Week 2:
Securing Linux & Common Services

Sign-in

https://jessh.zip/ccdcfallweek2

whoami

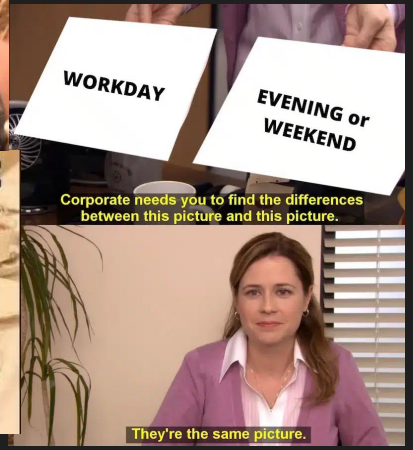
Sara Downing | @ihasbunnyboo

2nd year Computer Science major

CCDC Alternate Member 2024-2025

whoami

- **Medha Swarnachandrabalaji @medl100**
- **3rd year CS Major and Cyber Minor**
- **CCDC**
  - Alternate Member 2024-2025
  - Member 2025-2026
- **SWIFT Alumni Relations Coordinator**
- yapper



Weekly Schedule

Date	CCDC (1PM-4PM)
Aug 30	~~Intro, Business, and Networking~~
Sep 6	**Common Services and Securing Linux**
Sep 13	Securing Windows and Review/Tryouts AMA
Sep 20-21	CCDC Tryouts (1-5 PM)

Agenda

1 Linux

Navigating linux, intro to linux security and networking, and more

2 Services

Identify and explain common services found in CCDC

Securing Linux

01 Linux Basics

02 Linux Administration

03 Linux Security and Networking

04 Firewall

01

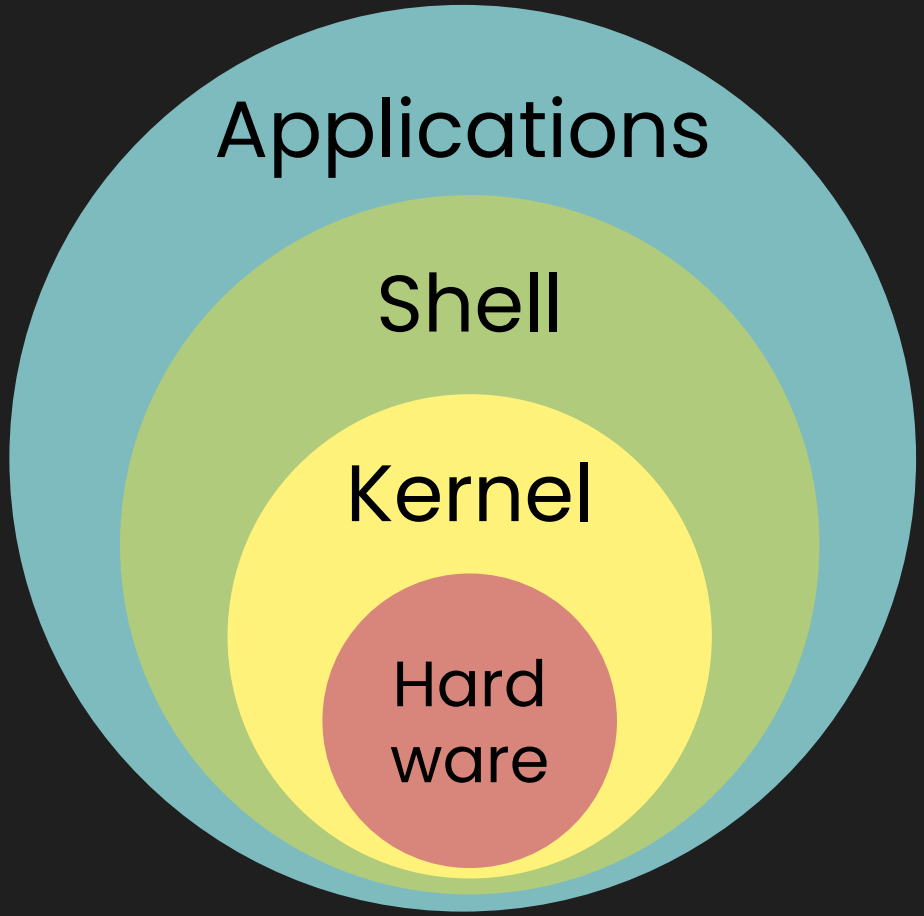
Linux Basics

What is Linux

- **Not** an operating system
  - Distributions or flavors of Linux
- Free & open-source **kernel**
- Built on **Unix** (unix-like)

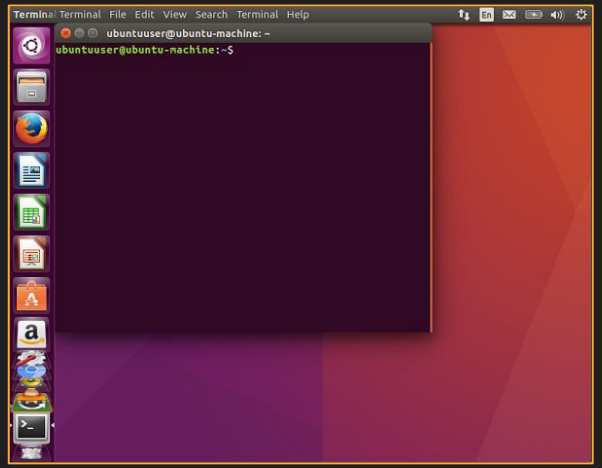





Applications
Shell
Kernel
Hard
ware

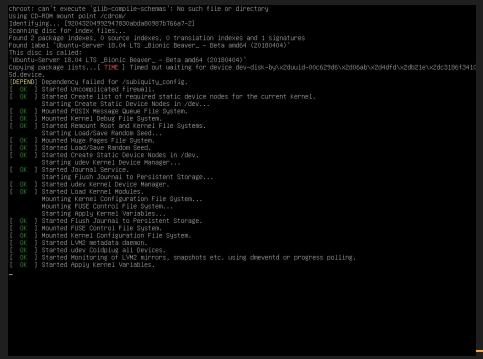
Terminals

Terminal Emulator

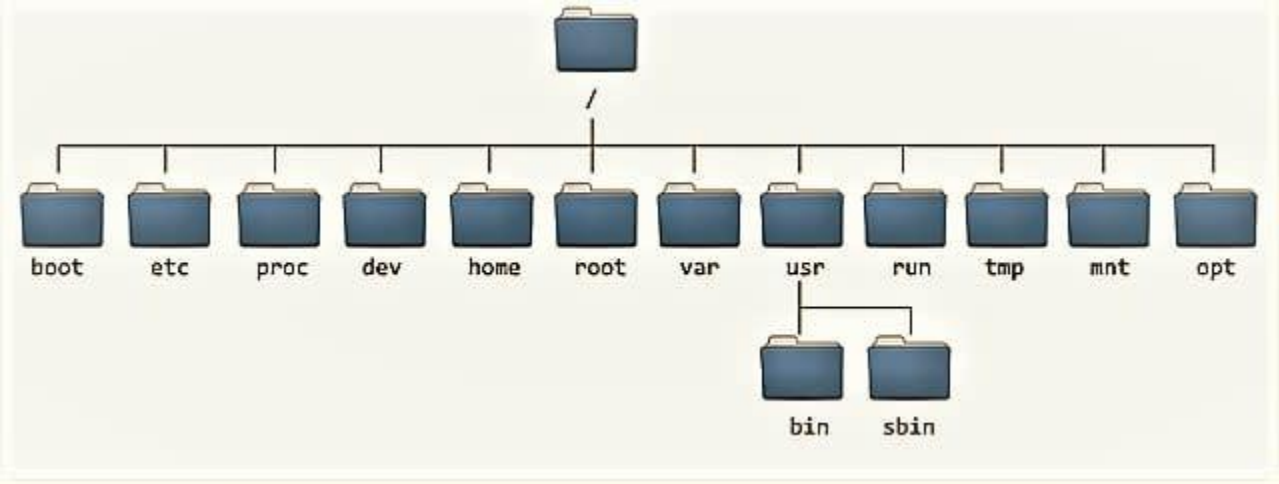


"Desktop" Version

"Server" Version



File Tree - Contents of /



Paths and Directories

Absolute Path

Starts with /

Relative Path

Starts with pwd (print working directory)

Current Directory

Use .

Previous Directory

Use ..

Examples

cd /home/user/Desktop/	cd ..
cd /var/www/html/	./script.sh
/etc/ssh/sshd_config	var/www/html/

root vs /root vs /

- root user (uid 0) = admin
- root (/) directory = start of file system
- root's home = /root

Shell and Syntax

command -options arguments

- EXAMPLE: ls
- EXAMPLE: cd /home/user1
- EXAMPLE: ls -la user1/Downloads
- EXAMPLE: ls -R

Viewing Files

ls (list) → **ls [flags] [filepath]**

Flags:

-l (more detailed view)

-a (show all files and directories)

```
jamie@debian:~$ ls -l
total 19208
-rwxr-xr-x 1 root  root   4703728 Dec 17 07:01 Battle.net-Setup.exe
drwxr-xr-x 3 jamie jamie     4096 Nov  5 03:30 Desktop
drwxr-xr-x 2 jamie jamie     4096 Jun  5  2018 Documents
drwxr-xr-x 3 jamie jamie     4096 Dec 17 06:49 Downloads
-rw-r--r-- 1 jamie jamie   179765 Dec 17 07:01 Linux_for_beginners.pdf
-rw-r--r-- 1 jamie jamie   458980 Dec 17 06:59 metamorphose2_0.8.2-1_all.deb
drwxr-xr-x 2 jamie jamie     4096 Apr 30  2018 Music
-rw-r--r-- 1 jamie jamie     1520 Dec 17 07:01 Neofetch
-rw-r--r-- 1 root  root  13902480 Dec 17 07:01 pdfsam_3.3.6-1_all.deb
-rw------- 1 root  root    375728 Dec 17 07:01 PDFsam_merge.pdf
drwxr-xr-x 2 jamie jamie     4096 Apr 30  2018 Pictures
drwxr-xr-x 2 jamie jamie     4096 Apr 30  2018 Public
drwxr-xr-x 2 jamie jamie     4096 Apr 30  2018 Templates
drwxr-xr-x 2 jamie jamie     4096 Apr 30  2018 Videos
```

Creating Files

touch → **touch [flags] [filename/filepath]**

[favorite text editor] [filename]

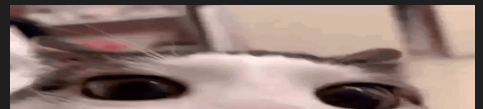
...many more for later...

Commands You Would Find with a Right-Click

cp (copy) - **cp [source] [destination]**

mv (move) - **mv [source] [destination]**

cat (concatenate) - **cat [filename]**



rm (remove) - **rm [flags] [filepath/filename]**

Flags :
-f or --force, do not prompt, only remove
-r or --recursive, remove content and subdirectories

mkdir (make directory) - **mkdir [flags] [path/directory_name]**

Flags:
-p or --parent

02

Linux Administration

$PATH

$PATH

The directory search order for commands you call

```
echo $PATH
```

/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin

Aliases

```
ccdc@ubuntu22:~$ alias
alias alert='notify-send --urgency=low -i "$([ $? = 0 ] && e
cho terminal || echo error)" "$(history|tail -n1|sed -e '\''
s/^\s*[0-9]\+\s*//;s/[;&|]\s*alert$//'\'')"'
alias ccdc='echo ceeceeDc'
alias egrep='egrep --color=auto'
alias fgrep='fgrep --color=auto'
alias grep='grep --color=auto'
alias l='ls -CF'
alias la='ls -A'
alias ll='ls -alF'
alias ls='ls --color=auto'
ccdc@ubuntu22:~$ alias ccdc='echo ceeceeDc'
ccdc@ubuntu22:~$ ccdc
ceeceeDc
ccdc@ubuntu22:~$
```

Strings n' Stuff

NANO

- **nano** <filename>
- installed by default mostly
- very basic
- CTRL+X to exit "Y" to save as same name


```
  GNU nano 2.0.9            File: txt_files/testfile                    Modified

Learn how to use nano to boost your terminal confidence!
Edit config files like a pro!
Make easy to-do lists and notes in a text-only format!
Do it via SSH from a smartphone or other computer!

# /etc/fstab: static file system information.
#
# Use 'blkid -o value -s UUID' to print the universally unique identifier
# for a device; this may be used with UUID= as a more robust way to name
# devices that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
proc            /proc           proc    defaults        0       0
# / was on /dev/sdb1 during installation
                                [ Read 17 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

VIM

- **vim** <filename>
- sometimes not installed by default
- extremely customizable
- :wq to close and save file
- 5 modes
- can run commands in the editor
- vimtutor to get started

```
#include <stdio.h>
void bubble(int arr[], int size) {
    int temp=0;
    for (int i = 0; i < size; i++) {
        for (int j = 0; j < size - i - 1; j++) { // elements excluding the sorted ones
            if (arr[j] > arr[j + 1]) {
                temp = arr[j];
                arr[j] = arr[j + 1];
                arr[j + 1] = temp;
            }
        }
    }
}
int main() {
  int arr[100], size;

  printf("Enter the count of elements of the array:\n");
  scanf("%d", &size);

blue  darkblue  default  delek  desert  elflord  evening  industry  koehler  morning  murphy  pablo  >
:colorscheme desert
```

SED (streeeeeeeeeeems)

- **sed** <script> <filename>
- sed -i 's/pattern/replace/g' file.txt
- Good for scripting out file changes
- Can use Regex for pattern matches

```
[Jul 14, 2024 - 19:24:46 (PDT)] exegol-attack bootcamps # cat file
the quick brown fox jumps over the lazy dog
[Jul 14, 2024 - 19:24:47 (PDT)] exegol-attack bootcamps # sed -i 's/fox/dog/' file; cat file
the quick brown dog jumps over the lazy dog
[Jul 14, 2024 - 19:24:50 (PDT)] exegol-attack bootcamps # sed -i 's/dog/wolf/' file; cat file
the quick brown wolf jumps over the lazy dog
[Jul 14, 2024 - 19:25:04 (PDT)] exegol-attack bootcamps # sed -i 's/the/a/g' file; cat file
a quick brown wolf jumps over a lazy dog
```

Moving Strings Around

- **STDIN (Standard Input Stream)** - takes strings as input
  - **"<" –** Redirects STDIN

```
user@                    :~$ cat < example1.txt
Goodluck at tryouts!
user@                    :~$
```

- **Pipes** - output of one command used for another.
  - **" | "** → not an L

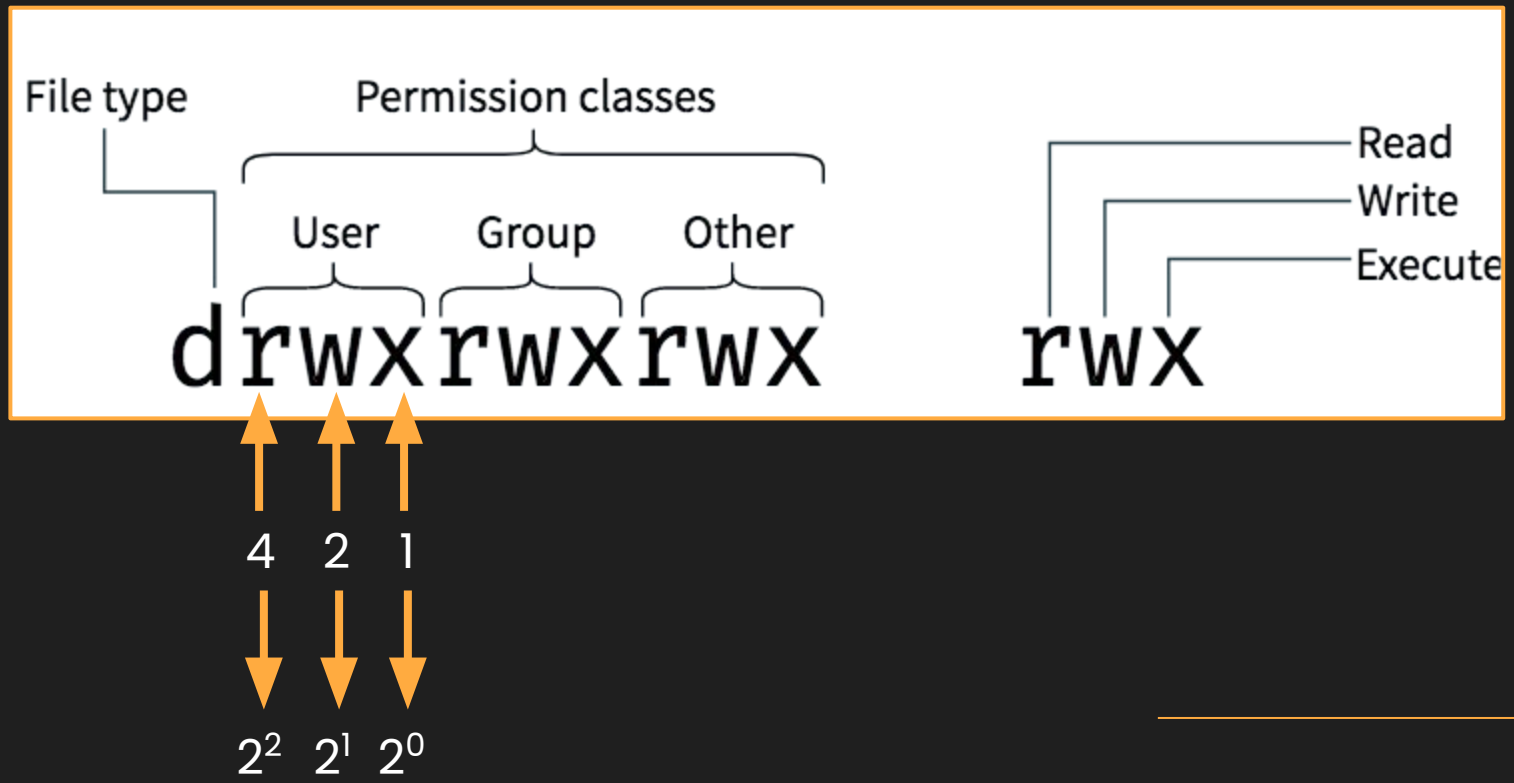
```
user@                    :~$ cat favoriteThings.txt | sort
Buttered Chicken
Cheeseburger
Computers
Food
Food
Iphone
Penguins
```

- **STDOUT (Standard Input Stream)** - output strings from command
  - **">" –** Redirects STDOUT

```
user@                    :~$ echo "Hello from Texas" > example1.txt
user@                    :~$ cat example1.txt
Hello from Texas
user@                    :~$
```

File Permissions

Linux File Permissions



Convert to octal

rwxr-xr-x

Convert to rwx

644

Convert to octal

r-x-w---x

Convert to rwx

777

Changing File Permissions

chmod to change permissions

chown to change file owner
Ex:
chown user1:group1 <file>
chown root:root notes.txt

CHMOD is used to change permissions of a file.

PERMISSION			COMMAND
U	G	W	
rwx	rwx	rwx	chmod 777 filename
rwx	rwx	r-x	chmod 775 filename
rwx	r-x	r-x	chmod 755 filename
rw-	rw-	r--	chmod 664 filename
rw-	r--	r--	chmod 644 filename
User	Group	World	

r = Readable
w = Writable
x = Executable
- = None

```
-bash-5.0$ chmod 777 file1
-bash-5.0$ chmod a+rwx file2
-bash-5.0$ ls -l
total 0
-rwxrwxrwx 1 nigerald nigerald 0 Jul 19 01:45 file1
-rwxrwxrwx 1 nigerald nigerald 0 Jul 19 01:45 file2
-bash-5.0$ chmod 744 file1
-bash-5.0$ chmod go+r file2
-bash-5.0$ ls -l
total 0
-rwxr--r-- 1 nigerald nigerald 0 Jul 19 01:45 file1
-rwxrwxrwx 1 nigerald nigerald 0 Jul 19 01:45 file2
```

Immutability

Make file immutable

chattr +i <file>

Check for immutable bit

lsattr <file>

Remove immutable bit

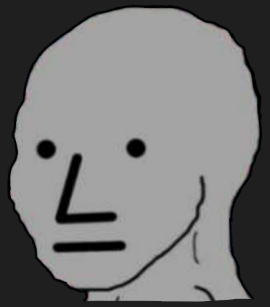
chattr -i <file>

this is an i

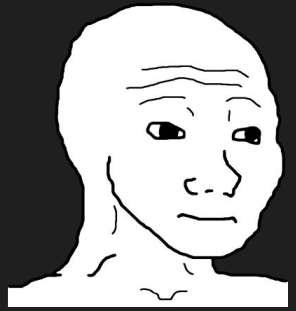
User IDs and Group IDs

root = 0

services < 1000



users > 999



I am ~~g~~root

sudo <command>

✨**sudo <command>**✨

sudo -i

sudo su

su <user>

su root

su -

Adding Users

adduser

wrapper for useradd

less clunky

prompts for password

useradd

much less efficient

doesn't create home directories

manually set password

Managing Users

Group Management

not group policy

groups users together

✨**usermod**✨

✨**id**✨

Password Management

passwd

- passwd (changes for current user)
- passwd user2 (changes for user2)

chpasswd

- Can be used for automation
- echo "user2:password" | chpasswd
- Alternatively use the format above and finish with Ctrl + D

```
root@ubuntu22:/home/ccdc# chpasswd
user2:secure_password
root@ubuntu22:/home/ccdc# passwd user2
New password:
Retype new password:
passwd: password updated successfully
root@ubuntu22:/home/ccdc# echo "user2:cool" | chpasswd
```

Processes

Program running on the computer

ps - List Processes

kill -9 <Process ID (PID)> - Kill process by ID

pgrep - Find PID from process name

Services

Process running in the background managed by the system

systemctl

On most modern distros

Simple

systemctl start sshd

:)

service

Usually works if systemctl doesn't

Simple

service sshd status

:)

rc.d / init.d

Systems without systemd

Pain. Location may vary

/etc/init.d/sshd start

:(

Different Distros

Debian-based

apt update

apt upgrade

apt install

apt purge/remove

RHEL-based

yum update

yum upgrade

yum install

yum remove/erase

Other

suffering

apk

pacman

solaris

Get Some Help

- Man pages
- Find and grep command
- --help parameter
- less or more
- head or tail
- tmux

Tmux Cheatsheet

Prefix: ctrl + b

Windows

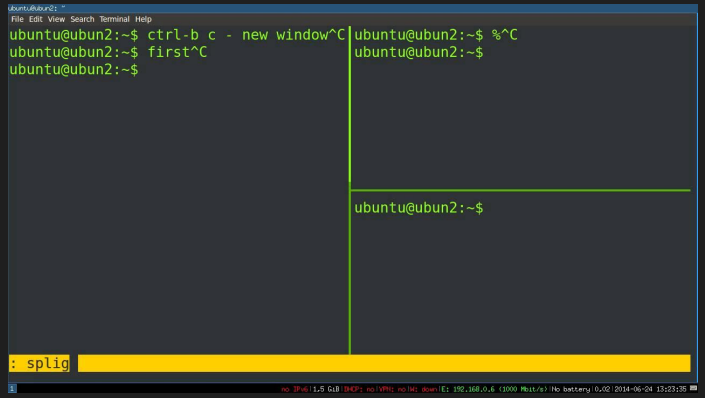
- New Window: **prefix** + c
- Switch between Windows: **prefix** + [number] OR (p)revious OR (n)ext
- Delete Window: **prefix** + &

Panes

- Split Horizontally: **prefix** + "
- Split Vertically: **prefix** + %
- Switch between panes: **prefix** + [arrow key]

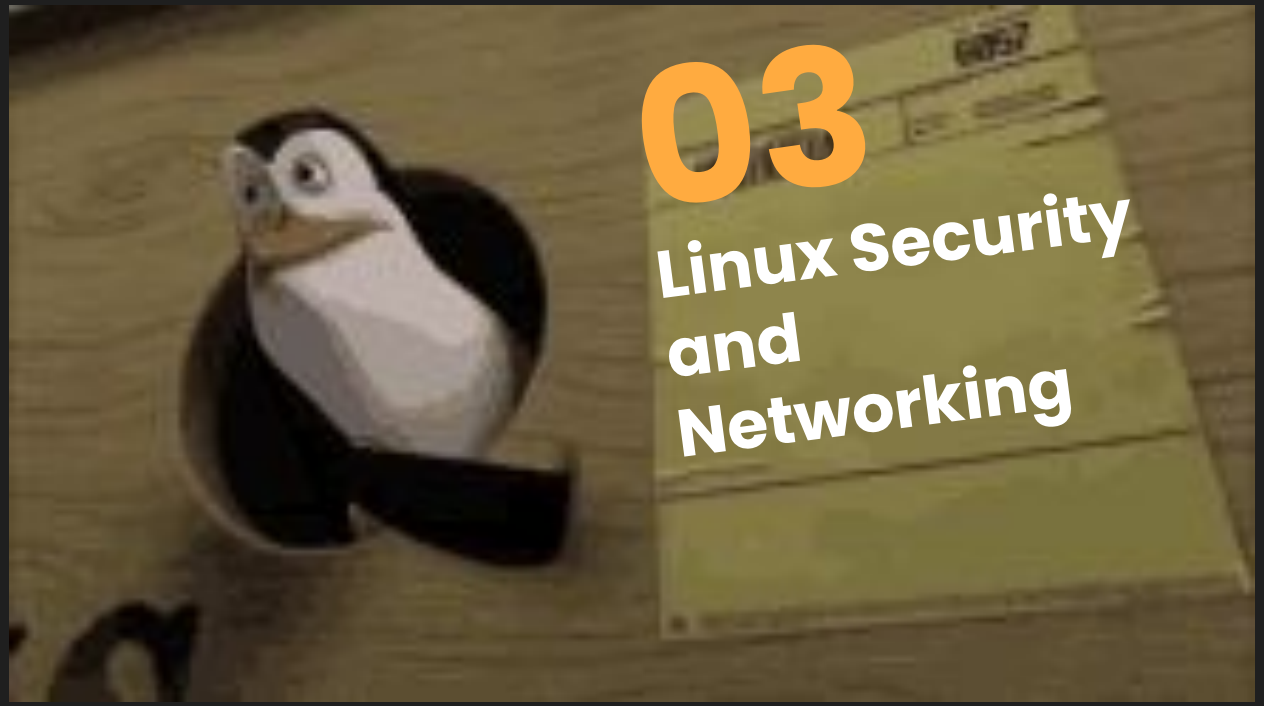
Other

- New Session: tmux
- Detach: **prefix** + d
- Reattach: tmux + a
- Fullscreen: **prefix** + z



Linux Tips & Tricks

- grep – Parse text using regular expressions
- cd - (“tack”) – Go to directory previously in
- cd ~ (tilde) – Go to user’s home directory
- Tab completion – Hit tab to autocomplete command
- Ctrl+L - clear terminal
- Ctrl+Shift+C and Ctrl+Shift+V – copy and paste into terminal (!CAUTION!)
- Ctrl+C – Kill running command
- Ctrl+R – Search command history
- Ctrl+U/Y – Cut everything before the cursor/Paste it back
- Home key/Ctrl+A, End Key/Ctrl+E – Go to beginning of line or end of line
- less – Different way to display contents of a file or command
- && and || – Run commands in sequence
- !! – Run previous command again
- yes – repeat input to answer prompts
- Alt+. – reuse recent arguments



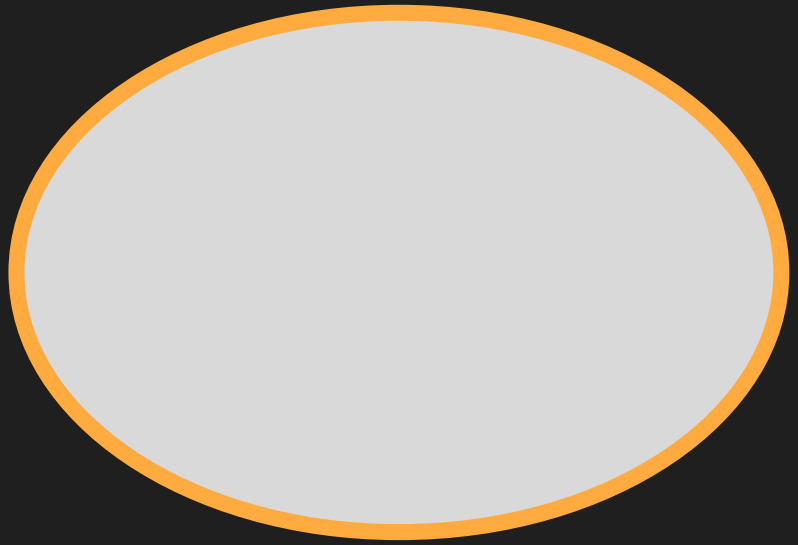
03

Linux Security and Networking

The Holy Square of User Management

/etc/passwd

/etc/group



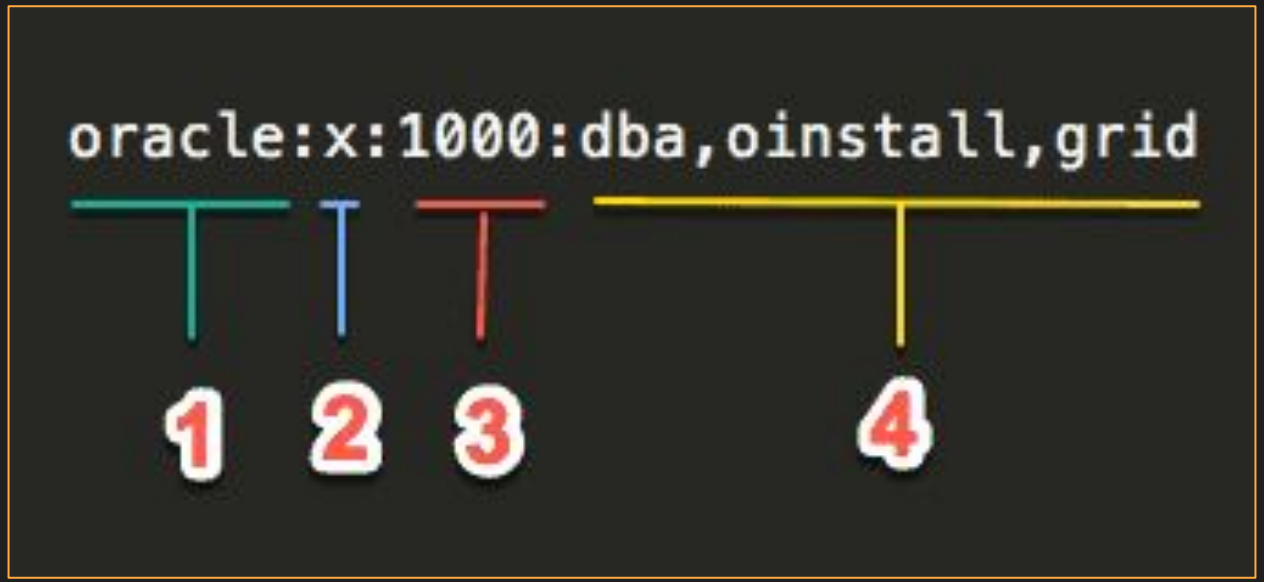
/etc/shadow

/etc/sudoers

/etc/passwd

```
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
```

/etc/group



1: username 2: password 3: GID 4: Members of Group

/etc/shadow

1: username

2: password hash
different algorithms

3: last changed time (epoch)
4: minimum days between password changes
5: maximum days password is valid

/etc/sudoers

```
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

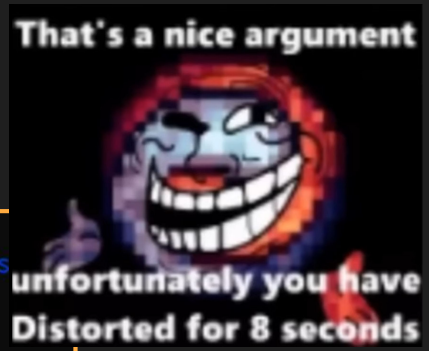
What is PAM?

- pluggable authentication module
- manages authentication
- common-auth (Debian)
  system-auth and password-auth (RHEL)

common-auth

```
#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
auth    [success=1 default=1]           pam_unix.so nullok
# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth    optional                        pam_cap.so
# end of pam-auth-update config
```



Windows PowerShell | root@kali: ~

```
ccdc@ubuntu24:~$
```

```
root@ubuntu24:/home/ccdc# vim /etc/pam.d/common-auth
```

```
[1] 0:ssh*                                                    "kali" 21:42 26-Jul-24
```

Random Linux Networking

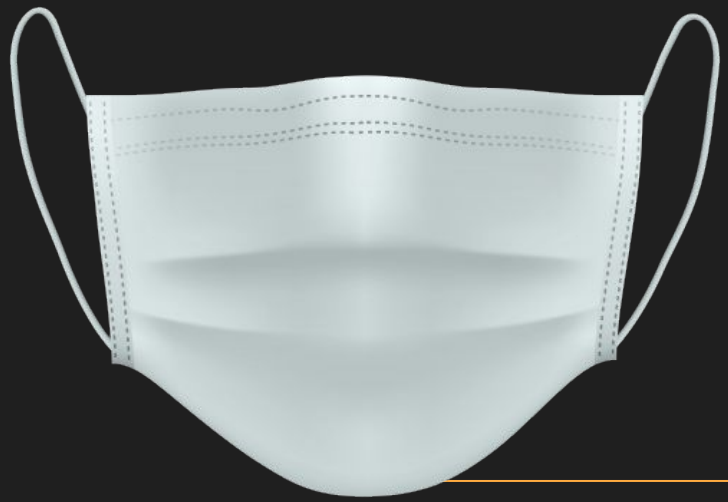
NetworkManager

(And other similar services)

NetworkManager, systemd-networkd

Manages network connections

Make sure it's running



Network Connections

Get your own IP via ip/ipconfig/ifconfig

View via netstat (may need net-tools) or ss

```
root@ubuntu20:/home/ccdc# ss -tulpn
Netid     State      Recv-Q     Send-Q               Local Address:Port           Peer Address:Port     Process
udp       UNCONN     0          0                    127.0.0.53%lo:53                 0.0.0.0:*         users:(("systemd-resolve",pid=766,fd=12))
udp       UNCONN     0          0              192.168.30.132%ens33:68                0.0.0.0:*         users:(("systemd-network",pid=764,fd=19))
tcp       LISTEN     0          4096                 127.0.0.53%lo:53                 0.0.0.0:*         users:(("systemd-resolve",pid=766,fd=13))
tcp       LISTEN     0          128                        0.0.0.0:22                 0.0.0.0:*         users:(("sshd",pid=1699,fd=3))
tcp       LISTEN     0          5                          0.0.0.0:8080               0.0.0.0:*         users:(("python3",pid=2214,fd=3))
tcp       LISTEN     0          128                           [::]:22                    [::]:*         users:(("sshd",pid=1699,fd=4))
tcp       LISTEN     0          511                              *:80                       *:*         users:(("apache2",pid=842,fd=4),("apache2",pid=841,fd=4),("apache2",pid=838,fd=4))
root@ubuntu20:/home/ccdc# netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      766/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1699/sshd: /usr/sbi
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN      2214/python3
tcp6       0      0 :::22                   :::*                    LISTEN      1699/sshd: /usr/sbi
tcp6       0      0 :::80                   :::*                    LISTEN      838/apache2
udp        0      0 127.0.0.53:53           0.0.0.0:*                           766/systemd-resolve
udp        0      0 192.168.30.132:68       0.0.0.0:*                           764/systemd-network
root@ubuntu20:/home/ccdc#
```

NMAP

Quickly identify open ports

```
┌──(root㉿kali)-[~]
└─# [07/25/24 7:37:13] nmap 172.16.127.31
Starting Nmap 7.94 ( https://nmap.org ) at 2024-07-25 19:37 PDT
Nmap scan report for 172.16.127.31
Host is up (0.00029s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:50:56:97:F2:30 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.14 seconds
```

04

Firewalls (but linux)

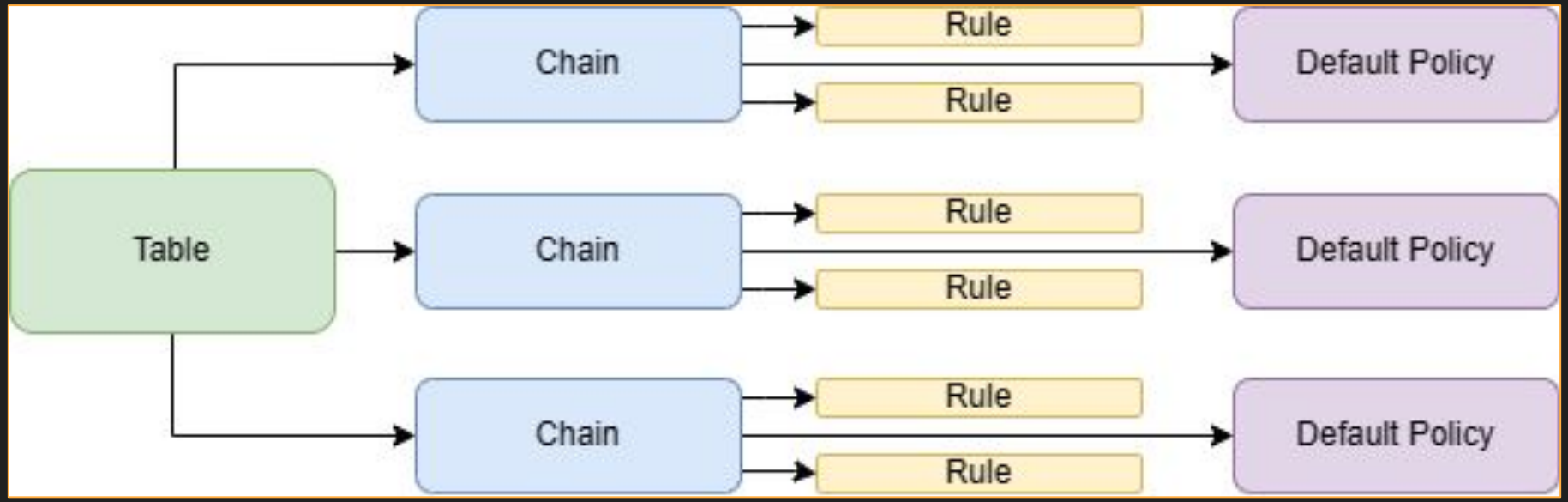
Firewalls

More ports = larger attack surface

Firewalls should operate with the **Implicit Deny** principle

Block by default, allow by exception

IP Tables – Overview



IP Tables - Filter Table

3 Chains:

- INPUT
- OUTPUT
- FORWARD

Default Policy:

```
iptables --policy INPUT DROP
iptables --policy OUTPUT DROP
iptables --policy FORWARD DROP
```

Flush Rules:

```
iptables -F
```

List Rules:

```
iptables -L
```

IP Tables - Filtering Revshell Example

Allow incoming on 80

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Drop incoming packets if they do not match a rule

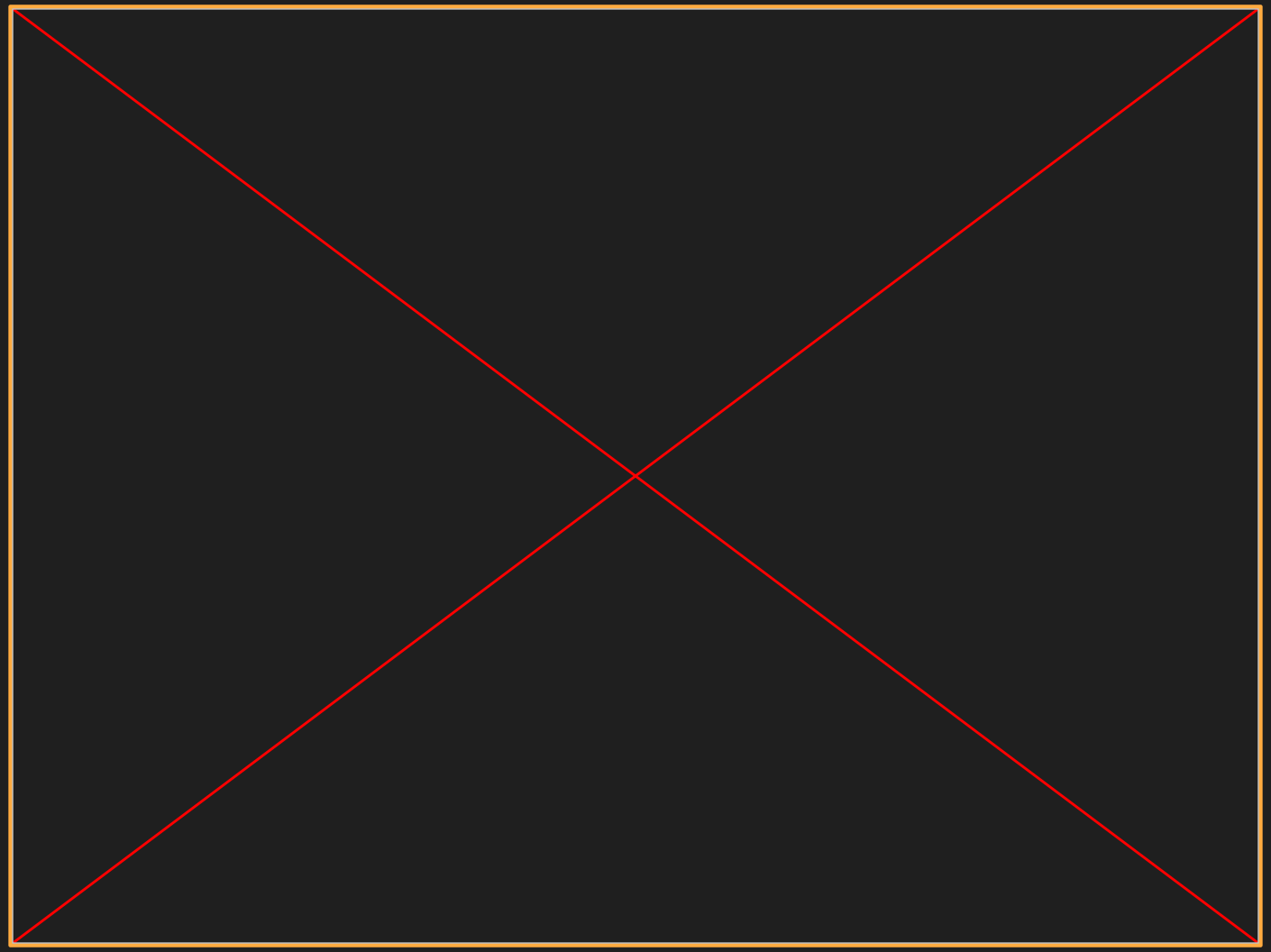
```
iptables -P INPUT DROP
```

Allow outgoing responsive connections

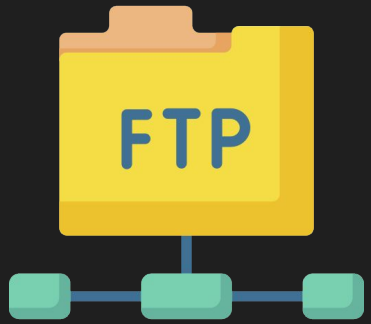
```
iptables -A OUTPUT -p tcp -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

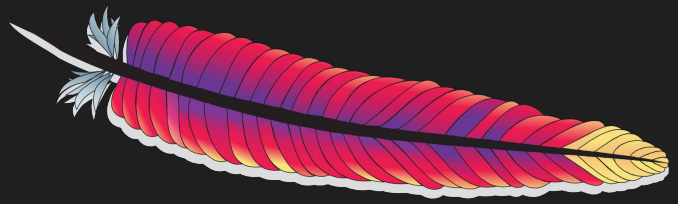
Drop outgoing packets if they do not match a rule

```
iptables -P OUTPUT DROP
```



Common Services





Agenda

1

Services

Thats it lol

Today's Objectives

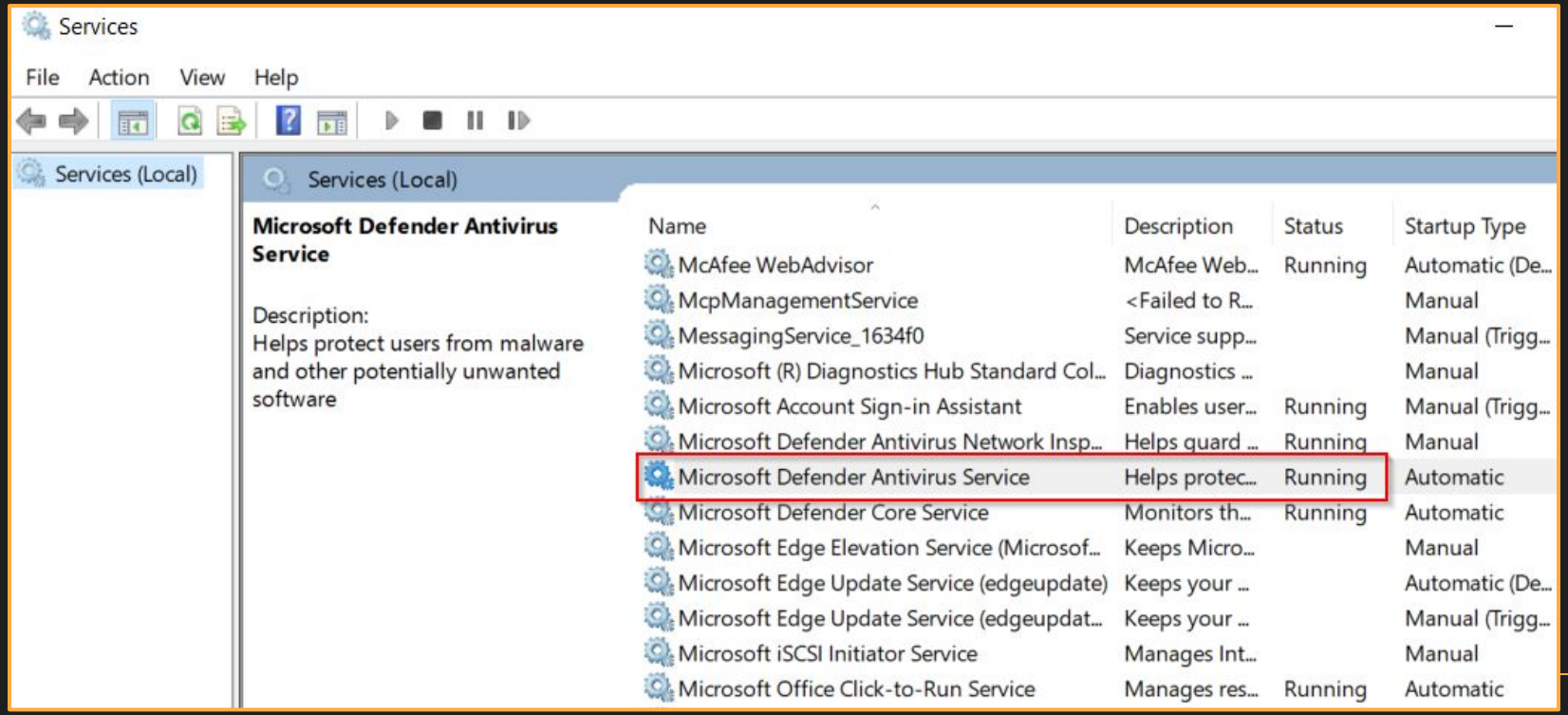
- ❑ Identify what a service is
  - ❑ Identify services present on a system
- ❑ Identify common CCDC services
- ❑ Understand service methodology
  - ❑ Install
  - ❑ Troubleshoot
- ❑ Understand service security
  - ❑ Configurations
  - ❑ Triaging

What is a Service?

1. Background process running on a host - "Host Services"
2. A functionality served by the business - "Business Services"
    - **Purpose**
        - To users -- public facing
            - SLAs
        - To business users -- internal

Not 1:1

Example: Host Service



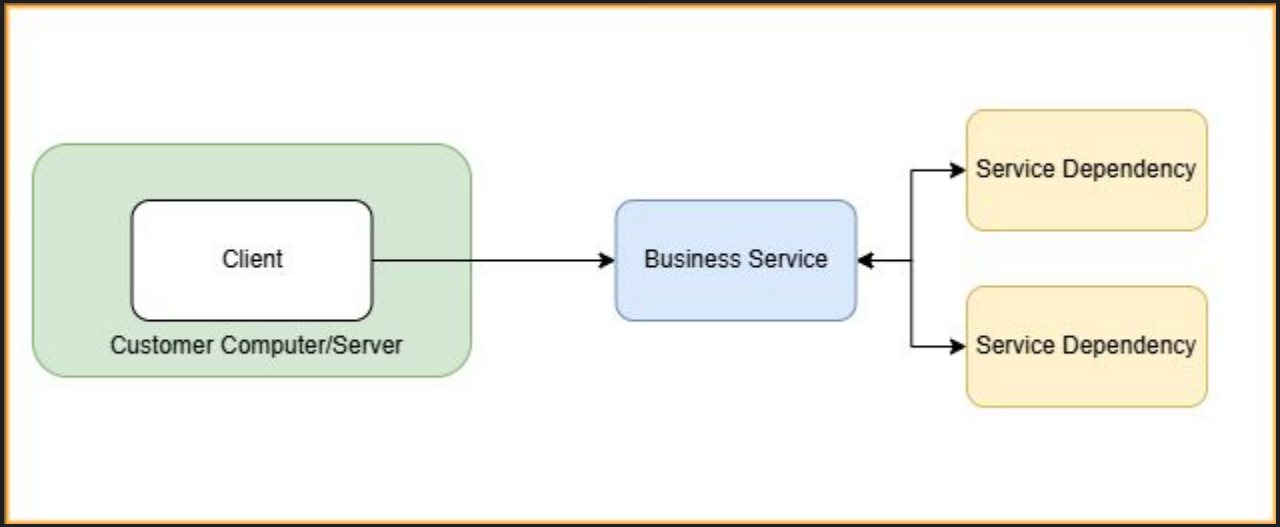
Windows Key + r ⇒ services.msc + enter

Example: Host Service

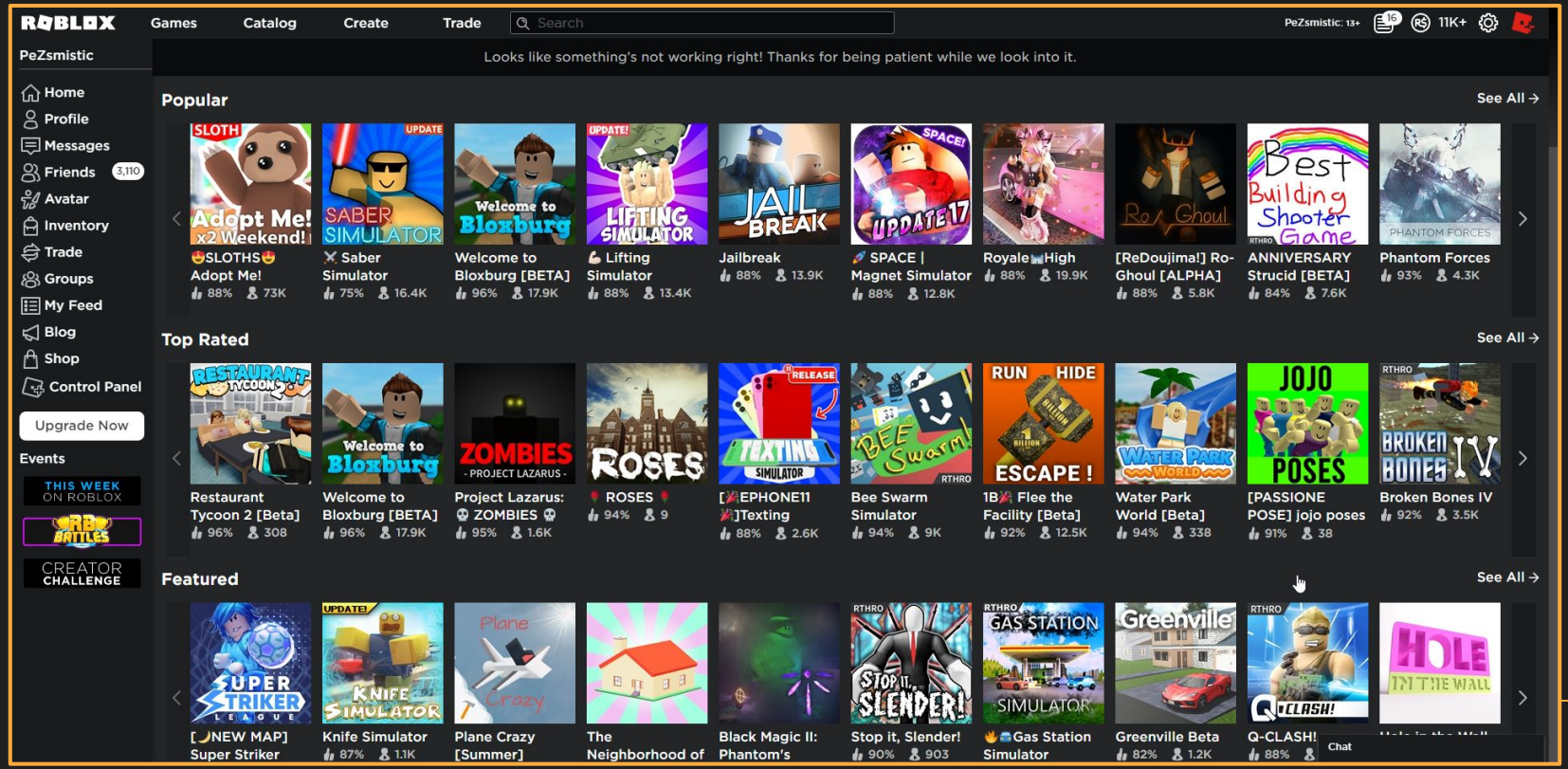
```
┌──(root㉿kali)-[/tmp/arsenal-kit]
└─# [07/4/24 7:22:22] systemctl list-units --type=service | head
  UNIT                                  LOAD   ACTIVE SUB     DESCRIPTION
  binfmt-support.service                loaded active exited  Enable support for additional executable binary formats
  colord.service                        loaded active running Manage, Install and Generate Color Profiles
  console-setup.service                 loaded active exited  Set console font and keymap
  containerd.service                    loaded active running containerd container runtime
  cron.service                          loaded active running Regular background program processing daemon
  dbus.service                          loaded active running D-Bus System Message Bus
  docker.service                        loaded active running Docker Application Container Engine
  getty@tty1.service                    loaded active running Getty on tty1
  haveged.service                       loaded active running Entropy Daemon based on the HAVEGE algorithm

┌──(root㉿kali)-[/tmp/arsenal-kit]
└─# [07/4/24 7:22:24] service --status-all | head
 [ - ]  apache-htcacheclean
 [ - ]  apache2
 [ - ]  apparmor
 [ - ]  atftpd
 [ + ]  binfmt-support
 [ - ]  bluetooth
 [ - ]  cgroupfs-mount
 [ - ]  console-setup.sh
 [ + ]  cron
 [ - ]  cryptdisks
```

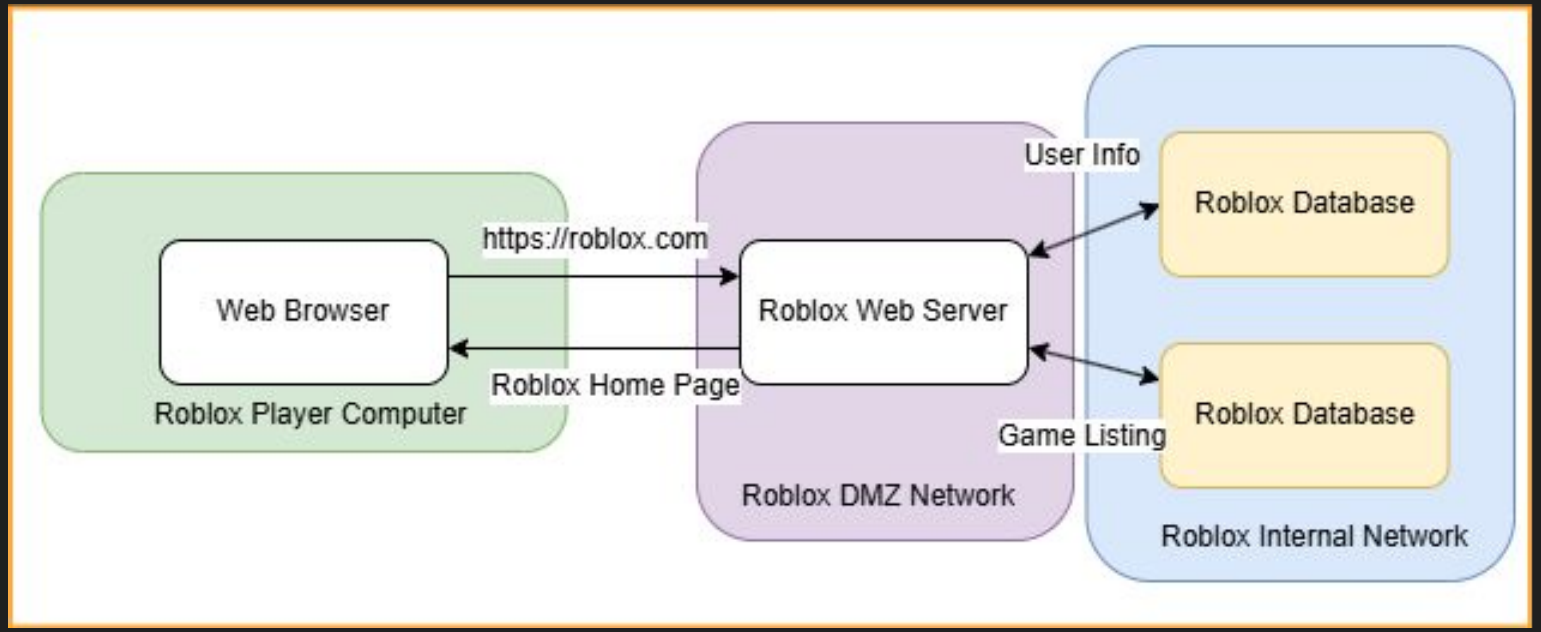
Business Service



Example: Business Service



Business Service



*This is not representative of Roblox's infrastructure at all, just a hypothetical diagram as an example

How can you secure a service?

Threat Modelling

Functionality

- What role does this service play in the business?
- How does this service work from a technical standpoint?
  - Ports?
  - Dependent services?

Identify Attacks

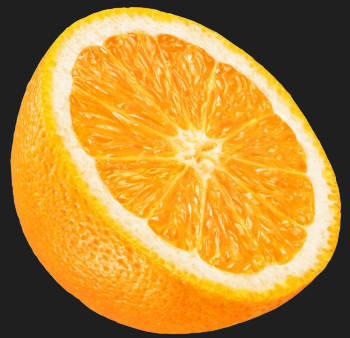
- What would impact the role of this service?
  - DOS?
  - Defacement?
- What impact does exploitation have to us?
  - Command Execution?
  - Information exposure?
- Requirements for the attack?
  - Network access?
  - (Un)authenticated?

Mitigations

- Is there a configuration or patch that affects the attack's requirements?
- How can I cut the attacker's access?
  - Host level?
  - Network level?
- Can I isolate the impact?

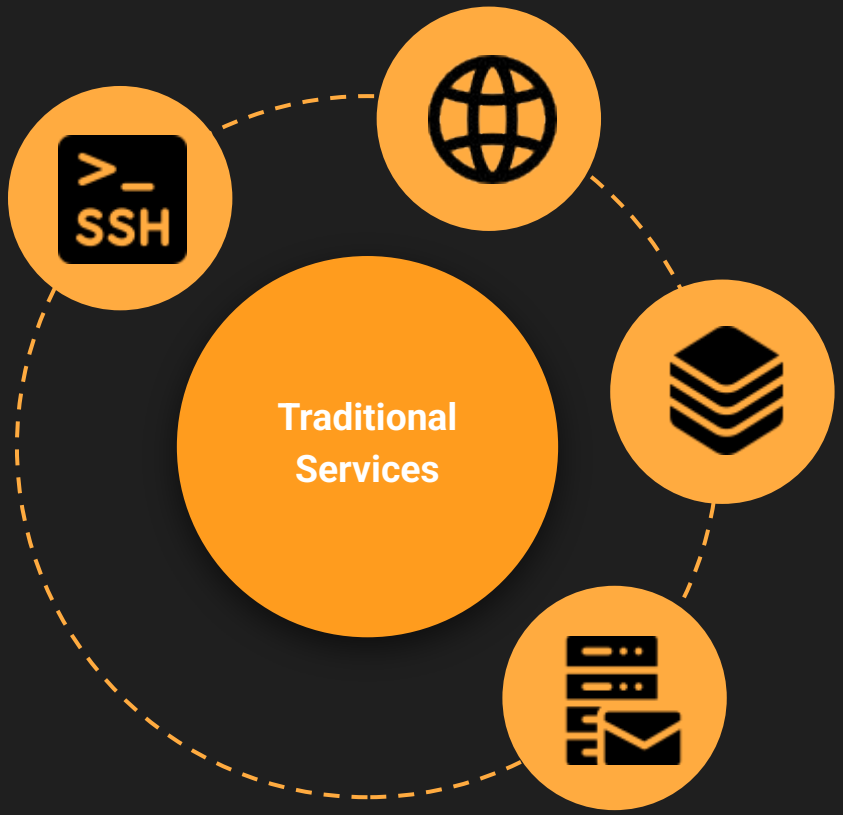
Is the Juice Worth the Squeeze?

- We want the most impact for the least effort
- We are on a time crunch
- Example:
  - You have a remotely accessible database server with an unknown amount of databases and users
    - Option A: Audit the database, apply principle of least privilege
    - Option B: Restrict ingress to a subnet



What Services Exist?

- Traditional
  - Remote Access (SSH/RDP)
  - Web Server
  - Databases
  - LDAP
  - Mail Servers
  - File Servers
- "Other stuff"
  - SAAS - Software as a Service
  - PAAS - Platform as a Service
  - Cloud Computing
  - etc.



In CCDC

- 10-30 Services
- 40% of Scoring

Relevant Services

- **Web Servers & Applications**
- **File Shares**
- Mail
- **Remote Access**
- **Databases**
- DNS
- Docker

Lab Goals (For each service)

What is it?

Functionally, examples

Management

Installation & Configuration

Security

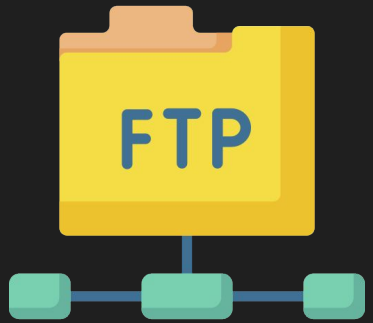
Threat Model each service

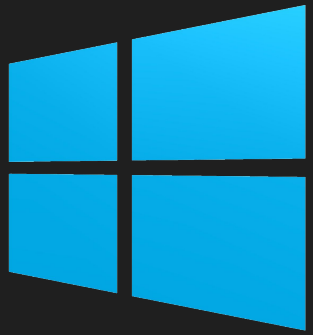
Remote Access

- SSH, RDP, VNC, WinRM
- Remote Access.. (crazy)
- TCP: 22, 3389, 5900, 5985/6

File Shares

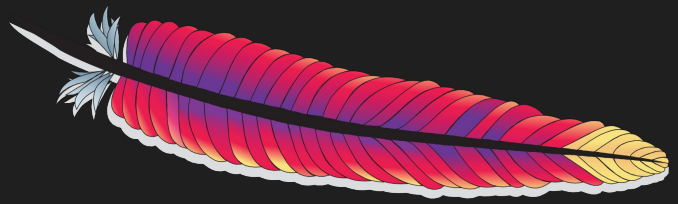
- Share files (crazy x2)
- FTP, SMB*
- TCP: 21, 445





Web Servers & Applications

- Web Servers
  - IIS, Apache2, Nginx
- Applications
  - XAMPP, Flask, etc.
- Other Uses
  - Reverse Proxies, Load Balancers
- TCP: 80, 443



Databases

- Store data (crazy x3)
- MySQL, MariaDB, PostgreSQL, MSSQL, Mongo, Cockroach
  - Yeah there's a lot
  - SQL is typically TCP:3306, except MSSQL

Application to CCDC

Operating in CCDC

- "An IT competition, with some focus on security" - someone probably
- We know how to set up & manage a service? What next?
  - Know the threat model for each service
  - Is the juice worth the squeeze?
    - Configure a password policy vs. changing passwords
    - Configure HTTPS vs. changing application admin's password
    - Is it even scored?
      - Block remote access ports
      - Change all database passwords vs. firewalling it
- **<u>INVENTORY</u>**

Homework (Due 9/13 @5:00 AM)

https://jessh.zip/ccdcfallweek2hw