1. Paket filter paket və ya məlumat ötürülməsi zamanı hansı məlumatlara nəzarət edir?

- Yalnız mənbə IP ünvanına və TCP portuna
- Yalnız mənbə IP ünvanına və UDP portuna
- Yalnız təyinat IP ünvanına və UDP portuna
- √ Həm mənbə, həm də təyinat İP ünvanları və TCP / UDP portlarına
- Yalnız təyinat IP ünvanına və TCP portuna

2. WEP, WPA və WPA2-ni sındırmaq üçün istifadə olunan alətlərə aiddir.

- ZoneAlarm
- Comodo
- Anti NetCut3
- √ coWPAtty
- Tinywall

3. Qurğular şəbəkəyə hansı formada qoşula bilər?

- Host-əsaslı müdaxilə aşkarlama sistemi vasitəsilə
- Tətbiq şlüzləri vasitəsilə
- Şəbəkə-əsaslı müdaxilə aşkarlama sistemi vasitəsilə
- √ Simsiz giriş nöqtələri vasitəsilə
- Təhlükəsizlik divarları vasitəsilə

4. Şəbəkə-əsaslı müdaxilə aşkarlama sistemlərinin (NIDS) yoxladığı trafik yükünü azaltmaq üçün nə etmək lazımdır?

- Antiviruslardan istifadə olunmalıdır.
- Şəbəkədən keçən trafiki azaltmaq lazımdır.
- Şəbəkədə yalnız hardware təhlükəsizlik divarları yerləşdirilməlidir.
- Şəbəkədə yalnız proqram təminatı (software)təhlükəsizlik divarları yerləşdirilməlidir.
- √ Təhlükəsizlik divarı kimi başqa filtrləmə cihazının arxasına yerləşdirilməlidir.

5. Media Girişinə Nəzarət (MAC) Ünvan Filtrləmə nədir?

- Texniki avadanlıq və proqram təminatı ilə bağlı problemlərin diaqnostikası və həllinin həyata keçirilməsidir.
- İntranet şəbəkəsində istifadəçilərin identifikasiyası prosesinin həyata keçirilməsini təmin edən təhlükəsizlik vasitəsidir.
- Trafikdəki hər bir paketin məzmununa ayrı-ayrılıqda baxır və çıxış və təyinat IP ünvanlarına, port nömrəsinə və istifadə olunan protokola əsaslanaraq, trafikin keçməsinə icazə verilib-verilməyəcəyini müəyyənləşdirir.
- OSİ modelinin nəqliyyat səviyyəsində qurularaq trafikdəki hər bir paketin məzmununa ayrı-ayrılıqda yoxlayır.
- √ MAC ünvanın simsiz nöqtənin təhlükəsizlik parametrlərinin icazə verilən filtr siyahısına daxil edilməsi və yalnız bu cihazın şəbəkəyə qoşulmasına icazə verilməsidir.

6. Firewallar nə üçün istifadə olunur?

- Texniki avadanlıq və proqram təminatı ilə bağlı problemlərin diaqnostikası və həlli üçün
- Kompüterlərin və internetin sürətini heç bir əlavə alət olmadan bir neçə dəfəyə qədər artırmaq üçün
- Cihaz və ya şəbəkə haqqında məlumat toplamaq və bu məlumatları hakerə ötürmək üçün
- √ Təhlükəsizliyinə şübhə etiyimiz şəbəkə üzrə həm daxili şəbəkəmizlə İnternet arasındakı sərhəddə, həm də daxili şəbəkəmizdə quraşdırmaq üçün
- Şəbəkədəki müştəri kompütrlərin sistem yenilənmələrini həyata keçirmək üçün

7. "Müştəri və təşkilat arasında qurulur və müştəri mesaj göndərərkən həmin sorğunu alır və onu OSİ modelinin application (tətbiq) səviyyəsində yoxlayır". Bu təhlükəsizlik divarının hansı növüdür?

- Application Gateways
- Packet Filtering
- √ Proxy
- Circuit-Level Gateways
- Stateful Packet Inspection

8. Skanerlər (Scanners) ...

- Şəbəkə və ya protokol analizatorudur, şəbəkədəki trafikə müdaxilə edə bilən bir vasitədir.
- Penetrasiya testinin həyata keçirildiyi şəbəkə növüdür
- Simsiz şəbəkələr tərəfindən köhnə cihazları dəstəkləmək üçün istifadə edilən təhlükəsizlik standartıdır.
- √ Təhlükəsizlik testi və qiymətləndirilməsi üçün şəbəkə qorunma alətidir.
- Yalnız UNIX-ə bənzər əməliyyat sistemlərində şəbəkə qorunma alətidir.

9. Simsiz Qorunan Giriş (Wireless Protected Access-WPA) nədir?

- Simsiz şəbəkələr tərəfindən köhnə cihazları dəstəkləmək üçün istifadə edilən təhlükəsizlik standartıdır.
- Penetrasiya testinin həyata keçirildiyi şəbəkə növüdür
- √ Şəbəkədəki istifadəçiləri autentifikasiya edən və yalnız təsdiqlənmiş istifadəçilərə simsiz şəbəkələrə qoşulmağa icazə verən vasitədir.
- Təhlükəsizlik testi və qiymətləndirilməsi üçün əsas vasitələrdən biridir.
- Hər bir simsiz giriş nöqtəsində olan və cihazlara mövcud şəbəkələri axtarmaq və müəyyən etmək üçün imkan yaradan vasitədir (addır).

10. Paket Filtrləmə (Packet Filtering) təhlükəsizlik divarları necə işləyir?

- Paketləri fərdi şəkildə deyil, vəziyyət cədvəli adlanan cədvəllərdən istifadə edərək çıxış və təyinat IP ünvanları, istifadə olunan portlar və artıq mövcud şəbəkə trafiki ilə müəyyən edilən verilmiş əlaqə üzərindən trafikə baxa bilir.
- OSİ modelinin nəqliyyat səviyyəsində qurularaq trafikdəki hər bir paketin məzmununa ayrı-ayrılıqda yoxlayır.
- OSI modelin sessiya təbəqəsində, TCP/İP modelinin isə TCP təbəqəsində işləyir.
- Müştəri və təşkilat arasında qurulur və müştəri mesaj göndərərkən həmin sorğunu alır və onu OSİ modelinin application (tətbiq) səviyyəsində yoxlayır.
- √ Trafikdəki hər bir paketin məzmununa ayrı-ayrılıqda baxır və çıxış və təyinat IP ünvanlarına, port nömrəsinə və istifadə olunan protokola əsaslanaraq, trafikin keçməsinə icazə verilib-verilməyəcəyini müəyyənləşdirir.

11. Şəbəkə administratorunun roluna aid deyil.

- Şəbəkədə istifadəçi hesablarının avtorizasiyasını həyata keçirmək
- Şəbəkə trafikinin monitorinqini aparmaq
- Şəbəkədə zərərli proqramları aşkar etmək və zərərsizləşdirmək
- √ Texniki avadanlıq və proqram təminatı ilə bağlı problemlərin diaqnostikası və həlli
- Şəbəkədə istifadəçi hesablarının autentifikasiyasını həyata keçirmək

12. WAN haqqında deyilən fikirlərdən hansı yanlışdır?

- Müxtəlif coğrafi ərazilərdən qoşulan insanların eyni məlumatları əldə edə bilməsinə xidmət edən şəbəkədir.
- √ Hardware və ya proqram təminatını paylaşmaq üçün yaradılmış şəbəkə növüdür.
- Bir-birindən uzun məsafədə olan fərdi kompüterlərin və ya LAN-ların bir-birinə qoşulmasıdır.
- Böyük bir coğrafi əraziyə quraşdırılır və telefon şəbəkəsi və ya radio dalğaları vasitəsilə birləşdirilir.
- Mövcud olan ən böyük WAN İnternetdir.

13. DNS neçənci portdan istifadə edir?

- 80
- 514
- 443
- √ 53
- 22

14. Domen adlar sistemi (DNS) nədir?

- İP ünvanların statik və dinamik olmasına qərar verən sistemdir.
- Sertifikatsız domen adlar və İP ünvanlar sistemidir.
- Domenlərə qadağan olunmuş İP-lərdən daxil olmanı məhdudlaşdıran serverdir.
- √ Domen adlarını və onlara bağlı olan İP ünvanları özündə saxlayan serverdir
- Domenləri hücumlardan qorumaq üçün yaradılmış təhlükəsizlik sistemidir.

15. İmzalara əsaslanan Host Əsaslı Müdaxilə Aşkarlama Sistemləri necə işləyir?

- Naməlum təhlükələri müəyyən etmək və zərərli davranışı qeyd etmək üçün maşın öyrənmə üsullarından istifadə edirlər
- İstifadəçilərin identifikasiyası prosesinin həyata keçirilməsini təmin edir.
√ Məlum təhlükələrin əvvəlcədən proqramlaşdırılmış siyahısından istifadə etməklə fəaliyyət göstərirlər.
- Yalnız İntranet şəbəkəsinin qurulması prosesində istifadə olunaraq istifadəçi səlahiyyətlərini özündə saxlayır.
- Lazımsız xidmətləri bloklayaraq şəbəkədəki istifadəçilərin veb resurslardan istifadəsini asanlaşdırır.

16. Təhlükəsizlik Divarı (Firewall) nədir?

- Lazımsız tətbiqi proqram təminatlarının silinməsi üçün istifadə edilən sistem proqram təminatı vasitəsidir
- Klaviaturada vurulan düymələri izləmək və ya qeyd etmək üçün istifadə edilən hardware və ya proqram təminatına əsaslanan vasitədir
- Sadəcə cihazlara tətbiq oluna bilən təhlükəsizlik tədbirləridir.
- Digər tərəfə sadəcə öz funksiyasını yerinə yetirmək üçün lazım olan mütləq minimum icazənin verilməsidir.
√ İstənməyən trafiki aşkar etmək və filtrləmək üçün şəbəkədə host səviyyəsində təhlükəsizlik qatının əlavə edilməsi alətlər dəstidir.

17. Digər tərəfə sadəcə öz funksiyasını yerinə yetirmək üçün lazım olan mütləq minimum icazənin verilməsi hansı prinsipə əsaslanır?

- Məxfilik prinsipinə
- Cavabdehlilik prinsipinə
- Bütövlük prinsipinə
√ Ən az səlahiyyət prinsipinə
- Faydalılıq prinsipinə

18. Host Əsaslı Müdaxilə Aşkarlama Sistemlərinin (HIDS) naməlum təhlükələri müəyyən etmək və zərərli davranışı qeyd etmək üçün maşın öyrənmə üsullarından istifadə etməklə fəaliyyət göstərən növü hansıdır?

- Şəbəkəyə əsaslanan
- Proqram Təminatına əsaslanan
- İmzalara əsaslanan
√ Anomaliyalara əsaslanan
- Aparat Təminatına əsaslanan

19. Qeyd edilənlərdən hansı hücum səthini azaltmağın yolu deyil?

- Lazımsız proqram təminatının silinməsi
- Proqram təminatı yeniləmələrinin vaxtında yerinə yetirilməsi
- Ortaq hesablarda dəyişikliklərin edilməsi
√ Yaddaşın düzgün bölüşdürülməsi
- Vacib olmayan xidmətlərin silinməsi və ya söndürülməsi

20. Rootkit troyan -

- şəbəkəni trafiklə dolduraraq əməliyyatları ləğv edir
- IM platformalarında login və parollarınızı oğurlayır
- uzaq şəbəkə bağlantısı vasitəsilə kompüterinizə tam nəzarət edə bilər
√ zərərli proqramın cihazınızda işləmə müddətini uzatmaq üçün obyekti gizlətmək və məqsədi daşıyır
- antivirus proqramı kimi görünür, lakin içərisində zərərli proqramı gizlədir

21. Botnet nədir?

- Xüsusi tarifli nömrələr ilə telefon əlaqəsi yaratmağa çalışan bir proqramdır
- Klaviaturada vurulan düymələri izləmək və ya qeyd etmək üçün istifadə edilən hardware və ya proqram təminatına əsaslanan vasitədir
- Qurban haqqında şəxsi məlumatları toplayıb nümayiş etdirdikləri reklamları fərdiləşdirmək üçün vasitədir.
- Cihaz və ya şəbəkə haqqında məlumat toplayan və bu məlumatları hakerə ötürən vasitədir.
√ Zərərli proqramı yaymaq üçün istifadə olunan yoluxmuş kompüterlər şəbəkəsidir.

22. - zərərli kodu icra edilə bilən fayllara daxil edir.

- Backdoor Trojan

- Trojan IM
- Ransom Trojan
- Polimorf virus
- √ Fayl infeksiyası virusu

23. Proqram təminatı təhlükəsizliyinin əsas texnikalarına aid olmayanları seçin:
1. Müdafiəçi proqramlaşdırma
2. Əmr inyeksiyası
3. Sandboxing
4. SQL inyeksiyaları
5. Təhdid modelləşdirmə
6. Buferin yüklənməsi

- 1,3,5
- 2,4,5
- √ 2,4,6
- 1,3,6
- 2,3,4

24. Veb skript virusu necə işləyir?

- Tərkibində virus olan faylı işlətdiyiniz zaman işə düşür
- zərərli kodu icra edilə bilən fayllara — sistemdə müəyyən funksiyaları və ya əməliyyatları yerinə yetirmək üçün istifadə edilən fayllara daxil edir
- proqram təminatı üçün istifadə olunan eyni makro dildə yazılır
- hər dəfə yoluxmuş fayl icra edildikdə kodunu dəyişir
- √ Veb-brauzerlərin və veb səhifələrin kodundan istifadə edir

25. ... proqram təminatının potensial risklər altında düzgün işləməyə davam etməsi üçün proqramı zərərli hücumdan və digər hücum risklərindən qorumaq üçün həyata keçirilən prosesdir.

- Hijacking
- Hardware təhlükəsizliyi
- Kibercinayətkarlıq
- Hacking
- √ Proqram təminatının təhlükəsizliyi

26. Fayl üçün hər bir istifadəçi sinfinə verilə biləcək icazələrə aid deyil:

- Yazmaq - Write
- İcra etmək - Execute
- İnkar etmək - Denied
- √ Silmək - Delete
- Oxumaq - Read

27. Qovluğun və ya Diskin şifrələnməsi hansı məhdudiyyətləri qoyur?

- Verilənlərin ələ keçirildiyi zaman məlumatın nəzərdə tutulan alıcısı olmayan hər kəsin məlumatı açıb oxumasının qarşısını alır.
- Məlumatların bütövlüyünü təmin edir və məlumatlarınızın hər hansı icazəsiz dəyişdirilməsinin qarşısını alır.
- Şəxsi və məxfi məlumatların yalnız nəzərdə tutulan alıcı tərəfindən baxılmasını təmin edir.
- √ Şifrənizi unudulduğu zaman, məlumatların bərpa edilməsində problemlər yaranır.
- Şifrələmə sizə sənədin müəllifinin kim olduğunu yoxlamağa imkan verir.

28. Sosial Mühəndislik Metodu hansıdır?

- Information Diving
- Dumpster Diving
- Pretexting
- √ Fişinq
- Skimming

29. Aşağıdakılardan hansı Bulud Komputinqdə təhdid sayıla bilər?

- Farminq
- Skimminq
- Çiyin Sörfinqi
- Fişinq
- √ Məxfiliyin Potensial İtkisi

30. Data təhlükəsizliyi üçün əsas təhlükələrə aid deyil:

- Sistem qəzaları və hard disk qəzaları
- Verilənlərin təsadüfi silinməsi və ya üzərinə yazılması
- Kompüter virusları
- √ Bulud komputinq
- Xətalı disklər və disk sürücüləri

31. Data nədir?

- √ emal edilməmiş və qeyri-mütəşəkkil faktlar və rəqəmlərdir
- korporativ məlumatların qorunması və icazəsiz giriş vasitəsilə məlumat itkisinin qarşısının alınması prosesidir.
- maliyyə və ya şəxsi mənfəət üçün qeyri-qanuni fəaliyyətlər həyata keçirmək üçün internetdən və ya kompüterdən istifadədir.
- istifadəçilərə resursları və məlumatları istənilən vaxt və istənilən yerdə digər cihazlarla paylaşmağa imkan verən internet əsaslı komputinq xidmətinin bir növüdür.
- qeyri-qanuni olaraq həssas məlumatları əldə etmək məqsədi ilə insanları manipulyasiya etmək və ya təsir etmək üsuludur.

32. Məxfilik ...

- məlumatların həqiqi, etibarlı olmasını və pozulmamasını və dəyişdirilməməsini təmin etmək deməkdir.
- məlumatların saxlandığı mühitin fiziki vəziyyətinə aiddir.
- məlumatın sahibi və ya yaradıcısı kimi düzgün atributlara aiddir.
- √ informasiyaya giriş hüququ olan istifadəçilər qrupunun təyini, informasiyanın istifadəsi və onun saxlandığı, emal edildiyi və ötürüldüyü sistemlərə icazəsiz müdaxilələrə məhdudiyyətlərin qoyulmasıdır
- Parker heksadının yeganə prinsipidir ki, ikili xarakter daşımır.

33. İnformasiya Təhlükəsizliyi Təlimatları nədir?

- İnformasiyaya giriş hüququ olan istifadəçilər qrupunun təyini, informasiyanın istifadəsinə, onun saxlandığı, emal edildiyi və ötürüldüyü sistemlərə kənardan müdaxilələrə məhdudiyyətlərin qoyulmasıdır.
- Seçilmiş sahə və ya tətbiq üçün minimum təhlükəsizlik nəzarətləri
- Seçilmiş metodlara, texnikalara və cihazlara müraciət edən informasiya təhlükəsizliyi siyasətlərində təhlükəsizlik tələblərinin təkmilləşdirilməsidir, tətbiqi məcburidir.
- √ Seçilmiş metodlara, texnikalara və cihazlara müraciət edən informasiya təhlükəsizliyi siyasətlərində təhlükəsizlik tələblərinin təkmilləşdirilməsidir, lakin tətbiqi məcburi deyil.
- Rəsmi təsdiq prosesi olmadan paylaşılan məlumatlardır.

34. Qeyd edilən Parker altılığı prinsiplərindən hansı CIA üçlüyünə daxil deyil?

- Məxfilik
- Əlçatanlıq
- Tamlıq
- √ Həqiqilik
- Bütövlük

35. Aşağıdakılardan hansı verilənlər bazası sistemidir?

- √ PostgreSQL
- Angular
- Python
- Android
- Fedora

36. Aşağıdakılardan hansı verilənlər bazası sistemidir?

- Angular
- C#
- √ MS Sql
- Linux
- Swift

37. Aşağıdakılardan hansı verilənlər bazası sistemidir?

- Linux
- Anaconda
- Solaris
- Python
- √ Oracle

38. Aşağıdakılardan hansı kodun təhlükəsizliyini təmin etmək üçün ən yaxşı təcrübələrdən hesab olunmur?

- Verilənlərin daxil edilməsinin yoxlanılması
- Rabitə Təhlükəsizliyi
- Kriptoqrafik Təcrübələr
- Doğrulama və parolun idarə edilməsi
- √ Steqanoqrafik Təcrübələr

39. Aşağıdakılardan hansı ümumi təhlükələr qrupuna aid edilə bilər?

- DDOS
- Watchfire kimi proqram skanerlərindən istifadə etmə
- Daxili və xarici istifadəçilər üçün ayrı serverlərdən istifadə
- √ Həssas məlumat oğurluğu
- Veb səhifələri və proqramları sınamaq və sazlamaq üçün ayrıca serverdən istifadə

40. Aşağıdakılardan hansı ümumi təhlükələr qrupuna aid edilə bilər?

- DDOS
- Veb səhifələri və proqramları sınamaq və sazlamaq üçün ayrıca serverdən istifadə
- √ Saytlararası sorğu saxtakarlığı (CSRF)
- Watchfire kimi proqram skanerlərindən istifadə etmə
- Daxili və xarici istifadəçilər üçün ayrı serverlərdən istifadə

41. Koda təsir edən təhlükəsizlik zəifliklərini seçin: 1.Qeyri- kafi logging və monitorinq; 2.Injection Flaws; 3.Saytlararası Skriptləmə (XSS);

- 1.20
- 3
- √ 1,2,3
- 2.30
- 1.30

42. Aşağıdakılardan hansı ümumi təhlükələr qrupuna aid edilə bilər?

- Watchfire kimi proqram skanerlərindən istifadə etmə
- Daxili və xarici istifadəçilər üçün ayrı serverlərdən istifadə
- DDOS
- Veb səhifələri və proqramları sınamaq və sazlamaq üçün ayrıca serverdən istifadə
- √ Saytlararası skript (XSS)

43. Təhlükəsiz proqramlaşdırma dedikdə nəzərdə tutulan anlayış aşağıdakılardan hansıdır?

- √ Təhlükəsiz proqramlaşdırma hər cür zəifliklərdən, hücumlardan və ya proqram təminatına və ondan istifadə edən sistemə zərər verə biləcək hər hansı bir prosesdən qorunmaq üçün proqram təminatında kodların yazılması üsuludur

- Təhlükəsiz proqramlaşdırma iş masasında yerləşən proqram təminatlarının hazırlanma qaydalarını öyrənən elm sahəsidir
- Sistem üçün mümkün təhlükələrin araşdırılması üsullarına təhlükəsiz proqramlaşdırma deyilir
- Təhlükəsiz proqramlaşdırma iş masasının təhlükəsizliyinin təmin edilməsi üsullarından biridir
- Təhlükəsiz proqramlaşdırma proqram təminatında kodların yazılması üsuludur

44. Aşağıdakılardan hansı proqramlaşdırma dilidir?

√ PHP
- Centos
- Django
- Redis
- Ubuntu

45. Aşağıdakılardan hansı proqramlaşdırma dilidir?

- Oracle
- Fedora
- Centos

√ Swift
- Pycharm

46. Aşağıdakılardan hansı proqramlaşdırma dilidir?

√ C++
- Centos
- MS SQL
- Pycharm
- Linux

47. Aşağıdakılardan hansı proqramlaşdırma dilidir?

- Oracle
- My SQL
- Linux

√ Java
- Redis

48. Aşağıdakılardan hansı proqramlaşdırma dilidir?

- Scatter

√ C#
- Ubuntu
- Windows
- Numpy

49. Aşağıdakılardan hansı proqramlaşdırma dilidir?

- Centos

√ Python
- Pycharm
- Matplotlib
- Eclipse

50. Aşağıdakılardan hansı proqramlaşdırma dilidir?

- Linux
- Pycharm
- Anaconda

√ Kotlin
- Solaris

51. " Etibarsız agentlər hədəflənmiş sistemdə öz skriptlərini icra etmək üçün saytlararası skript qüsurlarından istifadə edə bilərlər." - bu koda təsir edən hansı təhlükəsizlik zəifliyi hesab olunur?

- Məlum Zəiflikləri Olan Komponentlərdən İstifadə:
- √ Saytlararası Skriptləmə (XSS)
- Qeyri- kafi logging və monitorinq
- Injection Flaws
- Həssas Məlumatlara məruz qalma

52. " Komponentlər kitabxanalar, çərçivələr və digər proqram modullarından ibarətdir. Komponent həssasdırsa, o, etibarsız agent tərəfindən istismar edilə bilər " - bu koda təsir edən hansı təhlükəsizlik zəifliyi hesab olunur?

- Həssas Məlumatlara məruz qalma
- Injection Flaws
- Qeyri- kafi logging və monitorinq
- √ Məlum Zəiflikləri Olan Komponentlərdən İstifadə
- Saytlararası Skriptləmə (XSS):

53. " Həssas məlumatlar – məsələn, ünvanlar, parollar və hesab nömrələri – lazımi qaydada qorunmalıdır " - bu koda təsir edən hansı təhlükəsizlik zəifliyi hesab olunur?

- Qeyri- kafi logging və monitorinq
- Injection Flaws
- Saytlararası Skriptləmə (XSS)
- Həssas Məlumatlara məruz qalma
- √ Məlum Zəiflikləri Olan Komponentlərdən İstifadə

54. " Injection qüsurları etibarsız məlumatlar əmr və ya sorğunun bir hissəsi kimi göndərildikdə baş verir " - bu koda təsir edən hansı təhlükəsizlik zəifliyi hesab olunur?

- Həssas Məlumatlara məruz qalma
- Qeyri- kafi logging və monitorinq
- Saytlararası Skriptləmə (XSS)
- Həssas Məlumatlara məruz qalma
- √ Injection Flaws

55. Uyğunluğu müəyyən edin:

1. Texniki təhlükəsizlik
2. Trafik təhlükəsizliyi
3. Xətt təhlükəsizliyi

a. naqillər olmadan ötürülən və 3-cü şəxs tərəfindən ələ keçirilə bilən siqnal məlumatlarının yayılmasının qarşısını alır.
b. mərkəzi kompüter və uzaq terminallar kimi İT sistemlərinin rabitə xətlərini qoruyur.
c. mikrofonlardan, ötürücülərdən və ya dinləmələr zamanı məlumat rabitəsinin ələ keçirilməsinə qarşı müdafiə təmin edir.

- 1-a, 2-b, 3-c
- 1-b, 2-a, 3-c
- 1-c, 2-b, 3-a
- √ 1-c, 2-a, 3-b
- 1-b, 2-c, 3-a

56. Kommunikasiya təhlükəsizliyin alt sahələri hansılardır?
1. Xətt təhlükəsizliyi
2. E-poçt təhlükəsizliyi
3. Ötürmə təhlükəsizliyi
4. Trafik təhlükəsizliyi
5. Texniki təhlükəsizlik

- 3,4,5
- 1,2,4,5
- 1,2,3,4
- 1,2,3,4,5

√ 1,3,4,5

57. HTTPS məlumatı neçənci port üzərindən göndərir?

- 80
- 76
- 221
- 124
√ 443

58. HTTP və HTTPS OSI modelinin hansı səviyyələrində işləyirlər?

- Hər ikisi nəqliyyat səviyyəsində
- HTTP-nəqliyyat HTTPS isə tətbiq səviyyələrində
- HTTP-tətbiq, HTTPS isə təqdimat səviyyələrində
√ HTTP-tətbiq, HTTPS isə nəqliyyat səviyyələrində
- HTTP-fiziki, HTTPS isə təqdimat səviyyələrində

59. HTTPS istifadə edərək göndərilən məlumatlar hansı protokol vasitəilə qorunur?

- DNS
- FTP
√ TLS
- UDP
- TCP/IP

60. HTTP məlumatı neçənci port üzərindən göndərir?

- 443
√ 80
- 124
- 76
- 221

61. "Təşkilatdakı rolundan və ya mövqeyindən asılı olmayaraq əvvəlcədən müəyyən edilmiş qaydalar toplusuna və ya giriş icazələrinə uyğun olaraq ərazilərə, cihazlara və ya verilənlər bazalarına girişi idarə edir". Bu giriş nəzarət modellərinin hansı növüdür?

- Məcburi Giriş Nəzarəti
√ Qayda Əsaslı Giriş Nəzarəti
- İxtiyari Giriş Nəzarəti
- Rol Əsaslı Giriş Nəzarəti
- Atribut Əsaslı Giriş Nəzarəti

62. - sahibinə kompüter sistemindəki obyektə daxil olmaq icazəsi verən token və ya açardır.

- Giriş nəzarət siyahıları
√ Giriş nəzarət imkanları
- Şəbəkə ACL-ləri
- Giriş nəzarət modelləri
- Fayl ACL-ləri

63. Qeyd edilənlərdən hansı fayl giriş icazələrinə aid deyil?

- Əsas atributları oxumaq/dəyişdirmək
√ MAC ünvanlarını vvə İP ünvanları filtirləmək
- ACL oxumaq/dəyişdirmək
- Sinxron oxuma və yazma ilə yerli olaraq fayla daxil olmaq
- kataloqun məzmununu siyahıya almaq

64. Girişin ləğv edilməsi nədir?

- Müəyyən tərəfə və ya tərəflərə verilmiş resursa giriş imkanı verilməsidir.
- √ Bir şəxsə və ya sistemə bir resursa giriş icazəsi verdikdən sonra bu giriş icazəsinin əlindən alınmasıdır.
- Resursa müəyyən çərçivədə bəzi girişlərə icazə verilməsidir.
- Fayl sistemlərinə girişi idarə etmək və sistemlərin qoşulduğu şəbəkələrdə trafik axınına nəzarət etməkdir.
- Müəyyən resursa şəxssin girişinin qarşısının alınmasıdır.

65. Fayl sistemi siyahıları qeyd edilənlərdən hansı üzrə girişi nəzarətdə saxlamaq üçündür?

- Portlar
- √ Qovluqlar
- Mac ünvanlar
- Kommutatorlar
- İP-lər

66. Girişə nəzarət prosesinin yerinə yetirilməsi vəziyyətlərinə aid deyil.

- Girişə icazə verilməsi
- √ Giriş nəzarət imkanları
- Girişin məhdudlaşdırılması
- Girişin ləğv edilməsi
- Girişin rədd edilməsi

67. Fiziki giriş nəzarətinin əsas komponenti deyil.

- Giriş nöqtəsi
- √ Şəbəkə siyahıları
- İdarəetmə paneli
- Girişə nəzarət serveri
- Oxuyucular/klaviaturalar

68. Məlumatlara məntiqi və ya kompüter əsaslı girişə icazə verilməsi və ya rədd edilməsi dedikdə nə başa düşülür?

- Fiiki girişə nəzarət
- √ Məntiqi girişə nəzzarət
- Giriş nöqtəsi
- Atribut əsaslı giriş nəzarəti
- İdarəetmə paneli

69. Fiziki giriş nəzarəti nədir?

- məlumatlara məntiqi və ya kompüter əsaslı girişə icazə vermək və ya rədd etmək vasitəsidir.
- √ məkana girişin selektiv məhdudlaşdırılmasıdır.
- şəxsə lazım olan funksiyaları yerinə yetirmək imkanı vermək üçün yalnız minimum girişə icazə verilməsidir.
- Bir şəxsə və ya sistemə bir resursa giriş icazəsi verdikdən sonra bu giriş icazəsini əlindən alınmasıdır.
- istifadəçinin kimliyini təsdiq etdikdən sonra, ona sistem üzərində nə etməyə icazə verildiyini müəyyən ediməsidir

70. Qarşılıqlı autentifikasiya çoxfaktorlu autentifikasiya ilə birlikdə istifadə edildiyi zaman çoxfaktorlu autentifikasiya harada baş verməlidir?

- serverdən müştəriyə doğru
- √ yalnız müştəri tərəfində
- həm müştəri, həm server tərəfində
- ikisinin birlikdə istifadəsi mümkün deyil
- yalnız serverde

71. - şəxs və ya proses kimi hər hansı istifadəçinin və ya tətbiqin unikal şəkildə müəyyən edilməsi vasitəsidir.

- Autentifikasiya
- √ İdentifikasiya

- Qarşılıqlı autentifikasiya
- Çoxfaktorlu autentifikasiya
- Avtorizasiya

72. Qoşulmuş (Connected) Tokenlər necə işləyirlər?

- Fiziki və məntiqi əlaqəyə, həmçinin xüsusi daxiletmə qurğusuna ehtiyac olmadan, istifadəçinin daxil etdiyi autentifikasiya məlumatlarını göstərmək üçün ekrandan istifadə edilən token növüdür.
- √ Fiziki əlaqə vasitəsilə hardware təhlükəsizlik nişanını oxucuya sürüşdürməyi tələb edir və cihazın autentifikasiya məlumatını sistemə avtomatik daxil edir.
- Hər hansı fiziki əlaqə tələb etmədən məntiqi əlaqə yaratmaqla, radiotezlik identifikasiyası vasitəsilə autentifikasiya məlumatını ötürən token növüdür.
- Fiziki və məntiqi əlaqəyə ehtiyac olmadan, radiotezlik identifikasiyası vasitəsilə autentifikasiya məlumatını ötürür.
- Cihaza qoşulmağa və ya hər hansı giriş kodunu daxil etməyə ehtiyac olmadan simsiz əlaqə yaradır və sistem ya girişə icazə verir, ya da rədd edir.

73. Universallıq nəyə əsasən seçilən biometrik amildir?

- Müəyyən bir xüsusiyyətin fərdlər arasında nə qədər unikal olduğuna əsasən
- √ Sistem istifadəçilərinin hamısında mövcud olacaq biometrik xüsusiyyətə əsasən
- İstifadəçini daha sonra autentifikasiya edə biləcəyimiz bir xüsusiyyət əldə etməyin asanlıq dərəcəsinə əsasən
- hər hansı bir xüsusiyyətin sistemin istifadəçiləri tərəfindən nə dərəcədə qəbul ediləbilən olmasına əsasən
- Müəyyən bir xüsusiyyətin zamanla və yaşla dəyişməyə nə qədər müqavimət göstərməsinə əsasən

74. Autentifikasiyanın hansı faktoru fərdin unikal fiziki atributlarına, yəni biometrik məlumatlara əsaslanır?

- Bildiyiniz bir şey
- √ Olduğunuz bir şey
- Olduğunuz bir yer
- Etdiyiniz bir şey
- Sahib olduğunuz bir şey

75. Autentifikasiya dedikdə nə başa düşülür?

- İstifadəçi girişləri müxtəlif istifadəçi hesabları ilə doğrulandıqdan sonra onlara şəxsiyyətlərinə görə müxtəlif resurslara giriş icazəsi verilməsidir.
- √ Sistemə daxil olan istifadəçinin iddia etdiyi şəxs olduğunu sübut etməsi ilə şəxsiyyətinin təsdiqlənməsi prosesidir.
- Sistemin kənar müdaxilələrdən qorunması üçün təhlükəsizlik cihazlarının quraşdırılması prosesidir.
- İstifadəçilərin 3-cü tərəf tətbiqlərin API-lərini mövcud sistemə quraşdırması üçün vasitədir.
- Şəxs və ya proses kimi hər hansı istifadəçinin və ya tətbiqin unikal şəkildə müəyyən edilməsi vasitəsidir.

76. Twofish-i digər şifrələmə alqoritmlərindən fərqləndirən əsas xüsusiyyət nədir?

- Əməliyyatları bitlərlə deyil, verilənlərin baytları üzərində həyata keçirməsi
- √ Əvvəlcədən hesablanmış, açardan asılı əvəzetmə qutularından (S qutuları) istifadə etməsi
- Açar uzunluğunu ikiqat artırmaq performansı zəiflətsə də, gücün eksponensial artması
- 128 bitlik açar üçün 12 dövrdən istifadə etməsi
- Əvəzetmə-permütasiya şəbəkəsi prinsipinə əsaslanması

77. Hash funkisyalarında toqquşma müaviməti xassəsi nəyi təmin edir?

- Hash funksiyasını geri qaytarmaq hesablama baxımından çətin olmalıdır.
- Bir giriş və hash verildiyi zaman, eyni hash ilə fərqli bir giriş tapmaq çətin olmalıdır.
- giriş dəyərinə və onun hashinə malik olan və fərqli dəyəri orijinal daxilolma dəyərinin yerinə qanuni dəyər kimi əvəz etmək istəyən təcavüzkardan qoruyur.
- Əgər h hash funksiyası z hash dəyərini yaradıbsa, o zaman z-ə hash edən hər hansı x giriş dəyərini tapmaq çətin proses olmalıdır.
- √ Eyni hash ilə nəticələnən istənilən uzunluqda iki fərqli girişi tapmaq çətin olmalıdır.

78. 3 açarlı 3DES alqoritmi ilə şifrələmə zamanı -

- K2 açarı ilə tək DES istifadə edərək 1-ci addımın çıxışı şifrələnir.

- K1 açarı ilə tək DES istifadə edərək şifrəli mətn bloklarının şifrəsi açılır..
- 2-ci açarın çıxışı şifrəli mətn hesab olunur.
- K1 açarı ilə tək DES istifadə edərək ilkin açıq mətn blokları şifrələnir.
√ K1 açarı ilə tək DES istifadə edərək açıq mətn blokları şifrələnir.

79. Təhlükəsiz Hash Funksiyası olan SHA-2-nin hansı variantı yoxdur?

- SHA-256
- SHA-384
- SHA-512
√ SHA-128
- SHA-224

80. Hash funksiyalarının xüsusiyyətlərinə aid deyil.

- Uzunlu çıxışı, yəni hash dəyəri sabit olur.
- Hash dəyəri giriş məlumatlarından çox kiçik olduğuna görə, hash funksiyaları bəzən sıxılma funksiyaları adlanır.
√ Məşhur hash funksiyaları 64-256 bit arasında dəyərlər alır.
- İxtiyari uzunluqdakı məlumatları sabit uzunluğa qədər sıxır.
- N bit çıxışı olan hash funksiyası n-bit hash funksiyası adlanır.

81. Hansı xüsusiyyət assimmetrik şifrələmənin çatışmazlığıdır?

- Rəqəmsal imzaların istifadəsi ilə alıcı mesajın konkret göndəricidən gəldiyini yoxlaya bilir.
- Açarların mübadiləsinə ehtiyac olmadığı üçün açar paylama problemi yoxdur.
- Göndərənin mesajın göndərilməsini inkar edə bilməməsi üçün rədd edilməməyə imkan verir.
- Şəxsi açarların heç kimə ötürülməsi və ya açıqlanması lazım olmadığı üçün təhlükəsizlik səviyyəsi aşağıdır.
√ Açıq açarların autentifikasiyası olmadığı üçün açıq açarın göstərilən şəxsə məxsus olması təmin edilə bilmir

82. Elliptik əyri tənliyinin xüsusiyyətlərindən istifadə edən kriptoqrafik alqoritm hansıdır?

- 3DES
- AES
- DES
- RSA
√ ECC alqoritmi

83. RSA alqoritmində -

√ iki böyük sadə ədədin nəticəsi olan böyük tam ədədlərin faktorinqi ilə hesablanır.
- ixtiyari uzunluqdakı məlumatları sabit uzunluğa qədər sıxılır.
- elliptik əyri nəzəriyyəsinə əsaslanaraq elliptik əyri diskret loqarifmi hesablanır.
- heç bir açardan istifadə edilmədən məlumatların qorunması həyata keçirilir.
- Əsasən 128 və 256 bitlik açarlardan istifadə edilir.

84. DES şifrələmdə faktiki açar neçə bitlik olur?

- 256
- 128
- 2048
- 1024
√ 56

85. Simmetrik şifrələmənin xüsusiyyətlərinə aid deyil.

- Assimetrik şifrələmədən daha sürətlidir.
- AES, DES 3DES simmetrik şifrələmə alqoritmləridir.
- 128 və ya 256 bitlik açardan istifadə edir.
- Resurslardan az istifadə edir.
√ Kiçik ölçülü məlumatların ötürülməsi üçün istifadə olunur.

86. Hansı şifrələmədə mesajlar göndərən tərəfindən şifrələnir, vasitəçi nöqtədə – mesajlaşma xidməti provayderinə məxsus üçüncü tərəf serverində qəsdən deşifrə edilir və sonra yenidən şifrələnir və alıcıya göndərilir.

- Assimmetrik şifrələmə
- Simmetrik şifrələmə
- Rest şifrələmə
- √ Tranzit şifrələmə
- Ucdan-uca şifrələmə

87. Sosial Mühəndislik metodu olan Spear Phishing hücumları necə həyata keçirilir?

- E-poçtun yüksək vəzifəli heyət üzvlərindən gəldiyi iddia edilir.
- Veb trafiki qanuni saytlardan zərərli domenlərə yönləndirir.
- Qanuni şəxslərdən olduğu iddia edilən mətn mesajları 2FA-dan (iki faktorlu autentifikasiya) yan keçmək üçün digər üsullarla birlikdə istifadə olunur.
- √ Xüsusi təşkilatları və ya şəxsləri hədəf alır.
- Sosial mediada saxta müştəri xidmətləri hesabları vasitəsilə həyata keçirilir.

88. Ucdan-uca şifrələmə haqqında qeyd edilən fikirlərdən hansı yanlşdır?

- Göndərən və nəzərdə tutulan alıcıdan başqa heç kəsə tranzit zamanı mesaj məlumatını oxumağa icazə vermir
- Məlumatlar əldə edilə bilən vasitəçi serverdə saxlanıla bilər.
- √ Mesajın məzmunu ilə birlikdə göndərildiyi tarix və ya mübadilə iştirakçıları kimi məlumatları gizlədir.
- Hücumçular təhlükə altında olan son nöqtələrdən açarları əldə edə və oğurlanmış açıq açarla man-in-the middle hücumunu həyata keçirə bilərlər.
- Şifrələnmiş mesajlara müdaxilədən qoruyur.

89. Aşağıdakılardan hansı tətbiq mərhələsinin addımlarından hesab olunur?

- Proqram təminatı sisteminin layihələndirilməsi
- √ Layihənin paket proqramına çevrilməsi
- Forma və alətlərin kodlarının daxil edilməsi
- Formanı işlətməklə sınaqdan keçirmək
- Proqram təminatı sisteminin hazırlanacağı proqramlaşdırma dilinin və verilənlər bazasının seçilməsi

90. Aşağıdakılardan hansı test mərhələsinin addımlarından hesab olunur?

- √ Formanı işlətməklə sınaqdan keçirmək
- Proqram təminatı sisteminin hazırlanacağı proqramlaşdırma dilinin və verilənlər bazasının seçilməsi
- Proqram təminatı sisteminin layihələndirilməsi
- Layihənin paket proqramına çevrilməsi
- Forma və alətlərin kodlarının daxil edilməsi

91. Aşağıdakılardan hansı hazırlıq mərhələsinin addımlarından hesab olunur?

- Layihəni işlətməklə sınaqdan keçirmək
- √ Proqram təminatı sisteminin hazırlanacağı proqramlaşdırma dilinin və verilənlər bazasının seçilməsi
- Formanı işlətməklə sınaqdan keçirmək
- Sınaq ediləcək formaların müəyyən edilməsi
- Proqram təminatı sisteminin layihələndirilməsi

92. Aşağıdakılardan hansı proqramlaşdırma dilidir?

- Vmware
- QEMU
- SQL
- √ Java
- VirtualBox

93. Aşağıdakılardan hansı təhlil mərhələsinin addımlarından hesab olunur?

- Sınaq ediləcək formaların müəyyən edilməsi
- Proqram təminatı sisteminin hazırlanacağı proqramlaşdırma dilinin və verilənlər bazasının seçilməsi
- Formanı işlətməklə sınaqdan keçirmək
- Layihəni işlətməklə sınaqdan keçirmək
- √ Proqram təminatı sisteminin layihələndirilməsi

94. Aşağıdakılardan hansı güclü parol hesab olunur?

- Sql231
- 18412596
- DEleTe7612
- √ InsturctoR^^))80
- PASSw31

95. Aşağıdakılardan hansı verilənlər bazası sistemidir?

- √ Cassandra
- Pycharm
- Python
- Linux
- Anaconda

96. Aşağıdakılardan hansı verilənlər bazası sistemidir?

- Linux
- Matplotlib
- √ MongoDB
- Angular
- Pycharm

97. Aşağıdakılardan hansı verilənlər bazası sistemidir?

- Pyhon
- Swift
- Fedora
- Linux
- √ MariaDB

98. Aşağıdakılardan hansı verilənlər bazası sistemidir?

- Python
- Scatter
- Anaconda
- √ Redis
- Linux

99. Aşağıdakılardan hansı güclü parol hesab olunur?

- 65410
- CodE27
- 328905
- √ CoMPuteR^^))20
- App25

100. Aşağıdakılardan hansı güclü parol hesab olunur?

- 17403589
- sOfT12

- 1578
- Python48
- √ ApPlicaTioN^^))21

101. Aşağıdakılardan hansı verilənlər bazası sistemidir?

- Anaconda
- Numpy
- √ IBM Db2
- Matplotlib
- Solaris

102. Cavab variantlarından hansı Proqram təminatının inkişaf prosesi mərhələlərinin ardıcıllığını düzgün əks etdirir?. 1.Təhlil; 2.Hazırlıq; 3.Dizayn; 4.Tətbiq; 5.Test;

- 1,3,5,2,4
- 1,5,3,2,4
- 1,2,5,3,4
- √ 1,3,2,5,4
- 1,2,3,4,5

103. İnformasiya təhlükəsizliyi nədir?

- √ Qarşılaşa biləcək təhlükələrdən xəbərdar olmaq, işin davamlılığını təmin etmək, baş verə biləcək hər cür problemdə itkiləri minimuma endirmək, hər bir şəraitdə fərdlərin və qurumların aktivlərinin məxfiliyini, əlçatanlığını və bütövlüyünü qorumaq məqsədi daşıyır
- İnformasiya təhlükəsizliyi mümkün hücumları nəzərə almaqla, proqramlaşdırma dillərindən istifadə edərək təhlükəsiz proqram kodlarının yaradılması mexanizmidir.
- Qarşılaşa biləcək təhlükələrdən xəbərdar olmaq, işin davamlılığını təmin etmək, baş verə biləcək hər cür problemdə itkiləri minimuma endirmək, hər bir şəraitdə fərdlərin və qurumların aktivlərinin yalnız bütövlüyünü qorumaq məqsədi daşıyır
- Qarşılaşa biləcək təhlükələrdən xəbərdar olmaq, işin davamlılığını təmin etmək, baş verə biləcək hər cür problemdə itkiləri minimuma endirmək, hər bir şəraitdə fərdlərin və qurumların aktivlərinin yalnız əlçatanlığını qorumaq məqsədi daşıyır
- Qarşılaşa biləcək təhlükələrdən xəbərdar olmaq, işin davamlılığını təmin etmək, baş verə biləcək hər cür problemdə itkiləri minimuma endirmək, hər bir şəraitdə fərdlərin və qurumların aktivlərinin yalnız məxfiliyini qorumaq məqsədi daşıyır

104. Aşağıdakılardan hansı proqramlaşdırma dilidir?

- SQL
- QEMU
- Vmware
- VirtualBox
- √ C#

105. OWASP hansı fərqli ölçüdə işləyir?

- kitabxanalar və kriptoqrafiya
- idarəetmə, yoxlama və quraşdırma
- Səlahiyyələrin verilməsi və konfiqurasiyanın idarə edilməsi
- √ alətlər, sənədlər və icma
- Səhvlərin İdarə Edilməsi və kriptoqrafiya

106. OWASP neçə fərqli üsulda işləyir?

- 2
- 6
- 4
- √ 3
- 5

107. Rəqəmsal imza necə sistemdir?

- irarxik

√ assimmetrik
- rəqəmsal
- klassik
- simmetrik

108. Xətti cəbrə və modul hesaba əsaslanan poliqram əvəzetmə şifrəsi hansıdır?

- Vernam
√ Hill
- Playfair
- Bekon
- Sezar

109. 3DES necə alqoritmdir?

- Rəqəmsal
√ Simmetrik
- Texniki
- Hash
- Assimmetrik

110. randint(4, 1.5, 3.5, 6, 9). Nəticə necə ola bilər?

- (4, 3.5, 6)
√ (4,6,9)
- (3.5, 6, 9)
- (4, 1.5, 3.5)
- (1.5, 6, 9)

111. 2DES texnologiyası neçə bitlik açar ölçüsünə malikdir?

- 168
√ 112
- 28
- 14
- 56

112. list = [3,6,9,15,25,40,50,95] sampling = random.choice(list,k=4). Nəticə necə ola bilər?

- (4,12,30)
√ (3,8,40,95)
- (5,10,15,20)
- (1,3,7,15)
- (5,9,55,95)

113. randrange(3,9). Nəticə necə ola bilər?

- 10
√ 7
- 15
- 12
- 1

114. shuffle(7,2,9,3,5). Nəticə necə ola bilər?

- (9,11,15,7,9)
√ (3,2,7,5,9)
- (3,12,7,15,9)
- (13,2,7,1,9)
- (15,2,8,5,12)

115. Əsas mətni açar mətindən istifadə edərək VERNAM şifrələmə metodu ilə şifrələyin. Əsas mətn= "RANDOM", açar mətn = "DES"

- pistvh
- √ uefgse
- uwqsfh
- uafgse
- ueklsm

116. Assimmetrik şifrələmə zamanı nə baş verə bilər?

- şifrləmə açarı itirilə bilər
- √ şifrləmə açarı yayıla bilər
- şifrləmə açarı dəyişdirilə bilər
- şifrləmə açarı silinə bilər
- şifrləmə açarı qoruna bilər

117. shuffle()-in nəticə necə ola bilər

- verilmiş ardıcıllıqla təsadüfi nümunə ilə bir siyahını qaytarir
- bir ardıcıllığın göstərilən nümunəsini qaytarir
- təsadüfi say generatorunun daxili vəziyyətini qaytarir
- √ bir sıra götürür və qarışıq vəziyyətdə qaytarır
- verilmiş ardıcıllıqla tam ədədləri qaytarır

118. Təsadüfi say generatorunun daxili vəziyyətini qaytaran əmr hansıdır?

- sample()
- √ setstate()
- choices()
- random()
- shuffle()

119. Verilmiş ardıcıllıqla təsadüfi nümunə ilə bir siyahını qaytaran əmr hansıdır?

- setstate()
- √ choices()
- shuffle()
- random()
- sample()

120. Təsadüfi say generatoru(TSG) nədir?

- daim təsadüfi bir cümlə yaradır
- √ daim təsadüfi bir rəqəm yaradır
- daim psevdotəsadüfi bir cümlə yaradır
- daim təsadüfi bir söz birləşməsi yaradır
- daim psevdotəsadüfi bir rəqəm yaradır

121. Biri müasir kriptoqrafiyanın bölmələrinə aiddir

- texniki sistemlər
- √ simmetrik kriptosistemlər
- alqoritmik kriptosistemlər
- qapalı açarlı kriptosistemlər
- assimetrik kriptosistemlər

122. Qammalaşdırma alqoritmlərin mahiyyəti nədir?

- şifrələnən mətnin simvolları mətnin tərtib edildiyi əlifbanın simvolları ilə əvəz olunur

√ şifrələnən mətn simvollarının qamma şifrəsi simvolları ilə alınır
• təkrarlama və növbələmə ardıcıllığı ilə şifrələnən mətn blokuna çevirməsidir
• şifrələnən mətn simvollarının betta şifrəsi simvolları ilə alınır
• açıq mətnin simvollarının yeri dəyişdirilir

123. Müasir kriptoqrafiyanın neçə mühüm bölməsi var?

• 5
√ 4
• 2
• 1
• 3

124. Əvəzetmə alqoritmlərin mahiyyəti nədir?

• şifrələnən mətn simvolları qamma şifrəsi ilə alınır
√ şifrələnən mətn simvollarının qamma şifrəsi simvolları ilə alınır
• təkrarlama və növbələmə ardıcıllığı ilə şifrələnən mətn blokuna çevirməsidir
• şifrələnən mətnin simvolları mətnin tərtib edildiyi əlifbanın simvolları ilə əvəz olunmur
• açıq mətnin simvollarının yeri dəyişdirilir

125. "Cipher" mətnini ROT=5 olduqda SEZAR metodu ilə şifrələyin

• hnwida
√ hnumjw
• hnumsk
• awdfje
• hnuska

126. Statik açar nəyə deyilir?

• yeni istifadə olunan açar
• Dinamik şifrəni açan açar
• Yalnız birdəfə istifadə olunan açar
√ dəfələrlə istifadə olunan eyni bir açar
• istifadə olunmayan açar

127. "Texnologiya" mətnini ROT=13 olduqda SEZAR metodu ilə şifrələyin

• grkaqtmlope
• gsfhgdscbje
• grkafnmdtqp
√ grkabybntvl
• grkastuifbl

128. ASCII cədvəlinin 33 -dən 127 -ə qədər olan hissəsi nələri kodlaşdırmaq üçün nəzərdə tutulub?

• digər əlifba simvollarını
• əməliyyatları
• milli əlifba simvolları
√ latın hərflərinə, rəqəmlərə, hesabi əməliyyat və durğu işarələrinə uyğun gəlir
• psevdaqrafiki simvolları

129. ASCII cədvəlinin ilk 33 kodu nələri kodlaşdırmaq üçün nəzərdə tutulub?

• latın hərflərini
• rəqəmləri
• hesabi əməliyyat və durğu işarələri
√ əməliyyatlar və psevdaqrafiki simvolları
• milli əlifba simvollarını

130. Sezar şifrəsi necə adlanırdı?

- simmetrik
- dinamik
- blokvari
- √ monoəlifbalı
- Assimmetrik

131. Kriptoqrafiya nədir?

- İnformasiya mühafizəsi üsullarının hazırlanması haqqında elmdi
- informasiya emalı haqqında elmdir
- informasiyanın çevrilməsi haqqında elmdir
- √ Kriptoqrafiya məlumatın məxfiliyinin neçə təmin olunmasını öyrənən elmdir
- informasiya şifrələnməsi haqqında elmdir

132. Kriproqrafiyanın inkişafı hansı dövrü əhatə edir?

- √ XIV əsrin sonu
- XI əsrin sonu
- XIV əsrin əvvəli
- IX əsr
- XV əsrin sonu

133. Əsas mətni BLOK şifrələmə metodu ilə şifrələyin. K=2 Əsas mətn = SERVIS

- asqwyu
- nskqps
- vdkaic
- √ rbredb
- iuhgst

134. Axtarış motoru filtrləri nə edir?

- Fərdi kompüterdə və ya noutbukda proqram təminatı kimi quraşdırılmaqla uyğun olmayan məzmuna çıxışına nəzarət etmək üçün istifadə olunur.
- Müəyyən kontentə baxış üçün istifadəçinin şəxsi kimlik məlumatlarına uyğun olaraq məzmunun nümayişini həyata keçirir.
- Brauzerə əlavə edilə bilən plaginlər vasitəsilə məzmunun filtrasiyasını həyata keçirir.
- Webcontent-in yalnız müəyyən bir hissəsinə giriş təklif edir və hansı məzmunun əldə oluna biləcəyi ilə bağlı qərarı istifadəçi deyil, ISP verir.
- √ İstifadəçilərə axtarış nəticələrindən uyğun olmayan keçidləri süzgəcdən keçirən təhlükəsizlik filtrini təqdim edir.

135. Pharming hücumu necə baş verir?

- Brauzerə funksionallığı dəyişdirməyən əlavə funksionallıq təmin edir və nəticədə hücum həyata keçirilir.
- Müəyyən veb-saytlarda yerləşdirilmiş reklamlara daxil olmaqla brauzer kukilərinin ələ keçirilməsi həyata keçirilir.
- Kompüterə yalançı antivirus proqramlar yüklənməsi yolu ilə FK-də arxa qapı açaraq təcavüzkarın kompüterə daxil olmasına şərait yaradır.
- √ DNS yoluxmasından istifadə etməklə, serverdəki domen adı sistem cədvəli dəyişdirilərək mövcud saytın İP-si başqa İp ilə əvəz edilir, istifadəçilər avtomatik olaraq saxta saytlara yönləndirilir.
- Spam mesajlarına zərərli qoşmalar və linklər əlavə edilərək qurbanın həmin əlavəni yükləməsi və daxil olması tələb olunur və istifadəçi kompüterinə virus göndərilir.

136. Özünü təkrarlayan və nüsxələrini başqa kompüterlərə göndərən proqram

- Backdoor
- Troyan atı
- Məntiq bombası
- √ Worm
- Rootkit

137. HTTP-nin sonuncu təqdim edilən sorğu metodu hansıdır

- TRACE
- PUT
- CONNECT
- DELETE
√ PATCH

138. HTTP-nin mövcud versiyası neçə sorğu metodundan istifadə edir?

- 5
- 7
- 8
√ 9
- 3

139. Fişinq hücumunun planlaşdırma mərhələsində nə baş verir?

- Cinayətkarlar saxta e-poçt mesajlarını nəzərdə tutulan qurbanlara göndərirlər
- Təcavüzkarlar saxtakarlıq etmək üçün şirkəti və onların nəzərdə tutulan qurbanlarını müəyyən etdikdən sonra, e-poçt çatdırılması və məlumat toplama üsulları və alətləri hazırlayırlar.
√ Hücumun icraçıları hansı şirkət və ya təşkilatın adından saxtakarlıq edəcəklərinə qərar verir və həmin şirkətin müştəri e-poçt ünvanlarının siyahısını necə əldə edəcəyini öyrənir.
- Qurbanlardan toplanan məlumatlardan istifadə edərək, cinayətkarlar qanunsuz alış-veriş etməyə və ya qurbanın hesablarından pul köçürməyə başlayırlar.
- Qurbanların saxta internet səhifələrinə daxil etdikləri məlumatlar toplanır və qeydə alınır.

140. Bu hansı şifrələmə alqoritmidir?
- Göndərilən məlumatları 64 bitlik hissələrə parçalayır və hər birini ayrıca şifrələyir.
- 32 bitdən 448 bitə qədər dəyişən uzunluqlu açar alır.
- 16 iterasiyadan ibarətdir
- Hər iterasiya iki 32 bitlik sözə bölünmüş 64 bitlik blokda işləyir.
- Tək şifrələmə açarından istifadə edir.
- İctimai istifadə üçün pulsuzdur.

- AES
- DES
- 3DES
√ Blowfish
- RSA

141. Aşağıdakılardan hansı Autentifikasiya vasitələri kimi istifadə edilə bilər?

- Anket məlumatlar
√ Parol və biometrik xarakteristikalar (şəkil, barmaq izləri, səs və s.)
- Şəxsi əlaqələr
- İş yerinin adı
- İnformasiya təhlükəsizliyi üzrə biliklər

142. Autentifikasiya nədir?

- Susmaya görə təhlükəsizlik rejiminin qoşulmasıdır
- İnformasiya mühitində dövlətin, fiziki və hüquqi şəxslərin qorunmasının vəziyyətidir
- Proqram təminatının ilkin qəbulu (installyasiyası) və cari icrasının təhlükəsiz təşkilidir
- Təhlükəsiz proqram təminatının hazırlanması prosesinin təşkilidir
√ Subyekt tərəfindən təqdim edilmiş eyniləşdirmə məlumatlarının həqiqiliyinin yoxlanması prosesidir

143. "Qara qutu" testinin məqsədi nədir?

- Kiber hücumların müəyyən edilməsi
- İstehsalat təcrübələrində zəif cəhətlərin müəyyən edilməsi

- İstismar potensialını ölçmək üçün zəif cəhətlərin yoxlanılması
- √ Kodlaşdırma xətaları üçün mənbə kodunun skan edilməsi
- Məxfilik xassəsinin ödənilməsi

144. Aşağıdakılardan hansı daxiletmənin yoxlanılması üsullarından hesab olunur?

- Ağ qutu və Boz qutu testi
- İdentifikasiya proseduru
- Avtorizasiya proseduru
- √ Ağ qutu və Qara qutu testi
- Autentifikasiya proseduru

145. SAMM modelində biznes funksiyaları və təhlükəsizlik fəaliyyətləri neçə ayrı qrupda idarə olunur?

- √ 4
- 10
- 8
- 3
- 2

146. Daxiletmənin yoxlanılması üsulları neçə hissəyə bölünür?

- √ 2
- 6
- 4
- 3
- 5

147. Aşağıdakılardan hansı ağ qutu sınağı ilə qara qutu sınağı arasındakı fərqi ən yaxşı şəkildə təsvir edir?

- √ Ağ qutu testi proqramın daxili məntiqi strukturlarını yoxlayır
- Qara qutu sınağı biznes və maliyyə bölmələrini əhatə edir
- Ağ qutu sınağı müstəqil proqramçılar qrupu tərəfindən həyata keçirilir
- Qara qutu sınağı aşağıdan yuxarı yanaşmadan istifadə edir
- Qara qutu sınağı biznes bölmələrini əhatə edir

148. “Trusted Computing Group” tərəfindən irəli sürülən etibarlı hesablama konsepsiyası hansı əsas anlayışa diqqət yetirir?

- Məxfilik və Bərpa Oluna Bilənlik
- Məxfilik, Əlçatanlıq və Bərpa Oluna Bilənlik
- Məxfilik, Bütövlük
- √ Məxfilik, Bütövlük, Əlçatanlıq və Bərpa Oluna Bilənlik
- Bütövlük, Əlçatanlıq və Bərpa Oluna Bilənlik

149. “Trusted Computing Group” tərəfindən irəli sürülən etibarlı hesablama konsepsiyası neçə əsas anlayışa diqqət yetirir?

- 3
- 1
- 2
- √ 4
- 5

150. Tətbiq təhlükəsizliyini qiymətləndirmək və nəzərdən keçirmək nə vaxt daha düzgün addım hesab olunur?

- Dizayn mərhələsində
- Təhlil mərhələsində
- Hazırlıq mərhələsində
- √ Tətbiqin inkişafının bütün mərhələlərində
- Test mərhələsində

151. Aşağıdakılardan hansı OWASP təhlükəsiz kodlaşdırma təcrübələrindəndir?

- İnzibati nəzarət
- Simmetrik nəzarət
- Aktiv nəzarət
- √ Girişə nəzarət
- Detektiv nəzarət

152. Aşağıdakılardan hansı sql injection hücum növüdür?

- SYN Flood
- ICMP (Ping) Flood
- Password Dpraying
- √ Error-based SQLi
- Credential stuffing

153. Aşağıdakılardan hansı sql injection hücum növüdür?

- UDP Flood
- IP Null attack
- Volumetric attacks
- Appsec FAQ
- √ İn-band SQLi

154. Aşağıdakılardan hansı ddos hücum növü deyil?

- UDP Flood
- Volumetric attacks
- Protocol attack
- √ Appsec FAQ
- IP Null attack

155. Aşağıdakılardan hansı ddos hücum növü deyil?

- SYN Flood
- UDP Flood
- ICMP (Ping) Flood
- √ Credential stuffing
- IP Null attack

156. Aşağıdakılardan hansı ddos hücum növü deyil?

- ICMP (Ping) Flood
- UDP Flood
- √ Bonets
- HTTP Flood
- IP Null attack

157. Aşağıdakılardan hansı ddos hücum növü deyil?

- UDP Flood
- ICMP (Ping) Flood
- √ Password Dpraying
- SYN Flood
- HTTP Flood

158. Aşağıdakılardan hansı ddos hücum növüdür?

- Bonets
- LAPSE

- Password Dpraying
√ HTTP Flood
- Hybrid brute force attack

159. OWASP layihəsinin icma ölçüsünə aşağıdakılardan hansı daxildir?

- WebScarab
- test bələdçisi
- Metriklər
√ Tərcümələr
- LAPSE

160. OWASP layihəsinin sənədlər ölçüsünə aşağıdakılardan hansı daxildir?

- Forumlar
- Live CD
√ Test bələdçisi
- LAPSE
- Vikilər

161. OWASP layihəsinin sənədlər ölçüsünə aşağıdakılardan hansı daxildir?

- Live CD
- Forumlar
- Konfranslar
√ Appsec FAQ
- WebScarab

162. OWASP layihəsinin alətlər ölçüsünə aşağıdakılardan hansı daxildir?

- Appsec FAQ
- Bloqlar
- Metriklər
√ WebScarab
- Forumlar

163. OWASP layihəsinin alətlər ölçüsünə aşağıdakılardan hansı daxildir?

- Test bələdçisi
- Appsec FAQ
- Bloqlar
√ .NET Research
- Vikiler

164. OWASP layihəsinin icma ölçüsünə aşağıdakılardan hansı daxildir?

- Appsec FAQ
- Metriklər
- Test bələdçisi
√ Vikiler
- WebGoat

165. SAMM modeli hansı fərqli qrupda idarə olunur?

- Səlahiyyələrin verilməsi və konfiqurasiyanın idarə edilməsi
- alətlər, sənədlər və icma
√ idarəetmə, tikinti, yoxlama və quraşdırma
- kitabxanalar və kriptoqrafiya
- Səhvlərin İdarə Edilməsi və kriptoqrafiya

166. Autentifikasiya üçün hansı vasitələrdən istifadə edilə bilər?

- şəxsi əlaqələr
- informasiya təhlükəsizliyi bilikləri
- √ parol və biometrik xüsusiyyətlər
- iş yerinin adı
- profil məlumatları

167. "Yaxşı Hash Funksiyası" nələri nəzərdə tutur? Tam cavabı qeyd edin

- √ asanlıqla hesablanır və düymələr bərabər paylanmalıdır
- düymələr bərabər paylanmır
- çətinliklə hesablanır
- düymələr bərabər paylanmalıdır
- asanlıqla hesablanır

168. Böyük rəqəmi və ya mətni hash cədvəlində indeks kimi istifadə oluna bilən kiçik tam ədədə çevirən funksiya hansıdır?

- random funksiya
- loqorifmik funskiya
- √ hash funksiyası
- xətti funksiya
- müəyyənlik funksiyası

169. Blok şifrələməsi haqqında hansı doğrudur?

- şifrələnmiş mətni geri qaytarmaq mümkün deyil
- yalnız qarışıqlığa əsaslanır
- Heç biri
- √ şifrlənmiş mətni geri qaytarmaq çətindir
- düz mətnə asanlıqla çevrilə bilər

170. Əsas mətni açar mətindən istifadə edərək Affine şifrələmə metodu ilə şifrələyin.a=7, b=5, Əsas mətn = KRYPTO

- cvbhnm
- poklim
- dfgtry
- √ xurgiz
- qsdlkm

171. Əsas mətni açar mətindən istifadə edərək Affine şifrələmə metodu ilə şifrələyin.a=7, b=5, Əsas mətn = SERVER

- wertgh
- klpmnb
- √ bhuwhu
- scvfgh
- sdfplo

172. Bloklu şifrələdə hansından istifadə olunur ?

- XNOR
- √ XOR
- AND
- OR
- NOR

173. Bloklu şifrəyə nümunə olaraq şifrləri seçin: 1-DES 2-3DES 3-AES 4-RSA 5-BLOWFİSH

- 2;4

- 1;4;5
- 1;5
- 3;4;5

√ 1;2;3

174. Əsas mətni açar mətindən istifadə edərək Affine şifrələmə metodu ilə şifrələyin.a=5, b=2, Əsas mətn = LIST

- QYXZ
- SFGH
- HIJK
- OPQR

√ FQUZ

175. Sağ dövri sürüşdürmənin düsturu hansıdır?

- X`=XROSV
- X`=XSHLV
- X`=XSHRV
- X`=XROLV

√ X`=XRORV

176. Əsas mətni açar mətindən istifadə edərək Affine şifrələmə metodu ilə şifrələyin.a=5, b=2, Əsas mətn = KEY

- STU
- NBD
- YZN

√ AWO

- QJO

177. Hesabı sağa sürüşdürmən düsturu hansıdır?

- X`=XROSV
- X`=XRORV
- X`=XROLV
- X`=XSHLV

√ X`=XSHRV

178. Hesabı sola sürüşdürmə düsturu hansıdır?

- X`=XROSV
- X`=XRORV

√ X`=XSHLV

- X`=XSHRV
- X`=XROLV

179. Proqram təminatının və rəqəmsal imzanın müdafiəsində istifadə olunan sistem hansıdır?

- PGP
- AES
- 3DES
- DES

√ RSA sistemi

180. Məlumatın deşifrələnməsi şifrələnməsindən daha gec, imzanın yoxlanması isə onun yaradılmasından daha tez gedən alqoritm hansıdır?

- PGP
- MOD
- 3DES
- DES

√ RSA

181. Aşağıdakılardan hansı şifrələmə funksiyasına və əks funksiyanın mürəkkəbliyinə əsaslanır?

- Alqoritmin qeyri-xəttiliyi
- Alqoritmin dövrlüyü
- Alqoritmin xəttiliyi
- Alqoritmin zəifliyi
- √ Alqotimin dayanıqlığı

182. Blok sifrələməsindən istifadə edən AES və digər alqoritimlərdən daha yavaş alqoritm hansıdır?

- DES
- 3DES
- MOD
- PGP
- √ RSA

183. Əsas mətni açar mətindən istifadə edərək PLAYFAIR şifrələmə metodu ilə şifrələyin. Əsas mətn = "HACK", açar mətn = "FAIR"

- PSCV
- YJKL
- AFGH
- √ DBKP
- FBKP

184. Əsas mətni açar mətindən istifadə edərək PLAYFAIR şifrələmə metodu ilə şifrələyin. Əsas mətn = "CIPHER", açar mətn = "User"

- QWDFPL
- PLKJMN
- CVBNHJ
- √ IONKRA
- SDFHJK

185. Dictionary attack hansı funksiyanı yerinə yetirir?

- mümkün parollari əlifbaya görə tərs düzür
- mümkün parollari əlifbaya görə düzür
- √ bütün potensial parolları yoxlamaq
- loginə uyğun yeni parollar hazırlayır
- yeni parolları əlifbaya uyğun düzür

186. Əsas mətni açar mətindən istifadə edərək Hill şifrələmə metodu ilə şifrələyin. Əsas mətn = "security", açar mətn = "(1,3),(8,13)"

- bbahdksd
- √ ycggdzdf
- dfkwmvkd
- asvbhjop
- sjkiplfk

187. Şifrəni etibarlı şəkildə saxlayan texnologiya hansıdır?

- PGP
- Chrome
- E-poct
- Firefox
- √ KEEPASS

188. Əsas mətni açar mətindən istifadə edərək Hill şifrələmə metodu ilə şifrələyin. Əsas mətn = "(3,2,4),(7,1,1),(5,3,8)", açar mətn = "(1,4,2)"

- (1,9,3)
- (3,8,12)
- √ (19,13,7)
- (7,8,4)
- (2,9,11)

189. Əsas mətni Atbash şifrələmə metodu ilə şifrələyin. Əsas mətn = CODE

- KJFT
- SFHJ
- √ XLWV
- LPYH
- VGBH

190. Rəqəmsal imza və kriptoqrafik səsvermə üsulları kimi bir neçə kriptoqrafik protokolun qapılarını acan kriptosistem hansidir?

- DES
- PGP
- 3DES
- √ RSA
- ECC

191. Əsas mətni açar mətindən istifadə edərək VERNAM şifrələmə metodu ilə şifrələyin. Əsas mətn= "ATTACK", açar mətn = "MİDDLE"

- mnhgfs
- √ mbwdno
- sdfkjq
- liytdf
- asdlpy

192. Məlumat ötürülməsi üçün istifadə olunan ilk asimmetrik kriptosistemlərdən biri hansidir?

- ECC
- √ RSA
- PGP
- 3DES
- DES

193. Əsas mətni açar mətindən istifadə edərək VİJENER şifrələmə metodu ilə şifrələyin. Əsas mətn = "trojan", açar mətn = "none"

- MKJSGQ
- √ GFBXNB
- BVGSKQ
- LAKDBF
- DGKSBF

194. Ələ keçirilən şifrəli mətnə hücum necə adlanır?

- key-only attack
- √ ciphertext-only attack
- plaintext-only attack
- knownrtext-only attack
- read-only attack

195. Əsas mətni Atbash şifrələmə metodu ilə şifrələyin. Əsas mətn = "SYSTEM"

- HSNSBH
- RTLVHE
- ZCBIMI

- SIUYLU
√ HBHGVN

196. Əsas mətni açar mətindən istifadə edərək VİJENER şifrələmə metodu ilə şifrələyin. Əsas mətn = "epidemiya", açar mətn = "virus"

- ZWWEWHQPU
- ZVVVUUYQU
√ ZXZXWHQPU
- AXVXWHQPU
- AWZXUUYPU

197. Rəqəmsal imzanın funksiyasına aid deyil:

- məlumatın müəllifinin autentifikasiyası
- məlumatın müəllifliyindən imtinanın qeyri-mümkünlüyünə zəmanət
√ məlumatın məxfiliyi və əlçatanlığı
- məlumatın müəllifinin idetifikasiyası
- məlumatın bütövlüyünə nəzarət

198. Əsas mətni açar mətindən istifadə edərək VİJENER şifrələmə metodu ilə şifrələyin. Əsas mətn = "security", açar mətn = "hash"

- ZEVCVILG
- EUBYILF
- ZFUCJKMM
√ ZEUBYILF
- AFVBVKLG

199. Rəqəmsal imza alqoritmlərinə aid deyil

- ElGamal
- RSA
- ECDSA
- DSA
√ MAC

200. "Ən Az İmtiyaz Siyasəti (POLP) müəyyən edir ki, istifadəçi müəyyən tapşırığı yerinə yetirmək üçün tələb olunan minimum imtiyazlar dəstinə malik olmalıdır" - bu fikir hansı prinsipdə nəzərə alınmışdır?

- Təhlükəsizliyi sadələşdirmək prinsipi
- Vəzifələrin bölünməsi prinsipi
- Təhlükəsiz şəkildə uğursuzluq prinsipi.
√ Minimum güzəşt prinsipi
- Xidmətlərə etibar edilməməsi prinsipi

201. Aşağıdakılardan hansı İnferensial SQL inyeksiyası növüdür?

- Error-based SQLi
- Birliyə əsaslanan SQLi
√ Boolen
- Klassik SQLi
- Out-of-Band SQLİ

202. Aşağıdakılardan hansı təhlükəsizlik siyasəti hesab olunur?

- Secure in Design
- Secure Development Lifecycle (SDL)
- Secure by Default
- Secure in Deployment
√ Dərin Müdafiə Prinsipi

203. Aşağıdakılardan hansı Klassik SQL inyeksiyası (İn-band SQLi) növüdür?

- Out-of-Band SQLİ
- İnferensial SQLi
√ Error-based SQLi
- Boolen
- Zamana əsaslanan

204. Kriptoqrafiya nədir?

- İlkin mətnin yazılması
- Mətnin oxunması
- İlkin mətnin başqasına çatdırılması
√ İlkin mətnin şifrələnməsi
- İlkin mətnin ləğv edilməsi

205. OWASP layihəsində təhlükəsizlik baxımından ilkin layihə hesab olunur?

- Live CD
√ WebGoat
- .NET Research
- LAPSE
- WebScarab

206. "Tərtibatçılar tətbiqləri üçün təhlükəsizlik nəzarətlərini inkişaf etdirərkən çox mürəkkəb arxitekturalardan istifadə etməkdən çəkinməlidirlər" - bu fikir hansı prinsipdə nəzərə alınmışdır?

- Xidmətlərə etibar edilməməsi prinsipi
√ Təhlükəsizliyi sadələşdirmək prinsipi
- Təhlükəsiz şəkildə uğursuzluq prinsipi.
- Vəzifələrin bölünməsi prinsipi
- Hücum səthinin sahəsini minimuma endirilməsi prinsipi

207. "e-ticarət veb saytının istifadəçisi eyni vaxtda administrator kimi irəli çəkilməməlidir, çünki onlar sifarişləri dəyişdirə və məhsulları özlərinə çatdıra bilərlər" - bu fikir hansı prinsipdə nəzərə alınmışdır?

- Hücum səthinin sahəsini minimuma endirilməsi prinsipi
- Təhlükəsiz şəkildə uğursuzluq prinsipi.
- Xidmətlərə etibar edilməməsi prinsipi
- Təhlükəsizliyi sadələşdirmək prinsipi
√ Vəzifələrin bölünməsi prinsipi

208. Təhlükəsizlik siyasətləri neçə qrupa bölünür?

- 9
- 5
- 4
- 2
√ 10

209. Aşağıdakılardan hansı siyasət risklərə müxtəlif yollarla yanaşan çoxsaylı təhlükəsizlik nəzarətlərinin tətbiqin təhlükəsizliyini təmin etmək üçün ən yaxşı seçim olduğu fikrini təsdiqləyir?

- Təhlükəsiz şəkildə uğursuzluq prinsipi.
√ Dərin Müdafiə Prinsipi
- Hücum səthinin sahəsini minimuma endirilməsi prinsipi
- Təhlükəsizliyi sadələşdirmək prinsipi
- Xidmətlərə etibar edilməməsi prinsipi

210. Aşağıdakı siyasətlərdən hansı siyasət tətbiqin standart olaraq təhlükəsiz olmasını müəyyən edir?

√ Təhlükəsizlik standartlarının yaradılması prinsipi
• Hücum səthinin sahəsini minimuma endirilməsi prinsipi
• Dərin Müdafiə Prinsipi
• Xidmətlərə etibar edilməməsi prinsipi
• Təhlükəsiz şəkildə uğursuzluq prinsipi.

211. "Hər dəfə proqramçı öz tətbiqlərinə funksiyalar əlavə etdikdə, zəiflik riskini artırır" bu fikir hansı prinsipdə nəzərə alınmışdır?

• Xidmətlərə etibar edilməməsi prinsipi
• Təhlükəsizliyi sadələşdirmək prinsipi
• Təhlükəsiz şəkildə uğursuzluq prinsipi.
• Dərin Müdafiə Prinsipi
√ Hücum səthinin sahəsini minimuma endirilməsi prinsipi

212. Avtorizasiya nədir?

• Proqram təminatının ilkin qəbulu (installyasiyası) və cari icrasının təhlükəsiz təşkilidir
√ İstifadəçinin şəxsiyyətinə uyğun olaraq giriş hüquqlarının təyin olunduğu və idarə olunduğu mərhələdir
• Təhlükəsiz proqram təminatının hazırlanması prosesinin təşkilidir
• Susmaya görə təhlükəsizlik rejiminin qoşulmasıdır
• İnformasiya mühitində dövlətin, fiziki və hüquqi şəxslərin qorunmasının vəziyyətidir

213. Aşağıdakılardan hansı güclü parol hesab olunur?

• Linux16
• moBiLe202
• nuMpPy09
√ CybeR^^((99
• ORACLe19

214. Aşağıdakılardan hansı güclü parol hesab olunur?

• map15
• CoMPuteR54321
• 5322789
√ Practice^^((22
• LearniNg098

215. Aşağıdakılardan hansı verilənlər bazası sistemidir?

• Numpy
• Anaconda
√ SQLite
• Table
• Linux

216. Aşağıdakılardan hansı sql injection hücum növüdür?

• Appsec FAQ
• SYN Flood
• HTTP Flood
• IP Null attack
√ Out-of-band SQLi

217. Aşağıdakılardan hansı sql injection hücum növüdür?

• UDP Flood
• IP Null attack
• Volumetric attacks

- Bonets
√ Time-based Blind SQLi

218. Aşağıdakılardan hansı sql injection hücum növüdür?

- Bonets
√ Boolean-based Blind SQLi
- ICMP (Ping) Flood
- Password Dpraying
- Appsec FAQ

219. Aşağıdakılardan hansı sql injection hücum növüdür?

- HTTP Flood
- Appsec FAQ
- UDP Flood
√ Inferential SQLi
- Credential stuffing

220. Aşağıdakılardan hansı sql injection hücum növüdür?

- Password Dpraying
- UDP Flood
- IP Null attack
√ Union-based SQLi
- Bonets

221. Aşağıdakı variantlardan hansında Tətbiqə təsir edə biləcək təhdidlər düzgün qeyd edilmişdir?

- Kod təhdidləri
- Yalnız Proqrm təhdidləri
- Host və Proqram təhdidləri
- Yalnız şəbəkə təhdidləri
√ Şəbəkə, Host və Proqram təhdidləri

222. OWASP neçə sahəni özündə əks etdirən təhlükəsiz kodlaşdırma təcrübəsi təqdim edir?

√ 14
- 12
- 10
- 8
- 6

223. Aşağıdakılardan hansı təhlükəsiz kodlaşdırma üçün istifadə edilən alətlərdəndir?

- İDLE
- Auty
- Visual Studio
- Visual Code
√ Arachni

224. Aşağıdakılardan hansı təhlükəsiz kodlaşdırma üçün istifadə edilən alətlərdəndir?

- İDLE
- Visual Studio
- Visual Code
√ Code Warrior
- Google Autentificator

225. "Qeyri-müəyyənliyə əsaslanan təhlükəsizliyə heç vaxt etibar edilməməsi lazım olduğunu bildirir" bu fikir hansı prinsipdə nəzərə alınmışdır?

- Təhlükəsiz şəkildə uğursuzluq prinsipi.
- Təhlükəsizliyi sadələşdirmək prinsipi
√ Qeyri-müəyyənlik səbəbindən təhlükəsizlikdən əmin olmamaq prinsipi
- Hücum səthinin sahəsini minimuma endirilməsi prinsipi
- Xidmətlərə etibar edilməməsi prinsipi

226. "Tətbiqdə təhlükəsizlik problemi aşkar edilərsə, tərtibatçılar problemin əsas səbəbini müəyyən etməlidirlər" bu fikir hansı prinsipdə nəzərə alınmışdır?

- Xidmətlərə etibar edilməməsi prinsipi
- Dərin Müdafiə Prinsipi
- Hücum səthinin sahəsini minimuma endirilməsi prinsipi
√ Təhlükəsizlik problemlərinin düzgün şəkildə həll edilməsi prinsipi
- Təhlükəsiz şəkildə uğursuzluq prinsipi.

227. Aşağıdakı variantlardan hansında Avtorizasiya prosesi düzgün izah olunmuşdur?

- Proqram təminatının ilkin qəbulu (installyasiyası) və cari icrasının təhlükəsiz təşkilidir
- Təhlükəsiz proqram təminatının hazırlanması prosesinin təşkilidir
- Susmaya görə təhlükəsizlik rejiminin qoşulmasıdır
√ İstifadəçinin şəxsiyyətinə uyğun olaraq giriş hüquqlarının təyin olunduğu və idarə olunduğu mərhələdir
- İnformasiya mühitində dövlətin, fiziki və hüquqi şəxslərin qorunmasının vəziyyətidir

228. Kerberos aşağıdakılardan hansını istifadə edir?

- The Faraday cage, Port 389
- doğrulama xidməti
- Doğrulama xidməti, The Faraday
√ Biletlərin paylanması xidməti, doğrulama xidməti
- Port 389, Doğrulama xidməti

229. İstifadəçiyə şəbəkəyə daxil olmaq üçün iki maddə tələb olunur. Bu iki maddə nədir?

- Doğrulama və avtorizasiya
- Parol və autentifikasiya
- İdentifikasiya və doğrulama
√ İdentifikasiya və autentifikasiya
- Avtorizasiya və identifikasiya

230. Hansı identifikasiya metodu aşağıdakıları əhatə edir: giriş sorğusu, dəyər cavabını şifrələyir, server, çağırış, şifrləmə nəticələrini müqayisə edir və ya uğursuzluq?

- Security Tokens
√ CHAP
- Kerberos
- Sertifikatlaşdırma
- autentifikasiya

231. Hansı autentifikasiya mexanizmi təhlükəsiz mühitdə daha yaxşı işləyir?

- RADIUS autentifikasiya, avtorizasiya və mühasibat xidmətlərini təmin edən müştəri server sistemidir Radius autentifikasiya, avtorizasiya və mühasibat xidmətlərini təmin edən müştəri server sistemidir
- RADIUS, çünki o, müştəri-server parollarını şifrələyir
- TACACS+, çünki bu, uzaqdan giriş identifikasiyası xidmətidir
√ TACACS+, çünki müştəri-server danışıqları dialoqlarını şifrələyir
- RADIUS, çünki o, uzaqdan giriş identifikasiyası xidmətidir

232. Şəbəkənizə giriş əldə etmək üçün istifadəçilər barmaq izi və istifadəçi adı və parol təqdim etməlidirlər. Bu hansı autentifikasiya modelidir?

- domen girişi
- birdəfəlik parol
- Biometrik
- tək giriş
- √ Multifaktor

233. Aşağıdakılardan hansı iki autentifikasiya mexanizmi fiziki olaraq sahib olduğunuz bir şeyi tələb edir?

- Sertifikat, Smart kart
- istifadəçi adı və parol, Smart kart
- √ Smart kart, USB flash drive
- USB flash drive, istifadəçi adı və parol
- Sertifikat, USB flash drive

234. istifadəçilərin autentifikasiyası zamanı aşağıdakılardan hansı ümumi meyar deyil?

- özünün tərkib hissəsi olan nəyi isə
- bildiyi nəyi isə
- etdiyi nəyi isə
- sahib olduğu nəyi isə
- √ bəyənilən nəyi isə

235. Kerberos protokolu harada istifadə olunmur?

- Posix autentifikasiyası
- √ CHAP
- Active Directory
- NFS
- Samba

236. Autetifikasiya haqqında aşağıdakılar yanlışdır?

- RADIUS autentifikasiya, avtorizasiya və mühasibat xidmətlərini təmin edən müştəri server sistemidir Radius autentifikasiya, avtorizasiya və mühasibat xidmətlərini təmin edən müştəri server sistemidir
- Autentifikasiya hansısa varlığın doğruladığı bir məlumat parçasının doğruluğunun təsdiq edilməsidir
- CHAP istifadəçi adı və parolları şifrələdiyi üçün PAP-dan daha təhlükəsizdir
- PAP etibarsızdır, çünki istifadəçi adı və parollar aydın mətn kimi göndərilir
- √ MS-CHAPv1 müştəri və serverin qarşılıqlı autentifikasiyasına qadirdir

237. Aşağıdakılardan hansı istifadəçinin domen resursuna daxil ola bilməsi üçün istifadəçinin atmalı olduğu son addımdır?

- cavabdehlik
- √ Icazə
- autentifikasiya
- yoxlama
- doğrulama

238. Hansı şəbəkə təhlükəsizliyi identifikasiyası metodu bir giriş sessiyasında və ya əməliyyatda istifadə edilmək üçün proqram təminatı və ya aparat əsaslı ola bilər?

- smart kart
- icazə
- tək giriş
- iki faktorlu autentifikasiya
- √ birdəfəlik parol

239. Ümumi tək girişli identifikasiya konfiqurasiyalarının iki nümunəsi hansılardır?

- kerberos əsasında, multifaktorlu autentifikasiya
- √ smart kart əsasında, kerberos əsasında
- multifaktorlu autentifikasiya, biometrika əsasnda
- biometrika əsasında, kerberos əsasında
- biometrika əsasnda, smart kart əsasında

240. Aşağıdakılardan hansı şəxsin şəxsiyyətinin yoxlanılmasıdır?

- Cavabdehlik
- √ Autentifikasiya
- Parol
- smart kart
- Icazə

241. Kerberos hansı protakol əsasında yaranıb?

- X.509
- √ Needham-Schroeder simmertrik açar protokolu
- HTTP
- TC
- OAUTH 2.0

242. Kerberosda Credentials nədir?

- Kerberosun Kerberosdan xəbərdar olan xidmətlərə daxil olmaq üçün biletlər təyin edə biləcəyi unikal şəxsiyyəti təmsil edir.
- √ Bilet və ya servis açarı
- istifadəçinin şəxsiyyətini təsdiq edən məlumatlar
- İstifadəçi adı
- Açıq açar

243. Realm nədir?

- Servis açarı
- √ Məntiqi Kerberos şəbəkəsi
- Çoxluq
- Biletlərin verilməsi xidməti
- Authentifikasiya serveri

244. Kerberosda Principal nədir?

- Bilet
- √ Kerberosun Kerberosdan xəbərdar olan xidmətlərə daxil olmaq üçün biletlər təyin edə biləcəyi unikal şəxsiyyəti təmsil edir
- Açıq açar
- istifadəçinin şəxsiyyətini təsdiq edən məlumatlar
- Servis açarı

245. Kerberos aşağıdakılardan hansı tərəfindən yaradılmışdır?

- ORACLE
- √ MIT
- OKTA
- heç biri
- MICROSOFT

246. Kerberosauthentication həyata keçirərkən aşağıdakı amillərdən hansı nəzərə alınmalıdır?

- Kerberos icazəsiz giriş əldə etmək üçün orta hücumlarda olan insana qarşı həssas ola bilər.
- √ Kerberos bütün istifadəçi və resurs parollarının mərkəzdən idarə olunan verilənlər bazasını tələb edir.
- Kerberos aydın mətn parollarından istifadə edir.

- Kerberos etibarsızdır.
- Kerberos biletləri şəbəkə resurslarına təkrar hücumlar vasitəsilə saxtalaşdırıla bilər.

247. Kerberosun hansı versiyaları daha etibarlıdır?

- 3,4
√ 4,5
- 1,2
- 2,5
- 3,5

248. Əsas mətni BLOK şifrələmə metodu ilə şifrələyin. K=1 Əsas mətn = SERVIS

- vbfdtk
√ visrbr
- mjgcrd
- ertjhu
- dghjkb

249. Aşağıdakılardan hansı hesablara və ya portallara daxil olmaq üçün bir kompüter istifadəçisi tərəfindən yazılmış bir təhlükəsizlik kodudur?

- GPU
√ Mesaj doğrulama kodu(MAC)
- DES
- PGP
- RSA

250. Kriptoqrafiyaya və ölkə daxilində onun tətbiqinə nəzarət edən ölkələr qrupu hansılardır?

- sarı qrup
√ qırmızı qrup
- ağ qrup
- qara qrup
- yaşıl qrup

251. Media girişinə nəzarət ünvanı(MAC ünvanı) hansıdır?

- PGP
√ MIC
- DES
- 3DES
- RSA

252. Əsas mətni BLOK şifrələmə metodu ilə şifrələyin. K=2 Əsas mətn = SYSTEM

- vndjsa
- mkjdsa
- dvjcns
√ wvjzeb
- dfwplk

253. Ölkə daxilində kriptoqrafiyanın tətbiqi və ikili təyinatlı proqram vasitələrinin ixracına müəyyən nəzarəti həyata keçirmək niyyətində olan ölkələr qrupu hansıdır?

- qara qrup
- qırmızı qrup
- yaşıl qrup
√ sarı qrup
- ağ qrup

254. Əsas mətni BLOK şifrələmə metodu ilə şifrələyin. K=1 Əsas mətn = SYSTEM

- wergfh
- rtyhjk
- poebhf
- lkjqnk
- √ temwvj

255. Kiminsə şəxsi mülahizəsindən, alınma üsulundan asılı olmayan, yaxud çox az asılı olan informasiya necə informasiya hesab edilir?

- etibarlı
- güvənli
- anlayışlı
- aktual
- √ bütöv

256. Kriptoqrafiyanın tətbiqini praktiki olaraq məhdudlaşdırmayan ölkələr qrupu hansıdır?

- qara qrup
- qırmızı qrup
- sarı qrup
- ağ qrup
- √ yaşıl qrup

257. Hansı hashing növündə ilk dəfə kompüter oyun proqramlarında şahmat vəziyyətlərini kompakt şəkildə təmsil etmək üsulu kimi təqdim etmişdilər?

- √ Zobrist hashing
- dinamik hash
- Folding
- dəqiqlik hash funksiyası
- Trival

258. Elektron rəqəmsal imza yaradılarkən istifadə olunur ...

- gizli açarın ümumi parametrləri
- açıq açar
- məxfi açar və təhlükəsizlik zərfi
- gizli açar və gizli açarın ümumi parametrləri
- √ ümumi parametrlər, məxfi açar və açıq açar

259. Əsas mətni BLOK şifrələmə metodu ilə şifrələyin. K=2 Əsas mətn = SİMVOL

- plmnhg
- sdfjkl
- podhfj
- √ retehz
- uthgbf

260. Assosiativ massivlər və dinamik dəstlər nə vasitəsi ilə həyata keçirilir?

- xətti alqoritmlər
- şifrləmə
- √ hash cədvəlləri
- riyazi hesablama
- kodlaşdırma

261. Əsas mətni BLOK şifrələmə metodu ilə şifrələyin. K=1 Əsas mətn = SİMVOL

- iuytrh
- ertghk
- ythgjf
- plkjhg
- √ volret

262. Aşağıdakılardan hansı İnformasiya təhdidi anlayışıdır?

- Qəsdən törədilmiş təhlükələr başa düşülür
- √ Obyekt üçün informasiya təhlükəsi yaradan amil və ya amillər toplusu başa düşülür
- Əməkdaşlara qarşı yönələn təhlükələr başa düşülür
- Texniki avadanlıqlara qarşı yönələn təhlükələr başa düşülür
- Təbii fəlakətlər və təsadüfi proseslər başa düşülür

263. Hücumçu mərkəzli yanaşma necə izah olunur?

- Əsas diqqət qorunmağa ehtiyacı olan sistemə və ya proqram təminatına həvalə edilmiş aktivlərə (proqram tərəfindən işlənmiş məlumatlar) yönəldilir
- √ Əsas diqqət təcavüzkarın xüsusiyyətlərini, bacarıq dəstini və ya xidməti təhlükə altına almaq üçün hansı ssenarilərdən istifadə edə biləcəyini profilləşdirməyə yönəldilir.
- Əsas diqqət proqramın dizaynına yönəldilir
- Əsas diqqət sadəcə proqram koduna yönəldilir
- Diqqət qurulan proqram təminatına və dizayn, kodlaşdırmasında hansı zəifliklərin təqdim olunacağına yönəldilir

264. Aktiv mərkəzli yanaşma necə izah olunur?

- √ Əsas diqqət qorunmağa ehtiyacı olan sistemə və ya proqram təminatına həvalə edilmiş aktivlərə (proqram tərəfindən işlənmiş məlumatlar) yönəldilir
- Diqqət qurulan proqram təminatına və dizayn, kodlaşdırmasında hansı zəifliklərin təqdim olunacağına yönəldilir
- Əsas diqqət təcavüzkarın xüsusiyyətlərini, bacarıq dəstini və ya xidməti təhlükə altına almaq üçün hansı ssenarilərdən istifadə edə biləcəyini profilləşdirməyə yönəldilir.
- Əsas diqqət proqramın dizaynına yönəldilir
- Əsas diqqət sadəcə proqram koduna yönəldilir

265. Aşağıdakılardan hansı təhdid modelləşdirilməsinə yanaşma hesab olunur?

- Sadəcə hücum mərkəzli yanaşma
- Aktiv mərkəzli və Hücum mərkəzli yanaşma
- Proqram mərkəzli, Aktiv mərkəzli yanaşma
- √ Proqram mərkəzli, Aktiv mərkəzli və Hücum mərkəzli yanaşma
- Sadəcə Proqram mərkəzli yanaşma

266. Təhdid modelləşdirilməsi yanaşmaları neçə qrupa bölünür?

- 4
- 10
- 5
- √ 3
- 2

267. Xakerlərin yoxlama-yanılma yolu ilə şifrələri həll etmək üçün istifadə etdiyi bir rəqəmsal və kriptoloji hücum üsuludur?

- √ Brute - Force
- İn-Band SQLİ
- Smishing
- SQL İnyeksiyası
- DDOS

268. Dictionary attack (Lüğət hücumu) - hansı kiber hücum növunə aiddir?

- √ Brute - Force

- İn-Band SQLİ
- DDOS
- SQL İnyeksiyası
- Smishing

269. Paylanmış xidmətdən imtina hücumu aşağıdakılardan hansıdır?

- Vishing
- Brute-Force
- Qrupdankənar (Out-of-Band) hücumu
- İn-Band (Klassik) hücum
- √ DDOS

270. Aşağıdakılardan hansı Brute-Force hücum növləridir ?

- Qrupdankenar (Out-of-Band) SQLi və in - Band (klassik) hücum
- Lüğət hücumu və vishing
- smishing və vishing
- √ Lüğət hücumu və sadə kobud güc hücumu
- in-band (Klassik) SQLi və Lüğət hücumu

271. Brute-Force hücumu - ..... kiber hücum növüdür?

- İstifadəçini müxtəlif yollarla eyni olan, amma saxta hansısa sayta və ya digər resursa yönəldən hücum
- Verilənlər bazasında səhv mesajları yaratmağa səbəb olan hərəkətləri yerinə yetirən hücum
- Vahid HTTP cavabı almaq üçün verilənlər bazası tərəfindən yaradılan çoxsaylı seçilmiş ifadələri birləşdirən UNION SQL operatorundan istifadə edən hücum
- √ Güclü məlumat axının təsiri ilə e-poçt, sosial şəbəkə və s. hesab şifrələrinin qırılmasına kömək edən hücum
- Səsin avtomatik simuliyasiyası texnologiyasından istifadə olunan hücum

272. SQL inyeksiya neçə alt kateqoriyadan ibarətdir?

- 5
- 4
- 2
- 6
- √ 3

273. Verilənlər bazası fəaliyyətinin monitorinqi və məlumat itkisinin qarşısının alınması vasitələrinə nəzarət etmək üçün hansı nəzarətdən istifadə edilir?

- Profilaktik nəzarət
- Aktiv nəzarət
- Simmetrik nəzarət
- √ Detektiv nəzarət
- İnzibati nəzarət

274. Giriş, şifrələmə, tokenləşdirmə və maskalanmanı idarə etmək üçün hansı nəzarətdən istifadə edilir?

- Aktiv nəzarət
- Detektiv nəzarət
- İnzibati nəzarət
- √ Profilaktik nəzarət
- Simmetrik nəzarət

275. Verilənlər bazası üçün quraşdırma, dəyişiklik və konfiqurasiya idarəetməsini idarə etmək üçün hansı nəzarətdən istifadə edilir?

- Detektiv nəzarət
- Profilaktik nəzarət
- Aktiv nəzarət

- Simmetrik nəzarət
√ İnzibati nəzarət

276. Verilənlər bazasının əsas təhlükəsizlik növlərini seçin:
1.İdentifikasiya
2.Verilənlər Bazasının Şifrələnməsi
3.Ehtiyat verilənlər bazası
4.Fiziki Təhlükəsizlik
5.Tətbiq Təhlükəsizliyi

- 1,2,3
- 1,4,5
- 2,4,5
- 1,3,4,5
√ 1,2,3,4,5

277. Perimetr səviyyəsinə aşağıdakılardan hansı aiddir?

- Makalanma
- Girişə nəzarət siyahıları
- Tokenləşdirmə
√ Firewalllar
- Şifrələmə

278. Giriş səviyyəsinə aşağıdakılardan hansı aiddir?

- Firewalllar
- Tokenləşdirmə
- Makalanma
√ Girişə nəzarət siyahıları
- Şifrələmə

279. Verilənlər bazası səviyyəsinə aşağıdakılardan hansı aiddir?

- Girişə nəzarət siyahıları
- Virtual şəxsi şəbəkələr
- Firewalllar
√ Şifrələmə
- İcazələr

280. Verilənlər bazası səviyyəsinə aşağıdakılardan hansı aiddir?

- Girişə nəzarət siyahıları
- Virtual şəxsi şəbəkələr
- Firewalllar
√ Maskalanma
- İcazələr

281. Aşağıdakılardan hansı ddos hücum növüdür?

- Appsec FAQ
- Bonets
- İn-band SQLi
√ SYN Flood
- Out-of-Band SQLİ)

282. Aşağıdakılardan hansı ddos hücum növüdür?

- Live CD
√ ICMP (Ping) Flood
- WebScarab

- Bonets
- Credential stuffing

283. Aşağıdakılardan hansı ddos hücum növüdür?

- Bonets
- Hybrid brute force attack
- Credential stuffing
- √ UDP Flood
- WebScarab

284. Aşağıdakılardan hansı ddos hücum növüdür?

- Bonets
- LAPSE
- WebScarab
- Credential stuffing
- √ Volumetric attacks

285. Aşağıdakılardan hansı ddos hücum növüdür?

- Credential stuffing
- İn-band SQLi
- Password Dpraying
- √ Protocol attack
- Bonets

286. Aşağıdakılardan hansı brute force hücum növü deyil?

- √ IP Null attack
- Bonets
- Credential stuffing
- Hybrid brute force attack
- Password Dpraying

287. Aşağıdakılardan hansı brute force hücum növü deyil?

- Hybrid brute force attack
- Credential stuffing
- Password Dpraying
- Bonets
- √ WebGoat

288. Aşağıdakılardan hansı brute force hücum növü deyil?

- Credential stuffing
- Bonets
- Password Dpraying
- √ Whaling attack
- Hybrid brute force attack

289. Aşağıdakılardan hansı brute force hücum növü deyil?

- Bonets
- Hybrid brute force attack
- Credential stuffing
- Password Dpraying
- √ Ping Flood

290. Aşağıdakılardan hansı brute force hücum növü deyil?

√ CharGEN Flood
• Bonets
• Credential stuffing
• Hybrid brute force attack
• Password Dpraying

291. Aşağıdakılardan hansı brute force hücum növüdür?

• Appsec FAQ
• WebScarab
• Smurf attack
• Session attack
√ Bonets

292. Aşağıdakılardan hansı brute force hücum növüdür?

• Session attack
• LAPSE
√ Credential stuffing
• Error-based
• WebScarab

293. Aşağıdakılardan hansı təhdidlərin modelləşdirməsi yanaşmasıdır?

• Səlahiyyələrin verilməsi
• İdarəetmə mərkəzli
• Konfiqurasiyanın idarə edilməsi
√ Hücumçu mərkəzli
• Qeyr-aktiv mərkəzli

294. Aşağıdakılardan hansı təhdidlərin modelləşdirməsi yanaşmasıdır?

• Qeyr-aktiv mərkəzli
• İdarəetmə mərkəzli
• Səlahiyyələrin verilməsi
√ Aktiv mərkəzli
• Konfiqurasiyanın idarə edilməsi

295. Aşağıdakılardan hansı təhdidlərin modelləşdirməsi yanaşmasıdır?

• Səlahiyyələrin verilməsi
• Konfiqurasiyanın idarə edilməsi
• Qeyr-aktiv mərkəzli
• İdarəetmə mərkəzli
√ Proqram mərkəzli

296. Aşağıdakılardan hansı brute force hücum növüdür?

• IP Null attack
• Whaling attack
√ Password Dpraying
• CharGEN Flood
• Smurf attack

297. Aşağıdakılardan hansı brute force hücum növüdür?

• Ping Flood
• Error-based
• IP Null attack

√ Dictionary attack
• Session attack

298. Aşağıdakılardan hansı hücum mərkəzli yanaşmadır?

• Əsas diqqət qorunmağa ehtiyacı olan sistemə və ya proqram təminatına həvalə edilmiş aktivlərə (proqram tərəfindən işlənmiş məlumatlar) yönəldilir
√ Əsas diqqət təcavüzkarın xüsusiyyətlərini, bacarıq dəstini və ya xidməti təhlükə altına almaq üçün hansı ssenarilərdən istifadə edə biləcəyini profilləşdirməyə yönəldilir.
• Əsas diqqət sadəcə proqram koduna yönəldilir
• Əsas diqqət proqramın dizaynına yönəldilir
• Diqqət qurulan proqram təminatına və dizayn, kodlaşdırmasında hansı zəifliklərin təqdim olunacağına yönəldilir

299. Aktiv mərkəzli yanaşma dedikdə nə nəzərdə tutulur?

• Diqqət qurulan proqram təminatına və dizayn, kodlaşdırmasında hansı zəifliklərin təqdim olunacağına yönəldilir
√ Əsas diqqət qorunmağa ehtiyacı olan sistemə və ya proqram təminatına həvalə edilmiş aktivlərə (proqram tərəfindən işlənmiş məlumatlar) yönəldilir
• Əsas diqqət sadəcə proqram koduna yönəldilir
• Əsas diqqət proqramın dizaynına yönəldilir
• Əsas diqqət təcavüzkarın xüsusiyyətlərini, bacarıq dəstini və ya xidməti təhlükə altına almaq üçün hansı ssenarilərdən istifadə edə biləcəyini profilləşdirməyə yönəldilir.

300. SQL İnyeksiyasının növləri hansı variantda düzgün verilmişdir?

• İn-Band (Klassik), Qrupdankənar (Out-of-band) SQL inyeksiyası
√ İn-Band (Klassik), İnferensial (Kor), Qrupdankənar (Out-of-band) SQL inyeksiyası
• Brute-Forse, DDOS
• MS SQL, MySQL
• Vishing, Smishing

301. Aşağıdakılardan hansı Autentifikasiya anlayışını izah edir?

• Təhlükəsiz proqram təminatının hazırlanması prosesinin təşkilidir
√ Subyekt tərəfindən təqdim edilmiş eyniləşdirmə məlumatlarının həqiqiliyinin yoxlanması prosesidir
• İnformasiya mühitində dövlətin, fiziki və hüquqi şəxslərin qorunmasının vəziyyətidir
• Proqram təminatının ilkin qəbulu (installyasiyası) və cari icrasının təhlükəsiz təşkilidir
• Susmaya görə təhlükəsizlik rejiminin qoşulmasıdır

302. Simple brute force attack (Sadə kobud güc hücumu) - hansı kiber hücum növunə aiddir?

• SQL İnyeksiyası
√ Brute - Force
• İn-Band SQLİ
• FDCS
• DDOS

303. Siyasi, kommersiya, reklam və digər növ məlumatları kütləvi və anonim şəkildə istədiyi yerə göndərə bilən xüsusi proqrama ..... deyilir.

• Smishing
√ SPAM
• Brute-Force
• DDOS
• Vishing

304. Klassik SQL inyeksiyası (İn-band SQLi) necə izah olunur?

• Təcavüzkar serverə məlumat yükü göndərir və onun strukturu haqqında daha çox öyrənmək üçün serverin reaksiyasını və davranışını müşahidə edir.
√ Təcavüzkar hücumlarına başlamaq və nəticələrini toplamaq üçün eyni rabitə kanalından istifadə edir.

- Təcavüzkar bu hücum formasını yalnız veb proqram tərəfindən istifadə edilən verilənlər bazası serverində müəyyən funksiyalar işə salındıqda həyata keçirə bilər.
- Təcavüzkar proqramdan nəticə qaytarmağı tələb edən verilənlər bazasına SQL sorğusu göndərir. Nəticə sorğunun doğru və ya yalan olmasından asılı olaraq dəyişir.
- Hücumçu verilənlər bazasına SQL sorğusu göndərir ki, bu da verilənlər bazasını reaksiya verməzdən əvvəl (bir neçə saniyə ərzində) gözləməyə məcbur edir.

305. Kor SQL inyeksiyası (İnferensial SQLi- Blind) aşağıdakılardan hansıdır?

- Bu texnika vahid HTTP cavabı almaq üçün verilənlər bazası tərəfindən yaradılan çoxsaylı seçilmiş ifadələri birləşdirən UNION SQL operatorundan istifadə edir.
- Hücumçu verilənlər bazasına SQL sorğusu göndərir ki, bu da verilənlər bazasını reaksiya verməzdən əvvəl (bir neçə saniyə ərzində) gözləməyə məcbur edir.
- √ Təcavüzkar serverə məlumat yükü göndərir və onun strukturu haqqında daha çox öyrənmək üçün serverin reaksiyasını və davranışını müşahidə edir
- Təcavüzkar proqramdan nəticə qaytarmağı tələb edən verilənlər bazasına SQL sorğusu göndərir.Nəticə sorğunun doğru və ya yalan olmasından asılı olaraq dəyişir.
- Təcavüzkar verilənlər bazasında səhv mesajları yaratmağa səbəb olan hərəkətləri yerinə yetirir

306. Error-based SQLi aşağıdakılardan hansıdır?

- Hücumçu verilənlər bazasına SQL sorğusu göndərir ki, bu da verilənlər bazasını reaksiya verməzdən əvvəl (bir neçə saniyə ərzində) gözləməyə məcbur edir.
- √ Təcavüzkar verilənlər bazasında səhv mesajları yaratmağa səbəb olan hərəkətləri yerinə yetirir
- Təcavüzkar serverə məlumat yükü göndərir və onun strukturu haqqında daha çox öyrənmək üçün serverin reaksiyasını və davranışını müşahidə edir
- Bu texnika vahid HTTP cavabı almaq üçün verilənlər bazası tərəfindən yaradılan çoxsaylı seçilmiş ifadələri birləşdirən UNION SQL operatorundan istifadə edir.
- Təcavüzkar proqramdan nəticə qaytarmağı tələb edən verilənlər bazasına SQL sorğusu göndərir.Nəticə sorğunun doğru və ya yalan olmasından asılı olaraq dəyişir.

307. Zamana əsaslanan SQLİ dedikdə nə nəzərdə tutulur?

- Təcavüzkar proqramdan nəticə qaytarmağı tələb edən verilənlər bazasına SQL sorğusu göndərir.Nəticə sorğunun doğru və ya yalan olmasından asılı olaraq dəyişir.
- √ Hücumçu verilənlər bazasına SQL sorğusu göndərir ki, bu da verilənlər bazasını reaksiya verməzdən əvvəl (bir neçə saniyə ərzində) gözləməyə məcbur edir.
- Təcavüzkar serverə məlumat yükü göndərir və onun strukturu haqqında daha çox öyrənmək üçün serverin reaksiyasını və davranışını müşahidə edir
- Bu texnika vahid HTTP cavabı almaq üçün verilənlər bazası tərəfindən yaradılan çoxsaylı seçilmiş ifadələri birləşdirən UNION SQL operatorundan istifadə edir.
- Təcavüzkar verilənlər bazasında səhv mesajları yaratmağa səbəb olan hərəkətləri yerinə yetirir

308. Boolean SQLi dedikdə nə nəzərdə tutulur?

- Təcavüzkar verilənlər bazasında səhv mesajları yaratmağa səbəb olan hərəkətləri yerinə yetirir
- √ Təcavüzkar proqramdan nəticə qaytarmağı tələb edən verilənlər bazasına SQL sorğusu göndərir.Nəticə sorğunun doğru və ya yalan olmasından asılı olaraq dəyişir.
- Bu texnika vahid HTTP cavabı almaq üçün verilənlər bazası tərəfindən yaradılan çoxsaylı seçilmiş ifadələri birləşdirən UNION SQL operatorundan istifadə edir.
- Hücumçu verilənlər bazasına SQL sorğusu göndərir ki, bu da verilənlər bazasını reaksiya verməzdən əvvəl (bir neçə saniyə ərzində) gözləməyə məcbur edir.
- Təcavüzkar serverə məlumat yükü göndərir və onun strukturu haqqında daha çox öyrənmək üçün serverin reaksiyasını və davranışını müşahidə edir

309. Klassik SQL inyeksiyası (İn-band SQLi) neçə alt kateqoriyadan ibarətdir?

- 3
- √ 2
- 6
- 4
- 5

310. Texnoloji səhvlər neçə alt kateqoriyadan ibarətdir?

- 10
√ 12
- 6
- 4
- 5

311. Verilənlər bazası səviyyəsinə aşağıdakılardan hansı aiddir?

- Virtual şəxsi şəbəkələr
- Firewalllar
√ Tokenləşdirmə
- İcazələr
- Girişə nəzarət siyahıları

312. Aşağıdakılardan hansı verilənlər bazasının təhlükəsizliyinin səviyyələrindən hesab olunur?

- Tətbiq səviyyəsi
- Sahə səviyyəsi
- Test səviyyəsi
- Yoxlama səviyyəsi
√ Giriş səviyyəsi

313. Verilənlər bazasının təhlükəsizliyinin neçə səviyyəsi mövcuddur?

- 2
- 6
√ 3
- 5
- 4

314. Aşağıdakılardan hansı verilənlər bazasının təhlükəsizliyinə aiddir?

- Qarşılaşa biləcək təhlükələrdən xəbərdar olmaq, işin davamlılığını təmin etmək, baş verə biləcək hər cür problemdə itkiləri minimuma endirmək, hər bir şəraitdə fərdlərin və qurumların aktivlərinin yalnız əlçatanlığını qorumaq məqsədi aiddir
- Təhlükəsiz lahiyəhələndirmə prinsiplərinin tətbiqi, yəni mümkün hücumların nəzərə alınması və onların aradan qaldırılması üsulların reallaşdırılması aiddir
- Təhlükəsiz proqram təminatının hazırlanması prosesinin təşkili aiddir
√ Verilənlər bazasının özünün, onun ehtiva etdiyi verilənlərin, verilənlər bazası idarəetmə sisteminin və ona daxil olan müxtəlif proqramların qorunması aiddir.
- Qarşılaşa biləcək təhlükələrdən xəbərdar olmaq, işin davamlılığını təmin etmək, baş verə biləcək hər cür problemdə itkiləri minimuma endirmək, hər bir şəraitdə fərdlərin və qurumların aktivlərinin yalnız məxfiliyini qorumaq məqsədi aiddir

315. Aşağıdakılardan hansı verilənlər bazasının təhlükəsizliyinə aiddir?

- Qarşılaşa biləcək təhlükələrdən xəbərdar olmaq, işin davamlılığını təmin etmək, baş verə biləcək hər cür problemdə itkiləri minimuma endirmək, hər bir şəraitdə fərdlərin və qurumların aktivlərinin yalnız əlçatanlığını qorumaq məqsədi aiddir
- Təhlükəsiz proqram təminatının hazırlanması prosesinin təşkili aiddir
- Təhlükəsiz lahiyəhələndirmə prinsiplərinin tətbiqi, yəni mümkün hücumların nəzərə alınması və onların aradan qaldırılması üsulların reallaşdırılması aiddir
√ Verilənlər bazasının təhlükəsizliyinə verilənlər bazasının məxfiliyini, bütövlüyünü və əlçatanlığını yaratmaq və qorumaq üçün nəzərdə tutulmuş alətlər, nəzarət vasitələri və tədbirlər sırasına aiddir
- Qarşılaşa biləcək təhlükələrdən xəbərdar olmaq, işin davamlılığını təmin etmək, baş verə biləcək hər cür problemdə itkiləri minimuma endirmək, hər bir şəraitdə fərdlərin və qurumların aktivlərinin yalnız məxfiliyini qorumaq məqsədi aiddir

316. "Diqqət qurulan proqram təminatına və dizayn, kodlaşdırma və ya quraşdırma inteqrasiyasında hansı zəifliklərin və zəifliklərin təqdim olunacağına yönəldilir" bu fikir hansı təhdid modelləşdirilməsinə yanaşma üsulunu izah edir?

- Passiv mərkəzli
- Sistem mərkəzli
- Aktiv mərkəzli
- Hücumçu mərkəzli
√ Proqram mərkəzli

317. Aşağıdakı kateqoriyalardan hansı autentifikasiya üsullarını təsvir etmək üçün istifadə edilmir?

- token və ya smart kart
- PIN və ya parol
- sahib olduğunuz bir şey
- səs və ya üz tanıma kimi biometrik məlumatlar
- √ xoşladığınız bir şey

318. Hansı şəbəkə təhlükəsizliyi identifikasiyası metodu bir giriş sessiyasında və ya əməliyyatda istifadə edilmək üçün proqram təminatı və ya aparat əsaslı ola bilər?

- Tək giriş
- multifaktorlu
- Ağıllı kart
- √ Birdəfəlik parol
- İki faktorlu autentifikasiya

319. Aşağıdakı autentifikasiya rejimlərindən hansı daha təhlükəsizdir?

- √ Windows Autentifikasiyası
- SQL Server Autentifikasiyası
- Qarışıq rejim
- Kerberos
- qeyd olunanların hamısı

320. SQL Server nümunəsi ____ üzərində işləyərkən Windows Authentication Mode mövcud deyil.

- Windows 10
- qeyd olunanların hamısı
- √ Windows 98
- Windows 8
- Windows 7

321. Düzgün ifadəni göstərin.

- Doğrulama təşkilatlara yalnız autentifikasiya edilmiş istifadəçilərə və ya proseslərə qorunan resurslara giriş əldə etmək icazəsi verməklə şəbəkələrini təhlükəsiz saxlamağa imkan verir
- Doğrulama və avtorizasiya bir-biri ilə sıx bağlıdır
- √ hamısı düzgündür
- Kerberos internet kimi etibarsız şəbəkə üzərindən etibarlı hostlar arasında xidmət sorğularının autentifikasiyası üçün protokoldur.
- Autentifikasiya müştərinin şəxsiyyətinin yoxlanılması prosesidir

322. Təşkilatınız öz işçilərinə şəxsi şifrələmə açarı və xüsusi şəxsi məlumatlarla kodlanmış nişanlar təqdim edir. Kodlaşdırma təşkilatın şəbəkəsinə girişi təmin etmək üçün istifadə olunur. Hansı növ autentifikasiya metodundan istifadə olunur?

- Multifaktor
- Kerberos
- Biometrika
- √ Ağıllı kart
- Token

323. Məlumat mərkəzinə giriş əldə etməzdən əvvəl barmağınızı cihazda sürüşdürməlisiniz. Bu hansı autentifikasiya növüdür?

- Tokenlər
- Tək giriş
- Multifaktor
- ikili giriş
- √ Biometrika

324. Autentifikasiya və avtorizasiyanın ən təhlükəsiz üsulu hansıdır?

- Chap
- RADIUS
- TACACS
- √ Kerberos
- LDAP

325. Aşağıdakı autentifikasiya sistemlərindən hansı KeyDistribution Center-dən istifadə edir?

- Secutiry tokens
- Vpn
- Sertifikatlar
- √ Kerberos
- CHAP

326. Tətbiq səviyyəsinin firewallları həmçinin necə adlanır?

- ikinci nəsil firewalllar
- birinci nəsil firewalllar
- beşinci nəsil firewallar
- dördüncü nəsil firewalllar
- √ üçüncü nəsil firewalllar

327. Vəziyyətli Çoxlaylı firewalllar həmçinin necə adlanır?

- dördüncü nəsil firewalllar
- beşinci nəsil firewallar
- birinci nəsil firewalllar
- üçüncü nəsil firewalllar
- √ ikinci nəsil firewalllar

328. Packet filtering firewalllar həmçinin necə adlanır?

- dördüncü nəsil firewalllar
- beşinci nəsil firewallar
- ikinci nəsil firewalllar
- üçüncü nəsil firewalllar
- √ birinci nəsil firewalllar

329. Tətbiq səviyyəli şlyuz firewallları xüsusi _____ üçün şəbəkəni qoruyur.

- Şəbəkə səviyyəsinin protokolu
- Fiziki səviyyəsinin protokolu
- Sessiya səviyyəsinin protokolu
- Təqdimat səviyyəsinin protokulu
- √ Tətbiq səviyyəsinin protokolu

330. Dövrə səviyyəli(Circuit level) şlyuz firewallları OSI modelinin hansı qatında quraşdırılmışdır?

- Şəbəkə səviyyə(Network layer)
- Tətbiq səviyyə(Application layer)
- Təqdimat səviyyə(Presentation layer)
- √ Sessiya səviyyəsi(Session layer)
- Fiziki səviyyə(Physical layer)

331. Paket filterləmə firewalları şəbəkədə necə işləyir?

- çox böyük kompleks
- çox mürəkkəb

- çox sadə
- büyük
- √ daha kiçik

332. Paket filtrləmə firewallının bir üstünlüyü nədən ibarəttir?

- çox sürətli
- daha az sürətli
- daha az mürəkkəb
- daha səmərəli
- √ daha az xərc tələb edir

333. ACL nə deməkdir?

- Access Control Logs
- Any Control List
- √ Access Control List
- Anti Control List
- Access Condition List

334. Nə paket filterləmə Firewall faydalarını müəyyən edir?

- protokollar
- ünvanlar
- limanlar
- √ access control list
- siyasətlər

335. Firewall aşağıdakı hücumlardan hansını qoruyur?

- Shoulder surfing
- √ Denial of Service (DOS)
- Dumpster diving
- Surfing
- Phishing

336. Aşağıdakılardan hansı Software Firewall deyil ?

- Windows Firewall
- √ Linksys Firewall
- Microsoft Firewall
- Endian Firewall
- Outpost Firewall pro

337. ……. internet bağlantısı istifadə edərək quraşdırılan programdır və ya əməliyyat sistemləri ilə standart olarak gəlir

- Dövlət təftişi Firewall
- Hardware Firewall
- Microsoft Firewall
- Program təminatı
- √ Software Firewall

338. ….. cihaz və internetə qoşulan şəbəkə arasında bağlanan təhlükəsizlik divarı növüdür.

- Microsoft Firewall
- √ Hardware Firewall
- Dövlət təftişi Firewall
- Proqram təminatının təhlükəsizlik divarı
- NİDS

339. Firewalların neçə növü ola bilər?

- 1
- √ 3
- 4
- 2
- 5

340. Proxy server nədir?

- Veb-serverlərə girişi yükləmək üçün serverlərin qarşısında yerləşdirilir
- √ URL, domen, media və s. Kimi veb məzmun sorğularını filtrləyir
- Veb-serverlərə girişi qorumaq üçün serverlərin qarşısında yerləşdirirlir
- Veb-serverlərə girişi gizlətmək üçün serverlərin qarşısında yerləşdirilir
- Kompüteri açığ portlar üçünyoxlayır

341. Proxy serverə sahib olmaq üçün optimal yer haradadır?

- İki özəl şəbəkə arasında
- Heç bir serverdə
- Bütün serverlərdə
- √ şəxsi şəbəkə ilə içtimai şəbəkə arasında
- İki ictimai şəbəkə arasında

342. Daxili və xarici ünvanlar arasında tərcüməni həyata keçirən və əvvəllər əldə edilmiş veb səhifələri gələcəkdə daha tez təmin edə bilməsi üçün keşləyən vasitəçi kimi çıxış edən nədir?

- İP ünvan
- NAT server
- Dövlət maşın müfəttişi
- √ proxy server
- NİDS

343. Firewall nə edə bilməz?

- Proqramları silir
- Verilənləri bloklayır
- Hansı proqramların internetə daxil ola biləcəyini müəyyənləşdirir
- Hakerlərin kompüterinizə daxil olmasını dayandırır
- √ viruslardan qoruya bilmir

344. Aşağıdakılardan hansı firwallın əsas funksiyasıdır?

- Yapışdırılır
- Silinir
- √ monitorinq
- Hərəkət edir
- Kopyalanır

345. Firewall nədir?

- Bütün məzmunu bloklayır
- Verilənləri yaddaşa verir
- Virusları quraşdırır
- Sizə SD kartları verir
- √ hakerlərin qarşısını alır

346. Hansı Kerberos versiyası daha uzun bilet ömrünə malikdir?

- Versiya 6

- Versiya 4
- Yuxarıdakıların heç biri
- Versiya 3
√ Versiya 5

347. KDC(açar paylama mərkəzi) yanaşmasında istifadəçinin hər biri KDC ilə hansı növ açara malikdir?

- İkili açar
- Şəxsi Açar
- Açıq Açar
√ Paylaşılan Simmetrik Açar
- Heç biri

348. Kerberos Windows tərəfindən _ üçün populyar olaraq istifadə olunur.

- Avtorizasiya
- Giriş
- Şifrələmə
- Doğrulama
√ İdentifikasiyası

349. Kerberosda TGS:

- heç biri
- Token Granting Server
- Ticket Getting Server
√ Ticket Granting Server
- Token Getting Server

350. KDC nə deməkdir?

- Key Data Centre
- heç biri
- Centre of key data
√ Key Distribution Centre
- Centre for Key Distribution

351. Secure Development Lifecycle (SDL) (Təhlükəsiz İnkişaf Həyat Dövrü (SDL)) dedikdə nə nəzərdə tutulur?

- Təhlükəsiz lahiyəhələndirmə prinsiplərinin tətbiqi, yəni mümkün hücumların nəzərə alınması və onların aradan qaldırılması üsulların reallaşdırılması
- Proqram müəllifləri ilə müntəzəm olaraq əlaqə saxlanması, təhlükəsizlik üzrə yeni buraxılış, zəmanət, tövsiyə və məsləhətlərin əldə olunması
- Proqram təminatının ilkin qəbulu (installyasiyası) və cari icrasının təhlükəsiz təşkili
√ Təhlükəsiz proqram təminatının hazırlanması prosesinin təşkili
- Susmaya görə təhlükəsizlik rejiminin qoşulması

352. Secure by Default - dedikdə nə nəzərdə tutulur?

- Proqram müəllifləri ilə müntəzəm olaraq əlaqə saxlanması, təhlükəsizlik üzrə yeni buraxılış, zəmanət, tövsiyə və məsləhətlərin əldə olunması
- Təhlükəsiz proqram təminatının hazırlanması prosesinin təşkili
- Təhlükəsiz lahiyəhələndirmə prinsiplərinin tətbiqi, yəni mümkün hücumların nəzərə alınması və onların aradan qaldırılması üsulların reallaşdırılması
√ Susmaya görə təhlükəsizlik rejiminin qoşulması
- Proqram təminatının ilkin qəbulu (installyasiyası) və cari icrasının təhlükəsiz təşkili

353. Secure in Deployment (Yerləşdirmədə təhlükəsizlik) anlayışı aşağıdakılardan hansıdır?

- Susmaya görə təhlükəsizlik rejiminin qoşulması

- Proqram müəllifləri ilə müntəzəm olaraq əlaqə saxlanması, təhlükəsizlik üzrə yeni buraxılış, zəmanət, tövsiyə və məsləhətlərin əldə olunması
- Təhlükəsiz proqram təminatının hazırlanması prosesinin təşkili
- Təhlükəsiz lahiyəhələndirmə prinsiplərinin tətbiqi, yəni mümkün hücumların nəzərə alınması və onların aradan qaldırılması üsulların reallaşdırılması
- √ Proqram təminatının ilkin qəbulu (installyasiyası) və cari icrasının təhlükəsiz təşkili

354. Aşağıdakılardan hansı OWASP təhlükəsiz kodlaşdırma təcrübələrindəndir?

- √ Kriptoqrafik Təcrübələr
- Detektiv nəzarət
- İnzibati nəzarət
- Makalanma
- Tokenləşdirmə

355. Aşağıdakılardan hansı OWASP təhlükəsiz kodlaşdırma təcrübələrindəndir?

- Makalanma
- İnzibati nəzarət
- Detektiv nəzarət
- √ Parolun idarə olunması
- Tokenləşdirmə

356. Aşağıdakılardan hansı güclü parol hesab olunur?

- 12345
- vtL28
- 12122010
- √ Owasp2022))!!
- Vahid12

357. Aşağıdakılardan hansı Mobil təhlükəsizlik həllinin ümumi elementlərinə aiddir?

- Simmetrik nəzarət
- İnzibati nəzarət
- Detektiv nəzarət
- √ VPN ilə nəzarət
- Aktiv nəzarət

358. Etibarsız istifadəçi tərəfindən verilən məlumat server tərəfindən yaradılan HTTP cavabına daxil edildikdə baş verir - bu hansı XSS növüdür?

- Reflected XSS
- Müştəri XSS
- DOM XSS
- Stored XSS
- √ Server XSS

359. XSS inyeksiyasının neçə növü var?

- 5
- 4
- 3
- √ 2
- 7

360. Zərərli skriptlərin etibarlı veb-saytlara yeridildiyi inyeksiya növü aşağıdakılardan hansıdır?

- XML inyeksiyası
- İnferensial SQLİ

- Out of band SQLİ
- √ XSS inyeksiyası
- SQL inyeksiyası

361. Tampering (Saxtakarlıq) anlayışı necə izah olunur?

- İstifadəçi adı və parol kimi başqa istifadəçinin etimadnaməsinə qeyri-qanuni daxil olmaq və istifadə etmək məqsədi daşıyan təhdid hərəkəti
- Giriş icazəsi olmayan faylı oxumaq və ya ötürülən məlumatları oxumaq üçün təhdid əməliyyatı
- Veb serveri müvəqqəti olaraq əlçatmaz və ya yararsız etmək kimi etibarlı istifadəçilərə girişi rədd etmək məqsədi
- √ Verilənlər bazasındakı məlumatlar və İnternet kimi açıq şəbəkə üzərindən iki kompüter arasında tranzitdə olan məlumatların dəyişdirilməsi kimi davamlı olaraq məlumatları zərərli şəkildə dəyişdirmək
- Qadağan edilmiş əməliyyatları izləmək imkanı olmayan bir sistemdə qeyri-qanuni əməliyyatlar həyata keçirmək məqsədi

362. Deserializasiya nədir?

- obyektin vəziyyətinin bayt axınına çevrilməsi mexanizmidir
- obyektin vəziyyətinin bit axınına çevrilməməsi mexanizmidir
- obyektin vəziyyətinin bit axınına çevrilməsi mexanizmidir
- √ Java obyektini yenidən yaratmaq üçün bayt axınının istifadə edildiyi əks prosesdir
- obyektin vəziyyətinin bayt axınına çevrilməməsi mexanizmidir

363. Serializasiya nədir?

- obyektin vəziyyətinin bit axınına çevrilməsi mexanizmidir
- Java obyektini yenidən yaratmaq üçün bayt axınının istifadə edildiyi əks prosesdir
- obyektin vəziyyətinin bayt axınına çevrilməməsi mexanizmidir
- √ obyektin vəziyyətinin bayt axınına çevrilməsi mexanizmidir
- obyektin vəziyyətinin bit axınına çevrilməməsi mexanizmidir

364. ObjectOutputStream sinfində obyekti sıradan çıxarmaq üçün hansı metod istifadə edilir?

- writeObject()
- √ readObject()
- java.io.Serializable
- java.Serializable
- deleteObject()

365. ObjectOutputStream sinfində Obyektin seriallaşdırılması üçün hansı metod istifadə edilir?

- readObject()
- java.Serializable
- java.io.Serializable
- √ writeObject()
- deleteObject()

366. Java obyektini serializasiya etmək üçün istifadə olunan interfeys aşağıdakılardan hansıdır?

- C.io.Serializable
- io.Serializable
- java.Serializable
- java.Serializa
- √ java.io.Serializable

367. Spoofing (Saxtakarlıq) anlayışı aşağıdakı variantlardan hansında düzgün izah edilmişdir?

- Giriş icazəsi olmayan faylı oxumaq və ya ötürülən məlumatları oxumaq üçün təhdid əməliyyatı
- Veb serveri müvəqqəti olaraq əlçatmaz və ya yararsız etmək kimi etibarlı istifadəçilərə girişi rədd etmək məqsədi
- √ İstifadəçi adı və parol kimi başqa istifadəçinin etimadnaməsinə qeyri-qanuni daxil olmaq və istifadə etmək məqsədi daşıyan təhdid hərəkəti

- Qadağan edilmiş əməliyyatları izləmək imkanı olmayan bir sistemdə qeyri-qanuni əməliyyatlar həyata keçirmək məqsədi
- Verilənlər bazasındakı məlumatlar və İnternet kimi açıq şəbəkə üzərindən iki kompüter arasında tranzitdə olan məlumatların dəyişdirilməsi kimi davamlı olaraq məlumatları zərərli şəkildə dəyişdirmək

368. Aşağıdakılardan hansı Risklərin Sıralanması Metodologiyası anlayışıdır?

- Repudiation
- STRIDE
- Reproducibility (Təkrarlanma qabiliyyəti)
- Damage potential
- √ DREAD

369. Aşağıdakılardan hansı Təhdidlərin Təsnifatı Metodologiyası anlayışıdır?

- Tampering
- Repudiation
- DREAD
- Spoofing
- √ STRIDE

370. Təhdidlərin Təsnifatı Metodologiyası necə adlanır?

- Tampering
- DREAD
- Spoofing
- √ STRIDE
- Repudiation

371. Tətbiqə təsir edə biləcək təhdidlərdən hesab olunur?

- Host və Proqram təhdidləri
- Yalnız Proqrm təhdidləri
- Kod təhdidləri
- √ Şəbəkə, Host və Proqram təhdidləri
- Yalnız şəbəkə təhdidləri

372. Təhlükəsiz proqramlarin işlənib-hazırlanması və istifadə olunmasının əsas prinsipləri neçə qrupa bölünür?

- 6
- 3
- 4
- 2
- √ 5

373. Secure in Design - dedikdə nə nəzərdə tutulur?

- Proqram müəllifləri ilə müntəzəm olaraq əlaqə saxlanması, təhlükəsizlik üzrə yeni buraxılış, zəmanət, tövsiyə və məsləhətlərin əldə olunması
- √ Təhlükəsiz lahiyəhələndirmə prinsiplərinin tətbiqi, yəni mümkün hücumların nəzərə alınması və onların aradan qaldırılması üsulların reallaşdırılması
- Susmaya görə təhlükəsizlik rejiminin qoşulması
- Təhlükəsiz proqram təminatının hazırlanması prosesinin təşkili
- Proqram təminatının ilkin qəbulu (installyasiyası) və cari icrasının təhlükəsiz təşkili

374. Kompüter virusu kiçik proqramdır ki, bunlar:

- kompüterinizin aparatını məhv edəcək
- √ istəmədən başqa kompüterlərə ötürə bilərsiniz
- kompüterinizdən silinə bilməz
- hamısı doğrudur

- yalnız e-poçt vasitəsilə ötürülə bilər

375. Fayllarınızı icazəsiz girişdən qoruya bilərsiniz:

- yalnız dostlarınıza və ailənizə tez-tez ehtiyat nüsxələrini çıxararaq parollarınızı bilməyə imkan verir
- √ güclü parol seçmək və onu müntəzəm olaraq dəyişdirmək
- yaddaşda saxlamaqla
- heç bir halda
- heç vaxt kitabxana kimi ictimai yerdə kompüterlərdən istifadə etmə

376. Hakerlər:

- kompüterinizin aparatını məhv edəcək
- √ bəzən parolları oğurlayırlar ki, onlar onlayn hesabınıza daxil ola bilsinlər
- bir anda yalnız bir parol oğurlaya bilər
- heç biri
- nadir hallarda şəxsi məlumatları oğurlaya bilirlər

377. Kompüterdən Sui-istifadə Qanununa əsasən, aşağıdakılar qanunsuzdur:

- icazəsiz başqasının kompüter fayllarına baxın
- √ bunların hamısı
- başqasının kompüter fayllarında məlumatları icazəsiz dəyişdirmək
- bunların heç biri
- başqa cinayət törətmək niyyəti ilə icazəsiz başqasının kompüter fayllarına baxmaq

378. Siz özünüzü spam və ya saxta e-poçtlardan qoruya bilərsiniz:

- müxtəlif növ saxta e-poçtlardan xəbərdar olmaq
- spam filtrindən istifadə etməklə
- şübhəli olduğunuz linklərə heç vaxt klikləməyin
- √ bunların hamısı
- bunların heç biri

379. Başqasının kompüter fayllarına icazəsiz giriş əldə etmək kimi tanınır:

- müəllif hüquqlarının pozulması
- √ hacking
- məlumat oğurluğu
- variantların hamısı doğrudur
- virus hücumu

380. Xaricdə ilişib qaldıqlarını və bütün pullarının oğurlandığını söyləyən bir dostunuzdan ümidsiz kömək yalvarışı alırsınız. Siz etməlisiniz:

- e-poçta cavab verin
- √ e-poçtu silin
- e-poçtu ortaq bir dosta yönləndirin
- variantların hamısı doğrudur
- bir az pul göndər

381. Hacking aşağıdakı hallarda qanunsuzdur:

- Məlumatların Mühafizəsi Qanunu
- √ Kompüterdən Sui-istifadə Aktı
- Sağlamlıq və Təhlükəsizlik Qanunu
- variantların hamısı doğrudur
- Müəlliflik hüququ haqqında qanun

382. E-poçtdakı keçidin sizi risksiz, məsələn, banka məxsus olan orijinal veb-sayta aparıb-götürməyəcəyini aşağıdakılarla müəyyən edə bilərsiniz:

- e-poçtun silinməsi
√ klikləmədən linkə işarə edir
- linkə klikləməklə
- variantların hamısı doğrudur
- e-poçta cavab vermək

383. Müəyyən bir sayt üçün istifadəçi adınızı və şifrənizi əldə etməyə çalışan saxta e-poçt adətən:

- adınızla müraciət edin
√ orijinal görünən loqosu olan başlığa sahib olun
- dostdan gəldiyi görünür
- variantların hamısı doğrudur
- böyük məbləğdə pul təklif edin

384. Əgər tanınmış şirkətdən e-poçt məktubu alırsınızsa, lakin onun adı göndərənin ünvanında səhv yazılıbsa, aşağıdakıları etməlisiniz:

- orijinal olub olmadığını yoxlamaq üçün e-poçtdakı linkə klikləyin
√ mümkün fişinq dələduzluğu kimi bildirin
- yoxlamaq üçün e-poçtu dostunuza göndərin
- variantların hamısı yanlışdır
- səhvi göstərərək cavab verin

385. Fişinq e-poçtu hansıdır?

- almadığınız mallar üçün ödəniş tələb edir
√ fırıldaqçı veb-saytın linkinə tıklamağa təşviq edir
- təhqiredici və hədələyici dil ehtiva edir
- variantların hamısı doğrudur
- sizə maraq göstərmədiyiniz məhsulları təklif edir

386. Autentifikasiya Tətbiqlərinin məqsədlərinə aiddir:

- Hücum məqsədlidir
√ Tətbiq səviyyəsində autentikasiya(application-level authentication) və rəqəmsal imzaların dəstəklənməsi üçün hazırlanmışdır
- Monitorinq üçün hazırlanmışdır
- Dörd tərəflidir
- Tanınır

387. X.509 üç alternativ autentifikasiya proseduruna hansı aiddir?

- Dördtərəfli autentikasiya
√ Birtərəfli autentikasiya
- Təkpəncərəli autentikasiya
- Cütpəncərəli autentikasiya
- Beştərəfli autentikasiya

388. X.509 neçə alternativ autentifikasiya prosedurunu ehtiva edir?

- 1
√ 3
- 4
- 2
- 5

389. Aşağıdakılardan hansı Sertifikatlaşmaya aiddir?

- bəzi məlumat bazasını saxlayan paylanmış serverlər
√ saxtalaşdırıla bilmədiyi üçün sertifikatlar ictimai kataloqda(public directory) yerləşdirilə bilər
- açıq açar sertifikatlarını saxlaya bilər

- autentifikasiya xidmətləri üçün çərçivəni müəyyən edir
- CCITT X.500 kataloq xidməti standartlarının bir hissəsidir

390. Aşağıdakılardan hansı X.509 autentikasiya xidmətinə aiddir?

- 1912-ci ildə yaradılıb
√ CCITT X.500 kataloq xidməti standartlarının bir hissəsidir
- Biletin ömrü
- Kerberos server
- Realmlərarası identifikasiya

391. Aşağıdakılardan hansı Kerberos v4 və Kerberos v5 arasındakı fərqlərə aiddir?

- Açıq açar sertifikatlarını saxlaya bilər
√ Mesaj bayt sıralaması
- Sertifikatı yalnız CA dəyişdirə bilər
- Bəzi məlumat bazasını saxlayan paylanmış serverlər
- Autentifikasiya xidmətləri üçün çərçivəni müəyyən edir

392. Aşağıdakılardan hansı Kerberos v4 və Kerberos v5 arasındakı fərqlərə aid deyil?

- Realmlərarası identifikasiy
√ Açıq açar sertifikatlarını saxlaya bilər
- Biletin ömrü
- Mesaj bayt sıralaması
- Doğrulama yönləndirilməsi

393. Aşağıdakılardan hansı Kerberos v4 və Kerberos v5 arasındakı fərqlərə aiddir?

- açıq açar sertifikatlarını saxlaya bilər
√ internet protokolundan asılılıq
- sertifikatı yalnız CA dəyişdirə bilər
- bəzi məlumat bazasını saxlayan paylanmış serverlər
- autentifikasiya xidmətləri üçün çərçivəni müəyyən edir

394. Aşağıdakılardan hansı Kerberos v4-ə aiddir?

- autentifikasiya xidmətləri üçün çərçivəni müəyyən edir
- CA-ya çıxışı olan istənilən istifadəçi ondan istənilən sertifikatı əldə edə bilər
√ tək bir aləmlə məhdudlaşır
- saxtalaşdırıla bilmədiyi üçün sertifikatlar ictimai kataloqda(public directory) yerləşdirilə bilər

395. Aşağıdakılardan hansı Kerberos v4-ə aiddir?

- açıq açar sertifikatlarını saxlaya bilər
√ mühit çatışmazlıqlarını aradan qaldırır
- CA-ya çıxışı olan istənilən istifadəçi ondan istənilən sertifikatı əldə edə bilər
- saxtalaşdırıla bilmədiyi üçün sertifikatlar ictimai kataloqda(public directory) yerləşdirilə bilər
- autentifikasiya xidmətləri üçün çərçivəni müəyyən edir

396. Kerberos Version 5 nə zaman hazırlanmışdır?

- 1899-cu ilin əvvəlində
- 1975-ci ilin əvvəlində
√ 1990-cı illərin ortalarında
- 1995-cu ilin sonlarında
- 1957-ci ilin sonlarında

397. Hansı aşağı təhlükəsizlik təmin edir?

- bunlardan heç biri
- Tətbiq səviyyəli firewall
- Təqdimat səviyyəli firewall
√ Packet Filtering firewall
- Şəbəkə səviyyəli firewall

398. İkinci nəsil firewallara hansı daxildir?

- Fiziki səviyyəli firewall
- Tətbiq səviyyəli firewall
- Təqdimat səviyyəli firewall
√ Vəziyyətli çoxlaylı firewall
- Sessiya səviyyəli firewall

399. Packet Filter Firewall filterləri harada yerləşir?

√ Şəbəkə, köçürmə səviyyəsi
- Fiziki səviyyə
- Təqdimat səviyyə
- Sessiya səviyyə
- Tətbiq səviyyə

400. Proxy firewall filterləri harada yerləşir?

- Təqdimat səviyyə
- Fiziki səviyyə
- Sessiya səviyyə
√ Tətbiq səviyyəsi
- Şəbəkə səviyyə

401. Aşağıdakılardan hansı firewallın komponentlərindən deyil?

√ NET
- proxy
- router
- gateway
- packet filter

402. Birinci nəsil firewallara hansı daxildir?

- Fiziki səviyyəli firewall
- Sessiya səviyyəli firewall
- Tətbiq səviyyəli firewall
- Təqdimat səviyyəli firewall
√ Packet Filtering firewall

403. OSI modelinin hansı qatında paket süzgəcindən keçən firewalllar həyata keçirilir?

- Sessiya səviyyə
- Fiziki səviyyə
- Tətbiq səviyyə
√ Şəbəkə səviyyəsi
- Təqdimat səviyyə

404. Paket filtrləmə firewallları nəyin tərkibində yerləşdirilib?

- Repeater
- Switch
- Hub
√ Router

- Gateway

405. Firewall _____ olmalıdır ki, qoruduğu şəbəkə ilə mütənasib şəkildə böyüyə bilsin.

- Ölçüləbilən
- İri
- Möhkəm
- Sürətli
- √ Genişlənən

406. Hansı firewall digər üç növ firewallın birləşməsidir?

- Tətbiq səviyyəli gateway
- Dövrə səviyyəli gateway
- Paket filterləmə
- Təqdimat səviyyəli gateway
- √ Vəziyyətli çoxqatlı başlanğıc

407. Aşağıdakılardan hansı güclü parol hesab olunur?

- software23
- Windows01
- 4567006
- √ Ctrl24!
- Break9

408. Aşağıdakılardan hansı güclü parol hesab olunur?

- case12
- Program12
- 5615022006
- √ Python:B!
- com48

409. Aşağıdakılardan hansı güclü parol hesab olunur?

- Qwerty1234
- 15022006
- √ 12LojI:D!
- Ali1999
- Qwerty1

410. Etibarsız istifadəçi tərəfindən təmin edilən data DOM-u təhlükəli JavaScript çağırışı ilə yeniləmək üçün istifadə edildikdə baş verir - bu hansı XSS növüdür?

- Reflected XSS
- √ Müştəri XSS
- DOM XSS
- Server XSS
- Stored XSS

411. Serializasiya vasitəsilə tərtibatçı hansı hərəkətləri yerinə yetirə bilər:
1) Veb xidmətindən istifadə edərək obyektin uzaq proqrama göndərilməsi
2) Bir obyektin bir domendən digərinə ötürülməsi
3) Obyektin JSON və ya XML sətri kimi firewall vasitəsilə ötürülməsi
4) Tətbiqlər arasında təhlükəsizliyin və ya istifadəçiyə məxsus məlumatın saxlanılması

- √ 1,2,3,4
- 2,3,4
- 1,2,3
- 3.40

- 1.30

412. "Mesaj qəbul edən proqram tərəfindən əldə edildikdə, xidmətin digər komponenti mesajla səyahət etmiş məlumatlardan istifadə edərək istifadəçi identifikatorunun autentifikasiyasını həyata keçirə bilər" - bu hansı xidmətin nümunəsidir?

√ İdentifikasiya və autentifikasiya
- Məlumatların bütövlüyü
- Məxfilik
- SAMM
- Məlumatların aydınlığı

413. "Mesaj qəbul edən proqram tərəfindən alındıqda yoxlanıla bilər. Bu yoxlama onun məzmununun göndərən proqram tərəfindən ilk növbədə növbəyə qoyulmasından sonra qəsdən dəyişdirilib-düzəliş edilmədiyini müəyyən edir" - bu hansı xidmətin nümunəsidir?

- Məxfilik
- SAMM
√ Məlumatların bütövlüyü
- Məlumatların aydınlığı
- İdentifikasiya və autentifikasiya

414. "Mesaj proqram tərəfindən növbəyə qoyulduqda şifrələnə və qəbul edən proqram tərəfindən əldə edildikdə şifrəsi açıla bilər" - bu hansı xidmətin nümunəsidir?

- Məlumatların aydınlığı
- İdentifikasiya və autentifikasiya
- Məlumatların bütövlüyü
- SAMM
√ Məxfilik

415. Aşağıdakılardan hansı güclü parol hesab olunur?

- 12122010
- 12345
- Vahid12
- vtL28
√ SaMmOwAs^^))1

416. Aşağıdakılardan hansı güclü parol hesab olunur?

- Qwerty1
- 15022006
- Qwerty1234
√ QdYuV:D!
- Ali1999

417. "Giriş icazəsi olmayan faylı oxumaq və ya ötürülən məlumatları oxumaq üçün təhdid əməliyyatı" - bu hansı STRİDE növüdür?

- Spoofing (Saxtakarlıq)
- Denial of Service (Xidmətin rədd edilməsi)
- Repudiation (İnkar və ya Rədd edilmə)
√ Information Disclosure (İnformasiyanın Açıqlanması)
- Tampering (Saxtakarlıq)

418. "Təhdid, veb serveri müvəqqəti olaraq əlçatmaz və ya yararsız etmək kimi etibarlı istifadəçilərə girişi rədd etmək məqsədi daşıyır." - bu hansı STRİDE növüdür?

- Tampering (Saxtakarlıq)
- Information Disclosure (İnformasiyanın Açıqlanması)
- Spoofing (Saxtakarlıq)
- Repudiation (İnkar və ya Rədd edilmə)
√ Denial of Service (Xidmətin rədd edilməsi)

419. "Təhdid hərəkəti qadağan edilmiş əməliyyatları izləmək imkanı olmayan bir sistemdə qeyri-qanuni əməliyyatlar həyata keçirmək məqsədi daşıyırdı" - bu hansı STRİDE növüdür?

- Denial of Service (Xidmətin rədd edilməsi)
- Spoofing (Saxtakarlıq)
- Tampering (Saxtakarlıq)
- Information Disclosure (İnformasiyanın Açıqlanması)
- √ Repudiation (İnkar və ya Rədd edilmə)

420. Təhdid modelləşdirməsinə neçə yanaşma mövcuddur?

- 2
- 5
- 4
- √ 3
- 10

421. Mobil təhlükəsizlik üzrə ən yaxşı təcrübələri seçin:
1) Aydın siyasət və prosesləri qurulması
2) Parolun qorunması
3) Biometrik göstəricilərdən istifadə edilməsi

- 1.30
- 1.20
- 2.30
- 3
- √ 1,2,3

422. "Bitcoin və ya Ethereum kimi kriptovalyutaları hasil etmək üçün təşkilatın hesablama gücündən və ya fərdin kompüter gücündən onların xəbəri olmadan istifadə edərək cihazın emal qabiliyyətini və effektivliyini azaldır" bu hansı zərərli proqram formasıdır?

- Smishing
- Brute-Force
- DDOS
- √ Cryptojacking
- Vishing

423. "İstifadəçi autentifikasiya edildikdən və proqramdan istifadə etdikdən sonra digər təhlükəsizlik tədbirləri həssas məlumatların kibercinayətkar tərəfindən görünməsindən və hətta istifadəsindən qoruya bilər" bu fikir hansı tətbiq təhlükəsizliyi xüsusiyyətinə aiddir?

- Autentifikasiya
- Qeydiyyat
- Giriş və təhlükəsizlik testi
- √ Şifrələmə
- Avtorizasiya

424. Aşağıdakılardan hansı tətbiq təhlükəsizliyinin xüsusiyyətlərindən hesab edilir?

- Proqram müəllifləri ilə müntəzəm olaraq əlaqə saxlanması, təhlükəsizlik üzrə yeni buraxılış, zəmanət, tövsiyə və məsləhətlərin əldə olunması
- Susmaya görə təhlükəsizlik rejiminin qoşulması prosesi
- Proqram təminatının ilkin qəbulu (installyasiyası) və cari icrasının təhlükəsiz təşkili
- √ Şifrələmə prosesi
- Təhlükəsiz proqram təminatının hazırlanması prosesinin təşkili

425. Tətbiq təhlükəsizliyi xüsusiyyətlərini seçin:
1) Autentifikasiya
2) Avtorizasiya
3) Şifrələmə
4) Giriş və proqram təhlükəsizliyi testi

- 1.20

- 1,2,4
- 3.40
- √ 1,2,3,4
- 1,2,3

426. Aşağıdakılardan hansı tətbiq təhlükəsizliyinin xüsusiyyətlərindən hesab edilir?

- √ Doğrulama(autentifikasiya) prosesi
- Proqram təminatının ilkin qəbulu (installyasiyası) və cari icrasının təhlükəsiz təşkili
- Susmaya görə təhlükəsizlik rejiminin qoşulması prosesi
- Təhlükəsiz proqram təminatının hazırlanması prosesinin təşkili
- Proqram müəllifləri ilə müntəzəm olaraq əlaqə saxlanması, təhlükəsizlik üzrə yeni buraxılış, zəmanət, tövsiyə və məsləhətlərin əldə olunması

427. Aşağıdakılardan hansı tətbiq təhlükəsizliyinin xüsusiyyətlərindən hesab edilir?

- Susmaya görə təhlükəsizlik rejiminin qoşulması prosesi
- Təhlükəsiz proqram təminatının hazırlanması prosesinin təşkili
- Proqram müəllifləri ilə müntəzəm olaraq əlaqə saxlanması, təhlükəsizlik üzrə yeni buraxılış, zəmanət, tövsiyə və məsləhətlərin əldə olunması
- √ Avtorizasiya prosesi
- Proqram təminatının ilkin qəbulu (installyasiyası) və cari icrasının təhlükəsiz təşkili

428. İki faktorlu autentifikasiya tətbiqi aşağıdakılardan hansıdır?

- Visual Studio
- Meta Authenticator
- Google İndentificator
- √ Google Authenticator
- QEMU

429. İki faktorlu autentifikasiya tətbiqi aşağıdakılardan hansıdır?

- QEMU
- Meta Authenticator
- Microsoft İndentificator
- √ Microsoft Authenticator
- Visual Studio

430. Aşağıdakılardan hansı güclü parol hesab olunur?

- 12122010
- vtL28
- 12345
- Vahid12
- √ StRiDe:((

431. Aşağıdakılardan hansı güclü parol hesab olunur?

- Qwerty1
- Ali1999
- √ UneC:)!!
- 15022006
- Qwerty1234

432. Aşağıdakılardan hansı güclü parol hesab olunur?

- vtL28
- 12345
- Vahid12

√ vtL2845!
• 12122010

433. Aşağıdakılardan hansı güclü parol hesab olunur?

• 15022006
• Qwerty1234
• Qwerty1
• Ali1999
√ QvtL1566!

434. Tampering (Saxtakarlıq) hesab olunur?

• Veb serveri müvəqqəti olaraq əlçatmaz və ya yararsız etmək kimi etibarlı istifadəçilərə girişi rədd etmək məqsədi
• Giriş icazəsi olmayan faylı oxumaq və ya ötürülən məlumatları oxumaq üçün təhdid əməliyyatı
• İstifadəçi adı və parol kimi başqa istifadəçinin etimadnaməsinə qeyri-qanuni daxil olmaq və istifadə etmək məqsədi daşıyan təhdid hərəkəti
• Qadağan edilmiş əməliyyatları izləmək imkanı olmayan bir sistemdə qeyri-qanuni əməliyyatlar həyata keçirmək məqsədi
√ Verilənlər bazasındakı məlumatlar və İnternet kimi açıq şəbəkə üzərindən iki kompüter arasında tranzitdə olan məlumatların dəyişdirilməsi kimi davamlı olaraq məlumatları zərərli şəkildə dəyişdirmək

435. Spoofing (Saxtakarlıq) hesab olunur?

• Verilənlər bazasındakı məlumatlar və İnternet kimi açıq şəbəkə üzərindən iki kompüter arasında tranzitdə olan məlumatların dəyişdirilməsi kimi davamlı olaraq məlumatları zərərli şəkildə dəyişdirmək
• Giriş icazəsi olmayan faylı oxumaq və ya ötürülən məlumatları oxumaq üçün təhdid əməliyyatı
√ İstifadəçi adı və parol kimi başqa istifadəçinin etimadnaməsinə qeyri-qanuni daxil olmaq və istifadə etmək məqsədi daşıyan təhdid hərəkəti
• Veb serveri müvəqqəti olaraq əlçatmaz və ya yararsız etmək kimi etibarlı istifadəçilərə girişi rədd etmək məqsədi
• Qadağan edilmiş əməliyyatları izləmək imkanı olmayan bir sistemdə qeyri-qanuni əməliyyatlar həyata keçirmək məqsədi

436. Risklərin Sıralanması Metodologiyası necə adlanır?

• Repudiation
• Reproducibility (Təkrarlanma qabiliyyəti)
• Damage potential
• STRIDE
√ DREAD

437. Məlumat mərkəzinə giriş əldə etməzdən əvvəl barmağınızı cihazda sürüşdürməlisiniz. Bu hansı autentifikasiya növüdür?

• Tək giriş
√ Biometrika
• Tokenlər
• ikili giriş
• Multifaktor

438. Autentifikasiya və avtorizasiyanın ən təhlükəsiz üsulu hansıdır?

• Kerberos
√ TACACS
• LDAP
• Chap
• RADIUS

439. Aşağıdakı autentifikasiya sistemlərindən hansı KeyDistribution Center-dən istifadə edir?

• Secutiry tokens
√ Kerberos
• Sertifikatlar
• Vpn

- CHAP

440. Kerberos aşağıdakılardan hansını istifadə edir?

- The Faraday cage, Port 389
- √ Biletlərin paylanması xidməti, doğrulama xidməti+
- Doğrulama xidməti, The Faraday
- Doğrulama xidməti
- Port 389, Doğrulama xidməti

441. İstifadəçiyə şəbəkəyə daxil olmaq üçün iki maddə tələb olunur. Bu iki maddə nədir?

- Avtorizasiya və identifikasiya
- √ Doğrulama və avtorizasiya
- Parol və autentifikasiya
- İdentifikasiya və doğrulama
- İdentifikasiya və autentifikasiya+

442. Hansı identifikasiya metodu aşağıdakıları əhatə edir: giriş sorğusu, dəyər cavabını şifrələyir, server, çağırış, şifrləmə nəticələrini müqayisə edir və ya uğursuzluq?

- Sertifikatlaşdırma
- √ Security Tokens
- CHAP
- autentifikasiya
- Kerberos

443. Hansı autentifikasiya mexanizmi təhlükəsiz mühitdə daha yaxşı işləyir?

- TACACS+, çünki bu, uzaqdan giriş identifikasiyası xidmətidir
- √ TACACS+, çünki müştəri-server danışıqları dialoqlarını şifrələyir
- RADIUS, çünki o, uzaqdan giriş identifikasiyası xidmətidir
- RADIUS autentifikasiya, avtorizasiya və mühasibat xidmətlərini təmin edən müştəri server sistemidir
- RADIUS, çünki o, müştəri-server parollarını şifrələyir

444. Şəbəkənizə giriş əldə etmək üçün istifadəçilər barmaq izi və istifadəçi adı və parol təqdim etməlidirlər. Bu hansı autentifikasiya modelidir?

- Biometrik
- √ Multifaktor
- domen girişi
- birdəfəlik parol
- tək giriş

445. Aşağıdakılardan hansı iki autentifikasiya mexanizmi fiziki olaraq sahib olduğunuz bir şeyi tələb edir?

- Sertifikat, USB flash drive
- √ Smart kart, USB flash drive
- istifadəçi adı və parol, Smart kart
- Sertifikat, Smart kart
- USB flash drive, istifadəçi adı və parol

446. İstifadəçilərin autentifikasiyası zamanı aşağıdakılardan hansı ümumi meyar deyil?

- bildiyi nəyi isə
- √ bəyənilən nəyi isə
- özünün tərkib hissəsi olan nəyi isə
- sahib olduğu nəyi isə
- etdiyi nəyi isə

447. Kerberos protokolu harada istifadə olunmur?

- Samba
- √ CHAP
- Active Directory
- Posix autentifikasiyası
- NFS

448. Autetifikasiya haqqında aşağıdakılar yanlışdır?

- CHAP istifadəçi adı və parolları şifrələdiyi üçün PAP-dan daha təhlükəsizdir
- √ MS-CHAPv1 müştəri və serverin qarşılıqlı autentifikasiyasına qadirdir
- RADIUS autentifikasiya, avtorizasiya və mühasibat xidmətlərini təmin edən müştəri server sistemidir
- Autentifikasiya hansısa varlığın doğruladığı bir məlumat parçasının doğruluğunun təsdiq edilməsidir
- PAP etibarsızdır, çünki istifadəçi adı və parollar aydın mətn kimi göndərilir

449. Aşağıdakılardan hansı istifadəçinin domen resursuna daxil ola bilməsi üçün istifadəçinin atmalı olduğu son addımdır?

- autentifikasiya
- √ Icazə
- doğrulama
- cavabdehlik
- yoxlama

450. Hansı şəbəkə təhlükəsizliyi identifikasiyası metodu bir giriş sessiyasında və ya əməliyyatda istifadə edilmək üçün proqram təminatı və ya aparat əsaslı ola bilər?

- icazə
- smart kart
- √ birdəfəlik parol
- iki faktorlu autentifikasiya
- tək giriş

451. Ümumi tək girişli identifikasiya konfiqurasiyalarının iki nümunəsi hansılardır?

- kerberos əsasında, multifaktorlu autentifikasiya
- √ smart kart əsasında, kerberos əsasında
- multifaktorlu autentifikasiya, biometrika əsasnda
- biometrika əsasında, kerberos əsasında
- biometrika əsasında, smart kart əsasında

452. Aşağıdakılardan hansı şəxsin şəxsiyyətinin yoxlanılmasıdır?

- Cavabdehlik
- √ Autentifikasiya
- Parol
- smart kart
- Icazə

453. Sağlamlıq və Təhlükəsizlik qaydaları işəgötürəndən tələb edir:

- klaviaturadan istifadə üçün bilək dayaqları təmin edin
- √ kompüterdə işi planlaşdırın ki, tez-tez fasilələr olsun
- yuxarıdakıların hamısı
- heç biri
- eynəklərə ehtiyacı olan işçilər üçün, əgər kompüterdən istifadə edərək çox vaxt sərf edirlərsə, onlara pul ödəyin

454. Şəxsi məlumatları saxlayan təşkilatlara icazə verilir:

- məlumatları digər təşkilatlara satmaq

√ şəxslərin müəyyən edilə biləcəyi məlumatları çıxardıqdan sonra məlumatları tədqiqat məqsədləri üçün satmaq
• yuxarıdakıların heç biri
• hamısı
• məlumatları əbədi olaraq saxlayın

455. "Məlumat toplama vasitəsi" aşağıdakılardır:

• bir virus növü
• parolları oğurlamaq üçün istifadə edilən qeyri-qanuni proqram
• bir növ daxiletmə qurğusu
√ şəxslər haqqında məlumat toplamaq üçün istifadə olunan proqram təminatı
• hamısı

456. Aşağıdakı məlumatlardan hansı məktəbdə saxlanıldıqda "şəxsi məlumatlar" hesab olunur:

• məktəbin e-poçt ünvanı məktəbdəki şagirdlərin sayı
√ müəyyən bir şagirdin məktəbə qoşulduğu il
• bunların heç biri
• hamısı
• keçən il gcse üzrə şagirdlərin əldə etdikləri orta faiz a*-c qiymətləri

457. Fərdi məlumatların saxlanması ilə bağlı qanunda deyilir ki, əgər şirkət şəxsi məlumatlara sahibdirsə, o:

• məlumatları təhlükəsiz saxlayın
√ məlumatları dəqiq və yeni saxlayın
• yuxarıdakıların hamısı
• bunların heç biri
• insanlara onlar haqqında hansı məlumatların saxlanıldığını görməyə imkan verir

458. Əgər kimsə şirkətin onlar haqqında qeyri-dəqiq məlumatlara malik olduğundan şübhələnirsə:

• onlar haqqında hansı məlumatların saxlanıldığını öyrənmək üçün istənilən vaxt daxil ola bilərlər
√ onlar şirkətin onlar haqqında hansı məlumatlara malik olduğunu görmək hüququna malikdirlər
• onlar məlumatları düzəldə bilməyəcəklər
• şirkətdən üzr istəməlidirlər
• məlumatları özləri düzəldə bilərlər

459. Qanunda deyilir:

• yalnız dövlət təşkilatları sizin haqqınızda şəxsi məlumatları saxlaya bilər
√ təşkilat tərəfindən saxlanılan şəxsi məlumatlar hakerlərdən qorunmalıdır
• şəxsi məlumatlar ildə ən azı bir dəfə yenilənməlidir
• bütün şəxsi məlumatlar şifrələnməlidir
• informasiya azaddır

460. Fərdi məlumatların toplanması və saxlanması qaydalarını müəyyən edən Qanun belə adlanır:

• Cinayətdən Sui-istifadə Aktı
√ Məlumatların Qorunması Qanunu
• Fərdi Məlumatlar Qanunu
• Sağlamlıq və Təhlükəsizlik Qanunu
• Ağır cinayətlər

461. Aşağıdakılardan hansı supermarketin kompüter sistemində kimsə haqqında saxlanıla bilən "şəxsi məlumatlar"dır?

• Onların əlaqə nömrəsi
√ Bunların hamısı
• Keçən il supermarketdə xərclədikləri məbləğ
• Onların loyallıq kartı nömrəsi
• Onların ünvanı

462. Məktəb kimi bir təşkilat sizin haqqınızda şəxsi məlumatları saxlayır. Təşkilat:

- məlumatlarınızı öz kompüterində saxlamaq üçün sizdən icazə istəməlidir
√ Data Protection Registrar-da qeydiyyatdan keçməlidir
- yerli hakimiyyət orqanlarında qeydiyyatdan keçməlidir
- brauzer yaddaşından istifadə etməlidir
- getdiyiniz zaman məlumatları silməlisiniz

463. Aşağıdakılardan hansı Castin Smit adlı biri üçün "güclü" paroldur?

- Justin Smith
√ softcatsears-7
- JustinS
- SmithJ1
- Justin 123456

464. Parollarınızın tamamilə təhlükəsiz olduğuna əmin ola bilərsiniz, əgər:

- onlar ən azı 8 simvol uzunluğundadır
√ bunların hamısı
- bütün onlayn hesablarınız üçün müxtəlif parollardan istifadə edirsiniz
- parollarınızı brauzer yaddaşında saxlamırsınız
- onları müntəzəm olaraq dəyişdirirsiniz

465. Parol seçərkən aşağıdakıları etməlisiniz:

- ev heyvanınızın adı kimi yadda saxlamaq asan bir şey istifadə edin
√ sizin üçün bir şey ifadə edən hərf və rəqəmlərin birləşməsindən istifadə edin, lakin başqa heç kim deyil
- ingilis lüğətində olmayacaq xarici sözdən istifadə edin
- hamısını
- unutduğunuz halda bütün parollarınızı kompüterinizdə bir faylda saxlayın

466. Kompüterinizin zərərli proqrama yoluxmaması üçün aşağıdakıları etməməlisiniz:

- tanımadığınız insanların e-poçtlarını açın
√ Qeyri-qanuni saytlardan musiqi və ya proqram təminatı yükləyin
- şəxsi məlumatlarınızı sosial şəbəkələrdə yerləşdirin
- bunların heç biri
- e-poçt qoşmalarını açın

467. Aşağıdakılardan hansı doğrudur?

- Viruslar e-poçt vasitəsilə yayıla bilməz
√ Viruslar kompüterinizdə olan bütün məlumatları tamamilə məhv edə bilər
- Bunlardan heç biri
- Bunlardan hamısı
- Antivirus proqramı həmişə virusun kompüterinizə hücumunun qarşısını alacaq

468. Kompüter virusu ola bilər:

- fayllarınızın üzərinə yazın və məlumatlarınızı korlayın
√ bunların hamısı
- çox yaddaş istifadə edin və kompüterinizi yavaşlatın
- bunların heç biri
- kompüterinizdən vacib məlumatları oğurlayın

469. Bunlardan hansı kompüterinizdə zərərli proqram əlamətidir?

- Siz saxta e-poçt alırsınız

√ Əsas səhifəniz gözlənilmədən dəyişdi
• Brauzeriniz sizi daha yeni versiyaya yeniləmək üçün xəbərdarlıq edir
• bunların heç biri
• Brauzeriniz pop-up pəncərəni blokladığını sizə xəbər verir

470. "Malware" budur:

• bir virus növü
√ razılığı olmadan quraşdırılmış arzuolunmaz proqram
• proqram xətası
• bunların heç biri
• virusları aşkar etmək üçün təhlükəsizlik proqramı

471. Virus növüdür:

√ Boot-sector Virusu
• Tarix Virusu
• Display Virusu
• Office Virusu
• Wifi Virusu

472. Stealth Virus nədir?

• imza aşkarlanmasının qarşısını almaq üçün hər yeni hostla mutasiyaya uğrayır
• kodlarının bir hissəsi kimi özünü icra edilə bilən fayllara ilişdirir
• əsas yaddaşda qalıq əməliyyat sisteminin bir hissəsi kimi yerləşdirilir
√ virus Skanlama proqramlarından gizlətmək üçün açıq şəkildə hazırlanmışdır
• diskin yükləmə sektorunu yoluxdurur və əməliyyat sistemi işə salındıqda yayılır

473. Makro viruslara aiddir:

• Makro sənəd açılanda işləyə bilməz
• Sənədlərə yoluxa bilmir
• Məktubları redaktə edə bilmir
• Faylları silə bilməz
√ Platformadan asılı deyil

474. Antivirus Yanaşmalarına hansılar aiddir?

• Fəaliyyət tələləri
• Skanerlər
• Heuristik Skanerlər
√ Bütün cavablar aiddir
• Tam Təminatlı

475. Antivirus yanaşmaları neçə nəsildən ibarətdir?

• 7
• 8
• 3
• 5
√ 4

476. Müdaxilənin aşkar edilməsi üçün istifadə olunan tədbirlərə aid deyil:

• Sonuncu girişdən bəri vaxt
• Girişdə şifrə çatmazlığı (uğursuz/yanlış şifrə sayı)
• Gün və zamana görə giriş tezliyi
• Müxtəlif yerlərdə girişin tezliyi
√ Trojandan istifadə

477. Müdaxilənin aşkar edilməsi üçün istifadə olunan tədbirlərə aiddir:

- Defolt(susmaya görə) şifrələri yoxlamaq
- Trojandan istifadə
- √ Sonuncu girişdən bəri keçən vaxt
- "Suid" olan Shell proqramına daxil olmaq
- İstifadəçinin hobbiləri, ailə adları, ad günü və s. sınamaq

478. Şəbəkəyə müdaxilənin mərhələlərindən biri deyil:

- Şəbəkəni skan etmək
- √ Antivirusu aktif saxlamaq
- IRC (Internet Relay Chat) istifadə etmək
- "Suid" olan Shell proqramına daxil olmaq
- Açıq portlara qarşı "Exploit" skriptlərini işə salmaq

479. Şəbəkəyə müdaxilənin mərhələlərindən biridir:

- Antivirusu aktif saxlamaq
- √ Şəbəkəni skan etmək
- Autentifikasiya
- Dinamik IP ünvanından istifadə etmək
- Tətbiqlərə gələn yenilənmələri həyata keçirmək

480. Aşağıdakılardan hansı müdaxilə texnikalarına aid deyil?

- Defolt(susmaya görə) şifrələri yoxlamaq
- √ Autentifikasiya
- İstifadəçinin hobbiləri, ailə adları, ad günü və s. haqqında məlumat toplamaq
- İstifadəçinin telefon nömrəsi, sosial təminat nömrəsi, küçə ünvanı və s. sınamaq
- Bütün qısa sözləri sınaqdan keçirmək

481. Aşağıda qeyd olunan səbəblərdən hansı insanların kompüter virusu yaratmasının səbəbini qane etmir?

- Tədqiqat məqsədi
- √ Müdafiə
- Şəxsiyyət oğurluğu
- İntiqam
- Pranklar

482. Onlardan hansı virusun yayılmasının ideal yolu deyil?

- Yoluxmuş vebsayt
- √ Rəsmi Antivirus CD -ləri
- USB-lər
- rəsmi olmayan oyunlar
- E -poçtlar

483. Kompüter _____ özünü başqa proqramlara kopyalayaraq özünü təkrarlayan zərərli koddur.

- Proqram
- √ Virus
- qurd
- kod
- tətbiq

484. Aşağıdakılardan hansı virus növü deyil?

- Boot sector

√ Trojan
- Multipartite
- Direct Action
- Polymorphic

485. Kompüter virusunun _____ növü var.

- 5
√ 10
- 12
- 15
- 7

486. Neçənci ildə isə İPsec rəsmi olaraq təsdiq olunub?

- 2000
√ 1995
- 1998
- 1990
- 1997

487. IPSec-in tunel modelində tunelin mənası budur -

- IPSec paketləri digər trafikdən qorunan təhlükəsiz kabeldən keçir.
√ qorunan IP paketləri başqa bir IP başlığının (xarici başlıq) içərisindədir və bir çox IP paketlərinin xarici başlıqları daxili IP paketlərinin keçdiyi tunel divarı kimi görüntülənə bilər
- IPSec IP-ni əvəz edir və daha yüksək səviyyəli protokol paketləri (TCL, UDP) IP əvəzinə IPSec-in faydalı yüküdür.
- İPSec İP-ni əvəz etmir
- kabel elə bağlanıb ki, İP paketlərinin mühafizəsinə ehtiyac olmasın.

488. IPSec məxfiliyi (şifrələmədən istifadə etməklə, məsələn, 3DES), autentifikasiyanı (məlumatların mənşəyi və mesajın autentifikasiyası) və yenidən açarla təmin edir. Yenidən açarın mənası bunu nəzərdə tutur

- eyni açar təkrar istifadə olunur.
√ şifrələmə üçün eyni açardan istifadə edən çoxlu sayda paket, kriptoanalizdən istifadə edərək açarı çıxarmaq üçün rəqib tərəfindən toplana bilməz. Başqa sözlə, açar fasilələrlə dəyişdirilir.
- onun təsirini gücləndirmək üçün çoxlu şifrələmə raundlarından istifadə olunur.
- açarlar dəyişdirilmir
- bir neçə düymə eyni vaxtda istifadə olunur.

489. İnternet Protokolunda (IP), Başlıq Xətası Yoxlama Cəmi (HEC) hər hansı bir səhvin yoxlanılması üçün yeganə ölçüdür. Onun mövcudluğundan bunu deyə bilərik

- İP-də ən azı müəyyən təhlükəsizlik var.
√ IP məlumat sahəsinin etibarlılığı yoxdur, lakin başlıq var
- İP əlaqə yönümlü protokoldur.
- İP simsiz protokoldur
- IP əlaqəsiz protokoldur.

490. Doğrulama başlığı (AH) ilə kapsullaşdırılmış təhlükəsizlik yükü (ESP) arasındakı fərq ondan ibarətdir ki,

- ESP-nin faydalı yükü TLS, AH-ninki isə IP-dir
√ AH-də iki IP başlığı var, ESP isə yalnız bir
- AH faydalı yük kimi ESP ola bilməz
- AH-də bir İP başlıq var
- AH başlığı şifrələnir, ESP başlığı isə şifrələnmir

491. _____ rejimində IPSec orijinal IP başlığı daxil olmaqla bütün IP paketini qoruyur.

- Fiziki
- Heç biri

√ Tunnel
- Şəbəkə
- Nəqliyyat

492. İPSec _____ adlı SA dəstindən istifadə edir.

- SAB
√ SADB
- SAR
- heç biri
- SAD

493. IKE neçə protokola əsaslanır?

- 2
√ 3
- 5
- 1
- 4

494. _____ şəbəkə səviyyəsində paketin təhlükəsizliyini təmin etmək üçün IETF tərəfindən hazırlanmış protokollar toplusudur.

- SSL
√ İPSec
- Heç biri
- RSA
- PGP

495. _____ İP səviyyəsində paketlər üçün ya autentifikasiya, ya da şifrələmə və ya hər ikisini təmin edir.

- AH
√ ESP
- PGP
- RSA
- SSL

496. DNS serveri bu məlumatı vermək səlahiyyəti olmayan bir hostdan yanlış məlumatı qəbul etdikdə və istifadə etdikdə, o, _____ adlanır.

- DNS oğurlanması
√ DNS saxtakarlığı
- DNS icazəsi
- DNS kirayəsi
- DNS axtarışı

497. PGP, _____ adlı blok şifrəsindən istifadə edərək məlumatları şifrələyir.

- Şəxsi məlumatların şifrələmə alqoritmi
√ Beynəlxalq məlumat şifrələmə alqoritmi
- Lokal məlumatların şifrələnməsi alqoritmi
- Regional məlumatların şifrələnməsi alqoritmi
- İnternet məlumatlarının şifrələmə alqoritmi

498. Pretty Good Privacy (PGP) _____-da istifadə olunur

- Brauzer təhlükəsizliyi
√ Elektron poçtun təhlükəsizliyi
- WiFi təhlükəsizliyi
- Bluetooth təhlükəsizliyi
- FTP təhlükəsizliyi

499. Genişlənən autentifikasiya protokolu _____-da tez-tez istifadə olunan autentifikasiya çərçivəsidir.

- Simli metropoliten şəbəkəsi
- Simli şəxsi sahə şəbəkəsi
- Simli lokal şəbəkə
- √ Simsiz şəbəkələr
- Simli şəxsi local şəbəkə

500. Kompüter resursunu nəzərdə tutulan istifadəçilər üçün əlçatmaz etmək cəhdi _____ adlanır.

- Virus hücumu
- √ Xidmətdən imtina hücumu
- Botnet prosesi
- Polimorfizm
- Qurdların hücumu

501. WPA2 _____-da təhlükəsizlik üçün istifadə olunur

- Ethernet
- √ Wi-Fi
- E-poçt
- SİM
- Bluetooth

502. IP təhlükəsizliyinə hansı komponent daxildir?

- Doğrulama Başlığı (AH)
- √ Qeyd olunanların hamısı
- İnternet açarı mübadiləsi (IKE)
- Autentifikasiya ilə ESP
- Kapsülləşdirici Təhlükəsizlik Yükü (ESP)

503. n tunel rejimi, IPSec qoruyur _____

- IP başlığı
- √ Bütün IP paketi
- İP treyler
- İP şəbəkə
- IP yükü

504. IPSec _____ təhlükəsizliyi təmin etmək üçün yaradılıb.

- Nəqliyyat səviyyəsi
- √ Şəbəkə səviyyəsi
- Seans səviyyəsi
- Fiziki səviyyə
- Tətbiqi səviyyə

505. Genişlənən autentifikasiya protokolu _____-da tez-tez istifadə olunan autentifikasiya çərçivəsidir.

- Simli şəxsi sahə şəbəkəsi
- √ Simsiz şəbəkələr
- Simli metropoliten şəbəkəsi
- Simli şəxsi local şəbəkə
- Simli lokal şəbəkə

506. Kompüter resursunu nəzərdə tutulan istifadəçilər üçün əlçatmaz etmək cəhdi _____ adlanır.

- Virus hücumu

√ Xidmətdən imtina hücumu
• Botnet prosesi
• Polimorfizm
• Qurdların hücumu

507. WPA2 _____-da təhlükəsizlik üçün istifadə olunur

• Ethernet
√ Wi-Fi
• E-poçt
• SİM
• Bluetooth

508. IP təhlükəsizliyinə hansı komponent daxildir?

• Doğrulama Başlığı (AH)
√ Qeyd olunanların hamısı
• İnternet açarı mübadiləsi (IKE)
• Autentifikasiya ilə ESP
• Kapsülləşdirici Təhlükəsizlik Yükü (ESP)

509. Rəqəmsal imza tələb olunur:

• bütün e-poçt göndərişləri üçün
√ göndəricinin rabitədən imtina etməməsinə görə
• FTP əməliyyatı üçün
• heç biri
• və ya bütün DHCP server

510. Dinamik paket filtrləri firewall işləyən dördüncü nəsil firewalllardır

• TCP
√ TCP, UDP
• sessiya qatı
• URL
• UDP

511. Hash funksiyası tərəfindən yaradılmış həzm nə adlanır?

• autentifikasiya əlaqəsini dəyişdirmək
√ modifikasiya aşkarlama kodu
• mesajın autentifikasiya şifrəsi
• açar
• mesajın autentifikasiyasına nəzarət

512. Mesaj bütövlüyündə, təhlükəsiz hash alqoritmi 1(SHA-l) hash alqoritmləri neçə blokdan ibarət mesajdan n-bit mesaj həzmini yarada bilir?

• 1001
√ 512
• 2020
• 614
• 1510

513. Mesaj həzminin ….saxlanması lazımdır

• ictimai
√ gizli
• dogru
• simmetrik

- özəl

514. Aşağıdakılardan hansı Veb təhlükəsizliyi təhdidlərinə aiddir?

- modul
- √ Saytlar arası skript (XSS)
- logic bomb
- key
- firewall

515. Veb təhlükəsizliyi təhdidlərinə aid deyil

- kod enjeksiyonu
- √ computer scan
- SQL enjeksiyonu
- fişinq
- xidmətin rədd edilməsi

516. Veb təhlükəsizliyi təhdidlərinə aid deyil

- ransomware
- √ firewall
- kod enjeksiyonu
- viruslar və qurdlar
- SQL enjeksiyonu

517. Şəxsi şəbəkəyə və ya şəbəkədən icazəsiz girişin qarşısını almaq üçün nəzərdə tutulmuş sistem nə adlanır?

- computer scan
- √ firewall
- biotech
- virus
- digital scan

518. Aşağıdakılardan hansı məxfilik alqoritmindən istifadə edir?

- fayl şifrələməsi
- √ həm elektron məktublar, həm də fayl şifrələməsi
- elektron məktublar
- qəbuledici
- göndərən

519. Kompüter virusu nədir?

- heç biri
- freeware
- √ proqram təminatı(software)
- bacteria
- hardware

520. Faylı şifrələmənin əsas səbəbi nədir?

- ölçüsünü azaltmaq
- √ onun ötürülməsi üçün təhlükəsizliyini təmin etməkdir
- onu işə salma ardıcıllığına daxil etmək
- mesajı əl çatan etmək
- ehtiyat üçün hazırlamaq

521. Tətbiq proqramlarında hansı virus yayılır?

- yükləmə virusu
√ makro virus
- antivirus
- heç biri
- fayl virusu

522. Aşağıdakılardan hansı həqiqi şəbəkə ünvanlarını gizlədir və şəbəkəyə daxil olan və çıxan bütün mesajları ələ keçirmək üçün istifadə olunur?

- logic bomb
√ [RTYUIO32JHGFZXCV
- patches
- key
- fire wall

523. Məlumatların qəbulediciyə göndərildiyi kimi çatması lazım olduqda, ona … deyilir

- mesajın məxfiliyi
√ mesaj bütövlüyü
- mesaj göndərilməsi
- mesaj qəbulu
- mesaj sıçraması

524. Sənədin bütövlüyünü qorumaq üçün həm sənəd, həm də barmaq izi …

- istifadə olunmur
√ lazımdır
- lazım deyil
- olsa da olar, olmasa da
- əhəmiyyətsiz

525. Mesajın məxfiliyi … istifadə edir.

- simmetrik açardan
- şifrəli mətndən
- şifrədən
√ asimmetrik açardan
- barmaq izindən

526. Mac nə üçün istifadə olunur?

- mesajın ixtiyari əlaqəsi
√ mesajın identifikasiyası kodu
- mesajın autentifikasiya şifrəsi
- heç biri
- mesajın autentifikasiyasına nəzarət

527. Şifrələmə və şifrənin açılması məxfiliyi təmin edir, lakin … təmin etmir

- autentifikasiya
√ tamlıq
- modulluq
- hamısı
- gizlilik

528. Iki tərəf arasında sessiya simmetrik açarı neçə dəfə istifadə olunur?

- iki dəfə
√ yalnız bir dəfə
- şərtlərdən asılıdır

- heç vaxt
- bir neçə dəfə

529. Sənədin bütövlüyünü qorumağın bir yolu hansıdır?

- göz şüaları
√ barmaq izinin istifadəsi
- rentgen şüaları
- ultrabənövşəyi şüalar
- biometrik

530. Rəqəmsal imzanın …. Ehtiyacı var

- özəl açar sistemi
√ açıq açar sisteminə
- gizli açar
- heç biri
- paylaşılan açar sistemi

531. Mesajın və ya sənədin bütövlüyünü yoxlamaq üçün qəbuledici nə yaradır?

- hash-cədvəl
√ hash tag
- barmaq izi
- gizli açar
- hiper mətn

532. Hash funksiyası mesajın bütövlüyünə zəmanət verir. Mesajın ….. zəmanət verir

- əvəz etməsinə
√ dəyişməsinə
- pozulumasına
- emalına
- ümumi baxışına

533. Mesajın məxfiliyində ötürülən mesaj kim üçün məna kəsb etməlidir?

- göndərən
√ qəbuledici
- tərcüməçi
- yadda saxlayan
- modul

534. Mesajın autentifikasiyası …. Kənar bir xidmətdir

- mesajın məxfiliyi
√ mesaj bütövlüyü
- mesaj göndərilməsi
- mesaj qəbulu
- mesaj sıçraması

535. Təhlükəsiz hash alqoritmi 1(SHA-l) neçə bitlik mesaj həzminə malikdir?

- 512
√ 160
- 820
- 264
- 628

536. Asimmetrik açar kriptosistemi ilə məxfiliyin öz …. var.

- qurumları
√ problemləri
- tərcüməçisi
- modulu
- faktları

537. Virus növlərini seçin:

- 1, 4, 5
√ 1. Boot-sector Virusu
- 2, 3, 5
- 2, 4
- 2, 5

538. AES _____ müxtəlif konfiqurasiyaya malikdir.

- iki
- bir
- beş
√ üç
- dörd

539. _____ DES DES açarının ölçüsünü artırmaq üçün nəzərdə tutulmuşdur.

- yuxarıda göstərilənlərin heç biri
- yuxarıda göstərilənlərin hamısı
- İkiqat
- Dördqat
√ Üçqat

540. DES on altı ____ dəyirmi açar yaratmaq üçün açar generatorundan istifadə edir.

- 32-bit
- 108-bit
- 42-bit
√ 48-bit
- 54-bit

541. DES funksiyası _____ komponentdən ibarətdir.

- 5
- 1
- 3
- 2
√ 4

542. DES başlanğıc və son permutasiya blokuna və ____ dövrəyə malikdir.

- yuxarıda göstərilənlərin hamısı
- yuxarıda göstərilənlərin heç biri
√ 16
- 14
- 15

543. DES ABŞ hökuməti tərəfindən qəbul edilmiş (n) _____ metodudur.

- asimmetrik açar
√ simmetrik açar
- heç biri

- hamısı yanlışdır
- hər iki açar

544. Müasir şifrə adətən müxtəlif sadə şifrələrin birləşməsindən ibarət mürəkkəb ____ şifrədir.

- Yaxın
- √ dairə
- yuxarıda göstərilənlərin heç biri
- yuxarıda göstərilənlərin hamısı
- kvadrat

545. A(n) __ giriş və çıxış axınları arasında əlaqəni müəyyən etmək üçün cədvəldən istifadə edən N giriş və M çıxışı olan açarsız permütasyon şifrəsidir.

- S qutusu
- √ P-qutu
- yuxarıda göstərilənlərin heç biri
- yuxarıda göstərilənlərin hamısı
- T qutusu

546. A(n) _____ giriş və çıxış axınları arasında əlaqəni müəyyən etmək üçün düsturdan istifadə edən N giriş və M çıxışı olan açarsız əvəzetmə şifrəsidir.

- P-qutu
- √ S qutusu
- yuxarıda göstərilənlərin heç biri
- yuxarıda göstərilənlərin hamısı
- T qutusu

547. _____ şifrəsi şifrəli mətni yaratmaq üçün açıq mətn simvollarını yenidən təşkil edir.

- Qoşma
- əvəz
- Silmə
- √ transpozisiya
- Növbə

548. Sezar şifrəsi 3 açarı olan ____ şifrəsidir.

- transpozisiya
- √ növbə
- yuxarıda göstərilənlərin heç biri
- yuxarıda göstərilənlərin hamısı
- əlavə

549. ____ şifrəsi ən sadə bir əlifbalı şifrədir. 26 modulu ilə modul arifmetikadan istifadə edir.

- transpozisiya
- √ növbə
- yuxarıda göstərilənlərin heç biri
- yuxarıda göstərilənlərin hamısı
- əlavə

550. ____ şifrələri iki geniş kateqoriyaya bölmək olar: monoəlifbalı və poliəlifbalı.

- Transpozisiya
- √ Dəyişdirmə
- Daxili
- Qoşma
- Silmə

551. _____ şifrəsi bir simvolu digəri ilə əvəz edir.

- transpozisiya
- √ əvəz
- daxil etmə
- silmə
- qoşma

552. Asimmetrik açar şifrəsində alıcı _____ açarından istifadə edir.

- ictimai
- √ Şəxsi
- nə şəxsi, nə də ictimai
- şəxsi və ictimai
- ya şəxsi, ya ictimai

553. Asimmetrik açar şifrəsində göndərici _____ açarından istifadə edir.

- özəl
- √ ictimai
- nə ictimai, nə özəl
- ictimai və özəl
- ya ictimai və ya özəl

554. Şifrə(n)____ bir cüt açardan istifadə edir.

- simmetrik açar
- √ asimmetrik açar
- nə simmetrik , nə də asimmetrik
- hər iki açar
- simmetrik və ya asimmetrik

555. A(n) _____-da açar gizli açar adlanır.

- asimmetrik açar
- √ simmetrik açar
- nə simmetrik , nə də asimmetrik
- hər iki açar
- simmetrik və ya asimmetrik

556. Şifrə(n) _____-də göndərən və qəbul edən eyni açardan istifadə edir.

- asimmetrik açar
- √ simmetrik açar
- nə simmetrik, nə də asimmetrik
- hər iki açar
- simmetrik və ya asimmetrik

557. ____ transformasiyadan sonrakı mesajdır

- açıq mətn
- √ şifrəli mətn
- yuxarıda göstərilənlərin heç biri
- yuxarıda göstərilənlərin hamısı
- gizli mətn

558. ____ transformasiyadan əvvəl orijinal mesajdır.

- şifrəli mətn

√ açıq mətn
• yuxarıda göstərilənlərin heç biri
• yuxarıda göstərilənlərin hamısı
• gizli mətn

559. __ mesajları təhlükəsiz və hücuma qarşı immunitetli etmək üçün onları dəyişdirmək elmi və sənətidir.

• Kriptoqrafiya və Kriptanaliz
• nə Kriptoqrafiya, nə də Kriptanaliz
√ Kriptoqrafiya
• ya Kriptoqrafiya və ya Kriptanaliz
• Kriptanaliz

560. __, şifrənin üzərində işlədiyi ədəd və ya ədədlər toplusudur.

• şifrə
• yuxarıda göstərilənlərin hamısı
• yuxarıda göstərilənlərin heç biri
√ açar
• sirr

561. Şifrələmə alqoritmi ilə deşifrə alqoritminin birləşməsinə _____ deyilir.

• yuxarıda göstərilənlərin heç biri
• sirr
• açar
√ şifrə
• yuxarıda göstərilənlərin hamısı

562. A(n)_____ alqoritmi şifrəli mətni açıq mətnə çevirir.

• İcazə və Səlahiyyət
• Şifrələmə
• İcazə
√ transkript
• Səlahiyyət

563. A(n) _____ alqoritmi açıq mətni şifrəli mətnə çevirir

• İcazə və Səlahiyyət
• Səlahiyyət
• transkript
• İcazə
√ Şifrələmə

564. Kompüter sistemləri arasında rabitəni qorumaq üçün mesajların şifrələnməsi və deşifrə edilməsi üçün hansı alqoritmdən istifadə olunur?

• Şifrə və deşifrə etmək
• Hamısı
• deşifrə etmək
• snayper
√ Şifrə

565. RSA kriptosistemində iştirakçı öz açıq və şəxsi açarlarını yaratmaq üçün p = 3 və q = 11 iki sadə ədəddən istifadə edir. Şəxsi açar 7-dirsə, KOMPYUTER mətni açıq açarla necə şifrələnəcək?

• 25 9 19 4 12 4 25 27
• 9 27 25 4 12 4 25 27
• 25 27 4 25 12 4 25 27
• 9 27 4 25 21 8 26 24

√ 27 9 19 4 21 14 26 24

566. Fərz edək ki, N nəfərdən ibarət qrupdakı hər kəs simmetrik açar kriptoqrafik sistemindən istifadə edərək (N-1) digər insanlarla gizli ünsiyyət qurmaq istəyir. Hər hansı iki şəxs arasındakı ünsiyyət qrupun digər üzvləri tərəfindən yazılmamalıdır. Məxfilik tələbini yerinə yetirmək üçün bütövlükdə sistemdə tələb olunan açarların sayıdır

- 2n
- N/2
- (N-1)2
√ N(N-1)/2
- N(N-1)

567. Dinamik paket filtri firewallları dördüncü nəsil təhlükəsizlik divarlarıdır ki, onlar üzərində işləyirlər

- Tətbiq təbəqəsi
- sessiya qatı
√ TCP, UDP
- UDP
- PTS

568. Şifrələmə və deşifrə üçün eyni açardan hansı kriptoqrafiya növü istifadə olunur?

- Açar Kriptoqrafiya
- Kriptoqrafiya
- Polialfabetik
- Şifrələmə
√ Simmetrik kriptoqrafiya

569. Kriptoqrafiya ixtisaslaşdırılmış bir sahədir

- Bulud hesablama
- Kapital təhlükəsizliyi
- İnformasiya təhlükəsizliyi
√ Kibertəhlükəsizlik
- Qlobal Təhlükəsizlik

570. Şəbəkə təhlükəsizliyi ilə bağlı aşağıdakı bəyanatı nəzərdən keçirin: (a) Mesajın məxfiliyi o deməkdir ki, göndərən və alıcının məxfilik gözləntisi var. (b) Mesajın tamlığı o deməkdir ki, məlumat alıcıya göndərildiyi kimi çatmalıdır. (c) Mesajın autentifikasiyası o deməkdir ki, alıcı mesajın nəzərdə tutulan göndəricidən gəldiyinə əmindir. Bəyanatlardan hansı doğrudur?

- Yalnız (a)
- Yalnız (b) və (c)
√ (a), (b), (c)
- Yalnız (a) və (c)
- Yalnız (a) və (b)

571. MAC terminində kriptoqrafiya ilə bağlı “A” hərfi nəyi ifadə edir?

- Ünvan
- Giriş
√ İdentifikasiyanı
- İcazə
- Səlahiyyətlər

572. PGP Seqmentasiyaya aiddir.

- Adətən, maksimum 50.000 oktet uzunluqlu mesaja məhdudlaşdırılır.
- Qəbuledici bütün e-poçt başlıqlarını açır və bloku yenidən yığır.
- PGP böyük mesajı avtomatik olaraq alt hissələrə bölür.
√ PGP böyük mesajı avtomatik olaraq alt hissələrə bölə bilmir.
- Daha uzun mesajlar seqmentlərə bölünməlidir.

573. Aşağıdakılardan hansı PGP xidmətlətinə aiddir

- Firewall
- Kompüter cinayətkarlığı
- İP təhlükəsizliyi
- √ Autentifikasiya
- E-poçt təsdiqləmə

574. Aşağıdakılardan hansı PGP xidmətlətinə aid deyil.

- Autentifikasiya
- Sıxılma
- Seqmentasiya
- √ Firewall
- Məxfilik

575. PGP neçə xidmətdən ibarətdir.

- 2
- 6
- 12
- √ 5
- 3

576. Aşağıdakılardan hansı istənməyən kommersiya e-poçtu hesab olunur?

- Antivirus
- Casus proqram
- Zərərli proqram
- Virus
- √ Spam

577. Saxta e-poçt mesajları qanuni görünən bəzi saxta e-poçt mesajlarıdır və sizin məxfi bank təfərrüatlarınızı, məsələn, _____ təfərrüatları _____ və parollar tələb edir.

- ev adresi, hesab nömrəsi
- e-poçt, şəxsiyyət vəsiqəsi
- mobil telefon, istifadəçi adı
- √ kredit kartı, login ID
- e-poçt, hesab nömrəsi

578. İstənməyən toplu e-poçtlar (UBI) _____ adlanır

- MMS
- SMS
- Virus
- Zərərli elektron məktublar
- √ Spam e-poçtlar

579. Qeyri-qanuni hakerlər e-poçt sındırmalarından istifadə edərək _____ virus _____ və spam e-poçtları göndərə və yaya bilər.

- antivirus, yamaqlar
- antivirus, kukilər
- zərərli proqram, təhlükəsizlik yamaları
- √ troyan, yönləndirilmiş zərərli URL-lər
- sındırılmış proqram təminatı, yönləndirilmiş zərərli URL-lər

580. ___ istifadəçiləri saxta səhifələr vasitəsilə istifadəçi adlarını və parollarını ələ keçirmək üçün istifadə edilən texnikadır.

- DNS saxtakarlığı
- Kuki oğurluğu
- Sosial mühəndislik
√ Fişinq
- Banner tutma

581. Aşağıdakılardan hansı düzgün emaildir?

- userName@website@com
- userName@com
- userName.website.com
- userName.website@com
√ userName@website.com

582. Aşağıdakılardan hansı müdaxilə və ya hücum texnikasının qeyri-texniki növüdür?

√ Sosial mühəndislik
- Tərs mühəndislik
- Zərərli proqramların təhlili
- Zərərli proqramların yoluxması
- Zərərli proqramların yazılması

583. Əgər _____-də saxlanılan məlumatlar şifrələnməyibsə, onda kuki oğurlandıqdan sonra təcavüzkarlar kuki tərəfindən saxlanılan istifadəçi adı və parol kimi məlumatları görə bilər.

- sərt disk
- server
- yaddaş
√ kukilər
- karantin

584. ___ spam və fişinq hücumları ilə üzləşən zərərli proqramların yayılması üçün məşhur texnoloji mühitdir.

- Qələm sürücüsü
- Veb sayt
- Antivirus
- Bulud
√ E-poçt

585. Aşağıdakılardan hansı e-poçt təhlükəsizliyi üçün düzgün üsul deyil?

- E-poçt şifrələməsindən istifadə
- İki-faktorlu autentifikasiyadan istifadə
- Güclü parollardan istifadə
√ Tədqiq etmək üçün naməlum linklərə klikləmək
- Spam filtrləri və zərərli proqram skanerləri

586. ___ qeyri-rəsmi giriş, itki və ya hücuma qarşı e-poçt rabitəsi və hesablardakı həssas məlumatları qorumaq üsuludur.

- Elektron poçtun dəyişdirilməsi
- Elektron poçtun qorunması
- Elektron poçtun sındırılması
√ Elektron poçtun təhlükəsizliyi
- Elektron poçtun mühafizəsi

587. Aşağıdakılardan hansı e-poçt məlumatlarını oğurlamaq üçün əsas üsuldur?

- Tərs mühəndislik
- Giriş nöqtəsi skanlama

- Banner tutma
- √ Şifrə fişinqi
- DNS saxtakarlığı

588. Aşağıdakılardan hansı e-poçt məlumatlarını oğurlamaq üçün əsas üsuldur?

- Tərs mühəndislik
- Giriş nöqtəsi skanlama
- Banner tutma
- √ Kuki oğurlamaq
- DNS saxtakarlığı

589. E-poçt məlumatlarını oğurlamağın neçə əsas üsulu var?

- 2
- 6
- 5
- √ 3
- 4

590. Aşağıdakılardan hansı e-poçt məlumatlarını oğurlamaq üçün əsas üsuldur?

- Tərs mühəndislik
- √ Sosial mühəndislik
- Banner tutma
- Giriş nöqtəsi skanlama
- DNS saxtakarlığı

591. Aşağıdakılardan hansı şəbəkə təhlükəsizlik protokolları tərəfindən mesaj həzmini yaratmaq üçün istifadə olunur? (P) RSA (Q) SHA-1 (R) DES (S) MD5

- Yalnız P və R
- √ Yalnız Q və S
- Yalnız R və S
- Yalnız P və S
- Yalnız Q və R

592. Dinamik paket filtrləri firewall işləyən dördüncü nəsil firewalllardır

- Tətbiq qatı
- √ TCP, UDP
- UDP
- Sessiya qatı
- TCP

593. Şəxsi şəbəkəyə və ya şəbəkədən icazəsiz girişin qarşısını almaq üçün nəzərdə tutulmuş sistem nə adlanır?

- Kompüter skanı
- √ Firewall
- Biotexnologiya
- Casus proqram
- Rəqəmsal skan

594. Rəqəmsal imza tələb olunur:

- bütün e-poçt göndərilməsi üçün
- √ göndəricinin rabitədən imtina etməməsinə görə
- FTP əməliyyatları üçün
- ICMP serverləri üçün
- bütün DHCP serverləri üçün

595. Layer-4 firewall (nəqliyyat qatına qədər bütün protokol başlıqlarına baxa bilən cihaz) OLMAZ

- 21:00 və 5:00 ərzində bütün HTTP trafikini bloklayın
- √ 21:00 və 5:00 ərzində çox istifadəçi sistemində xüsusi istifadəçidən TCP trafikini bloklayır
- Müəyyən bir IP ünvanından gələn trafiki dayandırır, lakin bu ünvana gedən trafikə eyni IP ünvanına icazə verir
- bütün FTP trafikini bloklayır
- bütün ICMP trafikini bloklayın

596. ___ olduqca yaxşı məxfilik alqoritmindən istifadə edir.

- Elektron məktublar
- √ Həm Elektron məktublar, həm də Fayl şifrələməsi
- Seçimlərdən heç biri
- Fayl bloku
- Fayl şifrələməsi

597. Hesablamada, əvvəlcədən müəyyən edilmiş təhlükəsizlik qaydalarına əsasən daxil olan və gedən şəbəkə trafikini izləyən və nəzarət edən şəbəkə təhlükəsizlik sistemidir.

- Kompüter skanı
- Kuki
- √ Firewall
- Spam
- Casus proqram

598. Kompüter təhlükəsizliyi kontekstində kraker adı ilə kim tanınır?

- Ağ Papaqlı Hakerlər
- √ Qara papaqlı hakerlər
- Ssenari Kiddie
- Boz Papaqlı Hakerlər
- Elit Hakerlər

599. Faylın şifrələnməsinin əsas səbəbi

- Onun ölçüsünü azaldır
- √ Onu ötürmək üçün təmin edir
- Onu işə salma ardıcıllığına daxil edir
- Onu idarə edir
- Onu ehtiyat üçün hazırlayır

600. Tətbiq proqramlarında hansı virus yayılır?

- Yükləmə virusu
- √ Makro virus
- Antivirus
- Kompanyon-viruslar
- Fayl virusu

601. ____GIF şəklinin içərisinə daxil edilmiş kiçik proqramdır.

- Kuki
- √ Veb səhvi
- Spam
- Aparat
- Spyware proqram

602. ___ həqiqi şəbəkə ünvanlarını gizlədir və şəbəkəyə daxil olan və çıxan bütün mesajları ələ keçirmək üçün istifadə olunur.

- Məntiq bombası
√ [RTYUIO32JHGFZXCV
- Yamalar
- Kuki
- Firewall

603. Metod _____ iki tərəf üçün birdəfəlik sessiya açarı təqdim edir.

- random
√ Diffie-Hellman
- AES
- RSS
- DES

604. Açıq açar kriptoqrafiyasının geniş istifadə olunan üsullarından biri _____ alqoritmidir.

- B. RAS
√ RSA
- RAA
- RHA
- RSS

605. ECB və CBC _____ şifrədir.

- axın
√ blok
- yuxarıda göstərilənlərin heç biri
- yuxarıda göstərilənlərin hamısı
- sahə

606. ... kriptoqrafiyada eyni açar hər iki istiqamətdə istifadə olunur.

- açıq açar
- asimmetrik açar
- Seçimlərin heç biri düzgün deyil.
- gizli açar
√ simmetrik açar

607. ... kriptoqrafiyada eyni açardan göndərən və qəbul edən şəxs istifadə edir.

- asimmetrik açar
- açıq açar
√ simmetrik açar
- gizli açar
- Seçimlərin heç biri düzgün deyil.

608. … mesajı başqa bir şeylə örtərək gizlətmək deməkdir.

- Sıxılma
√ Steqanoqrafiya
- Şifrələmə
- Seçimlərin heç biri düzgün deyil.
- Kriptoqrafiya

609. … mesajın məzmununu şifrələmə yolu ilə gizlətmək deməkdir.

- Seçimlərin heç biri düzgün deyil
√ Kriptoqrafiya
- Sıxılma
- Steqanoqrafiya

- Şifrənin açılması

610. Aşağıdakı hücumlardan hansı əlçatanlığı təhdid edir?

- Təkrarlanır
- Maskaradlıq
- Modifikasiya
- √ Xidmətdən imtina
- Seçimlərin heç biri düzgün deyil.

611. Aşağıdakı hücumlardan hansı bütövlüyü təhdid edir?

- Dəyişiklik
- Trafik Təhlili
- Xidmətdən imtina
- √ maskaradlıq
- Seçimlərin heç biri düzgün deyil.

612. Üç təhlükəsizlik məqsədi …

- √ məxfilik, tamlıq və əlçatanlıq
- seçimlərin heç biri düzgün deyil.
- məxfilik, kriptoqrafiya və şifrənin açılması
- məxfilik, kriptoqrafiya və rədd edilməməsi
- məxfilik, şifrələmə və şifrənin açılması

613. Proksi firewall … qatında filtrlər aparır.

- seçimlərin heç biri düzgün deyil.
- nəqliyyat
- √ tətbiq
- şəbəkə
- təqdimat

614. Paket filtri firewall … Və ya … qatında filtrlər edir.

- √ şəbəkə; nəqliyyat
- seçimlərin heç biri düzgün deyil
- ərizə, sessiya
- şəbəkə; tətbiq
- nəqliyyat; tətbiq

615. ... e-poçt göndərilməsində təhlükəsizliyin bütün dörd aspektini təmin etmək üçün Phil Zimmermann tərəfindən icad edilmişdir.

- ESP
- AH
- SPE
- TLS
- √ Seçimlərin heç biri düzgün deyil

616. . .. nəqliyyat qatında təhlükəsizliyi təmin etmək üçün nəzərdə tutulmuşdur.

- SPE
- Seçimlərin heç biri düzgün deyil.
- √ TLS
- ESP
- AH

617. … protokolu mesajın autentifikasiyasını, bütövlüyünü və məxfiliyini təmin edir.

- SSP
- Seçimlərin heç biri düzgün deyil.
- AH
- SPE
√ ESP

618. .. protokolu mesajın autentifikasiyası və bütövlüyünü təmin edir, lakin məxfiliyi təmin etmir.

- Seçimlərin heç biri düzgün deyil.
- SSP
√ AH
- SPE
- ESP

619. … protokolu mənbə hostunun autentifikasiyası və IP paketi tərəfindən daşınan faydalı yükün bütövlüyünü təmin etmək üçün nəzərdə tutulmuşdur.

- ESP
√ AH
- SSP
- Seçimlərin heç biri düzgün deyil.
- SPE

620. … rejimində IPSec başlığı orijinal IP başlığının qarşısında yerləşdirilir.

- Seçimlərin heç biri düzgün deyil.
- şəbəkə
√ tunel
- keçid
- nəqliyyat

621. … rejimində IPSec başlığı IP başlığı ilə paketin qalan hissəsi arasında əlavə edilir.

- tunel
√ nəqliyyat
- səthi
- Seçimlərin heç biri düzgün deyil.
- keçid

622. IPSec iki müxtəlif rejimdə işləyir: … rejimi və … rejimi.

- nəqliyyat; şəbəkə
√ nəqliyyat; tunel
- şəbəkə, səth
- Seçimlərin heç biri düzgün deyil.
- tunel; səthi

623. IP Təhlükəsizliyi (IPSec) … səviyyəsində paketin təhlükəsizliyini təmin etmək üçün IETF (Internet Engineering Task Force) tərəfindən hazırlanmış protokollar toplusudur.

- məlumat bağlantısı
√ şəbəkə
- Seçimlərin heç biri düzgün deyil.
- firewall
- nəqliyyat

624. VPN texnologiyası təşkilatın məxfiliyini təmin etmək üçün eyni vaxtda iki üsuldan istifadə edir: … və…

- SSL; tunel çəkmə
√ IPSec; tunel çəkmə

- Seçimlərin heç biri düzgün deyil.
- KDC; SSL
- IPSec; SSL

625. … açıq açar və onun sahibi arasında məcburi əlaqəni təsdiqləyir.

- KDC
√ CA
- Seçimlərin heç biri düzgün deyil
- Seçimlərin hamısı düzgündür
- TLS

626. … simmetrik açar paylanması problemini həll edən etibarlı üçüncü tərəfdir.

- CA
√ KDC
- firewall
- Seçimlərin heç biri düzgün deyil.
- TLS

627. Rəqəmsal imza texnikasında bütün mesaj asimmetrik açardan istifadə edilməklə imzalandıqda, mesajı qəbul edən şəxs imzanı yoxlamaq üçün ... istifadə edir.

- onun və ya özünün açıq açarı
√ göndərənin açıq açarı
- Seçimlərin heç biri düzgün deyil
- onun öz simmetrik açarı
- onun və ya onun şəxsi açarı

628. _____ şəbəkə səviyyəsində paketin təhlükəsizliyini təmin etmək üçün IETF tərəfindən hazırlanmış protokollar toplusudur.

- PGP
√ IPSec
- IKE
- Yuxarıdakıların heç biri
- SSL

629. IKE _____digər protokollara əsaslanan mürəkkəb protokoldur.

- 2
√ 3
- 5
- 6
- 4

630. _____ IPSec adlanan SA dəstindən istifadə edir

- SAD
√ SADB
- SAS
- Yuxarıdakıların heç biri
- SAB

631. _____ həm gələn, həm də gedən təhlükəsizlik assosiasiyaları yaratmaq üçün nəzərdə tutulmuş protokoldur.

- SA
√ IKE
- CA
- AH
- KDC

632. ____olduqca yaxşı məxfilik (PGP) istifadə olunur

- Brauzer təhlükəsizliyi
- √ Elektron poçtun təhlükəsizliyi
- WiFi təhlükəsizliyi
- Bluetooth təhlükəsizliyi
- FTP təhlükəsizliyi

633. Hansı komponent IP təhlükəsizliyinə daxildir?

- Doğrulama Başlığı (AH)
- √ Qeyd olunanların hamısı
- İnternet açarı mübadiləsi (IKE)
- Təhlükəsizlik Assosiasiyaları (SA)
- Kapsülləşdirici Təhlükəsizlik Yükü (ESP)

634. _____ Tunel rejimində IPSec qoruyur

- IP başlığı
- √ Bütün IP paketi
- İP treyler
- IP ünvanı
- IP yükü

635. ____ IPSec təhlükəsizliyini təmin etmək üçün nəzərdə tutulmuşdur.

- Nəqliyyat təbəqəsi
- √ Şəbəkə səviyyəsi
- Sessiya qatı
- Təqdimat təbəqəsi
- Tətbiq təbəqəsi

636. Rəqəmsal imza nədir?

- Kompüter cinayətkalığıdır
- √ göndərilən məlumatı yoxlamaqla onun həqiqiliyinin müəyyənləşdirilməsini və sənədin imzalandıqdan sonra dəyişdirilmədiyinə zəmanəti təmin edən unikal elektron identifikator.
- VPN ilə eyni funksiyanı yerinə yetirir
- adətən simmetrik kriptoqrafiyaya əsaslanan imza növüdür
- Kompüter virusunun bir növüdür

637. S/MİME nin funksiyalarına aid deyil.

- Zərflənmiş Məlumat
- √ Deşifrə edilmiş məlumat
- Təmiz İmzalı Məlumat
- İmzalanmış və Zərflənmiş Məlumat
- İmzalanmış Məlumat

638. SMTP məhdudiyyətlərinə (Ötürə bilmir və ya problemi var) aid deyil.

- müəyyən ölçüdən böyük mesajlar
- √ Mütləq .doc uzantılı fayllardan istifadə olumalıdır.
- "milli dil" simvolları (ASCII olmayan)
- icra edilə bilən(.exe) fayllar və ya digər ikili fayllar (jpeg şəkli)
- ASCII-dən EBCDIC-ə tərcümə problemləri

639. “Sıxılma” nın uzantısı nədir.

- doc
√ ZİP
- xlxs
- pdf
- PPT

640. Şifrələmədə çevrilən məlumat _____ adlanır.

√ Sadə mətn
- Şifrələnmiş mətn
- Paralel mətn
- Şifrəsi açılmış mətn
- Kilidli mətn

641. ƏS-də resurslara daxil ola bilən nəzarət edən təhlükəsizlik xüsusiyyətləri.

√ Doğrulama
- İPsec
- Girişə nəzarət
- İdentifikasiya
- Validasiya

642. CHAP mənası?

- Circuit Handshake autentifikasiya protokolu
- Challenge Hardware autentifikasiya protokolu
√ Challenge Handshake autentifikasiya protokolu
- Circuit Hardware autentifikasiya protokolu
- Circuit Handmade autentifikasiya protokolu

643. İstifadəçi hüquqları ilə məşğul olan autentifikasiya narahatlığı.

- Funksional icazə
- Funksional icazə
- Avtomatik yoxlama
√ Ümumi giriş
- Funksional autentifikasiya

644. İstifadəçinin şəxsiyyətinin yoxlanılması prosesi.

- Validasiya
- Silmə
- Yoxlama
- İdentifikasiya
√ Doğrulama

645. Bunlardan hansı şəbəkə identifikasiyasının bir hissəsidir?

- barmaq izi
- Şifrə
- OTP
√ İstifadəçi İD
- göz skaneri

646. Hansı şəbəkə təhlükəsizliyinin məqsədi deyil?

- Doğrulama
- İdentifikasiya
- Qoruma
- Girişə nəzarət

√ Kilid

647. Gündəlik işlərdə istifadə olunan həm dövlət, həm də özəl kompüter şəbəkələrinin müxtəlifliyini əhatə edən sahə.

- Süni intellekt
- Kilid
- İT
√ Şəbəkə Təhlükəsizliyi
- ML

648. Faylın şifrələnməsinin əsas səbəbi ...

- Ömrün uzadır
- Onu ehtiyat üçün hazırlayır
- Onu ötürmə üçün təmin edir
√ Onun ölçüsünü azaltmaq
- Onu işə salma ardıcıllığına daxil edir

649. Tətbiqi proqram təminatında hansı virus yayılır?

- Yükləmə virusu
- Antivirus
- Troyan
√ Makro virus
- Fayl virusu

650. Rəqəmsal imza texnikasında bütün mesaj asimmetrik açarla imzalandıqda, mesajı göndərən şəxs mesajı imzalamaq üçün istifadə edir.

- onun öz simmetrik açarı
- göndərənin açıq açarı
- Seçimlərin heç biri düzgün deyil
√ öz şəxsi açarı
- onun öz açıq açarı

651. RSA-da, əgər A istifadəçisi B istifadəçisinə şifrəli mesaj göndərmək istəsə, açıq mətn ... açıq açarı ilə şifrələnir.

- şəbəkə
- Seçimlərin hamısı düzgündür
- Seçimlərin heç biri düzgün deyil
√ istifadəçi B
- istifadəçi A

652. Məxfilik üçün RSA alqoritmi … kriptoqrafiyadan istifadə edir.

- əvəzetmə
- şəxsi açar
- Seçimlərin heç biri düzgün deyil.
√ asimmetrik açar
- simmetrik açar

653. Məxfilik üçün istifadə edilən asimmetrik açar metodunda qəbuledici mesajın şifrəsini açmaq üçün özünün …-dan istifadə edir.

- simmetrik açar
- Seçimlərin heç biri düzgün deyil.
- açar yoxdur
- şəxsi açar
√ açıq açar

654. Məxfilik üçün istifadə edilən asimmetrik açar metodunda hansı açar ictimaiyyətə məlumdur?

- Seçimlərin heç biri düzgün deyil.
- hər iki açar
- yalnız şifrələmə açarı
√ yalnız deşifrə açarı
- açar yoxdur

655. Mesaj şifrələndikdən sonra ona … deyilir.

- çirkli mətn
- Seçimlərin heç biri düzgün deyil.
- mətn
√ şifrəli mətn
- açıq mətn

656. … kriptoqrafiyada hər kəsin hər kəsin açıq açarına çıxışı var.

- gizli açar
- özəl açar
- Seçimlərin heç biri düzgün deyil.
√ asimmetrik açar
- simmetrik açar

657. …-da tərəfin şəxsiyyəti sistemə girişin bütün müddəti ərzində bir dəfə yoxlanılır.

- mesajın bütövlüyü
- Seçimlərin heç biri düzgün deyil.
√ obyektin autentifikasiyası
- obyektin bütövlüyü
- mesajın autentifikasiyası

658. Rəqəmsal imza təmin etmir

- dürüstlük
√ məxfilik
- autentifikasiya
- inkar etməmək
- Bütün seçimləri təmin edir.

659. … mesaj üçün autentifikasiya, bütövlüyü və rədd edilməməsini təmin edə bilər.

- Şifrələmə/şifrənin açılması
- Seçimlərin heç biri düzgün deyil
- Doğrulama
√ Rəqəmsal imza
- Sıxılma

660. … o deməkdir ki, məlumat alıcıya göndərildiyi kimi çatmalıdır.

- Seçimlərin heç biri düzgün deyil.
- İnkar etməmək
- Doğrulama
√ Mesajın tamlığı
- Dürüstlük

661. … o deməkdir ki, göndərən və alan məxfilik gözləyir.

- Doğrulama
- İnkar etməmək
- Dürüstlük
√ Seçimlərin heç biri düzgün deyil

- Mesajın bütövlüyü

662. … kriptoqrafiya tez-tez qısa mesajlar üçün istifadə olunur.

- Seçimlərin heç biri düzgün deyil
- Simmetrik açar
- Gizli açar
- √ Asimmetrik açar
- Açıq açar

663. ... kriptoqrafiya çox vaxt uzun mesajlar üçün istifadə olunur.

- Seçimlərin heç biri düzgün deyil.
- Asimmetrik açar
- açıq açar
- √ Simmetrik açar
- gizli açar

664. Paket süzgəcindən keçirən firewalllar _____ şəbəkələrində effektiv işləyir.

- mürəkkəb
- daha kiçik
- böyük
- √ çox sadə
- çox böyük kompleks

665. Paket Filtrləmə təhlükəsizlik divarının bir üstünlüyü _____-dir.

- çox sürətli
- daha az mürəkkəb
- daha az xərc tələb edir
- √ daha səmərəli
- çox yavaş

666. Şəbəkə administratorları _____ _____ və _____ əsasında öz ACL qaydalarını yarada bilərlər.

- Ünvan, Şəbəkə topologiyası, Paket atributları
- Ünvan, Protokollar və təhlükəsizlik siyasətləri
- Ünvan, siyasətlər və Paket atributları
- √ Ünvan, Protokollar və Paket atributları
- Şəbəkə topologiyası, Protokollar və məlumat paketləri

667. Paket ACL meyarlarına cavab vermədikdə, paket _____

- düşür
- yaradılmışdır
- qəbul edildiyi kimi qəbul edilir
- √ yenidən göndərilir
- məhv edilmişdir

668. ACL _____ deməkdir

- Girişə Nəzarət Qeydləri
- Fişinq nəzarəti
- Giriş Şərtlərinin Siyahısı
- Anti-nəzarət siyahısı
- √ Girişə Nəzarət Siyahısı

669. _____ paket filtrləmə firewall qaydalarını müəyyən edir.

- açarlar
- Limanlar
√ Girişə Nəzarət Siyahısı
- Siyasətlər
- Protokollar

670. Kompüter _____ özünü başqa proqramlara kopyalayaraq özünü təkrarlayan zərərli koddur.

- proqram
√ virus
- qurd
- heç biri
- ərizə

671. Sistemin sındırılmasında aşağıdakılardan hansı ən vacib fəaliyyətdir?

- Məlumat toplanması
√ Parolların sındırılması
- Heç biri
- Hamısı
- İzlərin gizlədilməsi

672. Etik hakerlik və kibertəhlükəsizlikdə skanlamanın _____ növü var:

- 2
√ 3
- 4
- 5
- 1

673. Aşağıdakı port və İP ünvan skanerindən hansı istifadəçilər arasında məşhurdur?

- Cain and Abel
√ Angry IP Scanner
- Ettercap
- Heç biri
- Snort

674. Aşağıdakılardan hansı adətən Wi-Fi sındırma prosesində istifadə olunur?

- Wireshark
√ Aircrack-ng
- Hamısı
- Heç biri
- Norton

675. Aşağıdakılardan hansı mesajın bütövlüyünü yoxlamaq üçün istifadə olunan texnikaya aiddir?

- Rəqəmsal imza
√ Mesaj Digest
- Protokol
- Yuxarıdakıların hamısı
- Şifrənin açılması alqoritmi

676. Aşağıdakılardan hansı kompüterin daha əlçatan olmadığı halda prinsipin pozulmasına aiddir?

- Giriş nəzarəti
√ Mövcudluq
- hamısı
- Heç biri

- Məxfilik

677. Aşağıdakılardan hansı onlayn mühit və rəqəmsal media platforması ilə bağlı uyğun, etik davranışların araşdırılmasına aiddir?

- Kiber low
- √ Kiberetika
- Kibertəhlükəsizlik
- Yuxarıdakıların heç biri
- Kiber təhlükə

678. Aşağıdakılardan hansı öz ideyasını və ya ixtirasını başqalarının oğurlaması və ondan öz mənfəətləri üçün istifadə etməsinə aiddir?

- Piracy
- √ hamısı
- Əqli mülkiyyət hüquqları
- Yuxarıdakıların heç biri
- Plagiat

679. İnternet, şəbəkə və s. vasitəsilə gələn bütün məlumat paketlərini süzgəcdən keçirən proqram proqramı və ya aparat cihazı ola bilər. Bu, _____ kimi tanınır:

- Antivirus
- √ Firewall
- Zərərli proqram
- Yuxarıdakıların hamısı
- Cookies

680. Aşağıdakılardan hansı antivirus proqram növüdür?

- Quick heal
- √ hamısı
- Kaspersky
- heç biri
- Mcafee

681. _____ istifadəçinin kompüterinə virusları aşkar etmək və onlardan qaçmaq üçün nəzərdə tutulmuş proqram təminatı növüdür.

- Zərərli proqram
- √ Antivirus
- Həm B, həm də C
- heç biri
- Reklam proqramı

682. Aşağıdakılardan hansı adətən qurbanın internetdəki hər bir fəaliyyətini müşahidə edir, bütün məlumatları fonda toplayır və başqasına göndərir?

- Zərərli proqram
- √ Casus proqram
- Yuxarıdakıların hamısı
- Yuxarıdakıların heç biri
- Reklam proqramı

683. Aşağıdakılardan hansını kompüter təhlükələri sinfinə aid etmək olar?

- Fişinq
- √ DoS hücumu
- Yuxarıdakıların hamısı
- Yuxarıdakıların heç biri
- Tələb etmək

684. Dinamik paket filtrləri firewall dördüncü nəsil təhlükəsizlik divarlarıdır

- TCP
- √ Tətbiq təbəqəsi
- TCP, UDP
- Sessiya qatı
- UDP

685. 2000 elementi saxlayan 25 yuvalı T hash cədvəlini nəzərə alsaq, T üçün yük əmsalı α-dır.

- b.90
- √ a.80
- d.0.125
- e.0.521
- c.800

686. Ayrı-ayrı zəncirləmə alqoritmindən istifadə edərək hashing üçün ən pis halda axtarış vaxtı nədir?

- O(N^6)
- O(N^2)
- √ O(N)
- O(N^3)
- O(N log N)

687. Tam ədədlər üzərində aşağıdakı hash funksiyalarından hansı i üçün 0-dan 2020-yə qədər olan 0-dan 9-a qədər nömrələnmiş 10 qutu üzərində açarları ən bərabər şəkildə paylayacaq?

- h(i) =i^2 mod 10
- h(i) = (11 i^2) mod 10
- h(i) = (12 i) mod 9
- h(i) = (12 i) mod 10
- √ h(i) =i^3 mod 10

688. Müəyyən edilmiş yerdə arzu olunandan başqa açarın saxlandığı hal adlanır?

- açıq ünvanlama
- kopyalama
- hashing
- zəncirləmə
- √ toqquşma

689. Sadə keçiddə hansı məlumat strukturu uyğundur?

- binar əlaqəli siyahı
- tək əlaqəli siyahı
- dairə ilə əlaqəli siyahı
- √ ikiqat əlaqəli siyahı
- düzəlaqəli siyahı

690. Yük faktoru nədir?

- massivin orta ölçüsü
- şifrə heşi
- hesh cədvəlinin orta uzunluğu
- √ orta zəncir uzunluğu
- orta açar ölçüsü

691. Hansı verilənlər strukturu daimi axtarış vaxtı ilə məlumatları saxlamaq üçün heşinqdən istifadə edir?

- stack

- bağlı siyahı
- 2D massivi
- 1D massivi
√ hash cədvəli

692. Şifrələmə alqoritmi nədir?

- Əsasən şifrləməni tərsinə yerinə yetirərək onu yenidən düz mətnə çevirir.
- indi şifrələnmiş və göndərilməyə hazır olan mətn
- Açar orijinal düz mətnə edilən bütün keçidlər və əvəzetmələr haqqında məlumatları köhnələşdirir.
- O, təsadüfi məlumat axını kimi görünə bilər və oxunmazdır
√ Şifrələmə alqoritmi açıq mətni götürür və onu oxunmaz formata çevirir

693. Şifrətli mətn nədir?

- Açar orijinal düz mətnə edilən bütün keçidlər və əvəzetmələr haqqında məlumatları köhnələşdirir.
- açıq mətn yaradılan və şifrələmə metoduna göndərilən orijinal mesaja istinad edir.
- Əsasən şifrləməni tərsinə yerinə yetirərək onu yenidən düz mətnə çevirir.
√ Şifrə mətni indi şifrələnmiş və göndərilməyə hazır olan mətndir.
- indi şifrələnməmiş və göndərilməyə hazır olan mətn

694. Açıq mətn nədir?

- O, təsadüfi məlumat axını kimi görünə bilər və oxunmazdır.
- indi şifrələnmiş və göndərilməyə hazır olan mətn
- Əsasən şifrləməni tərsinə yerinə yetirərək onu yenidən düz mətnə çevirir.
√ açıq mətn şifrləmə metoduna yaradılan və göndərilən orijinal mesaja istinad edir.
- Açar orijinal düz mətnə edilən bütün keçidlər və əvəzetmələr haqqında məlumatları köhnələşdirir.

695. Açar nədir?

- Əsasən şifrləməni tərsinə yerinə yetirərək onu yenidən düz mətnə çevirir.
- O, təsadüfi məlumat axını kimi görünə bilər və oxunmazdır.
- Yaradılan və şifrələmə metoduna göndərilən orijinal mesaja aiddir.
- indi şifrələnmiş və göndərilməyə hazır olan mətn
√ Açar orijinal düz mətnə edilən bütün keçidlər və əvəzetmələr haqqında məlumatları köhnələşdirir

696. Simmetrik şifrələmədə şifrələnmiş mesaj ___ adlanır.

- Sadə mətn
- Ikinci mətn
- Əsas mətn
√ Şifrəli mətn
- Kodlanmış mətn

697. Data Şifrələmə Standartı (DES) eyni anda ___ bit üzərində işləyir

- 32
- 125
- 256
√ 64
- 16

698. Simmetrik şifrələmədə açar göndərən və qəbul edən tərəfindən ___-dir

√ məlumdur
- tərs
- naməlum
- paylaşdı
- dublikat

699. ___ informasiyanın bir formada, digər formada çevrilməsi prosesidir.

- bu cavabların hamısı düzgündür
- müdafiə
- köçürmə
- √ şifrələmə
- bu cavabların heç biri düzgün deyil

700. Açıq açar şifrələməsi alqoritmində ___ istifadə edir və ya yaradır.

- Şəxsi açar
- √ Bu cavabların hamısı düzgündür
- Asimmetrik
- Açıq açar
- Pseudo-təsadüfi nömrə