Államvizsga témakörök

Hálózatok biztonsága (TA83) tárgyhoz

2008. június

- **Alapfogalmak, alapvető támadások**
  passzív és aktív támadások, csomag szintű támadások, hálózati szintű támadások, social engineering típusú támadások
- **Rosszindulatú programok és támadások jellemrajza**
  férgek, vírusok (boot sector, program, macro), trójai faló, e-mail (lánclevelek, spam, vírusos csatolt file-ok, phising (adathalászat)), összetett fenyegetések, 0 day gap
- **Kriptográfia I.**
  alapfogalmak, titkos kulcsú blokk kódolók: DES, 3DES, AES. Blokktitkosítási üzemmódok
- **Kriptográfia II.**
  nyilvános kulcsú titkosítás (algoritmusok: RSA, DSA, PGP; mire lehet használni)
- **Biztonságos átvitel**
  SSL infrastruktúra (ssh, scp, https), VPN
- **Tűzfalak**
  alapfogalmak, tűzfalak fejlődése, fajtái, iptables, Zorp
- **Behatolás észlelés, megelőzés IDS, IPS**
- **UNIX Szerverek biztonsági kérdései**
  /etc/passwd, inetd, rendszer kialakítása (partíciók kiosztása, fejlesztői környezet hiánya, szolgáltatások és interaktív szerverek külön, külön napló (log) szerver), frissítések, user mode Linux, ACL, chroot, jail

- **Támadási lehetőségek**
  Programozói hibák kihasználása (C nyelven), UNIX vagy Linux szerver adminisztrálási hibáiból adódó betörések, jelszavak helyes megválasztása, szótáras törés. Miért nem szabad vakon bízni a titkosított kapcsolatokban? Webes biztonsági rések.

Dr. Lencse Gábor
egyetemi docens