

FI A DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Babe -Bolyai Cluj-Napoca
1.2 Facultatea	Facultatea de Matematică și Informatică
1.3 Departamentul	Departamentul de Informatică
1.4 Domeniul de studii	Informatică
1.5 Ciclu de studii	Master
1.6 Programul de studiu / Calificarea	Baze de date

2. Date despre disciplină

2.1 Denumirea disciplinei	Protocoloale de securitate în comunicații						
2.2 Titularul activităților de curs	Lect. Dr. Bufnea Darius-Vasile						
2.3 Titularul activităților 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

3. Timpul total estimat (ore pe semestru al activităților 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 învățământ	42	Din care: 3.5 curs	28	3.6 seminar/laborator	14
Distribuția fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie și notițe					35
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					45
Pregătire seminar/laboratoare, teme, referate, portofolii și eseuri					33
Tutoriat					10
Examinări					10
Alte activități:					0
3.7 Total ore studiu individual	133				
3.8 Total ore pe semestru	175				
3.9 Numărul de credite	7				

4. Precondiții (acolo unde este cazul)

4.1 De curriculum	<ul style="list-style-type: none"> Arhitectura Calculatoarelor, Sisteme de operare, Rețele de calculatoare, Programare Web, Aritmetică modulară și criptografie
4.2 De competențe	<ul style="list-style-type: none"> Cunoștințe elementare despre structura și modul de funcționare a rețelei Internet, cunoștințe elementare de criptografie, sisteme de operare, arhitectura calculatoarelor, baze de date, programare web, modelul client-server, algoritmică și programare

5. Condiții (acolo unde este cazul)

5.1 De desfășurare a cursului	<ul style="list-style-type: none"> Sală de curs dotată cu videoproiector
5.2 De desfășurare a seminarului/laboratorului	<ul style="list-style-type: none">

6. Competențele specifice acumulate

Competențe profesionale	<ul style="list-style-type: none"> • Dezvoltarea de aplicații bazate pe baze de date în Internet • Întreținerea site-urilor Web • Dezvoltarea de aplicații pentru e-commerce
Competențe transversale	<ul style="list-style-type: none"> • Însușirea de către student a algoritmilor de criptare cei mai des întâlniți precum și a diferitelor protocoale de la diverse nivele din stiva TCP/IP ce implementează acești algoritmi • Însușirea de către student a celor mai grave vulnerabilități în domeniu, precum și cu mecanismele de securitate și măsurile de luptă împotriva acestor vulnerabilități • Însușirea de către cursant a cerințelor de securitate legate de comerțul electronic pe Internet precum și a mecanismelor de securitate necesare a fi puse în practică în domeniu

7. Obiectivele disciplinei (reie îndin din grila competențelor acumulate)

7.1 Obiectivul general al disciplinei	Cursul își propune aprofundarea de către cursant a celor mai bune mecanisme de securitate care pot fi implementate și utilizate la elaborarea unui protocol, în Internet, la nivelul unui sistem de calcul, în elaborarea unei aplicații software.
7.2 Obiectivele specifice	<p>Cursul grupează câteva subiecte avansate din domeniul securității în rețele de calculatoare. Cursul este structurat pe baza arhitecturii TCP/IP de organizare a rețelelor de calculatoare, aspectele teoretice orientându-se spre fiecare nivel și set de protocoale din cadrul stivei TCP/IP. Cursul își propune:</p> <ul style="list-style-type: none"> • să prezinte și familiarizeze studentul cu algoritmi de criptare cei mai des întâlniți precum și cu diferitele protocoale de la diverse nivele din stiva TCP/IP ce implementează acești algoritmi; • să familiarizeze studentul cu cele mai grave vulnerabilități în domeniu, precum și cu mecanismele și măsurile de luptă împotriva acestor vulnerabilități; • să prezinte cursanților principalele provocări de securitate pe care le ridică comerțul electronic pe Internet; • să abordeze din punct de vedere legal și moral diferite subiecte precum infracționalitatea pe Internet și intimitatea utilizatorului; • să contribuie la înțelegerea acestor domenii prin studierea și dezvoltarea unor aplicații practice relevante.

8. Conținuturi

8.1 Curs	Metode de predare	Observații
1. Prezentarea bibliografiei și structurii cursului. Cerințe și evaluare. Vulnerabilități informatice. Politici de securitate informatică la diferite nivele ale stivei TCP/IP.	Expuneri, explicații, exemple, studii de caz	
2. Istoria atacurilor informatice. Virusologie. Anatomia unui virus informatic. Sisteme antivirus.	Expuneri, explicații, exemple, studii de	

	caz	
3. Securitatea sistemelor de operare. Securitatea sistemelor server în Internet. Arhitecturi de securitate în rețelele Enterprise. Atacuri locale și atacuri remote. Spyware și addware. Aplicații ale acestora în e-commerce.	Expuneri, explicații, exemple, studii de caz	
4. Anatomia unui exploit. Shell-code. Exemple.	Expuneri, explicații, exemple, studii de caz	
5. Mecanisme Firewall.	Expuneri, explicații, exemple, studii de caz	
6. Securitatea aplicațiilor Web. SQL Injection. JavaScript Injection. SMTP Injection. Cross Site Scripting.	Expuneri, explicații, exemple, studii de caz	
7. Algoritmi de criptare bază și pe chei publice și chei private. Semnături digitale. Certificate digitale.	Expuneri, explicații, exemple, studii de caz	
8. Infrastructuri bazate pe chei publice și servicii asociate acestora.	Expuneri, explicații, exemple, studii de caz	
9. Securitatea poștei electronice. DKIM. Mecanisme antispam: bayesian spam filters, DNS based black lists. PGP.	Expuneri, explicații, exemple, studii de caz	
10. Protocoale de securitate la nivel rețea și transport. IPSec. SSL și TLS. Securitate la nivel fizic și legătura de date.	Expuneri, explicații, exemple, studii de caz	
11. Vulnerabilități de tip Social Engineering. Infracționalitatea informatică. Asigurarea intimității utilizatorului.	Expuneri, explicații, exemple, studii de caz	
12. Smartcard-uri. Biometrice.	Expuneri, explicații, exemple, studii de caz	
13. Securitate în sistemul bancar și plăți electronice în Internet.	Expuneri, explicații, exemple, studii de caz	
14. Mecanisme și scheme de autentificare. Kerberos.	Expuneri, explicații, exemple, studii de caz	

Bibliografie

1. V. V. Patriciu, M. Ene-Pietrosanu, C. Vaduva, I. Bica, N. Voicu, Securitatea Comerțului Electronic, Editura ALL
2. V. V. Patriciu, M. Ene-Pietrosanu, I. Bica, J. Priescu, Semnături Electronice și Securitate Informatică, Editura ALL, 2006
3. Stallings William, Cryptography and Network Security, Prentice Hall, 1999
4. Oskar Andreasson, Iptables Tutorial, <http://www.frozentux.net/iptables-tutorial/iptables-tutorial.html>
5. F. Cohen, A Short Course on Computer Viruses, Wiley Professional Computing, 2 edition, April 1994
6. Mostafa Hashem, Protocols for Secure Electronic Commerce, CRC Press, 2004
7. B. Gladman, C. Ellison, N. Bohm, Digital Signatures, Certificates and Electronic Commerce, <http://jya.com/bg/digsig.pdf>
8. O'Mahony D., Electronic Payment Systems for E-Commerce, Artech House, 2001
9. Ford W., Secure Electronic Commerce, Prentice Hall, 2001
10. Weidong Kou, Payment Technologies for E-Commerce, Springer Verlag 2003
11. Vancea, Al. și alții, Programarea în limbaj de asamblare 80x86, Exemple și aplicații, pag. 317-323, Ed. Risoprint, 2005

12. Martin Boldt, Privacy-Invasive Software, cap. 2, cap. 7, Blekinge Institute of Technology, ISBN 978-91-7295-100-6		
8.2 Seminar / laborator	Metode de predare	Observa ii
1. Vulnerabilit i informatice. Virusologie. Anatomia unui virus informatic. Sisteme antivirus.	Dezbaterea, dialogul, exemple, conversa ii de aplicare	Seminarul se desf oar din dou în dou s pt mâni
2. Exploit-uri. Shell-code.	Dezbaterea, dialogul, exemple, conversa ii de aplicare	
3. Mecanisme Firewall.	Dezbaterea, dialogul, exemple, conversa ii de aplicare	
4. Securitatea aplica iilor Web	Dezbaterea, dialogul, exemple, conversa ii de aplicare	
5. Algoritmi de criptare baza i pe chei publice i chei private. Semn turi digitale. Certificate digitale.	Dezbaterea, dialogul, exemple, conversa ii de aplicare	
6. Securitatea po tei electronice	Dezbaterea, dialogul, exemple, conversa ii de aplicare	
7. Protocoale de securitate la nivel re ea i transport.	Dezbaterea, dialogul, exemple, conversa ii de aplicare	
Bibliografie		
1. E. Rescorla, HTTP Over TLS, RFC 2818, May 2000		
2. Kerberos: The Network Authentication Protocol, http://web.mit.edu/Kerberos/		
3. T. Ylonen, C. Lonvick, The Secure Shell (SSH) Protocol Architecture, RFC 4251, January 2006		
4. P. Hoffman, SMTP Service Extension for Secure SMTP over TLS, RFC 2487, January 1999		
5. OpenSSL: The Open Source toolkit for SSL/TLS, www.openssl.org		
6. T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346, April 2006		
7. S. Kent, Security Architecture for the Internet Protocol, RFC 2401, S. Kent, R. Atkinson		

9. Coroborarea con inuturilor disciplinei cu a tept rile reprezentan ilor comunit ii epistemice, asocia iilor profesionale i angajatori reprezentativi din domeniul aferent programului

<ul style="list-style-type: none"> • Cursuri cu un con inut similar exist în planul de înv mânt al tuturor marilor universit i din România i din str in tate. • Cursul abordeaz probleme fundamentale de securitate i deosebit de actuale în Internet. • Con inutul cursului acoper principalele aspecte necesare a fi însu ite de c tre cursant pentru a ocupa cu succes o pozi ie corespunz toare 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 final
10.4 Curs	Cunoa terea principalelor aspecte teoretice prezentate la curs	Examen par ial din prima jum tate a materiei	1/4
	Cunoa terea principalelor aspecte teoretice prezentate la curs	Examen final din a doua jum tate a materiei	1/4
10.5 Seminar/laborator	Elaborarea unui referat i a unui proiect pe o tem de securitate stabilit de	Sus inere oral de c tre cursant	1/2

	comun acord de cursant cu cadrul didactic dintre cele discutate la seminar.		
10.6 Standard minim de performan			
Pentru promovare trebuie cumulate urm toarele dou condi ii:			
<ul style="list-style-type: none"> • prezentarea referatului i a proiectului, activitate ce trebuie notat cel pu in cu nota 5; • minim media 5 între nota examenului par ial i cea ob inuta la examenul din sesiune. 			

Data complet rii

.....

Semn tura titularului de curs

Lect. Dr. Bufnea Darius-Vasile

Semn tura titularului de seminar

Lect. Dr. Bufnea Darius-Vasile

Data aviz rii în departament

.....

Semn tura directorului de departament

.....