Etik hakinq metodlarının tədrisi haqqında

Yadigar İmamverdiyev[1], Elşən Bağırov[2]
[1,2]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*yadigar@iit.science.az*, [2]*elsenbagirov1995@gmail.com*

***Xülasə*— Etik hakinq sistem və ya kompüter şəbəkəsində boşluqların, səhvlərin və ya zəif nöqtələrin tapılması prosesidir. Bu işdə ali məktəb tələbələrinə etik hakinq üzrə tədris kursunun keçirilməsinin vacibliyi tədqiq edilmiş, tədris zamanı meydana çıxan problemlər təhlil edilmişdir. O cümlədən, kursun məzmunu, tələbələrin davranış kodeksi, kursun tədrisi ilə bağlı bir sıra etik və hüquqi məsələlərə baxılmışdır.**

Açar sözlər— etik hakinq; informasiya təhlükəsizliyi; haker; tədris kursu; davranış kodeksi; kibertəhlükəsizlik

I. GİRİŞ

Kibertəhlükəsizliyin təmin edilməsi bütün ölkələr üçün prioritet məsələdir [1]. Bu cəhətdən son dövrlər etik hakinq metodlarının tədris olunması informasiya təhlükəsizliyi üzrə təhsilin zəruri komponentinə çevrilib [2]. Bu yanaşma yalnız müdafiə üsullarının tədrisinə əsaslanan yanaşma ilə müqayisədə daha hazırlıqlı peşəkar kadrlar yetişdirmək və ümumilikdə informasiya təhlükəsizliyini inkişaf etdirməyə imkan verir. Bir çox özəl konsaltinq qrupları böyüməkdə olan təşkilatlar üçün etik hakinq xidmətləri təklif edir. Lakin, bu böyük maliyyə vəsaiti tələb edir. Bunları nəzərə alaraq, institutda “İnformasiya mühafizəsi və təhlükəsizliyi” üzrə ixtisaslaşan magistrantların müasir tələblərə və çağırışlara uyğun hazırlanması, bu istiqamətdə aparılan elmi və praktiki işlərin təkmilləşdirilməsi məqsədilə institut rəhbərliyi tərəfindən şöbə qarşısında “Etik hakinq metodları” tədris kursunun işlənməsi və tədrisi məsələsi qoyulub.

Adətən, “hakinq” termini informasiya sistemində zəif yerlər tapmaqla sistemə icazəsiz girmək məqsədilə istifadə edilir. Lakin hakinq metodlarından cəmiyyətə faydalı məqsədlər üçün də istifadə etmək mümkündür. Çünki etik hakinq istənilən təşkilatda informasiya təhlükəsizliyinin səviyyəsini qiymətləndirməyin ən etibarlı yollarından biridir. Bu iş ona görə etik hesab edilir ki, yalnız informasiya sisteminin sahibinin xahişi ilə yerinə yetirilir və kompüter sisteminə zərər vurmadan, heç bir informasiya oğurlamadan arzuolunmaz müdaxilələrin qarşısını almaq məqsədini güdür. Etik hakinq boşluqları və nöqsanları aşkarlamaqla və aradan qaldırmaqla, səhvləri düzəltməklə təşkilatlara informasiya təhlükəsizliyinin səviyyəsini yüksəltmək imkanını verir [3, 4]. Bu səbəbdən etik hakerlər tərəfindən yerinə yetirilən nüfuzetmə testləri audit prosesi kimi qəbul edilir [4].

Dünyanın qabaqcıl universitetləri məzunların əmək bazarında rəqabətə dözümlü olması üçün informasiya təhlükəsizliyi üzrə nüfuzlu beynəlxalq sertifikatlar almasını da təşviq edirlər. Bu baxımdan, yaradılan tədris kursunda “Sertifikatlaşdırılmış Etik Haker” (Certified Ethical Hacker, CEH) sertifikat imtahanında əhatə olunan modullar nəzərə alınıb.

II. HAKERLƏRİN TİPLƏRİ

Hakerlərlə bağlı cəmiyyətdə belə bir stereotip vardır ki, onlar neqativ, kriminal, etik olmayan əməllər törədirlər. Halbuki, hakerlər yerinə yetirdiyi fəaliyyətlərinə görə bir neçə qruplara bölünür, həvəskar orta məktəb şagirdindən zərərli kriminalistlərə qədər bütün növ yaş kateqoriyalarından olan insanların həyatına nüfuz edə bilir [5].

A. Ağ şlyapalı hakerlər. Təhlükəsizlik mütəxəssisi və ya tədqiqatçısı kimi də tanınan etik hakerlərdir. Belə hakerlərə şirkətin bir işçisi kimi fəaliyyət göstərərək, boşluqları istismar etməyə icazə verilir [6, 7]. Çünki, bu şəxslər nüfuzetmə testlərini reallaşdırmağa qabil olan, adətən Elektron Ticarət Məsləhətçilərinin Beynəlxalq Şurası (The International Council of Electronic Commerce Consultants, EC-Council) tərəfindən lisenziyalaşdırılmış hakerlərdir. Belə hakerlərin qarşısında duran vəzifələrdən biri öz bilik və bacarıqlarını digər şəxslərə təhlükəsizliyi təmin etmək baxımından yalnız fayda vermək yolu ilə istifadə etməkdir [5, 8].

B. Qara şlyapalı hakerlər. Təhlükəsizlik üzrə öz yüksək bilik və bacarıqlarını neqativ məqsədlər üçün istifadə edən şəxslərdir və media tərəfindən sadəcə olaraq “haker” kimi də tanınırlar [8]. Fərdlər və təşkilatlar öz kritik informasiya aktivlərini, kompüterlərini belə növ hakerlərdən qorumaq üçün səfərbər olunmuşdur.

C. Boz şlyapalı hakerlər. Boz şlyapalı haker kompüter hakeri və ya kompüter üzrə təhlükəsizlik ekspertidir. O, bəzən qanunları və etik standartları pozur, lakin, onun məqsədi qara şlyapalı haker kimi zərərli yox, yalnız əyləncə xarakteri daşıya bilər [8]. Boz şlyapalı hakerlər daha çox ağ şlyapalı hakerlərə oxşayırlar. Fərq ondan ibarətdir ki, boz şlyapalı hakerlər sistem və ya şəbəkəni icazəsiz sındıraraq, şirkət rəhbərliyinə boşluğun necə istismar edildiyini deyil, yalnız müəyyən məbləğ qarşılığında onun necə aradan qaldırılmasını təklif edir. Onlar seçdiyi istiqamətin qanuni və ya qanunsuz olduğunu dərk edir, lakin çox vaxt neqativ istiqamətdə fəaliyyət göstərməyi üstün tuturlar [9].

III. ETİK HAKİNQ METODLARI KURSUNUN TƏLƏBLƏRİ

A. Kursun məzmunu. Müvafiq ixtisas üzrə təhsil alan magistrantlar kiber-hücum üçün zəruri informasiyanın

DOI: 10.25045/NCInfoSec.2019.40

toplanması, şəbəkənin daranması və resursların inventarlaşdırılması, şəbəkə protokolları, əməliyyat sistemləri və tətbiqi proqramlarda boşluqların analizi, əməliyyat sistemlərinin hakinqi, zərərli proqramların analizi, veb-serverlərin və simsiz şəbəkələrin sındırılması, informasiya təhlükəsizliyi vasitələrindən yayınma üsulları, nüfuzetmə testləri, DoS hücumlar və SQL-inyeksiya hücumlarının həyata keçirilməsi, seansların ələ keçirilməsi və s. kimi mövzuları nəzəri cəhətdən öyrənir və xüsusi (təcrid olunmuş) laboratoriya mühitində etik hakinq üsulları üzrə praktiki məsələləri yerinə yetirir [10,11].

B. Fiziki tələblər. Kursa hazırlıq üçün tələb olunan əsas fiziki hazırlıq müddəalarına aşağıdakıları misal göstərmək olar:

- kurs üzvlərinin hər birinin yüksək məhsuldarlığa malik kompüterlə təchiz olunması və yüksək sürətli internetə çıxışının təmin edilməsi;
- kompüterlərdə virtual maşın mühitində “Kali Linux” əməliyyat sisteminin quraşdırılması;
- onlayn rejimdə hakinq bacarıqlarının test edilməsi üçün xidmət göstərən veb serverin quraşdırılması və s.

Bundan başqa öyrənənlərin informasiya texnologiyaları, kompüter elmləri və digər əlaqədar ixtisaslar üzrə bakalavr və ya magistr dərəcəsinə mənsub olması və eyni zamanda, kompüter şəbəkələri, kompüter və onun periferik qurğuları, proqramlaşdırma biliklərinə mənsub olması, proqram təminatından düzgün istifadə siyasətinə riayət etmək kimi etik tələblər də mövcuddur.

Bütün nüfuzetmə test fəaliyyətlərinin avtorizə edilmiş rejimdə və qanun çərçivəsində yerinə yetirildiyindən əmin olmaq, zərərli hakerlərlə əlaqədə olmamaq və hər hansı zərərli fəaliyyət göstərməmək kimi tələblər irəli sürülür.

Əlavə olaraq, kibertəhlükəsizlik üzrə lokal və ya beynəlxalq yarışların keçirilməsi tələbələrin bir-biri ilə və təşkilatın mütəxəssisləri ilə sosial əlaqələrinin genişləndirilməsi, onların davranışının müsbət istiqamətdə yönəlməsi, qara şlyapalı hakerlərin neqativ cəhətləri və etik hakerlərin vacibliyini görmək üçün olduqca faydalıdır [12]. Belə yarışmalardan biri etik hakinqdə ən geniş yayılmış tədbir olan “Bayrağı ələ keçir!” (Capture the Flag, CTF) adı altında təşkil olunan yarışlarıdır. Burada iştirakçılar əvvəlcədən təyin olunmuş kiçik tapşırıqları yerinə yetirərək müxtəlif səviyyələrdə qiymətləndirmə üçün istifadə olunan bayraqları əldə etməlidirlər [13].

IV. ETİK HAKİNQ METODLARININ TƏDRİSİ İLƏ BAĞLI ETİK VƏ HÜQUQİ MƏSƏLƏLƏR

Etik hakinq metodlarının tədrisi ilə bağlı müəyyən etik və hüquqi məsələlər də meydana çıxır [2, 14]. Bəzi təhsilalanların öyrəndikləri hücum metodlarını və alətlərini məsuliyyətsiz şəkildə tətbiq edə biləcəyi ehtimalını nəzərə almaq zəruridir. Etik hakinq kurslarının iştirakçıları arasında keçirilən rəy sorğuları da bu ehtimalı təsdiqləyir.

Etik hakinq üsullarının öyrədilməsinə görə təşkilatların və pedaqoqların məsuliyyətini azaltmaq üçün bir sıra addımlar atılmalıdır. Əslində, etik davranış məsələsi informasiya təhlükəsizliyi üzrə hər bir tədris proqramının məcburi hissəsi olmalıdır. Etik hakinq metodları tədris edilən hər bir kursda hüquqi nəticələr və etik məsələlər müzakirə edilməlidir. Tələbələr anlamalıdırlar ki, hücum metodlarının öyrədilməsinin məqsədi kiber hücumların necə işlədiyini aydın başa düşməklə müdafiə metodlarını təkmilləşdirmək və müvafiq təhlükəsizlik həllərini tətbiq etməkdir.

Etik hakinq kursunu öyrənənlərin davranış kodeksini imzalaması nəzərdə tutulmalıdır. Həmin davranış kodeksində hər bir magistrantın davranış sərhədləri göstərilir və yolverilməz hərəkətlərin hüquqi nəticələri şərh olunur.

EC-Council tərəfindən hakerlər üçün davranış kodeksi hazırlanmışdır. Orada göstərilən müddəaların bəzisi aşağıda öz əksini tapmışdır [15]:

- İş mühitində əldə edilən fərdi məlumatları gizli və konfidensial saxlamaq (xüsusilə bu informasiya müştərilərə və onların şəxsi məlumatlarına aiddirsə), heç bir fərdi məlumatı (ad, elektron poçt ünvanı, sosial təhlükəsizlik nömrəsi, şəxsiyyət vəsiqəsinin nömrəsi və ya FİN kodu və digər unikal identifikasiya nömrəsi kimi məlumatları) müştərinin ilkin razılığı olmadan toplamaq, üçüncü tərəflə paylaşmamaq;
- başqalarının əqli mülkiyyət hüququnu pozmamaq;
- hər hansı bir elektron ticarət müştərilərinə, internet cəmiyyətinin üzvlərinə olan mümkün potensial təhlükə barədə uyğun şəxslərə və ya aiddiyyəti orqanlara məlumat vermək;
- qeyri-qanuni və ya qeyri-etik yolla əldə edilmiş proqram və ya proseslərdən bilərəkdən istifadə etməmək;
- aldadıcı maliyyə əməliyyatları (rüşvət, ikiqat faktura və digər) ilə məşğul olmamaq;
- kompüter şəbəkələrini təhlükə altına salmağa yönəlmiş qara şlyapalı hakerlər cəmiyyətində iştirak etməmək [15];

V. ETİK HAKİNQ METODLARININ TƏDRİSİ ZAMANI MEYDANA ÇIXAN PROBLEMLƏR

Etik hakinq metodlarının tədrisi ilə bağlı iki mühüm risklərin meydana gəldiyini vurğulamaq vacibdir. Birincisi, tələbələr kurs ərzində öyrəndiyi bilik və bacarıqlardan sui-istifadə edərək cəmiyyət üçün risk rolunu oynaya bilər. Bu isə onların gələcəkdə qara şlyapalı hakerə çevrilməsinə şərait yarada bilər. Başqa bir risk isə tədris kursu ərzində müəllimlə birlikdə yerinə yetirilmiş qeyri-qanuni fəaliyyətin tələbələr üçün risk yarada bilməyidir.

Etik hakinq metodlarının təcrid edilmiş mühitdə test edilməsi nəticəsiz qala bilər. Belə ki, qara şlyapalı hakerlər sistemi istismar etməzdən öncə boşluqları tapmalıdır. Bunun üçün onlardan kifayət qədər vaxt və səbr tələb olunur. Lakin, məhdud zaman çərçivəsində tələbələrdən bunu tələb etmək mümkünsüz görünür.

Təcrid edilmiş laboratoriya mühitində aparılan laboratoriya işləri üçün etik hakinq üsullarının icra edilməsi proseslərini hər hansı kompüter sisteminə zərər vurmadan təsvir edən öyrədici

xarakterli informasiya resuslarının qıtlığı mövcuddur [2, 4]. Buna görə də nəzəri hissəyə nisbətən tələbələrin hakinq üsullarını daha aydın təsəvvür etməsi üçün praktiki bacarıqların inkişaf etdirilməsində problemlər yaşanmaqdadır [16].

VI. ƏLAQƏDAR İŞLƏRİN İCMALI

[1]-də beynəlxalq təşkilatların və inkişaf etmiş bir sıra ölkələrin kibertəhlükəsizlik ixtisası üzrə bakalavr və magistr səviyyələrində ali təhsil standartları və qabaqcıl universitetlərin informasiya təhlükəsizliyi sahəsində təhsil proqramları analiz edilmişdir.

İnformasiya texnologiyalarının, eləcə də hakerlərin çevik surətdə inkişaf etməsi informasiya təhlükəsizliyinin təmin edilməsi istiqamətində mühüm addımlar atmağa vadar edir. Etik hakinq və ya nüfuzetmə testlərinin bir alət kimi istifadəsi təhlükəsizlik risklərini azaltmağa yardımçı olur. Lakin zərərli hakerlər əleyhinə belə üsulların bir çox menecerlər tərəfindən yayılmış dezinformasiya səbəbindən reallaşdırılmasından imtina edilir. [17]-də Malayziyadakı ali təhsil institutlarında haker qurbanlarının sayı analiz edilmiş, nüfuzetmə testlərinin İT təhlükəsizlik komponentinə çevrilməsinin vacibliyi, təhlükəsizlik menecerlərinə mövcud təhlükəsizlik mühiti üzərində nüfuzetmə testlərinin üstünlüyü tədqiq edilmişdir.

[16]-da ali məktəb tələbələrinə keçirilən kibertəhlükəsizlik üzrə təlimə mövcud yanaşmalar, onların üstün və çatışmayan cəhətləri, öyrətmə prosesi, müxtəlif növ laboratoriyalar və onların qurulması üçün tələblər, maarifləndirici oyunlar və yarışlar analiz edilmişdir.

NƏTİCƏ

Etik hakinq genişlənməkdə olan kibercinayətkarlardan və ya onların qruplaşmalarından kritik informasiya aktivlərini qorumaq üçün biznes və akademik təşkilatların ən vacib informasiya təhlükəsizliyi strategiyasına və alətinə çevrilməlidir. Çünki, etik hakerlərlə qara şlyapalı hakerlər arasındakı mübarizənin sona çatmayacağı proqnoz edilir.

Etik hakinq kursunun tədrisi öyrədilən bacarıqların zərərverici gücü və tələbələr üzərindəki neqativ təsirin azladılması məqsədilə öyrədənlərdən ciddi məsuliyyət tələb edildiyi aydın hiss olunur.

İSTİNADLAR

[1] Y. İmamverdiyev “Ali məktəblərdə kibertəhlükəsizlik üzrə mütəxəssis hazırlığı problemləri,” İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri IV respublika konfransı, s. 79–82, 2018.

[2] Z. Trabelsi, W. Ibrahim, “Teaching ethical hacking in information security curriculum: A case study,” IEEE Global Engineering Education Conference (EDUCON), pp. 130-137, 2013.

[3] B. Abu-Shaqra, R. Luppicini, “A technoethical study of ethical hacking communication and management within a Canadian University,” The Changing Scope of Technoethics in Contemporary Society, pp. 307-326, 2018.

[4] Y. Younis, K. Kifayat, L. Topham, et al., “Teaching Ethical Hacking: Evaluating Students’ Levels of Achievements and Motivations”, International Conference on Technical Sciences (ICST2019), pp. 554-559, 2019.

[5] B. Pashel, “Teaching students to hack: Ethical implications in teaching students to hack at the university level”, InfoSecCD Conference, pp.197-200, 2006.

[6] H. J. Kam, P. Menard, D. Ormond, P. Katerattanakul, “Ethical hacking: Addressing the critical shortage of cybersecurity talent,” PACIS, pp. 1-8, 2018.

[7] S. Patil, A. Jangra,M. Bhale et al., “Ethical hacking: The need for cyber security”, IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), pp. 1602-1606, 2017.

[8] A. S. Panimalar, P. Priyadharshini, R. Vijayabharathi, et al., “An overview of ethical hacking,” International Research Journal of Engineering and Technology (IRJET), vol. 5, pp.206-209, 2018.

[9] B. Sahare, A. Naik, S. Khandey, “Study of ethical hacking,” International Journal of Computer Science Trends and Technology (IJCST), vol. 2, pp. 6-10, 2014.

[10] R. Messier, “CEH v10 Certified Ethical Hacker Study Guide. 1st Edition”, Sybex, 2019, 592 p.

[11] S. Sinha, “Beginning ethical hacking with Kali Linux computational techniques for resolving security issues”, Apress, 2018, 440 p.

[12] R.E. Pike, “The “ethics” of teaching ethical hacking”, Journal of International Technology and Information Management, vol. 22, pp. 67-75, 2013.

[13] M. Lehrfeld, P. Guest, “Building an ethical hacking site for learning and student engagement”, SoutheastCon, pp. 1-6, 2016.

[14] A. M. Curbelo, A. Cruz, “Faculty attitudes toward teaching ethical hacking to computer and information systems undergraduates students”, Proceedings of the Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology, pp. 1-8, 2013.

[15] “Code of ethics”, https://www.eccouncil.org/code-of-ethics/

[16] L. Topham, K. Kifayat, Y. Younis, et al., “Cyber security teaching and learning laboratories: A survey”, Information & Security, vol.35, pp. 51-80, 2016.

[17] C. Kang, P. JosephNg, K. İssa, “A study on integrating penetration testing into the information security framework for Malaysian higher education institutions”, International Symposium on Mathematical Sciences and Computing Research (iSMSC), pp. 156-161, 2015.

ABOUT TEACHING ETHICAL HACKING METHODS

Yadigar Imamverdiyev[1], Elshan Baghirov[2]

[1,2]Institute of Information Technology of ANAS, Baku, Azerbaijan

[1]*yadigar@iit.science.az*, [2]*elsenbagirov1995@gmail.com*

Abstract— Ethical hacking is the process of finding vulnerabilities, weaknesses, and bugs through the system or computer networks. In this work, the importance of an ethical hacking course is investigated for high school students and the problems during the course of teaching. In addition, the student code of ethics, the content of course, and a number of ethical and legal issues related to the course teaching were explored.

Keywords— *ethical hacking; information security; hacker; teaching course; code of ethics; cybersecurity*