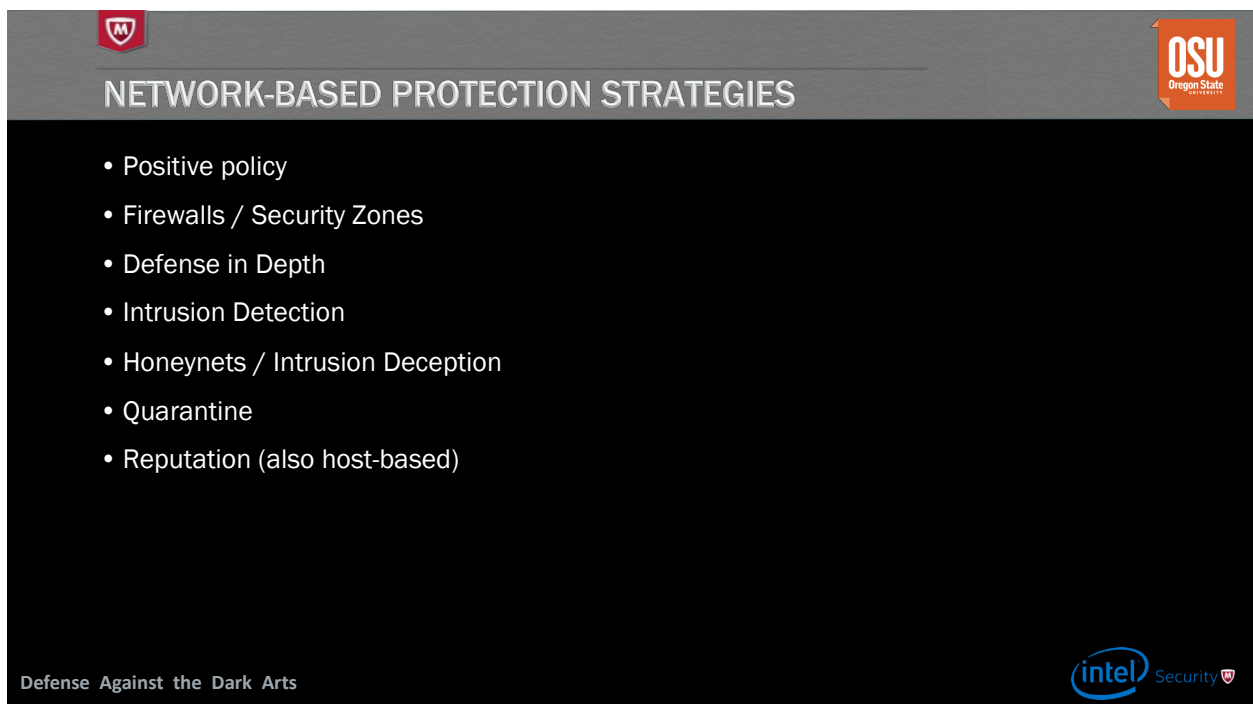


Network Security Purposes

- 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.”



The slide features a dark background with a light gray header. The header contains the OSU logo on the left and the text 'NETWORK-BASED PROTECTION STRATEGIES' in the center. The main content area lists seven strategies: Positive policy, Firewalls / Security Zones, Defense in Depth, Intrusion Detection, Honeynets / Intrusion Deception, Quarantine, and Reputation (also host-based). The footer includes the text 'Defense Against the Dark Arts' on the left and the Intel Security logo on the right.

OSU
Oregon State University

NETWORK-BASED PROTECTION STRATEGIES

- Positive policy
- Firewalls / Security Zones
- Defense in Depth
- Intrusion Detection
- Honeynets / Intrusion Deception
- Quarantine
- Reputation (also host-based)

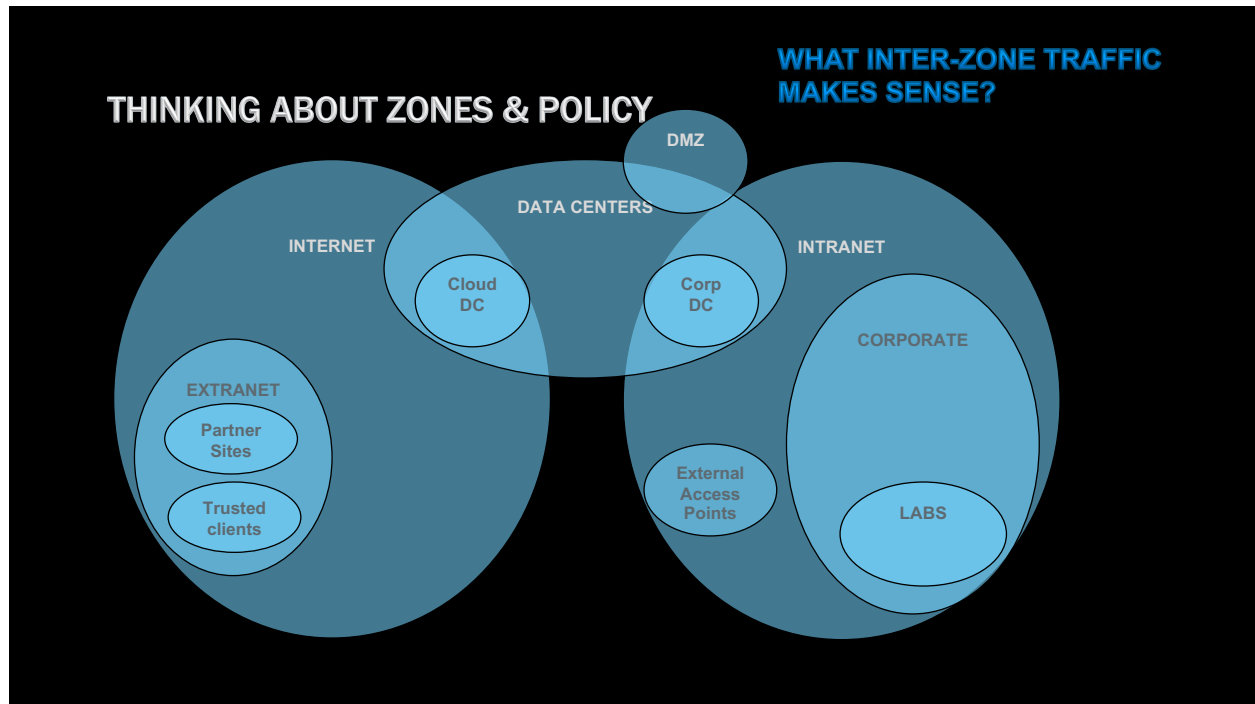
Defense Against the Dark Arts

intel Security

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
 - o Blacklist method as opposed to whitelist method
 - o Fails with unknown attacks (zero day attack)
 - o False positives
 - o YARA is a method of detection for known threats
- Honeynet
 - o Leaving a vulnerable system out to be attacked
 - o Requires specific information for deployment



- Quarantine
 - o Put the threat in a part of a network which does not allow the threat to access anything else
 - o Allows us to analyze behavior
- Reputation
 - o Security Certificates
 - o Past behavior or aggregated score
 - o Big data – a point where the amount of data changes the value of the data
- NextGen Firewall
 - o allows machines to look into packets to determine the safety of the packet.
 - o Allows for app identification

Threats

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

EXAMPLE USING WIRESHARK—HEADER ANALYSIS

Filter: tcp.stream eq 10550

No.	Time	Source	Destination	Protocol	Length	Info
400851	2004-12-15 17:47:27.858839	65.193.86.2	204.153.45.191	TCP	60	29280 > ftp [SYN] Seq=0 win=512 Len=0 MSS=1460
400852	2004-12-15 17:47:27.858840	65.193.86.2	204.153.45.191	TCP	60	29280 > ftp [SYN] Seq=0 win=512 Len=0 MSS=1460
400872	2004-12-15 17:47:27.864087	204.153.45.191	65.193.86.2	TCP	60	ftp > 29280 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1400
400873	2004-12-15 17:47:27.864087	204.153.45.191	65.193.86.2	TCP	60	ftp > 29280 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1400
401482	2004-12-15 17:47:27.958671	65.193.86.2	204.153.45.191	TCP	60	29280 > ftp [ACK] Seq=1 Ack=1 win=7300 Len=0
401483	2004-12-15 17:47:27.958671	65.193.86.2	204.153.45.191	TCP	60	TCP Dup ACK 401482#1] 29280 > ftp [ACK] Seq=1 Ack=1 win=7300 Len=0
421966	2004-12-15 17:47:30.832670	204.153.45.191	65.193.86.2	TCP	60	ftp > 29280 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1400
421967	2004-12-15 17:47:30.832671	204.153.45.191	65.193.86.2	TCP	60	ftp > 29280 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1400
422662	2004-12-15 17:47:30.927129	65.193.86.2	204.153.45.191	TCP	60	TCP Dup ACK 401482#2] 29280 > ftp [ACK] Seq=1 Ack=1 win=7300 Len=0
422663	2004-12-15 17:47:30.927130	65.193.86.2	204.153.45.191	TCP	60	TCP Dup ACK 401482#3] 29280 > ftp [ACK] Seq=1 Ack=1 win=7300 Len=0
422754	2004-12-15 17:47:30.939373	204.153.45.191	65.193.86.2	FTP	103	Response: 220-Serv-U FTP Server v5.2 for winsock ready...
422755	2004-12-15 17:47:30.939374	204.153.45.191	65.193.86.2	FTP	103	[TCP Fast Retransmission] Response: 220-Serv-U FTP Server v5.2 for winsock ready...

Things we learn:

- IP Addresses, apply DNS and whois
- FTP protocol (control connection)
- MAC addresses of the routers
- Packet sizes

Defense

Honeynet – used to slow down attackers

- act like a desirable target
- slow down responses

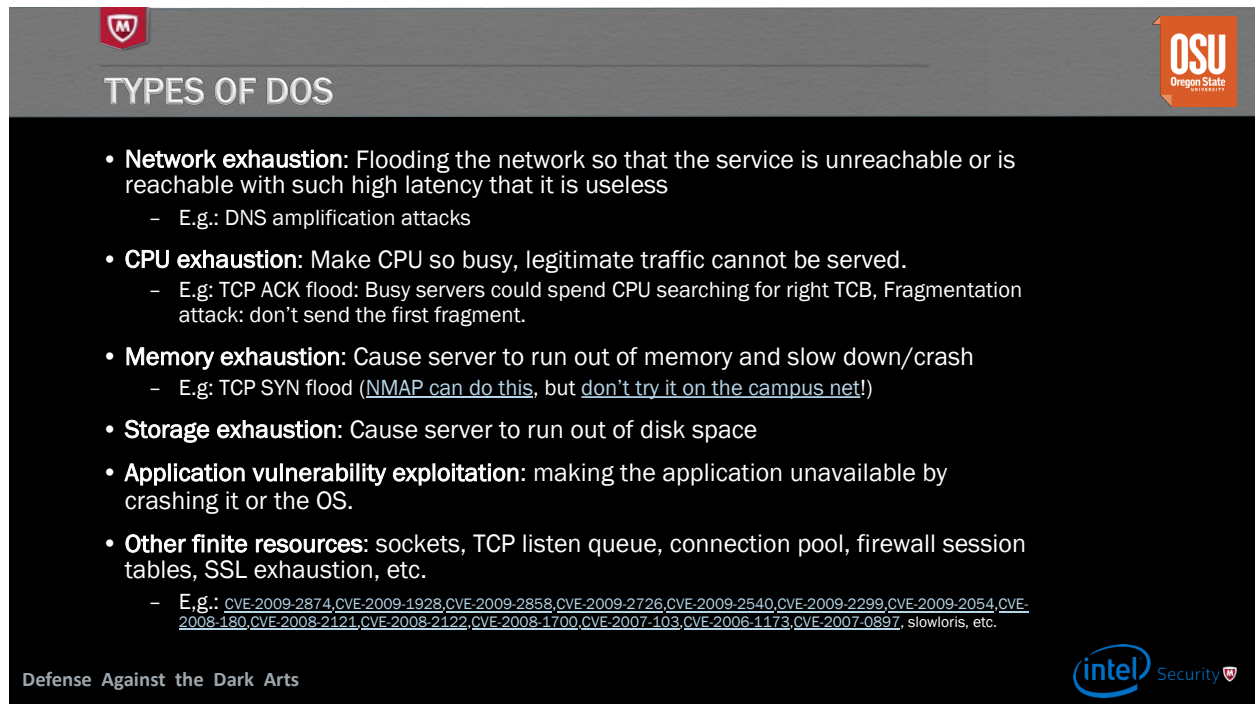
Spoofing

- 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



- Unintentional



TYPES OF DOS

- **Network exhaustion:** Flooding the network so that the service is unreachable or is reachable with such high latency that it is useless
 - E.g.: DNS amplification attacks
- **CPU exhaustion:** Make CPU so busy, legitimate traffic cannot be served.
 - E.g: TCP ACK flood: Busy servers could spend CPU searching for right TCB, Fragmentation attack: don't send the first fragment.
- **Memory exhaustion:** Cause server to run out of memory and slow down/crash
 - E.g: TCP SYN flood ([NMAP can do this](#), but [don't try it on the campus net!](#))
- **Storage exhaustion:** Cause server to run out of disk space
- **Application vulnerability exploitation:** making the application unavailable by crashing it or the OS.
- **Other finite resources:** sockets, TCP listen queue, connection pool, firewall session tables, SSL exhaustion, etc.
 - E.g.: [CVE-2009-2874](#), [CVE-2009-1928](#), [CVE-2009-2858](#), [CVE-2009-2726](#), [CVE-2009-2540](#), [CVE-2009-2299](#), [CVE-2009-2054](#), [CVE-2008-180](#), [CVE-2008-2121](#), [CVE-2008-2122](#), [CVE-2008-1700](#), [CVE-2007-103](#), [CVE-2006-1173](#), [CVE-2007-0897](#), slowloris, etc.

Defense Against the Dark Arts



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





NGFW POLICY



Match Active Directory group/user name

Policy sub-routines (templating)

ID	Source	Destination	Service	Action	Authentication	Logging
14.1.1	ANY	ANY	ANY	Continue		Stored, Accounted
14.1.2	Atlanta Internal Network	Not Internal	ANY	Allow		
14.1.3	Support	ANY	HTTP	Jump HTTP Sub-Policy		
1	adam	Atlanta DMZ	HTTP	Allow		
2	Partners	Extranet Servers	HTTP	Allow		
3	Not Internal	Intranet Servers	HTTP	Apply VPN: Client VPN	 Authorize client IP Client initiated Timeout = 3600	
14.1.4	Atlanta Internal Network	Helsinki Internal Network	HTTPS SSH	Allow	 Authorize client IP Client initiated Timeout = 3600	
Discard all						


Logical Expressions

Policy recognizes protocols and verifies them

Policy-based routing to VPN

Defense Against the Data

Named objects



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