2006. tavasz – **2**. vizsga **2**. rész név:

Vizsgafeladatok *hálózatok biztonsága* tárgyból

Figyelem! A kérdések közül 2 pont értékűt áthúzhat! Csak az **első át nem húzott 20 pont értékű** kérdésre adott válaszait vesszük figyelembe! Ha már rendelkezik ebből a részből korábban elfogadott (legalább 12 pontos) eredménnyel, akkor amennyiben ezt a feladatlapot értékelésre beadja, **ezen a vizsgán ez számít**! Amennyiben ebből a részből a 12 pontot eléri, az eredményét a következő vizsgára tovább viheti, ha a másik rész sikertelen.

1. Adja meg a tűzfal definícióját! (1 pont)

2. Milyen előnye van a proxy tűzfalnak az állapottartó csomagszűrővel szemben? Miért? (1 pont)

3. Miért volt szükség a transzparens proxytűzfalak létrehozására? (1 pont)

4. Milyen veszélyt rejt magában, ha egy DMZ-ben több szerver is található? (0.5 pont) Hogyan védekezne ellene? (0.5 pont)

5. Proxy tűzfal esetén miért nem kell a válaszcsomagokkal foglalkozni? (1 pont)

6. Hogyan épül fel a syslog.conf fájl egy sora, és ezek mit jelentenek? (2 pont)

7. Soroljon fel az Zorp tűzfalrendszer legfontosabb jellemzőiből 5 darabot (5x0.2 pont)

8. Rendelkezésére áll 3 db PC, hogy Zorp tűzfalrendszert készítsen belőle. Melyiket mire használja? (Több jó megoldás is lehetséges!) Megoldását indokolja! (Milyen szempontok alapján választotta azt?) (2 pont)

9. Biztonsági szempontból miért előnytelen az inetd szuperszerver használata? (1 pont)

2006. tavasz – **2**. vizsga **2**. rész név:

10. Ellenőrizze, hogy gépén milyen nyitott portok találhatók! Legyen gondos! (1 pont)

11. Egy biztonságos Linux rendszer kialakításakor milyen szempontok merülnek fel a partíciókkal kapcsolatban? (2 pont)

12. Mikor jelent biztonsági előnyt, ha egy szerveren nincs fejlesztői környezet? (1 pont)

13. Nevezzen meg egy biztonsági szempontból hasznos kernel patch-et és adja meg, hogy mire jó! (1 pont)

14. Adjon meg 5 szempontot (tanácsot), amit mentésekkel kapcsolatban fontosnak tart! (5x0.2 pont)

15. Miért (mihez) van szükség UML futtatásakor a gazdagépen kerneltámogatásra? (1 pont)

16. Milyen tulajdonságokkal kell rendelkeznie egy jó jelszónak? (1 pont)

17. Rendszergazdaként mit tehetünk annak érdekében, hogy egy esetleges betörés esetén észrevegyük, ha a támadó bizonyos programokat lecserélt? Legalább 3-at írjon! (1 pont)

18. Rendszergazdaként mit tehetünk a távolról kihasználható biztonsági rések kihasználásának a megelőzésére? Legalább 3-at írjon! (1 pont)

19. Mutasson be egy webes biztonsági rést, és adjon kielégítő módszert a megelőzésére! (1 pont)