KABLOSUZ AĞLARDA SALDIRI TESPİTİ

Yazar: Berkay İpek
Mentör: Burcu Yarar
Baskı: 2017

İÇİNDEKİLER

Kablosuz Ağlara Yapılan Saldırıların Tespiti Neden Gereklidir?

Teknolojinin ilerlemesi ile birlikte günlük hayatta kullandığımız tüm teknolojik araçların kablolarından kurtulduğumuzu görmekteyiz. Günlük hayatta internete girmek için en çok kablosuz ağları tercih ederiz ve bu işi günlük olarak kullandığımız dizüstü bilgisayarlarımızdan veya elimizden düşürmediğimiz cep telefonları sayesinde yaparız. Kablosuz cihazların kullanımının getirdiği yararlar kadar, birlikte getirdiği tehlikelerde göz ardı edilemeyecek düzeydedir. Bu tehlikelerin en başında ise kablosuz ağ güvenliği konusu gelmektedir. Saldırganlar kablosuz ağınız üzerinde açıklar aramakta ve bu açıklar doğrultusunda bazı yöntemler kullanarak, ağınıza saldırılar yapmaktadırlar.

Kablosuz Ağlara Gelen Saldırıları Aşağıdaki Gibi Sıralayabiliriz;

1) Erişim Kontrolü Saldırıları (Access Control Attacks)
2) Gizlilik Saldırıları (Confidentiality Attacks)
3) Bütünlük Doğrulama Saldırıları (Integrity Attacks)
4) Kimlik Doğrulama Saldırıları (Authentication Attacks)
5) Kullanılabilirlik Saldırıları (Availability Attacks)

1. Erişim Kontrolü Saldırıları (Access Control Attacks)

Bu saldırılar MAC filtrelemesi veya 802.11a, 802.11b, 802.11g, 802.11n gibi kablosuz ağ erişim protokollerine ve bunların sahip olduğu erişim kontrol önlemlerine karşı yayılmış olan frekansları dinleyerek, kontrol önlemlerini atlatıp ağa sızmaya çalışılan ataklardır.

	802.11a	802.11b	802.11g	802.11n
Frekans	5	2,4	2,4	2,4/5
Maksimum Hız	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Ortalama Kullanılabilen Hız (Kapasite)	27 Mbps	~5 Mbps	22 Mbps	130 Mbps
Kullanılan Kanal Sayısı/Örtüşmeyen Kanal Sayısı	12/8	11/3	11/3	22/11
Kapsadığı Mesafe	100 m	150 m	150 m	250 m

Resim 1 – Kablosuz Ağ 802.11 Standartları

1.1 Kablosuz Ağları Tarama (War Driving)

Wardriving, en çok bilinen ve başlangıç sayılabilen kablosuz ağ tespit etme yöntemidir. Araştırma isteklerini veya beacon (bağlantı kesme paketi) ile saldırganın dinlemeye geçmesi için gönderilen paketleri dinleyerek bir ağ keşfetmesidir.

1.2 Yetkisiz Erişim Noktası (Rogue Access Point)

Rogue Access Point, güvenli bir yerel ağa yetkisiz kurulmuş bir AP (Access Point)'dir. Bunu internete bağlanmak için kendine kablosuz bir bağlantı sağlamaya çalışan yetkisiz bir şirket çalışanı veya kötü amaçlı bir kişi yapabilir. Sonuç olarak şirket güvenlik politikalarınca kabul edilmeyen kablosuz bir yayın yapılmaktadır ve bu sayede ağa dışarıdan izinsiz giriş yapılabilir. Bu güvensiz durum ağdaki bilgilerin dışarıdan çalınmasına olanak sağlar. Rogue Access Pointler ciddi bir güvenlik açığı oluşturur.

1.3 Güvenli Olmayan Ağa Bağlanma (Adhoc Associations)

Sabit bir kablo alt yapısı olmadan, cihazların minimum konfigürasyonla kısa bir süre içerisinde oluşturabildikleri kablosuz ağa denir. Saldırı istasyonuna güvenliği engellemek için güvenli olmayan istasyona bağlanmaktır.

1.4 MAC Adres Sahteciliği (Mac Spoofing)

Saldırganın kullanılan ağ içerisini koklayarak (Sniff), ağı kullanan kişileri tespit eder ve sonrasında bu ağı kullanan kişilerden birinin MAC (Media Access Control) kimliğini kullanarak kendini ağı kullanan kişilerden biriymiş gibi gösterip yaptığı saldırı türüdür.

```
[root]# ifconfig eth0 hw ether 01:02:03:04:05:06
[root]# ifconfig eth0
eth0 Link encap:Ethernet HWaddr 01:02:03:04:05:06
inet addr:192.168.0.1 Bcast:192.168.0.255 Mask:255.255.255.0
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:4 dropped:0 overruns:0 carrier:4
collisions:0 txqueuelen:100
RX bytes:0 (0.0 b) TX bytes:168 (168.0 b)
Interrupt:11 Base address:0xdf00 Memory:df9ff000-df9ff038
```

Resim 2 – Linux işletim sistemine MAC Spoofing

1.5 IP Adresi Yanıltma (IP Spoofing)

İnternetin çalıştığı TCP/IP protokolü geliştirilirken güvenlik amacı temel olmadığından, protokol geliştirilirken bazı açıkları beraberinde getirmiştir. IP adresinin aldatılabilir yani değiştirilebilir olması sayesinde başka kişilerin IP adreslerinden istenilen internet aktivitesi yapılabiliyordu. Ancak günümüzde kullanmış olduğumuz işletim sistemlerinin protokoldeki açıkları kapatmasıdır.

1.6 802.1X Radius Cracking

Şeytan İkizi Erişim Noktası (Evil Twin Access Point)'nın kullanması için kaba kuvvet (Brute Force) atağı ile 802.1x erişim isteklerinden RADIUS gizliliklerini elde etme yöntemidir.

2. Gizlilik Saldırıları (Confidentiality Attacks)

Gizlilik saldırılarının asıl amacı kablosuz bağlantı yoluyla gönderilen özel bilgileri engellemek için yapılmaktadır.

2.1 Gizli Dinleme (Eavesdropping)

Bir ağ üzerinde iletim yapan cihazların verilerinin, saldırganlar tarafından araya girilerek alınmasıdır. Hatta bu saldırı tipinde kaynaktan elde edilen verinin değiştirilerek hedefe gönderilmesi de mümkündür.

2.2 Wep Anahtarı Kırma (Wep Key Cracking)

WEP anahtarının zayıf olmasından dolayı WPA ve WPA-2 gibi daha güvenli anahtarlar geliştirilmiştir. WEP anahtarının açığının olması, saldırganlara pasif ve aktif olmak üzere iki tür saldırı yapılmasına zemin hazırlar. Frekanslar dinlenerek bir yol bulunmaya çalışılır. Pasif Saldırılar IV'lardan elde edilen sonuçlara göre yapılan saldırılar olup, Aktif Saldırılar ise Replay(Tekrar) saldırıları ve mesajın içeriğini değiştirerek yapılan saldırılardır.

2.3 Şeytan İkizi Erişim Noktası (Evil Twin Access Point)

Saldırganlar, hedef olan sistemi şaşırtmak için kullanılan AP'yi klonlayarak kullanıcıların yeni AP'ye bağlanmasını sağlamaktadırlar. Bu işlem sayesinde klonlanmış AP'yi kullanan kişilerin tüm bilgilerini saldırganlar ele geçirebilmektedirler.

2.4 Erişim Noktası Üzerinde Sahte Portal Çalıştırmak (Access Point Phishing)

Saldırganlar, kullanıcının Evil Twin AP'ye ulaşmasından sonra bir web sunucusu kurabilir. Kullanıcıları internette kendi yaratmış oldukları web sitelerine yönlendirip, yaratmış oldukları zararlı kodların aracılığıyla kullanıcıların bilgilerini elde edebilirler.

2.5 Ortadaki Adam Saldırısı (Man in the Middle)

Bu saldırı türünde saldırganlar, hedef olan iki bilgisayar arasında kendilerini araya yerleştirirler ve bu sayede paylaşılanlardan bilgileri olur. Verilerin iki hedef arasında doğrudan iletilmesi yerine saldırgan üzerinden iletişime geçilir.

3. Bütünlük Doğrulama Saldırıları (Integrity Attacks)

Bu atak tipi, diğer atak tiplerini kolaylaştırmak veya alıcıyı yanıltmak için ataklar, sahte kontrol, yönetim ve kablosuz iletişim üzerinden veri paketleri gönderir.

3.1 Servis Reddi Saldırıları (Denial of Service - DoS Attacks)

Sistemde çalışan servislerin durdurulmasını veya çalışmasının yavaşlatılmasını sağlayan saldırı tipidir. Saldırının amacı, karşı tarafın bilgi erişimini veya servis kullanımını engellemeye çalışmaktır.

3.2 802.11 Paketi Püskürtme (Frame Injection)

Sahte 802.11 paketlerinin hedefin erişim noktalarına yada saldırgana göndererek, bir süre sonra hedef kaynağın servis dışı kalmasına veya gerekli bilgileri saldırgana sızdırmasını sağlar.

Aşamaları;

1- İlk önce erişim noktası araştırılır.
2- Hedefin açıkları aranır.
3- De-Authentication ve De-Association Saldıları için paketler enjekte edilir.

3.3 802.11 Veri Tekrarlama (802.11 Data Replay)

Bu saldırı tekrarı için hem paket toplamak, hemde bu paketleri yineleyerek enjekte amaçlıdır. Bu yöntemin içinde hem kayıt etmek hemde paket enjtekte tekrarları vardır.

3.4 802.1x EAP Tekrarlama (802.1x EAP Replay)

802.1x genişletebilir kimlik doğrulama protokollerinden paket yakalamak amaçlıdır. Bu sayede sisteme paketlerle tekrar saldırısı yapılabilir.

3.5 802.1x Radius Tekrarlama (802.1x Radius Replay)

Radius erişimi kabul veya ret mesajlarını tespit etmektedir. Erişim noktası ile kimlik doğrulama ana makinesi arasında tekrar saldırıları yapıldıktan sonra gelen adımdır.

4. Kimlik Doğrulama Saldırıları (Authentication Attacks)

Saldırganların amacı bu atakta kullanıcıların kimlik veya kimlik bilgilerini çalarak kullanmış oldukları ağa veya bir servise bağlanmak için kullanırlar.

4.1 Paylaşılmış Anahtarı Tahmin Etme (Shared Key Guessing)

WEP anahtarının kırılmış olması ile veya varsayılan 802.11 paylaşımlı anahtar kimlik doğrulayıcısını tahmin etme girişiminde bulunmaktır.

4.2 PSK Cracking

Sözlük (WordList) saldırı araçları kullanarak kaydedilmiş anahtar tokalaşma (handshake) paketlernden WPA/WPA2 PSK'yı elde etmektir.

4.3 Uygulama Girişi Hırsızlığı (Application Login Theft)

Kullanılan uygulamaya giriş yapılırken, açık metin protokollerinden kullanıcının girmiş olduğu bilgileri yakalamaktır. Örnek olarak; elektronik posta adresi, adres ve şifre gibi bilgileri.

4.4 Giriş Bilgilerinin Çalınması (Domain Login Cracking)

Sözlük (Wordlist) veya kaba kuvvet (Brute Force) saldırılarını kullanan karma NETBIOS şifre kırma yöntemi ile kullanıcının Windows Giriş Bilgisi ve Şifresini elde etmektir.

4.5 VPN Giriş Bilgilerinin Çalınması (VPN Login Cracking)

VPN'in doğrulama protokolleri üzerinde kaba kuvvet (Brute Force) saldırıları kullanarak, kullanıcının kimlik bilgilerini elde etme saldırılarıdır. Örnek olarak PPTP şifresi veya Ipsec Preshared Secret Key gibi bilgileri elde etmek gibi

4.6 802.1x Kimlik Hırsızlığı (802.1x Identity Theft)

Açık metin 802.1x kimlik yanıtlama paketleri ile kullanıcının kimlik bilgilerini almaktır.

4.7 802.1x Parola Tahmini (802.1x Password Guessing)

Yakalanan kullanıcı kimliğini kullanarak, kullanıcının şifresini tahmin etmek için tekrar ederek 802.1x kimlik doğrulamasının denenmesidir.

4.8 802.1x LEAP Kırılması (802.1x LEAP Cracking)

NT şifre karmalarını kırmak için sözlük saldırı araçları kullanarak yakalanmış EAP(LEAP) zayıf 802.1x paketlerinden kullanıcının kimlik bilgilerini elde etmektir.

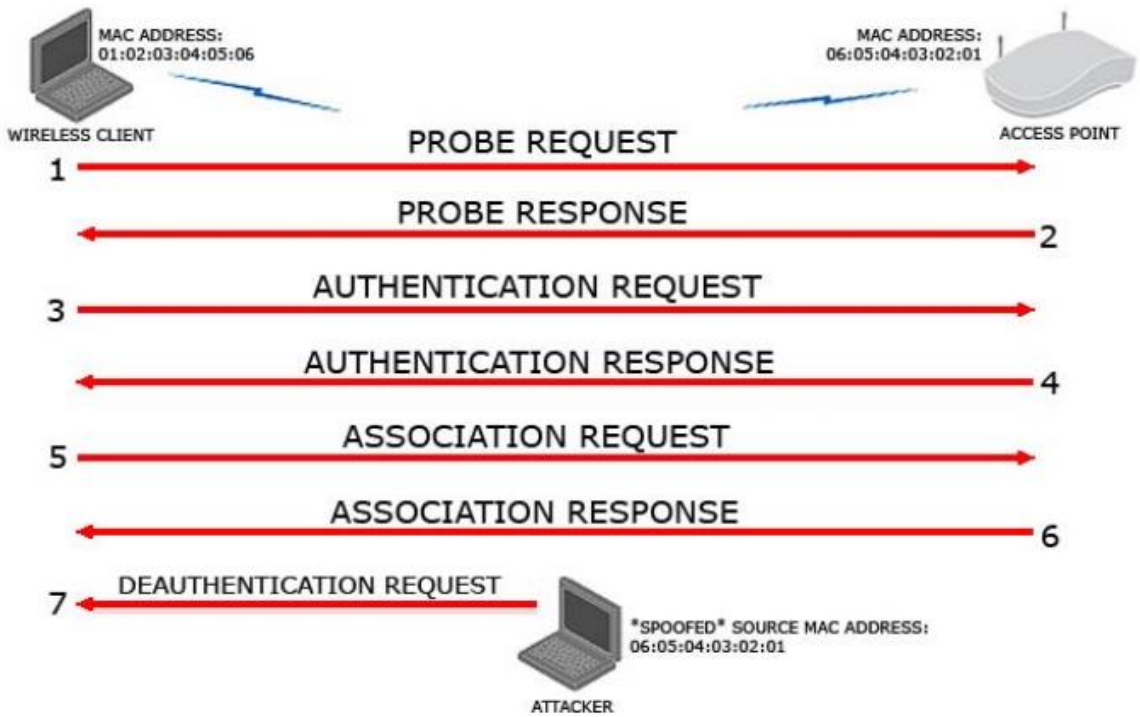
4.9 802.1x EAP Düşürülmesi (802.1x EAP Downgrade)

802.1x sunucusunu, sahte EAP-Response / Nak paketlerini kullanarak daha zayıf bir kimlik doğrulama tipine istekte bulunmaya zorlar.

4.10 DoS Atakları (Denial of Service Attacks)

De-authentication Saldırısı

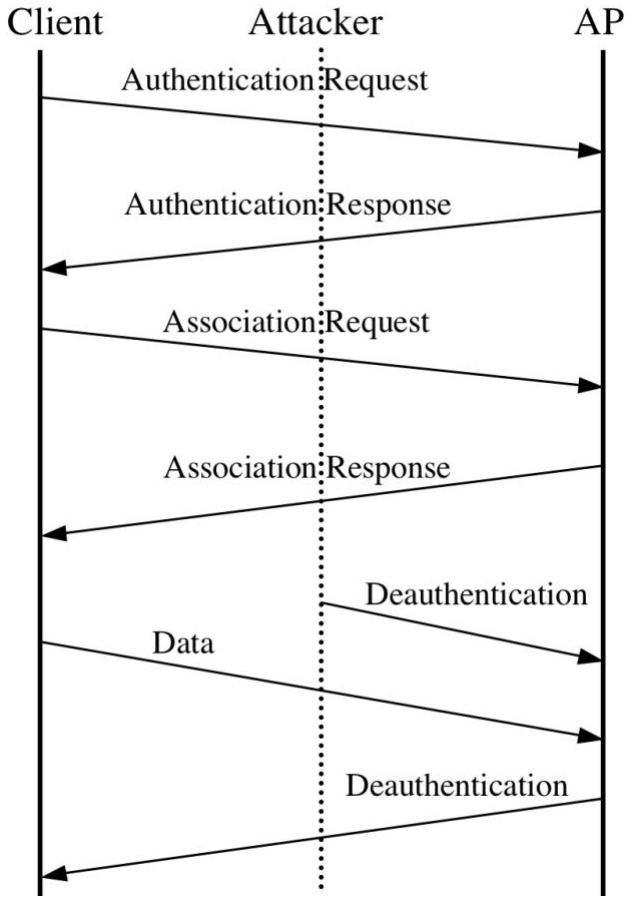
AP (Access Point) tarafından de-authentication paketi alan bir kullanıcı, AP ile arasındaki bağlantıyı koparır ve tekrar bağlanmayı dener. Bu saldırı türünde saldırgan, AP adına tüm veya belirli kullanıcılara taklit edilmiş de-authentication paketi göndererek ve bu işlemi sürekli yaparak kullanıcıyı ağdan düşürür ve bağlanmasını engeller. Bu saldırının amacı sahte de-authentication paketleri üreterek ortamdaki tüm kullanıcıları düşürmek ve kablosuz ağları işlevsiz hale getirmektir.



Resim 3 – De-authentication Saldırısının İşlem Sırası

Authentication / Association-Flood Saldırısı:

Bu saldırıda saldırgan çok sayıda ve farklı MAC adresleri üzerinden hedef AP'e authentication paketleri gönderir. AP, paket alışverişini tamamlamak için aldığı paketleri bir süre saklamak durumundadır. Kullanıcı AP'(Access Point)e bağlanmak istediği zaman birkaç doğrulama aşamasını yapmak zorundadır.



Resim 4 – Authentication / Association Saldırısı

5) Kullanılabilirlik Saldırıları (Availability Attacks)

Kullanılabilirlik Saldırılarının asıl amacı kullanıcıların kullanmış oldukları kablosuz ağ servislerinin verimini azaltmak veya servisin kullanılmasını engellemektir.

5.1 Erişim Noktası Hırsızlığı (Access Point Theft)

Fiziksel olarak, Erişim Noktasının kullanım alanından kaldırılmasıdır.

5.2 Radyo Frekansı Paraziti (RF Jamming)

Hedef olan WLAN ile aynı frekansta yayın yapan ya da eşdeğer izotopik yayılan gücü (EIRP) düzenlemesine aşan bir güce sahiptir.

5.3 Queensland DoS

CSMA (Carrier Sense Multiple Access)/CA ve Clear Channel Assessment (CCA)'dan yararlanılarak, kullanılan kanalın sürekli meşgul hale getirilmesidir.

5.4 802.11 Beacon Flood

Binlerce sahte 802.11 Beacon (Hat Kesme İletisi) üreterek, istasyonun doğru erişim noktasını bulmasını engellemektedir

5.5) 802.11 Associate / Authenticate Flood

Erişim noktasının dahil olma tablosunu doldurmak için farklı MAC adreslerinden sahte kimlik doğrulama veya katılma mesajları gönderir.

5.6 802.11 TKIP MIC Exploit

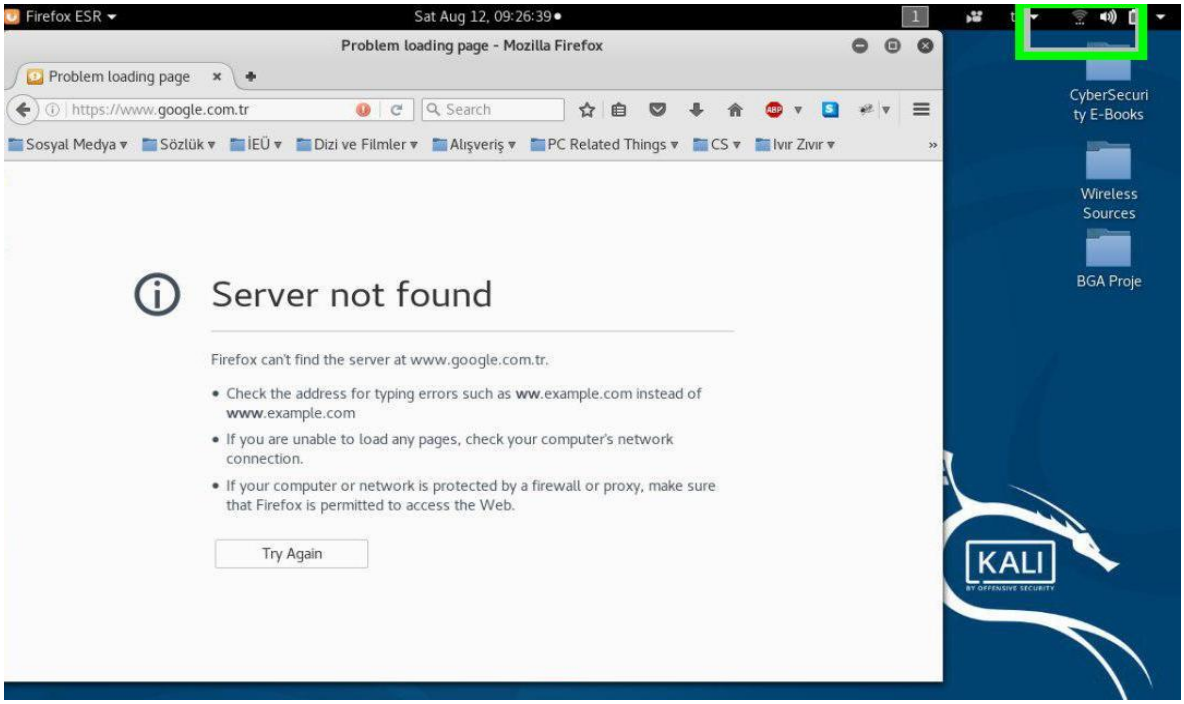
Geçersiz TKIP verileri üreterek, hedef erişim noktasının MIC eşiğini aşarak WLAN servislerinin kullanımını durdurmaktadır.

5.7 802.11 Sahte Kimlik Seli (802.11 Deauthenticate Flood)

Sahte kimlik bilgileri göndererek veya dahil olmama bilgileri göndererek, kullanıcıların AP'den bağlantılarının kesilmelerini sağlamaktadır.

```
root@Kali: ~
File  Edit  View  Search  Terminal  Help
######################### Welcome to Berkay İpek ############################
root@Kali:~# aireplay-ng --deauth 0 -a 90:B6:86:45:AB:60 -c 74:E5:43:C9:D9:46 wl
an1mon
09:25:02  Waiting for beacon frame (BSSID: 90:B6:86:45:AB:60) on channel 6
09:25:02  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [54|62 ACKs]
09:25:03  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [42|60 ACKs]
09:25:03  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [14|71 ACKs]
09:25:04  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [43|64 ACKs]
09:25:05  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [12|62 ACKs]
09:25:05  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [47|69 ACKs]
09:25:06  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [39|62 ACKs]
09:25:06  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [30|69 ACKs]
09:25:07  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [43|58 ACKs]
09:25:07  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 1|55 ACKs]
09:25:08  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [43|73 ACKs]
09:25:08  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [22|60 ACKs]
09:25:09  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [64|67 ACKs]
09:25:09  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|60 ACKs]
09:25:10  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|65 ACKs]
09:25:11  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|63 ACKs]
09:25:11  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|64 ACKs]
09:25:11  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 2|23 ACKs]
```

Resim 5 – Deauthenticate Flood



Resim 6 – Deauthenticate Atağı Sonucu Bağlantısı Koparılmış Kullanıcı

5.8 802.1x EAP-Start Flood

Amacı tekrar tekrar gönderilen EAP-Start mesajları ile hedef AP'in kaynaklarını tüketmek veya kullanım dışı bırakmaktır.

5.9 802.1x EAP-Failure

Aktif durumda ki bir 802.1x EAP değişimini izledikten sonra istasyona sahte EAP-Failure iletileri göndermektir.

5.10 802.1x EAP-of-Death

Kötü biçimlendirilmiş 802.1x EAP Kimlik yanıtı göndererek AP'i kullanım dışı bırakmaya çalışmaktır.

5.11) 802.1x EAP Length Attacks

Kötü uzunluk alanları ile yaratılmış tipik EAP mesajları göndererek AP veya Radius sunucusunu çökertmeye çalışmaktır.

Kablosuz Ağlara Gelen Saldırın Tespiti

Tespit Yöntemleri

Kablosuz ağlara gelen atakların geniş yelpazeye sahip olduğu bilinir. Bunun için Saldırı Tespit Sistemi (IDS "Intrusion Detection System") çift imza ve bilgi tabanlı olması gerekiyor.

İmza tabanlı tespitlerde bozuk ağ trafiğini algılamak için statik imza kullanılır. Bu tip eşleşmeler önceden tanımlanmış atak modelleri için sorunsuz çalışmaktadır. Örnek olarak, Sahte Access Point'i tespit etmek için, IDS yetkili yani bildirile Access Point listesini kullanır. Bu listeye göre eşleşmeyen bir Access Point varlığında uyarı verir.

Bilgi tabanlı algılamada, ağ trafiği için tarihsel bir altyapı kullanır. Ağ trafiği bu kullanılan altyapının dışına çıktığı zaman uyarı verir. Birçok kablosuz atak, imza ile eşleşmeyebilir. Acak IDS bu anormallikleri tespit edebilir. Örneğin, saldırgan WEP parolasını kırmak için paketler üretmek yerine kablosuz ağ üzerine tekrarlayabilir (Replay Attack). Saldırganın yapmış olduğu bu saldırı ağ trafiğinin artmasına neden olur.

Kablosuz Saldırı Tespit Sistemi ve Yanlış Pozitif

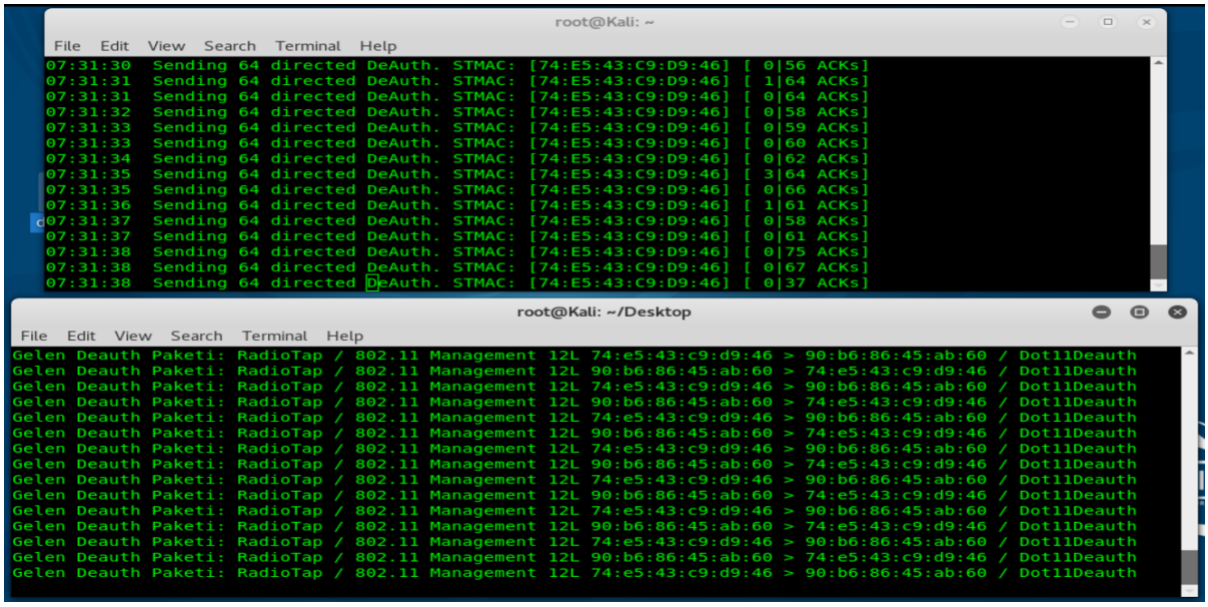
Kablosuz Ağ Tespit Sistemleri (WIDS “Wireless Intrusion Detection System”), Kablolu Saldırı Tespit Sistemlerine göre gerekli düzenlemeler yapılmadan daha doğru bilgiler vermezler. Özellikle Bilgi Tabanlı Tespit Motorları (Knowledge-Based Detection Engine) yanlış pozitif olmaya eğilimlidirler. Saldırgan tarafından tarihsel temel (Historical Baseline) değiştirilmiş ise verdikleri sonuç daha yanlış pozitif veya yanlış negatif verecektir. Bu yüzden tarihsel temel periyodik şekilde güncel ağ modelleri ile yenilenmeli ve güncel tutulmalıdır.

De-authentication Atağı Tespiti

Hedeflenen bir kullanıcıyı AP’den düşürmek ve yeniden bağlanmasını sağlamak için binlerce defa deneme olduğundan De-authentication işlemi çok fazla işlem yapar ve bu ağda gürültülere neden olur. De-authentication atağı ile birlikte kullanıcı ağa olan erişimini kaybedecektir.

De-authentication atağı kolayca tespit edilebilir çünkü ağa gelen ayrışma paketleri (Dissociation Packets) kablosuz ağ için normal değildir. Kablosuz Ağ Saldırı Tespit Sistemi (Wireless Intrusion Detection System) uyarı verecektir aşağıda ki gibi durumlarda;

1. De-authentication Flood’ı yapılması için Broadcast adresine gönderilir
2. Tekrarlanan Authentication denemeleri bir veya daha fazla host tarafından gerçekleştirilir.



```
07:31:30  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|56 ACKs]
07:31:31  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 1|64 ACKs]
07:31:31  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|64 ACKs]
07:31:32  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|58 ACKs]
07:31:33  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|59 ACKs]
07:31:33  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|60 ACKs]
07:31:34  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|62 ACKs]
07:31:35  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 3|64 ACKs]
07:31:35  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|66 ACKs]
07:31:36  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 1|61 ACKs]
07:31:37  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|58 ACKs]
07:31:37  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|61 ACKs]
07:31:38  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|75 ACKs]
07:31:38  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|67 ACKs]
07:31:38  Sending 64 directed DeAuth. STMAC: [74:E5:43:C9:D9:46] [ 0|37 ACKs]
```

```
Gelen Deauth Paketi: RadioTap / 802.11 Management 12L 74:e5:43:c9:d9:46 > 90:b6:86:45:ab:60 / Dot11Deauth
Gelen Deauth Paketi: RadioTap / 802.11 Management 12L 90:b6:86:45:ab:60 > 74:e5:43:c9:d9:46 / Dot11Deauth
Gelen Deauth Paketi: RadioTap / 802.11 Management 12L 74:e5:43:c9:d9:46 > 90:b6:86:45:ab:60 / Dot11Deauth
Gelen Deauth Paketi: RadioTap / 802.11 Management 12L 90:b6:86:45:ab:60 > 74:e5:43:c9:d9:46 / Dot11Deauth
Gelen Deauth Paketi: RadioTap / 802.11 Management 12L 74:e5:43:c9:d9:46 > 90:b6:86:45:ab:60 / Dot11Deauth
Gelen Deauth Paketi: RadioTap / 802.11 Management 12L 90:b6:86:45:ab:60 > 74:e5:43:c9:d9:46 / Dot11Deauth
Gelen Deauth Paketi: RadioTap / 802.11 Management 12L 74:e5:43:c9:d9:46 > 90:b6:86:45:ab:60 / Dot11Deauth
Gelen Deauth Paketi: RadioTap / 802.11 Management 12L 90:b6:86:45:ab:60 > 74:e5:43:c9:d9:46 / Dot11Deauth
Gelen Deauth Paketi: RadioTap / 802.11 Management 12L 74:e5:43:c9:d9:46 > 90:b6:86:45:ab:60 / Dot11Deauth
Gelen Deauth Paketi: RadioTap / 802.11 Management 12L 90:b6:86:45:ab:60 > 74:e5:43:c9:d9:46 / Dot11Deauth
Gelen Deauth Paketi: RadioTap / 802.11 Management 12L 74:e5:43:c9:d9:46 > 90:b6:86:45:ab:60 / Dot11Deauth
Gelen Deauth Paketi: RadioTap / 802.11 Management 12L 90:b6:86:45:ab:60 > 74:e5:43:c9:d9:46 / Dot11Deauth
Gelen Deauth Paketi: RadioTap / 802.11 Management 12L 74:e5:43:c9:d9:46 > 90:b6:86:45:ab:60 / Dot11Deauth
Gelen Deauth Paketi: RadioTap / 802.11 Management 12L 90:b6:86:45:ab:60 > 74:e5:43:c9:d9:46 / Dot11Deauth
Gelen Deauth Paketi: RadioTap / 802.11 Management 12L 74:e5:43:c9:d9:46 > 90:b6:86:45:ab:60 / Dot11Deauth
```

Resim 7 – De-authentication Paketlerinin Canlı Olarak İzlenmesi

File Edit View Search Tools Documents Help

Open Save

```
from scapy.all import *

def PacketHandler(pkt):
    if pkt.haslayer(Dot11) and pkt.type == 0 and pkt.subtype == 0xC:
        print "Deauth paket: %s" % (pkt.summary())

sniff(iface="wlxc4e9841c6b38", prn = PacketHandler)
```

Python Tab Width: 8 Ln 7, Col 52 INS

Resim 8 – De-authentication Paketlerinin İzlenmesini Sağlayan Kod Satırları

File Edit View Search Tools Documents Help

Open Save

```
from scapy.all import *

def PacketHandler(pkt):
    if pkt.haslayer(Dot11) and pkt.type == 0 and pkt.subtype == 0xC:
        print "Deauth paket: %s" % (pkt.summary())

sniff(iface="wlxc4e9841c6b38", prn = PacketHandler)
```

Python Tab Width: 8 Ln 7, Col 52 INS

Injection Atağı Tespiti

Network ağındaki fazla sayıda ki kopyalanmış paketlerin gözükmesi ile Injection atağı görüldüğü varsayılabilir. Gelen kopya paketler ile cevap verme eşik değerinin açılması AP'in yavaşlamasına sebep olabilir.

1. IV kopyalarının artması
2. Fazla sayıda kopyalanmış paketlerin alınması
3. Kısa süren De-authentication saldırıları

Injection Atağı Hız Çarpışması

Gelen kopya paketler ile cevap verme eşik değerinin açılması AP'in yavaşlamasına sebep olabilir.

Kablosuz saldırı tespit sistemi WEP şifresi kırılmasını tespit edebilir ama kaynak bağlanılmış sunucu olarak alınabilir ve kablo ile bağlantı olmadığından suçlu geri takip edilemez. Kablosuz ağı büyük bir kök olarak düşünürsek, MAC adresi çakışması olmayacaktır.

Ortadaki Adam Saldırısı Tespiti (Man-in-the-Middle Detection)

Ortadaki Adam Saldırısının başarılı olabilmesi için, MIM (Man-in-the-Middle) ın hedef olan AP ile arasında en az 5 kanal uzak olması gerekiyor. Bunun nedeni DoS (Denial of Service) saldırısı uygulandığı andaki oluşacak olan parazitten zarar görmemektir. Bu yüzden belirli olmayan bir kanaldaki ESSID'yi takip etmek uyarı verebilir. Bu atak tespiti kablosuz ağdaki tek AP için yararlı olabilir ancak büyük kablosuz ağlar için verimli olmayacaktır.

Büyük kablosuz ağlardaki çoklu AP'ler, komşu ağlarlaa çakışma olmasın diye farklı kanallara kurulum yapılır.

Ortadaki Adam Saldırısının Statik Liste ile Tespiti

Saldırı Tespit Sistemi(IDS) AP'leri tespit ederek tanımlanmış liste ile ESSID, BSSID ve kanal kombinasyonlarını karşılaştırma yapabilir. Kullanılan listede BSSIDler ve kullandıkları kanalların eşlenmiş olması tespit açısından önemlidir.

Şuan kullanılan Sahte Access Point ön işlemcileri kablosuz ağı tespit için ayrı BSSID ve ayrı kanal listesi kullanmaktadır. BSSID, tanımlanmamış bir kanal kullanıldığında, Saldırı Tespit Sistemi(IDS) bunu tanımlayamaz. Ortadaki adam saldırıları genellikle AP'in 5 kanal uzağındaki BSSID'yi kullandığından bu çok önemlidir.

BBISD! = Tanımlanmış BSSID => UYARI Tanımlanmamış BSSID
BSSID&! Tanımlanmış Kanal => UYARI BSSID, Tanımlanmamış Kanal

Bu tespit tipi dikkatli ve AP'in kopyasını alırken aynı BSSID ve kanal kombinasyonunu atlamadan alan saldırgan tarafından kolayca atlatılabilir.

Bilgi Tabanlı Ortadaki Adam SaldırıTespiti

Eğer saldırgan Sahte AP'i geçerli olan AP'in BSSID ve Kanal'ı ile ayarlarsa Statik Liste Tespit Sistemi başarısız olacaktır. Ancak OA (Ortadaki Adam) atağı, izlenilen AP'in sinyal gücüne göre tespit edilebilir. Saldırgan klonlanan sahte AP'i hedef olarak görülen AP'in yanına yerleştiremez, çünkü asıl AP'in yayacağı radyo frekansı atağın bozulmasına neden olacaktır. BSSID ve kanal iki yer kullanır yani IDS tarafından algılanan sinyal gücü değişecektir.

IDS Sensörünün artması, yapılan tespitin güvenirliğini arttıracaktır. Sinyal gücünü izlemek için daha fazla sensör yaratmak gerekiyor.

Not olarak, IDS düşük sinyal gücündeki Ortadaki Adam saldırılarını denetleyemez.

IDS Sensor	ESSID	BSSID	Channel	Signal Strength
0	Test	11:11:11:11:11:11	1	60
0	Test	22:22:22:22:22:22	6	70
1	Test	11:11:11:11:11:11	1	40
1	Test	22:22:22:22:22:22	6	50

Resim 9 – Veritabanındaki BSSID ve Kanal Kombinasyonu

Kaynaklar;

http://searchnetworking.techtarget.com/feature/Wireless-attacks-A-to-Z
http://searchnetworking.techtarget.com/feature/Wireless-attacks-A-to-Z
https://tr.linkedin.com/pulse/kablosuz-ağlara-yapılan-saldırı-türleri-özden-erçin-msc-
https://eincop.blogspot.com.tr/search/label/Linux%20%26%20Security

Wireless Network Attacks - CompTIA Network+ N10-006 - 3.2
Understanding Wireless Attacks & Detection -
GIAC Security Essentials Certification (GSEC)
Practical Assignment
Option 1 - Research on Topics in Information Security
Submitted by: Christopher Low 13 April 2005
Wireless Attacks from Intrusion Detection Perspective
GCIA Gold Certification
Author: Gary Deckerd, gdeckerd@secureworks.com
Adviser: Dominicus Adriyanto Hindarto
Accepted: November 23rd 2006

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.