Network Penetration Testing with Real-World Exploits and Security Remediation

Project Objectives

The objective of this project is to gain practical knowledge of penetration testing by identifying, exploiting, and securing network vulnerabilities. The focus is on real-world exploits, understanding system weaknesses, and learning how to fix them using professional tools and techniques.

Introduction

In the current digital era, protecting systems from cyber threats is a top priority. This project uses ethical hacking methods to simulate real attacks on a vulnerable system using Kali Linux and Metasploitable. The goal is to understand how hackers work, which vulnerabilities they target, and how those vulnerabilities can be patched to improve overall system security.

Theory Behind the Project

Penetration testing is a method of evaluating the security of a system by simulating an attack. It helps identify weak areas that can be exploited. Using tools like Nmap for scanning, Metasploit for exploitation, and John the Ripper for password cracking, we simulate how an attacker would gain unauthorized access and how we can prevent it.

Project Requirements

Operating Systems Used:

- Kali Linux – Attacker Machine

- Metasploitable 2 – Target Machine

Tools Used

- Nmap – Network scanning and service detection
- Metasploit Framework – Exploitation framework
- John the Ripper – Password hash cracking
- Netcat – Reverse shell and port communication
- Linux Command Line Tools – User and permission management

Task Breakdown

Task 1 – Basic Network Scan

Command Used:
`nmap -v YOUR_IP_RANGE`

Expected Result:
- Discovery of devices on the network
- IP addresses and open ports of those devices

Task 2 – Reconnaissance

Hidden Port Scanning:
Command:
`nmap -v -p- YOUR_TARGET_IP_ADDRESS`
Expected Result:
- Complete list of open ports including non-standard (hidden) ones

Total Hidden Ports Found: 7
List:
1. 8787/tcp
2. 47436/tcp
3. 50918/tcp
4. 59995/tcp
5. 60004/tcp
6. 3632/tcp
7. 5432/tcp

Service Version Detection:
Command:
`nmap -v -sV YOUR_TARGET_IP_ADDRESS`
Expected Result:
- Services running on open ports with version details

Operating System Detection:
Command:
`nmap -v -O YOUR_TARGET_IP_ADDRESS`
Expected Result:
- Operating system identification and device type information

Task 3 – Enumeration

Target IP Address: ENTER_YOUR_TARGET_IP_ADDRESS
Operating System: Linux Kernel 2.6.X
MAC Address: 00:0C:29:5D:FE:0B (VMware)
Device Type: General Purpose

CPE: cpe:/o:linux:linux_kernel:2.6
OS Details: Linux 2.6.9 – 2.6.33

Open Services (Excluding Hidden Ports):

21/tcp - open - ftp - vsftpd 2.3.4
22/tcp - open - ssh - OpenSSH 4.7p1 Debian 8ubuntu1

Hidden Ports with Service Versions:
8787/tcp - open - drb - Ruby DRb RMI (Ruby 1.8)
47436/tcp - open - mountd - 1-3 (RPC #100005)
50918/tcp - open - java-rmi - GNU Classpath grmiregistry
59995/tcp - open - nlockmgr - 1-4 (RPC #100021)
60004/tcp - open - status - 1 (RPC #100024)

Task 4 – Exploiting Services

Exploitation Performed On:
1. vsftpd 2.3.4 – Exploited using known backdoor vulnerability
2. OpenSSH – Attempted brute-force attack
3. Java RMI – Remote code execution using Metasploit module

Task 5 – Creating a User with Root Privileges

Command Used:
`adduser shubham`
Password Used: hello123

Entry in /etc/passwd:
narottam:x:1002:1002:Shubham,,,:/home/shubham:/bin/bash

Entry in /etc/shadow:
narottam:$1$8nWuasXV$pk6ZABfqT9NoHv1pPX8Rj.

Task 6 – Cracking Password Hash

1. Stored the password hash in a file named hash.txt
2. Cracked the password using:
`john hash.txt`
3. Displayed the result using:
`john hash.txt --show`

Task 7 – Remediation

vsftpd 2.3.4:
- Issue: Known backdoor vulnerability
- Current Version: 2.3.4
- Recommended Version: 3.0.3 or newer
- Fix: Update vsftpd using:

`sudo apt update && sudo apt install vsftpd`

OpenSSH 4.7p1:
- Issue: Old version with security flaws
- Current Version: 4.7p1
- Recommended Version: OpenSSH 9.x
- Fix: Upgrade via:
`sudo apt install openssh-server`

General Security Measures:
- Keep all services updated regularly
- Close all unused ports
- Use firewalls to restrict external access
- Enable fail2ban to prevent brute-force attacks
- Set strong password policies

References:
- https://nvd.nist.gov
- https://security-tracker.debian.org

Major Learnings from This Project

This project gave me a deep understanding of how attackers can find and exploit weaknesses in a network. I learned how to identify open ports, detect services, and gather system information. The practical exploitation part showed me how vulnerabilities like outdated FTP or RMI services can be a serious threat. Cracking password hashes taught me why strong passwords are so important. Most importantly, I realized how essential it is to keep software updated and configure systems securely to avoid breaches.