Bilgi Güvenliği ve Yönetim Sistemi All Of Time Questions

Vize 2020-11-23 Soruları Pazartesi: Saat 10: Soru Sayısı 40 Tane: Her Soru (Puanı) 2.50 Üzerinden

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. Varlık değerine bakarak

d. Sonraki yılda gerçekleşme oranını tahmin ederek **e. Önceki gerçekleşme değerlerine 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 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: **zaafiyet**

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**)

Bilgi Güvenliği 2020 Final Soruları Deprem Zamanı

Soru 1) Bir metin dosyası içerisine bir metin dosyası gizlemeye ne denir?

a. Stegonagrafi b. SAM c. LNS d. Polybus e. ADS

Soru 2) Tekrar başlatma **gerektiren güncellemeler** hangisi açısından risk oluşturur?

Veri sızması Backdoor **Rootkit**

Soru 3) 24 bitlik 1024*768 resi, bilgi saklamak için kullanılabilir kaç byte a sahiptir?

a. 256 b. 2.359.256 c. 786.432 **d. 2,359,296 (1024*768*296)** e. 884,736

Soru 4) Osman hedefındeki **sistemin haberleşme** araçlarını kullanılamaz hale getirmek istemedktedir. Burada istismar edilen unsur ve söz konusu saldırı tipi hangisi olabilir?

a.Gizlilik-Fiziksel saldırı b. Bütünlük-Veri slime **c.Kullanılabilirlik-Hizmet engelleme**

d. Erişilebilirlik-Veri değiştirme e. İnkar edilemezlik-Sosyal Mühendislik

Soru 5) Bilgi Güvenliği Yönetim Sistemi ile ilgili temel sertifikasyon hangisidir?

A) ISO IEC 27001 B) CEH C) BGYS-27001 D) LA E) ISO 6698

Soru 6) Hangisi bilgi güvenliği temel unsuları arasında değerlendirilebilecek bir özelliktir?

A) Hızlı Erişim **B) Gizlenme** C) Tutarlılık D) Optimallik E) Etkinlik

Soru 7) Bir verinin bütünlüğünün kontrolü için hangisi kullanılmaz?

A) MD5 B) SHA-1 C) SHA-2 D) HAVAL **E) RSA**

Soru 8) Aşağıdakiları açklayınız?

Mean time to repari: Onarıma kadar geçen ortalama süre

Mean time to recovery/ Mean time to restore: Özellikle yazılım sistemleri için onarma kader geçen ortlama süre

Mean time to respond: Müdahale için ortalama süre

Mean time to replace: Değişim için ortlama süre

Tanımları bilgi güvenliğinin hangi unsurunu tetikler?

A) Gizlilik B) Kalite **C)Kullanılabilirlik**

D) Bütünlük E) Yetiklendirme

Soru 9) Bilgi güvenlğinde **inkar** sağlar?

A) Elektronik imza B) Hash Fonksiyonları C) Şifreleme D) Yetkilendirme E) Doğrulama

Soru 10) Aşağıdakilerden hangisi siber ortamlar hakkında savunan tarafla bir bilgi değildir?

A) Güvenliğin en zayıf halkası B) Bilgisizlik, ilgisizlik, hafife **C) Bilgi birikimi (Yatırım, Eğitim ve Zaman)**

D) Kötücül kodların gelişerek yayılması E) Tehdit ve risklere karşı önlemlerin alınması

Soru 11) Bilgi güvenliğinde bütünlük hangisi ile sağlanır?

A) Steganaliz **B) Hash – Fonksiyonları** C) Şifreleme D) Yetiklendirme E) Kimlik doğrulama

Soru 12) Bilgi sitemlerin yetkisiz erişen saldırgranlar ya da kullanıcılar hakkında bilgi toplamaya yarayan tuzak sistemler hangisidir?

A) Echelon **B) Honeypot** C) Sistem D) Firewall E)Enigma

Soru 13) Elde ettiği hacking **tecübesini savunmaya** yönelik faaliyetlerde kullanan kişileri tanımlayan sertifika hangisidir?

A) ISO IEC 27001 **B) CEH** C) BSGYS-27001 D) ECO 350 E) ISO-6698

Soru14) Aşağıdakilerden hangisi bilgisayar virüsü ve zararlı yazılım bulaştırma ihtimali yüksek olan internet sitelerinden değildir?

A) Bahis siteleri B) Bedava oyun siteleri C) Kumuar siteleri D) Torrent Siteleri **E) Kişisel blog siteleri**

Soru 15) Bir konsept olarak araştırılması söylenen winrar password recovery aşağıdaki yöntemlerden hangisi kullanır?

A) Sözlük Saldırısı **B) Kaba Kuvvet Saldırısı** C) XL5 Password Recovery D) Sniffing E) Spoofing

Soru 16) Hangisi hackerların **e-posta saldırılarında** kullandığı yötemlerden biri değildir?

A) SQL İnjection B) Çerezleri çalmak C) Sosyal Mühendislik

D) Hesaba Şifre denemesi yapmak E) Phishing Saldırıları

Soru 17) Hangisi bir **siber saldırının** aşamalarından biri değildir?

A) Sistem Sahiplenme B) SALDIRI hazırlık evresi C) Veri toplama evresi

D) Command Execution, exploiting **E) Hedef hizmet veremez hale getimek**

Soru 18) Hnagisi bilgi güvenliği temel unsularından biri değildir?

A) Erişilebilirlik B) Gizlilik C) Güvenilirlik D) Bütünlük **E) İnkar Edilemezlik**

Soru 19) Hangisi güvenlik açığı anlamına gelmektedir?

A) Vulunerability B)..... C)..... D) Wisdom E) Availability

Soru 20) İçerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları hangi tek maddesinin kampsamındadır?

A) 5498 **B) 5651** C) 5237 D) 5979 E) 27001

Soru 21) Hangisi güvenlik yönetim pratiklerinden biri değildir?

A) Kurulum B) Politika C) Eğitim D) Risk Değerlendirmesi E) Denetim

Soru 22) Dış kaynaklı bir tehdit için hangisi istismar veya risk olamaz?

A) Güncellenmemiş antivirüs sistemi B) Hatalı güvenlik duvarı yapılandırması

C) Kredi kartı bilgilerinin çalınması **D) İş devamlılığının aksaması**

E) Kötü yetiklendirme ve izleme sisteminin olmayışı

Soru 23) Hangisi güvenlik öz değerlendirme rehberidir?

A) ISO IEC 27001 B) CISSP C) ISO IEC 27991 D) NIST 800-026 E) CISA

Soru 24) Hangisi web hizmetlerine ve web uygulamalarına gelebilecek olan salıdırıları **önleyecek trafik imazları** bulunan bilgi gövenliği yardımcı aracıdır?

A) MTA **B) IDS** C) IPS D) Firewall E) WAF

Soru 25) Kurumsal yapı gereği erişim yasağı bulunan sitelerin engellenmesi işlemlerini gerçekleştiren yapılara ne denir?

A) Yük dengeleyici **B) Url fitresi** C) Web vekil sunucu D) Ağ erişim kontrolü E) Ağ izleme si

Soru 26) Aşağıdaki şifreleme algoritmalarından hangisi kaba kuvvet saldırısına karşı deiğlerinden daha zayıftır?

A) AES **B) DES** C) RSA D) 3DES E) SHA

Soru 27) Firewall ya antivirüs mantığında çalışan bir yapı hangisine karış %100 güvensizdir?

A) Zeroday Atakları B) Virüslar C) Trojanlar **D) Dos Atakları** E) Truva

Soru 28) Elektronik imzanın hukuki ve teknik yönleri ile kullanılmasına ilişkin esasları düzenleyen yasa hangisidir?

Cevap: **5070**

Soru 29) Hasas verileri koruma altına alan yasa hangisidir?

Cevap: **6698**

Bilgi Güvenliği ve Yönetim Sistemi : Final Sınav Soruları ve Cevapları

Soru 1) Aşağıdakilerden hangisi Adli bilişimin çalışma alanlarından değildir?

a) Veri kurtarma b) Veri imha etme **c) Veri madenciliği** d) Veri saklama

Soru 2) Steganografi yazılımının amacı nedir?

a) Bir ağı dinlemek b) Bir excel belgesinin şifresini çözmek

c) Bir diskin imajını almak **d) Gizli bir mesaj göndermek (örneğin; ses, metin, resim, video vb.)**

Soru 3) ……., siber ortamda verimsiz vakit geçirmek anlamına gelir. Yanında verilen dimlede boş bırakılan yere gelmesi gereken ifade aşağıdakilerden hangisidir?

a) Siber Etik b) Siber Toplum c) Siber Kültür **d) Siber Aylaklık** e) Siber Istihbarat

Soru 4) Aşağıdakilerden hangisi biyometrik bilgi güvenliği sistemi değildir?

a) Yüz tanıma sistemleri **b) Optik okuyucu** c) Retina tarama d) El izi okuma

Soru 5) "En zayıf halka olan kişisel kullanıcıların siber tehdit araçları ve korunma yollan konusunda bilgilendirme gereklidir.' Yukarıdaki tanımı verilen unsur aşağıdakilerden hangisidir? (Siber Güvenlik Unsurlar makale)

a) Teknik Tedbirlerin Geliştirilmesi **b) Farkındalığın Artırılması**

c) Kapasitenin Geliştirilmesi d) Yasal Çerçevenin Oluşturulması

Soru 6) Bir sistemi kullanılamaz hale getirmek için birden fazla kaynak kullanan saldırı türü hangisidir?

a) Dos b) Spam c) Cyberfraud (Siber sahtecilik) d) Phishing **e) DDos**

Soru 7) Aşağıdakilerden hangisi dijital delil türlerinde değildir?

a) İnternet geçmişi b) E-Posta **c) İşletim Sistemi** d) Veri dosyaları

Soru 8) Bir bilgisayar **ağındaki keşif** saldırısının amacı nedir?

a) Veri trafiğini gözlemlenebilsin diye yönlendirmek b) Kullanıcıların ağ kaynaklarına erişimi engellemek

c) Hedef ağ ve sistem hakkında bilgi toplamak d) Ağ sunucularından veri çalmak e) Hiçbiri

Soru 9) "**Anomaly**" nedir?

a) Bir ağda meydana gelen olağandışı hareketlerdir b) Bir ağ cihazıdır

c) Bir ağ yazılımıdır d) Bir protokoldür

Soru 10) Kriptografi kullanılan servislerde aşağıdakilerden hangisi **Uygulama Katmanı** Çözümlerinden değildir?

a) SET **b) S/MIME** c) S-http d) SSH

Soru 11) Aşağıdakilerden hangisi kriptolama algoritmaları ve kriptolama türlerinden olan **Veri Özeti** Algoritmalarından değildir?

a) AES b) MD5 c) SHA-1 **d) SHA-256**

Soru 12) Aşağıdakilerden hangisi simetrik kriptolama yöntemidir?

a) AES b) Disffie-Helrnan c) ECC d) RSA

Soru 13)

|. Sahte e-posta ile kimlik avı yapma

||. Gönderilen çok sayıda istekle sunucuyu devre dışı bırakma

|||. Deneme yanılma yoluyla şifre tahmininde bulunma

Yukarıdaki **ifadelere denk gelen** kavramlar aşağıdaki seçeneklerin hangisinde doğru verilmiştir?

a) I. Phishing I I. DDos I I I. Sniffing

b) I. Rainbow I I. Phishing I I I Sniffing

c) I.Sniffing I I.DoS Brute Force

d) I.Brute Force II.Sniffıng III Phishing

e) I. Phishing I I. DDos I I I. Brute Force

Soru 14) Iyi niyetli, zarar vermeyen, amaçları **bilgisayar güvenliğini sağlamak** olan hacker türü aşağıdakilerden hangisidir?

a) Beyaz şapkalı b) Lamer c) Siyah şapkali d) Gri sapkalı

Soru 15) Aşağıdakilerden hangisi bir siber saldırı aşama değildir?

a) Halt(Durma) b) Recoinnaissance(Keşif)

c) Propagation(Yayılma) d) Command and Control(Kontrolii ele geçirme)

Soru 16) İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkındaki kanun aşağıdakilerden hangisidir?

a) Elektronik imza kanunu b) 5237 TCK

c) 5651 sayılı kanun d) 5271 CMK e) Cenevre Sözleşmesi

Soru 17) Aşağıdakilerden hangisi siber saldırı niteliği taşımaz?

a) E-posta kutunuza reklam ve virüs içerikli postaların düşmesi

b) Web taraşncınaın anasayfanın kendiliğinden değişmesi

c) Flash diskinizdeki bir klasöre tıkladığınızda kendini sürekli çoğaltması

d) Güncelleme gerektirmeyen bir program için sürekli olarak gmcelle penceresinin açılması

e) internet bankacılığı oturumunu açtığınızda şifre değişiminin talep edilmesi

Soru 18) Aşağıdakilerden hangisi Ulusal Siber Güvenliğin sağlanması için uzman personel eğitir?

a) TİB b) MIT **c) BTK** d) Siber Güvenlik Kurulu e) TÜBİTAK

Soru 19) Stenografide **gizli bilgiyi** taşıyan **orijinal dosyaya** ne denir?

a) Saklayıcı ortam b) Taşıyıcı ortam c) Gizleyici ortam **d) Stenografık taşıyıcı**

Soru 20) Aşağıdaki yöntemlerden hangisi bankacılık alanında düzenlenen saldırıların çoğunluğunda hedef sisteme sızmak için ilk adım olarak kullanılmaktadır?

a) Oltalama amaçlı e-posta gönderme b) işietim sistemi açıklıklarını kullanma

c) Sistem hakkında bilgi toplama d) Sosyal mühendislik e) BackDoor kullanma

Soru 21) Aşağıdakilerden hangisi aktif saldırı yöntemi değildir?

a) İnternet trafiğini takip b) Sniffer olayı **c) Eski mesajların tekrarlanması** d) IP aldatmacası

Soru 22) Kurum, kuruluş ve kullanıcıların **bilgi varlıklarını korumak amacıyla** kullanılan yöntemler, politikalar, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama deneyimleri ve kullanılan teknolojiler bütününe **siber güvenlik denir.** **DOĞRU** YANLİŞ

Soru 23) Phishing nedir?

a) İkna yöntemiyle gizli bilgilerin elde edilmesini amaçlayan bir sosyal mühendislik **rnetodudur**.

b) Yasal bir e-posta gibi görünen be kişisel bilgilerinizi talep eden e-posta mesajların genel adıdır.

c) Yukarıdakilerden hepsi doğrudur. d) Kimlik hırsızlığıdır. e) Yukarıdakilerden hiçbiri doğru değildir.

Soru 24) Aşağıdakilerden hangisi tehlikeli yazılımlara örnek değildir?

a) Yama olarak internetten indirilmiş herhangi bir program b) Crack programlar

c) Korsan mUzikler ve film dosyaları d) Korsan yazılı mlar **e) Yazılım güncellemeler**

Soru 25) Bilginin saklanması işlemini **kontrol etmek için ve gömülü bilginin elde edilmesini zorlaştırmak** için aşağıdakilerden hangisi kullanılmaktadır?

a) Stego-object b) Cover-data c) Stego-text **d) Stego-key**

Soru 26) Aşağıdakilerden hangisi **AES** şifrelerne için kullanılan algoritma değildir?

a) AES 64bit b) AES 256bit c) AES 128bit d) AES 192bit

Soru 27) Tecrübe veya öğrenme şeklinde veya iç gözlem şeklinde elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasına ne denir?

a) Veri b) Bilgi c) Hikmet **d) Özbilgi**

Soru 28) Aşağıdakilerden hangisi **HASH algoritması** değildir?

a) SHA-1 b) MD5 **c) WPA** d) Checksurn

Soru 29) İnternet ortamında yapılan yayınların içeriklerini izlemek ve gerekli tedbirleri almak hangi kurumun görevleri arasındadır?

a) TİB (Telekominikasyon İletişim Başkanlığı) **b) BTK (Bilişim Teknoloji Kurumu)**

c) siber Güvenlik Kurulu d) Cumhuriyet Kurulu e) TBMM

Soru 30) DOS ve DDOS saldırılarının **öncelikli hedefi** aşağıdakilerden hangisidir?

a) Hedefi iş göremez hale getirmek b) Hedefi ele geçirip saldırı amaçlı kullanmak

c) Hedef hakkında bilgi toplamak d) Hedeften veri çalmak

e) Hedefte yapılan tüm işlemleri izleme altına almak

Soru 31) Wireshark programında Protocol tree deki bütün alt dizilari kapatan seçenek hangisidir?

a) Collapse All b) Coloring Rules c) Ezpand All d) Show Packet in New

Soru 32) Genelde lise çağında olan, programlama bilgisi olmayan genellikle **e-postalara saldırı** işlemlerini öğrenen kişilere ne ad verilir?

a) Beyaz Şapkalı b) Gri Şapkalı c) Siyah Şapkalı **d) Script Kiddie**

Soru 33) Wireshark programında **yakalanmış paketlerin** nereden geldiğini gösteren seçenek hangisidir?

a) Source b) Destination c) No d) Protocol

Soru 34) Kötücül yazılımlara verilen genel ad nedir?

a) Malware b) Virüs c) Spyware d) Adware

35) Wireshark programında toplanan paketleri metin dosyası dışa aktarmaya yarayan seçenek hangisidir?
a) As "C5V" File b) As "PostScript" File c) As "PDML" file **d) As "Plain Text" File**

Soru 36) Aşağıdakilerden hangisi dijital delillerin, normal somut delillere göre farklarından değildir?

a) Dijital delillerin daha kolay bulunması b) Dijital delillerin bütünlüğü

c) Dijital delillerin inker edilememesi d) Dijital delillerin doğrulanması

Soru 37) Wireshark programında paket numarasına göre istenilen pakete zıplamaya yarayan seçenek aşağıdakilerden hangisidir?

a) Previous Packet **b) Go To Packet** c) Fonyard d) Go To Corresponding Packet

Soru 38) Bir web uygulamasında güvenli erişim yolu **(SSL)** kullanıldığı nasıl ayırt edilir?

I. Adres http ile değil https ile başlar. I I. Tarapoda kilit ikonu vardır.

I I I. Güvenilir bir sertifikası vardır. IV. Sertifikası geçerlidir.

a) |.||.|||.|V b) |.||.||| t) |||.|V d) |.||

Soru 39) Aşağıdakilerden hangisi **sayısal imza** olarak kabul edilir?

a) ECC (Elliptic Cunıe Cryptosystem) b) Twofish

c) DSA (Digital Signature Algorithm) d) Diffie-Helman

Soru 40) Internette üye olduğunuz bir sitede şifrenizi unuttuğunuzu varsayalım. Sitenin "**şifremi unuttum**" hizmetinden faydalandığınızda sistem e-mail adresinize, sisteme kayıt olurken gönderdiğiniz parolayı değil de "**parola sıfırlama linki**" gönderiyorsa o site veritabaninda hangi şifreleme algoritması kullanıllyordur?

a) CRC32 b) SMTP c) IPS **d) MD5** e) Adler32

Soru 41) Wireshark Programında Ethernet Filters seçeneklerinde hangisi **6 bitlik mac adresi** tipindedir?

a) eth.dst b) eth.type **c) eth,src** d) eth.len

Soru 42) Aşağıdakilerden hangisi internet bankacılığının güvenli kullanımı için alınması gereken öncelikli tedbirlerden değildir?

a) Güncel ve lisanslı koruma yazılımı kullanmak

b) Tek kullanımlık şifre üreten cihazlar kullanmak

c) Kaynağı belirsiz internet tarayıcısı eklentileri yüklememek

d) İnternet bankacılığına giriş için kullanılan telefona mobil yazılımları kurmak

e) Online bankacılık hesabı için statik IP adresi tanımlamak

Soru 43) Adli bilişimde dijital delillerin kanıt olarak kullandabilmesi için incelenmesi gereken safhalarından değildir?

a) Saklama b) Raporlama c) İnceleme d) Çözümleme

Soru 44) Bilginin bir varlık olarak **hasarlardan korunması, istenmeyen kişiler** tarafından elde edilmesini önlemeye bilgi güvenliği denir. **a) True** b) False

Soru 45) Aşağıdakilerden hangisi bilgi güvenliği kavramının temel ilkelerinden değildir?

a) Ulaşılabilirlik **b) Bilginin yönetilmesi** c) Bütünlük d) Gizliliğin korunması

Soru 46) Bir sisteme saldırı yapılmadan önce sistem hakkında bilgi edinilmesi gerekmektedir. Aşağıdakilerden hangisi bilgi toplama aşaması dışındadır?

a) İşletim sistemlerin tespiti **b) Kendi sistemini tanımak**

c) Network IP aralığını bulmak d) Açık port ve erişim noktalarının tespiti

Soru 47) Wireshark programı aşağıdakilerden hangisi için kullanılmaz?

a) Saldırı tespiti b) IP yönlendirme c) Ağ trafik tespiti **d) Veri madenciliği**

Final 2020-01-19 Soruları Salı - Saat 2.00 PM

Soru 1) Aşağıdakilerden hangisi iyi bir bilgi güvenliği programı içerisinde yer almaz?

a. Değerlendirme aşamasına yer verilmez b. Güvenlik örgütlemesi içerir

c. Politika, prosedür ve standartlar içerir d. Bilgiyi Sınıflandırma Risk yönetimi mevcuttur

Soru 2) İyi bir bilgi güvenliği analizi için hangi tür sorunlara cevap aranır?

a. Bu varlıkları nelere karşı korumalıyız? b. Bir tehdit'in varlıklarımızı bozma olasılığı nedir? **c. Hepsi**

d. Bir tehlikeli saldırı olması durumunda ivedi maliyet ne olacaktır e. Ne tür varlıkları korumakgereklidir?

Soru 3) Aşağıdakilerden hangisi potansiyel saldırı kaynakları arasında yer almaz?

a. Modem havuzu üzerinden b. Dahili Sistemler c. İnternet bağlantısı üzerinden

d. Çevresel faktörler e. Çevre ofis erişim noktaları

Soru 4) Güvenlik politikası için aşağıdakilerden hangisi yanlıştır?

a. Güvenlik işlerini tüm kurum faaliyetlerine entegre etmek amaçlanır **e. Tekniktir**

b. Zamanla güncellenmelidir c. Kolay anlaşılabilir olmalıdır d. Öneri tavsiye değil emir kipi kullanılır

Soru 5) Güvenlik Politikası oluşturulurken hangi sorulara cevap aranmaz?

a. Kime, nereye, ne zaman ve hangi yetkiyle izin yenilebilir?

b. Hangi aktiviteler tehdit olarak görülür ve güvenlik riski yaratırlar?

c. Ne tip gözden kaçmalar ve dikkatsizlikler olabilir? **d. Ne tür varlıkları korumak gereklidir?**

e. Güvenlik politikasının gerçekleştirilmesinde kim, ne yetki ve sorumluluğa sahiptir?

Soru 6) Aşağıdakilerden hangisi güvenlik politikası kavramları arasında yer almaz?

a. Prosedür b. Standart c. Temel d. Yönerge **e. Tehditler**

Soru 7) Aşağıdakilerden hangisi iyi bir güvenlik politikasında yer almaz?

a. Güvenlik hedefleri açıkça tanımlanmalıdır b. Kullanıcıdan beklenen gizliliğin seviyesini tanımlamalıdır.

c. Kuruluş üyelerinin görev ve sorumlulukları, açıklanan sonuçlarda belirtilmelidir.

d. Kuruluşta yer alan belirli kişiler tarafında erişilebilir olmalıdır.

e. Politikada açıklanan her bir konu doğru bir şekilde tannnlannıalidir.

Soru 8) Aşağıdakilerden hangileri **risk çeşitleri** arasında yer alır?

a. İnsan etkeni b. Cihaz hatası c. İç ve dış saldırılar d. Veri kaybı **e. Hepsi**

Soru 9) Aşağıdakilerden hangisi **pasif bilgi** toplama yöntemleri arasında yer almaz?

a. Whois b. ARIN c. Link Extraction **d. Nmap** e. theharvester

Soru 10) Aşağıdakilerden hangisi **varlık listeleri** için doğru değildir?

a. Risk analizi için başlangıç noktasıdır

b. VarlIdarm sahipleri ve değeri belirlenerek varlık envanteri oluşturulur.

c. Önce varlıklar ve isimleri tespit edilmelidir

d. Yazılım varlıkları en somut varlıklar olduğu için buradan başlanması kolaylık sağlayacaktır.

e. Varlık listesine, varlıklarm fiziksel yeri, formatı, yedeği olup olmadığı gibi olası bir felaketten kurtarma durumunda gerekli olacak bilgiler girilir.

Soru 11) Bir risk belirleme tablosunda kurumsal iş sürecinin bazı varlıkları yer alır. Aşağıdakilerden hangisi bu varlıklar arasında yer almaz?

a. çevresel b. bilgi c. alınan hizmet d. yazılım e. insan

Soru 12) Aşağıdakilerden hangisi insani ve kasıtlı tehdit türleri arasında yer almaz?

a. Hatalı Yönlendirme b. Bilgi değiştirme c. Hırsızlık d. Kötücül yazılım e. Dinleme

Soru 13) Aşağıdakilerden hangisi Risk değerlendirilmesi sonucu elde edilmez?

a. Kabul edilebilir risk seviyesi belirlenir
b. Güvenlik ihlalinin oluşma olasılığımn belirlenmesi.
c. Tüm çalışanlar listelenir.
d. Riskler kritiklik sırasına göre sıralanır.
e. Azaltılacak risk kalemlerinin öncelikleri belirlenir.

Soru 14) Aşağıdakilerden hangisi **klasik şifreleme** algoritmalarından biridir?

a. Simetrik Şifreleme b. Blok Şifreleme e. Dizi Şifreleme **d. Yer Değiştirme** e. Asimetrik Şifreleme

Soru 15) Whois için aşağıdakilerden hangisi doğrudur?

a. Alan adı bilgisi yer alır b.TCP 43. Portta çalışır c. TCP tabanlı bir sorgu protokolüdür
d. Pentrasyon testlerinin ikinci adımında gerçekleştirilir e. IP adresi sorgulamak için kullanılabilir

Soru 16) Aşağıdakilerden hangisi bir **paketin istediği adrese gidene kadar** hangi hostlar ve yönlendirmelerden geçtiğini gösterir?

a. Nmap b. TheHarvester **c.Traceroute** d. DIG e. Dirbuster

Soru 17) Aşağıdakilerden hangisi **Nmap** kullanılarak elde edilebilecek bilgiler arasında yer almaz?

a. Çalışan fiziksel aygıt tipleri
b. Ağa bağlı herhangi bir bilgisayarın işletim sistemi
c. Yazılımlarm hangi servisleri kullandığı
d. Bir paketin gönderilirken geçtiği hostlar
e. Bilgisayarın yazılımlarmın sürüm numaraları

Soru 18) Aşağıdaki tarama türlerinden hangisinde kaynak makina hedef makinayı tarama esnasında aktif olarak rol almaz?

a. FFP Bounce Scan b. ACK Scan c. IP Protocol Scan d. RPC Scan **e. Idle Scan**

Soru 19) Aşağıdakilerden hangisi aktif bilgi toplama araçları içerisinde yer almaz?

a. Nmap b. Wireshark c. Dig 111 **d. ARIN** e.Robtex

Soru 20) Aşağıdakilerden hangisi Pasif bilgi toplama yöntemleri arasında yer almaz?

a. Github b. Kariyer Siteleri **c. Masscan** d. Sosyal Paylaşım Ağları e. Arama Motorları

Soru 21) Hedef sistem üzerinde **iz bırakmadan** yapılan bilgi keşfi çalışmalarına …….. denir.

Yanıt: pasif bilgi toplama

Soru 22) Kurumun ihtiyaçlarıyla doğrudan ilişkili olan, genel terimlerin yer aldığı, yapı ve teknolojideki değişimlere göre esnek olarak hazırlanan kurumun güvenlik hedeflerini belirleyen yazılı dokümanlara …… denir.

Yanıt: 6563 Sayılı Kanun

Soru 23) Varlık üzerinde tehdit oluşturan bir zafiyetin bir tehdit ajanı tarafından kullanılmasına bağlı zarar beklentisine …….. denir.

Yanıt: risk

Soru 24) Herhangi bir saldırganın sisteme, yazılıma ve varlığa zarar vermek için yararlanabileceği, ilgili sistemde bulunan açıklıklar, eksiklikler ve zayıflıklara …….. denilir.

Yanıt: Açıklık, Vulnerability

Soru 25) Sistemde bulunan herhangi bir açıldlıktan faydalanılarak sisteme zarar verilmesi işlemine …… denir.

Yanıt: sömürücü, exploit

Soru 26) Zaafiyetlerden faydalanacak kişi veya örgüte …… denilir.

Yanıt: saldırganlar

Soru 27) Risk işleme sonrasında kalan riske ……. …… denir.

Yanıt: residual risk

Soru 28) Alfabenin harfleri, noktalama işaretleri, kelimeleri yerine semboller ve kısaltmalar kullanan çabuk yazma; not tutma sistemi olarak ta bilinen gizlenmiş bilgiye …….. denir.

Yanıt: steganography, Stenografi

Soru 29) Hedef sistem ile doğrudan iletişime geçilerek bilgi elde etme çalışmaları …….. dır.

Yanıt: **aktif bilgi toplama**

Soru 30) Açık ve gizli olmak üzere iki anahtarın varlığına dayalı şifreleme yöntemine …….. denir.

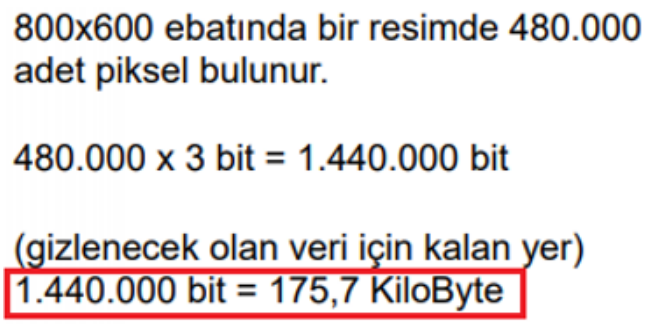
Yanıt: **Asimetrik Şifreleme (Asymetric Encryption)**

Soru 31) 800x600 boyutunda bir **RGB** resme kaç **KB** veri gizlenebilir?

800x600 boyutında bir resimde 480.000 adet piksel bulunur. 480.000 x 3 bit **= 1.440.000 bit**

(gizlenecek olan veri için kalanyer) 11.440.000 bit = **175,7 KiloByte**)

Yanıt: **175,7**



Soru 32) Dijital bir belge inkar edilemezlik özelliğini …….. ile kazanır.

Yanıt: **E-imza**

Soru 33) Bir sunucudaki **log** dosyasının **değiştirilip değiştirilmediğini** anlamak için …….. algoritmalarından faydalanırız.

Yanıt: **DNS**

Soru 34) Genel olarak source internet protocol numarasının değiştirilmesi şeklindeki saldırı türüne …….. denir.

Yanıt: **Spoofing**

Soru 35) Sezar **3 yapısına** göre **ABC** ifadesinin şifrelenmiş hali ……'dir.

Yanıt: **DEF**