

Forum:[Hack Forums](#)

Thread: [DNS spoofing tutorial](#)

Middle - January 4, 2011, 1:58 pm

Hello and welcome to another tutorial on wireless networks, although today this method can be used on wired networks as well!

Me and ac1dxtrem may one day incorporate all of our tutorials and scripts in to an ebook/bundle of sorts, we are unclear on what it will be but we know that we want to do something so we are outputting lots of stuff that you guys might find interesting and useful!

Ok so today's attack will be performed on my home wireless router, and I will be using Ubuntu 10.10 to perform the attack. I have just installed Ubuntu 10.10 so i will cover the packages that need to be installed to get this working as i have to do it myself!

If you are on Backtrack then these tools will already be included in your files so no need to worry about installation.

About the attack

ac1dxtrem has made a thread about the basics of this attack so i suggest you read that first; you can find it [here](#)

If you aren't that interested in the theory and just want to know how this attack can be done, then firstly i highly recommend you rethink your attitude towards hacking and secondly here is a very basic introduction to what will be done.

This is a very simple attack and you can make a bash script that performs it in 5 lines of code, and it is relatively easy to set up. What the end result of a DNS spoofing attack does is redirect all of the traffic on a network to a different IP address. So people trying to access "www.google.com" (173.194.37.104) will be redirected to XX.XX.XX.XX and you get to define that IP address.

What will we use?

To do this we will use a program called ettercap; ettercap is a utility that allows users an easy method of performing MITM attacks. Today though we are interested in the DNS spoofing capabilities of ettercap's DNS spoof plugin. This is very simple to set up although depending on what you want to do you can make it harder or easier.

Why will we use it?

Well first and foremost i think is simply 'teh lulz'. What i mean by this is that you can redirect all of the traffic on a network to a web page, and that web page could be a shock website, or a deface page, the ides of this is just to pwn a network and see the amount of humour that would arise. This is also quite a good thing to do as it isn't going to get you in as much trouble as some of the other methods. This is also easier to set up than other methods.

Another technique that uses DNS spoofing, is one that redirects traffic to a web page that prompts the user to download a "file". The file if of course your RAT/Keylogger/Stealer/Bot. There is already a detailed tutorial about this technique written by SB91 [here](#)

However the most infamous method is one that involves phishing. As this is against the forum rules

(and i am not 100% able to do it as i have never tried) i will not go into detail about this method. I will leave it up to you to work it out, if you are really interested in it. But please do not ask me (I will report you) or post on this forum about it as it is illegal black hat activity!

Getting ettercap

OK so for this tutorial i am running Ubuntu 10.10, if you are running a linux distro you should be able to follow these instructions, if you are on Backtrack you already have it. In a terminal type

Code `sudo apt-get install ettercap`

This will install ettercap to you machine very easily! Just enter y if it prompts you. To test if it is installed type:

Code `ettercap -v` That will display the version.

If you are on Windows or Mac you will have to install this yourself, have a look [here](#)

So how do i use this shiny new bit of software?

The answer is simple, as there are very few steps required to DNS spoof a network. We need to find 2 things first though, the gateway IP of the network and the interface that we are using. There are half a dozen ways to find these bits of info but the easiest command to use is probably:

Code `route -n`

This will display an out put like this:

[img]http://i.min.us/ib4YN6.png[/img]

What you see there is the gateway IP (192.168.1.254) and the Interface (wlan0). Yours could be different but that is the easiest way to find them. There are other ways to do it, but this is the most simple.

OK now we know our gateway and our interface, for me it is:

Gateway: 192.168.1.254

Interface: wlan0

Now we can use these in our next commands. The next part of this is to define where we are going to redirect the traffic. This needs to be in IP format. This means that you need to find a website that has a dedicated IP address and you are OK to redirect traffic to the home page. Alternatively you can set up an apache server and redirect traffic to there. I will cover that later, but for the moment let us get a proof of concept example going first.

Setting up the redirection rules

In my example i will redirect traffic to hackforums.net. So i need to find out the IP of hackforums.net there are many ways to do this but the easiest to explain in a tutorial is this:

Code `ping -c 1 hackforums.net | grep 'PING' | sed s/"("// | sed s/")"// | sed s/":"// | awk -F' ' '{ print $3}'`

That will put the IP of the website you put in hackforums.net's place. It is a tad long, but if you are making notes like you should be you can copy pasta it. Or just learn how to use ping it is VERY simple.

So hackforums IP is: 69.162.82.251

Now i advise at this point that you check that you ensure that that IP address resolves to where you want it to go to. So open up your browser (firefox) and put the IP address in the address bar. If you get the web page you want to redirect to then you are set!

Now we just need to put that information into our ettercap configuration. We do this with this line of code:

```
Code sudo echo "* A 69.162.82.251" >> /usr/share/ettercap/etter.dns
```

You obviously replace 69.162.82.251 with the IP you wish to redirect to. Now let's have a look at this command. All it does is (over)write '* A 69.162.82.251' to ettercap's dns configuration file. This means ALL traffic, the A means redirected to, and the IP is where it is redirected to. So if you put:

'google.com A 69.162.82.251' in you would redirect all of the clients trying to connect to google.com to 69.162.82.251.

This is also where you would enter the IP if you wanted to redirect traffic to a machine on the internal network, for example:

```
A 192.168.1.70
```

Would direct traffic to 192.168.1.70. I will cover why you might want to do this later on in the tutorial.

Running ettercap

Now we just need to run ettercap here is the command that I will be using in my example:

```
Code ettercap -T -q -i wlan0 -M arp:remote /192.168.1.254/ // -P dns_spoof
```

OK now to break this down:

ettercap = Run ettercap

-T = Run ettercap in text only mode

-q = Run in quiet mode (Only important info shown)

-i <interface> = This is where we specify the interface so '-i wlan0' means "use wlan0" this is where you put your interface that you found earlier with route -n

-M arp:remote = Mode; arp-remote (begin arp-poisoning the network)

/<gateway>/ = Become the Man in the Middle to the gateway specified (This is where you put in the gateway you found with route -n earlier and...

// = Become the MITM for all clients of the gateway. You can optionally specify a specific client to target here by adding their internal IP in like this /<internal IP>/ You can find internal IP with nmap, but that is not for now....

Result?!

Well you should hopefully see something a little like this:

"It was big so I hid it" ([Click to View](http://i.min.us/idLJMa.png))

Now you can see all of the websites being redirected to hackforums.net!

When you are finished press 'q' to quit.

Now that is the basics of using ettercap to DNS spoof, now I will talk about setting up an Apache server on your computer and redirecting traffic to that. The benefit of this is that you make the webpage that the victims are redirected to.

Setting up Apache

Now basically we use exactly the same methodology as before but we are creating the page that has been redirected to. First of all you need to install Apache, so in a terminal type:

```
Code sudo apt-get install apache2
```

Press yes if it asks you for it, and then you have it installed. Next you need to test if it is working. So begin Apache2 like this:

Code `sudo /etc/init.d/apache2 start`

Then open your browser put 127.0.0.1 in the address bar. You should see a page that says 'It works!' This is your web page now. You can edit it by going:

Code `sudo gedit /var/www/index.html &`

Now you make your web page from there. I suggest something like [this](#)

So now when you navigate to 127.0.0.1 you should see your web page in all its glory. now all you need to do is replace the IP address that you are spoofing to, to your internal IP address. You can find your internal IP address with this command:

Code `ifconfig | grep Bc | awk -F " " '{print$2}'`

Now you just put it in your ettercap configuration like as before:

Code `sudo echo "*" A 182.168.1.70(your internal IP)" >> /usr/share/ettercap/etter.dns`

Then test that apache is running and your webpage can be accessed by going to 127.0.0.1 then just run ettercap exactly as before, and the traffic will go to you instead of the IP of the website!

Tada!

So in very short this can be down with just 4 commands:

Code `gateway=$(route -n | grep -v Gateway | head -n 5 | tail -n -1 | awk -F " " '{print $2}' )`

`interface=$(route | grep -v Gateway | head -n 5 | tail -n -1 | awk -F " " '{print $8}' )`

`/etc/initd./apache2 start` (Optional)

`echo "*" A <IP TO REDIRECT TO>" >> /usr/share/ettercap/etter.dns`

`ettercap -T -q -i $interface -M arp:remote /$gateway/ // -P dns_spoof`

I hope you have enjoyed!

Here is a list of my other tutorials and scripts:

<https://hackforums.net/showthread.php?tid=896006>

disk0 - January 4, 2011, 2:26 pm

Yet another well written, easily understandable tutorial from Middle! Good job dude. I think you guys should definitely compile some tutorials you have written and release them. Maybe as a large PDF or something?

R Millz - January 4, 2011, 4:18 pm

yes, a nice looking long tut. gj would rep if i could

ac1dxtrem - January 4, 2011, 6:35 pm

Great job Middle ;) I am finishing my WEP & WPA encryption educational threadsr then I will link them to your tutorials ;) So we have my WEP Encryption + Your tutorial

WPA Encryption + Your tutorial

ARP Poisoning + Mine tutorial with ettercap + your tutorial with arpspoof

DNS Spoofing + This tutorial :) What do you think we need more ?

Middle - January 4, 2011, 11:16 pm

that is pretty much all of the major operations that one can do, covered. Maybe we could make a thread on advanced techniques or something....

ac1dxtrem - January 5, 2011, 4:05 am

And how about we make a white hat thread for all of them as well... ? It will be like: Method Explanation + Tutorial + How to fix the vulnerabilities ?

ac1dxtrem - January 5, 2011, 5:37 am

(Jan 5, 2011 06:05 AM)Notieboie Wrote: [\[CITE\]](#) I find this tutorial to be the best among all of your

tuts.

I really appreciate your work.

silly question: what if i want to redirect 1 target user (lets consider his ip is xx.11.22.33)
Then instead of // you will put /his ip address/ :)

Middle - January 5, 2011, 6:19 am

Yeah do what ac1dxrtrem says!

You can find all the internal IP's on your network with the nmap -sP command, something like:

```
nmap -sP <yourinternalnetwork>/24
```

But i think it differs for each type of network, although if it is 192.168.x.x (all that i have ever come across) it is:

```
nmap -sP 192.168.1.1/24
```

Ask ac1dxtrem about it he might no better than i do.

And yeah i did think about making a white hat version of all the stuff, however the issue is that it is quite simple.. i.e WPA2 and a good password. So i would say maybe we make a tutorial on Securing a Wi-Fi AP instead of a bit about how to secure against all the different attacks. Or we add a section at the end of each of the tutorials "How to prevent this".

If we made a White hat Wireless thread, you could cover using WPA, using a good key, Mac filtering and protection against arp-poisoning (Not sure how to do that) oh and hiding the essid and limiting the wireless range/online times....

ac1dxtrem - January 5, 2011, 6:29 am

Yeah we will talk about it on IRC the protection against ARP Poisoning is a real PAIN IN THE ASS I was studying it for a long time and I still can't understand the whole thing... it is really ADVANCED (but hey that makes it more interesting ;))

Middle - January 5, 2011, 7:26 am

yeah defintely!

SO basically there are two types of protection needed on a network internal and external.

External = Use WPA with a strong key, Enable Mac filtering, Change/Hide essid.

Internal = Stop arp-spoofing

The issue is the internal one, i have never really looked into it so i will see what i find.

I will be on IRC a bit later, i have to do some work now =[

This well be a really cool set of stuff!

EDIT: I have just had a quick poke around google, and it looks like small networks can be protected by assigning making the IP's static in the arp table. However a small network is not much point as it is easier to just see if anyone is doing anything phishy IRL. However Large networks can be protected by buying HQ switches that can prevent apr poisoning. So as far as a tutorial would go there isn't really much scope =[

lololo - January 5, 2011, 8:28 am

thanks a lot guys Middle brilliant job as always , and yes please make everything inside a pdf or something that can be read in Linux as well . cos my bookmarks is FULL lol Regards

Middle - January 5, 2011, 8:31 am

Is there an application that can read bbcode, adn then make like a pdf out of it?

Sounds weird i know but then i could just copy pasta all my tutorials into document, then somehow get a way of downloading all the images to the document...

It will be a pain in the ass....

<http://www.novapdf.com/kb/convert-a-web-page-to-pdf-100.html#firefox-pdf> maybe?

Also spoilers and yellow text with the grey background.... This is a big job lol

TheDoctor - January 5, 2011, 8:52 am

(Jan 4, 2011 02:58 PM){Middle} Wrote: [\[CITE\]](#) Then open your browser put 127.0.0.1 in the address bar. You should see a page that says 'It works!' This is your web page now. You can edit it by going: Code sudo gedit /var/www/index.html &Was the ampersand at the end of the command on purpose ? Typo, don't you think ? It forks the gedit command to the background.

Middle - January 5, 2011, 10:46 am

No that was on purpose, it means people don't close the terminl when gedit pops up and then subsequently close gedit.

CypherPunk - January 5, 2011, 11:02 am

chill guys , between i knew nmap simple scan lol , between 1 thing start making some 'advance' tutorials now :)

will be really helpful

disk0 - January 5, 2011, 7:24 pm

(Jan 5, 2011 09:52 AM)TheDoctor Wrote: [\[CITE\]](#) Was the ampersand at the end of the command on purpose ? Typo, don't you think ? It forks the gedit command to the background.

What the ampersand at the end of a command does is break the command from the terminal. For example, if you were running a command that normally would just hang (as opposed to giving control of the shell back to you), you could put an ampersand at the end of it, and it would run like normal, but you would still be able to use that terminal for other commands. Hope that helps.

(Jan 5, 2011 12:02 PM)Notieboie Wrote: [\[CITE\]](#) chill guys , between i knew nmap simple scan lol , between 1 thing start making some 'advance' tutorials now :)

will be really helpful

Is someone using Google translate for someone's username? lol

TheDoctor - January 6, 2011, 4:55 am

(Jan 5, 2011 11:46 AM){Middle} Wrote: [\[CITE\]](#) No that was on purpose, it means people don't close the terminl when gedit pops up and then subsequently close gedit.

(Jan 5, 2011 08:24 PM)disk0 Wrote: [\[CITE\]](#) What the ampersand at the end of a command does is break the command from the terminal. For example, if you were running a command that normally would just hang (as opposed to giving control of the shell back to you), you could put an ampersand at the end of it, and it would run like normal, but you would still be able to use that terminal for other

commands. Hope that helps.Ohh, my bad then. Thanks for the explanations.

Do0ks - January 11, 2011, 4:58 pm

Great tutorial man! Understood everything!

Thank you!!

Daenerys Targaryen - January 16, 2011, 8:31 am

Great tutorial. Using it right now.

I only have one problem.. I'm using it in VMware, and it doesn't find my MacBook (Where VMware is running on, airport).

VMWare is using my AWUS036H.. this needs to work, right? But ettercap doesn't find the host (Macbook..)

zpoll - January 16, 2011, 8:51 am

Can somebody explin it to me exactly?

Middle - January 16, 2011, 9:05 am

You don't need to use the Alfa for this to work, which is the good news, and i'm not too sure why it doesn't work. if you put /gateway/ // it will target the whole network.

Daenerys Targaryen - January 16, 2011, 9:42 am

Thx Middle,

Well it worked now. (I've flushed my MacBook DNS), but sometimes it still won't work .. :/

I'm using the Alfa on VMware, Airport on the Macbook.

So my connection of my macbook doesn't need to be bridged or so with my VMware, right?

Also; When I do the spoofing, the spoofing is a bit slow. Sometimes the page doesn't react at all. Is this normal?

Thx, great tut.

Djbengan - February 20, 2011, 1:48 pm

Lol, i ran this several times on my school, its fun to watch the meatspins pop up... :)

Anyways, i do find it easier to just run host www.yourhomepage.net when finding the ip, just a little tip :)

DownBelow - March 13, 2011, 12:55 am

when I get the windows version, do I install it with the install wizard? I didn't download yet

jamesbondbest - March 18, 2011, 11:41 pm

CAN we sniff WPA -PSK by using this tute?...i mean can i perform MITM and dns sppofing on WPA-PSK network....I am having aces to network

Middle - March 19, 2011, 3:10 am

This works on all forms of encryption

jamesbondbest - March 19, 2011, 6:03 am

Actually i followed ac1dxtrem tutroail and having problems will u give it a try ...here is a link

<https://hackforums.net/showthread.php?tid=695677&page=13>

check the last post

zerdnem - March 22, 2011, 11:56 pm

this tut really help me a lot. promise. ty

Xtr0id - March 23, 2011, 2:13 am

You post a greatly written tutorial sir ? Just wish I could connect to networks in bt to follow it

Middle - March 23, 2011, 10:00 am

Thats why you learn to war drive XD

Xtr0id - March 23, 2011, 1:08 pm

Wait! I figured it out (:

(wht does war driving have to do with connecting) something I'd like to do though

Ok now i can have heaps of fun with this tut lol, Thanks

edit: ok in my experience just now with this, I started the spoofing fun and went to my other computer to check but it still goes to the website I asked instead of spoofed website. But in ettercap it says "spoofed to (ip)"

Lol and I see a bunch of other people getting spoofed to that pr0n site. D:

but after i press q to quit, then I start getting spoofed to that site lol.

EnemyOfZionist - April 5, 2011, 2:24 pm

Hey nice tut, I wanted to ask you something. I am using my neighbours network and want to dns spoof it and give them a rat to install so I can control their computer. In this case I am not using a RAT, instead I want to use the java applet created using SET(social engineering toolkit). How do I make them redirect back to google and use the java applet to install.?Do you understand what I'm trying to say.

Middle - April 5, 2011, 2:28 pm

Not quite!

Do you mean that you want to redirect the targets to a java drive by hosted on your PC to infect them then redirect them back to google?

EnemyOfZionist - April 5, 2011, 4:28 pm

errm, not exactly I'm trying to say basically I wanted to redirect them to another website e.g some windows update but instead of using a RAT I wanted to know how can I use the server created from SET, as you may know that on the social engineering toolkit you can do many attacks such as site clone, For this attack I have to send the victim an email and they have to click on it and it will redirect them onto a site where they have to install a java popup but I wanted to know If I could do it by dns spoofing and placing that Java on to this attack.

shadowmon - April 29, 2011, 12:08 am

nice TuT. i find this very useful. imagine if your a blackhat. :)

redirecting to fake pages then log their account in. whoala! got the login & password. XP tn timer! :)

Zero?? - June 2, 2011, 3:56 am

YEAHHH!!!! You're effing awesome!

GeneralStarshade - July 10, 2011, 7:02 pm

This is an awesome tutorial, however, for some reason, I cannot get ettercap to poison the computers in my network. I am using backtrack 5, and connected to my home network. I followed the commands exactly, except I am redirecting web traffic to my own custom web page using the apache web server and my local IP address.

After running that last command

Code ettercap -T -q -i wlan0 -M arp:remote /192.168.0.1/ // -P dns_spoof

I don't get any results when I try to browse to different web sites on the computers that are supposed to be poisoned. Any suggestions?

xxbadzvincexx - July 11, 2011, 4:16 am

ok sir thanks for sharing this usefull tutorial ?

zenawenliang - December 21, 2011, 6:10 pm

Hey bro, when I install ettercap in Backtrack 5 it doesn't have a ettercap folder in usr/share Also, I am unable to install ettercap-gtk I'm not sure if that does anything though.

SpyFi - December 21, 2011, 6:38 pm

Thanks Middle! You always have something different besides WEP and WPA hacking.

Rainb?w Dash - January 28, 2013, 9:55 am

Hi I have a question I tried this on my own wifi to test it and after I was done testing it I hit q but when I try to go to some websites it takes me to the website I wanted to redirect to. How can I stop this from happening? <3

Sk8eR_PR - February 23, 2013, 9:00 am

I have a question about this...

Does this works redirecting the target when the target tries to browse somewhere after the first slash "/" like in example "google.com/users/"???

Because I am having this problem:

<https://hackforums.net/showthread.php?tid=3279638>

Thanks!

PedroDJ - February 23, 2013, 9:02 am

Thread is revived [01-05-2011, 12:58 AM (This post was last modified: 01-27-2011 10:13 PM by Middle.)]: I suggest to contact OP in PM :)

Ouija - May 6, 2013, 11:57 am

awesome. thanks for the tutorial mate. :)

Toasties - June 15, 2014, 7:38 am

Thank you for this tutorial I found it very useful

Keytone1 - March 9, 2015, 2:38 am

Interesting post man thanks alot:):):):)

MGN astro - June 3, 2015, 12:26 pm

Very nice tutorial. and this is what i was looking for ..

Thanks for help !!! man

..

a few questions though.

1' can i use this method of Dns spoofing with the Credential harvester in kali linux .

like i set the website by importing . Index.html of facebook . and its up and running now on 127.0.0.1 ..

if i type this on the browser.. my fake website . which is custom imported .. not cloned is showing up

..

so does this Dns spoofing work with with that method ..

I have seen some guys saying .. Site clone and custom import does not work the same on different DNS spoofing methods .. ?

and are you using UBUNTU ? if yes. then are those commands working with Kali linux ?

pomwtin - June 3, 2015, 2:34 pm

Yes, it would work, but DNS request have to be made, so you will have to bypass HSTS before that- for your example of facebook.

If you have proper tools on ubuntu, commands are the same as in on kali.

If i remember correctly, cardinal harvester has option to do dns spoofing by itself... Doesnt it?

Hacklinux - June 4, 2015, 8:23 am

Nice tutorial, thank you for sharing.

Regards!

DoxProxy - December 27, 2016, 7:44 pm

Nice tutorial, I have a question (I made a whole thread for this to in case other people have a similar issue but I have not been able to find any threads addressing an error like this one online anywhere - Hello Hack Forums! I cannot seem to get ettercap's dns spoofing function to work properly. I've seen many tutorials on youtube and through google, and after following them I always end up getting the same error: attacking machine says dns spoofed facebook to 192.168.x.x | While on the targeted machine the following browser error appears :

"Unable to connect

Firefox can't establish a connection to the server at {facebook}.

The site could be temporarily unavailable or too busy. Try again in a few moments.

If you are unable to load any pages, check your computer's network connection.

If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web."

If i go to my local ipv4 address in the browser (192.168.1.14) it will load but not if I go to facebook website. I edited etter.dns properly and etter.conf, I also started apache2 service and tried both with listening to port 8080 with sslstrip and without doing that. And I enabled ip forwarding (echo 1 >

/proc/sys/net/ipv4/ip_forward. It worked briefly two days ago when I targeted my Dad's laptop but I haven't been able to get it to work again since. Thanks for any help!! ?

Sheeple - December 27, 2016, 7:55 pm

(Dec 27, 2016 08:44 PM)firepaw100 Wrote: [CITE](#) Nice tutorial, I have a question (I made a whole thread for this to in case other people have a similar issue but I have not been able to find any threads addressing an error like this one online anywhere - Hello Hack Forums! I cannot seem to get ettercap's dns spoofing function to work properly. I've seen many tutorials on youtube and through google, and after following them I always end up getting the same error: attacking machine says dns spoofed facebook to 192.168.x.x | While on the targeted machine the following browser error appears :

"Unable to connect

Firefox can't establish a connection to the server at {facebook}.

The site could be temporarily unavailable or too busy. Try again in a few moments.

If you are unable to load any pages, check your computer's network connection.

If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web."

If i go to my local ipv4 address in the browser (192.168.1.14) it will load but not if I go to facebook website. I edited etter.dns properly and etter.conf, I also started apache2 service and tried both with listening to port 8080 with sslstrip and without doing that. And I enabled ip forwarding (echo 1 > /proc/sys/net/ipv4/ip_forward. It worked briefly two days ago when I targeted my Dad's laptop but I haven't been able to get it to work again since. Thanks for any help!! ?This thread is 4 years old. Thank for the gravedig

Darkforce16 - December 29, 2016, 6:01 pm

This is a great way to mess up my kids...but when i enter the code below:

Code ettercap -T -q -i wlan0 -M arp:remote /MyGatewayIP/ // -P dns_spoof

I get the output:

Code ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Incorrect number of token (///) in TARGET !!

I've also tried to put in a target range after /MyGatewayIP/ /IPaddress10-15/ -P dns_spoof but no luck

Running Kali on VM.