

Forum:[Hack Forums](#)

Thread: [who can help me out with scapy?](#)

yourmommy - February 9, 2017, 11:40 pm

who can help me with setting up scapy to deauth a AP on 5ghz 36 channel?

i have never run this program before, and the documentation what i have found is way to complex.

in the mean time i keep searching ofcourse. And if i have found a faster/better way i tell you guys!

Wifi Pineapple - February 10, 2017, 4:06 am

Why not use the aircrack-ng suite?

If you can't deauth with that, it won't work with scapy

pomwtin - February 10, 2017, 4:29 am

(Feb 10, 2017 05:06 AM)rpi3noob Wrote: [\[CITE\]](#) Why not use the aircrack-ng suite?

If you can't deauth with that, it won't work with scapy

DFS channels proves to be a problem... therefor scapy would be an alternative if it is not a driver issue.

OP capture one deauth package, load it in scapy, delete all checksums, modify it for your needs, recalculate checksums, lock to desired channel with airodump and send packet to your interface.

Yes, work with scapy can be a little confusing, and documentation is a bit complex as you already realised, so you'll have to do a bit of learning first.

Here are some docs I came along:

<https://phaethon.github.io/scapy/api/>

<http://www.secdev.org/projects/scapy/doc/>

<http://www.secdev.org/projects/scapy/files/scapydoc.pdf>

yourmommy - February 10, 2017, 8:33 pm

(Feb 10, 2017 05:29 AM)pomwtin Wrote: [\[CITE\]](#) DFS channels proves to be a problem... therefor scapy would be an alternative if it is not a driver issue.

OP capture one deauth package, load it in scapy, delete all checksums, modify it for your needs, recalculate checksums, lock to desired channel with airodump and send packet to your interface.

Yes, work with scapy can be a little confusing, and documentation is a bit complex as you already realised, so you'll have to do a bit of learning first.

Here are some docs I came along:

<https://phaethon.github.io/scapy/api/>

<http://www.secdev.org/projects/scapy/doc/>

<http://www.secdev.org/projects/scapy/files/scapydoc.pdf>

Thanks! I have just tested wifislax with build in program AIRSTORM. I then select 13 DESTRUCTION MODE. And put in the BSSID and the ESSID and the CHANNEL.

And then i got no internet :D. If that program run on my pi too, iam a happy person.

pomwtin - February 11, 2017, 12:58 am

Can you confirm this working on DFS channels too?

yourmommy - February 12, 2017, 5:45 am

(Feb 11, 2017 01:58 AM)pomwtin Wrote: [\[CITE\]](#) Can you confirm this working on DFS channels too?

just tested, and it dont work on DFS channels

pomwtin - February 12, 2017, 5:52 am

(Feb 12, 2017 06:45 AM)yourmommy Wrote: [\[CITE\]](#) just tested, and it dont work on DFS channels
Thanks for trying it out :)