

FIȘA DISCIPLINEI

Protocoale de securitate în comunicații

Anul universitar 2025-2026

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea Babeș-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 studii / Calificarea	Securitate cibernetică
1.7. Forma de învățământ	Cu frecvență

2. Date despre disciplină

2.1. Denumirea disciplinei		Securitate Web și în Internet				Codul disciplinei	MME8194
2.2. Titularul activităților de curs			Conf. dr. Darius-Vasile BUFNEA				
2.3. Titularul activităților de seminar			Conf. dr. Darius-Vasile BUFNEA				
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	4	din care: 3.2. curs	2	3.3. seminar/ laborator/proiect	1/0/1
3.4. Total ore din planul de învățământ	56	din care: 3.5. curs	28	3.6 seminar/laborator/proiect	28
Distribuția fondului de timp pentru studiul individual (SI) și activități de autoinstruire (AI)					ore
Studiul după manual, suport de curs, bibliografie și notițe (AI)					25
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					25
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii și eseuri					20
Tutoriat (consiliere profesională)					14
Examinări					10
Alte activități					0
3.7. Total ore studiu individual (SI) și activități de autoinstruire (AI)				94	
3.8. Total ore pe semestru				150	
3.9. Numărul de credite				6	

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	Arhitectura Calculatoarelor, Sisteme de operare, Rețele de calculatoare, Programare Web, Aritmetică modulară și criptografie
4.2. de competențe	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	Sală de curs dotată cu videoproiector
5.2. de desfășurare a seminarului/ laboratorului	Sală de curs dotată cu videoproiector

6.1. Competențele specifice acumulate¹

¹ Se poate opta pentru competențe sau pentru rezultatele învățării, respectiv pentru ambele. În cazul în care se alege o singură variantă, se va șterge tabelul aferent celeilalte opțiuni, iar opțiunea păstrată va fi numerotată cu 6.

Competențe profesionale/esențiale	- Capacitate avansată de analiză, proiectare și construcție securizată a sistemelor informatice, folosind o gamă variată de platforme hardware și software, limbaje și medii de programare și instrumente de modelare, verificare și validare. - Însușirea unei baze teoretice și practice solide în cea ce privește problematica comunicării prin medii nesigure precum și utilizarea protocoalele securizate în Internet.
Competențe transversale	- Aplicarea regulilor de muncă organizată și eficientă, responsabilitate și seriozitate față de munca depusă atât individual cât și în echipă. - Comunicare în limba engleză.

6.2. Rezultatele învățării

Cunoștințe	- Studentul/absolventul cunoaște cele mai bune mecanisme de securitate care pot fi implementate în Internet. - Studentul/absolventul cunoaște algoritmi matematici cei mai des folosiți în criptografie precum și cele mai importante protocoale din cadrul stivei TCP/IP ce implementează acești algoritmi. - Studentul/absolventul cunoaște principalele aspecte ale criptografiei aplicate în Internet, în special ale criptografiei cu cheie publică și privată. - Studentul/absolventul cunoaște cele mai populare tipuri de atacuri cibernetice care se pot desfășura în Internet și are cunoștințe despre modul de evitare a unor asemenea atacuri.
Aptitudini	- Studentul/absolventul este capabil să dezvolte sisteme software securizate. - Studentul/absolventul este capabil să identifice posibilele probleme de securitate în sistemele software. - Studentul/absolventul este capabil să utilizeze tehnicile de securitate în dezvoltarea sistemelor software. - Studentul/absolventul dobândește abilitățile de a utiliza diverse instrumente în procesul de testare pentru identificarea vulnerabilităților software. - Studentul/absolventul este capabil să proiecteze și să implementeze instrumente de verificare a securității.
Responsabilități și autonomie	- Studentul/absolventul își asumă responsabilitatea pentru produsul muncii sale, solicită feedback și îl utilizează constructiv. - Studentul/absolventul este capabil să coordoneze activități de management de proiect, folosindu-se de abilități de decizie, de gândire critică și inovativă, precum și de abilități digitale. - Studentul/absolventul este în măsură să ofere consultanță de specialitate și să elaboreze materiale de specialitate. - Studentul/absolventul utilizează strategii, metode și tehnici eficiente de învățare pe tot parcursul vieții, în vederea (auto)formării, (auto)dezvoltării personale și profesionale continue.

7. Obiectivele disciplinei (reieșind 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 și în elaborarea unei aplicații software.
--	--

7.2 Obiectivele specifice	• 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: ○ să prezinte și familiarizeze studentul cu algoritmii de criptare cei mai des întâlniți precum și cu diferitele protocoale de la diverse nivele din stiva TCP/IP ce implementează acești algoritmi; ○ o prezentare exhaustivă a principalelor aspecte ale criptografiei aplicate în Internet, în special ale criptografiei cu cheie publică și privată; ○ 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 și aspecte de securitate informatică la diferite nivele ale stivei TCP/IP.	Expuneri, explicații, exemple, studii de caz	
2. Istoria atacurilor informatice. Malware (clasificare). Virusologie. Anatomia unui virus informatic. Sisteme antivirus. Spyware și addware. Aplicații ale acestora în e-commerce. Rețele de tip Botnet.	Expuneri, explicații, exemple, studii de caz	
3. Vulnerabilități informatice. Securitatea sistemelor de operare.	Expuneri, explicații, exemple, studii de caz	
4. Securitatea sistemelor server în Internet. Arhitecturi de securitate în rețelele Enterprise.	Expuneri, explicații, exemple, studii de caz	
5. Securitatea rețelelor locale. Mecanisme firewall (host based, router based). Network & host scanning. Tipuri de scanări.	Expuneri, explicații, exemple, studii de caz	
6. Atacuri locale și atacuri remote. Escaladarea de privilegii. DDOS, flood.	Expuneri, explicații, exemple, studii de caz	
7. Buffer overflow. Anatomia unui exploit. Shell-code.	Expuneri, explicații, exemple, studii de caz	
8. Securitatea aplicațiilor Web. SQL Injection. SMTP Injection. Cross Site Scripting. CSRF. Unrestricted file upload.	Expuneri, explicații, exemple, studii de caz	
9. Algoritmi de criptare bazați pe chei publice și chei private. Semnături digitale. Certificate digitale.	Expuneri, explicații, exemple, studii de caz	
10. Infrastructuri bazate pe chei publice și servicii asociate acestora.	Expuneri, explicații, exemple, studii de caz	
11. Securitatea poștei electronice. DKIM. Mecanisme antispam: bayesian spam filters, DNS based black lists. PGP.	Expuneri, explicații, exemple, studii de caz	
12. Protocoale de securitate la nivel rețea și transport. IPSec. SSL și TLS. VPN	Expuneri, explicații, exemple, studii de caz	
13. Securitate la nivel fizic și legătura de date.	Expuneri, explicații, exemple, studii de caz	
14. Vulnerabilități de tip Social Engineering.	Expuneri, explicații, exemple,	

Infraționalitatea informatică. Asigurarea intimității utilizatorului (user privacy)	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 Comerțului Electronic, Editura ALL 27. V. V. Patriciu, M. Ene-Pietrosanu, I. Bica, J. Priescu, Semnături Electronice și 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	Observații
1. Vulnerabilități informatice. Virusologie. Anatomia unui virus informatic. Sisteme antivirus.	Dezbaterea, dialogul, exemple, conversații de aplicare	
2. Exploit-uri. Shell-code.	Dezbaterea, dialogul, exemple, conversații de aplicare	
3. Mecanisme Firewall.	Dezbaterea, dialogul, exemple, conversații de aplicare	
4. Securitatea aplicațiilor Web	Dezbaterea, dialogul, exemple, conversații de aplicare	
5. Algoritmi de criptare bazați pe chei publice și chei private. Semnături digitale. Certificate digitale.	Dezbaterea, dialogul, exemple, conversații de aplicare	
6. Securitatea poștei electronice	Dezbaterea, dialogul, exemple, conversații de aplicare	
7. Protocoale de securitate la nivel rețea și transport.	Dezbaterea, dialogul, exemple, conversații de aplicare	
Bibliografie		

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 the Web: 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: [Semnături electronice și infrastructuri de securitate](#), notițe de curs, 2009, Master Sisteme Distribuite în Internet, Univ. Babeș-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 conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

- Cursuri cu un conținut similar există în planul de învățământ al tuturor marilor universități din România și din străinătate.
- Cursul abordează probleme fundamentale de securitate și deosebit de actuale în Internet.
- Conținutul cursului acoperă principalele aspecte necesare a fi însușite de către cursant pentru a ocupa cu succes o poziție 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	Cunoașterea principalelor aspecte teoretice prezentate la curs	Examen parțial din prima jumătate a materiei	0.3
	Cunoașterea principalelor aspecte teoretice prezentate la curs	Examen final din a doua jumătate a materiei	0.3
10.5 Seminar/laborator	Elaborarea unor referate și a unor proiecte pe teme de securitate stabilite de comun acord de cursant cu cadrul didactic dintre cele discutate la seminar.	Susținere orală de către cursant	0.4
10.6 Standard minim de performanță			
Pentru promovare trebuie cumulate următoarele două condiții:			
• prezentarea de referate și proiecte, activitate ce trebuie notată cel puțin cu nota 5; • minim media 5 între nota examenului parțial și cea obținută la examenul din sesiune.			

11. Etichete ODD (Obiective de Dezvoltare Durabilă / Sustainable Development Goals)²

Nu se aplică.

² Păstrați doar etichetele care, în conformitate cu [Procedura de aplicare a etichetelor ODD în procesul academic](#), se potrivesc disciplinei și ștergeți-le pe celelalte, inclusiv eticheta generală pentru *Dezvoltare durabilă* - dacă nu se aplică. Dacă nicio etichetă nu descrie disciplina, ștergeți-le pe toate și scrieți "Nu se aplică".

Data completării:
14.04.2025

Semnătura titularului de curs
Conf. dr. Darius-Vasile BUFNEA

Semnătura titularului de seminar
Conf. dr. Darius-Vasile BUFNEA

Data avizării în departament:
...

Semnătura directorului de departament
Conf. dr. Adrian STERCA