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)

1. Açık ve gizli olmak üzere iki anahtarın varlığına dayalı şifreleme yöntemi RSA algoritması denir.
2. Hedef sistem ile doğrudan iletişime geçilerek bilgi elde etme çalışmaları aktif bilgi toplama
3. Alfabenin harfleri, noktalama işaretleri, kelimeleri yerine semboller ve kısaltmalar kullanan çabuk yazma; not tutma sistemi olarak ta bilinen gizlenmiş bilgiye **Stenografi denir**
4. **risk işleme sonrasında kalan riske** artık risk adı verilir
5. sistemde bulunan herhangi bir açıklıktan faydalanılarak sisteme zarar verilmesi işlemine **Sömürme – İstismar** (**Exploit) denir.**
6. **Kurumun ihtiyaçlarıyla doğrudan ilişkili olan, genel terimlerin yer aldığı, yapı ve teknolojideki değişimlere göre esnek olarak hazırlanan kurumun güvenlik hedeflerini belirleyen yazılı dokümanlara Yazımsal yöntemler denir (emin değilim)**
7. **Bir sistem üzerinde iz bırakmadan yapılan bilgi keşfi çalışmalarına pasif bilgi denir.**
8. Hangisi pasif bilgi toplama yöntemleri arasında yer almaz?
9. Kariyer siteleri
10. Github
11. Masscan
12. Sosyal paylaşım ağları
13. Arama motorları
14. Aktif bilgi toplama araçları arasında yer almaz?
15. Wireshark
16. Robtex
17. Dig
18. Nmap
19. Arın
20. Tarama türlerinde hangisinde kaynak makine hedef makineyı tarama esnasında aktif rol almaz?
21. RPC Scan
22. FTP Bounce scan
23. Idle scan
24. IP protocol scan

* ACK scan (emin değilim)

1. Bir paketin istediği adrese gidene kadar hangi hostlar ve yönlendirmelerden geçtiğini gösterir?
2. TheHarvester
3. DIG
4. Nmap
5. Dirbuster
6. Traceroute
7. Whois için hangisi doğru?
8. IP adresi sorgulamak için kullanılabilir
9. Pentrasyon testlerinin ikinci adımında gerçekleştirilir.
10. TCP tabanlı bir sorgu protokolüdür
11. TCP 43. Portta çalışır
12. Alan adı bilgisi yer alır
13. Hangisi klasik şifreleme algoritmalarından biridir?
14. Blok şifreleme
15. Yer değiştirme
16. Asimetrik şifreleme
17. Simetrik ş
18. Dizi ş
19. HANGİSİ risk değerlendirilmesi sonucu elde edilmez?
20. Kabul edilebilir risk seviyesi belirlenir
21. Azaltılacak risk kelimelerinin özellikleri belirlenir
22. Güvenlik ihlalinin oluşma olasılığının belirlenmesi
23. Riskler kritiklik sırasına göre sıralanır
24. Tüm çalışanlar listelenir
25. Hangisi insani ve kasıtlı tehdit türleri arasında yer almaz?
26. Hırsızlık
27. Hatalı yönlendirme
28. Dinleme
29. Kötücül yazılım
30. Bilgi değiştirme
31. Bir risk belirleme tablosunda kurumsal iş sürecinin bazı varlıkları yer alır. Hangisi bu varlıklar arasında yer almaz?
32. Alınan hizmet
33. İnsan
34. Bilgi
35. Çevresel
36. Yazılım
37. Hangisi varlık listeleri için doğru değildir?
38. Varlıkların sahipleri ve değerleri belirlenerek varlık envanteri oluşturulur.
39. Varlık listesine, varlıkların fiziksel yeri,formatı, yedeği olup olmadığı gibi olası bir felaketten kurtarma durumunda gerekli olacak bilgiler girilir.
40. Önce varlıklar ve isimleri tespit edilmelidir
41. Yazılım varlıkları en somut varlıklar olduğu için buradan başlanması kolaylık sağlayacaktır
42. Hangisi pasif bilgi toplama yöntemleri arasında yer almaz
43. Nmap
44. ARIN
45. Theharvester
46. Whois
47. Link extraction
48. Hangisi iyi bir güvenlik politikasında yer almaz?
49. Politikada açıklanan her bir konu doğru bir şekilde tanımlanmalıdır
50. Kuruluşta yer alan belirli kişiler tarafında erişilebilir olmalıdır
51. Kullanıcıdan beklenen gizliliğin seviyesini tanımlamalıdır
52. Güvenlik hedefleri açıkça tanımlanmalıdır
53. Kuruluş üyelerinin görev ve sorumlulukları, açıklanan sonuçlarda belirtilmelidir
54. Hangisi güvenlik politikası kavramları arasında yer almaz?
55. Yönerge
56. Temel
57. Tehditler
58. Prosedür
59. Standart
60. Güvenlik politikası oluşturulurken hangi sorulara cevap aramaz?
61. Güvenlik politikasının gerçekleştirilmesinde kim, ne yetki ve sorumluluğa sahiptir?
62. Ne tip gözden kaçmalar ve dikkatsizlikler olabilir?
63. Hangi aktiviteler tehdit olarak görülür ve güvenlik riski yaratırlar
64. Ne tür varlıkdan korumak gereklidir?
65. Kime, nereye, ne zaman ve hangi yetkiyle izin verilebilir?
66. Güvenlik politikası için hangisi yanlıştır?
67. Tekniktir
68. Zamanla güncellenmelidir
69. Güvenlik işlerimi tüm kurum faaliyetlerine entegre etmek amaçlanır
70. Kolay anlaşılabilir olmalıdır
71. Öneri tavsiye değil emir kipi kullanılır
72. Hangisi potansiyel saldırı kaynakları arasında yer almaz?
73. Dahili sistemler
74. İnternet bağlantısı üzerinden
75. Çevresel faktörler
76. Modem havuzu üzerinden
77. Çevre ofis erişim noktaları
78. İyi bir bilgi güvenliği analizi için hangi tür sorunlara cevap aranır?
79. Ne tür varlıkları korumak gereklidir
80. Bu varlıkları nelere karşı korumalıyız
81. Bir tehdit’in varlıklarımızı bozma olasılığı nedir
82. Bir tehlikeli saldırı olması durumunda ivedi maliyet ne olacaktır?
83. Hepsi
84. Aşağıdakilerden hangisi iyi bir bilgi güvenliği programı içerisinde yer almaz?
85. Risk yönetimi mevcuttur
86. Politika, prosedür ve standartlar içerir
87. Bilgiyi sınıflandırma
88. Güvenlik örgütlemesi içerir
89. Değerlendirme aşamasına yer verilmez