ANALIZA MALWARE ȘI INVESTIGAȚII DIGITALE

1. Date despre disciplină/modul

Facultatea	Calculatoare, Informatică şi Microelectronică				
Departamentul	Inginerie Software şi Automatica				
Ciclul de studii	Ciclul II, Studii superioare de master				
Programul de studii	Securitate informațională				
Anul de studii	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opţionalitate**	**Credite ECTS**
Anul I *(învăţământ cu frecvenţă)*	I	E	F – unitate de curs fundamentală	O - unitate de curs obligatorie	5

2. Timpul total estimat

Total ore în planul de învăţământ	**Din care**				
	Ore auditoriale		**Lucrul individual**		
	Curs	**Laborator/ seminar**	**Proiect de an**	**Studiul materialului teoretic**	**Pregătire aplicaţii**
Învăţământ cu frecvenţă	20	20		60	50

3. Precondiţii de acces la disciplină/modul

Conform planului de învăţământ	Programarea calculatoarelor, Programarea orientată pe obiecte, Arhitectura calculatoarelor, Sisteme de operare: mecanisme interne și principii de proiectare, Rețele de calculatoare
Conform competenţelor	Programare C/C++/Java/Python, Limbaje de asamblare x86, Arhitectura sistemelor de operare, Protocoale și analiza traficului de rețea

4. Condiţii de desfăşurare a procesului educaţional pentru

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector și acces la Internet. Fiecare student trebuie sa se prezinte cu cîte un laptop, pentru a putea îndeplini activitățile practice. Cursul va începe la timpul planificat și comunicat studentilor în prealabil. Convorbirile telefonice în timpul cursului nu sunt tolerate. Alternativ cursul se poate derula in sistem online, pe platforma educationala a universitatii.
Laborator/ seminar	Studenții vor fi evaluați în baza activității în timpul cursului și a lucrărilor practice la cunoașterea pe capitole a materialului studiat. La indicațiile profesorului studenții vor efectua lucrări practice și vor perfecta rapoarte. Toate lucrările de laborator vor fi prezentate pînă la sfîrșitul cursului.

5. Competenţe specifice acumulate

Competenţe profesionale	**C3 Modelarea sistemelor complexe de securitate și implementarea lor prin sisteme informatice** C3.1 Identificarea și definirea conceptelor, procedeelor și metodelor de securitate a informației folosite în realizarea *măsurilor de control ce reies din necesități* ale activității umane C3.2 Explicarea tehnologiilor potrivite pentru realizarea sistemelor de securitate necesare în activitățile organizațiilor C3.3 Utilizarea tehnologiilor moderne în definirea soluțiilor de securitate C3.4 Utilizarea de criterii și metode determinate de tehnologii pentru evaluarea conformității cu standardele de interoperabilitate C3.5 Dezvoltarea măsurilor de control și securitate utilizând tehnologii moderne de transmitere, stocare și procesare date în corespundere cu necesitățile unei organizații

	C4 Cercetarea științifica privind metodele și tehnologiile de dezvoltare a soluțiilor de securitate C4.1 Identificarea și definirea conceptelor și metodelor focusate pe *procesul de dezvoltare, implementare și utilizare a soluțiilor de securitate* C4.2 Explicarea conceptelor și metodelor folosite pentru dezvoltarea, implementarea și utilizarea măsurilor de control și securitate C4.3 Aplicarea limbajelor de programare, a mediilor de modelare și dezvoltare, a metodologiilor pentru crearea de sistemelor de securitate C4.4 Utilizarea de criterii și metode de evaluare a *procesului de elaborare* a sistemelor de securitate din punct de vedere a calității și performanțelor C4.5 Dezvoltarea și implementarea de software de securitate pentru probleme concrete din diverse domenii ale activității umane **C5 Managementul sistemelor de securitate în concordanța cu cerințele pieței** C5.1 Identificarea și definirea de componente arhitecturale hardware, software și de comunicații, precum și celor necesare la *descrierea unei infrastructuri de protecție* C5.2 Explicarea interacțiunii și funcționării componentelor arhitecturale și de infrastructură specifice domeniului securității C5.3 Aplicarea metodelor de bază pentru specificarea de soluții arhitecturale și de infrastructură pentru probleme tipice de securitate C5.4 Utilizarea de criterii și metode de *evaluare a caracteristicilor funcționale și nefuncționale ale componentelor* sistemului de securitate C5.5 Implementarea unei soluții arhitecturale și de infrastructură în baza unor constrângeri enunțate de proiectele din domeniul securității
Competenţe transversale	CT1. Comportarea onorabilă, responsabilă, etică, în spiritul legii, pentru a asigura reputația profesiei CT3. Demonstrarea spiritului de creativitate, inițiativă și acțiune, pentru actualizarea cunoștințelor profesionale, economice și de cultură organizațională

6. Obiectivele disciplinei/modulului

Obiectivul general	Însușirea conceptelor, metodelor și tehnicilor de analiza a programelor malițioase, precum și a metodelor de investigație digitală.
Obiectivele specifice	Prezentarea aspectelor teoretice și practice ale tehnicilor și metodelor de inginerie inversă. Dezvoltarea capacității de analiză, descriere, detectare a programelor malware pe platformele Windows/Linux/Android. Dezvoltarea deprinderilor în utilizarea instrumentelor de analiză malware. Însușirea abilităților de recunoaștere a unui sistem infectat.

7. Conţinutul disciplinei/modulului

Tematica activităţilor didactice	**Numărul de ore învăţământ cu frecvenţă**
Tematica cursului	
1. Tehnici criptografice utilizate de aplicatiile malitioase (sisteme criptografice asimetice si simetrice). Studiu de caz aplicatiile malitioase tip ransomware.	**4**
2. Analiza statică, dinamică și de comportament	**2**
3. Mecanismele de protecție în programele malițioase (obfuscare, criptare, anti debugging, anti sandboxing și virtualizare)	**2**
4. Utilitare utilizate in investigatiile digitale (analiza traficului de retea,	**4**
5. Analiza programelor malitioase pe diverse sisteme de operare	**2**
6. Atacuri tip APT	**2**
7. Realizarea investigatiilor digitale	**2**
8. Evaluarea de securitate ca parte impotriva aplicatiilor malitioase si zero-day vulnerability	**2**
Total curs:	**20**
Tematica lucrărilor de laborator	
L.1. Analiza traficului de rețea a programelor malițioase	**5**

Tematica activităţilor didactice	Numărul de ore învăţământ cu frecvenţă
L.2. Conceptele ingineriei inverse. Analiza statică, dinamică și de comportament. Tehnici de protecție în programele malițioase	**5**
L.3. Analiza programelor malițioase pe platforma Windows	**5**
L.4. Analiza programelor malițioase pe platformele Linux și Android	**5**
Total lucrări laborator:	**20**

8. Referinţe bibliografice

Principale	1. Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software (Andrew Honig, Michael Sikorski, 2012, No Starch Press) http://venom630.free.fr/pdf/Practical_Malware_Analysis.pdf 2. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation (Dang, Bruce -2014 – Wiley), https://repo.zenk-security.com/Reversing%20.%20cracking/Practical%20Reverse%20Engineering.pdf 3. Ahmed BALCI, Dan UNGUREANU, Jaromir VONDRUSKA, Malware Reverse Engineering Handbook, NATO CCDCOE, Tallinn, 2020. -56 p. https://ccdcoe.org/uploads/2020/07/Malware_Reverse_Engineering_Handbook.pdf 4. Dennis YURICHEV, Reverse Engineering for Beginners, 2016 -942 p., https://lira.epac.to/DOCS-TECH/Hacking/Reverse%20Engineering%20for%20Beginners.pdf
Suplimentare	1. E. Simion and V. Pasca, Cyber-Physical System Security, Chapter Challenges in cyber security - Ransomware Phenomenon, Proc. of the First Cyber-Physical Security, pp. 303-330, Springer International Publishing, Springer Nature Switzerland AG, 2018, Koc Ed., ISBN 978-3-319-98934-1. 2. V. Craciun, A. Mogage and Emil Simion, Trends in design of ransomware viruses, Proc. of the 11th International Conference on Security for Information Technology and Communication, Bucharest, 08-09 november 2018, Springer Verlag, C. Toma, J. L. Lanet Ed., vol. 11359, https://doi.org/10.1007/978-3-030-12942-2, ISBN 978-3-030-12941-5, pp. 259-272, (ACM Digital Library, Zentralblatt MATH, Scopus). 3. Mihai-Andrei Costandache and Marian-Stefan Mihalache and Emil Simion, New directions in the ransomware phenomenon, https://eprint.iacr.org/2020/1610.

9. Evaluare

Periodică		Curentă	Studiu individual	Proiect/teză	Examen
EP 1	**EP 2**				
Învăţământ cu frecvenţă					
15%	15%	15%	15%		40%

10. Criterii de evaluare

Activitate	Componente evaluare	Metodă de eevaluare, Criterii de evaluare	Pondere în nota finală a activității	Ponderea în evaluarea disciplinei
Evaluare periodică I	Conținut teoretic, teme 1-4	Test pe MOODLE	100%	**15%**
Evaluare periodică II	Conținut teoretic, teme 5-8	Test pe MOODLE	100%	**15%**
Evaluare curentă	Activitatea practică	Discuții în cadrul seminarelor	50%	**15%**
		Dosar completat cu Rapoarte pentru fiecare Studiu de caz în discuție	50%	
Studiul individual	Cercetare la temă	Prezentare/discurs public	100%	**15%**
Evaluarea finală	Conținut teoretic și prcatic	Examen oral. Notare conform baremului	100%	**40%**