Penetration Testing

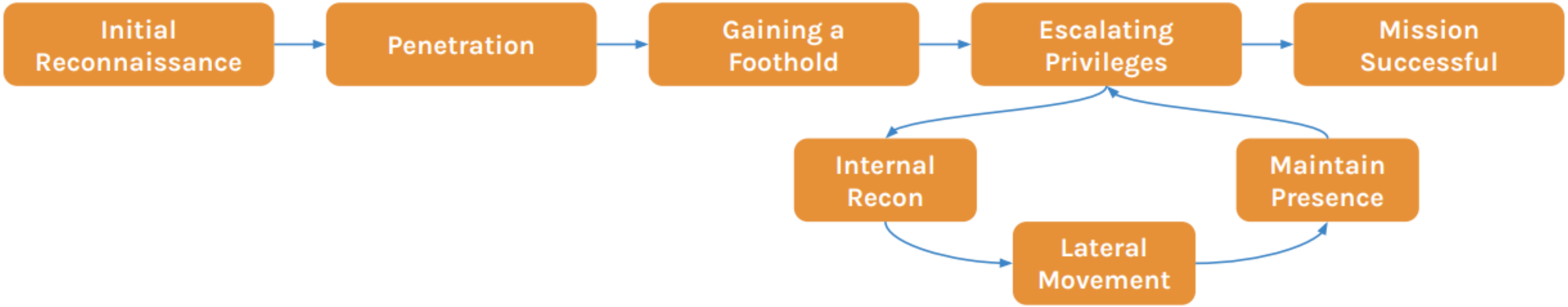
Module 1

Introduction

SIMPLIFIED ATTACK LIFECYCLE

- **Initial Reconnaissance**: It has two main steps, Selection of target and Research of Target
- **Penetration:** The intruder uses certain methods to compromise the target.
- **Gaining Foothold**: Maintain foothold of the compromised system. It is generally achieved by setting up a backdoor so that the machine can be accessed later.
- **Escalate Privileges**: Intruder will obtain a higher-level access to the compromised machine by multiple methods with the aim of obtain the administrator login.
- **Lateral Movement**: The intruder generally does not find the desired information on the first machine he has compromised. The attacker now tries to expand the exploitation process to other systems within the same network. If the intruder is caught during lateral movement, we get the exact intent of the intruder or exactly what information he might be after.
- **Maintain Presence**: The intruder will ensure remote access to the complete environment by installing multiple variants of malware backdoors.
- **Mission Complete**

SIMPLIFIED ATTACK LIFECYCLE



Initial Reconnaissance

Penetration

Gaining a Foothold

Escalating Privileges

Mission Successful

Internal Recon

Lateral Movement

Maintain Presence

WHAT IS VAPT?

- A form of stress testing, which exposes weakness or flaws in a computer system.
- The art of finding an Open Door.
- VAPT can be used to find flaws in
  - Specifications, Architecture, Implementation, Software, Hardware, and many more..
- **Vulnerability assessment** is the process of identifying, quantifying, and prioritizing the vulnerabilities in a system.
- **Penetration test** is an attack on a computer system that looks for security weaknesses, potentially gaining access to the computer's features and data.

Need for VAPT

- Improve information security and awareness
- Assess risk
- Mitigate risk immediately
- Reinforce the information security process
- Assist in decision making process
- Validate that current security mechanisms are working
- Compliance to various security standards and regulations such as NIST, ISO 27001, Information Technology Act 2000, SOX, HIPAA, PCI etc.

Penetration Testing

- A penetration test (pen test) is an authorized simulated attack performed on a computer system to evaluate its security.
- Penetration testers use the same tools, techniques, and processes as attackers to find and demonstrate the business impacts of weaknesses in a system.

Penetration Testing Process

1.Planning & Preparation

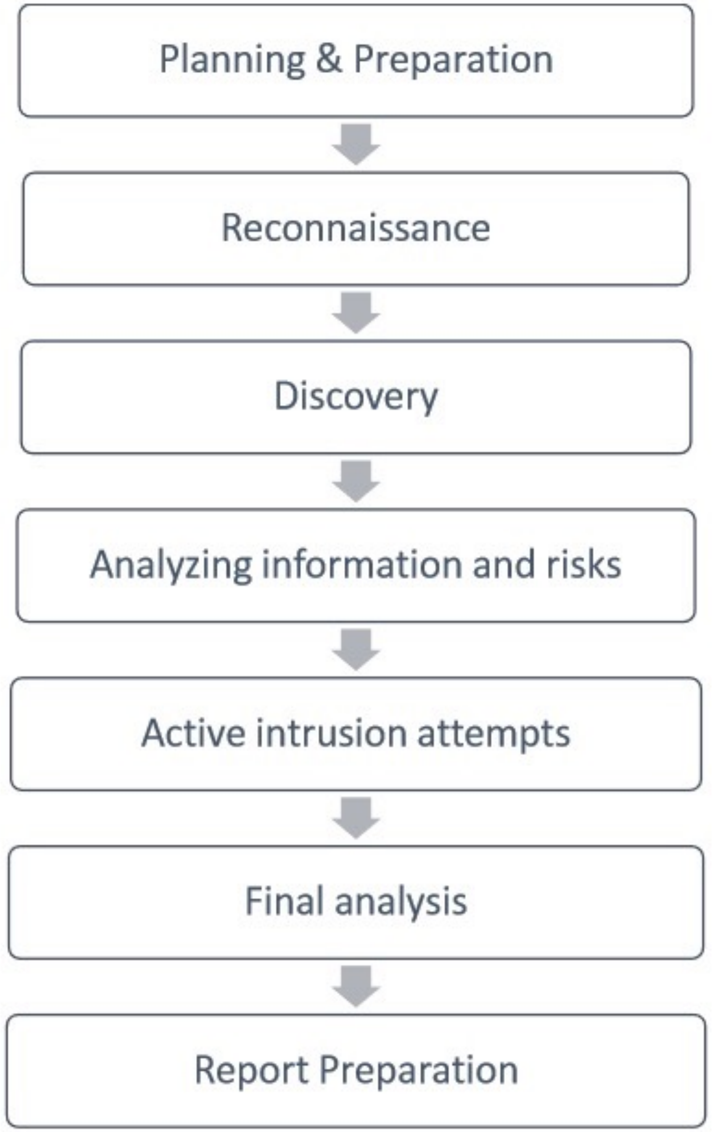
- Planning and preparation starts with defining the goals and objectives of the penetration testing.
- The client and the tester jointly define the goals so that both the parties have the same objectives and understanding.

2. Reconnaissance

- Reconnaissance includes an analysis of the preliminary information.
- The sole objective is to obtain a complete and detailed information of the systems.

3. Discovery

- A penetration tester will most likely use the automated tools to scan target assets for discovering vulnerabilities.
- A tester discovers,
  - **Network Discovery** – Such as discovery of additional systems, servers, and other devices.
  - **Host Discovery** – It determines open ports on these devices.
  - **Service Interrogation** – It interrogates ports to discover actual services which are running on them.



Planning & Preparation

Reconnaissance

Discovery

Analyzing information and risks

Active intrusion attempts

Final analysis

Report Preparation

Penetration Testing Process

4. Analyzing Information and Risks

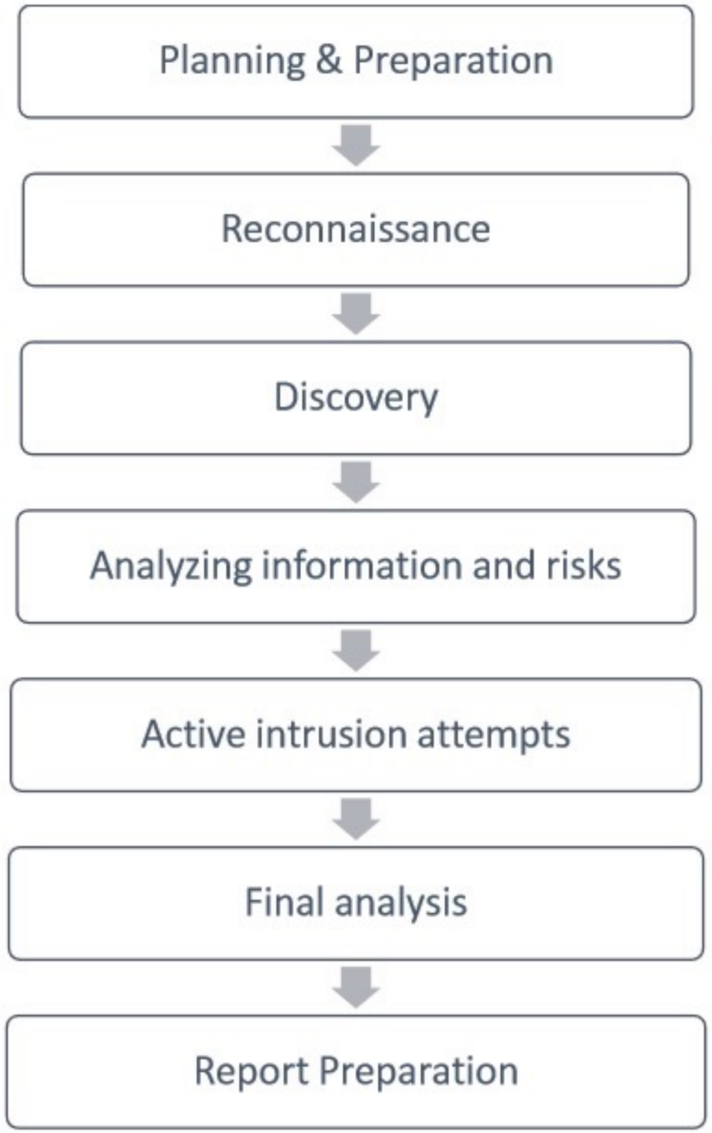
- Tester analyzes and assesses the information gathered before the test steps for dynamically penetrating the system.

5. Active Intrusion Attempts

- This is the most important step that has to be performed with due care.
- This step entails the extent to which the potential vulnerabilities that was identified in the discovery step which possess the actual risks.

6. Final Analysis

- This step primarily considers all the steps conducted (discussed above) till that time and an evaluation of the vulnerabilities present in the form of potential risks.
- the tester recommends to eliminate the vulnerabilities and risks.



Planning & Preparation

Reconnaissance

Discovery

Analyzing information and risks

Active intrusion attempts

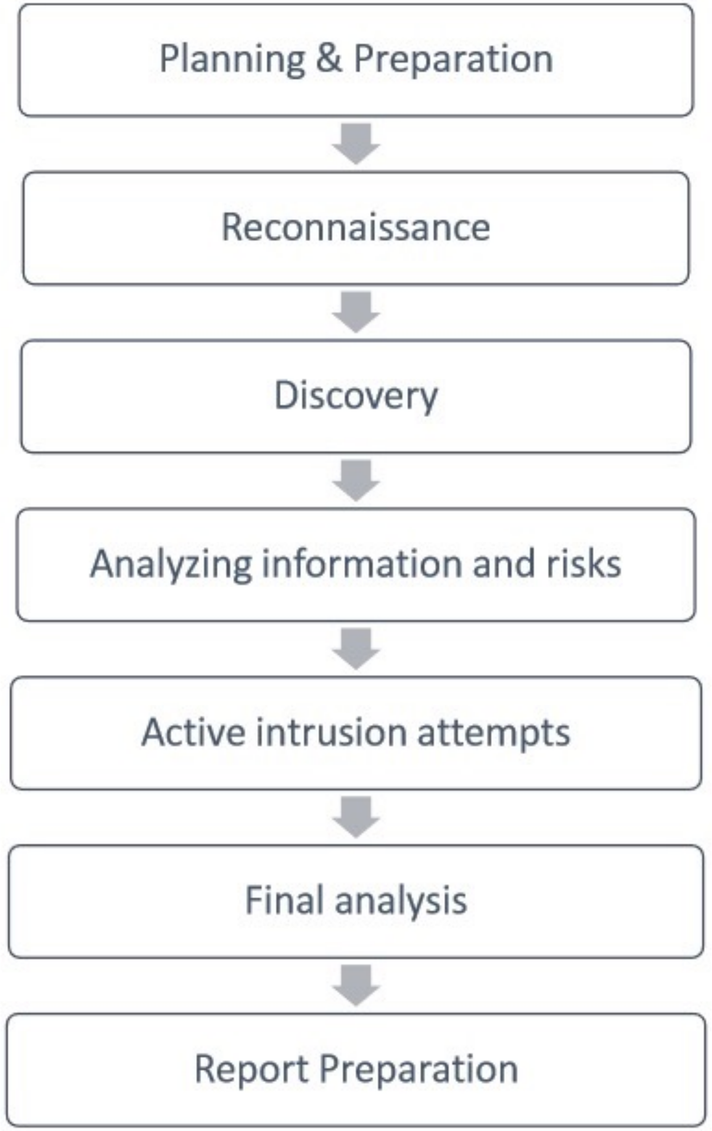
Final analysis

Report Preparation

Penetration Testing Process

7. Report Preparation

- Report must include overall testing procedures, followed by an analysis of vulnerabilities and risks.
- The high risks and critical vulnerabilities must have priorities and then followed by the lower order.
- While documenting the final report, the following points needs to be considered –
  - Overall summary of penetration testing.
  - Details of each step and the information gathered during the pen testing.
  - Details of all the vulnerabilities and risks discovered.
  - Details of cleaning and fixing the systems.
  - Suggestions for future security.



Planning & Preparation

Reconnaissance

Discovery

Analyzing information and risks

Active intrusion attempts

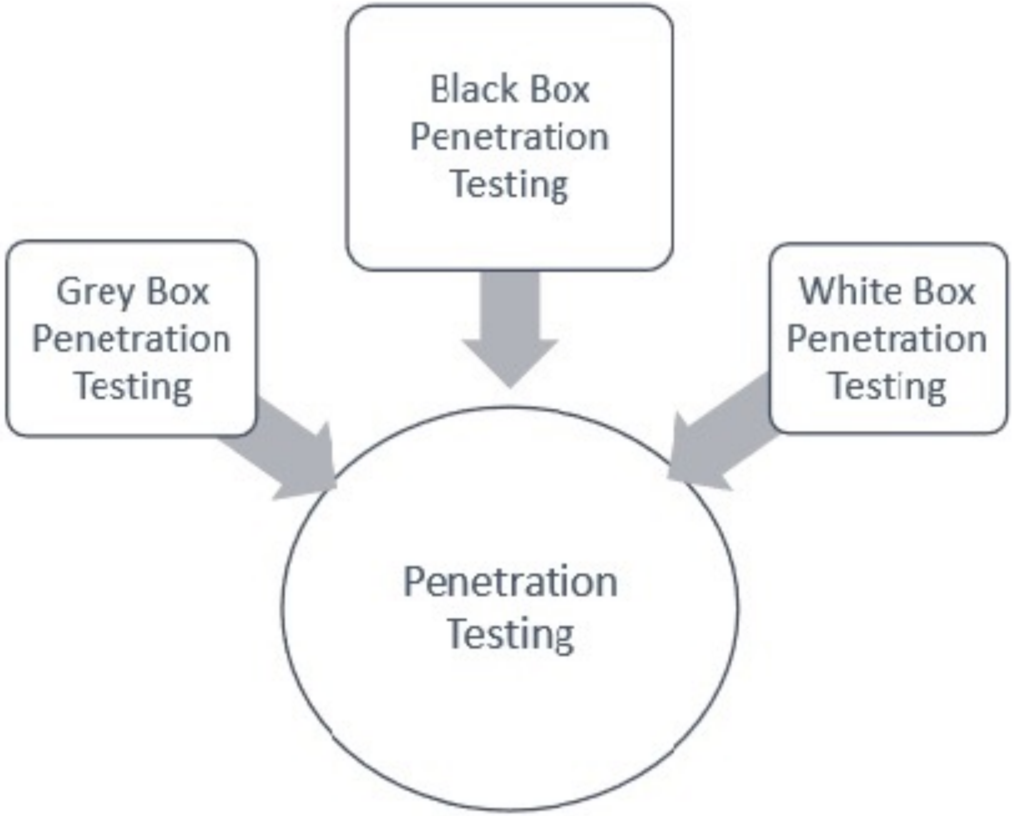
Final analysis

Report Preparation

Types of Penetration Testing Methodologies

Following are the important types of pen testing –

- Black Box Penetration Testing
- White Box Penetration Testing
- Grey Box Penetration Testing


Black Box Penetration Testing
Grey Box Penetration Testing
White Box Penetration Testing
Penetration Testing

Areas of Penetration Testing

- Network Penetration Testing
- Application Penetration Testing
- Social Engineering Penetration test
- Mobile Application penetration test
- API
- Cloud
- Embedded Devices(IoT)
- CI/CD Pipeline

Penetration Testing Tools

1. **Nmap:** It is a network exploration tool and security scanner. It can be used to identify hosts and services on a network, as well as security issues.
2. **Nessus:** It is a vulnerability scanner. It can be used to find vulnerabilities in systems and applications.
3. **Wireshark:** It is a packet analyzer. It can be used to capture and analyze network traffic.
4. **Burp Suite:** It is a web application security testing tool. It can be used to find security issues in web applications.

Cyber and Hacking laws in India

Cyber Crime And Can Hacking Be Ethical In India (khuranaandkhurana.com)

Penetration Standards and Certifications

Pen Testing Standards

- PCI DSS (Payment Card Industry Data Security Standard)
- OWASP (Open Web Application Security Project)
- ISO/IEC 27002, OSSTMM (The Open Source Security Testing Methodology Manual)

Certifications

- GPEN
- Associate Security Tester (AST)
- Senior Security Tester (SST)
- Certified Penetration Tester (CPT)
- CISSP
- CEH
- CompTIA Pentest+

- Penetration Testing Sample Test Cases (Test Scenarios)