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	11

2. Date despre disciplină

2.1	Denumirea disciplinei					Tratarea incidentelor de securitate și investigarea datelor digitale					
2.2	Aria tematica (subject area)					Calculatoare și Tehnologia Informației					
2.3	Responsabil de curs					Drd.ing. Dan LUȚAȘ (dlutas@bitdefender.com)					
2.4	Titularul activităților de laborator					Ing. Andrei LUȚAȘ (alutas@bitdefender.com)					
2.5	Anul de studii	II	2.6	Semestrul	3	2.7	Evaluarea	examen	2.8	Regimul disciplinei	DS/OB

3. Timpul total estimat

An/ Sem.	Denumirea disciplinei	Nr. săpt.	Curs	Aplicații			Curs	Aplicații			Studiu Individual	TOTAL	Credit
			[ore/săptămână]				[ore/semestru]						
				S	L	P		S	L	P			
II/3	Tratarea incidentelor de securitate și investigarea datelor digitale	14	2		1		28		14		88	130	5

3.1	Număr de ore pe săptămână	3	3.2	din care curs	2	3.3	aplicații	1
3.4	Total ore din planul de învățământ	42	3.5	din care curs	28	3.6	aplicații	14

Studiul individual	**Ore**
Studiul după manual, suport de curs, bibliografie si notițe	30
Documentara suplimentara in biblioteca, pe platformele electronice si pe teren	18
Pregătire seminarii / laboratoare, teme, referate, portofolii, eseuri	38
Tutoriat	0
Examinări	2
Alte activități	0

3.7	Total ore studiul individual	88
3.8	Total ore pe semestru	130
3.9	Număr de credite	5

4. Precondiții (acolo unde este cazul)

4.1	De curriculum	Securitatea informațiilor, Inginerie inversă și analiza de software malițios
4.2	De competențe	Arhitectura calculatoarelor, Arhitectura sistemelor de operare, Cunoștințe de bază de 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 aplicațiilor	Prezență la laborator obligatorie 100% pentru admiterea la examenul final

6. Competențe specifice acumulate

Competente 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
Competențe transversale	N/A

7. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

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. Conținuturi

8.1. Curs (programa analitică)		Metode de predare	Observații
1	Aspecte legale, gestionarea dovezilor digitale, limitări (steganografie, metadate)	Expunere la tablă, prezentare cu video-proiectorul, discuții	
2	Colectare dovezilor prin metode hardware, unelte de inspecție hardware		
3	Tratarea incidentelor de securitate (tratare, proceduri de răspuns - verificare, prioritizare, izolare, eradicare)		
4	Analiza discurilor și a sistemelor de fișiere (1): detalii despre NTFS, FAT, EXT3 etc.		
5	Analiza discurilor și a sistemelor de fișiere (2): unelte de procesare		
6	SO Windows: registry-ul (structură, unelte, tipuri de Informații)		
7	Analiza dump-urilor de memorie (1): crearea dump-urilor de memorie, framework-ul Volatility		
8	Analiza dump-urilor de memorie (2): căutarea de malware avansat, rootkit-uri etc.		
9	Analiza pachetelor de rețea (Wireshark): examinarea diferitelor atacuri, extragerea de date din pachete pentru reconstrucție		
10	Crearea de semnături pentru IDS/IPS: introducere în Snort, analiza și dezvoltarea de semnături Snort		
11	Corelare de evenimente: unelte de procesare a log-urilor pe Windows & Linux, log-uri specifice, timestamp-uri		
12	Investigații digitale pe dispozitive mobile: Android, unelte open/closed source		
13	Investigarea bazelor de date		
14	Subminarea uneltelor de investigare: ștergere sigură, criptarea disk-ului, prevenirea dump-urilor de memorie		
8.2. Aplicații (lucrări de laborator)		Metode de predare	Observații
1	Unelte și tehnici de inspecție hardware	Expuneri la tablă, exerciții la calculator, discuții și explicații suplimentare	
2	Unelte și tehnici de inspecție a sistemului de fișiere		
3	Unelte și tehnici de inspecție a Regystry-ului pe S.O. Windows si a dump-urilor de memorie. Windbg		
4	Inspecția pachetelor de rețea folosind utilitarul Wireshark. IDS, IPS, Snort. Aplicații		
5	Unelte și tehnici de inspecție a log-urilor. Corelare de evenimente		
6	Unelte și tehnici de inspecție pe dispozitive mobile si a bazelor de date		
7	Unelte și tehnici de subminare a investigației		

Bibliografie

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)

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor, profesionale și angajatori 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	10.1	Criterii de evaluare	10.2	Metode de evaluare	10.3	Ponderea 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%
Aplicații		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%

10.4 Standard minim de performanță

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.
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.

Responsabil curs
Dr.ing. Dan Luţaş

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	12

2. Date despre disciplină

2.1	Denumirea disciplinei				Elemente de securitate în configurarea sistemelor de calcul și a rețelelor de calculatoare						
2.2	Aria tematica (subject area)				Calculatoare și Tehnologia Informației						
2.3	Responsabil de curs				Conf.dr.ing. Emil CEBUC (emil.cebuc@cs.utcluj.ro)						
2.4	Titularul activităților de laborator				S.l.dr.ing. Bogdan IANCU (bogdan.iancu@cs.utcluj.ro)						
2.5	Anul de studii	II	2.6	Semestrul	3	2.7	Evaluarea	examen	2.8	Regimul disciplinei	DA/OB

3. Timpul total estimat

An/ Sem.	Denumirea disciplinei	Nr. săpt.	Curs	Aplicații			Curs	Aplicații			Studiu Individual	TOTAL	Credit
			[ore/săptămână]				[ore/semestru]						
				S	L	P		S	L	P			
II/3	Elemente de securitate în configurarea sistemelor și rețelelor	14	2		2		28		28		74	130	5

3.1	Număr de ore pe săptămână	4	3.2	din care curs	2	3.3	aplicații	2
3.4	Total ore din planul de învățământ	56	3.5	din care curs	28	3.6	aplicații	28

Studiul individual	**Ore**
Studiul după manual, suport de curs, bibliografie si notițe	30
Documentara suplimentara in biblioteca, pe platformele electronice si pe teren	20
Pregătire seminarii / laboratoare, teme, referate, portofolii, eseuri	22
Tutoriat	0
Examinări	2
Alte activități	0

3.7	Total ore studiul individual	74
3.8	Total ore pe semestru	130
3.9	Număr de credite	5

4. Precondiții (acolo unde este cazul)

4.1	De curriculum	Rețele de calculatoare, Arhitectura calculatoarelor
4.2	De competențe	Rețele de calculatoare, Arhitectura calculatoarelor

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 aplicațiilor	Prezență la laborator obligatorie 100% pentru admiterea la examenul final

6. Competențe specifice acumulate

Competente profesionale	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 informatice • 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 • C1.2 – Înțelegerea riscurilor de securitate specifice unor situații noi și legătura lor cu cele cunoscute anterior. Prevederea scenariilor posibile de securitate, în momentul în care soluțiile de securitate cunoscute sunt folosite într-o situație sau domeniu nou • 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 • 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 C3 - Analiza și evaluarea proprietăților de securitate a unui sistem de calcul. Identificarea erorilor de configurare și a vulnerabilităților software • 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 • 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 • 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. • 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 • 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
Competențe transversale	N/A

7. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

7.1	Obiectivul general al disciplinei	Înțelegerea și familiarizare cu structura tipică a rețelelor moderne din companii, privite din perspectiva administratorilor IT, cu accent pe aspectele de securitate, cum ar fi riscurile și incidentele de securitate din cadrul rețelelor de calculatoare și metodele de detectare și de prevenire a lor. Se urmărește dobândirea unei experiențe directe de instalare a unor servere de rețea tipice și configurare rolurilor cele mai uzuale (cum ar fi DHCP, DNS, Active Directory etc) punând un accent mare pe securitate.
7.2	Obiectivele specifice	1. Familiarizarea cu elementele de bază legate de virtualizarea sistemelor și a serverelor 2. Familiarizarea cu instalarea și configurarea unor servere și roluri tipice (atât Windows, cât și Linux) 3. Familiarizarea cu aspectele de bază legate de configurarea VLAN-urilor și a VPN-urilor, tehnologii pe larg folosite în rețelele tipice moderne 4. Familiarizarea cu elementele de bază a tehnologiilor de monitorizare și auditare a activităților de rețea 5. Înțelegerea celor mai importante aspecte de securitate în domeniul administrării sistemelor și a rețelelor de calcul

8. Conținuturi

8.1. Curs (programa analitică)		Metode de predare	Observații
1	Recapitularea cunoștințelor de bază de rețele de calculatoare (LAN, VLAN, WAN, IPv4/v6, TCP/IP, subnets, switch, router, OSI layers)	Expunere la tablă, prezentare cu video-proiectorul, discuții	
2	Securitatea echipamentelor de retea (Routere și switch-uri; console, telnet, SSH, local usernames & passwords, AAA, Port Security)		
3	Implementare Virtual LANs. Aspecte de securitate		
4	Reţele Virtuale Private (VPNs). Conexiuni remote și securitatea lor		
5	Monitorizarea, logarea și auditul activităților și traficului de rețea		
6	Tehnologii de detecție și prevenire a atacurilor (sisteme de tip IPS/IDS, detectarea scanărilor de rețea, a pachetelor greșit formatate, a atacurilor tip DoS etc)		
7	Soluții de virtualizare (VMware vSphere, Microsoft Hyper-V). Instalare, roluri și caracteristici, aspecte de securitate		
8	Windows Server 2012 R2 – Instalare si administrare Active Directory, DNS si DHCP server (Gestionarea utilizatorilor, grupurilor si a calculatoarelor din domeniu. Politici de domeniu)		
9	Windows Server 2012 R2 – Auditare fișiere și autentificare. Backup și Restore pentru Active Directory		
10	Windows Server Update Services – Instalare si configurare. Managementul update-urilor si a patch-urilor sistemelor de calcul		
11	Centos 7 Server – Instalare si configurare. Apache si FTP server		
12	Centos 7 Server – Roluri de Router și Firewall		
13	Alte teme importante de actualitate, noutăți legate de securitatea rețelelor		
14	Recapitulare		
8.2. Aplicații (lucrări de laborator)		Metode de predare	Observații
1	Recapitularea cunoștințelor de bază de rețele de calculatoare: IPv4, IPv6, DHCP, NAT/PAT, Wireshark	Expuneri la tablă, exerciții în laborator, discuții și explicații suplimentare	
2	Securitate, autentificare si monitorizare: telnet, SSH, local usernames & passwords, AAA, Port Security, 802.1x		
3	Implementare Virtual LANs si securizarea lor		
4	Implementarea funcțiilor de firewall și IPS la nivelul echipamentelor de rețea: liste de acces (IPv4, IPv6 ACLs), VPN		
5	Securitate, autentificare si monitorizare: SNMP, Syslog, NetFlow		
6	Securitate, autentificare si monitorizare: Network inspection tools		
7	Soluții de virtualizare. Microsoft Hyper-V: Instalare, roluri și caracteristici		
8	Soluții de virtualizare. Microsoft Hyper-V: aspecte de securitate		
9	Windows Server 2012 R2: Instalare si administrare Active Directory, DNS si DHCP server		
10	Windows Server 2012 R2: Backup și restore pentru Active Directory, auditare fișiere și autentificare, Windows Server Update Services (WSUS)		
11	Centos 7 Server: Instalare si configurare SO si servicii		
12	Centos 7 Server: Roluri de router și firewall		
13	Securitatea în reţele wireless LAN si mobile		
14	Test de laborator		

Bibliografie

1. The Practice of System and Network Administration (Limonceli, Thomas – 2007 – Addison-Wesley) (2nd ed)
2. UNIX and Linux System Administration Handbook (Nemeth, Evi – 2010 – Prentice Hall) (4th ed)
3. Mastering Windows Server 2012 R2 (Minasi, Mark – 2013 – Sybex)
4. CCNA Security 640-554 Official Cert Guide (Barker, Keith – 2012 – Cisco Press)

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

Se realizează prin discuții periodice cu reprezentanți ai angajatorilor importanți din domeniul securității informației.
Cursuri referitoare la aspecte de securitate în administrarea sistemelor de operare și rețelelor de calculatoare și domenii adiacente sunt prezente în cadrul multor alte masterate din domeniul securității calculatoarelor și a informațiilor, la universități din țară și străinătate, cum ar fi:

- Security Architectures and Network Defence, Master in Cyber Security and Management, The University of Warwick, IK, http://www2.warwick.ac.uk/fac/sci/wmg/education/wmgmasters/structure/modules/sand
- *Securitatea rețelelor de calculatoare*, Master de Securitatea tehnologiei informației, Academia Tehnică Militară, București, http://mta.ro/masterat/masterinfosec/curricula2014.html
- *Networking and Systems Requirement*, Master of Science in Information Security, Carnegie Mellon University, SUA, http://www.ini.cmu.edu/degrees/msis/courses.html
- *Network Security* și *Secure Operating Systems*, Master of Engineering in Cybersecurity, Cybersecurity Center, University of Mayland, http://www.cyber.umd.edu/education/meng-cybersecurity

10. Evaluare

Tip activitate	10.1	Criterii de evaluare	10.2	Metode de evaluare	10.3	Ponderea 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%
Aplicații		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%

10.4 Standard minim de performanță

Demonstrarea înțelegerii teoretice și practice a rolurilor de bază a serverelor de rețea, a echipamentelor de rețea (switch-uri, routere), și interacțiunea dintre ele.
Demonstrarea abilității de a instala un server cu roluri de bază, configurat conform practicilor și standardelor de securitate.
Demonstrarea cunoștințelor teoretice și a abilității practice de a monitoriza și analiza activitățile de rețea și/sau traficul de rețea tipică unei companii mici.

Responsabil curs
Conf.dr.ing. Emil Cebuc

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	13

2. Date despre disciplină

2.1	Denumirea disciplinei					Testarea vulnerabilității sistemelor informatice					
2.2	Aria tematica (subject area)					Calculatoare și Tehnologia Informației					
2.3	Responsabil de curs					Ing. Andrei LUȚAȘ (dlutas@bitdefender.com)					
2.4	Titularul activităților de proiect					Ing. Andrei LUȚAȘ, Drd. ing. Vlad Ioan TOPAN (alutas@bitdefender.com, itopan@bitdefender.com)					
2.5	Anul de studii	II	2.6	Semestrul	3	2.7	Evaluarea	examen	2.8	Regimul disciplinei	DS/OB

3. Timpul total estimat

An/ Sem.	Denumirea disciplinei	Nr. săpt.	Curs	Aplicații			Curs	Aplicații			Studiu Individual	TOTAL	Credit
			[ore/săptămână]				[ore/semestru]						
				S	L	P		S	L	P			
II/3	Testarea vulnerabilității sistemelor informatice	14	2			1	28			14	114	156	6

3.1	Număr de ore pe săptămână	3	3.2	din care curs	2	3.3	aplicații	1
3.4	Total ore din planul de învățământ	42	3.5	din care curs	28	3.6	aplicații	14

Studiul individual	**Ore**
Studiul după manual, suport de curs, bibliografie si notițe	10
Documentara suplimentara in biblioteca, pe platformele electronice si pe teren	20
Pregătire proiecte, laboratoare, teme, referate, portofolii, eseuri	79
Tutoriat	0
Examinări	5
Alte activități	0

3.7	Total ore studiul individual	114
3.8	Total ore pe semestru	156
3.9	Număr de credite	6

4. Precondiții (acolo unde este cazul)

4.1	De curriculum	Probleme de securitate la nivel de cod sursă
4.2	De competențe	Arhitectura calculatoarelor, Arhitectura sistemelor de operare, Cunoștințe de bază de rețele de calculatoare, Programare C și în limbaj de asamblare x86

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 aplicațiilor	Prezență la proiect 100% pentru admiterea la examenul final

6. Competențe specifice acumulate

Competente profesionale	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 informatice • C1.2 – Înțelegerea riscurilor de securitate specifice unor situații noi și legătura lor cu cele cunoscute anterior. Prevederea scenariilor posibile de securitate, în momentul în care soluțiile de securitate cunoscute sunt folosite într-o situație sau domeniu nou • 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 • 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 C3 - Analiza și evaluarea proprietăților de securitate a unui sistem de calcul. Identificarea erorilor de configurare și a vulnerabilităților software • 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 • 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 • 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. • 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 • 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
Competențe transversale	N/A

7. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

7.1	Obiectivul general al disciplinei	Conferirea capacității de a înțelege erorile de arhitectură/dezvoltare software ce introduc diferitele clase de vulnerabilități, de a găsi, prin metode specifice, astfel de vulnerabilități într-un sistem informatic și de a le exploata în scopul obținerii și menținerii accesului într-un sistem informatic. Se urmărește, de asemenea, dobândirea capacității de a realiza un raport tehnic coerent în care se detaliază problemele descoperite, impactul acestora asupra sistemului informatic și se propun soluții pentru rezolvarea lor.
7.2	Obiectivele specifice	Pentru atingerea obiectivelor generale, se urmărește: • Înțelegerea pașilor generali ai activității de testare a vulnerabilităților: definirea scopului, obținerea autorizației din partea beneficiarului, testarea în sine, realizarea raportului, prezentarea rezultatului final • Înțelegerea pașilor specifici testării vulnerabilității unui sistem informațional: culegerea de informații din surse publice, scanarea de porturi, enumerarea serviciilor, exploatarea vulnerabilităților, obținerea de privilegii sporite, identificarea și exploatarea unor noi ținte • Familiarizarea cu cele mai populare unelte folosite în pașii specifici testării de vulnerabilități (ca exemplu : nmap pentru scanarea de porturi) • Înțelegerea principalelor clase de vulnerabilități si a erorilor de programare de care sunt generate (Buffer/Heap overflow, SQL Injection, XSS, CSRF, LFI etc) • Familiarizarea cu folosirea limbajului de asamblare pentru a putea citi/construi shellcode-uri • Înțelegerea principalelor tehnici de reducere a posibilității de exploatare a

		vulnerabilităților (stack cookies, validarea lanțului SEH, DEP, ASLR) și a metodelor prin care acestea pot fi depășite. • Înțelegerea metodelor prin care se pot obține privilegii sporite, odată obținut accesul: exploatarea de vulnerabilități în nucleul sistemului de operare, folosirea serviciilor ce rulează cu privilegii sporite, etc. • Înțelegerea metodelor de creare de tuneluri între sisteme informatice ce se află în rețele diferite (tuneluri SSL) • Cunoașterea modului de redactare a raportului activității de testare a vulnerabilității sistemelor informatice și a informațiilor ce trebuie sa fie prezente în raport.

8. Conținuturi

8.1. Curs (programa analitică)		Metode de predare	Obs.
1	Introducere în testarea vulnerabilităților sistemelor informatice: scop, autorizare, rezultate, raportare, unelte de scanare a vulnerabilităților	Expunere la tablă, prezentare cu videoproiectorul, discuții	
2	Culegerea de informații: culegerea de informații din surse publice: google, dns, whois, SNMP, SMTP		
3	Scanarea de porturi: diferite metode, utilizarea uneltei nmap, identificarea sistemului de operare		
4	Enumerare: extragerea banner-elor, NetBios, identificarea serviciilor, identificarea versiunilor		
5	Vulnerabilități de corupere a memoriei: buffer/heap overflow, integer overflows, signed/unsigned		
6	Elemente de bază în utilizarea exploiturilor: asamblare x86, înțelegerea shellcode-urilor, modificarea shellcode-urilor, codificatoare, evitarea caracterelor nedorite		
7	Vulnerabilitățile aplicațiilor web (LFI, RFI, traversarea directoarelor, XSS, CSRF)		
8	Injecții SQL: tratarea diferitelor SGDB-uri: MS-SQL, Mysql, Oracle, Mongodb)		
9	Tehnici de exploatare: obținerea shell-ului inițial, tipuri de shell-uri, meterpreter)		
10	Scenarii de tunneling		
11	Obținerea de privilegii sporite: Windows/Unix, servicii implicite, vulnerabilități de kernel, servicii privilegiate		
12	Post-exploatare: obținerea de hash-uri de parole, pass-the-hash, forensics		
13	Scrierea raportului activității de testare a vulnerabilităților		
14	Evitarea ASLR, exploatarea folosind reutilizare de cod (ROP), exploituri de kernel		
8.2. Aplicații (proiect)		Metode de predare	Obs.
1	Familiarizarea cu laboratorul virtual de teste de penetrare. Culegerea de informații interne de pe un sistem penetrat (post-exploatare): obținerea de hash-uri de parole, pass-the-hash, forensics	Expuneri la tablă, exerciții demonstrative, discuții și explicații suplimentare legate de temele de proiect	
2	Culegerea de informații din surse publice: Google, DNA, whois, SNMP, SMTP etc. Scanarea porturilor, identificarea serviciilor, sistemului de operare, obținerea de alte detalii specifice unui anumit serviciu		
3	Penetrarea sistemelor/serviciilor cu vulnerabilități de corupere a memoriei		
4	Tehnici și unelte de exploatare: framework-ul *Metasploit*. Cod de acces (*Shellcode*): generare și modificare. Unelte de generare și depanare		
5	Vulnerabilități ale aplicațiilor Web și metode de penetrare: LFI, RFI, XSS, CSRF, traversare directoare, injecție de cod SQL etc.		
6	Metode de obținere de privilegii sporite		
7	Metode și unelte de creare de tunele de acces (*tunneling*)		

Bibliografie

1. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)
2. Metasploit: The Penetration Tester's Guide (Kennedy, David – 2011 – No Stach Press)
3. Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)
4. Hacking Exposed – Network Security Secrets Exposed (McClure, Stuart – 2012 – McGraw-Hill) (7th ed)
5. Diverse site-uri legate de pentesting (ex. http://www.offensive-security.com/metasploit-unleashed)

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor, profesionale și angajatori 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 domeniul pentesting sunt prezente în cadrul multor alte masterate din domeniul securității calculatoarelor și a informațiilor, sau în cadrul unor cursuri opționale, cum ar fi:

- *Offensive Security*, Dakota State University, USA
  http://catalog.dsu.edu/preview_course_nopop.php?catoid=8&coid=3804
- *CS6573 Penetration Testing and Vulnerability Analysis*, Masters in Cybersecurity, New York Polytechnic School of Engineering, New York, USA
  http://engineering.nyu.edu/academics/course/CS6573
- *Offensive Computer Security,* Florida State University, USA
  http://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/

10. Evaluare

Tip activitate	10.1	Criterii de evaluare	10.2	Metode de evaluare	10.3	Ponderea din nota finală
Curs		Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de curs		Examen practic de penetrare și scrierea unui raport de evaluare și penetrare și/sau examen scris și/sau tip grilă și/sau prezentarea unei teme de cercetare din domeniul cursului		50%
Aplicații		Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de proiect		Testarea vulnerabilității și penetrarea unor sistem de test și realizarea și prezentarea unui raport de evaluare și penetrare.		50%

10.4 Standard minim de performanță

Curs: Demonstrarea înțelegerii noțiunilor de bază, a principiilor și a metodelor utilizate în testarea vulnerabilității sistemelor informatice, cum ar fi : tipurile de vulnerabilități, erorile de arhitectură/programare ce introduc vulnerabilitățile, metodologia (pașii) de testare, uneltele folosite în fiecare pas al metodologiei, realizarea raportului activității de testare. Evaluare și penetrate un sistem în care aplicarea noțiunilor menționate este directă.
Proiect: Demonstrarea abilității practice de a realiza testarea vulnerabilității unui sistem informatic (în cadrul unui mediu virtual, controlat) parcurgând pașii din metodologia de testare, inclusiv realizarea raportului final. Evaluare și penetrare două din sistemele cu cea mai mică dificultate de penetrare.

Responsabil curs
Ing. Andrei Luţaş

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	14.1

2. Date despre disciplină

2.1	Denumirea disciplinei					Modele matematice pentru securitatea calculatoarelor					
2.2	Aria tematica (subject area)					Calculatoare și Tehnologia Informației					
2.3	Responsabil de curs					Prof.dr. Ioan RASA (ioan.rasa@math.utcluj.ro)					
2.4	Titularul activităților de seminar					S.l.Dr.ing. Ciprian OPRIȘA (coprisa@bitdefender.com)					
2.5	Anul de studii	II	2.6	Semestrul	3	2.7	Evaluarea	examen	2.8	Regimul disciplinei	DA/OP

3. Timpul total estimat

An/ Sem.	Denumirea disciplinei	Nr. săpt.	Curs	Aplicații			Curs	Aplicații			Studiu Individual	TOTAL	Credit
			[ore/săptămână]				[ore/semestru]						
				S	L	P		S	L	P			
II/3	Modele matematice pentru securitatea calculatoarelor	14	2	2			28	28			74	130	5

3.1	Număr de ore pe săptămână	4	3.2	din care curs	2	3.3	aplicații	2
3.4	Total ore din planul de învățământ	56	3.5	din care curs	28	3.6	aplicații	28

Studiul individual	**Ore**
Studiul după manual, suport de curs, bibliografie si notițe	36
Documentara suplimentara in biblioteca, pe platformele electronice si pe teren	16
Pregătire seminarii / laboratoare, teme, referate, portofolii, eseuri	20
Tutoriat	0
Examinări	2
Alte activități	0

3.7	Total ore studiul individual	74
3.8	Total ore pe semestru	130
3.9	Număr de credite	5

4. Precondiții (acolo unde este cazul)

4.1	De curriculum	N/A
4.2	De competențe	N/A

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 aplicațiilor	Prezență la seminar obligatorie 100% pentru admiterea la examenul final

6. Competențe specifice acumulate

Competente profesionale	C2 - Investigarea și analiza situațiilor de criminalitate informatică și a software-ului malițios prin metode avansate de tip inginerie inversă și monitorizare comportament • C2.5 – Elaborarea unor noi clase de atacuri sau software malițios, și propunerea unor noi proprietăți potrivite clasificării codurilor malițioase C3 - Analiza și evaluarea proprietăților de securitate a unui sistem de calcul. Identificarea erorilor de configurare și a vulnerabilităților software • 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 • 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 C4 - Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate • 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 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 • C5.2 – 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 • C5.3 – 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 • 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 • 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
Competențe transversale	N/A

7. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

7.1	Obiectivul general al disciplinei	În urma acestui curs, studenții trebuie să deprindă principiul de a privi informația prin modele matematice, prin însușirea tehnicilor fundamentale din teoria probabilităților, statistici și teoria numerelor.
7.2	Obiectivele specifice	• Capacitatea de a calcula probabilități • Capacitatea de a modela matematic sisteme din lumea reală • Capacitatea de a lucra cu modele statistice și de a extrage informații din datele din lumea reală • Capacitatea de a folosi primitive criptografice bazate pe teoria numerelor

8. Conținuturi

8.1. Curs (programa analitică)		Metode de predare	Observații
1	Probabilități	Expunere la tablă, prezentare cu video-proiectorul, discuții	
2	Teoria informației: entropie, informație mutuală		
3	Teoria informației: complexitate Kolmogorov, compresia datelor		
4	Variabile aleatoare, media și dispersia		
5	Corelație, regresie liniară, regresie logistică		
6	Support Vector Machines		
7	Funcții Kernel pentru Support Vector Machines		
8	Rețele Bayesiene, partea 1		
9	Rețele Bayesiene, partea 2		
10	Testarea ipotezelor statistice, partea 1		
11	Testarea ipotezelor statistice, partea 2		
12	Modele matematice în criptografie: Introducere		
13	Modele matematice în criptografie: Logaritmul discret, Diffie-Helman		
14	Modele matematice în criptografie: Factorizarea întregilor, RSA		
8.2. Aplicații (seminar)		Metode de predare	Observații
1	Probabilități	Expuneri la tablă, explicații suplimentare, discuții	
2	Entropie, informație mutuală		
3	Complexitate Kolmogorov, compresia datelor		
4	Variabile aleatoare		
5	Corelație și regresie		
6	Clasificarea aplicațiilor malițioase folosind Support Vector Machines		
7	Funcții Kernel pentru Support Vector Machines		
8	Tehnici Bayes de estimare		
9	Aplicații ale tehnicilor Bayes în detecția de spam		
10	Utilizarea clasificatorilor în securitate		
11	Testarea ipotezelor statistice		
12	Aplicații cu primitive criptografice		
13	Studiul unor atacuri asupra protocoalelor criptografice, partea 1		
14	Studiul unor atacuri asupra protocoalelor criptografice, partea 2		

Bibliografie

1. Ioan Rasa, Lectures on Probability Theory and Stochastic Processes, U.T.Pres 2006
2. Henry Stark, John Woods, Probability, Statistics, and Random Processes for Engineers (4th Edition), Prentice Hall, 2011
3. Jeffrey Hoffstein, Jill Pipher, J.H. Silverman, An Introduction to Mathematical Cryptography, Springer, 2010
4. Nello Cristianini, John Shawe-Taylor, An Introduction to Support Vector Machines and other kernel-based learning methods, Cambridge University Press, 2000

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor, profesionale și angajatori 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.
O serie din cursurile de securitate din programele de master, cum ar fi cele de criptografie, manipulare date masive, corectitudinea (din perspectiva securității) aplicațiilor și altele au la baza modele și metode matematice, ceea ce face absolut necesară cunoașterea acestora și capacitatea studenților de a aplica acele modele în domenii specifice securității sistemelor și informației. Exemple de master ce conțin cursuri de matematică aplicată:

- M.A. in Applied Mathematic, UCSandiego, USA, http://math.ucsd.edu/programs/graduate-program/ma-applied-mathematics/index.html

10. Evaluare

Tip activitate	10.1	Criterii de evaluare	10.2	Metode de evaluare	10.3	Ponderea din nota finală
Curs		Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de curs		Examen scris		50%
Aplicații		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		50%
10.4 Standard minim de performanță						
La finalul cursului, studenții trebuie să poată rezolva probleme ce implică teoria probabilităților, să poată lucra cu modele statistice și cu primitive criptografice.						

Responsabil curs
Prof.dr. Ioan Raşa

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	14.2

2. Date despre disciplină

2.1	Denumirea disciplinei					Criptografie aplicată					
2.2	Aria tematica (subject area)					Calculatoare și Tehnologia Informației					
2.3	Responsabil de curs					Prof.dr.ing. Alin SUCIU (asuciu@cs.utcluj.ro)					
2.4	Titularul activităților de seminar					Sl.dr.ing.Kinga MARTON (kinga.marton@cs.utcluj.ro)					
2.5	Anul de studii	II	2.6	Semestrul	3	2.7	Evaluarea	examen	2.8	Regimul disciplinei	DA/OP

3. Timpul total estimat

An/ Sem.	Denumirea disciplinei	Nr. săpt.	Curs	Aplicații			Curs	Aplicații			Studiu Individual	TOTAL	Credit
			[ore/săptămână]				[ore/semestru]						
				S	L	P		S	L	P			
II/3	Criptografie aplicată	14	2	2			28	28			74	130	5

3.1	Număr de ore pe săptămână	4	3.2	din care curs	2	3.3	aplicații	2
3.4	Total ore din planul de învățământ	56	3.5	din care curs	28	3.6	aplicații	28

Studiul individual	**Ore**
Studiul după manual, suport de curs, bibliografie si notițe	24
Documentara suplimentara in biblioteca, pe platformele electronice si pe teren	15
Pregătire seminarii / laboratoare, teme, referate, portofolii, eseuri	32
Tutoriat	0
Examinări	3
Alte activități	0

3.7	Total ore studiul individual	74
3.8	Total ore pe semestru	130
3.9	Număr de credite	5

4. Precondiții (acolo unde este cazul)

4.1	De curriculum	Securitatea informațiilor
4.2	De competențe	Programare C, Arhitectura sistemelor de operare, Cunoștințe de bază de 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 aplicațiilor	Prezență la seminar obligatorie 100% pentru admiterea la examenul final

6. Competențe specifice acumulate

Competente 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 C3 - Analiza și evaluarea proprietăților de securitate a unui sistem de calcul. Identificarea erorilor de configurare și a vulnerabilităților software • 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 • 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 C4 - Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate • C4.2 – Identificarea de noi scenarii în care este nevoie de introducerea unei soluții de securitate sau utilizarea unei unelte de securitate. Analiza soluțiilor de securitate propuse și compararea lor cu cele cunoscute anterior • C4.4 – 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 • 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 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 – Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate • 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 • 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
Competențe transversale	N/A

7. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

7.1	Obiectivul general al disciplinei	Familiarizarea studenților cu noțiunile și elementele de bază ale criptografiei, precum și cu folosirea și înțelegerea celor mai reprezentative și pe larg folosite primitive de criptografie, cum ar fi SHA256, AES128/256, RSA2048. Se urmărește dobândirea de către studenți a capacității de folosire a diverselor metode și tehnici de criptografie și de apreciere a valorii și implicațiilor acestora din punctul de vedere al securității informației, a capacității de a face corelări cu domeniul criptografiei pentru a putea căuta informații și analize mai detaliate referitoare la activitățile de dezvoltare a aplicațiilor și de analiză a incidentelor de securitate.

7.2	Obiectivele specifice	1. Înțelegerea primitivelor și metodelor criptografice existente (elementele lor de bază, funcționarea lor, rolul lor, interacțiunea dintre ele), 2. Înțelegerea metricilor și a metodelor de comparare și evaluare a securității unor primitive criptografice, 3. Însușirea abilității de a folosi în mod corespunzător primitive criptografice în aplicațiile proprii, 4. Însușirea abilității de a analiza cerințele și necesitățile unor proiecte software din punct de vedere criptografic.

8. Conținuturi

8.1. Curs (programa analitică)		Metode de predare	Observații
1	Elemente introductive și noțiuni fundamentale de criptografie	Expunere la tablă, prezentare cu video-proiectorul, discuții	
2	Aplicațiile criptografiei în lumea reală. Generatoare de numere aleatoare		
3	Criptografia simetrică. Cifruri de tip stream. OTP, eSTREAM		
4	Criptografia simetrică. Cifruri de tip block		
5	DES, AES128/196/256, alte cifruri de tip bloc		
6	Criptografia asimetrică (cu chei publice)		
7	RSA2048, alte cifruri asimetrice		
8	Funcții hash criptografice. SHA-1, SHA-2, SHA-3		
9	Semnături digitale și infrastructurile PKI. Sisteme de criptare hibride		
10	Gestiunea cheilor criptografice		
11	Noțiuni introductive de criptografie cuantică și criptografie probabilistică, exemple		
12	Noțiuni introductive de steganografie, exemple		
13	Noțiuni introductive de criptanaliză, studii de caz		
14	Prezentarea unor atacuri de implementare (tip side-channel)		
8.2. Aplicații (seminar)		Metode de predare	Observații
1	Algoritmi criptografici clasici – aplicații, partea 1	Expunere la tablă, discuții	
2	Algoritmi criptografici clasici – aplicații, partea 2		
3	Metode și utilitare de analiză a numerelor aleatoare și a pattern-urilor în fluxuri de date pentru analiza criptografică, partea 1		
4	Metode și utilitare de analiză a numerelor aleatoare și a pattern-urilor în fluxuri de date pentru analiza criptografică, partea 2		
5	Implementarea unor cifruri de tip stream în C		
6	Implementarea unor cifruri de tip bloc în C		
7	Implementarea unor funcții hash în C		
8	Folosirea bibliotecilor Windows CNG și OpenSSL		
9	Primitive de criptografie în hardware: TPM-ul		
10	Primitive de criptografie în hardware: instrucțiuni Intel AES		
11	Alte metode de criptografie hardware		
12	Prezentarea unor cazuri recente de atacuri criptografice 1. Discuții		
13	Prezentarea unor cazuri recente de atacuri criptografice 2. Discuții		
14	Topic-uri și metode noi de criptografie		

Bibliografie

1. Understanding Cryptography: A Textbook for Students and Practitioners, (Paar, Pelzl -2010, Springer-Verlag New York Inc .)
2. Cryptography Engineering: Design Principles and Practical Applications (Ferguson, Niels - 2010-Willey)
3. Cryptography and Network Security. Principles and Practice (Stallings, William – 2013 – Prentice Hall)
4. Cryptography: A Very Short Introduction (Piper, Fred – 2002 – Oxford University Press)
5. Microsoft MSDN, Cryptography API: Next Generation (disponibil online)
6. Diferite articole

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

- CSci 6331 Cryptography – The George Washington University – Washington DC, USA – Master of Science in Cybersecurity
- Cryptography (252-0407-00) – ETH Zurich – Elveția – Information Security Master
- Criptografie computațională – Academia Tehnica Militară – București – Master de Securitatea Tehnologiei Informației

10. Evaluare

Tip activitate	10.1	Criterii de evaluare	10.2	Metode de evaluare	10.3	Ponderea 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%
Aplicații		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		50%

10.4 Standard minim de performanță

Demonstrarea înțelegerii noțiunilor de bază, a principiilor și a metodelor uzuale din criptografie, cum ar fi: numere aleatoare, importanța problemelor fundamentale de matematică care stau la baza primitivelor de criptografie (cum ar fi problema de factorizării a două numere prime), proprietățile esențiale ale funcțiilor criptografice de hash, proprietățile criptografiei simetrice, noțiuni de criptanaliză, noțiuni și metode de atac criptografic, atacuri tip side-channel.
Demonstrarea abilității de a folosi corect, într-o aplicație proprie C, a unor primitive de criptografie (hash, semnături digitale, criptografie simetrică, criptografie asimetrică) deja existente și expuse de o librărie.

Responsabil curs
Prof.dr.ing. Alin Suciu

Director departament
Prof.dr.ing. Rodica Potolea

FISA DISCIPLINEI

1. Date despre program

1.1	Institutia de invatamint superior	Universitatea Tehnica din Cluj-Napoca
1.2	Facultatea	Automatica si 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 Informațiilor și Sistemelor de Calcul / Master
1.7	Forma de invatamint	IF – invatamant cu frecventa
1.8	Codul disciplinei	15

2. Date despre disciplina

2.1	Denumirea disciplinei					Activitate de cercetare 3					
2.2	Aria tematica (subject area)					Calculatoare și Tehnologia Informației					
2.3	Responsabil de curs					Nu e cazul					
2.4	Titularul activităţilor de proiect					Nu e cazul					
2.5	Anul de studii	II	2.6	Semestrul	3	2.7	Evaluarea	A/R	2.8	Regimul disciplinei	DS/OB

3. Timpul total estimat

An/ Sem	Denumirea disciplinei	Nr. sapt.	Curs	Aplicaţii			Curs	Aplicaţii			Stud. Ind.	TOTAL	Credit
			[ore/săpt.]				[ore/sem.]						
				S	L	P		S	L	P			
II/3	Activitate de cercetare 3	14		3				42			192	234	9

3.1	Numar de ore pe saptamina	3	3.2	din care curs	-	3.3	aplicatii	3
3.4	Total ore din planul de inv.	42	3.5	din care curs	-	3.6	aplicatii	42

Studiul individual	Ore
Studiul după manual, suport de curs, bibliografie și notițe	0
Documentare suplimentară în bibliotecă, pe platformele electronice și pe teren	30
Pregătire referate, portofolii, eseuri, rapoarte tehnice și articole științifice	45
Tutoriat	14
Examinări	3
Alte activități (implementare aplicații și prototipuri de validare, testare și evaluare)	100

3.7	Total ore studiul individual	192
3.8	Total ore pe semestru	234
3.9	Numar de credite	9

4. Preconditii (acolo unde este cazul)

4.1	De curriculum	Activitatea de cercetare 1 si 2
4.2	De competente	Competentele disciplinelor de mai sus

5. Conditii (acolo unde este cazul)

5.1	De desfasurare a cursului	Nu este cazul
5.2	De desfasurare a aplicatiilor	Echipamente si programe specifice temei de proiect

6. Competente specifice acumulate

Competente profesionale	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 • C5.3 - 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 • 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 • 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
Competențe transversale	CT2 - Abilități de analiză, planificare și coordonare de proceduri de lucru, etape de proiect și sarcini individuale necesare îndeplinirii unui proiect complex. Abilități de evaluare a rezultatelor și a progreselor, precum și de raportare prin sinteză a stării și derulării unui proiect, având o viziune globală de ansamblu CT3 **-** Exersarea deprinderii de autoeducare continuă și demonstrarea de abilități critice, analitice, inovatoare și de cercetare

7 Obiectivele disciplinei (reiesind din grila competentelor specific acumulate)

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	1. Validarea soluțiilor propuse și rafinarea lor 2. Obținerea unor rezultate aplicabile în situații reale 3. Publicarea unei lucrări științifice

8. Continuturi

8.1. Curs (programa analitica)		Metode de predare	Observații
1	Nu e cazul.		
8.2. Aplicații (proiect)		Metode de predare	Observatii
	1. Documentarea suplimentară asupra temei de disertație 2. Proiectarea de detaliu a componentelor sistemului ce implementează soluțiile propuse 3. Implementarea unui prototip a sistemului propus, care să valideze soluțiile propuse și să evidențieze eventualele lor limitări 4. Propunerea unor rafinări, îmbunătățiri ale soluțiilor testate 5. Elaborarea unui articol științific și trimiterea lui spre evaluare la o conferință sau jurnal din domeniul temei lucrării de disertație 6. Elaborarea unui raport tehnic de descriere a activităților derulate și a rezultatelor obținute	Colaborare îndrumător - student	
Bibliografie Se stabilește de către fiecare îndrumător de proiect de disertație în parte.			

9. Coroborarea continuturilor disciplinei cu asteptarile reprezentantilor comunitatii epistemice, asociatiilor, profesionale si angajatori din domeniul aferent programului

Se realizeaza prin întâlniri periodice cu reprezentanții mediului economic.

10. Evaluare

Tip activitate	10.1	Criterii de evaluare	10.2	Metode de evaluare	10.3	Ponderea din nota finala
Curs		Nu este cazul				
Aplicații		Pe baza cunoștințelor și rezultatelor obținute și a referatului elaborat		Evaluare orala Evaluare referat		60% 40%
10.4 Standard minim de performanta						
Implementare și testarea a cel puțin uneia dintre soluțiile propuse, elaborarea raportului tehnic.						

Responsabil curs
Indrumatorii de disertatie

Director departament
Prof.dr.ing. Rodica Potolea