# Penetration Testing Report
# Exploitation of Windows Operating System vulnerability

Ankush Uday Naik
Ethical Hacking Internship

December 22, 2025

# Contents

# List of Figures

# Chapter 1

# Introduction

Penetration testing is a controlled and authorized security assessment technique used to identify vulnerabilities in computer systems. This report documents the step-by-step penetration testing of a Windows 7 operating system using Kali Linux and the Metasploit Framework. The objective of this assessment is to identify security weaknesses, exploit them ethically, and analyze the results for defensive purposes.

**Note:** This penetration test was conducted strictly in a controlled lab environment for Testing purposes.

# Chapter 2

# Test Environment

- Attacker Machine: Kali Linux
- Target Machine: Windows 7
- Framework Used: Metasploit
- Scanning Tool: Nmap
- Network Type: Local Network

# Chapter 3

# Reconnaissance and Scanning

## 3.1 Nmap Scanning for Open Ports


Figure 3.1: Nmap scanning results for open ports in Windows 7

**Explanation:** The attacker initiated an Nmap scan to identify open ports and services running on the Windows 7 target. The scan revealed that port 445 (SMB service) was open, which is commonly associated with Windows file sharing and is a frequent attack vector.

**Output Analysis:** Port 445 being open indicates a potential SMB vulnerability that can be exploited using Metasploit.

## 3.2 Identifying SMB Vulnerability


Figure 3.2: Targeting SMB vulnerability on port 445

**Explanation:** After identifying the open SMB port, the attacker focused on exploiting known SMB vulnerabilities in Windows 7.

**Output Analysis:** The SMB service confirmed the presence of exploitable services, making the system vulnerable to remote code execution attacks.

# Chapter 4

# Exploitation Using Metasploit

## 4.1 Starting Metasploit Framework

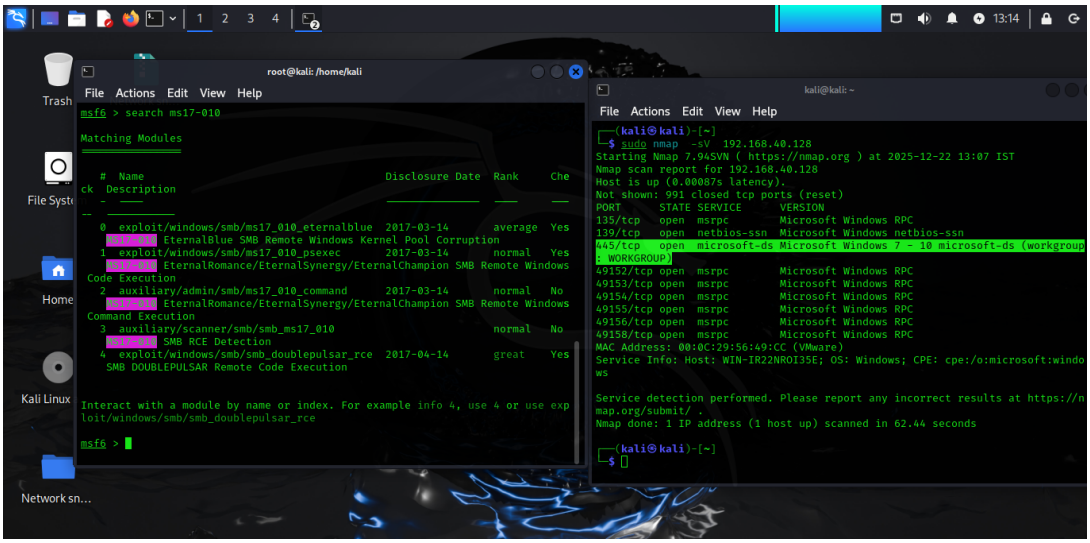


Figure 4.1: Starting Metasploit Framework

**Explanation:** The Metasploit Framework was launched to search for suitable exploits targeting the identified SMB vulnerability.

## 4.2 Selecting Appropriate Exploit

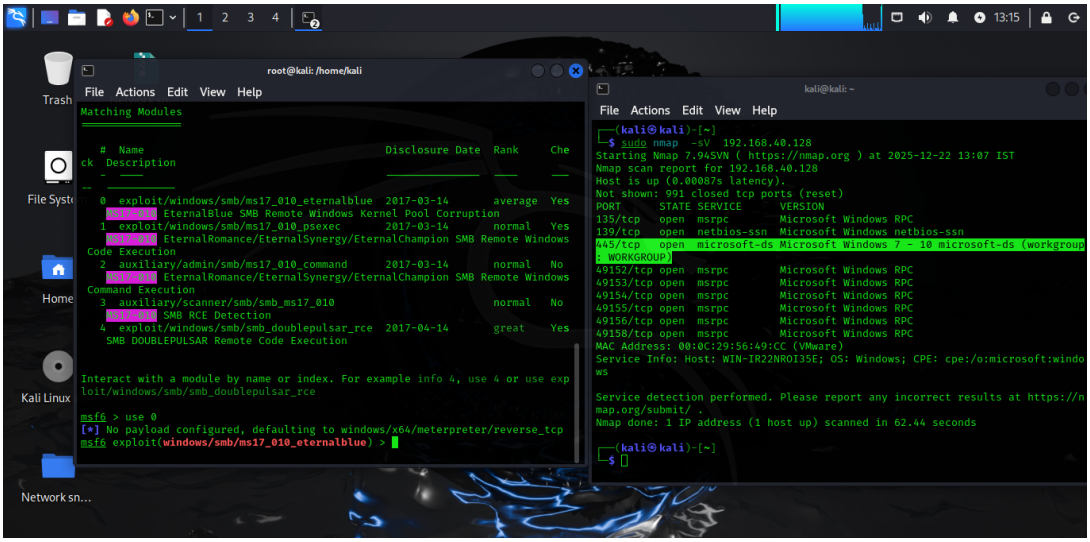


Figure 4.2: Selecting the appropriate exploit in Metasploit

**Explanation:** An appropriate exploit module compatible with the Windows 7 SMB vulnerability was selected.

**Output Analysis:** The exploit selection ensures compatibility with the target OS and service version.

## 4.3 Checking Required Exploit Parameters

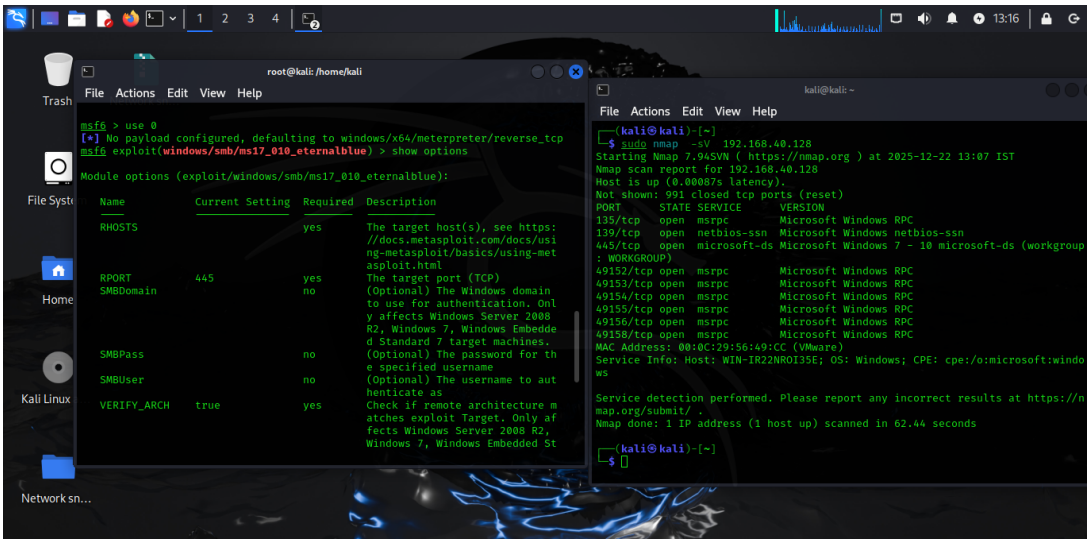


Figure 4.3: Checking required parameters for exploitation

**Explanation:** Before executing the exploit, required parameters such as RHOST and payload settings were reviewed.

## 4.4 Setting Target IP Address (RHOST)

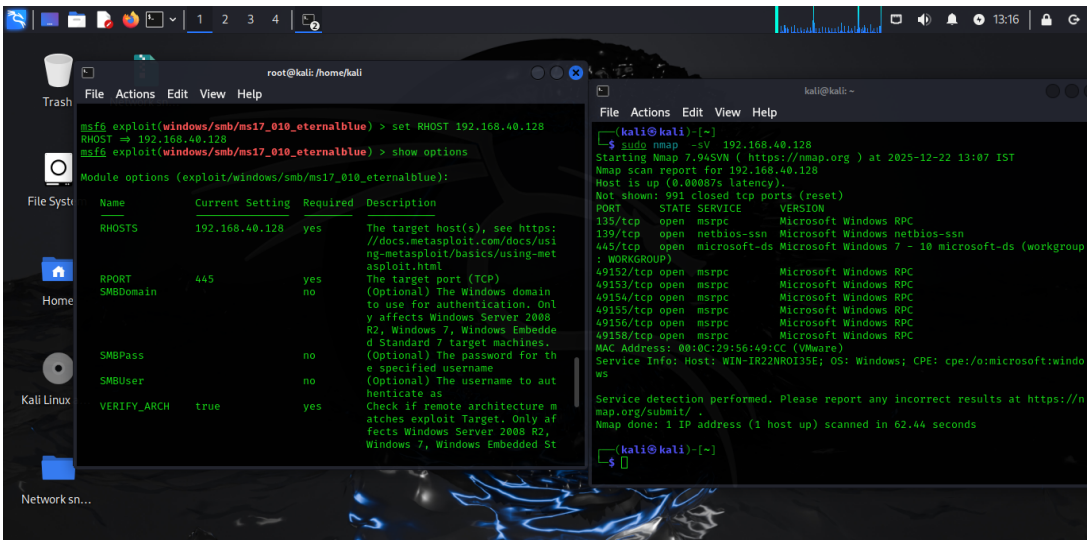


Figure 4.4: Setting RHOST parameter

**Explanation:** The target machine's IP address was set as RHOST to direct the exploit to the correct system.

## 4.5 Launching the Exploit


Figure 4.5: Launching the exploit

**Explanation:** The exploit was executed, attempting to gain unauthorized access to the Windows system.

**Output Analysis:** Successful exploitation messages indicate that the payload was delivered correctly.

## 4.6 Successful Meterpreter Session

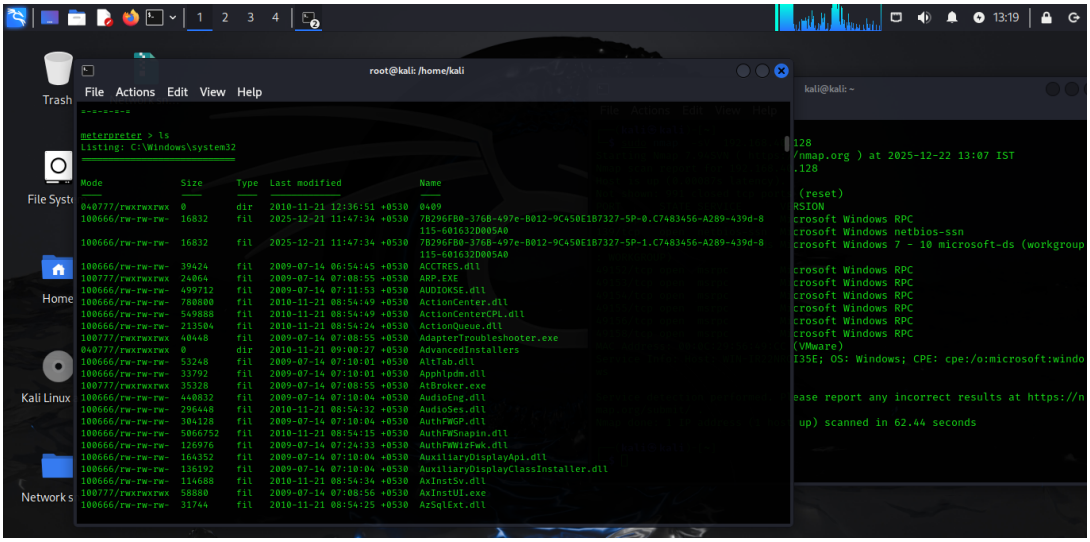


Figure 4.6: Successfully accessed Windows 7 shell

**Explanation:** A Meterpreter shell was successfully obtained, granting remote access to the Windows 7 system.

**Impact:** This confirms full system compromise with attacker-level control.

# Chapter 5

# Post-Exploitation

## 5.1 Accessing System Information Remotely

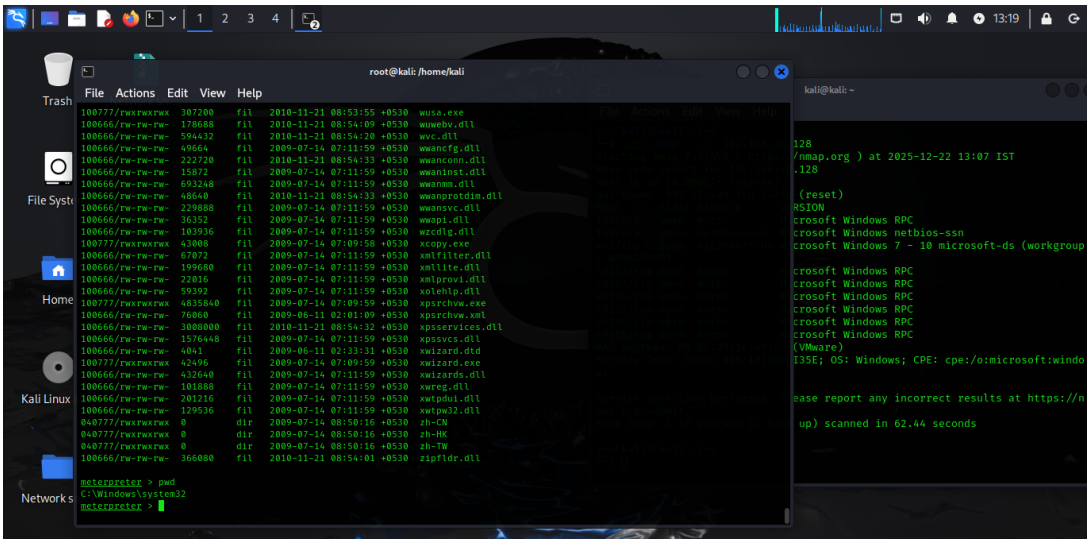


Figure 5.1: Accessing Windows system information remotely

**Explanation:** System commands were executed remotely to gather information such as OS version and user details.

## 5.2 Remote Control of Files and Directories

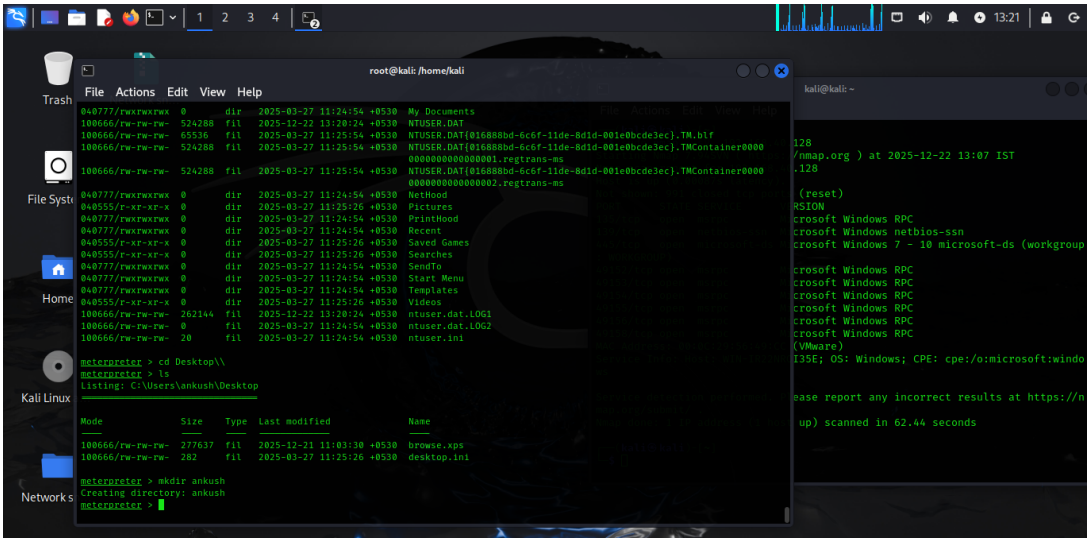


Figure 5.2: Remote creation of files and directories

**Explanation:** The attacker demonstrated the ability to create directories and files remotely, proving full control over the compromised system.

**Security Risk:** An attacker could install malware, modify files, or steal sensitive data.

# Chapter 6

# Conclusion

This penetration testing exercise demonstrated how an unpatched Windows 7 system with exposed SMB services can be fully compromised using Metasploit. The attack successfully achieved remote access, system control, and post-exploitation activities.

**Recommendations:**

- Disable SMB if not required
- Apply latest security patches
- Use strong firewall rules
- Upgrade unsupported operating systems

**Disclaimer:** This report is strictly for educational and ethical hacking purposes only.