CCDC Linux Week

Weekly Schedule

Date	CPTC (10AM-12PM)	CCDC (1PM-4PM)
~~Jul 11~~	~~Cyber Bootcamp Kickoff!~~	
~~Jul 18~~	~~Intro to Pen Testing~~	~~Business Week~~
~~Jul 25~~	~~Hacking Web Apps~~	~~Introduction to Networking~~
Aug 1	~~Hacking Linux~~	**Securing Linux** 
Aug 8	Hacking Windows	Securing Windows
Aug 15	Consulting	Common Services
Aug 22-23	CPTC Tryouts (All day)	
Aug 29-Sep 12		CCDC Fall
Sep 20-21		CCDC Tryouts (1-5 PM)

whoami

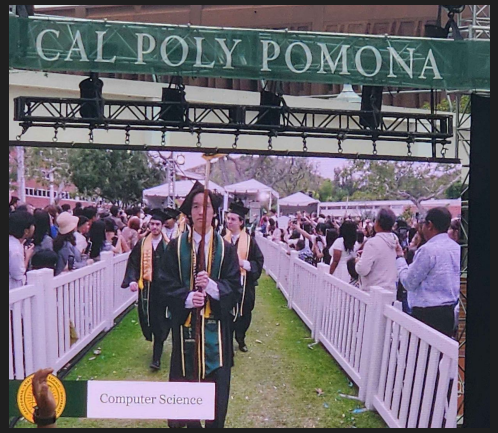
Adam Cheung | @adumb

IST Sysadmin Intern @ Esri

CCDC Co-Captain, Linux Lead 2026-2027
CCDC Linux Database 2025-2026

BS CS, Cyber Minor; MSIS 1st year
Sec+, Network+

slay da spire



whoami

Anson Ng | @2 acc

Cybersecurity Intern @ Varda

CCDC Linux Lead 2025-2026
Taco Bell IT 2024-2025
NCAE Cyber Games Nationals 2024-2025

senior citizen student

monkey brain

whoami

Natalie Tran | @natworking

CD&E Intern

CCDC (Co-)Captain 2025-2026
CCDC Networking 2024-2025

4th year CS

frogs <3

01 Linux Fundamentals

02 Linux Administration

03 Linux Security

04 Networking & Firewall

01

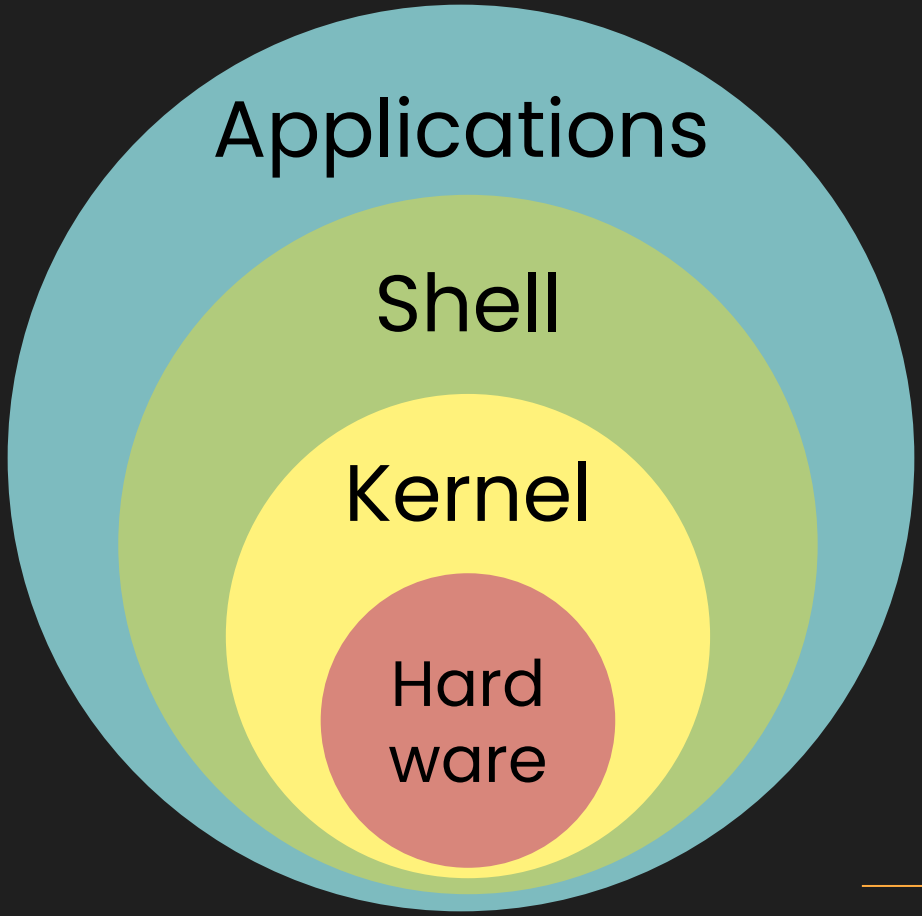
Linux Fundamentals

What is Linux

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

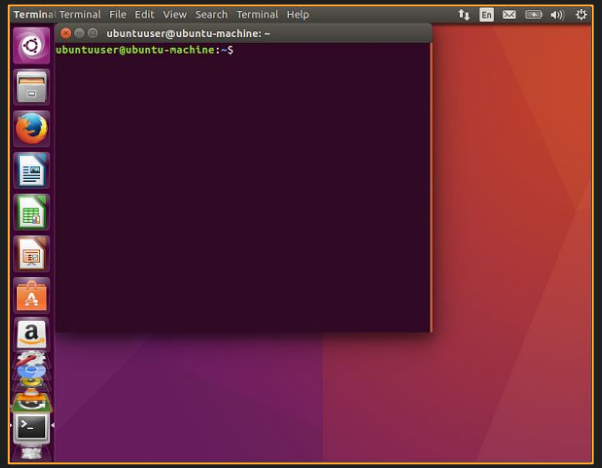





Applications
Shell
Kernel
Hard
ware

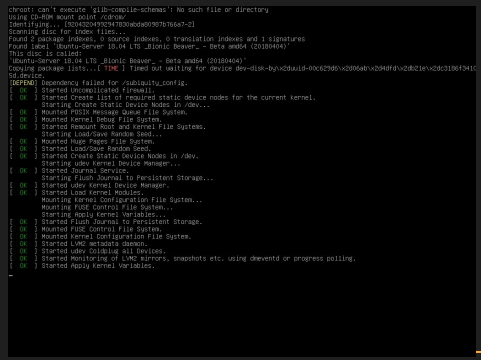
Terminals

Terminal Emulator



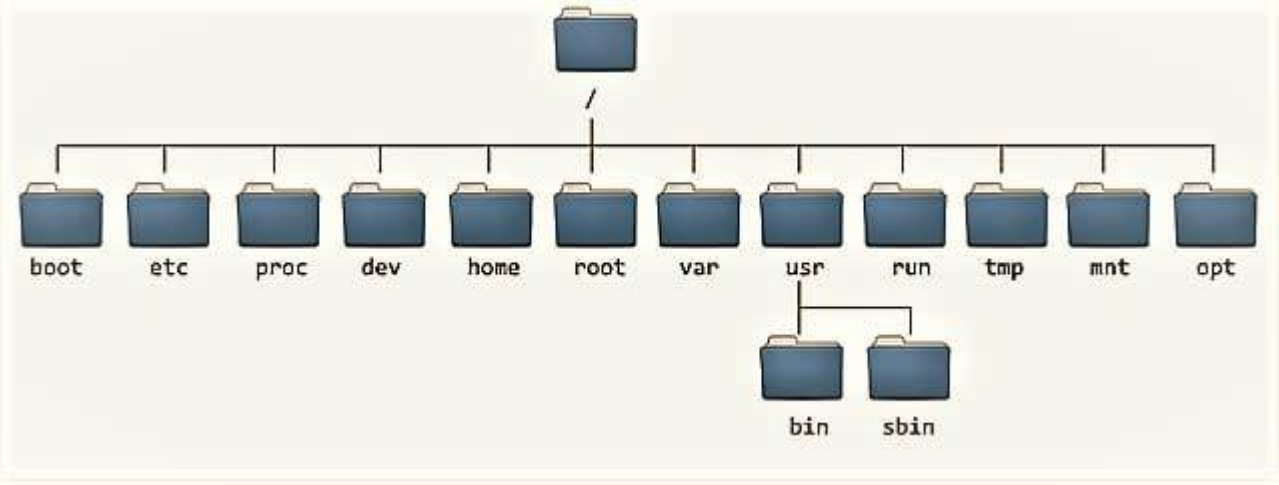
"Desktop" Version

"Server" Version



Linux File System

- Everything can be categorized into a File, Directory, or Link



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/	cd ~/Downloads
/etc/ssh/sshd_config	var/www/html/

root vs /root vs /

root user (uid 0) = admin

root (/) directory = start of file system

root user's home = /root

Shell and Syntax

command -options arguments

- EXAMPLE: ls
- EXAMPLE: cd /home/user1
- EXAMPLE: ls -la user1/Downloads
- EXAMPLE: iptables -L --line-numbers

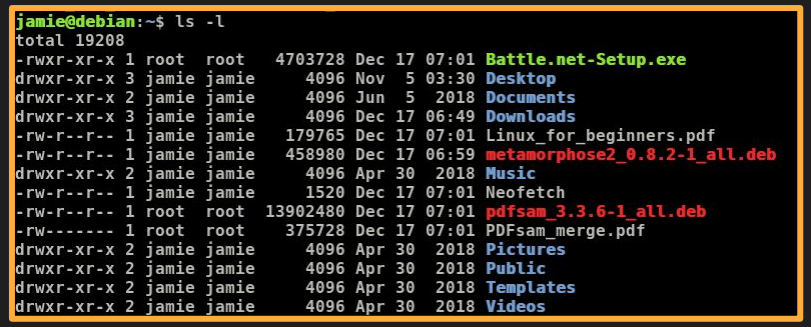
Listing Files

ls (list) → **ls [flags] [filepath]**

Flags:

-l (more detailed view)

-a (show all files and directories)



Creating Files

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

[favorite text editor] [filename]

nano, vim, vi

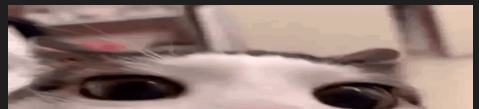
...many more for later...

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

Environment Variables

$PATH

An environment variable for 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

env

Command to list all currently set environment variables

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

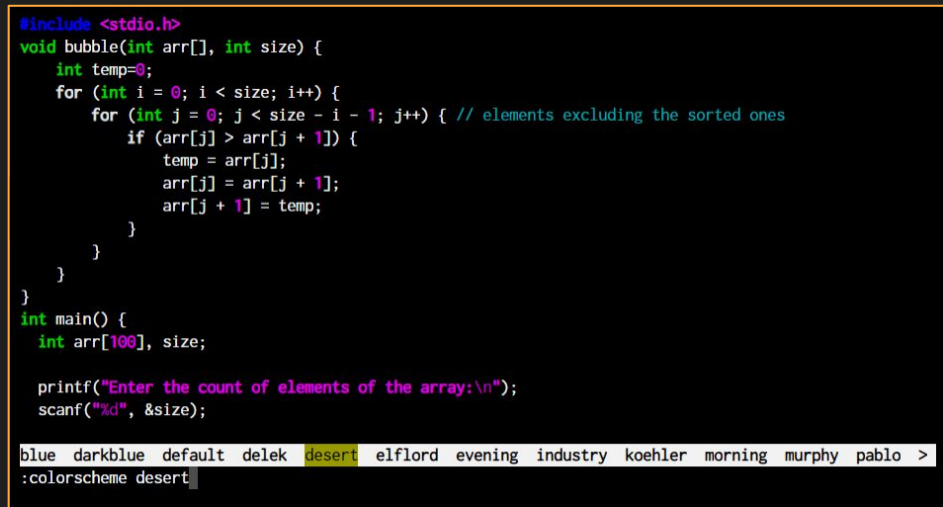

```
  GNU nano 2.0.9            File: txt_files/testfile                  Modified

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



SED

- **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
```

AWK

- **awk** <options> <script> <input>
- awk -F ',' '{print $2}' data.csv
- Good for filtering specific fields
- Similar to running a for loop on each line

```
ubuntu-user@HP:~$ awk '{print $1, $2}' employees.txt
John Manager
Stacy CEO
Duke Manager
Kate CEO
Sunil Manager
Duke CEO
Kate Manager
Sunil CEO
ubuntu-user@HP:~$
```

GREP

grep <options> "string to search for" <file>

cat <file> | grep "string"

Good for finding strings in a file

Lots of options

```
zunaid@Ubuntu:~$ grep "error" sample.txt
The word "error" appears here as lowercase.
This line mentions terror but not the actual error.
zunaid@Ubuntu:~$ grep -w "error" sample.txt
The word "error" appears here as lowercase.
This line mentions terror but not the actual error.
zunaid@Ubuntu:~$
```

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@                    :~$
```

Command line bash scripting

- bash scripts can be run using:

```
./file_name        Ex: ./my_script.sh

bash file_name     Ex: bash my_script.sh
```

NOTE: ensure your file has the executable (x) permission!

- With a bash shell, you can use bash code in the command line!

```
for line in $(cat poem);
do echo $line; done
```

Combining all the tools

Discuss among yourselves!

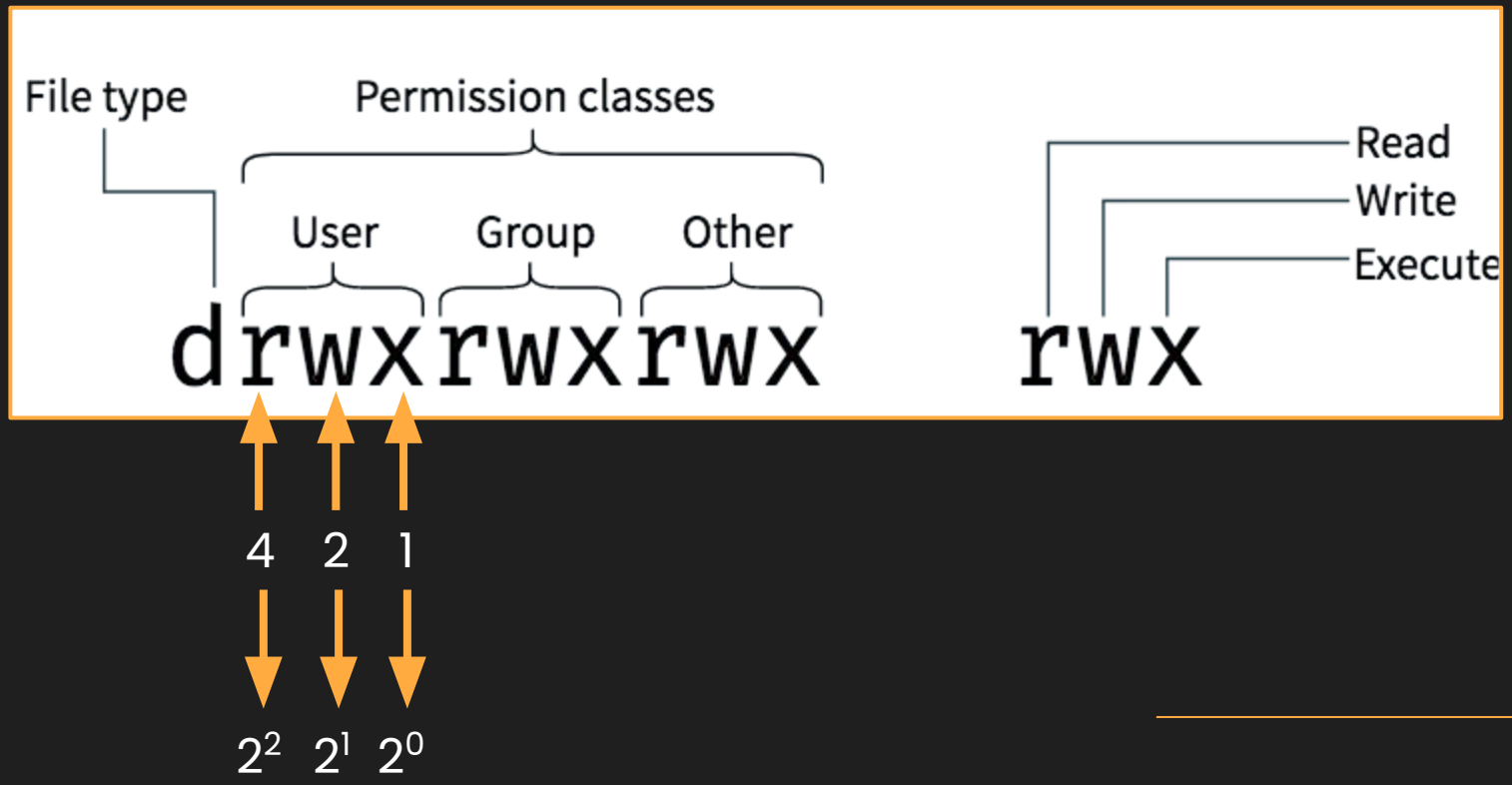
- What does the following command do?

```
cat /etc/passwd | grep -E ':(/bin/(bash|sh))$' | awk -F ':'
'{print $1}' > users
```

- TIP: Separate the command into segments split by pipes → | and process each segment one by one!

File Permissions

Linux File Permissions



Convert to octal

rwxr--r--

Convert to rwx

644

Convert to octal

r-x-w---x

Convert to rwx

755

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

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

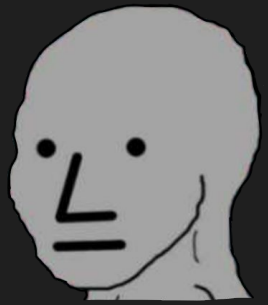
✨**usermod**✨

✨**id**✨

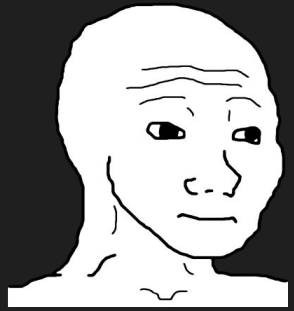
User IDs and Group IDs

root = 0

services < 1000



users > 999



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
```

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

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

:(

Services

Process running in the background managed by the system

systemctl <action> <service>

- systemctl status httpd
- systemctl start ssh
- systemctl enable nginx

service <service> <action>

- service httpd status
- service ssh start
- service nginx enable

status, start, enable, stop, disable, restart, mask

Processes

Program running on the computer

ps - List Processes for this terminal

- Often use "ps aux" instead for ALL processes

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

pgrep - Find PID from process name

Get Some Help

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

Tmux Cheatsheet

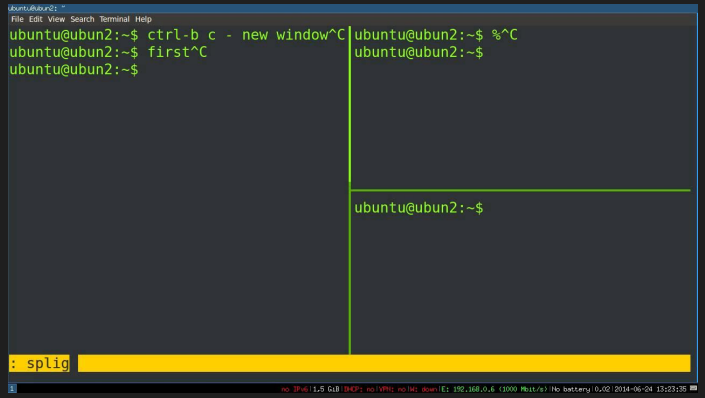
Prefix: ctrl + b

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 Shortcuts

- (ctrl + a) - go to the start of the command line
- (ctrl + e) - go to the end of the command line
- (ctrl + l) - clear screen
- (ctrl + left arrow) - go to the left most word
- (ctrl + right arrow) - go to the right most word
- (ctrl + r) - reverse search history based on typed letters
- (ctrl + p) - move back a command in history list
- (ctrl + n) - move forward a command in history list
- (ctrl + g) - exit reverse search mode
- (ctrl + u) - cut all text to left of cursor
- (ctrl + k) - cut all text to right of cursor
- (ctrl + w) - cut the word immediately preceding the cursor
- (Alt + d) - delete word after cursor
- (ctrl + y) - paste from clipboard (after cut)
- (!!) - repeat the last command
- (!$),(Alt + .) - insert the previous commands last argument

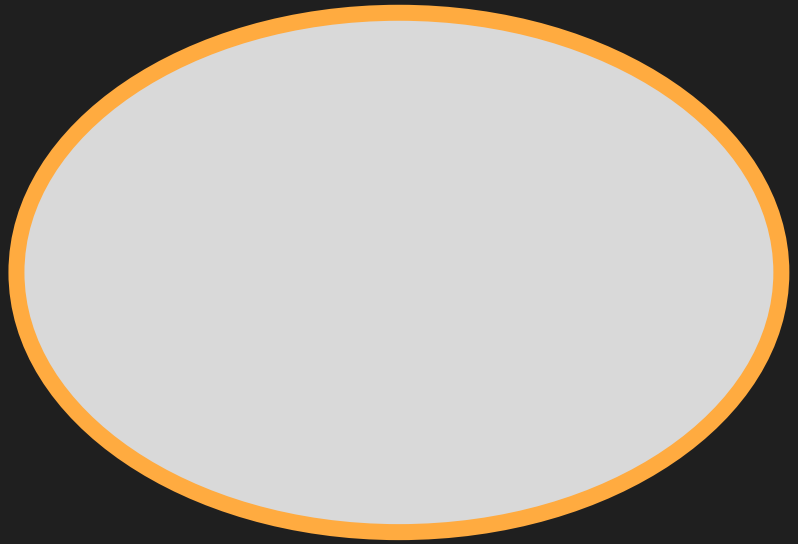
03

Linux Security

The Holy Square of User Management

/etc/passwd

/etc/group



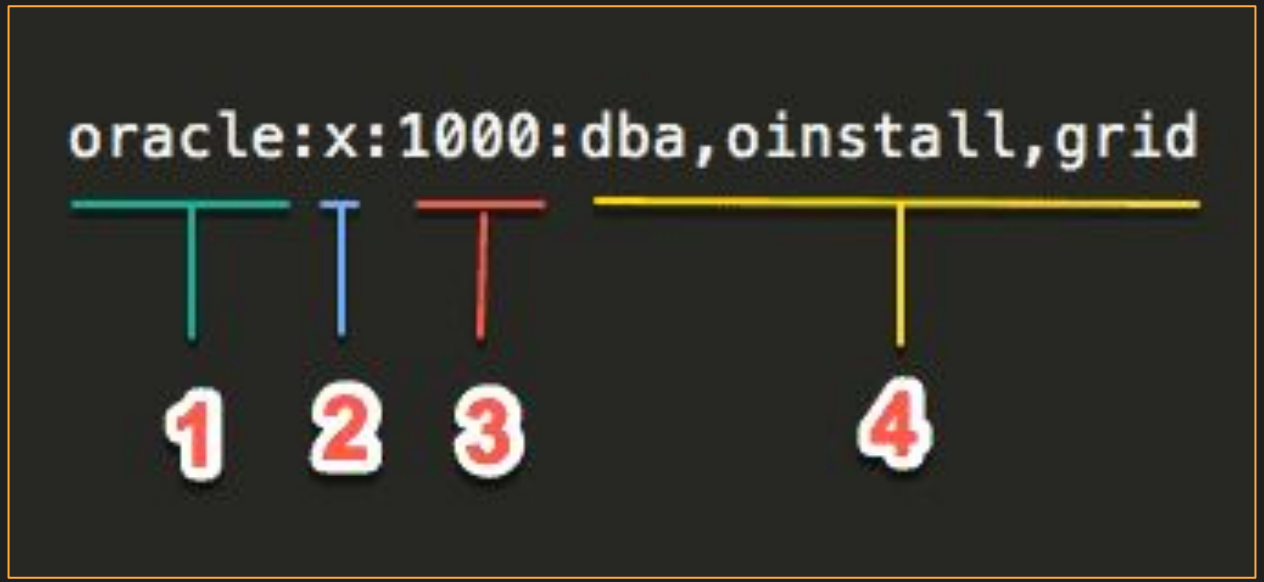
/etc/shadow

/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
```

cronjobs

- Tasks that run at regular intervals
  - Every day/week/month at certain times
- Can be good or bad
  - Always check for weird scripts!
  - crontab -e
  - /etc/cron.d
- If you have no use for it...
  - Kill it!
  - systemctl stop, disable, mask

```
# syntax of cron
#          ┌──────── sec (0 - 59)
#          │ ┌────── min (0 - 59)
#          │ │ ┌──── hour (0 - 23)
#          │ │ │ ┌── day (1 - 31)
#          │ │ │ │ ┌ month (1 - 12)
#          │ │ │ │ │ ┌ weekday (0 - 6)
#          │ │ │ │ │ │
#          │ │ │ │ │ │
#          * * * * * *   user-name   command to execute
          0 0 0 * * 6   root        /scripts/have_fun
```

04

Networking & Firewalls (but linux)

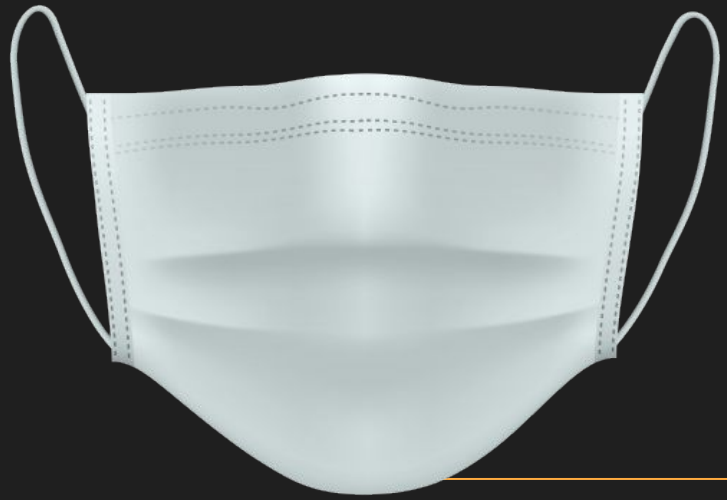
NetworkManager

(And other similar services)

NetworkManager, systemd-networkd, netplan

Manages network connections

Make sure it's running (systemctl)



Network Connections

Get NIC info with "ip a", "ifconfig", or "ipconfig"

View connections 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 on the network

```
┌──(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
```

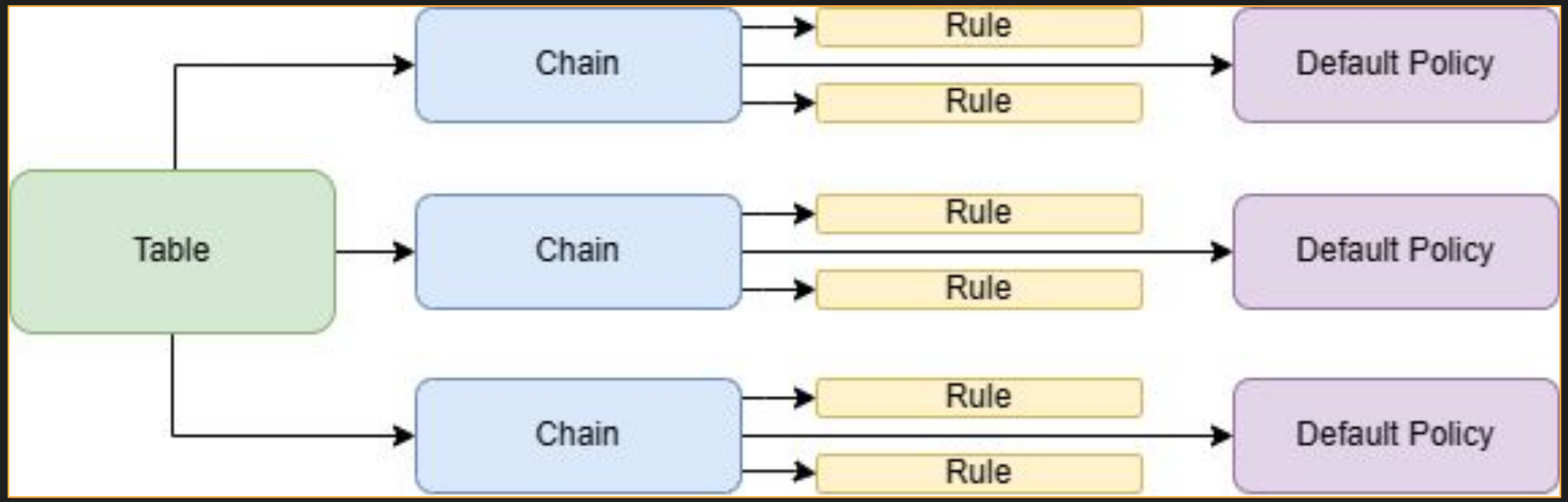
Firewalls

More ports = larger attack surface

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

Block by default, allow by exception

iptables - Overview



iptables - Filter Table

3 Chains:

- INPUT
- OUTPUT
- FORWARD

Default Policy*:

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

Flush Rules:

iptables -F

List Rules:

iptables -L --line-numbers

*be careful!!

iptables - Allowing HTTP 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
```

05

Secret Lab Slide

Homework !!

Due August 8th @ 5 AM PST
https://jessh.zip/2026ccdchw-4

Thanks!

Any questions? Please ask questions; we are available to help :D

Networking HW Walkthrough

- There's different ways to set up IPs for Windows and Linux.
- This will cover using the GUI for both

Things to Consider

Hostname	IP Address	Credentials
cd-su-router	**Part 1**	admin:pfsense
cd-su-linux	192.168.1.12	user:bruh root:bruh
cd-su-windows	192.168.1.19	Administrator:Password123

pod_1028_CCDC_Summer_Bootcamp_2026

pod number

Router Configuration

- The pfsense router's WAN is set to 172.16.255.1/16
- It needs to be set to 172.16.XX.1/16, where XX is the last two digits of the pod number
  - For this example, pod 1028 is used, so the WAN IP is 172.16.28.1/16
- Configuring the IP:
  - Change interface IP: 2
  - Interface → WAN: 1
  - Follow the directions to enter the correct IP, subnet mask, default gateway, and other prompts

Router Configuration

```
Enter an option: 2

Available interfaces:

1 - WAN (vtnet0 - static)
2 - LAN (vtnet1 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 172.16.28.1/16

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 172.16.0.1

Should this gateway be set as the default gateway? (y/n) y

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>
```

Router Configuration

```
Do you want to enable the DHCP server on WAN? (y/n) n

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to WAN...
 Reloading filter...
 Reloading routing configuration...

The IPv4 WAN address has been set to 172.16.28.1/16

Press <ENTER> to continue.
```

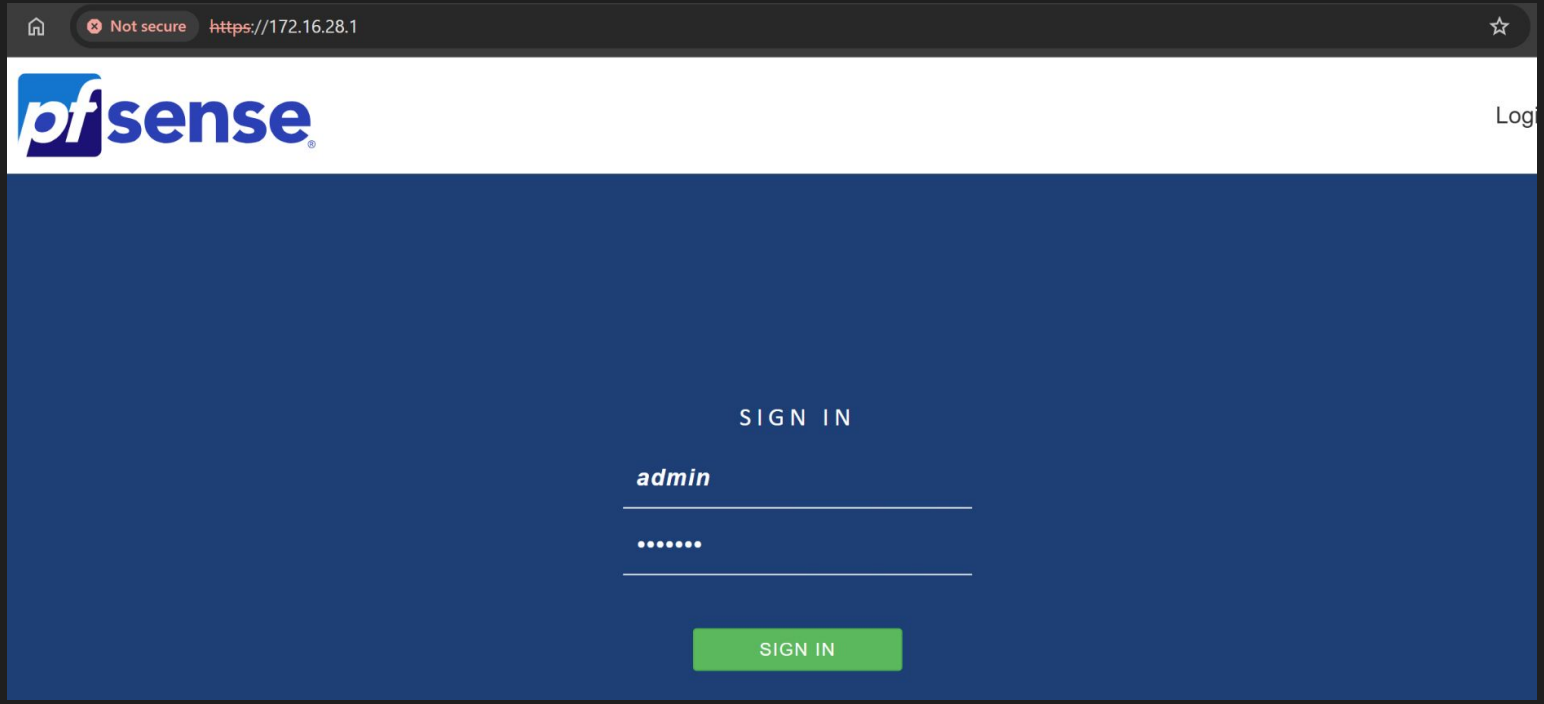
```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vtnet0     -> v4: 172.16.28.1/16
 LAN (lan)       -> vtnet1     -> v4: 192.168.1.1/24
```

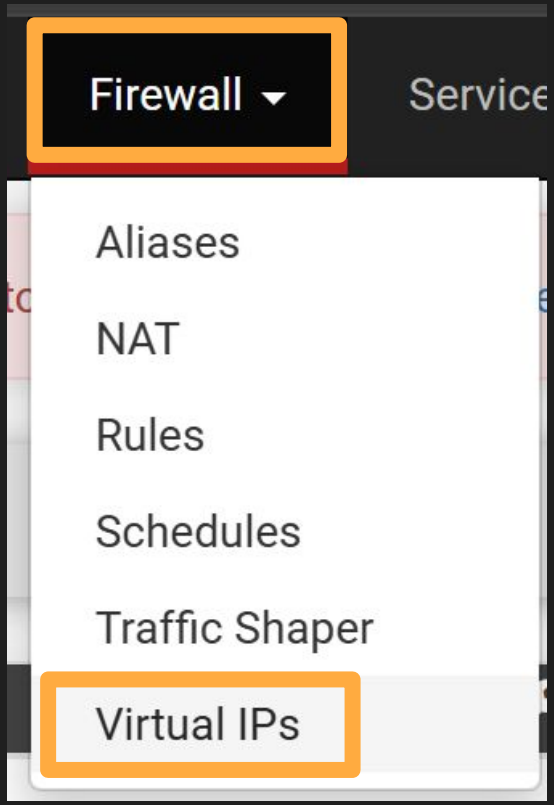
Router Configuration

- On the host (physical computer) go to the newly set WAN IP
  - Alternative: use the LAN IP (192.168.1.1) on the Linux/Windows VM to access the web configurator
- Sign in with the creds **admin:pfsense**
- Navigate to **Firewall > Virtual IPs**
- Edit the virtual IP address so that the third octet matches the new WAN's third octet
  - This will allow 1:1 NAT to work, all other NAT configurations were pre-made on the VM template
- Save and apply the change

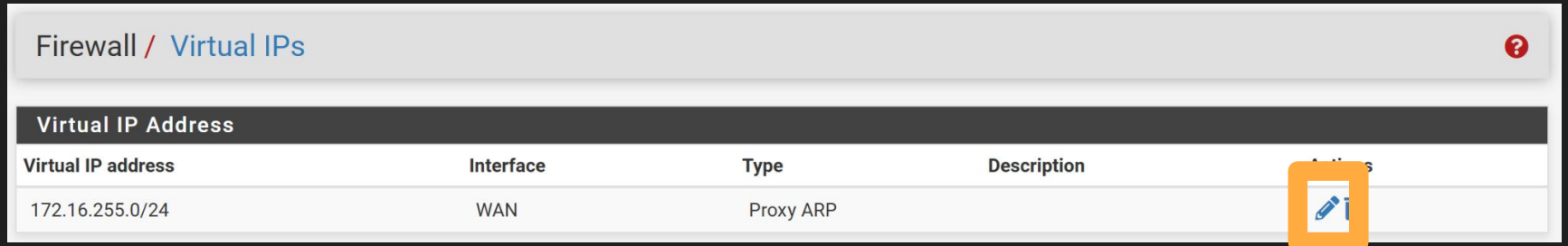
Router Configuration



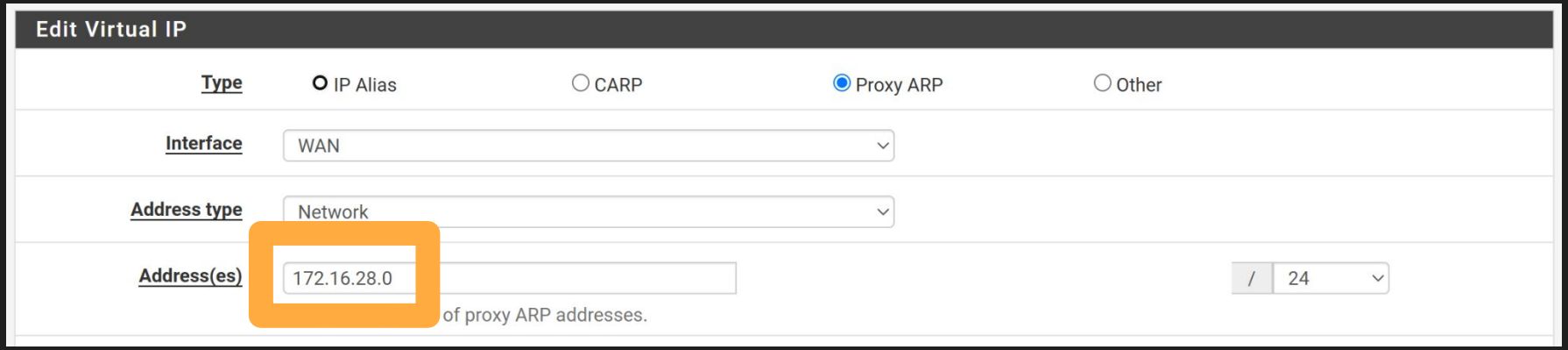
Router Configuration



Router Configuration



Router Configuration



Router Configuration

The VIP configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Virtual IP Address

Virtual IP address	Interface	Type	Description	Actions
172.16.28.0/24	WAN	Proxy ARP		

The changes have been applied successfully.

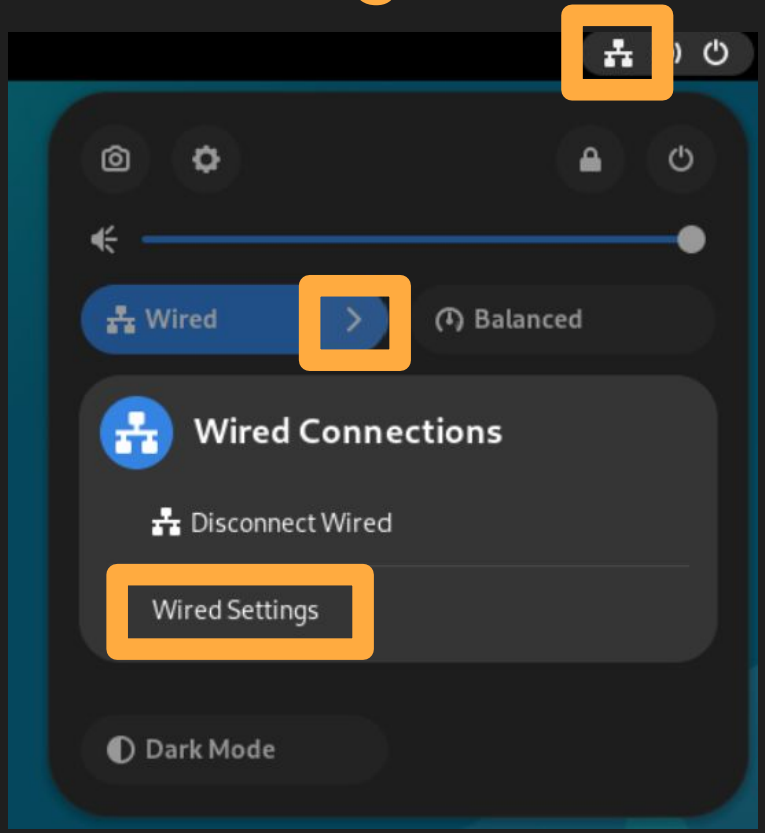
Virtual IP Address

Virtual IP address	Interface	Type	Description	Actions
172.16.28.0/24	WAN	Proxy ARP		

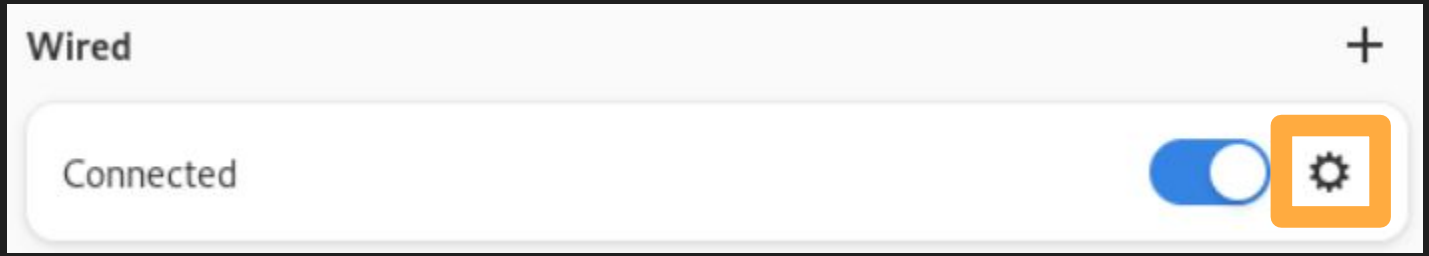
Linux Network Configuration

- Navigate to **wired connection icon (ethernet plug) > wired > wired settings**
- Click on the gear icon of the wired connection
- On the IPv4 tab:
  - Select manual because it will allow you to set a static IP
  - IP: 192.168.1.12
  - Subnet mask: 255.255.255.0 (corresponds to /24)
  - Default gateway: 192.168.1.1 (LAN IP of the router)
  - DNS: it can be kept as automatic, which will resolve to the router's DNS server, or use a public DNS server
- Toggle the connection slider twice to apply changes
- Check the configuration by displaying the IP address

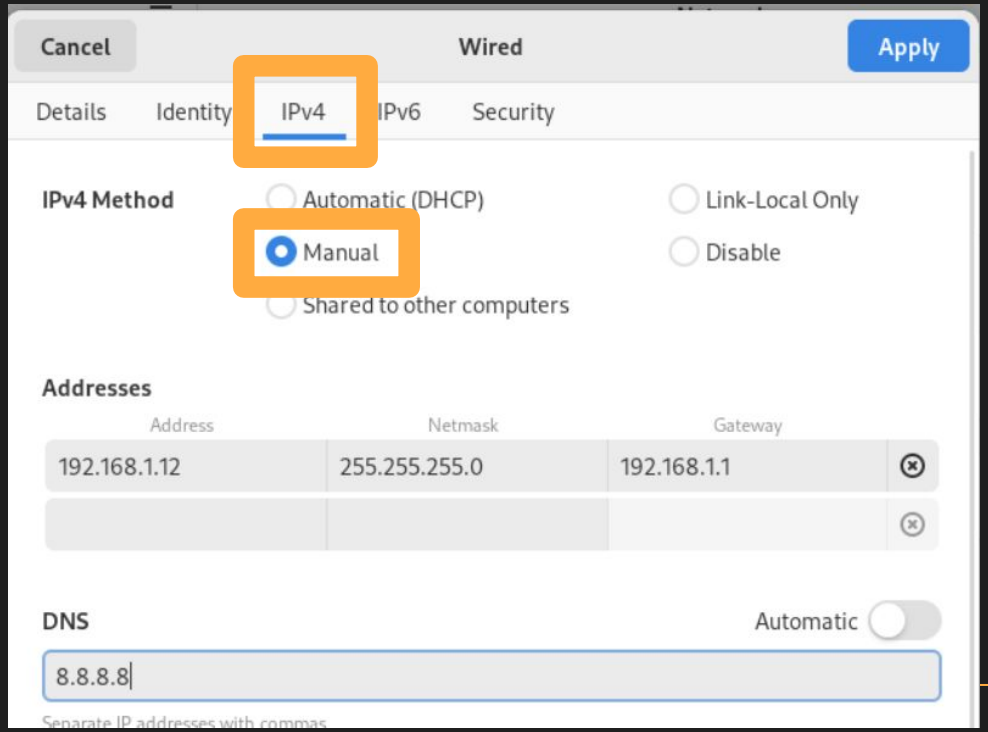
Linux Network Configuration



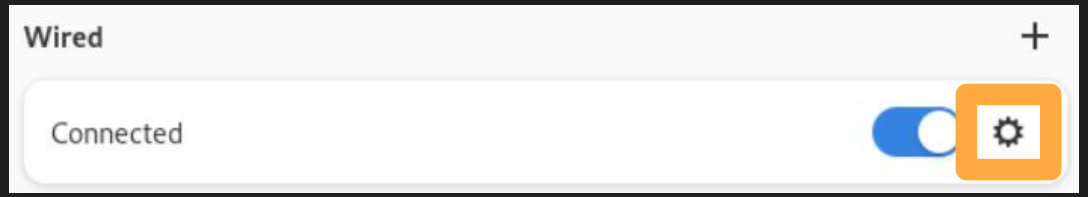
Linux Network Configuration



Linux Network Configuration



Linux Network Configuration



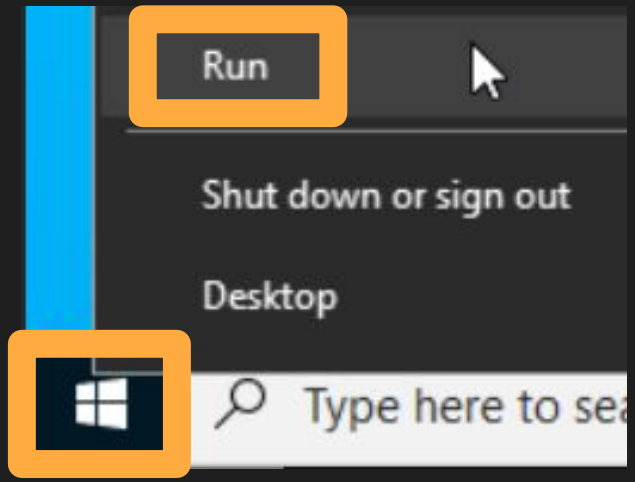
x2

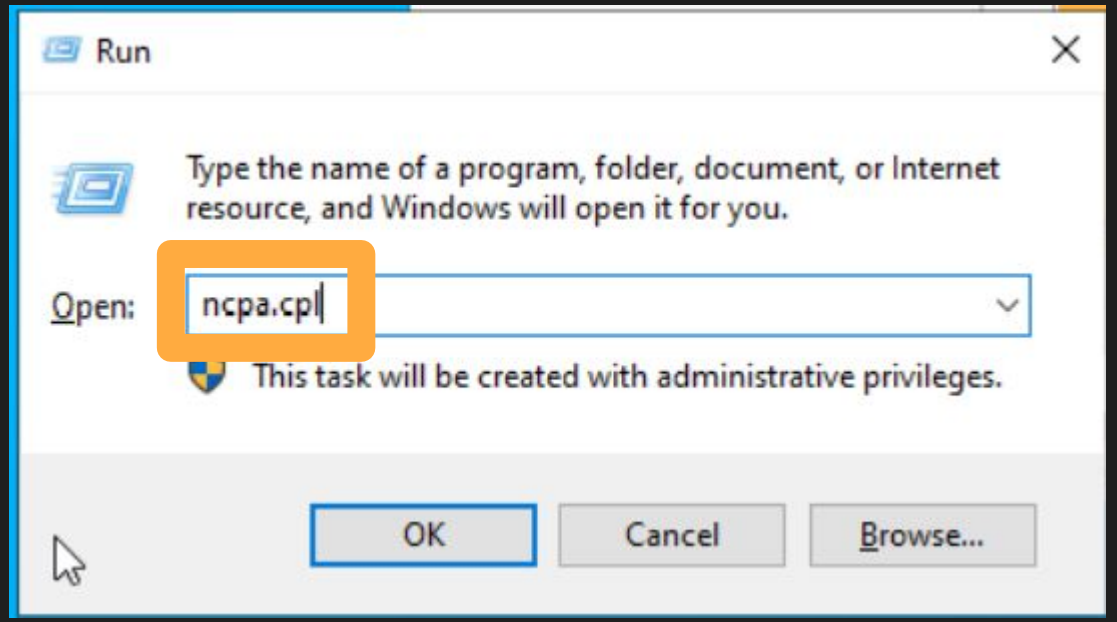
```
user@debian12:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:bf:b1:00 brd ff:ff:ff:ff:ff:ff
    alt
    ine  192.168.1.12/24  rd 192.168.1.255 scope global noprefixroute ens18
          referred_lft forever
    inet6 fe80::be24:11ff:febf:b100/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Windows Network Configuration

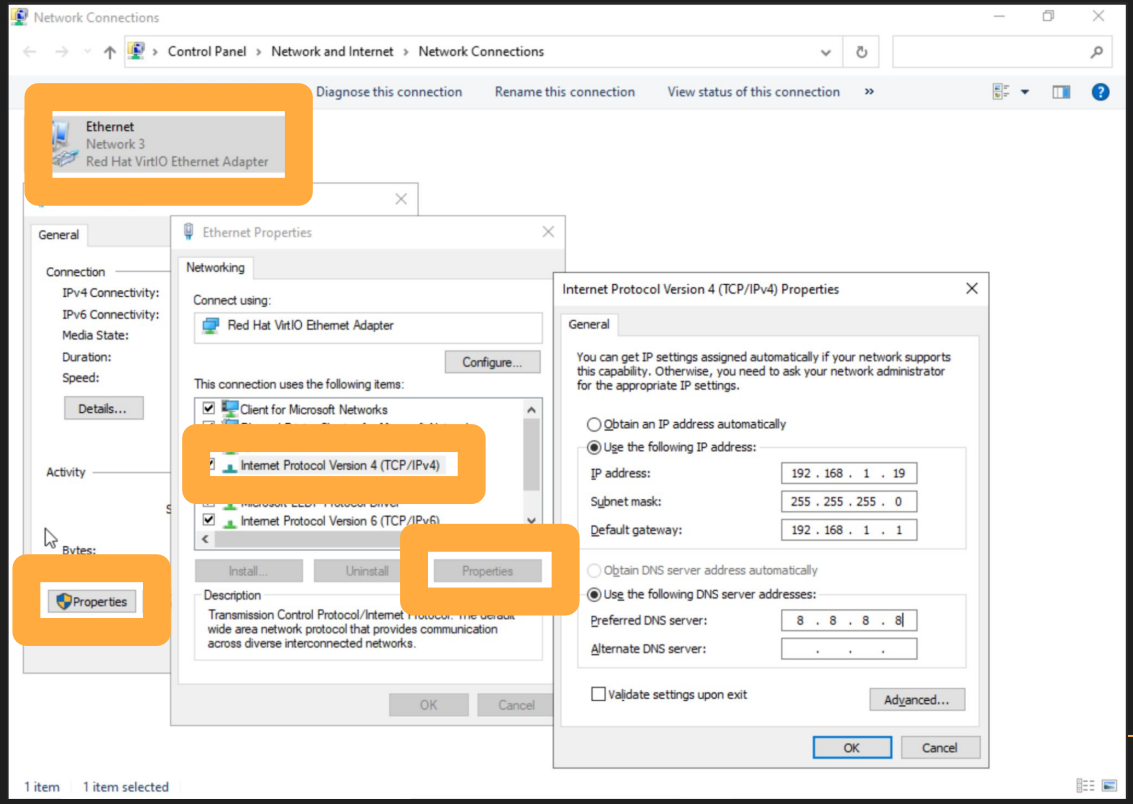
- Right click/two finger tap **Start > run**
- Enter ncpa.cpl to go to the network configuration
- Navigate to Ethernet > Properties > Internet Protocol Version 4 > Properties
- Fill out the network information:
  - IP: 192.168.1.19
  - Subnet mask: autofill on click
  - Default gateway: 192.168.1.1
  - DNS: 192.168.1.1 (pfsense's DNS server) or a public DNS server
- Apply the changes
- Display the IP address to check the configuration

Windows Network Configuration

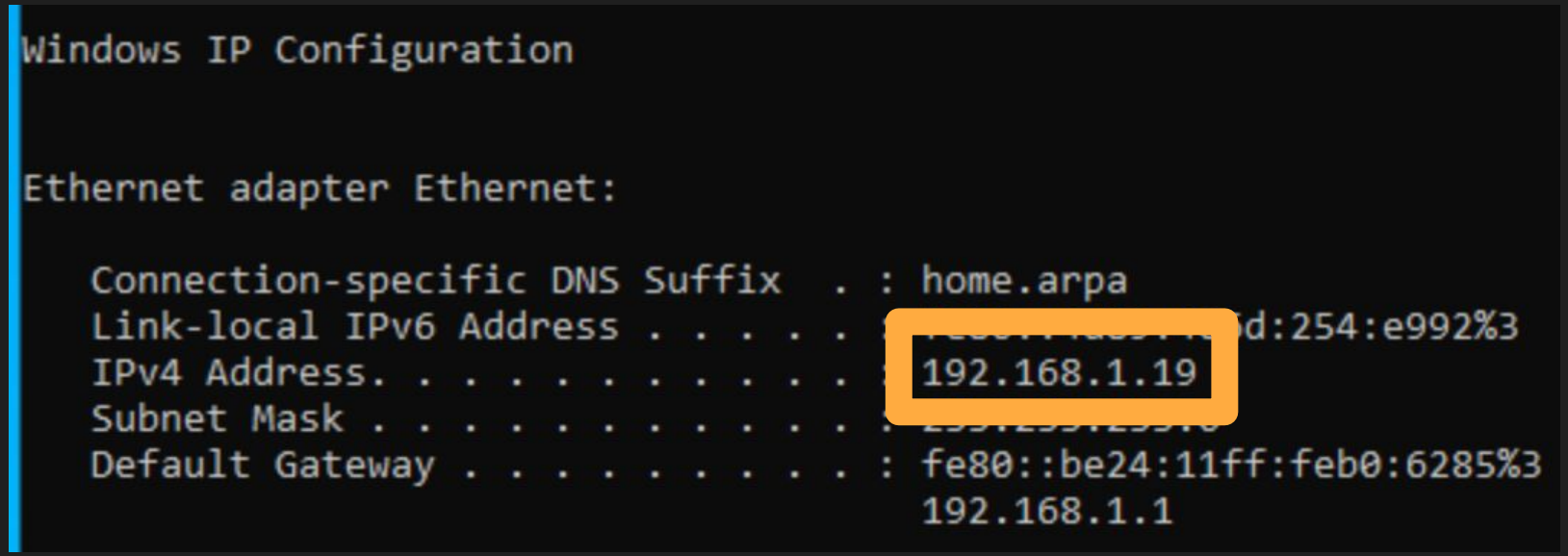




Windows Network Configuration



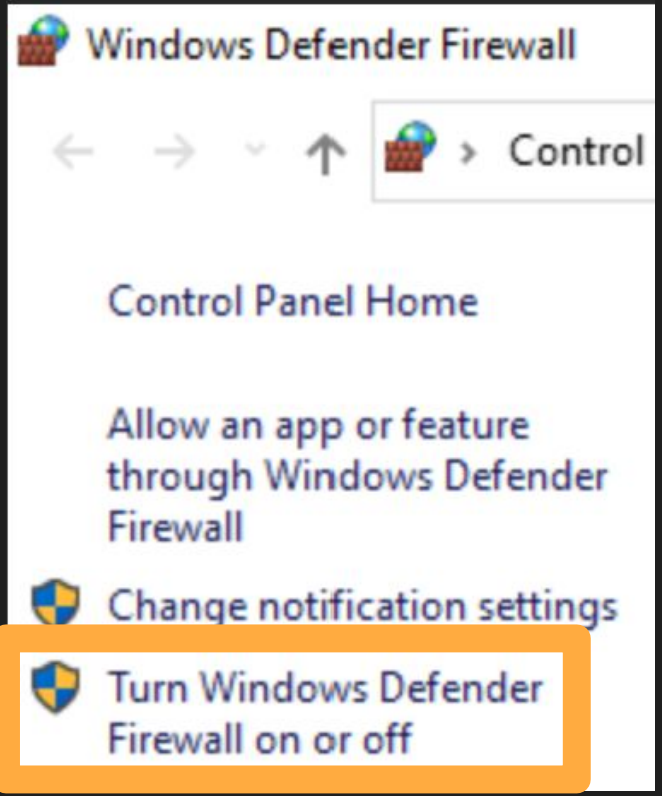
Windows Network Configuration

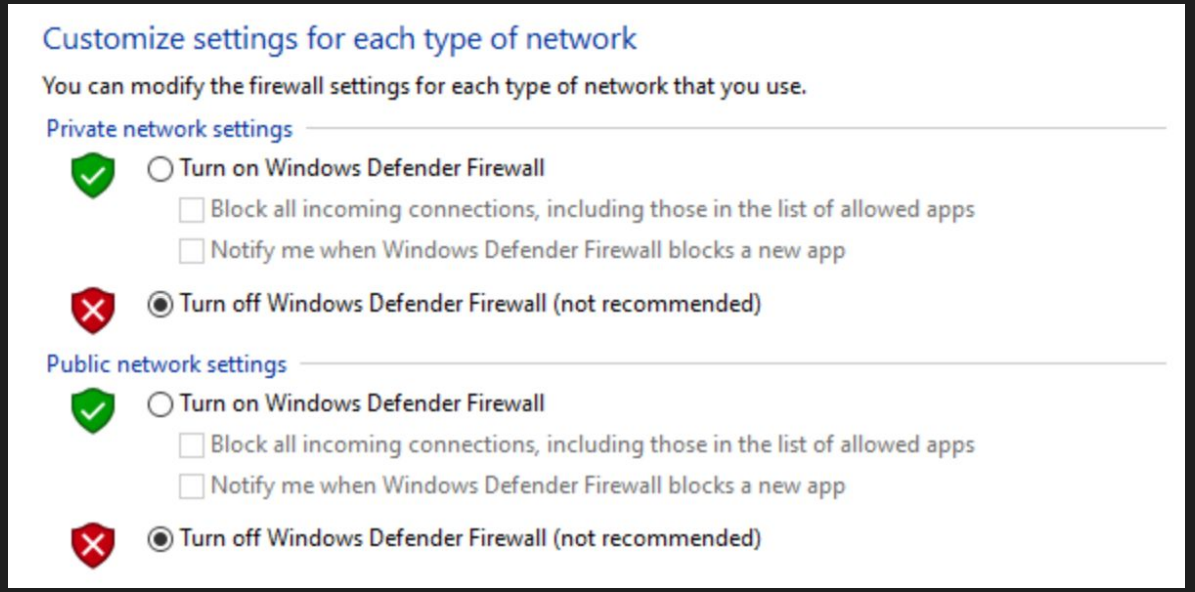


Windows Firewall

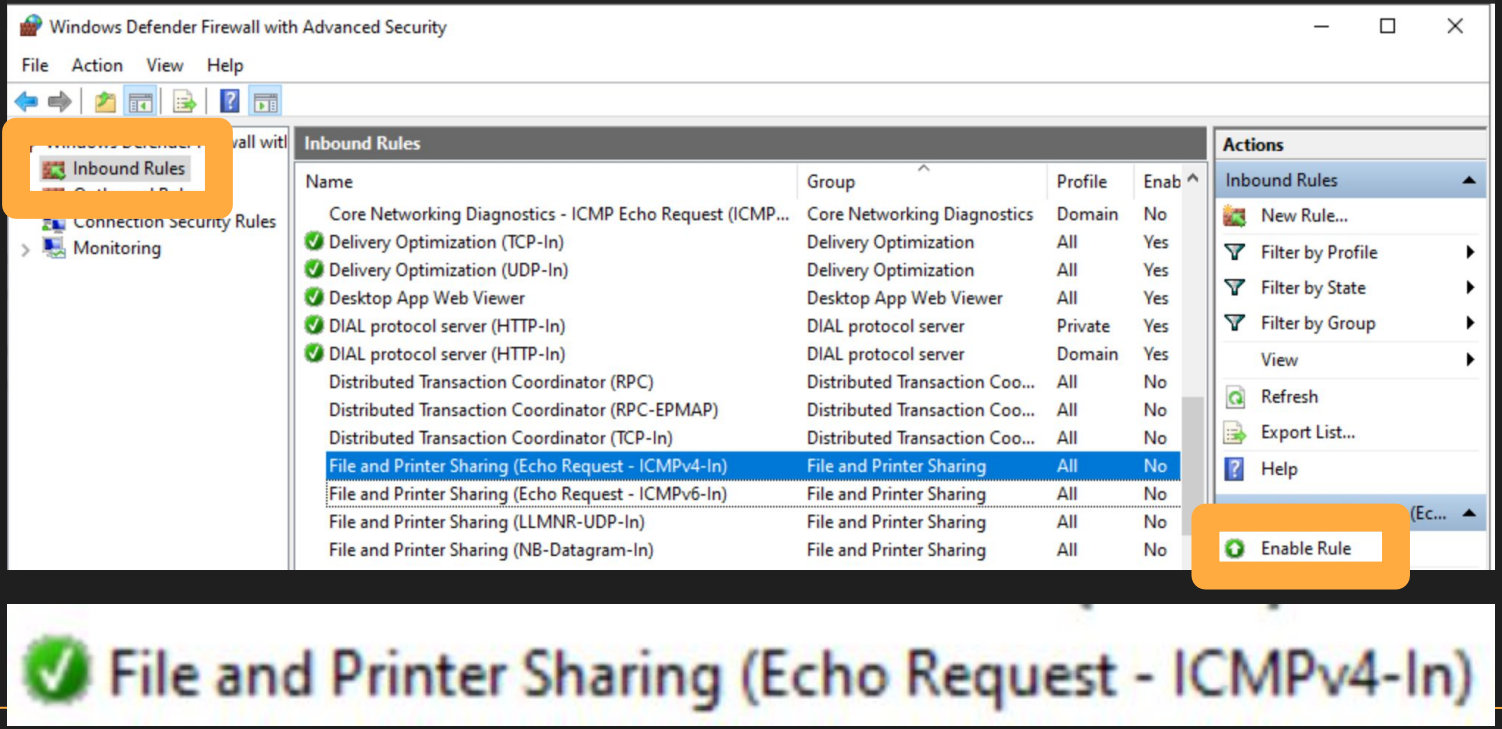
- Windows has ping/ICMP connections disabled, so it will not be pinged
- There are two workarounds:
  - Disable the firewall
    - Windows Defender Firewall > Turn firewall on/off > disable all profiles
  - Create a firewall rule to allow ICMP packets
    - Windows Defender Firewall with Advanced Security > Inbound rules > File and Printer Sharing (Echo Request - ICMPv4-In) > Enable rule

Windows Firewall: Disable Profiles





Windows Firewall: Enable ICMP



Check 1:1 NAT

- On the host machine (physical computer), go to the terminal and ping the Linux and Windows machines
  - Use the external IPs by translating the 192.168.1.0/24 network to the 172.16.XX.0/24 network

Check 1:1 NAT

```
PS C:\Users\trann> ping 172.16.28.12

Pinging 172.16.28.12 with 32 bytes of data:
Reply from 172.16.28.12: bytes=32 time=32ms TTL=62
Reply from 172.16.28.12: bytes=32 time=19ms TTL=62
Reply from 172.16.28.12: bytes=32 time=23ms TTL=62
Reply from 172.16.28.12: bytes=32 time=20ms TTL=62

Ping statistics for 172.16.28.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 32ms, Average = 23ms
PS C:\Users\trann> ping 172.16.28.19

Pinging 172.16.28.19 with 32 bytes of data:
Reply from 172.16.28.19: bytes=32 time=20ms TTL=126
Reply from 172.16.28.19: bytes=32 time=17ms TTL=126
Reply from 172.16.28.19: bytes=32 time=20ms TTL=126
Reply from 172.16.28.19: bytes=32 time=18ms TTL=126

Ping statistics for 172.16.28.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 20ms, Average = 18ms
```