHackMe room took me three days to complete. I got stuck on a task for so long, and since I'm such a slow reader, it took me a total of about 7 hours to complete.



Congratulations on completing Linux Process Analysis!!! 🎉

Points earned

96

Completed tasks

8

Room type

Walkthrough

Difficulty

Easy

Streak

3



This room counted toward joining the league! 🏆



metens [0x2][APPRENTICE] 🇺🇸

Rank

1006473

Badges

1

Streak

3

Completed rooms

5

Completed rooms

Certificates

Skills matrix

Badges

Created rooms

Yearly activity

Tickets



Offensive Security Intro

Hack your first website (legally in a safe environment) and experience an ethical hacker's job.

Easy

Free Walkthrough



OpenVPN

A guide to connecting to our network using OpenVPN.

Easy

Free Walkthrough



Linux Fundamentals Part 1

Embark on the journey of learning the fundamentals of Linux. Learn to run some of the first essential commands on an interactive terminal.

Info

Free Walkthrough



Linux File System Analysis

Perform real-time file system analysis on a Linux system to identify an attacker's artefacts.

Easy

Free Walkthrough



Linux Process Analysis

Perform thorough process and application analysis to identify an attacker's persistence methods.

Easy

Free Walkthrough