

Aşağıdakilerden hangisi IaaS avantajları içinde yer almaz?

- A. Çıkış için düşük engeller
- B. Azaltılmış ROI riski
- C. Streamlined ve otomatik ölçeklendirme
- D. Altyapı malzemelerinin paylaşılır olması
- E. Kullanım başına ödeme
- F.

Cevap : A

Hangisi bulut konuşlandırma yöntemlerinden değildir?

- A. Herkese açık bulut
- B. Özel bulut
- C. İletişim bulutu
- D. Topluluk bulutu
- E. Hibrit bulut

Cevap : C

Aşağıdakilerden hangisi kablosuz ağların taşıdığı riskler arasında değildir?

- A. Kablolu ağlara sızma
- B. Ağ topolojisinin ortaya çıkması
- C. İstenmeyen yerlere servis vermeme
- D. Trafik dinleyip verinin çözülmesi
- E. Servis dışı bırakma

Cevap : C

- 1-İstemci doğrulama sunucusundan, onun kimliğini ister. Doğrulama sunucusu, kimlik bilgisini istemciye gönderir.
- 2-Doğrulayıcı bağlantı isteğini alınca, tüm portları kapalı tutar, sadece istemci ile arasında bir port açar.
- 3-İstemci doğrulayıcıya bağlantı talebinde bulunur.
- 4-Doğrulayıcı, kullanıcıdan kimliğini ister. İstemci kimliğini gönderir, doğrulayıcı kimlik bilgisini doğrulama sunucusuna gönderir. Kimlik gönderildikten sonra kimlik kanıtlama süreci başlar. Sunucu kimliği doğrular ve doğrulayıcıya gönderir. Doğrulayıcı, istemcinin portunu yetkilendirilmiş duruma getirir.
- 5-İstemci, doğrulama sunucusunun kimliğini doğruladığında, veri trafiğine başlanır.

Yukarıda verilen 802.1x ile kimlik doğrulama adımlarının doğru sıralanışı hangisidir?

- A. 3-2-4-1-5
- B. 5-3-1-4-2
- C. 3-2-5-1-4
- D. 4-2-5-3-1
- E. 1-5-2-4-3

Cevap : A

NFC teknolojisi ile Bluetooth arasındaki farklardan hangisi yanlıştır?

- A. NFC, Bluetooth'a göre daha yüksek hızda çalışıyor.
- B. NFC' de Bluetooth aksine cihazlar arasında eşleşme yapılması gerekmiyor.
- C. NFC, Bluetooth'a göre daha az güç kullanıyor.
- D. Bluetooth'un aksine NFC cihazları arasında çok kısa sürede bağlantı kurulabiliyor.
- E. Bluetooth ile kıyaslandığında NFC kalabalık ortamda daha kullanışlıdır.

Cevap: A

Aşağıdakilerden hangisinde NFC cihazlarının çalışma modları doğru şekilde verilmiştir?

- A. Ad-Hoc mod - Infrastructure mod
- B. Ad-Hoc mod - Peer to Peer mod - Reader/Writer mod
- C. Peer to Peer mod - Access Point Router Mod - Card Emulation
- D. Station Bridge mod - Access Point Bridge mod - Ad-Hoc mod
- E. Reader/Writer mod - Peer to Peer mod - Card Emulation

Cevap: E

Hashing yöntemlerinden olan MD5 ve SHA'nın karşılaştırılmasıyla ilgili verilen seçeneklerden hangisi yanlıştır?

- A. MD-5'te 512-bitlik bloklar üzerinde işlem yapılırken, SHA'da 256-bitlik bloklar üzerinde işlem yapılır.
- B. SHA'daki ekleme işlemi, MD-5'te olan ekleme işlemiyle aynı şekilde yapılır.
- C. MD-5 algoritması 128-bit çıktı üretirken, SHA algoritması 168-bit çıktı üretmektedir.
- D. SHA girdi olarak 2^{64-1} uzunluğunda veri kabul etmektedir. MD-5 için sınırlama yoktur.
- E. MD-5'te her adımda döngü 16 kez tekrarlanır. SHA'da ise 20 kez tekrarlanır.

Cevap: A

Aşağıdakilerden hangisi Anahtarlı Hash Fonksiyonları(MAC) özelliklerinden biri değildir?

- A. Mesaj bütünlüğünü garantiler ve kanıtlar.
- B. Biri mesaj diğeri gizli anahtar olmak üzere fonksiyonel olarak iki parametresi bulunur.
- C. MAC algoritmaları dijital imzalara göre daha güvenlidir.
- D. Bankalarda mesaj doğrulama amacıyla yoğun olarak kullanılan algoritmalardan biridir.
- E. MAC algoritmasının kullanılabilmesi için gönderen ve alıcı olan tarafların gizli K anahtarını paylaşması gerekmektedir.

Cevap: C

Aşağıdakilerden hangisi SET (Secure Electronic Transactions-Güvenli Elektronik İşlemler)

protokolünün sağladığı temel servislerden biri değildir?

- A. Kimlik Tanılama
- B. Mesaj Bütünlüğü
- C. Anahtar Değişimi
- D. Gizlilik
- E. Linkleme

Cevap: C

Aşağıdakilerden hangisi ağ üzerinden başka bilgisayarlara erişim sağlamak, uzak bir bilgisayarda komutlar çalıştırmak ve bir bilgisayardan diğerine dosya transferi amaçlı geliştirilmiş bir protokoldür ?

- A. TLS (Transport Layer Security / İletim Katmanı Güvenliği)
- B. SET (Secure Electronic Transactions / Güvenli Elektronik İşlemler)
- C. PCT (Private Communication Technology / Kişisel İletişim Teknolojisi)
- D. SSH (Secure Shell / Güvenlik Kabuk)
- E. SSL (Secure Socket Layer / Güvenli Yuva Katmanı)

Cevap: D

Aşağıdakilerden hangisi steganografi yöntemleri arasında yer almaz ?

- A. Mobil Steganografi (Mobile Steganography)
- B. Görüntü Steganografi (Image Steganography)
- C. Ses Steganografi (Audio Steganography)
- D. Video Steganografi (Video Steganography)
- E. Metin Steganografi (Text Steganography)

Cevap: A

Aşağıdaki steganografi yöntemlerinden hangisi en fazla bilgi tutma kapasitesine sahiptir ?

- A. Görüntü Steganografi (24 bit renkli resim)
- B. Görüntü Steganografi (8 bit renkli resim)
- C. Görüntü Steganografi (24 bit siyah beyaz resim)
- D. Görüntü Steganografi (8 bit siyah beyaz resim)
- E. Ses Steganografi (Audio Steganography)

Cevap: A

- I. Mobility ve maliyet VPN 'in dezavantajlarındanıdır.
- II. Farklı loksasyonlardaki ağların tek bir özel ağmış gibi birbirine bağlanması Remote Access VPN 'e örnektir.
- III. Güvenlik açısından VPN türleri 3 tanedir: Trusted, Secure,Hybrid VPN.
- IV. Authentication,Encryption,Paket Filtreleme,Yetkilendirme VPN güvenliğini sağlar.
- V. Güvenli bir VPN oluşturmak için en çok kullanılan protokol IPV6 dır.

VPN 'e ilişkin yukarıdakilerden hangileri doğrudur?

- A. Yalnız I
- B. I,II
- C. I,III,IV
- D. Hepsi
- E. III,IV

Cevap: d

PPP(Point to Point Protocol) 'nin asıl çalışan kısmı, bağlantı kurulması,yapılandırılması,test edilmesi, parametrelerin ayarlanması ve bağlantının kapanmasından sorumlu olan; paket boyutunu düzeleyen,yapılandırma hatalarını tespit eden protokol hangisidir?

- A. LCP (Bağlantı Kontrol Protokolü)
- B. NCP
- C. IPCP
- D. HDLC
- E. TACACS+

Cevap: A

Aşağıdakilerden hangisi bulut teknolojileri avantajları arasında yer almaz ?

- A. Sistem Güncellemeleri
- B. Grup çalışması
- C. Anında Güncelleme
- D. Artırılmış veri güvenliği
- E. Sınırsız Depolama Kapasitesi

Cevap:A

Aşağıdakilerden hangisi Cloud Defenderın filtreme aşamalarından değildir?

- A. Sensor Filter
- B. Double Signature Filter
- C. Embedded Filter
- D. Puzzle Resolver Filter
- E. Hop Count Filter

Cevap:C

Aşağıdakilerden hangisi Ad-Hoc ağlarda güvenlik ilkelerinden değildir ?

- A. Ulaşılabilme
- B. Asıllama
- C. İnkâr etme
- D. Bütünlük
- E. Güvenilirlik

Cevap: C

Aşağıdakilerden hangisi bulut yığınının taban katmanı olan Infrastructure as a Service(IaaS) ' in avantajlarından değildir ?

- A. Genellikle platform-bağımsız
- B. Donanım ve insan kaynaklarındaparaharcamalarını önlemek
- C. Semantik birlikte çalışabilirlik (interoperability)
- D. Giriş için düşük engeller
- E. Streamlined ve otomatik ölçeklendirme

Cevap: C

Aşağıdakilerden hangisi Güvenlik Duvarı(Firewall) ile ilgili yanlıştır Bir bilgidir?

- A. Firewalllar genel olarak, özellikle networkteki diğer makinelerden farklı bir makinenin üstüne kuruludurlar.
- B. Ev ve küçük ofislerde internet bağlantısını sağlamak amacı ile kullanılır.
- C. Temel olarak bir yönlendirici programı ile beraber çalışan bir firewall, network üzerinde kendisine gelen paketlerin gitmelerine gereken yerlere gidip gidemeyeceğine karar verir.
- D. Kurumsal olarak da genelde bilgisayar ağına erişim kontrolü amacı ile kullanılır.
- E. Hiçbiri

CEVAP : B

Aşağıdakilerden hangisi yanlıştır?

- A. Gizlice Dinleme: MAC çerçeveleri ve veri paketleri parçalanarak başlık elde edilir. Komşu düğümler, yönlendirme bilgisi elde edilir.
- B. Aktif Ataklar: Amaç sadece gizlilik değil, bütünlüğü de bozmaktır. Ağa yetkisiz giriş, kaynakların izinsiz kullanımı, haberleşmenin ele geçirilmesidir.
- C. Pasif Ataklar: Amaç KAA üzerindeki verinin gizliliğini bozmak, herhangi bir emisyon gerçekleşmez.
- D. Trafik Analizi: Önemli bilgiler içeren ağ topolojisi düşman tarafından ele geçirilebilir. Merkeze yakın düğümlerden daha çok ağ trafiği olacağı için bu tip düğümlerin analiz ile tespit edilmesi ve DoS ataklara maruz bırakılması ağın erişilebilirliğini engelleyecektir.
- E. Hepsi

CEVAP : A

SQL Injection’da iki kritik meta karakter aşağıdakilerden hangisidir?

- A. ‘ (Tek tırnak) ve ; (Noktalı Virgül)
- B. ? (Soru işareti)
- C. * yıldız
- D. / (slash)
- E. + (artı)

Cevap:a

SQL Injection kodu daha sonra SQL Server örneğine geçirilen dizelerin içine sokulduğu _____ bir saldırıdır.

- A. Kötü niyetli
- B. Gereksiz
- C. Temiz
- D. Kötü niyetli olmayan
- E. Yararlı

Cevap:A

Aşağıdakilerden hangisi kod atak türü değildir ?

- A. Solucan
- B. Trojan Atı
- C. Sosyal Mühendislik
- D. Lojik Bombalar
- E. Rootkit

Cevap : C

Aşağıdakilerden hangisi bir Pasif atak türü değildir.

- A. Sniffing
- B. Footprinting
- C. DdoS
- D. Fingerprinting
- E. Backdoor

Cevap:c

Aşağıdaki algoritmalarından hangisi hash algoritması değildir?

- A) MD5
- B) SHA1
- C) CBCMAC
- D) RIPEMD
- E) MD6

CEVAP: C

2) Hash algoritması ile ilgili hangisi doğrudur?

- I.Algoritmanın ürettiği sonuçtan tekrar asıl metne dönüş mümkün değildir.
- II.Hash algoritması MD5,SHA olabilir.
- III.Bilgisayar ağlarında,internet trafiğinde,kimlik belirleme uygulamalarında kullanılabilir.
- IV.Keyfi uzunluktaki bir mesajdan 128 bitlik bir mesaj özeti çıkarır.

A)Yalnız I B)Yalnız III C)I,II,III D)Hepsi E)I,II

Cevap:D

Aşağıdakilerden hangisi Rol-Tabanlı Erişim Modelinin özelliklerinden değildir?

- A. Veri soyutlamasının mümkün olmasıyla veri sahipleri ve iş birimi yöneticileri hangi personelde hangi yetkilerin olduğunu rahatça kontrol edilebilir.
- B. RTEK görevler ayrılığı ilkesinin hem sistem içerisinde hem de sistemler arasında uygulanmasını kolaylaştırır.
- C. Roller, kurumsal görevler ile ilişkilendirileceğinden ‘en fazla yetki’ prensibi uygulanabilir.
- D. RTEK personel sirkülasyonu ve işten ayrılma oranı fazla olan kurumlar için avantajlıdır.
- E. Rol hiyerarşileri yaratmanın mümkün olmasıyla kullanıcı hak ve yetkilerinin yönetimi kolaylaşır.

CEVAP :C

Aşağıdakilerden hangisi yetkilendirme çeşitleri arasında yer almaz?

- A. Düzenli Yetkilendirme
- B. Explicit Yetkilendirme
- C. Implicit Yetkilendirme
- D. Dağıtık Yetkilendirme
- E. Merkezi Yetkilendirme

CEVAP : A

Aşağıdaki özelliklerden hangisi güvenlik duvarı için uygun olmaz?

- A. Ağ güvenliği için çok gerekli değildir.
- B. İç ve dış ağlar arası ağ trafiğini tanımlanan kurallara göre denetleyen bir ağ geçidi çözümüdür.
- C. Ev ve küçük ofislerde internet güvenliğini sağlamak amacı ile kullanılır.
- D. Güvenlik duvarı, yerel ağlar üzerindeki kaynakları diğer networkler üzerinden gelecek saldırılara karşı korur.
- E. Kurumsal olarak da genelde bilgisayar ağına erişim kontrolü amacı ile kullanılır.

Cevap: A

Aşağıdakilerden hangisi Firewallların tanımına aykırıdır?

- A. Sadece kurumsal firmalarda bilgisayar ağına erişimi engellemek için kullanılır.
- B. Network üzerinde kendisine gelen paketlerin gitmelerine gereken yerlere gidip gidemeyeceğine karar verir.
- C. Bir yönlendirici programı ile beraber çalışır.
- D. Güvenlik duvarları performans artırıcı ve izin politikası uygulayıcı amaçlar için de kullanılır.
- E. İç ve dış ağlar arası ağ trafiğini tanımlanan kurallara göre denetleyen bir ağ geçidi çözümüdür.

CEVAP: A

Aşağıdakilerden hangisi bulut teknolojisinin dezavantajlarından birisidir?

- A. Düşük Donanım Maliyeti
- B. Olası Güvenlik Açıkları
- C. Düşük Yazılım Maliyeti
- D. İşletim Sistemleri Arasında Geliştirilmiş Uyum
- E. Arttırılmış Dosya Formatı Uyumu

Cevap: B

Aşağıdakilerden hangisi bulut bilişimde tehditlere karşı kullanılan yöntemlerden biri değildir?

- A. Two- Factor kimlik doğrulaması
- B. Tokenization
- C. Dağıtık servise dayalı mimari kullanılması
- D. Server ve client kimlik doğrulaması
- E. Kimlik doğrulamaya dayalı sertifika

Cevap: C

Aşağıdakilerden hangisi siber tehditlerin amaçlarından değildir?

- A. Sisteme yetkisiz erişim sağlanması
- B. Hizmetlerin engellenmesi
- C. Sistemin korunması
- D. Bilgilerin ifşa edilmesi
- E. Bilgilerin değiştirilmesi

Cevap: C

- I. Yemleme (Phishing)
- II. Truva atı (Trojan)
- III. Bilgisayar virüsleri
- IV. DDos
- V. Kurtçuk(Worm)

Yukarıdakilerden hangileri siber tehdit araçlarındandır?

- A. Hepsi
- B. I, II, III
- C. III, IV, V
- D. IV, V
- E. I, II

Cevap: A

Aşağıdakilerden hangisi ağ dinleme araçlarından biridir?

- A. Paros
- B. Wireshark
- C. Hping
- D. Metasploit
- E. Nessus

Cevap: B

Aşağıdakilerden hangisi NMAP programının özelliklerinden değildir?

- A. Bir ağdaki canlı bilgisayarları tespit edebilmektedir.
- B. TCP ve UDP port taraması yapabilmektedir.
- C. Çalışan servisleri tespit edememektedir.
- D. Yazılımların sürümünü tahmin edebilmektedir.
- E. Raporlama yeteneği bulunmaktadır.

Cevap:C

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 artırır.

Cevap: C

I.TEMPEST

II.Faraday Kafesi

III. Gürültülü Ortam

Yukarıdakilerden hangileri kablolu hatlarda veri güvenliğini sağlamanın yolları arasında yer alır?

- A. Hepsi
- B. I ve II
- C. I ve III
- D. II ve III
- E. Yalnız I

Cevap:A

Aşağıdaki seçeneklerin hangisinde veritabanı ve desteklediği programlama dili bilgisi doğru verilmemiştir?

- A. ASP- SQL Server
- B. PHP-PostgreSQL
- C. ASP.NET-SQL Server
- D.PHP-SQL Server
- E. ASP.NET-MS Access

Cevap: E

Aşağıdakilerden hangisi SQL injection exploits türlerinden birisidir?

- A. Command-Execution
- B. Hepsi
- C. Local
- D. Remote
- E. SQL Injection

Cevap: B

Aşağıdaki güvenlik duvarı teknolojilerinden hangisi ISO/OSI modeline göre network katmanında çalışır?

- a)Paket Filtreleri
- b)Authentication Serverları
- c)Encryption Serverları
- d)Uygulama Katmanı Gatewayleri
- e)Hash Fonksiyonları

cevap= A

Gateway olarak yapılandırılmış bir network aygıtının , gateway özelliği taşıması için en az kaç network interface kartına sahip olması gerekmektedir?

- a)0
- b)1
- c)4
- d)3
- e)2

cevap= E

I.Reflected XSS

II.Stored XSS

III.DOM XSS

Yukarıdaki XSS açıklarından hangisinde / hangilerinde web sitesinde aktif olan tüm kullanıcılar etkilenir?

- A. Yalnız I
- B. I, II ve III
- C. I,II
- D. Yalnız III
- E. Yalnız II

CEVAP : E

DOM temelli XSS nasıl önlenir?

- A. Cookie'lerde HttpOnly Flag kullanılarak
- B. Session ID'leri URL'de göstermeyerek
- C. Önlenemez
- D. Her request farklı zamanlarda oluşturularak
- E. Web sitesinden gelen her input değerini kontrol ederek

cevap e

Aşağıdakilerden hangisi atak çeşitlerinden biri değildir?

- A. İçsek atak
- B. Dışsal atak
- C. Rastgele atak
- D. Kod Atak
- E. Phishing Atak

Cevap:C

Aşağıdakilerden hangisi footprinting için kullanılan araçlardan bir tanesidir?

- A. Tracert
- B. Worm
- C. Nessus
- D. Teardrop
- E. Rootkit

Cevap : A

Wireshark hangi penetration tool sınıfına girer?

- A. Paket Üreteçleri
- B. Port Tarayıcılar
- C. İşletim Sistemi Tespit Araçları
- D. Topoloji Çıkarım Araçları
- E. Ağ Dinleme Araçları

Cevap:E

Aşağıdakilerden hangisi açıklık tarayıcı bir toolstur?

- A. WireShark
- B. Nessus
- C. Ubuntu
- D. EtterCap
- E. NMap

Cevap:B

ARP Poisoning(Arp zehirlenmesi) saldırısından korunmak için hangileri kullanılabilir?

- I. Network kartlarına fiziksel ulaşımı engelleyerek sniffer kurulmasını engellemek
- II. Network switchlerinde port güvenliğini sağlayacak özellikleri aktif etmek
- III. Statik IP adresleri kullanmak ve ARP kayıtlarını statik olarak eklemek

- A. Hepsi
- B. Yalnız II
- C. I ve III
- D. Yalnız I
- E. I ve II

cevap : a

Aşağıdakilerden hangisi ARP Poisoning(Arp zehirlenmesi) için söylenemez.

- A. ARP Cache'teki MAC adresinin değiştirilmesiyle gerçekleşir
- B. Ağ dinlerken hiçbir saldırı yapılmaz
- C. İki bilgisayar arasındaki karşılıklı gönderilen bütün paketler önce saldırıya uğrar.
- D. Ağ dinlenerek IP ve MAC adresleri belirlenir
- E. Sisteme doğrudan zarar vermeyi, durdurmayı amaçlar.

cevap : e

Arp poisoning yapmak için hangi sıra takip edilmelidir?

- 1) zehirlenme işlemine başlanır.
- 2) Mapping tablosunu oluşturulur.
- 3) giden gelen paketleri dinlenilir.
- 4) ağ dinlenip kullanacak IP ve MAC adreslerini belirlenir.

- A. 1-3-2-4
- B. 3-1-2-4
- C. 1-2-3-4
- D. 2-3-1-4
- E. 4-3-2-1

CEVAP:E

Network'te sniffer olup olmadığını denetleyecek birden fazla araç vardır. Aşağıdakilerden hangisi veya hangileri buna örnektir.

- 1) Arp Watch
- 2) Promiscan
- 3) Antisniff
- 4) Prodetect

- A. Yalnız 1
- B. 1-2-3
- C. 1-3-4 3-4
- D. 1-3
- E. Hepsi

CEVAP: e

Aşağıdakilerden hangisi ARP zehirlenmesinden korunma yollarından biri değildir?

- A. Statik IP ve statik ARP ön belleği
- B. Layer2 ve Layer3 switch kullanımı
- C. Güvenlik duvarı
- D. Verileri şifrelemek
- E. Farklı VLAN tanımlanması

Doğru cevap : c

ARP poisoning ile ilgili aşağıdakilerden hangisi yanlıştır?

- A. Önbelleğe yönelik mac saldırısında spoofing kullanılır
- B. ARP ağdaki paketlerin geliş gidişini düzenler
- C. Asıl MAC adresleri poisoning esnasında değişmez
- D. ARP poisoning pasif bir saldıdır.
- E. ARP adres çözümleme protokolüdür

Doğru cevap: a

- 1.Tempest
- 2.Faraday
- 3.Gürültülü ortam
- 4.Uekae-Ettm

Yukarıdaki öncüllerden hangileri kablolu hatlarda veri güvenliğini sağlama yollarından değildir?

- A. Yanlız 1
- B. 1 ve 2
- C. Yanlız 4
- D. 1,2,3 ve 4
- E. 2 ve 3

cevap : c

- 1. Tempest
- 2. Spread spectrum
- 3. Echo data hiding

Yukarıdaki öncüllerden hangileri ses stenografi yöntemlerinden değildir?

- A. Yanlız 3
- B. Yanlız 2
- C. Yalnız 1
- D. 2 ve 3
- E. Hiçbiri

cevap : c

Steganografiyi kriptografiden ayıran özellik hangisidir?

- A. Steganografide mesajın varlığının gizlenmesi
- B. Kriptografide mesajın içeriğinin bozulması
- C. Kriptografide mesajın varlığının saklanması
- D. Steganografide mesajın içeriğinin bozulması
- E. Steganografide mesajın içeriğinin gizlenmesi

Doğru Cevap : a

Aşağıdakilerden hangisi doğrudur?

- A. Kriptografi yunanca "gizli yazı" demektir.
- B. Kriptografide mesajın varlığı bilinmez.
- C. Steganografi 1. Dünya Savaşına dayanır.
- D. Kriptografi mesajın içeriğini anlaşılmaz hale getirirken, steganografi mesajı görülmeyecek şekilde saklar
- E. Steganografi güvenilir değildir.

Doğru cevap : d

Aşağıda verilen VPN çeşitlerinin güvenlik açısından (en güvenli den en az güvenliye doğru) sıralanışı hangisinde doğru olarak verilmiştir?

- A. Trusted VPN,Secure VPN,Hybrid VPN
- B. Secure VPN,Trusted VPN,Hybrid VPN
- C. Hybrid VPN,Secure VPN,Trusted VPN
- D. Trusted VPN,Hybrid VPN,Secure VPN
- E. Secure VPN,Hybrid VPN,Trusted VPN

CEVAP : e

VPN güvenliği aşağıdakilerden hangisi ile sağlanmaz ?

- A. Web erişim kısıtlaması
- B. Şifreleme
- C. Paket Filtreleme
- D. Kimlik denetimi
- E. Yetkilendirme

CEVAP - a

Aşağıda verilenlerden hangisinde paket bağılığına bakılarak anormallik tespiti yapılamaz?

- A. FTP Başlığı
- B. IP Başlığı
- C. TCP Başlığı
- D. ICMP Başlığı
- E. Ethernet Başlığı

cevap: a

Aşağıda verilenlerden hangisi imza temelli bir STS türü olan Snort'un özelliklerinden değildir?

- A. IP ağları üzerinde gerçek zamanlı trafik analizi yapar.
- B. Snort programı açık yazılım olarak geliştirilmektedir.
- C. Program çalışırken gerçekleşen kötüye kullanımlara göre alarm verir.
- D. Ağ temelli saldırı tespit sistemi olarak görev yapar.
- E. Kural tabanlıdır ve kullanılan dil ile yeni kurallar tanımlanabilir.

cevap: c

Herhangi bir TCP/IP portuna dışardan gelen bağlantı isteklerini engelleyebilen ancak aynı port üzerinden dışarı çıkışlara izin veren yapı nedir ?

- A. FTP
- B. NPN
- C. Router
- D. Switch
- E. Firewall

Cevap:e

Aşağıdakilerden hangisi internet olanaklarından değildir?

- A. Telnet
- B. FTP
- C. NIC
- D. IRC
- E. WEB

Cevap: C

Aşağıda IPV6 için verilen bilgilerden hangisi yanlıştır?

- A. IPv4' ten IPv6' ya geçiş yapabilmek için uygulama seviyesi saldırıları açısından yeni güncellemelere ihtiyaç duyulmaktadır.
- B. IPV6 nın geniş adres uzayı nedeniyetüm ağı taramak imkansız hale gelmiştir.
- C. sahte cihazların tespiti için bilinen yöntemler IPV6 için değişmemiştir.
- D. IPv6 protokolünün tanımına göre tüm konaklar yönlendirme başlığını işleyebilmelidir.
- E. IPv6 ağlarında orta konaklarda parçalanma yapılmasına izin verilmemektedir.

cevap:a

Aşağıdakilerden hangisi IPv6 ile gelen güvenlik tehditleri arasında yer almaz?

- A. Taşıma saldırıları
- B. ICMPv6
- C. Ek başlıklar ile ilgili tehditler
- D. Tünelleme ve geçiş mekanizmaları
- E. Keşif tipi saldırılar

cevap: a

Aşağıdakilerden hangisi Türkiyede internet sağlayıcılarının ücretsiz olarak sunduğu, güvenli internet hizmetlerinin özelliklerinden biri değildir?

- A. Çocuk profili ve aile profili olmak üzere iki seçenek sunar.
- B. İstedığınız zaman bu hizmeti alabilir, değiştirebilir ve ya iptal edebilirsiniz.
- C. İnternette oluşabilecek her türlü tehlikeye karşı, kullanıcıyı koruma garantisi vermektedir.
- D. İnternete bağlanılan cihaza, herhangi bir yazılım yüklenmeden kullanılır.
- E. İnternet kullanıcılarının günlük gereksinimlerini kısıtlayacak bir işlevi yoktur.

Cevap: C

Aşağıdakilerden hangisi Türkiyede internet üzerinde yapılacak ulusal düzeyde politikalara etki eden, bürokrasiye tavsiye veren kuruluşlardan biri değildir?

- A. Ulaştırma Bakanlığı
- B. Bilgi Teknolojileri ve İletişim Kurumu
- C. Kıyıyari İnternet Araştırmaları Başkanlığı
- D. İnternet Kurulu
- E. Telekomünikasyon İletişim Başkanlığı

Cevap: C

gcd(48, 40) kaçtır ?

- A. 8
- B. 6
- C. 7
- D. 5
- E. 9

cevap:A

2) $3^{27} \pmod{10}$ da kaçtır?

- A. 3
- B. 1
- C. 2
- D. 0
- E. 4

cevap:A

Dos,DDoS (Distributed Denial of Service) saldırıları için aşağıdakilerden hangisi yanlıştır?

- A. DDoS ile saldırıyı yapan gizlenemez, bulunması çok kolaydır.bilgisayarlar üzerine düzenlenmiş bir çeşit hizmet aksatma yöntemidir.
- B. DoS saldırısı altındaki bir sunucu size hiç hizmet veremeyebilir ya da oldukça yavaş hizmet vermektedir.
- C. Distributed Denial of Service” (DDoS) DoS saldırısının dağıtılmış olarak gerçekleştirilmesine denir.
- D. Denial of Service” web siteleri veya
- E. Saldırı yapan kimse bu saldırıyı tek bir IP üzerinden değil birçok IP üzerinden gerçekleştirir.

cevap:A

Aşağıdakilerden hangisi Bulut Teknolojisi(Cloud Computing) dezavantajlarından değildir?

- A. Sabit İnternet Bağlantısı Gerektirmesi
- B. Düşük Hızlarda Düzgün Çalışmaması
- C. İşletim Sistemleri Arasında Geliştirilmiş Uyum
- D. Olası Güvenlik Açıkları
- E. Sistem Güncellemeleri

cevap : C

Gönderilen bilginin içindeki bitlerle matematiksel hesaplar yaparak bu sonucu da bilgiyle göndermek suretiyle bir mesaj içindeki hataları belirleme metoduna ne ad verilir?

- A. Collision Detection
- B. Carrier Sense
- C. Multiple Access
- D. Broad
- E. CRC
- F.

Cevap : E

Aşağıdakilerden hangisi yanlıştır ?

- A. Gizli anahtarların herkes tarafından bilinmesinin sakıncası yoktur.
- B. Şifreleme yönteminde bilgi , alıcı dışında başka bir kişi tarafından okunmaması ya da değiştirilmesi için kodlanır.
- C. Anahtar bir metin ile birlikte bir mesaj veya dijital imzayı şifrelemek üzere kullanılan özel bir sayıdır.
- D. Şifreleme ve şifreyi bir matematiksel algoritma ve anahtar gereklidir.
- E. Şifreleme ve şifreyi çözmek için bir matematiksel algoritma ve anahtar gereklidir.

Cevap : A

Aşağıdakilerden hangisi kablosuz algılayıcı ağların (KAA) zayıflıklarından biri değildir?

- A. Bilinen güvenlik yöntemleri işe yaramaz.
- B. Her işlem batarya ömrünün bitmesine sebep olur.
- C. Bilinen ağ yapısındaki şifreleme yöntemleri KAA'larda kullanılmaz.
- D. Mesafenin yanlış hesaplanması durumları oluşabilmektedir.
- E. Yanlış ortam bilgisini mesaj bütünlüğüne ekler.

Cevap: C

Aşağıdakilerden hangisi kablosuz algılayıcı ağlarda (KAA) kullanılan trafik analiz tekniklerinden değildir?

- A. Fiziksel katman trafik analizi
- B. MAC ve üst katmanlarda trafik analizi
- C. Paket bağlantılı trafik analizi
- D. Olay bağlantılı trafik analizi
- E. Aktif trafik analizi

Cevap: C

Amacı tanımlama ve loglama olan ,kötü niyetli ağ hareket ve bağlantılarının tespiti için kullanılan sistem aşağıdakilerden hangisidir?

- A. Ids
- B. Idps
- C. Firewall
- D. Ipds
- E. Ips

Cevap:A

Aşağıdakilerden hangisi saldırı tespit sistemlerinin kullanılmasının nedenlerinden biri değildir?.

- A. Saldırganların cezalandırılması ve keşfedilme riskinin artmasıyla problemleri davranışları engellemek.
- B. Saldırıları ve diğer güvenlik ölçütleri tarafından önlenemeyen diğer güvenlik ihlallerini bulmak.
- C. İzinsiz olarak erişimler hakkında bilgi sağlamamak.
- D. Var olan tehdidi belgelendirmek.
- E. Saldırı başlangıçlarını bulmak ve çözmek.

Cevap:C

Aşağıdakilerden hangisi donanım güvenlik duvarıdır?

- A. BitDefender
- B. McAfee
- C. Norton
- D. Fortigate
- E. Comodo

Cevap:D

Aşağıdakilerden hangisi yazılım güvenlik duvarı değildir?

- A. BitDefender
- B. Kaspersky
- C. Fortigate
- D. Comodo
- E. Norton

Cevap:C

Aşağıdakilerden hangisi siber saldırılara karşı geliştirilmiş bir güvenlik modeli değildir?

- A. Sybil Saldırılarına Karşı Geliştirilen Model
- B. SinkHole Saldırılarına Karşı Geliştirilen Model
- C. Cain Saldırılarına Karşı Geliştirilen Model
- D. WormHole Saldırılarına Karşı Geliştirilen Model
- E. Jamming Saldırılarına Karşı Geliştirilen Model

CEVAP :C

Aşağıdakilerden hangi kısıtı KAA' da güvenlik modelleri belirlerken dikkate almayız?

- A. Maliyetin fazla olması ve performansı düşürmesi.
- B. Kaynak tüketimini düşürmesi ve güvenlik performansını arttırması.
- C. Algılayıcı ağa yüklenecek model ile birçok saldırıyı etkilemesi
- D. Fazladan düğüm eklenmesini ve hata hoşgörüsünü desteklemesi.
- E. Ölçeklendirmeyi ve mobil algılayıcıya sahip KAA' larda da kullanılabilmesi.

CEVAP :A

Aşağıdakilerden hangisi NFC teknolojilerinin Uygulama Alanlarından değildir?

- A. Erişim yetkilendirme
- B. Kişisel ID
- C. Şifre Kırma
- D. Ödemeler(Mobil ödeme olanağı sağlayan sistemler)
- E. Dosya paylaşımında ve akıllı etiketlerde kullanılabilme

CEVAP : C

Aşağıdakilerden hangisi veya hangileri NFC cihazlarının çalışma modlarından ?

- I.Peer-to-Peer mode
- II.Reader/Writer mode
- III.Card emulation
- IV.Listen mode

- A. I,II ve III
- B. II ve III
- C. Yalnız I
- D. I ve III
- E. II ve IV

CEVAP : A

IpSec Network katmanı üzerinde aşağıdakilerden hangisini desteklemez?

- A. Replay Attack Protection
- B. Integrity
- C. Confidentiality
- D. Associations
- E. Authentication

cevap:D

Aşağıdakilerden hangisi Steganography'nin kullanım alanlarından biridir ?

- A. Değiştirmeye Dayalı Steganography
- B. Görüntü Steganography
- C. İşaret İşlemeye Dayalı Steganography
- D. İstatistiksel Steganography
- E. Yazımsal Steganography

cevap:B

Aşağıdakilerden hangisi güvenli internetin özelliklerinden değildir?

- A. Kolaydır ve bilgisayarınıza program kurmanıza gerek yoktur.
- B. Çocuk profili ve aile profili olmak üzere iki seçenek sunar.
- C. Aile profilinde zararlı içeriklere ulaşmak mümkündür.
- D. İstedığınız zaman bu hizmeti alabilirsiniz istediğinizde hizmet kapsamından çıkabilirsiniz.
- E. İnternet sağlayıcı tarafından ücretsiz olarak sağlanan ve zararlı içeriklere ulaşımı engelleyen sistemdir.

Cevap : C

Aşağıdakilerden hangisi Bilgi Teknolojileri ve İletişim Kurumu'nun Elektronik Haberleşme Yönetmeliği ile belirlenen tehditlerden biri değildir?

- A. Yetkisiz olarak ya da yetki aşımı ile güvenlik hassasiyetli alana girilmesi
- B. Deprem, sel, su baskını gibi doğal afetler
- C. Basit şifre politikaları
- D. Haberleşmenin yasal olmayan şekilde izlenmesi
- E. Doğru olmayan bir bilgi üretilerek bu bilginin başkalarına ulaştırılması

Cevap : C

Bilgi güvenliindeki en büyük açıklık nedir?

- A. Firewall
- B. Antivirüs programları
- C. Program eksiklikleri
- D. Portların açık bırakılması
- E. İnsan bilgisizliğı

Cevap: E

Her yıl duyurulan bilgi güvenliğı açıklıklarına göre ortalama en büyük bilgi güvenliğı açığı nedir?

- A. Sniffing
- B. Brute-Force attack
- C. ARP Poisoning
- D. Denial Of Service
- E. SQL injection

Cevap: E

Aşağıdakilerden hangisi bulut servis modellerinden birisidir?

- A. MaaS
- B. SaaS
- C. KaaS
- D. LaaS
- E. DaaS

Cevap : B

Aşağıdakilerden hangisi IaaS (Infrastructure as a Service)' ın avantajlarından değildir?

- A. Genellikle platform bağımsızdır
- B. Azaltılmış ROI riski
- C. Zayıf istemci (thin client)" uygulamaları tarafından sağlanan kullanıcı arayüzü
- D. Streamlined ve Otomatik Ölçeklendirme
- E. Kullanım başına ödeme

Cevap: C

Bir kablosuz sensör ağı mimarisinde izlemenin yapıldığı ortamda toplanan veri genelde 3 seviyede işlenir. Bunlar;

Her düğüm algılanıp, işledikleri veriyi komşularına yollamaktadır
İşlenmiş verinin baz (base) olarak adlandırılan merkeze yollanır
İzlenilecek ortamdaki olaylar, sensör düğümler tarafından algılanır

Yukarıdaki işlemlerin sıralaması aşağıdakilerden hangisinde doğru olarak verilmiştir?

- A. I-II-III
- B. III-II-I
- C. II-I-III
- D. I-III-II
- E. III-I-II

Cevap : E

Aşağıdakilerden hangisi bilindik saldırılara karşı kablosuz sensör ağlarında alınabilecek tedbirlerden değildir?

- A. Anahtar Tespit ve Yöntemleri
- B. Gizlilik ve Kimlik Doğrulama
- C. Sybil saldırısını ciddiye almamak
- D. Frekans Bozma(Jamming) ve Paket Enjeksiyonu
- E. Broadcast/Multicast Kimlik Doğrulama

Cevap : C

Aşağıdakilerden hangisi internet kurulu görev ilkelerinden değildir?

- A. Teknolojik gelişmeleri izleme
- B. Verimliliğin sağlanması
- C. Yararlı projeleri destekleme
- D. Güvenli internet ortamı oluşturma
- E. Ulusal içerik zenginliği sağlama

Cevap : C

Aşağıdaki bakanlıklardan hangisinin elektronik haberleşme güvenliğini sağlama görevi bulunmaktadır?

- A. Sağlık Bakanlığı
- B. Ulaştırma Bakanlığı
- C. Kültür ve Turizm Bakanlığı
- D. Orman ve Su İşleri Bakanlığı
- E. Gençlik ve Spor Bakanlığı

Cevap : B

Aşağıdakilerden hangisi aktif atak türünden olan DoS Atak türü değildir?

- A. Smurf
- B. Teardrop
- C. Logic Bomb
- D. Ping of Death
- E. DNS Cache Posining

CEVAP :C

Aşağıdakilerden hangisi insanları aynı günde doğmuş olmaları varsayımından hareket ederek; MD5 içindeki keyleri bulmak için yapılan bir saldırıdır?

- A. Birthday Atak
- B. Dictionary-based Atak
- C. Footprinting
- D. Fingerprinting
- E. Spyware ve Adware

CEVAP : A

Bulut bilişimin ayrıldığı üç segmet aşağıdakilerden hangi şıkta doğru verilmiştir?

- A. depolama,sunum,transport
- B. Bağlantı,transport,uygulama
- C. link , bağlantı , transport
- D. hizmet ,sunum , transport
- E. uygulama,depolama, bağlantı

cevap : E

Bulut bilişim hangi üç servis modeline göre güvenlik zorluklarını sınıflandırılmıştır?

- A. SaaS, PaaS, IaaS
- B. PaaS,SaaS,IaaS
- C. SaaS,PaaS,IaaS
- D. PaaS,SaaS,IaaS
- E. SaaS,PaaS,IaaS

cevap A

Aşağıdakilerden hangisi firewall için yanlış bir ifadedir?

- A. İç tehditlere karşı virüslü program ve dosyalara karşı koruma sağlar.
- B. Yerel ağlar üzerindeki kaynakları diğer networkler üzerinden gelecek saldırılara karşı koruyan, iç ve dış ağlar arası ağ trafiğini tanımlanan kurallara göre denetleyen bir ağ geçidi çözümüdür.
- C. Firewall'ın sistem üzerinde etkili kullanılması için bir ağ ortamı ile internet arasındaki tüm trafiğin Firewall üzerinden geçmesi gerekmektedir.
- D. Genellikle firewall, atakları önlemek için kurulur.
- E. İki ağ arasında konumlandırılarak bir ağı diğerinden korur.

Cevap: A

Aşağıda verilen Güvenlik duvarı ile ilgili bilgilerden hangisi doğrudur?

- A. Güvenlik duvarı tek bir sistemdir.
- B. Güvenlik duvarı kullanıma hazır yazılımdır.
- C. Güvenlik duvarı bütün problemlerinizi çözer.
- D. Güvenlik duvarı güvenlik politikalarını uygular.
- E. Güvenlik duvarı bilgisayarları, normal makinalar gibi üretici firma tarafından dağıtılan tam bir yazılım desteği gibi kurulmalıdır.

Cevap:D