THE GEEK STUFF
Linux | DB | Open Source | Web

≡ Menu

- Home
- Free eBook
- Start Here
- Contact
- About

Ettercap Tutorial: DNS Spoofing & ARP Poisoning Examples

by Lakshmanan Ganapathy on May 10, 2012

G+1 17 Tweet

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

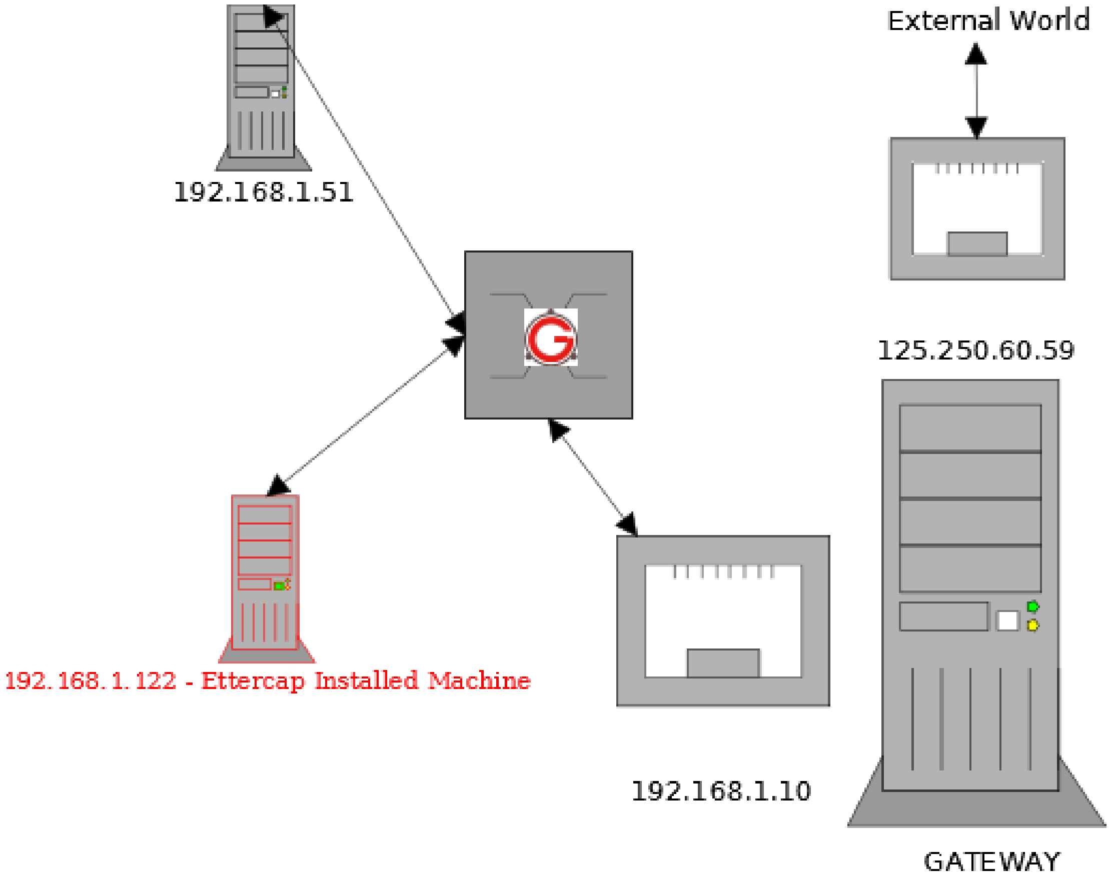
- Text Only – '-T' option
- Curses – '-C' option
- GTK – '-G' option
- Daemon – '-D' option

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

We have already explained about why we need ARP and the conceptual explanation of ARP cache poisoning in ARP-Cache-Poisoning. So please have a look into it, and this article will cover how to perform it practically.

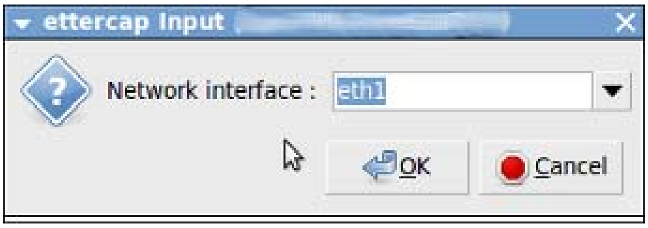
The following diagram explains the network architecture. All the attacks explained here will be performed on the following network diagram only. Using Ettercap in a production environment is not advisable.



Launch Ettercap using the following command in the 122 machine.

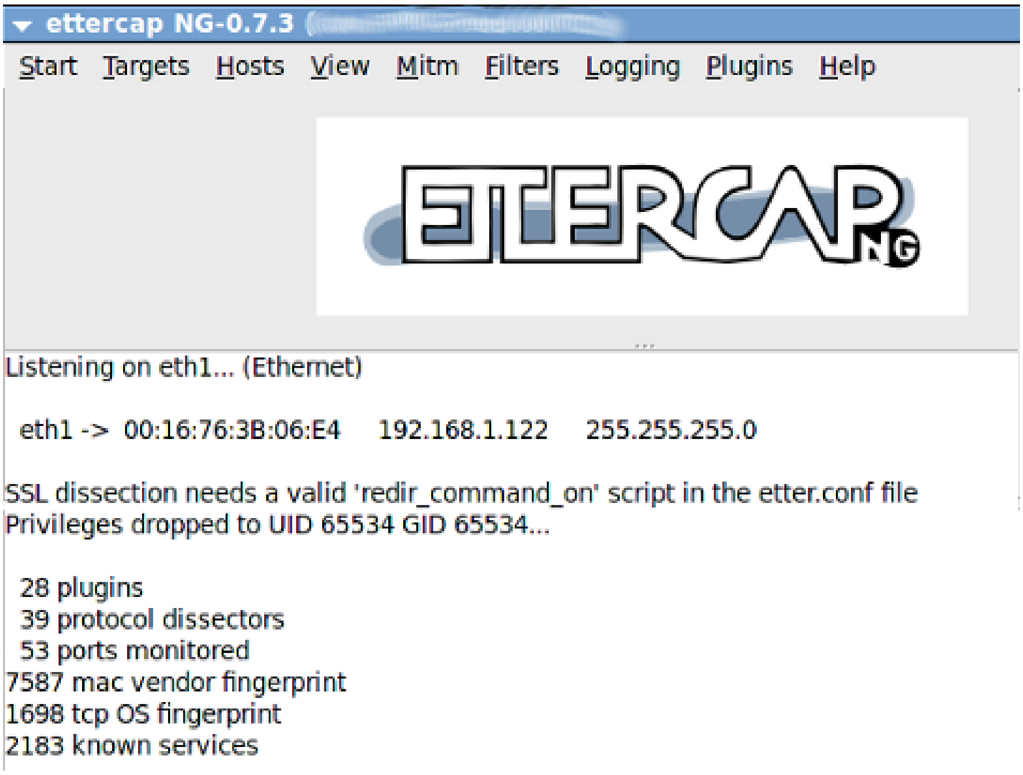
```
# ettercap -G
```

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.



Network interface : eth1

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



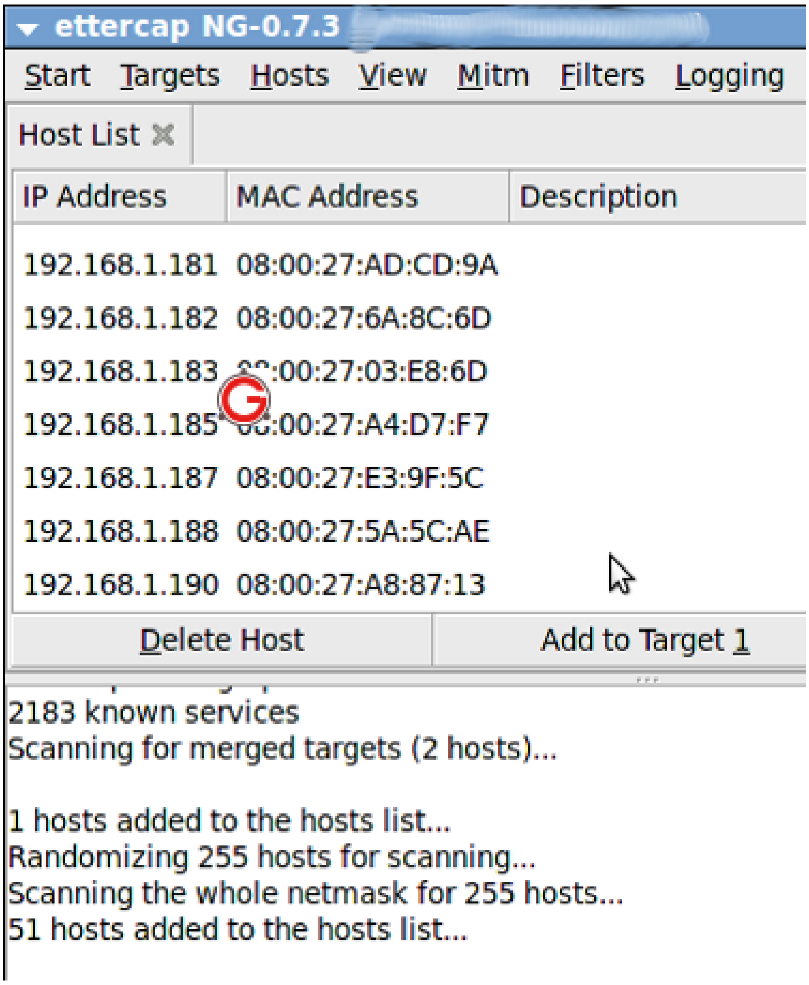
```
Listening on eth1... (Ethernet)

  eth1 -> 00:16:76:3B:06:E4    192.168.1.122    255.255.255.0

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...

  28 plugins
  39 protocol dissectors
  53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
```

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:

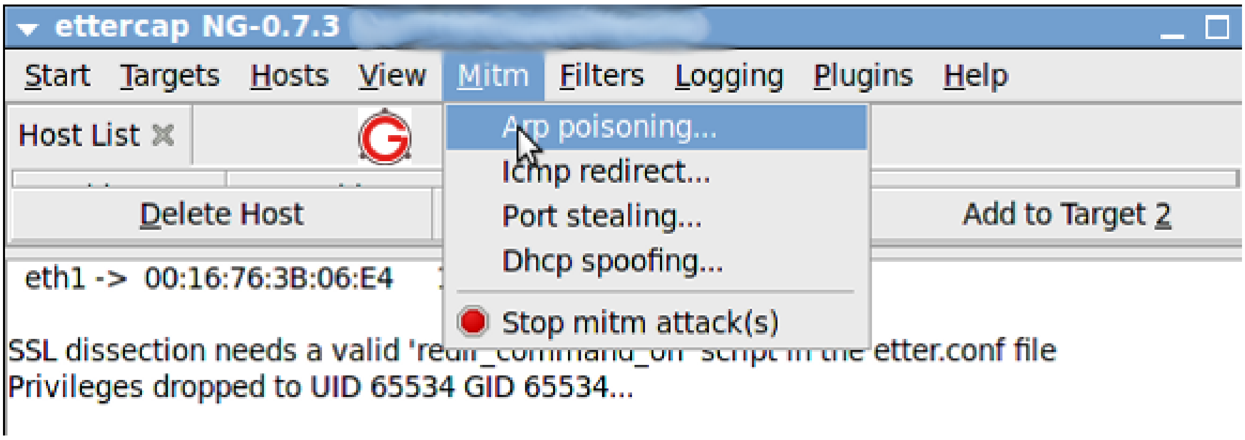


IP Address	MAC Address	Description
192.168.1.181	08:00:27:AD:CD:9A	
192.168.1.182	08:00:27:6A:8C:6D	
192.168.1.183	08:00:27:03:E8:6D	
192.168.1.185	08:00:27:A4:D7:F7	
192.168.1.187	08:00:27:E3:9F:5C	
192.168.1.188	08:00:27:5A:5C:AE	
192.168.1.190	08:00:27:A8:87:13	

```
2183 known services
Scanning for merged targets (2 hosts)...

1 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
51 hosts added to the hosts list...
```

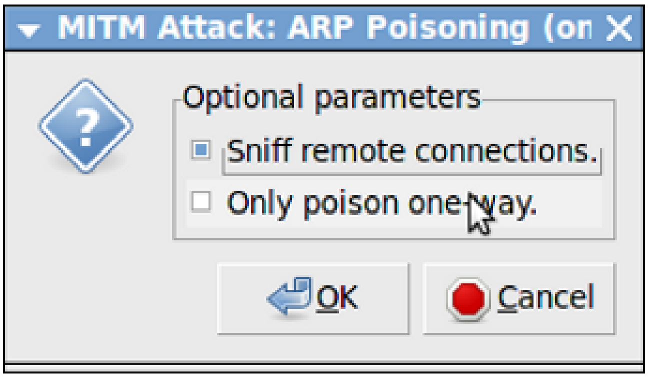
Now among the list, select “192.168.1.51” and click “Add to Target 1” and select “192.168.1.10” and click “Add to Target 2”.

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



```
eth1 -> 00:16:76:3B:06:E4

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...
```

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

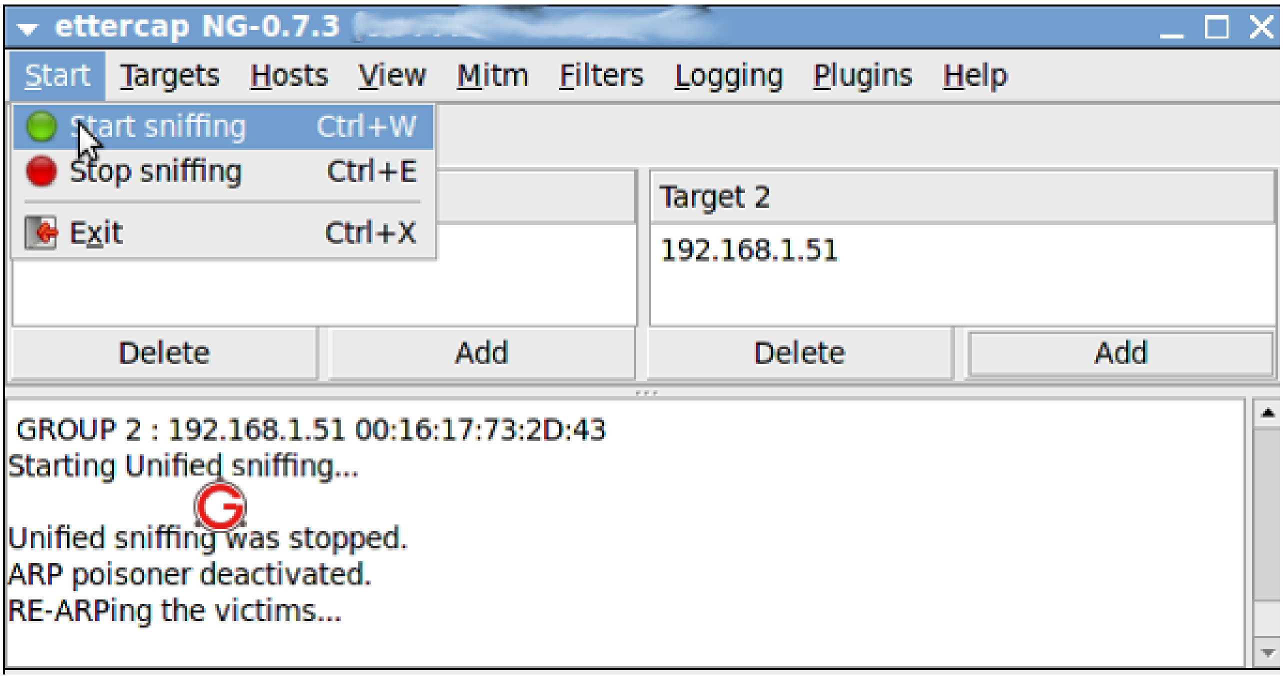


Optional parameters

☑ Sniff remote connections.

□ Only poison one-way.

Then click “Start->Start Sniffing as follows:

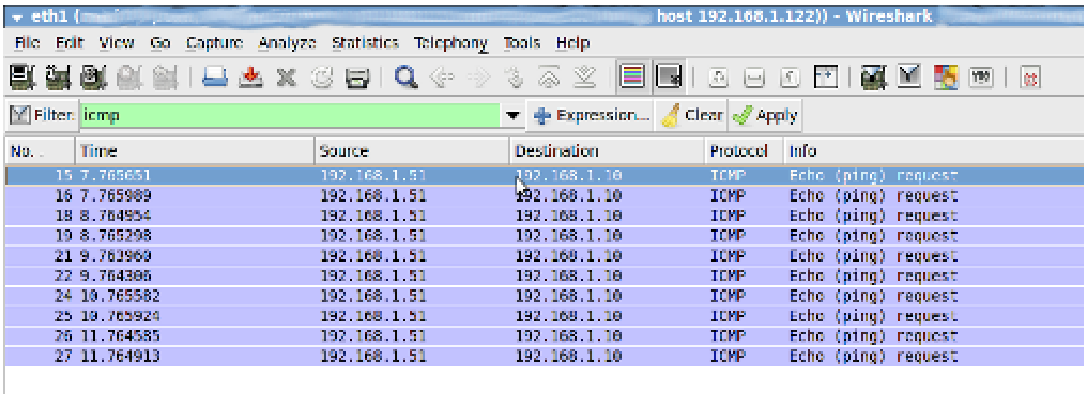


Target 2

192.168.1.51

```
GROUP 2 : 192.168.1.51 00:16:17:73:2D:43
Starting Unified sniffing...

Unified sniffing was stopped.
ARP poisoner deactivated.
RE-ARPing the victims...
```

Now Arp is poisoned, i.e, 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:



Filter: icmp

No.	Time	Source	Destination	Protocol	Info
15	7.765651	192.168.1.51	192.168.1.10	ICMP	Echo (ping) request
16	7.765989	192.168.1.51	192.168.1.10	ICMP	Echo (ping) request
18	8.764954	192.168.1.51	192.168.1.10	ICMP	Echo (ping) request
19	8.765298	192.168.1.51	192.168.1.10	ICMP	Echo (ping) request
21	9.763960	192.168.1.51	192.168.1.10	ICMP	Echo (ping) request
22	9.764306	192.168.1.51	192.168.1.10	ICMP	Echo (ping) request
24	10.765582	192.168.1.51	192.168.1.10	ICMP	Echo (ping) request
25	10.765924	192.168.1.51	192.168.1.10	ICMP	Echo (ping) request
26	11.764585	192.168.1.51	192.168.1.10	ICMP	Echo (ping) request
27	11.764913	192.168.1.51	192.168.1.10	ICMP	Echo (ping) request

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.

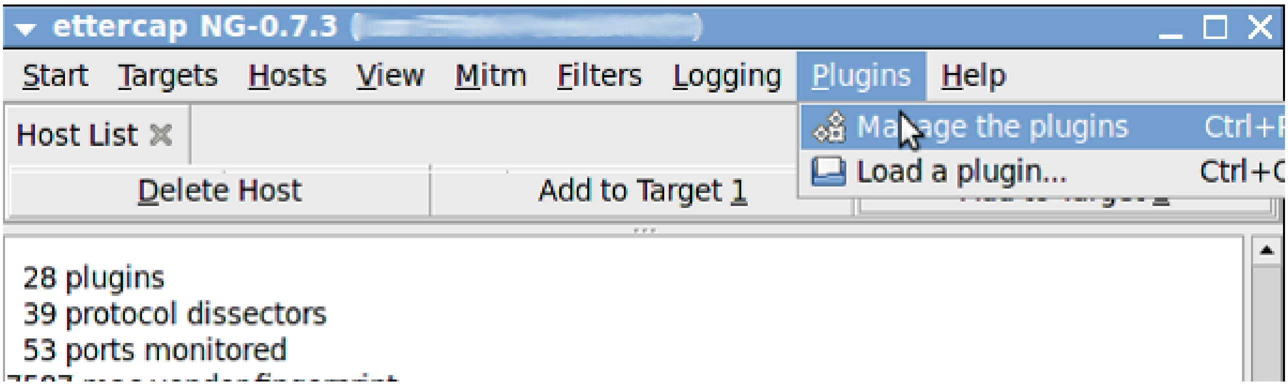
There are many plugins which comes by default with EtterCap. Once such plugin is called as DNSSpoof. We are going to use that plugin to test the DNS spoofing.

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

```
*.google.co.in 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.co.in PTR 192.168.1.12
```

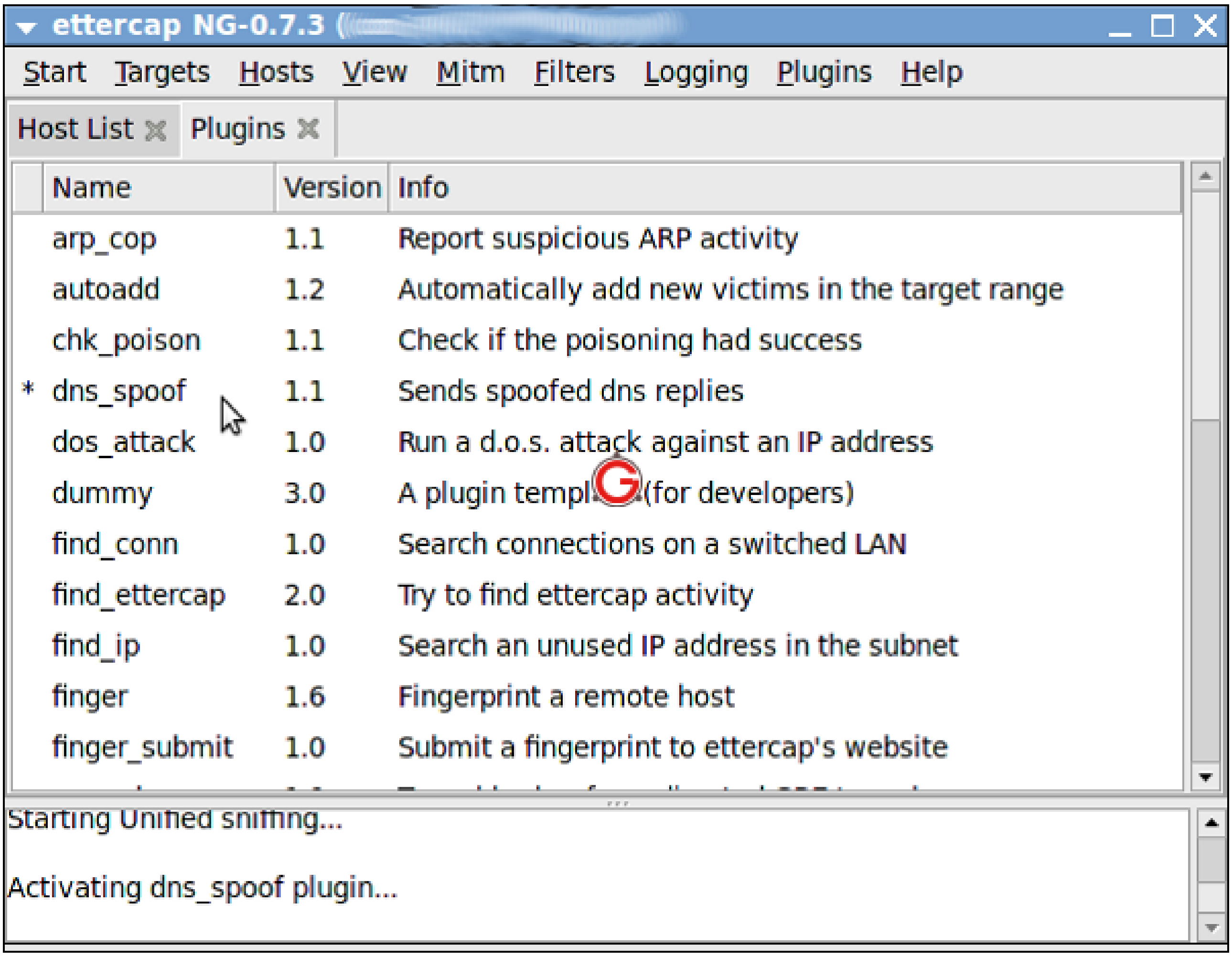
Here, 192.168.1.10 acts as the DNS server. In-order to perform DNS spoofing, first we need to do the ARP poisoning as explained above. Once ARP is done, follow the below steps

Click “Plugins->Manage Plugins” as follows:



```
28 plugins
39 protocol dissectors
53 ports monitored
```

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



	Name	Version	Info
	arp_cop	1.1	Report suspicious ARP activity
	autoadd	1.2	Automatically add new victims in the target range
	chk_poison	1.1	Check if the poisoning had success
*	dns_spoof	1.1	Sends spoofed dns replies
	dos_attack	1.0	Run a d.o.s. attack against an IP address
	dummy	3.0	A plugin templ (for developers)
	find_conn	1.0	Search connections on a switched LAN
	find_ettercap	2.0	Try to find ettercap activity
	find_ip	1.0	Search an unused IP address in the subnet
	finger	1.6	Fingerprint a remote host
	finger_submit	1.0	Submit a fingerprint to ettercap's website

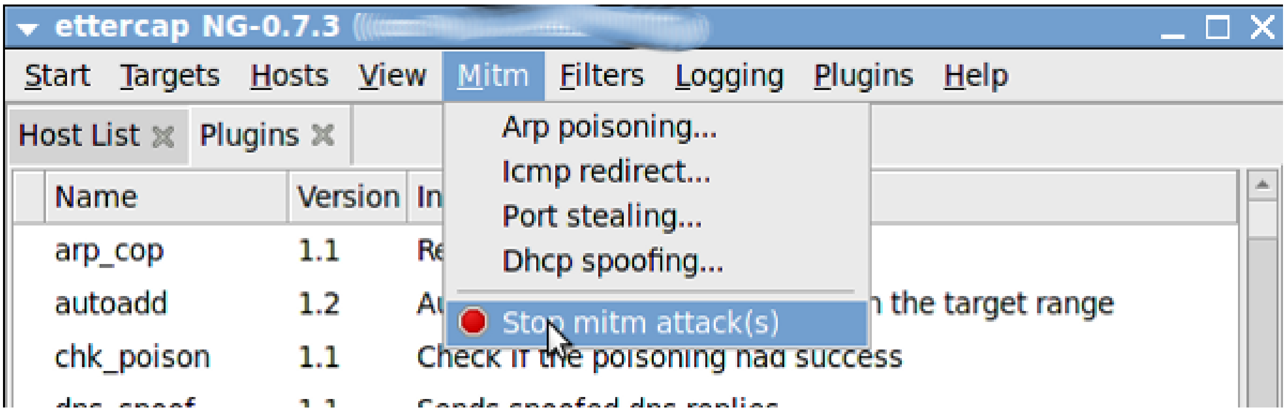
```
Starting Unified sniffing...

Activating dns_spoof plugin...
```

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.co.in (192.168.1.12): icmp_seq=1 ttl=64 time=3.56 ms
64 bytes from www.google.co.in (192.168.1.12): icmp_seq=2 ttl=64 time=0.843 ms
64 bytes from www.google.co.in (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:



Name	Version	In
arp_cop	1.1	Re
autoadd	1.2	Au … n the target range
chk_poison	1.1	Check if the poisoning had success

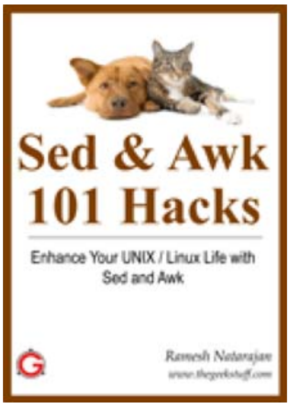
Finally, it doesn’t hurt to repeat the warning again. Do not execute this on a network or system that you do not own. Setup a small network/system for testing purpose and play around with this utility on it for learning purpose only.

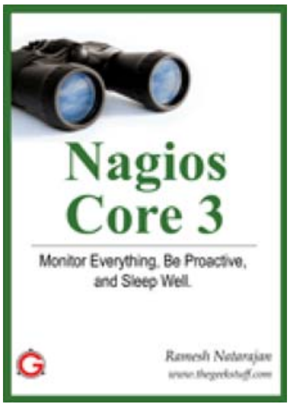
G+1 17 Tweet > Add your comment

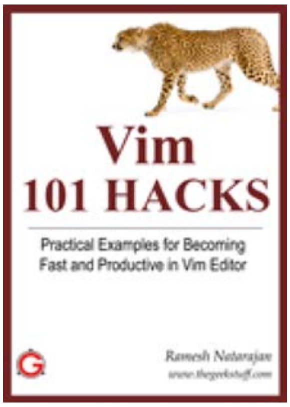
If you enjoyed this article, you might also like..

1. 50 Linux Sysadmin Tutorials
2. 50 Most Frequently Used Linux Commands (With Examples)
3. Top 25 Best Linux Performance Monitoring and Debugging Tools
4. Mommy, I found it! – 15 Practical Linux Find Command Examples
5. Linux 101 Hacks 2nd Edition eBook Free

- Awk Introduction – 7 Awk Print Examples
- Advanced Sed Substitution Examples
- 8 Essential Vim Editor Navigation Fundamentals
- 25 Most Frequently Used Linux IPTables Rules Examples
- Turbocharge PuTTY with 12 Powerful Add-Ons






Vim
101 HACKS
Practical Examples for Becoming Fast and Productive in Vim Editor
Ramesh Natarajan
www.thegeekstuff.com

{ 18 comments… add one }

- Jalal Hajigholamali May 10, 2012, 8:26 pm

  Hi,

  Very useful article

  Thanks a lot…

  Link
- deepak May 11, 2012, 12:37 am

  Can "ARP Poisoning" be done in wireless network ?

  Link
- Rajesh May 11, 2012, 9:25 pm

  Nice one.
  Thanks for this knowledge.

  thnaks
  Rajesh

Link

- mumus May 12, 2012, 12:45 pm

  Hi !

  Can we detect this type of attacks with SNORT ?

  Thanks

  Link
- Shakil May 12, 2012, 9:24 pm

  Why am I not able to select wlan interface for sniffing. Is it the Support for drivers(ettercap drivers) to work promiscuous is not integrated? Same thing I have observed for wireshark. Wlan is there for quite sometime but still I don't find any sniffing tool which works with wlan. Is there any complexity in making wireless lan work with sniffer?

  Thanks in advance.

  Link
- Shakil May 13, 2012, 3:14 am

  Thanks for the wonderful article. Keep up the good work.

  Link
- Lakshmanan Ganapathy May 14, 2012, 12:11 am

  @Shakil,

  I don't have a wireless lan with me. So I've never experimented it.

  @mumus

  I've not tried it. There are other tools which helps to detect the ARP poisoning. You can also try "arpalert".

  Link
- Vasudev May 24, 2012, 10:56 pm

  Very useful article. Thanks a lot for sharing such knowledgeable things. Keep up.

  Link
- joand May 25, 2012, 1:49 pm

  hi. i have virtual machine backtrack OS .and i do successfully mitm on my window xp….and got all the ssl logs… in Lan all successful execute as i say i have two ip ..lan is .192.168.1.x…and wan ip is 122.145.23.x like that..scan wan ip i got result many host ip live . …here is the question how can i redirect all outgoing and incoming traffic of these wan ip's through my host computer..
  2. or any other way to find host computers in my network as in my lan i am alone

  Link

- syarif July 19, 2012, 9:47 pm

  From what i know is, the wlan need to support monitor mode so u able to MITM.

  Link
- SuB September 3, 2012, 6:08 am

  What OS this tutorial is about?

  There is not /usr/share/ettercap/etter.dns in my Linux Backtrack 5 R2 !!!

  Link
- @SuB September 10, 2012, 8:27 pm

  @SuB In Backtrack try /usr/local/share/ettercap/etter.dns

  Link
- Tim December 30, 2013, 12:22 am

  @Sub also try the command :> locate etter.dns

  Link
- Amit Patel December 31, 2014, 10:27 pm

  Can you please let me know the spoofing with the DNS? DHCP restricts it to access.

  Link
- lenci February 10, 2015, 3:54 am

  ty very much

  Link
- Amrita February 11, 2015, 12:27 am

  @Shakil,

  for Wireshark have you spawned the process as root? Otherwise you may not find any interfaces for sniffing. It also does work with wireless; once you start the capture on your wireless interface you should see packets start appearing.

  Link
- amber May 12, 2015, 5:24 am

  I am using a kali and did changed the etter.dns for gmail to my ip but while i open with firefox at the client the firefox does not open to the neither of the page neither official gmail nor to my ip host server it shows certificate error of hsts and also didn’t work with chrome also.

  Link
- alex April 16, 2016, 3:20 am

  why am i not able to select an interface for sniffing same thing for wireshark

Link

Leave a Comment

Name

Email

Website

Comment

Submit

□ Notify me of followup comments via e-mail

Next post: Intro to DOCSIS Architecture, CM CMTS Protocol for Cable Modems

Previous post: 5 UNIX / Linux Traceroute Command Examples

RSS | Email | Twitter | Facebook | Google+

Search

POPULAR POSTS

- 12 Amazing and Essential Linux Books To Enrich Your Brain and Library
- 50 UNIX / Linux Sysadmin Tutorials
- 50 Most Frequently Used UNIX / Linux Commands (With Examples)
- How To Be Productive and Get Things Done Using GTD
- 30 Things To Do When you are Bored and have a Computer
- Linux Directory Structure (File System Structure) Explained with Examples
- Linux Crontab: 15 Awesome Cron Job Examples
- Get a Grip on the Grep! – 15 Practical Grep Command Examples
- Unix LS Command: 15 Practical Examples
- 15 Examples To Master Linux Command Line History
- Top 10 Open Source Bug Tracking System
- Vi and Vim Macro Tutorial: How To Record and Play
- Mommy, I found it! -- 15 Practical Linux Find Command Examples
- 15 Awesome Gmail Tips and Tricks
- 15 Awesome Google Search Tips and Tricks
- RAID 0, RAID 1, RAID 5, RAID 10 Explained with Diagrams
- Can You Top This? 15 Practical Linux Top Command Examples
- Top 5 Best System Monitoring Tools
- Top 5 Best Linux OS Distributions
- How To Monitor Remote Linux Host using Nagios 3.0
- Awk Introduction Tutorial – 7 Awk Print Examples
- How to Backup Linux? 15 rsync Command Examples
- The Ultimate Wget Download Guide With 15 Awesome Examples
- Top 5 Best Linux Text Editors
- Packet Analyzer: 15 TCPDUMP Command Examples
- The Ultimate Bash Array Tutorial with 15 Examples
- 3 Steps to Perform SSH Login Without Password Using ssh-keygen & ssh-copy-id
- Unix Sed Tutorial: Advanced Sed Substitution Examples
- UNIX / Linux: 10 Netstat Command Examples
- The Ultimate Guide for Creating Strong Passwords
- 6 Steps to Secure Your Home Wireless Network
- Turbocharge PuTTY with 12 Powerful Add-Ons

CATEGORIES

- Linux Tutorials
- Vim Editor

- Sed Scripting
- Awk Scripting
- Bash Shell Scripting
- Nagios Monitoring
- OpenSSH
- IPTables Firewall
- Apache Web Server
- MySQL Database
- Perl Programming
- Google Tutorials
- Ubuntu Tutorials
- PostgreSQL DB
- Hello World Examples
- C Programming
- C++ Programming
- DELL Server Tutorials
- Oracle Database
- VMware Tutorials

Ramesh Natarajan

G+ 关注

About The Geek Stuff

My name is Ramesh Natarajan. I will be posting instruction guides, how-to, troubleshooting tips and tricks on Linux, database, hardware, security and web. My focus is to write articles that will either teach you or help you resolve a problem. Read more about Ramesh Natarajan and the blog.

Contact Us

Email Me : Use this Contact Form to get in touch me with your comments, questions or suggestions about this site. You can also simply drop me a line to say hello!.

Follow us on Google+

Follow us on Twitter

Become a fan on Facebook

Support Us