FISA DISCIPLINEI

1. Date despre program

1.1	Institutia de invatamint superior	Universitatea Tehnica din Cluj-Napoca
1.2	Facultatea	Electronica, Telecomunicatii si Tehnologia Informatiei
1.3	Departamentul	Comunicatii
1.4	Domeniul de studii	Inginerie electronica si telecomunicatii
1.5	Ciclul de studii	Master
1.6	Programul de studii/Calificarea	Tehnologii si Sisteme de Telecomunicatii/ Inginer
1.7	Forma de invatamint	IF - Invaţamant cu frecventa
1.8	Codul disciplinei	EM0626

2. Date despre disciplina

2.1	Denumirea disciplinei					Securitatea in sisteme IT						
2.2	Aria tematica (subject area)					Inginerie electronica si telecomunicatii						
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	Aplicaţii			Curs	Aplicaţii			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	Numar de ore pe saptamina	2	3.2	din care curs	2	3.3	aplicatii	1
3.4	Total ore din planul de inv.	28	3.5	din care curs	28	3.6	aplicatii	14
Studiul individual								Ore
Studiul dupa manual, suport de curs, bibliografie si notite								36
Documentara suplimentara in biblioteca, pe platformele electronice si pe teren								8
Pregatire seminarii/laboratoare, teme, referate, portofolii, eseuri								24
Tutoriat								2
Examinari								3
Alte activitati								15

3.7	Total ore studiul individual	88
3.8	Total ore pe semestru	130
3.9	Numar de credite	5

4. Preconditii (acolo unde este cazul)

4.1	De curriculum	Retele de calculatoare, Sisteme de comutatie si rutare, Protocoale pentru Internet, Tehnici de secretizare a informaţiei
4.2	De competente	NU

5. Conditii (acolo unde este cazul)

5.1	De desfasurare a cursului	NU
5.2	De desfasurare a aplicatiilor	Universitatea Tehnica din Cluj-Napoca

6 Competente specifice acumulate

Competente profesionale	Cunoştinţe teoretice, (Ce trebuie sa cunoască)	După parcurgerea disciplinei studenţii vor cunoaşte: – principiile securitatii in sistemele IT (CIA – Confidentiality, Integrity, Avalability) – procesul: preventie, detectie si raspuns – pasii si metodele de raspuns la incidentele de securitate – bazele securitatii arhitecturilor de retea – mecanismele de securitate in Windows si Unix/Linux – metodele de securizare a aplicatiilor web – analiza aplicatiilor malitioase; mecanisme de preventie si detectie – metodele de management a riscului
	Deprinderi dobândite: (Ce ştie să facă)	După parcurgerea disciplinei studenţii vor fi capabili: – să utilizeze si sa configureze mecanismele de securitate din sistemele Windows – să utilizeze si sa configureze mecanismele de securitate din sistemele Unix/Linux – să evalueze securitatea unei aplicatii web – să analizeze caracteristicile unui virus – să evalueze riscul de securitate a unui sistem IT
	Abilităţi dobândite: (Ce instrumente ştie să mânuiască)	După parcurgerea disciplinei studenţii vor fi capabili: – să utilizeze instrumente specifice soft pentru testarea securitatii
Competenţe transversale		

7 Obiectivele disciplinei (reiesind din grila competentelor specific acumulate)

7.1	Obiectivul general al disciplinei	Dezvoltarea de competenţe profesionale în domeniul securitatii sistemelor IT
7.2	Obiectivele specifice	1. Asimilarea principiilor fundamentale prind securitatea sistemelor IT (retele de calculatoare, Windows, Unix) si a aplicatiilor web. 2. Obţinerea deprinderilor şi abilităţilor necesare pentru implementarea şi testarea securitatii sistemelor IT

8. Continuturi

8.1. Curs (programa analitică)		Metode de predare	Observaţii
1	Introducere în securitatea sistemelor IT	Expunere, discuţii	Video-proiector
2	Principiile securitatii sistemelor IT (Defence-in-depth)		
3	Etapele de raspuns la incidentele de securitate (Incident Response)		
4	Proiectarea arhitecturilor de retea 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 aplicatiilor 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. Aplicaţii (lucrări)		Metode de predare	Observaţii
1	Prezentarea şedinţelor de laborator şi a modului de desfăşurare al activităţilor practice	Expunere și aplicații	Calculatorul, softuri de analiza a securitatii
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 Engebretson - „The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy”, Syngress, 2nd 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, 2nd 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 informaţiei, ofiţer securitatea informaţiei, proiectant sisteme de securitate, specialist în proceduri şi 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 puţin 50% din subiectele tip grila şi obţinerea 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