Johnny Zhong
CS373 – Defense Against The Dark Arts
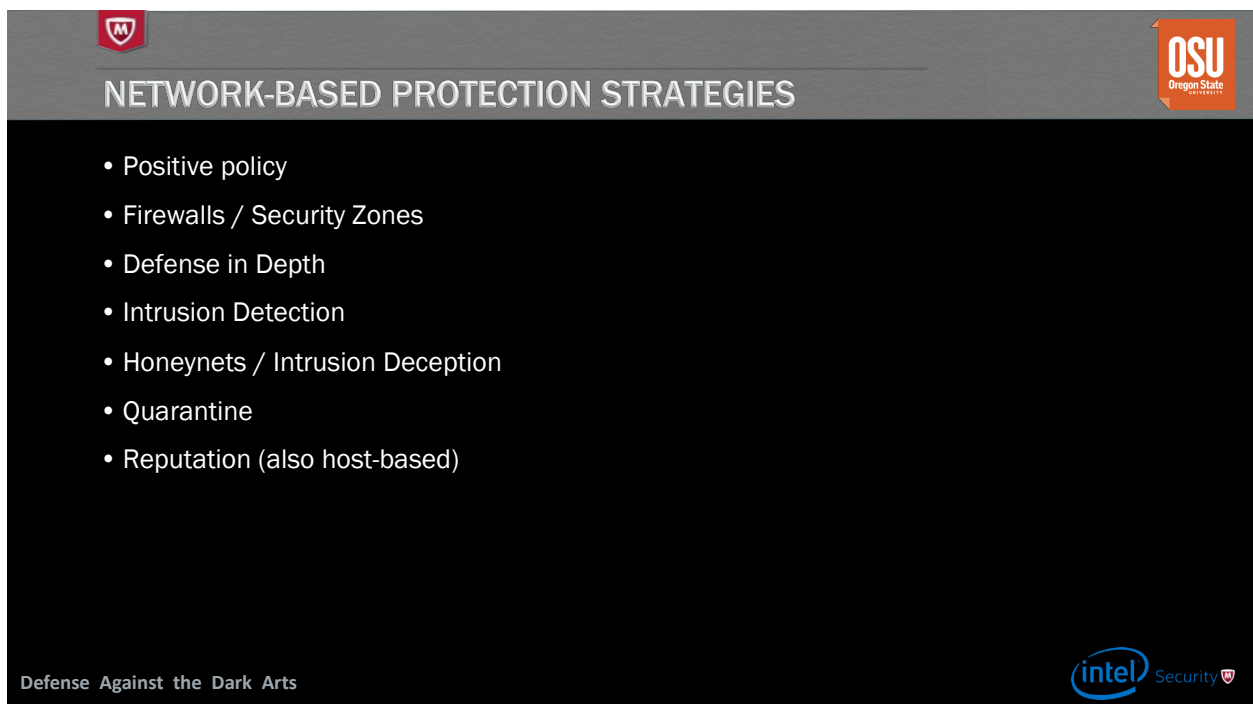Week 6 – Network Security Technologies

Network Security Purposes
- Prevention
- Critical data flowing in/out of network
- Prevention of DDOS
- Dealing with threats to network proper:
    o Turn off
    o Disable actions for

"Be liberal in what you accept and be conservative in what you send."

Protection Strategies
- Positive Policy/whitelisting - Allow only what you're expecting to have happen
- Firewall
    o allows the defender to have the advantage
    o Attack surface – set of operations the network is willing to respond to
    o Many kinds of firewalls
        ▪ Web gateway – acts as a proxy (any traffic bound for the outside world goes through this device), can be more selective than traditional firewalls
        ▪ Email gateway – smtp – filters mail
- Defense in Depth – defense method that assumes that outer security measures will fail. – castle analogy

- Intrusion Detection/Protection System
    - Blacklist method as opposed to whitelist method
    - Fails with unknown attacks (zero day attack)
    - False positives
    - YARA is a method of detection for known threats
- Honeynet
    - Leaving a vulnerable system out to be attacked
    - Requires specific information for deployment
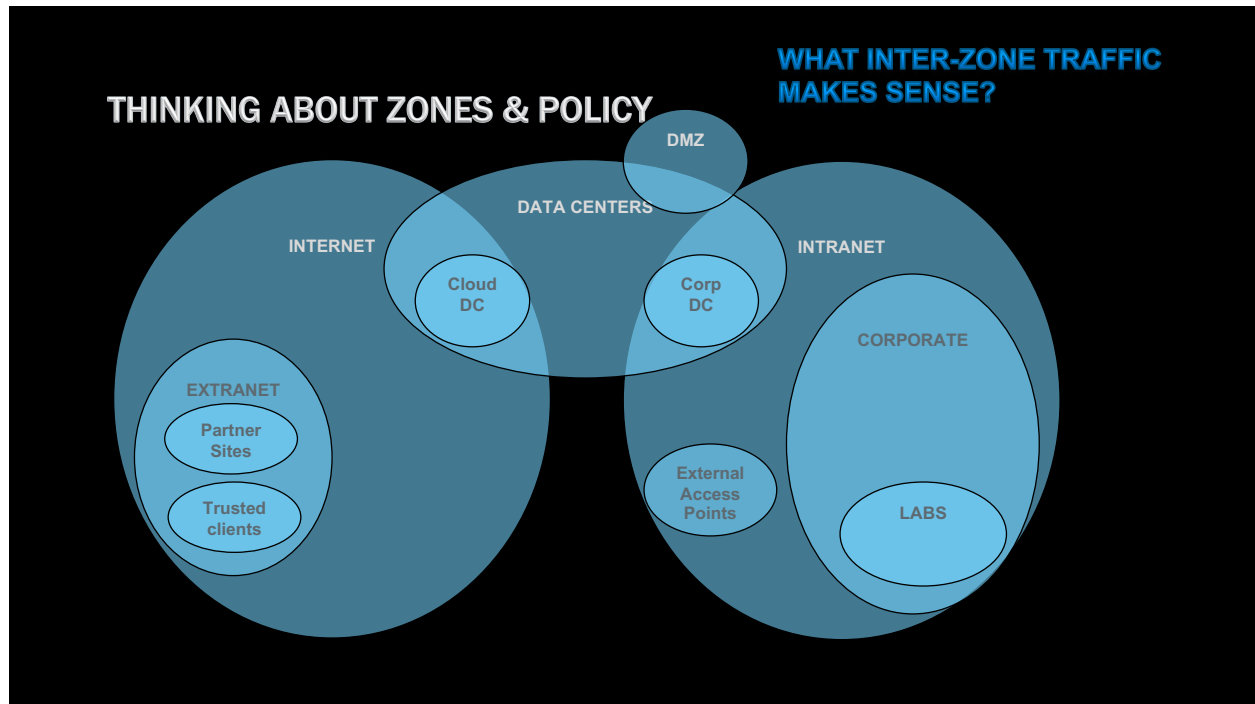
- Quarantine
    - Put the threat in a part of a network which does not allow the threat to access anything else
    - Allows us to analyze behavior
- Reputation
    - Security Certificates
    - Past behavior or aggregated score
    - Big data – a point where the amount of data changes the value of the data
- NextGen Firewall
    - allows machines to look into packets to determine the safety of the packet.
    - Allows for app identification

Threats
- MTM – Man in the Middle
    - Can be used for good and evil
    - Intercepts traffic on network
    - TCP Hijacking

- We don't protect against MITM
- Rewrite packet, change checksum
- Might be used for security reasons – removal of malware, change of outgoing file
  - Terminating Proxy – change connection
  - Remove meta characters from obfuscated URLs
  - SSL MITM – encrypting your data – firewalls
  - Detection of MITM – HMAC – large number of bits turn into a small number of bits.
    - Create HMAC off of the base data being sent
    - Attacker can double up the packet, causing issues
    - But can chain HMACs in order to prevent this from happening
  - N-squared problem solution – public key cryptography
    - Public key to lock
    - Private key to unlock
    - Many mechanisms to share data, through SSL
  - Dependency of each layer on each other introduces a vulnerability (hierarchy of trust)
  - Change to trusted certificates
  - Precise set of guarantees, not full guarantee

Lecture 2

Lab Notes:
Class A network – 8 bit
Class B network – 16 bit
Class C network – 24 bit subnet mask

Threat Recon

Why? – want to know where you want to deliver a payload

Active and Passive Recon

Passive Recon
- listening in to what's going on
- via switches, routers

Active Recon
- nmap
- ping

Wireshark Demo

Defense
Honeynet – used to slow down attackers
- act like a desirable target
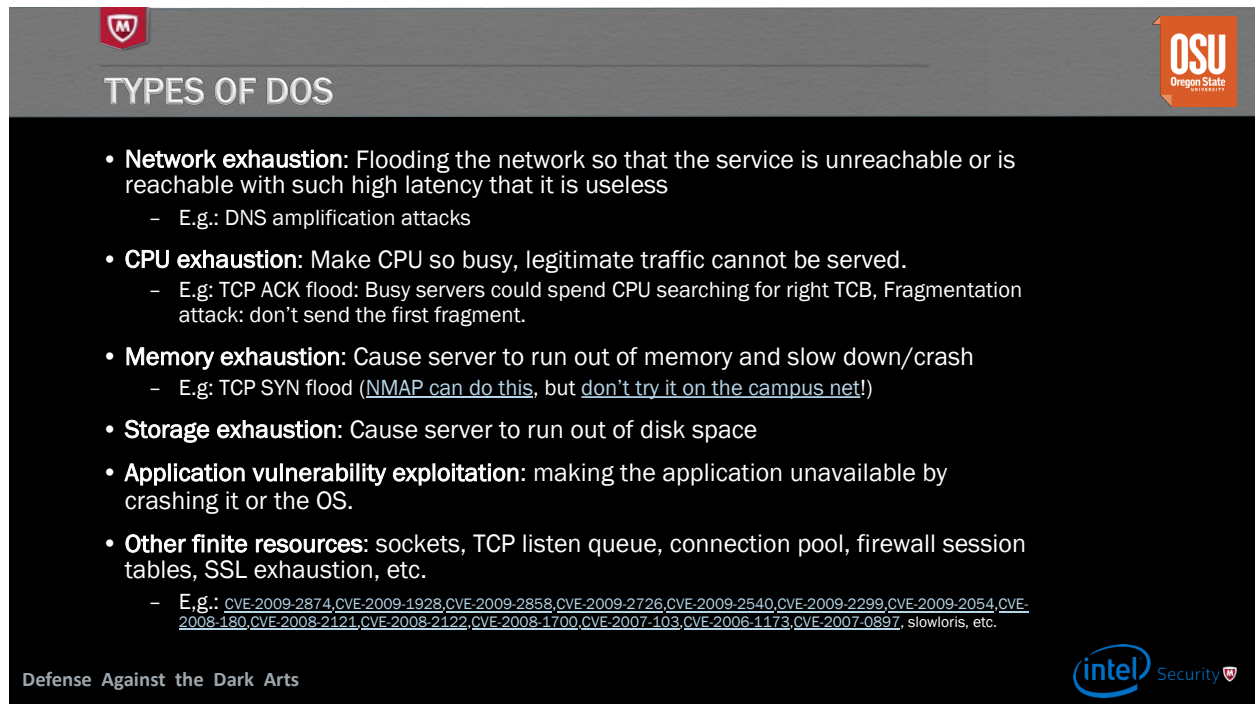- slow down responses

Spoofing
- get data that was intended for a different recipient
- DoS attacking
- LAND – LAN DoS
- Used in the industry - Can be used to mimic many hosts for testing
- Protection against spoofing
    o Egress filtering, ingress filtering
    o Ensure that the packet that we're receiving would normally come in through the port that it's actually coming in from.
    o What would the host do if this packet was to be sent from the host?
    o Aka reverse packet filtering
    o Ensuring we're getting the data through the correct interface

DOS Attacks:
- Why? – bring down network, hide real intent
- How? –
    o Send many requests to flood the target with requests.
    o Spoofing –
    o Ex: Slowloris.- tries to keep a connection open for a long time

- o Unintentional

Bugs and Backdoors

Shodan - Large collection of vulnerable routers
Not all users follow RFCs to the letter.

Defense

Stateful vs Stateless
Stateful – inspect packets to ensure they correspond to the existing connection
Stateless – apply policy rules and accept packets without checking

Fragmentation Attack: send highly fragmented packet so that the firewall has to reassemble the packet, taking up a large amount of buffer. Or send last packet first.

Deep Inspection: add inspection methods to packets

IKE: Internet Key Exchange (UDP)
Works like a public key exchange.
Establish an IPv4 tunnel.

Endpoint Context: understanding the nature of the traffic can help with understanding if an attack is happening.

Dynamic Analysis: A device that executes malware to determine the nature of the malware. Allows a user to view the activity in the box.

Reputation: Prevalence (how often) and Age (how old)

Wireshark Notes:
Follow TCP Stream – provides data on the TCP stream
Stats and Conversation – provides more data on conversations
Export Objects – allows user to get files and data on files that are sent through HTTP
Find Packet – search