

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] ~ Man in the Middle Attack via DHCP Exhaustion on Windows Server 2012 R2](#)

Goodies - April 11, 2015, 5:01 pm

When it comes to network attacks, we are constantly looking for the most recent and up-to-date attack vectors in modern network environments. With this tutorial, I'd like to go over the steps needed to become MITM of new network devices in networks with the most up-to-date software (Windows Server 2012 R2 and Windows 8.1). The goal of this is to inform you of how DHCP attacks work as well as protections against them to ensure the most secure environment for your users. This attack does not utilize ARP spoofing, so even if there are anti-ARP-spoofing security measures, such as an IPS or Dynamic ARP Inspection, it should still be able to run. This simple tutorial should give you a better understanding of how your network works.

Explanation:

The Dynamic Host Configuration Protocol (DHCP) was created to allow machines to connect to networks without statically assigning IP addresses and receiving information such as a default gateway, DNS servers, and an IP address. The four-way handshake is as follows:DHCPDISCOVER
A discovery packet is sent from the client to all nodes on the network over UDP. If a helper-address is defined in a router or switch, it can be forwarded to other networks for multi-scope DHCP networks. This is not covered in this tutorial, but the process is the same. This packet is meant to find all viable DHCP servers on the network.

DHCPOFFER

Each DHCP Server on the network that received a Discover packet will send an Offer packet. If the client receives multiple DHCP offer packets, it will select one of the servers based on a number of configuration parameters.

DHCPREQUEST

Once a client has determined which DHCP server it would like to use, it sends out a Request packet to that server letting it know that it would like to be apart of that scope. If there are multiple servers, the ones that were not selected will be sent a Request packet telling it that the client has declined the offer.

DHCHACK

The fourth and final packet is the Acknowledgement packet. This lets the client know that the parameters of the request are valid and the client has been associated with that DHCP scope and can now start using the resources. The DHCP Server will update its leases with the MAC address of the client mapping it to its given IP address.

Quite obviously, before the client has an IP address, all communication occurs on Layer 2 (via MAC address and switching) meaning it is MAC address dependent. The DHCP Exhaustion attack takes advantage of this by spoofing various MAC addresses to allow for multiple DHCP leases on a single client, and using all of the available leases in the DHCP server. This way, clients on the network that attempt to discover a DHCP server will not be able to connect to the real DHCP server (in this case, a Windows Server 2012 R2 machine). They will, however, be able to discover the attacker's machine who can serve them rogue DNS Servers and a Default Gateway without ARP spoofing which can then be used in various data gathering and Man-in-the-Middle techniques.

Tutorial:

In ye olde times, it may have sufficed to quickly write your own DHCP packets with minimal

configuration in SCAPY to run this attack, but as Servers become more resistant to such simple-minded methods, I choose to rely on already-established applications capable of execution this. The program that I will use is called DHCPig and can be downloaded at [this GitHub link](#).

1. Preparation:

We need to install the DHCP server that we will be using as well as download the DHCPig application and enable IPv4 packet forwarding. I have moved the pig file to the /usr/bin directory so I can execute it from anywhere with the pig command.

```
Code echo "1" > /proc/sys/net/ipv4/ip_forward
git clone https://github.com/kamorin/DHCPig.git
cp DHCPig/pig.py /usr/bin/pig
chmod +x /usr/bin/pig
rm -rf DHCPig
apt-get install udhcpd -y
```

2. Rogue DHCP Server:

Once the prerequisites have been installed, we can set up the DHCP server that we will deploy on the network. First, we need to know some information about the network. Attacker IP Address:

192.168.1.10

Default Gateway: 192.168.1.1

DHCP Range: 192.168.1.10-192.168.1.254

When we perform the exhaustion, it is important to exclude the addresses that are already in use. Otherwise, there will be IP conflicts within the network. This is a tell-tale sign that there is an error with the DHCP servers. In my case, there are no other devices, but I will show you how to exclude addresses nonetheless. The UDHCPCD configuration file is located at /etc/udhcpd.conf. You can use nano or the text editor of your choice to make changes.

Important configuration settings: Start and End IP address.

Interface on which UDHCPCD will run.

Different options: opt dns [attacker IP or rogue DNS server]

option subnet [subnet]

opt router [attacker IP]

Excluding IP Addresses with fake MAC addresses. For example: static_lease 00:00:00:00:00:00 192.168.1.4

static_lease 00:00:00:00:00:00 192.168.1.6

static_lease 00:00:00:00:00:00 192.168.1.5

Do not start the UDHCPCD server until you have exhausted the IP's on the legitimate server.

3. Execution:

Before we start the attack, we can see the DHCP server leases which only contains the Kali machine:

Spoiler ([Click to View](#))

Once the Pig application is installed, we simply have to execute pig eth0 where "eth0" is your networking interface.

Code pig eth0

As you watch the exhaustion take place on your machine, we can see the leases in the Windows Server 2012 R2 machine filling up with pseudo-random MAC addresses.

Attacker Machine: ([Click to View](#))

Windows Server: [\(Click to View\)](#)

When you see the following success message, you know that you are ready to deploy the UDHCPCD server. You can do this by starting the udhcpd service:

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

4. Impact:

Since the legitimate DHCP server is no longer capable of handling requests, the rogue DHCP server will be accepting all requests. When a new device joins the network, under these settings, they will use the attacker as the default gateway. Now, since this is not a layer 2 attack, we need to understand that this will only capture traffic that is destined to exit the network. You may still perform a Man in the Middle attack, as well as ARP poisoning to get L2 MITM, but if you are only interested in capturing Internet traffic, then this is perfectly sufficient. The impact that this can have on a network is enormous. After all, you control their gateway.

From a Windows 8.1 machine, I connected to the same network and got an IP address. This is the result:

Spoiler [\(Click to View\)](#)

Note that the default gateway is that of the attacker machine. This means that all network traffic that is not destined for a local network machine will be sent to you for further processing.

Protection:

There are several ways to protect against this attack, however, from my experience as a network engineer, very few network administrators actually implement this as they are often more focused on connectivity and simplicity than on security. Essentially all security engineers absolutely should implement these protections:

Dynamic ARP Inspection:
Dynamic ARP inspection will automatically inspect ARP packets and ensure that the source MAC addresses are coming from the correct port. This will protect against ARP spoofing, but it will do nothing to protect against randomly generated MAC addresses requesting DHCP leases. For example, if a machine on the network has a MAC address of 11:22:33:44:55:66 and is connected to port 30 on the switch, it will not accept any frames with that source MAC coming in on any other port.

MAC Limit Port Security:

Setting a maximum number of allowed MAC addresses per port will thwart the exhaustion attack. It allows only a certain number of devices to be connected to any one port. This is, however, a restrictive feature when using it on dot1q tagged ports ("trunks" in Cisco-speak), but enabling it on ports connected to host devices should be enough. Keep in mind that this will limit the number of virtual machines, for example, that you can run, but even with these two security features enabled, and if the attacker can run this from multiple machines/ports, it still wouldn't be comprehensive protection.

DHCP Snooping:

This is, perhaps, the most important security implementation. Essentially, it only allows certain DHCP packets to be processed on certain ports such as only allowing DHCP servers to reside on a small number of ports. If we just had this enabled on the switches, then the attacker would still be able to exhaust the DHCP leases on the server, but he would not be able to act as a DHCP server. It would be considered a DOS attack since it would deny new clients access to the network, but it is still less severe than becoming a Man in the Middle.

With all three of these protections, it would be very hard to initiate many network attacks and hackers would have to rely on remote exploits instead of network-based methods.

I hope you all learned something and enjoyed this simple tutorial!

Hooded Robin - April 11, 2015, 8:12 pm

This a great write up man, always love reading your stuff ?

I used dhcpg in a similar manner to eat up all available address and force clients to an evil dhcp server to pull off the linux dhcp shellshock attack (root exploit) when it was all the rage not too long ago ?

Goodies - April 11, 2015, 11:21 pm

(Apr 11, 2015 08:12 PM)Hooded Robin Wrote: [CITE](#) This a great write up man, always love reading your stuff ?

I used dhcpg in a similar manner to eat up all available address and force clients to an evil dhcp server to pull off the linux dhcp shellshock attack (root exploit) when it was all the rage not too long ago ?

That's awesome! PinkPanther and I actually wrote a DHCP server config for exactly that!

Also, I know this is simple, but I'm hoping that it will lead to slightly more complex tuts.

Ich - April 12, 2015, 1:48 pm

Very neat tutorial, Goodies! I always enjoy your stuff, I usually learn something new about networking. The possibilities are endless with this :) Simple, yet effective.

Not sure why this thread hasn't received more love

ElVirus - April 12, 2015, 7:40 pm

Nice Guide.

Learned something new. Thx for this Tut!!!

DrDinosaur - April 12, 2015, 7:41 pm

TL;DR. JK. Good job :) Now I have a lot better understanding of this attack.

xtremegamer1882 - April 13, 2015, 5:13 am

Great tutorial. Easy to understand. Thanks for sharing. ?

sp3ctrum - April 13, 2015, 1:33 pm

Very nice and detailed Tutorial goodies! Learned something new today that I will be deploying on my companies network (:

Goodies - April 16, 2015, 11:00 pm

Just under 200 views and 7 replies. Haha.

@-Gator-

I'd recommend NOT doing this in your company's network unless you have explicit permission to do so bcause this WILL cause connection issues; not to mention most companies, mine included, have a "do not hack me" rule in which doing such an attack on employees, even with the most innocent intentions, is still grounds for firing.

I should mention how easy this attack is to detect, by the way. The answer is "very."

1. Look at the MAC addresses of the exhausted IP addresses. With this program, they are in a clear pattern (you can change it in the source, though... keep in mind that no just any random MAC address will work with most modern-day switches. They need to be in certain ranges.)
2. Look at the switches' CAM tables to see which MAC addresses are attached to which port.

Or, better yet, just look at which untagged interfaces have multiple MAC addresses... It's not meant to be a covert attack, but if you do this on a pseudo-public network, there's not much they can do after-the-fact.

sp3ctrum - April 16, 2015, 11:10 pm

(Apr 16, 2015 11:00 PM)Goodies Wrote: [\[CITE\]](#) Just under 200 views and 7 replies. Haha.

@-Gator-

I'd recommend NOT doing this in your company's network unless you have explicit permission to do so because this WILL cause connection issues; not to mention most companies, mine included, have a "do not hack me" rule in which doing such an attack on employees, even with the most innocent intentions, is still grounds for firing.

I should mention how easy this attack is to detect, by the way. The answer is "very."

1. Look at the MAC addresses of the exhausted IP addresses. With this program, they are in a clear pattern (you can change it in the source, though... keep in mind that no just any random MAC address will work with most modern-day switches. They need to be in certain ranges.)
2. Look at the switches' CAM tables to see which MAC addresses are attached to which port.

Or, better yet, just look at which untagged interfaces have multiple MAC addresses... It's not meant to be a covert attack, but if you do this on a pseudo-public network, there's not much they can do after-the-fact.

Yea this needs more attention, guessing even with pictures, etc.. most users just don't understand or run away lol Thanks for the extra tips as well Goodies, and I wasn't going to run this on my companies main network, defiantly wouldn't end well for me xD Was just saying patch it because I'm a server administrator and most of our machines are Windows 08-12 and I'm quite sure this can be pulled off on our network. Just going to setup a test lab to present and deploy the given security measures.

Goodies - April 16, 2015, 11:18 pm

There's really no patch for this because it isn't a Windows error. In fact, blocking DHCP requests could block legitimate requests.

People can't seem to figure out that we, as security admins, know what you're doing. You're not in the shadows. When there's an attack on my network, 90% of the time it's very easy to find not only the machine, but its physical location within minutes of the attack actually being executed.

powerl105 - April 17, 2015, 1:05 pm

good stuff. going to test it out.....

amg64 - April 18, 2015, 2:39 am

Such an awesome thread with full of information, I was following most of your thread and what I can simply say that you making a very neat tutorial regardless of the readers is newbie or advanced. Thumbs up!

Keep sharing your information bro.

Lord_pYrOs - April 19, 2015, 8:46 pm

Very well written Goodies, this section needs more posts like this.

Goodies - April 20, 2015, 2:05 am

Hey, I appreciate it you guys. I'm always learning new security implementations at work. This attack is old, but effective nonetheless. I hope to have a tutorial on NTLM relaying and some SMB attacks for you all soon.

Windows 2012 R2 and 8.1 are vulnerable to RDP login via NTLM hashes. Should be interesting since they're the newest (available) OSes.

phuqer - April 21, 2015, 3:44 pm

As always, great job Goodies. If only we had more of you.

Hooded Robin - April 21, 2015, 8:12 pm

(Apr 21, 2015 03:44 PM)phuqer Wrote: [CITE](#) As always, great job Goodies. If only we had more of you.

i tried to use the recent mod_copy exploit to download and copy him, but all my attempts failed... I think he doesn't use proFTP ?

Valour - April 21, 2015, 10:08 pm

Cool tutorial there mate.. Looking at this, there are many different things that could be done.. DoS attacks against the whole network since we exhaust the DHCP server, exploits will become easier as we get more information about each device with ease, and many more (can't think of them now :D)

Archer - April 23, 2015, 10:06 am

I went and tested this out at a large public wifi and it seemed to work. I don't know much on pentesting or exploiting, but if I could figure it out then almost anyone could. Very well written guide here. Thanks so much!

#Skyline - April 24, 2015, 4:43 am

This is a very well explained tutorial.

This as been bookmarked :)

Gonna try this out on my test windows server at uni.

n0rtr3x - April 24, 2015, 1:34 pm

Well detailed tutorial. Thanks a lot bro :)

dotslash - April 25, 2015, 1:36 am

Very detailed tutorial , thank you , i just love MitM attacks!

Goodies - May 15, 2015, 4:06 pm

So, yeah, bumping because I got a PM regarding this thread... maybe someone else is interested?

pomwtin - May 15, 2015, 6:20 pm

Nice one Goodies :)

Do you maby know how widely "limit per MAC" is used?

I give this a go some time ago because of arp poisoning detection, but 2011 year (by other words relatively old) router didnt let me exhaust DHCP completely. So that left me under impression that this kind of attack does not have many chance of suceesing if attacker is not able to reconfigure

router.

I remembered now when i saw this thread and saw a chance to ask :)

Thanks :)

Goodies - May 15, 2015, 6:26 pm

(May 15, 2015 06:20 PM)pomwtin Wrote: [\[CITE\]](#) Nice one Goodies :)

Do you maby know how widely "limit per MAC" is used?

I give this a go some time ago because of arp poisoning detection, but 2011 year (by other words relatively old) router didnt let me exhaust DHCP completely. So that left me under impression that this kind of attack does not have many chance of suceesing if attacker is not able to reconfigure router.

I remembered now when i saw this thread and daw a chance to ask :)

Thanks :)

There are a couple of ways I can interpret this.

- 1) Limit DHCP Leases per MAC address
- 2) Limit MAC Address per port as per port security.

Well, to answer 1), it's very common to only allow 1 or so DHCP leases per MAC address. I don't even know how you can get multiple. The point of this DHCPig program is to spoof pseudo-random MAC addresses so that no two are the same.

As for 2), it's sad how uncommon it is. I very rarely ever see anything compliant with switch security best practices in live environments. In a switch, you should always limit the number of MAC addresses to a small amount (generally 5 to allow for VoIP phones and virtual machines if that's your thing), but it is often a huge hassle in large companies. Basically, any time you switch out a VoIP phone or change your network card, you get a new MAC address, and limiting them to 2 or so means you have to manually go in and override it. This isn't bad in a SMB (small to medium business), but in the corporate environments I work at, it becomes a huge hassle.

Does this answer your question at all, or were you asking something else entirely?

pomwtin - May 15, 2015, 6:35 pm

Yes, you answered my question, thanks!

Sory I specified my question so badly... I had in mind MAC per port.

Good to know this, looks like i misjudged it a bit..

Dmitriy - May 15, 2015, 9:33 pm

Great tutorial Goodies as always. I'll definitely try this out in the home lab environment. You make a lot of great tutorials, do you have your put together thread with links to all tutorials? that would be great, as it makes so much easier to find something.

Goodies - May 15, 2015, 11:40 pm

(May 15, 2015 09:33 PM)Hp88 Wrote: [\[CITE\]](#) Great tutorial Goodies as always. I'll definitely try this out in the home lab environment. You make a lot of great tutorials, do you have your put together thread with links to all tutorials? that would be great, as it makes so much easier to find something.

This thread has a handful of my favorite tutorials of mine. Check it out!

[\[Tutorial Compilation\] Goodies' Official Hacking Tutorial Compilation Thread](#) by [Goodies](#)

Ctrl4ltD31 - May 16, 2015, 10:02 am

nice tutorial!

I will definitely check out the other ones.

Goodies - May 22, 2015, 2:18 pm

Yesterday I migrated a Linux VM to my desktop that had a dhcp server running, so when I spun it up at my uni, I kinda fucked up our network for a bit by complete accident c:

At any rate, It remix died me of this.

-iLikeRainbows. - May 27, 2015, 3:04 am

Nice write up!

I've explored this avenue a few times in the past, however most clients - If not all, forbid this vector being used. Most of my engagements don't even allow MITM attacks.

However, It's nice to play around with now and then again in the lab!

Armada - May 27, 2015, 3:16 am

This has got to be one of the most thorough tutorials I have read on this site in a long time.

Very good article bro, clear and concise in explanation and the technical aspects required. Ive saved this to PDF for future reference.

Thanks for the article!

setgid - June 4, 2015, 7:57 pm

So.. How to set up a DHCP server on a VM and ARP spoofing?

No need to make it seem so flashy when in reality, it isn't.

Goodies - June 4, 2015, 8:00 pm

(Jun 4, 2015 07:57 PM)setgid Wrote: [\[CITE\]](#) So.. How to set up a DHCP server on a VM and ARP spoofing?

No need to make it seem so flashy when in reality, it isn't.
I don't know what you mean...

Setting up a DHCP server on Windows Server is trivially easy. Watch a video on YouTube.

And also, how did I make it seem 'flashy'? I just provided pictures of what it does and should look like...

Goodies - July 4, 2015, 6:04 pm

Not sure why this popped up in my threads since no one replied, but whatever. I'll bring this backup in case anyone else is interested.

#Skyline - August 20, 2015, 4:30 pm

Came up on google, in top results under dhcpig.
Trying this today in class for a custom lab.
Cheers Goodies.

Goodies - August 20, 2015, 9:42 pm

(Aug 20, 2015 04:30 PM)#Skyline? Wrote: [\[CITE\]](#) Came up on google, in top results under dhcpig.

Trying this today in class for a custom lab.

Cheers Goodies.

I didn't see it on the first page, but I did when I did this:

https://www.google.com/search?q=dhcpig+inurl%3Ahackforums&oq=dhcpig+inurl%3Ahackforums&gs_l=serp.3...7175.9950.0.10387.21.18.2.0.0.0.352.1879.9j3j2j1.15.0....0...1c.1.64.serp..20.1.121.7Ts3WiPyOnE

lol

#Skyline - August 21, 2015, 4:03 am

(Aug 20, 2015 09:42 PM)Goodies Wrote: [\[CITE\]](#) I didn't see it on the first page, but I did when I did this:

https://www.google.com/search?q=dhcpig+inurl%3Ahackforums&oq=dhcpig+inurl%3Ahackforums&gs_l=serp.3...7175.9950.0.10387.21.18.2.0.0.0.352.1879.9j3j2j1.15.0....0...1c.1.64.serp..20.1.121.7Ts3WiPyOnE

lol

I search via Phone, not sure why, but I click a link about dhcpig and I'm now posting within Goodies amazing tutorial. ?

I've set up the windows 2012 R2 server, gotta wait till next week to go back and do the lab. I'll let you know how I go with it.

hfakar - August 23, 2015, 11:41 pm

This tutorial is among the very few tutorials that i read entirely. Thank you, the thread is already in my bookmarks mate.

queryFrequency - August 24, 2015, 3:45 am

You're one cheeky mother fucker to be honest. However, you should explain the commands better, like "echo "1" > /proc/sys/net/ipv4/ip_forward" is to prevent a DoS attack to occur, and that "chmod +x /usr/bin/pig" gives permissions to the file to execute, etc. There are new people here who don't understand that.

There are several other issues I have with this tutorial, but I'll leave it at that.

(Apr 16, 2015 11:10 PM)ChillaXe Wrote: [\[CITE\]](#) Yea this needs more attention, guessing even with pictures, etc.. most users just don't understand or run away lol Thanks for the extra tips as well Goodies, and I wasn't going to run this on my companies main network, defiantly wouldn't end well for me xD Was just saying patch it because I'm a server administrator and most of our machines are Windows 08-12 and I'm quite sure this can be pulled off on our network. Just going to setup a test lab to present and deploy the given security measures.

I hope you die in a fire for just having the skiddy group name "Team Digi7al".

freemium - August 30, 2015, 2:44 pm

nice, I think I need to take some notes :):D