UNIVERSITATEA „LUCIAN BLAGA” DIN SIBIU
FACULTATEA DE ŞTIINȚE
CATEDRA DE INFORMATICĂ
Domeniul de studii de master: INFORMATICĂ
Specializarea: SISTEME ŞI TEHNOLOGII INFORMATICE AVANSATE

FIŞĂ DISCIPLINĂ

Denumirea disciplinei: Administrarea şi securitatea rețelelor de calculatoare
Codul disciplinei:
Anul de studiu şi semestrul în care se studiază disciplina: anul II/ semestrul I
Discipline anterioare cerute *:
Regimul disciplinei (obligatorie O, opțională A sau facultativă L): O
Categoria formativă (Cunoaştere aprofundată CA, Complementară CO, Cercetare CC): CA
Forma de evaluare (examen E, verificare V, colocviu C): E
Catedra care coordonează disciplina: Catedra Informatică
Titularul / titularii disciplinei: Lector.univ.dr. Florin Stoica

* disciplinele studiate anterior a căror cunoaştere este necesară pentru însuşirea disciplinei

Extinderea disciplinei în planul de învățământ *:				
Curs	Seminar	Laborator	Proiect	Total ($NOAD_{sem}$)
28		28		56

* numărul semestrial de ore de activități didactice directe

Obiectivele disciplinei
Obiectivele cursului Însuşirea terminologiei şi conceptelor de bază din domeniul securității, a celor mai folosite tehnici de atac şi mecanismele de protecție. Însuşirea conceptelor criptografiei moderne şi aplicarea acestora în securizarea sistemelor.
Obiectivele activităților aplicative (seminar, laborator, proiect) Dobândirea cunoştințelor şi aptitudinilor pentru rezolvarea de probleme practice din domeniul securizării rețelelor de calculatoare precum: configurare firewall-uri, protocoale de tunelare şi VPN, Ipsec, implementare algoritmi criptografici, detectarea şi evaluarea problemelor de securitate ce vizează aplicații/sisteme distribuite.

Conținutul disciplinei (capitolele cursului / tematica seminarului / lucrărilor practice / etapele proiectului)		
CURS		
Nr. crt.	**Tema**	**Nr.ore**

1	Introducere în securitatea sistemelor de calcul. Concepte de bază, modele de amenințare, scopuri de securitate.	2
2	Criptografie şi protocoale criptografice: codificare, autentificare, coduri de autentificarea mersajelor, funcții hash, funcții one-way, criptografie cu cheie publică, canale sigure, protocoale criptografice şi integrarea lor în sisteme distribuite, alte aplicații. Algoritmi pentru Semnături Digitale.	4
3	Securitate software. Secure software engineering, programare defensivă, buffer overrun şi alte probleme de implementare. Securitate legată de limbaje: analiza codului pentru detectarea erorilor de securitate, limbaje sigure, tehnici sandboxing.	4
4	Securitatea sistemelor de operare. Protecția memoriei, controlul accesului, autorizare, autentificarea utilizatorilor, asigurarea securității, evaluarea securității, drepturi digitale, etc.	2
5	Securitatea rețelelor. Firewall, sisteme de detectarea intruşilor, atacuri DoS şi apărare. Studii de caz: DNS, IPSec. Malicious code analysis şi apărare. Viermi, spzware, rootkit, botnet, etc. Securitate Web.	4
6	Retele Virtual Private VPN: Arhitecturi si tehnologii. Tunele IP-IP. Configurarea tunelelor IP-IP.	4
7	Protocolul IPSsec. IPSec in mod transport . IPSec in mod Tunel. Aplicatii la retele Linux-Windows.	4
8	Securitate la nivle IP: firewall-uri Linux, Windows, arhitectura, iptables. Configurarea unui firewall Linux. Arhitectura Firewall Windows XP, Windows 7, Windows 2008 Server	4
SEMINAR / LABORATOR / PROIECT		
Nr. crt.	**Tema**	**Nr.ore**
1	Algoritmi pentru Semnături Digitale	4
2	Scanarea in retea, interceptarea pachetelor in retea	2
3	Configurare firewall Linux. Firewall Windows XP/7, Windows 2008 Server	4
4	Exemple de probleme de securitate in software: validarea defectuoasa a intrarilor, programe setuid, greseli de configurare, limbaje macro, buguri	4
5	Unelte necesare pentru scrierea codului robust, buffer overflow si alte probleme de programare frecvente: exploatare si protectie	2
6	Folosirea uneltelor software criptografice (functii hash, openssl), exercitii de criptare/decriptare a unor mesaje	4
7	Detectarea problemelor de securitate pentru un site web prezentat, elaborarea unui raport asupra problemelor detectate	4

8	Proiectarea unei arhitecturi de Denial of Service controlabilă remote, simularea atacului asupra unui server ruland un serviciu configurat, restrangerea efectelor unui atac DOS.	2
9	Prezentare proiect	2

Descrierea metodelor de predare
La curs se va folosi expunerea, explicatia, exemplificarea si conversatia frontala. La laborator se va folosi explicatia, exemplificarea, invatarea prin descoperire. Pentru curs si laborator exista suport electronic care se da studentilor la inceputul cursului. La curs se vor folosi si slide-uri si exemplificare pe calculator.

Descrierea formelor şi metodelor de evaluare a cunoştinţelor
Evaluarea cunostintelor se va face continuu in cadrul lucrarilor de laborator, fiind urmarita si evaluata activitatea studentilor la fiecare laborator. Nota finala este formata din a) Media notelor acordate pentru activitatea la laborator 10% b) Nota proiect laborator 40% c) Nota de la examenul scris 50%

Bugetul de timp pentru studiul individual			
Denumirea activităţii	Nr. ore	Denumirea activităţii	Nr. ore
1. Descifrarea şi studierea notiţelor de curs	40	6. Elaborarea temelor de casă, referatelor …	48
2. Studiul după manual sau suport de curs		7. Pregătirea pentru evaluările periodice	
3. Studierea bibliografiei minimale indicate	20	8. Pregătirea pentru examinarea finală	20
4. Documentarea suplimentară *		9. Participarea la consultaţii	
5. Pregătirea seminariilor şi/sau laboratoarelor	40	10. Alte activităţi …	
Numărul total al orelor alocate studiului individual $NOSI_{sem}$			168

* în bibliotecă, pe INTERNET, pe teren …

Bugetul de timp şi creditele alocate disciplinei			
$NOAD_{sem}$	$NOSI_{sem}$	$NOT_{sem} = NOAD_{sem} + NOSI_{sem}$	**Numărul de credite**
56	168	224	8

Criteriile de evaluare a cunoştinţelor şi promovarea disciplinei	
Evaluările considerate pentru stabilirea notei finale:	**Ponderea evaluării în nota finală, %**
• Media notelor acordate la seminar	
• Media notelor acordate pentru activitatea la laborator	10
• Notele obţinute la testele periodice sau parţiale	40 (nota pe activitatea de proiect)
• Nota acordată pentru frecvenţa la curs	
• Notele acordate pentru temele de casă, referate, eseuri, traduceri, studii de caz …	
• Notele acordate pentru participarea la cercuri ştiinţifice şi/sau la concursuri profesiobnale	
• Nota acordată la examinarea finală	50
• Alte note	

Modalitatea de examinare finală *:
Lucrare scrisă cu subiecte teoretice şi aplicaţii

* lucrare scrisă descriptivă, lucrare scrisă cu subiecte teoretice şi aplicaţii, test grilă, examinare orală cu bilete …

Competențele specifice disciplinei *	
1. Competențe privind cunoaşterea şi înțelegerea:	●Cunoaşterea şi utilizarea adecvată a conceptelor fundamentale legate de securitatea sistemelor, algoritmi criptografici, protocoale securizate
2. Competențe în domeniul explicării şi interpretării:	●Capacitatea de a explica modul de dezvoltare a aplicațiilor securizate şi de evaluare a securității sistemelor ●Capacitatea de a interpreta rezultatele obtinute
3. Competențe instrumental - aplicative:	●Capacitatea de a utiliza unelte software criptografice ●Capacitatea de a proiecta şi realiza aplicații complexe care utilizeaza cod robust, securizat ●Capacitatea de a detecta probleme de securitate
4. Competențe atitudinale	Dezvoltarea atitudinii pozitive față de muncă şi responsabilitate pentru propria pregătire profesională Dezvoltarea spiritului de munca in echipa

- competențele generale sunt menționate în Fişa specializării

Bibliografie minimală:

1. Rescorla, Eric. SSL and TLS: Designing and Building Secure Systems. Reading, MA: Addison-Wesley, 2000. ISBN: 0201615983
2. Kaufman, Charlie, Radia Perlman, and Mike Speciner. Network Security: Private Communication in a Public World. 2nd ed. Upper Saddle River, NJ: Prentice Hall, 2002. ISBN: 0130460192
3. Smart, N. Cryptography: An Introduction. McGraw-Hill, 2002. ISBN: 0077099877

Data elaborării:
16.02.2010

Titularul / titularii disciplinei
lect. dr. Florin Stoica