

Tárgytematika / Course Description

Hálózatok biztonsága

NGM_TA016_1

Tárgyfelelős neve /

Teacher's name: Répás Sándor Rudolf

Félév / Semester: 2017/18/2

Beszámolási forma /

Assesment: Vizsga

Tárgy heti óraszám /

Teaching hours(week): 3/1/0

Tárgy féléves óraszám /

Teaching hours(sem.): 0/0/0

OKTATÁS CÉLJA / AIM OF THE COURSE

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. A tárgy része még a VPN elmélete és megvalósítása dedikált hálózati eszközökkel, illetve szoftverrel, valamint a szerverek biztonsági kérdései.

TANTÁRGY TARTALMA / DESCRIPTION

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.

Oktatási szünet

10.

Webes alkalmazások biztonsága

11.

WiFi biztonság, Linux szerverek biztonsági kérdései

12.

Mentés, archiválás, Windows rendszerek biztonsága

13.

2. ZH, Jogszabályok, biztonsági szabványok, ajánlások, minősítések

14.

ZH-k pótlása

SZÁMONKÉRÉSI ÉS ÉRTÉKELÉSI RENDSZERE / ASSESSMENT'S METHOD

Követelmény:

A félév során a hallgatók két előre kitűzött időpontban zárthelyi dolgozatot írnak. Ezek megírása kötelező, és pótlási lehetőség nincs, mivel az aláírás szükséges feltétele legalább egy elégséges ZH.

Kedvezmény:

Amely témakörből a hallgató legalább közepes ZH-t írt, és annak beszámítását kéri, abból a témakörből a vizsga első részét ("kis kérdések") kiválthatja.

Értékelés módja:

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

A vizsga két részből áll.

1. Az első rész az ún. "kis kérdések", itt mindkét ZH témakörében külön-külön 60%-ot kell elérni az elégségeshez. Aki valamely témakörből nem éri el ezt a szintet, annak vizsgajegye elégtelen, a vizsga további részében nem vehet részt. (A félévközi ZH-k legalább közepes eredménye ezen rész alól ad mentesítést.)

2. A második rész az ún. "feladatmegoldás" is írásbeli, ennek teljesítése csak az elégségesnél jobb vizsgajegy megszerzésében segít. (Az első részben elért pontokhoz a második rész pontjai hozzáadódnak.)

KÖTELEZŐ IRODALOM / OBLIGATORY MATERIAL

Kötelező irodalom:

Lencse Gábor: Hálózatok biztonsága, 2010. (elektronikus jegyzet, elérhető a tárgy honlapján)

A tárgy honlapja: http://www.tilb.sze.hu/cgi-bin/tilb.cgi?0=m&1=targyak&2=NGM_TA016_1

A lapot a hallgatóknak rendszeresen látogatniuk kell, rajta található az oktatási segédanyagok és a tárgy fontos hirdetései.

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