FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare si Tehnologia Informatiei
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Securitatea Informatiilor si Sistemelor de calcul/ Master
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	13.

2. Date despre disciplină

2.1 Denumirea disciplinei				***Testarea vulnerabilității sistemelor informatice***	
2.2 Titularii de curs				Drd. Ing. Radu Portase	
2.3 Titularul/Titularii activităţilor de seminar/laborator/proiect				Inf. Mihai Topan	
2.4 Anul de studiu	II	2.5 Semestrul	1	2.6 Tipul de evaluare *(E – examen, C – colocviu, V – verificare)*	E
2.7 Regimul disciplinei	*DA – de aprofundare, DS – de sinteza, DC – complementară*				DS
	DI – Impusă, DOp – opțională, DFac – facultativă				DI

3. Timpul total estimat

3.1 Număr de ore pe săptămână	3	din care:	Curs	2	Seminar		Laborator		Proiect	1
3.2 Număr de ore pe semestru	42	din care:	Curs	28	Seminar		Laborator		Proiect	14
3.3 Distribuţia fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie şi notiţe										10
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren										20
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri										73
(d) Tutoriat										0
(e) Examinări										5
(f) Alte activităţi:										0

3.4 Total ore studiu individual (suma (3.3(a)…3.3(f)))	108
3.5 Total ore pe semestru (3.2+3.4)	150
3.6 Numărul de credite	6

4. Precondiţii (acolo unde este cazul)

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

5. Condiţii (acolo unde este cazul)

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

6. Competenţele specifice acumulate

6.1 Competenţe profesionale	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
6.2 Competenţe transversale	N/A

7. Obiectivele disciplinei

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. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Introducere în testarea vulnerabilităților sistemelor informatice: scop, autorizare, rezultate, raportare, unelte de scanare a vulnerabilităților	2	Expunere la tablă, prezentare cu video-proiectorul, discuții	
Culegerea de informații: culegerea de informații din surse publice: google, dns, whois, SNMP, SMTP	2		
Scanarea de porturi: diferite metode, utilizarea uneltei nmap, identificarea sistemului de operare	2		
Enumerare: extragerea banner-elor, NetBios, identificarea serviciilor, identificarea versiunilor	2		
Vulnerabilități de corupere a memoriei: buffer/heap overflow, integer overflows, signed/unsigned	2		
Elemente de bază în utilizarea exploiturilor: asamblare x86, înțelegerea shellcode-urilor, modificarea shellcode-urilor, codificatoare, evitarea caracterelor nedorite	2		
Vulnerabilitățile aplicațiilor web (LFI, RFI, traversarea directoarelor, XSS, CSRF)	2		
Injecții SQL: tratarea diferitelor SGDB-uri: MS-SQL, Mysql, Oracle, Mongodb)	2		
Tehnici de exploatare: obținerea shell-ului inițial, tipuri de shell-uri, meterpreter)	2		
Scenarii de tunneling	2		
Obținerea de privilegii sporite: Windows/Unix, servicii implicite, vulnerabilități de kernel, servicii privilegiate	2		
Post-exploatare: obținerea de hash-uri de parole, pass-the-hash, forensics	2		
Scrierea raportului activității de testare a vulnerabilităților	2		
Evitarea ASLR, exploatarea folosind reutilizare de cod (ROP), exploituri de kernel	2		

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

1. 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

8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
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	1	Expuneri la tablă, exerciții demonstrative, discuții și explicații suplimentare legate de temele de proiect	
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	1		
Penetrarea sistemelor/serviciilor cu vulnerabilități de corupere a memoriei	1		
Tehnici și unelte de exploatare: framework-ul *Metasploit*. Cod de acces (*Shellcode*): generare și modificare. Unelte de generare și	1		

depanare			
Vulnerabilități ale aplicațiilor Web și metode de penetrare: LFI, RFI, XSS, CSRF, traversare directoare, injecție de cod SQL etc.	1		
Metode de obținere de privilegii sporite	1		
Metode și unelte de creare de tunele de acces (*tunneling*)	1		

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

1. 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

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

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

Se realizează prin discuții periodice cu reprezentanți ai angajatorilor semnificativi, în special cei care angajează pe proiecte din domeniul securității informațiilor.
Cursuri din 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	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 practic de penetrare și scrierea unui raport de evaluare și penetrare și/sau examen scris și/sau tip grilă (pe platforma Moodle) și/sau prezentarea unei teme de cercetare din domeniul cursului. In situații excepționale, care necesită desfășurarea activităților didactice de la distanță, examinarea poate avea loc online, de la distanță, folosind platformele Moodle și Teams.	50%
Seminar			
Laborator			
Proiect	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. In situații excepționale, care necesită desfășurarea activităților didactice de la	50%

		distanță, examinarea poate avea loc online, de la distanță, folosind platformele Moodle și Teams.	

Standard minim de performanţă

Curs. Prezența la **minim 50%** din orele de curs, pentru admiterea la examenul final. 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. Prezența la **obligatorie 100%** (o oră de proiect se poate recupera în timpul semestrului, iar alta în sesiunile de restanțe) pentru admiterea la examenul final. 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.

Data completării:	**Titulari**	**Titlu Prenume NUME**	**Semnătura**
	Curs	Drd. Ing. Radu Portase	
	Aplicații	Inf. Mihai Topan	

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