O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

“TASDIQLAYMAN”
O‘quv ishlari bo‘yicha prorektor
Dj.Sultanov
“____” _____ 2023-yil

Ro‘yxatga olindi: №_____
2023-yil “____” _____

ETHICAL HACKING I

O‘QUV DASTURI

Bilim sohasi: 600 000 - Axborot-kommunikatsiya texnologiyalari

Ta’lim sohasi: 610 000 - Axborot-kommunikatsiya texnologiyalari

Ta’lim yo‘nalishi: 60612100 - Kiberxavfsizlik injiniringi

Toshkent – 2023

Fan/modul kodi	O‘quv yili	Semestr	ECTS - kreditlar
	2023-2024	6	6
Fan/modul turi	**Ta’lim tili**		**Xaftadagi dars soatlari**
Majburiy	O‘zbek/rus		5

1.	Fanning nomi	Auditoriya mashg’ulotlari (soat)	Mustaqil ta’lim (soat)	Jami yuklama (soat)
	Foydalanishni boshqarish	**74**	**106**	**180**

2. I. Fanning mazmuni

Fanni o‘qitishdan maqsad – talabalarga kiberxavfsizlikni ta’minlash sohasida “Ethical hacking”ni nazariy va amaliy izlanishlar orqali tanishtirish hisoblanadi. “Ethical hacking”da foydalaniladigan turli zamonaviy yondashuvlar, usullar va vositalarni qo‘llashga doir bilimlar va ko‘nikmalar hosil qilishdan iborat.

Fanning vazifasi – talabalarga nazariy bilimlar, amaliy ko‘nikmalar berish, hamda “Ethical hacking” ning asosiy tushunchalari, kiberxavfsizlikda tahdidlar va zaifliklarni aniqlash va bartaraf etish, etik xakerlikda foydalaniladigan vositalarning ahamiyatini ochib berishdan iborat.

II. Asosiy nazariy qism (ma’ruza mashg’ulotlari)

II.I. Fan tarkibiga quyidagi mavzular kiradi:

1-mavzu. “Ethical hacking” tushunchasi va fanga kirish

Kursning qisqacha mazmuni va tarkibi. “Ethical hacking” va pentesting tushunchasi: xavfsizlik va pentesterlarning roli, pentesting usullari, tizim va tarmoq xavfsizligi xodimlari uchun sertifikatlash dasturlari va karyera. Qonuniylik va etika qoidalari.

2-mavzu. Ethical hackerlar uchun umumiy bilimlar manbasi

Bu soha uchun qo‘shimcha ma’lumotlar olish manbalari. Maxsus konferensiyalar: DEF CON, Black Hat konferensiyalari. DarkWeb tushunchasi: TOR brauser, hackerlik bozorlari, qidiruv tizimlari. Xakerlik tayyorlov kurslari, treyninglar, sohadagi xalqaro sertifikatlar. Kiber urushlar, terrorism. Davlat va nodavlat o‘yinchilar.

3-mavzu. TCP/IP konsepsiyasi mohiyati

TCP/IP modeli: ilova sathi, transport sathi, internet sathi. IP manzillash: IP-manzillarni rejalashtirish, IPv6 manzillash. 2 lik, 8 lik, 16 lik, Base-64 sanoq tizimlari mohiyati.

4-mavzu. Kompyuter tarmog‘i hujumlari

Zararli dasturlar: viruslar, makro-viruslar, tarmoq qurtlari, troyan otlari, josuslik dasturlari, reklama dasturlari. Zararli dasturlardan himoyalanish. Suqilib kirish hujumlari: DoS hujumi, DDoS hujumi, Buffer to‘lib toshishi, eavesdropping, MITM hujumi, seansni o‘g‘irlash(hijacking) hujumi. Fizik xavfsizlik masalalari: keylogger.

5-mavzu. Footprinting va Ijtimoiy muhandislik asoslari

Footprinting tushunchasi. Footprinting uchun veb-vositalar. Razvedka ishlarini olib borish: tashkilot veb sayti tahlili, boshqa footprinting vositalari, e-mail manzillari asosida, HTTP asosida, ma’lumotlarni to‘plash usullari. DNS zona transferi. Ijtimoiy muhandislik asoslari: yelka orqali qarash, ma’lumot titish(dumpster diving), noqonuniy foydalanish (piggybacking), fishing hujumlari.

6-mavzu. Kompyuter tarmoqlarida portlarni skanerlash asoslari

Port skanerlash tushunchasi: skanerlash turlari. Portlarni skanerlash vositalari: Nmap, Unicornscan, Nessus va OpenVAS. Ping skanerlash: Fping, Hping3, IP paketlarni tuslantirish(crafting). Skriptlash asoslari.

7-mavzu. Kiberxavfsizlikda “Enumeration” asoslari

“Enumeration” tushunchasi. Windows operatsion tizimida “enumeration”: NetBIOS asoslari, NetBIOS enumeratsiya vositalari, qo‘shimcha enumeratsiya vositalari. Unix(Linux) operatsion tizimida “enumeration”. SNMP.

8-mavzu. Kiberxavfsizlikda dasturlash asoslari

Dasturlash asoslari. C dasturlash tili. HTML asoslari. Perl dasturlash asoslari. OOP dasturlash asoslari. Python dasturlash asoslari: tushunchalar, python BLT tushunchasi, python shell(REPL), pythonda OOP. Ruby asoslari.

9-mavzu. Shaxsiy va Server kompyuterlar operatsion tizimidagi zaifliklar

Windows operatsion tizimida xavfsizlikdagi zaifliklar: windows fayl tizimi, masofaviy protseduralar chaqiruvi, NetBIOS, SMB, CIFS, “null sessions”, veb servislar, MS SQL serveri, buffer to‘lib toshishi, parollar va autentifikatsiya jarayonlarida zaifliklar. Windowsda zaifliklarni topish vositalari: Nessus Essentials. Windowsda zaifliklarga qarshi eng yaxshi amaliyotlar: “patching” asoslari, antivirus vositalari, log fayllar tahlili, passiv xizmatlar va portlarni o‘chirish. Linuxda zaifliklar: samba, zaifliklarni topish vositalari, qarshi himoya vositalari.

10-mavzu. O‘rnatilgan(Embedded) operatsion tizimlar va ularda kiberxavfsizlik asoslari

O‘rnatilgan(embedded) operatsion tizimlar. Windows va boshqa o‘rnatilgan operatsion tizimlar. O‘rnatilgan operatsion tizimlardagi zaifliklar: xususiyatlari va funksionalligi, zaifliklarni bartaraf etish(patching)ning qiyinligi, tarmoq qurilmalarida o‘rnatilgan tizimlar, xavfsizlik qurilmalarida, telefonlarda, smartfonlardagi zaifliklar. Rootkit. O‘rnatilgan operatsion tizimlarda zaifliklarga qarshi eng yaxshi amaliyotlar.

11-mavzu. Veb serverlarda xavfsizlik va kiberhujumlar

Veb ilovalarda xavfsizlik asoslari: veb ilovalar komponentalari, skriptlash tillari, ma’lumotlar bazalari. Veb ilovalarda zaifliklar: ilovalarda zaifliklar va qarshi choralar, veb ilovalar xavfsizligini baholash. Veb xakerlar va xavfsizlik testerlari uchun hujum vositalari: BurpSuite, ZedAttackProxy, Wapiti.

12-mavzu. Simsiz tarmoqlarda hujumlar va ulardan himoyalanish asoslari

Simsiz tarmoqlar asoslari. Simsiz tarmoq standartlari: IEEE 802.11 standarti, simsiz texnologiyalar, qo‘shimcha IEEE 802.11x loyihasi. Simsiz tarmoqlarda autentifikatsiya: 802.1x standarti. “Wardriving” tushunchasi va uning ishlash jarayoni, Vistumbler, Kismet. Simsiz tarmoqlarda xakerlik: xakerlik vositalari(aircrack-ng, WI-FI pineapple). Zaifliklarni aniqlash usullari va ularga qarshi choralar.

13-mavzu. “Ethical hacking”da kriptografiya asoslari

Kriptografiya asoslari va tarixi. Kriptografik algoritmlar: simmetrik, assimmetrik, elektron raqamli imzolar, maxfiy ma’lumotlarni shifrlash, xesh algoritmlar. PKI tushunchasi va uning komponentalari. Kriptografik hujumlar: tavallud sana hujumi, matematik hujum, brute-force hujum, MITM hujumi, SSL/TLS susaytirish hujumi, lug‘at hujumi, qaytalash (replay) hujumi. Parollarni buzish asoslari.

14-mavzu. Kompyuter tarmoqlarida himoya tizimlari va vositlari

Tarmoq qurilma(router)lari tushunchasi: tarmoq hujumlarini kamaytirishda routerlarning o‘rni, routerlar to‘g‘ri sozlash asoslari, ACL. Tarmoqlararo ekran vositalari: tarmoqlararo ekran texnologiyalarini baholash, tarmoqlararo ekran sozlanmalari, CISCO tarmoqlararo ekrani, tarmoqlararo ekran va router uchun risklar tahlili vositalari. Suqilib-

kirishlarni aniqlash va himoyalanish vositalri(IDS, IPS): Tarmoq asosidagi va host asosidagi IDS va IPS-lar, veb-filter vositalari, xavfsizlik operatsiyalari markazi. Honeypots va uning ishlash jarayoni.

15-mavzu. Xavfsizlikka yo‘naltirilgan operatsion tizimlar

Anonim operatsion tizimlar tushunchasi. Xavfsizlik va maxfiylik uchun yo‘naltirilgan operatsion tizimlar. Linux distroslari: Whonix operatsion tizimi imkoniyatlari, Qubes operatsion tizimi imkoniyatlari, Kali Linux operatsion tizimi imkoniyatlari, Parrot operatsion tizimi imkoniyatlari.

16-mavzu. Linux operatsion tizimi asoslari

Linux operatsion tizimi tarixi. Linux buyruqlari: ls, cd, finger, grep, ps, pstree, top, kill, mkdir, rm, mv, rmdir, chown, chmod, bg, fg, useradd, userdel, usermod, users, who buyruqlari. Direkroriya(directory)-lar: root, bin, sbin, etc, etc/passwd, etc/shadow, etc/group, etc/inittab, etc/motd, dev, boot, usr, var, proc direktoriyalar. Linux grafik foydalanuvchi interfeyslari: GNOME, KDE va boshqalar.

17-mavzu. Linux operatsion tizimi xavfsizligi va uni buzilishi

Linux operatsion tizimi sysfs fayl tizimi. Crond. Shell buyruqlari: touch, nice, locate. Linux tarmoqlararo ekrani: Iptable tushunchasi va uni sozlash. Syslog. Syslogd. Scripting. Linuxda parollar. Linux operatsion tizimini buzish: boot hack, backspace hack.

18-mavzu. Windows operatsion tizimi va unda hackerlik amaliyoti

Windows operatsion tizimi tarixi. “Boot” tushunchasi va uning ishlash jarayoni. Muhim windows fayllari. Windows log fayllari. Registrlar: usb ma’lumotlar, simsiz tarmoqlar, word hujjatlar, zararli dasturlar, o‘chirilgan dasturlar, parollar, UserAssist. Prefetch tushunchasi. Windows parolini xeshlash. Windows operatsion tizimini buzish texnikalari: xeshdan o‘tkazish, chntpw, NetUser script, tizim sifatida kirish, admin akkauntini topish. Windows scripting: net users, net view, net share, net service, netshell. Windows parolini buzish: oflayn NT registry editor, LCP, pwdump, ophcrack, John the Ripper. Windows OT-da zararkunanda dasturlarni topish: windows sysinternal. Cain and Abel

19-mavzu. Metasploit haqida fundamental tushunchalar

Metasploit tushunchasi. Metasploit tarixi va asoslari: exploit, payload, auxiliary, encoder. Metasploitning ishlash jarayoni. Msfconsole muhitidan foydalanish: sodda buyruqlar, qidiruv jarayonlari. Metasploit yordamida skanerlash: SMB skaner, SQL server skaner, SSH server skaner, anonim FTP serverlari skaneri. Exploitlardan foydalanish(misollar yordamida).

20-mavzu. Ethical hakerlik muhiti va uning tashkil etilishi

Shaxsiy pentesting laboratoriyasini tashkillashtirish: VirtualBox dasturini sozlash, Axigen mail serverini o‘rnatish, Kali Linux OVA muhitini yaratish va sozlash, Metasploitable2 muhitini yaratish va sozlash. Pentesting hisobotini shakllantirish. Penresting jarayonini bajarish: Nmap buyruqlari, Netcat va HTTP buyruqlari, wget buyruqlari, Nessus asosida enum4linux buyruqlari, CVE vebsaytida zaifliklar tadqiqi, yakuniy hisobotni yaratish.

21-mavzu. Ethical hakerlik muhitida standartlar

Pentesting standartlari va ularning ahamiyati. PCI DSS standarti. NIST 800-115 standarti: rejalashtirish, bajarish, yakunlash. NSA-IAM standarti. PTES standarti. CREST (UK) standarti. Standartlarni yagona yondashuvda birlashtirish. Aloqador standartlar: OWASP. Boshqa standartlar: ISO 27002, NIST 800-12, NIST 800-14.

III. Amaliy mashg’ulotlar bo‘yicha ko‘rsatma va tavsiyalar

Amaliy mashg’ulotlar uchun quyidagi mavzular tavsiya etiladi:

1. Tizim zaifliklarini tahlil qilish.
2. Tizim xavfsizligi darajasini baholash va zararkunanda dasturlardan himoyalanish.
3. Virtual mashinalar, ularni o‘rnatish va sozlash.
4. Windows xavfsizlik siyosati va uni amalga oshirish.
5. Linux operatsion tizimida xavfsizlik parametrlarini o‘rnatish va sozlash.
6. Windows operatsion tizimiga kirish hujumlarni tashkillashtirish, amalga oshirish va ularning xavfsizlikka ta’sirini o‘rganish.
7. Bug bounty usulida testlashni amalga oshirish.
8. Brauzerlardagi xavfsizlik parametrlari, ularni sozlash va o’zgartirish.
9. “TOR” brauzer yordamida DARKNET tarmog‘iga kirish va yopiq ma’lumotlarni qidirish.
10. Reverse engineering yordamida dasturiy vositalarni tahlil qilish.
11. Simsiz tarmoqlarga hujumlarni tashkillashtirish va amalga oshirish.

IV. Mustaqil ta’lim va mustaqil ishlar

Mustaqil ta’lim uchun tavsiya etiladigan tapshiriqlar:

1. Veb-ilovalarni penetratsion testlash: veb-ilovalardagi zaifliklarini aniqlash va bartaraf etishda ethical hackingni ahamiyati.
2. Ijtimoiy muhandislik (social engineering) hujumlari: Tashkilotlarda ijtimoiy muhandislik hujumlarini tahlil qilish va oldini olish uchun ethical hacking yondashuvi.
3. Mobil ilovalar xavfsizligida ethical hacking: mobil ilovalardagi keng tarqalgan zaifliklar va ekspluatatsiyalarni o‘rganish va ularni ethical hacking orqali bartaraf etish.
4. Tarmoq xavfsizligini baholash: tarmoq infratuzilmasidagi kiber zaifliklarini aniqlash va bartaraf etish uchun ethical hacking asosidagi yondashuv.
5. Kiber-sud-ekspertiza tekshiruvi: kiberjinoyat va sud-tibbiy dalillar to‘plamini tekshirish uchun ethical hacking yondashuvi.
6. Bulutli xavfsizlikda ethical hacking: bulutli hisoblashda xavfsizlik masalalari va ethical hacking yondashuvlarini o‘rganish.
7. IoT xavfsizligi: IoT qurilmalaridagi xavfsizlik zaifliklarini aniqlash va yumshatish uchun ethical hacking yondashuvi.
8. Simsiz tarmoq xavfsizligi: Simsiz tarmoqlardagi xavfsizlik zaifliklarini aniqlash va oldini olish uchun ethical hacking yondashuvi.
9. Blokcheyn xavfsizligi: blokcheynga asoslangan tizimlarda xavfsizlik zaifliklarini tahlil qilish va oldini olish uchun ethical hacking yondashuvi.
10. Parolni buzish usullari: turli xil parol turlarini tahlil qilish va buzish uchun ethical hacking yondashuvi.
11. Bug bounty dasturlari: xatoliklarni mukofotlash dasturlari va ularning axloqiy xakerlikni rag‘batlantirishdagi samaradorligini o‘rganish.
12. Kiberxavfsizlikda xavflarni baholash: Tashkilotlarda kiberxavfsizlik xatarlarini aniqlash va baholash uchun ethical hacking asoslangan yondashuv.
13. Xakerlik texnikasi va unga qarshi choralar: turli xakerlik usullari va ularga qarshi choralarni aniqlash va tahlil qilish uchun ethical hacking yondashuvi.
14. Ransomware hujumlari: Ransomware hujumlarining oldini olish va ularni qayta tiklash uchun ethical hacking yondashuvi.

	15. VoIP xavfsizligi: VoIP tizimlarida xavfsizlik zaifliklarini aniqlash va oldini olish uchun ethical hacking yondashuvi. 16. Zararli dasturlarni tahlil qilish: zararli dastur hujumlarini tahlil qilish va oldini olish uchun ethical hacking yondashuvi. 17. Elektron tijoratda kiberxavfsizlik: elektron tijorat tizimlarida kiberxavfsizlik muammolarini aniqlash va hal qilish uchun ethical hacking yondashuvi. 18. Simsiz kirishni aniqlash: simsiz tarmoqlarga ruxsatsiz kirishni aniqlash va oldini olish uchun ethical hacking yondashuvi. 19. Ijtimoiy media xavfsizligi: ijtimoiy media platformalarida xavfsizlik zaifliklarini tahlil qilish va oldini olish uchun ethical hacking yondashuvi. 20. Bank sektorida kiberxavfsizlik: bank tizimlarida kiberxavfsizlik muammolarini aniqlash va hal qilish uchun ethical hacking yondashuvi. 21. Elektron pochta xavfsizligi: elektron pochtaga asoslangan hujumlarning oldini olish uchun ethical hacking yondashuvi. 22. IoT da penetratsion testlash: IoT qurilmalaridagi xavfsizlik zaifliklarini aniqlash va bartaraf etish uchun ethical hacking yondashuvi. 23. Mobil qurilmalarning sud ekspertizasi: mobil qurilmalardan raqamli dalillarni to‘plash va tahlil qilish uchun ethical hacking yondashuvi. 24. Kiberxavfsizlik risklarini boshqarish: Tashkilotlarda kiberxavfsizlik xatarlarini aniqlash, baholash va boshqarish uchun ethical hacking ga asoslangan yondashuv. 25. Virtualizatsiya xavfsizligi: virtuallashtirilgan tizimlardagi xavfsizlik zaifliklarini aniqlash va oldini olish uchun ethical hacking yondashuvi. 26. Bulutli ilovalar xavfsizligini baholash: bulutga asoslangan ilovalar xavfsizligini baholash va yaxshilash uchun ethical hacking yondashuvi. 27. Brauzer xavfsizligi: veb-brauzerlardagi xavfsizlik zaifliklarini aniqlash va oldini olish uchun ethical hacking yondashuvi. 28. Tarmoqqa kirishni aniqlash: kompyuter tarmoqlariga ruxsatsiz kirishni aniqlash va oldini olish uchun ethical hacking yondashuvi. 29. Firewall xavfsizligi: Firewall tizimlarining samaradorligini sinab ko‘rish va yaxshilash uchun ethical hacking yondashuvi. 30. O‘rnatilgan tizimlarda penetratsion testlash: o‘rnatilgan tizimlardagi xavfsizlik zaifliklarini aniqlash va hal qilish uchun ethical hacking yondashuvi. 31. Xizmat ko‘rsatishni rad etish hujumlari: Xizmat ko‘rsatishni rad etish hujumlarining oldini olish va yumshatish uchun ethical hacking yondashuvi.
3.	**V. Fan o‘qitilishining natijalari (shakllanadigan kompetentsiyalar)** *Fanni o‘zlashtirish natijasida talaba:* • Ethical hacking aspektlarini xakerlik tushunchasi, qonuniy va etik xakerlik; • zararli dasturlar, Josuslik dasturlari, Fishing, vishing, smishing tushunchalari. Spam tushunchasi. Doksing tushunchasi. Ijtimoiy muhandislik usullari; • operatsion tizimlar kiberxavfsizligi tamoyillari; • brauzerlar xavfsizligi va zaifliklari; • bug bounty ning asosiy tushunchalari; • darknet tushunchasi, yopiq ma’lumotlar tarmog‘i; • ijtimoiy muhandislik, ijtimoiy tarmoqlar xavfsizligi; • fizik, apparat va dasturiy izolyatsiya tushunchalari; • Reverse engineering tushunchasi va dasturiy vositalarda reverse engineering ni qo‘llash; • Sandbox tushunchasi. Windows operatsion tizimida sandbox-dan foydalanish.
4.	**VI. Ta’lim texnologiyalari va metodlari** • ma’ruzalar; • amaliy ishlarni bajarish va xulosalash;

	• interfaol keys-studylar; • blits-so‘rovi; • guruhlarda ishlash; • taqdimotlar tayyorlash; • jamoa bo‘lib ishlash va himoya qilish uchun loyihalar.
5.	**VII. Kreditlarni olish uchun talabalar:** Fanga oid nazariy va uslubiy tushunchalarni to‘la o‘zlashtirish, tahlil natijalarini to‘g’ri aks ettira olish, o‘rganilayotgan jarayonlar haqida mustaqil mushohada yuritish va nazorat uchun berilgan vazifa va topshiriqlarni bajarish, yakuniy nazorat bo‘yicha yozma ishni yoki test topshirish.
6.	**Asosiy adabiyotlar** 1. S.K.Ganiyev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. –T.: «Fan va texnologiya», 2016, 372 bet. 74 2. S.K.Ganiyev, A. A.Ganiyev, Z.T.Xudoyqulov; Kiberxavsizlik asoslari: o'quv qo'llanma, -T.: “Nihol print” OK, 2021. – 224 b. 69 **Qo‘shimcha adabiyotlar** 1. S.K. Ganiyev, M.M. Karimov, K.A. Tashev; Axborot xavfsizligi: darslik/ O‘z R Oliy va o‘rta maxsus ta‘lim vazirligi, TATU. - Qayta nashr. - T.: Fan va Texnologiya, 2017. - 372 b. 2. Simpson Michael T., Kent Backman, and James Corley. *Hands-on ethical hacking and network defense*. Cengage Learning, 2010. 3. Easttom II, William Chuck. *Penetration testing fundamentals: A hands-on guide to reliable security audits*. Pearson IT Certification, 2018.
7.	Fan dasturi Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Kengashining 2023-yil 30-avgustdagi 9(731)/1(732)-son bayonnomasi bilan tasdiqlangan.
8.	**Fan/modul uchun mas'ullar:** N.N. Safoyev – Muxammad al-Xorazmiy nomidagi TATU, “Kiberxavfsizlik va Kriminalistika” kafedrasi katta o‘qituvchisi. S.M. Bozorov – Muxammad al-Xorazmiy nomidagi TATU, “Kriptologiya” kafedrasi assistenti. B. B. Turdibekov – Muxammad al-Xorazmiy nomidagi TATU, “Kiberxavfsizlik va Kriminalistika” kafedrasi o‘qituvchi-stajyori.
9.	**Taqrizchilar:** Z.T. Xudoyqulov – Muxammad Al-Xorazmiy nomidagi TATU, “Kriptologiya” kafedrasi mudiri, PhD (turdosh OTM). I.M. Bouquziyev– Renessans ta’lim universiteti, “Matematika va axborot texnologiyalari” kafedrasi PhD, dotsent. (turdosh OTM).