

Forum:[Hack Forums](#)

Thread: [\[TUT\] ? How to sniff the router password without resetting it ? \[TUT\]](#)

Turtle™ - February 3, 2013, 9:29 pm

Hello HF, keep in mind that this tutorial is aimed at people who either have a router that they don't want to reset and the default password doesn't work.

I remember that at one point, I was extremely frustrated because I couldn't find my router password. All tutorials about port forwarding only applied if it was the default password however, my parents had changed it, which also ruled out resetting the router (since my parent's were not retarded and that would look quite suspicious).

So using backtrack, I was able to successfully SE (social engineer)/ sniff the password of the router. In this tutorial, I will be going through the exact same steps that I used to do this. If you do not have backtrack or don't know how to set it up on a Virtual machine, you can find out how to do that in my tutorial [here](#). It's contained in the first half (but feel free to read the second part if you are interested in a technique of "hacking" people on your LAN without sending them any RATs or anything.)

So I will assume that you now have backtrack installed. Boot it up through Virtualbox and update it with

Code apt-get updateand then

Code apt-get upgrade

The update is not mandatory if you download backtrack 5r3 but it's always good to have an up to date version. In my experience, the updates on backtrack are sometimes very buggy so it's up to you.

We will now be using a tool called ettercap. What we will do with this tool is use the dns_spoof plugin. What this will do is wait for someone to enter in a specific URL (which you will choose) and redirect them to another IP (which will be your IP so that they are connected to you).

First, we are going to have to specify what URL to wait for them to type in. To do this, go to the file etter.dns which is located in

Code usr/local/share/ettercap/etter.dns

Now minimize the Virtualbox window and open up command prompt (or CMD), you can get to the CMD by going to

Code Start > Accessories > Command Prompt

In the black window that should pop up, you will insert the command

Code ipconfig

Spoiler ([Click to View](#))

Now look for the Default Gateway IP which for me is 192.168.1.1

(For the skids that think that you can hack me with my ipv4, you can't, the ipv4 only applies inside the LAN) Enter that IP into the address bar of your web browser and you should be greeted with a login screen like this.

Spoiler ([Click to View](#))

This is what we will be redirecting people to.

Now that you know your default gateway, restore your Virtualbox window and we will get to editing etter.dns. Start by scrolling down until you see where it says "Microsoft Sucks". You should see the microsoft website address redirecting to the linux website. We will be editing this to fit our own needs.

Now to specify what URL to redirect from and to, delete everything inside that section and enter in this.

Spoiler ([Click to View](#))

This will redirect anyone on the LAN to your router login page whenever they use google.ca or any google searches. Keep in mind that you can also add other things to the list to annoy the person even further. Remember, the goal is to annoy the person who has the router password so much that he/she logs in to the router to find out what's wrong.

For example, it can look like this to piss the person off further

Spoiler ([Click to View](#))

Save the file and exit it and open up a terminal. Do this by pressing the black button in the top right corner.

Spoiler ([Click to View](#))

Now we will use the command

Code ifconfig

Look on the very left. Mine says eth0 but yours may say something else, for example wlan0. Remember what it says, it's very important. If you get multiple results, use the one that contains your local IP. It should be similar to your default gateway. Mine is 192.168.1.166

Spoiler ([Click to View](#))

Now, finally we will commence the sniffing and redirecting. Enter in this command into another terminal

Code ettercap -Tqi eth0 -P dns_spoof -M ARP // //

Replace eth0 with whatever it was that was displayed when you used "ifconfig" There are other variations of this command, other options you can use, other targets you can target. In this example, we will be redirecting everyone in the whole network (hence the "// //")

This is what it should look like

Spoiler ([Click to View](#))

When it starts listing some IPs, it means that it has started to sniff the network and everything should now be working. You can test it yourself by trying to go to one of the websites that you put in the etter.dns file. You should be redirected to the router login window.

The minute that someone logs into the router, it will start spamming the window with the user and pass. This is what mine looked like.

Spoiler ([Click to View](#))

As you can see, the username was "admin" and the password was "Restricted"

THIS CONCLUDES MY TUTORIAL ABOUT HOW TO SNIFF YOUR ROUTER'S PASSWORD!
PLEASE POST, ALL YOU HAVE TO DO IS CLICK THIS BUTTON [HERE](#)

Sicarius - February 3, 2013, 9:39 pm

Well I never knew this. Good HQ tutorial! Well done.

einFreak - February 3, 2013, 9:45 pm

Thank you SO much! I will try this after school! Thanks a LOT!

SouqlRS - February 4, 2013, 12:24 am

(Feb 3, 2013 10:45 PM)einFreak Wrote: [\[CITE\]](#) Thank you SO much! I will try this after school!
Thanks a LOT!

Feedback please, did it work? ?

Turtle™ - February 4, 2013, 1:56 am

(Feb 4, 2013 01:24 AM)SouqlRS Wrote: [\[CITE\]](#) Feedback please, did it work? ?

Why? You've got nothing to lose from trying it. Try it yourself and see if it works yourself, it's all free and pretty easy.

DarkNecr0n - February 6, 2013, 11:12 am

Thanks but how can you disable it again? I tried to stop the command and also shut the virtual machine down but im still getting redirected :/

Edit: Ok nvm. DNS Flush solved it

BlackOverride - February 6, 2013, 12:52 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

Rainb?w Dash - February 6, 2013, 4:57 pm

Wow thanks man it always made me mad when Rarity changed the router password. <3

James Franco - February 8, 2013, 10:51 am

Thanks for this great tutorial I really appreciate the hard work that you put into this

Porcupine - March 19, 2013, 3:12 pm

Wow, i'm going to try this right now and see if this works!

What does HQ mean btw?

andq1 - March 19, 2013, 3:32 pm

(Mar 19, 2013 03:12 PM)Porcupine Wrote: [\[CITE\]](#) Wow, i'm going to try this right now and see if this works!

What does HQ mean btw?High Quality.

But yes indeed very nice tutorial, this wont come me handy because our stupid ISP has blocked port forwarding and so on because my mothers work pay for the Internet >.<

on-silo - March 19, 2013, 9:08 pm

Great read, turtles been putting out some awesome stuff, i havent tried this will test soon.

Zabuza? - March 19, 2013, 10:26 pm

HQ Post, thanks! Imma go and see if this works right now x3

(Mar 19, 2013 03:12 PM)Porcupine Wrote: [\[CITE\]](#) Wow, i'm going to try this right now and see if this works!

What does HQ mean btw?

HQ Means "High Quality" ? (I need 35 characters so just ignore this <--)

Canardo - March 20, 2013, 9:43 am

Wow thanks man it always made me mad when Rarity changed the router password

denyx - March 21, 2013, 1:32 am

I will try this on my wimax bm622i... i don't know the admin password..

Do you think this will work?

Turtle™ - March 21, 2013, 10:10 am

(Mar 21, 2013 01:32 AM)denyx Wrote: [\[CITE\]](#) I will try this on my wimax bm622i... i don't know the admin password..

Do you think this will work?

It will work as long as the connection is not encrypted

herrdeutschland - March 21, 2013, 10:48 am

i ve bookmarked this ,thanks for posting about it and keep up the good work

FireBlast - March 21, 2013, 1:55 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

Dani M - March 21, 2013, 2:22 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

CyberFPS - March 21, 2013, 4:14 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

j-lee - March 21, 2013, 5:03 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

Haseo™ - March 21, 2013, 5:17 pm

turtle you've made a very informative and helpful thread. You sir are a high quality member. Thank you for the share.

nicksaban1 - March 21, 2013, 6:06 pm

Good tut. I knew about this already, but I wish that I had a guide this simple and effective when I taught myself to use it.

toddyuk - March 31, 2013, 5:32 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

mini2476 - March 31, 2013, 7:07 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

Mon238 - March 31, 2013, 8:01 pm

Gonna try it out now.. Hope it works!!! :) Thank you

CX007-KHS - April 1, 2013, 1:20 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

Madara-Uchiha - April 1, 2013, 2:00 pm

Very helpful tutorial. Great member and HQ threads! ?

Cornflower Blue ???-? — April 2, 2013, 7:27 am

Thanks for this great tutorial I really appreciate the hard work that you put into this

smokie8090 - April 2, 2013, 8:13 am

Good HQ tutorial! Well done I like it

metall123 - April 2, 2013, 8:23 am

Thanks for this great tutorial I really appreciate the hard work that you put into this

chawk - April 2, 2013, 8:31 am

Thanks for this great tutorial I really appreciate the hard work that you put into this

kill3ry0u - April 2, 2013, 9:09 am

Thanks for this great tutorial I really appreciate the hard work that you put into this :)
Have to try it :)

Sinterklaas - April 2, 2013, 12:39 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

m0resleep - April 2, 2013, 12:50 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this ?

rester64 - April 2, 2013, 2:57 pm

very nice mate looks great thanks for thattt

polaczek123 - April 3, 2013, 2:15 pm

Why i know this? But i like tutorials! Thanks man!

nepetalactone cycloalkane - April 3, 2013, 2:16 pm

Thanks for making this will try this later.

prodigyhf - April 3, 2013, 2:20 pm

Fantastic tutorial OP. Will definitely use this in the future.

muzzy. - April 11, 2013, 3:20 am

Thanks for this great tutorial I really appreciate the hard work that you put into this ?

n0tacop - April 11, 2013, 5:36 am

just tried this out, GREAT JOB! I am going to go find more tutorials!

mr.fifou52 - April 11, 2013, 7:31 am

Great tutorial, I really appreciate the hard work that you put into this. Thanks ;)

tazbox2 - April 11, 2013, 10:07 am

Thank you, good tutorial I'm going to work.

Omarito - April 11, 2013, 11:31 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

Angryflash - April 12, 2013, 10:29 am

Can this be done just to sniff the password when they enter it into the default gateway? Like to pretty much get the password when they are trying to look at the router logs?

alexfaf - April 12, 2013, 10:43 am

Great Job! Thanks for this tut ?

Shkelqimi - April 12, 2013, 1:18 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this, and i have few questions !

1.Does it matter how is connected VMware, is connected NAT

Picture <http://snag.gy/pB9z7.jpg>

2.When i try to open Facebook, which I choose to spood this website, I can see that facebook.com spoofed to 192.168.1.1. see picture below

<http://snag.gy/8XX8j.jpg>

I dont get any prompt to type username and password of router panel !

3.When I try to open facebook.com, from other PC, connected to network, I dont get spoofed, so facebook opens normally, and I dont get any message on backtrack, saying 'spoofed'.

How to fix this prpbem ?

Finearts - April 12, 2013, 4:48 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

Nightstalk3r - May 14, 2013, 7:44 pm

Thanks alot, this tut really helped me! ?

loco1 - May 14, 2013, 10:05 pm

Thank you, good tutorial..will this find my neighbors internet password?

Turtle™ - May 14, 2013, 11:52 pm

(May 14, 2013 10:05 PM)loco1 Wrote: [\[CITE\]](#) Thank you, good tutorial..will this find my neighbors internet password?

No it will not, you have to be connected to the victim's network already in the first place. This was designed for people that are connected to a router and want to access it but don't want to reset it and don't know the password. It doesn't work if you aren't connected to it already, hell, you can't even get the login screen until you're actually on the LAN.

SouqIRS - May 15, 2013, 1:18 am

Thanks for this great tutorial I really appreciate the hard work that you put into this

Utopia - May 15, 2013, 6:40 am

How often do ordinary people log into their router? Some don't even know their password yet alone how to log into the router. I'll be waiting for years. Correct me if I'm wrong.

hejmark99 - May 15, 2013, 7:10 am

Thanks for this great tutorial I really appreciate the hard work that you put into this

Turtle™ - May 15, 2013, 8:10 am

(May 15, 2013 06:40 AM)Utopia Wrote: [\[CITE\]](#) How often do ordinary people log into their router? Some don't even know their password yet alone how to log into the router. I'll be waiting for years. Correct me if I'm wrong.

I'm guessing you didn't even read the tutorial? If you follow this tutorial, whenever your victim tries to go to a website (you can specify which website or websites), it'll bring up the router login page. Eventually, the person will get annoyed and simply log in to see what's wrong.

rand0 - May 17, 2013, 9:14 pm

Nice tut. The method I use is super long and complicated and involves a clone honeypot network etc. I think I like yours better. I will definitely give this a try!

Harry Fotter - June 19, 2013, 4:44 am

Hey man, it keeps say "Activating dns_spoof plugin" do i need to reinstall Bt? Do you have any idea what might be the problem? Thanks! (I already updated)

globemasters - June 19, 2013, 10:08 am

really it help me find my cisco router password
thanks for the share mate.

matixd12345 - June 19, 2013, 10:50 am

Thanks for this great tutorial I really appreciate the hard work that you put into this

B0\$\$ - July 8, 2013, 8:17 am

Thanks for this great tutorial I really appreciate the hard work that you put into this

Alex© - July 8, 2013, 9:38 am

Thanks for the tutorial, will really help people who are forget passwords like this

Illicit - July 8, 2013, 7:45 pm

Lolled so hard,
Sure....Of course 'apt get update' is to update Backtrack.

:D

(Great tutorial though)

SuperMario180 - September 26, 2013, 8:15 am

Nice Tuturial, thank you. It worked fine :)

IceTimux - September 26, 2013, 11:56 am

Thanks for the share this is a very good and HQ tutorial and I can see that allot of time and work has been put into it , :D

vico100 - October 20, 2013, 1:17 pm

thats a good tutorial . thanks for your time :)

xXNepalmXx - October 20, 2013, 1:23 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

onlineman - October 21, 2013, 4:27 am

I have a question, should I have physical access to the router or not ?

onlineman - October 21, 2013, 4:28 am

I have a question, should I have physical access to the router or not ?

Edit: Sorry for double post ?

hatrick - October 21, 2013, 4:29 am

Thanks for the Awesome and Easy to understand TUT!

le0ram - October 21, 2013, 10:38 am

Wow really good TUT, thanks a lot! Helpful, nice and explained.

TheDanishMods - October 22, 2013, 1:49 am

Thanks for this great tutorial. ?

iseeyou21 - October 23, 2013, 4:10 pm

This is an awesome tutorial. One question though:

Would this still work even if the router doesn't use basic authentication? For example, a network using the Xfinity/Comcast Wireless Gateway. Plugging in the Default Gateway (10.0.0.1) would direct to a WebGUI to login to the router.

yeemun - October 23, 2013, 9:19 pm

Thanks for this great tutorial , step by step , I will test it after download backtrack , Ty

Ramboy - October 24, 2013, 12:29 pm

This is awesome! Thank you for this tutorial. I did it on my home network and it worked like a charm. One question though:

How do I restore everything back to normal on all machines? I have 2 devices that i tested to use as a victim, and the only way to restore all webpages to normal is to flush the dns on every computer. Is there a way to do it remotely using backtrack too?

Hulkadin - October 26, 2013, 6:04 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

???Senpai - November 14, 2013, 9:18 pm

HQ tutorial, awesome work! I really appreciate the hard work.

asifa123 - November 14, 2013, 9:34 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

quiteer - November 19, 2013, 10:00 am

didnt work for me. might did something wrong :P maybe it is because my isp stays in control of the password at all times.

abdjoseph - November 19, 2013, 4:56 pm

Great tutorial.. Will definitely come handy.. thanks mate

Meaps - November 19, 2013, 5:53 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

lol

Wolfz - November 19, 2013, 5:55 pm

Thanks for share this, i will try to do it on my router.

multinotserp - December 5, 2013, 5:27 pm

It doesn't redirect... Also for the part where you need to pick one of the adapters (I think thats what they are) mine lists only twp: eth0 and lo but neither contains anything close to my local address.

StuffisKewl - December 7, 2013, 4:18 pm

Thanks! This is an awesome post. I will use this in the future :D

HarveySpecter - December 7, 2013, 6:59 pm

Thank you finally someone posted a thread like this. Keep up the great work.

Lines - December 15, 2013, 9:51 pm

Wow, very big thanks for this.

Took a few tries but I finally figured everything out, and I realized how easy it was at the end.

Thanks for this step by step tut.

My brother can change the password all he wants now, but anytime he goes on XDA, he will get that Default Gateway problem. & I will get that password <3

Dark Skies - December 17, 2013, 7:10 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

nice link too ;)

JovenRanger - December 17, 2013, 8:26 pm

how to sniff if different segmentation or want sniff Vlan ?

grady - December 17, 2013, 8:35 pm

Thanks, time to use this to mess with people.

DLeh - January 3, 2014, 7:59 am

Thanks for this great tutorial I really appreciate the hard work that you put into this.

Also quite easy to understand for newbs like me (:

StarCraft 2 - January 3, 2014, 8:01 am

Thanks for this great tutorial I really appreciate the hard work that you put into this

Mnikkilla - January 3, 2014, 8:17 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

mystry - January 4, 2014, 2:17 pm

thx....alot dat was helpfull ..i hope u keep going wid dat great tutourial

toxicstresser - January 4, 2014, 7:55 pm

Nice tutorial man! im going to test er now :D

anon_350 - January 5, 2014, 5:37 am

does this work if i run BT5r3 on computer A and wait for someone to log in on computer B (both on the same LAN)?

artisz - November 19, 2014, 4:55 am

Thanks for this great tutorial I really appreciate the hard work that you put into this

TheDome - February 20, 2015, 5:27 am

Thanks for this great tutorial I really appreciate the hard work that you put into this

h?ck?r - February 20, 2015, 7:29 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

Shinigami-san - February 21, 2015, 12:02 am

smart way of getting router's password by arp spoofing

OzTech - February 21, 2015, 4:49 am

Thanks for this great tutorial I really appreciate the hard work that you put into this

Instanz - February 21, 2015, 10:15 am

Thanks for this great tutorial I really appreciate the hard work that you put into this

TheLegendaryHatman - May 17, 2015, 11:42 pm

This will be very useful to leave running around schools and stuff, tyvm.

Unpuzzled - May 19, 2015, 7:36 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

Wow, i'm going to try this right now and see if this works!

tehrewinds - June 6, 2015, 5:23 am

wow...nice find man, def gonna have to try later.

MoneyMatters - June 6, 2015, 4:59 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

kunalkhari - June 6, 2015, 10:25 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this?

pr3lite - October 27, 2015, 7:56 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

limainfinita - October 31, 2015, 8:08 pm

check your pms please

and thank you, really nice tutorial

Slightning - November 1, 2015, 3:15 am

Thanks for this great tutorial I really appreciate the hard work that you put into this

steev - November 1, 2015, 9:02 am

can you explain how to sniff router on windows ?

saxlamara - November 1, 2015, 6:00 pm

nice :) in't any problem for router to crash from the traffic ?

Janekkowal - November 4, 2015, 4:48 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this ...

JOW - November 4, 2015, 4:54 pm

Hahah very easy and very clever it could be very useful thanks for the share!

picachu17 - May 31, 2016, 1:40 am

Thanks for this great tutorial I really appreciate the hard work that you put into this

xDerRuedix - June 1, 2016, 2:57 am

This is a HQ tutorial, thankssss

Toto1234 - June 1, 2016, 6:55 am

Thanks for t?his great tutorial I really appreciate the hard work that you put into this

DePeep - September 4, 2016, 2:40 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

TitaniumCreeper - September 5, 2016, 12:50 pm

Gonna try, seems cool! Hope it works :D

giggetto94 - September 9, 2016, 11:45 am

Amazing thread and great tutorial thanks for sharing!

San-Toss - December 12, 2016, 8:13 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

Atomikx - December 14, 2016, 6:16 am

so you're basically intercepting the pass and username but without any deauth method

RCE - December 19, 2016, 11:58 pm

i know exploit that called num0, in tb-link routers can grab router password, btw thanks for sharing ur method

Warxz - December 20, 2016, 3:56 am

Great tutorial! Thanks a lot for sharing this with us!

ez11 - June 20, 2017, 12:33 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this

provider - June 22, 2017, 2:14 am

nice tut

thanks for share

Misuu - June 23, 2017, 8:03 pm

Thanks for this great tutorial I really appreciate the hard work that you put into this??