კავკასიის უნივერსიტეტი
კავკასიის ტექნოლოგიების სკოლა

სილაბუსი	
სასწავლო კურსის დასახელება	კომპიუტერული უსაფრთხოება
სასწავლო კურსის კოდი	CTC 2244
სასწავლო კურსის ანოტაცია	კომპიუტერული/კიბერ უსაფრთხოების ძირითადი პრინციპები, მათი მიმოხილვა და კონფიგურაცია – კურსი მოიცავს კომპიუტერულ უსაფრთხოებას, სხვადასხვა ოპერაციული სისტემის გამოყენებით და განსხვავებული მიმართულებებით (ოპერაციული სისტემის, ქსელის და მომხმარებლის კუთხიდან). განხილულია კიბერ შეტევების, ინციდენტების და მუქარების ტიპები, მათი იდენტიფიცირება და შესაბამისი ტექნიკური საშუალებებით კომპიუტერული უსაფრთხოების უზრუნველყოფა.
სასწავლო კურსის სტატუსი	სავალდებულო
ECTS	5.00
სწავლის საფეხური	საბაკალავრო
სწავლების სემესტრი	4

#	ლექტორი	სამუშაო ადგილი	აკადემიური სარისხი	აკადემიური თანამდებობა კავკასიის უნივერსიტეტში	საკონტაქტო ტელეფონი	CU ელ-ფოსტა
1	გიორგი ახალაია	სამეცნიერო კიბერ უსაფრთხოების ასოციაცია - ტექნიკური დირექტორი	დოქტორი	ასოცირებული პროფესორი	598590158	gakhalaia@cu.edu.ge

კონსულტაციის დრო - შაბათი - 12:00 საათი

სასწავლო კურსის ფორმატი	
ლექცია	26 საათი
სემინარი	საათი
შუალედური/დასკვნითი გამოცდა	4.00 საათი
დამოუკიდებელი მუშაობა	95 საათი
კონსულტაცია	6 საათი

სასწავლო კურსის მიზანი	კურსის მიზანია სტუდენტებს შეასწავლოს კომპიუტერული უსაფრთხოების საფუძვლები და ძირითადი პრინციპები.

სწავლის შედეგი	საგნის შესწავლის შედეგად სტუდენტნი გამოიმუშავებს შემდეგ კომპეტენციებს: ცოდნა და გაცნობიერება • კომპიუტერული უსაფრთხოების აუცილებლობის ცოდნა; • სხვადასხვა დაცვის მექანიზმების ტექნიკური განხორციელების უნარი სისტემაში; • ფაილების დაცვის განხორციელების და სხვადასხვა ტიპის წვდომის კონტროლის საშუალებების ცოდნა; • ინტერნეტში უსაფრთხო ინფორმაციის მიღება/გაცვლა/დამუშავების განხორციელების საშუალებების ცოდნა; • უსაფრთხოების სხვადასხვა მოდელების ცოდნა; • სისტემაში აუთენტიფიკაციის და ავტორიზაციის მექანიზმების მართვის ცოდნა; • უკაბელო ქსელის უსაფრთხოების ძირითადი პრიციპების და ტექნიკური გადაწყვეტილებების განხორციელების უნარი; ცოდნის პრაქტიკაში გამოყენების უნარი • სისტემის უსაფრთხოების სხვადასხვა ტექნიკური საშუალებებით უზრუნველყოფის უნარი; • ფაილების უსაფრთხოების უზრუნველყოფის უნარი; • სისტემაში ინფორმაციის დაშიფრვის საშუალებების ცოდნა; • სხვადასხვა სახის პროტოკოლების უსაფრთხო გამოყენების უნარი; • კიბერ მუქარების და შეტევების იდენტიფიცირების უნარი; • ორგანიზაციის უსაფრთხოების პოლიტიკის გათვალისწინებით, არსებული სიტუაციის ანალიზის შედეგად რისკების მოპყრობის/მართვის და უსაფრთხოების გეგმის შემუშავების უნარი; დასკვნის გაკეთების უნარი • სისტემასა და ქსელში მოწყვლადობების აღმოჩენის, უსაფრთხოების შეფასების, კიბერ მუქარების კლასიფიკაციისა და უსაფრთხოებისათვის საჭირო შესაბამისი ძირითადი მექანიზმებისა და საშუალებების განხორციელების უნარი.

სავალდებულო ლიტერატურა	CEH Certified Ethical Hacker All-in-One Exam Guide Matt Walker 2012 Matt Walker 2012

დამხმარე ლიტერატურა და ინფორმაციის სხვა წყაროები	CEH™ Certified Ethical Hacker Study Guide Sean-Philip Oriyano 2016 Sean-Philip Oriyano 2016

სწავლებისა და სწავლის მეთოდები	1. ვერბალური, ანუ ზეპირსიტყვიერი მეთოდი. 2. პრაქტიკული მეთოდები 3. დისკუსია/დებატები 4. პრობლემაზე დაფუძნებული სწავლება 5. შემთხვევის ანალიზი (Case study) 6. ელექტრონული სწავლება (E-learning)

სტუდენტის მიმართ წაყენებული მოთხოვნები	სტუდენტი ვალდებულია: - შეასრულოს სასწავლო კურსით გათვალისწინებული დავალებები; - დაესწროს ლექცია-სემინარებს და პრაქტიკულ მეცადინეობებს; - არ შეუშალოს ხელი სასწავლო პროცესის მიმდინარეობას; - გამოცდების ჩაბარების დროს იხელმძღვანელოს გამოცდების ჩატარების შესახებ უნივერსიტეტში მოქმედი რეგულაციებით; - სემესტრის ბოლოს, შეაფასოს აკადემიური და ადმინისტრაციული პერსონალის მუშაობა; - დაიცვას უნივერსიტეტში დადგენილი სხვა წესები.

ცოდნისა და უნარ–ჩვევების შეფასების სისტემა
შეფასების მიზანია იმის გარკვევა, თუ რამდენად არის მიღწეული სასწავლო კურსით განსაზღვრული სწავლის შედეგები. სტუდენტთა შეფასება არის მრავალკომპონენტიანი და უზრუნველყოფს კურსის მიზნებისა და სწავლის შედეგების შეფასებას, რაც მიიღწევა კონკრეტული და გაზომვადი კრიტერიუმებისა და რუბრიკების გამოყენებით. სტუდენტთა შეფასება ეფუძნება შეფასების ოთხ ძირითად პრინციპს: ობიექტურობა, სანდოობა, ვალიდურობა, გამჭვირვალობა. სტუდენტთა შეფასებისას გამოიყენება ორი ტიპის შეფასება: განმსაზღვრელი და განმავითარებელი. განმსაზღვრელი შეფასების მიზანია სტუდენტის მიღწევის ზუსტი შეფასება. იგი აკონტროლებს სწავლის ხარისხს, ადგენს სტუდენტის მიღწევის დონეს სასწავლო კურსით განსაზღვრულ მიზნებთან მიმართებით. განმავითარებელი შეფასება სტუდენტის განვითარებაზეა მიმართული. იგი აწვდის სტუდენტს მიღწევებთან დაკავშირებით უკუკავშირს.
შეფასება 100-ქულიანი სისტემით მიმდინარეობს. შეფასების სისტემა უშვებს: ა) ხუთი სახის დადებით შეფასებას: ა.ა) (A) ფრიადი - შეფასების 91-100 ქულა; ა.ბ) (B) ძალიან კარგი - მაქსიმალური შეფასების 81-90 ქულა; ა.გ) (C) კარგი - მაქსიმალური შეფასების 71-80 ქულა; ა.დ) (D) დამაკმაყოფილებელი - მაქსიმალური შეფასების 61-70 ქულა; ა.ე) (E) საკმარისი - მაქსიმალური შეფასების 51-60 ქულა; ბ) ორი სახის უარყოფით შეფასებას: ბ.ა) (FX) ვერ ჩააბარა - მაქსიმალური შეფასების 41-50 ქულა, რაც ნიშნავს, რომ სტუდენტს ჩასაბარებლად მეტი მუშაობა სჭირდება და ეძლევა დამოუკიდებელი მუშაობით დამატებით გამოცდაზე ერთხელ გასვლის უფლება; ბ.ბ) (F) ჩაიჭრა - მაქსიმალური შეფასების 40 ქულა ან ნაკლები, რაც ნიშნავს, რომ სტუდენტის მიერ ჩატარებული სამუშაო არ არის საკმარისი და მას საგანი ახლიდან აქვს შესასწავლი.
სტუდენტს კრედიტი ენიჭება საბოლოო შეფასების საფუძველზე, რომელიც შედგება შუალედურ და დასკვნით შეფასებებში მიღებული ქულათა ჯამისაგან. სტუდენტის სწავლის შედეგების მიღწევის დონის შეფასება მოიცავს შუალედურ და დასკვნით შეფასებებს, რომელთათვისაც შეფასების საერთო ქულიდან (100 ქულა) საბოლოო შეფასებაში განსაზღვრულია ხვედრითი წილი და დადგენილია მინიმალური კომპეტენციის ზღვარი. კერძოდ, მაქსიმალური 100 ქულიდან შუალედური შეფასების ხვედრითი წილი არის 70 ქულა, ხოლო დასკვნითი შეფასების - 30 ქულა. შუალედური და დასკვნითი შეფასებების ორივე კომპონენტში დადგენილია მინიმალური კომპეტენციის ზღვარი. შუალედურ შეფასებებში განსაზღვრულია შეფასების მეთოდები, რომლებიც ჯამურად შეადგენენ 70 ქულას. შეფასების თითოეული მეთოდისთვის, შეფასება ეყრდნობა წინასწარ განსაზღვრულ სწავლების მიზანსა და დავალების ფორმაზე ორიენტირებულ, ზუსტ, მკაფიო კრიტერიუმებს და მასზე დაყრდნობით შემუშავებულ შეფასების სქემებს/რუბრიკებს. სტუდენტმა შუალედურ შეფასებებში ჯამურად უნდა დააგროვოს 70 ქულის სულ მცირე 59%, რომ მოიპოვოს დასკვნით გამოცდაზე გასვლის უფლება. სტუდენტს დასკვნითი/დამატებითი გამოცდა ჩაბარებულად ეთვლება, თუ მან მიიღო 30 ქულის სულ მცირე 60%. სტუდენტი უფლებამოსილია გავიდეს დამატებით გამოცდაზე, თუ იგი ვერ გადალახავს დასკვნითი გამოცდის მინიმალური კომპეტენციის ზღვარს. სტუდენტს დამატებით გამოცდაზე გასვლის უფლება აქვს აკადემიური კალენდრით დადგენილ პერიოდში, დასკვნითი გამოცდის შედეგების გამოცხადებიდან არანაკლებ 5 დღის ვადაში. საბოლოო შეფასებაში 0-50 ქულის ან შეფასების რომელიმე კომპონენტში (შუალედური/დასკვნითი) მინიმალური კომპეტენციის ზღვრის ვერ გადალახვის შემთხვევაში სტუდენტს უფორმდება F-0 ქულა.

ცოდნის შეფასების ფორმები და კრიტერიუმები				
გამოკითხვის ფორმა	გამოკითხვის რაოდენობა	გამოქვითული გამოკითხვის რაოდენობა	შეფასება	სულ ქულათა რაოდენობა
შუალედური გამოცდა	1	0	20.00	20.00
ფინალური გამოცდა	1	0	30.00	30.00
ზეპირი გამოკითხვა (გამოქვითვის მეთოდით)	6	1	2.00	10.00
ტესტი/საკონტროლო წერა (გამოქვითვის მეთოდით)	5	1	5.00	20.00
ჯგუფური პრეზენტაცია	1	0	11.00	11.00
საშინაო დავალება	3	0	3.00	9.00
ბონუსი	1	0	2.00	0.00
			ჯამი:	100.00

შეფასების კომპონენტები	შეფასების კრიტერიუმები
შუალედური გამოცდა	ტარდება წერითი სახით და მოიცავს გამოცდამდე განვლილ მასალას. ტესტი შედგება დახურული და ღია კითხვებისგან.
ფინალური გამოცდა	კურსის განმავლობაში განვლილი მთლიანი მასალა
ზეპირი გამოკითხვა (გამოქვითვის მეთოდით)	ლექციაზე აქტიურობა
ტესტი/საკონტროლო წერა (გამოქვითვის მეთოდით)	ტარდება წერითი სახით და მოიცავს ტესტირებამდე განვლილ მასალას. ტესტი შედგება დახურული და ღია კითხვებისგან.
ჯგუფური პრეზენტაცია	2-3 კაციანი ჯგუფები. წინასწარ შეთანხმებული თემის მიხედვით
საშინაო დავალება	პრაქტიკული დავალება
ბონუსი	ბონუს დავალება

ლექციებისა და სემინარების სემესტრში საათობრივი გადანაწილება	
I.0 კვირა	ლექცია 2.00 საათი
II.0 კვირა	ლექცია/სემინარი 2.00 საათი ზეპირი გამოკითხვა (გამოქვითვის მეთოდით)
III.0 კვირა	ლექცია/სემინარი 2.00 საათი ტესტი/საკონტროლო წერა (გამოქვითვის მეთოდით)
IV.0 კვირა	ლექცია/სემინარი 2.00 საათი ზეპირი გამოკითხვა (გამოქვითვის მეთოდით) საშინაო დავალება
V.0 კვირა	ლექცია/სემინარი 2.00 საათი ტესტი/საკონტროლო წერა (გამოქვითვის მეთოდით)
VI.0 კვირა	ლექცია/სემინარი 2.00 საათი ტესტი/საკონტროლო წერა (გამოქვითვის მეთოდით)
VII.0-IX კვირა	შუალედური გამოცდა 2.00 საათი
X.0 კვირა	ლექცია/სემინარი 2.00 საათი ზეპირი გამოკითხვა (გამოქვითვის მეთოდით) საშინაო დავალება
XI.0 კვირა	ლექცია 2.00 საათი
XII.0 კვირა	ლექცია/სემინარი 2.00 საათი ზეპირი გამოკითხვა (გამოქვითვის მეთოდით)
XIII.0 კვირა	ლექცია/სემინარი 2.00 საათი საშინაო დავალება ტესტი/საკონტროლო წერა (გამოქვითვის მეთოდით)
XIV.0 კვირა	ლექცია/სემინარი 2.00 საათი ზეპირი გამოკითხვა (გამოქვითვის მეთოდით) ჯგუფური პრეზენტაცია
XV.0 კვირა	ლექცია/სემინარი 2.00 საათი ტესტი/საკონტროლო წერა (გამოქვითვის მეთოდით) ზეპირი გამოკითხვა (გამოქვითვის მეთოდით)
XVI.0 კვირა	ლექცია/სემინარი 2.00 საათი ბონუსი
XVII.0-XIX კვირა	დასკვნითი გამოცდა 2.00 საათი
XX კვირა	დასკვნითი გამოცდის გადაბარება

სასწავლო კურსის შინაარსი	
მეცადინეობების კალენდარული გეგმა	
თარიღი	მეცადინეობის თემა, საშინაო დავალება, ლიტერატურა
ლექცია -2.00 საათიანი **თარიღი** 2022-09-09 **საათი** 13:30-15:25 **აუდიტორია** B14	**თემა** 1 ინფორმაციული უსაფრთხოების და კიბერ უსაფრთხოების საფუძვლები, პრინციპები, მათი ძირითადი მიმართულებები. **განსახილველი საკითხები** • რატომ არის საჭირო უსაფრთხოება? • Information Security და Cyber Security • რისკის შემცველი ფაქტორები • კიბერ უსაფრთხოების აუცილებლობა • კიბერ უსაფრთხოების ძირითად მიმართულებები • კიბერ უსაფრთხოების ძირითადი მოვალეობები • ტერმინოლოგია **სავალდებულო ლიტერატურა** CEH Certified Ethical Hacker All-in-One Exam Guide (1-27) **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა'** 'ლექტორის მიერ მოწოდებული მასალა, ელექტრონული რესურსები
ლექცია -2.00 საათიანი **თარიღი** 2022-09-16 **საათი** 13:30-15:25 **აუდიტორია** B14	**თემა** 2 Reconnaissance, ინფორმაციის შეგროვება და სკანირება **განსახილველი საკითხები** • სადაზვერვო მოქმედებები კიბერ უსაფრთხოებაში • ინფორმაციის შეგროვება • სკანირება კიბერ უსაფრთხოებაში • ქსელში აქტიური მანქანების გამოვლენა • Vulnerability Research • Footprinting • TCP და UDP პროტოკოლების საწყისები • სკანირება TCP და UDP პროტოკოლის გამოყენებით • სკანირებისთვის სხვადასხვა პროგრამების გამოყენება • DNS-ის საწყისები და მისი გამოყენება ინფორმაციის შესაგროვებლად • Google Hacking **სავალდებულო ლიტერატურა** CEH Certified Ethical Hacker All-in-One Exam Guide (53-121) **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა'** 'ლექტორის მიერ მოწოდებული მასალა, ელექტრონული რესურსები ზეპირი გამოკითხვა (გამოქვითვის მეთოდით)
ლექცია -2.00 საათიანი **თარიღი** 2022-09-23 **საათი** 13:30-15:25 **აუდიტორია** B14	**თემა** 3 ქსელური უსაფრთხოება და Sniffing-ი (ნაწილი #1) **განსახილველი საკითხები** • რა არის სნიფინგი • აქტიური და პასიური სნიფინგი • ARP, MAC, L2 მიმოხილვა • სნიფინგისთვის საჭირო პროგრამების და ხელსაწყოების გამოყენება • სნიფინგი და IDS სისტემები • Firewall-ები • Firewall-ის ტიპების, მათი გამოყენების ტექნიკის და ტექ. ექსპლუატაცის განხილვა • ანტივირუსების ტიპები და მათი მუშაობის პრინციპი **სავალდებულო ლიტერატურა** CEH Certified Ethical Hacker All-in-One Exam Guide (121-155) **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა'** 'ლექტორის მიერ მოწოდებული მასალა, ელექტრონული რესურსები ტესტი/საკონტროლო წერა (გამოქვითვის მეთოდით)

ლექცია -2.00 საათიანი **თარიღი** 2022-09-30 **საათი** 13:30-15:25 **აუდიტორია** B14	**თემა** 4 ქსელური უსაფრთხოება და Sniffing-ი (ნაწილი #2) **განსახილველი საკითხები** • რა არის სნიფინგი • აქტიური და პასიური სნიფინგი • ARP, MAC, L2 მიმოხილვა • სნიფინგისთვის საჭირო პროგრამების და ხელსაწყოების გამოყენება • სნიფინგი და IDS სისტემები • Firewall-ები • Firewall-ის ტიპების, მათი გამოყენების ტექნიკის და ტექ. ექსპლუატაცის განხილვა • ანტივირუსების ტიპები და მათი მუშაობის პრინციპი **სავალდებულო ლიტერატურა** CEH Certified Ethical Hacker All-in-One Exam Guide (121-155) **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა'** 'ლექტორის მიერ მოწოდებული მასალა, ელექტრონული რესურსები ზეპირი გამოკითხვა (გამოქვითვის მეთოდით) საშინაო დავალება
ლექცია -2.00 საათიანი **თარიღი** 2022-10-07 **საათი** 13:30-15:25 **აუდიტორია** B14	**თემა** 5 ქსელური ტრაფიკის მართვა; კავშირის უზრუნველყოფის ალტერნატიული მეთოდები და უსაფრთხოება **განსახილველი საკითხები** • კავშირის ტიპები • უსაფრთხო კავშირის მიმოხილვა; აუცილებელი პარამეტრები • ტრაფიკის გადამისამართება • Proxy ის მუშაობის პრინციპები; • ქსელური ტრაფიკის მართვის პროგრამული პაკეტები • ქსელში კავშირის შიფრაცია; დაცვის მექანიზმები • VPN ის მუშაობის პრინციპი და შესაბამისი პროგრამული პაკეტების მიმოხილვა • პროგრამული პაკეტების გამოყენების სიმულაცია **სავალდებულო ლიტერატურა** CEH Certified Ethical Hacker All-in-One Exam Guide **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა'** 'West J., Dean T., Andrews J. - CompTIA Network Guide to Networks, Seventh Edition - 2016 ტესტი/საკონტროლო წერა (გამოქვითვის მეთოდით)
ლექცია -2.00 საათიანი **თარიღი** 2022-10-21 **საათი** 13:30-15:25 **აუდიტორია** B14	**თემა** 6 სისტემაზე შეტევა **განსახილველი საკითხები** • პაროლების სტრუქტურის გათავისება • სისტემაში პაროლების შენახვის და მენეჯმენტის განხილვა • Authentication • Password Cracking • Key loggers and other spyware technology • Malware • Malware_ების ტიპები და მათი მუშაობის მექანიზმები • OS.-ზე შეტევა **სავალდებულო ლიტერატურა** CEH Certified Ethical Hacker All-in-One Exam Guide (155 - 193) **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა'** 'ლექტორის მიერ მოწოდებული მასალა, ელექტრონული რესურსები ტესტი/საკონტროლო წერა (გამოქვითვის მეთოდით)
2.00 საათიანი შუალედური გამოცდა	

ლექცია -2.00 საათიანი **თარიღი** 2022-11-11 **საათი** 18:00-19:50 **აუდიტორია** B14	**თემა** 7 Social Engineering and Physical Security **განსახილველი საკითხები** • სოციალური ინჟინერია და მისი გამოყენება • დაცვა სოციალური ინჟინერიისგან • სოციალური ინჟინერიის სხვადასხვა ტიპების მიმოხილვა • Phishing • სოციალური ინჟინერია და სტატისტიკა • ფიზიკური უსაფრთხოება • ფიზიკური უსაფრთხოების ხელსაწყოები **სავალდებულო ლიტერატურა** CEH Certified Ethical Hacker All-in-One Exam Guide (193 - 219) **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა'** 'ლექტორის მიერ მოწოდებული მასალა, ელექტრონული რესურსები ზეპირი გამოკითხვა (გამოქვითვის მეთოდით) საშინაო დავალება
ლექცია -2.00 საათიანი **თარიღი** 2022-11-18 **საათი** 15:45-17:40 **აუდიტორია** B14	**თემა** 8 Web based hacking: Servers and Applications **განსახილველი საკითხები** • ვებ სერვერების ტიპები • სხვადასხვა სახის ვებ შეტევების მიმოხილვა • ვებ სერვისების სუსტი მხარეების გამოვლენა • ვებ შეტევებისთვის საჭირო სხვადასხვა სახის მოწყობილობების გამოყენებადობის განხილვა • ვებ შეტევებისგან თავდაცვა **სავალდებულო ლიტერატურა** CEH Certified Ethical Hacker All-in-One Exam Guide (219 - 251) **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა'** 'ლექტორის მიერ მოწოდებული მასალა, ელექტრონული რესურსები
ლექცია -2.00 საათიანი **თარიღი** 2022-11-25 **საათი** 13:30-15:25 **აუდიტორია** B14	**თემა** 9 უკაბელო ქსელის უსაფრთხოება (ნაწილი #1) **განსახილველი საკითხები** • უკაბელო ქსელის მიმოხილვა • WiFi სიხშირეები და მათი სტანდარტები • უკაბელო ქსელის უსაფრთხოებისთვის საჭირო მექანიზმების განხილვა • უკაბელო ქსელზე არსებული შეტევების მიმოხილვა • WEP, WPA, WPA • უკაბელო ქსელებში უსაფრთხოებისთვის და კომპრომაციისთვის საჭირო პროგრამების განხილვა • უკაბელო ქსელის გამოყენება არ გამოყენების სიტუაციური მოდელის განხილვა **სავალდებულო ლიტერატურა** CEH Certified Ethical Hacker All-in-One Exam Guide (251 - 283) **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა'** 'ლექტორის მიერ მოწოდებული მასალა, ელექტრონული რესურსები ზეპირი გამოკითხვა (გამოქვითვის მეთოდით)

ლექცია -2.00 საათიანი **თარიღი** 2022-12-02 **საათი** 13:30-15:25 **აუდიტორია** B14	**თემა** 10 უკაბელო ქსელის უსაფრთხოება (ნაწილი #2) **განსახილველი საკითხები** • უკაბელო ქსელის მიმოხილვა • WiFi სიხშირეები და მათი სტანდარტები • უკაბელო ქსელის უსაფრთხოებისთვის საჭირო მექანიზმების განხილვა • უკაბელო ქსელზე არსებული შეტევების მიმოხილვა • WEP, WPA, WPA2 • უკაბელო ქსელებში უსაფრთხოებისთვის და კომპრომაციისთვის საჭირო პროგრამების განხილვა • უკაბელო ქსელის გამოყენება არ გამოყენების სიტუაციური მოდელის განხილვა **სავალდებულო ლიტერატურა** CEH Certified Ethical Hacker All-in-One Exam Guide (251 - 283) **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა'** 'ლექტორის მიერ მოწოდებული მასალა, ელექტრონული რესურსები საშინაო დავალება ტესტი/საკონტროლო წერა (გამოქვითვის მეთოდით)
ლექცია -2.00 საათიანი **თარიღი** 2022-12-09 **საათი** 13:30-15:25 **აუდიტორია** B14	**თემა** 11 Spyware, Trojan და სხვადასხვა ქსელური ტიპის შეტევების მიმოხილვა. (ნაწილი #1) **განსახილველი საკითხები** • Spyware • Trojans • ტროიანის გავრცელების მეთოდები • ტროიანის გავრცელების შემდგომი შედეგები • DoS შეტევა • DDoS შეტევა • Smurf Attack • Session Hijacking • Sequence Prediction **სავალდებულო ლიტერატურა** CEH Certified Ethical Hacker All-in-One Exam Guide (283 - 311) **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა'** 'ლექტორის მიერ მოწოდებული მასალა, ელექტრონული რესურსები ზეპირი გამოკითხვა (გამოქვითვის მეთოდით) ჯგუფური პრეზენტაცია
ლექცია -2.00 საათიანი **თარიღი** 2022-12-16 **საათი** 13:30-15:25 **აუდიტორია** B14	**თემა** 12 Spyware, Trojan და სხვადასხვა ქსელური ტიპის შეტევების მიმოხილვა. (ნაწილი #2) **განსახილველი საკითხები** • Spyware • Trojans • ტროიანის გავრცელების მეთოდები • ტროიანის გავრცელების შემდგომი შედეგები • DoS შეტევა • DDoS შეტევა • Smurf Attack • Session Hijacking • Sequence Prediction **სავალდებულო ლიტერატურა** CEH Certified Ethical Hacker All-in-One Exam Guide (283 - 311) **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა'** 'ლექტორის მიერ მოწოდებული მასალა, ელექტრონული რესურსები ტესტი/საკონტროლო წერა (გამოქვითვის მეთოდით) ზეპირი გამოკითხვა (გამოქვითვის მეთოდით)

ლექცია -2.00 საათიანი **თარიღი** 2022-12-23 **საათი** 13:30-15:25 **აუდიტორია** B14	**თემა** 13 კრიპტოგრაფია **განსახილველი საკითხები** • კრიპტოგრაფიის მნიშვნელობა • კრიპტოგრაფიის აუცილებლობა • როგორ მუშაობს კრიპტოგრაფია • კრიპტოგრაფიის ალგორითმების მიმოხილვა • კრიპტოგრაფიის გამოყენება სხვადასხვა დაცვის მექანიზმებში • შეტევები კრიპტოგრაფიის სხვადასხვა ალგორითმებზე • კრიპტოგრაფიის გამოყენება ყოველდღიურ ცხოვრებაში და მისი მეშვეობით კიბერ უსაფრთხოების უზრუნველყოფა • განვლილი მასალის გადახედვა • კურსის შეჯამება • დასკვნითი გამოცდისთვის მომზადება **სავალდებულო ლიტერატურა** CEH Certified Ethical Hacker All-in-One Exam Guide (27-53) **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა'** 'ლექტორის მიერ მოწოდებული მასალა, ელექტრონული რესურსები ბონუსი
2.00 საათიანი ფინალური გამოცდა	