



TANTÁRGYPROGRAM	
VILLAMOSMÉRNÖKI SZAK	TAGOZAT: NAPPALI
TÁVKÖZLÉS-INFORMATIKA 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
Tantárgyfelelős neve: Dr. Lencse Gábor	
A tantárgyprogramot készítette: Dr. Lencse Gábor, Répás Sándor	Eredeti dátum: 2005. május 4. Utolsó módosítás: 2015. február 2.

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 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), Hálózati operációs rendszerek (NGB_TA047_1), Kommunikációs rendszerek programozása (NGB_TA024_1)							

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, RAID
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 (RSA, DSA, PGP, PKI, CA)
5.	Levelezés biztonsága (DKIM, SPF, szűrés, titkosítás, aláírás)
6.	VPN
7.	Biztonsági eszközök (Tűzfalak, Proxyk, IDS, IPS, WAF)
8.	Hálózati eszközök biztonsága (NTP, SYSLOG, RADIUS, Switch)
9.	Webes alkalmazások biztonsága (Vendég előadó)
10.	WiFi biztonság, Linux szerverek biztonsági kérdései
11.	Mentés, archiválás, Windows rendszerek biztonsága
12.	<i>TMDK miatt oktatási szünet</i>
13.	2. ZH , Jogszabályok, biztonsági szabványok, ajánlások, minősítések
14.	ZH-k pótlása

A laborfoglalkozások anyaga

Okt. hét	Témakör
1.	RAID alkalmazása Linux rendszereken
2.	OpenVPN telepítés
3.	Windows adathordozó titkosítás
4.	E-mail titkosítás, digitális aláírás
5.	Vírus, SPAM szűrés, Postfix, amavis, clamav
6.	MySQL alapok
7.	1. ZH
8.	pfSense vagy Squid telepítése, beállítása
9.	Webes alkalmazások támadása (Vendég előadó)
10.	Cisco switch hardening
11.	Windows tűzfal, víruskeresés, mentés, visszaállítás
12.	<i>TMDK miatt oktatási szünet</i>
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 adatretjtés” 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 félév során elsajátított gyakorlati anyagból ellenőrző mérésen kell beszámolni.** Sikertelen ellenőrző mérés pótlására egy lehetőség van. Aki az ellenőrző mérést legalább elégséges szinten nem teljesíti, a tárgyból aláírást nem kaphat.

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

A félév vizsgával zárul. A vizsgára bocsátás feltétele a megszerzett aláírás. A vizsgára a NEPTUN rendszeren keresztül jelentkezni kell, kivétel, ha valaki megajánlott jegyet kapott, és szeretné azt elfogadni. (Megajánlott jegy esetén a vizsgára való jelentkezés egyben a megajánlott jegy elutasítását is jelenti!)

A vizsga írásbeli.

Értékelés módja:

Ha a ZH-k átlaga legalább 4.0, akkor megajánlott jegy kapható a következők szerint:

$$V=40\%ZH1+40\%ZH2+20\%E$$

Vizsga esetén:

$$V=80\%Sz+20\%E$$

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: Répás Sándor, PhD hallgató

Mérésvezető: Répás Sándor, PhD hallgató

Laborfoglalkozások: L1-7 Távközlés-informatika Labor

Répás Sándor
PhD hallgató

Dr. Lencse Gábor
tantárgyfelelős