Defansif Güvenlik Temelleri (Defensive Security Basics)

Gizlilik, bütünlük, erişilebilirlik (CIA)

En yaygın Siber Saldırılar;

Ele Geçirme Saldırıları (internet tarayan botlar) (dos, ddos veya veri sızıntısı için)
Veri Sızıntısı
Hizmet Engelleme

Defansif Güvenlik Çalışma Alanları

Ağ Güvenliği
Adli Bilişim
Zararlı Yazılım Analizi
DevSecOps
Bulut Güvenliği
Sistem Güvenlik Mühendisi
SOC Analyst
Layer 1, 2, 3

OSI Modelleri

Fiziksel Katman: Verinin kablo üzerinde alacağı fiziksel yapıyı tanımlar.
Veri Bağlantısı Katmanı: Fiziksel katmana erişmek ve kullanmak ile ilgili kuralları belirler.
Ağ Katmanı: Veri paketine farklı bir gönderilmesi gerektiğinde yönlendiricilerin kullanacağı bilginin eklendiği katmandır.
Taşıma Katmanı: Üst katmanlardan gelen veriyi ağ paketi boyutunda parçalara böler.
Oturum Katmanı: İki bilgisayardaki uygulama arasındaki bağlantının yapılması, kullanılması ve bitirilmesi işlemleri yapılır.
Sunum Katmanı: Yollanan verinin karşı bilgisayar tarafından anlaşılacak şekilde çevrilir.
Uygulama Katmanı: Bilgisayar uygulaması ile ağ arasında bir arabirim sağlar. OSI katmanları arasında sadece bu katman diğer katmanlara servis sağlamaz.

TCP/IP vs OSI

DATA - Application
UDP header | UDP data - Transport
IP header |IP data - Internet
Frame header | Frame data | Frame footer - Link

Defansif Güvenlik Uyg.

Content Gateway
Firewall
VPN
IDS
IPS
NAC

Güvenlik Duvarı Türleri

Ağa gelen ve giden paketlerin trafiğini kontrol eder.

- Packet Filters Firewall
- Stateful Inspection Firewall
- Application Layer Firewall
- Host-based Firewall vs. Network Firewall

VPN (Özel Sanal Ağ)

- PPTP
- Site-to-Site
- L2TP
- IPSec
- SSL and TLS
- MPLS
- Hybrid

IDS & IPS

- Detection
- Protection

Kitap

Türkay Henkoğlu - Adli Bilişim: Dijital Delillerin Elde Edilmesi ve Analizi

NAC

Yetki kontrolü ile erişim sağlanması

EDR / Gelişmiş Antivirüs

Son kullanıcı cihazlarına yüklenen ajanlar sayesinde cihaz üzerindeki etkinlikleri denetleyip, servera durum hakkında bilgi gönderen güvenlik uyg.

Zero Day'e karşı etkili bir savunma.

Data Loss Prevention

Gönderilmesi istenmeyen hash != gönderilen dosyanın hash'i

- Dosyayı gönder

Password Spray Attack

Parola püskürtme, yaygın olarak kullanılan birkaç parola ile çok sayıda hesaba (kullanıcı adı) erişmeye çalışan bir saldırıdır. Geleneksel kaba kuvvet saldırıları, parolayı tahmin ederek tek bir hesaba yetkisiz erişim elde etmeye çalışır.

Web Application Firewall (WAF)

Layer 7 içeriklerini kontrol eder, eğer zararlı bir payload görürse isteği durdurur

(İÇERİĞİ TAMAMEN AÇIP OKUYOR, PROBLEM)

Gerçek IP'nizi bilmiyorlar

SIEM

Log kaynaklarından topladığı logları belirli korelasyonlardan geçirip filtreleyerek, aksiyon alır.

Honeypot (Bal küpü)

Gerçek sistemler gibi davranır.
Saldırganın yapacağı adımların keşfi, önlemlerin alınması ve engellenmesi.
İstihbarat sağlama, log artışı..
Yapacağı adımları loglama.

Next generation SIEM

Yapay zeka ile SIEM

Merkezi Güvenli İzleme ve Olay Yönetimi

NXLog
Rsyslog,
Cron.log, Linux sistemlerde zamanlanmış log.

Kayıt Yapılandırma Ayarları

Ajansız Servis ve protokoller
SSH/SCP/RSYNC
WMI

Ajan tek taraflı
Ajansız network'i ikiye katlar, yavaşlatır.

Syslog Kayıt Dereceleri

0 emerg
1 alert (en kısa zamanda düzeltilmeli)
2 crit
3 err
4 warning (aksiyon alınmazsa hataya dönüşebilir)
5 notice (olağan dışı fakat hata değil)
6 info (normal durumlar)
7 debug (hata ayıklama)

Log Toplama Sistemlerinin (Logger) Görevi

Merkezi Log Toplama Sistemleri

Kayıtların değiştirilmediğinden emin olunmasını
5651 kanunu
Belirli şartlarda olan firmaların veya sistemlerin log kayıtlarının (kull direkt etkileşime geçtiği veya kullandığı firewall ve dns işlemlerinde zaman damgası ile arşivlenmesi gerekir.

Belirli log cinsleri var.

Bu loglar belirli merkezi log cinsleştirme de
İstenen periyot ve şekillerde sıkıştırılıp hash değeri alınır.
Hash değeri sayesinde değiştirilemez. Değişiklik durumunda hashler uyuşmaz.