

Forum:[Hack Forums](#)

Thread: [Legion | ARP Poisoning | Alternative To Cain & Abel](#)

Niggz - January 13, 2014, 1:06 pm

- ARP Poisoning -

What is ARP Poisoning?

ARP Poisoning or ARP Spoofing is an attack where the hacker cracks into the victims Address Resolution Protocol and redirects all the traffic that the victim is receiving or sending to themselves. In this attack the hacker has the ability to become the Man in The Middle which can actually edit the packets that are interacting with the victims computer. That basically means that the hacker can deliver fake messages from one person to another or do what ever he wants with them. I'll give you an example of what I mean.

Quote:Josh(Victim): (Sent) yo wazzup mah home shizzle Fred!

(Means To Send It To Fred But Gets In Hands Of Hacker Instead.)

Quote:Hacker: (Receives) yo wazzup mah home shizzle Fred!

(Edits Message To) Fred your gay

Before You Start:

Please note that you will need BackTrack 5 or Kali Linux for this to work. If you do not have it then this tutorial will not help you in any way.

1. Open up the Terminal on the Backtrack desktop and type this to enable IP Forwarding:

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

2. After the previous code was entered Type This:

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

3.Finally type this in:

Code `sslststrip -p -l 1000`

Now that you have ARP Poisoned you are ready to become the Man In The Middle.

Open up a new tab and type:

Code `arp spoof -i eth2 -t (victims IP v4 Address here.) (Your Backtrack IP v4 Address.)`

Note that this could easily be used as an alternative to Cain & Abel/Wireshark when pulling IP Addresses.

tobi7400 - January 13, 2014, 1:10 pm

Do you mind adding some picture for noobs?

And is this only on lan network?

Im gone brah - January 13, 2014, 1:13 pm

Address Resolution Protocol poisoning is easily made with ettercap.

You should explain what the functions does and so on, this is one of the shortest guide, I've seen in a long time.

Niggz - January 13, 2014, 1:15 pm

(Jan 13, 2014 02:13 PM)Zayne Wrote: [\[CITE\]](#) Address Resolution Protocol poisoning is easily made with ettercap.

You should explain what the functions does and so on, this is one of the shortest guide, I've seen in a long time.

I just wanted to release an alternative method.

Im gone brah - January 13, 2014, 1:17 pm

You don't need backtrack or Kali in order to get this to work.

Also I want to add that you could easily install a package to get that running on a normal linux distro.

Niggz - January 13, 2014, 1:19 pm

(Jan 13, 2014 02:17 PM)Zayne Wrote: [\[CITE\]](#) You don't need backtrack or Kali in order to get this to work.

Also I want to add that you could easily install a package to get that running on a normal linux distro.

"I just wanted to introduce a new method to hackforums" -SI0w

Vincenzo? - January 13, 2014, 1:23 pm

(Jan 13, 2014 02:19 PM)SI0w Wrote: [\[CITE\]](#) "I just wanted to introduce a new method to hackforums" -SI0wWhat are you talking about new method?

http://www.youtube.com/watch?v=zG-_Y17lKpg
2007.

and it's dated even back.

Crake - January 13, 2014, 1:24 pm

I love it! I've been wanting to do ARP spoofing manually for a while.

CodeEcho: Seriously? There's not a tutorial on HF yet about it; probably because certain skids would find it too confusing. Obviously the method has been around for much longer (in fact, it dates back a hell of a lot further than '07 if you'd like to do some actual research)

Vincenzo? - January 13, 2014, 1:25 pm

(Jan 13, 2014 02:24 PM)emanb29 Wrote: [\[CITE\]](#) I love it! I've been wanting to do ARP spoofing manually for a while.

CodeEcho: Seriously? There's not a tutorial on HF yet about it; probably because certain skids would find it too confusing. Obviously the method has been around for much longer (in fact, it dates back a hell of a lot further than '07 if you'd like to do some actual research)Just stating that it's not a new method.

Niggz - January 13, 2014, 1:26 pm

(Jan 13, 2014 02:23 PM)CodeEcho Wrote: [\[CITE\]](#) What are you talking about new method?
http://www.youtube.com/watch?v=zG-_Y17lKpg

2007.

When a teacher in school says "Okay class, today we are going to learn a new subject." Do you think that she means a whole new type of math equation that she has recently discovered that no one else knows about?

Im gone brah - January 13, 2014, 1:26 pm

emanb29 Wrote:-snip-
Was that joke.

Spoiler ([Click to View](#))

Is it hard to open DoS and write in all the commands which he provided? It's noob proof.

/Quit thread

Niggz - January 13, 2014, 1:29 pm

(Jan 13, 2014 02:26 PM)Zayne Wrote: [\[CITE\]](#) Was that joke.

Spoiler ([Click to View](#))

Is it hard to open DoS and write in all the commands which he provided? It's noob proof.

/Quit thread

I think he is saying that all the commands on the thread look intimidating to beginners. But once you get down to it it's not that hard to be honest.

Stop bashing everyone on the thread.

Crake - January 13, 2014, 1:31 pm

(Jan 13, 2014 02:25 PM)CodeEcho Wrote: [\[CITE\]](#) Just stating that it's not a new method.
Agreed; but it's certainly new to HF.

(Jan 13, 2014 02:29 PM)SI0w Wrote: [\[CITE\]](#) I think he is saying that all the commands on the thread look intimidating to beginners. But once you get down to it it's not that hard to be honest.

Stop bashing everyone on the thread.

That is correct. I was referring to the skids who have no idea how to open a bash prompt, and fear white-on-black windows.

Ascendon - January 13, 2014, 2:03 pm

This is obviously too advanced for you

This is not new.

Everyone starts off manually until they find something magic called ettercap.
Sslstrip doesn't work half the time.

Niggz - January 13, 2014, 2:24 pm

(Jan 13, 2014 03:03 PM)Ascendon Wrote: [\[CITE\]](#) This is obviously too advanced for you

This is not new.

Everyone starts off manually until they find something magic called ettercap.
Sslstrip doesn't work half the time.
Jesus, read some of the older posts!

Ascendon - January 13, 2014, 2:34 pm

(Jan 13, 2014 03:24 PM)SI0w Wrote: [\[CITE\]](#) Jesus, read some of the older posts!
Jesus, please learn from older posts on all of your tutorials and improve your overall quality.

Vincenzo? - January 13, 2014, 2:46 pm

(Jan 13, 2014 03:34 PM)Ascendon Wrote: [\[CITE\]](#) Jesus, please learn from older posts on all of your tutorials and improve your overall quality. I highly agree with this post.
?

Niggz - January 13, 2014, 3:08 pm

(Jan 13, 2014 03:34 PM)Ascendon Wrote: [\[CITE\]](#) Jesus, please learn from older posts on all of your tutorials and improve your overall quality.
Quality not quantity.

Learn the difference.

Ascendon - January 13, 2014, 3:20 pm

(Jan 13, 2014 04:08 PM)SI0w Wrote: [\[CITE\]](#) Quality not quantity.

Learn the difference.
I said quality though .-.

Wat even..

Crake - January 13, 2014, 3:39 pm

(Jan 13, 2014 03:03 PM)Ascendon Wrote: [\[CITE\]](#) Everyone starts off manually until they find something magic called ettercap.

Sslstrip doesn't work half the time.

Of course sslstrip doesn't work most of the time, but sometimes it does.

Most people start with Cain & Abel looking up how to hack wifi or hack passwords.

~OMC~ - January 13, 2014, 3:50 pm

Hmm I never knew this I'll keep this in mind in case my cain and able act's up