Auditing Fundamentals

Course Introduction

Alexis Ahmed

Senior Penetration Tester @HackerSploit
Offensive Security Instructor @INE

Course Topic Overview

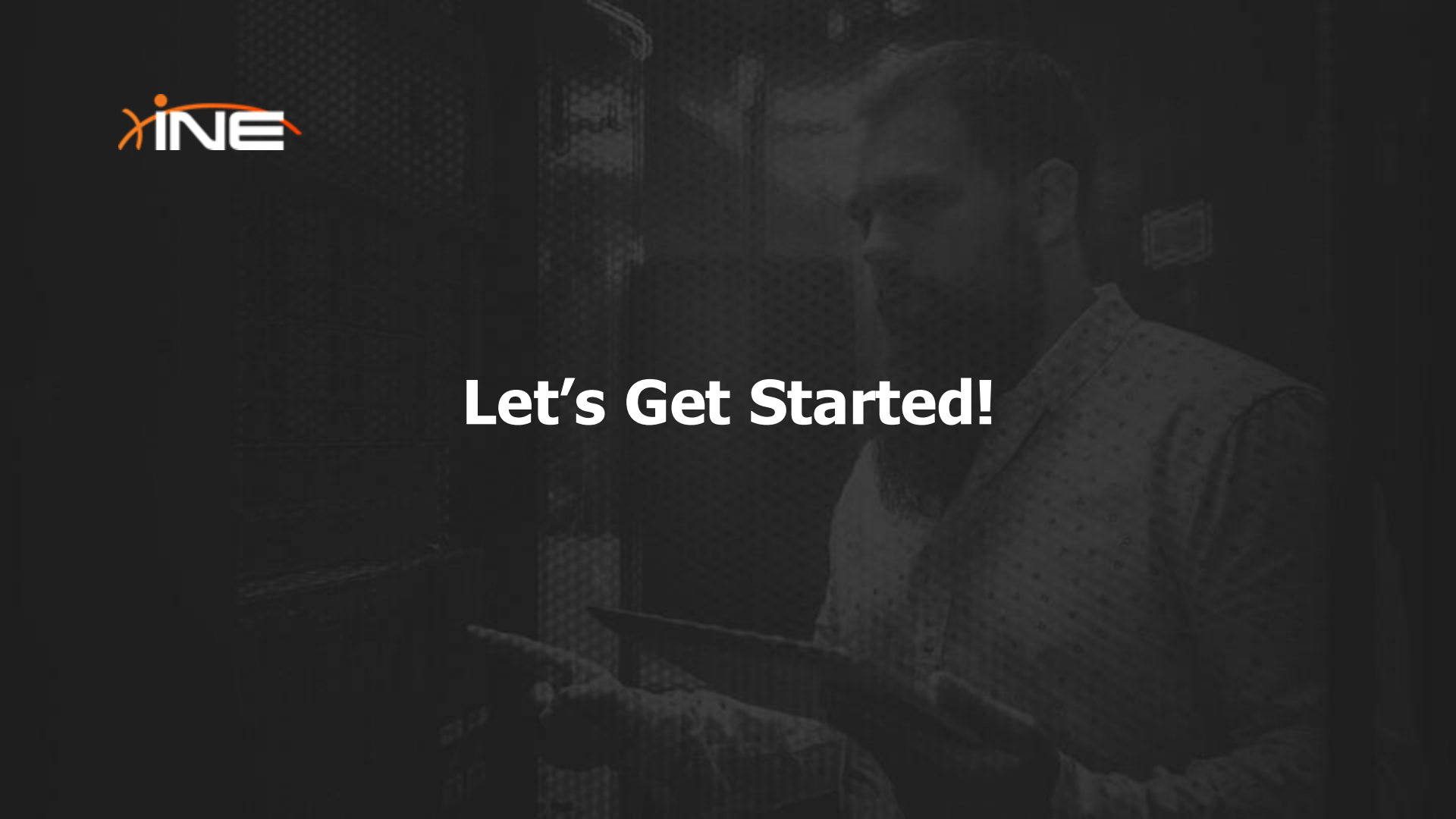
- Introduction To Security Auditing
- Essential Terminology
- Security Auditing Process/Lifecycle
- Types of Security Audits
- The Link between Security Auditing & Penetration Testing
- Compliance Standards, Regulations and Frameworks

Prerequisites

- Basic Understanding of Cybersecurity Concepts: Familiarity with fundamental cybersecurity principles and terminology.
- Basic Understanding of the Penetration Testing Lifecycle and methodology.
- Knowledge of Network and Application Security: Understanding of network protocols, architecture, and common security practices.
- Basic Familiarity with Security Tools: Experience using security tools such as Nessus, Nmap, and Wireshark.
- Awareness of Compliance Standards: Basic knowledge of regulatory requirements and industry standards (e.g., PCI DSS, ISO 27001).

Learning Objectives/Outcomes:

- Understand the Role of Security Auditing: Grasp the importance and objectives of security auditing within an organization.
- Differentiate Between Audits, Assessments, and Tests: Clearly distinguish between security auditing, vulnerability assessments, and penetration tests.
- Learn the Security Auditing Process: Gain knowledge of the steps involved in conducting a comprehensive security audit.
- Assess Compliance Requirements: Understand how to evaluate and ensure compliance with regulatory standards.
- Apply Security Auditing Techniques: Learn practical techniques for auditing networks, systems, applications, and policies.
- Integrate Audits with Penetration Testing: Understand how security auditing supports and enhances penetration testing efforts.


Let’s Get Started!

Overview of Security Auditing

What is Security Auditing?

- Security Auditing is a systematic process of evaluating and verifying the security measures and controls in place within an organization to ensure they are effective, appropriate, and compliant with relevant standards, policies, and regulations.

- It involves reviewing various aspects of the organization's information systems, networks, applications, and operational procedures to identify vulnerabilities, weaknesses, and areas for improvement.

Importance of Security Auditing

1. Identifying Vulnerabilities and Weaknesses:

- Security audits help uncover vulnerabilities and weaknesses in an organization's information systems and infrastructure that could be exploited by attackers.

- Regular audits ensure that security controls are effective and up-to-date, minimizing the risk of breaches.

Importance of Security Auditing

2. Ensuring Compliance:

- Organizations must comply with various regulatory requirements and industry standards to protect sensitive data and maintain trust with customers and stakeholders.

- Security audits help verify compliance with standards such as GDPR, HIPAA, PCI DSS, and ISO 27001, avoiding legal and financial penalties.

Importance of Security Auditing

3. Enhancing Risk Management:

- Audits provide a comprehensive assessment of an organization's security posture, identifying and prioritizing risks based on their potential impact.
- Effective risk management strategies can be developed and implemented based on audit findings to mitigate identified risks.

Importance of Security Auditing

4. Improving Security Policies & Procedures:

- Security audits review the effectiveness of existing security policies and procedures, identifying areas for improvement.
- Updated and robust security policies and procedures help create a strong security culture within the organization.

Importance of Security Auditing

6. Supporting Business Objectives:

- A strong security posture supports overall business objectives by ensuring that critical business operations are protected from disruptions caused by security incidents.

- Audits help build customer trust and confidence, as clients are assured that their data is handled securely and responsibly.

Importance of Security Auditing

7. Continuous Improvement:

- Security auditing is not a one-time activity but an ongoing process that promotes continuous improvement.
- Regular audits ensure that security measures evolve to address new threats and vulnerabilities, maintaining a proactive approach to security.

Essential Terminology

Essential Terminology

Term	Definition	Importance
Security Policies	Formal documents that define an organization's security objectives, guidelines, and procedures to protect information assets.	Establishes the framework for implementing and enforcing security controls.
Compliance	Adherence to regulatory requirements, industry standards, and internal policies related to security and data protection.	Ensures that the organization meets legal obligations and best practices.
Vulnerability	A weakness in a system or process that can be exploited to gain unauthorized access or cause harm.	Identifying vulnerabilities is crucial for assessing and improving security measures.
Control	A safeguard or countermeasure implemented to mitigate risks and protect information assets.	Controls are designed to prevent, detect, or respond to security threats and weaknesses.
Risk Assessment	The process of identifying, analyzing, and evaluating risks to an organization’s information assets.	Helps prioritize security measures based on the likelihood and impact of identified risks.

Essential Terminology

Term	Definition	Importance
Audit Trail	A chronological record of events and activities that provides evidence of actions taken within a system.	Supports accountability and traceability during security audits and investigations.
Compliance Audit	An examination of an organization's adherence to regulatory requirements and industry standards.	Validates whether the organization meets the necessary compliance criteria and identifies areas for improvement.
Access Control	Measures and mechanisms used to regulate who can access specific information or systems and what actions they can perform.	Protects sensitive information from unauthorized access and misuse.
Audit Report	A formal document that presents the findings, conclusions, and recommendations resulting from a security audit.	Communicates audit results and provides guidance for improving security practices.

Security Auditing Process/Lifecycle

Security Auditing Process

1. Planning and Preparation

- Define Objectives and Scope: Determine the goals of the audit and the specific systems, processes, and controls to be evaluated.
- Gather Relevant Documentation: Collect policies, procedures, network diagrams, and previous audit reports.
- Establish Audit Team and Schedule: Assemble the audit team and set a timeline for the audit activities.

Security Auditing Process

2. Information Gathering

- Review Policies and Procedures: Examine the organization’s security policies, procedures, and standards.
- Conduct Interviews: Interview key personnel to understand security practices and identify potential gaps.
- Collect Technical Information: Gather data on system configurations, network architecture, and security controls.

Security Auditing Process

3. Risk Assessment

- Identify Assets and Threats: List critical assets and potential threats to those assets.
- Evaluate Vulnerabilities: Assess existing vulnerabilities in systems and processes.
- Determine Risk Levels: Assign risk levels based on the likelihood and impact of identified threats and vulnerabilities.

Security Auditing Process

4. Audit Execution

- Perform Technical Testing: Conduct technical assessments such as vulnerability scans, penetration tests, and configuration reviews.
- Verify Compliance: Check adherence to relevant regulations and standards.
- Evaluate Controls: Assess the effectiveness of security controls and practices.

Security Auditing Process

5. Analysis and Evaluation

- Analyze Findings: Review data collected during the audit to identify security weaknesses and areas for improvement.
- Compare Against Standards: Measure the organization's security posture against industry standards and best practices.
- Prioritize Issues: Rank findings based on their severity and potential impact on the organization.

Security Auditing Process

6. Reporting

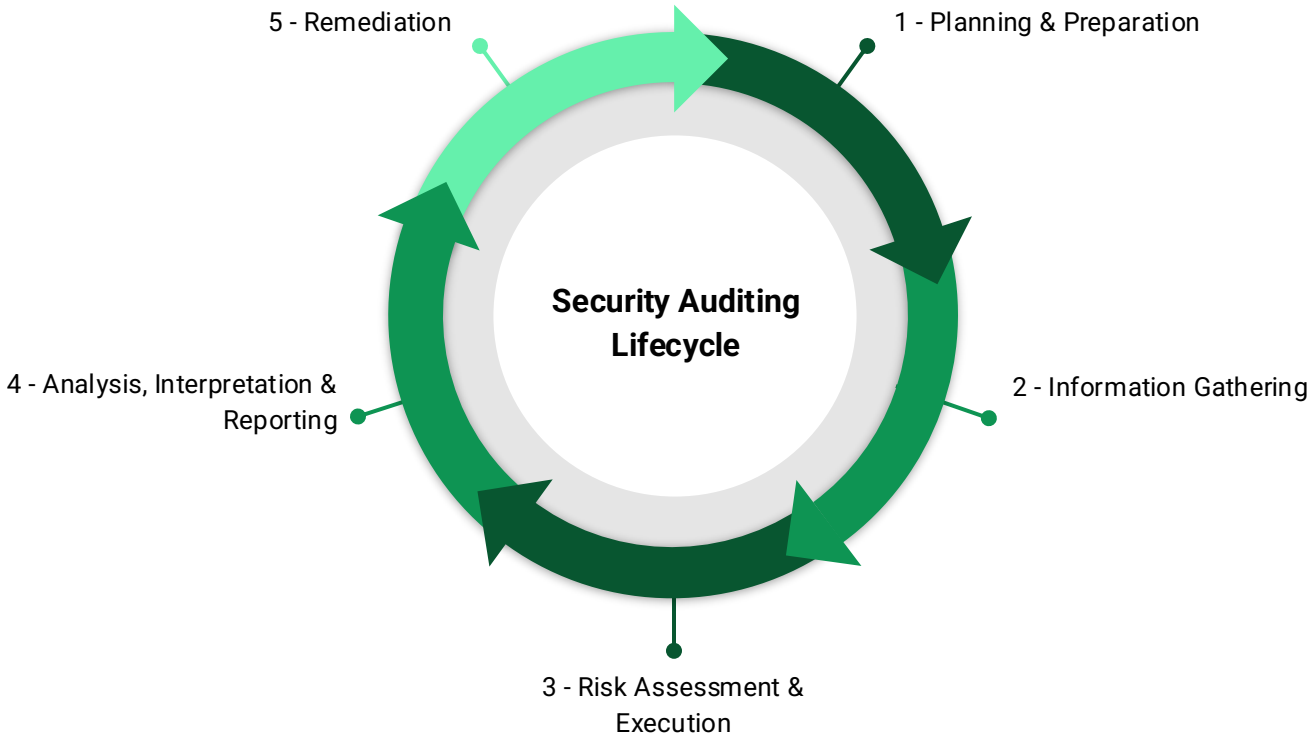
- Document Findings: Create a detailed report outlining audit findings, including identified vulnerabilities, non-compliance issues, and ineffective controls.
- Provide Recommendations: Offer actionable recommendations to address identified issues and enhance security.
- Present Results: Share the audit report with relevant stakeholders and discuss key findings and recommendations.

Security Auditing Process

7. Remediation

- Develop Remediation Plans: Work with the organization to create plans for addressing the audit findings.
- Implement Changes: Assist in implementing recommended changes and improvements.
- Conduct Follow-Up Audits: Schedule follow-up audits to ensure that remediation efforts have been completed and are effective.
- Monitor and Update: Continuously monitor the organization’s security posture and update security measures as needed.

Security Auditing Lifecycle



Types of Security Audits

Types of Security Audits

- Security audits can be categorized based on their scope, methodology, and the aspects of the organization they focus on.
- For penetration testers, understanding these different types of security audits is crucial to tailor their testing strategies effectively.
- The next slide outlines the main types of security audits:

Types of Security Audits

Security Audit	Objective	Importance	Example
Internal Audits	Conducted by the organization's internal audit team or security professionals to evaluate the effectiveness of internal controls and compliance with policies.	Internal audits provide insight into the organization’s self-assessment of its security posture and highlight areas that may require more in-depth testing.	An internal audit might review user access controls to ensure that only authorized personnel have access to sensitive data.
External Audits	Performed by independent third-party auditors to provide an unbiased evaluation of the organization’s security measures and compliance with external standards.	External audits often serve as benchmarks for compliance and security effectiveness. Penetration testers can use these findings to guide their testing efforts.	A company undergoing a PCI DSS compliance audit might hire an external auditor to validate its security controls and ensure they meet the required standards.
Compliance Audits	Focus on verifying that the organization complies with specific regulatory requirements and industry standards (e.g., GDPR, HIPAA, PCI DSS).	Compliance audits help identify regulatory gaps that penetration testers can address through targeted testing.	A healthcare provider might undergo a HIPAA compliance audit to ensure that patient data is protected according to federal regulations.

Types of Security Audits

Security Audit	Objective	Importance	Example
Technical Audits	Focus on assessing the technical aspects of the organization's IT infrastructure, including hardware, software, and network configurations.	Technical audits provide a detailed view of the technical controls in place, highlighting areas where penetration testing can uncover vulnerabilities.	A technical audit might involve a thorough review of firewall configurations to ensure they are properly securing the network perimeter.
Network Audits	Assess the security of the organization's network infrastructure, including routers, switches, firewalls, and other network devices.	Network audits can reveal vulnerabilities in network design and configurations that penetration testers can exploit to assess network security.	A network audit might identify insecure protocols being used for data transmission, prompting penetration testers to test for potential exploits.
Application Audits	Evaluate the security of software applications, focusing on code quality, input validation, authentication mechanisms, and data handling.	Application audits highlight security flaws in applications that penetration testers can exploit to demonstrate real-world attack scenarios.	An application audit might reveal vulnerabilities such as SQL injection or cross-site scripting (XSS) in a web application.

Security Auditing & Penetration Testing

Security Auditing & Penetration Testing

- In order for you to operate successfully as a penetration tester, it is imperative that you understand **when, how and why** Security Audits are performed and how they relate to and affect penetration testing.

- The reason this is important is because Security Audits and Penetration testing are two separate types of security assessments that have their own unique scope, objectives and desired outcomes.

- Furthermore, given the separation, it is important to understand when each is performed (sequentially), and whether they can be combined into a singular process/assessment.

Security Auditing & Penetration Testing

- Before we dive into the when and the how, we first need to understand the differences between a Security Audit and a Penetration Test, more specifically, the differences in their objectives, scope and outcomes.

- Understanding the differences between the two will paint a clearer picture as to when each assessment is performed and how they (potentially) feed into each other.

Security Auditing vs. Penetration Testing

	Security Audit	Penetration Test
Purpose	Evaluate an organization's overall security posture by assessing compliance with policies, standards, and regulations. It focuses on the effectiveness of security controls, processes, and practices.	Simulate real-world attacks to identify and exploit vulnerabilities in systems, networks, or applications. It focuses on technical weaknesses and how they can be exploited by attackers.
Scope	Comprehensive, covering various aspects such as policies, procedures, technical controls, physical security, and compliance with regulations.	Specific to the systems, networks, or applications being tested. The scope is defined to focus on particular areas of interest.
Methodology	Typically involves reviewing documentation, conducting interviews, performing technical assessments, and evaluating compliance with security standards.	Involves using various tools and techniques to attempt to breach systems, exploit vulnerabilities, and assess the effectiveness of security defenses.
Outcome	Identifies gaps in security policies, procedures, and controls. Provides recommendations for improving overall security and ensuring compliance.	Provides a detailed assessment of vulnerabilities and potential attack vectors. Offers recommendations for mitigating identified risks and improving security defenses.
Frequency	Often performed on a regular basis (e.g., annually or biannually) or as required by compliance regulations.	Typically performed as needed, such as after significant changes to systems, on a regular schedule, or as part of compliance requirements.

Sequential Approach

- **Perform Security Audit First**: Companies often conduct a security audit first to evaluate their overall security posture, ensure compliance with regulations, and identify areas for improvement in policies and procedures.

- **Conduct Penetration Test Afterwards**: Based on the findings of the audit, a penetration test may be performed to assess the effectiveness of technical controls and identify specific vulnerabilities.

Sequential Approach

Advantages

+ Provides a comprehensive view of security from both policy and technical perspectives.

+ Identifies and addresses gaps in both procedural and technical controls.

+ Helps prioritize remediation efforts based on audit findings.

Combined Approach

- **Integrate Security Audit and Penetration Testing**: Some organizations choose to combine security audits and penetration tests, often through a holistic security assessment that incorporates both elements.

Advantages

+ Streamlines the assessment process by combining policy, procedural, and technical evaluations.
+ Provides a more complete picture of the organization's security posture in a single engagement.
+ Can be more efficient and cost-effective by addressing both compliance and technical vulnerabilities simultaneously.

Example

Example: Sequential Approach

- Consider a fictional organization, "SecurePayments Inc.," which processes credit card transactions and must adhere to PCI DSS standards.

- In this example, “SecurePayments Inc.” is using a sequential approach to assess their overall security posture. The organization has already performed a security audit through an independent audit firm and are using the findings in the audit report as the basis of their remediation plan/efforts.

- As part of their remediation plan, the organization has decided to hire you (or your firm) to perform a penetration test with a focus on ensuring PCI DSS compliance.

Example: Sequential Approach

- The external audit performed by the independent audit firm outlined the following findings:
  - Inadequate encryption for cardholder data in transit.
  - Weak/inadequate network security controls and traffic monitoring.
  - Weak access control policies that allow excessive permissions.
  - Outdated incident response procedures
- The corresponding recommendations for the findings outlined above are:
  - Implement strong encryption protocols for data in transit.
  - Revise access control policies to follow the principle of least privilege.
  - Update and test incident response procedures regularly.

The company followed the Security Audit lifecycle/process outlined in the “Security Auditing Process/Lifecycle video and made the necessary improvements based on the recommendations.

Example: Sequential Approach

SecurePayments Inc. - Penetration Test

Objectives:

- After making the necessary changes/improvements based on the findings and recommendations in the external audit report, "SecurePayments Inc.," has hired you to test the technical controls and security measures implemented based on audit findings to verify whether they are effective.

Example: Sequential Approach

SecurePayments Inc. - Penetration Test

Phase 1: Planning and Preparation:

During the initial phase, you identify that the PCI DSS scope includes the cardholder data environment (CDE). You review SecurePayments Inc.'s network diagrams and PCI DSS self-assessment questionnaires to understand their current security measures and compliance status.

Objectives:

- Define the scope of the penetration test to focus on the areas identified in the audit, such as network security and application vulnerabilities.
- Set up a testing schedule and inform stakeholders.

Example: Sequential Approach

SecurePayments Inc. - Penetration Test

Phase 2: Information Gathering and Reconnaissance:

- You gather information on SecurePayments Inc.'s security policies, such as their access control policies, encryption standards, and incident response procedures.
- You also review their most recent PCI DSS audit report to identify areas of concern highlighted by auditors.

Example: Sequential Approach

SecurePayments Inc. - Penetration Test

Phase 3: Penetration Test Execution:

- Conduct network scanning, enumeration and vulnerability assessments to identify weaknesses, misconfigurations or vulnerabilities.
- Attempt exploitation of identified vulnerabilities to assess their impact.
- Test the effectiveness of newly implemented encryption and access controls.

Example: Sequential Approach

SecurePayments Inc. - Penetration Test

Phase 4: Findings and Recommendations:

- Outcome: The penetration test uncovers additional vulnerabilities:
  - An exposed administrative interface that allows unauthorized access.
  - SQL injection vulnerabilities in a customer-facing web application.

- Recommendations:
  - Secure the administrative interface by implementing additional authentication and access controls.
  - Patch the SQL injection vulnerabilities and conduct a thorough review of application security.

Example: Sequential Approach

Summary of Sequential Approach

- Security Audit Results:
  - Identified compliance gaps and policy deficiencies.
  - Provided recommendations for improving security policies and procedures.

- Penetration Testing Results:
  - Revealed specific technical vulnerabilities.
  - Offered targeted recommendations to address these technical weaknesses.

Governance, Risk & Compliance (GRC)

Governance, Risk & Compliance (GRC)

- Governance, Risk, and Compliance (GRC) is a comprehensive framework used by organizations to manage and align their governance practices, risk management strategies, and compliance with regulatory requirements.

- This holistic approach helps organizations maintain transparency, accountability, and resilience in an increasingly complex regulatory environment.

Governance, Risk & Compliance (GRC)

Governance

- Governance refers to the framework of policies, procedures, and practices that ensure an organization achieves its objectives, manages its risks, and complies with legal and regulatory requirements.
- Components:
  - Policy Development: Creating clear, comprehensive security policies.
  - Roles and Responsibilities: Defining roles and responsibilities for security management.
  - Accountability: Establishing accountability mechanisms for security performance.

Governance, Risk & Compliance (GRC)

Risk

- Risk management involves identifying, assessing, and mitigating risks that could negatively impact an organization's assets and operations.

- Components:
  - Risk Identification: Recognizing potential threats and vulnerabilities.
  - Risk Assessment: Evaluating the likelihood and impact of identified risks.
  - Risk Mitigation: Implementing measures to reduce or eliminate risks.

Governance, Risk & Compliance (GRC)

Compliance

- Compliance ensures that an organization adheres to relevant laws, regulations, and industry standards.

- Components:
  - Regulatory Requirements: Meeting legal obligations such as GDPR, HIPAA, or PCI DSS.
  - Internal Policies: Adhering to internal security policies and procedures.
  - Audits and Assessments: Conducting regular reviews to ensure compliance.

Importance of GRC in Penetration Testing

- Comprehensive Security Assessment: Understanding GRC helps testers conduct more thorough and relevant assessments.
- Enhanced Reporting: Knowledge of GRC allows testers to frame their findings in the context of organizational policies, risk management, and compliance requirements.
- Strategic Recommendations: Testers can provide more strategic recommendations that align with the organization's GRC framework, helping to strengthen overall security posture.

Common Standards, Frameworks & Guidelines

Frameworks, Standards and Guidelines

- Frameworks: Provide a structured approach to implementing security practices, often flexible and adaptable to various organizations and industries.
- Standards: Set specific requirements and criteria that must be met to achieve compliance; often mandatory in regulated industries.
- Guidelines: Offer recommended practices and advice to improve security; generally not mandatory but considered best practices.

Frameworks

NIST Cybersecurity Framework (CSF)

- Overview: A set of guidelines and best practices developed by the National Institute of Standards and Technology (NIST) to help organizations manage and reduce cybersecurity risk.
- Key Focus: Core functions include Identify, Protect, Detect, Respond, and Recover.

COBIT (Control Objectives for Information and Related Technologies)

- Overview: A framework for developing, implementing, monitoring, and improving IT governance and management practices.
- Key Focus: Aligning IT goals with business objectives, managing IT risks, and ensuring compliance with regulations.

Standards

ISO/IEC 27001

- Overview: An international standard for information security management systems (ISMS) that outlines best practices for managing and protecting sensitive information.
- Key Focus: Establishing, implementing, maintaining, and continually improving an ISMS.

PCI Data Security Standard (PCI DSS)

- Overview: A set of security standards designed to protect payment card information and ensure secure processing of credit card transactions.
- Key Focus: Requirements for protecting cardholder data, maintaining a secure network, and implementing robust access control measures.
- Legal Requirement: Required for organizations that handle credit card transactions.

Standards

HIPAA (Health Insurance Portability and Accountability Act)

- Overview: A U.S. law that sets standards for protecting sensitive patient information and ensuring privacy and security of health data.
- Key Focus: Privacy Rule, Security Rule, and Breach Notification Rule.
- Legal Requirement: Required for healthcare providers, health plans, and other entities handling protected health information.

Standards

GDPR (General Data Protection Regulation)

- Overview: A regulation in the European Union that governs data protection and privacy for individuals within the EU and the European Economic Area (EEA).
- Key Focus: Data protection principles, rights of data subjects, and obligations for data controllers and processors.
- Legal Requirement: Required for organizations processing personal data of individuals within the EU/EEA.

Guidelines

CIS Controls (Center for Internet Security Controls)

- Overview: A set of best practices and actionable steps to help organizations improve their cybersecurity posture.
- Key Focus: Foundational and advanced security controls organized into categories such as basic, foundational, and organizational controls.

Guidelines

NIST SP 800-53

- Overview: A publication by NIST that provides a catalog of security and privacy controls for federal information systems and organizations.
- Key Focus: Security controls for federal information systems, including controls for risk management and information security.
- Legal Requirement: Required for U.S. federal agencies and organizations handling federal data.

Phase 1 - Develop a Security Policy

From Audit to Pentest

- We will use a practical example to explain and demonstrate how security audits work, how they are performed and how they relate to a penetration test.

- The objective of this section is to provide you with tacit knowledge of how results from security audits affect the objectives and scope of a penetration test, in addition to outlining the changes/adaptations that need to be made when performing a pentest for an organization that is required to comply with specific standards or regulations.

From Audit to Pentest

Background:

- Company: SecureTech Solutions

Description:

- SecureTech Solutions is a fictitious cybersecurity consultancy that specializes in securing IT infrastructure for various clients.
- In this example, we will be demonstrating the process of developing a security policy for Linux servers, performing a risk assessment using the NIST SP 800-53 framework, performing a security audit and testing the remediations.
- This example will guide you through the entire process, from initial policy creation to auditing and penetration testing, highlighting the importance of compliance with industry standards.

Phase 2 - Developing a Security Policy

Objectives:

- Establish a baseline security policy for Linux servers that aligns with NIST SP 800-53 guidelines, ensuring that servers are configured and managed securely.
- This policy should ensure that Linux servers are secure and protected from unauthorized access, vulnerabilities, and other security threats.
- It will be used to establish baseline security requirements for configuring, maintaining, and monitoring Linux servers within the organization, aligned with NIST SP 800-53.

Phase 1 - Developing a Security Policy

Security Policy Development Process: Requirements Gathering

- Purpose: Define the purpose and scope of the security policy.
- Access Control: Outline user account management, authentication methods, and privilege management.
- Audit and Accountability: Specify logging requirements and log review procedures.
- Configuration Management: Define baseline configurations, software update practices, and change management.
- Identification and Authentication: Enforce strong password policies and unique user identification.

Phase 1 - Developing a Security Policy

Security Policy Development Process: Requirements Gathering

- System and Information Integrity: Implement malware protection, security monitoring, and vulnerability management.
- Maintenance: Outline controlled maintenance and approved maintenance tools.

Phase 1 - Developing a Security Policy

Simple Security Policy for Linux Servers Aligned with NIST SP 800-53

Policy Area	Control ID	Policy Statement
Access Control (AC)	AC-2, AC-5	User Accounts: Only authorized personnel shall be granted access to Linux servers. Each user must have a unique user account; shared accounts are prohibited. Inactive accounts must be disabled or removed within 30 days.
	IA-2, IA-5	Authentication: Enforce strong password policies: minimum length of 12 characters, including upper/lower case letters, numbers, and special characters. Use SSH key-based authentication where possible; disable password-based SSH access. Implement two-factor authentication (2FA) for privileged accounts.
Audit and Accountability (AU)	AU-2, AU-3	System Logging: Enable and configure system logging to capture critical events. Use rsyslog or journald for centralized logging.
	AU-6, AU-7	Log Review: Regularly review logs for suspicious activities. Retain logs for at least 90 days.

Phase 1 - Developing a Security Policy

Simple Security Policy for Linux Servers Aligned with NIST SP 800-53

Policy Area	Control ID	Policy Statement
Configuration Management	CM-2	Configuration Baseline: Maintain a secure baseline configuration for all Linux servers. Use configuration management tools (e.g., Ansible, Puppet) to enforce configurations.
	CM-3, CM-5	Software Updates: Keep the system and installed software up to date. Apply security patches within 30 days of release.
Identification and Authentication (IA)	IA-5	Password Management: Enforce password complexity and expiration policies. Use password managers to securely store and manage passwords.
	IA-4	User Identification: Ensure all users are uniquely identified.

Phase 1 - Developing a Security Policy

Simple Security Policy for Linux Servers Aligned with NIST SP 800-53

Policy Area	Control ID	Policy Statement
System and Information Integrity (SI)	SI-3	Malware Protection: Implement malware detection and prevention measures. Regularly scan servers for malware.
	SI-4	**Security Monitoring: Monitor systems for security breaches or anomalies. Use tools like Lynis to perform regular security audits.**
Maintenance (MA)	MA-2	Controlled Maintenance: Perform regular maintenance on servers according to documented procedures.
	MA-3	Maintenance Tools: Use only approved maintenance tools and ensure they are secure.

Phase 2 - Security Auditing With Lynis

Phase 2 - Security Auditing With Lynis

Objective: Perform a security audit on a Linux server using Lynis, identify vulnerabilities, and remediate the findings based on the security policy.

1. Installing and Running Lynis:

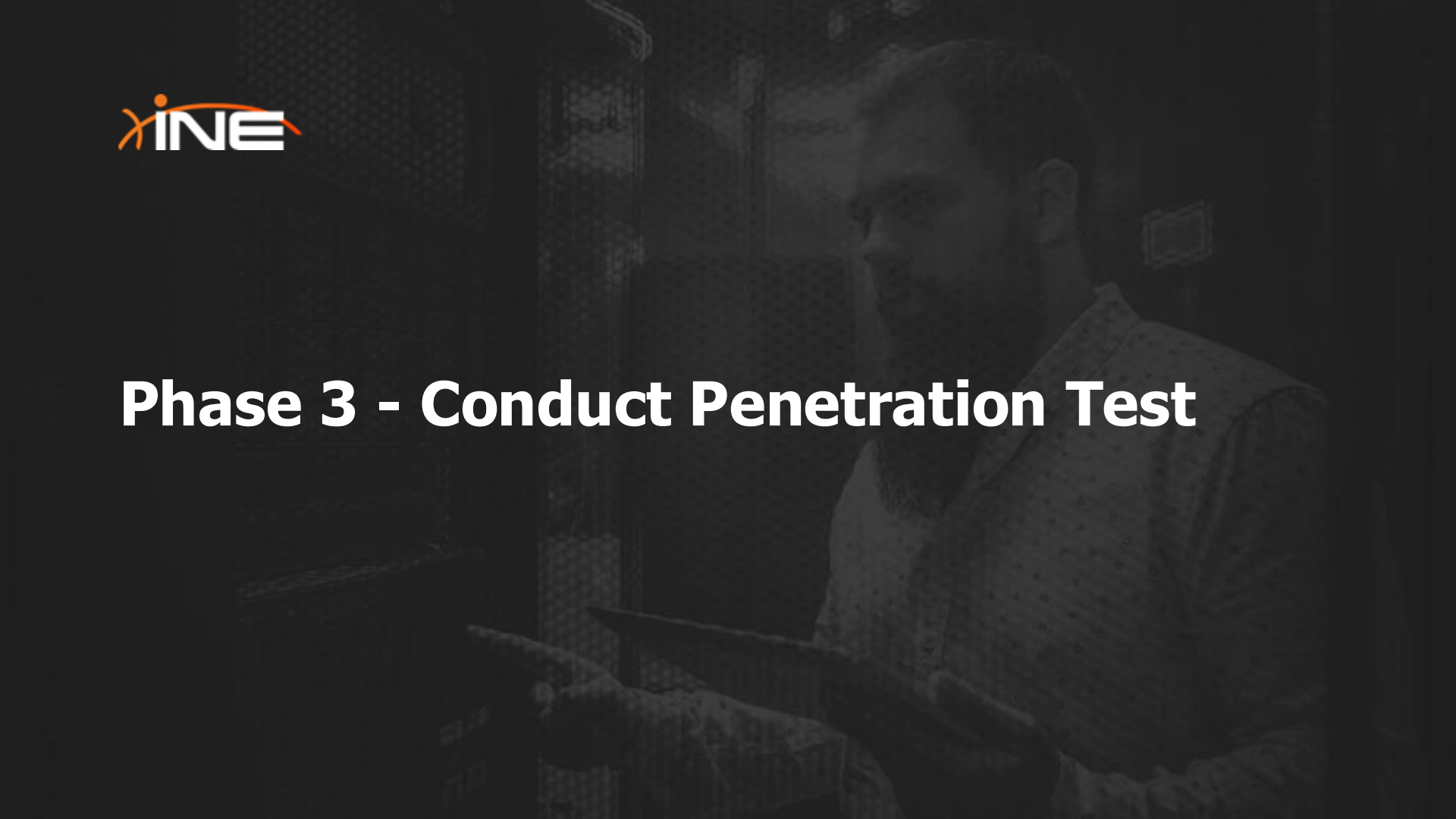
- Install Lynis: Install Lynis on the Linux server.
- Audit the Server: Run a Lynis audit scan on the target Linux server.
- Review the Report: Analyze the Lynis report to identify security issues and recommendations.

Phase 2 - Security Auditing With Lynis

2. Remediation:

- Address Findings: Remediate vulnerabilities identified in the Lynis report (e.g., updating software, enforcing password policies).
- Update Security Policy: Document remediation actions and update the security policy to reflect changes.

Demo: Security Auditing With Lynis



Phase 3 - Conduct Penetration Test

Phase 3 - Conduct Penetration Test

Objective: To validate the effectiveness of remediation actions through a penetration test, ensuring that the Linux server is secure and compliant with the security policy.

1. Execution:

- Network Scan: Use Nmap to identify open ports and services.
- Vulnerability Scanning: Use Metasploit to find and exploit vulnerabilities.
- Web Application Testing: Use Burp Suite to test web applications (if applicable).

Phase 3 - Conduct Penetration Test

2. Validating Remediation:

- Compare Results: Compare initial audit findings with penetration test results to verify that vulnerabilities have been addressed.
- Check for New Vulnerabilities: Identify and remediate any new vulnerabilities introduced during the remediation phase.

Phase 3 - Conduct Penetration Test

3. Reporting:

- Executive Summary: Provide an overview of the penetration test and major findings.
- Methodology: Detail the tools and techniques used during the test.
- Findings: Describe vulnerabilities found, including severity and potential impact.
- Recommendations: Offer steps to further secure the system.

Demo: Conduct Penetration Test

Auditing Fundamentals

Course Conclusion

Learning Objectives/Outcomes:

- Understand the Role of Security Auditing: Grasp the importance and objectives of security auditing within an organization.
- Differentiate Between Audits, Assessments, and Tests: Clearly distinguish between security auditing, vulnerability assessments, and penetration tests.
- Learn the Security Auditing Process: Gain knowledge of the steps involved in conducting a comprehensive security audit.
- Assess Compliance Requirements: Understand how to evaluate and ensure compliance with regulatory standards.
- Apply Security Auditing Techniques: Learn practical techniques for auditing networks, systems, applications, and policies.
- Integrate Audits with Penetration Testing: Understand how security auditing supports and enhances penetration testing efforts.


Thank You!

EXPERTS AT MAKING YOU AN EXPERT