

Forum:[Hack Forums](#)

Thread: [cannot connect to rogue AP](#)

trogne - May 17, 2017, 3:22 pm

I cannot connect to my rogue AP.

I have strictly followed and revised all the same steps seen on many tutorials.

Here's what I've done :

I have a wired internet connection on interface "eth0" :

/etc/network/interfaces :

Code auto eth0

iface eth0 inet static

address 192.168.1.222

netmask 255.255.255.0

network 192.168.1.0

broadcast 192.168.1.255

gateway 192.168.1.1

dns-nameservers 8.8.8.8 8.8.4.4

Command to start the monitor interface :

Code airmon-ng start wlan0

Now "wlan0mon" is up.

Command:

Code airbase-ng --essid "free hotspot" -c 6 wlan0mon

Access point "free hotspot" is available.

I keep this terminal open.

On a second terminal :

Commands :

Code ifconfig at0 up

ifconfig at0 192.168.2.1/24

File /etc/dhcp/dhcpd.conf :

Code authoritative;

default-lease-time 600;

max-lease-time 7200;

subnet 192.168.2.0 netmask 255.255.255.0 {

option routers 192.168.2.1;

option subnet-mask 255.255.255.0;

option domain-name "free hotspot";

option domain-name-servers 8.8.8.8,192.168.1.1;

range 192.168.2.2 192.168.2.40;

}

File /etc/default/isc-dhcp-server :

Code INTERFACESv4="at0"

Command :

Code systemctl start isc-dhcp-server

Command :

Code iptables-saveOutput :

Code # Generated by iptables-save v1.6.0 on Wed May 17 18:17:29 2017

*nat

:PREROUTING ACCEPT [1919:78709]

:INPUT ACCEPT [65:3788]

:OUTPUT ACCEPT [749:48483]

:POSTROUTING ACCEPT [17:1222]

-A PREROUTING -p udp -j DNAT --to-destination 192.168.1.1

-A PREROUTING -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 10000

-A PREROUTING -p udp -m udp --dport 53 -j REDIRECT --to-ports 53

-A POSTROUTING -o eth0 -j MASQUERADE

COMMIT

Completed on Wed May 17 18:17:29 2017

Generated by iptables-save v1.6.0 on Wed May 17 18:17:29 2017

*filter

:INPUT ACCEPT [56139:15930360]

:FORWARD ACCEPT [7973:922124]

:OUTPUT ACCEPT [48640:11215379]

-A FORWARD -i at0 -j ACCEPT

COMMIT

Completed on Wed May 17 18:17:29 2017

Command for forwarding :

Code echo "1" -> /proc/sys/net/ipv4/ip_forward

Command to add route:

Code route add -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.2.1

Now everything should be ok.

However, if I connect to my AP "free hotspot", I can see on the first terminal that the client is associating (well, trying to associate).

I can also see that DHCP seems to work :

Code May 17 17:58:32 kali dhcpcd[12000]: DHCPREQUEST for 192.168.2.2 from 80:5a:04:d1:cc:33 (android-491cfd6b15033dd2) via at0

May 17 17:58:32 kali dhcpcd[11822]: DHCPREQUEST for 192.168.2.2 from 80:5a:04:d1:cc:33 (android-491cfd6b15033dd2) via at0

But it won't connect to the AP.

If I use my phone next to me, and trying to connect, it will say "connected" for one second, then automatically disconnect.

I use Kali 2. My network card is an Intel Centrino Wireless-N 1000.

If I can't connect to the AP, could it be because of the network card ?

If not, what can it be ?

Thank you for your help!

Patrick

trogne - May 19, 2017, 8:14 am

Or is it possible that new devices (android and hp laptop) are detecting the fake AP and disconnects ?

(edit of main post : "DHCPREQUEST" was followed by "DHCPACK")

quirky - May 19, 2017, 8:55 am

not sure, but with your internal card i don't think that's going to work. with "iw list" you will discover that your wireless card doesn't support some interface modes. it is recommended that you use an external dongle for what are you trying to achieve

trogne - May 19, 2017, 9:36 am

Thank you. That's interesting.

Maybe I'll order an external card and try that on my "Kali VM on Windows 10".

But is there a good card that works with Windows 10 ?

Cause based on what I read, there are absolutely no card that supports "Kali VM on Windows 10" well (maybe you can get connection, but monitor mode won't work, etc.).

If you know a card that works well for "Kali VM on Windows 10", please tell.

Thanks!