

Forum:[Hack Forums](#)

Thread: [Mana-toolkit on NetHunter + RogueAP infos](#)

Bigj80 - June 7, 2017, 12:06 am

Hi everybody,
greetings from Italy.

I'm having a hard time finding a good RogueAP provider (with captive portal login) on Nethunter 3 on a Nexus 5x.

Wifiphisher and wifi-pumpkin don't work even in VNC session.

Had full hope in Mana-toolkit since it was preinstalled with the distribution, but, almost as any other pre-installed tool, it just don't work properly.

Mana-toolkit doesn't work either on Kali 2017, so my first question is, did anybody manage to make it run properly ? Github repository is full of unresolved issues and the project itself looks pretty outdated and abandoned.

I can run the 'start-noupstream.sh' script and everything seems to be working, but there's no way to make the captive portal show up, as many others are complaining about on the github.

I don't understand if there is a problem with dnsspoof (starts fine and logs entries), dnsmasq (IP, gw, netmasks are assigned correctly), iptables (I have not enough experience with them yet), or apache (service running and captive portal virtual host enabled).

So my second question is: can you suggest me a valid alternative to mana-toolkit fully working on NetHunter ?

Many thanks
S.

Clutch - June 7, 2017, 1:03 am

Haven't been able to find one myself, so I've started creating my own. It's far from done, so if you find a better solution I'd be interested as well

Bigj80 - June 7, 2017, 2:44 am

I will end up writing one too on my own (good exercise I guess), but I feel like it's quite absurd that one of the most useful tools for a mobile penetration testing device just doesn't exist... also wondering why almost ++nothing++ works out of the box in the Nethunter3 image...