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 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 învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	12.00

2. Date despre disciplină

2.1 Denumirea disciplinei	***Elemente de securitate în configurarea sistemelor de calcul și a rețelelor de calculatoare***				
2.2 Titularii de curs	Conf. dr. ing. Cebuc Emil - emil.cebuc@cs.utcluj.ro				
2.3 Titularul / Titularii activităţilor de seminar / laborator / proiect	Conf. dr. ing. Iancu Bogdan - bogdan.iancu@cs.utcluj.ro				
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*				DA
	DI – Impusă, DOp – opțională, DFac – facultativă				DI

3. Timpul total estimat

3.1 Număr de ore pe săptămână	4	din care:	Curs	2	Seminar		Laborator	2	Proiect	
3.2 Număr de ore pe semestru	56	din care:	Curs	28	Seminar		Laborator	28	Proiect	
3.3 Distribuţia fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie şi notiţe										25
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren										20
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri										22
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activităţi:										0
3.4 Total ore studiu individual (suma (3.3(a)...3.3(f)))										69
3.5 Total ore pe semestru (3.2+3.4)										125
3.6 Numărul de credite										5

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Rețele de calculatoare, Arhitectura calculatoarelor
4.2 de competenţe	Rețele de calculatoare, Arhitectura calculatoarelor

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Prezență la laborator obligatorie 100% pentru admiterea la examenul final

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 • **C1.1** - 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
6.2 Competenţe transversale	N/A

7. Obiectivele disciplinei

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. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Recapitularea cunoștințelor de bază de rețele de calculatoare (LAN, VLAN, WAN, IPv4/v6, TCP/IP, subnets, switch, router, OSI layers)	2		
Securitatea echipamentelor de rețea (Routere și switch-uri; console, telnet, SSH, local usernames & passwords, AAA, Port ecurity)	2		
Implementare Virtual LANs. Aspecte de securitate	2		
Rețele Virtuale Private (VPNs). Conexiuni remote și securitatea lor	2		
Monitorizarea, logarea și auditul activităților și traficului de rețea	2		
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)	2		
Soluții de virtualizare (VMware vSphere, Microsoft Hyper-V). Instalare, roluri și caracteristici, aspecte de securitate	2		
Windows Server 2012 R2 – Instalare si administrare Active Directory, DNS si DHCP server (Gestionarea utilizatorilor, grupurilor si a calculatoarelor din domeniu. Politici de domeniu)	2		
Windows Server 2012 R2 – Auditare fișiere și autentificare. Backup și Restore pentru Active Directory	2		
Windows Server Update Services – Instalare si configurare. Managementul update-urilor si a patch-urilor sistemelor de calcul	2		
Centos 7 Server – Instalare si configurare. Apache si FTP server	2		
Centos 7 Server – Roluri de Router și Firewall	2		
Alte teme importante de actualitate, noutăți legate de securitatea rețelelor	2		
Recapitulare	2		

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

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)

8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Recapitularea cunoștințelor de bază de rețele de calculatoare: IPv4, IPv6, DHCP, NAT/PAT, Wireshark	2		
Securitate, autentificare si monitorizare: telnet, SSH, local usernames & passwords, AAA, Port Security, 802.1x	2		
Implementare Virtual LANs si securizarea lor	2		
Implementarea funcțiilor de firewall și IPS la nivelul echipamentelor de rețea: liste de acces (IPv4, IPv6 ACLs), VPN	2		
Securitate, autentificare si monitorizare: SNMP, Syslog, NetFlow	2		
Securitate, autentificare si monitorizare: Network inspection tools	2		
Soluții de virtualizare. Microsoft Hyper-V: Instalare, roluri și caracteristici	2		

Soluții de virtualizare. Microsoft Hyper-V: aspecte de securitate	2		
Windows Server 2012 R2: Instalare si administrare Active Directory, DNS si DHCP server	2		
Windows Server 2012 R2: Backup și restore pentru Active Directory, auditare fișiere și autentificare, Windows Server Update Services (WSUS)	2		
Centos 7 Server: Instalare si configurare SO si servicii	2		
Centos 7 Server: Roluri de router și firewall	2		
Securitatea în rețele wireless LAN si mobile	2		
Test de laborator	2		

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 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)

**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 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	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 scris și/sau tip grilă și/sau prezentarea unei teme de cercetare din domeniul cursului onsite.	50%
Seminar	-	-	-
Laborator	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 onsite.	50%
Proiect	-	-	-

Standard minim de performanţă:

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.

Data completării: 03.06.2024	**Titulari**	**Titlu Prenume NUME**	**Semnătura**
	Curs	Conf.dr.ing. Emil Cebuc	
	Aplicații	Conf.dr.ing. Bogdan Iancu	

Data avizării în Consiliul Departamentului Calculatoare 20.02.2024	Director Departament, Prof.dr.ing. Rodica Potolea
Data aprobării în Consiliul Facultății de Automatică și Calculatoare 22.02.2024	Decan, Prof.dr.ing. Mhaela Dînșoreanu