

Kablosuz Ağlar Ve Güvenlik

Son yıllarda ADSL bağlantıların her ortama girmesi ve dizüstü bilgisayarlardaki fiyat düşüşü kablosuz ağ kullanımını büyük oranda arttırdı. Yeni alınan ADSL modemlerin çoğunda kablosuz ağ özelliği de birlikte geliyor. Kablosuz ağ kullanımı hem pratik hem de kullanışlı fakat gerekli önlemler alınmazsa güvenlik noktasında biraz sıkıntılıdır. Bu yazıda kablosuz ağlar ve bu ağlarda güvenliği sağlayacak temel bileşenler anlatılmıştır.

Bir konunun güvenliğinin sağlanabilmesi için bazı temel detayların bilinmesi gerekir. Kablosuz ağların güvenliği konusunun anlaşılabilmesi için güvenliği sağlayacak ya da güvenlik açığına sebep olacak bileşenlerin neler olduğuna bir gözatalım.

Kablosuz Ağ arabirim çalışma modları

Kablosuz ağ adaptörleri kullandıkları sürücüye ve yapacağı işleve bağlı olarak dört farklı modda çalışabilir. Bunlar: Managed, Master(hostap), Ad-hoc ve Monitor mod.

Master Mod: Etraftaki kablosuz ağ istemcilerine hizmet vermek için kullanılan mod. Erişim noktası olarak adlandırılan cihazlarda kablosuz ağ adaptörleri bu modda çalışır.

Managed Mod: Bir erişim noktasına bağlanarak hizmet alan istemcinin bulunduğu mod.

Ad-Hoc Mod: Arada bir AP olmaksızın kablosuz istemcilerin haberleşmesi için kullanılan mod.

Monitor Mod: Herhangi bir kablosuz ağa bağlanmadan pasif olarak ilgili kanaldaki tüm trafiğin izlenmesine olanak sağlayan mod. Kablosuz ağlarda güvenlik konusunda sık sık kullanılan bir moddur.

Promiscious mod ve monitor mod farkı

Klasik yapılan hata promiscious mod ve monitor modun karıştırılmasıdır. Bu iki moda birbirinden tamamen farklıdır.

Monitor mod, bir kablosuz ağ arabiriminin herhangi bir ağa bağlanmadan o ağa ait tüm trafiği izleyebilmesine olanak verir. Promiscious mod ise bir ağa bağlanıldığında o ağda –duruma göre- tüm trafiği izleyebilmenizi sağlar.

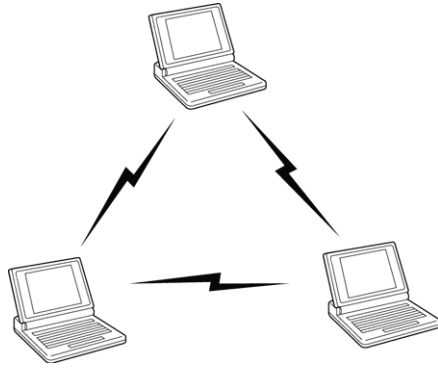
Kablosuz ağlarda Wireshark gibi sniffer araçları kullanırken Promiscious mod seçili ise bazen hiç paket yakalayamazsınız. Bu kullandığınız kablosuz ağ adaptörünün ya da sürücüsünün promiscious mod desteklemediğini gösterir.

Yaygın Kablosuz Ağ Yöntemleri

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, diğeri 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 olarak iki bilgisayarı bu aracı cihazlar ile konuşturacağız.



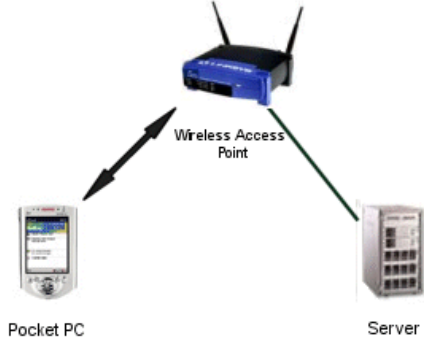
Oysa bunlardan başka bir seçeneğimiz daha var -tabi eğer her iki bilgisayarda kablosuz ağ adaptörü varsa-. Bu iki cihazın kablosuz ağ adaptörlerini Ad-hoc modda çalışacak şekilde ayarlırsak ve internete çıkan bilgisayarda bağlantı paylaşımı yaparsak iki makinede özgür bir şekilde interneti kullanabilecektir.

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 ya da kullandığınız dizüstü bilgisayarın kendi sistemi ile kolaylıkla Ad-hoc mod kablosuz ağ kurulabilir.

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

Infrastructure mode : Erişim noktası bağlantı yöntemi



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 Ağlarda Güvenlik Önlemleri

Kablosuz ağlardaki en temel güvenlik problemi verilerin havada uçuşmasıdır. Normal kablolu ağlarda switch kullanarak güvenliğini fiziksel sağlayabiliyorduk ve switch’e fiziksel olarak bağlı olmayan makinelerden korunmuş oluyorduk. Oysaki kablosuz ağlarda tüm iletişim hava üzerinden kuruluyor ve veriler gelişigüzel ortalıkta dolaşıyor.

Kablosuz ağlarda güvenlik sağlama amaçlı alınacak temel Önlemler

Erişim noktası Öntanımlı Ayarlarının Değiştirilmesi

Kablosuz ağlardaki en büyük risklerden birisi alınan erişim noktası cihazına ait öntanımlı ayarların değiştirilmemesidir. Öntanımlı ayarlar erişim noktası ismi, erişim noktası yönetim konsolunun herkese açık olması, yönetim arabirimine girişte kullanılan parola ve şifreli ağlarda ağın şifresidir. Yapılan araştırmalarda kullanıcıların çoğunun bu ayarları değiştirmedeği görülmüştür.

Kablosuz ağların güvenliğine dair yapılması gereken en temel iş öntanımlı ayarların değiştirilmesi olacaktır.

Erisim Noktası İsmi görünmez kılma: SSID Saklama

Kablosuz ağlarda erişim noktasının adını(SSID) saklamak alınabilecek ilk temel güvenlik önlemlerinden biridir. Erişim noktaları ortamdaki kablosuz cihazların kendisini bulabilmesi için 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.

SSID saklama her ne kadar bir önlem olsa da teknik kapasitesi belli bir düzeyin üzerindeki insanlar tarafından rahatlıkla öğrenilebilir. Erişim noktasının WEP ya da WPA protokollerini kullanması durumunda bile SSID’lerini şifrelenmeden gönderildiğini düşünürsek ortamdaki kötü niyetli birinin özel araçlar kullanarak bizim erişim noktamızın adını her durumda öğrenebilmesi mümkündür.

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. Dolayısı ile bu tip ağlarda 802.1x kullanmadan tam manası ile bir güvenlik sağlanamayacaktır.

MAC tabanlı erişim kontrolü

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

Linux altında MAC adresi değiştirmek bize bir komut kadar uzaktadır.

```
# ifconfig eth1 hw ether 00:10:09:AA:54:09:56
```

Ya da mac-changer ile MAC adresi değişimi yapılabilir.

Şifreleme Kullanma

Kablosuz ağlarda trafiğin başkaları tarafından izlenmemesi için alınması gereken temel önlemlerden biri de trafiği şifrelemektir. Kablosuz ağlarda şifreleme WEP(*wired equivalent privacy*) ve WPA(*Wi-Fi Protected Access*) olarak adlandırılan iki protokol üzerinden yapılır. Her iki protokol de ek güvenlik önlemleri alınmazsa günümüzde güvenilir kabul edilmez. İnternette yapılacak kısa bir arama ile Linux altında uygun bir kablosuz ağ adaptörü kullanılarak tek komutla WEP korumalı ağlara nasıl sızıldığı izlenebilir. Bugüne kadar WEP kullananlara hep WPA’ya geçmeleri ve uzun karmaşık parola seçmeleri

önerilirdi. Zira WPA, WEP'in zayıf kaldığı noktaları güçlendirmek için yazılmış bir protokoldü . Fakat 2008'in son aylarında iki üniversite öğrencisinin yaptığı çalışma pratikte WPA'nın ~15 dakika da kırılabilceğini ispat etmiş oldu. Aslında çalışma WPA'da değil WPA'nın kullandığı TKIP(emporal Key Integrity Protocol) bileşenindeki açıklıktan kaynaklanıyordu. Dolayısı ile WPA ve AES şifreleme kullanarak gerçek manada güvenlik elde etmek mümkün.

Sonuç olarak ;

- Erişim noktalarının öntanımlı ayarları mutlaka değiştirilmeli
- Şifreleme olmadan güvenlik olmaz
- AP ile İstemci arasındaki MAC adresleri her durumda açık bir şekilde gider
- MAC adreslerini değiştirmek oldukça kolay
- WEP/WPA ile korunmuş ağlar ek güvenlik önlemleri alınmazsa güvenli değildir.

Katmanlı güvenlik anlayışı gereğince yukarıda anlatılan yöntemlerin uygulanması güvenliğinizi bir adım daha arttıracaktır.

Kablosuz Ağlarda Keşif

Kablosuz ağlarda keşif yakın çevrede bulunan erişim noktalarının tespitidir. İşi abartıp WLAN araçlarını arabalarına alarak ya da yaya olarak yol boyunca etrafta bulunan kablosuz ağları keşfetmeye yönelik çalışmalara Wardriving, erişim noktalarının özelliklerine göre(şifreleme desteği var mı? Hangi kanalda çalışıyor vs) buldukları yerlere çeşitli işaretlerin çizilmesine ise WarChalking deniyor.

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 monitor mode destekleyen kablosuz ağ arabirimleri ile 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 ama gizli cihazları belirlemeye çalışır.

Aktif keşif araçlarına en iyi örnek NetStumbler verilebilir. Ücretsiz olarak kullanılabilen Netstumbler çalıştırıldığında kapsama alanında anons yapan tüm aktif cihazları bularak bunları raporlar.

Netstumblerin çalışması ya da bir erişim noktasını keşfetmesi için erişim 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 izler ve kaydeder. 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 özelliklerini de belirleyebilir daha da ötesinde şifreleme kullanılmıyorsa tüm trafiği dinler. Yeteri kadar korkutucu değil mi? Şirket ağınızda kullandığınız makinelerin IP bilgileri vs yabancı ellere gitmesini ister miydiniz?

Kablosuz Ağları Dinleme

Kablosuz ağlarda veriler havada uçtuğu 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 protokolleri ile uyumlu kablosuz ağlarda pasif dinleme yapmaya yarayan bir araçtır. Aynı zamanda kablosuz ağlar için pasif keşif aracı olarak ve basit manada saldırı tespit sistemi 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 bazı saldırı tespit sistemleri kolaylıkla aldatılabilir. Özellikle şifresiz bir iletişim yöntemi tercih edilmişse Kismet bu noktada kablosuz ağdaki tüm herşeyi görebilir.

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

```
Network List (BSSID)
Name          T W Ch  Pkts/s  Flags  IP Range  Size
+ Adhoc networks  G N 011  467    0.0.0.0   3k
+ Probe networks  G N ---  19    0.0.0.0   0B
EIGM          A N 006   1    0.0.0.0   0B
<no ssid>     A Y ---  33    0.0.0.0   2k
! BCFire       A O 011 20697  0.0.0.0   0B
! Guest        A N 011 20997  0.0.0.0   0B
! dsmo         A O 011 20364  0.0.0.0   0B
! BCPolice     A O 011 20783  0.0.0.0   0B
! BCIY         A O 011 20943  0.0.0.0   0B
! BCCity-Staff A O 011 20327  0.0.0.0   0B
! FAMERA       A O 011 73617  U 10.0.0.129 22M

Info
Networks  14
Pkts/s    152331
Cryptd    24
Weak      0
Noise     185
Discard   185
Pkts/s    152

ipw220
Ch: 11
Elapsed  00:45:20

Status
ALERT: Suspicious client 00:1E:2A:4A:0B:00 - probing networks but never participating.
ALERT: Suspicious client 00:16:44:A7:F3:7A - probing networks but never participating.
ALERT: Suspicious client 00:18:DE:EA:12:20 - probing networks but never participating.
ALERT: Suspicious client 00:0D:ED:93:18:D6 - probing networks but never participating.
Battery: AC charging 34%
```

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

Halka Açık Kablosuz Ağlardaki Tehlikeler

Kablosuz ağların belki de en işe yarar olduğu durumlar halka açık olanlarıdır. Hemen hemen tüm büyük alışveriş merkezlerinde, lokanta ve kafelerde 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. Ortama dahil olan birisi basit MITM atakları ile tüm trafiği üzerinden geçirip içeriğini inceleyebilir, ötesinde değiştirebilir.

Başka kimlikte biraz daha paranoyak bir saldırgan gelip ağa dahil olmadan yine tüm trafiği monitor modda izleyebilir hatta eğer bu ortamda Hotmail, Yahoo, Gmail ya da https kullanan sistemlerinize erişiyorsanız saldırgan da kişisel giriş parolanızı bilmeden ilgili sitelerin size gönderdiği cookie'leri çalarak aynı sistemlere erişebilir.

Diğer bir tehlike de saldırganın trafik izleme için zahmete girmeden ortamda bulunan erişim noktalarından birinin ismini taklit ederek sahte erişim noktası oluşturmasıdır. Böylece bazı kullanıcılar aslıyla aynı isme sahip belki daha iyi çeken sahte erişim noktasına bağlanacak ve buradan işlemlerini yapacaktır. Bu da bir saldırgan için ağına bağlanan tüm istemciler üzerinde mutlak hakimiyet kurması manasına gelir.

Kısacası halka açık kablosuz ağlarda internet kullanmak buzda dansa benzer. Dolayısı ile dikkatli olmak ve güvenli sörf için uygun araçlar kullanmak gerekir. Bu tip ağlarda internete girmeniz gerekiyorsa ya VPN üzerinden ya da TOR benzeri şifreli iletişim sağlayan networkler üzerinden girmeniz trafiğinizin başkaları tarafından izlenmesini önleyecektir.

Kablosuz Ağ Güvenlik Testleri için Ortam oluşturma

Kablosuz Ağlarda güvenlik konusu pratiği zor olan bir konudur. Bunun temelde iki sebebi vardır. Birincisi kablosuz ağ adaptörleri sürücü eksikliğinden genelde Windows altında test yapacak fonksiyonlara sahip değildir. Bu gibi testler için Linux kullanılması çok daha pratik olacaktır. Diğer bir konu da başkalarının kablosuz ağları üzerinden yapılacak testler etik olmayacağı için kendi kablosuz ağ ortamınızda çalışmalar yapmanız gerektiğidir. Eğer kullanılan Erişim Noktası(Access Point) paylaşımlı ise yapacağınız testlerden diğer kullanıcılar etkilenecektir.

Bu durumda son çare olarak yeni bir donanım almak kalıyor. Diğer bir yöntem de bir adet USB üzerinden çalışan kablosuz ağ adaptörü alıp Vmware içerisinden bu adaptörü kullanmaktır. Böylece hem mobil bir AP'e sahip olacaksınız hem de kablosuz ağlarda güvenlik testi yaparken Windows'un kısıtlayıcı özelliklerine takılmadan Linux üzerinden istediğiniz işlemleri yapabileceksiniz. Böylece istediğinizde sanal bir AP'ye istediğinizde de Linux altında test yapmak için kullanabileceğiniz kablosuz bir ağ adaptörüne ulaşmış olacaksınız.

Vmware ile Kablosuz Ağ adaptörlerini Kullanma

Gerçek işletim sisteminizde kullandığınız wireless kartları Vmware altında da aynı özelliklerde kullanmak ne yazık ki mümkün olmuyor. Vmware'den arabirim modunu bridge , nat yapılarak wifi kartınızın yararlandığı bağlantı Vmware makineye sağlanabilir fakat bu vmware üzerinde wireless bir

kart olarak algılanmaz. Sıradan bir ethernet kartı gibi Vmware'in kendi sürücülerini kullanarak işlem yapılır.

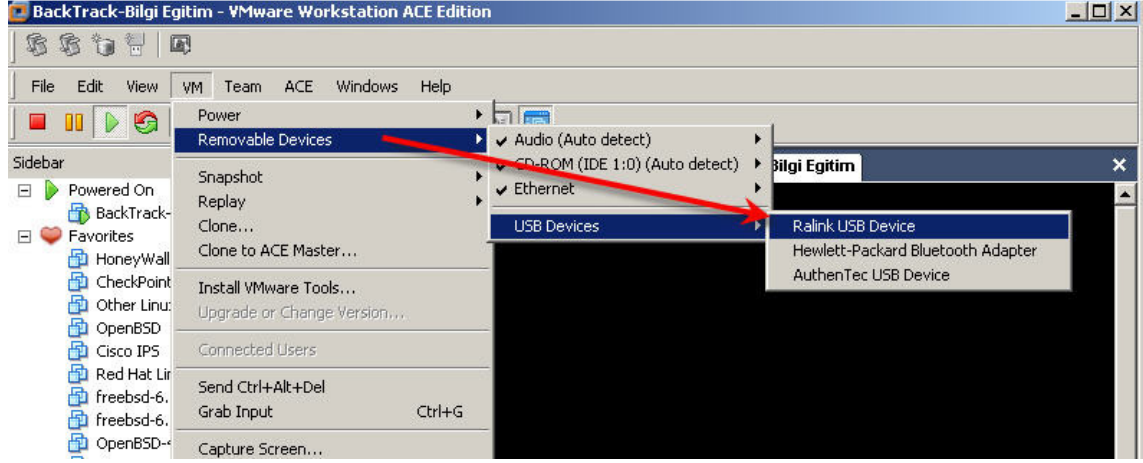


Bu durumda Wireless ağlara bağlanıp analiz yapma imkanımız yok. USB bir wifi kartı alıp bunu Vmware'e tanıtarak kullanacaksınız. (Gerçek sisteminizin Windows, Vmware'deki sisteminiz Linux ise) USB wireless kartınızı Vmware altında gerçek özellikleri kullanabilmek için Vmware sürümü 6.x , Vmware player kullanıyorsanız güncel sürümü olmalı. Bundan sonrası Vmware'in menülerinden

usb cihazı Vmware'e wireless kart olarak tanıtmak ve sürücünün sağladığı wireless özelliklerini kullanmaya kalıyor.

Not:Vmware'in kullanacağı usb wireless kartı gerçek işletim sisteminin tanınması gerekmez.

Vmware'de usb wireless kartını aktif etme

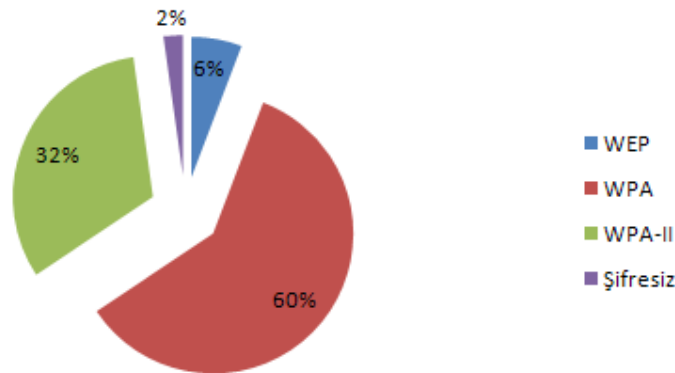


Türkiye’de Kablosuz Ağ Kullanımı Ve Güvenlik Araştırması

Yaklaşık bir ay önce Türkiye’de kablosuz ağların güvenlik açısından durumunu incelemek için bir çalışma başlattık. Bu çalışma kablosuz ağ kullanımında kullanıcıların güvenlik açısından ne durumda olduğunu belirlemek. Çıkan sonuçlar net durumu tam olarak yansıtmasa da Türkiye’deki kablosuz ağ kullanıcılarının ortalama durumunu gösterir nitelikte.

Çalışmanın şifreli ağ kullanımı ile ilgili sonuçları:

Güvenli Kablosuz Ağ Kullanımı



Huzeyfe ÖNAL - huzeyfe@lifeoverip.net

<http://www.lifeoverip.net>