warmup:

What is the CVE for the exploit allowing unauthorized people to claim root access even when explicitly forbidden?

CYBER
TROY HIGH
Est 2010
DEFENSE

practice round recap

- how was it?
- did you guys have fun?
- was there anything you guys felt we didn’t cover?
- any other comments?

http://bit.ly/linuxbasicblank

Services/Processes/Perms

Processes vs Services?

Processes

- Either background or foreground
- Usually an instance of an executable such as a command or script
- Has a PID (proc ID)

Services

- Background
- Consists of 1+ process
- Generally treating the system as a server for users to be “served” some kind of functionality
- i.e. ssh, ftp, apache

You might come across things known as daemons. They are essentially background tasks with no association with terminal sessions (entirely system run).

Services stuff

Services

You already have seen one, openssh is a service

There are others like FTP servers for file transfer, Apache for websites, and many more

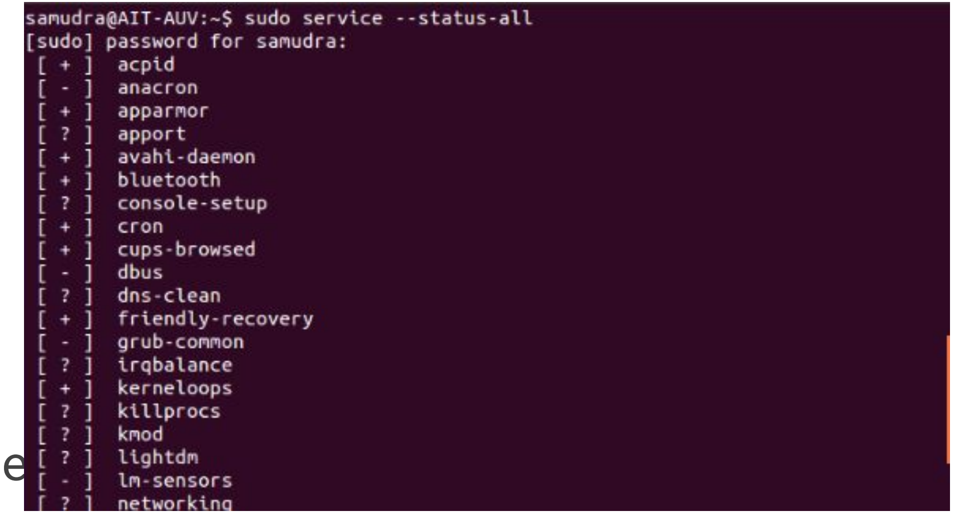
To check what you have live, use:

```
    service --status-all
```

service --status-all

- [+] means active
- [-] means off
- [?] means the service is masked

Basically, some services have code in them that tell the “service” command its status. If the service doesn’t have it, though, it becomes [?].



```
samudra@AIT-AUV:~$ sudo service --status-all
[sudo] password for samudra:
 [ + ]  acpid
 [ - ]  anacron
 [ + ]  apparmor
 [ ? ]  apport
 [ + ]  avahi-daemon
 [ + ]  bluetooth
 [ ? ]  console-setup
 [ + ]  cron
 [ + ]  cups-browsed
 [ - ]  dbus
 [ ? ]  dns-clean
 [ + ]  friendly-recovery
 [ - ]  grub-common
 [ ? ]  irqbalance
 [ + ]  kerneloops
 [ ? ]  killprocs
 [ ? ]  kmod
 [ ? ]  lightdm
 [ - ]  lm-sensors
 [ ? ]  networking
```

Service commands

Some more service commands for specific services to note:

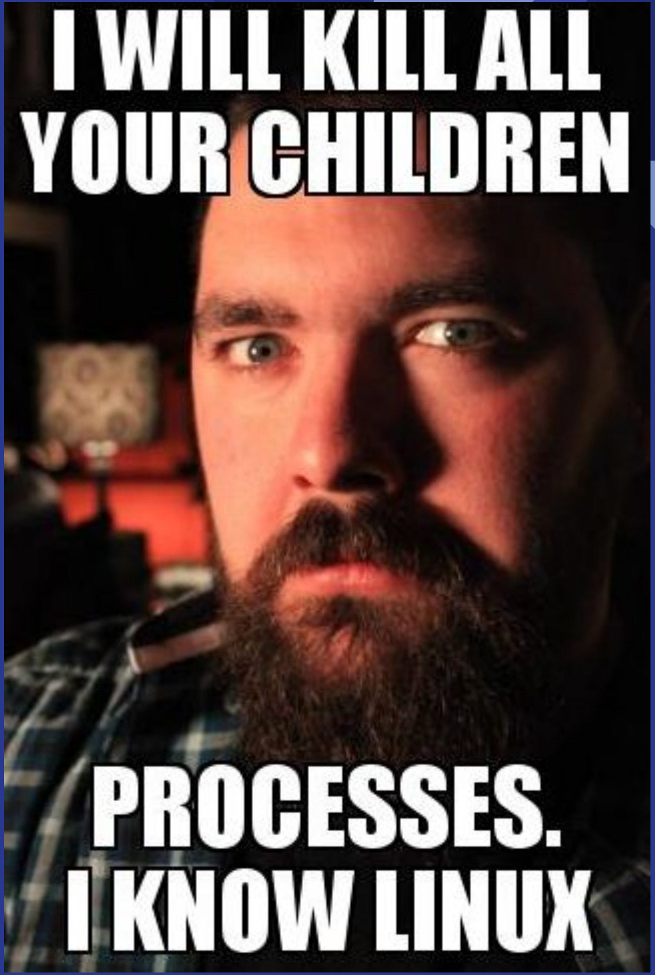
```
service <service name> restart

service <service name> stop

service <service name> status
```

Similar to package hunting

tldr; check services for bad/extra stuff

You should be looking for services of things that are either malware potentially, or just stuff you don't need. For example, if README says you are an OpenSSH server, then you that means you won't need any other kind of remote desktop services running. Additionally, you might find the service for a package you want to delete. Just don't delete critical services

Process stuff



How see processes

To see what processes are currently running:

```
    ps -aux | less
```

To see if a particular process is running:

```
    ps -aux | grep <proc name>
```

NOTE: grepping the output of the “ps -aux” command will always return at least 1 process. Can anyone guess why?

How to kill children but people are cool with it

If you find a process that you want to then use:

```
    kill -9 <PID>
```

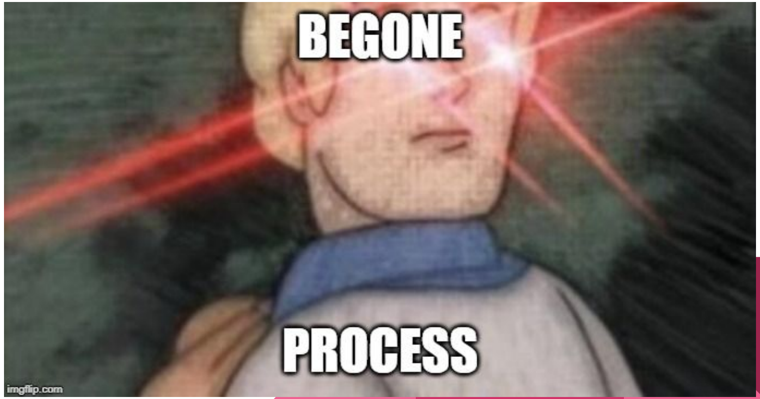
or:

```
    killall <exact proc name>
```

or:

```
    pkill <partial proc name>
```

I recommend using kill -9



Why do processes?

tldr; in cyberpatriot, processes may give you hints to other points. In real life, it might reveal hacker/malware stuff

In cyberpatriot, processes are not usually worth points itself, but can sometimes lead you to discovering things about what’s going on your system! For example you might find secret background malware running or something like that.

In real life, finding what’s running on your computer is really important so you know if there is background stuff like hackers on your computer or things running!

Permissions

There are 3 kinds of permissions

Permissions set is the group of permissions for a type category of users.

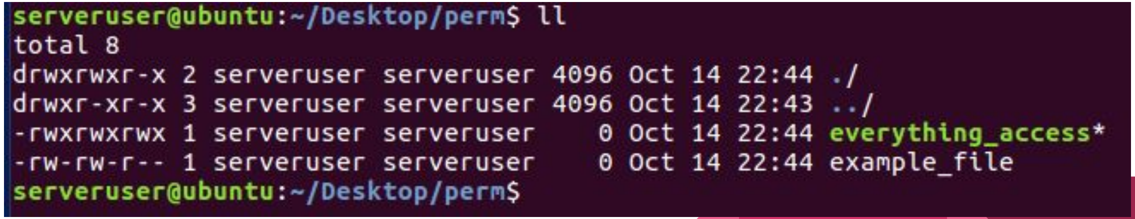
These permissions are in 3 groups:
> Owner, Owner Group, Everyone else

Permissions set: rwx

r: read access

w: write access

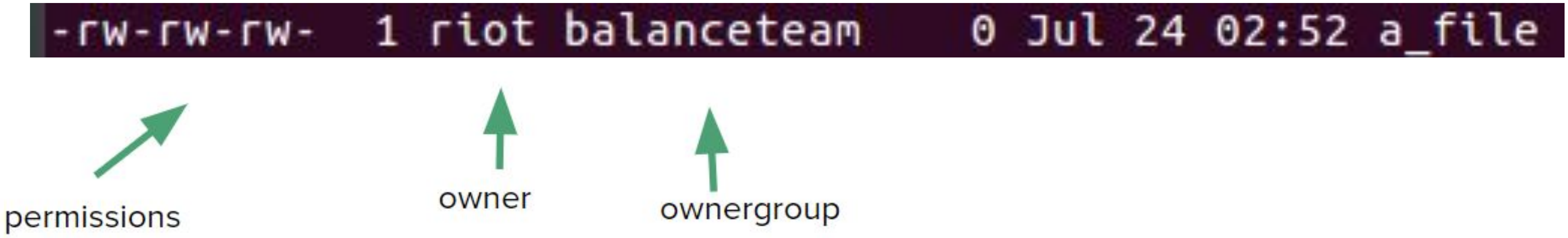
x: execute access



```
serveruser@ubuntu:~/Desktop/perm$ ll
total 8
drwxrwxr-x 2 serveruser serveruser 4096 Oct 14 22:44 ./
drwxr-xr-x 3 serveruser serveruser 4096 Oct 14 22:43 ../
-rwxrwxrwx 1 serveruser serveruser    0 Oct 14 22:44 everything_access*
-rw-rw-r-- 1 serveruser serveruser    0 Oct 14 22:44 example_file
serveruser@ubuntu:~/Desktop/perm$
```

Who’s who

- By default, the creator of a file/directory is the owner of it. The file/directory also belongs to that user’s usergroup.
- Permissions, owner, and ownergroup can all be edited



```
-rw-rw-rw-  1 riot balanceteam    0 Jul 24 02:52 a_file
```

Simple way to change permissions

```
sudo chmod [permission_set] <filename>

sudo chown <new_owner> <filename>

sudo chgrp <new_group> <filename>

To set permission set:

u,g,o +/-/= rwx

Ex: sudo chmod o-wx a_file

Ex: sudo chmod u+rwx,o=r a_file
```

Talking about ways to edit permissions be like

It is harder and memorization,
but faster.
Do you want to know? we can skip if you don’t want to know it (it’s just for speedy peeps)

Understanding it in binary

how to count in binary:

binary has 2 digits: 1 & 0 (true or false)

$000_2=0_{10}$

$001_2=1_{10}$

$010_2=2_{10}$

$011_2=3_{10}$

$100_2=4$, etc…

how to convert binary to decimal:

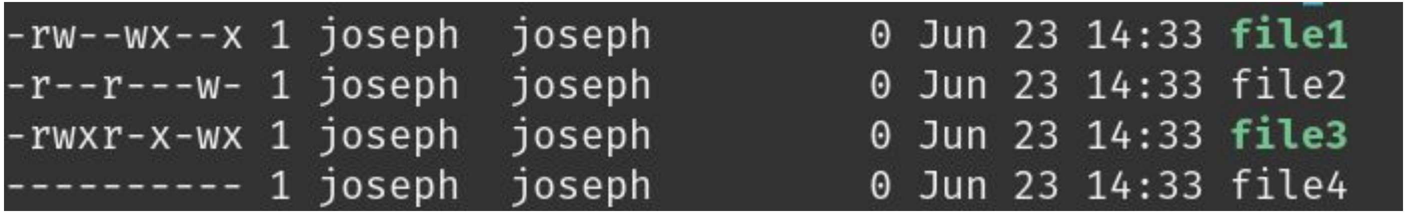
- start at the rightmost digit
- that digit is x^0
- the next digit is x^1
- then x^2,... and so on
- x is how many 2’s there are (either 0 or 1)
- add them up so: 101_2=
- $2^2+0^1+2^0=4+0+1=5_{10}$

Changing permissions

So basically Linux can represent a permission set (rwx) as either yes-or-no (true or false) so 0 or 1. So if a file had rwxrwxrwx it would be like 111111111. But remember! A permission set is just a group 3 at a time so it's more like 111 111 111. Based on the last slide, we can therefore turn it into $111_2=7_{10}$. So if we wanted to set rwxrwxrwx to a file we can use the command:

```
    chmod 777 <file name>
```

Instead of chmod =rwxrwxrwx <file name>



```
-rw--wx--x 1 joseph  joseph          0 Jun 23 14:33 file1
-r--r---w- 1 joseph  joseph          0 Jun 23 14:33 file2
-rwxr-x-wx 1 joseph  joseph          0 Jun 23 14:33 file3
---------- 1 joseph  joseph          0 Jun 23 14:33 file4
```

What are the numerical values of these files?
(DON’T SHOUT THEM OUT, WAIT TO BE CALLED)

http://bit.ly/linuxfeedbackform

reminder: if you’ve got any feedback or questions!!!

Kahoot:

https://play.kahoot.it/v2/?quizId=50d8e9d0-739d-415a-b9a8-ef88a0a6e4f1