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 kanunuyla ("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 İfşası

29. Varlıkların değerlerinin belirlenmesi kaça 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 İhtima**li

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 kaça 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 senoryosu nasıl gerçekleşir?
    - **Sıradan bir hırsızdan daha planlı bir çalışma**
    - **Sızılması düşünülen sistemi incele**
    - **Ön hazırlık**
    - **Harekete geç ve saldır**
    - **Açıklıkları tespit ve…**
    - **Ağı 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)**
    - **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 kullarak atılan ve ağ geçitlerine erişimin test edildiği komuta **PİNG** 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 RİPPER(En çok kulllanılan)**
- **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 trafından telefonuma veya emil 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 hemd e saldırı amaçlı çalışan hacker. Amacı sadece kazanmaktı.

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 mğhendislik örnekleri?
- **Bir web sitesinin tasarım olarak benzerini yapıp, domain olarakta 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 Cybertreat 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?
Özbilgi

83. Öz bilginin nasıl kullanılacağını kavramaya nedir?

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

84. Steganografi kaça 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 ulaşıma zorlamaktır.

87. Bilgi gizleme kaça ayrılır?
    -Gizli kanallar –Stegonagrafi –Gerçek kimliği saklama
    -Telif hakkı işaretlemesi

88. Stegonagrafi kaça ayrılır?
    -Dilbilim steganografisi –Teknik stegonagrafisi

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 kullanılmaktdır?
    -Dosya tabanlı steganografi (Görüntü, ses ve text dosyaları
    -Ağ paket steganografisi (Veriler IP paketleri içine gizlenmektedir.)
    -Protokol Kapsüllenmesi *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 Steganografinın 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 yöntemlerinın 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 yönteme nedir?
Pasif steganaliz

121. Gizli mesajın bir kısmını veya benzerini elde etmeyi sağlayan yönteme 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 hangisir?
Ettercap (Ağ geometrisini çıkarma ve işletim sistemi tespitleri yapar.)

135. Çok hızlı bir şifre kırma işlemini hangi güvenlik aracıyla yaparız?
J**ohn 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