

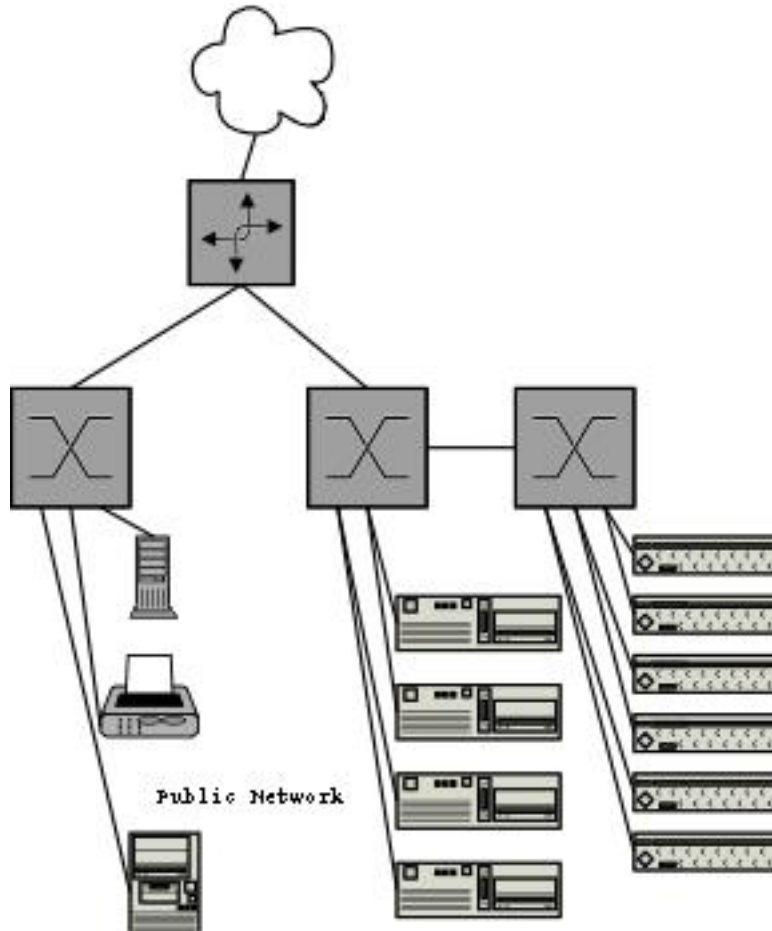
# **Network Security**

**Jon Hart & Muncus  
Crew**

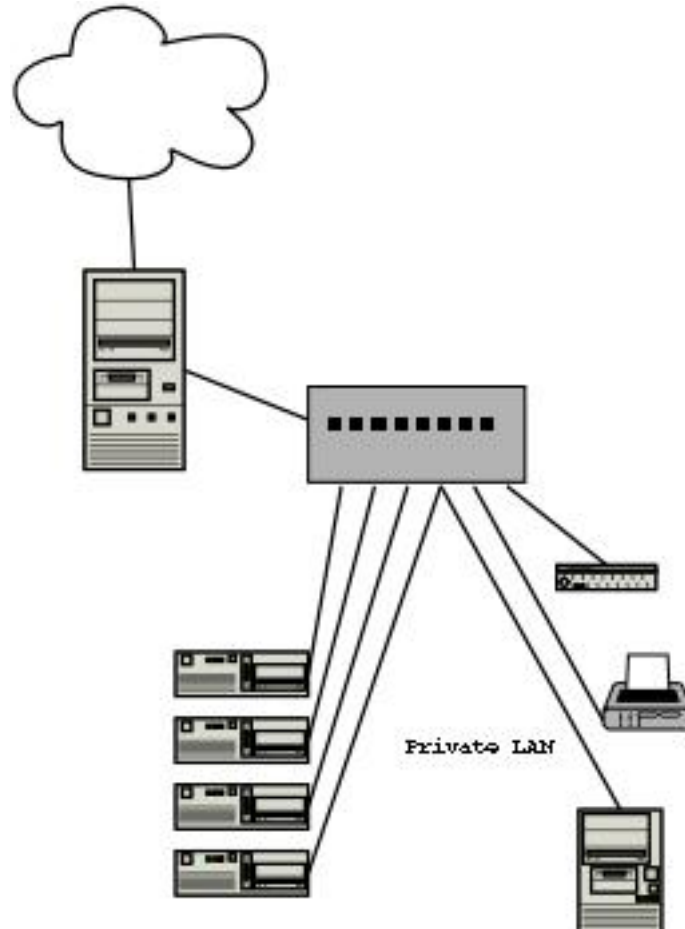
# Disclaimer

- This talk:
  - ◆ Is not all inclusive
  - ◆ Will focus mostly on TCP/IP + Ethernet based networks
    - Much like the one used at CCS, CTF, home, etc
  - ◆ Many topics can be applied to other types of networks or security considerations
  - ◆ You will be punished and possibly serve jail time if you do this on networks that you don't own or otherwise have permission to poke at
  - ◆ Attacking, probing, or poking at CCS/NU networks will likely get you expelled.

# CCS Network Diagram



# CTF Network Diagram



# Where do I start?

- Read. Learn. Do.
- Know your network
- Think like the attacker
- "How to Secure Your Network by Breaking Into it"

# Know your network

- Aka Info/Recon Gathering
  - ◆ Scan, Poke, Prod, which gets you...
    - A list of services
    - Network layout
    - And, with any luck, avenues of attack

# Know your network (cont.)

- Tools you can't live without:
  - ◆ nmap
  - ◆ nessus
  - ◆ mbsa
  - ◆ nc/telnet
  - ◆ firewalk
  - ◆ packet crafting tool

# Network scanning

- Aka "mapping"
- More of an information gathering process
- Figure out how a network is configured:
  - ◆ Network topology
  - ◆ Access Control Lists (ACLs)
  - ◆ What devices are in use, and how
- May allow you to discover misconfigurations

# Network scanning: Defensive

- A good firewall ruleset, ACL, etc:
  - ◆ pf, ipf, ipchains, iptables, PIX, Cisco ACL, etc)
- Rate-limiting and monitoring:
  - ◆ cricket, mrtg
- Anomaly Detection:
  - ◆ Spade
- Know your network. What is 'normal'?

# Network scanning: Offensive

- Firewall

# Host scanning

- Aka "portscanning"
- Again, mostly an information gathering process
- Figure out how a host is configured:
  - ◆ OS Type and version, maybe even specific options
  - ◆ Open Ports (services offered)
  - ◆ Allowed protocols

# Host scanning: Defensive

- A good firewall:
  - ◆ Block everything, allow only whats needed
  - ◆ Stateful
  - ◆ Windows: ZoneAlarm, built-in
  - ◆ Linux: ipchains or iptables
  - ◆ \*BSD, Solaris: pf, ipf
- Logging:
  - ◆ Logwatch, logsurfer

# Host scanning: Offensive

- nmap
- nmap
- nessus
- Xprobe
- nc/telnet
- Google
- Pen and paper
- nmap

# So you have a target...

- What should I look for?
  - ◆