24-) Asimetrik şifreleme algoritmalarının atası olan ilk algoritma aşağıdakilerden hangisidir?
a) RSA b) 3-DES c) DH (Diffie-Helman) d) AES e) ElGamal

25-) Aşağıdakilerden hangisi Asimetrik şifreleme algoritmalarından biridir?
a) RC4 b) DES c) 3-DES d) RSA e) AES

26-) $13^{422} \equiv$? (mod31)
a) 10 b) 22 c) 14 d) 32 e) Hiçbiri

27-) Virüs ile ilgili verilen özelliklerden hangisi yanlıştır?
a) Kendi kendine çalışmaz b) Dosyaları bozar c) Kendi kendine çalışır
d) Bir dosya üzerinden hareket ederler e) Genellikle veri dosyalarını değiştirir

28-) $\frac{1}{5}$ (mod6)=? İşlemin sonucu aşağıdakilerden hangisidir?
a) 6 b) $\frac{1}{5}$ c) 5 d) 1 e) Hiçbiri

29-) Z_{60}'da Affine Cipher yöntemi için anahtar uzayı boyutu nedir?
a) 60 b)16 c) 3600 d) 960 e) Hiçbiri

30-) Aşağıdaki özelliklerden hangisi paket üreteçlerinin kullanım amaçlarından biri değildir?
a) TCP/IP yığınını test etmek
b) Güvenlik duvarı kural tablosunu test etmek
c) Parçalı paketler göndermek
d) Pakete ait bayrakları (flag) değiştirerek sistemin işletim sistemini değiştirmek
e) Sistemi devre dışı bırakmak ya da ele geçirmek

31-) Aşağıdakilerden hangi şifre kırma araçlarının kullanım alanlarından biri değildir?
a) Sistemin güvenlik seviyesini zayıflatmak
b) Ağı dinleyerek şifreleri yakalama
c) Sözlük (dictionary) veya kaba kuvvet (bruteforce) saldırısıyla şifre kırma
d) Saklanmış şifreleri kırma
e) Çevrimdışı şifre kırma

32-) RSA algoritmasında n=p.q formülündeki p ve q değerleri için hangisi doğrudur?
a) Her ikisi de asal olmak zorundadır
b) Birinin asal olması yeterlidir
c) Aralarında asal olmalıdırlar
d) İkisi de asal değildirlere
e) Hiçbiri

33-) ABD Başkanı Obama tarafından ilk kez 2014'te kullanılan "Siber Savaş" kavramı hangi ülkenin ABD'ye karşı saldırısından dolayı kullanılmıştır?
a) Rusya b) Çin c) İran d) Kuzey Kore e) Estonya

34-) TEMPEST Nedir?
a) Güvenlik duvarı b) Sosyal Mühendislik c) Şifreleme Yöntemi
d) Elektromanyetik Darbe Sızıntı Standardı e) Bilgisayar çeşidi

35-) Aşağıdakilerden hangisi Faraday Kafesi'nin özelliklerinden biri değildir?
a) İletken teller ile ağ biçiminde kaplanmış ve topraklanmış her kafesle bu koruma gerçekleştirilebilir.
b) Dışarıdaki elektrik alan içeri etki edemez, mesela yıldırımlar gibi statik elektrik boşalmaları iletkenlerden geçer ve içeri sıçramaz.
c) Ağ gözü sıklığı arttıkça koruma azalır.
d) Günlük hayatta kullanıldığı alanlardan biri, yanıcı parlayıcı maddelerin depolandığı binalardır.
e) Topraklama kalitesi korumayı arttırır.

Not:** Her soru (1,8) puan değerindedir. Notlandırmada yanlış cevaplar dikkate alınmayacak doğru cevaplar üzerinden değerlendirme yapılacaktır. Cevaplar kesinlikle cevap anahtarına işaretlenecektir. **Cevap Anahtarına işaretlenmeyen cevaplar dikkate alınmayacaktır!!!

15.-)Bir backdoor trojanı ile kurban makinesini ele geçirmek nasıl sağlanabilir?
a) Keyloggerdan alınan IP adresi kurban makineye bağlantı için yeterlidir.
b) Screenloggerdan alınan IP adresi kurban makineye bağlantı için yeterlidir.
c) Sadece trojanla bağlantı sağlanamaz kurban makineye bağlantı için yeterlidir.
d) İlk bağlantı için DOS tan ipconfig /flushdns komutu ile DNS ayarı yapılması gerekir.
e) Erişimi bulunan kurban makinesine phishing yöntemiyle aldatma uygulanıp bir dosyaya trojan bind edilerek bağlantı sağlanabilir.

16.-) ARP tablosunun görevi nedir?
a) Anahtarlama yapar.
b) Network içerisindeki IP adreslerini ve IP adreslerine karşılık gelen MAC adreslerini tutar.
c) İletimde kullanılan anahtarların herkes tarafından bilinmesini sağlar.
d) Yerel ağa bağlı olan geniş alan ağlarının listesini tutar.
e) İki farklı yerel ağ arasında zehirleme işlemi yapılabilmesine olanak sağlar.

17.-) ARP Poisoning işlemi ARP Cache'teki MAC adresinin değiştirilmesiyle gerçekleştirilir. Bu manipülasyon yapılmadan önce saldırıyı gerçekleyecek kişi ne yapmalıdır?
a) Ağı dinleyerek IP ve MAC adreslerini belirler.
b) Ağ üzerine saldırılar yapmalıdır.
c) Ağ üzerinden gelen mesajları kaydetmelidir.
d) Ağlar arasındaki iletişimi engellemelidir.
e) Hiçbiri

18.-) Aşağıdakilerden hangisi Penetration Testing'in asıl amacıdır?
a) Sistemin zafiyetlerinin tespit edilmesidir.
b) Sistemin zafiyetlerinin ve performansının test edilmesidir.
c) Sistemin kullanışlılığının ve verilebilecek zararın boyutunun ölçülmesidir.
d) Sistemlerin DoS atak larına karşı dayanıklılığının tespit edilmesidir.
e) Sosyal Mühendisliğin uygulanmasına ortam sağlamaktır.

19.-)Aşağıdakilerden hangisi penetration tools değildir?
a) Ağ dinleme araçları
b) Açıklık tarayıcılar
c) Web güvenliği test araçları
d) Topoloji çıkarım araçları
e) Kablolu ağ araçları

20.-) Aşağıdakilerden hangisi modern kriptografinin ilgilendiği konulardan biri değildir?
a) Mesajın istenmeyen kişiler tarafından anlaşılmaması
b) Mesajın iletilmesi sırasında değiştirilmemesi
c) Mesajı gönderenin daha sonra mesajı kendisinin gönderdiğini yalanlayamaması
d) Mesajın kimin tarafından gönderildiğinin anlaşılabilmesi
e) Mesajın kimin tarafına ne kadar sürede gönderileceğinin belirlenmesi

21.-) Bir şifreleme algoritmasının performansını hangi kriterlere göre belirleyebiliriz??
a) Kırılabilme süresinin uzunluğu
b) Şifreleme ve çözme işleminde ihtiyaç duyulan bellek miktarı
c) Bu algoritmaya dayalı şifreleme uygulamalarının esnekliği
d) Algoritmanın kurulacak sisteme uygunluğu
e) Hepsi

22.-) Aşağıdakilerden hangisi asimetrik şifreleme özelliklerinden biri değildir?
a) Kriptografinin ana ilkeleri olarak sayılan; bütünlük, kimlik doğrulama ve gizlilik hizmeti güvenli bir şekilde sağlanabilir
b) Anahtarı kullanıcı belirleyebilir
c) Anahtar uzunlukları bazen sorun çıkarabilir
d) Şifrelerin uzunluğundan kaynaklanan algoritmaların yavaş çalışması gerçekleşebilir
e) Asimetrik şifreleme algoritmalarında anahtar ile şifre çözme anahtarı aynıdır

23.-) Aşağıdaki bilgilerden hangisi blok şifreleme algoritmaları için yanlıştır?
) Orijinal metni veya şifreli metni bloklara bölerek şifreleme/deşifreleme işlemini yapar
DES,AES blok şifreleme algoritmalarından bazılarıdır
k şifreleme karıştırma ve yayılma tekniklerine dayanır
ngüde farklı anahtar kullanılır
k şifreleme algoritmalarıdır

16.) Bir backdoor trojanı ile kurban makinesini ele geçirmek nasıl sağlanabilir?
a) Keylogger'dan alınan IP adresi kurban makinesiyle bağlantı için yeterlidir.
b) Screenlogger'dan alınan IP adresi kurban makinesiyle bağlantı için yeterlidir.
c) Sadece trojanla bağlantı sağlanamaz kurban makinesiyle verilir bulaştırılması gerekir.
d) İlk bağlantı için DOS tarı işletmeliz. Phishing komutu ile DNS ayarı yapılması gerekir.
e) Erişimi sadece kurban makinesine phishing yöntemiyle aldatma uygulanıp bir dosyaya trojan bind edilerek bağlantı sağlanabilir.

16.) ARP zehirlenmesinin görevi nedir?
a) Anahtarlama yapar.
b) Network içerisindeki IP adreslerini ve IP adreslerine karşılık gelen MAC adreslerini tutar.
c) İletimde kullanılan anahtarların herkes tarafından bilinmesini sağlar.
d) Yerel ağa bağlı olan gerçek ve sahte bütün MAC adreslerini tutar.
e) İki farklı yerel ağ arasında zehirleme işlemi yapılabilmesine olanak sağlar.

17.) ARP Poisoning işlemi ARP Cache'teki MAC adresinin değiştirilmesiyle gerçekleştirilir. Bu manipülasyon yapılmadan önce saldırıyı gerçekleştirecek kişi ne yapmalıdır?
a) Ağ dinleyerek IP ve MAC adreslerini belirler.
b) Ağ üzerine saldırılar yapmalıdır.
c) Ağ üzerinden gelen mesajları kaydetmelidir.
d) Ağlar arasındaki iletişimi engellemelidir.
e) Hiçbiri

18.) Aşağıdakilerden hangisi Penetration Testing'in asıl amacıdır?
a) Sistemin zafiyetlerinin tespiti edilmesidir.
b) Sistemin kullanışlılığının ve performansının test edilmesidir.
c) Sistemin Dos saldırılarına karşı dayanıklılığının tespit edilmesidir.
d) Sistemlerin Dos saldırılarına karşı dayanıklılığının tespit edilmesidir.
e) Sosyal Mühendisliğin uygulanmasına ortam sağlamaktır.

19.) Aşağıdakilerden hangisi penetration tools değildir?
a) Ağ dinleme araçları
b) Açıklık tarayıcılar
c) Web güvenliği test araçları
d) Topoloji çıkarım araçları
e) Kablolu ağ araçları

20.) Aşağıdakilerden hangisi modern kriptografinin ilgilendiği konulardan biri değildir?
a) Mesajın istenmeyen kişiler tarafından anlaşılmaması
b) Mesajın iletilmesi sırasında değiştirilmemesi
c) Mesajı gönderenin daha sonra mesajı kendisinin gönderdiğini yalanlayamaması
d) Mesajın kimin tarafından gönderildiğinin anlaşılabilmesi
e) Mesajın karşı tarafa ne kadar sürede gönderileceğinin belirlenmesi

21.) Bir şifreleme algoritmasının performansını hangi kriterlere göre belirleyebiliriz?
a) Kırılabilme süresinin uzunluğu
b) Şifreleme ve çözme işleminde ihtiyaç duyulan bellek miktarı
c) Bu algoritmaya dayalı şifreleme uygulamalarının esnekliği
d) Algoritmanın kurulacak sisteme uygunluğu
e) Hepsi

22.) Aşağıdakilerden hangisi asimetrik şifreleme özelliklerinden biri değildir?
a) Kriptografinin ana ilkeleri olarak sayılan: bütünlük, kimlik doğrulama ve gizlilik hizmeti güvenli bir şekilde sağlanabilir
b) Anahtarı kullanıcı belirleyebilir
c) Anahtar uzunlukları bazen sorun çıkarabilir
d) Şifrelerin uzunluğundan kaynaklanan algoritmaların yavaş çalışması gerçekleşebilir
e) Asimetrik şifreleme algoritmalarında anahtar ile şifre çözme anahtarı aynıdır

23.) Aşağıdaki bilgilerden hangisi blok şifreleme algoritmaları için yanlıştır?
a) Orjinal metni veya şifreli metni bloklara bölerek şifreleme/deşifreleme işlemini yapar
b) DES-AES blok şifreleme algoritmalarından bazılarıdır
c) Blok şifreleme algoritmalarında karıştırma ve yayılma tekniklerine dayanır
d) Her döngüde farklı anahtar kullanılır
e) Asimetrik şifreleme algoritmalarıdır

28.03.2017

BİLGİSAYAR AĞLARINDA GÜVENLİK ARA SINAVI TEST SORULARI

1-) Bilgisayar Ağlarında Güvenlik için neler sağlanmalıdır?
a) Bütünlük b) Erişebilirlik c) Gizlilik d) Doğrulama e)Hepsi

2-) Güvenlik zincirinde ki en zayıf halka aşağıdakilerden hangisidir?
a) Güvenlik Duvarı b) Sistem c) Ağ Bileşenleri d) İnsan e)Hiçbiri

3-) İlk Siber Savaş hangi ülkeye yapılmıştır?
a) ABD b) İran c) Estonya d) Çin e)Rusya

4-) Stuxnet Solucanı ilk hangi ülke tarafından zarar verme amaçlı kullanılmıştır?
a) ABD b) İran c) Estonya d) Çin e)Rusya

5-) Aşağıdakilerden hangisi siber tehdit amaçlarından değildir?
a) Sisteme yetkisiz erişim b) Bilgi güvenliğini sağlama c) Hizmetlerin engellenmesi
d) Bilgilerin ifşa edilmesi e) Bilgilerin çalınması

6-) Aktif atak ile ilgili verilenlerden hangisi yanlıştır?
a) Sisteme doğrudan zarar vermeyi, durdurmayı ya da bozmayı amaçlar
b) Veri içeriği değiştirilmediği için aktif saldırıları ortaya çıkartmak çok güçtür
c) Sistemi durdurur ya da bozarlar
d) Atak yapan kişi (saldırgan) sistemi ya da servisi engellemeyi ya da kötüye kullanmayı amaçlar
e) Servis durdurma amaçlanmaktadır

7-) Aşağıdakilerden hangisi Kod Ataklarında kullanılan zararlı yazılımlardan birisi değildir?
a) Virüsler b) Worm c) Pretexter d) Logic Bomb e) Adware

8-) Aşağıdakilerden hangisi keşif ataklarına örnek olarak gösterilebilir?
a) Spoffing b) ARP Zehirlemesi c) Sniffing d) DDoS Atak e) Hiçbiri

9-) Virüs ve Solucanlar arasındaki temel fark nedir?
a) Verilen Zarar b) Ortam c) Çoğalma ve Yayılma d) Hedef e)Hiçbiri

10-) Aşağıdakilerden hangisi genel olarak sunucudan hizmet bekleyen kullanıcılara hizmetini engellemek için yapılan saldırı türüdür?
a) Truva Atları b) Solucanlar c) DoS Saldırısı d) Hoaxlar e) Boot virüsleri

11-) DoS ve DDoS atakları aşağıdaki güvenlik ilkelerinden hangisini etkilemektedir?
a) Gizlilik (confidentiality)
b) Bütünlük (integrity)
c) Kimlik doğrulama (authentication)
d) Red olmayan (non-repudiation)
e) Erişilebilirlik (availability)

12-) İnternet ortamında kişileri; yasal bir şirket, ajans veya organizasyon olduğuna inandırarak, kişisel ve finansal bilgilerini elde etme yöntemine ne ad verilir?
a) Phishing b) Brute-Force c) Spam d) KeyNote e)Hepsi

13-) Önceden hazırlanmış bir olası parolaları içeren dosya yardımıyla parolayı bulmaya çalışan atak türü hangisidir?
a) Brute Force Atak b) Birthday Atak c) Dictionary-Based Atak d) Spoofing e) Port Stealing

14-) Hedef sistemde yer alan cihazların konumlarını tespit etmek ve topolojisini elde etmek için ..... kullanılır. Bu alanda en önemli araçlardan biri sıklıkla kullanılan .....komutudur.
Yukarıdaki boşlukları tamamlayan kelimeler aşağıdakilerden hangisinde doğru olarak verilmiştir?
a) Topoloji çıkarım araçları /ping
b) Topoloji çıkarım araçları / Wireshark
c) Port tarayıcılar/ping
d) Kablosuz ağ araçları/ ping
e) Açıklık tarayıcılar / Ettercap