**TS ISO/IEC 27001**

“Bilgi Güvenliği Yönetim Sertifikası “

* 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.

**Kötücül Yazılım(Malware)**

* Virüs
* Truva Atı(Trojan)
* Arka Kapılar(Back Door)
* Tarayıcı Soyma(Browser Hijacking)
* Korumasızlık Sömürücüleri(Exploit)
* Solucan(Worm)
* Casus Yazılım(Spyware)
* Klavye Dinleme Sistemleri(Keylogger)
* Kök Kullanıcı Takımları(Rootkits)
* Tavşanlar(Wabbits)
* Sazan Avlama(Phishing)
* Koklayıcı(Sniffer)
* Kandırıcı(Spoofer)
* Şifre Kırıcılar(Password Cracker)
* Reklam Yazılım(Adware)
* Ağ Taşkını(Flooder)

İP ve Mac Sniffing: Ağ Paketlerini dinler, Source ve Destination kontrol eder.

İP ve Mac Spoofing: Ağ Paketlerini dinler, Source ve Destination kontrol eder. Ayrıca Paketlere hedef bilgisayarın mac ve ip adresiymiş gibi sahte paketler yollar ve iletişim sağlar.

Bilgi güvenliğinin en temel unsurları şunlardır:

* Gizlilik (confidentiality),
* Kullanılabilirlik (availability),
* Kimlik kanıtlama (authentication)
* Bütünlük (integrity),
* İnkâr edememe (non-repudiation)
* Sorumluluk (accountability),
* Erişim denetimi (access control),
* Güvenilirlik (reliability)
* Emniyet (safety)

Uygulama katmanındaki güvenlik protokolleri: Kerberos, S/MIME, PGP

Ulaşım katmanındaki güvenlik protokolleri: SSL, SSH, PCT, TLS

İnternet katmanı protokolü: IPSec, IKMP

**Saldırı**

* Saldırgan
  + Solo Saldırı
  + Çoklu Saldırı
* Hedef
  + Tek Hedefli Saldırı
  + Çok Hedefli Saldırı
  + Ağ Saldırısı
* Yol
  + Doğrudan Saldırı
  + Dolaylı Saldırı
* Kasıt
  + Bilgi Hırsızlığı
  + Kaynak Yıkımı
  + Ön Saldırı
  + DoS Saldırı
* Araç
  + Yerel Saldırı
  + Uzaktan Saldırı

**İletişim Protokollerini Kullanan Saldırılar;**

* IP sahteciliği (IP Spoofing)
* TCP dizi numarası saldırısı (TCP sequence number attack)
* ICMP atakları
* Ölümcül ping
* TCP SYN seli atağı (TCP SYN Flood Atatck)
* IP parçalama saldırısı (IP Fragmentation Attack)
* Internet yönlendirme saldırısı (Internet Routing Attack)
* UDP sahteciliği ve dinleme (UDP Spoofing and Sniffing)
* UDP portunu servis dışı bırakma saldırısı (UDP port Denial of Sevice attack)
* Rastgele port taraması (Random port scanning)
* ARP saldırıları (ARP attacks)
* Ortadaki adam saldırıları

**IP Saldırıları;**

IP V4’te bulunan güvenlik eksikliklerinden faydalanılarak yapılan atak türleridir. Bazıları şunlardır.;

* Out of Band Nuke
* Land
* Teardrop
* Boink
* Smurf
* Suffer3

**Uygulama Katmanı Saldırıları**

* DNS, SMTP, NFS saldırıları
* Uzaktan giriş ile saldırılar
* URL sahteciliği
* Kötü niyetli java ve ActiveX uygulama parçacıklar
* Sistem log seli (güvenlik dosyasına çok sayıda giriş yapılarak log dosyasının dolmasına ve sistemin kapatılmasına neden olur)

**İşletim Sistemlerinin Güvenliği**

İşletim sistemleri seçilirken göz önünde bulundurulan özellikler şunlardır:

* Kurulum kolaylığı
* Donanım gereksinimleri, sürücü edinebilme
* Kullanım ve yönetim
* Güvenilirlik
* Güvenlik
* Uyumluluk
* Fiyat
* Destek

**Sistem Güvenlik Seviyeleri**

* D
  + D1: En düşük düzeyde güvenlik
* C
  + C1: İsteğe (kullanıcıya) bağlı güvenlik
  + C2: Kontrollü erişim
* B
  + B1: Etiketli güvenlik
  + B2: Yapısal güvenlik
  + B3: Güvenlik alanlı Koruma
* A
  + A1: En yüksek düzeyde güvenlik
* D seviyesi
  + D1 Seviyesi
    - Mevcut en düşük güvenlik olanaklarını sunar
    - Bu seviyede bir güvenliğe sahip sistem bütün olarak güvensizdir.
    - Donanım elemanları için herhangi bir koruma mekanizması yoktur.
    - İşletim sistemi kolaylıkla ele geçirilebilir ve istenen amaca uygun bir şekilde kullanılabilir.
    - Sistem kaynaklarına yetkili kişilerin ulaşmasını denetleyecek bir erişim kontrol sistemi yoktur.
    - MS-DOS, MS-Windows 3.1/95/98 ve Apple Macintosh bu sınıftadır.
* C
  + C1
    - Sınırlı bir güvenlik koruması vardır.
    - Daha çok kullanıcı hatalarından sistemi korumak için gerekli tanımlamaları vardır.
    - Dışarıdan gelecek saldırılara karşı koruma mekanizmaları yoktur.
    - Ayrıca donanım için bazı güvenlik mekanizmaları bulunmaktadır. Donanım elemanlarına istenmeyen kişilerin ulaşması zorlaştırılmıştır.
    - Erişim kontrolü kullanıcı adı ve parolasına göre yapılmakta ve hakkı varsa sisteme alınmaktadır.
    - UNIX ve IBM MVS (Multiple Virtual Storage) bu sınıfa örnektir.
  + C2
    - C1 seviyesine göre daha güvenli hale getirilmiştir.
    - Bu seviyede kaynaklara kontrollü erişim sağlanabilmektedir.
    - Yani erişimler için sadece geçerli haklar göz önünde bulundurulmayarak sonradan yapılan yetkilendirilmelerde kontrol edilir.
    - Bunun için de sistemde yapılan her iş için kayıt tutulur.
    - Yapılan işlemlerin kontrol edilmesi ve kayıt edilmesi C1’de ortaya çıkabilen güvenlik problemlerini ortadan kaldırmaktadır.
    - Fakat fazladan yapılan kontrol ve kayıt işlemleri işlemci zamanını harcayacak ve diskten alan alacaktır. Güvenlik arttıkça kaynaklara erişimdeki hız düşecektir.
    - Bu seviyeye örnek sistemler Windows NT 4.0 ve Digital Equipment VAX/VMS 4.x ‘tir.
* B
  + B1
    - Çok katmanlı güvenlik yapısı kurulmasını sağlar (gizli, en gizli vb.)
    - Sistemde güvenliği sağlanacak nesnelerin diğerlerinden kesinlikle ayrılması gerekmektedir bu nesneler manyetik ortamlarda saklanır.
    - Bu seviyeye örnek olarak OSF/1, AT&T V/MLS, IBM MVS/ESA sistemleri verilebilir.
  + B2
    - Bu seviyedeki güvenlik için sistemdeki tüm nesnelerin (birimlerin) etkilenmesi gerekir.
    - Disk ile saklama birimleri veya terminaller bir ve ya daha fazla olabilecek güvenlik seviyesi ile ilişkilendirilebilir.
    - Güvenlik düzeyi yüksek bir cihaz ile düşük bir cihazın haberleşmesinde problem çıkacaktır, bunlara dikkat edilmesi ve çözülmesi gereklidir.
    - Bu seviyeye örnek olarak Honeywell Information System’in Multics sistemi ve Trusted XENIX verilebilir.
  + B3
    - Güvenliği donanımların uygun kurulumlarıyla sağlamaya çalışan yöntemi içerir. B2 seviyesine göre daha sağlam ve ciddi bir sistem tasarımı vardır. Güvenlik yönetimi, güvenli kurtarma ve saldırı ya da oluşan zararların sistem yöneticisine bildirilmesi gibi özellikleri içerir.
    - Bu seviyeye örnek olarak Honeywell XTS-200 verilebilir.
* A
  + A1
    - En üst güvenliği sunan seviyedir.
    - Donanım ve yazılım açısından dizayn, kontrol ve doğrulama işlemlerini içerir.
    - Daha önce bahsedilen güvenlik seviyelerindeki tüm bileşenleri içerir.
    - Bir sistemin dizayn, geliştirme ve gerçekleştirme aşamalarında güvenlik isteklerinin sağlanması beklenir.
    - Her aşamayla ilgili olarak dokümantasyonun da yapılması gerekmektedir.

**Güvenlik Süreçleri**

* **Önleme**(prevention)

Kişisel bilgisayar güvenliği ile ilgili önlemler;

* + Virüs tarama programlarının kurulu olması, ve bu programların ve işletim sistemi hizmet paketlerinin ve hata düzeltme ve güncellemelerinin düzenli aralıklarla yapılması,
  + bilgisayarda şifre korumalı ekran koruyucu kullanılması,
  + bilgisayar başından uzun süreliğine ayrı kalındığında sistemden çıkılması,
  + kullanılan şifrelerin tahmininin zor olacak şekilde belirlenmesi, bu şifrelerin gizli tutulması ve belirli aralıklarla değiştirilmesi,
  + disk paylaşımlarında dikkatli olunması,
  + Internet üzerinden indirilen veya e-posta ile gelen dosyalara dikkat edilmesi,
  + önemli belgelerin parola ile korunması veya şifreli olarak saklanması,
  + gizli veya önemli bilgilerin e-posta, güvenlik sertifikasız siteler gibi güvenli olmayan yollarla gönderilmemesi,
  + kullanılmadığı zaman İnternet erişiminin kapatılması,
  + önemli bilgi ve belgelerin düzenli aralıklarla yedeklerinin alınması

Kurumsal ortamlarda bilgisayar güvenliğinde uygulanması gereken önlemler;

* + İşletim sistemi ve yazılımların servis paketlerinin ve güncellemelerin düzenli aralıklarla incelenmesi,
  + Kullanıcı haklarının asgari seviyede tutulması, kullanılmayan protokol, servis, bileşen ve proseslerin çalıştırılmaması,
  + Veri iletişiminde şifreleme tekniklerinin, korunmasızlık tarayıcıları, Sanal Özel Ağ (Virtual Private Network) kullanılması,
  + Açık Anahtar Altyapısı (Public Key Infrastructure) ve e-imza kullanımı
  + Biometrik tabanlı sistemlerin kullanımı olarak sıralanabilirler.
* **Saptama**(detection)

Saptama sürecinde kullanılan yöntemlerden bazıları şunlardır:

* Güvenlik duvarları n Saldırı tespit sistemleri (intrusion detection system)
* Ağ trafiği izleyiciler
* Kapı (port) tarayıcılar
* Gerçek zamanlı koruma sağlayan karsı virüs ve casus yazılım araçları
* Dosya sağlama toplamı (checksum) kontrol programları
* Ağ yoklayıcı (sniffer) algılayıcıları
* **Karşılık Verme** (response ya da reaction)
  + Karşılık verme, önleme süreci ile baş edilemeyen ve saptama süreçleri ile belirlenmiş saldırı girişimlerini, mümkünse anında veya en kısa zamanda cevap verecek eylemlerin ifa edilmesi olarak tanımlanabilir.
  + Hızlı karşılık verme, bu saldırıları püskürtmek için güvenlik sistemini tamamlayan esaslı bir öğe olarak ortaya çıkmaktadır.
  + Saldırı tespit sistemleri, bu tespite cevap verecek birilerinin veya bir sistemin olması ile anlam kazanabilir. Aksi takdirde bu durum, hiç kimsenin duyup da önemsemediği bir araba alarmının getireceği faydadan öteye gitmez.
  + Saldırı tam olarak önlenmese bile; sistemin normal durumuna dönmesine, saldırıya sebep olan nedenlerin belirlenmesine, gerektiği durumlarda saldırganın yakalanmasına, güvenlik sistemi açıklarının belirlenmesine ve önleme, saptama ve karşılık verme süreçlerinin yeniden düzenlenmesine olanak verir.
  + Saldırı tespit edilince yapılması gereken işlerin, daha önceden iyi bir şekilde planlanması, bu sürecin etkin bir şekilde işlemesini ve zaman ve para kaybetmemeyi sağlayacaktır.
  + Yıkım onarımı (disaster recovery), bu aşama için gerçekleştirilen ve en kötü durumu ele alan esaslı planların başında gelir.

**Güvenlik Duvarları (Firewall)**

Bir güvenlik duvarı, bilgisayara ve ağa veri geçişini denetleyen, belirli kriterlere uymayan paketleri geçirmeyen bir yazılım programı veya donanım parçasıdır.

3’e ayrılırlar:

* **Paket Filtreleyici Güvenlik Duvarları (Packet Filtering Firewalls)**

Gelen IP paketlerinin iletilip iletilmeyeceğine daha önceden belirlenmiş bir takım kurallara göre karar veren çok portlu bir araçtır. Bu güvenlik duvarları, üzerlerinden geçen paketleri incelerler ve bunları verinin kaynağına, hedefine, kaynak ve hedef portuna bağlı olarak çeşitli kurallarla karşılaştırırlar. Bu güvenlik duvarları ile bilgilerin belirli türlerini engellemek, iyi bilinen portları kapatmakla kolayca yapılabilir. Bu güvenlik duvarları verinin içeriğine bakmazlar.

Sadece şu bilgilere göre filtreleme yaparlar:

* + Kaynak ve hedef IP adresleri
  + Kaynak ve hedef port numaraları
  + TCP bağlantı bayrakları

Stateful inspection; Checkpoint Software Technologies tarafından bulunmuştur. Eski IP paketlerine ait bilgiler saklanır. Arkadan gelen paketler daha hızlı geçerler.

Dezavantajları;

* + Sistem yöneticisinin saldırıları anlamasına yardımcı olabilecek kayıt tutma (logging) kabiliyeti çok azdır.
  + Paket filtreleme kuralları doğrudan test edilmek için zordurlar. Dolayısıyla, test edilemeyen açık noktalar kalabilmektedir.
  + Eğer karışık filtreleme kuralları gerekirse bunlar yönetilemez bir hale gelebilirler
* **Devre Düzeyinde Güvenlik Duvarları (CircuitLevel Firewalls)**

Bu tip güvenlik duvarları, dışarıdan bilgi akışına sadece içerideki bilgisayarlardan istek geldiğinde izin verir. Dışarıya giden isteklerin kaydı tutulur ve sadece isteğe karşılık gelen cevaba izin verilir. Bu tip bir güvenlik duvarının en önemli avantajlarından biri, dışarıdakilerin bütün bir ağı sadece güvenlik duvarının adresi olarak görmesidir. Böylelikle, ağın gerisi korunmuş olur. Güvenlik duvarı açana kadar bütün portlar kapalıdır. Ana dezavantajı ise, diğer filtreleme yöntemleriyle birleştirilmediği takdirde içeriden gelen herhangi bir veri isteğine izin vermesidir. Kablo/DSL yönlendiricileri bu yöntemi birincil olarak kullanırlar. Daha belirgin olarak, bunlar internet paylaşımlı devre düzeyinde ağ geçitlerinin bir kombinasyonu olan NAT (Network Address Translation) kullanırlar. Devre düzeyinde ağ geçitleri arasında SOCKS yaygın olarak kullanılmaktadır

**SOCKS**

İstemci yazılımına ve/veya TCP/IP yığınına modifikasyon gerektirir. İki parçadan oluşur;

* SOCKS sunucusu (daemon)

SOCKS sunucusu uygulama katmanında çalışır. SOCKS istemcisi uygulama ve ulaşım katmanları arasında çalışır

* SOCKS istemcisi (kütüphanesi).
* **Uygulama Düzeyinde Güvenlik Duvarları veya Vekil Sunucular (Application-Level Firewalls or Proxy Servers)**
  + “Proxy” olarak da anılan bu güvenlik duvarları, devre düzeyindekilere benzer şekilde, ağa giriş ve çıkış için tek geçiş olarak davranırlar.
  + En önemli fark ise bilgiyi ele alış şekillerindedir.
  + Devre düzeyindeki güvenlik duvarları adres ve port bilgisine bakarken, bu güvenlik duvarları daha detaylı olarak inceler ve içeriğe bakar.
  + Bu yöntemi kullanan güvenlik duvarları, yaygın veri türlerinin güvenlik duvarından geçmesine izin vermeden önce proxy uygulamaları çalıştırırlar.
  + Bunun iki önemli avantajı vardır;
    - İlki, dış kaynaklar güvenlik duvarı arkasındaki bilgisayarlar arasında doğrudan bağlantıya izin vermemesi,
    - Diğeri ise verinin içeriğine bakılarak filtreleme yapılabilmesidir.
  + Uygulama düzeyindeki güvenlik duvarları sundukları kontrol düzeyleri nedeniyle çok güvenlidirler fakat önemli konfigürasyon gereksinimleri vardır.
  + Ayrıca, paketleri geçirmekte de, çalışan proxy uygulamaları nedeniyle, diğer güvenlik duvarlarına göre yavaştırlar.
  + İstemci bilgisayarlara da dışarıdaki kaynaklara erişim için ayrıca proxy konfigürasyonları yapılması gerekir.
  + Kullanıcı asıllama ve yetkilendirmesi yapılır
  + Kullanıcı asıllama için gerekli bilgiler başka bir güvenlik sunucusunda tutulabilir
  + Bunun için en çok kullanılan protokoller;
    - Livingston Enterprises firmasına ait olan RADIUS
    - Cisco firmasına ait olan TACACS
  + Bir sunucuya bağlanmadan önce uygulama düzeyinde bir ağ geçidine bağlanmak işlemi saydamlaştırılabilir. Buna “saydam vekillik (transparent proxy)” denir
  + Bu güvenlik duvarları da devre düzeyindeki güvenlik duvarları gibi internet paylaşımı ile bütünleşmiştir
  + Bu tip güvenlik duvarları genellikle büyük bilgisayar ağlarını korumak için iş amaçlı kullanılmaktadırlar.
* **Güvenlik Duvarı Konfigürasyonları**
  + En yaygın kullanılan:
    - Çift-Evli Güvenlik Duvarları (Dual-Homed Firewalls)
    - Perdelenmiş Alt Ağ Güvenlik Duvarı (Screened Subnet Firewall)
* **Özet**
  + Paket filtreleyici güvenlik duvarları basit bir güvenlik çözümü sağlarlar ve paketlerdeki verinin içeriğine bakmazlar
  + Devre düzeyindeki güvenlik duvarları dışarıdan gelen paketler için tek giriş noktasıdır. Dışarıdaki bilgisayarlar sadece bunun adresini bilirler. Böylelikle, arkasındaki ağı güvenli bir şekilde korur. Ayrıca, asıllama ve yetkilendirme de yapılır. Burada da verinin içeriğine bakılmaz
  + Uygulama düzeyindeki güvenlik duvarları ise bilginin içeriğine bakarak paketi geçirip geçirmeyeceğine karar verir. Asıllama ve yetkilendirme mekanizmaları kullanır.
  + Çift-evli güvenlik duvarları daha güvenli bir yapı sunarken performans ve esneklik bakımından perdelenmiş alt ağ güvenlik duvarlarından daha düşük seviyededirler.

**Şifreleme Bilimi ve 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.
* Sezar
  + Şifrelenecek metin alfabede kendinden sonra gelecek 3. harfle yer değiştirerek oluşturulmaktadır.
* Pigpen
* Ebced
* Enigma
* Echelon
* Steganografi
* MD5
* RSA
* SHA1
* SHA2

**Bilgi Gizleme**

* Gizli Kanallar (Covert Channels)

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

* Steganografi (Steganography)
  + Dilbilim Steganografi (Linguistic Steganography )

Burada veriyi gizlemek için text üzerinde değişiklikler yapılmaktadır. Bunlardan bazıları; grafik kullanılarak yapılabilir, text’in yapısı değiştirilerek yapılabilir yada amacı sadece veriyi saklamak olan yeni bir text yaratılabilir.

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.

* + Teknik Steganografi (Tehnical Steganography)
* Gerçek Kimliği Saklama (Anonymity)
* Telif hakkı İşaretlemesi (Copyright marking)
  + Güçlü Telif hakkı İşaretlemesi (Robust Copyright Marking)
    - Parmak İzi (Fingerprinting)
    - Filigran (Watermarking)
      * Farkedilemez Filigran (Imperceptible Watermarking)
      * Görünür Filigran (Visible Watermarking)
  + Kolay İşaretleme (Fragile Watermarking)

**Tehdit Modelleme**

**Faydaları;**

**Uygulamanın daha iyi anlaşılması**: Uygulamanızın özelliklerinin analizi için zaman harcamak zorunda kalmanız, uygulamanızın ve parçalarının nasıl çalıştığı konusunda size daha geniş bir bakış açısı sağlayacaktır.

**Tehditlerin belirlenmesi:** Herhangi bir yazılımsal süreç başlamadan, başka bir deyişle uygulama kodlanmaya başlamadan, sisteminizi ilgilendiren tehditlerin belirlenmesini sağlayacaktır.

**Kod hatalarının kolayca belirlenmesi:** Kod hatalarının birçoğu tehdit modellemede ortaya çıkacaktır.

**Proje takımının yeni üyelerinin uygulamaya uyumu:** Yeni işe başlayan birinin yüzde yüz performansla çalışmaya başlaması ve proje takımına uyum sağlaması için her zaman belirli bir sürenin geçmesi gerekmektedir. Tehdit modellemenin bütün uygulamayı gösterecek sistemli ve yapısal bir modelleme olması, yeni işe başlayan çalışanların uygulamayı hızlı bir şekilde öğrenmesini sağlayacaktır.

**Testçiler için faydaları:** Testçilere hangi tehditlere göre test araçları hazırlamaları gerektiği hususunda katkı sağlayacaktır.

**Diğer proje takımları için faydaları:** Sizin ürününüzle alakalı proje geliştiren diğer ürün geliştirme takımları, sizin oluşturduğunuz tehdit modellemeyi incelemelidirler. Bu sayede, diğer takımlar yeni bir tehdit modelleme oluşturmak zorunda kalmayacaktır ve uygulamanın tümünü görmek manasında proje hız kazanacaktır.

**Modelleme Döngüsü;**

* Uygulamanın Ayrıştırılması
  + Girdi Geçerleme
    - §Uygulamanız kapsamındaki bütün girdiler geçerlendi mi?
    - Saldırgan uygulamanıza kötü niyetli veri enjekte edebilir mi?
    - Veri ayrı güvenlik çemberlerinden geçerken, geçerlemeye tabi tutuluyor mu?
    - Veri tabanındaki veri güvenilir mi?
  + Kimlik Denetleme
    - Şifre ve kullanıcı gibi gizli veriler ağ üzerinden geçerken güvenliği sağlanıyor mu?
    - Sıkı kullanıcı hesabı politikaları kullanılıyor mu?
    - Kullanıcılar güvenlik düzeyi yüksek şifre almaya zorlanıyorlar mı?
    - Kullanıcı şifreleri için şifre doğrulama uygulamaları kullanılıyor mu?
  + Yetkilendirme
    - Giriş noktaları için hangi önlemler alındı?
    - Veri tabanında yetkilendirme nasıl şart koşuluyor?
    - Bağlantı kopmasında ya da hata anında uygulama güvenliği sağlanıyor mu?
  + Yapılandırma Yönetimi
    - Uygulamanız hangi yönetimsel arayüzleri içeriyor?
    - Bu arayüzlerin güvenliği nasıl sağlanıyor?
    - Uzaktan yönetici yetkilendirmesi nasıl yapılıyor?
    - Hangi yapılandırma bilgileri saklanıyor ve bunların güvenliği nasıl sağlanıyor?
  + Kritik Veri
    - Uygulama kapsamında hangi kritik bilgiler işlenmektedir?
    - Bu gizli bilgiler olduğu yerde ve ağ üzerinde nasıl korunuyor?
    - Nasıl bir şifreleme tekniği kullanılıyor ve şifreleme anahtarları nerede tutuluyor?
  + Oturum Yönetimi
    - Oturum tanımlama bilgileri nasıl tutuluyor?
    - Oturum bilgilerinin çalınmaması için ne gibi tedbirler alınıyor?
    - Oturum bilgileri ağ üzerinden geçerken güvenliği nasıl sağlanıyor?
  + Kriptografi
    - Hangi şifreleme algoritmaları ve yöntemleri kullanılmaktadır?
    - Şifreleme anahtarları ne kadar süredir kullanılmakta ve bunların güvenliği nasıl sağlanmakta?
    - Uygulamanın kullandığı kendi şifreleme tekniği var mı?
    - Şifreleme anahtarları ne kadar sürede bir değiştirilmektedir?
  + Parametre Değiştirme
    - Uygulama oynanmış parametreyi tespit edebiliyor mu?
    - Form alanlarındaki, HTTP başlıklarındaki, oturum tanımlama bilgilerindeki parametreleri geçerliyor mu?
  + Hata Yönetimi
    - Uygulama hata durumlarının nasıl üstesinden geliyor?
    - Hata bilgileri kullanıcıya iletilliyor mu?
    - Bu hata bilgilerinde sistemin kritik bilgilerini içeren uyarılar bulunuyor mu?
  + Denetleme Ve Kayıt
    - Uygulamanız bütün sunucu ve katmanlarda denetleme ve kayıt mekanizmasına sahip mi?
    - Kayıt dosyalarının güvenliği nasıl sağlanıyor?
* Tehditlerin Belirlenmesi

STRIDE sınıflandırma modeli kullanılabilir. STRIDE modeli aşağıda belirtilmiştir:

* + Kimlik Yanıltması (Spoofing Identity): Yanıltma tehditleri saldırganların başka bir kullanıcı gibi davranmaları ya da geçerli bir sunucu gibi davranarak diğer sunucuları yanıltma amacı güder. Kimlik yanıltmaya örnek olarak, yasa dışı olarak başka bir kullanıcının şifre ve kullanıcı ismi gibi gizli bilgilerine ulaşmayı ve bu bilgileri kullanmayı gösterebiliriz.
  + Verinin Değiştirilmesi (Tampering with Data): Bu işlem verinin kötü niyetli bir şekilde değiştirilmesi manasına gelir. Internet üzerinden akan verinin değiştirilmesi buna örnek olarak gösterilebilir.
  + Inkar (Repudiation): Bu tip tehditler, bazen saldırganın gerçekleştirdiği ama bunu inkâr edebileceği tehditler olarak görülür. Inkar tipi tehditler kredi kartı gibi işlemlerde kendini gösterir. Kullanıcı bazı alımlarda bulunur ve sonra yapmadığını iddia eder. Başka bir örnek de e-posta örneği olabilir. Size gelen bir maili, karşı taraf ben atmadım diye inkâra başvurabilir.
  + Bilginin Açığa Çıkarılması (Information Disclosure): Bu tip tehditler, bazı bilgilerin onları görmemesi gereken kullanıcılar tarafından görünmesini kapsar. Örnek olarak, bir kullanıcının okumaması gereken bir dosyaya erişim hakkı olması ya da bir saldırganın ağ trafiğini dinleyip bazı bilgileri elde etmesidir.
  + Hizmet Dışı Bırakma (Denial of Service): Hizmet dışı bırakma atakları sistemlerin kullanılmaz hale gelmesini sağlayan ataklardır. Web sunucusunun kullanılmaz hale gelmesi bu tip ataklara örnek olarak gösterilebilir. Sistemlerin güvenirliliği ve sürekliliği sağlamaları adına bu tip ataklara önlem almaları gerekmektedir.
  + Yetki Kazanma (Elevation of Privilege): Bu tür ataklarda, yetkisiz bir kullanıcı sistemi kullanmak üzere yetki kazanır ve bütün sisteme zarar vermek ya da kontrolü altına almak için sisteme giriş yapar.
* Tehditlerin Derecelendirilmesi

Derecelendirmedeki amaç, öncelikle hangi tehdit üzerinde duracağımıza karar vermek ve bir sıralama oluşturmaktır. Bu derecelendirme yöntemlerinden DREAD adlı yöntemi örnek satın alma uygulamamız için kullanacağız.

* + Zarar Potansiyeli (Damage Potential): Tehdidin gerçekleşmesi durumunda, zarar ne kadar büyüklükte olacaktır. En kötü durum 10 ile gösterilebilecekken, en hafif durum 0 ile gösterilebilir. Yetki tehditleri genellikle 10 ile gösterilir. Tıbbi, mali, ya da askeri veri içeren uygulamalar içi zarar potansiyeli yüksek kabul edilir.
  + Uygulanabilirlik (Reproducibility): Potansiyal bir saldırının başarıya ulaşma şansını belirlemeye çalışır. Belirli bir tehditin, saldırgan için başarılı bir saldırı olma kolaylığının incelenmesini ön görür.
  + Sömürülebilirlik (Exploitability): Bu tehdit kapsamında bir atağı gerçellemek için ne kadar tecrübe ve çaba gerekmektedir. Örneğin, acemi bir kullanıcı, normal ev bilgisayarı ile tehdite bir atak uyguluyabiliyorsa bu ciddi bir durumdur ve bu tehdit sömürülebilirlik manasında 10 alabilir.
  + Etkilenen Kullanıcılar (Affected User): Eğer bu tehdit bir saldırıya dönüştürülür ve saldırı başarılı olursa ne kadar kullanıcının bundan zarar göreceği araştırılır. Mesela, bir sunucuyla alakalı bir tehdit, birçok kişiyi ilgilendireceğinden yüksek önem arz eder.
  + Keşfedilebilirlik (Discoverability): Açıklığın kolay ya da zor bulunabileceğinin ya da keşfedilebileceğinin değerlendirmesi yapılır.

Örnek;

Tehdit #1: Kasıtlı kullanıcı başka bir kullanıcının sipariş bilgilerini ağ üzerinden dinler.

8 Puan - Zarar Potansiyali: Başkasının gizli sipariş bilgilerini okuyabilmek ciddi bir sorun.

10 Puan - Uygulanabilirlik: Tamamen uygulanabilir.

7 Puan - Sömürülebilirlik: Ağ üzerinde yer edinmeli ve ağı dinlemeli.

10 Puan - Etkilenen Kullanıcılar: Yöneticiler dâhil herkes etkilenebilir.

10 Puan - Keşfedilebilirlik: Bu açıklığın kolayca bulunacağını varsayalım.

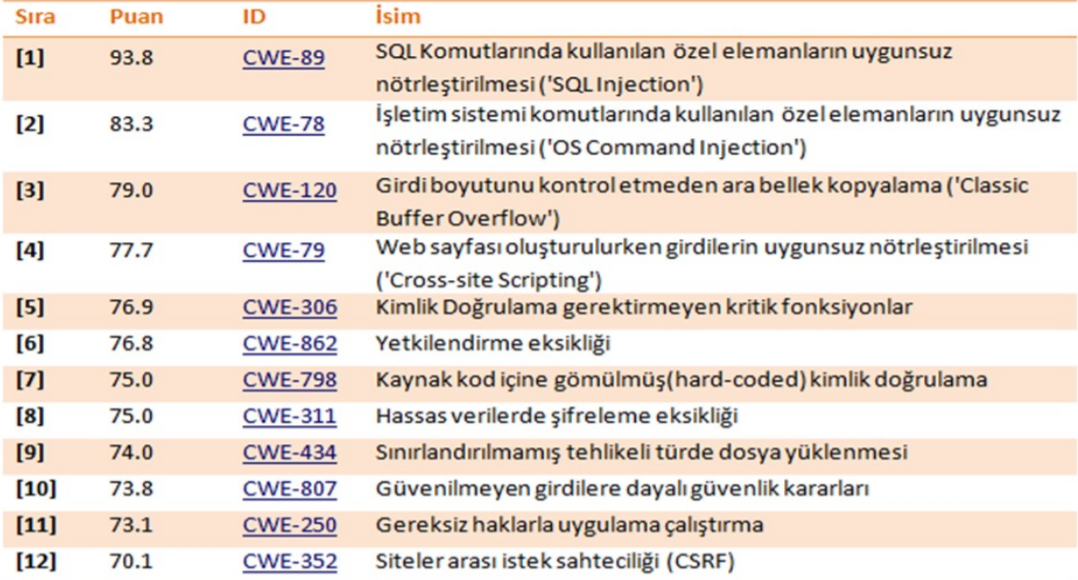
DREAD ile ölçülen risk oranı = (8+10+7+10+10)/5 = 9 Puan(9/10 “Yüksek”)

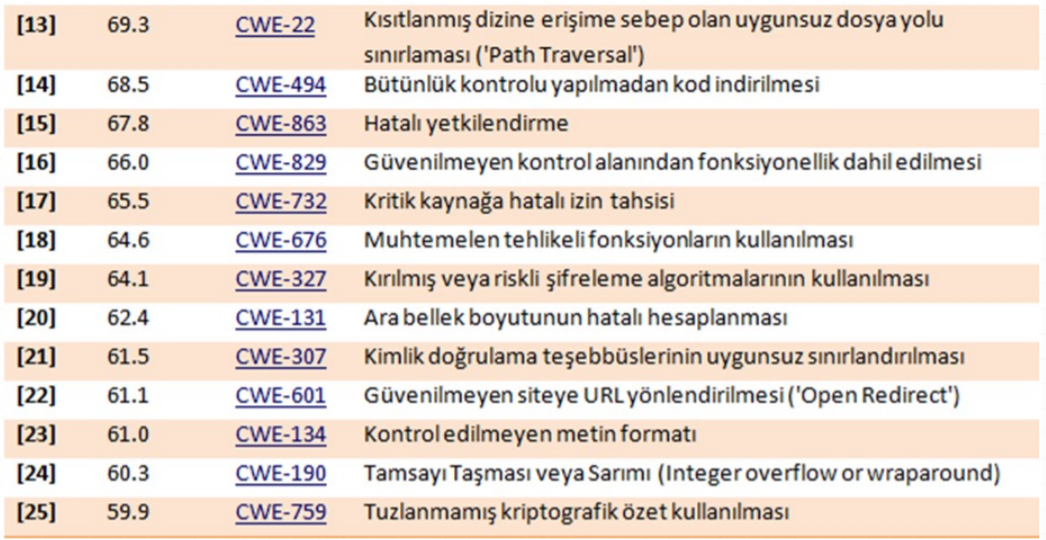
* Tehditlerin Azaltılması

Tehditler belirlendikten ve önem sırasına göre sıralandıktan sonra her tehdit için ne yapılması gerektiği kararlaştırılmalı. Bu karar dört farklı şekilde olabilir:

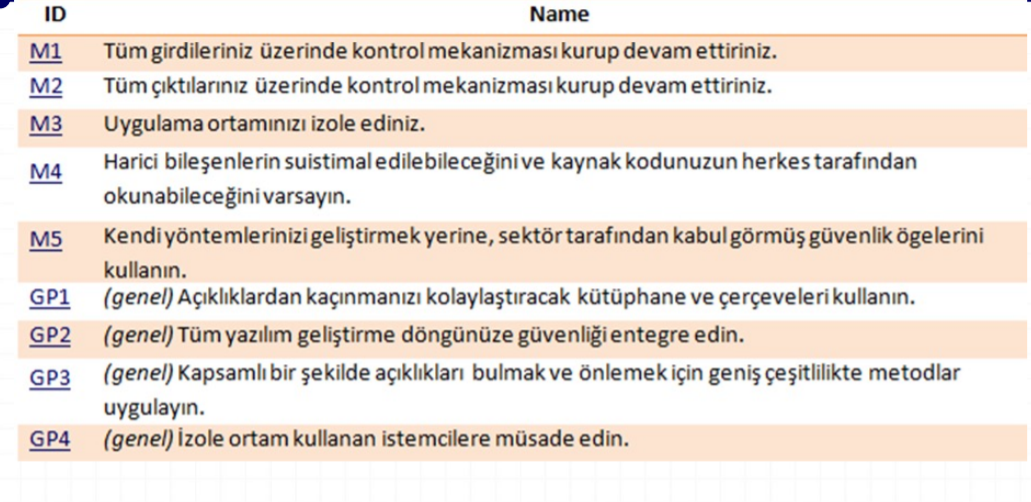
* + Herhangi bir tedbir almama: Bu yöntem genellikle doğru olmayan bir yöntemdir. En sonunda uygulamanın içerisindeki bu açıklık başınızı ağrıtabilir ve önlem almak zorunda kalabilirsiniz. Daha sonradan alacağınız önlem çok daha pahalıya size mal olabilir.
  + Kullanıcıyı uyar: Diğer bir yol ise, kullanıcının bu hususta bilgilendirilmesi ve uygulamanın o özelliğini kullanıp kullanmayacağının kendisine bırakılmasıdır. Buna örnek olarak Microsoft Internet Bilgi Servisi (IIS) verilebilir. Bu sistem, yöneticiyi eğer SSL/TLS kullanmazsa kullanıcı bilgilerinin şifresiz bir şekilde ağda gezeceğini belirtir. Bu yöntem de birçok durumda problemli bir yöntemdir. Kullanıcıların çoğu nasıl seçim yapacaklarını bilmezler. Aslında çoğu zaman, kullanıcının karşısına çıkarılan seçenek, kullanıcı için anlaşılması zor bir seçenektir. Diğer bir durum ise, kullanıcılar genellikle hazır ayarları kabul ederler ya da uyarıları görmezden gelirler.
  + Problemi ortadan kaldır: Problemi çözmek için yeterli zamanınız yoksa kısaca tehdit altında olduğunu düşündüğünüz özelliğe sahip parçayı sistemden çıkarmanız yeterlidir.
  + Problemi çöz: En kesin ve gerçekçi çözüm budur. Teknolojiyi kullanarak, problemi azaltma ya da tamamen çözme yoluna gidilmelidir. Bu yöntem aynı zamanda en zor yöntemdir. Tasarımcılar, geliştiriciler, testçiler ve güvenlik ekibi için daha fazla iş yükü ve daha fazla maliyet demektir.

**Güvenli Yazılım Geliştirme ve En Tehlikeli 25 Hata**





**Risk Azaltma Konuları**



**Anomali Belirleme**

* Üç çeşit istatiksel yöntem tanımlanmıştır
  + Eşik metriği
  + İstatiksel momentler
  + Markov modelleri
* Kural Tabanlı Sızma Belirleme
  + Herhangi bir komut dizisinin önceden bilinen ve sistemin güvenlik politikasını ihlal edecek işlemler yapıp yapmadığını tespit eder ve potansiyel sızmaları raporlar.
  + Sistemin zarar görebilecek yerlerinin ve buralara karşı yapılabilecek potansiyel saldırıların bilgisinin önceden bilinmesi gerekir.
  + Bu sistemler kural kümesinde bulunmayan saldırılara müdahale edemezler.
* Belirtim Tabanlı Sızma Belirleme
  + Bir dizi komutun bir programın ya da sistemin çalışma şekline zarar verip vermediğini belirler.
  + Sistemin güvenlik durumunu değiştirebilecek programların belirlenmesi ve kontrol edilmeleri gerekmektedir.
  + Sistemde ne olabileceği şekillendirilir.
  + Bilinmeyen saldırılara karşı çözüm.
  + Zor kısmı; belirtimlerinin çıkarılması gereken programları iyi seçme.
* Ajan
  + Veri kaynaklarından bilgi toplar.
  + Anında gönderme – Ön işlemeli gönderme
  + Yönetici potansiyel bir saldırıdan şüphelenmesi halinde ajanların çalışma şekillerini değiştirmelerini sağlayabilir.
  + Tek bir konak, birçok konak, ağ
  + Konak Tabanlı Bilgi Toplama
    - Sistem ve uygulama kayıtları üzerinde çalışırlar.
    - Olabildiğince sade bir tasarım.
  + Ağ Tabanlı Bilgi Toplama
    - Ağdaki çeşitli araçlardan ve yazılımlardan faydalanırlar.
    - İçerik incelemesi
    - Yerleştirilme yerleri iyi seçilmeli
* Yönetici
  + Analiz motoru ile herhangi bir saldırı veya saldırı başlangıcı olup olmadığını kontrol eder.
  + Bir veya birden fazla analiz modeli kullanabilir.
  + Ayrı bir sistem üzerinde bulunur.
  + Birçok yönetici üzerinde çalıştıkları kural kümelerini ve profilleri değiştirebilme özeliğine sahiptir.
* Bildirici
  + Yöneticiden aldığı bilgilere göre hareket eder.
  + Sistem yöneticisine bir saldırının yapılmakta olduğunun haber vermek.
  + Saldırıya karşılık vermek.
* Sızma Belirleme Sistemlerinin Örgütlenmesi

Üç temel yaklaşım var

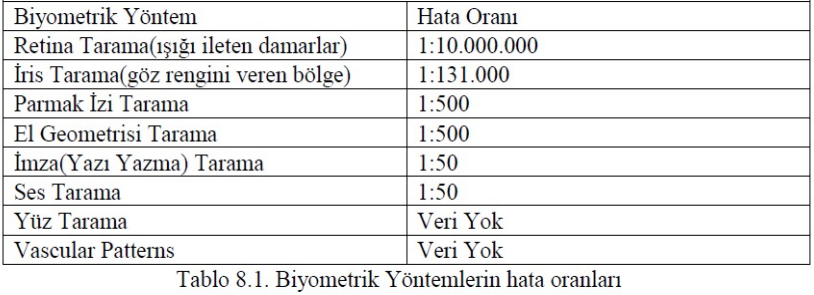
* Ağ Trafiğini İzlemek (NSM)
* Konakları ve Ağları Birlikte İzlemek (DIDS)
* Özerk Aracılar Kullanmak
* Ağ Trafiğini Sızmalara Karşı İzlemek
  + Kaynak, varış ve hizmet üçlüsü izlenir.
  + Elde edilen bilgiler üç eksene yerleştirilerek bir matris oluşturulur.
  + Beklenen değerler matrisi ile maskelenerek terslikler ortaya çıkarılır.
  + Matrisler sıradüzeni ile aşım engellenir.
  + İmzalar da yapıya eklenebilir.
* Konakları ve Ağı Birlikte İzlemek
  + Konakların ve ağın izlenmesini iç içe koyarak ayrı ayrı izlemeyle belirlenemeyen saldırıları belirleyebilir.
  + Director adında merkezi bir uzman sistem kullanır.
  + Uzman sistemnin altı katmanlı bir yapısı vardır.
  + DIDS üzerine kurulan GrIDS sıradüzensel bir yapıyla bu yaklaşımın geniş alan ağlarına uygulanmasını sağlar.
* Özerk Aracılar
  + Director, tekil hata noktası oluşturur.
  + Bu yaklaşımda uzman sistem her bir ayrı bir izleme ile görevli aracı parçalara ayrılır.
  + Parçalardan biri çalışmazsa diğerleri onun boşluğunu doldurabilir.
  + Parçalardan birine yapılan saldırı tüm ağın güvenliğini etkilemez.
  + Yapısı gereği ölçeklenebilir.
* Engelleme
  + İdeal şartlarda sızma denemeleri henüz başında engellenir.
  + Hapsetme, saldırganları saldırılarının başarılı olduğuna inandırarak sınırlı bir alana sıkıştırmaktır. Hapiste gerçek dosya yapısına çok benzer bir dosya yapısı kullanılır, iyice kısıtlanmış saldırganın davranışları böylece gözlenebilir.
  + Bu kavram, ayrıca, çok güvenlik seviyeli ağlarda da kullanılabilir.
  + Bir başka örnekte sistem çağrılarında bir terslik olması durumunda sistem çağrıları özellikle geciktiriliyor.
  + Normal kullanıcılar bundan etkilenmezken, saldırganlar kısa sürede iki saati aşkın bekleme sürelerine erişiyorlar

**Güvenlik Araçları**

* Nmap
  + Network Mapper
  + Ağ araştırması ve güvenlik denetlemesi yapan açık kaynaklı ücretsiz bir yazılım.
  + Alışılmışın dışında IP paketleri göndererek tarama yapar.
* 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.)
* Ethereal
  + Canlı bir ağ üzerindeki verileri incelemek veya disk üzerine kaydetme amacıyla kullanılır
* 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.
  + Gerçek zamanlı alarm mekanizması.
* Tcpdump
  + Ağ inceleme ve veri yakalama amaçlı klasik bir sniffer.
  + Ağ hareketlerini incelemede kullanılır.
* 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 kullanılır
  + 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.
* GFI LANguard
  + Sistemdeki güvenlik hasar risk analizini otomatik olarak yapan bir araç.
  + Ağ taraması yapar.
  + Her makinenin servis paket durumunu, yamanmamış güvenlik açıklarını, açık paylaşım alanlarını ve portlarını, çalışan uygulamalarını, vb. birçok bilgiyi raporlar.
* 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.
  + Geliştirilme amacı zayıf unix şifrelerini tespit etmek.
  + 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)
* Tripwire
  + Bütünlük analizi yapan araçların büyükbabası.
  + Dosya ve dizinlerin bütünlüklerinin bozulup bolulmadığını inceler.
  + Herhangi bir değişim sonrası sistem yöneticilerini uyarır.
* Wireshark
  + 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.
  + Şebeke problemlerinde sorun çözme
  + Güvenlik problemlerini sınamak
  + Uygulamaya konan protokollerde oluşan hataları onarmak veya arındırmak
  + Ağ problemlerinin içindeki bilgileri öğrenebilmek amacıyla kullanılmaktadır
  + Çeşitli kriterlerde paket arar ve filtreler
  + Birçok protokol için şifre çözme desteği sunar. (IPsec,ISAKMP,Kerberos,SNMPv3, SSL/TLS, WEP, ve WPA/WPA2'yi içerir).
  + 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

**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.



**Örüntü Tanıma**

Örüntü Tanıma, gereksiz detaylardan arındırılmış olan giriş datasından çıkartılan anlamlı özellikler yardımıyla teşhis sınıflarına ayrılan verinin sınıflandırılmasıdır.

* 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

**Biyometrik Tanıma Teknikleri**

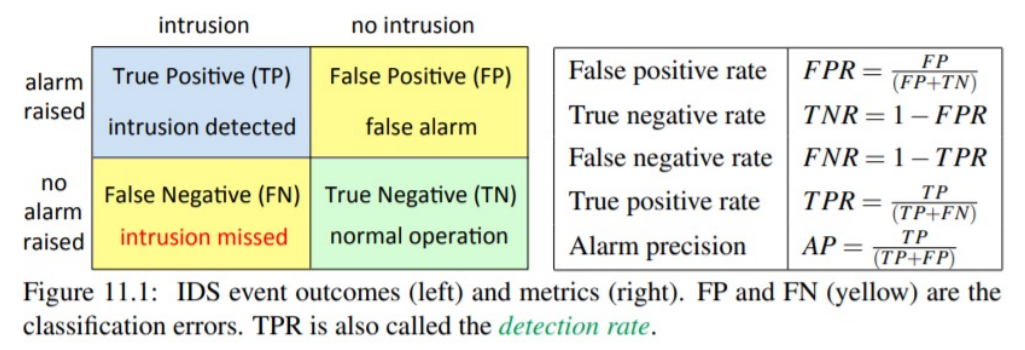
* Parmak izi tanıma
* Optik Tanıma
* Yüz Yapısı Tanıma
* Ses Tanıma
* İmza Tanıma
* Yazma Ritmi Tanıma
* Toplardamar İzi Tanıma
* Avuç içi izi
* Kulak Şeklinden tanıma

**Saldırı Tespiti ve Ağ Tabanlı Saldırılar**

**Saldırı tespit sistemi (Intrusion detection system - IDS)**

* Bir IDS, izinsiz girişleri ve diğer olumsuz olayları, devam etmekte iken veya olaydan sonra tespit eder.
* IDS'nin temeli, bulmayı kolaylaştıran ve adli analizi destekleyen kanıtları toplayan bir izleme sistemidir. Uygulamada, gerçekte ne olduğunu çözmek genellikle insan uzmanlar tarafından analiz gerektirir ve keşif, yeni saldırılar için açık uçlu olabilir
* Pasif izlemenin ötesinde bir saldırı önleme sistemi (intrusion prevention system - IPS), örneğin devam eden ihlalleri durdurmak veya ağ yapılandırmalarını değiştirmek gibi aktif yanıtları içerir. Güvenlik duvarını bir adım öteye taşıyan bir IPS, paketleri değiştirebilir, kötü amaçlı yazılımları kaldırabilir veya bağlantıları sonlandırmak için TCP sıfırlamaları gönderebilir; bilgisayar tabanlı IPS, işlemleri sonlandırabilir
* Sensörlerin olay akışlarını nereden topladığına bağlı olarak iki tamamlayıcı IDS kategorisi vardır;
* Ağ tabanlı IDS'ler (NIDS)
  + NIDS olayları, stratejik bir gözlem noktasında, örneğin bir ağ geçidinde veya bir LAN (yerel alan ağı) anahtarında elde edilen paketlerden türetilir.
* Host Tabanlı IDS'ler (HIDS)
  + işletim sistemi çekirdek tarafından oluşturulan işlemlerden ve denetim kayıtlarından, uygulama günlüklerinden (kullanıcı kimliğini not ederek), dosya sistemi değişikliklerinden (dosya bütünlüğü kontrolleri, dosya izinleri, dosya erişimleri) ve sistem çağrısı izlemesinden türetilebilir
  + Bilgisayara, ağ erişimlerine, gelen / giden paket içeriklerine ve ağ arayüzlerindeki durum değişikliklerine (açık portlar, çalışan servisler) özeldir.
  + Kaynak kullanım modelleri (CPU süresi, disk alanı) şüpheli işlemleri ortaya çıkarabilir.

**IDS OLAY SONUÇLARI**



**Anomali Tabanlı Yaklaşımlar**

* Avantaj:
  + Daha önce görülmemiş saldırılar tespit edilebilir.
* Dezavantajlar
  + Özniteliklerin seçimi zordur.
  + Saldırıların eğitim esnasında olmadığı varsayımı gerçekçi olmayabilir.
  + Normal profiller normal davranışları zaman içinde öğreniyor ise saldırganlar kendi davranışlarını normal profillere yerleştirebilirler.

**Paket Dinleme**

* İyi Kullanım
  + IPS için gerçek zamanlı analiz (IDS için de hızlı işlem önemlidir).
  + Ağ izleme (ağdaki faaliyetler, trafik düzenleri ve kullanım hakkında öngörü sağlar).
  + Ağ adli analizi.
* Kötü kullanım
  + Saldırı amacıyla (iyi bir önlem: şifreleme)

**Zafiyet Değerlendirme Araçları**

* Hem bilgisayar tabanlı araçlar hem de ağ tabanlı araçlar kullanılır, ağ tabanlı araçlar üç kategoriye ayrılır:
  + Keşif araçları (reconnaissance tools) (örnek: Nmap)
    - Port tarayıcıları
    - İşletim sistemi parmakizi çıkarma
  + Zafiyet tarayıcıları (örnek: Nessus)
  + Sızma testi araçları (yetkilendirilmiş) / sömürü araç takımları (siyah şapkalar) (örnek: Metasploit).

**DoS Saldırı Sınıfları**

* Gizli uygulama kusurlarından (zafiyetler) yararlanır.
* Kaynakları (bant genişliği, CPU, ana bellek, disk) tüketir.
  + Sabit kaynakları tüketerek (örnek: SYN Flooding),
  + Yoğun kaynak gerektiren işlemlerin talep edilmesi (örneğin, asimetrik anahtar çiftlerinin oluşturulması).
* Dağıtık DOS (DDOS)
* SYN Selleme (SYN Flooding)
* Smurf Saldırısı
  + Ping paketleri ve yanlış IP adresleri kullanan ICMP flood: bir yükseltme (amplification) faktörü elde etmek için yayın adreslerini (broadcast address) kullanır.
  + Bir yerel ağ yayın adresine gönderilen paket, o ağdaki tüm ana bilgisayarlara gider.

Giriş ve Çıkış Filtreleme

DNS Çözümleme

* Pharming Saldırısı: Alan adı - IP adres dönüşümlerinde değişiklik yapmak.
  + Bilinen bazı saldırı vektörleri:
    - Yerel dosyalar.
    - Ara DNS sunucuları.
    - Ağ üzerinden cevap değişiklikleri.
    - Sahte DNS sunucuları.
    - DNS Zehirleme (DNS Poissoning)

ARP Sahtekarlığı (Spoofing)

Koruma Yöntemleri;

* ARP sahtekarlığı, IP adresini MAC adresiyle eşleyen statik, salt okunur cihaz ARP tabloları tarafından durdurulabilir.
* manuel olarak ayarlamak ve güncellemek ekstra çaba gerektirir.
* Çeşitli araçlar ARP sahtekarlığını algılayabilir ve önleyebilir.
* örneğin ARP yanıtlarını çapraz kontrol ederek.
* Tercih edilen uzun vadeli bir çözüm, güncellenmiş bir Adres Çözümleme Protokolünde güvenilir bir kimlik doğrulama yöntemi kullanmaktır.

**Güvenlik Duvarları**

İki temel kategoriye ayrılır:

* Paket filtreleri
* Vekil (Proxy) Güvenlik Duvarları

**Paket Filtre Firewall**

* Bir ağ güvenliği güvenlik duvarı, iki ağ veya bir ağ ve bir cihaz arasında veri geçişine izin verebilen veya reddeden ve isteğe bağlı olarak değiştirebilen erişim kontrolü işlevi sağlayan bir ağ geçididir.
* Ağ güvenlik duvarları en yaygın olarak sınır-temelli savunmalarda hizmet eder ve güvenilir bir özel (dahili) ağı, güvenilmeyen bir genel (harici) ağdan (ör. İnternet) korur.

**Paket Filtreleme Kuralları**

* Bir paket filtre güvenlik duvarı, bir yönetici tarafından yapılandırılır.
* <koşul,eylem> biçiminde bir kural listesi içerir.
* Bir "ilk eşleştirme kuralı" güvenlik duvarında, bir paket için gerçekleştirilen eylem, koşulu karşılanan ilk kural tarafından belirtilen eylemdir.
* Temel eylemler şunlardır:
  + 1. İZİN VER (paketin geçmesine izin ver
  + 2. DÜŞÜR (sessizce paketi atın — tip-1 reddetme)
  + 3. REDDET (geçirme ama aynı zamanda kaynağı bilgilendirmeye çalış — tip-2 reddetme).
* Ek olarak, ikinci bir eylem, örneğin syslog genel sistem günlük kaydı hizmetini kullanarak paketi günlüğe kaydetmektir.
* Verimlilik için, çoğu paket filtresi eşleştirme kuralı beş TCP / IP başlık alanına (src addr, src port, dst addr, dst port, prot) ve eğer ICMP ise ICMP türü ve kodunu temel alır.
* Bazen diğer başlık alanları (paket boyutu, bayraklar) da kullanılır.
* Daha karmaşık kurallar ve akıllı paket filtreleme, yük (payload) verilerini, örneğin URL'e dayalı bir izin verme veya reddetme kararını içerebilir - ancak uygulama yüklerinin incelenmesi genellikle paket filtrelerinin kapsamının dışındadır.

**Durumsuz ve Durumlu Güvenlik Duvarları**

* Basit bir durumsuz paket filtresinde, her paket diğerlerinden bağımsız olarak işlenir (önceki paketlere bağımlı olmaksızın).
* Bunun aksine, durumlu bir paket filtresi, daha sonraki paketlerin işlenmesinde kullanılmak üzere paketler işlenirken seçilen ayrıntıları izler.
* Durum ayrıntıları bir güvenlik duvarı durum tablosunda tutulur. Bu genellikle TCP bağlantı durumlarının izlenmesi anlamına gelir; Oluşturulan veya devam eden bağlantı kurulumlarına karşılık gelen kaynaklara sahip paketler, yeni kaynaklardan farklı şekilde ele alınır.

**Vekil (Proxy) Güvenlik Duvarları**

Paket filtre dışında vekil olarak isimlendirilebilen iki farklı türden güvenlik duvarı daha vardır:

* Devre seviyesinde Vekil (Circuit-level Proxy): bağlantıları genel olarak tek bir vekil noktası üzerinden aktarır; ana amaç önce bağlantıya izin veya red kararını vermek ve ardından verileri aktarmaktır.
* Uygulama seviyesinde Filtre (Application-level Filters): önceden belirlenmiş ve yetki verilmiş bir dizi uygulama için birden çok özel işlemci aracılığıyla uygulamaya-özgü işlemler gerçekleştirir.

**SSH (Secure Shell)**

SSH'den önce, uzaktan oturum açma (rlogin, telnet), ve ilgili Unix uzaktan erişim komutları (rsh, rcp, rexec) ve dosya aktarımı (ftp), ağ üzerinden verileri ve parolaları açıktan gönderiyor idi.

* SSH ve SSH kullanarak oluşturulan yardımcı programlar daha güvenli alternatifler olarak tasarlandı (gizlilik, doğruluk, kimlik doğrulama sağlayacak şekilde).
* Güvenilir paket aktarımı için TCP'yi kullanan SSH, hem uzak hizmetlere oturum açmak için gönderilen parolaları hem de kimlik doğrulama sonrası devam eden TCP bağlantılarını koruyan taşıma katmanında bir güvenlik tüneli sağlar.
* SSH ile, uzak bir ana bilgisayarda bulunan herhangi bir programın güvenlik tüneli üzerinden çalıştırılabilmesi mümkün olur

**SSH Protokolleri**

Üç parçadan oluşur:

* Taşıma katmanı protokolü: sunucu kimlik doğrulama, şifreleme, bütünlük koruma.
* Kullanıcı kimlik doğrulama protokolü:
  + İstemci parolası (veya tek-kullanımlık parolalar)
  + Kerberos
  + İstemci açık-anahtar
* Bağlantı protokolü: Tek bir tünelin birden fazla amaç için kullanılmasını sağlar (mantıksal kanallar) (çoklama)

**Şifreli Tüneller ve VPN’ler**

* Normal TCP/IP paketleri düz metindir. Tüm paket içeriği (başlık ve yük) paket akışına erişimi olan tüm partiler (yönlendiriciler, anahtarlar, geçitler, vb.) tarafından görülebilir.
* Koruma için fikirlerden biri gönderici tarafta tüm paketin şifrelenmesidir. Fakat, bu protokolleri çalışmaz kılar: başlık bilgilerinin okunması imkansız olur.
* Bu sebeple paket başlıkları da şifrelenecek ise bu pkaetin başka bir paket içerisine konumlandırılması gerekir. Alternatif olarak, paketin sadece yük kısmı korunabilir.
* Tünelleme kavramı kapsülleme (encapsulation) ile doğrudan ilgilidir: Bir protokol (başlık ve yük) diğer birinin yükü olur.
* Tünelleme için yaygın olarak kullanılan iki protokol SSH ve Ipsec’dir.
* Tünel kurulduktan sonra uygulamalar ve kullanıcılar başka bir değişikliğe gerek duymadan güvenli hale gelirler.
* Tünellerin bir diğer uygulaması da Sanal Özel Ağlardır (VPN).

**IPsec**

* TLS ve SSH’den farklı olarak IPsec protokolü ağ katmanında bir güvenlik servisi sunar. Bu sayede tüm taşıma ve uygulama katmanı protokolleri otomatik olarak korunur.
* VPN’ler için IPsec üç protokol ileçok geniş bir yelpazede güvenlik servisleri sunar:
  + IKE (Internet Key Exchange)
  + AH (Authentication Header)
  + ESP (Encapsulating Security Payload)
* Ağ katmanında değişiklik gerektirdiği için TLS veya SSH’ye göre daha karmaşıktır ve uzmanlık gerektirir.
* IPsec politikaları ile tüm paketlerin VPN üzerinden gitmemesi sağlanabilir (politika tabanlı paket filtreleme).

**TLS ve HTTPS**

Bir TLS İstemci-Sunucu kanalı iki aşama ile kurulur:

* El Sıkışma Katmanı
  + Anahtar değişimi
  + Sunucu parametreleri
  + Bütünlük ve kimlik doğrulama
* Kayıt Katmanı
  + Anlaşma sağlanan parametrelerle uygulama verisinin korunması Anahtar Değişimi (TLS 1.3)
  + Amaç: Bir ana (master) anahtar oluşturmak (istemci nonce ve sunucu nonce değerleri de kullanılır)
    - Üç seçenek:
      * Diffie-Hellman Ephemeral (DHE)
      * pre-shared key (PSK)
      * PSK + DHE
    - Sunucu Kimlik Doğrulama için PSK, RSA imzalama veya eliptik eğri opsiyonları mevcuttur.
    - İstemci Kimlik Doğrulama TLS’de isteğe bağlıdır ve genelde kullanılmaz.

**Tarayıcı Çerezleri**

* HTTP'nin kendisi durumsuz bir protokoldür - ardışık HTTP isteklerinde hiçbir protokol durumu korunmaz.
* Dil tercihi veya alışveriş sepeti verileri gibi durumları koruyabilmek rahatlık ve işlevsellik sağlar. Bu konuda çözüm yollarından birisi HTTP çerezleridir.
* Temel fikir, sunucunun sınırlı boyutta veriyi istemciye (tarayıcı) iletmesidir; bu veri sonraki isteklerde aynı sunucu sitesine veya sayfasına döndürülür.
* Varsayılan olarak, bunlar tarayıcı belleğinde saklanan kısa ömürlü oturum çerezleridir; sunucu tarafından yapılan ayarlamalar ile kalıcı çerezler olarak ömürleri uzatılabilir.
* Birden çok çerez (sunucu tarafından seçilen farklı adlarla), tek bir HTTP response mesajında birden çok Set-Cookie başlığı kullanılarak belirli bir kaynak sunucu tarafından ayarlanabilir.
* Bir kaynak sunucu sayfasındaki tüm çerezler, daha sonraki ziyaretlerde - çerez başına kapsam özniteliklerine bağlı olarak muhtemelen diğer ana bilgisayarlara da (Çerez istek başlığı kullanılarak) döndürülür.
* Bir sunucu tarafından ayarlanan çerez, bir "ad = değer" çiftinden ve sıfır veya daha fazla öznitelikten oluşur.

**Aynı-Köken Politikası (Same-Origin Policy)**

* Aynı-Köken politikası (SOP), belgeleri izole etmek için bir erişim kontrol felsefesidir.
* Genel fikir, bir kaynaktan (orijinden) gelen bir sayfanın (belgenin) başka bir kaynaktan bir sayfaya müdahale etmemesi (erişmemesi veya değiştirmemesidir).
* Bu, İ5 ilkesinin bir uygulamasıdır .
* Bir HTML belgesinin başka bir kısıtlama olmaksızın farklı host1 ve host2’den sayfa yüklemesine ve karıştırmasına izin verdiğimizi varsayalım.
* Ortaya çıkan birleştirilmiş belgede host1’deki JavaScript, host2 ile ilişkili verilere erişebilir.
* Eğer host1 kötü niyetli ise ve host2 örneğin bir bankacılık sitesiyse bu sorunludur.
* Bu nedenle bazı kurallara ihtiyaç vardır - ancak katı host izolasyon politikaları, işbirliği yapan alt domain’ler (ör. Bir çevrimiçi ürünün katalog ve satın alma bölümleri) arasında istenen etkileşimi karşılayamaz.
* Bu aynı zamanda, üçüncü taraf reklamlarını gösteren işlenen sayfaların çerçevelerine gömülmeyi içeren İnternet reklamcılık modelini de bozacaktır.
* Bu tür fiili gereksinimler, izolasyonla ilgili kuralların bu tür işlevselliğin rahatlığına ve faydasına eşlik etmesi için motive eder.

**Kimlik Doğrulama Çerezleri**

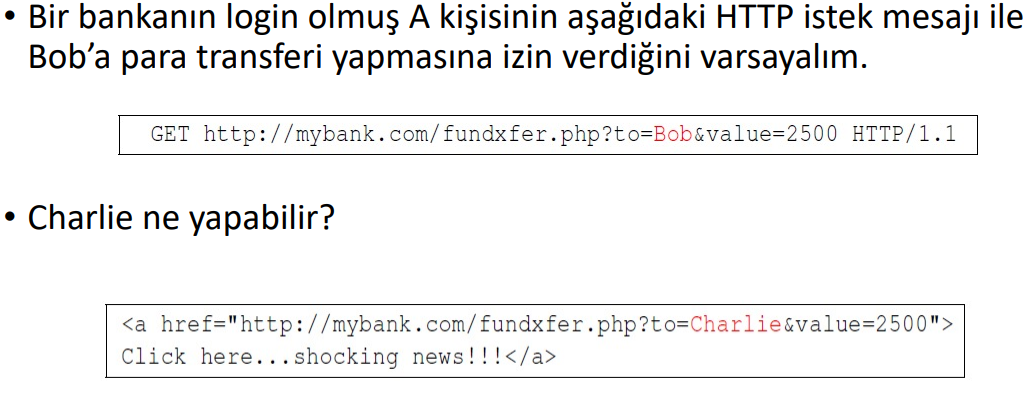
* Kullanıcı kimlik doğrulaması gerektiren siteler için, kullanıcı genellikle bir açılış sayfasında oturum açar, ancak daha sonra ziyaret edilen aynı site sayfalarının her biri için yeniden kimlik doğrulaması istenmez.
* Oturumun kimlik doğrulama sonucu sunucu tarafında veya kimlik doğrulama çerezi olarak kaydedilir.
* Sunucu, çerez kullanım süresinden daha kısa bir oturum sona erme süresi belirleyebilir (sonrasında yeniden kimlik doğrulama gerekir).
* Çerez kalıcıysa ve tarayıcı kalıcı çerezleri devre dışı bırakmadıysa, kimlik doğrulama çerezi, doğrulanmış oturumu tarama penceresinin ömründen daha uzun süreye yayabilir.

**Çerez Hırsızlığı**

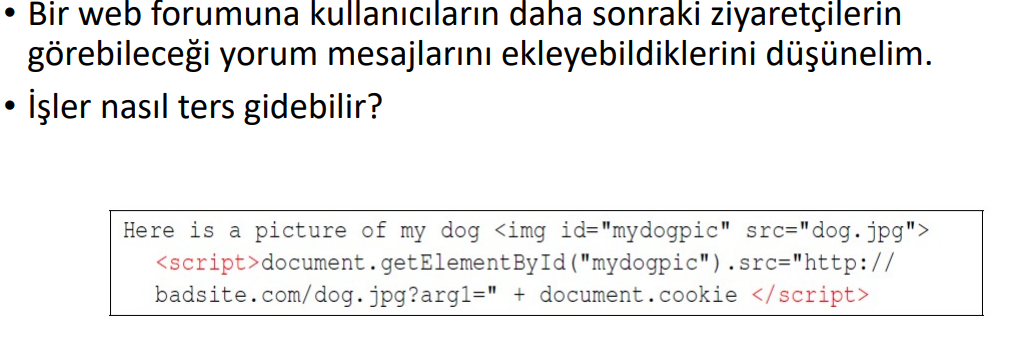
* Kötü niyetli Javascript
* Güvenilir olmayan HTTP Proxy’ler
* Scriptler dışında istemci tarafında kötü niyetli yazılımlar
* İstemci makineye fiziksel erişim

**Cross-Site Request Forgery (CSRF)**

* Get ile ilgili durumlar.



**Cross-Site Scripting (XSS)**



**SQL Enjeksiyon Saldırısı**

* Bir web sitesinde oturum açmak isteyen bir kullanıcıya bir tarayıcı formu sunulduğunu ve bir kullanıcı adı ve şifre girdiğini varsayalım.
* Bir HTTP request mesajı, bu değerleri web sayfasına taşır; burada bir sunucu tarafı komut dosyası, bunları dizi değişkenlerine (un, pw) atar.
* Değerler, doğrulama için arka uç SQL veritabanına gönderilmek üzere bir SQL sorgu dizisine yerleştirilir.

**Wireshark**

Kullanım Alanları;

* 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

**FİLTRELER**

* 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 yakala
* ip.addr IPv4 adresi Source(kaynak) veya Destination(hedef)
* 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
* 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
* 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