Ettercap Tutorial: DNS Spoofing & ARP Poisoning Examples

by Lakshmanan Ganapathy, http://www.thegeekstuff.com/2012/05/ettercap-tutorial/

Ettercap stands for Ethernet Capture.

Ettercap is a comprehensive suite for man in the middle attacks.

It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

Download and Install

Download the install the Ettercap package from Ettercap. You can also install from the mirror as follows:

```
# apt-get install ettercap-gtk ettercap-common
```

This article explains how to perform DNS spoofing and ARP poisoning using Ettercap tool in Local Area Network (LAN).

Warning: Do not execute this on a network or system that you do not own. Execute this only on your own network or system for learning purpose only. Also, do not execute this on any production network or system. Setup a small network/system for testing purpose and play around with this utility on it for learning purpose only.

Ettercap Basics

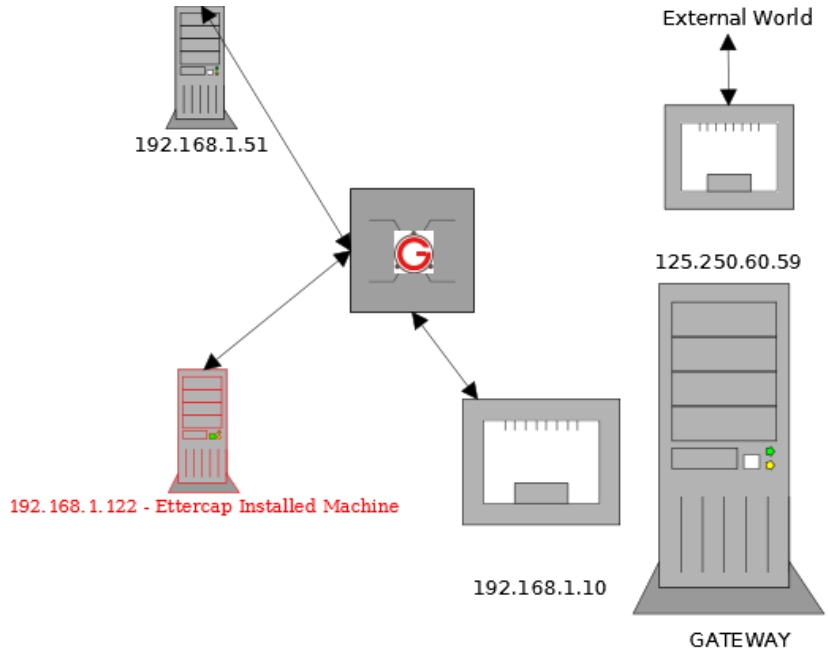
First let's learn some basics about Ettercap. Ettercap has the following 4 types of user interface

- Text Only – '-T' option
- Curses – '-C' option
- GTK – '-G' option
- Daemon – '-D' option

In this article, we will mainly focus on the "Graphical GTK User Interface", since it will be very easy to learn.

Launching an ARP Poisoning Attack

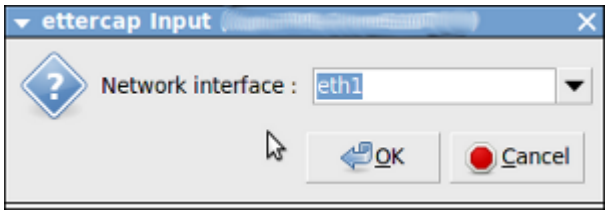
The following diagram explains the network architecture. All the attacks explained here will be performed on the following network diagram only. Using Ettercap in a production environment is not advisable.



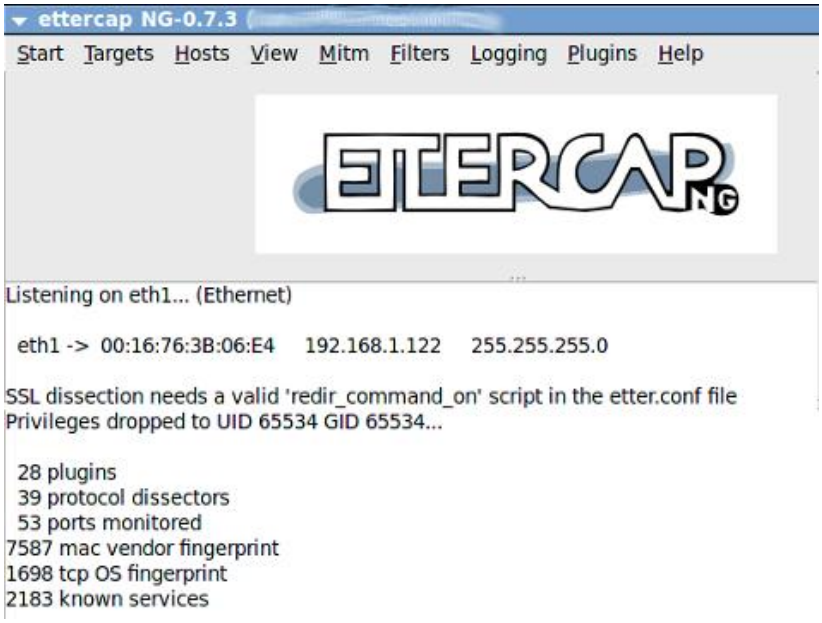
Launch Ettercap using the following command in the 122 machine.

ettercap -G

Click “Sniff->Unified Sniffing”. It will list the available network interface as shown below. Choose the one which you want to use for ARP Poisoning.



Once you have chosen the interface the following window will open:

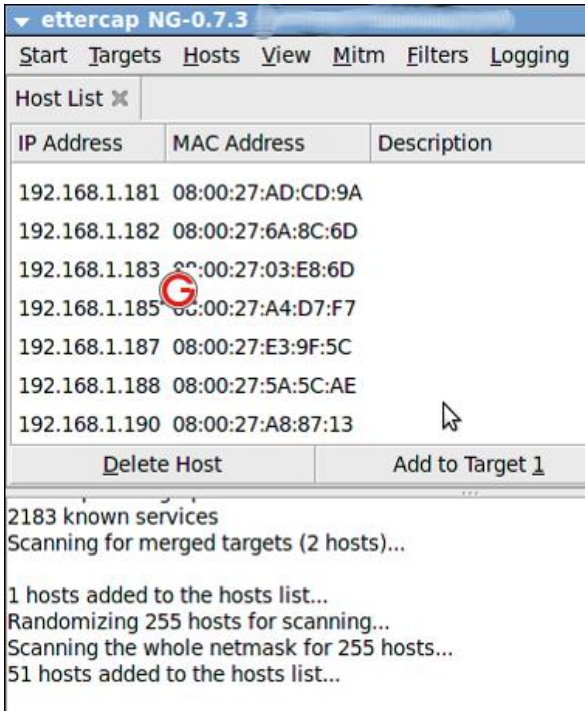


The next step is to add the target list for performing the ARP poisoning. Here we will add 192.168.1.51 and 192.168.1.10 as the target as follows.

Click “Hosts->Scan for Host”.

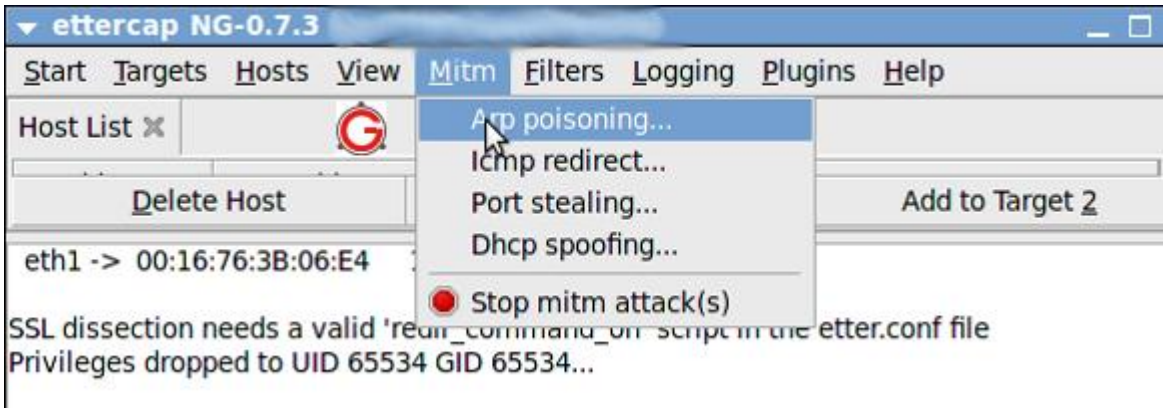
It will start to scan the hosts present in the network.

Once it is completed, click “Hosts->Host List”. It will list the available hosts in the LAN as follows:

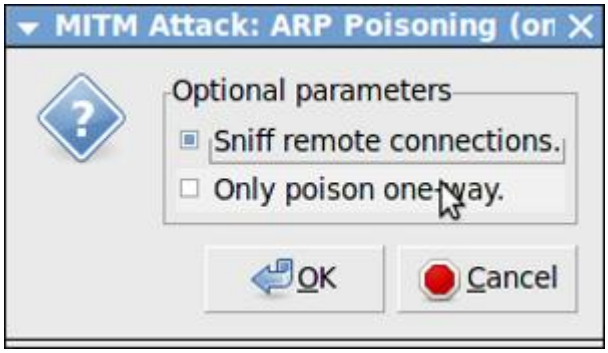


Now among the list, select “192.168.1.51” and click “Add to Target 1” and select “192.168.1.10” and click “Add to Target 2”.

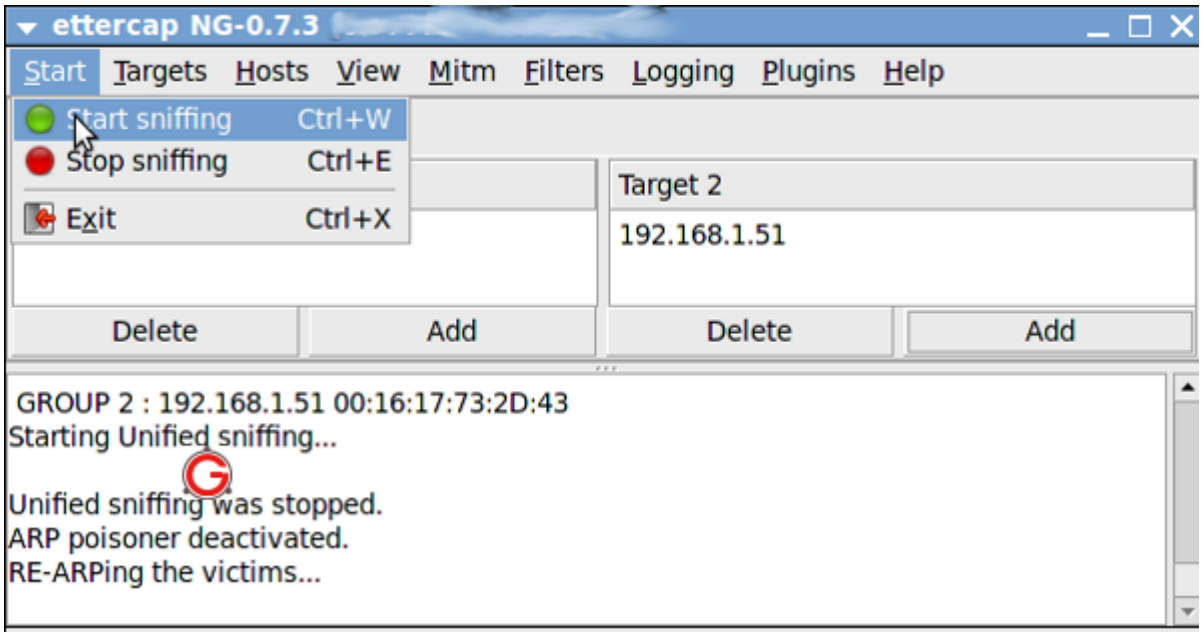
Now select “Mitm->Arp Poisoning” as follows:



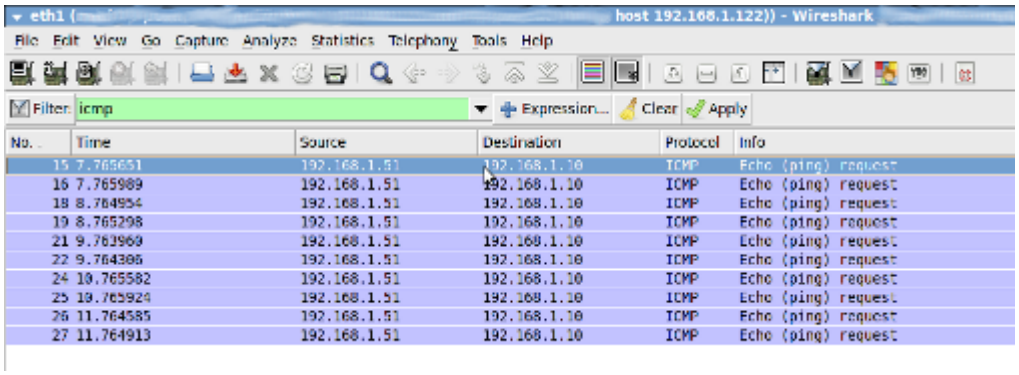
The following dialog box will open. Select “Sniff Remote Connection” and click “ok”:



Then click “Start->Start Sniffing as follows:



Now Arp is poisoned, i.e, the *.122* machine starts to send ARP packets saying “I’m 1.10”. In-order to verify it, from 192.168.1.51 “ping 192.168.1.10”. Open “Wireshark” application in 192.168.1.122 machine, and put a filter for ICMP. You will get the ICMP packets from 192.168.1.51 to 192.168.1.10 in 192.168.1.122 as follows:



Launching DNS Spoofing Attack in LAN

The concept of DNS is as follows.

- Machine A said 'ping google.com'
- Now it has to find that IP address of google.com
- So it queries the DNS server with regard to the IP address for the domain google.com
- The DNS server will have its own hierarchy, and it will find the IP address of google.com and return it to Machine A

Here we will see how we can spoof the DNS.

There are many plugins which comes by default with EtterCap. Once such plugin is called as DNSSpoof. We are going to use that plugin to test the DNS spoofing.

Open the /usr/share/ettercap/etter.dns in the 122 machine and add the following,

*.google.ie A 192.168.1.12

*.google.com A 192.168.1.12

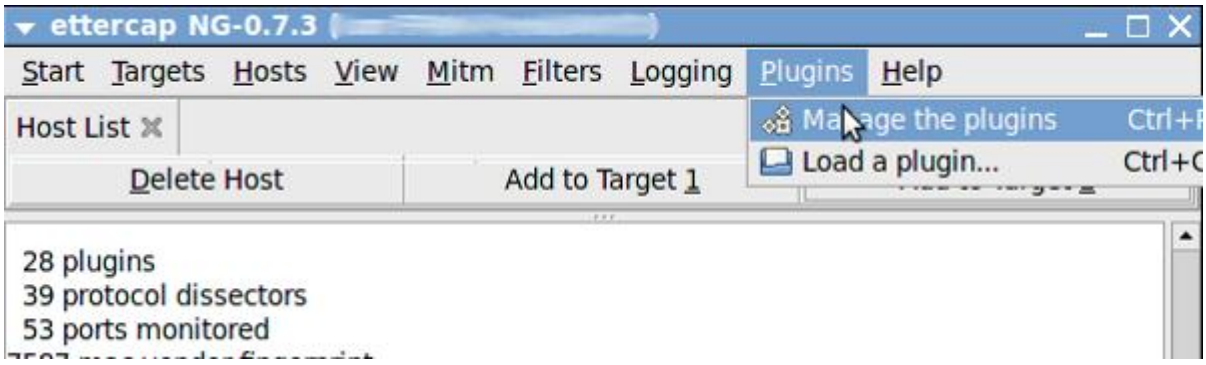
google.com A 192.168.1.12

www.google.com PTR 192.168.1.12

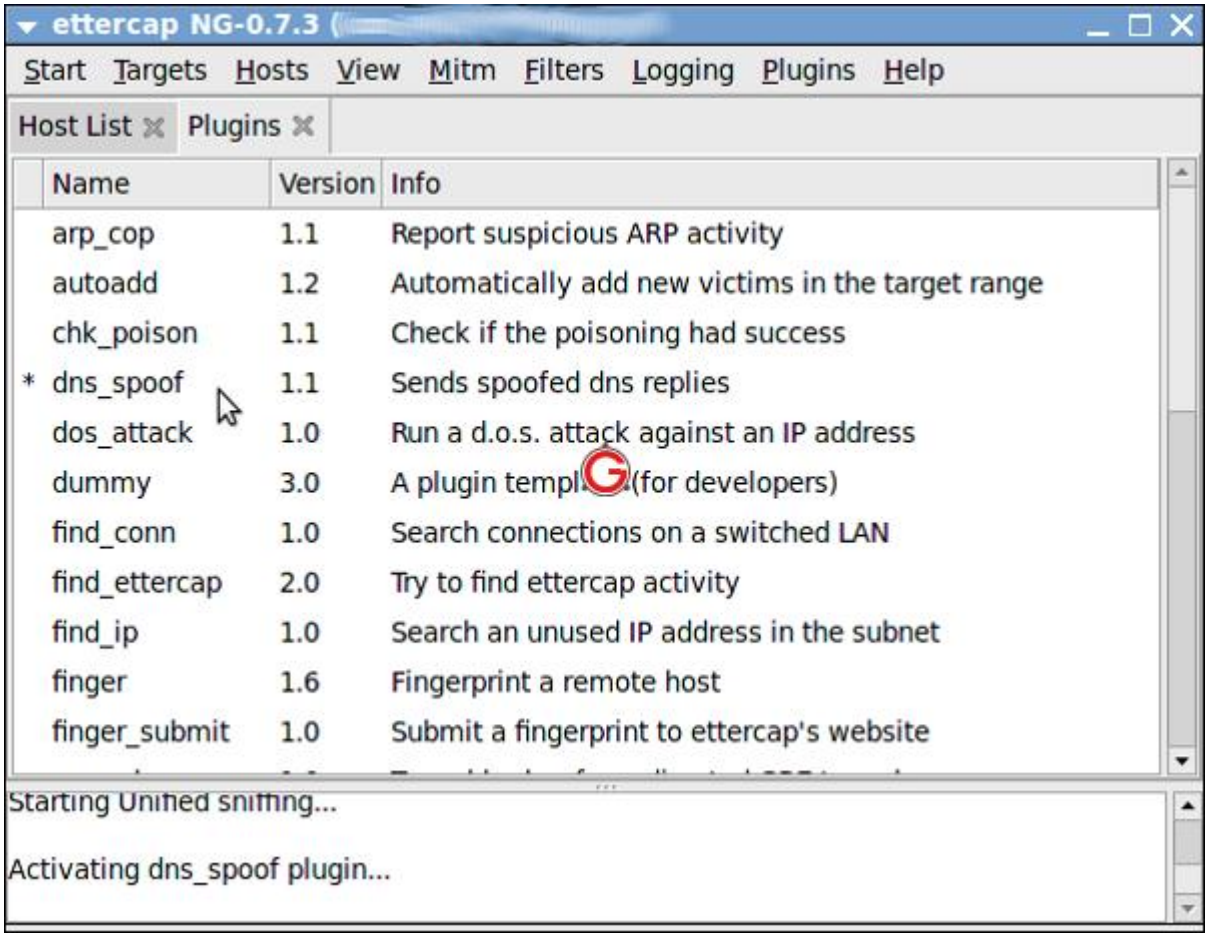
www.google.ie PTR 192.168.1.12

Here, 192.168.1.10 acts as the DNS server. In-order to perform DNS spoofing, first we need to do the ARP poisoning as explained above. Once ARP is done, follow the below steps

Click "Plugins->Manage Plugins" as follows:



Select the "dns_spoof" plugin and double click to activate it as follows:



Now from 192.168.1.51 ping google.com

$ ping google.com

PING google.com (192.168.1.12) 56(84) bytes of data.

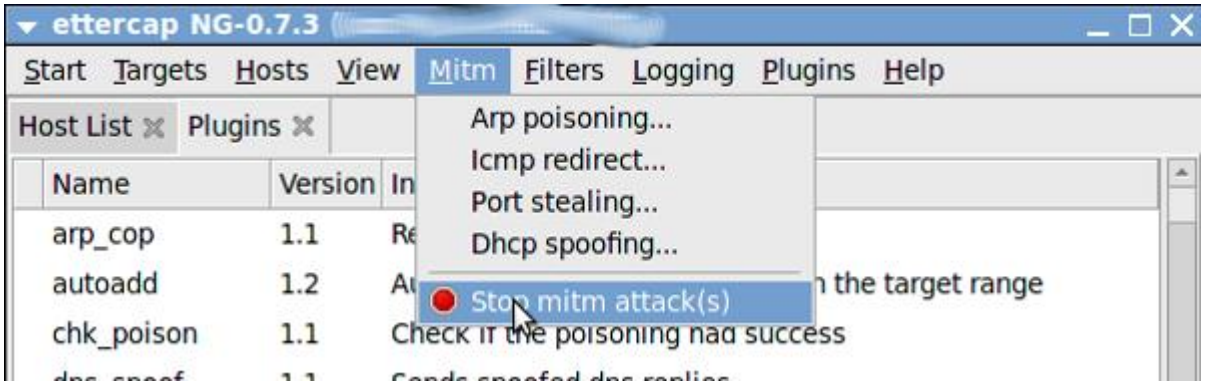
64 bytes from www.google.ie (192.168.1.12): icmp_seq=1 ttl=64 time=3.56 ms

64 bytes from www.google.ie (192.168.1.12): icmp_seq=2 ttl=64 time=0.843 ms

64 bytes from www.google.ie (192.168.1.12): icmp_seq=3 ttl=64 time=0.646 ms

You can see that it returns a local machine's IP address which we have given in the configuration.

Hope this articles provides some insight into ARP Poisoning and DNS Spoofing. Once everything is done, remember to stop MITM attack as follows:



Finally, it doesn't hurt to repeat the warning again. Do not execute this on a network or system that you do not own. Setup a small network/system for testing purpose and play around with this utility on it for learning purpose only.