Ettercap DNS Redirection Tutorial

Written by: Finn Orfano • Edited by: Bill Bunter
Updated Feb 4, 2011 • Related Guides: Ip Address | BBC | Configuration File

One of Ettercap's most powerful plugins allows attackers to redirect web traffic on their local network. This can be used to phish passwords or to trick users into downloading malicious software. Find out what methods attackers use and what you can do to protect yourself inside.

Ettercap & Plugins

Ettercap is a powerful and expandable network sniffer. Most of this expandability is derived from its plugins. Today we are going to use the 'dns-spoof' plugin to redirect web traffic on a target machine. If you have no previous experience with Ettercap, you should take a look at my previous tutorial on the basics of network sniffing with Ettercap.

An Example Configuration

Before we launch our dns redirection attack we need to edit the dns-spoof plugin's configuration file located at '/usr/share/ettercap/etter.dns'.

Glancing at the top of the configuration file we can see the following example.

microsoft.com A 198.182.196.56

**.microsoft.com A 198.182.196.56*

This is an A-query (note the A) that redirects the domain name microsoft.com to the former IP address of linux.org. The first entry for 'microsoft.com' redirects the main domain, whereas the second entry '*.microsoft.com' uses a wildcard to redirect the traffic from all of microsoft.com's subdomains (e.g. downloads.microsoft.com).

Setting up the Redirect

For the sake of an example, lets say that we wanted to redirect cnn.com to bbc.co.uk. First we need the ip address of bbc.co.uk. There are a number of ways to find this, but the easiest is to use the 'host' command.

host bbc.co.uk

This returns the IP address of BBC as '212.58.224.138'. Armed with this knowledge we can add the following lines to our etter.dns configuration file.

cnn.com A 212.58.224.138

*.cnn.com A 212.58.224.138

Starting Ettercap

Now, having configured etter.dns we can begin our attack. Start ettercap in its graphical mode with

ettercap -G

If you need any more information on starting Ettercap (and if you need to use it on a WEP key protected network), you should glance at my previous tutorial.

Start sniffing by clicking Sniff >> Unified Sniffing and typing in the name of the interface you want to use. If you don't know what your interface, try the default then check what interfaces are active using 'ifconfig' and 'iwconfig'. The next step is to scan for hosts: Hosts >> Scan for hosts and choose targets: Hosts >> Host list. Select the router as target 1 and any other clients you want to attack as target 2.

To start capturing and redirecting traffic we need to ARP poison the network so click on Mitm >> Arp Poisoning to begin. Now click Start >> Start sniffing.

Enabling the Plugin

To continue, we need to enable the dns-spoof plugin. In the menu select Plugins >> Manage plugins to open the plugins panel. Double clicking on a plugin activates it, so go ahead and double click on dns-spoof.

Now test your configuration! When the target machine browses to cnn.com they should be greeted by bbc.co.uk.

Here is what the clients will see when they attempt to access CNN.

But wait... that's not the BBC homepage. What's the problem? BBC hosts numerous sites and services under that same IP address so is not able to resolve it directly to the BBC homepage. This was an intentionally imperfect tutorial as this is one of the most common problems you will run into when redirecting addresses. There is no simple solution to this problem, so before redirecting it is always best to see what the IP will resolve to (i.e. we should have browsed to the ip address in our web browser and checked the output).

What next?

So has redirecting CNN accomplished for us? Not much. For dns-redirection to be an effective attack strategy we need to redirect to something more malicious. By far the most common use of dns-spoofing is to redirect to an executable hosted by the attacker and trick the client into running it. Expect a tutorial on the practical applications of dns-spoofing soon!

If you enjoyed this article, be sure to check out Bright Hub's Wireshark Sniffing, Ettercap Wifi Sniffing and WIFI WEP Cracking tutorials!

NEXT ARTICLE »

WE ALSO RECOMMEND...

- **WiFi Security in a Few Easy Steps**
- **Security and Penetration Testing with Backtrack Linux**
- **Does BackTrack Have the Security Testing Tools You Need?**
- **Easy Hack - Why WEP Is a Bad Idea for Your Network**
- **Secure Connection Tips for the iPad**

Like

Add New Comment

Post as ...

Showing 3 comments

Sort by Popular now ▼ Subscribe by email Subscribe by RSS

Real-time updating is **paused**. (Resume)

KDragon 1 year ago

this is only for dns spoofing if you want to have the victim go to google.com and have it download a file that would be up to the web server that you point to with the ip address.

Like Reply

ME 2 years ago

Haven't tried this, but try changing etter.dns so that it has line like the following:

*/path/to/the/download.mp3 A ip.ad.dr.es

or

*website/path/to/download.mp3 A ip.ad.dr.es

Like Reply

tom 2 years ago

works well, thanks, but what if you wanted to redirect to a certain url download link, i.e .../.../music/song.mp3?

would you just change the ip address for the actual link?

many thanks

Like Reply

blog comments powered by **DISQUS**

©2012 Bright Hub Inc. All rights reserved.