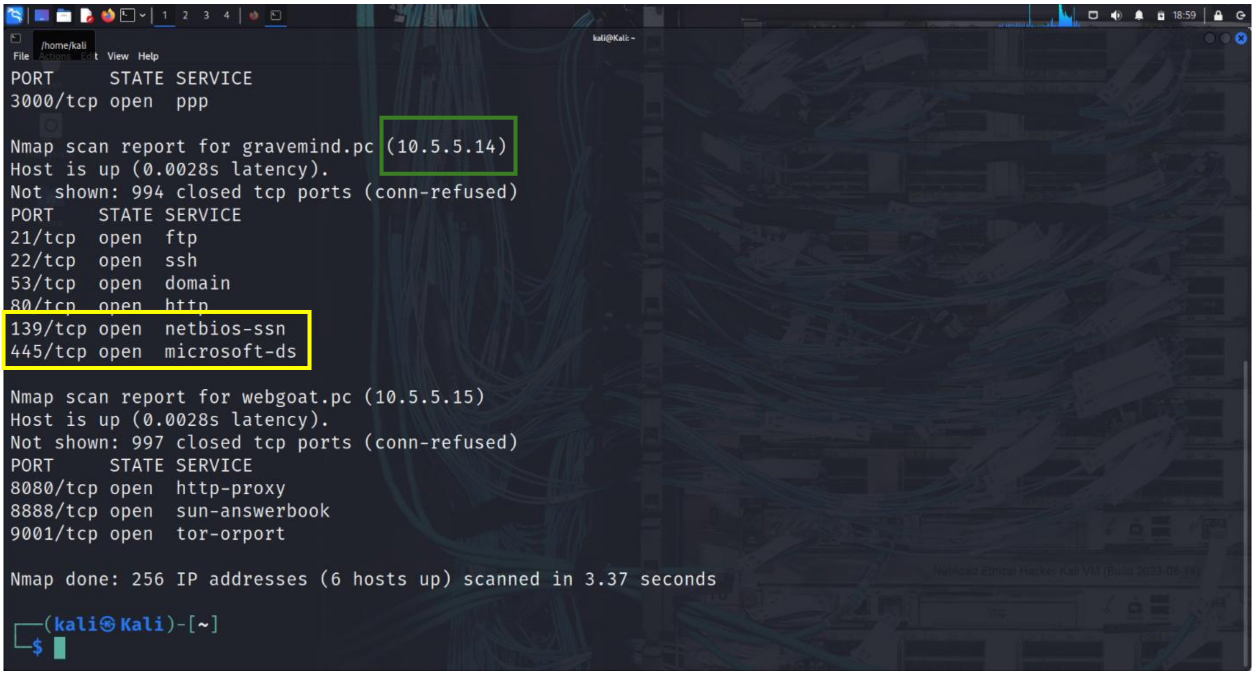
Challenge 3: Exploit open SMB Server Shares

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.

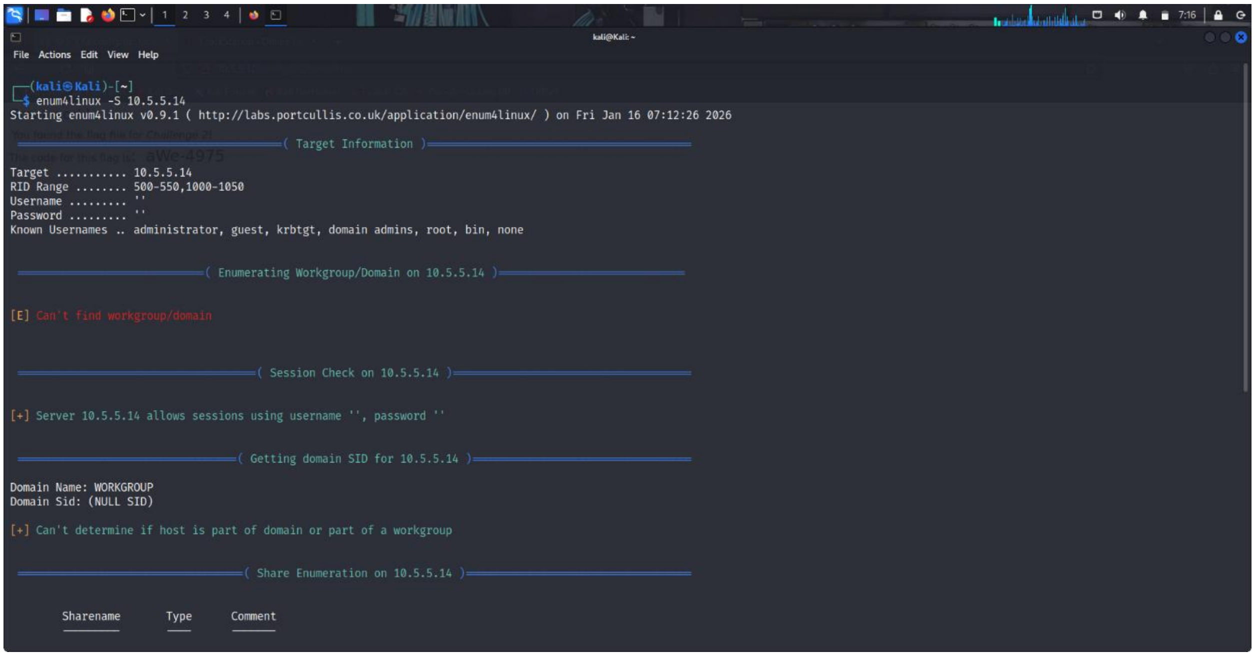
Which host on the 10.5.5.0/24 network has open ports indicating it is likely running SMB services?



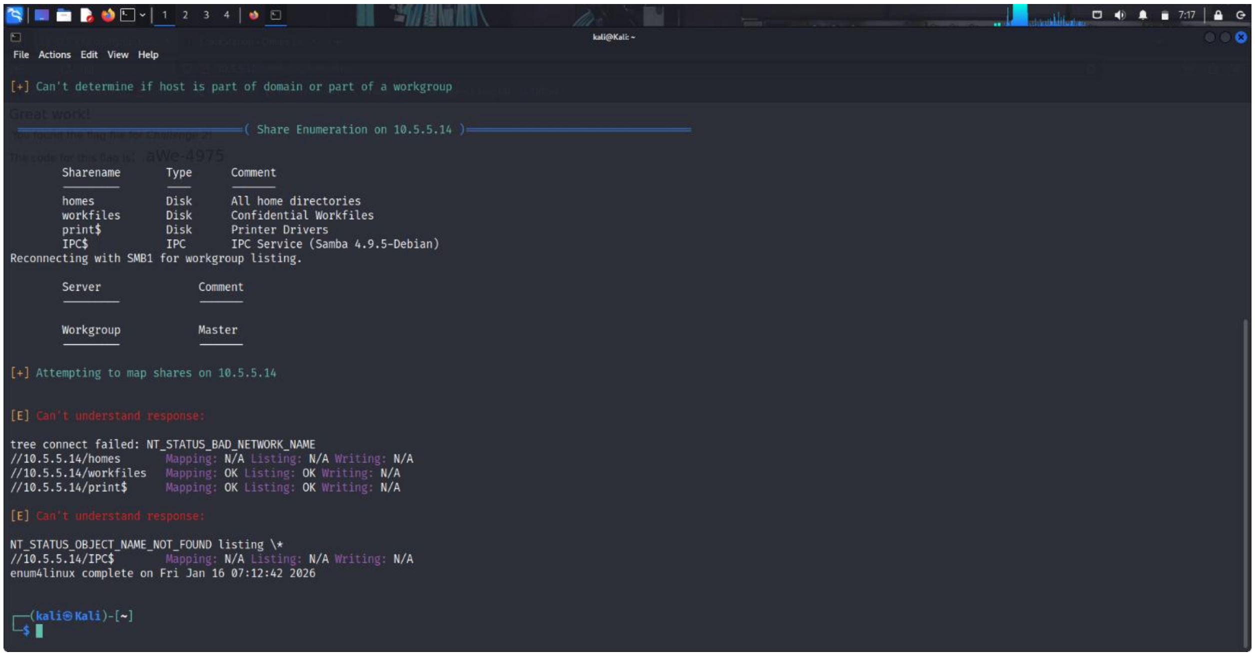
```
PORT     STATE SERVICE
3000/tcp open  ppp

Nmap scan report for gravemind.pc (10.5.5.14)
Host is up (0.0028s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap scan report for webgoat.pc (10.5.5.15)
Host is up (0.0028s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
8080/tcp open  http-proxy
8888/tcp open  sun-answerbook
9001/tcp open  tor-orport

Nmap done: 256 IP addresses (6 hosts up) scanned in 3.37 seconds

┌──(kali㉿Kali)-[~]
└─$
```

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.

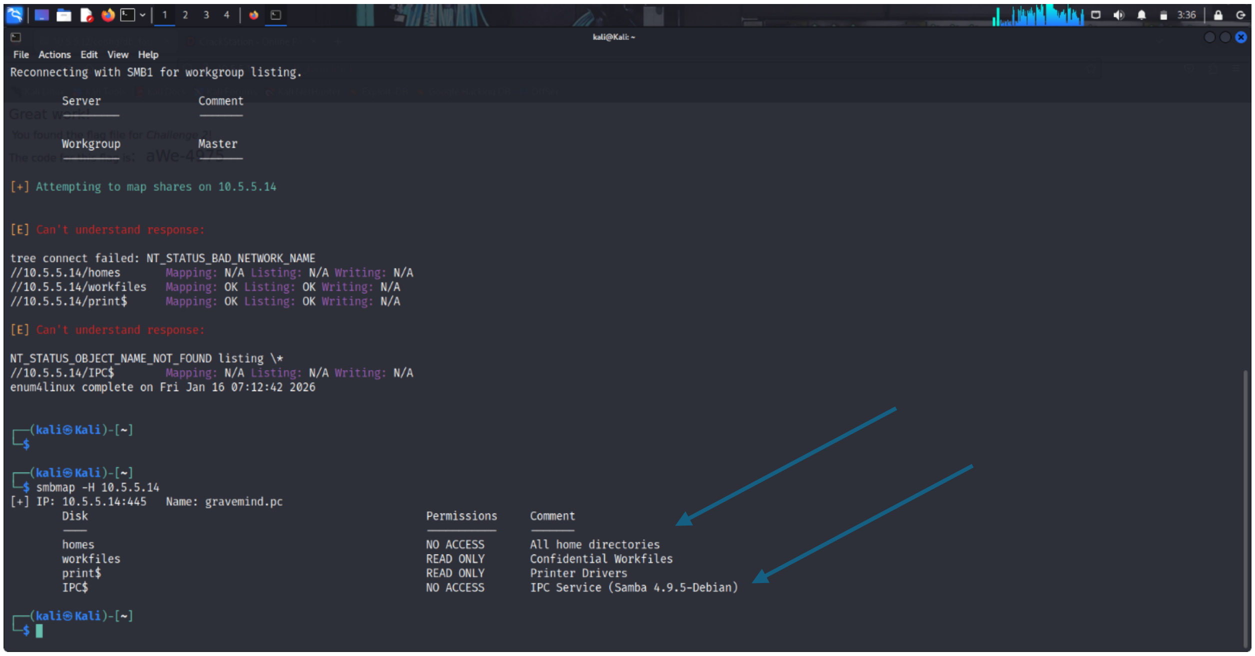


```
┌──(kali㉿Kali)-[~]
└─$ enum4linux -S 10.5.5.14
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jan 16 07:12:26 2026

 ===========================( 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 ''


 ============================( 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 )============================


        Sharename       Type      Comment
        ---------       ----      -------
```



```
[+] 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 Fri Jan 16 07:12:42 2026


┌──(kali㉿Kali)-[~]
└─$ 
```

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



```
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 Fri Jan 16 07:12:42 2026


┌──(kali㉿Kali)-[~]
└─$

┌──(kali㉿Kali)-[~]
└─$ smbmap -H 10.5.5.14
[+] IP: 10.5.5.14:445   Name: gravemind.pc
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        homes                                                   NO ACCESS       All home directories
        workfiles                                               READ ONLY       Confidential Workfiles
        print$                                                  READ ONLY       Printer Drivers
        IPC$                                                    NO ACCESS       IPC Service (Samba 4.9.5-Debian)

┌──(kali㉿Kali)-[~]
└─$
```

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

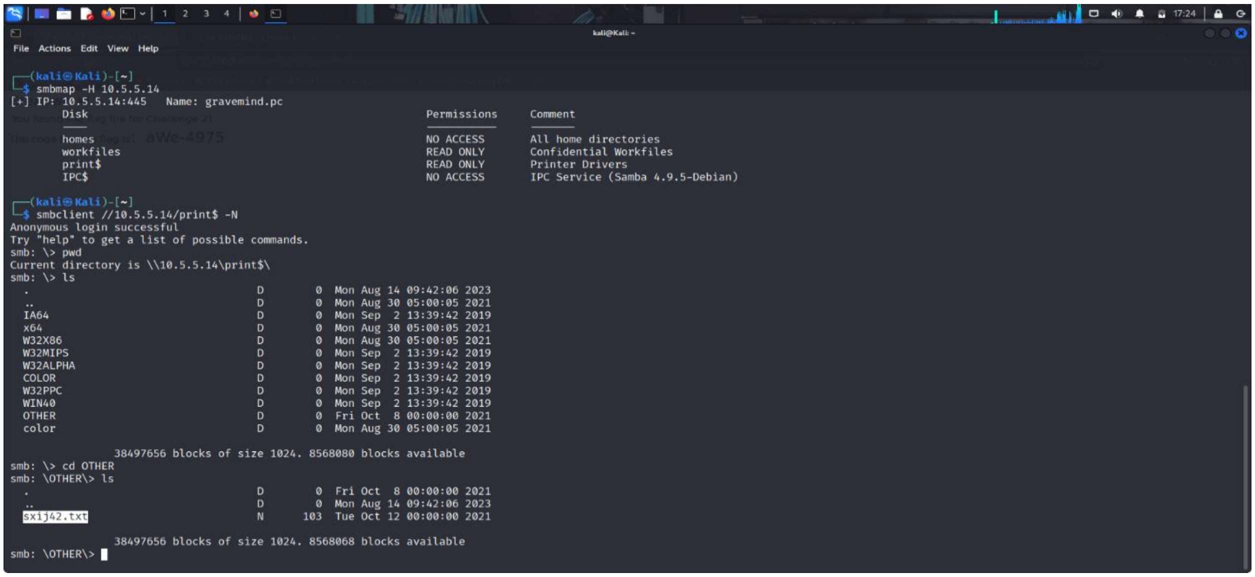
homes workfiles print$ IPC$

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.

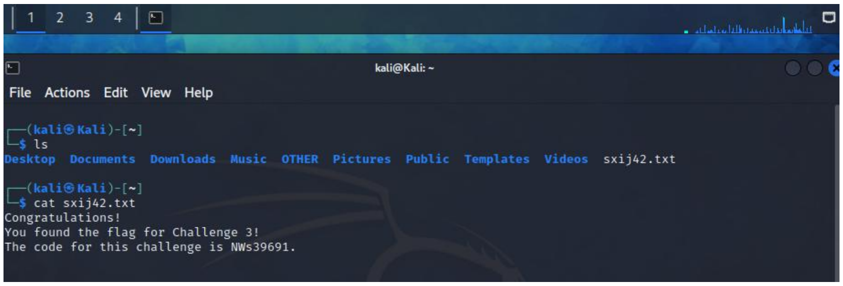
Locate the file with the Challenge 3 code. Download the file and open it locally.

In which share is the file found?



```
┌──(kali㉿Kali)-[~]
└─$ smbmap -H 10.5.5.14
[+] IP: 10.5.5.14:445   Name: gravemind.pc
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        homes                                                   NO ACCESS       All home directories
        workfiles                                               READ ONLY       Confidential Workfiles
        print$                                                  READ ONLY       Printer Drivers
        IPC$                                                    NO ACCESS       IPC Service (Samba 4.9.5-Debian)

┌──(kali㉿Kali)-[~]
└─$ smbclient //10.5.5.14/print$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> pwd
Current directory is \\10.5.5.14\print$\
smb: \> ls
  .                                   D        0  Mon Aug 14 09:42:06 2023
  ..                                  D        0  Mon Aug 30 05:00:05 2021
  IA64                                D        0  Mon Sep  2 13:39:42 2019
  x64                                 D        0  Mon Aug 30 05:00:05 2021
  W32X86                              D        0  Mon Aug 30 05:00:05 2021
  W32MIPS                             D        0  Mon Sep  2 13:39:42 2019
  W32ALPHA                            D        0  Mon Sep  2 13:39:42 2019
  COLOR                               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                               D        0  Mon Aug 30 05:00:05 2021

                38497656 blocks of size 1024. 8568080 blocks available
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. 8568068 blocks available
smb: \OTHER\>
```

In which share is the file found? print$
What is the name of the file with the Challenge 3 code? sxij42.txt
What is the Challenge 3 code? NWs39691
Enter the code for Challenge 3 below.



```
┌──(kali㉿Kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  OTHER  Pictures  Public  Templates  Videos  sxij42.txt

┌──(kali㉿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?

There are two efficient ways to stop unwanted access to SMB servers:

1) Firewall rules and network segmentation: By limiting access to only the appropriate segments of incoming SMB communication (TCP port 445) from untrusted networks, firewalls can stop external attacks and stop the spread of malware.

2) Turn off SMBv1 and put robust SMB security in place: To improve security and stop credential theft, uninstall SMBv1 because of its weaknesses, impose newer SMB versions, activate SMB Signing, and utilize Kerberos authentication. When combined, these tactics enhance safe communication and lessen vulnerability to attacks.