

Forum:[Hack Forums](#)

Thread: [Intercepting packets using man in the middle attack.](#)

demiurge666 - July 1, 2016, 12:20 am

Hello,

I'm trying to intercept and modify packets with python in a man in the middle attack. Is there a module to do that?

Thx in advance.

?BORNE? - July 1, 2016, 5:33 am

I think scapy is used for this kind of work

demiurge666 - July 1, 2016, 6:53 am

Yes, i've done research for this module and i already use it for arp poisoning but apparently scapy can't modify packets on the fly or drop incoming packets to send new ones to the victim.

Preddy - July 1, 2016, 3:26 pm

Scapy is very slick and powerful packet manipulation lib. It offers lot of possibilities. As for you yes It can be done but you need to find a solution that filters packets and pass thru your recv/send app. Likely a kernel module will do the job. [iptables/netfilter]

```
""apt-get install build-essential python-dev libnetfilter-queue-dev""  
""pip install NetfilterQueue"" --> (github.com/kti/python-netfilterqueue)
```

```
pypi.python.org/pypi/NetfilterQueue/  
coresecurity.com/corelabs-research/open-source-tools/impacket  
//secdev.org/projects/scapy/doc/usage.html
```

Now you need to code protocol structure for intercepting packets on fly. (TCP-UDP-ICMP..)

PHP Code

```
<?php  
#!/usr/bin/env python2.7
```

```
from scapy.all import *  
from netfilterqueue import NetfilterQueue
```

```
def modify(packet):  
    pkt = IP(packet.get_payload()) #converts the raw packet to a scapy compatible string  
  
    #modify the packet all you want here  
  
    packet.set_payload(str(pkt)) #set the packet content to our modified version  
  
    packet.accept() #accept the packet
```

```
nfqueue = NetfilterQueue()
#1 is the iptables rule queue number, modify is the callback function
nfqueue.bind(1, modify)
try:
    print "[*] waiting for data"
    nfqueue.run()
except KeyboardInterrupt:
    pass
```

Goodies - July 1, 2016, 4:56 pm

Edit: Oh shit, looks like I'm too late. I started this when I was in LA, but by the time I got back, Preddy had already answered...

Well, I was going to write it using pure SCAPY, but it turned out to be buggy as all hell and not worth posting. The NFQueue way is DEFINITELY the way to go. Keep in mind, it only runs on unix. On Kali 2, you may need to install the packages "libnetfilter-queue-dev" and "libnfnetlink-dev".

If you want me to write a POC, let me know...

demiurge666 - July 2, 2016, 1:01 am

these solutions seems great but it's not available on windows (Sorry for my lack of precision in this thread). I don't want to install a linux distro or a virtual machine just for that. What i'm searching is an alternative of NFQueue for windows.

SIM-2015410 - July 2, 2016, 4:45 pm

(Jul 2, 2016 01:01 AM)demiurge666 Wrote: [\[CITE\]](#) these solutions seems great but it's not available on windows (Sorry for my lack of precision in this thread). I don't want to install a linux distro or a virtual machine just for that. What i'm searching is an alternative of NFQueue for windows.

If you are serious about doing this kind of thing, you will really just need to migrate to Linux at some point. Linux has much better tools and control over things like packet management whereas Windows deals with most of it without giving the user control. There is a reason Linux is used by professionals over Windows.

Goodies - July 2, 2016, 5:38 pm

(Jul 2, 2016 04:45 PM)MeshCollider Wrote: [\[CITE\]](#) If you are serious about doing this kind of thing, you will really just need to migrate to Linux at some point. Linux has much better tools and control over things like packet management whereas Windows deals with most of it without giving the user control. There is a reason Linux is used by professionals over Windows.

If you could condense this to about 5 words or so, this would be what I'd have on my grave stone.

Mr. Robot - July 2, 2016, 5:40 pm

(Jul 2, 2016 05:38 PM)Goodies Wrote: [\[CITE\]](#) If you could condense this to about 5 words or so, this would be what I'd have on my grave stone.

"Just migrate to Linux"

SIM-2015410 - July 2, 2016, 7:19 pm

(Jul 2, 2016 05:40 PM)Mr. Robot Wrote: [\[CITE\]](#) "Just migrate to Linux"

This ^

Its like that verb "defenestrate":

Remove Windows off your computer or throw your computer out the window.

Mr. Robot - July 2, 2016, 8:07 pm

(Jul 2, 2016 07:19 PM)MeshCollider Wrote: [\[CITE\]](#) This ^
Its like that verb "defenestrate":
Remove Windows off your computer or throw your computer out the window.
I also like the expression because his avatar is a bird :)

Anzee - July 2, 2016, 8:09 pm

Try network based attacks like ARP poisoning.

SIM-2015410 - July 2, 2016, 8:14 pm

(Jul 2, 2016 08:09 PM)Anzee Wrote: [\[CITE\]](#) Try network based attacks like ARP poisoning.
All you have done is suggested he do what he was asking lol

Anzee - July 2, 2016, 8:16 pm

(Jul 2, 2016 08:14 PM)MeshCollider Wrote: [\[CITE\]](#) All you have done is suggested he do what he was asking lol
Not really?

He's looking to intercept and modify them and a library like pypcap could do the job but actually intercepting the packets?

Goodies - July 2, 2016, 8:18 pm

I wrote a POC code using purely SCAPY but it ended up not working right on Windows (at least not Python3 port)... I'll post it when I get home but it was nothing special... just make sure you delete BOTH the IP and TCP checksums after modifying the payload O.o that fucked me up for a cool minute...

demiurge666 - July 3, 2016, 12:20 am

Ok linux is great, i've been on it for a while in the past but i've migrated to windows because linux is a pain in the ass for gaming and from time to time i like to play video games. I also think that a true hacker can deal with a shitty os like windows or mac (Plus i don't have enough space on my hard drive to install linux). I think the solution for me is to add a specific rule to the firewall with python but there is no iptable on windows and i really don't understand how to add rules to the firewall with command lines. If i figure it out, i could drop the incoming packets and send my own packets to the victim. For example, the victim want to connect to facebook, i receive the packets, i drop them and i send my own packets to his browser in this way the victim will receive a fake facebook login page or a page that has nothing to do with facebook.

Goodies - July 3, 2016, 7:25 am

(Jul 3, 2016 12:20 AM)demiurge666 Wrote: [\[CITE\]](#) Ok linux is great, i've been on it for a while in the past but i've migrated to windows because linux is a pain in the ass for gaming and from time to time i like to play video games. I also think that a true hacker can deal with a shitty os like windows or mac (Plus i don't have enough space on my hard drive to install linux).

A couple things.

I'm in a similar boat. I've been a Linux user since I was 14, but since I bought my new laptop, I've kept it on Windows for work reasons.

"I also think that a true hacker can deal with a shitty os like windows or mac."

It's not really the skill of the hacker that's in question here... it's the flexibility of the operating system and the availability of low-level networking. Windows is severely limited compared to Linux. Also, Mac is pretty flexible in this area. You can do a surprising amount on a Mac.

Quote:I think the solution for me is to add a specific rule to the firewall with python but there is no iptable on windows and i really don't understand how to add rules to the firewall with command lines.

If i figure it out, i could drop the incoming packets and send my own packets to the victim. For example, the victim want to connect to facebook, i receive the packets, i drop them and i send my own packets to his browser in this way the victim will receive a fake facebook login page or a page that has nothing to do with facebook.

That's not quite how it works O.o

Also, the trouble with facebook is that most browsers have major sites' (facebook, google, yahoo, etc...) SSL certs hard-coded into the browser. You won't be able to hijack it without explicitly installing your fake SSL cert as an accepted cert on their end.

demiurge666 - July 3, 2016, 7:57 am

Oh! I 've forgotten about SSL certificate. So i need to drop the packets from the victims and find a way to have a good certificate? You 've convinced me about linux. I'm gonna go buy a new hard drive and install debian on it.

Goodies - July 3, 2016, 7:58 am

(Jul 3, 2016 07:57 AM)demiurge666 Wrote: [\[CITE\]](#) Oh! I 've forgotten about SSL certificate. So i need to drop the packets from the victims and find a way to have a good certificate? You 've convinced me about linux. I'm gonna go buy a new hard drive and install debian on it.

I suggest using a virtual machine for now O.o there's no point in installing it on a dedicated HDD.

demiurge666 - July 3, 2016, 10:11 am

yes of course but it's not only for linux. I need more space for series and stuff. As i have two HDD i have 2 os.

TERR - July 3, 2016, 9:57 pm

(Jul 2, 2016 07:19 PM)MeshCollider Wrote: [\[CITE\]](#) This ^

Its like that verb "defenestrate":

Remove Windows off your computer or throw your computer out the window.

I love when linux users hate windows because they can't reverse engineer the OS.

It's sad, but most linux programmers are inferior.

OP Look into using a third party driver like winpcap.

Most user-mode packet sniffers hook ws2_32 routines respectively or end up using winpcap. Wireshark uses a NDIS filter.

We are in the python section, so forget about those ideas, just stick to using winpcap. There are many public wrappers written in python.

(Jul 2, 2016 08:16 PM)Anzee Wrote: [\[CITE\]](#) Not really?

He's looking to intercept and modify them and a library like pypcap could do the job but actually intercepting the packets?

winpcap.org/docs/docs_40_2/html/group__wpcap__tut6.html