SZÉCHENYI ISTVÁN EGYETEM
MŰSZAKI TUDOMÁNYI KAR
INFORMATIKAI ÉS VILLAMOSMÉRNÖKI INTÉZET
TÁVKÖZLÉSI TANSZÉK

TANTÁRGYPROGRAM	
VILLAMOSMÉRNÖKI SZAK TÁVKÖZLÉS-INFORMATIKA SZAKIRÁNY	TAGOZAT: NAPPALI
A tantárgy tantervi címe: **HÁLÓZATOK BIZTONSÁGA**	**Az oktatásért felelős tanszék:** **Távközlési Tanszék**
A tantárgy kódja: **NGB_TA028_1**	**Tantárgy ekvivalencia** Ekvivalens tárgy(ak) kódja(i): N_TA83
Tantárgyfelelős neve: **Dr. Lencse Gábor**	Érvényesség (max): 2008. december 31.
A tantárgyprogramot készítette: **Dr. Lencse Gábor**	**Eredeti dátum: 2005. május 4.** **Utolsó módosítás: 2009. február 10.**

1. A tantárgy szerepe a szakképzés céljának megvalósításában:

Számítógép-hálózatok biztonsági kérdéseinek feltárása, tudatosítása, az alapvető támadási és védekezési módszerek megismertetése, elemzése. A hallgatók képesek legyenek egy adott intézmény biztonsági kérdéseit elemezni, megoldásra javaslatot adni; legyenek tudatában a javasolt megoldások és saját ismereteik korlátainak.

2. A tantárgy témájának szakmai háttere, indokoltsága:

A tárgy keretében a hallgatók megismerik a kriptográfia alapfogalmait, a lehetséges támadások típusait. Betekintést nyernek a nyilvános és titkos kulcsú titkosítási eljárásokba és a legfontosabb kriptográfiai protokollokba. Elsajátítják a tűzfalakkal kapcsolatos alapvető ismereteket és gyakorolják valamely tűzfal (pl. Zorp) telepítését és beállítását. A tárgy része még a VPN elmélete és megvalósítása dedikált hálózati eszközökkel, illetve szoftverrel, valamint a szerverek biztonsági kérdései.

3. Tantárgyi jellemzők:

Oktatott félévek száma: 1				KREDITPONT: 4			
Javasolt tanrendi hely	Félévi követelmény				Oktatási félév		
6. félév	vizsga	Folyamatos számonkérés	ötfokozatú beszámoló	háromfokozatú beszámoló	páros	páratlan	mind-kettő
Törzsanyag							
Kötelezően választható	x				x		
Szabadon választható							

HETI ÓRASZÁM				
Kontakt óra			konzultációs óra	önálló hallgatói munkaóra
Elmélet	gyakorlat	labor		
2		2		1

Előtanulmányi feltételek (legfeljebb 3 tantárgy, vagy egy modul):

számítógép-hálózatok (NGB_TA007_1)

Erősen ajánlottak még, mert nélkülük a hallgatóknak gondja lehet a tárgy követelményeinek teljesítésével:

hálózati operációs rendszerek I., protokollok és szoftverek, kommunikációs rendszerek programozása

4. Tanagyag tartalma oktatási hétre bontva:

Az alábbi táblázatok csak tájékoztató jellegűek, a tananyag ütemezése változhat!

Az előadások anyaga:

Okt. hét	Témakör
1.	Bevezetés: a tárgy témaköre, alapfogalmak, hálózati támadások fajtái
2.	Rosszindulatú programok és támadások jellemrajza: férgek, vírusok trójai faló, e-mail (spam, vírusos csatolt file-ok) phising (adathalászat), összetett fenyegetések.
3.	Kriptográfiai bevezető, történet, alapfogalmak, titkos kulcsú blokk kódolók: DES, 3DES
4.	nyilvános kulcsú titkosítás (algoritmusok: RSA, DSA, PGP; mire lehet használni)
5.	Biztonságos átvitel: SSL infrastruktúra (ssh, scp, https),
6.	VPN (IPSec)
7.	Tűzfalak: alapfogalmak (portszűrés, állapottartó csomagszűrő, ALF), IPTABLES
8.	Zorp alapok, Zorp proxitűzfal beállítása
9.	Behatolás észlelés, megelőzés IDS, IPS
10.	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
11.	Támadások bemutatása: puffer túlcsordulás (C-ben), UNIX vagy Linux szerver adminisztrálási hibáiból adódó betörések,
12.	jelszavak helyes megválasztása, szótáras törés. Miért nem szabad vakon bízni a titkosított kapcsolatokban? Webes biztonsági rések.
13.	A félév elején oktatott hálózati támadások demonstrációja
14.	Adatmentés. (meghívott előadó)

A laborfoglalkozások anyaga

Okt. hét	Témakör
1.	RAID rendszerek, LVM
2.	Levelező rendszerek biztonsága, Postfix-amavis-clamav
3.	Apache 2 webszerver SSL beállítása
4.	IPtables kicsit mélyebben, az ideális tűzfal megtervezése
5.	User Mode Linux létrehozása, konfigurálása
6.	Wifi kártyák beállítása, ndiswrapper
7.	OpenVPN konfigurálás
8.	chroot, jailing technikák
9.	weblapok biztonsága
10.	WEP, WPA, WPA2, a vezeték nélküli hálózatok biztonsága
11.	Jelszóbiztonság, JTR
12.	Támadási technikák (külső előadó)
13.	Ellenőrző mérés
14.	Pótmérés

Kötelező irodalom:

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:

Buttyán Levente, Vajda István: „Kriptográfia és alkalmazásai” Typotex, Budapest, 2004
Virrasztó Tamás: „Titkosítás és adatrejtés” NetAcademia Kft., 2004.
Simson Garfinkel, Gene Spafford & Alan Schwartz: Practical Unix and Internet security, O’Reilly, 3rd ed. 2003.
Vir V. Phoha: Internet Security Dictionary, Springer-Verlag, New York, 2002.
Eris Cole, Ronald Krutz and James W. Conley: Network Security Bible, Wiley Publishing, Inc. Indianapolis, Indiana, 2005.
W. Stallings: Cryptography and Network Security, 3rd ed. Prentice Hall, 2003.
RFC 2828: Internet Security Glossary

5. Félévközi hallgatói munka:

Követelmény:

Az előadásokon való részvétel nem kötelező, de erősen ajánlott, mert a tárgyhoz jelenleg még nem létezik olyan jegyzet, amely a tárgy anyagát teljes egészében lefedné.
A laborgyakorlatokon való részvétel erősen ajánlott. A gyakorlatokon szereplő ismeretek is a tárgy anyagának részét képezik! 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 a szorgalmi időszak utolsó napján 12:00 óráig az ellenőrző mérést legalább elégséges szinten nem tejesíti, a tárgyból aláírást nem kaphat.**

A félév során 2-3 alkalommal a hallgatók zárthelyi dolgozatot **írhatnak**. Ezek megírása nem kötelező, és pótlási lehetőség sincs. A ZH-k eredménye a vizsga anyagát és eredményét nagy mértékben befolyásolja! (Amely témakörből a hallgató legalább elégséges ZH-t írt, és annak beszámítását kéri, abból a hallgatónak kevesebb feladatot kell vizsgán megoldania.)

A félév vizsgával zárul. A vizsgára bocsátás feltétele a megszerzett aláírás. A vizsgára a NEPTUN rendszeren keresztül jelentkezni kell.
A vizsga három részből áll. Aki az első részben ("kis kérdések") nem érte el a 60%-ot, annak vizsgajegye elégtelen, a továbbiakban nem vesz részt. (A félévközi ZH-k legalább elégséges eredménye ezen rész alól ad mentesítést.) A második rész ("feladatmegoldás") is írásbeli, majd ezt követi a szóbeli, ahol az előző két rész értékelése - az első részben a 60% el nem érése miatt kapott elégtelen kivételével - a hallgató teljesítménye alapján felülbírálható.

Értékelés módja:

A vizsgajegybe beszámítjuk a félév közben végzett munkát is.

$$V=70\%H+30\%E$$

Ahol:

V	Vizsgajegy
H	A háromrészes vizsgán nyújtott teljesítmény értékelése
E	Ellenőrző mérés osztályzata

De minden egyes komponensnek önmagában is legalább elégségesnek kell lennie.

6. A tantárgy oktatásának személyi és tárgyi feltételei

Előadó: Dr. Lencse Gábor egyetemi docens
Mérésvezető: Kovács Ákos tanszéki mérnök
Laborfoglalkozások: L1-7 Távközlés-informatika Labor

Dr. Borbély Gábor tanszékvezető	Dr. Lencse Gábor tantárgyfelelős