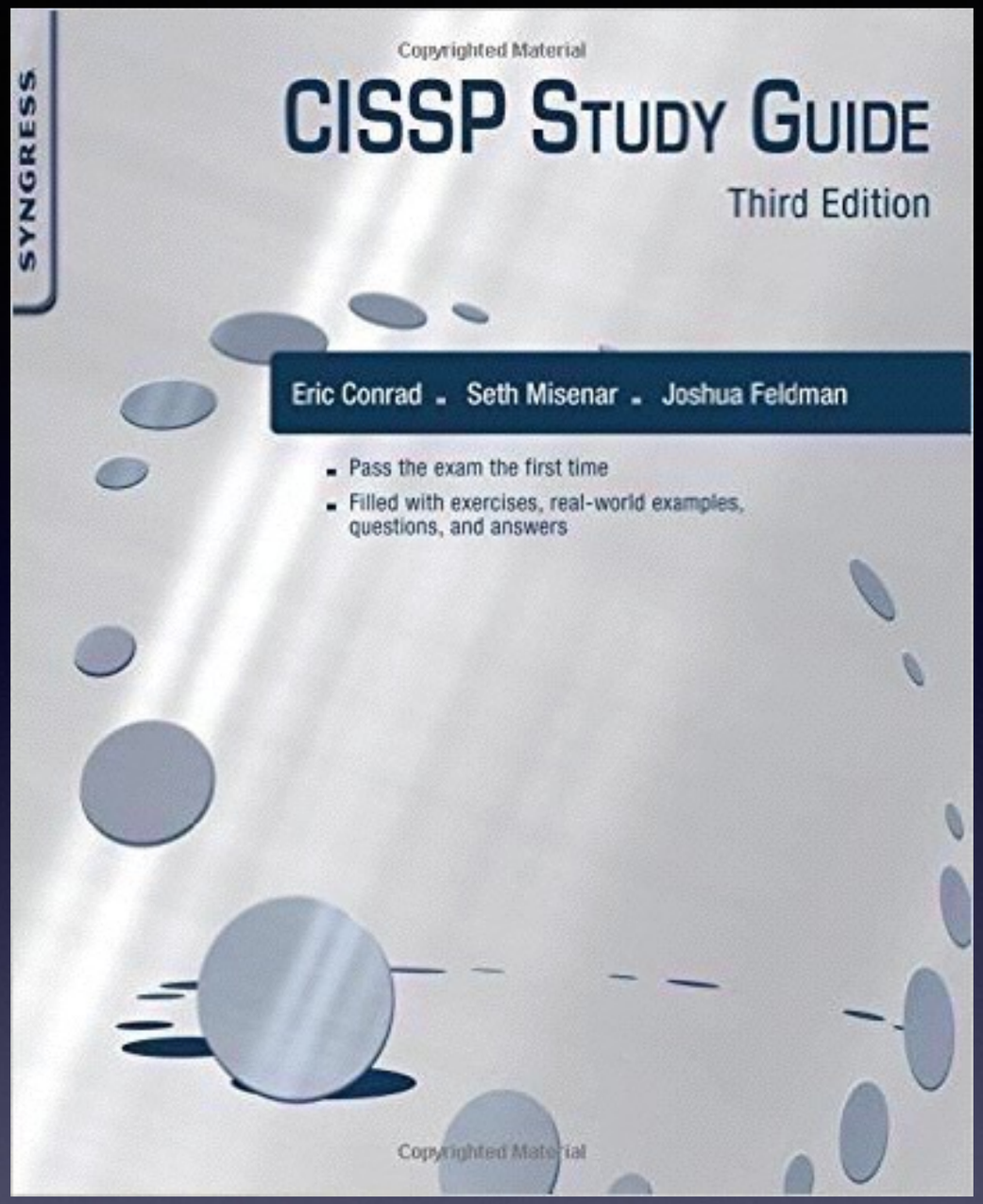
CNIT 125: Information Security Professional (CISSP Preparation)



Ch 7. Security Assessment and Testing

Assessing Access Control

Penetration Testing

- **Authorized white hat hacker breaks into an organization**

Penetration tests may include the following tests:

- Network (Internet)
- Network (internal or DMZ)
- War dialing
- Wireless
- Physical (attempt to gain entrance into a facility or room)

Social Engineering

- **Exploiting the human mind**
- **Often tricks the user into clicking a link**
- **Zero-knowledge (black box) test**
  - **No information provided to attacker**
- **Full-knowledge test**
  - **Provides pen tester with network diagram, policies and procedures, and sometimes results from previous pen testers**
- **Partial-knowledge test**

Penetration Tester Tools and Methodology

- **Metasploit (open source)**
- **Core Impact and Immunity Canvas (closed source)**
- **Methodology**

- Planning
- Reconnaissance
- Scanning (also called enumeration)
- Vulnerability assessment
- Exploitation
- Reporting

Assuring Confidentiality, Data Integrity, and System Integrity

- **Pen testers must ensure confidentiality of data they access**
- **Report should be treated as confidential**

Vulnerability Testing

- **Also called Vulnerability Scanning**
- **Uses a tool like Nessus or OpenVAS**
- **Finds vulnerabilities**
- **Requires manual verification and assessment**
- **Must be matched to real threats to find true risk**

Security Audit

- **Tests against a public standard**
- **Such as PCI-DSS (Payment Card Industry Data Security Standard)**

Security Assessment

- **View many controls across multiple domains**
  - **Policies and procedures**
  - **Administrative controls**
  - **Change management**
  - **Other tests (pen tests, vuln assessments, security audits)**

Internal and Third Party Audits

- **Internal audits**
  - **Assessing adherence to policy**
- **External audits**
  - **Require security professionals to play a role**
  - **Response and remediation to audit findings**
  - **Demonstrating mitigations**

Log Reviews

- **Easiest way to verify that access control mechanisms are working**

- Network Security Software/Hardware:
  - Antivirus logs
  - IDS/IPS logs
  - Remote Access Software (such as VPN logs)
  - Web proxy
  - Vulnerability management
  - Authentication servers
  - Routers and firewalls
- Operating System:
  - System events
  - Audit records
- Applications
  - Client requests and server responses
  - Usage information
  - Significant operational actions [1]

Centralized Logging

- **A central repository allows for more scalable security monitoring and intrusion detection**
- **Syslog transmits log data in plaintext over UDP port 514**
- **Log retention**
  - **May be relevant to legal or regulatory compliance**

Software Testing Methods

Software Testing Methoda

- **Discovering programmer errors**
- **Custom apps don't have a vendor providing security patches**
- **Source code review helps**
- **Two general approaches:**
  - **Static and dynamic analysis**
  - **Also manual code review**
  - **Pair programming is employed in agile programming shops**

Static and Dynamic Testing

- **Static testing: the code is not running**
  - **Review source code for insecure practices, unsafe functions, etc.**
  - **Unix program lint**
  - **Compiler warnings**
- **Dynamic testing: while code is executing**
- **White box testing: tester has source code**
- **Black box: tester has no internal details**

Traceability Matrix

- **Maps customer requirements to software testing plan**

Synthetic Transactions

- **Simulating business activities**
- **Often used for Web apps**

Software Testing Levels

- **Unit testing**
  - **Tests components like functions, procedures, or objects**
- **Installation testing**
  - **Tests software as it is installed and first operated**
- **Integration Testing**
  - **Testing multiple software components as they are combined into a working system**

Software Testing Levels

- **Regression testing**
  - **Testing softare after updates, modification, or patches**
- **Acceptance testing**
  - **Testing to ensure the software meets the customer's requirements**
  - **When done by customer, called User Acceptance Testing**

Fuzzing

- **A type of black box testing**
- **Sends random malformed data into software programs**
- **To find crashes**
- **A type of dynamic testing**
- **Has found many flaws**

Combinatorial Software Testing

- **Seeks to identify and test all unique combinations of software inputs**
- **Pairwise testing (also called *all pairs testing*)**

Misuse Case Testing

- **Formally model an adversary misusing the application**
- **A more formal and commonly recognized way to consider negative security outcomes is *threat modeling***
- **Microsoft highlights it in their Security Development Lifecycle (SDL)**

Test Coverage Analysis

- **Identifies the degree to which code testing applies to the entire application**
- **To ensure that there are no significant gaps**

Analyze and Report Test Outputs

- **Security test results are easy to produce**
- **Actually improving security is much more difficult**
- **Data must be analyzed to determine what action to take**