Univerzita Pavla Jozefa Šafárika v Košiciach

Prírodovedecká fakulta

AUTOMATIZÁCIA ANALÝZY OSÔB POMOCOU OTVORENÝCH ZDROJOV

BAKALÁRSKA PRÁCA

Študijný odbor:	**Informatika**
Školiace pracovisko:	**Ústav informatiky**
Vedúci záverečnej práce:	**RNDr. Eva Marková**
Konzultant:	**doc. RNDr. JUDr. Pavol Sokol, PhD.**

Košice 2024

Roman Rapco

Poďakovanie

Rád by som poďakoval vedúcej bakalárskej práce RNDr. Eve Markovej za cenné pripomienky a za obetavosť počas tvorby mojej bakalárskej práce.

Univerzita P. J. Šafárika v Košiciach
Prírodovedecká fakulta

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta:	Roman Rapco
Študijný program:	informatika (jednoodborové štúdium, bakalársky I. st., denná forma)
Študijný odbor:	Informatika
Typ záverečnej práce:	Bakalárska práca
Jazyk záverečnej práce:	slovenský
Sekundárny jazyk:	anglický

Názov: Automatizácia analýzy osôb pomocou otvorených zdrojov

Názov EN: Automation of people analysis using open sources

Cieľ: (1) Analýza a porovnanie aktuálnych prístupov a nástrojov pre analýzu osôb pomocou otvorených zdrojov.
(2) Návrh nástroja pre automatizáciu analýzy osôb pomocou otvorených zdrojov.
(3) Implementácia a vyhodnotenie nástroja pre automatizáciu analýzy osôb pomocou otvorených zdrojov.

Literatúra: (1) Hassan, Nihad A., and Nihad A. Hassan. "Gathering evidence from OSINT sources." Digital Forensics Basics: A Practical Guide Using Windows OS (2019): 311-322.
(2) Evangelista, João Rafael Gonçalves, et al. "Systematic literature review to investigate the application of open source intelligence (osint) with artificial intelligence." Journal of Applied Security Research 16.3 (2021): 345-369.

Vedúci:	RNDr. Eva Marková
Konzultant:	doc. RNDr. JUDr. Pavol Sokol, PhD.
Oponent:	RNDr. Dávid Varga
Ústav :	ÚINF - Ústav informatiky
Riaditeľ ústavu:	doc. RNDr. Ondrej Krídlo, PhD.

Dátum schválenia: 14.05.2024

Abstrakt

V tejto bakalárskej práci sa zaoberáme problematikou automatizácie analýzy osôb pomocou otvorených zdrojov. V úvode sa venujeme terminológii OSINT-u a základným informáciám o tomto procese získavania informácií. Zameriavame sa na analýzu a porovnanie existujúcich prístupov a nástrojov využívaných v tejto oblasti. Na základe tejto analýzy je navrhnutý nástroj, ktorý efektívne využíva aplikačné rozhranie (API) na získavanie údajov z rôznych otvorených zdrojov. Cieľom navrhnutého nástroja je automatizovať proces analýzy osôb pomocou OSINT techník, čím sa značne znižuje časová náročnosť a zároveň sa zvyšuje efektivita získavania relevantných informácií. Implementácia nástroja je popísaná a následne ukázaná na príkladoch. Výsledky tejto práce poskytujú prehľad o aktuálnom stave v oblasti analýzy osôb.

Kľúčové slová: *analýza osôb, informácie/dáta, nástroje, OSINT, verejné zdroje*

Abstract

In this bachelor thesis, we address the problem of automating the analysis of people using open sources. In the introduction, we discuss the terminology of OSINT and basic information about this information retrieval process. We focus on the analysis and comparison of existing approaches and tools used in this field. Based on this analysis, a tool is proposed that makes effective use of an application programming interface (API) to retrieve data from various open sources. The objective of the proposed tool is to automate the process of analyzing people using OSINT techniques, which significantly reduces the time consumption while increasing the efficiency of retrieving relevant information. The implementation of the tool is described and then demonstrated with examples. The results of this work provide an overview of the state-of-the-art in the field of person analysis.

Keywords: *person analysis, information/data, tools, OSINT, public resources*

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

V tejto práci sa venujeme analyzovaniu osôb pomocou verejne dostupných informácií a online nástrojov. Open-Source Intelligence (OSINT) má v súčasnej dobe veľmi veľké využitie v rámci informačnej bezpečnosti a kybernetickom výskume. Táto téma je čím ďalej tým viac dôležitejšia v dnešnej digitálnej dobe, kedy je prístup k informáciám z verejných zdrojov kľúčový pre rôzne odvetvia, vrátane bezpečnosti, výskumu a napríklad aj obchodnej analýzy.

Ak sa nato pozrieme z iného uhla pohľadu, napríklad z pohľadu útočníka, v súčasnosti sú hackerské skupiny čoraz viac sofistikovanejšie než kedykoľvek predtým, a to vďaka zlepšujúcim sa nástrojom, softvérom a technikám, ktoré útočníci používajú. Predtým, ako vykonajú samotný útok sa snažia špehovať svoje obete a získať, čo najviac informácií, aby mohli identifikovať slabé miesto danej obete. Najjednoduchší spôsob je čerpať z najväčšieho svetového zdroja informácií – webu. Internet je nekonečný zdroj, ktorý môžu kyberzločinci jednoducho zneužiť.

Vďaka OSINT-u používajú špecialisti IT bezpečnosti často rovnaké informačné zdroje ako kyberzločinci aj keď ich zámer použitia je odlišný. Techniky OSINT-u môžu byť využívané aj pre zisťovanie vlastných zraniteľností, napríklad v aplikáciách a využiť ich pre následnú podporu odolnosti voči ďalším útokom alebo únikom dôležitých dát pre firmu. OSINT vieme využiť aj na identifikáciu potenciálneho útočníka, teda či daný človek vôbec existuje a nie je vymyslený. Techniky a nástroje OSINT sa začali využívať približne od 80. rokov 20. storočia pre vojenské a spravodajské služby. Tieto dôležité informácie sa získavali práve z otvorených zdrojov. Napriek tomu, že v danom čase neexistovali žiadne sociálne siete, bolo možné pracovať len s informáciami z médií a verejne dostupných databáz. OSINT-ové metódy sa potom začali používať aj štátnymi orgánmi v trestnom konaní, ktoré sa tak mohli dostať k dôležitým informáciám pre vyšetrovanie zločinov a ochranu národnej bezpečnosti [**1**] . Práve ľudia, ako vyšetrovatelia to mali náročné, keďže mali za úlohu zhromažďovať všetky dostupné informácie o rôznych osobách. Často to však bol veľmi zdĺhavý a časovo

náročný proces, pretože sa to robilo manuálne.

Každoročne sa usporiadavajú súťaže pri hľadaní nezvestných osôb. Jednou z mojich najhlavnejších motivácií je touto prácou pomôcť ostatným lepšie pochopiť OSINT a využiť vedomosti v súťažiach pri hľadaní informácií o nezvestných osobách, ktorej výsledky sú následne poskytované orgánom.

Hlavným cieľom tejto práce je poskytnúť trošku komplexnejší pohľad na problematiku OSINT-u. Ďalším cieľom tejto práce je analyzovať existujúce nástroje a porovnať ich. A posledný cieľom je navrhnúť nástroj na automatizáciu analýzy osôb pomocou otvorených zdrojov, implementovať ho a vyhodnotiť.

Kapitola 1

OSINT

Definícia OSINT (Open-Source Intelligence) alebo Spravodajstvo z otvorených zdrojov je proces, ktorý sa zaoberá zhromažďovaním, spracovaním a analýzou údajov a dát z verejných zdrojov. Najhlavnejším znakom OSINT-u je zhromažďovanie verejne dostupných dát legálnou cestou. Žiadne informácie a dáta nezahŕňajú dôverné alebo utajované zdroje. Všetky analyzované údaje zväčša pochádzajú z rôznych typov zdrojov a celkový obraz vzniká vytvorením ich kombinácie [1] . Ďalej si upresníme, čo presne je informácia, a kedy pochádza z verejných zdrojov.

1.1 Open-source informácia

Informácia zahŕňa správu spolu s jej významom pre príjemcu. Ide o správu, ktorá vyjadruje určitý stav, slúži na dosiahnutie konkrétneho cieľa alebo vyvoláva nejakú akciu. Správa sa stáva informáciou buď prostredníctvom ľudskej interpretácie, spracovaním algoritmami alebo uložením v súboroch . Podľa Shannonovej teórie informácií je informácia mierou stredného informačného obsahu, prenositeľného daným kódovaním [2] . Je veľmi dôležité poznamenať, že informácia a spravodajská informácia (Intelligence), nemajú rovnaký význam. Informácie sa považujú za surové dáta, pokiaľ im neudelíme žiaden význam. Až keď tieto dáta analyzujeme detailnejšie, stávajú sa spravodajskými informáciami (Intelligence). Iným spôsobom, ako na to nazerať, je položiť si otázku 'Prečo sú tieto dáta dôležité?' a týmto informáciám tak prideliť zmysel a význam. V rámci OSINT-u, ďalej spomínané verejné zdroje a otvorené zdroje majú rovnaký význam. Každý používa iné pomenovanie, ale myslí sa to isté. Zdrojom Open-Source informácie môže byť skoro čokoľvek a pritom hovoríme o údajoch, ktoré sú napríklad publikované a odvysielané pre verejnosť, dostupné na požiadanie, dostupné na zá-

klade predplatného, získané návštevou akéhokoľvek miesta, alebo účasťou na podujatí a podobne [3] . Sú verejne dostupné pre kohokoľvek, patria tu napríklad:

- sociálne médiá,
- verejné databázy,
- online fóra a diskusné príspevky,
- noviny,
- rádio a televízia,
- tlačové konferencie,
- verejné vládne údaje, a podobne.

1.2 White intelligence

White intelligence nazývaný aj ako OSINT (Open-Source Intelligence) je čoraz častejšie využívaný. Táto forma má cieľ podporiť legitímne a etické aktivity, ako sú napríklad bezpečnostné analýzy a výskumy. Ako sme už spomínali, tak OSINT využíva informácie z otvorených, teda verejných zdrojov.

Okrem white intelligence existuje aj grey a black intelligence. Základným rozdielom medzi týmito formami je etická stránka metódy získavania informácii. White intelligence je úplne legálny spôsob získavania údajov, ktoré pochádzajú z otvorených zdrojov. Pre príklad si môžeme vziať Slovensko a jeho obchodný register, ktorý je verejne dostupný.

Grey intelligence posúva hranice svojich možností ešte ďalej tým, že okrem informácií z otvorených a legálnych zdrojov využíva aj pokročilé techniky, ako napríklad forenznú analýzu, pozorovanie osôb či používanie falošnej identity na preniknutie do konkrétneho prostredia.

Black intelligence sa posúva ešte ďalej smerom ku kontroverzným spôsobom získavania informácií. Snaží sa vyvinúť nátlak, používa provokáciu, odpočúvanie, krádež identít, nabúranie sa do systémov či prelomenie prihlasovacích údajov a hesiel [4] .

1.3 Fázy OSINT-u

Open-Source Intelligence sa delí na 4 fázy:

- OSD
- OSIF
- OSINT
- OSINT-V

Open Source Data (OSD) je sústredené na zhromažďovanie surových údajov v rôznych zdrojov - cieľom je teda zber údajov bez analýzy a spracovania. Medzi OSD môžeme zaradiť napríklad rozhlas, metadáta, obrázky, dátové súbory, elektronické dokumenty, fotografie, audio alebo aj video záznamy.

Open Source Information (OSIF / OSINF) sa týka počiatočného zoskupenia a filtrovania dát na základe nejakého kritéria, ktoré boli zhromaždené počas OSD. Sú to akékoľvek informácie, ktoré sa dajú získať legálne. Proces spracovania, triedenia a analyzovania týchto informácií sa nazýva OSINT. Príkladmi môžu byť knihy, články a rôzne príspevky na určité témy.

Open Source Intelligence (OSINT) je proces spracovania informácií z verejných zdrojov (OSIF / OSINF). Do procesu spadá triedenie, filtrovanie, analyzovanie a overenie pravdivosti informácií. Výstupom tohto procesu je informácia s nejakou pridanou hodnotou (napr. ovplyvniť rozhodovanie, analýza politickej či spoločenskej situácie, zlepšenie bezpečnosti).

Validated Open Source Intelligence (OSINT-V) je založené na overení informácií, ktoré sú dostupné z iných verejných zdrojov. Môžu sa porovnávať s informáciami získanými prostredníctvom grey alebo black intelligence. Tieto informácie majú vysoký stupeň pravdivosti po overení. Vypracovať ju môže len profesionál zameraný na overovanie informácií s prístupom k tajným spravodajským zdrojom, pracujúci pre štát alebo koaličný štáb [4] .

1.4 Účel OSINT-u

Využitie OSINT-u podľa účelu:

1. **Zvedavosť a osobný záujem:** Mnoho ľudí používa OSINT na získavanie informácií o rôznych témach, novinkách, trendoch alebo udalostiach, ktoré ich zaujímajú.

2. **Špehovanie a nežiadúce sledovanie:** Bohužiaľ, OSINT môže byť zneužitý aj na nežiadúce sledovanie jednotlivcov, aj keď nie sú zločinci apod. Títo prenasledovatelia používajú OSINT na získavanie osobných informácií a sledujú životy ľudí bez ich súhlasu.

3. **Kontrola minulosti (ang. background check):** Priemysel a zamestnávatelia často využívajú OSINT na overenie minulosti a pozadia potencionálnych zamestnancov alebo obchodných partnerov. Tento proces pomáha zabezpečiť bezpečnosť a integritu organizácií a zvyšuje dôveru medzi zaujatými stranami.

4. **Hľadanie nezvestných osôb:** OSINT sa používa aj na hľadanie nezvestných osôb. Tento proces často využívajú napríklad sukromný detektívi, vyšetrovatelia FBI alebo záchranné tímy.

5. **Riešenie bezpečnostných incidentov a ich prevencia:** Bezpečnostné organizácie a inštitúcie využívajú OSINT na monitorovanie potencionálnych hrozieb, identifikáciu zraniteľností a riešenie bezpečnostných incidentov. Slúži to na zlepšenie ochrany a bezpečnosti danej spoločnosti a jej aktív.

Ako každá jedna vec v živote má svoje dobré a zlé stránky, tak ani OSINT nie je jej výnimkou. Na jednej strane sú bezpečnostné tímy a penetrační testeri. Sú zameraní na odhalenie verejných informácií o interných aktívach a iných informáciách, ktoré sú dostupné mimo organizácie. Ich cieľom je chrániť organizácie, jednotlivcov a spoločnosť pred potenciálnymi nebezpečenstvami a zabezpečiť bezpečnosť a integritu informačných systémov. Tu patria napríklad: otvorené porty, neopravený softvér so zraniteľnosťami a ďalšie uniknuté informácie patriacej organizácii.

Na druhej strane máme útočníkov alebo skupiny útočníkov, ktorí sa snažia dosiahnuť svoje ciele, zväčša ilegálne. Ich ciele, zámer a motivácia sa veľmi často líšia. Niektorí útočníci môžu mať politický alebo aktivistický zámer a využívať OSINT na získavanie informácií o politikoch, vládnych organizáciách, alebo iných skupinách.

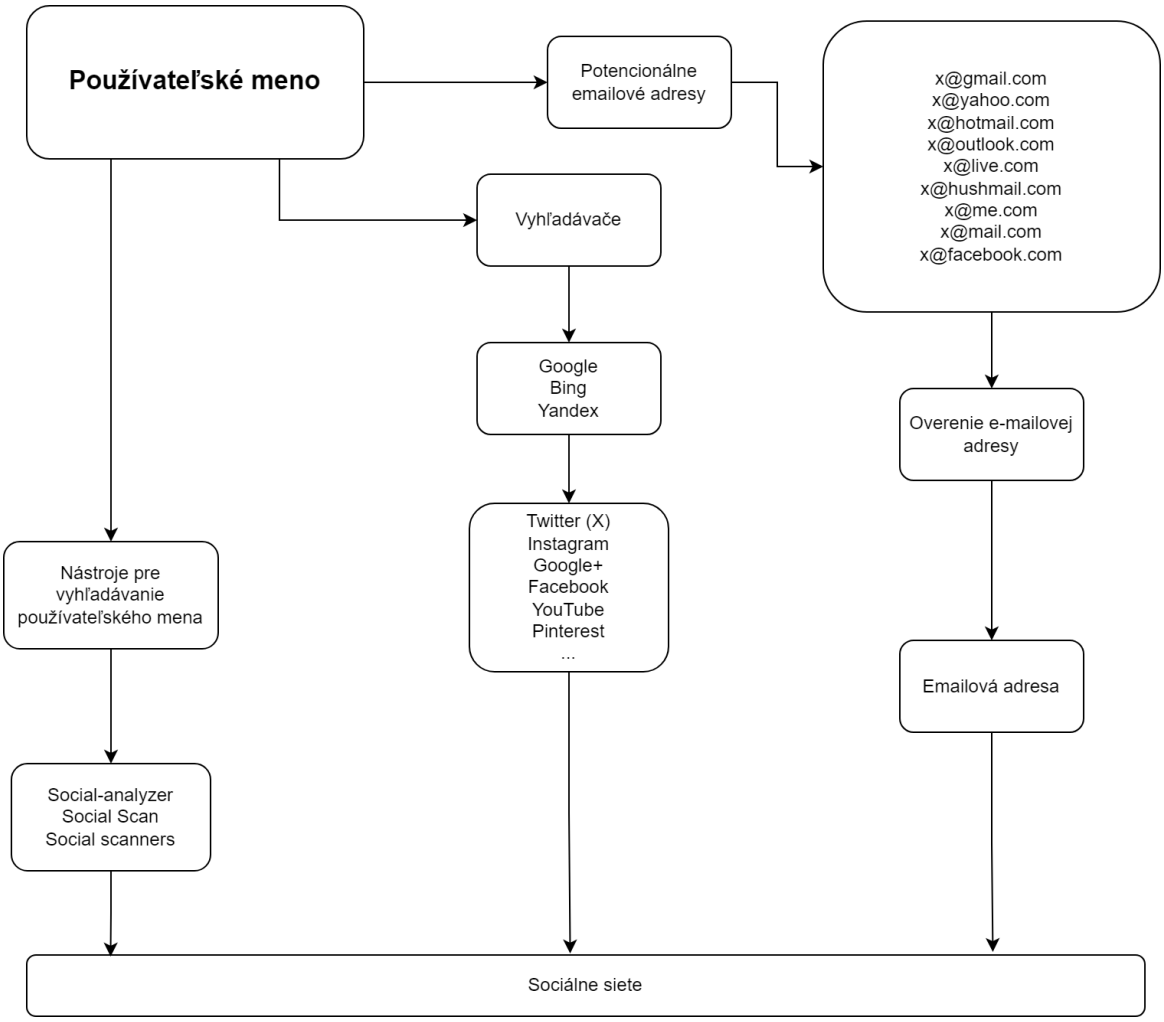
Útočníci veľmi radi využívajú sociálne inžinierstvo na získavanie citlivých informácií. Pomocou OSINT-u si vedia zistiť informácie o zamestnancoch firmy na sociálnych sieťach a potom ich použiť na vytvorenie spear-phishingových kampaní zameraných na osoby, ktoré majú prístup citlivým zdrojom [5] .

1.5 Proces OSINT analýzy

Než začneme analyzovať osobu, najprv si musíme povedať, čo všetko chceme analyzovať. Dostupných je veľa druhov informácií o osobe, ktoré nám môžu pomôcť pri analyzovaní, ako napríklad: používateľské meno, emailová adresa, reálne meno, telefónne číslo, ale aj mapy, dokumenty, obrázky, videá, vozidlá (ŠPZ), atď. Ak by sme mali napríklad k dispozícii používateľské meno osoby, ktorú hľadáme, tak by sme vedeli vydedukovať jej potencionálnu emailovú adresu. Potom pomocou emailovej adresy môžeme hľadať ďalšie spojitosti s danou osobou. Pri e-mailovej adrese to funguje opačne taktiež. Z e-mailovej adresy vieme vydedukovať používateľské meno.

V tejto bakalárskej práci sme sa rozhodli venovať procesom OSINT analýzy podľa používateľského mena, e-mailovej adresy a napokon podľa reálneho mena (meno a priezvisko). Využitie online nástrojov, aplikácii a API rozhrania namiesto manuálneho vyhľadávania dokáže ušetriť množstvo času a úsilia pri vyhľadávaní informácií. Niektoré nástroje pre dopyt využívajú API rozhranie (ang. Application programming interface). API je rozhranie, ktoré umožňuje jednej aplikácii komunikovať s inou aplikáciou alebo systémom. V našom prípade komunikujeme my ako systém, s aplikáciou, teda nástrojom. Táto komunikácia prebieha pomocou definovaného rozhrania. Tieto rozhrania sú väčšinou definované tak, že jedna aplikácia pošle požiadavku na spracovanie a druhá vráti odpoveď. Teda túto architektúru môžeme nazvať aj ako klient-server komunikáciu. Architektúra API môže používať rôzne formáty odpovede, ako napríklad XML, JSON, CSV a iné [6] .

Nasledujúce diagramy budú podobné vo využití online nástrojov a API vyhľadávaní, ale budú sa líšiť v tom, ako dosahujú výsledky.

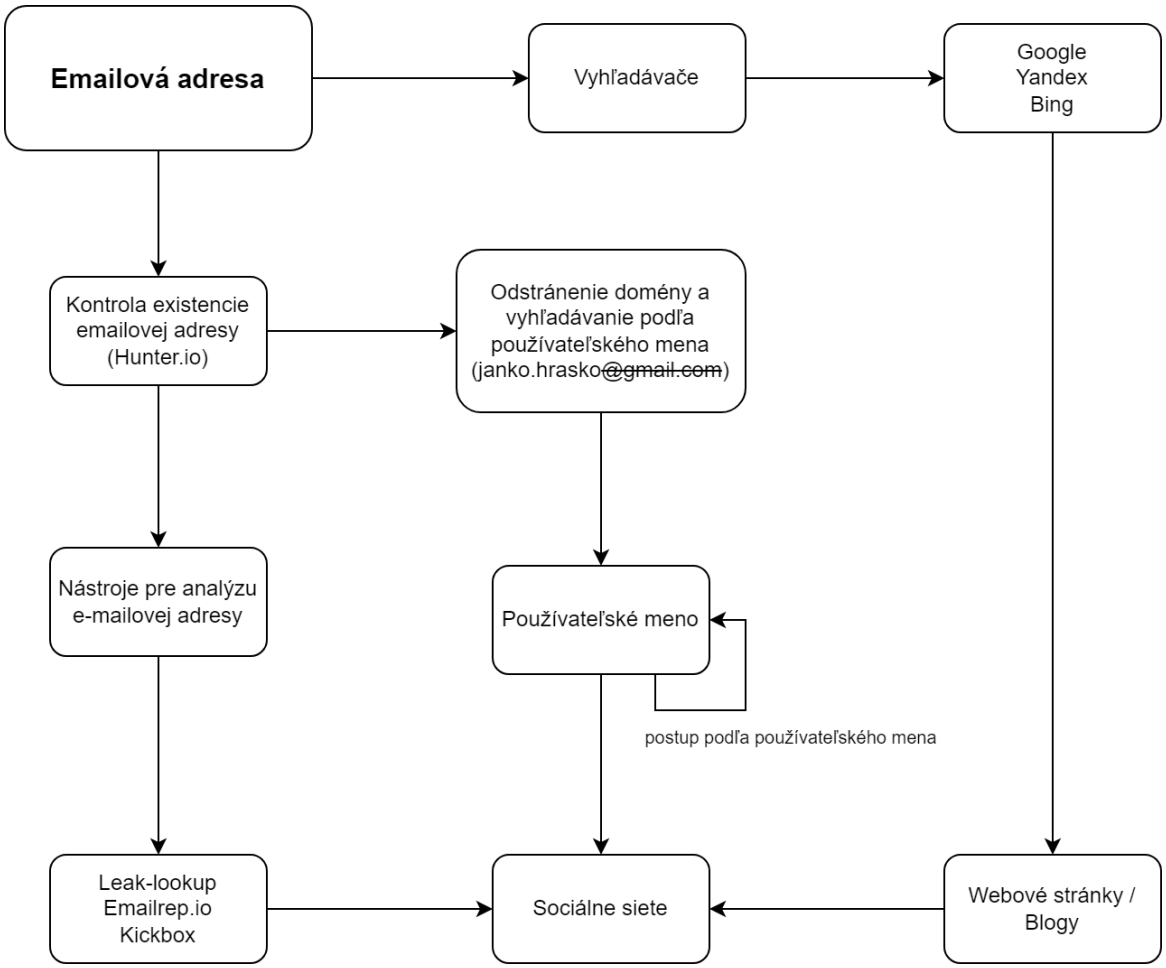


Obr. 1.1: Diagram používateľského mena

Na obrázku 1.1 môžeme vidieť, ako podľa teórie vieme z používateľského mena zistiť potencionálnu e-mailovú adresu, a to tak, že pridáme e-mailové domény za používateľské meno. Potom všetky tieto domény vieme overiť na nejakých online nástrojoch či na nich existuje dané používateľské meno.

Iný spôsob by bolo použiť vyhľadávače a manuálne prehľadávať pomocou nich sociálne médiá, ako napríklad Twitter (X), Instagram, Facebook alebo YouTube, a tak nájsť daného používateľa. S rôznymi vyhľadávačmi, ako sú napríklad Google, Bing alebo Yandex vieme použiť takzvaný 'google dorks' [7] a nájsť tak sociálne médiá spojené s používateľským menom.

Nemôžeme vynechať online nástroje pre vyhľadávanie používateľského mena. Tieto nástroje nám pomôžu nájsť na akých rôznych webových stránkach je dané používateľské meno zaregistrované. Využité nástroje môžu byť online alebo aj aplikácie či spustiteľný kód s API vyhľadávaním. Nástroje, ktoré nám pomáhajú vyhľadávať pro-



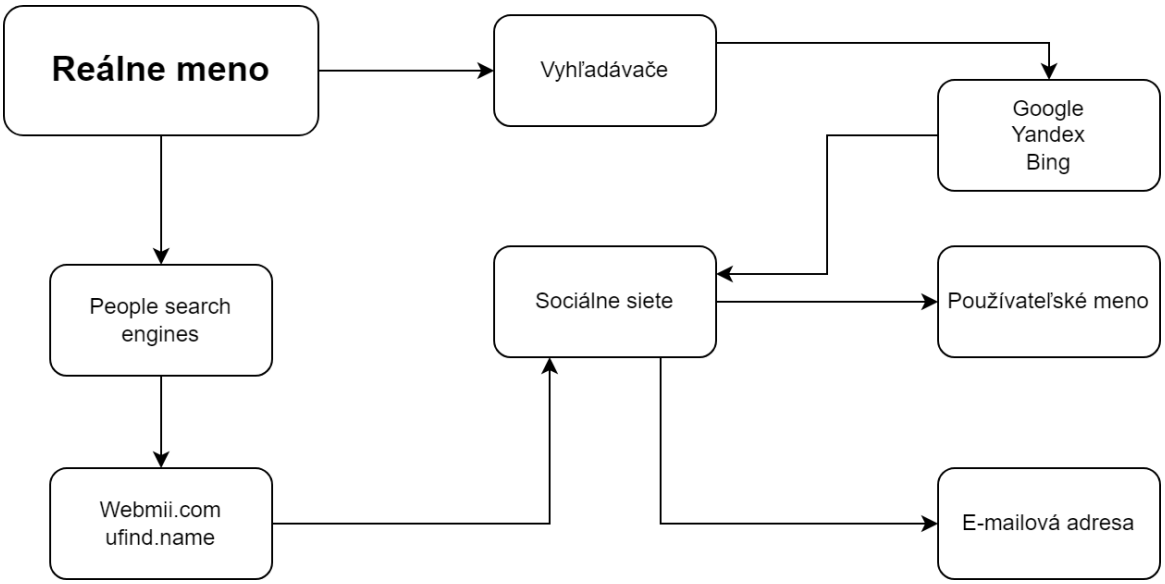
Obr. 1.2: Diagram e-mailovej adresy

fily s daným používateľským menom, sú napríklad Social-analyzer [8], Social-scan [9] alebo Social-scanners [10] .

Na obrázku 1.2 je popísaný postup ako získať informácie o osobe pomocou e-mailovej adresy. Ako prvý krok vieme skontrolovať existenciu e-mailovej adresy. Po odstránení domény z e-mailovej adresy vieme získať potencionálny používateľské meno. Ďalej k nemu vieme pridať iné domény, a tak otestovať ďalšie potencionálne e-mailové adresy spojené s týmto používateľským menom. S používateľským menom vieme prejsť na postup vyhľadávanie informácií podľa používateľského mena a nájsť tak profily na sociálnych sieťach spojených s daným používateľom.

S vyhľadávačmi ako sú Google, Yandex a Bing vieme taktiež využiť 'google dorks' a nájsť tak informácie ohľadom e-mailovej adresy. Po prezretí webových stránok vieme naraziť na používateľské meno spojené s touto e-mailovou adresou.

S e-mailovou adresou nám tu pribúdajú úniky dát z rôznych databáz webových stránok. Vieme využiť napríklad službu Leak-lookup [11] alebo diagnostiku e-mailovej



Obr. 1.3: Diagram reálneho mena

adresy pomocou služby Emailrep.io [12] . Na výstupe sa vieme dostať k sociálnym sieťam danej osoby.

Na obrázku 1.3 je postup získavania informácií o osobe pomocou jej reálneho mena. Manuálne vieme zadať ich meno do vyhľadávania rôznych sociálnych sietí, ako sú napríklad Twitter (teraz už X) alebo Facebook. Na týchto sociálnych sieťach vieme nájsť dôležité informácie, no nie vždy sú verejne dostupné, záleží od používateľa, a ako si oni určili ich verejnosť. Ďalej vieme využiť vyhľadávače, ako sú napríklad Google, Bing a Yandex, teda využiť 'google dorks'. Google dorking je na manuálne vyhľadanie informácií mimo USA ten najsilnejší nástroj. Mimo USA môžeme využiť vyhľadávače pre hľadanie informácií o osobách ako sú napríklad Webmii [13] alebo ufind.name [14] . Tieto vyhľadávače nám môžu pomôcť pri hľadaní dôležitých informácií a pri hľadaní profilov používateľa na sociálnych sieťach. Zo sociálnych sietí je možné získať a analyzovať údaje týkajúce sa používateľských mien a e-mailových adries.

1.6 Sock Puppet

Sock Puppets (j.č. ponožková bábka) sú podrobne vytvorené falošné účty na sociálnych sieťach, ktoré slúžia na použitie OSINT-u bez toho, aby prezradili svoju skutočnú identitu. Majú nejaký konkrétny cieľ a sú súčasťou techniky sociálneho inžinierstva OSINT. Túto techniku Sock Puppet môže používať ktokoľvek, napríklad vyšetrovatelia, detektívi, hackeri, polícia, novinári alebo stalkeri, teda ktokoľvek, kto sa chce vydávať za niekoho iného. Sock Puppet účty sa vytvárajú, aby mali prístup k obsahu na rôznych stránkach, napríklad na platformách sociálnych médií, kde je obsah dostupný len s vytvoreným účtom. Na vytvorenie Sock Puppet-u je potrebné, aby bol dôveryhodný a tváril sa ako skutočná osoba. Sock Puppet-y majú reálne meno, skutočné telefónne čísla, adresu, fotografie, číslo kreditnej karty, rôzne účty na sociálnych sieťach, ale aj priateľov atď.

Sock Puppet sa dá využiť rôznymi spôsobmi, ako napríklad:

1. Vyšetrovatelia vedia zhromažďovať informácie a robiť výskum niektorých vyšetrovaní.

2. Útočníci môžu používať Sock Puppet účet na sociálne inžinierstvo, aby získali informácie.

3. Detektívi využívajú Sock Puppet aby sa vcítili do povahy niekoho na zhromaždenie informácií.

Sock Puppet by nemal nikdy byť spojený s pôvodným majiteľom. Ak chceme anonymizovať účet tak, aby nezaznamenal pôvodnú IP adresu alebo polohu, je potrebné použiť VPN pri jeho vytváraní. Treba si ale dávať pozor a prihlasovať sa vždy cez rovnakú sieť. Aby vyzeral účet čo najreálnejšie a legitímne, treba ho používať dlhodobo, to znamená denne niečo zverejňovať, sledovať ľudí a mať priateľov. V kapitole nižšie popisujeme, ako si vytvoriť Sock Puppet [15] .

1.6.1 Vytvorenie Sock Puppet účtu

Pre vytvorenie Sock Puppet účtu potrebujeme meno. Pre vygenerovanie falošného mena môžeme použiť stránku FakeNameGenerator [16] alebo elfqrin fakeid [17] . Z týchto generátorov falošných identít vieme vytvoriť osobu, ktorá neexistuje s menom, priezviskom, adresou, e-mailovou adresou, fyzickými vlastnosťami, kreditnou kartou,

dátumom narodenia, obľúbenou farbou či s ŠPZ vozidla, ktoré vlastní a mnoho iných druhou informácií. Tieto informácie sa dajú dodatočne meniť, ako si zmienime.

Ďalej potrebujeme e-mailovú adresu zodpovedajúcu tomuto menu. Na vytvorenie e-mailovej adresy vieme použiť ľubovoľného poskytovateľa e-mailovej služby, ako napríklad Gmail . Medzi najpoužívanejších poskytovateľov e-mailových služieb patrí:

- Gmail.com
- Yahoo mail
- Proton Mail
- Mail.com

Odporúčaná e-mailová adresa je mail.com, ale treba sa uistiť, že nepoužívate už existujúcu e-mailovú adresu.

Ďalším krokom je vygenerovanie tváre pre nami vytvorenú falošnú identitu. Na vygenerovanie tváre vieme použiť napríklad túto službu ThisPersonDoesNotExist [18] . Táto stránka využíva AI a pomocou neho vytvára falošné tváre, ktoré neexistujú v reálnom svete, takže sa budete vydávať za živú osobu.

Ak by sme chceli OSINT posunúť ešte viac do hĺbky, tak si zariadime jednorazový telefón a SIM kartu, ktorý nebude nijako prepojený s nami. SIM kartu použijeme iba pre Sock Puppet účet a nič viac. Robí sa to, pretože niektoré webové stránky potrebujú overenie pomocou telefónneho čísla, aby nevznikalo veľa falošných účtov a identít.

Kapitola 2

Analýza osôb pomocou otvorených zdrojov

V dnešnej digitálnej ére je obrovské množstvo informácií o ľuďoch dostupných online. Tieto informácie sa môžu týkať rôznych aspektov, od reálneho mena až po adresu bydliska. Existuje množstvo nástrojov na každý jeden z týchto aspektov, a preto ich vieme porovnávať a hodnotiť ich funkčnosť a efektivitu v rámci analýzy osôb.

V tejto kapitole sa zameriame na rôzne prístupy k analýze osôb prostredníctvom otvorených zdrojov (OSINT). Najprv poskytneme prehľad existujúcich prác a štúdií, ktoré sa venujú tejto problematike. Následne sa podrobne zaoberáme technikami vyhľadávania informácií pomocou používateľského mena, e-mailovej adresy a reálneho mena.

Používateľské mená sú často konzistentné naprieč rôznymi platformami, čo umožňuje sledovať online prítomnosť jednotlivcov a ich aktivitu na sociálnych sieťach či iných webových stránkach. E-mailové adresy môžu odhaliť ďalšie informácie, ako sú sekundárne účty alebo iné služby, ktoré daná osoba používa. Analýza reálneho mena môže viesť k objaveniu verejných profilov, dôležitých záznamov a ďalších údajov. Popíšeme si bližšie aplikácie, služby a techniky, ktoré sú použité na získavanie týchto informácií. Predtým než prejdeme k ďalšej časti si uvedieme prehľad niektorých populárnych nástrojov a služieb, ktoré sa používajú na analýzu osôb. Tento obrázok tabuľky 2.1 a 2.2 poskytuje informácie o jednotlivých nástrojoch, ich funkcionalite, dostupnosti API, cene a ďalších relevantných aspektoch. Tabuľka obsahuje nasledujúce informácie:

- OSINT nástroje: Meno konkrétneho nástroja alebo služby.

- Krajina: Krajina v ktorej vieme daný nástroj alebo službu použiť.
- Zameranie: Oblasť alebo téma, na ktorú je nástroj alebo služba špecializovaná.
- Cena: Informácia o cene použitia nástroja alebo služby.
- API: Áno/Nie, či je k dispozícii API pre automatizovaný prístup k dátam.
- Cena API: Cena použitia API, ak je dostupné, prádzne políčko alebo - znamená že API nie je implementované.
- Registrácia API: Je alebo nie je potrebná registrácia pre použitie.

OSINT nástroje	Krajina	Zameranie
Dehashed	univerzálne použitie	e-mailová adresa, používateľské meno, reálne meno, adresa, telefónne číslo, IP adresa
Leakcheck	univerzálne použitie	e-mailová adresa, používateľské meno
Email Address Validator	univerzálne použitie	e-mailová adresa
socialscan	univerzálne použitie	používateľské meno
social-scanner	univerzálne použitie	používateľské meno
social-analyzer	univerzálne použitie	používateľské meno
kickbox	univerzálne použitie	e-mailová adresa
emailrep.io	univerzálne použitie	e-mailová adresa
leak-lookup	univerzálne použitie	e-mailová adresa
Hunter	univerzálne použitie	e-mailová adresa, názov firmy, lokácia firmy, doména
Have I Been Pwned	univerzálne použitie	e-mailová adresa, heslá
ThatsThem	univerzálne použitie	reálne meno, adresa, telefónne číslo, e-mailová adresa, IP adresa, ŠPZ
Sherlock	univerzálne použitie	používateľské meno
ufind.name	univerzálne použitie	reálne meno
WhatsMyName	univerzálne použitie	používateľské meno
Blackbird	univerzálne použitie	používateľské meno
Spokeo	USA	reálne meno, e-mailová adresa, telefónne číslo, adresa
FamilySearch	USA	reálne meno
Pipl	USA	reálne meno
fake name generator	univerzálne použitie	reálne meno
thispersondoesnotexist	univerzálne použitie	reálna osoba
true people search	USA	reálne meno, telefónne číslo, adresa bydliska, e-mailová adresa
fast people search	USA	reálne meno, telefónne číslo, adresa bydliska
search people free	USA	reálne meno, telefónne číslo, adresa bydliska, e-mailová adresa

Tabuľka 2.1: Porovnanie nástrojov č.1

OSINT nástroje	CENA	API	Cena API	Registrácia API
Dehashed	spoplatnene	A	spoplatnene	A
Leakcheck	bezplatne	A	bezplatne	A
Email Address Validator	bezplatne	A	bezplatne	A
socialscan	bezplatne	N	_	_
social-scanner	bezplatne	A	bezplatne	A
social-analyzer	bezplatne	N	_	_
kickbox	bezplatne	A	bezplatne	A
emailrep.io	bezplatne	A	bezplatne	A
leak-lookup	bezplatne	A	bezplatne	A
Hunter	bezplatne	A	bezplatne	A
Have I Been Pwned	bezplatne	A	spoplatnene	A
ThatsThem	bezplatne	N	_	_
Sherlock	bezplatne	N	_	_
ufind.name	bezplatne	N	_	_
WhatsMyName	bezplatne	N	_	_
Blackbird	bezplatne	N	_	_
Spokeo	bezplatne	A	spoplatnene	A
FamilySearch	bezplatne	A	bezplatne	A
Pipl	spoplatnene	A	spoplatnene	A
fake name generator	bezplatne	A	_	_
thispersondoesnotexist	bezplatne	A	bezplatne	A
true people search	bezplatne	A	bezplatne	A
fast people search	bezplatne	A	bezplatne	A
search people free	bezplatne	A	bezplatne	A

Tabuľka 2.2: Porovnanie nástrojov č.2

Tento prehľad umožňuje rýchle porovnanie a výber najvhodnejšieho nástroja alebo služby pre konkrétnu analýzu osôb. V prípade fake name generator odkaz na API nebol dostupný, takže nevieme či ešte stále funguje alebo je k dispozícii.

Postupne sa zaoberáme existujúcimi výskumami a prácami v danej oblasti, prechádzame k analýze prostredníctvom používateľského mena, reálneho mena, e-mailovej adresy a nakoniec popisujeme služby, ktoré vieme použiť na analýzu na Slovensku.

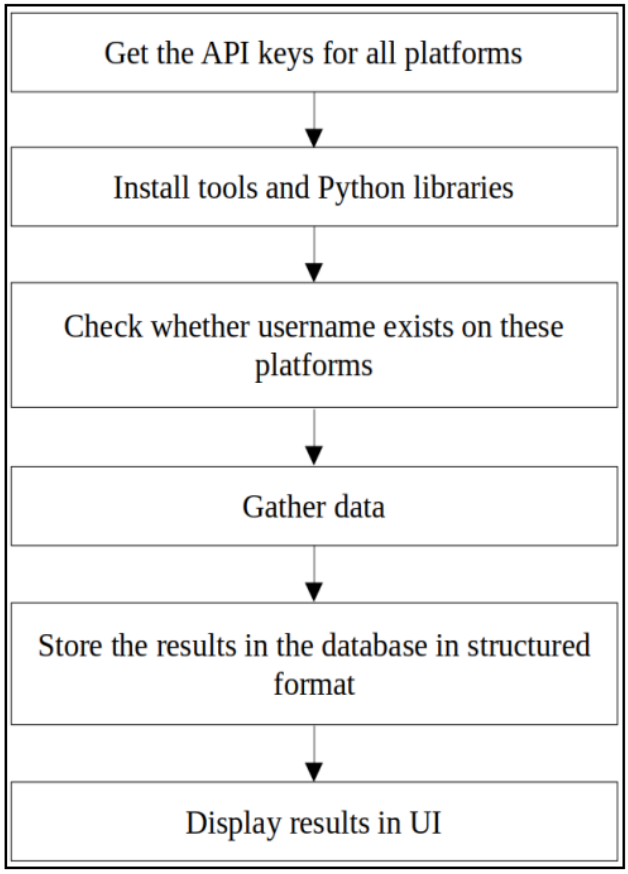
2.1 Podobné práce

V tejto sekcii sme sa venovali analýze a porovnávaniu tejto práce s podobnými existujúcimi štúdiami v literatúre. Cieľom je pozrieť sa na rozdiely, prínosy a podobnosti v rámci danej oblasti. Tieto práce boli vybrané na základe relevancie a významu s touto prácou.

Prvý článok, ktorým sa zaoberáme je od autora Martina Nobili a spol. [19]. Hlavnou témou je prehľad hlavných nástrojov OSINT, ktoré slúžia na boj proti sociálnemu inžinierstvu a prevenciu jeho útokov. Presnejšie, poukazuje na rôzne nástroje a ich získavanie informácií, ako je napríklad e-mailová adresa, sociálne profily, telefónne čísla, a tak ďalej. Popisuje metodológiu OSINT, preskúmavanie OSINT nástrojov, experimentáciu s rôznymi typmi nástrojov a ich analýzou a diskusiu a budúce štúdiá. Taktiež porovnávajú pozitívnu a chybovú mieru týchto nástrojov. V článku sa nachádzajú aj popisy rôznych nástrojov a služieb, ktoré využívame v našom nástroji.

Ďalší článok v poradí, od autorov Manohari D a spol. [20], kde sa venujú získavaniu informácií pomocou OSINT nástrojov a hľadaniu cenných informácií, ktoré môžu zabrániť útoku na cieľ. Cieľom proaktívnych opatrení je vedieť predvídať kybernetické útoky a tak im aj predchádzať. V článku sa zaoberajú novými opatreniami proti kybernetickým hrozbám a kybernetickej kriminalite, ktoré sa dajú dosiahnuť vylepšením získavania informácií pomocou OSINT. Autori článku popisujú vyhľadávanie informácií o používateľskom mene a reálnom mene pomocou rôznych nástrojov ako je napríklad nástroj Sherlock. Sekcie o vyhľadávaní sociálnych profilov a vyhľadávaní emailovej adresy a telefónneho čísla sú taktiež zahrnuté v tomto článku.

V treťom článku od autorov Ashok Yadav a spol. [21] sa obracajú na trochu iný smer, a to na strojové učenie a hĺbkové učenie. V tomto článku popisujú aktuálny stav



Obr. 2.4: Vývojový diagram navrhovaného systému [22]

OSINT nástrojov a techník a ich stav použitia pre rôzne aplikácie v kyberbezpečnosti. Autori bližšie analyzujú výzvy a budúce smery pre rôzne autonómne modely a systémy.

V predposlednom článku od autorov Nilesh Sambhe a spol. [22] sa zaoberajú vytváraním softvéru, teda nástroja, ktorý získava verejne dostupné informácie o osobách a zhromažďuje dáta v štruktúrovanej podobe na jednom mieste. Tento nástroj prehľadáva profil používateľa na rôznych sociálnych sieťach a zhromažďuje tieto informácie. Tieto informácie sú dostupné pre používateľa s možnosťou exportovať informácie do rôznych digitálnych dokumentárnych foriem. Implementácia nástroja a proces získavania a zobrazovania výsledkov je podobný, ako v našom prípade pri nástroji. Článok obsahuje obrázok 2.4 pre systém vývoja nástroja v danom článku.

Piaty a posledný článok je od autorov JAVIER PASTOR-GALINDO a spol. [23]. Tento článok opisuje súčasný stav OSINT so zameraním na služby a techniky, ktoré posilňujú oblasť kybernetickej bezpečnosti. Článok je rozdelený na dve časti. Prvá časť sa zaoberá analyzovaním silných stránok tejto metodiky a navrhuje spôsoby uplatnenia v oblasti kyberbezpečnosti. Druhá časť sa zaoberá obmedzeniami pri používaní OSINT. Keďže v tejto oblasti je ešte veľa, čo sa dá skúmať, tak autori popisujú niektoré otvorené výzvy, ktoré bude potrebné niekedy v budúcnosti riešiť.

Všetky články sa z časti venujú problematike OSINT-u a každý článok nám dodal nové poznatky v oblasti bezpečnosti a OSINT-u. Tieto články nás výrazne ovplyvnili a pomohli nám pri návrhu a implementácii zostrojeného nástroja, aby sme dosiahli čo najlepšie výsledky.

2.2 Nástroje pre analýzu používateľského mena

Po získaní používateľského mena pre online platformu, môže táto informácia naviesť k ďalšiemu potencionálnemu množstvu dát. Väčšina aktívnych používateľov internetu používajú rovnaké používateľské meno na viacerých webových stránkach. Napríklad používateľské meno 'roman6126' na Instagrame môže byť rovnaká osoba 'roman6126' na Tiktoku. Manuálne vyhľadávanie používateľského mena môže byť dobrý začiatok, ale vyhľadávať na všetkých dostupných online platformách a webových stránkach na internete by bolo časovo náročné a skoro nemožné. Preto ak navštívime jeden z nástrojov, ktoré spomenieme, môže nám to pomôcť v prehľadávaní webových stránok a online platforiem a vo výsledku dostaneme dostupnosť týchto používateľských mien na konkrétnych webových stránkach alebo priamo odkaz na profil, kde sa nachádza.

KnowEm [24] je jedna zo služieb pre vyhľadávanie používateľského mena. Na hlavnej stránke sa nachádza jedno vyhľadávacie pole, do ktorého, keď zadáme používateľské meno, tak skontroluje jeho dostupnosť na všetkých populárnych webových stránkach. Ak zobrazená webová stránka je priesvitná a slovo 'available' je prešKrtnuté, tak to znamená, že daný profil na webovej stránke už existuje a nie je dostupné pre kohokoľvek iného. Ak stránka nie je priesvitná a nemá slovo 'available' prešKrtnuté, to znamená, že profil na takejto stránke neexistuje a môže byť vytvorené. Odkaz, ktorý sa nachádza nižšie a má oranžové pozadie nás odkáže na novú webovú stránku, kde je vyhľadávanie používateľského mena na ďalších viac ako 500 sociálnych sieťach. Toto vyhľadávanie sa delí na 14 ďalších kategórií. Pre rozkliknutie danej kategórie stačí kliknúť na 'pozrite si túto kategóriu'. Manuálne prehľadávanie vyžaduje určitý čas,

avšak môže poskytnúť množstvo zaujímavých informácií. Stránka síce nemá protokol HTTPS, ale to by nemal byť veľký problém.

WhatsMyName [25] je služba, ktorý sa po prvý krát objavila v roku 2020 a funguje veľmi podobne ako predošlé zmienené nástroje. Avšak je veľmi dobré mať nástroj, navyše ktorý má funkcie naviac. Výsledky tohto dopytu vieme exportovať do schránky, XLSX, CSV alebo do PDF. Táto webová stránka má taktiež na výber kategórie a môže medzi nimi filtrovať výsledky. Ak by táto služba podporovala technológiu API, mala by oveľa väčšie využitie a efektívne by skrátila čas pri vyhľadávaní sociálnych účtov o danom používateľovi.

2.3 Nástroje pre analýzu e-mailovej adresy

Analýza e-mailovej adresy poskytuje cenné informácie, ktoré nám umožňujú lepšie porozumieť a identifikovať používateľa. E-mailová adresa sa skladá z dvoch hlavných častí: elektronická adresa identifikujúca meno používateľa a názov domény poskytovateľa elektronickej pošty daného užívateľa.

Používateľské meno predstavuje osobnú identifikáciu používateľa a môže obsahovať dôležité informácie, ako sú meno, priezvisko alebo iné identifikátory. Tento údaj nám môže poskytnúť dôležité indície o používateľovi, jeho preferenciách a aktivitách na internete. Napríklad, používateľské meno v e-mailovej adrese môže byť rovnaké ako na rôznych online platformách, čo nám umožňuje identifikovať používateľa na týchto platformách a sledovať jeho aktivity.

Druhá časť e-mailovej adresy, doménový názov, poskytuje informácie o poskytovateľovi e-mailovej služby. Tento údaj nám môže poskytnúť informácie o organizácii, inštitúcii alebo spoločnosti, ktorej používateľ patrí. Napríklad, v prípade e-mailovej adresy 'meno.priezvisko@upjs.sk' nám doménový názov 'upjs.sk' hovorí, že používateľ je spojený s Univerzitou Pavla Jozefa Šafárika.

HaveIBeenPwned [26] je zlatý štandard pre únik údajov v komunite OSINT nadšencov. Táto služba povoľuje na vstup používateľské meno alebo e-mailovú adresu, ale najviac spoľahlivé výsledky sú len pre e-mailovú adresu. Vo výsledku je popis každého úniku dát z databázy stránok, kde bola daná e-mailová adresa nájdená, teda zaregistrovaná. Tieto popisy sú detailné a nápomocné, keďže píšu typ služby, z ktorej bol únik a počet kompromitovaných používateľov.

Dehashed [27] je veľmi podobný nástroj ako predošlý HIBP, ale s tým rozdielom, že Dehashed zahŕňa do svojej databázy aj menej známe úniky z databáz, ktoré ešte

neboli zverejnené na HIBP. Ak by sme skombinovali tieto dva výsledky, tak by sme vedeli s väčšou šancou povedať, že daná e-mailová adresa je reálna a nie vymyslená. Dehashed má taktiež platenú verziu nástroja, kde za menší poplatok môžeme vidieť uniknuté heslá.

2.4 Nástroje pre analýzu reálneho mena

Reálne meno používateľa je jedným z najdôležitejších identifikačných údajov. Pri analýze reálneho mena vieme získať množstvo dôležitých informácií o danej osobe. Okrem základných informácií, ktoré máme k dispozícii, ako sú meno a priezvisko vieme zistiť aj ďalšie údaje, ako sú napríklad pohlavie, vek, etnický pôvod a ďalšie osobné charakteristiky, ktoré nám pomôžu pri analýze osoby. Navyše vieme taktiež identifikovať sociálneho účty spojené s danou osobou. Môžeme zistiť, s kým je osoba spojená a aké vzťahy má jednotlivcami, organizáciami alebo so skupinami. Celkovo, analýza reálneho mena je kľúčovým prvkom v procese identifikácie a analýzy online používateľov. Poskytuje nám dôležité informácie o používateľoch, ich identite a aktivitách, ktoré nám pomáhajú lepšie porozumieť ich správanie a ako interagujú s inými osobami.

ThatsThem [28] je webová stránka pre vyhľadávanie informácií o osobe podľa reálneho mena. Tento nástroj má veľa možností na vstup. Na výber do vstupu vieme zadať:

- meno a priezvisko s mestom, štátom alebo ZIP kódom,
- adresu bývania,
- telefónne číslo,
- e-mailovú adresu,
- IP adresu,
- alebo identifikačné číslo vozidla.

Do vstupu je lepšie zadať s menom a priezviskom aj mesto a štát, ale nie je to nevyhnutné. Výsledkom vstupu mena a priezviska je adresa bydliska, telefónne číslo, domovská IP adresa, akékoľvek e-mailové adresy spojené s týmto bydliskom, finančné detaily, náboženstvo a vek osoby. Finančné detaily a náboženstvo nie sú spoľahlivé dáta. Tento nástroj má vcelku skvelé výsledky vzhľadom k tomu, že je zadarmo, každopádne funguje iba v štátoch USA.

Spokeo [29] je jeden z najznámejších vyhľadávačov pre reálne meno. Spokeo má dve verzie, prémiovú, platenú verziu a bezplatnú verziu. Platená verzia poskytuje širokú škálu dostupných a presných údajov, avšak vyžaduje určitú finančnú investíciu. Výsledky pre zadané meno sú zobrazené až po zadaní mesta a štátu do vyhľadávania. Teda výsledkom sú iba profily zo zadaného mesta a štátu. Po vybraní profilu sa zobrazia výsledky. Profil zväčša obsahuje celé meno, pohlavie, rok a bývalé bydlisko. Všetky odkazy a dáta, ktoré nie sú dostupné, sú dostupné len v prémiovej verzii.

2.5 Nástroje pre analýzu na Slovensku

Pri analýze osôb na Slovensku je k dispozícii niekoľko špecifických nástrojov a zdrojov informácií, ktoré môžu byť mimoriadne užitočné. Medzi tieto nástroje patria verejné registre, databázy a služby, ktoré zhromažďujú a sprístupňujú údaje o jednotlivcoch. Dôležitým zdrojom sú napríklad katastre nehnuteľností, ktoré poskytujú informácie o vlastníckych vzťahoch k nehnuteľnostiam. Ďalej môžeme využiť obchodný register, ktorý obsahuje údaje o podnikateľských subjektoch a ich štatutároch. Tieto nástroje sú kľúčové pre získavanie relevantných a overených informácií pri analýze osôb na Slovensku.

V nasledujúcom obrázku si uvedieme prehľad rôznych nástrojov, ktoré sú k dispozícii na analýzu osôb na Slovensku. Tieto nástroje sú zoskupené ako v predošlej tabuľke podľa zamerania, dostupnosti API, ceny a požiadavky na registráciu. Táto tabuľka poskytuje komplexný prehľad, ktorý ukazuje porovnanie rôznych nástrojov pre rôzne kritéria potrieb analýzy. Na obrázkoch nižšie môžete vidieť tabuľky 2.3 a 2.4, ktoré sumarizujú tieto údaje:

OSINT nástroje	Zameranie
sport.iedu	reálne meno, športový klub, národný športový zväz
kdeje.info	reálne meno
zbgis.skgeodesy.sk	obec, katastrálne územie, číslo parcely, číslo listu vlastníctva, priezvisko a meno vlastníka
kataster.skgeodesy.sk	listy vlastníctva, parcely registra C, parcely registra E, byty a nebytové priestory, fyzické osoby
google.sk/maps	reálne meno, ulica, mesto, reštaurácie, hotely, zážitky, múzeá, lekárne, bankomaty, kostoly, obchody
generator rodneho cisla	rodné číslo
telefonny zoznam	telefónne číslo, reálne meno, ulica, číslo ulice, psč, mesto
o2 overenie operátora	telefónne číslo
telekom overenie operátora	telefónne číslo
slick.ly/sk	telefónne číslo
orsr.sk	obchodné meno, identifikačné číslo sídla, spisová značka, reálne meno osoby
zrsr.sk	IČO, obchodné meno, reálne meno, adresa prevádzkarne, cezhraničný poskytovateľ služby na území SR
rpo.sk	identifikátor právnickej osoby a podnikateľa, plné meno, právnickej osoby, právna forma...
ives.minv.sk	vyhľadávanie organizácií, fyzická osoba, právnická osoba
finstat.sk	spoločnosť alebo IČO
finreg.sk	názov firmy, meno osoby, ičo, dič, ič dph, adresa
dlznik.zoznam.sk	firmy, dlžníci, inštitúcie
portaludzs.sk	overenie poistného vzťahu poistenca
potvrdeniaonavsteveskoly	potvrdenie o návšteve školy (rodné číslo študenta)

Tabuľka 2.3: Nástroje na Slovensku č.1

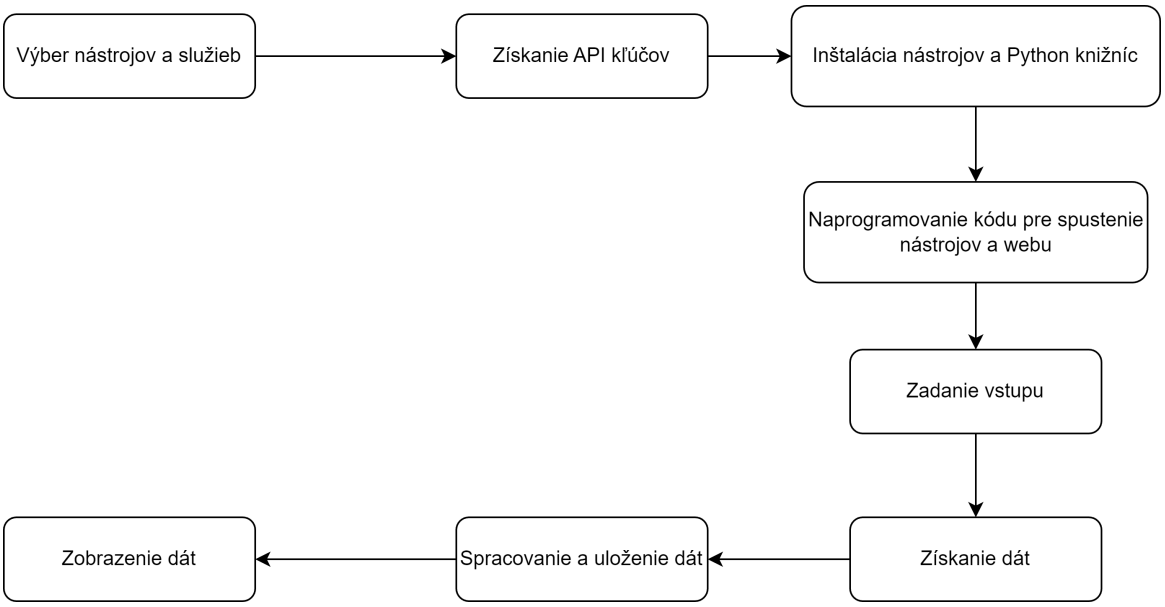
OSINT nástroje	API	Cena	Registrácia
sport.iedu	N	bezplatne	N
kdeje.info	N	bezplatne	N
zbgis.skgeodesy.sk	N	bezplatne	N
kataster.skgeodesy.sk	N	bezplatne	N
google.sk/maps	N	bezplatne	N
generator rodneho cisla	N	bezplatne	N
telefonny zoznam	N	bezplatne	N
o2 overenie operátora	N	bezplatne	N
telekom overenie operátora	N	bezplatne	N
slick.ly/sk	N	bezplatne	N
orsr.sk	N	bezplatne	N
zrsr.sk	A	bezplatne	N
rpo.sk	A	bezplatne	A
ives.minv.sk	N	bezplatne	N
finstat.sk	A	bezplatne	N
finreg.sk	N	bezplatne	N
dlznik.zoznam.sk	N	bezplatne	N
portaludzs.sk	N	bezplatne	N
potvrdeniaonavsteveskoly	N	bezplatne	N

Tabuľka 2.4: Nástroje na Slovensku č.2

Kapitola 3

Návrh nástroja na automatizáciu

Všetky dáta, ktoré sa získavajú pomocou rôznych nástrojov a služieb môžu byť zobrazované napríklad na webovej stránke. Niektoré nástroje je však potrebné nainštalovať a použiť v termináli. Vyššie v kapitole o OSINT sme diskutovali, že architektúra API môže poskytovať rôzne formáty odpovedí pri komunikácii medzi serverom a klientom. V našom prípade by bolo najvhodnejšie pracovať s jednotným formátom dát, pričom najčastejšie používaným formátom je JSON. Ak nástroj alebo služba podporuje technológiu API kľúčov, vo väčšine prípadov bude odpoveď servera v formáte JSON. Po prijatí údajov zo servera je potrebné ich uložiť, následne spracovať do čitateľného formátu a zobraziť vo webovom rozhraní, aby sa bežný používateľ mohol ľahšie orientovať v texte. Na obrázku 3.5 môžeme vidieť diagram pre funkčnosť a návrh na implementáciu tohto nástroja.



Obr. 3.5: Diagram implementácie nástroja

Technológie, ktoré boli použité v implementácii zahŕňajú Python, API kľúče, Python knižnicu requests, html, JSON a Flask. Ako prvý krok je výber nástrojov a služieb, ktoré budeme používať. V druhom kroku sa budeme venovať inštalácii doplnkových nástrojov, teda nástrojov a služieb, s ktorými budeme pracovať a ešte technológie ktoré v implementácii budeme využívať. V predposlednom kroku sa zameriame na spracovanie a ukladanie dát. Po prijatí dát zo servera je potrebné ich spracovať a uložiť do správneho formátu. V poslednom kroku sa zameriame na zobrazenie týchto spracovaných dát vo webovom rozhraní. Tento krok zahŕňa implementáciu užívateľského rozhrania pomocou webových technológií, ako je Flask.

Nástrojov na hľadanie informácií o osobách je veľké množstvo a nie každý z nich je zadarmo. Ako sme spomínali, niektoré nástroje sú platené a niektoré majú skúšobnú dobu, ale pár z nich je aj voľne dostupných.

Existuje množstvo bezplatných a veľmi užitočných nástrojov. Informácie je možné vyhľadávať napríklad prostredníctvom „Google dorks“. Vďaka tomuto vieme vyhľadávať viac špecificky, súbory alebo údaje z konkrétnych domén. Podobne vieme využívať aj Bing, Yandex alebo Searx, metavyhľadávač, ktorý umožňuje zhromažďovať anonymne výsledky z viac vyhľadávacích služieb. Nižšie v pod kapitole si bližšie popíšeme výber nástrojov a služieb v našom návrhu na automatizáciu analýzy osôb.

3.1 Výber nástrojov a služieb

Pri výbere nástrojov pre automatizáciu sme sa pozerali na viacero faktorov, ale najhlavnejšie z nich bola ich cenovú dostupnosť či majú k dispozícii API alebo knižnicu a, či majú výstupy v JSON formáte. Nástroje a služby, ktoré sme použili pre analýzu e-mailovej adresy sú:

- Leak-Lookup - overuje či pri účtoch spojených s danou e-mailovou adresou nedošlo k úniku dát z rôznych databáz.
- Emailrep.io - je to podobná služba ako služba overovania existencie e-mailovej adresy, ale s pridanými funkciami, ako sú napríklad: únik údajov, profily spojené s e-mailovou adresou, reputácia, prvý krát videná e-mail adresa online, počet referencií atď.
- Hunter.io [30] - je nástroj na vyhľadávanie e-mailov, ktorý pomáha obchodníkom nájsť kontaktné informácie súvisiace s akoukoľvek doménou, taktiež sa dá použiť aj na overovanie e-mailov.
- Kickbox [31] - overuje či daná e-mailová adresa nie je jednorazová.

Nástroje a služby, ktoré sme použili pre analýzu používateľského mena:

- Social-scanner - je webová aplikácia, ktorá nájde pre zadané používateľské meno profil na viac ako 996 webových stránkach sociálnych sietí.
- Social-scan - je nástroj, ktorý ponúka overenie používania používateľského mena na online platformách.
- Social-analyzer - je nástroj na analýzu a vyhľadávanie profilu používateľského mena na viac ako 1000 webových stránkach sociálnych sietí.

Nástroje a služby, ktoré sme použili pre analýzu reálneho mena:

- Webmii.com - je vyhľadávač, ktorý využíva google dorking na nájdenie informácií o osobe.
- Ufind.name - je vyhľadávač, ktorý kladie dôraz na nájdenie sociálnych sietí spojených s reálnym menom.
- Google dorks - je špecifické vyhľadávanie, kde sa používajú pokročilé operátory a filtre na vyhľadávanie informácií, ktoré nie sú dostupné prostredníctvom bežného vyhľadávania.

3.1.1 API kľúče využívaných nástrojov a služieb

API kľúče sú súčasťou nášho riešenia implementácie nástroje, pretože sú nevyhnutné pre autentifikáciu a autorizáciu pri prístupe k externým službám a zdrojom dát. Zabezpečujú, že len autorizovaní používatelia a aplikácie môžu pristupovať k zdrojom a vykonávať operácie na API. Na získanie API kľúčov pre nástroje a služby, s ktorými pracujeme, je potrebné sa zaregistrovať na príslušných webových stránkach poskytovateľov týchto služieb.

Po úspešnej registrácii na tieto webové služby je API kľúč k dispozícii okamžite. Stačí kliknúť niekde, kde sa webová stránka odkazuje na API kľúče. Avšak, v niektorých prípadoch je nutné osobitne požiadať o API kľúč a očakávať jeho pridelenie, ktoré sa často uskutočňuje prostredníctvom e-mailu. Medzi služby, ktoré poskytujú API kľúč ihneď po registrácii, patria: Leak-Lookup, Hunter.io, Kickbox a Social-scanner. Služba, na ktorú si treba počkať na odpoveď, je v našom prípade Emailrep.io. Kľúče potom stačí jednoducho pridať do kódu, aby sme sa pri dopytoch na webové služby autorizovali.

3.2 Inštalácia doplnkových nástrojov

Doplnkové nástroje sú kritickou súčasťou procesu implementácie nášho nástroja. Po vybraní hlavných technológií, ako sú Python, Flask a JSON, je nevyhnutné zabezpečiť, aby boli k dispozícii aj ďalšie doplnkové nástroje a knižnice potrebné na správne fungovanie nástroja.

Jedným z hlavných krokov pri inštalácii doplnkových nástrojov je importovanie potrebných knižníc a modulov do nášho vývojového prostredia. To zahŕňa import modulov pre prácu s JSON formátom, ktoré nám umožňujú efektívne spracovanie dát vo formáte JSON ako aj import knižnice Flask, ktorá slúži na vytvorenie webového servera a jednoduchého vytvorenia webového rozhrania pre náš nástroj.

Navyše, počas inštalácie doplnkových nástrojov by sme mali zabezpečiť, aby boli k dispozícii aj potrebné aplikácie a knižnice na analýzu používateľského mena. Medzi tieto nástroje patria Social-Scan a Social-Analyzer, ktoré nám poskytujú špecifické funkcie na analýzu a sledovanie sociálnych médií používateľa. Ak na vstupe bude zadané používateľské meno, potom chceme na jeho základe vygenerovať potencionálne e-mailové adresy a skontrolovať ich existenciu.

Importovanie všetkých týchto technológií je pomerne jednoduché, najmä ak nám integrované vývojové prostredie (IDE) ponúka možnosť automatickej inštalácie. Teda najvýhodnejšie a časovo najefektívnejšie je zvoliť hneď na začiatku správne vývojové prostredie pre náš nástroj, teda aplikáciu. Možnosť nainštalovať tieto aplikácie a technológie nájdeme zvyčajne jednoducho na oficiálnych webových stránkach daných nástrojov alebo na ich repozitároch na platforme GitHub.

3.3 Spracovanie a uloženie dát

Na odoslanie požiadavky je potrebné mať k dispozícii URL webovej stránky, ktorú cieľový server identifikuje. Ďalej je nevyhnutné definovať parametre, ktoré budú súčasťou tejto požiadavky. Tieto parametre môžu zahŕňať informácie ako meno a priezvisko, e-mailovú adresu alebo používateľské meno, v závislosti od požiadaviek našeho nástroja. Po zadaní vstupných údajov do nášho nástroja a ich odoslaní na servery čakáme na odpoveď. Táto odpoveď môže byť vo forme JSON dát alebo môže obsahovať informácie o stave požiadavky, ako napríklad upozornenie na prekročenie limitu použitia API, alebo oznam o nesprávnom formáte odoslanej požiadavky.

Po získaní dát, ktoré nám boli odoslané zo servera, je prvým krokom procesu spra-

```
{
    "error": "false",
    "message": {
        "hathway.net": [],
        "collection-4-eu": [],
        "nestle.com": [],
        "dropbox.com": [],
        "warcraftloot.net": [],
        "botsoflegends.com": [],
        "btc-e.com": [],
        "gfuel.com": [],
        "github.com": []
    },
    "source osint tool": "leak_lookup"
},
```


Obr. 3.6: Výstup nástroja pre e-mailovú adresu č.1

covania údajov získaných cez API služby a nástroje, s ktorými pracujeme. Tento proces zahŕňa parsovanie dát vo formáte JSON. V prípade, že server odpovedá vo formáte JSON, stačí tieto dáta uložiť. Pre každú aplikáciu pridávame identifikátor zdroja a názov aplikácie, ktorá nám tieto dáta poslala, aby sme mohli jednoducho identifikovať ich pôvod pri ukladaní do formátu JSON súboru. Tento postup zabezpečuje, že dáta zostanú usporiadané pri ďalšom používaní nástroja.

Dáta, s ktorými pracujeme, sú zoskupené podľa parametrov, s ktorými pracujeme. To znamená, že všetky odpovede z nástrojov obsahujúcich e-mailové adresy budú uložené do spoločného poľa JSON dát. Tento prístup sa aplikuje analogicky aj na ostatné parametre. Na obrázkoch 3.6, 3.7 a 3.8 môžeme vidieť príklad JSON dát pre analýzu e-mailovej adresy.

```
{
    "email": "test@gmail.com",
    "reputation": "none",
    "suspicious": true,
    "references": 457,
    "details": {
        "blacklisted": true,
        "malicious_activity": true,
        "malicious_activity_recent": false,
        "credentials_leaked": true,
        "credentials_leaked_recent": false,
        "data_breach": true,
        "first_seen": "07/01/2008",
        "last_seen": "05/02/2024",
        "domain_exists": true,
        "domain_reputation": "n/a",
        "new_domain": false,
        "days_since_domain_creation": 10505,
        "suspicious_tld": false,
        "spam": false,
        "free_provider": true,
        "disposable": false,
        "deliverable": false,
        "accept_all": false,
        "valid_mx": true,
        "primary_mx": "gmail-smtp-in.l.google.com",
        "spoofable": true,
        "spf_strict": false,
        "dmarc_enforced": false,
        "profiles": [
            "twitter"
        ]
    },
```


Obr. 3.7: Výstup nástroja pre e-mailovú adresu č.2

```
{
    "data": {
        "status": "invalid",
        "result": "undeliverable",
        "_deprecation_notice": "Using result is deprecated, use status instead",
        "score": 0,
        "email": "test@gmail.com",
        "regexp": true,
        "gibberish": false,
        "disposable": false,
        "webmail": true,
        "mx_records": true,
        "smtp_server": true,
        "smtp_check": false,
        "accept_all": false,
        "block": false,
        "sources": []
    },
    "meta": {
        "params": {
            "email": "test@gmail.com"
        }
    },
```


Obr. 3.8: Výstup nástroja pre e-mailovú adresu č.3

3.4 Zobrazenie dát

Posledná časť, ktorou sme sa zaoberali je zobrazenie dát. Hoci je možné čítať dáta priamo zo súboru vo formáte JSON, ich rozsiahly obsah môže spôsobovať problémy pri čítaní pre bežného používateľa. Preto je vhodné vytvoriť užívateľské rozhranie, ktoré tento proces zjednoduší a sprístupní nám údaje vo viac priehľadnejšej forme.

Na tento účel sme sa rozhodli využiť webový framework Flask, ktorý nám umožňuje vytvoriť jednoduchý a efektívny front-end. Prvým krokom je vytvorenie Python skriptu, ktorý spúšťa webovú aplikáciu na lokálnom serveri (localhost). Tento Python skript je zodpovedný za inicializáciu aplikácie a spracovanie požiadaviek od používateľa.

Následne sme vytvorili hlavný HTML súbor, index.html, ktorý slúži ako úvodná stránka našej aplikácie. Táto stránka obsahuje niekoľko polí pre zadanie vstupných údajov, ako sú e-mailová adresa, používateľské meno a reálne meno. Okrem toho sú na stránke umiestnené tlačidlá, ktoré spustia príslušné skripty na vyhľadávanie informácií o zadaných údajoch.

Aby sme zabezpečili prehľadné zobrazenie výsledkov, vytvorili sme samostatné HTML súbory pre každý typ vyhľadávaných údajov: e-mailové adresy, používateľské mená a reálne mená. Tieto súbory sú štruktúrované tak, aby výsledky boli jasné a ľahko čitateľné.

Po zadaní vstupných údajov a kliknutí napríklad na tlačidlo 'Search Email' sa spustí skript, ktorý odošle požiadavku na server a spustí vyhľadávanie informácií o e-mailovej adrese. Výsledky tohto vyhľadávania sa následne zobrazia na príslušnej HTML stránke. Podobný postup sa analogicky uplatňuje aj pre používateľské mená a reálne mená.

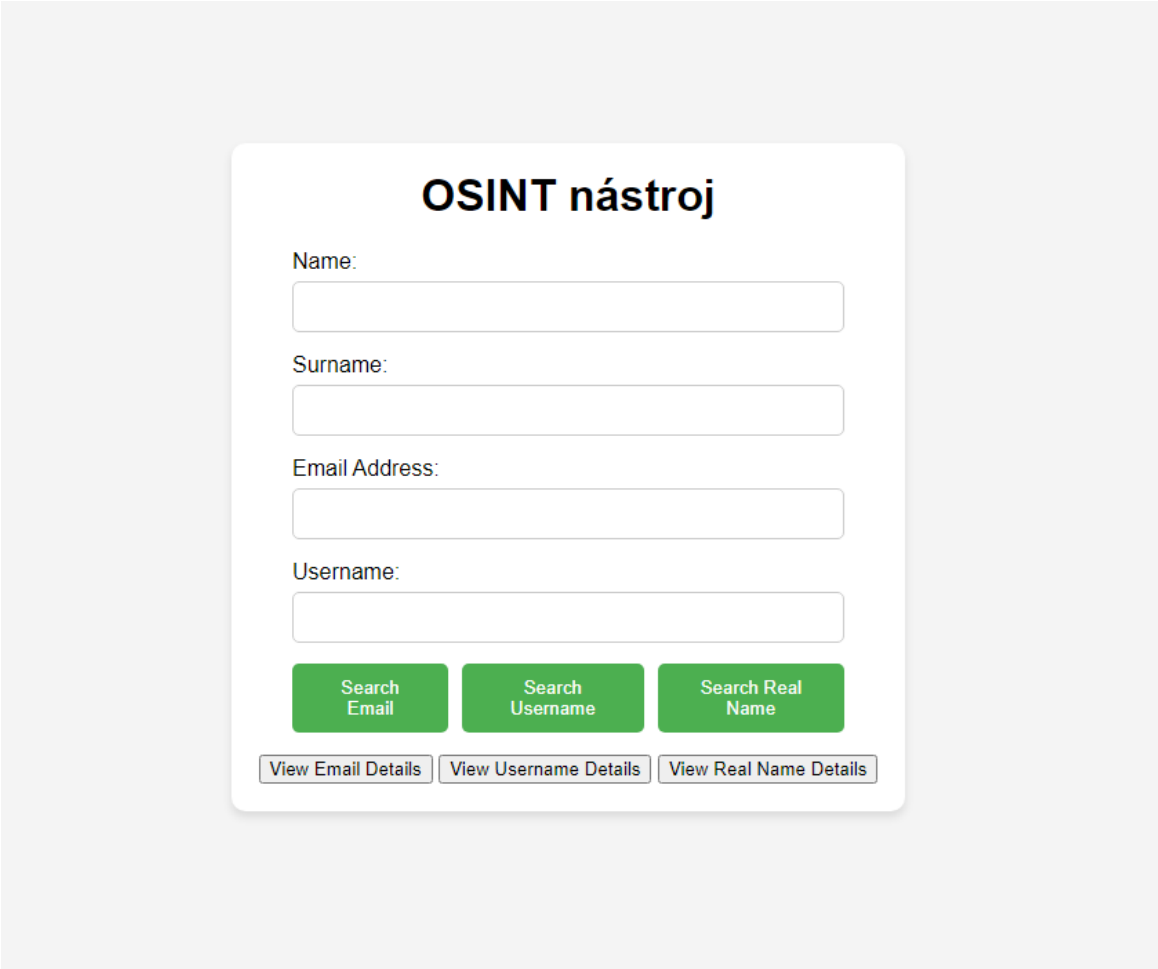
Následne, ak chceme zobraziť podrobné informácie o výsledkoch vyhľadávania, používateľ môže kliknúť na tlačidlo 'View Email Details', ktoré ho presmeruje na stránku s detailnými informáciami o e-mailovej adrese. Tento intuitívny a prehľadný systém nám zabezpečí, že používateľ môže jednoducho navigovať medzi rôznymi sekciami aplikácie a získať potrebné informácie bez zbytočnej námahy.

Nástroj bol navrhnutý s implementáciou kontrolných mechanizmov, ktoré zabezpečujú správne fungovanie a zamedzujú výskytu chýb v procese spracovania a zobrazovania dát. Napríklad, ak používateľ klikne na tlačidlo 'View Email Details' bez toho, aby predtým spustil vyhľadávanie podľa e-mailovej adresy, nástroj nezobrazí žiadne údaje. Namiesto toho sa objaví hláška informujúca používateľa, že nie sú k dispozícii

žiadne dáta.

Rovnako, ak niektoré z povinných polí nie sú správne vyplnené, napríklad ak pole pre e-mailovú adresu nie je vyplnené pri pokuse o vyhľadávanie podľa e-mailu, skript sa nespustí. Týmto spôsobom sa zabezpečí, že všetky požiadavky sú správne špecifikované pred ich odoslaním na server.

Všetky dáta, ktoré sa zobrazujú používateľovi, sú načítané z JSON súborov, avšak pred zobrazením sú tieto dáta filtrované. Tým sa zabezpečuje, že používateľovi sú prezentované iba relevantné a potrebné informácie, čím sa minimalizuje riziko zahltenia zbytočnými dátami. Tento prístup zvyšuje prehľadnosť a efektivitu práce s nástrojom. Na obrázku 3.9 môžeme vidieť hlavné menu nástroja po spustení aplikácie.



Obr. 3.9: Hlavné menu nástroja

3.5 Otestovanie na modelovom prípade

Ukážeme, ako nástroj funguje v praxi a aké výsledky môžeme očakávať pri vyhľadávaní informácií o jednotlivcoch prostredníctvom používateľského mena, reálneho mena a e-mailovej adresy. Na ilustráciu použijeme niekoľko obrázkov výsledkov, ktoré náš nástroj generuje.

Najprv sa zameriame na otestovanie e-mailovej adresy. Po zadaní e-mailovej adresy náš nástroj prehľadá dostupné zdroje a nástroje, ktoré dokážu získať dodatočné informácie spojené s touto adresou, ako sú pripojené služby, sociálne siete a ďalšie relevantné údaje.

Na obrázkoch 3.10 a 3.11 môžeme vidieť odpovede od každej služby a nástroja, ktoré sme použili. Služba Leak-lookup nám poskytla informácie s atribútmi Error: false a Message s prázdnym výsledkom. Atribút Error: false indikuje, že nedošlo k žiadnej chybe a požiadavka bola úspešne spracovaná. Atribút Message poskytuje

výsledok kontroly úniku dát, pričom prázdny výsledok znamená, že naša e-mailová adresa nebola nájdená v žiadnych zaznamenaných únikoch. Služba Emailrep.io nám poskytla podrobné informácie o e-mailovej adrese vrátane nasledujúcich atribútov ako napríklad: 'reputation', ktorá hodnotí reputáciu danej e-mailovej adresy; 'suspicious', indikujúci, či je e-mailová adresa považovaná za podozrivú; 'data breach', ktorý ukazuje, či bola e-mailová adresa súčasťou nejakého úniku dát; 'domain exists', potvrdzujúci existenciu domény; a 'disposable', indikujúci, či je e-mailová adresa jednorazová. Služba Hunter.io nám poskytla komplexné informácie týkajúce sa e-mailovej domény. V prvej časti analýzy, zameranej na e-mailové adresy, nám služba dodala status doručiteľnosti e-mailu, indikátor, či je e-mailová adresa nezmyselná (gibberish), teda vytvorená náhodnými písmenami a číslami, ktoré nedávajú zmysel, či je e-mailová adresa jednorazová (disposable), a či je typu webového mailu. Vzhľadom na to, že e-mailová doména UPJŠ nie je webový mail, služba nebola schopná poskytnúť presné výsledky pre túto doménu, ktorá nie je bežne rozpoznávaná ako Gmail alebo podobné služby.

V druhej časti analýzy sa Hunter.io zameriava na doménu a poskytuje informácie ako skóre (score), názov spoločnosti (company), pozíciu (position) ak je dostupná, status, telefónne číslo (phone number), a odkazy na sociálne siete ako Twitter a LinkedIn.

Email Address Details

leak_lookup

Error: false

Message:

emailrep_io

email: romanrapco@upjs.sk

reputation: low

suspicious: True

credentials_leaked: False

credentials_leaked_recent: False

data_breach: False

first_seen: never

last_seen: never

domain_exists: True

domain_reputation: low

days_since_domain_creation: 2440

disposable: False

primary_mx: upjs-sk.mail.protection.outlook.com

spoofable: True

Obr. 3.10: Výsledky e-mailovej adresy č.1

hunter_io2

status: invalid

result: undeliverable

_deprecation_notice: Using result is deprecated, use status instead

score: 0

email: romanrapco@upjs.sk

gibberish: False

disposable: False

webmail: False

hunter_io

First Name: Roman

Last Name: Rapco

Email: roman.rapco@upjs.sk

Score: 95

Domain: upjs.sk

Accept All: False

Position: None

Twitter: None

LinkedIn URL: None

Phone Number: None

Company: Pavol Jozef Šafárik University in Košice

Date: 2024-03-24

Status: valid

Obr. 3.11: Výsledky e-mailovej adresy č.2

Ďalším príkladom je analýza používateľského mena. Po zadaní konkrétneho používateľského mena do nášho nástroja prehľadávame rôzne online platformy a sociálne siete, aby sme zistili, kde všade sa toto meno používa. Na priloženom obrázku 3.12 môžeme vidieť podrobné informácie o používateľskom mene z rôznych nástrojov a služieb. K dispozícii máme odkazy na rôzne webové stránky, ktoré nám identifikoval nástroj Social-Scanner, ako sú napríklad chess.com, Pinterest alebo Facebook. V druhej časti sú uvedené výsledky z nástroja Social-Scan, ktoré indikujú, či je dané používateľské meno už obsadené alebo je ešte k dispozícii, teda či ho niekto už používa. Tretia časť obsahuje výstupy z nástroja Social-Analyzer, ktoré tiež zahŕňajú odkazy na webové stránky. Posledný odkaz vedie na Google dork, ktorý umožňuje vyhľadávať informácie o zadanom používateľskom mene.

Username Details

Links

- https://chess.com/member/romrap
- https://codex.wordpress.org/wiki/User:romrap
- https://facebook.com/romrap
- https://giphy.com/romrap
- https://pinterest.com/romrap
- https://xvideos.com/profiles/romrap
- https://vk.com/romrap
- https://romrap.weebly.com/
- https://zhihu.com/people/romrap

- GitHub: Not available
- Twitter: That username has been taken. Please choose another.
- Instagram: This username isn't available. Please try another.
- GitLab: Available
- Reddit: Available
- Tumblr: Available

- https://chaturbate.com/romrap/
- https://facebook.com/romrap
- https://vk.com/romrap

Google Dork

https://www.google.com/search?q=%22romrap%22

Obr. 3.12: Výsledky používateľského mena

Obr. 3.13: Výsledky reálneho mena

Posledným príkladom je analýza reálneho mena. Po zadaní reálneho mena do nášho nástroja sa generujú odkazy s rôznymi vyhľadávacími operátormi a s využitím rôznych webových prehliadačov. Na obrázku 3.13 je možné vidieť odkazy na rôzne webové stránky a výsledky vyhľadávania s daným menom, vrátane stránok ako Webmii, UFind.name, Google dorking na rôzne webové stránky, Bing vyhľadávač, Yandex, Yahoo, a podobne.

Záver

Hlavným cieľom tejto bakalárskej práce bolo oboznámiť čitateľa s problematikou OSINT-u. Ďalším cieľom bolo ukázať veľké množstvo nástrojov, ktoré sú k dispozícii, porovnať ich a analyzovať funkčnosť. Posledným cieľom tejto práce bolo navrhnúť nástroj na automatizáciu analýzy osôb pomocou otvorených zdrojov a nakoniec ho implementovať a porovnať s existujúcimi nástrojmi.

V prvej časti tejto práce bola popísaná základná teória OSINT-u. Ako delíme fázy OSINT-u. Potom účel OSINT-u a proces analýzy. Ako, prečo a pomocou čoho analyzovať osoby. A nakoniec prvej časti, čo je to Sock Puppet účet, jeho vytvorenie, načo nám slúži a akú rolu zohráva v spoločnosti.

Druhá časť tejto práce sa zameriava dôkladnejšie na analýzu osôb pomocou rôznych otvorených a verejných zdrojov. Táto sekcia poskytuje detailnejší pohľad na podobné práce a nástroje, ktoré sa zameriavajú na analýzu používateľských mien, reálnych mien a e-mailových adries. Okrem toho sa venujeme aj analýze nástrojov dostupných v Slovenskom prostredí. Táto časť bola viac praktického charakteru a zahŕňa porovnanie jednotlivých nástrojov a služieb.

Tretia časť tejto práce sa zameriava na výber nástrojov a služieb, ktoré sú kritické pre úspešnú implementáciu nášho nástroja. Tento segment zahŕňa detailné opisy API, postupov inštalácie doplnkových nástrojov, procesy spracovania a ukladania dát ako aj metódy zobrazenia týchto dát. Súčasťou tejto časti bol aj príklad použitia, konkrétne praktické výsledky testované na vstupných údajoch autora práce.

Celkovo sme sa snažili úspešne splniť stanovené ciele a predstavili sme komplexný pohľad na problematiku OSINT-u a jeho aplikáciu v kybernetickej bezpečnosti. OSINT je nevyhnutný pre zvýšenie úrovne kybernetickej bezpečnosti. Naše porovnanie existujúcich nástrojov a implementácia vlastného nástroja na automatizáciu analýzy osôb pomocou otvorených zdrojov ukazuje rozmanitosť a dôležitosť OSINT nástrojov v súčasnom svete kybernetickej bezpečnosti.

Zoznam použitej literatúry

[1] Ružičková, Michaela, 2023. OSINT: Čo sú otvorené zdroje informácií a ako ich používať (DISINFO BASICS) [online]. [cit. 2024-04-13]. Dostupné na: https://infosecurity.sk/projekty/osint-co-su-otvorene-zdroje-informacii-a-ako-ich-pouzivat-disinfo-basics/.

[2] *OSINT Open-Source Intelligence [online]. [cit. 2024-04-13]*. Dostupné na: https://pdfweb.truni.sk/e-ucebnice/usi/data/3369654e-2e03-4dd0-91b2-4cea893f87eb.html?ownapi=1.

[3] Gill, Ritu, . *Open-Source Intelligence [online]. [cit. 2024-04-13]*. Dostupné na: https://www.sans.org/blog/what-is-open-source-intelligence/.

[4] *OSINT — what is it and what does it have to do with open sources of information? [online]. [cit. 2024-04-13]*. Dostupné na: https://medium.com/transparent-data-eng/osint-what-is-it-and-what-does-it-have-to-do-with-open-sources-of-information-ec35daeea1c0.

[5] *Open-Source Intelligence (OSINT) [online]. [cit. 2024-04-15]*. Dostupné na: https://www.imperva.com/learn/application-security/open-source-intelligence-osint/.

[6] *Čo je API (Application Programming Interface) [online]. [cit. 2024-04-16]*. Dostupné na: https://smartyacademy.sk/co-je-api-application-programming-interface/.

[7] *Google operátory a Google dorks (Návod) [online]. [cit. 2024-04-17]*. Dostupné na: https://www.ifocus.sk/blog/google-operatory-a-google-dorks/.

[8] *Social analyzer [online]. [cit. 2024-04-17]*. Dostupné na: https://rapidapi.com/hailbytes-hailbytes-default/api/social-scanner.

[9] *Social scan [online]. [cit. 2024-04-17]*. Dostupné na: https://github.com/iojw/socialscan.

[10] *Social scanners [online]. [cit. 2024-04-17]*. Dostupné na: https://github.com/qeeqbox/social-analyzer.

[11] *Leak lookup [online]. [cit. 2024-04-17]*. Dostupné na: https://leak-lookup.com/.

[12] *Emailrep.io [online]. [cit. 2024-04-17]*. Dostupné na: https://emailrep.io/.

[13] *Webmii [online]. [cit. 2024-04-17]*. Dostupné na: https://webmii.com/.

[14] *Ufind.name [online]. [cit. 2024-04-17]*. Dostupné na: https://ufind.name/.

[15] *What are Sock Puppets in OSINT | How to Create One [online]. [cit. 2024-04-17]*. Dostupné na: https://www.cybervie.com/blog/what-is-sock-puppets-in-osint-how-to-create-one/.

[16] *Fakenamegenerator [online]. [cit. 2024-04-17]*. Dostupné na: https://www.fakenamegenerator.com/.

[17] *Fake id generator [online]. [cit. 2024-04-18]*. Dostupné na: https://www.businer.com/.

[18] *Thispersondoesnotexist [online]. [cit. 2024-04-20]*. Dostupné na: https://thispersondoesnotexist.com/.

[19] Nobili, Martina, 2023. Review OSINT tool for social engineering. In: *Frontiers in Big Data*. Vol. 6.

[20] Manohari, D, ES Adithya a K Vijayakumar, 2023. Information Retrieval using OSINT and GHDB. In: *2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*. IEEE, . S. 1–7.

[21] Yadav, Ashok, Atul Kumar a Vrijendra Singh, 2023. Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security. In: *Artificial Intelligence Review*. Vol. 56, no. 11, s. 12407–12438.

[22] Sambhe, Nilesh et al, 2021. Using OSINT to gather information about a user from multiple social networks. In: *INFORMATION TECHNOLOGY IN INDUSTRY*. Vol. 9, no. 2, s. 207–211.

[23] Pastor-Galindo, Javier et al, 2020. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. In: *IEEE Access*. Vol. 8, s. 10282–10304.

[24] *Knowem [online]. [cit. 2024-04-20]*. Dostupné na: https://knowem.com/.

[25] *Whatsmyname [online]. [cit. 2024-04-20]*. Dostupné na: https://whatsmyname.app/.

[26] *HaveIBeenPwned [online]. [cit. 2024-05-10]*. Dostupné na: https://haveibeenpwned.com/.

[27] *Dehashed [online]. [cit. 2024-05-10]*. Dostupné na: https://dehashed.com/.

[28] *Thatsthem [online]. [cit. 2024-05-10]*. Dostupné na: https://thatsthem.com/.

[29] *Spokeo [online]. [cit. 2024-05-10]*. Dostupné na: https://www.spokeo.com/.

[30] *Hunter.io [online]. [cit. 2024-05-10]*. Dostupné na: https://hunter.io/.

[31] *Kickbox [online]. [cit. 2024-05-10]*. Dostupné na: https://kickbox.com/.