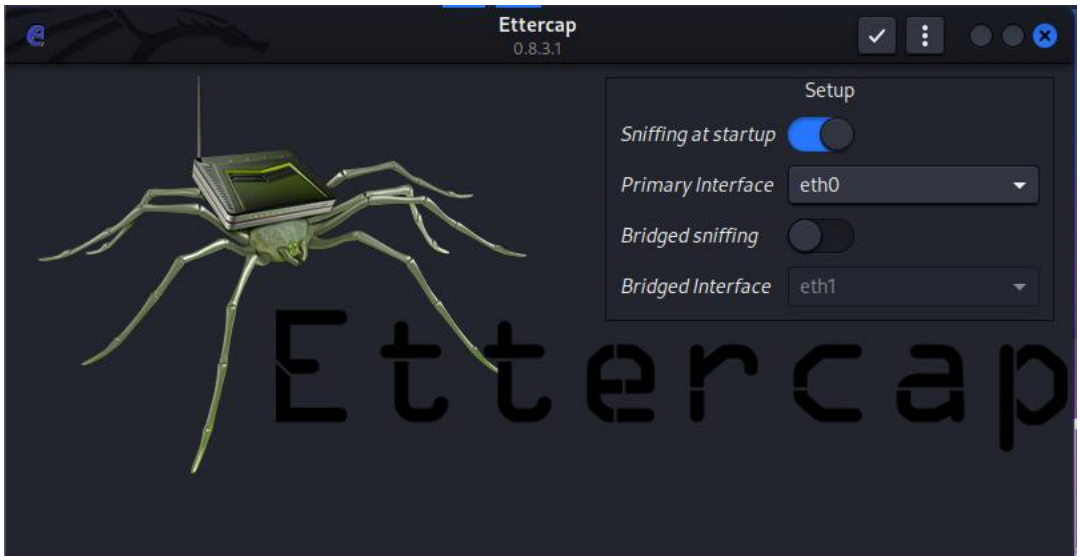
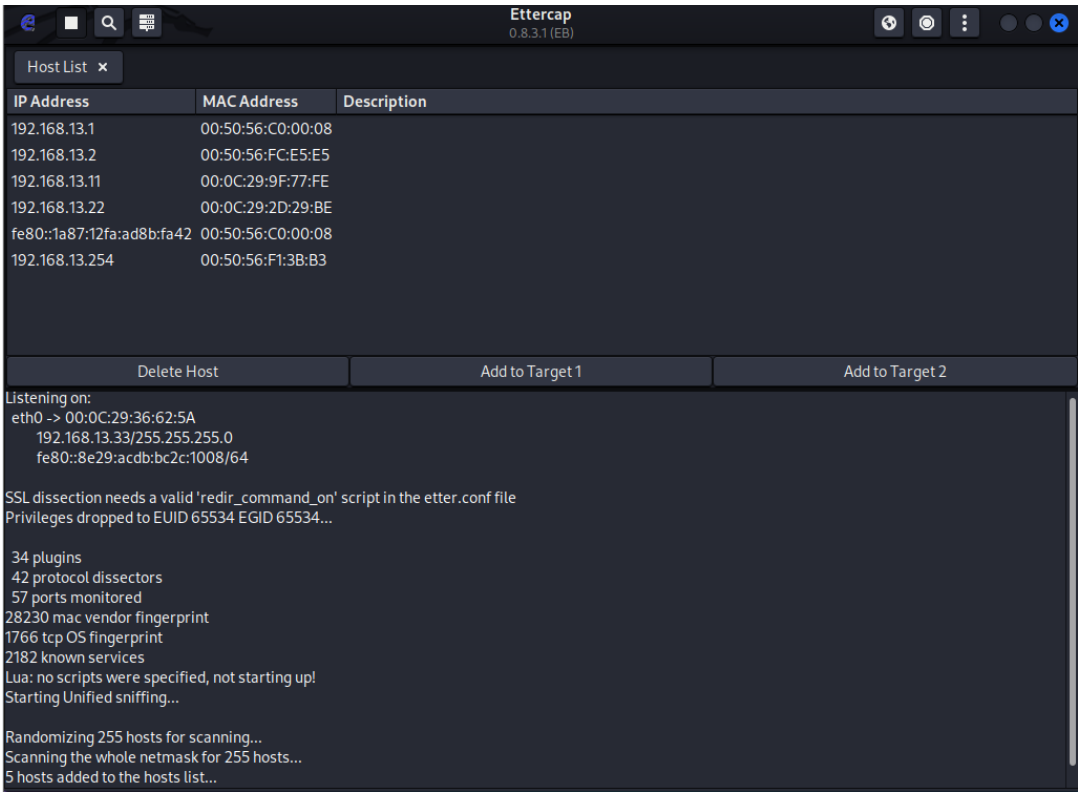
MITM attack with ARP Poisoning using Ettercap

1. Power-on all three VMs in the NAT subnet (VMnet8).
2. Start with Kali => Click on Applications => 09-Sniffing & Spoofing => ettercap-graphical => type “kali” for the Password to authenticate the operation:

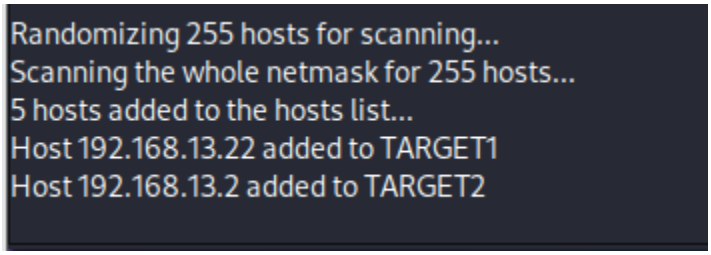


Click on the check-mark button ☑ at the top panel => Click on the ⋮ button => Hosts => Scan for hosts :

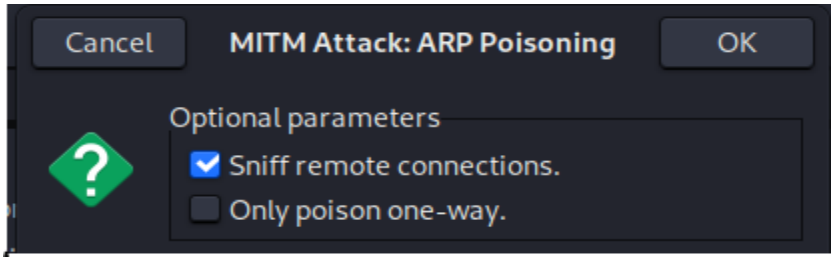
3. Click on the Hosts list button on the top-left:



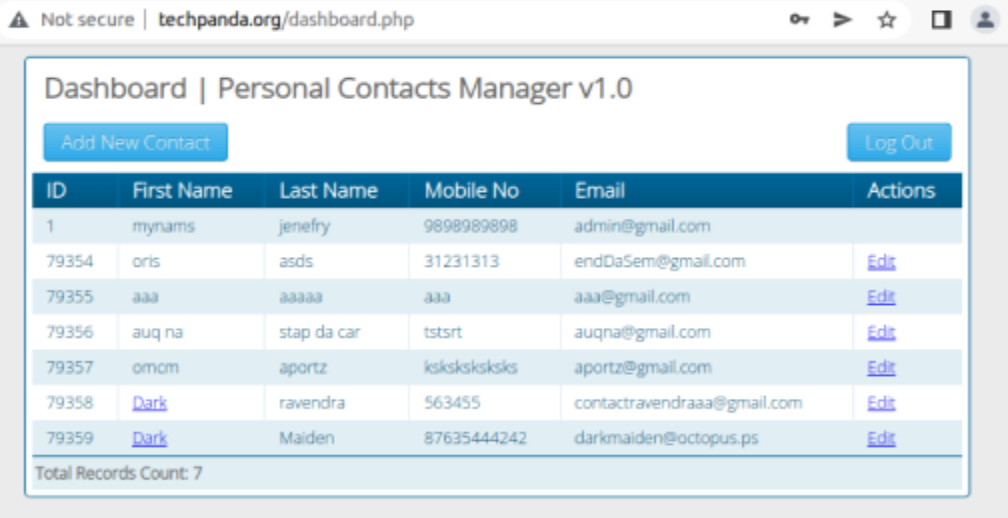
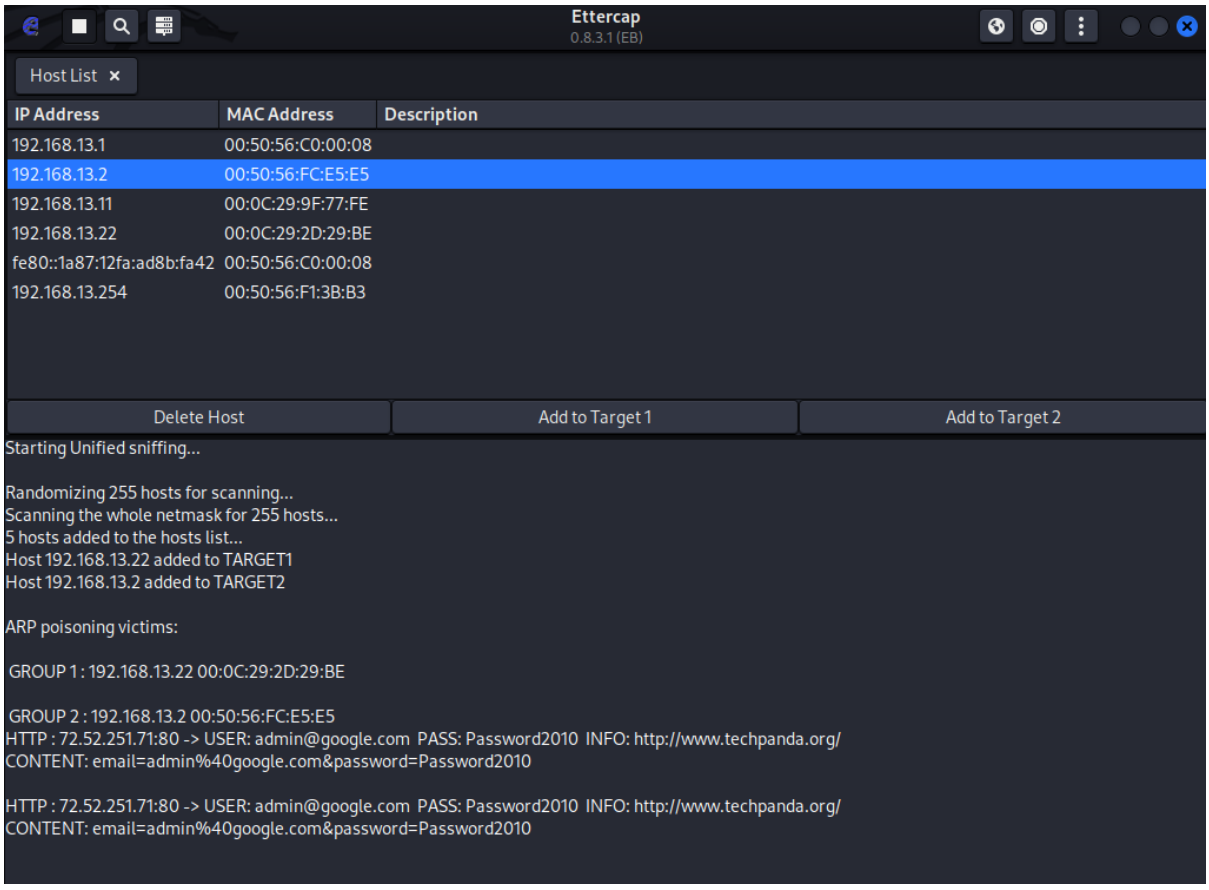
4. Let's target Ubuntu VM2 (ip: 192.168.13.22) with the help of the default gateway (ip: 192.168.13.2). Select the ip: 192.168.13.22 from the Host List, and click on "Add to Target1" button. Then select the ip:192.168.13.2 from the Host List, and click on "Add to Target2" button.



5. Click on MITM Menu button at the top right => ARP Poisoning... => check "sniff remote connections" => OK



6. Switch to Ubuntu VM2, open a browser and type in the url: www.techpanda.org, then enter the username: **admin@google.com** and the password: **Password2010.** If log in successfully, you will see a screen look like this:



7. Now switch to Kali VM to see the results: