**ETHICAL HACKING PROJECT**

INTRODUCTION:

The purpose of this project is to simulate real-world network penetration testing and defense mechanisms using vulnerable virtual environments and professional-grade tools. It focuses on replicating how attackers scan, enumerate, exploit, and compromise networked systems and how defenders can detect, respond to, and remediate these actions. The project aims to provide hands-on experience with ethical hacking methodologies and cybersecurity best practices.

This simulation uses two primary virtual machines:

* **Kali Linux**, an advanced penetration testing Linux distribution used by ethical hackers and security professionals.
* **Metasploitable**, a deliberately vulnerable Linux-based virtual machine designed for testing and learning about security vulnerabilities.

The project is divided into multiple tasks that follow the typical penetration testing lifecycle:

1. **Network Scanning** – Identification of live hosts and open ports using tools like Nmap.
2. **Reconnaissance** – Gathering intelligence about the network, services, and systems, including hidden ports and service versions.
3. **Enumeration** – Extracting detailed information from services such as usernames, shares, and configurations.
4. **Exploitation** – Exploiting known vulnerabilities in the target system’s services using tools like Metasploit to gain unauthorized access.
5. **Privilege Escalation** – Creating a new user with root-level access on the target system.
6. **Password Cracking** – Extracting and cracking password hashes to gain deeper system access using tools like John the Ripper.
7. **Remediation** – Proposing solutions to fix identified vulnerabilities and enhance the target system’s security.

The project not only demonstrates how attacks are carried out but also emphasizes the importance of **defensive measures** such as patching outdated software, using strong passwords, and configuring services securely. By completing this project, students gain insight into the mindset of both attackers and defenders, developing critical skills necessary for real-world cybersecurity roles.

PROJECT REQUIREMENTS:

Two Operating System:

1. Kali Linux (Attacking machine)
2. Metasploitable machine ( Target Machine)

TOOLS USED:

* Nmap
* Metasploit Framework
* John the Ripper
* Metaspolitable2

TASKS:

**Network Scanning**

**Task 1: Basic Network Scan**

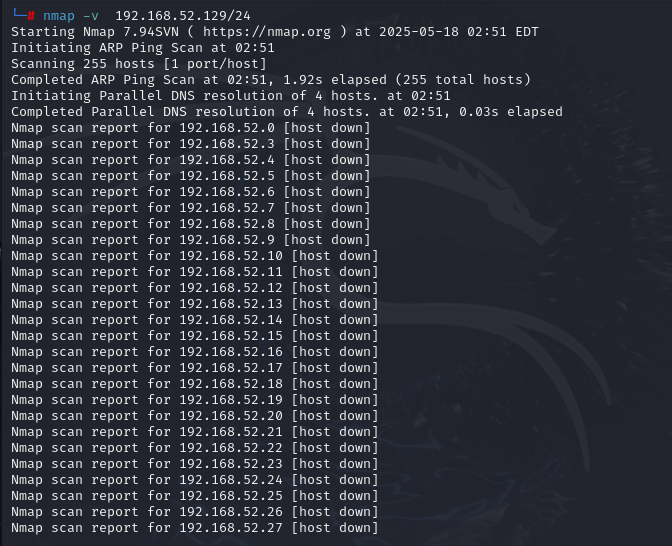
Step 1: Open a terminal on your Kali Linux machine.

Step 2: Run a basic scan on your local network.

nmap -v 192.168.52.129/24

Expected Output: A list of devices on the network, their IP addresses, and the open ports. This -v Option will show a detailed view of the running scan.

**Ouput of the Scan**



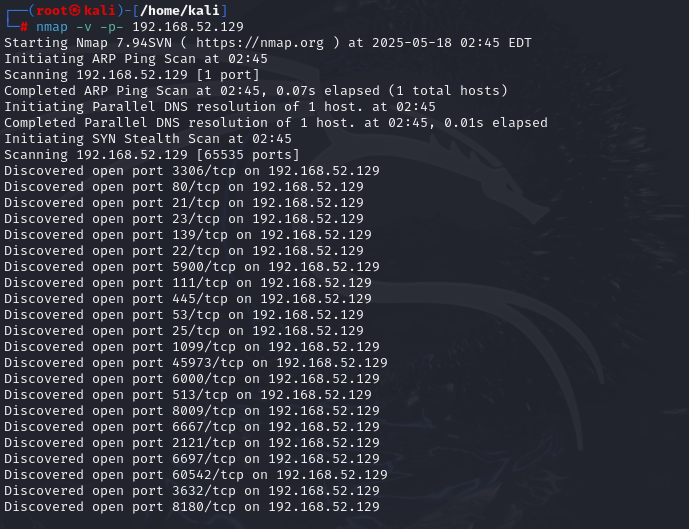
**Task 2 – Reconnaissance**

**1: Scanning for hidden Ports**

Step 1: To scan for hidden ports , we have to scan whole range of ports on that specific targeted ip address.

nmap -v -p- 192.168.52.129Expected Output: A list of hidden ports with services.

**Output**

****

**Total Hidden Ports = 7**

List of hidden ports

1.8787/tcp open msgsrvr

2.35917/tcp open unknown

3.36440/tcp open unknown

4.41865/tcp open unknown

5.45435/tcp open unknown

6.6697/tcp open ircs-u

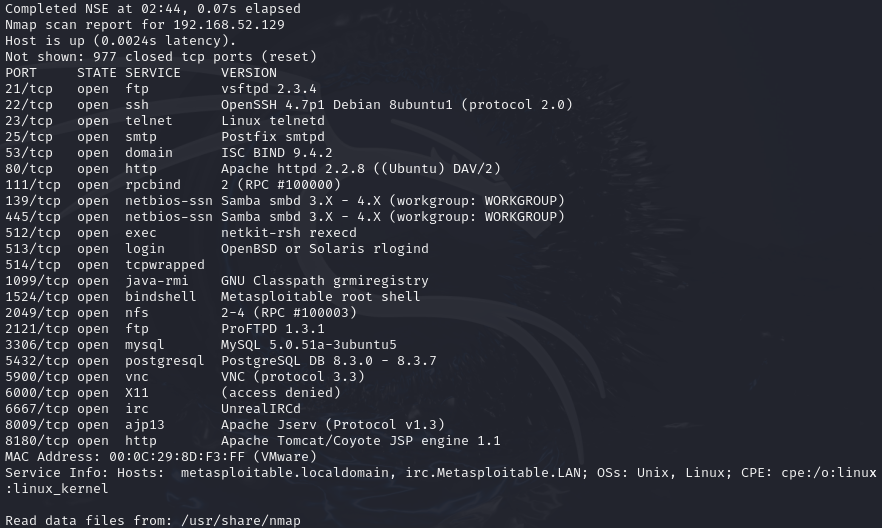
7.8009/tcp open ajp13

**2: Service Version Detection**

Step 1: Use the -sV option to detect the version of services running on open ports:

nmap -v -sV 192.168.52.129Expected Output: A detailed list of open ports and the services running on them, including version information.

**Output**

****

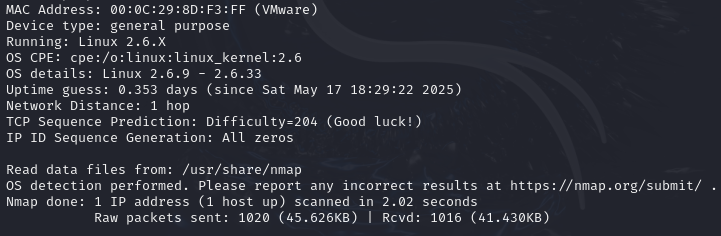
**3: Operating System Detection**

Step 1: Use the -O option to detect the operating systems of devices on the network:

nmap -v -O 192.168.52.129

Expected Output: The operating system details of the devices on the network.

**Output**



**Task 3: Enumeration**

**Target IP Address:** 192.168.52.129

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

**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 sntp | Postfix sntp |
| 53/tcp | Open domain | ISC BIND 9.4.2 |
| 80/tcp | Open http | Apache httpd 2.2.8 |
| 111/tcp | Open rpcbind | 2(RPC #100000) |
| 139/tcp | Open netbios-ssn | Samba smbd 3.X-4.X |
| 445/tcp | Open netbios-ssn | Samba smbd 3.X-4.X |
| 512/tcp | Open exec | Netkit-rsh rexecd |
| 513/tcp | Open login |  |
| 514/tcp | Open shell | Netkit rshd |
| 1099/tcp | Open java-rml | GNU classpath |
| 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 |
| 5432/tcp | Open postgresql | PostgreSQL DB 8.3.0 |
| 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 |
|  |  |  |

**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)

47436/tcp open mountd 1-3 (RPC #100005)

50918/tcp open java-rmi GNU Classpath grmiregistry

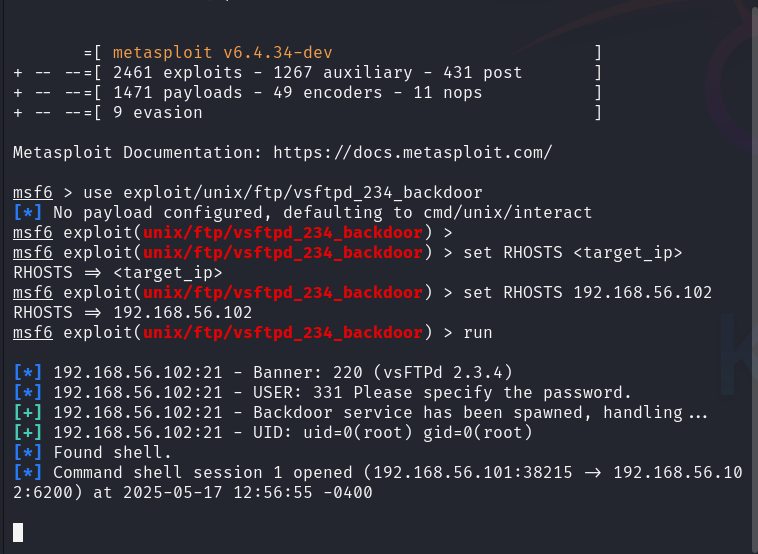
59995/tcp open nlockmgr 1-4 (RPC #100021)

60004/tcp open status 1 (RPC #100024)

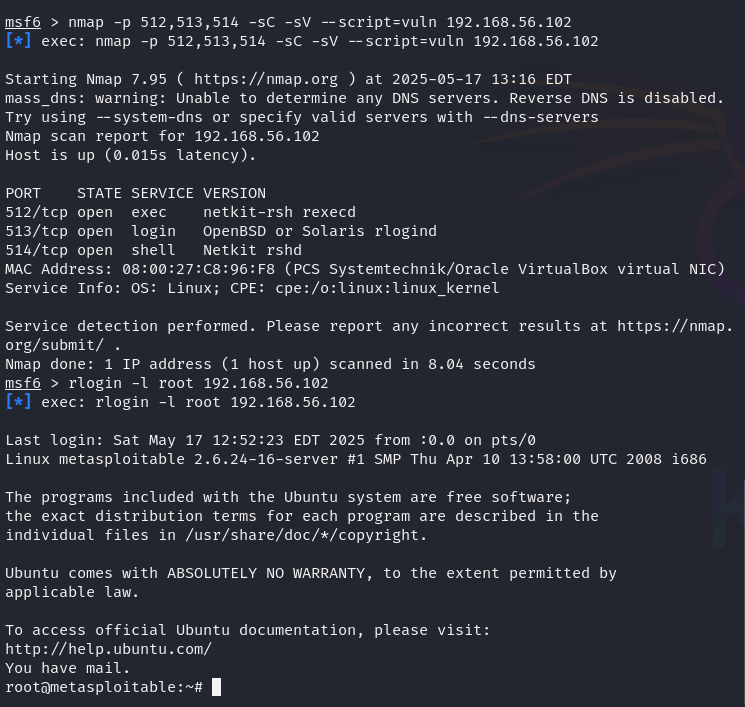
**Task 4- Exploitation of services**

**1. Exploit vsftpd 2.3.4 – Backdoor Command Execution**

* Vulnerability: Backdoor command execution vulnerability (CVE-2011-2523)
* Exploit Module: exploit/unix/ftp/vsftpd\_234\_backdoor

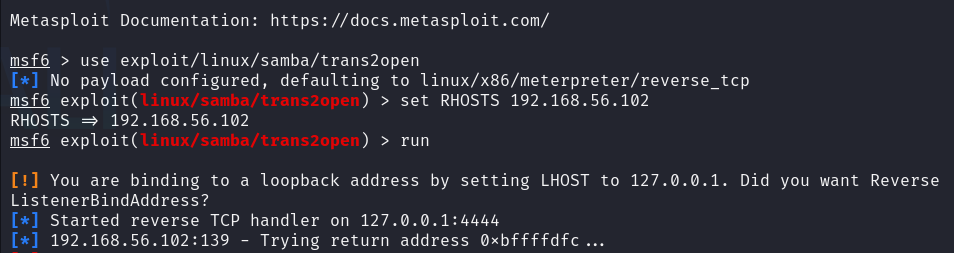


**2. Exploiting R Services (Port 512,513,514)**

****

**3. Exploit Samba smbd – Remote Command Execution**

* **Vulnerability:** Samba trans2open overflow (CVE-2003-0201)
* **Exploit Module:** exploit/linux/samba/trans2open



**Task 5 - Create user with root permission**

adduser suruchi

Set a simple password example 12345 or hello or 987654321

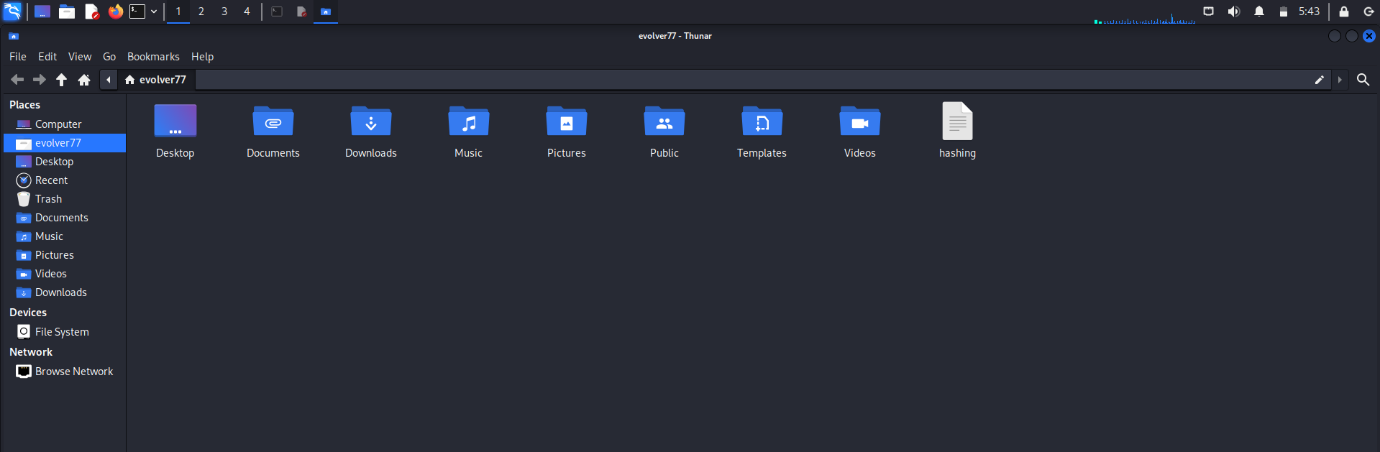
Get the details of user in /etc/passwd

Get the details of password hash in /etc/shadow

**Hash** suruchi:$1$M/R1KkTD$XGDnXXTvygtDeyM3JiDlU0:20224:0:99999:7:::

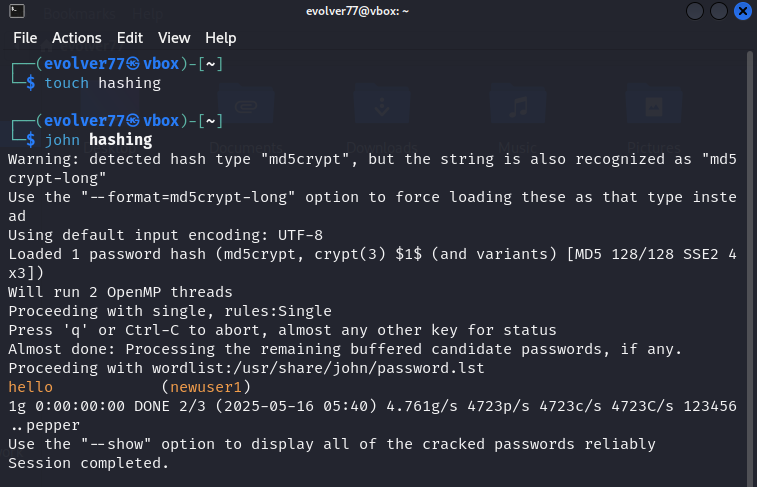
**Task 6 - Cracking password hashes**

Store the password hash in a text file

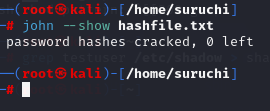


Cracking password with prebuilt wordlist of john in default mode

John hashing



John hashing –show



**Task 7: Remediation**

**Identified Issues and Recommendations:**

1. **Outdated FTP Server (vsftpd 2.3.4):**
   * Vulnerable to backdoor attack.
   * **Remediation:** Upgrade to latest secure version (e.g., vsftpd 3.0.5).
2. **Outdated SSH Server (OpenSSH 4.7p1):**
   * Susceptible to brute force and potential RCE.
   * **Remediation:** Update to latest version (e.g., OpenSSH 9.6).
3. **Insecure Java RMI Service:**
   * Allows remote code execution.
   * **Remediation:** Disable or restrict RMI access with firewall rules.

**Major Learnings**

* Understood practical use of **Nmap** for scanning and enumeration.
* Gained experience in **service exploitation** and **user privilege escalation**.
* Learned **password cracking techniques** using John the Ripper.
* Developed insight into **security best practices and remediation strategies**.