Adatbiztonság (VIHIM 100) 1.kZH **Név:**
2015.10.19.

Neptun kód:

Feladatok:

1) a) Definiálja a One Time Pad rejtjelezést! (2p)
b) Definiálja az optimalitási tulajdonságát! (3p)

2) a) Adja meg a CBC-MAC blokk rejtjelezési mód blokksémáját (kódolást és dekódolást)! (3p)
b) Adjon meg kettő biztonsági előnyt és kettő biztonsági hátrányt az adott mód esetén (röviden fejtse is ki azokat)! (2p)

3) Sorolja fel és értelmezze a digitális és az analóg aláírás közös biztonsági tulajdonságait! (5p)

4) a)A CIA hármasban milyen biztonsági fogalmakat takarnak a kezdőbetűk? (4p)
b) Az SSH1 támadásnál a támadó az ismert nyilvános kulccsal saját titkosított csomagot illesztett az adatok közzé. Kifigyelte, hogyha megismétli a csomagot, akkor az ellenőrző összeg sem romlik el. A leírt támadás esetén a CIA hármasból melyik elem sérült? (2p)

5) Intel X86 szegmens védelem esetén a támadó meg szeretne változtatni egy memória területet, ahová ő nem írhat. Ezért megkéri a nagy privilégiummal futó kódot (operációs rendszert), hogy az adott területre olvasson be adatokat. Hogyan védték ki ezt a helyzetet?
(4p)

6) a) Ismertesse a kanári (stack ellenőrzéses) módszer működését! (4p)
b) Érték szerint milyen kanári típusokat ismer? (2p)
c) Hogyan lehet ezt a védelmet kijátszani? (2p)

Pontozás: **1**: 1-12 p **2**: 13-18 p **3**: 19-24 p **4**: 25-29 p **5**: 30-33 p

Megoldások:

1)
a) Előadás slide.
b) Előadás slide.

2)
a) Előadás slide.
b) Előadás slide és az ott hivatkozott tankönyvi részlet.

3) Előadás slide.

4)
a) ***C****onfidential – bizalmasság vagy titkosság,* ***I****ntegrity - sértetlenség (integritás),****A****vailability - rendelkezésre állás.*
b) *sértetlenség*

5) *Request Priveleg Level bevezetésével.*
Hozzáférés engedélyezett, ha max(CPL; RPL) <= DPL. Tehát ha a hívónak joga volt az adott területre írni, akkor ez a nagyobb privilégiummal rendelkező kódnak is engedélyezett

6)
a) *Érzékeny információ van a kanári előtt, így a visszatérési címet nem kell felülírni.*
b) *Konstans, terminátor (olyan konstans érték, amelyet nem tudunk bevinni), véletlen, véletlen XOR művelettel (hogy függvényhívásonként más értéke legyen.)*
c) *SEH vagy függvénypointer (virtuális pointer) támadásával, mivel az indirekt hívás még a visszatérés, azaz a kanári érték ellenőrzése előtt lefut.*