

**T.C.
MİLLÎ EĞİTİM BAKANLIĞI**

BİLİŞİM TEKNOLOJİLERİ

AĞ GÜVENLİĞİ

Ankara, 2013

- Bu modül, mesleki ve teknik eğitim okul/kurumlarında uygulanan Çerçeve Öğretim Programlarında yer alan yeterlikleri kazandırmaya yönelik olarak öğrencilere rehberlik etmek amacıyla hazırlanmış bireysel öğrenme materyalidir.
- Millî Eğitim Bakanlığınca ücretsiz olarak verilmiştir.
- **PARA İLE SATILMAZ.**

İÇİNDEKİLER

AÇIKLAMALAR	iii
GİRİŞ	1
ÖĞRENME FAALİYETİ-1	3
1. AĞ İLETİŞİMİ TEHDİTLERİ	3
1.1. Ağ Saldırı Riskleri	4
1.1.1. Bilgi Hırsızlığı	4
1.1.2. Kimlik Hırsızlığı	5
1.1.3. Veri Kaybı ve Veri Kullanma	5
1.1.4. Hizmet Aksatma	5
1.2. Ağ İletişim Tehditleri	6
1.2.1. Haricî ve Dâhili Tehditler	6
1.3. Sosyal Mühendislik	8
1.3.1. Sahte Senaryo Uydurma	9
1.3.2. Oltalama (Phishing)	9
1.3.3. Sesle / Telefonla Oltalama (Vishing)	9
1.4. Saldırı Yöntemleri	9
1.4.1. Hizmet Reddi (Denial of service-DoS)	10
1.4.2. Dağıtılmış Hizmet Reddi ((Distributed Denial of Service-DDoS)	10
1.4.3. Deneme Yanılma	11
1.4.4. Casus Yazılımlar	12
1.4.5. İzleme Tanımlama Bilgileri	13
1.4.6. Reklam Yazılımları	13
1.4.7. Açılır Pencereler	13
1.4.8. Spam	13
1.5. Güvenlik Önlemleri	14
1.5.1. Tanımlama ve Kimlik Doğrulama İlkeleri	14
1.5.2. Parola ilkeleri	15
1.5.3. Kabul Edilebilir Kullanım İlkeleri	15
1.5.4. Uzaktan Erişim İlkeleri	15
1.5.5. VPN Bağlantıları	15
1.5.6. Ağ Bakım Yordamları	16
1.5.7. Olay İşleme Yordamları	16
UYGULAMA FAALİYETİ	17
ÖLÇME VE DEĞERLENDİRME	18
ÖĞRENME FAALİYETİ-2	20
2. GÜVENLİK ARAÇLARI VE UYGULAMALAR	20
2.1. Güvenlik Duvarı	20
2.2. Spam Filtresi	22
2.3. Yamalar ve Güncellemeler	23
2.4. Casus Yazılımlardan Korunma Yazılımları	23
2.5. Açılır Pencere Engelleyicileri	25
2.6. Antivirüs Yazılımlar	27
UYGULAMA FAALİYETİ	32
ÖLÇME VE DEĞERLENDİRME	33
ÖĞRENME FAALİYETİ-3	35

3. KABLOSUZ ORTAM GÜVENLİĞİ	35
3.1. Kablosuz LAN (Yerel Ağ) Güvenliği.....	35
3.2. SSID	38
3.3. WLAN'a Saldırıları.....	38
3.4. WLAN'a Erişimi Sınırlama	39
3.5. WLAN'da Kimlik Doğrulama	40
3.6. WLAN'da Şifreleme.....	41
3.6.1. WEP.....	41
3.6.2. WPA	42
3.7. WLAN'da Trafik Filtreleme	43
UYGULAMA FAALİYETİ	44
ÖLÇME VE DEĞERLENDİRME	46
MODÜL DEĞERLENDİRME	48
CEVAP ANAHTARLARI.....	50
KAYNAKÇA.....	52

AÇIKLAMALAR

ALAN	Bilişim Teknolojileri
DAL / MESLEK	Ağ İşletmenliği
MODÜLÜN ADI	Ağ Güvenliği
MODÜLÜN TANIMI	Bu modül, Ağ sistemi güvenliğini oluşturmak ve güvenlik tedbirlerini almak için gerekli temel bilgi ve becerilerin kazandırıldığı bir öğrenme materyalidir.
SÜRE	40/24
ÖN KOŞUL	Ethernet modülünü tamamlamış olmak
YETERLİK	Ağ güvenliğini sağlamak
MODÜLÜN AMACI	Genel Amaç Bu modül ile gerekli ortam sağlandığında; ağın sorunsuz ve güvenli çalışması için güvenlik önlemlerini alarak güvenlik araçlarını kullanabilecek, sorunsuz ve güvenli çalışan kablosuz ağ yapılandırabileceksiniz. Amaçlar 1. Güvenlik önlemlerini alabileceksiniz. 2. Güvenlik araçlarını kullanabileceksiniz. 3. Kablosuz ortam güvenliğini sağlayabileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	Ortam: Ağ kurulu bilgisayar laboratuvarı Donanım: Erişim noktası (Access Point) veya kablosuz modem, iki adet bilgisayar
ÖLÇME VE DEĞERLENDİRME	Modül içinde yer alan her öğrenme faaliyetinden sonra verilen ölçme araçları ile kendinizi değerlendireceksiniz. Öğretmen modül sonunda ölçme aracı (çoktan seçmeli test, doğru-yanlış testi, boşluk doldurma, eşleştirme vb.) kullanarak modül uygulamaları ile kazandığınız bilgi ve becerileri ölçerek sizi değerlendirecektir.

GİRİŞ

Sevgili Öğrenci,

Bilgisayar ağları, bilgi alışverişinin çok hızlı bir şekilde gerçekleştiği ve bilgiye kolay ulaşım sağlayan bir bilgi havuzudur. Bu ortamı oluşturan ve önemli verileri içerisinde barındıran ağ güvenliğinin önemi de gün geçtikçe artmaktadır.

Dev bir bilgisayar ağı ve bunun sonucu oluşan *İnternet* herkes için vazgeçilmez bir bilgi kaynağıdır. Bütün mesleklerde bilgisayar kullanılması, kişisel bilgisayarların her eve girmesi, *İnternete* ulaşmanın çok kolay ve ucuz bir hâle gelmesi istisnasız her bilgisayarın bir bilgisayar ağına bağlı olması anlamına gelmektedir.

Bilgisayar sistemlerine ve ağlarına yönelik saldırılar ciddi miktarda para, zaman, prestij ve değerli bilgi kaybına neden olabilir. Bu saldırıların hastane bilişim sistemleri gibi doğrudan yaşamı etkileyen sistemlere yönelmesi durumunda kaybedilen insan hayatı da olabilir.

Bilgisayar ağlarının bu denli önemli hâle gelmesi ile birlikte ağ güvenliğini sağlama konusunda bilgi sahibi olma ve işine hâkim olan teknik elemanlara ihtiyaç da artmıştır.

Bu modül sonunda edineceğiniz bilgi ve becerilerle ağ güvenliğini tanıma güvenlik tehditlerini önceden tespit edebilme ve önleme, ağ kullanıcılarına düşen görevleri bilme ve sorunlara çözüm üretebilme, kablosuz ağ güvenliği bilgilerini ve yeteneklerini eksiksiz biçimde kazanacaksınız. Mevcut bilgisayar ağlarını daha verimli hâle getirmek için saldırılara karşı çözüm üretebilecek, karşılaşılan sorunlara önce veya sonra hızlı bir şekilde müdahale edebileceksiniz.

ÖĞRENME FAALİYETİ-1

AMAÇ

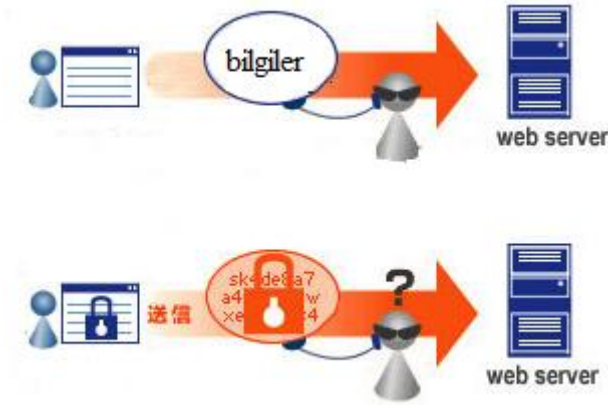
Bu faaliyet sonunda ağ güvenliğine olabilecek muhtemel saldırıları öğrenecek ve bu saldırılara karşı güvenlik önlemleri almayı öğreneceksiniz.

ARAŞTIRMA

- Bilgisayar ağların da karşılaşılan güvenlik tehditlerinin hangisi olduğunu öğreniniz.
- Ağ güvenliği için potansiyel riskleri belirleyerek bunların önlemlerinin nasıl alındığını öğreniniz.

1. AĞ İLETİŞİMİ TEHDİTLERİ

Bilgisayar ağlarının yaygınlaşması, *İnternet* aracılığı ile elektronik işletmelerin ortaya çıkması ve İnternet üzerinden ticaretin yaygınlaşmasıyla birlikte bilgisayar ağları oluşabilecek saldırılara karşı zayıflık göstermeye başlamıştır. Ağlardaki bu zayıflıklar iş uygulamalarında ürün kaybına ve şirketlerin ciddi anlamda zarar görmesine neden olmaktadır.



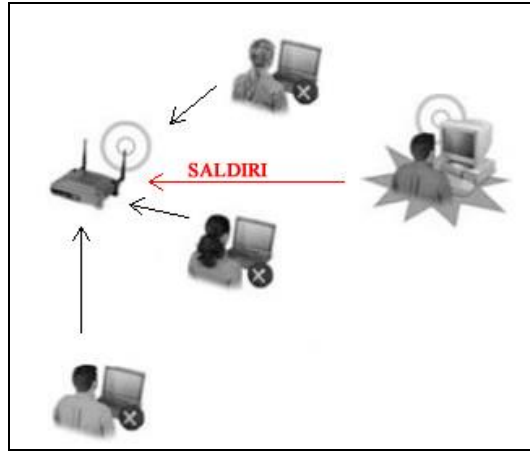
Resim 1.1: Ağ güvenlik önlemleri

İnternet ağı kişisel veya iş ilişkileri arasında bilgi akışını sağlayan ve düzenleyen bir iletişim aracı hâline gelmiştir. İnternet üzerinde bilgi kaybı olabilir veya gizlilik ihlal edilebilir. İnternet üzerindeki bu tür güvenlik açıklıkları kullanıcıları İnternete karşı güvensizleştirebilir. Bu sorun da web tabanlı şirketler için büyük risk olur. Bu tür güvenlik açıklıklarına karşı önlem almak kişisel kullanıcılar ve şirketler için gündeme gelmiştir.

1.1. Ağ Saldırı Riskleri

Kablolu veya kablosuz tüm bilgisayar ağları günlük kullanımda önemli bir yer tutmaktadır. Bilgisayar sektöründe çalışanlar, zamanın çoğunu bilgisayar başında geçirmektedir. Aynı zamanda bireyler ve kuruluşlar da bu sektörde çalışanlar gibi e-posta, düzenleme, dosya yönetimi, hesaplama gibi farklı işlevler için bilgisayarları ve ağlarını kullanmaktadır. Güvensiz bir ağda yetkisiz bir kişinin saldırısı yüksek maliyetli ağ kesintilerine yol açabilir.

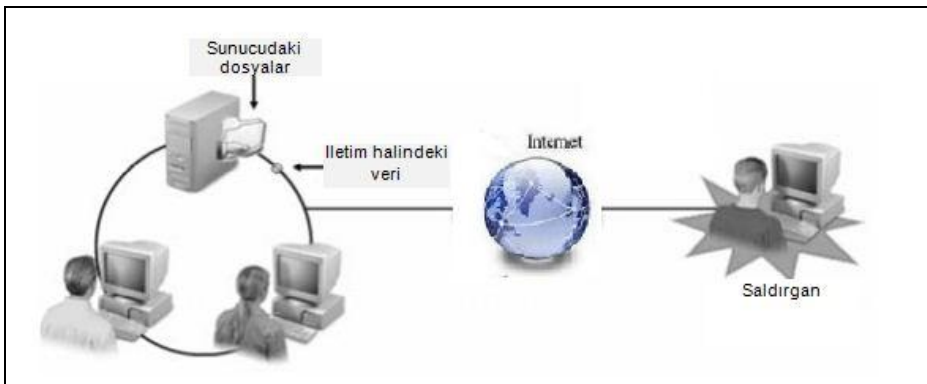
Saldırıcıyı gerçekleştirenler, yazılımın zayıflıkları, kullanıcı adına ve bu kullanıcıya ait parolayı tahmin etme ve donanım saldırıları gibi daha düşük düzeyli teknik yöntemlerle kolayca ağa erişim kazanabilir.



Resim 1.2: Ağ Saldırıları

1.1.1. Bilgi Hırsızlığı

Bilgi hırsızlığı izinsiz ağa erişimin, korumalı ağ bilgilerini elde etmek amacıyla kullanıldığı bir saldırıdır. Saldırgan, bir sunucuda veya bilgisayarda, daha önce kimlik doğrulaması için çaldığı bilgileri kullanabilir ve dosyalarda saklanan verileri okuyabilir. Saldırgan, ağ iletişimini izleyen ve veriyi yakalayan bir aygıt veya program olan, donanım veya yazılım tabanlı paket yoklayıcı kullanarak ağ ortamında geçiş hâlindeki veriyi çalabilir.



Resim.1.3: Bilgi hırsızlığı

Bu tür yapılan bilgi hırsızlığı yasadık olarak ÷lkemizde suç kabul edilmektedir. Tescilli bilgilerin çalınması, bilgisayar kullanarak ekonomik dolandırıcılık, bilgi veya ağların sabotajı Türkiye Cumhuriyeti kanunlarında suç kabul edilmektedir.

1.1.2. Kimlik Hırsızlığı

Kimlik hırsızlığı, kişinin izni olmadan kişisel bilgilerinin elde edilmesidir. Kimlik hırsızlığını kullanarak kişinin kredi kart numarası, ehliyet numarası, vatandaşlık numarası, İnternet bankacılığı bilgileri, e-posta şifre parolası ve önemli diğerk kişisel bilgilerin bir başkası tarafından çıkar sağlamak amacı ile yapılan dolandırıcılık türüdür. TCK'ye göre bu suç sayılmaktadır.



Resim 1.4: Kimlik hırsızlığı

Kimlik hırsızlığına uğranılmış ise bu birkaç yoldan anlaşılabilir:

- İzinsiz çevrim içi satın almalar yapıldığında,
- Kişi üzerinden çeşitli kurumlarda kredi veya telefon hattı başvuruları sonucu borçlanma bilgileri geldiğinde,
- Kişinin bilgi dahilinde olmadan sosyal paylaşımlar olduğunda.

Bu gibi durumlarda adli mercilere başvurmak gerekmektedir.

1.1.3. Veri Kaybı ve Veri Kullanma

Kişisel bilgisayarlar ve işletmelerde kullanılan bilgisayarlarda veriler elektronik ortamda saklanmaktadır. Bu verilerin erişilemez veya kullanılamaz hâle gelmesine veri kaybı adı verilmektedir. Veriler ağdaki bilgisayarlar üzerinde saklanabilir veya yedeklenebilir. Herhangi bir bilgisayar ağına gönderilen veri, o veriyi almaya yetkisi olmayan kişilerce ele geçirilebilir. Bu kişiler iletişimi gizlice gözetleyebilir ya da gönderilen bilgi paketini değiştirebilir. Bunu birçok metod kullanarak yapabilir. Örneğin, bilgi iletişimde bir alıcının IP numarasını kullanarak sanki o alıcymış gibi gönderilen verileri istediği gibi kullanabilir. Veya Üniversitelerin sistemlerine izinsiz bir giriş yaparak öğrenci not bilgisini geçer bir nota çevirmek gibi.

1.1.4. Hizmet Aksatma

Kişisel veya işletmelerdeki kullanıcıların yasal haklarını kullanmalarını engelleme olarak tanımlanabilir. Ağ haberleşmesinde kullanıcı adı ve parolasını kullanamaması, kullanıcıların web hizmetine bağlanamaması gibi durumlarda ağa dışarıdan müdahale olduğu anlaşılabilir.

1.2. Ağ İletişim Tehditleri

Bilişim teknolojilerindeki gelişmeler kullanıcılara büyük kolaylık sağlarken aynı zamanda pek çok tehdidi de beraberinde getirmektedir. İletişim ağlarında ki güvenlik açıkları kullanıcıların sisteminin ele geçirmekten öte kişisel bilgileri ve büyük firmaların gizli bilgilerini ele geçirilmesine ve bu sayede maddi kazançlar elde etmeye yönelik olmaya başlamıştır. Yeni nesil tehditler kullanıcılardan, güvensiz ağlardan kaynaklanabilir.

İnternetin genişlemesi ile beraber ağ uygulaması da beklenmedik şekilde genişlemiştir. Bu gelişmeyle birlikte ağ kurulumu işletmeye alındıktan sonra ağ yönetimi ve ağ güvenliği büyük önem kazanmıştır. Çünkü İnternete bağlı ağ sistemleri arasında dolaşan hiçbir veri gerekli önlemler alınmadığı takdirde güvenli değildir. Ağın güvenilir biçimde çalıştırılması anahtar sözcük konumuna gelmiştir. Çünkü ağın günümüz teknolojisi ile kurulumu çalıştırılmasıyla iş bitmemekte esas iş ağ performansının ve güvenilirliğinin sağlanmasında bitmektedir.

Genellikle ağ yapısına yapılan saldırıların çoğu iç ağdan gelir. Ağa açılan bilgisayarın verdiği hizmete göre ne tür saldırıya uğrayacağı ve saldırı türleri de ortaya çıkabilir. Ağa yapılan saldırılar donanıma veya yazılıma yönelik olabilir. Donanıma yönelik saldırılarda veri depolama kaynaklarına veya ağ cihazlarına yönelik olabilir. Yazılıma yönelik saldırılar ise kullanıcı verilerine erişim sağlamak için olabilir.

Potansiyel saldırı kaynakları, bilgisayarın bağlı olduğu geniş ağ üzerinden, *İnternet* bağlantısı üzerinden, modem havuzu üzerinden olabilmektedir.

1.2.1. Haricî ve Dâhili Tehditler

Harici tehditler, ağ dışında çalışan kullanıcılardan gelir. Bu kişilerin bilgisayar sistemlerine veya ağa yetkili erişimi bulunmamaktadır. Harici saldırganlar, ağa saldırılarını genellikle *İnternet* üzerinden, kablosuz ağlardan veya çevirmeli erişim sunucularından gerçekleştirir. Bu saldırılar maddi ve manevi zarara yol açar ve engellemek için güvenliğin artırılması gerekir.

İstemci-sunucu ortamında ağ yöneticileri çok farklı bir savaşın içindedir. Ağlarındaki her erişim noktasından saldırılara açıktır. İnternet çok sayıda sistemin birbirine bağlanmasını sağlayarak kendine özgü problemleri de beraberinde getirmiştir.



1.5: Harici tehdit saldırısı

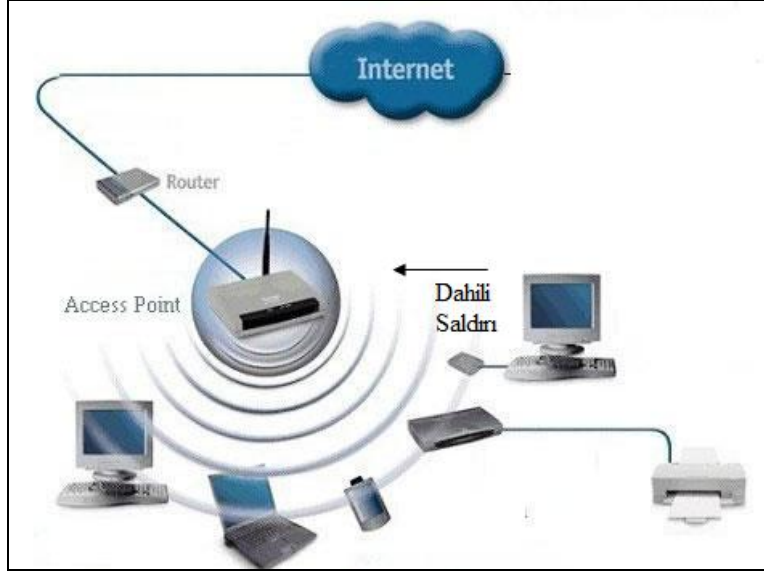
Dâhili tehditler ise; bir kullanıcının hesabı üzerinden ağa yetkisiz erişimi olduğunda ya da ağ ekipmanına fiziksel erişimi olduğunda gerçekleşir. Dâhili saldırgan, ilkeleri ve kişileri tanır. Bu kişiler genellikle hangi bilgilerin ve savunmasız olduğunu ve bu bilgileri nasıl elde edebileceğini bilir. Fakat, dahili saldırılar her zaman kasıtlı olmaz. Bazı durumlarda, dahili bir tehdit, ağ dışındayken bilmeden dahili ağa virüs veya güvenlik tehdidi getiren güvenilir bir çalışandan da gelebilir.

Güvenlik, dâhili ağlarda da önemli bir konudur. Firma çalışanları bazen veri hırsızlığı yapabilir ya da sisteme virüs bulaştırabilir.

Bir işletmedeki bazı çalışanlar, ağa bağlanmak için kullandıkları şifre, kötü niyetli çalışanlar (cracker) tarafından tahmin edilebilir şekilde seçerlerse bu bir güvenlik açığı oluşturur. Veya yalnızca merkezde bir güvenlik duvarı ile korunan ve bu merkeze özel kiralık devre ile bağlı bulunan bir şubede, herhangi bir kullanıcının telefon hattı ile *İnternete* bağlanması da bir güvenlik açığı oluşturabilir.

Bazı firma çalışanları da yanlışlıkla *İnternette* ya da floppy diskten bir belge yüklerken bilgisayara virüs bulaştırabilir ve kendi bilgisayarına bulaştırdığı virüsün farkına varmadan ağ içindeki diğer bilgisayarlarla bilgi alışverişi ile bu virüsü tüm ağa yayabilir. Bu soruna karşı alınabilecek önlem, tüm bilgisayarlara virüs koruma programı yüklemek ve bir belge yüklerken ekrana uyarı mesajları gelmesini sağlamaktır.

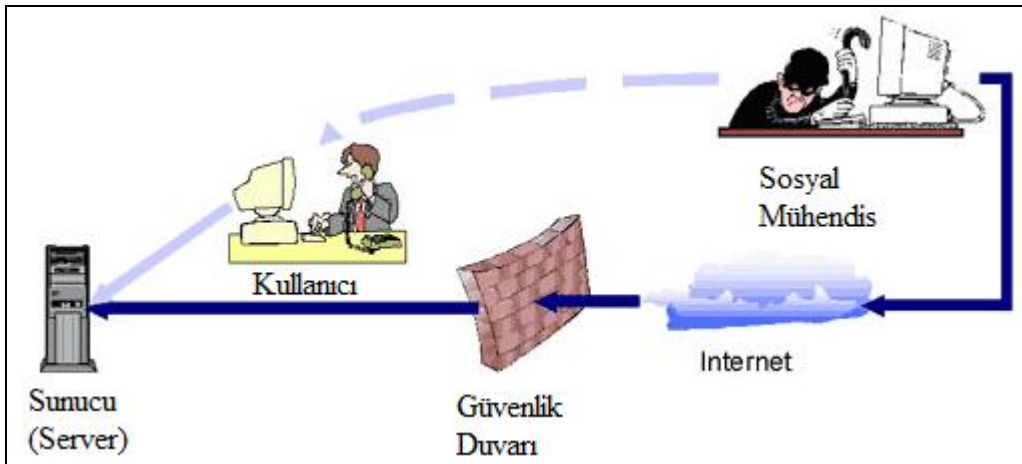
İşletmede çalışan meraklı kullanıcılar casus gibidir. Bu kullanıcı diğer çalışanlarla arasındaki rekabet nedeniyle, erişim yetkisine sahip olmadığı birtakım gizli bilgilere ulaşmaya çalışır. Mesajlara ya da maaş bilgilerine erişmek masum olabilir ancak önemli ve gizli finansal bilgilere ulaşmak, o şirket için büyük tehlike oluşturabilir.



Resim 1.6: Dâhili tehdit saldırısı

1.3. Sosyal Mühendislik

Sosyal mühendislik, insanlar arasındaki iletişimdeki ve insan davranışındaki modelleri açıklıklar olarak tanıyıp bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan müdahalelere verilen isimdir. Sosyal mühendis, kendisini sistem sorumlusu olduğunu söyleyerek kullanıcının şifresini öğrenmeye çalışmak veya teknisyen kılığında kurumun içerisine fiziksel olarak sızmak veya çöp tenekelerini karıştırarak bilgi toplamak gibi değişik yollarla yapılabilir. Kurum çalışanları kimliğini kanıtlamayan kişilere kesinlikle bilgi aktarmamalı, iş hayatı ile özel hayatını birbirinden ayırmalıdır. Kurum politikasında bu tür durumlarla ilgili gerekli uyarılar yapılmalı ve önlemler alınmalıdır.



Resim 1.7: Sosyal mühendislik

İnsan faktörü içermeyen bir bilgisayar sistemi yoktur. Güvenlik zincirindeki en zayıf halka insandır.

Sosyal mühendislikte süreç;

- Bilgi toplama,
- İlişki kurma,
- İstismar etme,
- Uygulama olarak sıralanabilir.

Sosyal mühendislikte en yaygın kullanılan tekniklerden üçü şunlardır: sahte senaryo uydurma, oltalama (phishing) ve sesle oltalama (vishing).

1.3.1. Sahte Senaryo Uydurma

Genellikle telefonla iletişim üzerinden gerçekleşen bir yöntemdir. Saldırganın amacına ulaşmak için sahte bir senaryo oluşturması ve bu senaryonun satırları arasından saldırılanın erişimindeki hassas bilgiye (bir sonraki adımda kullanmak üzere kişisel bilgiler ya da şifreler, güvenlik politikaları gibi erişim bilgileri) ulaşması şeklinde gelişir. Telefondaki işlemlerde yetkilendirme için ihtiyaç duyulan bilgiler genellikle başka kanallardan erişilebilir bilgiler (kimlik numarası, doğum tarihi vb.) olduğu için sahte senaryolar uydurmak ve istenen bilgileri elde etmek çoğunlukla uygulanabilir bir saldırı yöntemi olmaya devam etmektedir. Saldırganın senaryonun ana hattı dışına çıkabilecek durumları da göz önüne alıp hazırlık yapması, başarı oranını artıran bir etkidir.

1.3.2. Oltalama (Phishing)

Kimlik avcısının geçerli bir dış kuruluşu temsil ediyor gibi davrandığı bir sosyal mühendislik biçimidir. Genellikle e-posta üzerinden hedef bireyle (phishee) iletişim kurar. Kimlik avcısı, kullanıcıları kandırmak ve güvenilir bir kurumdan aradığını kanıtlamak için parola veya kullanıcı adı gibi bilgilerin doğrulanmasını isteyebilir.

1.3.3. Sesle / Telefonla Oltalama (Vishing)

Kimlik avcılarının, IP üzerinden ses (VoIP) uygulamasını kullandığı yeni bir sosyal mühendislik biçimidir. Sesle oltalamada, güvenilir bir kullanıcıya geçerli bir telefon bankacılığı hizmeti gibi görünen bir numarayı aramasını bildiren sesli mesaj gönderilir. Daha sonra kullanıcının yaptığı aramaya bir hırsız tarafından müdahale edilir. Doğrulama için telefonda girilen banka hesap numaraları veya parolalar çalınır.

1.4. Saldırı Yöntemleri

Saldırıları ağ üzerinden olacağından ağa bağlı cihazlar her zaman saldırıya açık durumdadır. Saldırganlar ağ üzerinden hedef makinaya ulaşarak yazılım veya donanıma zarar vermek isteyebilir. Bunun yanı sıra bir işletmenin ağına ulaşarak veritabanındaki verilere erişebilir, değiştirebilir veya silebilir. Saldırgan ağın *Internet* bağlantısını kesebilir. Hedef makinaya truva tı gibi program yükleyerek kullanıcıyı takibe alabilir. Aynı zamanda saldırıya uğrayan ağa girebilmek için farklı yöntemler kullanılabilir.

1.4.1. Hizmet Reddi (Denial of service–DoS)

Hizmet reddi (Denial of service-DoS) hizmet aksatma amaçlı bir saldırı çeşitidir. Bir sisteme yapılan düzenli saldırılar sonucunda sistem çalışamaz ve hizmet veremez hâle gelebilir. Ayrıca DoS saldırılarıyla hedef sisteme ait kaynakların tüketilmesi de amaçlanır. Bir kişinin bir sisteme düzenli veya arka arkaya yaptığı saldırılar sonucunda hedef sistemin kimseye hizmet veremez hâle gelmesi veya o sisteme ait tüm kaynakların tüketimini amaçlanır. Bu saldırı önemli sunucuların servis vermeyi durdurması gibi büyük sorunlara yol açabilir.

Bir DoS saldırısının yaptıkları;

- Network'ü trafik ile doldurmak böylece normal network trafiğini engellemek,
- İki makine arasındaki iletişimi bozar, bu sayede bir servise erişimi engeller,
- Özel birinin bir servise erişimini engeller,
- Servisin belirli bir sistem veya kişi ile iletişimini bozar.

Günümüzde en çok karşılaşılan yaygın DoS saldırısı şunlardır:

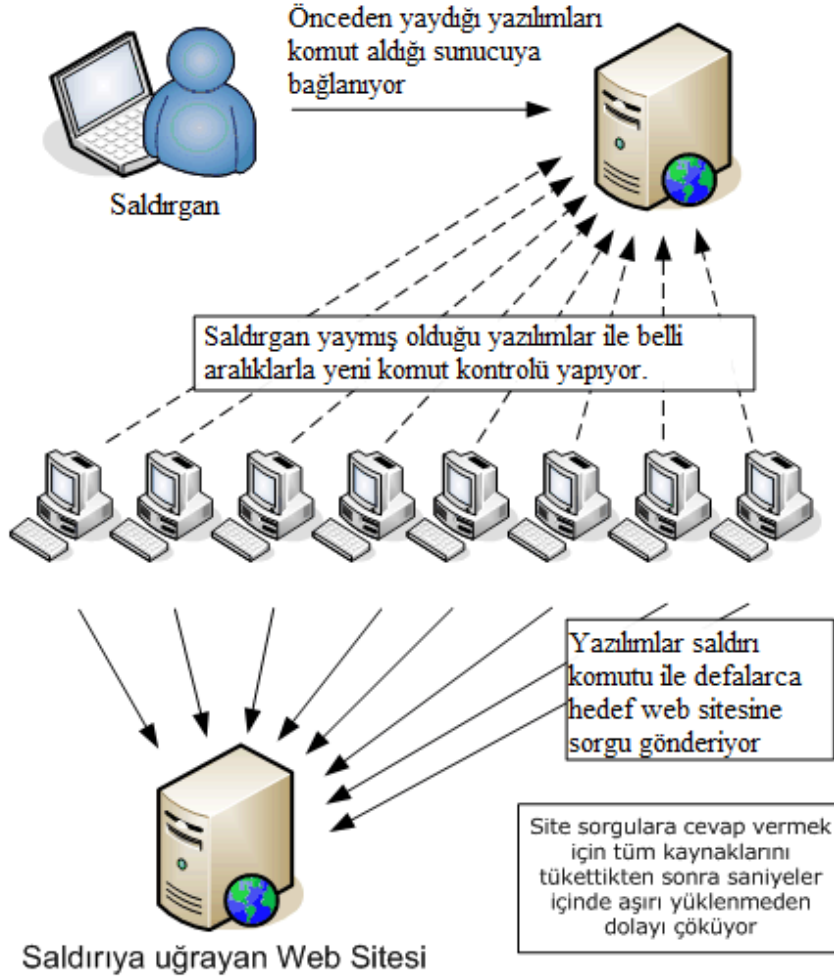
- **SYN (eşzamanlı) taşması:** Sunucuya gönderilen ve istemci bağlantısı isteyen paket taşmasıdır. Paketlerde kaynak IP adresleri geçersizdir. Sunucu bu sahte isteklere yanıt vermekle uğraşırken geçerli isteklere yanıt veremez.
- **Ping of death (Ölüm pingi):** Bir cihaza, IP tarafından izin verilen maksimum boyuttan (65,535 bayt) büyük bir paket gönderilir. Bu tür saldırılar artık bilgisayar sistemleri üzerinde etkili değildir.

1.4.2. Dağıtılmış Hizmet Reddi ((Distributed Denial of Service–DDoS)

Dağıtılmış hizmet reddi (DDoS) saldırıları DoS saldırılarının farklı kaynaklardan yapılması ile gerçekleşir. Saldırganlar bazı yazılımlar tasarlayarak (Truva atı, solucan vb.) bu yazılımları *İnternet* kullanıcılarına e-mail ya da çeşitli yollarla yükleyerek geniş kitlelere yayar. Bu şekilde yetki elde ettikleri çok sayıdaki *İnternet* kullanıcılarının bilgisayarlarını istedikleri zaman istedikleri siteye binlerce sorgu göndermek için kullanır.

Saldırganın kontrolü altındaki onlarca bilgisayardan tek bir sunucuya binlerce sorgu göndermekte; bu da hedef makinenin band tüketmesine ya da tıkanmasına neden olmaktadır.

DDOS Saldırısının Yapısı



Resim 1.8: DDoS saldırı yapısı

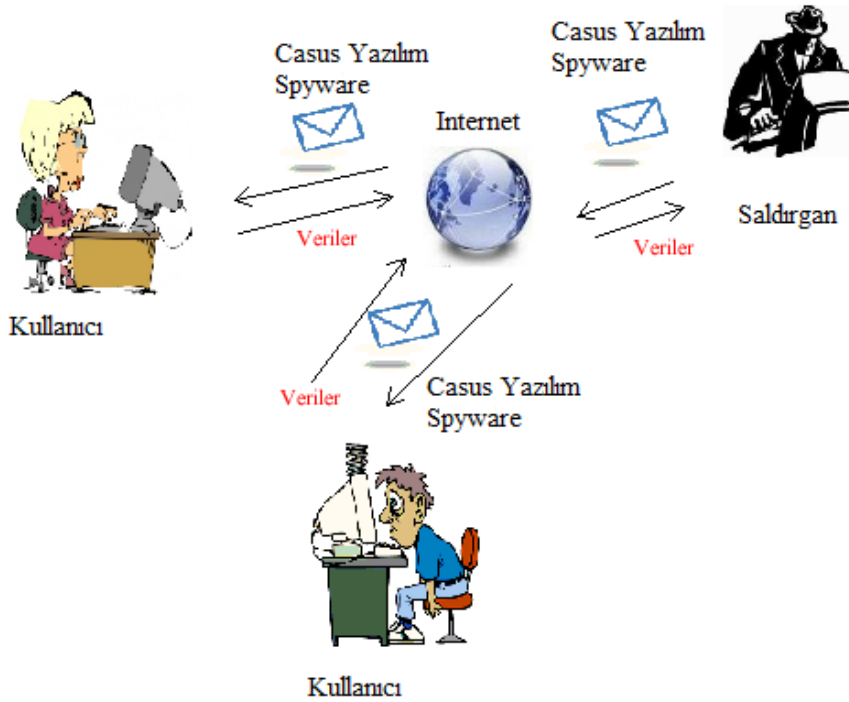
1.4.3. Deneme Yanılma

Ağ kesintilerine yol açan saldırıların tümü özel olarak DoS saldırıları değildir. Hizmet reddine yol açabilen başka bir saldırı türü de deneme-yanılma saldırısıdır. Deneme yanılma saldırılarında hızlı bir bilgisayar, parolaları tahmin etmeye veya bir şifreleme kodunun şifresini çözmeye çalışmak için kullanılır. Saldırgan, koda erişim kazanmak veya kodu çözmek için art arda hızlı şekilde çok sayıda olasılığı dener. Deneme yanılma saldırıları, belirli bir kaynakta aşırı trafik oluşması nedeniyle veya kullanıcı hesaplarının kilitlemesiyle hizmet reddine yol açabilir.

1.4.4. Casus Yazılımlar

Casus yazılım (spyware) kişisel bilgi toplama veya kullanıcının onayı alınmadan bilgisayarın yapılandırmasını değiştirme gibi belirli davranışları gerçekleştiren programlardır. Casus yazılımlar genellikle kullanıcının onayı alınmadan bilgisayara kurulur. Kurulduktan sonra kullanıcının İnternette gezinti bilgileri toplanabilir. Bu bilgiler reklam veren kişi ya da kuruluşlara veya İnternetteki diğer kişilere gönderilir ve parola, hesap numarası gibi bilgileri de içerebilir.

Casus yazılım genellikle bir dosya indirilirken, başka bir program yüklenirken veya bir açılır pencereye tıkladığında bilmeden yüklenir. Bilgisayarı yavaşlatabilir ve dâhili ayarları değiştirerek diğer tehditler için daha fazla zayıflık oluşturabilir. Ayrıca casus yazılımı bilgisayardan kaldırmak çok zor olabilir.



Resim 1.9: Casus yazılım tehditi

Casus yazılımlardan korunmak için;

- İşletim sisteminin güvenlik duvarı etkinleştirilmelidir.
- İşletim sistemi güncelleştirilmesi yapılmalıdır.
- Tarayıcının güvenlik ayarı yapılmalıdır.
- Anti-virüs yazılım kullanılmalıdır.
- İnternette dosya yüklenirken dikkat edilmeli ve dosya antivirüs taramasından geçirilmelidir.

1.4.5. İzleme Tanımlama Bilgileri

İzleme tanımlama bilgileri bir çeşit casus yazılımdır ancak her zaman kötü amaçlı değildir. Bir *İnternet* kullanıcısı web sitelerini ziyaret ettiğinde o kullanıcıya ilişkin bilgileri kaydetmek için tanımlama bilgisi (cookie) kullanılır. Tanımlama bilgileri, kişiselleştirme ve diğer zaman kazandıran tekniklere izin verdiği için kullanışlı ve aranan yazılımlar olabilir. Kullanıcının birçok web sitesine bağlanabilmesi için tanımlama bilgilerinin etkinleştirilmiş olması gerekir.

1.4.6. Reklam Yazılımları

Reklam yazılımı, kullanıcının ziyaret ettiği web siteleri temel alınarak kullanıcı hakkında bilgi toplamak için kullanılan yazılım biçimidir. Bu bilgiler daha sonra hedeflenmiş reklamcılık için kullanılır.

Reklam yazılımı genellikle "ücretsiz" bir ürün karşılığında kullanıcı tarafından yüklenir. Kullanıcı bir tarayıcı penceresini açtığında, Reklam yazılımı kullanıcının *İnternet*teki sörf hareketlerine dayanarak ürün veya hizmetlerin reklamını yapan yeni tarayıcı pencerelerini açabilir. İstenmeyen tarayıcı pencereleri ard arda açılarak, özellikle *İnternet* bağlantısı yavaş olduğunda *İnternette* sörf hareketini çok zor hale getirebilir. Reklam yazılımının kaldırılması çok zor olabilir.

1.4.7. Açılır Pencereleler

Açılır pencereler bir web sitesi ziyaret edildiğinde görüntülenen ek reklam pencereleridir. Reklam yazılımından farklı olarak, açılır pencereler kullanıcı hakkında bilgi toplamak için tasarlanmamış olup genellikle yalnızca ziyaret edilen web sitesiyle ilişkilidir.

Açılır pencereleri engellemek için tarayıcı özelliklerinden açılır pencere engelleyicisini etkinleştirmek gerekmektedir.

1.4.8. Spam

Bir e-postanın talepte bulunmamış, birçok kişiye birden, zorla gönderilmesi durumunda, bu e-postaya istenmeyen e-posta yani spam denir. Spamlar genellikle kitlesele veya ticari amaçlı olabilir.

Satıcılar bazen hedeflenmiş pazarlamayla uğraşmak istemez. Ürün veya hizmetlerinin birilerinin ilgisini çekmesi umuduyla e-posta reklamlarını olabildiğince fazla son kullanıcıya göndermek ister. Spam; *İnternet* hizmeti sağlayıcısını, e-posta sunucularını ve tek tek son kullanıcı sistemlerini aşırı yükleyebilen ciddi bir ağ tehdididir.

Spam listeleri genellikle arama sayfalarının taranması, tartışma gruplarının üye listelerinin çalınması veya web üzerinden adres aramalarıyla oluşturulur.

Spamlar ev bilgisayarlarını denetim altına almak için virüs, solucan ve Truva atı gibi yazılım tekniklerini kullanır. Bu bilgisayarlar daha sonra sahibinin bilgisi olmadan spam

göndermek için kullanılabilir. Spamler e-posta yoluyla veya anlık mesajlaşma yazılımıyla gönderilebilir.



Resim 1.10: Spam saldırısı

İnternetteki her kullanıcının yılda 3.000'den fazla spam e-postası aldığı tahmin edilmektedir. Spam, *İnternet* bant genişliğinin büyük miktarını tüketir ve bugün birçok ülkenin spam kullanımıyla ilgili yasa çıkarmasına neden olacak kadar ciddi bir sorundur.

1.5. Güvenlik Önlemleri

Ağ kaynaklarını iç ve dış tehditlerden korumak güvenlik önlemlerinin ilk sırasında yer almaktadır. Kurumlarda ağ kavramı iç ağ veya dış ağ ayrımı yapmaksızın kurumdaki bir kullanıcıya veya bilgisayara erişilmesi gündeme gelmiştir. Ağa bu şekilde erişilmesi güvenlik tehditleri de göz önüne alınması gereken bir konu olmuştur. Ağa güvenliği İnternette ya da yerel ağdan gelebilecek muhtemel saldırılara karşı korunması düşünülmektedir. Ağ üzerinden erişim kontrolü mevcut ağ kaynaklarını korumanın temel yoludur.

Bir güvenlik ilkesi geliştirildiğinde, bu ilkenin etkili olması için tüm ağ kullanıcılarının bu güvenlik ilkesini destekleyip izlemesi gerekir.

1.5.1. Tanımlama ve Kimlik Doğrulama İlkeleri

Bilgisayar ağlarında tanımlama belirli bir kimlik sahibinin gönderilen mesaja bu bilgiyi eklemesi ile ifade edilir. Kimlik doğrulama, sunucu bilgisayar tarafından belirli kullanıcıları tanımlamak ve kendi verilerine erişim izinlerini doğrulamak için kullanılan işlemdir. İletişimde bulunan bilgisayarların birbirlerinin kimliklerini doğrulamaları için aynı kimlik doğrulama metodunu kullanması gerekir. Tanımlama ve kimlik doğrulama işlemleri yerel ve geniş ağlarda kullanılabilir.

1.5.2. Parola ilkeleri

Bilgisayar ağlarında güvenlik önlemlerinde biri de ağa erişim için parola korumasıdır. İnternet erişimi için veya dosya sunucusuna erişim için güvenlik uzmanları parolalı koruma yöntemini geliştirmiştir. Parola ilkeleri, etki alanı hesapları veya yerel kullanıcı hesapları için de kullanılabilir.

1.5.3. Kabul Edilebilir Kullanım İlkeleri

Güvenlik tehditlerinin çoğu tanınmış web sitelerinden gelebilir. Web sitelerine erişimlerini yönetmeyen organizasyonlar risk altındadır. Ağ güvenlik filtreleme çözüm olarak kabul edilebilir. Web kategorisi organizasyonların dünya çapında kabul edilebilir kullanım ilkelerini kolaylıkla yönetmesini, casus yazılım, dolandırıcılık, klavye hareketlerini kaydetme ve diğer tehditleri içeren sitelere erişimi yasaklamasını sağlar.

1.5.4. Uzaktan Erişim İlkeleri

Uzaktan erişerek kullanılacak sistem başka bir binada veya kilometrelerce uzakta olabilir. Telnet, *İnternete* bağlı herhangi bir makineye uzaktan bağlanmak için geliştirilen bu yöntemin genel adıdır. Uzaktan Erişim yapılacak bilgisayarı bir uzaktan erişim sunucusu gibi çalışmak üzere yapılandırarak, uzak veya hareketli çalışanların kuruluşunuzun ağlarına bağlanması sağlanabilir. Uzak kullanıcılar, bilgisayarları ağa fiziksel olarak bağlıymış gibi çalışabilir.

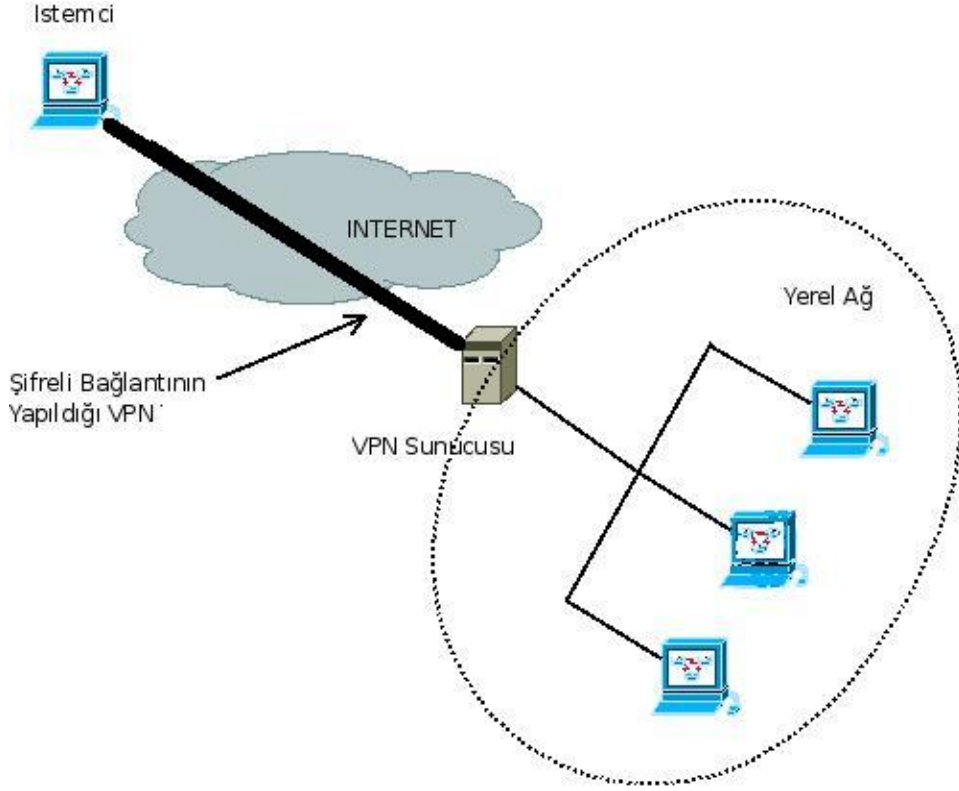
Genellikle yerel ağ bağlantısı üzerinden bağlanan bir kullanıcı tarafından kullanılabilen tüm hizmetler (dosya ve yazdırma paylaşımı, Web sunucusu erişimi ve ileti hizmeti dahil olmak üzere), uzaktan erişim bağlantısı ile etkinleştirilir. Örneğin, yönlendirme ve uzaktan erişim hizmetini çalıştıran bir sunucuda, istemciler sürücü bağlantıları kurmak ve yazıcılara bağlanmak için kullanılabilir. İşletim sistemi dahilinde ki uzaktan yardım iste uygulamasını kullanarak veya uzaktan erişim programlarını bilgisayara kurarak bilgisayara uzaktan erişim sağlanabilir.

Uzaktan erişim sağlanırken güvenlik önlemleri göz önünde bulundurulması gerekmektedir. Erişime izin verilecek bilgisayara parola koruma yapılarak güvenlik önlemi alınabilir.

1.5.5. VPN Bağlantıları

Ağ güvenlik önlemlerinden biri de VPN (Virtual Private Network-Sanal Paylaşımlı Ağ) kullanılmasıdır. VPN çalışma mantığı, aslında olmayan ama farklı hatlar üzerinden ki *İnternet* sistemleri, uydu bağlantıları, kablo net yapıları farklı noktada olan iki ağı aynı ağda çalıştırmak kullanılabilir. Örneğin, iki farklı ülkede iki ayrı ağ kurmak için VPN kullanılır. VPN kullanıcıya hem dosyalarını aynı ağda paylaşmasını hem de içerde çalışan programları veya e-posta programlarını VPN yazılımı ile güvenli şekilde yapacaktır.

VPN kullanarak yapılan her bağlantıda, veri paketlerinin her biri ayrı ayrı şifrelenerek gönderilir. Güvenliği sağlayan sadece verinin şifrelenmiş olması değil, ayrıca verinin geçtiği yol boyunca içeriğinin bozulmamış olması da önemlidir.



Resim 1.11: VPN bağlantısı

1.5.6. Ağ Bakım Yordamları

Ağ cihazı işletim sistemlerini ve son kullanıcı uygulamalarını güncelleme yordamlarını belirler.

1.5.7. Olay İşleme Yordamları

Güvenlik olaylarının nasıl işleneceğini açıklar.

UYGULAMA FAALİYETİ

Uygulamadaki ağ iletişimi tehditlerini belirleyip not ediniz.

İşlem Basamakları	Öneriler
➤ Olası ağ saldırılarını not ediniz.	➤ Ağ saldırıları konu başlığından yararlanabilirsiniz.
➤ Hizmet Reddi saldırısını neler yaptıklarını not ediniz.	➤ Saldırı Yöntemleri konu başlığından yararlanabilirsiniz.
➤ Casus Yazılımlardan korunma yöntemlerini not ediniz.	➤ Saldırı Yöntemleri konu başlığından yararlanabilirsiniz.
➤ Ağ saldırılarından korunmak için hangi güvenlik önlemlerinin kullanılabileceğini not ediniz.	➤ Güvenlik önlemleri konu başlığından yararlanabilirsiniz.

KONTROL LİSTESİ

Bu faaliyet kapsamında aşağıda listelenen davranışlardan kazandığınız beceriler için **Evet**, kazanamadığınız beceriler için **Hayır** kutucuğuna (X) işareti koyarak kendinizi değerlendiriniz.

Değerlendirme Ölçütleri	Evet	Hayır
1. Olası Ağ saldırılarını not edebildiniz mi?		
2. Hizmet reddi saldırısının neler yapabileceğini not edebildiniz mi?		
3. Casus yazılımlardan nasıl korunulacağını not edebildiniz mi?		
4. Saldırılarından korunulacak önlemleri not edebildiniz mi?		

DEĞERLENDİRME

Değerlendirme sonunda “**Hayır**” şeklindeki cevaplarınızı bir daha gözden geçiriniz. Kendinizi yeterli görmüyorsanız öğrenme faaliyetini tekrar ediniz. Bütün cevaplarınız “**Evet**” ise “Ölçme ve Değerlendirme”ye geçiniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

1. Aşağıdakilerden hangisi bir ağ saldırısı **değildir**?
A) Bilgi hırsızlığı
B) Veri Kaybı
C) Hizmet Aktarma
D) Veri Kullanma
2. Aşağıdakilerden hangisi sosyal mühendislik süreçlerinden **değildir**?
A) İstismar olma
B) Bilgi Toplama
C) İlişki kurma
D) Uygulma
3. Aşağıdakilerden hangisi DoS saldırısının yaptığı bir eylemdir?
A) Ağ güvenliğini sağlamak
B) Servisi sağlamak
C) İşletim sistemini durdurmak
D) Network trafiğini engellemek
4. Casus yazılımlardan korunmak için aşağıdakilerden hangisi yapılabilir?
A) Tarayıcı kullanılmalı
B) İşletim sistemi güncelleştirilmesi yapılmalı
C) Kablosuz bağlantı sağlanmalı
D) Web gezintisi iptal edilmeli
5. Aşağıdakilerden hangisi güvenlik önlemlerinden biri **değildir**?
A) Kimlik doğrulama
B) VPN bağlantı
C) Uzaktan kablosuz bağlantı
D) Parola İlkeleri

Aşağıdaki cümlelerin başında boş bırakılan parantezlere, cümlelerde verilen bilgiler doğru ise D, yanlış ise Y yazınız.

6. () Bir e-postanın talepte bulunmamış, birçok kişiye birden, zorla gönderilmesi durumunda, bu e-postaya istenmeyen e-posta yani spam denir.
7. () VPN kullanılarak yapılan her bağlantıda veri paketleri şifrelenmez.
8. () DDoS saldırıları DOS saldırılarının tek kaynaktan yapılması ile gerçekleşir.
9. () Reklam yazılımı, kullanıcının ziyaret ettiği web siteleri temel alınarak kullanıcı hakkında bilgi toplamak için kullanılan yazılım biçimidir.

10. () Kimlik hırsızlığı ile izinsiz ađa eriřimin, korumalı ađ bilgilerini elde etmek amacıyla kullanıldıđı bir saldırdır.

DEĐERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlıř cevap verdiđiniz ya da cevap verirken tereddüt ettiđiniz sorularla ilgili konuları faaliyete geri dđnerek tekrarlayınız. Cevaplarınızın tümü dođru ise bir sonraki öğrenme faaliyetine geçiniz.

ÖĞRENME FAALİYETİ-2

AMAÇ

Ağ güvenlik araçlarını kullanabilecek ve olası ağ saldırılarından ağı koruyabileceksiniz.

ARAŞTIRMA

- Ağ ortamına dışarıdan gelebilecek saldırılar neler olduğunu not ediniz.
- Ağ güvenliğini sağlamak için kullanılacak yazılımları not ediniz.

2. GÜVENLİK ARAÇLARI VE UYGULAMALAR

Gelişen teknoloji, bilgisayar sistemleri kurulumu oldukça kolay hâle getirmiştir. Teknoloji aynı zamanda, sistem kurulmasını da kötü amaçlı kişilerce yıkılmasını da kolay hâle getirmektedir. Bu nedenle “güvenlik” önemli bir sorun olarak karşımıza çıkmaktadır.

Bilgi güvenliği, özellikle e-ticaret ve e-devlet uygulamalarının yaygınlaşmasıyla birlikte oldukça önemli bir hâle gelmiştir. Bilginin güvenli bir şekilde iletilmesi, işlenmesi ve saklanması bilişim uzmanlarının başlıca görevlerinden birisi olmuştur. İletilen bilginin veya bilgiyi ileten sistemin gerekli güvenlik özelliklerini sağlayıp sağlamadığını test etmek ve denetlemek için ağ güvenliği test ve denetim araçları kullanılmaktadır. Bu araçlardan bazıları ücretsizdir, bazıları ise belirli bir ücretlendirmeye tabidir.

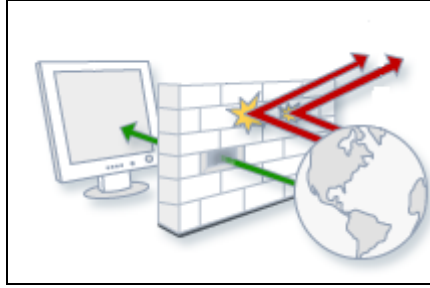
2.1. Güvenlik Duvarı

Ağ güvenliğini sağlayabilmek için bir ağ güvenlik duvarı (network firewall) kullanılır. Bir ağ güvenlik duvarı kullanarak ağı dış saldırılardan korunabilir, ağa gelen ve ağdan giden verileri denetlenebilir ve yönetilebilir, istenmeyen istemcilerin (client) İnternet bağlantısı kesilebilir mevcut İnternet bağlantısının bant genişliğini yönetilebilir.

Güvenlik duvarı kurulduğu konumda gelen ve giden ağ trafiğini kontrol ederek bilgisayarın ya da bilgisayar ağına yetkisiz veya istenmeyen kişilerin çeşitli yollardan erişim sağlamasını engellemeye yarayan yazılım veya donanımdır.

Güvenlik duvarları;

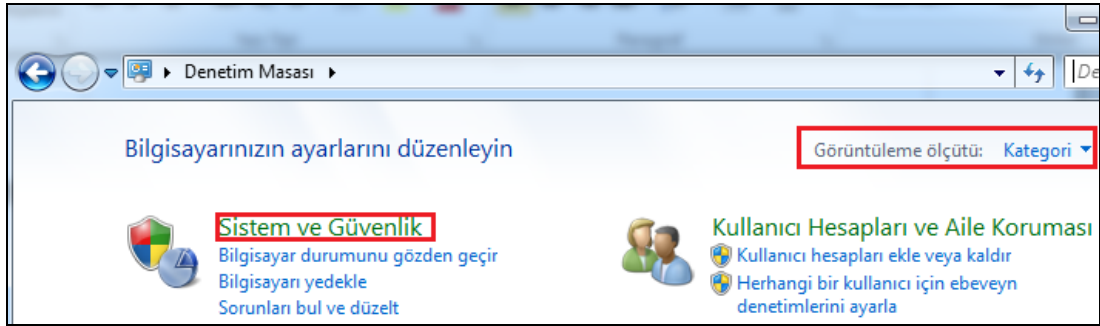
- Ev ve küçük ofislerde İnternet güvenliğini sağlamak amacı ile kullanılırken,
- Kurumsal olarak da genelde bilgisayar ağına erişim kontrolü amacı ile kullanılır.



Resim 2.1: Güvenlik duvarı

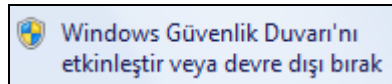
Güvenlik duvarı yazılımı işletim sistemi dahilinde bulunmakta veya özel bir program yüklenerek de güvenlik duvarı kullanılabilir. İşletim sistemi üzerindeki güvenlik duvarını açmak için;

- Başlat simgesine tıklanır ve Denetim Masası seçilir.
- Kategori görünümünde Sistem ve Güvenlik seçilir.



Resim 2.2: Sistem ve Güvenlik Seçilmesi

- Güvenlik Duvarı'na tıklanır.
- Ekranı gelen pencerede Güvenlik Duvarı'nı etkinleştir veya Devre Dışı Bırak bölümü seçilir (Güvenlik Duvarı açık ise kapatılabilir veya kapalı ise açılabilir.).



Resim 2.3: Güvenlik Duvarı Etkinleştirme

Güvenlik Duvarı donanım olarak ise yalnızca güvenlik duvarı özelliği ile kullanılan geniş bantları karşılayabilen güvenlik çözümleridir. Ayrı bellek ve işlemci kullandığı için oldukça hızlıdır. Genelde yüz bilgisayar ve üzerindeki ağlarda tercih edilir. Çalışma mantığında veriyi ağa girmeden karşılamak olduğu için iç ağda herhangi işlem yapmadan veri bloklanabilir. DoS saldırıları gibi güvenlik problemlerine çözüm sunar.



Resim 2.3: Firewall (Güvenlik Duvarı) donanımı

2.2. Spam Filtresi

Spam Filtreleri, sunucuya gelen e-postaları bir süzgeçten geçirerek istenilmeyen e-postaları tespit eden ve kullanıcının gelen kutusuna (inbox) düşmesine engel olan programlardır. E-postalar spam filtrelerinde birçok kural ve kriterlere göre değerlendirilir. Her bir kural spam filtresi tarafından belirlenmiş olan belli puana sahiptir. Başlangıçta sıfır olan puan spam filtrelerinin kurallarına uyan her hangi bir eşleşme görüldüğünde bu puan toplam puana eklenir.

Spam filtrelerinin kontrol ettiği bazı kurallar;

- İçeriğin de ve başlıkta çok fazla ünlem işareti kullanmak,
- “Mutlaka okuyun.”, “Çok kolay zengin olun.”, “Hayatınızın fırsatı” gibi spam çağrıştıran ifadeler kullanmak,
- Başlıkta ve içerikte çok fazla ya da bütün kelimelerin büyük harflerden oluşması,
- İçeriğin çok fazla parlak kırmızı, yeşil gibi renkler kullanmak,
- E-postanın temiz olmaması, özellikle MS Word gibi uygulamalardan yaratılması,
- İçeriğinin sadece koca bir resimden oluşması, hiç yazıya yer verilmemesi,

Örnek olarak spam filtreleri e-posta içeriğinde ve başlıklar da “Bedava”, “Ücretsiz” gibi kelimelerin olup olmadığını kontrol eder. E-postada bu kelimeleri gördükleri her seferinde bir puan atar. Bütün kuralların kontrolünden sonra toplam bir “Spam Score” puanını oluştur ve bu skor, spam filtresi tarafından tanımlanmış limit puandan fazla ise e-posta istenmeyen (junk) klasörüne gönderilir veya alıcıya ulaşamaz. E-posta adreslerinde

spam olarak algılanan mailler genellikle **Gereksiz Posta** (Junk Mail) klasöründe belli bir süre tutulur.

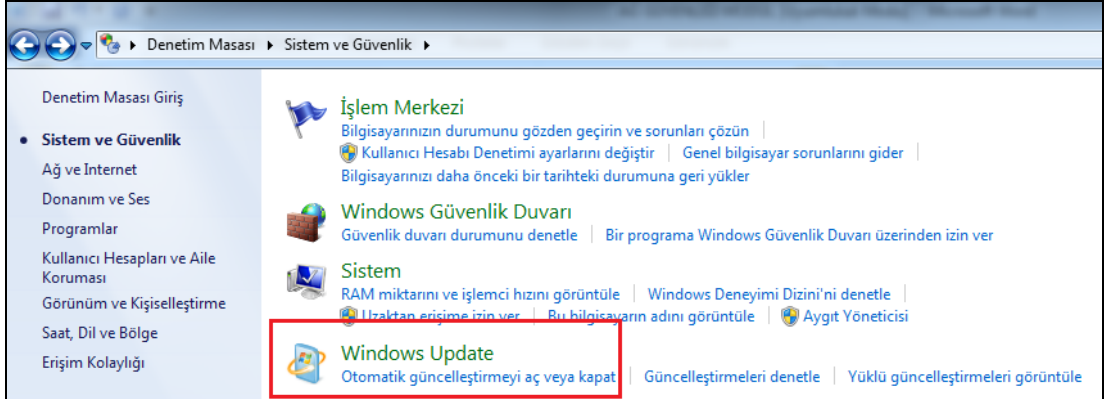
2.3. Yamalar ve Güncellemeler

Yazılımlarda zaman zaman hatalar veya eksiklikler keşfedilir. Bilgisayar sistemlerini dışarıdan gelecek saldırılara (virüs ya da bilgisayar korsanı) açık hâle getiren bu zaafllara güvenlik açıklığı denir ve ancak yazılımlar güncellenerek kapatılabilir. Bu açıklıkları giderme amacı ile yazılım ve işletim sistemleri geliştiricileri yeni sürümler, yazılım yamaları, ya da hizmet paketleri yayımlar.

Geliştirici firmaların politikalarına göre farklı işletim sistemleri ve programlar ister otomatik (*Internet* bağlantısı üzerinden programın kendisi tarafından) ister elle (kullanıcı tarafından) güncellenebilir.

İşletim sisteminde güvenlik yaması (security patch) üründeki güvenlik açıklığını kapatır. Güncelleme (update) ise işletim sistemindeki bir problemi giderir. Güvenlik yamalarını üreticinin *Internet* adresinden indirmek ve bilgisayara kurmak en güvenli yoldur.

İşletim sisteminin otomatik olarak güncelleştirilmesi istenirse Denetim Masası'ndan **Sistem Güvenlik** sekmesi seçilir. Sistem güvenlik penceresinde **İşletim sistemi güncelleştirmesini aç / kapat** seçilir. Update kısmında güncelleştirmeler el ile de denetlenebilir.

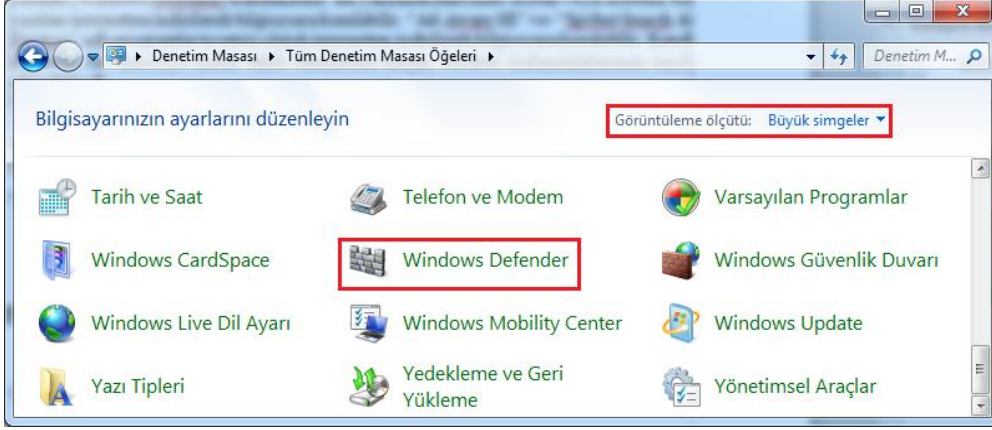


Resim 2.4: İşletim sistemi güncelleştirme

2.4. Casus Yazılımlardan Korunma Yazılımları

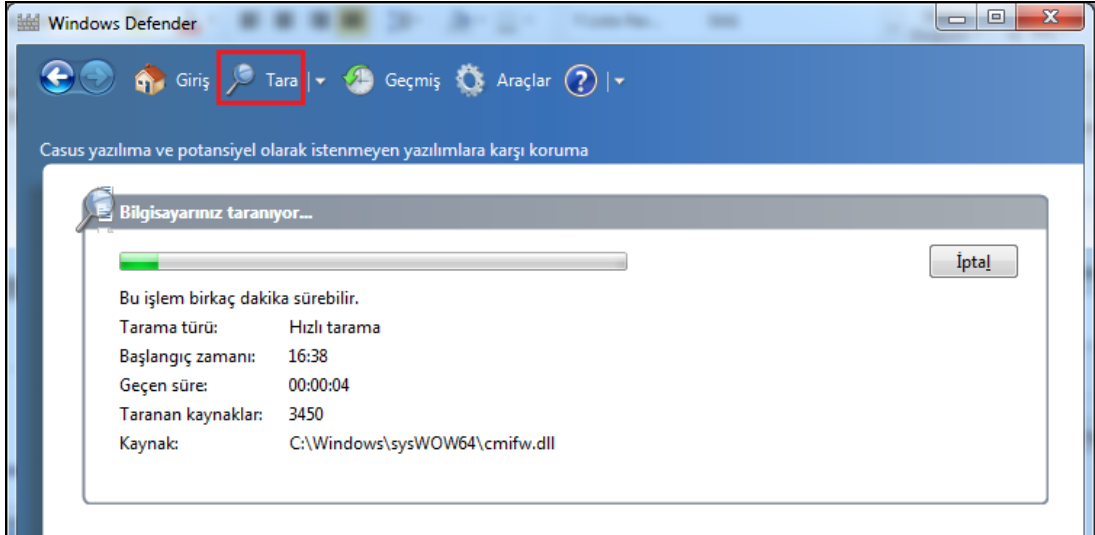
Casus yazılımlar, bilgisayar kullanıcılarının gündemine artarak giren bir problem olmuştur. Casus yazılımlardan bilgisayarı korumak için işletim sistemi dâhilinde olan yazılım (Windows Defender) kullanılabilir. Bu yazılımın haricinde ücretli veya ücretsiz bir yazılım İnternette indirilerek bilgisayara kurulabilir. “Ad-Aware SE” ve “Spybot Search & Destroy” adlı programlar ücretsiz olarak İnternette indirilerek bilgisayara kurulabilir. Kendi başlarına bir dereceye kadar etkili olmalarına karşın, beraber kullanıldıklarında hayli etkindir.

İşletim sisteminde bulunan korunma yazılımına ulaşmak için **Başlat** simgesine tıklanır ve **Denetim Masası** seçilir. Denetim Masası penceresinde Görüntüleme Ölçütü Büyük Simgeler / Küçük Simgeler seçili iken Yazılım seçilir.



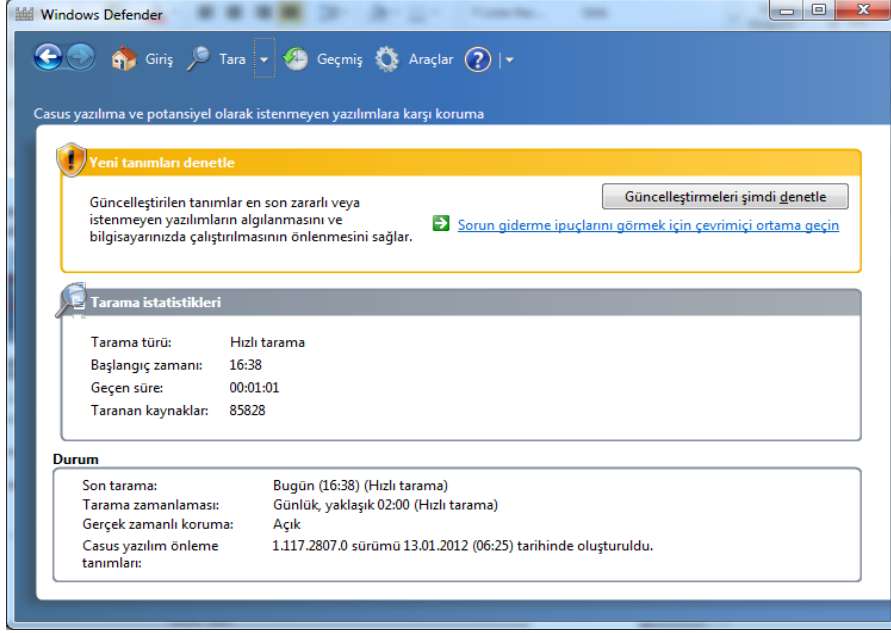
Resim 2.5: Denetim Masası, Windows Defender

Ekrana gelen pencerede **Tara** butonuna basılarak bilgisayarda ki casus yazılım taramasına başlanabilir.



Resim 2.6: Casus yazılım taraması

Tarama işlemi sonunda tarama istatistikleri ve tarama durumu görüntülenir.



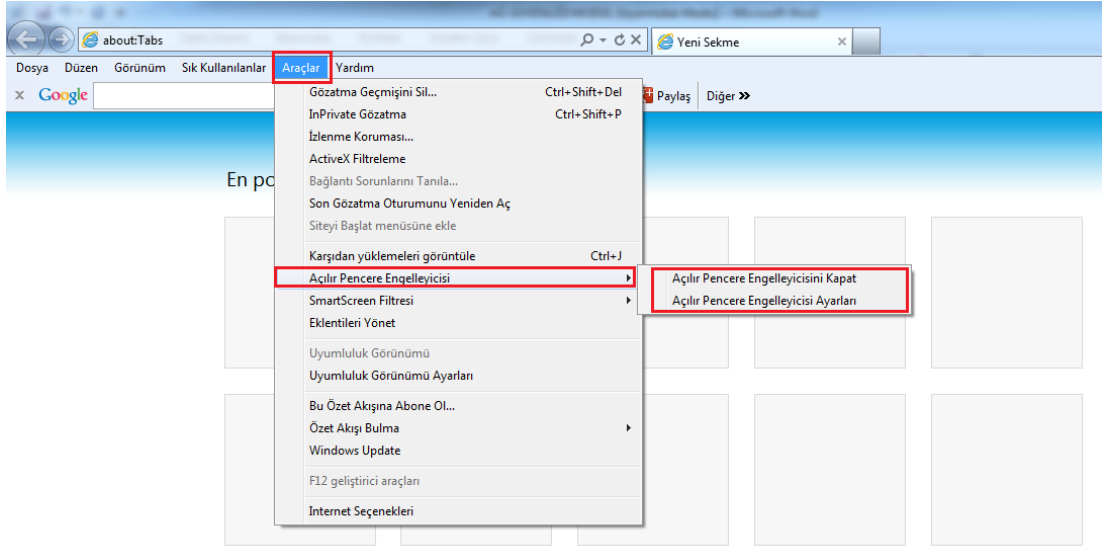
Resim 2.7: Tarama istatistikleri

2.5. Açılır Pencere Engelleyicileri

İstenmeden açılan pencereler, tarama sırasında kullanıcıya sormadan kendiliğinden açılan pencerelerdir. Boyutları değişebilir ama genelde ekranın tamamını kaplamaz. Açılır pencereleri engellemek için bilgisayarda kullanılan tarayıcı üzerinde ayarlamaları yapmak yeterli olur. İşletim sisteminin üzerindeki tarayıcı veya kullanıcının kendisinin bilgisayara kurduğu tarayıcılarda bu özellikler bulunmaktadır. Açılır pencereleri engellemek için öze programlarda kullanılabilir.

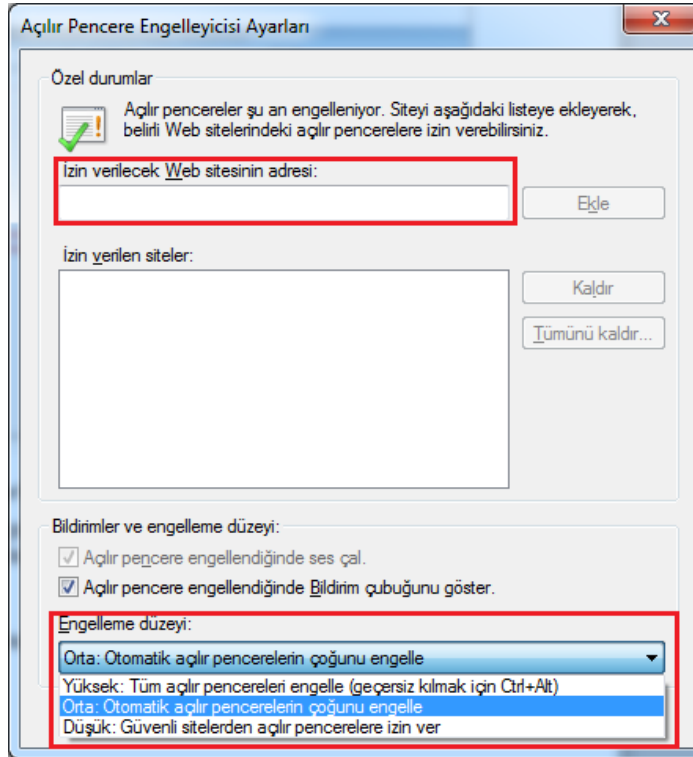
Açılır Pencere Engelleyicisi varsayılan olarak etkindir. Açılır Pencere Engelleyicisi ayarından bağımsız olarak, açılır pencerelerin boyut ve konumu üzerinde sınırlamalar bulunur. Açılır pencereler görüntülenebilir masaüstü alanından daha geniş olarak veya bu alanın dışında açılmaz.

İşletim sistemi üzerinde bulunan tarayıcıda açılır pencere engelleyicisini etkinleştirmek ya da ayarlarını değiştirmek için **Menü Çubuğu**'nda **Araçlar** menüsünden **Açılır Pencere Engelleyici** tıklanır.



Resim 2.8: Açılır Pencere Engelleyicisi

Açılır Pencere Engelleyicisi Ayarları penceresi kullanarak açılır penceresi olan *İnternet* sitelerinden izin verilecek olanları izinli listesine eklenebilir. Ayrıca engelleme düzeyi de bu pencereden ayarlanabilir.



Resim 2.9: Açılır Pencere Engelleyici Ayarları

2.6. Antivirüs Yazılımlar

Bilgisayar sistemlerinin düzgün çalışmalarını engelleyen, veri kayıplarına, veri bozulmalarına ve çeşitli yollarla kendisini kopyalayan kötü amaçlı yazılımlara virüs denir. Her geçen gün yeni virüsler çıkmakta veya var olanların özellikleri değiştirilerek tekrar piyasaya sürülmektedir. Virüsler; bilgisayar sistemlerinin çalışmasını aksatma ve bozmanın yanı sıra verilerin silinmesi veya çalınması gibi kötü amaçları gerçekleştirmek için hazırlanmaktadır.

Antivirüs bilgisayarı zararlı yazılımlardan korumak için hazırlanan güvenlik yazılımlarına denir. Antivirüs programları genel olarak zararlı programları bulup yok etmek ve bilgisayar kullanıcılarının tercihlerine göre farklı görevleri vardır. Örneğin, çoğu antivirüs otomatik görevleri vardır. Virüs ve zararlı kodlar bulunduğu kullanıcıya bu kodu içeren program için ne yapılması gerektiğini de sorar.

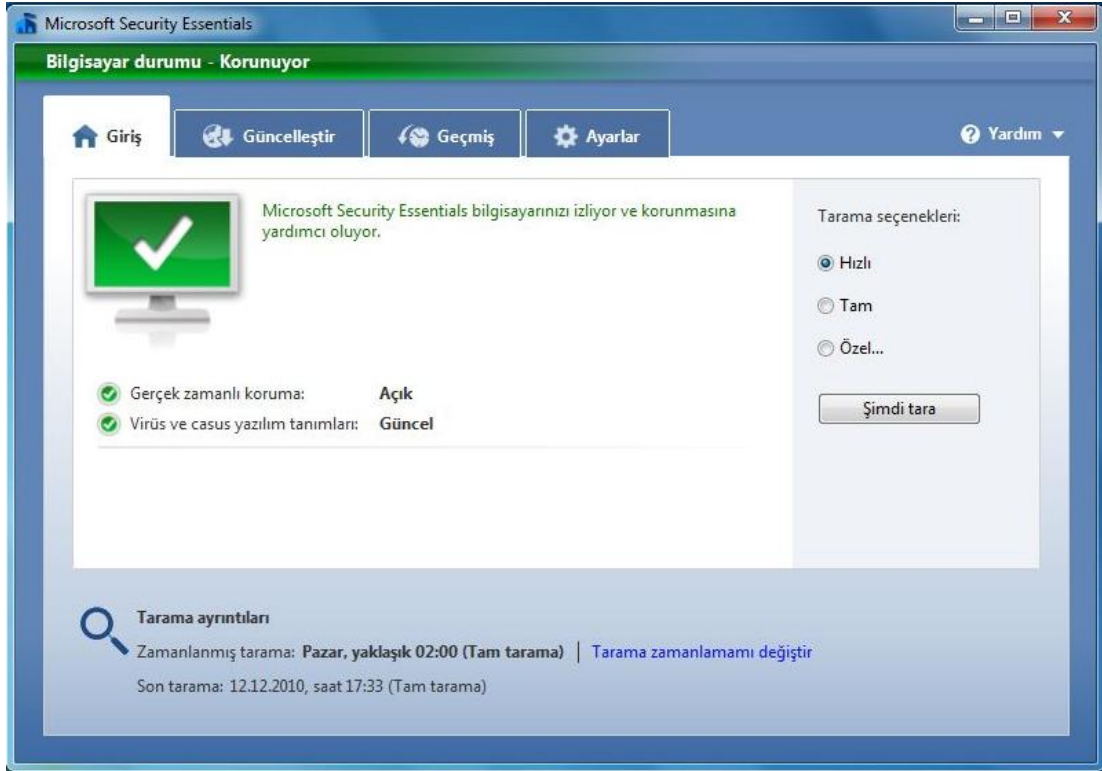
Bazı virüslerin verdiği zararlar geri dönüşümü mümkün olmayan hatalara neden olabilir, bu yüzden her bilgisayarda güncel ve lisanslı bir antivirüs programı bulunması gerekmektedir.

Antivirüs programları tek başlarına tam bir güvence sağlayamazlar bunun yanında, antispyware (casus yazılımlardan korunma), firewall (güvenlik duvarı) gibi güvenlik yazılımları da bilgisayara kurulmuş ve güncel tutuluyor olması gerekmektedir.

Bilgisayarda bulunan lisanslı işletim sisteminin sunduğu antivirüs programını işletim sisteminin *Internet* adresinden bilgisayara indirilerek bilgisayara kurulabilir. Antivirüs programları işletim sisteminde arka planda sessizce ve etkili şekilde çalışır ve bilgisayarda kesilmeler veya uzun bilgisayar bekleme süreleri olmadan kullanıcıya rahat bir kullanım sunulur. Çoğu antivirüs programının bilgisayara kurulumları basit, kullanımları kolaydır.

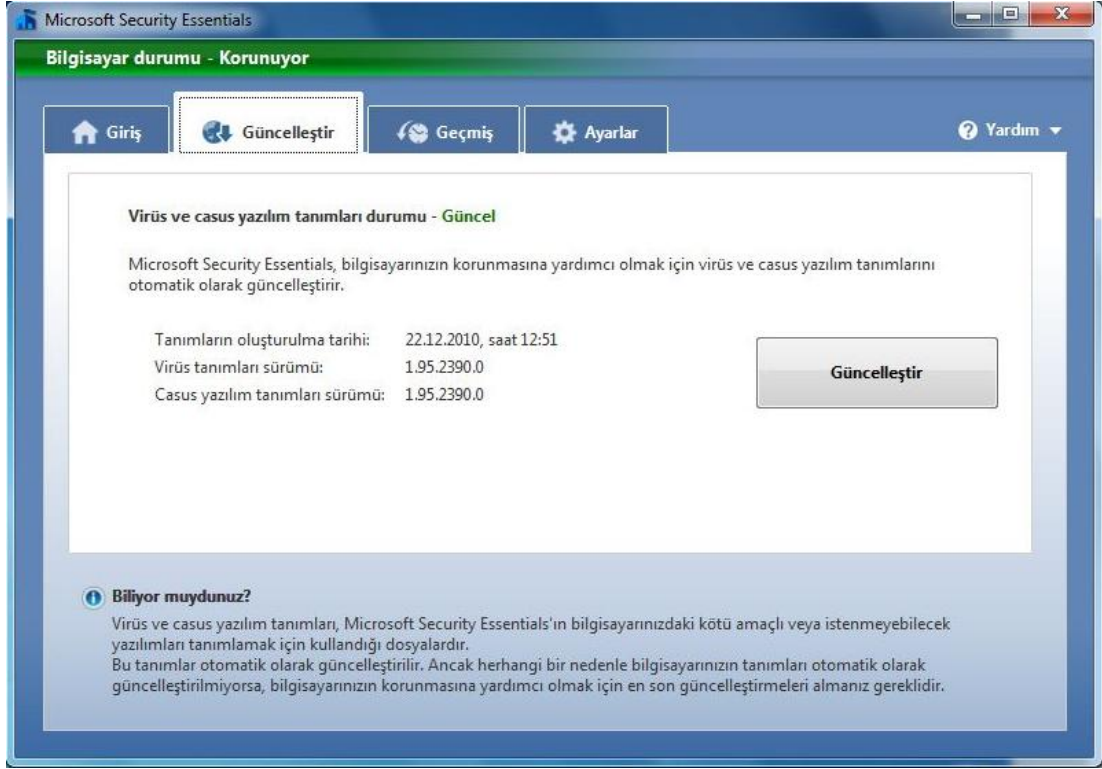
İşletim sisteminin sunduğu antivirüs programının kullanılması;

- Programın **Giriş** sayfasında **Şimdi Tara** butonuna basıldığında sistemi otomatik taranır. **Tam** seçeneği seçildiğinde bilgisayardaki tüm dosyalar taranır. **Özel** seçeneği işaretlediğinde ise açılan pencerede seçilen klasörler taranır.



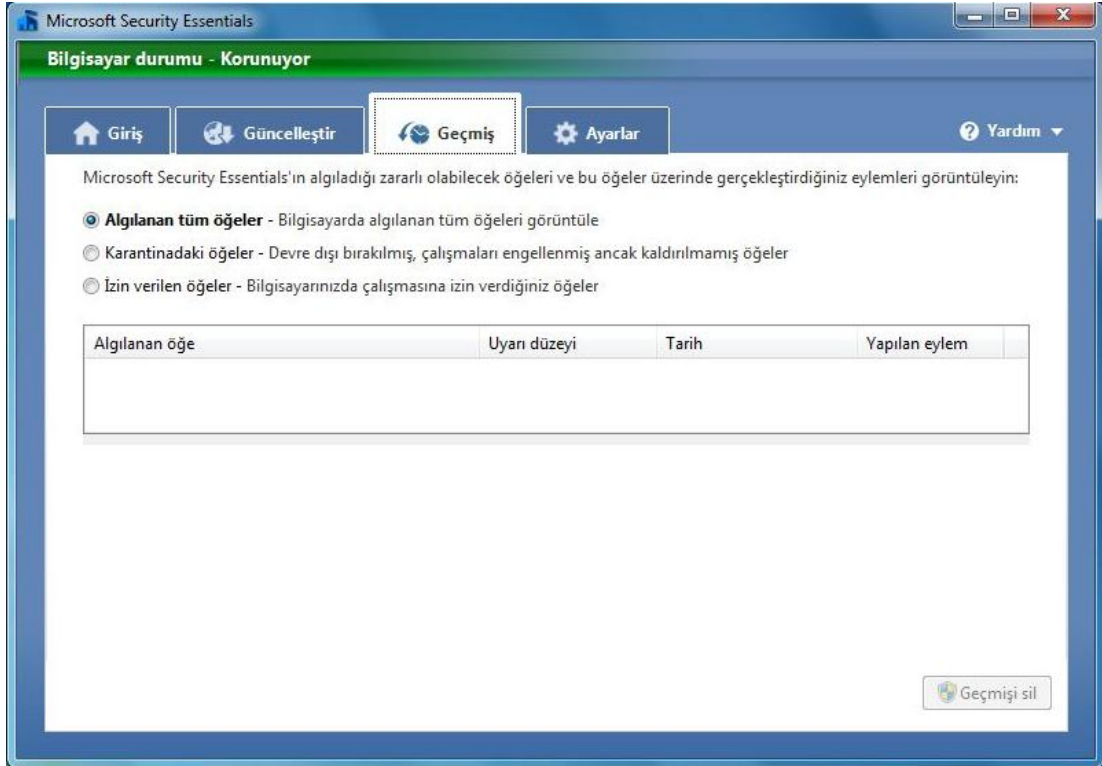
Resim 2.10: Antivirüs Programı Giriş Sayfası

- **Güncelleştirme** sayfasında antivirüs programının kullanıcı tarafından elle güncelleştirme yapması sağlanır. Güncelleme yapılabilmesi için bilgisayarda denetim masasında bulunan otomatik güncellemelerin açık olması gerekmektedir.



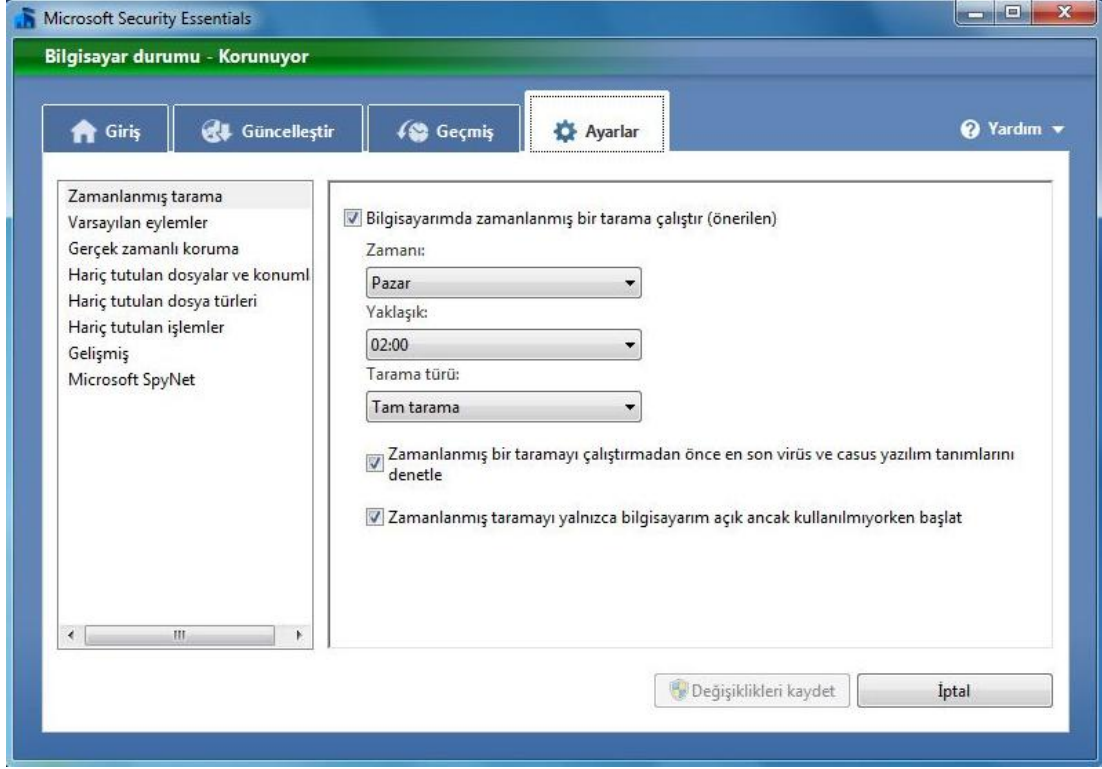
Resim 2.11: Antivirüs Programı Güncelleme

- **Geçmiş** sayfasında bilgisayarda algılanan virüsler varsa listelenecektir. Buradaki listeyi silmek için Geçmiş sil butonuna basılabilir. Liste silindiğinde virüslerin sildiği anlamına gelmez. Virüsler zaten silinmiştir.



Resim 2.12: Antivirüs Programı Geçmiş Sayfası

- **Ayarlar** sayfasında tarama ayarları zamanlanması, korunma durumu, taranacak sürücü ayarları yapılabilir.



Resim 2.13: Antivirüs Programı Ayarlar Sayfası

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➤ Bilgisayarınızdaki güvenlik duvarını etkinleştiriniz.	➤ Denetim Masası – Sistem Güvenlik sekmesinden yararlanınız.
➤ E-posta adresinizde spam olarak gelen postaları kontrol ediniz.	➤ E-posta adresindeki gereksiz postalar klasörünü kontrol ediniz.
➤ Bilgisayarınızda güncellemeleri kontrol ediniz.	➤ Denetim Masası-Sistem Güvenlik sekmesinden yararlanınız.
➤ Casus yazılımlardan korunmak için bilgisayarda kullanılan yazılımı kontrol ediniz.	➤ Denetim Masası-Sistem Güvenlik sekmesinden yararlanınız.
➤ Bilgisayarınızda açılır pencere engelleyicisini aktifleştiriniz.	➤ Tarayıcı menüsünden Araçlar sekmesinden yararlanınız.
➤ Bilgisayarınıza antivirüs yazılım kurarak tarama işlemi yapınız.	➤ Bilgisayarınıza antivirüs yazılımı kurarak tarama işlemi yapabilirsiniz.

KONTROL LİSTESİ

Bu faaliyet kapsamında aşağıda listelenen davranışlardan kazandığınız beceriler için **Evet**, kazanamadığınız beceriler için **Hayır** kutucuğuna (X) işareti koyarak kendinizi değerlendiriniz.

Değerlendirme Ölçütleri	Evet	Hayır
1. Güvenlik Duvarını etkinleştirebildiniz mi?		
2. E-Posta adresinizde spam kontrolü yaptınız mı?		
3. Güncelleştirmeleri kontrol edebildiniz mi?		
4. Casus yazılımlardan korunma yazılımı açabildiniz mi?		
5. Tarayıcınızda açılır pencere engelleyicisini aktifleştirebildiniz mi?		
6. Antivirüs yazılımı kullanarak tarama işlemi yapabildiniz mi?		

DEĞERLENDİRME

Değerlendirme sonunda “**Hayır**” şeklindeki cevaplarınızı bir daha gözden geçiriniz. Kendinizi yeterli görmüyorsanız öğrenme faaliyetini tekrar ediniz. Bütün cevaplarınız “**Evet**” ise “Ölçme ve Değerlendirme”ye geçiniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

1. Güvenlik duvarına ulaşmak için aşağıdakilerden hangisi kullanılır?
A) Sistem Penceresi
B) Görev Yöneticisi
C) Denetim Masası
D) Masaüstü
2. Güvenlik duvarını açma / kapatma işlemi aşağıdaki sekmelerden hangisi kullanılır?
A) Sistem Güvenlik
B) Görünüm Kişiselleştirme
C) Ağ ve İnternet
D) Erişim Kolaylığı
3. Aşağıdakilerden hangisi spam filtreme kurallarından **değildir**?
A) İçeriğin sürekli resimden oluşması
B) İçeriğin büyük harflerden oluşması
C) İçeriğin yazıdan oluşması
D) İçeriğin parlak renklerden oluşması
4. İşletim sistemi güvenlik açıklarını kapatmak için aşağıdakilerden hangisi uygulanabilir?
A) Sürücü ekleme
B) Güvenlik yaması ekleme
C) Bağlantı noktası ekleme
D) Güç seçenekleri ayarlama
5. Casus yazılımlardan korunma yazılımına işletim sistemi dâhilinde nasıl erişilir?
A) Tarayıcı-Araçlar
B) Bilgisayarım-Özellikler
C) Denetim Masası
D) Başlat-Donatılar

Aşağıdaki cümlelerin başında boş bırakılan parantezlere, cümlelerde verilen bilgiler doğru ise D, yanlış ise Y yazınız.

6. () İstenmeden açılan pencereler, tarama sırasında kullanıcıya sormadan kendiliğinden açılan pencerelerdir.
7. () Casus yazılımlardan korunmak için tarayıcıdan İnternet seçenekleri ayarları değiştirilebilir.
8. () Bilgisayar sistemlerinin düzgün çalışmalarını engelleyen, veri kayıplarına, veri bozulmalarına ve çeşitli yollarla kendisini kopyalayan kötü amaçlı yazılımlara virüs denir.

9. () Antivirüs programının geçmiş sayfasında algılanan virüs listesi silindiğinde virüsler bilgisayardan silinecektir.
10. () Antivirüs programının güncelleştirme için zaman ayarları yapılamaz. Bu ayarlar kurulduğunda otomatik olarak yapılır ve değiştirilemez.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları faaliyete geri dönerek tekrarlayınız. Cevaplarınızın tümü doğru ise bir sonraki öğrenme faaliyetine geçiniz.

ÖĞRENME FAALİYETİ-3

AMAÇ

Sorunsuz ve güvenli çalışan kablosuz ağ yapılandırarak kablosuz ağı yönetebileceksiniz.

ARAŞTIRMA

- Kablosuz ağ kurmak için gerekli donanımların neler olduğunu öğreniniz.
- Kablosuz ağ çeşitlerini araştırarak nasıl bağlanılır?
- Kablosuz ağ güvenliklerinin nasıl sağlandığını öğreniniz.

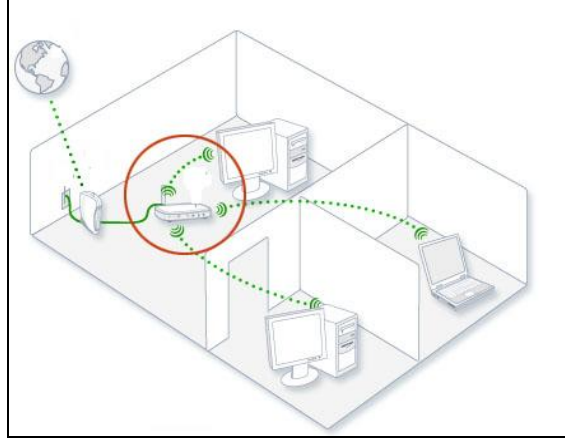
3. KABLOSUZ ORTAM GÜVENLİĞİ

3.1. Kablosuz LAN (Yerel Ağ) Güvenliği

Kablosuz ağ, iki veya daha fazla bilgisayar arasında kablo ile oluşturulan yapısal ağın kablo yerine alıcı ve verici cihazlar arasında radyo dalgaları ile iletişim sağlanan ve daha uzak mesafeler arasında ağ imkanı sunan bir teknoloji bütünüdür. Kablosuz yerel ağlar sağlık kurumları, hipermarketler, üretim kuruluşları, fabrikalar, akademik kurumlar ve ambarlar gibi birçok alanda yaygın hale gelmiştir. Günümüzde kablosuz yerel ağlar birçok iş sahasında genel amaçlı bağlantı alternatifini olarak kabul edilmektedir.

Kablosuz ağ da kablosuz ağ bağdaştırıcısı (ağ kartı), kablosuz modem veya kablosuz yönlendirici (router) gibi donanımlar kullanılabilir.

Kablosuz ağlardaki en temel güvenlik problemi verilerin havada transfer edilmesidir. Kablolu ağlarda switch ya da hub kullanarak güvenliği fiziksel olarak sağlanabilir ve switche / hub'a fiziksel olarak bağlı olmayan cihazlardan güvenlik önlemi alınabilir. Kablosuz ağlarda tüm iletişim hava üzerinden kurulur.



Resim 3.1: Kablosuz ađ

Kablosuz ađlarda güvenlik açıkları ađa saldırılara neden olabilir. Kablosuz ađa giren saldırgan ađdaki kullanıcıların yapabilecekleri her şeyi yapabilecektir. Bilgisayarlardaki dosyaları dizinleri kopyalayabilir, zararlı programları bilgisayara kurabilir. Tüm ađ trafiđini kaydedilip inceleyebilir. Kablosuz ađı dıřarıdan kullananlar, servis reddi atakları, spam yaymak gibi bazı kanunsuz iřler için ađı kullanılabilirler. Bu iřlerin sonuçları ise kablosuz ađ yetkilisini bađlar.

Kablosuz ađda güvenliđi sađlamak için;

- Eriřim noktasının veya kablosuz modem arayüz kullanıcı adı řifresi deđiřtirilebilir. Kablosuz ađda arayüze bađlanmak için tarayıcıya ara yüzün adresi yazılır.

Resim 3.2: Arayüze giriř penceresi

Arayüzü şifresi değiştirmek için Gelişmiş Ayarlar sekmesi kullanılarak arayüze giriş için kullanılan kullanıcı adı ve şifresi değiştirilebilir. Erişim noktası veya modem üreticileri firmalarına göre bu ayarın yeri değişiklik gösterilebilir.

Resim 3.3: Arayüzü kullanıcı adı, şifre

- Erişim noktasının (Access point) veya modem yazılımı güncellenmelidir. Arayüzü kullanılarak ayarlar sekmesinden yazılımı kullan seçeneği kullanılabilir.
- Erişim noktası veya kablosuz modem kullanılmadığı zamanlarda kapatılabilir.
- Mac Adresini filtrelemek, kullanıcının Mac adresi ile girilmeyen cihazların erişim noktasına bağlanmasını engeller. Modeminizin ya da erişim noktasının kablosuz ayarlar / güvenlik bölümünde Mac adres filtrelemesi kullanılabilir.

Resim 3.4: MAC adresi filtreleme

Kablosuz ağ güvenliğini sağlamanın bir diğer yolu da güçlü bir şifreleme yapılmasıdır. Kablosuz ağ donanımının kullanıcıya sunduğu en yüksek şifreleme yöntemi ayarlar sekmesinden seçilebilir.

- Kablosuz ağda IP havuzu belirlenerek havuzda bulunan IP adreslerinin ağa bağlanması sağlanabilir. Bu yöntem kullanılarak ağ trafiği hızlanabilir.

Resim 3.5: IP filtreleme

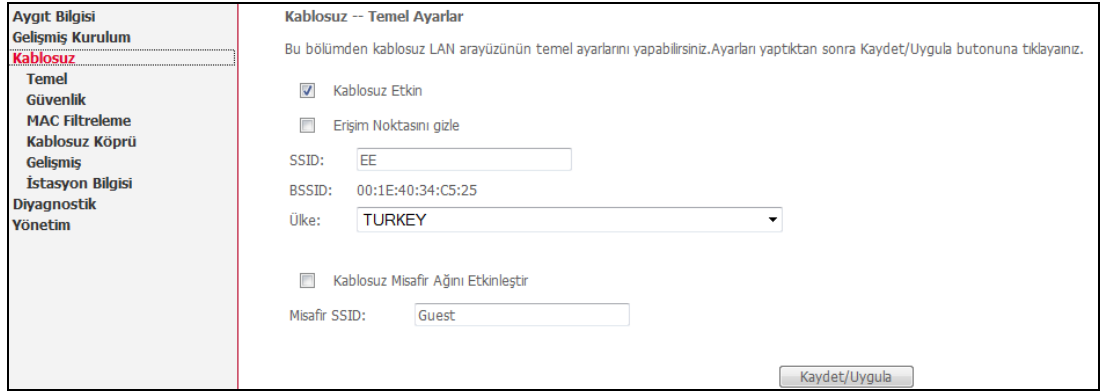
3.2. SSID

Hizmet Kümesi Tanıtıcısı (Service Set Identifier / SSID), belirli bir kablosuz ağa verilen addır. Kablosuz ağ adı (SSID) kablosuz yönlendirici üzerinde belirlenir. Kablosuz yönlendirici, atanmış SSID'yi yayınlayacak veya yayınlamayacak şekilde ayarlanabilir. Kablosuz yönlendirici SSID'yi yayınlayacak şekilde ayarlanmışsa kablosuz ağ bir yayın yapan ağdır ve saldırganlar tarafından bu ağ adı görüntülenebilir. Kablosuz yönlendirici SSID 'yi yayınlamayacak şekilde ayarlanmışsa, kablosuz ağ bir yayın yapmayan ağdır.

Yayın yapan bir ağ üzerinde kullanılan kablosuz yönlendirici kapsama alanında olan kablosuz bağdaştırıcılara sahip bilgisayarlar ağ SSID'yi algılama ve görüntüleme özelliğine sahiptir. Bu özellik, bağlanılabilecek kullanılabilir kablosuz ağlar aranmasında kullanılabilir.

Yayın yapmayan bir ağ üzerinde kullanılan kablosuz yönlendirici kapsama alanında olan kablosuz bağdaştırıcılara sahip bilgisayarlar ağ SSID'yi algılayabilir, ancak görüntüleyemez. Yayın yapmayan bir ağa bağlanabilmek için, bu ağın SSID'nin bilinmesi gerekir.

SSID adı arayüzde kablosuz sekmesi kullanılarak aktif/pasif konuma getirilebilir.



The screenshot shows a web-based configuration interface for wireless LAN settings. On the left, there is a sidebar menu with options: 'Aygıt Bilgisi', 'Gelişmiş Kurulum', 'Kablosuz', 'Temel', 'Güvenlik', 'MAC Filtreleme', 'Kablosuz Köprü', 'Gelişmiş', 'İstasyon Bilgisi', 'Diyagnostik', and 'Yönetim'. The 'Kablosuz' option is selected. The main content area is titled 'Kablosuz -- Temel Ayarlar'. Below the title, there is a text box stating: 'Bu bölümden kablosuz LAN arayüzünün temel ayarlarını yapabilirsiniz. Ayarları yaptıktan sonra Kaydet/Uygula butonuna tıklayınız.' The settings include: 'Kablosuz Etkin' (checked), 'Erişim Noktasını gizle' (unchecked), 'SSID:' (text input field with 'EE'), 'BSSID:' (text input field with '00:1E:40:34:C5:25'), 'Ülke:' (dropdown menu with 'TURKEY'), 'Kablosuz Misafir Ağını Etkinleştir' (unchecked), and 'Misafir SSID:' (text input field with 'Guest'). At the bottom right, there is a 'Kaydet/Uygula' button.

Resim 3.6: SSID ayarı değiştirme

3.3. WLAN'a Saldırıları

Kablosuz ağlardaki hızlı yaygınlaşma ve hız artışı, güvenlik önlemlerinin de daha fazla dikkate alınmasını mecburi kılmaktadır. Sistem yöneticilerinin ve ev kullanıcılarının konuyla ilgili olarak bilgi sahibi olmaları ve daha bilinçli davranmaları çok önemlidir. Ev kullanıcılarının konuyla ilgili olarak bilinçlendirilmeleri oldukça zordur. Bu nedenle, ev kullanıcılarını ilk etapta koruma görevi, kablosuz ağ erişim noktası satan ve İnternet erişimi sağlayan firmalar tarafından verilmesi en uygun yöntem olacaktır.

Kablosuz ağlardaki güvenlik açıklarının bilincinde olan saldırganlar kablosuz ağları saptamak için özel teknikler ve yazılımlar kullanmaktadır. Bu yazılımlar ile ellerindeki kablosuz ağ kartının sürekli frekans taraması yapmasını sağlayarak sinyaline ulaşabildiği kablosuz ağların yerlerini not etmektedir. Araçlarında kablosuz ağ kartı bulunan bir dizüstü

bilgisayar veya avuçi bilgisayar olarak gezen saldırganlar, bu yöntem ile kablosuz ağların bulunduğu yerleri saptamaktadır. Geçmişte sinyal aldıkları yerleri tebeşir ile işaretleyen saldırganlar, artık GPS cihazları ile kablosuz ağları haritada işaretlemeye başladı. İhtiyaç duydukları anda ise özel yazılımlar kullanarak bu ağlara giriş yapabilmektedir.

Kablosuz ağların yöneticileri, kablosuz ağ saldırılarından en az seviyede etkilenebilmek için kablosuz ağlarında şifreleme protokolünü kullanmalı, en az 128 Bit bir algoritma seçmeli, ayrıca kablosuz ağa girebilecek olan SSID ve MAC adreslerini de filtrelemelidir. Bu önlemlere ek olarak halka açık olması planlanmayan bir kablosuz ağ için bağlantı sinyalinde alt limit belirlemekte ciddi bir güvenlik önlemidir.

Kablosuz ağ saldırılarının bir çeşidi de erişim noktası yanıltma (Spoof) ve MAC Adresi Dinleme (Sniff)dir. Güçlü kimlik formları kullanıldığında Erişim Kontrol Listeleri kabul edilebilir bir güvenlik seviyesi sağlamaktadır. Fakat MAC adresleri için geçerli değildir. MAC adresleri web kullanılabilir durumda iken dahi şifresiz metin olarak saldırgan tarafından kolaylıkla dinlenebilir. Ayrıca, kablosuz ağ kartlarının bir yazılım vasıtası ile MAC adresleri kolaylıkla değiştirilebilir. Saldırgan tüm bu avantajları kullanarak ağa girebilmektedir.

MAC adresini dinlemek çok kolaydır. Paket yakalama yazılımı kullanarak saldırgan kullanılan bir MAC adresini tespit eder. Eğer kullandığı kablosuz ağ kartını izin veriyorsa MAC adresini bulduğu yeni MAC adresine değiştirebilir ve artık hazırdır. Eğer saldırgan yanında kablosuz ağ donanımları bulduruyorsa ve yakınında bir kablosuz ağ varsa aldatma (spoof) saldırısı yapabilir demektir. Aldatma saldırısı yapabilmek için, saldırgan kendine ait olan erişim noktasını yakınındaki kablosuz ağa göre veya güvenebileceği bir *İnternet* çıkışı olduğuna inanan bir kurbanı göre ayarlamalıdır. Bu sahte erişim noktasının sinyalleri gerçek erişim noktasından daha güçlüdür. Böylece kurban bu sahte erişim noktasını seçecektir. Kurban bir kere iletişime başladıktan sonra, saldırgan onun şifre, ağ erişim ve diğer önemli bütün bilgilerini çalacaktır. Bu saldırının genel amacı aslında şifre yakalamak içindir.

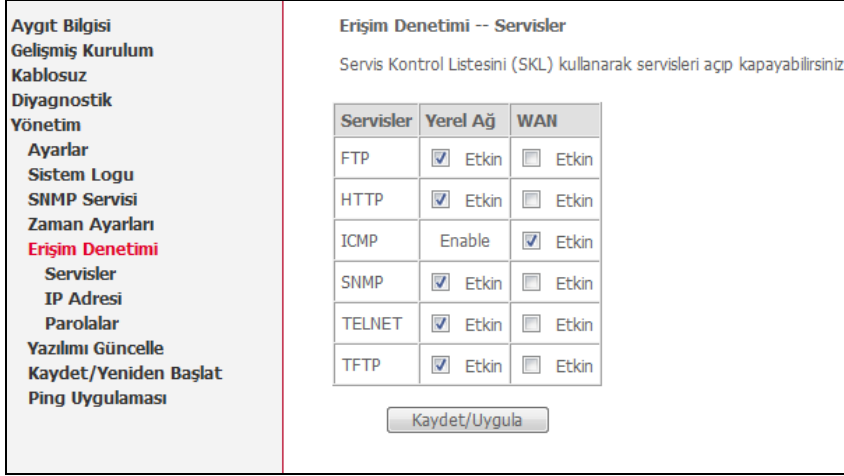
Kablosuz ağa saldırılar öncelikle kablosuz ağın algılanması ile başlamaktadır. Daha sonra ağda şifreleme yapılmışsa bu şifrelemeyi kırmak ve ağa girmeye çalışılacağı da unutulmamalıdır.

3.4. WLAN'a Erişimi Sınırlama

Kablosuz ağ güvenliğinde MAC ve IP adresi filtreleme yöntemlerinden farklı olarak erişim noktası sınırlama ayarları mevcuttur. Güvenlik duvarı arkasında bulunan erişim noktaları incelendiğinde zayıf noktaları olarak kablosuz ağ girişleri, konferans odalarındaki ethernet portları, taşınabilir laptoplar ve yetkilendirme yapılmamış diğer uçlar (PC, yazıcı vs) gözü çarpmaktadır. Bu noktalar ağın toplam güvenliği için ciddi risk oluşturmaktadır.

Kablosuz ağlarda, ağ erişim kontrolü (NAC) de kullanılabilir. NAC kurumların iletişim ağını kullananların, ilgili kurumun güvenlik politikası kurallarına uygunluğunu denetleyen bir güvenlik teknolojisidir. NAC ile sadece şirket ağ politikalarına uyan ve güvenilir olan masaüstü bilgisayar, dizüstü bilgisayar, sunucu ve cep bilgisayarının (PDA) şirket ağına bağlanmasına izin verilmektedir.

Kablosuz ağ kullanıcılarının ağa erişimlerini sınırlama işleminden biri de ağda kullandıkları hizmetlerin (http, ftp, telnet vb.) sınırlandırılmasıdır. Bu hizmetleri sınırlandırmak için erişim noktası (Access Point) ya da modemın ara yüzü kullanılarak yönetim sekmesinden erişim denetimi bölümü seçilerek ulaşılabilir.



Resim 3.7: Erişim sınırlama

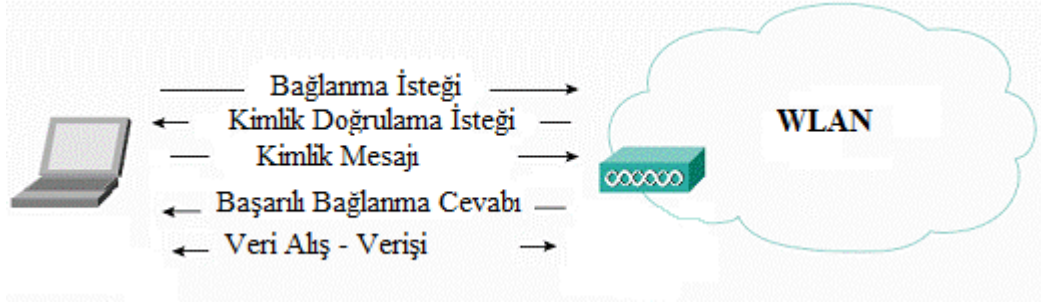
3.5. WLAN'da Kimlik Doğrulama

Kablosuz ağ standardı kimlik doğrulama için iki adet mekanizma sunar bunlar, açık kimlik doğrulama ve paylaşılmış anahtar kimlik doğrulamasıdır. Standart dâhilinde olmayana ancak sıkça kullanılan diğer iki yöntem de SSID (Service Set Identifier) ve MAC (Media Access Control) değerlerinin kimlik doğrulamada kullanılmasıdır. SSID değerinin kullanılması aslında ağın mantıksal olarak bölümlere ayrılmasını sağlar ve bir kimlik doğrulama mekanizması olarak düşünülmüş bir yöntem değildir ancak güvenliği artırıcı ek bir önlem olarak değerlendirilebilir. Her hangi bir istemcinin ağdan hizmet alabilmesi için doğru SSID değeri ile yapılandırılmış olması gerekir.

Kimlik doğrulamadaki en önemli şeylerden biri de doğrulamanın kesinlikle kullanıcı tabanlı olmaması ve yalnızca cihazın kimlik doğrulamasının yapılmasıdır. Bu da her iki yöntem için bir zayıflık olarak görülebilir.

Kimlik doğrulaması temelde şu adımlardan oluşur;

- İstemci tüm kanalları kullanarak bir mesaj çerçevesi gönderir.
- Ulaşılabilen erişim noktaları bir mesaj çerçevesi ile cevap verir.
- İstemci hangi erişim noktasına bağlanacağına karar verir ve bir kimlik doğrulama isteği yollar.
- Erişim noktası ise bir kimlik doğrulama mesajı yollar.
- Başarılı bir kimlik doğrulamanın ardından istemci bir ilişki istek çerçevesi yollar.
- Erişim noktası bir ilişki cevap çerçevesi yollar.
- Bu adımdan sonra artık istemci veri gönderme ve veri alma işlemini gerçekleştirebilir.



Resim 3.8: WLAN kimlik doğrulama

3.6. WLAN'da Şifreleme

Kablosuz ağların güvenliğinin sağlanması için ağların şifrelenmesi yöntemi geliştirilmiştir. 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.

3.6.1. WEP

802.11 standardı, kablosuz alan ağlarında ortaya çıkan haberleşmelerin tanımlandığı bir standarttır. WEP (Wired Equivalent Privacy) algoritması her türlü haricî saldırıdan kablosuz haberleşmeyi korumak için kullanılır. WEP'in ikinci fonksiyonu ise kablosuz ağa yetkisiz erişimleri engellemektir. WEP bir mobil cihaz istasyonu ve erişim noktası arasındaki kablosuz haberleşme kurmak ve paylaşımında bulunabilmek için bir şifreye ihtiyaç duyar. Bu şifre ya da güvenlik anahtarı veri paketlerini göndermeden önce onları şifrelemek ve gönderim sonrasında değişikliğe uğrayıp uğramadıklarını için diğer bir ifadeyle doğruluk kontrolü yapmak amacıyla kullanılır.

WEP, 802.11 standardıyla beraber geliştirilmiş olan temel güvenlik birimidir. Kablosuz düğümler arasındaki iletimde şifreleme ve veri bütünlüğünü sağlama işlemlerini gerçekleştirmeye çalışır. WEP şifreleme için kullanıcı ve erişim sağlayıcı tarafında 40 bitlik statik bir anahtar tanımlanır. Ayrıca WEP, akış şifresini elde etmek için 24 bitlik bir ilklendirme vektörü (Initialization Vector-IV) kullanılır.

WEP'in çalışması şu şekildedir

- Veri bütünlüğünü sağlamak amacıyla, veri bir doğrulama algoritmasına (integrity check) tabi tutularak, doğrulama bitleri (ICV-Integrity Check Value) elde edilir.
- Bu doğrulama bitleri verinin sonuna eklenir.
- 24 bitlik IV statik anahtarın başına eklenir; 64 bitlik paket oluşturulur.
- 64 bitlik bu paket RC4 (rastgele sayı üretici-PseudoRandom Number Generator-PRNG) algoritması ile şifrelenir.

- 2. adımda elde edilen veri ile 4. adımda elde edilen veri bir XOR işleminden geçer.
- Elde edilen bu verinin başına tekrar IV eklenir ve iletilecek şifreli veri elde edilir. Elde edilen bu verinin başına, alıcı ve vericinin MAC adresi eklenerek kablosuz ortama gönderilir.
- Şifreli veri, karşı tarafta aynı işlemler tersi yönde uygulanarak açılır.

Kablosuz ağa WEP şifresi verebilmek için erişim noktasının ya da modem arayüzüne girerek kablosuz sekmesinden güvenlik bölümüne tıklanır.

Resim 3.9: WEP şifreleme

3.6.2. WPA

WPA kablosuz ağlar için geliştirilmiş bir şifreleme standardıdır. Bu standart daha önceki WEP (Wired Equivalent Privacy-Kabloya Eş Güvenlik) sisteminin yetersizliğine karşılık geliştirilmiştir. WPA, veri şifreleme ve kullanıcı kimlik denetimi alanlarında bilgi güvenliği sunmaktadır. WPA, veri şifreleme işlemini geliştirmek için bu konuda yeni bir yöntem sunarak şifreleme anahtarlarını otomatik olarak dağıtır. Bir bit veri bile şifreleme anahtarlarıyla korunur. Bu çözüm aynı zamanda, veri üzerinde bütünsel bir kontrol yaparak, verileri ele geçirmek isteyen kişilerin bilgileri değiştirmesini engeller. WPA, kurumsal kullanıcıların korunması için, ağ üzerindeki her bir kullanıcıya kimlik denetimi uygularken, bu kullanıcıları veri hırsızlığı amacıyla düzenlenmiş ağlara geçişini de engeller. Aynı zamanda WPA ile 48 bitlik bir şifreleme yapılır.

Kablosuz ağa WPA şifresi verebilmek için erişim noktasının ya da modem arayüzüne girerek kablosuz sekmesinden güvenlik bölümüne tıklanır.

ADSL	Kablosuz
Temel	
Güvenlik	
MAC Filtreleme	
Gelişmiş	
İstasyon Bilgisi	

Kablosuz -- Güvenlik

Bu bölümden kablosuz LAN güvenlik ayarlarını yapabilirsiniz. Ayarları yaptıktan sonra "Uygula" butonuna basınız.

SSID Seç: EE

Ağ Kimlik Denetimi: WPA

WPA Group Şifresi Aralığı: 0

Radius Sunucu IP Adresi: 0.0.0.0

Radius Portu: 1812

Radius Şifresi:

WPA Şifreleme: TKIP

WEP Şifreleme: Etkin Değil

Kaydet/Uygula

Resim 3.10: WPA şifreleme

3.7. WLAN’da Trafik Filtreleme

WLAN’a kimlerin erişim kazanacağını ve iletilen verileri kimlerin kullanabileceğinin denetlenmesinin yanı sıra WLAN üzerinden iletilen trafik türünün de denetlenmesi yararlıdır. Trafik filtrelemesi kullanılarak bu gerçekleştirilir.

Trafik filtrelemesi, istenmeyen trafiğin kablosuz ağa girmesini veya kablosuz ağdan çıkmasını engeller. Trafik, erişim noktası üzerinden geçerken erişim noktası tarafından filtreleme yapılır. Belirli bir MAC veya IP adresinden trafiği kaldırmak ya da belirli bir MAC veya IP adresine trafiği hedeflemek için filtreleme yapılabilir. Bu işlev, belirli uygulamaları da bağlantı noktası numaralarına göre engelleyebilir. İstenmeyen ve şüpheli trafik ağdan kaldırılarak, önemli trafiğin hareketine daha fazla bant genişliği adanır ve WLAN’ın başarımı artırılır. Örneğin, kimlik doğrulama sunucusu gibi belirli bir makineyi hedefleyen tüm telnet trafiğini engellemek için trafik filtreleme kullanılabilir. Kimlik doğrulama sunucusuna yönelik telnet girişimleri şüpheli olarak değerlendirilir ve engellenir.

UYGULAMA FAALİYETİ

Verilen basamakları kablosuz ağ için uygulayınız.

İşlem Basamakları	Öneriler
➤ Erişim noktanızın (veya modeminizin) ara yüz giriş bilgilerinizi değiştiriniz.	➤ Tarayıcı kullanarak arayüze giriş yapabilirsiniz.
➤ Güvenlik için kablosuz ağınızda MAC filtreleme yapınız ve sadece kendi MAC adresinizi giriniz.	➤ Ara yüzünde MAC adresini girerek MAC filtrelemeyi etkinleştirebilirsiniz.
➤ Kablosuz ağınızda IP havuzu oluşturarak IP filtreleme işlemi yapınız.	➤ Ara yüzünde Güvenlik sekmesinden yararlanabilirsiniz.
➤ Kablosuz ağınızda SSID adınızı değiştiriniz.	➤ Ara yüzdeki Kablosuz-Temel Ayarlar sekmesinden yararlanabilirsiniz.
➤ Kablosuz ağınızın SSID adını gizleyiniz.	➤ Ara yüzdeki Kablosuz-Temel Ayarlar sekmesinden yararlanabilirsiniz.
➤ Kablosuz ağınızdaki hizmetlerin erişimlerini sınırlayınız.	➤ Ara yüzündeki Yönetim-Erişim Denetimi sekmesinden yararlanabilirsiniz.
➤ Kablosuz ağınıza şifreleme yöntemlerinden WEP şifrelemesi uygulayarak şifreleme yapınız.	➤ Ara yüzdeki Kablosuz – Güvenlik – Ağ kimlik Denetimi sekmesini kullanabilirsiniz.
➤ Kablosuz ağınıza şifreleme yöntemlerinden WPA şifrelemesi uygulayarak şifreleme yapınız.	➤ Ara yüzdeki Kablosuz-Güvenlik-Ağ kimlik Denetimi sekmesini kullanabilirsiniz.

KONTROL LİSTESİ

Bu faaliyet kapsamında aşağıda listelenen davranışlardan kazandığınız beceriler için **Evet**, kazanamadığınız beceriler için **Hayır** kutucuğuna (X) işareti koyarak kendinizi değerlendiriniz.

Değerlendirme Ölçütleri	Evet	Hayır
1. Erişim noktanızın (veya modeminizin) ara yüz giriş bilgilerinizi değiştirebildiniz mi?		
2. Güvenlik için kablosuz ağınızda MAC filtreleme yapabildiniz mi ?		
3. Kablosuz ağınızda IP havuzu oluşturarak IP filtreleme işlemini yapabildiniz mi?		
4. Kablosuz ağınızda SSID adınızı değiştirebildiniz mi?		
5. Kablosuz ağınızın SSID adını gizleyebildiniz mi?		
6. Kablosuz ağınızdaki hizmetlerin erişimlerini sınırlayabildiniz mi?		
7. Kablosuz ağınıza şifreleme yöntemlerinden WEP şifrelemesi uygulayabildiniz mi?		
8. Kablosuz ağınıza şifreleme yöntemlerinden WPA şifrelemesi uygulayabildiniz mi?		

DEĞERLENDİRME

Değerlendirme sonunda “**Hayır**” şeklindeki cevaplarınızı bir daha gözden geçiriniz. Kendinizi yeterli görmüyorsanız öğrenme faaliyetini tekrar ediniz. Bütün cevaplarınızı “**Evet**” ise “Ölçme ve Değerlendirme”ye geçiniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

1. Kablosuz yerel ağ güvenliği sağlamak için aşağıdakilerden hangisi **YAPILMAZ**?
A) Ara yüze giriş bilgileri değiştirme
B) Erişim Noktasının yazılımını güncelleme
C) Bilgisayar adını değiştirme
D) Erişim noktası bağlı olunmadığı zamanlarda kapatma
2. SSID anlamı aşağıdakilerden hangisidir?
A) Bilgisayar adı
B) Ara yüz adı
C) Kablosuz ağ adı
D) Şifreleme adı
3. Aşağıdakilerden hangisi kablosuz ağ saldırı çeşididir?
A) Erişim noktası yanıltma
B) Tarayıcıya girme
C) Erişimi kesme
D) IP adresine girme
4. Aşağıdakilerden hangisi kablosuz ağda kimlik doğrulama işlemlerinden **DEĞİLDİR**?
A) İstemcinin mesaj çerçevesi yollaması
B) İstemcinin kimlik doğrulama isteği yollaması
C) Erişim noktasının kimlik doğrulama mesajı yollaması
D) İstemcinin kimlik doğrulama mesajı yollaması
5. Aşağıdakilerden hangisi şifreleme yöntemlerindedir?
A) WLAN
B) 820.11
C) WEP
D) WAN

Aşağıdaki cümlelerin başında boş bırakılan parantezlere, cümlelerde verilen bilgiler doğru ise **D**, yanlış ise **Y** yazınız.

6. () Kablosuz ağlarda WEP 24 bitlik bir şifreleme yapar.
7. () MAC filtreleme yapmak için ara yüz de Kablosuz-Güvenlik sekmelerine girilir.
8. () IP havuzu oluşturarak filtreleme yapmak kablosuz ağ için güvenlik açığı oluşturur.
9. () Yayın yapmayan bir ağ üzerinde kullanılan kablosuz yönlendirici kapsama alanında olan kablosuz bağdaştırıcılara sahip bilgisayarlar ağ SSID'yi algılayabilir ve görüntüleyebilir.

10. () MAC Adresi Dinleme (Sniff) saldırısı ile erişim noktasının MAC adresi değiştirilebilir.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları faaliyete geri dönerek tekrarlayınız. Cevaplarınızın tümü doğru ise Modül Değerlendirme'ye geçiniz.

MODÜL DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

1. Aşağıdakilerden hangisi ağ iletişim tehditlerinden **değildir**?
A) Ağın içinden gelecek saldırılar
B) Ağın dışından gelecek saldırılar
C) Sosyal mühendislik
D) Sosyal iletişim
2. Aşağıdakilerden hangisi donanıma yönelik bir saldırıdır?
A) Yazıcılara
B) Tarayıcılara
C) Veri depolama kaynaklarına
D) Kullanıcı hesaplarına
3. Aşağıdakilerden hangisi VPN bağlantısını ifade eder?
A) Sanal paylaşımlı ağ
B) Sanal paylaşımsız ağ
C) Sanal kablosuz ağ
D) Sanal yerel ağ
4. Aşağıdakilerden hangisi güvenlik önlemlerinden biri **değildir**?
A) Tanımlama ve kimlik doğrulama
B) Sosyal mühendislik
C) VPN Bağlantı
D) Ağ Bakım Yordamları
5. İşletim sisteminin güncellemelerini aktif hâle getirmek için aşağıdakilerden hangisi kullanılır?
A) Denetim Masası-Ağ Paylaşım Merkezi
B) Denetim Masası-Programlar
C) Donatılar-Sistem Araçları
D) Denetim Masası-Sistem Güvenlik
6. SPAM e-posta aşağıdakilerden hangisinde tutulur?
A) Gelen kutusu
B) Silinmişler
C) Gereksiz postalar
D) Taslaklar
7. Aşağıdaki sekmelerin hangisinde MAC adresi filtreleme yapılabilir?
A) Aygıt bilgisi
B) WAN
C) Kablosuz
D) Yerel Ağ

8. Aşağıdakilerden hangisi kablosuz ağda hizmet sınırlama işlemlerinden **değildir**?
A) Telnet
B) FTP
C) HTTP
D) DHCP
9. Aşağıdakilerden hangisi WPA şifreleme yönteminin avantajlarındanır?
A) Veri şifreleme ve Kimlik denetimi
B) Veri transferi
C) Erişim noktası sorgulama
D) İstemci denetimi
10. Aşağıdakilerden hangisi kablosuz ağ güvenliği sağlamak için **kullanılmaz**?
A) Ağ trafiği filtreleme
B) Kimlik doğrulama
C) Erişim kolaylığı
D) Erişim denetimi

Aşağıdaki cümlelerin başında boş bırakılan parantezlere, cümlelerde verilen bilgiler doğru ise D, yanlış ise Y yazınız.

11. () Sahte senaryo uydurma yönteminde saldırganın senaryonun ana hattı dışına çıkabilecek durumları da göz önüne alıp hazırlık yapması, başarı oranını artıran bir etkendir.
12. () DDoS saldırıda; saldırganın kontrolü altındaki onlarca bilgisayardan tek bir sunucuya binlerce sorgu göndermekte; bu da hedef makinenin band tüketmesine ya da tıkanmasına neden olmaktadır.
13. () Güvenlik duvarı kurulduğu konumda gelen ve giden ağ trafiğini kontrol ederek bilgisayarın ya da bilgisayar ağına yetkisiz veya istenmeyen kişilerin çeşitli yollardan erişim sağlamasını engellemeye yarayan yazılım veya donanımdır.
14. () Antivirüs yazılımları güncelleme işlemi yapmadan bilgisayar taraması daha güvenli bir yoldur.
15. () Kimlik doğrulamadaki en önemli şeylerden biri doğrulamanın kullanıcı tabanlı olması ve cihazın kimlik doğrulamasının yapılmamasıdır.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları faaliyete geri dönerek tekrarlayınız. Cevaplarınızın tümü doğru ise bir sonraki modüle geçmek için öğretmeninize başvurunuz.

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ-1'İN CEVAP ANAHTARI

1	C
2	A
3	D
4	A
5	C
6	Doğru
7	Yanlış
8	Yanlış
9	Doğru
10	Yanlış

ÖĞRENME FAALİYETİ-2'NİN CEVAP ANAHTARI

1	C
2	A
3	C
4	B
5	C
6	Doğru
7	Yanlış
8	Doğru
9	Yanlış
10	Yanlış

ÖĞRENME FAALİYETİ-3'ÜN CEVAP ANAHTARI

1	C
2	C
3	A
4	D
5	D
6	Doğru
7	Doğru
8	Yanlış
9	Yanlış
10	Yanlış

MODÜL DEĞERLENDİRMENİN CEVAP ANAHTARI

1	D
2	C
3	A
4	B
5	D
6	C
7	C
8	D
9	A
10	C
11	Doğru
12	Doğru
13	Doğru
14	Yanlış
15	Yanlış

KAYNAKÇA

- DİRİCAN Okan Can, **TCP/IP ve Ağ Güvenliđi**, Açık Akademi Yayınları, İstanbul, 2005.
- ÖZBİLEN Alper, **Bilgisayar Ağları ve Güvenliđi**, Pusula Yayıncılık, Ankara, 2005.
- ŞEN Ömer Faruk, Özgür ÖZDEMİRCİLİ, **Ağ Güvenliđi İpuçları**, Açık Akademi Yayınları, İstanbul, 2006.
- UÇAN N. Osman, OSMAN Onur, **Bilgisayar Ağları ve Ağ Güvenliđi**, Nobel Akademik Yayıncılık Eğitim Danışmanlık Tic. Ltd. Şti, Ankara, 2007.