

Cyber@UC Meeting 39

Guest Speaker Dr. Williams
CEH Networking

If You're New!

- Join our Slack **ucyber.slack.com**
- Feel free to get involved with one of our committees: **Content, Finance, Public Affairs, Outreach, Recruitment**
- **Ongoing Projects:**
 - Malware Sandboxing Lab
 - Cyber Range
 - RAPIDS Cyber Op Center



Announcements

- **Dr. Williams Visiting**
- We're planning **school visits**, reach out!
- Logo designs welcome!
- **Board Game Night!!! February 2nd**, next Friday





Public Affairs

- Please fill out Google form for **GroupMe** Numbers!
<https://goo.gl/forms/94i9kMJgtpDGXsC22>
- Our brand new **YouTube** channel has just been made. We will be live streaming meetings, events, etc and posting relevant videos to the channel. Please subscribe!
youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Follow us on our social media:

Facebook: <facebook.com/CyberAtUC/>

Twitter: <twitter.com/UCyb3r>

Instagram: <instagram.com/cyberatuc/>


Website: <gauss.ececs.uc.edu/UC.yber/>

Weekly Content

APT Review Dark Caracal

- They have been operating since at least 2012
 - Recently revealed by an exposed server on the open internet
 - Focused around mobile phones instead of computers as a large-scale hacking group, one of the first of their kind
 - Thousands of victims in over 21 countries
 - Traced back to a building owned by the Lebanese General Directorate of General Security (GDGS), one of the Lebanese intelligence agencies
 - Targeted governments, military personnel, utilities, financial institutions, manufacturers, defense contractors, medical professionals, educators, academics, etc.
- 

Dark Caracal (Continued)

- 4 personas within the group have been found through the leaked information and individuals believed to be matched with those personas have been identified.
 - Conduct cyber attack campaigns across multiple platforms: Android, Windows, Mac, and Linux on targets in NA, EU Middle East, and Asia.
 - Stolen documents, call records, text messages, audio recordings, browsing history, contacts, photos, location data.
 - Relied on Social Engineering and non zero-day exploits through Facebook and WhatsApp messaging.
- 

Dark Caracal (continued)

- After visiting malicious sites, victims were served fake updates to secure apps, like WhatsApp which would eventually download the Dark Caracal malware called Pallas onto the mobile device.
- Pallas is capable of stealing most of the information on your phone, like two-factor authentication codes, texts, etc.
- Pallas relies on permission granted at installation to access data.
- Dark Caracal also makes use of FinFisher and CrossRAT.
- Overall Dark Caracal has stolen over 252,000 contacts, 485,000 texts, and 150,000 call records from android devices alone.
 - Sensitive data like bank information has also been stolen.



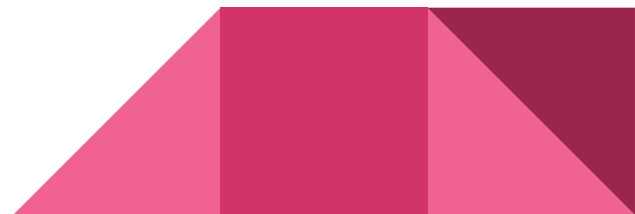
Dark Caracal Sources

<https://thehackernews.com/2018/01/dark-caracal-android-malware.html>

https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

<https://blog.lookout.com/dark-caracal-mobile-apt>

<https://en.wikipedia.org/wiki/FinFisher>





Guest Speaker:
Dr. Williams

Part 2: Systems Overview

My cat might have to have his one remaining
tooth removed.





Differences from last week

Based on everyone's feedback and input:

- More Color
- More Graphics
- More Content

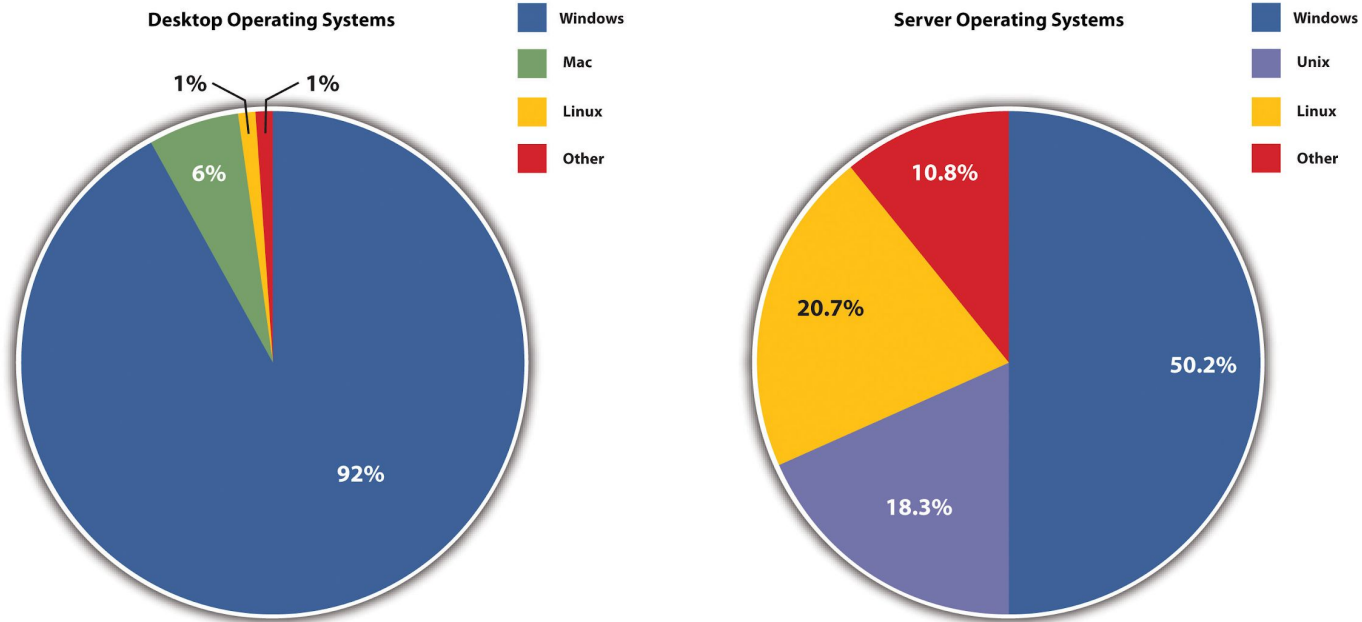
And as promised:

- Things you can do to follow along
- This week will be more technical

The Topics Today Go Something Exactly Like This

- **Single Systems**
 - Common OS Arch-Types
- **Small Networks**
 - Data Bus
 - IPv4, MAC, & Ports
 - TCP and UDP
 - NAT and DHCP
 - FireWalls
- **Large Networks**
 - Switches and Hubs
 - Intrusion Detection Systems
 - IPv4 & IPv6
 - VPN
- **Inter-Networks**
 - DNS & ICANN

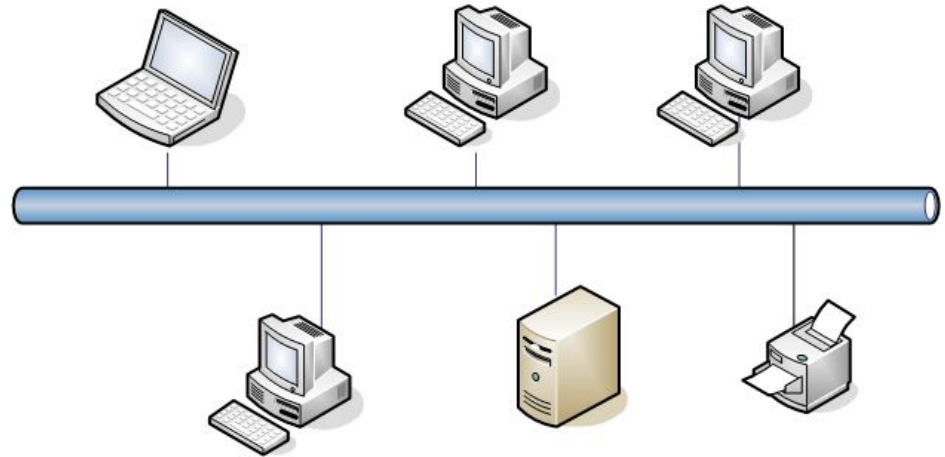
We have a single system, but what is on it?



We have a handful of systems, how do we connect them?

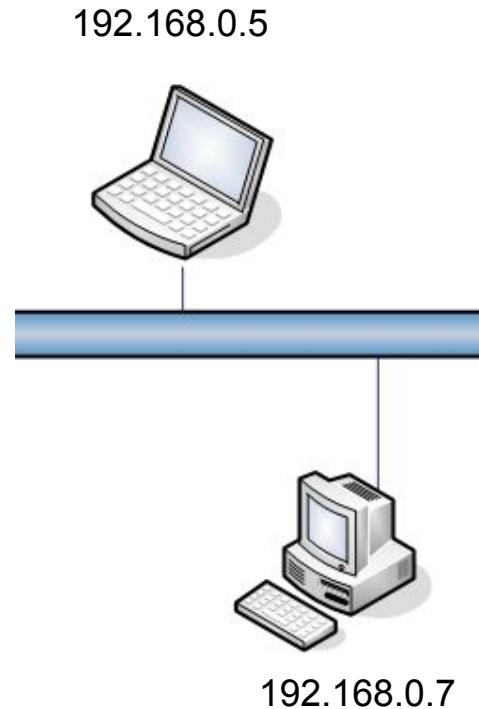
- At a high level, we just connect all of the devices on one network
- For this abstract purpose, assume we can connect clients, servers, and peripherals directly to the same network

BUS Topology



How do we tell these individual devices apart?

- Follow along with:
 - **ipconfig /a** for Windows
 - **ifconfig** for Linux and Mac
- We can give each device a **physical address (MAC)** which is integrated into the device's network connector
- We can give each device a **network-specific address (IP)** which is given to the device when it connects to the network
- Typically applications that access the network will use IP address to connections





More on IPv4

- Most of the world uses IPv4
- IPv4 is starting to be replaced by IPv6 which allows larger networks
- The first three octets make the **network address**, which details the network the host is connected to
- The fourth number is the **host address**, which is the individual device identifier on the network
- You can think of an IPv4 address as being similar to a house number and street address.
- You can request an new IP from a network if you don't want to use the one you were assigned

192.168.0.1
2716 Jefferson



More on MAC

- The MAC address is assigned to the network card when it is manufactured
- MAC addresses identify both the **manufacturer of the interface** and the **interface** itself
- Because the MAC is tied to the network through software, it is quite trivial to change your MAC address through a tool such as **macchanger**
- MAC addresses could once be used to track devices but most modern devices will randomize their MAC when joining a new network to prevent this

ff:ff:ff:aa:aa:aa



Ports

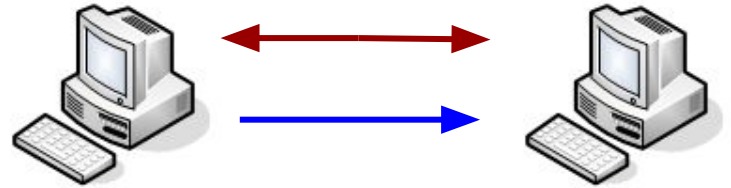
- To tell apart data that is sent to specific programs on the computer we use ports
- Ports are numbered on the range 1-65535 but typically only the lower 800 are used for most applications
- Web servers use port 80 as a standard HTTP port
- Applications are not explicitly bound to a certain port, it's just common practice to use certain ports with certain applications

Port	Protocol	Application
20	TCP	FTP Data
21	TCP	FTP control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	Both	DNS
67,68	UDP	DHCP
80	TCP	HTTP
443	TCP	SSL

How do we send data between systems?

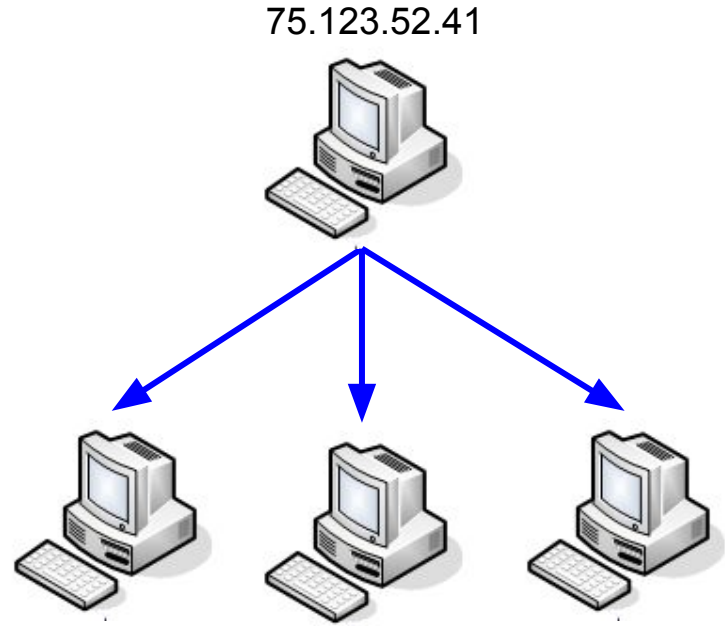
- Transport Control Protocol (TCP)

- Two systems establish a connection stream, then end the connection when data is transferred.
 - Involves a 3 way handshake followed by a finish packet. SYN, SYN-ACK, ACK
 - Provides error correction
 - Typically used for sending large amounts of data and verifying the reception of data.
- User Datagram Protocol (UDP)
- No connection is established.
 - Requires no handshake.
 - Provides no error correction.
 - Typically used for small, one way data transmission or one to many (multicast) transmissions.



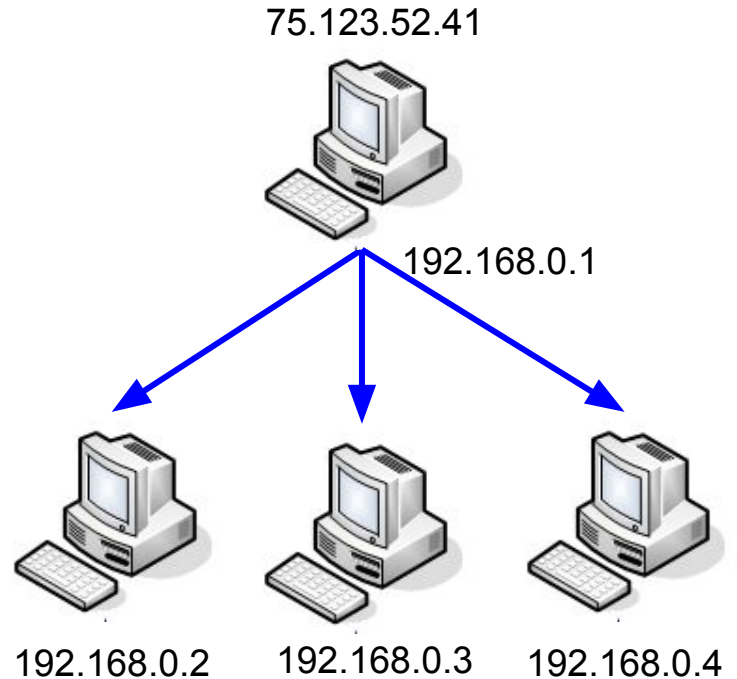
Network Address Translation (NAT)

- We would run out of IPv4 addresses very quickly if every device was given a unique NAT identifier.
- Instead, typically your home router is assigned a public IP and then gives the devices behind it internal IP addresses via DHCP
- The outside world will see your routers IP



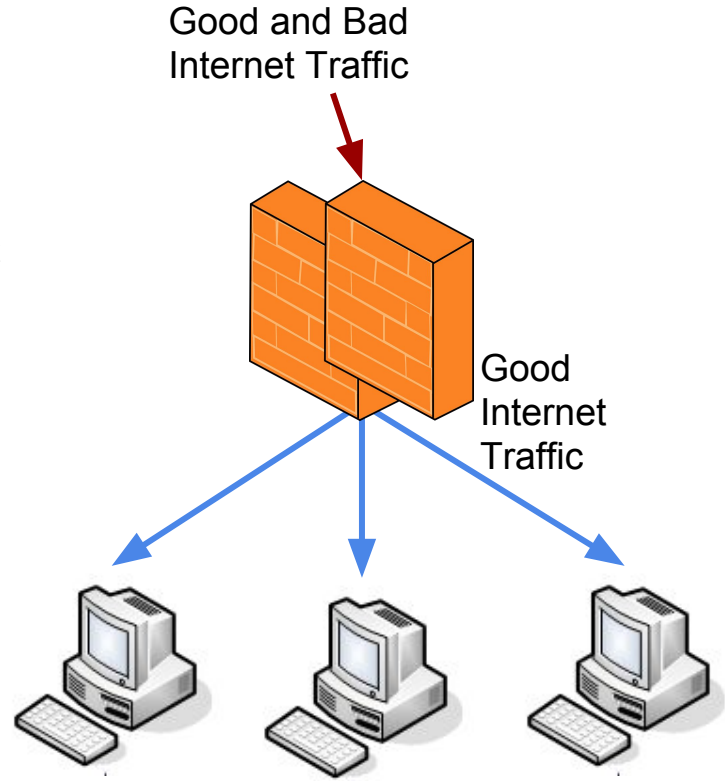
Dynamic host Configuration Protocol (DHCP)

- Because you need an IP address to talk to other computers your router can assign internal network IP's.
- Typically this IP range starts at 192.168.0.1 with the router and counts up. Another common IP range would be 10.##.#.1 etc.
- You can also request a specific network address from the router.



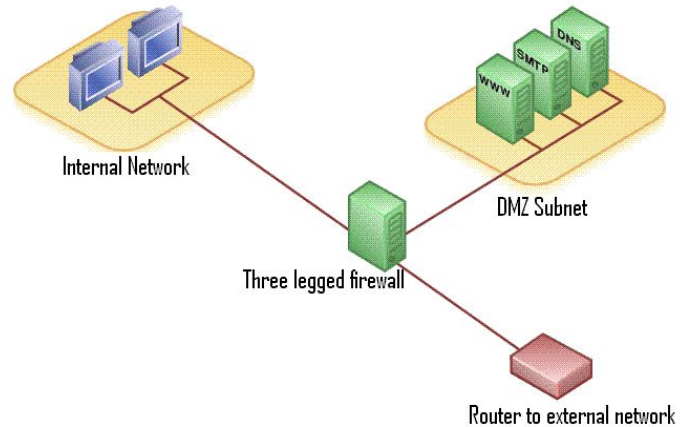
Fire Walls

- Most routers also have a firewall built in, just not a good one.
- Firewalls are supposed to let good things through and keep bad things out.
- They are typically passive systems that follow simple allow/disallow rules that correspond to certain ports.
- Example: allow TCP over port 80 (http).



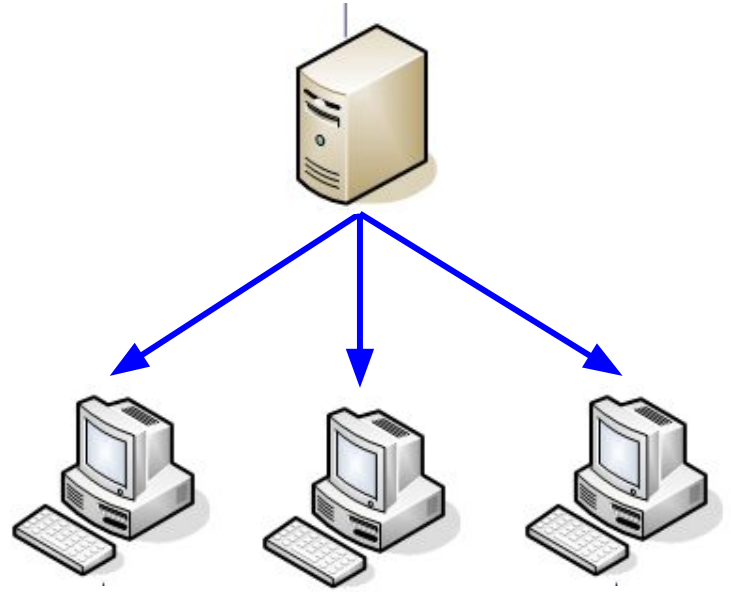
Large Networks

- Large networks such as major business require multiple layers of security
- Large networks may include several smaller networks for different purposes
- You may have a full access network, a restricted development network, and an air gapped internal only network all in one building
- Large networks will start to use more advanced hardware that home networks typically won't need.



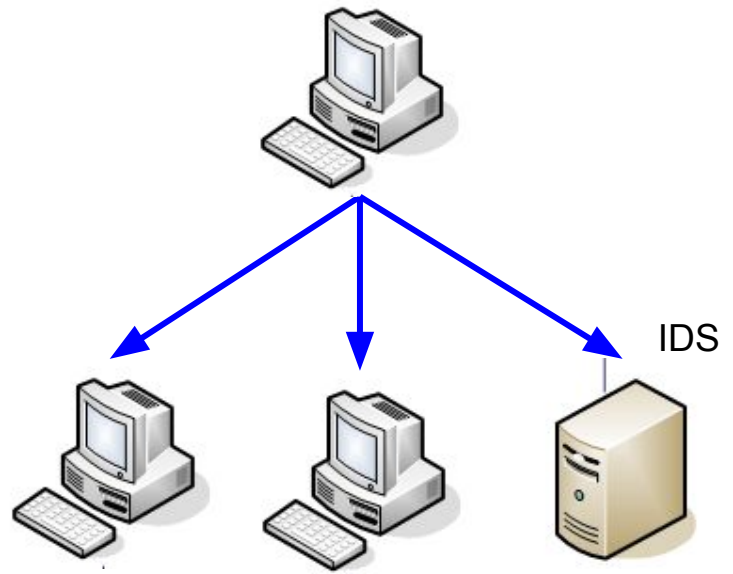
Switches and Hubs

- Switches and hubs are simple ways of extending network access physically
- **Switches** will send network traffic only to the **intended receiver**
- **Hubs** will send network traffic to **all receivers**



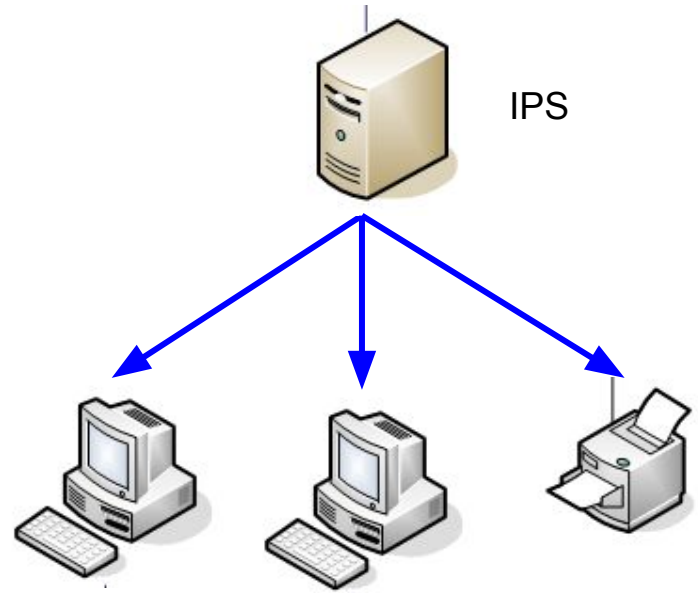
Intrusion Detection Systems (IDS)

- Intrusion Detection Systems will monitor traffic on a network and look for things that look malicious and report the event
- A field of research for IDS's is implementing machine learning to detect malicious patterns.



Intrusion Prevention Systems (IPS)

- Intrusion Prevention Systems will monitor traffic on a network and function as a dynamic firewall.
- IPS's are active when compared to passive firewalls.
- IPS's are inline just as a firewall are..
- Unlike intrusion DETECTION systems, Intrusion PREVENTION systems will cut off access/quarantine hosts that show malicious activity.





IPv6

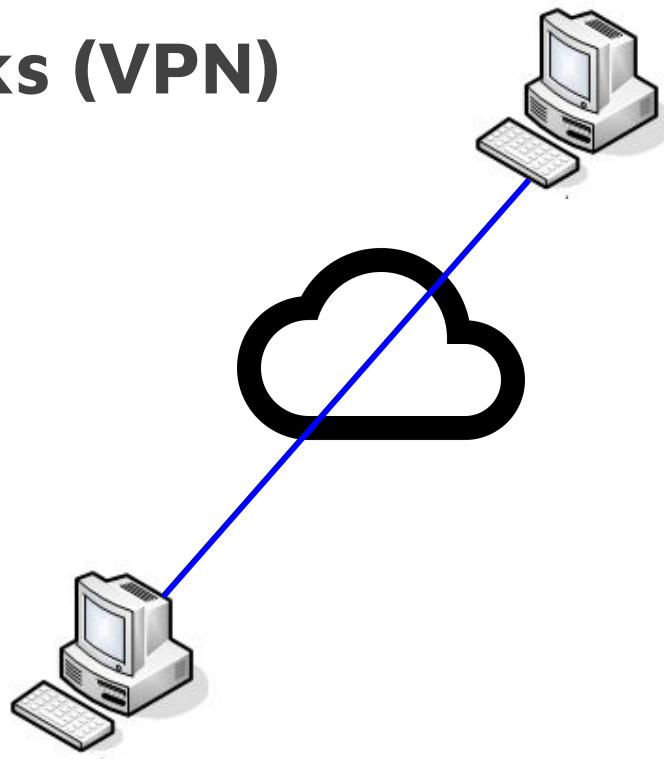
- IPv6 is meant to replace IPv4 in the future
- IPv6 uses hexadecimal to distinguish from IPv4
- IPv4 addresses are only 32 bits long whereas
- IPv6 addresses are 128 bits long

2001:0db8:85a3:0000:0000:8a2e:0370:7334

4563 West Street

Virtual Private Networks (VPN)

- VPN's are a way of allowing two or more systems to act as if they are on the same local area network over the internet
- VPN's can be used for users to remotely connect into work site services
- UC provides a VPN for faculty and students
- We used OpenVPN to connect with Franco's class for the red team operation





Domain Name Servers (DNS)

- You can identify a website as an IP or domain name.
- DNS allows a domain to link to an address.
- DNS records are kept on DNS servers.
- DNS records can be thought of like a phone book for the internet.

DNS Name -> IP Address
www.google.com -> 172.217.2.36



Sample Questions

- Here are a few questions you may see on the CEH exam.



1. What device acts as an intermediary between an internal client and a web resource?

- A. Router
- B. PBX
- C. VTC
- D. Proxy



2. What is the proper sequence of the TCP three-way handshake?

- A. SYN-ACK, ACK, ACK
- B. SYN, SYN-ACK, ACK
- C. SYN-SYN, SYN-ACK, SYN
- D. ACK, SYN-ACK, SYN



3. A scan of a network shows that port 23 is open; what protocol is this aligned with?

- A. Telnet
- B. NetBIOS
- C. SSH
- D. SMTP



4. Which technology allows the use of a single public address to support many internal clients?

- A. VPN
- B. Tunneling
- C. NTP
- D. NAT



5. Which of these protocols is a connection-oriented protocol?

- A. FTP
- B. UDP
- C. POP3
- D. TCP