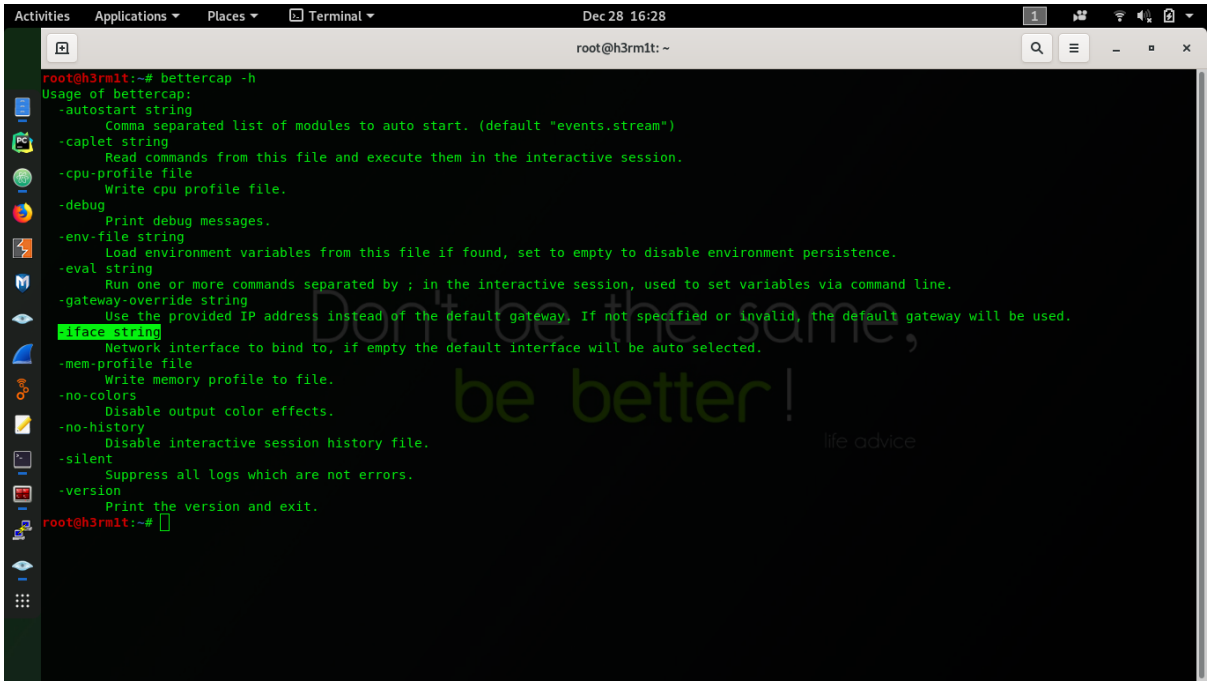
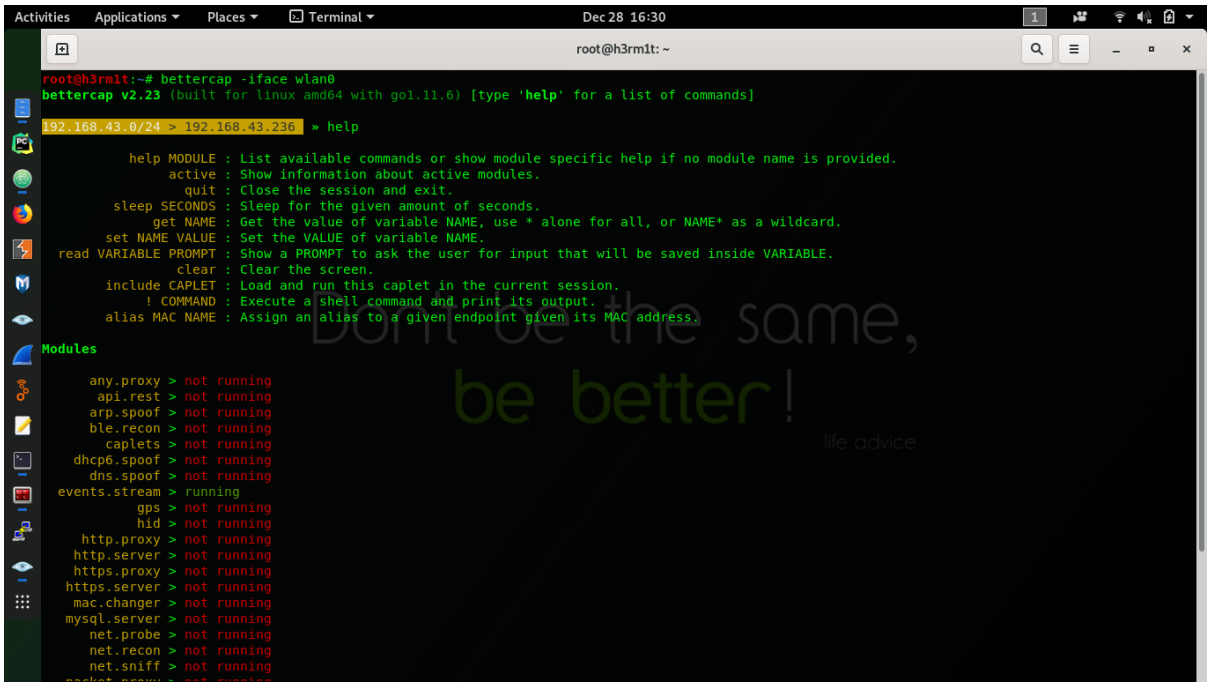
BetterCap Basic Usage:

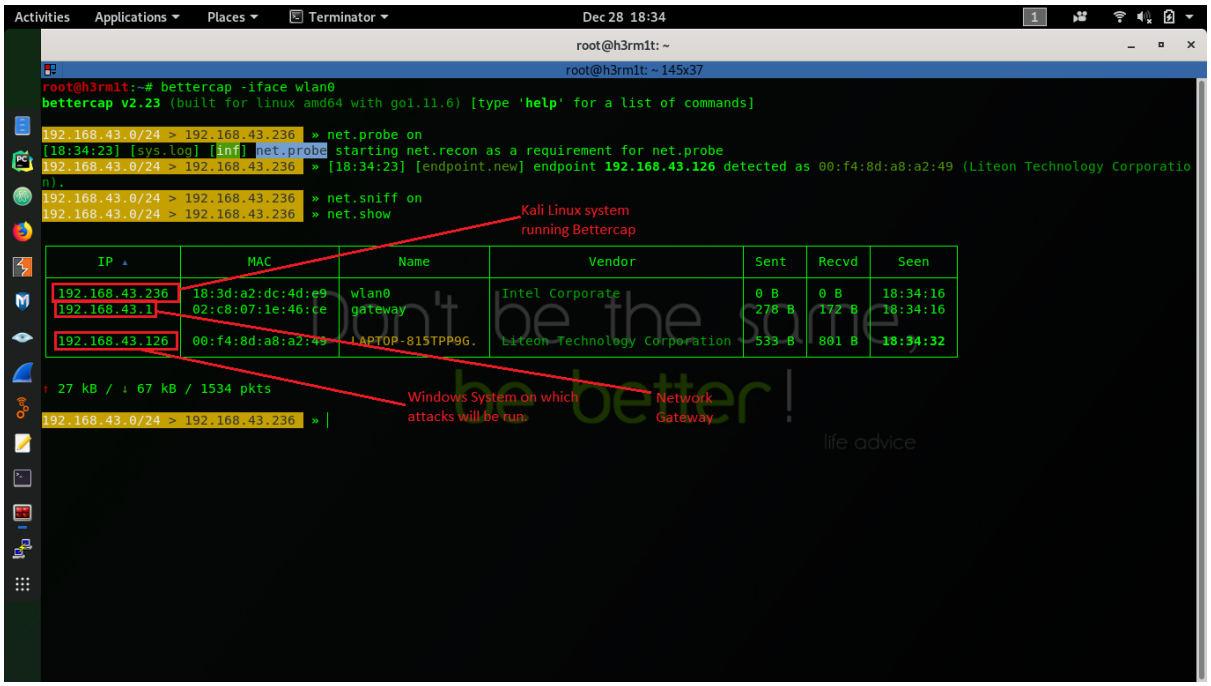
1. Help command shows the start-up options for Bettercap.



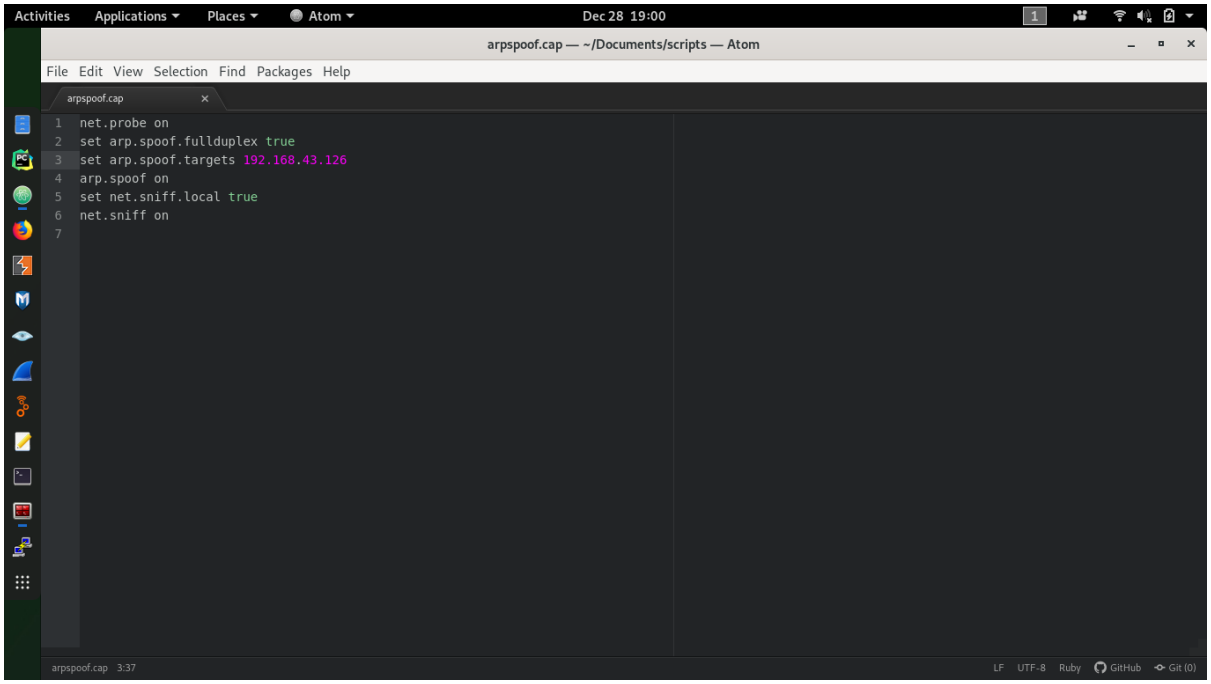
2. Start bettercap by binding it to a interface and show all the available modules using the 'help' command.



3. Switch on the net.probe and net.sniff modules and scan the network for all connected devices.

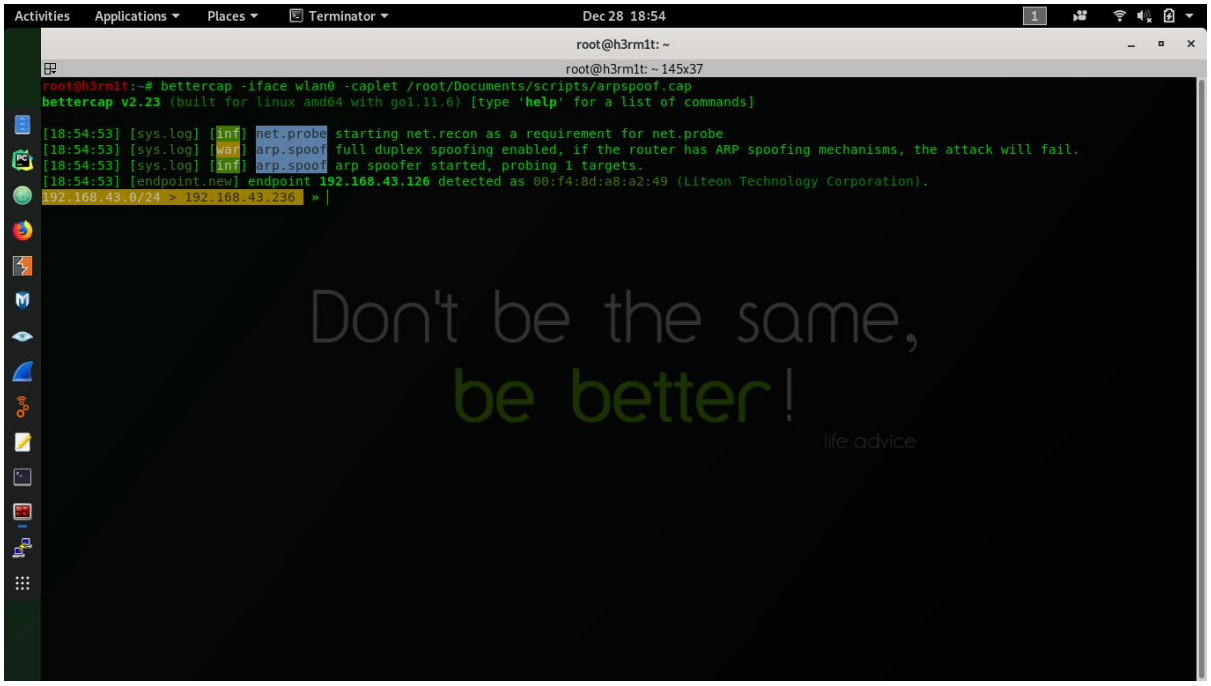


4. Instead of typing commands manually after starting bettercap, all the commands can be types in a text file which can be saved as a caplet(with a .cap extension). Then while starting bettercap this caplet file can be called using the '-caplet' parameter.

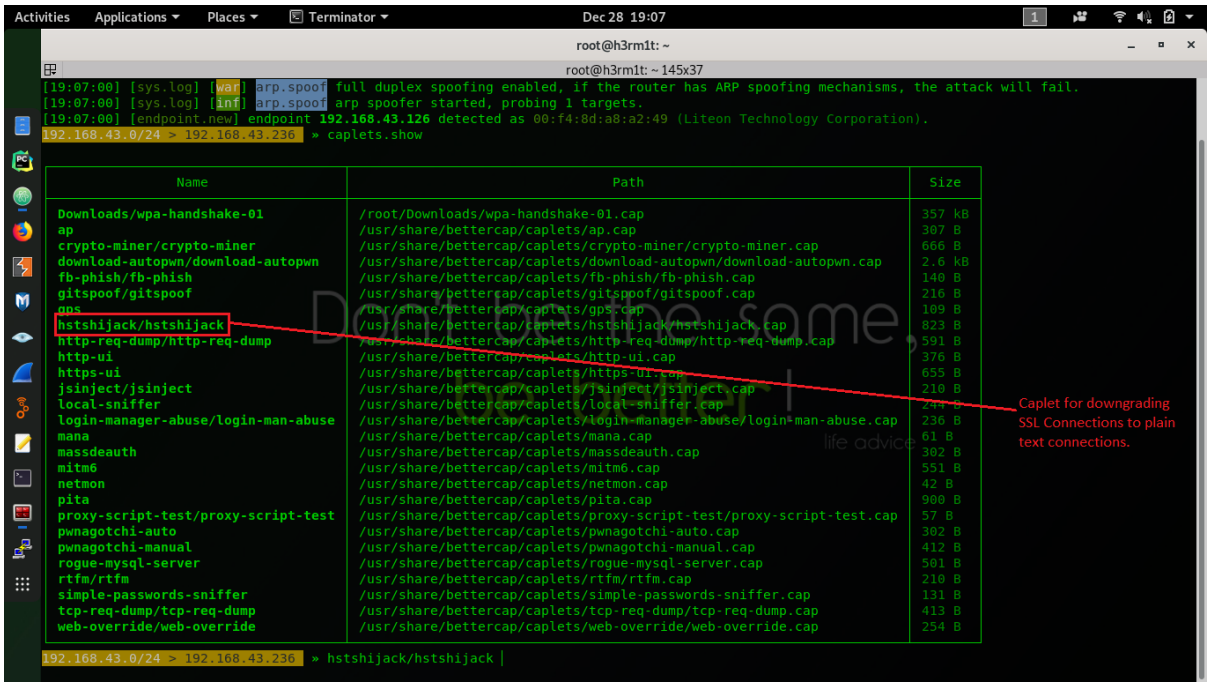


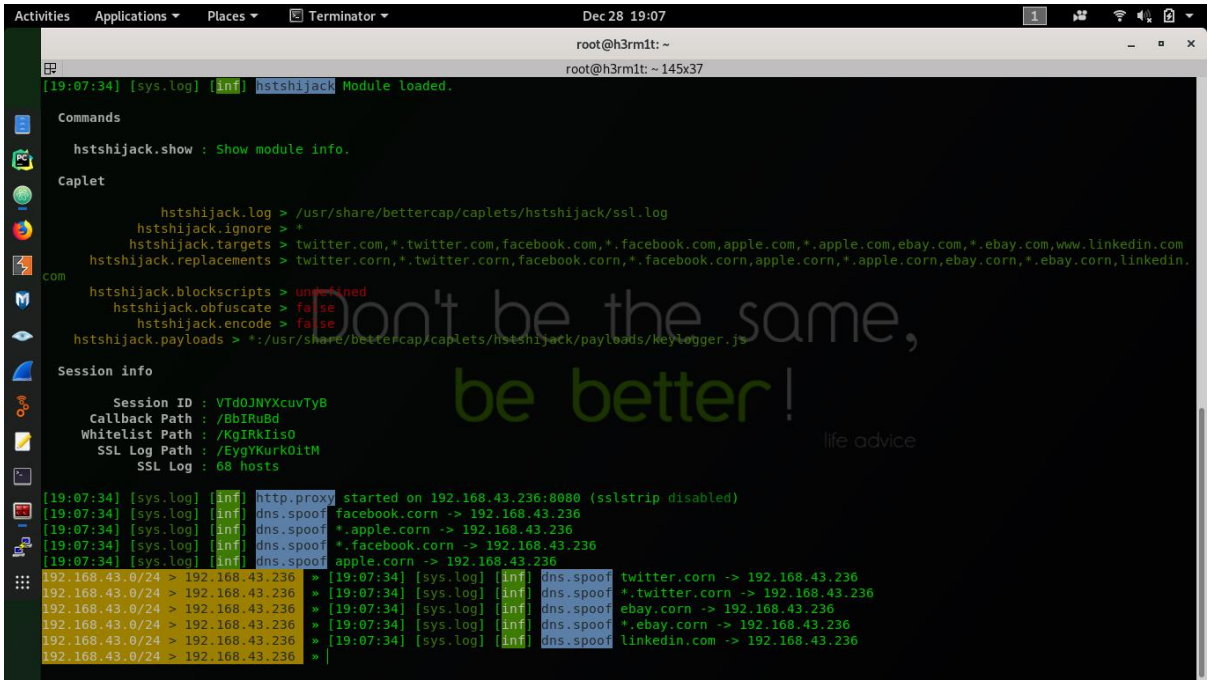
ARP Spoofing with BetterCap:

5. Start Bettercap with the caplet file created in the previous step.

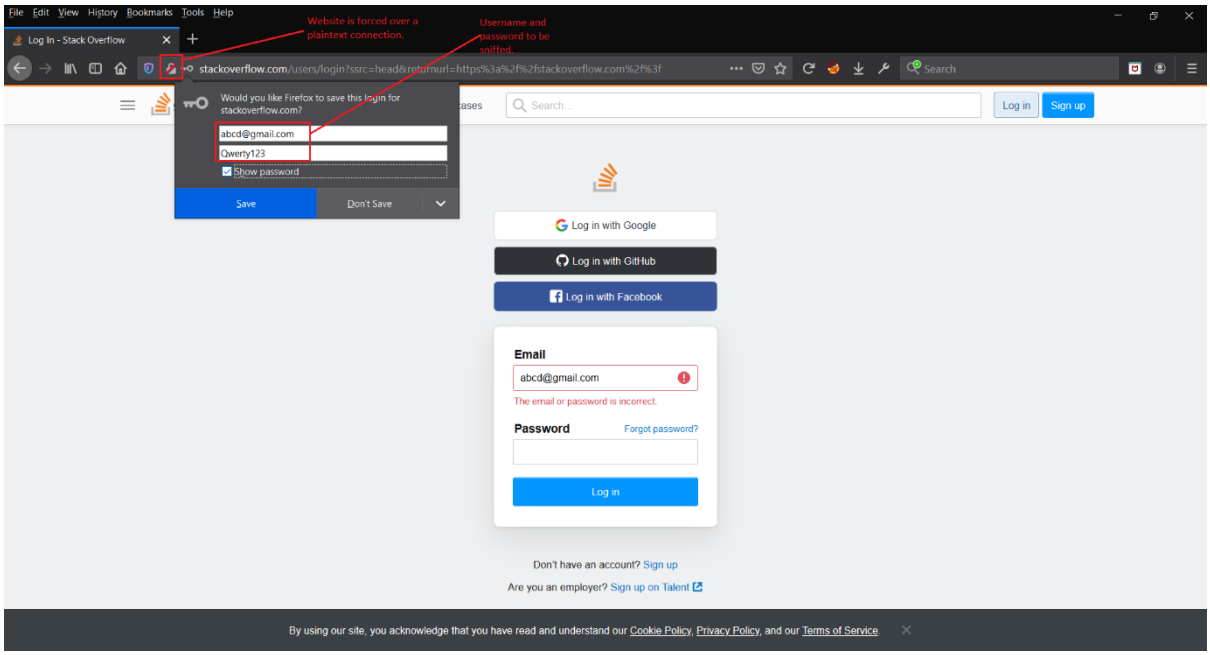


6. Display the list of in-built caplets available in bettercap using the 'caplet.show' command and select the hstshijack/hstshijack caplet.

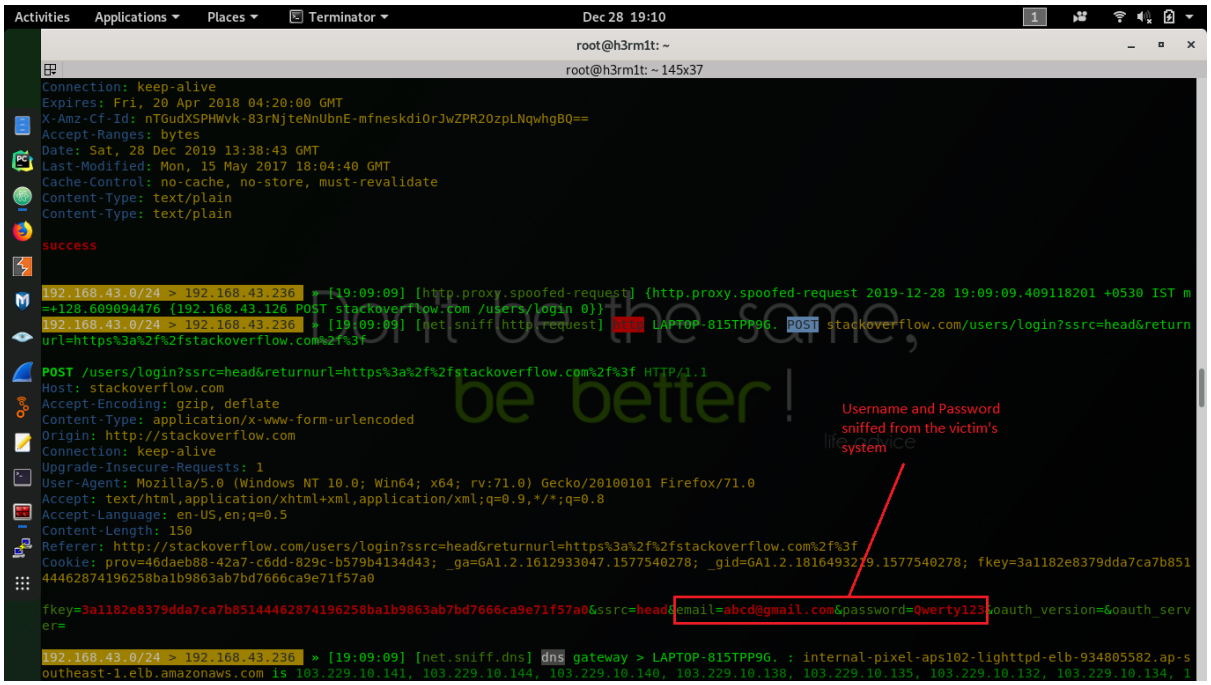




7. Once the caplet is executed, open a browser in the windows system (i.e. Victim system) and open a website that is normally opens on SSL.

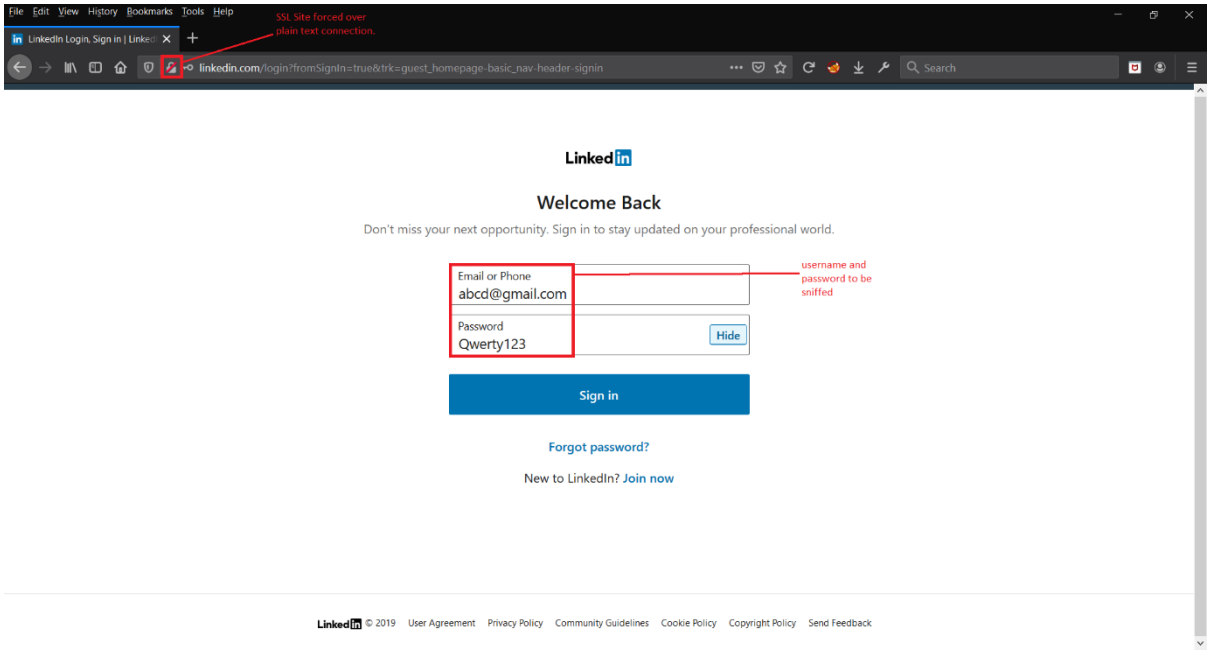


8. Check the bettercap UI for the sniffed username and password.

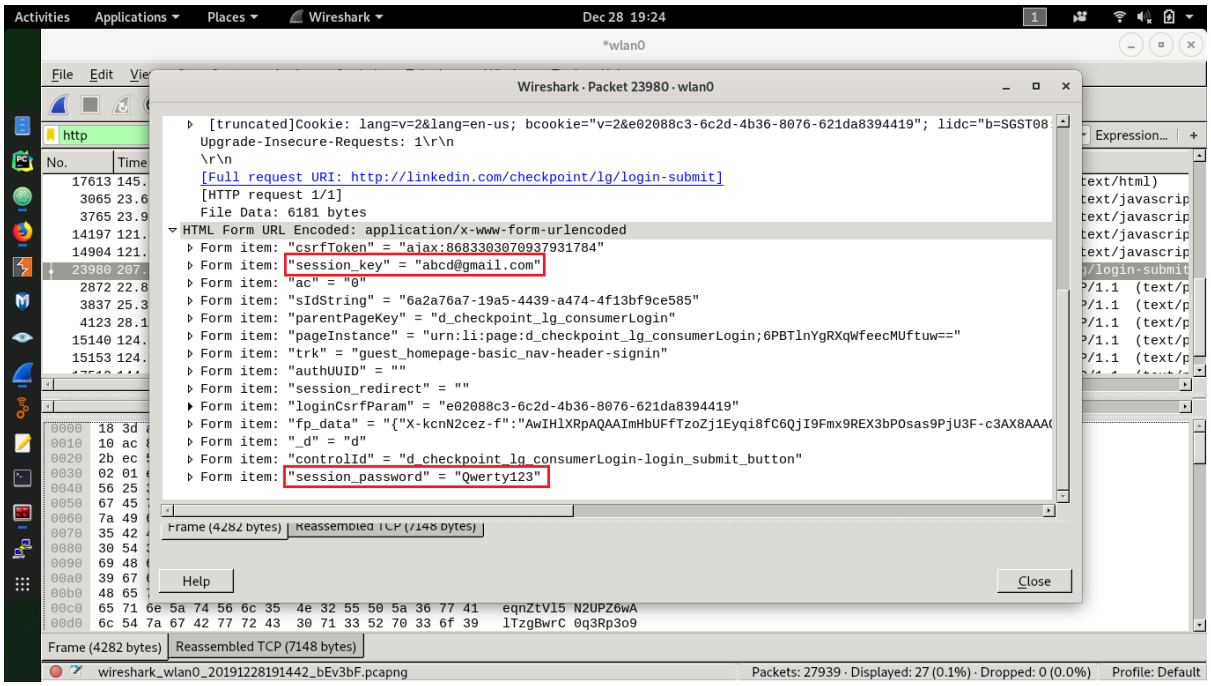


P.S. – Sometimes the bettercap UI becomes so cluttered that it's difficult to find the sniffed username and password. For such cases, Wireshark can be used to find out the Username and password as shown in the next example.

9.



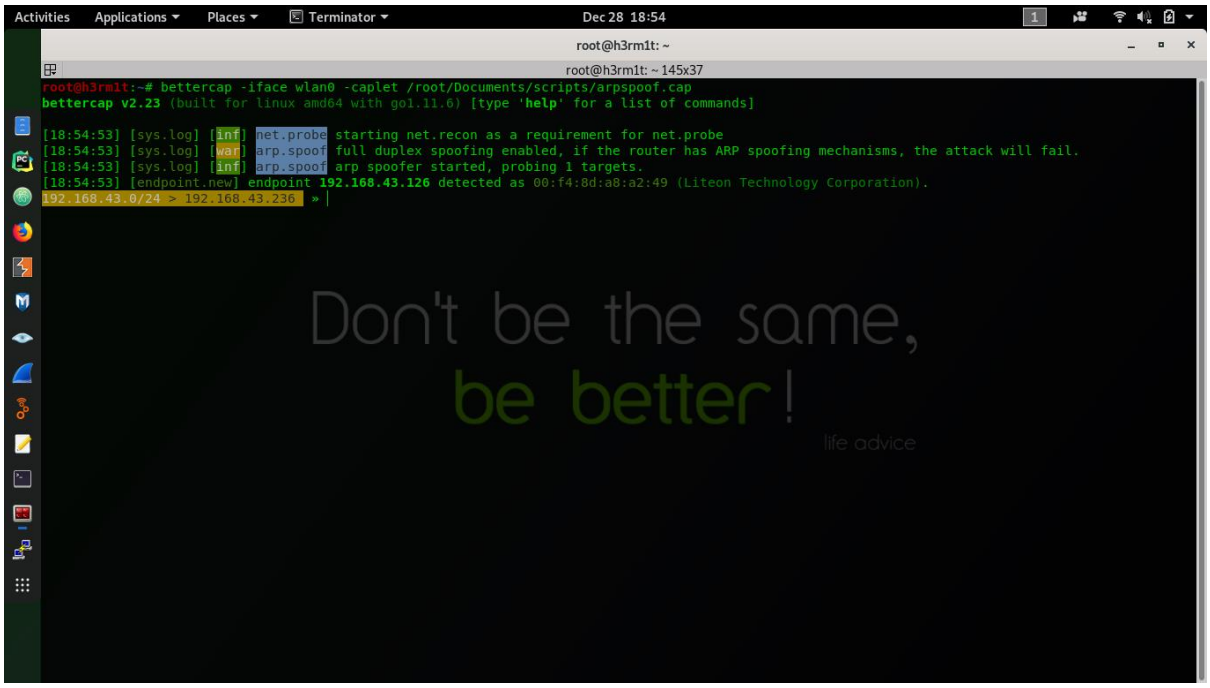
10.



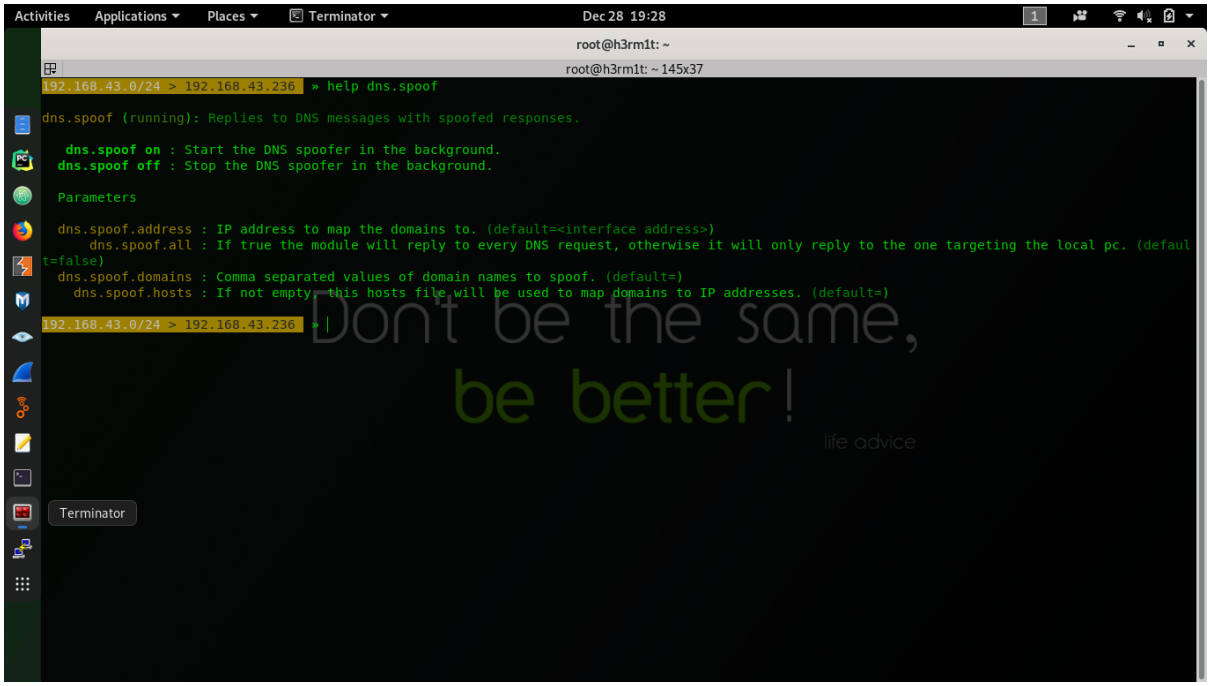
P.S. – These attacks won't work against sites like Facebook, Twitter etc as these sites use HSTS(HTTP Strict Transport Security). Any SSL site, where HSTS is not implemented can be downgraded to a plain test connection using the above-mentioned technique. For more details on HSTS, refer to [this URL].

DNS Spoofing with BetterCap:

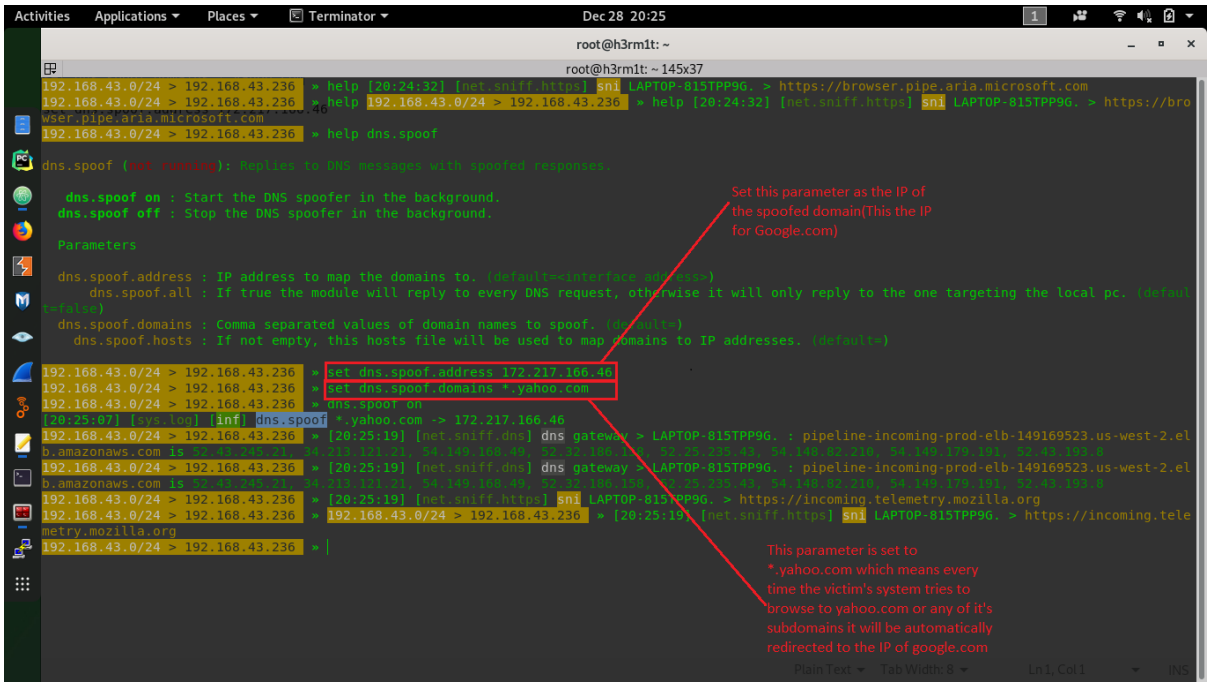
1. Start BetterCap with the arpspoof caplet created earlier.



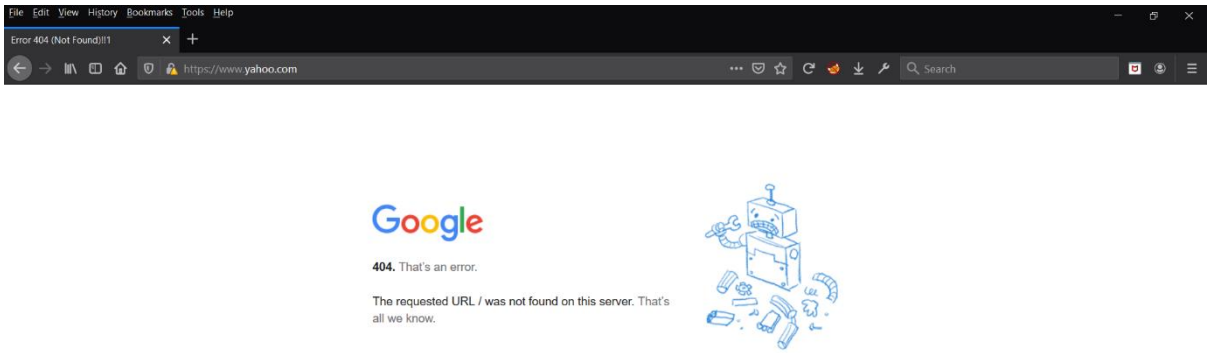
2. Use the 'help dns.spoof' command to check the available parameters for DNS spoofing.



3. Set the ‘dns.spoof.address’ and ‘dns.spoof.domains’ to the required values and turn on dns.spoof module.



4. Browse to yahoo.com in the windows system (i.e. victim System).



Even though the site is not accessible, still a yahoo.com page is redirected to a Google page.

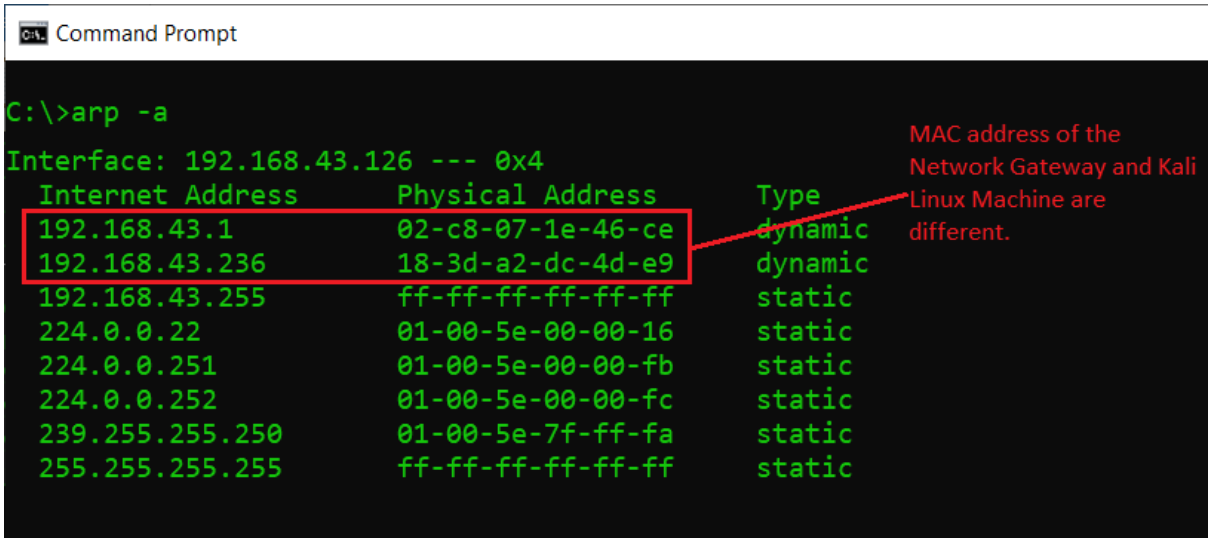
Remediation / Countermeasures:

To stay protected against MITM attacks you can either use **ARP tables** or tools like **XArp** or **Wireshark.**

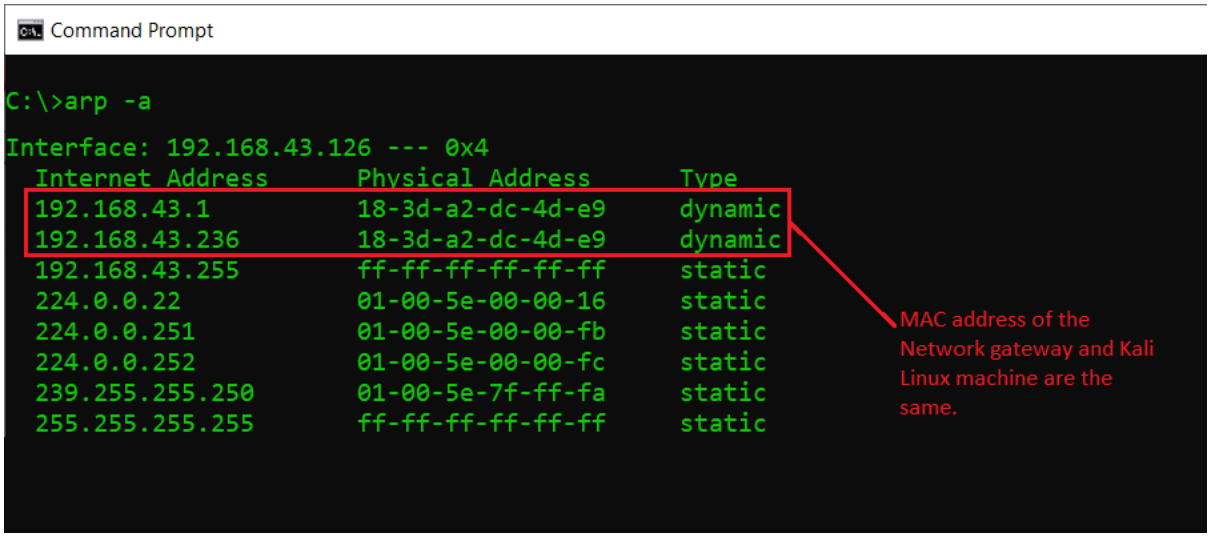
1. ***ARP Tables:***

Systems keep an ARP look-up table where they store information about what IP addresses are associated with what MAC addresses. When trying to send a packet to an IP address, the system will first consult this table to see if it already knows the MAC address. If there is a value cached, ARP is not used.

If the IP address is not found in the ARP table, the system will then send the IP address over a broadcast packet to the network using the ARP protocol. Any machine with the requested IP address will reply with an ARP packet and this includes the MAC address which can receive packets for that IP.



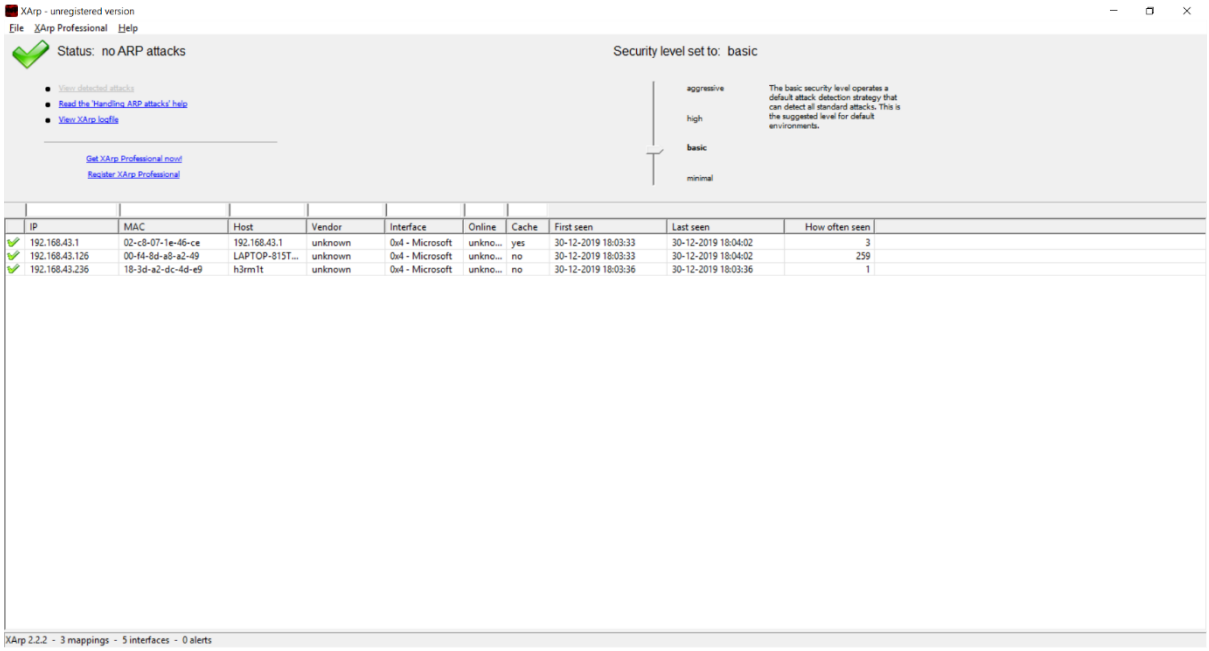
Before ARP Spoofing



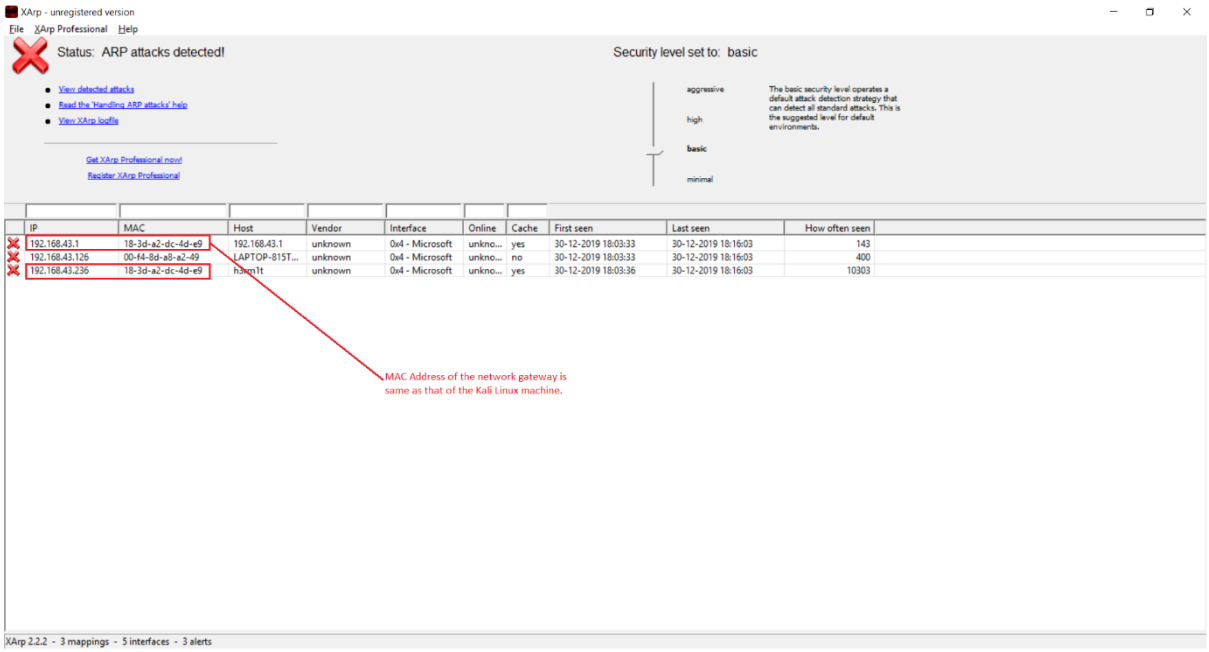
After ARP Spoofing

2. ***Using XArp:***

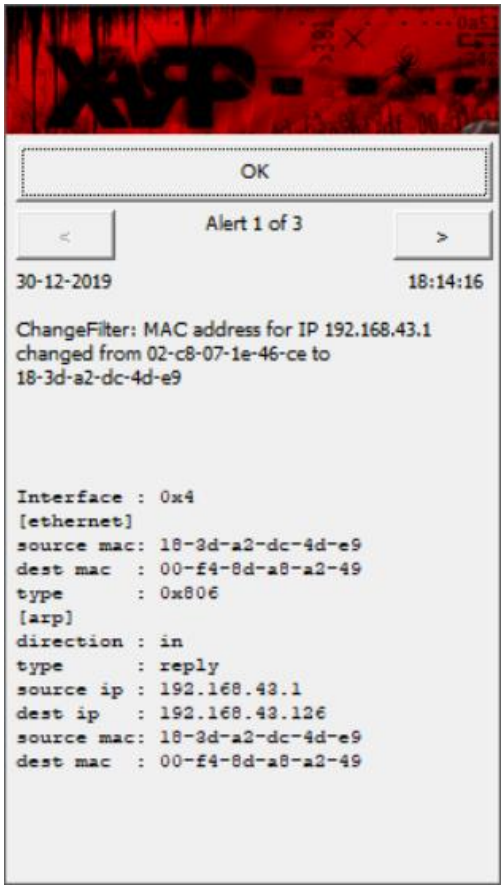
Using the ARP table and continuously to monitor for ARP spoofing attacks is not the most feasible idea. Instead you can use a Tool like XArp which automatically notifies you whenever there is an ARP spoofing network happening on the Network.



Before Attack



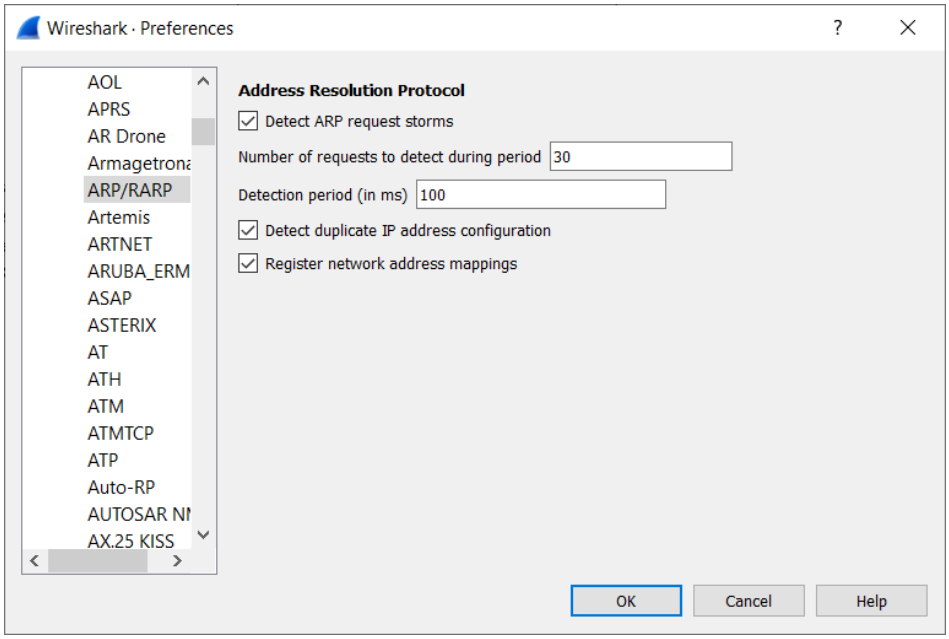
After Attack



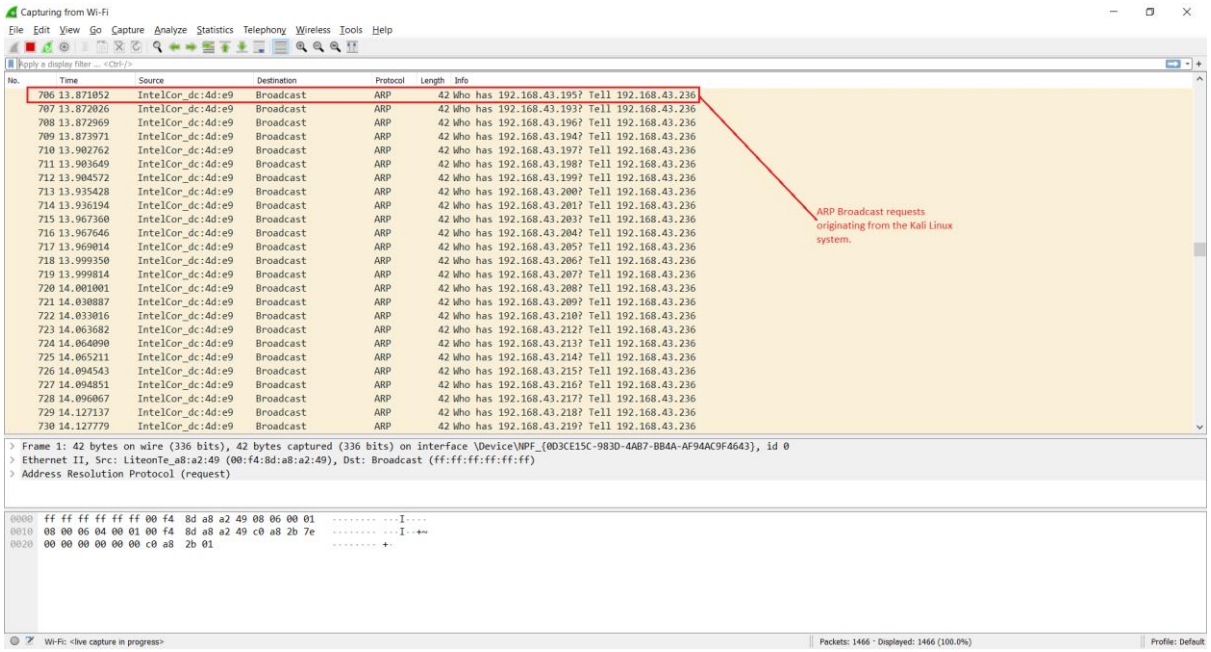
Popup Message whenever ARP Spoofing attack happens

3. Using Wireshark:

As a Network Administrator, if you have to monitor ARP spoofing attacks happening in your local network, you can use Wireshark. However, first you have to make sure that Wireshark is able to identify the ARP requests. For this, in the Wireshark GUI, go to **Edit > Preferences > Protocols > ARP/RARP** and click the check box for **'Detect ARP Request Storms'.**



Now you are ready to detect ARP spoofing attacks.



****