

## Bilgi Güvenliđi 2020 Final Soruları Deprem Zamanı

**Soru 1)** Bir metin dosyası ierisine bir metin dosyası gizlemeye ne denir?

- A) Stegonagrafi**
- B) SAM
- C) LNS
- D) Polybus
- E) ADS

**Soru 2)** Tekrar bařlatma gerektiren gncellemeler hangisi aısından risk oluřturur?

- A)
- B)
- C) Veri sızması
- D) Backdoor
- E) Rootkit**

**Soru 3)** 24 bitlik 1024\*768 resi, bilgi saklamak iin kullanılabilir ka 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 hedefindeki sistemin haberleřme aralarını kullanılamaz hale getirmek istemedktedir. Burada istismar edilen unsur ve sz konusu saldırı tipi hangisi olabilir?

- A) Gizlilik-Fiziksel saldırı
- B) Btnlk-Veri slime
- C) Kullanılabilirlik-Hizmet engelleme**
- D) Eriřilebilirlik-Veri deđiřtirme
- E) İnkâr edilemezlik-Sosyal Mhendislik

**Soru 5)** Bilgi Gvenliđi Ynetim Sistemi ile ilgili temel sertifikasyon hangisidir?

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

**Soru 6)** Hangisi bilgi gvenliđi temel unsuları arasında deđerlendirilebilecek bir zelliktir?

- A) Hızlı Eriřim
- 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)** Aşağıdakileri açıklayınız?

**Mean time to repair:** Onarıma kadar geçen ortalama süre

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

**Mean time to respond:** Müdahale için ortalama süre

**Mean time to replace:** Değişim için ortalama süre

Tanımları bilgi güvenliğinin hangi unsurunu tetikler?

- A) Gizlilik
- B) Kalite
- C) **Kullanılabilirlik**
- D) Bütünlük
- E) Yetkilendirme

**Soru 9)** Bilgi güvenliğinde 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 alma
- 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) Yetkilendirme
- E) Kimlik doğrulama

**Soru 12)** Bilgi sistemlerin yetkisiz erişen saldırırganlar 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) XLS Password Recovery
- D) Sniffing
- E) Spoofing

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

- A) SQL Injection**
- 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 getirmek**

**Soru 18)** Hnagisi bilgi güvenliđi temel unsularından biri deđildir?

- A) Eriřilebilirlik
- B) Gizlilik
- C) Güvenilirlik
- D) Bütünlük
- E) İnkâr Edilemezlik**

**Soru 19)** Hangisi güvenlik açığı anlamına gelmektedir?

- A) Vulnerability**
- B)
- C)
- D) Wisdom
- E) Availability

**Soru 20)** İçerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlölük ve sorumlulukları hangi tek maddesinin kapsamındadır?

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

**Soru 21)** Hangisi güvenlik yönetim pratiklerinden biri deđildir?

- A) Kurulum**
- B) Politika
- C) Eğitim
- D) Risk Deđerlendirmesi
- 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) Kötü yetiklendirme ve izleme sisteminin olmayışı
- E) İş devamlılıđının aksaması**

**Soru 23)** Hangisi güvenlik öz deđerlendirme 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 saldırıları önleyecek trafik imazları bulunan bilgi güvenliği 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) Web vekil sunucu
- C) Url fitresi**
- D) Ağ erişim kontrolü
- E) Ağ izleme sistemi

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

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

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

- A) Zero-day Atakları
- B) Virüsler
- 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**

1) Aşağıdakilerden hangisi Adli bilişimin çalışma alanlarından değildir? (2.hafta) a) Veri kurtarma b) Veri imha etme c) Veri madenciliği d) Veri saklama C
2) Steganografi yazılımının amacı nedir? (4.hafta) a) Bir diskin imajını almak b) Bir excel belgesinin şifresini çözmek c) Gizli bir mesaj göndermek (örneğin; ses, metin, resim, video vb.) d) Bir ağı dinlemek
3) ....., siber ortamda verimsiz vakit geçirmek anlamına gelir. Yanda verilen cümlede boş bırakılan yere gelmesi gereken ifade aşağıdakilerden hangisidir? a) Siber Etik b) Siber Toplum c) Siber Kültür d) Siber Aylaklık e) Siber İstihbarat
4) Aşağıdakilerden hangisi biyometrik bilgi güvenliği sistemi değildir? (8.hafta) a) Yüz tanıma sistemleri b) Optik okuyucu c) Retina tarama d) El izi okuma
5) “En zayıf halka olan kişisel kullanıcıların siber tehdit araçları ve korunma yolları 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 e) Ulusal Politika ve Stratejinin Geliştirilmesi
6) Bir sistemi kullanılamaz hale getirmek için birden fazla kaynak kullanan saldırı türü hangisidir? (1.Hafta) a) Dos b) Spam c) Cyberfraud(Sibersahtecilik) d) Phishing e) DDos
7) Aşağıdakilerden hangisi dijital delil türlerinde değildir? (2.hafta) a) İnternet geçmişi b) E-Posta c) İşletim Sistemi d) Veri dosyaları
8) Bir bilgisayar ağındaki keşif saldırısının amacı nedir? a) Ağ sunucularından veri çalmak b) Kullanıcıların ağ kaynaklarına erişimi engellemek c) Hedef ağ ve sistem hakkında bilgi toplamak d) Veri trafiğini gözlemlenebilsin diye yönlendirmek e) Hiçbiri
9) “Anomaly” nedir? a) Bir ağda meydana gelen olağandışı hareketlerdir. b) Bir ağ cihazıdır c) Bir ağ yazılımıdır.

d) Bir protokoldür
10) Kriptografi kullanılan servislerde aşağıdakilerden hangisi Uygulama Katmanı Çözümlerinden değildir? a) SET b) S/MIME c) S-http SSH
11) Aşağıdakilerden hangisi kriptolama algoritmaları ve kriptolama türlerinden olan Veri Özeti Algoritmalarından değildir? a) AES b) MD5 c) SHA-1 d) SHA-256
12) Aşağıdakilerden hangisi simetrik kriptolama yöntemidir? a) AES b) Diffie-Hellman c) ECC d) RSA
13)  . Sahte e-posta ile kimlik avı yapma   . Gönderilen çok sayıda istekle sunucuyu devre dışı bırakma    . Deneme yanılma yoluyla şifre tahmininde bulunma  Yukarıdaki ifadelerle denk gelen kavramlar aşağıdaki seçeneklerin hangisinde doğru verilmiştir? a)  . Phishing   . DDos    . Sniffing b)  . Rainbow   . Phishing    . Sniffing c)  .Sniffing   .DoS    . Brute Force d)  .Brute Force   . Sniffing    . Phishing e)  . Phishing   . DDos    . Brute Force
14) İyi niyetli, zarar vermeyen, amaçları bilgisayar güvenliğini sağlamak olan hacker türü aşağıdakilerden hangisidir? a) Beyaz şapkalı b) Lamer c) Siyah şapkalı d) Gri şapkalı
15) Aşağıdakilerden hangisi bir siber saldırı aşama değildir? a) Reconnaissance(Keşif) b) Halt(Durma) c) Propagation(Yayılma) d) Command and Control(Kontrolü ele geçirme)
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
17) Aşağıdakilerden hangisi siber saldırı niteliği taşımaz? a) E-posta kutunuza reklam ve virüs içerikli postaların düşmesi b) Web tarayıcınızın anasayfanın kendiliğinden değişmesi c) Flash diskinizdeki bir klasöre tıkladığınızda kendini sürekli çoğaltması d) Güncelleme gerektirmeyen bir program için sürekli olarak gmcelle penceresinin açılması e) İnternet bancacılığı oturumunu açtığınızda şifre değişiminin talep edilmesi

18) Aşağıdakilerden hangisi Ulusal Siber Güvenliğin sağlanması için uzman personel eğitir?	a) TİB b) MIT c) <b>BTK</b> d) Siber Güvenlik Kurulu e) TÜBİTAK
19) Stenografide gizli bilgiyi taşıyan orijinal dosyaya ne denir?	a) Saklayıcı ortam b) Taşıyıcı ortam c) Gizleyici ortam d) <b>Stenografik taşıyıcı</b>
20) Aşağıdaki yöntemlerden hangisi bankacılık alanında düzenlenen saldırıların çoğunluğunda hedef sisteme sızmak için ilk adım olarak kullanılmaktadır?	a) Ortalama amaçlı e-posta gönderme b) İşletim sistemi açıklıklarını kullanma c) <b>Sistem hakkında bilgi toplama</b> d) Sosyal mühendislik e) BackDoor kullanma
21) Aşağıdakilerden hangisi aktif saldırı yöntemi değildir?	a) İnternet trafiğini takip b) Sniffer olayı c) <b>Eski mesajların tekrarlanması</b> d) IP aldatmacası
22) Phishing nedir?	a) İkna yöntemiyle gizli bilgilerin elde edilmesini amaçlayan bir sosyal mühendislik metodudur. b) Kimlik hırsızlığıdır. c) Yasal bir e-posta gibi görünen ve kişisel bilgilerinizi talep eden e-posta mesajlarının genel adıdır. d) <b>Yukarıdakilerden hepsi doğrudur.</b> e) Yukarıdakilerden hiçbirisi doğru değildir.
23) 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.	<b>DOĞRU</b> YANLIŞ
24) Aşağıdakilerden hangisi tehlikeli yazılımlara örnek değildir?	a) Yama olarak internetten indirilmiş herhangi bir program b) Crack programlar c) Korsan müzikler ve flim dosyaları d) Korsan yazılımlar e) <b>Yazılım güncellemeler</b>
25) Bilginin saklanması işlemini etmek için ve gömülü bilginin elde edilmesini zorlaştırmak için aşağıdakilerden hangisi kullanılmaktadır?	a) Stego-object b) Cover-data c) Stego-text d) <b>Stego-key</b>



26) Aşağıdakilerden hangisi AES şifreleme için kullanılan algoritma değildir?

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

27) 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

28) 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

29) Aşağıdakilerden hangisi HASH algoritması değildir?

- a) SHA-1
- b) MD5
- c) WPA
- d) Checksum

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

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

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

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

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

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

34) Kötücül yazılımlara verilen genel ad nedir?

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

35) Wireshark programında toplanan paketleri metin dosyası dışı aktarmaya yarayan seçenek hangisidir?

- a) As "CSV" File
- b) As "PostScript" File
- c) As "PDML" file
- d) **As "Plain Text" File**

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

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

- a) Previous Packet
- b) **Go To Packet**
- c) Forward
- d) Go To Corresponding Packet

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

- |. Adres http ile değil https ile başlar.
- ||. Tarayıcıda kilit ikonu vardır.
- |||. Güvenilir bir sertifikası vardır.
- |V. Sertifikası geçerlidir.

- a) **|,||,|||,|V**
- b) |,||,|||
- c) |||,|V
- d) |,||

39) Aşağıdakilerden hangisi sayısal imza olarak kabul edilir?

- a) ECC ( Elliptic Curve Cryptosystem )
- b) Twofish
- c) **DSA ( Digital Signature Algorithm )**
- d) Diffie-Helman

40) İnternette 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 veritabanında hangi şifreleme algoritması kullanılıyordur?

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

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

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

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

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

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

44) Bilginin bir varlık olarak hasarlardan korunması, istenmeyen kişiler tarafından elde edilmesini önlemeye bilgi güvenliği denir.

- a) True
- b) False

45) Aşağıdakilerden hangisi bilgi güvenliğinin temel ögesi değildir?

- a) Gizlilik
- b) Erişilebilirlik
- c) Çeşitlilik
- d) Bütünlük

46) Aşağıdakilerden hangisi bilgi güvenliği kavramının temel ilkelerinden değildir?

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

47) 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

48) Wireshark programı aşağıdakilerden hangisi için kullanılmaz?

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

1. Bilgi Gizleme nedir?  
**Steganography**
2. Saldırgan terimleri nelerdir?  
**Attacker, Hacker, Intruder**
3. Klavye dinleme sistemi nedir?  
**Keylogger**
4. Kötücül yazılım analizi nedir?  
**Malware**
5. Kaynak kod istismarı-korunmasızlık sömürücü nedir?  
**Exploit**
6. Hizmet aksattırma saldırısı nedir?  
**DoS(Denial of the Service)**
7. Dağıtık hizmet aksattırmaya nedir?  
**DdoS**
8. Casus yazılıma nedir?  
**Spyware**
9. Kök kullanıcı takımına nedir?  
**Rootkit**
10. Koklayıcı, ağ izleyici nedir?  
**Sniffer**
11. Bilgi güvenliğinin temel amacı nedir?  
**Gizlilik (Confidentiality),  
Bütünlük (Integrity),  
Kullanılabilirlik (Availability)**
12. Gizlilik nedir?  
**Kuruma özel ve gizliliği olan bilgilere, sadece yetkisi olan kişilerin sahip çıkmasıdır.**
13. Bütünlük nedir?

**Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.**

14. Kullanılabilirlik nedir?

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

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

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

16. Bilgi güvenliğinden kim sorumludur?

**Bilginin sahibi, Bilgiyi yöneten, Bilgiyi kullanan  
(bilgi güvenliğinden herkes sorumludur.)**

17. Bilgi nedir?

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

18. Hangisi güvenlik yönetim pratiklerinden değildir?

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

19. Risk değerlendirmesi nedir?

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

20. Risk yönetimi nedir?

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

21. Risk yönetimi aşamaları nelerdir?

- **Risk yönetim ekibi kurma**
- **Tehdit ve zaafiyetleri doğrulama**
- **Organizasyon varlıklarının değerlerini belirleme**
- **Riske karşı yapılacak hareketleri belirleme**

22. Risk yönetimi kavramları nelerdir?

**Tehdit, Zaafiyet, Kontroller**

23. Tehdit nedir?

**Organizasyonu olumsuz etkileyebilecek olan insan yapımı veya doğal olaylar**

24. Zaafiyet nedir?

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

25. Kontroller nedir ve nelerdir?

**Zaafiyetlerin boyutunu azaltıcı, koruyucu veya etkilerini azaltıcı önlemler**

– Caydırıcı Kontroller

– Saptayıcı Kontroller

– Önleyici Kontroller

– Düzeltici Kontroller

26. Doğal tehdit belirleme olayları nelerdir?

**Deprem, sel, kasırga**

27. İnsan yapımı dış kaynaklı tehdit belirleme olayları nelerdir?

**Virüs, Web Sayfası Değişimi, Dağıtık Servis Engelleme**

28. İnsan yapımı iç kaynaklı tehdit belirleme olayları nelerdir?

**E-Posta Okuma, Kaynaklara Yetkisiz Erişim, Bilgi Hırsızlığı, Bilgi Hırsızlığı, Gizli Bilgilerin ifşası**

29. Varlıkların değerlerinin belirlenmesi kaç a ayrılır?

**Nitel ve nicel**

30. Tekil Kayıp Beklentisi (SLE) = Varlık Değeri x Etki Düzeyi

31. Yıllık Kayıp Beklentisi (ALE) = Tekil Kayıp Beklentisi x Yıllık Gerçekleşme İhtimali

32. Nicel Risk Değerlendirmesi nedir?

**Sürecin tüm elemanlarına sayısal değer verilmelidir.**

**Varlık,**

**Etki Düzeyi,**

**Korunma Verimliliği,**

**Korunma Maliyeti vb**

33. Nitel Risk Değerlendirmesi nedir?

**Değerlendirme çıktısı sayısal olmayacaktır.**

34. Riske Karşı Davranış Belirleme kaçaya ayrılır?

- **Riskin azaltılması**
- **Riskin aktarılması**
- **Riskin kabul edilmesi**
- **Riskin rededilmesi**

35. Potansiyel hasar veya durumların sigorta ettirilmesi nedir?

**Riskin aktarılması**

36. Riskin gerçekleşmesi durumunda oluşacak potansiyel kaybın kabul edilmesine ne nedir?

**Riskin kabul edilmesi**

37. Riskin inandırıcı bulunmaması ve göz ardı edilmesine nedir?

**Riskin reddilmesi**

38. Bir önlemin uygulanmasına ve kullanılmasına nedir?

**Riskin azaltılması**

39. Politika türleri nelerdir?

**Duyuru politikaları**

**Bilgilendirici politikalar**

**Yasal politikalar**

40. Duyuru politikası nedir?

**Çalışanların, davranışlarının sonuçlarını bildiğinden emin olunmasıdır.**

41. Çalışanların bilgilendirilmesini ve eğitilmesini, görevlerinin ve beklentilerin bilincinde olmalarını hedefleyen politika hangidir?

**Bilgilendirme politikası**

42. Güvenlik kontrollerinin amacı nedir?

**Kurumun geliştirdiği güvenlik mekanizmalarının uygulanmasını sağlamak.**

43. Güvenlik kontrol türleri nelerdir?

**– Yönetimsel \*İşe Alım Süreci \*Çalışan Kontrolleri \*İşten Çıkarma Süreci**

**– Teknik – Fiziksel**

44. Organizasyonun sahip olduğu güvenlik altyapısı ve güvenlik yönetim sürecinin periyodik olarak takip edilmesine nedir?

**Denetim**

45. Güvenlik Yönetim Sürecinin işleyişi nasıldır?

- Güvenlik politikası oluşturma
- Güvenlik politikası uygulama
- Güvenlik politikası denetimi
- Güvenlik politikasının analizi ve iyileştirilmesi

46. Bilgi Güvenliği Sertifikasyonları nelerdir?

- CISA,
- CISSP,
- ISO 27001 LA,
- CEH

47. 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

48. Saldırı Motifleri nelerdir?

- Merak
- Maddi kazanç arzusu
- Ün kazanma isteği
- Kin-öç
- Terörist amaçlı faaliyet
- İtibarsızlaştırmak
- Sadece eğlence için
- Politik sebepler
- Meydan okuma
- Vatanperverlik



49. Siber saldırı senaryosu nasıl gerçekleşir?

- Sıradan bir hırsızdan daha planlı bir çalışma
- Sızılması düşünülen sistemi incele
- Ön hazırlık
- Harekete geç ve saldır
- Açıklıkları tespit ve...
- Ağ izle ve gizlen
- Sistemi sahiplen
- İz bırakma

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

- Whois Veritabanı sorgulama
- DNS ve IP Veritabanı Sorgulama
- Domain Registration
- Nslookup

51. WHOIS sorgulaması nelerdir?

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

52. 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.

53. IP ve IP sorgulamada kullanılan İnternet temsilci veritabanları nelerdir?

- ARIN ([www.arin.net](http://www.arin.net))
- AFRINIC
- APNIC
- LACNIC
- RIPE

54. Nslookup nedir?

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

55. 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.**

56. Google ile bilgi toplamaya ne denir?

**Google Hacking**

57. 7. Port olan Echo portunu kullanarak atılan ve ağ geçitlerine erişimin test edildiği komuta

**PING** denir. (ICMP)

58. Nmap (Network Mapper) port tarama da kullanılabilecek bir araçtır.

**DOĞRU**

59. Parmak izi tespitine (Fingerprinting) denir.

60. Cookie nedir?

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

61. Şifrelere saldırı yöntemleri nelerdir?

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

62. Sosyal mühendislik nedir?

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

63. Hybrid saldırı yöntemi nasıl oluşur?

**Önce sözlük içindeki kelimeleri daha sonra da brute force mantığı ile çalışır.**

64. Brute force saldırısı nedir?

**olabilecek bütün kombinasyonların şifre üzerinde denenmesidir.**

65. Sözlük saldırısı nasıl yapılır?

**Bir sözlük ya da belirlenen kelimelerin şifre için denenmesidir.**

66. Uzak sisteme şifre deneyebilen araçlar nelerdir?

- **ENUM**
- **NAT**
- **HYDRA**
- **TSGRINDER**

67. Şifre kırma araçları nelerdir?

- **LC5**
- **JOHN THE RIPPEN(En çok kullanılan)**
- **CAIN&ABLE**

68. Exploit nedir?

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

69. DOS ve DDOS arasındaki fark nelerdir?

**DoS sistemleri çalışmaz hale getirmek için yapılan saldırı.**

- **DDoS, DoS saldırısının yüzlerce, binlerce farklı sistemden yapılması.**

70. Phishing-oltalama saldırı nereye uygulanır?

**Korsanlar tarafından telefonuma veya email adreslerimize banklar tarafından gönderiliyormuş gibi mesajların gelmesi ile gerçekleştiriyorlar.**

71. SPOOFING saldırı türü nedir?

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

72. Sistemi Sahiplenmede kullanılabilecek yapılar?

**Backdoor – Trojan – Rootkit – Netcat**

73. Backdoor saldırı türü nedir?

**Sisteme başarıyla sızan bir saldırgan sonradan tekrar erişmek isteyebilecektir.**

74. Rootkit saldırı türü nasıl gerçekleşir?

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

75. Netcat ne işe yarar ?

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

76. DÜNYADAKİ BİLİŞİM SUÇLARI EN ÇOK HANGİ ÜLKELERDE İŞLENİYOR ?

**Amerika, Türkiye, Rusya, Çin ve Brezilya**

77. 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 hem de saldırı amaçlı çalışan hacker. Amacı sadece kazanmaktır.

78. 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.**

79. Sosyal mühendislik örnekleri?

- **Bir web sitesinin tasarım olarak benzerini yapıp, domain olarak çok benzer bir domain alıp, bilgilerimize erişmek**
- **Reklam'lara tıkla para kazan vs. sahte siteler.**

80. AĞ GÖRSELLEŞTİRME SİSTEMİ çeşitleri nelerdir?

**Honeymap**  
**Norse- map**  
**Digital atak map**  
**Kaspersky Cyberthreat Real-Time Map**  
**Wordfence**  
**Sucuri**  
**Trend micro**  
**Threat Cloud**  
**Akamai**  
**Malwaretech Live Map**  
**ESG MalwareTracker**  
**Fortinet Threat Map**

81. İşlenmiş veri olarak ve bir konu hakkında var olan belirsizliği azaltan kaynağa nedir?

**Bilgi**

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

**Öz bilgi**

83. Öz bilginin nasıl kullanılacağını kavramaya nedir?

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

84. Steganografi kaçaya ayrılır?

- **Metin steganografisi –Resim steganografisi**
- **Yazı steganografisi**

85. 'Bilgi gizleme bilgisayar ortamındaki ----- işlemine benzer bir durumdur' boş bırakılan yere ne gelir?

**Encapsulation (Kapsülleme)**

86. Encapsulation'ın asıl amacı nedir?

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

87. Bilgi gizleme kaçaya ayrılır?

- Gizli kanallar –Steganografi –Gerçek kimliği saklama**
- Telif hakkı işaretlemesi**

88. Steganografi kaçaya ayrılır?

- Dilbilim steganografisi –Teknik steganografisi**

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

**Gizli kanallar**

90. Gizli kanalların amacı nedir?

- İletişimimizdeki veriyi saklamaya çalışmak**
- İletişiminin amacını saklamak**

91. Gizli Kanallar hangi alanlarda kullanılmaktadır?

- Dosya tabanlı steganografi (Görüntü, ses ve text dosyaları**
- Ağ paket steganografisi (Veriler IP paketleri içine gizlenmektedir.)**
- Protokol Kapsüllemesi \*SSL (Secure Sockets Layer) \*SSH (Secure Shell)**

92. Veri gönderimi sırasında gerçek kimliği saklayarak bilginin bilinmeyen yada anlaşılamayan biri üzerinden gidiyor olduğu izlenimi verilerek gönderilen yapıya nedir?

**Gerçek Kimliği Saklama (Anonymity)**

93. Bir nesnenin içerisine bir verinin gizlenmesine nedir?

**Steganografi**

94. İçerisine bilgi gizlenen ortama nedir?

### **Cover-data (örtü verisi)**

95. Bilgi gizlemede oluşan ortama nedir?

**Stego-text veya Stego-object**

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

**Stego-key**

97. Taşıyıcı verinin text olduğu steganografiye nedir?

**Dilbilim steganografisi**

98. Dilbilim steganografisinde kullanılan yöntemler nelerdir?

**-Açık kodlar -Şemagramlar**

99. Teknik Steganografinin kapsadığı alanlar nelerdir?

**- Görünmez mürekkep -Gizli yerler -Microdot  
- Bilgisayar tabanlı yöntemler**

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

**Görünmez mürekkep**

101. Kimsenin göremeyeceği gizli yerlere saklama tekniğine nedir?

**Gizli yerler**

102. Bilgiyi noktalar halinde sayfaya gizlemeye nedir?

**Microdotlar**

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

**Bilgisayar tabanlı yöntemler**

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

**-Açık alan yöntemleri -Yazımsal yöntemler  
-Anlamsal yöntemler**

105. Açık alan yöntemlerinin uygulama alanları nelerdir?

- Satır kaydırma
- Satır sonu boşluk bırakma
- Cümle içi boşluk bırakma
- Sağ hizalama

- Gelecek kodlaması

106. Görüntü steganorafisi yöntemleri nelerdir?

- 1.En önemsiz bite ekleme
2. Maskeleme ve filtreleme
3. Algoritmalar ve dönüşümler

107. 0-255 arası 1 byte ile temsil edilen görüntünün hangi seviyededir?

**Gri-seviye**

108. Renkli dijital görüntüler kaç bittir?

**24 bit ve 8 bit**

109. 24 bitlik bir görüntü için pixel başına kaç byte düşer?

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

110. 8 bitlik görüntüler pixel başına kaç byte düşer

**1 byte**

111. 8 bitlik görüntülerde kullanılan renkler nelerdir?

**-beyaz –kırmızı -mavi ve –yeşil**

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

**Maskeleme ve filtreleme**

113. ‘Teknik olarak filigran bir steganografik biçim değildir’

**Doğru**

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

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

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

**Ses steganografisinde**

116. Gizli verilerin şifrelerini kırmak için sözlük saldırısı yapabilen araca nedir?  
**Stegbreak**
117. ----- resim içerisindeki veriyi tespit etmek için kullanılan araca nedir?  
**Stegdetect**
118. Watermarking'in amacı nedir?  
**ses veya görüntü dosyasının bazı özel modifikasyonlarla saklanması değildir. Amacı; Steganografi gibi sadece gizleme değil.**
119. Amaçlarına göre Steganaliz yöntemleri nelerdir?  
**-Aktif steganaliz – Pasif steganaliz**
120. Gizli verinin sadece varlığını tespit eden yöntem nedir?  
**Pasif steganaliz**
121. Gizli mesajın bir kısmını veya benzerini elde etmeyi sağlayan yöntem nedir?  
**Aktif steganaliz**
122. 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)**
123. 'Savunmadan çok "saldırı"ya yönelik araçlara----- denir' boş bırakılan yere ne gelir?  
**Güvenlik araçları**
124. Ağ araştırması ve güvenlik denetlemesi yapan açık kaynaklı ücretsiz yazılıma nedir?  
**Nmap**
125. Güçlü, güncel ve ücretsiz bir uzaktan güvenlik tarama aracına nedir?  
**Nessus (farkı: kurallara bağlı değildir.)**
126. protokol analizi yapan araçlara ne denir?  
**Ethereal**



127. Canlı bir ağ üzerindeki verileri incelemek veya disk üzerine kaydetme işlemi hangi güvenlik aracıyla yapılır?  
**Ethereal (metin tabanlı)**
128. Gerçek zamanlı trafik analizi ve paket kayıtlaması yapabilen ücretsiz bir ağ saldırı belirleme sistemine nedir?  
**Snort**
129. Protokol analizi, içerik araştırması ve eşlemesi yapabilen güvenlik aracına nedir?  
**Snort**
130. Ağ inceleme ve veri yakalama amaçlı klasik bir sniffer ve Metin tabanlı güvenlik aracı ?  
**Tcpdump**
131. Verilen deyimleri eşleyerek belirli bir ağ arayüzündeki paket başlıklarını gösteren güvenlik aracına nedir?  
**Tcpdump**
132. (2. katman)ağ bilgilerine ulaşmayı kolaylaştıran güvenlik aracına nedir?  
**Dsniff**
133. Sistemdeki güvenlik hasar risk analizini otomatik olarak yapan araç hangisidir?  
**GFI LANguard**
134. Anahtarlamalı yerel ağlar için kullanılan bir sniffer, araya girme ve kayıt yapan güvenlik aracı hangisidir?  
**Ettercap (Ağ geometrisini çıkarma ve işletim sistemi tespitleri yapar.)**
135. Çok hızlı bir şifre kırma işlemi hangi güvenlik aracıyla yaparız?  
**John the Ripper**
136. Uygulama düzeyinde ağa bağlı araçlar üzerinde hasar risk analizi yapabilen ve Ağdaki güvenlik açıklarını yakalamada en iyi güvenlik aracı hangisidir?  
**ISS Internet Scanner**



**Vize 2020-11-23 Soruları Pazartesi: Saat 10: 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, Dikeyksen 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: **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 deęiřip deęiřmedięi bilgi gvenlięi ilkelerinden.....ile ilgilidir.

Cevap: **Btnlk**

**Soru 25)** Gncel bir ktcl yazılım tr olan ve fidye yazılımı olarak bilinen yazılıma.....denir.

Cevap: **Ransomware**

**Soru 26)** Dijital delillerin kanıt olarak deęer kazanabilmesi iin incelenmesi gereken son ařama.....'dır.

Cevap: **Raporlama**

**Soru 27)** Bir siber saldırı senaryosu aısından bakıldığında sosyal mhendislik ařamasına tekabl eden veya o ařamadaki eylemlerin genelini ifade eden sazan avlama olarak da bilinen yntemlerin genel adı.....'dır. (literatrdeki orjinal ifadeyi veriniz)

Cevap: **phishing**

**Soru 28)** Uzak bir hedefdeki sunucunun aktif olup olmadıęını.....protokol ile ęreniriz.

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

**Soru 29)** DNS'in aılımı.....

Cevap: **Domain Name System**

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

Cevap: **Internet Protocol**

**Soru 31)** Geliřtirilecek bir yazılımda zel bir port kullanılacaksa.....bařvuru yapılır.

Cevap: **Viyana** → Telafuzu tam doęru deęil

**Soru 32)** Bir řifre iin olası tm ihtimallerin denenmesi řeklindeki saldırıya.....denir. (cevabınızı ya ingilizce ya da trke olarak yazın. her iki dilde birlikte yazmayın!)

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

**Soru 33)** Yakın tarihin en byk siber saldırılarından biridir. İran nkleer santrallerini hedef alsa da birok lke etkilenmiřtir. 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 hedefindeki 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. İnkâr 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)** Aşağıdakileri açıklayınız?

**Mean time to repair:** Onarıma kadar geçen ortalama süre

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

**Mean time to respond:** Müdahale için ortalama süre

**Mean time to replace:** Değişim için ortalama süre

Tanımları bilgi güvenliğinin hangi unsurunu tetikler?

- A) Gizlilik
- B) Kalite
- C) **Kullanılabilirlik**
- D) Bütünlük
- E) Yetkilendirme

**Soru 9)** Bilgi güvenliğinde 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 alma
- 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) Yetkilendirme
- E) Kimlik doğrulama

**Soru 12)** Bilgi sistemlerin yetkisiz erişen saldırırganlar 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) Kumar 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) XLS Password Recovery
- D) Sniffing
- E) Spoofing

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

- A) SQL Injection**
- 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 getirmek**

**Soru 18)** Hnagisi bilgi güvenliđi temel unsularından biri deđildir?

- A) Eriřilebilirlik
- B) Gizlilik
- C) Güvenilirlik
- D) Bütünlük
- E) İnkâr Edilemezlik**

**Soru 19)** Hangisi güvenlik açığı anlamına gelmektedir?

- A) Vulnerability**
- B)
- C)
- D) Wisdom
- E) Availability

**Soru 20)** İçerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlölük ve sorumlulukları hangi tek maddesinin kapsamındadır?

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

**Soru 21)** Hangisi güvenlik yönetim pratiklerinden biri deđildir?

- A) Kurulum**
- B) Politika
- C) Eğitim
- D) Risk Deđerlendirmesi
- 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) Kötü yetiklendirme ve izleme sisteminin olmayışı
- E) İş devamlılıđının aksaması**

**Soru 23)** Hangisi güvenlik öz deđerlendirme 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 saldırıları önleyecek trafik imazları bulunan bilgi güvenliği 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) Web vekil sunucu
- C) Url fitresi**
- D) Ağ erişim kontrolü
- E) Ağ izleme sistemi

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

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

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

- A) Zero-day Atakları
- B) Virüsler
- 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**

1) Aşağıdakilerden hangisi Adli bilişimin çalışma alanlarından değildir? (2.hafta)

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

2) Steganografi yazılımının amacı nedir? (4.hafta)

- 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.)**

3) ....., siber ortamda verimsiz vakit geçirmek anlamına gelir. Yanda 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

4) Aşağıdakilerden hangisi biyometrik bilgi güvenliği sistemi değildir? (8.hafta)

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

5) "En zayıf halka olan kişisel kullanıcıların siber tehdit araçları ve korunma yolları 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

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

- a) Dos      b) Spam      c) Cyberfraud(Sibersahtecilik)      d) Phishing      **e) DDos**

7) Aşağıdakilerden hangisi dijital delil türlerinde değildir? (2.hafta)

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

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

9) "Anomaly" nedir?

- a) Bir ağda meydana gelen olağandışı hareketlerdir.      b) Bir ağ cihazıdır  
c) Bir ağ yazılımıdır.      d) Bir protokoldür

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

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

11) Aşağıdakilerden hangisi kriptolama algoritmaları ve kriptolama türlerinden olan Veri Özet' Algoritmalarından değildir?

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

12) Aşağıdakilerden hangisi simetrik kriptolama yöntemidir?

- a) AES      b) Diffie-Hellman      c) ECC      d) RSA

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 II. DDos III. Sniffing      b) I. Rainbow II. Phishing III Sniffing  
c) I.Sniffing II.DoS Brute Force      d) I.Brute Force II.Sniffing III Phishing  
e) I. Phishing II. DDos III. Brute Force

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

- a) Beyaz şapkali      b) Lamer      c) Siyah şapkali      d) Gri şapkali

15) Aşağıdakilerden hangisi bir siber saldırı aşama değildir?

- a) Halt(Durma)      b) Reconnaissance(Keşif)  
c) Propagation(Yayılma)      d) Command and Control(Kontrol ele geçirme)

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

17) Aşağıdakilerden hangisi siber saldırı niteliği taşımaz?

- a) E-posta kutunuza reklam ve virüs içerikli postaların düşmesi  
b) Web tarayıcısının anasayfanın kendiliğinden değişmesi  
c) Flash diskinizdeki bir klasöre tıkladığınızda kendini sürekli çoğaltması  
d) Güncelleme gerektirmeyen bir program için sürekli olarak gncelle penceresinin açılması  
e) **internet bancacılığı oturumunu açtığınızda şifre değişiminin talep edilmesi**

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

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

19) Stenografide gizli bilgiyi taşıyan orijinal dosyaya ne denir?

- a) Saklayıcı ortam                      b) Taşıyıcı ortam                      c) Gizleyici ortam                      d) **Stenografik taşıyıcı**

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

- a) Oltalama amaçlı e-posta gönderme                      b) İşietim sistemi açıklıklarını kullanma  
c) **Sistem hakkında bilgi toplama**                      d) Sosyal mühendislik                      e) BackDoor kullanma

21) Aşağıdakilerden hangisi aktif saldırı yöntemi değildir?

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

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** YANLIŞ

23) Phishing nedir?

- a) İkna yöntemiyle gizli bilgilerin elde edilmesini amaçlayan bir sosyal mühendislik yöntemidir.
- b) Kimlik hırsızlığıdır.
- c) Yasal bir e-posta gibi görünen ve kişisel bilgilerinizi talep eden e-posta mesajları= genel adıdır.
- d) Yukarıdakilerden hepsi doğrudur.**
- e) Yukarıdakilerden hiçbirisi doğru değildir.

24) Aşağıdakilerden hangisi tehlikeli yazdımlara örnek değildir?

- a) Yama olarak internetten indirilmiş herhangi bir program
- b) Crack programlar
- c) Korsan müzikler ve film dosyaları
- d) Korsan yazılımlar
- e) Yazılım güncellemeler**

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

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

26) Aşağıdakilerden hangisi AES şifreleme için kullanılan algoritma değildir?

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

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**

28) Aşağıdakilerden hangisi HASH algoritması değildir?

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

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

- a) TİB (Telekomünikasyon İletişim Başkanlığı)
- b) BTK (Bilişim Teknoloji Kurumu)**
- c) Siber Güvenlik Kurulu
- d) Cumhuriyet Kurulu
- e) TBMM

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

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

- a) **Collapse All**                      b) Coloring Rules                      c) Expand All                      d) Show Packet in New

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**

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

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

34) Kötücül yaolımlara verilen genel ad nedir?

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

35) Wireshark programında toplanan paketleri metin dosyası dışı aktarmaya yarayan seçenek hangisidir?

- a) As "CSV" File                      b) As "PostScript" File                      c) As "PDML" file                      d) **As "Plain Text" File**

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

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



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

I. Adres http ile değil https ile başlar.

II. Tarapoda kilit ikonu vardır.

III. Güvenilir bir sertifikası vardır.

IV. Sertifikası geçerlidir.

**a) I.II.III.IV**

b) I.II.III

t) III.IV

d) I.II

39) Aşağıdakilerden hangisi sayısal imza olarak kabul edilir?

a) ECC ( Elliptic Curve Cryptosystem )

b) Twofish

**c) DSA ( Digital Signature Algorithm )**

d) Diffie-Helman

40) İnternette 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 veritabanında hangi şifreleme algoritması kullanılıyordur?

a) CRC32

b) SMTP

c) IPS

**d) MD5**

e) Adler32

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

a) eth.dst

b) eth.type

**c) eth.src**

d) eth.len

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**

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

**a) Saklama**

b) Raporlama

c) İnceleme

d) Çözümleme

44) Bilginin bir varlık olarak hasarlardan korunması, istenmeyen kişiler tarafından elde edilmesini önlemeye bilgi güvenliği denir.

- a) **True**                      b) False

45) Aşağıdakilerden hangisi bilgi güvenliğinin temel ögesi değildir?

- a) Gizlilik                      b) Erişilebilirlik                      c) **Çeşitlilik**                      d) Bütünlük

46) Aşağıdakilerden hangisi bilgi güvenliği kavramının temel ilkelerinden değildir?

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

47) 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

48) Wireshark programı aşağıdakilerden hangisi için kullanılmaz?

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

...

---

## Final (2020-2021)

- 1) Dijital bir belge inkar edilemezlik özelliği **Dijital imza/elektronik imza** ile kazanır.
- 2) 800x600 boyutunda bir RGB resme kaç KB veri gizlenebilir?  
 $800*600*1= 480000$  (emin değilim)
- 3) Açık ve gizli olmak üzere iki anahtarın varlığına dayalı şifreleme yöntemi RSA algoritması denir.
- 4) Hedef sistem ile doğrudan iletişime geçilerek bilgi elde etme çalışmaları **aktif bilgi toplama**
- 5) Alfabenin harfleri, noktalama işaretleri, kelimeleri yerine semboller ve kısaltmalar kullanan çabuk yazma; not tutma sistemi olarak ta bilinen gizlenmiş bilgiye **Stenografi** denir
- 6) risk işleme sonrasında kalan riske **artık risk** adı verilir
- 7) sistemde bulunan herhangi bir açıklıktan faydalanılarak sisteme zarar verilmesi işlemine **Sömürme – İstismar (Exploit)** denir.
- 8) Kurumun ihtiyaçlarıyla doğrudan ilişkili olan, genel terimlerin yer aldığı, yapı ve teknolojiye göre esnek olarak hazırlanan kurumun güvenlik hedeflerini belirleyen yazılı dokümanlara **Yazımsal yöntemler** denir (emin değilim)
- 9) Bir sistem üzerinde iz bırakmadan yapılan bilgi keşfi çalışmalarına **pasif bilgi** denir.
- 10) Hangisi pasif bilgi toplama yöntemleri arasında yer almaz?
  - a) Kariyer siteleri
  - b) Github
  - c) **Masscan**
  - d) Sosyal paylaşım ağları
  - e) Arama motorları
- 11) Aktif bilgi toplama araçları arasında yer almaz?
  - a) Wireshark
  - b) Robtex
  - c) Dig
  - d) Nmap
  - e) **Arın**

- 12) Tarama türlerinde hangisinde kaynak makine hedef makineyi tarama esnasında aktif rol almaz?
- a) RPC Scan
  - b) FTP Bounce scan
  - c) Idle scan
  - d) IP protocol scan
  - ACK scan (emin değilim)
- 13) Bir paketin istediği adrese gidene kadar hangi hostlar ve yönlendirmelerden geçtiğini gösterir?
- a) TheHarvester
  - b) DIG
  - c) Nmap
  - d) Dirbuster
  - e) Traceroute
- 14) Whois için hangisi doğru?
- a) IP adresi sorgulamak için kullanılabilir
  - b) Pentrasyon testlerinin ikinci adımında gerçekleştirilir.
  - c) TCP tabanlı bir sorgu protokolüdür
  - d) TCP 43. Portta çalışır
  - e) Alan adı bilgisi yer alır
- 15) Hangisi klasik şifreleme algoritmalarından biridir?
- a) Blok şifreleme
  - b) Yer değiştirme
  - c) Asimetrik şifreleme
  - d) Simetrik ş
  - e) Dizi ş
- 16) HANGİSİ risk değerlendirilmesi sonucu elde edilmez?
- a) Kabul edilebilir risk seviyesi belirlenir
  - b) Azaltılacak risk kelimelerinin özellikleri belirlenir
  - c) Güvenlik ihlalinin oluşma olasılığının belirlenmesi
  - d) Riskler kritiklik sırasına göre sıralanır
  - e) Tüm çalışanlar listelenir

- 17) Hangisi insani ve kasıtlı tehdit türleri arasında yer almaz?
- a) Hırsızlık
  - b) **Hatalı yönlendirme**
  - c) Dinleme
  - d) Kötücül yazılım
  - e) Bilgi değiştirme
- 18) Bir risk belirleme tablosunda kurumsal iş sürecinin bazı varlıkları yer alır. Hangisi bu varlıklar arasında yer almaz?
- A) Alınan hizmet
  - B) İnsan
  - C) Bilgi
  - D) Çevresel**
  - E) Yazılım
- 19) Hangisi varlık listeleri için doğru değildir?
- a) Varlıkların sahipleri ve değerleri belirlenerek varlık envanteri oluşturulur.
  - b) Varlık listesine, varlıkların fiziksel yeri, formatı, yedeği olup olmadığı gibi olası bir felaketten kurtarma durumunda gerekli olacak bilgiler girilir.
  - c) Önce varlıklar ve isimleri tespit edilmelidir
  - d) Yazılım varlıkları en somut varlıklar olduğu için buradan başlanması kolaylık sağlayacaktır**
- 20) Hangisi pasif bilgi toplama yöntemleri arasında yer almaz?
- a) **Nmap**
  - b) ARIN
  - c) Theharvester
  - d) Whois
  - e) Link extraction
- 21) Hangisi iyi bir güvenlik politikasında yer almaz?
- a) Politikada açıklanan her bir konu doğru bir şekilde tanımlanmalıdır
  - b) Kuruluştaki yer alan belirli kişiler tarafından erişilebilir olmalıdır**
  - c) Kullanıcıdan beklenen gizliliğin seviyesini tanımlamalıdır
  - d) Güvenlik hedefleri açıkça tanımlanmalıdır
  - e) Kuruluş üyelerinin görev ve sorumlulukları, açıklanan sonuçlarda belirtilmelidir

- 22) Hangisi güvenlik politikası kavramları arasında yer almaz?
- a) Yönerge
  - b) Temel
  - c) Tehditler
  - d) Prosedür
  - e) Standart
- 23) Güvenlik politikası oluşturulurken hangi sorulara cevap aramaz?
- a) Güvenlik politikasının gerçekleştirilmesinde kim, ne yetki ve sorumluluğa sahiptir?
  - b) Ne tip gözden kaçmalar ve dikkatsizlikler olabilir?
  - c) Hangi aktiviteler tehdit olarak görülür ve güvenlik riski yaratırlar
  - d) Ne tür varlıktan korumak gereklidir?
  - e) Kime, nereye, ne zaman ve hangi yetkiyle izin verilebilir?
- 24) Güvenlik politikası için hangisi yanlıştır?
- a) Tekniktir
  - b) Zamanla güncellenmelidir
  - c) Güvenlik işlerimi tüm kurum faaliyetlerine entegre etmek amaçlanır
  - d) Kolay anlaşılabilir olmalıdır
  - e) Öneri tavsiye değil emir kipi kullanılır
- 25) Hangisi potansiyel saldırı kaynakları arasında yer almaz?
- A) Dahili sistemler
  - B) İnternet bağlantısı üzerinden
  - C) Çevresel faktörler
  - D) Modem havuzu üzerinden
  - E) Çevre ofis erişim noktaları
- 26) İyi bir bilgi güvenliği analizi için hangi tür sorunlara cevap aranır?
- a) Ne tür varlıkları korumak gereklidir
  - b) Bu varlıkları nelere karşı korumalıyız
  - c) Bir tehdit'in varlıklarımızı bozma olasılığı nedir
  - d) Bir tehlikeli saldırı olması durumunda ivedi maliyet ne olacaktır?
  - e) Hepsi
- 27) Aşağıdakilerden hangisi iyi bir bilgi güvenliği programı içerisinde yer almaz?
- a) Risk yönetimi mevcuttur
  - b) Politika, prosedür ve standartlar içerir
  - c) Bilgiyi sınıflandırma
  - d) Güvenlik örgütlemesi içerir
  - e) Değerlendirme aşamasına yer verilmez