NETWORKING

49TH DIVISION EDUCATION NIGHT

DISCLAIMER

- *We are an ethical hacking club*
- *We will not be held accountable for the abuse of the concepts taught*
- *The materials presented is for the education of attendees*

ANNOUNCEMENTS

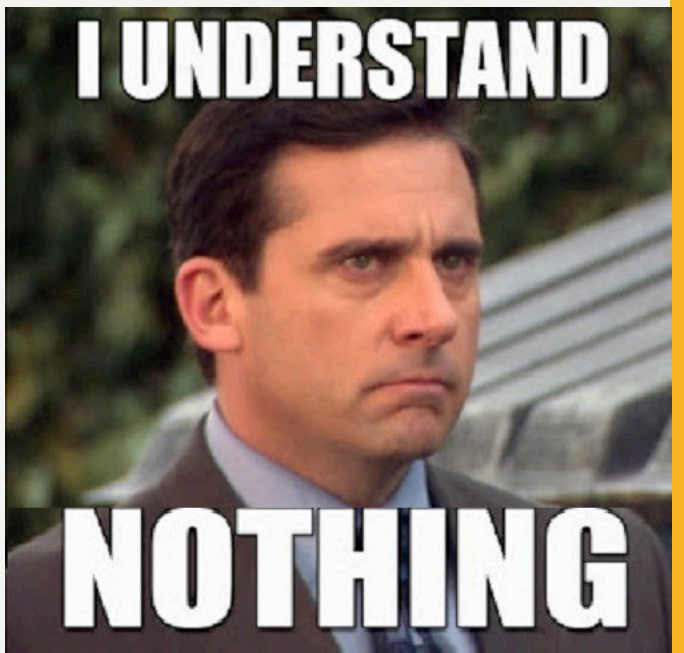
- No competition practice this upcoming Friday and Saturday (*Spring Break*)
- Competition Team formation details
- NCL Codes have been distributed
- Signing up For NCL - https://cyberskyline.com/events/ncl
- Lab Hours are pinned in the #lab channel

WHO AM I

- Blackmanta (*slack*) Trevon (*IRL*)
- Graduate Student
- Competition Enthusiast
- Linux Junky
- Professional Lurker

RECAP

- Passive and Active scanning
- Nmap can be used for finding open ports
  - nmap –T4 –A [IP OF MACHINE] –Pn
- Key ideas of Enumeration
  - Dirb, Dirbuster, gobuster, Fuzzers (burpsuite, zap)
- HTB Traverxec
  - *walk through to getting user*




QUESTIONS?

NETWORKING CRASH COURSE

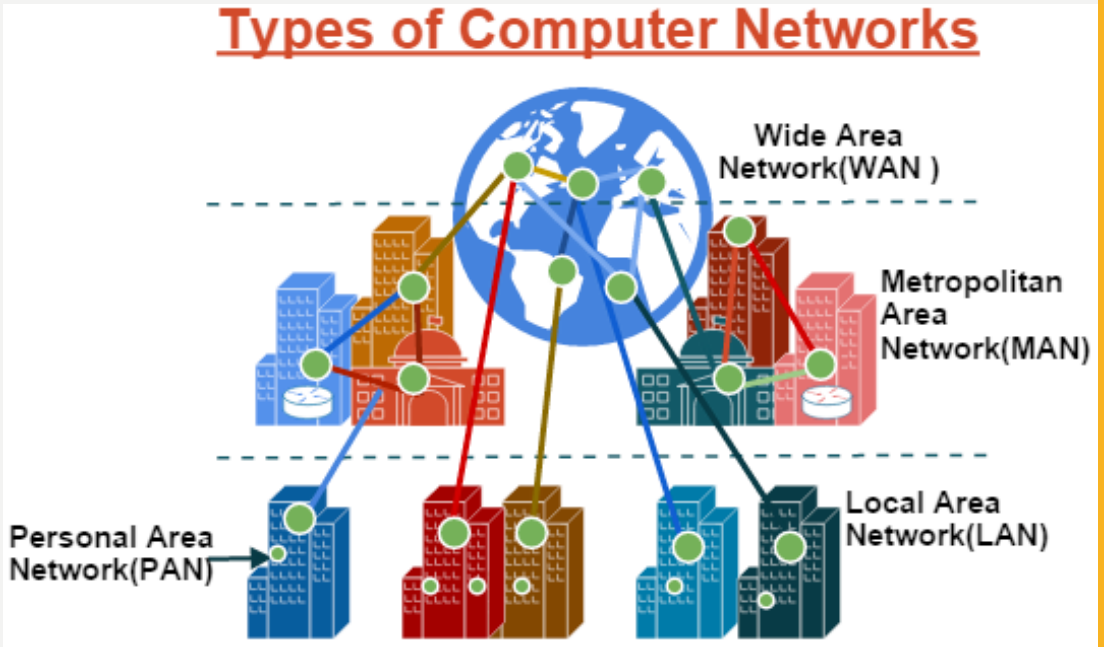
- Understand how systems communicate
- Foundational understanding is important
- Find or report network abuse

OSI MODEL (OPEN SYSTEM INTERCONNECTION)

- TCP/IP Model
  - Link
  - Network
  - Transport
  - Application
- TCP and UDP
- *What ports are listening on your computer?*

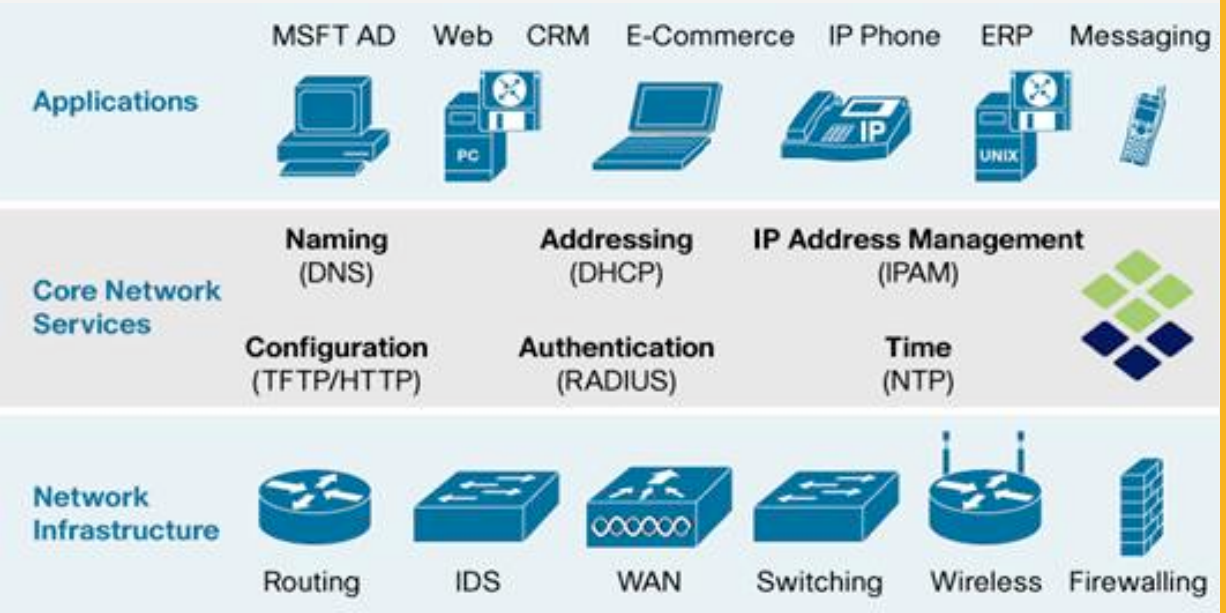
TYPES OF NETWORKS

- (LAN) Local area network
- (WAN) Wide area network
- (WLAN) Wireless local area networks



SERVICES

- Services need to communicate
- Understanding how network services work (python socket programming)
- Tooling to open ports on machines
  - Netcat
  - Telnet
  - Almost any programming language



NETWORK ABUSE

- Reverse Shells
  - Bypass egress firewall rules
  - Can operate with any protocol combination
- Port forwarding with SSH
  - Local port forwarding
  - Remote port forwarding

INTO THE BOX

REGISTRY

RESOURCES

- Reverse Shell Cheat Sheet Pentest monkey
- Extensive Reverse Shell Cheat Sheet Github PayloadAllTheThings
- Sans Presentation
- SSH Tunneling
- Living off the land
- GTFObins