

# **Capturing HTTP Credentials using Wireshark**



**Model Institute of Engineering & Technology (Autonomous) Permanently  
Affiliated to the University of Jammu Accredited by NAAC with “A” Grade  
Jammu, India 2025**

# Capturing HTTP Credentials using Wireshark



---

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

Tools: Wireshark, Browser, ping

Author: Shavita Raina

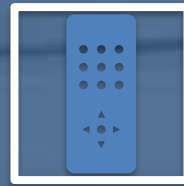
Date: 26-07-2025

# Objective



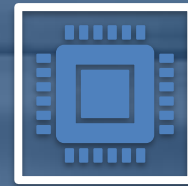
## Demonstrate

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



## Use

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

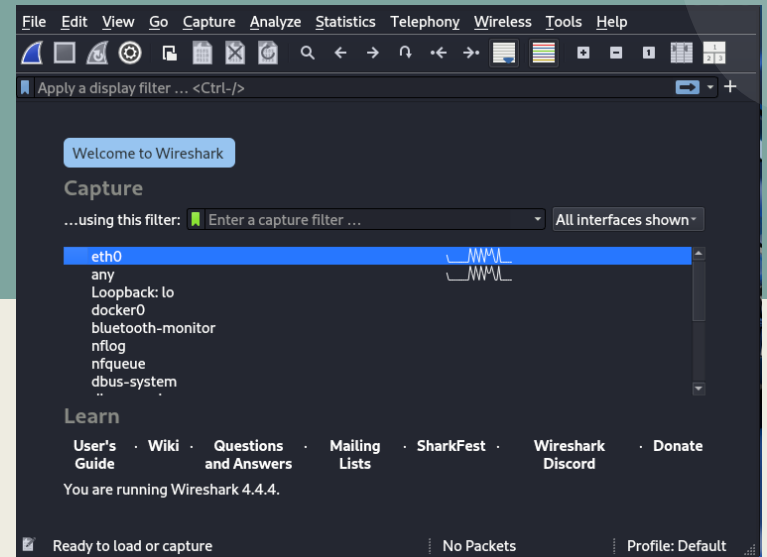


## Analyze

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

# Starting Wireshark

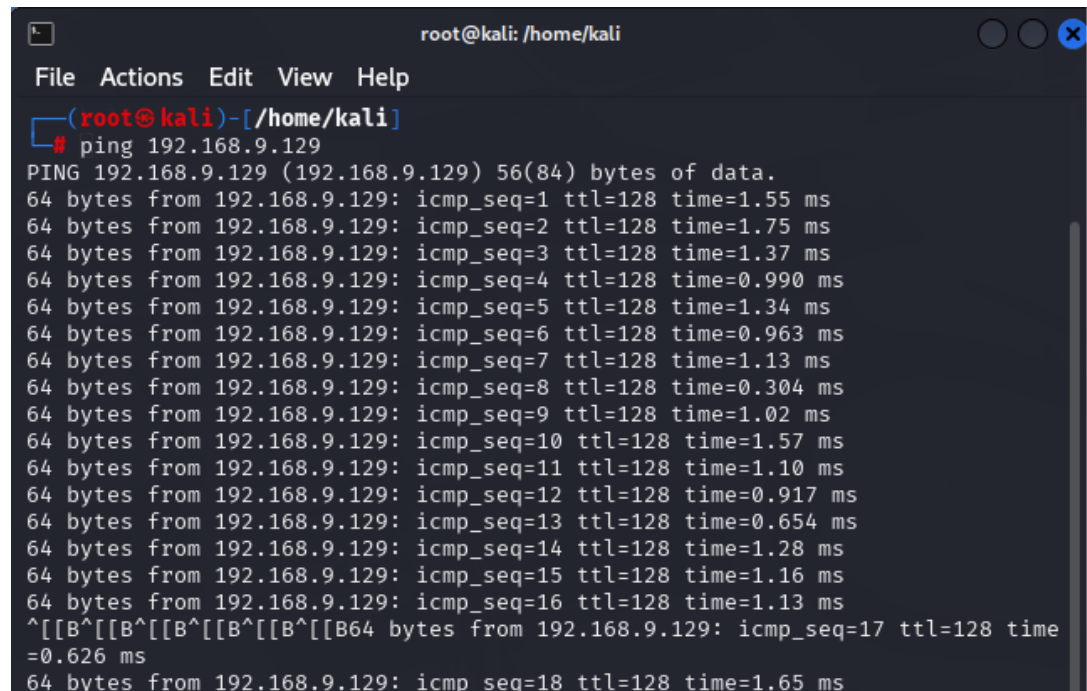
- - Launch Wireshark with `sudo wireshark`.
- - Select the `eth0` interface to capture packets.



# Confirming Target is Live

---

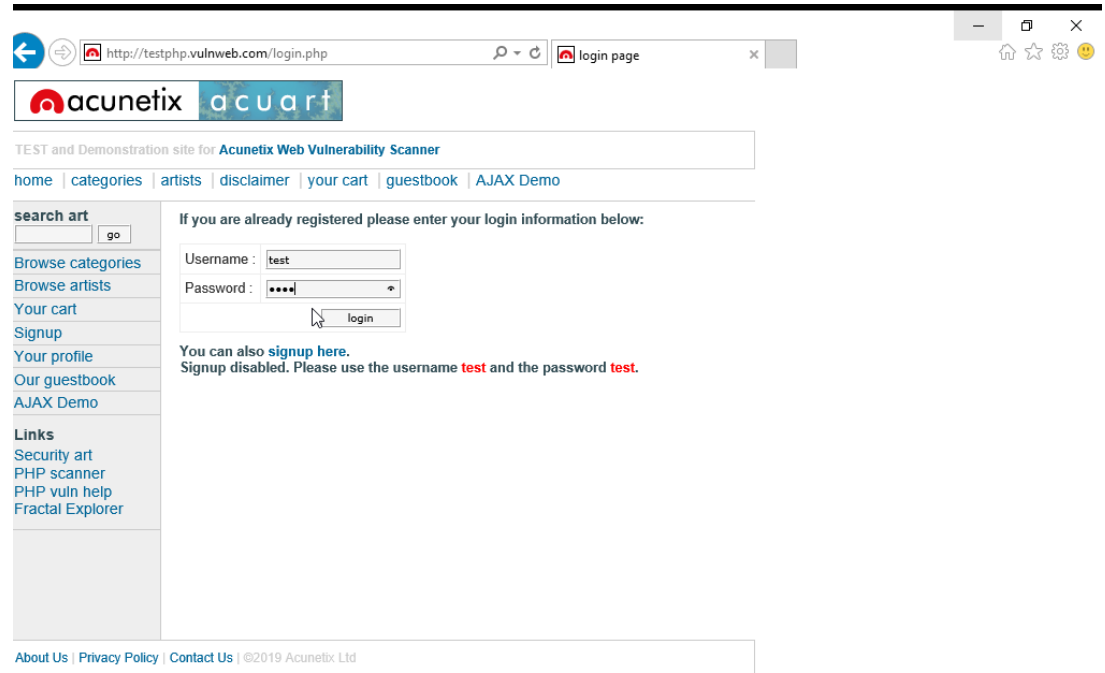
- - Use `ping 192.168.9.129` to verify the Windows machine is active.
- - Replies confirm it's reachable for packet sniffing.



```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# ping 192.168.9.129
PING 192.168.9.129 (192.168.9.129) 56(84) bytes of data.
64 bytes from 192.168.9.129: icmp_seq=1 ttl=128 time=1.55 ms
64 bytes from 192.168.9.129: icmp_seq=2 ttl=128 time=1.75 ms
64 bytes from 192.168.9.129: icmp_seq=3 ttl=128 time=1.37 ms
64 bytes from 192.168.9.129: icmp_seq=4 ttl=128 time=0.990 ms
64 bytes from 192.168.9.129: icmp_seq=5 ttl=128 time=1.34 ms
64 bytes from 192.168.9.129: icmp_seq=6 ttl=128 time=0.963 ms
64 bytes from 192.168.9.129: icmp_seq=7 ttl=128 time=1.13 ms
64 bytes from 192.168.9.129: icmp_seq=8 ttl=128 time=0.304 ms
64 bytes from 192.168.9.129: icmp_seq=9 ttl=128 time=1.02 ms
64 bytes from 192.168.9.129: icmp_seq=10 ttl=128 time=1.57 ms
64 bytes from 192.168.9.129: icmp_seq=11 ttl=128 time=1.10 ms
64 bytes from 192.168.9.129: icmp_seq=12 ttl=128 time=0.917 ms
64 bytes from 192.168.9.129: icmp_seq=13 ttl=128 time=0.654 ms
64 bytes from 192.168.9.129: icmp_seq=14 ttl=128 time=1.28 ms
64 bytes from 192.168.9.129: icmp_seq=15 ttl=128 time=1.16 ms
64 bytes from 192.168.9.129: icmp_seq=16 ttl=128 time=1.13 ms
^[[B^[[B^[[B^[[B^[[B64 bytes from 192.168.9.129: icmp_seq=17 ttl=128 time
=0.626 ms
64 bytes from 192.168.9.129: icmp seq=18 ttl=128 time=1.65 ms
```

# Target Accesses Vulnerable Web Page

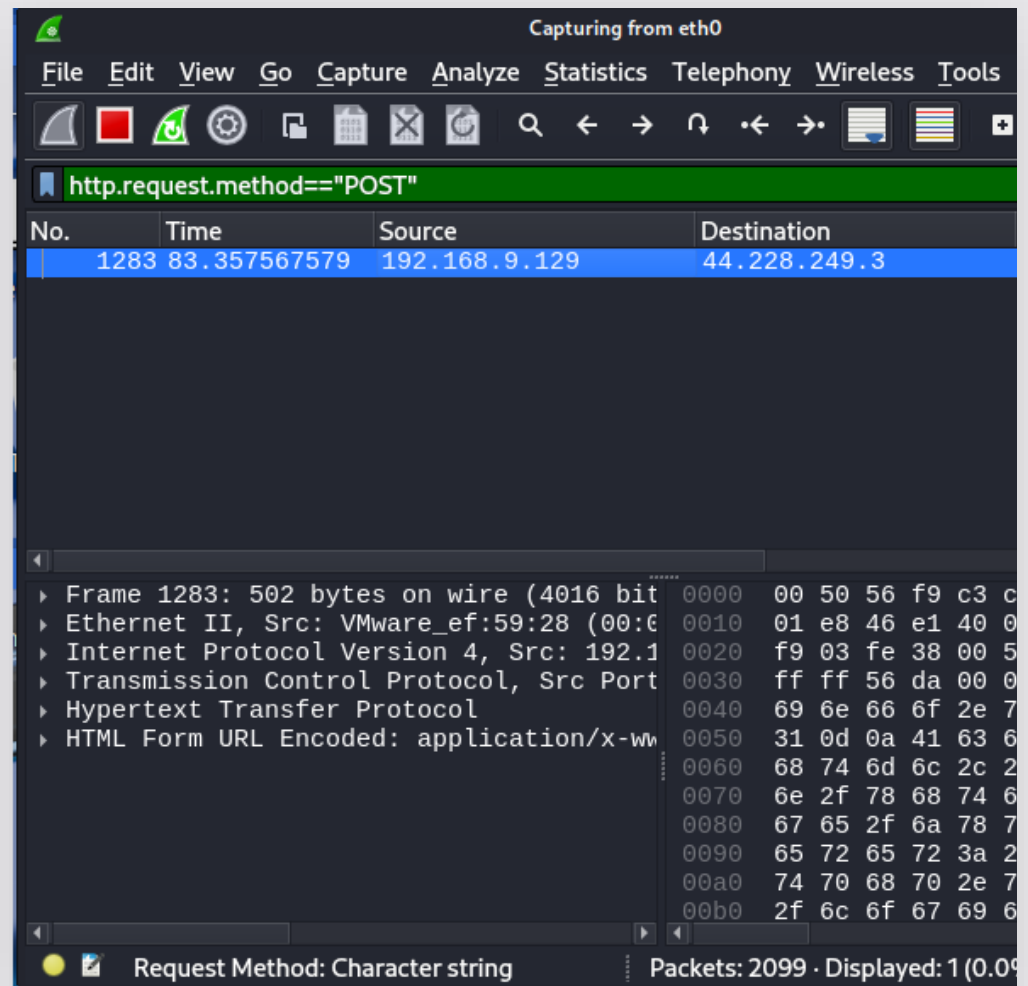
- - Victim logs into `http://testphp.vulnweb.com`.
- - Credentials:  
Username = test,
- Password = test
- - Site uses HTTP (insecure).



The screenshot shows a web browser window with the address bar displaying `http://testphp.vulnweb.com/login.php`. The page features the Acunetix logo and a navigation menu with links: [home](#), [categories](#), [artists](#), [disclaimer](#), [your cart](#), [guestbook](#), and [AJAX Demo](#). On the left, there is a sidebar with a search bar and a 'go' button, followed by links: [Browse categories](#), [Browse artists](#), [Your cart](#), [Signup](#), [Your profile](#), [Our guestbook](#), and [AJAX Demo](#). Below these are 'Links' to [Security art](#), [PHP scanner](#), [PHP vuln help](#), and [Fractal Explorer](#). The main content area has a heading 'If you are already registered please enter your login information below:' and a login form with fields for 'Username' (containing 'test') and 'Password' (containing masked characters '\*\*\*\*'). A 'login' button is positioned below the password field. Below the form, a message states: 'You can also [signup here](#). Signup disabled. Please use the username **test** and the password **test**.' The footer contains links for [About Us](#), [Privacy Policy](#), and [Contact Us](#), along with the copyright notice '©2019 Acunetix Ltd'.

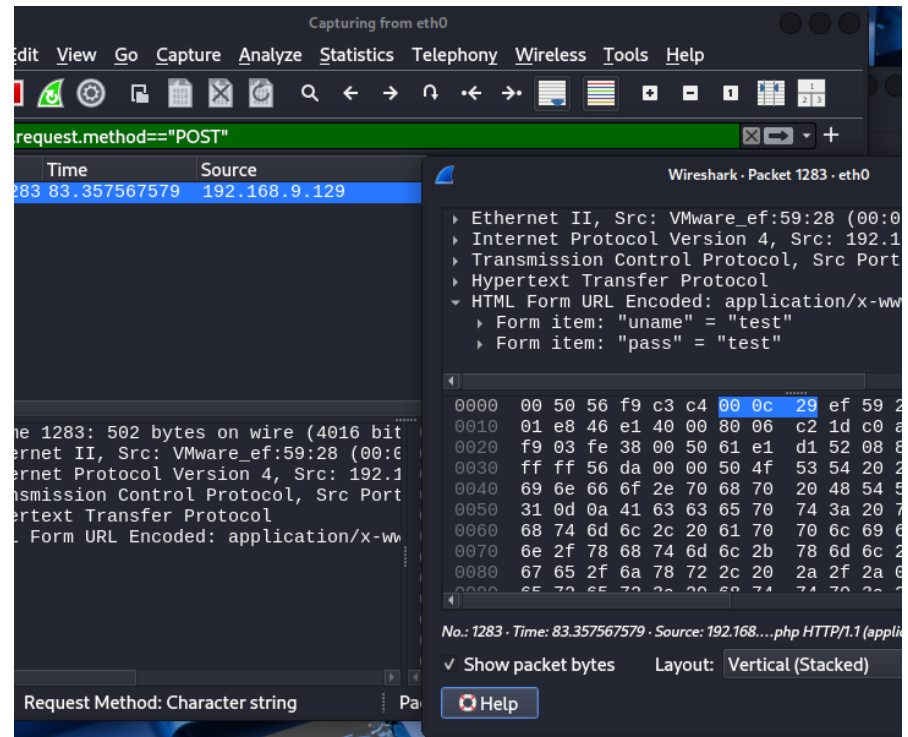
## Capture HTTP POST Packet

- - 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`

```
(root@kali)-[/home/kali]  
# 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.

