FIŞA DISCIPLINEI

1. Date despre program

Facultatea	Inginerie Electrică și Știința Calculatoarelor
Departamentul	Calculatoare
Domeniul de studii	Calculatoare și tehnologia informației
Ciclul de studii	Masterat
Programul de studii	Știința și ingineria calculatoarelor

2. Date despre disciplină

Denumirea disciplinei	**REȚELE DE CALCULATOARE - ARHITECTURI AVANSATE ȘI SECURITATE**					
Anul de studiu	I	Semestrul	1	Tipul de evaluare	E	
Regimul disciplinei	Categoria formativă a disciplinei DF - fundamentală, DS - de specializare, DC – complementară					DF
	Categoria de opționalitate a disciplinei: DOB – obligatorie, DOP – opțională, DFA - facultativă					DOB

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore, pe săptămână	3	Curs	1	Seminar		Laborator/lucrări practice	2	Proiect	
I b) Totalul de ore (pe semestru) din planul de învăţământ	42	Curs	14	Seminar		Laborator/lucrări practice	28	Proiect	

Distribuția fondului de timp pe semestru	ore
II. Studiu individual	155
III. Examinări	3
IV. Alte activități (precizați):	

Total ore studiu individual (II+III)	158
Total ore pe semestru (I.b+II+III+IV)	200
Numărul de credite	8

4. Competențe specifice acumulate

Competențe transversale	CT1. Lucrează în echipe
Competențe profesionale	CP1. Efectuează cercetare științifică CP4. Concepe designul produsului CP5. Asigură managementul de proiect CP6. Aplică politici de securitate informatică CP9. Proiectează hardware CP10. Testează hardware CP12. Modelează și simulează hardware

5. Rezultatele învățării

Cunoștințe	Aptitudini	Responsabilitate și autonomie
Studentul/absolventul identifică, descrie critic, sintetizează și utilizează, ca bază pentru cercetarea originală, concepte și metode avansate privind arhitecturile și protocoalele rețelelor de calculatoare.	Studentul/absolventul cercetează, dezvoltă noi cunoștințe și proceduri privind conceperea și evaluarea arhitecturilor de rețele avansate, proiectând și implementând soluții eficiente pentru sisteme distribuite și securizate.	Studentul/absolventul poate desfășura în condiții de autonomie activități care implică inovație tehnologică, cercetare științifică și comunicare tehnică în știința și ingineria calculatoarelor.

6. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

Obiectivul general al disciplinei	● Formarea competențelor avansate de proiectare, analiză și protejare a infrastructurilor de rețea, prin înțelegerea arhitecturilor moderne (rețele wireless, rețele 4G/5G și mecanisme de mobilitate) și aplicarea metodologiilor și instrumentelor specifice de securitate (TLS, IPsec, DNSSEC, firewall/IDS), astfel încât studenții să poată diagnostica și mitiga riscuri în scenarii reale, cu respectarea normelor etice și legale.
	● Dezvoltarea competențelor operaționale de analiză, configurare, testare și securizare a rețelelor de calculatoare, prin utilizarea unor medii izolate și reproductibile. Activitățile practice urmăresc analiza traficului, investigarea controlată a vulnerabilităților specifice protocoalelor și serviciilor de rețea și evaluarea mecanismelor de protecție și control.

7. Conținutul predării și învățării

Curs	Nr. ore	Metode de predare	Observații
● Introducere ● Recapitulare - stiva de protocoale TCP/IP	2	expunerea, prelegerea-dezbaterea	
● Rețele mobile și wireless o Wireless Caracteristicile legăturilor și rețelelor wireless Wi-Fi: rețele locale fără fir IEEE 802.11 Rețele celulare (telefonie mobilă): 4G și 5G	2	expunerea, prelegerea-dezbaterea	
o Mobilitate Managementul mobilității: principii Managementul mobilității: în practică Rețele 4G/5G Mobile IP Mobilitate: impact asupra protocoalelor de nivel superior	2	expunerea, prelegerea-dezbaterea	
● Securitatea rețelelor de calculatoare o Ce reprezintă securitatea rețelelor? o Principiile criptografiei o Integritatea mesajului, autentificare	4	expunerea, prelegerea-dezbaterea	
o Securizarea e-mailului o Securizarea conexiunilor TCP: TLS o Securitate la nivelul rețea: Ipsec o Securitate în rețelele wireless și mobile o Securitate operațională: firewall-uri și IDS	4	expunerea, prelegerea-dezbaterea	

Bibliografie minimală recomandată

1. J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 9th ed. Boston, MA, USA: Pearson, **2025**.
2. J. Henry, B. Gupta, B. Hart, and M. Smith, *Wi-Fi 7 In Depth: Your Guide to Mastering Wi-Fi 7, the 802.11be Protocol, and Their Deployment*. Boston, MA, USA: Addison-Wesley Professional, **2024**.
3. G. Cheng, Z. Qian, Y. Jiang, Z. Yang, and T. Rajamanickam, *Wi-Fi 7: Principles, Technology, and Applications*. Singapore: Springer, **2024**.
4. E. Dahlman, S. Parkvall, and J. Skold, *5G/5G-Advanced: The New Generation Wireless Access Technology*, 3rd ed. Cambridge, MA, USA: Academic Press (Elsevier), **2023**.
5. C. Cox, *An Introduction to 5G: The New Radio, 5G Network, 5G Advanced and Beyond*, 2nd ed. Hoboken, NJ, USA: Wiley, **2025**.
6. R. Johnson, *QUIC Protocol Design and Implementation: Definitive Reference for Developers and Engineers*. San Jose, CA, USA: HiTeX Press, **2025**.
7. A. Yarali, *From 5G to 6G: Technologies, Architecture, AI, and Security*. Hoboken, NJ, USA: Wiley–IEEE Press, **2023**.
8. X. Wang and R. Lu, Eds., *5G Wireless Network Security and Privacy*. Hoboken, NJ, USA: Wiley, **2023**.
9. H. Yao, C. Zheng, X. Fu, Y. Yang, and I. Ungurean, "Charger and receiver deployment with delay constraint in mobile wireless rechargeable sensor networks," *Ad Hoc Networks*, vol. 126, p. 102756, **2022**, doi: 10.1016/j.adhoc.2021.102756.
10. H. Yao, Q. Zhang, X. Fu, Y. Yang, and I. Ungurean, "Charger and receiver deployment for trajectory coverage with delay constraint in mobile wireless rechargeable sensor networks," *Ad Hoc Networks*, vol. 149, p. 103237, Oct. **2023**, doi: 10.1016/j.adhoc.2023.103237

Aplicații (laborator)	Nr. ore	Metode de predare	Observații
● Sniffing-ul (interceptarea) și spoofing-ul (falsificarea) pachetelor folosind biblioteca Scapy (Python)	2	Lucrări practice, experiment	Lucrările de laborator se desfășoară într-un mediu virtualizat Ubuntu (Oracle VM VirtualBox), iar scenariile de atac și vulnerabilitățile sunt experimentate în condiții controlate și izolate, utilizând containere Docker.
● Analiza atacului ARP cache poisoning și a scenariului man-in-the-middle (MITM)	2	Lucrări practice, experiment	
● Redirecționare ICMP. Analiza unui atac man-in-the-middle (MITM) bazat pe redirecționare ICMP	2	Lucrări practice, experiment	
● Vulnerabilitățile protocolului TCP. TCP SYN flood, TCP reset, deturnarea unei sesiuni TCP, reverse shell	2	Lucrări practice, experiment	
● Vulnerabilitățile protocolului TCP. Atacul Mitnick	2	Lucrări practice, experiment	
● Protocolul DNS. Atacul de otrăvire a cache-ului DNS. Falsificarea răspunsurilor DNS	2	Lucrări practice, experiment	
● Protocolul DNS. Atacul Kaminsky	2	Lucrări practice, experiment	
● Protocolul DNS. Atacul DNS Rebinding. Atacuri asupra dispozitivelor IoT	2	Lucrări practice, experiment	
● Extensii de securitate DNS (DNSSEC)	2	Lucrări practice, experiment	
● Firewall in Linux. Netfilter și iptables	2	Lucrări practice, experiment	
● Analiza tehnicilor de traversare a mecanismelor de filtrare utilizând redirecționarea porturilor și tunelarea VPN	2	Lucrări practice, experiment	
● Vulnerabilitatea de depășire a memoriei tampon (buffer overflow) pe un server	2	Lucrări practice, experiment	
● Comportamentul de auto-duplicare și propagare al viermilor. Viermele Morris	4	Lucrări practice, experiment	

Bibliografie minimală recomandată

1. I. Ungurean, *Arhitecturi avansate de rețele de calculatoare – Îndrumar de laborator*. [Online]. Available: http://eed.usv.ro/~ioanu/AARC/, **2025**. (Acces pe bază de credențiale furnizate la laborator.)
2. W. Du, *Computer & Internet Security: A Hands-on Approach*, 3rd ed. Syracuse, NY, USA: Wenliang Du, **2022**. ISBN: 978-1-7330039-4-0
3. W. Du, *Computer Security: A Hands-on Approach (Computer & Internet Security)*, 3rd ed. Syracuse, NY, USA: Wenliang Du, **2022**. ISBN: 978-1-7330039-5-7
4. W. Du, *Internet Security: A Hands-on Approach (Computer & Internet Security)*, 3rd ed. Syracuse, NY, USA: Wenliang Du, **2022**. ISBN: 978-1-7330039-6-4
5. P. Biondi și comunitatea Scapy, *Scapy Documentation, Release 2.6.1*, 5 nov. **2024**. [Online]. Disponibil: https://scapy.readthedocs.io/
6. J.-P. Aumasson, *Serious Cryptography: A Practical Introduction to Modern Encryption*, 2nd ed. San Francisco, CA, USA: No Starch Press, **2024**
7. J. Seitz and T. Arnold, *Black Hat Python: Python Programming for Hackers and Pentesters*, 2nd ed. San Francisco, CA, USA: No Starch Press, **2021**
8. J. M. Ortega, *Python for Security and Networking: Leverage Python Modules and Tools in Securing Your Network and Applications*, 3rd ed. Birmingham, U.K.: Packt, **2023**
9. S. P. Kane și K. Matthias, *Docker: Up & Running: Shipping Reliable Containers in Production*, 3rd ed. Sebastopol, CA, USA: O'Reilly Media, **2023**

8. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Evaluare finală	Evaluarea nivelului de însușire și înțelegere a conceptelor, principiilor și metodelor specifice arhitecturilor avansate și securității rețelelor de calculatoare; capacitatea de a identifica, explica, analiza și corela mecanismele și protocoalele studiate; capacitatea de a argumenta alegerea unor soluții tehnice adecvate unor scenarii date.	Evaluare finală prin test-grilă online administrat prin intermediul platformei Moodle 3.	50%
Evaluare pe parcurs	Capacitatea de a configura, testa și analiza scenarii de rețea în medii controlate; utilizarea corectă a instrumentelor și metodelor specifice; interpretarea rezultatelor obținute și justificarea soluțiilor tehnice adoptate; desfășurarea autonomă și responsabilă a activităților practice; documentarea și prezentarea clară a rezultatelor obținute.	Evaluare continuă prin probe practice și metode orale, pe baza realizării, prezentării și verificării rezultatelor obținute la fiecare lucrare de laborator.	50%

Fișa disciplinei include, dacă este cazul, elemente adaptate persoanelor cu dizabilități, în funcție de tipul și gradul acestora.

Data completării	Grad didactic, nume, prenume, semnătura titularului de curs	Grad didactic, nume, prenume, semnătura titularului de aplicație
23.09.2026	conf. dr. ing. Ioan UNGUREAN	conf. dr. ing. Ioan UNGUREAN

Data avizării	Grad didactic, nume, prenume, semnătura responsabilului de program
24.09.2026	prof. dr. ing. Ștefan-Gheorghe PENTIUC

Data avizării în departament	Grad didactic, nume, prenume, semnătura directorului de departament
24.09.2026	Prof. dr. ing. Ovidiu-Andrei SCHIPOR

Data aprobării în consiliul facultății	Grad didactic, nume, prenume, semnătura decanului
25.09.2026	Prof. dr. ing. Laurențiu-Dan MILICI