Capturing HTTP Credentials using Wireshark

Environment: Kali Linux (Attacker), Windows Server (Victim)

Tools: Wireshark, Browser, ping

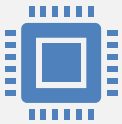
Author: Adarshvardhan singh

Date: 26-07-2025

Objective

- Demonstrate how unencrypted HTTP login credentials can be captured over the network.

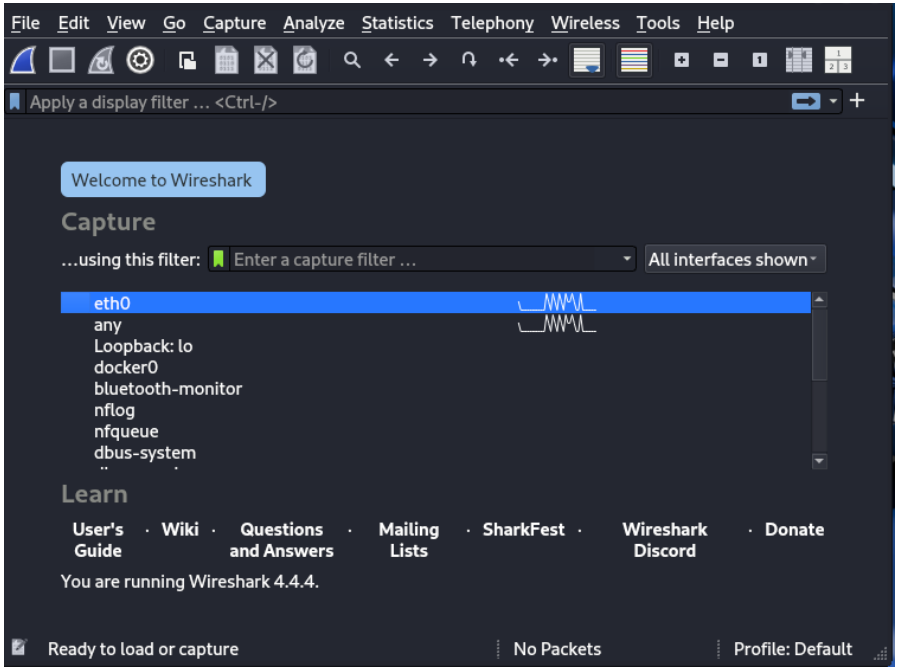
- Use Wireshark on Kali Linux to monitor traffic from a Windows machine.



- Analyze packets to retrieve sensitive data like usernames and passwords.

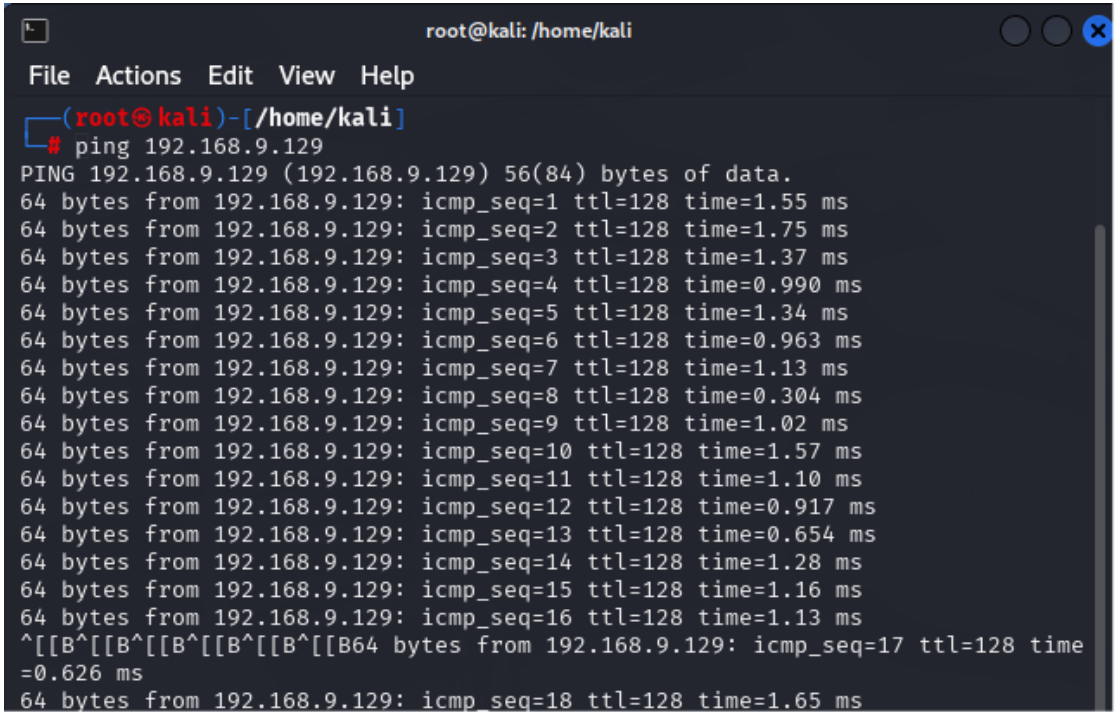
Starting Wireshark

- - Launch Wireshark with `sudo wireshark`.
- - Select the `eth0` interface to capture packets.



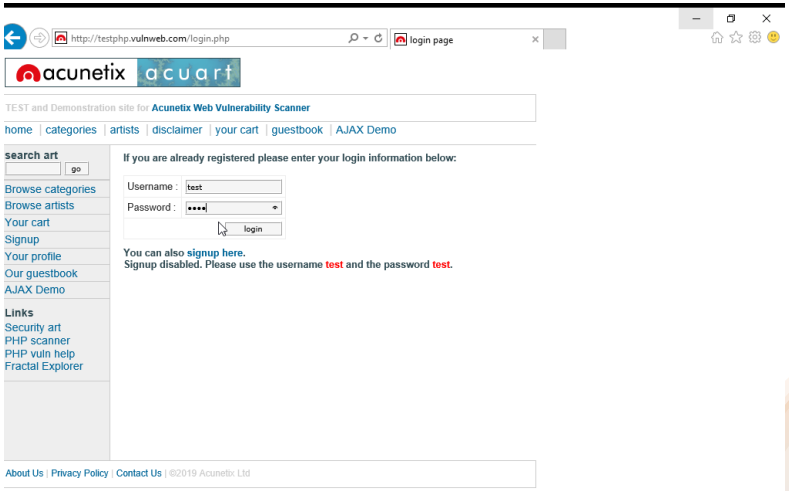
Confirming Target is Live

- - Use `ping 192.168.9.129` to verify the Windows machine is active.
- - Replies confirm it's reachable for packet sniffing.



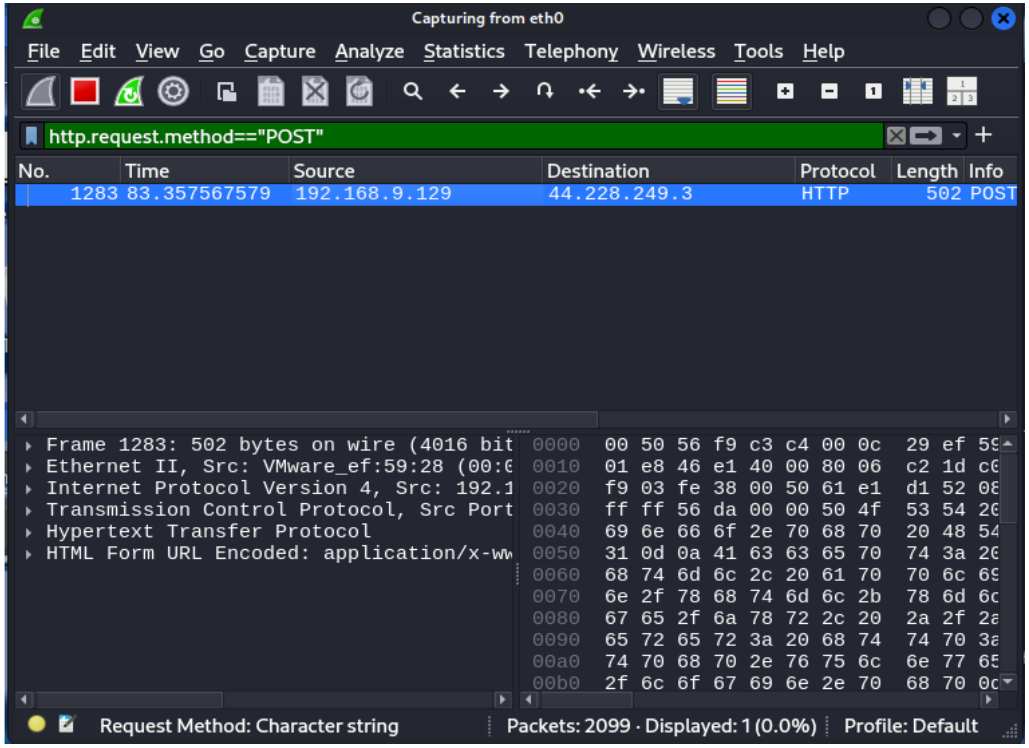
Target Accesses Vulnerable Web Page

- - Victim logs into `http://testphp.vulnweb.com`.
- - Credentials: Username = test,
- Password = test
- - Site uses HTTP (insecure).



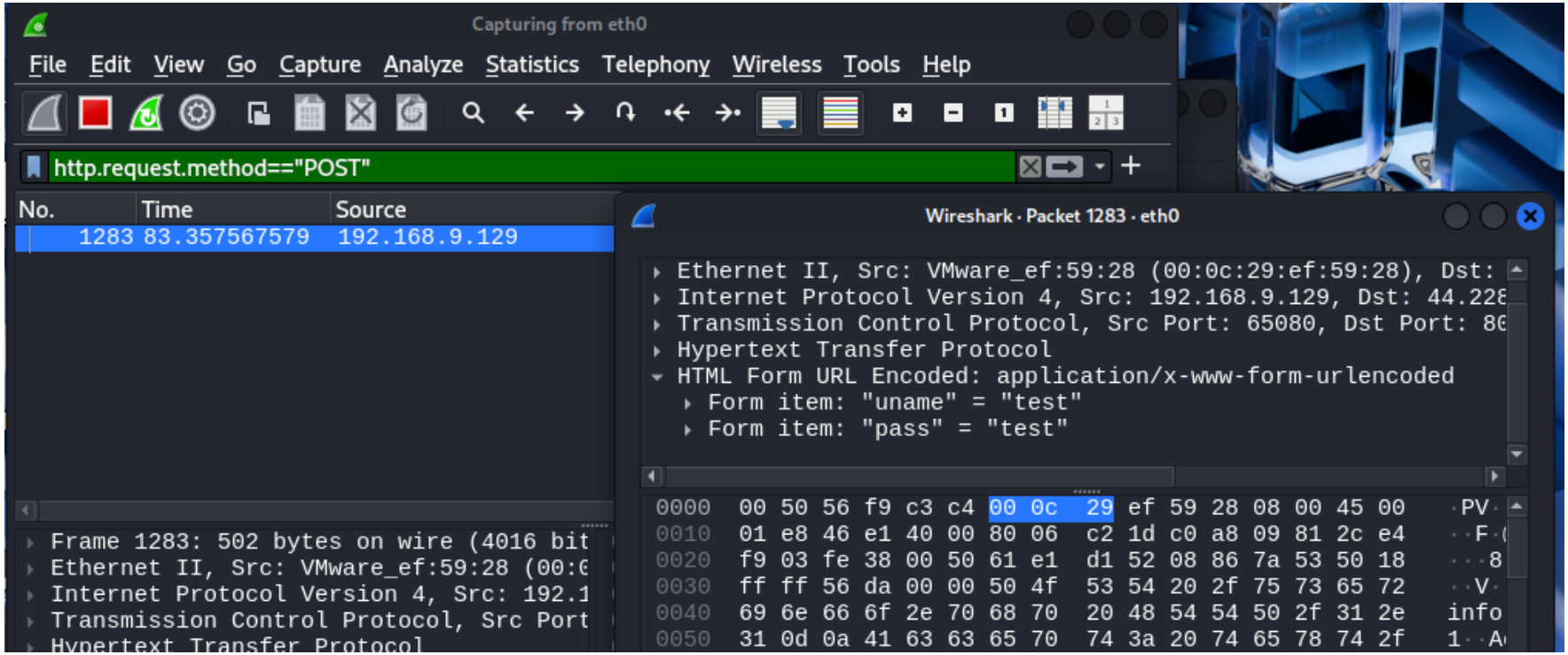
Capture HTTP POST Packet

- - Apply Wireshark filter:
- `http.request.method == "POST"`
- - Observe traffic from 192.168.9.129 to 44.228.249.3



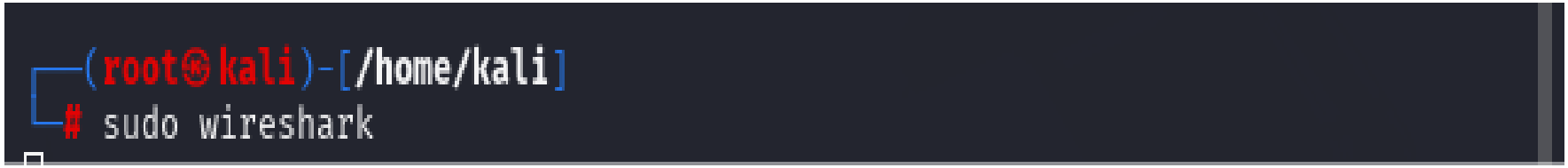
Analyze Packet Details

- - Packet reveals: `uname=test&pass=test`
- - Confirms credentials sent in plain text (insecure HTTP).



Wireshark Launch Command

- Command used to start Wireshark with root privileges:
- sudo wireshark



Conclusion & Recommendation

- - Captured credentials show the danger of unencrypted HTTP login forms.
- - Recommendations:
- • Use HTTPS to secure communications.
- • Avoid logging into sensitive accounts on insecure networks.
- • Monitor internal traffic for potential data leaks.