**Hafta:1 Kavramlar:**

Bilgi: Kişi ya da kurumlar için kıymet teşkil eden ve korunması gereken bir metadır.

Gerçeklik: Doğada hazır bulunan her şey.

Veri: Bir durum hakkında birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca sayısal ortamlarda bulunan ve taşınan sinyaller olarak tanımlanır.

Bilgi: Veri’nin anlam ifade edecek şekilde düzenlenmesidir.

Özbilgi: Tecrübe öğrenme veya iç gözlem şeklinde elde edilen gerçeklerin ve doğruların veya bilginin farkında olunması ve anlaşılmasıdır. (KAVRAYIŞ)

Sıcaklık gerçeklik derece veri sıcaklığın el yakması bilgi sıcak bir şeye dokunarak elinin yanmasını hissetmek özbilgi.

Hikmet: Özbilginin nasıl kullanılacağını kavramak.

Bilgi Güvenliği: Bilginin bir varlık olarak hasarlardan korunması, doğru teknoloji ve araçlarla doğru şekilde bilginin her türlü ortamda istenmeyen kişiler tarafından elde edilmesini önlemektir.

Biometrik Korunma Yolları: Parmak izi ile çalışan sistemler, ses tanıma sistemleri, dijital imza, gözün retina ve iris tabakasından yararlanarak çalışan sistemler.

Bilgi Güvenliği Sertifikası: TS ISO / IEC 27001 sertifikası denir:

Bilgi Güvenliği:

Gizliliğin Korunması:sadece yetkili kişilerce ulaşılır.

Bütünlük: Eksizsiz

Ulaşılabilirlik: Gereken durumlarda ulaşabilirim

Kötücül Yazılım: Malware-Malicious Software Bulaştığı bilgisayar sisteminde veya ağ üzerindeli diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış yazılımların genel adıdır.

Kötücül Yazılım Türleri:

Virüsler: En tehlikeli: Win32/Ska, Laroux, Marker , Ethan , Class , Win32 / Pretty

Truva Atları (Trojens)

Arka Kapılar (Back Doors)

Tarayıcı Soyma (browser hjacking)

Korunmasızlık Sömürücüleri (Exploit)

Solucanlar (Worms)

Casus Yazılım (Spyware)

Klavye Dinleme (Keylogger)

Kök Kullanıcı Takımları (Rootkits)

Tavşanlar(Wabbits)

KÖTÜCÜL YAZILIM TÜRLERİ:

Phishing (Sazan Avlama) , Koklayıcı (Sniffing), Kandırıcı (spoofer) ,Şifre kırıcılar (password cracker) , reklam Yazılımı (adware), ağ taşkını (flooder)

KÖTÜCÜL YAZILIMLARDAN KORUNMA:

İşletim sistemlerini güncel tut

Anti-spyware (Casus karşı yazılım)

Host bloklama

E-posta kontrölü

Browser kullanımı

Ofis Programları

Firewall

BİLİŞİM: Elektronik cihazlar yardımıyla bilgilerin işlenmesidir.

Telekomünikasyon, ağ haberleşme, uydu vb.

BİLİŞİM SUÇU: Bilişim yolları kullanılarak işlenilen suçlar.

İnsanlar neden bilişim suçu işler ? ► Maddi kazançi itibar düşürmek, intikam, sosyal hayat yerine sanal hayat, zevk

DELİLLENDİRME: Bir suç ile o suçun kim tarafından işlendiğini ispat edici nitelikleri yetkili mercilere sunma.

DİJİTAL DELİL:

Sanal ortamlardaki suçluların tespiti için bulunan deliller. Elektronik ve manyetik iletilen veya kaydedilen veriler. Ör: Parmak izi, DNA,

DİJİTA DELİL SORUNLARI:

1. Bütünlük
2. Doğrulanması
3. İnkar Edilememesi
4. Doğruluğu
5. Sonradan ele alınabilirliği

DİJİTAL DELİL TİPLERİ:

1. Veri dosyaları
2. Silinmiş dosyalar
3. Kayıp alanlardan gelen verilerl
4. Dijital foto ve video
5. Sunucu kayıtları
6. E-posta
7. Chat kayıtları
8. İnternet geçmişi
9. Web sayfaları
10. Log

UÇUÇU VERİLER:

1. CPU Kaydedicileri
2. Yazıcı bilgileri
3. Bellek içeriği
4. Yedeklenen veya ayrılabilen medya içeriği
5. Sürücü içeriği
6. Sürücü durumu
7. Ağ bağlantı durumu

DİJİTAL SALDIRI:

Bilgiyi bozmak, çalmak, sızdırmak veya bilişim sistemindeki donanım ve yazılımlara zarar vermeye çalışmak. Aktif veya pasif olabilir.

PASİF SALDIRI:

Saldırgan taraf pasif kalıyor ve sadece sistemi gözetliyor. Mesaj içeriği okumak

AKTİF SALDIRI:

Saldırgan baya aktif.

Türleri:

1. Rol Yapma (sniffer olayı, IP aldatmacası)
2. Eski mesajların tekrarlanması
3. Aktarılan mesajı değiştirme
4. Hizmet dışı bırakma , engelleme.

HACKER:

Kültür ve bilgi düzeyi yüksek, programlama bilen ve bir işletim sistemini hatmetmiş kişilerdir.

HACKİNG:

Bir sisteme sızma ya da zarar verme.

CRACKER:

Bilgisayar uygulamarını kıran kişiler.

LAMER:

Küçük yaşta ve hacker özentisi kişiler.

Script Kiddie: Lamer’ın bir tık üstü , az bilgisi var.

SİBER:

Bilgisayar ağlarına ait olan, internete ait olan.

SİBER ALAN:

Soyut olarak iletişim kurulan sistemler. İnternet = siber alem=siber alan

SİBER ZORBALIK:

Bilgi iletişim teknolojilerini kullanarak bir birey veya gruba zarar verme davranışlarının tümüdür.

ELEKTORNİK ZORBALIK: Kişilerin şifrelerini ele geçirme, web sitelerini hackeleme, spam içeren e-postalar.

ELEKTRONİK İLETİŞİM ZORBALOIĞI: Alay etme, isim takma, dedikodu, hakaret , fotoğgra fyayınlama.

SİBER SALDIRI:

Bilgi sistemleri doğrultusunda elektronik araçların ve bilgisayar programlarının kullanılarak ulusal denge ve çıkarların tahrip edilmesini amaçlayan kişisel ve politik olarak motive olmuş amaçlı eylem ve etkinliklerdir.

SİBER TEROR:

SİBER ORDULAR:

SİBER AHLAK:

Adli: Adalatle ilgili , adalate intikal eden olay.

Adli: Computer Forensics

ADLİ BİLİŞİM SAFHALARI:

1. Toplama(Collection)
2. İnceleme (Examination)
3. Çözümleme (Analysis)
4. Raporlama (Reporting)

**Hafta:2 Kavramlar: SİBER BİLGİ GÜVENLİĞİ**

SİBER GÜVENLİK:

Kurum kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler, politikalar, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler ve kullanılan teknoloji bütünü.

BİLGİ: Bir konu hakkında belirsizliği azaltan kaynaktır (Shannon) Veri-Data, Bilgi-Information, Özbilgi- knowledge

DATA:Datum-vermeye cesaret etmek , verilen şey Öklid

GERÇEKLİK-VERİ – ÖLÇÜM

VERİ-BİLGİ – İSPAT

KAVRAYIŞ- BİLGİ-ÖZBİLGİ

GÜVENLİK: Karşılaşılacak tehditlere karşı önlem alma.

BİLGİ GÜVENLİĞİ: 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.

15 Kasım 1940 500 savaş uçağı İngiliz coventry şehrini bombaladı

Kod adı “ay ışığı sonatı”

Enigma kullanılarak şifrelendi.

SİBER ORTAMLAR:

W32/STUXNET – Dev bir virüs. En çok etkilenen Iran oldu. En çok hindistanda yayıldı.

SİBER TEHDİT AMAÇLARI:

Sisteme yetkisiz erişim

Sistemi bozmak

Hizmet engellemek

Bilgiyi değiştirmek, bozmak , yok etmek, çalmak, ifşa etmek.

Confidentiality ► Gizlilik

Integrity ► bütünlük

Availibity ► mevcudiyet- ulaşılabilirlik, geçerlilik

Non-Repudiation ► inkar edememe

Authenntication ► yetkilendirme

**Hafta:3 Kavramlar: GÜVENLİK VE HACKİNG**

Bilişim suçları her yıl 2 kat artıyor.

NE YAPABİLİRİZ?

Şifre güvenliği

e-postalara tıklama

istek ve aktivitelere katılma

gerçek bilgileri paylaşma

birden fazla e-posta ve şifre kullan

WLM-2011 programı ile bilgisayarı güvenilen bilgisayar seçmek.

Dünyada bilişim suçları en çok hangi ülkede işleniyor?

Brezilya ,Rusya,Türkiye

PHREAKERS: Santral ve telefon hatlarını açıkların kullanan hacker

KEVIN DAVID MITNICT : Bilgisayar korsanı

DENNIS RITCHIE : c ve c++

SOSYAL MÜHENDİSLİK ÖRNEKLERİ:

Sahte mail

Web sitesi benzeri web site

Reklam tıkla kazan

Firma yetkilisiyim kardeşim açar mısın?

**Hafta:4 Kavramlar: GÜVENLİK VE HACKİNG**

Wireshark

Wimax

İşletim sistemleri

WIRESHAR : 1998 – Ethereal adıyla başladı.

Bir paketi yakalar ve içeriğini görüntüler. TCP/IP mesajlarını analiz eder.

KULLANIM YERLERİ:

1. Şebeke problemlerini giderme
2. Güvenlik probmelmerlini sınamak
3. Protokellerde oluşan hataları çzöek
4. Ağ problemlerini düzeltmek
5. Ağ trafiği
6. Veri madenciliği
7. Saldırı tespiti
8. Port tarama tespiti
9. Dos ataklarını bulma (Denial of service)
10. Bağlantı sorun tespiti
11. Casus yazılım tespiti

Tutulan bilgiler kayıt edilebilir.

No: Paket numaras

Time : Paketin zaman damgası

Source Pkaetin nereden geldiğini gösterir.

Destination: Paketin nereye gittiğini gösterir

Protocol: Protokol isminin kısa versiyonudur.

Info: Paket içeriği hakkında bilgi verir.

WİRESHARK ARAYÜZÜNÜN NASIL OLDUĞUNU ANLATTI:

İEEE 802.16 : Telsiz Kentsel alan ağı standardı (1999)

Wİmax: Worldwide Interoperability for microwave Access)

Baz İstasyonu ► Kullanıcı İstasyonu Downlink

Kullanıcı İstasyonu ► Baz istasyonu uplink

Arası pmp

WİMAX GENEL OLARAK BİR TANITILDI. ES GEÇTİM:

LİNUX: 1991 Linus Torvaldas Finldandiyalı öğrenci Intel 80386

5 Ekim 1991’de Linux’un ilk sürümü yayınlandı.

Linux, OpenBSD, FreeBSD, Irix, Solaris Unix türevleridir.

LİNUX DAGİTİMLARİ: Suse, red hat, fedora , knoppix

USER APPLİCATİONS OS SERVİCES

KERNEL

HARDWARE CONTROLLERS

Hardwre- CPU, HDD, Keyboard, Mouse, Monitör, RAM

LİNUX: Birden çok kullanıcı, çok görevli, çok işlemci TCP/IP, Kabuklar

PAROLAR : /etc/passwd ► Parolanın yeri

İYİ PAROLA: İki sözcüğün arasına rakam ya da noktalama.

Seçilen cümlenin sözcüklerinin bas harfleri

MKPASSWD : Parola yapıcı

ANLPASSWD : Parola kısıtlayıcı

-rwxr-x--- 1 karin users 403 Dec 4 15.30 deneme

Karin dosyayı okur yazar yürütür

Users ise okur ve yürütür

Diğerleri bir halt yiyemez.

Tripwire paketi ile dosya değişiklik denetimi yapılmalı.

Şifreleme: PGP (Pretty Good Privacy), CFS (Cryptographic File System)

**Hafta:5 Kavramlar: Şifreleme Bilimi ve Teknikleri:**

KRİPTOGRAFİ: Bilgiyi şifreli hale dönüştürme işlemidir.

KRİPTOANALİZ: Bir şifreleme sistemini veya sadece şifreli mesajı inceleyerek, şifreli mesajın açık halini elde etmeye çalışan kriptoloji disiplinidir.

ŞİFRELEME (ENCRYPTİON): Düz metni şifreli metne çevirme sürecidir.

ŞİFRE ÇÖZME (DESCRIPTION) : Şifrelenmiş metni düz metne çevirme işlemidir.

ANAHTAR (KEY) : Şifreli metnin nasıl elde edildiğine dair kod parçasıdır.

SEZAR ŞİFRELEME: Şifrelenecek metin alfabe de kendinden sonra gelecek 3.harfle yer değiştirir.

B ►E A ►

C = P+3(MOD 29) A =0 oluyor harf sayısı mod yanında oluyor. A geldiğinde 3 ötelenecek ve d sayısına denk gelecek

PİGPEN (MASON) ŞİFRELEME: Her bir harfin bir şekilde elde edildiği bir şifreleme

ECHELON SİSTEM: Dünyanın en büyük casusluk ağı.

PROMIS: Birçok banka sisteminin kilitlenebileceği, mali krizler çıkarılabileceği, ihalalere baskın

ENIGMA: Elektromekanik bir şifre çözme makinesidir.

1919 yılında balmanlar tarafından kullanıldı

RESİM : Dosya başlığı (Header) ve piksellerden oluşur.

Her piksel renk içeren bloktur.

Her piksel 3 renkten oluşur. 3 byte yer kaplar.

800\*600 ebat resim 480.000 adet piksel barındırı = 1.440.000

HASH : Büyük tanım bölgelerini küçük bölgere dönüştürülür. Keyfi sonlu boyutlu bit şeritleri n-bit diyebileceğimiz sabit uzunluklu şeritlere dönüştürür.

MESAJ ÖZETİ: Hash sonucu çıkan sayısal bilgi.

BİLİNEN HASH FONKSİYONLARI: MD-4 , MD-5 ve SHA

MD5 (Message-Digest algorithm5)

Tek yönlü şifreleme. 128 bit haline getirilir.

SHA-1 (Secure Hash Algorithm)

Tek yönlü. Verileri 160 bit uzunluğunda özetler.

SHA-2 (224,256,384,512) bit uzunluğu

DES (Data Encryptipn Standard) ► Veri şifreleme standardi

DEA (Data encryption Algorithm)► Veri şifreleme algoritması

RSA (Açık Anahtar Algoritması): 1978 ► Ron Rivest Adi Shamir Leonard Adleman

* İki farklı asal asyı seç p=61, q=53
* N=p\*q değerini bul n = 3233
* Totient hesapla = (61-1)\*(53-1) = 3120
* 1 ile 3120 arasında 3120 ile aralarında asal bir sayı seç e = 17
* D değeri 3’nin mod(3120)’e göre çarpmaya göre tersi olarak hesaplayalım.
* Ortak Anahtar = n=3233, e=17
* M şifrele = m^17(mod 3233)
* M çöz c^2753(mod 3233)

BİTLOCKER: Windows 7 ile gelen sürücü şifreleme özelliği.

WEP (Wired Equivalent Privacy) Kablosuz Ağ veri bağ tabakası şifreleme yöntemidir.

WEP-64 ► 40 bit kullanır.

WEP-128 ► 104 bit kullanır

WEP-256 ► 232 bit kullanır.

WPA (Wi-fi Protected Access)

WPA- PSK (Paylaşımlı Mod)

WPA BİRAZ DERİNE GİRDİ: BAKARSIN

**Hafta:6 Kavramlar: STEGANOGRAFİ:**

WPA BİRAZ DERİNE GİRDİ: BAKARSIN

ENCAPSULATION : (Kapsülleme): Bir modülün yaptığı işlemlerin bir kısmını, bu işlemleri nasıl gerçekleştirdiği bilgisini dışarıdan bilinçli olarak saklamaktır.

Amacı, bilgiyi saklamak değil gerek erişimi öncelemek ve dış öğeleri içeriğe standart, önceden tanımlı arayüzler aracılığıyla ulaşıma zorlamaktır.

GİZLİ KANALLAR

* İletimimizdeki veriyi saklamaya çalışmak
* İletişimin amacını saklamak
* Veri transferi dikkatsiz kişilerce doğruymuş gibi gelecektir.
* Veriyi karıştırmak için ek şifreye gerek yoktur.
* Kullanım alanlar:
  + Dosya tabanlı steganografi – görüntü ses ve text
  + Ağ paket steganogrofisi
  + Protokol kapsüllenmes – ssl(Secure Sockets Layer) ssh (Secure Shell)

STEGANOGRAFI

* Bir nesnenin içerisine bir verinin gizlenmesi

COVER-DATA (örtü-verisi): Bilgi gizlenen ortam

STEGO-KEY: Bilginin saklanması işlemini kontrol etmek için ve gömülü bilginin elde edilmesini zorlaştırmak için kullanılır.

STEGO-TEXT-STEGO-OBJECT : Bilgi ile birlitek olan ortam

DİL-BİLİM STEGANOGRAF : Text ile verinin taşındığı tip.

* Text üzerinde değişiklikler yapılarak veri gizlenir.
* Grafix kullanılabilri
* Text yapısı değiştirilir
* Yada amacı saadece gizleme olan text yazılır.

TEKNİK STEGANOGRAFİ : Görünmüz mürekkep, Gizli yerler, Microdot, Bilgisayar tabanlı yöntemler.

METİN STEGANOGRAFİ:

* Taşıyıcı ortam metindir.
* Uygulaması zor
* Saklanacak veri az
* Metin tabanlı sistemler ya orijinal metne ya da biçimlendirmesine ihtiyaç duyar

Açık Alan Yöntemleri:

1. Cümle İçi boşluk bırakma: Tek boşluk ► 0 Çift boşluk ► 1
2. Satır Kaydırma : satırlar yukarı kaydırılır düşey olarak bitmap dosya olarak açılabilir.
3. Satır Sonu boşlukları: İki boşluk bir bit dört boşluk iki bit sekiz boşluk dört bit gizler.
4. Sağ hizalama: Kelimeler arası boşluklar
5. Gelecek Kodlaması: Bazı harflerin boyları değiştirilir.

Yazılımsal Yöntemler:

*Noktalama işaretleri kullanılır.*

Anlamsal Yöntemler:

* w.Bender tarafından atıldı
* Eş anlamlı kelimeler kullanılır.

GÖRÜNTÜ STEGANOGRAFİ:

1. En önemsiz bite ekleme ► 0-255 arasında 1 byte ile gray skala elde edilir. Renkli görüntüler 24 bit ya da 8 bit olabilir. 24 bitli grüntü bir piksel başına 3 byte kullanır. Kırmızı Mavi , Yeşil. Her byte için son biti değiştir. 8 bitlik görüntü piksel başına 1 byte kullanır. Pek iyi değiş.
2. Maskeleme Filtreleme : 24 bit ve gri seviye için kullanılıyor.
3. Algoritmalar ve Dönüşümler: JPEG ► ksteg , STEGO ► dost , Picture ► Mark, SureSign, S-tools

GERÇEK KİMLİĞİ SAKLAMA

* Veri gönderimi sırasında gerçek kimlik saklanarak ta bilginin bilinmeyen ya da anlaşılamayan biri üzerinden gidiyor izlenimi verilerek te bilgi zarar görmeden gönderilebilmektedir.

**Hafta-7 Kavramlar: Yazılım Güvenliği**

PROGRAM: Bilgisayarları çalıştırmak için ihtiyaç duyulan kod yığınları.

YAZILIM GÜVENLİĞİ: Yazılımların tersine mühendislik ve araçları ile algoritmalarının ortaya çıkartılmasını veya değiştirilmesini engellemeyi amaçlar.

DEBUGGER: Derlenmiş programın çalışma anında assembly kodlarına dönüştürülmesi ve üzerinde değişiklik yapılmssını sağlayan araçtır.

DİSASSEMBLER: Derlenmiş programın çalıştırıladan çözümlesinmesini sağlayan araçtır.

TEHDİT MODELLEME AMAÇ :

* Tehditlerin saptanması
* Tehditlerin hangisinin azaltılmasının gerektiğinin bulunması
* Hangi yöntemle azaltılacağının seçilmesi

NİYE TEHDİT MODELLEME?:

* Uygulamayı daha iyi anlamak (kim yönetici kim değil)
* Tehditleirn belirlenmesi
* Kod hatalarını anlamak
* Uygulamaya hızlı uyum
* Testçilerin rahatlaması

TEHDİT MODELLEME DÖNGÜSÜ:

1. Uygulamanın ayrıştırılması
2. Tehditlerin Belirlenmesi
3. Tehditlerin Derecelendirilmesi
4. Tehditlerin Azaltılması

UYGULAMANIN AYRIŞTIRILMASI:

* Uygulama alt parçalara ayrıştırılır.
* Güvenlik Çemberi, Akış diyagramı giriş noktaları, ayrıcalıklı kod parçaları belirlenir.

Güvenlik Çember:

* O çemberin içindeki bütün giriş noktaları güvenli bir şekilde korunuyordur.
* Bütün girdiler bir geçerlemeye sahiptir.

Akış Diyagramları:

* Uygulama bütünü kapsayacak şekilde akış diyagramı çizilir.
* Uygulama parçalara bölünür ve öyle çizilir.

İçerik diyagramı:

* Giriş noktalarını belirle.
* Ayrıcalıklı kod parçalarını belirle.
* Girdi geçerleme
* Kimlik denetleme
* Yetkilendirme
* Yapılandırma yönetimi
* Kritik veri

Tehditlerin Belirlenmesi:

* STRIDE sınıflandırma modeli ile tehditler sınıflandırılabilir.