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	11.

2. Date despre disciplină

2.1 Denumirea disciplinei				***Tratarea incidentelor de securitate și investigarea datelor digitale***	
2.2 Titularii de curs				Dr. ing. Dan LUȚAȘ (dlutas@bitdefender.com)	
2.3 Titularul/Titularii activităţilor de seminar/laborator/proiect				Drd. Ing. Andrei LUȚAȘ (vlutas@bitdefender.com)	
2.4 Anul de studiu	II	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	3	din care:	Curs	2	Seminar		Laborator	1	Proiect	
3.2 Număr de ore pe semestru	42	din care:	Curs	28	Seminar		Laborator	14	Proiect	
3.3 Distribuţia fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie şi notiţe										30
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren										18
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri										33
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activităţi:										0

3.4 Total ore studiu individual (suma (3.3(a)...3.3(f)))	83
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	Securitatea informațiilor, Inginerie inversă și analiza de software malițios
4.2 de competenţe	Arhitectura calculatoarelor, Arhitectura sistemelor de operare, Cunoștințe de bază de rețele de calculatoare

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 C5 - Rezolvarea corectă și eficientă a unor probleme complexe de securitate informatică din lumea reală. Operarea cu metode și modele matematice, tehnici și tehnologii aferente inginerești și informatice specifice domeniului securității informațiilor și sistemelor de calcul • C5.1 – Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate • C5.2 – Analiza și interpretarea de situații noi complexe din lumea reală, prin prisma cunoștințelor fundamentale din domeniul securității informațiilor și sistemelor de calcul. Identificarea și corelarea unor soluții similare cu cele cunoscute, precum și plasarea corectă a ideilor noi în domeniul cercetării și dezvoltării de soluții de securitate informatice • C5.4 – Stabilirea corectă a limitărilor de aplicabilitate în lumea reală a diferitelor tehnologii de securitate. Evaluarea riscurilor potențiale rămase și a priorității lor. Determinarea unor posibile noi arii și metode de cercetare teoretice sau tehnologice care ar putea soluționa riscurile și limitările identificate
6.2 Competenţe transversale	N/A

7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	Familiarizarea studenților cu noțiunile și elementele de bază ale procesului de răspuns la incidente de securitate, conferirea capacității de înțelegere a modului de organizare a activității de răspuns la incidente, de înțelegere a ce, cum, când s-a întâmplat în cadrul unui incident informatic, de a interveni în timp optim pentru atenuarea efectelor incidentului și de a preveni viitoare incidente similare. Se urmărește, de asemenea, conferirea capacității de a analiza în detaliu aspectele tehnice ale incidentului prin investigarea (identificarea, colectarea și analiza) artefactelor digitale rezultate în cadrul acestuia.
7.2 Obiectivele specifice	1. Înțelegerea modului de planificare a activității de răspuns la incidentele de securitate (organizarea echipei, rolul membrilor, competențele necesare, interacțiunea între aceștia) 2. Înțelegerea și utilizarea uneltelor specifice prevenirii apariției incidentelor de securitate (patching-ul vulnerabilităților, monitorizarea log-urilor) 3. Înțelegerea și utilizarea uneltelor specifice în analiza incidentelor de securitate 4. Înțelegerea mecanismelor și utilizarea uneltelor specifice diferitelor tipuri de investigații digitale (a discului, a memoriei volatile, a capturilor de trafic de rețea, a bazelor de date) 5. Înțelegerea tehnicilor prin care poate fi îngreunată activitatea de investigare a datelor digitale (criptarea discului, prevenirea analizei memoriei volatile etc)

8. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Aspecte legale, gestionarea dovezilor digitale, limitări (steganografie, metadate)	2	Expunere la tablă, prezentare cu video-proiectorul, discuții	
Colectare dovezilor prin metode hardware, unelte de inspecție hardware	2		

Tratarea incidentelor de securitate (tratare, proceduri de răspuns - verificare, prioritizare, izolare, eradicare)	2		
Analiza discurilor și a sistemelor de fișiere (1): detalii despre NTFS, FAT, EXT3 etc.	2		
Analiza discurilor și a sistemelor de fișiere (2): unelte de procesare	2		
SO Windows: registry-ul (structură, unelte, tipuri de Informații)	2		
Analiza dump-urilor de memorie (1): crearea dump-urilor de memorie, framework-ul Volatility	2		
Analiza dump-urilor de memorie (2): căutarea de malware avansat, rootkit-uri etc.	2		
Analiza pachetelor de rețea (Wireshark): examinarea diferitelor atacuri, extragerea de date din pachete pentru reconstrucție	2		
Crearea de semnături pentru IDS/IPS: introducere în Snort, analiza și dezvoltarea de semnături Snort	2		
Corelare de evenimente: unelte de procesare a log-urilor pe Windows & Linux, log-uri specifice, timestamp-uri	2		
Investigații digitale pe dispozitive mobile: Android, unelte open/closed source	2		
Investigarea bazelor de date	2		
Subminarea uneltelor de investigare: ștergere sigură, criptarea disk-ului, prevenirea dump-urilor de memorie	2		

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

1. Incident Response and Computer Forensics (Prosise, Chris – 2014 – McGraw-Hill) (3nd ed)
2. Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder (Murdoch, Don – 2014 – CreateSpace Independent Publishing)
3. File System Forensic Analysis (Carrier, Brian – 2005 – Addison-Wesley)
4. The Practice of Network Security Monitoring: Understanding Incident Detection and Response (Bejlitch, Richard – 2013 – No Strach Press)
5. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory (Ligh, Michael Hale – 2014 – Wiley)
6. Placing the Suspect Behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects (Shavers, Brett – 2013 – Syngess)

8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Unelte și tehnici de inspecție hardware	1	Expuneri la tablă, exerciții la calculator, discuții și explicații suplimentare	
Unelte și tehnici de inspecție a sistemului de fișiere	1		
Unelte și tehnici de inspecție a Regystry-ului pe S.O. Windows si a dump-urilor de memorie. Windbg	1		
Inspecția pachetelor de rețea folosind utilitarul Wireshark. IDS, IPS, Snort. Aplicații	1		
Unelte și tehnici de inspecție a log-urilor. Corelare de evenimente	1		
Unelte și tehnici de inspecție pe dispozitive mobile si a bazelor de date	1		
Unelte și tehnici de subminare a investigației	1		

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. Incident Response and Computer Forensics (Prosise, Chris – 2014 – McGraw-Hill) (3nd ed)
2. Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder (Murdoch, Don – 2014 – CreateSpace Independent Publishing)
3. File System Forensic Analysis (Carrier, Brian – 2005 – Addison-Wesley)
4. The Practice of Network Security Monitoring: Understanding Incident Detection and Response (Bejlitch, Richard – 2013 – No Strach Press)
5. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory (Ligh, Michael Hale – 2014 – Wiley)
6. Placing the Suspect Behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects (Shavers, Brett – 2013 – Syngess)

** 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 din tematica Incident Response și Forensic Analysis sunt prezente în cadrul multor alte masterate din domeniul securității calculatoarelor și a informațiilor, cum ar fi:

- *CS6963 Digital Forensics*, Masters in Cybersecurity, New York Polytechnic School of Engineering, New York, USA, http://engineering.nyu.edu/academics/course/CS6963
- *CSEC 661 Digital Forensics Investigation*, Master of Science in Digital Forensics and Cyber Investigation, University of Maryland University College, USA http://www.umuc.edu/academic-programs/masters-degrees/digital-forensics-and-cyber-investigations.cfm
- Masters in Computer Forensics, University of Westminster, UK, http://www.westminster.ac.uk/courses/subjects/computer-science-and-software-engineering/postgraduate-courses/full-time/p09fpcfs-msc-computer-forensics

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 distanță, examinarea poate avea loc online, de la distanță, folosind platformele Moodle și Teams.	50%
Seminar			
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 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.	50%
Proiect			

Standard minim de performanţă

Curs. Prezența la **minim 50%** din orele de curs, pentru admiterea la examenul final. Demonstrarea înțelegerii noțiunilor de bază a activității de răspuns la incidentele de securitate cibernetică, cum ar fi : necesitatea planificării activității de răspuns, componența echipei și competențele necesare membrilor, analiza incidentului. Demonstrarea înțelegerii noțiunilor de bază a activității de investigare a datelor digitale, cum ar fi : tipuri specifice de investigații digitale (disc, memorie volatilă etc), gestionarea probelor, metode de prevenire și de detecție rapidă a incidentelor. Demonstrarea înțelegerii limitărilor tehnicilor de investigare digitală.

Aplicații. Prezența la laborator **obligatorie 100%** (un laboratoar se pot recupera în timpul semestrului, iar altul în sesiunile de restanțe) pentru admiterea la examenul final. Demonstrarea abilității practice de a înțelege și a reconstitui, pe baza analizei unor artefacte digitale (cum ar fi analiza traficului de rețea, analiza log-urilor, analiza codului malițios folosit) desfășurarea unui atac în cadrul unui incident de securitate.

Data completării:	Titulari	Titlu Prenume NUME	Semnătura
	Curs	Dr. ing. Dan LUȚAȘ	
	Aplicații	Drd. ing. Andrei LUȚAȘ	

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