Security Operations Management

Brian Olliff

Defensive Engineering Instructor

Topics

Identity & Access Management
Passwords
Directory Management
Single Sign-On
Log Management
Asset & System Management
Vulnerability Identification
Remediating Vulnerabilities

Learning Objectives

- Understand the identity & access management lifecycle processes
- Be able to explain secure password management
  - Secure passwords, password storage and transmission, MFA
- Understand identity directories, federation, and single sign-on
- Understand log collection processes and systems used to analyze logs
- Be able to explain proper asset management methods
  - Inventories & mobile device management
- Understand the importance of change management and its processes
- Understand vulnerability management
  - Identification and discovery
  - Gathering additional information
  - Remediation options

Identity & Access Lifecycle

Identity & Access Management (IAM)

- Everything used to manage identities and authentication/authorization
- Includes multiple parts
  - Policies, processes, and technology
  - Identification of users
  - Authentication of accounts
  - Proper authorization to access resources
- Tools and technologies
  - Password management
  - IAM life cycle
  - Directory management
  - SSO

IAM Life Cycle

- All accounts/credentials go through specific steps
  - Credentials created and securely issued to users
  - Proper permissions & privileges assigned
  - Permissions and identities revoked when needed
- Identity and access management life cycle
  - Registration and identity validation
  - Privileges provisioning
  - Access review
  - Access revocation

Registration and Identity Validation

- First step occurs when user is onboarded to organization
  - Typically performed by HR department as part of hiring process
- Information provided to organization & used to create account(s)
  - Info is used to validate individual's identity (prove who they are)
  - DL/ID card, SS card, etc
  - Background check
  - Security clearance verification (if needed)
- Information may vary depending on level of privileges being granted
- After verification and validation, identity (account) created and assigned
  - Unique to individual

Privilege Provisioning

- After identity created and assigned, access rights established
  - Following least privilege, separation of duties, & need to know
- Method depends on access models in use at organization
  - May involve request to resource admin/owner
    - Not assigned until approved
  - May be templated-based and automatic
- Highly sensitive permissions may require additional steps (NDA, etc)
- Provisioning also applies to existing accounts
  - Job role change
  - Employee transfers
- With identity creation/registration, part of “account provisioning”

Review and Revocation

- Access review
  - Periodic/continuous reviews of access rights & privileges
    - Scheduled, as well as event-driven
  - Multiple purposes
    - Ensure org security policies are followed
    - Verify permissions are still appropriate
    - Helps eliminate privilege creep
- Access revocation
  - Occurs when employee leaves organization, or changes job role within org
  - Partial or complete revocation of access rights
  - Should follow formal, documented process

Password Management

Passwords

- Most common type of knowledge-based authentication
  - Also the weakest type of authentication
- Weakness mostly due to human factors
  - Tendency to use same password across multiple systems/accounts
  - Habit of writing down passwords
  - Usage of simple passwords that are easy to guess/crack
  - Tendency to not change default passwords
- Password management includes
  - All policies, procedures, technology to protect organization & users
  - Password creation, storage, and reset

Password Creation

- Process requires established standards & policies for secure passwords
  - Several factors must be considered
- Password strength
  - Weak passwords are easily cracked, brute-forced, or guessed
  - Complexity and length requirements
  - NIST SP 800-63
- Age
  - Maximum age of password before required to change
- Reusability
  - Reusing same password repeatedly, or on multiple systems
  - Same password with very small changes (incrementing number, etc)

Password Generation

- User generated
  - Easiest for users to remember
  - Typically riskiest type, but password requirements can help
- System-generated
  - Normally randomly created
  - More secure than user-generated, much harder for users to remember
    - Leads to users writing them down
- One-time password and token
  - Randomly generated, can only be used once
  - Typically implemented using token device (hardware or software)
  - Token often protected by PIN

Multifactor Authentication

- Using two or more types of authentication to verify users
  - Passwords, token codes, biometric, etc
- Authentication factors
  - Something you know (password, PIN)
  - Something you have (smartcard, physical token, smartphone)
  - Something you are (biometrics)
- Cisco Duo
  - Can integrate with existing user directories (Active Directory, etc)
  - Protection for on-premise and cloud-based systems
  - Integrates with multiple third-party applications & solutions
  - Policy-based access
  - Options for device posture checks

Password Storage & Transmission

- Passwords must be securely stored and transmitted when used
- Should never be stored in plain text format
  - Password hashes instead of passwords
  - If stored in files (not recommended), should be encrypted
    - Password manager recommended instead
- Always need to be transmitted over network or internet
  - Network segmentation to minimize transmission
  - Encrypted data streams when transmitted
    - HTTPS instead of HTTP for web traffic
    - SSH instead of Telnet for network device management

Password Resets

- Passwords always need to be reset for various reasons
  - User forgets, PW change doesn't work, etc
- Reset procedures must be secure
  - Policies documented and enforced
  - Attacker should never be access means to reset passwords
- Typically manual process assigned to help desk
  - May not be feasible in very large organizations
- Automatic methods
  - Internal website for users, secured with additional authentication method
    - Security questions (not recommended)
    - Security token

Synchronization

- Organizations typically have multiple systems requiring authentication
  - Independently, users need to remember several credentials
- Synchronization allows users to set password once
  - Management system automatically pushes to other systems
- Benefits
  - Users only need one set of credentials
  - Reduced management overhead for authentication
- Drawbacks
  - Synchronization process becomes critical piece of infrastructure
  - If credentials compromised, attackers can access all systems
- User directory systems also used

Directory Management

Directories

- Collection of user, system, network, device information
- Frequently used for identification, authentication, authorization of users
  - *Directory services*
- Capabilities to apply settings and policies to users/systems
- Benefits
  - Centralized location for identity and policy management
  - Reduces management overhead
- Drawbacks
  - Single point of failure
    - Replication and distribution can mitigate
  - Not all other systems can interface

ITU-T X.500

- Collection of standards and protocols for directory organization
- Hierarchical organization
  - Data is shown in directory information tree (DIT)
  - Stored in directory information base (DIB)
- Each entity has unique identifier - distinguished name (DN)
  - Common name (CN), Country (C), Organization unit (OU)
- Data access
  - Directory service agent (DSA) - provides access to information in DIB
  - Directory user agent (DUA) - connects to DSA for requests
  - Directory Access Protocol (DAP) - used for comm between DUA & DSA
  - Several others

Lightweight Directory Access Protocol (LDAP)

- Based on X.500
  - Shares many characteristics
  - Same type of hierarchical organization in database
  - Same naming conventions (distinguished names - DNs)
- DUA -> **LDAP client**
- DSA -> **LDAP server**
- Active Directory uses LDAP protocol
- LDAP and X.500-based systems can coexist

Single Sign-On

Single Sign-On (SSO)

- Authentication with one system, one time
  - Directory systems (LDAP) are type of SSO
- Different than using same password on all systems
  - Password synchronization
- User authenticates first time against primary authentication system
  - Multiple ways initial authentication can occur
  - Successive authentications performed using token/other proof of auth
- Drawbacks
  - Can be difficult to implement
    - Technical differences between systems & applications
  - Single point of failure
  - Risk of account compromise

Types of SSO

- Kerberos
  - Protocol used for SSO
  - Uses “tickets” for proof of authentication
  - Major component of Active Directory
- Federated SSO
  - SSO model that provides authentication/authorization across organizations
- OAuth
  - Framework for third-party authorization mechanisms
  - Part of federated SSO systems
- OpenID
  - Works with OAuth to provide authentication profiles

Kerberos

- Key Distribution Center (KDC)
  - Authenticates principals and issues tickets
    - Principals - users, service accounts, devices, applications
  - Consists of Authentication Service and TGS (Ticket Granting Service)
- Principal authenticates with KDC (domain controller in AD)
  - Sends request to authentication service for TGT (ticket granting ticket)
    - Request includes date/time of computer, user's hashed password
- Authentication service checks directory for presence of user account
  - Attempts to decode request by matching PW hash with one stored in AD
  - Verifies request has not expired
- Once verified, responds with TGT and TGS session key
  - TGT - includes client name, IP address, timestamp - encrypted with KDC key

Federation

Federation

- One set of credentials used across multiple organizations
  - Organizations use different IAM systems
  - Federated identity
- Requires establishing *trust* between organizations
- Core components
  - Principal
    - User requesting service, identity to be authenticated
  - Service provider
    - System that hosts services for the principal
  - Identity provider (IdP)
    - Service provider that manages authentication and authorization
  - Assertion
    - Information from authentication authority (IdP)

Authentication Process

- User attempts to access resources on SP
- SP redirects user to SSO server (IdP) for authentication
- User authenticates with IdP
- IdP provides assertion (proof of identification) directly to SP
- SP grants user access to requested resources
  - Uses information supplied by IdP in assertion

- Multiple protocols and frameworks used to implement process
  - SAML, OAuth, OpenID Connect

Security Assertion Markup Language (SAML)

- XML-based framework
- Shares authentication and authorization information
- Assertions contain
  - Authentication statement - info about auth, auth method, timestamp, etc
  - Attribute statement - information about principal
  - Authorization statement - information about what principal permitted to do
- Two ways of functioning
  - IdP initiated
  - SP initiated

OAuth

- Open framework to provide authorization to third-party entities
  - Also allows sharing of other user information (name, email, etc)
- Provides 3rd-party access to restricted resources w/o passing credentials
- Consists of four different roles:
  - Client
    - Requesting entity - frequently another site/service/app
  - Resource server
    - What the client is attempting to access
  - Authorization server
    - Processes authorization requests, provides auth token
  - Resource owner (user)
    - Individual/entity controlling access to resources

OAuth Process

1. Client sends auth request to resource owner or authorization server
   a. LinkedIn -> user requesting access to Google contacts
2. Resource owner (or auth server) sends authorization grant to client
   a. User authorizes LinkedIn to access contacts
3. Client sends auth grant to authorization server as proof request granted
   a. LinkedIn sends grant to Google
4. Authorization server authenticates client, sends access token
   a. Google authenticates LinkedIn
5. Client sends access token to resource server
   a. LinkedIn sends to Google Contacts
6. Resource server verifies token and allows access

OpenID Connect

- Multiple versions of OpenID, current is *OpenID Connect*
- OpenID 2.0 process very similar to SAML
- OpenID Connect no longer uses authorization functionality
  - Works with OAuth as authentication profile
- User attempts to access asset on relying party (RP)
  - System that holds resource user wants to access
  - RP sends authentication request to OpenID provider (OP) for user
    - OAuth authorization request to access user identity
  - User authenticates with OP, which asks for consent
  - OP then issues authorization code which is sent to RP

Log Collection & Analysis

Logs

- Event
  - “Any observable occurrence in a system or network” - NIST SP 800-61r2
  - Any data that systems generate that can be used to indicate an incident
- Incident
  - Event that violates organizational security policies
  - Determined by collecting and analyzing event logs
- Logs
  - Formal record of an event
  - Includes useful information
    - Timestamps, IPs, hostname, log message, username, etc

Log Collection

- First step in process of event management
- Most systems can generate and send logs to remote collector
  - Storage considerations - space, integrity, confidentiality
- Common information in logs
  - Usernames (sometimes passwords)
  - Activity performed on system
  - Timestamps
  - Successful or unsuccessful attempt
  - Detailed configuration change information
  - IPs, subnet info, MAC addresses
  - Files accessed or modified

Log Categories

- As defined by NIST SP 800-92
- Security software/systems
  - AV/EDR systems, IPS/IDS
  - Proxy systems
  - Any network infrastructure device
  - Vulnerability management systems
- Operating systems
  - System events and audit information
- Applications
  - Significant operations & usage (what was done in the application)
  - Network information (connection, session info)

Log Analysis

- After collection of logs, correlation and analysis
  - Taking logs from multiple sources and combining for actionable intelligence
- Review and analyze to detect possible security incidents
  - Mostly automated using Security Information & Event Manager (SIEM)
  - Can be manually performed on smaller datasets (time consuming)
    - Often needed for incident verification and auditing
- Log retention
  - How long do logs need to be kept?
  - Documented in log retention policy

Syslog

- One of most common event notification (logging) protocols
- Three main components
  - Originator - system that generates syslog message
  - Collector - systems that receives message (syslog server)
  - Relay - forwards messages from originator to other relays or collectors
- Can operate on either TCP or UDP port 514 (standard)
- Commonly include facility code and severity code
  - Facility - shows process, application, or system that generated log
  - Severity - importance of message (0-7, lower number more critical)
- Each message has header
  - Priority, timestamp, hostname, application name, process ID

SIEM &
SOAR

Security Information & Event Management

- Centralized system for log collection, analysis, alerting, reporting, etc
- Log collection
  - Can receive logs from multiple sources
  - Accepts multiple log formats
  - Provides log storage and indexing
- Log normalization
  - Takes multiple different log formats, extracts similar attributes
  - Data stored in common format/template
  - Provides faster event analysis and classification
  - Non-normalized logs typically stored for archive, forensics purposes

SIEM Functionality

- Log aggregation
  - Ingests multiple logs from multiple sources
  - Combines information using common information
- Log correlation
  - Associates different logs & events together
    - From multiple sources, formats, times, etc
  - One of most powerful, useful features of SIEM
  - Allows creation of actionable information based on multiple pieces of info
- Reporting
  - Real-time and historical data based on indexed log information
  - Provides visibility info collected data using dashboards

SIEM Integration

- Combine information from logs with other systems in infrastructure
  - Identity and access management
  - Netflow collectors
- Helps provide additional context for events
  - Information about users that is not included in logs
    - Department, phone number, etc
  - Additional network flow information
- Cisco ISE + Stealthwatch

Security Orchestration, Automation, & Response

- Additional component with SIEM
- Provide additional response capabilities
  - Threat hunting and management
  - Vulnerability management
  - Incident response
  - Automating security operations tasks
- Commonly deployed with SIEM
  - Take event info from SIEM and integrate with other systems on network
- Can be standalone product, or integrated with SIEM

Asset Management

Assets

- Anything that has value to an organization
  - Physical
    - Technical - switches/routers, desktop workstations, servers
    - Non-technical - desks, chairs, buildings
  - Personnel
  - Software
  - Data & information
- Must be properly protected against unauthorized access and use
  - Protected from threats
- Asset management - policies & procedures to manage asset lifecycle

Asset Inventory

- Organizations must know what they have
  - Can’t protect if not aware
- ISO 27005 defines primary and supporting assets
  - Primary - business processes & information
  - Supporting - software, hardware, network devices, personnel, sites, etc
- Inventory lists out all relevant assets to track
  - Relevancy will depend on organization
  - Should include physical and virtual assets, on-premise and cloud-based
- Accuracy is critical piece of effective inventory management
  - Requires periodic audits to ensure accuracy
- Recommended information
  - Location, description, asset owner & classification, configuration

Asset Ownership

- All assets should be assigned an owner
  - Individual or entity (group, department, etc)
- Assigned (or updated) when asset is created, acquired, or transferred
- Owner responsibilities:
  - Maintaining inventory of assets in their control
  - Classify their assets
  - Ensure proper protection of assets
  - Periodic review of applicable policies (classification and access control)
  - Proper disposal of asset
- Responsible for asset throughout its entire life cycle
  - Can delegate daily operations to others (custodian)

Asset Policies

- Describe what user is responsible for & their expected behavior
- Acceptable use policy (AUP)
  - Describes what a user is permitted to do with/to particular asset
  - Normally require acceptance before assets are issued to users
- Return policies (and processes)
  - What users should do when asset no longer needed
    - Termination, transfer, end of contact, etc.
  - Applies to physical and virtual assets
- Users required to acknowledge and follow policies

Classification & Labeling

- Classification - label based on risk to organization
  - Unauthorized access that affects confidentiality, integrity, or availability
  - Typically assigned by asset owner
    - May be policies in org that dictate what labels get applied
- Labeling will vary by organization (industry, size, compliance req, etc)
  - Top secret = very high risk of damage to organization
  - Confidential = some damage
  - Unclassified = no significant damage
- Processes should exist to guide classification & labeling
  - Information on changing classification
- Physical assets should have physical labels or markings
  - Visible and conspicuous

Handling Assets & Information

- Procedures should exist on how to securely handle all assets
  - At rest, in use, and in transit
  - Access controls that match classifications
  - Auditing of access records/controls
  - Secure storage of assets
- Media management - policies/procedures for secure handling of media
  - Access, marking, storage, use, transport, sanitization/disposal
  - Typically refers to removable media (USB, external HDs, etc)
  - Sensitive data requires drives to be encrypted
  - Secure disposal and destruction
- Removable media typically higher risk to organization
  - Easily moved and used

Enterprise Mobility Management

Mobile Assets

- Smartphones, laptops, tablets, etc
- Can be more difficult to secure due to mobility
  - Not always on enterprise network
  - Not always owned by organization
- Bring-your-own-device (BYOD)
  - Allowing employees to use personal devices to access company resources
  - Can increase productivity, depending on policies
- Enterprise Mobility Management (EMM)
  - Policies, processes, & technology to securely manage mobile devices
  - BYOD or organization-owned devices
  - MDM (mobile device management) & MAM (mobile app management)

Mobile-Related Threats

- Identified by NIST SP 800-124
- Lack of physical security controls
- Use of untrusted devices
- Use of untrusted networks
- Untrusted applications
- Interaction with other systems
- Use of untrusted content
- Location services

Enterprise Mobile Device Life Cycle

- Proposed by NIST SP 800-124
- Initiation
  - Planning, strategy selection, developing security policies, etc
- Development
  - Creation of deployment plan, choosing authentication, encryption, etc
- Implementation
  - Testing of plan, provisioning devices in production
- Operation and maintenance
  - Ongoing tasks during life cycle - reviewing access, patch management, etc
- Disposal
  - Media sanitization, destruction, similar to asset management

Mobile
Device Management

Mobile Device Management (MDM)

- System to manage deployment, monitoring, & security of mobile devices
  - Policy-driven, with many capabilities
- Restrict hardware use (camera, GPS, Bluetooth, etc)
- Security restrictions based on device posture
- Monitoring and alerting on any security policy violations
- Manage encryption settings (communication, and device)
- Remote wiping (selective or full)
- Enforce device lock (PIN, password, etc)
- DLP policy management
- Application restrictions
  - Coupled with MAM for additional functionality

MDM

- Typically offered by third-party vendor/solution
  - Can also be from mobile provider - not common
- Policy management is performed over the air (OTA)
- Management can be on-premise or cloud-based
  - Cloud-based
    - Can be more flexible and more affordable
    - Faster to implement and easier to scale
  - On-premise
    - Higher level of control
    - More control of data
    - May be required by regulation

Cisco BYOD Management

BYOD Architecture

- Based on Cisco Unified Access design
  - Provides guidelines for BYOD implementation for organizations
- Mobile devices
  - Corporate or personally owned devices
- Wireless access points (APs)
- Wireless LAN controllers
  - Centralized point for wireless AP configurations and monitoring
  - Can enforce authorization policies for endpoints
- Cisco ISE (Identity Services Engine)
  - Identity management, profiling, authentication, authorization, access controls

BYOD Architecture

- AnyConnect Secure Mobility Client
  - Offers security for when device on-premise and off-premise
  - On-premise - client-side authentication & authorization using 802.1x
  - Off-premise - VPN connectivity
- Integrated Services Routers (ISRs)
  - Home and remote branch office use
  - Can combine multiple services/functions into one device
- Aggregation Services Routers (ASRs)
  - Used on campus networks
  - Aggregate home/branch office traffic to connect to corporate network

BYOD Architecture

- Cloud web security
  - Web proxies in Cisco cloud environments
  - Scan for malicious traffic & enforce policies for web traffic
  - Useful for roaming users
- Cisco ASA (Adaptive Security Appliance)
  - Multifunction appliance typically placed on network edge
  - VPN server, NGFW, IPS

MDM Integrations

- Cisco ISE
  - Can integrate with multiple third-party MDM solutions
  - Help enforce device policies and compliance
  - Supports two-way data exchange
    - Additional information about endpoint
    - ISE can take actions on endpoint through MDM
- Cisco Meraki
  - Cloud-based enterprise mobility management
  - Manages multiple types of devices (phones, laptops, WAPs, etc)
  - Similar functionality to other EMM tools
    - Added integration between Cisco systems/devices

Change Management

Configuration and Change Management

- Configuration management
  - Policies, procedures, and technology to maintain configuration integrity
  - Can apply to any asset in an organization
- Change management
  - Policies procedures, and technology that help manage changes
    - Modification of assets, systems, data, etc
    - Addition or removal of assets and their configurations
- Both can be included in asset management

Configuration Management

- Maintaining resource/asset integrity through processes
  - Initialization, modification, and monitoring of configurations
- Requires inventory of assets and their configurations
- Configuration item (CI)
  - Target of the configuration control process
  - Individual asset or group of assets (router, server, application, etc)
  - Can also be documentation for assets
  - Contains attributes to describe (OS/app version, installed apps, IP, etc)
- Configuration record - CI attributes and their relationships
  - Stored in configuration management database (CMDB)

Security Focused Configuration Management (SeCM)

- Builds on “standard” configuration management
- Typically consists of four phases
  - Planning
    - Define policies and procedures
    - Integrate procedures into IT and security policies
  - Identifying and implementing configuration
    - Creation of security baseline configurations and baseline CIs
  - Controlling changes
    - Manage changes to ensure integrity of security baselines
    - Change management process
  - Monitoring
    - Ensures that CIs stay in compliance of policies
    - Maintaining secure baselines

Change Management

- Policies and processes for changes to systems, infrastructure, etc
- Three main types of changes
  - Standard
    - Common changes, usually preauthorized and low risk
    - May not need to follow formal change management process
  - Emergency
    - Urgent change (systems down, process non-functional, etc)
    - Typically has separate change management process
  - Normal
    - Other changes (not standard or emergency)
    - Standard full change management procedure

Change Management Process

- Create request for change (RFC)
  - Includes overview plan, description, motivation
- Record and review RFC
  - Request formally documented in change management system
  - Initial review to ensure requested change is necessary and appropriate
- Assess and evaluate change
  - Change review board/committee reviews
  - Determination if full change control process is needed
  - Security impact is determined and evaluated
- Change build and test authorized
  - Test plan formally authorized by change authority
  - Should confirm any security impacts from previous step

Change Management Process

- Build and test coordination
  - Technical group receives info for authorized change
  - Begins testing process
- Deployment authorization
  - If testing goes to plan, change authorized for deployment
  - If additional information/testing needed, previous steps possibly repeated
- Change implementation
- Review change
  - After deployment/implementation, testing performed
    - Ensure change was deployed correctly and without issue
  - If no issues, change record updated and request closed

Security Impact Analysis

- Usually performed by security team member to determine any issues
- Understand change
- Identify any vulnerabilities
  - Analyze info from vendor, other vulnerability intelligence provider
  - May include security analysis of code (if applicable)
- Assess risks
  - Identify possible threats, calculate likelihood of exploitation
  - Accept, mitigate, add countermeasures, or avoid (change rejected)
- Determine impact on existing security controls
- Plan additional countermeasures (if needed)

Vulnerability Discovery

Vulnerability Management

- Process of identifying and eliminating or reducing vulnerabilities
  - Requires research, documentation, threat intelligence, etc
  - Multiple tools and processes
  - Inventory of environment is critical

- Three primary phases
  - Vulnerability identification
  - Analysis and prioritization
  - Remediation

Vulnerability Discovery

- Multiple ways to discover vulnerabilities in environment
  - Active searching and scanning
  - Passive notifications
- Vulnerability scans
  - Software running on network to scan and identify known vulnerabilities
- Penetration testing
  - Tests exploitation of vulnerabilities, may discover unknown vulnerabilities
- Vendor announcements (disclosures)
  - Notifications from software/system vendors of discovered vulnerabilities

Vulnerability Scanners

- Commonly used by organizations to manage internal vulnerabilities
- Only used to discover known vulnerabilities
- Active scanner
  - Scanner probes systems and analyzes responses to determine vulnerabilities
  - Credentialed and non-credentialed (authenticated or non-authenticated)
    - Using authenticated account to scan system can result in more info
  - Agent vs agentless
    - Agent can continuously monitor system and report back to scanner
- Passive scanner
  - Observes network traffic to determine presence of vulnerabilities
- Can be prone to false positives
  - Analysis may show vulnerability, but not present or not exploitable

Vulnerability Scanning Process

- Identify which systems are in scope of scan
  - Typical to have different types of scans with groups of systems
  - Systems usually identified by hostname or IP address
- Notify system owners/admins about scan
  - Vuln scanners have possibility of causing downtime (not common)
- Run scan
  - One-time scan or recurring on schedule
- Analyze results
  - Prioritize based on CVSS score and threat posed to organization
  - Identify possible false positives (system owners may perform)

Penetration Testing

- Also known as ethical hacking assessment
- May be performed by organization, or contracted third-party
- Attempts to exploit known discovered vulnerabilities (non-destructively)
- Can discover unknown vulnerabilities
- Several types, typically classified based on information provided to tester
  - White box
    - Tester given information about network and systems
    - Simulates insider threat
  - Black box
    - Tester given no information, simulates external attacker
    - Can be less complete/thorough than white box
  - Gray box

Vulnerability Information

Vendor Announcements

- Once vulnerabilities discovered (regardless of method), more info needed
- Vendor announcements typically contain more detailed information
  - Also known as *security advisory*
  - Include identifier (vendor ID, CVE), affected products, impact, remediation

- Vendors may provide API for automatic consumption of information
  - Open Vulnerability and Assessment Language (OVAL)
  - Common Vulnerability Reporting Framework (CVRF)

Vulnerability Repositories

- Aggregators to find information about specific vulnerabilities
  - Also used to see lists of vulnerabilities for specific product, app, OS, etc
- MITRE CVE repository
  - Primary repository for vulnerabilities and descriptions
  - Issue CVE IDs
- National Vulnerability Database
  - Provides additional information on vulnerabilities, including CVSS score
- US-CERT
  - Weekly summaries of vulnerabilities
- CERT-EU
- Japan Computer Emergency Response Team
- Australian Cyber Emergency Response Team

Product Vulnerability Management

- Processes for developers/vendors to manage vulnerabilities in products
  - Typically handled by PSIRT (Product Security Incident Response Team)
- Cisco Security Vulnerability Policy - 7 phases
  - Awareness
  - Active management
  - Fix determined
  - Communication plan
  - Integration and mitigation
  - Notification
  - Feedback

Vulnerability Disclosure

- Two main ways to disclose - full disclosure & coordinated disclosure
- Full disclosure
  - All details about vulnerability are disclosed
  - Can help IRT and provide temporary mitigations
  - Includes enough details for threat actors to build exploit
- Coordinated disclosure
  - Relevant information still disclosed
  - Information that could be used to build exploit is omitted
  - Most vendors & security researchers use

Security Content Automation Protocol (SCAP)

- Standardized method for security automation
- Can be used with multiple security language formats
  - OVAL, XCCDF, AI (Asset Identification), etc
- Enumerations
  - CVE - Common Vulnerabilities & Exposures
  - CPE - Common Platform Enumeration
  - CCE - Common Configuration Enumerations
- Metrics
  - CVSS - Common Vulnerability Scoring System
  - CCSS - CCSS - Common Configuration Scoring System
  - CWSS - Common Weakness Scoring System
  - CMSS - Common Misuse Scoring System

Vulnerability Analysis & Remediation

Analysis

- Confirm that system is vulnerable (not false positive)
- Understand vulnerability technical details and prioritize
  - Vendor documentation, vulnerability announcement, etc
  - Risk assessment to determine possible impact and priority
    - Performed with vuln severity and system criticality in mind
- CVSS 3.1
  - Industry standard for scoring vulnerabilities
  - Three aspects and scores - base, temporal, environmental
  - Base scores
    - 0 - None
    - 0.1 - 3.9 - Low
    - 4.0 - 6.9 - Medium
    - 7.0 - 8.9 - High
    - 9.0 - 10.0 - Critical

CVSS Base Group

- Basic characteristics of vulnerability
  - Do not change over time, do not depend on user-specific environment
- Exploitability metrics - measure how vulnerability can be exploited
  - Attack vector (AV) - level of access attacker needs in order to exploit
  - Attack complexity (AC) - conditions outside attacker's control
  - Privileges required (PR) - permissions attacker must have to exploit
  - User interaction (UI) - is user interaction required for exploit?
  - Scope (S) - impact on other systems other than one being scored
- Impact metrics - how confidentiality, integrity, availability affected
  - Confidentiality (C)
  - Integrity (I)
  - Availability (A)

CVSS Temporal & Environmental

- Temporal - assessment of vulnerability as it changes over time
  - Exploit code maturity (E) - public exploit available?
  - Remediation level (RL) - is fix or workaround available?
  - Report confidence (RC) - level of confidence in existence of vulnerability

- Environmental - vulnerability with org environment taken into account
  - Security requirements - importance of CIA requirements for system
  - Modified base metrics - org can tweak base metrics to suit environment

Remediation

- Remediation highly dependent on vulnerability and affected system(s)
- Patching or updates is most common method
  - Often requires testing, maintenance windows, change control, approval, etc
  - Can take some time based off various requirements
- Workarounds
  - Technical solutions to prevent exploitation without affecting system
  - Ex: dropping potential malicious traffic, adding additional security control
- Mitigation
  - Solution that limits exposure or impact of vulnerability
  - Does not eliminate risk of exploit, does not remove or patch vulnerability

Patch Management

Patch Management

- NIST SP 800-40r3 - process of identifying, acquiring, installing, and verifying patches for products and systems
- Most common type of vulnerability remediation
  - Many other reasons for patches besides vulnerabilities
- Patch - fix for a specific bug or vulnerability
- Update - full package install
  - Typically includes all patches up to that point
- Patching process typically not managed by security teams
  - Usually IT/infrastructure teams manage
  - System owners may be responsible

Patching Process

- Identify systems where patches are needed
  - Requires inventory of systems and software, and configurations
- Prioritize systems that require patching
  - Patches may apply to multiple systems (multiple types of systems)
  - Not all systems will require immediate patching
    - Mission critical systems are high priority
    - Test/dev systems lower priority
- Evaluate existing/new countermeasures
  - Existing controls may provide level of mitigation to vulnerability until patched
  - Workarounds or additional controls can be put in place
  - Change management process can delay patching

Patching Process

- Starting change control/management process
  - Exact procedures will vary by organization
  - Review/complete RFC (request for change)
  - Determine if patch needs to follow full change management process
  - Test & perform security impact assessment
  - Once change authorized, apply patch
  - Verify effectiveness and functionality of system
- Update configuration records
  - Patching updates version numbers and patch data on systems
  - Records should be updated to correspond, including any documentation

Patch Deployment Models

- Can assist with inventory process and deployment of patches/updates
- Agent based
  - Software installed on system that reports back to central server
  - Continuous communication
  - Can retrieve patch from management server and automatically apply
- Agentless
  - Single system that scans environment to determine patching requirements
  - Typically requires administrative access on targets
  - Less reliable than agent based, may not be able to automatically install
- Passive monitoring
  - Uses network traffic to determine software/OS versions
  - Least intrusive, least reliable, cannot install patches

Deployment Options

- Update all systems that require at same time
  - May require downtime, depending on system redundancy
- Phased deployments
  - Update some systems based on priority and risk assessment
  - May require less downtime, greater time period to apply
- Push deployment/automatic deployment
  - Patch is automatically applied on system, usually agent based
- Pull deployment/manual deployment
  - Administrator required to manually download/install patch

EXPERTS AT MAKING YOU AN EXPERT