Class #9 – Chapters 14 & 15

Jake Smithula

CISSP® MENTOR PROGRAM – SESSION NINE

INTRODUCTION

Agenda –

- Welcome
- Introduction
- Controlling and Monitoring Access
- Single Sign On (SSO)
- Access Control Attacks
- Security Assessment & Testing
- Vulnerability Assessment & Testing
- Security Audits & Metrics

CISSP® MENTOR PROGRAM – SESSION NINE

FRSECURE CISSP MENTOR PROGRAM LIVE STREAM

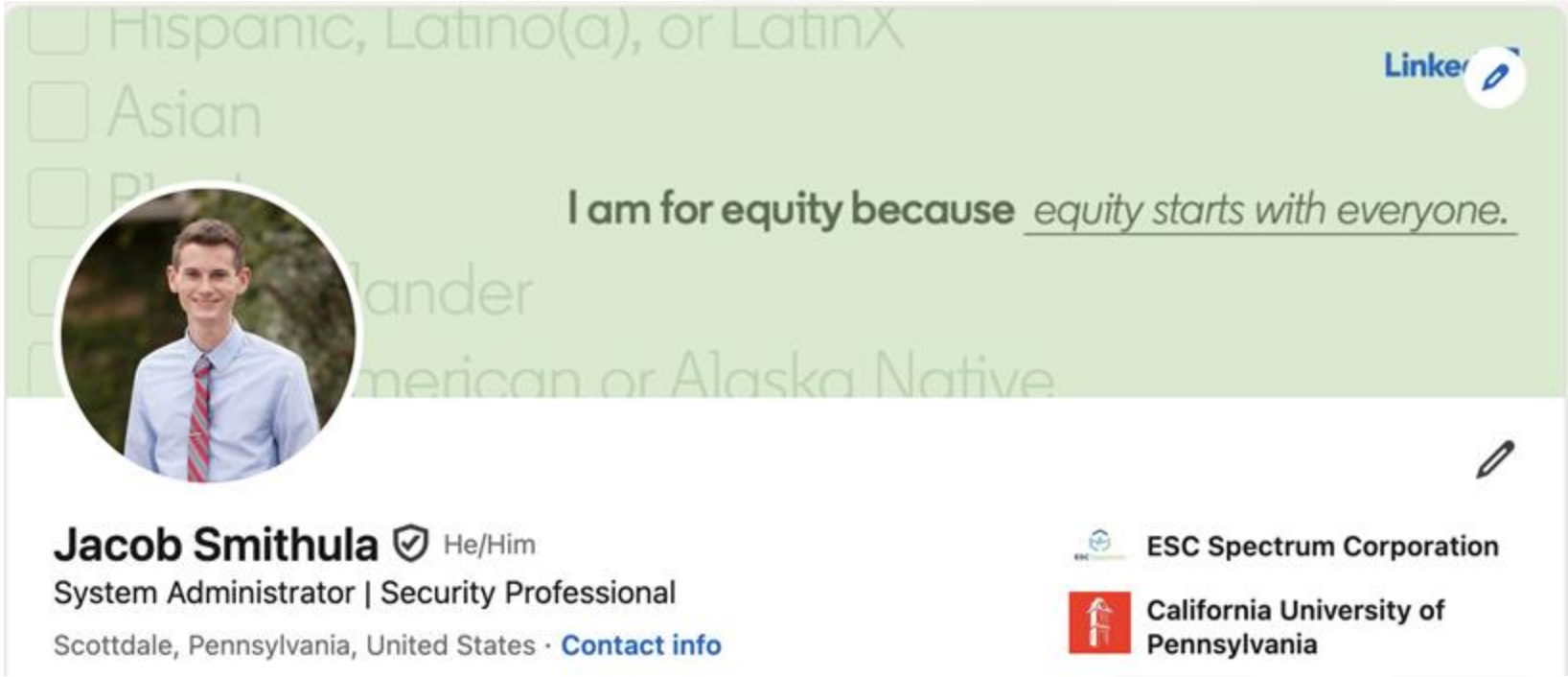
Quick housekeeping reminder.

- The online/live chat that's provided while live streaming on YouTube is for constructive, respectful, and relevant (about course content) discussion **ONLY**.
- At **NO TIME** is the online chat permitted to be used for disrespectful, offensive, obscene, indecent, or profane remarks or content.
- Please do not comment about controversial subjects, and please **NO DISCUSSION OF POLITICS OR RELIGION**.
- Failure to abide by the rules may result in disabling chat for you.
- **DO NOT share or post copywritten materials. (pdf of book)**

CISSP® MENTOR PROGRAM – LEAD MENTOR INTRO

WHOAMI

Jake Smithula



https://www.linkedin.com/in/smithula/

Chapter 14: Controlling and Monitoring Access

Permissions, Rights & Privileges

- **Permissions** – What you can do with an object, create, read update or delete (CRUD)
- **Rights** – Action you can take on an object, restore from backup, change wallpaper, connect a device
- **Privileges** – Combination of rights and permissions. Think Administrator or root, you can access any file or perform any action.

Chapter 14: Controlling and Monitoring Access

Implicit Deny

- Default security stance: “That which is not explicitly allowed is denied”
- Unlisted permissions are automatically blocked
- Common in firewalls, ACLs, and IAM policies
- Reduces risk from misconfiguration

Chapter 14: Controlling and Monitoring Access

Access Control Matrix & Capability List

Access Control Matrix: Rows = users, columns = resources

Capability List: Focused on subjects, a table for one user would have their individual permissions, rights and privileges.

Chapter 14: Controlling and Monitoring Access

Constrained Interface

- Restricts user access through controlled means
- Only shows authorized functions or data
- Reduces risk of misuse or data exposure
- Used in:
- ATMs
- Kiosks
- Management portals

Chapter 14: Controlling and Monitoring Access

Content-Dependent Control

Access is based on the **actual data** being accessed
Example: Only see customer data from your region
Often used in database systems and DLP tools

Context-Dependent Control

Access based on **circumstances or environment**
Examples:
Time of day
Location/IP address
Device or connection type
Supports risk-based authentication

Chapter 14: Controlling and Monitoring Access

Least Privilege

Users only get the access they need to do their jobs
Reduces attack surface
Applies to users, applications, and systems
Enforced via role design and permission reviews

Separation of Duties

Divides responsibilities to reduce fraud and error
No single person has full control
Example: One person initiates a transaction, another approves it
Supports accountability

Chapter 14: Controlling and Monitoring Access

Rule-Based Access Control

Access based on specific rules or conditions
Often used with firewalls, routers
Example: “Allow access between 8 AM and 5 PM”

Attribute-Based Access Control (ABAC)

Access based on attributes of user, resource, and environment
Highly flexible
Example: “Managers in HR can access payroll data during business hours”

Chapter 14: Controlling and Monitoring Access

Mandatory Access Control (MAC)

Based on labels: Top Secret, Confidential, etc.
Only administrators can change access rules
Used in military/government environments
Enforces “need to know” and classification levels

Risk-Based Access Control

Evaluates risk before granting access
Uses machine learning
Based on past activity
Makes predictive conclusions

Chapter 14: Controlling and Monitoring Access

Discretionary Access Control (DAC)

Owner decides access rights
Used in most operating systems (e.g., Windows, Linux)
Flexible but less secure
Prone to privilege creep

Chapter 14: Controlling and Monitoring Access

Role-Based Access Control (RBAC)

Access assigned to roles, not individuals
Users inherit rights from roles
Common in enterprise environments
Easy to manage at scale

Chapter 14: Controlling and Monitoring Access

Privilege Creep

- Accumulation of unnecessary permissions over time
- Often caused by job changes, project access not revoked
- Increases risk of insider threats or lateral movement
- Mitigated by:
- Access reviews
- Role audits
- Least privilege enforcement

Chapter 14: Controlling and Monitoring Access

Single Sign-On (SSO)

User logs in once to access multiple systems
Reduces password fatigue
Grant and revoke permissions centrally
A compromise can expose multiple systems

External Protocols

- SAML – XML based standard, authentication, authorization, and attribute information
- Oauth – Exchanges information with APIs, not for authentication
- OpenID – JSON Based standard, authentication and authorization

Internal Network Protocols

- Kerberos
- RADIUS
- TACACS+

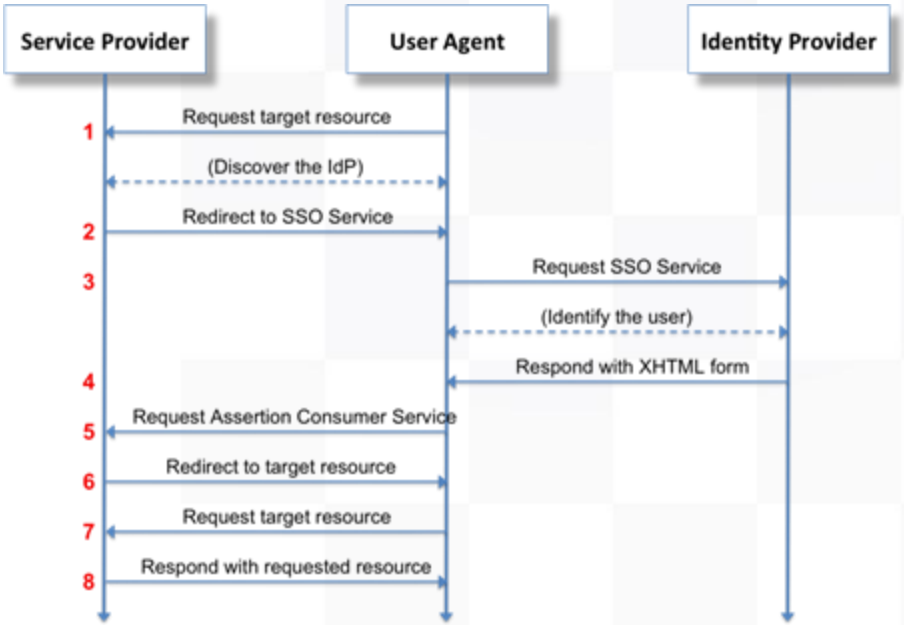
Chapter 14: Controlling and Monitoring Access

Single Sign-On (SSO)

SAML

XML based standard
authentication, authorization, and attribute information

Three Roles:
User Agent (UA)
Service Provider (SP)
Identity Provider (IdP)



Chapter 14: Controlling and Monitoring Access

Single Sign-On (SSO)

Oauth

An open protocol to allow secure authorization in a simple and standard method from web, mobile and desktop applications.

Exchanges information with APIs, not for authentication

Example, Allowing a music app to post what you are listening to on Facebook.

Chapter 14: Controlling and Monitoring Access

Single Sign-On (SSO)

OpenID (OIDC)

- JSON Based standard, authentication and authorization
- Built on top of Oauth 2.0
- Similar to SSO
- Implemented on web apps
- Example: Log into Shake Shack account with Google, Facebook, Apple, etc.

Chapter 14: Controlling and Monitoring Access

Single Sign-On (SSO)

Kerberos

- Third party authentication service, can be used for SSO
- Based on a key distribution model
- Provides authentication of clients and servers

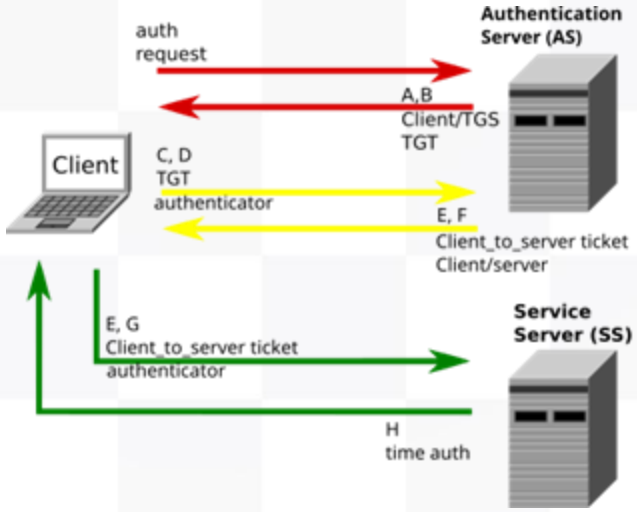
- Weakness
- KDC compromise can affect every key in the realm
- Keys and tickets may be recoverable on a local host

Chapter 14: Controlling and Monitoring Access

Single Sign-On (SSO)

Kerberos (Continued)

Kerberos Components



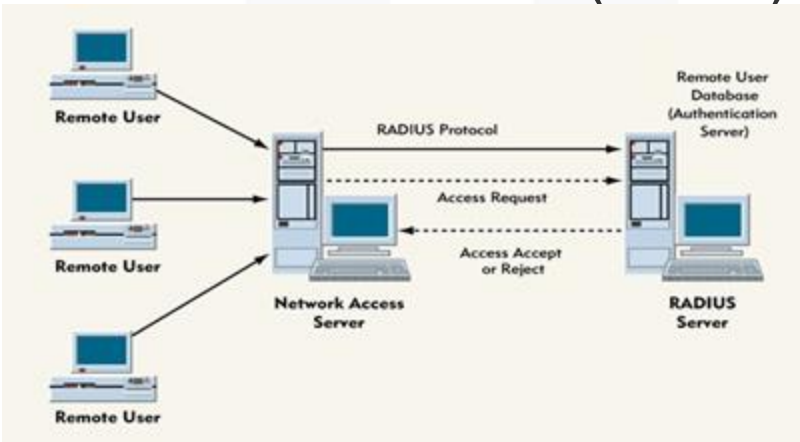
- ***Principal***: Client (user) or service
- ***Realm***: A logical Kerberos network
- ***Authentication Server*** (AS): Authenticating principles
- ***Ticket***: Data that authenticates a principal's identity
- ***Credentials***: a ticket and a service key
- ***KDC***: Key Distribution Center
- ***TGS***: Ticket Granting Service
- ***TGT***: Ticket Granting Ticket
- ***C/S***: Client Server, regarding communications between the two

Chapter 14: Controlling and Monitoring Access

Single Sign-On (SSO)

RADIUS

- Uses the User Datagram Protocol (UDP) ports:
  - 1812 (authentication) and
  - 1813 (accounting)
- Request and response data is carried in Attribute Value Pairs (AVPs)

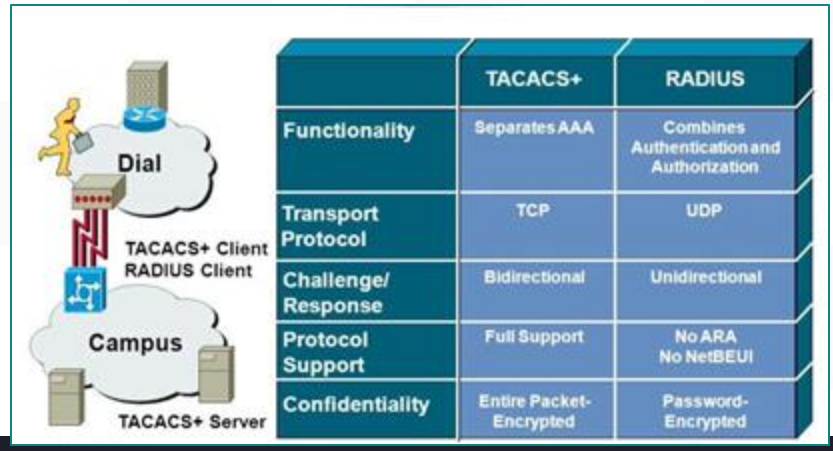


Chapter 14: Controlling and Monitoring Access

Single Sign-On (SSO)

TACACS+

- Originally developed by Cisco, now an open standard
- Uses TCP port 49
- Authentication is similar to RADIUS
- RADIUS only encrypts the password (leaving other data, such as username, unencrypted); TACACS+ encrypts all data below the TACACS+ header



	TACACS+	RADIUS
Functionality	Separates AAA	Combines Authentication and Authorization
Transport Protocol	TCP	UDP
Challenge/ Response	Bidirectional	Unidirectional
Protocol Support	Full Support	No ARA No NetBEUI
Confidentiality	Entire Packet-Encrypted	Password-Encrypted

Chapter 14: Controlling and Monitoring Access

Zero Trust

- “Never trust, always verify” – Trust no user or device by default
- Access is dynamic and policy based
- Assumes a breach is always possible, internal networks aren’t safe by default
- Enforces least privilege and segmentation
- Requires continuous verification and centralized controls

Chapter 14: Controlling and Monitoring Access

Common Access Control Attacks

- Password Attacks
- Dictionary Attacks
- Brute Force Attacks
- Password Spraying
- Credential Stuffing
- Rainbow Table Attacks
- Birthday Attacks
- Mimikatz
- Pass the Hash Attacks
- Sniffer Attacks

Chapter 14: Controlling and Monitoring Access

Access Control Attacks

Privilege Escalation

- Gaining unauthorized access to higher privileges
- Can be **vertical** (user → admin) or **horizontal** (peer access)
- Exploits:
- Unpatched systems
- Misconfigured permissions
- Exploitable code or services

Chapter 14: Controlling and Monitoring Access

Access Control Attacks

Password Attacks

- Target weak authentication systems
- Attack types include:
- Dictionary
- Brute force
- Credential stuffing
- Password spraying
- Rainbow table
- Birthday attacks

Chapter 14: Controlling and Monitoring Access

Access Control Attacks

Dictionary Attacks

- Uses precompiled list of common passwords
- Fast, efficient against weak passwords
- Defeated by:
- Strong password policies
- Account lockout
- MFA

Chapter 14: Controlling and Monitoring Access

Access Control Attacks

Brute Force Attacks

- Tries every possible combination
- Very slow without computing power
- More effective against short or poorly encrypted passwords
- Defenses:
- Strong hashing
- Lockout policies
- MFA

Chapter 14: Controlling and Monitoring Access

Access Control Attacks

Password Spraying

- Tries a few common passwords across many accounts
- Evades lockouts triggered by rapid, repeated guesses
- Very effective against enterprise environments
- Countermeasures:
- MFA
- Behavioral analytics
- Lockouts with delay

Chapter 14: Controlling and Monitoring Access

Access Control Attacks

Credential Stuffing

- Uses known username/password pairs from past breaches
- Automated and scalable
- Relies on password reuse
- Defenses:
- MFA
- Password managers
- Breach detection

Chapter 14: Controlling and Monitoring Access

Access Control Attacks

Rainbow Table Attacks

- Use precomputed hash values to reverse hashed passwords
- Fast and powerful against unsalted hashes
- Defeated by:
- Salting passwords
- Strong hashing algorithms
- MFA

Chapter 14: Controlling and Monitoring Access

Access Control Attacks

Birthday Attacks

- Based on probability theory (birthday paradox)
- Finds two inputs that produce the same hash (collision)
- Exploits weak hashing algorithms (e.g., MD5)
- Mitigation: Use collision-resistant hashes (e.g., SHA-256+)

Chapter 14: Controlling and Monitoring Access

Access Control Attacks

Pass-the-hash Attacks

- Attacker captures NTLM hash, reuses it without cracking
- Enables lateral movement across Windows systems
- Doesn’t require plaintext password
- Defenses:
- Kerberos over NTLM
- Privileged Access Workstations
- Credential isolation

Chapter 14: Controlling and Monitoring Access

Access Control Attacks

Sniffer Attacks

- Packet capture plain text information
- Defenses:
- SSL / Encryption
- Least privilege

Chapter 14: Controlling and Monitoring Access

Access Control Attacks

Mimikatz

- Open-source post-exploitation tool
- Extracts plaintext passwords, hashes, Kerberos tickets from memory
- Used in **pass-the-hash** and **pass-the-ticket** attacks
- Blocked by:
- LSA protection
- Credential guard
- Principle of least privilege

Chapter 14: Controlling and Monitoring Access - Quiz

Which access control model assigns permissions based on user roles?

A. DAC
B. RBAC
C. MAC
D. ABAC

Chapter 14: Controlling and Monitoring Access - Quiz

Which principal ensures that actions not explicitly allowed are denied?

A. Lest privilege
B. Implicit deny
C. Separation of duties
D. Need to know

Chapter 14: Controlling and Monitoring Access - Quiz

Which attack tries a few common password across many accounts?

A. Brute force
B. Credential stuffing
C. Password spraying
D. Dictionary attack

Chapter 14: Controlling and Monitoring Access

Access Control Summary

- Access control enforces **Confidentiality, Integrity, Availability (CIA)**.
- Models: **MAC, DAC, RBAC, ABAC, Rule-Based**.
- Core principles: **Least Privilege, Separation of Duties, Implicit Deny**.
- SSO Protocols: **Kerberos, SAML, OAuth, OpenID, RADIUS, TACACS+**.
- Threats: **Password attacks, Privilege Escalation, Pass-the-Hash**.

Joke Break

What kind of access control attack could a dog be responsible for?

Joke Break

What kind of access control attack could a dog be responsible for?

A sniffer attack

Chapter 15: Security Assessment & Testing

Introduction to Security Assessment and Testing

- Validates the effectiveness of security controls
- Identifies vulnerabilities before they're exploited
- Supports compliance, risk management, and operational assurance
- Includes: scanning, testing, audits, reviews, and monitoring

Chapter 15: Security Assessment & Testing

Security Testing Objectives

- Confirm control effectiveness
- Identify weaknesses before attackers do
- Meet compliance requirements
- Support business risk decisions

Chapter 15: Security Assessment & Testing

Security Audits

- Formal review of security posture and practices
- Can be internal or external
- May focus on:
- Policies and procedures
- Technical controls
- Regulatory compliance
- Evidence-based and structured

Chapter 15: Security Assessment & Testing

External Security Audit Engagements

- SOC 1 – Controls that may impact financial reporting
- SOC 2 – Controls that may impact information security (confidentiality, integrity and availability. Confidential and typically not shared outside the organization.
- SOC 3 – Similar to SOC 2 but results are intended for public disclosure

Chapter 15: Security Assessment & Testing

External Security Audit Reports

- Type 1 – Provides the auditor's opinion on the description of control provided by management. Think reviewing policies on paper.

- Type 2- The auditor ensure the operation effectiveness of the controls. Typically covers an extended time period. These are considered more reliable.

Chapter 15: Security Assessment & Testing

Security Assessments

- Broader than audits
- Combine reviews, testing, interviews, and analysis
- Help identify security gaps and risk areas
- Can be qualitative or quantitative

Chapter 15: Security Assessment & Testing

Vulnerability Scanning

- Identifies known flaws and misconfigurations
- Uses signature-based detection
- Should be regular and automated
- Not the same as penetration testing
- Results must be analyzed and prioritized

Network scans: Open ports, services

Credentialed scans: Authenticated, deeper visibility

Non-credentialed scans: Surface-level only

External vs. internal scans

Chapter 15: Security Assessment & Testing

Vulnerability Scanning Limitations

- Cannot detect zero-day vulnerabilities
- May produce false positives or negatives
- Does not test exploitability or business impact
- Still essential as a baseline

Chapter 15: Security Assessment & Testing

Network Discovery Scanning

- Maps devices, systems, and open ports
- Often first step in vulnerability scanning
- Tools: Nmap, Angry IP Scanner
- Risks: May trigger alerts or overwhelm systems if misconfigured

Chapter 15: Security Assessment & Testing

Types of Network Discovery Scanning

- **TCP SYN:** Sends a packet with the SYN flag
- **TCP Connect:** Tries to open a full connection to the remote system
- **TCP ACK:** Sends a packet with ACK flag, indicating it's part of an open connection
- **XMAS Scanning:** Sends FIN, PSH, & URG flags

Chapter 15: Security Assessment & Testing

Network Discovery Port Status

- **Open:** An application is accepting connections
- **Closed:** Open on the firewall but nothing is accepting a connection
- **Filtered:** Unable to determine the status due to a firewall rule

Port	Service
22	FTP
53	DNS
443	HTTPS
3389	RDP

Chapter 15: Security Assessment & Testing

Web Application Vulnerability Scanning

- Targets web applications and APIs
- Looks for:
- SQL injection
- Cross-site scripting (XSS)
- Insecure cookies, headers
- Broken authentication
- Tools: OWASP ZAP, Burp Suite, Nikto

Chapter 15: Security Assessment & Testing

Interpreting Scan Results

- Don’t treat every finding equally
- Consider:
- Exploitability
- Asset criticality
- Exposure (internal vs. external)
- Compensating controls
- Prioritize based on business risk

Detection, Validation. Remediation

Chapter 15: Security Assessment & Testing

Describing Vulnerabilities

Common Vulnerabilities and Exposures (CVE):

Unique identifier for publicly known vulnerabilities
Managed by MITRE
Example: CVE-2023-4567

Chapter 15: Security Assessment & Testing

Describing Vulnerabilities

Common Vulnerability Scoring System (CVSS):

Rates vulnerability severity (0.0 to 10.0)
Based on exploitability, impact, and environment
Three metric groups:
Base (intrinsic severity)
Temporal (current state)
Environmental (org-specific)

Chapter 15: Security Assessment & Testing

CCE, CPE, XCCDF, OVAL – Overview

- **CCE:** Common Configuration Enumeration (standardized misconfiguration IDs)
- **CPE:** Common Platform Enumeration (standard names for software/hardware)
- **XCCDF:** XML-based format for security checklists
- **OVAL:** Open Vulnerability and Assessment Language (automates security state info)

Chapter 15: Security Assessment & Testing

Penetration Testing Overview

- Simulates a real-world attack
- Actively exploits vulnerabilities
- Often includes social engineering and physical access
- Requires skilled testers and clear rules of engagement

Black Box: No internal knowledge (simulates external attacker)
White Box: Full knowledge of systems (simulates insider)
Gray Box: Partial knowledge (simulates partner or compromised account)

Chapter 15: Security Assessment & Testing

Penetration Testing Phases

Planning: Define scope, objectives, get authorization
Discovery/Reconnaissance: Gather information
Attack/Exploitation: Attempt access or disruption
Reporting: Document findings, impact, and recommendations

Chapter 15: Security Assessment & Testing

Application Code Review

- Manual or automated inspection of source code
- Identifies security flaws early
- Looks for:
- Input validation issues
- Hardcoded credentials
- Poor error handling
- Logic errors

Chapter 15: Security Assessment & Testing

Static Application Security Testing (SAST)

- Analyzes source code or binaries without running the app
- Finds flaws early in the development cycle
- Common tools: Checkmarx, Fortify, SonarQube
- Fast and scalable

Chapter 15: Security Assessment & Testing

Dynamic Application Security Testing (DAST)

- Tests a running application from the outside
- Focuses on runtime behavior and inputs
- Detects real-world vulnerabilities (e.g., XSS, SQLi)
- Common tools: OWASP ZAP, Burp Suite

Chapter 15: Security Assessment & Testing

Fuzz Testing (Fuzzing)

- Sends malformed or unexpected input to the system
- Helps find crashes, memory leaks, logic errors
- Common in software testing and protocol testing
- Often automated (e.g., AFL, Peach Fuzzer)

Chapter 15: Security Assessment & Testing

Interface Testing

- Focuses on communication between systems, modules, or APIs
- Verifies proper input/output handling
- Ensures secure integration
- Especially important for web services and microservices

Chapter 15: Security Assessment & Testing

Misconfiguration Testing

- Identifies weak or incorrect system settings
- Common findings:
- Open ports
- Default credentials
- Unpatched services
- Directory browsing
- Use automated tools and checklists (e.g., CIS Benchmarks)

Chapter 15: Security Assessment & Testing

Common Security Metrics

- Number of vulnerabilities detected
- Time to patch (TTP)
- Incident response time
- User policy violations
- Percentage of systems compliant with baseline

Chapter 15: Security Assessment & Testing

Key Performance Indicators (KPIs)

- Track progress toward strategic objectives
- Should align with business goals
- Examples:
- % of users completing security training
- Reduction in phishing click rates
- Mean time to detect/respond (MTTD/MTTR)

Chapter 15: Security Assessment & Testing

Key Risk Indicators (KRIs)

- Early warning signs of increasing risk
- Help prioritize preventative action
- Examples:
- Spike in failed login attempts
- Unusual outbound network traffic
- Increase in dormant accounts

Chapter 15: Security Assessment & Testing

Continuous Monitoring

- Ongoing observation of security controls and environments
- Enables rapid detection of changes or threats
- Supports risk-based decision-making
- Powered by automation, analytics, and threat intelligence

Chapter 15: Security Assessment & Testing

Training and Exercises

- **Red Team:** Those trying to gain access
- **Blue Team:** Those trying to secure access
- **White Team:** Observers and judges

- **Purple Team**: The red and blue team working together to share knowledge and tactics

Chapter 15: Security Assessment & Testing

Secure Management Practices

- **Review Logs Regularly:** Check for privilege abuse, unknown activity, and review access. Use NTP to make sure everything is in sync
- **Verify Backups:** Ensure you can restore the data without issue
- **Review Accounts:** Check for inactive accounts, privilege creep, unknown users, and ensure terminated users do not have access.
- **Security Awareness Training:** Educate users about common and new threats, and what to do when they have concerns or questions

Chapter 15: Security Assessment & Testing - Quiz

What does a SOC Type 2 report assess?

A. Control design
B. Incident response
C. Operational effectiveness over time
D. Business continuity

Chapter 15: Security Assessment & Testing - Quiz

What is the goal of fuzz testing?

A. Determine source code quality
B. Prioritize vulnerability remediation
C. Find input handling flaws
D. Determine credential strength

Chapter 15: Security Assessment & Testing - Quiz

Which of the following is a Key Risk Indicator (KRI)

A. Percentage of employees completing security training
B. Increase in dormant accounts
C. Mean time to resolution
D. System uptime

Chapter 15: Security Assessment & Testing

Summary

- Purpose: Validate controls, find weaknesses, and support risk decisions.
- Methods: **Audits, vulnerability scans, pen testing, code reviews**.
- Tools: **SAST, DAST, Fuzzing, OVAL, CVE/CVSS systems**.
- Metrics: **KPIs, KRIs, Continuous Monitoring**.
- Engagements: **Red/Blue/Purple Teaming**, SOC audits (SOC 1, 2, 3).
- Best practices: Risk-based prioritization, regular scanning, clear reporting.

CISSP® MENTOR PROGRAM – SESSION NINE

Chapter 14 & 15

The end!

- You made it to the end of session 9!

- Domains:
- 3 – Security architecture and engineering
- 5 – Identity and access management
- 6 – Security assessment and testing
- 8 – Software development security

I'll see you all on Wednesday!