



# Özgür Yazılımlar ile Kablosuz Ağ Denetimi

Fatih Özavcı

[fatih.ozavci@gamasec.net](mailto:fatih.ozavci@gamasec.net)

Afşin Taşkiran

[afsin.taskiran@avea.com.tr](mailto:afsin.taskiran@avea.com.tr)



- Kablosuz Ağ Güvenliği
- Kablosuz Ağ Güvenlik Denetim Süreci
  - Denetim Kapsamının Belirlenmesi
  - Kablosuz Ağ Altyapısı Analizi
  - Kriptolama Analizi
    - Kimlik Doğrulama ve Yetkilendirme
    - WEP/WPA Kriptolama Kırılması
  - Kablosuz Ağ İstemcileri Analizi
- Denetim Sürecinde Kullanılabilecek Araçlar
  - Araçlar ve Özellikleri
  - Kullanım Amaçları

# Kablosuz Ağlarda Güvenlik Sorunu

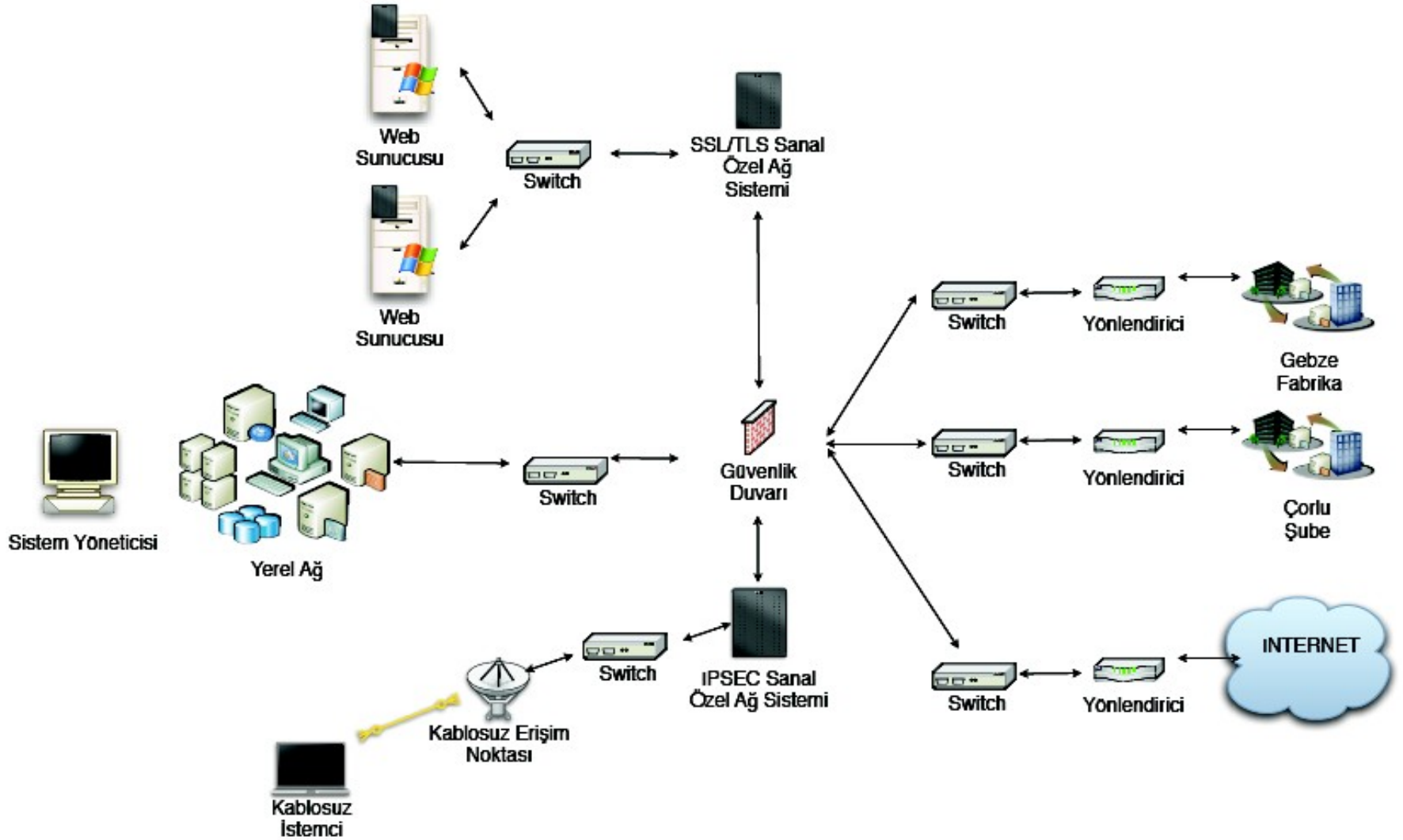


- Kablosuz Ağ Altyapıları, tasarım, yerleşim ve kimlik doğrulama eksikliklerinden kaynaklanan çok sayıda güvenlik sorunundan etkilenmektedir.
  - Açık Erişim, Tekrarlama Saldırıları, Sahte Erişim Noktaları
  - WEP/WPA Kırılması
  - İstemcilerin kandırılması, İstismar Edilmesi
- Kablosuz Ağlar İnternette Daha Güvenli Değildir !!!
- Kablosuz Ağ Güvenlik Sorunları
  - Hatalı Yerleşim Doğrudan Kurum Ağına Bağlantı İmkânı Vermektedir
  - Kriptosuz ve Açık Erişim ile Kullanım
  - Kriptolama Eksiklikleri Nedeniyle Tüm İletişim Dinlenebilmektedir
  - Erişim Denetimi Eksiklikleri Kolayca Kablosuz Ağa Dahil Olunabilmektedir
  - MAC Temelli Korumaların Kolayca Aşılması
  - Kullanıcı Kimlik Yönetiminin Kullanılmaması



- Kablosuz ağ denetimi sezgisel veya anlık tecrübe gerektirmez, kontrol listeleri ile yapılabilir.
  - İyi Planlanmış Kontrol Listesi
  - Kontrollerin Uygulanması için Araçlar
- Kablosuz Ağ Denetiminde Hassas Noktalar
  - Ağ Altyapısı ve Tasarım Analiz Edilmeli
    - Ağ Parçalarının Amacı ve Bağlantıları
    - Yerleşim ve Erişim Denetimi Analizi
    - Kimlik Doğrulama Yöntemleri
    - Kriptolama Kullanımı
  - Kablosuz İstemci Analizi
  - Kablosuz Ağ Yönetim Süreci Analiz Edilmeli
    - İstemcilerin Yönetimi ve Yetkilendirilmesi
    - Yöneticilerin Görevleri ve Hakları

# Kablosuz Ağ Denetim Süreci



# Kablosuz Ağların Saptanması



- Yetkili/Yetkisiz/Sahte Ağları Saptama
- Kablosuz Ağların Özelliklerinin Politikalarla Uyumu
- Kismet, Aircrack-NG

```
Network List (Autofit)
```

Name	T	W	Ch	Packts	Flags	IP Range	Info
! GS-Sample	A	Y	011	57		0.0.0.0	Ntwrks 6
. GS_WR1	A	0	004	218		0.0.0.0	Pckets 328
+ Probe networks	G	N	---	5		0.0.0.0	Cryptd 0
. ZyXEL	A	0	006	10		0.0.0.0	
. buffie	A	0	011	9		0.0.0.0	

```
CH 11 ][ Elapsed: 2 mins ][ 2009-03-13 12:46
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:14:C1:43:73:B0	204	125	0	0	11	54	WEP	WEP	GS-Sample
00:14:C1:43:64:C4	204	218	0	0	4	54	WPA2	CCMP	PSK GS_WR1
00:02:CF:AD:74:7A	184	81	0	0	6	54	WPA	TKIP	PSK ZyXEL
00:1A:2A:BC:2B:06	178	81	0	0	11	54	WPA	TKIP	PSK buffie
00:1A:2A:C8:AB:B1	169	2	0	0	11	54	WPA	TKIP	PSK ADSL

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
00:14:C1:43:64:C4	00:16:CB:B6:81:46	220	0-	1	0	14
(not associated)	00:21:FE:5A:B6:5F	188	0-	1	0	3
(not associated)	00:0D:F0:3E:1E:98	180	0-	2	0	17 iem-01
(not associated)	00:C0:49:56:F3:97	170	0-	11	0	4

```
Status  
Found new prob  
Found new netw  
Found new netw  
Found new prob  
Battery: AC 98%
```

# Kriptolama ve Eriřim Analizi



- Açık Eriřim Sorunu
- Açık Eriřim + Web Temelli Doğrulama Sorunu
- Yetersiz Kriptolama Kullanımı
  - WEP İletişim Kelimesi Tercihleri
  - WPA/TKIP İletişim Kelimesi Tercihleri
- 802.1x / EAP Desteđi
- Kriptolamaya Yönelik Saldırıları
  - Açık Ağda Paket Yakalama, Ortadaki Adam Saldırısı
  - WEP Kriptolaması Kırma
  - WPA/TKIP Kriptolaması Kırma

# WEP Kriptolamanın Kırılması



- Ağla Sahte İlişkilendirme Sağlanır (Sadece İlişkilendirme)
- Ağa Çok Sayıda Sorunlu Paket Enjekte Edilir
- Bir Diğer Kart ile Sorunlu Paketler ve Tüm İletişim Yakalanır
  - Weak IV vs Data
- Uygun Kriptoanaliz Saldırısı Başlatılır (Chop Chop, PTW vb.)

```
Aircrack-ng 1.0 rc2

[00:00:00] Tested 7240 keys (got 11768 IVs)

KB    depth  byte(vote)
0     18/ 25  15(14080) 48(14080) 4A(14080) 58(14080) 91(14080) 95(14080) E7(14080) 0F(13824)
1     2/ 27   43(16384) F1(15616) 37(15360) 3F(15360) F8(15360) 99(15104) BF(15104) 17(14848)
2     6/ 11   CE(15616) 08(14848) 27(14848) 4B(14848) 7A(14848) 7E(14848) A5(14848) E3(14848)
3     0/ 1    75(18944) 10(16384) F7(16128) 93(15872) DA(15616) 3E(15104) A8(14848) C1(14848)
4     0/ 1    43(19200) BB(15872) DC(15872) 93(15360) BF(15360) 37(15104) A5(15104) 33(14848)

KEY FOUND! [ 15:43:22:75:43 ]
Decrypted correctly: 100%
```

# WPA Kriptolamanın Kırılması



- 3 Tür Saldırı Mevcuttur
  - Doğrudan Deneme/Yanılma ve Sözlük Saldırısı Yöntemi
  - PSK Özeti Alınması ile İstenen Sistemde Deneme/Yanılma
    - Sözlük vs Hazır Veri Özetleri
  - Kriptoanaliz ile WPA/TKIP Kriptolamanın Kırılması

```
Aircrack-ng 1.0 rc2

[00:00:00] 4 keys tested (66.39 k/s)

KEY FOUND! [ gamasec123 ]

Master Key      : D3 2D 03 94 1E 72 24 95 B3 1E 75 12 1B 08 0D 6F
                  3A 73 FF B9 F0 BF 2F 6B E3 33 7B D9 0A DC 90 BA

Transient Key   : BE CE 60 B3 E8 DC 03 1A C7 CA FF 74 3E 91 DB C3
                  B0 F4 E1 2A E4 72 01 BA 08 EA A9 87 F0 17 DA 84
                  6B 26 F9 4D 6E 91 1F BC 50 62 AC F8 97 D5 33 41
                  4F 99 F7 0E BD AE A2 9F 41 39 39 E9 D7 93 C6 3C

EAPOL HMAC     : 46 34 6A 31 7C 0F 99 D0 C5 C2 4D F3 34 AD 62 9A
```



- Kurum İçindeki Kablosuz İstemciler Ağ Geçitleridir
  - Yazılım Kurulumunda Otomatik Oluşturulan Açık Ağlar
  - Köprü Bağlantıların Kullanımı
- İstemci İşletim Sistemi ve Yazılım Sorunları
  - Belirli İsimlerdeki Ağlara Otomatik Olarak Bağlanmak
    - Tüm E-postaların Sahte SMTP ile Alınması
    - Web Ziyaretinde Bilinen Browser Açıkları Kullanımı
    - Sahte Dosya Sunucusu/Servisi Oluşturma
  - Sahte Erişim Noktaları Kullanmak
    - Ortadaki Adam Saldırıları
    - Servis Engelleme Saldırıları
  - İstemci Cihaz Sürücülerindeki Programlama Sorunları
    - İstemcide Komut Çalıştırma
    - Servis Engelleme Saldırıları



- Ağdaki Kablosuz Ağ Eriřim Noktaları Saptanması
  - Eriřim Noktalarının Keři
  - Yönetim Servisleri ve Destek Servislerinin Analizi
  - Ön Tanımlı Őifre ve Yönetim Sorunları
  
- Gömülü Yazılım Sorunları
  - Gömülü Servislerin Güncelleme Eksiklikleri
  - Web Temelli Yönetim Güvenlik Sorunları
  - SNMP Temelli Güvenlik Sorunları
  
- Ağ Yerleřimi
  - Doğrudan Yerel Ağa Bağlı Eriřim Noktaları

# Kablosuz Ağ Süreç Denetimi



- İstemci ve Erişim Tanımlama Politikaları
  - İstemci Tanımlama Onay Süreci
  - Erişilebilir Servisler ve Ağlar
  - Geçerlilik Süresi
  - Kimlik Doğrulama ve Erişim Denetim Yöntemi
    - 802.1x, WEP, WPA, WPA2, Mac Temelli Erişim Denetimi
- Kablosuz Ağ Cihazı Yönetim Politikaları
  - Yöneticiler ve Görevler
  - Yapılandırma Değişim Yönetimi
  - Yönetim Servisleri Tercihi
- Yönetim Servislerinin Güvenliği
  - Yönetim Servislerinin Konumlandırması ve Erişim Yönetimi
  - Yönetici Kimliği ve Doğrulama Yönetimi
  - Yönetici Hesaplarının Yetkilendirmesi
  - Yönetim Erişimlerinin Kayıt Edilmesi



- Denetim kuruma/sisteme/yazılıma özel olmalıdır, bu nedenle her bir testin özelleştirilmesi gerekmektedir
- Farklı denetim adımlarında alınan çıktıların birleştirilmesi ve beraber değerlendirilmesi gerekmektedir
- Bazı özel testlerin tanımlanabilmesi, kullanılacak test şekillerinin döngülere sokulabilmesi gerekmektedir
- Basit, hızlı ve amaca hizmet eden yazılımlar denetim sürecinin verimini arttırmaktadır
- Kaynak kodu açık, yapılan işlemin net olarak görünebileceği araçlar tercih edilmelidir
- Özgür yazılımlar genellikle bu şartları veya fazlasını sunmaktadır
- Ticari yazılımlar kısıtlı özelliklerde ve yetersiz performanslar ile çalışabilmektedir



- <http://www.aircrack-ng.org/>
- GPL Lisansı ile Geliştiriliyor
- Neredeyse Tüm Saldırıları, Aircrack ile Örnekleniyor
  - Kablosuz Ağların Saptanması
  - Kablosuz Ağ ile Sahte İlişkilendirme
  - WEP Kırma Saldırıları (Korek, PTW, Chop chop)
  - WPA Sözlük Saldırıları
  - WPA/TKIP Kırılması
  - Sahte Erişim Noktaları Oluşturmak
  - Servis Engelleme Saldırıları (Erişim Kesme, Sahte Erişim Nok.)
- Özel Cihaz Sürücüsü Desteği Gerektiriyor
  - Birçok Linux kablosuz ağ kartı sürücüsü sorunsuz
- Windows, Linux ve Birçok Platformda Çalışıyor

# Diğer Araçlar



## ➤ Kismet

- <http://www.kismetwireless.net/>
- Kablosuz Ağların Saptanması, İstemcilerin Görülmesi
- Paket Yakalama

## ➤ Metasploit Framework / Karmetasloit

- <http://www.metasploit.com/redmine/projects/framework/wiki/Karmetasloit>
- Kablosuz İstemcilerin Ele Geçirilmesi
  - Sahte Erişim Noktaları
  - Otomatik Ele Geçirme
  - Kablosuz Ağlar İçin Servis Engelleme Saldırıları
  - Kablosuz Ağ Kartı Sürücülerini için Exploit Örnekleri

## ➤ Wireshark

- <http://www.wireshark.org>
- Paket Yakalama, İletişim Çözümleme



## ➤ Backtrack Linux Dağıtımı

- Çok Sayıda Güvenlik Denetim Aracı İçermektedir
  - Nmap, Wireshark, Hping, Kismet, Aircrack-NG
- Yazılım Kurulumu Gerekmeden, CD'den Canlı Olarak Çalışır
- Sanal Makine Kullanımı ile Tercih Edilebilir
- Hazır Kablosuz Ağ Sürücüleri ile Sorunsuz Denetim

## ➤ KisMAC

- <http://kismac-ng.org/>
- Mac OS X için Hazırlanmıştır
- Paket Yakalama, Enjekte Etme ve Şifre Kırma Özellikleri Bulunuyor

## ➤ Ettercap

- <http://ettercap.sourceforge.net/>
- ARP Saldırıları, Ortadaki Adam Saldırıları



*Teşekkürler....*