



TANTÁRGYPROGRAM	
VILLAMOSMÉRNÖKI SZAK	TAGOZAT: NAPPALI
TÁVKÖZLÉS-INFORMATIKA, INFOKOMMUNIKÁCIÓ SZAKIRÁNY	
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 Érvényesség (max): 2008. december 31.
Tantárgyfelelős neve: Dr. Lencse Gábor	
A tantárgyprogramot készítette: Derka István	Eredeti dátum: 2005. május 4. Utolsó módosítás: 2011. február 02.

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	öt fokozatú beszámoló	három fokozatú beszámoló	páros	páratlan	mindkettő
Törzsanyag								
Kötelezően választható		x				x		
Szabadon választható								
HETI ÓRASZÁM								
Kontakt óra			konzultációs óra			önálló hallgatói munkaóra		
Elmélet	gyakorlat	labor				1		
2		2						
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. Tananyag 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) phishing (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),
6-7.	VPN – várhatóan a jegyzeten túlmenő mélységben!
8.	Tűzfalak: alapfogalmak (portszűrés, állapotartó csomagszűrő, ALF), IPTABLES
9-10.	Zorp alapok, Zorp proxítűzfal beállítása (várhatóan meghívott előadóval!)
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.	Zárthelyi
14.	Behatolás észlelés, megelőzés IDS, IPS

A laborfoglalkozások anyaga

Okt. hét	Témakör
1.	RAID rendszerek, LVM
2.	Levelező rendszerek biztonsága, Postfix-amavis-clamav
3.	Apache 2 webservert 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 található: oktatási segédanyagok, mérési utasítások, hirdetések.

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 teljesíti, a tárgyból aláírást nem kaphat.**

A félév során egy alkalommal a hallgatók **zárthelyi dolgozatot írnak**. Ennek megírása kötelező, és egy pótlási lehetőség van. **A ZH legalább elégséges teljesítése az aláírás szükséges feltétele!**

Az ellenőrző mérés és a zárthelyi dolgozat pótlására - az előbbieken túlmenően – még IV jelleggel sincs lehetőség! Aki valamelyik félévközi követelményt nem tudja teljesíteni – a pótlási lehetőségek igénybevételének ellenére sem – az aláírás megtagadva bejegyzést kap!

A félév **szóbeli vizsgával** zárul. A vizsgára bocsátás feltétele a megszerzett aláírás. A vizsgára a NEPTUN rendszeren keresztül jelentkezni kell.

Értékelés módja:

A vizsgajegybe beszámítjuk a félév közben végzett munkát is.

$$V=25\%ZH+25\%E+50\%Sz$$

Ahol:

V	Vizsgajegy
Sz	Szóbeli vizsgán mutatott teljesítmény
E	Ellenőrző mérés osztályzata
ZH	ZH osztályzata

De minden egyes komponensnek önmagában is legalább elégségesnek kell lennie!

6. A tantárgy oktatásának személyi és tárgyi feltételei

Előadó: Derka István, egyetemi tanársegéd

Mérésvezető: Kovács Ákos tanszéki mérnök

Laborfoglalkozások: L1-7 Távközlés-informatika Labor

Dr. Borbély Gábor
tanszékvezető

Dr. Lencse Gábor
tantárgyfelelős