*Experiment No: 3*

***Aim:*** ARP spoofing using arpwatch

***Theory:***

Arpwatch is a computer software tool for monitoring Address Resolution Protocol traffic on a computer network. It generates a log of observed pairing of IP addresses with MAC addresses along with a timestamp when the pairing appeared on the network. It also has the option of sending an email to an administrator when a pairing changes or is added. Network administrators monitor ARP activity to detect ARP spoofing, network flip-flops, changed and new stations and address reuse. arpwatch was developed by Lawrence Berkeley National Laboratory, Network Research Group, as open-source software and is released under the BSD license.

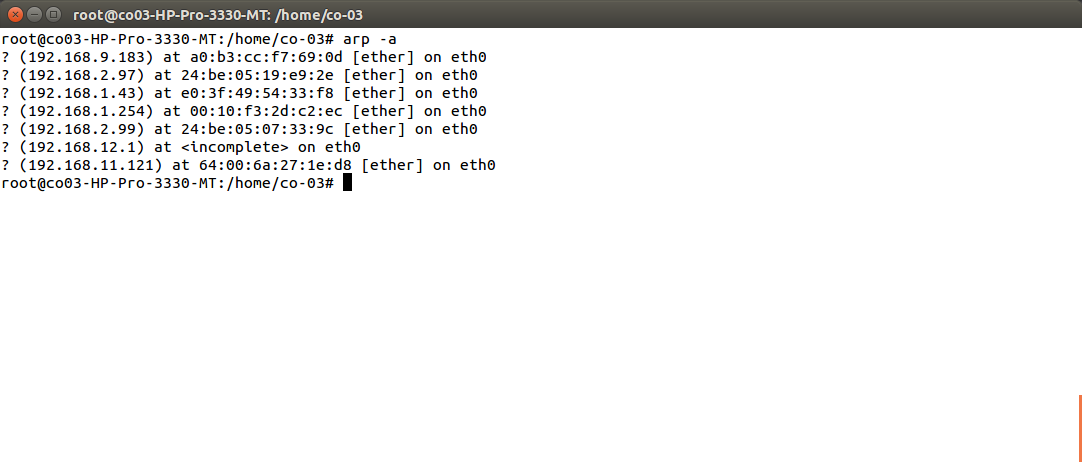
**arpwatch**

**[ -dN** ] [ **-f** *datafile* ] [ **-i** *interface* ][ **-n** *net*[/*width* ]] [ **-r** *file* ] [ **-u** *username* ] [ **-e** *username* ] [ **-s** *username* ] [ **-R** seconds ] [ **-Q** ] [ **-z** ignorenet/ignoremask ]

/etc/init.d/arpwatch start

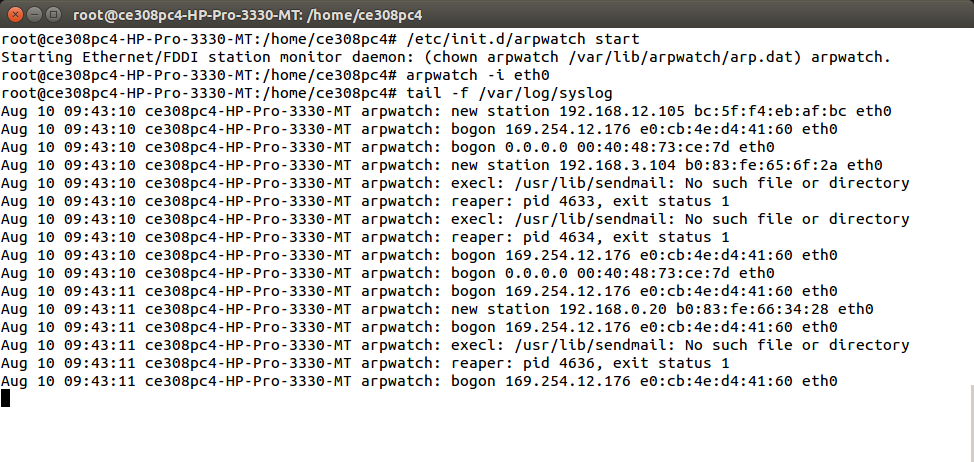


arp -a



arpwatch -i eth0

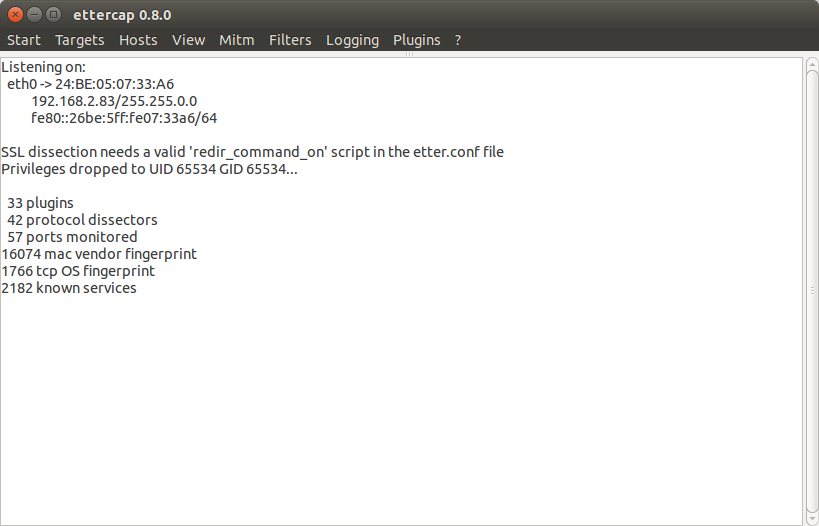
tail -f /var/log/syslog



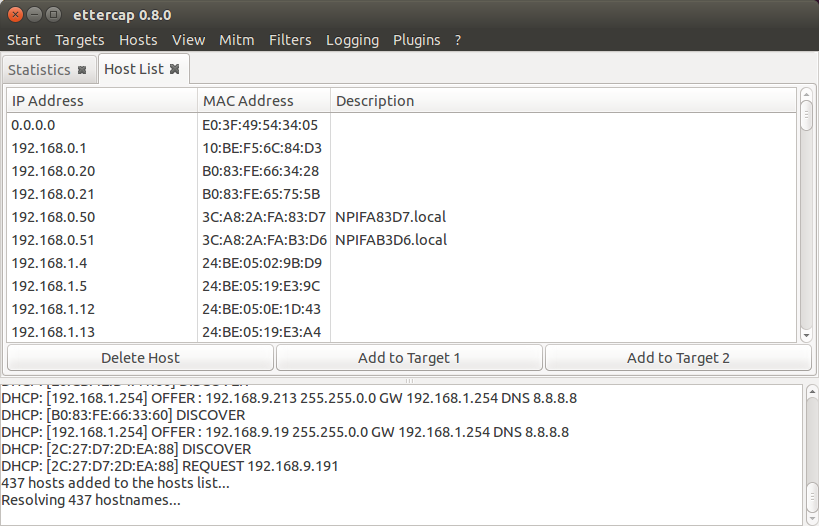
***Ettercap***

Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN. It can be used for computer network protocol analysis and security auditing. It runs on various Unix-like operating systems including Linux, Mac OS X, BSD and Solaris, and on Microsoft Windows. It is capable of intercepting traffic on a network segment, capturing passwords, and conducting active eavesdropping against a number of common protocols.

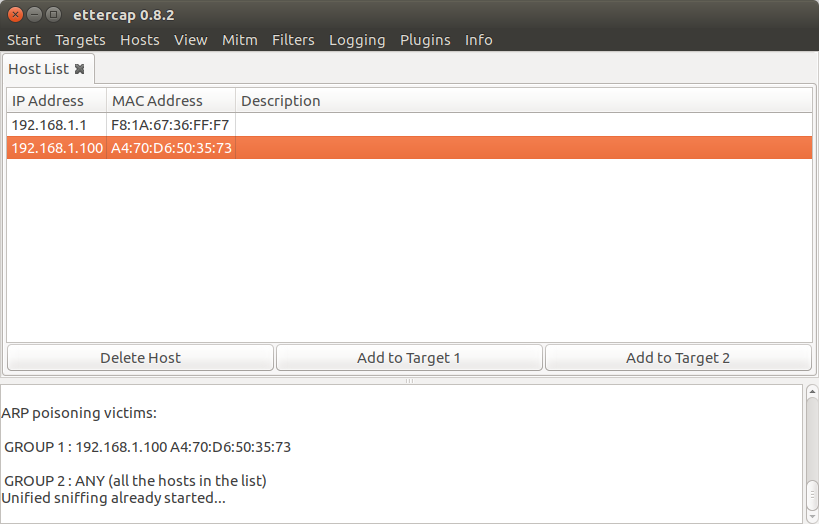
ettercap -G



After Scanning Hosts



After adding host to target list ARP spoofing is started



***Conclusion:*** Thus, we've studied how to implement and detect arp spoofing using arpwatch.