MD-2045, CHIŞINĂU, STR. Studenţilor 9/7, TEL: 022 509-908, www.utm.md

TESTE DE PENETRARE ȘI SISTEME DE EXPLOATARE

1. Date despre unitatea de curs/modul

Facultatea	Calculatoare, Informatică și Microelectronică				
Catedra/departamentul	Ingineria Software şi Automatică				
Ciclul de studii	Studii superioare de master, ciclul II				
Programul de studii	Securitate Informaţională				
Anul de studii	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opţionalitate**	**Credite ECTS**
I (învăţământ cu frecvenţă);	1	PA	S – unitate de curs specialitate	O - unitate de curs obligatorie	5

2. Timpul total estimat

Total ore în planul de învăţământ	**Din care**		
	Lucrul individual		
	Proiect de an	**Studiul materialului teoretic**	**Pregătire aplicaţii**
150	75	45	30

3. Precondiţii de acces la unitatea de curs/modul

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

4. Condiţii de desfăşurare a procesului educaţional

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

5. Competenţe specifice acumulate

Competenţe profesionale	**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.

6. Obiectivele unităţii de curs/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 intrumentele necesare la realizarea testelor de penetrare

7. Conţinutul unităţii de curs/modulului

Tematica activităților practice pentru realizarea Proiectului
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.
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
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
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
Identificarea vulnerabilităților la nivel de aplicații Testarea aplicațiilor identificate în baza metodologiei Top 10 OWASP
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
Tehnici de post-exploatare Obținerea accesului privilegiat. Extragerea informației sensibile din cadrul sistemelor exploatate. Efectuarea atacurilor pivotate de pe sistemele explotate
Clasificarea vulnerabilităților identificate Calcularea riscului vulnerabilităților depistate. Identificare metodelor de remediere a vulnerabilităților depistate
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

8. Referinţe 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. 10. 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. 5. Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, aprobat prin Hotărîrea Guvernului nr. 811 din 29 octombrie 2015.

9. Evaluare

Periodică		**Curentă**	**Studiu individual**	**Proiect/teză**	**Examen**
EP 1	**EP 2**				
-	-	-	-	100%	-
Standard minim de performanţă Prezentarea realizării sarcinilor de realizare a proiectului. Obținerea notei minime de „5”					

10. Criterii de evaluare

Activitate	**Componente evaluare**	**Metodă de eevaluare, Criterii de evaluare**	**Pondere în nota finală a activității**	**Ponderea în evaluarea disciplinei**
Proiect/Lucare de an	O tematică la alegere	Prezentare/discurs public	100%	**100%**