Cyber@UC Meeting 40

CEH Networking

If You're New!

- Join our Slack **ucyber.slack.com**
- **SIGN IN!**
- 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 Visited** last week
- We're planning **school visits,** reach out!
- Logo designs welcome!
- **Board Game/Game Night**!!! **February 2nd**, Friday at 6pm
- **Dodgeball Team**

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

Git with Github, great but not perfect...

- Source Repositories, good for development
- Limited by the tools and security to interact with

- PS. Demo will not be perfect...

Git exploit with Escape Sequences...caveat….

- Command-line only
- Possibly only a certain version of Linux/terminal affected
- Demo will be using github.uc.edu, not github.com
- Article posted on 2017/December/13
- Reportedly posted to git's security mailing list

- Article Link :
  https://www.twistlock.com/2017/12/13/hiding-content-git-escape-sequence-twistlock-labs-experiment/
- Github-Article-Link : https://github.com/twistlock/gitPocDiff

Start Demo

- Also, don't do any of this
- Just poc, not meant to create Mr. Robot

If !Demo, goto link

Link to Article:
https://www.twistlock.com/2017/12/13/hiding-content-git-escape-sequence-twistlock-labs-experiment/

CrossRAT

- Remember Dark Caracal?
- When going through what was found, a new cross platform malware called CrossRAT 0.1was found, believed to be developed by or for Dark Caracal
- Dark Caracal doesn't use zero days
- Written in Java, making it easy to reverse engineer
- Only 2/58 popular AVs can detect CrossRAT
- Persistent surveillance, key logger
- Advise to install behaviour-based threat detection software
- Article includes a method to check for infection

https://thehackernews.com/2018/01/crossrat-malware.html

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:
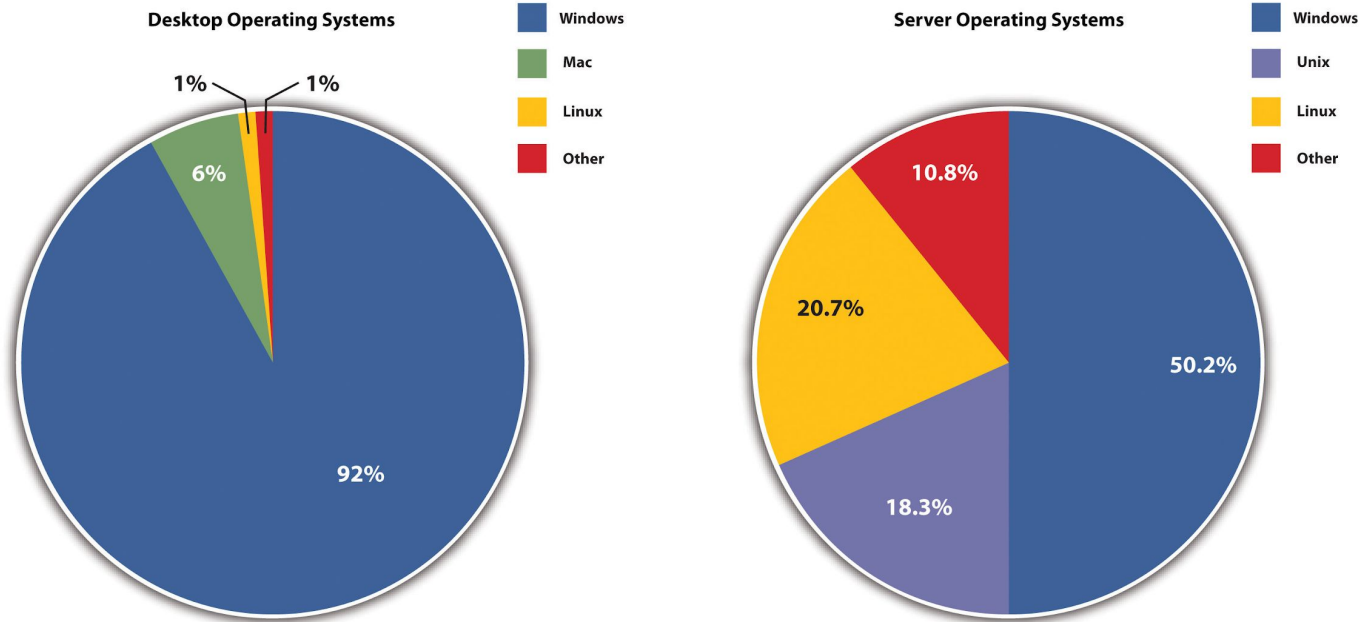
- More Color
- More Graphics
- More Content

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?

Desktop Operating Systems

- Windows
- Mac
- Linux
- Other

1%
1%
6%
92%

Server Operating Systems

- Windows
- Unix
- Linux
- Other

10.8%
20.7%
50.2%
18.3%

# 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
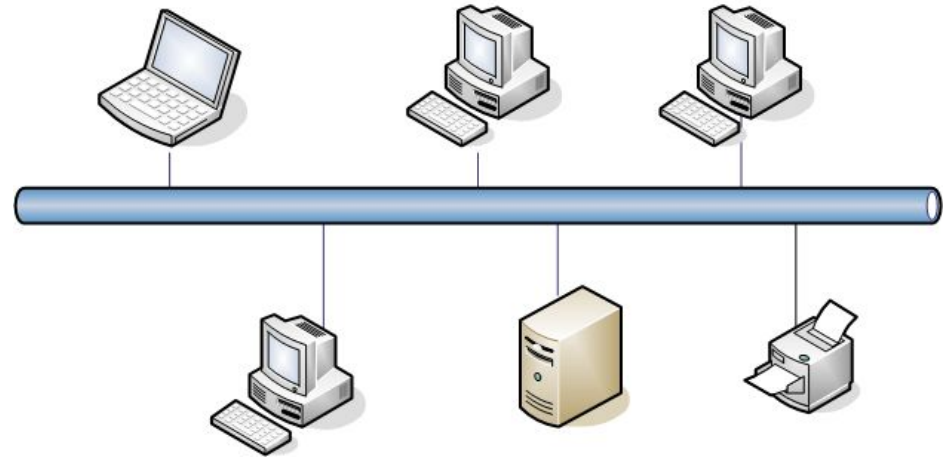
How do we tell these individual devices apart?

192.168.0.5

- 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

192.168.0.7
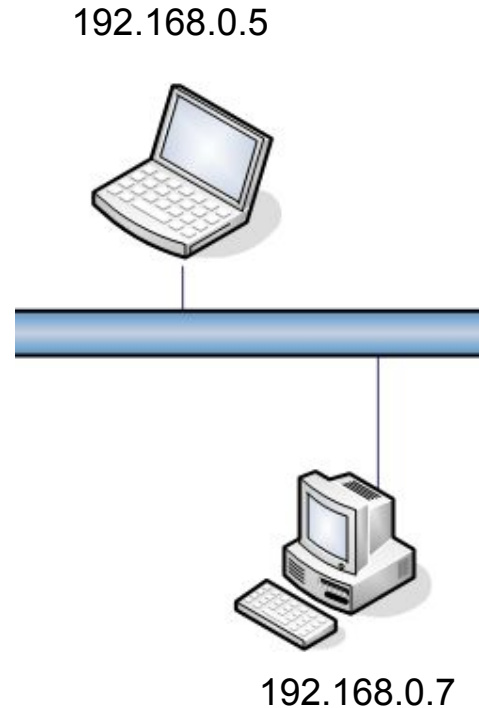
More on IPv4

- 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 octet 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 IP from a network if you don't want to use the one you were assigned

192.168.0.1
2716 Jefferson

IP's in Cyber Security

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 told 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
    - Involves a 3 way handshake followed by a finish packet (SYN, ACK, SYN)
    - 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
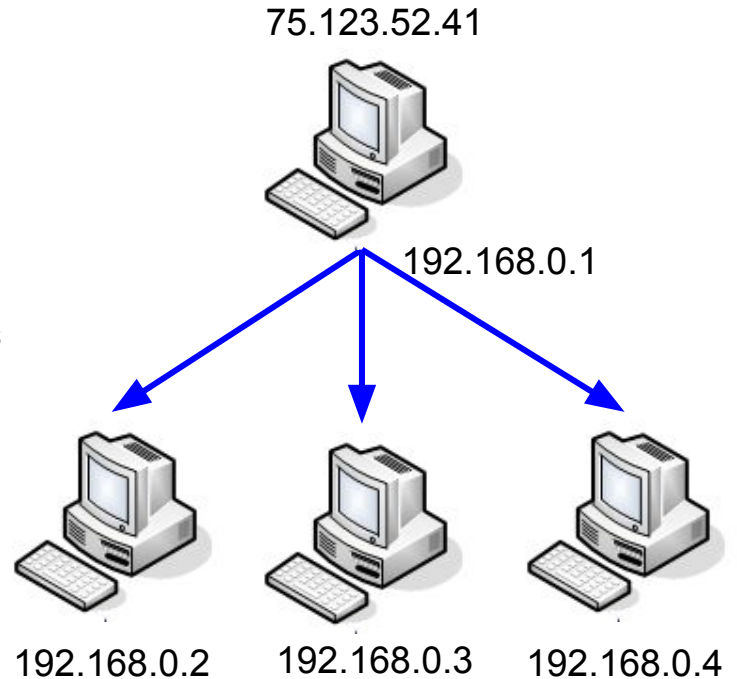   - Typically used for small, one way data transmission or one to many (multicast)transmissions
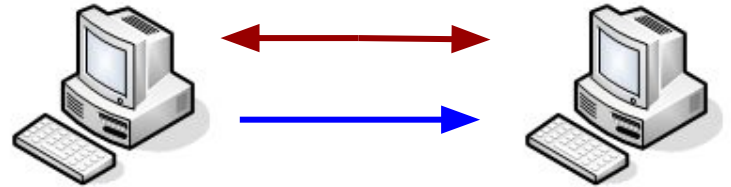
Network Address Translation (NAT)

75.123.52.41

- We would run out of IPv4 addresses very quickly if every device was given a unique one
- Instead, typically your home router is assigned a public IP and then gives the devices behind it internal IP addresses with DHCP
- The outside world will see your IP as that of the router
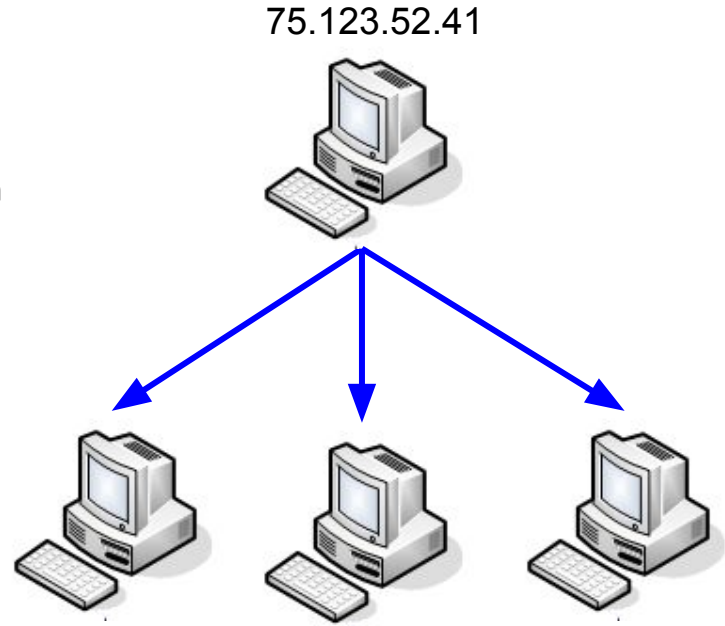
Dynamic Host Configuration Protocol (DHCP)

- Because you still need an IP address to talk to other computers your router can also assign internal IP's to your network
- Typically this IP range starts at 192.168.0.1 or 192.168.1.1 with the router and counts up
- You can also request a specific network address form the router

75.123.52.41

192.168.0.1

192.168.0.2   192.168.0.3   192.168.0.4

Fire Walls

Good and Bad
Internet Traffic

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

Good
Internet
Traffic
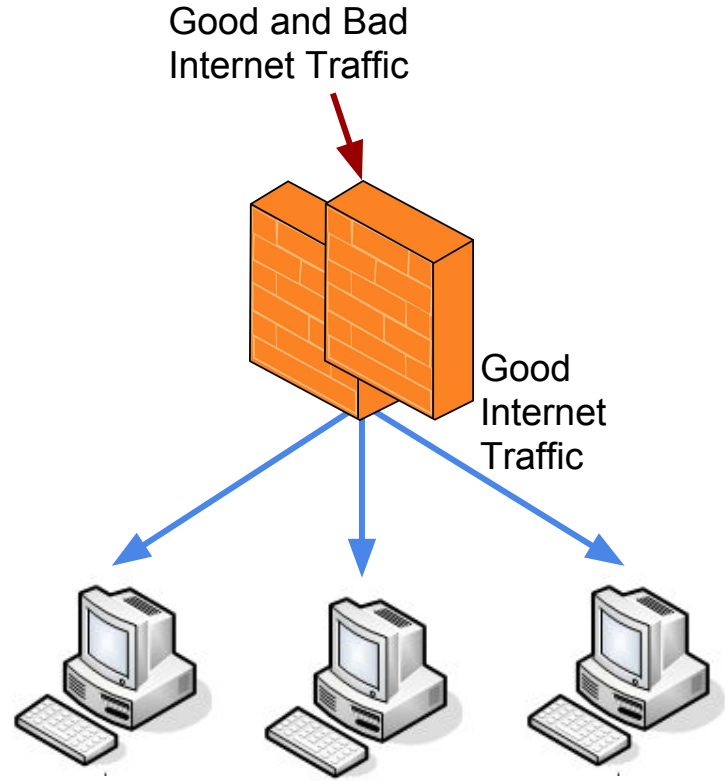
Firewall Demo

Large Networks

- Large networks such as major business require multiple layers of security
- Large networks may include several smaller networks for different purposes
- I.e. 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

Internal Network

DNS

SMTP

WWW

DMZ Subnet

Three legged firewall

Router to external network
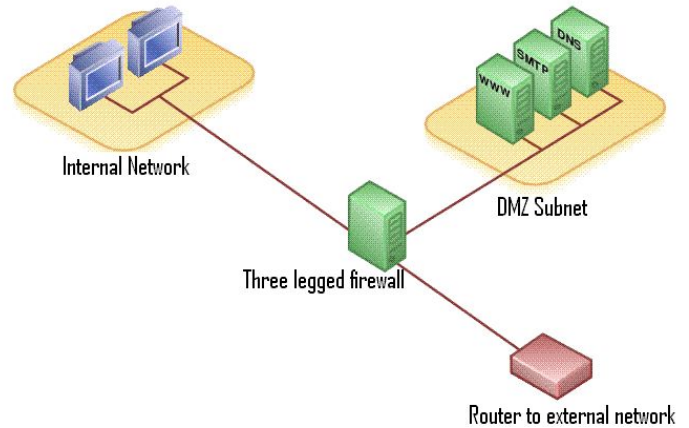
Switches and Hubs

- 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**
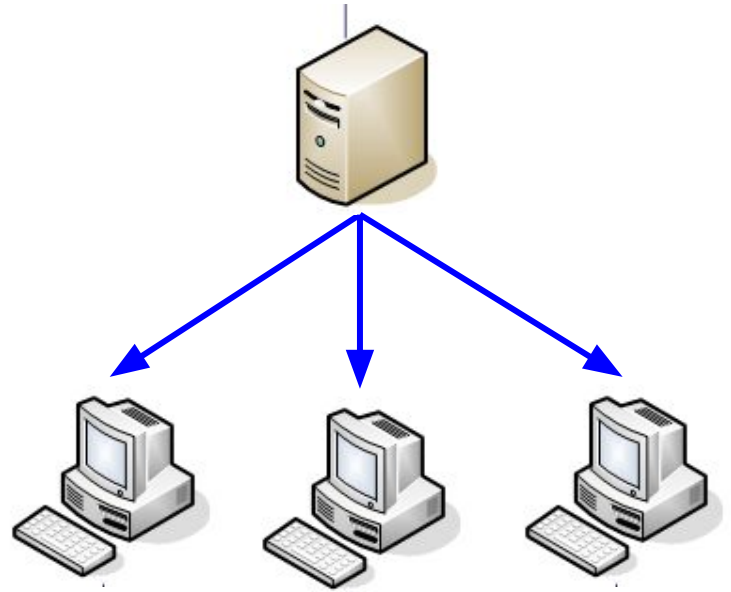
# Intrusion Detection Systems (IDS)

- Intrusion Detection Systems will monitor traffic on a network and look for things that look malicious and report the event
- Some very high end IDS's use machine learning to recognize and adapt to use patterns on the network
- 2 popular IDS's are Suricata and Snort

IDS
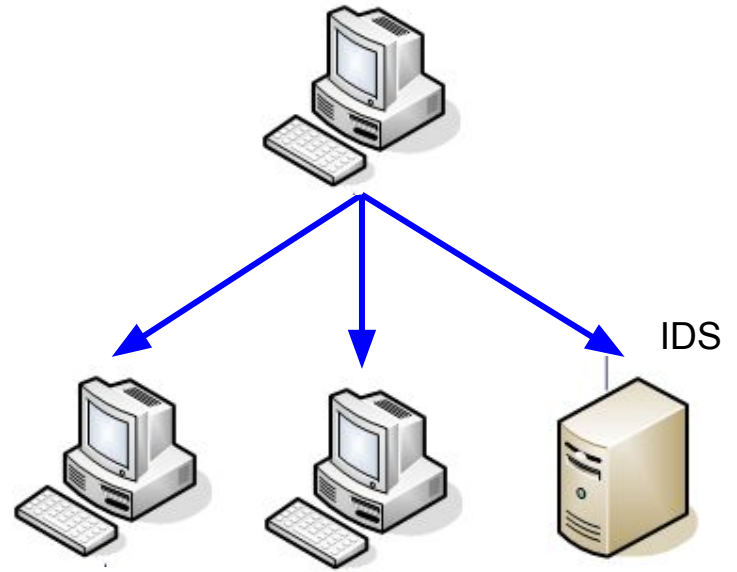
IDS Demo

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 or detection systems
- IPS's are inline just as a firewall would be

IPS
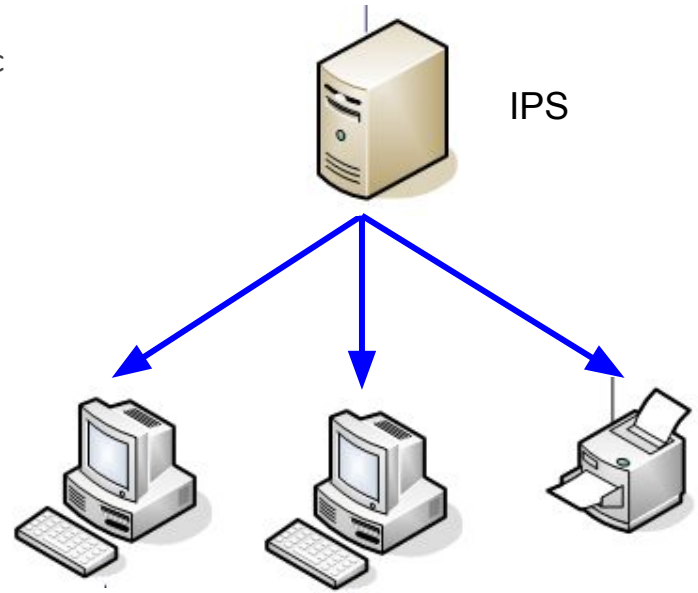
IPv6

- 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
- Can contain part of the mac address
- 340,282,366,920,938,000,000,000,000,000,000,000,000

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

4563 West Street

Virtual Private Network

- VPN's are a software way of allowing two or more systems to act as if they are on the same physical 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 use a OpenVPN to connect with Franco's class for the red team simulation
- Information sent over VPN is seen only by the VPN owner
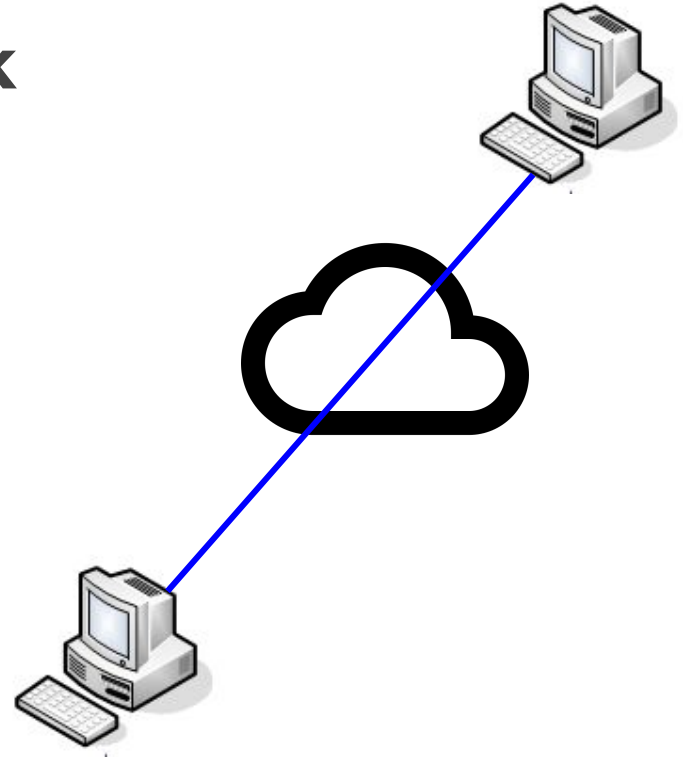
Domain Name System

- Sometimes you want to type a name instead of an IPv4 address
- DNS allows a domain to link to an address
- DNS records are kept on DNS servers (Google's is 8.8.8.8)
- DNS records can be thought of like a phone book for the internet

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

DNS Poisoning

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