YMT 311-Bilgi Sistemleri ve Güvenliği

Güvenlik, Hacking, Hacker Kavramları

Konu Başlıkları

- Bilişim güvenliği
- Bilişim güvenliği niçin önemlidir ?
- Hacker,
- Hacker çeşitleri,
- Hacker'lardan korunma yolları,
- Sosyal Mühendislik kavramı,
- Sosyal Mühendislik çeşitleri,
- Sosyal Mühendislerin kullandığı yöntemler,
- Sosyal Mühendislerinden korunma yolları

BİLİŞİM GÜVENLİĞİ NEDİR VE NİÇİN ÖNEMLİDİR?

- Bilişim suçları ve Güvenlik araştırması nın her yıl hazırladığı rapora göre bilişim suçları neredeyse her yıl 2 katına arttığı gözlenmiştir.
- Bilişim teknolojilerinin hayatımızın her alanında girmiş olmasıyla birlikte faydaları kadar bize dokunan zararları da ortaya çıkmıştır. Bilişim teknolojileri geliştikçe sistemlere yapılan saldırılar artmakta ve saldırı teknolojileri gelişmektedir.

BİLGİ GÜVENLİĞİMİZ İÇİN NELER YAPABİLİRİZ ?

- Şifre güvenliği
- Güvenilmeyen adreslerden gelen e-posta'ları okumak için dahi olsa açmamak (Resimli E-posta eklentileri)
- Geliştiricisi bilinmeyen Facebook Application 'lara katılmamak
- Tanımadığımız kişilerden gelen isteklere, aktivitelere katılmamak (Facebook, MSN vs.)
- Gerçek bilgilerimizi her yerde paylaşmamak (e-posta, TC kimlik No vs.)
- İnternette verdiğimiz tüm bilgilere birilerinin ulaştığını düşünerek her düşündüğümüzü, yaptığımızı vs. ulu orta paylaşmamak ☺
- Bilgi güvenliğimiz için birden fazla adres (e-posta vs.) kullanmaya özen göstermeliyiz.

Bunları biliyor muydunuz ?

- MSN‘de hotmail ve windowslive.com gibi uzantılarda tek bir şifre ile korunurken, gmail vs. gibi Microsoft haricindeki diğer uzantılarda MSN ve mailin aynı şifre olması zorunlu değil.
- Facebook ‘da hangi bilgisayardan (hatta browser’dan) giriş yaptıysan o bilgisayarın bilgilerini kayıt edip, eğer bilmediğin bir ortamdan adresine giriş yapılmış ise oturumu sonlandırabiliriz.
- WLM 2011 ile birlikte bir bilgisayarı güvenilen bir bilgisayar olarak gösterip, şifreni unuttuğunda direk güvenilen bilgisayar üzerinden hiçbir soru sorulmaksızın yeni şifre oluşturabiliriz.

HACK – HACKER KAVRAMLARI ?

- Hacker: Bilişim teknolojilerindeki bilgisini İYİ veya KÖTÜ olmak üzere bir sistemi ele geçirmek üzere kullanan kişi
- Hack: Kısaca bir hacker'ın yaptığı saldırıya verilen genel ad

DÜNYADAKİ BİLİŞİM SUÇLARI EN ÇOK HANGİ ÜLKELERDE İŞLENİYOR ?

- Türkiye, Rusya ve Brezilya

- Sebep: Bilişim suçlarına olan cezaların yetersiz kalması ve yeterince uygulanamaması

HACKER ÇEŞİTLERİ

- Yaptığı saldırı düzeyine göre Beyaz ve siyah şapkalı olmak üzere ikiye ayrılır.
- Ayrıca, siyah şapkalı hackerlar kendi içinde ayrılabilir.
- -Script Kiddies (Lamer): Kendini bir şey zanneden hacker
- -Phreakers: Santral ve telefon hatlarının açıklarını kullanan hacker
- -Crackers: PC yazılımlarını kıran ve yayınlayan hacker
- -Grey Hat Hackers: Hem savunma hemde saldırı amaçlı çalışan hacker. Amacı sadece kazanmaktır

DÜNYANIN EN ÜNLÜ HACKER‘I KİMDİR ? YAPTIĞI SALDIRILAR

- **Kevin David Mitnick** (**Condor** olarak da bilinir) (d. 6 Ağustos, 1963), ilk bilgisayar korsanlarından olup en meşhurudur. 15 Şubat 1995'te FBI tarafından yakalanmıştır. Fujitsu, Motorola, Nokia ve Sun Microsystems gibi şirketlerin bilgisayar ağlarına izinsiz girmekten suçlu bulunarak 5 yıl hapis cezası almıştır. Cezası 21 Ocak 2000'de, bilgisayarlara yaklaşma yasağı 21 Ocak 2003'te bitmiştir. Günümüzde, beyaz şapkalı bir bilgisayar korsanı olarak güvenlik danışmanlığı yapmakta ve dünya çapında kongrelere katılmaktadır.
- Mitnick, fotoğrafı FBI'in "En Çok Arananlar" listesinde yer alan ilk hacker olarak kayıtlara geçti ve neredeyse listeden hiç eksik olmadı. "İflah olmaz bir suçlu" olan çocuk ruhlu Mitnick "Sanal Dünya'nın Kayıp Çocuğu" olarak da tanındı.

DENNIS RITCHIE VEYA KEN THOMPSON‘I TANIYOR MUSUNUZ ?

- İlk başlar siyah şapkalı hacker olup sonradan beyaz şapkalılara katılan ünlü hacker’lardan.
- Esas ünleri C ve C++ Dillerini yazıp, Unix işletim sisteminin baş mimarı olmalarıdır.
- C programlama dili bugün hâlâ yazılım dünyasında aktif olarak kullanılmaktadır ve C++, Java, C# gibi modern programlama dillerini de etkilemiş konumdadır.

DENNIS RITCHIE VEYA KEN THOMPSON‘I TANIYOR MUSUNUZ ?

- Ünlü Linux işletim sistemi ve onun araçları Dennis Ritchie’nin yaptıklarına dayanmaktadır. Windows işletim sistemi de Unix uyumlu araçlar ve geliştiriciler için C derleyicileri içermektedir.

Ken Thompson (solda) ile Dennis Ritchie (sağda)

SOSYAL MÜHENDİSLİK KAVRAMI =?

- Akıllı insan kendi aklını kullanır. Daha akıllı insan ise hem kendi aklını hem de başkalarının aklını kullanır.

- BT alanında yeterli teknik bilgiye sahip olup açık aramaktansa insanların zayıf ve bilgisiz noktalarını kötü niyetli kullanan yaratıktır

SOS. MÜH. ÇEŞİTLERİ ?

- İnsan tabanlı ve PC Tabanlı olmak üzere ikiye ayırabiliriz.

- PC tabanlı Sos. Müh. hem aklını hem de PC bilgilerini kullanan kişidir desek herhalde yanlış olmaz.

SOS. MÜH. ÖRNEKLERİ?

- Sahte mail (Bir kişi ya da kurum adına mail göndererek kandırma)
- Bir web sitesinin tasarım olarak benzerini yapıp, domain olarakta çok benzer bir domain alıp, bilgilerimize erişmek
- Reklam'lara tıkla para kazan vs. sahte siteler.
- Kendisini bir firmanın yetkili kişisi gibi tanıtıp bilgilerine erişmek.

YMT 311-Bilgi Sistemleri ve Güvenliği

Şifreleme Bilimi ve Teknikleri

Konu Başlıkları

- Kriptoloji
- Sezar
- Pigpen
- Ebced
- Enigma
- Echelon
- Steganografi
- MD5
- RSA
- SHA1
- SHA2

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Kriptoloji**
  - **Kriptografi** :Bilgiyi şifreli hale dönüştürme işlemidir.
  - **Kriptoanaliz** :Bir şifreleme sistemini veya sadece şifreli mesajı inceleyerek, şifreli mesajın açık halini elde etmeye çalışan kriptoloji disiplinidir.

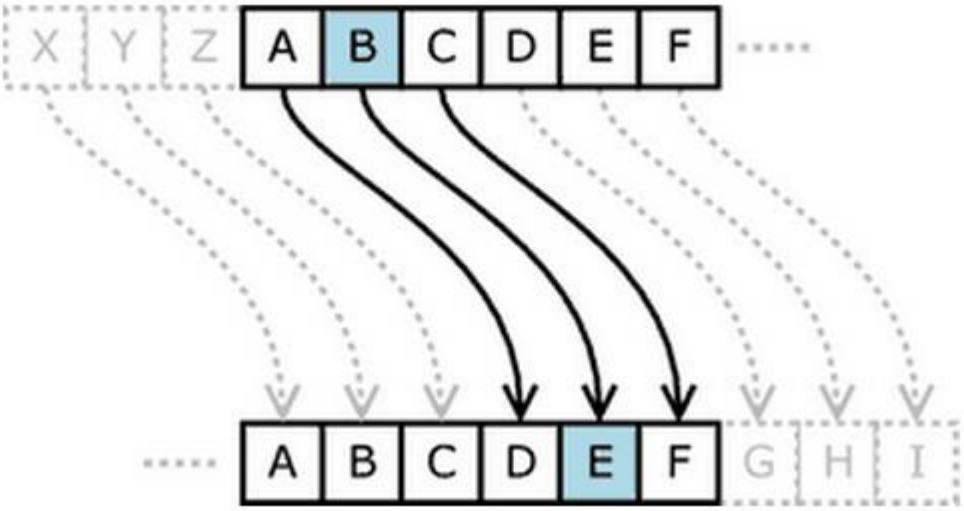
Şifreleme Bilimi ve Şifreleme Teknikleri

- **Şifreleme (Encryption):** Düz metni şifreli metne çevirme sürecidir.
- **Şifre Çözme(Decryption):** Şifrelenmiş metni düz metne çevirme işlemidir.
- **Anahtar(Key):**Şifreli metnin nasıl elde edildiğine dair kod parçasıdır.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Sezar Şifreleme**

- Şifrelenecek metin alfabede kendinden sonra gelecek 3. harfle yer değiştirerek oluşturulmaktadır.



Şifreleme Bilimi ve Şifreleme Teknikleri

C≡P+3(Mod29)

Şifrelemek istediğimiz metnimiz “BU MESAJ ÇOK ÖNEMLİDİR” olsun.

Mesaja karşılık gelen sayısal denklileri yazmadan önce belli kelimelerin tanınmasına dayana başarılı şifre çözme tekniklerini engellemek için mesajı beşli bloklara böleriz..

BUMES AJÇOK ÖNEML İDİR.

Harflerin sayısal denkliklere dönüştürülmesiyle;

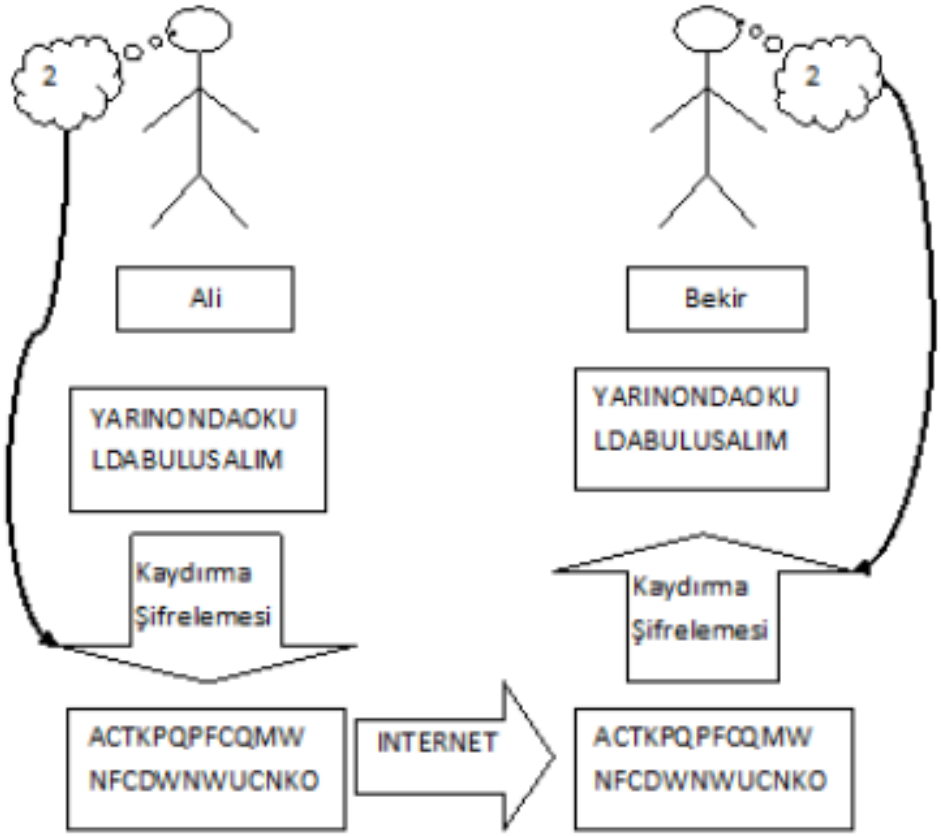
1 24 15 5 21 0 12 3 17 13 18 16 5 15 14 11 4 11 20

elde ederiz.

$C \equiv P + 3 (\mathrm{mod}\, 29)$ Caesar dönüşümünün uygulanmasıyla

4 27 18 8 24 3 15 6 20 16 21 19 8 18 17 14 7 14 23

Şifreleme Bilimi ve Şifreleme Teknikleri



Şifreleme Bilimi ve Şifreleme Teknikleri

- **EBCED HESABI**
- Ebced hesabı, Ebced rakamlarını yani alfabetik bir sayı sistemini kullanarak, kelimelerin sayısal değerini hesaplamaktır. Arap alfabesinin eski sıralanışından (elif, ba, cim, dal) ilk dört harfinin okunuşlarıyla (E-B-Ce-D) türetilmiş bir sözcüktür.

elif ا	1	Ha ح	8	sin س	60	te ت	400
be ب	2	Tı ط	9	`ayn ع	70	peltek se ث	500
cim ج	3	yâ ي	10	fe ف	80	Hı خ	600
dal د	4	kef ك	20	Sad ص	90	zel ذ	700
he ه	5	lâm ل	30	kaf ق	100	Dad ض	800
vav و	6	mim م	40	ra ر	200	Zı ظ	900
ze ز	7	nun ن	50	şın ش	300	ğayn غ	1000

Şifreleme Bilimi ve Şifreleme Teknikleri

- Özellikle Mimar Sinan'ın eserlerinde, boyutların modüler düzeninde çok sık kullanılmıştır.

- Süleymaniye'de zeminden kubbe üzengi seviyesi 45
- kubbe alemi 66 arşın yüksekliktedir .

- Ebced'e göre "Âdem' 45, "ALLAH" lafzı da 66 etmektedir.
- Yine Selimiye'de de kubbeyi taşıyan 8 ayağın merkezlerinden geçen dairenin çapı 45 arşındır.

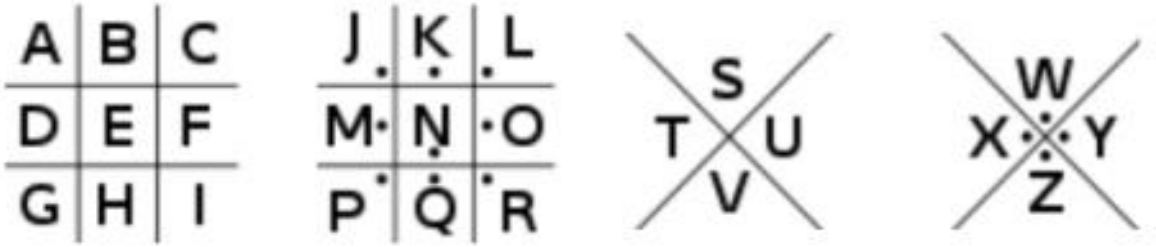
- Kubbe kenarı zeminden 45,
- minare alemi buradan itibaren 66 arşındır.
- Süleymaniye ve Selimiye'nin görünen silüetleri 92 arşındır
- bu da "Muhammed" kelimesinin ebced karşılığıdır.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Tarih düşürme sanatı**
- Ebced hesabının en fazla kullanıldığı yer hiç şüphesiz tarih düşürmedir.
- Bunun için o olayın tarihini verecek ustalıklı bir kelime veya mısra söylenir ki, hesaplandığında o olayın tarihi ortaya çıkar.
- "*Tarih düşürme sanatı*" adı verilen bu sanat divan edebiyatı boyunca kullanılmış ve kitabelerde yer almıştır.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Pigpen (Mason) Şifrelemesi**



Şifreleme Bilimi ve Şifreleme Teknikleri

- **Echelon Sistem**

- Dünyanın en büyük casusluk ağı olarak bilinir.

- Dünyadaki sayısal trafiğin %90 bu sistem ile dinlendiği iddia edilmektedir.
  - Belirli kelimeler sisteme girilerek bu kelimelerin geçtiği konuşmalar incelenmektedir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Diğer bir sistem ise **PROMİS** (Dava Yönetim Sistemi)

- Bu sistem ile;

  - Birçok ülkenin banka sisteminin kilitlenebileceği
  - Kontrollü mali krizler çıkarılabileceği
  - Uluslar arası ihalelere girecek şirketlerin dinlendiği

  İddia edilmektedir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **ENİGMA**
  - Elektromekanik bir şifre çözme makinesidir.
  - 1919 yılında geliştirilen makine Almanlar tarafından kullanılmıştır.
  - II. Dünya savaşında önemli bir rol oynamıştır.
  - İngilizler tarafından ele geçirilen bir gemide enigmanın kullanma kitabı ele geçirilmiştir.
  - II. Dünya savaşının bu sayede 1 yıl daha erken bittiği düşünülmektedir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Steganografi**
  - Eski Yunanca'da "gizlenmiş yazı" anlamına gelen bilgiyi gizleme bilimidir.
    - Resim
    - Ses
    - Video

    ortamlarına bilgiler gizlenebilir.

Şifreleme Bilimi ve Şifreleme Teknikleri

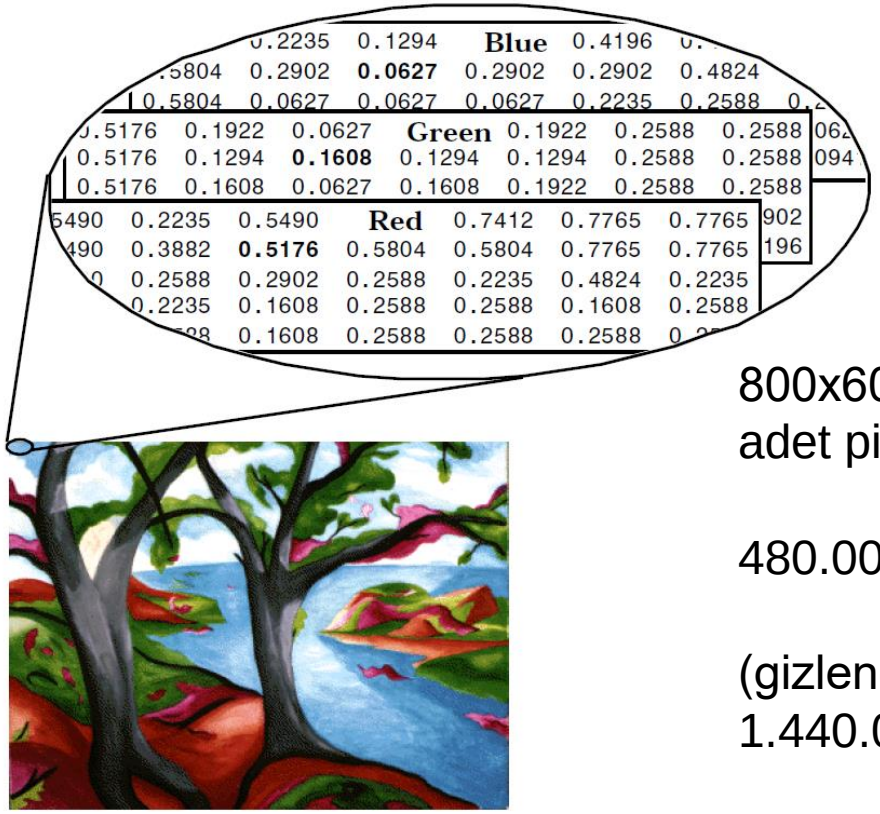
Bilginin Saklandığı Resim

Saklanan Resim

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Steganografi**
  - Resim dosyalarının özellikleri;
  - 1- Bütün resimler dosya başlığı (header) ve piksellerden oluşur.
  - 2- Her piksel sadece bir renk içeren küçük bir bloktur.
  - 3- Her pikseldeki renk temel 3 rengin karışımından elde edilir.
  - 4- Her pikselde bu 3 rengin verileri tutulur. Her temel renk 1 pikselde 1 byte (0..255) yer kaplar, yani 1 piksel 3 byte veri taşır.

Şifreleme Bilimi ve Şifreleme Teknikleri



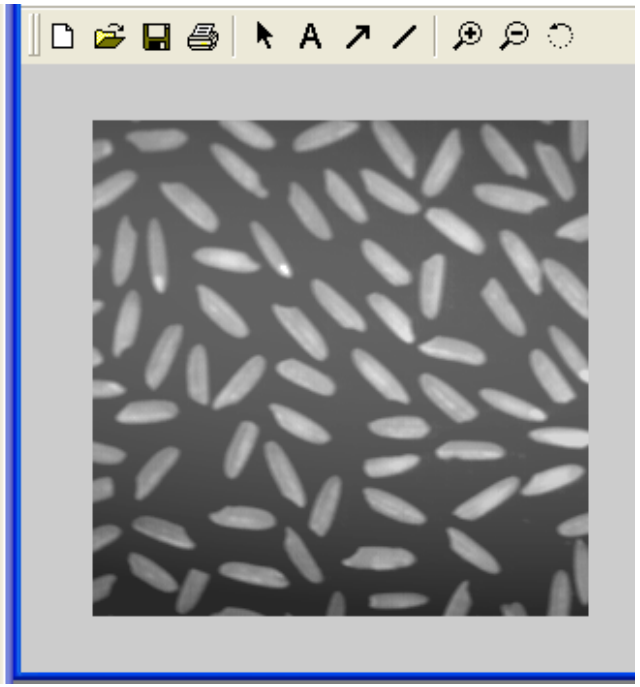
800x600 ebatında bir resimde 480.000 adet piksel bulunur.

480.000 x 3 bit = 1.440.000 bit

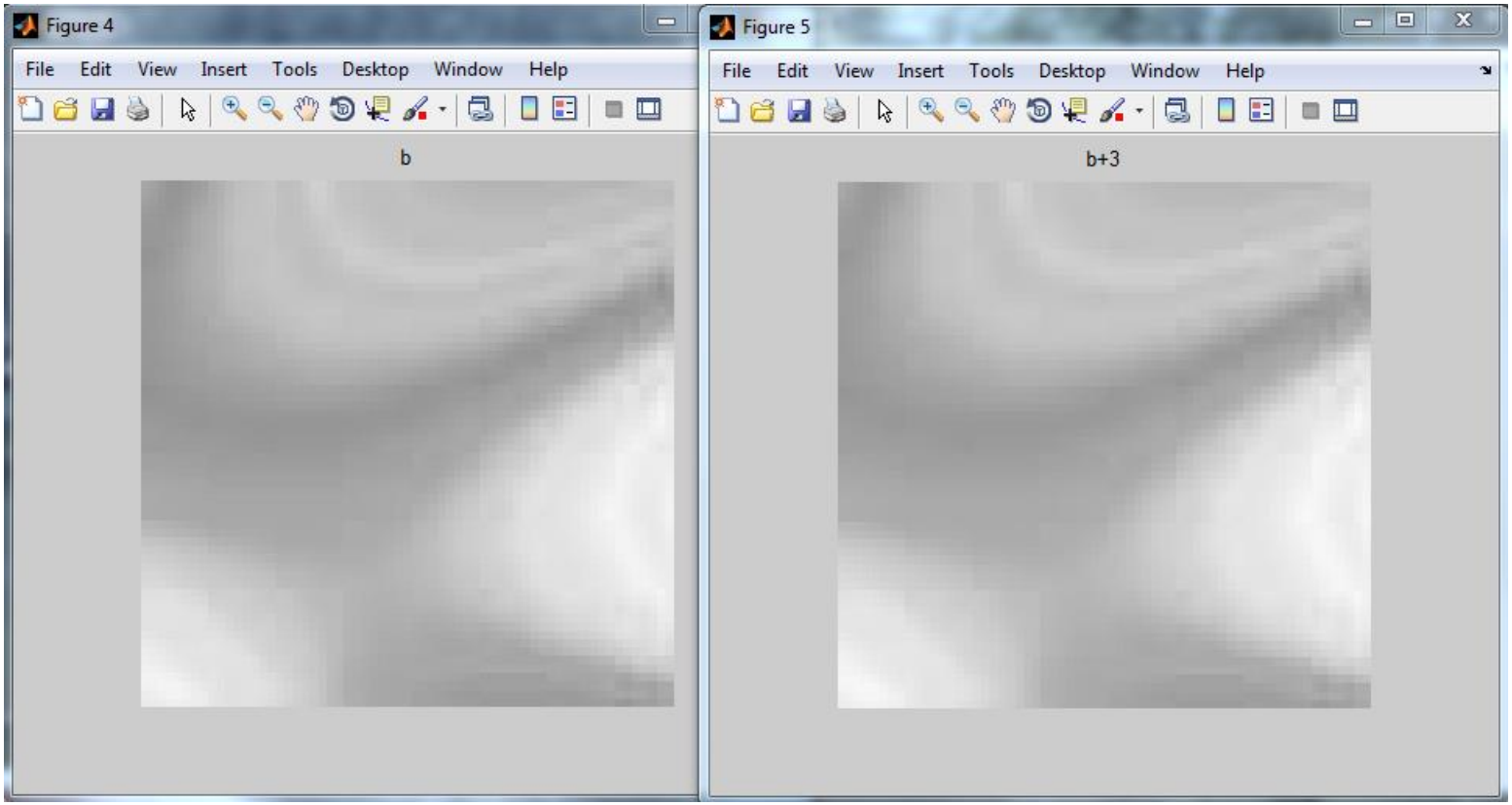
(gizlenecek olan veri için kalan yer)
1.440.000 bit = 175,7 KiloByte

Şifreleme Bilimi ve Şifreleme Teknikleri

1	2	3	4	5	6	7	8
81	80	81	81	81	81	81	81
81	81	81	82	81	81	81	81
82	81	81	81	81	82	81	81
81	82	82	82	82	82	82	82
82	82	82	82	82	82	82	82
82	82	82	82	82	82	82	82
82	83	83	83	83	83	83	83
83	83	83	83	83	83	83	83
83	83	83	84	84	84	84	84
91	90	96	97	98	100	100	97
112	113	118	120	120	126	126	123
131	132	135	135	136	142	146	143
145	145	146	145	147	153	159	162
148	149	149	149	148	155	166	169
152	148	149	149	150	160	174	179
152	149	149	152	152	166	177	184
157	153	155	155	157	168	177	175
161	155	155	157	152	163	158	155
160	158	152	152	144	141	133	124
156	151	146	136	127	118	110	99
143	135	128	115	109	98	94	88



Şifreleme Bilimi ve Şifreleme Teknikleri



Şifreleme Bilimi ve Şifreleme Teknikleri

- **HASH**

- Büyük tanım bölgelerini küçük değer bölgelerine dönüştürülür.

- Hash fonksiyonu girdi olarak bir mesajı alır ve ***hash kodu, hash sonucu, hash degeri*** veya kısaca ***hash*** ile belirtilen bir çıktı üretir.

- Daha kesin bir ifadeyle bir hash fonksiyonu keyfi sonlu boyutlu bit şeritlerini n-bit diyebileceğimiz sabit uzunluklu şeritlere dönüştürür.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **HASH**
- Başka bir ifadeyle hash fonksiyonu gönderilecek mesajdan matematiksel yollarla sabit uzunlukta sayısal bilgi üretme işlemidir.
- Üretilen sayısal bilgi ''mesaj özeti'' olarak bilinir. Mesaj özeti anlamsız bir bilgidir.
- Hash fonksiyonu geri dönüşümü olmayan bir fonksiyondur.
- Yani mesajın özetine bakarak mesajın kendisini elde etmek mümkün değildir. En iyi bilinen hash fonksiyonları MD-4, MD-5 ve SHA'dır.
- Örneğin; Sayısal İmzalama

Şifreleme Bilimi ve Şifreleme Teknikleri

- Bu süreci kimyasal bir reaksiyon gibi düşünebilirsiniz.
- Yumurta pişirildikten sonra yumurtanın eski haline dönüştürülmesi imkansızdır. Bu durumda hash sonucu karşıdaki bilgisayara gönderildiği esnada, orijinal mesajın da hash sonucuyla birlikte gönderilmesi gerekiyor.
- Alıcı bilgisayar, orijinal mesaja hash fonksiyonunu uygulayıp, çıkardığı sonucu kendisine orijinal mesajla gönderilen hash sonucuyla karşılaştırıyor.
- Eğer alıcı bilgisayarın oluşturduğu hash sonucu, mesajla birlikte
- gönderilen hash sonucuyla aynıysa, alıcı bilgisayar kendisine gelen orijinal mesajın üzerinde oynama yapılmadığından emin olmuş oluyor.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **MD5(Message-Digest algorithm5)**

- Tek yönlü (açık anahtarlı) şifreleme tekniğidir. Bir yere gönderilecek veri 128 bitlik özetler hâlinde şifrelenir.

- "**oktay**" kelimesi için MD5 şifreleme:

- f55694370a2e688a08edd2a3ee184e0d

Şifreleme Bilimi ve Şifreleme Teknikleri

- **SHA-1(Secure Hash Algorithm)**
- Tek yönlü (açık anahtarlı) şifreleme tekniğidir.Verileri 160 bit uzunluğunda özetler.
- Web alanında geniş kullanımı vardır.
- SHA-2 adı altında hazırlanmış 224, 256, 384, 512 bit uzunluğunda özetler üreten çeşitleri vardır.

Şifreleme Bilimi ve Şifreleme Teknikleri

Şifreleme Algoritması	Şifrelenecek Veri	Şifrelenmiş Veri
MD5	fatma	38ab93488e52710515c3095a83a92bcf
MD5	burak	39109a5bb10ccb7aff1313d369804b74
MD5	fırat	fbc06de89851f43007f2996a31e9f1b1
MD5	firat	e652dc5596070e8dc3fedfb32be655a6
SHA-1	fatma	5e927503d30f50bd44c9a31c6625984c442b78ae
SHA-1	burak	da7169592c4847350b7262ccf9f7b41b72c9d0be
SHA-1	firat.edu.tr	cdfe0a27180d66d4a4f69494c3f417786b15ba20
SHA-1	www.firat.edu.tr	26e8799f7d049f8fd908b597b7f4bd28c3f8edfd

Şifreleme Bilimi ve Şifreleme Teknikleri

Örneğin “**oktay**” kelimesinin SHA-1 ve SHA-2 özetleri aşağıdaki gibidir.

SHA-1 (160bit)	22771aca22f13b0e26b3011542bde186a5c47690
SHA-256	f6ff3f7aa48c6357fb3f9d09f8fdde97060e3121afc0db0e35ec807c62922456
SHA-384	d64f697923b1c8c425643c0f03f86c3c12b0af576521e41096cef9e95474661f947453a5ab2430928dfd02a381af93e2
SHA-512	278179b20946ee2cb093545ca8727f53607ba058acb2ed888aac8f32ecaf74d8572479ff6380fbf34be9c274080eeb1e7f055b32e3204ce2bda6afd1714ac75c

Şifreleme Bilimi ve Şifreleme Teknikleri

- **DES (Veri Şifreleme Standardı, Data Encryption Standard)**
- DES, veri şifrelemek ve şifrelenmiş verileri açmak için geliştirilmiş bir standarttır.
- Esas olarak kullanılan algoritmaya DEA yani Data Encryption Algorithm (Veri Şifreleme Algoritması) adı verilir.
- Bu algoritmanın standartlaştırılmış haline DES denilmektedir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **RSA Açık Anahtar Algoritması**

  RSA, güvenliği tam sayıları çarpanlarına ayrımanın algoritmik zorluğuna dayanan bir tür Açık anahtarlı şifreleme yöntemidir. 1978'de Ron Rivest, Adi Shamir ve Leonard Adleman tarafından bulunmuştur.

  Bir RSA kullanıcısı iki büyük asal sayının çarpımını üretir ve seçtiği diğer bir değerle birlikte ortak anahtar olarak ilan eder. Seçilen asal çarpanları ise saklar. Ortak anahtarı kullanan biri herhangi bir mesajı şifreleyebilir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Yeterince büyük iki adet asal sayı seçilir: Bu sayılar örneğimizde p ve
- q olsunlar.
- n=pq
- ϕ(n) = (p-1)(q-1) *(Totient değeri)*
- 1 < e < ϕ(n)
- d ≡ 1 mod (ϕ(n)). *(e'nin mod(φ(n)) çarpmaya göre tersi)*

- Şifreleme işlemi:
- c = me mod n

- Şifrenin Açılması:
- m = c
- d mod n

Şifreleme Bilimi ve Şifreleme Teknikleri

- İki farklı asal sayı seçelim. p=61 ve q=53 olsun.
- n=pq değerini hesaplayalım. $61 \times 53 = 3233$
- Totient değerini hesaplayalım. (61-1)(53-1)=3120
- 1 ile 3120 arasında 3120 ile aralarında asal olan bir değeri seçelim. e=17 olsun.
- d değeri, e'nin mod (3120)'e göre çarpmaya göre tersi olarak hesaplayalım. d=2753.
- **Ortak Anahtar: (n=3233, e=17)**
- Her bir m mesajını şifreleyecek fonksiyon $m^{17} \pmod{3233}$.
- **Özel Anahtar(n=3233, d=2753)**
- Herhangi bir c şifreli mesajını çözme fonksiyonu $c^{2753} \pmod{3233}$.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Örneğin;
- m=65 i şu şekilde şifreleriz. *(bitler)*
  - $c=65^{17}(\text{mod } 3233)=2790$.
  - c=2790'nın şifresini şu şekilde çözeriz.
    $m=2790^{2753}(\text{mod } 3233)=65$

Örneğin m=123 olsun:

17 mod 3233 = 855 olarak şifreli metin bulunur.
açacak taraf için tersi işlem uygulanır:

2753 mod 3233 = 123 şeklinde orijinal mesaj geri elde edilir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **BitLocker Şifreleme**

- Windows 7 işletim sistemi ile gelen özelliklerden biri de Bitlocker sürücü şifreleme özelliğidir.

- Windows'un eski versiyonlarında dosyalar ayrı ayrı şifrelenebiliyordu. Bu özellik sayesinde sürücünün kendisi şifrelenebilmektedir.

- Şifrelenmiş bir sürücüye yeni bir dosya attığımızda bu dosya bitlocker tarafından otomatik olarak şifrelenir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Ayrıca bitlocker ile yapılan şifreleme işlemlerinde şifreleme için gerekli dosyalarda sürücü içersinde depolanır.
- Dolayısıyla şifrelerimizi ele geçirmek isteyenler için gerekli olan bilgiler de sürücü içersinde muhafaza edilerek güvenlik düzeyi artırılmış oluyor.
- Bitlocker ile şifrelenmiş bir sürücüye erişmek için parola koruması yada akıllı kartlarda kullanabiliyoruz.
- Windows 7 de,Vista'dan farklı olarak harici depolama aygıtlarımızı da şifreleyebiliyoruz.Yani flash disklerimizi de şifreleyebiliyoruz.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **WEP Şifreleme**
- WEP (Wired Equivalent Privacy), kablosuz ağ Veri bağ tabakasında çalışan şifreleme yöntemidir.
- Standart olan WEP şifrelemesi WEP-64 olarak bilinir ve 40 bitlik anahtar kullanır.
- Günümüzde WEP kullanan ağlarda daha çok 104 bitlik anahtar kullanan WEP-128'e rastlanır. Daha güvenli ağlar 232 bitlik anahtarı mümkün kılan WEP-256 kullanıyor olabilir.
- Günümüzde bu şifreleme yetersiz kaldığından daha güvenli olan WPA şifreleme yöntemi yaratılmıştır

Şifreleme Bilimi ve Şifreleme Teknikleri

- **WPA Şifreleme**
  - WEP şifreleme sisteminden daha güvenli olduğu söylenen ve WEP şifrelemeden daha yeni bir teknolojidir.
  - WPA (Wi-Fi Protected Access)Wi-Fi korumalı Erişim olarak adlandırılır.WPA , WEP'in açıklarını geçici olarak da olsa kapatmaya yönelik bir standarttır.
  - İki modda çalışır.
  - Birincisi WPA-PSK denilen paylaşımlı anahtar koruması ,
  - İkincisi ise yeni protokol olan TKIP(Temporal Key Integrity Protocol)'in şifrelemesi ve 802.1X asıllama ile güvenliktir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **WPA Şifrelemesi**
- İstemci ile AP (Erişim Noktası) bağlantı kurmadan önce, aygıtların birbirini bulması gerekiyor.
- Mevcut WLAN ağlarının bir listesini görüntülemek için, istemci “araştırma sorgusu” gönderir.
- Yani “*Merhaba, biri var mı*?” mesajıdır bu.
- “*Evet, burdayız*” diye karşılık gelince daha sonra AP’ler SSID bilgisini (Hizmet Kümesi Tanımlayıcı) yani WLAN’ın
- ismini
- zaman bilgisini
- ve diğer bilgileri aktarır.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Daha sonra istemci “Açık Sistem İsteği” (Open System Request) göndererek ağlara şifreli olup olmadıklarını soruyor.
- Yönlendirici de buna uygun yanıtı veriyor.
- İstemcinin sıradaki adımı ise, yönlendiriciden kendisini ağa dahil etmesini istemek.
- Bu “Bağlanma İsteği”ne AP’den bir “Bağlanma Yanıtı” geliyor.
- Eğer sistem şifresiz ise, istemci “Açık Sistem Doğrulama” (OSA) ile kimliğini doğruluyor.
- AP bunun üzerine kimlik saptamanın başarılı olduğunu belirten bir ileti yayınlayıp bağlantıyı kuruyor.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Şifreli bir bağlantı kurmak içinse;**
  - WPA'nın da kendi içinde iki çeşidi var:
  - Biri işyerlerine, diğeri ise küçük özel ağlara yöneliktir.
  - Aralarındaki fark;
  - Bağlantı kurma sırasında, istemcinin sizin belirlediğiniz bir parolayı, yani PSK (önceden paylaşılmış anahtar) kullanılıyor olması
  - Şirket WLAN'larında ise anahtar dağıtımından sorumlu "*Radius server*" adlı özel bir sunucunun PSK'nın yerine geçiyor olması

Şifreleme Bilimi ve Şifreleme Teknikleri

- WPA'nın ilk adımında;
- İstemci ile erişim noktası, WLAN ağ adı SSID'yi, ana parola olarak kullanarak bir PMK (eşleştirme ana anahtarı) oluşturuyorlar.
- Aygıtlar şu anda PMKSA (Eşleştirme Ana Anahtarı Güvenlik Bağlantısı) denilen bir konumda bulunuyor.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Daha sonra taraflar, adına PTK (Geçici Eşleştirme Anahtarı) denilen 512 bitlik bir anahtar daha oluşturuyorlar.
- Bunun için de aygıtlar 4 taraflı bir el sıkışma protokolü uyguluyor.
- Yönlendirici, öncelikle istemciye içinde rasgele rakam bulunan bir çerçeve yolluyor.
- Bu ileti şifresiz olduğundan,kablosuz ağ üzerinden salt metin olarak iletiliyor.Ancak bu,güvenliği tehlikeye atmıyor çünkü en kötü durumda 4 taraflı el sıkışma başarısız oluyor ve yönlendirici bu işlemi yeni baştan başlatıyor.

Şifreleme Bilimi ve Şifreleme Teknikleri

- İstemci ise aşağıdaki parametreleri kullanarak PTK (Geçici Eşleştirme Anahtarı)'yi oluşturuyor:

- SNonce (gelişigüzel bir sayı)
- ANonce (AP için bir gelişgüzel sayı)
- PMK (Eşleştirme Ana Anahtarı) ve aygıtların MAC adresleri.

Şifreleme Bilimi ve Şifreleme Teknikleri

- PTK (Geçici Eşleştirme Anahtarı)'dan yönlendirici ve istemci tarafından dört geçici anahtar daha elde ediliyor:

- EAPOL anahtarı-şifreleme anahtarı
- EAPOL anahtarı-doğrulama anahtarı (bu sayede aygıtlar daha sonra asıl veri anahtarının aktarımını şifreleyebiliyor),
- veri şifreleme anahtarı
- ve veri doğrulama anahtarı.

- Bunların hepsi de 128 bit uzunluğundadır.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Sıradaki ileti, istemciden yönlendiriciye gidiyor ve SNonce(gelişigüzel bir sayı)'ı içeriyor. Böylece yönlendirici aynı PTK'yi hesaplayabiliyor.
- Bağlantı henüz şifrelenmemiş olsa da, değişiklikleri saptayan MIC algoritması (Mesaj Doğruluk Denetimi) üzerine kuruludur.
- Gönderici, veri paketlerini seri olarak numaralıyor. Seri numarası da mesaja ekleniyor.
- Alıcı, seri numarası verilen paketleri kontrol ediyor ve paketler eşleşmezse, alıcı bu paketleri çöpe atıyor. Bu da çoğu korsan saldırısını daha en baştan eliyor.

Şifreleme Bilimi ve Şifreleme Teknikleri

- 4 taraflı el sıkışmanın üçüncü aşamasında yönlendirici istemciye bir “başarılı” paketi göndererek iki aygıtın da aynı geçici anahtara sahip olduğunu doğruluyor.
- El sıkışmasını sona erdirmek için, istemci, yönlendiriciye anahtar oluşturmanın sonlandığını belirten bir MIC mesajı gönderiyor.
- Bunun üzerine, yönlendirici, MIC’i kullanarak mesajı kontrol ediyor ve üzerindeki anahtarları etkinleştiriyor.

Kaynaklar

- [1] IEEE Std 802.16-2004--IEEE standard for local and metropolitan areanetworks, part 16: "***Air Interface for Fixed Broadband Wireless Access Systems***".
- [2] David Johnston ve Jesse Walker--INTEL: "***Overview of IEEE 802.16 Security***"
- [3] Kitti Wongthavarawat--Thai Computer Emergency Response Team (ThaiCERT) National Electronics and Computer Technology Center,Thailand: "***IEEE 802.16 WiMax Security***"
- [4] Loutfi Nuaymi, Patrick Maillé, Francis Dupont, Raphaël Didier--École Nationale Supérieure des Télécommunications de Bretagne:"***Security issues in WiMAX/IEEE 802.16 BWA System***"
- [5] Yun Zhou ve Yuguang Fang--Department of Electrical and Computer Engineering,University of Florida, Gainesville:"***Security of 802.16 in Mesh Mode***"

YMT 311-Bilgi Sistemleri ve Güvenliği

Ağ Güvenliği

Konu Başlıkları

- Wireshark
- Wimax
- Güvenli İşletim Sistemleri

Wireshark

- Wireshark,1998 yılında Ethereal adıyla faaliyete başlayan bir projedir.
- Wireshark ismiyle çıkan bu yazılım bilgisayara ulaşan paketleri yakalamaya ve bu paketlerin içeriğini görüntülemeye imkan tanır. Bir başka deyişle bilgisayara bağlı olan her türlü ağ kartlarındaki (Ethernet kartı veya modem kartı) tüm TCP/IP mesajlarını analiz eden bir programdır.
- Wireshark günümüzde çok amaçlı kullanılmaktadır.
- *Şebeke problemlerinde sorun çözme
- *Güvenlik problemlerini sınamak
- *Uygulamaya konan protokollerde oluşan hataları onarmak veya arındırmak
- *Ağ problemlerinin içindeki bilgileri öğrenebilmek amacıyla kullanılmaktadır.

WiRESHARK ÖZELLİKLERİ

- Windows,Unix,OS X,Solaris,FreeBSD,NetBSD ve birçok işletim sistemleri için uygundur.
- Yerel ağ arayüzünden paketleri tutar, ayrıntılı bir şekilde protokol bilgileriyle görüntüler.
- Tutulan bilgileri kaydetme özelliği vardır.
- Çeşitli kriterlerde paket arar ve filtreler.
- Çeşitli istatistikleri yapılan ayarlar doğrultusunda kullanıcıya sunar.
- Birçok protokol için şifre çözme desteği sunar. (IPsec,ISAKMP,Kerberos,SNMPv3, SSL/TLS, WEP, ve WPA/WPA2'yi içerir).

Wireshark kullanimi ile ilgili örnekler

- Ağ trafik tespiti
- Veri madenciliği
- Saldırı tespiti
- Port tarama tespiti
- Virüslerin bulaştığını veya Denial of Service(Dos) ataklarını bulma tespiti
- Bağlantı sorunu tespiti
- Casus yazılım tespiti

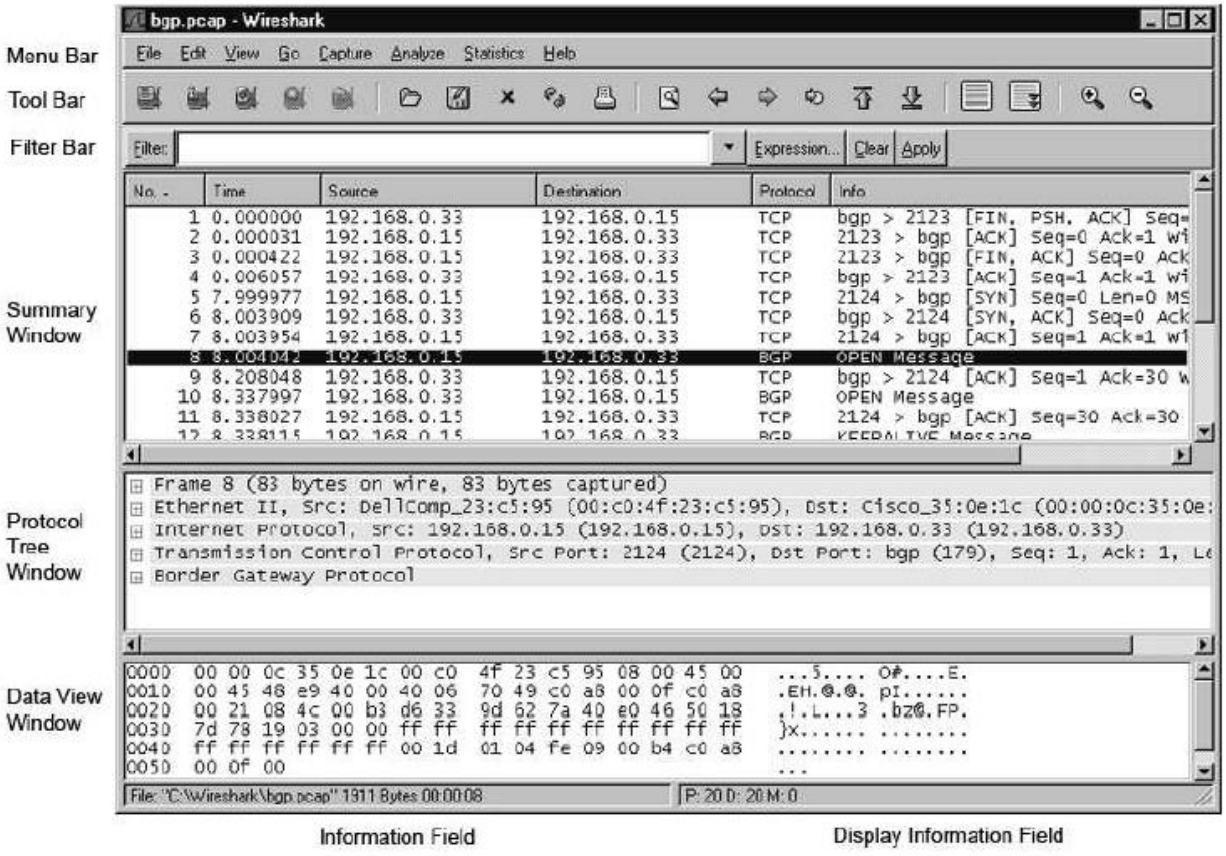
Wireshark bileşenleri

- Wireshark iletişim ağının iç yüzünde neler olduğunu kavramamızı sağlar.
- Bu özelliğiyle; uygulama protokollerinde, ağ uygulamalarındaki sorunları
- çözmede, ağı test etmede ve canlı ağ bağlantılarındaki sorunları
- çözmemizde bize yardımcı olur. Yani, iletişim ağı ile teknik düzey
- arasında etkileşim sağlayarak pek çok problemi çözmemizi sağlar. Bu
- bölümde wireshark'ın grafiksel kullanıcı ara yüzündeki ana bileşenleri
- tanımlayacağız :

Wireshark bileşenleri

- Main window
- Menu bar
- Tool bar
- Summary window
- Protocol Tree window
- Data View window
- Filter bar
- Information field
- Display information

Wireshark Görseli



ANA PENCERE (MAIN WINDOW)

Menu Bar	Menudeki maddelerin, grafiksel ara yüzünü içeren klasik bir uygulamadır.
Tool Bar	Wireshark'ın sık kullanılan fonksiyonlarının kısa yollarını içerir. Kullanıcıya göre ayarlanabilir.
Filter Bar	Yakalanan paketleri, istenilen sekilde ayrılarak gösterilmesini sağlar.
Summary Window	Yakalan paketlerin her biri için, bir satırlık özet bilgi sunar.
Protocol Tree Window	Summary window 'da seçili olan paketin detaylı bilgilerini, kullanıcıların anlayacağı şekilde düzenleyerek sunar.
Data View Window	Summary Window 'da seçili olan paketin, detaylı bilgilerini, herhangi bir düzenleme yapmadan sunar.
Display Information Field	Yakalanmış paketlerin numaralarını, güncel olarak gösterir.

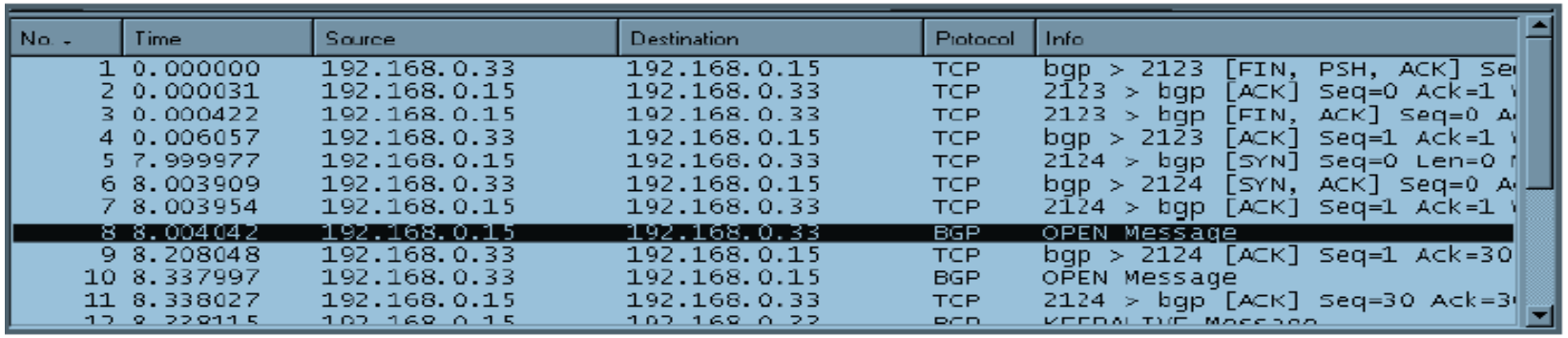
SUMMARY WINDOW

- Yakalanmış paketlerin tamamına buradan bakılabilir. Her bir dosyanın içeriği bir satır olarak sunulur, satırlar belli özelliklerine göre sütunlara ayrılır.

Sütun adı	Tanımı
No	Yakalanan dosyanın içindeki paketlerin numarasını temsil eder. Görüntüleme filtresi (display fitler)kullanılmadığı sürece bu numara değiştirilemez.
Time	Paketin zaman damgasıdır.
Source	Paketin nereden geldiğini gösterir.
Destination	Paketin nereye gittiğini gösterir.
Protocol	Protokol isminin kısa versiyonudur.
Info	Paket içeriği hakkında ekstra bilgi gösterir.

SUMMARY WINDOW

- Bu dosyalar daha ayrıntılıda incelenebilir. Herhangi bir dosya seçilirse "Packet Details" ve "Packet Bytes" pencereleri açılır. Bir paketin içeriğine bakılacak olursa, Ethernet paketinin içinde IP, onun içinde TCP bulunur. Ethernet tarayıcısı kendi bilgisini(örneğin Ethernet Adresleri) yazar, IP tarayıcısı onun üstüne kendi bilgisini(örneğin IP adresleri) yazar ve TCP tarayıcısı da onun üstüne IP bilgisini yazacaktır.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.33	192.168.0.15	TCP	bgp > 2123 [FIN, PSH, ACK] Se
2	0.000031	192.168.0.15	192.168.0.33	TCP	2123 > bgp [ACK] Seq=0 Ack=1
3	0.000422	192.168.0.15	192.168.0.33	TCP	2123 > bgp [FIN, ACK] Seq=0 A
4	0.006057	192.168.0.33	192.168.0.15	TCP	bgp > 2123 [ACK] Seq=1 Ack=1
5	7.999977	192.168.0.15	192.168.0.33	TCP	2124 > bgp [SYN] Seq=0 Len=0
6	8.003909	192.168.0.33	192.168.0.15	TCP	bgp > 2124 [SYN, ACK] Seq=0 A
7	8.003954	192.168.0.15	192.168.0.33	TCP	2124 > bgp [ACK] Seq=1 Ack=1
8	8.004042	192.168.0.15	192.168.0.33	BGP	OPEN Message
9	8.208048	192.168.0.33	192.168.0.15	TCP	bgp > 2124 [ACK] Seq=1 Ack=30
10	8.337997	192.168.0.33	192.168.0.15	BGP	OPEN Message
11	8.338027	192.168.0.15	192.168.0.33	TCP	2124 > bgp [ACK] Seq=30 Ack=3

Tablo 1.3 : Summary Window Sütunu

SUMMARY WINDOW

- Gözüktüğü gibi bu paket; Border Gateway Protocol (BGP) oturumunda, *192.168.0.15* ve*192.168.0.33* adresleri arasında yakalanmıştır. Bu paket seçilerek, açılan "Protocol Tree Window" ve "Data View Window" bölümlerinden daha da ayrıntılı incelenebilir.

PROTOCOL TREE WINDOW

- Paketi bütün protokollerin bir üst ağacı (tree) olarak canlandıralım. Her bir protokol için ağaç düğümü(tree node) oluşturulur. Bu ağaç düğümleri sayesinde, protokol alanı Daha geniş bir şekilde tanımlanabilir. Herhangi bir ağaç düğümünün alt ağaca sahip olması, Onun daha geniş bilgiler gösterecek şekilde genişletilebileceğini veya sadece özet bilgiler gösterecek şekilde daraltılabileceğini gösterir. Protocol tree window, wireshark'ın paketi çözümleyerek oluşturduğu ağacı denetleme imkanı sunmaktadır.

PROTOCOL TREE WINDOW

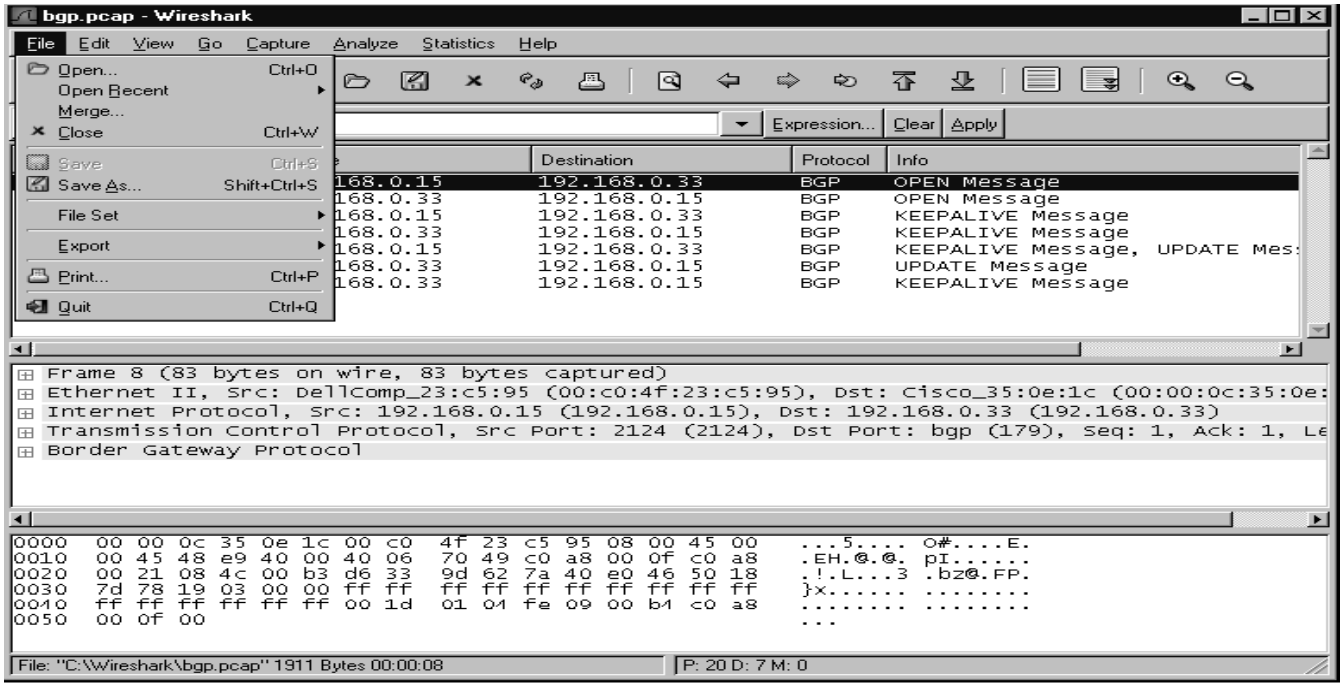
Wireshark arayüzü ;menü çubuğu, araç çubuğu, görüntüleme filtresi çubuğu, özet Alanı, protokol ağacı alanı ve veri alanı olmak üzere 6 bölümden oluşur. Menü Çubuğu;

- File (Dosya Menüsü)
- Edit (Ekleme Menüsü)
- View (Görüntü Menüsü)
- Go (Git Menüsü)
- Capture (Yakalama Menüsü)
- Analyze (Analiz Menüsü)
- Statistics (Statik Menüsü)
- Help (Yardım Menüsü)

olmak üzere 8 bölümden oluşmaktadır.

File(dosya menüsü)

- Bu menü dosya açma, kaydetme,yazdırma gibi temel işlevleri yapabileceğimiz bölümdür.



Tablo 1.4

File(dosya menüsü)

- Open (*ctrl+O*): Hazırda var olan önceden kaydedilmiş wireshark ya da başka
- desteklediği paket analiz yazılımlarının ürettiği dosyaları görüntülemek için
- kullanılır.
- Open Recent(Son dosyayı aç): Son kullanılan dosyaları açmada kolaylık sağlar.
- Merge(Birleştir): Kaydedilmiş dosyaları birleştirmede kullanılır.
- Close (*ctrl+W*): Açık olan dosyadan çıkar.
- Save (*ctrl+S*): Görüntülenmekte olan paketleri kaydeder.
- Save As (*ctrl+shift+S*): Farklı kaydeder.
- File Set(Dosya Ayarları):
- List Files(Dosya Listesi):Dosya listesini oluşum tarihi, son değişim tarihi, boyutu
- Şeklinde dosya dizisi içerisinde gösterir.
- Next File(Sonraki dosya): Dosya dizisi içinde varolanı kapatıp sonrakine atlar
- Previous File(Önceki dosya): Dosya dizisi içinde varolanı kapatıp bir öncekine atlar.

Export

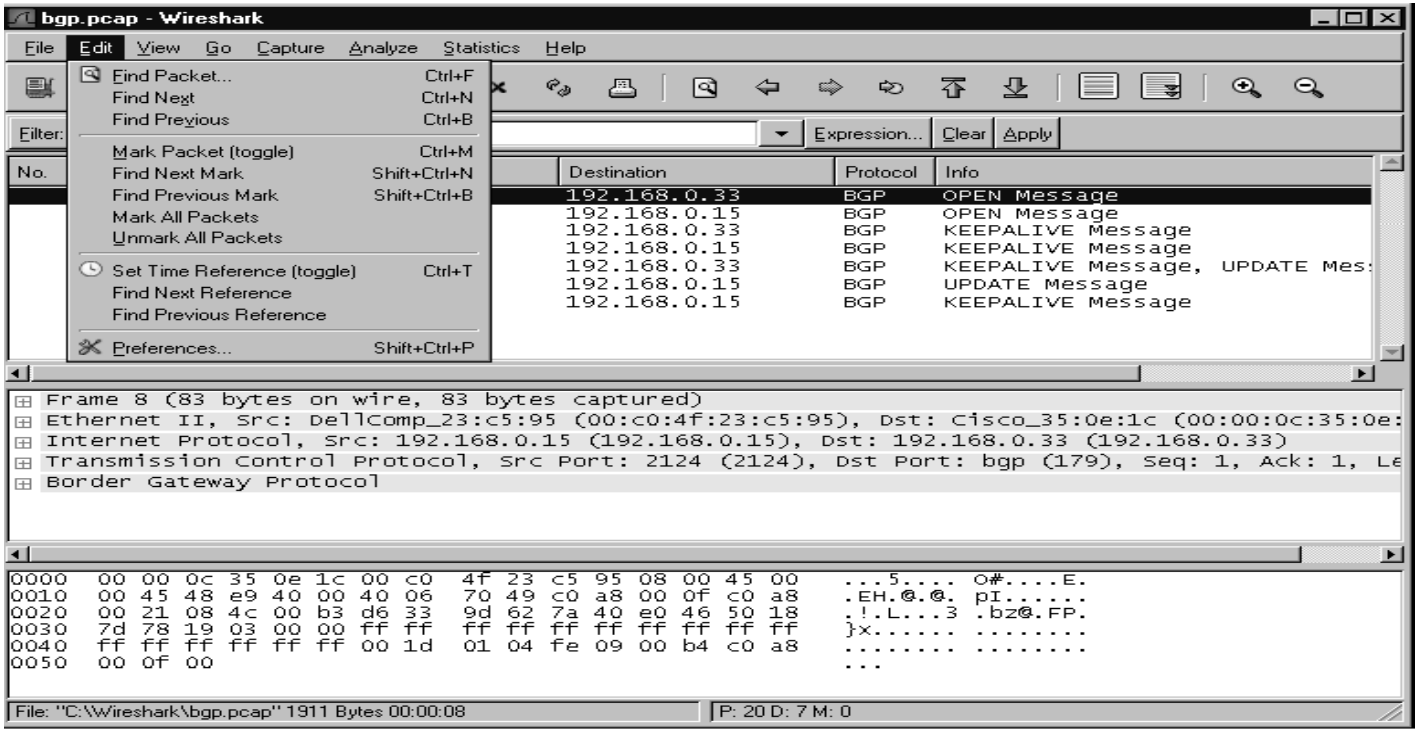
- As “Plain Text” File: Toplanan paketleri metin dosyası olarak dışa aktarmaya yarar. Özet ve ayrıntı bölümlerini aktarır.
- As “PostScript” File: İstenen paketleri postscript dosyası olarak dışa aktarmaya yarar. Wireshark seçilen ayrıntı bölümü bilgilerini aktarır.
- As "CSV" (Comma Separated Values packet summary) File: Wireshark özet bölümündeki bilgileri virgülle ayrılmış şekilde düz metin dosyası olarak dışa aktarır.
- As “C Arrays” Paket Bytes File: Paket veri değerlerini hex byteları olarak aktarır.
- As XML ”
- PSML” (Packet Summary) File: Paketleri PSML (packet summary markup language) XML
- dosya formatında dışa aktarmaya yarar.
- As "PDML" File: Paketleri PDML (packet details markup language) XML dosyası
- olarak aktarmaya yarar.

Selected Packet Bytes

- Objects > http : Paketler içerisinden http protokollü paketleri ve Objelerini dışarı aktarmaya yarar.
- Print (*ctrl+P*):Seçilen paketleri yazdırmaya yarar.
- Quit(*ctrl+Q*):Programdan çıkar.

Edit

- Edit menüsü kullanıcı tanımlı işlemleri ve paket arama gibi işlemleri yapmamızı sağlar. Edit menüsünün içeriği gösterilmiştir.



Edit

- Copy (*Shift+ctrl+C*): Veri bölmesinden tıklanan değeri filtre ifadesi olarak kopyalar. İstenilen bölüm seçilerek sağ fare menüsünden de yapılabilir .
- Find Packet (*ctrl+F*): Birçok kritere göre arama yapmanıza imkan sağlar. Display filter seçeneği seçiliyse wireshark filtreleme kriterlerine göre arama yapar. Basit protokol taramalarından kuvvetli filtreleme ifadelerine kadar birçok türde etkin arama yapabilirsiniz.
- Hex Value:Paket veri kümesi içerisinde belirtilen hex değerlerinde arama yapar.
- String: Girilen string i liste, ayrıntı ya da veri alanlarında belirlenen kriterlere göre arar .String options alanından arama büyük küçük harf duyarlı ve karakter seti belirtilerek yapılabilir. Direction alanında ise taramanın aşağı yada yukarı yapılacağı belirtilir.
- Find Next (*ctrl+N*): Belirlenen kriterde bir sonraki paketi bulur.
- Find Previous (*ctrl+B*) : Belirlenen kriterde bir önceki paketi bulur.

Edit

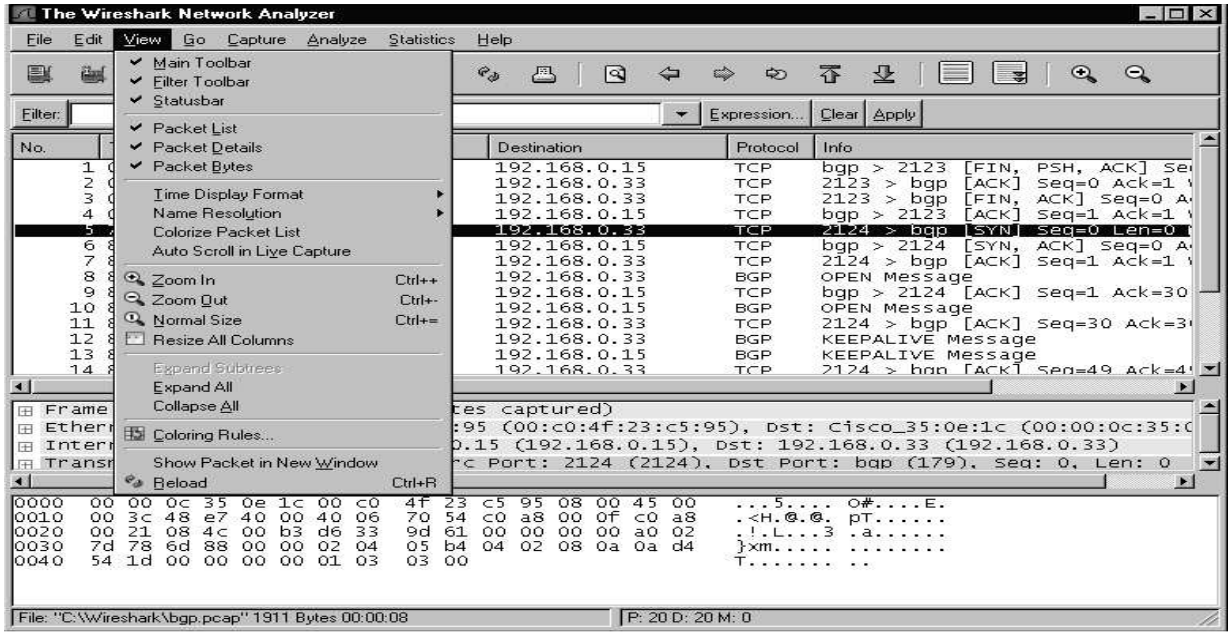
- Mark Packet (*ctrl+M*) : Seçilen paketi işaretler.
- Find Next Mark (*shift+ctrl+N*) : Bir sonraki işaretli paketi bulur.
- Find Previous Mark (*shift+ctrl+B*) : Bir önceki işaretli paketi bulur.
- Mark All Packet: Bütün paketleri işaretler.
- Unmark All Paket: Bütün işaretleri kaldırır.
- Set Time Referance (*ctrl+T*): Seçilen paketi zaman referansı olarak alır ve sonraki paketlerde o pakete göre zaman değerleri alır.
- Find Next Referance: Bir sonraki referans alınan paketi bulur.
- Find Previous Referance: Bir önceki referans alınan paketi bulur.
- Configuration Profiles (*shift+ctrl+A*): Profil ekle sil işlemlerini yapar.
- Preference (*shift+ctrl+P*): Programla ilgili ayarlamaları yaptığımız bölümdür.
- User İnterface bölümünde program için pencere düzeni, renk, font ayarlamaları ve bunlar gibi görünümü kişiselleştirmeye yarayan seçenekler bulunur.

Edit

- Capture : Paketleri yakalamak için kullanılacak default ağ arabirimi, eş zamanlı paket görüntüleme ve promiscouos mod seçimi (promiscouos mod : Yönlendirme olmadan bütün paketlerin bütün istemcilere dağıtıldığı durumda paketin hedefine bakılmadan bütün paketlerin takibi olayıdır. Root yetkisi gerektirir.), otomatik kaydırma çubuğu hareketi, ve yakalanan paketlerin türlerine göre sayıları ve % oranlarını veren info penceresinin saklanması seçenekleri bulunur.
- Printing: Yazdırmak için gereken ayarlar bulunmaktadır. Dosya çıktısı konumu, yazdırma komutu ve çıktı türü “düz metin ya da post script seçenekleri” Bulunmaktadır .Varsayılan yazdırma komutu lpr dir.
- Name Resolutions: Adres dönüşüm işlemlerini etkinleştirebileceğiniz alandır.
- Protocols: ihtiyaca göre wireshark üzerinde paketlerin protokollere göre kullanım ayarlamalarını yapabileceğiniz bölümdür.

View

- Wireshark ana ekranımızın görüntüsünü düzenlememizi sağlayan menüdür.
- Toolbar lar eklenebilir, çıkarılabilir, paketlere özel renk ayarları yapılabilir.



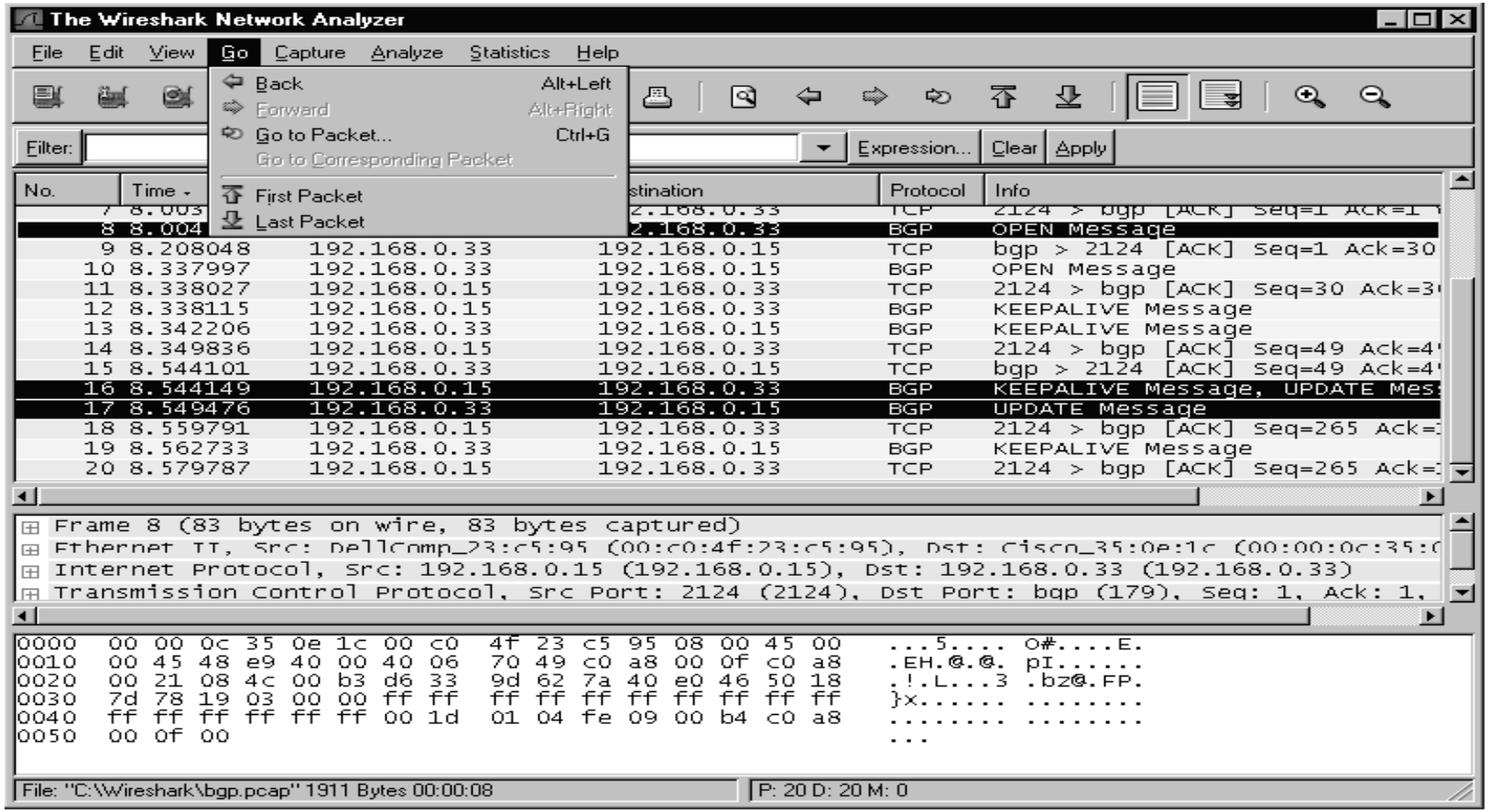
View

- Packet Details(Paket Detayları): Paketlerin detaylarını ASCII kodunda gösteren
- Bölgeyi ekler ya da kaldırır.
- Packet Bytes: Data Window penceresini ekler ya da kaldırır.
- Time Display Format Summary: Window da zaman görünümün nasıl gözükeceğini ayarlamamızı sağlar.
- Colorize Packet List: Paketlerin renk özelliğini açar ya da kapar.
- Auto Screen in Live Capture: Summary Windowun güncellenmesini açıp kapamaya yarar.
- Zoom In: Font ve column size ları büyütmeye yarar.
- Zoom Out: Font ve column size ları küçültmeye yarar.
- Normal Size: Zoom In ve out la büyütüp küçülttüğümüz fontları default değere döndürmemizi sağlar.
- Expand Subtrees: Protocol tree deki seçili alt diziyi açar.

View

- Expand All: Protocol tree deki bütün alt dizileri açar.
- Collapse All: Protocol tree deki bütün alt dizileri kapatır.
- Coloring Rules: Paketler için Renk ayarlarını yapmamızı sağlar.
- Show Packet in New: Window Paket detaylarını yeni bir pencerede görmemizi sağlar.

Go

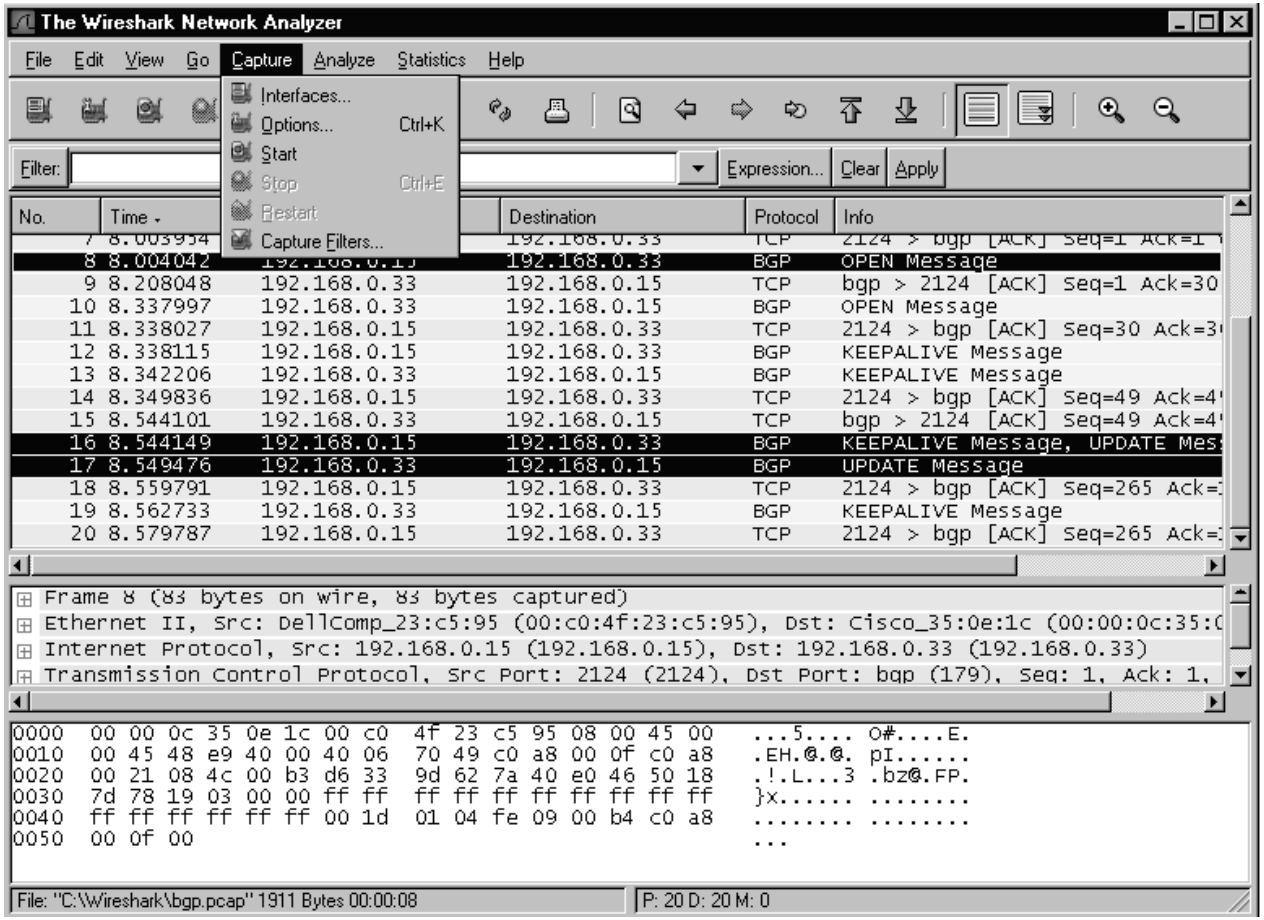

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Back Alt+Left
Forward Alt+Right
Go to Packet... Ctrl+G
Go to Corresponding Packet
First Packet
Last Packet
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
8 8.004 2.168.0.33 BGP OPEN Message
9 8.208048 192.168.0.33 192.168.0.15 TCP bgp > 2124 [ACK] Seq=1 Ack=30
10 8.337997 192.168.0.33 192.168.0.15 BGP OPEN Message
11 8.338027 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=30 Ack=3
12 8.338115 192.168.0.15 192.168.0.33 BGP KEEPALIVE Message
13 8.342206 192.168.0.33 192.168.0.15 BGP KEEPALIVE Message
14 8.349836 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=49 Ack=4
15 8.544101 192.168.0.33 192.168.0.15 TCP bgp > 2124 [ACK] Seq=49 Ack=4
16 8.544149 192.168.0.15 192.168.0.33 BGP KEEPALIVE Message, UPDATE Mes
17 8.549476 192.168.0.33 192.168.0.15 BGP UPDATE Message
18 8.559791 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=265 Ack=
19 8.562733 192.168.0.33 192.168.0.15 BGP KEEPALIVE Message
20 8.579787 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=265 Ack=
Frame 8 (83 bytes on wire, 83 bytes captured)
Internet Protocol, Src: 192.168.0.15 (192.168.0.15), Dst: 192.168.0.33 (192.168.0.33)
Transmission Control Protocol, Src Port: 2124 (2124), Dst Port: bgp (179), Seq: 1, Ack: 1,
0000 00 00 0c 35 0e 1c 00 c0 4f 23 c5 95 08 00 45 00 ...5.... O#....E.
0010 00 45 48 e9 40 00 40 06 70 49 c0 a8 00 0f c0 a8 .EH.@.@. pI......
0020 00 21 08 4c 00 b3 d6 33 9d 62 7a 40 e0 46 50 18 .!.L...3 .bz@.FP.
0030 7d 78 19 03 00 00 ff ff ff ff ff ff ff ff ff ff }x...... ....
0040 ff ff ff ff ff ff 00 1d 01 04 fe 09 00 b4 c0 a8 ....
0050 00 0f 00 ...
File: "C:\Wireshark\bgp.pcap" 1911 Bytes 00:00:08
P: 20 D: 20 M: 0

Tablo 1.7

Go

- Back (*ctrl+sol*): Bir önceki baktığınız pakete atlar.
- Forward (*ctrl+sağ*): Ziyaret edilen bir sonraki pakete zıplar.
- Go To Packet (*ctrl+G*): Paket numarasına göre istenilen pakete zıplar.
- Go To Corresponding Packet: Seçilen pakete karşılık gelen pakete zıplar .
- Previous Packet (*ctrl+yukarı*): Seçili paketten önceki pakete zıplar.
- Next Packet (*ctrl+aşağı*): Seçili paketten sonraki pakete zıplar.
- First Packet: Yakalanan ilk pakete zıplar.
- Last Packet: Yakalanan son pakete zıplar.

Capture


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Interfaces...
Options... Ctrl+K
Start
Stop Ctrl+E
Restart
Capture Filters...
Filter:
Expression... Clear Apply
No. Time Destination Protocol Info
8 8.004042 192.168.0.33 BGP OPEN Message
9 8.208048 192.168.0.33 192.168.0.15 TCP bgp > 2124 [ACK] Seq=1 Ack=30
10 8.337997 192.168.0.33 192.168.0.15 BGP OPEN Message
11 8.338027 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=30 Ack=3
12 8.338115 192.168.0.15 192.168.0.33 BGP KEEPALIVE Message
13 8.342206 192.168.0.33 192.168.0.15 BGP KEEPALIVE Message
14 8.349836 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=49 Ack=4
15 8.544101 192.168.0.33 192.168.0.15 TCP bgp > 2124 [ACK] Seq=49 Ack=4
16 8.544149 192.168.0.15 192.168.0.33 BGP KEEPALIVE Message, UPDATE Mes
17 8.549476 192.168.0.33 192.168.0.15 BGP UPDATE Message
18 8.559791 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=265 Ack=
19 8.562733 192.168.0.33 192.168.0.15 BGP KEEPALIVE Message
20 8.579787 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=265 Ack=
Frame 8 (83 bytes on wire, 83 bytes captured)
Ethernet II, Src: DellComp_23:c5:95 (00:c0:4f:23:c5:95), Dst: Cisco_35:0e:1c (00:00:0c:35:0
Internet Protocol, Src: 192.168.0.15 (192.168.0.15), Dst: 192.168.0.33 (192.168.0.33)
Transmission Control Protocol, Src Port: 2124 (2124), Dst Port: bgp (179), Seq: 1, Ack: 1,
0000 00 00 0c 35 0e 1c 00 c0 4f 23 c5 95 08 00 45 00 ...5.... O#....E.
0010 00 45 48 e9 40 00 40 06 70 49 c0 a8 00 0f c0 a8 .EH.@.@. pI......
0020 00 21 08 4c 00 b3 d6 33 9d 62 7a 40 e0 46 50 18 .!.L...3 .bz@.FP.
0030 7d 78 19 03 00 00 ff ff ff ff ff ff ff ff ff ff }x...... ....
0040 ff ff ff ff ff ff 00 1d 01 04 fe 09 00 b4 c0 a8 ....
0050 00 0f 00 ...
File: "C:\Wireshark\bgp.pcap" 1911 Bytes 00:00:08
P: 20 D: 20 M: 0

Capture

- İnterfaces: Wiresharkın kullanacağı ağ arabirimi ve özellikleri ayarlanır.
- Options: Uygulama sırasında kullanılacak ağ arabirimi seçimi adres çözümleme özellikleri, görünüm özellikleri uygulama durdurmak için ayarlanacak özellikler gibi bir çok ayarlanabilir bölüm içermektedir.
- IP address: Seçilen ağ arabirimin sahip olduğu ip adresidir.
- Limit each packet to n bytes : Paket yakalama işlemi sırasında uyulacak tampon sınırdır. Seçili olmadığı durumda default değeri 65535 bytes tır. Default değerde bırakmanız önerilir.
- Capture packets in promiscuous mode : Hub kullanılan ağlarda yalnızca kullanılan makine ile ilgili paketleri değil gelen bütün paketleri hedeflerine bakmadan toplama özelliğidir.
- Capture Filter: Paket yakalama sırasında filtreleme özelliği sunar. İstenmeyen paketlerin yakalanmasını engelleyerek hem analiz işlemini kolaylaştırır hemde programın çalışması sırasında daha az paket ile sistem kaynaklarını idareli kullanır.

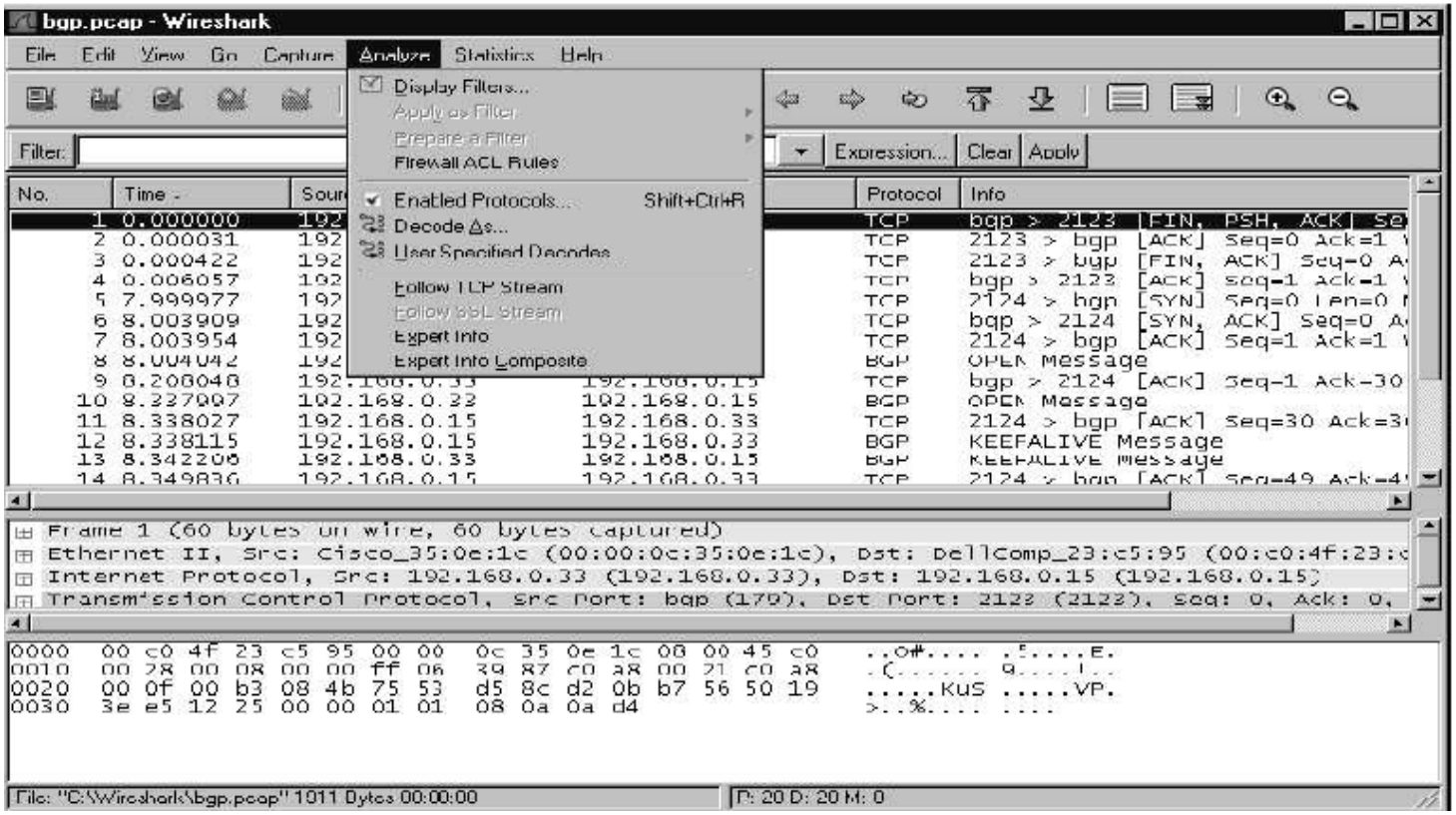
Capture File(s) Alanı

- File: Yakalama dosyası olarak kullanılacak dosya ismi belirtmene yarar. Default olarak boştur.
- Use multiple files: Tek dosya kullanımı yerine wireshark otomatik olarak yeni bir dosyayla yer değiştirir.
- Next file every n megabyte(s): Belirtilen boyutta (kilobyte,megabyte,gigabyte) paket yakalandıktan sonra bir diğer dosyaya geçer.
- Next file every n minute(s): Belirtilen süre geçtikten sonra diğer dosyaya geçer.
- Ring buffer with n files: Belirtilen sayıda dosya aşıldığında en eski dosyayı siler.
- Stop capture after n file(s):Belirtilen sayıda dosya değiştikten sonra yakalama işlemini durdurur.

Stop Capture. Alanı

- ... after n packet(s) : Belirtilen sayıda paket yakalandıktan sonra yakalama işlemini durdurur.
- ... after n megabytes(s): Belirtilen kb,mb,gb miktardan sonra yakalama işlemini durdurur.
- ... after n minute(s): Belirtilen süre sonunda (saniye, dakika, saat, gün) yakalama işlemini durdurur.
- Display Options Alanı:
- Update List Of Packets İn Real Time: Yakalanan paketleri eşzamanlı olarak anında ekranda görmenize yarar.
- Automatic Scrolling in Live Capture: Kaydırma çubuğu otomatik olarak son yakalanan pakete göre iner.
- Hide Capture info Dialog: Yakalanan paketlerin protokollere göre sayı ve Oranını veren bilgi penceresini saklar.

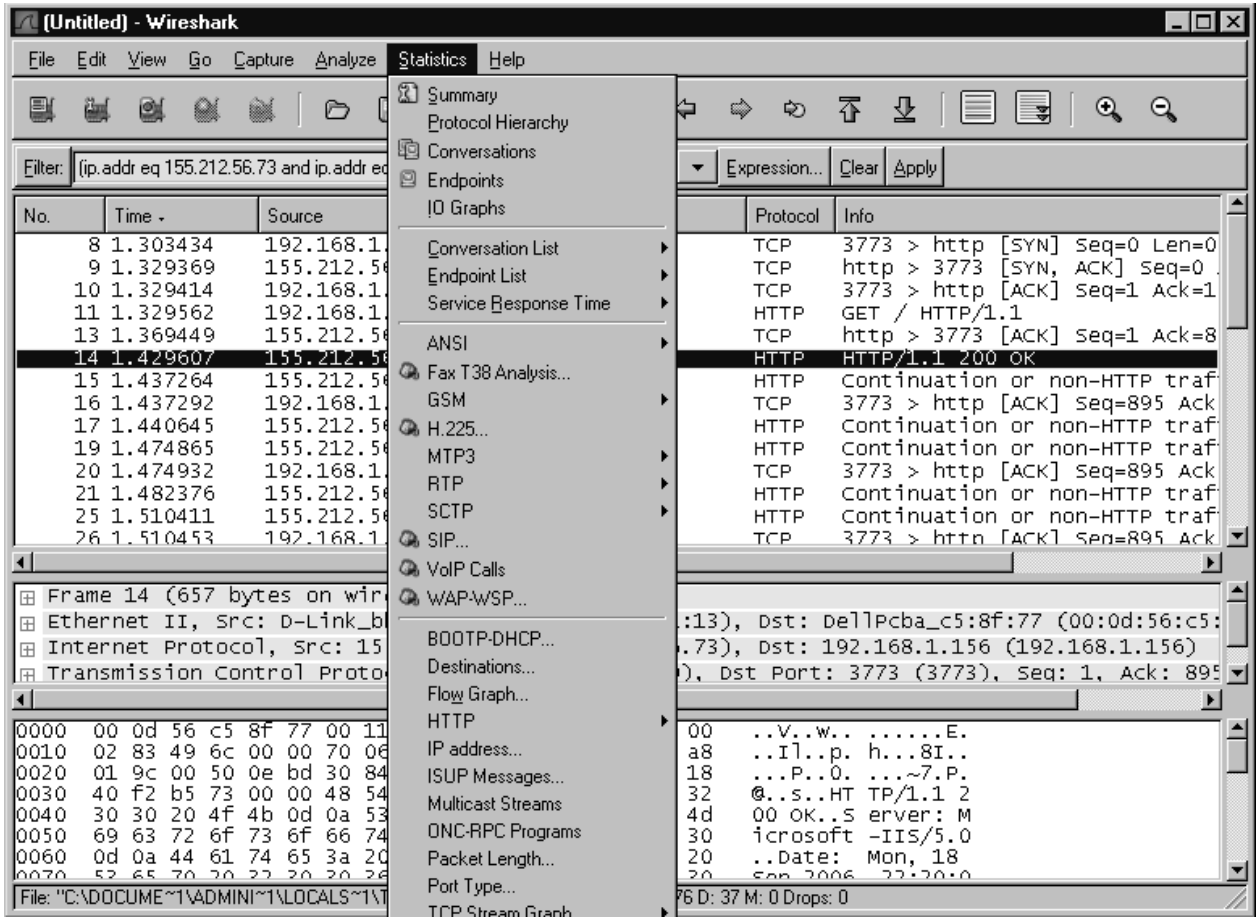
Analyze


bgp.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Display Filters...
Apply as Filter
Prepare a Filter
Firewall ACL Rules
Enabled Protocols... Shift+Ctrl+R
Decode As...
User Specified Decodes
Follow TCP Stream
Follow SSL Stream
Expert Info
Expert Info Composite
Filter:
Expression... Clear Apply
No. Time - Protocol Info
1 0.000000 TCP bgp > 2123 [FIN, PSH, ACK]
2 0.000031 TCP 2123 > bgp [ACK] Seq=0 Ack=1
3 0.000422 TCP 2123 > bgp [FIN, ACK] Seq=0
4 0.006057 TCP bgp > 2123 [ACK] Seq=1 Ack=1
5 7.999977 TCP 2124 > bgp [SYN] Seq=0 Len=0
6 8.003909 TCP bgp > 2124 [SYN, ACK] Seq=0
7 8.003954 TCP 2124 > bgp [ACK] Seq=1 Ack=1
8 8.004042 BGP OPEN Message
9 8.208048 TCP bgp > 2124 [ACK] Seq=1 Ack=30
10 8.327997 BGP OPEN Message
11 8.338027 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=30 Ack=3
12 8.338115 192.168.0.15 192.168.0.33 BGP KEEPALIVE Message
13 8.342206 192.168.0.33 192.168.0.15 BGP KEEPALIVE Message
14 8.349836 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=49 Ack=4
Frame 1 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_35:0e:1c (00:00:0c:35:0e:1c), Dst: DellComp_23:c5:95 (00:c0:4f:23:c
Internet Protocol, Src: 192.168.0.33 (192.168.0.33), Dst: 192.168.0.15 (192.168.0.15)
Transmission Control Protocol, Src Port: bgp (179), Dst Port: 2123 (2123), Seq: 0, Ack: 0,
0000 00 c0 4f 23 c5 95 00 00 0c 35 0e 1c 08 00 45 c0 ..O#.... .5....E.
0010 00 28 00 08 00 00 ff 06 39 87 c0 a8 00 21 c0 a8 .(...... 9....!..
0020 00 0f 00 b3 08 4b 75 53 d5 8c d2 0b b7 56 50 19 .....KuS .....VP.
0030 3e e5 12 25 00 00 01 01 08 0a 0a d4 >..%.... ....
File: "C:\Wireshark\bgp.pcap" 1011 Bytes 00:00:00
P: 20 D: 20 M: 0

Analyze

- Display Filter: Yakalanan paketleri belirtilen ifadelere göre sıralar.
- Apply As Filter: Seçilen paketin kaynak ve hedef adresine göre filtreleme yapar. And (&&), or(||), and not (&& !) ve or not (|| !) eklemeleriyle ifade güçlendirilir ve daha özelleşmiş arama yapılabilir.
- Prepare a Filter: Filtre ifadesini değiştirir ama hemen uygulamaz. Üstteki filtre uygulaması koşulları bunun içinde geçerlidir.
- Firewall ACL Rules :Cisco IOS, Linux Netfilter (iptables), OpenBSD pf ve Windows Firewall (via netsh) için firewall kural ifadesi oluşturur. Yeni kullanıcılar için mükemmel ötesi bir özelliktir.
- Decode As: Paketleri belirli protokollere göre decode eder.
- Enabled Protocols (*shift+ctrl+R*): Yakalama işlemi sırasında istenmeyen protkollerin kaldırılmasına imkan verir. Capture filter gibi düşünülebilir.
- Decode As: Geçici olarak protokol çevrim işi yapar.
- User Specified Decodes: Hali hazırda var olan çevrimleri görüntüler.
- Follow TCP Stream: Seçilen paketle ilgili tcp bağlantılarının tüm tcp segmentlerini ayrı bir pencerede gösterir.
- Follow SSL Stream: Follow TCP stream ile aynı özelliktedir fakat SSL stream için çalışır.

Statistics


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Summary
Protocol Hierarchy
Conversations
Endpoints
IO Graphs
Conversation List
Endpoint List
Service Response Time
ANSI
Fax T38 Analysis...
GSM
H.225...
MTP3
RTP
SCTP
SIP...
VoIP Calls
WAP-WSP...
BOOTP-DHCP...
Destinations...
Flow Graph...
HTTP
IP address...
ISUP Messages...
Multicast Streams
ONC-RPC Programs
Packet Length...
Port Type...
Filter:
Expression... Clear Apply
No. Time Source Protocol Info
8 1.303434 TCP 3773 > http [SYN] Seq=0 Len=0
9 1.329369 TCP http > 3773 [SYN, ACK] Seq=0
10 1.329414 TCP 3773 > http [ACK] Seq=1 Ack=1
11 1.329562 HTTP GET / HTTP/1.1
13 1.369449 TCP http > 3773 [ACK] Seq=1 Ack=8
14 1.429607 HTTP HTTP/1.1 200 OK
15 1.437264 HTTP Continuation or non-HTTP traf
16 1.437292 TCP 3773 > http [ACK] Seq=895 Ack
17 1.440645 HTTP Continuation or non-HTTP traf
19 1.474865 HTTP Continuation or non-HTTP traf
20 1.474932 TCP 3773 > http [ACK] Seq=895 Ack
21 1.482376 HTTP Continuation or non-HTTP traf
25 1.510411 HTTP Continuation or non-HTTP traf
Frame 14 (657 bytes on wir
Ethernet II, Src: D-Link_b
Internet Protocol, Src: 15
Transmission Control Proto
0000 00 0d 56 c5 8f 77 00 11
0010 02 83 49 6c 00 00 70 06
0020 01 9c 00 50 0e bd 30 84
0030 40 f2 b5 73 00 00 48 54
0040 30 30 20 4f 4b 0d 0a 53
0050 69 63 72 6f 73 6f 66 74
0060 0d 0a 44 61 74 65 3a 20
File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\T
D: 37 M: 0 Drops: 0

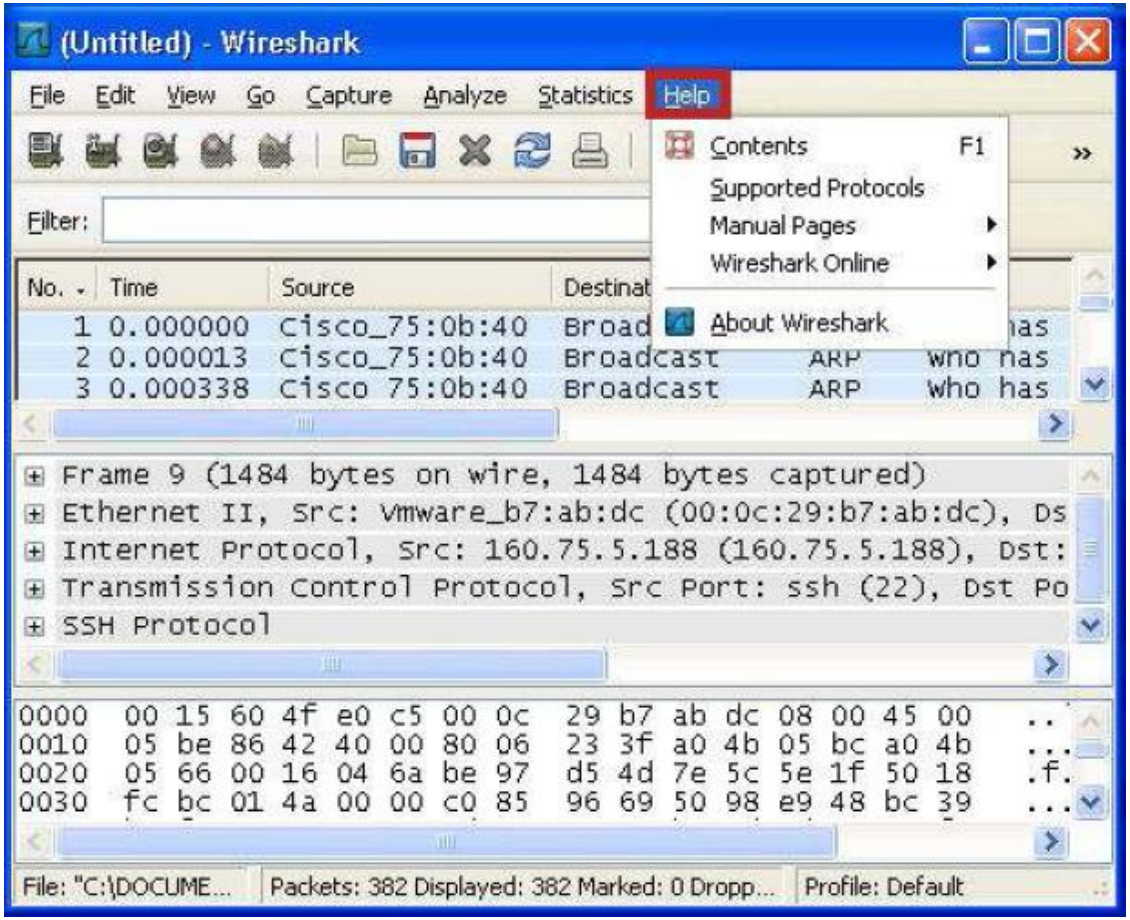
Statistics

- Summary: Açık olan yakalama dosyasında dosya formatı, paket sayısı, boyut, ilk ve son paket yakalama zamanları , filtre ve yakalama arabirimine ilişkin verileri içerir.
- Protocol Hierarchy : Yakalanan paketlerin ağaç şeklinde katman ve protokol hiyerarşisini gösterir. Her sıra bir protokole ait istatistiksel değerleri tutar. Seçilen sıra filtre ifadesi olarak kullanabilir.
- Conversations: Kaynak ve hedef noktaları arasındaki trafiğin istatistik bilgisini verir. Noktalar arasındaki toplam gelen giden paket ve byte miktarı portlara göre listelenir. Conversations penceresi endpoint penceresiyle benzerdir. Listedeki her bir sıra bir diyaloğun istatistiksel değerlerini verir. Adres çözümleme özelliği Conversations penceresi içinde, programın başlangıcında “capture options” bölümünden, preferences altında name resolutions bölümünden ya da view menusu altında name resolutions bölümünden seçildikten sonra kullanılabilmektedir. Limit to display filter özelliği ise herhangi bir filtreleme yönergesi tanımlandığı durumda kullanılabilmektedir.
- Endpoints: Hedef ve kaynak adresi ayrımı yapmadan her son nokta için istatistik bilgisini verir. Desteklenen her protokol için ayrı bir sekme mevcuttur .Her sekmede yakalanan son nokta sayıları belirtilmektedir.

Statistics

- IO Graphs: Belirtilen özelliklerde paketlerin zamana göre akış grafiğini verir. Ağda durum kontrolü için oldukça faydalı bir özelliktir. Bu özellikle normal paket akış diyagramında ağda meydana gelecek herhangi bir anormallik hemen farkedilebilir.
- Graphs: Grafik ayarlamalarının yapıldığı kısımdır.
- Service Response Time: İstek ve cevap arasındaki zamanı gösterir. Service response time istatistikleri DCERPC,Fibre, Channel, H.225 RAS, LDAP,MGCP, ONCRPC, SMB, ANSI,GSM,H.225 gibi protokoller için kullanılır.
- Wlan Traffic Statics: Yakalanan kablosuz ağ trafiğinin istatistik bilgisinin sunar.

Help


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Contents F1
Supported Protocols
Manual Pages
Wireshark Online
About Wireshark
Filter:
No. Time Source Destinat
1 0.000000 Cisco_75:0b:40 Broad
2 0.000013 Cisco_75:0b:40 Broadcast ARP who has
3 0.000338 Cisco 75:0b:40 Broadcast ARP who has
Frame 9 (1484 bytes on wire, 1484 bytes captured)
Ethernet II, Src: Vmware_b7:ab:dc (00:0c:29:b7:ab:dc), Ds
Internet Protocol, Src: 160.75.5.188 (160.75.5.188), Dst:
Transmission Control Protocol, Src Port: ssh (22), Dst Po
SSH Protocol
0000 00 15 60 4f e0 c5 00 0c 29 b7 ab dc 08 00 45 00
0010 05 be 86 42 40 00 80 06 23 3f a0 4b 05 bc a0 4b
0020 05 66 00 16 04 6a be 97 d5 4d 7e 5c 5e 1f 50 18
0030 fc bc 01 4a 00 00 c0 85 96 69 50 98 e9 48 bc 39
File: "C:\DOCUME... Packets: 382 Displayed: 382 Marked: 0 Dropp... Profile: Default

Help

- Help kısmı Wireshark'ın yardım menüsünün bulunduğu kısımdır.
- Contents: Wireshark online yardımı gösterir.
- Supported Protocols: Desteklenen protokolleri gösterir.
- Manual Pages :UNIX-Style kullanıcı sayfalarına ulasan bir alt menüdür.
- Wireshark Online: Online wireshark kaynaklarına ulaşmak için bir alt menüdür.
- About Wireshark :Wireshark ile ilgili bilgileri gösterir.

Filtreleme

- Filtre özelliği,
- Wiresharkta dinleme sırasında veya dinlemenin ardından paketler arasında istenilen özellikteki paketleri görüntülemekte kullanılabilir. Capture options penceresinden belirtilen capture filter, paket yakalama sırasında wiresharkın uyacağı koşulları belirtir. Capture filter penceresinde Wiresharkın paket yakalama sırasında uyacağı kurallar için bir liste sunulmuştur.
- Ethernet address 00:08:15:00:08:15 : Ethernet II altında kaynak veya hedef adreslerinde belirtilen mac adresine ait paketleri yakalar.
- not broadcast and not multicast: Broadcasting ve multicasting paketlerini yakalamaz.
- not arp: Arp paketlerini yakalamaz.

Filtreleme

- IP address 192.168.0.1 : Belirtilen ip adresini hedef yada kaynak adres kısımlarında barındıran paketler yakalanır.
- IPX only : İlgili protokole ilişkin paketleri yakalar.
- TCP only : İlgili protokole ilişkin paketleri yakalar.
- UDP only : İlgili protokole ilişkin paketleri yakalar.
- TCP or UDP port 80 (http) : Port 80 için tcp ve udp paketlerini yakalar.
- HTTP TCP port (80) : Port 80 için http ve tcp paketlerini yakalar.
- No ARP and no DNS : DNS ve ARP paketleri harici paketleri yakalar NonHTTP and nonSMTP to/from www.wireshark.org : Belirtilen adres için http ve smtp harici paketleri yakalar.

EN ÇOK KULLANILAN FİLTRELER

- 1.IP FILTERS

Filter	Tip	Tanım
ip.addr	IPv4 adresi	Source(kaynak) veya Destination(hedef)kaynak
ip.src	IPv4 adresi	Source adres
ip.dst	IPv4 adresi	Destination adres
ip.host	Karakter dizisi	Source veya Destination host adres
İp.src.host	Karakter dizisi	Source host adres
İp.proto	8 bit integer	Protokol
İp.version	8 bit integer	IP versiyonu

EN ÇOK KULLANILAN FİLTRELER

- 2.ETHERNET FILTERS

Filter	Tip	Tanım
eth.addr	6 bit mac adres	Source(kaynak) veya Destination(hedef) adres
eth.src	6 bit mac adres	Source adres
eth.dst	16 bit integer	Destination adres
eth.len	16 bit integer	Uzunluk
eth.type	16 bit integer	Tip

EN ÇOK KULLANILAN FİLTRELER

- 3.TCP FILTERS

Filter	Tip	Tanım
tcp.ack	32 bit integer	Acknowledgement numarası
tcp.analysis.ack_lost_segment	-	Ack yapılmıs kayıp paket tcp.analysis.duplicate_ack - Tekrar edilmis ack
tcp.analysis.duplicate_ack	-	Tekrar edilmiş ack
tcp.analysis.duplicate_ack_num	32 Bit integer	Tekrar edilen ack numarası
tcp.analysis.flags	-	TCP analiz bayrakları(uyarı)
tcp.port	16 bit integer	Source veya Destination port numarasına göre

IEEE 802.16 ve WiMAX

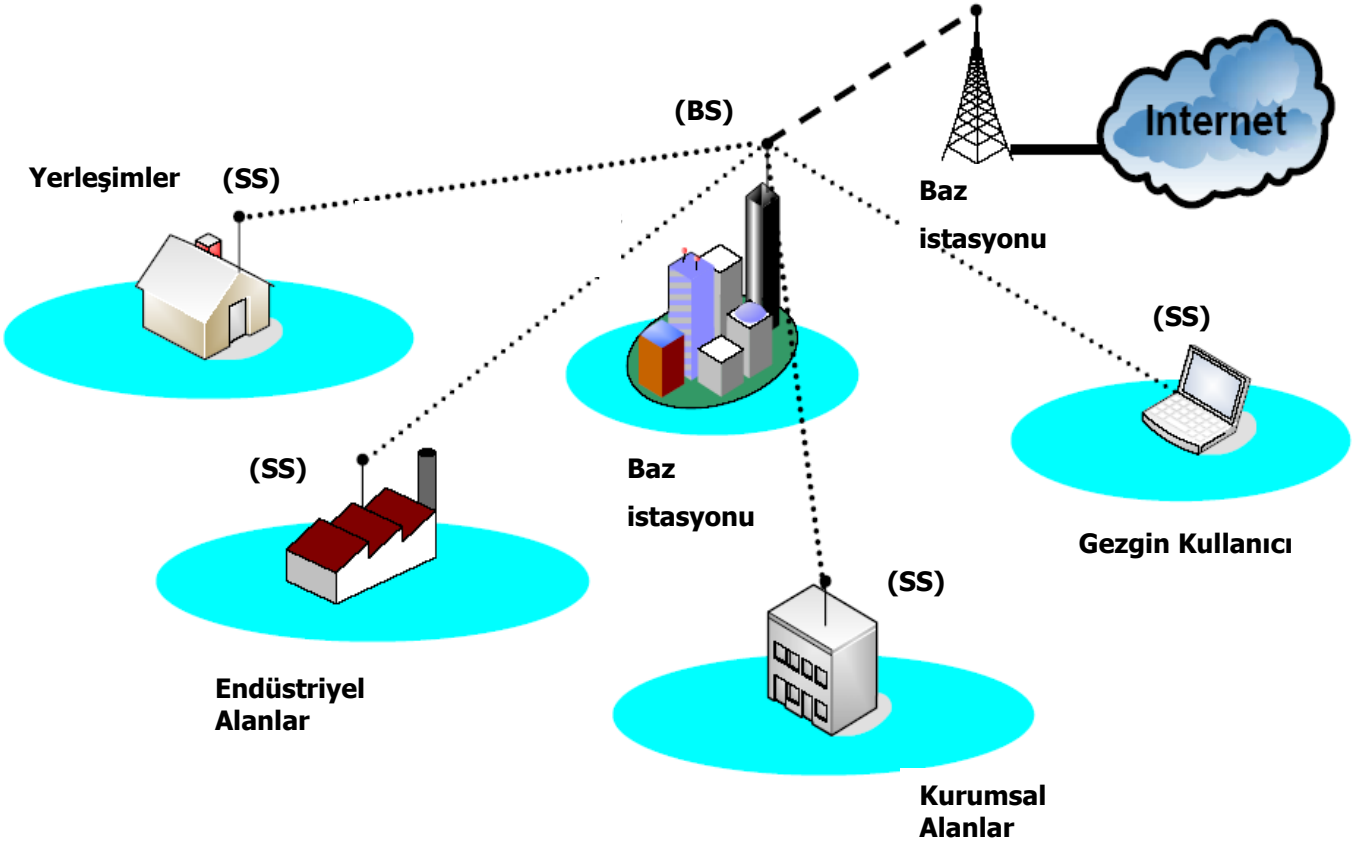
- IEEE 802.16: Telsiz Kentsel alan ağı standardı (Wireless MAN),(1999).
- WiMAX (Worldwide Interoperability for Microwave ACCess):

  802.16 standardını destekleyen uç birimlere telsiz alanda yüksek bandgenişliği (BWA) sağlamayı amaçlayan bir forumun standardı (2001).
- Yüksek hızda kesintisiz telsiz iletişim
  - 70 Mbps
  - Kapsama alanı: 50-70 km'ye kadar
  - Veri
  - Ses (isteğe-bağlı)
  - Görüntü (isteğe-bağlı)
  - VoIP
  - Videokonferans

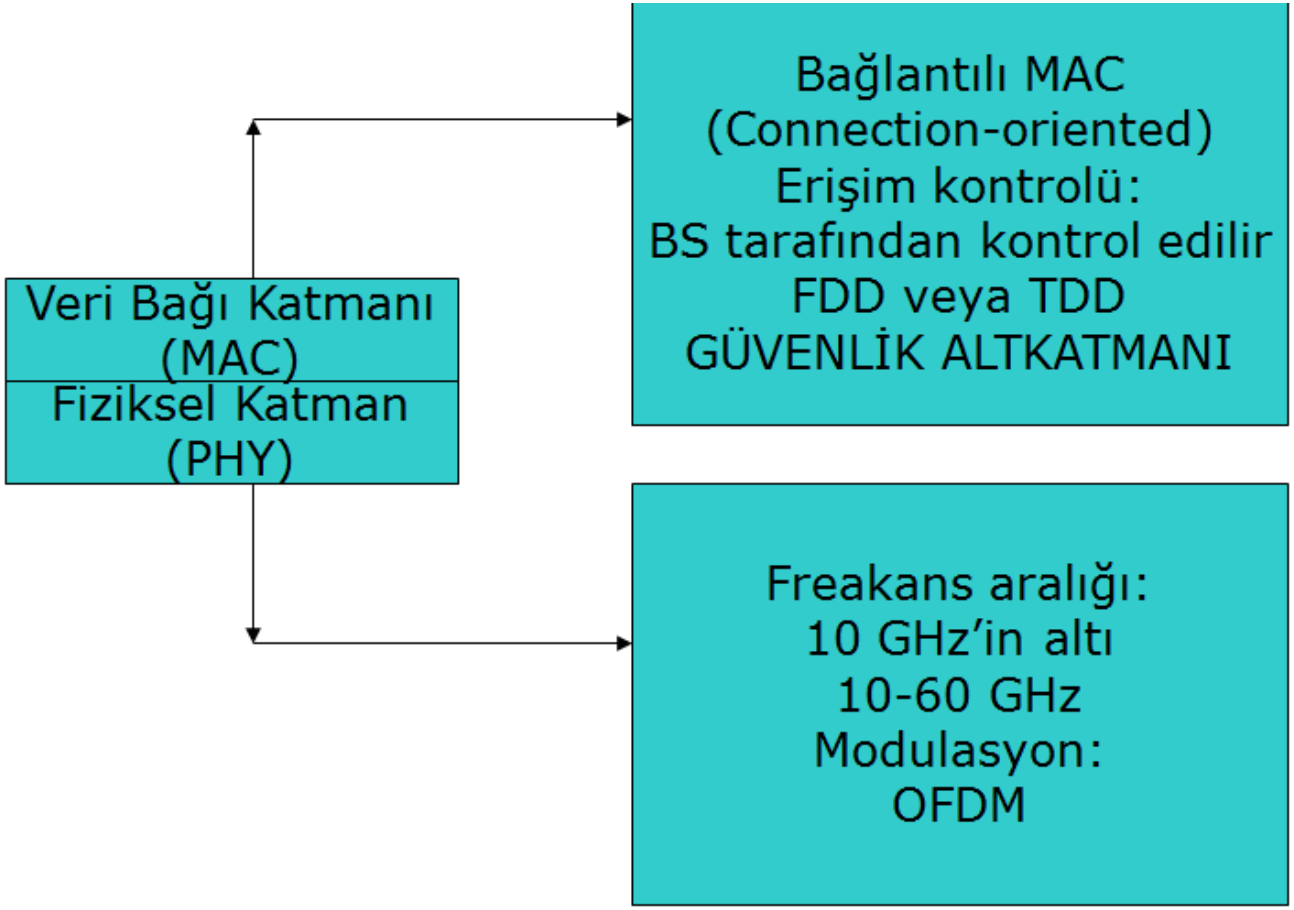
IEEE 802.16 ve WiMAX

- İletişim Türleri:
  - Baz istasyonu(BS)→ Kullanıcı İstasyonu(SS): Downlink
  - Kullanıcı İstasyonu(SS)→ Baz İstasyonu(BS): Uplink
  - Baz İstasyonu(BS)-kullanıcı İstasyonları (SS) arası
    - Tek noktadan Çok noktaya (PMP)
  - Kullanıcı İstasyonları arası
    - Ağ (mesh) yapısı

WiMAX Genel Yapısı



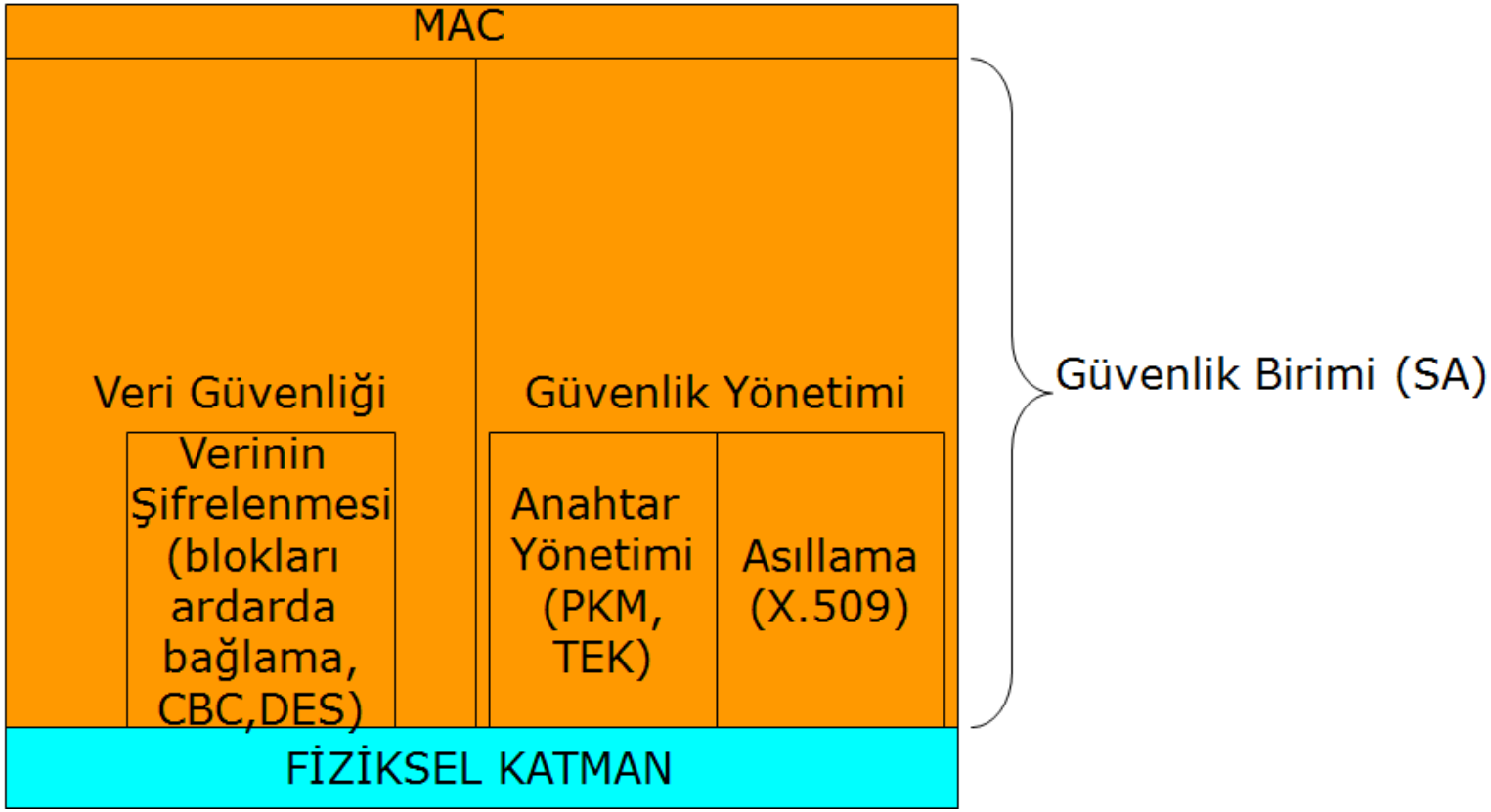
WiMAX katmansal Analiz



802.16 Güvenlik Standardı

- 5 kavrama dayalı bir yapı
  - Veri Şifreleme
    - MAC başlığı dışındaki kısma uygulanıyor
  - Anahtar Yönetimi
    - PKM
  - “Güvenlik Birimi” nin oluşturulması
    - Birimler arasında saydam bir iletişim kontrolü
  - Bağlantıların güvenlik birimine iletilmesi
  - Kriptografik süreç
    - Güvenlik biriminin veri şifrelemesi, asıllama ve anahtar alışverişi sırasında uyguladığı metodlarve girdiği durumlar

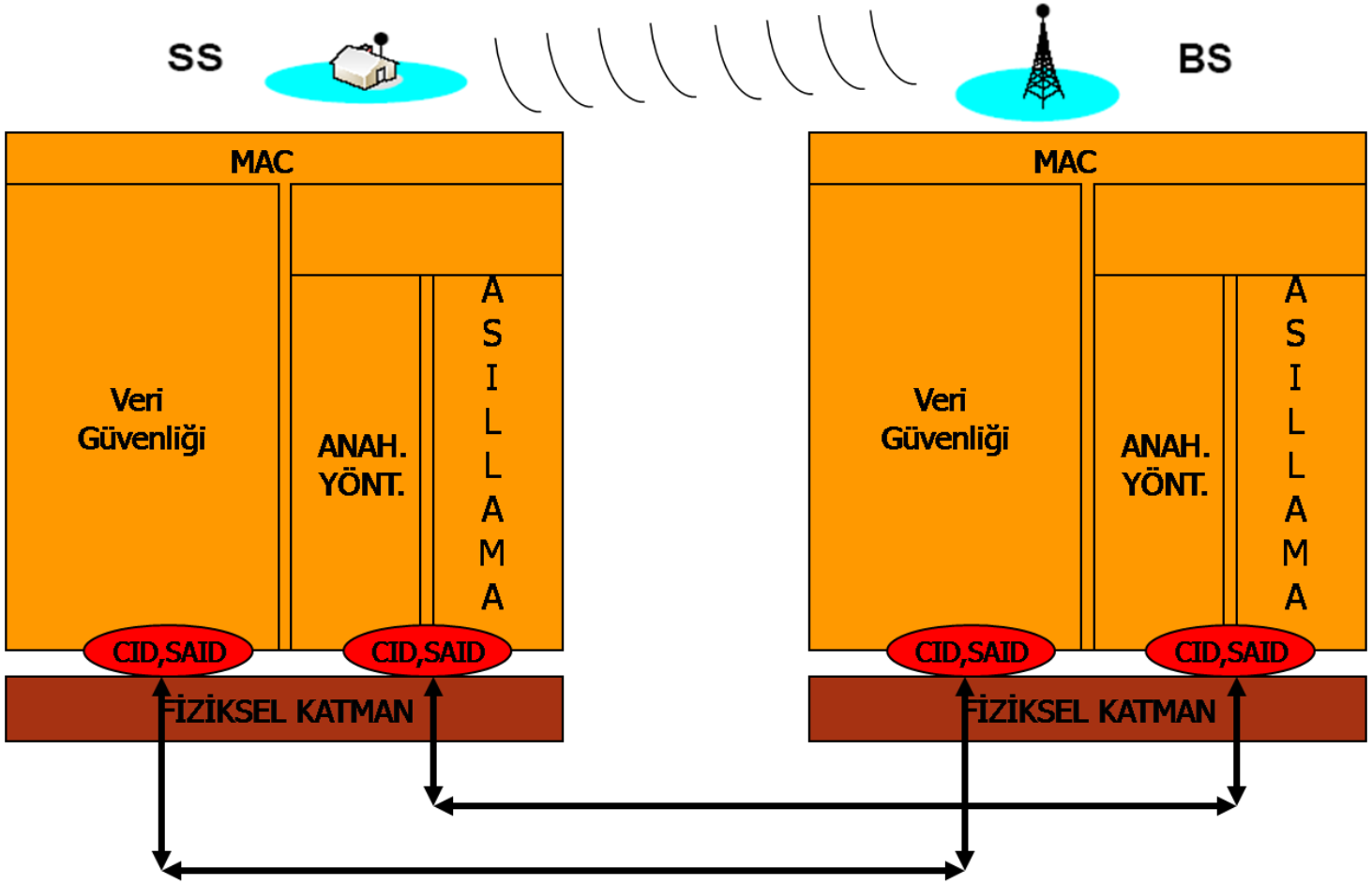
WiMAX Güvenlik Altkatmanı(1/2)



WiMAX Güvenlik Altkatmanı(2/2)

- Güvenlik Birimi (SA):
  - BS-SS arasındaki her türlü güvenlik bağlantısını sağlar.
  - 16-bitlik bir belirteci vardır (SAIP).
  - Tutulan parametler:
    - Her düzey için bir bağlantı ID'si(CID).
    - Kriptografik bilgiler(CBC, DES vs)
    - Güvenlik Bilgileri(Anahtar, IV)

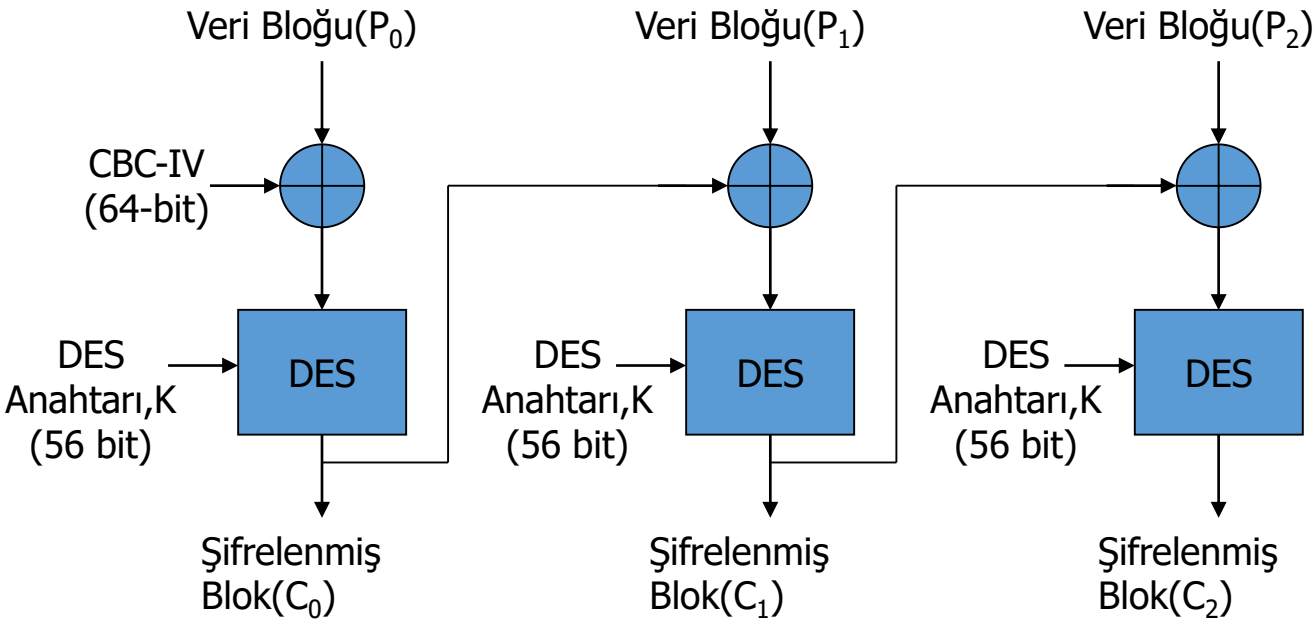
WiMAX Güvenlik Altyapısı



Veri Güvenliği (1/2)

- Şifreleme
  - Kullanılan Algoritma
    - DES
      - 56 bit anahtar
      - 64 bitlik bloklar
  - Kullanılan Şifreleme Kipi
    - “Şifreleme Bloklarını ardarda Bağlama Kipi” (Cipher Block Chaining,CBC)
    - CBC-IV: başlama vektörü TEK anahtar değiştokuşu sırasında öğrenilir
    - XOR: Çerçevedeki senkronizasyon alanında belirtilir.

Veri Güvenliği (2/2)



Şifreleme:

$$C_i = K[P_i \oplus C_{i-1}]$$

Şifre Çözme:

$$P_i = C_{i-1} \oplus K^{-1}[C_i]$$

Güvenlik Yönetimi(1/7)

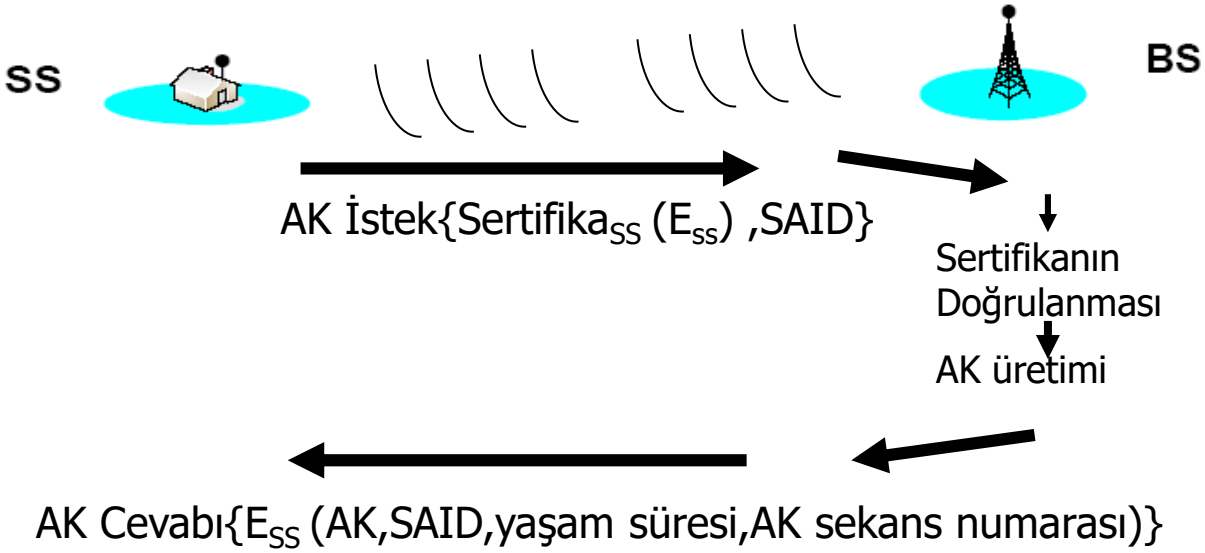
- Asıllama
  - Açık anahtarlı kriptografi kullanılır.
  - SS ile BS arasında SAID alışverişi
  - SS için kullanılan yöntem: X.509 sertifikalama
    - Üretici Sertifikası
      - Kendi kendine veya üçüncü kişi tarafından
      - Üretici bilgileri(WiMAX forumuna uygunluk)
    - SS sertifikası
      - Üretici tarafından
      - SS'in Seri numarası
      - SS'in MAC adresi
    - SS'ler açık-gizli anahtar çiftleri ile donatılmıştır
      - RSA tabanlı bir algoritma ile
      - Herhangi bir lokal algoritmayla dinamik olarak

Güvenlik Yönetimi(2/7)

- BS için ayrıca asıllama yok
  - BS, üretici sertifikasının açık anahtarını kullanarak SS'i asıllar.
  - Böylece standarda uygunluk anlaşılmış olur.
  - SS'in gizli anahtarının iyi saklandığı varsayılır.

Güvenlik Yönetimi(3/7)

- Asıllama anahtarı(AK,128-bit) alışverişi yapılır
  - Açık anahtar ile şifreli olarak gönderilir.
  - BS ve SS AK'yı elde ettikten sonra asıllama tamamlanmış olur.
  - SS periyodik olarak AK tazelemesi yapar.



Güvenlik Yönetimi(4/7)

- Anahtar oluşumu
  - Privacy Key Management (PKM)
  - Güvenlik birimi(SA) tarafından yönetilir.
  - SS'ler, PKM protokolünü BS'den asıllama ve trafik güvenliği parametrelerini almak için kullanır.
  - Asıllama anahtarı ve oturum tazeleme de PKM tarafından yönetilir.

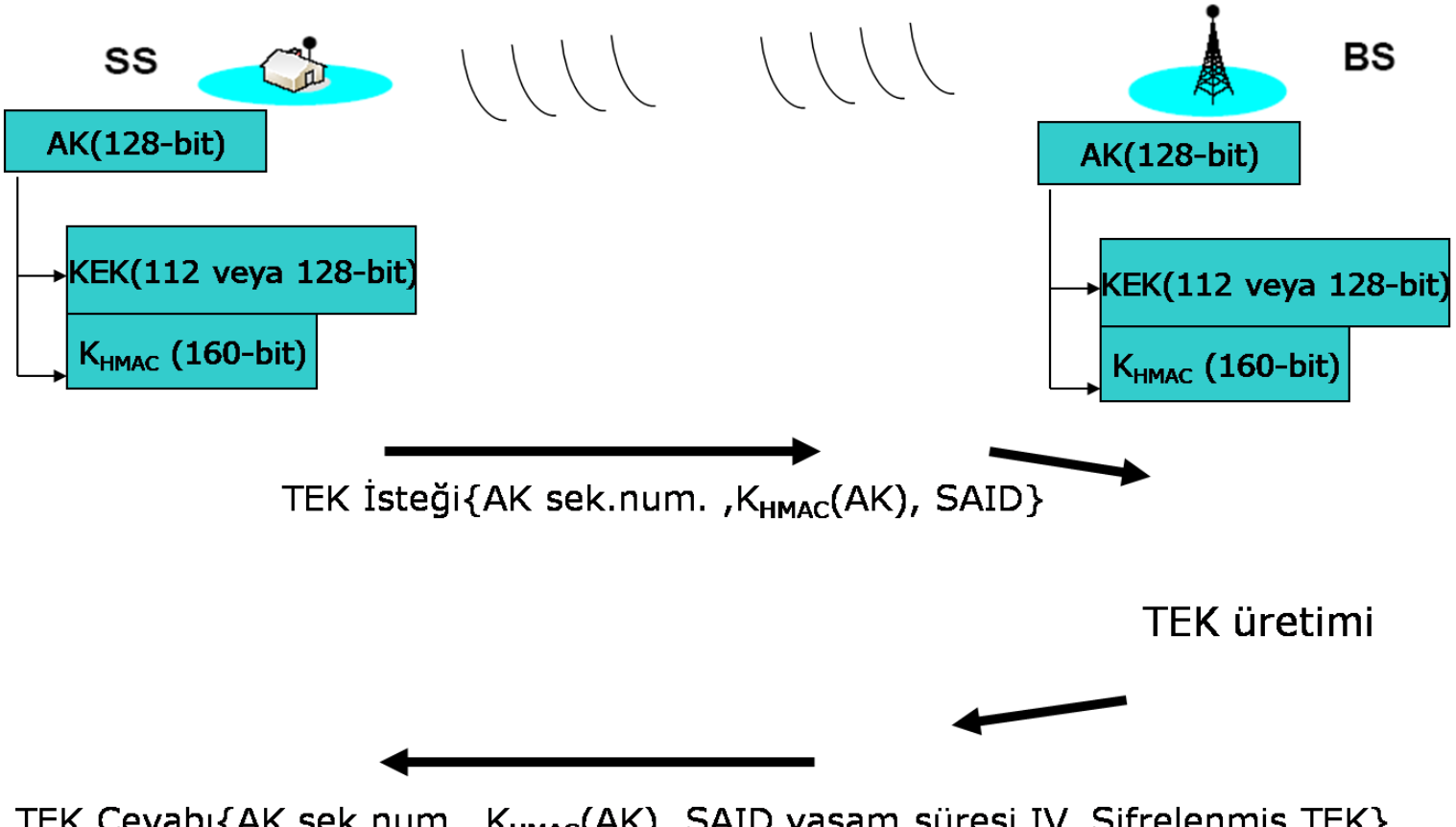
Güvenlik Yönetimi(5/7)

- Anahtar alışverişi
  - AK oluşumundan sonra, Traffic Encryption Keys (TEK) alışverişi yapılmalıdır.
    - TEK'ler 56-bitlik DES anahtarlarıdır.
    - Bu aşamda da AK'dan yardım alınır.
      - AK, BS'te anahtar oluşturulmasında kullanılacak olan Key-Encyrption Key(KEK) oluşturulmasında(112 yada 128 bit olabilir) ve HMAC'teki K anahtarı olarak kullanılır.
      - TEK, yukarıdaki anahtarlardan bağımsız olarak BS tarafından üretilir

Güvenlik Yönetimi(6/7)

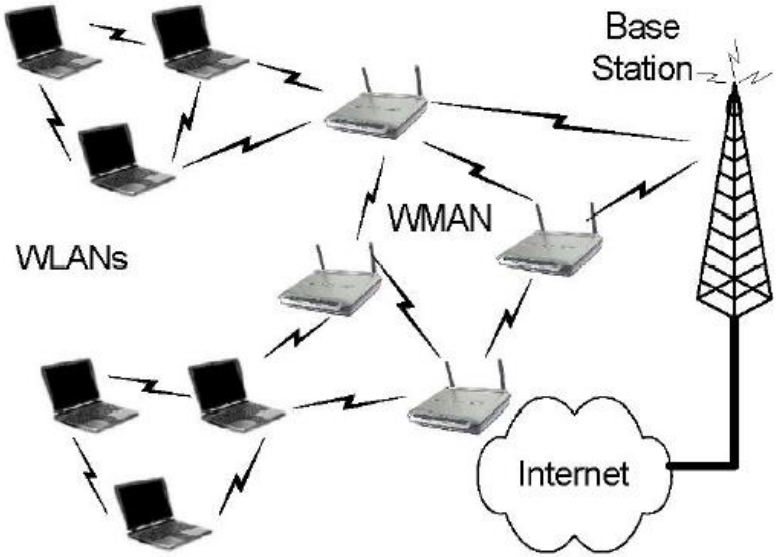
- TEK'in gönderilmesi:
  - 3DES ile
    - (112-bitlik KEK ile)
  - RSA ile
    - (SS'in Açık anahtarı ile)
  - AES ile
    - (128-bitlik KEK ile)
- Anahtar alışverişindeki asıllama,AK doğrulaması ve bütünlük HMAC-SHA1 ile sağlanır.

Güvenlik Yönetimi(7/7)



WiMAX Ağ(Mesh) yapısında Güvenlik(1/2)

- SS'ler BS olmadan birbirleriyle haberleşebilir→Mesh yapının en önemli özelliği BS'nin kapsama alanında artış olur
- Ağda bir düğüm çöktüğünde yada BS çöktüğünde tüm iletişim kesilmez.



WiMAX Ağ(Mesh) yapısında Güvenlik(2/2)

- Ağa katılmak isteyen bir düğüm kendisine en yakın düğümü “sponsor düğüm” ilan eder.
- İstemci düğüm,kendisini asıllaması için elçi düğüme mesaj gönderir.
- PMP’teki güvenlik işlemlerinin benzeri sponsor düğüm tarafından yapılır.
- Asıllama işini yapan gerçek düğümle bir tünel kuran elçi düğüm, istemci düğüme mesajları iletir.
  - Asıllama mesajları
  - Anahtar alışverişi
- Mesh’e dahil olan düğüm, diğer düğümlerle iletişime geçebilir.

Güvenlik Altyapısının Analizi(1/5)

- Veri şifrelemesindeki sorunlar
  - DES algoritması günümüzde kırılabilir bir algoritma haline gelmiştir.
    - Deneme-yanılma ve Brute-Force saldıralarına dayanıksızdır.
    - 128-bitlik AES kullanılabilir
      - Daha yavaş ama güvenliği arttırıcı bir yöntem

Güvenlik Altyapısının Analizi(2/5)

- Tekrar saldıralarına dayanıksızdır.
  - Aktif saldırılar gerçekleştirilebilir.
    - Telsiz ortamın doğasından kaynaklanan araya girebilme özelliğini ortadan kaldıracak bir yapı yok
    - Tekrar saldıraları için
      - Rastgele bir sayı
      - Paket numarası
      - Sekans numarası

Güvenlik Altyapısının Analizi(3/5)

- CBC Başlangıç vektörü tahmin edilebilir.
  - Seçilen Açık metin saldırısı yapılarak gerçek metin elde edilebilir.
  - Bazı çözümler
    - Başlangıç vektörü için
      - Her bir metin için değil, her bir çerçeve için IV üretimi
      - Bu IV'nin veriye gömülmesi
      - Şifreleme yükü artar!

Güvenlik Altyapısının Analizi(4/5)

- Anahtar Yönetimindeki sorunlar:
  - TEK'te kullanılan sekans numarasının 2-bit olması
    - Her bir tekrar saldırısında %25 bir olasılıkla TEk bulabilinir!
  - Rastgele üretilen TEK'lerin nasıl bir rassal fonksiyonla üretildiği konusunda bilgilendirme yapılmıyor.
    - Değişik üreticilerin oluşturduğu bir ağda güvensizlik ve dengesizlik yaratabilir.
  - BS tarafından oluşturulan AK'nin tazeligine güvenilmeli!
    - SS bunu kontrol etmiyor.

Güvenlik Altyapısının Analizi(5/5)

- Asıllamadaki problemler
  - Çift taraflı bir asıllama yok.
    - BS asıllanmıyor.
      - Ortadaki adam saldırısı yapılabilir.
  - Asıllama protokolunde gönderilen mesajlar doğrulama için yetersiz
    - EAP(Extensible Authentication Protocol) tabanlı bir asıllama yapılabilir.
      - EAP-TLS(Transport Layer Securty)
      - EAP-MD5

GÜVENLİ İŞLETİM SİSTEMLERİ

- ✓ **Tarihçe**
- ✓ **Linux İşletim sistemi nedir , nelerden oluşur**
- ✓ **Linux Mimarisi**
- ✓ **Neden Linux ?**
- ✓ **Linux İşletim Sistemlerinin Özellikleri**

LINUX

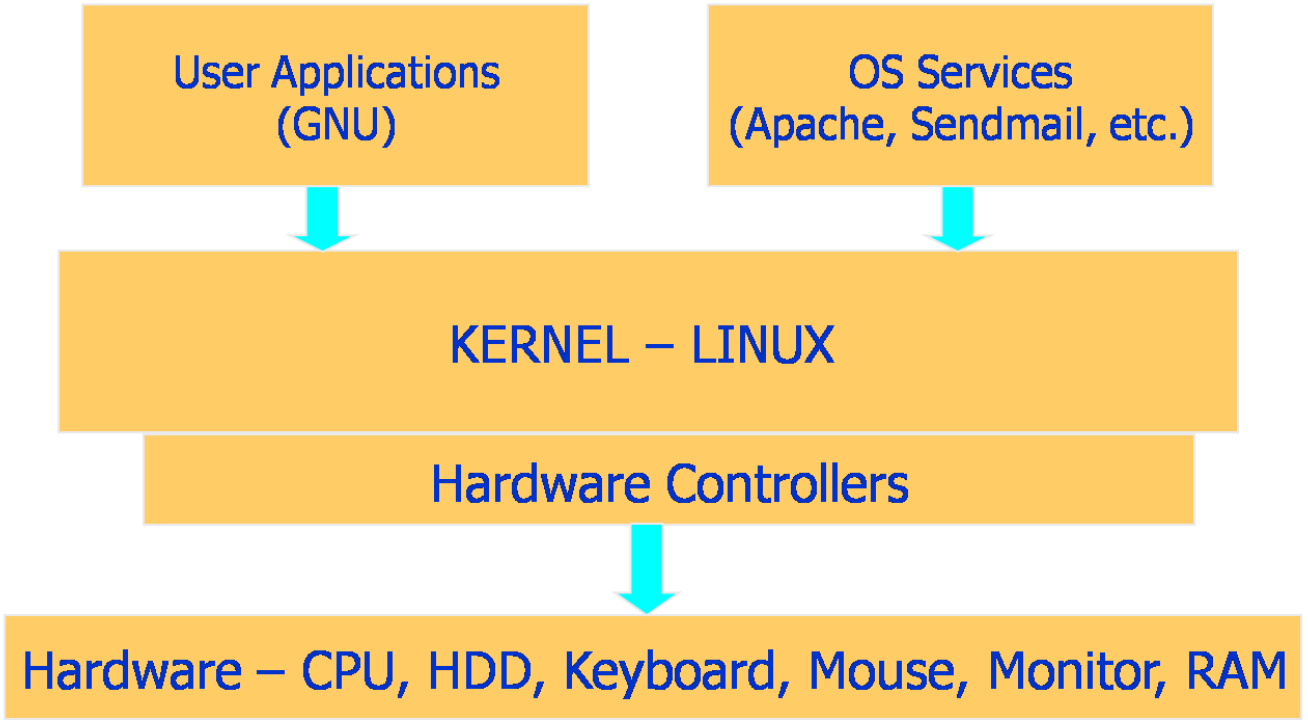
- Tarihçe
  - 1991'de Linus Torvalds adında Finlandiyalı bir öğrenci bilgisayar mühendisliği eğitimi alırken Intel'in 80386 geliştirmek için çıkartmıştır.
  - Minix de olmasını istediği özellikleri yeni işletim sistemine ekledi.
  - 5 Ekim 1991 de Linux un ilk sürümü 0.02 yi MIT'nin haber listelerinde Dünya ya duyurdu.

Linux işletim sistemi nedir?

- Unix bir işletim sistemi ailesine verilen ortak bir isimdir.
- Linux (resmi olarak olmasa da), OpenBSD, FreeBSD, Irix, Solaris, Aix... çeşitli Unix türevleridir.
- Linux, Unix sistemlerinin tüm avantajlarını taşır.Çok kullanıcılı ve bilgisayar ağlarında kullanılmak üzere tasarlanmıştır.
- Linux dağıtımları ;
  - Suse, Red Hat, Fedora, Knoppix vs

Linux işletim sistemi

LINUX MİMARİSİ



Neden LINUX ?

- Hız
- Maliyet
- Yaygınlık
- Güvenlik
- Sağlamlık

LINUX İşletim Sistemi Özellikleri

- Birden çok kullanıcı desteği
- Çok görevli olması
- Çok işlemci desteği
- TCP/IP desteği
- Dosya yapısı
- Kabuklar (shell)

1.Fiziksel Güvenlik

- **1.1 BIOS Güvenliği**

➢Parola ayarı yapmak gerekir .

➢ Konulan parola caydırıcı etki yapabilir.

➢ Tam anlamıyla güvenli sayılmaz.

2. Çekirdek (Kernel) Güvenliği

- Güncel tutmak
- Yamalı Çekirdek olmasından emin olmak
- Çekirdeğin derlenmesi gerekir.

3. Kullanıcı Güvenliği

- Kullanıcılara yeni hesap açarken onlara gerekli olan kadar , minimum imtiyaz hakkı verilmelidir.
- Ne zaman login ,log-off olduklarını belirleyen kayıtlar mutlaka tutulmalıdır.
- Aktif olmayan hesaplar silinmelidir.Aktif olmayan hesaplar log dosyaları kontrol ederek görülebilir.

3. Kullanıcı Güvenliği

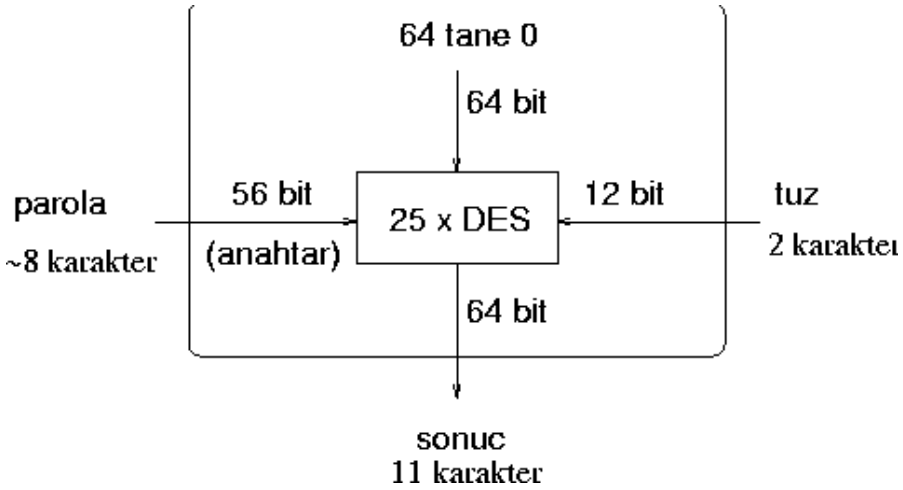
- Root hesabı adına dikkat edilmesi gerekenler ;
- Root olarak giriş izni çok kullanıcıya verilmemelidir.
- Root olarak rlogin/sh/rexec(r-utilities) kullanılmamalıdır. Kesinlikle .rhosts dosyası yani özel erişim dosyası yaratılmamalıdır.

4. Parolalar

- Çok-kullanıcılı işletim sistemlerinde kullanıcının kimliğinin belirlenmesi büyük önem taşımaktadır. Hem sistemi kullanmaya yetkisi olmayan kişilerin sisteme girmelerinin engellenmesi, hem de sistemdeki kullanıcıların birbirlerinden ayırt edilebilmeleri için, her kullanıcıya bir parola verilir ve sisteme giriş başta olmak üzere tüm kritik işlemlerde kullanıcıya parolası sorulur.
- Parolalar, diğer kullanıcı bilgileriyle birlikte, parola dosyasında (**/etc/passwd**) tutulur. Bu dosyadaki her satir, bir kullanıcı ile ilgili bilgileri saklar. Bir satırdaki alanlar, sırasıyla, kullanıcı adı, parola, kullanıcı numarası, grup numarası, ad, kişisel dizin ve komut yorumcusudur.

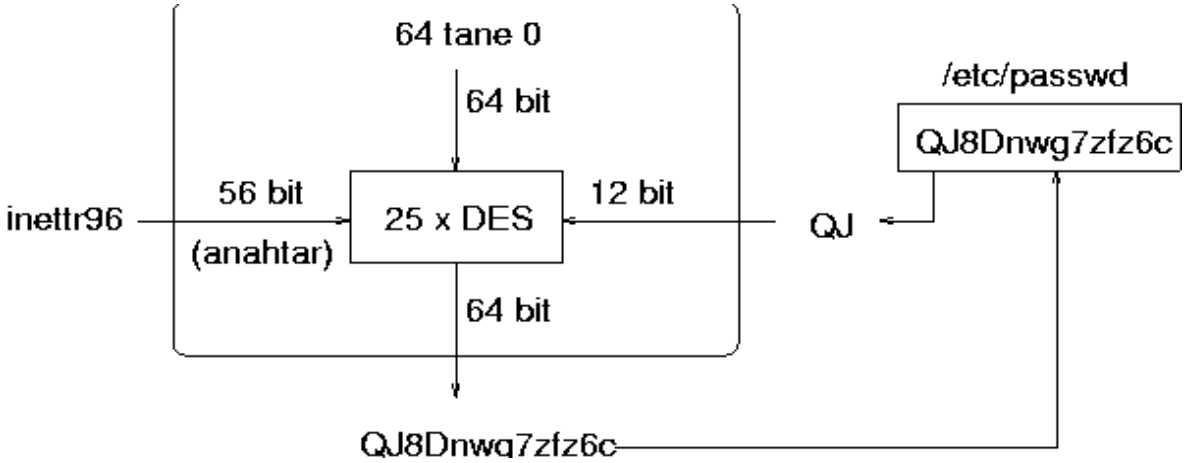
4.1 Parolaların Şifrelenmesi

- **Crypt** fonksiyonu ile şifreleme



4.1 Parolaların Şifrelenmesi

- **Parola Denetimi**



4.2 Parola Seçimi

Şu tip parolalar kolay tahmin edilebilen parolalar sayılmaktadır:

- Kullanıcı ile yakinliği olan kişilerinkiler (kendisi, ailesi, arkadaşları, yakınları) basta olmak üzere bütün erkek ve kadın isimleri
- Doğum tarihleri
- Kullanıcı ile ilgili herhangi bir bilgi (kullanıcı adı, oda numarası, telefon numarası, arabasının plaka numarası, sosyal güvenlik numarası)
- Yer isimleri
- Bilgisayar terimleri
- Klavyede belli bir düzene göre ardarda gelen harflerden oluşan parolalar (qwerty)
- Anlamlı bir sözcük
- Yalnızca küçük (ya da yalnızca büyük) harflerden oluşan parolalar
- Yukarıdakilerden birinin başına ya da sonuna bir rakam eklenerek oluşturulan parolalar
- Yukarıdakilerin ters yazılışları

4.2 Parola Seçimi

İyi bir parola üretmek için önerilen iki yöntem vardır:

- İki sözcüğün arasına bir rakam ya da noktalama işareti konarak birleştirilmesi
- Seçilen bir cümlenin sözcüklerinin bas harfleri

4.3 Tehlikeler

Bir saldırganın parola dosyasını eline geçirmesi birkaç şekilde mümkün olabilir:

- Bir kullanıcının parolasını elde ederek sisteme girer ve dosyayı alır.
- Bazı programlardaki hatalardan yararlanarak sisteme girmeden dosyayı alır.
- Sistemdeki bir kullanıcı parola dosyasını saldırgana gönderir.
- Saldırgan, sistemdeki kullanıcılardan biridir.

4.4. Önlemler

- Parola Seçiminin Kullanıcıya Bırakılmaması
  - Sistem sorumlusu ya da rasgele parola üreten program tarafından parola verilmesi gerekir.
  - mkpasswd programı
- Parola Seçiminin Kısıtlanması
  - anlpasswd
- Parola Dosyasının Sistem Sorumlusu Tarafından Kırılması
  - crack
- Parolaların Geçerlilik Surelerinin Kısıtlanması
- Gölge Parolalar
  - Parolalar gölge dosyasına (/etc/shadow) şifrelenmiş parolalar konur.
  - Shadow Password Suite

5. Dosya Güvenliği

- Her dosyanın bir sahibi, bir de grubu vardır. Dosya üzerinde kimin hangi işlemleri yapabileceğine dosyanın sahibi olan kullanıcı karar verir. Erişim hakları, dosyanın sahibi, grubu ve diğerleri için ayrı ayrı belirtilir.
- Her biri için dosyanın okunmasına (read), yazılmasına (write) ve çalıştırılmasına (execute) izin verilebilir. Böylece her dosya için üç tane üçlüden oluşan bir erişim hakları listesi elde edilir.

-rwxr-x--- 1 karin users 4030 Dec 4 15:30 deneme

- Örnekteki ``deneme'' dosyasının sahibi “karin" kullanıcısı, grubu "users" grubudur. “karin” kullanıcısı dosyayı okuyabilir, yazabilir ve çalıştırabilir; "users" grubundaki kullanıcılar okuyabilir ve çalıştırabilir; diğer kullanıcıların ise hiçbir hakki yoktur.

5.1. Tehlikeler

- **Dosyanın izinsiz Olarak Okunması**
  - Kullanıcıların kişisel dosyalarının ve e-postalarının okunması
- **Dosyanın Yetkisiz Kişilerce Değiştirilmesi**
  - Sistem dosyalarının değiştirilmesi
  - Yetkili kullanıcı yaratılabilir
  - Kayıt dosyalarının silinebilmesi

5.2. Önlemler

- **Dosya Değişikliklerinin Denetimi**
  - Dosya imzaları oluşturma
  - Tripwire paketi kullanılmalı
- **Şifreleme**
  - PGP (Pretty Good Privacy) kullanılması
  - CFS (Cryptographic File System)

Sonuç

- 802.16 standardındaki 2 düzeyli yapı,802.11'e göre geliştirilmeye daha elverişli bir altyapı oluşturmakta.
- Sertifika otoriteleri hakkında daha açık bilgiler verilmeli.
- Veri şifreleme yöntemi:DES yetersiz
- Tek taraflı bir asıllama söz konusu
  - Geliştirilmesi gereken bir nokta
  - EAP kullanılabilir
- Anahtar üretiminde problemler var
  - Tekrar saldırıların engellenebilmesi için rastgele sayıların üretilmesi gerekiyor.

Kaynaklar

- [1] IEEE Std 802.16-2004--IEEE standard for local and metropolitan areanetworks, part 16: "***Air Interface for Fixed Broadband Wireless Access Systems***".
- [2] David Johnston ve Jesse Walker--INTEL: "***Overview of IEEE 802.16 Security***"
- [3] Kitti Wongthavarawat--Thai Computer Emergency Response Team (ThaiCERT) National Electronics and Computer Technology Center,Thailand: "***IEEE 802.16 WiMax Security***"
- [4] Loutfi Nuaymi, Patrick Maillé, Francis Dupont, Raphaël Didier--École Nationale Supérieure des Télécommunications de Bretagne:"***Security issues in WiMAX/IEEE 802.16 BWA System***"
- [5] Yun Zhou ve Yuguang Fang--Department of Electrical and Computer Engineering,University of Florida, Gainesville:"***Security of 802.16 in Mesh Mode***"

Kaynaklar

- http://www.linuxplanet.com/linuxplanet/interviews/4495/1
- www.linuxsecurity.com
- www.linux.org.tr
- IMPROVING THE SECURITY OF YOUR UNIX SYSTEM ,David A. Curry, Systems Programmer ,Information and Telecommunications Sciences and Technology Division
- Linux Sistem Güvenliği Raporu ,2003

BİR SALDIRININ SENARYOSU

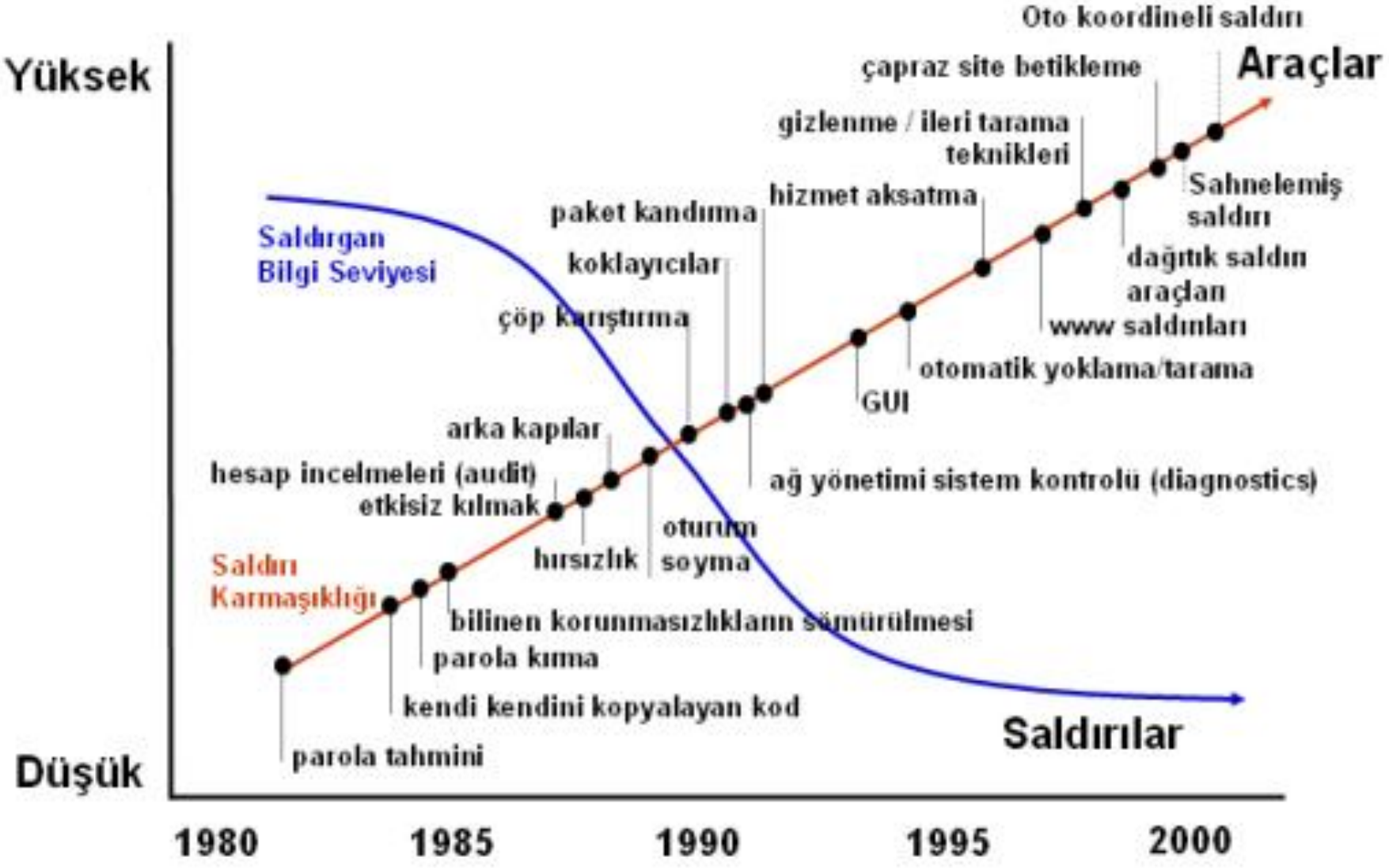
Saldırı Aşamaları

- Veri Toplama Aşaması
- Saldırı Hazırlık Aşaması
- Saldırı Aşaması
- Command Execution
- Açıklar ve Exploiting
- Sosyal Mühendislik & Phishing
- İzleme ve Gizlenme
- Sistemi Sahiplenme
- İzleri Silme

Saldırı Motifleri nelerdir?

- Merak
- Maddi kazanç arzusu
- Ün kazanma isteği
- Kin-öç
- Terörist amaçlı faaliyet
- İtibarsızlaştırmak
- Sadece eğlence için
- Politik sebepler
- Meydan okuma
- Vatanperverlik

Saldırı Karmaşıklığı-Saldırgan Teknik Bilgisi



Banka soygunu- Olası Senaryo

- Banka hangi bölgede?
- Bölgenin güvenilirliği?
- Bankada bulunan güvenlik durumu?
- Çıkışta kaçılabilecek güzergahın durumu?
- Güvenlik kameraları?
- Saldırıyı gerçekleştirme şekli ?

Siber Saldırılar- Olası Senaryo

- *Mantık aynıdır*
- *Sıradan bir hırsızdan daha planlı bir çalışma*
- *Sızılması düşünülen sistemi incele*
- *Ön hazırlık*
- *Harekete geç ve saldır*
- *Açıklıkları tespit ve…*
- *Ağı izle ve gizlen*
- *Sistemi sahiplen*
- *İz bırakma!*

Veri Toplama Aşaması-Kapsam

- Bilgi Toplamak
- Network IP aralığını bulmak
- Bulunan IP aralığındaki aktif sistemlerin tespiti
- Açık port ve erişim noktalarının tespiti
- İşletim sistemlerin tespiti
- Portlarda çalışan servislerin tespiti
- Network haritasının çıkartılması

Veri Toplama Aşaması

- Hedef sistemin en iyi şekilde tanınmasıdır
- Siber saldırı olaylarında saldırgan tarafından hedefi tanımanın yolları;
- Whois Veritabanı sorgulama
- DNS ve IP Veritabanı Sorgulama
- Domain Registration
- Nslookup

Veri Toplama Aşaması- Whois

- Domain isimlerinin tescil edilip edilmediğini, tescil edilmiş ise kim tarafından, ne zaman alındığını, alınan domainin bitiş tarihini öğrenebilmemiz için sunulan hizmete **domain sorgulama** veya **Whois Lookup** denir.

Veri Toplama Aşaması- Whois

- DNS adresleri
- Domain bitiş süresi
- IP adresi
- Domain'i kaydeden kullanıcının irtibat adresleri
- E-mail bilgileri
- Telefon bilgileri

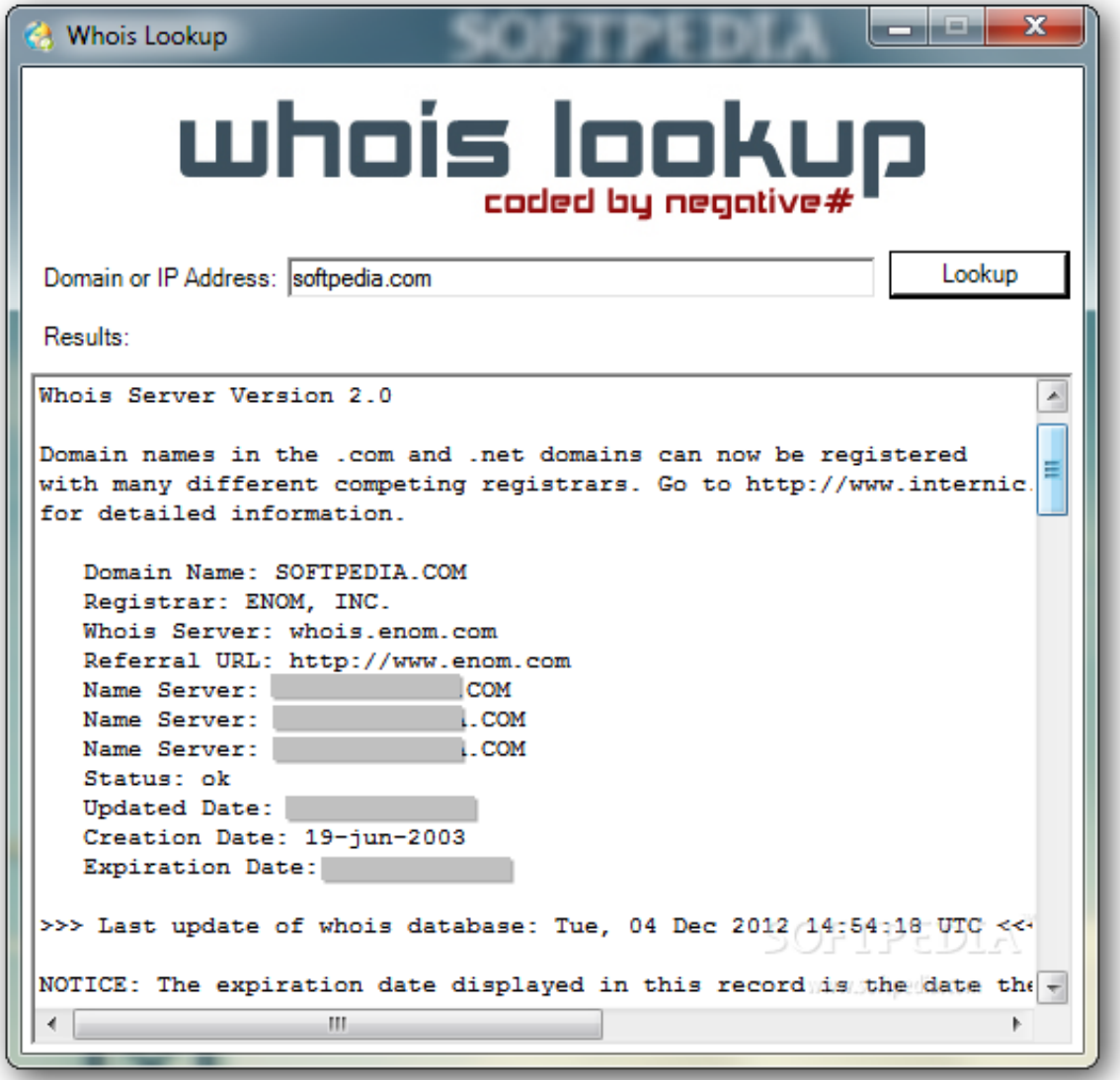
Veri Toplama Aşaması- Whois- Örnek bir domain sorgulaması

```
** Registrant:
   NETIX BİLİŞİM TEKNOLOJİLERİ YAZILIM DANIŞMANLIK EĞİTİM VE İLETİŞİM
HİZMETLERİ SAN.TİC.LTD.ŞTİ.
   fırat teknokent teknoloji geliştirme bölgesi arge-
   2 binası no:20 MERKEZ ELAZIĞ
   Elazığ,
     Türkiye
   netixbilisim@gmail.com
   + 535-920-9299
   +


** Registrar:
NIC Handle              : fp39-metu
Organization Name       : İsim Tescil İnternet Teknolojileri A.Ş
Address                 : Bulgurlu Mah. Selvili Sok. No: 16

                          İstanbul,
                          Türkiye
Phone                   : + 90-216-3299393-
Fax                     : + 90-216-3292333


** Domain Servers:
ns1.isimtescil.net
ns2.isimtescil.net

** Additional Info:
Created on..............: 2012-Sep-10.
Expires on..............: 2014-Sep-09.
```

Veri Toplama Aşaması- Whois- Kullanılabilecek Araçlar

- http://www.whois.com.tr
- http://whois.sc
- http://www.internic.net/whois.html
- Netscan Tools
- Trout

Veri Toplama Aşaması- Whois



IP ve IP sorgulama

İnternet temsilci veritabanları

- ARIN (www.arin.net)
- AFRINIC
- APNIC
- LACNIC
- RIPE

Hedef sistem alt ağ bloklarının çıkarılmasına yönelik IP taramalarının yapılabileceği sistemler.

DNS&DNS sorgulama

- Saldırgan sistem ile ilgili whois sorgusu yaptığı zaman DNS bilgilerini, NS (Name servers) veya Domain servers adı altında görür. Daha sonra detaylı DNS sorgulamaları ile daha fazla veriye ulaşabilir * . DNS sunucusu konfigürasyonunda hata varsa Zone Transfer denen DNS sunucusunun çalıştığı domain ile ilgili tüm bilgileri isteyebilir. (***nslookup – Sam Spade***). DNS ile hedef sistemin IP adresi öğrenilebilir, IP bloğu bilgisine sahip olunabilir.

*
(Hacking interface: syf:48-50)

nslookup

- DNS sunucusuna sorgu gönderip cevap almayı sağlar. Amaç DNS ‘ten IP bilgisine ulaşmaktır.

Detaylı Bilgi

- http://support.microsoft.com/kb/200525

Network aralığını tespit etmek

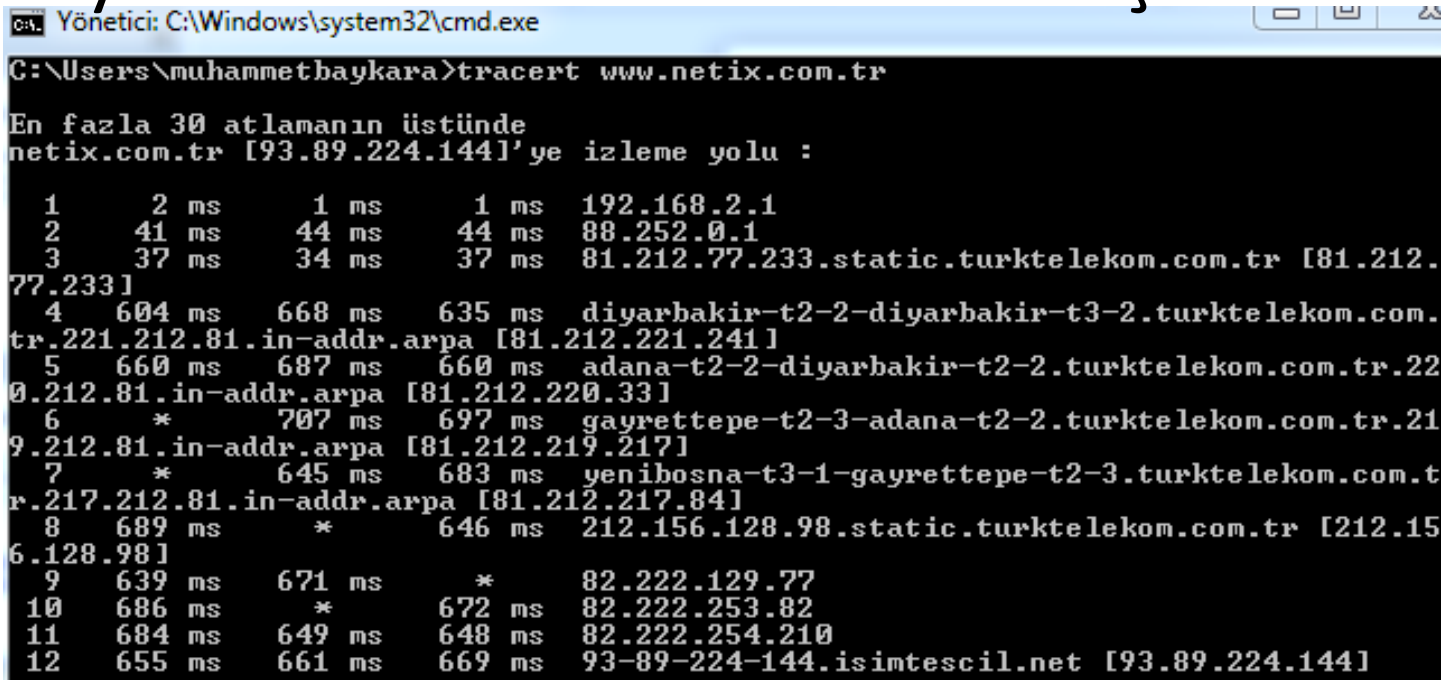
- Hedef network IP aralığının tespiti önemlidir.
- Böylece saldırgan hedefinin tüm internete açık sistemlerinin açıklıklarını tespit edebilecektir.
- Smartwhois
- My IP Suite
- Nscan

Network Haritalama

- IP adresleri tespit edildikten sonra hedef networke ulaşırken paketlerin hangi yolu takip ettiği tespit edilerek network hakkında bilgi sahibi olmaya çalışılabilir. Bunun için ***traceroute*** yapısı kullanılır;
- Windows → tracert www.firat.edu.tr
- Linux → traceroute www.firat.edu.tr

Traceroute

- Verinin noktadan noktaya ulaşımı sırasında izlenen yol.
- Bu yol izlenerek network haritası çıkarabilir.



Traceroute araçları

- Neotrace Pro → Mcafee Visual Trace
- Path Analyzer :
  network haritasını çıkarmayı sağlayan yazılım
  (www.pathanalyzer.com)
- Visual Route :
  Görsel traceroute yapan araçlardan biri
  (www.visualroute.com)

E-posta ile bilgi toplama

- Hedef bir networkte hiç yer almayan bir eposta adresine mail gönderildiğinde mail serverlar böyle bir e posta olmadığı hakkında bilgi vermek amaçlı yanıtlarlar. Bu yanıtta hedef network hakkında IP adresi ve bazı bilgiler elde edilebilir.
- Ayrıca ***E-mail header*** kayıtlarını araştıran ve bu yapılardan ip bilgisi elde etmeye yarayan ***E mail tracker pro*** vb. yazılımlar da kullanılmaktadır.

IP adresinden konum tespiti

- Bazı web siteleri bu konuda hizmet vermektedir.

Hedef Web Sitesi Hakkında Bilgi Toplama

- www.archive.org : 1996… -

  ortaklık yapılan firmalar,

  yayınlanan içerikler

  e mail adresleri

- Robots.txt

  indexlenmesi istenilmeyen dosyalar

  site sahibinin arama motorlarından gizlemek istediği alanları sağlamakla beraber kötü amaçlı kişilere de gizli klasör yollarını verir

Hedef Web Sitesi Hakkında Bilgi Toplama

- Robots.txt


```
User-Agent: ia_archiver
Disallow:

User-Agent: *
Disallow: /note/
Disallow: /search.php
Disallow: /click.php
Disallow: /search_caf.php
Disallow: /t.php
Disallow: /exitpage/
Disallow: /popup/
Disallow: /r.php
Disallow: /secondary_feed/
```

Hedef Web Sitesi Hakkında Bilgi Toplama

- netcraft.com:
  - web sunucu özellikleri
  - önceki zaman dilimlerinde kullanılan IP
  - en son ne zaman restart edildiği *

* tekrar başlatma isteyen güncelleştirmeler!

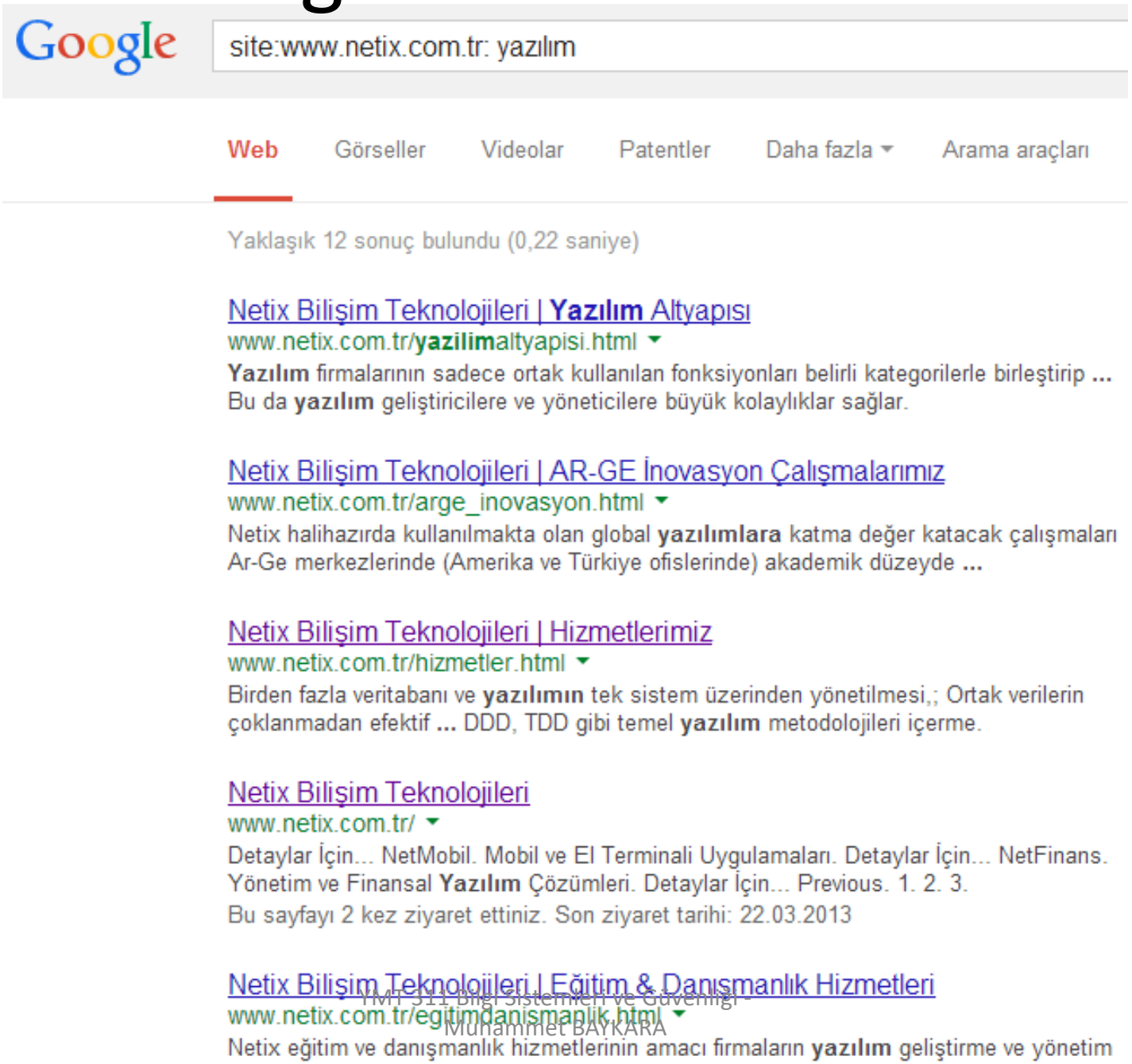
- webhosting.info

Google ile bilgi toplama

- Arama motorlarının kötü kullanımı!
- Google hacking

Google ile arama- intitle

Google ile arama- site



Google ile arama-

- Filetype:mdb belirtilen dosya uzantısı arar
- Allintext:arananveri: Sayfa başlık ve URL hariç, web sayfası metinlerini arar
- Diğer bilgi Toplama yöntemleri
  - Kariyer Siteleri
  - Sosyal siteler
  - İnsan arama motorları(pipl,peoplefind,peekyou…)

Saldırı Hazırlık Evresi-Tarama(Scanning)

- ICMP paketleri ile aktif sistemleri tespit etmek
- Kullanılabilecek araçlar
- Hedef sistemde çalışan portları dinleyen servisler
- Tcp header
- Kullanılabilecek araçlar: port tarayıcılar
- Ip adreslerini gizlemek
- Kullanılabilecek araçlar

ICMP

- Echo portu- 7. port
  - TCP/IP düzgün yapılandırılmış mı ?
  - Bilgisayarın aktif olup olmadığının tespiti
  - Ağ geçitlerine erişimin testi

  komut: ping

  - Windows : ping www.firat.edu.tr (3 adet ICMP echo paketi gönderir ve cevap bekler)
  - Linux : ping www.firat.edu.tr –c 3

ICMP-Kullanılabilecek Araçlar

- Angry IP Scanner

Belirtilen bir IP aralığını ICMP paketleri ile tarar. Böylece port tarayıcı, web sunucu tespiti, ftp sunucu tespiti yapılabilir. (www.angryziber.com)

- Diğer araçlar:
- Net Scan Tools (netscantools.com)
- Ws_PingproPack(ipswitch.com)

Portları Dinleyen Servisleri Bulmak

- Port, sistemlerimize açılan network servislerinin çalışmasını sağlayan sanal kapılardır.
- Hedef sistemdeki açık portların tespiti saldırgana sistemde çalışan servislerin bilgisini verir.
- Bu aşamada Port Tarayıcı sistemlerden yardım alınabilir.

Port Tarama

- 65535
- 0 kullanılmıyor
- 1-1024 : ayrıcalıklı, iana.org
- Iana: DNS yönetimi, ip adresleme ve internet protokollerinin denetimi

Port Tarama-Kullanılabilecek araçlar

- Nmap (Network Mapper):
  - Port tarama
  - Hedef işletim sistemi
  - Çalışan servis bilgileri ve sürümleri
  - nmap.org

  - Super Scan
  - Net Gadgets

Port tarama

- ***Shadow security scanner:***
  - Web uyg. ya da sunucudaki açıklıkları bulup bu açıkları kapatabilmeyi sağlar.
  - Tüm windows hizmetlerini, portları, olası DOS saldırılarını ve güvenlik açığı olabilecek tüm alanları tarayabilmektedir.
  - Onlarca scanner arasında CISCO, HP ve diğer network araçlarının sistem hatalarını ve aksaklıklarını bulan tek scanner!

Port tarama

- **GFI LANGuard Network Security Scanner**:
  - Muhtemel güvenlik açıklıklarını tarar ve açıklıkları korsandan önce tespit etmek amaçlı kullanılabilir.

acuNETIX Web vulnerability SCANNER

- Kişisel bilgisayar veya sunucuları taramakla yetinmez. Web uygulamalarını da tarayarak **SQL Enjeksiyon** ve **Cross Site Scripting** gibi bir çok tehlikeli açığı tespit edebilir.

Parmak izi tespiti(Fingerprinting)

- Uzaktaki makinenin işletim sistemini tespit etmektir. Araçlar;
- Autoscan(autoscan-network.com)
- Lan view (jxdev.com)
- Lan state (jxdev.com)
- Look@lan (lookatlan.com)

Saldırı Aşaması

- Sistem hakkında bilgi toplama aşamalarından sonraki aşama saldırı girişimidir.
- Web uygulamasına, sunucu bilgisayara veya herhangi bir sisteme saldırı girişimi yapılabileceğinden bu aşama çok yönlü olarak incelenmelidir.

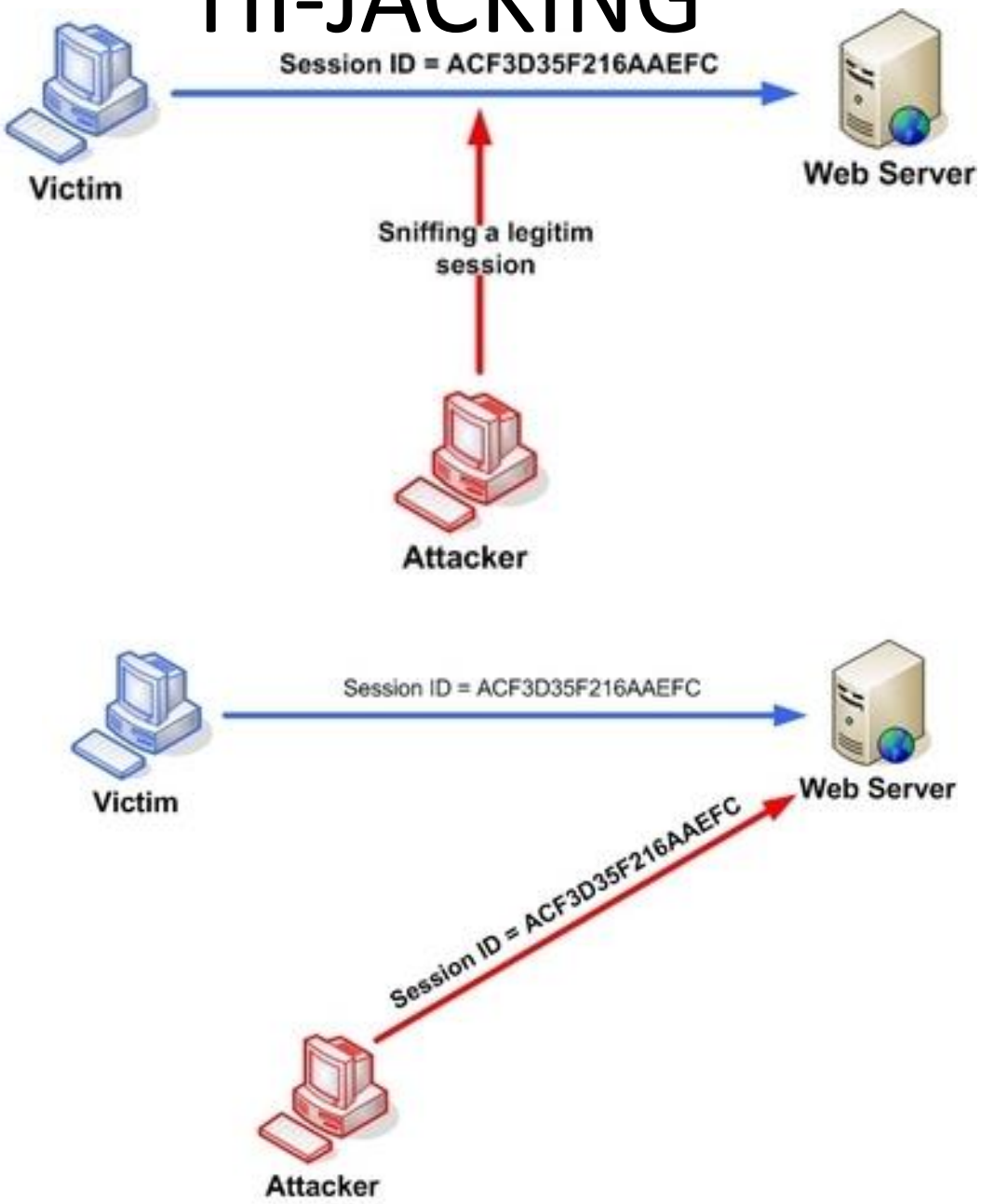
Cookie HI-Jacking

- Cookie adı verilen tanımlama bilgileri, sunucu bilgisayar tarafından istemci bilgisayarlara yerleştirilen küçük dosyalardır.
- Cookie'ler tarayıcı ve sunucu arasındaki iletişimin hatırlanmasını sağlar.
- Korsanlar tarafından da kullanılabilirler

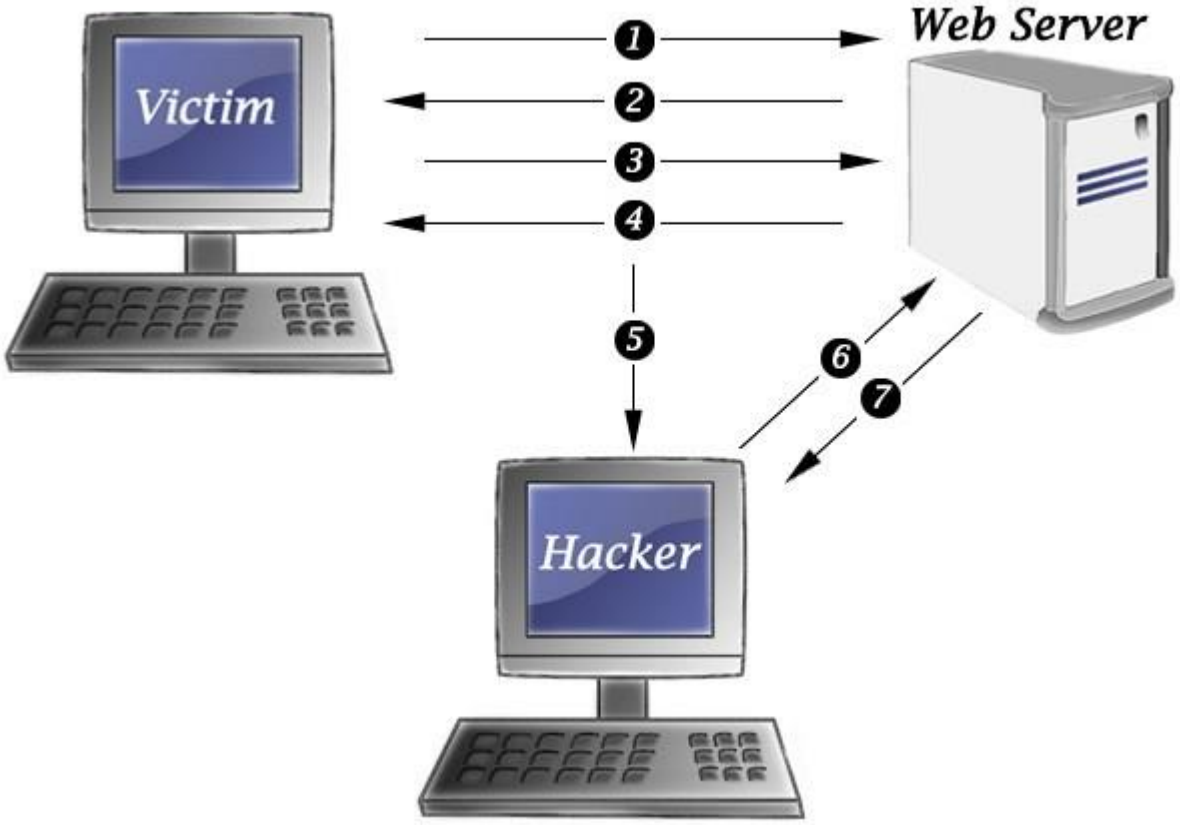
Cookie HI-Jacking

- Normal şartlarda tarayıcı ve sunucu arasında iletilmesi gereken bilgiler korsanlar tarafından sniffer yazılımları ile, trojanlar veya Cross Site Scripting saldırılarla veya javascript kodlarıyla ele geçirilebilir.

HI-JACKING


Session ID = ACF3D35F216AAEFC
Victim
Web Server
Sniffing a legitim session
Attacker
Session ID = ACF3D35F216AAEFC
Victim
Web Server
Session ID = ACF3D35F216AAEFC
Attacker

Cookie-Session HI-JACKING

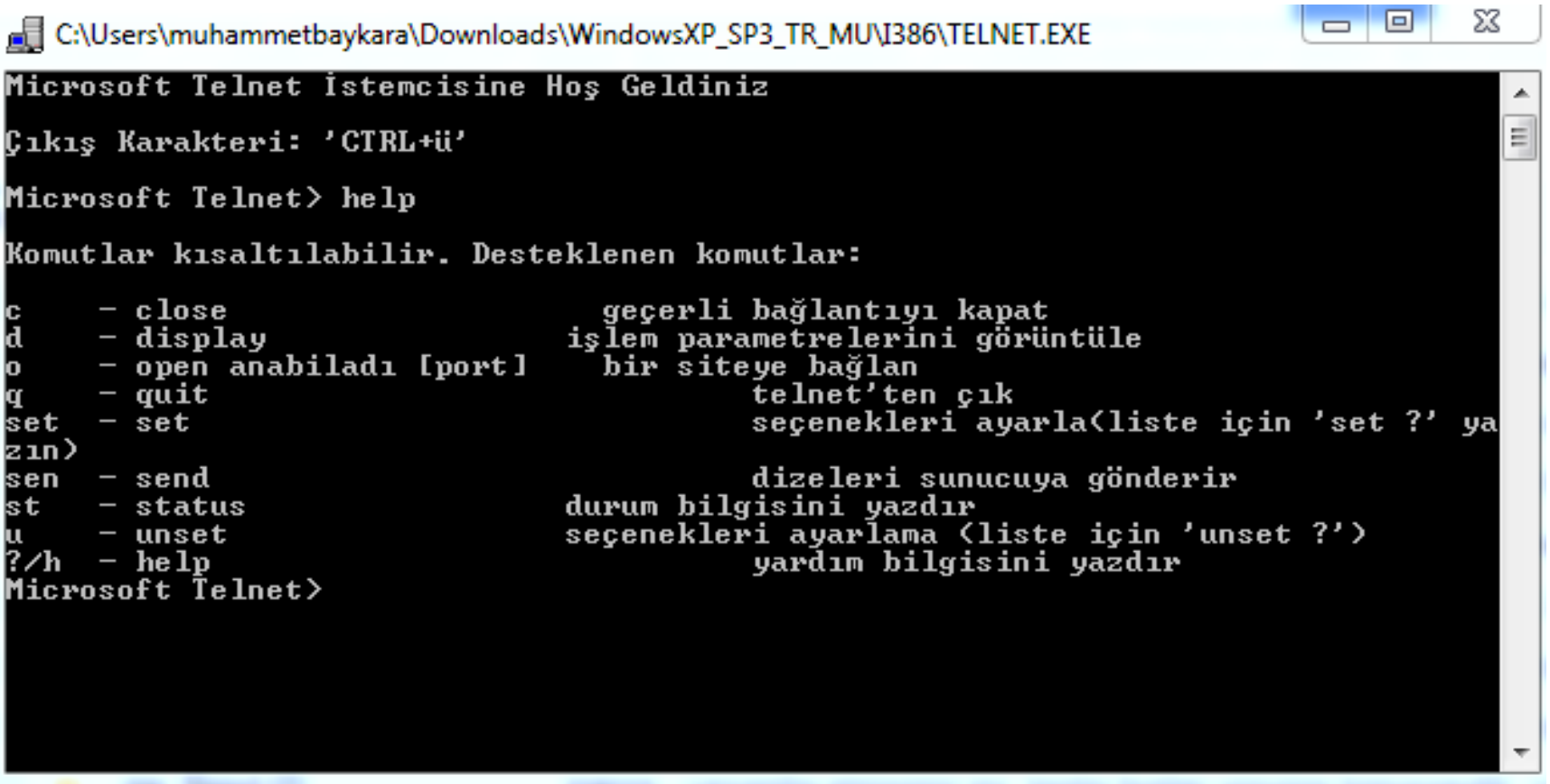


- Man in the middle- Ortadaki Adam saldırısı detaylı bilgi için http://blog.cergis.com/posts/9/prevent-session-hijacking

Cookie HI JACKING-korunma yöntemleri

- Güvenli HTTPS protokolü kullanılmalı
  - Bankacılık, online alışveriş sistemleri…
- Tanımlama bilgilerine sınırlama getirilmeli
  - CCleaner
- Java script ve activeX düzenlemeleri yapılmalı

Terminal Network-Telnet



Uzaktaki bir bilgisayara bağlanırken, sisteme yerel erişim sağlıyormuş gibi bağlanır.

telnet zaafiyetleri ve korunma yolları

- İletişimde şifreleme yapılmıyor
- İletişimde trafiği izleyen birinin olup olmadığı tespit edilemiyor
- Bu vb. zaafiyetlerinden dolayı SSH (Secure Shell) gibi protokoller kullanılabilir.

Şifre tahmin etme

- İlk aşamada uzak erişim için açık olan servisler ile sisteme bağlanılmaya çalışılır.
- Uzaktan şifre denenebilecek servisler:
  - Dosya ve yazıcı paylaşımı
  - RDP(remote desktop protocol) port 3389
  - SSH(secure shell) port 22
  - FTP port 21
  - telnet port 23
  - SMTP port 25

Şifrelere Saldırı Yöntemleri

- **Sözlük Saldırısı(Dictionary attack):** Bir sözlük ya da belirlenen kelimelerin şifre için denenmesidir.
- **Brute Force:** olabilecek bütün kombinasyonların şifre üzerinde denenmesidir.
- **Hybrid:** önce sözlük içindeki kelimeleri daha sonra da brute force mantığı ile çalışır.
- **Sosyal Mühendislik:** insani ilişkiler ile şifrelerin elde edilmeye çalışılması

Uzak sisteme şifre deneyebilen araçlar

- Enum+:

  uzak sisteme dosya yazıcı paylaşımı açık ise şifre deneyebilen bir yazılımdır. Brute force saldırısı yapabilir. (detay için bkz: securityforest.com Category : enumeration)

- Nat
- Hydra
- Tsgrinder

Kullanıcı hesaplarının şifreleri nerede?

- Windows sistemlerde kullanıcı şifreleri; Windows\system32\config altında SAM veritabanında tutulur. OS çalışırken bu dosya kilitlenmektedir. Dolayısıyla taşınması ya da kopyalanması mümkün değildir. Ancak bazı yazılımlar yerel SAM veritabanına müdahele edebilmektedir!

Hangi Yazılımlar SAM'e müdahale edebilmektedir?

- ***LC5 :*** Lophtcrack, çalışan bir sistemden SAM veritabanını açabilir ve şifrelere belirlenen yöntemlerle saldırıda bulunabilir (atstake.com).
- ***Cain&Able:*** önemli şifre kırma ve birçok aracı içerisinde bulunduran bir yazılımdır (oxid.it).
- ***John The Ripper:*** Pek çok şifreleme yöntemiyle oluşturulmuş hashleri kırabilen en hızlı araçlardan biridir. Komut satırı aracı olup hem windows hem unix sistemlerin şifrelerini kırabilmektedir. En çok kullanılan şifre kırıcılardan biri!

Exploit etmek?

- Exploit, sistemin zayıflıklarından faydalanarak sisteme giriş sağlayabilen veya zarar veren kod.
- Zayıflıkların tespitinde kullanılabilecek bazı kaynaklar da mevcuttur:
- securityfocus.com bu anlamdaki en iyi sitedir. Yeni bulunan açıklıkları sadece duyuran bir sitedir.
- Milworm.com ise securityfocus un aksine hackerların en çok ziyaret ettiği sitelerden biridir. Bir açıklık tespit edildiğinde kaynak kodlarını hemen yayınlar.

Zayıflıkların takip edilebileceği siteler

- Securityfocus.com
- Milworm.com
- Securityteam.com/exploits
- Securityvulns.com
- osvdb.org
- Nvd.nist.gov

Keylogger

- Eğer saldırgan network üzerinden sisteme sızmada başarısız oluyorsa, sisteme dışarı bilgi taşıyacak bir yazılım kurulmasını sağlayabilir.
- E-posta yoluyla, kullanıcı sistemin başında değilken trojan ya da keylogger kurabilir.
- Bazı kurumlarda kullanıcı aktiviteleri de ticari bazı keylogger lar ile izlenmektedir.
- Keylogger, sistemde gizli olarak çalışan, klavye ile OS arasına girip basılan tuşları, ekran görüntülerini ve internet aktivitelerini kayıt eden programlardır.

Keylogger

- İki çeşittir:
  - Yazılım Tabanlı
    - Spector pro
    - E-Blaster
    - Ardamax
    - Wire Tap
    - USB Dumper
  - Donanım Tabanlı

* Anti Keylogger Elite

Veri Gizleme- ADS

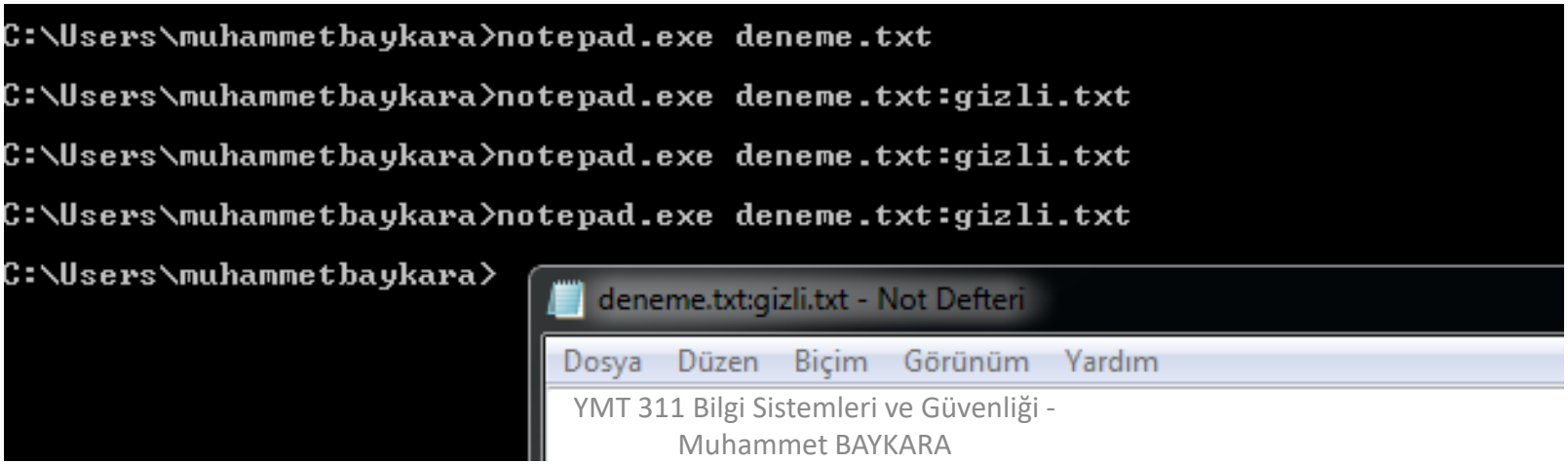
- NTFS
- ADS (Alternate Data Streams)

Örnek:

Metin belgesi içinde gizli bir başka metin belgesi

C:\notepad.exe deneme.txt

C:\notepad.exe deneme.txt:gizli.txt



ADS tespit edebilen yazılımlar

- LNS
- GMER
- Visual ADS Detector

Steganography

- Popüler bir veri saklama bilimi
- Resmin içine gizli veri saklamak
- Yasa dışı örgütler
- İçerikteki veri şifrelenedebilir

Steganography araçları

- ImageHide
- Mp3Stego
- StegoVideo
- Snow

Steganography Tespiti

- Kesin sonuç verebilen bir yöntem ya da yazılım yoktur.
- Kısıtlı da olsa kullanılan yazılımlar
  - Stegdetect
  - Stegbreak
  - SIDS

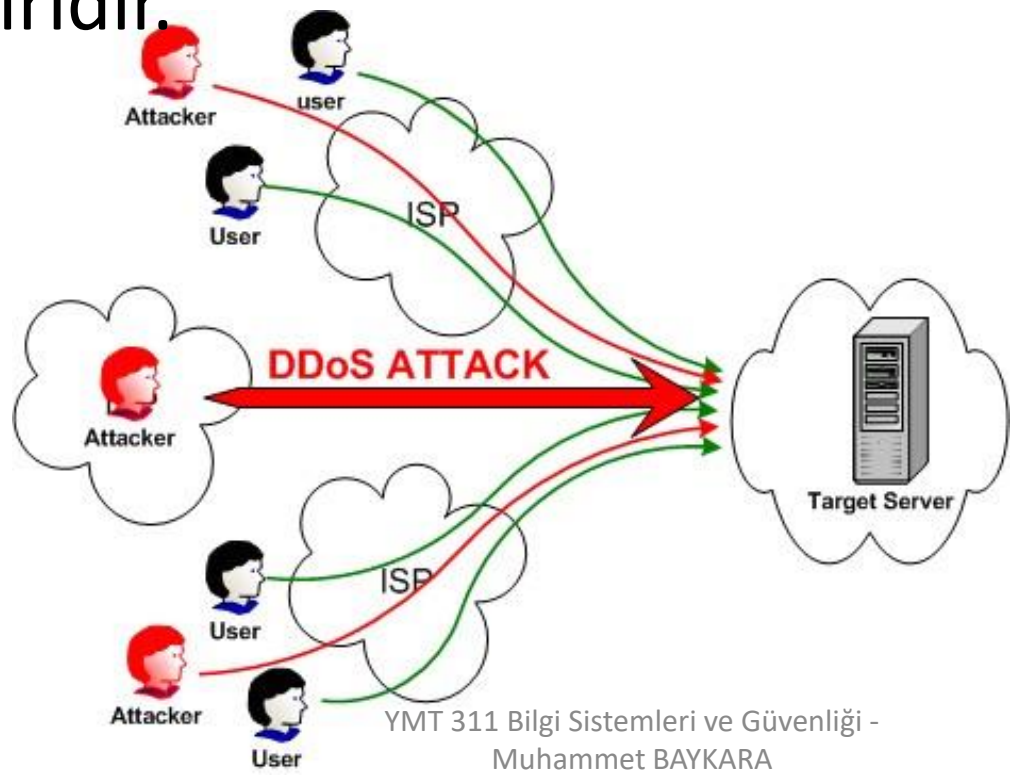
Steganography uygulamaları

- **Susan eats truffles. Under pressure, that helps everything before owning Major Bullwinkle.**
- ☺gizli bilgi?
- Bazı örnekler ve kaynaklar için;

http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/uygulamalarla-steganografi-3.html

Denial of Service- DoS

- Sistemin aşırı yüklenme sebebiyle hizmet vermesi gereken kullanıcılara hizmet vermesini engellemek ya da sistemi yavaşlatmak amaçlı saldırıdır.



DoS ? DDoS

- DoS sistemleri çalışmaz hale getirmek için yapılan saldırı.
- DDoS, DoS saldırısının yüzlerce, binlerce farklı sistemden yapılması.

Ddos hakkında yanlış bilinenler

- Bizim Firewall DOS'u engelliyor
- Bizim IPS DOS/DDOS'u engelliyor...
- Linux DOS'a karşı dayanıklıdır
- Biz de DDOS engelleme ürünü var
- Donanım tabanlı firewallar DOS'u engeller
- Bizde antivirüs programı var

- DOS/DDOS Engellenemez

DoS amaç?

- Sisteme sızma değildir!
- Sistemleri ve sistemlere erişim yollarını işlevsiz kılmak!
- E-postaların, web sitelerinin, telefonların çalışmaması!

DoS kimler yapar?

- Hacker grupları
- Devletler
- Sıradan kullanıcılar
- Çeşitli otomatik ddos atak yazılımlarıyla farklı türlerden DoS/DDoS saldırıları yapılabilmektedir.

En çok yapılan DoS yöntemleri

- SYN Flood
- HTTP Get Flood
- UDP Flood
- DNS DOS
- Amplification DOS Saldırıları
- Şifreleme-Deşifreleme DOS saldırıları
- BGP protokolü kullanan DoS saldırıları

Ddos sonucunda

Hazırlayan : Muhammet BAYKARA

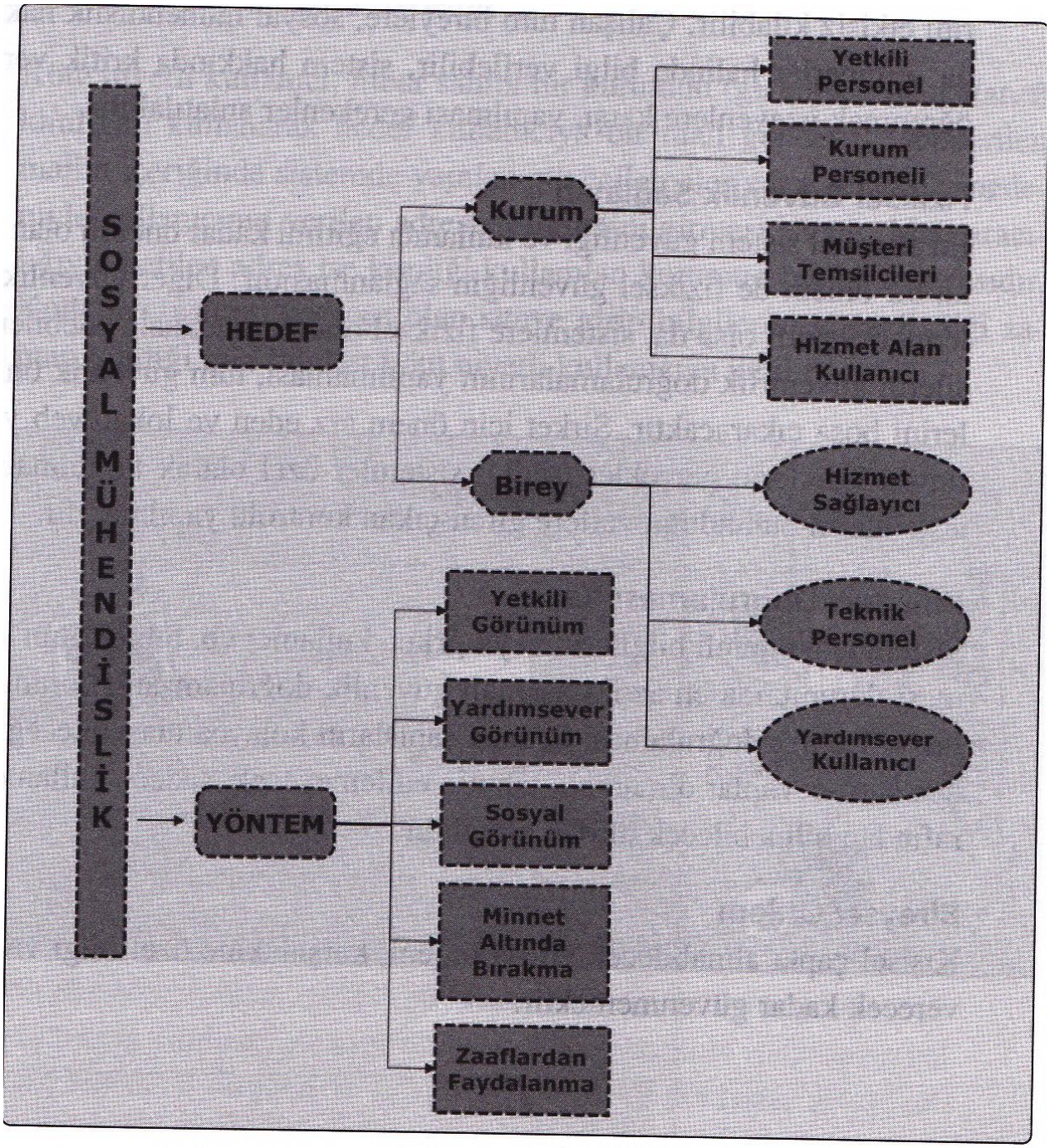
KAYNAKLAR

- Hacking Interface
- Bilişimin Karanlık Yüzü
- Casus Yazılımlar ve Korunma Yöntemleri
- Ağ ve Yazılım Güvenliği

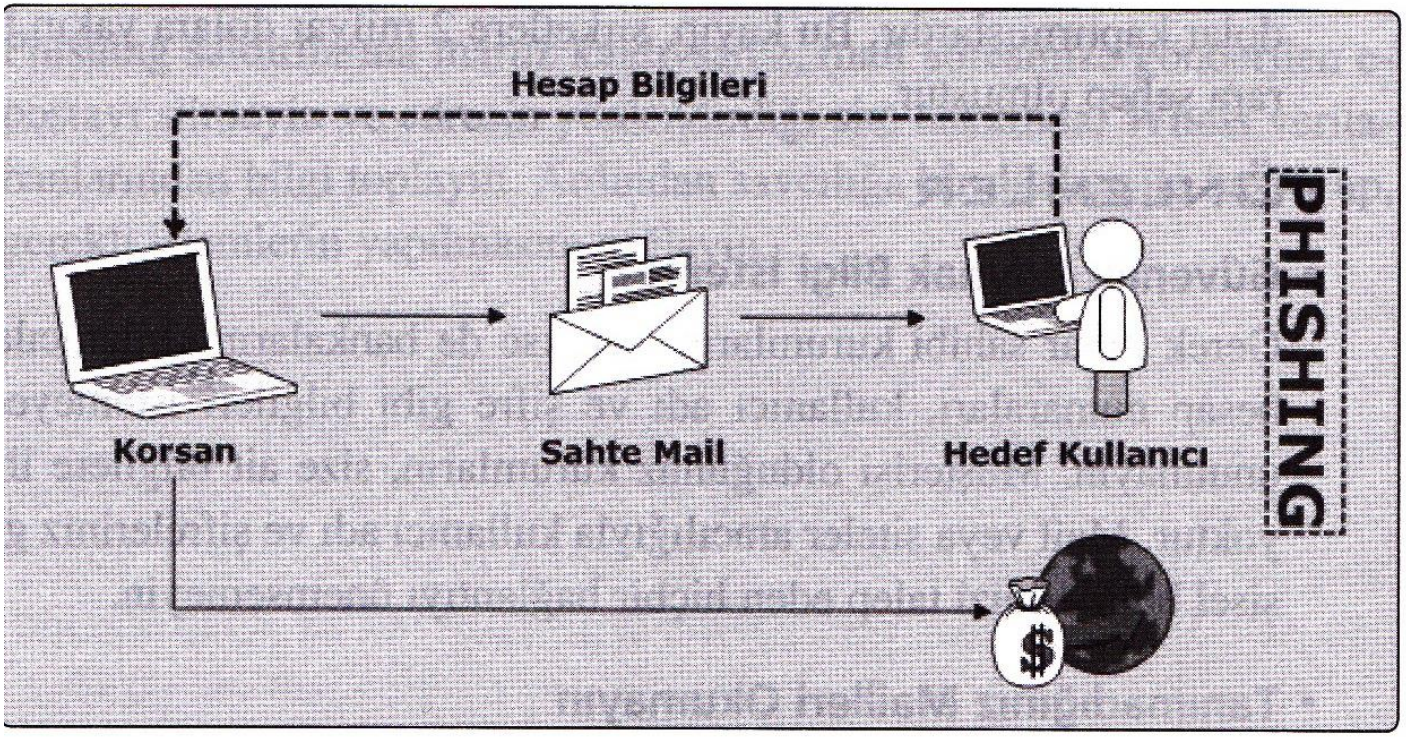
Bir Saldırının Senaryosu-2

Command Execution

- SQL Injection
- LDAP Injection
- Xpath Injection (XML)
- SSI Injection
- XSS


SOSYAL MÜHENDİSLİK
HEDEF
YÖNTEM
Kurum
Birey
Yetkili Personel
Kurum Personeli
Müşteri Temsilcileri
Hizmet Alan Kullanıcı
Hizmet Sağlayıcı
Teknik Personel
Yardımsever Kullanıcı
Yetkili Görünüm
Yardımsever Görünüm
Sosyal Görünüm
Minnet Altında Bırakma
Zaaflardan Faydalanma

Phishing-oltalama



Phishing-Oltalama- Örnek E-mail

Örnek Bir Phishing Saldırısı

Sayın Müşterimiz;

A Bank olarak kullanıcı güvenliğini sağlamak amacıyla Türkiye'de ilk defa gerçekleştirilecek olan SMS ile tek kullanımlı şifre uygulamasına geçiyoruz. Online bankacılık işlemlerinde giriş yapabilmek için kullanılacak şifre, bankamız aracılığıyla tek kullanımlık olmak üzere cep telefonunuza SMS aracılığıyla iletilecektir.

Müşterilerimizin güvenliği için zorunlu olan bu uygulamanın aktif olabilmesi için bilgilerinizi güncellemeniz gerekmektedir.

Kullanıcı bilgilerinizi güncellemek için tıklayın.

A Bank

(*A Bank örnektir.*)

İzleme ve Gizlenme

- SNIFFING:
  - Wireshark (wireshark.org)
  - Microsoft Network Monitor
  - Pilot (cacetech.com)
  - EtherDetect (.com)
  - Dsniff (//monkey.org/~dugsong/dsniff)
  - Ntop(linux sistemler için, ntop.org)
  - Etherape, network probe, tcpdump/windump, IRIS

İzleme ve Gizlenme

- SPOOFING: IPBaşlık formatı!

Internet protokolü paketlerin yönlendirilmesi sırasında gelen paketin gerçek bir Ethernet arayüzüne sahip bir node'dan gelip gelmediğinin kontrolünü yapmaz. Bu saldırganların ilgisini çeken bir durumdur.

IP paketi içerisindeki Kaynak IP bilgisinin değiştirilmesiyle hedefteki yapıdan ve sistemden gizlenme şeklindeki saldırı türüdür.

Sistemi Sahiplenme

- Saldırıların sürekliliğini sağlamak için bazı yöntemlerle sistemin ele geçirildikten sonra, daha sonraki zamanlar için sahiplenilmesi.
- Amaç;
  - Sisteme sonradan tekrar erişim sağlamak
  - Yetkileri artırmak
  - Kullandığı dosyaları gizlemek
  - Uzaktan dosya çekmek
  - Sistemi/ ağı izlemek vb…

Sistemi Sahiplenme

- Bu amaçla kullanılabilecek yapılar;
  - Backdoor
  - Trojan
  - Rootkit
  - Netcat

Sistemi Sahiplenme-Backdoor

- Sisteme başarıyla sızan bir saldırgan sonradan tekrar erişmek isteyebilecektir. Bu amaçla backdoor araçları kullanılır.
- Kullanılan backdoor araçları sistem yöneticisinden habersiz, korsanın sisteme bıraktığı scriptleri çalıştırabilir ve ağ/internet üzerinden ilgili detayları korsana iletebilir.

Backdoor ile sömürü şekilleri

- Belirli periyotlarla korsan bilgisayarla bağlantı
- Sistem üzerinden herhangi bir servisi aktif etme
- Sniffing imkanı ile şifre gibi bilgileri yakalama
- Sisteme uzaktan dosya çağırma.
  - Reverse www shell.

Sistemi Sahiplenme-Trojan/Truva atı

- İstemci- Sunucu mantığı
  - Trojanlı sistem açıldığında hemen istemcisi ile sunucusu iletişime başlar
- Kendi başına çalışmama
  - Standart bir trojan kendi kendini çalıştırmaz. Sosyal mühendislik ile veya resim, oyun, program dosyası görüntüsüyle hedefe yüklenebilir…

Sistemi Sahiplenme-Rootkit

- Hedef bir sistemin dosya ve süreçlerini gizlemek veya değiştirmek suretiyle manipüle eden uygulamalardır.
  - Süreç ve dosyaları gizleyebilme
  - Registry kayıtlarını gizleyebilme
  - Ağ trafiğini izleyebilme
  - Sistem kontrolünü dışarıya verebilme
  - Arka kapı açabilme vb bir çok görevi yapabilirler.

Sistemi Sahiplenme- Rootkit

- Chkrootkit
- Rkhunter
- Sophos anti-rootkit
- F-secure blacklight

Sistemi Sahiplenme- Netcat

- Tcp veya udp ile gerçekleştirilen bağlantılarda verileri işlemek için kullanılan uygulamalardan birisidir.
- Belirlenen port üzerinden hedefe TCP bağlantısı gerçekleştirilebilir.

Ön Söz

Bilgisayar korsanları, önemli bilgiler içeren web uygulamalarına arama motorları sayesinde kolayca erişebiliyorlar. Hedeflenen anahtar kelimeler ile web sitelerinden önemli bilgiyi almak saniyeler sürüyor.

Dizin listelemeye açık dizinler, hata mesajları, yönetici veya kullanıcı bilgileri/dosyaları, çeşitli veritabanı dosyaları veya önemli veri içeren dosyalar, sunucular hedeflenerek önemli bilgiler elde edilir.
Örneğin ; Hedef bir firma hakkında genel iletişim bilgileri , telefon numaraları, e-postaları, şirket yapısı gibi gibi bilgiler, güvenlik zaafiyeti olan uygulamaya sahip adresler, web server bilgileri arama motorları sayesinde kolayca elde edilebilmekte.

Belge mümkün olduğu kadar kısa ve basit tutulmuş ve saldırganların hacking yaparken Google arama motorunu nasıl etkili şekilde kullandıkları somut örneklerle anlatılmıştır.

Google Hacking

Google en iyi ve en geniş içeriğe sahip kendini kanıtlamış bir arama motorudur.Google örümcekleri sıklıkla websitelerini ziyaret eder ve içeriğini (sayfalar , klasorler ,dizinler vb.) indeksleyerek veritabanına kaydeder. Arama sonuçlarında belirli kriterlere göre sıralar.
Temel kullanım bilgilerini aşağıdaki adresten öğrenebilirsiniz;
http://www.google.com/help/basics.html

Gelişmiş Google Operatörleri

Google, kendisi için özel anlama sahip sorgu kelimeleri olan çeşitli gelişmiş operatörleri destekler. Tipik olarak bu operatörler arama işlemini etkilemekte ve hatta Google'a farklı türde arama yapmasını söylemektedirler.

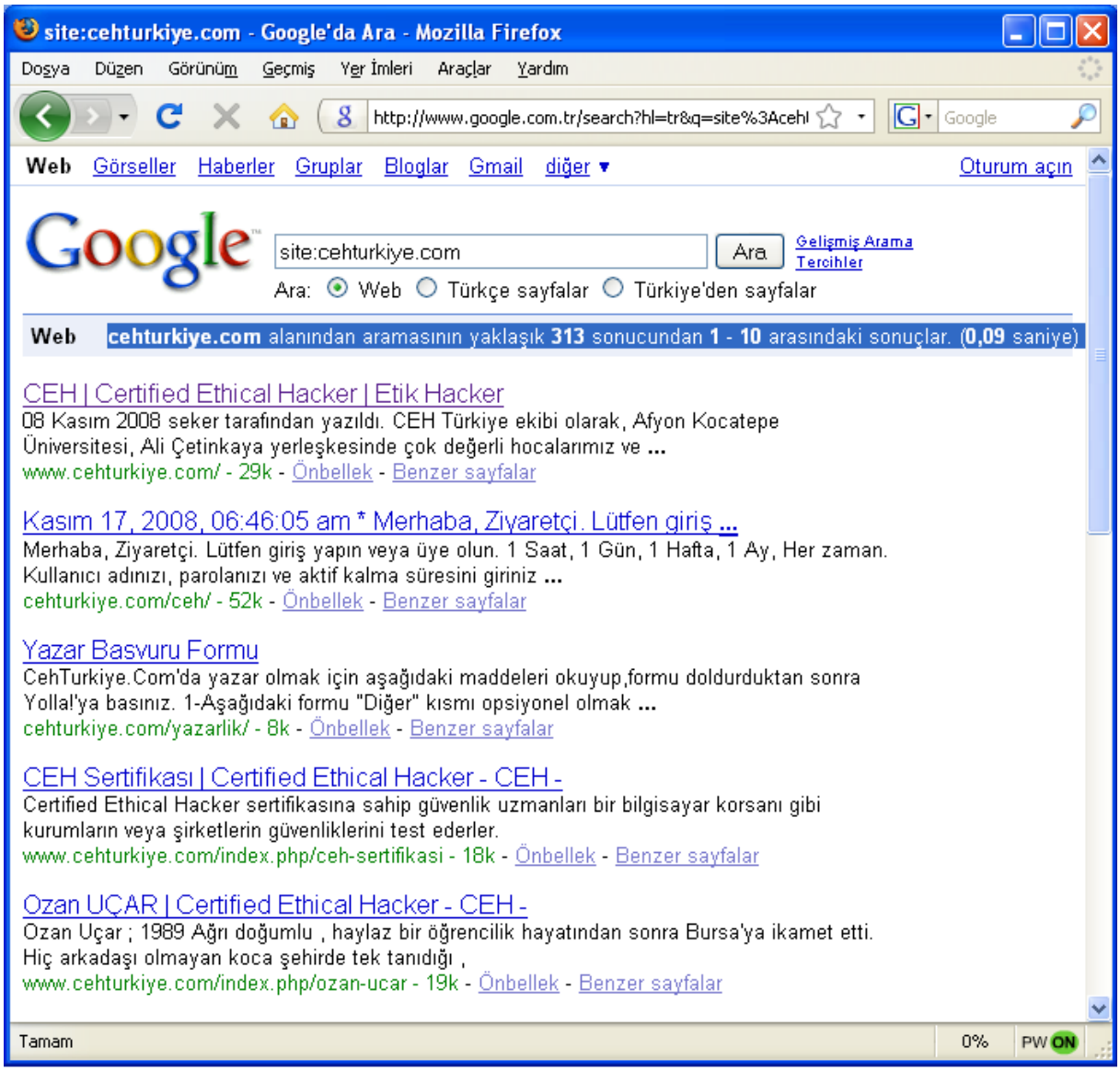
Google gelişmiş operator lislesine aşağıdaki adresten ulaşabilirsiniz;

http://www.google.com/help/operators.html

Bir Domain İçin Arama

[site:] operatörü ile arama yapılarak Google sonuçları, istenilen alan adındaki web siteleriyle sınırlandırılabilir.
Bir örnek ile inceleyelim :
Örnek #1 :

```
site:cehturkiye.com
```



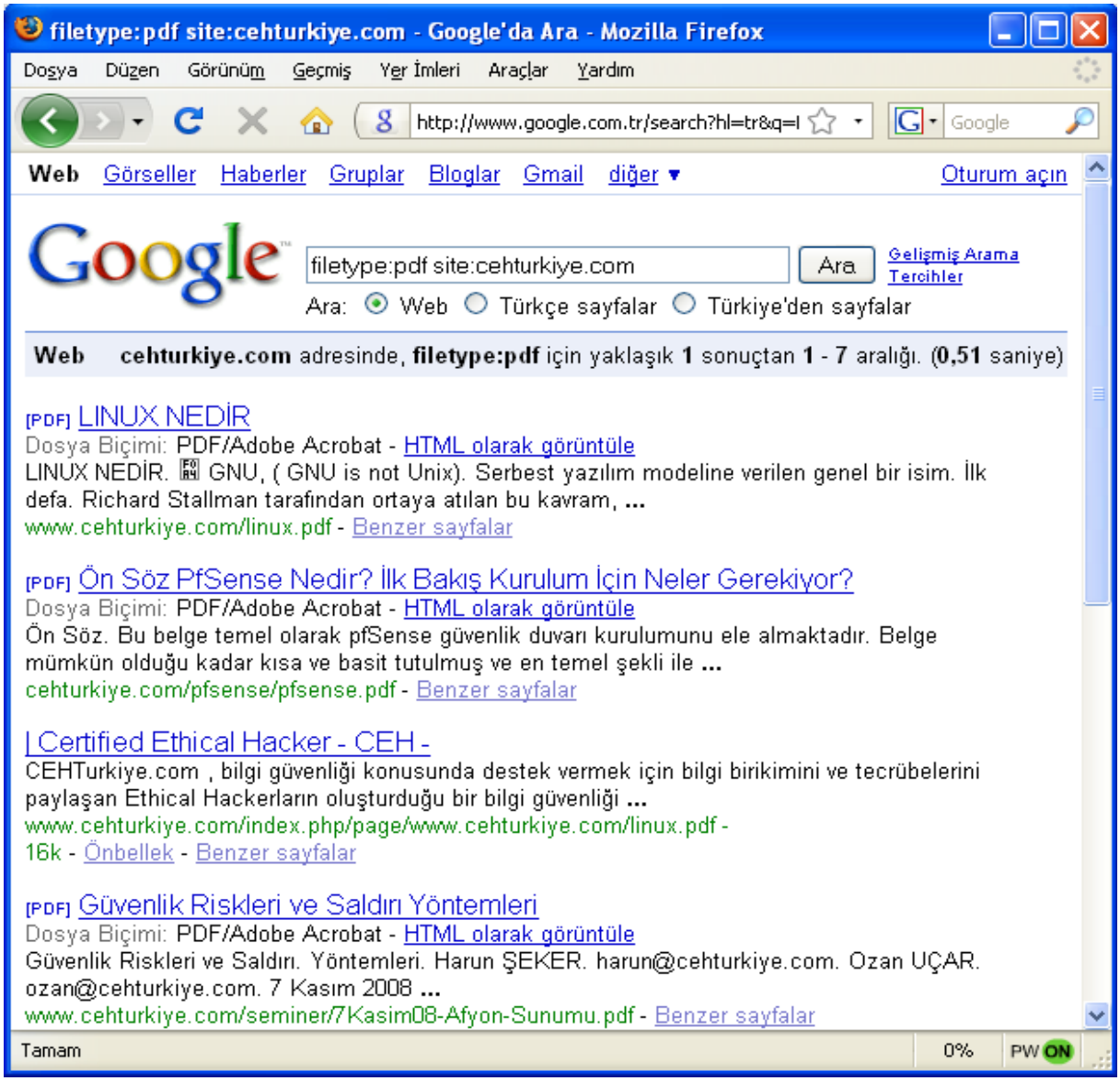
Yukarıdaki resimde de görüldüğü gibi google , daha önce farklı zamanlarda hedef site (cehturkiye.com) ile ilgili gezip keşfettiği ve veritabanına kaydettiği tüm içeriği sundu.

Özel Dosya Arama

[Filetype:] operatörü ile evrensel olarak google ön belleğinde olan siteler üzerinde veya hedef bir site üzerinde istenilen dosya türü listelenebilir ; Örnek #2:

```
filetype:pdf  site:cehturkiye.com
```

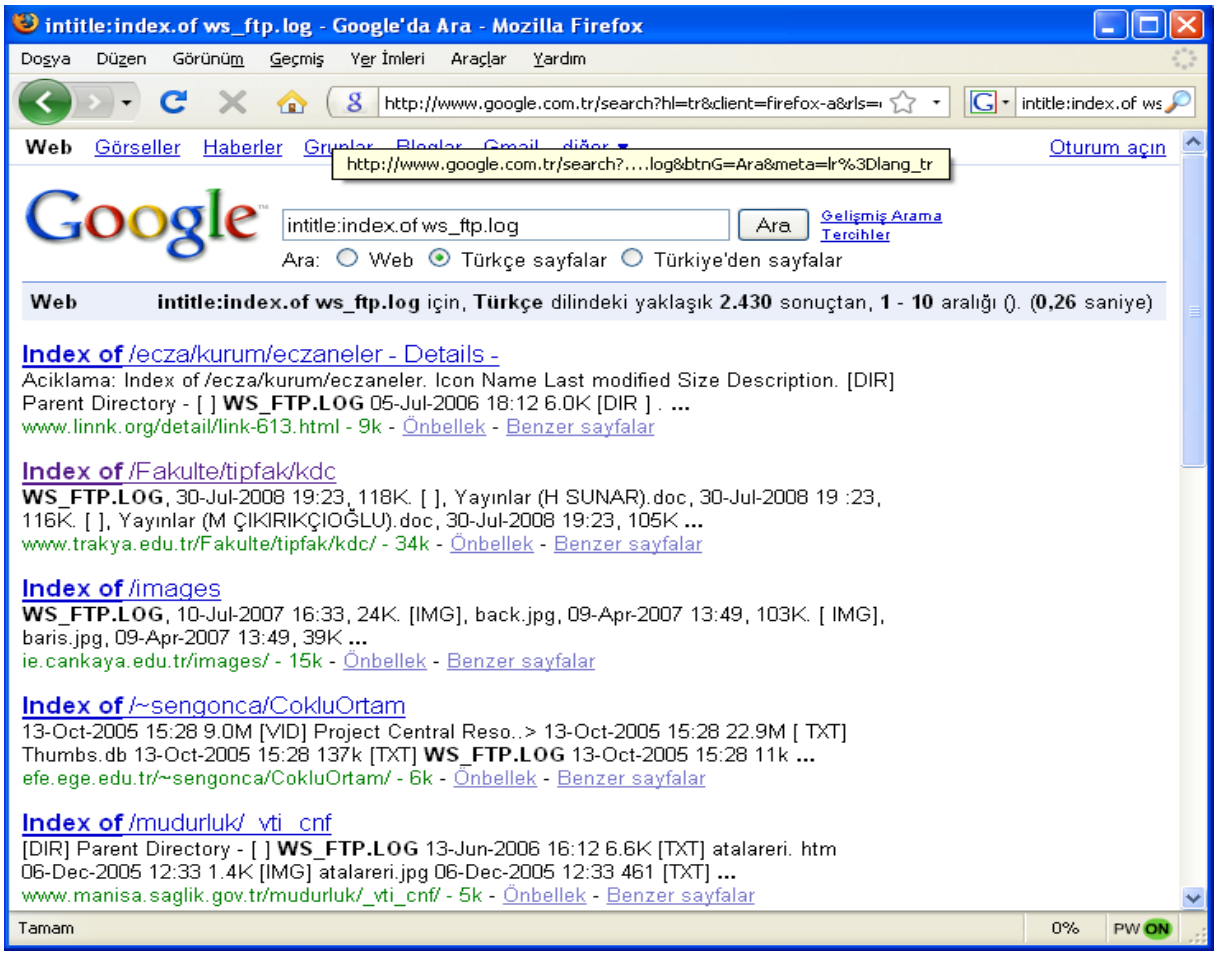
cehturkiye.com da bulunan **.pdf** uzantılı dosyaları listeleyebiliriz.
Bu arama tekniği örneklerle çoğaltılabilir.Saldırganların hedef site üzerinde bulmak istedikleri uzantıları aramakda sıklıkla kullanırlar.



Dizin Listeleme

[intitle:] operatorü kullanılarak **intitle:index.of** ile dizinler listelenebilir.
Örnek #3 :

intitle:index.of ws_ftp.log



ws_ftp.log anahtar kelimesini ekleyerek ws_ftp.log dosyasının olduğu dizinleri listeleyebiliriz. ws_ftp.log dosyası ; ftp olaylarının kayıt edildiği dosyadır bulunduğu adresdeki ftp olayları ile ilgili özel bilgiler görüntülenebilir.

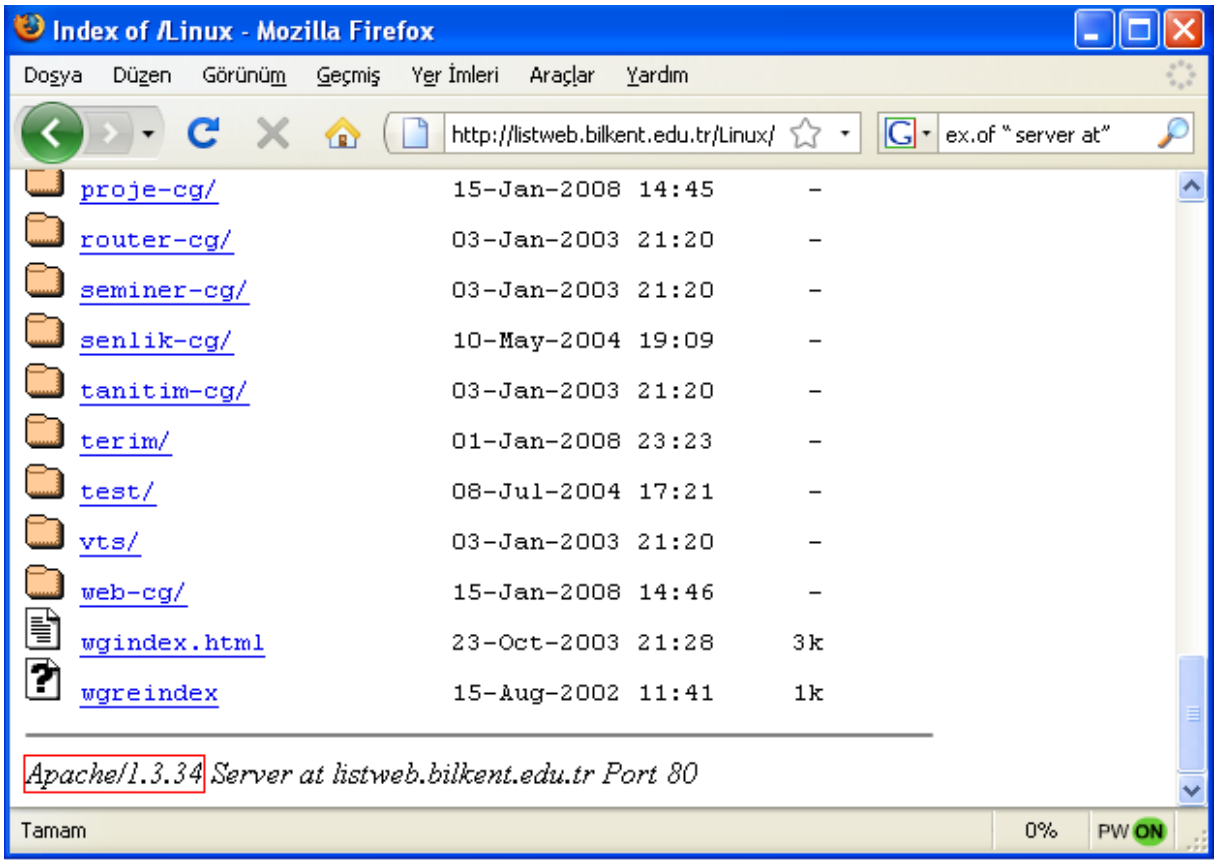
Örnek;
http://www.trakya.edu.tr/Fakulte/tipfak/kdc/WS_FTP.LOG

104.12.31 16:18 B e:\DocumentsandSettings\umid\MyDocuments\wwwroot_31_05_2004\Fakulte\tipfak\kdc\Hasta_Bilgilendirme_kitabi.pdf --> 193.255.140.21 /var/www/html/a1/kdc Hasta_Bilgilendirme_kitabi.pdf

Örnek #4 :

intitle:index.of “server at”

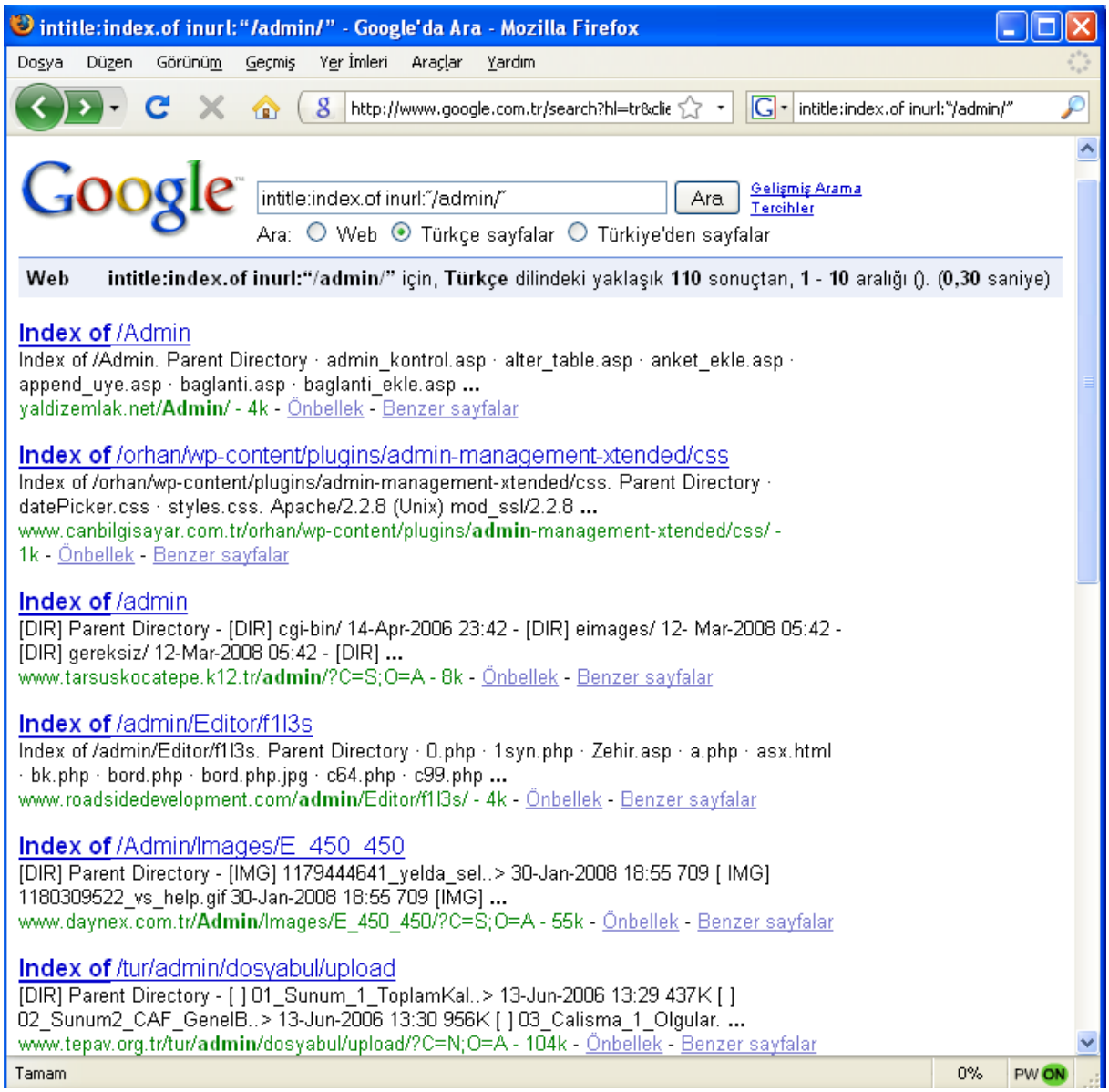
Özel dizinleri listelerken **“server at”** anahtar kelimesini ekleyerek sitelerin sunucu bilgisini öğrenebiliriz.Bu örnekler çoğaltılabilir ve amaca göre farklı aramalar gerçekleştirilebilir.



Örnek #5 :

intitle:index.of inurl:"/admin/"

intitle:index.of ile birlikte **inurl:"/admin/"** yazarak admin dizini olan listelemeye açık siteleri görüntüleyebiliriz.



Güvenlik Zaafiyeti Olan Web Uygulamalarının Tespiti

Saldırganlar ve kötü niyetli hackerlar güvenlik zaafiyetini keşfettikleri uygulamalara sahip siteleri bulmak için arama motorlarını sıkca kullanırlar.

Örnek web açıklıkları ve google arama yöntemleri

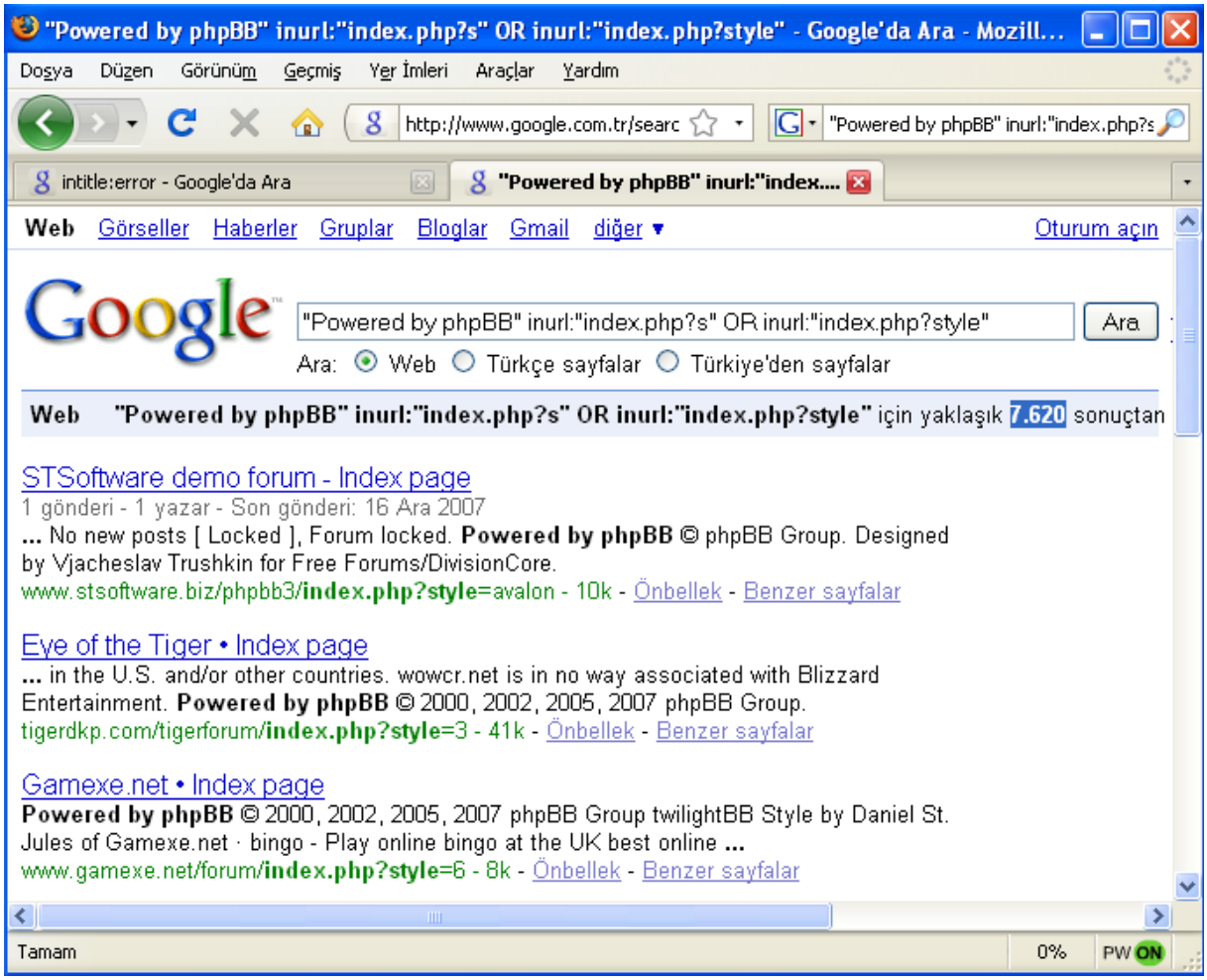
Query	Vulnerability
"Powered by A-CART"	A-CART 2.x vulnerable to cross-site scripting
inurl:"dispatch.php?atknodetype" | inurl:class.atkdateattribute.js.php	Achievo .8.x could allow remote code execution
intitle:guestbook "advanced guestbook 2.2 powered"	Advanced Guestbook v2.2 has an SQL injection problem that allows unauthorized access
"Powered by AJ-Fork v.167"	AJ-Fork, a fork based on the CuteNews 1.3.1 core, is susceptible to multiple vulnerabilities
"BlackBoard 1.5.1-f | ¬© 2003-4 by Yves Goergen"	BlackBoard 1.5.1 has a remote file inclusion vulnerability
"BosDates Calendar System " "powered by BosDates v3.2 by BosDev"	BosDates 3.2 is vulnerable to SQL injection
inurl:changepassword.cgi —cvs	changepassword.cgi allows for unlimited repeated failed login attempts
"Copyright ¬© 2002 Agustin Dondo Scripts"	CoolPHP 1.0 has multiple vulnerabilities
"Powered by CubeCart 2.0.1"	CubeCart 2.0.1 has an SQL injection vulnerability
*"Powered *: newtelligence" ("dasBlog 1.6"| "dasBlog 1.5"| "dasBlog 1.4"|"dasBlog 1.3")*	DasBlog versions 1.3–1.6 are susceptible to an HTML injection vulnerability in their request log
"Powered by DCP-Portal v5.5"	DCP-Portal version 5.5 is vulnerable to SQL injection
"2003 DUware All Rights Reserved"	DUForum 3.0 may allow a remote attacker to carry out SQL injection and HTML injection attacks
"inurl:/site/articles.asp?idcategory="	Dwc_Articles 1.6 has multiple input validation problems
inurl:custva.asp	EarlyImpact Productcart v1.5 contains multiple vulnerabilities
inurl:"/becommunity/community/index.php?pageurl="	E-market prior to 1.4.0 contains various vulnerabilities
intitle:"EMUMAIL - Login" "Powered by EMU Webmail"	EMU Webmail 5.6 messaging product is susceptible to a cross-site scripting vulnerability
"Powered by FUDforum"	FUDforum 2.0.2 allows manipulation of arbitrary server files
"1999-2004 FuseTalk Inc" -site:fusetalk.com	FuseTalk forums (v4) are susceptible to cross-site scripting attacks
"Powered by My Blog" intext: "FuzzyMonkey.org"	FuzzyMonkey 2.11 has an SQL injection vulnerability
"Powered by Gallery v1.4.4"	Gallery 1.4.4 allows remote code execution
intitle:gallery inurl:setup "Gallery configuration"	Gallery default configuration files allow gallery modification
inurl:"messageboard/Forum.asp?"	GoSmart Message Board (specific versions) are susceptible to SQL injection attack and cross-site scripting attack
intitle:welcome.to.horde	Horde Mail prior to 2.2 has had several reported vulnerabilities
"Powered by IceWarp Software" inurl:mail	IceWarp Web Mail (versions prior to 5.2.8) is reported prone to multiple input validation vulnerabilities
"Ideal BB Version: 0.1" -idealbb.com	Ideal BB 0.1 is susceptible to multiple vulnerabilities
"Powered by Ikonboard 3.1.1"	IkonBoard 3.1.1 allows cross-site scripting
*"Powered by Invision Power Board(U) v1.3 Final ¬© *"*	Invision Power Board v1.3 is vulnerable to SQL injection
inurl:wiki/MediaWiki	MediaWiki 1.3.5 has a cross-site scripting vulnerability
*"Powered by Megabook *" inurl:guestbook.cgi*	MegaBook 2.0 is prone to multiple HTML injection vulnerabilities
"Powered by mnoGoSearch - free Web search engine software"	mnGoSearch 3.1.20 and 3.2.10 contain a buffer overflow vulnerability

Örnek #6 :
Geniş bir kesim tarafından kullanılan phpBB (popular open source forum software) forum scriptinde güvenlik zaafiyeti bulan saldırgan phpBB kullanan web sitelerini topluca bulmak isteyecektir.Bunun için google.com da kücük bir arama ile hızlıca google önbelleğinde ki tüm phpBB kullanan siteleri tespit edebilir.

Güvenlik zaafiyetinin duyurusuna ve exploit kodlarına aşağıdaki adresten erişebilirsini:
http://www.milw0rm.com/exploits/1469

"Powered by phpBB" inurl:"index.php?s" OR inurl:"index.php?style"

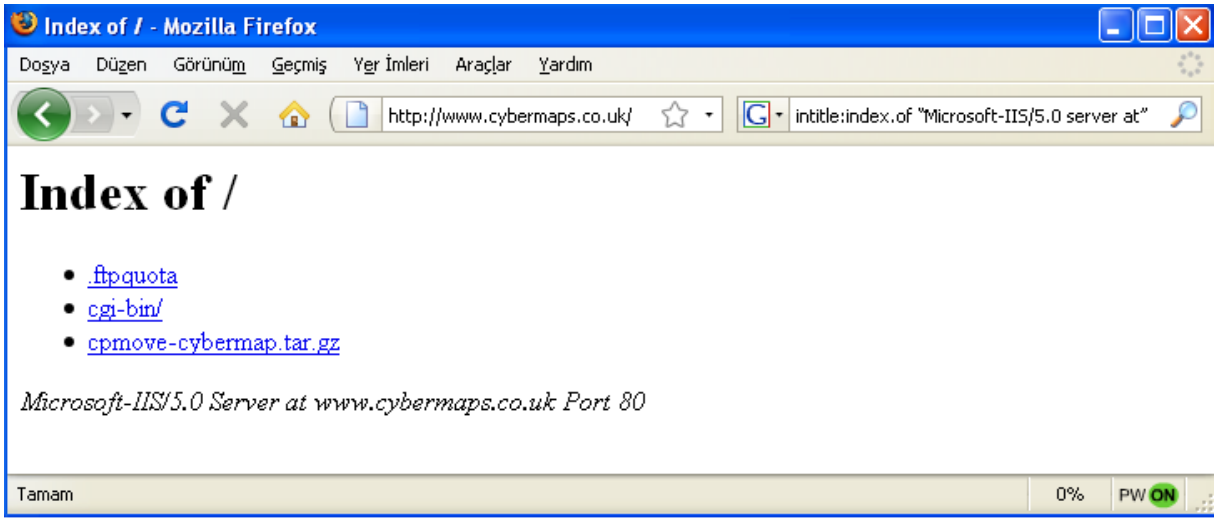
Yapılan arama için yaklaşık 7.620 kayıt bulundu **:)**



Web Serverların Tespiti

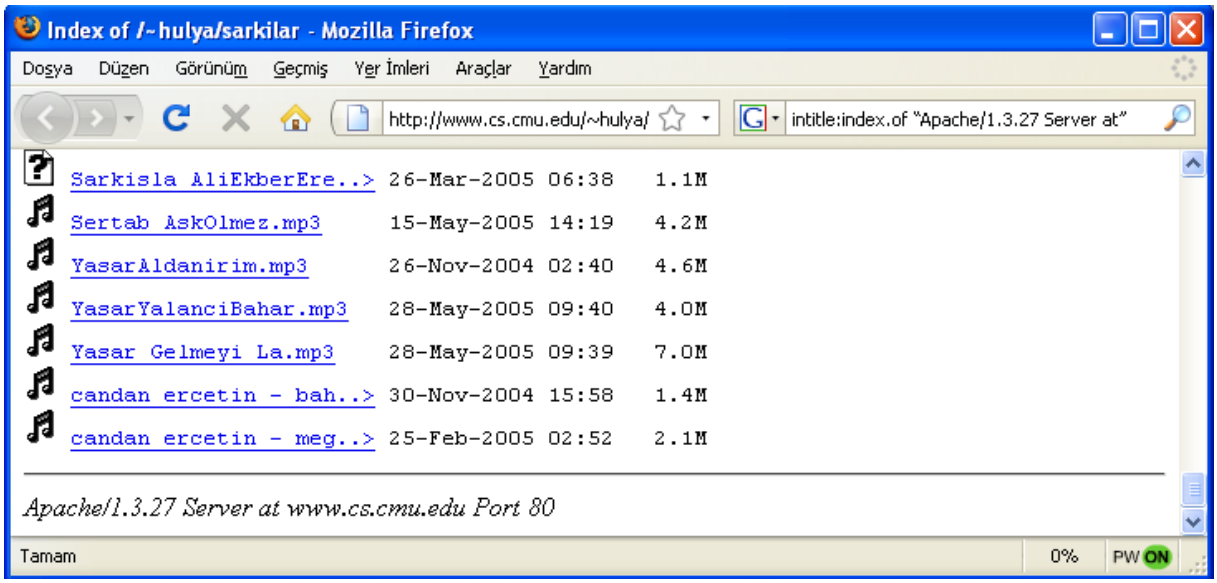
"Microsoft-IIS/5.0 server at"

Microsoft-IIS/5.0 web serverları tespit etmek için **"Microsoft-IIS/5.0 server at"** sorgusu kullanılabilir.



"Apache/1.3.27 Server at"

Apache web serverları tespit etmek için **"Apache/1.3.27 Server at"** sorgusu kullanılabilir.

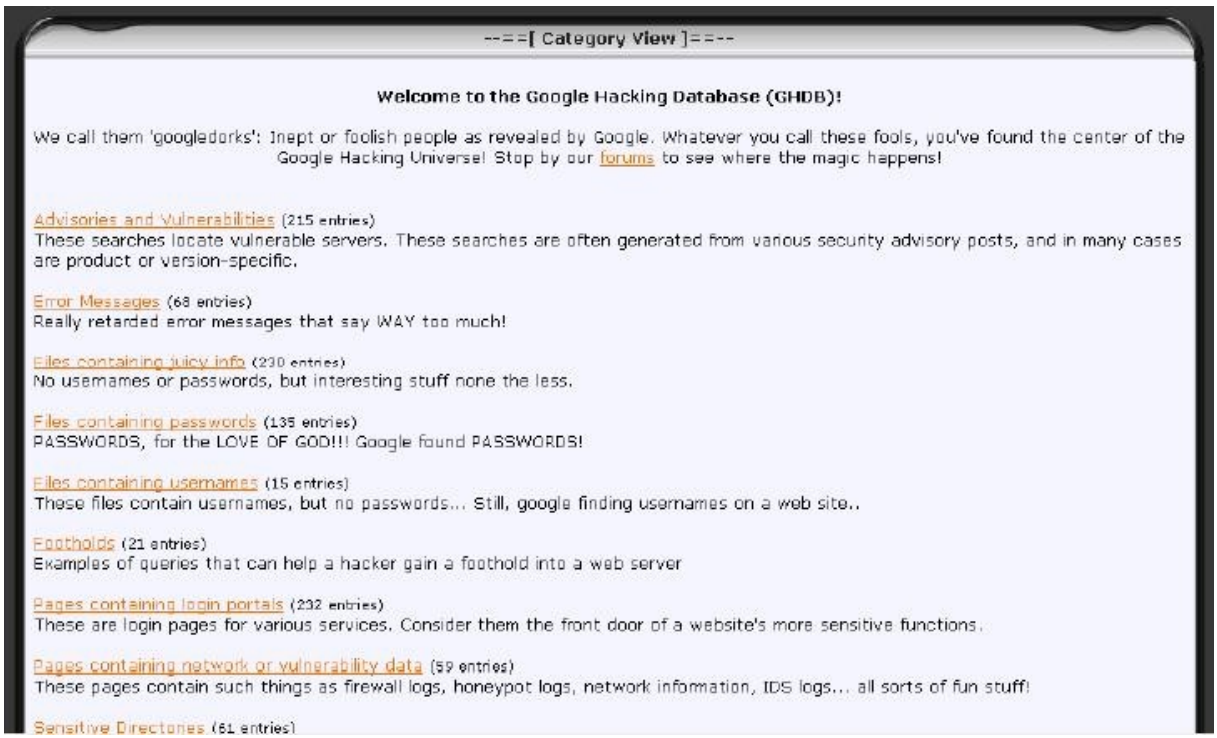


Google Hacking Araçları

Google Hacking Database (GHDB)

Hassas ve önemli bilgilere erişmek için google arama sorgularını içerir.
Daha fazlası için aşağıdaki adresi ziyaret edebilirsiniz;

http://johnny.ihackstuff.com

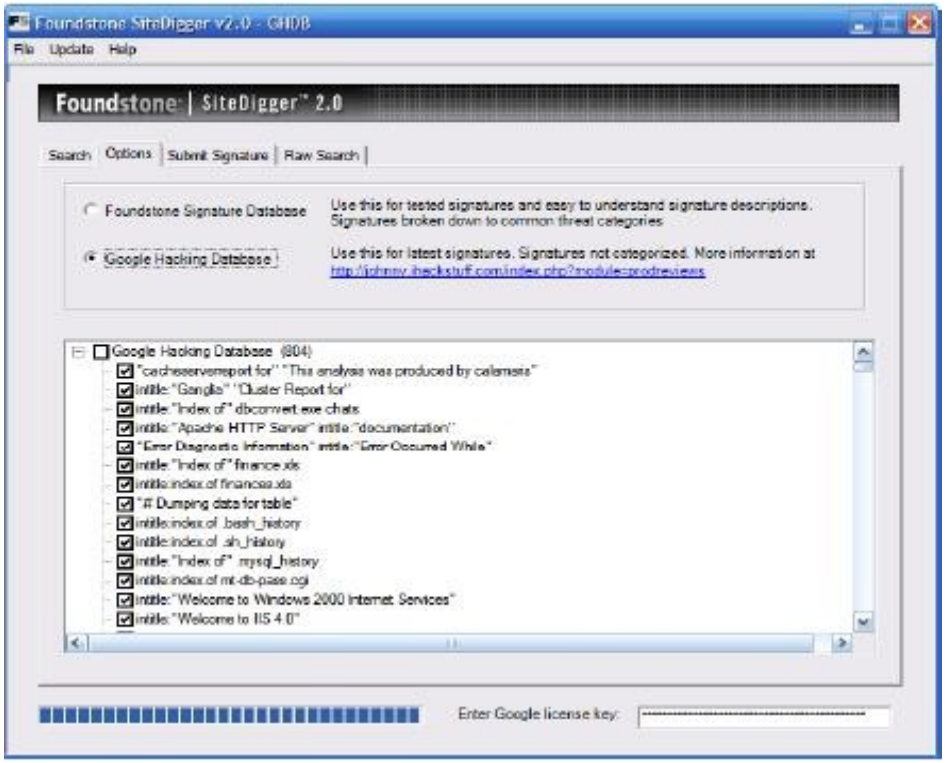


SiteDigger Tool

Google önbelleğinde değişik güvenlik zaafiyetleri, hataları, yanlış konfigurasyonu olan siteleri bulmakiçin kullanılan güzel bir araçtır.

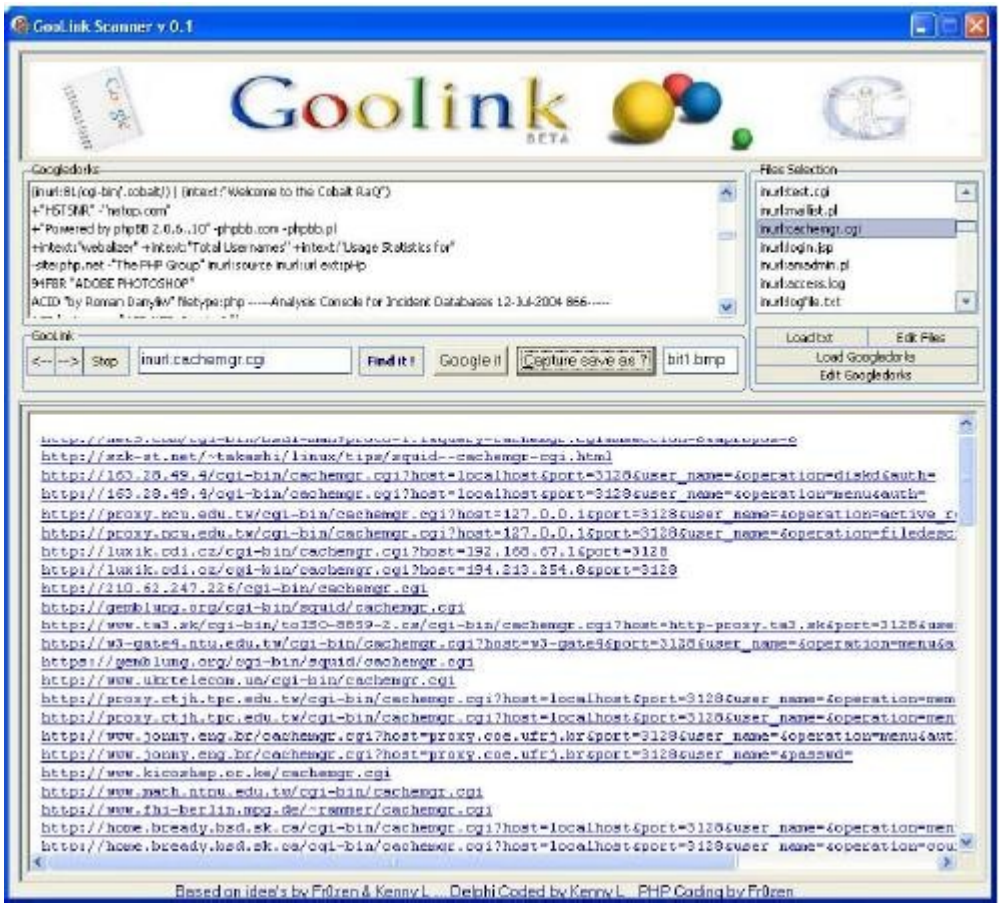
SiteDigger için aşağıdaki adresi ziyaret edebilirsiniz;

http://www.foundstone.com/us/resources/proddesc/sitedigger.htm



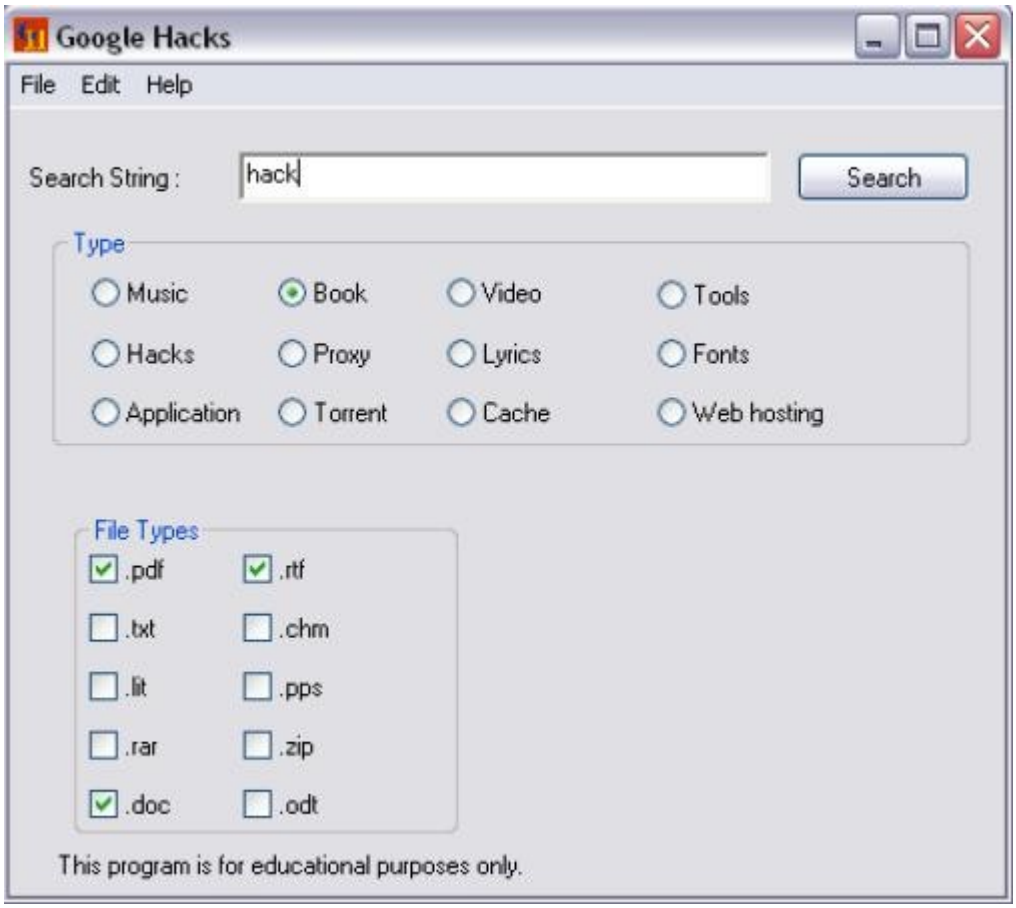
Goolink Scanner

SiteDigger Tool ile benzer görevi yapan pratik bir araç.



Google Hacks
(code.google.com/p/googlehacks/)

Belirttiğiniz dosya ve dosya uzantılarına göre google önbelleğinde arama yapar.Müzik , kitap, video, araç vs. aramak için ideal bir araç.



Referanslar

www.google.com
www.cehturkiye.com
johnny.ihackstuff.com
www.milw0rm.com

Güvenlik Araçları

- Savunmadan çok “saldırı”ya yönelik araçlar.
- Amaç, saldırganlardan önce sistemdeki açıkları ortaya çıkarıp gereken önlemleri almak.

Nmap

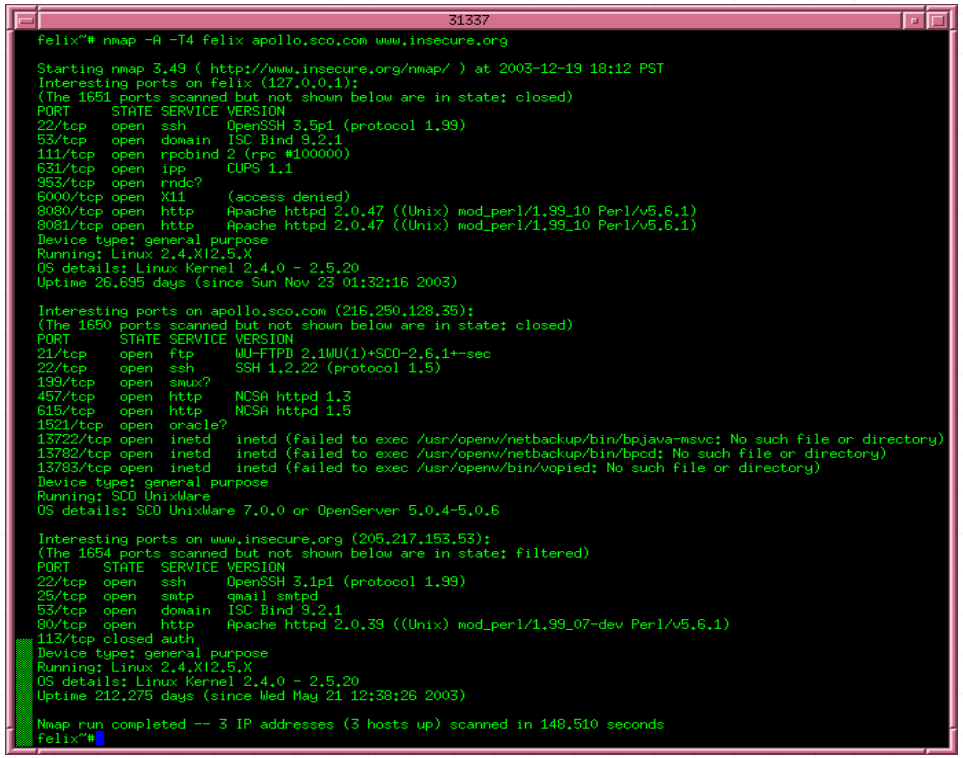
- “Network Mapper”
- Ağ araştırması ve güvenlik denetlemesi yapan açık kaynaklı ücretsiz bir yazılım.
- Geniş ölçekli ağları taramak için tasarlanmıştır.
- Alışılmışın dışında IP paketleri göndererek tarama yapar.

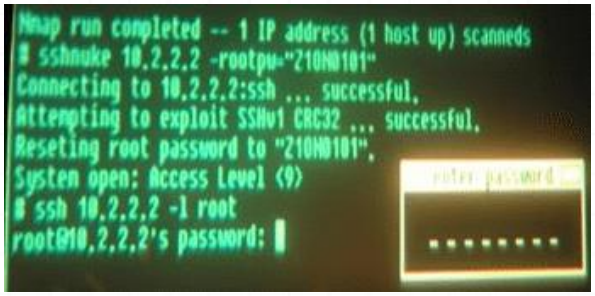
Nmap

- Ağdaki canlı bilgisayarlar
- Çalışan servisler (Uygulama adı ve versiyonu)
- Koşulan işletim sistemi
- Varsa kullanılan güvenlik duvarı

Nmap Görselleri

- www.insecure.org/nmap





Nessus

- Güçlü, güncel ve ücretsiz bir uzaktan güvenlik taraması aracı.

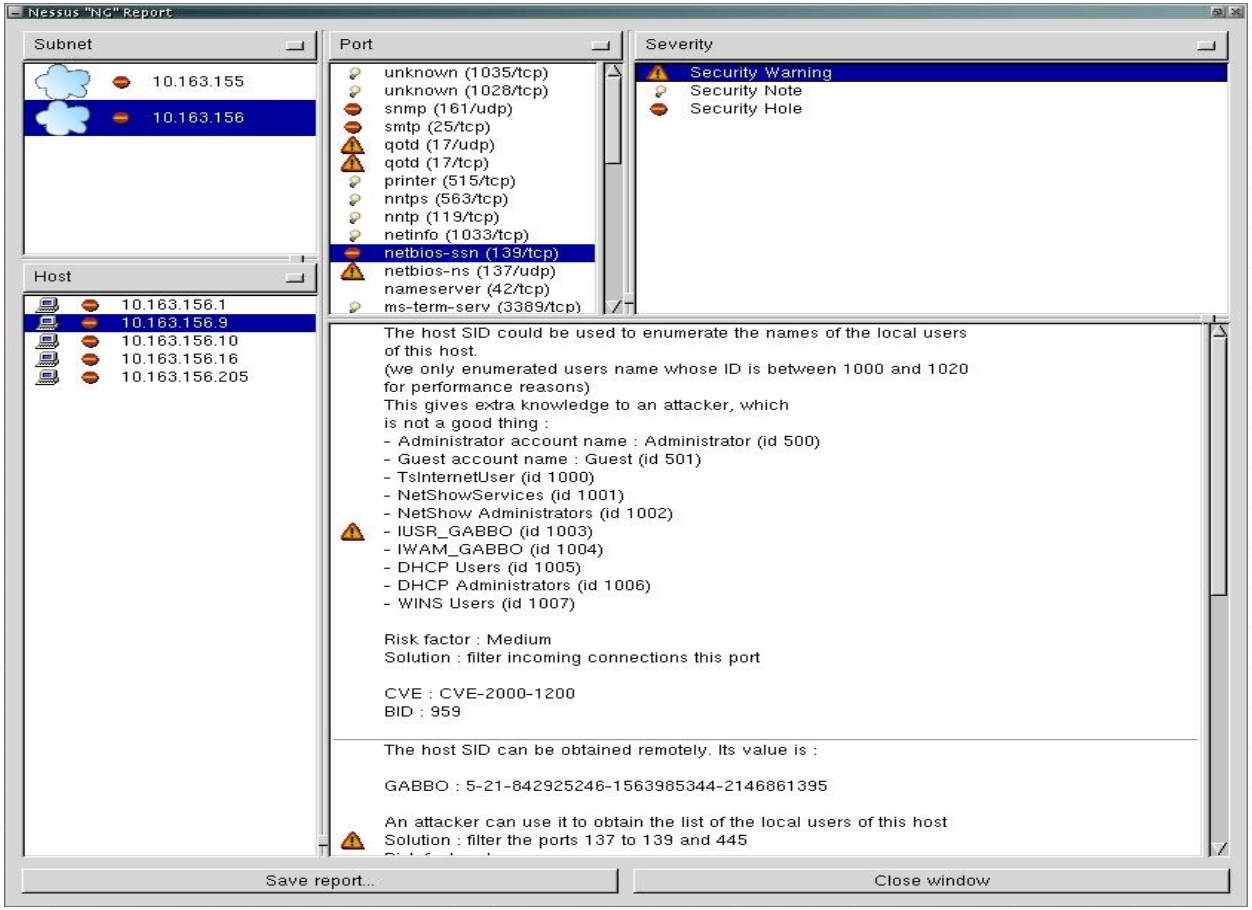
- Diğerlerinden en büyük farkı bilinen kurallara bağlı olmaması. (Örnek: web sunucusu 1234 numaralı portta çalışsa bile nessus onu bulup güvenlik taraması yapabiliyor.)

Nessus

- Platform: Unix ve benzeri sistemler + Windows
- Çok çeşitli raporlama yetisi (HTML, XML, LaTeX, and ASCII)
- Uyumlu ek (plug- in) yazılımları ve GTK arayüzü ile kullanışlı

- www.nessus.org

Nessus Görseli



Ethereal

- Unix ve windows üzerinde çalışabilen bir protokol analizi aracı.
- Canlı bir ağ üzerindeki verileri incelemek veya disk üzerine kaydetme amacıyla kullanılır.
- Her paket için ayrıntılı bilgi gösterebilen interaktif bir arayüzü vardır.

Ethereal

- Metin tabanlı versiyonu tethereal.
- Ücretsiz.

www.ethereal.com

Snort

- Gerçek zamanlı trafik analizi ve paket kayıtlaması yapabilen ücretsiz bir ağ saldırı belirleme sistemi.
- Protokol analizi, içerik araştırması ve eşlemesi yapabilir.
- Tampon taşırma, gizli port taramaları, CGI saldırıları, SMB yoklamaları, işletim sistemi belirleme saldırıları gibi birçok saldırı veya yoklamayı belirleyebilir.

Snort

- Esnek bir kural yazma dili
- Modüler uyumlu ek yazılım mimarisi.
- Gerçek zamanlı alarm mekanizması.
  (syslog, windows eventlog, winpopup, vb.)
- Arayüz yazılımı ACID.

www.snort.org

tcpdump

- Ağ inceleme ve veri yakalama amaçlı klasik bir sniffer.
- Metin tabanlı
- Ağ hareketlerini incelemede kullanılır.
- Verilen deyimleri eşleyerek belirli bir ağ arayüzündeki paket başlıklarını gösterebilir.
- Nmap tcpdump altyapısını kullanır.
- www.tcpdump.org

DSniff

- Güçlü bir ağ denetleme ve giriş testi (penetration test) amcına yönelik araçlar takımı.
- dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf ve webspy araçları ağ üzerinde pasif bir şekilde kayda değer veri araştırmasında kullanılı. (şifre, e-posta, vb.)

DSniff

- arpspoof, dnsspoof ve macof normalde saldırganın ulaşamayacağı (2. katman) ağ bilgilerine ulaşmasını kolaylaştırır.
- sshmitm ve webmitm ssh ve https oturumalrında monkey-in-the-middle saldırılarında kullanılır.

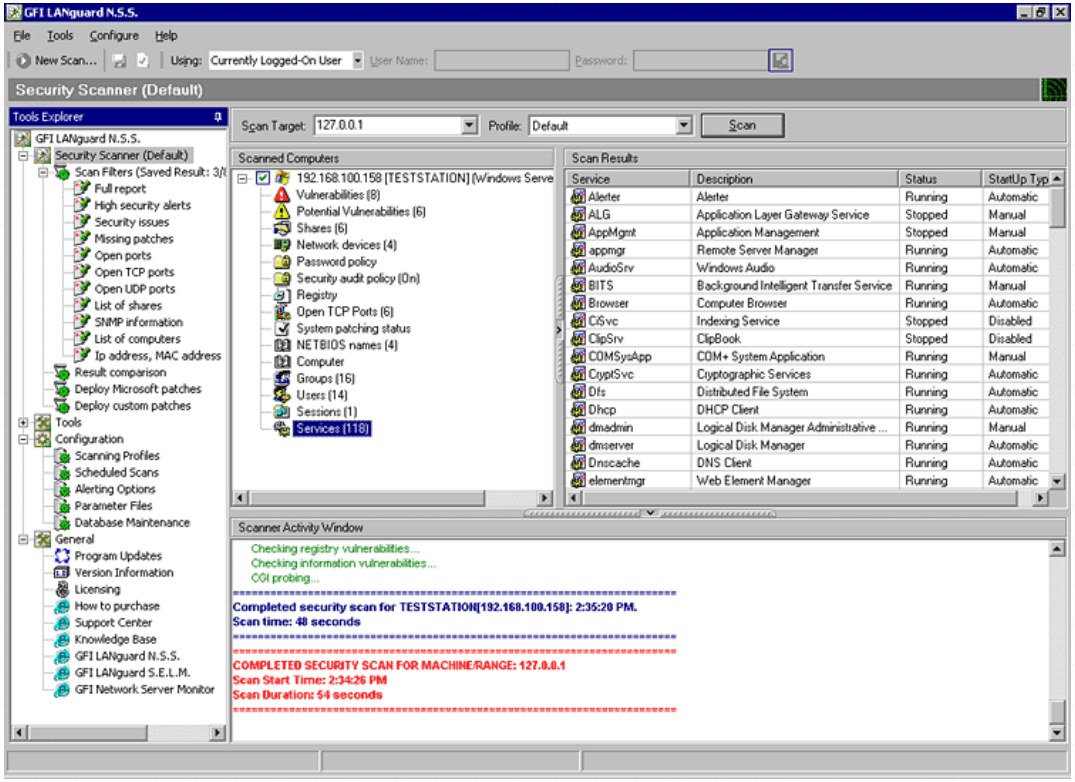
http://naughty.monkey.org/~dugsong/dsniff/

GFI LANguard

- Sistemdeki güvenlik hasar risk analizini otomatik olarak yapan bir araç.
- Windows üzerinde çalışır.
- Ağ taraması yapar.
- Her makinenin servis paket durumunu, yamanmamış güvenlik açıklarını, açık paylaşım alanlarını ve portlarını, çalışan uygulamalarını, vb. birçok bilgiyi raporlar.

GFI LANguard

- Ücretli bir yazılımdır. (Windows tabanlı!)
- Deneme sürümü mevcut.
- www.gfi.com



Ettercap

- Anahtarlamalı yerel ağlar için kullanılan bir sniffer, araya girme ve kayıt yapma aracıdır.
- Şifreli olanlar da dahil birçok protokol için aktif ve pasif inceleme özelliği vardır.
- Kurulmuş bağlantılara veri enjeksiyonu yapma ve filtreleme özellikleri vardır.
- Ağ geometrisini çıkarma ve işletim sistemi tespitleri yapabilir.

John the Ripper

- Çok hızlı bir şifre kırıcısı.
- Unix (11'i resmi olarak desteklenen birçok farklı mimarisinde), DOS, Win32, BeOS ve OpenVMS üzerinde çalışabilir.
- Geliştirilme amacı zayıf unix şifrelerini tespit etmek.
- Unix crypt(3) şifre özü, Kerberos AFS ve Windows NT/2000/XP LM özlerini kırabilir.
- Aynı zamanda sürekli güncellenen şifre veritabanı vardır.

ISS Internet Scanner

- Uygulama düzeyinde ağa bağlı araçlar üzerinde hasar risk analizi yapabilen ücretli bir yazılım.
- Ağdaki güvenlik açıklarını yakalamada çok iyi fakat çok pahalı bir yazılım. (ucuz + iyi = nessus)

www.iss.net

tripwire

- Bütünlük analizi yapan araçların büyükbabası.
- Dosya ve dizinlerin bütünlüklerinin bozulup bolulmadığını inceler.
- Herhangi bir değişim sonrası sistem yöneticilerini uyarır.
- Açık kaynak kodlu versiyonu Linux için www.tripwire.org da mevcut.
- Diğer sistemler için ücretli.

- www.insecure.org

BİYOMETRİK GÜVENLİK SİSTEMLERİ

- Biyometrik tanıma, datayı kodlama veya şifreleme /deşifreleme için vücut özelliklerini kullanan bir süreçtir. Parmak izi, retina ve iris, avuç içi izi,yüz yapısı ve ses tanıma günümüzde sıkça araştırılan biyometrik tanıma teknikleridir. Bu özellikler her şahsa özel olduğu için biyometrik yöntemler hırsızlık ve dolandırıcılığa kısmen de internet üzerinde ticarete cevap olabilecektir.Bu yeni teknolojinin özelliği parola veya PIN numarası yerine çalınamayan kaybolmayan veya yeniden oluşturulamayan biyometrik özelliğin kullanılmasıdır. Bir endüstri uzmanına göre, Kullanıcının erişim haklarına sahip olabilmek için onun parmağını kesmedikçe, biyometrik tanıma erişim kontrolü için mükemmel bir yöntemdir.

BİYOMETRİK GÜVENLİK SİSTEMLERİ

- Tablo 8.1 ‘de ifade edildiği üzere biyometrik yöntemleri kullanmak için oldukça fazla seçenek bulunmaktadır.Tablo 8.1 ‘de verilmiş olan biyometrik yöntemler bugüne kadar kararlılığı test ve kabul edilmiş olan yöntemlerdir.Bunlar için daha doğru bir ifade kullanılması gerekirse bu yöntemler bilinen biyometrik yöntemlerdir.Bu yöntemlerin ötesinde halihazırda araştırma aşamasında olan bir çok biyometrik yöntemde bulunmaktadır.Bunlar arasında en dikkat çekici olanlarından birisi insanların kulak yapılarını algılayıp tanıyan sistemlerdir.Bu da göstermektedir ki insanların kendilerine has olan bütün uzuvları biyometrik tanımlayıcı olarak kullanılabilir. Bu da biyometrik sistemlerin ana amacını oluşturmaktadır.

BİYOMETRİK GÜVENLİK SİSTEMLERİ

Biyometrik Yöntem	Hata Oranı
Retina Tarama(ışığı ileten damarlar)	1:10.000.000
İris Tarama(göz rengini veren bölge)	1:131.000
Parmak İzi Tarama	1:500
El Geometrisi Tarama	1:500
İmza(Yazı Yazma) Tarama	1:50
Ses Tarama	1:50
Yüz Tarama	Veri Yok
Vascular Patterns	Veri Yok

Tablo 8.1. Biyometrik Yöntemlerin hata oranları

Biyometriğin Tarihçesi

- Bugünün biyometrik tanıma süreçleri geçmişteki bazı yaygın biyometrik tekniklerinden türetilmiştir. Doğal olarak en yaygın olan ve suçluların tespitinde, çalışanların lisanslarında kullanılan parmak izidir. Bu süreç, yazılı kopya üzerinden manuel olarak haftalarca süren bir inceleme sonucunda bazen de yanlış sonuçlar vererek gerçeklenirdi. Bilgisayar teknolojisinin gelişmesiyle, bazı kuruluşlar, arşivlerini elektronik olarak tutmaya ve parmak izi eşleştirme sürecini daha hızlı ve doğru olarak yapmaya başladılar. Parmak izi tanıma sürecinin sonraki adımı sadece kişileri tanımak değil aynı zamanda belirli yerlere erişimlerini denetlemektir. Bu teknik ile birlikte biyometrik tanıma koddaki bilginin çözümlenmesiyle, kişilerin belirli yerlere girişlerini sağlayacak biyometrik parola olarak kullanılmaya başlamıştır.

Biyometrik Tanıma Nasıl Çalışır?

- Tanıma, iletilen veya bir veritabanında saklanan bilginin anlaşılmasına yardım eden bir matematiksel süreçtir, ve bir kripto sistemini belirleyen üç ana faktör vardır, matematiksel süreç veya algoritmanın karmaşıklığı, mesajı anlamakta kullanılan tanıma özelliğinin uzunluğu, anahtar yönetimi olarak bilinen anahtarın emniyetli saklanması. 68 Dr.İ.SOĞUKPINAR G.Y.T.E. Bil.Müh.Böl. Algoritmanın karmaşıklığı, ters işlem ile doğrudan bağıntısı olması nedeniyle önemlidir. Bazıları tanımanın bu alanının kolayca kırılabileceğini düşünür, bununla birlikte kripto sistemleri saldırılara karşı zafiyet olan en az bu üç faktörü içerecek şekilde iyi tasarlanır.

Biyometrik Tanıma Nasıl Çalışır?

- Mesajı anlamakta kullanılan tanıma anahtarının uzunluğu, tanıma sürecinin ikinci en önemli parçasıdır. Daha kısa olan anahtarlar brute force saldırılarına karşı daha zayıftır. Bunun anlamı bir kişinin hesaba girebilmek için bütün mümkün parola kombinasyonlarını denemesi demektir.
- Parola veya PIN numarası gibi biyometrik olmayan tanıma süreçlerinde, anahtarın uzunluğuna bağlı olarak enformasyon yetkisiz kişilerce erişilmeye karşı güvensizdir.Örneğin üç karakterlik bir şifre, mümkün olan permutasyonlar bakımından on karakter uzunluğundaki bir şifreye göre daha zayıftır. Mevcut bilgisayar gücü ile, 64 karakter uzunluğundaki bir anahtarın bulunabilmesi için gerekli permutasyonlarının hesabı dört yüz yıl alabilecektir Biyometrik tanıma, personel tanımlayıcısı ile normal anahtar karakterlerinin yerlerini değiştiren bir standart karakter uyuşturma yapar. Bu biyometrik anahtar olmadan veriye erişilemez.

Biyometrik Tanıma Nasıl Çalışır?

- Anahtarların emniyetli olarak saklanması tanıma sürecinin en zayıf yönüdür. En kolay olarak gözüken saklama süreci en zor işlemdir çünkü parola veya PIN numarası kaybolabilir veya çalınabilir. İyi tanıma özelliği çok uzun olan ve hatırlanamayan parolaların, kağıtta akıllı kartlarda, veya disketlerde saklanarak yetkisiz kişilerin erişiminin önlenmesidir. Biyometrik tanıma sistemleri anahtarın kaybetme veya çalınma olmadan taşınmasını mümkün kılar.

Örüntü Tanıma Teknikleri

- Örüntü Tanıma, gereksiz detaylardan arındırılmış olan giriş datasından çıkartılan anlamlı özellikler yardımıyla teşhis sınıflarına ayrılan verinin sınıflandırılmasıdır.
- Görüntü, geçici mantıksal gibi değişik örüntü sınıfları mevcuttur. Geniş bir yorumlama ile örüntü tanımayı birçok akıllı faaliyette kullanabiliriz. Tek bir teorisi olmayan örüntü tanıma geniş çaptaki problemin çözümünde kullanılabilir. Bununla birlikte birkaç standart model aşağıda özetlenmiştir.

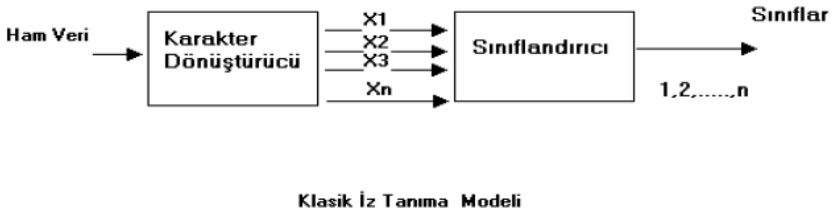
Örüntü Tanıma Teknikleri

- İstatistiksel veya bulanık örüntü tanıma
- Sentetik veya yapısal örüntü tanıma
- Bilgi tabanlı örüntü tanıma(Yapay sinir ağları, Uzman sistemler)
- Burada istatistiksel yaklaşım ile kendimizi sınırlandıracağız. Örüntü tanımayı, bir girişi bir sınıfa atayan sınıflandırma olarak göreceğiz.. Problemi böyle sınırlamakla ihtiyaçlarımızı gören bazı yararlı teknikleri geliştirecek ve aşağıdaki temel kavramlar üzerinde yoğunlaşacağız:
- Sınıflandırma
- Özellikler
- Özellik vektörleri
- Standart sınıflandırma modelleri

Sınıflandırma Modeli

- Görsel örüntü ile çalıştığımızı ve Roman alfabesinin 26 harfini temsil eden örüntüyü bildiğimizi kabul edelim. Buradan örüntü tanıma problemini, giriş verisini 26 sınıftan birisine atama olarak ifade edebiliriz.(Şekil 8-1) Genelde girişin sınıf 1 veya Sınıf 2 veya .. veya …Sınıf c 'ye ait olduğu şeklinde kendimizi sınırlayacağız..

Şekil 8-1. Harflerden oluşan Görsel örüntü



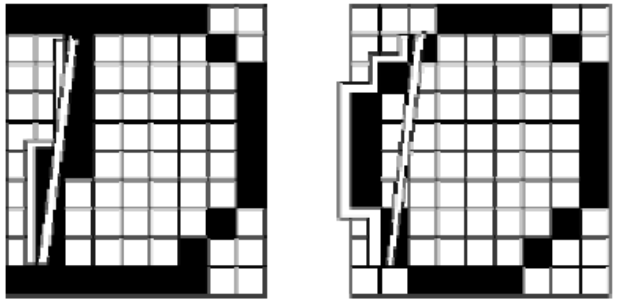
Şekil 8-2. Örüntü(iz) tanıma modeli

Sınıflandırma Modeli

- Daha ileriye giderek, görsel girişi sayısal hale getirmek için bir kamera kullandığımızı ve bir karakteri parlaklık değerlerinin dizisi olarak ayrıştırdığımızı kabul edelim. Bilgisayar bu veriyi 70 Dr.İ.SOĞUKPINAR G.Y.T.E. Bil.Müh.Böl. nasıl sınıflandıracaktır. Belli bir yaklaşım, girişi, her bir sınıf için standart bir örüntü ile karşılaştırmak ve en iyi uyuşan sınıfı seçmektir. Bu yaklaşımdaki açık problem neyin karşılaştırılacağı ve uyuşmanın mertebesini ölçmenin söylenmeyeceğidir.(Şekil 8-2.) Aynı sınıfa ait olan girişlerin, farklı sınıflardaki örüntüler arasındaki farklılığa göre değişkenliği örüntü tanıma problemlerini böyle karmaşıklaştırır. Bu problemin üstesinden gelmenin bir yolu karakteristik özelliklerin araştırılmasıdır.

Özellikler

- Bir nesne veya bir olayı sınıflandırmanın tek yolu onun karakteristik özelliklerinin veya belirleyici niteliklerinin ölçülmesidir. Örneğin yazılı bir harfi sınıflandırmak için onun alan ve çevresini bilmek faydalı olacaktır. Onun alanının çevresinin karesine oranı ile onun sıkılığını ölçebilirdik.Onun yatay eksene göre üst ve altta kalan kısımlarının alanlarını karşılaştırarak simetrikliğini ölçebiliriz.(En iyi ölçmenin simetriklik olduğu düşünülebilir.)
- Bazı özellikler önemli küçük farklara duyarlı olabilir. Örneğin Şekil 8-3'te gösterilen "D" harfini "O"'dan ayırt etmek için sol tarafın düzlüğü ölçülebilir, belki de düz çizgi farkının yay uzunluğuna oranı ölçülebilir Açıkçası, çözülmesi gereken önemli bir özellik olan belirleyici niteliklerin tasarımı bir bilimden çok sanattır.



Şekil 8-3: D ve O harflerine ait görsel veri

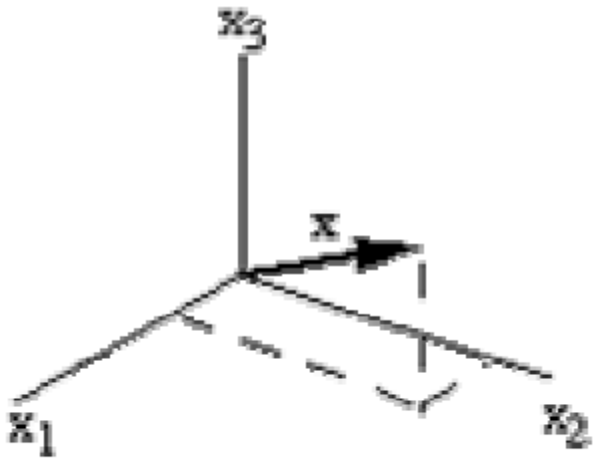
Belirleyici Özellik Vektörleri

- Herhangi bir nesne veya olayı sınıflandırmak için sıkça belirleyici özelliklerin sabit bir kümesi elde edilir. Örneğin her zaman,.
- x1 = alan
- x2 = çevre
- ...
- xd = yay uzunluğu / Düz çizdi uzaklığı her zaman ölçülebilir.
- Bu durumda, belirleyici özellik kümesini, x belirleyici özellik vektörü olarak düşünebiliriz, burada
- x, d boyutlu bir sütun vektörüdür. Şekil 8-4 de gösterilmiştir.

Belirleyici Özellik Vektörleri

- Benzer olarak, x'i d boyutlu belirleyici özellik uzayında bir nokta olarak düşünebiliriz.

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_d \end{bmatrix}$$



Şekil 8-4: Özellik vektörü

Standart Sınıflandırma Modelleri (*Klasik Model)*

- Aşağıdaki klasik model örüntü tanıma için önde gelir.

- Belirleyici özellik çıkartıcı olarak adlandırılan bir sistem veya program, bir özellik vektörü olan x'in elemanlarına karşılık gelen belirleyici özellikleri x1, x2, ..., xd olan d sayısal kümesini belirlemek için ham veriyi işler. Sınıflandırıcı denilen bir sistem veya program, x'i alır ve Sınıf 1 sınıf 2 , , sınıf c 'den birine atar.

Standart Sınıflandırma Modelleri (*Klasik Model)*

- Belirleyici özellik çıkartıcının tasarımı çoğunlukla probleme bağlıdır. İdeal belirleyici özellik çıkartıcı aynı sınıftaki bütün örüntüler için aynı x özellik vektörünü, farklı sınıftaki örüntüler için ise farklı özellik vektörünü üretmelidir. Pratikte, farklı girişler, belirleyici özellik çıkartıcı tarafından farklı özellik vektörü üretilmesin sağlar, fakat sınıf içindeki değişkenliğin sınıf arasındakine göre küçük olmasını bekleriz.

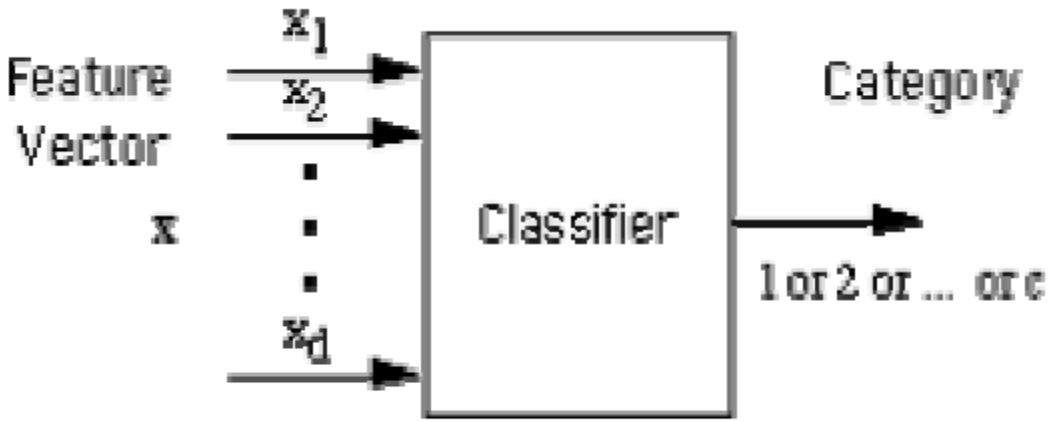
Standart Sınıflandırma Modelleri (*Klasik Model)*

- Bu noktada, belirleyici özellik çıkartıcının tasarımcısının yapabileceğinin en iyisi ile işini tamamladığını kabul ederiz, ve özellik vektörü örüntüleri ayırt etmek için gerekli olan bilgiyi içerir. Verilen belirleyici özellik kümesinden sınıflandırıcıyı tasarlamak bizim işimizdir.

Basit Sınıflandırıcılar

Bir sınıflandırıcı tasarlama yaklaşımı için en az iki yol vardır:

- Makul bir çözümün varsayımı ve onu probleme uydurulması
- Problemin matematik modelinin çıkartılması ve en iyi sınıflandırıcının üretimi



Şekil 8-5: Basit sınıflandırıcı

Basit Sınıflandırıcılar

Daha çok sezgisel olan ilk yöntem pratikte daha çok kullanılır, ve bizim ele alacağımız yaklaşımdır. Basit bir çözüm ile başlayacağız, karakteristiklerinin analizi, zayıf yönlerin belirlenmesi, ve sadece gerektiği şekilde karmaşıklaştırma.. Bu bölümde aşağıdaki kavramlar üzerinde duracağız:

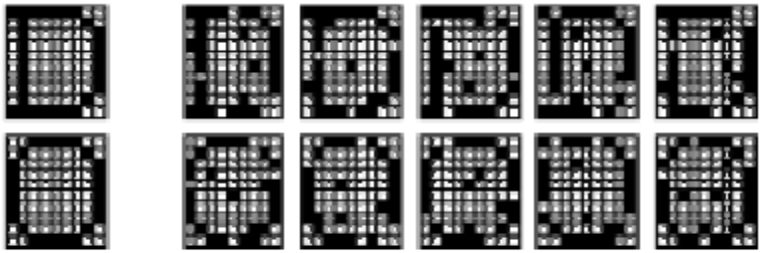
- Şablon Uyuşturma(Template matching)
- En az mesafe sınıflandırıcılar(Minimum-distance classifiers)
- Metrikler(Metrics)
- İç Çarpımlar(Inner products)
- Doğrusal farklılıkların anlaşılması(Linear discriminants)
- Karar sınırları(Decision boundaries)

Şablon Uyuşturma (Template Matching)

- Şablon uyuşturma örüntü sınıflandırma için doğal bir yaklaşımdır. Örneğin Şekil 8-6'da gösterilen gürültülü "D" ve "O" yu düşünelim. Gürültüsüz versiyon şablon olarak sol tarafta gösterilmiştir. Gürültülü örneklerin birisini sınıflandırmak için, onu iki şablon ile karşılaştırmak gerekir. Bu işlem aşağıdaki yöntemlerden birisi ile yapılabilir:
- Uyuşmaların miktarını say(uyuşan siyahlar siyah, uyuşan beyazlar ise beyaz).
- En fazla sayıda uyuşan sınıfları ayıkla. Bu en fazla karşılıklı ilişki yaklaşımıdır.
- Uyuşmayanların miktarını say (Siyah yerde beyaz, beyaz yerde siyah olmalı). En az sayıda uyuşmayanların olduğu sınıfları ayıkla. Bu en az hata yaklaşımıdır.

Şablon Uyuşturma (Template Matching)

- Şablon uyuşturma , eğer farklılıklar sınıf içinde kalırsa iyi çalışır. Açıkça, bu örnekte karakterlerde öteleme, dönme, kırpma, çarpıklık, genişleme veya, büzülme gibi başka bozukluk olmadığı için yöntem çalışır. Yöntem bütün problemlerde çalışmayacaktır fakat uygun olduğu zaman çok verimlidir. Aynı zamanda kullanışlı şekilde genelleştirilebilir.



Şekil 8-6: Şablon Uyuşturma

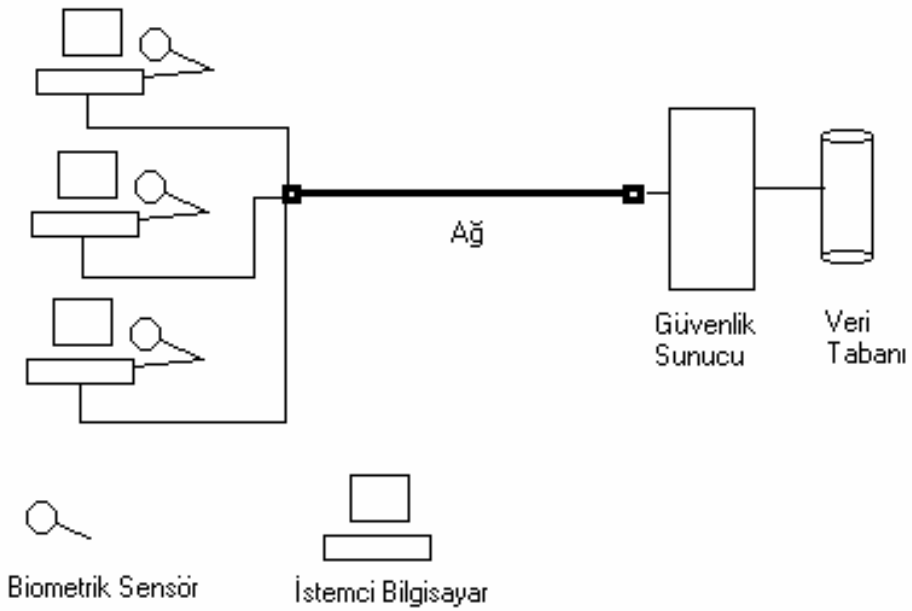
Biyometrik Sistemlerin Kuramsal Tasarım Yöntemleri

- Şimdiye kadar ki bölümlerde biyometrik yöntemlerin genel çalışma prensiplerinden öte bu tür sistemlerin çalışabilmeleri için nasıl bir fazladan donanıma ihtiyaç duyduklarını anlatıldı.Örneğin bir parmakizi tanıma sisteminde her istemci için bir CCD kamera içeren sensöre ihtiyaç vardı. Bahsedilen sensörlerin içeriklerinin farklı olmasına rağmen yaptıkları iş aynıdır. Bütün biyometrik sistemlerin kurulumu için istemci başına bir sensör gerekmektedir.Daha sonra buradan okutulan bilgiler tasarlanan sistemin mimarisine bağlı olarak işletilirler. Şekil 8-22'de bir biyometrik sisteme ait kuramsal çizim yer almaktadır.

Biyometrik Sistemlerin Kuramsal Tasarım Yöntemleri

Biyometrik sistemlerin tasarımı için uygulanan iki model vardır.

- On-line Model
- Off-line Model



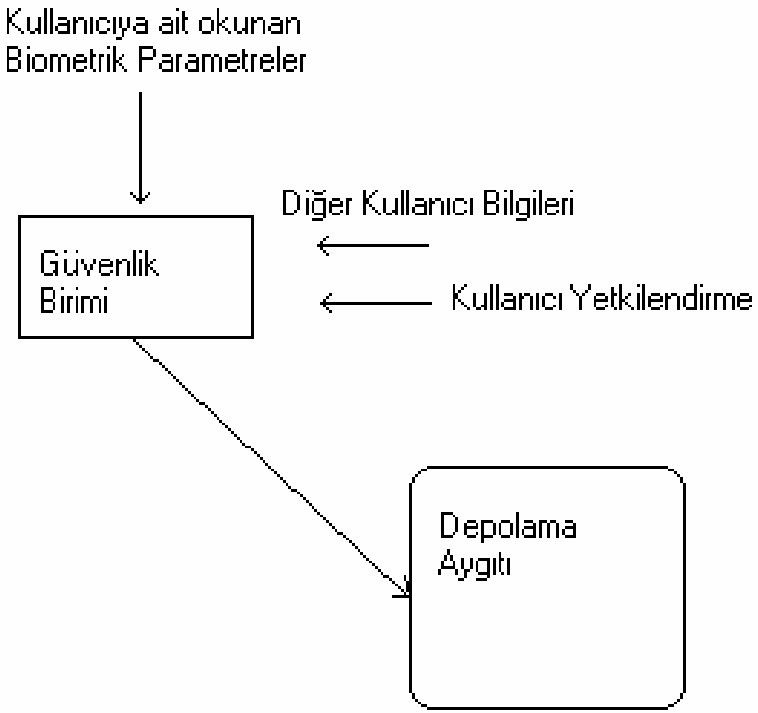
On-line Model

- On-line model yapısında, kullanıcı okunması gereken biyometrik parametresini sisteme okutturur. Sistem almış olduğu biyometrik parametreleri eğer gerekliyse şifreleyerek ağ üzerinden güvenlik parametrelerinin tutulduğu sunucuya gönderir. Sunucu bu parametreleri veritabanı içerisindeki bilgilerle karşılaştırır. Eğer kullanıcı sisteme kayıtlı biriyse sisteme giriş izni gönderir. Kullanıcı tanımlanamadıysa sistem giriş izni vermez. Günümüzde on-line sistemler kullanılmaktadır.

On-line Model

- On-line bir sistemde önemli olan nokta biyometrik bilgileri okuyan sensörlerin sunucuya çok güvenli bir şekilde bağlanmaları gerekmektedir. Bunun için ya sensörler ve sunucu arasında güvenli bir yol tayin edilmelidir yada bilgiler yukarıda bahsedildiği üzere çok iyi şifrelenmiş olarak gönderilmelidir.Bilgilerin herhangi bir nedenden dolayı yetkisiz insanların eline geçmesi sistemin büyük bir zaafa uğramasına sebep olabilir. Öyleyse parametreler öyle bir şekilde şifrelenmeli ki bu parametreler bir şekilde elde edilse bile kullanılamamalılar

On-line Model

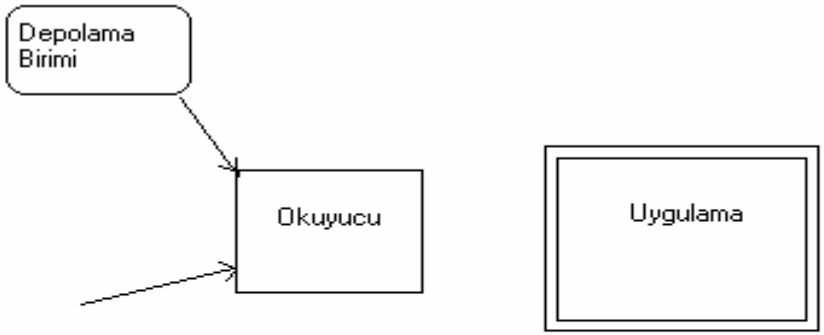


Off-line Model

- Off-line sistemlerde ,On-line sistemlerde olduğu gibi gerçek zaman bir doğrulama işlemi yapılmaz. Bunun için gerekli olan bir manyetik kart gibi aparatlar kullanmaktır. Kullanıcıya ait olan bilgiler bu kart üzerinde tutulurlar. Kullanıcı sisteme girmek istediği zaman bu kartı kullanır. Bu tür sistemlerde güvenlik tamamen kullanıcının inisiyatifindedir. Kendisine verilmiş olan depolama aygıtını çok iyi korumak zorundadır. Tersi bir durumda sistemin güvenilirliğinden söz etmek gerçekçi olmayacaktır.

Off-line Model

- Bu sebeplerden dolayı off-line bir sistem tasarlanırken güvenlik açısından üzerinde çok daha fazla düşünülmesi gereklidir.



Biyometrik Tanıma Teknikleri

Bu gün birçok biyometrik tanıma uygulaması vardır. Aşağıda bunların türleri verilmiştir.

- Parmak izi tanıma
- Optik Tanıma
- Yüz Yapısı Tanıma
- Ses Tanıma
- İmza Tanıma
- Yazma Ritmi Tanıma
- Toplardamar İzi Tanıma
- Avuç içi izi
- Kulak Şeklinden tanıma

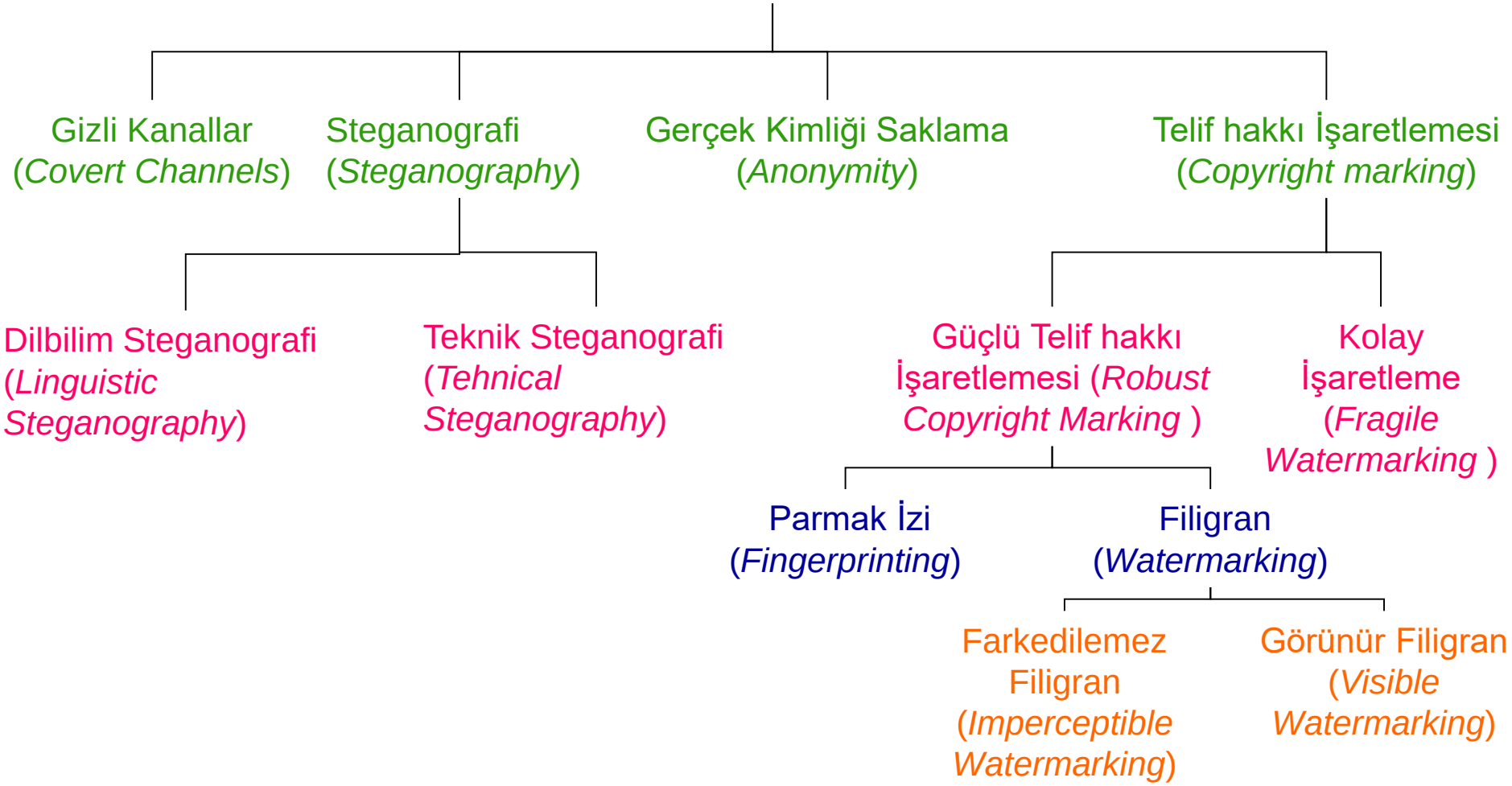
Konu Başlıkları

- Metin Steganografi
- Resim Steganografi
- Ses Steganografi

Bilgi Gizleme

- Bilgi gizleme bir mesajın yada bilginin, herhangi bir masum görünüşlü ortam içine saklanarak bir diğer kişiye iletilmesidir.
- Bilgi gizleme bilgisayar ortamındaki encapsulation işlemine benzer bir durumdur.
  - Encapsulation (Kapsülleme)
    - Bir modülün yaptığı işlemlerin bir kısmını, bu işlemleri nasıl gerçekleştirdiği bilgisini dışarıdan bilinçli olarak saklamaktır.
    - Encapsulation'ın asıl amacı içeriği saklamak değil kontrolsüz ve gereksiz erişimi engellemek, dış öğeleri, içeriğe standart, önceden tanımlı arayüzler aracılığıyla ulaşıma zorlamaktır.

Bilgi Gizleme



Gizli Kanallar (Covert Channels)

İki kişi arasında gizli bilgilerin eldeğiştirmesi için iletişimi sağlayan kanaldır. Gizli kanal kurulması iki kişinin karşılıklı anlaşmasını gerektirmektedir.

Gizli Kanalların amaçları:

- İletişimimizdeki veriyi saklamaya çalışmak
- İletişiminin amacını saklamak

Gizli Kanallar (Covert Channels)

Böylece;

- Gerçek veri transferi, dikkatsiz gözlere zararsız ve kanuna uygunmuş gibi gözükecektir.
- Veriyi karıştırmak için ayrı bir şifreleme yapılmasına gerek kalmayacaktır.

Gizli Kanallar (Covert Channels)

- Gizli Kanallar çeşitli alanlarda kullanılmaktadır. Bunlar;
  - Dosya tabanlı steganografi
    - Görüntü, ses ve text dosyaları
  - Ağ paket steganografisi
    - Veriler IP paketleri içine gizlenmektedir.
  - Protokol Kapsüllenmesi
    - SSL (Secure Sockets Layer) üstünde TCP paketleri içerisine
    - SSH (Secure Shell) üstünde TCP paketleri içerisine

Gerçek Kimliği Saklama (Anonymity)

- Veri gönderimi sırasında gerçek kimliği saklayarak bilginin bilinmeyen yada anlaşılamayan biri üzerinden gidiyor olduğunu izlenimi verilerek te bilgi zarar görmeden gönderilebilmektedir.
- Fakat ağlar üzerinde bilinmeyen kullanıcı olayı ağ yöneticilerinin daha fazla dikkatini çekmekte ve bilgi güvenliği tehlikeye girmektedir.
- Bu yüzden sadece çok gerektiği durumlarda kullanılması uygundur.

Steganografi (Steganography)

- Bu yaklaşım, bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir.
- Ses, sayısal resim, video görüntüleri üzerine veri saklanabilir.
- Bu veriler metin dosyası olabileceği gibi, herhangi bir görüntü içerisine başka bir görüntüyü gizlemekte olasıdır.

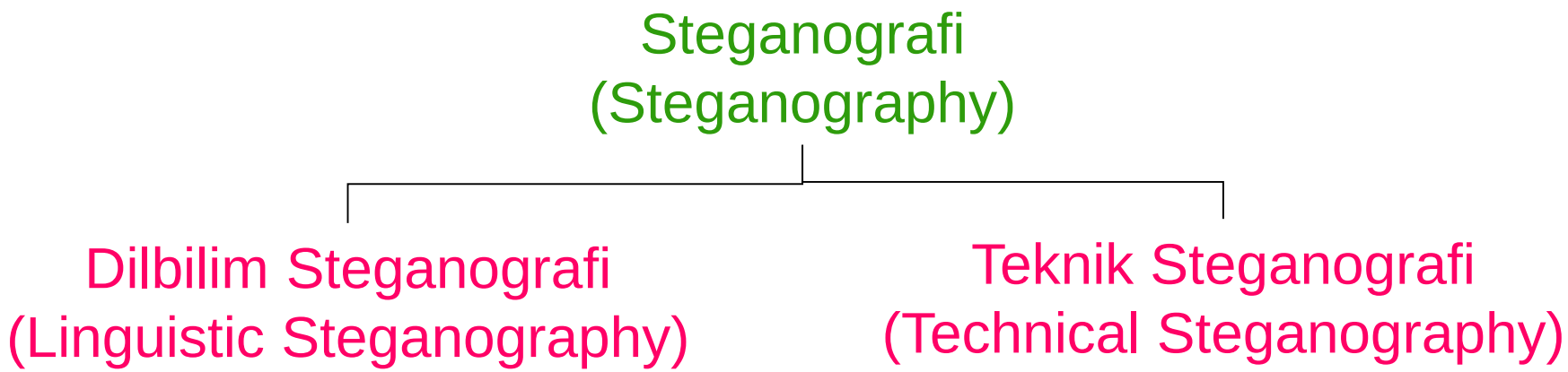
Steganografi

- Bu yaklaşımda içine bilgi gizlenen ortam cover-data (örtü verisi), ve oluşan ortama da stego-text veya stego-object denilmektedir.

- Bir stego-key (stego-anahtarı), bilginin saklaması işlemini kontrol etmek için ve gömülü bilginin elde edilmesini zorlaştırmak için kullanılmaktadır.

Steganografi

Steganografi kendi içinde iki kısma ayrılmaktadır.



Dilbilim Steganografi (Linguistic Steganography)

- Dilbilim steganografi, taşıyıcı verinin text olduğu steganografi koludur.
- Burada veriyi gizlemek için text üzerinde değişiklikler yapılmaktadır.
- Bu değişiklikler şu şekilde yapılabilir.değişiklik yapmanın çeşitli yolları vardır.
- Bunlardan bazıları;
  - grafik kullanılarak yapılabilir
  - text'in yapısı değiştirilerek yapılabilir
  - yada amacı sadece veriyi saklamak olan yeni bir text yaratılabilir

Linguistic Steganography

Dilbilim Steganografi'de kullanılan yöntemler şunlardır:

- Açık kodlar
  - Gizli mesaj, açıkça okunabilir fakat zararsız bir mesaj haline gelir.
  - Bu işlem; maskeleme, boş şifreler ve ızgaralama ile yapılmaktadır.
- Şemagramlar
  - Gizli mesaj, açık metinin ufak fakat gizli bir detayının içine gizlenmektedir.
  - Bunun için grafiksel değişiklikler yapılmaktadır.
  - Kullanılan yöntemler; farklı yazı tipleri kullanmak, eski daktilo yazılarını kullanmak, resimler içinde boşluklar kullanmak vb.

Teknik Steganografi (Technical Steganography)

Teknik Steganografi bir çok konuyu içine almaktadır.

- Bunları bazı başlıklar altında toplayabiliriz;
  - Görünmez mürekkep: Geleneksel haline gelmiş olan görünmez mürekkeple yazma yöntemidir.
  - Gizli yerler: Kimsenin göremeyeceği gizli yerlere saklama (bavul, kasa vb.)
  - Microdot'lar: Bilgiyi noktalar halinde sayfaya gizleme
  - Bilgisayar tabanlı yöntemler: Text, ses, görüntü, resim dosyalarını kullanarak veri gizleme yöntemleridir.

Steganografinin Kullanım Alanları

- Metin Steganografi (Text Steganography)
- Görüntü Steganografi (Image Steganography)
- Ses Steganografi (Audio Steganography)

Metin Steganografi

- Metin Steganografi taşıyıcı ortamın text olduğu Steganografi alanıdır.
- Metin steganografi genelde uygulanması zor bir veri gizleme şeklidir.
- Metin Steganografi'de saklanacak veri miktarı azdır.
- Bunun nedeni taşıyıcı text'in içindeki gereksiz alanların ve boşlukların miktarının az olmasıdır.
- Metin tabanlı gizleme yöntemlerinin hepsi, gizli mesajı geri çözebilmek için ya orijinal metne, yada orijinal metnin biçimlendirme bilgisine ihtiyaç duyar.

Metin Steganografi

Metin Steganografi veri saklanacak yerlerin özelliklerine göre aşağıdaki yöntemleri kullanır.

1. Açık Alan Yöntemleri (Open Space Methods)
2. Yazımsal Yöntemler
3. Anlamsal Yöntemler

1- Açık Alan Yöntemleri (Open Space Methods)

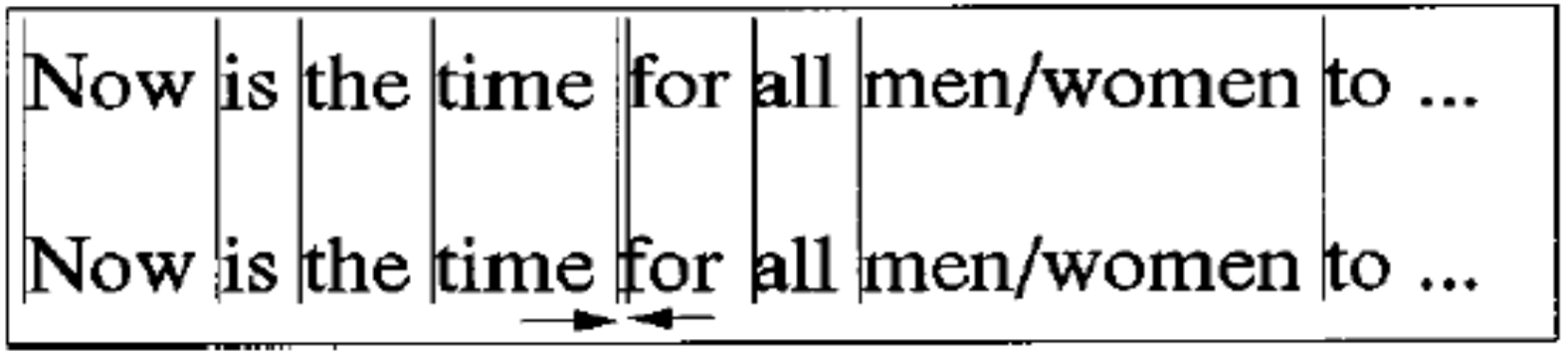
- Bu yöntemler, anormal gözükmeyen iki kelime arasında extra boşluklar, satır sonu boşlukları ile çalışmaktadır.
- Bununla birlikte Açık Alan Yöntemleri'nin ASCII kodları ile kullanılması daha uygundur.

Açık Alan Yöntemleri

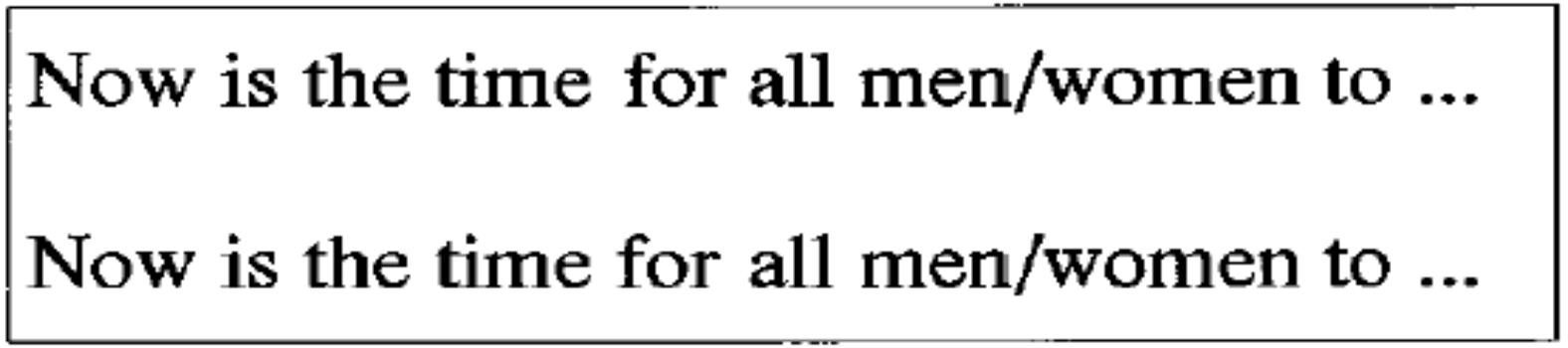
- Açık alan yöntemleri de kendi içerisinde 5 farklı uygulama tipine sahiptir.
  - Cümle içi boşluk bırakma
  - Satır kaydırma
  - Satır sonu boşluk bırakma
  - Sağ hizalama
  - Gelecek kodlaması

a) Cümle İçi Boşluk Bırakma

- Cümle içi boşluk bırakma yöntemi;
  - İngilizce dil yapısında, bir noktadan sonra tek bir boşluk bırakarak “0”ı saklar.
  - Çift boşluk eklemek ise “1”i saklar.
  - Bu işlem işe yarar, ancak çok küçük bir veriyi saklamak için çok büyük veriye ihtiyaç duyar.
  - Bununla birlikte bir çok kelime işleme programı da çift boşlukları otomatik olarak temizler.



(a)



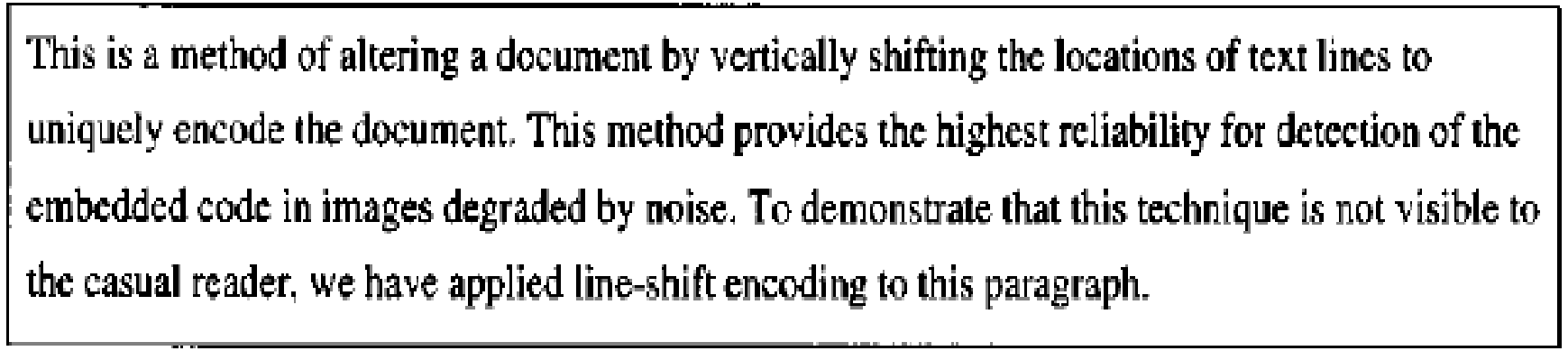
(b)

(a) Üst satır'da "for" kelimesinden önce bir boşluk eklenmektedir, alt satırda for ile all arasında daha fazla boşluk vardır.

(b) Dikey çizgiler olmadan text'in nasıl gözüktüğü

b) Satır Kaydırma Kodlaması

- Bu yöntemde text satırları düşey olarak kaydırılarak gömülecek mesajın kodlanması sağlanır.
- Gömülmüş kelime yine text dosyası yada bitmap dosya olarak açılabilir.


This is a method of altering a document by vertically shifting the locations of text lines to uniquely encode the document. This method provides the highest reliability for detection of the embedded code in images degraded by noise. To demonstrate that this technique is not visible to the casual reader, we have applied line-shift encoding to this paragraph.

Burada ikinci satır 1/300 inch yukarıya kaydırılmıştır.

c) Satır Sonu Boşluk Bırakma

- Satır sonu boşluğu yöntemi, her satırın sonundaki boşluktan faydalanır.
- Veri, tüm satır sonlarında daha önceden belirlenen sayıda boşluklar bırakarak gizlenir.
- Örneğin, iki boşluk bir bit, dört boşluk iki bit, sekiz boşluk dört bit vb. gizler.
- Bu yöntem, iç boşluk metodundan daha iyi çalışır çünkü satır sonundaki boşluk sayısı arttırılarak daha fazla veri gizlenebilir.

d) Sağ Hizalama

- Metinlerin sağa hizalanması da metin dosyalarında veri saklanmasında kullanılabilir.
- Kelimeler arasındaki boşluklar hesaplanıp kontrol edilerek, masum metin dosyalarına veri gizlenebilir.
- Kelimeler arasındaki tek boşluk “0”ı, çift boşluk “1”i temsil eder.

Sağ Hizalama

- Ancak bu yöntem, normal bir boşluk ile gizlenmiş bir boşluk arasındaki farkı anlamak imkansız olduğu için çözme işlemini zorlaştırır.
- Bu amaçla, Manchester kodlamasını temel olan başka bir teknik kullanılır.
- “01” “1” olarak, “10” “0” olarak yorumlanır. Bununla birlikte “00” ve “11” ise null boşluk bitlerini gösterir.

e) Gelecek Kodlaması

- Bu yöntemde, b, d, T gibi harflerin yatay/düşey uzunlukları gibi bazı metin özelliklerini değiştirerek, biçimlendirilmiş metin içine gizli mesajları saklamayla ilgilenir.
- Bu yöntem, her biçimlenmiş metnin, gizli mesaj saklamak için kullanılabilecek çok sayıda özelliği olmasından dolayı, uzak ara durdurulması en zor yöntemdir.

(a)

(b)

(c)

(a) Herhangi bir kodlama yapılmamış orijinal metin.

(b) Sadece seçilen karakterler üzerinde yapılmış gelecek kodlaması.

(c) Gelecek kodlamasının abartılmış gösterimi

2- Yazımsal Yöntemler (Syntactic Methods)

- Bu yöntem, dökümanı kodlamak için noktalama işaretlerini kullanır.
- Örneğin aşağıdaki iki cümle de ilk bakışta aynıymış gibi gözükmektedir, fakat dikkatlice bakıldığında ilk cümlenin fazladan bir ‘,’ işareti içerdiği görülür.
- Bu yapıların biri “1”, diğeride “0” olarak belirlenir ve kodlama işlemi bu şekilde yapılır.
  - “bread, butter, and milk”
  - “bread, butter and milk”

3- Anlamsal Yöntemler (Semantic Methods)

- Bu yöntem W. Bender tarafından ortaya atılmıştır.
- Bu yöntemde eşanlamlı kelimelere birincil ve ikincil değerler atanmaktadır.
- Sonra bu değerler “1” ve “0” olarak binary’e dönüştürülür.
  - Örneğin “*big*” kelimesi birincil, “*large*” kelimesi de ikincil olarak işaretlenmiş olsun.
  - Birincil “1”, ikincil de “0” olarak binary’e çevrilir.

Görüntü Steganografi

Bilgilerin görüntü dosyaları içerisine saklanmasının çeşitli yöntemleri vardır. Bunlar:

1. En önemsiz bite ekleme
2. Maskeleme ve filtreleme
3. Algoritmalar ve dönüşümler

1- En Önemsiz Bite Ekleme (Least Significant Bit Insertion)

- En önemsiz bite ekleme yöntemi yaygın olarak kullanılan ve uygulaması basit bir yöntemdir.
- Fakat yöntemin dikkatsizce uygulanması durumunda veri kayıpları ortaya çıkmaktadır.
- 0-255 arası 1 byte ile temsil edilen gri-seviye (gray-scale) görüntüler vardır.
- Renkli dijital görüntüler 24 bit yada 8 bit olabilir.

24 bit görüntüler

- 24 bitlik bir görüntü bir pixel başına 3 byte kullanmaktadır.
- Her pixel için renk üç ana renkten elde edilir.
  - Kırmızı (red), Yeşil (green), Mavi (blue)
- Her byte'ta son biti değiştirmek suretiyle her pixel'de 3 bitlik bilgi saklayabiliriz.
- Yani 24 bitlik 1024x768 resim, bilgi saklamak için kullanılabilir 2.359.296 bit (294.912 byte)'e sahiptir.
- Eğer gizlemek istediğimiz mesajı resmin içine gömmeden önce sıkıştırırsak çok daha fazla sayıda bilgiyi gizleyebiliriz.

8 bit görüntüler

- 8 bitlik görüntüler pixel başına 1 byte kullanmaktadırlar.
- 8 bitlik görüntüler renk sınırlaması yüzünden pek iyi bir sonuç vermezler.
- Saklanacak bilgi, saklama ortamını çok fazla değiştirmeyecek şekilde dikkatlice seçilmelidir.
- Orijinal görüntüde son bite ekleme işlemi yapıldığında, renk girişi göstergeleri değişmektedir.
- 8 bitlik görüntülerde 4 basit renk kullanılmaktadır. Bunlar; beyaz, kırmızı, mavi ve yeşildir.
  - Bu renklerin renk paletinde karşılık gelen girişleri ise sırasıyla şöyledir:
    - 0 (00), 1 (01), 2 (10), 3 (11)

Gri-seviye görüntüler

- Bununla 0 (siyah) ile 255 (beyaz) arasında tam sayılar elde edilebilir. Bu sayılar arasındaki değerler gri'dir ve bundan dolayı bir resime ait tam sayı "gri ton seviye" (gray level) olarak isimlendirilir.
- İkili sayı sistemine göre 10110111 sayısını ele alalım. Bu sayı onluk düzende 183 sayısının karşılığıdır.
- Sondaki bit'in 1 veya 0 olması bu değeri çok fazla değiştirmeyecektir.
- Sondaki bit değerimiz eğer 0 olsaydı bu değer 182 olacak ve renk üzerinde gözle görülecekbüyük bir değişikliğe neden olmayacaktır.

2- Maskeleme ve Filtreleme (Masking and Filtering)

- Maskeleme ve filtreleme teknikleri genellikle 24 bit ve gri-seviye görüntüler üzerinde işaretleme (marking) ve filigran yapılarak uygulanmaktadır.
- İşaretleme yada filigran tekniklerinin görüntülere sıkça uygulanması nedeniyle, görüntünün değişmesi korkusu olmadan uygulanabilmektedir.
- Teknik olarak filigran bir steganografik biçim değildir.

Algoritmalar ve Dönüşümler (Algorithms and Transformations)

- Son bite ekleme yöntemi bilgi gizlemek için oldukça kolay ve hızlı bir yöntemdir, fakat görüntüye uygulanan işlemler yada kayıplı sıkıştırmalar sonucunda bilgi zarar görebilmektedir.
- Yüksek kalitedeki resimlerin sıkıştırılarak örneğin jpeg formatı kullanılarak internet üzerinden gönderilmesi daha uygundur. Bunun için gizlenen bilginin kaybolmaması ve görüntünün sıkıştırılmasını sağlayan bazı yöntemler ve steganografik araçlar ortaya çıkarılmıştır.

Algoritmalar ve Dönüşümler (Algorithms and Transformations)

Hem sıkıştırma hemde bilgi gizleme işlemlerini yapan

- Jpeg- jsteg
- Stego-Dos
- Picture-Mark
- SureSign
- S-Tools

Algoritmalar ve Dönüşümler (Algorithms and Transformations)

Orjinal resim

Stego-Dos kullanılarak içine veri gömülmüş resim

Ses Steganografi

İnsan işitme sistemi (Human auditory system-HAS) aralığı yüzünden, ses sinyalleri içerisine bilgi gizleme oldukça uğraş gerektiren bir konudur.

HAS 1/1.000'den daha büyük frekans aralığını farkedebilir. Aynı zamanda HAS nereden geldiği belli olmayan gürültülere de oldukça duyarlıdır.

Ses Steganografi

Ses sinyalleri üzerinde uğraşırken ses dosyalarının hangi karakteristiklere sahip olduklarını bilmemiz gerekmektedir. İki ana özelliğe sahiptirler:

Basit niceleme (quantisation) metodu: Yüksek kaliteli dijital seslerin 16-bit doğrusal niceleme ile ifadesinde en çok kullanılan yöntemdir. WAV(Windows Audio-Visual) ve AIIF(Audio Interchange File Format). Bazı sinyal bozulmaları bu formatta ortaya çıkabilir.

Geçici seçme oranı: Ses için en çok kullanılan oranlar 8 kHz, 9.6 kHz, 10 kHz, 12 kHz, 16 kHz, 22.05 kHz ve 44.1 kHz ‘dir. Bu değer frekans aralığının kullanılabilecek en üst seviyesidir.

YMT 311-Bilgi Sistemleri ve Güvenliği

Ders hakkında Bilgilendirme ve temel kavramlar

Ders Hakkında Temel Bilgilendirme

Ders Sorumlusu: Dr. Muhammet BAYKARA

Ders. Lab. Yardımcısı : Arş. Gör. Fırat Artuğer

Ders Saatleri : 3 saat teori, **2 saat laboratuar**

Dersler A405'te uygulamalar ise laboratuar ortamında yapılacaktır.

Devam / Devamsızlık Durumu : Teori : **%30** – Uygulama : **%20**

Dersin Amacı : Bu derste; bilgi ve bilgisayar güvenliği konuları, unsurları ve süreçleri üzerinde durulacak ve yüksek derecede bir güvenlik için uygulanması gerekenler anlatılacaktır. Bilgi ve bilgisayar güvenliğine neden önem verilmesi gerektiği ve bilgi güvenliğinin en temel anlamda nasıl oluşturulabileceği gibi sorulara kapsamlı cevaplar aranmaya çalışılacak, bu kapsamda bilgi güvenliği yazılımları ve proje uygulamaları ortaya konulacaktır.

Dersin İşleniş Biçimi & Nasıl Geçerim!?

- Teorik anlatım
- Haftalık Ödevler
- Dönemlik araştırma ve uygulama projesi
  - Raporlama + Sunum
- Ara sınav, Final Sınavı ve Quizler
- Ders Geçme Notu = (Ara sınav(%33) + Haftalık Ödevler(%33) + Quizler(%34)) *0,4 + ((Final+Proje)/2)*0,6

Dersin Amacı

- Bilgi güvenliği konularında farkındalık ve temel düzeyde teorik ve pratik bilgiler öğrenmenizi sağlamak
- Bilgi güvenliği temel kavram, standart, metodoloji, yöntem ve stratejilerini öğrenmenizi sağlamak
- Araştırma yeteneğinizi geliştirmek
- Kişisel ve kurumsal bilgi güvenliğinin sağlanması konusunda fikir sahibi olmanızı sağlamak

Temel Kaynaklar

1. Kamil Burlu, ***Bilişimin Karanlık Yüzü*** , Nirvana yayınları, 3.baskı, 2010.
2. G. Canbek, Ş. Sağıroğlu, ***Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri***, Grafiker Ltd. Şti. Aralık 2006.
3. Türkay HENKOĞLU, ***Adli Bilişim : Dijital Delillerin Elde Edilmesi ve Analizi,*** Pusula Yayınları, 2011.
4. ***Veri ve Ağ Güvenliği Ders Notları***, İ.Soğukpınar, G.Y.T.E.Bilg.Müh.Bölümü
5. Hamza Elbahadır, ***Hacking Interface***, Kodlab Yayınları, 2010.
6. Bünyamin Demir, Dikeyeksen Yayınları, ***Yazılım Güvenliği Saldırı ve Savunma, 2013.***
7. Ömer Çıtak, Level Yayınları, ***Ethical Hacking*****, 2016.**
8. Kevin D. Mitnick, Çevirmen(Nejat Eralp Tezcan) ***Aldatma Sanatı***
9. Canan Çimen, Sedat Akleylek, Ersan Akyıldız, ***Şifrelerin Matematiği: Kriptoğrafi***, ODTU Yayınları, Ankara.
10. ***Computer and Information Security*** - Handbook
11. ***Elements of Computer Security Book***
12. ***Cryptography And Network Security Principles And Practices***" Stallings Will, Prentice Hall, 2003.
13. ***Security Engineering***, R. Anderson, Wiley, New York, 2001.

Konu Başlıkları

- Bilgi ve bilgisayar güvenliğine giriş, temel kavramlar
- Siber bilgi güvenliği, güvenlik ve hacking kavramları
- Ağ güvenliği
- Şifreleme teknikleri
- Steganografi
- Yazılım güvenliği, bilgi güvenliği yönetimi ve ilgili mevzuatlar
- Sızma belirleme, Saldırı tespit ve engelleme sistemleri
- Bilgi güvenliğinde kullanılan temel araçlar
- Biyometrik güvenlik sistem ve araçları
- Bir siber saldırının senaryosu

Temel Kavramlar

- Bilgi Güvenliği Sistemleri: Information Security Systems
- Bilgisayar Güvenliği: Computer Security
- Saldırı, Sızma, Atak: Attack, Intrusion, Hack
- Saldırgan: Attacker, Hacker, Intruder
- Güvenlik Açığı, Açıklık: Vulnerability
- Bilgi: Information, Öz Bilgi: Knowledge
- Hikmet: Wisdom
- Saldırı Tespit Sistemleri: Intrusion Detection Systems
- Saldırı Önleme Sistemleri: Intrusion Prevention Systems
- Gizlilik: Confidentiality
- Bütünlük Doğruluk: Integrity
- Kullanılabilirlik, erişilebilirlik: Availabilty

Temel Kavramlar

- Sosyal Mühendislik: Social Engineering
- Şifreleme: Cryptology
- Bilgi Gizleme: Steganography
- Klavye dinleme sistemi: Keylogger
- Kötücül yazılım (analizi): Malware (analysis)
- Kaynak kod istismarı-korunmasızlık sömürücü: exploit
- Arka kapılar: backdoor
- Hizmet aksattırma saldırısı: DoS(Denial of the Service)
- Dağıtık hizmet aksattırma: DDoS
- Sağanak: spam
- Casus yazılım: spyware
- Solucan :worm
- Truva atı: trojan horse
- Kök kullanıcı takımı: rootkit
- Koklayıcı, ağ izleyici: sniffer

Temel Kavramlar

- Bilgi Güvenliğinin temel amacı, elektronik veya diğer ortamlarda bulunan her türlü bilgi için,

  - Gizlilik (Confidentiality)
  - Bütünlük (Integrity)
  - Kullanılabilirlik (Availability)…

temel özelliklerini sürekli olarak sağlamaktır.

Temel Kavramlar

Temel Kavramlar- Bilgi Güvenliği

Bilgi Güvenliği Temel Unsurları

- Gizlilik : Bilginin yetkisiz kişilerin eline geçmemesidir.
- Bütünlük : Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.
- Erişilebilirlik : Bilginin ilgili ya da yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır.

Temel Kavramlar- Standartlar

- **TS ISO IEC 27001** Bilgi Güvenliği Yönetim Sistemi
- UEKAE BGYS-0001 Bilgi Güvenliği Yönetim Sistemi Kurulum Kılavuzuna bilgiguvenligi.gov.tr den ulaşılabilir.

Bilgi Güvenliği - Kim Sorumlu?

- Bilgi güvenliğinin sağlanmasından **herkes sorumludur**.
- Bu sorumluluklar yasal olarak da ifade edilmiş ve **5651 sayılı kanun** *"İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi"* amacı ile düzenlenmiştir.

Bilgi Güvenliği – Kim Sorumlu?

- Herhangi bir bilgi sisteminde aşağıdaki konumlardan **herhangi birisinde iseniz sorumluluğunuz var** demektir.
  - Bilginin sahibi
  - Bilgiyi kullanan
  - Bilgi sistemini yöneten
- Bu durum çok geniş bir kitleyi içerdiğinden *"bilgi güvenliğinin sağlanmasından herkes sorumludur"* diye genelleme yapmakta bir sakınca yoktur.

Bilgi

- İşlenmiş veridir.
- Bilgi diğer önemli iş kaynakları gibi kurum için değeri olan ve dolayısıyla uygun bir şekilde korunması gereken bir kaynaktır.
- Bir konu ile ilgili belirsizliği azaltan kaynak bilgidir.

(Shannon – Information Theory)

Güvenlik Üzerine…

- Güvenlik risk yönetimidir (Anonim)
- Bir sistem, yazılımı ihtiyaçlarınız ve beklentileriniz doğrultusunda çalışıyorsa güvenlidir (Practical UNIX and Internet Security)
- Güvenlik, bulunurluk, kararlılık, erişim denetimi, veri bütünlüğü ve doğrulamadır.

Güvenlik ve İnsan

- Güvenlik, teknoloji kadar insan ve o insanların teknolojiyi nasıl kullandığı ile ilgilidir.
- Güvenlik sadece doğru teknolojinin kullanılmasından daha ileride bir hedeftir.
- Doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılmasıdır.

Teknoloji

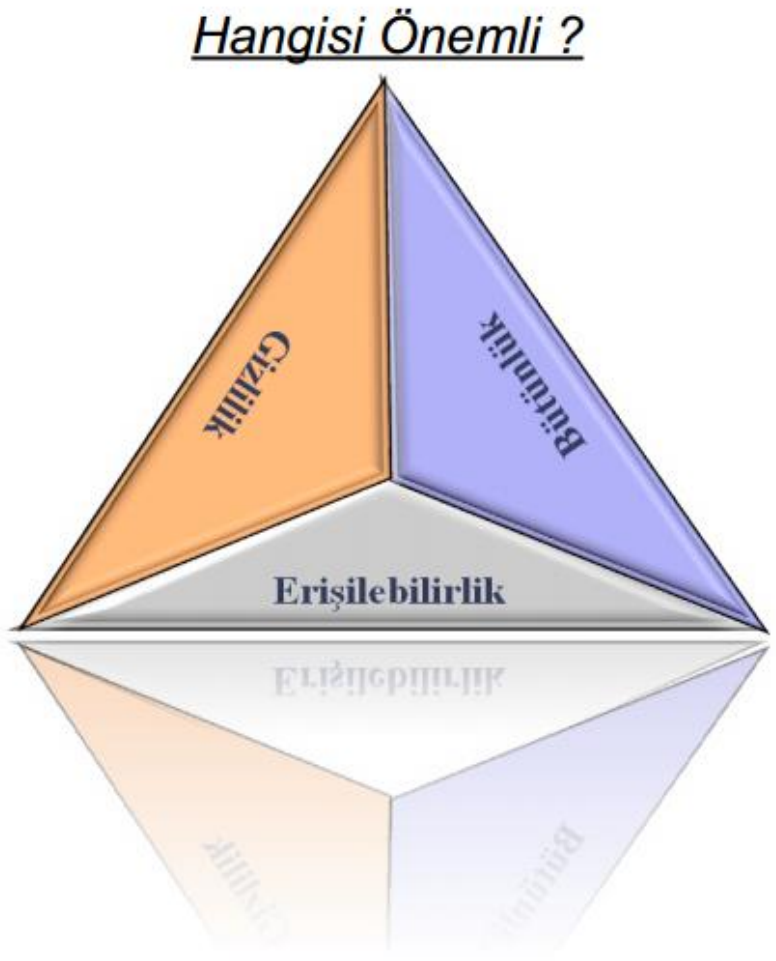
“Eğer teknolojinin tek başına güvenlik probleminizi çözebileceğini düşünüyorsanız, güvenlik probleminiz ve güvenlik teknolojileri tam anlaşılmamış demektir.”

(Bruce Schneier – Şifreleme Uzmanı)

Güvenlik Yönetim Pratikleri

- Gizlilik, Bütünlük, Erişilebilirlik
- Risk Değerlendirmesi ve Yönetimi
- Politika, Prosedür ve Rehberler
- Politika Uygulamaları
- Eğitim
- Denetim

Gizlilik, bütünlük, erişilebilirlik



Gizlilik
Kuruma özel ve gizliliği olan bilgilere, sadece yetkisi olan kişilerin sahip olması

Bütünlük
Kurumsal bilgilerin yetkisiz değişim veya bozulmalara karşı korunması

Erişilebilirlik
Kurumsal bilgi ve kaynakların ihtiyaç duyan kişilerce sürekli erişilebilir durumda olması

Risk Değerlendirmesi

- Kurumsal işleyişi etkileyebilecek olan risklerin belirlenmesi ve değerlendirilmesi sürecidir.
- Bir risk değerlendirmesi yapılmadan, kurumsal işleyişin politika, prosedür ve uygulamalarıyla ne kadar korunduğu belirlenemez.
- Risk yönetimi konusunda yetkililere -tercihen üst yönetim- ihtiyaç duyulmaktadır.
- Üst yönetimin onayı ile sürecin önemi ve verimi artacak, çalışanlar politika ve prosedürlere daha fazla önem verecektir.

Risk Yönetimi

- Kurumun karşı karşıya olduğu risklerin belirlenmesi,
- Varlıkların zaafiyetlerinin ve karşı karşıya oldukları tehditlerin belirlenmesi,
- Ortaya çıkan riskin nasıl yönetileceği ve nasıl hareket edileceğinin planlanması sürecidir.

Risk Yönetimi

- Aşamalar:
  - Risk yönetim ekibi kurma
  - Tehdit ve zaafiyetleri doğrulama
  - Organizasyon varlıklarının değerlerini belirleme
  - Riske karşı yapılacak hareketleri belirleme

  - Kavramlar:
  - Tehdit
  - Zaafiyet
  - Kontroller

Risk Yönetimi Kavramları

- **Tehdit**

  Organizasyonu olumsuz etkileyebilecek olan insan yapımı veya doğal olaylar

- **Zaafiyet**

  Varlıkların sahip olduğu ve istismar edilmesi durumunda güvenlik önlemlerinin aşılmasına neden olan eksiklikler

- **Kontroller**

  Zaafiyetlerin boyutunu azaltıcı, koruyucu veya etkilerini azaltıcı önlemler

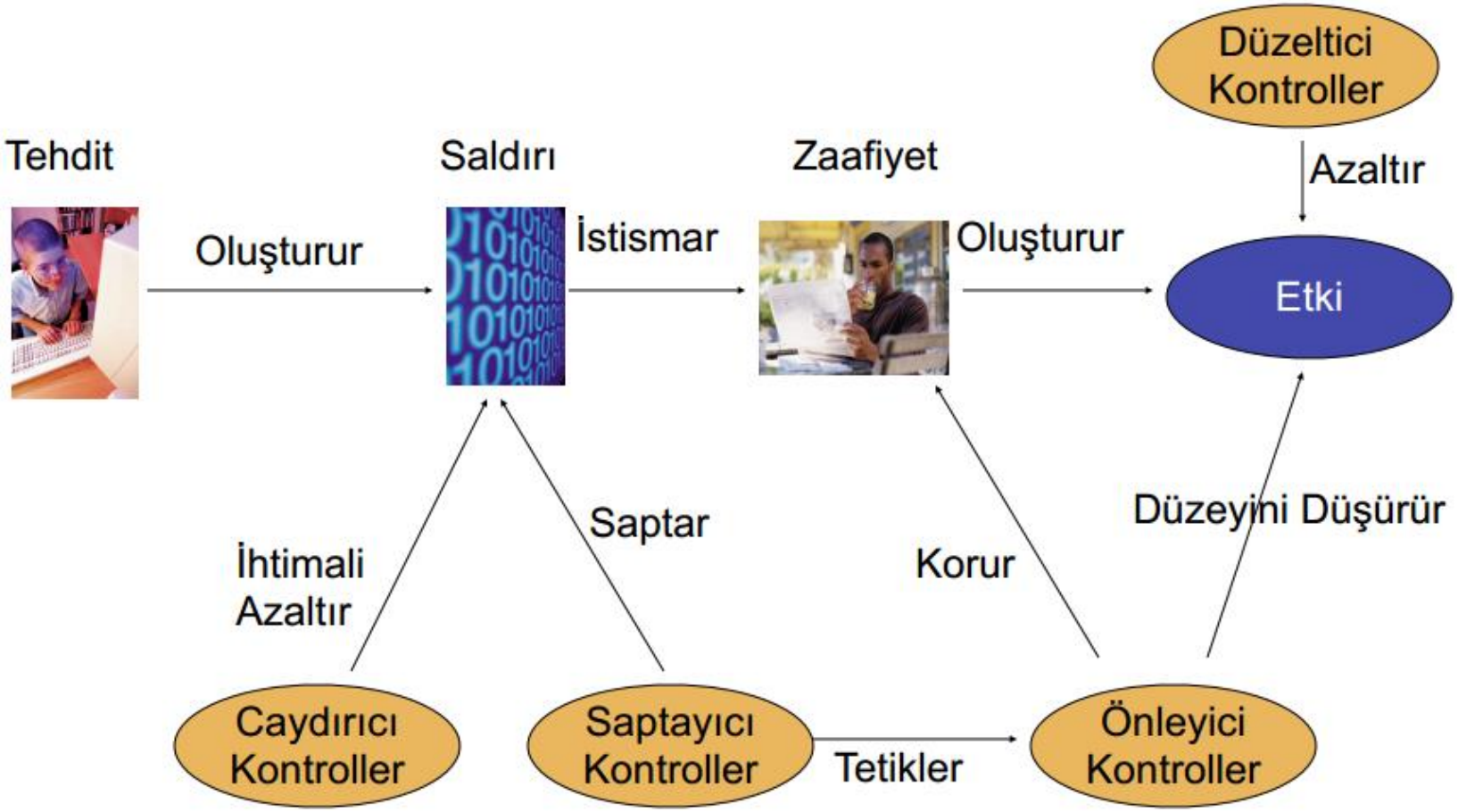
– Caydırıcı Kontroller

– Saptayıcı Kontroller

– Önleyici Kontroller

– Düzeltici Kontroller

Risk Yönetimi Kontrolleri



Risk Yönetimi Takımı

- Tek başına yapılabilecek bir iş değildir, yardımcılar ve diğer önemli departmanlardan çalışanlar ile yapılmalıdır. Böylece riski görmek ve kavramak daha kolay olacaktır.

  Potansiyel Gruplar ;

– Bilişim Sistemleri Güvenliği

– Bilişim Teknolojileri ve Operasyon Yönetimi

– Sistem Yöneticileri

– İnsan Kaynakları

– İç Denetim

– Fiziksel Güvenlik

– İş Devamlılığı Yönetimi

– Bilgi Varlıklarının Sahipleri

Tehditleri Belirleme

- **Doğal Olaylar**

  Deprem, Sel, Kasırga

- **İnsan Yapımı Olaylar**

  -Dış Kaynaklı Olaylar

  Virüs, Web Sayfası Değişimi, Dağıtık Servis Engelleme

  -İç Kaynaklı Olaylar

  *Çalışanlar

  E-Posta Okuma, Kaynaklara Yetkisiz Erişim, Bilgi Hırsızlığı

  *Eski Çalışanlar (Önceki Hakların Kullanımı, Bilgi Hırsızlığı, Gizli Bilgilerin İfşası)

Zaafiyet, tehdit ve risk

Tehdit Tipi	Tehdit	Zaafiyet/İstismar	Oluşan Risk
İç Kaynaklı İnsan Yapımı	Çalışan	Kötü yetkilendirme ve izleme sistemi olmayışı	Veri değişimi veya yok edilmesi
Dış Kaynaklı İnsan Yapımı	Saldırgan	Hatalı güvenlik duvarı yapılandırması	Kredi kartı bilgilerinin çalınması
Doğal	Yangın	Kötü yangın söndürme sistemi	İnsan hayatı kaybı
Dış Kaynaklı İnsan Yapımı	Virüs	Güncellenmemiş anti-virüs sistemi	İş devamlılığının aksaması
Teknik İç Tehdit	Sabit Disk Bozulması	Veri yedeği alınmaması	Veri kaybı, çok miktarda iş kaybı

Varlıkların Değerlerinin Belirlenmesi

- Gerçek risk yönetimi için hangi varlığın kurum için daha değerli olduğu doğru biçimde belirlenmelidir.
- Sayısal/Nicel Risk Değerlendirmesi yapılacak ise varlıklara para birimi cinsinden değer atanmalıdır.
- Eğer Sayılamayan/Nitel Risk Değerlendirmesi yapılacak ise varlıkların önceliklerinin belirlenmesi yeterlidir; ancak çıkacak sonuçların sayısal olmayacağı da ön görülmelidir.

Nicel Risk Değerlendirmesi

- Sayısal risk değerlendirme yöntemidir, sayılar ve para birimleri ile risk belirlenir.
- Sürecin tüm elemanlarına sayısal değer verilmelidir.
  - Varlık, Etki Düzeyi, Korunma Verimliliği, Korunma Maliyeti vb.
- Temel kavramlar ve formüller ile risk değerlendirmesi yapılır.
  - Tekil Kayıp Beklentisi (SLE)
    - *Tekil Kayıp Beklentisi = Varlık Değeri x Etki Düzeyi
  - Yıllık Gerçekleşme İhtimali (ARO)
    - * Tehditin bir yıl içinde gerçekleşme ihtimali
  - Yıllık Kayıp Beklentisi (ALE)
    - * Yıllık Kayıp Beklentisi = Tekil Kayıp Beklentisi x Yıllık Gerçekleşme İhtimali

Nitel Risk Değerlendirmesi

- Nicel tanımlama tüm varlıklara veya tehditlere kolayca uygulanamaz, Nitel tanımlama ise öncelik ve önem seviyelerine göre değerlendirmedir.
- Değerlendirme çıktısı sayısal olmayacaktır, bu durum üst yönetim

tarafından önceden bilinmelidir.

- Soru/Cevap veya Öneriler ile öncelikler belirlenebilir
- Örnek Önceliklendirme Değerleri : Düşük/Orta/Yüksek

– Düşük : Kısa sürede telafi edilebilen durumlar için

– Orta : Organizasyonda orta düzey maddi hasar oluşturan, giderilmesi için maddi harcamalar gereken durumlar için

– Yüksek : Organizasyon sonlanması, müşteri kaybı veya yasal olarak önemli kayıp oluşturacak durumlar için

* NIST 800-026 (National Institue of Standarts and Technology)

(Security Self-Assessment Guide for Information Technology Systems)

Riske Karşı Davranış Belirleme

- **Riskin Azaltılması**

– Bir önlem uygulanarak veya kullanılarak riskin azaltılması

- **Riskin Aktarılması**

– Potansiyel hasar veya durumların sigorta ettirilmesi

- **Riskin Kabul Edilmesi**

– Riskin gerçekleşmesi durumunda oluşacak potansiyel kaybın kabul edilmesi

- **Riskin Reddedilmesi**

– Riskin inandırıcı bulunmaması ve gözardı edilmesi

Politika Prosedür ve Rehberler

- Organizasyonun güvenlik öncelikleri, organizasyon yapısı ve beklentileri yazılı olarak hazırlanmalıdır.
- Üst yönetim, organizasyonun güvenlik önceliklerini belirlemede kilit role ve en üst düzey sorumluluğa sahiptir.
- Hazırlanan politika, prosedür ve rehberler, yasalarla ve sektörel sorumluluklarla uyumlu olmalıdır.
- Hazırlanan dökümanlar, çalışanlardan beklentileri ve karşılanmayan beklentilerin sonuçlarını açıkça ifade etmelidir.

Politika Türleri

- **Duyuru Politikaları**

–Çalışanların, davranışlarının sonuçlarını bildiğinden emin olunması hedeflenmektedir.

- **Bilgilendirici Politikalar**

–Çalışanların bilgilendirilmesini ve eğitilmesini sağlayarak, görevlerinin ve beklentilerin bilincinde olmaları hedeflenmektedir.

- **Yasal Politikalar**

–Organizasyonun attığı adımların, yasal ve sektörel sorumluluklar ile uyumlu olmasının sağlanması hedeflenmektedir.

Güvenlik Kontrolleri

- Güvenlik kontrollerinin amacı, kurumun geliştirdiği güvenlik mekanizmalarının uygulanmasını sağlamaktır.
- Güvenlik Kontrol Türleri
  - Yönetimsel
    - *İşe Alım Süreci
    - *Çalışan Kontrolleri
    - *İşten Çıkarma Süreci
  - Teknik
  - Fiziksel

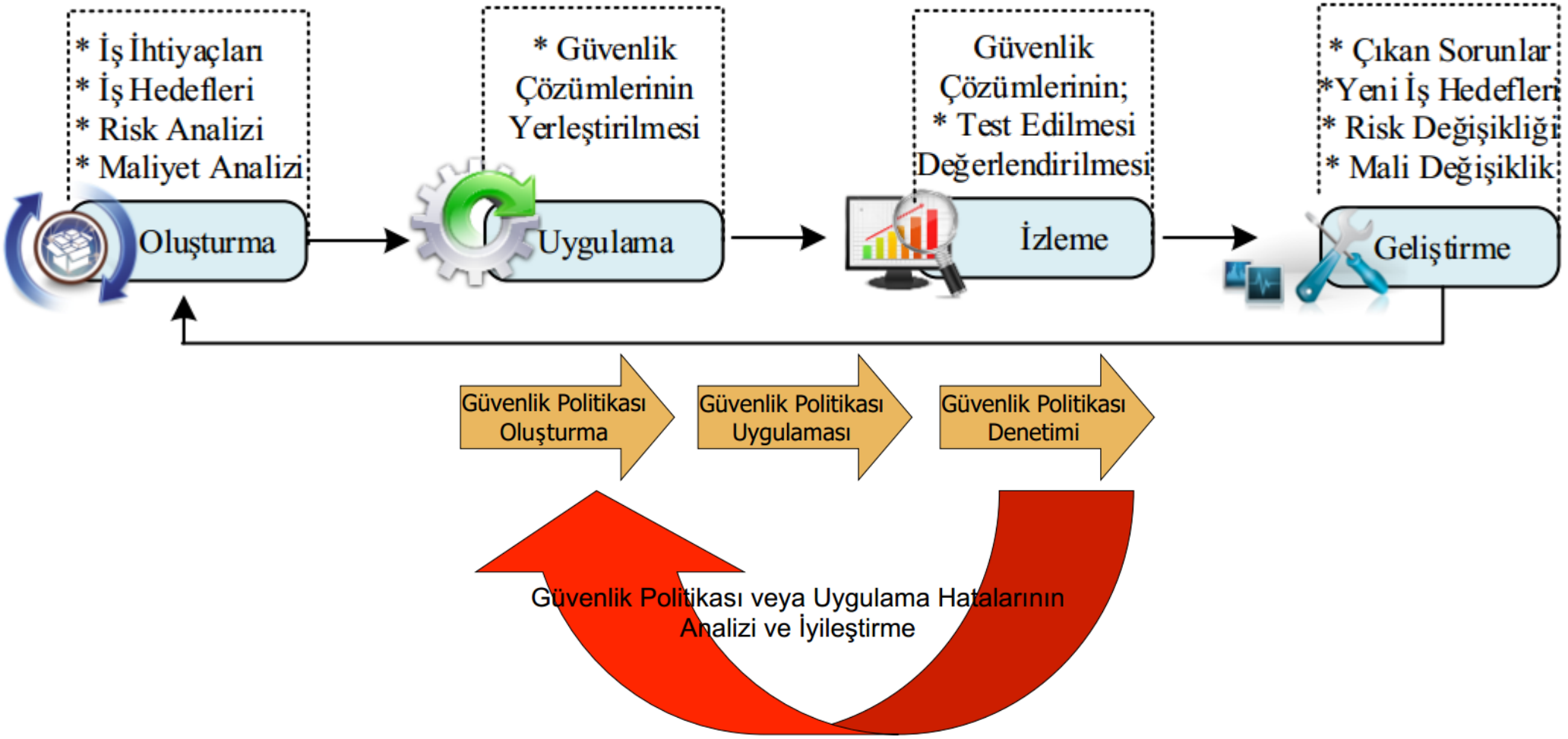
Eğitim

- Çalışanlar, kurum politikaları, görevleri, sorumlulukları, kullanmakta oldukları ekipmanlar ve gerekli teknolojiler konusunda eğitilmelidir.
  - Kısa Süreli Eğitimler
  - Uzun Süreli Eğitimler
  - Farkındalık Eğitimleri
- Eğitim Süreci Bileşenleri
  - Organizasyonun Hedefleri ve Gereksinim Değerlendirmesi
  - İhtiyaçlar Doğrultusunda Uygun Eğitimin Belirlenmesi
  - Eğitim Yöntemleri ve Araçlarının Belirlenmesi
  - Eğitim Verimlilik Değerlendirmeleri

Denetim

- Organizasyonun sahip olduğu güvenlik altyapısı ve güvenlik yönetim süreci periyodik olarak denetlenmelidir.
- Denetim süreci kullanılarak, politikalar ile uygulamaların uyumluluğu, doğru kontrollerin doğru yerlerde uygulandığı ve çalışanlara sunulan eğitimlerin gerçekten işe yaradığı doğrulanabilir.
- Politika denetimlerinde standart yöntem ve şekiller uygulanması zordur. Ancak uygulanan politikaların uyumlu olduğu standartların denetim süreçleri bu konuda rehberlik sağlayabilir.
- Kurum içi veya bağımsız denetçiler tarafından sağlanabilir.

Güvenlik Yönetim Süreci



Bilgi Güvenliği - Sertifikasyon

- CISA,
- CISSP,
- ISO 27001 LA,
- CEH

Bilgi Güvenliği Alanındaki Güncel Meslekler

- #1 Information Security Crime Investigator/Forensics Expert
- #2 System, Network, and/or Web Penetration Tester
- #3 Forensic Analyst
- #4 Incident Responder
- #5 Security Architect
- #6 Malware Analyst
- #7 Network Security Engineer
- #8 Security Analyst
- #9 Computer Crime Investigator
- #10 CISO/ISO or Director of Security
- #11 Application Penetration Tester
- #12 Security Operations Center Analyst
- #13 Prosecutor Specializing in Information Security Crime
- #14 Technical Director and Deputy CISO
- #15 Intrusion Analyst
- #16 Vulnerability Researcher/ Exploit Developer
- #17 Security Auditor
- #18 Security-savvy Software Developer
- #19 Security Maven in an Application Developer Organization
- #20 Disaster Recovery/Business Continuity Analyst/Manager

Bazı Kaynaklar

- http://muhammetbaykara.com/
- http://www.nsa.gov/
- http://www.bilgiguvenligi.gov.tr/
- http://www.bga.com.tr/
- http://www.cehturkiye.com/
- http://www.iso27001bilgiguvenligi.com/
- http://www.bilgimikoruyorum.org.tr/

  http://www.bilgiguvenligi.org.tr/

Nasıl Bir Proje Gerçekleştirebilirim?

- Kurumsal Bilgi Güvenliği açısından ülkelerin geliştirdiği stratejilerin ve ülkelerin bilgi güvenliğine bakış açılarının değerlendirilmesi. (Model, yazılım, strateji, istatistik vb.)
- Saldırı Tespit Sistemlerinin incelenmesi ve geliştirilmesi.
- Snort, ossec, pokemon, bro, firestorm vb. incelenmesi ve olası yeni alanlara uyarlanması
- Anomali temelli saldırı tespit sistemi geliştirilmesi.mpute
- Verilerin güvenli bir şekilde iletilmesine yönelik olarak kripto-steganografi uygulamaları.
- Xss, sql injection açıklıklarının tespitine yönelik uygulamalar.
- Sosyal Mühendislik maillerinin tespit edilmesine yönelik uygulamalar.
- Spam maillere yönelik olarak spamsavar.
- Web loglarının incelenmesiyle saldırı analizi uygulaması.
- DOS, syn flood saldırılarının analiz ve tespiti için çeşitli uygulamalar

Nasıl Bir Proje Gerçekleştirebilirim?

- Web güvenliğini sağlamak amaçlı uygulamalar (CAPTCHA, vb…).
- Biyometrik güvenlik sistemleri, iris tanıma, parmak izi tanıma vb. sistem güvenliği yazılımları
- Tek kullanımlık şifre üretimi ve uygulamaları
- E ticaret güvenliğinin sağlanmasına yönelik geliştirmeler
- Yazılım güvenliği, güvenli kod çalışmaları ve uygulamalar
- Windows azure ile güvenli bir bulut bilişim uygulamaları
- Yazılım Tanımlamalı Ağlarda güvenlik uygulamaları
- Mobil yazılımlarda güvenlik açıklarını önleme-mobil güvenlik.
- Mobil Bulut Bilişim uygulamaları (MCC)
- Veri merkezi-bulut yapısı: Data center networking
- Kötücül yazılım tespitlerine yönelik uygulamalar-Antimalware

Nasıl Bir Proje Gerçekleştirebilirim?

- Güvenlik duvarı uygulamaları
- Antivirüs, antimalware, antispyware uygulamaları
- Web uygulama güvenlik duvarı uygulamaları
- Veritabanı güvenlik duvarı uygulamaları
- E-posta güvenliğinin sağlanmasına yönelik uygulamalar
- Zaafiyet tarama sistemleri
- Kayıt toplama ve korelasyon sistemleri- SIEM
- Sıfırgün zararlı yazılım tespit sistemleri- zeroday
- Ağ izleme, performans analizi ve veri kaçakları önleme sistemleri

Tubitak Yarışmaları ve Destekleri-Yönlendirme

- **DETAYLAR İÇİN RESİMLERİ TIKLAYINIZ**

YMT 311-Bilgi Sistemleri ve Güvenliği

Bilgi ve Bilgi Güvenliği

Konu Başlıkları

- Giriş
- Bilişim Suçları
- Bilgi ve Bilgi Güvenliği
- Sonuç
- Sorular
- Kaynaklar

Giriş

- Bilişim dünyasında bilgi ve bilgi varlıklarının öneminin gün geçtikçe artması, buna paralel olarak bilişim güvenliğinin öneminin de artmasını sağlamıştır. Uluslararası bir ağ sistemi olan İnternet ortamındaki verilerin veya bilgilerin korunması için donanımsal ve yazılımsal güvenlik tedbirleri alınmaktadır.

- Ancak, bu tedbirler sisteme veya bilişim cihazlarına yapılan saldırıları tamamen engelleyememektedir. Bu bağlamda bilişim suçlarının incelenmesi, saldırganların tespit edilmesi için birçok akademik ve ticari çalışmalar yapılmaktadır.

Giriş

- Bu bölümde, bilişim suçları, bilgi ve bilgi güvenliği konuları genel olarak incelenmiştir. Ayrıca bu konularda bilişim suçlarına örnek teşkil edecek saldırılar belirtilmektedir.

Bilgi ve Bilgi Güvenliği
(.Bilgi, Bilginin Değeri)

- En basit tanımlaması ile bilgi kişi ya da kurumlar için kıymet teşkil eden ve para gibi korunması gereken kıymetli bir metadır. Meta ifadesi ile eşya kast edilirken bunun yerine varlık ifadesi de kullanılmaktadır.
- Günümüzde bilgi ön plana çıkmış gibi gözükse de, aslında bilgi; dünün ve bugünün anahtarları iken, geleceğin şekillenmesinde de her zaman anahtar rollere sahiptir.

Bilgi ve Bilgi Güvenliği
(Bilginin Gelişim Evreleri)

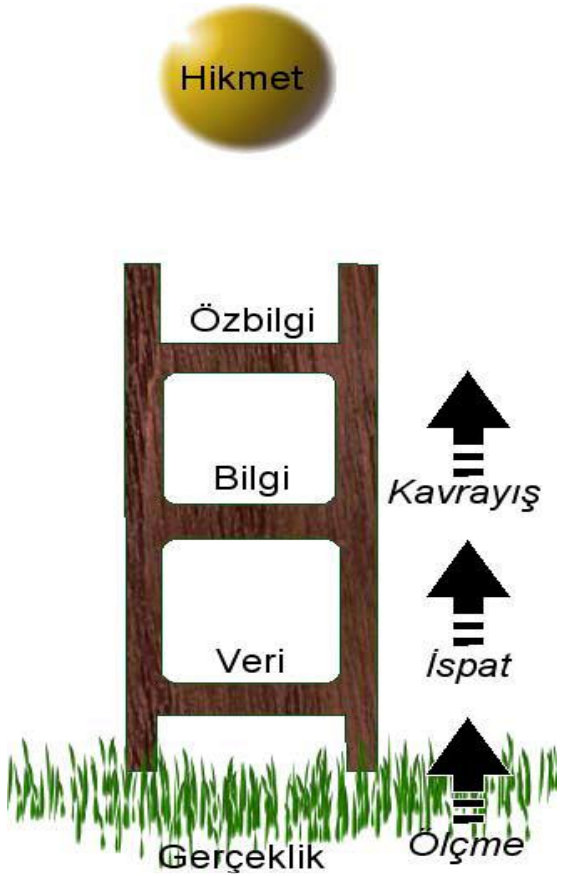
- İnsan bilincinden bağımsız olarak var olanlar veya hikmete ulaşmak için veri haline gelmeye hazır doğada bulunan her şey *gerçeklikdir*.
- Bilişim teknolojisi açısından *veri*, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanabilir.
- *Bilgi;* verinin belli bir anlam ifade edecek şekilde düzenlenmiş halidir. Bilgi; işlenmiş veri olarak ve bir konu hakkında var olan belirsizliği azaltan bir kaynak olarak da tanımlanabilmektedir. Kısaca, veri üzerinde yapılan uygun bütün işlemlerin (mantığa dayanan dönüşüm, ilişkiler, formüller, varsayımlar, basitleştirmeler, v.s.) çıktısı, bilgi olarak ifade edilebilir.

Bilgi ve Bilgi Güvenliği
(Bilginin Gelişim Evreleri)

- *Özbilgi*; tecrübe veya öğrenme şeklinde veya iç gözlem şeklinde elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasıdır. Verilerin bir araya getirilip, işlenmesi bilgiyi oluştursa da özbilgi, kullanılan bilgilerin toplamından daha üstte bir kavramdır. Bir güç oluşturabilecek, katma değer sağlayabilecek veya bir araç haline dönüşmek üzere, daha fazla ve özenli olarak işlenmiş bilgi, asıl değerli olan özbilgidir.

Bilgi ve Bilgi Güvenliği
(Bilginin Gelişim Evreleri)

- Hikmet (wisdom), tasavvur, ileri görüş ve ufkun ötesini görme yetisi ile en ileri seviyede soyutlama ve bir kişinin özel bir iş sahasındaki meslek hayatı boyunca elde edilmiş deneyimin özüdür. Hikmet, ayrıca, güvenilir yargıda bulunmak ve karar vermek için öz bilginin nasıl kullanılacağını kavramak olarak da tanımlanmaktadır.



Bilgi ve Bilgi Güvenliği
(Bilgi Güvenliği)

- *Bilgi güvenliği;* bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak tanımlanır.
- Bilgi güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür.

Bilgi ve Bilgi Güvenliği
(Bilgi Güvenliği)

- Bilgi güvenliğinin sağlanması için kullanılabilecek birçok yöntem olmakla beraber yeni sayılabilecek biometrik alanda yapılan bilgi güvenliği çalışmaları da mevcuttur. Bu biometrik korunma yolları arasında parmak izi ile çalışan sistemler, el ve parmakların şekline göre çalışan sistemler, ses tanıma sistemleri, dijital imza, gözün retina ve iris tabakasından yararlanılarak çalışan sistemler mevcuttur. Buna örnek olarak Kuzey Carolina'daki uluslararası havaalanında kullanılan iris ile çalışan güvenlik sistemi örnek olarak gösterilebilir [18].

Bilgi ve Bilgi Güvenliği
(Bilgi Güvenliği Sertifikasyonu)

- Büyüklüğü ne olursa olsun, ihtiyaç duyan tüm kurumların, kuruluşların bilgilerinin gizlilik, bütünlük ve erişebilirliklerini sağlamak amacı ile kurdukları bilgi güvenliği yönetim sistemini belgelendirmek ve bunu üçüncü taraflara kanıtlamak amacı ile aldıkları; bağımsız belgelendirme kuruluşlarının, yaptıkları denetim sonucu düzenledikleri ve kurumdaki bilgilerin güvenliklerinin sağlanmasına yönelik sistematik bir uygulamanın olduğunun kanıtını sağlamak üzere *kurum* adına düzenlenen sertifikaya veya belgeye TS ISO/IEC 27001 *Bilgi Güvenliği Yönetim Sistemi Belgesi* veya TS ISO/IEC 27001 *Bilgi Güvenliği Yönetim Sistemi Sertifikası* denir.

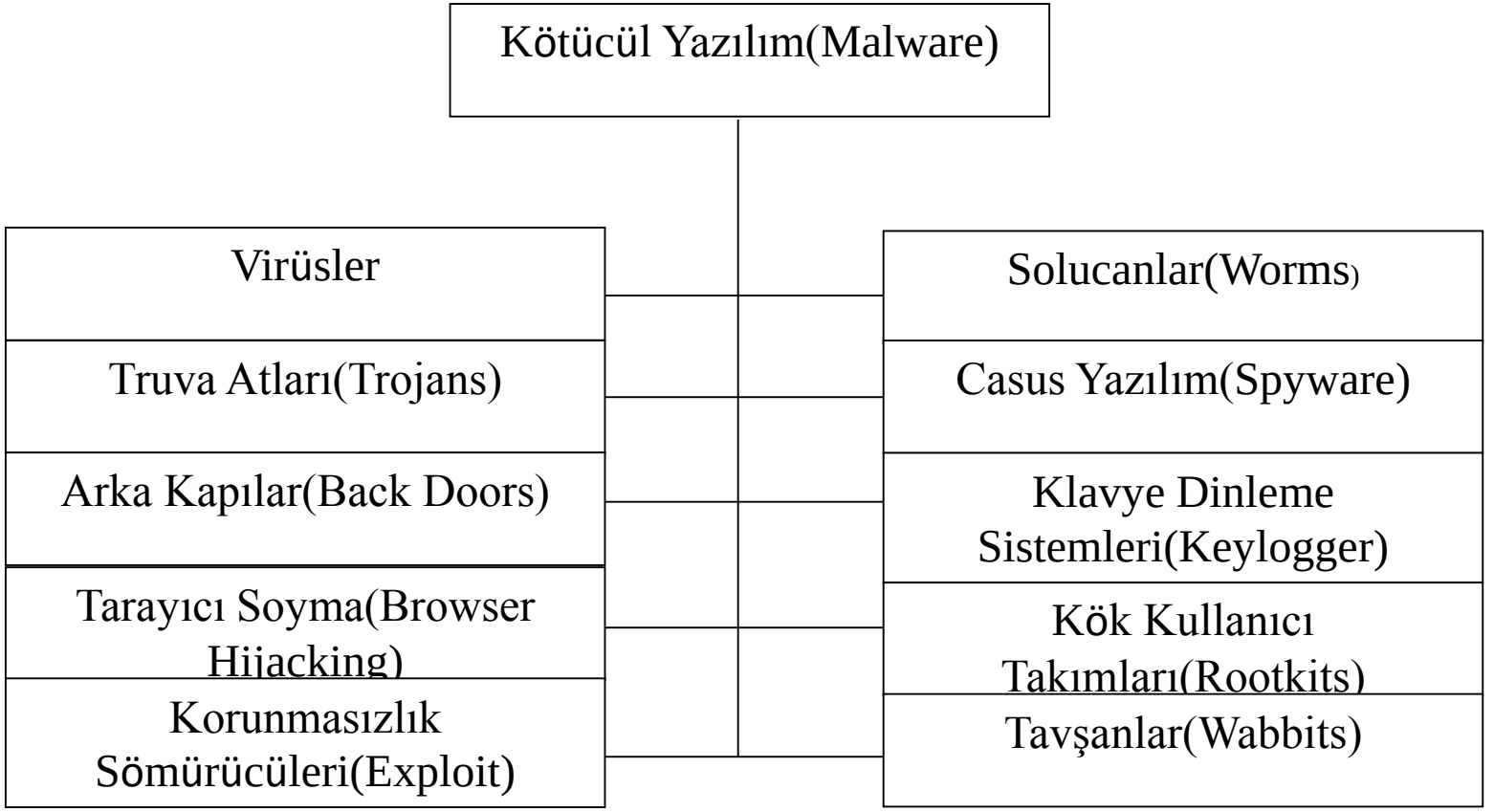
Bilgi ve Bilgi Güvenliği
(Bilgi Güvenliği Sertifikasyonu)

- TS ISO/IEC 27001 bilgi güvenliği yönetim sistemi kurmak ve belgelendirmek bir firmaya, şirkete veya kuruluşa bilgi güvenliği kavramının temel ilkelerini sağlamaktadır. Bilgi güvenliği kavramının temel ilkeleri kısaca G-B-U (C-I-A) kısaltması ile gösterilebilir. Bu kısaltmalar:
  - Gizliliğin korunması (bilgiye ulaşımın, sadece yetki sahibi kişilerce olabildiğinin garanti altına alınması)
  - Bütünlük (bilginin ve bilgi işleme yöntemlerinin, doğruluğunun ve eksiksizliğinin korunması)
  - Ulaşılabilirlik (gereken durumlarda yetkili personelin, bilgiye ve ilgili varlıklara ulaşabilmesinin garanti edilmesi), şeklinde tanımlanır.

Bilgi ve Bilgi Güvenliği
(Kötücül Casus Yazılımlar)

- Kötücül yazılım (malware, İngilizce “malicious software”in kısaltılmışı), bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış yazılımların genel adıdır.

Bilgi ve Bilgi Güvenliği
(Kötücül Casus Yazılımlar)



Tablo 1. Kötücül Yazılım Ana Türleri

Bilgi ve Bilgi Güvenliği
(Kötücül Casus Yazılımlar)

VİRÜS İSMİ	TİPİ	KARIŞTIĞI OLAYLAR	YÜZDE
Win32/Ska	File	140	13.28%
Laroux	Macro	124	11.76%
Marker	Macro	122	11.57%
Ethan	Macro	69	6.55%
Class	Macro	59	5.60%
Win32/Pretty	File	52	4.93%
Win32/NewApt	File	48	4.55%
Melissa	Macro	47	4.46%
Tristate	Macro	44	4.17%
Freelinks	Script	42	3.98%
Win32/Babylonia	File	32	3.04%
Cap	Macro	31	2.94%
Win32/Fix	File	31	2.94%
Thus	Macro	29	2.75%
Win32/Explore.Zip	File	21	1.99%
Win95/CIH	File	19	1.80%

Tablo 2. En Meşhur Virüsler

Bilgi ve Bilgi Güvenliği
(Kötücül Casus Yazılımlar)

Yeni kötücül yazılımlardan bir kısmı şunlardır:

- Sazan avlama (phishing),
- Koklayıcı (sniffer),
- Kandırıcı (spoofer)
- Şifre kırıcılar (password cracker),
- Reklâm yazılım (adware),
- Ağ taşkını (flooder),

bununla beraber daha birçok yeni kötücül yazılımın varlığından bahsedilmektedir [26].

Bilgi ve Bilgi Güvenliği
(Kötücül Casus Yazılımların Bulaşma Yöntemleri)

- Çoğunlukla ücretsiz dağıtılan uçtan uça dosya paylaşımı (P2P) programları, ekran koruyucular ve oyunlar içine casus yazılım bohçalanması ile bulaşma,
- Faydalı bir yazılım kurulumunun yanında; dosya, klasör ve sistem kütüğü isimlerini zararsız, bilindik veya sisteme ait isimler vererek saptanmasını ve sistemden kaldırılmasını zorlaştırarak sisteme yerleşme,
- Uç kullanıcı lisans sözleşmelerinde yanıltıcı veya eksik bildirim ile kullanıcıya zararlı bir yazılımı bilgisayarına kurdurtma,

Bilgi ve Bilgi Güvenliği
(Kötücül Casus Yazılımların Bulaşma Yöntemleri)

- Herhangi bir programın kurulumu sırasında, aslında casus yazılım özelliği taşıyan başka yardımcı ve ek yazılımların kullanıcıya belirtilerek kurdurulması,
- E-posta dosya eklentisi ile e-posta'da verilen bir web adresine gidildiğinde veya doğrudan HTML içerikli e-postaların okunması ile casus yazılım bulaşması,
- İnternet tarayıcılarında bulunan korunmasızlık ve açıklardan yararlanarak kurulum,
- Özellikle internet üzerinden kullanıcıyı aldatıcı mesajlarla yanıltıp; her hangi bir casus yazılımın kurulumunun başlatılması,

Bilgi ve Bilgi Güvenliği
(Kötücül Casus Yazılımların Bulaşma Yöntemleri)

- Çocukları ve bilinçsiz kullanıcıları aldatıcı taktikler kullanmak,
- Çok çeşitli sosyal mühendislik ve insan hatası kaynaklı yöntemler, olarak özetlenebilir.

Bilgi ve Bilgi Güvenliği
(Bilgisayarlarda Kötücül Yazılımların Belirtileri)

- Bilgisayarın her zamanki başarımı düşüyorsa,
- İnternet üzerinde tarayıcı ile sörf ederken istenmedik siteler açılıyorsa,
- İnternet tarayıcısındaki arama çubuğu bölümünde aranmak istenen anahtar kelime girildiğinde ayarlanmış olan arama motoru yerine başka bir arama motoru arama sonuçlarını gösteriyorsa,
- İnternet tarayıcısındaki Sık Kullanılanlar (Favorites) veya Yer İmi (Bookmark) bölümünde yabancı sitelere bağlantılar eklenmişse,
- İnternet tarayıcısının başlangıçta gösterdiği site olan “Başlangıç Sayfası” (Home Page), ayarlanandan başka bir siteyi gösteriyorsa ve bu ayar tekrar düzeltildiğinde yine farklı siteler açılışta ortaya çıkıyorsa,

Bilgi ve Bilgi Güvenliği
(Bilgisayarlarda Kötücül Yazılımların Belirtileri)

- İnternet tarayıcısında daha önce olmayan araç çubukları varsa,
- Sistem tepsisinde (system tray) daha önce bilinmeyen bir simge varsa,
- İnternet'e bağlantı olmadığı durumlarda bile kullanıcı adı ile hitap eden çıkıveren (pop-up) reklamlar görünüyorsa,
- İnternet sayfasında bazı tuşlar çalışmıyorsa (örneğin bir web formu doldururken bir sonraki yazım alanına geçmek için kullanılan sekme (tab) tuşu çalışmıyorsa),
- Bilgisayar ile faal olarak çalışılmadığı bir sırada bilgisayar kasasındaki sabit disk hareketini gösteren lamba sürekli yanıp sönüyorsa,

Bilgi ve Bilgi Güvenliği
(Bilgisayarlarda Kötücül Yazılımların Belirtileri)

- İnternet'e erişim olmadığı sırada sistem tepsisindeki ağ bağlantısını gösteren (iki bilgisayar şeklinde gösterilen) simgede veri aktarımını gösteren hareketler görülüyorsa,
- CD sürücüsü kendi kendine açılıp kapanıyorsa,
- Rastgele hata mesajları çıkıyorsa,
- İnternet'e modem ile bağlanıp da büyük meblağlarda telefon faturası geliyorsa, sistemde çok büyük ihtimalle casus yazılım bulunmaktadır [19,26].

Bilgi ve Bilgi Güvenliği
(Bilgisayarların Kötücül Casus Yazılımlardan Korunması)

Saldırganlar, amaçlarına ulaşmak için çok farklı teknikler içeren saldırılar gerçekleştirmektedirler. Alınabilecek bazı güvenlik önlemlerini gerçekleştirmek bilgisayar güvenliği açısından iyi sonuçlar verecektir. Bu güvenlik tedbirleri aşağıdaki başlıklar halinde özetlenebilir:

- *Kötücül Yazılımlardan Korunma*
- *İşletim Sistemi Güncellemeleri:*
- *Anti-Spyware (Casus Karşı Yazılım):*
- *Host (Sunucu) Bloklama*
- *E-posta kontrolü*
- *Browser (İnternet Tarayıcısı) kullanımı*
- *Ofis Programları*
- *Güvenlik Duvarı (Firewall)*

Bilişim Suçları

- Büyük bir ivme ile önemi artmakta olan bilgi güvenliği ve gün geçtikçe artan bilişim suçlarının adli olarak incelenmesi konuları büyük önem kazanmaktadır.

- Bilişim suçları yakın zamanda ortaya çıkan bir ifade olduğundan bazı kavramların birleşimi ile kendisine tanım bulmaya çalışmıştır. Bu kavramlar tanımlanarak bilişim suçu tanımı daha iyi anlaşılabilecektir.

Bilişim Suçları

- Hukuki anlamda suç, bir toplumdaki hukuki kurumlar tarafından ceza veya güvenlik tedbiri yaptırımına bağlanmış fiildir [1]. Uygulamada ise suç; başka insanların veya tüzel kişiliklerin haklarına tecavüz etmek veya yanlış ya da zararlı olduğu için yasaklanan ve bazı durumlarda cezalandırılan davranış olarak tanımlanabilir [2]. Suçu gerçekleştiren kişiye suçlu denir. Hukuki anlamda bir kimsenin suçlu kabul edilebilmesi için suçun o kimse tarafından işlendiğinin hukuki süreçler sonucunda somut deliller ile ispatlanması gerekmektedir.

Bilişim Suçları

- En genel anlamıyla bilişim alanında kullanılan araçlardan yararlanılarak işlenilen suçlar, bilişim suçu olarak tanımlanmaktadır. Bununla beraber bilişim suçları TCK'de bilişim sistemleri kullanılarak işlenen suçlar olarak tanımlanmaktadır. Bilginin, programların, servislerin, ekipmanların veya haberleşme ağlarının yıkımı, hırsızlığı, yasadışı kullanımı, değiştirilmesi veya kopyalanması da, bilişim suçları olarak tanımlanmaktadır [4].

Bilişim Suçları

- Bir bilişim suçunu işlemedeki nedenler arasında maddi kazanç elde etmek, kişilerin itibarını sarsmak, intikam almak, sosyal hayatta insanlara aktaramadığını sanal ortamda gerçekleştirmek, karalamak veya yakalanma ihtimalinin zor olduğunu düşünerek zevk amaçlı saldırı yapmak gibi sebepler ortaya çıkmaktadır.

Bilişim Suçları

(Ülkemizde Bilişim Suçlarının Durumu ve Örnekler)

- İnternetin yaygınlaşması ile bilişim suçu olarak tanımlayamayacağımız ancak millet menfaatine gibi görünen olaylarda mevcuttur. Bu olaylara somut bir örnek verilirse, mesai saatleri içerisinde bankada sıra bekleyerek işlemlerini tamamlamak isteyen müşterilerle ilgilenmeyen bir çalışanın, bilgisayarında oyun oynadığının görüntülenmesi ve görüntülerin internet ortamına aktarılması olayları da mevcuttur. Bu durum, suç kabul edilmeyip millet menfaatine gözüktüğünden görüntüyü internete aktaran kişi hakkında inceleme başlatılmamış olup, bilişim suçu kapsamına alınmamıştır.

Bilişim Suçları

(Ülkemizde Bilişim Suçlarının Durumu ve Örnekler)

- Ülkemizde artan bilişim suçlarının incelenmesi ve hukuki anlamda kontrolün sağlanması için çalışmalar yapıldığı görülmekte ancak uygulamada henüz istenen seviyeye ulaşılamadığı anlaşılmaktadır.

Bilişim Suçları

(Bilişim Suçlarında Kullanılan Dijital Deliller)

- **Delil:** İşlenen bir suç olayında fail/faillerin ortaya çıkarılabilmesi için ipuçları niteliğinde toplanan kaynaklar *delil* olarak tanımlanır. Bu deliller, aydınlatılması istenen olayın en önemli parçalarıdır. Bu elde edilen deliller bir araya getirilerek tüm resim görülmeye çalışılır. Böylece aydınlatılmak istenen olay bir çözüme kavuşturulmuş olur.

Bilişim Suçları

(Bilişim Suçlarında Kullanılan Dijital Deliller)

- **Delillendirme:** Suçların tespiti ve yargılanmasındaki en önemli husus *delillendirme* olarak tanımlanmaktadır. *Delillendirme* kısaca, bir suç ile ilgili o suçun kim tarafından ve ne şekilde işlendiğini ispat edici nitelikte bilgiler elde edilmesi ve bunun adli mercilere sunulması şeklinde tanımlanabilir.

Bilişim Suçları

(Bilişim Suçlarında Kullanılan Dijital Deliller)

- **Dijital Delil:** Sanal ortamda işlenen suçlardaki, suçluların tespit edilmesi için elde edilen kanıtlar *dijital delil* olarak isimlendirilmektedir. Bir bilişim suçu ile ilgili, elektronik veya manyetik bir ortam üzerinden iletilen veya bu ortamlara kaydedilen bilgilere dijital delil denilmektedir. Bir suçun nasıl olduğunu veya suçtaki kritik elemanları adresleyen teorileri destekleyen veya çürüten, bilgisayar sistemleri kullanılarak kayıt edilen veya iletilen veriler" olarak tanımlamıştır. Dijital deliller "bir suçun işlendiğini gösteren veya suç ile kurban ya da suç ile faili arasında bir ilişki sağlayan veriler" olarak karşımıza çıkmaktadır [7].

Bilişim Suçları

(Dijital Delillerin Özellikleri)

- Dijital deliller, parmak izi veya DNA gibi gizli veriler olabilirler.
- Dijital deliller, kolaylıkla ve hızla sınırları aşabilirler.
- Dijital deliller, kolaylıkla değiştirilebilir, zarar verilebilir veya silinebilirler.
- Dijital deliller, bazen zaman ile sınırlı olabilirler.
- Dijital deliller, genellikle uçucu verilerdir.
- Dijital deliller, güvenliği sağlanmaz ise çabuk deformasyona uğrayabilirler.
- Dijital deliler, yapı itibariyle, fiziksel delillere göre daha hassas ve kolay bozulur niteliktedirler.

Bilişim Suçları

(Dijital Delillerin Özellikleri)

Dijital deliller, normal somut delillere göre yapı itibariyle bazı sıkıntıları barındırmaktadırlar. Bu sıkıntılar şu şekilde özetlenebilir:

1. Dijital Delillerin Bütünlüğü
2. Dijital Delillerin Doğrulanması
3. Dijital Delillerin İnkar Edilememesi
4. Dijital Delillerin Doğruluğu:
5. Dijital Delillerin Daha Sonradan Ele Alınabilirliği [7,11].

Bilişim Suçları

(Dijital Delillerin Bulunduğu Yerler)

Bilişim suçlarındaki dijital delillerin elde edildiği birçok kaynak olabilir. Bunlar genel olarak şu şekilde sıralanabilir:

- Bilgisayar sistemleri (Masaüstü, dizüstü, sunucu vb.)
- Bilgisayar bileşenleri (HDD, memory vb)
- Erişim kontrol araçları(Smart kartlar, biometrik tarayıcılar)
- Çağrı cihazları, Dijital kameralar, PDA ve PALM cihazları
- Harici harddiskler , Hafıza kartları, Network araçları (Modem, yönlendirici, anahtar)
- Yazıcılar, tarayıcılar ve fotokopi makineleri
- Çıkarılabilir yedekleme üniteleri (Disket, CD, DVD…)
- Telefonlar,Kredi kartı okuyucuları,GPS

Bilişim Suçları

(Dijital Delillerin Bulunduğu Yerler)

Dijital deliller birçok tipte karşımıza çıkmaktadır. Bunlardan bazıları şu şekildedir:

- Veri dosyaları
- Kurtarılmış, silinmiş dosyalar
- Kayıp alanlardan kurtarılmış veriler
- Dijital fotoğraf ve videolar
- Sunucu kayıt dosyaları
- E-posta
- Chat kayıtları
- İnternet geçmişi
- Web sayfaları
- Kayıt (log)

Bilişim Suçları

(Dijital Delillerin Bulunduğu Yerler)

Dijital delillerin elde edildiği alanlardan en çok göze çarpanları şunlardır:

- Bilgisayarlar (Masaüstü, dizüstü bilgisayar, PDA, sunucu, istemci)
- Elektronik aygıtlar
- Veri havuzları
- Bir sistemde yapılan işlemleri gösteren kayıtlar, geçmiş bilgileri, erişim listeleri
- Yedekleme üniteleri
- Yazılımlar
- E-Postalar
- Çerezler gibi internet ile ilgili dosyalar[7,11].

Bilişim Suçları

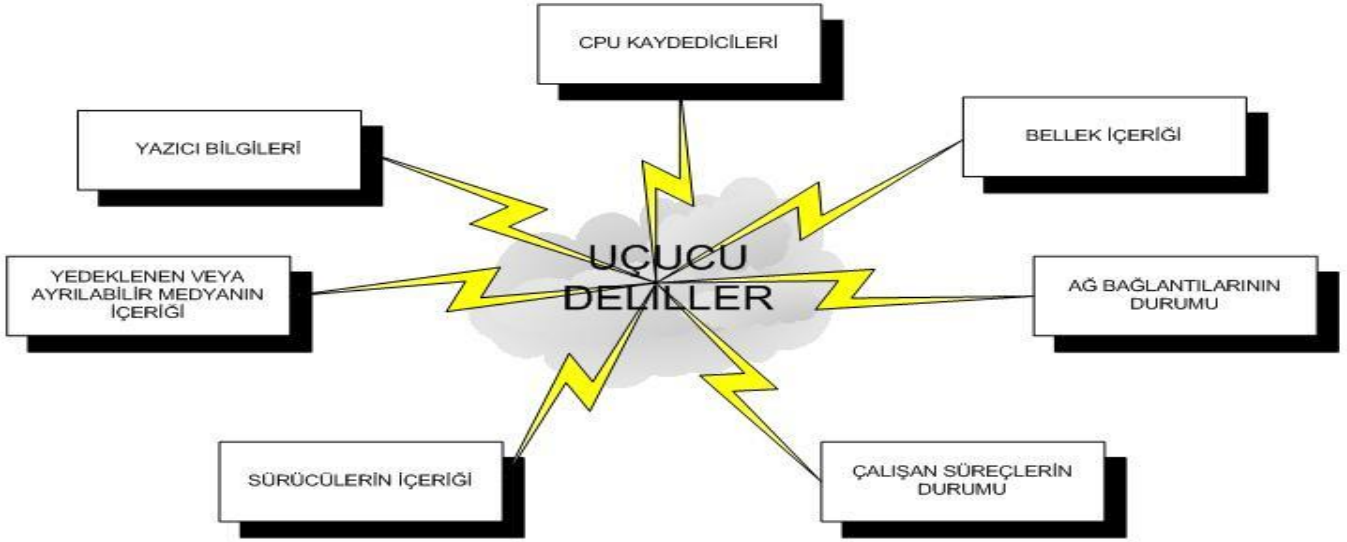
(Dijital Delillerin Toplanması)

- Sanal bir suçun varlığından şüpheleniliyor ise söz konusu suç veya vaka ile ilgili potansiyel delillerin toplanması gerekmektedir. Sürecin doğru bir şekilde işlemesi için öncelikle uygun prosedürleri ve gerekli hukuki şartları anlamak ve sağlamak büyük önem arz etmektedir. Geleneksel delil toplama, delillerin daha sonradan incelenmek üzere sahiplenilmesi anlamına gelmektedir. Fakat dijital delillerde durum biraz farklıdır. Delillerin doğrudan toplanması esnasında bazılarının kaybedilmesi, bozulması ile karşılaşılabilir.

Bilişim Suçları

(Dijital Delillerin Toplanması)

- Uçucu veriler (Ör: bellek, CPU kaydedicileri, çalışan süreçlerin durumu) dediğimiz elektrik kesildiğinde içeriği sıfırlanan ve tekrar kurtarılması mümkün olmayan delillerdir



Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- *Saldırı* ifadesi en bilindik anlamda kötülük yapmak, yıpratmak amacıyla, bir kimseye karşı doğrudan doğruya silahlı veya silahsız bir eylemde bulunma, hücum, taarruz veya bir sistemin kullanılamaz hale getirilmesi için yapılan her türlü meşru veya gayri meşru hareketler olarak tanımlanabilir. Bilişim sistemlerine yapılan saldırılar da *dijital saldırı* olarak tanımlanmaktadır. Dijital saldırılardaki amaç, bilgiyi çalmak, bozmak, sızdırmak veya bilişim sistemindeki yazılım ve donanımlara zarar vermek olarak belirtilebilir. Dijital saldırıları aktif ve pasif saldırı olarak ikiye ayırmak mümkündür.

Bilişim Suçları

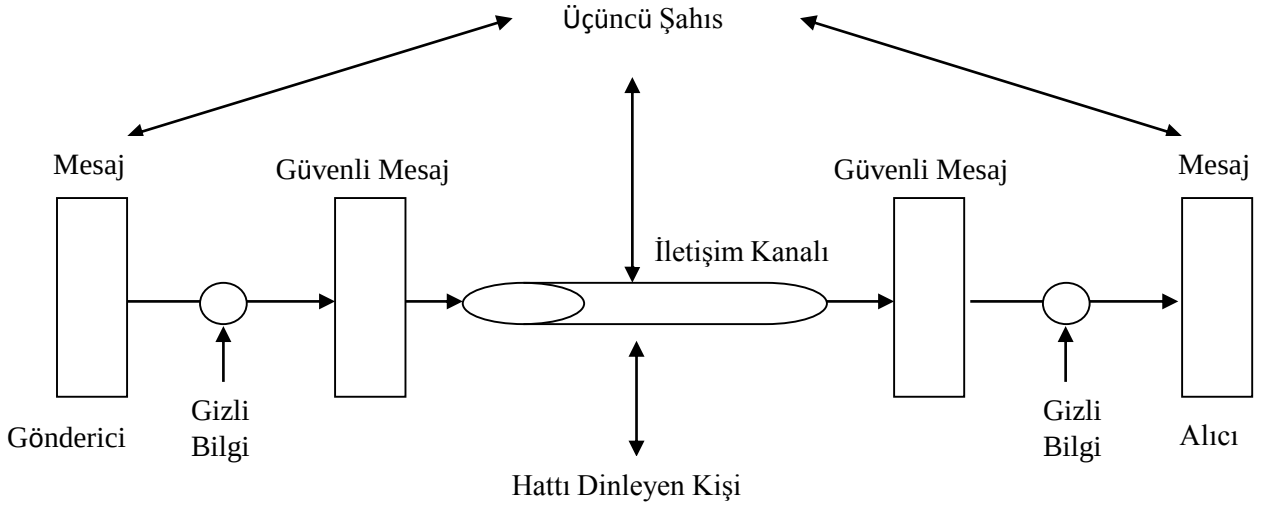
(Dijital Saldırılar ve Dijital Saldırganlar)

- *Pasif saldırıda,* saldırgan taraf pasif davranmakta ve çoğu zaman sadece sistemi gözetlemekle yetinmektedir. Bu saldırı şeklindeki saldırganın yakalanması çoğu zaman daha güç olmaktadır. Pasif saldırı yöntemlerine örnek olarak; Mesajın içeriğini edinme, trafiğin akışını takip etme gibi yöntemler verilebilir.
- *Aktif saldırı* yönteminde ise saldırgan aktif olarak rol oynar ve sistemin içerisine dahil olur. Sistemi savunan tarafın, saldırganı yakalama veya tespit etme ihtimali yüksektir. Aktif saldırı yöntemlerine örnek olarak olarak;
- Rol yapmak (Sniffer olayı, IP aldatmacası vb.)
- Eski mesajın tekrarlanması
- Aktarılan mesajı değiştirme
- Hizmet dışı bırakma/engelleme, gibi yöntemler sayılabilir.

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- Şekilde görüleceği gibi aktif veya pasif saldırı mesajın çıkış noktasından başlayarak varış noktasına kadar üçüncü şahıs olarak adlandırılan saldırgan tarafından herhangi bir bölgede gerçekleştirilebilir.



Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- *Hackerlar (saldırganlar),* kültür ve bilgi düzeyi oldukça yüksek olan, en az bir işletim sisteminin yapısını tam olarak bilen, programcılık deneyimleri yüksek ve konusunda ileri eğitimler alarak uzun yıllarını bu işlere adamış kişilerdir [9]. Diğer bir tanımda ise işletim sistemlerini tam manası ile bilen, derinliklerine inen, bilgisayarla derinlemesine ilgilenen, programlamayı profesyonel düzeyde bilen bilgisayar uzmanlarıdırlar [8].

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- Yapılan hacker tanımlamalarına bakılarak farklı niyette çalışan hackerler olduğu görülmektedir. Hackerlar; beyaz şapkalı hacker, siyah şapkalı hacker ve gri şapkalı hacker olarak sınıflandırılmaktadırlar.
- *Hacking* olarak ifade edilen kavram ise bir sisteme sızma ya da zarar verme anlamında yapılan saldırıların genel adıdır.
- *Beyaz şapkalı hackerlar* bilgi bakımından siyah şapkalılardan aşağı kalmamakla beraber; iyi niyetli, zarar vermeyen, amaçları bilgisayar güvenliğini sağlamak olan kişilerdir [8].

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- *Siyah şapkalı hacker* kavramı ise tamamen kötü niyetli, sırf kazanç elde etmek ve karşıya zarar verme amacıyla sistemlere sızan, bilgi çalan, korsanlar için kullanılır. Bu grup hackerların amacı bilgi çalmak veya sisteme zarar vermektir [8]. Siyah şapkalı hackerlar bazı çalışmalarda korsan, saldırgan veya 3. şahıs olarak da adlandırılmaktadırlar.
- Beyaz şapkalı ve siyah şapkalı grubun arasında kalan *gri şapkalı hacker* olarak adlandırılan bir grup vardır ki bunlar yerine göre siyah yerine göre de beyaz şapkalı hacker gibi hareket ederler.

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- Bilişim sistemlerine zarar vermek amaçlı çalışan kişiler genelde *cracker* tanımlamasına dahildirler.
- Siyah şapkalı hackerlara nazaran daha zararsız olarak tanımlayabileceğimiz *Lamer* ifadesi genelde küçük yaşta ve hacker özentisi olan, birkaç hacker işlemini bilen ancak programlama bilgisi olmayan, herkesin yapabileceği işleri yaparak ün kazanmak isteyen kullanıcılardır. *Script Kiddie* ise genelde lise çağında olan, programlama bilgisi olmayan genellikle e-postalara saldırma işlemlerini öğrenen kişilerdir. Lamerlara göre fazla hacking bilgileri vardır [8].

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- Siber kelimesi bilgisayar ağlarına ait olan, internete ait olan, sanal gerçeklik manalarına gelmektedir.
- Soyut olarak iletişim kurulan sistemler *siber alan* olarak tanımlanmaktadır. Dünya üzerindeki en büyük iletişim sistemi olan interneti anlatan sanal alem ve siber alem kavramlarının ikisi de doğru birer önermedir. Siber alanın yaygınlaşması bazı kavramlarında beraberinde ortaya çıkmasına sebep olmuştur.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- Zorbalık denince sözlü veya fiziksel şiddet anlamları akla gelir. *Siber zorbalık,* bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba, özel ya da tüzel bir kişiliğe karşı yapılan teknik ya da ilişkisel tarzda zarar verme davranışlarının tümüdür. Elektronik zorbalık ve elektronik iletişim zorbalığı olmak üzere iki çeşit siber zorbalık mevcuttur.
- Siber zorbalık veya tehdidin en çok sosyal medya sitelerinde meydana geldiği görülmektedir. Genellikle fotoğraf ve video yayınlama tarzında gerçekleşen bu eylemler bazen sözlü alay ifadeleri ile mahremiyetlere zarar vermektedir.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- *Elektronik zorbalık,* kişilerin şifrelerini ele geçirme, web sitelerini hackleme (bir sisteme izinsiz girmek), spam (zararlı virüs) içeren e-postalar gönderme gibi teknik olayları içeriyor. Bu tip saldırılar, bireylerin web siteleriyle sınırlı kalmayıp, kurumların ve devletlerin siteleri, yazılım ya da donanımlarını da olumsuz etkiliyor.
- *Elektronik iletişim zorbalığı* ise bilgi ve iletişim teknolojilerini kullanarak kişileri sürekli rahatsız etme (cyber-stalking), alay etme, isim takma, dedikodu yayma, hakaret ya da kişinin rızası olmadan fotoğraflarını yayınlama gibi ilişkisel saldırı davranışlarını içeriyor. Bu da direkt olarak insanın duygu ve psikolojisini etkiliyor [14].

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- Bilgi sistemleri doğrultusunda elektronik araçların, bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması aracılığıyla, ulusal denge ve çıkarların tahrip edilmesini amaçlayan kişisel ve politik olarak motive olmuş, amaçlı eylem ve etkinlikler *siber saldırı* olarak isimlendirilmektedir. Siber saldırılar genellikle İnternet üzerinden yapılan tecrübeli hackerların yapabildiği saldırı biçimidir.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- *Siber Terörizm(Savaş)* belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılmasıdır [13].
- Siber terörde, saldırganların elektronik bir saldırı yaparak bir barajın kapaklarını açabilecekleri, ordunun haberleşmesine girip yanıltıcı bilgiler bırakabilecekleri, kentin bütün trafik ışıklarını durdurabilecekleri, telefonları felç edebilecekleri, elektrik ve doğalgazı kapatabilecekleri, bilgisayar sistemlerini karmakarışık hale getirebilecekleri, ulaşım ve su sistemlerini allak bullak edebilecekleri, bankacılık ve finans sektörünü çökertebilecekleri, acil yardım, polis, hastaneler ve itfaiyelerin çalışmasını engelleyebilecekleri, hükümet kurumlarını alt üst edebilecekleri, sistemin birden durmasına neden olabilecekleri ihtimaller dahilindedir.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- *Siber ordular* ulusal güvenliği sanal ortamda sağlayan ordulardır. Siber orduların öneminin farkında olan Amerika Birleşik Devletleri gibi gelişmiş ülkeler sanal ortamda saldırı tespit yöntemleri oluşturmaya yönelik yarışmalar düzenleyerek konu hakkında yetenekli kişileri bu ordularına dahil etmektedirler. Pentagonun düzenlediği güvenlikle ilgili bir yarışmada birinci olan bir Türk öğrencinin Pentagon'dan davet mektubu alması buna bir örnektir [15].

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- Bilişim dünyasında yeni bir kavram olarak yer bulmaya başlayan siber ahlak olarak da tanımlayabileceğimiz siber etik en genel anlamı ile gerçek hayatta iyi bir birey olmak için yapılan fiillerin sanal ortamda da yapılması olarak tanımlanmaktadır.
- Sanal alemde davranış kuralları konusunda özellikle genç kuşağın eğitilmesi gerekmektedir. Günlük yaşamında hırsızlık yapmayı ahlaki değerleriyle veya toplumsal statüsü ile bağdaştıramayan bir genç net ortamında rahatlıkla hırsızlık yapabilmekte veya başkalarına zarar verebilmektedir.

Bilişim Suçları

(Adli Bilişim)

- Adli kelimesi TDK'nin sözlüklerinde adliye teşkilâtı ve hizmeti ile ilgili, adaletle ilgili olarak tanımlanmaktadır. Bu bağlamda adalete intikal etmesi gereken hadiselerin tamamına ise *adli vaka* veya *adli olay* denmektedir.
- Adli bilişim teriminin kökeni, İngilizce orijinal ismi ile Computer Forensics'tir

Bilişim Suçları

(Adli Bilişim Çeşitleri)

1. **Bilgisayar Adli Bilişimi (Computer Forensics) :** Daha çok bir bilgisayar üzerinde yapılacak araştırmalarla ilgilenir. Örneğin: Harddisk, RAM, işletim sistemi üzerinde yapılacak araştırmaları kapsar.
2. **Bilgisayar Ağlarına Yönelik Adli Bilişim (Network Forensics) :** Ağ sistemleri ve iletişimine yönelik incelemeyi kapsar.
3. **Bilgisayar Ağ Cihazlarına Yönelik Adli Bilişim (Network Device Forensics):** Yönlendirici, switch gibi cihazlar üzerinde yapılacak incelemeyi kapsar.
4. **İnternet Adli Bilişimi (İnternet Forensics):** Genel olarak internet kaynakları ve internet sistemleri üzerinde yapılan araştırmayı kapsar.
5. **Bilgi Adli Bilişimi (Information Forensics):** Bütün olarak bilgiyi içeren her türlü materyali barındıran sistemler üzerinde yapılan incelemeyi kapsar.

Bilişim Suçları

(Adli Bilişim Çalışma Alanları)

- Adli bilişimin çalışma alanlarından bazıları ana başlıklar halinde şöyle sıralanabilir:
- Veri kurtarma
- Veri imha etme
- Veri saklama
- Veri dönüştürme
- Şifreleme(Kriptografi)
- Şifre çözme
- Gizlenmiş dosya bulma.

Bilişim Suçları

(Adli Bilişimin Faydaları)

- Adli bilişim, yalnızca bilişim suçlarına has bir delil toplama metodu değildir. Bilişim suçlarından başka, klasik suçlara ilişkin olarak da ihtiyaç duyulan deliller, yine elektronik aygıtlar içerisinde de yer alabilir. Örneğin, bir bilişim suçu olmayan bir hırsızlık vakasında, soygun planı ve buna ilişkin haritalar bilgisayar ile hazırlanmış ve halen bilgisayarda mevcut olabilir. Bu bilgilere ulaşmada da yine adli bilişim devreye girecektir. Bu duruma en bariz örnek olarak; hala devam etmekte olan *Ergenekon* soruşturması ile alakalı bazı verilere, bilgisayar kayıtlarından ulaşılması gösterilebilir.

Bilişim Suçları

(Adli Bilişim Uzmanlığı)

- *Adli bilişim uzmanı*, bilişim sistemleri konusunda ileri derecede bilgi sahibi olan kimsedir.
- Adli bilişim uzmanı kabul edilmek için birtakım sertifika programları mevcuttur. Bu programlardan birine devam ederek sertifika almak ve adli bilişim uzmanı sıfatına sahip olmak mümkündür.
- Bu sertifika programlarından en çok kabul edilenleri şunlardır: EnCase Certified Examiner (ENCE), Certified Computer Examiner (CCE), Certified Computer Crime Investigator (CCCI), Computer Forensic Computer Examiner (CFCE), Certified Information Forensics Investigator (CIFI), Professional Certified Investigator (PCI) [16].

Bilişim Suçları

(Adli Bilişimde Dijital Delillerin Kanıt Olarak Kullanılabilmesi)

- Adli bilişimde elektronik bulgunun, bir hukuki delile dönüştürülme süreci belli prosedürleri takip eder. Uygulanan bu prosedürlerden sonra dijital delil, kendisini bir hukuki delil olarak ortaya koyar. İşte bu prosedüre, *adli bilişim safhaları* denilmektedir. Adli bilişimde dijital delillerin kanıt olarak kullanılabilmesi için incelenmesi gereken dört safha şu şekildedir [16]:
- Toplama (Collection)
- İnceleme (Examination)
- Çözümleme (Analysis)
- Raporlama (Reporting)

Sonuç

- Bilgi güvenliği konusunda güvenlik açıklarının önlenebilmesi için, kişilerin ve kurumların basitten en karmaşık yöntemlere kadar bir dizi önlemler alması gerekir. Ancak, tüm önlemler alınmış olsa da, sürekli gelişen saldırı teknikleri yüzünden, hiç kimse ve hiç bir kuruluş kendini %100 güvende hissetmemelidir. Saldırılar; kötü niyetli kişiler, arkadaşlarımız veya tanıdığımız kişilerden gelebilir.

Sonuç

- Alınması gereken en temel önlemler, risklere karşı sürekli uyanık olmak, bu çalışmada açıklanan saldırı tekniklerine karşı uyanık olmak, yeni gelişmeler ışığında gerekli güncellemeleri yaparak saldırılardan etkilenme olasılığını en aza indirgemek olarak belirtilebilir. Güvenliğin statik değil dinamik bir sürece sahip olduğu, koruma ve sağlamlaştırma ile başladığını, bir hazırlık işlemine ihtiyaç duyulduğu, saldırıların tespit edilmesinden sonra hızlıca müdahale edilmesi gerektiği ve sistemde her zaman iyileştirme yapılması gerektiği unutulmamalıdır.

YMT 311-Bilgi Sistemleri ve Güvenliği

Siber Bilgi Güvenliği

Konu Başlıkları

- Genel Bakış ve Terminoloji
- Gündemdekiler
- Mevcut Durum Analizi
- Güncel Tehdit ve Tehlikeler
- Nasıl bir SBG? Öneriler
- Sonuç ve Değerlendirmeler

Tanım : Siber Güvenlik?

- “Kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler, politikalar, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama deneyimleri ve kullanılan teknolojiler bütünü” olarak tanımlanıyor.

Bilgi Nedir ?

- İşlenmiş veridir.
- Bir konu hakkında belirsizliği azaltan kaynaktır (Shannon).
- Kişi/kurum/kuruluşlar için önemli ve değerli olan bir kaynaktır ve korunması gerekir.
- Veri (data), bilgi (information), ve özbilgi (knowledge)

Bilgi Nedir ?

- Boşlukta ve zamanda yer kaplar.
- Gürültü çıkarmadan hareket edemez.
- Bilginin hareket etmesi için enerji gerekir.
- Bilgi yaşam ve herhangi bir düzenli etkinlik için gereklidir.
- Bilgi hem maddesiz biçim; hem biçimsiz maddedir.
- Işık gibi, bilgi'nin de ağırlığı vardır. Bir GB, bir parmak izinden daha az ağırlıktadır.
- Bilgi zaman içinde hareketli veya donmuş olabilir.
- Bilgi, bir soruya tatmin edici, belki de rahatsızlık verici cevaptır.
- Bir taşın ağırlığı ile bunu tanımlamak için gerekli bilgi birbirine eşittir.
- Bilgi, katı hale sahiptir; donarak katılaşır (depolama).
- Bilgi, sıvı hale sahiptir; akar (iletişim).
- Bir yerlerde bilgi hareket eder; evren gümbürder ve gerçeği gürler.
- Maddeden farklı olarak bilgi aynı anda birden fazla yerde olabilir.
- El sıkışma bir bilgidir. Bir baş sallama, bir bakış, bir iç çekiş.
- Bilgi, rastsallık denizinde parlar.

BİLGİ (Veri)?

- İngilizce karşılığı olarak “data”,
- Latince “datum” (çoğul şekli “data” ve “vermeye cesaret etmek” fiilinin geçmiş zamanı, dolayısıyla “verilen şey”)
- Latince “data” (dedomena) kavramının M.Ö. 300 yıllarında Öklid’in bir çalışmasında geçtiği bildirilmektedir.
- Dilimizde de verilen şey anlamında, “veri” olarak kullanılmaktadır.
- Bilişim teknolojisi açısından veri, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanabilir.

BİLGİ (Bilgi)?

- Bilgi, verinin belli bir anlam ifade edecek şekilde düzenlenmiş halidir.
- Veri ve ilişkili olduğu konu, bağlamı içinde bilgi üretecek şekilde bir araya getirilir.
- İşlenmiş veri olarak da ifade edilebilecek bilgi, bir konu hakkında var olan belirsizliği azaltan bir kaynaktır.
- Veri üzerinde yapılan uygun bütün işlemlerin (mantığa dayanan dönüşüm, ilişkiler, formüller, varsayımlar, basitleştirmelerin) çıktısıdır.

BİLGİ (Özbilgi)?

- Tecrübe veya öğrenme şeklinde veya iç gözlem şeklinde elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasıdır.
- Verileri bir araya getirip, işlemek bilgiyi oluştursa da; özbilgi, kullanılan bilgilerin toplamından daha yüksek bir değer sahip bir kavramdır.
- Bir güç oluşturabilecek, katma değer sağlayabilecek veya bir araç haline dönüşmek üzere, daha fazla ve özenli olarak işlenmiş bilgi, asıl değerli olan özbilgidir.

Veri-Bilgi-Özbilgi ?

- Veri (data), bilgi (information), özbilgi (knowledge) basamaklarıdır.
- Gerçeklik (reality) ile hikmet (wisdom) arasında gösterilen bu merdivenin basamakları
- Çoğu durumda her basamak, atlanmadan teker teker geçilir.
- Yukarıya çıktıkça elimizdeki şeyin miktarı azalırken; değeri artar.
- Yine yukarıya çıktıkça bir sonraki basamağa adım atmak daha da zorlaşır ya da daha çok çaba ister.
- Genel olarak bilimin getirdiği yöntemlerden ölçme ile,
- eldeki gerçeklikten **veriye ulaşılır;**
- ispat ile, veriden **bilgiye ulaşılır ve**
- kavrayış ile, bilgiden **özbilgiye ulaşılır.**
- Bir özbilginin gerçeklik haline dönüştürülmesi de mümkündür. Bunun için yönetim biliminden yararlanılır.

Güvenlik?

- Karşılaşılabilecek tehditlere karşı önlem alma
- Kişi ve kurumların BT kullanırken karşılaşabilecekleri tehdit ve tehlikelerin daha önceden analizlerinin yapılarak gerekli önlemlerin alınmasını sağlama

Bilgi Güvenliği?

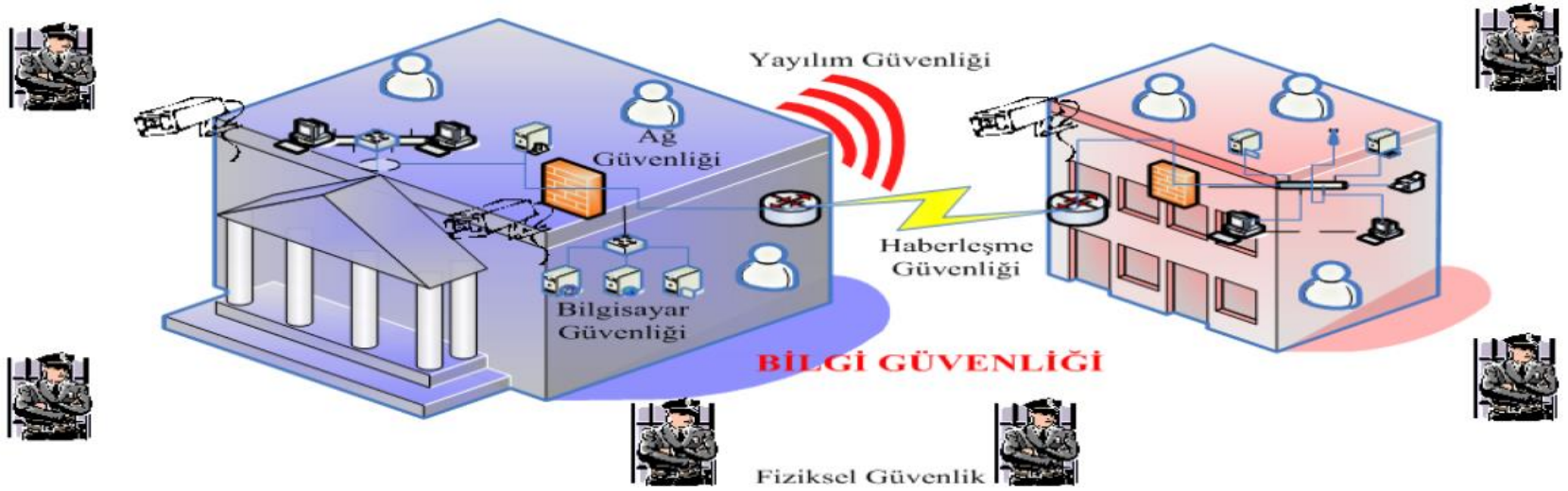
- Bilginin değerli veya değersiz olduğunu belirlemek veya bilginin taşıdığı değeri ölçmek, en az bilginin kendisi kadar önemlidir.
- Bilgiyi değerlendirirken bilginin kalitesini gösteren özelliklere bakılması gerekir.
- Doğruluk, güncellik, konuyla ilgili olma, bütünlük ve öz, gereksinimlere uyum gösterme, iyi sunulma ve fiziksel ve idrak yolu ile erişim gibi ölçütler bilginin kalitesini belirleyen etmenlerden bazılarıdır.
- Bilginin çok önemli bir varlık olması, ona sahip olma ile ilgili bazı konuların düzenlenmesi ve yeni şartların getirdiği özelliklere göre ayarlanmasını gerekmektedir.
- Bilgi en basit benzetme ile para gibi bir metadır.

Bilgi Güvenliği?

- Dünya gündeminde bir konudur.
- Bilginin bir varlık olarak hasarlardan korunması
- Doğru teknolojinin doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda istenmeyen kişiler veya sistemler tarafından elde edilmesini önleme

Bilgi Güvenliği?

- Bilgiye sürekli olarak **erişilebilirliğin sağlandığı bir ortamda,** bilginin göndericisinden alıcısına kadar **gizlilik** içerisinde,bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden **bütünlüğünün sağlanması ve güvenli** bir şekilde iletilmesi **sürecidir.**



Siber Bilgi Güvenliği ?

- Bilgi Güvenliği nerede sağlanmalı ?
  - Üretim
  - Erişim
  - İşleme
  - Depolama
  - Aktarma
  - Yok etme

Siber Güvenliğin Temel Hedefi?

- Kurum ve kuruluşların veya en genel anlamda ulusların bilgi varlıkları ve kaynaklarını hedeflenen amaçlar doğrultusunda organizasyon, insan, finans, teknik ve bilgi değerlerini dikkate alarak, varlıkların ve kaynakların başlarına **KÖTÜ BİR ŞEYLER GELMEDEN korumaktır.**

Tanım (ABD Başkanı Barack Obama)

- “Ülke olarak karşılaşılan çok ciddi ekonomik ve ulusal güvenlik sağlama hedeflerinden birisi olup hükümet veya ülke olarak henüz tam anlamıyla önlem alamadığımız bir hususdur.” “Amerika’nın sayısal altyapısını kapsamlı olarak güven altına alma yaklaşımlarının geliştirilmesi ve bilgi ile haberleşme altyapısının savunulmasına yönelik olarak federal çözümlerin gözden geçirilmesi” emrini verir. **"21. yüzyılda Amerika’nın ekonomik zenginliği, siber güvenliğe bağlı olacaktır."** ***Mayıs 2009***

Ülkemizdeki Tanımlar..

Ulaştırma Bakanı Sn. Binali Yıldırım

- “bilgi sistemi güvenliğinde ortak akıl ve ortak hareketle hattı müdafaa yerine sathı müdafaanın başarılı bir şekilde gerçekleştirilme girişimi”,
- “devletin birinci dereceden ilgilenmesi gereken bir mesele olarak görüyoruz.”
- “siber savaş tehdidine karşı hazırlıklı olmanın, kurumların bilgi sistemi güvenliği olaylarına müdahale yeteneği ile kurumlar arası koordinasyon yeteneğini tespit ederek, alınacak önlemler ve bilincinin arttırılmasını amaçlamak”

Faydalar

1.Zamandan bağımsızlık
2.Mekandan bağımsızlık
3.Hız
4.Verimlilik
5.Gelişim/Değişim
6.Hayatı kolaylaştırıyor
7.Yönetmeyi kolaylaştırıyor
8.Denetlemeyi kolaylaştırıyor

Zararlar

1. Bilmeyenler için kontrolü zor..
2. Açıklarını bilenleri öne çıkarıyor..
3. Kötülere çok yardımcı oluyor..
4. Bilmeyenlere hayatı dar ediyor..
5. Bağımlılık yapıyor..
6. Kişisel gelişimi kısmen olumsuz etkiliyor..
7. Gelişmemiş toplumları köleleştiriyor..

60 saniyede neler oluyor? -1

- 168 milyon e-posta gönderiliyor.
- 1500’den fazla blog iletisi yayımlanıyor.
- 70’den fazla domain adı alınıyor.
- Flicker üzerinden en az 6600 fotograf paylaşılıyor.
- Skype üzerinden 370000 dakika konuşuluyor
- Scribd üzerinden en az 1600 okuma gerçekleşiyor.
- Pandora’da 13000 saatten fazla müzik akıyor.
- 13 000 IPhone uygulaması indiriliyor..

60 saniyede neler oluyor? -2

Facebook

- En az 695000 Facebook durum güncellemesi yapılıyor.
- 79364 duvar iletisi yazılıyor.
- 510040 yorum yapılıyor.

Twitter

- 320 Twitter hesabı açılıyor
- En az 98000 Tweet atılıyor.
- 13000 fazla iPhone uygulaması indiriliyor.

60 saniyede neler oluyor? -3

Youtube

- 600000’den fazla yeni görüntü yayımlanıyor.
- Dünya genelinde YouTube'de kalma süresi 25 saatten fazla.

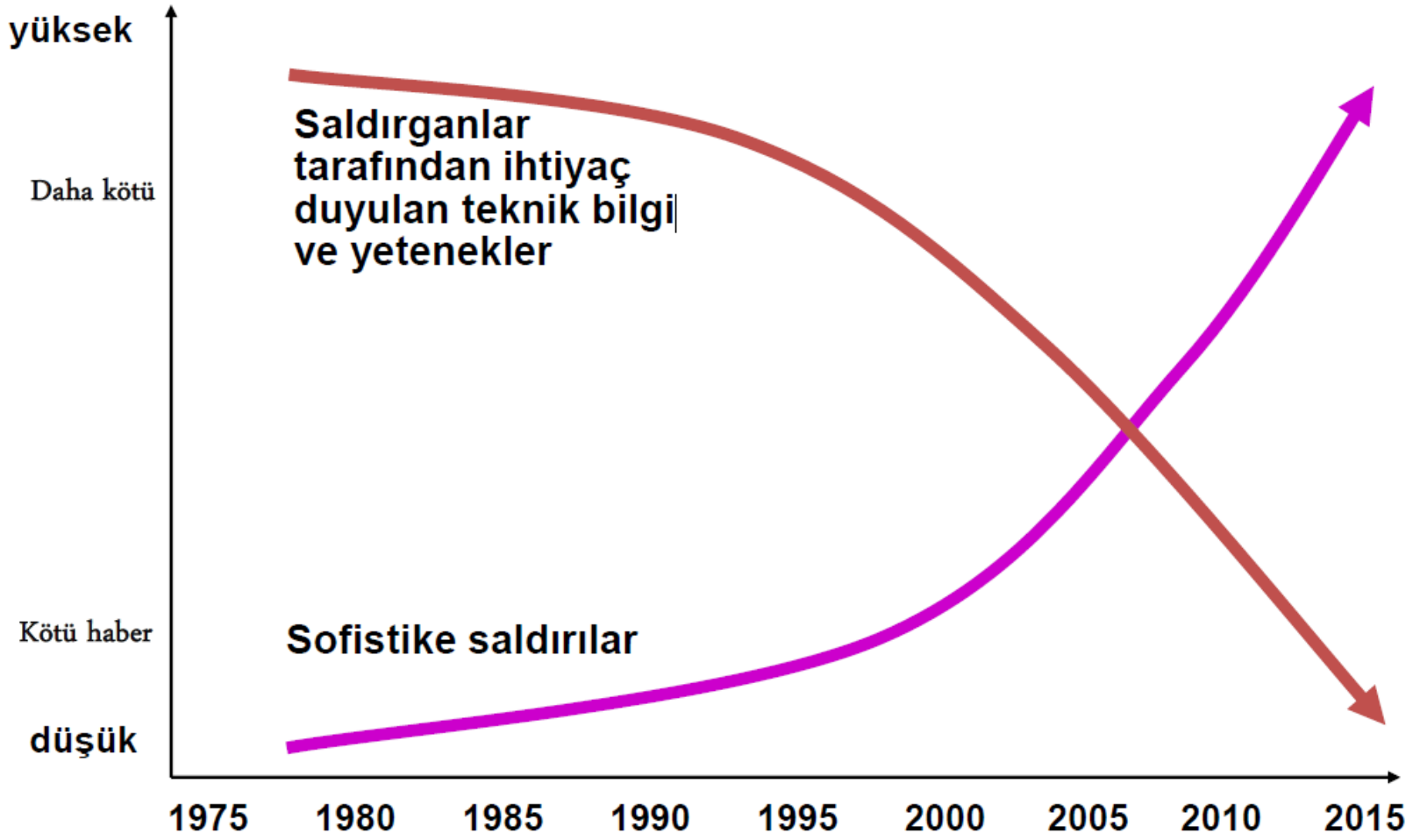
Yahoo

- en az 100 soru ve 40 cevap Yahoo’da akıyor.

LinkedIn

- LinkedIn’e 100’den fazla profil ekleniyor.

Siber Ortamlar



Siber Ortamlar

Ulusal Askeri Stratejiler doğrultusunda;

- 15 Kasım 1940'da 500 savaş uçağı İngiliz Coventry şehrini bombaladı.
- Kod adı "Ay Işığı Sonatı" (Ludwig van Beethoven)
- Bu saldırı Enigma kullanılarak şifrelenmişti.
- Yüzlerce ölü ile beraber şehrin üçte ikisi yıkıldı.
- Kendi bilgi ve bilgi sistemlerimizi etkin bir şekilde kullanırken amaç savaşı kazanmak

Siber Ortamlar

- 1952’de Amerikan Ulusal Güvenlik Ajansı (NSA)
- Amerikan karar vericilere ve askeri liderlere zamanında bilgi sağlamak için Başkan Truman tarafından kurulmuş 1960'da Rusya'ya iltica eden iki NSA görevlisi ABD'nin 40 ülkenin haberleşmesini dinlediğini açıklamışlardır.

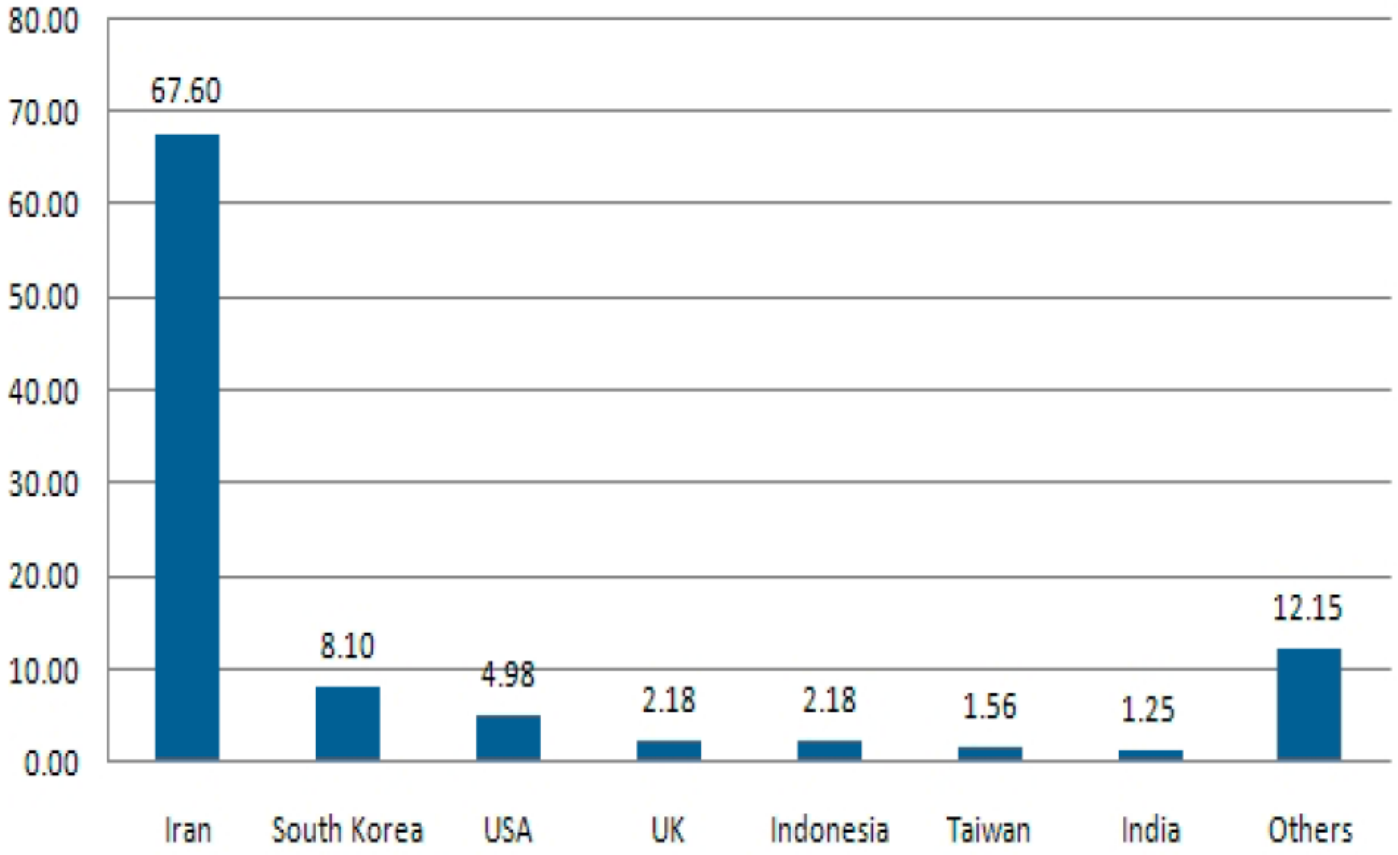
Siber Ortamlar

- Bilgiye her yerden erişilebiliyor..
- Arama motorları var..
- Sosyal ağlar..
- Sanal ortamda bir savaş var..
- İnsan beyni okunabiliyor..
- Akla hayale gelmedik yaklaşımlar geliştiriliyor..
- İzleme hat safhada..

STUXNET Neler Öğretti

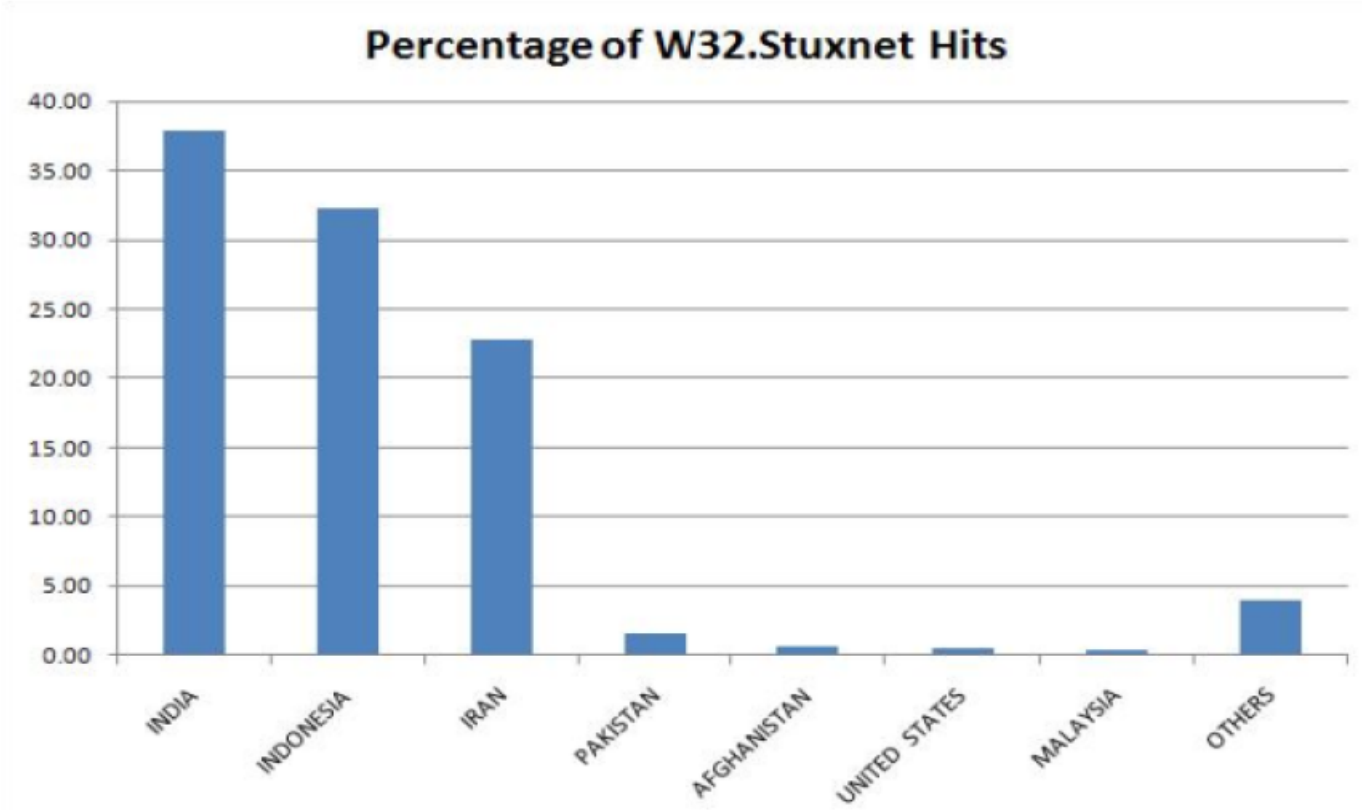
- Ezber bozan bir yaklaşım
- Altyapıya saldırı için planlanmış
- Önemli sistemlerin korunaklı olmadığı
- Kolaylıkla sistemlere zarar verilebileceği
- Bir ülkenin nükleer programını durdurabilecek kadar önemli
- Spekülasyon ile ülkelerin prestijlerine zarar verme

Etkilenen Sistemler



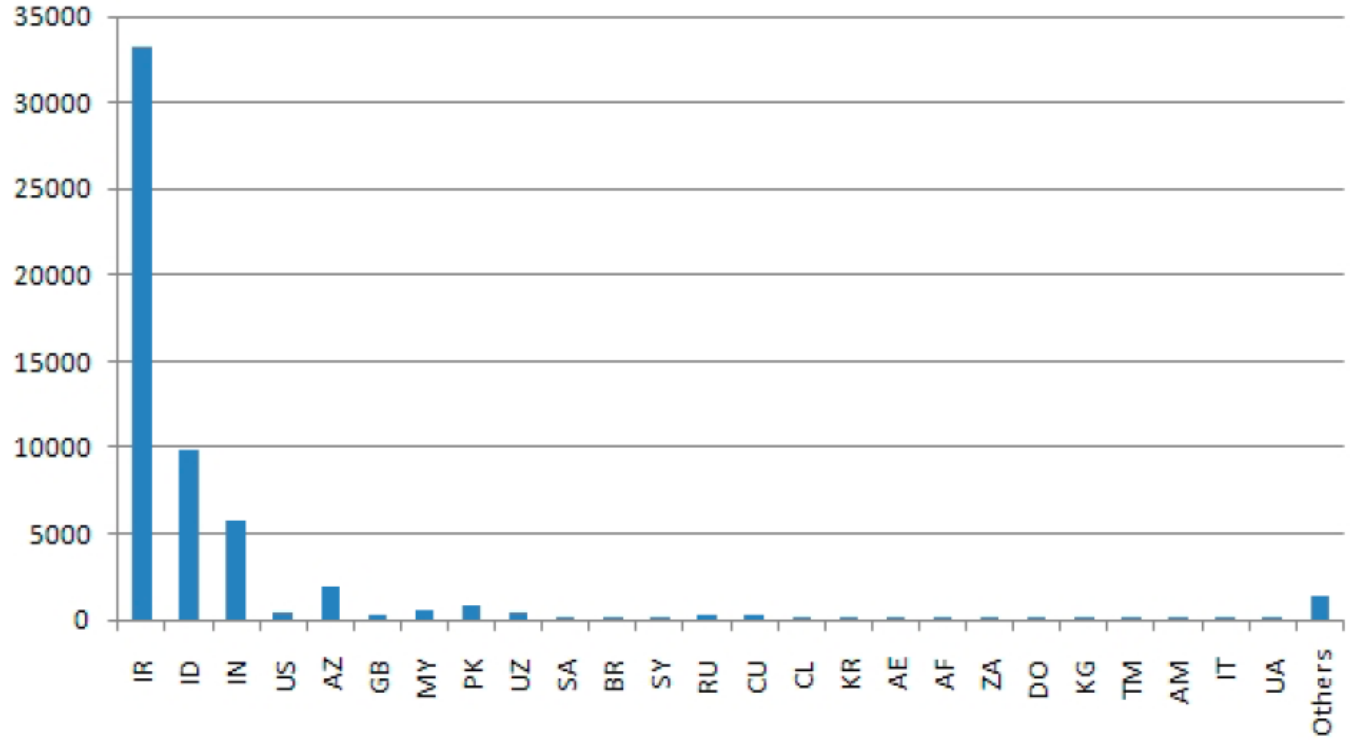
Etkilenen Sistemler

- USB Sürücülerde Yayılma

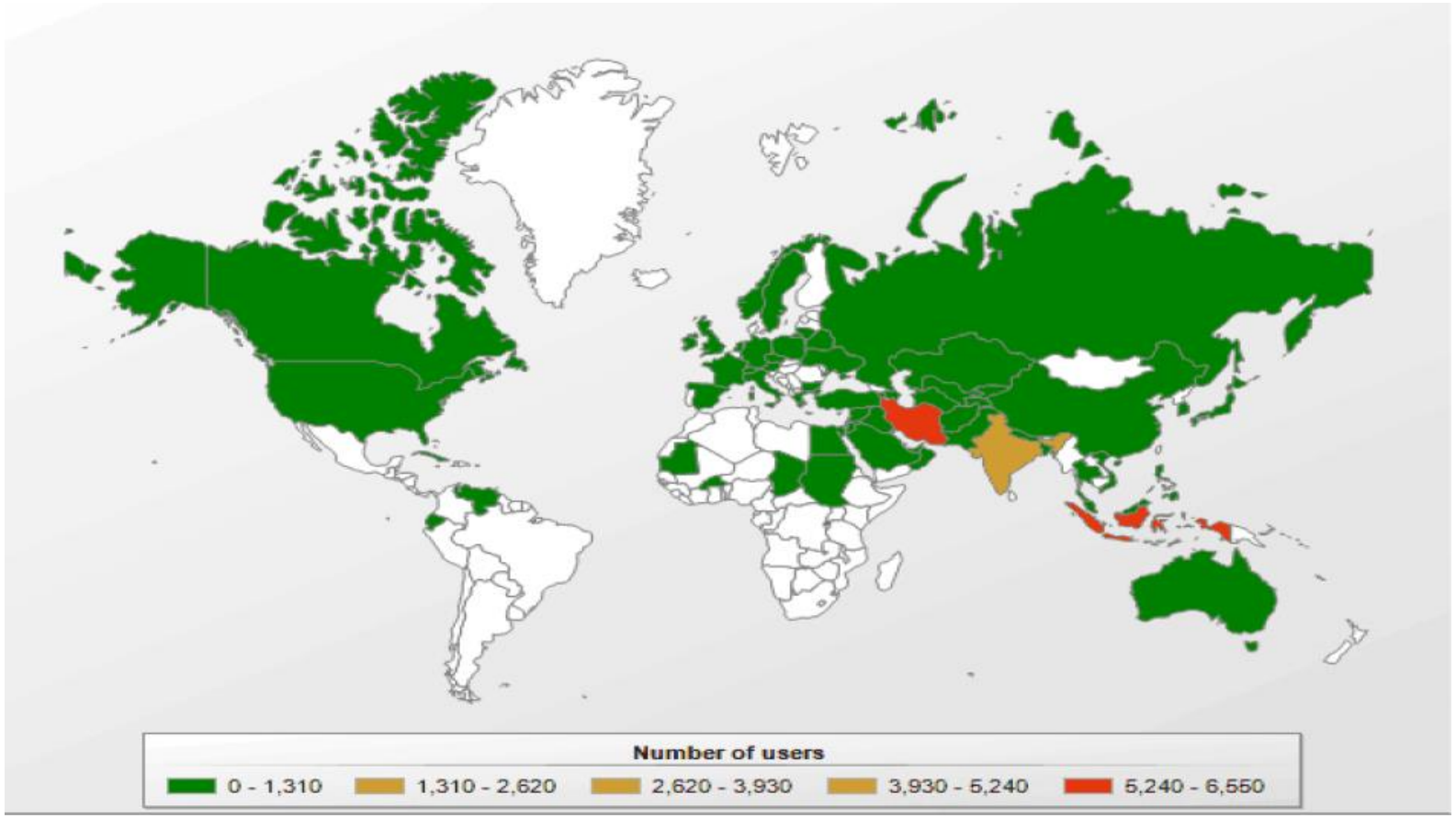


Etkilenen Organizasyonlar

- WAN IP



Stuxnet’den Dünya Çapında Etkilenme



Siber Tehditlerin Amaçları

- Sisteme yetkisiz erişim
- Sistemin bozulması
- Hizmetlerin engellenmesi
- Bilgilerin
  - Değiştirilmesi
  - Yok edilmesi
  - İfşa edilmesi
  - Çalınması

Siber Ortamlar

İyilerin ve Kötülerin amansız savaşı

- Saldıran Taraf
- Savunan Taraf

Siber Ortamlar

- **Saldıran Taraf**
  - Saldırılar artmakta
  - Saldırı bilgi seviyesi hızla azalmakta
  - Kötücül kodlar gelişerek ve değişerek hızla yayılmakta
  - Organize sanal suç örgütlerini kurma
  - İyilerden hep bir adım önde

Siber Ortamlar

Savunan Taraf

- Güvenliğin en zayıf halkası
- Bilgisizlik, ilgisizlik, hafife alma,
- %100 Güvenliğin sağlanamaması **%99,9 Korunma + %0,1 Korunmasızlık=%100 güvensizlik**
- Bilgi birikimi (Yatırım, Eğitim ve zaman)
- Kişilere güven duygusu
- E-dünyanın doğasında olan güvensizlik

Siber Ortamlar

Siber Bilgi Güvenliği ?

- Üretim
- Erişim
- İşleme
- Depolama
- Aktarma
- Yok etme

Siber Güvenlik Kültürünün Oluşturulması

Bireysel Stratejiler

- Tehlikelerin farkında olmak
- Çok katmanlı bir savunma mekanizması oluşturmak
  - Çoklu araçlar
  - Yama programları
  - Güncellemeler
- Sosyal medyada gizlilik seçeneklerini iyi değerlendirmek
- Verilerinizin nerede olduğundan emin olun
- Kötü çocuk gibi düşünün
- Çocukların erişilebilirliğini sınırlayın

CIA

- Confidentiality – Gizlilik
  - Bilgi ne anlama geliyor
- Integrity – Bütünlük
  - Değişim olmadığı doğrulanabiliyor mu?
- Availability – Geçerlilik
  - İhtiyaç duyulduğunda bilgiye erişilebiliyor mu ?

<u>Ek özellikler</u>

- Non-repudiation – İnkar edememe
- Authentication -Yetkilendirme

Sonuç

- Bilgi Güvenliği **ürün veya hizmet değildir.**
- İnsan faktörü, teknoloji ve eğitim unsurları üçgeninde **yönetilmesi zorunlu olan karmaşık süreçlerden oluşan, süreklilik arz eden bir süreçtir.**
- Üç unsur arasında tamamlayıcılık olmadığı sürece **yüksek seviyede bir güvenlikten bahsedebilmek mümkün değildir.**
- Yüksek seviyede E-Devlet güvenliğinden bahsedebilmek için **Kurumsal ve Bireysel anlamda Bilgi Güvenliğinin gerekleri yerine getirilmelidir.**