

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] DNS Spoof to steal passwords!](#)

SIM-2015410 - March 23, 2014, 8:59 pm

Hello Again HF!,

Welcome to another Hacking Tutorial by MeshCollider.

If you are interested, here are links to my other hacking tutorials: Spoiler ([Click to View](#))

Metasploit 1: <https://hackforums.net/showthread.php?tid=4124763>

Metasploit 2: <https://hackforums.net/showthread.php?tid=4124800>

Metasploit 3: <https://hackforums.net/showthread.php?tid=4124838>

Cracking WiFi - WEP: <https://hackforums.net/showthread.php?tid=4126315>

Remote view a webcam/microphone: <https://hackforums.net/showthread.php?tid=4126349>

Cracking WiFi - WPA/WPA2: <https://hackforums.net/showthread.php?tid=4127410>

Hacking/Crashing windows 7 with a shortcut file:

<https://hackforums.net/showthread.php?tid=4127314>

PDF backdoor: <https://hackforums.net/showthread.php?tid=4127426>

Cracking passwords can take a lot of time and energy - especially if they are complex. Another alternative to steal a password is a phishing attack - clone a website, and host a modified copy to store credentials. But the trick is to get victims to actually visit your website. That is where a DNS spoof attack comes in.

DNS stands for Domain Name Service. A DNS server is responsible for converting websites addresses in the format "hackforums.net" to the IP address of the website. A DNS attack is a type of Man in the middle attack (MITM). We will be using the Kali Linux OS, which comes with the required software preinstalled. We will be using the Social Engineering Toolkit (S.E.T.) and Ettercap to capture credentials. Lets begin:

1) Open the Social Engineering Toolkit in Kali Linux:

Navigate to the correct directory:

Code `cd /usr/share/setRun se-toolkit:`

Code `./se-toolkit`

2) Clone and Host a copy of the website you want to steal passwords on:

Enter the commands in this order:

"1 (Social Engineering Attacks)" > "2 (Website Attack Vectors)" > "3 (Credential Harvester Attack)" > "2 (Site Cloner)".

Then enter your computers IP (found by using the ifconfig command), and enter the URL of the website you want to clone (e.g. facebook.com).

3) If you receive no error messages, now we need to get victims to navigate to our site!

Open a new terminal, and run the ettercap GUI by using this command:

Code `ettercap -G` Click "Sniff > Unified Sniffing" and select the network interface you are using to connect to the network you want to attack.

Then choose "hosts > scan for hosts" and wait for the scan to finish. When the scan has found all the hosts on the network, open "hosts > host list".

4) Select the victims you want to attack:

Add the router of the network to target 1 and any computers you want to "poison" to target 2. If either the target 1 group or target 2 group are left empty, the entire network will be attacked. After you have added the victims to the target lists, choose "MITM > ARP Poisoning", tick "sniff remote connections" and click Ok.

5) Create our "custom" DNS server:

Navigate to "/usr/share/ettercap" and open "etter.dns" with any text editor of your choice. Scroll to the bottom, and follow the example template to enter a DNS record. It will look something like this:

Code example.com A 192.168.1.10

*.example.com A 192.168.1.10

www.example.com PTR 192.168.1.10 Replace "example.com" with the website address you are imitating (e.g. facebook.com), and "192.168.1.10" with the IP address of your computer (the host).

Now, navigate back to your ettercap window, and click "Plugins > Manage plugins..." and double click on "dns_spoof" to activate it.

6) Begin collecting passwords!

Choose "Start > Start sniffing" and you are finished! Any visitors to example.com will in fact see your cloned version of the webpage and you will be able to see their credentials in the S.E.T. terminal window. Test the password out to check it works!

Thanks for reading, please reply with your thanks if you enjoyed this and/or found it useful.

Watch out for future hacking tutorials from me - further wireless cracking, metasploit and other common hacking topics!

Written by MeshCollider ?

phackman - March 28, 2014, 11:51 pm

something not working for me : I can use SET, clone facebook. But i'm on linux backbox my etter.dns is in another doc. I founded it and modded it for redirect facebook.com to my ip. The probleme is I can start ettercap and arp spoof my network, but the dns spoof plugin is not working (i ping facebook.com from another pc in my network and its the real ip, not my set page)

Thanks for this tut man!

SIM-2015410 - March 29, 2014, 2:11 pm

Make sure that the other pc has cleared the DNS cache, and re try. Glad you liked the tutorial.

kamrulahsan06 - April 3, 2014, 11:57 am

Very HQ tutorial as always :) Thank you for all of your HQ tutorial

iDuL - April 3, 2014, 3:07 pm

Thanks for the contribution, it's a shame this doesn't have more replies which it definitely should.

skill369zz - April 3, 2014, 9:30 pm

Thanks for the help much thankfull!!<3

KappaPride - April 3, 2014, 9:34 pm

Would this work on my vps?

If so Please pm me to help set up!

-Thanks in advance

SIM-2015410 - April 3, 2014, 9:55 pm

(Apr 3, 2014 09:34 PM)Semsec Wrote: [\[CITE\]](#) Would this work on my vps?

If so Please pm me to help set up!

-Thanks in advance

Sorry, I have never tried this with a VPS. Could you give me a bit more info about how you use your VPS and how it is setup? I'm not sure whether I can help though sorry ?

batsauto - April 15, 2014, 9:10 pm

Nice tutorial. I'm gonna test it out :)

Raoulb1_ - April 15, 2014, 10:30 pm

The MFOD module is more steady when it comes to DNS spoofing, I'm more a fan of ARP poisoning it's verfy effective.

SIM-2015410 - April 16, 2014, 12:07 pm

(Apr 15, 2014 10:30 PM)Raoulb1_ Wrote: [\[CITE\]](#) The MFOD module is more steady when it comes to DNS spoofing, I'm more a fan of ARP poisoning it's verfy effective.

The tutorial actually uses ARP poisoning lol.

KappaPride - April 16, 2014, 12:09 pm

Like installing the os on my vps and setting it up using ssh.

SIM-2015410 - April 16, 2014, 12:39 pm

(Apr 16, 2014 12:09 PM)Semsec Wrote: [\[CITE\]](#) Like installing the os on my vps and setting it up using ssh.

Well you should be able to install kali on the vps, but I don't think you can use ssh for this. It works by poisoning the computers on the network to redirect traffic through your machine. If you wanted, I think you can just set up a packet sniffer wireshark, url snarf, etc. to capture the packets that are traveling through your vps.

xinyonghu - April 16, 2014, 3:24 pm

So the tutorial can be used only in the LAN environment ?

SIM-2015410 - April 16, 2014, 5:47 pm

(Apr 16, 2014 03:24 PM)xinyonghu Wrote: [\[CITE\]](#) So the tutorial can be used only in the LAN environment ?

Yes, ettercap dns_spoof plugin poisons the ARP cache of any computers in your domain subset.

billybobzz - April 16, 2014, 5:53 pm

This only works on my local network, right?

sorry you just answered this above.

Skribles - August 28, 2014, 9:50 pm

Does this work for all / every website?

What is the best way to do this anon? Redirecting users to your IP sounds a bit sketch but then again I've never done this before.

What type of information do you get when a user is redirected? How are the passwords logged? What about usernames? IP?

Thanks!

peasxnt - August 28, 2014, 10:55 pm

Very impressed with this tut, loved your pervious will definitely find this useful in the future

Firmus - August 29, 2014, 4:07 am

Very good writing style(it's makes the things understandable) and good method.
Thank you so much! :)

Skribles - September 2, 2014, 9:53 am

Liked your write up man. Thanks for the quick response too.

kulme - September 2, 2014, 3:58 pm

If you want WAN DNS Spoof. This is requirement:

1. 1 or 2 VPS (2 good)
2. Hacked router login

Install Simple DNS Plus. Port forwarding DNS port.

Login to hacked router and update DNS 1 and DNS 2 with your VPS public IP.

Very very simple. LOL

* DNS port is 53

Exodian - July 29, 2015, 5:48 am

Is it possible to hijack a website and spoof their dns to display a message on the website. How would I go about doing this and is there any tutorials on HF?

rahimakbulut - July 29, 2015, 8:04 am

thanks bro, good system. ++++++

herewegoforums - July 30, 2015, 2:11 pm

This is cool bro. Thanks .

But i have one question . and that is -

What about if the victim is already surfing facebook and he or she didnt close that web page !
what could we do from this point ?

The DNS poisoning or DNS redirecting will not work, since the website is already cached!, how can we delete the cache data on the victim computer or maybe the whole entire network ?

I would be more pleased, if you help me with any ideas on this PLEASE ?

DolphinSky - July 30, 2015, 2:12 pm

Thanks for this guide, I will try this right now.

Poison - July 30, 2015, 3:21 pm

Verry usefull tutorial! Thank you keep it up!

skr4f - August 1, 2015, 11:13 am

Thank you for inspiration!

KnockSteadys - August 19, 2015, 10:22 pm

very nice work you did man thanks

ForceJew - March 12, 2016, 12:18 pm

Awesome all ur tutorials are great! Amazing person

JK1337 - March 12, 2016, 1:45 pm

Thank you for this! Nice tutorial. I will check your other tutorials for sure!

G_LO - March 17, 2016, 12:51 am

Nice Work, still working till now. Thanks For This

ExclenKr - March 17, 2016, 4:02 pm

This Will not work with Facebok/google/Twitter etc because of the implementation of SSL.

?Xe - March 18, 2016, 4:58 am

Yo dude it's an awesome tutorial, thanks for the share! People do read and use it, they just forget to say thankyou. So just know when you post tutorials people are always learning something from them and benefiting from them. Thanks <3

Catinashoebox1337 - March 20, 2016, 9:23 pm

Yes very nice read. Every tut helps me learn new things.

Pekls - March 23, 2016, 7:11 am

Nice tut lets hack my neighbor

harisondoom - March 23, 2016, 9:54 am

Very interesting, will try later.