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 c. Önce varlıklar ve isimleri tespit edilmelidir

b. VarlIdarm sahipleri ve değeri belirlenerek varlık envanteri oluşturulur.

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.

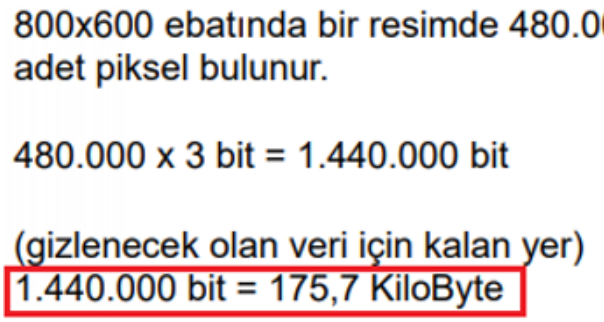
Yanıt: Asimetrik Şifreleme (Asymetric Encryption)

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