Information Security Audit

Zehra Irem Kuyucu

Vilnius Gediminas Technical University
Faculty of Fundamental Sciences
Department of Information Technologies

2025

Outline

Introduction

- Security auditing represents a systematic, evidence-based approach to evaluating an organization's security posture
- NIST definition: "an independent review and examination of system records and activities to test for adequacy of system controls, ensure compliance with established policy and operational procedures, and recommend any necessary changes"
- Encompasses technical, operational, and governance aspects of information security

Goals of Security Auditing

- **Risk identification and assessment**: Identify vulnerabilities, threats, and potential impacts
- **Compliance verification**: Ensure adherence to regulatory requirements and industry standards
- **Security control effectiveness evaluation**: Determine if controls function as intended
- **Security posture improvement**: Drive remediation of identified weaknesses
- **Documentation and evidence collection**: Establish records of security status
- **Awareness and accountability promotion**: Highlight importance of security practices

Types of Security Audits

1. **Compliance Audits**
   - Evaluate adherence to regulatory requirements and internal policies
   - Examples: PCI DSS, HIPAA, ISO/IEC 27001, GDPR
2. **Vulnerability Assessment**
   - Discover potential security weaknesses before exploitation
   - Employs structured methodology: scope definition, information gathering, vulnerability identification

Types of Security Audits (continued)

3. **Penetration Testing**
   - Controlled simulation of real-world attacks
   - Actively exploits discovered vulnerabilities to demonstrate business impact
4. **Information Management Audits**
   - Evaluate controls governing information assets throughout lifecycle
   - Focus on information classification, handling, and protection

The Audit Process

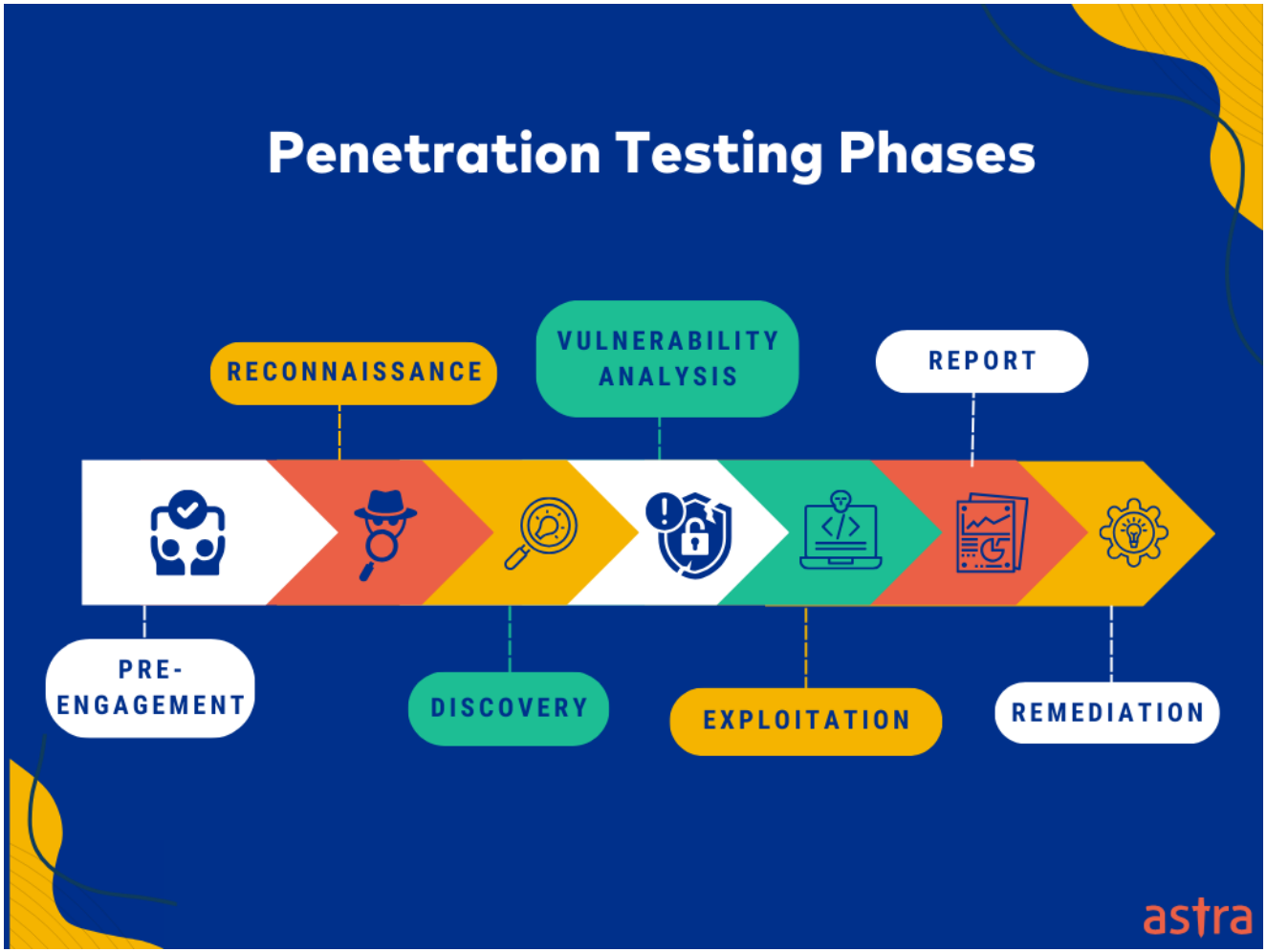

Figure:
https://www.getastra.com/blog/security-audit/penetration-testing-phases/

Pre-Engagement Interactions

- Establish foundation for effective security audits
- Define parameters and expectations before technical activities
- For penetration testing: especially critical due to potentially disruptive nature
- Components:
  - Scoping discussions
  - Rules of engagement
  - Legal considerations
  - Logistical planning
  - Data handling protocols

Intelligence Gathering

- Foundational reconnaissance phase
- Collect information about systems, networks, and organizational structure
- For penetration testing: includes both passive and active techniques
  - **Passive**: collecting publicly available information
  - **Active**: direct interaction with target systems
- Produces target lists, network maps, and vulnerability hypotheses

Threat Modeling

- Bridges intelligence gathering and technical testing
- Systematically analyzes how attackers might compromise assets
- Process includes:
  - System characterization
  - Threat actor identification
  - Vulnerability analysis
- Methodologies: STRIDE, MITRE ATT&CK framework
- Produces prioritized list of potential vulnerabilities and attack vectors

Vulnerability Analysis

- Systematic examination to identify security weaknesses
- Process includes:
  - Vulnerability scanning with automated tools
  - Manual assessment techniques
  - Vulnerability validation
  - Comprehensive documentation
  - Scoring and prioritization (e.g., using CVSS)
- Implementation varies by audit objectives

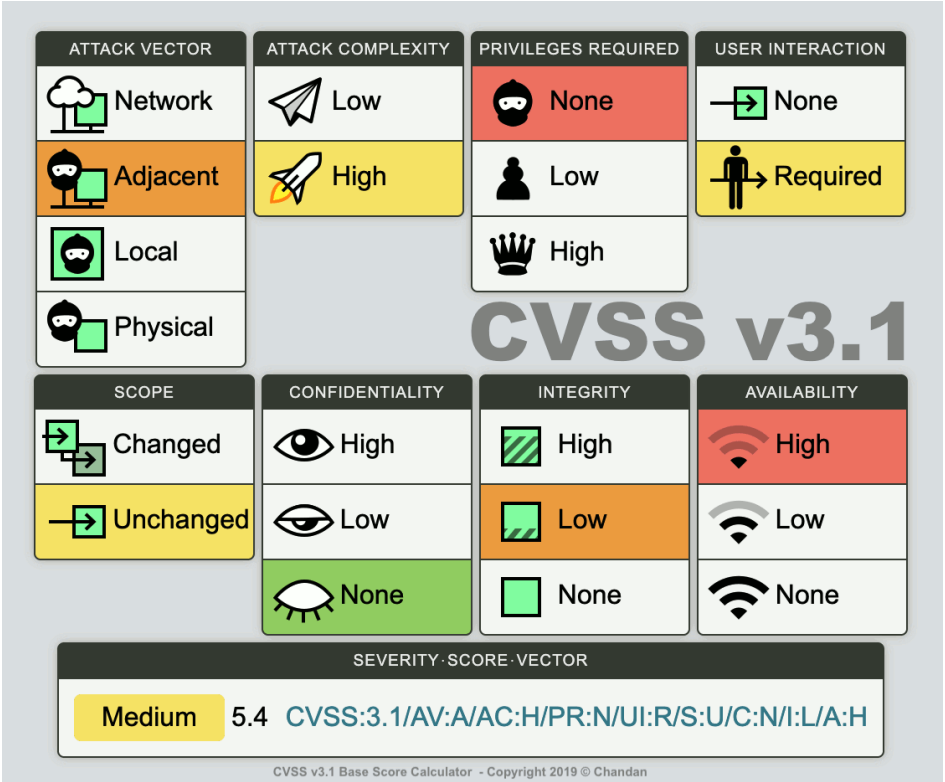

Figure:
https://chandanbn.github.io/cvss/

Exploitation

- Active phase of penetration testing
- Attempts to leverage vulnerabilities for unauthorized access
- Process includes:
  - Target selection
  - Exploitation technique development
  - Execution with detailed documentation
  - Close communication with organizational contacts
- May include social engineering to evaluate human-oriented controls

Post-Exploitation

- Activities conducted after successful system compromise
- Demonstrates potential for escalation and organizational impact
- Common activities:
  - Establishing persistence
  - Privilege escalation
  - Lateral movement
  - Evidence collection
  - Covering tracks
- Provides compelling evidence of potential security impacts

Reporting

- Critical bridge between technical findings and organizational action
- Components include:
  - Comprehensive documentation
  - Executive summaries
  - Detailed technical findings
  - Risk ratings
  - Remediation recommendations
  - Strategic improvement recommendations
- Formal documentation often supplemented by presentations

Conclusions

- Security auditing is a vital component of organizational risk management
- Provides insights into vulnerability exposure, control effectiveness, and compliance
- Specialized assessment types address specific organizational needs
- Structured process enables systematic evaluation of security posture
- Effective security auditing transforms technical findings into actionable intelligence
- Enables targeted improvements and resource allocation

References

- NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations
- NIST Special Publication 800-160: Systems Security Engineering
- ISO/IEC 27007:2020: Guidelines for information security management systems auditing
- ISACA IT Audit Framework (ITAF)
- MITRE ATT&CK Framework
- COBIT 2019 Framework: Introduction and Methodology
- Penetration Testing Execution Standard (PTES) Technical Guidelines

Thank You

Questions?

Zehra Irem Kuyucu
Information Security Management
Vilnius Gediminas Technical University