Siber Güvenliğe Giriş

Siber güvenlik, siber ağlara bağlı sistemleri ve tüm verileri yetkisiz kullanıma veya zararlara karşı korumak için devam eden çabadır.

Kişisel verilerimiz;
- Tıbbi veriler
- İstihdam
- Online bilgi
- Kimliğimiz
- Eğitim verileri
- Finansal veriler
- Bilgi işlem cihazlarındaki veriler

Tüm verilerimiz dijital olarak, online bir alanda, internette, bulutta saklandığından bunun güvenliğini sağlamalıyız.

• Siber sadece İnternet değildir, çok daha fazlasıdır.

Varlık - Asset

CIA Üçlüsü
Confidentiality, Integrity, Availability
Gizlilik, Bütünlük ve Uygunluk (kullanılabilirlik)

- Kimlik doğrulama
- Şifreleme
- Erişim kısıtlama

- Verilerin doğru ve bütün olmasını temsil eder.
- (Checksum)
- (Hash)
  - MD-5
  - SHA-1
  - SHA-256
  - SHA-512

- Erişebilme
- Bilgilerinizi verilerinizi kullanabilmek, ulaşabilmektir
  - Yedek alınması
  - Güncellenmesi önemlidir.

• OAuth 2.0
• Asıl yetkilendirme

Şifre ✗ Parola
dBebCA512det ↔ Ilove You

Saldırganlar kişisel veya finansal kazanç için güvenlik açığından yararlanmaya çalışan bireyler veya gruplardır.

- Amatörler
  - Script kiddies de denir. Genellikle saldırmak için hazır araçlar ve talimatlar kullanırlar. Az yada çok az kapasiteye sahiptirler.
- Hackerlar
  - Beyaz Şapkalı
    - Güvenliğinin geliştirilmesi incelenmesi, zayıf yönlerin keşfedilmesi için sistemlere girerler
    - Bir izin doğrultusunda...
  - Gri Şapkalı
    - İzinsiz şekilde sistemlere sızarlar
    - Amaçları zarar vermek veya bilgiyi çalmak değildir.
  - Siyah Şapkalı
    - İzinsiz şekilde sistemlere sızıp veri çalma veya zarar verme amacı güden kişilere denir
- Organize Hackerlar

CamScanner ile tarandı

SİBER SALDIRGANLAR

Dışarıdakiler

- Organize Saldırganlar
- Hacktivistler
- Amatörler

İçeridekiler

Çalışanlar
Eski çalışanlar
Sözleşmeli personel
Güvenilir iş ortakları

⊕ Gizli verileri yanlış kullanma
⊕ İş sunucularını veya ağ altyapısını tahrip etme
⊕ Virüs bulaşmış USB ortamını kurumsal bilgisayar sistemine bağlamak
⊕ Kötü amaçlı e-posta veya web sitelerine girerek kötü amaçlı yazılımı ağa bulaştırma.

SALDIRILAR KAVRAMLAR TEKNİKLER

1) Güvenlik Açıklarını Bulma

Güvenlik açıkları her türlü yazılım ve donanım ortamında olabilir.
Exploit, güvenlik açığından yararlanmak için yazılmış bir programdır.

- Yazılımsal Güvenlik Açıklıkları
  - -Arabellek taşması (Buffer Overflow)
  - -Doğrulanmamış Girdi (Non-Validated Input)
  - -Yarış Koşulu (Race Conditions)
  - -Güvenlik Uygulamalarındaki Zayıflıklar
  - -Erişim denetim sorunları
- Donanımsal Güvenlik Açıklıkları

Keşif Ataklari
- internet bilgi araştırması
- ping taraması
- port taraması
- paketleri dinlemek
- sosyal mühendislik

KÖTÜ AMAÇLI YAZILIM TÜRLERİ (MALWARE

Malware, veri çalmak, erişim denetimlerini atlatmak veya bir sisteme zarar vermek için kullanılan programlar veya kod parçalarıdır.

- Casus Yazılım — Etkinlik izleyicileri, tuş vuruşu toplama, veri yakalama
- Adware — Reklam yazılımı
- Bot — Gizlenmiş şekilde otomatik eylem gerçekleştirmek için tasarlanmıştır. En kötüleri botnet
- Ransomware — Fidye yazılımıdır. Verileri ödeme yapılıncaya kadar şifreli halde rehin alır.
- Scareware — Korkuya dayalı bir eylem yapmaya ikna etmeye yönelik yazılımlardır.
- Rootkit — Arka kapı oluşturmak amacıyla işletim sistemini değiştirmek için kullanılır.
- Virüs — Sisteme izinsiz işlenmiş yaptırım programlarıdır. Görünüşte pek bulunmuyor. Başka dosyaya yapışır. Öğe dosyalara bulaşmaya çalışır. Payload zamanını bekler

CamScanner ile tarandı

↳ Truva Atı
Trojen

Virüsten yeniden oluşturulmasını sağlayan virüstür.
Temiz gibi görünen programların içinde saklı kötü amaçlı kod parçacıklarıdır. Kendi kendini çoğaltabilir

↳ Solucanlar
(Worm)

Ağlardaki kötü amaçlı yazılımları kullanarak kendini çoğaltan, klonlayan kodlardır. Ağları yavaşlatır. Kendiliğinden çalışabilir

↳ Man-in-the-middle
(MITM)

Saldırganın, kullanıcının izni olmadan bir cihaz üzerinde kontrolü ele geçirmesine sebep olur.

↳ Man-in-the-mobile
(MITMO)

MITM'in bir varyasyonudur. Bu sefer mobil cihaz üzerinde kontrolü sağlamak için saldırılır.

KÖTÜ AMAÇLI YAZILIM BELİRTİLERİ

CPU kullanımında artış
Bilgisayar hızında azalma
Ağda yavaşlama
Dosyaların değişikliği, silinmesi
Bilinmeyen dosyalar, simgeler

Erişim Aktörleri

- Basit parolalar (Brute force)
- Yazılımsal hatalar
  - İşletim sistemleri
  - Buffer overflow
  - SQL injection vb.
- Aradaki adam Aktörleri (Man in the middle)
- Zorunlu Yöntemler

SOSYAL MÜHENDİSLİK

Bireyleri eylemleri gerçekleştirmeye veya gizli bilgileri ifşa etmeye yönlendirmeye çalışan bir artistik saldırısıdır.

↳ Pretexting
Saldırganın bir kişiyi ikna etmesi ve veri elde etmesi için yalan söylemesidir.

↳ Tailgating
Saldırgan güvenli bir yere yetkili kişiyi takip etmesidir.

Kimlik Avı (Phishing)
Kötü niyetli kişi, güvenilir bir karakter mail gönderiyormuş gibi görünür ve ortaya bir yem koyar. Örneğin ödül kazandınız!, der gibi.

- Wifi parolası kırma
- Sosyal Mühendislik: Parolayı bilen bir kişiye söyletilmesi
- Kaba kuvvet (Brute force): Bir world listteki tüm sifrelerin teker teker denemesi
- Ağ koklama (Network Sniffing): Parola göda düz metin olarak gidiyorsa saldırgan bunu görebilir.

CamScanner ile tarandı

Güvenlik açıklarından yararlanma — Saldırı Adımları

whois — internet veritabanı
nmap — araç

1-) Hedef sistem hakkında bilgi toplanır
- Bağlantı noktası
- Tarayıcı
- Sosyal Mühendislik

2-) Bu bilgiler doğrultusunda nasıl saldırabileceğinin planı yapılır. Hedef sistemde varsıyon analizi yapılır.

3-) Bulunan bu versiyonların, uygulamaların, güvenlik açıkları araştırılır.

4-) Güvenlik açığı bulunursa saldırgan önceden yazılmış exploit arar veya kendisi kendisi yazabilir.

DoS (Denial of Service) (Hizmet Reddi)

Bir tür ağ saldırısıdır. Ağın hizmet dışı kalmasını amaçlanmasını hedefler

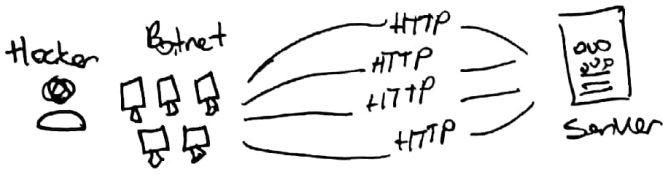
Ezici Trafik Miktarı - Overhelming Quantity of Traffic

Bir ağa, bilgisayara, uygulamaya işleyemeyeceği bir hızda ve miktarda veri gönderilmesidir.

Kötü Amaçlı Biçimlendirilmiş Paketler - Malicious Formatted Packets

Alıcıya hatalar ile dolu veri gönderildiğinde, alıcının işlemede zorlandığı durumdur.

DDoS (Distributed DoS) Attack



Dos saldırısına benzer ama birden çok kaynaktan gelir.
Bir saldırgan botnet adı verilen virüslü ara bilgisayardan oluşan bir ağ oluşturur. Enfekte olmuş bilgisayarlara zombi bilgisayar denir. Birçok zombi bilgisayara sahip olduğunda hacker Dos saldırısı için kaynak vardır ve birçok kaynaktan dos saldırısı düzenler.

SEO Zehirlenmesi

SEO Arama Motoru Optimizasyonunun kısaltılmasıdır. Web sitelerinin hangisinin daha yukarıda hangisinin daha aşağıda görüntüleneceğini belirleyen teknik bir seydir. Kötü amaçlı sitelerin SEO algoritmasına oynayarak sitesine gelecek trafiği artırmayı amaçlarlar.

CamScanner ile tarandı

KENDİMİZİ NASIL KORURUZ

+ Güvenlik duvarını açık tutun ve güncelleyin → Yazılımsal güvenlik duvarı / Yönlendirici üzerindeki güvenlik duvarı
+ Antivirüs ve Antispyware kullanın ve güncelleyin
+ İşletim sistemini ve uygulamalarınızı güncel tutun
+ Güçlü parolalar kullanın

Güvenilmeyen IoT cihazları firewall dışında IOT cihazları diğer ten cihazlardan daha çok tehdit oluşturur.

'İnternet erişimi olan IoT cihazlarında bir açık olması durumunda saldırganlar bunu rahatlıkla kullanabilir

Çözüm Yalıtılmış ağ kullanmak

Kablosuz ağları güvenli kılmak için;

- Fabrikasyon SSID'leri ve parolaları değiştirilmelidir.
- SSID'yi yayınlamamak bir seçenektir
- WPA2 şifrelemeyi etkin kılın.
- Cihaz güncellemelerini kontrol edin
- VPN kullanılabilir.
- Herkese açık wifi'lerden kaçının
- Dosya ve medya paylaşımı ile yapılandırılması veya şifreli olması önemlidir.
- Bluetooth'u kapalı tutun

Parolalar;

- Her hesabın benzersiz bir parolası olmalı
- Zayıf parollalar kullanmaktan kaçının
- Parola yöneticisi kullanabilirsiniz (Önerilmez)
+ Herhangi bir dildeki sözcük ve kelimeleri kullanmayın
+ Sözlük kelimelerin yaygın yazım yanlışlarını kullanmayın
+ Bilgisayar adlarını ve kişisel adlarını kullanmayın.
+ Özel karakterler kullanın
+ On (10) veya daha fazla karakter içeren parola oluşturun.
+ Unutma durumları için cümle kullanabilirsiniz
  → Passphrase
  + Anlamlı bir cümle
  + Özel karakter içeren
  + Ne kadar uzun o kadar iyi
  + Yaygın ifadelerden kaçının

Verilerimizi Şifrelemek (Encryption)

Şifreleme, verilerin yetkisiz taraflarca okunamayacağı şekilde dönüştürmektir.

İki faktörlü kimlik doğrulama

Fiziksel Nesne → Biyometrik tarama

VERİLERİMİZİ YEDEKLEMELİYİZ

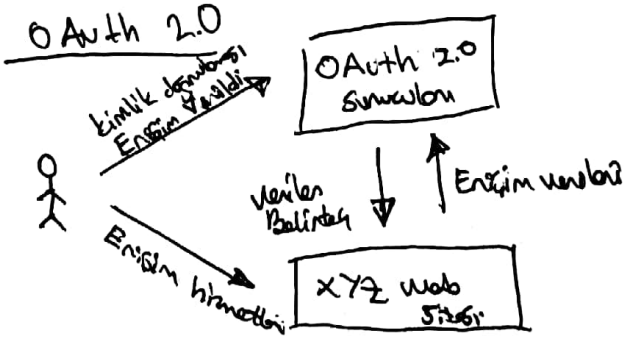
Harici Cihazlar / Bulutlar

Verileri kalıcı olarak silmek

Çöp kutusuna taşıdığımızda veya sildiğimizde, veriler sadece işletim sistemimizden erişemeyiz. Fakat adli araçlar (Forensic tool) kullanarak manyetik bir şekilde veriler okunabilir. Bunu önlemek için silinen kısmın üzerine tekrar tekrar 0 ve 1 'ler yazılmalıdır.

⊕ SDelete (Windows)
⊕ Shred (Linux)
⊕ Secure Empty Trash (Mac OS)

OAuth 2.0



CamScanner ile tarandı

KURUMUN KORUNMASI

· GÜVENLİK DUVARI TÜRLERİ

Hangi iletişimlere izin verildiğini ve aygıtlar veya ağdan izin verildiğini denetlemek ve filtrelemek için tasarlanmıştır.

Ağ Katmanı Güvenlik Duvarı
- Kaynak ve hedef IP adreslerine göre filtreleme

~~Aktarım katmanı~~

Aktarım Katmanı Güvenlik Duvarı
- Kaynak ve hedef veri bağlantı noktalarına göre filtreleme
  Hedef portlara ve bağlantı durumlarına göre

Uygulama Katmanı Güvenlik Duvarı
- Uygulama program ve hizmete dayalı filtreleme

Bağlam duyarlı uygulama güvenlik duvarı
- Kullanıcı, cihaz, rol, uygulama türü ve tehdit profiline göre filtreleme

Proxy Sunucusu

URL, etki alanı, medya vb. web içerikli istemcilerin filtrelemesi.

TERS proxy sunucusu

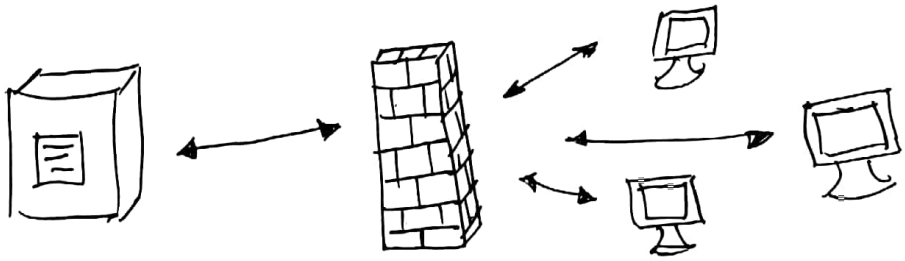
Web sunucularının önüne yerleştirilir. Ters proxy sunucuları web sunucularına erişimi kontrol, gizler, üzerindeki yükü boşaltır ve değiştirir.

Ağ adresi Çevirisi (NAT) güvenlik duvarı

ağ ana bilgisayarının özel adreslerini gizler veya maskeler

Ana bilgisayar tabanlı güvenlik duvarı

tek bir bilgisayar işletim sisteminde bağlantı noktalarının ve sistem servis çağrılarının filtrelemesi portların ve sistem çağrılarının



BAĞLANTI NOKTASI TARAMA

Ağda bir aygıtta çalışan her uygulamaya bir tanımlayıcı atanır. Bu bağlantı noktası numarası adı verilen bağlantı noktası (PORT) taraması bilgisayarda çalışan işletim sistemini ve açık hizmetleri keşfetmek için kötü amaçlı kullanılabilir, aynı zamanda sistem yöneticisi tarafından güvenlik için zararsız şekilde kullanılabilir.

NMAP (Port tarama aracı)
ZENMAP (Port tarama programı)

Bu portlar genelde;

Open veya Accepted – Açıktırlar
Closed, Denied veya Not Listning – Kapalıdır.
Filtered, Dropped veya Blocked – Belirsizdir.

Güvenlik Duvarı
İzin verilen trafiği geçiren
İzin verilmeyen trafiği geçirmeyen sistem

IDS – Saldırı Tespit Sistemi
- Ağ uyarısı oluşturur
- Algılamayı loglara kaydeder

IPS – Saldırı önleme sistemi
↳ Saldırıyı bloklar

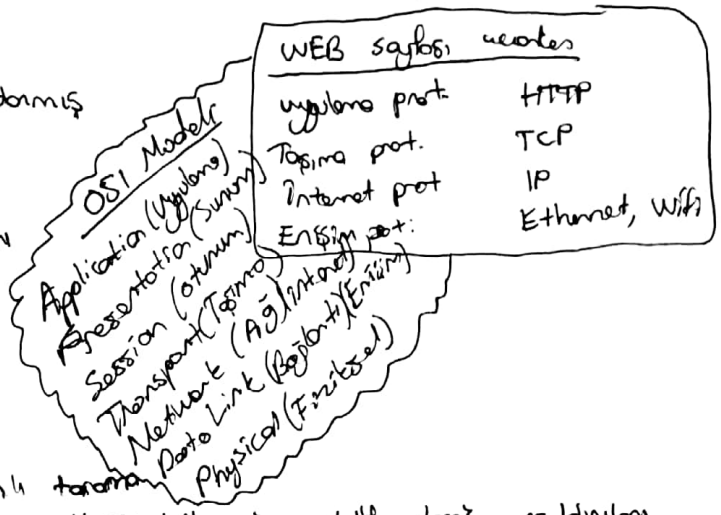
CamScanner ile tarandı

GÜVENLİK UYGULAMALARI

Güvenlik cihazları, yönlendirici veya güvenlik duvarı bir ağ aygıtına takılabilen bir kart veya kendi işlemcisine ve önbelleğe alınmış belleğe sahip bir modül gibi bağımsız cihazlar olabilir.

Yönlendiriciler
Güvenlik duvarları
IPS → Saldırı önlemeye odaklanmış
VPN
Malware / Antivirüs

Diğerleri; WEB Eposta güvenlik cihazları
Şifre çözme aygıtları
İstemci erişim
Denetim sunucuları
Güvenlik yönetim sistemleri



GERÇEK ZAMANLI SALDIRI ALGILAMA

// Edge'den uç noktasına Gerçek zamanlı tarama
Güvenlik duvarı ve IDS/IPS aygıtlarını kullanarak aktif olarak saldırıları tarama gerekli
Aktif tarama cihazları ve yazılımları, bağlam tabanlı analiz ve davranışları algılamayı kullanarak ağ anomalilerini algılamalıdır.

// DDOS SALDIRILARI VE GERÇEK ZAMANLI YANIT

ZARARLI YAZILIMLARA KARŞI KORUMA

Sıfırıncı gün saldırılarının sürekli varlığını ve uzun süre var olan gelişmiş kalıcı tehditlere (APT) karşı nasıl savunma sağlarsınız.
KURUMSAL DÜZEYDE KÖR AMAÇLI YAZILIM ALGILAMA

Ağ yöneticileri APT saldırılarına karşı gün sürekli izlemelidir.
AMP, ana bilgisayarın uç noktalarında bağımsız bir sunucu olarak değiştirilen yazılımdır.

AMP
- Güvenli Operasyon Merkez Ekibi
- Olay Müdahale Ekibi
- Tehdit Algılama Zekası
- Güvenlik Altyapısı Müh. Ekibi

EN İYİ GÜVENLİK UYGULAMALARI

Risk değerlendirmesi gerçekleştirin
Güvenlik ilkesi oluşturma
Fiziksel güvenlik önlemleri
İnsan kaynakları güvenlik önlemleri
Yedekleme yapma ve test etme
Güvenlik yamalarını ve Güncelleştirmeleri koruma
Erişim denetimlerini çalıştırma
Olay yanıtını düzenli olarak test etme
Ağ izleme, analiz, yönetim araçları uygulayın
Anti-virüsü aygıtlara uygulayın
Kapsamlı uç nokta güvenlik çözümü uygulayın
Kullanıcıları eğitin
Verileri şifreleyin

TCP Atakları
↳ SYN Flood Atağı
↳ DoS

Modem / Router

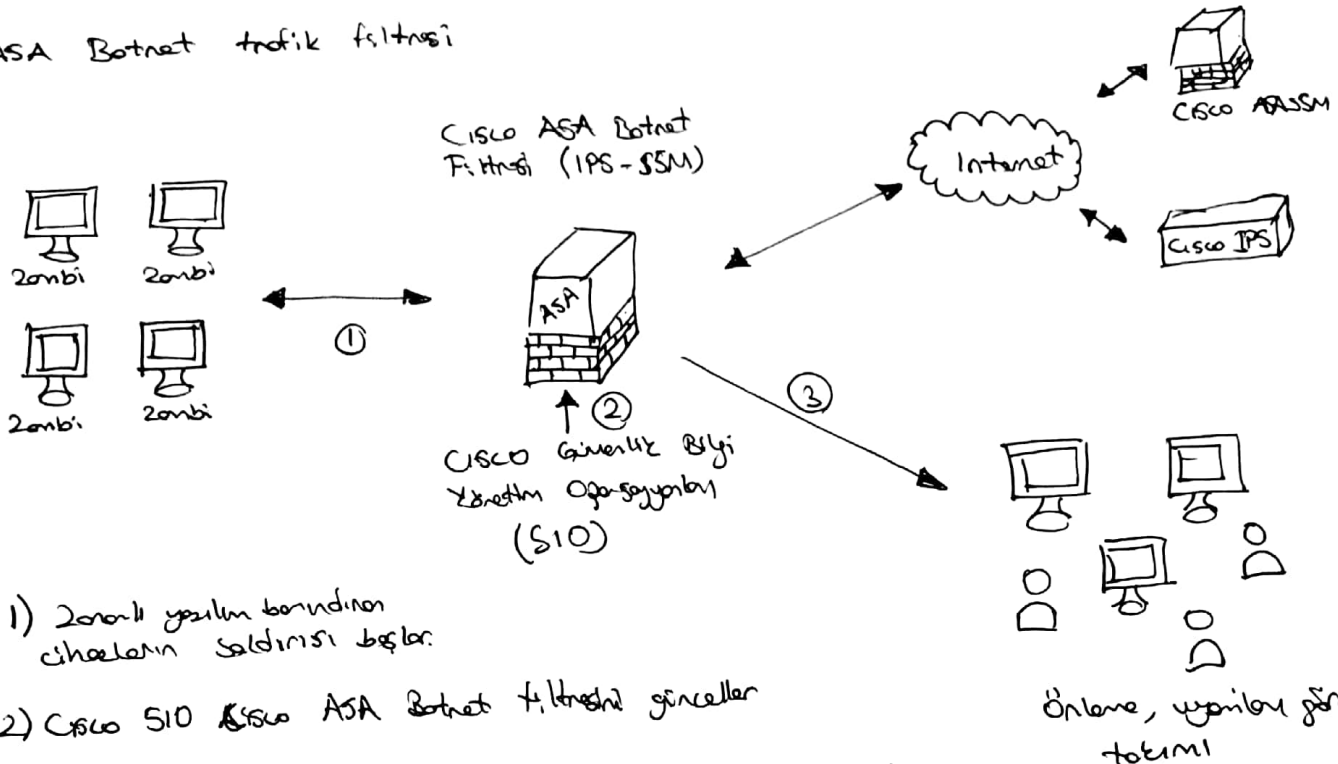
IP Atakları
↳ Ip spoofing

HTTP Atakları
↳ SQL injection
↳ DOS
↳ DDOS
↳ XSS Cross Site S
↳ :::

Data Link Atakları
↳ ARP zehirlenmesi

CamScanner ile tarandı

ASA Botnet trafik filtresi



1) Zombi yazılım bombardıman cihazların saldırısı başlar.

2) Cisco SIO Cisco ASA Botnet filtresini günceller

3) Uygulama, önleme, araştırma ve direktife için güvenlik ekiplerine gider.

SİBER SAVAŞTA ÖLÜM ZİNCİRİ
Bilgi sistemlerinin saldırısının aşamalarıdır.

1- Kaşif, Keşif → Saldırgan hedef hakkında bilgi toplar
2- Silahlanma → Saldırgan hedefe göndermek için paket oluşturur, plan yapar.
3- Teslimat → Sosyal Mühendislikle konuşturarak hedefe bu paketi yüklemeyi

amaçlar
4- İstismar → İstismar yürütülür.
5- Kurulum → Bu paket sayesinde arka kapılar açılır
6 - Komut ve Kontrol → Hedefe ilk amaçlı yazılım ve arka kapılar yüklenir. Paketin kontrolü sayesinde sistemin kontrolü ele geçirilir.
7 - Eylem → Yapacağını yapar.

SİBER TEHDİTLERİN EVRİMİ — Behavior-Based Security

İki bilgisayar arasındaki iletişimin yakalanıp analiz edilmesi sonucu herhangi bir anormali olup olmadığının araştırılmasıdır.

BAL KÜPÜ (HONEYPOT)
Siber Tehdit Savunma Çözümü mimarisi

Virüsler (1990'lar) — Savunma Antivirüs, Güvenlik duvarı = ILOVEYOU = Melissa = Anna Kournikova

Solucanlar (2000'ler) — Saldırı algılama ve önleme = Nimda = SQL slammer = Conficker

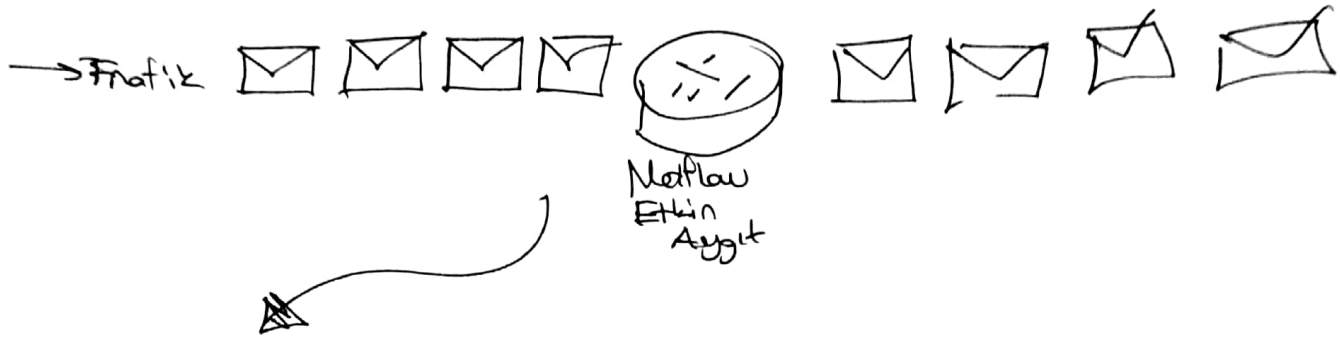
Botnetler (2010'lar) — İtibar, DLB, Uygulama farkında güvenlik duvarı = Tedrao = Rustock = Conficker

APT'ler (Yönlendirilen saldırılar) Günümüz — Gözlemleme ve toplama = Aurora = Shady Rat = Duqu

CamScanner ile tarandı

NETFLOW Akış oluşturma

Bir ağ üzerinde akan verileri hakkında bilgi toplamak için kullanılır
Netflow bilgileri ağ trafiğiniz için bir fatura gibidir
Netflow ile donatılmış güvenlik cihazları, ağa giren, çıkan ve ağ üzerinde transfer edilen veriler hakkında bilgi raporlar.



Paketi İncele
Kaynak IP adresi
Hedef ip adresi
Kaynak port
Hedef port
3. katman protokolü
Tos bayt (DSCP)
Giriş arayüzü

CSIRT Kuruluşları
Bilgisayar Güvenliği Olay Yanıt Ekibi (CSIRT)

NETFLOW PROTOKOLÜ
Paket bilgilerini alır, rapor oluşturur

Honeypotlar
Saldırganlar için ortaya yem bırakılır.

Mail Security
Web Security
DNS Security
AAA sunucusu
Ağa girmeden kimlik denetimi yapar

OLAY ÖNLEME VE ALGILAMA PROGRAMLARI

SIEM - Güvenlik Bilgileri ve Olay Yönetimi

↳ ağ üzerindeki güvenlik cihazlarından güvenlik uyarılarını günlükleri, gerçek zamanlı ve geçmiş verileri toplayan ve analiz eden programdır

DLP - Veri Kaybı Önleme Yazılımı

Hassas verilerin bir ağdan çalınmasını engellemeki için tasarlanmış yazılım veya donanımdır.

Cisco ISE ve TrustSec - Cisco Identity Service Engine

IDS - Saldırı Algılama Sistemi

Algılamak, Günlüğe kaydetmek, raporlamak

IPS - Saldırı Önleme Sistemi

(Snort)

IDS'in sadece saptadığını
IPS'in de saldırıyı önlemek için yaptığını

CamScanner ile tarandı