MD-2068, CHIŞINĂU, STR. STUDENŢILOR, 9/7, TEL: 022 50-99-63, www.utm.md

TEHNICI DE INGINERIE INVERSĂ

1. Date despre disciplină

Facultatea	Calculatoare, Informatică și Microelectronică				
Departamentul	Ingineria Software și Automatică				
Ciclul de studii	Studii superioare de licență, ciclul I				
Programul de studii	0714.4 Automatică și Informatică				
Anul de studii	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opționalitate**	**Credite ECTS**
Anul III *(învățământ cu frecvență)*	6	E	L– unitate de curs la liberă alegere	A - unitate de curs opțională	3

2. Timpul total estimat

Total ore în planul de învățământ	**Din care**				
	Ore auditoriale		**Lucrul individual**		
	Curs	**Laborator/seminar**	**Proiect de an**	**Studiul materialului teoretic**	**Pregătire aplicații**
Învățământ cu frecvență	15	30/0		15	30

3. Precondiții de acces la disciplină

Conform planului de învățământ	Programarea calculatoarelor, Programarea orientată pe obiecte Arhitectura calculatoarelor, Sisteme de operare: mecanisme interne și principii de proiectare.
Conform competențelor	Programare C/C++, Limbaje de asamblare x86, Arhitectura sistemelor de operare.

4. Condiții de desfășurare a procesului educațional pentru

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector, PC/laptop și acces la internet. Nu vor fi tolerate întârzierile, precum și convorbirile telefonice în timpul cursului.
Lucrări practice/ seminare	Studenții vor fi evaluați prin teste teoretice și lucrări practice la cunoașterea pe capitole a materialului studiat. Evaluările vor fi petrecute peste o săptămână după ce materialul a fost predat la curs. La indicațiile profesorului studenții vor efectua lucrări practice și vor perfecta rapoarte. Termenul de susținere a testelor și/sau de predare a lucrărilor de laborator este de o săptămână după petrecerea acesteia. Pentru susținerea sau predarea cu întârziere a testelor sau a lucrărilor acestea se vor depuncta cu 1pct./săptămână de întârziere.

5. Competențe specifice acumulate

Competențe profesionale	**C1 Competențe privind operarea cu concepte și metode științifice în domeniul ingineriei inverse** • Identificarea și definirea conceptelor, teoriilor și metodelor tehnicile de inginerie inversă. • Analiza și înțelegerea claselor de software malițios, noi tehnici de atac, persistență, escaladarea privilegiilor etc., precum și compararea lor cu tehnicile cunoscute. • Utilizarea tehnologiilor moderne de analiză, dezasamblare și depanare a software-ului. • Recunoașterea comportamentală a sistemelor infectate cu malware. • Definirea și analiza exploit-urilor.
Competențe transversale	**C2** Identificarea, descrierea și derularea activităților organizate într-o echipă cu dezvoltarea capacităților de comunicare și colaborare, dar și cu asumarea diferitelor roluri (de execuție și conducere). **C3** Identificarea oportunităților de formare continuă și valorificarea eficientă a resurselor și tehnicilor de învățare pentru propria dezvoltare.

6. Obiectivele disciplinei

Obiectivul general	Însușirea conceptelor, metodelor și tehnicilor de inginerie inversă.
Obiectivele specifice	Prezentarea aspectelor teoretice și practice ale tehnicilor și metodelor de inginerie inversă. Dezvoltarea capacității de analiză, descriere, detectare a programelor malware. Dezvoltarea deprinderilor în utilizarea instrumentelor de analiză malware. Însușirea abilităților de recunoaștere a unui sistem infectat.

7. Conținutul disciplinei

8. Tematica activităților didactice	Numărul de ore învățământ cu frecvență
Tematica prelegerilor	
T.1. Introducere. Descrierea cursului**.** Structura și procedura de parcurgere.	2
T.2. Tehnici, metode și instrumente de analiză malware.	2
T.3. Tehnici de obfuscare a programelor malware. Detecție**.**	1
T.4. Analiza statică a codului sursă/malware.	1
T.5. Instrumente și tehnici de analiză statică (ex:VirusTotal, HybridAnalysis).	1
T.6. Dezasamblarea software-ului. Instrumente (ex: IDA, Ghidra).	1
T.7. Analiză dinamică a codului sursă/malware.	1
T.8. Analiza comportamentală a software-ului. Instrumente (ex. Process Monitor, Process Explorer).	1
T.9. Sisteme de sandboxing (ex: Cuckoo Sandbox, Windows Sandbox)	1
T.10 Instrumente și tehnici de depanare software (ex: IDA, WinDbd; Breakpoint)	1
T.11 Analiza traficului de rețea.	1
T.12 Analiza și detecția sistemelor infectate.	1
T.13 Analiza exploit-urilor.	1
Total ore de curs:	**15**

Tematica lucrărilor de laborator/seminarelor	
L.1. Setarea și configurarea mediului virtual pentru analiza malware**.**	4
L.2. De-obfuscarea codului malițios javascript	4
L.3. Analiza statică a programelor malware.	4
L.4. Dezasamblarea software utilizând IDA/Ghidra.	4
L.5. Analiza traficului de rețea.	4
L.6 Analiza și recunoașterea unui sistem infectat.	4
L.7 Analiza exploit-urilor.	6
Total lucrări de laborator/seminare:	**30**

9. Referințe bibliografice

Principale	1. 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 2. 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 3. Dennis YURICHEV, Reverse Engineering for Beginners, 2016 -942 p., https://lira.epac.to/DOCS-TECH/Hacking/Reverse%20Engineering%20for%20Beginners.pdf 4. CS 675 Reverse Software Engineering, Masters in Computer Science, Drexel University, Philadelphia, USA, https://www.cs.drexel.edu/~spiros/teaching/CS675/
Suplimentare	1. The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler (Eagle, Chris – 2011 – No Strach Press). 2. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software (Sikorski, Michael – 2012 – No Strach Press).

10. Utilizarea IA generativă

Permisiunea de utilizare	Utilizarea IA generative în cadrul temelor și proiectelor este permisă, cu condiția ca studenții să respecte următoarele reguli: • IA generativă poate fi utilizată pentru generarea de idei, structuri de text sau cod, dar toate materialele generate trebuie să fie revizuite și ajustate de către student pentru a se asigura că acestea corespund cerințelor academice.

	• Orice utilizare a IA generative trebuie să fie declarată în secțiunea de apendice a fiecărei lucrări, folosind fraza: "În timpul pregătirii acestei lucrări, autorul a utilizat [NUME INSTRUMENT / SERVICIU] în scopul [MOTIV]. După utilizarea acestui instrument/serviciu, autorul a revizuit și editat conținutul după cum a fost necesar și își asumă întreaga responsabilitate pentru conținutul lucrării."
Restricții de utilizare	Studenții nu trebuie să considere IA generativă ca o sursă de încredere pentru informații, deoarece nu oferă referințe clare sau surse documentate. • Nu este permisă citarea directă a conținutului generat de IA în lucrările academice ca și cum ar fi sursă primară. • Activitățile în care este interzis utilizarea IA generativă sunt specificare de profesor și sunt de regulă evaluări intermediare și finale sau care nu presupun activități de dezvoltare a competenților profesionale.

11. Evaluare

Periodică		**Curentă**	**Proiect**	**Examen**
EP 1	**EP 2**			
Învățământ cu frecvență				
20%	20%	20%	-	40%
Standard minim de performanță. Prezența și activitatea la prelegeri și lucrări practice. Prezentarea proiectului de an. Obținerea notei minime de „5” la fiecare lucrări practice și proiectul de an.				

12. Criterii de evaluare

Activitate	**Componente evaluare**	**Metodă de evaluare, Criterii de evaluare**	**Pondere în nota finală a activității**	**Ponderea în evaluarea disciplinei**
Învățământ cu frecvență				
Evaluare periodică I	Conținut teoretic, teme 1-7	Test pe MOODLE	100%	**20%**
Evaluare periodică II	Conținut teoretic, teme 8-13	Test pe MOODLE	100%	**20%**
Evaluare curentă	Activitatea practică	Discuții în cadrul orelor de practică	50%	**10%**
		Raport pentru fiecare lucrare de practică încărcat pe MOODLE	50%	
Lucrul individual/Proiect de an	Cercetare la temă	Referat/Prezentare/discurs public. Raportul încărcat pe MOODLE	100%	**10%**
Evaluarea finală	Conținut teoretic și practic	Test pe MOODLE	100%	**40%**