

Név:

Neptun kód:

| | | | | | | |
|----|----|----|----|----|----|----------|
| 1. | 2. | 3. | 4. | 5. | 6. | Σ |
| | | | | | | |

ADATBIZTONSÁG PÓTZÁRTHELYI

2010. május 13.

1. Tegyük fel, hogy DES rejtjelezést használtunk. A 64 bites üzenetblokkon belül, a blokk végén 4 bites hibadetekciós ellenőrzőösszeget alkalmazunk. Kimerítő kulcskereséses támadást végzünk. Elegendő lenne-e 12 rejtjeles blokk megfigyelése a gyakorlatilag egyértelmű kulcsazonosításhoz? (20 pont)

Igen Nem Magyarázat:

2. Tegyük fel, hogy A és B kölcsönösen azonosítani kívánják egymást, amelyet arra kívánnak alapozni, hogy ismerik egymás jelszavát (P_A, P_B).

a.) Biztonságos-e az alábbi protokoll? (15 pont)

1. $A \rightarrow B$: ID_A, k^P_A
2. $B \rightarrow A$: ID_B, k^P_B
3. $A \rightarrow B$: $z1 = E_B(P_A)$
4. $B \rightarrow A$: $z2 = E_A(P_B)$
5. A: $D_A(z2) = P_B ?$
- B: $D_B(z1) = P_A ?$

b.) Biztonságos-e a protokoll, ha A és B ismerik egymás nyilvános kulcsát, s nem kerül sor az 1-2. lépésekre? (10 pont)

(ID: azonosító, k^P : nyilvános kulcs, E, D: nyilvános kulcsú kódoló, dekódoló transzformáció)

2.a. Igen Nem Magyarázat:

2.b. Igen Nem Magyarázat:

3. Válaszoljon a következő kérdésekre!
- Hogyan működik az integritásvédelem a WEP protokollban? (4 pont)
 - Mutassa meg, hogyan tud a támadó tetszőleges módosítást végezni a WEP üzeneteken az integritásvédelem ellenére! (4 pont)
 - Hogyan védekezik a WEP az üzenet-visszajátszás ellen? (4 pont)
 - Tegyen javaslatot a visszajátszás elleni mechanizmus javítására! (4 pont)

4. Adott az alábbi tűzfal szabályhalmaz:

| | | | | |
|---|-----|---------------|----------------|--------|
| 1 | tcp | 10.1.1.0/25 | any | deny |
| 2 | udp | any | 192.168.1.0/24 | accept |
| 3 | tcp | 10.1.1.128/25 | any | deny |
| 4 | udp | 172.16.1.0/24 | 192.168.1.0/24 | deny |
| 5 | tcp | 10.1.1.0/24 | any | accept |
| 6 | udp | 10.1.1.0/24 | 192.168.0.0/16 | deny |
| 7 | udp | 172.16.1.0/24 | any | accept |

Keressen példát a következő inkonzisztenciatípusokra, és válaszát röviden indokolja!

- Shadowing (5 pont)
 - Generalization (5 pont)
 - Correlation (5 pont)
5. Válaszoljon a következő kérdésekre!
- A Bayes-tétel alapú spam szűrés milyen adatbázist tart nyilván? (3 pont)
 - Mondjon olyan hátrányt, ami miatt egy P2P botnet rosszabb egy centralizálttal szemben! (3 pont)
 - Mi a lényegi különbség egy csomagszűrő és egy application layer proxy között? (3 pont)
6. Van egy szerverünk, amely 4 kbyte méretű leveleket 3 db/sec sebességgel tud feldolgozni. A szerver egy 1024/1024 kbit/sec sebességű vonal végén van. Egy támadó folyamatosan leveleket küld a szerverre DoS támadási céllal, olyan sebességgel, hogy a szerver kapacitását pontosan 100%-ban kösse le. A levél átvitele során 20% overhead (többlet) keletkezik a TCP,IP átvitel miatt. Hány százalékában használja ki a támadó az ADSL letöltési irányú csatornáját a támadás közben? (15 pont)

Pontozás: 1: <=39, 2: 40 - 54, 3: 55 - 69, 4: 70 - 84, 5: 85 - 100