PLAINTEXT HTTP TRAFFIC ANALYSIS REPORT

Analyst: Precious Anyanwu
Date: *26/01/2026*
Case ID: NET-HTTP-001

---

1. Case Summary

This lab exercise demonstrates how HTTP traffic is transmitted in plaintext and can be intercepted and read using packet capture tools. The objective was to illustrate the security risk of unencrypted protocols by observing client-server communication over port 80.

Traffic was generated locally and captured to analyze packet contents and visibility of transmitted data.

---

2. Lab Environment

Component	Description
OS	Kali Linux
Capture Tool	tcpdump
Server Tool	Netcat (nc)
Client Tool	Netcat (nc)
Network Interface	Loopback (127.0.0.1)
Protocol Observed	HTTP (Port 80)

---

3. Tools Used

- **tcpdump** – Network packet capture
- **Netcat (nc)** – Used to simulate client-server communication

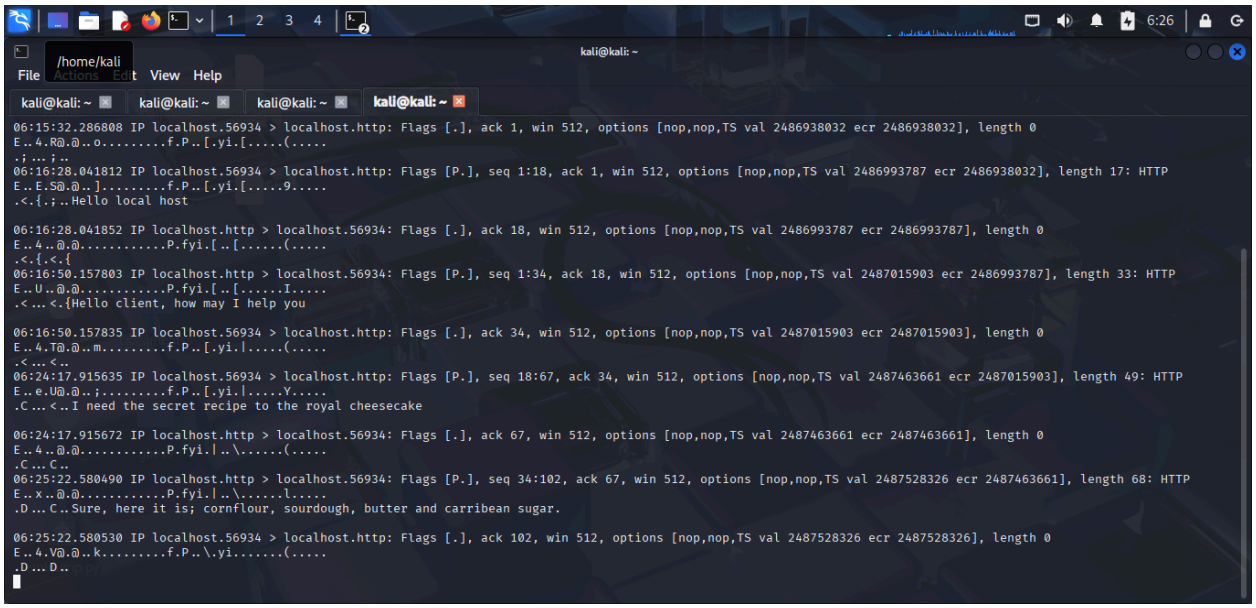
---

4. Packet Capture Setup

Traffic capture was started on the loopback interface:

```
sudo tcpdump -i lo -A
```

The `-A` option displays packet contents in readable ASCII format. This allows direct observation of transmitted data without encryption.



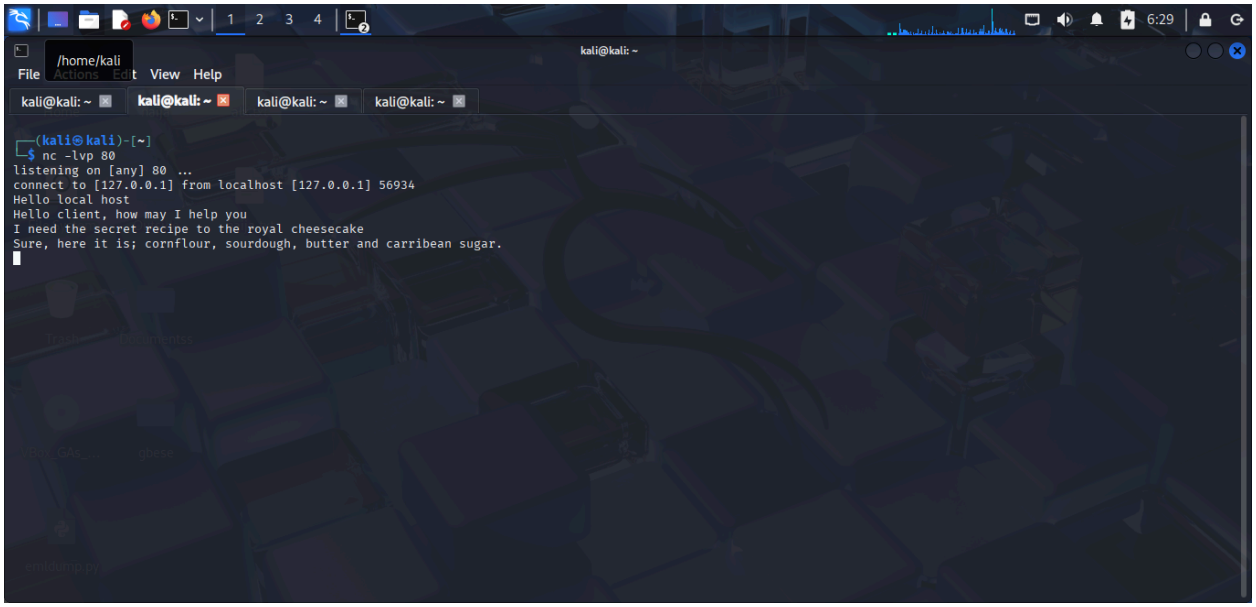
---

5. Server Configuration

A local server was created to listen for incoming traffic on port 80:

```
nc -lvp 80
```

This configured the system to act as a basic server waiting for client connections.



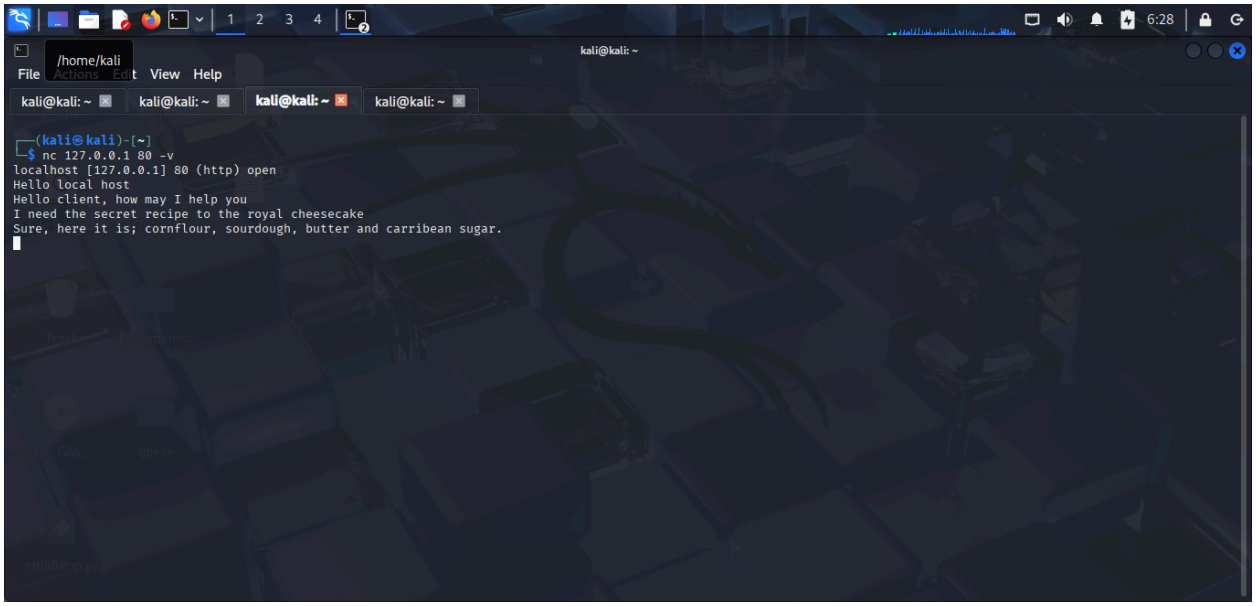
---

6. Client Connection

A client connection was initiated to communicate with the server:

```
nc 127.0.0.1 80 -v
```

This established communication between the client and server, generating observable network traffic.



---

7. Key Observation — Plaintext Transmission

The captured packets revealed that:

- Data transmitted over HTTP appeared in readable text
- Packet contents were visible in ASCII format
- No encryption or obfuscation was applied

This confirms that HTTP transmits data in plaintext.

---

8. Security Implications

Because HTTP traffic is unencrypted:

- Sensitive data can be intercepted
- Credentials and session data may be exposed
- Attackers on the same network can monitor communication

This demonstrates why HTTPS (HTTP over TLS) is required to secure data in transit.

---

9. Conclusion

This lab provided practical evidence that HTTP traffic is not secure due to lack of encryption. Observing plaintext packets reinforces the importance of using secure protocols in modern network environments.

Understanding protocol security weaknesses is essential for SOC analysts and network security professionals responsible for monitoring and protecting organizational traffic.