Bilgi Güvenliği ve Yönetim Sistemi: Vize 2020-11-23 Soruları Pazartesi: Saat 10:00

Toplam Soru Sayısı 40 Tane: Her Soru (Puanı) 2.50 Üzerinden Puan

Soru 1) Hangisi dersin bu dönemlik değerlendirmesinde başvurulacak unsurlardan biri değildir?

a. Ödev **b. Quiz** c. Proje d. Final e. Ara Sınav

Soru 2) Aşağıdakilerden hangisi internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi" amacı ile düzenlenmiştir?

a.TS ISO IEC 27001 b. ISO 27001-5651 c. ISO 27001 LA d. UEKAE BGYS-0001 **e. TCK 5651**

Soru 3) Hangisi güvenlik yönetim pratiklerinden birisi değildir?

a. Denetim b. Eğitim e. Risk Değerlendirmesi ve Yönetimi

c. Politika, Prosedür ve Rehberler **d. Siber Saldırı Analiz Sistemi**

Soru 4) Hangisi bilgi güvenliğinin temel unsurlarından birisi değildir?

a. Bütünlük b. Erişilebilirlik c. Gizlilik **d. Doğrulama** e. Kullanılabilirlik

Soru 5) Nicel risk değerlendirmesi kapsamındaki hesaplardan biri olan yıllık kayıp beklentisi hesaplanırken yıllık gerçekleşme ihtimalini nasıl değerlendirirsiniz?

a. Korunma maliyetine bakarak

b. Tekil kayıp beklentisine bakarak

c. Sonraki yılda gerçekleşme oranını tahmin ederek

d. Önceki gerçekleşme değerlerine bakarak e. Varlık değerine bakarak

Soru 6) Hangisi dönem projesi olarak önerdiğim konseptlerden birisi değildir?

a. Biyometrik güvenlik sistemleri b. Security information event management

c. Arama motoru optimizasyonu d. Sosyal medya analizi e. Antivirüs sistemleri

Soru 7) Güvenlik yönetim süreci, yazılım yaşam döngüsü gibi bir güvenlik yaşam döngüsü olarak ele alındığında 3. aşamada hangisi yer alır?

a. izleme b. Oluşturma c. Analiz d. Uygulama e. Geliştirme

Soru 8) Hangisi dersin amaçlarından biri değildir?

a. Araştırma yeteneğinizi geliştirmek.

b. Bilgi güvenliği konularında farkındalık ve temel düzeyde teorik ve pratik bilgiler öğrenmenizi sağlamak.
c. Bilgi sistemlerinin açıklıklarını tespit ederek sistemlere sızma yapabilmeniz için teknikler öğrenmenizi sağlamak.

d. Bilgi güvenliği temel kavram, standart, metodoloji, yöntem ve stratejilerini öğrenmenizi sağlamak.

e. Kişisel ve kurumsal bilgi güvenliğinin sağlanması konusunda fikir sahibi olmanızı sağlamak.

Soru 9) Dijital delillerin.....

dijital delillerin özellik ya da sorunlu bazı durumlarının ifade edilmek istendiğini düşünün. Buna göre yukarıdaki ifade aşağıdakilerden hangisi ile tamamlanamaz?

a. farklı zamanlarda değerlendirilebilmesi b. doğrulanamaması

c. inkar edilememesi d. bütünlüğü **e. doğruluğu**

Soru 10) Hangisi adli bilişim görev alanlarından biri değildir?

a. Veri imha Etme b. Steganografi c. Şifre Çözme d. Veri Kurtarma **e. Veri Üretme**

Soru 11) Hangisi dersin temel kaynakları arasında önerilen kaynaklardan birisidir?

a. Kamil Burlu, Bilişimin Karanlık Yüzü , Nirvana yayınları.

b. Bünyamin Demir, Bilgisayar ve Casus Yazılımlar, Dikeyeksen Yayınları.

c. Muhammet Baykara, Bilişim Sistemleri İçin Saldırı Tespit ve Engelleme Yaklaşımlarının Tasarımı ve Gerçekleştirilmesi, Fırat Üniversitesi Yayınları.

d. Ömer Çıtak, Beyaz Sapkalı Hacker Eğitimi, Papatya Yayınları.

e. Hamza Elbahadır, Saldırı ve Savunma Teknikleri, Kodlab Yayınları.

Soru 12) Ağ cihazlarının aksaklıkların' bulması ile ünlenen yazılım hangisidir?

a. Acunetix Vulnerability Scanner

b. GFI Lan Guard Network Security Scanner

c. Nmap

d. Net Gadgets

e. Shadow Security Scanner

Soru 13) Kurulum ve çeşitli konfigürasyon özelliklerini ders kapsamında paylaştığımız SNORT konseptinde açık kaynak bir yazılımdır.

a. security information event management b. honeypot temelli saldırı tespit sistemi

c. anti malware d. tuzak sistem **e. ağ tabanlı saldırı tespit sistemi**

Soru 14) Hangisi bilgi güvenliği alanındaki güncel mesleklerden biri değildir?

a. Incident Responder **b. Computer Security Developer**

c. Network Security Engineer d. Malware Analyst e. Security Architect

Soru 15) Dersle ilgili olarak verilen temel kavramlardan hangisi yanlış ifade edilmiştir?

a. Exploit : Korunmasızlık Sömürücü b. Integrity : Bütünlük **c. DoS : Disk Operating System**

d. Non-repudiation : inkar Edilemezlik o e. Confidentiality : Gizlilik

Soru 16) Hangi temel kavramın anlamı doğru olarak verilmiştir?

a. Worm: Truva Atı b. Spyware: Ağ İzleyici **c. Rootkit: Kök Kullanıcı Takımı**

d. Exploit: Arka Kapı e. Wisdom: Öz Bilgi

Soru 17) Bilgi güvenliğinin temel amacı hangisidir?

a. Yetkilendirmenin sağlanması b. Gizliliğin sağlanması **c. Minimum Risk**

d. Erişilebilirliğin sağlanması e. Bütünlüğün sağlanması

Soru 18) Hangisi diğerlerinden farklıdır?

a. Test edilmemiş güvenlik sistemi b. Yetkisiz kişilerin erişimi c. Yanlış eksik altyapı yatırımları
d. Çalışandan gelen tehditler **e. Bant genişliğine kasteden saldırılar**

Soru 19) Verilenlerden hangisi yanlıştır?

a. Bir konu ile ilgili belirsizliği azaltan kaynak veridir.

b. Bir sistem yazılımı ihtiyaçlarınız ve beklentileriniz doğrultusunda çalışıyorsa güvenlidir.

c. Bilgi güvenliğinin sağlanmasından herkes sorumludur.

d. Güvenlik, teknoloji kadar insan ve o insanların teknolojiyi nasıl kullandığı ile ilgilidir.

e. Güvenlik risk yönetimidir.

Soru 20) Kurum ya da kuruluşları olumsuz etkileyebilecek unsurlara.....denir.

Cevap: **Tehdit**

Soru 21) Varlıkların sahip olduğu ve istismar edilmesi durumunda güvenlik önlemlerinin aşılmasına neden olan eksikliklere.....denir.

Cevap: **Zafiyet**

Soru 22) Bilgi güvenliği alanında dünya genelinde yaygın olarak kullanılan uluslararası standart dır.

Cevap: **ISO 27001**

Soru 23) Beyaz şapkalı hacker anlamına gelen kısaltmadır. Aynı zamanda bilgi güvenliği alanındaki temel standart ve yine bu alandaki önemli eğitimlerden biri.....dır.

Cevap: **Ethical Hacking**

Soru 24) Bir dosyanın değişip değişmediği bilgi güvenliği ilkelerinden.....ile ilgilidir.

Cevap: **Bütünlük**

Soru 25) Güncel bir kötücül yazılım türü olan ve fidye yazılımı olarak bilinen yazılıma.....denir.

Cevap: **Ransomware**

Soru 26) Dijital delillerin kanıt olarak değer kazanabilmesi için incelenmesi gereken son aşama.....'dır.

Cevap: **Raporlama**

Soru 27) Bir siber saldırı senaryosu açısından bakıldığında sosyal mühendislik aşamasına tekabül eden veya o aşamadaki eylemlerin genelini ifade eden sazan avlama olarak da bilinen yöntemlerin genel adı.....'dır. (literatürdeki orjinal ifadeyi veriniz)

Cevap: **phishing**

Soru 28) Uzak bir hedefdeki sunucunun aktif olup olmadığını.....protokolü ile öğreniriz.

Cevap: **Internet Control Message Protocol (ICMP)**

Soru 29) DNS'in açılımı.....

Cevap: **Domain Name System**

Soru 30) IP,.....ifadesinin kısaltmasıdır.

Cevap: **Internet Protocol**

Soru 31) Geliştirilecek bir yazılımda özel bir port kullanılacaksa.....başvuru yapılır.

Cevap: **Viyana** → Telafuzu tam doğru değil

Soru 32) Bir şifre için olası tüm ihtimallerin denenmesi şeklindeki saldırıya.....denir. (cevabınızı ya ingilizce ya da türkçe olarak yazın. her iki dilde birlikte yazmayın!)

Cevap: **Brute Force** (Kaba Kuvvet Saldırısı)

Soru 33) Yakın tarihin en büyük siber saldırılarından biridir. İran nükleer santrallerini hedef alsa da birçok ülke etkilenmiştir. Bu saldırı hangi isimle bilinir?

Cevap: **Stuxnet**

Soru 34) Uzaktaki bir makinenin işletim sistemini tespit etmek için yapılan çalışmalara genel olarak ne ad verilir.

Cevap: **Fingerprinting**

Soru 35) Snort saldırı tespit sisteminde paket yakalamak için kullanılan kütüphane nedir?

Cevap: **Libpcap** (library)

Soru 36) Snort saldırı tespit sisteminde paket analizi için kullanılan kütüphane nedir?

Cevap: **Tcpdump**

Soru 37) Bilginin sadece yetkili kişiler tarafından erişilebilir olması.....ilkesi ile sağlanır.

Cevap: **Gizlilik**

Soru 38) Günümüzde saldırı karmaşıklığı ile saldırganın teknik bilgisi arasında ters orantı vardır.

Doğru Yanlış

Soru 39) Açık istiharat toplama anlamındaki metodolojiye ne isim verilir?

Cevap: **OSINT** (Open Source Intelligence)

Soru 40) Ders kapsamında tanıtılan üstveri analiz aracının adı nedir?

Cevap: **Foca** (Fingerprinting Organizations with Collected Archives)
