2006. tavasz név:

II. ZH *hálózatok biztonsága* tárgyból

Figyelem! A kérdések közül 2 pont értékűt áthúzhat! Csak az **első 20 pont értékű át nem húzott** kérdésre adott válaszait vesszük figyelembe! Ahhoz, hogy a ZH a vizsgába beszámítson, legalább a pontok 60%-át, azaz 12 pontot kell megszerezni. A zárthelyi megírása, sőt beadása sem kötelező. Ez csak egy lehetőség, de ugyanakkor csak egy lehetőség, pótZH nem lesz. A be nem adott vagy gyenge eredményű ZH nem jelent hátrányt a vizsgán, sőt a beszámíthatóság határát elérő ZH esetén is a hallgató dönti el, hogy kéri-e a ZH eredmény beszámítását vagy sem.

1. Mutassa meg a lényeges különbséget a kapcsolatok szempontjából az állapottartó csomagszűrő és a proxytűzfal között! (1 pont)

2. Nevezzen meg 5 konkrét tűzfalat! (1 pont)

3. Az ún. „hardver tűzfalak” gyártói milyen biztonsági előnyt tulajdonítanak a terméküknek? Miért kétes értékű ez? (1 pont)

4. Mit tud a Zorp OS-ről? (1 pont)

5. Miért szükséges a /etc/passwd fájl mellett a /etc/shadow fájl használata? (1 pont)

6. Egy biztonságos Linux rendszer kialakításakor mit célszerű külön partícióra tenni? Ezeket milyen opciókkal célszerű felmountolni? (elérhető: 5x (0.1+0.3) pont, azaz max. 2 pont)

7. Egy cég szerver és tűzfal rendszerének a kialakítását kell megoldania. Rendelkezésére áll 5db PC. Milyen szolgáltatásokat mire telepít fel? Legyen kreatív! (2 pont)

8. Miben nyújt többet a syslog-ng a syslognál? (1 pont)

9. Milyen érvek szólnak (biztonsági szempontból) a saját Linux kernel fordítása mellett? És ellene? (2x1 pont)

10. Mi az a busybox? (1pont)

11. Mit jelent (hogyan lehet) a User-Mode Linuxot biztonsági céllal használni? (1 pont)

12. A biztonsági szempontokon kívül milyen egyéb szempontokat tud felsorakoztatni az UML biztonsági célú használata mellett? (rendelkezésre állási, gazdasági, környezetvédelmi) (1 pont)

13. Milyen más hasonló virtualizációs megoldásokat ismer az UML-en kívül? (1 pont)

14. Mit tárolna LDAP címtárban? Soroljon fel legalább 3-at! (Legyenek értelmesek!) (1 pont)

15. Miért nem szabad vakon bízni a titkosított kapcsolatokban? (1 pont)

16. Mutasson be egy programozói hibát, amit ki lehet használni a format string attack támadással! Hogyan lehet kihasználni? (2 pont)

17. A WPA milyen authentikációs megoldásokat használ? (2db elég) (1 pont)

18. Mit tud a *mandatory access control*ról? (1 pont)