Ethical Hacking Project

Scanning and Enumerating a Local Network with Nmap

Project: Simulating Real-World Network Exploitation and Defense

---

Project Objectives

To understand and apply techniques in:

- Network scanning
- Service enumeration
- Vulnerability exploitation
- Privilege escalation
- Password cracking
- Security remediation

Tools Used

- Kali Linux (Attacker Machine)
- Metasploitable (Target Machine)
- Nmap
- John the Ripper
- Metasploit Framework

Task 1: Basic Network Scan

Command: `bash nmap -v 192.168.1.0/24`

Expected Output: ``` Nmap scan report for 192.168.1.10 Host is up (0.0010s latency). PORT STATE SERVICE 22/tcp open ssh 80/tcp open http

Nmap scan report for 192.168.1.15 Host is up (0.0020s latency). PORT STATE SERVICE 21/tcp open ftp ```

Task 2: Reconnaissance

2.1 Scanning for Hidden Ports

Command: `bash nmap -v -p- 192.168.1.10`

Expected Output: `PORT STATE SERVICE 21/tcp open ftp 22/tcp open ssh 8787/tcp open drb 47436/tcp open mountd 50918/tcp open java-rmi 59995/tcp open nlockmgr 60004/tcp open status`

Total Hidden Ports: 7

2.2 Service Version Detection

Command: `bash nmap -v -sV 192.168.1.10`

Expected Output: `PORT STATE SERVICE VERSION 21/tcp open ftp vsftpd 2.3.4 22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 8787/tcp open drb Ruby DRb RMI 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)`

2.3 Operating System Detection

Command: `bash nmap -v -O 192.168.1.10`

Expected Output: `Running: Linux 2.6.X OS CPE: cpe:/o:linux:linux_kernel:2.6 OS details: Linux 2.6.9 - 2.6.33`

Task 3: Enumeration Summary

| Parameter | Details | |---|---| | Target IP Address | 192.168.1.10 | | Operating System | Linux 2.6.9 - 2.6.33 | | MAC Address | 00:0C:29:5D:FE:0B (VMware) | | Device Type | General-purpose |

Open Services (Excluding Hidden Ports)
`21/tcp open ftp vsftpd 2.3.4 22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1`

Hidden Services
`8787/tcp open drb Ruby DRb RMI 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: Exploitation of Services

- `vsftpd 2.3.4` – Exploited via known backdoor vulnerability
- `OpenSSH 4.7p1` – Brute-force attack executed successfully
- `Java RMI` – Remote code execution achieved via Metasploit module

---

Task 5: Creating a Privileged User

Command: `bash adduser shashwat Password: hello`

/etc/passwd Entry: `shashwat:x:1001:1001:Shashwat,,,:/home/shashwat:/bin/bash`

/etc/shadow Hash: `shashwat:$1$8nWuasXV$pk6ZABfqT9NoHv1pPX8Rj.`

Task 6: Cracking Password Hash

Stored Hash in `hashes.txt`: `shashwat:$1$8nWuasXV$pk6ZABfqT9NoHv1pPX8Rj.`

Cracking Commands: `bash john hashes.txt john hashes.txt --show`

Cracked Password: `hello`

Task 7: Remediation and Recommendations

Identified Vulnerabilities & Fixes:

1. **vsftpd 2.3.4** – Vulnerable backdoor
   Fix: Upgrade to vsftpd 3.0.5

2. **OpenSSH 4.7p1** – Outdated, brute-forceable
   Fix: Upgrade to OpenSSH 9.6

3. **Java RMI Service** – Allows remote execution
   Fix: Disable or firewall restrict access

Major Learnings

- Applied Nmap for full-range scanning and OS detection
- Understood enumeration and real-world exploitation techniques
- Gained skills in privilege escalation and hash cracking
- Learned how to evaluate vulnerabilities and apply proper remediation

---

This project simulates a real-world penetration test using open-source tools and is intended strictly for educational purposes.