



# Security+

## Domain 4: Security Operations Part 1

SY0-701

# Brian Olliff

Defensive Engineering Instructor

---

# Topics

## **Security Techniques**

- **Endpoints**
- **Servers**
- **Wireless**
- **Mobile**
- **Applications**

## **Asset Management**

## **Vulnerability ID/Analysis**

## **Logging & Monitoring**

## **Network Security**

- **Firewalls**
- **IDS/IPS**
- **NAC**

# Learning Objectives

- Be able to apply security techniques to various systems & devices
  - + Endpoints and servers
  - + Wireless and mobile systems
- Understand the importance, and steps in, asset management processes
- Be able to explain the vulnerability management process
  - + Identification and analysis
  - + Response and remediation
- Understand logging, monitoring, and alerting systems
- Be able to apply various network security techniques
  - + Firewall security
  - + Intrusion detection/prevention systems

# Endpoint & Server Hardening



# Secure Baselines

---

- Standard configurations & settings
  - Network devices, software, workstations, servers, etc
- Establish consistent configurations/rules for configuration & security
- CIS Benchmarks (Center for Internet Security)
  - Published best practice guides
  - Available for various compliance programs
    - PCI-DSS, NIST 800-53, SOX, ISO 27000
  - Product-focused benchmarks (specific applications, servers, devices, etc)
- Configuration management tools used to maintain
  - Manage, deploy, and ensure compliance with baselines
  - SCAP - Security Content Automation Protocol

## What is Security Hardening?

---

- All devices, software, etc have default settings when purchased
  - Tools, techniques, best practices to reduce vulnerability
  - Goal: Reduce security risk by minimizing attack surface
  - Improving system security by changing default configuration
  - Remove extra functions and applications
  - Disable unnecessary services
  - Change default passwords/accounts
- 
- Awareness of current attack vectors
  - Awareness of your environment and attack surface
  - Careful balance between security and usability

# Standard Hardening Recommendations

---

- Recommendations apply to any type of device/system
- Use baseline configurations and checklists
- Change all default passwords (usernames if possible)
- Close unused & unnecessary network ports
  - Only use secure management protocols
- Stop/disable any unneeded services
- Routinely audit systems to ensure controls still adequate
- Audit and update baselines as needed



## Switches & Routers

---

- Disable unused services and interfaces (telnet, HTTP, etc)
- Secure management protocols
  - SSH instead of telnet
  - HTTPS instead of HTTP
- ACLs (access control lists) to restrict access to device
- Logging & monitoring
  - Repeated login failures, configuration changes, etc
- Port security
  - MAC filtering, 802.1x, etc
- Physically secure device locations

# Servers

---

- Ensure security patches and updates applied regularly
  - Security improvements, vulnerability remediation, etc
- Configure firewalls and IPS systems
  - Network or host-based
- Use strong passwords, MFA, PAM (privileged access management)
- Logging & monitoring
  - Repeated login failures, config changes (similar to network equipment)
- Install (and config/monitor) AV/EDR
- Physically secure hardware

## Workstations & Endpoints

---

- Standard hardening steps
- Disk encryption for workstations
  - Protects sensitive data and cached credentials
- Limit (or eliminate) administrative access for standard users
- Restrict applications that can be installed
- Prevent users from changing critical configuration settings
  - Software updates/patches
  - Device lock/logout times
  - Firewall settings
  - Endpoint protection software
- Restrict access to removable media usage

# Embedded System Hardening



# Embedded Systems & RTOS

---

- Selection of controls based on security and integrity of OS
  - Based on guidelines, best practices, benchmarks
- Standard hardening strategies
  - Regular system updates
  - Disable unnecessary services
  - Change default credentials
  - Limit network access
- Network-level protections
  - Segmentation is most important & effective
  - Addition of firewalls, IPS
  - Secure management protocols (SSH, TLS, etc)
- Regular audits and tests are required

# ICS & SCADA

---

- IT vs OT (Information Technology, Operational Technology)
  - IT manages data
  - OT devices control physical world
- Systems often interface with critical infrastructure
  - Utility generation
  - Systems handling hazardous materials
- Control network separated from rest of enterprise network
  - IT and OT networks must be separate
- Careful testing of all updates (software, firmware, etc)
- Heavy restrictions for removable devices (USB drives)
- Unidirectional gateway (data diode)
  - Only permits network traffic to flow in one direction

# Internet of Things (IoT) Devices

---

- Common in most organizations (and households)
- Types of devices
  - Thermostats
  - Media devices (AppleTV, Chromecast, Roku, etc)
  - Security cameras, doorbell cameras
  - Smoke detectors, security systems, smart locks
  - HVAC systems (also fall into ICS category)
- Securing can be difficult
  - Use same general guidelines as other systems
- Network segmentation is critical
- If possible, disallow access to enterprise network entirely

# Wireless Security





# Installation Considerations

---

- WAP (Wireless access point)/AP
  - Devices with radios that generate wireless signal
  - Each wireless network identified by SSID (service set identifier)
- Placement is important
  - Avoid interference between APs operating on same channel/frequency
- Site survey
  - Collecting info about location to properly build wireless infrastructure
  - Usually starts with floor plan
    - Takes into consideration walls, floors, other electronics
  - Measures wireless infrastructure to identify strong & weak signal locations
- Heat map
  - Visual representation of strong/weak signal locations
  - Used to tweak AP settings - adjust power, change channels, add/relocate

# Cryptographic Protocols

---

- Older standards used wired equivalent privacy (WEP)
  - Insecure and should never be used
- WPA (Wi-Fi Protected Access) is the current standard
  - Can use PSK (Pre-shared key) or enterprise-level authentication
  - WPA1
    - Better than WEP, but also no longer secure enough
  - WPA2
    - Uses AES (Advanced Encryption Standard) ciphers with 128-bit keys
    - CCMP - Provides authenticated encryption
    - Still has weaknesses, no longer the standard

# Cryptographic Protocols

---

- WPS - Wi-Fi Protected Setup
  - Used with WPA2
  - Button on AP (sometimes device), and PIN
  - Generates random SSID and PSK for connection
  - Vulnerable to brute force attacks
- WPA3
  - SAE - Simultaneous Authentication of Equals
    - Replaces WPA-PSK (pre-shared key)
    - Wi-Fi password cannot be intercepted from captured data
  - Enhanced Open - all traffic encrypted, even when not using password
  - AES CCMP replaced with GCMP
  - Wi-Fi Easy Connect - Connect devices by scanning QR code
    - Replaces WPS - Wi-Fi Protected Setup

# Authentication Protocols

---

- WPA2 - PSK authentication
  - Passphrase that generates key to encrypt communications
  - All clients use same key to connect
- WPA3
  - Still uses passphrase, but different means of generating session keys
- Enterprise authentication
  - Used on WPA2/WPA3-Enterprise
  - 802.1x authentication (same as switches)
    - Uses RADIUS server to verify credentials
    - Supports multiple EAP types (Extensible Authentication Protocol)
  - Each user uses their own credentials to connect

## RADIUS Authentication Process

---

- AP configured with RADIUS server IP and shared secret
    - AP is RADIUS client
1. Wireless device (supplicant) connects to AP
  2. AP prompts supplicant for credentials
  3. Supplicant submits credentials, encrypted using shared secret
  4. RADIUS client sends to AAA server
  5. AAA server decrypts using same shared secret
  6. If supplicant authenticated, AAA server returns Access-Accept packet

# Mobile Security



# Deployment Models

---

- BYOD (Bring your own device)
  - Device is owned by employee
  - Will be required to meet organizational requirements
  - Security profile/software required on device for management
  - Corporate apps installed as needed by users
  - Highest security risk to organization
- Corporate owned
  - COBO (Corporate owned, business only)
  - COPE (Corporate owned, personally-enabled)
    - Device is owned by the organization
    - Allowed for personal usage as well
    - Acceptable use policies apply
  - CYOD (Choose your own device)
    - Similar to COPE, but employees choose device from available list

# Mobile Device Management (MDM)

---

- Central management of mobile devices
- Set and enforce policies for security, applications, mobile features, etc
  - Authentication requirements (PIN, password, etc)
  - Mandatory applications on device & allowed application list
  - Email account configuration
  - Camera usage, bluetooth settings, etc
- Often allows for remote full/selective wiping of devices
- Can be coupled with mobile application management (MAM)
  - Sets policies for applications that access/process company data
  - Prevent data transfer to personal apps
  - Often used with BYOD and corporate-owned devices



# Connection Methods

---

- Cellular
  - Connection not controlled by organization
  - Policies to restrict data transmitted over cellular
    - Ex: require VPN for certain data types or network locations
- Wi-Fi
  - Strong enterprise networks can reduce risk of eavesdropping
  - Ad hoc - devices connect to each other, non-permanent
  - Wi-Fi Direct - one-to-one connections, uses WPS
  - Tethering - sharing cellular connection over wireless (hotspot)
    - Can also use Bluetooth or USB (one device at a time)

## Short-range Connectivity

---

- Bluetooth
  - Several security risks
    - Device discovery - allows connection to other nearby devices
      - Non discoverable devices can still be detected
    - Authentication - usually simple PIN (sometimes default of 0000)
    - Malware and vulnerabilities
    - Bluejacking - unsolicited message over Bluetooth (w/o authentication)
- NFC (near-field communication)
  - Used for various purposes (payments, read passive tags, exchange contacts)
  - No encryption in communication
  - Malicious NFC tags
  - Attackers can pick up RF signals from distance
  - NFC skimming

# Location Services

---

- Uses network services to determine physical location of device
  - GPS - uses satellites to determine latitude and longitude
  - IPS - uses other network devices to triangulate location
    - Wireless APs, cell towers, Bluetooth beacons, etc
- Geofencing - virtual boundary created based on physical location
  - Limit access to resources based on location
  - Ex: Disable camera/microphone while in restricted security zone
- Privacy concerns with location
  - Careful protection of data required
  - Storing location data may have regulatory restrictions

# Application Security



# Secure Coding Techniques

---

- Input validation
  - User input fields can be abused for injection attacks (SQLi, etc)
  - Field entries should be checked to ensure info is appropriate
  - Client side - checked before sent to server
  - Server side - checked by server, but before acceptance and processing
  - Types
    - Allowlist, blocklist, data type, range, regex, encoding
- Secure cookies
  - All cookies should have an expiration date
  - Attributes can be set to implement
  - Secure - only sent over HTTPS
  - HttpOnly - prevent client-side scripts from accessing
  - SameSite - limit where/when cookies are sent

# Secure Coding Techniques

---

- Static code analysis
  - Examine source code to identify potential issues
    - Vulnerabilities, errors, poor practice, etc
  - Helps to catch issues early in dev cycle
  - Tools to assist with automation - check against specified rules
- Code signing
  - Use digital signature to verify integrity and authenticity
  - Same digital signature process
    - Private key to create hash of code
    - Requires publicly trusted certificate
  - Does not necessarily mean software is safe - malware can be signed

# Sandboxing

---

- Running software in isolated environment
  - Running processes can be isolated from each other
- Multiple uses and purposes
  - Software testing and debugging
    - Development or security analysis
  - Browser tab isolation
  - Mobile applications
  - Virtual machines and containers
- Frequently used in security operations
  - Testing suspected malicious software
  - Analyze and understand malware processes

## Other Application Protections

---

- Proper error handling
  - Application should behave in controlled manner with errors/exceptions
  - Structured exception handler (SEH) - tells application what to do
- Secure data handling to prevent unnecessary exposure
  - Encryption at rest and in transit
- Monitoring
  - Log errors and exceptions
  - Applications written with ability to send logs to external systems
  - Integrated monitoring for possible security events
    - Multiple login failures
    - Unusual data transfer



# Asset Management



# Asset Procurement

---

- Requires policies and processes in place to properly manage
- Applies to product & service purchases
  - And contract management
- Authorized vendor/supplier lists
  - Reputable, well-known vendors that prioritize security
- Prioritize purchases that integrate well with existing infrastructure
  - Firewalls, IPS, SIEM, etc
  - Strong security controls built in
- TCO - Total cost of ownership
  - How much will this product/service cost over its entire lifetime?
  - Maintenance, updates, potential security incidents

# Assignment and Classification

---

- Assignment
  - Asset owners - individuals/departments responsible for assets
  - Establishes accountability for equipment/software
  - Helps ensure proper management and protection of assets
- Classification
  - Organizing by value, purpose, criticality, etc
  - Placing into categories helps organize and manage security controls
    - Ex: different baselines for specific purpose devices
- Require periodic reviews and audits
  - Assets are purchased, decommissioned, moved

# Monitoring and Tracking

---

- Inventory as primary method of tracking
  - Full list of ALL assets
  - Network devices, servers, workstations, software, etc
- Track location, owner, status, patch level, etc
- Multiple methods of enumerating devices
  - Manual inventory process
  - Network scanning
  - Asset management software
  - Configuration management database
  - MDM (for mobile devices)
  - Cloud asset discovery

# Asset Decommissioning

---

- Secure methods to dispose/retire assets while meeting compliance reqs
- Normally focus on data
  - Files, DBs, configurations, scanned documents, etc
- Sanitization
  - Removing sensitive information from storage
  - Specialized techniques - wiping, degaussing, encryption, etc
  - Data should be unrecoverable after process complete
- Destruction
  - Physical or electronic elimination
    - Shredding, crushing, incinerating
    - Overwriting multiple times, degaussing
- Certification
  - Documentation and verification of data sanitization or destruction

# Identifying Vulnerabilities



# Vulnerability Scans

---

- System designed to test hosts (network, server, etc)
  - Checks open ports, running services, patches, configurations, etc
- Uses vulnerability database to identify potential vulnerabilities from scan
  - Can assist with finding missing patches, configuration errors, etc
- Requires good inventory of systems on network
  - Some scanners will assist with compiling
- Process
  - Scans run against identified targets
  - Report compiled from scanner
    - Each result is categorized and assigned a score
  - Analysis to identify remediation steps/false positives
- Scanners require continuous updates (vulnerability feeds)

## Types of Vulnerability Scans

---

- Non-credentialed scan (non authenticated)
  - Does not require username/password on device
  - Equivalent of unprivileged user/attacker
  - Will not be able to detect all vulnerabilities on host
  - Commonly used for external scans/web app scans
- Credentialed scan (authenticated)
  - Requires account configured on host that scanner uses
    - Can restrict permissions based on appropriate needs
  - Allows more in-depth results and analysis
  - Misconfigurations, security setting issues, etc
  - Equivalent of privileged user (compromised account, etc)



# Application Scanning

---

- Specific scanning method to identify application vulnerabilities
  - Frequently used when developing applications
- Evaluates code/behavior of individual application
- Static analysis
  - Review of application code without running program
- Dynamic analysis
  - Analysis while application is running
  - Useful for testing for injection vulns, improper input validation, etc
- Package monitoring - assess security of 3rd party packages, libraries, etc
  - SBOM - Software bill of materials
  - Supply chain risk management

# Threat Intelligence

---

- Threat feeds
  - Real-time info about threats and vulnerabilities, from multiple sources
  - Provide data that vulnerability scanners do not
  - Assist with targeting remediation efforts and security controls
- Open source intelligence (OSINT)
  - Publicly available information
  - Blogs, social media, forums, dark web, etc
- Proprietary/closed sources
  - Research and data available as paid subscription to commercial platform
  - Information usually much more detailed, possibly provided earlier
- Information sharing organizations
  - Groups that specialize in exchanging data about emerging threats/vulns

# Deep/Dark Web

---

- Deep web - any part of web not indexed by search engine
  - Designed to be “hidden” from normal browsers, but can be easily found
- Dark net
  - Network that overlays traditional internet
  - Requires specialized software to access
  - Typically offers anonymous usage, isolation from 3rd party analysis
- Dark web
  - Sites & content accessible only on dark net - continuously changing
  - Typically not searchable, must know specific URLs
  - Can provide valuable research information
  - Not only for illegal activity

## Other Identification Methods

---

- Penetration testing (pen test)
  - Attempt to breach organization's network
  - More in-depth than vulnerability scanning, demonstrates impact
  - Can discover vulnerabilities that scanners might miss
    - Configuration errors, application design, etc
    - Chained vulnerability exploits
  - Three main types of pen tests
    - Unknown environment (black box)
    - Known environment (white box)
    - Partially known environment (grey box)
- Audits
  - Examine code, features, products, policies, supply chain
  - Often based on frameworks and standards

# Bug Bounties

---

- Organization offers incentives for vulnerability discovery and reporting
- May be performed by individuals or teams
- Typically public programs to attract diverse skill sets/perspectives
- Responsible disclosure
  - Programs established to encourage vulnerability reporting
  - Allows organizations change to remediate before exploits available
  - Guidelines for how to report
  - Goal is to encourage researchers to not initially publicly disclose

# Vulnerability Analysis



## CVE (Common Vulnerabilities & Exposures)

---

- Developed and operated by MITRE
- Identify, define, and catalog publicly disclosed vulnerabilities
- CVE Record - CVE-YYYY-####
  - YYYY: Year the vulnerability was identified
  - ####: At least 4 digits to identify vulnerability (in order discovered)
  - Description of vulnerability
  - Reference URLs
  - Date entry was created
- Feeds into NVD (National Vulnerability Database, run by NIST)
  - CVSS score - numerical indication of severity

# CVSS (Common Vulnerability Scoring System)

---

- Standard for assigning scores to vulnerabilities
- Based on characteristics of vulnerability
  - Does it require local network access to exploit?
  - Is user intervention required?
- Severity levels
  - Non - 0
  - Low - 0.1 - 3.9
  - Medium - 4.0 - 6.9
  - High - 7.0 - 8.9
  - Critical - 9.0 - 10



# Processing Vulnerabilities

---

- Identify false positives
  - Item identified by scanner as vulnerability, but is not
  - Firewall port identified as being open, but no listening server
  - Software identified as vulnerable, but not installed
- False negatives
  - Vulnerabilities NOT reported, but actually exist
  - Ex: Vulnerable software on system, but scan causes software to crash
  - Updates to scanner software & repeated scans can help eliminate
- Prioritization
  - Highest severity, most critical software
  - Highest risk to organization is most important
  - Severity, ease of exploit, potential impact, etc

## Analysis Considerations

---

- Vulnerability classification
  - Type of system affected, nature of vulnerability, impact to org
- Exposure factor (EF)
  - How much would asset be affected by compromise or vulnerability exploit?
  - Helps assess potential loss/impact if vulnerability exploited
- Impacts
  - How would the organization be affected by a vulnerability being exploited?
  - Financially, reputation damage, regulatory issues, downtime
- Environmental variables
  - Differences in each network/infrastructure that could affect impact
  - External threat landscape
  - Regulations and compliance requirements
- Organizational risk tolerance

# Response & Remediation



# Remediation

---

- Patching
  - Standard updates and security patches to software and devices
  - Fixes known vulnerabilities to prevent exploitation
  - Centralized patch management eases process
    - Integrated with inventory management and vulnerability management
- Cybersecurity insurance
  - Can provide financial protection in event of a breach/incident
  - Does not mitigate vulnerabilities, but may assist with related costs
- Segmentation
  - Divide network into physical/logical portions to isolate and mitigate risk
  - Helps prevent lateral movement

# Remediation

---

- Compensating controls
  - Used when vulnerability cannot be completely eliminated
  - Additional layer of control to help mitigate risk
  - Extra monitoring, additional authentication, encryption
- Exceptions & exemptions
  - Used when vulnerabilities cannot be remediated for various reasons
    - Business critical system cannot be taken down for patching
    - Technical issues (lack of patch, legacy system, etc)
    - Cost too high to warrant mitigation
  - Form of risk acceptance

# Validate Remediation

---

- Ensure mitigation/remediation actions were successful
  - Correct implementation and functionality
- Human error can lead to incorrect implementation
- Checks for additional vulnerabilities introduced by previous fix
  - Or other issues that may arise due to fix
- Rescanning
  - Additional vulnerability scan to verify no longer present
- Auditing
  - Examination of steps taken to address vulnerability
  - Performed to ensure policies and best practices followed, docs updated
- Verification
  - Confirming results using various manual/automated testing, log review, etc.

# Reporting

---

- Vulnerability management process is not complete without reports
- Records of what vulnerabilities were found, and how addressed
- Assist with prioritization of actions
- Use CVSS scores to rate severity of vulnerabilities
  - Also consider impact of vulnerability in organization's environment
- Help to identify potential impact of each vulnerability
  - Possible outcomes of exploit (data breach, downtime, reputation)
- Recommendations for how to address each vulnerability
  - Patch, config change, other mitigation
- Different levels of reporting based on audience
  - Less technical for management
  - More technical for system admins/owners

# Monitoring Systems





# Infrastructure Monitoring

---

- Ensures proper operation of systems and devices
- Network monitors
  - Different from network traffic monitoring
  - Collects information about network infrastructure devices
    - CPU/memory, disk usage, temperature, network link errors, etc
  - Can be collected using SNMP (Simple Network Management Protocol)
- Netflow
  - Cisco-developed flow reporting information
  - Collects statistics about traffic, instead of contents of packets
  - Trends and patterns in traffic, including anomalies
  - Can assist in detecting malicious behavior

# Systems & Application Monitoring

---

- System monitors
  - Similar to network monitor
  - Information reported via software installed or SNMP
  - Event logs - security, application, etc
  - Many logs correspond to specific user activity
- Application monitors
  - Numerous third-party and proprietary solutions for monitoring applications
  - Usually include “heartbeat” - verification it’s running and responding
  - Cloud providers offer their own monitoring
    - App health, VM status, network utilization, security/other alerts

# Logging & Monitoring Activities

---

- Log aggregation
  - Taking logs from multiple sources and combining into one location
  - Normalization - convert/translate logs into one common format
    - Account for differences between formats, vendors, systems
  - Allows correlation, analysis, and alerting from one central location (SIEM)
    - Examine & interpret relationship between different data points
- Alerting
  - Notification based on rules - used for further investigation
  - Can tie into threat intelligence feed in SIEM for “smarter” alerts
  - Lead to analysis, containment, eradication, recovery (if all needed)
    - Response and remediation

## Response & Reporting

---

- Two primary responses to alerts in a SIEM - validation, quarantine
- Validation
  - True positive - needs further investigation and action - treated as incident
  - False positive - alert generated, but no actual threat or malicious activity
- Quarantine
  - Isolate source of malicious indicator (device, file, IP address, etc)
- Reporting
  - Helps provide insight into security controls and their effectiveness
  - Reports usually tailored to their intended audience
  - Requires determination of most important data in report
    - Authentication, patch levels, account anomalies, incident response
- Archiving
  - Keep report, log, alert data for a predefined period for historical use

# Alert Tuning

---

- Process to ensure alerting rules are generating proper events
  - Reduce false positives and false negatives
  - Too many false positives - analysts tend to look for reason to dismiss
- Eliminate alert fatigue
- Careful balance between too many alerts/not enough alerts
  - Reducing number of alerts can lead to increase in false negatives
- Methods
  - Refine detection rules
  - Redirect certain types of alerts (network, infrastructure, etc)
  - Continuous monitoring and feedback
  - Machine learning methods
    - Monitor alerts, and how analysts respond to them

# Logging & Monitoring Tools



## Security Information & Event Management (SIEM)

---

- Designed to collect, aggregate, and correlate log data
- Collects from devices across infrastructure
  - Switches, routers, servers, endpoints, IDS, firewalls, vuln scanners, DLP, etc
- One point of management for analysis and investigations
  - “Single pane of glass”
- Agent-based collection
  - Software installed on host to collect data and send to SIEM
  - Common on Windows, Linux, and MacOS
- Listener-based collection
  - Hosts configured to send data straight to SIEM without additional agent
  - Common on network equipment, devices that cannot support agent
- Sensors
  - Any device to collect or sniff traffic from network

# Benchmarks

---

- Monitoring systems can scan and compare against benchmarks
  - Public/standardized or internal
- Can identify lacking controls, misconfigurations, compliance checks
- SCAP (Security Content Automation Protocol)
  - Assists scanners with determining if systems meet baselines
  - OVAL (Open Vulnerability and Assessment Language)
    - XML schema describes security state based with vulnerability reports
  - XCCDF (Extensible Configuration Checklist Description Format)
    - Develop/audit best practice config checklists/rules
    - Machine-readable format to assist with automation



## Contributing Tools

---

- Vulnerability scanners
  - Reports total number of vulnerabilities per host
  - Reporting to SIEM can show overall vulnerability “health” of network
    - Total number of vulnerabilities per host
    - Number of hosts with specific vulnerability
- Anti-virus (or EDR)
  - Detects various types of malware, can alert standalone or through SIEM
  - Most will have some blocking capabilities
  - Similar to vulnerability scanner, can help showing overall security
- Data loss prevention
  - Helps with sensitive data protection
  - Logs into SIEM can show trends & alert to suspicious activity
  - Logs can be correlated with other data in SIEM

# Securing with Firewalls











## Firewall Rules

---

- Define how firewall should handle inbound/outbound traffic
  - For specific IP, IP range, or network interface
- Rules implemented using ACLs (access control lists)
  - Ordered list, processed from top to bottom
  - Allow or deny traffic based on criteria in rule
  - “Implicit deny” at bottom of list
    - Blocks traffic if no other rule matches
- Rules can be based on IP, port number, protocol, application, etc
  - Capabilities depend on type of firewall in use
- Recommendations
  - Block inbound requests from private IP addresses
  - Block protocols only used on internal network (DHCP, ICMP, routing)
  - Confirm correct functionality using pen tests

## Firewall Rules

---

	Protocol	Source	Port	Destination	Port
   	IPv4 TCP	*	*	192.168.1.100	443 (HTTPS)
   	IPv4 TCP	*	*	192.168.1.100	80 (HTTP)

```
permit tcp any 192.168.1.100 https
permit tcp any 192.168.1.100 http
```

```
permit tcp any 192.168.1.100 443
permit tcp any 192.168.1.100 80
```

## Screened Subnet

---

- Separates public-facing servers from restricted internal network
- Uses two firewalls placed at different network locations
- “Edge” firewall
  - Connected between public (internet) and screened subnet
  - Filters & restricts traffic to/from screened subnet from public network
- Internal firewall
  - Connected between screened subnet and internal (secure) network
  - Filters traffic between screened subnet and internal LAN
  - Typically blocks almost all traffic, unless specifically needed
- Dual firewall configuration allows for secure location for public hosts
  - Also permits communication with internal network, but isolated from public

# **Intrusion Detection & Prevention Systems**



# IDS/IPS

---

- Intrusion detection system & intrusion prevention system
- Similar capabilities in detecting threats
  - Both monitor network traffic (or host, depending on type)
- IDS detects and alerts, but takes no action
- IPS perform same detection, but can take blocking or preventative action
- Host-based or network-based
  - HIDS - installed on individual hosts, monitor system behavior
  - Can identify insider threats, file changes, logins, system processes, etc
  - NIDS - monitor network traffic only
  - Can identify threats across/between multiple systems & network
- Implementing both is recommended

## Example Solutions

---

- Snort
  - Open source IDS
  - Uses rule-based detection
  - Combines signature, protocol, and anomaly detection
- Suricata
  - IDS/IPS
  - Compatible with Snort rulesets
- Security Onion
  - Linux distribution
  - IDS, network monitoring, log management
  - Includes Suricata



## Detection Methods

---

- Signature-based detection
  - Also called pattern-matching - traffic must match pattern to be detected
  - Analysis engine contains predefined DB of attack patterns, file signatures
  - Requires frequent (sometimes paid subscription) updates
- Behavioral and anomaly based
  - Analysis engine can recognize normal, baseline activity
  - Anything deviating from baseline can generate an alert
  - Can lead to increased false positives and false negatives while “learning”
  - UEBA - user and entity behavior analytics
  - NTA - network traffic analysis
- Trend analysis
  - Assists in identifying patterns and threats (understanding over time)
  - Used to help tune detection of IDS/IPS systems

# Secure Protocol Implementation



## Secure Protocols

---

- Original communication protocols designed for functionality, not security
  - HTTP, Telnet, FTP
- Secure alternatives
  - HTTPS, SSH, SFTP/FTPS
- Secure protocols usually more complicated to configure
  - Certificate obtained & installed, key handling, troubleshooting
- Selection of secure protocols - risk assessment & protocols review
  - What type of data & sensitivity?
  - What type of communication/transport? (Web, device management, etc)
- Port configuration depends on protocol
  - Can change ports to non-default if needed

# Transport Layer Security (TLS)

---

- SSL developed in 1990s to secure HTTP traffic
  - Adopted as standard named TLS
  - SSL acronym still widely used, technology is TLS
  - SSL is no longer secure
- Used to secure many different protocols and VPNs
- Previous TLS versions allowed downgrade for legacy clients
  - Ex: Client request TLS 1.2 server to use 1.0 instead
  - TLS 1.3 (current as of recording) does not permit downgrade
- Cipher suite - set of algorithms supported by client & server
  - TLS 1.3 uses simplified suite

# Directory Services

---

- Database of “subjects” - computers, users, groups, devices, etc
- Provides authentication and authorization services
- Typically based on LDAP (Lightweight Directory Access Protocol)
  - Port 389 - no security, plaintext communication
- Authentication (binding)
  - No authentication - anonymous access granted to directory
  - Simple bind - client must supply credentials, but transmitted in cleartext
  - Simple Authentication and Security Layer (SASL)
    - Client/server negotiate authentication mechanism (ex: Kerberos)
    - Uses STARTTLS to require encryption
    - Used by AD
  - LDAPS - cert on server, secure tunnel created for communication
    - Port 636

# SNMP

---

- SNMP agents
  - Process that runs on device/system
  - Maintains DB - management information base (MIB)
    - Statistics about activity of system
  - Can initiate “trap” - sends information to management system
- SNMP monitor
  - Manages and monitors SNMP agents, polling at regular intervals
  - Receives trap information from agents
- Change default community names (send in plaintext)
- ACLs to restrict access to specific hosts
- SNMPv3 when possible (uses authentication instead of community names)

# File Transfer

---

- FTP (file transfer protocol) still popular - efficient and cross platform
- All data (including authentication) transmitted plaintext
- SFTP - SSH FTP
  - Wraps FTP session inside SSH tunnel (port 22)
  - Requires server and client software that supports SSH
- FTP over SSL/TLS
  - Explicit TLS (FTPES) - upgrades unsecure connection to secure (port 21)
    - Protects credentials, requires additional command to protect data
  - Implicit TLS (FTPS) - negotiates TLS tunnel before FTP commands
    - Uses port 990

# Network Access Control





# Network Access Control

---

- Authenticate and authorize a device to access the network
- Ability to verify compliance with security policies
- “Profiles” users and devices
  - Operating system version & patch level
  - AV/EDR software up to date
  - Device type and location
- Work with VLANs for device isolation and posturing
  - VLAN dynamically set based on defined criteria and device settings
  - Isolated VLAN for non-compliant devices (quarantine)
    - Restricted access, but enough to become compliant

# NAC Methods

---

- Agent-based
  - Software installed on device, communicates with NAC platform
  - Provides detailed info about device compliance level/status
  - Can allow automatic remediation
  - Provides more information and functionality than agentless
  - Persistent or non-persistent
- Agentless
  - Port-based access controls
  - Network scanner to evaluate device
  - Less functionality and information than agent-based
    - Can be used with any device that connects to network

# DNS Filtering



# DNS Filtering

---

- Checks DNS requests against database of domains
  - Malicious or blocked by org
- Benefits
  - Acts as proactive control
    - Blocks access to known phishing, malware sites
  - Control to enforce organization AUP
  - Protects all devices on network without needing client/agent
  - Cost-effective, simple setup and configuration
- Implementation options
  - Third party vendors (some free\*)
  - DNS server configuration
  - DNS firewall
  - Open source options

# DNS Security

---

- Organization DNS servers should only accept queries from local hosts
  - Ideally, authenticated
- Controls to prevent unauthorized record/configuration changes
- Disallow zone transfers
  - Method of DNS footprinting
  - Returns all DNS records in domain
- DNSSEC (DNS Security Extensions)
  - Method to mitigate against spoofing and DNS poisoning attacks
  - Packages responses signed with private key (Zone Signing Key)
    - Zone Signing Key is signed by Key Signing Key
  - Returns packages with public key for integrity verification