FIŞA DISCIPLINEI
Anul universitar 2021-2022

Decan,
Prof. Vasile-Ion Manta

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică „Gheorghe Asachi” din Iaşi
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare şi tehnologia informației
1.5 Ciclul de studii[1]	Master
1.6 Programul de studii	Securitatea spațiului cibernetic

2. Date despre disciplină

2.1 Denumirea disciplinei/Cod		Sisteme de detecție și prevenție a atacurilor informatice / SSC.IA.106					
2.2 Titularul activităţilor de curs		ș.l. dr. ing. Cristian Nicolae Buțincu					
2.3 Titularul activităţilor de aplicaţii		ș.l. dr. ing. Cristian Nicolae Buțincu					
2.4 Anul de studii[2]	1	2.5 Semestrul[3]	2	2.6 Tipul de evaluare[4]	Examen	2.7 Tipul disciplinei[5]	DS

3. Timpul total estimat al activităţilor zilnice (ore pe semestru)

3.1 Număr de ore pe săptămână	4	din care 3.2 curs	2	3.3a sem.	-	3.3b laborator	2	3.3c proiect	-
3.4 Total ore din planul de învățământ[6]	56	din care 3.5 curs	28	3.6a sem.	-	3.6b laborator	28	3.6c proiect	-

Distribuţia fondului de timp[7]	Nr. ore
Studiul după manual, suport de curs, bibliografie şi notiţe	34
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	28
Pregătire seminarii/laboratoare/proiecte, teme, referate şi portofolii	28
Tutoriat[8]	
Examinări[9]	4
Alte activităţi:	

3.7 Total ore studiu individual[10]	94
3.8 Total ore pe semestru[11]	150
3.9 Numărul de credite	6

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum[12]	●
4.2 de competenţe	●

5. Condiţii (acolo unde este cazul)

5.1 de desfăşurare a cursului[13]	● Tablă, videoproiector
5.2 de desfăşurare a seminarului / laboratorului / proiectului[14]	● Sală de laborator cu calculatoare și acces la internet

6. Competenţele specifice acumulate[15]

[1] *Licenţă / Master*
[2] *1-4 penrtru licenţă, 1-2 pentru master*
[3] *1-8 pentru licenţă, 1-3 pentru master*
[4] *Examen, colocviu sau VP A/R – din planul de învăţământ*
[5] *DF - disciplină fundamentală, DID - disciplină în domeniu, DS – disciplină de specialitate sau DC - disciplină complementară - din planul de învăţământ*
[6] *Este egal cu 14 săptămâni x numărul de ore de la punctul 3.1 (similar pentru 3.5, 3.6abc)*
[7] *Liniile de mai jos se referă la studiul individual; totalul se completeaza la punctul 3.7.*
[8] *Între 7 şi 14 ore*
[9] *Între 2 şi 6 ore*
[10] *Suma valorilor de pe liniile anterioare, care se referă la studiul individual.*
[11] *Suma dintre numărul de ore de activitate didactică directă (3.4) şi numărul de ore de studiu individual (3.7); trebuie să fie egală cu numărul de credite alocat disciplinei (punctul 3.9) x 24 de ore pe credit.*
[12] *Se menţionează disciplinele obligatoriu a fi promovate anterior sau echivalente*
[13] *Tablă, vidoproiector, flipchart, materiale didactice specifice etc.*
[14] *Tehnică de calcul, pachete software, standuri experimentale, etc.*
[15] *Competenţele din Grilele G1 şi G1bis ale programului de studii, adaptate la specificul disciplinei, pentru care se repartizează credite (www.rncis.ro sau site-ul facultăţii)*

Număr de credite alocat disciplinei[16]:		**6**	Repartizare credite pe competenţe[17]
Competenţe profesionale	CP1	Cunoașterea conceptelor avansate din domeniul științei calculatoarelor și tehnologiei informației și capacitatea de a opera cu aceste concepte.	1.4
	CP2	Cercetarea științifică și practică privind securitatea sistemelor informatice complexe.	1.2
	CP3	Rezolvarea problemelor pe baza metodelor și tehnologiilor de securizare a sistemelor informatice complexe.	1
	CP4	Utilizarea de instrumente specifice domeniului în vederea identificării vulnerabilităților și a amenințărilor de securitate cibernetică.	1.5
	CP5	Proiectarea și dezvoltarea de soluții software cu un înalt grad de securitate orientate pe prevenția și răspunsul la incidente de securitate cibernetică.	0.5
	CP6		
	CPS1		
	CPS2		
Competenţe transversale	CT1	Aplicarea, în contextul respectării legislației, a drepturilor de proprietate intelectuală, a principiilor, normelor și valorilor codului de etică profesională în cadrul propriei strategii de muncă riguroasă, eficientă și responsabilă.	0.1
	CT2	Identificarea rolurilor și responsabilităților într-o echipă specializată, luarea deciziilor și atribuirea de sarcini, cu aplicarea de tehnici de relaționare și muncă eficientă în cadrul echipei.	0.1
	CT3	Dezvoltarea spiritului de creativitate, inițiativă și acțiune, pentru actualizarea cunoștințelor profesionale, economice și de cultură organizațională.	0.2
	CTS		

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

7.1 Obiectivul general al disciplinei	● Înțelegerea conceptelor și formarea abilităților de a lucra cu sisteme de detecție și prevenție a atacurilor informatice
7.2 Obiective specifice	● Prezentare generală a tipurilor de sisteme de detecție a intruziunilor și a modalităților de prevenție a acestora ● Prezentarea generală a framework-urilor de securitate și a conceptelor din spatele schimburilor de informații în domeniul cybersecurity ● Mecanisme cloud de protecție împotriva atacurilor DDoS

8. Conţinuturi

8.1 Curs[18]	Metode de predare[19]	Observaţii
1. Framework-uri de securitate (2h) 1.1. NIST 1.2. ISO 27K 1.3. COBIT 1.4. Cyber Essentials Framework 2. Tipuri de Sisteme de Detecție a Intruziunilor (IDS) (2h) 2.1. Network based IDS (Snort, Suricata) 2.2. Host based IDS (OSSEC, File Integrity Monitoring) 2.3. Soluții hibride HIDS & NIDS (AT&T Cybersecurity) 2.4. Integrarea pachetelor IDS/IPS pe dispozitive hardware (Mikrotik, Netgate pfSense) 3. Network based intrusion detection systems (NIDS) (2h) 3.1. Principii de plasare a senzorilor 3.2. STAT Framework și infrastructura MetaSTAT 3.3. Analiza traficului de rețea 4. Host based intrusion detection systems (HIDS) (2h) 4.1. Principii de plasare a senzorilor 4.2. Analiza și monitorizarea configurației sistemelor 4.3. Analiza și monitorizarea aplicațiilor (Tripwire, AFICK)	prelegere cu videoproiector	

[16] *Din planul de învăţământ*

[17] *Creditele alocate disciplinei se distribuie pe competenţe profesionale şi transversale în funcţie de specificul disciplinei*

[18] *Titluri de capitole şi paragrafe*

[19] *Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuţii cu studenţii (pentru fiecare capitol, dacă este cazul)*

5. Detecția bazată pe semnături (2h) 6. Detecția bazată pe anomalii (2h) 7. Stateful protocol analysis detection (2h) 8. Sisteme de Prevenție a Intruziunilor (IPS) (4h) 8.1. Identificarea posibilelor incidente 8.2. Modalități de jurnalizare 8.3. Tehnici de stopare a incidentelor 8.4. Coduri de bune practici în raportarea incidentelor 9. Malware Information Sharing Platform (4h) 9.1. Introducere în Cybersecurity Information Sharing 9.2. Extinderea modelelor datelor în MISP 9.3. Culegerea, prelucrarea și analiza datelor în cadrul unui exercițiu OSINT 10. Tehnici de contracarare IDS/IPS (Evasion techniques) (2h) 10.1. Decodarea unidirecțională și bidirecțională a protocoalelor 10.2. Implementarea man-in-the-middle (MiTM) în IDS/IPS 10.3. Reasamblarea segmentelor de date 10.4. NGFW (Next-Generation Firewall) 11. Mecanisme cloud pentru protecție împotriva atacurilor tip DDoS (2h) 11.1. Etapele contracarării atacurilor tip DDoS specifice cloud 11.2. Studii de caz CDN: Cloudflare, Akamai, Amazon CloudFront, Reblaze 12. Honeypots (2h) 12.1. Server-side și Client-side honeypots 12.2. Honeypot-uri specializate (spam, malware, baze de date, spider, ssh, http) 12.3. Studiu de caz: implementarea unui honeypot SSH/Telnet în Python		
Bibliografie curs: 1. V. Kumar, J. Srivastava, A. Lazarevic, “Managing cyber threats : issues, approaches, and challenges”, Springer, 2005 2. N. Archibald, G. Ramirez, N. Rathaus, J. Burke, B. Caswell, R. Deraison, “Nessus, Snort, and Ethereal Power Tools”, Syngress, 2005 3. B. Caswell, J. Beale, A. Baker, “Snort IDS and IPS Toolkit”, Syngress, 2007 4. P. A. Porras, “A State Transition Analysis Tool For Intrusion Detection”, University of California at Santa BarbaraComputer Science Dept. College of Engineering Santa Barbara, 1993 5. S. McClure, J. Scambray, G. Kurtz, “Hacking Exposed –Network Security Secrets Exposed”, ediția a 7-a, McGraw-Hill Education, 2012 6. Fortinet HandBook, https://docs.fortinet.com/document/fortigate/6.0.0/handbook, 2020 7. C. Keong, L. Pan, Y. Xiang, “Honeypot Frameworks and Their Applications”, Springer, 2018		
8.2a Seminar	Metode de predare[20]	Observaţii
8.2b Laborator	Metode de predare[21]	Observaţii
1. Analiza traficului de rețea 2. Network based IDS - Snort 3. Network based IDS - Surricata 4. Network based IDS - Zeek (Bro) 5. Host based IDS 6. Pachete IDS/IPS pe dispozitive hardware 7. Detecția bazată pe semnături 8. Detecția bazată pe anomalii 9. Introducere în MISP. Scrierea regulilor YARA. 10. Configurări avansate în MISP 11. Exercițiu Open-Source Intelligence în MISP 12. Module MISP. Integrarea în comunitatea MISP 13. man-in-the-middle (MiTM) în Next-Generation Firewall (NGFW); Exercițiu ENISA Honeypots CERT 14. Implementarea unui honeypot SSH/Telnet în Python	demonstrații, discuții, analiză	
8.2c Proiect	Metode de predare[22]	Observaţii
Bibliografie aplicaţii (seminar / laborator / proiect): 1. https://www.snort.org/documents		

[20] *Discuţii, dezbateri, prezentare şi/sau analiză de lucrări, rezolvare de exerciţii şi probleme*

[21] *Demonstraţie practică, exerciţiu, experiment*

[22] *Studiu de caz, demonstraţie, exerciţiu, analiza erorilor etc*.

2. https://suricata.readthedocs.io/en/latest/
3. https://docs.zeek.org/en/current/
4. https://yara.readthedocs.io/en/latest/
5. https://github.com/MISP/misp-book
6. https://pymisp.readthedocs.io/en/latest/
7. Honeypots CERT Exercise Handbook, 2012, https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/Honeypots_CERT_Exercise_Handbook.pdf
8. https://cowrie.readthedocs.io/en/latest/

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului[23]

- Cunoștințele acumulate în cadrul acestei discipline sunt necesare pentru o bună înțelegere a conceptelor din spatele sistemelor de detecție și prevenție a atacurilor informatice.
- Competențele dobândite vizează, în principal, familiarizarea studenților cu tehnologiile sistemelor de detecție și prevenție a atacurilor informatice.
- Domeniul detecției și prevenției atacurilor informatice este unul extrem de dinamic, iar cererea pe piața muncii pentru specialiști în acest domeniu este în continuă creștere.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare		10.3 Pondere din nota finală
10.4a Examen	● Cunoştinţe teoretice şi practice însuşite (cantitatea, corectitudinea, acurateţea)	Teste pe parcurs[24]:		60% (minim 5)
		Teme de casă:		
		Alte activităţi[25]:		
		Evaluare finală:	100% (minim 5)	
10.4b Seminar	● Frecvenţa/relevanţa intervenţiilor sau răspunsurilor	Evidenţa intervenţiilor, portofoliu de lucrări (referate, sinteze ştiinţifice)		
10.4c Laborator	● Cunoaşterea aparaturii, a modului de utilizare a instrumentelor specifice; evaluarea unor instrumente sau realizări, prelucrarea şi interpretarea unor rezultate	● Chestionar scris ● Răspuns oral ● Caiet de laborator (lucrări experimentale, referate) ● Demonstraţie practică		40% (minim 5)
10.4d Proiect	● Calitatea proiectului realizat, corectitudinea documentaţiei proiectului, justificarea soluţiilor alese	● Autoevaluarea, prezentarea şi/sau susţinerea proiectului ● Evaluarea critică a unui proiect		
10.5 Standard minim de performanţă[26]				

Data completării, Semnătura titularului de curs, Semnătura titularului de aplicaţii,

13.01.2021 ș.l. dr. ing. Cristian Nicolae Buțincu ș.l. dr. ing. Cristian Nicolae Buțincu

Data avizării în departament, Director departament,

13.01.2021 Conf.dr.ing. Andrei Stan

[23] *Legătura cu alte discipline, utilitatea disciplinei pe piaţa muncii*

[24] *Se va preciza numărul de teste şi săptămânile în care vor fi susţinute.*

[25] *Cercuri ştiinţifice, concursuri profesionale etc.*

[26] *Se particularizează la specificul disciplinei standardul minim de performanţă din grila de competenţe a programului de studii, dacă este cazul.*