Challenge 4

Target: 10.5.5.11

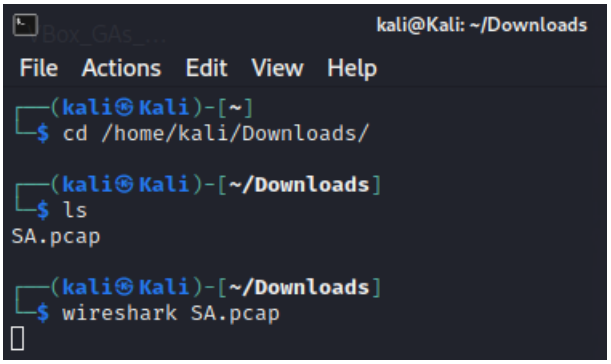
Vulnerability: Clear-Text Data Transmission & Information Disclosure

1. Executive Summary

During the reconnaissance phase, a network traffic capture file (`SA.pcap`) was analyzed to identify communications between a client and a web server. The analysis revealed that the server was transmitting data over unencrypted HTTP, allowing for the discovery of sensitive directories and the retrieval of a protected challenge code.

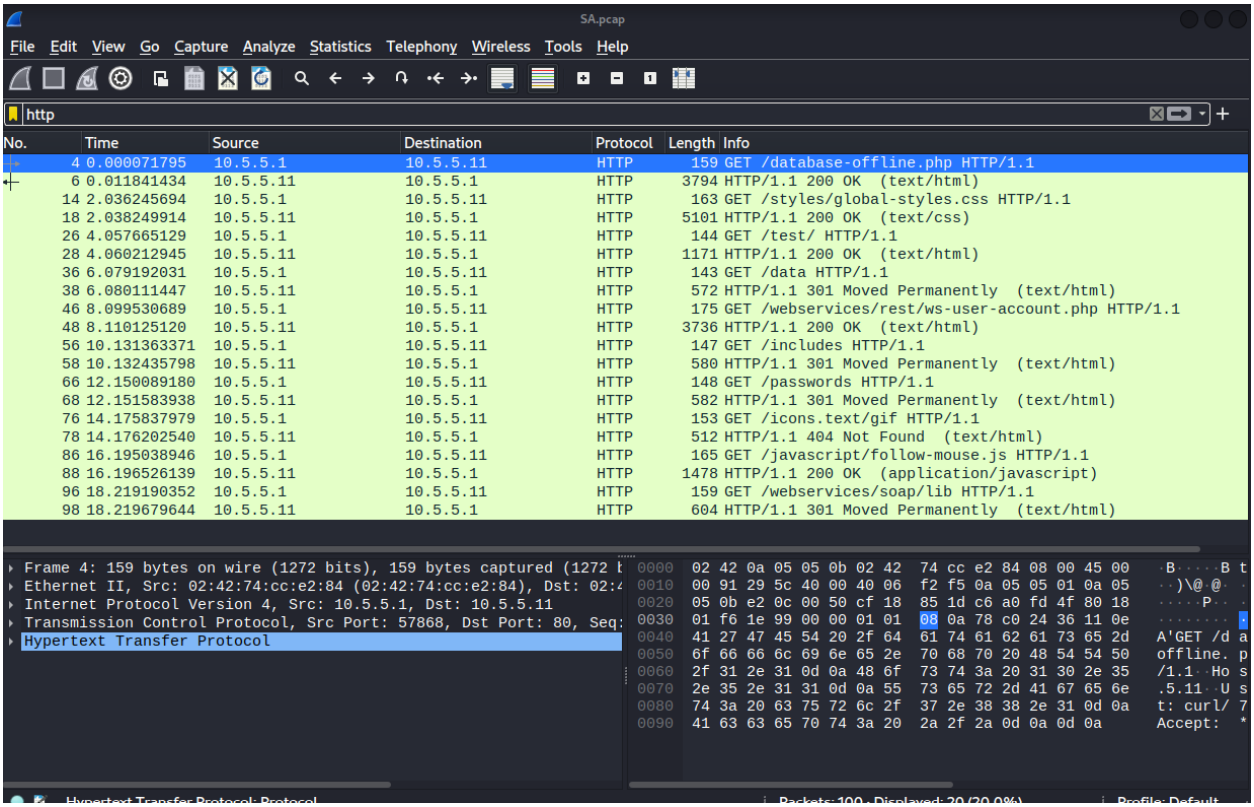
2. Packet Analysis (Wireshark)

The file `SA.pcap` was analyzed using Wireshark with an HTTP display filter. This revealed the internal structure of the web server at **10.5.5.11**.



Evidence Found:

- **Target IP:** 10.5.5.11
- **Source IP:** 10.5.5.1
- **Protocol:** HTTP (TCP Port 80)
- **Revealed Directories:** * `/data/`
    - `/passwords/`
    - `/test/`
    - `/includes/`



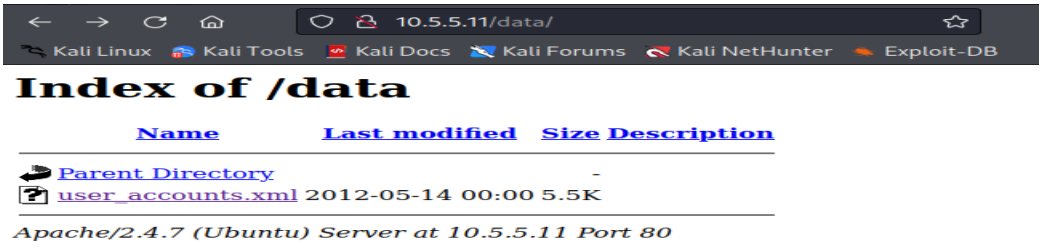
3. Exploitation (Data Retrieval)

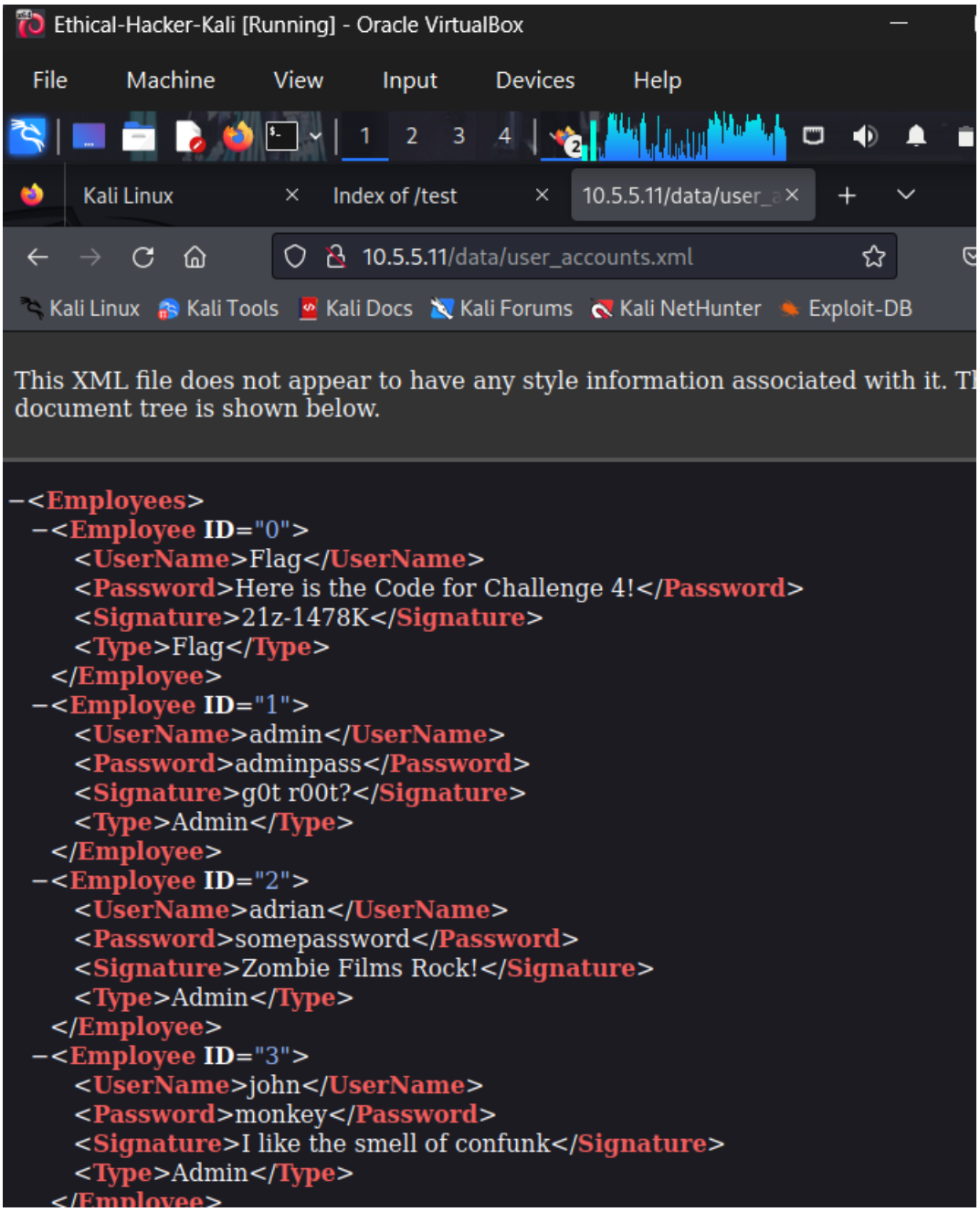
By using a web browser to navigate to the directories discovered in the traffic capture, the following sensitive file was located:

- **Final URL:** `http://10.5.5.11/data/user_accounts.xml`
- **File Content:** employees username, password, signature
- **Challenge 4 Code:** 21z-1478K

Proof of Concept:

The web browser successfully displayed the directory index, confirming that the server does not restrict directory browsing and transmits file contents in clear text.





4. Remediation Recommendations

To prevent attackers from sniffing network traffic to find sensitive information, the following remediation steps are required:

1: Implement Transport Layer Security (HTTPS)

The web server should be configured to use **HTTPS (TLS/SSL)**.

- **Effect:** This encrypts the entire communication session. Even if an attacker captures the packets, the URLs, directory names, and file contents will be unreadable "ciphertext."

2: Disable Directory Indexing

Configure the web server to prevent the listing of files within directories.

- **Effect:** If an attacker discovers a directory name (like `/passwords/`), the server will return a "403 Forbidden" error instead of a list of files, unless the attacker knows the exact filename.