Practicing Safe Cyber

Sandboxed Environments and More

Attendance Form:

https://da.gd/VDqZ9

SIGN IN PLEASE :DDD

https://da.gd/VDqZ9

whoami

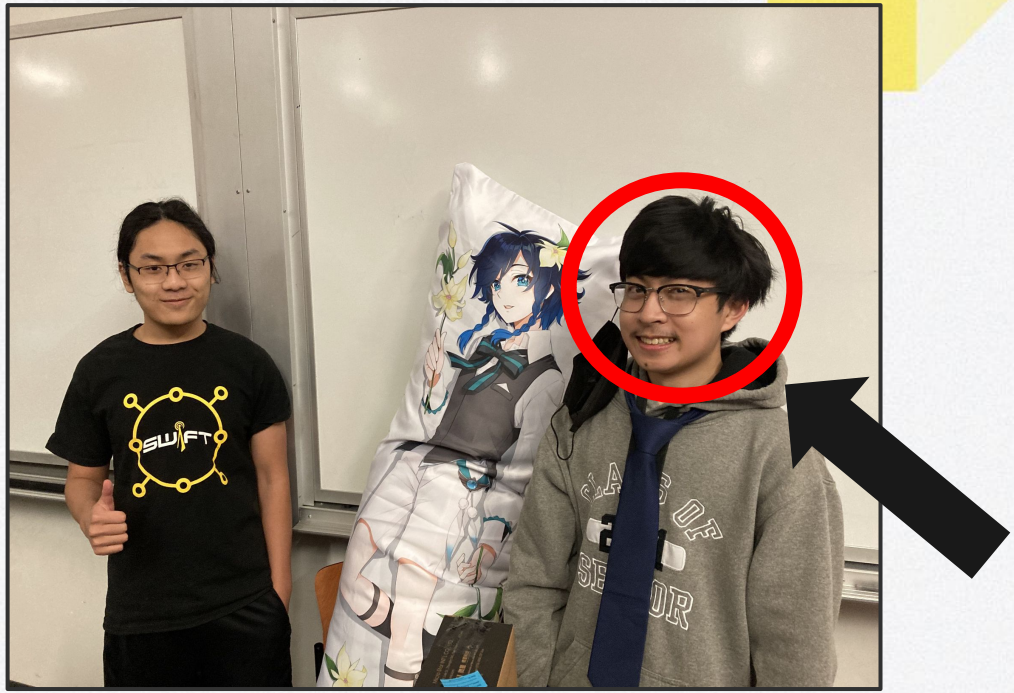
Gabriel Fok
CISSP
CCDC Captain
CPTC Co-captain
CCDC 2020-????
CPTC 2021-???

whoami

Dylan Tran
OSCP
Fumo collector
CPTC/CCDC 2021-????

whoami

Jacob "Chet Apichart" Jayme
Band Lover 2017-2021
CPTC 2021-2022
CCDC 2021-????



What is safe cyber?

Safe cyber is **safely** using computers, the Internet, and related technologies while researching potentially dangerous content. This includes **social engineering awareness**, **sandboxing**, and **ethical research**.

Agenda

1

Basic Practices

General safety and more

2

IT Fundamentals

Need-to-know info/theory

3

Virtual Machines

Dirtbox? No. Sandboxes

4

Containers

Contain ur excitementhahah!

01

Basic Practices

General safety and research

Staying Safe Online

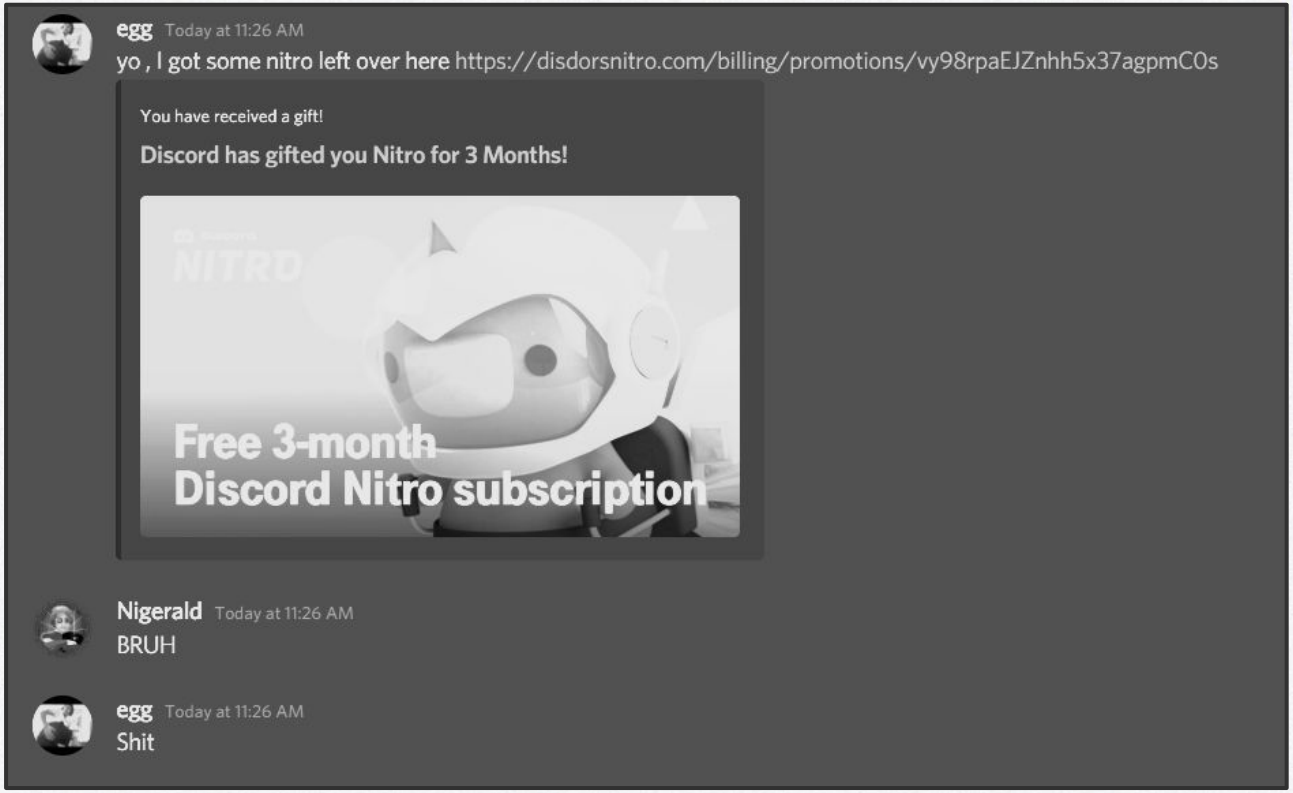
Phishing

- Scams
- Fake people or links
- Fake Sites

Malware

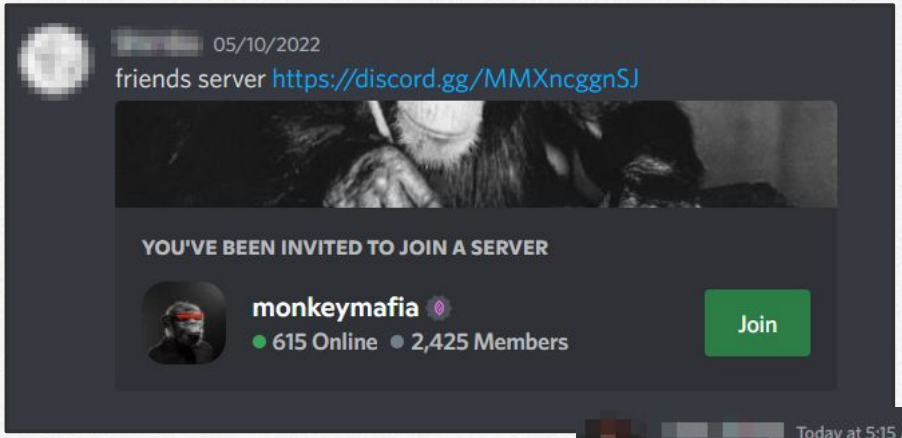
- Executables
- Macro-embedded documents

Exhibit A: Phishing



- Check links
- Check email address
- Don't run suspicious files
- Reality sucks. If it sounds too good, it's probably fake.

Exhibit B: More Phishing



- Unusual activity from friends?
- Verify legitimacy, double check with them

Exhibit C: Funky sites

- Check your urls
- Is there a lot of redirects?
- HTTPS on?
- Use adblockers and popup blockers

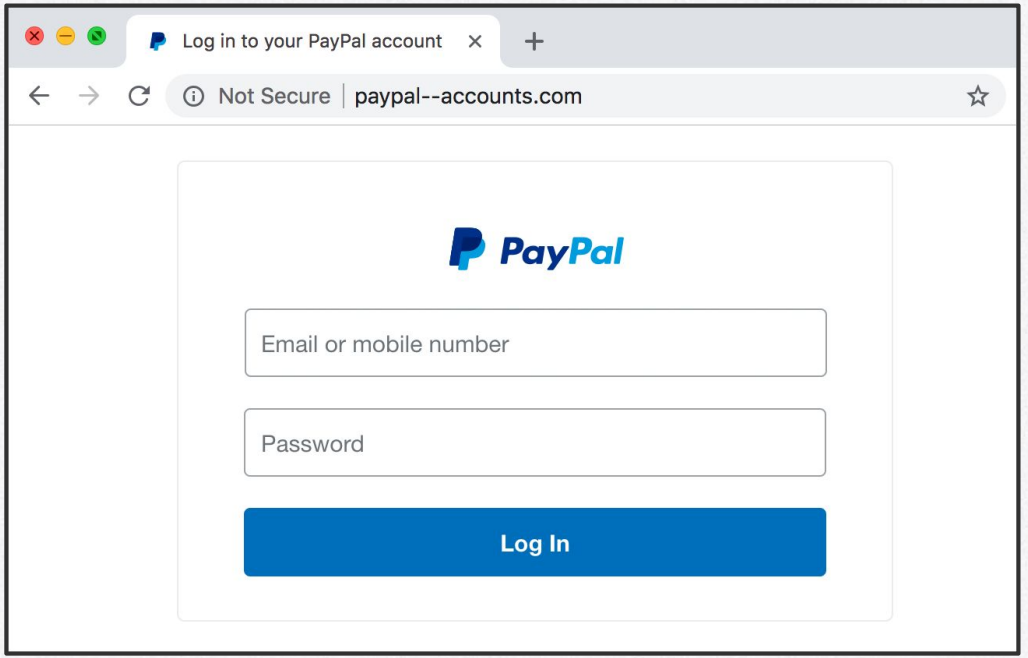
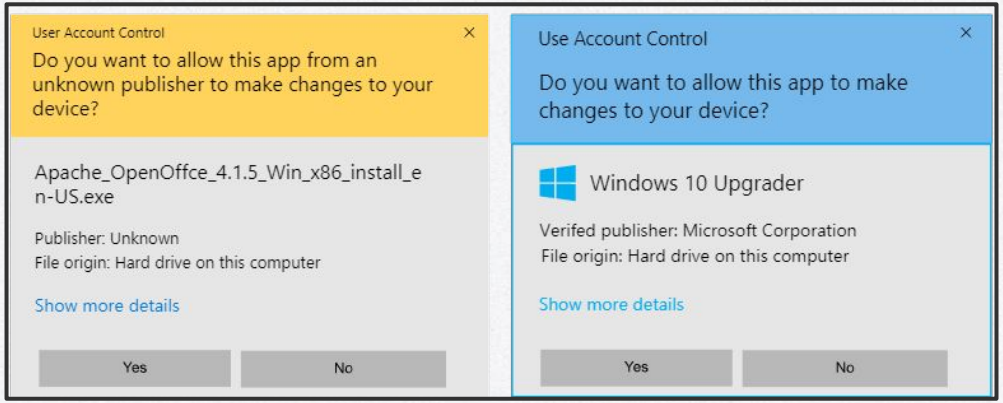
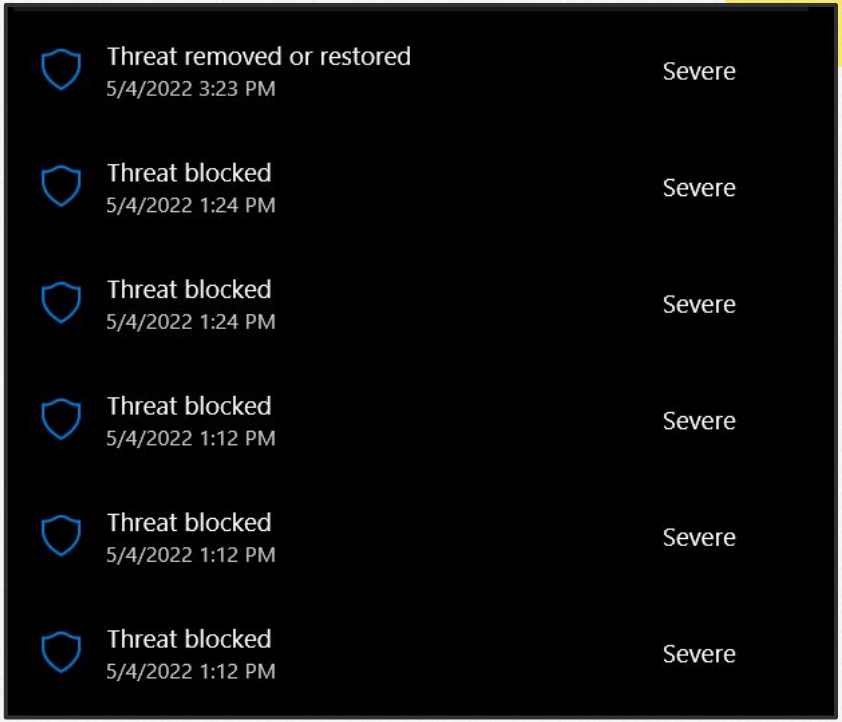


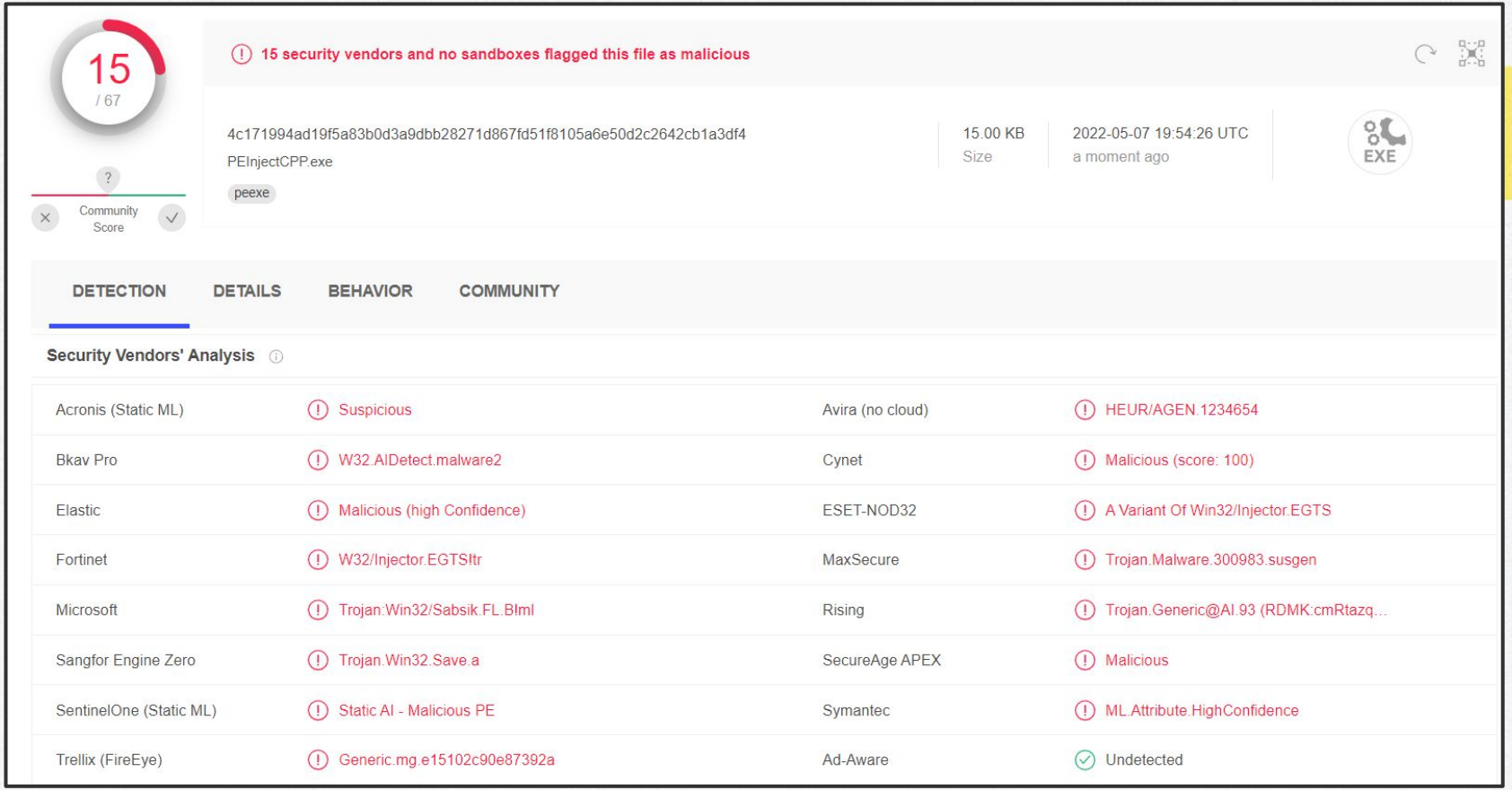
Exhibit D: Malware?

- If defender pops off, it's probably bad
- If it asks to be run with Admin, be careful

Unverified vs verified

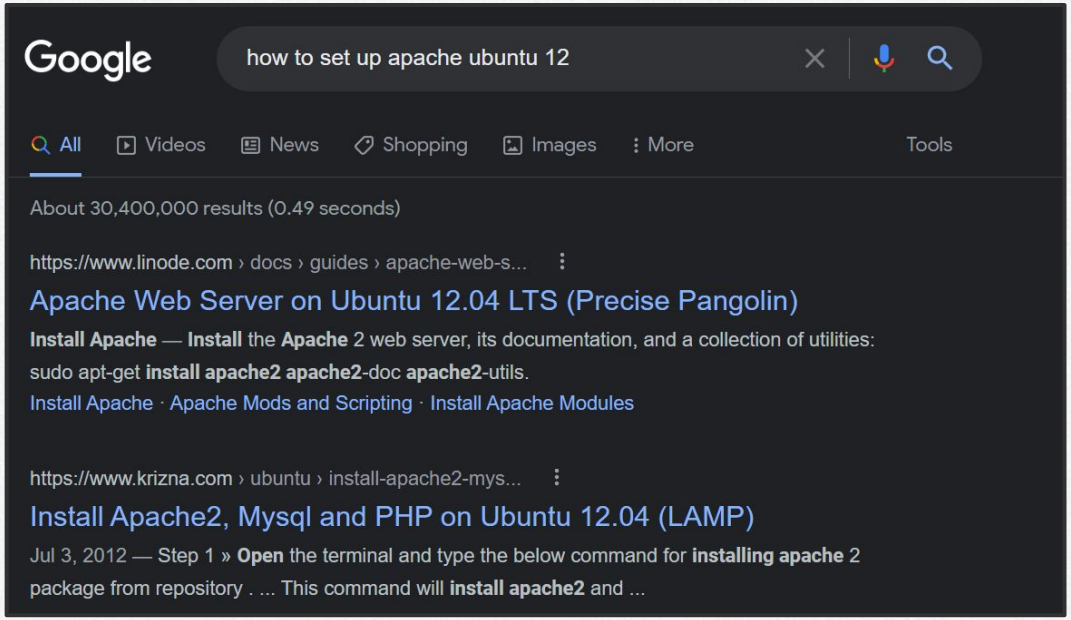





15
/ 67
Community Score
15 security vendors and no sandboxes flagged this file as malicious
4c171994ad19f5a83b0d3a9dbb28271d867fd51f8105a6e50d2c2642cb1a3df4
PEInjectCPP.exe
peexe
15.00 KB
Size
2022-05-07 19:54:26 UTC
a moment ago
EXE
DETECTION
DETAILS
BEHAVIOR
COMMUNITY
Security Vendors' Analysis
Acronis (Static ML) Suspicious
Avira (no cloud) HEUR/AGEN.1234654
Bkav Pro W32.AIDetect.malware2
Cynet Malicious (score: 100)
Elastic Malicious (high Confidence)
ESET-NOD32 A Variant Of Win32/Injector.EGTS
Fortinet W32/Injector.EGTSltr
MaxSecure Trojan.Malware.300983.susgen
Microsoft Trojan:Win32/Sabsik.FL.Blml
Rising Trojan.Generic@AI.93 (RDMK:cmRtazq...
Sangfor Engine Zero Trojan.Win32.Save.a
SecureAge APEX Malicious
SentinelOne (Static ML) Static AI - Malicious PE
Symantec ML.Attribute.HighConfidence
Trellix (FireEye) Generic.mg.e15102c90e87392a
Ad-Aware Undetected

How to Google

- General enough to get results, specific enough to fit your situation
- Use quotes and tacks
- Searches can tell you what you are missing from your search
- Don't be afraid to Google



```
┌──(nored0x㉿NoRed0x)-[/usr/share/doc/python3-impacket/examples]
└─$ python3 GetUserSPNs.py karim.net/admin:p@ssw0rd -dc-ip 192.168.128.140 -request
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

ServicePrincipalName             Name          MemberOf  PasswordLastSet
-------------------------------  ------------  --------  -------------------
MSSQLSvc/domainAD.karim.net:1443 mssqlserver             2021-03-02 04:18:35.504812
karim/support1user               support1user            2021-03-04 01:32:34.159099
HTTP/domainAD.karim.net          websvc                  2021-03-04 12:56:27.264377


[-] Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
```

If you find this **error** from Linux: **`Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)`** it because of your local time, you need to synchronise the host with the DC: `ntpdate <IP of DC>`

Doing Something

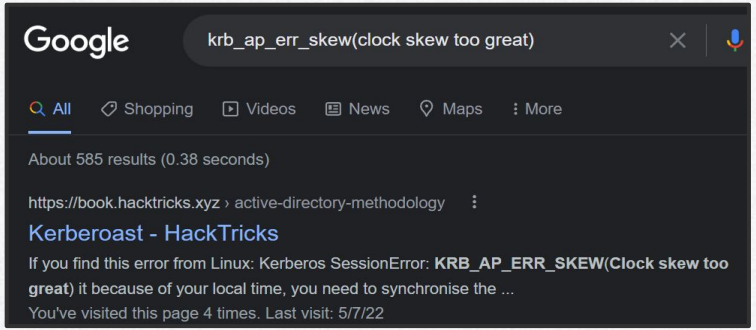
Run into error

Read

Find solution

Google Error

Find text in an article in search results



02

IT Infra Fun

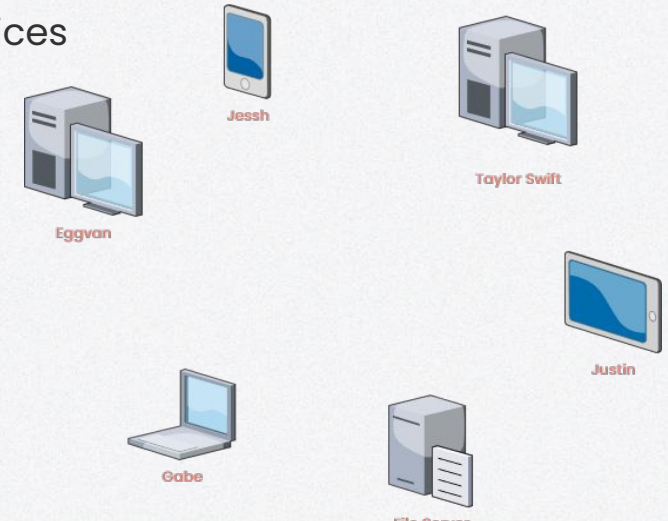
Fun with In-fun-structure (so fun)

Components - Hardware

Hardware

Physical components of your infra. Include:

- Desktop Computers
- Laptops
- Tablets, smartphones, and other mobile devices
- Printers/scanners
- Servers and data centers
- Routers
- Switches



Printer

Team [redacted]
From: IT Staff
To: [redacted]

Hello [redacted]

We have configured the printer. Please let us know if there is anything else you would want us to provide.

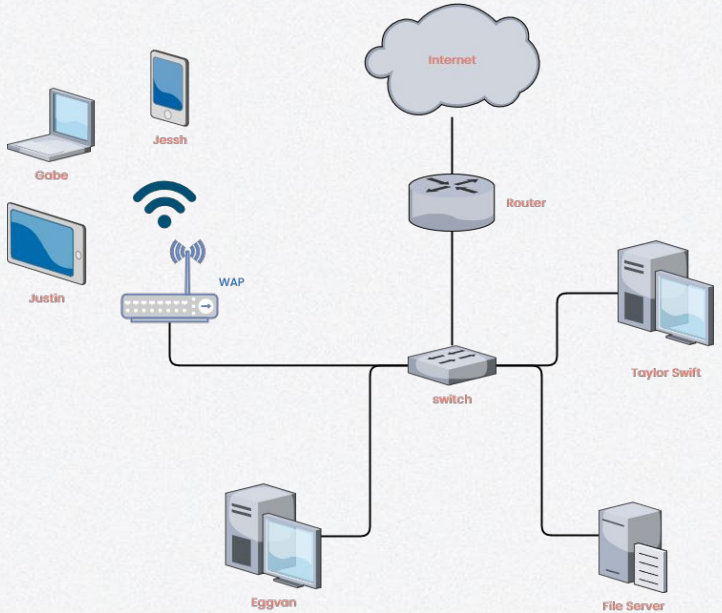
Thanks,
[redacted]

Components - Networks

Networks

Allow you to combine devices into a single network and connect them to the internet, as well as share resources across the network.

- Internet Connectivity
- Network Enablement
- Firewalls and Security
- Routers
- Switches
- Cables



Components - Software

Software

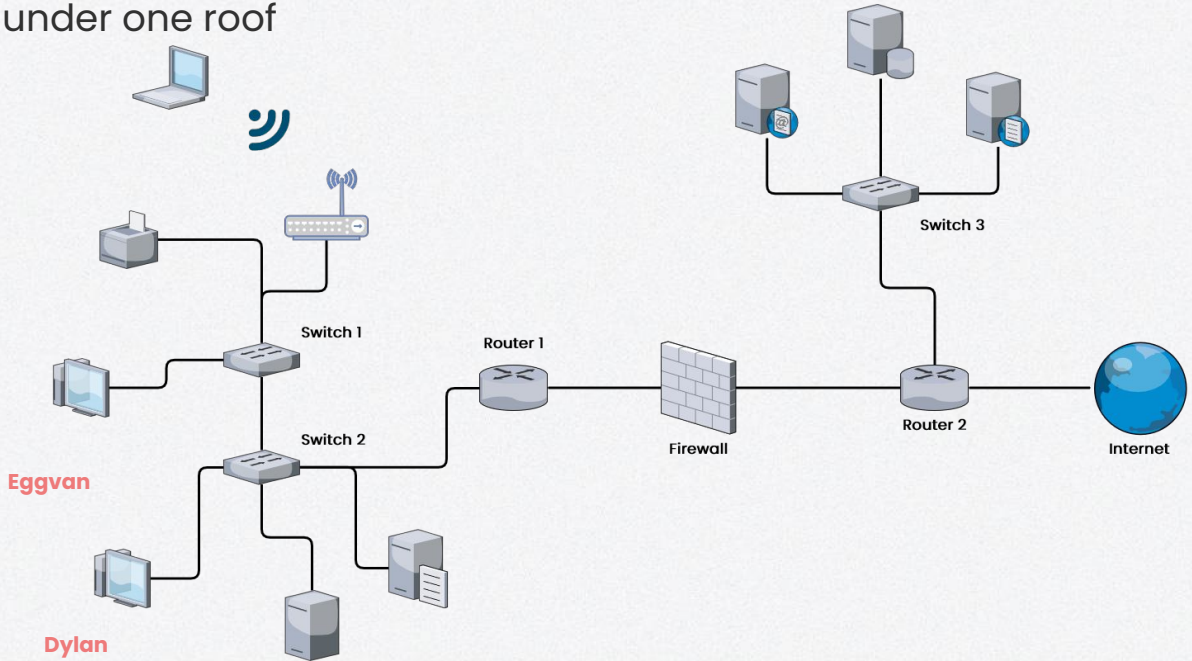
Includes the various programs and applications that a business uses to function. Includes:

- Content Management Systems (CMS)
- Customer Relationship Management (CRM)
- Operating Systems
- Web servers
- Custom software for internal work

Traditional IT Infrastructure

Main components are hardware and software:

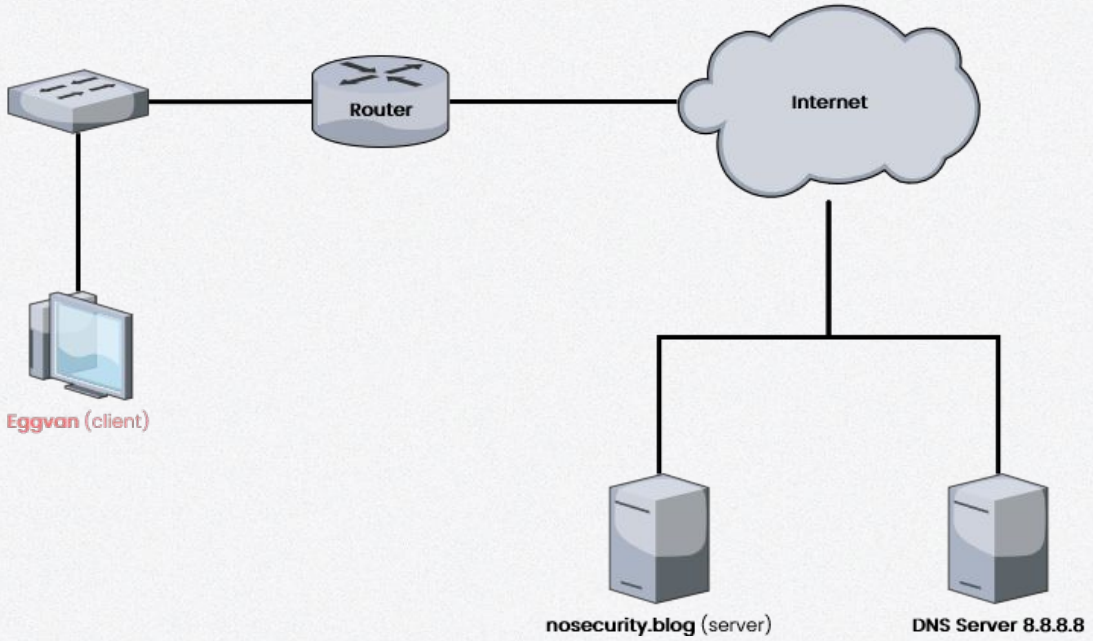
- Various servers and desktop PCs.
- All equipment located under one roof
- Networking hardware



When you type in a web address into your browser....

Say you want to visit nosecurity.blog, how do you get there?

1. DNS
2. Sends HTTP request to server
3. If server approves, will respond with "200"
4. Browser then re-assembles the small chunks into a complete epic website

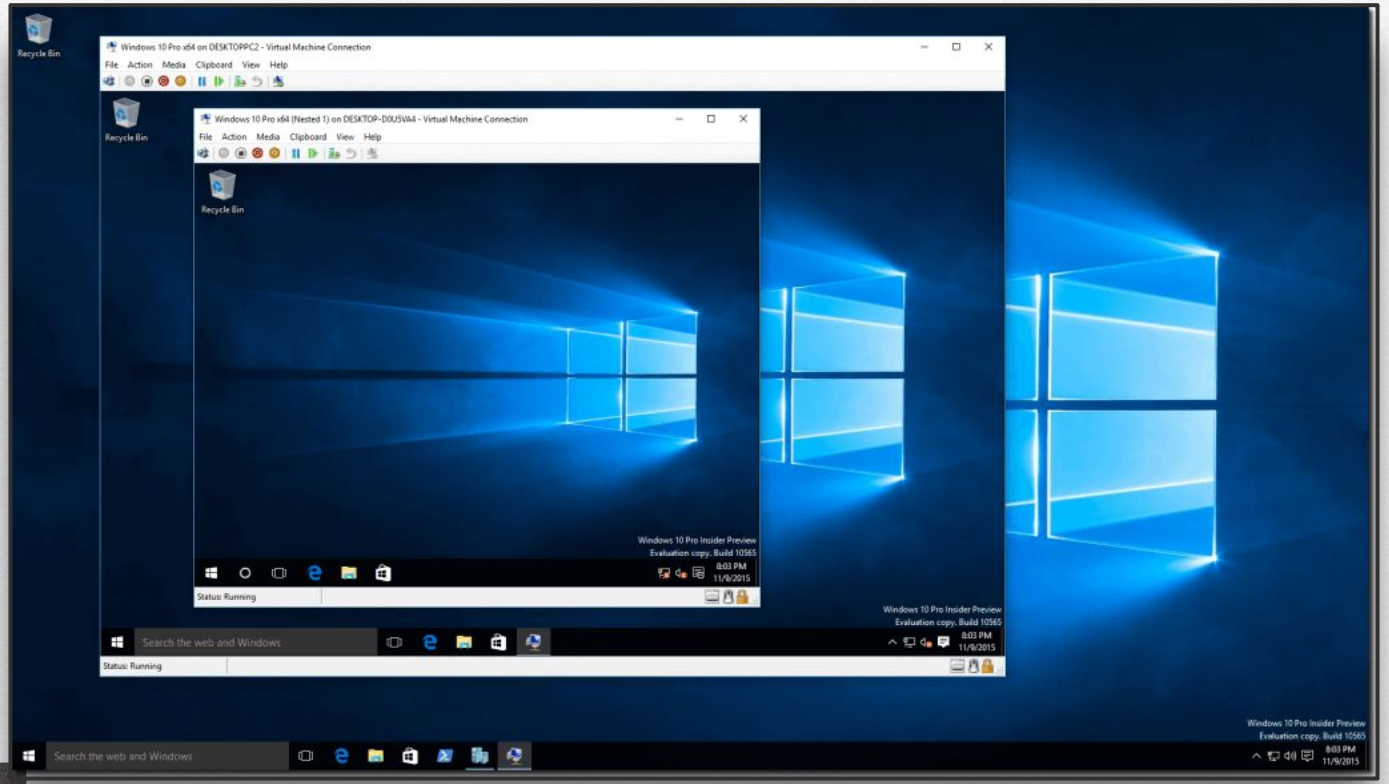


03

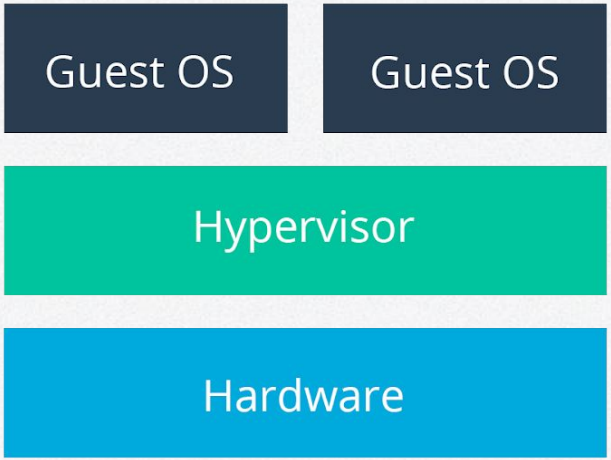
Virtual Machines

What, how, and why?

What is a virtual machine?



Type 1 Virtual Machine Components



Virtual Machine

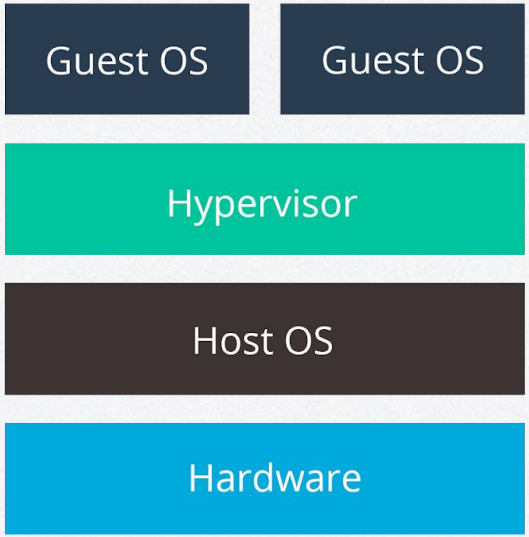
Type 1 Hypervisor

Hardware

Runs directly on physical hardware

Dedicated hardware

Type 2 Virtual Machine Components



Virtual Machine

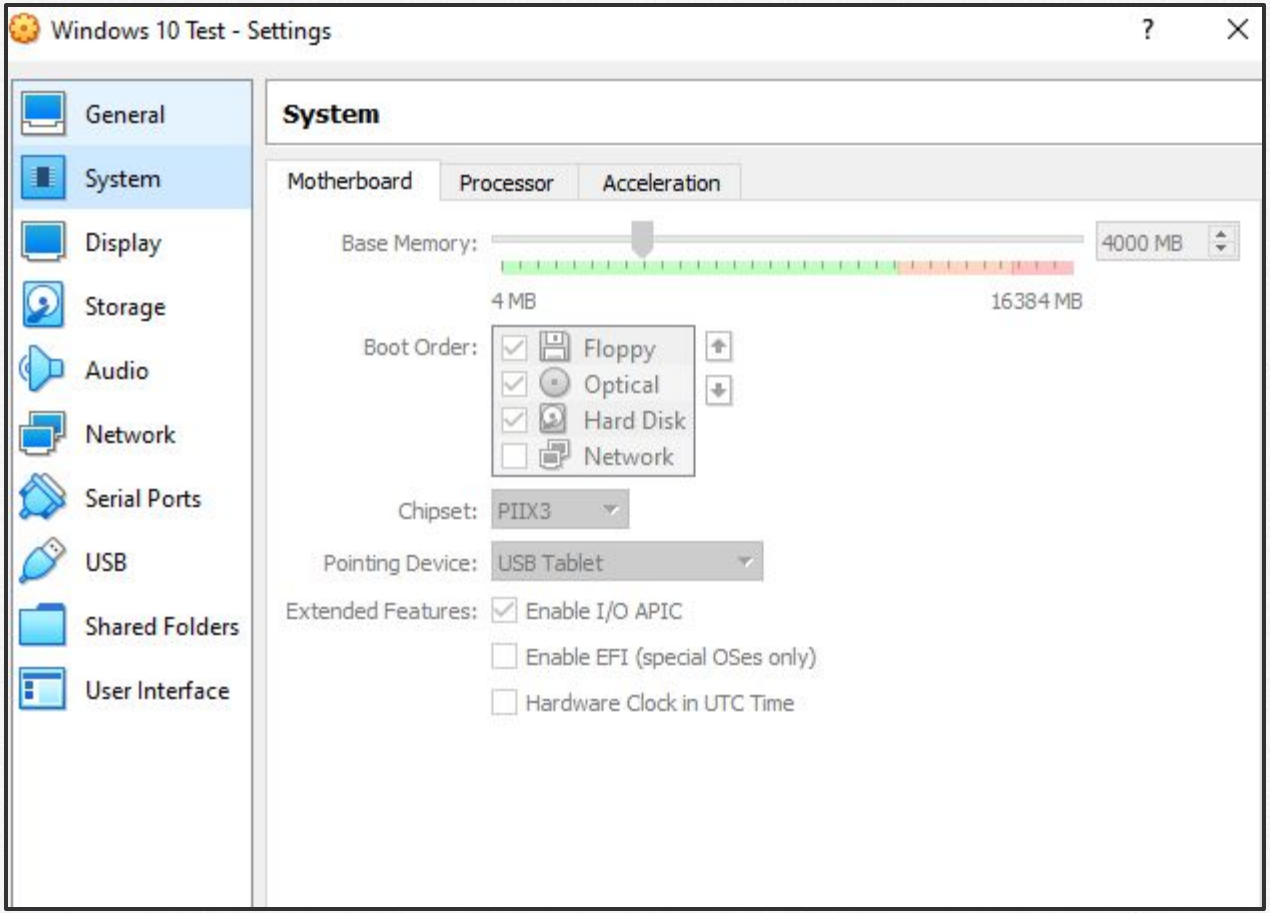
Type 2 Hypervisor

Hardware

Runs on top of the Host OS

How to VM

- Type 2 Hypervisor (VMware or Virtualbox)
- Virtual machine iso
- Create VM, make sure you load iso in
    - Allocate resources
        - At least 4GB of RAM and 40GB of storage for Windows
        - At least 1GB of RAM and 10GB of storage for Linux


Windows 10 Test - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
System
Motherboard
Processor
Acceleration
Base Memory:
4000 MB
4 MB
16384 MB
Boot Order:
Floppy
Optical
Hard Disk
Network
Chipset:
PIIX3
Pointing Device:
USB Tablet
Extended Features:
Enable I/O APIC
Enable EFI (special OSes only)
Hardware Clock in UTC Time

Why VMs?

Computer inside a computer

Lab Environments

Outdated Software

Hardware Efficiency

Run Different OSs

Application Testing

Before we move on...

If you would like to have more practice!

Windows 10 ISO

https://da.gd/g0MwDe

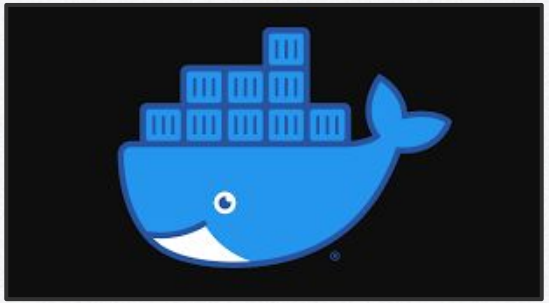
Ubuntu 20.04 ISO

https://da.gd/Y0NFX

04

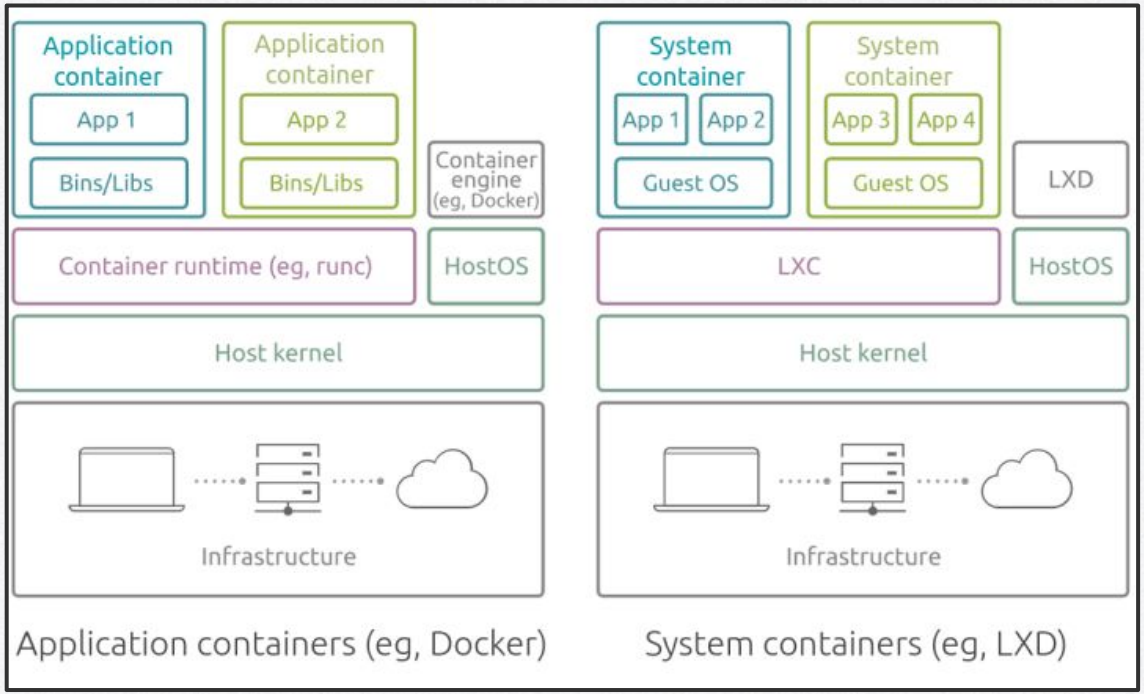
Containers

Contain your services



What are containers

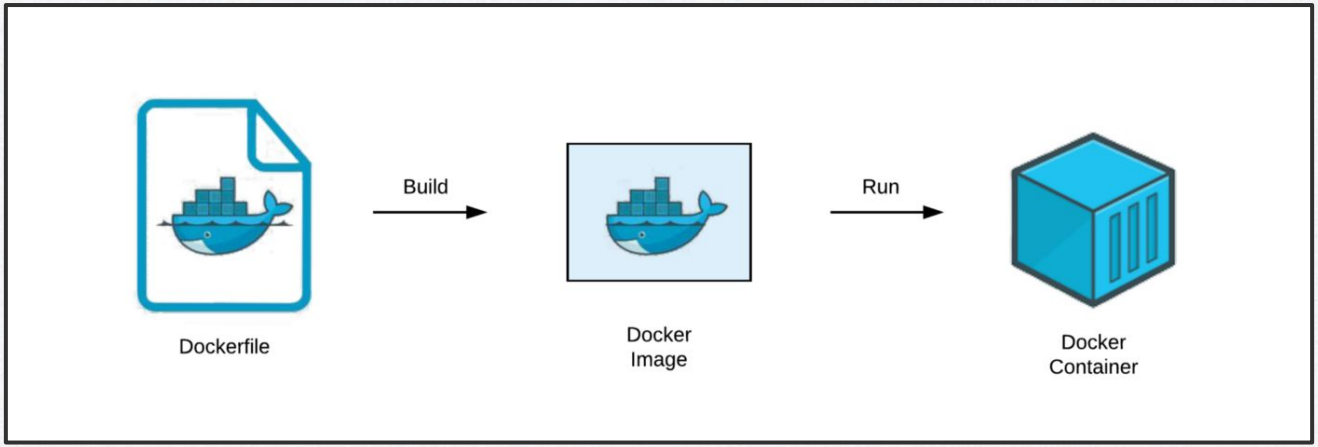
- System Containers
  - Operating System, long lasting, multiple applications
- Application Containers
  - Bare minimum for running a single service



Why Containers?

Dockerfiles => Easy to create images

Docker-compose => Easy to run image as containers



05

Blooket

Blooket

Blooket

06

Lab Time.

Learn by doing.

Lab Instructions

Make sure vpn first (https://da.gd/ccdcvpn) ⇒ https://elsa.sdc.cpp

- Log into Vsphere and find your resource pool
- Create a new user account on both VMs
- Windows 10
  - Set up a firewall
  - Set up a secure password policy
  - Promote the user you created to Administrator level privilege
  - Change your ip address and dns server
- Ubuntu 20.04
  - Set up a firewall
  - Set up an Nginx web server
  - Set a static IP address
  - Create a text file with the following text: "Hello World!", and use one of the following text editors: nano, vim or gedit.
  - Set up SSH and remotely login with SSH through the Windows 10 machine.

Takeaways

- Hopefully you learned about:
  - Windows 10
    - lusrmgr.msc
    - secpol.msc
    - gpedit.msc
  - Ubuntu 20.04
    - Commands
      - cat, ls, cd, apt, chmod, mkdir, mv, cp, netstat, ip a, systemctl, nano, vim, gedit, ssh, ufw

Any questions?

Please ask something I am lonely and in dire need of any form of social interaction