Azərbaycan Respublikası Elm və Təhsil Nazirliyi
Lənkəran Dövlət Universiteti

"Təsdiq edirəm"
Tədrisin təşkili və təlim
texnologiyalari üzrə prorektor
vəzifəsini icra edən:
dos.Z.İ.Məmmədov
07 fevral 2025

Fənn sillabusu

İxtisas: İnformasiya təhlükəsizliyi
Kafedra: Texnologiya və texniki elmlər
I. Fənn haqqında məlumat:
Fənnin adı: Kiber təhlükəsizliyinin əsasları
Kodu: İPFS-B 03.2
Tədris ili: I tədris ili, (2024-2025) Semestr: II
Tədris yükü: Auditoriya saatı 60 (30 saat mühazirə, 30 saat laboratoriya)
Tədris forrması: Əyani
Tədris dili: Azərbaycan dili
AKTS üzrə kredit: 6 kredit
Auditoriya N: 215
Saat: 9^{30} ,14^{40} , 11^{20}
II. Müəllim haqqında məlumat:
Adı, soyadı, elmi dərəcəsi və elmi adı: Vüsalə Muradova Xudaşirin qızı, t.ü.f.d., dosent
Məsləhət saatı: IV gün saat 12^{20} -13^{30}
E-mail ünvanı: vusala.muradoav@lsu.edu.az
Kafedranın ünvanı: Lənkəran şəhər Fizuli 170 a Tədris korpusu
III. Tövsiyyə olunan dərsliklər və dərs vəsaitləri:

Əsas ədəbiyyat

1. Parasram S. V., Samm A., Boodoo D., Johansen G., Allen L., Heriyanto T., & Ali S., "Kali Linux 2018: Assuring Security by Penetration Testing, 4th Edition. 2018, 518 p.
2. Chapple M., Seidl D., CompTIA Security+ Study Guide: Exam SYO- 601. "Sybex". 2021, 672 p.
3. Əbdiyeva-Əliyeva G., Kibertəhlükəsizliyin əsasları. 2022, 208 s.

Əlavə ədəbiyyat

4. Əliquliyev R.M., İmamverdiyev Y.N., İnformasiya təhlükəsizliyi insidentləri. Bakı: İnformasiya texnologiyaları, 2012, 212 s.
5. Charles J.B, Christoper G., Philip A.C., Donald S., Cybersecurity Essentials. "Sybex", 2018, 784 s.
6. Ozkaya E., Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity. Packt Publishing, 2019, 396 p.
7. https://tryhackme.com/

VI. Prekvizitlər: Fənnin tədrisi üçün öncədən informasiya təhlükəsizliyi probl... onu xarakterizə edən amillərin tədrisi vacibdir.

V. Korekvizitlər: Bu fənnin tədrisi ilə eyni vaxtda başqa fənlərin də təd... olunmasına zərurət yoxdur.

VI. Fənnin təsviri və məqsədi: "Kibertəhlükəsizliyin əsasları" fənninin tədrisi zamanı tələbələrə əsas kibertəhlükəsizlik anlayışları, Kali linux mühitində müxtəlif praktiki tapşırıqların yerinə yetirilməsi, sızma testi metodologiyası, məlumat toplanması prosesi, müxtəlif alətlərlə dərama və inventarlaşdırma üsulları, boşluqların analizi, sistemin hakinqi metodologiyası, DDOS hücumları və onlardan müdafiə üsulları, steqanoqrafiya tətbiqləri, müxtəlif sosial mühəndislik hücumları, naqilsiz şəbəkələrin təhlükəsizliyi məsələləri üzrə lazımi biliklər tədris olunur və sadalanan istiqamətlər üzrə parktiki laboratoriya tapşırıqları yerinə yetirilir.

VII. Davamiyyətə verilən tələblər:

Fənn üzrə semestr ərzində buraxılmış auditoriya saatlarının ümumi sayı Elmi Şuranın 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:

Qiymətləndirmə zamanı Elmi Şuranın 16 may 2024-cü il tarixli qərarina uyğun olaraq qiymətləndirmə meyarları nəzər alınır.

Tələbələrin biliyi 100 ballı sistemlə qiymətləndirilir. Bundan 50 balı tələbə semestr ərzində, 50 balı isə imtahanda toplayır. Semestr ərzində toplanan 50 bala aşağıdakılar aiddir: 30 bal kollokviuma görə, 20 bal seminar və ya laboratoriya dərslərində fəaliyyətinə görə. İmtahanda qazanılan balların maksimum miqdarı 50-dir. İmtahan biletinə bir qayda olaraq fənni əhatə edən 5 sual daxil edilir.

Qiymət meyarları aşağıdakılardır:

-10 bal- tələbə keçirilmiş materialları dərindən başa düşür, cavabı dəqiqdir və hərtərəflidir.

- 9 bal - tələbə keçirilmiş materialları tam başa düşür, cavabı dəqiqdir və mövzunun mətnini tam açа bilir.
- 8 bal - tələbə cavabında ümumi xarakterli bəzi qüsurlara yol verir.
- 7 bal - tələbə keçirilmiş materialları başa düşür, lakin nəzəri cəhətdən bəzi məsələləri əsaslandıra bilmir.
- 6 bal - tələbənin cavabı əsasən düzgündür.
- 5 bal - tələbənin cavabında çatışmamazlıqlar 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 - suallara cavab yoxdur.

Tələbənin imtahanda topladığı balın miqdarı 17-dən az olmamalıdır. Əks təqdirdə tələbənin imtahan göstəriciləri semestr ərzində tədris fəaliyyəti nəticəsində topladığı bala əlavə olunmur.

Semestr nəticələrinə görə yekun qiymətləndirmə (imtahan və imtahana qədərki ballar əsasında)

51 baldan aşağı "qeyrikafi" -F,
51 - 60 bal "qənaətbəxş" -E,
61 - 70 bal "kafi" -D,
71 - 80 bal "yaxşı" -C,
81 - 90 bal "çoxyaxşı" -B,

IX. Davranış qaydalarının pozulması:Tələbə Universitetin daxili nizam-intizam qaydalarını pozduqda əsasnamədə nəzərdə tutulan qaydada tədbir görüləcək.

X. Təqvim mövzu planı: Mühazirə 30 saat, seminar 30 saat. Cəmi: 60 saat

№	Keçirilənmühazirə, seminar, məşgələ, laboratoriyavəsərbəstmövzuların məzmunu	Saat	Tarix
1	2	3	4
	Mühazirə mövzuları		
1.	**Mövzu № 1. Kibertəhlükəsizliyin əsas anlayışları** Plan: 1. Kibertəhlükəsizliyə giriş. 2. "Kibertəhlükəsizlik" və "informasiya təhlükəsizliyi" anlayışları arasındakı fərqlər. 3. Kibertəhlükəsizliyinin təmin edilməsi metodları Mənbə: 1,3,4	2	
2.	**Mövzu № 2. GNU-Linux əməliyyat sistemi. Kali Linux** Plan: 1. Əməliyyat sistemi anlayışı. 2. GNU-Linux əməliyyat sistemi və onun qısa tarixi. 3. Virtual maşının kompüterə quraşdırılması və konfiqurasiyası. 4. Kali Linux-un əsas komandaları Mənbə: 2,3,4	2	
3.	**Mövzu 3. Sızma testi metodologiyası** Plan: 1. Giriş: Əsas anlayışlar, vəzifələr, istifadə alətləri. 2. Sızma testinin növləri. 3. Sızma testi metodologiyaları. 4. Sızma testinin mərhələləri. 5. Sızma testi etikası. Mənbə: 1,3, 4	2	
4.	**Mövzu 4. Kəşfiyyat və məlumat toplanması** Plan: 1. Kiberhücum hədəfi barədə müxtəlif mənbələrdən informasiyanın toplanması metodları və alətləri. Mənbə:1,3, 4	2	
5.	**Mövzu № 5. Darama və inventarlaşdırma üsulları** Plan: 1. Daramanın növləri. 2. Şəbəkənin daranması üsulları. 3. Nmap. 4. Şəbəkə obyektlərinin inventarlaşdırılması konsepsiyası və üsulları. Mənbə : 2,3,4	2	
6.	**Mövzu № 6. Boşluqların daranması** Plan: 1. Boşluqların idarə edilməsinin həyat dövrü. 2. Nessus ilə boşluqların daranması. 3. Metasploit aləti və onun imkanları	2	

	Mənbə: 1,3,4.		
7.	**Mövzu № 7.** Sistemin hakinqi metodologiyası Plan: 1. Sistemin hakinq edilməsi metodologiyası, keyloqqerlər. 2. Casus proqram təminatı, izlərin gizlədilməsi alətləri Mənbə: 1,3, 4,	2	
8.	**Mövzu № 8.** Sosial mühəndislik hücumları Plan: 1.Sosial mühəndislik anlayışı. 2. Sosial mühəndislik prosesi. növləri. 3. Sosial mühəndislik hücum metodları. 4. Bəzi real sosial mühəndislik nümunələri. 5. Əsas təhlükəsizlik tədbirləri. Mənbə: 1,3,4.	2	
9.	**Mövzu 9. DDoS hücumları və müdafiə üsulları** Plan: 1. DoS və DDoS hücumları. 2. DoS hücumlara nümunələr. 3. DDoS hücum alətləri. 4. DoS hücumlardan müdafiə mexanizmləri Mənbə: 1,3, 4.	2	
10.	**Mövzu 10. İmtiyazın artırılması və girişin təmin olunması** Plan: 1. İmtiyazın artırılmasının növləri. 2. Boşluq üçün eksploytun axtarılması (Metasploit, Search). Bekdorlar Mənbə : 2,3,4	2	
11.	**Mövzu 11. Veb tətbiqlərin təhlükəsizliyi** Plan: 1. OWASP yanaşması. 2. Veb sistemlərə hücumların əsas sinifləri. 3. SQL inyeksiyanın növləri. 4. XSS-hücumlar (Saytlararası senari icrası) OWASP ZAP skaneri. 5. Burp Suite ilə veb tətbiqlərin test edilməsi Mənbə : 1,2,3	2	
12.	**Mövzu 12. Naqilsiz şəbəkələrin təhlükəsizliyi** Plan: 1. Naqilsiz şəbəkələrin növləri. 2. Naqilsiz lokal şəbəkələrdə təhlükəsizlik protokolları Mənbə : 1,2,3	2	
13.	**Mövzu 13. Naqilsiz şəbəkələrdə sızma testi** Plan: 1. Naqilsiz şəbəkələrin test edilməsi alətləri. 2. Aircrack-ng ilə sızma testinin metodikası Mənbə : 1,2,3	2	
14.	**Mövzu 14. Sızma testləri barədə hesabat hazırlanması alətləri** Plan: 1. Sızma testləri üzrə hesabatların növləri. 2. Texniki hesabatın əsas bəndləri. Dradis freymvorku. Faraday IDE, MagicTree və Pipal.	2	

	2. Texniki hesabatın əsas bəndləri. Dradis freymvorku. Faraday IDE, MagicTree və Pipal. Mənbə: 1,2,3		
15.	**Mövzu 15. Kursun ümumi dəyərləndirilməsi** Plan: 1. Kursun ümumi müzakirəsi. Suallar, cavablar və təkliflər Mənbə: 1,2,3	2	
	Cəmi	**30**	
	Seminar mövzuları		
1.	**Kibertəhlükəsizliyin əsas anlayışları**	2	
2.	**GNU-Linux əməliyyat sistemi. Kali Linux**	2	
3.	**Sızma testi metodologiyası**	2	
4.	**Kəşfiyyat və məlumat toplanması**	2	
5.	**Darama və inventarlaşdırma üsulları**	2	
6.	**Boşluqların daranması**	2	
7.	**Sistemin hakinqi metodologiyası**	2	
8.	**Sosial mühəndislik hücumları**	2	
9.	**DDoS hücumları və müdafiə üsulları**	2	
10.	**İmtiyazın artırılması və girişin təmin olunması**	2	
11.	**Veb tətbiqlərin təhlükəsizliyi**	2	
12.	**Naqilsiz şəbəkələrin təhlükəsizliyi**	2	
13	**Naqilsiz şəbəkələrdə sızma testi**	2	
14.	**Sızma testləri barədə hesabat hazırlanması alətləri**	2	
15.	**Kursun ümumi dəyərləndirilməsi**	2	
	Cəmi	**30**	

XI. Fənn üzrə tələblər, tapşırıqlar:

Fənnin tədrisinin sonunda tələbələr **"Kibertəhlükəsizliyin əsaları "** kursundan müəyyən biliklərə malik olmalı, o cümlədən fənn haqqında nəzəri və praktik şəkildə fikirlərini əsaslandırmağı bacarmalıdırlar.

" Kibertəhlükəsizliyin əsasları " fənninin tədrisi zamanı tələbələrə kompüterin strukturuna aıd olan müxtəlif bölmələrinin və praktik tətbiqini öyrədilməsi fənn üzrə qoyulan əsas tələblərdən biridir: " Kibertəhlükəsizliyin əsasları " fənninin tədrisi zamanı qoyulan tələblər aşağıdakı kimidir:

- Mühazirə mətninin hazırlanması,
- test tapşırıqları,
- referat işləri,
- fərdi tapşırıqlar,
- praktiki məsələlər.

XII.Təlimin nəticələri

Fənnin mənimsənilməsi nəticəsində tələbələr bilməlidirlər:

- Informasiya resurslarına yönəlmiş təhdidlərin təsnifatını
- Girişin əldə olunmasının əsas yollarını
- Kiberhücumların motivi
- Kibertəhlükəsizlik
- Domenlərlə işləməsi qaydalarını
- Əsas növləri

- Fərdi xüsusiyyətlərini
- Strategiyasının qurulması

XIII. Tələbələrin fənn haqqında fikrinin öyrənilməsi:

XIV.Birinci kollekvium sualları

1. Kibertəhlükəsizliyə giriş.
2. "Kibertəhlükəsizlik" və "informasiya təhlükəsizliyi" anlayışları arasındakı fərqlər.
3. Kibertəhlükəsizliyinin təmin edilməsi metodları
4. Əməliyyat sistemi anlayışı.
5. GNU-Linux əməliyyat sistemi və onun qısa tarixi.
6. Virtual maşının kompüterə quraşdırılması və konfiqurasiyası.
7. Kali Linux-un əsas komandaları
8. Giriş: Əsas anlayışlar, vəzifələr, istifadə alətləri.
9. Sızma testinin növləri.
10. Sızma testi metodologiyaları.
11. Sızma testinin mərhələləri.
12. Sızma testi etikası.
13. Kiberhücum hədəfi barədə müxtəlif mənbələrdən informasiyanın toplanması metodları və alətləri.
14. Daramanın növləri.
15. Şəbəkənin daranması üsulları.

Ikinci kollekvium sualları

1. Nmap.
2. Şəbəkə obyektlərinin inventarlaşdırılması konsepsiyası və üsulları.
3. Boşluqların idarə edilməsinin həyat dövrü.
4. Nessus ilə boşluqların daranması.
5. Metasploit aləti və onun imkanları
6. Sistemin hakinq edilməsi metodologiyası, keyloqqerlər.
7. Casus proqram təminatı, izlərin gizlədilməsi alətləri
8. Sosial mühəndislik anlayışı.
9. Sosial mühəndislik prosesi. növləri.
10. Sosial mühəndislik hücum metodları.
11. Bəzi real sosial mühəndislik nümunələri.
12. Əsas təhlükəsizlik tədbirləri.
13. DoS və DDoS hücumları.
14. DoS hücumlara nümunələr.
15. DDoS hücum alətləri.

XV. Fənnin imtahan sualları:

I ci blok

1. Kibertəhlükəsizliyə giriş.
2. "Kibertəhlükəsizlik" və "informasiya təhlükəsizliyi" anlayışları arasındakı fərqlər.
3. Kibertəhlükəsizliyinin təmin edilməsi metodları
4. Əməliyyat sistemi anlayışı.
5. GNU-Linux əməliyyat sistemi və onun qısa tarixi.
6. Virtual maşının kompüterə quraşdırılması və konfiqurasiyası.
7. Kali Linux-un əsas komandaları
8. Giriş: Əsas anlayışlar, vəzifələr, istifadə alətləri.
9. Sızma testinin növləri.

II ci blok

10. Sızma testi metodologiyaları.
11. Sızma testinin mərhələləri.
12. Sızma testi etikası.
13. Kiberhücum hədəfi barədə müxtəlif mənbələrdən informasiyanın toplanması metodları və alətləri.
14. Daramanın növləri.
15. Şəbəkənin daranması üsulları.
16. Nmap.
17. Şəbəkə obyektlərinin inventarlaşdırılması konsepsiyası və üsulları.
18. Boşluqların idarə edilməsinin həyat dövrü.

III cü blok

19. Nessus ilə boşluqların daranması.
20. Metasploit aləti və onun imkanları
21. Sistemin hakinq edilməsi metodologiyası, keyloqqerlər.
22. Casus proqram təminatı, izlərin gizlədilməsi alətləri
23. Sosial mühəndislik anlayışı.
24. Sosial mühəndislik prosesi. növləri.
25. Sosial mühəndislik hücum metodları.
26. Bəzi real sosial mühəndislik nümunələri.
27. Əsas təhlükəsizlik tədbirləri.

IV cü blok

28. DoS və DDoS hücumları.
29. DoS hücumlara nümunələr.
30. DDoS hücum alətləri.
31. DoS hücumlardan müdafiə mexanizmləri
32. İmtiyazın artırılmasının növləri.
33. Boşluq üçün eksploytun axtarılması (Metasploit, Search). Bekdorlar
34. OWASP yanaşması.
35. Veb sistemlərə hücumların əsas sinifləri.
36. SQL inyeksiyanın növləri.

V ci blok

37. XSS-hücumlar (Saytlararası senari icrası) OWASP ZAP skaneri.
38. Burp Suite ilə veb tətbiqlərin test edilməsi

39. Naqilsiz şəbəkələrin növləri.
40. Naqilsiz lokal şəbəkələrdə təhlükəsizlik protokolları
41. Sızma testləri üzrə hesabatların növləri.
42. Texniki hesabatın əsas bəndləri. Dradis freymvorku. Faraday IDE, MagicTree və Pipal.
43. Sızma testləri üzrə hesabatların növləri.
44. Texniki hesabatın əsas bəndləri. Dradis freymvorku. Faraday IDE, MagicTree və Pipal.
45. Kursun ümumi müzakirəsi. Suallar, cavablar və təkliflər

" Kibertəhlükəsizliyin əsasları" fənninin sillabusu 050631 - "İnformasiya texnologiyaları" ixtisasının tədris planı və fənn proqramı əsasında tərtib edilmişdir.

Sillabus **"Texnologiya və texniki elmlər"** kafedrasında müzakirə edilərək, təsdiq edilmişdir (07 fevral 2025-ci il, protokol № 01).

Fənn müəllimi: **dosent, V. X. Muradova**

Kafedra müdiri: **dosent, R. F. Əliyev**