BSD

Pdf: 1.

Siber Güvenlik: Kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler.

Bilgi Nedir?

* İşlenmiş veriden bir konu hakkında belirsizliği azaltan kavram.

Veri - Bilgi - Özbilgi?

Genel olarak bilimin getirdiği yöntemlerden ölçme ile,
- eldeki gerçeklikten Veriye,
- ispat ile, veriden Bilgiye,
- Kavrayış ile, veriden Özbilgiye ulaşılır.

Güvenlik?
Karşılaşabilecek tehditlere karşı önlem alma.

- Bilgi Güvenliği?
- Doğruluk, güncellik, konuyla ilgili olma, bütünlük ve öz, gerçeksinimlere uyum gösterme, iyi sunulma ve fiziksel veya ırak yolu ile erişim gibi ölçütler bilginin kalitesini belirleyen etmenlerden bazılarıdır.

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

Siber bilgi güvenliği temel Hedefi

---, Kaynakların başlarına kötü bir şey gelmeden korumaktır.

Bireysel Stratejiler.
* Tehlikenin farkında olmak
* Çok katmanlı bir savunma mekanizması oluşturmak.
- Yama programı - Güçlü araçlar - Düzenlemeler.
* Sosyal medyadaki gizlilik seçeneklerini iyi değerlendirmek.
* Verilerin nerede olduğundan emin olun.

Pdf 2.:

Bilginin Belirsizlik Evreleri:

* Var haline gelmeye hazır boşlukta bulunan herşey Belirsizlik.

* Bilişim teknolojisinin açısından Veri, bir durum hakkında birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller olarak tanımlanabilir.

* Bilgi: verinin belli bir anlamı ifade edecek şekilde düzenlenmiş halidir.

* Öz Bilgi: tecrübe veya öğrenme şeklinde veya ilk gözlem şeklinde elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasıdır.

Bütünlüğün Korunması: Bilgiye ulaşımın sadece yetkili 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 Casus Yazılımlar (Malware)

Yeni kötücül yazılımlardan bir kısmı şunlardır:

* Sahte oltalama (Phishing)
* Koklayıcı (Sniffer)
* Kandırıcı (Spoofer)
* Şifre kırıcılar (Password Cracker)
* Reklam yazılım (Adware)
* Ağ taşkını (Flooder)

Kötücül yazılımların bazı bulaşma yöntemleri:

- E-posta dosya eklentisi ile e-posta'da verilen bir web adresine gidildiğinde veya doğrudan HTML içerikli e-postaların okunması ile casus yazılımların bulaşması,

- İnternet tarayıcılarında bulunan korumasızlık ve açıklardan yararlanarak kurulma.

- Özellikle internet üzerinden kullanıcıyı aldatıcı mesajlarda yanıltıp herhangi bir casus yazılımının kurulumunun başlatılması.

Kötücül yazılımların belirtileri:

- Bilgisayarın her zamanki başarımı düşüyorsa.

- İnternet üzerinde tarayıcıda istenmedik siteler açılıyorsa.

- Tarayıcıdaki favoriler kısmındaki veya yer imi bölümünde yabancı site bağlantıları eklenmişse.

- İnternete modem ile bağlanıp da büyük meblağlarda telefon faturası geliyorsa ve bunlar gibi farklı durumlar varsa büyük ihtimalle casus yazılım vardır.

Bazı önlemler:

- İşletim sis. güncellemeleri
- Anti-Spyware (Casus karşı yazılım)
- Host bloklama
- E-posta kontrolü
- Browser kullanımı
- Ofis programları
- Güvenlik Duvarı (Firewall)

Pdf 3.

Dünyadaki bilişim suçları en çok hangi ülkede?

- Türkiye, Rusya ve Brezilya

Sebep: Bilişim suçlarına olan cezaların yetersiz kalması ve yeterince uygulanmaması

Hacker Çeşitleri

- Beyaz ve Siyah olarak ikiye ayrılır.
- Ayrıca, siyah şapkalı hackerlar kendi içinde ayrılabilir.
- Script Kiddies (Lamer): Kendini birşey zanneden hacker.
- Phreakers: Santral ve telefon hatlarının açıklarını kullanan hacker.
- Crackers: PC yazılımlarını kıran ve yaygınlaştıran hacker.
- Grey Hat Hackers: Hem savunma hem de saldırı amaçlı hacker.

Sosyal Mühendislik = Akıllı insan kendi aklını kullanır. Daha akıllı olan insan ise hem kendi hem de başkalarının aklını kullanır.

BT alanında yeterli teknik bilgiye sahip olup açık aramaktan ziyade insanların zayıf ve bilgisiz noktalarını kötü niyetli kullanan yaratıktır.

Pdf 1.

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. TCP/IP mesajlarını analiz eden bir programdır.

Amaçları:
- Şebeke problemleri sorun çözme. ✓
- Güvenlik testi ✓
- Protokollerde hataları onarmak. ✓
- Ağ problemlerinin içindeki bilgileri öğrendik. ✓

Wireshark bileşenleri:

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

Wireshark kullanımı ile örnekler
- Ağ trafik tespiti
- Veri madenciliği
- Saldırı tespiti
- DoS ataklarını bulma tespiti ✓

Wireshark bileşenleri
Wireshark iletişim ağının iç yüzünde neler old. kavramamızı sağlar.

Veri Şifreleme (Wireshark)
- Şifreleme
  Kullanılan algoritma
  DES - 54 bitlik anahtar
  - 64 bitlik bloklar.

Pdf 5.

Kriptasistemler

→ Kimlik doğrulama ve şifreleme verinin güvenliğini sağlamaya yarayan birbiriyle bağlantılı iki teknolojidir.

→ Kimlik doğrulama, haberleşmede her iki taraftaki bulunanların ne söylüyorlar ise doğru olmasını sağlama süreci.

→ Şifreleme ise iletişim sırasında verinin hem güvenliğini sağlamak hem de değiştirilmesini önlemeye yönelik işlemdir.

Aşağıdaki protokoller açık metin kullanır

→ FTP (File Transfer Protokol), IMAP (Internet Message Access Protokol), SNMP (Simple Network Management Protokol) doğrulama işlemi açık metin ile yapılır.

→ SMTP (Simple Mail Transfer Protokol) Posta mesajlarının içeriği açık mesaj olarak değitilir.

- HTTP (Hyper Text Transfer Protokol) Sayfa içeriği ve formlardaki bilgilerin içeriği açık metin olarak gönderilir.

Ağ üzerinden Yapılan Saldırı Türleri

✓ İfşaat - Açığa Çıkarma (Disclosure)
✓ Sıra değiştirme
✓ Trafik Analizi
✓ Zamanlamayı Değiştirme
✓ Tekrarlı gönderme (Masquerade)
✓ İnkarcılık
✓ İçeriği Değiştirme

Şifreleme Nedir?

Şifrelenecek mesaj düz-metin (plaintext)

Veriyi şifeleyken ve çözerken kullanılan matematiksel metoda şifreleme algoritması denir.

Şifreleme ve çözme genelde anahtar kullanılarak yapılır.

Şifreleme Algoritmasının Performans Kriterleri
- Şifrenin uzunluğu ✓
- Zaman karmaşıklığı ✓
- Bellek karmaşıklığı ✓
- Bu algoritmaya dayalı şifreleme uygulamalarının esnekliği ✓

Şifreleme Algoritmaları
- Simetrik (Hızlı, daha az güvenli, tek anahtar)
- Asimetrik (Daha karmaşık, 2 anahtar, daha güvenli)

Simetrik Şifreleme:

→ Bu algoritmada şifreleme ve şifre çözmek için 1 tane gizli anahtar kullanılmakta.
→ Kullanılan anahtar başkalarından gizlidir. ve şifreleme yapan ile çözecek kişide arasında anlaşmış ortak bir anahtardır.

Avantajları

* Hızlı olması (Asimetriğe görede daha hızlıdır.)
* İçerdiği basit işlemlerden dolayı elektronik cihazlarda uygulamak daha kolaydır.
* Simetrik algoda kullanılan anahtarın boyu ve dolayısıyla bit sayısı çok daha küçüktür.

Kuvetli yönü
- Hızlı
- Donanımla birlikte kullanılabilir.
- Güvenli

Zayıf Yönü
- Güvenli anahtar dağıtımı zor.
- Kapasite sorunu
- Kimlik doğ. ve bütünlük ilkeleri hizmetlerini güvenli bir şekilde gerçekleştirmek zor.

2'ye Ayrılır.

1. Blok Hafızasız
→ Veriyi bloklar halinde işler.
→ Bazen bağımsız bazende birbirine bağlı olarak şifrelenir.
→ İç hafıza yok. (Hafızasız Şifreleme)
→ Bütünlük kontrolü gerektiren uyg. tercih edilir.

2. Dizi
→ Veriyi bir bit dizisi olarak alır
→ Bir üreteç aracılığı ve anahtar yardımıyla istenilen uzunlukta kayan anahtar adı verilen bir dizi üretilir.
→ Kayan anahtar üretimi zamana bağlı ve bu yüzden hafızalı şifreleme denir.
→ Telsiz haberleşmesi gibi gürültülü ortamlarda ses iletimini sağlamak için kullanılır.

Simetrik Şifreleme - DES

* DES yapısı blok şifreleme örneğidir.
* Şifrelenecek olan metni parçalara bölerek (blok) her parçayı birbirinden bağımsız olarak şifreler. ve şifrelenmiş metni açmak tarafa aynı işlemi blok üstünde yapar.
* 64 bitlik
* 64 bitlik veriyi 56 bitlik anahtar kullanarak şifreler.
* Dezavantajı anahtar uzunluğunun 56 bit olmasıdır.
* Brute force saldırısında yetersiz.
* Daha güvenli olması için DES, Triple-DES olarak geliştirildi.

Triple-DES
Bankacılık sistemlerinde kullanılmakta.
Şifreleme, deşifreleme, şifreleme.
Standart DES'in 112 veya 168 bitlik 2 veya 3 anahtarla çalışması.

Diğerleri ise
IDEA
Twofish
SRDN
AES
RC4
MD5
SHA

Asimetrik Şifreleme
* 2 farklı anahtar
* Bu sistemde bir tane şifreleme için (public key) ve bundan farklı olarak bir tanede şifre çözmek için (private key) anahtar.
* Çok büyük asal sayılar kullanılır.

Asimetriğin;

Kuvvetli Yönleri:

* Kriptografinin ana ilkeleri olarak sayılan - bütünlük, kimlik doğrulama ve gizlilik hizmeti güvenli şekilde sağlanır.
* Anahtarı kullanıcı belirleyebilir.

Zayıf Yönleri:

* Şifrelerin uzunluğundan dolayı yavaş
* Anahtar uzunlukları bazen sorun çıkartabilmesi

Avantajları;

⇒ Simetrik şifrelemeye göre kurulması daha zor.

⇒ Private - key'lerin karşılıklı aktarılması gerekmez. Yani simetrikteki anahtar değişim problemi çözülmüş olur.

⇒ Public Keylerin bize şifreli mesaj göndermek isteyenler tarafından bilinmesi gerektiğinden bu anahtarlar internette bir sunucu ile rahatça değiştirilmektedir.

⇒ 2 anahtarla şifrelemeden dolayı inkar edememeyi sağlar.

Dezavantajları.

⇒ Anahtarları kullanarak bilgileri çözme işlemlerinde CPU zamanının çok fazla olması.

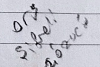
⇒ Bu zaman ileti uzunluğu ile üssel olarak artmakta.

Diffie Helman
RSA
DSA
ECC

İletişim Protokollerini Kullanan Saldırılar.

1. Internet Protokol Adresi - Ip Adresi

TCP/IP standartını kullanan bir ağdaki cihazların birbirini tanımak, iletişim kurmak ve veri haberleşmesinde bulunmak için kullandıkları noktalara aşağıdaki 4 sayıdan oluşur.



IP Protokol Türleri

2 tür internet protokolü bulunur.

Ipv4 : Günümüzde kull. olan standart standart int. protokolü.
* 32 bittir.

Ipv6 : Artan ağ kullanıcısı sayısına bağlı olarak daha büyük bir IP adresine ihtiyaç duyulmuştur.
* Bu ihtiyacı karşılamak için ve Ipv4'ün eksikliklerini gidermek amacıyla 128 bitten oluşur.

IP Sahteciliği (IP Spoofing)
* Spoofing IP paketlerinin yanlış kaynak adres kull. gönderilmesidir. Bu işlem;
- Saldırıdaki kişinin IP adresini gizlemesi, yanlış taraf yada kişiyi saldırı yapan olarak göstermesi
- Güvenilir bir kullanıcı gibi görünmesi yanında network trafiğini izlemesi.

Korunma yöntemleri;
→ Hedef IP ve MAC kontrolünün yapılması.
→ Güvenlik duvarı
→ Paket filtreleme
→ Şifreleme yöntemleri

TCP SYN PAKETİ AKIŞI SALDIRILARI

* TCP/IP servislerini devre dışı bırakmak için.
* TCP bağlantı temelli
* İletişim kuran 2 bilgisayar paketlerini önceden kurulmuş bir hat üzerinden aktarır

P Servis Durdurma Saldırıları

(Smurf), saldırgan hedef bilgisayardan ping isteğinde bulunur.

P parçalama Saldırıları

MTU Nedir?

- MTU değeri bir ağa girişteki maks kapasiteyi belirler.
- MTU değerleri farklı iki ağ arasında geçişlerde eğer ilk ortamın MTU değeri daha büyükse IP paketlerinde yeni girilecek ortama göre parçalama işlemi yapılır.

UDP Portlamadan Saldırılar

* UDP, TCP/IP protokol grubunun iki aktarım katmanı protokolünden birisidir.
* Ağ üzerinden paketi gönderip gidip gitmediğini takip etmez ve paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yok.
* Bilgisayarın servisini kilitlemeyi ve performansını kötüleştirmeyi başarabilir.

ARP Saldırıları

IP adreslerini fiziksel adrese dönüştürmek için kullanılır.
Bir paketin nereye gideceğini fiziksel adresi belirler.

Önlem Olarak: ✓ Statik veya dinamik ARP komutları kullanım
✓ ARP sınırlama

Final

Bsg.pptx okuyt

0. Gün Saldırıları (Zero-Day Attacks)

Yazılım veya sistemlerdeki keşfedilmemiş güvenlik açıklarından yararlanılan saldırılardır.

Tehlike Sebepleri:
* Açığın bilinmemesi ve tespit edilememesi. ✓
* Geleneksel güvenlik kısıtlamalarının etkisizliği. ✓
* Büyük farklılık etki alanı ve kritik hedefler. ✓

Örnekler: WannaCry (2017), Stuxnet (2010), Google Chrome Açığı (2021)

Korunma yöntemleri:
- Güncellemeler - siber güvenlik yazılımları - ağ segmentasyonu - Zero Trust yaklaşımı - eğitim ve geçici

TCPDump:

Unix/Linux sistemlerinde ağ analizi için kullanılan bir komut satırı aracı.

Özellikler
* Paket yakalama, analiz ve raporlama
* Filtreleme seçenekleri ve düşük sistem seçenekleri

Kullanım Alanı:
* 0. Gün saldırıları gibi anormal ağ davranışlarını tespit etmek
* Saldırı değişikliklerinin belirlenmesi ve logları analiz edilerek önlemlerin iyileştirilmesi

Sık Kullanılan TCPDump Parametreleri:
* -i : esnek bir ağ kesinti dinleme
* -n : DNS çözümlemesini devre dışı bırakma
* -t : Zaman damgası gösterimi devre dışı.
* -w : Paketleri kaydetme.
* -c : Yakalanacak paket miktarının belirlenmesi
* -s : Paket boyutunu ayarlama
* -v : Ayrıntılı loglama, ek bilgilerle değişim analizi

Kimler Yapar?
1. Siber Suçlular
2. Hacktivistler
3. Kurum Casusları
4. Siber Savaş Aktörleri

DDoS.pptx

DoS ve DDoS Saldırıları:

Amaç: Hedef sistemleri aşırı yüklerek hizmetlerin erişilemez hale getirmeyi sağlamaktır.

Farkları:

- DoS = Tek bir cihazdan gelen saldırılar, daha küçük ayarlar ve kolay tespit edilebilir.

- DDoS = Botnet adı verilen ele geçirilmiş içeriğin gelen büyük değişiklik saldırıların, tespiti ve savunması zordur.

Botnet ve Zombi Bilgisayarlar:

Botnet: Zararlı yazılımlarla birlikte bilgisayarlarla oluşturulan ağ.

Kullanımı: DDoS saldırılarını güçlendiriyor, fidye patlaması (RDoS), spam gönderimi ve veri hırsızlığı.

DDoS Saldırı Türleri:

1. Taşkın = TCP SYN Taşkını, UDP Taşkını, ICMP Ping Taşkını
2. Amplifikasyon = DNS ve NTP Amplifikasyonu
3. Bağlantı Tükenmesi = Slowloris, HTTP Flood
4. Parçalanma = Gözyaşı Saldırısı.

Savunma Türleri (TCP/IP)

1. Güvenlik Duvarları = Şüpheli Parçacık filtreleri

2. Trafik Şekillendirme = Aşırı yüklenmeyi azaltır.

3. CDN ve Yük Dengelemeye = Trafiği dağıtarak yükü hafifletir.

4. Gerçek Zamanlı İzlemeye = Anormal trafik tespiti sağlar.

5. Düzenli Güncellemeler = Güvenlik açıklarını kapatır.

6. Bulut Tabanlı Koruma = Trafiği filtreleyerek saldırıların süresini azaltır.

Örnekler =

- Mirai Botnet

- Türk Telekom

GPS - Spoofing Slayt

GPS Nedir?

ABD hükümetine ait, USAF tarafından işletilen uzay tabanlı radyo - navigasyon sistemi

Bölümler = Uzay Segmenti, Kontrol Segmenti, Kullanıcı Segmenti

Kullanım Alanları
- Ulaşım
- Havacılık
- Denizcilik
- Askeri
- Spor
- Sivil

GPS Spoofing Nedir?

Cihazların konum veya zaman bilgilerini manipüle etmek için sahte GPS sinyalleri yayma işlemi.

Amaç = Cihazları yanlış yönlendirme, sistemleri sabote etme, stratejik avantaj

Spoofing nasıl çalışır?

1. Radyo Sinyali Yayma: Sahte sinyallerle gerçeğini bastırma
2. Navigasyon mesajı taklidi: Gerçek sinyalleri taklit ederek yanıltması
3. Zamanlama Değişikliği: Sinyallerin zaman dalgalarını değiştirme

Kullanılan Araçlar ve Teknikler:
- Radyo frekansı vericileri (HackRF One, USRP)
- Yazılım tabanlı araçlar (GPS-SDR-SIM, GNSS-SDR).
- Antenler, amplifikatörler, GPS simülatörleri

Spoofing Türleri:
1. Statik: Sabit bir yanlış konum

2. Dinamik: Değişen yanlış konum.

GPS spoofing

Kullanım Alanları:
- Askeri : Hedef belirleme, takip.
- Sivil : Trafik kontrol
- Endüstriyel : Dronların sahte konumlara yönlendirilmesi.

Riskler:
* Yanlış yönlendirme, kritik sistemlerin çökmesi
* Otonom sistemlere tehdit, kamu güvenliği riski.

Korunma Yöntemleri:
- Kriptografik doğrulama : GPS sinyallerine şifreleme eklemek
- Farklı Sistemlerle entegrasyon : GLONASS, Galileo gibi alternatif sistemler
- Sinyal Analizi : Uydu verilerindeki tutarsızlıkları belirlemek
- Eğitim ve Farkındalık : Kullanıcıları bilinçlendirmek.

İzlenecek Çözümler:
Kuantsal Şifreleme :
Yapay Zeka Destekli Sinyal Analizi
Hibrit Sistemler

İstihbarata Blockchain Teknolojisinin Kullanımına - Slaytı

Tanım ve Avantajlar

Blockchain : Merkezi olmayan bir yapıda, verilerin kronolojik ve değiştirilemez şekilde kaydedilmesini sağlayan dijital defter teknolojisi.

Avantajları:
+ Veri güvenliği
+ Şeffaflık
+ Küresel İşbirliği
+ kimlik doğrulama
+ Erişim yönetimi

İstihbaratta Kullanımı:
* Veri Güvenliği = Merkezi olmayan yapısıyla verilerin manipüle edilmesini engeller, güvenli veri paylaşımını sağlar.
* Askeri İstihbarat = Güvenli veri paylaşımı, veri bütünlüğü, izlenebilirlik ve yapay zeka ile entegrasyon gibi alanlarda blokchain kullanılır.
+ Zorluklar = Eski sistemlerde entegrasyon, ölçeklenebilirlik sorunları, eğitim ve maliyetler.

lockChain kullanım Örnekleri:

1. Askeri Uygulamalar: Veri güvenliği, hızlı karar alma, ve kritik dağıtım süreçlerinde verimlilik sağlanır.
2. Ülkeler Arası İşbirliği: Blockchain, istihbarat paylaşımı ve güvenli iletişim için uluslararası işbirliğini arttırır.

Sonuç:

Blockchain, istihbarat ve askeri alanda veri güvenliği, şeffaflık ve operasyonel verimlilik sunar. Ancak, teknolojinin benimsenmesi için eski sist. entegrasyon, eğitim ve maliyet sorunlarının çözülmesi gerekmektedir.

Siber Güvenlik ve Yapay Zeka - Özet - slayt. 2. GÜN

Yapay zeka ile Güçlendirilmiş Güvenlik Çözümleri

1. Güvenlik Duvarları: AI destekli sistemler anormal ağ trafiğini sürekli analiz ederek güvenliği arttırır.
2. Anomali Tespiti: AI, normalden sapmaları belirleyerek hızlı müdahale sağlar.
3. İzleme Sistemleri: Potansiyel tehditleri gerçek zamanlı tanımlayıp yanıt verir.

Siber Tehditler ve AI tabanlı Çözümler

* Zararlı yazılımlar: AI, malware türlerini hızlı ve doğru sınıflandırır.
* Veri ihlalleri: AI çözümleri, veri ihlalleri öncesi ve sonrasında etkili yanıtlar sunar.
* Phising Saldırıları: Yapay zeka, şüpheli e-postaları analiz ederek kullanıcıları korur.

AI ile Malware Sınıflandırma

Malware türleri: Virüs, truva atları, solucanlar ve fidye yazılımları gibi farklı kategorilere ayrılabilir.

Yapay Zeka Destekli Siber Saldırılar

* DDoS Saldırıları: AI destekli saldırılar daha karmaşık hale gelerek savunmayı zorlaştırır.

* Deepfake Dolandırıcılığı: Sahte video konferanslarla yüksek miktarda para transferleri yapabilir.

* Kaba Kuvvet: AI algoritmaları, parolaları hızlıca tahmin ederek kimlik bilgilerini ele geçirebilir.

Başarı Hikayesi:
Darktrace: Anomali tespitiyle veri ihlali önlenir.
Zoogle: AI, günlük 100 milyonun üzerinde oltalama (phising) girişimini engeller.
Cylance: 0 gün saldırılarını makine öğrenimi ile tespit ederek kritik yapıyı korur.

Avantajlar

1. Verimlilik = Oto. süreçlerle güvenlik yönetiminde etkinlik artar.
2. Doğruluk = AI, verileri inceleyerek daha yüksek doğruluk oranları sunar.
3. Hız = Anlık geri dönüşlerle tehtidlere hızlı yanıt sağlanır.

Zorluklar:

* Saldırganların AI Kullanımı: AI'ı kötüye kullanarak sofistike saldırılar düzenlenir.
* Yanlış Pozitifler / Negatifler: AI sist. tehtidleri yanlış sınıflandırabilir.
* Eğitim Verisi Eksikliği: Kaliteli veri eksikliği, AI'nin doğru çalışmasını engelleyebilir.

Kritik Altyapılarda Siber Güvenlik - Özet (Okyt)

Siber Güvenlik ve Kritik Altyapı Tanımı:

Siber Güvenlik: Bilgisayarlar, ağlar, yazılımlar ve verileri dijital tehditlerden koruma.

Kritik Altyapı: Ekonominin ve devletin sağlıklı işlemesi için önemli olan fiziksel ve siber sistemler.

Kritik Altyapı Kullanımı ve Örnekler:

1. Enerji, Telekomünikasyon, Sağlık, Finans, Ulaşım ve Savunma sektörleri kritik yapılara örnektir.

2. ABD ve Türkiye'deki Kullanımı: SCADA sistemleriyle enerji tesisleri gibi altyapılar kontrol edilir.

Kritik Yapılara Yönelik Saldırılar:

1. Siber Saldırılar: Sistemleri çökertmek veya bilgi çalmak amaçlanır.

2. Fiziksel Saldırılar: Altyapıya doğrudan zarar verme

3. DDoS Saldırılar: Aşırı yükleme yaparak hizmetleri kesintiye uğratma

4. Tedarik Zinciri Saldırıları: Dolaylı erişim sağlama

5. Enerji Altyapısına Saldırılar: Elektrik kesintileri yaratma.

6. Su ve Atık Sist. Saldırıları: Su temini ve arıtmayı sabote etme

7. Ulaşım Altyapısı Saldırıları: Ulaşımı engelleme ve kaos yaratma.

Kritik Altyapı Güvenliği

Ulusal Politikalar: Kritik altyapıların korunması için ulusal pol. ve mevzuatlar gerekli.
Teknik Önlemler: SCADA sist. güvenlik açıkları düzenli izlenmeli, milli yazılım çözümleri geliştirilmelidir.
İş birliği ve Eğitim: Uluslararası işbirliği ve kullanıcıların bilinçlendirilmesi önemlidir.

Bal Küpü ve OSI Katmanı Temelli Saldırılar - Özet (Sleyt)

Bal Küpü (Honeypot) Nedir?

Gerçek bir sistem gibi davranarak saldırganların dikkatini çekip davranışlarını izlemeyi amaçlayan güvenlik mekanizması.

Amaç: Saldırganların aktivitelerini ve motivasyonlarını anlamak, güvenlik açıklarını tespit ederek savunma stratejileri geliştirmek.

Çalışma Prensibi: Saldırganları cezbetmek, aktivitelerini izlemek ve veri toplamak.

Bal Küpü Türleri:
1. Düşük Etkileşimli Honeypotlar: Saldırganlarla sınırlı etkileşim sağlar, temel saldırıları tespit eder.
2. Orta Etkileşimli Honeypotlar: Daha fazla etkileşim sunar, saldırganların komutlarını ve araçlarını analiz eder.
3. Yüksek Etkileşimli Honeypotlar: Gerçek sistem gibi davranır, karmaşık saldırıları analiz eder.
4. Üretim ve Araştırma Honeypotları: Gerçek sistemleri korumak veya saldırganların yöntemlerini analiz etmek için kullanılır.

OSI Katmanlarına Göre Siber Saldırılar (Donanım ve Yazılımların birbiriyle uyumlu)
1. Fiziksel Katman: Kablo kesme, elektromanyetik parazit, donanım manipülasyonu gibi saldırılar.
2. Veri Bağı Katmanı: MAC flooding, ARP spoofing gibi yöntemler
3. Ağ Katmanı: IP spoofing, DDoS saldırıları, Man-in-the-Middle saldırıları.
4. Taşıma Katmanı: SYN flooding, TCP reset saldırıları.
5. Oturum Katmanı: Oturum kaçırma.
6. Sunum Katmanı: Kod enjeksiyonu.
7. Uygulama Katmanı: SQL injection, XSS, DDoS saldırıları.

Honeypotların Avantaj ve Dezavantajları.

Avantaj: Gerçek zamanlı veri toplama, düşük yanlış alarm oranı, ekonomik çözüm.

Dezavantajları: Tespit edilme riski, bakım zorluğu, izolasyon gereksinimi.

Sızma Testi - Özet (Slayt.)

Sızma testinin Tanımı ve Önemi:
Sızma testi, sist., ağların veya uygulamaların güvenlik açıklarını tespit etmek ve kontrol sağlamak amacıyla yapılan simüle edilmiş bir siber saldırıdır.

Önemi; Gerçek saldırganlardan önce güvenlik açıklarını belirlemek, sistem direncini ölçmek ve çalışanların güvenlik farkındalığını artırmak için kritik öneme sahiptir.

Sızma testi aşamaları

1. Bilgi Toplama (Bilgi edinme)
2. Network Haritalama (Zayıf nokta belirleme)
3. Sınıflandırma (Açık portları, servisleri ve zafiyetleri analiz etme)
4. Sömürme (Zafiyetleri kullanarak sızma)
5. Ayrıcalık Yükseltme (Daha derin erişim)
6. İz Temizleme (Yapılan eylemlerin izini temizleme)
7. Raporlama (Bulguların ve çözüm önerilerinin detaylı şekilde sunulması)

Sızma Türleri

* Bilgi Seviyesine Göre:
  - Black Box (Kara Kutu): Sist. hakkında hiçbir bilgi verilmez.
  - White Box (Beyaz Kutu): Tüm sist. bilgileri sağlanır.
  - Gray Box (Gri Kutu): Sınırlı bilgi sağlanır.

* Hedef Alanına Göre:
  - Network, Web, Mobil uyg., Sosyal Müh. vs.

Kullanılan Araçlar
* Bilgi Toplama = Nmap, Whois
* Zafiyet tarama = Nessus
* Web uygulamaları = Burp Suite, OWASP ZAP.
* Kablosuz Ağ = Aircrack-ng.
* Sömürme = Metasploit
* Şifre Kırma = John the Ripper, Hashcat
* Ağ Trafiği Analizi = Wireshark
* Sosyal Mühendislik = SET

Etik Sızma Testi Prensipleri:
- Etik ve Yasal Çerçeve: Yasal yetki alınarak test yapılmalıdır.
- Gizlilik: Test sırasında toplanan veriler korunmalıdır.
- Hedef Odaklılık: Sistemleri güçlendirmeye yönelik testler yapılmalıdır.
- Raporlama: Sonuçlar açık ve anlaşılır şekilde sunulmalıdır.

Karşılaşılan Zorluklar:
- Sistemlere Zarar Verme Riski: Sızma testi sırasında sistem çökebilir.
- Eksik veya Yanıltıcı Sonuçlar: Yanlış pozitif veya negatif sonuçlar.
- Hukuki ve Etik Sorunlar: İzinsiz erişim gibi etik ihlaller.
- Zaman ve Kaynak Kısıtlamaları: Sınırlı kaynaklarla tam analiz yapılamaz.

SQL Injection ve XSS Saldırıları - Özet

SQL Injection: Kötü niyetli kullanıcıların bir web uygulamasının veri tabanı sorgularını manipüle ederek veri tabanına yetkisiz erişim sağlamasına neden olan bir güvenlik açığıdır.

Amaç: Veri çalmak, veri silmek, değiştirmek veya sist. kontrolü sağlamak

Türleri:
1. Classic SQL Injection: Doğrudan zararlı komutların eklenmesi
2. Union-Based SQL Injection: İki sorgunun birleştirilmesi
3. Blind SQL Injection: Doğru/Yanlış cevaplarla veri tabanı yanıtlarının analiz edilmesi.
4. Error-Based ": Hatalardan faydalanarak bilgi elde etme
5. Time-Based ": Sunucu yanıt sürelerine dayanarak analiz.
6. Second-Order ": Veri tabanına kaydedilen zararlı kodların daha sonra tetiklenmesi
7. Out-of-Band ": DNS veya HTTP gibi protokoller aracılığıyla yanıt elde edilmesi.

Korunma Yöntemleri: Parametrik Sorgular kullanımı, Web Uyg. Güvenlik Duvarı kullanımı, giriş doğrulama ve temizleme mekanizmaları.

XSS (Cross-Site Scripting)
XSS, web sitelerinde kullanıcıların tarayıcılarına zararlı JS kodlarının enjekte edilmesiyle oluşan bir güvenlik açığıdır.
Türleri:
- Stored XSS: Zararlı kodun veritabanına kaydedilerek kalıcı hale gelmesi
- Reflected XSS: " " anlık olarak çalıştırılması.
- DOM-Based XSS: " " DOM üzerinde çalıştırılması.

XSS Saldırı Tehlikeleri:
Kullanıcı oturumlarının ele geçirilmesi
Zararlı yazılım yüklenmesi
Sahte pop-uplar aracılığıyla bilgi çalma

Korunma Yöntemleri: Kullanıcı verilerini doğrulamak ve filtrelemek, HTML özel karakterlerini kaçırmak, Content Security Policy kullanımı.

Örnek Saldırılar
* XSS: British Airways, eBay gibi platformlarda XSS açıklarından yararlanılarak kullanıcı verileri çalındı.
* SQL Injection: Guess.com, British Royal Navy, Yahoo gibi platformda SQL Injection saldırıları ile büyük veri ihlalleri gerçekleşti

Sonuç
XSS ve SQL Injection saldırıları, webde en sık karşılaşılan güvenlik açıklarındandır ve ciddi veri ihlallerine yol açar. Bu saldırılardan korunmak için kullanıcı girdilerinin doğru şekilde doğrulanması, parametrik sorguların kullanılması ve modern güvenlik araçlarının entegrasyonu kritiktir.

Ödev 3

Kriptanaliz - Özet (Slayt)

Kriptanaliz, şifrelenmiş metinlerin çözümünü araştıran kriptoloji dalıdır.

Amacı, şifreli metinlerden mümkün old. fazla bilgi toplamak

Hedefi = Şifreleme işleminin şifrelenmesi ve belirli şifreli mesajlar için anahtarların çözülmesidir.

Önemi = Kriptanaliz, bilgi güvenliği stratejilerini elde etmek ve elde edilen sonuçların sonuçları için kritik bir disiplindir.

Kriptanaliz Teknikleri

1. Kaba Kuvvet : Tüm olası anahtar kombinasyonlarını deneyerek şifreyi çözme yöntemi.
2. Sözlük Saldırısı : Önceden belirlenmiş bir kelime listesi kullanılarak şifreyi kırmaya çalışır.
3. İstatiksel Analiz : Şifreli metindeki karakterlerin özelliklerini inceleyerek şifreyi çözme.
4. Düz Metin ve Seçilmiş Düz Metin Saldırıları : Şifrelemenin zayıflıklarını tespit etmek için düz metinlerle yapılan saldırıdır.
5. Seçilmiş Şifreli Metin Saldırısı : Ayrıntılı şifreli metinlere karşılık gelen düz metinler kullanılarak şifreyi çözme.
6. Doğrusal Kriptanaliz : Şifreleme işlemlerinin doğrusal doğrultulu inceleyerek anahtarları belirleme.
7. Yan Kanal Saldırıları : Donanım emisyonları gibi dolaylı etkileri izleyerek bilgi toplama.

Uygulama Alanları

- Siber Güvenlik : Ağ güvenliği, veri şifreleme sist. ve güvenlik protokollerini değerlendirilmesinde kullanılır.
- Endüstriyel Uygulamalar : Finansal Sistemler, telekominikasyon ve savunma amaçlı verileri ele etmek için kullanılır.
- Eğitim ve Araştırma : Yeni güvenlik açıklarının belirlenmesi ve kripto analiz tekniklerinin geliştirilmesi için incelemeler yapılır.

Güncel Gelişmeler

- Kuantum Kriptanaliz : Kuantum bilgisayarların, geleneksel şifreleme yöntemlerini kırabilme potansiyeli vardır. Kuantum sonrası kriptografi, bu tehtidlere karşı yeni çözümler sunar.

Sonuç :

Kriptanaliz, dijital güvenliğin sürekliliğinde vazgeçilmezdir. Kuantum bilgisayarlar ve yapay zeka teknolojileri, kriptanaliz tekniklerinin sürekli güncellemesini gerektirir.

Kuantum Kriptografi - Özet

Tarihçe = 1960 - 1990'lar Stephen Wiesner

Kuantum Kriptografi: Nedir?

Kuantum mekaniğinin temel prensiplerine dayalı daha güvenli iletişim sağlar.

Kuantum anahtar dağıtımı (QKD) ile güvenli anahtar paylaşımı yapılır. Dış müdahale anında tespit edilir.

Temel Prensipler

- Kuantum belirsizlik ilkesi: Bilgiye dış müdahaleler anında fark edilir.
- Süperpozisyon ve Dolanıklık: Bilgiyi korumak için kuantum fiziğin özelliklerini kullanır.

Avantajı

* Kuantum bilgisayarların bile aşamayacağı bir güvenlik seviyesi sunar.
* Dinleme girişimlerini anında tespit eder.

Dezavantajları ve Sınırlamaları

* Teknoloji henüz gelişme aşamasında, altyapı ve maliyet sorunları var.
* Uzun mesafeli iletişimde zorluklar.

Şifreleme - Özet (Slayt)

Şifrelemenin Çalışma Prensibi

1. Birdi = şifrelenmesi istenen veri
2. Şifreleme = Verinin şifrelenmesi
   → Simetrik : Aynı anht. hem şifreleme hemde çözmek için kullanılır
   → Asimetrik : Açık anht. ile ayrı, özel anht. ile aynı şifrelem 4.
3. Şifreli veri = Doğru anahtar ile çözüm.
4. Şifre çözme = Verinin orj halne dönüştürülmesi

RSA = Asimetriktir. Özel anahtar sahibinde kalır.

Etik ve Yasal Boyutlar

Yasal = GDPR, CCPA gibi düzenlemelerde veri sağlama koşulunu sağlar.
Kötüye Kullanım = Bank Web'de yasadışı faaliyetler ve fidye yazılımı saldırıları gibi kötü niyetli kullanım örn. verdir

---

Dinamik Anahtar Değişimi

Dinamikler arası Değişim

* Her girişte farklı bir anahtar oluşturulur Verilerin güvenli şifrelenmesi ve uygulanması için gereklidir.

Dinamik Anahtar Değişim Türleri

1. Seçici Anahtar Değişimi = Her kullanıcı hesabında yeni anahtar oluşturulur. (DHE)
2. Oturum Tabanlı // = Her oturum için anahtar üretilir (TSL / SSL)
3. Zamana Dayalı // = Anahtarlar belirli zaman aralıklarıyla değiştirilir
4. Anahtar Döndürme = Sabit anahtarlar periyodik olarak yenilenir.
5. Hibrit Anahtar Değişimi = Simetrik ve Asimetrik şifreleme yöntemlerini birleştirir.

Kullanım Alanları

→ VPN ve Ağ Güvenliği (VPN bağlantılarında)
→ E-ticaret (Kredi kartı güvenliği)
→ Kablosuz İletişim (WPA3 gibi kablosuz ağların güvenliği için)
→ IoT (Akıllı cihazlar arasında)
→ Kripto Para İşlemleri
→ Askeri ve Savunma Sistemleri

Saldırı ve Güvenlik

→ Man-in the-Middle Sald. (MitM): MitM saldırılarına karşı korunma sağlar.

→ Brute Force Sald. : Oturum açma bilgilerinin değişmesi için, saldırganların eski anahtarların ele geçirmesi boşa çıkarılır


HK
SOWACODEHK.COM.TR