EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

SPRÁVA A DOHLED NAD POČÍTAČOVOU SÍTÍ

OSINT

Metodický list

Autor: doc. Ing. Jaroslav Dočkal, CSc., Metodik: Bc. Jaroslav Tihlařík

Recenzent: Ing. Vladimír Šulc, Ph.D.

Rok vydání: 2023

Obsah

Cíle

- Orientovat se v rozsáhlé škále produktů OSINT
- Získat praktické zkušenosti s použitím nejznámějších OSINT produktů
- Seznámit se s omezeními při práci s komerčními produkty OSINT

Dovednosti

- Použití OSINT nástrojů pro zjištění veřejných informací o sledovaném objektu
- Umět zjistit parametry obrázků

Pracovní prostředí

Úlohu lze realizovat v prostředí:

- Cylab JCEKB
- Offline Security Classroom

Pro práci budeme potřebovat následující nástroje:

- Kali s nástroji theHarvester, Maltego a Recon-ng
- Infooozi bude na Kali třeba doinstalovat
- Python – knihovny Pillow a EXIF
- Libovolný prohlížeč

Průběh výuky

1 Teoretická část

1.1 Úvod

Naše digitální společnost neustále roste, a jak to dělá, vytváří spoustu dat, která jsou základem mnoha druhů zpravodajské činnosti. Potíž je v tom, že čím více dat je, tím více času zabere jejich prohledání. To je místo, kde přichází OSINT a stává se neocenitelným přínosem pro každou organizaci.

Open-Source Intelligence (OSINT) je typ zpravodajství o hrozbách, ve kterém může společnost shromažďovat informace o svých bezpečnostních obavách z celé řady zdrojů. Tyto zdroje mohou zahrnovat webové stránky sociálních médií, stránky elektronického obchodu a dokonce i terénní průzkumy provedené odborníky na bezpečnost.

Prvním krokem penetračního testu nebo aktivity červeného týmu je shromáždit co nejvíce informací o cíli. Obecně platí, že shromažďování informací začíná získáváním informací ze zdrojů, které může kdokoli vidět. Tomu se říká open-source inteligence nebo OSINT. Rozšířenost aktivity na sociálních sítích učinila OSINT dostupnější. Útočník tedy může snadno shromáždit požadovaná data pro vyhodnocení profilu.

V dalším textu bude definován pojem OSINT[1] a podíváme se, jak mohou různí aktéři používat OSINT k podpoře zpravodajských potřeb v různých situacích.

1.2 Definice OSINT

Open source inteligence je multimetodická metodologie pro shromažďování, analýzu a rozhodování o datech zpřístupněných ve veřejně dostupných zdrojích pro použití ve zpravodajském kontextu. Termín „open“, vyjadřuje skutečnost, že informace může legálně získat kdokoliv ze zdrojů, které jsou bezplatné nebo veřejné. Tyto informace jsou získávány bez porušení právních norem týkajících se duševního vlastnictví[2].

OSINT využívá různé zdroje a neomezuje se pouze na online data. Například fyzické publikace, jako jsou knihy, nebo jakákoli forma média, jako je televizní nebo rozhlasové vysílání, jsou všechny považovány za zdroje OSINT. V důsledku digitalizace nyní mnoho informací OSINT pochází z online zdrojů. Prostředky OSINT však nejsou omezeny na online data. Zdroje OSINT zahrnují například fyzické publikace, knihy a jakýkoli druh média, jako je televizní nebo rozhlasové vysílání.

[1] Vychází se zde primárně ze zdroje https://redfoxsecurity.medium.com/introduction-to-osint-2c92597988d1

[2] Duševním vlastnictvím se rozumí všechna výhradní práva přiznaná k duševním výtvorům. Dělí se na dvě kategorie: průmyslové vlastnictví, které zahrnuje vynálezy (patenty), ochranné známky, průmyslové vzory a modely a zeměpisná označení; a autorské právo, které zahrnuje umělecká a literární díla. Od roku 2009, kdy vstoupila v platnost Smlouva o fungování Evropské unie (SFEU), má EU výslovnou pravomoc přijímat předpisy i v oblasti práv duševního vlastnictví (článek 118) (materiály EU 2022)

OSINT obecně pomáhá organizaci mít přehled o veřejných informacích. Pomáhá také snižovat potenciální útočnou plochu, a tak zabraňuje únikům informací. Například následující úlohy se dle dle (Redfox Security 2022) provádějí pomocí OSINT:

- *Objevování a lokalizace aktiv mimo bezpečnostní perimetr*: OSINT pomáhá IT a týmům pro kybernetickou bezpečnost objevit a lokalizovat veřejně přístupná aktiva. Prostřednictvím OSINT lze informace dostupné v každém aktivu zmapovat a posoudit z hlediska citlivých nebo kritických informací, které lze zneužít. Obecně nástroje OSINT pomáhají při mapování a evidenci dat veřejného majetku společnosti, která jsou veřejně dostupná a přístupná.
- *Vyhledání relevantních dat a informací mimo organizaci:* Nástroje OSINT pomáhají najít relevantní data mimo organizaci, jako jsou domény nebo porty mimo perimetr sítě organizace. Tato funkce je užitečná zejména pro organizaci, která nedávno sloučila nebo získala jinou organizaci, protože pomáhá najít relevantní informace dostupné mimo právě získanou organizaci.
- *Přijímání nezbytných opatření se shromážděnými údaji*: Shromážděná data mohou být masivní a neuspořádaná. Nástroje OSINT převádějí data na smysluplné informace, které lze použít jako užitečné informace. Nástroje OSINT také pomáhají dávat data dohromady a přednostně řešit citlivá data a jejich problémy.

1.3 Výhody OSINT pro fyzickou bezpečnost

Většina podniků zaujímá k bezpečnosti přístup „stráž u brány“. Jinými slovy, čekají, až se něco pokazí, přiměřeně reagují. Ale takový reaktivní přístup selhává. Za prvé, organizace, které s předstihem nevyhodnocují svá zranitelná místa, mají vyšší pravděpodobnost, že budou v budoucnu zasaženy bezpečnostním incidentem. Navíc může být nákladnější reagovat na incident poté, co k němu dojde, než mu zabránit úplně.

Zaujetí proaktivnějšího postoje s využitím informací shromážděných z otevřených zdrojů má pro týmy zajišťující fyzickou bezpečnost dle (LifeRaft 2022) několik výhod, jako jsou například:

- *Lepší alokace zdrojů*. Bezpečnostní lídři mohou používat OSINT ke kvantifikaci rizik v peněžním vyjádření. To představuje cenné informace při přidělování omezených zdrojů nebo zdůvodňování investic do bezpečnostních programů vedoucím pracovníkům a členům představenstva.
- *Zmírnění rizik*. Bezpečnostní manažéři mohou OSINT použít k posouzení zranitelnosti své organizace a vypracování strategií zmírňování. Předběžná varování ze zpravodajství s otevřeným zdrojovým kódem mohou bezpečnostním týmům často umožnit zabránit incidentům dříve, než k nim vůbec dojde.
- *Kratší doba odezvy*. OSINT může upozornit bezpečnostní týmy na incidenty téměř okamžitě, jakmile k nim dojde. Nejen, že to znamená ušetřit drahocenné minuty nebo hodiny, které se počítají nejvíce. Zpravodajství získaná z otevřených zdrojů může také vést k lepším rozhodnutím v kritických dobách, kdy jde do tuhého.
- *Nižší náklady*. Výhody OSINT nakonec plynou až do konečného výsledku. Zmírnění a rychlejší reakce na incidenty znamenají méně prostojů, méně pokut od regulačních orgánů a menší ztráty v podobě krádeží nebo podvodů.

- *Levnější kapitál*. Pokud dokážete řídit rizika lépe než vaši kolegové, vaše firma bude mít předvídatelnější příjmy. Postupem času akcionáři a věřitelé odměňují tuto předvídatelnost nižší rizikovou prémií kapitálu. V závislosti na velikosti podniku a jeho nákladech na financování se tato zvýšená předvídatelnost může pro společnost promítnout do přidané tržní hodnoty. A tyto výhody jdou daleko za bezpečnost lidí a majetku.
- *Použití OSINT může být přínosem pro řadu oddělení v organizaci, od marketingu a lidských zdrojů až po logistiku a nákup*. A umožněním operací, kam se jiní bojí vkročit, mohou organizace používající tyto nástroje a techniky získat konkurenční výhodu nad konkurenty, kteří nemají žádné možnosti OSINT.

Open source inteligence samozřejmě nepředstavuje nějaké zázračné řešení pro bezpečnostní programy. Podle definice může OSINT odhalovat pouze hrozby, které se objevují ve veřejné doméně. Analytici tedy budou mít potíže s odhalováním škodlivých jedinců, kteří skrývají své aktivity. A open source inteligence nikdy nebude schopna nahradit všechny aspekty dobře strukturovaného bezpečnostního programu.

1.4 Možnosti použití OSINT pro zvýšení úrovně podnikové bezpečnosti

Než se nechat nachytat při špatné reakci na neočekávaný incident, je mnohem levnější shromažďovat informace předem a s včas řešit problémy. Jaké benefity může OSINT pro zvýšení úrovně kybernetické bezpečnosti přinést dle (LifeRaft 2022):

- *Výkonná ochrana*. OSINT se stal nezbytným nástrojem pro ochranu VIP pracovníků. Například na cestách mohou skenovat otevřené zdroje a provádět regionální hodnocení rizik, identifikovat možná rizika a nastavovat alternativní cestovní plány. Kromě toho se vysoce postavení jednotlivci často ocitají vystaveni násilným hrozbám online. Nástroje OSINT umožňují podrobně detekovat ohrožující příspěvky, ověřit hrozbu a naplánovat vhodnou reakci.
- *Krizová reakce*. Lidé často hlásí události na sociálních sítích několik hodin nebo dokonce dní před tím, než události zachytí zpravodajské kanály. Neustálým sledováním těchto kanálů mohou být bezpečnostní týmy upozorněny na krizi téměř okamžitě, jakmile nastane. Kromě toho mohou komentáře shromážděné prostřednictvím otevřených zdrojů, jako jsou fotografie, zvuk a komentáře, umožnit analytikům reagovat efektivněji.
- *Ochrana IP adres*. Pokročilý software OSINT dokáže odhalit zločinecké sítě na webu, které se zabývají paděláním, pirátstvím obsahu a nelegálním streamováním. Bezpečnostní týmy také používají techniky open source inteligence k identifikaci škodlivých zasvěcenců prodávajících důvěrně držená tajemství společnosti online, jako jsou patenty, výzkumné plány nebo plány produktů.
- *Ochrana značky*. Nepovolené aktivity pod logem dané organizace mohou poškodit pověst firmy (tj. předstírání identity vedoucích pracovníků, překlepy na webových stránkách nebo podvody se zaměstnáním). To by mohlo zahrnovat i trestnou činnost na majetku společnosti, jako je obchod s lidmi. Open source inteligence však organizacím umožňuje identifikovat a řešit tyto problémy.

- *Detekce úniku dat*. Náhodné úniky dat zaměstnanci a dalšími zúčastněnými stranami představují pro organizace podceňovanou hrozbu. Zaměstnanec může například zveřejnit obrázek svého pracovního odznaku na sociálních sítích. Osoby se zlými úmysly mohou tyto informace zneužít k vytvoření falešných přihlašovacích údajů a získat neoprávněný přístup k zařízením společnosti. Ale sledováním otevřených kanálů mohou analytici tato porušení odhalit a řešit dříve, než nastanou nějaké problémy.
- *Ochrana dodavatelského řetězce*. Zmatek v dodavatelském řetězci může mít za následek zmeškání termínů pro dodávky produktů. Předcházení takovým problémům vyžaduje mít po ruce všechny dostupné informace týkající se vznikajících a současných hrozeb. Jistě, v tomto procesu hrají roli nové technologie, jako jsou senzory IoT a blockchain. OSINT však poskytuje těm, kdo rozhodují, kontext, který potřebují k efektivní adaptaci v krizi.
- *Zabezpečení událostí*. Událost by mohlo narušit mnoho problémů: narušitelé, hluční fanoušci, špatné počasí. Naštěstí informace o hrozbách z online chatování umožňují včas odhalit potenciální problémy. S těmito informacemi mohou bezpečnostní týmy pracovat na zmírnění rizik, rychleji reagovat na incidenty a efektivněji nasazovat zdroje.
- *Kybernetická bezpečnost*. Inteligence umožňuje technickým týmům identifikovat a opravit zranitelná místa v síťových systémech. Díky tomu mohou organizace rychleji reagovat na porušení, ke kterým již došlo. Nebo ještě lépe, mohou být schopni zastavit kybernetické útoky dříve, než k nim vůbec dojde.
- *Analýza rizik*. OSINT dokáže zachytit „klábosení“ na místě a poskytnout vhled do myšlení a názorů místních obyvatel v regionu. To by mohlo představovat neocenitelnou informaci pro osoby s rozhodovací pravomocí při zvažování nového projektu nebo expanzi na jiné území.
- *Prevence podvodů a ztrát*. Týmy pro boj proti podvodům a ztrátám potřebují aktuální podrobnosti o nejnovějších technikách krádeží. Překvapivě se zločinci často chlubí svými činy online. Tyto informace umožňují organizacím lépe chránit své operace před krádežemi a podvody.
- *Due diligence*[3]: Obchodování s osobami, které perou špinavé peníze, daňovými podvodníky nebo jinými zločinci, může poškodit pověst dané organizace. A vzhledem k rostoucím pokutám ze strany regulátorů investovali rozhodující činitelé více úsilí do due diligence. Při vstupu na nové trhy nebo přivedení nového zákazníka mohou zpravodajské týmy pomoci vedoucím pracovníkům vyhnout se obchodování s pochybnými partnery a posoudit potenciální střety zájmů.

Některá rizika, která jsou spojena s nástroji OSINT, jsou:

- *Prozrazení vyšetřovatele*: Toto je nejběžnější riziko, protože provádění vyšetřování OSINT může prozradit toho, kdo data hledal.
- *Ztráta přístupu k informacím*: Prozrazení vyšetřovatele může vést ke ztrátě přístupu k informacím.

Nestačí své vyhledávání omezit na typické vyhledávače, jako je Bing, Yahoo nebo Google při provádění OSINT. Např. v (OSINT Handbook 2022) je v roce 2020 používaných vyhledávacích nástrojů uvedeno 20. Tyto vyhledávače

[3] Due diligence (anglicky náležitá pečlivost nebo náležitá opatrnost), např. při auditu hospodaření.

prohledávají pouze povrchový web, který tvoří pouze 4 % veškerého dostupného webového obsahu; zbytek je ukryt hluboko ve spodních vrstvách a vyžaduje speciální přístup.

1.5 Typy datových zdrojů OSINT

Škála datových zdrojů je široká:

- sociální média
- Deep Web
- Dark web
- blogy
- digitální tržiště
- mapy
- knihovny
- noviny
- časopisy
- veřejné záznamy
- fóra
- fotky
- adresáře
- knihy
- rádio
- úniky dat
- archiv
- vyhledávače
- Pasters[4]
- chan tabule[5]

1.6 Identifikátory a pivoty

Identifikátory jsou jedinečné vlastnosti, které popisují objekt, vlastnost nebo jednotlivce. Každý jeden identifikátor může existovat ve více souborech dat na libovolném počtu míst na internetu. Ale samy o sobě vám jediný identifikátor mnoho neřekne.

[4] Paste je informace, která byla „vložena“ na veřejnou webovou stránku určenou ke sdílení obsahu, jako je Pastebin. Tato veřejná fóra jsou často využívána hackery pro jejich schopnost anonymně sdílet kritické a citlivé informace, jako jsou soubory s hesly odcizené během hackingu.
[5] Bulletiny, např. 4chan

Identifikátorem mohou být:

- URL stránka
- bitcoinová adresa
- vyhledávací dotaz
- obrázek
- obchodní jméno
- číslo kreditní karty
- časové razítko
- ovládání sociálních médií
- adresa
- jméno
- příjmení
- koníčky
- obsazení
- vztahy
- geo-souřadnice
- operační systém
- telefonní číslo
- poskytovatel hostitele webu
- IP adresa
- heslo
- narozeniny
- titul
- emailová adresa
- číslo SPZ

Zkušení analytici OSINT používají k získání více informací o tématu techniku zvanou „pivoting“. Pivotování znamená hledání stejného identifikátoru v různých souborech dat za účelem odhalení nových identifikátorů. Lze například zahájit vyšetřování pouze anonymním blogovým příspěvkem. Při vyhledávání v registrech domén WhoIS pomůže najít jméno a e-mailovou adresu. Rychlé vyhledávání Google může odhalit fotografie, uzavřít kontakty a účty na sociálních sítích. V tomto případě jsme přešli z adresy URL webu na jméno, e-mailovou adresu a další informace. Při větším pátrání lze vytvořit úplný profil zkoumaného objektu.

1.7 Sock Puppet

1.7.1 Význam pojmu

Sock Puppet (doslovný překlad „ponožková loutka“) je falešná persona nebo alternativní online identita používaná ke shromažďování a vyšetřování informací z otevřeného zdroje o cíli. Sock Puppet je vytvářen s cílem, aby profil nebyl propojen zpět s vyšetřovatelem. To je zásadní pro zajištění provozní bezpečnosti, která ochrání vyšetřovatele před odvetou nebo zabrání tomu, aby si cíl uvědomil, že je vyšetřován konkrétní entitou.

Údržba a správa Sock Puppetu také vyžaduje podrobné pochopení mnoha různých platforem, které vyšetřovatel použije k vytvoření účtů pro falešnou osobu. Jak se tyto zásady mění, mohou se měnit i informace, které jsou zveřejněny nebo sdíleny.

1.7.2 Doporučení

Na (Kellep 2022) lze najít doporučení, jak efektivně vytvořit a používat funkční Sock Puppet:

1. Chcete-li účet anonymizovat, aby nezaznamenával původní IP adresu nebo umístění, důrazně se doporučuje při vytváření účtu použít VPN nebo TOR. Kromě toho se to doporučuje provést z veřejného připojení Wi-Fi.
2. Některé platformy sociálních médií, jako je Facebook, mohou jednotlivcům bránit ve vytvoření účtu z připojení VPN nebo TOR. V takovém případě se doporučuje použít veřejnou Wi-Fi.
3. Při přihlašování k účtu Sock Puppet se ujistěte, že vždy používáte VPN, TOR nebo veřejnou Wi-Fi, za žádných okolností by tvůrce neměl používat přímou IP adresu, která na ně může odkazovat.
4. Je třeba zajistit zdání legitimity účtu produkcí každodenní aktivity, používat jej po dlouhou dobu a vytvářet online spojení.
5. Při vytváření názvu účtu se doporučuje použít generátor falešných jmen, např. z *https://www.fakenamegenerator.com/*. Přitom bude vyšetřovateli poskytnuta identita osoby, která nikdy neexistovala. Identita bude mít jméno, adresu, rodné příjmení matky, váhu, výšku, datum narození a mnoho dalších užitečných informací, které potřebujete k vytvoření osoby. Ženské účty pak mají větší úspěch při tvorbě Sock Puppet.
6. Nyní, když byla vytvořena identita, se důrazně doporučuje poskytnout obrázek. Tvůrce má dvě možnosti, použít kresleného avatara nebo poskytnout obraz člověka, který neexistuje, pomocí umělé inteligence (viz https://thispersondoesnotexist.com/). Nedoporučuje se použít obličej skutečné osoby, protože jednotlivci mohou pomocí nástrojů, jako je Google, identifikovat původního vlastníka fotografie.
7. Při vytváření e-mailového účtu pro Sock Puppet se doporučuje použít jakéhokoli poskytovatele e-mailu, jako je gmail.com, mail.com nebo yahoo.com. Jak již bylo uvedeno, je třeba se ujistit, že IP adresa nemůže být propojena s tvůrcem.
8. Lze získejte vypalovačku mobilního telefonu a SIM karty, které lze použít k ověření účtu. Ujistěte se, že nemáte telefon propojený zpět s vyšetřovatelem platbou v hotovosti nebo kreditní kartou na základě ochrany osobních údajů.
9. Mít více než jeden Sock Puppet je vysoce doporučeno pro případ, že se něco pokazí, vyšetřovatel pak bude mít aktivní zálohu.

Sock Puppety jsou důležité pro ochranu vyšetřovatele, věci se v online světě rychle mění a je důležité, aby vyšetřovatel držel krok se změnami.

1.7.3 Profilové obrázky

1.7.3.1 Zdroje falešných obrázků

Pokud chcete realistický profilový obrázek a nechcete používat celebritu či neznámou osobu, existuje několik webových stránek, které mohou poskytnout použitelný falešný obrázek:

- This Person Does Not Exist (thispersondoesnotexist.com)
- Boredhumans (https://boredhumans.com/faces.php)
- Massless Face Maker (https://unstable.massless.io/tool/face-maker-ai/)
- Generated Photos Face Generator (https://generated.photos/face-generator)

1.7.3.2 Detaily profilu

Nástroj Fake Name Generator Tool (https://www.fakenamegenerator.com/) a Random Name Generator (https://www.random-name-generator.com/) poskytují nejen falešné jméno, ale několik dalších falešných údajů včetně narozenin, e-mailové adresy a adresy bydliště, které lze použít pro své loutky. Web Face Info (*https://fakeinfo.net/)* také může poskytnout falešná uživatelská jména, jména, obrázky falešných profilů na sociálních sítích a textové zprávy.

1.7.3.3 Ověření

Někdy Instagram (*https://help.instagram.com/1053588012132894*) vyžaduje, abyste ověřili svůj účet nahráním selfie videa? Např. Sketchfab (*https://sketchfab.com/tqyw/collections*) umožňuje vygenerovat video jednotlivce (který neexistuje), pohybujícího se ze strany na stranu, který projde ověřovacím testem.

1.7.3.4 Analýza obrázku

Nástroje, které používají AI, se staly velmi užitečnými zejména pro analýzu obrazu během vyšetřování OSINT, zde jsou některé:

1.7.3.4.1 Zpětné (reversní) vyhledávání obrázků

Google, Bing, Yandex, Primeyes a TinEye používají AI ke generování výsledků. OSINTCombine (https://www.osintcombine.com/reverse-image-analyzer) má také reverzní analyzátor vyhledávání obrázků, který kombinuje výsledky Google a Yandex. Search4faces (https://search4faces.com/en/) zase umožňuje vyhledávat tváře a také najít uživatele TikToku.

1.7.3.4.2 Odebírání/přidávání položek do obrázků

Cleanup.pictures (https://cleanup.pictures/) umožňuje odstranit jakýkoli nežádoucí materiál z obrázku, což je skvělé pro účely geolokace nebo pro vylepšení výsledků obrácených obrázků. Další platformou, která to umí, je Deep Angel (https://creativitywith.ai/deepangel/).

1.7.3.4.3 Jasnost/Vylepšení obrázku

Máte rozmazaný obraz a chcete to změnit? Můžete použít některý z nástrojů, které opravují kvalitu resp. rozlišení obrázků: Lets Enhance (https://letsenhance.io/), Myheritage Photo Enhancer (https://www.myheritage.cz/photo-enhancer) či App Remini (https://app.remini.ai/).

1.7.3.5 Identifikace položek

1.7.3.5.1 Ptactvo

Merlin Bird ID (https://merlin.allaboutbirds.org/) pomáhá zjistit druh ptáka prostřednictvím zvuků, které vydává, nebo prostřednictvím obrázku ptáka. Pokud tedy bod zájmu nahrál video/fotografii s ptákem na pozadí, lze si ověřit, kde se bod zájmu nachází, pokud pták pochází z určité oblasti.

1.7.3.5.2 Auta

Carnet (https://carnet.ai/) umožňuje identifikaci vozidla včetně čísla modelu a roku. To lze také použít k identifikaci vozidel například v Google Street View.

1.7.3.5.3 Jídlo

Pomocí Caloriemamy (https://www.caloriemama.ai/) lze identifikovat různé druhy potravin.

1.7.3.5.4 Rostliny

Plantnet (https://apps.apple.com/au/app/plantnet/id600547573) umožňuje identifikovat různé rostliny.

1.8 Nástroje a techniky OSINT

Existuje spousta nástrojů OSINT, placených i neplacených. Nejdůležitější věcí, kterou je třeba pochopit, je, že proces OSINT znamená použití informací, které mají být zpracovány pomocí určité technologie s cílem zjistit více informací o osobě nebo subjektu.

Techniky OSINT lze rámcově rozdělit do dvou hlavních kategorií:

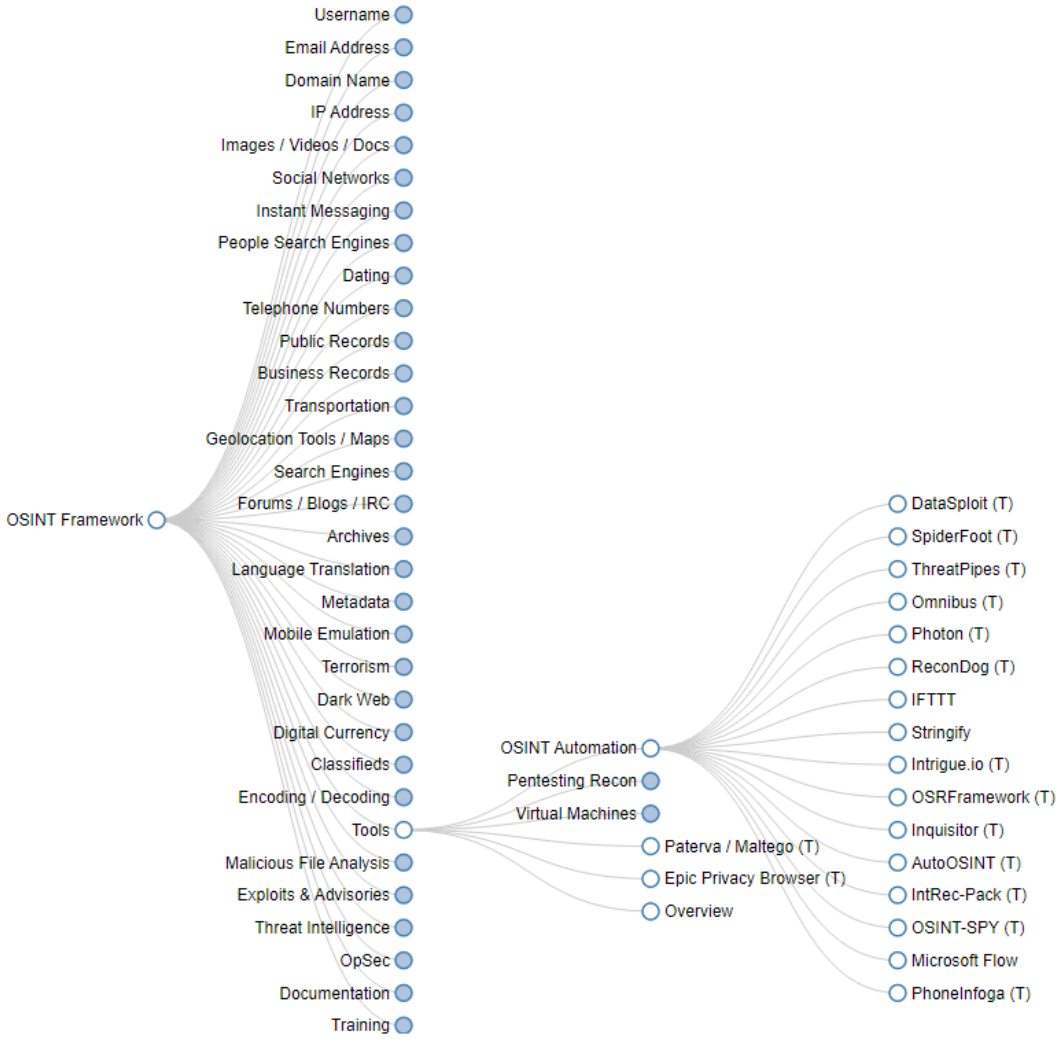
- *Aktivní OSINT*: Zahrnuje skenování portů a systému a přímý kontakt s cílem. Výsledky jsou spolehlivější a spolehlivější, spolu s vysokým rizikem detekce.
- *Pasivní OSINT*: V této kategorii je kontakt navázán pomocí služeb třetích stran. Protože zahrnuje třetí stranu, výsledky vyhledávání nemusí být spolehlivé a mohou obsahovat mnoho falešně pozitivních a negativních výsledků. Proto je riziko odhalení v této kategorii poměrně nízké.

Pokud je při použití aktivní metody cíl odhalen, může zničit důkazy nebo přijmout odvetná opatření proti vám a vaší organizaci. Kromě toho má aktivní výzkum tendenci mít úzký rozsah. Z definice je to náročné na zdroje a těžko se škáluje. Bezpečnostní týmy, které se na tuto metodu příliš spoléhají, by tedy mohly přijít o další hrozby. To znamená, že aktivní sběr musí být vysoce přesný. Většina technik OSINT proto spadá do pasivní kategorie.

Analytici mají třetí možnost, nazývanou *semi-pasivní sběr*, která spadá mezi předchozí dvě. Tento přístup zahrnuje použití aktivních shromažďovacích opatření služby třetí strany k provádění pasivní analýzy.

Na *https://start.me/p/BnrMKd/01-ncso* je kolekce odkazů na *https://start.me/p/DPYPMz/the-ultimate-osint-collection* (autor se podepisuje jako hatless1der) a hub zdrojů na *https://start.me/p/BnrMKd/01-ncso.* Na *https://www.bellingcat.com/category/resources* je řada článků a případových studií, na stránkách *https://osintcurio.us/* poskytuje komunita sdružená kolem projektu *The OSINT Curious Project* řadu tipů a videí.

Možný rámec OSINT lze nalézt na https://osintframework.com/. Podívejme se např. na přehled obecných vyhledávacích strojů na obr. 1.8.1. Z nejznámějších metod budou v dalším textu některé podrobnění popsány a ty, které se dají v kratším čase použít byly zařazeny mezi příklady pro cvičení.



Obr. 1,8.1 Přehled obecných vyhledávacích strojů používaných pro OSINT (https://osintframework.com/)

1.8.1 Google Dorking:

Hlavním účelem je vyhledávání textu na stránkách webového serveru, které jsou přístupné veřejnosti. Google je však mnohem silnější nástroj, než se na první pohled zdá. Vyhledávací operátory jsou prvním nástrojem pro vyhledávání a pokročilejší operátory naleznete na: (GoogleGuide 2022)

Nejpoužívanějšími operátory jsou:

- inurl: Vyhledá adresu URL, která odpovídá jednomu z klíčových slov.
- intitle: Vyhledá všechny nebo jakékoli výskyty klíčových slov v názvu.
- filetype: Hledá určitý typ souboru, který je uveden v dotazu.
- ext: používá se k rozlišení mezi soubory s konkrétními příponami, jako je .log.
- mezipaměť: odhaluje verzi webové stránky, kterou Google uložil do mezipaměti.

Google Dorking, také známý jako „hackování" Google[6], je proces používání složitých vyhledávacích výrazů k získání požadovaných výsledků. Seznam operátorů a aktualizovanou databázi dotazů obsahuje (Google Dorks 2022), Google Hacking Database (GHDB 2022) je kategorizovaný index dotazů internetového vyhledávače určený k odhalování zajímavých a obvykle citlivých informací zveřejněných na internetu. Ve většině případů nebyly tyto informace nikdy určeny ke zveřejnění, ale kvůli mnoha faktorům byly tyto informace propojeny ve webovém dokumentu, který prošel vyhledávač, který následně následoval tento odkaz a indexoval citlivé informace.

Výhodou Googlu je bezplatná cena (samozřejmě), poskytuje přitom omezené výsledky a vyžaduje hodně pokusů a omylů. Metoda je kontroverzní, protože může překročit hranici z hlediska „veřejnosti" informace. Lze např. najít odkaz na soubor PDF obsahující seznam hesel, ale jeho stažení může být trestně stíhatelným trestným činem.

1.8.2 Censys

Vytváří prohledávatelné databáze internetových zařízení a sítí. Tak jako Google umožňuje prohledávat webové stránky, Censys Search umožňuje prohledávat hostitele a certifikáty na internetu. Na datové sady hostitelů a certifikátů se lze dotazovat prostřednictvím webového uživatelského rozhraní nebo rozhraní API.

Censys původně začal jako akademický výzkumný projekt na University of Michigan. Je volně dostupný pro nekomerční použití. Akademickým a jiným nekomerčním výzkumníkům je poskytován bezplatný přístup ke stejným datům jako zákazníkům na nejvyšší úrovni. Používá Google BigQuery a skenuje 107 protokolů a 3500+ portů. S bezplatným účtem je kvóta 250 dotazů měsíčně.

Přehled základních pravidel je na https://support.censys.io/hc/en-us/articles/360059608451-Censys-Search-Language. Na https://support.censys.io/hc/en-us/articles/6228280987540-Regular-Expressions-in-Censys-Search-2-0 je použití regulárních výrazů. Censys původně podporoval vyhledávání regulárních výrazů proti skenovaným datům. Vzhledem k tomu, že tato funkce byla používána zřídka a měla problémy s kompatibilitou s indexy Elasticsearch, byla tato funkce omezena na komerční uživatele (Durumeric 2021).

Censys lze použít nejen k identifikaci aktiv připojených k internetu a internetu věcí/průmyslového internetu věcí (IoT/IIoT), ale také průmyslových řídicích systémů a platforem připojených k internetu.

1.8.3 ´;--have I been pwned?

Jedná se o webovou stránku (https://haveibeenpwned.com), na které si uživatelé internetu mohou ověřit, zda jejich osobní údaje nebyly odhaleny v důsledku úniku dat. Uživatelé mohou vyhledávat své vlastní informace zadáním svého

[6] Proces známý jako „Google Hacking" zpopularizoval v roce 2000 Johnny Long, profesionální hacker, který začal katalogizovat tyto dotazy v databázi známé jako Google Hacking Database.

uživatelského jména nebo e-mailové adresy a stránka shromažďuje a analyzuje stovky databázových výpisů a vkládání, které obsahují informace z miliard napadených účtů. Uživatelé mají možnost přihlásit se k odběru e-mailových upozornění, pokud se jejich e-mailová adresa objeví v nadcházejících výpisech. Použití Have i been pwned? je bezplatné, použití API je za měsíční poplatwk 3,5 USD. Omezen je však na telefonické a e-mailové kontroly.

Přehled historicky největších úniků dat lze nalézt v (Tunggal 2022). Největší únik dat historie zaznamenala aplikace Dubmash[7] v roce 2018, kdy uniklo 162 milionů jedinečných e-mailových adres, uživatelských jmen a hash hesel DBKDF2. V roce 2019 se tato data objevila pro prodej na dark webu a byla šířena.

1.8.4 PimEyes

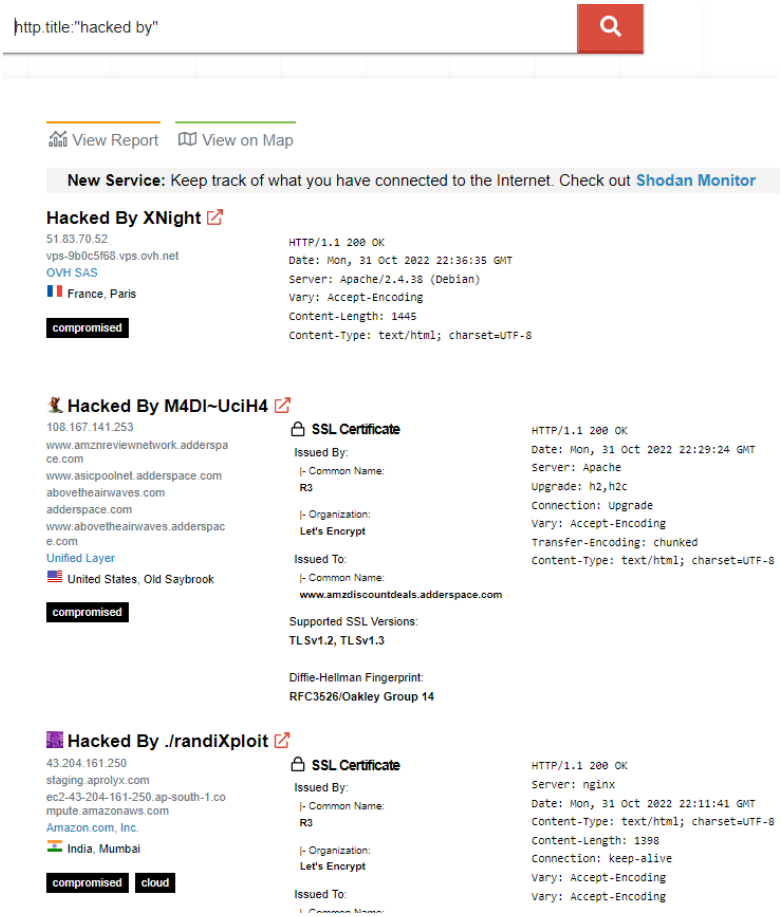
PimEyes je zpětný vyhledávač obrázků pro fotografie využívající nejmodernější techniky, jako je rozpoznávání obličeje a umělá inteligence. Uživatelé mohou snadno zahájit vyhledávání nahráním obrázku tváře dané osoby. Když je obrázek umístěn na web PimEyes, trvá nástroji méně než sekundu, než vyhledá na internetu podobné obrázky předmětu. Je důležité si uvědomit, že PimEyes při vyhledávání nezohledňuje stránky sociálních sítí. Místo toho aplikace hledá fotografie, které může vidět kdokoli na webech, blozích a dalších otevřených platformách.

1.8.5 Shodan

Shodan je oblíbený nástroj OSINT, který lze použít k nalezení vystavených aktiv. S pomocí Shodan lze zjistit geografická místa, kde se nacházejí zranitelná zařízení po celém světě. Pokud jde o zařízení, Shodan má obrovský dosah, protože tento nástroj lze použít k zobrazení živých kamerových kanálů.

Webové vyhledávače, jako je Google, jsou skvělé pro vyhledávání webových stránek. Ale co když vyšetřovatele zajímá měření toho, které země jsou stále propojenější? Nebo pokud chce vědět, která verze Microsoft IIS je nejoblíbenější? Nebo chce najít kontrolní servery pro malware? Možná se objevila nová chyba zabezpečení, může zjistit, kolik hostitelů by mohla ovlivnit? Lze také vyhledávat zařízení s nastavenými defaultními hesly anebo hacknuté servery, viz obr. 1.8.5.1.

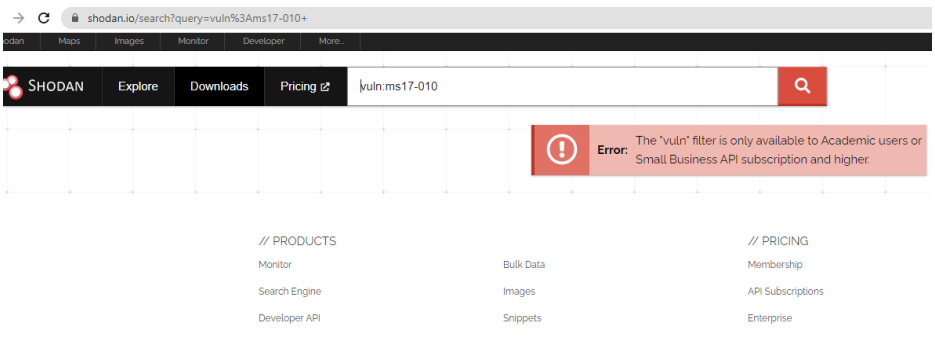
[7] Aplikace, která umožňuje uživatelům chytrých telefonů, aby znovu vytvářeli zkopírované hudební videa.



Obr. 18.5.1 Zjišťování hacknutých serverů

Tradiční webové vyhledávače vám na tyto otázky odpovědět neumožňují. Nejzásadnější rozdíl je v tom, že Shodan prochází celý internet, zatímco Google prochází webové servery. Zařízení s weby však tvoří pouze nepatrný zlomek toho, co je skutečně připojeno k internetu. Cílem Shodanu je poskytnout úplný obraz o internetu.

Co tedy Shodan indexuje? Většina dat pochází z bannerů, což jsou metadata o softwaru, který běží na zařízení. Mohou to být informace o softwaru serveru, jaké možnosti služba podporuje, uvítací zpráva nebo cokoli jiného, co by klient chtěl vědět před interakcí se serverem. Za větší možnosti se platí tím, že použití Shodanu vyžaduje větší znalost syntaxe příkazů. Dalším problémem je, že smysluplné použití vyžaduje buď placenou verzi anebo alespoň akademický účet (což se středních škol netýká) aLE i akademické účty mají svá omezení (viz obr. 1.8.5.2) a tak nebyl Shodan zařazen do praktické části tohoto scénáře.



Obr. 1.8.5.2 I při akademickém účtu lze narazit na řadu omezení. Vzkaz je srozumitelný: “Zaplať”.

1.8.6 Infoooze

Infoooze je výkonný a uživatelsky přívětivý nástroj, který umožňuje rychle a snadno sbírat informace o konkrétním cíli. S Infoooze lze snadno vyhledávat informace o webových stránkách, IP adresách, uživatelských jménech a další, to vše z jednoduchého rozhraní příkazového řádku.

Jednou z klíčových vlastností Infoooze je jeho schopnost pracovat jako globální balíček, který umožňuje používat jej z libovolného adresáře na počítači. Má také schopnost automaticky ukládat výsledky vyhledávání do textového souboru. To znamená, že k informacím, které jsou shromážděny, lze později snadno přistupovat a odkazovat na ně.

Infoooze se snadno instaluje a používá, takže je ideálním nástrojem pro každého, kdo hledá rychlé a efektivní shromažďování informací.

1.8.7 theHarvester

theHarvester je jednoduchý, ale výkonný nástroj navržený pro použití během průzkumné fáze red týmového hodnocení nebo penetračního testu. Shromažďováním informací pomáhá určit prostředí externích hrozeb domény. Nástroj shromažďuje jména, e-maily, adresy IP, subdomény a adresy URL pomocí více veřejných zdrojů, které mj. Zahrnují prohlížecí stroje z produktů: Census, Shodan, Baidus, Bing, Hunter, Qwant, yahoo pro prohledávání domén používá Virustotal atd. (blíže https://github.com/laramies/theHarvester).

1.8.8 Recon-ng

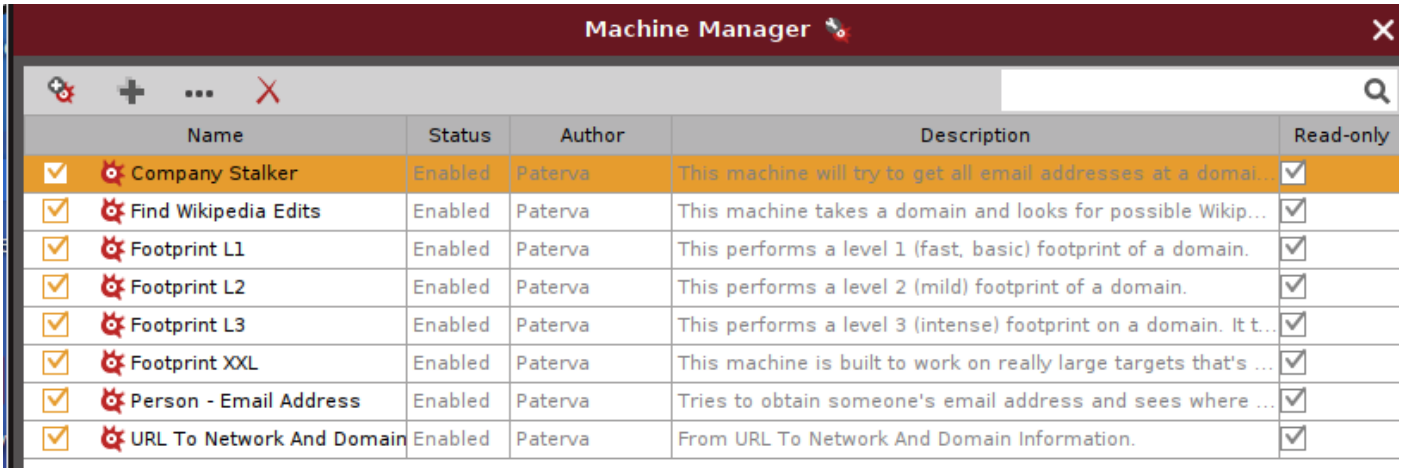
Recon-ng jsou bezplatné rámcové nástroje pro průzkum, které se používají k rychlému provádění průzkumu na webu s otevřeným zdrojovým kódem. Je to podobné jako metasploit framework. Jedná se o kompletní nástroj používaný k nalezení IP adresy cíle, nalezení chybové injekce SQL, vyhledávání Geo-IP, Banner grabování, DNS vyhledávání, skenování portů, subdoménové informace, reverzní IP pomocí WHOIS vyhledávání. Může být použit k nalezení různých bitů a částí informací. Data jsou sbírána automaticky a ukládána do databáze.

1.8.9 Maltego

Žádné hodnocení open source není úplné bez použití Maltega. Je nedílnou součástí OSINT. Důvodem, proč je Maltego velmi populární a široce používané, nejsou jen jeho funkce, ale také jeho reprezentace dat. Maltego má různé sady zobrazení, jako je hlavní zobrazení, bublinové zobrazení a zobrazení entity. A také můžeme změnit typ pohledu. Výsledek vypadá velmi snadno na pochopení, protože pro různé typy entit se používají různé typy ikon a jejich vztahy jsou dobře vyjádřeny šipkami. Práce s ním však není snadná

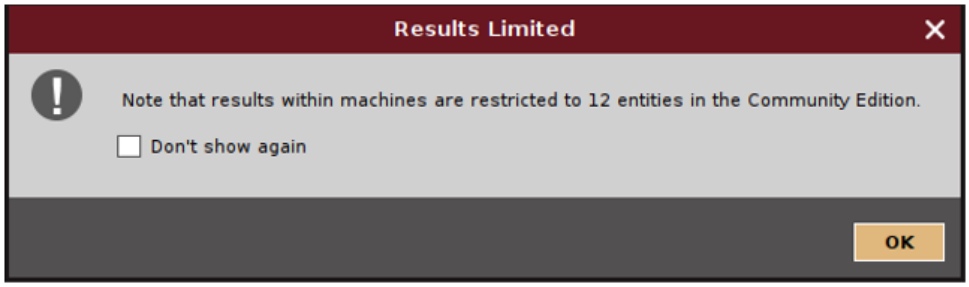
Maltego představuje model vztahu mezi entitami. Kromě extrahování dat pomocí různých transformací a strojů lze data vzít z jiných zdrojů a zahrnout je do grafu pro vytvoření většího obrazu. K tomu je třeba vzít příslušný typ entity z levého pruhu entity a přenést jej do grafu, poté vložit data, která jsme našli, a jednoduše je připojit k příslušné entitě nebo entitám. Pokud nenajdeme vhodnou entitu pro daný datový typ, Maltego umožní vytvořit novou entitu a použít ji podle našich potřeb. Díky tomu je velmi snadné využít výhod funkce dolování dat a dále ji rozšířit pro účely analýzy dat.

Maltego využívá řadu strojů, ale pro komunitu jr jich vyčleněna omezená sada, viz obr. 1.8.9.1.



Obr. 1.8.9.1 Stroje, ke kterým je povolen přístup členům komunity

Přes všechny klady Maltega smysluplná práce vyžaduje delší školení a registraci do komunity. A ani členství v komunitě neuchrání od nepříjemných překvapení – ukázka je na obr. 1.8.9.2.



Obr. 1.8.9.2 Ukázka jednoho z omezení členství v komunitě, pro rozsáhlejší použití je třeba platit.

1.8.10 Exif Viewer

“Exchangeable Image File Format” je to, co EXIF znamená. Metadata EXIF jsou další data, která jsou uložena v souboru obrázku. Důležité informace, jako je expozice, datum a čas, clona atd., jsou uchovávány jako součást souboru obrázku, když je fotografie zachycena digitálním fotoaparátem. Dokonce i GPS souřadnice mohou být uchovány na zařízeních, která mají povoleny lokalizační služby. Pohled na tyto informace vám může pomoci pochopit, jak byl snímek pořízen.

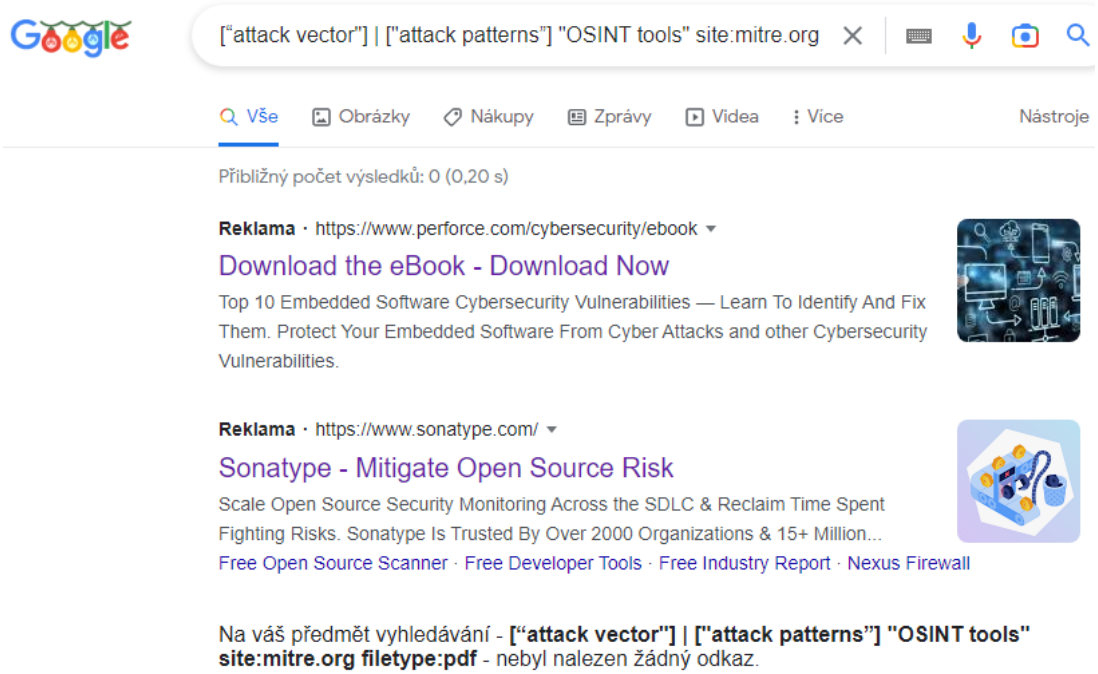
2 Praktická část

2.1 Použití Google Dorku

2.1.1 Zadání

Pomocí Google Dorku najděte nejvýznamnější nástroje o OSINT ve formátu pdf publikovaných v doméně mitre.org.

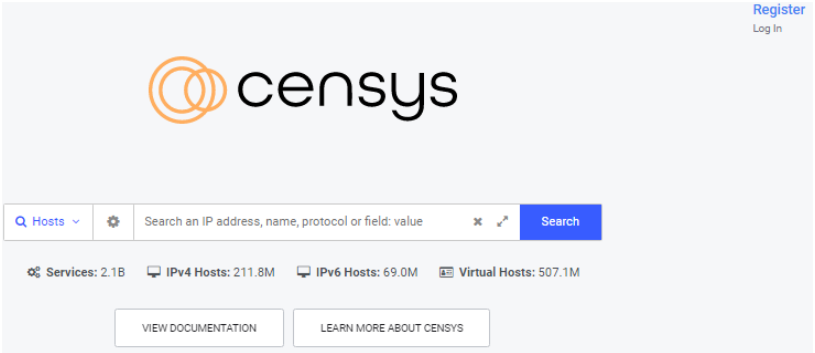
2.1.2 Řešení



2.2 Použití Censysu

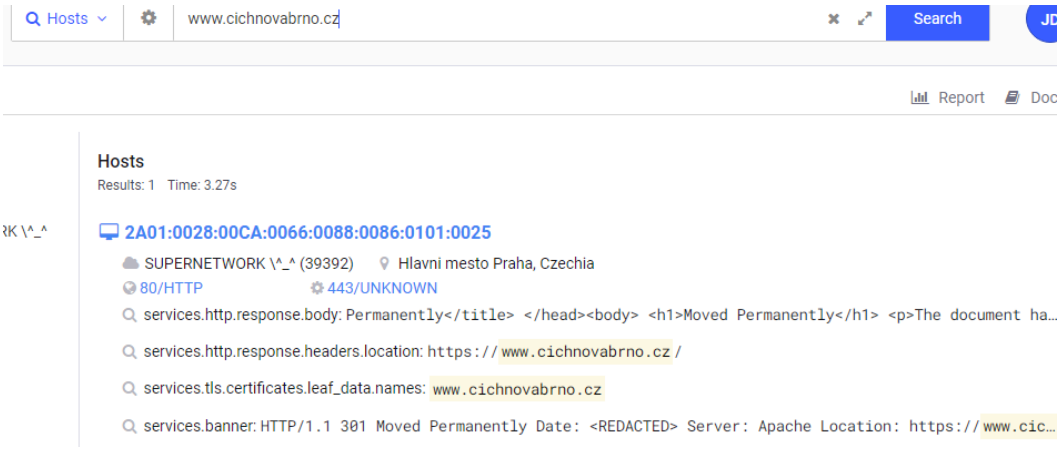
2.2.1 Zadání

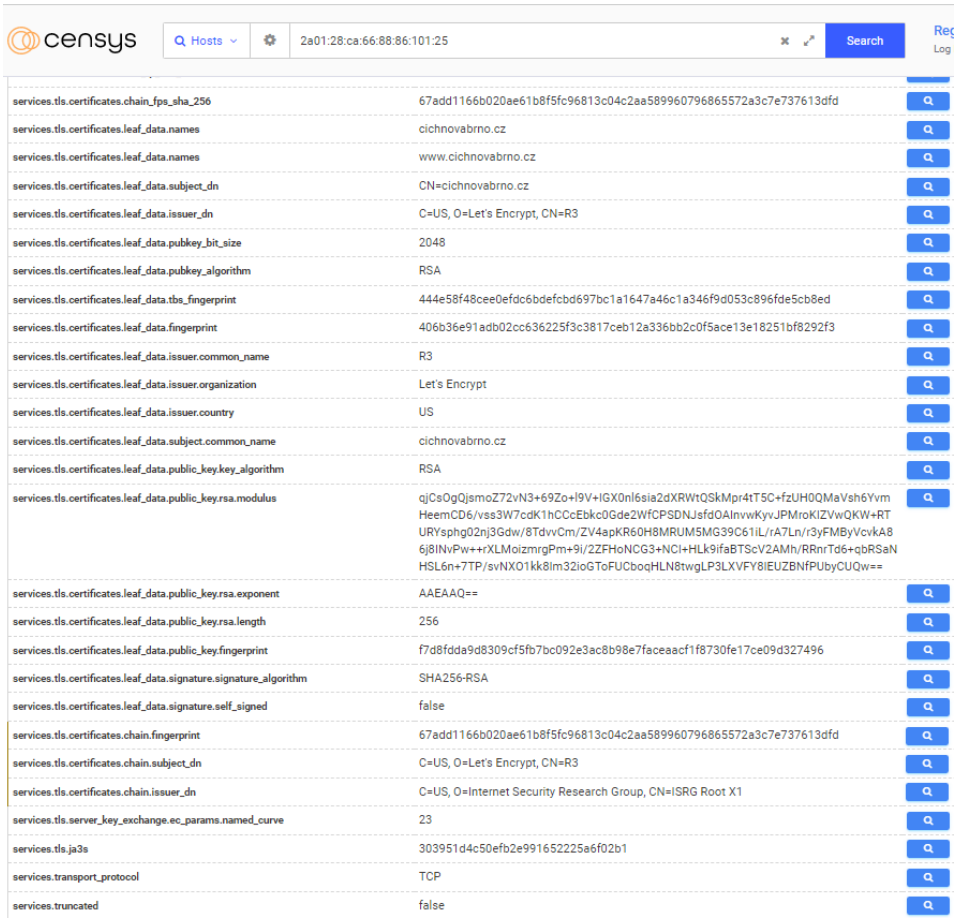
Za pomoci nástroje Censys zjistěte IP adresu pro www.cichnovabrno.cz, použitou kryptosadu a termín vypršení certifikátu. Nezapomeňte se zaregistrovat na https://search.censys.io/ - viz obr. 2.2.1.1 vpravo nahoře, odkaz na registrační stránky lze snadno přehlédnout.



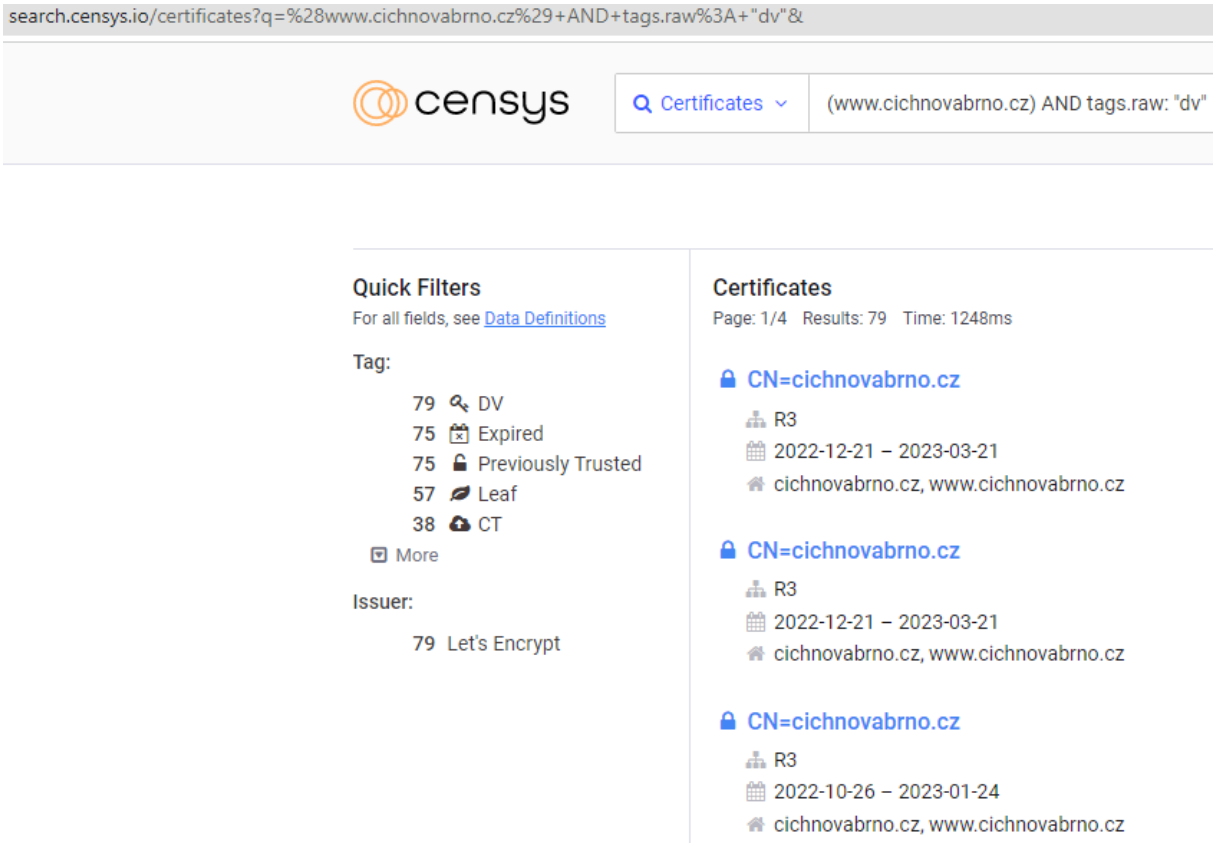
Obr. 2.2.1.1 Na Censys se je třeba zaregistrovat.

2.2.2 Řešení





Použitá kryptosada je TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

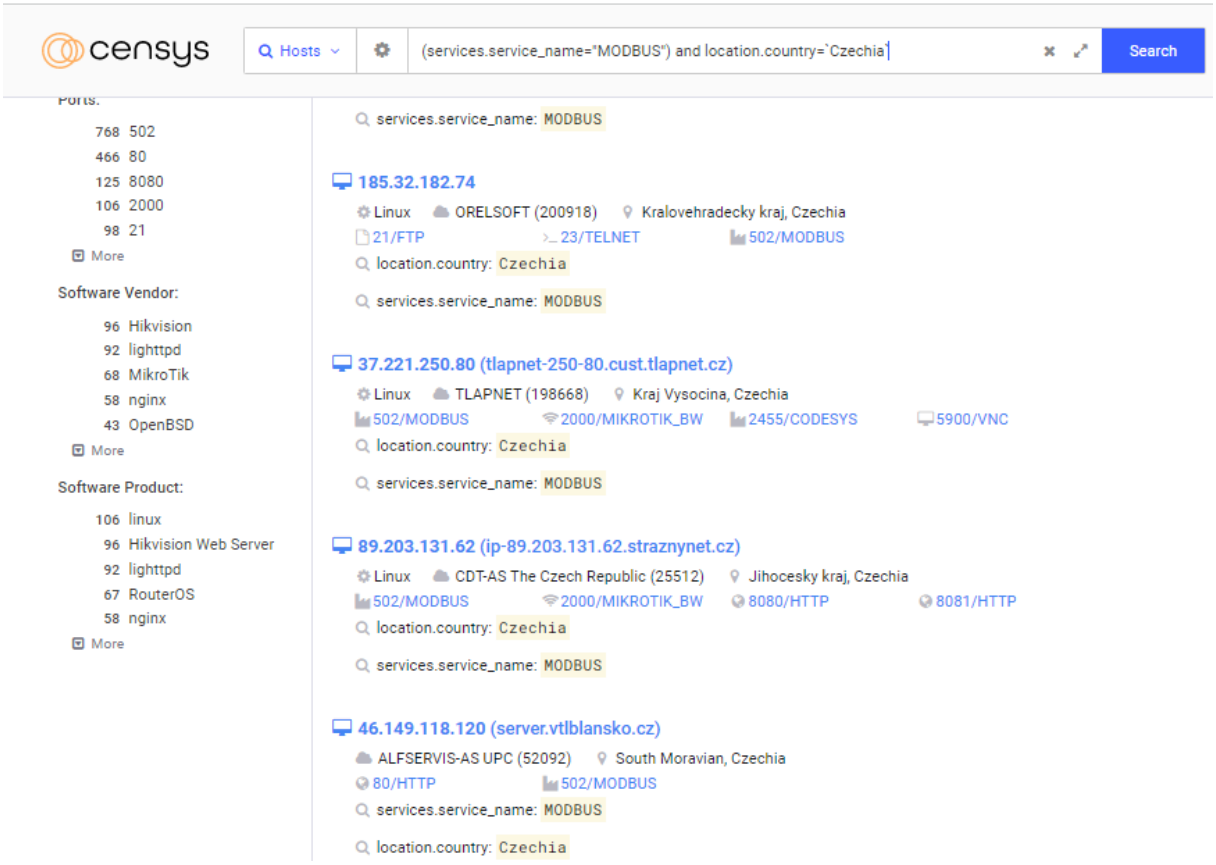


2.3 Použití Censysu pro IoT

2.3.1 Zadání

Za pomoci nástroje Censys zjistěte vhodné cíle pro útoky na Internet věcí (Scada engine a MODBUS protokol) v České republice.

2.3.2 Řešení



2.4 Použití Infoooze

2.4.1 Zadání

Zjistěte pomocí Infooze registrační údaje školy do Internetu. Od kterého roku škola má škola internetoové připojení? Návod: Před instalací Infoooze si mainstalujte nodejs. Použijte Kali, pokud se rozhodnete pro použijetí Ubuntu, aktualizujte jeho verzi.

2.4.2 Řešení

https://www.golinuxcloud.com/open-source-intelligence-osint-tools/

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo su

┌──(root㉿kali)-[/home/kali/Desktop]
└─# sudo apt-get install nodejs
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nodejs is already the newest version (14.19.0-deb-1nodesource1).
0 upgraded, 0 newly installed, 0 to remove and 491 not upgraded.

┌──(root㉿kali)-[/home/kali/Desktop]
└─# sudo npm install infoooze -g -s
/usr/bin/infoooze -> /usr/lib/node_modules/infoooze/bin/infoooze.js
/usr/bin/infooze -> /usr/lib/node_modules/infoooze/bin/infoooze.js
```

```
/usr/bin/infoze -> /usr/lib/node_modules/infoooze/bin/infoooze.js
┌──────────────────────────────────────────────────┐
│                                                  │
│   Thank You for Installing Infoooze@1.2.2        │
│                                                  │
│      Type infoooze -h for Help Menu              │
│   Don't forget to give this project a star!      │
│                                                  │
└──────────────────────────────────────────────────┘
+ infoooze@1.2.2
added 300 packages from 223 contributors in 59.393s

┌──(root㉿kali)-[/home/kali/Desktop]
└─# infoooze -h
 Usage: infoooze [options] [command]

 Commands:
  help     Display help
  version  Display version

 Options:
  -n, --dnslookup       domain name system lookup
  -d, --domainage       find website Age
  -x, --exif            extracts Exif metadata from image
  -g, --gitrecon        find github user info
  -e, --headerinfo      find website headers
  -h, --help            Output usage information
  -i, --instaRecon      find Instagram users info
  -p, --iplookup        find IP info
  -m, --mailfinder      find email with specific name
  -t, --portscan        find open ports
  -s, --subdomain       find subdomains of website
  -c, --subdomainrecon  find subdomains passively
  -l, --urlexpand       long url of shorten URL
  -u, --useragent       find browser info
  -r, --userrecon       username reconnaissance
  -v, --version         Output the version number
  -a, --webscan         analyze suspicious URLs
  -w, --whoislookup     find doamin's whois info
  -y, --youtubelookup   find video metadata

 Examples:
  - find username on diffrent social networks
  $ infoooze -r YOUR_USERNAME

  - find doamin's whois info
  $ infoooze -w google.com

  - find instagram username info
  $ infoooze -i therock

  - find IP address details
  $ infoooze -p 1.1.1.1
```

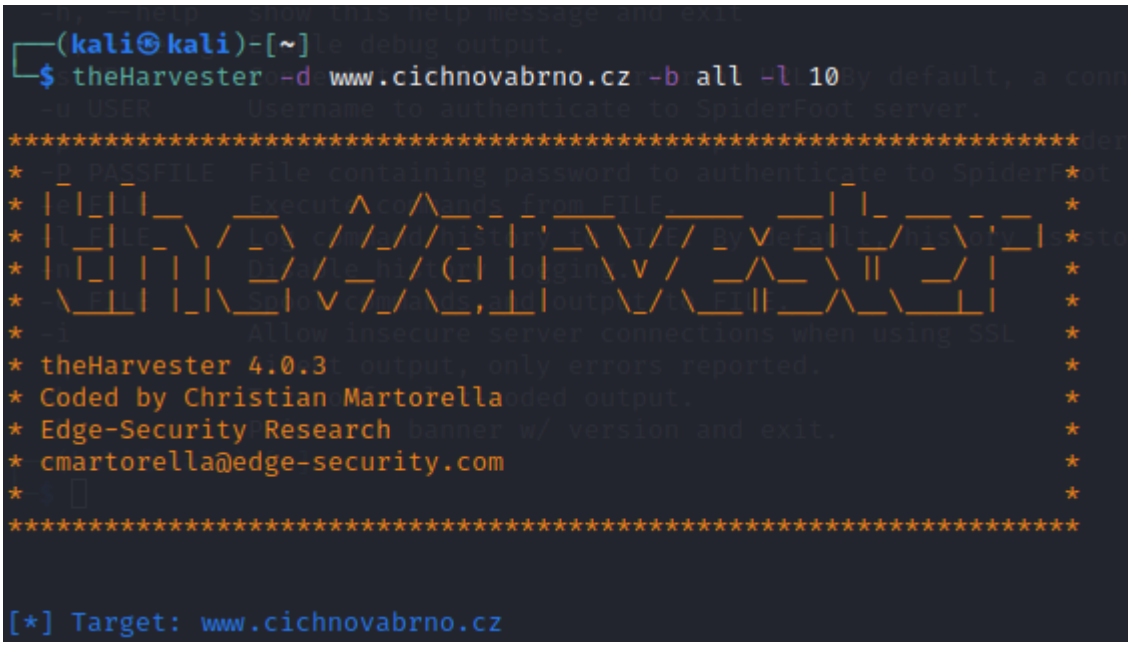
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# infoooze -w cichnovabrno.cz

 ______      __
|_   _|    / _|
  | |  _ __ | |_ ___   ___   ___ ________
  | | | '_ \|  _/ _ \ / _ \ / _ \_  / _ \
 _| |_| | | | || (_) | (_) | (_) / /  __/
|_____|_| |_|_| \___/ \___/ \___/___\___|
                        v1.2.2


[!] Results will be saved in /home/kali/Desktop/results/infoooze_whois_13112022184740.txt
[01] Full text available at : % http://www.nic.cz/page/306/intended-use-of-supplied-data-and-information/
[02] Whoisd server version : 3.12.2
[03] Timestamp : Sun Nov 13 23:47:42 2022
[04] Domain : cichnovabrno.cz
[05] Registrant : A24CONTACT-15496
[06] Nsset : NSS:GLOBE-SGLO000001:1 NSS:GLOBE-SGLO000001:1
[07] Keyset : A24-KEYSET A24-KEYSET
[08] Registrar : REG-ACTIVE24 REG-ACTIVE24 REG-ACTIVE24 REG-ACTIVE24 REG-ACTIVE24
[09] Registered : 08.06.2012 04:01:23
[10] Changed : 08.06.2012 07:08:35 15.05.2018 21:32:00 28.10.2021 22:12:07 15.05.2018 21:32:00 10.09.2019 15:48:38
[11] Expire : 08.06.2023
[12] Contact : A24CONTACT-15496 ACTIVE24
[13] Org : Stredni odborna skola, Stredni odborne uciliste informatiky a spoju ACTIVE 24, s.r.o.
[14] Name : Stredni odborna skola, Stredni odborne uciliste informatiky a spoju ACTIVE 24, s.r.o.
[15] Address : Cichnova 23 Brno 624 00 CZ Sokolovská 394/17 Praha 8 186 00 CZ
[16] Created : 01.12.2008 12:49:54 01.10.2007 02:00:00 29.04.2008 12:35:02 26.11.2008 14:12:02
[17] Nserver : alfa.ns.active24.cz (81.95.96.2, 2a02:4a8:ac24:100::96:2) beta.ns.active24.cz (81.0.238.27, 2001:1528:151::12) gama.ns.active24.sk
[18] Tech c : ACTIVE24 ACTIVE24
[19] Dnskey : 257 3 13 0EK9ChwJW+CVCvP7mizQwEnR2OJpHgbLmilGV5OyqncZoOufo9fIbVrvxT6qid/T9sAWH7KOfzItPxkVOIbRjg==
Thank You for using Infoooze

┌──(root㉿kali)-[/home/kali/Desktop]
└─#
```

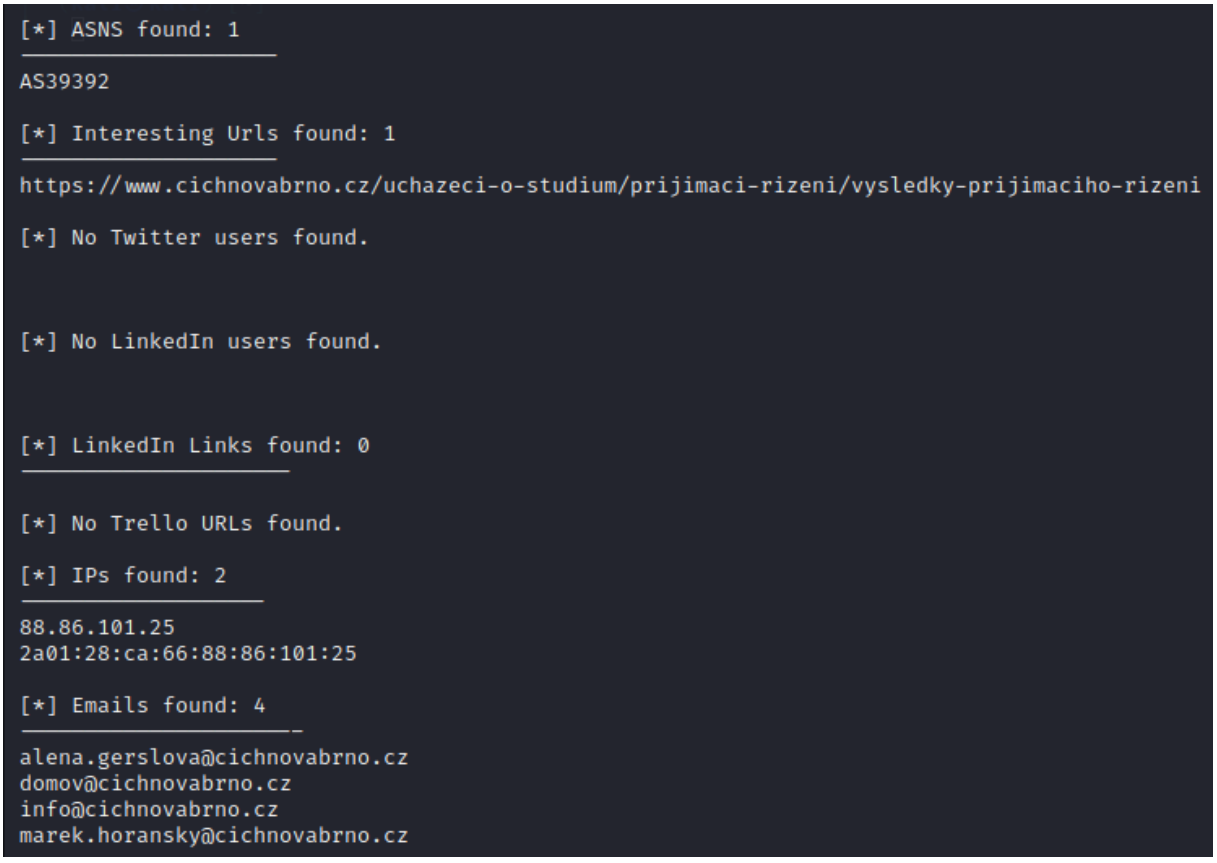
2.5 Použití theHarvesteru

2.5.1 Zadání

Za pomoci nástroje theHarvester zjistěte jméno správce sítě své školy.

2.5.2 Řešení





2.6 Použití nástroje Recon-ng

2.6.1 Zadání

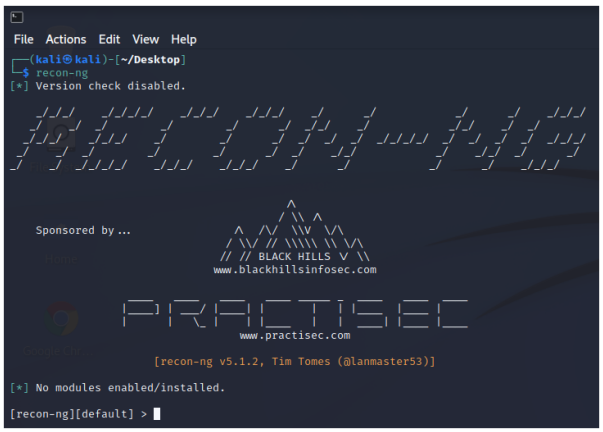
Za pomoci nástroje recon-ng zjistěte informace o subdoménách používaných Facebookem.

2.6.2 Návod k postupnému řešení

2.6.2.1 Dílčí úkol 1

Začněte toto cvičení otevřením Kali Linuxu ve vašem virtuálním počítači. Poté jako uživatel root otevřete terminál a zadejte:

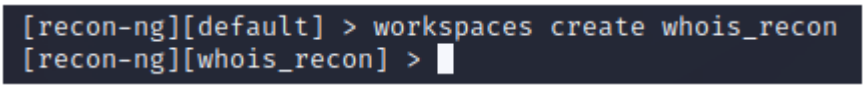
```
recon-ng
```



2.6.2.2 Dílčí úkol 2

Recon-ng nabízí uživatelům možnost vytvářet různé pracovní stanice na základě jejich projektových potřeb. Pro tuto laboratoř budeme shromažďovat informace WHOIS. Vytvořte tedy novou laboratoř zadáním následujícího:

```
workspaces create whois_recon
```



2.6.2.3 Dílčí úkol 3

Začneme shromažďováním informací WHOIS o cílovém názvu domény. Vzhledem k tomu, že informace WHOIS jsou dostupné komukoli, je v pořádku to udělat pro jakoukoli doménu. Doména, na kterou se zaměříme, je opět „facebook.com“, ale tuto laboratoř můžete provést pro jakoukoli jinou doménu, kterou chcete.

Pro vyhledávání informací WHOIS budeme muset nainstalovat moduly z tržiště. Začneme hledáním všech souvisejících informací týkajících se cílové stránky ve WHOIS. K tomu musíme nejprve nainstalovat vyhledávací modul WHOIS. Chcete-li to provést, zadejte:

```
marketplace search whois
```

```
[recon-ng][whois_recon] > marketplace search whois
[*] Searching module index for 'whois' ...

  +-------------------------------------------------------------------------------+
  |                    Path                    | Version |     Status    | Updated    | D | K |
  +-------------------------------------------------------------------------------+
  | recon/companies-domains/viewdns_reverse_whois | 1.1     | not installed | 2021-08-24 |   |   |
  | recon/companies-multi/whois_miner             | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/domains-companies/whoxy_whois           | 1.1     | not installed | 2020-06-24 |   | * |
  | recon/domains-contacts/whois_pocs             | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/netblocks-companies/whois_orgs          | 1.0     | not installed | 2019-06-24 |   |   |
  +-------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][whois_recon] >
```

Chceme nainstalovat čtvrtou možnost, která je „recon/domains-contacts/whois_pocs“.

marketplace install recon/domains-contacts/whois_pocs

```
[recon-ng][whois_recon] > marketplace install recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Reloading modules ...
[recon-ng][whois_recon] >
```

Chcete-li načíst modul pro použití, zadejte:

```
modules load recon/domains-contacts/whois_pocs
```

Abychom mohli začít hledat, musíme nastavit zdroj zadáním:

```
options set SOURCE facebook.com
```

```
[recon-ng][whois_recon] > modules load recon/domains-contacts/whois_pocs
[recon-ng][whois_recon][whois_pocs] > options set SOURCE facebook.com
SOURCE ⇒ facebook.com
[recon-ng][whois_recon][whois_pocs] >
```

Poté, chcete-li zobrazit informace o tomto modulu a jak se používá, zadejte „info“ a stiskněte Enter.

```
[recon-ng][whois_recon][whois_pocs] > info

      Name: Whois POC Harvester
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the
  'contacts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  facebook.com   yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][whois_recon][whois_pocs] >
```

Nyní jsme připraveni vyhledat v WHOIS informace týkající se „facebook.com“. Jednoduše zadejte „run“ a stiskněte Enter pro zahájení vyhledávání.

Jak uvidíte, o facebook.com se zobrazí různé kontaktní informace a informace o poloze. Tyto informace budou automaticky uloženy na naší pracovní stanici.

2.6.2.4 Dílčí úkol 4:

Recon-ng: Nyní se pokusíme pomocí HackerTarget.com API objevit co nejvíce subdomén s jejich IPv4 adresou pro facebook.com. Bude třeba importovat modul „hackertarget“, jako jsme to udělali dříve pro „whois_pocs“.

Než to uděláme, bude nutné nejprve napsat „back“ a stisknutím klávesy Enter modul whois_pocs opustit. Začneme pak hledáním marketplace pro moduly „hackertarget“ pomocí příkazu:

```
marketplace search hackertarget
```

Měla by se zobrazit pouze jedna možnost, a to „recon/domains-hosts/hackertarget“. Tuto možnost lze zvýraznit a stisknutím ctrl + shift + c kopírovat cestu k modulu a pak ji vložit pomocí ctrl + shift + v. K instalaci modulu použijte:

```
[recon-ng][whois_recon][whois_pocs] > back
[recon-ng][whois_recon] > marketplace search hackertarget
[*] Searching module index for 'hackertarget' ...

  +-------------------------------------------------------------------------------+
  |              Path               | Version |     Status    |  Updated   | D | K |
  +-------------------------------------------------------------------------------+
  | recon/domains-hosts/hackertarget | 1.1     | not installed | 2020-05-17 |   |   |
  +-------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][whois_recon] >
```

Nainstalujeme si modul hackertarget:

```
marketplace install recon/domains-hosts/hackertarget
```

```
[recon-ng][whois_recon] > marketplace install recon/domains-hosts/hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][whois_recon] >
```

a pak si modul zavedeme do paměti:

```
modules load recon/domains-hosts/hackertarget
```

```
[recon-ng][whois_recon] > modules load recon/domains-hosts/hackertarget
[recon-ng][whois_recon][hackertarget] >
```

Nyní jsme připraveni začít hledat v HackerTarget informace o subdoménách týkajících se Facebooku. Nejprve nastavte zdroj zadáním:

```
options set SOURCE facebook.com
```

```
[recon-ng][whois_recon][hackertarget] > options set SOURCE facebook.com
SOURCE ⇒ facebook.com
[recon-ng][whois_recon][hackertarget] >
```

Pokud chcete vidět nějaké informace o tom, k čemu a jak se tento modul používá, jednoduše napište „info“ a stiskněte Enter.

Když dáte „run“, vyjede vám přes 500 záznamů subdomén. Tyto informace mohou být užitečné pro útočníka, který se může zaměřovat na Facebook. Tyto informace lze použít k útoku na různé subdomény a jejich IP adresy spojené s Facebookem, které nemusejí být všechny stejně dobře bezpečné zabezpečené.

K čemu jsme došli:

- Když dáte „run“, vyjede vám přes 500 záznamů subdomén. Tyto informace mohou být užitečné pro útočníka, který se může zaměřovat na Facebook.
- Tyto informace lze použít k útoku na různé subdomény a jejich IP adresy spojené s Facebookem, které nemusejí být všechny stejně dobře bezpečné zabezpečené.

2.7 Použití nástroje PimEyes

2.7.1 Zadání

Nalezněte na internetu fotografii známé osobnosti a pomocí nástroje PimEyes zjistěte a spočítejte aktuální počet fotografií na internetu.

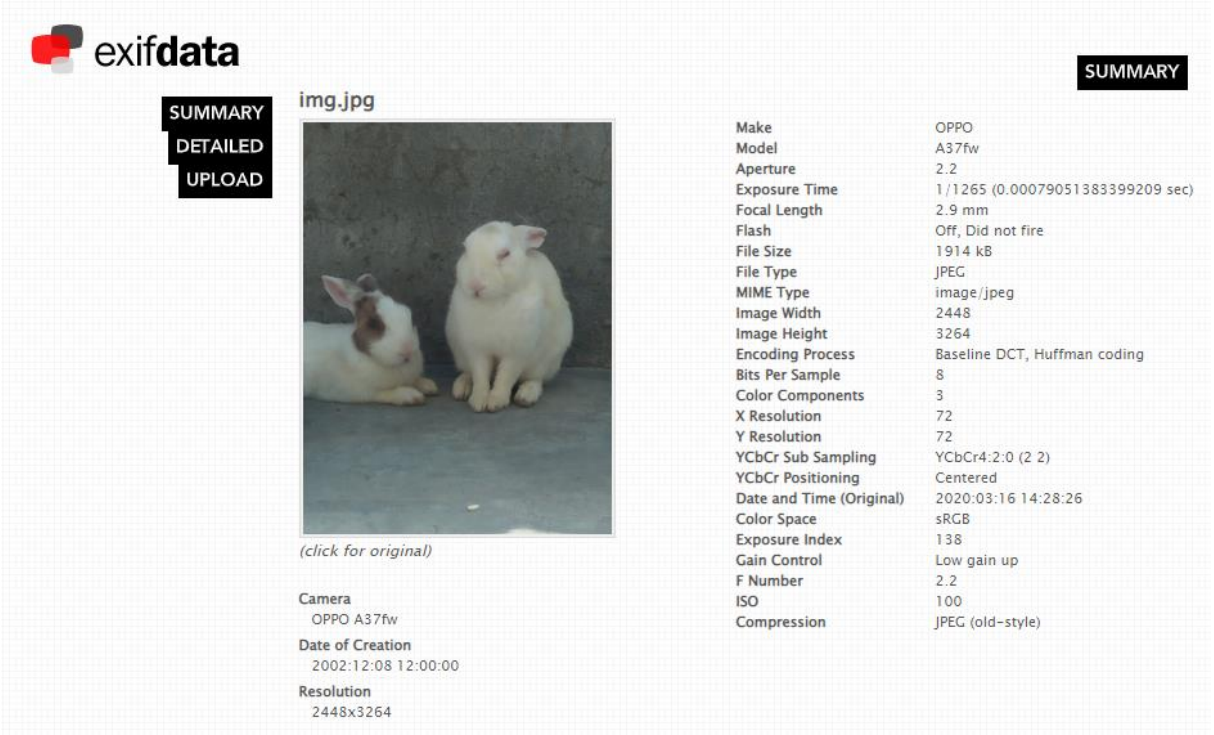
2.7.2 Možné řešení

2.8 Použití nástroje exifdata

2.8.1 Zadání

Zjistěte parametry učitelem zadaného obrázku.

2.8.2 Možné řešení



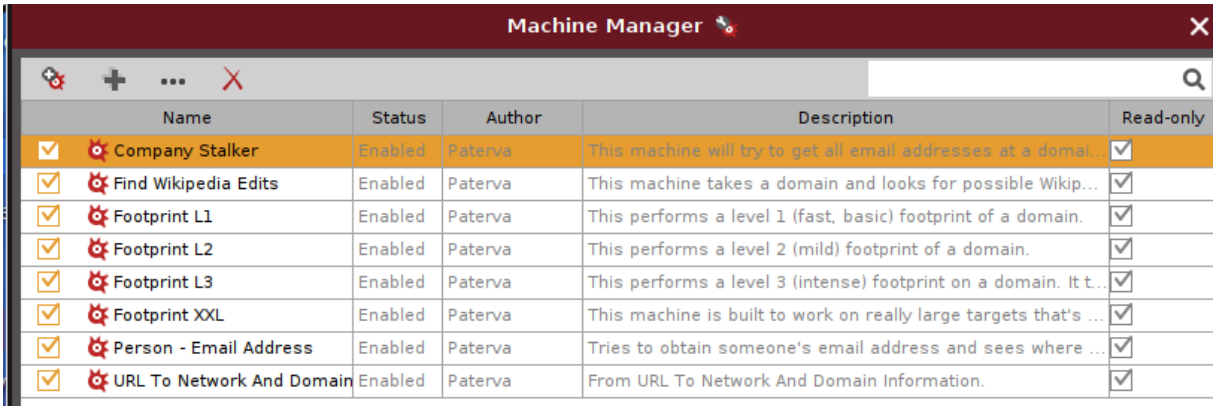
2.9 Použití nástroje Maltego (volitelný příklad, případně domácí úkol)

2.9.1 Zadání

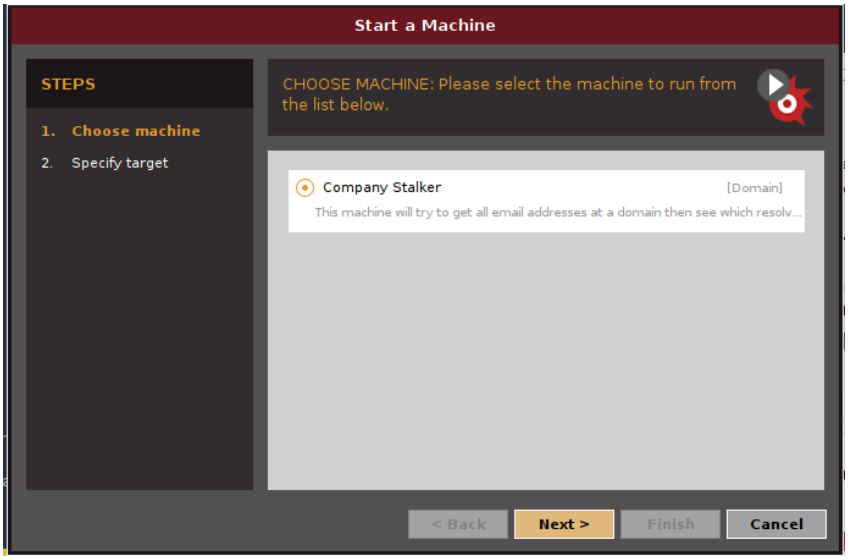
Registrujte se jako člen komunity a použijte stroj “Machiny Stalker” pro zjištění informačních zdrojů ma www.cichnovabrno.cz.

2.9.2 Řešení

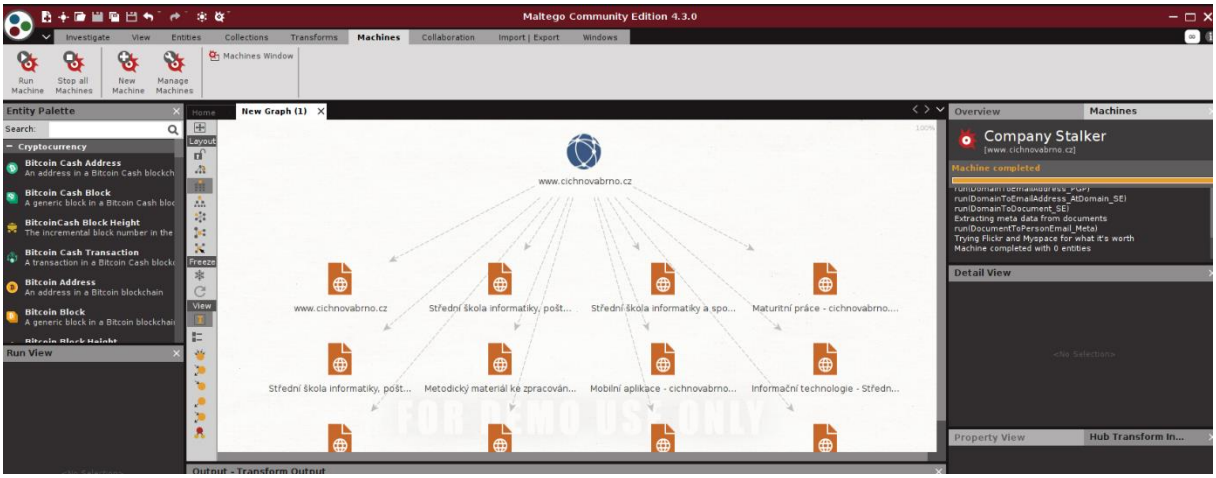
1. Výběr Company Stalkera ze sady strojů dostupných pro členy komunity



2. Spuštění Company Stalkera



3. Řešení úlohy



2.10 Použití knihoven Pillow a EXIF v Pythonu (volitelný příklad, případně domácí úkol)

2.10.1 Zadání

Zjistěte parametry vybraného obrázku pomocí programování v Pythonu. Lze získat více informací než bez programování?

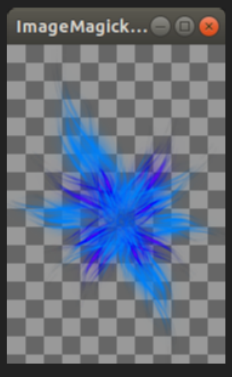
2.10.2 Řešení

Instalace pillow

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> pip install pillow
Requirement already satisfied: pillow in c:\python38\lib\site-packages (7.2.0)
```

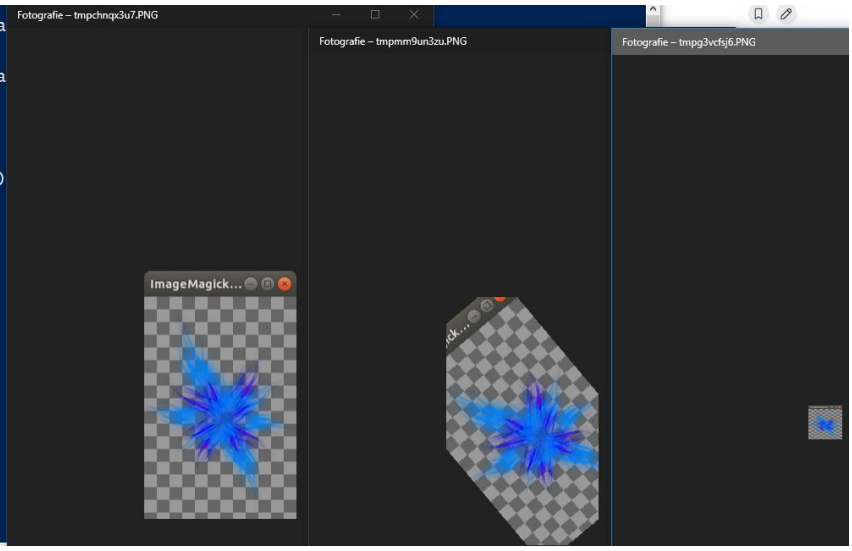
Zobrazení obrázku

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporat

PS C:\Windows\system32> python
Python ActivePython 3.8.2 (ActiveStat
 on win32
Type "help", "copyright", "credits" o
>>> from PIL import Image
>>>
>>>
>>> img = Image.open(r"C:\test.png")
>>> img.show()
>>>
```



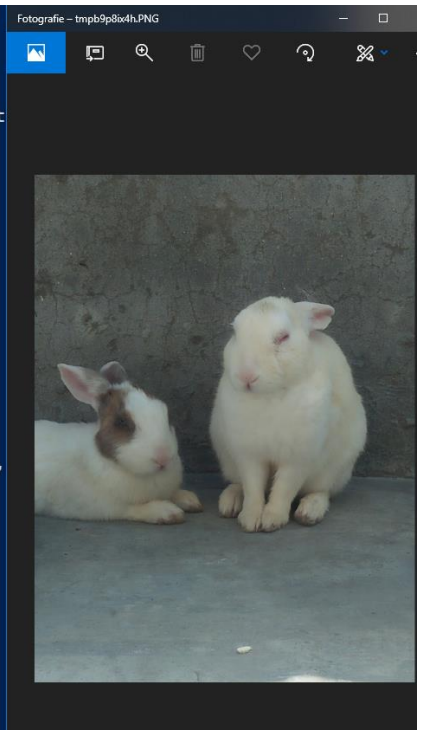
Další metody použitelné při použití knihovny pillow

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corpora

PS C:\Windows\system32> python
Python ActivePython 3.8.2 (ActiveSta
 on win32
Type "help", "copyright", "credits"
>>> from PIL import Image
>>>
>>>
>>> img = Image.open(r"C:\test.png")
>>> img.show()
>>> print(img.mode)
RGBA
>>> print(img.size)
(180, 293)
>>> print(img.format)
PNG
>>> angle = 40
>>> r_img = img.rotate(angle)
>>> r_img.show()
>>> size=(40,40)
>>> r_img = img.resize(size)
>>> r_img.show()
>>>
```



Extrakce základních metadat

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> python
Python ActivePython 3.8.2 (ActiveState Software Inc.) based on
 on win32
Type "help", "copyright", "credits" or "license" for more informat
>>> from PIL import Image
>>> from PIL.ExifTags import TAGS
>>> import sys
>>>
>>> # cesta k obrazku
>>> imagename = "C:\img.jpg"
>>>
>>> # ctu data obrazku za pouziti PIL
>>> image = Image.open(imagename)
>>> image.show()
>>>
>>> # extrakt zakladnich metadat
>>> info_dict = {
...     "Filename": image.filename,
...     "Image Size": image.size,
...     "Image Height": image.height,
...     "Image Width": image.width,
...     "Image Format": image.format,
...     "Image Mode": image.mode,
...     "Image is Animated": getattr(image, "is_animated", False),
...     "Frames in Image": getattr(image, "n_frames", 1)
... }
>>>
>>> for label,value in info_dict.items():
...     print(f"{label:25}: {value}")
...
Filename                 : C:\img.jpg
Image Size               : (2448, 3264)
Image Height             : 3264
Image Width              : 2448
Image Format             : JPEG
Image Mode               : RGB
Image is Animated        : False
Frames in Image          : 1
>>>
```

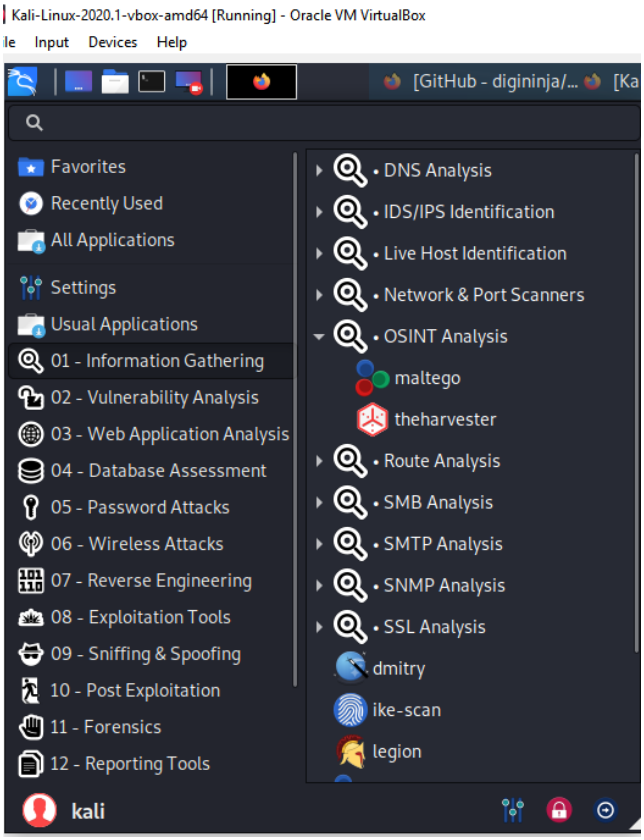


Extrakce všech metadat spojených s obrázkem

```
Frames in Image          : 1
>>> # extrakt EXIF dat
>>> exifdata = image.getexif()
>>>
>>> # iterování přes všechna datová pole EXIF
>>> for tag_id in exifdata:
...     # ziskej nazev znacky, misto lidsky necitelne ID znacky
...     tag = TAGS.get(tag_id, tag_id)
...     data = exifdata.get(tag_id)
...     # dekodovani bytu
...     if isinstance(data, bytes):
...         data = data.decode()
...     print(f"{tag:25}: {data}")
...
ExifVersion               : 0220
ComponentsConfiguration   : □□□
ShutterSpeedValue         : 10.304
DateTimeOriginal          : 2020:03:16 14:28:26
DateTimeDigitized         : 2002:12:08 12:00:00
ApertureValue             : 2.27
FlashPixVersion           : 0100
ColorSpace                : 1
ExifImageWidth            : 2448
Flash                     : 16
FocalLength               : 2.93
ExifImageHeight           : 3264
ExifInteroperabilityOffset: 474
GainControl               : 1
Make                      : OPPO
Model                     : A37fw
YCbCrPositioning          : 1
ExposureIndex             : 138.0
ExposureTime              : 0.00079051383399209 49
XResolution               : 72.0
YResolution               : 72.0
FNumber                   : 2.2
GPSInfo                   : {29: '2020:03:16', 7: (8.0, 58.0, 25.0)}
ISOSpeedRatings           : 100
ResolutionUnit            : 2
ExifOffset                : 138
MakerNote                 :  <  □6   □  □(
>>>
```

Shrnutí a závěr

OSINT zahrnuje širokou škálu nástrojů. U těch komplexnějších je jejich plné a více smysluplné využití možné jen u placených verzí resp. účtů. Některé z těchto nástrojů patří mezi sadu aplikací Kali Linuxu.



Zvláště zajímavý vývoj je u Maltego, kde v roce 2022 došlo ke 12 integracím, mj. s censysem, např. pro Python 3.6+ lze použít:

```
$ pip install censys-maltego
```

```
$ canari create-profile censys_maltego
```

V roce 2022 bylo v Maltego Academic & Non-Profit Programu podpořeno 55 akademických institucí a 20 neziskových organizací a dále nezávislí výzkumníci. Autor tohoto textu navázal emailové spojení s Maltego Technologies GmbH a obdržel obratem požadované materiály. Další vývoj je třeba sledovat a žáky seznámit s aktuálním stavem integrace.

Seznam použitých zdrojů

(Durumeric 2021) DURUMERIC Zakir. Censys Search 2.0 Official Launch Announcement. Blog June 1, 2021. Dostupné z: https://censys.io/censys-search-2-launch-announcement/

(GHDB 2022) Exploit Database. Dostupné z: https://www.exploit-db.com/

(GoogleGuide 2022) GoogleGuide. *This page was last modified on: Saturday January 29, 2022.* Dostupné z: https://www.googleguide.com/advanced_operators_reference.html

(Google Dorks 2022) Google Dorks List and Updated Database in 2022. *Last updated: Oct 21, 2022. Dostupné z: https://www.boxpiper.com/posts/google-dork-list*

(James 2022) JAMES, Cyril. OSINT and top 15 open-source intelligence tools, Sep 20, 2022. Dostupné z: https://medium.com/bugbountywriteup/osint-and-top-15-open-source-intelligence-tools-f5132bf9e40f

(LifeRaft 2022) Open Source Intelligence: The Beginners' Guide to OSINT. LifeRaft. Dostupné z: https://www.liferaftinc.com/blog/the-beginners-guide-to-osint

(materiály EU 2022) Duševní, průmyslové a obchodní vlastnictví. Fakta a čísla o Evropské unii. Dostupné z: https://www.europarl.europa.eu/ftu/pdf/cs/FTU_2.1.12.pdf

(OSINT Handbook 2022) OPEN SOURCE INTELLIGENCE TOOLS AND RESOURCES HANDBOOK 2020. I-intelligence 2020. https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf

(Tunggal 2022) Tunggal, Abi Tyas. The 67 Biggest Data Breaches (Updated September 2022). UpGuard updated Oct 10, 2022. Dostupné z: https://www.upguard.com/blog/biggest-data-breaches

(Redfox Security 2022) Redfox Security. Introduction to OSINT. Oct 20 2022, Dostupné z: https://redfoxsecurity.medium.com/introduction-to-osint-2c92597988d1

(TMC Source 2022) Open-Source-Intelligence-Resources. Dostupné z: https://github.com/TCM-Course-Resources/Open-Source-Intellingence-Resources