OVERVIEW

AutoPixieWps is a script to automate the pixiewps
attack>https://github.com/wiire/pixiewps
for kali linux, and nethunter nexus devices.

Credits goes to Wiire and all who have been working on that
project

this script is meant for people who wants to check if
someone can gain the wpa key,
and or if you are protected from this attack
Any illegal use of this program is strictly forbidden!.

FEATURES

Kill reaver as soon as e-hash2 is gained.

Manual input target router without scan

Wash scan > target router from scan list

Save resuslts to logfile

option to ignore router from wash scan if it has been
cracked, or if PixieWps failed to crack the hash

DEPENDENCIES

since AutoPixieWps not actually an attack, but merely
controls pixiewps and reaver
you need pixieWps and forked reaver that outputs PKE:
AuthKey: E-hash1: E-hash2: hashes.

USAGE

first time, it is needed to add executable permissions for
autopixie.
```
chmod +x autopixie.py
```

to run:
```
./autopixie.py
```

on any promt, input "0" as aswer to go back to menu (exept
under settings when creating new rules)

CHANGES
13.4.2015:
changed autopixie to not run reaver with -S and run
pixiewps with -e -r -s -z -a -n

to be added:
multi attack, attack multiple accesspoints from wash scan,
(if multiple routers are in same channel, it will try
hashing them all at once, and then move on to the next
channel)