

## 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