Ethical Hacking

Session 16

Penetration Testing

Learning Objectives

1. Understand the concept of penetration testing
2. Describe the importance of security audit before pen test
3. Explain the process of vulnerability assessment
4. Define testing points and locations
5. List common penetration testing techniques
6. Explain types of pen testing
7. Explain phases of penetration testing
8. Describe the different phases in the penetration testing methodology

Introduction to Penetration Testing 1-7

- Penetration test or pen test is an attack on a computer system to:

Introduction to Penetration Testing 2-7

- **The Penetration Testing:**
  - Is an activity that shows the short falls in the organisation's security model.
  - Is a process that helps ethical hackers to identify the target systems and access them like hackers, but for good purpose.
  - May target a white box or black box and provide information about the vulnerability and the upcoming threats to the ethical hackers.
  - Informs about the available defense tools or strategies and the techniques that are used in the penetration test.

Introduction to Penetration Testing 3-7

- Is a broader concept as it not only shows the vulnerability in the system but also displays if the defenses can be defeated.
- Shows the security issues found in the test to the system owner or manager.
- Perfectly assesses the potential danger and outlines the countermeasures to minimise future risk.

Introduction to Penetration Testing 4-7

- The features of the Penetration test are as follows:

Determines the possible set of attack strategies, tools and techniques.	Assesses the high-risk vulnerabilities that are emerged from the combination of low-risk vulnerabilities.	Determines difficult or impossible vulnerabilities.
Assesses the effect and scale of attack on the potential business and operations.	Checks the capability of network defenders that fight against attacks.	Displays the evidence to support investments in organisational security and technology.

Introduction to Penetration Testing 5-7

- A full security audit includes penetration test for the system.
- Most of the ethical hackers follow common approach to penetrate a system.

- In the penetration testing, ethical hacker:
  - Evaluates the security of the computer system and network by trying all possible attacks that an attacker may use.
  - Use common methodologies to attack a system.
  - Has limited resources such as equipments, time and skilled resources.
  - Should use these resources to reduce attack on the maximum possible area of the target.

Introduction to Penetration Testing 6-7

- The main purpose of pen test is to gather security data of computer system and network and find out the vulnerabilities.

- The pen test is performed with the help of various techniques such as:
  - Network enumeration
  - DNS queries
  - Operating system identification
  - Network queries
  - Ping sweeps
  - Port scanning

Introduction to Penetration Testing 7-7

- To perform penetration testing, the organisation must give a written approval for the testing and clear state the scope of work for testing.

Security Audit 1-2

- **Security Audit:**
  - Is a methodical and organised assessment of a security policy applied by the organisation with the purpose of maintaining security.
  - Is performed by the organisations on all resources as it helps them strengthen the security.
  - Helps organisations to identify the potential risks and the attacks against the network and resources that are important as a valuable data.
  - Helps the security auditors, who understand the organisation's resources and structure, to conduct the security audits.

Security Audit 2-2

- A security audit involves:
  - Assessment of system's software and hardware configuration
  - Verifications of available security measures
  - Evaluation of processes of data handling and resources
  - Testing standard policies and procedures of the organisation
- The security audits are performed to ensure that the organisations use their standard security information resources and policies.

Vulnerability Assessment 1-4

- **Vulnerability Assessment:**
  - Helps the organisation to find the security weaknesses with the help of network scanning.
  - Helps ethical hackers to search IP-enabled devices, enumerate systems, operating systems and applications.
  - Helps hackers to identify common security errors such as weak account password, weak file and folder access permission, default application and so on.

Vulnerability Assessment 2-4

- Vulnerability assessment helps to identify:
  - The system configuration
  - The operating system (OS) installed on the system
  - IP protocols
  - Transmission Control Protocol (TCP)/User Datagram Protocol (UDP)
  - Installed applications and ports

- The software packages installed in the system scan the systems and network devices for vulnerability and exposures index (CVE).
- They help to identify the common attacks such as enumeration of security information and denial-of-service attacks.

Vulnerability Assessment 3-4

- The vulnerability report includes the weak and hidden areas of applications and false positives.

- The network engineer who scans the system and network devices must have knowledge of:
  - Various operation systems
  - Software applications
  - Hardware devices
  - Network devices
  - Scanning applications

Vulnerability Assessment 4-4

- The network administrator or a person who scans the system can use two types of automated vulnerability scanners:

Network-based scanners	Host-based scanners
• The network-based scanners perform scanning activity from outside.	• The host-based scanners need a software agent or client for installation on the host.

Penetration Testing Roadmap

- **Penetration Test:**
  - Performs security audits on a computer system or network by launching attack using the malicious way by the ethical hacker or the expert network administrator.
  - Evaluates the system and informs the administrator about its strengths and weakness.
  - Uses various rules, methods, practices, procedures and so on while performing security audit.
  - Displays a roadmap comprises with practices that are used to analyse the system.

Why Penetration Testing? 1-2

- **A Penetration Testing:**
  - Has an immense importance in evaluating and maintaining the network and system security.
  - Helps organisations to identify the loopholes by resuming attacks on the system.
  - Uses the human-based analysis as well as script-based analysis of the target area.
  - Also provides the risk assessment report, which helps organisations to arrange some preventive measures against the security attacks.

Why Penetration Testing? 2-2

- The following are the reasons for performing penetration testing:
  - Understand threats and risks to data of an organisation.
  - Reduce the extra security cost by identifying the security loopholes and vulnerabilities.
  - Provide complete assessment of organisation's security policy, procedure, design and implementation.
  - Maintain industry regulation certifications such as BS7799 and HIPPA.
  - Setup best practices for handling vulnerabilities.
  - Test and validate the efficiency of security controls and protections.
  - Categorise vulnerabilities.
  - Prepare comprehensive approach to prevent attacks and exploitation.
  - Estimate the efficiency of system and network devices.
  - Perform security changes in the system and the network.

Testing Points 1-2

- Penetration test is a process and it has a start point and an end point.
- When the purpose of penetration testing is finding maximum vulnerability, using a white box testing is a good idea and the maximum information will be shared with the testers.
- It helps in identifying the hidden vulnerabilities that are undetected because of obscurity measures.

Testing Points 2-2

- Organisations may hamper the effective pen test while preparing highly important information such as names and user IDs of system administrators.

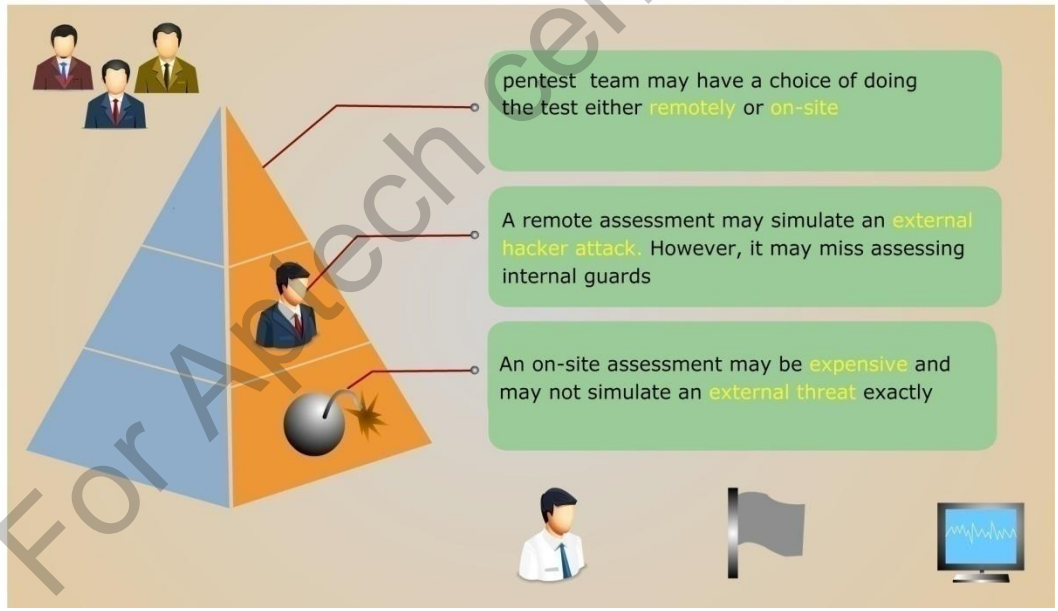
- Therefore, there has to be a balance between the testing activity by the testers and realistic information.

Testing Locations 1-4

- The pen testing team sometimes may have:
  - Preference of location for the pen test.
  - A choice of doing the test remotely or on-site.
- They can decide the place in the network from where they can start pen testing.
- Sometimes, organisations want to perform the pen testing from a remote location.

Testing Locations 2-4

- If the team is based on another continent and if they have to perform online pen testing, then the assessment would be little more expensive than the remote assessment.
- Following figure shows testing locations:



Testing Locations 3-4

- The testing location influences the pen test results.
- If the team performs pen testing over the Internet, it provides a more realistic test environment.
- However, if the testing team gets in-house atmosphere with well-configured perimeter firewall and robust application, the pen test team may not learn effectively.
- When the testing team performs the external assessment, then in that case the team may not assess the additional inner network defenses.

Testing Locations 4-4

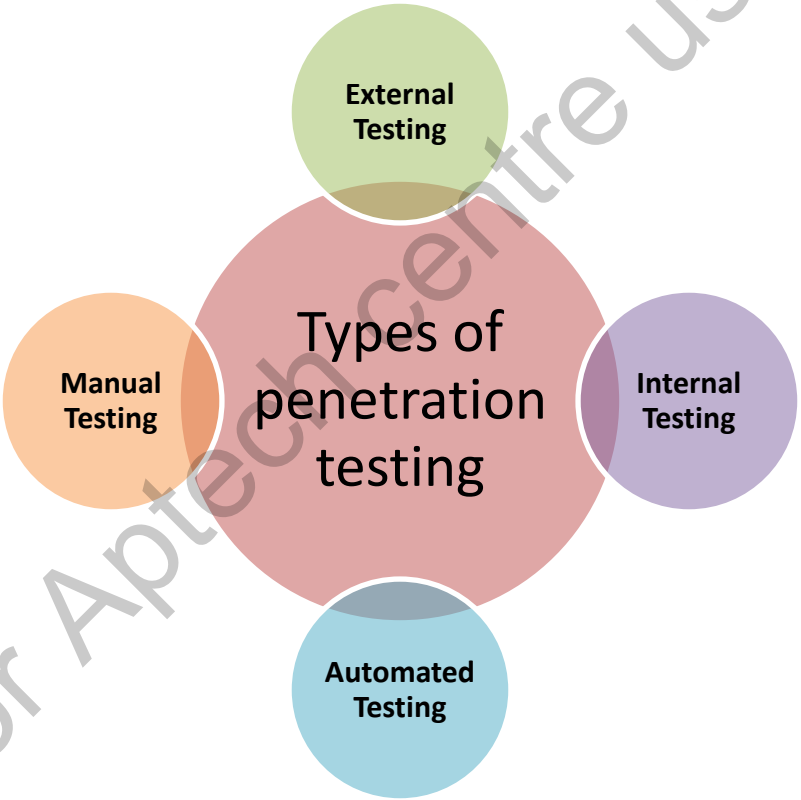
- Sometimes, organisation may have a global network (across continents) and contain multiple systems.
- In this case, the location for the testing is selected depending on the network and system security status of the organisation.

Types of Penetration Testing 1-8

- There are various types of penetration testing depending upon the situation, location, time and so on.
- The pen testing team determines the preferable pen testing type according to the need of security status and performs the pen testing.
- The ultimate purpose of all these pen testing types is same as they search for vulnerability in the system and the network; only their ways are different.

Types of Penetration Testing 2-8

- Following are the types of penetration testing:



Types of Penetration Testing 3-8

- **External Testing:**
  - Is a conventional approach of pen testing that focuses on servers, network infrastructure, applications and so on.
  - May perform without the prior knowledge of black box or with the full disclosure of the topology and white box.
  - Collaborates public information of the target and analyse it to perform testing.

Types of Penetration Testing 4-8

- **Internal Testing:**
  - Uses same methods as the external testing but has a more versatile view regarding security.
  - Is performed using various logical and physical network access points.
  - Following tests are included under internal testing:
    - Black-hat testing
    - White-hat testing
    - Gray-hat testing
    - Announced testing
    - Unannounced testing

Types of Penetration Testing 5-8

- **Automated Testing:**
  - Is preferred by some organisations along with security assessment of their systems and network devices.
  - Helps network administrator to perform the security test and scan using the security tools and applications, to assess vulnerabilities and threats.
  - Performs only external penetration testing by utilising the black box approach and is unable to show complete and secure solution from the testing.
  - Minimises the traffic needed during the testing.

Types of Penetration Testing 6-8

- A complete security assessment includes various elements such as:
  - Organisation's security policy
  - Firewall rule-base analysis
  - Architectural review
  - Application testing
  - Benchmarking

- Being an automated process, the security policy and the architectural elements in the testing are not used completely and may need support from a security expert.

Types of Penetration Testing 7-8

- **Manual Testing:**
  - Is preferred by many organisations for their security purposes instead of using the seasonal as well as automated testing.
  - Helps the security professionals to view the problem from the attacker's perspective and search solutions accordingly.
  - Helps them to use various methods to dig the loopholes in the security model.

Types of Penetration Testing 8-8

The phases in the manual pen testing are as follows:

1. Gathering basic information
2. Social engineering
3. Scanning the information and data
4. Vulnerability assessment
5. Exploiting vulnerabilities

In the manual testing, the testing team requires:

- Testing plan
- Testing design
- Testing schedule
- Attentive documentation

– All these elements play important role in manual testing, but the documentation:
  - Provides support to capture the results of the entire testing process
  - Also shows the results of the testing team in assessing the security postures of the organisation.

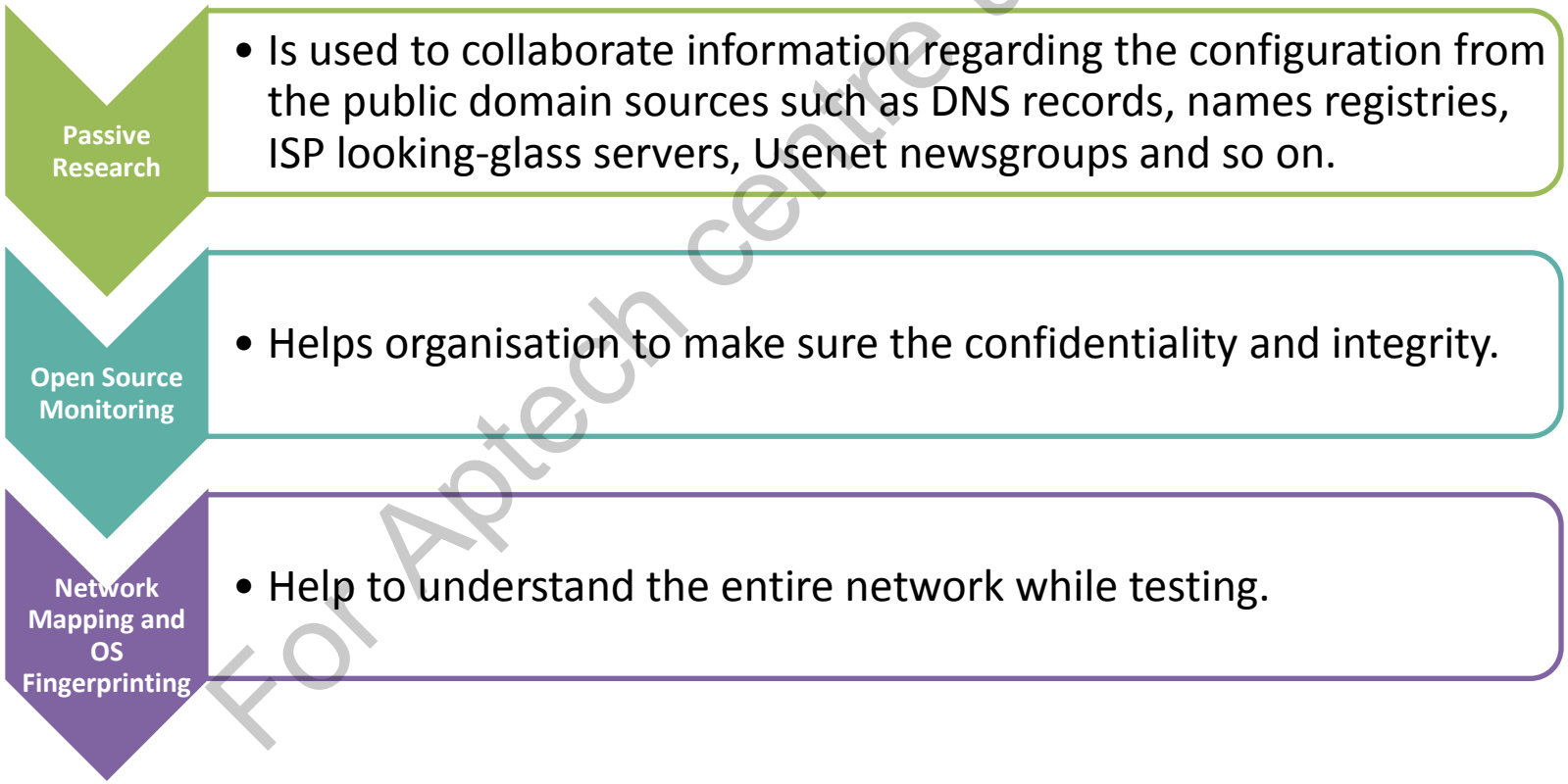
Types of Pen Test Tools

- Following are some of the commonly used penetration testing tools:

– Nmap	– Snort
– Cain & Abel	– Burpsuite
– Metasploit	– Lopthcrack
– W3af	– Acutenix
– Nessus	– Wireshark
– Httprint	– Aircrack
– Netcraft	– Backtrack

Common Penetration Testing Techniques 1-3

- Following are some of the common penetration testing techniques:



Common Penetration Testing Techniques 2-3

Spoofing

- Is an activity by someone to pretense as someone else.
- Is used for both internal and external penetration test.

Network Sniffing

- Takes place when the hacker forges the destination IP address in the IP header.
- Is used to capture data when it goes through the network.

Trojan Attack

- Is an activity of installing Trojan on the user's system through Internet, email, CD-ROM and so on to perform malicious attacks.

Common Penetration Testing Techniques 3-3

Brute Force Attacks

- Is used to guess session IDs and attempt multiple patterns until the session ID is identified.

Vulnerability Scanning

- Is a technique used to identify the weaknesses in a security system to repair and improve the system security.

Scenario Analysis

- Is a final phase of pen testing that performs the risk assessment of vulnerabilities accurately.

Phases of Penetration Testing 1-6

- Following are the types of penetration testing:

Phases of Penetration Testing 2-6

Pre-attack Phase

- **In the Pre-attack Phase:**
  - The testing team gathers information about the target system and network area of the organisation.
  - The testing team performs following activities:
    - Define rules of engagement
    - Identify customer requirements
    - Prepare a checklist of the testing requirements
    - Describe pen testing scope
    - Sign penetration testing contract
    - Sign confidentiality and Non-disclosure Agreement (NDA)
    - Gather information of the target system and network area

Phases of Penetration Testing 3-6

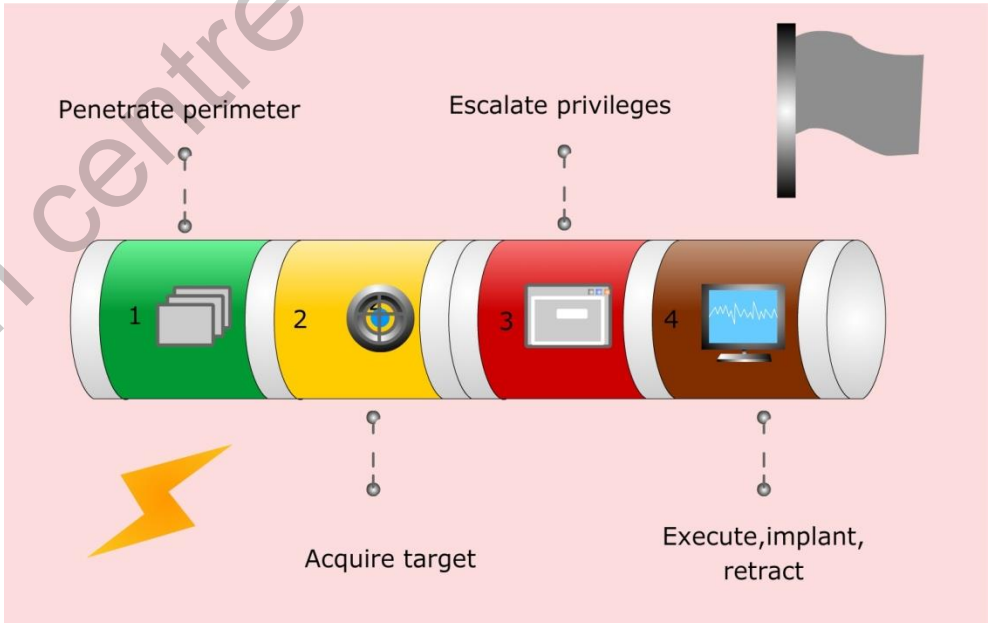
Attack Phase

- **In the Attack Phase:**
  - The testing team prepares the strategy to perform attack with the help of gathered information.
  - The team may perform scanning before preparing the strategy.
  - The team or attacker identifies the vulnerability in the system and the network and use weak security loopholes to enter in the system.
  - Once the attacker enters in the system, the backdoor is installed to maintain access to the system and exploits to achieve the purpose.

Phases of Penetration Testing 4-6

Attack Phase

- As shown in the figure, in the attack phase, the attacker needs to:
  - Penetrate perimeter
  - Execute and implant
  - Acquire target
  - Escalate privileges



Phases of Penetration Testing 5-6

Post-attack Phase

- **In the Post-attack Phase:**
  - The testing team has to restore the network to its original state.
  - The testers clean up the testing processes and remove vulnerabilities that are identified.
  - The tester identifies where the security fails in the system and where the tester should fix the security system or network.

Phases of Penetration Testing 6-6

Post-attack Phase

- The testing team performs the following activities in the post-attack phase:
  - Remove all the files from the system
  - Clear all registry entries
  - Remove all created vulnerabilities
  - Restore all the files
  - Restore the user settings and changes
  - Restore all the tools
  - Restore the network to the pre-test stage
  - Map the network state
  - Document and capture all the registered logs while performing the test
  - Analyse results and present to the organisation

Penetration Testing Methodology 1-4

- Following are the types of penetration testing:

Information Gathering	• This is very important phase in penetration testing. • The testing team gathers information using various tools, online sources, http requests, crafted requests, scanners and so on.
Vulnerability Analysis	• In this phase, the team identifies and then analyse vulnerabilities on the network and the system. • It gives an idea of overall structure of the flaws that exist in the system.
External Penetration Testing	• External penetration testing helps to identify whether the network is secure or not. • The testing team performs the penetration testing like attackers but do not harm the network. • It helps the team to identify the loopholes in the network and make it more secure.

Penetration Testing Methodology 2-4

Internal Network Penetration Testing

- In internal network penetration testing, the team identifies internal network flaws and pretends like a real attack.
- The methods used for internal network penetration testing are port scanning, internal network scanning, system fingerprinting, firewall and ACL testing and so on.

Router and Switches Penetration Testing

- By doing router and switches penetration testing, the testing team can determine the thorough router security, data transfer and Internet speed, bandwidth, router performance and security assessment of router.

Firewall Penetration Testing

- Firewall penetration testing analyses security efficiency and identifies the security status of the firewall network against attacks performed by network intruders.

Penetration Testing Methodology 3-4

Intrusion Detection System (IDS) Penetration Testing	• IDS could be software or hardware. IDS penetration testing tests the strength of the IDS. • This testing can be performed using the IDS informer, an evasion gateway and so on.
Wireless Network Penetration Testing	• Wireless network is less protected than the wired network. • Therefore, it has to be tested and enhancement should be implemented to make it more secure.
Denial-of Service Penetration Testing	• The main aim of DoS attack is to slow down the Website or crash it by sending multiple requests so that it cannot handle them. • By using the DoS attack, the testing team can check the intensity of attack on the Web server or Website.

Penetration Testing Methodology 4-4

- Following are some more phases in the penetration testing methodology:

  - Application Penetration Testing
  - SQL Injection Penetration Testing
  - Source Code Penetration Testing
  - Social Engineering Penetration Testing
  - Stolen Laptops, PDA and Cell Phones Penetration Testing
  - Mobile Device Penetration Testing
  - VoIP Penetration Testing
  - Physical Security Penetration Testing
  - Data Leakage Penetration Testing
  - Log Management Penetration Testing
  - Security Patches Penetration Testing
  - Database Penetration Testing
  - Password Cracking Penetration Testing
  - Surveillance Camera Penetration Testing
  - VPN Penetration Testing
  - Virus and Trojan Detection
  - Cloud Penetration Testing
  - Virtual Machine Penetration Testing
  - War Dialing
  - File Integrity Checking
  - SAP Penetration Testing
  - Telecom and Broadband Penetration Testing
  - Email Security Penetration Testing

Summary 1-3

- Penetration testing also known as pen test, is an attack on a computer system to find the security gaps and weaknesses, checking for getting access of it and understanding the data and functionality.
- A vulnerability assessment and the penetration testing look similar, but penetration testing is a broader concept as it not only shows the vulnerability in the system but also displays if the defenses can be defeated.
- The main purpose of pen test is to gather security data of computer system and network and find out the vulnerabilities.
- A security audit is a methodical and organised assessment of a security policy applied by the organisation with the purpose of maintaining security.

Summary 2-3

- The security audits are generally performed to ensure that the organisations have used their standard security information resources and policies.
- Vulnerability assessment helps the organisation to find the security weaknesses with the help of network scanning.
- A penetration testing helps organisations to identify the loopholes by resuming attacks on the system. It uses the human-based analysis as well as script-based analysis of the target area.
- The testing location has an influence on the pen test result.
- There are various types of penetration testing depending upon the situation, location, time and so on.

Summary 3-3

- The types of penetration testing are external testing, internal testing, automated testing and manual testing.
- Some of the common penetration testing techniques are Passive research, Open Source monitoring, Network mapping and OS fingerprinting, Spoofing, Network sniffing, Trojan attacks, Brute force attacks, Vulnerability scanning, Scenario analysis and so on.
- The phases of penetration testing are Pre-attack phase, Attack phase and Post-attack phase.
- Some of the phases in the penetration testing methodology are Information Gathering, Vulnerability Analysis, External Penetration Testing, Internal Network Penetration Testing, Router and Switches Penetration Testing, Firewall Penetration Testing, IDS Penetration Testing, Wireless Network Penetration Testing, DOS Penetration Testing and so on.