MITM Attack Using Ettercap and Wireshark (Lab Setup)

1. On the attacker machine, open Ettercap.
2. Select the network interface based on your OS environment (e.g., eth0, wlan0).
3. After setting the interface, click on the Accept icon.
4. Scan the IP addresses connected to the internet.
5. Once scanning is complete, it will display a message like '16 hosts added to the host list.'
6. Click on the Host List icon (located near the search icon).
7. In the host list, set the victim's IP address as Target 1 and the router's IP address as Target 2.
8. After setting the targets, click on the Menu icon.
9. Under the list of attacks, choose ARP Poisoning.
10. After starting ARP poisoning, open Wireshark for packet analysis.
11. Select the same network interface (e.g., eth0) in Wireshark.
12. Now packets will start appearing in Wireshark.
13. While packet analysis is ongoing, go to the victim system and open a browser.
14. Visit http://www.vulnweb.com.
15. Click on the second link on the page (as shown in your reference image).
16. Once the page opens, click on Sign Up.
17. Enter a username and password, then submit the form.
18. Go back to the attacker machine and search in Wireshark using the filter:

    http.request.method == "POST"
19. Click the matching packet from the list.
20. Click the arrow icon to expand the details.
21. Look under the HTML Form URL section to see the captured username and password.