

Challenge 3: Exploit open SMB Server Shares

In this part, I wanted to discover if there are any unsecured shared directories located on an SMB server in the [10.5.5.0/24](#) network. I can use any of the tools you learned in earlier labs to find the drive shares available on the servers.

Step 1: Scan for potential targets running SMB.

Used scanning tools to scan the [10.5.5.0/24](#) LAN for potential targets for SMB enumeration.

Command: nmap -p139,445 [10.5.5.0/24](#)

```
(root@Kali)-[~/home/kali] # nmap -sN 10.5.5.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-17 16:01 UTC
Nmap scan report for mutillidae.pc (10.5.5.11)
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE
3306/tcp  open|filtered  mysql
MAC Address: 02:42:0A:05:0B (Unknown)

Nmap scan report for dwva.pc (10.5.5.12)
Host is up (0.0000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE
80/tcp   open|filtered  http
MAC Address: 02:42:0A:05:0C (Unknown)

Nmap scan report for juice-shop.pc (10.5.5.13)
Host is up (0.0000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE
3000/tcp  open|filtered  ppp
MAC Address: 02:42:0A:05:0D (Unknown)

Nmap scan report for gravemind.pc (10.5.5.14)
Host is up (0.0000050s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open|filtered  ftp
22/tcp    open|filtered  ssh
53/tcp    open|filtered  domain
80/tcp    open|filtered  http
139/tcp   open|filtered  netbios-ssn
445/tcp   open|filtered  microsoft-ds
MAC Address: 02:42:0A:05:0E (Unknown) ←

Nmap scan report for webgoat.pc (10.5.5.15)
Host is up (0.0000050s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE      SERVICE
8080/tcp  open|filtered  http-proxy
8888/tcp  open|filtered  sun-answerbook
9001/tcp  open|filtered  tor-orport
MAC Address: 02:42:0A:05:0F (Unknown)

Nmap scan report for 10.5.5.1
Host is up (0.0000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE
22/tcp    open|filtered  ssh
```

Which host on the [10.5.5.0/24](#) network has open ports indicating it is likely running SMB services?

Gravemind.pc (10.5.5.0/24)

Ports opened 139 and 445

Services opened: netbios-ssn and microsoft-ds

Step 2: Determine which SMB directories are shared and can be accessed by anonymous users

Command: enum4linux -S 10.5.5.14

-S: This option get share list

```
[root@Kali]~[/home/kali]$ enum4linux -S 10.5.5.14/24
# smbclient -L //10.5.5.14/24
Password for [WORKGROUP\root]:
Anonymous login successful

      Sharename          Type          Comment
      _____            _____
      homes             Disk          All home directories
      workfiles         Disk          Confidential Workfiles
      print$            Disk          Printer Drivers
      IPC$              IPC           IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

      Server          Comment
      _____          _____
      Workgroup       Master

[root@Kali]~[/home/kali]
```

Step 3: Investigate each shared directory to find the file

Use the SMB-native client to access the drive shares on the SMB server. Use the dir, ls, cd, and other commands to find subdirectories and files.

Command: smbclient -L //10.5.5.14 -N

-L: Get a list of shares available on a host

-N: Don't ask for a password

```

└─(root㉿Kali)-[~/home/kali]
# smbclient //10.5.5.14/print$ -N ←
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.
..
IA64  Name          Last modified  Size  D
x64   W32X86        2017-10-31 17:31  -    0
W32MIPS Directory   2017-10-31 17:31  -    0
W32ALPHA      2017-10-31 17:31  -    0
COLOR/       2017-10-31 17:31  D    0
W32PPC/       2017-10-31 17:31  D    0
WIN40/        2017-10-31 17:31  D    0
OTHER         2021-08-30 05:00:05  D    0
Apache/2.4.10 (Debian) Server at 10.5.12 Port 80  Mon Aug 30 05:00:05 2021
38497656 blocks of size 1024. 4192948 blocks available
smb: \> cd color
smb: \color\> ls
.
..
38497656 blocks of size 1024. 4192948 blocks available
smb: \color\> cd ..
smb: \> cd OTHER ←
smb: \OTHER\> ls
.
..
sxij42.txt ←
38497656 blocks of size 1024. 4192948 blocks available
smb: \OTHER\> cat sxij42
cat: command not found
smb: \OTHER\> cat sxij42.txt ←
cat: command not found
smb: \OTHER\> get sxij42.txt ←
getting file \OTHER\sxij42.txt of size 103 as sxij42.txt (8.4 KiloBytes/sec) (average 8.4 KiloBytes/sec)
smb: \OTHER\> cat sxij42.txt
cat: command not found
smb: \OTHER\> █

```

Locate the file with the Challenge 3 code. Download the file and open it locally.

```

└─(root㉿Kali)-[~/home/kali]
# cat sxij42.txt
Congratulations!
You found the flag for Challenge 3!
The code for this challenge is NWs39691.

```

Step 4: Research and propose SMB attack remediation.

What are two remediation methods for preventing SMB servers from being accessed?

Two key remediation methods for preventing unauthorized SMB server access are:

- Network segmentation and firewall rules to restrict access to trusted IPs/VLANs
- Disabling legacy SMB versions (SMBv1) and enforcing strong authentication (like Kerberos/NTLMv2 with MFA) to prevent exploits and interception.