KALI LINUX OPERATSION TIZIM YORDAMIDA OCHIQ KODLI RAZVEDKANI AMALGA OSHIRISH USULLARINI TAHLIL QILISH

Rustamov Shamiljon Xasanovich
Axborot texnologiylari va menejment universiteti PhD p.f.f.d
E-mail: shamiljon1988@gmail.com
Norboyev Bexzod Uktam o‘g‘li
Axborot texnologiylari va menejment universiteti asistenti
E-mail: b.norboyev@atmu.uz
Boboqulov Behro‘z Muzaffar o‘g‘li
Axborot texnologiylari va menejment universiteti, magistr
E-mail: boboqulovbehruz639@gmail.com

Annotatsiya: Ushbu maqolada Kali Linux operatsion tizimi yordamida ochiq kodli razvedka OSINTni amalga oshirish usullari, va ochiq kodli razvedkada qo‘llaniladigan vositalar ularning imkoniyatlari ko‘rib chiqiladi. Kali Linux Operatsion tizimidagi vositalar uning imkoniyatlari, axborot xavfsizligidagi o‘rni amaliy misollar bilan o‘rganilib, tahlil qilinadi. Ochiq kodli razvedkani amalga oshirishda ushbu vositalarning afzalliklari, qo‘llashdagi ehtiyot choralar hamda real xavflar baholandi. Shuningdek OSINT vositalarini ishlatishda e’tibor qaratilishi lozim bo‘lgan axloqiy va huquqiy masalalarga ham alohida to‘xtalib o‘tiladi.Bundan tashqari ma’lumotlarimiz ochiqlanmasligi uchun takliflarlar va xulosalar beriladi va olingan natijalar orqali ochiq kodli razvedka texnologiyalarining amaliyotdagi ahamiyati va dolzarbligi yoritiladi.

Kalit so‘zlar: Kali Linux, OSINT,OSINT Framework, Maltego, theHarvester,Shodan,Spiderfoot,Domen,Subdomen,amass,Holehe,Whatweb,Google Dorks,Razvedka.

Аннотация. В данной статье рассматриваются методы реализации разведки по открытым источникам (OSINT) с использованием операционной системы Kali Linux, а также инструменты, применяемые в открытой разведке, и их функциональные возможности. Инструменты операционной системы Kali Linux, их возможности и роль в обеспечении информационной безопасности изучаются и анализируются на основе практических примеров. Оцениваются преимущества использования данных инструментов при проведении OSINT, меры предосторожности при их применении, а также потенциальные реальные угрозы. Кроме того, особое внимание уделяется этическим и правовым вопросам, которые необходимо учитывать при использовании OSINT-инструментов. Также предлагаются рекомендации и выводы, направленные на предотвращение утечки персональных данных. На основе полученных результатов раскрывается практическая значимость и

ISSN 3030-3907

актуальность технологий разведки по открытым источникам в современных условиях.

Ключевые слова: Kali Linux, OSINT, OSINT Framework, Maltego, theHarvester, Shodan, SpiderFoot, домен, субдомен, Amass, Holehe, WhatWeb, Google Dorks, разведка.

Abstract. This article examines the methods of implementing Open Source Intelligence (OSINT) using the Kali Linux operating system, as well as the tools used in open-source intelligence and their capabilities. The tools available in the Kali Linux operating system, their functionalities, and their role in information security are studied and analyzed through practical examples. The advantages of using these tools in conducting OSINT, the necessary precautions during their application, and potential real-world risks are evaluated. In addition, special attention is given to ethical and legal issues that must be considered when using OSINT tools. Furthermore, recommendations and conclusions are provided to prevent the disclosure of sensitive information. Based on the obtained results, the practical significance and relevance of open-source intelligence technologies in real-world applications are highlighted.

Keywords: Kali Linux, OSINT, OSINT Framework, Maltego, theHarvester, Shodan, SpiderFoot, domain, subdomain, Amass, Holehe, WhatWeb, Google Dorks, intelligence.

Kirish

Bugungi kunda axborot xavfsizligini ta’minlash uchun ochiq razvedka texnologiyalarini o‘rganish va ularni amaliyotga tadbiq etish dolzarb bo‘lib bormoqda. Ayniqsa, xakerlik faoliyatlarining kuchaygani, soxta sahifalar va ma’lumot o‘g‘riligining ko‘paygani sharoitida OSINT vositalari orqali xavflarni erta aniqlash imkoniyati muhim ahamiyatga ega.Axborot texnologiyalarining jadal rivojlanishi nafaqat hayotning turli sohalarida yangiliklar va qulayliklar yaratmoqda, balki axborot xavfsizligiga doir yangi muammolarni ham yuzaga keltirmoqda. Hozirgi kunda tashkilotlar va alohida shaxslar faoliyatida raqamli axborot muhim o‘rin tutgani sababli, uni ishonchli himoyalash dolzarb masalaga aylangan. Xavfsizlikni ta’minlashda ochiq manbali razvedka – OSINT (Open Source Intelligence) usullaridan foydalanish muhim ahamiyat kasb etmoqda.

Ochiq manbali razvedka – bu ijtimoiy tarmoqlardan, veb-saytlardan, forumlardan, ommaviy axborot vositalardan va boshqa erkin ochiq manbalardan ma’lumot to‘plash va ularni taxlil qilish orqali xavf-xatarlarni aniqlash, tahdid manbalarini baholash va qarorlar qabul qilishga asos bo‘luvchi axborotlarni jamlash jarayonidir.

Ushbu sohada keng qo‘llaniladigan Kali Linux operatsion tizimi – axborot xavfsizligining mutaxassislari uchun mo‘ljallangan va maxsus vositalar to‘plamini

ISSN 3030-3907

o‘z ichiga olgan kuchli platforma hisoblanadi. Kali Linux operatsion tizim yordamida OSINT vositalarini qo‘llash va turli manbalar orqali ma’lumot yig‘ish, foydalanuvchilarning faolligini tahlil qilish va taxdidlarni aniqlash jarayonlari soddalashtiradi.Kali Linux tizimida ochiq kodli razvedka (OSINT) vositalaridan foydalanish usullari, ularning afzalliklari, texnik imkoniyatlari, xavfsizlik jihatlari hamda real amaliyotdagi qo‘llanilishi tahlil qilinadi.

Ochiq kodli razvedka (OSINT) - bu ochiq manbalardan olingan ma’lumotlarni to‘plash, tahlil qilish va ulardan amaliy razvedka ma’lumotlari olish jarayoni. Bu soha zamonaviy kiberxavfsizlik, jurnalistika, qonuniy tergovlar va biznes razvedkasi kabi sohalarda muhim rol o‘ynaydi. OSINT ning asosiy maqsadi – ommaviy axborot vositalari, ijtimoiy tarmoqlar, davlat ro‘yxatlari va boshqa ochiq manbalardan olingan ma’lumotlarni saralab, ularni ma’lum bir masalani hal qilish yoki tahdidlarni aniqlash uchun ishlatishdir. OSINT ochiq manbalardan ma’lumotlarni yig‘ish va tahlil qilish: ijtimoiy tarmoqlar, ma’lumotlar bazalari, sun’iy yo‘ldosh tasvirlari va hatto messenjerlar. Bugungi kunda OSINT nafaqat qo‘lda qidirish, balki botlar, asboblar va skriptlar yordamida avtomatlashtirishdir.
OSINT manbalari va to‘plash usullari

OSINT manbalari olti asosiy kategoriyaga bo‘linadi:

- Ommaviy axborot vositalari – gazetalar, jurnallar, radio va televideniye;
- Internet manbalari – bloglar, forumlar, ijtimoiy tarmoqlar (Facebook, Instagram, Telegram);
- Davlat ma’lumotlari – ochiq budjetlar, sud hujjatlari, rasmiy bayonotlar;
- Ilmiy nashrlar – konferensiyalar, dissertatsiyalar, patentlar;
- Korporativ ma’lumotlar – moliyaviy hisobotlar, sanoat tahlillari
- Adabiyot – texnik hisobotlar, ishchi hujjatlar.

OSINT uchun ishlatilishi mumkin bo‘lgan ma’lumot manbalari quyidagilarni o‘z ichiga oladi:

Offline manbalar:

- davlat hisobotlari va hujjatlari;
- akademik tadqiqotlar va jurnallar;
- korporativ hisobotlar va konferensiya materiallari;
- an’anaviy ommaviy axborot vositalari (televideniye, radio, gazeta);

Online manbalar:

- internet qidiruv tizimlari (Google, Bing, Yandex);
- ijtimoiy tarmoqlar (Facebook, Instagram, Telegram);
- video platformalari (YouTube, Dailymotion);
- bloglar, forumlar va onlayn hamjamiyatlar.

Ochiq kodli razvedkani amalga oshirish vositalari

ISSN 3030-3907

Maltego - Maltego 2007-yilning 23-oktiyabirida ilk ishga tushirilganidan buyon butun dunyo bo‘ylab deyarli bir million tijorat va jamoat foydalanuvchilari tomonidan yuklab olingan tasdiqlangan vositadir.havolalarni tahlil qilish uchun yaxlit vositadir. Maltego real vaqt rejimida ma’lumotlarni yig‘ish va ma’lumot to‘plash, shuningdek, ushbu ma’lumotni tugunga asoslangan grafikda ko‘rsatishni taklif qiladi, bu ma’lumotlar o‘rtasida naqshlar va bir nechta tartibli ulanishlarni osongina aniqlash mumkin.

Maltego quyidagi sub’ektlar o‘rtasidagi munosabatlarni aniqlash uchun ishlatilishi mumkin:

Shaxslar.

Ismlar;

Elektron pochta manzillari;

Taxalluslar

Odamlar guruhlari (ijtimoiy tarmoqlar)

Kompaniyalar.

Tashkilotlar

Veb-saytlar.

Internet infratuzilmasi, masalan:

Domenlar

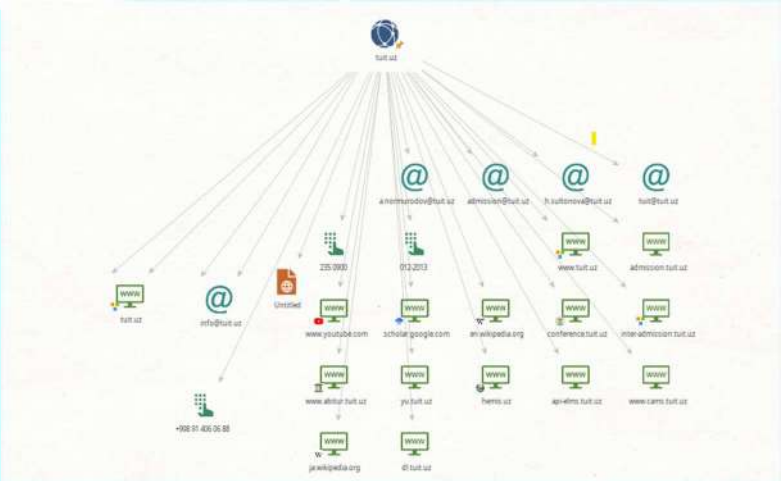
DNS nomlari

Netbloklar

IP manzillar

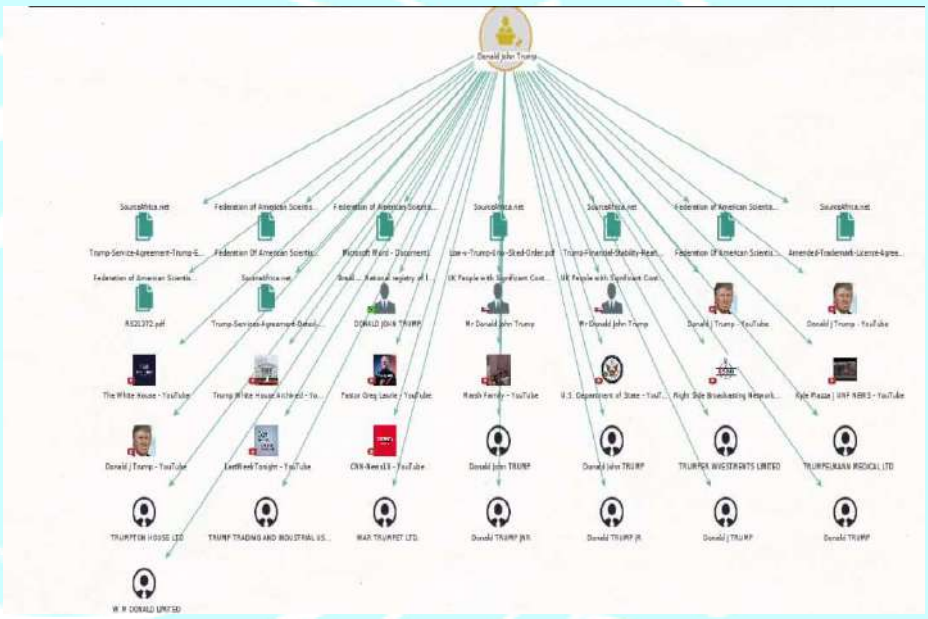
Aloqalar

Hujjatlar va faylla.



1-rasm.Maltegoda tuit.uz saytini osint qilish.

ISSN 3030-3907



2-rasm.Maltegoda shaxs haqida osint qilish.

Spiderfoot – SpiderFoot ochiq manbali razvedka (OSINT) avtomatlashtirish vositasidir. U deyarli barcha mavjud ma'lumotlar manbalari bilan integratsiyalashgan va ma'lumotlarni tahlil qilish uchun bir qator usullardan foydalanadi, bu ma'lumotlarni boshqarishni osonlashtiradi. SpiderFoot-da toza va intuitiv veb-interfeysni ta'minlash uchun o'rnatilgan veb-server mavjud, ammo undan to'liq buyruq qatori orqali ham foydalanish mumkin. U Python 3 da yozilgan va MIT litsenziyasiga ega.

Spiderfootning asosiy xususiyatlari quyidagilar:

vebga asoslangan UI yoki CLI;

200 dan ortiq modular;

python 3.7+;

csv/json/gexf eksporti;

api kalitini eksport/import qilish;

maxsus so'rovlar uchun SQLite back-end;

yuqori darajada sozlanishi;

to'liq hujjatlashtirilgan;

vizualizatsiya;

qorong'i veb-qidiruv uchun TOR integratsiyasi;

docker-ga asoslangan joylashtirishlar uchun Dockerfile;

dnstwist, Whatweb, Nmap va CMSeeK kabi boshqa vositalarni chaqirishi mumkin.

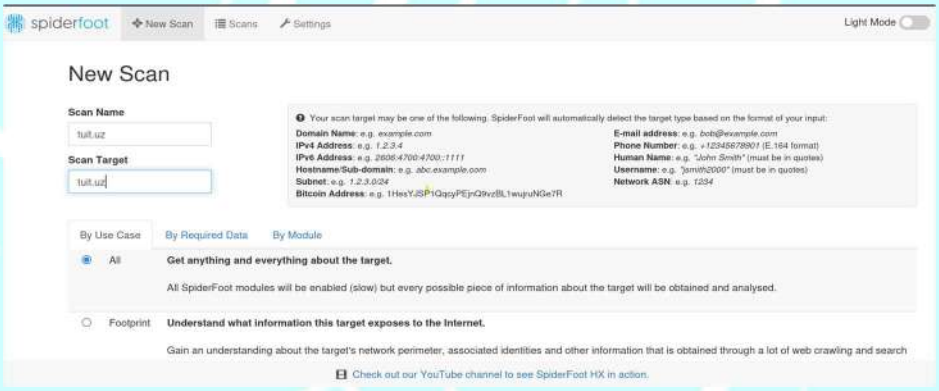
SpiderFoot hujumda (masalan, qizil jamoa mashqlari yoki penetratsion testda) maqsadingizni aniqlash uchun yoki mudofaa maqsadida Internet orqali siz yoki tashkilotingiz fosh qilgan narsalar haqida ma'lumot to'plash uchun ishlatilishi mumkin.

SpiderFoot skanerlashda biz quyidagi ob'ektlarni aniqlash mumkin:

– ip manzili;

ISSN 3030-3907

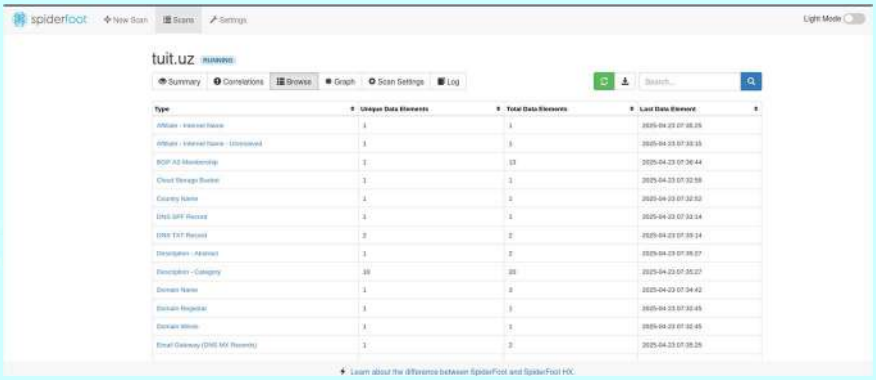
– domen/sub-domen nomi;
– xost nomi;
– tarmoq quyi tarmog‘i (CIDR);
– asn;
– e-pochta manzili;
– telefon raqami;
– foydalanuvchi nomi;
– shaxsning ismi;
bitcoin manzili;



3-rasm.spiderfoot ishchi oynasi.



4-rasm.spiderfootda natijaning ko‘rinishi



5.1-dars.spiderfootda domen haqida ma’lumot beruvchi oynasi.

ISSN 3030-3907

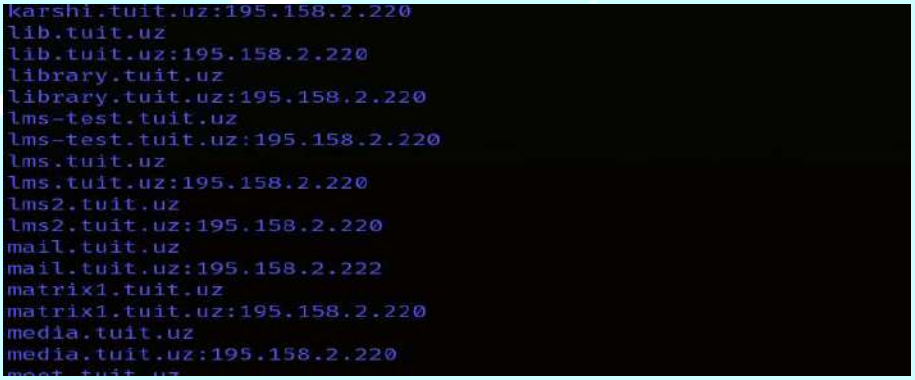


5.2-dars.spiderfootda domen haqida ma’lumot beruvchi oynasi.



6-rasm.spiderfootda server haqida ma’lumot olish

theHarvester -d domen_nomi -b all bu buyruq barcha bazasidan domenlarni emaillarni va sabdomenlarni topib beradi.Theharvestrni imkoniyatlar keng OSINT tool hisoblanadi.u bizga quyidagi imkoniyatlarni taqdim qiladi.Bular ip manzillarini,subdomenlarni,url manzillarni, email adreslarni topib beradi.



7-rasm.tuit.uz saytining subdomenlari.

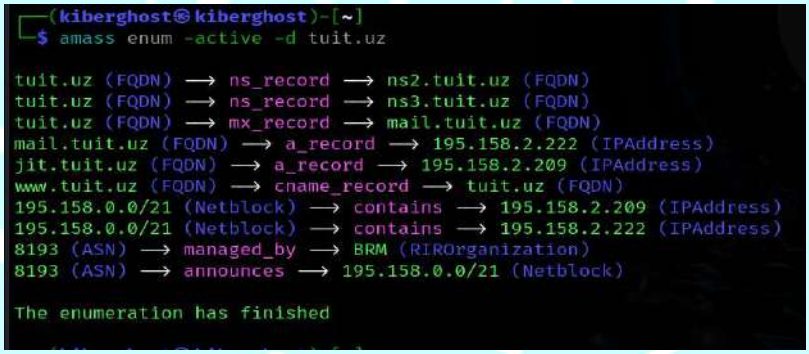


8-rasm.tuit.uz sayti orqali topilgan ip manzillar

ISSN 3030-3907

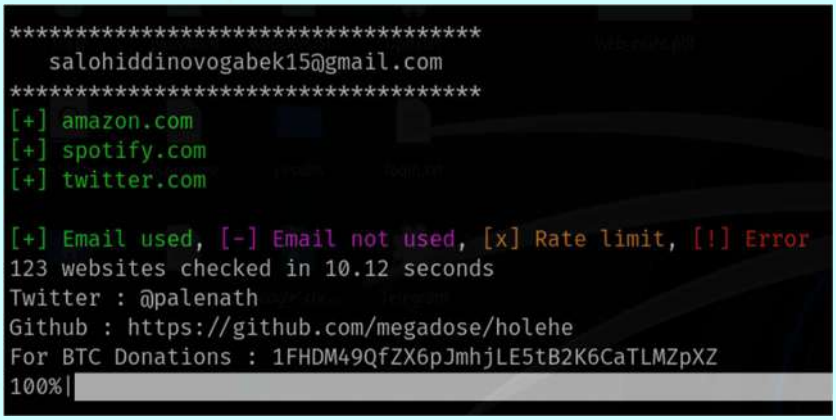


9-rasm.tuit.uz saytida topilgan urllar.



10-rasm.ammasda domenni aktiv tahlil qilish.

Holehe — bu ochiq kodli OSINT vositalaridan biri bo‘lib, u orqali foydalanuvchining email manzilga asoslangan holda turli mashhur onlayn platformalarda (masalan: Twitter, Instagram, GitHub, Netflix, Spotify va boshqa xizmatlarda) shu emailga bog‘langan akkauntlar mavjud yoki yo‘qligini aniqlash mumkin. Ushbu vosita akkauntlar mavjudligini aniqlashda tezkor va passiv razvedka usulida ishlaydi.Bir qator imkoniyatlari bor email orqali profillarni taxlil qilib beradi.OSINT uchun ancha qulay hisoblanadi.loginlar



11-rasm.holeheda email orqali topilgan natija.

Shodan qidiruv tizimi bo‘lib, foydalanuvchilarga turli filtrlar yordamida Internetga ulangan har xil turdagi serverlarni (veb-kameralar, marshrutizatorlarserverlar va boshqalar) qidirish imkonini beradi . Ba'zilar uni xizmat bannerlari uchun qidiruv tizimi sifatida ham ta'riflaydilar, bu esa server mijozga qaytarib yuboradigan metama'lumotlardir. Ushbu metama'lumotlar server

ISSN 3030-3907

dasturiy ta'minoti, xizmat qanday variantlarni qo‘llab-quvvatlashi, xush kelibsiz xabari yoki mijoz server bilan o‘zaro aloqada bo‘lishdan oldin bilishi kerak bo‘lgan boshqa narsalarni o‘z ichiga olishi mumkin.

“Google Dorks” deb nomlangan ushbu kengaytirilgan qidiruvlar xakerlarga maxsus qidiruv buyruqlari va kalit so‘zlardan foydalangan holda tizimlaringizdagi yashirin ma'lumotlarni va hatto xavfsizlikning zaif tomonlarini topishga imkon beradi. Google Dorks, shuningdek, Google xakerligi deb ataladi, aniqroq natijalarni berish uchun maxsus buyruqlardan foydalanadigan ilg‘or qidiruv usullari.

Oddiy kalit so‘zlarni kiritish o‘rniga Google Dorks qidiruvlarni qisqartirish va yashirin ma'lumotlarni topish uchun “filetype:”, “inurl:”, “intitle:” yoki “site:” kabi buyruqlarni birlashtiradi.

Bugungi kunda turli xil soxalarda Google Dorks orqali turli xavflarga duch kelishgan.Bularga misol tariqasida biz quyidagilarni keltirishimiz mumkin.

Sog‘liqni saqlashda:bemorlarning varqalari,ular haqidagi ma’lumotlar,tibbiy ko‘rikdagi ma’lumotlar.

Texnologiyada:dasturning kodi,API kalitlar,server tafsilotlari,ularning ishlash texnikalari.

Ishlab chiqarish sohasida:Mahsulotlarning loyihalari,texnik xizmat ko‘rsatish jurnallarini msol qilishimiz mumkin.

Kompaniyalar o‘zlarining xavlarini baholay olishlari va shuningdek o‘zlarining ma’lumotlarini himoya qilish choralarini ko‘rishlari kerak.

OSINT vositalari tahlili

Vosita nomi	Vazifasi	Ma’lumot oladigan bazasi	Ishlash tezligi
Maltego	Ijtimoiy tarmoq va dark web ma’lumotlarini tahlil qilish, shaxslar haqida ma’lumot yig‘ish, vizualizatsiya	Ijtimoiy tarmoqlar, dark web, turli identifikatsiya ma’lumotlari	O‘rta (vizualizatsiya sababli)
Spiderfoot	Raqamli izlarni xaritalash, IP manzillar, domen nomlari va boshqa ma’lumotlarni avtomatik tahlil qilish	IP manzillar, domen nomlari, elektron pochta manzillari,	O‘rta (keng qamrovli tahlil sababli)

ISSN 3030-3907

theHarvester	Domen va elektron pochta manbalarini ochiq manbalardan yig‘ish va tez tahlil qilish (subdomain va host ma'lumotlari).	Qidiruv tizimlari (Google, Bing), PGP keyserverlar, Shodan, DNS yozuvlari va umumiy ochiq manbalar.	Past–O‘rta (faqat ochiq manbalardan boshlab)
amass	Passiv va aktiv subdomain aniqlash, DNS enumeratsiyasi, sertifikat va tarmoq tarmoqlash.	DNS yozuvlari, Certificate Transparency (crt.sh va boshqalar.), texnologik tizimlar, web arxivlar va turli OSINT APIlari.	O‘rta (passiv + ba’zi faol harakat qilish)
Holehe	Elektron pochta manzilining turli platformalarda ro‘yxatdan o‘tganligini tekshirish	120+ sayt va ijtimoiy tarmoqlar (X, Instagram, Imgur, va boshqalar)	Juda tez (faqat e-pochta tekshirish)
Recon-ng	Ochiq manbalardan ma’lumot yig‘ish, hujum yuzasini tahlil qilish, domen ma’lumotlarini yig‘ish	Turli internet manbalar, API integratsiyalari, domeni ma’lumotlari	Tez (avtomatlashtirilgan)
shodan	Internetga ulangan qurilmalarni qidirish, zaifliklarni aniqlash	Internet qurilmalari, serverlar, xizmatlar, zaifliklar bazalari	O‘rta-tez (ma’lumotlar hajmiga bog‘liq)

Bugungi kunda ma’lumotlarimiz OSINT bazasiga aylanmasligi uchun har bir shaxs quyidagilarga amal qilishi kerak.

– Bularga ijtimoiy tarmoqlardan foydalanganda rasmlarini yuklamaslik.

ISSN 3030-3907

– Ijtimoiy tarmoqdan foydalanayotganda,anonimlik qoidalariga rioya qilishlari kerak.

– O‘qigan universiteti,yoshi ish joyi,yashash manzilini qo‘ymasliklari kerak.

– Ma’lumotlar bazasini xavfsiz parollar va maxfiy ma’lumotlar bilan himoya qilish zarur.

– Shaxsiy xavfsizlikka rioya qilish kerak.Korxona yoki tashkilotlarda xodimlarni tushuntirish ishlari olib borish kerak.

– Online xaridlarni amalga oshirayotganda ilovalarga o‘tib to‘lovlarni amalga oshirish.

– Umuman internet ishlatiladigan joylarda xodimlarni audit qilib borish kerak,pochta alohida bo’lishi kerak,

Xulosa

Kali Linux operatsion tizimi asosida ochiq kodli razvedka OSINT usullarini tahlil qilish va amaliy qo‘llash asosiy maqsad qilib olingan bo‘lib, quyidagi natijalarga erishildi:

– ochiq manbalarga asoslangan razvedka OSINT tushunchasi, uning usullari va bosqichlari chuqur o‘rganildi;

– Kali Linuxda OSINT vositalari amaliy misollar asosida tahlil qilindi;

– domen va subdomenlarni aniqlash email orqali ro‘yxatdan o‘tilgan saytlarni topish bosqichlari amaliyotda bajarildi.

Bugungi kunda axborot xavfsizligi bilan bog‘liq tahdidlar ortib borayotgani sababli, OSINT texnologiyalaridan samarali foydalanish dolzarb ahamiyat kasb etmoqda. Mazkur ishda ishlab chiqilgan yondashuvlar axborot tizimlarining zaifliklarini aniqlash va tahlil qilishda qo‘llanishi mumkin bo‘lib, ularning xavfsizligini mustahkamlashda muhim amaliy ahamiyatga ega ekani ilmiy asosda isbotlab berildi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Wilson Bautista. Practical Cyber Intelligence: How action-based intelligence can be an effective response to incidents (Packt Publishing, 2018, 361 bet).

2. Diego Rodrigues. Kali Linux OSINT: Fundamentals and Advanced

3. Shoniyozova YQ, Turdiyeva M.A., Norboyev BU TARMOQLARNING HUJUMLARNING profilaktikasi TIZIMLARI //INNOVATSIONNYE MEXANIZMY I STRATEGICHESKIE PRIORITETY NAUCHNO. – 2020. – S. 46.

4. Shoniyozova, YQ, M.A.Turdiyeva, BU Norboyev. "TARMOQLARNI HUJUMLARNI OLDINI OLISH TIZIMLARI". INNOVATSIONNYE MEXANIZMY I STRATEGICHESKIE PRIORITETY NAUCHNO (2020): 46.

5. Shoniyozova, YQ, Turdiyeva, MA, & Norboyev, BU (2020). TARMOQLARNING HUJUMLARINI OLDINI OLISH TIZIMLARI.

ISSN 3030-3907

INNOVATSIONNYE MEXANIZMY I STRATEGICHESKIE PRIORITETI NAUCHNO , 46.

6. Kadyrov, B. K. (2022). Perspectives of problems in the study of database science in the Credit-Module System and their solutions. International Journal of Formal Education, 2(1), 16-22.

7. Kurbanov, J., Halikov, A., & Ortikov, M. (2019). Devices for magnetization and demagnization of rail lashes and their comparative analysis with existing. In Технические науки: проблемы и решения (pp. 50-53).

8. Rustamov AB RAQAMLI SANOAT STRUKTURASINI INNOVATSION RIVOJLANTIRISHNING NAZARIY TAMOYILLARI // Iqtisodiyot va jamiyat. - 2024. - № 12-2 (127). - B. 757-761.

9. Rustamov, AB "RAQAMLI SANOAT STRUKTURASINI INNOVATSION RIVOJLANTIRISHNING NAZARIY TAMOYILLARI." Iqtisodiyot va jamiyat 12-2 (127) (2024): 757-761.

10. Rustamov, A. B. (2024). RAQAMLI SANOAT STRUKTURASINI INNOVATSION RIVOJLANTIRISHNING NAZARIY TAMOYILLARI. Iqtisodiyot va jamiyat , (12-2 (127)), 757-761.

ISSN 3030-3907