JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Network Probes and Attacks

CYBER INCIDENT RESPONSE

Network Probes and Attacks

- Much of your incident handling will involved network probes and attacks

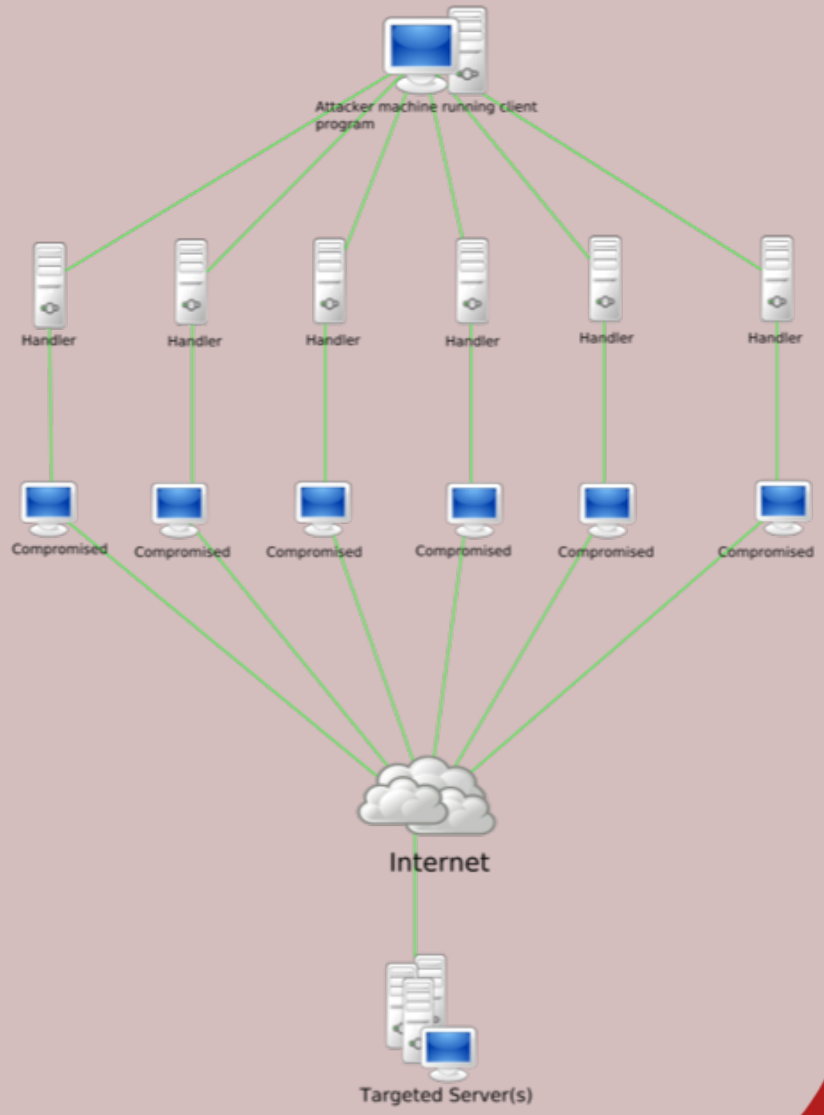
- Network probes are usually part of reconnaissance efforts and are easy to detect (like a port scan)

Denial of Service (DoS)

- Detection:
  - Attacks on a given network, system, or service from a single source
  - Attempts to overwhelm system or network
- Prevention:
  - Block the attacker using your firewall or IPS

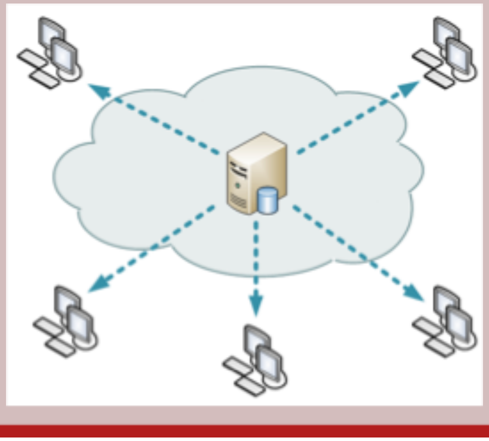
Distributed Denial of Service (DDoS)

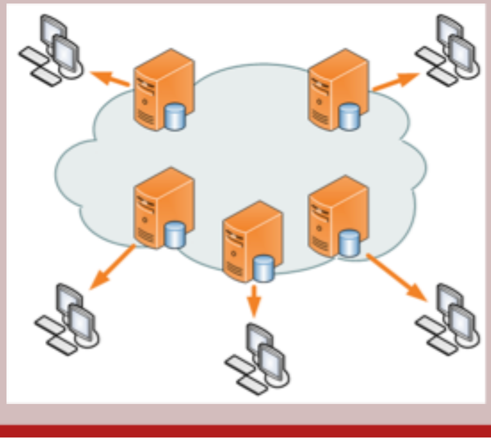
- Attacks on a given network, system, or service from simultaneous multiple sources
- Attempts to overwhelm system or network



Distributed Denial of Service (DDoS)

- Detection:
  - Traffic coming from known botnet IPs
  - Monitoring your traffic and usage patterns
- Prevention:
  - Network designed with distributed network of endpoints (like Akamai)
  - Ensure your networks can scale upwards





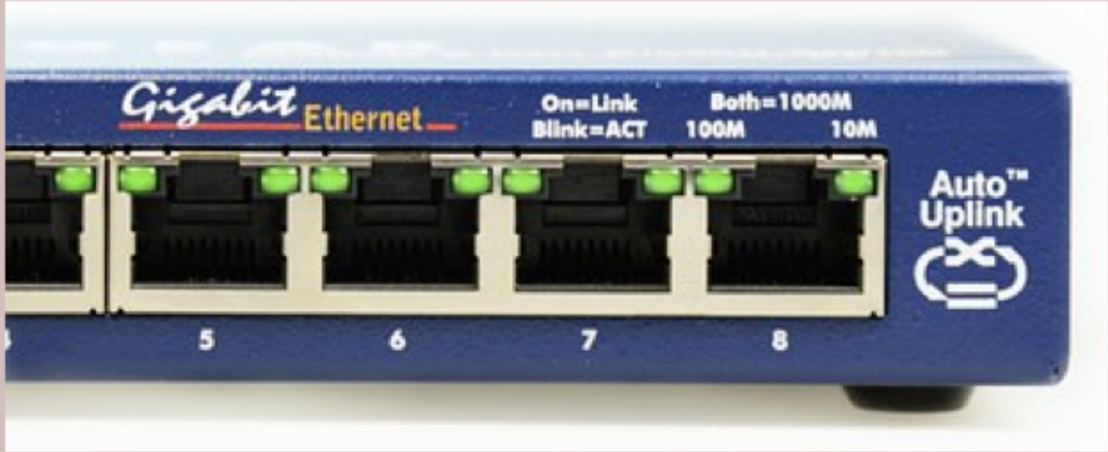
Detecting Rogue Devices

- MAC Address Validation
  - Ensure all devices are “Known Devices”
  - Check device MAC against vendor codes
- Scan the Network to identify devices
- Conduct physical site inspections
- Analyze traffic for irregular behavior

Rogue Wired Devices

- Usually occurs when an employee or attacker connects a wired device
  - Adds a switch or hub to the network

- Network Access Control and Port Security can prevent this occurring



Rogue Wireless Devices

- Can be detected by conducting wireless surveys and mapping the area
- Often used as an Evil Twin to trick users to connect to them and steal information