Cyber@UC Meeting 70

Networking and Basic Security

If You’re New!

- Join our Slack: cyberatuc.slack.com **(URL changed!)**
- **SIGN IN!** *(Slackbot will post the link in #general every Wed@6:30)*
- Feel free to get involved with one of our committees:

  Content *Finance* *Public Affairs* *Outreach* *Recruitment*

- Ongoing Projects:
  - Research lab!

Announcements

- **US Bank visit** *THIS FRIDAY*
  - Friday Sept 28th 2pm
- **Chipotle fundraiser**
  - Saturday Nov 3rd 4pm-8pm
- **MakeUC Hack-a-thon** this weekend
  - 8:30 AM September 29 outside of **Baldwin 755**
  - Runs from 9AM to 9PM
- **NSA Codebreaker Challenge** has started codebreaker.ltsnet.net
- Outreach to **Lakota East**
- Think about **Elections**
- **Register to vote!** vote.gov

Public Affairs

Useful videos and weekly livestreams on **YouTube**:

youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Follow us for club updates and cybersecurity news:

- **Twitter:** @CyberAtUC
- **Facebook:** @CyberAtUC
- **Instagram:** @CyberAtUC

For more info: cyberatuc.org

Weekly Content

Mirai Botnet Developers Work W/ FBI

- Three men associated with developing the Mirai botnet managed to receive probation, fines, etc. over jail time, due to “extraordinary cooperation” with the government
- Mirai is a botnet, enslaves IoT devices and uses them for large scale attacks
- Claimed to be for DDoSing Minecraft servers, found selling DDoS services
- Initially were selling their botnet’s services but attempted to distance themselves by releasing the source code online, many copycats arose
- Named after Mirai Nikki, the anime
- FBI and Justice Department recommended light sentencing due to their extraordinary assistance in identifying other cybercriminals
- One of the developers is currently working part time at a cybersec firm

Newegg hacked

- Same group behind Ticketmaster and British Airways data breaches from earlier this year
- Magecart hacking group infiltrated and stole payment information between August 14th and 18th of 2018
- Utilized a digital credit card skimmer, inserting malicious javascript into the checkout page of Newegg, exfiltrating the information to a remote server
- Both mobile and desktop were affected
- Potentially millions affected, >50 mill visitors to Newegg every month
- Only used 15 lines of script

xBash malware, new chimera like malware

- Windows and Linux are both vulnerable
- Has ransomware, cryptomining, botnet, and self-propogation features
- Attributed to Iron Group, a.k.a. Rocke, a Chinese speaking APT
- Scans for certain services/ports and uses weak user/pass guessing
- Ransomware does not have decryption functionality
- Only mines and worms on Windows machines
    - Worms through Hadoop, Redis, and ActiveMQ vulnerabilities
- Developed in Python, converted into an executable through PyInstaller
    - PyInstaller also helps avoid detection

Recommended Readings

https://www.darkreading.com/threat-intelligence/hacking-back-simply-a-bad-idea/a/d-id/1332856

https://thehackernews.com/2018/09/scan4you-malware-scanner.html

https://thehackernews.com/2018/09/twitter-direct-message-api.html

https://thehackernews.com/2018/09/4g-ee-wifi-modem-hack.html

https://thehackernews.com/2018/09/android-ios-hacking-tool.html

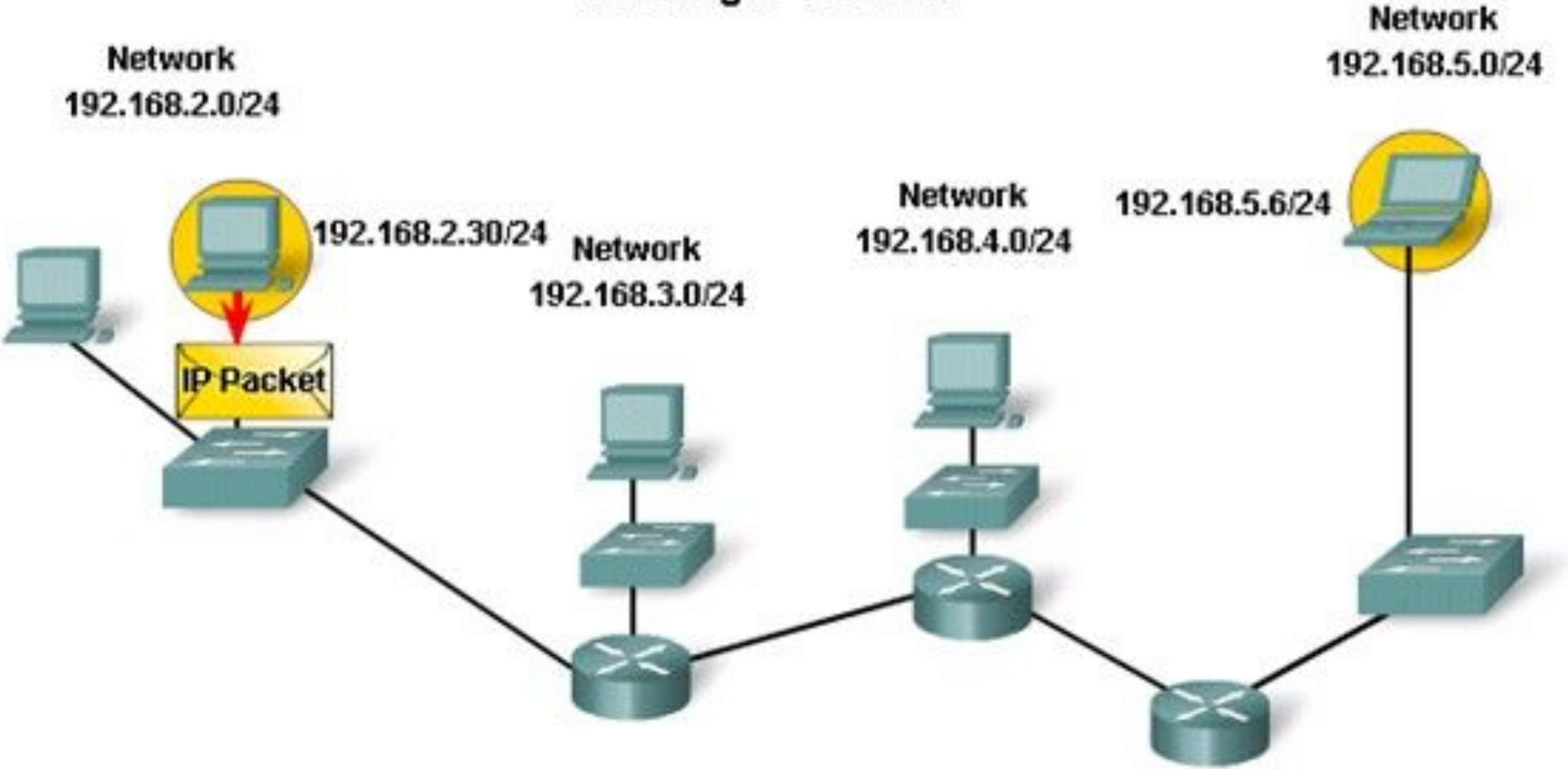
https://thehackernews.com/2018/09/windows-zero-day-vulnerability.html

Networking
Part 1

What is computer networking?

- Group of interconnected computers capable of sharing information and hardware resources through transportation of information
- Break data down into packets, unit of data transferred between from the source to the destination
- These packets travel across the network making many stops along the way
- How do these packets know where to go? OSI Model

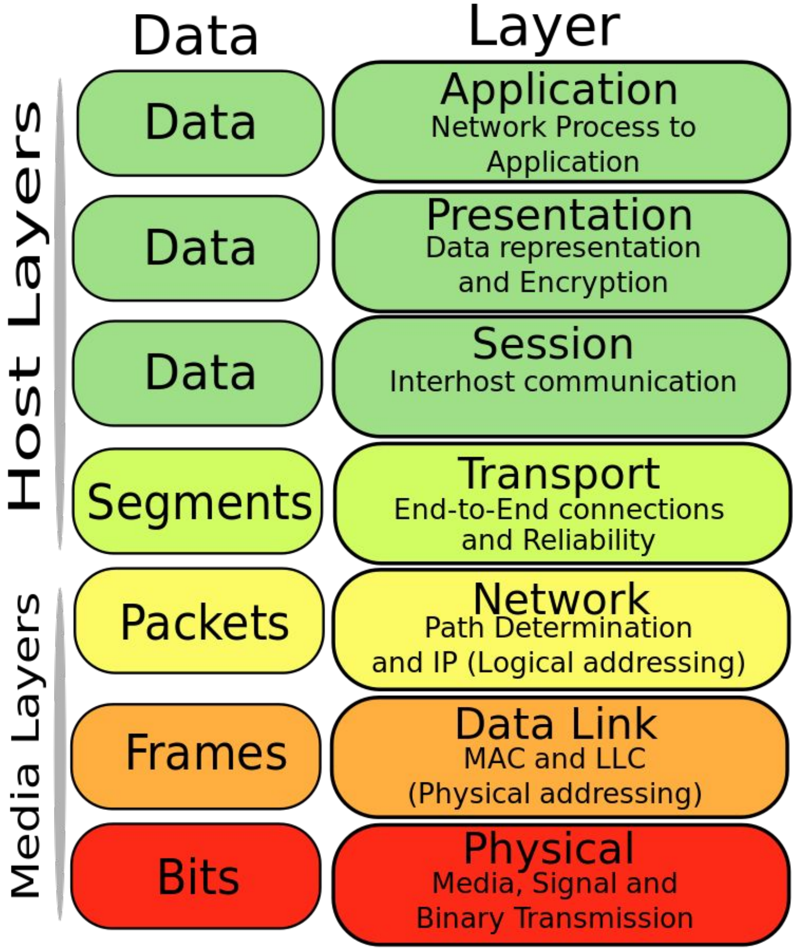
Routing IP Packets



OSI Model

- **Application**: Communicates with the software creating/assembling the packets
- **Presentation**: Communicates information to and from application layer in a standardized format
- **Session**: manages sessions for applications
- **Transport**: manages end-to-end communication, original source and final destination
- **Network**: manages the pathing from one node to the next
- **Datalink**: manages data for during travel between the nodes
- **Physical**:transmission of bits over physical medium

OSI Model



	Data	Layer
Host Layers	Data	Application Network Process to Application
	Data	Presentation Data representation and Encryption
	Data	Session Interhost communication
	Segments	Transport End-to-End connections and Reliability
Media Layers	Packets	Network Path Determination and IP (Logical addressing)
	Frames	Data Link MAC and LLC (Physical addressing)
	Bits	Physical Media, Signal and Binary Transmission

IPv4 vs IPv6

- Try typing ipconfig into cmd, or ifconfig for linux
- Your IP is your address, it is meant to uniquely identify you from everyone else
- The addresses available in IPv4 was running out, so IPv6 was invented
  - IPv4 maxes at 4.3 billion possible addresses
- IPv6 has 3.4 x 10^38 possible addresses

DHCP

- Dynamic Host Configuration Protocol
- Automatically assigning unique IP addresses
- A device acts as the DHCP server, usually the router
- Device requests IP from router, router assigns an IP to the device
- Easy to get an IP without risk of doubling up on an already taken IP
- Having the IP be dynamic and subject to change can cause problems

NAT

- Network Address Translation
- Helped with reducing strain of limited IPv4 addresses
- A device, such as a router acts as an agent between the device and everything upstream
- Allows one to be used to represent all computers connected to that router
- Different forms, static, dynamic, overloading, overlapping
- Follow the link below to get more detailed illustrations of each
- https://computer.howstuffworks.com/nat.htm

Network Security

Intrusion detection systems (IDS)

- A device (or devices) that is attached to a network (Usually, sometimes software)
- Listens to network traffic for anything out of the ordinary or anything that is flagged as malicious
- Warns network administrator, but does not actively stop flagged traffic
- Primarily used to make sure there are known patterns and records of network traffic

Intrusion prevention systems (IPS)

- Functions as a packet filter - Denies or allows traffic, but allows most everything through
- Useful for denying specific patterns that are known to be malicious

Examples: Suricata, Snort, Bro

VPN

Remote Access

- Connects one device to a remote network to provide “local” access to the remote network
- If you have an application for your desktop, it is this kind

Site-to-site

- Mostly used by businesses or organizations with multiple offices
- Connection is from router to router
- Essentially a tunnel between two networks

Example: IVPN, tinc