

## FIȘA DISCIPLINEI

### 1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Facultatea de Electronică, Telecomunicații și Tehnologia Informației
1.3 Departamentul	Comunicații
1.4 Domeniul de studii	Inginerie electronică, telecomunicații și tehnologii informaționale
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Telecomunicații (TC) / Master
1.7 Forma de învățământ	IF – învățământ cu frecvență
1.8 Codul disciplinei	TC17.30

### 2. Date despre disciplină

2.1 Denumirea disciplinei	Securitatea sistemelor IT						
2.2 Aria de conținut	Arie teoretică Arie metodologică Arie de analiză						
2.3 Responsabil de curs	Sl.dr.ing. Tudor BLAGA – <a href="mailto:Tudor.Blaga@com.utcluj.ro">Tudor.Blaga@com.utcluj.ro</a>						
2.4 Titularul activităților de seminar / laborator / proiect	Sl.dr.ing. Tudor BLAGA – <a href="mailto:Tudor.Blaga@com.utcluj.ro">Tudor.Blaga@com.utcluj.ro</a>						
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 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					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					12
Pregătire seminarii / laboratoare, teme, referate, portofolii și eseuri					20
Tutoriat					3
Examinări					3
Alte activități: .....					
3.7 Total ore studiu individual					58
3.8 Total ore pe semestru					100
3.9 Numărul de credite					4

### 4. Precondiții (acolo unde este cazul)

4.1 de curriculum	
4.2 de competențe	

### 5. Condiții (acolo unde este cazul)

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

### 6. Competențele specifice acumulate

Competențe profesionale	C4. Conceperea, implementarea și operarea serviciilor de date, voce, video, multimedia, bazate pe înțelegerea și aplicarea notiunilor fundamentale din domeniul comunicațiilor și transmisiunii informației C5. Selectarea, instalarea, configurarea și exploatarea echipamentelor de telecomunicații fixe sau mobile și echiparea unui amplasament cu rețele uzuale de telecomunicații
Competențe transversale	N/A

### 7. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

7.1 Obiectivul general al disciplinei	Dezvoltarea de competențe privind principiile securității în sistemele IT (confidențialitate, integritate, disponibilitate) și procesele de prevenție, detecție și răspuns.
7.2 Obiectivele specifice	<ol style="list-style-type: none"> <li>Dezvoltarea de deprinderi și abilități necesare pentru utilizarea și configurarea mecanismelor de securitate din sistemele de operare Windows, UNIX/Linux.</li> <li>Dezvoltarea de deprinderi și abilități necesare pentru evaluarea securității unei aplicații web, și pentru analizarea caracteristicilor unui virus informatic</li> <li>Dezvoltarea de deprinderi și abilități necesare pentru evaluarea riscului de securitate a unui sistem IT</li> </ol>

### 8. Conținuturi

8.1 Curs	Metode de predare	Observații
1. Introducere în securitatea sistemelor IT	Expunere la tablă, prezentare cu videoprojector, discuții.	Nu este cazul.
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 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 aplicațiilor web (1)		
10. Securitatea aplicațiilor web (2)		
11. Analiza aplicațiilor malicioase (Malware)		
12. Notiuni de risc management		
13. Managementul securității informațiilor: ISO27001		

14. Recapitulare, discutie tipuri subiecte examen		
<b>Bibliografie</b>		
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.		
<b>8.2 Laborator</b>	Metode de predare	Observații
1. Prezentarea ședințelor de laborator și a modului de desfășurare al activităților 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		
<b>Bibliografie</b>		
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 conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului**

Competențele dobândite vor fi folosite în următoarele ocupații conform COR (Clasificarea Ocupațiilor din România): Inginer emisie; Inginer electronist, transporturi, telecomunicații; Inginer imagine; Inginer sunet; Proiectant inginer electronist; Proiectant inginer de sisteme și calculatoare; Inginer șef car reportaj; Inginer șef schimb emisie; Inginer proiectant comunicații; Inginer sisteme de securitate; Inginer suport vânzări; Dezvoltator de aplicații multimedia; Inginer operare rețea; Inginer testare sisteme de comunicații; Manager proiect; Inginer de trafic; Consultant pentru sisteme de comunicații.

**10. Evaluare**

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Nivelul cunoștințelor teoretice și a deprinderilor dobândite	Test teoretic (nota T) : examen scris cu întrebări grilă	T, max 10 pct. 50%
10.5 Laborator	Nivelul abilităților practice dobândite	Proiect (P): examen oral și practic bazat pe laborator	P, max. 10 pct. 50%

**10.6 Standard minim de performanță**

**Nivel calitativ:**

*Cunoștințe minimale:*

- ✓ Înțelegerea conceptelor de bază privind principiile securității în sistemele IT (confidențialitate, integritate, disponibilitate)
- ✓ Înțelegerea conceptelor de bază privind procesele de prevenție, detectie și răspuns.

*Competențe minimale:*

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

**Nivel cantitativ:**

- ✓  $T \geq 5$ ,  $P \geq 5$  și  $(T+P)/2 \geq 5$

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