Azərbaycan Respublikası Elm və Təhsil Nazirliyi
Lənkəran Dövlət Universiteti

"Təsdiq edirəm"
Tədris məsələləri üzrə prorektor v.i.e:
dos. Zaur Məmmədov
"07 " yanvar 2026-cı il

Fənn sillabusu
(işçi tədris proqramı)

İxtisasın şifri və adı: 6006017-İnformasiya təhlükəsizliyi
Fakultə: Aqrar və mühəndislik
Kafedra: Texnologiya və texniki elmlər

I. Fənn haqqında məlumat:
Fənnin adı: Nüfuzetmə sınaqlarının əsasları ("Nüfuzetmə sınaqlarının əsasları" işçi fənn proqramı,Lənkəran Dövlət Universitetinin Texnologiya və texniki elmlər kafedrasının 07.01.2026-cı il 5 №-li protokoluna əsasən)
Kodu: İPF-B20
Tədris ili: III tədris ili (2025/2026)
Semestr: VI (yaz)
Tədris yükü: 75 (45 saat mühazirə, 30 saat laboratoriya)
Təhsilalma forması: Əyani
Tədris dili: Azərbaycan dili
AKTS üzrə kredit: 8 kredit

II. Müəllim haqqında məlumat:
Soyadı,adı,ata adı,elmi dərəcəsi və elmi adı:
Mühazirə müəllimi: **Dəmirov Asəf Ağacəfər oğlu, t.ü.f.d.,dosent.**
Laboratoriya müəllimi:**Salmanlı Salman Əliqulu oğlu, müəllim.**
Kafedranın ünvanı: Lənkəran şəhəri Füzuli 170 a, LDU-nun 1 saylı tədris binası
Məsləhət saatı: V gün saat 12^{20} -13^{55} , V gün saat 12^{20} -13^{55}
E-mail ünvanı: asef.demirov@gmail.com, salmansalmanli654@gmail.com

III.Tövsiyyə olunan dərsliklər və dərs vəsaitləri:

Əsas ədəbiyyat

1.Weidman, G.*Penetration Testing: A Hands-On Introduction to Hacking* No Starch Press, 2014.
2.Engebretson, P.*The Basics of Hacking and Penetration Testing.*Syngress, 2013.
3.Chapple, M., Seidl, D.*CompTIA PenTest+ Study Guide* Sybex, 2022.
4.Stallings, W., Brown, L.*Computer Security: Principles and Practice* Pearson Education, 2018.
5.Whitman, M., Mattord, H.*Principles of Information Security* Cengage Learning, 2021.

Əlavə ədəbiyyat

6.Andress, J. *The Basics of Information Security.* Syngress, 2014.
7.Scambray, J., Shema, M., Sima, C.*Hacking Exposed: Network Security Secrets & Solutions.* McGraw-Hill, 2019.
8.McNab, C.*Network Security Assessment.*O'Reilly Media, 2016.
9.Pfleeger, C., Pfleeger, S., Margulies, J. *Security in Computing.*Pearson, 2015.

10.Mühazirələr. Nüfuzetmə sınaqlarının əsasları.Dəmirov Asəf Ağacəfər oğlu, t.ü.f.d.,dosent.LDU-2026.

IV. Prerekvizit fənlər: Fənnin tədrisi üçün öncədən başqa bir fənnin tədrisinə zəruri yoxdur..

V. Korekvizit fənlər: Fənnin tədrisi ilə eyni zamanda başqa fənnin tədrisinə ehtiyac yoxdur.

VI. Fənnin təsviri və məqsədi:

"Nüfuzetmə sınaqlarının əsasları" fənni informasiya sistemlərinin, kompüter şəbəkələrinin və tətbiqlərin təhlükəsizlik səviyyəsinin qiymətləndirilməsi məqsədilə aparılan nüfuzetmə sınaqlarının (penetration testing) nəzəri və praktik əsaslarını öyrədir. Fənn çərçivəsində tələbələr informasiya təhlükəsizliyinin əsas anlayışları, nüfuzetmə sınaqlarının mərhələləri, istifadə olunan metodoloji yanaşmalar, risklərin müəyyənləşdirilməsi və təhlükəsizlik boşluqlarının qiymətləndirilməsi prinsipləri ilə tanış olurlar.
Tədris zamanı nüfuzetmə sınaqlarının yalnız icazəli və etik çərçivədə aparılması, hüquqi məsuliyyət və peşə etikası xüsusi vurğulanır. Fənn real sistemlər üzərində deyil, simulyasiya olunmuş və tədris məqsədli mühitlərdə tətbiq olunan yanaşmalara əsaslanır.

Bu fənnin əsas məqsədi tələbələrdə:
İnformasiya təhlükəsizliyi sahəsində fundamental biliklərin formalaşdırılması
-Nüfuzetmə sınaqlarının məqsədini, rolunu və əhəmiyyətini dərk etmə
-Sistem və şəbəkələrdə mövcud ola biləcək təhlükəsizlik risklərini analitik yanaşma ilə qiymətləndirmə bacarığı
-Zəifliklərin istismarına deyil, onların qarşısının alınmasına yönəlmiş düşüncə tərzi
-Nüfuzetmə sınaqlarının nəticələrini texniki və idarəetmə səviyyəsində düzgün təqdim etmə vərdişləri
-Etik, hüquqi və peşəkar davranış normalarına riayət etmə mədəniyyəti formalaşdırmaqdır.

Tələbələrə informasiya sistemləri və şəbəkələrdə təhlükəsizlik boşluqlarının müəyyənləşdirilməsi və qiymətləndirilməsi üçün nüfuzetmə sınaqlarının nəzəri əsaslarını, metodoloji yanaşmalarını və etik-hüquqi çərçivəsini öyrətmək.
Fənnin vəzifələri
İnformasiya təhlükəsizliyi anlayışlarını sistemli şəkildə izah etmək
Nüfuzetmə sınaqlarının mərhələlərini və məqsədlərini öyrətmək
Risk və zəiflik anlayışlarını təhlil etmək
Təhlükəsizlik qiymətləndirmə nəticələrinin sənədləşdirilməsi bacarığı formalaşdırmaq
Etik və hüquqi məsuliyyət şüurunu aşılamaqdan ibarətdir.

VII.Davamiyyətə verilən tələblər: Fənn üzrə semestr ərzində buraxılmış auditoriya saatlarının ümumi sayı LDU-nun Elmi Şurasının 16 may 2024-cü il tarixli qərarına uyğun olaraq davamiyyət meyarları nəzərə alınmaqla müəyyən olunmuş həddən yuxarı olduğu halda tələbə həmin fəndən imtahana buraxılmır, onun həmin fənn üzrə akademik borcu qalır.

VIII.Qiymətləndirmə: Fənn üzrə tələbələrin biliyi 100 ballıq sistemlə qiymətləndirilir.Yəni tələbənin fənn üzrə toplaya biləcəyi balın maksimum miqdarı 100-ə bərabərdir.

Bu balın yarısı (50 balı) tələbənin semestr müddətində fəaliyyətinin nəticəsinə (cari qiymətləndirmə), digər yarısı isə (digər 50 balı) imtahanın nəticəsinə (aralıq qiymətləndirmə) görə verilir.

Fənn üzrə cari qiymətləndirmənin nəticəsinə görə verilən maksimum 50 bala aşağıdakılar daxildir:

- 20 bal - seminar dərslərində fəaliyyətinə görə;
- 30 bal - kollokviumların nəticələrinə görə.

Qiymətləndirmə zamanı LDU-nun Elmi Şurasının 16 may 2024-cü il tarixli qərarına uyğun olaraq qiymətləndirmə meyarları nəzər alınır.

İmtahanda qazanılan balların maksimum miqdarı 50-dir. İmtahan yazılı şəkildə aparılır və imtahan biletinə bir qayda olaraq fənn üzrə tədris olunan mövzulara aid 5 sual daxil edilir. Hər sual maksimum 10 bal olmaqla qiymətləndirilir (aşağıda qeyd olunan qiymət meyarına əsasən) ki, bu da toplamda fənn üzrə aralıq qiymətləndirmənin nəticəsinə görə verilən maksimum 50 balı təşkil edir.

Qiymət meyarları aşağıdakılardır:

- 10 bal - tələbə keçilmiş materialı dərindən başa düşür, cavabı dəqiq və hərtərəflidir;
- 9 bal - tələbə keçilmiş materialı tam başa düşür, cavabı dəqiqdir və mövzunun məzmununu tam açа bilir;
- 8 bal - tələbə cavabında ümumi xarakterli bəzi qüsurlara yol verir;
- 7 bal - tələbə keçilmiş materialı yaxşı başa düşür, lakin nəzəri cəhətdən bəzi məsələləri əsaslandıra bilmir;
- 6 bal - tələbənin cavabı əsasən düzgündür;
- 5 bal - tələbənin cavabında çatışmazlıqlar var, mövzunu tam əhatə edə bilmir;
- 4 bal - tələbənin cavabı qismən doğrudur, lakin mövzunu izah edərkən bəzi səhvlərə yol verir;
- 3 bal - tələbənin mövzudan xəbəri var, lakin fikrini əsaslandıra bilmir;
- 1-2 bal - tələbənin mövzudan qismən xəbəri var;
- 0 bal - cavab yoxdur.

Tələbənin fənn üzrə aralıq qiymətləndirmə balının (imtahanda topladığı balın) miqdarı 17-dən az olmamalıdır. Əks təqdirdə tələbənin fənn üzrə aralıq qiymətləndirmə balı cari qiymətləndirmə balına (semestr ərzində tədris fəaliyyəti nəticəsində topladığı bala) əlavə olunmur.

Fənn üzrə cari və aralıq qiymətləndirmənin ümumi nəticəsinə görə tələbənin biliyi yekun olaraq aşağıdakı kimi qiymətləndirilir:

Bal aralığı (göstərilən ballar daxil olmaqla)	Hərflə işarəsi	Sözlə yazılışı
91-100 bal	A	əla
81-90 bal	B	çox yaxşı
71-80 bal	C	yaxşı
61-70 bal	D	kafi
51-60 bal	E	qənaətbəxş
51-baldan aşağı	F	qeyri-kafi

IX. Davranış qaydalarının pozulması:

Tələbə Universitetin Daxili intizam qaydalarını pozduqda onun barəsində mövcud qanunvericilik çərçivəsində müvafiq tədbir görüləcəkdir.

X.Təqvim mövzu planı: Mühazirə – 45 saat, laboratoriya –30 saat, Cəmi 75 – saat

Mühazirə mövzuları

S/s	Mövzunun adı və məzmunu	Saat
1.	**Mövzu № 1.Nüfuzetmə sınaqlarına giriş** Plan: 1.Penetrasiya testinin anlayışı və məqsədi 2.Red Team, Blue Team, Purple Team **Mənbə:10** [1-10]	2
2.	**Mövzu № 2.İnformasiya təhlükəsizliyində etik və hüquqi çərçivə** Plan: 1.Etik hakerlik 2.Qanunvericilik və icazə prinsipləri **Mənbə:10** [11-20]	2
3.	**Mövzu № 3. Nüfuzetmə sınaqlarının növləri** Plan: 1.Black box,White box,Gray box 2.Daxili və xarici testlər **Mənbə:10** [21-30]	2
4.	**Mövzu № 4. Nüfuzetmə sınaqlarının mərhələləri** Plan: 1.Planning 2.Reconnaissance 3.Exploitation 4.Reporting **Mənbə:10** [31-40]	2
5.	**Mövzu № 5. Təhlükə modelləşdirilməsi və risk anlayışı** Plan: 1.Risk analizi 2.CVSS əsasları **Mənbə:10** [41-50]	2
6.	**Mövzu № 6. Passiv kəşfiyyat (Passive Reconnaissance)** Plan: 1.OSINT anlayışı 2.Açıq mənbələrin analizi **Mənbə:10** [51-60]	2
7.	**Mövzu № 7. Aktiv kəşfiyyat (Active Reconnaissance)** Plan: 1.Şəbəkə skanlaması 2.Port və servis aşkarlanması **Mənbə:10** [61-70]	2
8.	**Mövzu № 8. Şəbəkə əsaslı hücumlara giriş** Plan: 1.TCP/IP zəifliklər 2.ARP, DNS hücumları **Mənbə:10** [71-80]	2
9.	**Mövzu № 9. Əməliyyat sistemlərində zəifliklər** Plan:	2

Cəmi 75 – saat.

Saat

Ta

	1.Windows əsaslı zəifliklər 2.Linux əsaslı zəifliklər **Mənbə:10** [81-90]		
10	**Mövzu № 10. Zəiflik skanerləri** Plan: 1.Avtomatik və manual analiz fərqləri **Mənbə:10** [91-100]	2	
11.	**Mövzu № 11. Exploit anlayışı və növləri** Plan: 1.Local exploitlər 2.Remote exploitlər **Mənbə:10** [101-110]	2	
12.	**Mövzu № 12. Parol hücumları** Plan: 1.Brute force 2.Dictionary attack **Mənbə:10** [111-120]	2	
13.	**Mövzu № 13. Sosial mühəndislik hücumları** Plan: 1.Phishing 2.Pretexting **Mənbə:10** [121-130]	2	
14.	**Mövzu № 14. Veb tətbiqlərə giriş** Plan: 1.Veb tətbiqlərə giriş 2.Veb arxitektura 3.HTTP/HTTPS **Mənbə:10** [131-140]	2	
15.	**Mövzu № 15. Veb tətbiqlərdə əsas zəifliklər** Plan: 1.OWASP Top 10-ə giriş **Mənbə:10** [141-150]	2	
16.	**Mövzu № 16. SQL Injection hücumları** Plan: 1.SQL Injection hücumları 2.İş prinsipi və növləri **Mənbə:10** [151-160]	2	
17.	**Mövzu № 17. XSS və CSRF hücumları** Plan: 1. XSS və CSRF hücumları 2.Reflected, Stored, DOM XSS **Mənbə:10** [161-170]	2	
18.	**Mövzu № 18. Fayl yükləmə və autentifikasiya zəifliklər** Plan: 1.Fayl yükləmə zəifliklər 2.Autentifikasiya zəifliklər **Mənbə:10** [171-180]	2	
19.	**Mövzu № 19. Wireless şəbəkələrdə nüfuzetmə sınaqları** Plan: 1.Wireless şəbəkələrdə nüfuzetmə sınaqları 2.Wi-Fi təhlükəsizliyi **Mənbə:10** [181-190]	2	

20.	**Mövzu № 20. Post-exploitation mərhələsi** Plan: 1.Post-exploitation mərhələsi 2.Privilege escalation **Mənbə:10** [191-200]	2
21.	**Mövzu № 21.Logların silinməsi və izlərin gizlədilməsi (nəzəri)** Plan: 1.Logların silinməsi 2.İzlərin gizlədilməsi (nəzəri) **Mənbə:10** [201-210]	2
22.	**Mövzu № 22.Hesabatlaşdırma və sənədləşmə** Plan: 1.Hesabatlaşdırma və sənədləşmə 2.Texniki və idarəetmə hesabatları **Mənbə:10** [211-220]	2
23.	**Mövzu № 23.Müasir trendlər və müdafiə mexanizmləri** Plan: 1. Müasir trendlər və müdafiə mexanizmləri 2. Zero Trust 3. Bug Bounty proqramları **Mənbə:10** [221-230]	1
	Cəmi mühazirə:	**45 s.**

S/s	Laboratoriya mövzusunun adı	Saat	Tarix
1.	Təhlükəsiz laboratoriya mühitinin qurulması.Virtual maşınların hazırlanması	2	
2.	OSINT alətləri ilə passiv kəşfiyyat	2	
3.	Şəbəkə skanlaması və port analizi	2	
4.	Servis və versiya aşkarlanması	2	
5.	Zəiflik skaneri ilə analiz	2	
6.	Manual zəiflik analizi	2	
7.	Parol hücumlarının icrası (təlim mühiti)	2	
8.	Sosial mühəndislik ssenarilərinin analizi	2	
9.	SQL Injection zəifliyinin aşkarlanması	2	
10.	XSS zəifliyinin test edilməsi	2	
11.	Fayl yükləmə zəifliklərinin yoxlanılması	2	
12.	Wireless şəbəkə təhlükəsizliyinin analizi	2	
13.	Privilege escalation ssenarisi	2	
14.	Post-exploitation mərhələsinin icrası	2	
15.	Penetrasiya test hesabatının hazırlanması	1	
Cəmi laboratoriya:		**30 s.**	
Fənn üzrə cəmi:		**75 s.**	

XI. Fənn üzrə tələblər:

Nüfuzetmə sınaqlarının mərhələlərini izah edə bilməlidir.
Əsas zəifllikləri aşkarlaya və qiymətləndirə bilməlidir.
Etik və hüquqi çərçivədə penetrasiya testi aparma bacarığı qazanmalıdır.
Texniki hesabat hazırlaya bilməlidir.

Fənnin sonunda tələbələr nüfuzetmə sınaqlarının əsas prinsiplərini anlayan, təhlükəsizlik boşluqlarını müəyyən edib qiymətləndirə bilən və informasiya sistemlərinin

qorunmasının gücləndirilməsinə töhfə verən ilkin səviyyəli informasiya təhlükəsizliyi mütəxəssisi kimi formalaşmalıdırlar.

XII.Fənnin tədrisi üçün nəzərdə tutulan tədris və öyrənmə metodları:
Təlim prosesində fərqli tədris metodlarından istifadə edilməlidir. Bu metodlar tələbəyönümlü yanaşmanı və tələbələrin təlim prosesindəki fəal rol oynamasını təşviq etməlidir. İstifadə edilə biləcək tədris və öyrənmə üsullarına aşağıdakıları nümunə olaraq göstərmək olar:

- mühazirələr,
- təcrübi tapşırıqlar:
- təqdimatlar və müzakirələr,
- problemlərə əsaslanan tədris:
- rol oyunlar, hesabatlar:
- qrup qiymətləndirməsi:
- ekspert metodu;
- simulyasiyalar.

XII. Fənn üzrə təlimin nəticələri:
Fənni bitirən tələbə:
Nüfuzetmə sınaqlarının mərhələlərini izah edə bilir
Əsas zəifliklər aşkarlaya və qiymətləndirə bilir
Etik və hüquqi çərçivədə penetrasiya testi aparma bacarığı qazanır
Texniki hesabat hazırlaya bilir

Fənnin sonunda tələbələr nüfuzetmə sınaqlarının əsas prinsiplərini anlayan, təhlükəsizlik boşluqlarını müəyyən edib qiymətləndirə bilən və informasiya sistemlərinin qorunmasının gücləndirilməsinə töhfə verən ilkin səviyyəli informasiya təhlükəsizliyi mütəxəssisi kimi formalaşırlar.

XIII. Tələbələrin fənn haqqında fikrinin öyrənilməsi:

XIV. Kollokvium sualları

I Kollokvium sualları
1.Penetrasiya testinin anlayışı və məqsədi
2.Red Team, Blue Team, Purple Team
3.Etik hakerlik
4.Qanunvericilik və icazə prinsipləri
5.Black box,White box,Gray box
6.Daxili və xarici testlər
7.Planning
8.Reconnaissance
9.Exploitation
10.Reporting
11.Risk analizi
12.CVSS əsasları
13.OSINT anlayışı
14.Açıq mənbələrin analizi
15.Şəbəkə skanlaması

II Kollokvium sualları
16.Port və servis aşkarlanması

17.TCP/IP zəifliklər
18.ARP, DNS hücumları
19.Windows əsaslı zəifliklər
20.Linux əsaslı zəifliklər
21.Local exploitlər
22.Remote exploitlər
23.Brute force
24.Dictionary attack
25.Brute force
26.Dictionary attack
27.Phishing
28.Pretexting
29.Veb tətbiqlərə giriş
30.Veb arxitektura

XV. İmtahan sualları:

1.Penetrasiya testinin anlayışı və məqsədi
2.Red Team, Blue Team, Purple Team
3.Etik hakerlik
4.Qanunvericilik və icazə prinsipləri
5.Black box,White box,Gray box
6.Daxili və xarici testlər
7.Planning
8.Reconnaissance
9.Exploitation
10.Reporting
11.Risk analizi
12.CVSS əsasları
13.OSINT anlayışı
14.Açıq mənbələrin analizi
15.Şəbəkə skanlaması
16.Port və servis aşkarlanması
17.TCP/IP zəifliklər
18.ARP, DNS hücumları
19.Windows əsaslı zəifliklər
20.Linux əsaslı zəifliklər
21.Local exploitlər
22.Remote exploitlər
23.Brute force
24.Dictionary attack
25.Brute force
26.Dictionary attack
27.Phishing
28.Pretexting
29.Veb tətbiqlərə giriş
30.Veb arxitektura
31. HTTP/HTTPS
32. Veb tətbiqlərdə əsas zəifliklər
33. OWASP Top 10-ə giriş
34. SQL Injection hücumları
35. İş prinsipi və növləri

36. XSS və CSRF hücumları
37. Reflected, Stored, DOM XSS
38. Fayl yükləmə zəiflikləri
39. Autentifikasiya zəiflikləri
40. Wireless şəbəkələrdə nüfuzetmə sınaqları
41. Wi-Fi təhlükəsizliyi
42. Post-exploitation mərhələsi
43. Privilege escalation
44. Logların silinməsi
45. İzlərin gizlədilməsi (nəzəri)
46. Hesabatlaşdırma və sənədləşmə
47. Texniki və idarəetmə hesabatları
48. Müasir trendlər və müdafiə mexanizmləri
49. Zero Trust
50. Bug Bounty proqramları

"Nüfuzetmə sınaqlarının əsasları" fənninin sillabusu bakalavr pilləsi üzrə **6006017-** İnformasiya təhlükəsizliyi ixtisasının təhsil proqramı, tədris planı və bu fənnin işçi fənn proqramı əsasında tərtib edilmişdir.
Sillabus **"Texnologiya və texniki elmlər "** kafedrasında müzakirə edilərək təsdiq edilmişdir **(07.01.2026-cı il, protokol № 5).**

Fənn müəllimi: dosent,A.A. Dəmirov.

m, S.Ə. Salmanlı.

Kafedra müdiri: dosent, R. F. Əliyev