

## Tárgytematika

### Hálózatok biztonsága

NGB\_TA028\_1

Tárgyfelelős neve: Derka István

Félév: 2014/15/2

Beszámolási forma: Vizsga

Tárgy heti óraszám: 2/0/2

Tárgy féléves óraszám: 0/0/0

### OKTATÁS CÉLJA

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.

### TANTÁRGY TARTALMA

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.

### SZÁMONKÉRÉSI ÉS ÉRTÉKELÉSI RENDSZERE

#### 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 vizsgajegybebeszámítjuk 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!***

---

## KÖTELEZŐ IRODALOM

### **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