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

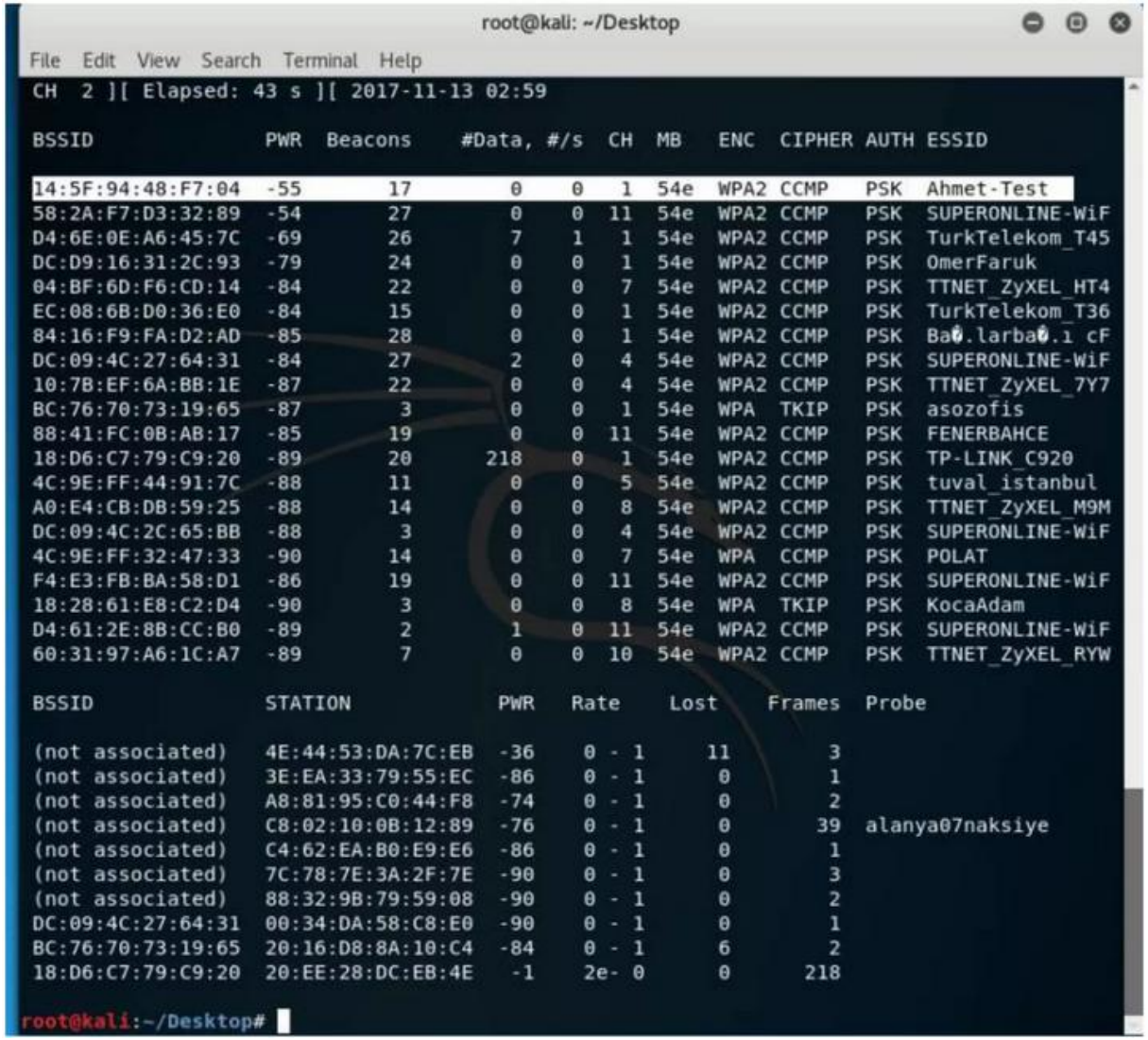
Saldırı Araçları

- **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.

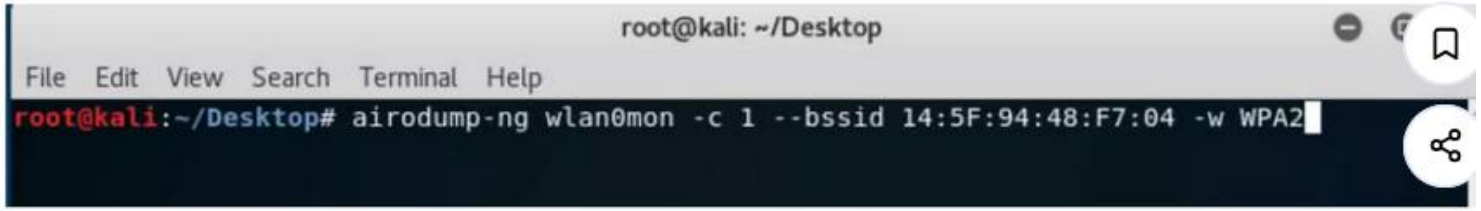
Saldırı Araçları

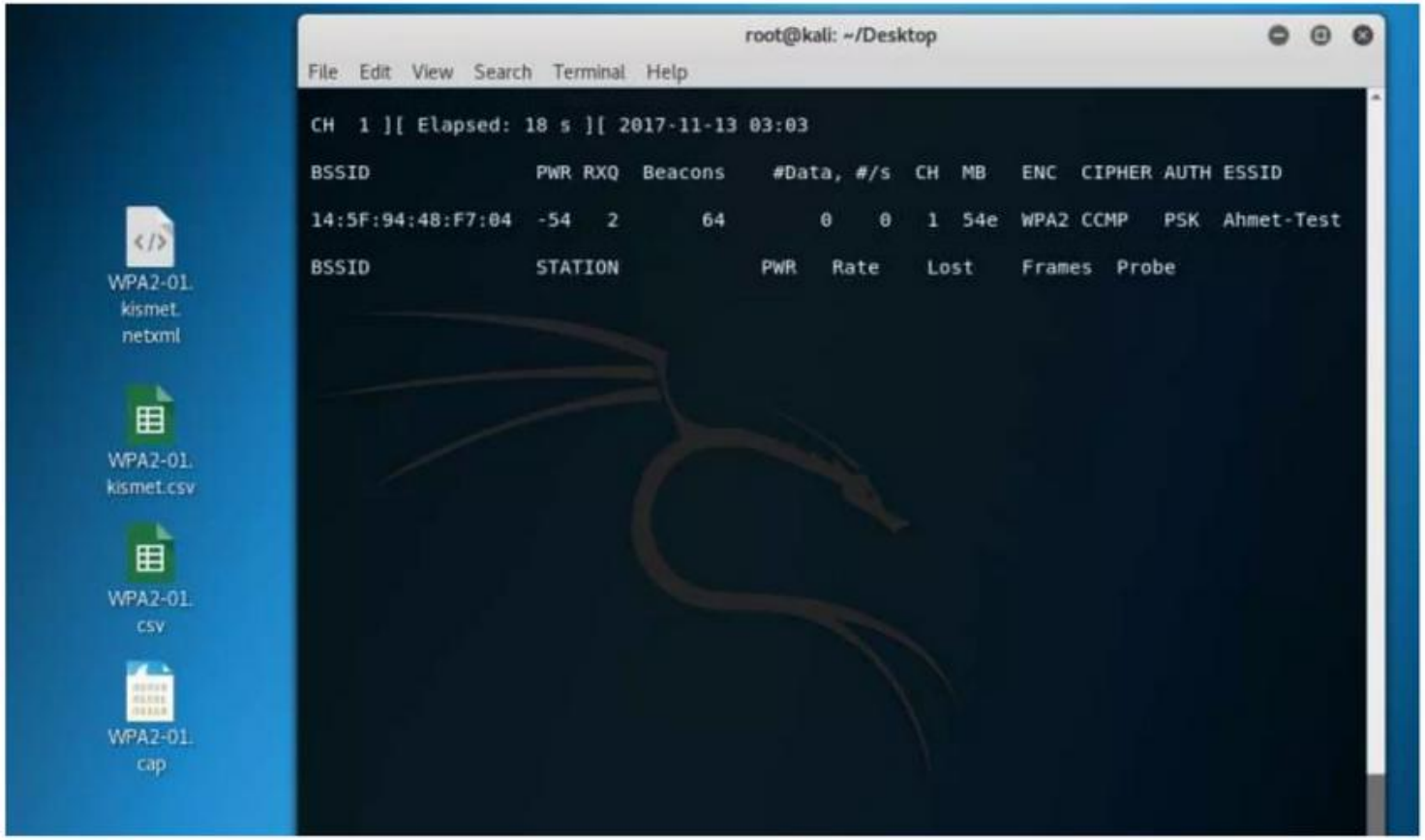
```
root@kali:~# iwconfig
lo        no wireless extensions.

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

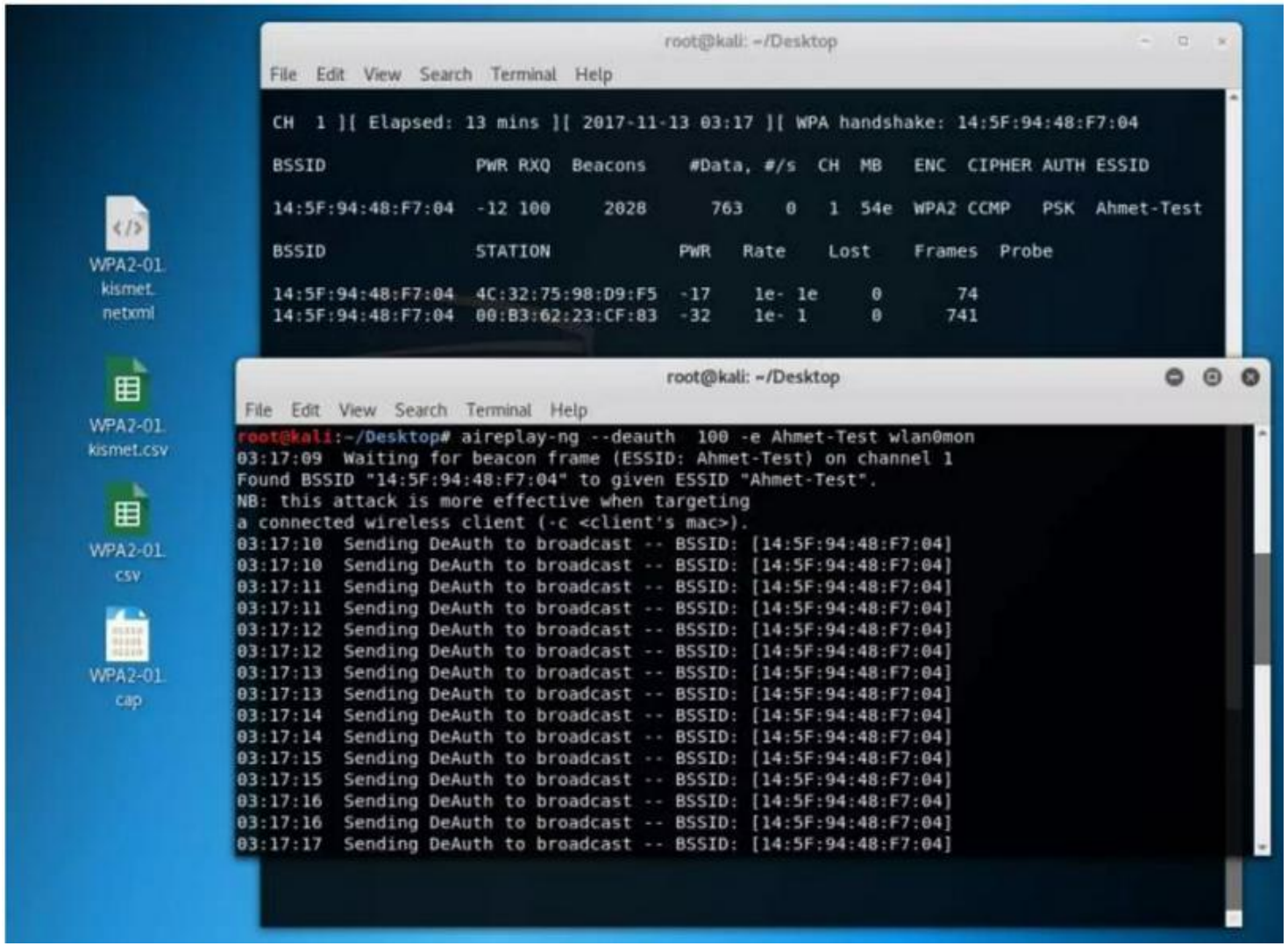


Saldırı Araçları

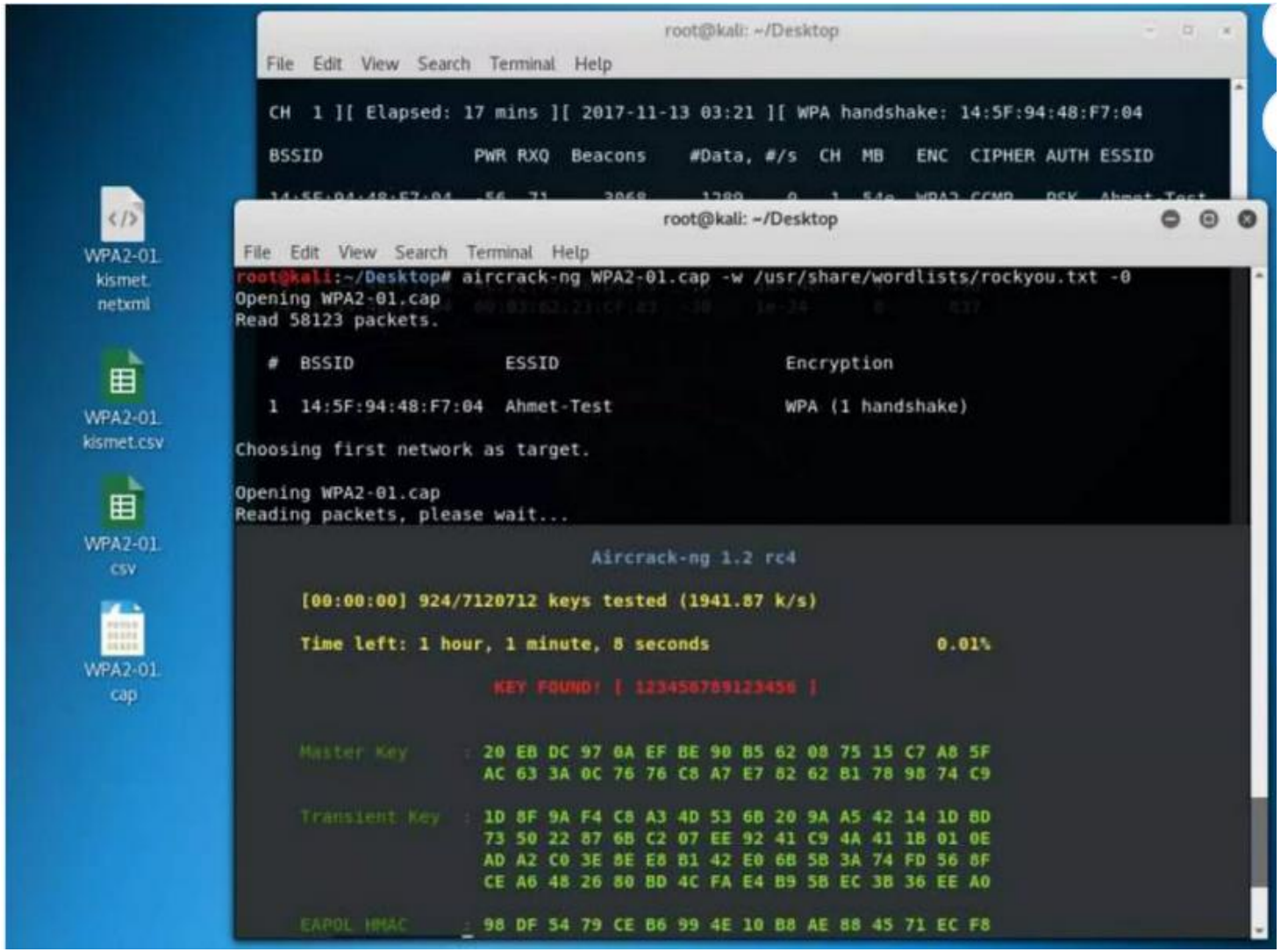




Saldırı Araçları



Saldırı Araçları



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