



FISA DISCIPLINEI

1. Date despre program

1.1	Instituația de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2	Facultatea	Electronica, Telecomunicații și Tehnologia Informației
1.3	Departamentul	Comunicații
1.4	Domeniul de studii	Inginerie electronică și telecomunicații
1.5	Ciclul de studii	Master
1.6	Programul de studii/Calificarea	Tehnologii și Sisteme de Telecomunicații/ Inginer
1.7	Forma de învățământ	IF - Învățământ cu frecvență
1.8	Codul disciplinei	EM0519

2. Date despre disciplina

2.1	Denumirea disciplinei	Securitatea în sisteme IT									
2.2	Aria tematică (subject area)	Inginerie electronică și telecomunicații									
2.3	Responsabil de curs	Sl.dr.ing. Tudor Mihai BLAGA – tudor.blaga@com.utcluj.ro									
2.4	Titularul disciplinei	Sl.dr.ing. Tudor Mihai BLAGA									
2.5	Anul de studii	II	2.6	Semestrul	I	2.7	Evaluarea	Examen	2.8	Regimul disciplinei	OPT

3. Timpul total estimat

An/ Sem	Denumirea disciplinei	Nr. sapt.	Curs			Aplicații			Stud. Ind.	TOTAL	Credit		
			[ore/săpt.]			[ore/sem.]							
			S	L	P	S	L	P					
II/I	Securitatea Sistemelor IT	14	2	0	1	0	28	0	14	0	88	130	5

3.1	Număr de ore pe săptămână	2	3.2	din care curs	2	3.3	aplicații	1
3.4	Total ore din planul de inv.	28	3.5	din care curs	28	3.6	aplicații	14
Studiul individual								Ore
Studiul după manual, suport de curs, bibliografie și note								36
Documentarea suplimentară în bibliotecă, pe platformele electronice și pe teren								8
Pregătire seminar/laboratoare, teme, referate, portofolii, eseuri								24
Tutoriat								2
Examinări								3
Alte activități								15
3.7	Total ore studiul individual	88						
3.8	Total ore pe semestru	130						
3.9	Număr de credite	5						

4. Precondiții (acolo unde este cazul)

4.1	De curriculum	Retele de calculatoare, Sisteme de comutație și rutare, Protocoale pentru Internet, Tehnici de secretizare a informației
4.2	De competente	NU

5. Condiții (acolo unde este cazul)

5.1	De desfășurare a cursului	NU
5.2	De desfășurare a aplicațiilor	Universitatea Tehnică din Cluj-Napoca

6 Competențe specifice acumulate

Competențe profesionale	Cunoștințe teoretice, (Ce trebuie să cunoască)	După parcurgerea disciplinei studenții vor cunoaște: <ul style="list-style-type: none"> – principiile securității în sistemele IT (CIA – Confidentiality, Integrity, Availability) – procesul: prevenție, detecție și răspuns – pașii și metodele de răspuns la incidentele de securitate – bazele securității arhitecturilor de rețea – mecanismele de securitate în Windows și Unix/Linux – metodele de securizare a aplicațiilor web – analiza aplicațiilor malicioase; mecanisme de prevenție și detecție – metodele de management a riscului
	Deprinderi dobândite: (Ce știe să facă)	După parcurgerea disciplinei studenții vor fi capabili: <ul style="list-style-type: none"> – să utilizeze și să configureze mecanismele de securitate din sistemele Windows – să utilizeze și să configureze mecanismele de securitate din sistemele Unix/Linux – să evalueze securitatea unei aplicații web – să analizeze caracteristicile unui virus – să evalueze riscul de securitate a unui sistem IT
	Abilități dobândite: (Ce instrumente știe să mănuiască)	După parcurgerea disciplinei studenții vor fi capabili: <ul style="list-style-type: none"> – să utilizeze instrumente specifice soft pentru testarea securității
Competențe transversale		

7 Obiectivele disciplinei (reiesind din grila competențelor specific acumulate)

7.1	Obiectivul general al disciplinei	Dezvoltarea de competențe profesionale în domeniul securității sistemelor IT
7.2	Obiectivele specifice	1. Asimilarea principiilor fundamentale privind securitatea sistemelor IT (rețele de calculatoare, Windows, Unix) și a aplicațiilor web. 2. Obținerea deprinderilor și abilităților necesare pentru implementarea și testarea securității sistemelor IT

8. Continuturi

8.1. Curs (programa analitică)		Metode de predare	Observații
1	Introducere în securitatea sistemelor IT	Expunere, discuții	Video-proiector
2	Principiile securității sistemelor IT (Defence-in-depth)		
3	Etapele de răspuns la incidentele de securitate (Incident Response)		
4	Proiectarea arhitecturilor de rețea securizate		
5	Securitatea sistemelor Windows 1		
6	Securitatea sistemelor Windows 2		
7	Securitatea sistemelor Unix/Linux 1		
8	Securitatea sistemelor Unix/Linux 2		
9	Securitatea aplicațiilor web 1		

10	Securitatea aplicatiilor web 2		
11	Analiza aplicatiilor malitioase (Malware)		
12	Notiuni de risc management		
13	Managementul securitatii informatiilor: ISO27001		
14	Recapitulare, discutie tipuri subiecte examen		
8.2. Aplicatii (lucrări)		Metode de predare	Observatii
1	Prezentarea ședințelor de laborator și a modului de desfășurare al activităților practice	Expunere și aplicații	Calculatorul, softuri de analiza a securității
2	Etapele unui program de Security Awareness		
3	Definirea programului de Security Awareness 1 (miniproiect)		
4	Definirea programului de Security Awareness 2 (miniproiect)		
5	Securitatea sistemelor Windows 1		
6	Securitatea sistemelor Windows 2		
7	Securitatea sistemelor Unix/Linux 1		
8	Securitatea sistemelor Unix/Linux 2		
9	Unelte pentru testarea securitatii aplicatiilor web: Burp, Accunetix		
10	Exploatarea vulnerabilitatilor aplicatiilor web		
11	Dezasamblarea si analiza comportamentului unui virus		
12	Studiu de caz: evaluarea riscului in functie de impact si de probabilitate		
13	Sustinere miniproiecte		
14	Recuperari laboratoare		
Bibliografie			
1. Peter Kim - „The Hacker Playbook: Practical Guide To Penetration Testing”, CreateSpace, 2014			
2. Patrick Englebretson - „The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy”, Syngress, 2 nd edition, 2013			
3. Daniel Dieterle - „Basic Security Testing with Kali Linux”, CreateSpace, 2014			
4. Eric Cole - „Network Security Bible”, Wiley, 2009			
5. Dafydd Stuttard & Marcus Pinto - „The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws”, Wiley, 2 nd edition, 2011			

9. Coroborarea continuturilor disciplinei cu asteptarile reprezentantilor comunitatii epistemice, asociatiilor, profesionale si angajatori din domeniul aferent programului

Competentele achizitionate vor fi necesare angajatilor in urmatoarele ocupatii posibile conform COR (administrator sistem de securitate bancară, consultant de securitate, director departament securitate, inginer sisteme de securitate, manager securitatea informației, ofițer securitatea informației, proiectant sisteme de securitate, specialist în proceduri și instrumente de securitate a sistemelor informatice)

10. Evaluare

Tip activitate	10.1	Criterii de evaluare	10.2	Metode de evaluare	10.3	Ponderea din nota finala
Curs		Rezolvare subiecte tip grila		Examen scris		50%
Aplicatii		Prezentare proiect laborator		Sustinere orala		50%
10.4 Standard minim de performanta						
Răspuns corect la cel puțin 50% din subiectele tip grila și obținerea unei note minime de 5 în cadrul proiectului de laborator.						

Data completarii	Titularul de disciplina	Responsabil de curs
12.04.2014	Sl.dr.ing. Tudor Mihai BLAGA	Sl.dr.ing. Tudor Mihai BLAGA

Data avizarii in departament
05.06.2014

Director departament
Prof.dr.ing. Virgil Dobrota