SUMMARY:

This write-up covers the THM Pre-Security path.

https://tryhackme.com/path-action/presecurity/join

Contents

---

1. Network Fundamentals

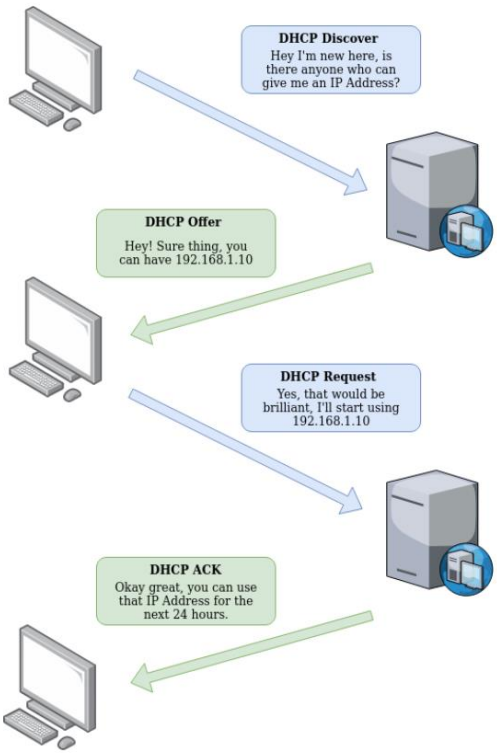
What is networking: https://www.youtube.com/watch?v=42u_2e6eNF4

- Identifying devices on a network:
  - IP Address: Briefly, an IP address (or Internet Protocol) address can be used as a way of identifying a host on a network for a period, where that IP address can then be associated with another device without the IP address changing.
  - MAC Address: Devices on a network will all have a physical network interface, which is a microchip board found on the device's motherboard. This network interface is assigned a unique address at the factory it was built at, called a MAC (Media Access Control) address.
- Ping (ICMP)
  - Ping uses ICMP (Internet Control Message Protocol) packets to determine the performance of a connection between devices, for example, if the connection exists or is reliable.

Intro to LAN: https://www.youtube.com/watch?v=csYtPidvvFQ

- Topologies: ring, bus, star, mesh
- Switches: Switches are dedicated devices within a network that are designed to aggregate multiple other devices such as computers, printers, or any other networking-capable device using ethernet.
- Routers: Switches are dedicated devices within a network that are designed to aggregate multiple other devices such as computers, printers, or any other networking-capable device using ethernet.
- Subnetting: Subnetting is achieved by splitting up the number of hosts that can fit within the network, represented by a number called a subnet mask. Subnets use IP addresses in three different ways:
  - Identify the network address
  - Identify the host address
  - Identify the default gateway
- ARP: A MAC address and an IP address, the ARP protocol, or Address Resolution Protocol for short, is the technology that is responsible for allowing devices to identify themselves on a network. Simply, the ARP protocol allows a device to associate its MAC address with an IP address on the network. Each device on a network will keep a log of the MAC addresses associated with other devices.
- DHCP: IP addresses can be assigned either manually, by entering them physically into a device, or automatically and most commonly by using a DHCP (Dynamic Host Configuration Protocol) server. When a device connects to a network, if it has not already been manually assigned an IP address, it sends out a request (DHCP Discover) to

see if any DHCP servers are on the network. The DHCP server then replies with an IP address the device could use (DHCP Offer). The device then sends a reply confirming it wants the offered IP Address (DHCP Request), and then lastly, the DHCP server sends a reply acknowledging this has been completed, and the device can start using the IP Address (DHCP ACK).



OSI Model: https://www.youtube.com/watch?v=hWIktHvNjeM

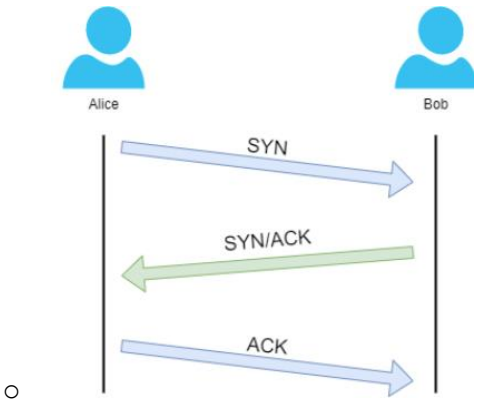
- Layer 7 – Application layer: The application layer of the OSI model is the layer that you will be most familiar with. This familiarity is because the application layer is the layer in which protocols and rules are in place to determine how the user should interact with data sent or received.
- Layer 6 – Presentation layer: Layer 6 of the OSI model is the layer in which standardization starts to take place. Because software developers can develop any software such as an email client differently, the data still needs to be handled in the same way — no matter how the software works.
- Layer 5 – Session layer: Once data has been correctly translated or formatted from the presentation layer (layer 6), the session layer (layer 5) will begin to create a connection to the other computer that the data is destined for. When a connection is established, a session is created. Whilst this connection is active, so is the session. The session layer (layer 5) synchronizes the two computers to ensure that they are on the same page before data is sent and received.
- Layer 4 – Transport Layer: Layer 4 of the OSI model plays a vital part in transmitting data across a network and can be a little bit difficult to grasp. When data is sent between devices, it follows one of two different protocols that are decided based upon several factors:
    - TCP
    - UDP
- Layer 3 – Network Layer: The third layer of the OSI model (network layer) is where the magic of routing & re-assembly of data takes place (from these small chunks to the larger chunk). Firstly, routing simply determines the most optimal path in which these chunks of data should be sent. Whilst some protocols at this layer

determine exactly what is the "optimal" path that data should take to reach a device; we should only know about their existence at this stage of the networking module. Briefly, these protocols include OSPF (Open Shortest Path First) and RIP (Routing Information Protocol).

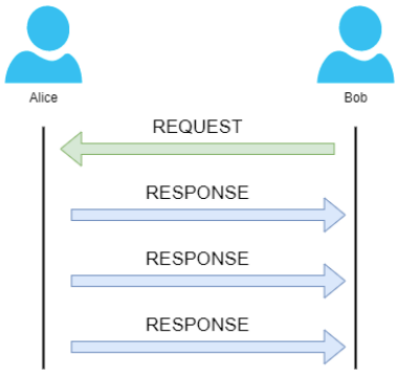
- Layer 2 – Data Link Layer: The data link layer focuses on the physical addressing of the transmission. It receives a packet from the network layer (including the IP address for the remote computer) and adds in the physical MAC (Media Access Control) address of the receiving endpoint. Inside every network-enabled computer is a Network Interface Card (NIC) which comes with a unique MAC address to identify it.
- Layer 1 – Physical Layer: This layer is one of the easiest layers to grasp. Put simply, this layer references the physical components of the hardware used in networking and is the lowest layer that you will find. Devices use electrical signals to transfer data between each other in a binary numbering system (1's and 0's).

Packets and Frames: https://www.youtube.com/watch?v=vzcLrE0SfiQ

- TCP/IP 3-way handshake:



- UDP/IP:



- Ports 101: Any port that is within 0 and 1024 (1,024) is known as a common port. When a connection has been established (recalling from the OSI model's room), any data sent or received by a device will be sent through these ports. In computing, ports are a numerical value between 0 and 65535 (65,535).

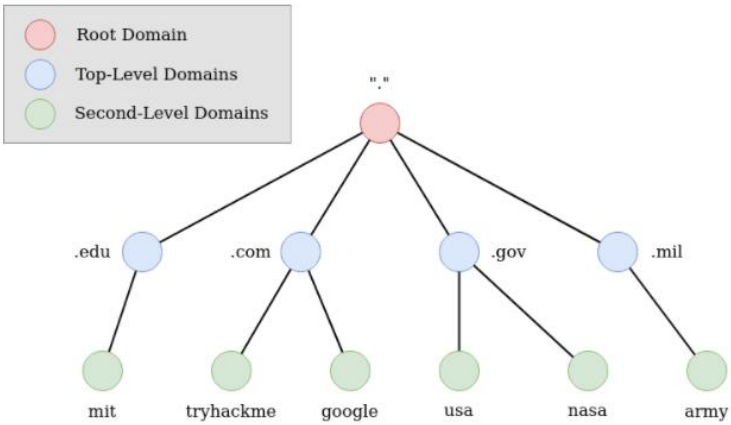
Extending your network: https://www.youtube.com/watch?v=uMkjvpux70I

- Port forwarding: Port forwarding is configured at the router of a network. Port forwarding is an essential component in connecting applications and services to the Internet. Without port forwarding, applications, and services such as web servers are only available to devices within the same direct network.
- Firewalls: A firewall is a device within a network responsible for determining what traffic is allowed to enter and exit. Think of a firewall as border security for a network. An administrator can configure a firewall to permit or deny traffic from entering or exiting a network based on numerous factors such as:

- VPN: A Virtual Private Network (or VPN for short) is a technology that allows devices on separate networks to communicate securely by creating a dedicated path between each other over the Internet (known as a tunnel). Devices connected within this tunnel form their own private network.

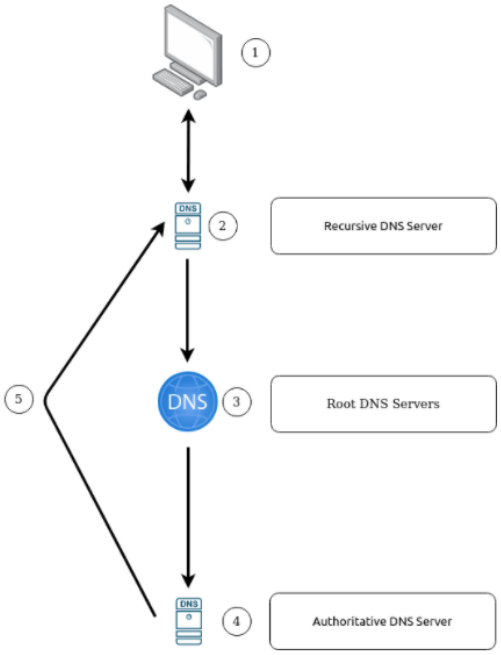
2. How Web Works

DNS: https://www.youtube.com/watch?v=jpTY1S5vs9k

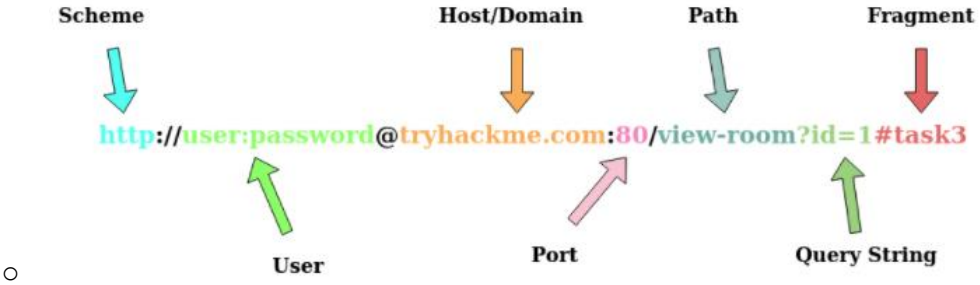
- DNS (Domain Name System) provides a simple way for us to communicate with devices on the internet without remembering complex numbers. Much like every house has a unique address for sending mail directly to it, every computer on the internet has its own unique address to communicate with it called an IP address. An IP address looks like the following 104.26.10.229, 4 sets of digits ranging from 0 - 255 separated by a period. When you want to visit a website, it's not exactly convenient to remember this complicated set of numbers, and that's where DNS can help. So instead of remembering 104.26.10.229, you can remember tryhackme.com instead.
- Domain hierarchy:
  - 

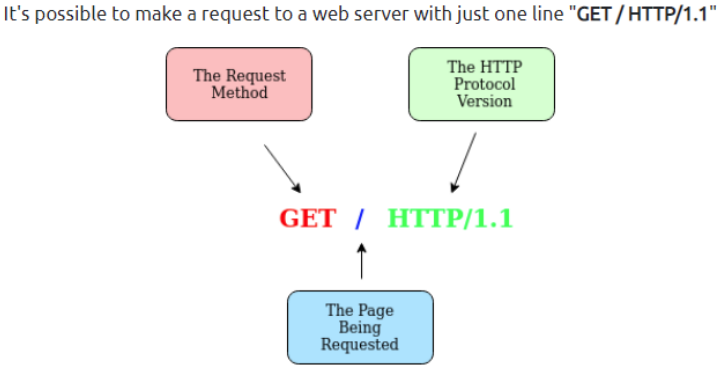
- Record types:
  - A Record
    - These records resolve to IPv4 addresses, for example 104.26.10.229
  - AAAA Record
    - These records resolve to IPv6 addresses, for example 2606:4700:20::681a:be5
  - CNAME Record
    - These records resolve to another domain name, for example, TryHackMe's online shop has the subdomain name store.tryhackme.com which returns a CNAME record shops.shopify.com. Another DNS request would then be made to shops.shopify.com to work out the IP address.
  - MX Record
    - These records resolve to the address of the servers that handle the email for the domain you are querying, for example an MX record response for tryhackme.com would look something like alt1.aspmx.l.google.com. These records also come with a priority flag. This tells the client in which order to try the servers, this is perfect for if the main server goes down and email needs to be sent to a backup server.
  - TXT Record
    - TXT records are free text fields where any text-based data can be stored. TXT records have multiple uses, but some common ones can be to list servers that have the authority to send an email on behalf of the domain (this can help in the battle against spam and spoofed email). They

can also be used to verify ownership of the domain name when signing up for third party services.

- Making a request:
  - 

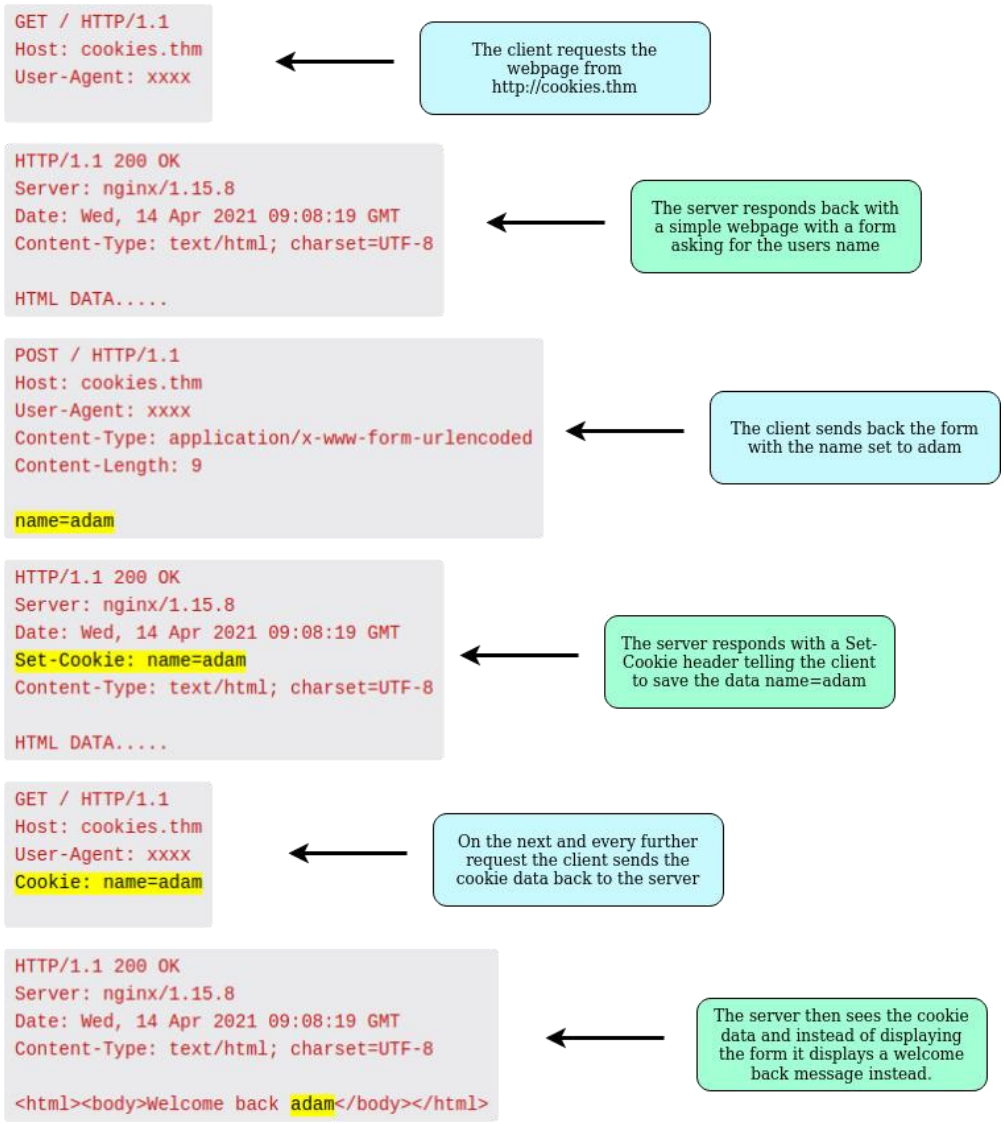
HTTP: https://www.youtube.com/watch?v=XZyapIKV3Rw

- Requests and responses:
  - 

  - 

- HTTP Methods:
  - HTTP methods are a way for the client to show their intended action when making an HTTP request. There are a lot of HTTP methods but we'll cover the most common ones, although mostly you'll deal with the GET and POST method.

  - GET Request: This is used for getting information from a web server.
  - POST Request: This is used for submitting data to the web server and potentially creating new records
  - PUT Request: This is used for submitting data to a web server to update information
  - DELETE Request: This is used for deleting information/records from a web server.
- Status codes: https://developer.mozilla.org/en-US/docs/Web/HTTP/Status
- Headers: Headers are additional bits of data you can send to the web server when making requests. Although no headers are strictly required when making a HTTP request, you'll find it difficult to view a website properly.
- Cookies: You've probably heard of cookies before, they're just a small piece of data that is stored on your computer. Cookies are saved when you receive a "Set-Cookie" header from a web server. Then every further request you make, you'll send the cookie data back to the web server. Because HTTP is stateless (doesn't keep track of your previous requests), cookies can be used to remind the web server who you are, some personal settings for the website or whether you've been to the website before. Let's take a look at this as an example HTTP request:



How websites work: https://www.youtube.com/watch?v=iWoiwFRLV4I

Putting it all together – how the web works: https://www.youtube.com/watch?v=Aa_FAA3v22g

3. Linux Fundamentals

Part 1: https://www.youtube.com/watch?v=kPylihJRG70

- Basic Commands:
  - echo Output any text that we provide
  - whoami Find out what user we're currently logged in as!
  - ls listing
  - cd change directory
  - cat concatenate
  - pwd print working directory
  - man manual
  - –help help flag
  - find -name *.txt find all .txt files
  - grep searches the contents of files for specific values that we are looking for

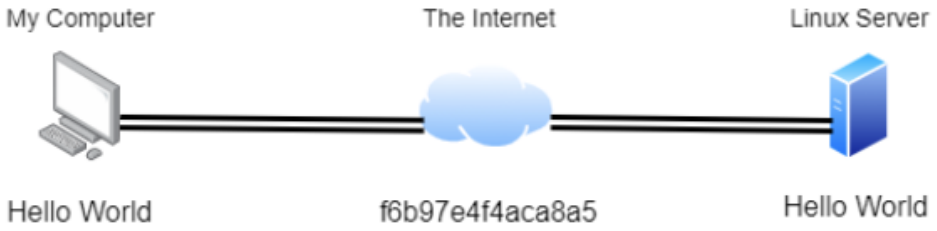
Using "grep" to find any entries with the IP address of "81.143.211.90" in "access.log"

```
tryhackme@linux1:~$ grep "81.143.211.90" access.log
81.143.211.90 - - [25/Mar/2021:11:17 + 0000] "GET / HTTP/1.1" 200 417 "-" "Mozilla/5.0
(Linux; Android 7.0; Moto G(4))"
tryhackme@linux1:~$
```

- Operators
  - & This operator allows you to run commands in the background of your terminal.
  - && This operator allows you to combine multiple commands together in one line of your terminal.
  - > This operator is a redirector - meaning that we can take the output from a command (such as using cat to output a file) and direct it elsewhere.
  - >> This operator does the same function of the > operator but appends the output rather than replacing (meaning nothing is overwritten).

Part 2: https://www.youtube.com/watch?v=7Zt2Mp2IeBI

- SSH: Secure Shell or SSH simply is a protocol between devices in an encrypted form. Using cryptography, any input we send in a human-readable format is encrypted for travelling over a network -- where it is then unencrypted once it reaches the remote machine, such as in the diagram below.



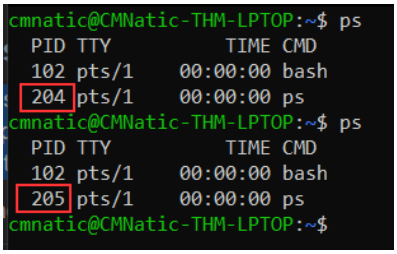
- Using SSH to Login to Your Linux Machine
  - The syntax to use SSH is very simple. We only need to provide two things:
    - 1. The IP address of the remote machine
    - 2. Correct credentials to a valid account to login with on the remote machine

- Flags and Switches: Most commands allow for arguments to be provided. These arguments are identified by a hyphen and a certain keyword known as flags or switches.
- Filesystem interaction continued
    - Command Full Name Purpose
    - touch touch Create file
    - mkdir make directory Create a folder
    - cp copy Copy a file or folder
    - mv move Move a file or folder
    - rm remove Remove a file or folder
    - file file Determine the type of a file
- Permissions
    - ls -l check permissions
    - Switching between users on a Linux install is easy work thanks to the su command. Unless you are the root user (or using root permissions through sudo), then you are required to know two things to facilitate this transition of user accounts:
        - The user we wish to switch to
        - The user's password
    - The su command takes a couple of switches that may be of relevance to you. For example, executing a command once you log in or specifying a specific shell to use. I encourage you to read the man page for su to find out more. However, I will cover the -l or --login switch.
- Common directories
    - /etc : The etc folder (short for etcetera) is a commonplace location to store system files that are used by your operating system.
    - /var : This folder stores data that is frequently accessed or written by services or applications running on the system. For example, log files from running services and applications are written here (/var/log), or other data that is not necessarily associated with a specific user (i.e., databases and the like).
    - /root : There isn't anything more to this folder other than just understanding that this is the home directory for the "root" user.
    - /tmp : This is a unique root directory found on a Linux install. Short for "temporary", the /tmp directory is volatile and is used to store data that is only needed to be accessed once or twice. Similar to the memory on your computer, once the computer is restarted, the contents of this folder are cleared out.

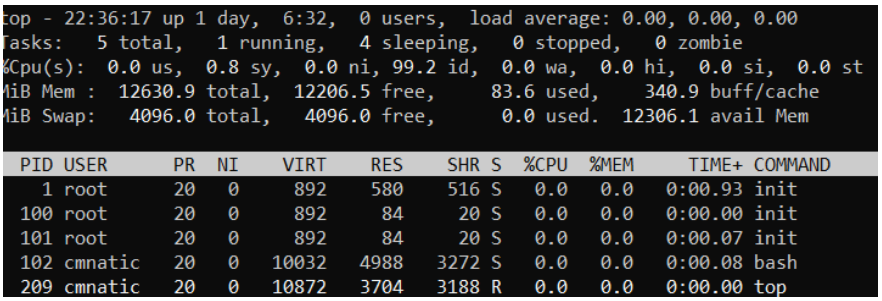
Part 3: https://www.youtube.com/watch?v=bwgaZCb2ft8

- Terminal text editors: nano, vim
- General/useful utilities:
    - wget allows us to download files from the web via HTTP -- as if you were accessing the file in your browser.
    - Scp
        - Secure copy, or SCP, is just that -- a means of securely copying files. Unlike the regular cp command, this command allows you to transfer files between two computers using the SSH protocol to provide both authentication and encryption.
        - Working on a model of SOURCE and DESTINATION, SCP allows you to:
            - Copy files & directories from your current system to a remote system
            - Copy files & directories from a remote system to your current system

- Processes We can use the friendly ps command to provide a list of the running processes as our user's session and some additional information such as its status code, the session that is running it, how much usage time of the CPU it is using, and the name of the actual program or command that is being executed:



- Another very useful command is the top command; top gives you real-time statistics about the processes running on your system instead of a one-time view. These statistics will refresh every 10 seconds, but will also refresh when you use the arrow keys to browse the various rows. Another great command to gain insight into your system is via the top command



- Managing Processes
  - You can send signals that terminate processes; there are a variety of types of signals that correlate to exactly how "cleanly" the process is dealt with by the kernel. To kill a command, we can use the appropriately named kill command and the associated PID that we wish to kill. i.e., to kill PID 1337, we'd use kill 1337.
  - Below are some of the signals that we can send to a process when it is killed:
    - SIGTERM - Kill the process, but allow it to do some cleanup tasks beforehand
    - SIGKILL - Kill the process - doesn't do any cleanup after the fact
    - SIGSTOP - Stop/suspend a process
  - systemctl -- this command allows us to interact with the systemd process/daemon. Continuing on with our example, systemctl is an easy to use command that takes the following formatting: systemctl [option] [service]
    - For example, to tell apache to start up, we'll use systemctl start apache2. Seems simple enough, right? Same with if we wanted to stop apache, we'd just replace the [option] with stop (instead of start like we provided)
    - We can do four options with systemctl:
      - Start
      - Stop
      - Enable
      - Disable
- Cron: Users may want to schedule a certain action or task to take place after the system has booted. Take, for example, running commands, backing up files, or launching your favourite programs on, such as Spotify or

Google Chrome. We're going to be talking about the cron process, but more specifically, how we can interact with it via the use of crontabs. Crontab is one of the processes that is started during boot, which is responsible for facilitating and managing cron jobs.

- Let's use the example of backing up files. You may wish to backup "cmnatic"'s "Documents" every 12 hours. We would use the following formatting:
  - 0 *12 * * * cp -R /home/cmnatic/Documents /var/backups/
- An interesting feature of crontabs is that these also support the wildcard or asterisk (*). If we do not wish to provide a value for that specific field, i.e. we don't care what month, day, or year it is executed -- only that it is executed every 12 hours, we simply just place an asterisk.
- This can be confusing to begin with, which is why there are some great resources such as the online "Crontab Generator" that allows you to use a friendly application to generate your formatting for you! As well as the site "Cron Guru"!
- Crontabs can be edited by using crontab -e, where you can select an editor (such as Nano) to edit your crontab.

- Package management
  - apt
  - dpkg

4. Windows Fundamentals

- The file system used in modern versions of Windows is the New Technology File System or simply NTFS.
  - Before NTFS, there was FAT16/FAT32 (File Allocation Table) and HPFS (High Performance File System).
- The Windows folder (C:\Windows) is traditionally known as the folder which contains the Windows operating system.
  - The folder doesn't have to reside in the C drive necessarily. It can reside in any other drive and technically can reside in a different folder.
  - This is where environment variables, more specifically system environment variables, come into play. Even though not discussed yet, the system environment variable for the Windows directory is %windir%.
  - The System32 folder holds the important files that are critical for the operating system.
    - You should proceed with extreme caution when interacting with this folder. Accidentally deleting any files or folders within System32 can render the Windows OS inoperational.
- User accounts can be one of two types on a typical local Windows system: Administrator & Standard User. The user account type will determine what actions the user can perform on that specific Windows system.
  - An Administrator can make changes to the system: add users, delete users, modify groups, modify settings on the system, etc.
  - A Standard User can only make changes to folders/files attributed to the user & can't perform system-level changes, such as install programs.
- User account control: When a user with an account type of administrator logs into a system, the current session doesn't run with elevated permissions. When an operation requiring higher-level privileges needs to execute, the user will be prompted to confirm if they permit the operation to run.
- The System Configuration utility (MSConfig) is for advanced troubleshooting, and its main purpose is to help diagnose startup issues.
- What is the System Information (msinfo32) tool?

  - Per Microsoft, "Windows includes a tool called Microsoft System Information (Msinfo32.exe). This tool gathers information about your computer and displays a comprehensive view of your hardware, system components, and software environment, which you can use to diagnose computer issues."
  - The information in System Summary is divided into three sections:
    - Hardware Resources
    - Components
    - Software Environment
- What is Resource Monitor (resmon)?
  - Per Microsoft, "Resource Monitor displays per-process and aggregate CPU, memory, disk, and network usage information, in addition to providing details about which processes are using individual file handles and modules. Advanced filtering allows users to isolate the data related to one or more processes (either applications or services), start, stop, pause, and resume services, and close unresponsive applications from the user interface. It also includes a process analysis feature that can help identify deadlocked processes and file locking conflicts so that the user can attempt to resolve the conflict instead of closing an application and potentially losing data."
  - As some of the other tools mentioned in this room, this utility is geared primarily to advanced users who need to perform advanced troubleshooting on the computer system.
  - In the Overview tab, Resmon has four sections:
    - CPU
    - Disk
    - Network
    - Memory
- The Windows Registry (per Microsoft) is a central hierarchical database used to store information necessary to configure the system for one or more users, applications, and hardware devices.
  - The registry contains information that Windows continually references during operation, such as:
    - Profiles for each user
    - Applications installed on the computer and the types of documents that each can create
    - Property sheet settings for folders and application icons
    - What hardware exists on the system
    - The ports that are being used.
  - Warning: The registry is for advanced computer users. Making changes to the registry can affect normal computer operations.
  - There are various ways to view/edit the registry. One way is to use the Registry Editor (regedit).