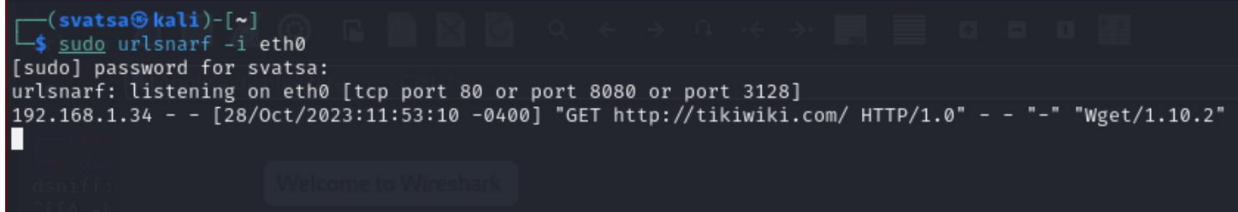


Assignment 9 – Packet Sniffing

CYSE 450 Ethical Hacking and Penetration Testing

Task: Performing an ARP Spoofing Attack

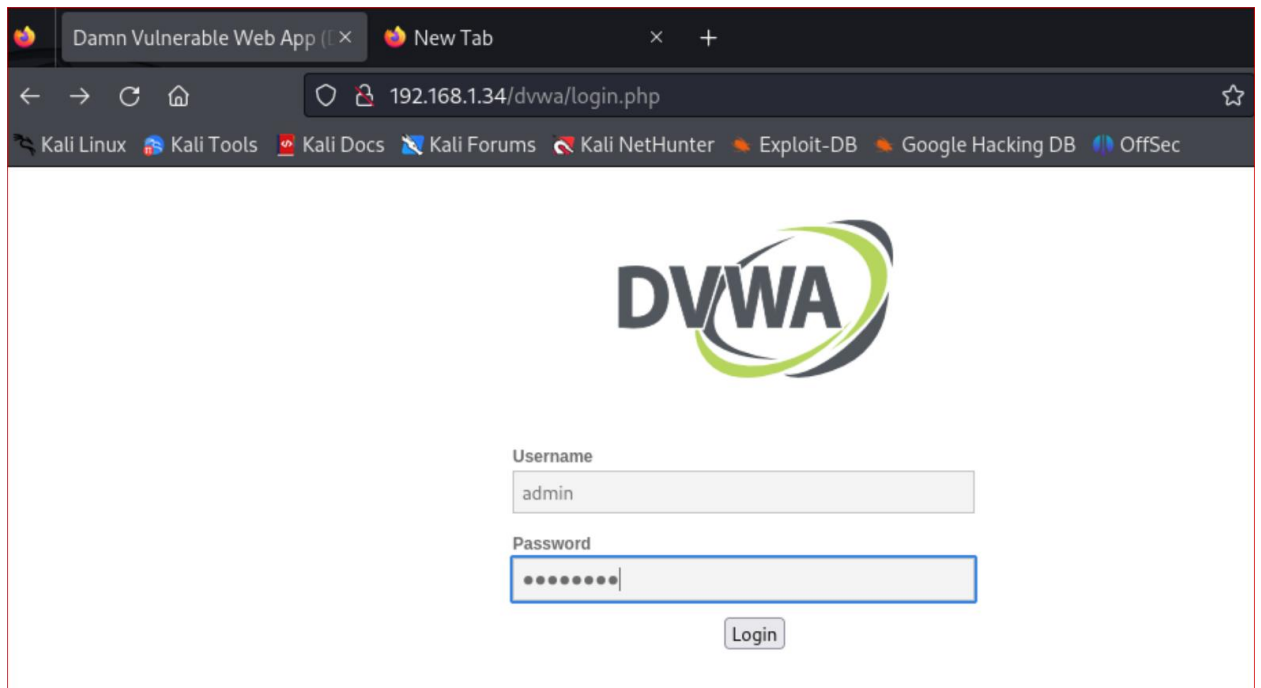
1. Power on and login to Kali Linux and Metasploitable2 (Target Machine) [NOTE: You can choose windows XP/7 as an alternative for metasploitable2, if you want]
2. Open a root terminal on the Kali Linux virtual machine and discover the IP addresses of the other machines on the network to spoof them (that is, pretend to be them) using **netdiscover** tool/command.
3. You need to allow the Kali Linux machine to forward packets on behalf of other machines by enabling IP forwarding. Make sure that you're a root user on Kali Linux, and then enable IP forwarding by setting the IP forwarding flag.
4. Generate multiple fake ARP replies by running the following command (in root terminal):
arpspoof -i eth0 -t IP-address_of_Victim IP address of-Gateway
5. Also trick the router into believing you are the victim so that you can intercept incoming internet traffic on the victim's behalf. Open a new root terminal and run the command that follows:
arpspoof -i eth0 -t IP address of-Gateway IP-address_of_Victim
6. Check the Arp table in the target Machine. Did you notice any changes in the MAC address for the gateway?
7. In another terminal in Kali VM, type the following command to Extract the URLs running.



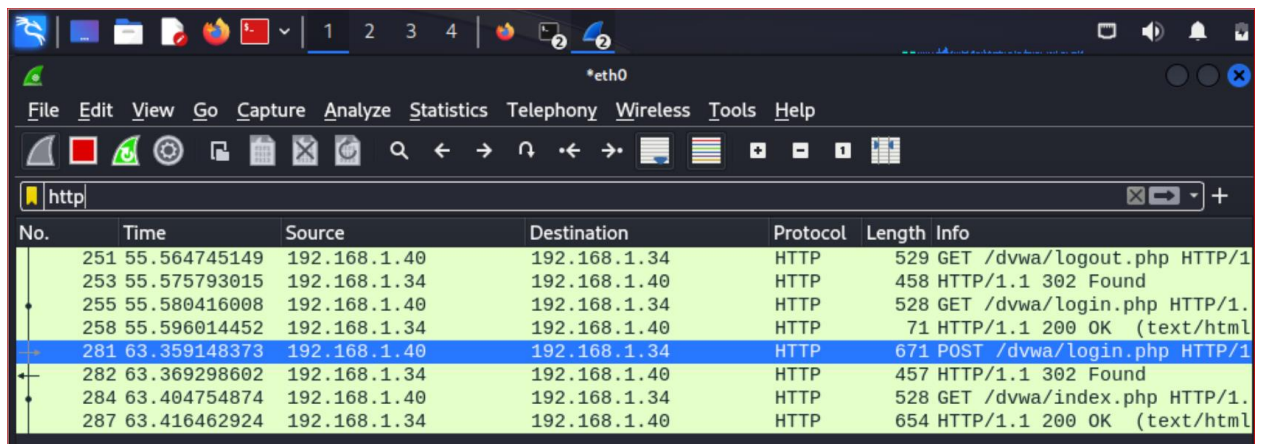
```
(svatsa@kali)-[~]  
$ sudo urlsnarf -i eth0  
[sudo] password for svatsa:  
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]  
192.168.1.34 - - [28/Oct/2023:11:53:10 -0400] "GET http://tikiwiki.com/ HTTP/1.0" - - "-" "Wget/1.10.2"  
█
```

8. Open a browser in kali Linux and type the IP address of Metasploitable2 (Target Machine). Then go to DVWA page which would look like the following screenshot.

Login using **username : admin** and **password : password** or **admin** (These should be provided in the same login page of DVWA)



9. Now open Wireshark inside Kali Linux and filter with **http**:



10. Analyze **HTTP POST** packet to capture the credentials you used to login to DVWA page in Metasploitable2 VM.