1-Hangisi dersin bu dönemlik değerlendirmesinde başvurulacak unsurlardan biri değildir ?

* Quiz (kısa sınav)

* Ara Sinav

* Ödev

* Proje

* Final

2-Hangisi dersin amaçlarindan biri değildir?

*Bilgi güvenliği konularinda farkindalik ve temel düzeyde teörik ve pratik bilgiler öğrenmenizi saglamak.

*Bilgi güvenligi temel kavram, standart, metodoloji, yöntem ve stratejilerini öğrenmenizi sağlamak.

*Araştirma yeteneginizi geliştirmek.

*Kişisel ve kurumsal bilgi güvenliginin sağlanmasi konusunda fikir sahibi olmanizi sağlamak.

*Bilgi sistemlerinin açikliklarini tespit ederek sistemlere sızma yapabilmeniz için teknikler öğrenmenizi saglamak.

3- Hangisi dersin temel kaynakları arasında önerilen kaynaklardan birisidir?

Birini seçin:

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

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

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

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

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

4- Dersle ilgili olarak verilen temel kavramlardan hangisi yanlış ifade edilmiştir?

Birini seçin:

a. DoS : Disk Operating System // Dos : denial of service

b. Confidentiality : Gizlilik

c. Non-repudiation : İnkar Edilemezlik

d. Integrity : Bütünlük

e. Exploit : Korunmasızlık Sömürücü

5- Hangi temel kavramın anlamı doğru olarak verilmiştir?

Birini seçin:

a. Rootkit: Kök Kullanıcı Takımı

b. Wisdom: Öz Bilgi

c. Spyware: Ağ İzleyici

d. Worm: Truva Atı

e. Exploit: Arka Kapı

6- Bilgi güvenliğinin temel amacı hangisidir?

Birini seçin:

a. Yetkilendirmenin sağlanması

b. Erişilebilirliğin sağlanması

c. Gizliliğin sağlanması

d. Bütünlüğün sağlanması

e. Minimum Risk

7- Hangisi diğerlerinden farklıdır?

Birini seçin:

a. Test edilmemiş güvenlik sistemi

b. Yanlış eksik altyapı yatırımları

c. Yetkisiz kişilerin erişimi

d. Bant genişliğine kasteden saldırılar

e. Çalışandan gelen tehditler

8- Verilenlerden hangisi yanlıştır?

a. Bilgi güvenliğinin sağlanmasından herkes sorumludur.

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

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

d. Güvenlik risk yönetimidir.

e. Bir konu ile ilgili belirsizliği azaltan kaynak veridir.

9- Bilginin sadece yetkili kişiler tarafından erişilebilir olması gizlilik ilkesi ile sağlanır.

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

Birini seçin:

a. TCK 5651

b. TS ISO IEC 27001

c. ISO 27001 LA

d. UEKAE BGYS-0001

e. ISO 27001-5651

11- Hangisi güvenlik yönetim pratiklerinden birisi değildir?

Birini seçin:

a. Siber Saldırı Analiz Sistemi

b. Denetim

c. Risk Değerlendirmesi ve Yönetimi

d. Politika, Prosedür ve Rehberler

e. Eğitim

12- Hangisi bilgi güvenliğinin temel unsurlarından birisi değildir?

Birini seçin:

a. Bütünlük

b. Gizlilik

c. Kullanılabilirlik

d. Doğrulama

e. Erişilebilirlik

13-Kurum ya da kuruluşlari olumsuz etkileyebilecek unsurlara tehdit denir.

14- Varlıkların sahip olduğu ve istismar edilmesi durumunda güvenlik önlemlerinin aşılmasına neden olan eksikliklere zafiyet denir.

15- Nicel risk değerlendirmesi kapsamındaki hesaplardan biri olan yıllık kayıp beklentisi hesaplanırken yıllık gerçekleşme ihtimalini nasıl değerlendirirsiniz?

Birini seçin:

a. Tekil kayıp beklentisine bakarak

b. Sonraki yılda gerçekleşme oranını tahmin ederek

c. Önceki gerçekleşme değerlerine (istatistiki verilere) bakarak

d. Varlık değerine bakarak

e. Korunma maliyetine bakarak

16- Hangisi dönem projesi olarak önerdiğim konseptlerden birisi değildir?

Birini seçin:

a. Antivirüs sistemleri

b. Biyometrik güvenlik sistemleri

c. Security information event management

d. Sosyal medya analizi

e. Arama motoru optimizasyonu

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

Birini seçin:

a. Uygulama

b. Analiz

c. Oluşturma

d. Geliştirme

e. İzleme

18- Bilgi güvenligi alaninda dünya genelinde yaygin olarak kullanilan uluslararasi standart iso 27001 dir.

19- Beyaz şapkalı hacker anlamına gelen kısaltmadır. Aynı zamanda bilgi güvenliği alanındaki temel standart ve yine bu alandaki önemli eğitimlerden biri CEH dır.

20- Bir dosyanın değişip değişmediği bilgi güvenliği ilkelerinden bütünlük ile ilgilidir.

21- Güncel bir kötücül yazılım türü olan ve fidye yazılımı olarak bilinen yazılıma ransomware denir.

22- Dijital delillerin doğrulanamaması

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

Birini seçin:

a. doğruluğu

b. bütünlüğü

c. doğrulanamaması

d. farklı zamanlarda değerlendirilebilmesi

e. inkar edilememesi

23- Hangisi adli bilişim görev alanlarından biri değildir?

Birini seçin:

a. Steganografi

b. Veri Kurtarma

c. Veri İmha Etme

d. Veri Üretme

24- Dijital delillerin kanıt olarak değer kazanabilmesi için incelenmesi gereken son aşama raporlama 'dır.

25- 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 ***phishing*** 'dır. (literatürdeki orjinal ifadeyi veriniz)

26-günümüzde saldiri karmaşikligi ile saldirganin teknik bilgisi arasinda ters oranti vardir.

* Dogru

* Yanls

27-Uzak bir hedefteki sunucunun aktif olup olmadigini ICMP Protokolü ile öğreniriz.

28- DNS açılımı Domain Name System

29- İP, Internet protocol ifadesinin kısıtlamasıdır.

30- Geliştirilecek bir yazılımda özel bir port kullanılacaksa … başvuru yapılır.

31- Ağ cihazlarının aksaklıklarını bulması ile ünlenen yazılım hangisidir?

Birini seçin:

a. Shadow Security Scanner

b. Acunetix Vulnerability Scanner

c. Net Gadgets

d. GFI Lan Guard Network Security Scanner

e. Nmap

32- Bir şifre için olası tüm ihtimallerin denenmesi şeklindeki saldırıya brute force / kaba kuvvet denir. (cevabınızı ya ingilizce ya da türkçe olarak yazın. her iki dilde birlikte yazmayın!)

33- Kurulum ve çeşitli konfigürasyon özelliklerini ders kapsamında paylaştığımız SNORT ..... konseptinde açık kaynak bir yazılımdır.

a. tuzak sistem

b. honeypot temelli saldırı tespit sistemi

c. ağ tabanlı saldırı tespit sistemi

d. anti malware

e. security information event management

34-Yakin tarihin en büyük siber saldirilarindan biridir. iran nükleer santrallerini hedef alsa da birçok ülke etkilenmistir. Bu saldiri hangi isimle bilinir? stuxnet

35- Açık istihbarat toplama anlamındaki metodolojiye ne isim verilir?

OSINT

36- Hangisi bilgi güvenliği alanındaki güncel mesleklerden biri değildir?

Birini seçin:

a. Incident Responder

b. Malware Analyst

c. Security Architect

d. Computer Security Developer

e. Network Security Engineer

37- Uzaktaki bir makinenin işletim sistemini tespit etmek için yapılan çalışmalara genel olarak ne ad verilir.

fingerprinting

38- snort saldırı tespit sisteminde paket yakalamak için kullanılan kütüphane nedir?

Lib backup

39- snort saldırı tespit sisteminde paket analizi için kullanılan kütüphane nedir?

Tcpdump

40- Ders kapsamında tanıtılan üstveri analiz aracının adı nedir? (Metadata analiz aracı)

foca aracı