# Network Penetration Testing

## Index

### Introduction to Penetration Testing

Penetration testing, often referred to as pen testing, is a simulated cyber attack against a computer system, network, or web application to identify security vulnerabilities that an attacker could exploit. The goal is to identify weaknesses before they can be exploited maliciously.

### Types of Penetration Testing

1. **Black Box Testing**: The tester has no prior knowledge of the infrastructure and simulates an external hacking attempt.
2. **White Box Testing**: The tester has full knowledge of the system, including source code and architecture.
3. **Grey Box Testing**: The tester has partial knowledge of the system, representing an insider threat or an attacker with some knowledge of the network.

### Pen Testing Services

Penetration testing services can be categorized into various types, including network services testing, web application testing, wireless network testing, social engineering testing, and physical security testing.

### Penetration Testing Phases

1. **Planning and Preparation**: Define the scope and goals of the test, including the systems to be addressed and the testing methods to be used.
2. **Discovery**: Gather information about the target through various techniques like scanning and reconnaissance.
3. **Exploitation**: Attempt to exploit identified vulnerabilities to understand the potential impact.
4. **Post-Exploitation**: Assess the potential damage and identify ways to maintain a foothold in the system.
5. **Reporting**: Document the findings, providing detailed information about vulnerabilities and recommended remediation steps.

### Pre-Engagement Actions

Before starting a penetration test, several pre-engagement activities must be conducted:

- Define the rules of engagement (ROE).
- Establish communication protocols.
- Obtain legal authorization.
- Understand the client's requirements and expectations.

### OSINT (Open Source Intelligence)

OSINT involves gathering information from publicly available sources to support the penetration testing process. This includes data from social media, public records, websites, and more. OSINT helps in understanding the target better and identifying potential attack vectors.

### Exploitation (Automated)

Automated exploitation involves using tools and scripts to exploit known vulnerabilities. Tools like Metasploit can automate the process of identifying and exploiting vulnerabilities, providing a more efficient way to test systems.

### Password Cracking

Password cracking involves techniques used to recover passwords from data stored or transmitted by computer systems. Methods include:

- **Brute Force Attack**: Trying all possible combinations.
- **Dictionary Attack**: Using a predefined list of words.
- **Rainbow Table Attack**: Using precomputed tables of hash values.

**Practical Assignment – III**

**Scenario Example: Company ABC's Network Penetration Test**

**Objective**: To identify and exploit vulnerabilities in Company ABC's network to improve its security posture.

**Scope**:

- External network testing
- Internal network testing (after initial compromise)
- Web application testing

**Steps**:

1. **Planning and Preparation**:
   - Define the scope: Include all external IP addresses, the internal network, and specific web applications.
   - Obtain authorization from Company ABC's management.
2. **Discovery**:
   - Perform OSINT to gather information about Company ABC.
   - Use network scanning tools (e.g., Nmap) to identify open ports and services.
3. **Exploitation**:
   - Use automated tools (e.g., Metasploit) to exploit identified vulnerabilities.
   - Conduct manual testing for web application vulnerabilities (e.g., SQL injection, XSS).
4. **Post-Exploitation**:
   - Assess the extent of the compromise.
   - Attempt to escalate privileges and move laterally within the network.
5. **Reporting**:
   - Document all findings, including vulnerabilities exploited and data accessed.
   - Provide remediation recommendations to Company ABC's IT team.

**Results**:

- Identified multiple vulnerabilities in the external network, including outdated software and weak passwords.

- Exploited a SQL injection vulnerability in a web application, gaining access to the database.
- Provided detailed recommendations to Company ABC for improving their security posture.

**Outcome**: Company ABC implemented the recommended changes, significantly improving their network security and reducing the risk of future attacks.