

## FIȘA DISCIPLINEI

### 1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare și Tehnologia Informației
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Securitatea Informațiilor și Sistemelor de calcul/ Master
1.7 Forma de învățământ	IF – învățământ cu frecvență
1.8 Codul disciplinei	6.

### 2. Date despre disciplină

2.1 Denumirea disciplinei	<b>Dezvoltarea și securitatea modulelor kernel</b>				
2.2 Titularii de curs	Drd. Ing. Radu-Marian PORTASE (rportase@bitdefender.com)				
2.3 Titularul/Titularii activităților de seminar/laborator/proiect	Drd. Ing. Radu-Marian PORTASE (rportase@bitdefender.com)				
2.4 Anul de studiu	I	2.5 Semestrul	2	2.6 Tipul de evaluare ( E – examen, C – colocviu, V – verificare)	E
2.7 Regimul disciplinei	DA – de aprofundare, DS – de sinteza, DC – complementară				DA
	DI – Impusă, DOp – opțională, DFac – facultativă				DI

### 3. Timpul total estimat

3.1 Număr de ore pe săptămână	4	din care:	Curs	1	Seminar		Laborator	3	Proiect	
3.2 Număr de ore pe semestru	56	din care:	Curs	14	Seminar		Laborator	42	Proiect	
3.3 Distribuția fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie și notițe										12
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate și pe teren										12
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii și eseuri										43
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activități:										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. Precondiții (acolo unde este cazul)

4.1 de curriculum	Sisteme de operare
4.2 de competențe	Programare C, Programare în limbaj de asamblare x86, Arhitectura calculatoarelor, Arhitectura sistemelor de operare

### 5. Condiții (acolo unde este cazul)

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

### 6. Competențele specifice acumulate

6.1 Competențe profesionale	<p>C4. Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate</p> <ul style="list-style-type: none"> <li>C4.1 – Cunoașterea principiilor și noțiunilor de bază necesare dezvoltării și testării unui cod sigur din punctul de vedere al securității. Cunoașterea claselor uzuale de software și unelte de securitate. Cunoașterea arhitecturilor de SO și platformelor necesare dezvoltării soluțiilor de securitate</li> </ul>
-----------------------------	--

	<ul style="list-style-type: none"> <li>• 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</li> <li>• 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</li> <li>• 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</li> </ul> <p>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 ingineresti și informatice specifice domeniului securității informațiilor și sistemelor de calcul</p> <ul style="list-style-type: none"> <li>• C5.1 – Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate</li> <li>• 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</li> <li>• 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</li> <li>• C5.5 – Realizarea de activități de cercetare cu finalitate practică demonstrată prin prototipuri software și/sau hardware funcționale, cu aplicabilitate în domeniul securității informațiilor și sistemelor de calcul</li> </ul>
6.2 Competențe transversale	N/A

## 7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	Dobândirea de către studenți a unei bune înțelegeri generale a dezvoltării modulelor kernel (driver), în special sub SO Windows. Se urmărește însușirea unei experiențe practice și o familiarizare cu conceptele specifice, utilitarele și metodele de dezvoltare și depanare de bază, precum și înțelegerea diferențelor dintre dezvoltarea aplicațiilor și dezvoltarea modulelor kernel. Un accent particular se pune pe înțelegerea arhitecturii kernelului Windows și de funcționare a modulelor kernel din punct de vedere a implicațiilor de securitate.
7.2 Obiectivele specifice	Se urmărește înțelegerea și dobândirea abilității de manipulare și dezvoltare a: <ol style="list-style-type: none"> <li>1. arhitecturii generale a kernelului Windows,</li> <li>2. diferitelor tipuri de module kernel,</li> <li>3. metodelor de dezvoltare și depanare a modulelor kernel,</li> <li>4. interacțiunii dintre modulele kernel și aplicații,</li> <li>5. implicațiilor dpdv al securității a modulelor kernel,</li> <li>6. posibilităților de a îmbunătăți securitatea unui sistem de calcul folosind module kernel.</li> </ol>

## 8. Conținuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Arhitectura Windows Kernel; Utilitare pentru dezvoltarea și depanarea modulelor kernel pentru Windows	1	Expunere la tablă, prezentare cu video-proiectorul, discuții	
Depanarea modulelor kernel; Concepte fundamentale specifice	2		

dezvoltării modulelor kernel Windows, partea 1 și 2			
Operații I/O sub Windows (I/O Manager, IRP processing); Managementul memoriei (Memory Manager), partea 1 și 2	2		
Topic-uri specifice driverelor pentru filtrarea operațiilor kernel (Operații registry, file-system, procese etc.), partea 1 și 2	2		
Întreruperi și excepții (Interrupts, APCs, DPCs)	1		
Modelele de drivere tip KMDF / UMDF	1		
Programarea driverelor USB	1		
Dezvoltarea driverelor de filtrare rețea. Platforma WFP	1		
Securitatea modulelor Kernel în Windows	1		
Analiza structurilor interne specifice kernel-ului Windows	1		
Recapitulare	1		
Bibliografie ( <i>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</i> )			
1. Windows Kernel Programming (Yosifovich, Pavel – 2019 - CreateSpace Independent Publishing Platform )			
2. Windows Internals (Russovich, Mark – 2012 – Microsoft Press) (6th ed)			
3. Windows NT File System Internals (Nagar, Rajeev – 2006 – OSR Reprint)			
4. Windows Driver Kit (WDK) (Microsoft – 2010-2014 – electronic)			
5. Windows Operating System Internals Curriculum Resource Kit (CRK) (Microsoft – 2006 – electronic)			
6. Windows Research Kernel 1.2 (Microsoft – 2006 – electronic)			
8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Familiarizarea cu utilitarele de dezvoltare și depanare	3		
Dezvoltarea unui driver NT Legacy, a unui DLL user-mode și a unei aplicații de control tip command-line – partea 1 și 2	6		
Dezvoltarea unui driver tip anti-virus – studierea exemplarelor de drivere minifilter din WDK. Dezvoltarea modulului inițial și a utilitarului de control și test tip command-line	3		
Dezvoltarea unui driver tip anti-virus – filtrări de operații file system	3		
Dezvoltarea unui driver tip anti-virus – filtrări de operații registry	3		
Dezvoltarea unui driver tip anti-virus – interceptarea și filtrarea unor alte operații (e.g. notificări de pornire procese, operații cu handel-uri de procese)	3	Expuneri la tablă, discuții, explicații suplimentare, coordonarea realizării exercițiilor de laborator	
Dezvoltarea pe parcursul a mai multor laboratoare a unor drivere Windows diverse, din mai multe teme posibile: <ul style="list-style-type: none"> <li>• drivere de filtrare USB,</li> <li>• drivere de filtrare, emulare sau criptare storage,</li> <li>• drivere anti-rootkit (identificarea proceselor și a fișierelor ascunse, invizibile din Windows Explorer / Task Manager),</li> <li>• drivere de filtrare rețea (WFP).</li> </ul>	15		
Prezentarea și evaluarea soluțiilor temelor de laborator și a activităților de laborator	6		
Bibliografie ( <i>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</i> )			
1. Windows Internals (Russovich, Mark – 2012 – Microsoft Press) (6th ed)			
2. Windows NT File System Internals (Nagar, Rajeev – 2006 – OSR Reprint)			
3. Windows Driver Kit (WDK) (Microsoft – 2010-2014 – electronic)			
4. Windows Operating System Internals Curriculum Resource Kit (CRK) (Microsoft – 2006 – electronic)			
5. Windows Research Kernel 1.2 (Microsoft – 2006 – electronic)			

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

### 9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și 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.

Cunoașterea bună a arhitecturii Windows Kernel este esențială pentru înțelegerea corespunzătoare a multor tehnici de atac și vulnerabilități relevante în ultimii ani. Cunoașterea dezvoltării driverelor este esențială pentru a putea înțelege arhitectura, funcționarea și limitările multor soluții de securitate pe larg folosite astăzi (cum ar fi soluții de

securitate tip anti-virus sau firewall).

Cursuri de driver development sunt prezente în relativ puține alte universități, exemple fiind:

- ECE 446 – Device Driver Development, George Mason University, Fairfax, USA  
[http://catalog.gmu.edu/preview\\_course\\_nopop.php?catoid=19&coid=226124](http://catalog.gmu.edu/preview_course_nopop.php?catoid=19&coid=226124)
- COP 5641 – Linux Kernel & Device Driver Programming, Florida State University, USA  
<http://www.cs.uni.edu/~diesburg/courses/dd/syllabus.html>

O parte din detaliile cursului sunt prezentate în alte facultăți în cadrul cursurilor de Sisteme de Operare.

## 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 și/sau prezentarea unei teme de cercetare din domeniul cursului	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	50%
Proiect			

Standard minim de performanță:

**Curs.** Prezența la **minim 50%** din orele de curs, pentru admiterea la examenul final. Demonstrarea (e.g. în cadrul examenului, în cadrul interacțiunii de laborator) înțelegerii noțiunilor de bază specifice arhitecturii Windows kernel, a modulelor / driverelor kernel, și a dezvoltării driverelor kernel sub Windows.

**Aplicații.** Prezența la laborator **obligatorie 100%** (2 laboratoare se pot recupera în timpul semestrului, iar alte 2 în sesiunile de restanțe) pentru admiterea la examenul final. Dezvoltarea unui driver Windows de tip anti-virus și înțelegerea funcționării lui.

Responsabil curs  
Drd. Ing. Radu Marian Portase

Director departament  
Prof.dr.ing. Rodica Potolea

## FIȘA DISCIPLINEI

### 1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare și Tehnologia Informației
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Securitatea Informațiilor și Sistemelor de calcul/ Master
1.7 Forma de învățământ	IF – învățământ cu frecvență
1.8 Codul disciplinei	7.

### 2. Date despre disciplină

2.1 Denumirea disciplinei	<b>Auditul sistemelor informatice și managementul riscurilor de securitate</b>				
2.2 Titularii de curs	Drd.ing. Dan LUȚAȘ ( <a href="mailto:dlutas@bitdefender.com">dlutas@bitdefender.com</a> )				
2.3 Titularul/Titularii activităților de seminar/laborator/proiect	Drd.ing. Dan LUȚAȘ ( <a href="mailto:dlutas@bitdefender.com">dlutas@bitdefender.com</a> )				
2.4 Anul de studiu	I	2.5 Semestrul	2	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	1	Laborator		Proiect	
3.2 Număr de ore pe semestru	42	din care:	Curs	28	Seminar	14	Laborator		Proiect	
3.3 Distribuția fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie și notițe										48
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate și pe teren										18
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii și eseuri										15
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activități:										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. Precondiții (acolo unde este cazul)

4.1 de curriculum	Securitatea informațiilor
4.2 de competențe	Arhitecturi de calculatoare, Sisteme de operare

### 5. Condiții (acolo unde este cazul)

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

### 6. Competențele specifice acumulate

6.1 Competențe profesionale	<p>C1. Identificarea și înțelegerea problemelor de securitate ce pot apărea în diverse domenii de utilizare a sistemelor de calcul. Aplicarea adecvată a elementelor de bază ale managementului securității și ale modalităților de evaluare și management al riscurilor de securitate informatică</p> <ul style="list-style-type: none"> <li>• C1.1 – Cunoașterea noțiunilor, conceptelor și principiilor teoretice și practice avansate aferente domeniului general al securității informațiilor și sistemelor de calcul. Cunoașterea conceptelor aferente riscurilor, evaluării riscurilor și managementului securității</li> <li>• C1.2 – Înțelegerea riscurilor de securitate specifice unor situații noi și legătura lor cu cele cunoscute anterior. Prevederea scenariilor posibile de</li> </ul>
-----------------------------	--

	<p>securitate, în momentul în care soluțiile de securitate cunoscute sunt folosite într-o situație sau domeniu nou</p> <ul style="list-style-type: none"> <li>• C1.3 – Modelarea unor noi tipuri de riscuri de securitate, evidențierea impactului asupra utilizatorului, asupra sistemelor și aplicațiilor existente. Identificarea unor soluții posibile și evaluarea lor</li> <li>• C1.4 – Stabilirea limitelor maxime de securitate oferite de soluții nou propuse. Plasarea corectă a riscurilor de securitate și a posibilelor soluții într-un cadru de repere bine cunoscute anterior</li> <li>• C1.5 – Elaborarea de modele teoretice noi de analiză a proprietăților de securitate sau evaluarea securității oferite de diverse soluții</li> </ul> <p>C3. Analiza și evaluarea proprietăților de securitate a unui sistem de calcul. Identificarea erorilor de configurare și a vulnerabilităților software</p> <ul style="list-style-type: none"> <li>• C3.1 – Cunoașterea teoretică și practică a diverselor scenarii de configurare sau mentenanță greșită a sistemelor de calcul, precum și a claselor de vulnerabilități software și atacuri informatice tipice</li> <li>• C3.2 – Analiza și înțelegerea unor protocoale de comunicare și module software noi, pentru identificarea unor vulnerabilități posibile. Utilizarea listelor dedicate, recunoscute în domeniu, de clase și tipuri de vulnerabilități și configurări greșite pentru analiza și validarea unui sistem informatic nou din punct de vedere al securității</li> <li>• C3.3 – Capacitatea de a analiza critic, din punctul de vedere al testării vulnerabilității, configurarea unei rețele, sistem de calcul sau aplicații software, fără să existe informații anterioare. Capacitatea de a identifica informații vizibile, servicii expuse etc.</li> <li>• C3.4 – Evaluarea limitărilor teoretice și practice oferite de diverse metode și tehnologii de detectare a vulnerabilităților și configurărilor greșite ale sistemelor de calcul. Determinarea unor corelări constructive între diverse metode de detecție</li> </ul>
6.2 Competențe transversale	N/A

## 7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	Familiarizarea studenților cu noțiunile și elementele de bază ale activităților de audit și management de securitate a sistemelor informaționale și conferirea capacității de a înțelege procesul de audit al sistemelor informaționale, conform standardelor internaționale (ISACA)
7.2 Obiectivele specifice	<ol style="list-style-type: none"> <li>1. Înțelegerea procesului de auditare a sistemelor informaționale, cu referire la standardele internaționale (ISACA)</li> <li>2. Înțelegerea procesului de guvernare și management IT, împreună cu activitatea de audit al guvernării și managementului IT</li> <li>3. Înțelegerea proceselor de achiziție, dezvoltare și implementare a sistemelor informaționale, împreună cu activitatea de audit al acestor procese</li> <li>4. Înțelegerea proceselor de operare, întreținere și suport a sistemelor informaționale, asigurarea continuității afacerii și planurilor de recuperare în caz de dezastru, împreună cu activitatea de audit al acestor procese</li> <li>5. Înțelegerea procesului de asigurare a protecției sistemelor informaționale (managementul securității sistemelor informaționale, controlul accesului, securitatea infrastructurii de rețea, securitatea fizică), împreună cu activitatea de audit aferentă</li> </ol>

## 8. Conținuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Introducere în managementul securității și auditul sistemelor Informatic	2	Expunere la tablă, prezentare cu video-proiectorul, discuții	
Guvernarea IT (roluri și responsabilități, strategii de securitate, politici, standarde și proceduri, metrice de guvernare)	2		
Auditul guvernării IT	2		
Managementul riscului (evaluarea riscului - evaluarea	2		

vulnerabilităților, evaluarea amenințărilor, analiză, monitorizare) și auditul managementului riscului			
Planificarea continuității afacerii și recuperarea după dezastru (audit și administrare - analiza Impactului, RPO/RTI, copii de siguranță)	2		
Tratarea incidentelor (proceduri de răspuns la incidente, dezvoltarea unui plan de răspuns la incidente, testarea răspunsului la incidente/BCP/DRP)	2		
Managementul proiectelor software: ciclul de viață a dezvoltării software, fazele de certificare și acreditare, sisteme de aplicații business (comerț electronic, schimbul electronic de date, aplicații bancare, transfer electronic de fonduri)	2		
Auditul managementului de proiect	2		
Operațiuni de securitate informațională (administrarea patch-urilor, administrarea configurațiilor) și întreținere, audit (sisteme de operare, infrastructură de rețea)	2		
Administrarea securității informaționale (framework-uri, audit), acces logic (controlul accesului software, identificare, autorizare), acces fizic și audit	2		
Securitatea infrastructurii de rețea (LAN, WAN, Wireless, Firewall, IDS, IPS, VoIP, PBX, testarea vulnerabilităților de rețea)	2		
Auditul infrastructurii de rețea (a componentelor prezentate în cursul 11)	2		
Managementul securității informației (governare, managementul riscului, dezvoltarea și gestionarea unui program de securitate a informației)	2		
Prezentare de sinteză a subiectelor studiate, evidențierea concluziilor esențiale, discuții și prezentări pe subiecte propuse de studenți	2		
<p>Bibliografie (<i>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</i>)</p> <ol style="list-style-type: none"> <li>1. CISA Certified Information Systems Auditor Study Guide (Cannon, David – 2011 – Sybex) (3rd ed)</li> <li>2. IT Auditing Using Controls to Protect Information Assets (Davis, Chris – 2011 – McGraw-Hill) (2nd ed)</li> <li>3. CISM Review Manual 2013 (ISACA – 2012 – ISACA) (11th edition)</li> <li>4. The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments (Landoll, Douglas – 2011 – CRC Press) (2nd ed)</li> <li>5. Diferite articole</li> </ol>			
8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Importanța securității & auditului sistemelor informatice	1	Expuneri la tablă, explicații suplimentare, discuții	
Management-ul riscului. Recuperarea după dezastru: tehnici și principii	1		
Importanța patch-urilor de securitate. Securitate de rețea	1		
Analiza unor rapoarte tehnice și articole recente: vulnerabilități în sistemele de operare	1		
Analiza unor rapoarte tehnice și articole recente: vulnerabilități în infrastructura de rețea	1		
Analiza unor rapoarte tehnice și articole recente: vulnerabilități în aplicații	1		
Analiza unor rapoarte tehnice și articole recente: atacuri avansate	1		
<p>Bibliografie (<i>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</i>)</p> <ol style="list-style-type: none"> <li>1. CISA Certified Information Systems Auditor Study Guide (Cannon, David – 2011 – Sybex) (3rd ed)</li> <li>2. IT Auditing Using Controls to Protect Information Assets (Davis, Chris – 2011 – McGraw-Hill) (2nd ed)</li> <li>3. CISM Review Manual 2013 (ISACA – 2012 – ISACA) (11th edition)</li> <li>4. The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments (Landoll,</li> </ol>			

Douglas – 2011 – CRC Press) (2nd ed)

5. Diferite articole

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

**9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și 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 audit și security risk management sunt prezente în cadrul multor alte masterate din domeniul securității calculatoarelor și a informațiilor, cum ar fi:

- IT&C Audit – IT&C Security Master Program - THE BUCHAREST ACADEMY OF ECONOMIC STUDIES, [http://ism.ase.ro/files/Curriculum/Y2012-2014/analytical-programs/en/S4/ISM\\_PA\\_EN\\_024.pdf](http://ism.ase.ro/files/Curriculum/Y2012-2014/analytical-programs/en/S4/ISM_PA_EN_024.pdf)
- Information Technology Auditing - Master of Science in Information Systems Audit and Control – Georgia State University, <http://cis.robinson.gsu.edu/academic-programs/ms-is-audit/curriculum/>
- Audit & Security - Information Security and Audit, MSc – University of Greenwich <http://www2.gre.ac.uk/study/courses/pg/inftec/isa/cms-courses?banner=COMP1431&year=1415>

**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 de tip grilă	60%
Seminar	Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de seminar	Prezentarea unei teme de cercetare din domeniul cursului și/sau rezolvarea și prezentarea soluției unor probleme similare cu cele discutate în timpul orelor de seminar	40%
Laborator			
Proiect			

Standard minim de performanță:

**Curs.** Prezența la **minim 50%** din orele de curs, pentru admiterea la examenul final.

**Aplicații.** Prezența la seminar **obligatorie 100%** (un seminar se poate recupera în timpul semestrului, iar altul în sesiunile de restanțe) pentru admiterea la examenul final.

Capacitatea de a defini și explica în context noțiunile de bază a activităților de audit al sistemelor informaționale și management al securității sistemelor informaționale, cum ar fi: procesul de audit, procesul de guvernare și management IT, procesele de achiziție, dezvoltare, implementare, operare, întreținere, suport și asigurare a protecției sistemelor informaționale, împreună cu mecanismele de audit specifice fiecărui proces.

Responsabil curs  
Drd. Ing. Dan Luțaș

Director departament  
Prof.dr.ing. Rodica Potolea



## FIȘA DISCIPLINEI

### 1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare și Tehnologia Informației
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Securitatea Informațiilor și Sistemelor de calcul/ Master
1.7 Forma de învățământ	IF – învățământ cu frecvență
1.8 Codul disciplinei	8.

### 2. Date despre disciplină

2.1 Denumirea disciplinei	<b>Securitate Web</b>				
2.2 Titularii de curs	Conf.dr.ing. Teodor ȘTEFĂNUȚ ( <a href="mailto:teodor.stefanut@cs.utcluj.ro">teodor.stefanut@cs.utcluj.ro</a> )				
2.3 Titularul/Titularii activităților de seminar/laborator/proiect	Drd.ing. Vlad Ioan TOPAN ( <a href="mailto:itopan@bitdefender.com">itopan@bitdefender.com</a> )				
2.4 Anul de studiu	I	2.5 Semestrul	2	2.6 Tipul de evaluare ( E – examen, C – colocviu, V – verificare)	E
2.7 Regimul disciplinei	DA – de aprofundare, DS – de sinteza, DC – complementară				DA
	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 Distribuția fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie și notițe										16
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate și pe teren										16
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii și eseuri										49
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activități:										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. Precondiții (acolo unde este cazul)

4.1 de curriculum	Probleme de securitate la nivel de cod sursă
4.2 de competențe	Programare web, Baze de date, Rețele de calculatoare

### 5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2. de desfășurare a seminarului / laboratorului / proiectului	Prezență la laborator obligatorie 100% pentru admiterea la examenul final

### 6. Competențele specifice acumulate

6.1 Competențe profesionale	<p>C1 - Identificarea și înțelegerea problemelor de securitate ce pot apărea în diverse domenii de utilizare a sistemelor de calcul. Aplicarea adecvată a elementelor de bază ale managementului securității și ale modalităților de evaluare și management al riscurilor de securitate informatică</p> <ul style="list-style-type: none"> <li>• C1.1 – Cunoașterea noțiunilor, conceptelor și principiilor teoretice și practice avansate aferente domeniului general al securității informațiilor și sistemelor de calcul. Cunoașterea conceptelor aferente riscurilor, evaluării riscurilor și managementului securității</li> <li>• C1.2 – Înțelegerea riscurilor de securitate specifice unor situații noi și legătura lor cu cele cunoscute anterior. Prevederea scenariilor posibile de</li> </ul>
-----------------------------	---

	<p>securitate, în momentul în care soluțiile de securitate cunoscute sunt folosite într-o situație sau domeniu nou</p> <ul style="list-style-type: none"> <li>• C1.3 – Modelarea unor noi tipuri de riscuri de securitate, evidențierea impactului asupra utilizatorului, asupra sistemelor și aplicațiilor existente. Identificarea unor soluții posibile și evaluarea lor</li> <li>• C1.4 – Stabilirea limitelor maxime de securitate oferite de soluții nou propuse. Plasarea corectă a riscurilor de securitate și a posibilelor soluții într-un cadru de repere bine cunoscute anterior</li> <li>• C1.5 – Elaborarea de modele teoretice noi de analiză a proprietăților de securitate sau evaluarea securității oferite de diverse soluții</li> </ul> <p>C3 - Analiza și evaluarea proprietăților de securitate a unui sistem de calcul. Identificarea erorilor de configurare și a vulnerabilităților software</p> <ul style="list-style-type: none"> <li>• C3.1 – Cunoașterea teoretică și practică a diverselor scenarii de configurare sau mentenanță greșită a sistemelor de calcul, precum și a claselor de vulnerabilități software și atacuri informatice tipice</li> <li>• C3.2 – Analiza și înțelegerea unor protocoale de comunicare și module software noi, pentru identificarea unor vulnerabilități posibile. Utilizarea listelor dedicate, recunoscute în domeniu, de clase și tipuri de vulnerabilități și configurări greșite pentru analiza și validarea unui sistem informatic nou din punct de vedere al securității</li> <li>• C3.3 – Capacitatea de a analiza critic, din punctul de vedere al testării vulnerabilității, configurarea unei rețele, sistem de calcul sau aplicații software, fără să existe informații anterioare. Capacitatea de a identifica informații vizibile, servicii expuse etc.</li> <li>• C3.4 – Evaluarea limitărilor teoretice și practice oferite de diverse metode și tehnologii de detectare a vulnerabilităților și configurărilor greșite ale sistemelor de calcul. Determinarea unor corelări constructive între diverse metode de detecție</li> <li>• C3.5 – Propunerea unor noi metode de clasificare, identificare sau analiză pentru vulnerabilitățile și configurările greșite de sisteme. Crearea unor soluții și utilitare software care să identifice și analizeze astfel de cazuri</li> </ul> <p>C4 - Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate</p> <ul style="list-style-type: none"> <li>• C4.1 – Cunoașterea principiilor și noțiunilor de bază necesare dezvoltării și testării unui cod sigur din punctul de vedere al securității. Cunoașterea claselor uzuale de software și unelte de securitate. Cunoașterea arhitecturilor de SO și platformelor necesare dezvoltării soluțiilor de securitate</li> <li>• 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</li> <li>• C4.4 – Evaluarea unor proiecte software existente și identificarea greșelilor de securitate din punctul de vedere al arhitecturii, modului de programare sau procedurilor de testare. Propunerea unor noi metode de dezvoltare și testare</li> </ul>
6.2 Competențe transversale	N/A

## 7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	Înțelegerea vulnerabilităților comune prezente în aplicațiile Web, a modului în care acestea pot fi exploatare cu intenții malițioase și a tehnicilor de dezvoltare, instalare și configurare a aplicațiilor Web securizate
7.2 Obiectivele specifice	<ol style="list-style-type: none"> <li>1. Înțelegerea modului de funcționare a aplicațiilor Web</li> <li>2. Dezvoltarea abilității de a identifica vulnerabilități în implementarea aplicațiilor Web</li> <li>3. Înțelegerea tehnicilor de exploatare a vulnerabilităților aplicațiilor Web (XSS, SQL injection etc.)</li> <li>4. Dezvoltarea aptitudinilor de scriere de cod securizat pentru aplicațiile Web</li> </ol>

5. Dezvoltarea aptitudinilor de configurarea corectă a aplicațiilor Web, din perspectiva securității

## 8. Conținuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Privire de ansamblu asupra tehnologiilor Web (1): concepte generale (clienți/serve, web 2.0, DOM etc.), arhitectura aplicațiilor web (frontend/middleware/backed)	2	Expunere la tablă, prezentare cu video-proiectorul, discuții	
Privire de ansamblu asupra tehnologiilor Web (2): protocoale (stiva ISO-OSI, HTTP, FTP, TCP, SOAP etc.) și limbaje (HTML, CSS, SVG, JS, XML, JSON, PHP, Python, Ruby etc.)	2		
Securitatea Web (1): autentificare (identitate), autorizare, criptare și legislație în domeniu	2		
Securitatea Web (2): confidențialitate, integritate și disponibilitate, nivelul rețea (firewalls, IPS)	2		
Securitatea serverelor (1): vulnerabilități și atacuri (OWASP, atacuri prin injecții SQL/hijack de sesiune/SSL/referințe directe de obiecte/etc.)	2		
Securitatea serverelor (2): asigurarea disponibilității (atacul (D)DoS) și configurarea corectă	2		
Securitatea clienților (browser-e Web) (1): vulnerabilități (browser, pluginuri Flash/Java/etc., cookies, DNS, clickjacking)	2		
Securitatea clienților (browser-e Web) (2): configurare, sandboxing, scripturi utilizator, malware/spyware	2		
Criptografie pentru Web: concepte generale, chei publice/private, certificate, integritatea mesajelor, protocoale (SSL, HTTPS etc.)	2		
Măsurile proactive de securitate: detectarea intruziunilor în aplicații web, gestionarea de incidente, honeypots	2		
Securitatea pentru Web 2.0: paradigma AJAX, cloud computing etc.	2		
Programare sigură pentru Web (1): validarea intrărilor/sanitizarea erorilor, identitatea, controlul accesului, gestionarea sesiunilor	2		
Programare sigură pentru Web (2): gestionarea datelor cu sensibilitate mare, practici corecte de programare	2		
Prezentare de sinteză a subiectelor studiate, evidențierea concluziilor importante, discutarea unor subiecte propuse de studenți	2		
<p>Bibliografie (<i>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</i>)</p> <ol style="list-style-type: none"> <li>24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)</li> <li>Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)</li> <li>Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)</li> <li>The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)</li> <li>The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Syngress)</li> <li>Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)</li> <li>Diferite articole și site-uri Web</li> </ol>			
8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Dezvoltarea unei aplicații minimale Web (frontend/middleware/backend)	1	Expunere la tablă, explicații suplimentare, discuții, exerciții de laborator	
Analiza de pachete de rețea în protocoale Web, implementarea / configurarea unui firewall	1		
Analiza atacurilor Web: OWASP, vulnerabilități de sesiune, injecții SQL	1		
Analiza atacurilor Web: XSS, CSRF, referințe directe nesecurizate, SSL	1		
Analiza și exploatarea de vulnerabilități în browser-ele Web:	1		

JavaScript, traversare de path-uri si în plugin-uri de browser-e Web (Flash, Java etc.)			
Programare sigură: validarea intrărilor, evitarea expunerii publice a detaliilor cazurilor de eroare, tratarea datelor sensibile, practici corecte etc.	1		
Utilizarea instrumentelor de validare a site-urilor Web: scannere de vulnerabilități cunoscute si fuzzere	1		
Bibliografie ( <i>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</i> ) <ol style="list-style-type: none"> <li>24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)</li> <li>Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)</li> <li>Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)</li> <li>The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)</li> <li>The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)</li> <li>Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)</li> <li>Diferite articole și site-uri Web</li> </ol>			

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

### 9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și 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 securitate web sunt prezente în cadrul multor alte masterate din domeniul securității calculatoarelor și a informațiilor, cum ar fi:

- XACS241 - Web Security 2.0 (Stanford) – <http://scpd.stanford.edu/search/publicCourseSearchDetails.do?method=load&courseId=1284858>
- 06-20009 Network Security (University of Birmingham) – <http://www.cs.bham.ac.uk/internal/modules/2010/20009/>
- Internet and Security (Nottingham University) – <http://targetpostgrad.com/course/31312-internet-and-security>
- Master of Science in Cybersecurity (University of Maryland) – <http://www.umuc.edu/academic-programs/masters-degrees/cybersecurity.cfm>
- Applied Cyber Security (MIT) – [http://web.mit.edu/professional/short-programs/courses/applied\\_cyber\\_security.html](http://web.mit.edu/professional/short-programs/courses/applied_cyber_security.html)

### 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 și/sau prezentarea unei teme de cercetare din domeniul cursului	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	50%
Proiect			

Standard minim de performanță:

Capacitatea de a defini și explica conceptele elementare de securitate a aplicațiilor Web (SQL injection, XSS, CSRF, configurare) și a riscurilor la care sunt expuse datele și aplicațiile publicate pe Web.

Capacitatea de a identifica vulnerabilități de bază (SQL injection, XSS, CSRF, de configurare) în codul sursă al aplicațiilor web. Capacitatea de a scrie cod securizat pentru aplicații Web de complexitate mică.

Responsabil curs  
Conf.dr.ing. Teodor Ștefănuț

Director departament  
Prof.dr.ing. Rodica Potolea

## FIȘA DISCIPLINEI

### 1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare și Tehnologia Informației
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Securitatea Informațiilor și Sistemelor de calcul/ Master
1.7 Forma de învățământ	IF – învățământ cu frecvență
1.8 Codul disciplinei	9.1

### 2. Date despre disciplină

2.1 Denumirea disciplinei	<b>Sisteme de date masive și securitatea calculatoarelor</b>				
2.2 Titularii de curs	Conf.dr.ing. Camelia LEMNARU ( <a href="mailto:camelia.lemnaru@cs.utcluj.ro">camelia.lemnaru@cs.utcluj.ro</a> )				
2.3 Titularul/Titularii activităților de seminar/laborator/proiect	S.I.Dr.ing. Ciprian OPRIȘA ( <a href="mailto:coprisa@bitdefender.com">coprisa@bitdefender.com</a> )				
2.4 Anul de studiu	I	2.5 Semestrul	2	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	2	Seminar		Laborator	2	Proiect	
3.2 Număr de ore pe semestru	56	din care:	Curs	28	Seminar		Laborator	28	Proiect	
3.3 Distribuția fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie și notițe										32
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate și pe teren										18
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii și eseuri										43
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activități:										0
3.4 Total ore studiu individual (suma (3.3(a)...3.3(f)))							94			
3.5 Total ore pe semestru (3.2+3.4)							150			
3.6 Numărul de credite							6			

### 4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Baze de date
4.2 de competențe	Statistică și probabilități

### 5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2. de desfășurare a seminarului / laboratorului / proiectului	Prezență la laborator obligatorie 100% pentru admiterea la examenul final

### 6. Competențele specifice acumulate

6.1 Competențe profesionale	<p>C2. Investigarea și analiza situațiilor de criminalitate informatică și a software-ului malițios prin metode avansate de tip inginerie inversă și monitorizare comportament</p> <ul style="list-style-type: none"> <li>• C2.1 – Cunoașterea aprofundată a clasificării, caracteristicilor și particularităților aferente diferitelor tipuri de atacuri informatice și softurilor malițioase</li> <li>• C2.3 – Capacitatea de a face corelări și de a putea identifica obiecte potențial malițioase chiar dacă nu se poate analiza complet obiectul respectiv</li> </ul>
-----------------------------	--

	<ul style="list-style-type: none"> <li>• 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</li> <li>• C2.5 – Elaborarea unor noi clase de atacuri sau software malițios, și propunerea unor noi proprietăți potrivite clasificării codurilor malițioase</li> </ul> <p>C4. Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• 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</li> <li>• 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</li> </ul> <p>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 ingineresti și informatice specifice domeniului securității informațiilor și sistemelor de calcul</p> <ul style="list-style-type: none"> <li>• C5.1 – Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate</li> <li>• 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</li> <li>• C5.3 – Aplicarea unor modele matematice și informatice teoretice sau cu o arie mai generală de aplicabilitate pentru a analiza, evalua și rezolva probleme diverse de securitate/confidențialitate din lumea reală</li> <li>• C5.5 – Realizarea de activități de cercetare cu finalitate practică demonstrată prin prototipuri software și/sau hardware funcționale, cu aplicabilitate în domeniul securității informațiilor și sistemelor de calcul</li> </ul>
6.2 Competențe transversale	N/A

## 7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	Dobândirea deprinderii de a lucra cu colecții masive de date. Ținând cont că numărul de programe malițioase este în continuă creștere, se dorește ca studenții să fie capabili să le gestioneze, clasifice și să găsească noi modele pentru detecția acestora.
7.2 Obiectivele specifice	<ul style="list-style-type: none"> <li>• Dobândirea abilității de a utiliza limbaje de scripting și baze de date pentru a manipula colecții masive de date</li> <li>• Înțelegerea paradigmei Map-Reduce și abilitatea de a proiecta și implementa sisteme distribuite</li> <li>• Cunoașterea unor algoritmi și tehnici pentru căutarea datelor în colecții masive</li> <li>• Deprinderea unor modele pentru clasificarea și învățarea automată a regulilor de detecție a programelor malițioase</li> </ul>

## 8. Conținuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Introducere în limbaje de scripting: limbajul Python	2	Expunere la tablă,	
Procesarea datelor în Python	2	prezentare cu video-	

Baze de date relaționale și nerelaționale: proprietățile ACID, algebra relațională, teorema CAP	2	proiectorul, discuții	
Paradigma Map-Reduce	2		
Analiza complexității algoritmilor Map-Reduce	2		
Tehnici simple de căutare în colecții masive: indexare, hashing	2		
Tehnici avansate de căutare în colecții masive: căutarea elementelor similare, identificarea similarităților între programe	2		
Tehnici avansate de căutare în colecții masive: reversed index, locality-sensitive hashing	2		
Analiza link-urilor: algoritmul PageRank, tehnici de SEO	2		
Tehnici de clustering: K-means, clustering ierarhic	2		
Tehnici avansate de clustering pentru colecții masive	2		
Construcția de modele pentru predicții: regresie liniară, regresie logistică, arbori de decizie	2		
Clasificatori avansați: perceptronul, Support Vector Machines	2		
Reducerea dimensionalității	2		
Bibliografie ( <i>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</i> )			
1. Mining of Massive Datasets (Rajarman, Anand – 2011 – Cambridge)			
2. Pattern Recognition and Machine Learning (Bishop, Christopher – 2007 – Springer)			
3. MongoDB: The Definitive Guide (Chodorow, Kristina – 2013 – O'Reilly) (2nd ed)			
4. Data Science for Business: What you need to know about data mining and data-analytic thinking (Provost, Foster – 2013 – O'Reilly)			
5. Learning Python (Lutz, Mark – 2013 – O'Reilly) (5th ed)			
6. Diferite articole			
8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Introducere în limbajul Python	2	Scurte expuneri la tablă, tutoriale, ghiduri de lucru, demonstrații <i>live</i> , explicații suplimentare, discuții, propunerea spre rezolvare a unor probleme de diferite tipuri și grade de complexitate	
Structuri de date în Python	2		
Biblioteci de funcții specifice pentru operarea cu colecții de date	2		
Extragerea de trăsături pentru identificarea programelor potențial malițioase	2		
Stocarea și accesarea colecțiilor de date: baze de date, utilizarea indecșilor	2		
Algoritmi de tip Map-Reduce pentru procesarea colecțiilor de fișiere potențial malițioase	2		
Calculul similarității între programe	2		
Construcția unui reversed index, folosind tehnica Map-Reduce	2		
Regăsirea aplicațiilor similare în colecții masive: locality-sensitive hashing	2		
Tehnici de clustering pentru identificarea familiilor de malware, partea 1	2		
Tehnici de clustering pentru identificarea familiilor de malware, partea 2	2		
Clasificatori pentru malware și spam, partea 1	2		
Clasificatori pentru malware și spam, partea 2	2		
Evaluare și verificare	2		
Bibliografie ( <i>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</i> )			
1. Mining of Massive Datasets (Rajarman, Anand – 2011 – Cambridge)			
2. Pattern Recognition and Machine Learning (Bishop, Christopher – 2007 – Springer)			
3. MongoDB: The Definitive Guide (Chodorow, Kristina – 2013 – O'Reilly) (2nd ed)			
4. Data Science for Business: What you need to know about data mining and data-analytic thinking (Provost, Foster – 2013 – O'Reilly)			
5. Learning Python (Lutz, Mark – 2013 – O'Reilly) (5th ed)			
6. Diferite articole			

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

### 9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și 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 cu topic-uri legate de big data sunt prezente în cadrul multor alte masterate, însă puține dintre ele se focalizează și pe domeniul securității calculatoarelor și a informațiilor. Oricum, atât clasificarea software-ului malițios, cât și a spam-urilor reprezintă în practică colecții masive de date, a căror prelucrare necesită metode de învățare automată și prelucrare a datelor masive. Exemple ar fi:

- *Big Data*, Masters in Computer and Information Security, University of Liverpool, UK <http://www.liv.ac.uk/study/online/programmes/information-technology/msc-computer-and-information-security/module-details/>
- *Big Data Management and Security*, Graduate Certificate Program, Missouri University of Science and Technology, USA, <http://dce.mst.edu/credit/certificates/bigdatamanagementandsecurity/>
- CS246, *Mining Massive Data Sets*, Stanford, <http://web.stanford.edu/class/cs246/>  
CSE 599, *Machine Learning for Big Data*, Computer Science & Engineering, University of Washington

Există numeroase alte programe de masterat care se specializează pe big data și business analytics, care predau metode și tehnici care se pot aplica cu succes și în cadrul analizei datelor de securitate.

### 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 și/sau prezentarea unei teme de cercetare din domeniul cursului	50%
Seminar			
Laborator	Abilitatea de rezolvare a unor probleme specifice domeniului	Realizarea activităților de laborator și rezolvarea temelor de casă și/sau a unor probleme în cadrul unui examen practic	50%
Proiect			

Standard minim de performanță:

La finalul cursului, studenții trebuie să fie capabili să manipuleze colecții mari de date, atât nestructurate cât și structurate în baze de date, folosind algoritmi secvențial și distribuiți, de tip Map-Reduce. Principalele operații pe care studenții trebuie să demonstreze că le-au deprins sunt căutarea în colecții masive, clasificarea și clusterizarea elementelor, respectiv construirea de modele predictive.

Responsabil curs  
Conf.dr.ing. Camelia Lemnaru

Director departament  
Prof.dr.ing. Rodica Potolea



## FIȘA DISCIPLINEI

### 1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare și Tehnologia Informației
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Securitatea Informațiilor și Sistemelor de calcul/ Master
1.7 Forma de învățământ	IF – învățământ cu frecvență
1.8 Codul disciplinei	9.2

### 2. Date despre disciplină

2.1 Denumirea disciplinei	<b>Sisteme de securitate bazate pe hardware și virtualizare</b>				
2.2 Titularii de curs	Conf.dr.ing. Adrian COLEȘA ( <a href="mailto:adrian.colesa@cs.utcluj.ro">adrian.colesa@cs.utcluj.ro</a> )				
2.3 Titularul/Titularii activităților de seminar/laborator/proiect	Conf.dr.ing. Adrian COLEȘA ( <a href="mailto:adrian.colesa@cs.utcluj.ro">adrian.colesa@cs.utcluj.ro</a> )				
2.4 Anul de studiu	I	2.5 Semestrul	2	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	2	Seminar		Laborator	2	Proiect	
3.2 Număr de ore pe semestru	56	din care:	Curs	28	Seminar		Laborator	28	Proiect	
3.3 Distribuția fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie și notițe										24
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate și pe teren										12
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii și eseuri										56
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activități:										0
3.4 Total ore studiu individual (suma (3.3(a)...3.3(f)))							94			
3.5 Total ore pe semestru (3.2+3.4)							150			
3.6 Numărul de credite							6			

### 4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Programarea calculatoarelor, Programare în limbaj de asamblare, Sisteme de operare, Arhitectura calculatoarelor, Securitatea informațiilor
4.2 de competențe	Programare în C și limbaj de asamblare x86, cunoașterea funcționalității unui SO, cunoașterea conceptelor fundamentale referitoare la securitatea sistemelor și informației

### 5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Tablă, proiector, calculatoare
5.2. de desfășurare a seminarului / laboratorului / proiectului	Tablă, proiector, calculatoare

### 6. Competențele specifice acumulate

6.1 Competențe profesionale	<p>C2 - Investigarea și analiza situațiilor de criminalitate informatică și a software-ului malițios prin metode avansate de tip inginerie inversă și monitorizare comportament</p> <ul style="list-style-type: none"> <li>• C2.1 – Cunoașterea aprofundată a clasificării, caracteristicilor și particularităților aferente diferitelor tipuri de atacuri informatice și softurilor malițioase</li> <li>• C2.2 – Analiza și înțelegerea a noi clase de software malițios, noi tehnici de</li> </ul>
-----------------------------	--

	<p>atac, persistență, escaladarea privilegiilor etc., precum și compararea lor cu tehnicile cunoscute</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• C2.5 – Elaborarea unor noi clase de atacuri sau software malițios, și propunerea unor noi proprietăți potrivite clasificării codurilor malițioase</li> </ul> <p>C4 - Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate</p> <ul style="list-style-type: none"> <li>• C4.1 – Cunoașterea principiilor și noțiunilor de bază necesare dezvoltării și testării unui cod sigur din punctul de vedere al securității. Cunoașterea claselor uzuale de software și unelte de securitate. Cunoașterea arhitecturilor de SO și platformelor necesare dezvoltării soluțiilor de securitate</li> <li>• 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</li> <li>• 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</li> <li>• 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</li> </ul> <p>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 ingineresti și informatice specifice domeniului securității informațiilor și sistemelor de calcul</p> <ul style="list-style-type: none"> <li>• C5.1 – Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate</li> <li>• 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</li> <li>• 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</li> </ul>
6.2 Competențe transversale	N/A

## 7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	Cunoașterea modalităților prin care diferite tehnologii hardware moderne (de platformă, de procesor etc.), în general, și cele de virtualizare, în particular, pot fi folosite pentru îmbunătățirea securității sistemelor și informației.
7.2 Obiectivele specifice	<ol style="list-style-type: none"> <li>1. Înțelegerea principalelor funcționalități hardware oferite de arhitectura x86 pentru securitatea aplicațiilor și informației</li> <li>2. Înțelegerea principalelor funcționalități hardware oferite de arhitectura x86 pentru virtualizare</li> <li>3. Capacitatea de dezvoltare a unui mini-hipervizor utilizând funcționalitățile hardware de virtualizare ale arhitecturii x86</li> <li>4. Cunoașterea principalelor tehnici de utilizare a virtualizării pentru asigurarea securității aplicațiilor și informației</li> <li>5. Capacitatea de implementare și de evaluare critică (context, avantaje,</li> </ol>

**8. Conținuturi**

8.1 Curs	Nr.ore	Metode de predare	Observații
Conceptele fundamentale ale virtualizării și principalele tehnici de implementare	2	Expunere la tablă, prezentare cu video-proiectorul, discuții	
Funcționalitatea de bază oferită de arhitecturile hardware pentru virtualizare (ex. Intel VT-X)	2		
Funcționalitatea de virtualizare a memoriei oferită de arhitecturile hardware (ex. Intel EPT)	2		
Introspecția memoriei ca tehnică de securitate a sistemelor	2		
Metode de protecție a datelor și aplicațiilor folosind virtualizarea	2		
Metode de detecție a aplicațiilor și codului malițios folosind virtualizarea (lista proceselor ascunse, cod injectat etc.)	2		
Tehnici avansate folosite în introspecției memoriei: introspecția aplicațiilor utilizator, protejarea împotriva tehnicilor de remapare a memoriei virtuale, optimizări, tehnici de generare a codului de introspecție independent de SO din mașina virtuală, tehnici de generare automată a codului de introspecție	2		
Funcționalitatea de virtualizare a spațiului de adrese ale dispozitivelor I/O oferită de arhitecturile hardware (ex. Intel VT-d), și evitarea atacurilor de tip DMA	2		
Problema nivelurilor multiple de virtualizare ( <i>nested virtualization</i> ) și suportul hardware oferit în acest sens	2		
Tehnici de izolare și protecție a integrității aplicațiilor și datelor (ex. virtualizarea, Intel SGX)	2		
Tehnologii hardware pentru protecția sistemelor (1): Intel MPX, Intel Anti-Theft Technology, Intel IPT, etc.	2		
Tehnologii hardware pentru protecția calculatoarelor (2): funcționalitatea TPM-urilor, UEFI Secure Boot, etc.	2		
Funcționalitatea hardware de verificare și asigurare a integrității (ex. Intel TXT) și utilizarea în tehnicile de securitate bazate pe virtualizare	2		
Folosirea virtualizării și a funcționalității hardware de verificare a integrității datelor pentru asigurarea securității și integrității aplicațiilor client ce interacționează cu servicii ce gestionează date confidențiale.	2		
Bibliografie ( <i>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</i> )			
1. Intel, „Intel 64 and IA-32 Architectures Software Developer's Manual”, Volume 1-3, 2014, <a href="http://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-manual-325462.pdf">http://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-manual-325462.pdf</a>			
2. B. Parno, J. McCune, A. Perrig, „Bootstrapping Trust in Modern Computers”, Springer, 2011, <a href="http://research.microsoft.com/pubs/154093/bootstrappingtrustbook.pdf">http://research.microsoft.com/pubs/154093/bootstrappingtrustbook.pdf</a>			
3. Intel, „Intel Trusted Execution Technology (TXT). Software Development Guide”, 2014, <a href="http://www.intel.com/content/www/us/en/software-developers/intel-txt-software-development-guide.html">http://www.intel.com/content/www/us/en/software-developers/intel-txt-software-development-guide.html</a>			
4. D. Weinstein, „Advanced x86: Virtualization with Intel VT-x”, 2012, online: <a href="http://opensecuritytraining.info/AdvancedX86-VTX.html">http://opensecuritytraining.info/AdvancedX86-VTX.html</a>			
5. A. Segall, „Introduction To Trusted Computing”, 2013, online: <a href="http://opensecuritytraining.info/IntroToTrustedComputing.html">http://opensecuritytraining.info/IntroToTrustedComputing.html</a>			
6. Articole indicate pe parcurs. Vezi <a href="http://www.citeulike.org/group/18034">http://www.citeulike.org/group/18034</a> cu etichete precum: <i>virtualization, introspection, light-virtualization, trusted, hvs-course (to be added)</i>			
8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Componente de bază ale unui mini-HV: încărcător, organizarea memoriei, unelte de depanare, suport pentru sisteme multiprocesor.	2	Scurte expuneri la tablă, tutoriale, ghiduri de lucru,	
Pornirea unei MV de testare (1): setarea structurilor VCPU/PCPU și VMCS, trecerea cu toate procesoarele în VMXROOT	2	demonstrații <i>live</i> , explicații	

Pornirea unei MV de testare (2): controlul MV, tratarea unor evenimente VMEXIT de test	2	suplimentare, discuții, propunerea spre rezolvare a unor probleme de diferite tipuri și grade de complexitate	
Pornirea unei MV Windows (1): tratare evenimente VMEXIT pentru pornire cod MBR	2		
Pornirea unei MV Windows (2): tratare evenimente VMEXIT pentru pornire cod MBR	2		
Pornirea unei MV Windows (3): injectare harta E820 modificată, redirectare INT 0x15	2		
Pornirea unei MV Windows (4): tratarea tuturor evenimentelor VMEXIT generate de pornirea SO din MV	2		
Izolarea și protecția memoriei folosind EPT (1): izolarea și protecția hipervizorului	2		
Izolarea și protecția memoriei folosind EPT (2): metode de protecție	2		
Introspecția (1): detecția proceselor ascunse folosind structuri de date din Windows	2		
Introspecția (2): protejarea diferitelor structuri de date din SO (spațiul kernel) și din aplicațiile utilizator (spațiul utilizator) in Windows	2		
Introspecția (3): tehnici de detecție/protecție independente de SO	2		
Protecția datelor cu Intel SGX, MPX	2		
Prezentări, demonstrații, discuții, evaluare	2		
Bibliografie ( <i>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</i> )			
1. Intel, „Intel 64 and IA-32 Architectures Software Developer's Manual”, Volume 1-3, 2014, <a href="http://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-manual-325462.pdf">http://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-manual-325462.pdf</a>			
2. B. Parno, J. McCune, A. Perrig, „Bootstrapping Trust in Modern Computers”, Springer, 2011, <a href="http://research.microsoft.com/pubs/154093/bootstrappingtrustbook.pdf">http://research.microsoft.com/pubs/154093/bootstrappingtrustbook.pdf</a>			
3. Intel, „Intel Trusted Execution Technology (TXT). Software Development Guide”, 2014, <a href="http://www.intel.com/content/www/us/en/software-developers/intel-txt-software-development-guide.html">http://www.intel.com/content/www/us/en/software-developers/intel-txt-software-development-guide.html</a>			
4. D. Weinstein, „Advanced x86: Virtualization with Intel VT-x”, 2012, online: <a href="http://opensecuritytraining.info/AdvancedX86-VTX.html">http://opensecuritytraining.info/AdvancedX86-VTX.html</a>			
5. A. Segall, „Introduction To Trusted Computing”, 2013, online: <a href="http://opensecuritytraining.info/IntroToTrustedComputing.html">http://opensecuritytraining.info/IntroToTrustedComputing.html</a>			
6. Articole indicate pe parcurs. Vezi <a href="http://www.citeulike.org/group/18034">http://www.citeulike.org/group/18034</a> cu etichete precum: <i>virtualization, introspection, light-virtualization, trusted, hvs-course (to be added)</i>			

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

### 9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și 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.

Acest curs este unul de specializare și de aprofundare a cunoștințelor, într-un domeniu care deocamdată, din câte știm noi, nu este prezent în curricula altor programe de master de securitatea informațiilor. Considerăm, însă, că înțelegerea practică a detaliilor legate de virtualizarea hardware, precum și dobândirea unei înțelegeri generale a diferitelor tehnologii hardware de creștere a securității prezente pe sistemele moderne este esențială. Peste 80% din noile servere x86 sunt servere virtualizate, iar tehnologiile de virtualizare sunt prezente deja nu numai pe servere și calculatoare portabile, dar chiar în unele tablete, telefoane mobile și sisteme industriale. Domeniul securității prin virtualizare a fost și este în continuare intens cercetat atât în zona academică, precum și în domeniul industrial în ultimii 10-15 ani.

### 10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Abilitatea de definire a conceptelor specifice problemelor de securitate la nivelul unei arhitecturi hardware și de expunere a metodelor de asigurare a	Examen scris și/sau tip grilă și/sau prezentarea unei teme de cercetare din domeniul cursului	50%

	securității prin mecanisme hardware și virtualizare. Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de curs		
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	50%
Proiect			
Standard minim de performanță: <b>Curs.</b> Prezența la <b>minim 50%</b> din orele de curs, pentru admiterea la examenul final. Cunoașterea și capacitatea de a explica principalele concepte de virtualizare și funcționalitatea de bază oferită de procesoarele Intel pentru securitate (SGX, MPX, TXT etc.) și virtualizare (VT-X). Cunoașterea și capacitatea de a explica tehnica de introspecție bazată pe virtualizare și o metodă de asigurare a securității bazată pe introspecție. <b>Aplicații.</b> Prezența la laborator <b>obligatorie 100%</b> (2 laboratoare se pot recupera în timpul semestrului, iar alte 2 în sesiunile de restanțe) pentru admiterea la examenul final. Extinderea mini-hipervizor-ului de laborator furnizat, astfel încât să pornească o mașină virtuală (MV) cu Windows, folosind funcționalitatea EPT și obținerea listei proceselor active din acea MV.			

Responsabil curs  
 Conf.dr.ing. Adrian Coleșa

Director departament  
 Prof.dr.ing. Rodica Potolea

## FIȘA DISCIPLINEI

### 1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare și Tehnologia Informației
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Securitatea Informațiilor și Sistemelor de calcul/ Master
1.7 Forma de învățământ	IF – învățământ cu frecvență
1.8 Codul disciplinei	10.

### 2. Date despre disciplină

2.1 Denumirea disciplinei	<b>Activitate de cercetare 2</b>				
2.2 Titularii de curs	Nu e cazul				
2.3 Titularul/Titularii activităților de seminar/laborator/proiect	Nu e cazul				
2.4 Anul de studiu	I	2.5 Semestrul	2	2.6 Tipul de evaluare ( E – examen, C – colocviu, V – verificare)	V
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	14	din care:	Curs		Seminar		Laborator		Proiect	14
3.2 Număr de ore pe semestru	196	din care:	Curs		Seminar		Laborator		Proiect	196
3.3 Distribuția fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie și notițe										
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate și pe teren										25
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii și eseuri										
(d) Tutoriat										
(e) Examinări										4
(f) Alte activități:										
3.4 Total ore studiu individual (suma (3.3(a)...3.3(f)))										29
3.5 Total ore pe semestru (3.2+3.4)										225
3.6 Numărul de credite										9

### 4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Activitatea de cercetare 1
4.2 de competențe	Competențele disciplinei de mai sus

### 5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Nu este cazul
5.2. de desfășurare a seminarului / laboratorului / proiectului	Echipamente și programe specifice temei de proiect

### 6. Competențele specifice acumulate

6.1 Competențe profesionale	<p>C2 - Investigarea și analiza situațiilor de criminalitate informatică și a software-ului malițios prin metode avansate de tip inginerie inversă și monitorizare comportament</p> <ul style="list-style-type: none"> <li>• C2.1 - Cunoașterea aprofundată a clasificării, caracteristicilor și particularităților aferente diferitelor tipuri de atacuri informatice și softurilor malițioase</li> <li>• 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</li> </ul>
-----------------------------	---

	<ul style="list-style-type: none"> <li>• C2.3 - Capacitatea de a face corelări și de a putea identifica obiecte potențial malițioase chiar dacă nu se poate analiza complet obiectul respectiv</li> <li>• 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</li> <li>• C2.5 - Elaborarea unor noi clase de atacuri sau software malițios, și propunerea unor noi proprietăți potrivite clasificării codurilor malițioase</li> </ul> <p>C3 - Analiza și evaluarea proprietăților de securitate a unui sistem de calcul. Identificarea erorilor de configurare și a vulnerabilităților software</p> <ul style="list-style-type: none"> <li>• C3.1 - Cunoașterea teoretică și practică a diverselor scenarii de configurare sau mentenanță greșită a sistemelor de calcul, precum și a claselor de vulnerabilități software și atacuri informatice tipice</li> <li>• C3.2 - Analiza și înțelegerea unor protocoale de comunicare și module software noi, pentru identificarea unor vulnerabilități posibile. Utilizarea listelor dedicate, recunoscute în domeniu, de clase și tipuri de vulnerabilități și configurări greșite pentru analiza și validarea unui sistem informatic nou din punct de vedere al securității</li> <li>• C3.3 - Capacitatea de a analiza critic, din punctul de vedere al testării vulnerabilității, configurarea unei rețele, sistem de calcul sau aplicații software, fără să existe informații anterioare. Capacitatea de a identifica informații vizibile, servicii expuse etc.</li> <li>• C3.4 - Evaluarea limitărilor teoretice și practice oferite de diverse metode și tehnologii de detectare a vulnerabilităților și configurărilor greșite ale sistemelor de calcul. Determinarea unor corelări constructive între diverse metode de detecție</li> <li>• C3.5 - Propunerea unor noi metode de clasificare, identificare sau analiză pentru vulnerabilitățile și configurările greșite de sisteme. Crearea unor soluții și utilitare software care să identifice și analizeze astfel de cazuri</li> </ul> <p>C4 - Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate</p> <ul style="list-style-type: none"> <li>• C4.1 - Cunoașterea principiilor și noțiunilor de bază necesare dezvoltării și testării unui cod sigur din punctul de vedere al securității. Cunoașterea claselor uzuale de software și unelte de securitate. Cunoașterea arhitecturilor de SO și platformelor necesare dezvoltării soluțiilor de securitate</li> <li>• C4.2 - Identificarea de noi scenarii în care este nevoie de introducerea unei soluții de securitate sau utilizarea unei unelte de securitate.</li> <li>• Analiza soluțiilor de securitate propuse și compararea lor cu cele cunoscute anterior</li> <li>• 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</li> <li>• C4.4 - Evaluarea unor proiecte software existente și identificarea greșelilor de securitate din punctul de vedere al arhitecturii, modului de programare sau procedurilor de testare. Propunerea unor noi metode de dezvoltare și testare</li> <li>• 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</li> </ul>
6.2 Competențe transversale	N/A

## 7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	Deprinderea de abilități și competente de cercetare, proiectare, dezvoltare și evaluare în domeniul securității informațiilor și sistemelor de calcul, calculatoarelor și al tehnologiei informațiilor.
---------------------------------------	---

7.2 Obiectivele specifice	<ol style="list-style-type: none"> <li>1. Definirea obiectivelor activității de cercetare corespunzătoare temei lucrării de disertație</li> <li>2. Cunoașterea exactă a soluțiilor existente pentru diverse aspecte ale problemei abordate</li> <li>3. Stabilirea unor direcții concrete de cercetare</li> <li>4. Propunerea unor posibile soluții viabile ale problemelor identificate</li> </ol>
---------------------------	--

## 8. Conținuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
-			
Bibliografie ( <i>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</i> )			
-			
8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
<ol style="list-style-type: none"> <li>1. Documentarea suplimentară asupra temei de disertație, realizarea unei clasificări pe principii critice a soluțiilor existente pentru diverse aspecte ale problemei abordate</li> <li>2. Enunțarea unor ipoteze de lucru, posibile soluții și justificarea lor teoretică</li> <li>3. Estimarea efortului necesar implementării și validării soluțiilor propuse</li> <li>4. Stabilirea programului de cercetare teoretică și experimentală</li> <li>5. Elaborarea schemei generale sau a arhitecturii sistemului ce urmează a fi dezvoltat</li> <li>6. Proiectarea componentelor sistemului dezvoltat</li> <li>7. Efectuarea de experimente, teste și verificări</li> <li>8. Elaborarea unui raport tehnic de descriere a activităților derulate și a rezultatelor obținute</li> </ol>	14	Colaborare îndrumător - student	
Bibliografie ( <i>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</i> )			
Se stabilește de către fiecare îndrumător de proiect de disertație în parte.			

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

## 9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului

Se realizeaza prin întâlniri periodice cu reprezentanții mediului economic.
---

## 10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs			
Seminar			
Laborator			
Proiect	Pe baza cunoștințelor și rezultatelor obținute și a referatului elaborat	Evaluare orala Evaluare referat	60% 40%
Standard minim de performanță: Propunerea a cel puțin unei soluții, stabilirea planului de cercetare și lucru, elaborarea arhitecturii generale a sistemului, elaborarea raportului tehnic.			

Responsabil curs  
Îndrumătorii de disertație

Director departament  
Prof.dr.ing. Rodica Potolea