CSF 434/534: Advanced Network and System Security

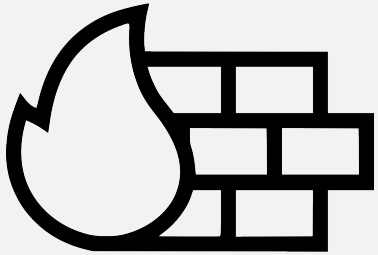
Week 05 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes

Firewalls



Firewalls

The universal security control

- Standard issue
  - Home, office, and in your operating system
- Control the flow of network traffic
  - Everything passes through the firewall
- Corporate control of outbound and inbound data
  - Sensitive materials
- Control of inappropriate content
  - Not safe for work, parental controls
- Protection against evil - Anti-virus, anti-malware

Firewalls

Network based firewalls

- Filters traffic by port number
  - OSI layer 4 (TCP/UDP)
  - Some firewalls can filter through OSI layer 7
- Can encrypt traffic into/out of the network
  - Protect your traffic between sites
- Can proxy traffic
  - A common security technique
- Most firewalls can be layer 3 devices (routers)
  - Usually sits on the ingress/egress of the network

Firewalls

Stateless firewall

- Does not keep track of traffic flows
  - Each packet is individually examined, regardless of past history
  - Traffic sent outside of an active session will traverse a stateless firewall

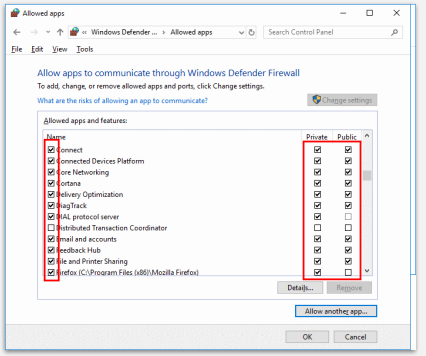
Stateful firewall

- Stateful firewalls remember the “state” of the session
  - Everything within a valid flow is allowed

Firewalls

Application-aware security devices

- The OSI Application Layer
  - All data in every packet
- Can be called different names
  - Application layer gateway
  - Stateful multilayer inspection
  - Deep packet inspection
- Requires some advanced decodes
  - Every packet must be analyzed and categorized before a security decision is determined



Firewalls

Firewall rules

- Access control lists (ACLs)
  - Allow or disallow traffic based on tuples
  - Groupings of categories
  - Source IP, Destination IP, port number, time of day, application, etc.
- A logical path
  - Usually top-to-bottom
- Can be very general or very specific
  - Specific rules are usually at the top
- Implicit deny
  - Most firewalls include a deny at the bottom
  - Even if you didn’t put one

VPN Concentrators

VPN Concentrators

VPN Concentrator

- Virtual Private Network
  - Encrypted (private) data traversing a public network
- Concentrator
  - Encryption/decryption access device
  - Often integrated into a firewall
- Many deployment options
  - Specialized cryptographic hardware
  - Software-based options available
- Used with client software
  - Sometimes built into the OS

VPN Concentrators

Remote access VPN

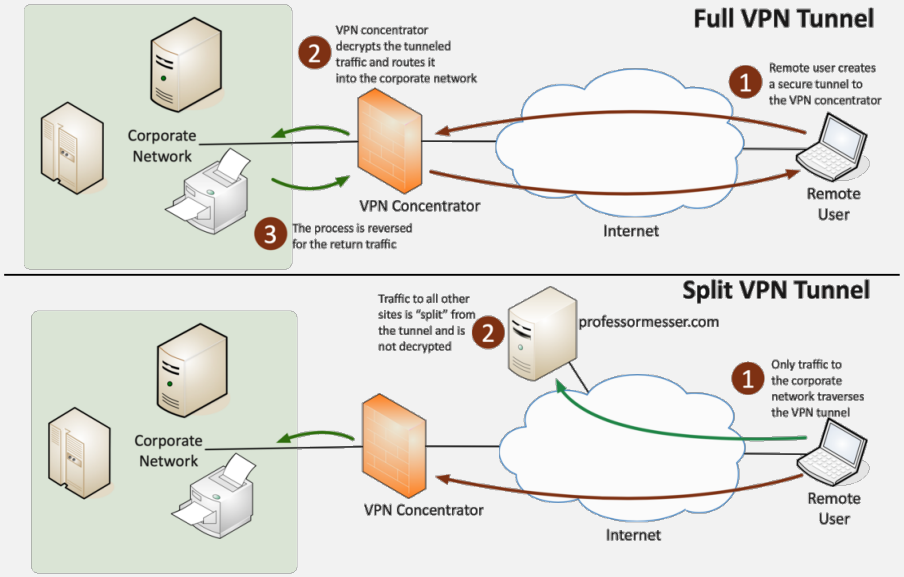
- On-demand access from a remote device
  - Software connects to a VPN concentrator
- Some software can be configured as always-on

VPN Concentrators

SSL VPN (Secure Sockets Layer VPN)

- Uses common SSL/TLS protocol (tcp/443)
  - (Almost) No firewall issues!
- No big VPN clients
  - Usually remote access communication
- Authenticate users
  - No requirement for digital certificates or shared passwords (like IPSec)
- Can be run from a browser or from a VPN client
  - Across many operating systems

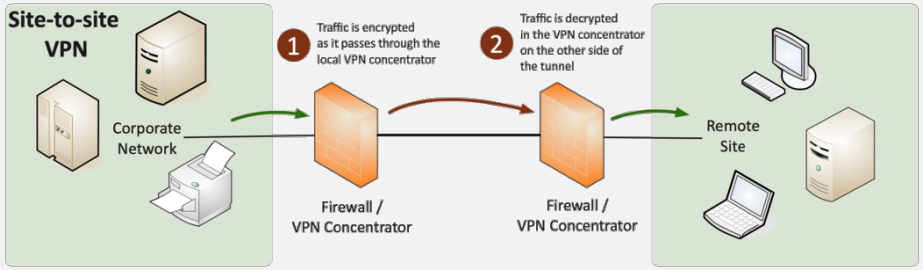
VPN Concentrators



VPN Concentrators

Site-to-site VPN

- Always-on
  - Or almost always
- Firewalls often act as VPN concentrators
  - Probably already have firewalls in place

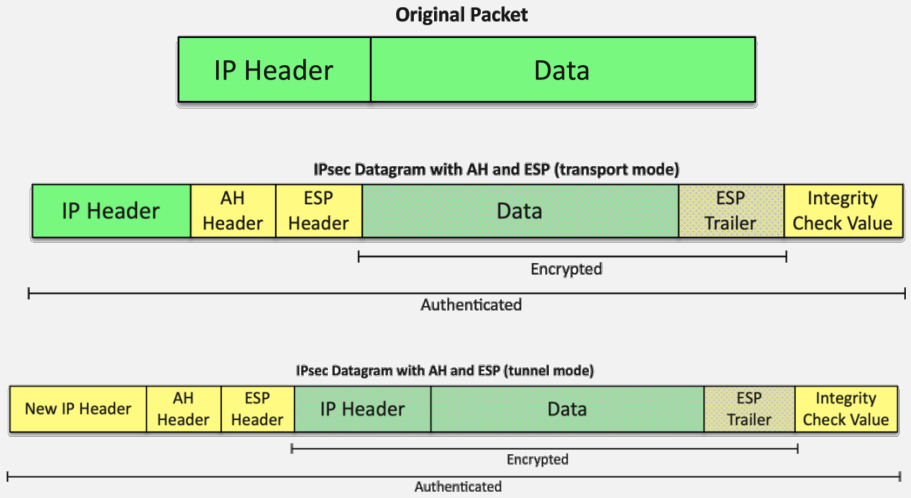


VPN Concentrators

IP Sec (Internet Protocol Security)

- Security for OSI Layer 3
  - Authentication and encryption for every packet
- Confidentiality and integrity/anti-replay
  - Encryption and packet signing
- Very standardized
  - Common to use multi-vendor implementations
- Two core IPSec protocols
  - Authentication Header (AH)
  - Encapsulation Security Payload (ESP)

VPN Concentrators



VPN Concentrators

Authentication Header

- Hash of the packet and a shared key
  - MD5, SHA-1, or SHA-2 are common
  - Adds the AH to the packet header
- Provides:
  - Data integrity, Origin authentication, Replay attack protection, Keyed-hash mechanism, No confidentiality/encryption

Encapsulation Security Payload (ESP)

- Encrypts the packet
  - MD5, SHA-1, or SHA-2 for hash, and 3DES or AES for encryption
  - Adds a header, a trailer, and an Integrity Check Value
- Provides:
  - Data confidentiality (encryption), Limited traffic flow confidentiality, Data integrity, Anti-replay protection

Network Intrusion Detection and Prevention Systems (IDS/IPS)

Network Intrusion Detection and Prevention (IDS/IPS)

N(IDS) and N(IPS)

- Intrusion Detection System / Intrusion Prevention System
  - Watch network traffic
- Intrusions
  - Exploits against operating systems, applications, etc.
  - Buffer overflows, cross-site scripting, other vulnerabilities
- Detection vs. Prevention
  - Detection – Alarm or alert
  - Prevention – Stop it before it gets into the network

Network Intrusion Detection and Prevention (IDS/IPS)

Passive monitoring

- Examine a copy of the traffic
  - Port mirror (SPAN), network tap
- No way to block (prevent) traffic

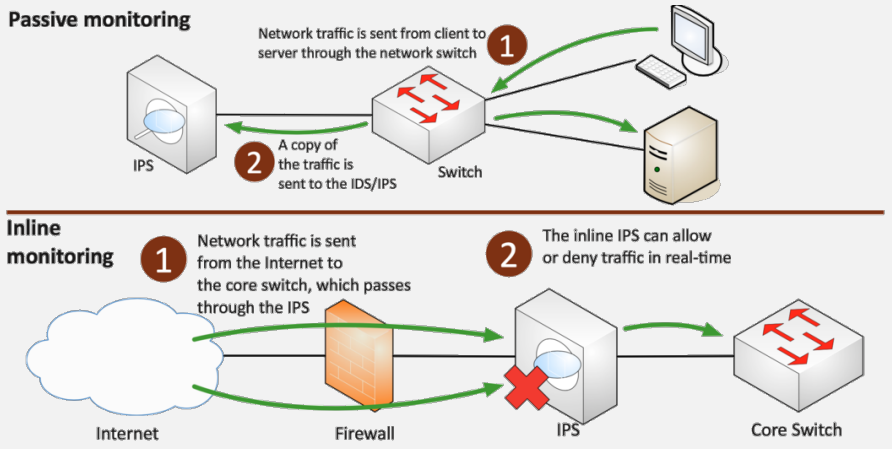
Out-of-band response

- When malicious traffic is identified, IPS sends TCP RST (reset) frames
  - After-the-fact
  - Limited UDP response available

Inline monitoring

- IDS/IPS sits physically inline
  - All traffic passes through the IDS/IPS

Network Intrusion Detection and Prevention



Network Intrusion Detection and Prevention (IDS/IPS)

In-band response

- Malicious traffic is immediately identified
  - Dropped at the IPS
  - Does not proceed through the network

Identification technologies

- Signature-based - Look for a perfect match
- Anomaly-based - Build a baseline of what's "normal"
- Behavior-based - Observe and report
- Heuristics - Use artificial intelligence to identify

Network Intrusion Detection and Prevention (IDS/IPS)

IDS/IPS Rules

- You determine what happens with unwanted traffic
  - Block, allow, send an alert, etc.
- Thousands of rules
  - Or more
- Rules can be customized by group
  - Or as individual rules
- This can take time to find the right balance
  - Security / alert "noise" / false positives

Network Intrusion Detection and Prevention (IDS/IPS)

False Positives

- A report that isn't true
  - A false alarm or mistaken identity
- IDS/IPS information
  - Only as good as the signatures
  - Some legitimate traffic could be marked as malicious
  - Time-consuming to research and resolve
- Workstation antivirus
  - April 2017: Webroot Antivirus
  - Windows files quarantined as malicious
  - Facebook and Bloomberg marked as phishing sites
- Consider a second opinion
  - http://www.VirusTotal.com

Network Intrusion Detection and Prevention (IDS/IPS)

False Negatives

- A report missed identifying something
  - You didn't get a notification
- Malicious traffic got through your defenses
  - You'll probably see the results of this
- It's difficult to know when this happens
  - It's completely silent
- Get catch/miss rates with industry tests
  - IPS, anti-virus

Router and Switch Security

Router and Switch Security

Router

- Routes traffic between IP subnets
- OSI layer 3 device
- Routers inside of switches sometimes called “layer 3 switches”
- Layer 2 = Switch ~ Layer 3 = Router
- Often connects diverse network types
- LAN, WAN, copper, fiber

Router and Switch Security

Access Control Lists (ACLs)

- Used to allow or deny traffic
  - Also used for NAT, QoS, etc.
- Defined on the ingress or egress of an interface
  - Incoming or outgoing
- ACLs evaluate on certain criteria
  - Source IP, Destination IP, TCP port numbers, UDP port numbers, ICMP
- Deny or permit
  - What happens when an ACL matches the traffic?
- ACLs have evolved through the years
  - Standard vs. Extended, numbered vs. named

Router and Switch Security

Anti-spoofing

- Prevent a bad guy from using someone else’s address
  - Man-in-the-middle, DDoS, etc.
- Filter reserved IP addresses
  - An RFC 1918 address should not be routed to or from the Internet
  - A simple ACL will work
- Enable Reverse Path Forwarding (RPF)
  - The response to an inbound packet should return the same way
  - If it doesn’t, then drop the packet right now

Router and Switch Security

Switches

- Bridging done in hardware
  - Application-specific integrated circuit (ASIC)
- An OSI layer 2 device
  - Forwards traffic based on data link address
- Many (many) ports
  - The core of an enterprise network
- High bandwidth
  - Many simultaneous packets

Router and Switch Security

Switch port security

- The inside of your network is relatively insecure
  - We often spend our time protecting against the outside
- Copper and wireless (and fiber)
  - It's all a conduit to your network
  - Wireless doesn't even have to be in the building
- It's often very easy to connect to the network
  - We want the conference rooms to be convenient

Router and Switch Security

Network Access Control (NAC)

- IEEE 802.1X - Port-based Network Access Control (NAC)
  - You don't get access until you authenticate
  - Makes extensive use of EAP and RADIUS
  - Extensible Authentication Protocol /Remote Authentication Dial In User Service
- We're talking about physical interfaces
  - Not TCP or UDP ports
- Administrative enable/disable
  - Disable your unused ports
- Duplicate MAC address checking
  - Stop the spoofers

Router and Switch Security

Loop Prevention

- Connect two switches to each other
  - They'll send traffic back and forth forever
  - There's no "counting" mechanism at the MAC layer
- This is an easy way to bring down a network
  - And somewhat difficult to troubleshoot
  - Relatively easy to resolve
- Spanning Tree Protocol
  - IEEE standard 802.1D to prevent loops in bridged (switched) networks (1990)
  - Created by Radia Perlman
  - Used practically everywhere

Router and Switch Security

Flood Guard

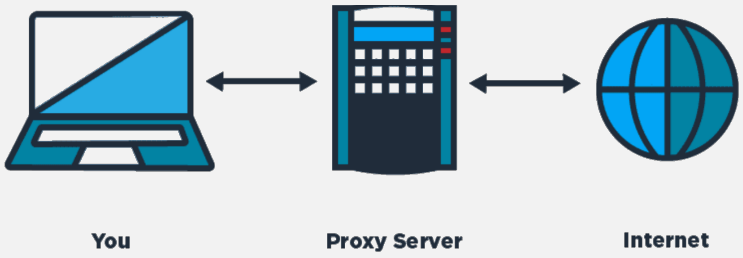
- Configure a maximum number of source MAC addresses on an interface
  - You decide how many is too many
  - You can also configure specific MAC addresses
- The switch monitors the number of unique MAC addresses
  - Maintains a list of every source MAC address
- Once you exceed the maximum, port security activates
  - Interface is usually disabled by default

Router and Switch Security

Layer 3 switches

- A switch (Layer 2) and router (Layer 3) in the same physical device
- Switching still operates at OSI Layer 2, routing still operates at OSI Layer 3
- There's nothing new or special happening here

Proxies



Proxies

Proxies

- Sits between the users and the external network
- Receives the user requests and sends the request on their behalf (the proxy)
- Useful for caching information, access control, URL filtering, content scanning
- Applications may need to know how to use the proxy (explicit)
- Some proxies are invisible (transparent)

Proxies

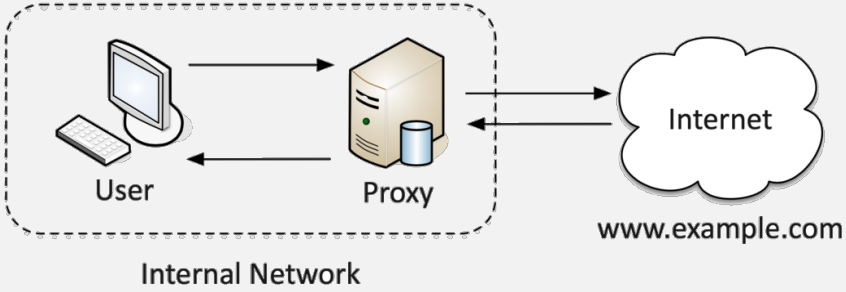
Application proxies

- One of the simplest “proxies” is NAT
  - A network-level proxy
- Most proxies in use are application proxies
  - The proxy understands the way the application works
- A proxy may only know one application
  - HTTP
- Many proxies are multipurpose proxies
  - HTTP, HTTPS, FTP, etc.

Proxies

Forward Proxy

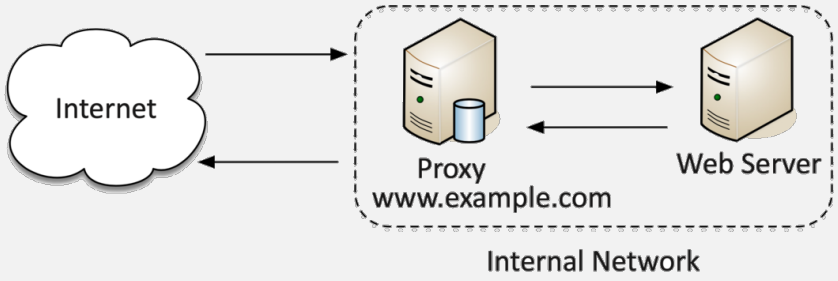
- An “internal proxy”
  - Commonly used to protect and control user access to the Internet



Proxies

Reverse Proxy

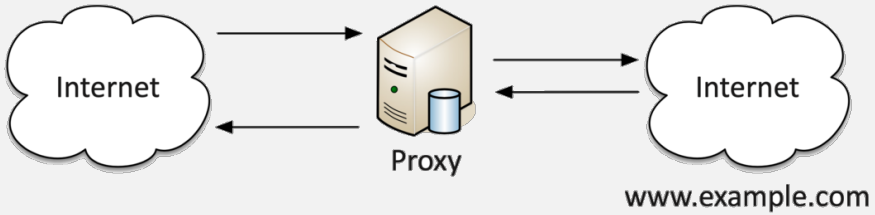
- Inbound traffic from the Internet to your internal service



Proxies

Open Proxy

- A third-party, uncontrolled proxy
  - Can be a significant security concern
  - Often used to circumvent existing security controls



Load Balancers

Load Balancers

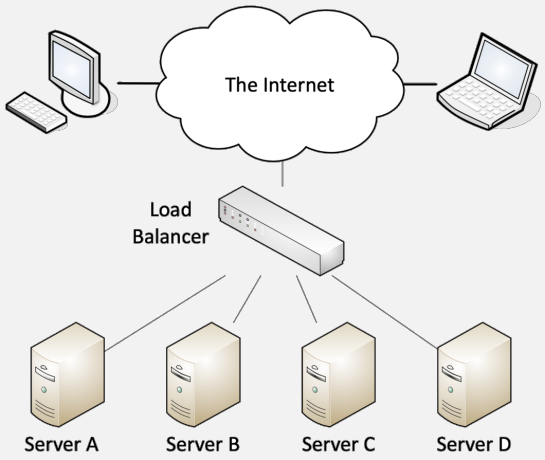
Balancing the Load

- Distribute the load
  - Multiple servers
  - Invisible to the end-user
- Large-scale implementations
  - Web server farms, database farms
- Fault tolerance
  - Very fast convergence

Load Balancers

Load Balancer

- Configurable load
  - Manage across servers
- TCP offload
  - Protocol overhead
- SSL offload
  - Encryption/Decryption
- Caching - Fast response
- Prioritization - QoS
- Content switching
  - Application-centric balancing



Load Balancers

Scheduling

- Round-robin
  - Each server is selected in turn
- Weighted round-robin
  - Prioritize the server use
- Dynamic round-robin
  - Monitor the server load and distributed to the server with the lowest use

Load Balancers

Active/Active load balancing

- Active/Active load balancingAffinity - A kinship, a likeness
- Many applications require communication to the same instance
  - Each user is “stuck” to the same server
  - Tracked through IP address or session IDs
  - Source affinity

Active/passive load balancing

- Some servers are active
  - Others are on standby
- If an active server fails, the passive server takes its place

Access Points

Access Points

Wireless Access Point (WAP)

- Not a wireless router
  - A wireless router is a router and a WAP in a single device
    - Wifi router = router + access point
- WAP is a bridge
  - Extends the wired network onto the wireless network
  - WAP is an OSI layer 2 device

Access Points

SSID management

- Service Set Identifier
  - Name of the wireless network
  - LINKSYS, DEFAULT, NETGEAR
- Change the SSID to something not-so obvious
- Disable SSID broadcasting?
  - SSID is easily determined through wireless network analysis
  - Security through obscurity

Access Points

MAC filtering

- Media Access Control
  - The “hardware” address
- Limit access through the physical hardware address
  - Keeps the neighbors out
  - Additional administration with visitors
- Easy to find working MAC addresses through wireless LAN analysis
  - MAC addresses can be spoofed
  - Free open-source software
- Security through obscurity

Access Points

Power Level Controls

- Usually a wireless configuration
  - Set it as low as you can
- How low is low?
  - This might require some additional study
- Consider the receiver
  - High-gain antennas can hear a lot
  - Location, location, location

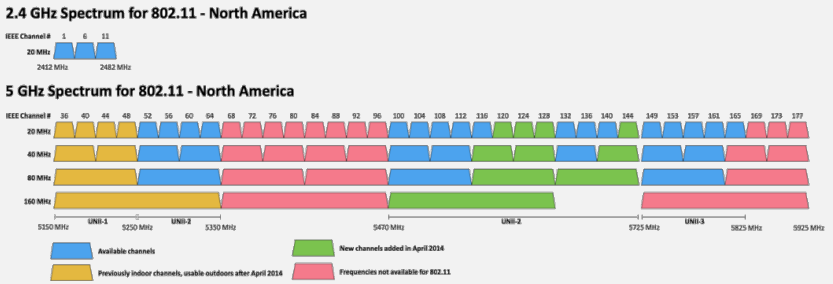
Access Points

Band selection and bandwidth

- Throughput
  - Maximum theoretical throughputs
  - Actual throughput can vary widely
- Frequency
  - 2.4 GHz and 5 GHz
    - sometimes both
- Distance
  - A combination of antennas
  - Attenuation
- Channels
  - Non-overlapping channels would be ideal

Wireless Network Technologies

- Omnidirectional antennas
- Directional antennas



Access Points

Wireless LAN controllers

- Centralized management of WAPs
  - A single “pane of glass”
- Deploy new access points
- Performance and security monitoring
- Configure and deploy changes to all sites
- Report on access point use
- Usually a proprietary system
  - The wireless controller is paired with the access points

Access Points

Managing wireless configurations

- LWAPP
  - Lightweight Access Point Protocol
  - Cisco proprietary - CAPWAP is an RFC standard, based on LWAPP
  - Manage multiple access points simultaneously
- Thick/fat access points
  - The access point handles most wireless tasks
  - The switch is not wireless-aware
- Thin access points
  - Just enough to be 802.11 wireless
  - The intelligence is in the switch
  - Less expensive

SIEM

SIEM

SIEM

- Security Information and Event Management
  - Security events and information
- Security alerts
  - Real-time information
- Log aggregation and long-term storage
  - Usually includes advanced reporting features
- Data correlation
  - Link diverse data types
- Forensic analysis
  - Gather details after an event

SIEM

Time Synchronization

- Switches, routers, firewalls, servers, workstations
  - Every device has its own clock
- Synchronizing the clocks becomes critical
  - Log files, authentication information, outage details
- Automatic update with NTP (Network Time Protocol)
  - No flashing 12:00 lights
- Flexible - You control how clocks are updated
- Very accurate
  - Accuracy is better than 1 millisecond on a local network

SIEM

Syslog

- Standard for message logging
  - Diverse systems, consolidated log
- Usually a central logging receiver
  - Integrated into the SIEM
- You're going to need a lot of disk space
  - No, more. More than that.
- WORM drive technology
  - Write Once Read Many
  - Protect important security logs

SIEM

Event de-duplication

- Event storms
  - When it rains, it pours
- Filter out the noise
  - Focus on the real problems
- Flapping (down/up/down)
  - Timers used to suppress ongoing messages
- Configurable suppression
  - Define your own event handling
  - Useful for automating responses

SIEM

Automated alerting and triggers

- Constant information flow
  - Important metrics in the incoming logs
- Track important statistics
  - Exceptions can be identified
- Send alerts when problems are found
  - Email, text, call, etc.
- Create triggers to automate responses
  - Open a ticket, reboot a server

Data Loss Prevention

Data Loss Prevention

Data Loss Prevention (DLP)

- Where's your data?
  - Social Security numbers, credit card numbers, medical records
- Stop the data before the bad guys get it - Data "leakage"
- So many sources, so many destinations
  - Often requires multiple solutions in different places

Data Loss Prevention (DLP) systems

- On your computer - Data in use, Endpoint DLP
- On your network - Data in motion
- On your server - Data at rest

Data Loss Prevention

USB Blocking

- DLP on a workstation - Allow or deny certain tasks
- November 2008 - U.S. Department of Defense
  - Worm virus "agent.btz" replicates using USB storage
  - Bans removable flash media and storage devices
- All devices had to be updated -
  - Local DLP agent handled USB blocking
- Ban was lifted in February 2010 - Replaced with strict guidelines

Data Loss Prevention

Cloud based DLP

- Located between users and the Internet
  - Watch every byte of network traffic
  - No hardware, no software
- Block custom defined data strings
  - Unique data for your organization
- Manage access to URLs - Prevent file transfers to cloud storage
- Block viruses and malware - Anything traversing the network

Data Loss Prevention

DLP and email

- Email continues to be the most critical risk vector
  - Inbound threats, outbound data loss
- Check every email inbound and outbound
  - Internal system or cloud-based
- Inbound
  - Block keywords, identify impostors, quarantine email messages
- Outbound
  - Fake wire transfers, W-2 transmissions, employee information

Data Loss Prevention

Emailing a spreadsheet template

- November 2017
- Boeing employee emails spouse a spreadsheet to use as a template
- Contained the personal information of 36,000 Boeing employees
  - In hidden columns
  - Social security numbers, date of birth, etc.
- Boeing sells its own DLP software
  - But only uses it for classified work

Network Access Control

Network Access Control

Edge vs. access control

- Control at the edge
  - Your Internet link
  - Managed primarily through firewall rules
  - Firewall rules rarely change
- Access control
  - Control from wherever you are
    - Inside or outside
  - Access can be based on many rules
    - By user, group, location, application, etc.
  - Access can be easily revoked or changed
    - Change your security posture at any time

Network Access Control

Posture assessment

- You can't trust everyone's computer
  - BYOD (Bring Your Own Device)
  - Malware infections / missing anti-malware
  - Unauthorized applications
- Before connecting to the network, perform a health check
  - Is it a trusted device?
  - Is it running anti-virus? Which one? Is it updated?
  - Are the corporate applications installed?
  - Is it a mobile device? Is the disk encrypted?
  - The type of device doesn't matter
  - Windows, Mac, Linux, iOS, Android

Network Access Control

Health checks/posture assessment

- Persistent agents
  - Permanently installed onto a system
  - Periodic updates may be required
- Dissolvable agents
  - No installation is required
  - Runs during the posture assessment
  - Terminates when no longer required
- Agentless NAC
  - Integrated with Active Directory
  - Checks are made during login and logoff
  - Can't be scheduled

Network Access Control

Failing assessment

- What happens when a posture assessment fails?
  - Too dangerous to allow access
- Quarantine network, notify administrators
  - Just enough network access to fix the issue
- Once resolved, try again
  - May require additional fixes

Mail Gateways

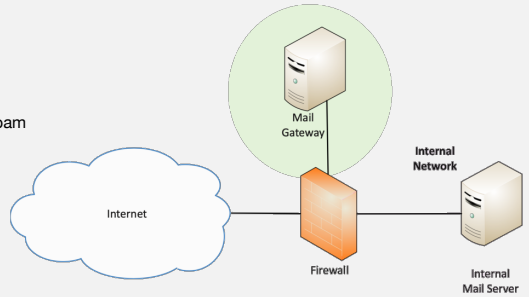
Mail Gateways

Mail gateways

- Unsolicited email
  - Stop it at the gateway before it reaches the user
  - On-site or cloud-based

Email filtering

- Inbound and outbound email
  - Examine the traffic
- Unsolicited email advertisements - Spam
- Control of phishing attempts
  - Email is a large attack vector
- Anti-virus - Block bad attachments
- DLP - Data Loss Prevention
  - Block confidential information in emails



Mail Gateways

Identifying spam

- Whitelist
  - Only receive email from trusted senders
- SMTP standards checking
  - Block anything that doesn't follow RFC standards
- rDNS - Reverse DNS
  - Block email where the sender's domain doesn't match the IP address
- Tarpitting
  - Intentionally slow down the server conversation
- Recipient filtering
  - Block all email not addressed to a valid recipient email address

Mail Gateways

Email Encryption

- Mail can be easily intercepted
  - And most mail is not encrypted
- Send and receive sensitive information
  - The encryption mechanisms aren't always seamless
- Encryption can be required on the gateway
  - Based on policy
  - Force the encryption, send a password to the sender
  - Send a text message to the recipient
- Many email clients support encryption
  - Email gateway recognizes the encryption

Other Security Devices/ Hardware

Other Security Devices

SSL accelerators

- You have a server farm full of web servers
- Asymmetric encryption is hard
  - Much more computationally intense than symmetric encryption
- The SSL handshake uses asymmetric encryption
  - Transfers the symmetric key using the asymmetric encryption
- Offload the handshake process to hardware
  - May use a different device
  - SSL offload, SSL termination
- Symmetric conversation continues
  - May not encrypt at all between the accelerator and the web server

Other Security Devices

SSL/TLS decryption

- Commonly used to examine outgoing SSL
  - For example, from your computer to your bank
- Wait a second. Examine encrypted traffic? Is that possible?
- SSL/TLS relies on trust
  - Without trust, none of this works

Other Security Devices

Trust me, I'm SSL

- Your browser contains a list of trusted CAs
- Your browser doesn't trust a web site unless a CA has signed the web server's encryption certificate
  - The web site pays some money to the CA for this
- The CA has ostensibly performed some checks
  - Validated against the DNS record, phone call, etc.
- Your browser checks the web server's certificate
  - If it's signed by a trusted CA, the encryption works seamlessly

Other Security Devices

Hardware Security Module (HSM)

- High-end cryptographic hardware
  - Plug-in card or separate hardware device
- Key backup
  - Secured storage
- Cryptographic accelerators
  - Offload that CPU overhead from other devices
- Used in large environments
  - Clusters, redundant power

Other Security Devices

Media gateways

- Converts between PSTN (Public Switched Telephone Network) and VoIP
  - ISDN trunk on one side, Ethernet with VoIP on the other
  - SIP on one side, H.323 on the other
  - The combinations are many and varied
- Security is a significant concern
  - Disable all voice communication (DoS)
  - Make outbound calls
    - Spam, malicious services
  - Listen to voice communication
    - Corporate espionage

Software Security Tools

Software Security Tools

Passive vs. active tools

- Passive security
  - You're a network ninja
- Watch the packets go by
  - There's a lot to learn
  - Top talkers, servers, clients, applications, operating systems, services
- Active security
  - Send traffic to a device, watch the results
  - Query a login page
  - Try a known vulnerability
  - Check account access

Software Security Tools

Protocol analyzers

- Solve complex application issues
  - Get into the details
- Gathers packets on the network
  - Or in the air
  - Sometimes built into the device
- View traffic patterns
  - Identify unknown traffic
  - Verify packet filtering and security controls
- Large scale storage
  - Big data analytics

Software Security Tools

Network/Port Scanners

- Active - scan for IP addresses and open ports
  - And operating systems, services, etc.
- Pick a range of IP addresses
  - See who responds to the scan
- Visually map the network
  - Gather information on each device
  - IP, operating system, services, etc.
- Rogue system detection
  - It's difficult to hide from a layer 2 ARP
- Nmap/Zenmap, Angry IP Scanner

Software Security Tools

Wireless scanners and crackers

- Wireless monitoring - Packet capturing
- Wireless attacks
  - Rogue access point, deauthentication attacks, etc.
- Cracking - Find a wireless network key
  - WEP - Cryptographic vulnerabilities
    - Relatively straightforward
- WPA1 PSK and WPA2 PSK
  - Dictionary brute force, rainbow tables
- Many open source projects - Aircrack-ng Suite, Fern

Software Security Tools

Password crackers

- Passwords are stored as hashes - It's a one-way trip
- Some are stored without much complexity
  - Relatively straightforward to brute-force a weak hash
- Get the hashes - Can be the hardest part
- Use a good wordlist or use rainbow tables
  - Common passwords, multiple languages, etc.
- Many tools available
  - John the Ripper, Ophcrack

Software Security Tools

Vulnerability scanners

- Did you miss a security patch?
  - We'll find it
- Minimally invasive, but still active
  - Unlike a penetration test
- Gather as much information as possible
  - We'll separate wheat from chaff later
- Microsoft Baseline Security Analyzer, Tenable Nessus
  - Scan one or many devices
  - Automate the process, report on findings

Software Security Tools

Configuration compliance scanners

- Do your devices meet your minimum security configurations?
  - Need to comply with internal requirements or industry regulations
- Check for various configurations
  - Operating system version, installed applications, network settings, anti-virus/anti-malware settings and versions, server configurations, etc.
- Auditing may be ongoing
  - Report on current status, identify changes over time
  - Integrated with login process and/or VPN connection

Software Security Tools

Exploitation frameworks

- So many opportunities for exploits
  - The browser, operating system, applications, embedded devices, etc.
- How can you build an exploit?
  - Try many different techniques
- Many different frameworks
  - BeEF - The Browser Exploitation Framework Project
  - RouterSploit - Router Exploitation Framework
  - Metasploit - Build your own vulnerability tests or use modules in the existing exploit database

Software Security Tools

Data sanitization tools

- Time to upgrade that hard drive
  - What happens to the data on the old drive?
- Overwrite the data once, and it's gone
  - One and done
- Sanitize entire drives
  - Darik's Boot and Nuke (DBAN)
- Sanitize individual files or folders
  - Microsoft SDelete
- Don't forget about caches and temporary files
  - Data is stored in many places

Software Security Tools

Stenoganography tools

- Greek for "concealed writing"
  - Security through obscurity
- Message is invisible
  - But it's really there
- The covertext
  - The container document or file

Software Security Tools

Common steganography techniques

- Network based
  - Embed messages in TCP packets
- Use an image
  - Embed the message in the image itself
- Invisible watermarks
  - Yellow dots on printers
  - Serial number and timestamp

Software Security Tools

Honey pots

- Attract the bad guys - And trap them there
- The bad guys are probably a machine
  - Makes for interesting recon

Honeynets

- Create a virtual world to explore
- Many different options
  - http://www.projecthoneypot.org/, honeyd
- Constant battle to discern the real from the fake

Software Security Tools

Backup Utilities

- Protect from unexpected downtime
  - Malware infection, ransomware, server defacement
- Real-time file sync - rsync
- Regular partial backups
  - Hourly incremental backups
- Full backups
  - Complete file backups
  - System images
- Complete coverage, fast recovery

Software Security Tools

Banner grabbing

- Applications can be chatty
  - They sometimes say too much
- The banner is always there
  - But usually behind the scenes
- Capture it with telnet, nc, or an automated tool (i.e., Nmap)

CSF 434/534: Advanced Network and System Security

Week 05 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes