

Tételsor

1. A „biztonság” szó jelentése számítógépes környezetben. Fizikai biztonság, a szerverszoba kialakítása. Szoftver biztonság, jellemző biztonsági problémák. Adatbiztonság, mentés és archiválás. A szolgáltatás biztonsága, rendelkezésre állás.
2. A biztonság, a költségek, a teljesítmény és a kényelem kapcsolata. A támadók és a támadások típusai, védekezési módok.
3. A titkosítás alapfogalmai. Titkosítási modell. Klasszikus rejtjelezések. Caesar-féle rejtjelezés, k-eltolás, általános egyábécés rejtjelezések, keverő kódok és az egyszer használatos bitminta.
4. Számítógépes titkosítások napjainkban és a múltban. A redundancia és a frissesség szerepe a kriptográfiában. Szimmetrikus kulcsú titkosítások. DES és 3DES algoritmusok.
5. Titokmegosztás, a szimmetrikus kulcsok problémái. Nyilvános kulcsú titkosítások, a nyilvános és titkos kulcsok egyéb felhasználási lehetőségei. Az RSA algoritmus. A Diffie-Hellmann kulcscsere.
6. Jelszavak, jelszavak kezelése. A felhasználói jelszavakkal szemben támasztott követelmények, jelszavak védelme. Néhány a felhasználó jelszavak tesztelésére és ellenőrzésére szolgáló alkalmazás bemutatása.
7. A RAID funkciója, típusai, működése. A RAID szintek bemutatása működés, tárolókapacitás, redundancia szempontjából. A RAID erősségei és gyenge pontjai.
8. A hálózat felosztása tűzfalak segítségével. Külső és belső hálózatok, DMZ. Tűzfalmegoldások topológia szerint. Állapotkövető és állapotmentes tűzfalak összehasonlítása.
9. Védett és nem védett kimenő hálózati kapcsolatok. Az SSH lehetőségeinek rövid bemutatása. Az SSH hitelesítés folyamata. Hitelesítés SSH kulcsokkal, az SSH kulcsok előnyei és hátrányai, gyakorlati felhasználási területek.
10. Az e-mailek szerepének változása. Elektronikus levelek biztonságos kezelése, tárolása. Visszaélési lehetőségek, biztonsági problémák az e-mailekkel kapcsolatban. E-mail üzenetek titkosítása, biztonságos kapcsolatok a levelező szerverrel. SMTP szerverek.
11. Hálózati állományrendszerek általános jellemzése. Állományok azonosítása, elnevezése, az elhelyezkedés függetlenség elve. Leképzési táblák. A távoli eljárashívások és a helyi átmeneti tárák működésének, előnyeinek, hátrányainak összehasonlítása. Elosztott fájlrendszerek sebessége, teljesítménye.
12. Állapotmentes és állapottartó kiszolgálók. Az NFS és az AFS fájlrendszerek felépítése, működése.
13. A hálózati operációs rendszerek legfontosabb elemeinek bemutatás a Windows 2000/2003 Server (vagy más) termékcsalád legfontosabb jellemzői és szolgáltatásai alapján.
14. Statikus és dinamikus csatornakiosztás a közegelési alrétegben. ALOHA és réselt ALOHA. A CSMA és CSMA/CD jellemzése. A Manchester kódolás bemutatása egy példán keresztül. Az Ethernet ütközéskezelési technikája. Kapcsolás Ethernet hálózatokban.
15. A DIX és az IEEE 802.3 keretformátum részletes bemutatása és összehasonlítása. A 802.3u és a 802.3z Ethernet szabványok kialakulása, működése, felhasználása. Az egyes szabványok lehetséges átviteli közegei.

16. Sebesség és hatékonyság az Ethernet hálózatokban. A szórási és ütközési tartományok szerepe, jelentősége, kialakítása a gyakorlatban. Üzenetszórás a második rétegben. Szórási vihar.
17. A vezeték nélküli adatátvitel lehetséges megoldásainak (látható és nem látható fénnnyel történő átvitel, rádiófrekvenciás átvitel) bemutatása, előnyök, hátrányok ismertetése. Az IrDA és Bluetooth szabványok bemutatása.
18. A 802.11a/b/g szabványok részletes bemutatása. A használni kívánt szabvány kiválasztásának szempontjai. A WLAN hálózatok hardverei. WLAN topológiák és felhasználási területeik.
19. WLAN biztonsági problémák és megoldások. A WLAN biztonság fokozásának lehetőségei. WEP hitelesítés és titkosítás. A WEP gyengeségei, lehetséges támadási pontok. Élet a WEP után, a 802.11i, a WPA és a WPA2 áttekintése. Az IEEE 802.1x hitelesítés lépései.
20. Mobil adatátvitel. A CSD és HSCSD átvitel alapjai, jellemzői. Csomagkapcsolt mobil átvitel, a GPRS és a működési osztályok paraméterei. Az EDGE szabvány. Harmadik generációs szabványok, UMTS és HSDPA. Az egyes technológiák összevetése sebesség, költség és felhasználási lehetőségek alapján.
21. A rendszerfelügyelet alapvető feladatai és eszközei. Gyakorlati megoldások linux és/vagy Windows környezetben.