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-korunmasızlık sömürücü nedir?

**Exploit**

1. Hizmet aksattırma saldırısı nedir?

**DoS(Denial of the Service**

1. Dağıtık hizmet aksattırmaya nedir?

**DdoS**

1. Casus yazılıma nedir?

**Spyware**

1. Kök kullanıcı takımına nedir?

**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 ilgili yada yetkili kişiler tarafından ulaşılabilir ve kullanılabilir durumda olmasıdır.**

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

**5651 sayılı kanunuyla (“İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi")**

1. Bilgi güvenliğinden kim sorumludur?

**Bilginin sahibi, Bilgiyi yöneten, Bilgiyi kullanan**

**(bilgi güvenliğinden herkes sorumludur.)**

1. Bilgi nedir?

**İşlenmiş veridir ve Kurum için değeri olan ve dolayısıyla uygun bir şekilde korunması gereken bir kaynaktır.**

1. Hangisi güvenlik yönetim pratiklerinden değildir?

* **Gizlilik, Bütünlük, Erişilebilirlik**
* **Risk Değerlendirmesi ve Yönetimi**
* **Politika, Prosedür ve Rehberler**
* **Politika Uygulamaları**
* **Eğitim**
* **Denetim**

1. Risk değerlendirmesi nedir?

**Kurumsal işleyişi etkileyebilecek olan risklerin belirlenmesi ve değerlendirilmesi sürecidir.**

1. Risk yönetimi nedir?

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

1. Risk yönetimi aşamaları nelerdir?

* **Risk yönetim ekibi kurma**

**• Tehdit ve zaafiyetleri doğrulama**

**•Organizasyon varlıklarının değerlerini belirleme**

**• Riske karşı yapılacak hareketleri belirleme**

1. Risk yönetimi kavramları nelerdir?

**Tehdit, Zaafiyet, Kontroller**

1. Tehdit nedir?

**Organizasyonu olumsuz etkileyebilecek 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, Bilgi Hırsızlığı, Gizli Bilgilerin İfşası**

1. Varlıkların değerlerinin 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 İhtima**li
3. Nicel Risk Değerlendirmesi nedir?

**Sürecin tüm elemanlarına sayısal değer verilmelidir.**

**Varlık,**

**Etki Düzeyi,**

**Korunma 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 nedir?

**Riskin kabul edilmesi**

1. Riskin inandırıcı bulunmaması ve göz ardı edilmesine nedir?

**Riskin reddilmesi**

1. Bir önlemin uygulanmasına ve kullanılmasına nedir?

**Riskin 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 hangidir?

**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 edilmesine 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 Gizlenme**

**• Sistemi Sahiplenme**

**• İzleri Silme**

1. Saldırı Motifleri nelerdir?

• **Merak**

**• Maddi kazanç arzusu**

**• Ün kazanma isteği**

**• Kin-öç**

**• Terörist amaçlı faaliyet**

**• İtibarsızlaştırmak**

**• Sadece eğlence için**

**• Politik sebepler**

**• Meydan okuma**

**• Vatanperverlik**

1. Siber saldırı senoryosu nasıl gerçekleşir?

**•** **Sıradan bir hırsızdan daha planlı bir çalışma**

**• Sızılması düşünülen sistemi incele**

**• Ön hazırlık**

**• Harekete geç ve saldır**

**• Açıklıkları tespit ve…**

**• Ağı izle ve gizlen**

**• Sistemi sahiplen**

**• İz bırakma**

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

**• Whois Veritabanı sorgulama**

**• DNS ve IP Veritabanı Sorgulama**

**• Domain Registration**

**• 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 İnternet temsilci veritabanları nelerdir?

**• ARIN (**[**www.arin.net**](http://www.arin.net)**)**

**• AFRINIC**

**• APNIC**

**• LACNIC**

**• RIPE**

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 kullarak atılan ve ağ geçitlerine erişimin test edildiği komuta **PİNG** denir. **(ICMP)**
2. Nmap (Network Mapper) port tarama da kullanılabilecek bir araçtır.

**DOĞRU**

1. Parmak izi tespitine (**Fingerprinting**) denir.
2. Cookie nedir?

**Cookie’ler tarayıcı ve sunucu arasındaki iletişimin hatırlanmasını sağlar.**

1. Şifrelere saldırı yöntemleri nelerdir?

* **Sözlük Saldırısı(Dictionary attack)**
* **Brute Force**
* **Hybrid**
* **Sosyal Mühendislik**

1. Sosyal mühendislik nedir?

**İnsanların zayıf ve bilgisiz noktalarını kullanır. insani ilişkiler ile şifrelerin elde edilmeye çalışılması**

1. Hybrid saldırı yöntemi nasıl oluşur?

**önce sözlük içindeki kelimeleri daha sonra da 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?

* **LC5**
* **JOHN THE RİPPER(En çok kulllanılan)**
* **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 trafından telefonuma veya emil adreslerimize banklar tarafından gönderiliyormuş 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 manipüle eden uygulamalardır.**

1. Netcat ne işe yarar ?

**Belirlenen port üzerinden hedefe TCP veya UDP İLE bağlantısı gerçekleştirilebilir.**

1. DÜNYADAKİ BİLİŞİM SUÇLARI EN ÇOK HANGİ ÜLKELERDE İŞLENİYOR ?

**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

• -**Crackers:** PC yazılımlarını kıran ve yayınlayan hacker

• -**Grey Hat Hackers:** Hem savunma hemd e saldırı amaçlı çalışan hacker. Amacı sadece kazanmaktı.

1. SOS. MÜH. ÇEŞİTLERİ ?

**• İnsan tabanlı ve PC Tabanlı olmak üzere ikiye ayırabiliriz.**

**• PC tabanlı Sos. Müh. hem aklını hem de PC bilgilerini kullanan kişidir desek herhalde yanlış olmaz.**

1. Sosyal mğhendislik örnekleri?

**• Bir web sitesinin tasarım olarak benzerini yapıp, domain olarakta çok benzer bir domain alıp, bilgilerimize erişmek**

**• Reklam’lara tıkla para kazan vs. sahte siteler.**

1. AĞ GÖRSELLEŞTİRME SİSTEMİ çeşitleri nelerdir?

**Honeymap**

**Norse- map**

**Digital atak 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 nedir?

**Bilgi**

1. Tecrübe veya öğrenme şeklinde gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasına nedir?

**Özbilgi**

1. Öz bilginin nasıl kullanılacağını kavramaya nedir?

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

1. Steganografi kaça ayrılır?

**- Metin steganografisi –Resim steganografisi**

**- Yazı steganografisi**

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

**Encapsulation (Kapsülleme)**

1. Encapsulation'ın asıl amacı nedir?

**içeriği saklamak değil kontrolsüz ve gereksiz erişimi engellemek, dış öğeleri, içeriğe standart, önceden tanımlı arayüzler aracılığıyla ulaşıma zorlamaktır.**

1. Bilgi gizleme kaça ayrılır?

**-Gizli kanallar –Stegonagrafi –Gerçek kimliği saklama**

**-Telif hakkı işaretlemesi**

1. Stegonagrafi kaça ayrılır?

**-Dilbilim steganografisi –Teknik stegonagrafisi**

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

**Gizli kanallar**

1. Gizli kanalların amacı nedir?

**-İletişimimizdeki veriyi saklamaya çalışmak**

**-İletişiminin amacını saklamak**

1. Gizli Kanallar hangi alanlarda kullanılmaktdır?

**-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 üzerinden gidiyor olduğu izlenimi verilerek gönderilen yapıya nedir?

**Gerçek Kimliği Saklama (Anonymity)**

1. Bir nesnenin içerisine bir verinin gizlenmesine nedir?

**Steganografi**

1. İçerisine bilgi gizlenen ortama nedir?

**Cover-data (örtü verisi)**

1. Bilgi gizlemede oluşan ortama nedir?

**Stego-text veya Stego-object**

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

**Stego-key**

1. Taşıyıcı verinin text olduğu steganografiye nedir?

**Dilbilim steganografisi**

1. Dilbilim steganografisinde kullanılan yöntemler nelerdir?

**-Açık kodlar -Şemagramlar**

1. Teknik Steganografinın kapsadığı alanlar nelerdir?

**- Görünmez mürekkep -Gizli yerler –Microdot**

**- Bilgisayar tabanlı yöntemler**

1. Geleneksel haline gelmiş olan görünmez mürekkeple yazma yöntemine nedir?

**Görünmez mürekkep**

1. Kimsenin göremeyeceği gizli yerlere saklama tekniğine nedir?

**Gizli yerler**

1. Bilgiyi noktalar halinde sayfaya gizlemeye nedir?

**Microdotlar**

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

**Bilgisayar tabanlı yöntemler**

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

**-Açık alan yöntemleri -Yazımsal yöntemler**

**-Anlamsal yöntemler**

1. Açık alan yöntemlerinın uygulama alanları nelerdir?

**• Satır kaydırma**

**• Satır sonu boşluk bırakma**

**Cümle içi boşluk bırakma**

**• Sağ hizalama**

**• Gelecek kodlaması**

1. Görüntü steganorafisi yöntemleri nelerdir?

**1.En önemsiz bite ekleme**

**2. Maskeleme ve filtreleme**

**3. Algoritmalar ve dönüşümler**

1. 0-255 arası 1 byte ile temsil edilen görüntünün hangi seviyededir?

**Gri-seviye**

1. Renkli dijital görüntüler kaç bittir?

**24 bit ve 8 bit**

1. 24 bitlik bir 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 uygulanmaktadır.’ Boş bırakılan yere ne gelir?

**Maskeleme ve filtreleme**

1. ‘Teknik olarak filigran bir steganografik biçim değildir’

**Doğru**

1. Hem sıkıştırma hemde bilgi gizleme işlemlerini yapan algoritmalar ve dönüşümler nelerdir?

**-Jpeg- jsteg**

**- Stego-Dos**

**-Picture-Mark**

**-SureSign**

**-S-Tools**

1. WAV(Windows Audio-Visual) ve AIIF(Audio Interchange File Format) yöntemleri nerede kullanılır?

**Ses steganografisinde**

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

**Stegbreak**

1. ---------- resim içerisindeki veriyi tespit etmek için kullanılan araca nedir?

**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 eden yönteme nedir?

**Pasif steganaliz**

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

**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. ‘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 nedir?

**Nmap**

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

**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 nedir?

**Snort**

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

**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 nedir?

**Tcpdump**

1. (2. katman)ağ bilgilerine ulaşmayı kolaylaştıran güvenlik aracına nedir?

**Dsniff**

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

**GFI LANguard**

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

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

1. Çok hızlı bir şifre kırma işlemini hangi güvenlik aracıyla yaparız?

J**ohn 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**