MD-2068, CHIŞINĂU, STR. STUDENŢILOR, 9/7, TEL: 022 50-99-63, www.utm.md

TESTE DE PENETRARE ŞI SISTEME DE EXPLOATARE

1. Date despre disciplină/modul

Facultatea	Calculatoare, Informatică şi Microelectronică				
Departamentul	Inginerie Software şi Automatică				
Ciclul de studii	Ciclul II, Studii superioare de master				
Programul de studii	Securitate informațională				
Anul de studii	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opţionalitate**	**Credite ECTS**
Anul I *(învățământ cu frecvenţă)*	I	PA	S – uniate de curs de specialitate	O - unitate de curs obligatorie	5

2. Timpul total estimat

Total ore în planul de învățământ		**Din care**		
		Ore auditoriale	**Lucrul individual**	
		Proiect	**Studiul materialului teoretic**	**Pregătire aplicații**
Învățământ cu frecvență	**150**	40	70	40

3. Precondiții de acces la disciplină/modul

Conform planului de învățământ	Pentru a atinge obiectivele cursului masteranzii trebuie să posede abilități de analiză și testare a soluțiilor informaționale. Aceste competențe sunt formate de următoarele unitățile de curs: Managementul și auditul securității informaționale, Bazele securității informaționale, Securitatea rețelelor de comunicații, Ingineria inversă, Programe malițioase și antivirus
Conform competențelor	Explicarea metodelor inginerești și științifice privind analiza și identificarea breșelor de securitate informațională a întreprinderii

4. Condiții de desfășurare a procesului educațional pentru

Proiect	Se va realiza proiectul conform condițiilor impuse. La consultațiile stabilite se vor prezenta rezultatele fiecărei etape de realizare a proiectului.

5. Competențe specifice acumulate

Competențe profesionale	**C1 Operarea cu concepte și metode științifice în domeniul Securității informaționale** C1.1 Identificarea și definirea conceptelor, teoriilor și metodelor de planificare a testelor de penetrare C1.2 Explicarea fazelor de penetrare prin utilizarea tehnicilor, conceptelor și principiilor științifice C1.3 Rezolvarea problemelor din domenii de activitate umană prin aplicarea în special al tehnicilor și metodelor de penetrare C1.5 Modelarea unor probleme de securitate folosind metodele de cercetare științifică **C2 Cercetarea științifica privind aspectele organizaționale și informaționale ale securității** C2.1 Identificarea și definirea conceptelor, teoriilor și metodelor folosite în realizarea de *analize focusate pe protecția oamenilor și informației* privind sistemele ce operează la nivel de organizații C2.2 Explicarea conceptelor și metodelor folosite în realizarea de analize privind sistemele de management și de securitate ce operează la nivel de organizații C2.3 Obținere autorizației pentru efectuarea testului de penetrare din partea posesorului sistemului informațional. Argumentarea necesității unui test de penetrare destinat posesorului sistemului informațional C2.5 Elaborarea unui proiect (specificație de sistem) în condițiile existenței unui sistem de securitate. **C3 Modelarea sistemelor complexe de securitate și implementarea lor prin sisteme informatice** C3.1 Efectuarea scanării de porturi și identificării serviciilor disponibile. Identificarea aplicațiilor accesibile din cadrul sistemului informațional. Descoperirea topologiei infrastructurii scanate și prezentare acesteia în formă de schemă C3.2 Explicarea tehnologiilor potrivite pentru realizarea sistemelor de securitate necesare în activitățile organizațiilor C3.3 Utilizarea tehnologiilor moderne în definirea soluțiilor de securitate C3.5 Dezvoltarea măsurilor de control și securitate utilizând tehnologii moderne de transmitere, stocare și procesare date în corespundere cu necesitățile unei organizații

	C4 Cercetarea științifica privind metodele și tehnologiile de dezvoltare a soluțiilor de securitate C4.1 Identificarea și definirea conceptelor și metodelor focusate pe procesul de dezvoltare, implementare și utilizare a soluțiilor de securitate C4.2 Identificare metodelor de exploatare potrivite pentru vulnerabilitățile identificare din cadrul sistemului informațional supus testării de penetrare. Aplicarea exploit-urilor identificate în baza impactul acestora asupra sistemului vulnerabil C4.3 Aplicarea limbajelor de programare, a mediilor de modelare și dezvoltare, a metodologiilor pentru crearea de sistemelor de securitate C4.4 Utilizarea de criterii și metode de evaluare a procesului de elaborare a sistemelor de securitate din punct de vedere a calității și performanțelor **C5 Managementul sistemelor de securitate în concordanța cu cerințele pieței** C5.1 Identificarea și definirea de componente arhitecturale hardware, software și de comunicații, precum și celor necesare la descrierea obiectivelor sistemului de management al SI C5.2 Explicarea interacțiunii și funcționării componentelor arhitecturale și de infrastructură specifice domeniului securității C5.4 Pregătirea conținutului în baza unei structuri predefinite. Includerea descrierii lucrărilor efectuate în urma fiecărei etape a testului de penetrare.
Competențe transversale	CT1. Aplicarea principiilor, normelor și valorilor eticii profesionale CT3. Demonstrarea spiritului de inițiativă și acțiune pentru actualizarea propriilor cunoștințe profesionale, economice și de cultura organizațională CT2. Identificarea, descrierea și derularea activităților organizate într-o echipă cu dezvoltarea capacităților de comunicare și colaborare, dar și cu asumarea diferitelor roluri (de execuție și conducere).

6. Obiectivele disciplinei/modulului

Obiectivul general	Să documenteze procesele de analiză și de identificare a vulnerabilităților și amenințărilor de securitate.
Obiectivele specifice	Să achiziționeze un set de cunoștințe și abilități practice necesare pentru realizarea testelor de penetrare. Să aplice metodele și instrumentele necesare la realizarea testelor de penetrare

7. Conținutul disciplinei/modulului

Tematica activităților didactice	Numărul de ore
	învățământ cu frecvență
T1. Tipuri de teste de penetrare. Identificare sistemului informațional ce va fi supus testului de penetrare și definirea tipului de testare Obținere autorizației pentru efectuarea testului de penetrare din partea posesorului sistemului informațional. Argumentarea necesității unui test de penetrare destinat posesorului sistemului informațional.	**5**
T2. Fazele unui test de penetrare. Planificarea unui test de penetrare Definirea diapazoanelor de IP adrese externe și interne ce urmează a fi supuse testului de penetrare	**5**
T3. Colectarea informației despre sistemul informațional Efectuarea scanării de porturi și identificării serviciilor disponibile. Identificarea aplicațiilor accesibile din cadrul sistemului informațional. Descoperirea topologiei infrastructurii scanate și prezentare acesteia în formă de schemă	**5**
T4. Identificarea vulnerabilităților la nivel de sisteme și infrastructură Să se obțină informația necesară despre vulnerabilitățile sistemelor de operare și a serviciilor aferente în baza versiunii detectate	**5**
T5. Identificarea vulnerabilităților la nivel de aplicații Testarea aplicațiilor identificate în baza metodologiei Top 10 OWASP	**4**
T6. Exploatare vulnerabilităților. Tehnici de exploatare Identificare metodelor de exploatare potrivite pentru vulnerabilitățile identificare din cadrul sistemului informațional supus testării de penetrare. Aplicarea exploit-urilor identificate în baza impactul acestora asupra sistemului vulnerabil	**4**
T7. Tehnici de post-exploatare Obținerea accesului privilegiat. Extragerea informației sensibile din cadrul sistemelor exploatate. Efectuarea atacurilor pivotate de pe sistemele exploatate	**4**
T8. Clasificarea vulnerabilităților identificate Calcularea riscului vulnerabilităților depistate. Identificare metodelor de remediere a vulnerabilităților depistate	**4**

Tematica activităților didactice	Numărul de ore învățământ cu frecvență
T9. Raportul testului de penetrare Lucrul asupra raportului final. Pregătirea conținutului în baza unei structuri predefinite. Includerea descrierii lucrărilor efectuate în urma fiecărei etape a testului de penetrare. Elaborarea concluziilor finale și a recomandărilor necesare	**4**
Total:	**40**
Tematica lucrărilor practice	

8. Referințe bibliografice

Principale	1. Mark Stamp, *Information security. Principles and Practice,* Second Edition, SanJose State University, AJOHN WILEY&SONS, USA, 2011. - 608 p. 2. Aurel Şerb, Constantin Baron, Narcisa Isăilă, *Securitatea informatică în societatea informaţională*, Bucureşti : Pro Universitaria, 2013. – 546 p. 3. Dumitru Oprea, *Protecţia şi securitatea informaţiilor*. Ed. II, Polirom, Iaşi, 2007. – 445 p. 4. Popa Sorin Eugen, Securitatea sistemelor informatice, Bacău, 2007. – 136 p. 5. Ion I. Bucur, *Tehnologii, structuri și managementul rețelelor de calculatoare,* - resursă electronică. 6. Al. Astahov, *Искусство управления информационными рисками*, ДМК, Москва, 2010. – 316 p. 7. Nicolas Mayer, *Model-based Management of Information System Security Risk*, Namur, Belgium, 2009. – 295 p. 8. M.E. Whitman, H.J.Mattord, *Management of Information Security*, 3rd Edition, Course Technology, 2010. 9. A.Calder, S.Watkins, *A Manager's Guide to Data Security and ISO 27001/ISO27002*, 4th Edition, Kogan Page, 2008. D.Landool, *The Security Risk Assessment Handbook*, Auerbach Publications, 2006.
Suplimentare	1. NIST, NIST 800-30 Risc Management Guide for Information Technology Systems, http://www.csrc.nist.gov/publications 2. OECD, *Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July2002.* www.oecd.org 3. http://www.isaca.org/cobit/ 4. HOTĂRÎRE GUVERN Nr. 201 din 28.03.2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică. Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, aprobat prin Hotărîrea Guvernului nr. 811 din 29 octombrie 2015.

9. Utilizarea IA generativă

Permisiunea de utilizare	Utilizarea IA generative în cadrul temelor și proiectelor este permisă, cu condiția ca studenții să respecte următoarele reguli: • IA generativă poate fi utilizată pentru generarea de idei, structuri de text sau cod, dar toate materialele generate trebuie să fie revizuite și ajustate de către student pentru a se asigura că acestea corespund cerințelor academice. • Orice utilizare a IA generative trebuie să fie declarată în secțiunea de apendice a fiecărei lucrări, folosind fraza: "În timpul pregătirii acestei lucrări, autorul a utilizat [NUME INSTRUMENT / SERVICIU] în scopul [MOTIV]. După utilizarea acestui instrument/serviciu, autorul a revizuit și editat conținutul după cum a fost necesar și își asumă întreaga responsabilitate pentru conținutul lucrării."
Restricții de utilizare	Studenții nu trebuie să considere IA generativă ca o sursă de încredere pentru informații, deoarece nu oferă referințe clare sau surse documentate. • Nu este permisă citarea directă a conținutului generat de IA în lucrările academice ca și cum ar fi sursă primară. • Activitățile în care este interzis utilizarea IA generativă sunt specificare de profesor și sunt de regulă evaluări intermediare și finale sau care nu presupun activități de dezvoltare a competențîlor profesionale.

10. Evaluare

Periodică și curentă		Evaluarea finală
Evaluare 1	**Evaluare 2**	
30%	30%	40%
Standard minim de performanță: definirea unei probleme a unui grup social și descrierea în ansamblu a soluției/soluțiilor utilizând tehnologia informației și comunicației.		
Prezența și activitatea la seminarele/atelierele de lucru; *Obținerea notei „5” la fiecare dintre evaluări;* *Obținerea notei „5” la lucrarea de examinare finale;* Evaluarea curentă, fiind de tip formativ și oferind studenților/echipei un feedback continuu la activitățile de proiectare sau modulele integrate, asigură evaluarea studentului cu nota echipei de lucru. Examenul final, fiind o evaluare sumativă, se realizează oral în baza proiectului prezentat public de echipă și discuții/interviuri individuale (în prezența echipei sau nu). Aprecierile obținute la examinare sunt individuale și constituie 40% din nota finală.		

11. Criterii de evaluare

Activitate	Componente evaluare	Metodă de evaluare, criterii de evaluare	Pondere în nota finală a activității	Ponderea în evaluarea disciplinei
Evaluare I	Prezența și participarea la seminare	Observație directă, fișă de prezență	50%	**30 %**
	Calitatea lucrărilor realizate în timpul atelierelor	Analiză practică, punctaj pentru fiecare sarcină rezolvată	50%	
Evaluare II	Prezentarea unei soluții funcționale	Evaluare practică, demonstrarea funcționalității soluției propuse	70%	**30 %**
	Colaborarea în echipă și respectarea termenelor	Feedback de la colegi și observațiile coordonatorului	30%	
Evaluarea finală	Prezentarea publică a proiectului final	Examinare orală, claritatea expunerii, justificarea deciziilor	60%	**40%**
	Documentația proiectului (conținut, structură, claritate)	Analiza documentației conform criteriilor predefinite	40%	