Network Security Practices
CY5150
Task 7

Submitted By:
Sonam Ghatode(001305171)

Table of Contents

Kali Source IP and MAC: 2

Target Details: 2

Introduction to Ettercap: 3

Target ARP table before and during the attack: 5

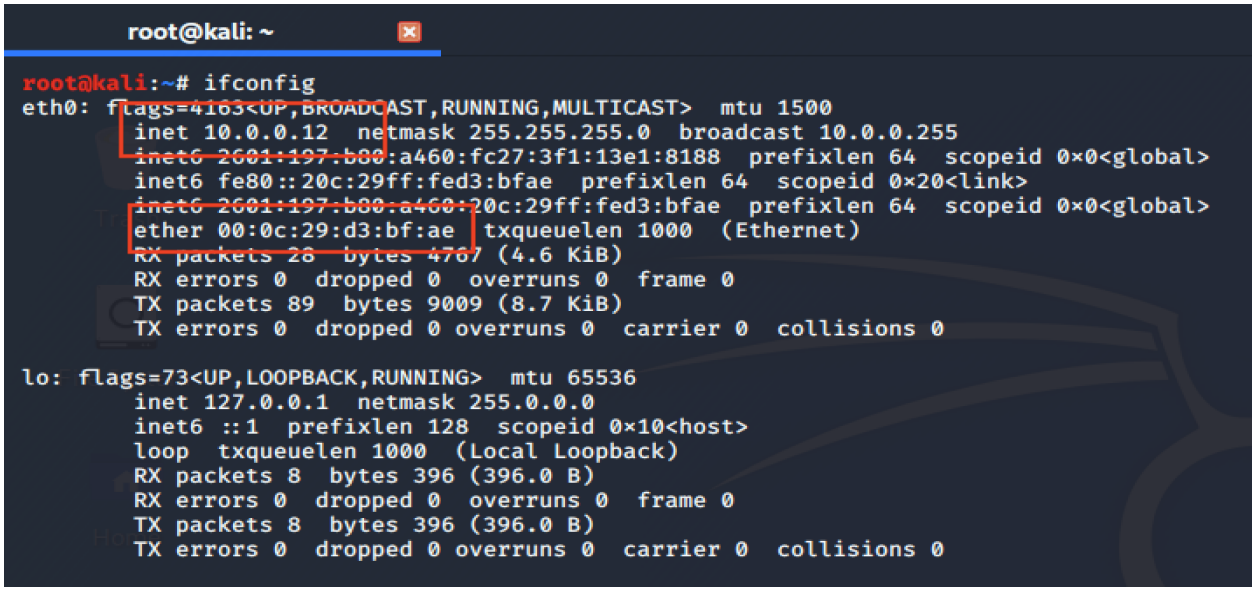
Target Desktop accessing khoury.neu.edu during attack: 6

Tcpdump output in kali displaying target IP passing traffic during ARP poisoning: 6

References: 8

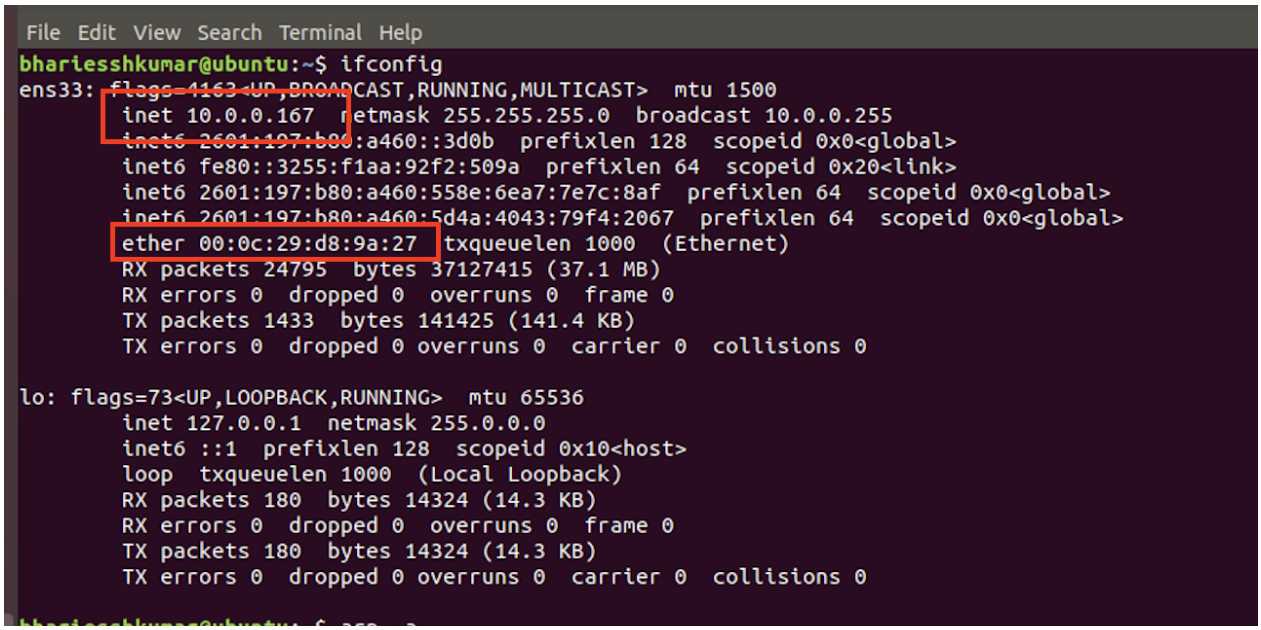
Kali Source IP and MAC:

Source IP: 10.0.0.12
MAC: 00:0C:29:D3:BF:AE



Target Details:

Target OS: Ubuntu
Target IP: 10.0.0.167
Target MAC(from victim's system): 00:0C:29:D8:9A:27
Target MAC(from Ettercap): 4C:1D:96:7D:E7:A4



Introduction to Ettercap:

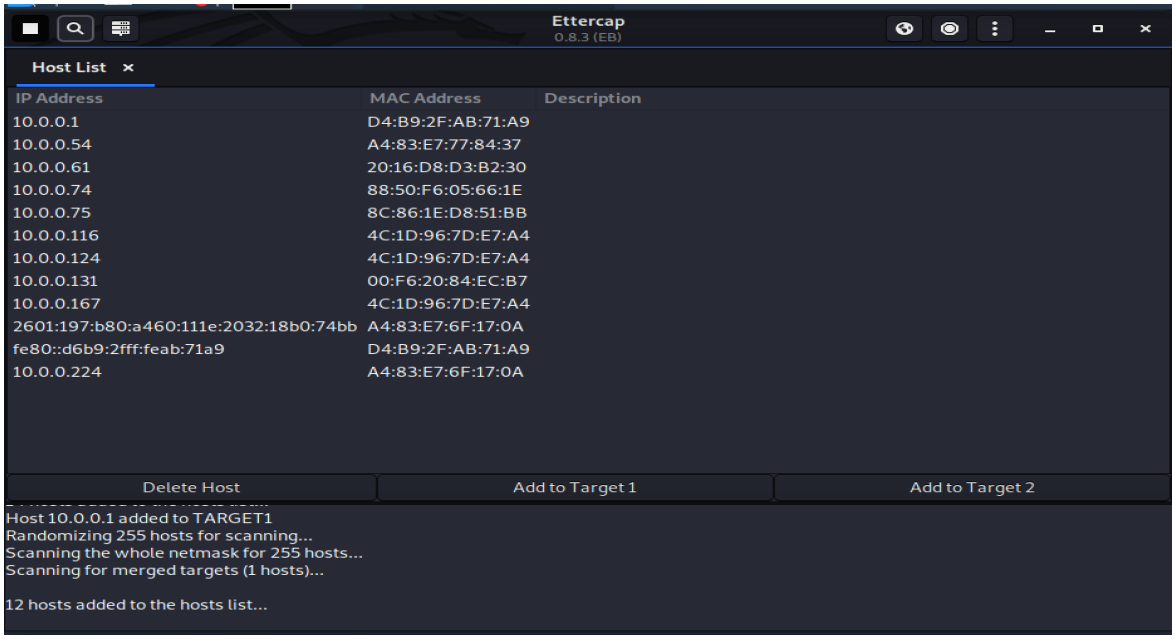
Ettercap is an open source network security tool that launches Man-In-The-Middle(MITM) attacks on LAN and can be used for network protocol analysis and security auditing. It is capable of intercepting traffic on a network, capturing passwords, and active eavesdropping against a number of common protocols. It works by keeping the network interface into promiscuous mode and by ARP poisoning the target machines.

Ettercap has four modes of operation:

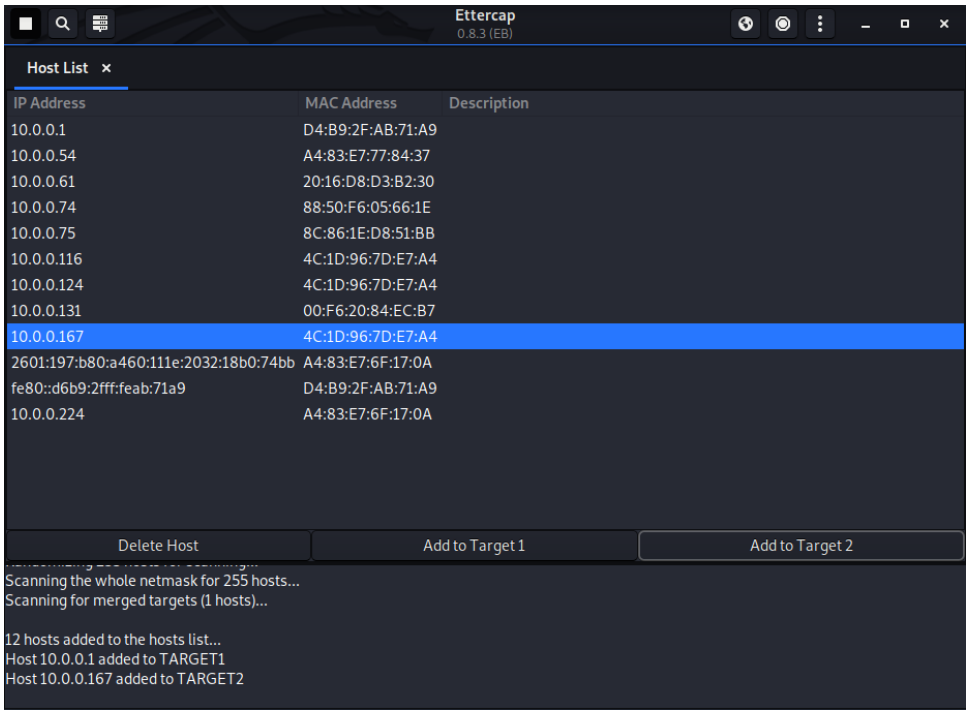
- IP-based: packets are filtered based on source and destination of IP packet.
- MAC-based: packets are filtered based on MAC address, useful for sniffing connections through a gateway.
- ARP-based: uses ARP poisoning to sniff on a switched LAN between two hosts.
- PublicARP-based: uses ARP poisoning to sniff on a switched LAN from a victim host to all other hosts.

In this task, ARP-poisoning had to be done. Ettercap is a UI-based application that uses Target 1 as the gateway(i.e. Router) via which the attacker is connected to the internet, and Target 2 as the IP of the scanned target in the same network. Ettercap allows to first search the hosts in the same network and then launch ARP spoofing on the desired target. To launch the ARP Spoof attack on the victim without DOSing the victim needed the attacker to enable IP forwarding in the system. In kali, the command **sudo sysctl -w net.ipv4.ip_forward=1** is used to enable IP forwarding to ensure traffic is forwarded to the gateway to prevent DOSing the target.

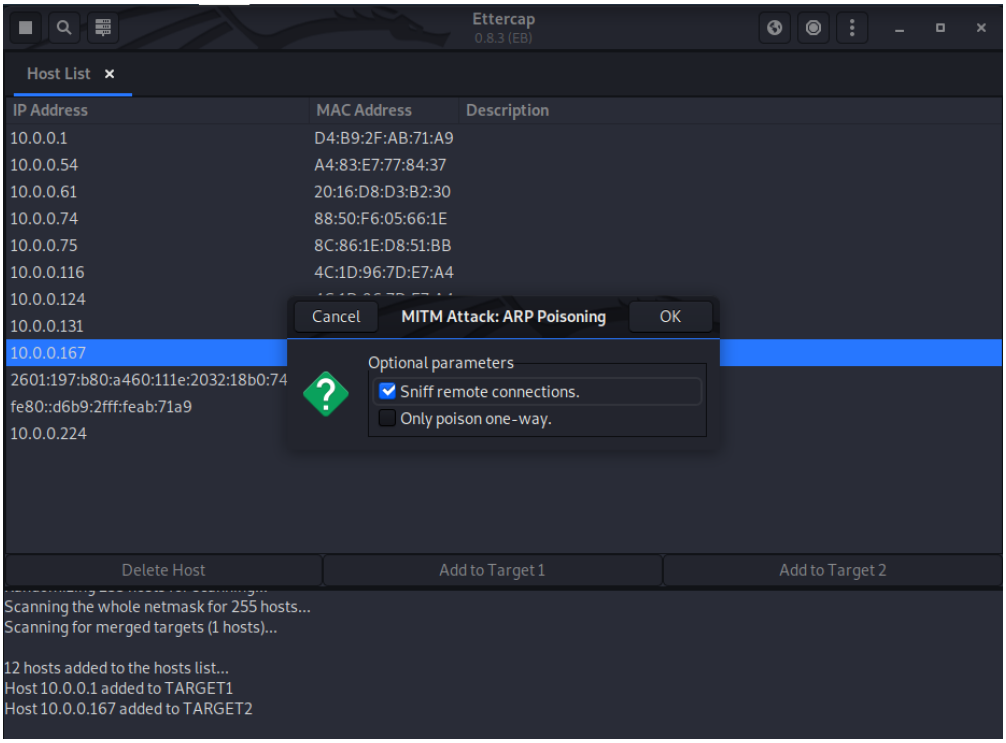
To attack a host in the network, scanning was done first using the ettercap tool. Following shows the screenshot of the scanned hosts:



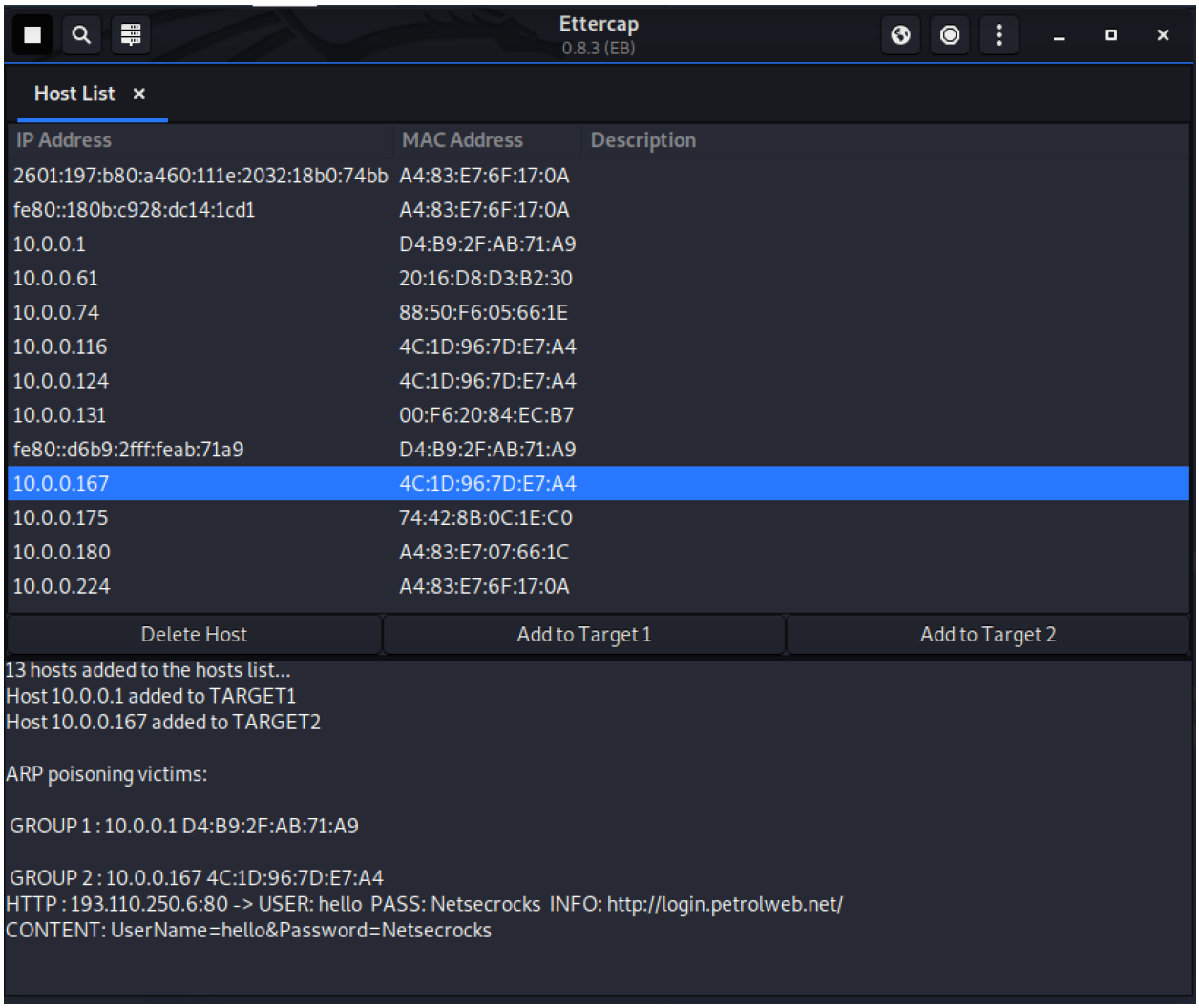
Among these, 10.0.0.167 was identified as the host I wanted to attack. Therefore, gateway(router) with IP 10.0.0.1 was added as Target 1 and 10.0.0.167 was added as Target 2 to launch ARP Spoofing attack:



After adding the targets, MITM attack was launched:

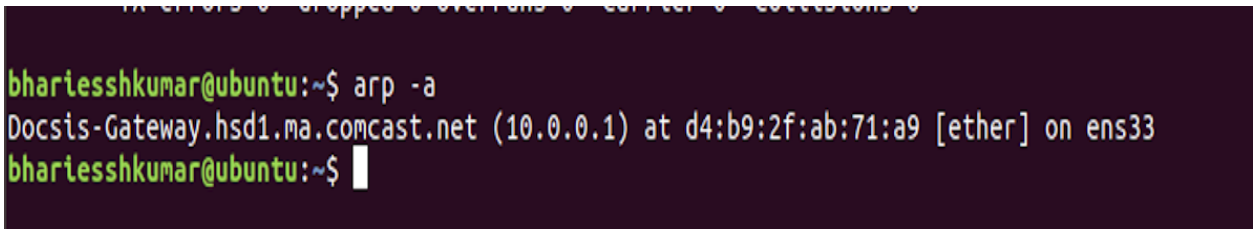


After starting the attack, if the victim tried to access any site which did not have HTTPS, the credentials were in plaintext and prone to sniffing. We searched a site that did http login, following was the result when it was accessed using victim machine:

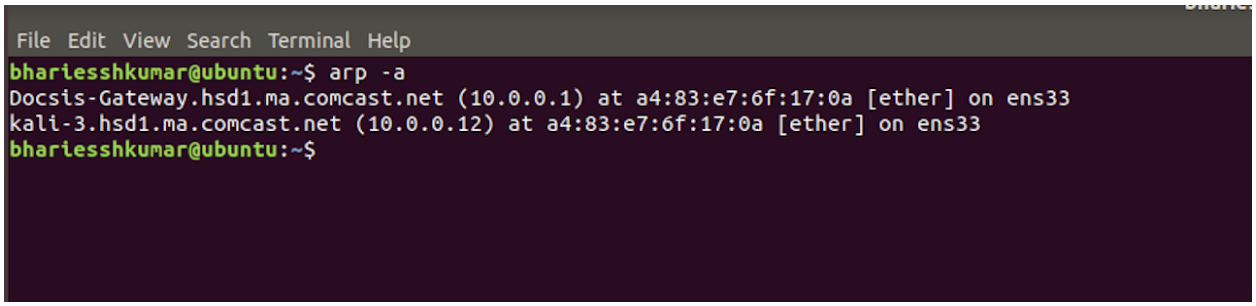


Target ARP table before and during the attack:

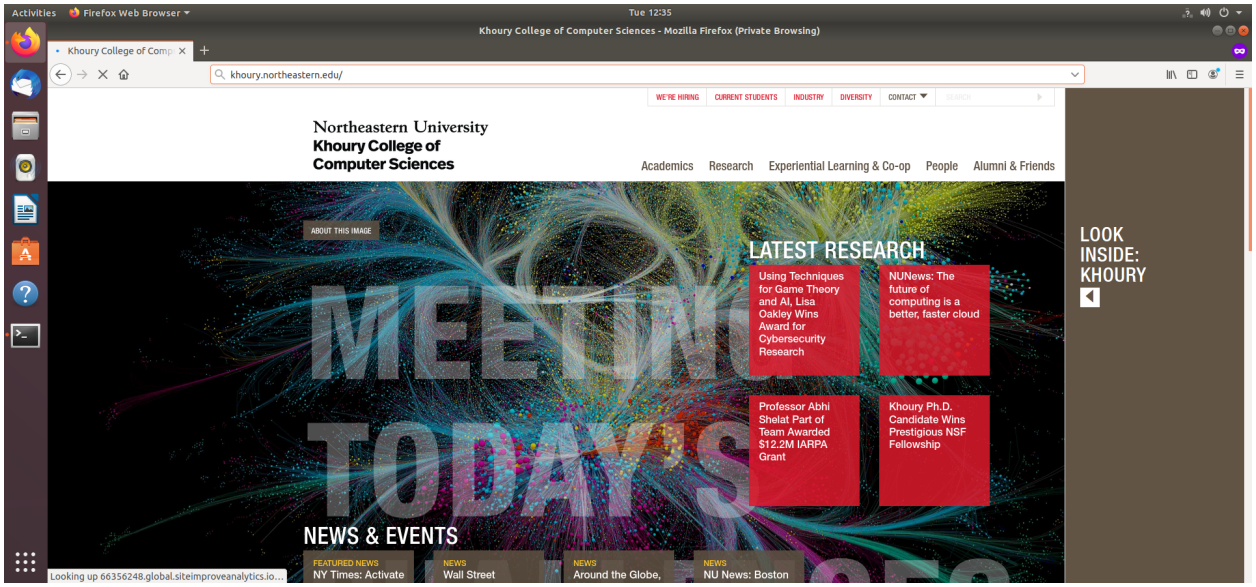
In this screenshot, the gateway's actual MAC is there i.e. ARP entry before the attack:



During the attack, Gateway's address got changed to the attacker's MAC(both the entries have same MAC):

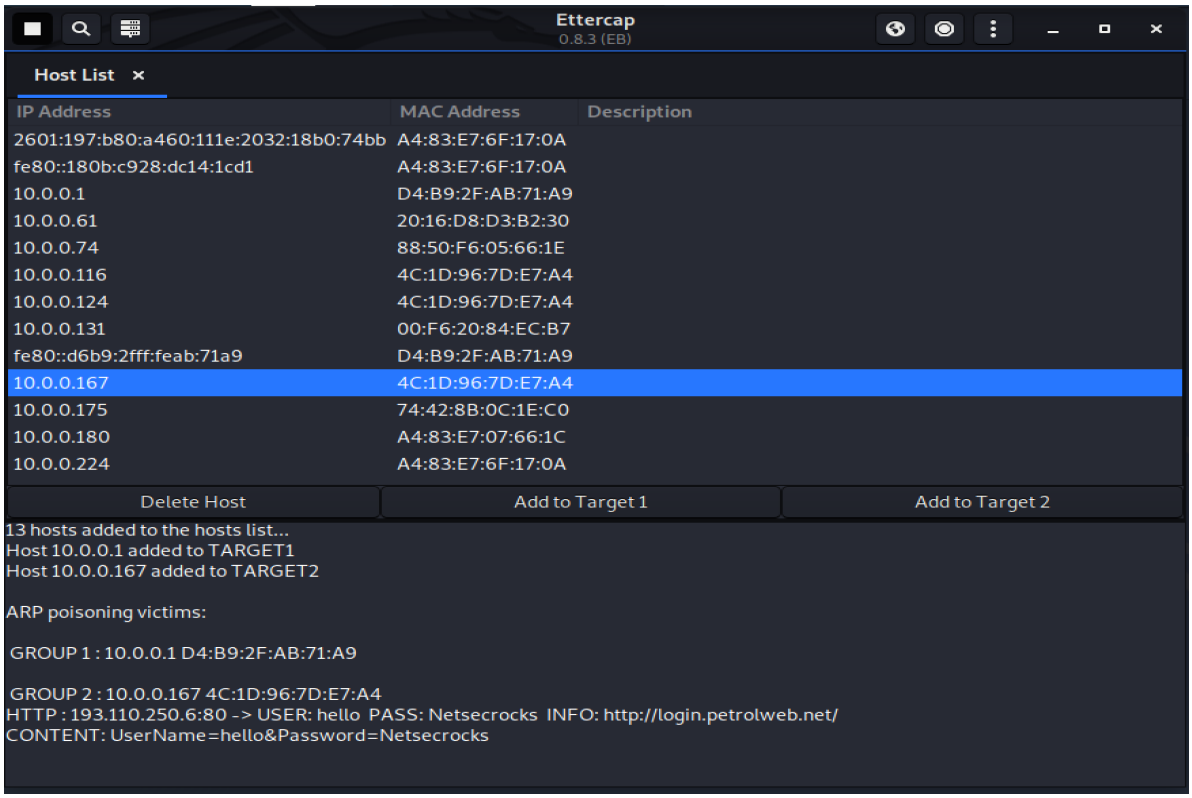


Target Desktop accessing khoury.neu.edu during attack:

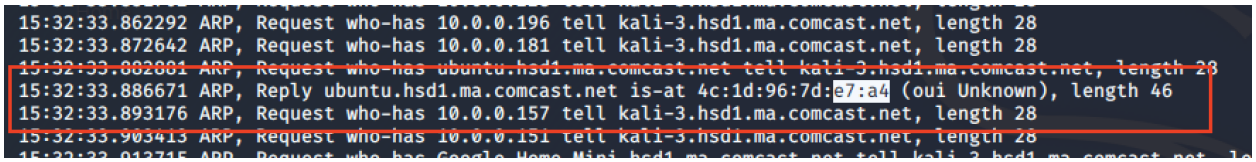


Tcpdump output in kali displaying target IP passing traffic during ARP poisoning:

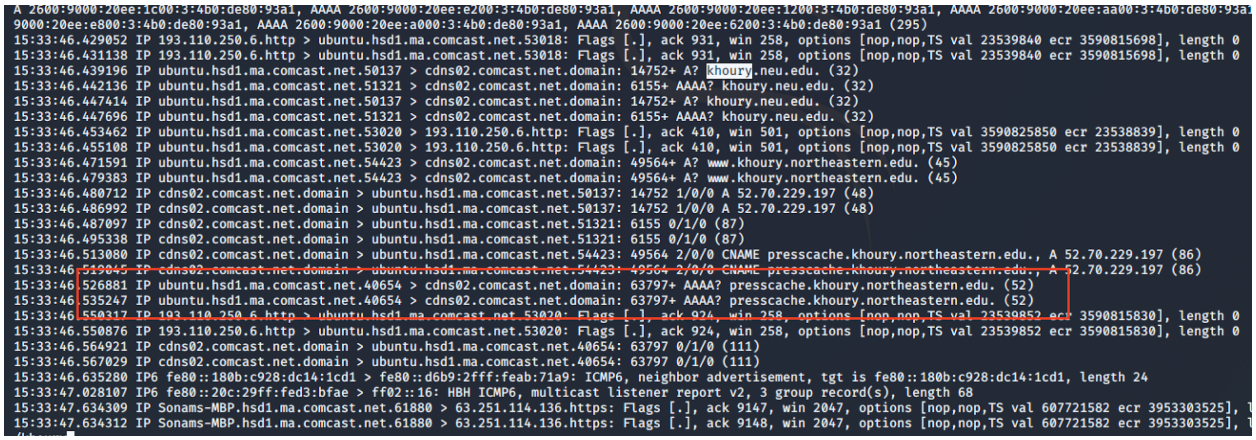
Screenshots showing the target scanned using Ettercap accessing khoury.neu.edu from attacker as gateway:



MAC, as scanned by Ettercap for 10.0.0.167 is 4C:1D:96:7D:E7:A4. The following screenshot shows the name for the listed MAC in tcpdump:



And the screenshot of the victim's request going through system:



References:

[1] https://en.wikipedia.org/wiki/Ettercap_(software)