OSINT VOSITALARI (MALTEGO, SHODAN, THE HARVESTER)
ИНСТРУМЕНТЫ OSINT: MALTEGO, SHODAN И THE HARVESTER
OPEN SOURCE INTELLIGENCE TOOLS: MALTEGO, SHODAN, AND THE HARVESTER

Behzod Sobirjonov Qahramonovich
FarDu Axborot texnologiyalari
kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Abdusamadova Ma’sumaxon Abdulhamid qizi
FarDu Axborot tizimlari va texnologiyalari
yo‘nalishi 2-bosqich talabasi
abdusamatovamasumaxon1014@gmail.com
Telefon raqam: 94-042-21-08
https://doi.org/10.5281/zenodo.20027378

Annotatsiya. Mazkur ilmiy maqolada ochiq manbali razvedka (OSINT) tushunchasi, uning nazariy asoslari va zamonaviy axborot xavfsizligi tizimidagi o‘rni keng yoritilgan. Tadqiqot doirasida OSINT texnologiyalarining ma’lumot yig‘ish, qayta ishlash va tahlil qilish jarayonlaridagi ahamiyati ilmiy jihatdan asoslab berilgan.

Ishda Maltego, Shodan hamda theHarvester vositalarining funksional imkoniyatlari, ishlash prinsiplari va amaliy qo‘llanilish sohalari chuqur tahlil qilingan. Xususan, Maltego yordamida bog‘lanishlar tahlili, Shodan orqali internet infratuzilmasini skanerlash va theHarvester vositasi orqali passiv razvedka olib borish jarayonlari ilmiy asosda ko‘rib chiqilgan.

Tadqiqot natijalari shuni ko‘rsatadiki, OSINT vositalari kiberxavfsizlikni ta’minlash, zaifliklarni aniqlash va katta hajmdagi ochiq ma’lumotlarni tizimli tahlil qilishda muhim ahamiyat kasb etadi. Shu bilan birga, ushbu texnologiyalardan foydalanishda axloqiy va huquqiy me’yorlarga rioya qilish zarurligi ta’kidlangan.

Kalit so‘zlar: OSINT, ochiq manbali razvedka, kiberxavfsizlik, ma’lumotlar tahlili, Maltego, Shodan, theHarvester, axborot xavfsizligi, data mining, link analysis

Annotation (English): This scientific article examines the concept of Open Source Intelligence (OSINT), its theoretical foundations, and its role in modern information security systems. The study provides a comprehensive analysis of the importance of OSINT technologies in the processes of data collection, processing, and analysis.

Within the framework of the research, the functional capabilities, operating principles, and practical applications of Maltego, Shodan, and theHarvester are thoroughly analyzed. In particular, link analysis using Maltego, internet infrastructure scanning via Shodan, and passive reconnaissance with theHarvester are considered from a scientific perspective.

The results of the study demonstrate that OSINT tools play a significant role in ensuring cybersecurity, identifying vulnerabilities, and conducting systematic analysis of large volumes of open-source data. At the same time, the importance of adhering to ethical and legal standards in the use of these technologies is emphasized.

Keywords: OSINT, open source intelligence, cybersecurity, data analysis, Maltego, Shodan, theHarvester, information security, data mining, link analysis

Аннотация (Russian): В данной научной статье рассматривается понятие открытой разведки (OSINT), её теоретические основы и роль в современных системах информационной безопасности. В работе обоснована значимость технологий OSINT в процессах сбора, обработки и анализа данных.

В рамках исследования проведён подробный анализ функциональных возможностей, принципов работы и областей применения инструментов Maltego, Shodan и theHarvester. В частности, рассмотрены методы анализа связей с использованием Maltego, сканирование интернет-инфраструктуры с помощью Shodan, а также пассивная разведка с применением theHarvester.

Результаты исследования показывают, что инструменты OSINT играют важную роль в обеспечении кибербезопасности, выявлении уязвимостей и системном анализе больших объёмов открытых данных. Вместе с тем подчёркивается необходимость соблюдения правовых и этических норм при использовании данных технологий.

Ключевые слова: OSINT, открытая разведка, кибербезопасность, анализ данных, Maltego, Shodan, theHarvester, информационная безопасность, data mining, анализ связей

OSINT vositalari: Maltego, Shodan va theHarvester

Kirish

Axborotlashgan jamiyat sharoitida ma’lumotlar strategik resursga aylangan bo‘lib, ularni yig‘ish, qayta ishlash va tahlil qilish jarayonlari davlatlar, tashkilotlar va shaxslar faoliyatida muhim o‘rin egallaydi. Shu nuqtai nazardan, OSINT (Open Source Intelligence) — ochiq manbalardan razvedka ma’lumotlarini olish texnologiyasi zamonaviy axborot xavfsizligi, kiberrazvedka va analitik faoliyatning ajralmas qismiga aylandi.

OSINT yopiq yoki maxfiy manbalardan farqli ravishda, internet tarmoqlari, ommaviy axborot vositalari, ijtimoiy platformalar, ilmiy bazalar va boshqa erkin foydalanish mumkin bo‘lgan resurslardan ma’lumot yig‘ishga asoslanadi. Bu esa uni qonuniy, arzon va keng ko‘lamli tahlil vositasiga aylantiradi.

Mazkur ilmiy ishda OSINT sohasida keng qo‘llaniladigan uchta muhim vosita — Maltego, Shodan va theHarvester funksional imkoniyatlari, ishlash prinsiplari hamda amaliy ahamiyati chuqur tahlil qilinadi.

OSINTning nazariy asoslari va metodologiyasi

OSINT konsepsiyasi razvedka faoliyatining klassik tamoyillariga asoslangan bo‘lib, u quyidagi bosqichlarni o‘z ichiga oladi: ma’lumotlarni yig‘ish (collection), saralash (processing), tahlil qilish (analysis) va natijalarni taqdim etish (dissemination).

OSINTning samaradorligi asosan quyidagi omillarga bog‘liq:

- ma’lumotlarning ishonchliligi va aniqligi
- manbalar xilma-xilligi
- tahlil algoritmlarining mukammalligi
- avtomatlashtirish darajasi

Zamonaviy OSINT vositalari sun’iy intellekt, ma’lumotlar konini qazib olish (data mining), grafik tahlil (link analysis) va katta ma’lumotlar (big data) texnologiyalariga asoslanadi. Shu sababli ular nafaqat ma’lumot yig‘ish, balki murakkab bog‘lanishlarni aniqlash imkonini ham beradi.

Maltego vositasining ilmiy-tahliliy tavsifi

Maltego — bu ochiq manbalardan olingan ma’lumotlar o‘rtasidagi bog‘lanishlarni aniqlash va vizual tahlil qilishga mo‘ljallangan kompleks platforma hisoblanadi. Ushbu tizim “link analysis” metodologiyasiga asoslanadi, ya’ni obyektlar (shaxs, domen, IP manzil, tashkilot) o‘rtasidagi aloqalarni grafik model ko‘rinishida aks ettiradi.

Maltego arxitekturasi transformlar tizimiga asoslangan bo‘lib, u tashqi ma’lumot manbalariga so‘rov yuborish orqali yangi ma’lumotlarni avtomatik ravishda yig‘adi. Har bir transform ma’lum turdagi ma’lumotni kengaytirishga xizmat qiladi, bu esa rekursiv qidiruv imkonini yaratadi.

Ushbu vositaning ilmiy ahamiyati shundaki, u murakkab tarmoqlarni (network structures) vizual analiz qilish orqali yashirin bog‘lanishlarni aniqlash imkonini beradi. Masalan, kiberjinoyatlarni tergov qilishda yoki ijtimoiy tarmoqlarda ta’sir doirasini aniqlashda Maltego samarali hisoblanadi.

Shodan tizimining funksional modeli va kiberxavfsizlikdagi o‘rni

Shodan — bu internet infratuzilmasini tahlil qilishga mo‘ljallangan maxsus qidiruv tizimi bo‘lib, u global tarmoqdagi qurilmalarni indekslash orqali ishlaydi.

An’anaviy qidiruv tizimlari (masalan, veb-sahifalarni indekslovchi tizimlar)dan farqli ravishda, Shodan serverlar, IoT qurilmalar, sanoat nazorat tizimlari (ICS/SCADA) va boshqa tarmoqqa ulangan obyektlarni aniqlaydi.

Shodanning ishlash prinsipi quyidagicha:

- internet bo‘ylab port skanerlash
- xizmat bannerlarini yig‘ish
- qurilma konfiguratsiyasini aniqlash
- ma’lumotlarni indekslash va qidiruvga taqdim etish

Ushbu tizim kiberxavfsizlik nuqtai nazaridan muhim ahamiyatga ega, chunki u ochiq portlar, noto‘g‘ri sozlangan serverlar va zaifliklarni aniqlash imkonini beradi. Shu bilan birga, Shodan noto‘g‘ri qo‘llanilganda xavfli vositaga aylanishi mumkin, chunki u zaif tizimlarni aniqlash orqali kiberhujumlarga zamin yaratadi.

Theharvester vositasining ma’lumot yig‘ish mexanizmi

theHarvester — bu OSINT doirasida passiv ma’lumot yig‘ish uchun mo‘ljallangan vosita bo‘lib, u asosan domenlar, email manzillar, subdomenlar va boshqa metama’lumotlarni aniqlashga xizmat qiladi.

theHarvester turli ochiq manbalardan (qidiruv tizimlari, PGP serverlari, ijtimoiy tarmoqlar) ma’lumot yig‘adi. Ushbu jarayon “passive reconnaissance” deb ataladi, ya’ni tizimga bevosita ta’sir o‘tkazmasdan ma’lumot olishni anglatadi.

Ushbu vosita quyidagi algoritmik jarayonlarga asoslanadi:

- qidiruv tizimlariga so‘rov yuborish
- natijalarni pars qilish (parsing)
- ma’lumotlarni filtrlash va strukturaga keltirish

theHarvesterning ilmiy qiymati uning oddiyligi va samaradorligida bo‘lib, u dastlabki razvedka bosqichida muhim rol o‘ynaydi.

OSINT vositalarining solishtirma tahlili

Mazkur vositalar funksional jihatdan turli yo‘nalishlarga ixtisoslashgan:

- Maltego — bog‘lanishlar va tarmoqlarni vizual tahlil qilish

- Shodan — internet infratuzilmasini skanerlash va qurilmalarni aniqlash
- theHarvester — dastlabki ma’lumot yig‘ish va identifikatsiya

Ularning integratsiyalashgan holda qo‘llanilishi yanada samarali natijalar beradi, chunki har bir vosita OSINT jarayonining ma’lum bosqichini optimallashtiradi.

Xulosa

OSINT texnologiyalari zamonaviy axborot tahlili va kiberxavfsizlik tizimlarining muhim komponenti hisoblanadi. Maltego murakkab tarmoqlarni vizual tahlil qilish imkonini bersa, Shodan global internet infratuzilmasining holatini baholashda muhim vosita hisoblanadi, theHarvester esa boshlang‘ich razvedka bosqichini samarali tashkil etadi.

Ushbu vositalarning ilmiy asosda va qonuniy doirada qo‘llanilishi katta hajmdagi ma’lumotlarni tizimli ravishda o‘rganish va tahlil qilish imkonini beradi. Kelajakda sun’iy intellekt va katta ma’lumotlar texnologiyalarining rivojlanishi OSINT vositalarining yanada takomillashuviga olib kelishi kutilmoqda.

Adabiyotlar, References, Литературы:

1. Michael Bazzell Open Source Intelligence Techniques — *Open Source Intelligence Techniques*. 8-nashr, 2023.
2. Maltego Official Documentation, 2024.
3. Shodan Official Documentation, 2024.
4. theHarvester Documentation va GitHub sahifasi, 2023.
5. European Union Agency for Cybersecurity — *OSINT and Cyber Threat Intelligence Report*, 2022.
6. NIST — *Cyber Threat Information Sharing Guide*, 2021.