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: № 1150
2023-yil “3” 09

TARMOQ KRIMINALISTIKASI
FANINING O‘QUV DASTURI

Bilim sohasi:	600000	– Axborot-kommunikatsiya texnologiyalari
Ta’lim sohasi:	610000	– Axborot-kommunikatsiya texnologiyalari
Mutaxassisligi:	70611004	– Telekommunikatsiya tizimlari va tarmoqlarida axborot xavfsizligi

Toshkent 2023

Fan/modul kodi 2.01	O‘quv yili 2023-2024	Semestr 2	ESCTS kreditlar 6
Fan/modul turi majburiy	Ta’lim tili O‘zbek/rus		Haftadagi dars soatlari 4

	Fanning nomi	Auditoriya mashg‘ulotlari (soat)	Mustaqil ta’lim (soat)	Jami yuklama (soat)
1.	Tarmoq krimina-listikasi	60	120	180

2.

I. Fanning mazmuni

Fanni o‘qitishdan maqsad – talabalarda tarmoqqa oid kompyuter jinoyatlarini tadqiq qilish bo‘yicha nazariy va amaliy bilim hamda ko‘nikmalarni shakllantirishdan iborat.

Fanning vazifasi – talabalarda raqamli, tarmoq kriminalistika sohasi, tarmoqqa oid kompyuter jinoyati turlari va ularni aniqlash usullari va vositalari bo‘yicha tasavvurni hosil qilish, ularni tarmoq muhitida qo‘llash bo‘yicha ko‘nikma va malakani shakllantirishdan iborat.

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

I. Fan tarkibiga quyidagi mavzular kiradi:

1-mavzu. Tarmoq kriminalistikasi faniga kirish.

Raqamli kriminalistika va uning asosiy tushunchalari, turlari, vositalari. Kriptografik xeshlash. Tarmoq kriminalistikasi va uning zaruriyati. Insidentlarga javob berish.

2-mavzu. Tarmoq asoslari.

Tarmoq protokollari. OSI va TCP/IP tarmoq modeli. IP, ICMP, TCP, UDP protokollari. Portlar. DNS, DHCP, ARP.

3-mavzu. Host tomoni vositalari.

Xizmatlar. Ulanishlar. Vositalar: netstat, nbstat, ifconfig/ipconfig, Sysinternals, ntop, Task Manager/Resource Monitor, ARP, /proc Filesystem.

4-5-mavzular. Tarmoq paketini tutib olish va tahlillash.

Tarmoq paketi. Paketni tutib olish vositalari: Tcpdump/Tshark, Wireshark, Network Miner, Taps, Port Spanning, ARP Spoofing. Passiv skanerlash. Wireshark yordamida paketni tahlillash: paketni dekodlash, filtrlash, statistika, fayllarni to‘plash.

6-ma’ruza. Tarmoq hujumi turlari.

DOS hujumi: SYN Floods, noto‘g‘ri shakllangan paket, UDP Floods, kengaytirilgan hujumlar, taqsimlangan hujumlar. Zaifliklardan foydalanish. Ichki tahdidlar. Ilova hujumlari: SQL ineksiya, XSS hujumi.

7-mavzu. Joylashuvni bilish.

Vaqt zonalari. whois dasturi. Traceroute vositasi. GeolokatsiY. Joylashuvga asoslangan xizmatlar. WiFi joylashuvi.

8-9-mavzular. Tarmoq hujumiga qarshi tayyorgarlik ko‘rish.

NetFlow protokoli. Log fayllar va ularda hodisalarni qaydlash. Syslog. Windows Event Logs. Firewall log fayli. Router va svitch loglari. Log serverlar va monitoring. Antivirus. Insidentlarga javob berishga tayyorgarlik ko‘rish. Google Rapid Response. Axborot xavfsizligi va hodisalarni boshqarish (SIEM).

10-11-mavzular. Suqilib kirishlarni aniqlash tizimlari.

Suqilib kirishlarni aniqlash (IDS) usullari: signaturaga asoslangan, evristik. Hostga va tarmoqqa asoslangan IDSlar. IDS vositalar: Snort, Suricata, Sagan, Bro, Tripwire, OSSEC.

12-mavzu. Tarmoqlararo ekran va ilovalar loglaridan foydalanish.

Syslog. Markazlashgan loglarni tashkil qilish. Log xabarlarni o‘qish. LogWatch. Loglarni tozalash. Tarmoqlararo ekran loglari. Proksi loglari. WAF (Web Application Firewall) loglari. Umumiy log formati.

13-mavzu. Aloqador hujumlar.

Vaqtni sinxronlash, vaqt zonalari. Network Time Protocol. Loglarni yig‘ish va boshqarish. Syslog. Muddat. Plaso vositasi. PacketTotal vositasi.

14-15-mavzular. Tarmoqni skanerlash.

Portni skanerlash. OTni tahlil qilish. Scripts. Banner Grabbing. Ping Sweeps. Zaifliklarni skanerlash. Port Knocking. Tunellash. Passiv ma’lumotlarni to‘plash.

III. Amaliy mashg‘ulotlar

Amaliy mashg‘ulotlar uchun quyidagi mavzular tavsiya etiladi:

1. Wireshark snifferini o‘rnatish va ishga tayyorlash.
2. Wireshark snifferi yordamida HTTP protokolini tahlillash.
3. Wireshark snifferi yordamida TCP protokolini tahlillash.
4. Wireshark snifferi yordamida IP protokolini tahlillash.
5. Wireshark snifferi yordamida DHCP protokolini tahlillash.
6. Wireshark snifferi yordamida ICMP protokolini tahlillash.
7. Wireshark snifferi yordamida 802.11 WiFi protokolini tahlillash.
8. Wireshark snifferi yordamida SSL protokolini tahlillash.
9. OWASP webgoat simulyatorida DoS hujumini amalga oshirish.
10. OWASP webgoat simulyatorida XSS hujumini amalga oshirish.
11. OWASP webgoat simulyatorida SQL ineksiya hujumini amalga oshirish.

	12. LogWatch dasturiy vositasi yordamida operatsion tizim va tarmoq vositalari log fayllarini tahlillash. 13. Hostga asoslangan suqilib kirishlarni aniqlash vositalari yordamida trafikni tahlillash. Amaliy mashg‘ulotlar multimediya qurilmalari bilan jixozlangan auditoriyada bir akademik guruhga bir professor-o‘qituvchi tomonidan o‘tkazilishi zarur. Mashg‘ulotlar faol va interaktiv usullar yordamida o‘tilishi, mos ravishda munosib pedagogik va axborot texnologiyalar qo‘llanilishi muqsadga muvofiq. **IV. Mustaqil ta’lim va mustaqil ishlar** Talabaga berilgan mustaqil ishning asosiy maqsadi – o‘qituvchi rahbarligi va nazoratida muayyan o‘quv ishlarini mustaqil ravishda bajarish uchun bilim va ko‘nikmalarni shakllantirish va rivojlantirish. Mustaqil ta’lim uchun tavsiya etiladigan mavzular: 1. Kompyuter jinoyatlari, ularning tasnifi va turlari. 2. Kiberjinoyatchilik va uning turlari. 3. Kompyuter vositalari va tizimlarini kriminalistik tadqiq qilish. 4. Raqamli steganografiya va suv belgilari. 5. Raqamli kriminalistikada insidentlarni boshqarish. 6. Tarmoq protokollari va ularning vazifalari. 7. Zaifliklarni aniqlash vositalarining tadqiqi. 8. Tarmoq steganografiyasi va uning turlari. Mustaqil o‘zlashtiriladigan mavzular bo‘yicha talabalar tomonidan mustaqil ishlar tayyorlash va uni taqdimot qilish tavsiya etiladi.
3.	**V. Ta’lim natijalari / Kasbiy kompetensiyalar** Fanni o‘zlashtirish natijasida talaba: – tarmoq protokollari, tarmoq hujumlari, tarmoqda suqilib kirish usullari, log fayllarni boshqarish va tarmoqni skanerlash haqida ***tasavvurga ega bo‘lishi***; – tarmoq vositalarini, tarmoqda zaifliklarini skanerlash va himoyalash vositalarini ***bilishi va ulardan foydalana olishi***; – tarmoqda hujumga sabab bo‘luvchi zaifliklarni, log fayllarni, tarmoq anomaliyalarni, suqilib kirishlarni, kompyuter jinoyatchiligini tahlillash ***ko‘nikmalariga ega bo‘lishi*** kerak.
4.	**V. Ta’lim texnologiyalari va metodlari:** – ma’ruzalar; – interfaol keyslar-stadilar; – seminarlar (mantiqiy fikrlash, tezkor savol javoblar); – guruhlarda ishlash; – taqdimotlarni qilish.

5.	**VI. Kreditlarni olish uchun talablar:** 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 joriy va oraliq nazorat shakllarida berilgan vazifa va topshiriqlarni bajarish, yakuniy nazorat bo‘yicha yozma ishni topshirish.
6.	**Asosiy adabiyotlar** 1. S.Y.Yusupov, Sh.R.Gulomov, N.B.Nasrullayev. Raqamli kriminalistika: o‘quv qo‘llanma. – T.: «Aloqachi», 2019, 282 bet. 2. С.Ю.Юсупов, Ш.Р.Гуломов. Цифровая криминалистика: учебное пособие. –Т.: «Fan va texnologiya», 2018, 318 стр. **Qo‘shimcha adabiyotlar** 3. Joshi, R. C., and Emmanuel S. Pilli. Fundamentals of Network Forensics. Springer, 2016. 4. Datt, Samir. Learning Network Forensics. Packt Publishing Ltd, 2016. 5. Mishra, Charit. Mastering Wireshark. Packt Publishing Ltd, 2016. 6. R.Messier. Network Forensics. Published by John Wiley & Sons, Inc. Indianapolis, Indiana, 2017. **Internet saytlari** 7. https://chousensha.github.io/blog/2014/08/15/pentest-lab-webgoat/ 8. https://net.academy.lv/labwork/net_LW-06EN_Wireshark-Traffic.pdf 9. https://owasp.org/www-pdf-archive/OWASP_-_WebGoat_-_Introduction_to_XSS.pdf 10. https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/introduction-to-network-forensics-handbook.pdf
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 ma’sullar:** Xudoykulov Zarif Turakulovich – Muxammad al-Xorazmiy nomidagi TATU, “Kriptologiya” kafedrasi mudiri, PhD., dotsent.
9.	**Taqrizchilar:** Allanov O.M. – Muhammad Al-Xorazmiy nomidagi TATU, “Kiberxavfsizlik va kriminalistika” kafedrasi mudiri, PhD (turdosh OTM). Kadirov M.M. – Toshkent davlat texnika universitetining “Axborot texnologiyalari” kafedrasi dotsenti, PhD (turdosh OTM).