FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	**Universitatea “Alexandru Ioan Cuza” din Iaşi**
1.2 Facultatea	**Facultatea de Informatica**
1.3 Departamentul	**Informatica**
1.4 Domeniul de studii	**Informatica**
1.5 Ciclul de studii	**Master, Semestru 2**
1.6 Programul de studii / Calificarea	

2. Date despre disciplină

2.1 Denumirea disciplinei			Securitatea sistemelor de operare si sisteme malitioase				
2.2 Titularul activităţilor de curs			**Conf. Dr. Gavrilut Dragos**				
2.3 Titularul activităţilor de seminar			**Cont. Dr. Gavrilut Dragos**				
2.4 An de studiu	**1**	**2.5** Semestru	**1**	**2.6** Tip de evaluare		**2.7** Regimul disciplinei*	**OP**

** OB – Obligatoriu / OP – Opţional*

3. Timpul total estimat (ore pe semestru şi activităţi didactice)

3.1 Număr de ore pe săptămână	**2**	din care: **3.2** curs	**2**	**3.3** seminar/laborator	**2**
3.4 Total ore din planul de învăţământ	**28**	din care: **3.5** curs	**28**	**3.6** seminar/laborator	**28**
Distribuţia fondului de timp					ore
Studiu după manual, suport de curs, bibliografie şi altele					**14**
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					**14**
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					**28**
Tutoriat					**-**
Examinări					**4**
Alte activităţi					**-**

3.7 Total ore studiu individual	**56**
3.8 Total ore pe semestru	**116**
3.9 Număr de credite	**5**

4. Precondiţii (dacă este cazul)

4.1 De curriculum	**Notiuni de POO. Programare in C++. Arhitectura calculatoarelor.**
4.2 De competenţe	

5. Condiţii (dacă este cazul)

5.1 De desfăşurare a cursului	-
5.2 De desfăşurare a seminarului/ laboratorului	**-**

6. Competenţe specifice acumulate

Competenţe profesionale	**C1. Metode de analiza a programelor malitioase** **C2. Metode de dezinfectie a sistemelor infectate** **C3. Modalitati de creare a unui scanner pentru identificarea SPAM-urilor**
Competenţe transversale	**CT1. Dezvoltarea capacitatii de validare si scriere corecta a unui produs software** **CT2. Intelegerea functionarii unui malware si a modului cum afecteaza el un sistem de operare**

7. Obiectivele disciplinei (din grila competenţelor specifice acumulate)

7.1 Obiectivul general	Pregatirea studentilor pentru a putea aplica tehnici de reverse engineering pentru identificarea de posibile probleme la nivelul codului compilat
7.2 Obiectivele specifice	La finalizarea cu succes a acestei discipline, studenţii vor fi capabili să: ▪ Iidentifice malware pe baza comportamentului lor ▪ Utilizare tool-uril free de dezinfectie existene ▪ Creare unui scanner pentru identificarea SPAM-urilor

8. Conţinut

8.1	**Curs**	**Metode de predare**	**Observaţii** (ore şi referinţe bibliografice)
1.	Clasificarea malware-ilor (1)	C	2
2.	Clasificarea malware-ilor (2)	C	2
3.	Clasificarea malware-ilor (3)	C	2
4.	Istoria malwareilor si evolutia atacurilor malitioase (1)	C	2
5.	Istoria malwareilor si evolutia atacurilor malitioase (2)	C	2

6.	Ransomware (tehnici de tip scareware)	C	2
7.	Ransomware (tehnici de tip locker)	C	2
8.	Exploit-uri moderne (EternalBlue, DoublePulsar)	C	2
9.	Atacuri targetate (1)	C	2
10.	Atacuri targetate (2)	C	2
11.	Malware recenti (1)	C	2
12.	Malware recenti (2)	C	2
13.	Malware recenti (3)	C	2
14.	Malware recenti (4)	C	2

Bibliografie

Referinţe principale:

Referinţe suplimentare:

8.2	**Seminar / Laborator**	**Metode de predare**	**Observaţii** (ore şi referinţe bibliografice)
1.	Pregatirea unei masini virtuale pentru analiza de POC-uri cu actiuni specifice malwareilor	L	2
2.	Analiza de POC-uri cu comportamente similare malware-ului	L	2
3.	Analiza de POC-uri cu comportamente similare malware-ului	L	2
4.	Analiza de POC-uri cu comportamente similare malware-ului	L	2
5.	Analiza de POC-uri cu comportamente similare malware-ului	L	2
6.	Analiza de POC-uri cu comportamente similare malware-ului	L	2
7.	Primul test (dezinfectie)	L	2
8.	Detectie si testare algoritm de anti-spam	L	2
9.	Detectie si testare algoritm de anti-spam	L	2
10.	Detectie si testare algoritm de anti-spam	L	2

11.	Detectie si testare algoritm de anti-spam	L	2
12.	Detectie si testare algoritm de anti-spam	L	2
13.	Detectie si testare algoritm de anti-spam	L	2
14.	Detectie si testare algoritm de anti-spam	L	2

Bibliografie

- **Advanced Malware Analysis , Christopher C. Elisan**
- **Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software, Michael Sikorski and Andrew Honig**
- **Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code, Michael Ligh , Steven Adair, Blake Hartstein, Matthew Richard**

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

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere în nota finală (%)
10.4 Curs		Examen	33%
10.5 Seminar/ Laborator		Proiecte si teme de laborator	66%
10.6 Standard minim de performanţă			
Minim 5 la laborator, minim 5 media finala.			

Data completării

Titular de curs
Gavrilut Dragos

Titular de seminar
Gavrilut Dragos

Data avizării în departament

Director de departament