1. Bilgi Gizleme Nedir?

Steganography

1. Saldırgan terimleri nelerdir?

Attacker, Hacker, Intruder

1. Klavye dinleme sistemi nedir?

Keylogger

1. Kötücül yazılım analizi nedir?

Malware

1. Kaynak kod istismarı-korumasızlık sörücü nedir?

Exploit

1. Hizmet aksattırma saldırısı nedir?

DoS(Denail of the Service)

1. Dağıtık hizmet aksattırmaya nedir?

DdoS

1. Casus yazılıma ne denir?

Spyware

1. Kök kullanıcı takımına ne denir?

Rootkit

1. Koklayıcı, ağ izleyici nedir?

Sniffer

1. Bilgi güvenliğinin temel amacı nedir?

Gizlilik (Confidentiality)

Bütünlük (Integrity)

Kullanılabilirlik (Availability)

1. Gizlilik nedir?

Kuruma özel ve gizliliği olan bilgilere, sadece yetkisi olan kişilerin sahip çıkmasıdır.

1. Bütünlük nedir?

Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.

1. Kullanılabilirlik nedir?

Bilginin yetkili kişiler tarafından ulaşılabilir ve kullanılabilir durumda olmasıdır.

1. Bilgi güvenliği sorumlulukları yasal olarak hangi kanunla ifade edilmiştir?

5651 sayılı kanunuyla(“internet ırtamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi”)

1. Bilgi güvenliğinden kim sorumludur?

Bilgini sahibii Bilgiyi yöneten, Bilgiyi kullanan

(Bilgi Güvenliğinden herkes sorumludur.)

1. Bilgi nedir?

İşlenmiş veridir ve kurum için değeri olan ve dolayısıylauygun bir şekilde korunması gereken bir kaynaktır.

1. Hangisi güvenlik yöntem pratiklerinden değildir?

Gizlilik, Bütünlük, Erişebilirlik

Risk Değerlendirmesi ve Yöntemi

Politika, Prosedür ve Rehberler

Politika Uygulamaları

Eğitim

Denetim

1. Risk Değerlendirmesi nedir?

Kurumsal işleyişi etkileyebilecek olan risklerin belirlenmesi ve değerlendirilmesi sürecidir.

1. Risk yöntemi nedir?

Ortaya çıkan riskin nasıl yönetileceği ve nasıl hareket edileceğinin planlanması sürecidir.

1. Risk yöntemi aşamaları nelerdir?

Risk yönetim ekibi kurma

Tehdit ve zaafiyetleri doğrulama

Organizasyon varlıklarının değerlerini belirleme

1. Risk yönetimi kavramları nelerdir?

Tehdit, Zaafiyet, Kontroller

1. Tehdit nedir?

Organizasyonu olumsuz etkileyecebilecek olan insan yapımı veya doğal olaylar

1. Zaafiyet nedir?

Varlıkların sahip olduğu ve istismar edilmesi durumunda güvenlik önlemlerinin aşılmasına neden olan eksiklikler

1. Kontroller nedir ve nelerdir?

Zaafiyetlerin boyutunu azaltıcı, koruyucu veya etkilerini azaltıcı önlemler

Caydırıcı Kontroller

Saptayıcı Kontroller

Önleyici Kontroller

Düzeltici Kontroller

1. Doğal tehdit belirleme olayları nelerdir?

Deprem, Sel, Kasırga

1. İnsan yapımı dış kaynaklı tehdit belirleme olayları nelerdir?

Virüs, Web Sayfası Değişimi,Dağıtık Servis Engelleme

1. İnsan yapımı iç kaynaklı tehdit belirleme olayları nelerdir?

E-Posta okuma, Kaynaklara Yetkisiz Erişim, Bilgi Hırsızlığı, Gizli Bilgilerin İfşası

1. Varlıkların değerinin belirlenmesi kaça ayrılır?

Nitel ve Nicel

1. Tekil Kayıp Beklentisi (SLE) = Varlık Değeri x Etki Düzeyi
2. Yıllık Kayıp Beklentisi (ALE) = Tekil Kayıp Beklentisi x Yıllık Gerçekleşme İhtimali
3. Nicel Risk Değerlendirmesi nedir?

Sürecin tüm elemanlarına sayısal değer verilmelidir.

Varlık, Etki Düzeyi, Koruma Verimliliği, Korunma Maliyeti vb.

1. Nitel Risk Değerlendirmesi nedir?

Değerlendirme çıktısı sayısal olmayacaktır.

1. Riske Karşı Davranış Belirleme kaça ayrılır?

Riskin azaltılması

Riskin aktarılması

Riskin kabul edilmesi

Riskin rededilmesi

1. Potansiyel hasar veya durumların sigorta ettirilmesi nedir?

Riskin aktarılması

1. Riskin gerçekleşmesi durumunda oluşacak potansiyel kaybın kabul edilmesine ne denir?

Riskin kabul edilmesi

1. Riskin inandırıcı bulunmaması ve göz ardı edilmesine ne denir?

Riskin rededilmesi

1. Bir önlemin uygulanmasına ve kullanılmasına ne denir?

Risk azaltılması

1. Politika türleri nelerdir?

Duyuru politikaları

Bilgilendirici politikalar

Yasal politikalar

1. Duyuru politikası nedir?

Çalışanların, davranışlarının sonuçlarını bildiğinden emin olunmasıdır.

1. Çalışanların bilgilendirilmesini ve eğitilmesini, görevlerinin ve beklentilerin bilincinde olmalarını hedefleyen politika hangisidir?

Bilgilendirme politikası

1. Güvenlik kontrollerinin amacı nedir?

Kurumun geliştirdiği güvenlik mekanizmalarının uygulanmasını sağlamak

1. Güvenlik kontrol türleri nelerdir?

Yönetimsel ( İşe Alım Süreci – Çalışan Kontrolleri – İşten Çıkarma Süreci)

Teknik

Fiziksel

1. Organizasyonun sahip olduğu güvenlik altyapısı ve güvenlik yönetim sürecinin periyodik olarak takip edilmesi nedir?

Denetim

1. Güvenlik Yönetim Sürecinin işleyişi nasıldır?

Güvenlik politikası oluşturma

Güvenlik politikası uygulama

Güvenlik politikası denetimi

Güvenlik politikasının analizi ve iyileştirilmesi

1. Bilgi güvenliği Sertifikasyonları nelerdir?

CISA, CISSP, ISO 27001 LA, CEH

1. Saldırı aşamaları nelerdir?

Veri Toplama Aşaması

Saldırı Hazırlık Aşaması

Saldırı Aşaması

Command Execution

Açıklar ve Exploiting

Sosyal Mühendislik & Phishing

İzleme ve Gizleme

Sistemi Sahiplenme

İzleri Silme

1. Saldırı Motifleri nelerdir?

Merak, Maddi kazanç arzusu, Ün kazanma isteği, Kin-Öç, Terörist amaçlı faaliyetler, İtibarsızlaştırmak, Sadece eğlence için, politik sebepler, Meydan okuma, Vatanperverlik

1. Siber saldırı senaryosu nasıl gerçekleşir?

Sıradan bir hırsızdan daha planlı bir çalışma, Sızılmaı düşünülen sistemi incele, Ön hazırlık, Harekete geç ve saldır, Açıklıkları tespit, Ağı izle ve gizlen, Sistemi sahiplen, İz bırakma

1. Siber saldırı olaylarında saldırgan tarafından hedefi tanımanın yolları nelerdır?

Whois Veritabanı sorgulama, DNS ve IP Veritabanı sorgulama, Domain Registraction, Nslookup

1. WHOIS sorgulaması nelerdir?

DNS adresleri, Domain bitiş süresi, IP adresi, Domain’i kaydeden kullanıcının irtibat adresleri, E-mail bilgileri, Telefon bilgileri

1. WHOIS LOOKUP nedir?

Domain isimlerinin tescil edilip edilmediğini, tescil edilmiş ise kim tarafından, ne zaman alındığını, alınan domainin bitiş tarihini öğrenebilmemiz için sunulan hizmete domain sorgulama veya Whois Lookup denir.

1. IP ve IP sorgulamada kullanılan internet temsilci veri tabanları nelerdir?

ARIN([www.arin.net](http://www.arin.net)), AFRINIC, APNIC, LACNIC, RİPE

1. Nslookup nedir?

DNS ile hedef sistemin IP adresi öğrenilebilir, IP bloğu bilgisine sahip olunabilir. Amaç DNS’ten IP bilgisine ulaşmaktır.

1. Traceroute yapısı nasıl çalışır?

IP adresleri tespit edildikten sonra hedef networke ulaşırken paketlerin hangi yolu takip ettiği tespit edilerek network hakkında bilgi sahibi olmaya çalışılabilir.

1. Google ile bilgi toplamaya ne denir?

Google Hacking

1. 7. Port olan Echo portunu kullanarak atılan ve ağ geçitlerine erişimin test edildiği komuta **PİNG** denir. **(IMCP)**
2. Nmap ( Network Mapper) port tarama da kullanılabilecek bir araçtır. **DOĞRU**
3. Parmak izi tespitine **(Fingerprinting)** denir.
4. Cookie nedir?

Cookie’ler tarayıcı ve sunucu arasındaki iletişimin hatırlanmasını sağlar.

1. Şifrelere saldırı yöntemleri nelerdir?

Sözlük saldırısı (Dictionary atack)

Brute Force

Hybrid

Sosyal Mühendislik

1. Sosyal mühendislik nedir?

Akıllı insan kendi aklını kullanır. Daha akıllı insan ise hem kendi aklını hem de başklarının aklını kullanır. İnsanların zayıf ve bilgisiz noktalarını kullanır. İnsani ilişkiler ile şifrelerin elde edilmeye çalışılması

1. Hybrid saldırı yöntemi nasıl oluşur?

Önce sözlük içindeki kelimeleri daha sonrada brute force mantığı ile çalışır.

1. Brute force saldırısı nedir?

Olabilecek bütün kombinasyonların şifre üzerinde denenmesidir.

1. Sözlük saldırısı nasıl yapılır?

Bir sözlük ya da belirlenen kelimelerin şifre için denenmesidir.

1. Uzak sisteme şifre deneyebilen araçlar nelerdir?

ENUM, NAT, HYDRA, TSGRINDER

1. Şifre kırma araçları nelerdir?

LCS, JOHN THE RİPPER (En çok kullanılan), CAIN&ABLE

1. Exploit nedir?

Exploit, sistemin zayıflıklarından faydalanarak sisteme giriş sağlayabilen veya zarar veren kod.

1. DOS ve DDOS arasındaki fark nelerdir?

DoS sistemleri çalışmaz hale getirmek için yapılan saldırı.

DdoS, DoS saldırısının yüzlerce, binlerce farklı sistemden yapılması.

1. Phishing-oltalama saldırı nereye uygulanır?

Korsanlar tarafından telefonuma veya e-mail adreslerimize bankalar tarafından göderiliyormuş gibi mesajların gelmesi ile gerçekleştiriyorlar.

1. SPOOFING saldırı türü nedir?

IPBaşlık formatı yani IP paketi içerisindeki Kaynak IP bilgisinin değiştirilmesiyle hedefteki yapıdan ve sistemden gizlenme şeklindeki saldırı türüdür.

1. Sistemi sahiplenmede kullanılabilecek yapılar?

Backdoor - Trojan – Rootkit – Netcat

1. Backdoor saldırı türü nedir?

Sisteme başarıyla sızan bir saldırgan sonradan tekrar erişmek isteyebilecektir.

1. Rootkit saldırı türü nasıl gerçekleşir?

Hedef bir sistemin dosya ve süreçlerini gizlemek veya değiştirmek suretiyle manipule eden uygulamalardır.

1. Netcat ne işe yarar?

Belirlenen port üzerinden hedefe TCP veya UDP ile bağlantısı gerçekleştirilebilir.

1. Ünyadaki bilişim suçları en çok hangi ülkelerde işleniyor?

Amerika , Türkiye, Rusya, Çin ve Brezilya

1. Hacker çeşitleri?

**Script Kiddies(Lamer):** Kendini bir şey zanneden hacker

**Phreakers:** Santral ve telefon hatlarının açıklarını kullanan hacker

**Grey Hat Hackers:** Hem savunma hem de saldırı amaçlı çalışan hacker. Amaçı sadece kazanmaktı.

1. Sosyal mühendislik çeşitleri ?

İnsan tabanlı ve PC tabanlı olmak üzere ikiye ayırabiliriz.

PC tabanlı sosyal mühendis hem aklını hem de PC bilgilerini kullanan kişidir desek herhalde yanlış olmaz.

1. Sosyal mühendislik örnekleri?

Bir web sitesinin tasarım olarak benzerini yapıp, domain olarakta çok benzer bir domain alıp, bilgilerinize erişmek

Reklam’lara tıkla para kazan vs. Sahte siteler.

1. İlk başlar da siyah şapkalı olup sonradan beyz şapkalılara katılan ünlü hacker kimdir?

Dennis Ritchie Ve Ken Thompson

1. Çok hızlı şifre kırma işlemin hangi güvenlik aracıyla yaparız?

John the Ripper

1. Uygulama düzeyinde ağa bağlı araçlar üzerinde hasar risk analizi yapabilen ve ağdaki güvenlik açıklarını yakalamada en iyi güvenlik aracı hangisidir?

ISS Internet Scanner

1. Wireshark nedir ne işe yarar?

Ethereal adıyla faaliyete başlayan bir projedir. Wireshark ismiyle çıkan bu yazılım 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.

1. Wireshark programı hangi işletim sistemlerinde çalışır?

Windows, Unix, OS X, Solaris, FreeBSD, NetBSD, ve bir çok işletim sistemleri için uygundur.

1. Wireshark nerelerde kullanılır?

Ağ trafik tespiti, Veri madenciliği, Saldırı tespiti, Port tarama tespiti, Virüslerin bulaştığını veya Denail of Service(DoS)ataklarını bulma tespiti, Bağlantı sorunu tespiti, Casus yazılım tespiti

1. WiMax nedir?

IEEE 802.16:Telsiz kentsel alan ağı standardı (Wireless MAN)

1. Şifreleme de kullanılan ve günümüz de kırılabilen algoritma hangisidir?

**DES**(Deneme-yanılma ve Brute-Force saldırılarına dayanaksızdır)

1. AES kaç bitliktir?

**128 Bit**

1. Güvenlik birimi hangi katmanlar arasındadır?

**MAC-FİZİKSEL**

1. Verini şifrelenmesi(blokları ard arada bağlama) hangi alt katman da oluşur?

**DES, CBC**

1. SAIP’ler kaç bitliktir?

16 Bit

1. Güvenlik yöntemi nasıl sağlanır?

3DES ile, RSA ile, AES ile, HMAC-SHA1 ile sağlanır.

1. Unix türevleri nelerdir?

OpenBSD, FreeBSD, Irix, Solaris, Aix.... çeşitli Unix türevleridir.

1. Parolaların şifrelenmesi hangi fonksiyon ile olur?

Crypt fonksiyonu ile şifreleme ve passwd

1. Kriptografi nedir?

Bilgiyi şifreli hale dönüştürme işlemidir.

1. Kriptoanaliz nedir?

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

1. Şifreleme(Encryption): Düz metni şifreli metne çevirme işlemidir.
2. Şifre Çözme(Decryption): Şifrelenmiş metni düz metne çevirme işlemidir.
3. Anahtar(Key): Şifreli metnin nasıl elde edildiğine dair kod parçasıdır.
4. Sezar Şifreleme, şifrelenecek metin alfabede kendinden sonra gelecek 3.harfle yer değiştirerek oluşturulmaktadır.
5. EBCED hesabı, Arap alfabesinin eskı sıralanışından(elif, ba, cim, dal) ilk dört harfinin okunuşlarıyla (E – B – Ce – D) türetilmiş sözcüktür.
6. Pigpen (Mason) Şifrelemesi, Şekilli şüküllü şifreleme
7. Dünyanın en büyük casusluk ağı hangisidir?

**Echelon Sistem**

1. PROMİS(Dava Tönetim Sistemi) nedir?

Bu sistem ile;

Birçok ülkenin banka sisteminin kitlenebileceği

Kontrollü mail krizler çıkarılabileceği

Uluslararası ihalelere girecek şirketlerin dinlendiği iddaa edildi.

1. Elektromekanik bir şifre çözme makinesi hangisidir?

ENİGMA

1. Ağ Görselleştirme Sistemi çeşitleri nelerdir?

Honeymap, Norse-Map, Digital atack map, Kaspersky Cybertreat Real-Time Map, Wordfence, Sucuri, Trend micro, Threat Cloud, Akamai, Malwaretech Live Map, ESG MalwareTracker, Fortinet Threat Map

1. İşlenmiş veri olarak ve bir konu hakkında var olan belirsizliği azaltan kaynağa ne denir?

Bilgi

1. Tecrübe veya öğrenme şeklindegerçeklerin, doğruların veya bilginin,farkında olunması ve anlaşılmasına ne denir?

Özbilgi

1. Özbilginin nasıl kullanılacağını kavramaya ne denir?

Hikmet(not: veri -> bilgi -> özbilgi -> hikmet)

1. Steganografi(gizlenmiş yazı) kaça ayrılır?

Metin steganografisi, Resim steganografisi, Ses steganografisi

1. HASH nedir?

Büyük tanım bölgelerini küçük değer bölgelerine dönüştürülür.

1. En iyi bilinen hash fonksiyonları nelerdir?

MD-4, MD-5, SHA’dır.

1. MD-5 kaç bitliktir?

128 Bit

1. SHA-1 kaç bittir?

160 bit

1. SHA-2 bit uzunlukları nelerdir?

224, 256, 384, 512 bit uzunluğunda özetler üreten çeşitleri vardır.

1. RSA Açık Anahtar Algoritması nedir?

RSA, güvenliği tam sayıları çarpanlarına ayırmanın algoritmik zorluğuna dayanan bir tür Açık anahtarlı şifreleme yöntemidir.

1. Windows 7 işletim sistemi ilke gelen şifreleme özelliği nedir?

Bitlocker sürücü şifreleme özelliğidir.

1. WEP Şifreleme nerede kullanılır?

WEP (Wired Equivalent Privacy) kablosuz ağ Veri-bağ tabakasında çalışan şifreleme yöntemidir.

1. WPA Şifrelemesi nerede kullanılır?

İstemci ile AP (Erişim Noktası) bağlantı kurmadan önce, aygıtların birbirini bulması gerekiyor.

1. ‘Bilgi gizleme bilgisayar ortamındaki ............... işlemine benzer bir durumdur’ boş bırakılan yere ne gelir?

Encapsulation (Kapsülleme)

1. Encapsulation’ın asıl amacı nedir?

İçeriği saklamak değil kontolsüz ve gereksiz erişimi engellemek, dış öğeleri, içeriğe standart, önceden tanımlı arayüzler aracılığıyla ulaşıma zorlamaktır.

1. Bilgi gizleme kaça ayrılır?

Gizli kanallar – Steganografi – Gerçek kimliği saklama – Telif hakkı işratlemesi

1. Steganografi kaça ayrılır?

Dilbilim steganografisi – Teknik steganografisi

1. İki kişi arasında gizli bilgilerin eldeğiştirmesi için iletişimi sağlayan kanala ne denir?

Gizli kanallar

1. Gizli kanalların amacı nedir?

İletişimdeki veriyi saklamaya çalışmak

İletişimin amacını saklamak

1. Gizli Kanallar hangi alanlarda kullanılmaktadır?

Dosya tabanlı steganografi (Görüntü, ses ve text dosyaları)

Ağ paket steganografisi ( Veriler IP paketleri içine gizlenmektedir.)

Protokol Kapsüllenmesi \* SSL (Secure Sockets Layer)

\*SSH (Secure Shell)

1. Veri gönderimi sırasında gerçek kimliği saklayarak bilginin bilinmeyen yada anlaşılamayan biri üzerinen gidiyor olduğu izlenimi verilerek gönderilen yapıya ne denir?

Gerçek Kimliği Saklama (Anonymity)

1. Bir nesnenin içerisine bir verinin gizlenmesine ne denir?

Steganografi

1. İçerisine bilgi gizlenen ortama ne denir?

Cover-data (Örtü verisi)

1. Bilgi gizlemede oluşan ortama ne denir?

Stego-text veya Stego-object

1. Bilginin saklaması işlemini kontrol etmek için ve gömülü bilginin elde edilmesini zorlaştırmak içim kullanılan ortama ne denir?

Stego-key

1. Taşıyıcı verinin text olduğu steganografiye ne denir?

Dilbilim steganografisi

1. Dilbilim steganografisinde kullanılan yöntemler nelerdir?

Açık kodlar – Şemagramlar

1. Teknik Steganografini kapsadığı alanlar nelerdir?

Görünmez mürekkep – Gizli yerler – Microdot – Bilgisayar tabanlı yöntemler

1. Geleneksel haline gelmiş olan görünmez mürekkeple yazma yöntemine ne denir?

Görünmez mürekkep

1. Kimsenin göremeyeceği gizli yerlere saklama yöntemine ne denir?

Gizli yerler

1. Bilgiyi noktalar halinde sayfaya gizlemeye ne denir?

Microdotlar

1. Text, ses, görüntü, resim dosyalarını kullanarak veri gizleme yöntemine ne denir?

Bilgisayar tabanlı yöntemler

1. Metin Steganografi veri saklanacak yerlerin özelliklerine göre hangi yöntemler kullanılır?

Açık alan yöntemleri – Yazımsal yöntemler – Anlamsal yöntemler

1. Açık alan yöntemlerinin uygulama alanları nelerdir?

Satır kaydırma – Satır sonu boşluk bırakma – Cümle içi boşluk bırakma – Sağ hizalama – gelecek kodlaması

1. Görüntü steganografisi yöntemleri nelerdir?
2. En önemsiz bite ekleme
3. Maskeleme ve filtreleme
4. Algoritmalar ve dönüşümler
5. 0-255 arası 1 byte ile temsil edilen görüntünün hangisi seviyesidir?

Gri-seviye

1. Renkli dijital görüntüler kaç bittir?

24bit ve 8 bit

1. 24 bitlik görüntü için pixel başına kaç byte düşer?

3 byte ( pixel için 3 ana renk vardır.- kırmızı – mavi – yeşil)

1. 8 bitlik görüntüler pixel başına kaç byte düşer ?

1 byte

1. 8 bitlik görüntülerde kullanılan renkler nelerdir?

-beyaz –kırmızı –mavi ve –yeşil

1. ‘ ......... teknikleri genellikle 24 bit ve gri- seviye görüntüler üzerinde işaretleme (marking) ve filigran yapılarak uygulamaktadır.’ Boş bırakılan yere ne gelir?

Maskeleme ve filtreleme

1. ‘ Teknik olarak filigran bir steganografik biçim değildir’ **Doğru**
2. Hem sıkıştırma hem de bilgi gizleme işlemlerini yapan algoritmalar ve dönüşümler nelerdir?

Jpeg , jsteg , Stego-Dos , Picture-Mark , SureSign , S-Tools

1. Stego-Dos: içine veri gömülmüş resim
2. WAV ( Windows Audio-Visual) ve AIFF (Audio Interchange File Format) yöntemleri nerede kullanılır?

Ses steganografisinde

1. Gizli verilerin şifrelerini kırmak için sözlük saldırısı yapabilen araca ne denir?

Stegbreak

1. ............ resim içerisindeki veriyi tespit etmek için kullanılan araca ne denir?

Stegdetect

1. Watermarking’in amacı nedir?

Ses veya görüntü dosyasının bazı özel modifikasyonlarla saklanması değildir.Amacı; Steganografi gibi sadece gizleme değil.

1. Amaçlarına göre Steganaliz yöntemleri nelerdir?

Aktif Steganaliz- Pasif Steganaliz

1. Gizli verinin sadece varlığını tespit een yönteme ne denir?

Pasit steganaliz

1. Gizli mesajın bir kısmını veya benzerini elde etmeyi sağlayan yönteme ne denir?

Aktif steganaliz

1. Çalıştığı boyuta göre Steganaliz yöntemleri nelerdir?

Uzaysal dağılımlı veri üzerinde çalışan metotlar (Resim)

Zamana dağılmış veri üzerinde çalışan metotlar (Ses)

Hem uzaysal hem de zamana yayılmış veri üzerinde çalışan metotlar (Video)

1. Sızma testleri ne işe yarar?

Bir sistemdeki kullanıcıların ver süreçlerin hareketleri,

Genellikle istatiksel öngörülen bir örtüye dayanır.

Sistemin güvenlik politikasını altüst edecek komut veya komutlar dizini içermez.

Sistemde olan ve süreçlerin hareketlerine kısıtlamalar (olumlu veya olumsuz) getiren belirtimler kümesine uyar.

1. Rootkit nedir?

Çalışan süreçleri, dosyaları veya sistem bilgilerini işletim sisteminden gizlemek suretiyle varlığını gizlice sürdüren bir program veya programlar grubudur. Amacı yayılmak değil bulunduğu sistemde varlığını gizlemektir.

1. Sızma belirleme Modelinde Anomali Modeli nedir?

Beklenmeyen davranışın olası bir sızmanın kanıtı olacağı varsayımı kullanılır.

1. Kural Tabanlı Sızma Belirleme nedir?

Herhangi bir komut dizisinin önceden bilinen ve sistemin güvenlik politakasını ihlal edecek işlemler yapıp yapmadığını tespit eder ve potansiyel sızmaları raporlar.

1. Belirtim Tabanlı Sızma Belirleme nedir?

Bir dizi komutun bir programın yada sistemin çalışma şekline zarar verip vermediğini belirler.

1. Konak Tabanlı Bilgi Toplama nedir?

Sistem ve uygulama kayıtları üzerinde çalışırlar.

Olabildiğince sade bir tasarım

1. Ağ Tabanlı Bilgi Toplama nedir?

Ağdaki çeşitli araçlardan ve yazılımlardan faydalanırlar.

İçerik incelemesi yapar.

1. Sızma Beirleme Sistemlerinin Örgütlenmesi nelerdir?
2. Ağ Trafiğini İzlemek (NSM)
3. Konakları ve Ağları Birlikte İzlemek(DIDS)
4. Özerk Aracılar Kullanmak
5. Sızma yöntemleri nelerdir?

Hazırlık , Tanıma aşaması , Yakalam aşaması , Temizleme aşaması , Kurtarma aşaması , Kovalama aşaması

1. Bilgi Güvenliği ürün veya hizmet değildir.
2. ‘ Savunmadan çok “Saldırı” ya yönelik araçlara ........... denir. ’ boş bırakılan yere ne gelir?

Güvenlik araçları

1. Ağ araştırması ve güvenlik denetlemesi yapan açık kaynaklı ücretsiz yazılıma ne denir?

Nmap

1. Güçlü, güncel ve ücretsiz bir uzaktan güvenlik tarama aracına ne denir?

Nessus (farkı: kurallara bağlı değildir.)

1. Protokol analizi yapan araçlara ne denir?

Ethereal

1. Canlı bir ağ üzerindeki verileri incelemek veya disk üzerine kaydetme işlemi hangi güvenlik aracıyla yapılır?

Ethereal (metin tabanlı)

1. Gerçek zamanlı trafik analizi ve paket kayıtlaması yapabilen ücretsiz bir ağ saldırı belirleme sistemine ne denir?

Snort

1. Protokol analizi, içerik araştırması ve eşlemesi yapabilen güvenlik aracına ne denir?

Snort

1. Ağ inceleme ve veri yakalama amaçlı klasik bir sniffer ve metin tabanlı güvenlik aracı?

Tcpdump

1. Verilen deyimleri eşleyerek belirli bir ağ arayüzündeki paket başlıklarını gösteren güvenlik aracına ne denir?

Tcpdump

1. (2.katman) ağ bilgilerine ulaşmayı kolaylastıran güvenlik aracına ne denir?

Dsniff

1. Sistemdeki güvenlik hasar risk analizini otomatik olarak yapan araç hangisidir?

GFI LANguard

1. Anahtarlamalı yerel ağlar için kullanılan bir sniffer, aramaya girme ve kayıt yapan güvenlik aracı hangisidir?

Ettercap (Ağ geometrisini çıkarma ve işletim sistemi tespitleri yapar.)

1. Biyometrik tanıma teknikleri nelerdir?

Parmak izi tanıma

Optik tanıma

Yüz yapısı tanıma

Ses tanıma

İmza tanıma

Yazma ritmi tanıma

Toplardamar izi tanıma

Avuç içi izi

Kullak şeklinden tanıma

( en dikkat çekici olanlardan birisi insanların kulak yapılarını algılayıp tanıyan sistemlerdir.)