

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. Definiálja a tűzfal feladatát! (1 pont)

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

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

4. Mi az a demilitarizált zóna és mire használják? (1 pont)

5. Ha egy Unix rendszerben /etc/shadow fájlt használunk, van-e szükség a /etc/passwd fájlra is? (0.2 pont)
Válaszát indokolja! (0.8 pont)

6. Mi a különbség a NAT és a NAPT között? (Ezt már tavaly tanulták, de idén is tudni kell!) (1 pont)

7. A gyakorlatban mire használható a netfilter/iptables? (legalább 3-at kérek az 1 pontért)

8. Miért célszerű külön napló szerveret használni? (1 pont)

9. Sorolja fel a Zorp tűzfalrendszer legfontosabb elemeit a feladataikkal együtt (4db)!(2 pont)

10. Adjon meg egy-egy olyan Linux disztribúciót, amelyiket biztonsági szempontból jónak illetve rossznak tart!
(1 pont)

11. Az **nmap localhost** parancs használatával nem talált a szerverén nyitott portot. Mit állíthat (és mit NEM) ekkor a szerveréről biztonsági szempontból? (1 pont)
12. Állapítsa meg egy Unix paranccsal, hogy melyik program figyel a 70-es porton! (1 pont)
13. Soroljon fel 5 opciót, amit Unix alatt partíciók felmountolásakor használhatnak, és mindegyiknél adja meg a jelentését is! (1 pont)
14. Miért célszerű külön szerverre tenni a hálózati szolgáltatásokat (pl. webszerver, DNS, stb.) és az interaktív felhasználókat? (1 pont)
15. Milyen szempontok/érvek merülnek fel az operációs rendszer és/vagy program frissítések feltelepítésével kapcsolatban? (1 pont)
16. Mi a különbség a VMware és az UML között? (mi az, amit csinál; lehetőségek; teljesítmény; ár) (2 pont)
17. Milyen programozói hibára van szüksége a túlsordulásos támadáshoz? (0.5 pont) Hogyan lehet kihasználni? (1.5 pont)
18. PHP esetén milyen veszélyt rejt magában az a megoldás, ha az URL-ben fájlnevet fogadunk el? (pl. egy menüpontot a megfelelő aloldalt leíró fájl nevének URL-beli megadásával érhetünk el) (1 pont)
19. Mire (hol) érdemes IPS-t használni és mire (hol) nem? (1 pont)