Tanulmányi követelmények

Hálózatok biztonsága (TA83) tárgyhoz

2006/2007. tanév 2. félév

Előtanulmányi feltétel: Számítógép-hálózatok (ta37)

A tananyaghoz rendelt kreditpont: 4

A tanterv szerinti óraszámok: 3 kontakt óra, 1 konzultációs óra, 1 óra önálló tanulásra

A tárgy kontakt óráit előadások töltik ki az órarend szerint. A konzultációs órák keretében a hallgatók laboratóriumi foglalkozásokon vesznek részt egyéni feliratkozás alapján.

A félévben elhangzó főbb témakörök:

- Bevezetés: a tárgy témaköre, alapfogalmak, hálózati támadások fajtái (aktív és passzív). Csomag szintű támadások (IP spoofing, Smurf, SYN flood, Xmas/Ymas), hálózati szintű támadások (switch-ek elleni támadás, ARP poisoning, ICMP redirect, RIP távolságvektor hamisítás, source route IP opció, DNS (cache) ellen való támadás), social engineering típusú támadások (DNS átregisztráció, jelszó megkérdezése, gyenge jelszavak)
- Rosszindulatú programok és támadások jellemrajza. Férgek, vírusok (boot sector, program, macro), trójai faló, rejtekajtó, bomba. E-mail: spam, vírusos csatolt file-ok, phising (adathalászat), lánclevél, piramisjáték, hoax „e-mail-mint-vírus”. Összetett fenyegetések, biztonsági rések egyre gyorsabb kihasználása: 0 day gap protection
- Kriptográfiai bevezető, történet, alapfogalmak, titkos kulcsú blokk kódolók: DES, 3DES, AES. Kulcs menedzsment (kulcsgenerálás, -tárolás, -továbbítás). Nyilvános kulcsú titkosítás (algoritmusok: RSA, DSA), kriptográfiai hash függények (MD5, SHA). Blokktitkosítási üzemmódok. Kriptográfiai protokollok: üzenethitelesítés, digitális aláírás, kulcscsere protokollok, partnerhitelesítés. Nyilvános kulcsú infrastruktúra.
- Biztonságos átvitel: SSL/TLS infrastruktúra és alkalmazásai. SSL/TLS, OpenSSL, OpenSSH (ssh, scp, X11 forwarding), az s végű protokollok (pl. https). VPN: a VPN értelmezése/fajtái, az IPsec protokollcsalád, FreeS/WAN és Openswan.
- PGP: A digitális boríték elve, a PGP kulcsgondozása, a PGP használata.
- Tűzfalak: alapfogalmak, fejlődésük (portszűrés, állapottartó csomagszűrő, ALF). Netfilter (iptables), Zorp.
- Behatolás észlelése és kezelése. IDS (Snort, LIDS kernel patch, honeypot), IPS.
- UNIX Szerverek biztonsági kérdései: /etc/passwd, inetd, szolgáltatások felderítése. Egy bizonságos rendszer kialakítása (partíciók kiosztása, fejlesztői környezet hiánya, szolgáltatások és interaktív szerverek külön, külön napló (log) szerver, kernel fordítás, frissítések, mentések, dokumentáció). ACL, chroot, jail. A user mode Linux és biztonsági alkalmazása.
- Központosított felhasználó menedzsment: NIS, NIS+, LDAP címtár
- Gyakorlati dolgok: valamely támadások megvalósítása, puffer túlcsordulás (C-ben), UNIX vagy Linux szerver adminisztrálási hibáiból adódó betörések, jelszavak helyes megválasztása, szótáras törés. Miért nem szabad vakon bízni a titkosított kapcsolatokban? Webes biztonsági rések.
- Vezeték nélküli hálózatok biztonsági kérdései.

Kötelező irodalom:

- Lencse Gábor: Hálózatok biztonsága (béta verziójú jegyzet, elérhető a tárgy honlapján)
- A tárgy honlapja a http://www.tilb.sze.hu szerveren érhető el. A lapot a hallgatóknak rendszeresen látogatniuk kell, rajta találhatók: oktatási segédanyagok, mérési utasítások, hirdetmények.

Ajánlott irodalom:

1. Buttyán Levente, Vajda István: „Kriptográfia és alkalmazásai”, Typotex, Budapest, 2004.
2. Simson Garfinkel, Gene Spafford & Alan Schwartz: „Practical Unix & Internet Security”, Third Edition, O'Reilly, Sebastopol, CA, USA, 2003,
3. Vir V. Phoha: „Internet Security Dictionary” Springer, New York, NY, USA, 2002.
4. Virrasztó Tamás: „Titkosítás és adatrejtés” NetAcademia Kft., 2004.
5. http://www.google.co.hu ;-)

Félévi követelmények:

Az előadásokon való részvétel nem kötelező, de erősen ajánlott.
A laborgyakorlatokon való részvétel kötelező. **Aki 30%-nál többet hiányzik, a tárgyból aláírást nem kaphat.** A gyakorlatok időpontját külön órarend rögzíti. A hallgatók a gyakorlatokra megadott időpontok valamelyikére előre jelentkeznek. A félév során elsajátított gyakorlati anyagból ellenőrző mérésen kell beszámolni. Az ellenőrző mérésre a hallgatóknak előzetesen jelentkezniük kell. Sikertelen ellenőrző mérés pótlására egy lehetőség van. **Aki május 10-én 12:00 óráig az ellenőrző mérést legalább elégséges szinten nem tejesíti, a tárgyból aláírást nem kaphat.**

A félév során előre meghirdetett időpontokban, összesen 2 alkalommal a hallgatók zárthelyi dolgozatot **írnak**. **Az ZH-k egyenkénti legalább 2-es érdemjegye az aláírás megszerzésének szükséges feltétele!** (Pótlásra ZH-nként 1-1 lehetőség van.)

Mivel a tárgy félévközi számonkérésű, aki az aláírást megszerezte, az egyben legalább elégséges osztályzatot is kap, aki az aláírást nem szerezte meg, annak további pótlási lehetősége nincs!

A félév végi jegy kiszámítása:

$$J=40\%ZH_1+40\%ZH_2+20\%EM$$

Ahol:

J	Félév végi jegy
ZH_i	Az i. ZH osztályzata
E	Ellenőrző mérés osztályzata

De minden egyes komponensnek önmagában is legalább elégségesnek kell lennie!

Győr, 2007. február 4.

Dr. Lencse Gábor
egyetemi docens
/tantárgyfelelős/