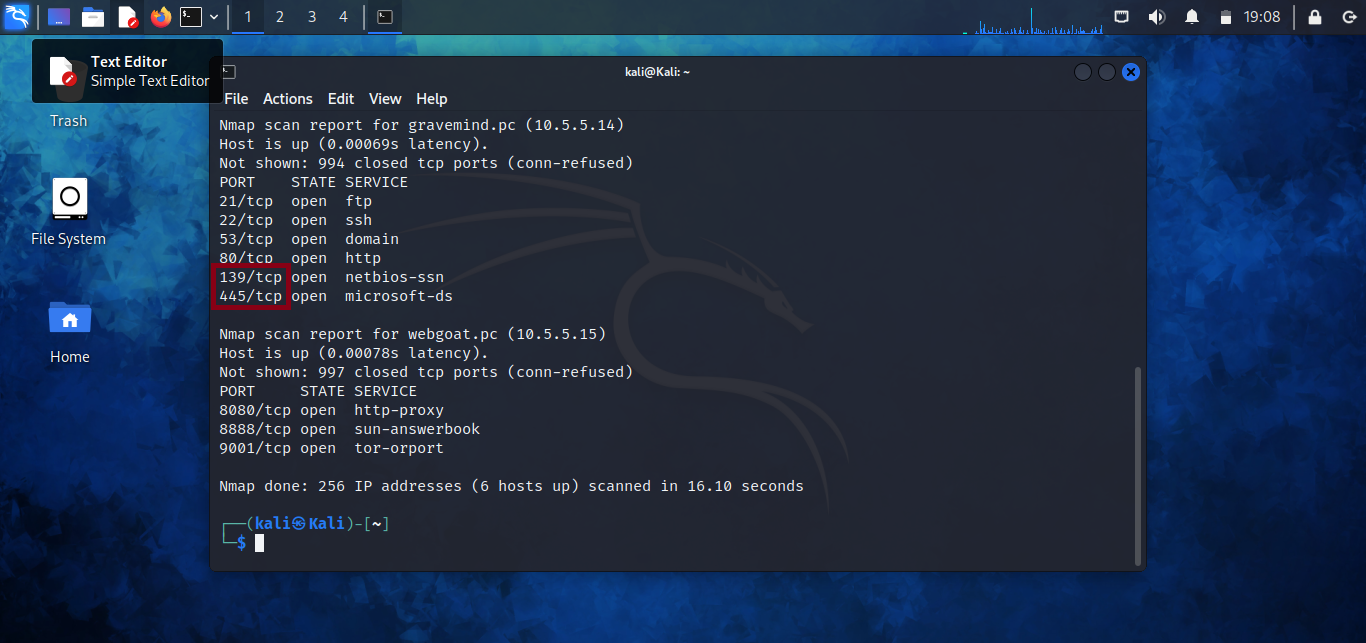
**Challenge 3: Exploit Open SMB Server Shares**

In this challenge, you must discover if there are any unsecured shared directories located on an SMB server within the 10.5.5.0/24 network. Using reconnaissance and enumeration tools, you will identify anonymous-accessible SMB shares, access them, and retrieve the Challenge 3 flag file.

**Step 1: Scan for Potential Targets Running SMB**

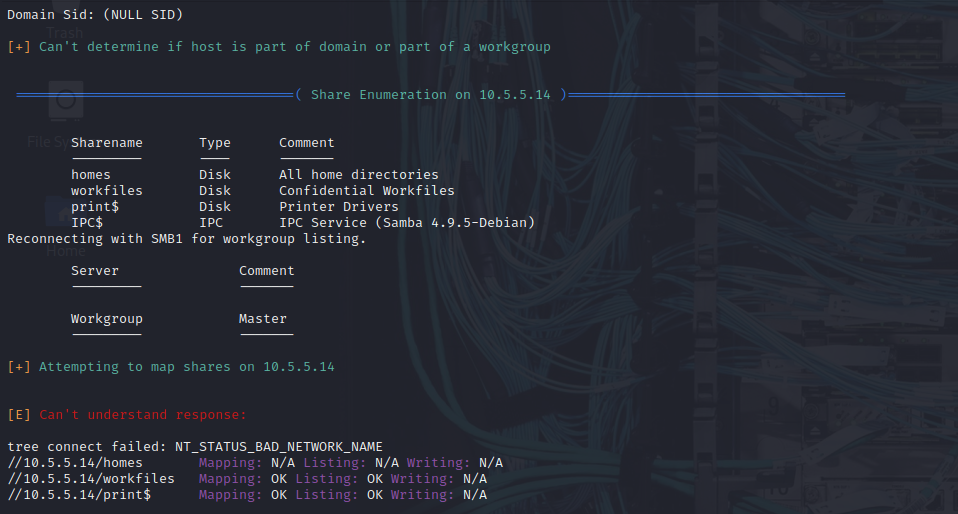
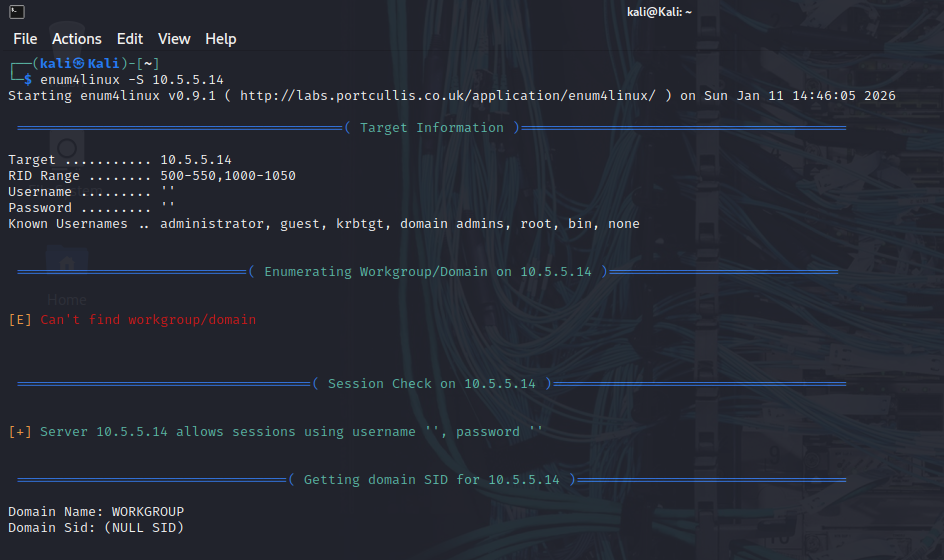
* Scanned the 10.5.5.0/24 network with nmap command **'nmap 10.5.5.0/24'** for hosts with open ports associated with SMB services and found the host 10.5.5.14 with ports 139 and 445 open. These ports are associated with SMB services.

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


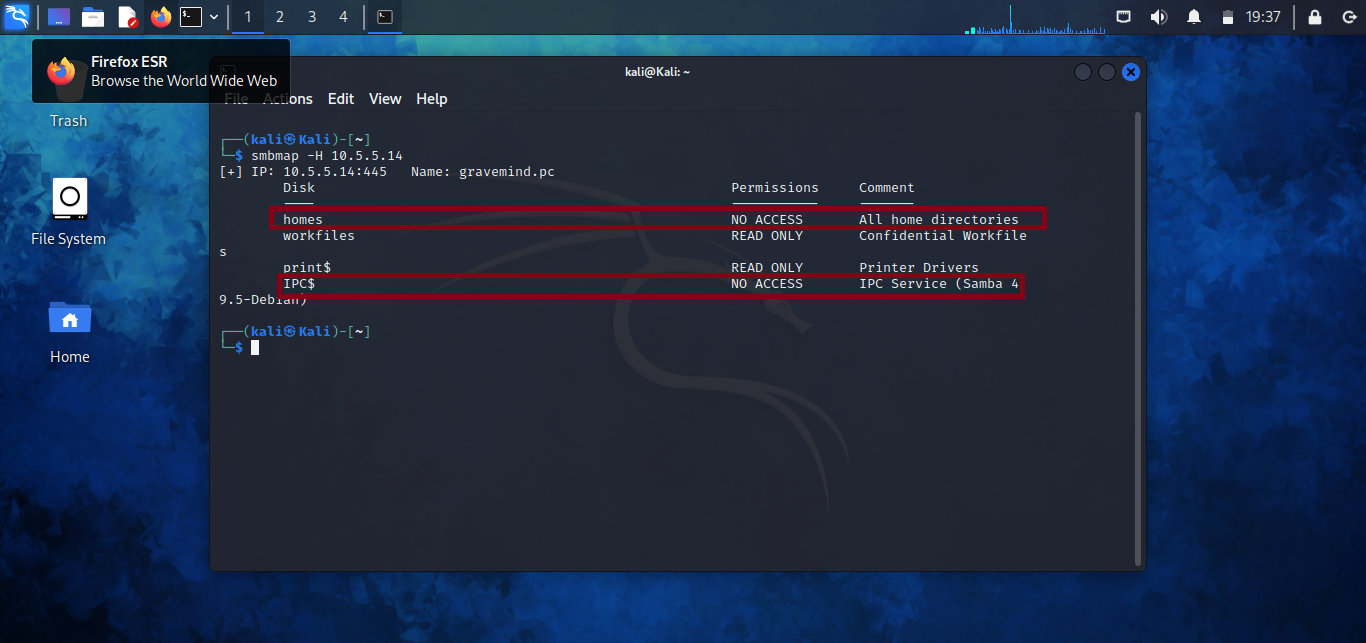
10.5.5.14

**Step 2: Enumerate SMB Shares Accessible by Anonymous Users**

* Enumerated SMB shares on the identified host using enum4linux with the command **enum4linux -S 10.5.5.14**



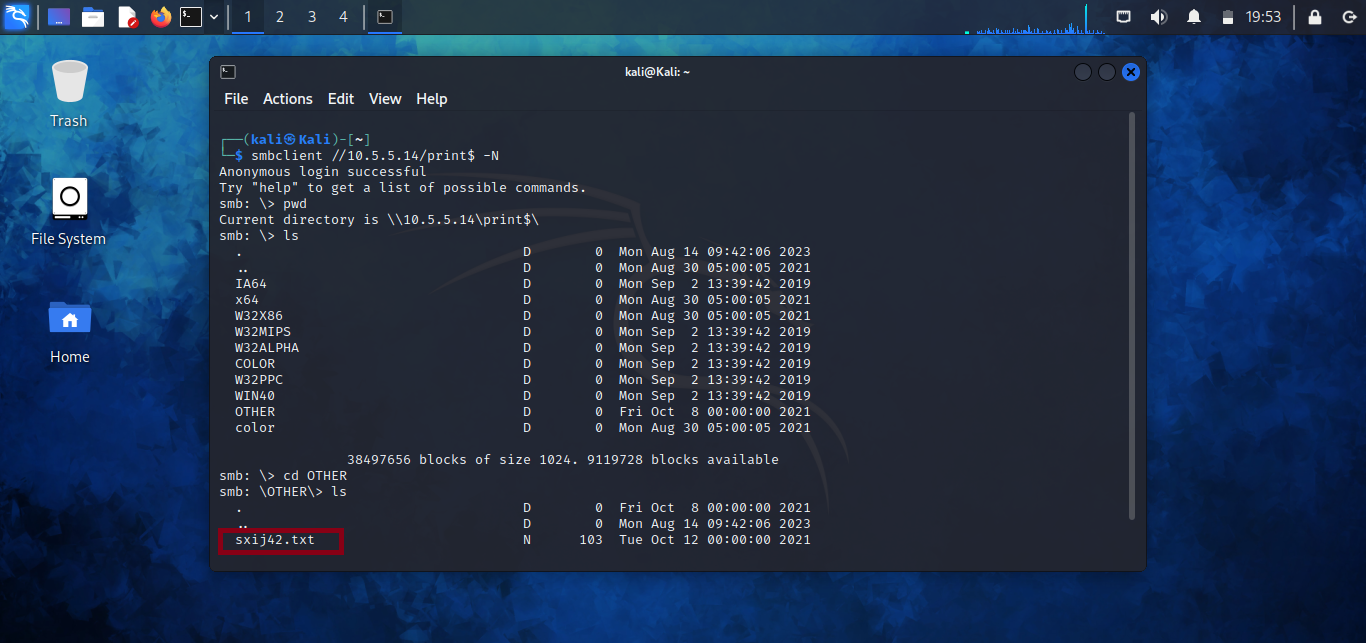
* Determined which shares could be accessed without valid user credentials using the commad smbmap -H 10.5.5.14



**What shares are listed on the SMB server? Which ones are accessible without a valid user login?**  
homes workfiles print$ IPC$

**Step 3: Locate and Retrieve the Challenge 3 File**

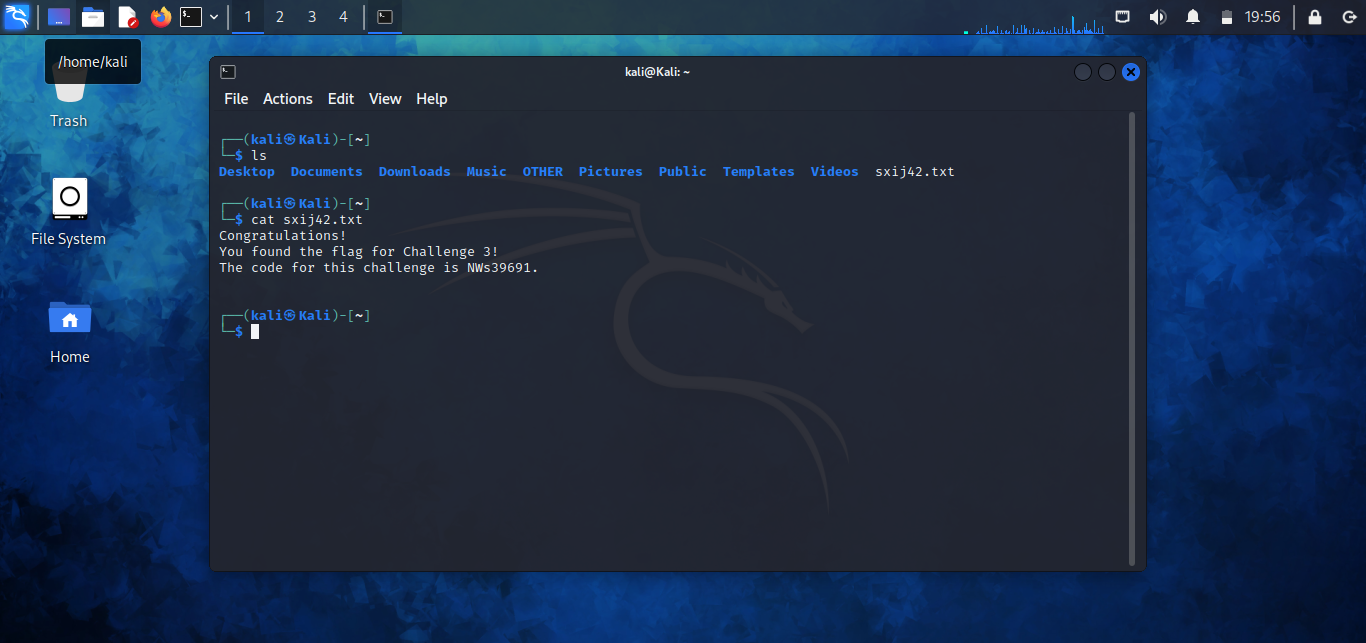
* Accessed the SMB server using an SMB client
* Navigated through shared directories to locate the file containing the Challenge 3 code
* Downloaded and opened the file locally



**In which share is the file found?**  
print$

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

**What is the Challenge 3 code?**  
NWs39691



**Step 4: Research and Propose SMB Attack Remediation**

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

**SMB Attack Remediation**

* **Restrict SMB access through network controls** by limiting exposure to trusted IP ranges only. This can be achieved using firewalls, VLAN segmentation, and disabling SMB access on public-facing interfaces, preventing unauthorized users from connecting to SMB services.
* **Harden SMB authentication and permissions** by disabling anonymous access, enforcing strong passwords, and applying the principle of least privilege to shared resources. Proper user authentication and restricted share permissions reduce the risk of unauthorized access and data leakage.

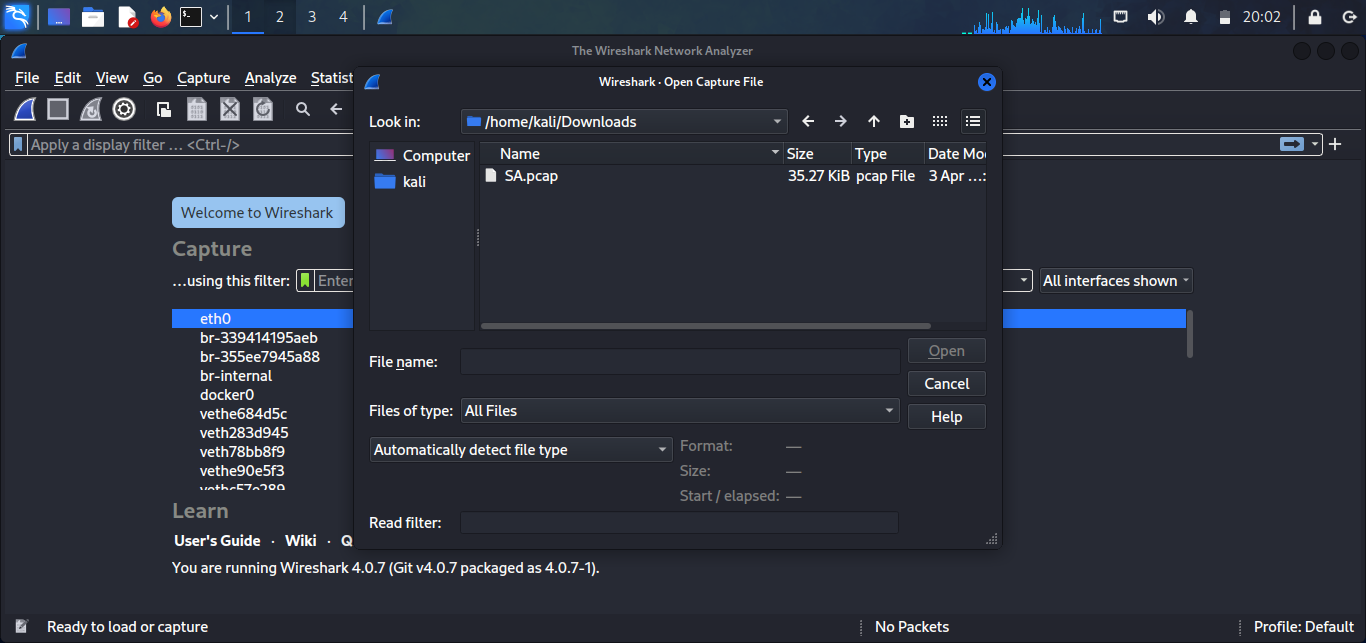
**Challenge 4: Analyze a PCAP File**

**Instructions**

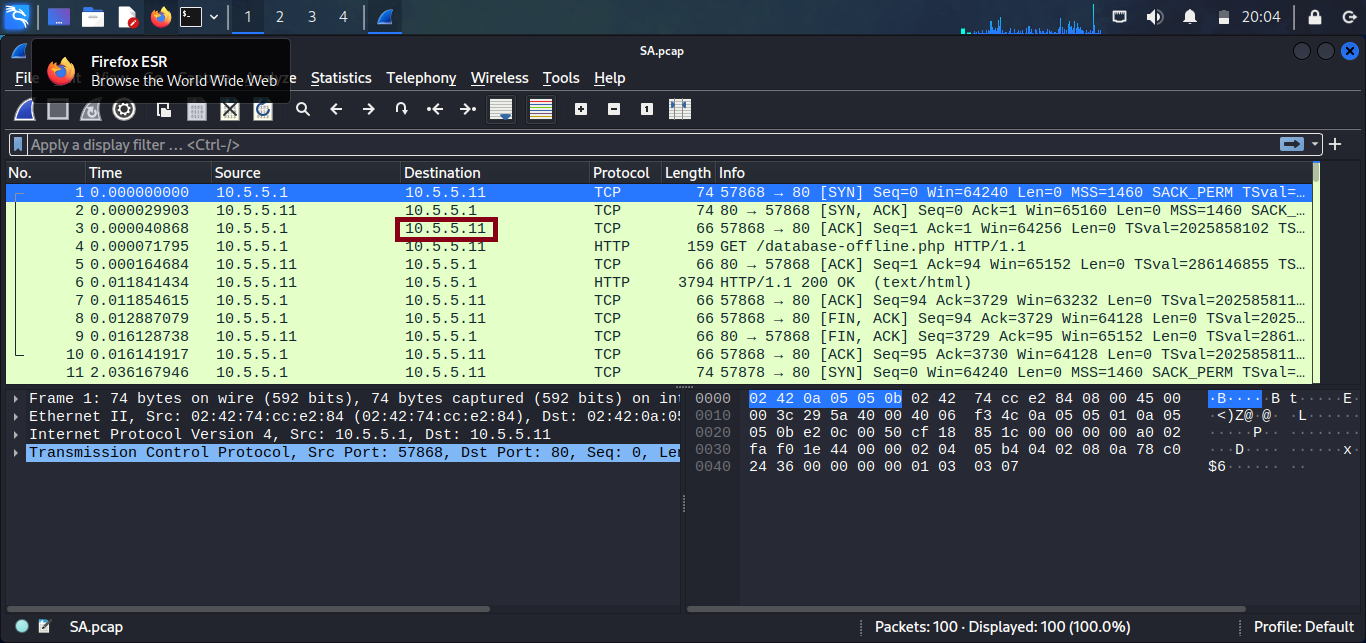
A PCAP file captured during reconnaissance was analyzed to identify sensitive information transmitted in clear text. The Challenge 4 flag was retrieved by inspecting network traffic.

**Step 1: Analyze the PCAP File**

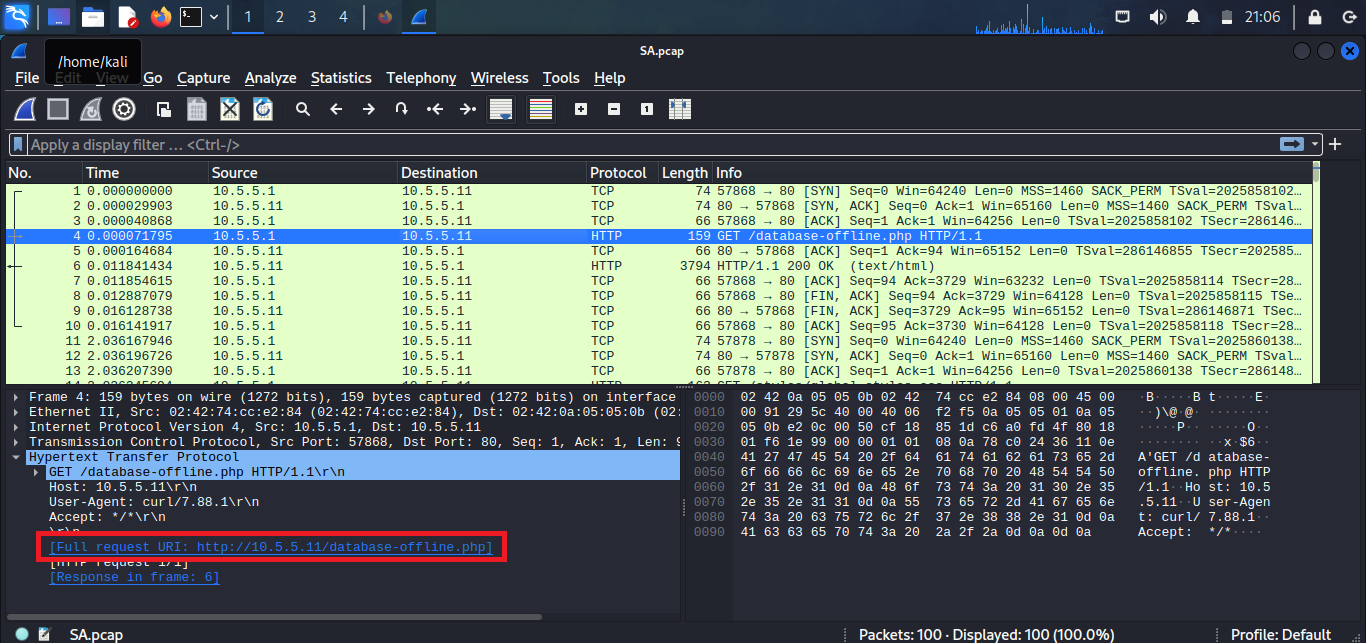
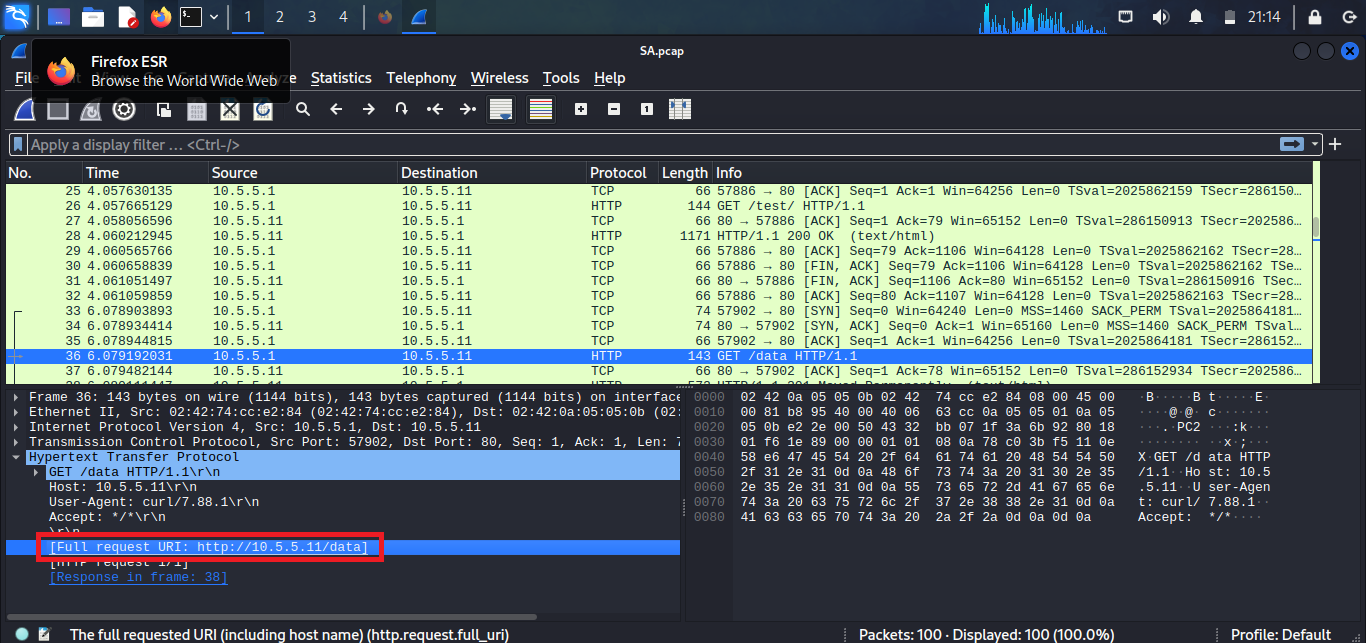
* Opened SA.pcap in Wireshark



* Identified the target IP address as 10.5.5.11 and explored the http packets to identify exposed directories



* Found the paths **10.5.5.11/database-offline.php/, 10.5.5.11/data/ and 10.5.5.11/test/** in the http packets

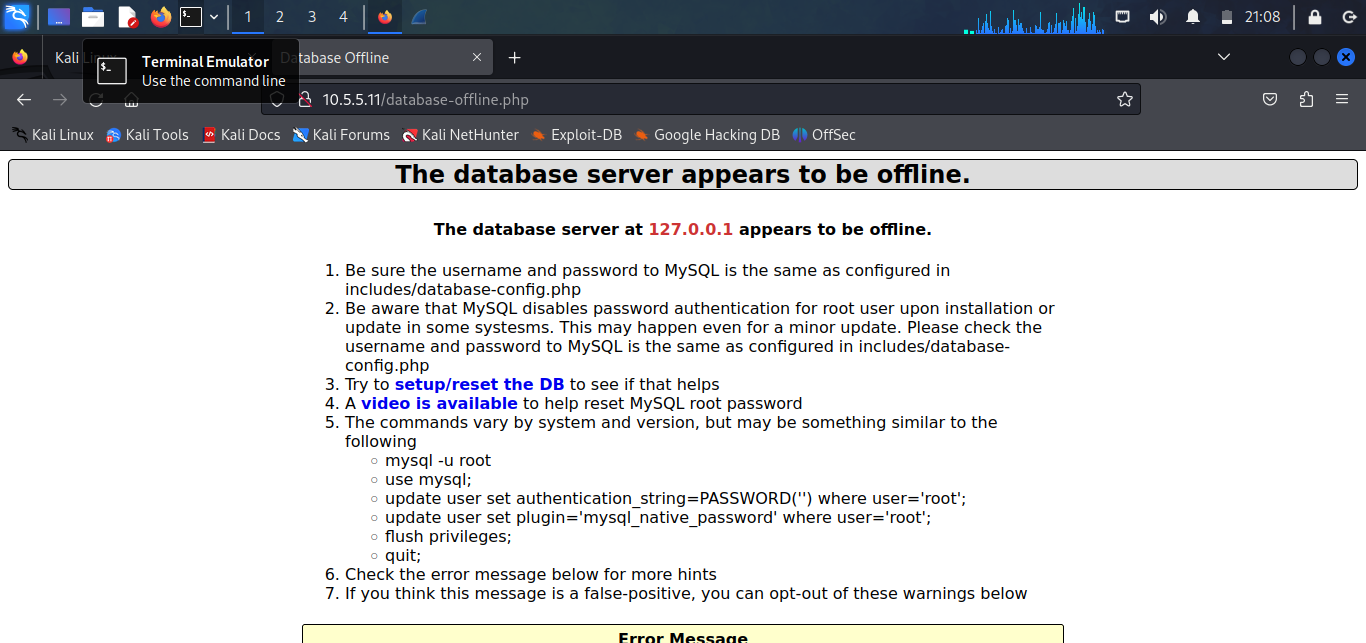
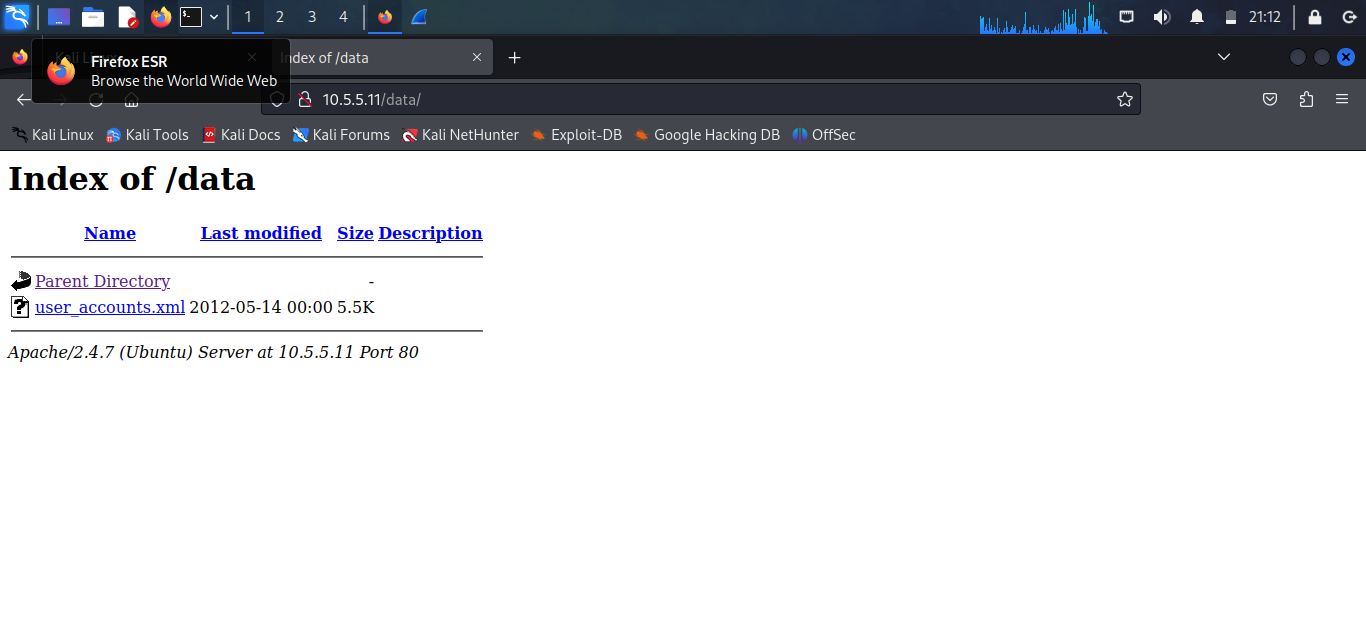
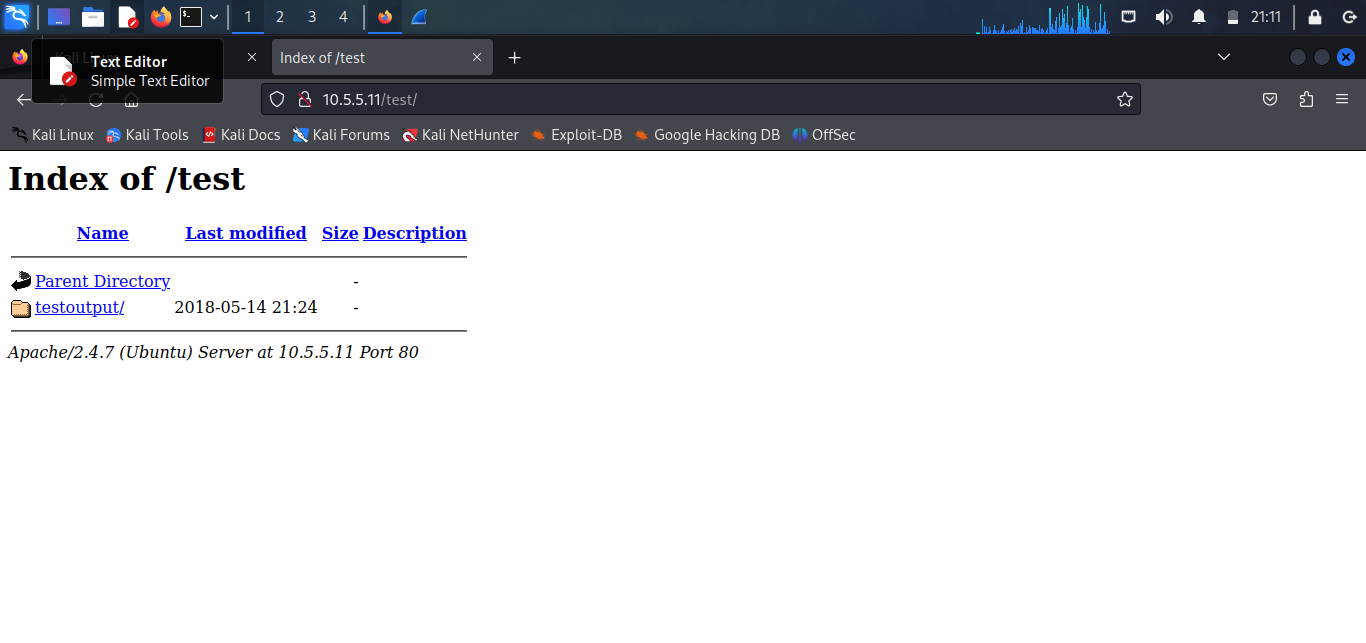
 

**What is the IP address of the target computer?**  
10.5.5.11

**What directories are revealed?**  
10.5.5.11/data, 10.5.5.11/database-offline.php, 10.5.5.11/test

**Step 2: Locate the Challenge 4 File**

* Used a web browser to access discovered URLs

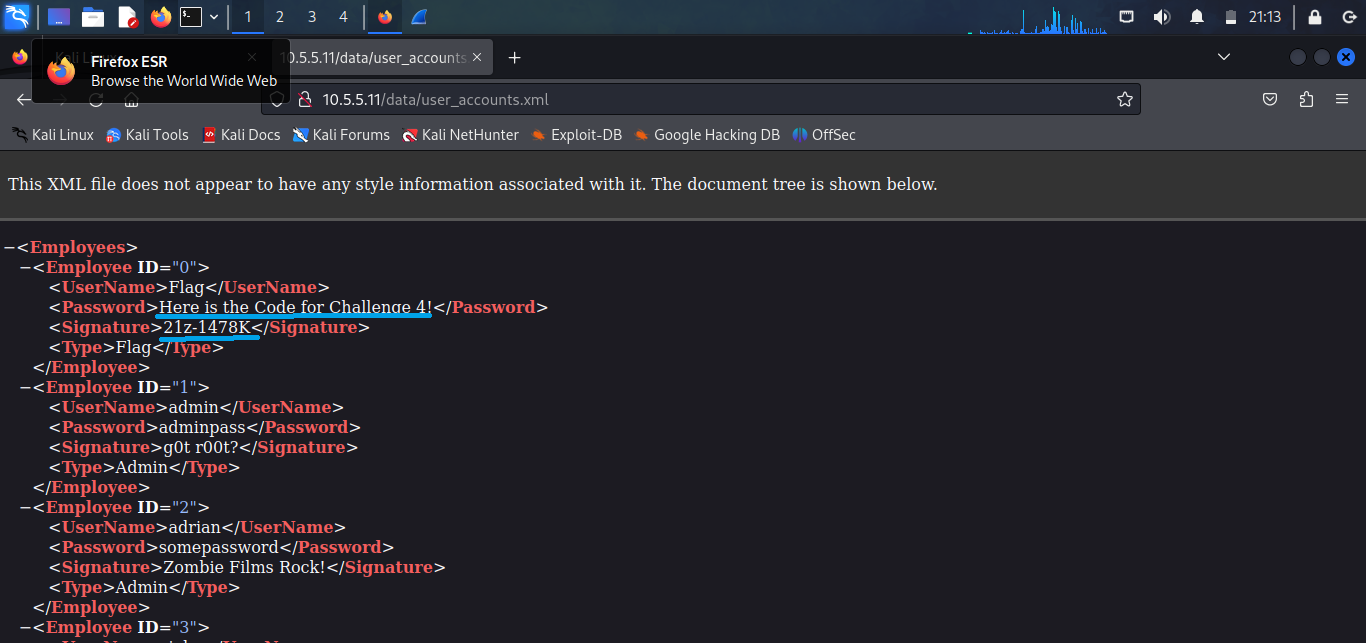
  

* Located and opened the file containing the Challenge 4 code which was in the /data/user\_accounts.xml path

**What is the URL of the file?**  
<http://10.5.5.11/data/user_accounts.xml>

**What is the content of the file?**  
username, password and signatures

**What is the Challenge 4 code?**  
21z-1478K



**Step 3: Research and Propose Remediation**

**What are two methods to prevent file content from being transmitted in clear text?**

**Clear-Text Data Transmission Remediation**

* **Encrypt data in transit using secure communication protocols** such as HTTPS (TLS), SFTP, FTPS, or SMB signing and encryption. Encryption ensures that file contents cannot be read or altered by attackers intercepting network traffic.
* **Disable or replace insecure protocols that transmit data in clear text**, including FTP, HTTP, Telnet, and older SMB versions. Replacing them with encrypted alternatives prevents sensitive file content from being exposed during transmission.