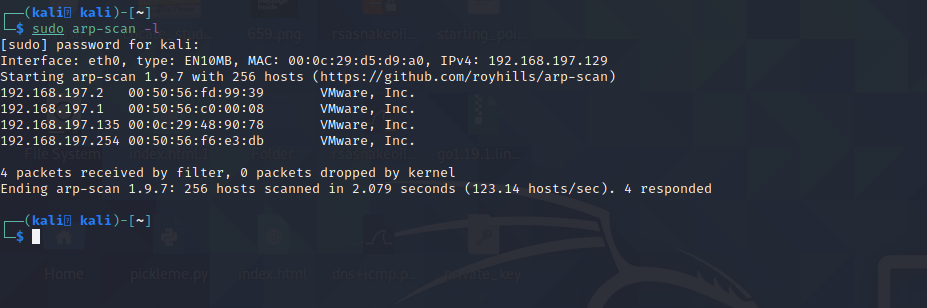
**Name: Shangirne Kharbanda**

**Registration Number: 20BAI1154**

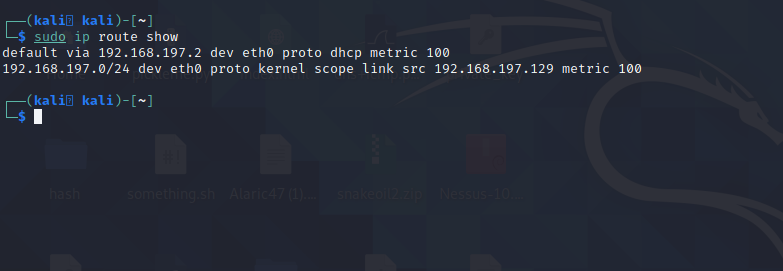
**LAB-7 ISM**

**ARP SPOOFING**

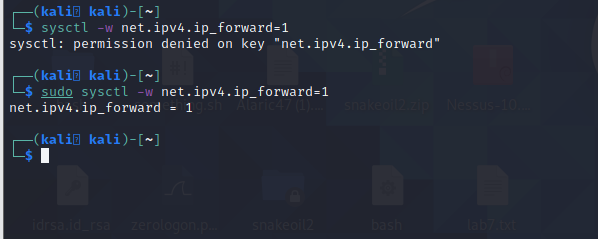
We will first run an **arp scan to find out the IP of metasploitable**.



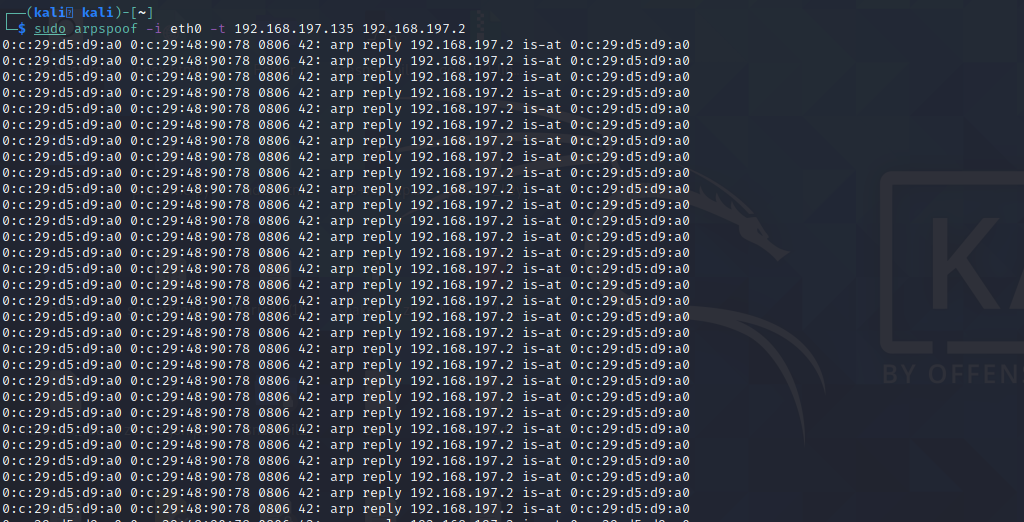
We can see that the **IP of metasploitable2 is 192.168.197.135**



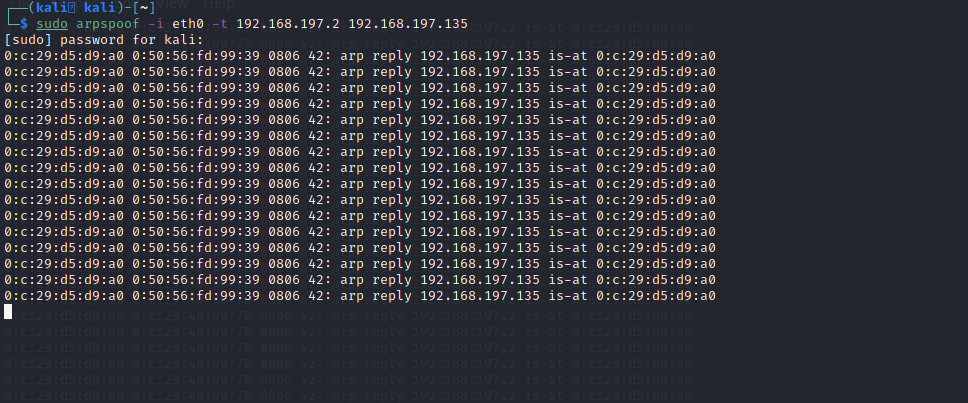
We use the following command to check theforwarding, if it works it shows result as true.



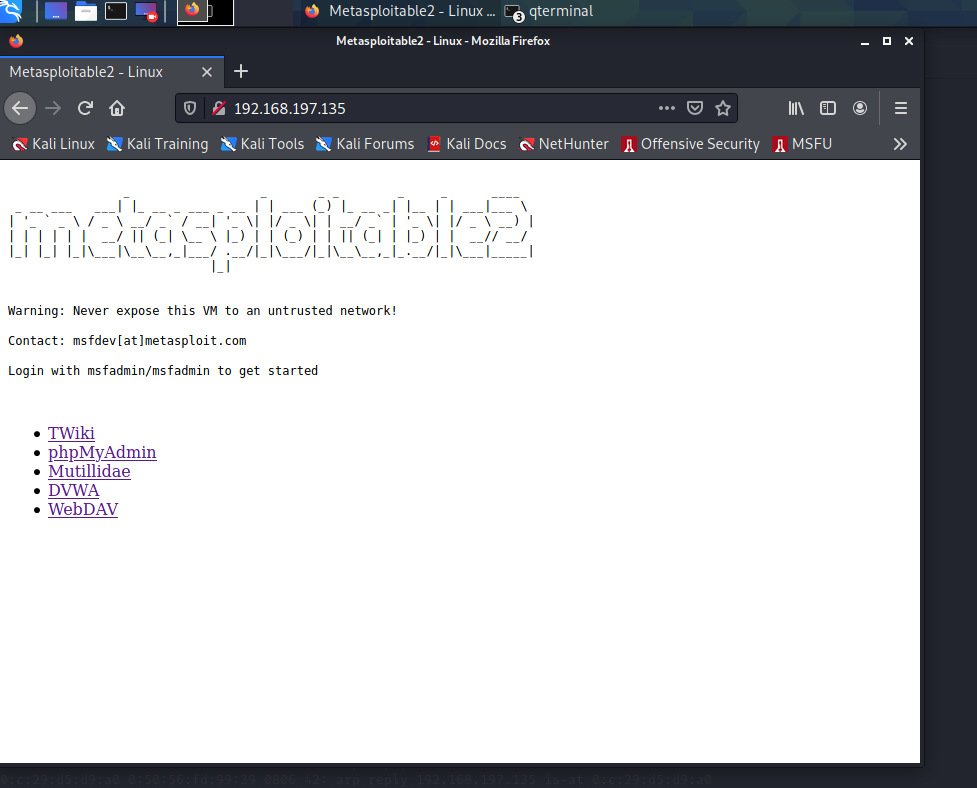
Now we will start our ARP spoofing attack.



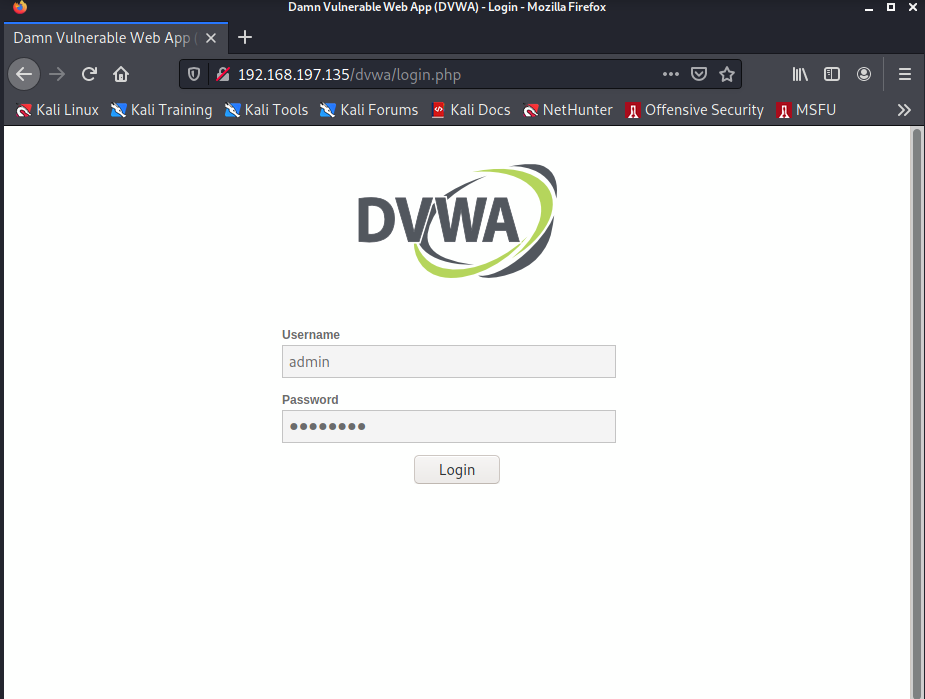
We open another terminal and swap the IP addresses in the command as shown below and run arpspoof again.



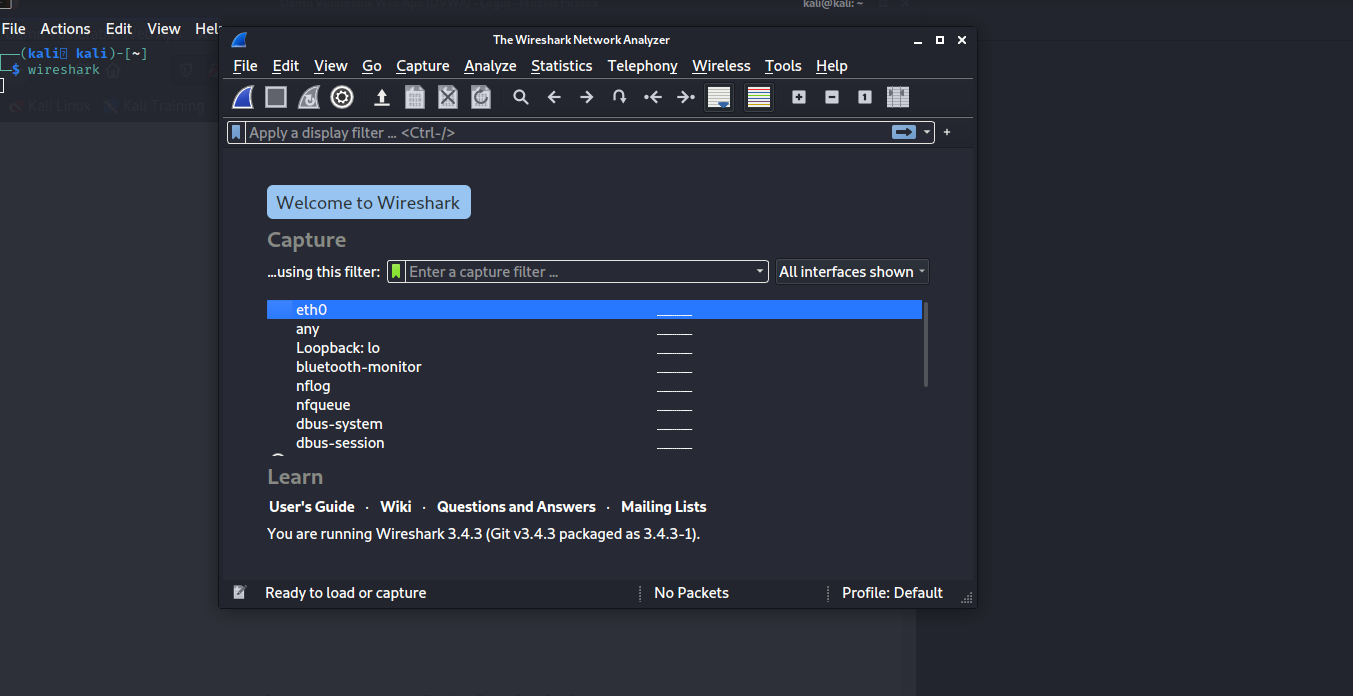
Now open the browser and type in the IP of Metasploitable2.



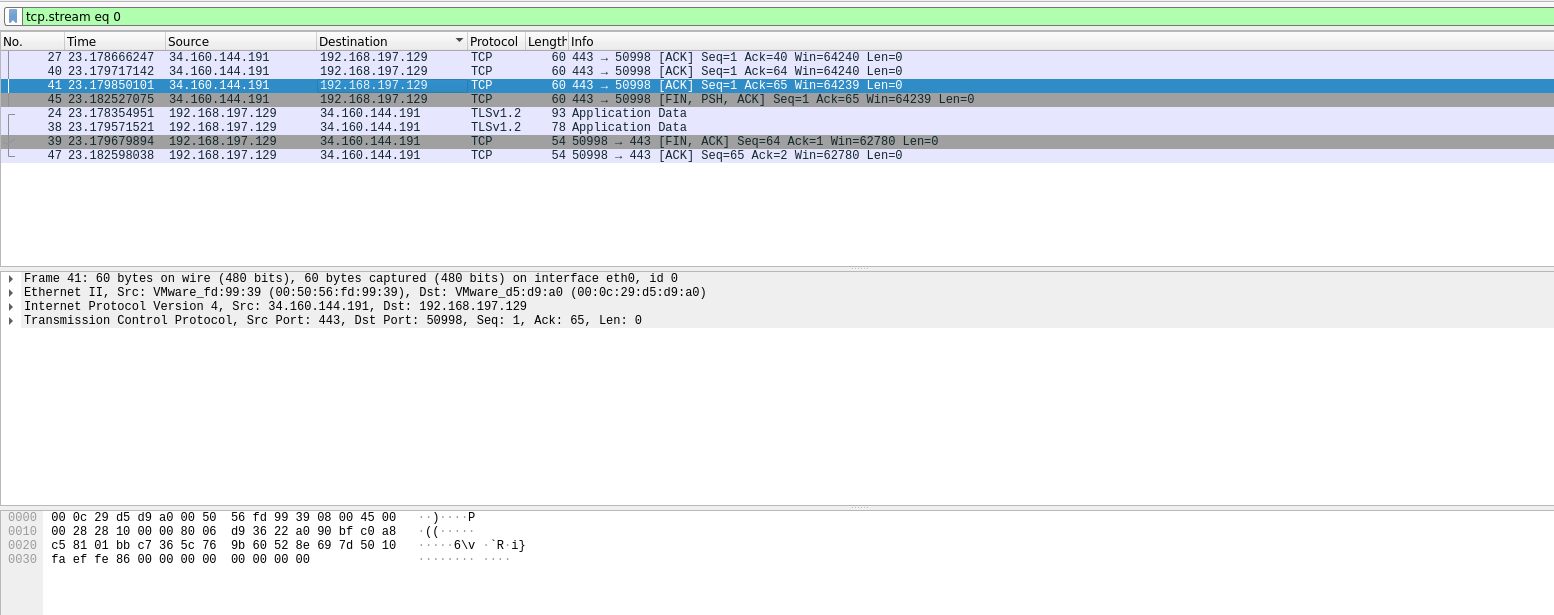
Go to DVWA and type in username as “admin” and password as “password”.



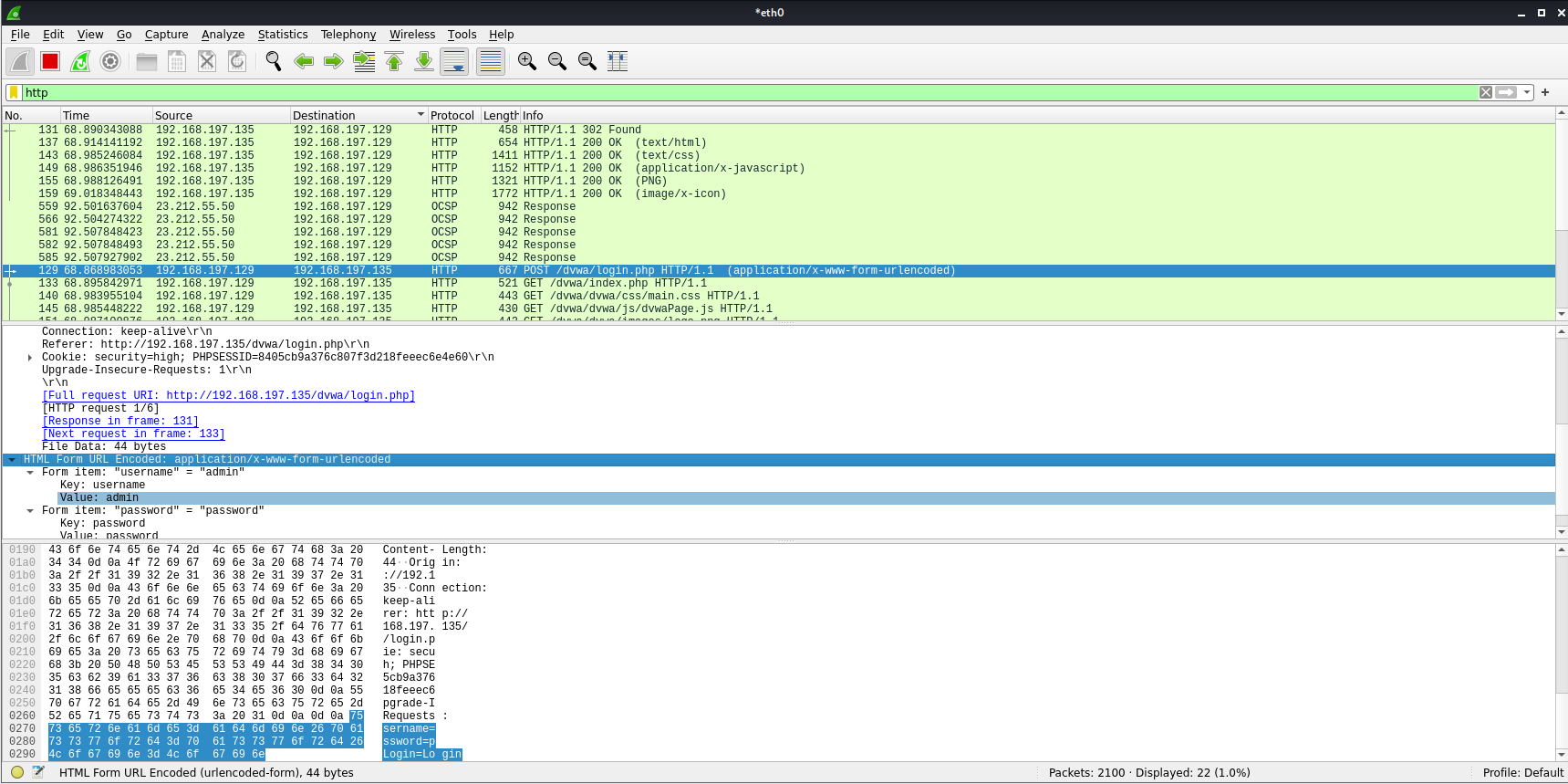
Now we will open Wireshark to capture the packets on both ends on interface eth0.



We will look at the TCP stream in Wireshark first.



After looking at **http stream** in wireshark, we scroll down and **find the HTTP packet that is containing username and password** that we used to log into DVWA in metasploitable2.



Next, we use the driftnet command to display images of websites which were used.





**Thus, we have successfully completed our implementation of MITM attack.**