

Forum:[Hack Forums](#)

Thread: [\[TUT\] DNS Spoofing - LAN Hacking Technique \[TUT\]](#)

xchg - April 23, 2015, 1:32 am

DNS Spoofing Tutorial | By:

Hello Hackfourms!

Today I'm going to teach you about "DNS Spoofing".

Please note:

This tutorial was meant to inform the Hack Forums community of a modern technique countless hackers are using to harm innocent people. This tutorial is meant to be purely educational. By reading this tutorial, you agree that you will not replicate the steps I have listed below on ANY Wi-Fi but your own; and you will not use these techniques to manipulate the web requests of anyone but yourself without the proper consent. If you haven't already, please read the [Help Docs](#)/Rules before commenting below. Thank you.

Overview of Tutorial:

[@]Getting an understanding of DNS Spoofing.

[@]Tools and requirements.

[@]Downloading and set-up.(Sub section)

[@]Performing a DNS Spoofing attack.

[@]How to prevent DNS Spoofing.

[@]Recap

[@]Getting an understanding of DNS Spoofing.

Wikipedia defines "DNS spoofing" as the following:

"DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer)."

en.wikipedia.org/wiki/DNS_spoofing

To put it short, by the end of this tutorial you will be able to manipulate web requests on your OWN wireless network. For example: if your targeted computer tries to reach www.facebook.com, you can manipulate the web request to redirect the targeted computer to send a web request to a web server hosted on your computer, stating that facebook.com is blocked on your Wi-Fi, or redirect someone to your own version of www.facebook.com which has a much cooler GUI than the original.

[@]Tools and Requirements.

[+]Cain and Abel

[+]Windows Operating System (or Windows virtual machine)

[+]Note taking application

[@]Downloading and set-up (detailed)

Spoiler ([Click to View](#))

#1 - Downloading Cain and Abel

Info: Cain and Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using

Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols.

Download Link: <http://www.oxid.it/cain.html>

Directions:

Upon navigating to the [link](#), you will find a webpage that looks something like this:

You want to select the option that reads: "Download Cain & Abel v4.9.56 for Windows NT/2000/XP".

When the file has completed downloading, you want to take the following measures to ensure Cain and Abel is ready for use:

1. Disable the windows firewall
2. Always run Cain and Abel as administrator (you may want to enable this in the property section of the application.)
3. Make sure you are connected to the desired wireless network (DO NOT USE THIS ON ANY NETWORK BUT YOUR OWN)

[@]Performing a DNS Spoofing attack

Spoiler ([Click to View](#))

Step 1: Start up Cain and Abel

(Make sure Cain is running with administrative privileges and the Windows firewall is disabled)

Step 2: Navigate to the "Sniffer" tab, enable the "sniffer", and start a scan on your network (using the plus icon and pressing start scan) (this will locate the IP addresses of all devices on your network, as well as the mac address and OUI footprints).

Step 3.

Once you find all the IP address listed, its now your job to locate which IP address is your router, and which one is your targeted computer.

For example:

My router's IP address is: 192.168.1.1

While my targeted computer's IP address is: 192.168.1.7

Step 4.

Now its time to begin ARP on your selected computer and redirect traffic!

Firstly, select the ARP tab on the lower tab set.

Second, you want to click inside of the upper tab set on the ARP tab.

Step 5.

This will enable the plus button on the options menu above. After this is enabled, you want to click

the plus button.

Upon doing this, you will be prompted by a selection module. which will ask you to select two IP addresses. If you were paying attention up to now, that is where those two previous IP addresses you wrote down come into use.

In the first selection box, you want to select your routers IP address. In my case, its 192.168.1.1
Yours may be different.

After clicking your routers IP address, the next selection module will load a series of results. The results are all the other IP addresses associated with your router. This is where you will select one or more of the IP addresses as the targeted computer. The targeted computer can be any OS; including phones, tablets, Linux, OSX, Windows, or any other which has the ability to communicate with the internet.

Step 6. Click the ARP button to activate the ARP poisoning.

Step 7.

Once poisoning is activated, navigate to the tab on the left titled, "ARP-DNS".

Step 8. Add your entry.

Begin by right clicking on the ARP-DNS form. This should prompt you with a selection menu. The options include: "Add to List", "Edit", "Remove from List", "Remove All". You want to select "Add to List".

A form should prompt you to enter in the desired information.
(And of course, pictures are provided)

For mine, I entered in facebook.com, and my IPv4 for the address to redirect packets to.

Step 9.

Have the targeted computer try to access the "DNS Name Request" you entered in ARP-DNS. For me, it was <http://www.facebook.com>

If you did it right, the connection will time out, since there is no server to be accessed on your IP address (or maybe there is, its none of my concern).

If you wanted the targeted computer to be redirected to a different website, like google, or yahoo answers or some shit, you would simply resolve the IP address of that website and enter it into the box in ARP-DNS. This will work, assuming that the website allows direct IP address access, which most web hosts don't allow.

If you wanted the targeted computer to redirect to a web server hosted on your computer, you would simply set up an Apache webserver, and create a small simple website, hosted on your computer. The webpage they would be redirected to could be anything you would like, but nothing illegal ?

[®]How to prevent DNS Spoofing.

Spoiler ([Click to View](#))

How to Prevent It:

- 1.Maintain the DNS software Up-to-Date.
 - 2.Allow updates and zone transfers from trusted sources.
 - 3.Maintain a Separate DNS server for public services and for internal services.
 - 4.Use secure key for signing the updates recieved from other DNS server.
- (infosecawareness.in/sysadmin/dns-spoofing)

[@]Recap

DNS Spoofing is a dangerous modern hacking technique which can be found in coffee shops, malls, and many other public places in which Wi-Fi is widely available. Its important that you brace yourself with the knowledge of how DNS Spoofing works, so you can better know how to protect yourself against it.

Don't learn to hack, hack to learn.

I hope you enjoyed the tutorial! A few solid hours of research went into the making of this tutorial and it would really help if you left some feedback in the comments below.

I'm planning on doing more tutorials such as this one in the near future (trying to give back to the community a little more); so tell me if there is anything I need improvement on, or anything you really liked about this tutorial! Have an awesome day!

samrokzz - April 23, 2015, 8:17 am

There are many cain and able tutorials are here , and it's a nice one among them ,
Thanks for sharing .

paplo - April 23, 2015, 10:43 am

Wow thanks man! I'm doing a security project at school and this is just perfect for testing. Cheers!

xchg - April 23, 2015, 12:36 pm

Yea I thought this was an interesting tutorial for others to associate themselves with.

P0pz - April 24, 2015, 8:34 am

Good tutorial, I prefer doing this on linux with ettercap and redirecting all traffic to the desired site but

showing that this can be done in windows as well can be also very helpful. Thanks, keep this up.

zokorzik - April 24, 2015, 3:38 pm

really educational thanks for the tutorial :)

xchg - April 24, 2015, 4:24 pm

Good to know you guys like the tutorial, thanks for leaving feedback!

dotslash - April 25, 2015, 1:40 am

nice tutorial , hope one day they find how to sniff https porotocol on LAN

roleeswagger - April 25, 2015, 10:55 am

Thanks for sharing with us this tutorial :)

xchg - April 26, 2015, 4:44 am

(Apr 25, 2015 10:55 AM)S4mick Wrote: ([CITE](#)) Thanks for sharing with us this tutorial :)

Yea no problem

I hope you found it very useful

samihassanegypt - April 26, 2015, 10:50 am

Hey there , awesome tutorial! I shared it on my blog I hope you dont mind ; if you are interested in referencing. Please PM ME

xchg - April 26, 2015, 1:10 pm

(Apr 26, 2015 10:50 AM)samihassanegypt Wrote: [\[CITE\]](#) Hey there , awesome tutorial! I shared it on my blog I hope you dont mind ; if you are interested in referencing. Please PM ME

No I don't mind at all, just give credit where credit is deserved :)

samihassanegypt - May 1, 2015, 5:23 am

(Apr 26, 2015 01:10 PM)Kro?? Wrote: [\[CITE\]](#) No I don't mind at all, just give credit where credit is deserved :)

I sure did , no worries ;)

Vector.A+ - May 1, 2015, 9:32 am

nice one , ettercap is a nice tool for this too

xchg - May 1, 2015, 4:33 pm

(May 1, 2015 05:23 AM)samihassanegypt Wrote: [\[CITE\]](#) I sure did , no worries ;)

Thanks so much!

Would you mind linking me to it? Lol I don't want to prove that you gave me credit; I just wanna check out your blog.

Musa1337 - May 1, 2015, 4:42 pm

The only thing I don't get is if this is only working on LAN or if it is also working on WiFi? Thanks. Now I know why people are always concerned about giving their WiFi passwords to other people.

UkVenoM - May 1, 2015, 10:39 pm

HQ Post, This is a contribution to HF, Great work OP ?

F-Nuke - May 1, 2015, 11:21 pm

HQ tutorial. Thank you for your contribution.

xchg - May 2, 2015, 2:03 am

(May 1, 2015 04:42 PM)Musa1337 Wrote: [\[CITE\]](#) The only thing I don't get is if this is only working on LAN or if it is also working on WiFi? Thanks. Now I know why people are always concerned about giving their WiFi passwords to other people.

LAN=Local area network

LAN is WiFi

Yea you should never give out your wifi password to people. This is also a big issue for places like Starbucks

n3y4k0 - May 2, 2015, 7:16 am

Interesting topic, thank you.

xchg - May 2, 2015, 10:06 pm

(May 2, 2015 07:16 AM)n3y4k0 Wrote: [\[CITE\]](#) Interesting topic, thank you.

Glad this is gaining some publicity.

This is something frequently used by criminals in botnets and other forms of malware.

Chronosphere - May 3, 2015, 3:02 am

very nice tutorial thanks a lot for sharing it :)

pulkitkumar - May 3, 2015, 9:16 am

Such a Great tutorial Loved it Man!!!

I am Gonna Try it Out on my phone

xchg - May 3, 2015, 7:13 pm

(May 3, 2015 09:16 AM)pulkitkumar Wrote: [\[CITE\]](#) Such a Great tutorial Loved it Man!!!

I am Gonna Try it Out on my phone

Yea when I first tried it out I did it to my phone from my computer and it works fine.?

TearProgrammer - May 4, 2015, 5:13 am

This is awesome, thanks! Is there anyway you can spoof https? Secured sites such as facebook, twitter, etc... Don't appear to work? :(

xchg - May 9, 2015, 10:06 am

(May 4, 2015 05:13 AM)TearProgrammer Wrote: [\[CITE\]](#) This is awesome, thanks! Is there anyway you can spoof https? Secured sites such as facebook, twitter, etc... Don't appear to work? :(

Yes there is, but I suggest you do research on this elsewhere; as HF does not allow any discussion of phishing ?

Krat0s2 - May 9, 2015, 10:33 am

Great tutorial Kross.

I would like to suggest only one thing. There are times when Google Chrome considers the setup of Cain and Abel as malicious software and you can't download it. Just use IE(yeah Internet Explorer) since that shit software does not scan anything.

And Cain and Abel rocks , this little program is a best, program way bacj then and still works. I do not even have to disable the firewall.

Side note, can you PM about the https part? I have have good reason why I need this and I can explain in detail about it if you have an interest. Anyway that is up to you , and thank you again for the thread.

Cheers.

Bulma - May 9, 2015, 10:35 am

Nice tutorial. Was looking for something long time ago,thank for sharing.It will help me a lot.

UkVenoM - May 9, 2015, 11:25 am

(May 9, 2015 10:33 AM)Krat0s2 Wrote: [\[CITE\]](#) I would like to suggest only one thing. There are times when Google Chrome considers the setup of Cain and Abel as malicious software and you can't download it.

When Chrome blocks a download, you can go into the recent downloads by pressing Ctrl+J and you will be given the option to download it without intervention.

xchg - May 10, 2015, 8:02 am

(May 9, 2015 11:25 AM)UkVenoM Wrote: [\[CITE\]](#) When Chrome blocks a download, you can go into the recent downloads by pressing Ctrl+J and you will be given the option to download it without intervention.

Thanks for clearing this up man!

There is no doubt in my mind other will have issues with this?

Lures - May 10, 2015, 12:23 pm

Ignore this I accidentally posted to the wrong thread somehow, sorry not sure what happend. ?

is there a way to delete?

CybexAlpha - May 10, 2015, 12:57 pm

lol thats a interesting thing

striking - May 11, 2015, 5:37 pm

@Kross I have a few questions, as I did everything as you mentioned, but it's not working.

1. When I click "Start/Stop Sniffer", it pops up with that message, see the [picture](#).

2. I click OK and everything and continue. When I scanned my network for the IP addresses (I was it Ethernet connection at that moment, no Firewall) I found just 1 IP address, and there should be more. So I logged into my router and found that there currently 2 IP's connected. One of them was my Smart TV and the other one my smartphone. But I was seeing just the Smart TV. Well what ever I decided to give a try and start the ARP poisoning and added ARP-DNS and so on. When I tried to open these 2 web pages I putted in Cain&Abel using my TV, it was not working.

3. So here are my questions. Why I couldn't see my phone after the scan? And why even when I did it on my TV it was not working, I mean it should work because the TV has web browser, but it doesn't.

Please advise :)

BenkaTv - May 12, 2015, 12:05 pm

Thanks dude! i really need this <3

xchg - May 12, 2015, 12:21 pm

(May 11, 2015 05:37 PM)striking Wrote: [\[CITE\]](#) @Kross I have a few questions, as I did everything as you mentioned, but it's not working.

1. When I click "Start/Stop Sniffer", it pops up with that message, see the [picture](#).

2. I click OK and everything and continue. When I scanned my network for the IP addresses (I was it Ethernet connection at that moment, no Firewall) I found just 1 IP address, and there should be more. So I logged into my router and found that there currently 2 IP's connected. One of them was my Smart TV and the other one my smartphone. But I was seeing just the Smart TV. Well what ever I decided to give a try and start the ARP poisoning and added ARP-DNS and so on. When I tried to open these 2 web pages I putted in Cain&Abel using my TV, it was not working.

3. So here are my questions. Why I couldn't see my phone after the scan? And why even when I did it on my TV it was not working, I mean it should work because the TV has web browser, but it doesn't.

Please advise :)

Could you please reupload your picture through imgur so I can get a better look?

Hope we can get this resolved!

striking - May 12, 2015, 3:23 pm

OK here you go, see it uploaded in the new [place](#)

I just tried with connected Apple Ipad and I found it. I added it in the list and there were packages going out and in on the first half of the screen on ARP mode. On the second half below there are

some

"Full-Routing" and "Half-Routing" packages and IP addresses. On the left panel we can see "ARP-CERT" = 22 and also "ARP-HTTPS" = 54, I thought that the HTTPS is where you can steal passwords from visited websites, but I don't see any of that there. Let's get back to the point, even when it seems like it's working something on the Ipad, when I tried to open the 3 webpages I included, I was

not redirected at least on time.

I'm thinking if we enter in Cain&Abel for example "www.facebook.com" and if you open on the poisoned device "https://www.facebook.com" if that will be the same and if it work or no?

Beyond that I don't know what is the f**king problem :(May be is something with the message on the uploaded picture I shown you. I hope you can help me out with that one.

UPDATE: OK there is another update. I just connected my smartphone and I re-scan and saw the IP. I don't know why it was not working yesterday o.O But now see whats happened, I tried the first listed webpage and I was redirected successfully. I tried facebook and the page was restricted saying that may be someone is trying to steal my password and so on. Why is not working with facebook?

Then I tried with my last webpage and first I was redirected to the mobile version of the page, and I don't know if should work in such a case but it didn't. So then I opened the web based version but I was still not redirected. Now why worked just with one website? Why is not working with facebook, did you tried it with facebook?

And why is not working with the Apple Ipad at all?

There too many discrepancies and I don't know why, I thought it will work as a charm, because It looks simple "trick"... ?

0Boy - May 12, 2015, 3:37 pm

Great tutorial, something different. keep it coming

xchg - May 13, 2015, 1:46 pm

(May 12, 2015 03:23 PM)striking Wrote: [CITE](#) OK here you go, see it uploaded in the new [place](#)

I just tried with connected Apple Ipad and I found it. I added it in the list and there were packages going out and in on the first half of the screen on ARP mode. On the second half below there are some

"Full-Routing" and "Half-Routing" packages and IP addresses. On the left panel we can see "ARP-CERT" = 22 and also "ARP-HTTPS" = 54, I thought that the HTTPS is where you can steal passwords from visited websites, but I don't see any of that there. Let's get back to the point, even when it seems like it's working something on the Ipad, when I tried to open the 3 webpages I included, I was

not redirected at least on time.

I'm thinking if we enter in Cain&Abel for example "www.facebook.com" and if you open on the poisoned device "https://www.facebook.com" if that will be the same and if it work or no?

Beyond that I don't know what is the f**king problem :(May be is something with the message on the uploaded picture I shown you. I hope you can help me out with that one.

UPDATE: OK there is another update. I just connected my smartphone and I re-scan and saw the IP. I don't know why it was not working yesterday o.O But now see whats happened, I tried the first listed webpage and I was redirected successfully. I tried facebook and the page was restricted saying that may be someone is trying to steal my password and so on. Why is not working with

facebook?

Then I tried with my last webpage and first I was redirected to the mobile version of the page, and I don't know if should work in such a case but it didn't. So then I opened the web based version but I was still not redirected. Now why worked just with one website? Why is not working with facebook, did you tried it with facebook?

And why is not working with the Apple Ipad at all?

There too many discrepancies and I don't know why, I thought it will work as a charm, because It looks simple "trick"... ?

Okay this is how it works:

On a computer running a windows OS, connected to a Wi-Fi network, with the correct settings inputted into Cain and Abel, you will be able to reroute traffic sent to a specific website, to a different IP address.

The IP address you are rerouting traffic to HAS to be running a web server and allow direct ip address access OR YOU WILL NOT BE ABLE TO CONNECT.

The targeted device can be anything. The first time I tried this, I did it to one of my old Android phones. It worked flawlessly. Since I did not have any web server running on the ip address it was rerouting to, it simply said "cannot connect to the web server" when the mobile phone attempted to access facebook.com

On an iPad, it should still work fine.

As far as the error message goes, I could not find anything on google or their help page regarding that error specifically. If you are stilling having this issue and its still effecting you significantly, then I would do some more research. As far as the password stealing goes, that is disallowed black hat activity on HF, therefore I cannot further discuss this with you.

Hope I provided at least some helpful feedback.

Neos07 - May 13, 2015, 3:14 pm

Thanks For The Tutorial Dude! (y)

xchg - May 13, 2015, 3:17 pm

(May 13, 2015 03:14 PM)Neos07 Wrote: [\[CITE\]](#) Thanks For The Tutorial Dude! (y)

Thanks for leaving a comment!

Luc4s - May 13, 2015, 3:42 pm

I prefer ettercap, but great tutorial!

xchg - May 14, 2015, 9:37 am

(May 13, 2015 03:42 PM)Luc4s Wrote: [\[CITE\]](#) I prefer ettercap, but great tutorial!

Thanks for the incite luc4s!

Glad you found the tutorial helpful

frafri - May 17, 2015, 4:15 pm

Amazing tutorial. Thanks for sharing. Could you make one on ettercap when you get a chance, to have a better understanding!

xchg - May 17, 2015, 5:40 pm

(May 17, 2015 04:15 PM)frafri Wrote: [\[CITE\]](#) Amazing tutorial. Thanks for sharing. Could you make

one on ettercap when you get a chance, to have a better understanding!

Sure Id be happy too

I have a lot of experience with ettercap so it shouldn't be too hard.

Ill post a link to it in the thread when im done

Merc35 - May 20, 2015, 3:37 pm

Great Tutorial, very detailed and very informative, well put together and well done, thanks for this ?

Hey Krat0s2, thanks for this tip, I was having a shit of a time trying to D/L with Firefox ?

(May 9, 2015 10:33 AM)Krat0s2 Wrote: [\[CITE\]](#) Just use IE(yeah Internet Explorer) since that shit software does not scan anything.

Luki2442 - May 21, 2015, 12:05 pm

?? greaaaaat thx for sharing mate

Mourinho1994 - October 16, 2016, 1:51 pm

Hi, I wanted to know if you could help me. Do yo know how to host boot on a dedicated server?

There's a game that has one, and everytime I look for the ip on cain and abel, it keeps coming up with the same one's. Please could you get back to me on how to get around this. Thanks