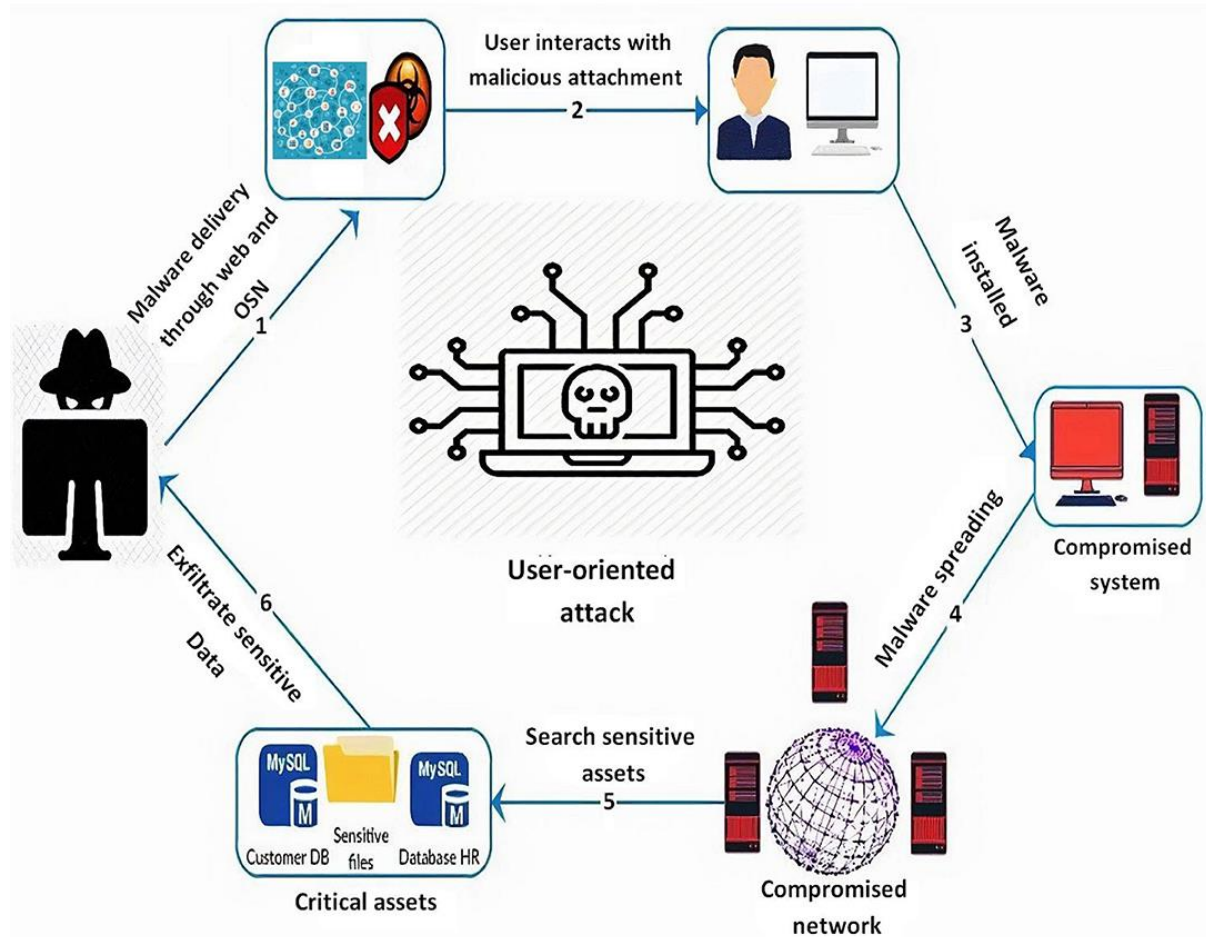


Challenge 3: Exploit open SMB Server Shares



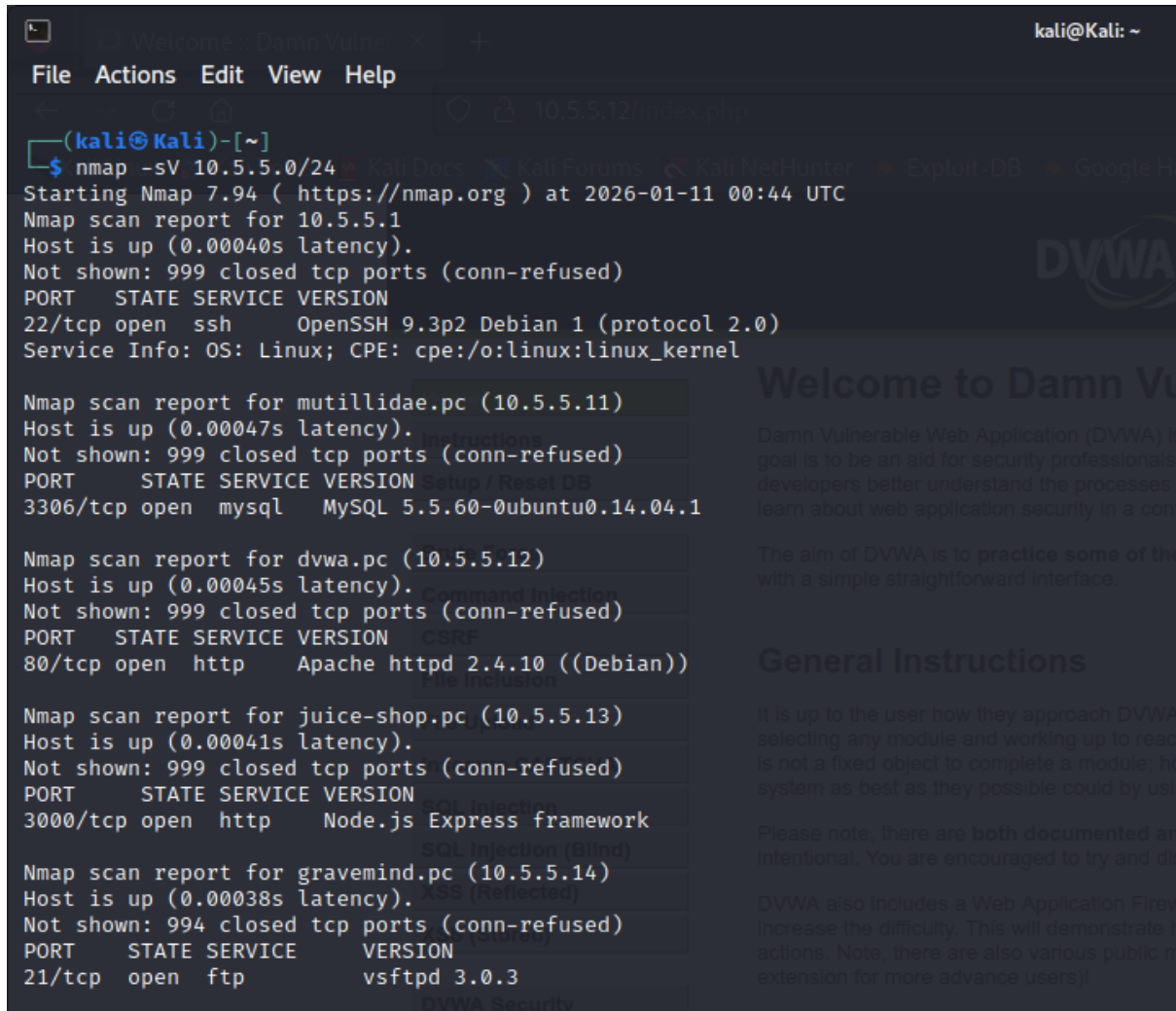
[This Photo](#) by Unknown Author is licensed under [CC BY](#)

In this part, you want to discover if there are any unsecured shared directories located on an SMB server in the 10.5.5.0/24 network. You 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.

Use scanning tools to scan the 10.5.5.0/24 LAN for potential targets for SMB enumeration.

Command: `nmap -sV 10.5.5.0/24`



```
(kali@kali)-[~]
$ nmap -sV 10.5.5.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-11 00:44 UTC
Nmap scan report for 10.5.5.1
Host is up (0.00040s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.3p2 Debian 1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for mutillidae.pc (10.5.5.11)
Host is up (0.00047s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql    MySQL 5.5.60-0ubuntu0.14.04.1

Nmap scan report for dvwa.pc (10.5.5.12)
Host is up (0.00045s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http     Apache httpd 2.4.10 ((Debian))

Nmap scan report for juice-shop.pc (10.5.5.13)
Host is up (0.00041s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
3000/tcp  open  http     Node.js Express framework

Nmap scan report for gravemind.pc (10.5.5.14)
Host is up (0.00038s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
```

Cisco Ethical Hacker Capstone Activity Challenge 3 – Exploit open SMB Server Shares

The image shows a Kali Linux terminal window with the following content:

```

File Actions Edit View Help
3000/tcp open  http      Node.js Express framework

Nmap scan report for gravemind.pc (10.5.5.14)
Host is up (0.00038s latency)
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
22/tcp    open  ssh          OpenSSH 7.9p1 Debian 10-deb10u2 (protocol 2.0)
53/tcp    open  domain       ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
80/tcp    open  http         nginx 1.14.2
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: GRAVEMIND; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for webgoat.pc (10.5.5.15)
Host is up (0.00043s latency)
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
8080/tcp   open  http-proxy   nginx 1.18.0
9001/tcp   open  jdbc         HSQLDB JDBC (Network Compatibility Version 2.3.4.0)
1 service unrecognized despite reporting data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
_
SF-Port8080-TCP:V=7.94K1=7KD=1/11Time=69627272K=x86_64-pc-linux-gnuK=Ge
SF:rtrequest,65,"HTTP/1.1\1x20404\x20Not\x20Found\r\nConnection:\x20close\r
SF:NContent-Length:\x200\r\nDate:\x20Sun,\x2011\x20Jan\x202026\x2000:44:3
SF:4\x20GMT\r\n\r\n"}&#x2D;Options,65,"HTTP/1.1\1x20404\x20Not\x20Found\r
SF:NConnection:\x20close\r\nContent-Length:\x200\r\nDate:\x20Sun,\x2011\x
SF:20Jan\x202026\x2000:44:34\x20GMT\r\n\r\n"}&#x2D;Request,42,"HTTP/1.1\
SF:20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20clos
SF:NContent-Length:65,"HTTP/1.1\1x20404\x20Not\x20Found\r
SF:NConnection:\x20close\r\nContent-Length:\x200\r\nDate:\x20Sun,\x2011\x2
SF:0Jan\x202026\x2000:44:34\x20GMT\r\n\r\n"}&#x2D;Socks,42,"HTTP/1.1\1x20400
SF:\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n

```

Which host on the 10.5.5.0/24 network has open ports indicating it is likely running SMB services?

10.5.5.14 is the host on the 10.5.5.0/24 network has open ports indicating it is likely running SMB services.

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

Use a tool to scan the device that is running SMB and locate the shares that can be accessed by anonymous users.

Command: enum4linux -S 10.5.5.14

Cisco Ethical Hacker Capstone Activity Challenge 3 – Exploit open SMB Server Shares

```
kali@Kali: ~  
File Actions Edit View Help  
(kali@Kali)-[~]  
$ enum4linux -S 10.5.5.14  
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Jan 11 06:55:54 2026  
  
===== ( Target Information ) =====  
Target ..... 10.5.5.14  
RID Range ..... 500-550,1000-1050  
Username ..... ''  
Password ..... ''  
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none  
  
===== ( Enumerating Workgroup/Domain on 10.5.5.14 ) =====  
[E] Can't find workgroup/domain  
  
===== ( Session Check on 10.5.5.14 ) =====  
[+] Server 10.5.5.14 allows sessions using username '', password ''  
Great link...  
  
===== ( Getting domain SID for 10.5.5.14 ) =====  
Domain Name: WORKGROUP  
Domain Sid: (NULL SID)  
[+] Can't determine if host is part of domain or part of a workgroup  
  
===== ( Share Enumeration on 10.5.5.14 ) =====
```

```
kali@Kali: ~  
File Actions Edit View Help  
[+] Can't determine if host is part of domain or part of a workgroup  
  
===== ( Share Enumeration on 10.5.5.14 ) =====  


| 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.  


| Server    | Comment |
|-----------|---------|
| Workgroup | Master  |

  
[+] Attempting to map shares on 10.5.5.14  
  
[E] Can't understand response:  
tree connect failed: NT_STATUS_BAD_NETWORK_NAME  
//10.5.5.14/homes Mapping: N/A Listing: N/A Writing: N/A  
//10.5.5.14/workfiles Mapping: OK Listing: OK Writing: N/A  
//10.5.5.14/print$ Mapping: OK Listing: OK Writing: N/A  
  
[E] Can't understand response:  
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*  
//10.5.5.14/IPC$ Mapping: N/A Listing: N/A Writing: N/A  
enum4linux complete on Sun Jan 11 06:56:04 2026
```

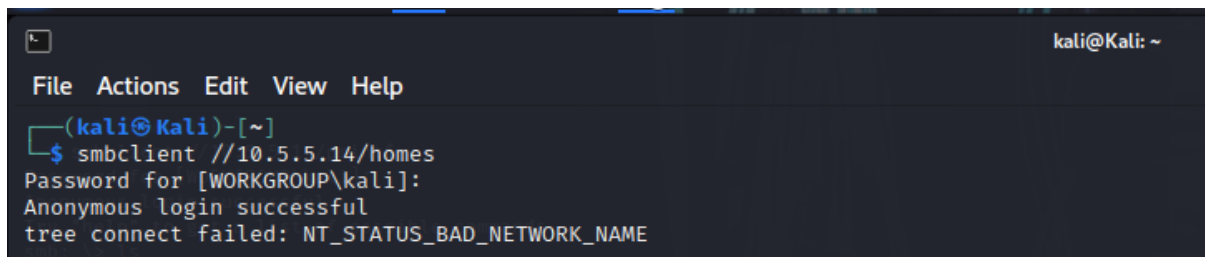
What shares are listed on the SMB server? Which ones are accessible without a valid user login?

homes, IPC\$, print\$ and workfiles. home, workfiles and print\$ are accessible without valid user credentials.

Step 3: Investigate each shared directory to find the file.

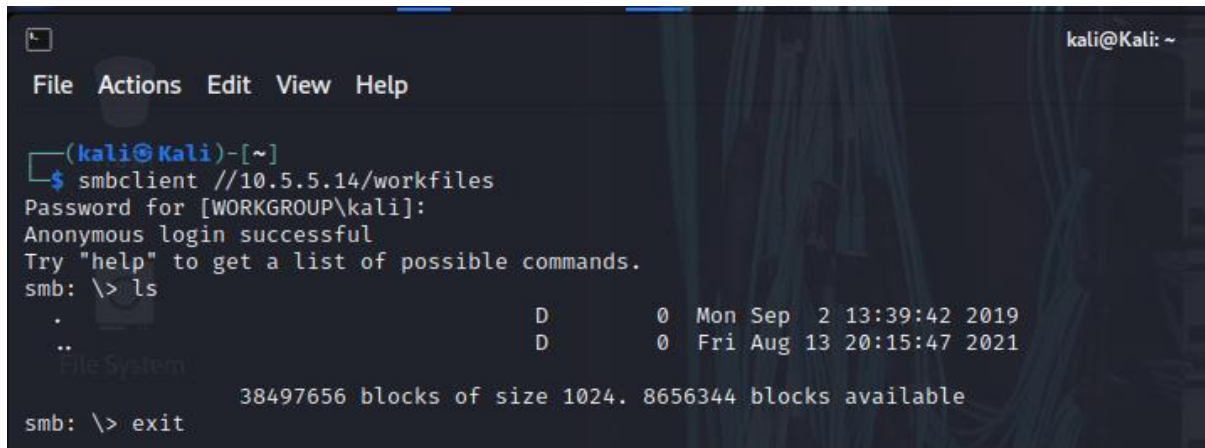
Use the SMB-native client to access the drive shares on the SMB server. Use the dir, ls, cd, and other commands to find subdirectories and files.

Command: `smcclient //10.5.5.14/homes`

A terminal window with a dark background and light-colored text. The window title is "kali@Kali: ~". The menu bar shows "File Actions Edit View Help". The prompt is "(kali@Kali)-[~]". The user enters the command "\$ smbclient //10.5.5.14/homes". The output shows "Password for [WORKGROUP\kali]:", "Anonymous login successful", and "tree connect failed: NT_STATUS_BAD_NETWORK_NAME".

```
(kali@Kali)-[~]
$ smbclient //10.5.5.14/homes
Password for [WORKGROUP\kali]:
Anonymous login successful
tree connect failed: NT_STATUS_BAD_NETWORK_NAME
```

Command: `smcclient //10.5.5.14/workfiles`

A terminal window with a dark background and light-colored text. The window title is "kali@Kali: ~". The menu bar shows "File Actions Edit View Help". The prompt is "(kali@Kali)-[~]". The user enters the command "\$ smbclient //10.5.5.14/workfiles". The output shows "Password for [WORKGROUP\kali]:", "Anonymous login successful", and "Try 'help' to get a list of possible commands.". The user enters "smb: \> ls". The output shows a directory listing with two entries: "." and "..", both marked as "D" (directories) with timestamps "0 Mon Sep 2 13:39:42 2019" and "0 Fri Aug 13 20:15:47 2021" respectively. The user enters "smb: \> exit".

```
(kali@Kali)-[~]
$ smbclient //10.5.5.14/workfiles
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                               D          0 Mon Sep  2 13:39:42 2019
..                              D          0 Fri Aug 13 20:15:47 2021
File System
38497656 blocks of size 1024. 8656344 blocks available
smb: \> exit
```

Command: `smcclient //10.5.5.14/print$`

Cisco Ethical Hacker Capstone Activity Challenge 3 – Exploit open SMB Server Shares

```

kali@Kali: ~
File Actions Edit View Help

(kali@Kali)-[~]
$ smbclient //10.5.5.14/print$
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                  d\wa.pc          ff02:1          D          0 Mon Aug 14 09:42:06 2023
..                 d\wa.vb          ff02:1          D          0 Mon Aug 30 05:00:05 2021
IA64               ff02:1          D          0 Mon Sep  2 13:39:42 2019
x64                D          0 Mon Aug 30 05:00:05 2021
W32X86             IP_list.txt Pictures Videos D          0 Mon Aug 30 05:00:05 2021
W32MIPS            Music Public an D          0 Mon Sep  2 13:39:42 2019
W32ALPHA           OTHER Templates badfil D          0 Mon Sep  2 13:39:42 2019
COLOR              kali@Kali-~ D          0 Mon Sep  2 13:39:42 2019
W32PPC             D          0 Mon Sep  2 13:39:42 2019
WIN40              D          0 Mon Sep  2 13:39:42 2019
OTHER              D          0 Fri Oct  8 00:00:00 2021
color              kali@Kali-~ D          0 Mon Aug 30 05:00:05 2021

38497656 blocks of size 1024. 8656344 blocks available
smb: \> cd COLOR
smb: \COLOR\> ls
.                  D          0 Mon Sep  2 13:39:42 2019
..                 D          0 Mon Aug 14 09:42:06 2023

38497656 blocks of size 1024. 8656344 blocks available
smb: \COLOR\> cd ..
smb: \> pwd

```

```

kali@Kali: ~
File Actions Edit View Help

smb: \> cd COLOR
smb: \COLOR\> ls
.                  D          0 Mon Sep  2 13:39:42 2019
..                 D          0 Mon Aug 14 09:42:06 2023

38497656 blocks of size 1024. 8656344 blocks available
smb: \COLOR\> cd ..
smb: \> pwd
Current directory is \\10.5.5.14\print$
smb: \> cd OTHER
smb: \OTHER\> ls
.                  D          0 Fri Oct  8 00:00:00 2021
..                 D          0 Mon Aug 14 09:42:06 2023
sxij42.txt         N          103 Tue Oct 12 00:00:00 2021

38497656 blocks of size 1024. 8656332 blocks available
smb: \OTHER\> get sxij42.txt
getting file \OTHER\sxij42.txt of size 103 as sxij42.txt (100.6 KiloBytes/sec) (average 100.6 KiloBytes/sec)
smb: \OTHER\> exit

(kali@Kali)-[~]
$ pwd
/home/kali

(kali@Kali)-[~]
$ ls
Desktop      Music      Templates  capture1.pcap  nmap_version.txt  scan_os_host23.txt  scan_smba.txt
Documents    OTHER      Videos    discovery_scan.txt  packetdump.pcap   scan_psva.txt       scan_vpsv_host23.txt
Downloads    Pictures  an         ifconfig.txt     scan_enum_users.txt  scan_results.htm    sfa_cert.html

```

```
kali@Kali: ~  
File Actions Edit View Help  
.  
..  
sxij42.txt  
38497656 blocks of size 1024. 8656332 blocks available  
smb: \OTHER\> get sxij42.txt  
getting file \OTHER\sxij42.txt of size 103 as sxij42.txt (100.6 KiloBytes/sec) (average 100.6 KiloBytes/sec)  
smb: \OTHER\> exit  
(kali@Kali)-[~]  
$ pwd  
/home/kali  
(kali@Kali)-[~]  
$ ls  
Desktop      Music      Templates  capture1.pcap  nmap_version.txt  scan_os_host23.txt  scan_smba.txt  
Documents    OTHER      Videos    discovery_scan.txt  packetdump.pcap  scan_psva.txt      scan_vpsv_host23.txt  
Downloads    Pictures   an         ifconfig.txt     scan_enum_users.txt  scan_results.htm    sfa_cert.html  
IP_list.txt  Public    badfile.txt  nmap_version     scan_host23.txt     scan_results.txt    sxij42.txt  
(kali@Kali)-[~]  
$ cat sxij42.txt  
Congratulations!  
You found the flag for Challenge 3!  
The code for this challenge is NWS39691.  
(kali@Kali)-[~]  
$
```

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

Command: `smb: \OTHER\> get sxij42.txt`

Command: `smb: \OTHER\> cat sxij42.txt`

In which share is the file found?
`print$/OTHER`

What is the name of the file with Challenge 3 code?
`sxij42.txt`

Enter the code for Challenge 3 below.

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 are

1. disabling anonymous access and enforcing authentication
2. restricting SMB traffic using firewall rules or access control lists