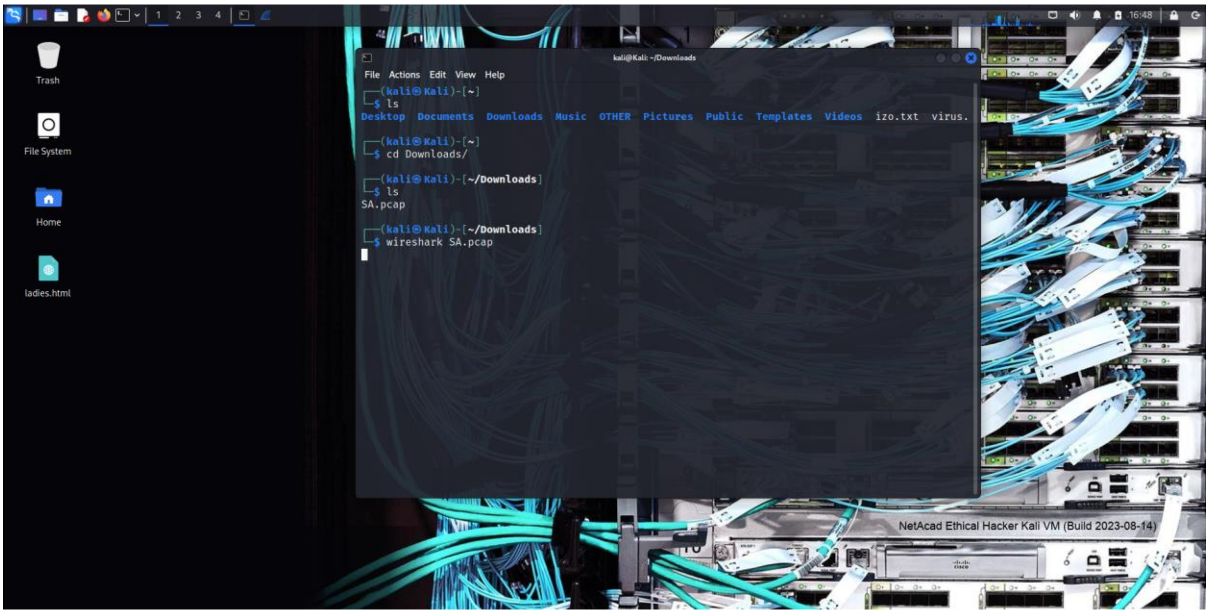
Challenge 4: Analysed a PCAP file to find information

Using the pcap file located on the Downloads subdirectory within the kali user home directory (SA.pcap), I used reconnaissance to capture the traffic using Wireshark.

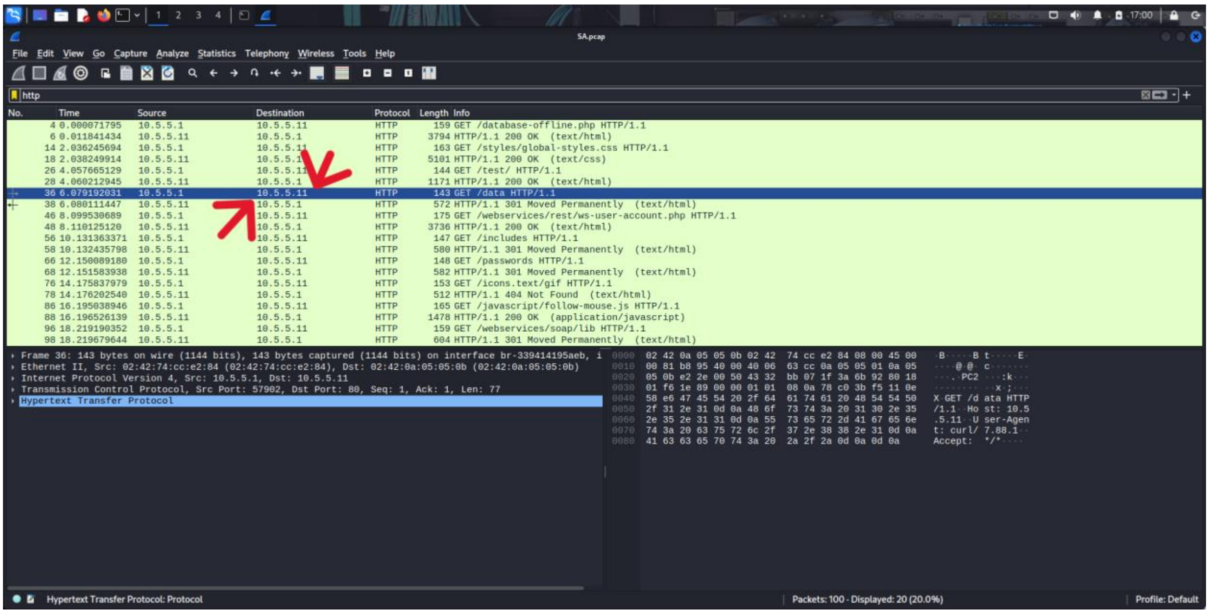


Trash
File System
Home
ladies.html
kali@Kali: ~/Downloads
File Actions Edit View Help
16:48
NetAcad Ethical Hacker Kali VM (Build 2023-08-14)

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

┌──(kali㉿Kali)-[~]
└─$ cd Downloads/

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

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

Step 1: Find and analyse the SA.pcap file

Analyse 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



SA.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
17:00

```
http
```

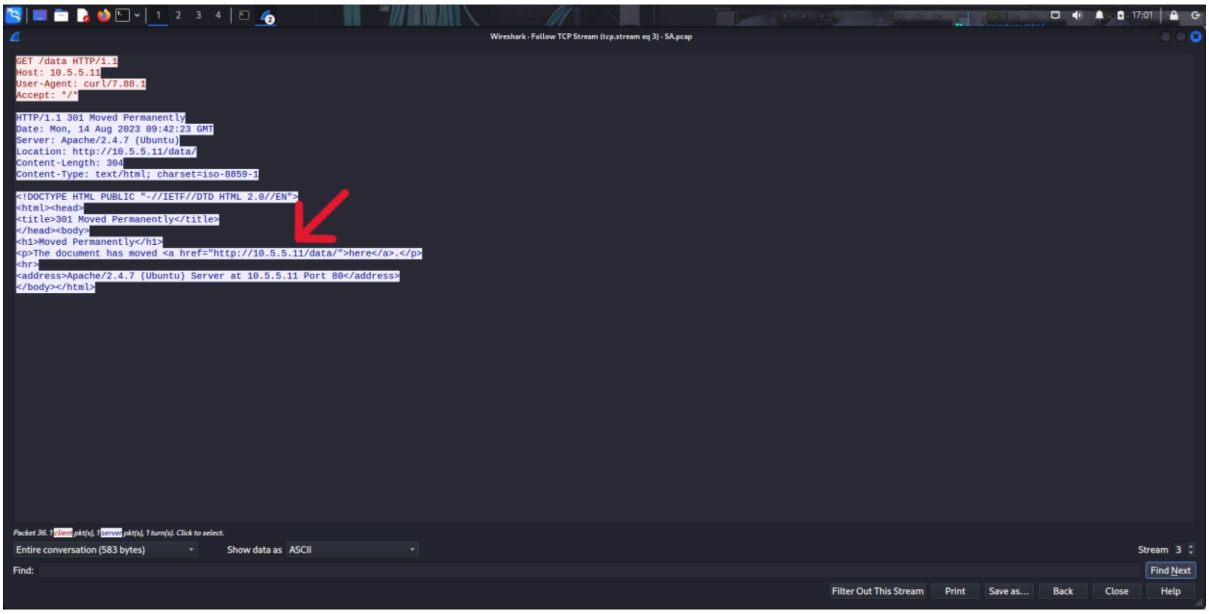
```
No.   Time          Source       Destination  Protocol Length Info
    4 0.000071795   10.5.5.1     10.5.5.11    HTTP      159 GET /database-offline.php HTTP/1.1
    6 0.011841434   10.5.5.11    10.5.5.1     HTTP     3794 HTTP/1.1 200 OK  (text/html)
   14 2.036245694   10.5.5.1     10.5.5.11    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
   98 18.219679644  10.5.5.11    10.5.5.1     HTTP      604 HTTP/1.1 301 Moved Permanently  (text/html)
```

```
› Frame 36: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface br-339414195aeb, i
› 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: 57902, Dst Port: 80, Seq: 1, Ack: 1, Len: 77
› Hypertext Transfer Protocol
```

```
0000  02 42 0a 05 05 0b 02 42  74 cc e2 84 08 00 45 00   ·B····B t·····E·
0010  00 81 b8 95 40 00 40 06  63 cc 0a 05 05 01 0a 05   ····@·@· c·······
0020  05 0b e2 2e 00 50 43 32  bb 07 1f 3a 6b 92 80 18   ·····PC2 ···:k···
0030  01 f6 1e 89 00 00 01 01  08 0a 78 c0 3b f5 11 0e   ········ ··x·;···
0040  58 e6 47 45 54 20 2f 64  61 74 61 20 48 54 54 50   X·GET /d ata HTTP
0050  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 31 30 2e 35   /1.1··Ho st: 10.5
0060  2e 35 2e 31 31 0d 0a 55  73 65 72 2d 41 67 65 6e   .5.11··U ser-Agen
0070  74 3a 20 63 75 72 6c 2f  37 2e 38 38 2e 31 0d 0a   t: curl/ 7.88.1··
0080  41 63 63 65 70 74 3a 20  2a 2f 2a 0d 0a 0d 0a      Accept:  */*····
```

Hypertext Transfer Protocol: Protocol | Packets: 100 · Displayed: 20 (20.0%) | Profile: Default

Follow the TCP streams to see paths revealed in the captured traffic.



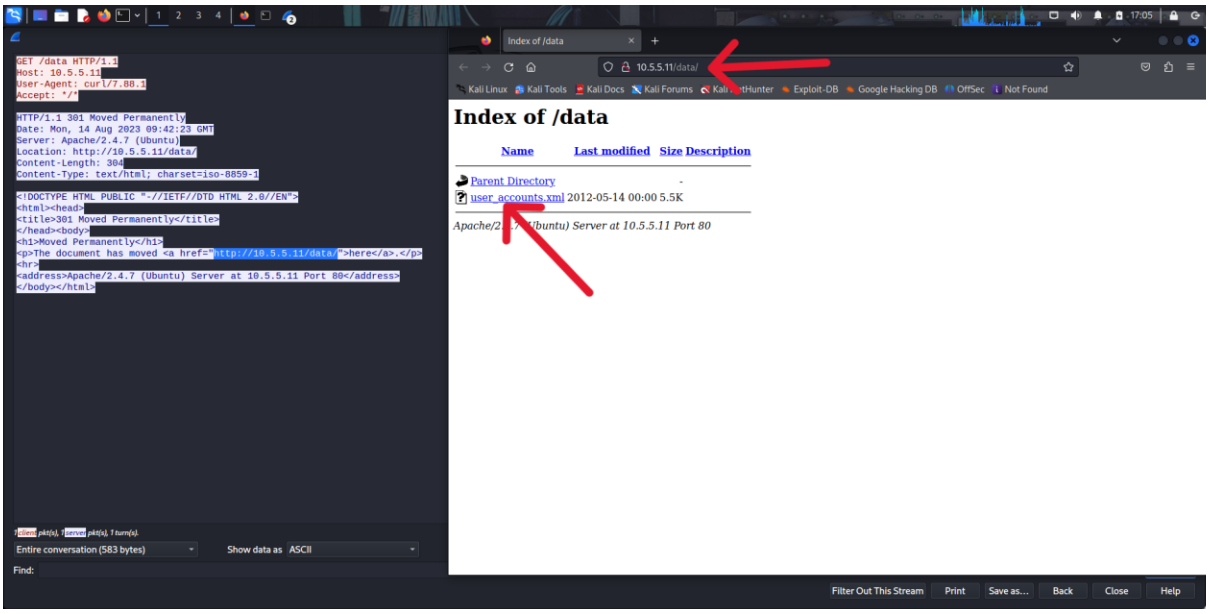
```
GET /data HTTP/1.1
Host: 10.5.5.11
User-Agent: curl/7.88.1
Accept: */*

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>
```

Packet 36. 1 client pkt(s), 1 server pkt(s), 1 turn(s). Click to select.

Entire conversation (583 bytes)   Show data as ASCII   Stream 3

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



```
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>
```

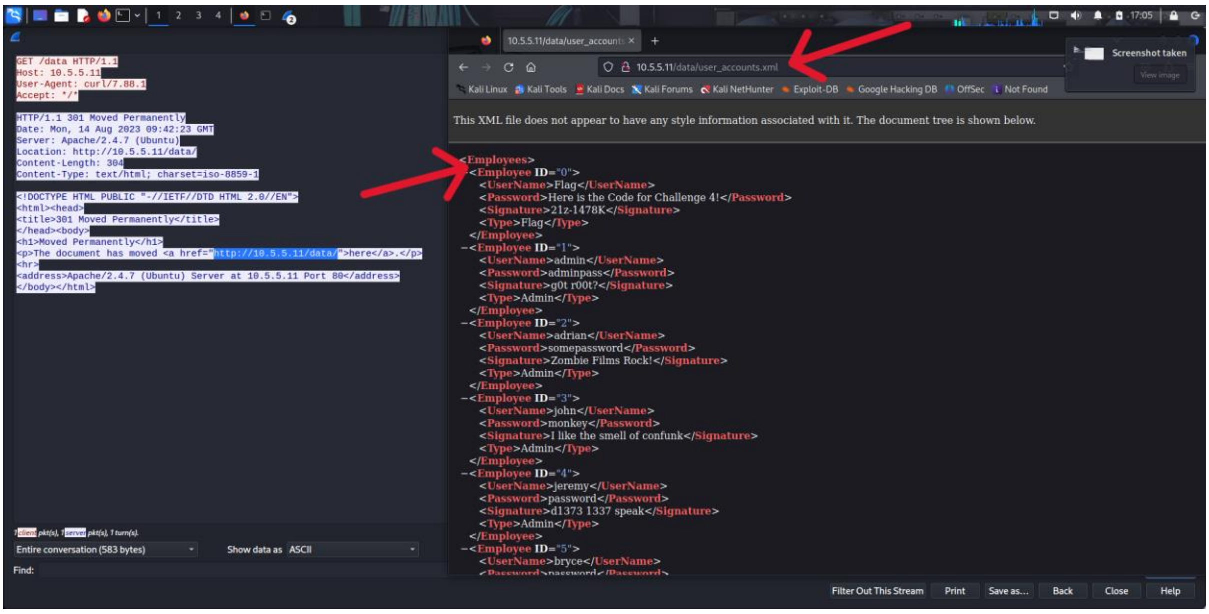
10.5.5.11/data/

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



```
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>
```

1 client pkt(s), 1 server pkt(s), 1 turn(s).

Entire conversation (583 bytes)   Show data as ASCII

10.5.5.11/data/user_accounts.xml

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>
```

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

There are two key remediation methods that would help prevent unauthorised viewing of the file contents:

- Data encryption by rendering data unreachable without a key
- Implementing robust access controls like strong passwords, multifactor authentication, and permissions.