R40 Anexa 1

FIŞA DISCIPLINEI
(masterat)

1. Date despre program

Instituţia de învăţământ superior	**Universitatea Ștefan cel Mare din Suceava**
Facultatea	**Facultatea de Inginerie Electrică și Știința Calculatoarelor**
Departamentul	**Departamentul de Calculatoare Electronică și Automatică**
Domeniul de studii	**Inginerie Electronică, Telecomunicații și Tehnologii Informaționale**
Ciclul de studii	**Master**
Programul de studii	**Securitate Cibernetică**

2. Date despre disciplină

Denumirea disciplinei	Managementul și auditarea securității sistemelor informatice și de comunicații					
Titularul activităţilor de curs	S.l. dr.ing. Doru Balan					
Titularul activităţilor aplicative	drd. Edi TIMOFTE					
Anul de studiu	II	Semestrul	3	Tipul de evaluare	E	
Regimul disciplinei	Categoria formativă a disciplinei DSI – Discipline de sinteză; DAP – Discipline de aprofundare					DAP
	Categoria de opţionalitate a disciplinei: DI - impusă, DO - opţională, DF - facultativă					DI

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore, pe săptămână	3	Curs	1	Seminar		Laborator/lucrări practice	Laborator	1	Proiect	1
I b) Totalul de ore (pe semestru) din planul de învăţământ	42	Curs	14	Seminar		Laborator/lucrări practice	Laborator	14	Proiect	14

II. Distribuţia fondului de timp pe semestru	ore
II.a) Studiul după manual, suport de curs, bibliografie şi notiţe	25
II.b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	28
II.b) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	27
II.d) Tutoriat	
III. Examinări	3
IV. Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	80
Total ore pe semestru (Ib+II+III+IV)	125
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		• PC, videoproiector (prezentări PPT, software specializat)
Desfăşurare aplicaţii	Laborator	• PC, videoproiector, software specializat, suporturi electronice pentru aplicaţii, prezentări PPT, materiale pentru aplicaţii, referate, 12 stații de lucru etc
	Proiect	• PC, videoproiector, software specializat, suporturi electronice pentru aplicaţii, prezentări PPT, materiale pentru aplicaţii, referate, 12 stații de lucru etc

6. Competenţe specifice acumulate

Competenţe profesionale	• C4 Însușirea tehnicilor de operare și utilizare a aparaturii și aplicațiilor profesionale specifice ariei Securității Cibernetice • C5. Identificarea și combaterea riscurilor și pericolelor privind expunerea sistemelor informatice la atacuri cibernetice

	• C6. Soluționarea incidentelor de securitate folosind instrumente specifice, proiectarea și dezvoltarea de instrumente și aplicații specifice securității cibernetice
Competenţe transversale	CT2. Managementul proiectelor complexe şi utilizarea a diverse moduri de comunicare scrisă şi orală

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

Obiectivul general al disciplinei	• Identificarea și combaterea riscurilor și pericolelor privind expunerea sistemelor informatice la atacuri cibernetice prin gestionarea de procese de auditare a securității sistemelor informatice și de comunicații
	• Se urmărește identificarea elementelor fundamentale privind realizarea testelor de securitate, realizarea de operațiuni de identificare a serviciilor și sistemelor, descoperirea de vulnerabilități pentru a realiza sisteme informatice și de comunicație rezistente la atacuri în rețea.

8. Conţinuturi

Curs	Nr. ore	Metode de predare	Observaţii
• Elemente introductive prind evaluarea securității sistemelor informatice și de comunicații. Scopuri și implicare în realizarea de teste de securitate.	2	prelegerea, conversația, exemplificarea.	
• Resurse pentru realizarea testelor de securitate. OSINT. Inginerie socială.	2		
• Teste de securitate la nivel de rețea. Rețea internă. Rețea externă.	2		
• Teste de securitate la nivel de echipamente de infrastructură de rețea. Securitatea resurselor web.	2		
• Evaluarea securității resurselor Wireless și IoT	2		
• Securitatea infrastructurilor critice și tehnologiilor operaționale. Testarea securității resurselor în Cloud	2		
• Analiza rezultatelor testelor de securitate. Rapoarte de securitate. Acțiuni ulterioare auditului de securitate.	2		

Bibliografie

1. Dafydd Stuttard and Marcus Pinto, "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws," Wiley, 2019.
2. David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni, "Metasploit: The Penetration Tester's Guide," No Starch Press, 2011.
3. Jon Erickson, "Hacking: The Art of Exploitation," No Starch Press, 2008.
4. Justin Seitz, "Black Hat Python: Python Programming for Hackers and Pentesters," No Starch Press, 2014.
5. Gordon Lyon, "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning," Nmap Project, 2009.
6. Georgia Weidman, "Penetration Testing: A Hands-On Introduction to Hacking," No Starch Press, 2014.
7. Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy," Syngress, 2013.
8. Raphael Hertzog, Jim O'Gorman, and Mati Aharoni, "Kali Linux Revealed: Mastering the Penetration Testing Distribution," Offsec Press, 2017.
9. Kevin D. Mitnick and William L. Simon, "The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders, and Deceivers," Wiley, 2005.
10. TJ O'Connor, "Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers," Syngress, 2012.
11. Ben Clark, "Red Team Field Manual," CreateSpace Independent Publishing Platform, 2014.
12. Wil Allsopp, "Advanced Penetration Testing: Hacking the World's Most Secure Networks," Wiley, 2017.
13. Peter Kim, "The Hacker Playbook 3: Practical Guide to Penetration Testing," Wiley, 2018.
14. Don Murdoch and Gary McIntyre, "Blue Team Handbook: Incident Response Edition," CreateSpace Independent Publishing Platform, 2014.
15. Andrei Dumitrescu, "Wireless Hacking: How to Hack Wireless Networks," CreateSpace, 2015.
16. Offensive Security Certified Professional (OSCP), Offensive Security, 2019.
17. Certified Information Systems Security Professional (CISSP), (ISC)², 2018.
18. Certified Ethical Hacker (CEH), EC-Council, 2019.
19. Certified Information Security Manager (CISM), ISACA, 2019.
20. CompTIA Security+, CompTIA, 2020.

Aplicaţii (laborator)	Nr. ore	Metode de predare	Observaţii
• Identificare resurse de laborator necesare pentru teste de securitate. Virtualizare. Instrumente. Resurse vulnerabile.	2	prelegerea, conversația, exemplificarea.	
• Explorarea și exploatarea vulnerabilităților sistemelor informatice și de comunicații	2		
• Tehnici pentru obținerea accesului si escaladarea drepturilor de acces.	2		
• Teste de securitate la nivel de aplicații web	2		
• Teste de securitate la nivel de resurse wireless	2		
• Tehnici de analiza traficului, inginerie socială și tunelare.	2		
• Analiza rezultate obținute prin teste de securitate. Realizare raport de audit. Urmărire măsuri de securizre.	2		

Bibliografie

1. "Metasploit: The Penetration Tester's Guide" , David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni, 2011, No Starch Press
2. "Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" , Dafydd Stuttard, Marcus Pinto, 2019, Wiley
3. "The Art of Exploitation", Jon Erickson, 2008, No Starch Press
4. "Penetration Testing: A Hands-On Introduction to Hacking" , Georgia Weidman, 2014, No Starch Press
5. "Hacking: The Art of Exploitation", Jon Erickson, 2003, No Starch Press
6. "The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws" , Dafydd Stuttard, Marcus Pinto, 2011, Wiley
7. "Penetration Testing: Procedures & Methodologies", EC-Council, 2010, Cengage Learning
8. "Advanced Penetration Testing: Hacking the World's Most Secure Networks", Wil Allsopp, 2017, Wiley
9. "Black Hat Python: Python Programming for Hackers and Pentesters", Justin Seitz, 2014, No Starch Press
10. "The Mobile Application Hacker's Handbook" , Dominic Chell, Ollie Whitehouse, 2015, Wiley

Aplicaţii (proiect)	Nr. ore	Metode de predare	Observaţii
• Evaluare și dezvoltare resuse de tip poligon de securitate	2	prelegerea, conversația, exemplificarea.	
• Evaluare și dezvoltare resurse pentru identificarea serviciilor și vulnerabilităților sistemelor informatice și de comunicație	2		
• Identificarea mecanisme și tehnici de atac avansat asupra sistemelor informatice și de comunicații	2		
• Analiza rezultatelor furnizate sau obținute prin diverse tehnici, mecanisme și instrumente folosite în teste de evaluare a securității sistemelor informatice și de comunicații	2		
• Mecanisme de atac, obținere acces și escaladare privilegii	2		
• Studiu prind testele de securitate in diverse medii: infrastructură de rețea, aplicații și servicii de date	2		
• Realizarea și analiza unui raport de audit de securiate informațională	2		

Bibliografie

[1] G. C. Church, "Hacking Exposed 7: Network Security Secrets and Solutions," McGraw-Hill Osborne Media, 2012.
[2] C. Peltier and K. Blackley, "Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management," Auerbach Publications, 2011.
[3] S. Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy," Elsevier, 2013.
[4] T. Wilhelm and M. Craig, "Penetration Testing: A Hands-On Introduction to Hacking," No Starch Press, 2014.
[5] G. D. Wydman, "The Basics of Web Hacking: Tools and Techniques to Attack the Web," Elsevier, 2013.
[6] D. Kennedy, J. O'Gorman, R. Wakeman, and D. Erb, "Metasploit: The Penetration Tester's Guide," No Starch Press, 2011.
[7] G. S. Weidman, "Advanced Penetration Testing: Hacking the World's Most Secure Networks," Wiley, 2017.
[8] T. Ryan, J. Portwood, and J. Sims, "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning," Nmap Project, 2009.
[9] V. Einwachter and T. Thiel, "Penetration Testing and Network Defense," Pearson Education, 2010.
[10] R. Shimonski, "Cyber Reconnaissance, Surveillance and Defense," Syngress, 2014.

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

- **Conţinutul disciplinei se regăseşte în curricula disciplinelor similare de la facultăți de profil din țară și din străinătate.**

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs			
	Nota acordată la examinarea finală	Evaluare prin probă finală scrisă și orală - evaluare de referate de studiu	50
Laborator	Media notelor acordate la lucrări practice	Evaluare continuă (prin metode orale, probe practice, sau proiecte de studiu)	25
Proiect	Nota acordata proiectului de studio individual	Evaluare continuă (prin metode orale, probe practice, sau proiecte de studiu)	25
Standard minim de performanță			
• Identificarea principalelor metode de evaluare a securității sistemelor informatice și de comunicații. • Identificarea rezultatelor urmărite prin realizarea unui unui adit de securitate asupra sistemelor informatice și de comunicații.			

Data completării	Semnătura titularului de curs	Semnătura titularului de aplicaţie
18.09.2024		

Data avizării	Semnătura responsabilului de program
20.09.2024	

Data avizării în departament	Semnătura directorului de departament
23.09.2024	

Data aprobării în consiliul facultăţii	Semnătura decanului
27.09.2024	