Intro to Cyber warfare

Attacks and Countermeasures

What is Cyber warfare?

- Use of computers and computer networks to slow, manipulate, or cease the operational capacity of other computers.

Why attack?

- Profit
  - Sabotage your rivals
  - Bank information
- Tactical advantage
  - Wartime espionage
  - Intelligence gathering
  - System corruption
- Because
  - Some men just want to watch the world burn

Methods of attack

- Mostly a two-step process
- Passive
  - Packet sniffing (eavesdropping) for collecting information, authentication info.
- Active
  - Brute force – Computer guesses auth. Info.
  - Packet Injection – Data modification
  - IP Address spoofing – making a machine think you're someone else
  - DDoS Attack – Sending tons of requests to a server
  - Man-in-Middle – Intercepting, changing, passing

Countermeasures

- Detect
  - Find out if you're being attacked
- Identify
  - Find out what kind of attack
- Counter
  - Use the counter most effective to the attack

NOTE: Specific attacks require specific counters. Most attacks built to be covert.

Countermeasures

- Sniffing
  - Look for interfaces in promiscuous mode (passing all traffic through CPU.) Two ways: Host-based (software) and Network-based (processes and log files) Best defense is end-end encryption.
- IP Spoofing
  - Routers usually perform an IP check of incoming connections, to see if they are reachable from the interface. If not, they are discarded.

Countermeasures

- Data Modification
  - Checksums
- DDoS; Bruteforce
  - IP packet filtering

What now?

- Bring computer + Flash drive tomorrow
- First practice round Oct 1st – 10th
  - Use this to see what we're up against.