FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Babeş-Bolyai Cluj-Napoca
1.2 Facultatea	Facultatea de Matematică şi Informatică
1.3 Departamentul	Departamentul de Informatică
1.4 Domeniul de studii	Informatică
1.5 Ciclul de studii	Master
1.6 Programul de studiu / Calificarea	Baze de date

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)	Protocoale de securitate în comunicaţii Security protocols in communications						
2.2 Titularul activităţilor de curs	Lect. Dr. Bufnea Darius-Vasile						
2.3 Titularul activităţilor de seminar	Lect. Dr. Bufnea Darius-Vasile						
2.4 Anul de studiu	1	2.5 Semestrul	2	2.6. Tipul de evaluare	E	2.7 Regimul disciplinei	Obligatorie
2.8 Codul disciplinei	MMR8001						

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1 Număr de ore pe săptămână	3	Din care: 3.2 curs	2	3.3 seminar/laborator	1
3.4 Total ore din planul de învăţământ	42	Din care: 3.5 curs	28	3.6 seminar/laborator	14
Distribuţia fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie şi notiţe					35
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					45
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					30
Tutoriat					13
Examinări					10
Alte activităţi:					0

3.7 Total ore studiu individual	133
3.8 Total ore pe semestru	175
3.9 Numărul de credite	7

4. Precondiţii (acolo unde este cazul)

4.1 De curriculum	• Arhitectura Calculatoarelor, Sisteme de operare, Reţele de calculatoare, Programare Web, Aritmetică modulară şi criptografie
4.2 De competenţe	• Cunoştinţe elementare despre structura şi modul de funcţionare a reţelei Internet, cunoştinţe elementare de criptografie, sisteme de operare, arhitectura calculatoarelor, baze de date, programare web, modelul client-server, algoritmică şi programare

5. Condiţii (acolo unde este cazul)

5.1 De desfăşurare a cursului	• Sală de curs dotată cu videoproiector

5.2 De desfăşurare a seminarului/laboratorului	•

6. Competenţele specifice acumulate

Competenţe profesionale	• Capacitate avansată de modelare a fenomenelor şi proceselor specifice din domenii economice, industriale şi ştiinţifice, folosind cunoştinţe fundamentale din matematică, statistică şi informatică • Capacitate avansată de analiză, proiectare şi construcţie a sistemelor informatice, folosind o gamă variată de platforme hardware şi software, limbaje şi medii de programare şi instrumente de modelare, verificare şi validare • Modelarea si conceptualizarea modelelor de proiectare / implementare pentru sisteme distribuite şi baze de date. • Dezvoltarea de aplicaţii pe arhitecturi masiv paralele (cloud computing, structuri grid) şi a comunicaţiilor în timp real, mobile computing, wireless, bluetooth etc. • Conceperea şi utilizarea de modele pentru formalizarea conceptului de web semantic. • Capacitatea de a preda elevilor din ciclul liceal concepte şi teorii specifice informaticii, în măsura în care titularul diplomei de disertaţie în informatică posedă un certificat de absolvire a modulului de pregătire pedagogică
Competenţe transversale	• Cunoaşterea aprofundată a dezvoltărilor teoretice, metodologice şi practice specifice informaticii • Utilizarea sistematică a cunoştinţelor de specialitate în informatică la modelarea şi interpretarea unor situaţii noi, în contexte de aplicare mai largi decât cele cunoscute • Cunoaşterea şi utilizarea integrată a aparatului conceptual şi metodologic specific informaticii pentru soluţionarea unor situaţii incomplet definite, pentru rezolvarea unor probleme teoretice şi practice noi • Utilizarea nuanţată şi pertinentă a criteriilor şi metodelor de verificare, validare şi evaluare a soluţiilor software realizate, capacitatea de a formula judecăţi de valoare şi de a fundamenta deciziile constructive • Elaborarea şi conducerea de proiecte software complexe, de natură practică sau de cercetare, utilizând un spectru larg de metode cantitative şi calitative • Capacitate avansată de comunicare în medii profesionale diferite, de utilizarea adecvată a vocabularului informatic în comunicarea profesională, în limba engleză • Capacitate de lucru în echipă, asumarea de roluri de execuţie şi de conducere, realizarea sarcinilor profesionale în condiţii de autonomie şi responsabilitate

7. Obiectivele disciplinei (reieşind din grila competenţelor acumulate)

7.1 Obiectivul general al	Cursul îşi propune aprofundarea de către cursant a celor mai bune

disciplinei	mecanisme de securitate care pot fi implementate şi utilizate la elaborarea unui protocol, în Internet, la nivelul unui sistem de calcul şi în elaborarea unei aplicaţii software.
7.2 Obiectivele specifice	Cursul grupează câteva subiecte avansate din domeniul securităţii în reţele de calculatoare. Cursul este structurat pe baza arhitecturii TCP/IP de organizare a reţelelor de calculatoare, aspectele teoretice orientându-se spre fiecare nivel şi set de protocoale din cadrul stivei TCP/IP. Cursul îşi propune: • să prezinte şi familiarizeze studentul cu algoritmii de criptare cei mai des întâlniţi precum şi cu diferitele protocoalele de la diverse nivele din stiva TCP/IP ce implementează aceşti algoritmi; • o prezentare exhaustivă a principalelor aspecte ale criptografiei aplicate în Internet, în special ale criptografiei cu cheie publică şi privată; • să familiarizeze studentul cu cele mai grave vulnerabilităţii în domeniu, precum şi cu mecanismele şi măsurile de luptă împotriva acestor vulnerabilităţi; • să prezinte cursanţilor principalele provocări de securitate pe care le ridică comerţul electronic pe Internet; • să abordeze din punct de vedere legal şi moral diferite subiecte precum infracţionalitatea pe Internet şi intimitatea utilizatorului; • să contribuie la înţelegerea acestor domenii prin studierea şi dezvoltarea unor aplicaţii practice relevante.

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii
1. Prezentarea bibliografiei şi structurii cursului. Cerinţe şi evaluare. Vulnerabilităţi informatice. Politici şi aspecte de securitate informatică la diferite nivele ale stivei TCP/IP.	Expuneri, explicaţii, exemple, studii de caz	
2. Istoria atacurilor informatice. Malware (clasificare). Virusologie. Anatomia unui virus informatic. Sisteme antivirus. Spyware şi addware. Aplicaţii ale acestora în e-commerce. Reţele de tip Botnet.	Expuneri, explicaţii, exemple, studii de caz	
3. Vulnerabilităţi informatice. Securitatea sistemelor de operare.	Expuneri, explicaţii, exemple, studii de caz	
4. Securitatea sistemelor server în Internet. Arhitecturi de securitate în reţelele Enterprise.	Expuneri, explicaţii, exemple, studii de caz	
5. Securitatea reţelelor locale. Mecanisme firewall (host based, router based). Network & host scanning. Tipuri de scanări.	Expuneri, explicaţii, exemple, studii de caz	
6. Atacuri locale şi atacuri remote. Escaladarea de privilegii. DDOS, flood.	Expuneri, explicaţii, exemple, studii de caz	
7. Buffer overflow. Anatomia unui exploit. Shell-code.	Expuneri, explicaţii, exemple, studii de caz	
8. Securitatea aplicaţiilor Web. SQL Injection. SMTP Injection. Cross Site Scripting. CSRF. Unrestricted file upload.	Expuneri, explicaţii, exemple, studii de caz	
9. Algoritmi de criptare bazaţi pe chei publice şi chei private. Semnături digitale. Certificate digitale.	Expuneri, explicaţii, exemple, studii de caz	

10. Infrastructuri bazate pe chei publice şi servicii asociate acestora.	Expuneri, explicaţii, exemple, studii de caz	
11. Securitatea poştei electronice. DKIM. Mecanisme antispam: bayesian spam filters, DNS based black lists. PGP.	Expuneri, explicaţii, exemple, studii de caz	
12. Protocoale de securitate la nivel reţea si transport. IPSec. SSL si TLS. VPN	Expuneri, explicaţii, exemple, studii de caz	
13. Securitate la nivel fizic şi legătura de date.	Expuneri, explicaţii, exemple, studii de caz	
14. Vulnerabilităţi de tip Social Engineering. Infracţionalitatea informatică. Asigurarea intimităţii utilizatorului (user privacy).	Expuneri, explicaţii, exemple, studii de caz	

Bibliografie

1. F. Cohen, A Short Course on Computer Viruses, Wiley Professional Computing, 2nd edition, 1994
2. Michael Sikorski, Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 2012
3. Peter Kim, The Hacker Playbook 2: Practical Guide To Penetration Testing, CreateSpace, 2015
4. Martin Boldt, Privacy-Invasive Software, cap. 2, cap. 7, Blekinge Institute of Technology, ISBN 978-91-7295-100-6
5. Michal Zalewski, Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks, No Starch Press, 2005
6. Michael Hale Ligh, Andrew Case, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, John Wiley & Sons, 2014
7. Chris Sanders, Jason Smith, Applied Network Security Monitoring: Collection, Detection, and Analysis, Syngress, 2013
8. Shon Harris, Allen Harper, Gray Hat Hacking, Second Edition: The Ethical Hacker's Handbook, McGraw-Hill Osborne, 2008
9. Michal Zalewski, The Tangled Web: A Guide to Securing Modern Web Applications, No Starch Press, 2011
10. Michael A. Davis and Sean M. Bodmer, Hacking Exposed Malware and Rootkits: Malware and Rootkits Secrets and Solutions, McGraw-Hill Education, 2009
11. Michael Gregg, The Network Security Test Lab: A Step-by-Step Guide, John Wiley & Sons, 2015
12. William Stallings, Network Security Essentials: Applications and Standards, Pearson, 5th edition, 2013
13. Stuart Mcclure, Joel Scambray, Hacking Exposed 7: Network Security Secrets and Solutions, McGraw-Hill Education, 7th edition, 2012
14. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 6th edition 2013
15. Gordon Fyodor Lyon, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, Nmap Project, 2009
16. Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security: Private Communication in a Public World, Prentice Hall, 2002
17. Eric Cole, Ronald L. Krutz, James Conley, Brian Reisman, Mitch Ruebush, Dieter Gollmann, Rachelle Reese, Network Security Fundamentals, John Wiley & Sons, 2008
18. Michael J. Stewart, Network Security, Firewalls and VPNs, Jones & Bartlett Learning, 2nd edition, 2013
19. Timur Mehmet, Firewall Hacking Secrets For Security Professionals, HackerStorm, 2015
20. Oskar Andreasson, Iptables Tutorial, http://www.frozentux.net/iptables-tutorial/iptables-tutorial.html
21. Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, John Wiley & Sons, 2nd edition, 2011
22. Jon Erickson, Hacking: The Art of Exploitation, No Starch Press, 2nd edition, 2008
23. Vancea, Al. si altii, Programarea in limbaj de asamblare 80x86, Exemple si aplicatii, pag. 317-323, Ed. Risoprint, 2005
24. Klaus Schmeh, Cryptography and Public Key Infrastructure on the Internet, Wiley, 2007

25. Johannes A. Buchmann, Evangelos Karatsiolis, Introduction to Public Key Infrastructures, Springer, 2013
26. V. V. Patriciu, M. Ene-Pietrosanu, C. Vaduva, I. Bica, N. Voicu, Securitatea Comerţului Electronic, Editura ALL
27. V. V. Patriciu, M. Ene-Pietrosanu, I. Bica, J. Priescu, Semnături Electronice şi Securitate Informatică, Editura ALL, 2006
28. Sharon Conheady, Social Engineering in IT Security: Tools, Tactics, and Techniques: Testing Tools, Tactics & Techniques, McGraw-Hill Education, 2014
29. Christopher Hadnagy, Paul Wilson, Social Engineering: The Art of Human Hacking, John Wiley & Sons, 2010

8.2 Seminar / laborator	Metode de predare	Observaţii
1. Vulnerabilităţi informatice. Virusologie. Anatomia unui virus informatic. Sisteme antivirus.	Dezbaterea, dialogul, exemple, conversaţii de aplicare	Seminarul se desfăşoară din două în două săptămâni
2. Exploit-uri. Shell-code.	Dezbaterea, dialogul, exemple, conversaţii de aplicare	
3. Mecanisme Firewall.	Dezbaterea, dialogul, exemple, conversaţii de aplicare	
4. Securitatea aplicaţiilor Web	Dezbaterea, dialogul, exemple, conversaţii de aplicare	
5. Algoritmi de criptare bazaţi pe chei publice şi chei private. Semnături digitale. Certificate digitale.	Dezbaterea, dialogul, exemple, conversaţii de aplicare	
6. Securitatea poştei electronice	Dezbaterea, dialogul, exemple, conversaţii de aplicare	
7. Protocoale de securitate la nivel reţea şi transport.	Dezbaterea, dialogul, exemple, conversaţii de aplicare	

Bibliografie

1. 1 Justin Pot: A History of Computer Viruses & The Worst Ones of Today;
2. Jeremy Paquette: A History of Viruses;
3. Moheeb Abu Rajab, Lucas Ballard, Panayiotis Mavrommatis, Niels Provos, Xin Zhao: The Nocebo* Effect on theWeb: An Analysis of Fake Anti-Virus Distribution;
4. Martin Boldt: Privacy-Invasive Software, cap. 2, cap. 7;
5. Steve Hanna: Shellcoding for Linux and Windows Tutorial;
6. Writing shellcode;
7. Lisa Bogar: SUID, SGID;
8. Vivek Gite, Explain Linux / UNIX TCP Wrappers, 2009;
9. Port Scanning – How a Port Scan Works;
10. James Messer: Secrets of Network Cartography: A Comprehensive Guide to nmap;
11. TCP Idle Scan;
12. V. V. Patriciu: Semnaturi electronice si infrastructuri de securitate, notiţe de curs, 2009, Master Sisteme Distribuite în Internet, Univ. Babeş-Bolyai;
13. DomainKeys Identified Mail (DKIM);
14. OpenSSL: The Open Source toolkit for SSL/TLS, www.openssl.org;
15. Steve Friedl: An Illustrated Guide to IPsec.

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului

- Cursuri cu un conţinut similar există în planul de învăţământ al tuturor marilor universităţi din România şi din străinătate.
- Cursul abordează probleme fundamentale de securitate şi deosebit de actuale în Internet.
- Conţinutul cursului acoperă principalele aspecte necesare a fi însuşite de către cursant pentru a ocupa cu succes o poziţie corespunzătoare în cadrul unei companii de profil.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Cunoaşterea principalelor aspecte teoretice prezentate la curs	Examen parţial din prima jumătate a materiei	1/4
	Cunoaşterea principalelor aspecte teoretice prezentate la curs	Examen final din a doua jumătate a materiei	1/4
10.5 Seminar/laborator	Elaborarea unor referate şi a unor proiecte pe teme de securitate stabilite de comun acord de cursant cu cadrul didactic dintre cele discutate la seminar.	Susţinere orală de către cursant	1/2
10.6 Standard minim de performanţă			
Pentru promovare trebuie cumulate următoarele două condiţii: • prezentarea de referate şi proiecte, activitate ce trebuie notată cel puţin cu nota 5; • minim media 5 între nota examenului parţial şi cea obţinuta la examenul din sesiune.			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
.....	Lect. Dr. Bufnea Darius-Vasile	Lect. Dr. Bufnea Darius-Vasile

Data avizării în departament

.....

Semnătura directorului de departament

….....