FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare si Tehnologia Informatiei
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Securitatea Informatiilor si Sistemelor de calcul/ Master
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	3.

2. Date despre disciplină

2.1 Denumirea disciplinei				***Inginerie inversă și analiza de software malițios***	
2.2 Titularii de curs				Drd. ing. Andrei Mihalca (amihalca@bitdefender.com)	
2.3 Titularul/Titularii activităţilor de seminar/laborator/proiect				Drd. ing. Andrei Mihalca (amihalca@bitdefender.com) Ing. Gergo Szeles	
2.4 Anul de studiu	I	2.5 Semestrul	1	2.6 Tipul de evaluare *(E – examen, C – colocviu, V – verificare)*	E
2.7 Regimul disciplinei	*DA – de aprofundare, DS – de sinteza, DC – complementară*				DS
	DI – Impusă, DOp – opțională, DFac – facultativă				DI

3. Timpul total estimat

3.1 Număr de ore pe săptămână	4	din care:	Curs	1	Seminar	1	Laborator	2	Proiect	
3.2 Număr de ore pe semestru	56	din care:	Curs	14	Seminar	14	Laborator	28	Proiect	
3.3 Distribuţia fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie şi notiţe										16
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren										16
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri										35
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activităţi:										0

3.4 Total ore studiu individual (suma (3.3(a)...3.3(f)))	69
3.5 Total ore pe semestru (3.2+3.4)	125
3.6 Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Programarea calculatoarelor, Arhitectura calculatoarelor, Sisteme de operare
4.2 de competenţe	Limbaje de asamblare x86, Programare C, Arhitectura sistemelor de operare

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Tabla, proiector, calculatoare
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Tabla, proiector, calculatoare

6. Competenţele specifice acumulate

6.1 Competenţe profesionale	C2. Investigarea și analiza situațiilor de criminalitate informatică și a software-ului malițios prin metode avansate de tip inginerie inversă și monitorizare comportament • C2.1 – Cunoașterea aprofundată a clasificării, caracteristicilor și particularităților aferente diferitelor tipuri de atacuri informatice și softurilor malițioase • C2.2 – Analiza și înțelegerea a noi clase de software malițios, noi tehnici de atac, persistență, escaladarea privilegiilor etc., precum și compararea lor cu tehnicile cunoscute • C2.3 – Capacitatea de a face corelări și de a putea identifica obiecte

	potențial malițioase chiar dacă nu se poate analiza complet obiectul respectiv • C2.4 – Determinarea limitărilor teoretice și practice oferite de diverse metode de automatizare a analizei software-ului malițios. Propunerea de alternative mai bune unde este posibil • C2.5 – Elaborarea unor noi clase de atacuri sau software malițios, și propunerea unor noi proprietăți potrivite clasificării codurilor malițioase C4. Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate • C4.2 – Identificarea de noi scenarii în care este nevoie de introducerea unei soluții de securitate sau utilizarea unei unelte de securitate. Analiza soluțiilor de securitate propuse și compararea lor cu cele cunoscute anterior • C4.3 – Dezvoltarea unor module software complexe respectând principiile metodologiilor de dezvoltare corectă a unui software din perspectiva securității. Dezvoltarea unor utilitare de analiză sau de validare a securității • C4.5 – Dezvoltarea unor module software sau a unor utilitare care să ajute la asigurarea unui înalt grad de securitate. Propunerea unor scenarii și modalități de testare a unor proiecte existente, cu scopul de a verifica și asigura calitatea lor din punctul de vedere al securității
6.2 Competenţe transversale	N/A

7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	Familiarizarea studenților cu softurile malițioase, înțelegerea modului de funcționare a atacurilor informatice, obținerea cunoștințelor necesare pentru recunoașterea și investigarea unui sistem infectat
7.2 Obiectivele specifice	1. Înțelegerea modului de funcționare a unui software malițios 2. Obținerea cunoștințelor necesare pentru identificarea unui software malițios 3. Însușirea abilității de recunoaștere a unui sistem infectat

8. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Arhitectura sistemelor x86	1	Expunere la tablă, prezentare cu video-proiectorul, discuții	
Limbajul de asamblare x86	1		
Structura sistemelor de operare Microsoft Windows: user-mode, kernel-mode, Win32 APIs	1		
Formatul fișierelor MZPE (1)	1		
Formatul fișierelor MZPE (2)	1		
Dezasamblarea codului compilat	1		
Decompilarea programelor	1		
Rularea in sisteme virtualizate și unelte de monitorizare	1		
Depanare folosind depanatoare (ex. OllyDgb)	1		
Tehnici de anti-analiza si anti-emulare	1		
Packer-e și protectoare	1		
Malware polimorfici și metamorfici	1		
Analiza exploit-urilor	1		
Analiza aplicațiilor mobile	1		

Bibliografie *(bibliografia minimală a disciplinei conținând cel puțin o lucrare bibliografică de referință a disciplinei, care există la dispoziţia studenţilor într-un număr de exemplare corespunzător)*

1) Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software (Sikorski, Michael – 2012 – No Strach Press)
2) The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler (Eagle, Chris – 2011 – No Strach Press)
3) The Art Of Computer Virus Research And Defense (Szor, Peter - 2005 - Addison-Wesley)
4) Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation (Dang, Bruce -

2014 - Wiley)
5) The Life of Binaries (Xeno Kovah – 2013 – http://opensecuritytraining.info/LifeOfBinaries.html)

8.2 Aplicații (**seminar**/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Recapitulare elemente de bază în programare în limbaj de asamblare		Expuneri la tablă, exerciții pe calculator, discuții și explicații suplimentare	
Elemente specifice de securitate în programare în limbaj de asamblare			
Programare folosind Win32-APIs (1)			
Programare folosind Win32-APIs (2)			
Decompilarea și analiza programelor folosind IdaPro (1)			
Decompilarea și analiza programelor folosind IdaPro (2)			
Decompilarea și analiza programelor folosind IdaPro (3)			
Analiza dinamica în sisteme virtualizate si unelte de monitorizare			
Analiza dinamica folosind OllyDbg			
Sisteme de sandbox-ing			
Analiza sistemelor infectate			
Dezinfecția sistemelor infectate			
Analiza exploit-urilor			
Colocviu de evaluare a cunoștințelor			

Bibliografie *(bibliografia minimală pentru aplicații conținând cel puțin o lucrare bibliografică de referință a disciplinei care există la dispoziția studenților într-un număr de exemplare corespunzător)*

1) Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software (Sikorski, Michael – 2012 – No Strach Press)
2) The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler (Eagle, Chris – 2011 – No Strach Press)
3) The Art Of Computer Virus Research And Defense (Szor, Peter - 2005 - Addison-Wesley)
4) Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation (Dang, Bruce - 2014 - Wiley)
5) The Life of Binaries (Xeno Kovah – 2013 – http://opensecuritytraining.info/LifeOfBinaries.html)

*Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.

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

Se realizează prin discuții periodice cu reprezentanți ai angajatorilor semnificativi, în special cei care angajează pe proiecte din domeniul securității informațiilor.
Cursuri de inginerie inversă și analiză de software malițios sunt prezente în cadrul multor alte masterate din domeniul securității calculatoarelor și a informațiilor, cum ar fi:

- *CS 675 Reverse Software Engineering*, Masters in Computer Science, Drexel University, Philadelphia, USA. https://www.cs.drexel.edu/~spiros/teaching/CS675/
- *CISC6800 Malware Analytics and Software Security*, Fordham University, Masters Degree in Cybersecurity, New York, USA http://www.fordham.edu/academics/colleges__graduate_s/undergraduate_colleg/school_of_profession/pcs_home/degrees_and_programs/ms_cybersecurity_94711.asp
- *Malware*, Masters in Cybersecurity, Tallinn University of Technology, Estonia. http://www.ttu.ee/studying/masters/masters_programmes/cyber-security/cyber-security-4/

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de curs	Examen scris și/sau tip grilă (pe platforma Moodle) și/sau prezentarea unei teme de cercetare din domeniul cursului. In situații excepționale, care necesită desfășurarea activităților didactice de la	50%

		distanță, examinarea poate avea loc online, de la distanță, folosind platformele Moodle și Teams.	
Seminar	Abilitatea de analiză a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de seminar	Realizarea activităților de seminar și rezolvarea temelor de casă și/sau a unor probleme de analiză software malițios în cadrul unui examen scris. In situații excepționale, care necesită desfășurarea activităților didactice de la distanță, examinarea poate avea loc online, de la distanță, folosind platformele Moodle și Teams.	10%
Laborator	Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de laborator	Realizarea activităților de laborator și rezolvarea temelor de casă și/sau a unor probleme de analiză software malițios în cadrul unui examen practic. In situații excepționale, care necesită desfășurarea activităților didactice de la distanță, examinarea poate avea loc online, de la distanță, folosind platformele Moodle și Teams.	40%
Proiect			

Standard minim de performanţă

Curs. Prezența la **minim 50%** din orele de curs, pentru admiterea la examenul final. Demonstrarea înțelegerii modului de funcționare a unui program malițios.

Aplicații. Prezența la laborator **obligatorie 100%** (1 seminar / 2 laboratoare se pot recupera în timpul semestrului, iar alte 2 / 1 în sesiunile de restanțe) pentru admiterea la examenul final. Identificarea prin analiză statică a unui software malițios. Identificarea prin analiză dinamică a unui software malițios.

Data completării:	**Titulari**	**Titlu Prenume NUME**	**Semnătura**
	Curs	Drd.ing. Andrei Mihalca	
	Aplicații	Drd.ing. Andrei Mihalca	
		Ing. Gergo Szeles	

Data avizării în Consiliul Departamentului Calculatoare	Director Departament Prof.dr.ing. Rodica Potolea
Data aprobării în Consiliul Facultății de Automatică și Calculatoare	Decan Prof.dr.ing. Liviu Miclea