FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei
1.3 Departamentul	Comunicaţii
1.4 Domeniul de studii	Inginerie electronică, telecomunicaţii şi tehnologii informaţionale
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Tehnologii Multimedia (TM) / Master
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	TM16.10

2. Date despre disciplină

2.1 Denumirea disciplinei	Securitatea sistemelor IT						
2.2 Aria de conţinut	Arie teoretică Arie metodologică Arie de analiză						
2.3 Responsabil de curs	Sl.dr.ing. Tudor BLAGA – Tudor.Blaga@com.utcluj.ro						
2.4 Titularul activităţilor de seminar / laborator / proiect	Sl.dr.ing. Tudor BLAGA – Tudor.Blaga@com.utcluj.ro						
2.5 Anul de studiu	2	2.6 Semestrul	3	2.7 Tipul de evaluare	E	2.8 Regimul disciplinei	DS/ DO

3. Timpul total estimat

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					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					12
Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri					20
Tutoriat					3
Examinări					3
Alte activităţi:					

3.7 Total ore studiu individual	58
3.8 Total ore pe semestru	100
3.9 Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	
4.2 de competenţe	

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Cluj-Napoca
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Cluj-Napoca

6. Competenţele specifice acumulate

Competenţe profesionale	C4. Conceperea, implementarea si operarea serviciilor de date, voce, video, multimedia, bazate pe întelegerea si aplicarea notiunilor fundamentale din domeniul comunicatiilor si transmisiunii informatiei C5. Selectarea, instalarea, configurarea si exploatarea echipamentelor de telecomunicatii fixe sau mobile si echiparea unui amplasament cu retele uzuale de telecomunicatii
Competenţe transversale	N/A

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

7.1 Obiectivul general al disciplinei	Dezvoltarea de competente privind principiile securitatii in sistemele IT (confidentialiate, integritate, disponibilitate) si procesele de preventie, detectie si raspuns.
7.2 Obiectivele specifice	1. Dezvoltarea de deprinderi si abilitati necesare pentru utilizarea si configurarea mecanismelor de securitate din sistemele de operare Windows, UNIX/Linux. 2. Dezvoltarea de deprinderi si abilitati necesare pentru evaluarea securitatii unei aplicatii web, si pentru analizarea caracteristicilor unui virus informatic 3. Dezvoltarea de deprinderi si abilitati necesare pentru evaluarea riscului de securitate a unui sistem IT

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii
1. Introducere în securitatea sistemelor IT	Expunere la tablă, prezentare cu videoproiector, discuţii.	Nu este cazul.
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 de cloud public: Amazon Web Services (1)		
6. Securitatea sistemelor de cloud public: Amazon Web Services (2)		
7. Securitatea sistemelor de operare Unix/Linux (1)		
8. Securitatea sistemelor de operare 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		

Bibliografie

1. P. Kim, The Hacker Playbook: Practical Guide To Penetration Testing, CreateSpace Independent Publishing Platform, 2014
2. P. Engebretson, The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy", Syngress, 2nd edition, 2013
3. D.W. Dieterle, Basic Security Testing with Kali Linux 2, CreateSpace Independent Publishing Platform, 2016
4. E. Cole, Network Security Bible, Second Edition, John Wiley & Sons, 2009
5. D. Stuttard, M. Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Wiley, Second edition, 2011
6. A. Anthony, Mastering AWS Security: Create and Maintain a Secure Cloud Ecosystem, Packt Publishing 2017.

8.2 Laborator	Metode de predare	Observaţii
1. Prezentarea şedinţelor de laborator şi a modului de desfăşurare al activităţilor practice	Experimente practice pe echipamente fizice, virtuale, in cloud si pe emulatoare.	Nu este cazul.
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 de cloud public: Amazon Web Services (1)		
6. Securitatea sistemelor de cloud public: Amazon Web Services (2)		
7. Securitatea sistemelor de operare Unix/Linux (1)		
8. Securitatea sistemelor de operare 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. P. Kim, The Hacker Playbook: Practical Guide To Penetration Testing, CreateSpace Independent Publishing Platform, 2014
2. P. Engebretson, The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy", Syngress, 2nd edition, 2013
3. D.W. Dieterle, Basic Security Testing with Kali Linux 2, CreateSpace Independent Publishing Platform, 2016
4. E. Cole, Network Security Bible, Second Edition, John Wiley & Sons, 2009
5. D. Stuttard, M. Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Wiley, Second edition, 2011
6. A. Anthony, Mastering AWS Security: Create and Maintain a Secure Cloud Ecosystem, Packt Publishing 2017.

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

Competentele dobandite vor fi folosite in urmatoarele ocupatii conform COR (Clasificarea Ocupațiilor din România): Inginer emisie; Inginer electronist, transporturi, telecomunicatii; Inginer imagine; Inginer sunet; Proiectant inginer electronist; Proiectant inginer de sisteme si calculatoare; Inginer sef car reportaj; Inginer sef schimb emisie; Inginer proiectant comunicatii; Inginer sisteme de securitate; Inginer suport vânzari; Dezvoltator de aplicatii multimedia; Inginer operare retea; Inginer testare sisteme de comunicatii; Manager proiect; Inginer de trafic; Consultant pentru sisteme comunicatii.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Nivelul cunostintelor teoretice si a deprinderilor dobandite	Test teoretic (nota T) : examen scris cu intrebari grila	T, max 10 pct. 50%
10.5 Laborator	Nivelul abilitatilor practice dobandite	Proiect (P): examen oral si practic bazat pe laborator	P, max. 10 pct. 50%
10.6 Standard minim de performanţă			

Nivel calitativ:

Cunoştinţe minimale:

- ✓ Intelegerea conceptelor de baza privind principiile securitatii in sistemele IT (confidentialiate, integritate, disponibilitate)
- ✓ Intelegerea conceptelor de baza privind procesele de preventie, detectie si raspuns.

Competenţe minimale:

- ✓ Să poată configura mecanisme de securitate in sistemele de operare Windows, UNIX/ Linux.
- ✓ Să poată evalua securitatea unei aplicatii web
- ✓ Să poată evalua riscul de securitate al unui sistem IT

Nivel cantitativ:

- ✓ T ≥ 5, P≥ 5 si (T+P)/2≥ 5

Data completării:	Titulari	Titlu Prenume NUME	Semnătura
13.09.2022	Curs	Sl.dr.ing. Tudor BLAGA	
	Aplicații	Sl.dr.ing. Tudor BLAGA	

Data avizării în Consiliul Departamentului COM
13.09.2022

Director Departament Comunicații
Prof.dr.ing. Virgil DOBROTĂ

Data aprobării în Consiliul Facultății ETTI
21.09.2022

Decan
Prof.dr.ing. Ovidiu POP