Kablosuz Ağlar Ve Güvenlik

Son yıllarda özellikle ADSL hizmetinin genişlemesi ile birlikte kablosuz ağ destekli modemlerin kullanımı da artmıştır. Bu tip modemlerdeki kablosuz ağ özelliğinin sağladığı esneklikler ve kolay kullanımı sayesinde artık her evde bir kablosuz ağ oluşmaya başladığını görüyoruz. Özellikle fiyat/kullanım özelliği oranındaki başarım kablosuz ağların yaygınlaşmasında önemli rol oynamıştır.

Teknolojiye kafa diretmek olmaz avantajlarından "zarar görmeden" maksimum seviyede yararlanmak lazım diyorsanız kullandığınız sistemi tanımanız şarttır. Bu ayki yazıda kablosuz ağların çalışma mantıkları, güvenlik açıkları ve korunma yolları üzerinde durdum. Eminim yazı sonunda daha dikkatli bir kablosuz ağ kullanıcısı olacaksınız.

Kablosuz ağlarda günümüzde kullandığımız kablolu ağlardan farklı bazı önemli noktalar vardır. Bu noktaların daha iyi anlaşılabilmesi için sadece kablosuz ağlara özel batı tanımların, terimlerin bilinmesinin faydalı olacağını düşünüyorum.

Kablosuz Ağ Terimleri

Frame: Iki kablosuz ağ cihazı arasında gidip gelen veri.

WEP : Kablosuz ağlarda sık kullanılan şifreleme protokolü.

WPA : WEP'de çıkan güvenlik açıklarının giderilmesi ve yeni özelliklerin eklenmesi ile çıkarılmış güvenlik protokolü.

Access Point: Kablosuz ağ cihazlarının bağlanarak bir ağ oluşturduğu merkezi cihaz. Bu cihaz bir donanım olabileceği gibi özelleştirilmiş bir Linux dağıtımı da olabilir.

SSID : Access Point(Erişim Noktası)'nın tanımlayıcı adı.

802.11x : IEEE tarafından tanımlanmış ve kablosuz ağ cihazlarının nasıl çalışacağının belirtildiği standartlar dizisi.

Yaygın Kablosuz Ağ Yöntemleri

Etrafımıza baktığımızda yoğun bir kablosuz ağ kullanımı görüyoruz. Fakat bu ağlar hangi mantıkta çalışıyor, getirilerinin yanında götürüleri nelerdir, hiç düşündünüz mü? Kullanımı bu kadar basitleştirilen kablosuz ağların ardında oldukça kompleks bir yapının yattığını söylersek abartmış olmayız.

Kablosuz ağlar temelde iki modda çalışır: bunlardan biri Ad-hoc diğeri de Infrastructure mod olarak adlandırılmıştır. Genellikle, kablosuz ağı kullanım amacımıza göre bu iki mod'dan birini seçme durumunda kalırız.

Ad-hoc Mode: Bilgisayardan bilgisayara bağlantı Yöntemi:

Ad-hoc mod, iki kablosuz ağ cihazının arada başka bir birleştiriciye(AP) ihtiyaç duymadan haberleşebildiği durumdur. Teknik olarak Independed Basic service set olarak da bilinir(IBSS). Ad-hoc bağlantıları genellikle evde kişisel işlerimiz için kullanırız. Mesela, bir evde iki bilgisayar ve birinin internet bağlantısı var, diğer bilgisayarıda internete çıkarmak istersek önümüze iki seçenek çıkıyor: ya iki bilgisayar arasında bir kablo çekerek iki bilgisayarı direk birbirine bağlayacağız ya da bir hub/switch alarak iki bilgisayarı bu aracı cihazlar ile konuşturacağız.

Oysa bunlardan başka bir seçeneğimiz daha var -tabi eğer her iki bilgisayarda kablosuz ağ adaptörü varsa-. Bu iki cihazın kablosuz ağ adaptörlerini Ad-hoc modda çalışacak şekilde ayarlarsak ve internete çıkan bilgisayarda bağlantı paylaşımı yaparsak iki makinede özgür bir şekilde interneti kullanabilecektir. Burada makinelerin Linux, Windows ya da Mac. olması farketmez. Tanımlanan değerler standartlara uygun olduğu müddetçe her işlemi kolaylıkla yapabiliriz.

Piyasada 20-30 $ dolara bulabileceğiniz USB kablosuz ağ adaptörleri ile kolaylıkla Ad-hoc mod kablosuz ağ kurabilirsiniz.

Kısaca Ad-hoc mod için herhangi bir AP'e gerek duymadan kablosuz ağ cihazlarının birbirleri arasında haberleşmesidir diyebiliriz.

Infrastructure mode

Infrastructure mode ortamdaki kablosuz ağ cihazlarının haberleşmesi için arada AP gibi bir cihaza ihtiyaç duyulmasıdır. Ad-hoc moda göre biraz daha karmaşıktır ve özel olarak ayarlamadıysak işletim sistemimiz bu modu kullanacak şekilde yapılandırılmıştır. Teknik olarak "Basic Service Set" olarak da bilinir(BSS). Infrastructure modda kablosuz ağ istemcileri birbirleri ile direkt konuştuklarını düşünürler fakat tüm paketler AP aracılığı ile iletilir. Burada ağa dahil olmayan herhangi bir kablosuz

ağ cihazının tüm trafiği izleme riski vardır. Bu sebeple Infrastructure mod kullanırken genellikle iletişim şifrelenir. Şifreleme amaçlı olarak WEP ya da WPA gibi protokoller kullanılır. Şifreli iletişimde aradaki trafik izlense bile anlaşılmaz olacaktır.

Kablosuz Ağ Standartları

Çeşitli firmalar tarafından üretilmiş kablosuz ağ cihazlarının birbirleri ile sorunsuz haberleşebilmesi için uyması gerektikleri bazı standartlar vardır. Bu standartları IEEE belirler, kablosuz ağlar için 802.11 ailesi belirlenmiştir.. Günümüzde yoğun kullanılan bazı 802.11x standartları ve özelikleri;

- 802.11b
  - 2.4 GHz aralığında çalışır
  - Max bant genişliği 11Mbps
  - 30-75m arası performans
  - Günümüzde yaygın kullanılıyor

- 802.11a
  - 5GHz aralığında yayın yapar
  - Max bant geişliği 54Mbps
  - 25-50m civarında performans

- 802.11g
  - 802.11b uyumlu
  - 2.4 GHz aralığında
  - 54 Mbps'e kadar çıkan hız kapasitesi

- 802.11i
  - Güvenli WLAN kullanımı için düşünülmüş
  - 802.11a ve 802.11b WLAN'lari arasındaki iletişimin şifrelenmesini belirler
  - AES TKIP(temporary key integrity protocol) gibi yeni şifreleme metodları kullanır.

Kablosuz Ağlarda Linux Kullanımı..

Linux sistemler kablosuz ağ yapılandırması için zengin seçeneklere sahiptir. Her Linux dağıtımının kendi grafik arabirimli yapılandırması olduğu gibi tüm Linux dağıtımları için geçerli komutları kullanmak da her zaman hazır seçenek olarak durmaktadır.

Bir kablosuz ağ cihazının neler yapabileceğini düşünelim; öncelikle bulunduğu çevredeki çalışır vaziyette bulunan erisim noktalarını görmek isteyecektir, bulduğu erişim noktalarından birini seçerek bağlanmak ve gerekli IP yapılandırmasını girmesi gerekecektir, ya da erişim noktası tarafındfan verilen hazır bilgileri kullanacaktır. Eğer erişim noktasında güvenlik amaçlı şifreleme kullanılmışsa kullanılan protokole(WEP/WPA) uygun anahtarın da doğru şekilde girilmesi gerekir.

Kapsama alanında bulunan Erişim Noktalarını(Access Point) keşfetmek için "iwlist" komutu uygun parametreler ile kullanılır.

Linux makinemizdeki wireless Ethernet arabiriminin eth1 olduğunu varsayarsak çevremizdeki AP'leri aşağıdaki komut ile görebiliriz.

```
root@byte: ~# iwlist eth1 scan
    eth1      Scan completed :
              Cell 01 - Address: 00:05:60:D5:CE:76
                        ESSID:"Byte Test"
                        Mode:Master
                        Frequency:2.417GHz
                        Quality:0/10  Signal level:-70 dBm  Noise level:-256 dBm
                        Encryption key:off
                        Bit Rate:1Mb/s
                        Bit Rate:2Mb/s
                        Bit Rate:5.5Mb/s
                        Bit Rate:11Mb/s
              Cell 02 - Address: 00:04:2B:52:15:58
                        ESSID:"Sebil Net"
                        Mode:Master
                        Frequency:2.467GHz
                        Quality:0/10  Signal level:-22 dBm  Noise level:-256 dBm
                        Encryption key:on
                        Bit Rate:1Mb/s
                        Bit Rate:2Mb/s
                        Bit Rate:5.5Mb/s
                        Bit Rate:11Mb/s
```

Peki hangi arabirimimizin kablosuz ağ adaptörü olduğunu nasıl anlarız? Bunun için de iwconfig komutu parametresiz kullanılırsa Linux bilgisayarımızda bulunan ağ adaptörleri inceleyerek hangilerinin kablosuz ağ adaptörü olduğunu bize söyleyecektir.

Bulunan erişim noktalarından herhangi birine bağlanmak için iwconfig komutunu kullanıyoruz.

root@byte: ~# iwconfig eth1 essid "Byte Test"

root@byte: ~# ifconfig eth1 up

root@byte: ~# ifconfig eth1 192.168.1.2 netmask 255.255.255.0

ya da otomatik ip aldırmak için

root@byte: ~# dhclient eth1

komutlarını kullanabiliriz.

Yapılandırılmış arabirime ait özellikleri görmek istersek;

root@byte: ~# iwconfig eth1

```
eth1    IEEE 802.11-DS  ESSID:"Byte Test"
          Mode:Managed  Frequency:2.457GHz  Access Point: 00:05:60:D5:CE:76
          Bit Rate:2Mb/s   Tx-Power=15 dBm   Sensitivity:1/3
          RTS thr:off   Fragment thr:off
          Encryption key:on
          Power Management:off
          Link Quality:46/92 Signal level:-51 dBm  Noise level:-94 dBm
          Rx invalid nwid:0  invalid crypt:0  invalid misc:0
```

komutunu vermemiz yeterlidir.

Bağlanmak istediğimiz erisim noktası WEP kullanacak şekilde ayarlandıysa bunu da parametre olarak belirtmeliyiz.

```
root@byte: ~# iwconfig eth1 key 1234576890123456789012345
```

İki Bilgisayarı arada "Erişim Noktası" olmadan konuşturmak

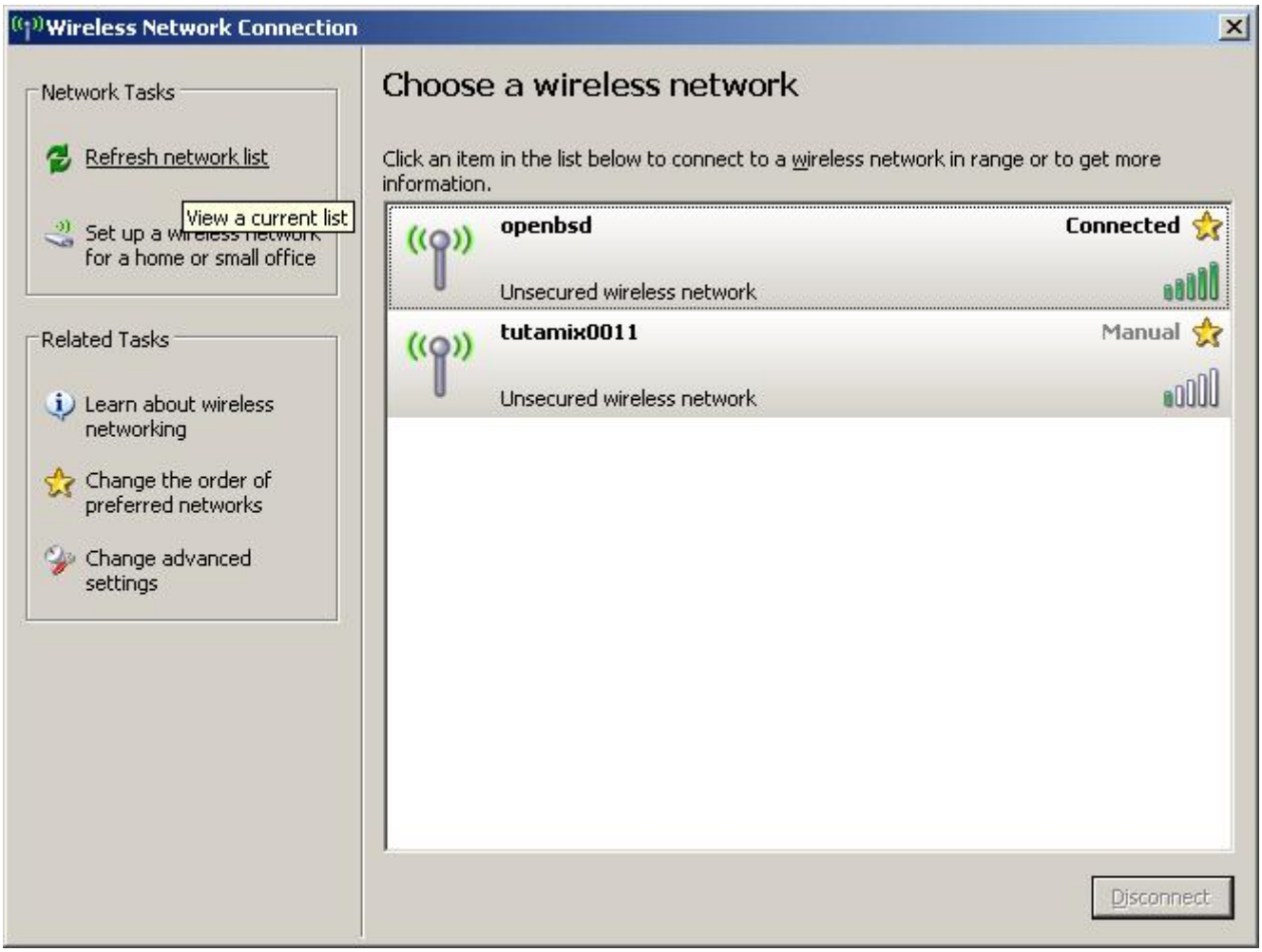
Ev ağımızda bulunan iki makineyi arada kablo olmadan haberleştirmek istersek Ad-hoc mod kullanırız demiştik. Şimdide bu işlemin Linux ve Windows işletim sistemleri kullanaılarak nasıl tasarlandığına bakalım .

Linux tarafında kablosuz ağ adaptörünü Ad-hoc moda almak için tek bir komut yeterlidir.

root@byte: ~# iwconfig eth1 essid "openbsd" mode Ad-hoc

root@byte: ~# ifconfig eth1 100.100.100.1

Linux tarafında gerekli yapılandırmaları yaptıktan sonra Windows işletim sisteminin kablosuz ağ yönetim aracını açarak etraftaki kablosuz ağları görüntülemesini isteyebiliriz ya da bu değerleri elle girebiliriz. Gireceğimiz değerlerin Linux'a girdiğimiz değerlerle aynı olmazsa Ad-hoc ağımız çalışmayacaktır.



Bir diğer önemli husus da her iki makinedeki ağ yapılandırmasının uygun olması, yani iki makinanın da aynı alt ağda (subnet) olmasıdır. Linux makinede kablosuz ağ arabrimine 100.100.100.1 IP adresini atamiştik ayni şekilde Windows makineyede bu ağdan bir IP(100.100.100.2 gibi) ataması yapalım ki iki makine birbirleri ile doğrudan haberleşebilsin.

Bir Linux makineyi Erişim noktası olarak kullanmak…

Linux makineleri sadece Ad-hoc mod için değil tam bir erişim noktası amaçlı da kullanabiliriz. Bunun için gerekli olan tek şey kullanacağımız kablosuz ağ arabiriminin "Host Ap" oladak adlandırılan modu desteklemesidir. Bu modu destekleyen herhangi bir kablosuz ağ arabirimini Linux makineye taktıktan sonra Ad-hoc mode gibi kolaylıkla kendimizi erisim noktası olarak tanıtır ve çevremizdeki kablosuz cihazlara hizmet verebiliriz. Burada bahsettiğimiz birebir gerçek AP özelliğidir.

Kablosuz Ağlarda Güvenlik Sorunu

Bu kadar teorik bilgiden sonra gelelim asıl konumuza: kablosuz ağlarda güvenlik sorunu. Bu kadar kolaylıklar sağlayan her teknolojide kaçınılmaz bazı tasarım eksiklikleri, güvenlik açıkları olacaktır.

Kablosuz ağlardaki en temel güvenlik problemi verilerin havada uçuşmasıdır. Normal kablolu ağlarda switch ya da hub kullanarak güvenliğimizi fiziksel sağlayabiliyorduk ve switche/hub'a fiziksel olarak bağlı olmayan makinelerden korunmuş oluyorduk. Oysaki kablosuz ağlarda tüm iletişim hava üzerinden kuruluyor ve veriler gelişigüzel ortalıkta dolaşıyor.

Erisim Noktasnı görünmez kılma: SSID Saklama

Kablosuz ağlarda erişim noktasının adını(SSID) saklamak alınabilecek ilk temel güvenlik önlemi olarak gözüküyor. Fakat bu tip ağların çalışma yöntemlerine bakacak olursak bu ismin(SSID) sadece belirli seviyedeki kullanıcılardan saklanabileceğini görmüş oluruz. Erişim noktaları ortamdaki kablosuz cihazların kendisini bulabilmesi için kendilerini devamlı anons ederler. Teknik olarak bu anonslara "beacon frame" denir. Güvenlik önlemi olarak bu anonsları yaptırmayabiliriz ve sadece erişim noktasının adını bilen cihazlar kablosuz ağa dahil olabilir. Böylece Windows, Linux da dahil olmak üzere birçok işletim sistemi etraftaki kablosuz ağ cihazlarını ararken bizim cihazımızı göremeyecektir.

Diğer bir sorun da erisim noktasının WEP ya da WPA prokollerini kullanması durumunda bile SSID'lerini şifrelemeden göndermesidir. Bu da ortamdaki kötü niyetli birinin özel araçlar kullanarak bizim erişim noktamızın adını her durumda öğrenebilmesini sağlayacaktır.

Erişim Kontrolü

Standart kablosuz ağ güvenlik protokollerinde ağa giriş anahtarını bilen herkes kablosuz ağa dahil olabilir. Kullanıcılarınızdan birinin WEP anahtarını birine vermesi/çaldırması sonucunda WEP kullanarak güvence altına aldığımız kablosuz ağımızda güvenlikten eser kalmayacaktır. Zira herkeste aynı anahtar olduğu için kimin ağa dahil olacağını bilemeyiz.

MAC tabanlı erişim kontrolü

Piyasada yaygın kullanılan erisim noktası(AP) cihazlarında güvenlik amaçlı konulmuş bir özellik de MAC adresine göre ağa dahil olmadır. Burada yapılan kablosuz ağa dahil olmasını istediğimiz cihazların MAC adreslerinin belirlenerek erisim noktasına bildirilmesidir. Böylece tanımlanmamış MAC adresine sahip cihazlar kablosuz ağımıza bağlanamayacaktır. Yine kablosuz ağların doğal çalışma yapısında verilerin havada uçuştuğunu göz önüne alırsak ağa bağlı cihazların MAC adresleri de havadan geçecektir, burnu kuvvetli koku alan bir hacker bu paketleri yakalayarak izin verilmiş MAC adreslerini alabilir ve kendi MAC adresini kokladığı MAC adresi ile değiştirebilir
.

MAC adresleri değiştirilemez diye öğrendiyseniz bilgilerinizi bir daha kontrol etmekte fayda var. Evet MAC adresleri cihazlar üzerinde tanımlı gelir ve değiştirilemez ama biz cihazı kullanan işletim sistemine vereceğimiz komutlarla MAC adresini farklı gösterebiliriz.

Linux altında MAC adresi değiştirmek bize bir komut kadar u zaktadır.

root@byte: ~# ifconfig eth1 hw ether 00:10:09:AA.54:09:56

Sonuç olarak ;

- AP ile İstemci arasındaki MAC adresleri açık bir şekilde gider
- MAC adreslerini değiştirmek oldukça kolay

Dolayısı ile bu da kesin bir güvenlik sağlamayacaktır.

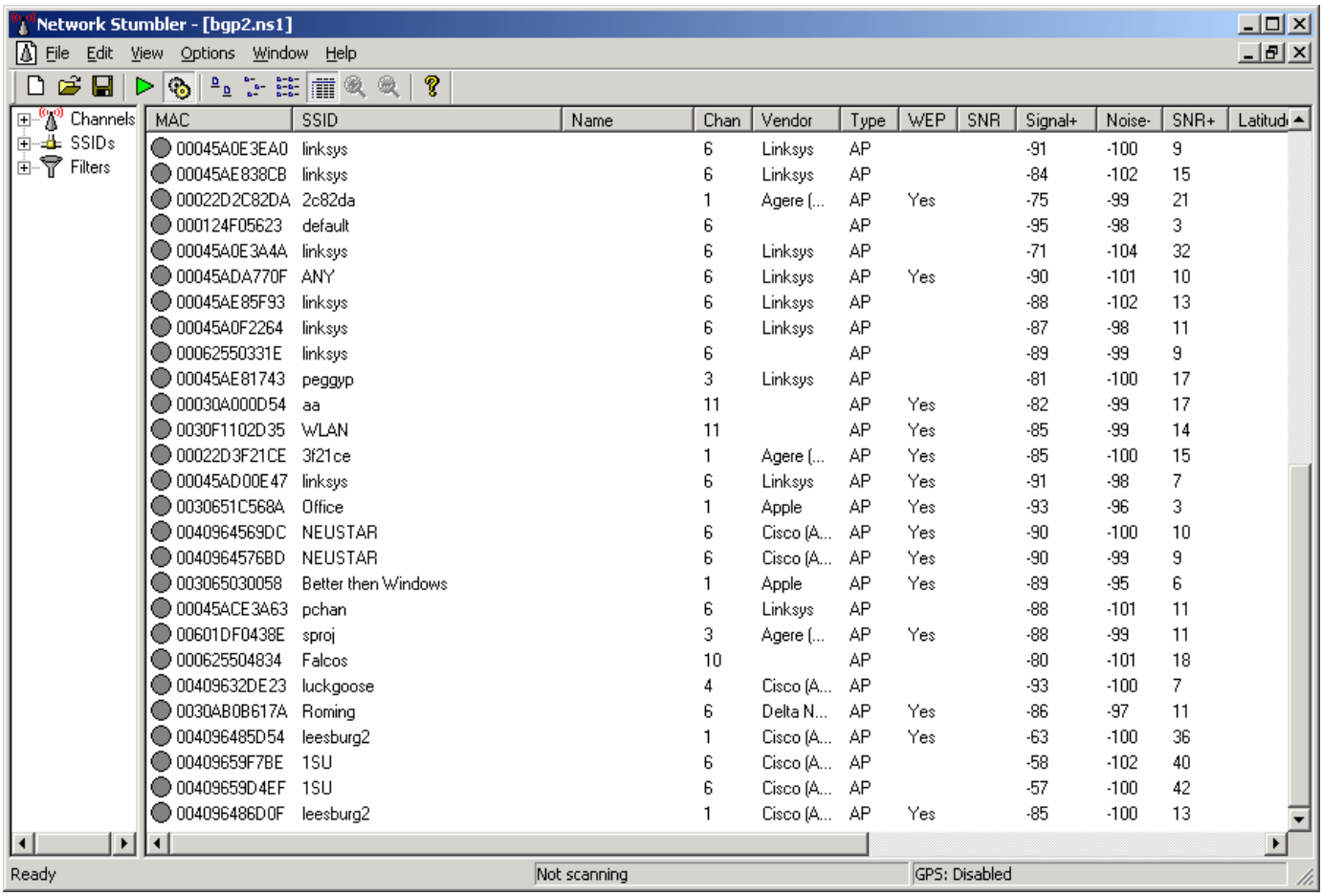
Kablosuz Ağlarda Keşif

Kablosuz ağlarda keşif civar çevrede bulunan erisim noktalarının tespitidir. İşi abartıp WLAN araçlarını arabalarına alarak yol boyunca etrafta bulunan kablosuz ağları keşetmeye yönelik durumlara Wardriving, erisim noktalarının özelliklerine göre(şifreleme desteği var mı? Hangi kanalda çalışıyor vs) bulundukları yerlere çeşitli işaretlerin çizilmesine ise WarChalking deniyor. Ülkemizde henüz yaygınlaşmasa da, Amerika gibi kablosuz ağların çok yoğun olduğu ülkelerde sık karşılaşılabilecek durumlardır.

War driving için çeşitli programlar kullanılabilir fakat bunlardan en önemlileri ve iş yapar durumda olanları Windows sistemler için Netstumbler , Linux sistemler için Kismet'dir. Kismet aynı zamanda Windows işletim sisteminde de çalışabilmektedir.

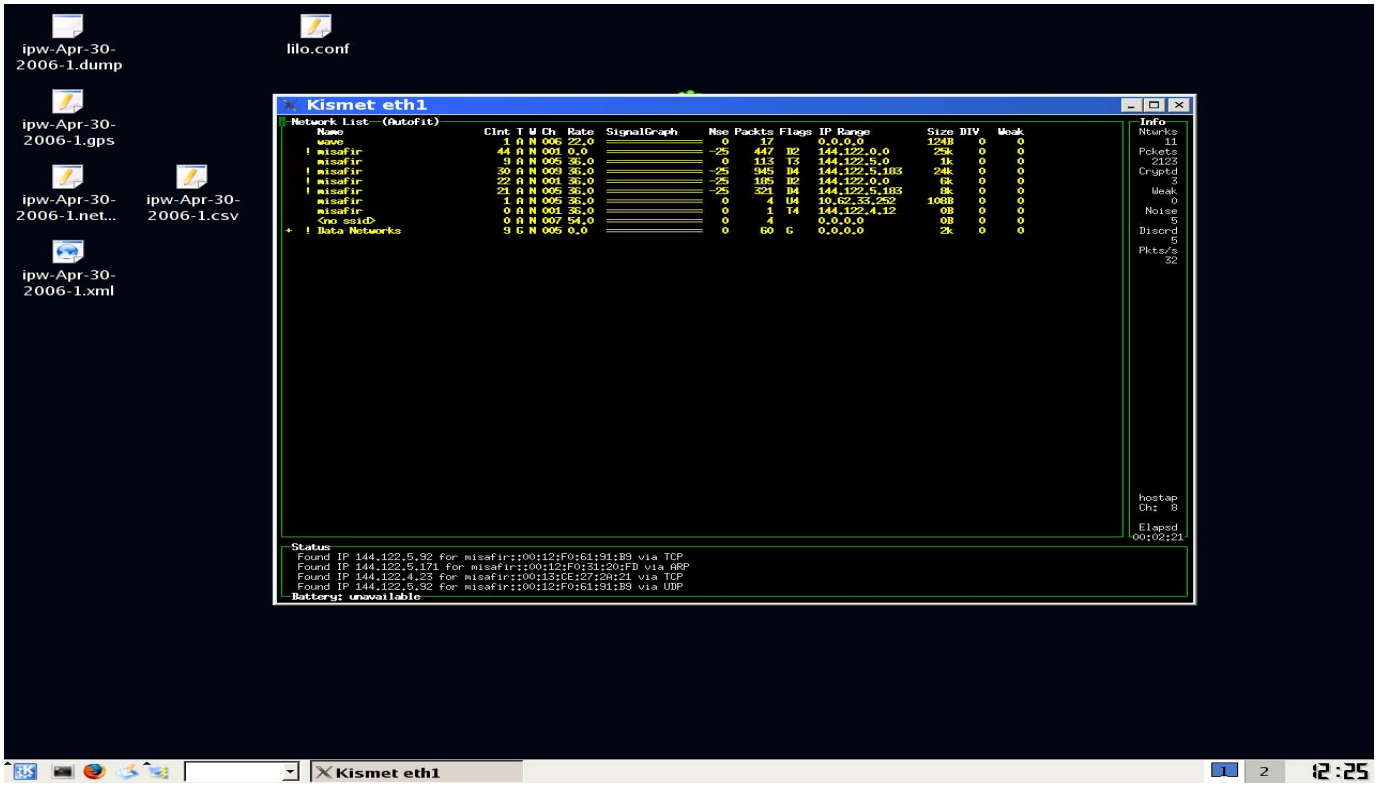
Kablosuz ağlarda keşif, Pasif ve aktif olmak üzere ikiye ayrılır. Adından da anlaşılacağı gibi aktif keşiflerde keşif yapan kendisini belirtir ve aktif cihazları aradığını anons eder. Pasif keşif türünde ise tam tersi bir durum söz konusudur. Pasif keşif gerçekleştiren cihaz kesinlikle ortama herhangi birşey anons etmez, sadece ortamdaki anonsları dinleyerek aktif cihazları belirlemeye çalışır.

Aktif keşif araçlarına en iyi örnek NetStumbler verilebilir. Ücretsiz olarak kullanılabilen Netstumbler çalıştırıldığında kapsama alanındaki tüm aktif cihazları bularak bunları raporlar. Netstumblerin çalışması ya da bir erisim noktasını keşfetmesi için erisim noktasının kendisini anons etmesi lazımdır. Yani basit güvenlik önlemi olarak aldığımız SSID saklama işlemi Netstumbler'i şaşırtacaktır.



Pasif keşif aracı olarak kullanılabilen Kismet ise Netstumbler'a göre oldukça fazla özellik içerir ve kötü niyetli birinin elinde tam donanımlı gizli bir silaha dönüşebilir.

Kismet, kablosuz ağ adaptörlerine özel bir modda çalıştırarak(monitor mode) etrafta olan biteni izlemek ve yorumlamakla yetinir. Böylece bulunduğu ortamdaki tüm trafiği görerek aktif, pasif erişim noktası cihazlarını tüm özellikleri ile birlikte belirler. Sadece erişim noktası cihazlarını belirlemekle kalmaz, bu cihazlara bağlı tüm istemci cihazları ve özeliklerini de belirler. Yeteri kadar korkutucu değil mi? . Şirket ağınızda kullandığınız makinelerin IP bilgileri vs yabancı ellere gitmesini ister miydiniz?

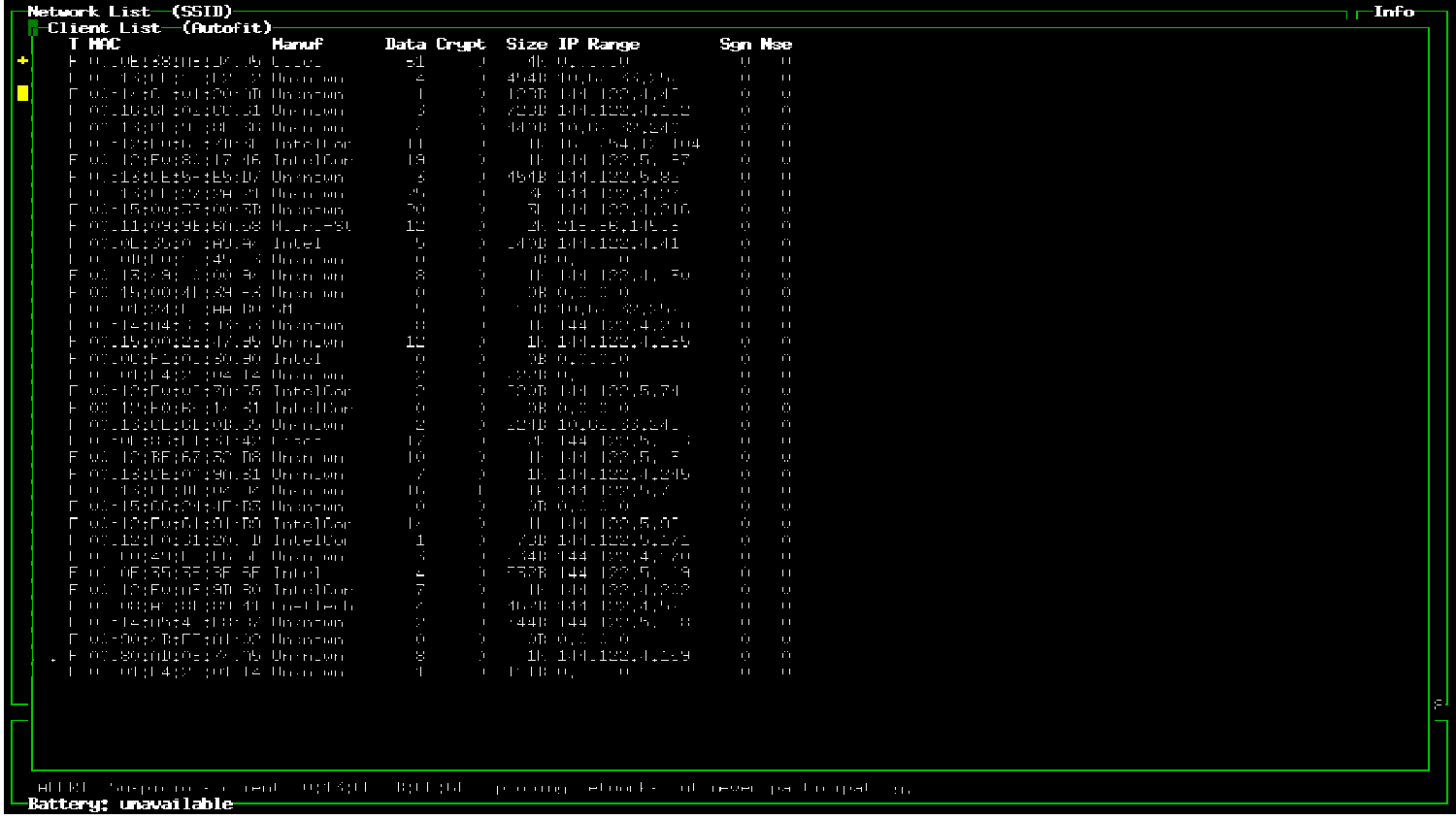


Kablosuz Ağları Dinleme

Kablosuz ağlarda veriler havada uçuştuğu için dinleme yapmak kablolu ağlara göre daha kolaydır. Amaca uygun kullanılan bir dinleme aracı ile bir kablosuz ağdaki trafik ağa dahil olmadan rahatlıkla izlenebilir. Linux sistemlerde kablosuz ağ trafiği dinlemek için Kismet adlı program tercih edilir.

Kismet, monitoring (rfmon) mod destekleyen kablosuz ağ arabirimleri için düşünülmüş 802.11b, 802.11a ve 802.11g protokolü ile çalışan kablosuz ağlarda pasif dinleme yapmaya yarayan bir araçtır. Aynı zamanda kablosuz ağlar için pasif keşif aracı olarak da kullanılabilir.

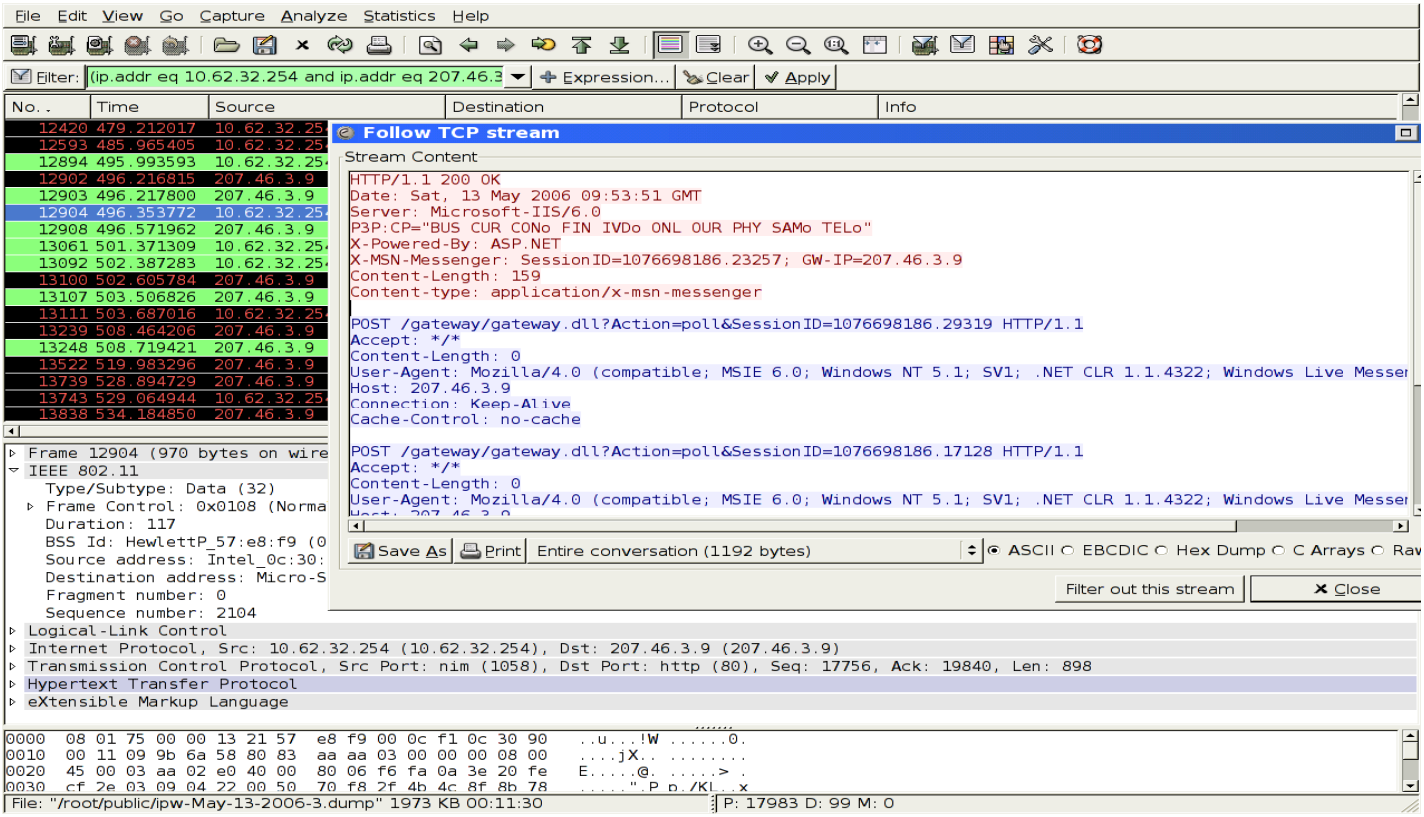
Kismet ile dinleme yapılırken etraftaki erişim noktaları ya da istemciler rahatsız edilmez. Tamamen pasif modda bir dinleme yapıldığı için kablosuz ağları korumaya yönelik saldırı tespit sistemleri kolaylıkla aldatılmış olur. Özellikle şifresiz bir iletişim yöntemi tercih edilmişse Kismet bu noktada kablosuz ağdaki tüm herşeyi görebilir. Ekte bu seneki Linux şenliklerinde sunum için hazırladığım Kismet'in ekran görüntüsünü görebilirsiniz: ağa dahil olmadan çevre civardaki erişim noktalarını ve bu erişim noktasına bağlı tüm kablosuz ağ istemcilerinin MAC ve IP bilgilerinin kismet tarafından rapor edilmiş hali.



Kismet ve ek bir iki araç kullanılarak MAC adres tabanlı güvenlik önlemi alınmış kablosuz ağlara kolaylıkla giriş yapılabilir.

Kismet aynı zamanda kablosuz ağlarda izinsiz giriş tespiti içinde kullanılabilir. Ağa erişim izni olmayıp da giriş deneyiminde bulunan kullanıcılar Kismet tarafından rahatlıkla belirlenerek raporlanacaktır.

Yine kismet aracı tarafından kaydedilmiş trafiğin Ethereal(Trafik Analiz aracı) ile analiz edilmiş haline bakacak olursak hiç yetkimiz olmadığı halde kablosuz ağdaki istemcilerin nerelere eriştiğini ve neler yaptığını görmemiz zor değildir.



Nasıl Korunacağız ?

Özellikle kablosuz ağlarda tehlike oluşturabilecek potsansiyelleri belirleyerek işe girişelim. Kablosuz ağlarda risk oluşturan kullanıcı kitlesini üçe ayırabiliriz;

- Meraklı Bilgisayar kullanıcıları
- Bandgenişliği hırsızları
- Hackerlar

Meraklı bilgisayar kullanıcıları , hiçbir şekilde kurtulamayacağımız, aslında göründüğü kadar da tehlikeli olmayan kısmı oluşturur. Konu hakkında teorik bilgileri olmadığı için yapmak istedikleri işleri otomatize araçlara havale ederler ve bunların çıktıları ile yetinirler. Bu kullanıcı grubunu oluşturan kimliklerden korunmak için SSID saklama, MAC adres tabanlı erişim denetimi gibi temel güvenlik önlemlerini almanız yeterli olacaktır.

Diğer bir kullanıcı kitlesi de şifrelenmemiş ya da eksik yapılandırılmış kablosuz ağları kullanan “bant genişliği hırsızları “olarak da adlandırabileceğimiz zararsız kullanıcılardır. Bunların tek amacı varolan kablosuz ağı kullanmaktır. Kablosuz ağdan kendileri de yararlandıkları için zarar vermezler. Ağınızda yavaşlıktan şikayet ediyorsanız ilk düşünülecek kategorideki kimliklerdir.

Hackerlar, bu tip kimlikler bilgi seviyelerine göre değişecektir. Bazıları için ileri düzey güvenlik önlemleri almadan korunmanız imkansızdır. Yine de WEP/WPA gibi protokolleri kullanırsanız bu tip kimliklerden gelecek saldırı riski azalacaktır. Bir nevi caydırma politikası olarak da düşünebiliriz.

Ev Kullanıcıları için Tavsiyeler

Evinde kablosuz ağ kullananlar için temel seviyede güvenlik önlemi almak yeterli olacaktır. İlk olarak Kullandığımız erişim noktası cihazının adını(SSID) değiştirmeliyiz. Zira erişim noktasının adını varsayılan olarak bırakmamız cihazın yazılımında çıkacak bir güvenlik açığının ilk bizim donanımımızda denenmesi demektir. Yine benzer şekilde cihaz markası ve modelini bilen kötü niyetli birileri cihazın yönetim arabirimine ulaşarak varsayılan kullanıcı adı ve parolalarını deneyecektir. Bu sebeple alınan cihazların varsayılan değerleri – özellikle yönetim arabirimine giriş için kullanılan hesap bilgileri- mutlaka değiştirilmelidir.

Cihaz destekliyorsa SSID yayınını da kesebiliriz. Sadece kendi belirlediğimiz istemcilere cihazın adını vererek bağlantı kurmasını sağlamak da iyi bir önlem olacaktır.

Yine kullandığımız erisim noktasına bağlı olarak WEP ya da WPA kullanarak iletişimi şifrelemekte fayda var. WEP anahtarını seçerken de olabildiğince karışık bir anahtar seçmek bir nebze daha faydalı olacaktır.

Şirket Ağları için tavsiyeler

Şirket ağlarında kullanılan erişim cihazları kesinlikle yerel ağla direkt haberleştirilmemelidir. Araya bir güvenlik duvarı konularak kablosuz ağ istemcilerinin yerel ağa girişleri sınırlandırılarak olası saldırı girişimlerinde iç ağımızın etkilenmesini önlemiş oluruz.

Mac adresi tabanlı güvenlik kontrolü şirket ağlarından da alınması gereken temel güvenlik önlemlerindendir. Fakat sadece mac adresi tabanlı denetim yapıp bırakmak bir işe yaramayacaktır. Ağımızdaki MAC-IP değişikliklerini izleyen ve raporlayan bir araç da güvenliğin kontrolünü sağlamada önemli bir adım olarak karşımıza çıkıyor.

En basitinden ağa yeni eklenen ve ağda IP, MAC adreslerini değiştiren cihazlar uygun bir yazılım ile kontrol edilmelidir. Linux ve UNIX sistemlerde arpwatch yazılımı bu işi oldukça iyi yapmaktadır. Aynı yazılımın Windows versiyonu(winarpwatch) da ücretsiz olarak kullanılabilir.

Kablosuz ağlar için tasarlanmış saldırı tespit yazılımları kullanılabilir. Fakat bu tip yazılımların yönetimi ve ağa uygulanması zaman alacaktır.

Erisim noktası cihazınız destekliyorsa WPA kullanımı iyi bir seçim olacaktır. Şirket ağlarında kesinlikle WEP kullanımı tercih edilmemelidir. Erişim noktası cihazının özelliklerine bağlı olarak EAP olarak adlandırılan ve çeşitli şekillerde kimlik doğrulama özelliği sağlayan protokollerde kullanılmalıdır.

Halka Açık Kablosuz Ağlardaki Tehlikeler

Kablosuz ağların belki de en işe yarar olduğu durumlar halka açık olanlarıdır. Hemen hemen tüm büyük alışveriş merkezlerinde bu tip ağlara rastlayabiliriz. Bazıları erişim için kullanıcı adı / parola istese de yukarıda anlattığım yöntemler kullanılarak bu tip ağlar rahatlıkla kandırılabilir. Gelelim bu tip ağlardaki risklere;

Öncelikle aynı erişim noktasına bağlı tüm istemcilerin trafiği şifrelenmemiş bir şekilde havada dolaşacaktır. Bunun içinde MSN görüşmeleriniz, e-postalarınız ve ziyaret ettiğiniz siteler de dahil.

Hemen kafamızda minik bir senaryo kuralım: Herkese açık bir kablosuz ağ ortamına gelen kötü niyetli bir kullanıcı diz üstü bilgisayarını açarak ortama dahil oluyor ve kablolu ağlarda da kullanılabilen trafik dinleme ve değiştirme araçlarını kullanmaya başlıyor. Beş dakika sonra tüm trafiği erişim noktası üzerinden değil de kendisi üzerinden geçirmeyi başarıyor ve istediği işlemleri bu trafik üzerinde yapıyor. Mesela bir istemci www.galatasaray.org adresine girmek isterken onun isteğini www.antu.com'a yönlendirebilir ve daha niceleri.

Burada kurduğumuz senaryo oldukça zor gözükmesine rağmen işini bilen kötü niyetli biri tarafından kolaylıkla başarılabilir. Peki o zaman ne yapacağız? Böyle bir nimetten faydalanmayacağız mı dediğinizi duyar gibiyim. Kullanım riskini bildikten sonra kullanmamanız için hiçbir sebep yok. Ama eğer güvenli bir iletişim istiyorsanız ya VPN kullanmanızı ya da benzeri bir özellik sağlayan TOR aracını kullanmanızı öneririm.

Ileri Düzey okumalar için

http://ferruh.mavituna.com/article/?1113
http://www.enderunix.org/docs/kablosuz_alan_aglari/

**Düzeltme ve kaykilarindan dolayi Enis KARAASLAN'a tesekkur ederim.

Huzeyfe ÖNAL <Huzeyfe@enderunix.org> Haziran 2006