1. Toplanmış məlumatların analizi və audit hesabatının hazırlanması

2. Açıq açarlı kriptoqrafiya (biristiqamətli və gizli girişli biristiqamətli funksiyalar)

3. Kibertəhlükəsizlik anlayışı. Kibertəhlükəsizliyin üç aspekti

4. Sistemin hakinq edilməsi metodologiyası. Keyloqqerlər

5. RSA alqoritmində -dir. gizli açarını hesablayın.

1. ISO/IEC 27001 standartına uyğunluğun auditi

2. Diffi-Hellman açar mübadiləsi sxemi

3. Konfidensial informasiya. Dövlət sirri

4. Boşluqların qiymətləndirilməsi sistemləri. Boşluqların skorinqi sistemi (CVSS)

5. Eyler funksiyasının qiymətini hesablayın:

1. Sızma testləri

2. Eyler funksiyası və onun əsas xassələr

3. 3A (Autentifikasiya, Avtorizasiya və Audit)

4. Kompüter virusları və kompüter viruslarının təsnifatı

5. RSA alqoritmində -dir. mətnini şifrləyin.

1. Kibertəhlükəsizliyin təmin edilməsi metodları

2. RSA alqoritmi

3. Müdaxilə anlayışı və sui-istifadələrin aşkarlanması metodları

4. İzlərin gizlədilməsi alətləri

5. Hesablamalarla göstərin ki, 2 ədədi modulu üçün primitiv elementdir.

1. Anomaliyaların aşkarlanması metodları

2. Sadə ədədlərin generasiyası. Qüvvətin hesablanması alqoritmi

3. Hədəfyönümlü hücumlar. APT-hücum kampaniyaları

4. Soxulcanlar və onların təsnifatı

5. ElGamal imza sxemində , gizli açar , imzalanan məlumat -dir. Müvəqqəti açar seçilib və -dir. Rəqəmsal imza cütünü hesablayın.

1. Kiberhücumların məqsədləri. Kiberhücumların təsnifatı

2. Açarsız heş funksiyaların tərifi və xassələri. Heş funksiyaların iterativ modeli

3. Müdaxilələrin aşkarlanması sistemlərinin ümumi modeli

4. Troyanlar və onların təsnifatı

5. ElGamal imza sxemində , gizli açar olarsa, açıq açarını hesablayın.

1. Müdaxilələrin aşkarlanması sistemlərinin təsnifatı

2. Kriptoqrafik heş funksiayalar və onların növləri

3. “Cyber kill chain” modeli

4. DoS-hücumlar və üçsəviyyəli DDoS arxitekturası

5. RSA alqoritmində -dir. şifrmətnini deşifrləyin.

1. İnsident anlayışı

2. SHA-1 heş funksiyası

3. Etik hakinq anlayışı. Kali Linux

4. Zərərli proqramların digər növləri: Backdoor-lar, rutkitlər, butkitlər

5. Hesablamalarla göstərin ki, 5 ədədi modulu üçün primitiv element deyil.

1. CERT-komandaları. CSIRT xidmətləri

2. SHA-2 heş funksiyaları və SHA-3 standartı

3. Sosial mühəndislik üsulları

4. DDoS-hücumlara nümunələr

5. Diffi-Hellman açar mübadiləsi sxemində sistem parametrləri -dür. Alisin gizli açarı olsun. Bob ona ədədini göndəribsə, onların ortaq məxfi açarını hesablayın.

1. CERT-in əsas xidmətləri

2. Rəqəmsal imza və məlumatı əlavə etməklə rəqəmsal imza modeli

3. İnformasiyanın toplanması. İnformasiya toplanmasının metodologiyası

4. DDoS-hücum alətləri

5. Diffi-Hellman açar mübadiləsi sxemində sistem parametrləri -dir. Bobun gizli açarı olsun. Alis ona ədədini göndəribsə, onların ortaq məxfi açarını hesablayın.

1. İnformasiya təhlükəsizliyi insidentlərinin emalı prosesləri

2. Sonlu dövri qruplar və diskret loqarifmləmə məsələsi

3. Şəbəkənin daranması. Daramanın növləri və metodologiyası

4. DDoS-hücumlardan müdafiə mexanizmləri

5. RSA alqoritmində -dür. açıq açarını hesablayın.

1. İnformasiya təhlükəsizliyi insidentlərinin emalı prosesləri

2. Əl-Gamal rəqəmsal imza sxemi

3. ICMP-darama. TCP- və UDP-zondlama

4. OWASP (Open Web Application Security Project) yanaşması – A01-A10:2021

5. RSA alqoritmində -dir. Açıq açar seçilibsə, gizli açarı hesablayın.

1. İnsident sübutlarının toplanması. İşıqfor protokolu

2. Elektron imza anlayışı

3. Şəbəkə inventarlaşdırılması və inventarlaşdırma üsulları

4. Veb sistemlərə hücumların əsas sinifləri

5. ElGamal imza sxemində , açıq açar olarsa, gizli açarını tapın.

1. “Narıncı kitab” və təhlükəsizlik səviyyələri

2. Açıq açarlar infrastrukturu (SXM, QM, istifadəçi, sertifikatlar bazası)

3. NetBIOS, SNMP, LDAP, NTP, SMTP inventarlaşdırma

4. SQL inyeksiyanın metodologiyası

5. ElGamal imza sxemində , açıq açar olarsa, gizli açarını tapın.

1. Audit planının işlənməsi. Audit yoxlamaları və məlumat toplanması

2. Açıq açarlar infrastrukturunun (Aİİ) arxitekturası

3. Boşluqların idarə edilməsinin həyat dövrü

4. SQL inyeksiyanın növləri

5. Eyler teoreminin köməyi ilə hesablayın: 5-1mod 26=?

1. ISO/IEC 15408 standartı

2. Rəqəmsal sertifikat və ona daxil olan sahələr

3. Boşluqlar üzrə məlumat mənbələri

4. Kibertəhlükəsizliyin auditi anlayışı

5. φ(*n*) = 192, *n*= *pq* verilib, burada *p*, *q* sadə ədədlərdir. *p*−*q* = 4 olarsa, *n*-ni tapın.

1. ISO/IEC 27001:2013 standartı

2. Diffi-Hellman açar mübadiləsi sxemi

3. Şəbəkənin daranması. Daramanın növləri və metodologiyası

4. İzlərin gizlədilməsi alətləri

5. RSA kriptosistemində açıqmətn Y=X3 mod 15 düsturu ilə şifrlənmişdir. Y=8 isə, X=?

1. Hədəfyönümlü hücumlar. APT-hücum kampaniyaları

2. Eyler funksiyası və onun əsas xassələr

3. Müdaxilələrin aşkarlanması sistemlərinin təsnifatı

4. Kompüter virusları və kompüter viruslarının təsnifatı

5. RSA kriptosistemində açıq mətn Y=X7 mod 15 düsturu ilə şifrlənmişdir. isə,

1. Anomaliyaların aşkarlanması metodları

2. RSA alqoritmi

3. Sosial mühəndislik üsulları

4. Troyanlar və onların təsnifatı

5. RSA kriptosistemində açıq açar kimi verilmişdir. Açıq mətn isə, şifrlənmiş mətni tapın.

1. 3A (Autentifikasiya, Avtorizasiya və Audit)

2. Rəqəmsal imza və məlumatı əlavə etməklə rəqəmsal imza modeli

3. Müdaxilələrin aşkarlanması sistemlərinin ümumi modeli

4. Soxulcanlar və onların təsnifatı

5. Diffi-Hellman açar mübadiləsi protokolunda sistem parametrləri p=11, g=2-dir. Alis , Bob isə gizli açarını seçərək protokol üzrə hesablamaları və ötürmələri ediblər. Ortaq məxfi açarı hesablayın.

1. Sızma testləri

2. Açarsız heş funksiyaların tərifi və xassələri. Heş funksiyaların iterativ modeli

3. Şəbəkə inventarlaşdırılması və inventarlaşdırma üsulları

4. DoS-hücumlar və üçsəviyyəli DDoS arxitekturası

5. Diffi-Hellman açar mübadiləsi protokolunda sistem parametrləri p=11, g=7-dir. Alis , Bob isə gizli açarını seçərək protokol üzrə hesablamaları və ötürmələri ediblər. Ortaq məxfi açarı hesablayın.

1. Müdaxilə anlayışı və sui-istifadələrin aşkarlanması metodları

2. SHA-2 heş funksiyaları və SHA-3 standartı

3. “Cyber kill chain” modeli

4. DDoS-hücumlara nümunələr

5. ElGamal imza sxemində *p* =19, *g* =10-dur və Alis *y*= 4 açıq açarı ilə *m* =14 məlumatını imzalayıb. İmza (15, 14) cütüdür. İmzanın doğruluğunu yoxlayın.

1. Konfidensial informasiya. Dövlət sirri

2. SHA-1 heş funksiyası

3. Toplanmış məlumatların analizi və audit hesabatının hazırlanması

4. SQL inyeksiyanın növləri

5. ElGamal imza sxemindən istifadə etməklə aşağıdakı parametrlər üçün imzanı hesablayin: *p* = 11, *g* = 2; gizli açar *x* =4, məlumat *m* =6 və *k*=3.

1. ISO/IEC 27001 standartına uyğunluğun auditi

2. Kriptoqrafik heş funksiayalar və onların növləri

3. Boşluqlar üzrə məlumat mənbələri

4. Kibertəhlükəsizliyin auditi anlayışı

5. ElGamal imza sxemində , gizli açar , açıqmətn -dir. Müvəqqəti açar seçilib və -dir. Rəqəmsal imza cütünü hesablayın.

1. Kibertəhlükəsizlik anlayışı. Kibertəhlükəsizliyin üç aspekti

2. Sadə ədədlərin generasiyası. Qüvvətin hesablanması alqoritmi

3. Audit planının işlənməsi. Audit yoxlamaları və məlumat toplanması

4. SQL inyeksiyanın metodologiyası

5. Eyler funksiyasının qiymətini hesablayın: