Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informatiky a kvantitativních metod

Návrh testovacího prostředí za využití nástrojů ATT&CK

Diplomová práce

Autor práce: Bc. Jiří Bönsch
Studijní obor: Aplikovaná Informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové 2023

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 23. dubna 2023 Jiří Bönsch

Poděkování

Tímto bych chtěl poděkovat vedoucímu diplomové práce Mgr. Josefu Horálkovi, Ph.D. za odborné vedení práce, poskytnuté rady a přínosné konzultace. Zároveň bych chtěl poděkovat rodině a přátelům za jejich pomoc a podporu.

Anotace

Cílem práce bylo poukázat na současný stav kybernetické bezpečnosti a vytvořit jednoduché a srozumitelné testovací prostředí spolu s návodem na jeho použití. Byla provedena rešerše literatury, kde jsou zkoumány nejnutnější informace nutné k pochopení kybernetické bezpečnosti, hrozby v podobě druhů útočníků a nejčastější typů útoků. Také jsou představeny základní principy testování, které jsou poté vyzkoušeny pomocí vytvořeného testovacího prostředí na simulované infrastruktuře s využitím scénářů, jenž napodobují reálné chování útočníka. Aby měla práce relevantní dopad, je simulovaná infrastruktura založena na reálné infrastruktuře využívané ve skutečné organizaci. Výsledkem je zhodnocení scénářů, ukázka silných i slabých stránek infrastruktury a postupy, jak sestavit a upravit testovací prostředí pro potřeby testování v praxi.

Annotation

Title: Design of test environment using ATT&CK tools

The aim of this work was to highlight the current state of cyber-security and create a simple and understandable testing environment along with instructions for its use. A literature review was conducted, examining the essential information necessary for understanding cyber-security, threats posed by different types of attackers, and the most common types of attacks. Basic testing principles were also introduced and tested using the created testing environment on simulated infrastructure using scenarios that mimic real attacker behavior. To ensure the work has relevant impact, the simulated infrastructure is based on real infrastructure used in an actual organization. The results include an evaluation of the scenarios, demonstration of strengths and weaknesses of the infrastructure, as well as procedures for creating and modifying the testing environment for practical testing purposes.

Obsah

1 Úvod **1**

2 Cíl práce **3**

3 Metodika zpracování **4**

4 Relevantnost problematiky kybernetické bezpečnosti **5**
4.1 Studie trendů kybernetické bezpečnosti 5

5 Nejčastější kybernetické útoky **11**
5.1 Malware 12
5.2 Sociální inženýrství 19
5.3 Threat against data 22
5.4 Threat against availability 24
5.5 Ostatní útoky 25

6 Kategorie útočníků **28**
6.1 Příležitostný útočník 28
6.2 Script kiddie 28
6.3 Hacktivista 29
6.4 Hacker na objednávku 29
6.5 Kyberkriminálník 30
6.6 Státem podporovaný útočník 30
6.7 Insider (vnitřní osoba) 31

7 Testování **33**
7.1 Rozsah testování 34
7.2 Metodologie testování 35

8 Zavedené nástroje v problematice Testování **37**
8.1 MITRE ATT&CK 37
8.2 Nástroje 41

9 Příprava praktické části práce **44**
9.1 Popis testovacího prostředí 44
9.2 Popis testované infrastruktury 48

10 Testované scénáře **51**
10.1 Scénář 1 – *Recon* 51

10.2 Scénář 2 – *Discovery* a *Elevate-privileges* 53
10.3 Scénář 3 – *Discovery, Impact* a *Lateral movement* 72

11 Závěry a doporučení **76**

Seznam použitých zdrojů **78**

Seznam zkratek **83**

Seznam obrázků **84**

Seznam ukázek kódů **86**

1 Úvod

V dnešní době tráví velká část lidské populace díky rozvoji moderních technologií značné množství času interakcemi s těmito technologiemi. Ať už se jedná o internet, IoT (Internet of Things) zařízení, mobilní bankovnictví nebo sociální sítě, lidé se na technologiích stávají čím dál více závislí. Technologie nám usnadňují všední život, dovolují práci z domova nebo přináší příležitosti, které i jen pár let zpátky neexistovaly. Tento rozvoj bohužel nemá jen klady, přinesl zároveň hrozby, kterým nyní populace čelí. I když jsou kladeny stále větší nároky na bezpečnost, nezdá se to být dostatečné. Některé hrozby, jako malware, jsou pro lidstvo nové, jiné jsou staré jako lidstvo samo a pouze se novým okolnostem přizpůsobily. Jedním příkladem za všechny je Sociální inženýrství, s rozvojem internetu je přístup k informacím jednoduchý a není tak problém tímto typem útoku ohrožovat velké množství populace. Internet navíc přinesl dostupnost informací nejen běžným občanům, ale i útočníkům, kteří proto nemají problém vytvářet propracované útoky ani získávat nové metodologie útoku.

Existuje také nezměrné množství hrozeb, kterým nečelí jen lidé, ale i firmy, a dokonce státy. Státy na celém světě se staly na kybernetickém světě zcela závislé a jakékoli jeho selhání může ohrozit jejich funkčnost, navíc odpoutat se od něj je již nemožné[1]. Je jasné, že v prostředí, v němž mezi sebou soupeří státy, je značné úsilí věnováno jak zabezpečení, tak útoku. Rozdíly mezi kybernetickým útokem, kybernetickým zločinem a kybernetickou válkou jsou ve většině případů založeny pouze na účastnících těchto situací[1, 2]. Způsoby útoku či hrozby mají jen minimální vliv na zařazení do předchozích kategorií, zohledněn bývá pouze výsledek. Vyšší účast států v kybernetickém světě však nese následek i na jejich obyvatelstvo a organizace působící na území daného státu. Pokrok digitalizace sice usnadňuje mnohým obyvatelům život, je však potřebné myslet i na rizika, která obyvatelům hrozí primárně v podobě úniku osobních informací. Je nutné vytvářet, dodržovat a obnovovat předpisy, jenž zajišťují holistickou obranu všech subjektů. Stejně tak je ale nutné uznat, že praktické příklady mnohdy daným předpisům protiřečí, nebo naopak ukazují, že předpis v reálném světě není aplikovatelný. Je tedy nutné propojit idealistický pohled na obranu v rámci předpisů a nařízení s pohledem praktickým. Právě za tímto účelem je nutné nastavené předpisy testovat skutečnými útoky, aby bylo možné určit, zda opravdu splňují důvod svého vzniku.

Tato diplomová práce je rozdělena na dvě primární části – teoretickou a praktickou. V teoretické části jsou zkoumány nejnutnější informace nutné k pochopení kybernetické bezpečnosti. Jsou představeny nejčastější hrozby nejen z pohledu útoků, ale také útočníků spolu s jejich motivacemi a metodikami. Také jsou představeny základní teoretické principy testování, které jsou poté vyzkoušeny v praktické části práce. Proto bylo vytvořeno

testovací prostředí, simulovaná infrastruktura a scénáře, napodobující reálné chování útočníka. Aby měla práce relevantní dopad, je simulovaná infrastruktura založena na reálné infrastruktuře využívané ve skutečné organizaci. Výsledkem jsou cenná data ukazující silné i slabé stránky infrastruktury, a také postupy, jak sestavit a upravit testovací prostředí pro potřeby testování v praxi.

2 Cíl práce

Diplomová práce je zaměřena na zkoumání oblasti kybernetické bezpečnosti. Cílem práce je obeznámit neznalou osobu s nejzákladnějšími termíny kybernetické bezpečnosti a připravit pro tuto osobu jednoduché a srozumitelné testovací prostředí, které lze použít k testování taktik a technik MITRE ATT&CK. Takto obeznámená osoba by posléze měla být schopna otestovat bezpečnost vlastní infrastruktury.

Teoretická část práce se věnuje předání základních informací o kybernetické bezpečnosti. Za účelem dosažení primárního cíle je zkoumána relevantnost kybernetické bezpečnosti, jsou vysvětleny nejčastější útoky, s nimiž je možné se setkat, a také jsou představeny nejčastější typy útočníků. V návaznosti na praktickou část jsou také popsány základní principy testování a představeny vybrané nástroje. Vědomosti obsažené v této části jsou důležité pro optimální využití praktické části práce.

Praktická část práce cílí na tvorbu a vysvětlení testovacího prostředí. Obsahuje postup pro vytvoření testovacího prostředí, přípravu testovacích nástrojů a řešení pro možné problémy, které při prvotním nasazení mohou nastat. Dále se tato část práce věnuje ukázce využití připravených nástrojů na realistických scénářích testování, které jsou založeny na poznatcích získaných z teoretické části práce. Závěrem je ukázka testování na infrastruktuře, jež modeluje reálnou strukturu, a také ukázka a kontext možných výstupů tohoto testování.

3 Metodika zpracování

Metodický postup pro tuto diplomovou práci byl rozdělen do dvou částí (teoretické a praktické), které se sestávaly z několika provázaných částí.

Teoretická část za zabývá analýzou oblasti kybernetické bezpečnosti. Za tímto účelem byla provedena rešerše současné literatury, zhodnocení získaných dat o kybernetických útocích v posledních letech a také představení základů testování.

Praktická část práce je zaměřena na vytvoření jednoduchého a srozumitelného testovacího prostředí s následným ověřením jeho funkcionality. Využívá k tomuto účelu poznatky zjištěné v teoretické části. Byly vytvořeny testovací scénáře, které jsou následně využity k testování reálné i simulované infrastruktury. Aby simulovaná infrastruktura co nejvíce odpovídala skutečné, zakládá se na dotazníkovém šetření a konzultaci s administrátorem této infrastruktury. Pokud je to možné, je preferováno, aby testování bylo prováděno oproti skutečné infrastruktuře. Z důvodu ochrany osobních a interních dat organizace nejsou v této diplomové práci uváděna jména ani jiné identifikační údaje.

V práci jsou testovány dvě hypotézy:

- Je možné vytvořit jednoduché testovací prostředí a seznámit s jeho ovládáním neznalého uživatele?
- Jsou výsledky získané z testovaného prostředí realistické a mají praktický význam pro zlepšení bezpečnosti skutečné infrastruktury?

Problematika Kybernetické bezpečnosti zatím není v České republice řešena na úrovni srovnatelné se zbytkem světa, proto i naši odborníci využívají zahraniční odbornou literaturu. Z toho důvodu bylo pro zpracování této diplomové práce čerpáno převážně ze zahraničních zdrojů a literatury, při psaní byly využity pojmy, obrázky či grafy, u nichž bylo ponecháno původní znění, protože při doslovném překladu by mohlo dojít ke špatné interpretaci uváděných pojmů.

4 Relevantnost problematiky kybernetické bezpečnosti

Relevantnost problematiky kybernetické bezpečnosti potvrzuje nejen množství akademických textů, které zkoumají tuto problematiku, ale také stále větší zájem všeobecné veřejnosti. Hlavním důvodem je vzrůstající povědomí populace způsobené především medializací útoků sociálního inženýrství nebo ransomwarových kampaní, které populaci v poslední době ovlivňovaly. V době psaní této práce je v popředí například ransomwarový útok na dětskou nemocnici *SickKids*, při němž došlo k omezení optimální funkčnosti nemocnice zašifrováním důležitých interních systémů[3]. I když se Ransomwarová skupina *LockBit* omluvila a zdarma poskytla nemocnici *decryptor*, nemění to nic na vážnosti situace – skutečnosti, že takový útok vůbec nastal. A bohužel není jediným ransomwarovým útokem zaměřeným na zdravotnictví, naopak je možné předpokládat, že v budoucnu nastanou i další útoky. A příští útok nemusí být veden skupinou, která se řídí silným morálním kompasem. Důležité je na závěr poznamenat, že tento morální kompas platí jen na omezení funkčnosti které může vést ke smrti. Nevztahuje se na méně kritické instituce nebo ani na prodej již získaných zdravotních dat na černém trhu.

Kybernetická bezpečnost si zaslouží dlouhodobou pozornost společnosti. Existují hrozby, které jsou dobře prostudované, a víme, jak se jim efektivně bránit. Existují hrozby, kterým je sice obtížné se bránit, ale jsou omezené rozsahem, a tak je obrana uskutečnitelné. Ale existují také hrozby, na než obrana zatím neexistuje. A tyto hrozby je nutné najít a zkoumat, aby bylo možné ochranu vytvořit.

4.1 Studie trendů kybernetické bezpečnosti

Dlouhodobě můžeme v rámci kybernetické bezpečnosti rozeznávat několik klíčových zaměření. Zajímavé jsou změny v prioritách zaměření v určitém období, které můžeme zkoumat na literatuře. Velké změny lze zaznamenat především před a po pandemii Covidu-19[4]. Jako i u jiných odvětví můžeme celou sféru dělit na 2 části, část akademickou a část veřejnou. Je jasné, že zaměření těchto dvou částí budou lehce rozdílná, proto je nutné dívat se na ně odděleně, třebaže se v mnoha ohledech překrývají a ovlivňují. Důvodem, proč zkoumáme rozdíl před a po Covidu-19, je rapidní navýšení adopce digitálních technologií, které v této době proběhlo. Ztížené pracovní podmínky vyžadovaly zavádění nových technologií, to ale zároveň znamená nová bezpečnostní rizika vzniklá nejen z těchto technologií, ale i z přístupu k jejich využívání. Je značný rozdíl v bezpečnosti práce uživatele, nachází-li se v uzavřené síti uvnitř společnosti nebo při připojování na dálku při práci z domova.

Akademická literatura

V akademické sféře je možné vidět zaměření výzkumu. Dlouhodobě populárními tématy

jsou *cyber risk management, detekce malwaru* nebo *systémy detekce přístupu*. Tato témata je možné nalézt jak před, tak i po pandemii Covidu-19. Témata, která byla mnohem více zkoumána před pandemií, jsou například využití *Machine learningu*, a to jak pro detekci hrozeb, tak pro hledání nových vektorů útoku, dále *Blockchain* a *Cryptoměny*. Pandemie způsobila velký obrat v myšlení a reorganizaci priorit, což vedlo ke zkoumání témat, která byla nutná aplikovat okamžitě nebo která byla nutná pro budoucí fungování společnosti. Objevují se zde mnohem více témata zaměřená na *Zdravotnictví, Bankovní sektor* nebo *zranitelnosti dodavatelského řetězce*. Všechna tato témata mají jasný vznik v okolnostech pandemie a jejich zkoumání je prováděno i roky po pandemii samotné.[4]

Všeobecná literatura

Všeobecná literatura poukazuje na zájmy a zvědavost lidu, proto zde lze odvodit zaměření i problémy populace. Před pandemií byly nejčastější témata zaměřená na *finančně zaměřené kybernetické útoky*. Ty spolu s běžnými tématy jako *běžné bezpečnostní zranitelnosti, úniky dat* a *malwarové incidenty*, vzbuzovaly největší zájem médií[4]. Pandemie nicméně tato témata rapidně změnila a zájem lidu se postupně začal zaměřovat na útoky, které se během pandemie značně rozšířily. Největší hrozbou se staly *Sociální inženýrství* nebo *ransomwarocé* útoky, také útoky na *Zdravotnictví* byly mnohem častěji reportovány medii. Tématem, které je v obou obdobích významné je *malware*, jeho primární zaměření se však liší. Před pandemií se literatura týkala hlavně ovlivnění správného chodu firem, po pandemii se psalo spíše o dopadech na digitální infrastrukturu, jako jsou *služby v cloudu*.

Současné trendy

V současných trendech však dominuje konflikt na Ukrajině. Je známé, že Rusko provádělo přípravu roky před samotným vypuknutím války na Ukrajině. Zdroje poukazují na incidenty již v roce 2014[5], asi nejničivějším je však *NotPetya* z roku 2017[6]. Faktem také je, že Rusko se nikdy neostýchalo využívat kybernetické útoky ve svůj prospěch, přestože bylo mnohokrát varováno. Naopak, jejich používání je často těžkopádné a dalo by se říci i nezodpovědné. Příkladem je útok mířený na olympijské hry v Tokyu[7]. Není proto překvapením zaznamenání hned několika kybernetických útoků před samotným vypuknutím války[8]. Zajímavé jsou ale markantní změny, které nastaly po samotném vypuknutí konfliktu, a jejich vliv na bezpečnost do budoucna. Nejlepším průvodcem těmito změnami může být každoroční report vydávaný organizací ENISA (European Union Agency for Cybersecurity)[2]. Z tohoto reportu jsou snadno rozpoznatelné hlavní trendy, stačí zohlednit celkové rozdělení reportu. Hlavními zájmy jsou *Ransomware, Malware, Sociální Inženýrství, Hrozby pro data, Hrozby pro dostupnost, Dezinformace a Supply-chain útoky*. Samotné hrozby jsou blíže vysvětleny v následujících kapitolách. Důležité je poukázat na trendy útoku na supply-chain a dezinformace. Nelze říci, že tyto útoky v předchozích letech neexistovaly, v porovnání

se současnou situací to tak ale téměř vypadá. Jejich závažnost a také množství rapidně vzrostlo. Není tak divu, že se objevují na listu hlavních hrozeb.

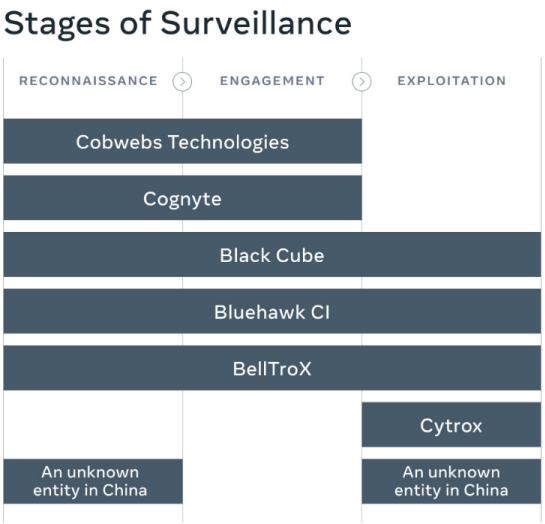
Obrázek 1: Primární hrozby identifikované agenturou ENISA Zdroj: [2]

Pegasus spyware

Speciální zmínku si zaslouží Pegasus spyware a celkově průmysl špehování na zakázku. Za zrodem Pegasus spywaru stojí Izraelská společnost NSO Group. Pegasus je využíván pro špehování, překvapivě jsou však cílovým zákazníkem státní instituce a totalitní režimy. Průmysl špehování na zakázku funguje celosvětově a zaměřuje se stále více na běžné uživatele internetu. Cílem je nejen zisk informací, ale také manipulace cílů za účelem kompromitování jejich zařízení a účtů. Většina zprostředkovatelů těchto služeb tvrdí, že služby jsou určené pro sledování zločinců a teroristů. Tomuto tvrzení však jednoznačně protiřečí výzkum provedený společností ENISA. Více než 30,000 aktivistů za lidská práva, novinářů a právníků po celém světě bylo cílem špehování. V Evropě byl hlášen vysoký počet případů právě se špionážním softwarem Pegasus od NSO. Monitorováni například politici Španělska a vůdci katalánské nezávislosti. Navíc sama skupina NSO uvedla, že pět států EU (Evropská unie) používá jejich špionážní software Pegasus.[2]

Další entity v průmyslu špehování na zakázku

Facebook je jeden ze zdrojů informací, které se používají pro špehování. Meta se snaží tuto činnost zredukovat a tak provedla kroky proti 7 různým entitám operujícím špehování na zakázku. Tyto entity sídlily v Číně, Izraeli, Indii a Severní Makedonii, avšak svoje působení zaměřovaly na lidi ve více než 100 zemích po celém světě. Obrázek 2 ukazuje ovlivněné entity, je zde vidět, na kterých částech řetězce sledovací operace se jednotlivé entity podílely.



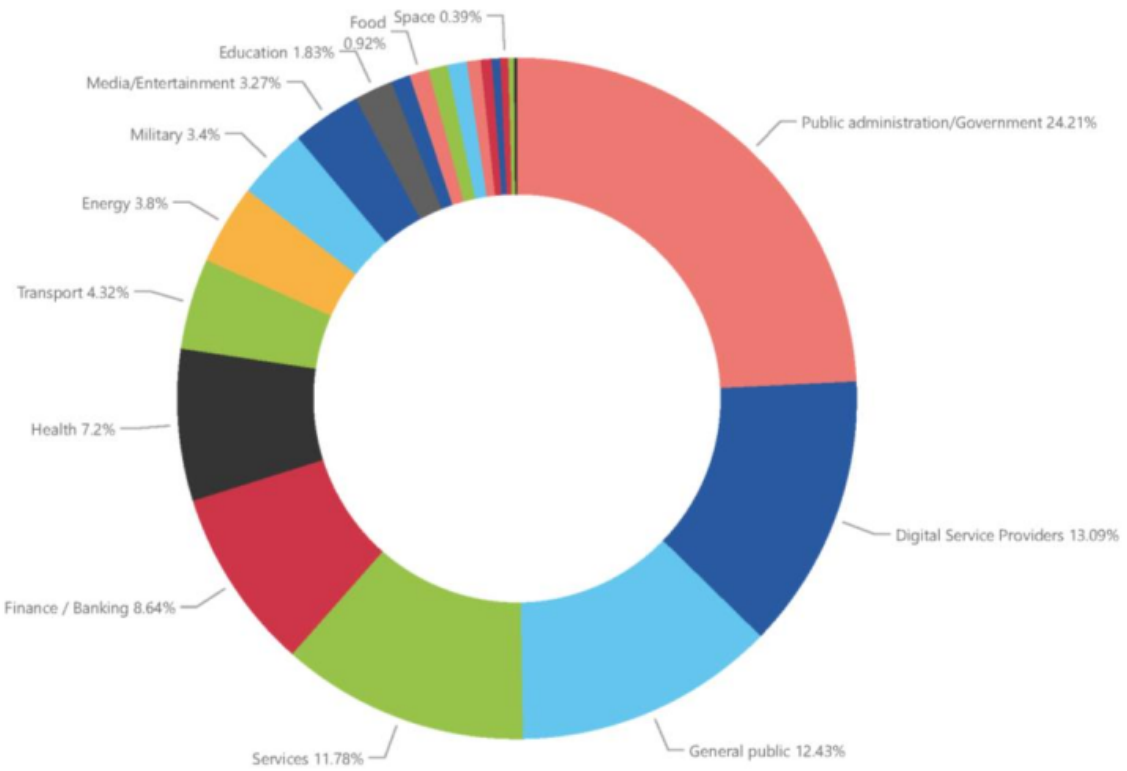
Obrázek 2: Entity identifikované společností Meta Zdroj: [9]

Řetězec se skládá z *průzkumu*, *navázání kontaktu* a *využití*. První fází řetězce sledování, a obvykle nejhůře zaznamenatelnou, je *průzkum* . Cíl sledování je potichu profilován s využitím softwaru k automatickému sběru dat z celého internetu. Informace o cíli pochází ze všech dostupných online zdrojů, a to jak volně přístupných, tak i placených nebo nelegálních. Jsou to data z veřejných webů, jako jsou blogy nebo sociální média, dále data z platforem pro správu znalostí, jako je například Wikipedia. V neposlední řadě jsou data sbírána ze stránek na *dark webu*, kde lze naleznout výpisy z napadených databází. Druhá fáze řetězce je *navázání kontaktu*. Právě zde je největší možnost odhalit sledování a s ním spojený útok, proto je velmi důležitá obezřetnost. Tato část řetězce je zaměřena na navázání kontaktu s cíli nebo lidmi v jejich blízkosti. Primárním cílem je vybudovat s cílem důvěru, získat nebo ověřit informace z předchozího kroku a v neposlední řadě připravit cíl na třetí fázi řetězce. Za tímto účelem jsou zde využívány taktiky sociálního inženýrství. Používají se fiktivní nebo ukradené identity, byli osloveni lidé prostřednictvím e-mailů, telefonních hovorů, textových zpráv nebo zpráv na sociálních médiích. *Využitím* je myšlena manipulace cíle. Tato poslední část řetězce sledování obnáší vytváření phishingových domén, které jsou navržené tak, aby cíle oklamaly. Domény se snaží získat od cíle informace nebo ho přesvědčit k provedení akce,

která není v jeho nejlepším zájmu. Jako cenné informace jsou brány přihlašovací údaje, například k e-mailovému účtu, sociálním médiím, finančním službám nebo do firemní sítě. Za nežádoucí akce se považuje instalace malwaru, specificky spywaru pro další zisk informací nebo ransomwaru pro peněžitý zisk.[9]

Nejvíce napadené odvětví

Z již zmíněného reportu[2] je možné vyčíst, ve kterých odvětvích je zaznamenáno nejvíce útoků. Útoky jsou jen zřídka omezené na jeden sektor, ve většině případů i útok zaměřený na specifický sektor přetéká díky provázanosti do ostatních. Tento pohled na sektory je i přesto důležitý právě kvůli připravenosti jednotlivých sektorů na útoky. Můžeme očekávat, že sektor zabývající se zprostředkováním digitálních služeb bude mít jinak připravenou ochranu než například vládní sektor. A to nejen díky primárnímu zaměření sektoru, ale také dopadu úspěšných útoků v minulosti a předvídanému dopadu budoucích útoků.



Obrázek 3: Nejvíce napadené sektory (v období červenec 2021 – červen 2022) Zdroj: [2]

Na první pohled je z obrázku 3 vidět, že téměř čtvrtina útoků byla zaznamenána ve vládním sektoru. Kolem 13% útoků míří na sektor zprostředkování digitálních služeb a dalších 13 % na širokou veřejnost. Lze očekávat, že množství útoků v těchto sektorech je ovlivněno

snadností propagace útoku a v případě veřejnosti navíc ještě celkovým množstvím možných cílů. Zajímavá je také poznámka v reportu týkající se sektorů bankovnictví a zdravotnictví. V době sledování byly tyto sektory v rámci celé sledované periody napadány konzistentně. Zajímavý, hlavně v kontextu války na Ukrajině, je také armádní sektor, kde je zaznamenáno kolem 3 procent útoků. Tato nízká procentní reprezentace by mohla být způsobena metodologií sestavování tohoto reportu. Útoky byly zaznamenávány pomocí OSINT (Open Source Inteligence), neboli volně dostupných informací[10]. Volně dostupné informace mají mnohá omezení. Je jich velké množství a proto je nutné užitečná data dolovat, nicméně jen málokdy je na první pohled zřejmé, která informace je užitečná. V tomto případě je však hlavním problémem jejich vznik. Informace se nazývají volně dostupné, protože je tvůrce volně zpřístupnil široké veřejnosti. I když společnosti začínají být zodpovědnější v nahlašování útoků, lze stále předpokládat, že některé byly přehlédnuty nebo nenahlášeny. Ve vojenském sektoru bude limitace informací prioritou. Proto bude v kombinaci s propagandou obou stran konfliktu a limitací nežádoucích informací velmi obtížné sestavovat jakoukoli přesnou reprezentaci útoků.

5 Nejčastější kybernetické útoky

Mezi nejčastější útoky dlouhodobě patří *denial-of-service*, *man-in-the-middle*, *malware* a samozřejmě *sociální inženýrství*[1]. Také zaznamenané útoky v roce 2022 jsou v souladu s tímto trendem. Jsou to však velmi obecné kategorie, v nichž se specifika velmi liší. Například pod malware se řadí již zmíněný spyware ale také ransomware, adware, rootkits, etc. Pouze použití ransomwaru v roce 2022 vzrostlo o 41 %, primárně v první polovině roku, a také čas na odhalení a nápravu úspěšného útoku trval o 49 dní déle, než bylo běžné. V kategorii sociální inženýrství je již dlouhodobě nejčastějším útokem phishing. Jeho oblíbenost spočívá v jeho efektivitě a relativně nízkých nákladech na provedení. Počet zaznamenaných útoků téměř každoročně stoupá[10], není tak divu, že jen za první polovinu roku 2022 byl zaznamenán nárůst v četnosti útoků o 48 %. V této době bylo nahlášeno přes 11 tisíc útoků, které stály cíle 12.3 milionů dolarů. Je nutné poznamenat, že statistiky se týkají pouze *zaznamenaných* útoků. Mnoho společností tyto útoky veřejně neoznamuje, nejčastěji z důvodu zachování dobré pověsti. Horší možností může být to, že útok ani nezaznamenali.[11]

Nové cíle

Stále více útoků se zaměřuje na *Supply-chain* a IoT. To ovšem není překvapující, protože už v předchozích letech bylo možné zaznamenat neklid mezi Ruskem a Ukrajinou. Přípravy na ozbrojený konflikt samozřejmě zahrnují útoky na infrastrukturu, a to i v online prostředí. *Supply-chain* je výborným cílem ze dvou důvodů. Úspěšný útok v jedné části řetězce dovoluje šíření po celku a dopad úspěšného útoku je proto významný. Výzkumná zpráva od Accenture[12] odhadla škody způsobené v Eurozóně těmito útoky na 112.7 bilionů euro. Odhad na období 2022/2023 spojený právě s válkou je v nejlepším případě 242 bilionů euro a v nejhorším případě až 920 bilionů. Také útoky na IoT zařízení stoupají. Není tomu však díky zvýšené oblíbenosti u útočníků nebo lepších metodách útoku, zvýšení plyne téměř čistě ze zvyšujícího množství zařízení. IoT zařízení jsou používána všude, najdeme je v domácnostech, firmách, továrnách nebo kasinech. Tato zařízení ulehčují lidský život, bohužel jsou také novým rizikem, protože zabezpečení není při vývoji těchto zařízení priorita. Proto jsou cílem útočníku ať už jako přídavek do botnetu nebo jako slabý článek obrany společnosti. Zní opravdu špatně, když se povede útočníkům ukrást důvěrné informace z kasina pomocí chytrého thermometeru akvária[13]. O vážnosti situace svědčí i veřejná prohlášení o zranitelnostech, která vydávají přímo státy. Například pro monitorovací zařízení vozidel MiCODUS MV720 toto prohlášení vydala americká vláda[14]. A není divu, toto zařízení nejen monitoruje vozidlo, ale je i schopné odpojit přívod paliva. Jelikož je toto zařízení nachází hlavně v armádní a policejní technice, je to opravdu velký problém.[11]

Zdroje nejčastějších útoků

Právě z těchto důvodů je nutné podívat se na nejčastější kategorie útoků. V předchozím

textu byly mnohé zmíněny, následuje jejich rozbor do hloubky. Kategorie byly zvoleny z kombinací několika zdrojů, jako je ENISA[2], Cisco[15] nebo NIST (National Institute of Standards and Technology)[16].

5.1 Malware

Tento termín se používá pro škodlivý software a zahrnuje známé hrozby jako jsou viry, červy, trojské koně, spyware a ransomware. Do systému se dostávají díky nepozornosti uživatele nebo s využitím některé z mnoha zranitelností[15]. Malware je důvod, proč si uživatelé musí dávat pozor, na jaké linky klikají, jaké programy instalují a také odkud programy stahují. Stále častěji malware předstírá, že je legitimní software. Mezi nejznámější napodobované programy patří Skype, Adobe Acrobat, VLC nebo 7zip[17]. Škodlivému softwaru se bohužel nevyhnul ani státní sektor, nicméně není jen jeho cílem, ale také prostředkem k šíření. Zkoumání z roku 2022 ukazuje, že je možné najít desítky instancí hostování škodlivého softwaru přímo v doménách spojených se státními institucemi[18]. Tento problém není specifický pro jeden stát, ale je to celosvětový problém, jak je možné vidět na obrázku 4. Závažnost problému tkví hlavně v přístupu uživatelů. Státní stránky nejsou blokované, naopak k nim existuje implicitní důvěra a tak běžné uživatele ani nenapadne, že musí být obezřetní.

Obrázek 4: Zneužití státní infrastruktury Zdroj: [18]

Obrana a detekce

Obrana proti malwaru je složitá, nelze totiž ukázat na jednu specifickou chybu, kterou je nutné opravit, aby bylo zabráněno opětovnému nakažení. Existují však dobré uživatelské

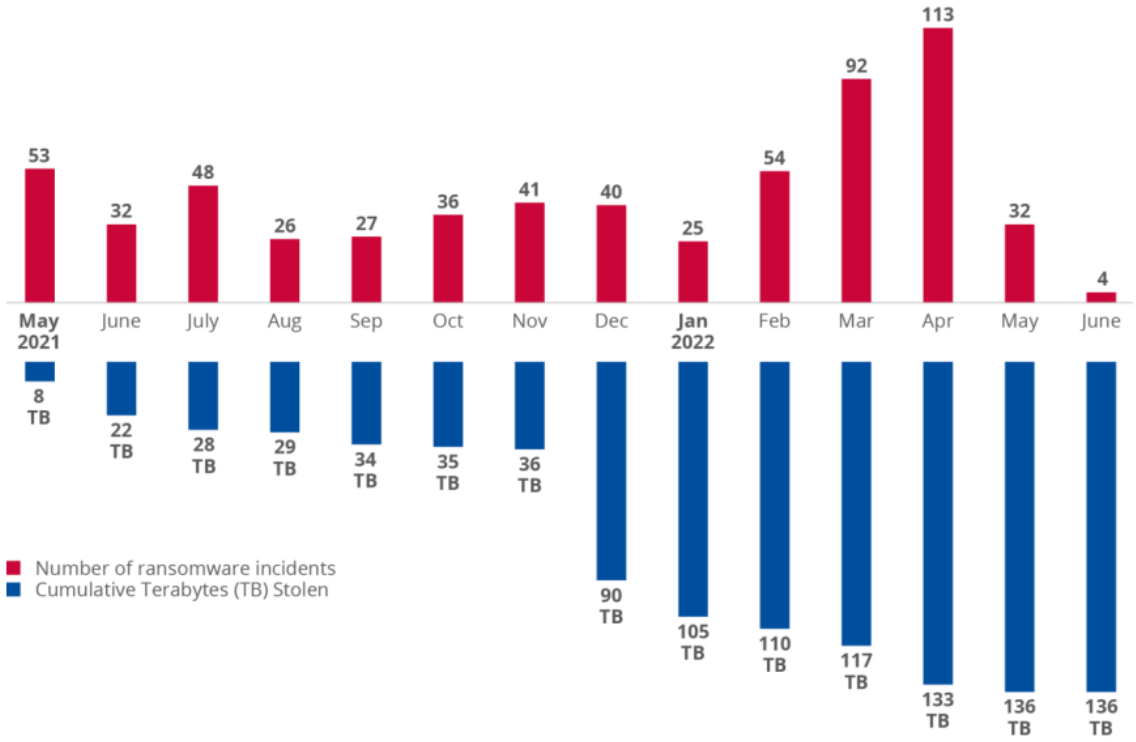
praktiky, které riziko infikování stroje malwarem snižují. Absolutním základem je aktualizování softwaru používaného zařízení. Mnoho velkých firem aktivně sleduje bezpečnostní incidenty spojené s jejich zařízeními a snaží se své uživatele chránit pomocí bezpečnostních aktualizací. Pro detekci malwaru je vhodný antivirus, který je schopný v online databází nalézt nejznámější rysy malwarových kampaní a ty pak detekovat v nainstalovaných souborech. Pokud nastane podezření na malware, je proto dobré pomocí antiviru zkontrolovat soubory. Podezření by mělo nastat při výrazném zpomalení zařízení, nemožnosti vypínat programy, vyskakování reklam nebo cizích pokusech o přihlášení k osobním účtům. Aby se předešlo samotné instalaci malwaru, je nutné dbát na bezpečné chování uživatele, hlavně co se týče procházení internetu, instalace programů a klikání na soubory nebo odkazy v emailech. Jak již bylo zmíněno, malware může být zabalen společně s legitimním softwarem, je proto velmi důležité instalovat programy pouze z ověřených, ideálně oficiálních zdrojů. Pozor na stránky, které napodobují oficiální stránky daného produktu, protože na nich lze malware očekávat s jistotou. Nutné je také dávat pozor na podezřelé odkazy nebo soubory v emailech, to jsou totiž hlavní vektory útoku, přes které se do zařízení může dostat malware. V poslední řadě je nutné zmínit USB (Universal Serial Bus) zařízení. Pokud je to možné, uživatel by neměl nikdy zapojovat ke svému zařízení neznámé USB zařízení. Ty jsou totiž nejen hrozba v podobě přenašeče malwaru ale dokonce i hrozba samotnému zařízení. Příkladem takto nebezpečného zařízení je USBKill[19]. Toto zařízení na testování hardwaru se při napojení do USB portu nabije a pak vypustí svůj náboj zpět do portu. Novější verze jsou dokonce schopné nabití dopředu, což znamená, že jsou schopná útočit na vypnutá zařízení a obchází všechny známé bezpečnostní protokoly.

5.1.1 Ransomware

Za zvláštní zmínku stojí ransomware, jelikož je to velmi nebezpečný a útočníky oblíbený malware. Jedná se o typ útoku, při němž útočníci přebírají kontrolu nad cílovými daty a požadují výkupné výměnou za obnovení dostupnosti těchto dat nebo zachování jejich tajnosti. Útočníci tak přímo ohrožují dostupnost, důvěrnost i integritu dat. Jednoduché ransomwarové útoky data pouze odcizí a vyhrožují vypuštěním, popřípadě uzamknou systém, aby nebylo možné se k datům dostat. Nejčastější jsou však sofistikované ransomwarové útoky, kde jsou data zašifrována a klič nebo program pro jejich odšifrování je oběti poskytnut až po zaplacení výkupného. Ve výjimečných případech se stává, že klíč k odšifrování dat není poskytnut nikdy. Důvodem, proč jsou tyto situace výjimečné, je dlouhodobý pohled ransomwarových skupin na svůj business. Nejen že neposkytování klíčů by vedlo k neplacení výkupného, ale také to snižuje okruh cílů, které mohou v budoucnu napadnout. Zašifrovaná data nemá cenu znovu napadat, nikdo za ně nezaplatí druhé výkupné. Navíc by takové chování mohlo vézt k celkové nechuti společností výkupné platit, protože by neměli jistotu získání dat nazpět. Tyto myšlenkové pochody útočníků nemůžou být překvapením. Z inter-

ních dokumentů a logů skupiny Conti je zřejmé, že alespoň některé ransomwarové skupiny operují jako běžná společnost[20]. Ve skupině byli zaměstnáni manažeři a náboráři, útočníci pracovali převážně během pracovního týdne a dokonce měli nárok na placenou dovolenou a jiné benefity. K rozšíření tohoto typu útoku přispívá také koncept Ransomware as a Service (RaaS), ten dovoluje i nezkušeným útočníkům operovat s velice sofistikovaným softwarem. Naopak zkušení útočníci nemusí ztrácet čas hledáním cílů, ale soustředí se pouze na vyvíjení ransomwarových nástrojů a technickou podporu. Z každého úspěšně provedeného útoku jim totiž náleží část peněz.[2]

Monitorování



Obrázek 5: Počet zaznamenaných Ransomware incidentů a velikost ukradených dat ve sledovaném období květen 2021 až červen 2022 Zdroj: [2]

Jak je vidět z obrázku 5, ransomwarové útoky byly v době sledování, tedy období od května 2021 do června 2022, časté a dopad na data byl značný. Sledování těchto útoků je však velmi obtížné, protože pokud dochází pouze k vydírání, firmy mohou výkupné zaplatit a pokusit se zamlčet existenci útoku. Se stoupajícími částkami výkupného je nicméně tato možnost stále méně validní. Spíše se firmy obrací na pojištění proti ransomwaru, což však ironicky zvyšuje jejich atraktivnost coby cíle, jelikož je zde jisté zaplacení výkupného. Dalším problémem monitorování je abstrakce ze strany útočníka. Pro zmatení vyšetřovatelů

nejsou pro ransomwarové skupiny neobvyklé změny názvu spolu s falešným odchodem do důchodu. Stejná skupina pak pod jiným názvem operuje nadále, může však pozměnit styl provádění útoků nebo používané nástroje. Díky rivalitě mezi skupinami často dochází ke krádežím zdrojových kódů, což zase znesnadňuje identifikování vztahu s původní skupinou. Častým vodítkem bývají adresy krypto peněženek, protože výplaty výkupného jsou vždy v kryptoměně, například v Bitcoinu. To samozřejmě také ztěžuje vystopování a trestní stíhání pachatelů. Bez nadsázky lze říci, že monitorování ransomwarových skupin je složitější než obrana proti jejich útokům.[2]

Změny v metodice

Ze zaznamenaných dat jasně vyplývá pokles útoků s počátečním vektorem prostřednictvím RDP (Remote Desktop Protocol), neboli protokolem vzdálené plochy. Stále je to však druhý nejpoužívanější vektor útoku pro ransomware. Útočníci stále prolamují slabá RDP přihlašovací jména a hesla, zejména pokud není povolena MFA (Multifactor Authentication), v překladu vícefaktorová autentizace. MFA je velmi dobrou obranou proti neznalým útočníkům a jednodušším útokům, bohužel není nepřekonatelná. Nejpoužívanějším vektorem útoku je samozřejmě phishing. Za povšimnutí stojí nízké náklady na využití těchto metod útoku a jejich značný výnos, což je jeden z hlavních důvodů jejich oblíbenosti mezi útočníky. Zajímavým trendem jsou změny ve způsobu vydírání společností – klasický ransomwarový útok nejdříve sbírá informace, poté k nim zamezí přístup a posléze vydírá společnost. Teprve pokud společnost odmítne zaplatit výkupné je útok veřejně oznámen. Získaná data jsou také prodávána nebo volně dostupná na internetových fórech *dark webu*. Některé ransomwarové skupiny však začaly používat jiný postup. Oběti je nabídnuto, aby si data *koupila* dříve, než je zakoupí její konkurenti. Útočníci také již po provedení útoku změnili vzhled webových stránek oběti, aby na útok upozornili. Takto prováděný útok vede k veřejnému hanobení oběti a má přímý vliv na vztahy s veřejností a reputaci společnosti. Dalším znepokojivým trendem je vytváření dedikovaných stránek s daty o napadených přímo na veřejném internetu. Tento postup zvolil *ALPHV*, také známý jako *BlackCat* ransomware, který operuje jako RaaS[21]. Na tomto webu se nacházely informace o zákaznících i zaměstnancích a ti si tak mohli snadno zkontrolovat, zda byli útokem zasaženi. Vytvoření takto veřejného repozitáře se stalo novým způsobem, jak donutit třetí strany, aby se identifikovaly. Lze předpokládat, že postižení zákazníci sami kontaktují majitele webu, aby zaplatili za stažení dat.

5.1.2 Spyware

Specifický malware, jehož primárním cílem je shromažďování dat, se nazývá spyware. Při infikování zařízení sbírá osobní a citlivé informace nejen o uživateli, ale i o samotném zařízení a získané informace spyware posílá nazpět svému tvůrci. Všechny tyto činnosti samozřejmě

provádí spyware bez souhlasu a znalosti uživatele. Infikování je stejné jako u většiny malwaru – spyware je nevědomky nainstalován uživatelem. Oblíbenou metodou je přibalení spywaru k jinému programu nebo přes podvodné odkazy a soubory, které spouští instalační skripty. Data, na která se útočníci zaměřují, jsou převážně přihlašovací údaje, údaje o bankovních účtech a kreditních kartách nebo také chování na internetu. Všechna tato data lze totiž prodat na černém trhu nebo rovnou využít k další nelegální činnosti. Spyware je jedním z nejčastěji používaných způsobů kybernetických útoků. Jeho oblíbenost spočívá v obtížnosti odhalení a při štěstí ve velkém výnosu.[22, 23]

Typy

Všechny typy spywaru monitorují uživatelskou aktivitu, rozlišujeme je na další typy podle toho, k čemu takto získaná data využívají a jak data získávají. Některé spywary pořizují snímky obrazovky, jiné pouze monitorují běžící programy nebo jen vstup z klávesnice. Vzácně je tento software dokonce schopen zapínat kameru či mikrofon a z nich nahrávat záznamy. Dalším možným bodem odlišení jednotlivých typů jsou jejich dodatečné vlastnosti. Některé typy spywaru mají schopnost instalovat další software, což umožňuje útočníkovi rozšířit své kompetence na zařízení, ať už se jedná o pokročilejší sběr dat, manipulaci dat nebo změny nastavení přímo na daném zařízení. Mezi nejpoužívanější typy patří[22, 23]:

- Adware,
- Keylogger,
- Infostealer,
- Red Shell spyware,
- Cookies,
- Rootkit.

Adware

Cílem adwaru je automatické zobrazování reklam bud přímo v prohlížeči nebo přímo v operačním systému zařízení. V kontextu malwaru se jedná o tajně nainstalovaný software bez souhlasu uživatele. Problémem je časté využívání k zobrazování invazivních nebo klamavých reklam.[22]

Keylogger

Keyloggery jsou specifické programy pro zaznamenávání stisknutí kláves uživatelem, kde po zaznamenání získané informace ukládá v plaintextové nebo zašifrované formě. Pokud keylogger funguje samostatně, tak tyto data také zasílá útočníkovi, častější je však použití keyloggeru spolu s dalším spyware. Primárním cílem útočníka jsou běžně zadávané věci,

které jsou v softwarem chráněny. Jedná se například o přístupové údaje, soukromé zprávy a emaily.[22]

Infostealer

Infostealer, asi neklasičtější představa spywaru, je útočníky využíván pro shromažďování informací z napadeného zařízení. Již zmíněné keyloggery je možné uvažovat jako podtřídu tohoto spywaru. Jiné infostealery jsou například schopné prohledávat data na zařízení pro určité informace, určité soubory nebo typy souborů. Častým cílem jsou přístupové údaje, emaily, zápisy z komunikačních aplikací nebo internetová historie. Hlavní rozdíly mezi infostealery jsou však ve způsobu operace. Některé infostealery existují na zařízení až do jejich objevení nebo zničení zařízení. Stále zasílají útočníkovi informace, což bývá primárním důvodem jejich objevení. Zákeřnější typy jsou schopné najít a exfiltrovat všechna žádaná data najednou a posléze vymazat nejen sama sebe, ale také se pokusit po sobě odstranit všechny stopy. Pokud nejsou detekovány při tomto jednom přenosu, není pak možnost pro uživatele poznat, že byl napaden.[22]

Red Shell spyware

Specializovaný spyware na sledování online aktivity hráčů, který je nainstalován právě s danou hrou. Jeho cílem je sbírat data spojená s danou hrou, která zasílá vývojáři. Původní záměr tvůrců je využít takto získaná data pro vývoj lepších her a pomáhat společnostem dělat lepší marketingová rozhodnutí. Hlavním problémem je však instalace tohoto softwaru bez vědomí uživatelů a jejich výslovného souhlasu.[22]

Cookies

Cookies původně vznikly jako užitečná pomůcka, například pro přihlášení do oblíbených webových stránek uživatele nebo zachování instance v e-shopu. Jsou také využívány pro zobrazování reklam spojených se zájmem uživatele, kterého sledují. Jak již bylo naznačeno, problém je ve sledování online chování uživatele na internetu. To cookies plně kvalifikuje jako spyware, který sleduje nejen historii prohlížení, ale zaznamenává i pokusy o přihlášení. Útočník s dostatečnými znalostmi a vybavením je tak schopen zpětně obnovit přihlášenou instanci. Není proto divu, že o cookies se již delší dobu zajímá legislativa a hlavní internetové prohlížeče jejich činnost již v základu omezují nebo dokonce kompletně zakazují.[22]

Rootkit

Možná nejnebezpečnějším typem spyware je Rootkit, jenž umožňuje útočníkovi infiltrovat zařízení a získat přístup na velmi hluboké úrovni. Rootkit je proto velmi obtížné odhalit. Díky hlubokému přístupu má útočník značnou kontrolu nad zařízením, kterou většinou využije k instalaci a skrytí dalšího malwaru. Při prvotním nakažení využívá rootkit pro získání přístupu nejčastěji bezpečnostní zranitelnosti v samotném systému zařízení nebo

administrátorské přístupy. Jeho prvotní kroky jsou však detekovatelné dobrým antivirovým softwarem.[22]

Dopad

Jedním z nejčastějších problémů způsobených spywarem je krádež dat. Všechna data mají pro útočníky cenu, některá jsou však vyhledávaná více nežli jiná. Útočník se například může snažit sestavit falešnou identitu, kterou pak sám použije k další trestné činnosti nebo ji prodá na černém trhu. Také přístupové údaje k účtům mohou být cenná data, vzácné účty se na černém trhu prodávají i za stovky dolarů. Dalším příkladem cenných dat jsou přístupová práva, která může útočník použít k většímu kybernetickému útoku. Vedlejším efektem spywaru jsou problémy s přístupem k internetu nebo problémy na interní síti, které vznikají právě kvůli zasílání získaných dat tvůrci spywaru. Dalším ukazatelem je zpomalení zařízení, jelikož v závislosti na sofistikovanosti spywaru běžícího na pozadí bude zařízení ovlivněno. V horších případech může spyware zařízení dokonce nevratně poškodit. To se stává, pokud je spyware špatně navržen nebo nezáleží na dlouhodobém sledování, ale jde pouze o krátkodobou extrakci dat.[22, 23]

Pegasus spyware

Jak již bylo zmíněno, spyware je také používán pro špehování na zakázku. Již zmíněný Pegasus spyware spadá právě do této kategorie a je to výborný příklad. Také více jak 30,000 aktivistů za lidská práva, novinářů a právníků po celém světě bylo cílem špehování. Jeho použití ve státech EU potvrdil i samotný tvůrce NSO. Pegasus je velmi sofistikovaný spyware, o jeho schopnostech svědčí fakt, že společnost NSO musí získat povolení od izraelského ministerstva obrany předtím, než může být nástroj licencován pro jakéhokoli klienta. V minulosti u něj výzkumníci pozorovali použití hned několika *zero-day* zranitelností zřetězených za sebou k získání kontroly nad celým zařízením. Pegasus poté zapnul mikrofon, kameru, četl zprávy, poslouchal hovory a sledoval polohu zařízení. Všechna tato data posléze zasílal na NSO servery, kde k nim měli přístup zadavatelé špehování. Při pohledu na oznámené případy používání Pegasus spywaru se často objevuje velmi nepříjemný společný motiv. Proti cílené oběti dochází znepokojivě často k nějaké fyzické akci. Existují případy, které vedly k uvěznění, fyzickým hrozbám, útokům a zastrašování. Nejhorším případem je však vražda. Jamal Khashoggi byl novinář ze Saúdské Arábie a původně blízký přítel královské rodiny. Po jmenování Mohameda bin Salmána korunním princem byl však nucen uprchnout ze země, začal proto velmi otevřeně mluvit o represi v Saúdské Arábii. V říjnu 2018 byl v Turecku nalákán do budovy saúdského konzulátu kvůli zřízení dokumentů pro bezpečný návrat do Saúdské Arábie. Z budovy však nikdy nevyšel, byl uškrcen a rozčtvrcen. Zkoumání odhalilo, že NSO nainstalovalo Pegasus na telefon jeho manželky Hanan Elatr jen několik měsíců před jeho smrtí[24]. Mezi potencionálními cíli instalace Pegasus spyware bylo nalezeno taká číslo telefonu jeho snoubenky, lze předpokládat, že cílem sledování byl i

sám Jamal Khashoggi. Při zohlednění těchto skutečností je použití Pegasus spyware zcela neetické.[25, 2]

5.2 Sociální inženýrství

Sociálního inženýrství je možné definovat takto: Jedná so o útok, kdy se útočník snaží přimět cíl útoku, aby provedl akce, které nejsou v jeho nejlepším zájmu[10]. Příkladem akcí může být instalace malwaru, vydání informací nebo třeba jen povolení vstupu do budovy nebo areálu. V době psaní tohoto textu je sociální inženýrství jedním z nejpoužívanějších útoků. Zaměření tohoto útoku na lidský faktor znamená, že obrana je často obtížně proveditelná. Rutinně tomuto typu útoku propadají specialisté na bezpečnost nebo bezpečnostní výzkumníci. Za efektivitou tohoto útoku stojí využívání faktů z psychologie, sociologie a studia interakce lidí s technologiemi. Výsledkem je používaní stejných manipulačních technik, které lze pozorovat v mnoha dalších odvětvích, jako je například marketing. Využívá nejen legitimní chyby lidského myšlení, jako například bias, ale také lidské zvyky a charakter. Například otevírání dveří člověku, který nese těžké věci. To je pro většinu lidí slušnost, avšak i to je jeden ze způsobů, jak může útočník překonat ochranu budovy. Dveře zabezpečené čtečkou karet nejsou překážkou, pokud vám je legitimní pracovník pomůže otevřít. Velká část sociálního inženýrství je postavena na představení věrohodné záminky. To je možné zaznamenat v mnoha podobách, ať už se jedná o podvodný e-mail, v němž útočník předstírá, že je vaší bankou, nebo podvodný telefonát, kde útočník přesvědčí nápomocného operátora, aby mu pomohl převést *ztracené* číslo na novou Subscriber Identity Module (SIM) kartu. V zámince však spočívá také nejlepší obrana, jelikož malé detaily jsou to, co nejčastěji odhalí útok sociálního inženýrství. V již zmíněném emailu od banky je v adrese například **M0NETA(s nulou místo velkého O)** nebo při hovoru s operátorem není daný člověk schopen odpovědět na základní otázky, které se například týkají místa nebo roku narození. S tím však souvisí další další bod ochrany, omezení veřejně dostupných informací. O naprosto každém člověku existují veřejně dostupné informace, rozhoduje však to, jak těžké je tyto informace získat. Jedním z nejhorších provinění jsou veřejné profily na sociálních sítích, dvojnásob pokud daná osoba vykazuje špatnou komunikační hygienu. Pokud na Twitter cíl napíše, že jeho banka stojí za nic a zmíní přesné jméno banky, útočník ví, které jméno banky má použít a nemusí posílat emaily náhodně. Pokud na veřejném Facebookovém profilu má cíl zadané datum narození, zná ho automaticky i útočník. V nepříjemném místě proto stojí pracovní sociální sítě jako LinkedIn, kde kvůli pracovním příležitostem je žádoucí zadávat mnoho identifikačních údajů, je však možné, že je zneužije útočník.[10]

Trendy

Report od společnosti ENISA poukazuje na fakt, že ve zhruba 82 % závažných bezpečnostních incidentů figuruje lidský faktor a minimálně 60 % incidentů v Evropě, na Středním

východě a v Africe zahrnuje využití sociálního inženýrství. Takto velká čísla spočívá v oblíbenosti tohoto typu útoků. Výhod pro útočníka je totiž mnoho. V rámci většiny typů útoků není útočník ovlivněn lokací, jeho počáteční náklady bývají minimální, a přesto je výnosnost těchto útoků značná. Navíc ačkoli jsou prováděny kurzy a semináře na zvýšení povědomí o těchto útocích, jejich účinnost bývá smíšená. Také skupiny provádějící ransomware se silně spoléhají na prvotní přístup pomocí sociálního inženýrství. Nemůže proto být divu, že už jen samotný přístup je prodejný a jsou útočníci, kteří se na něj specializují a další kroky operací nechávají na jiných skupinách. Velmi často napadanými cíli jsou finanční instituce, které útočníci velmi rádi napodobují. Útoky jsou ve formě platebních podvodů, jejichž počet i sofistikovanost rok od roku narůstá. Dalšími často napadanými sektory jsou zdravotnický nebo technologický sektor. Není proto divu, že náklady spojené specificky s phishingem byly v roce 2021 v porovnání s rokem 2015 více než trojnásobné. Časově i peněžně nejnáročnější jsou úkony spojené s vyčištěním, opravou a forenzní analýzou napadených systémů. V poslední době byly také zaznamenány dlouhodobé podvody zaměřené na kybernetickou špionáž, převážně íránskými skupinami. Útočníci se vydávají například za vědce, kteří zvou své kolegy a novináře na falešnou konferenci. Pozvánky na tuto konferenci vedly na webové stránky zaměřené na krádež přihlašovacích údajů. Dalším možným příkladem je vydávání se za atraktivní ženu na sociálních médiích. Cílem je buďto z cílů postupně extrahovat informace nebo po dlouhodobějším kontaktu a získání důvěry zaslat škodlivé dokumenty, po jejichž otevření je kompromitováno zařízení oběti útoku. Bohužel tyto kampaně bývají velmi úspěšné, a tak je téměř jisté jejich využití i v budoucnu.[2]

Typy útoků

Je možné rozlišovat několik hlavních kategorií sociálního inženýrství. Je jasné, že kategorie jsou různě rozsáhlé a obsahují vlastní pod-kategorie, pro pochopení je však vhodné jednodušší roztřídění. Hlavní kategorie jsou představeny v tomto seznamu[2, 10]:

- Phishing – podvodné e-maily,
- Vishing – podvodné telefonáty,
- SMSing – podvodné Short Message Service (SMS),
- Personální útok – útočník osobně napadá lokaci.

5.2.1 Phishing

Phishing jsou podvodné e-maily, kde největší roli hraje zvolená záminka. Nejčastěji je cílem nasměrovat cíl na podvodné stránky pro krádež nebo ověření informací, druhým nejčastějším cílem je získat prvotní přístup do uzavřeného systému. Zajímavé informace pro útočníka jsou například přihlašovací údaje, které se pokusí zjistit vytvořením kopie přihlašovací

stránky banky a na tuto stránku zašle cíli emailem odkaz. V získání přístupu naopak často figurují infikované soubory. Phishing existuje v mnoha podobách. Velmi známé jsou emaily typu *Nigerijský princ*, které fungují na zasílání velkého počtu emailů a přirozené filtraci v podobě odpovědí. Genius tohoto útoku je v tom, že na emaily s takto jasným podvodem budou odpovídat pouze lidé, kteří jsou náchylní k podlehnutí danému podvodu. Hlavní nebezpečí phishingu však tkví ve specializovaných útocích, zaměřených na jednu určitou osobu. Útočník stráví týdny nebo i měsíce zjišťováním informací o cílené osobě a poté vytváří jeden specifický útok, který je v drtivé většině případů úspěšný. Tato podkategorie má název *spear-phishing*. Ještě specializovanější podkategorií je *whaling*, kdy je útok zaměřen na jednu vysoce postavenou osobu ve společnosti, jako je například vedoucí oddělení nebo prezident organizace. Velmi znepokojující je každoroční nárůst počtu těchto útoků.[10]

PhaaS

Jedním z důvodů zvýšení sofistikovanosti útoků a jejich rozšíření je PhaaS (Phishing as a Service) Útočníci stále častěji využívají již připravené materiály nabízené phishingovými sadami místo tvorby vlastních. Využití těchto sad mívá jen krátkou životnost, většina dokonce není využívána déle jak jeden den. Výhodou však bývají perfektní lokalizace pro útok a základní informace pro tvorbu obsahu nerozeznatelného od legitimního. Dříve bylo možné poznat phishingový email pomocí špatné gramatiky, dnes už tomu tak není. Zajímavým úskalím je však šance podvodu. Některé sady obsahují *dodatečnou* funkcionalitu, která například odesílá získané přihlašovací údaje nejen útočníkům ale i vlastníkům phishingové sady. To pro oběti útoku znamená, že odcizené informace se šíří rychleji a nikdo nad nimi nemá úplnou kontrolu.[2]

5.2.2 Vishing

Forma sociálního inženýrství zaměřená na podvodné telefonáty se nazývá vishing. Hlavní rozdíl oproti již představenému phishingu je silná zpětná vazba, kterou má útočník k dispozici během hovoru. Vishing tak klade mnohem větší důraz na improvizaci a komunikační schopnosti útočníka. Útok, který nebyl tak dobře připraven, je možné zachránit dobrým využitím nově získaných informací. Je to také mnohem rychlejší a interaktivnější forma sociálního inženýrství. Při zaslání phishingového e-mailu můžeme čekat dny nebo i týdny na zjištění úspěšnosti útoku, při vishingu je to otázka minut. Všechny okolnosti však nejsou jen ve prospěch útočníka. Rychlost a komunikace také znamená, že náhodná interakce může zkazit výborně připravený útok. Je jasné, že v komunikaci po telefonu nelze poslat škodlivý link. Proto je primárním cílem útočníka zisk nebo ověření informací. Jako nový trend se ukazují podvody s bankovními účty, kdy útočník přesvědčí oběť, aby převedla peníze na *bezpečný* účet. Princip je snadný, útočník se vydává za policistu nebo zaměstnance finanční instituce a obeznámí oběť o faktu, že jejich běžný účet je napaden a mohli by tak o své

peníze přijít. *Bezpečný* účet je však pod kontrolou útočníka, a tak jedním převodem některé oběti za pár minut ztratili celoživotní úspory. Report společnosti ENISA jasně ukazuje, že ve sledovaném období (1. čtvrtletí 2021 až 1. čtvrtletí 2022) se počet případů vishingu zvýšil o více jak 550 %. Je nepochybné, že tento trend bude nadále pokračovat díky vzrůstající oblíbenosti u útočníků.[2, 10]

5.2.3 SMShing

SMShing je verze sociálního inženýrství prováděná přes SMS zprávy. Forma je velmi podobná phishingu, liší se však v přístupu lidí k SMS. Příchozí email oběť vyřizuje v prostředí, kde má čas se mu věnovat a dávat si pozor na podezřelé detaily. SMS je však vyřizována většinou hned při jejím příchodu, obzvláště pokud vypadá jako krize. Příkladem může být kampaň FluBot, jejímž cílem jsou Android zařízení. Oběť nejprve obdrží SMS zprávu, která se vydává za doručovatelské společnosti nebo falešný software. Cílem zprávy je přimět uživatele, aby nainstaloval podvodnou aplikaci a dodal jí oprávnění. Podvodná aplikace je pak schopna monitorovat seznam kontaktů, uložená nebo zadávaná čísla kreditních karet, přihlašovací údaje do internetového bankovnictví nebo zachytává SMS a v nich přicházející jednorázová hesla. FluBot se navíc sám šíří z napadeného zařízení právě zasíláním zpráv na záznamy v seznamu kontaktů.[2, 10]

5.2.4 Personální útok

Personální útoky jsou speciální kategorií útoků sociálního inženýrství, kdy se útočník snaží fyzicky dostat k citlivým datům společnosti. Tento typ útoku je v porovnání s ostatními velmi vzácný, většinou se jedná o předem domluvené testovací akce. Důvod, proč tento útok stojí za zmínku, je jeho efektivnost. V dnešní době jsou servery velmi dobře chráněné proti přístupu z internetu, co když ale někdo přijde a zapojí do něj USB flash disk? Je jasné, že tento typ útoku je pro útočníka velmi nebezpečný a náročný, vyžaduje schopnosti, které nejsou standardní, a dokonce i specializované nástroje. Jejich efektivitu však nelze popřít a jsou mnohdy opomíjeny jako možný vektor útoku.[10]

5.3 Threat against data

Tato sekce se zabývá útoky, které primárně ohrožují integritu a bezpečí dat. Každá společnost v dnešní době vytváří, shromažďuje a zpracovává ohromné množství dat. To vedlo k rozvoji správy a analýzy dat, kde lepší techniky a postupy vedou k rychlejším procesům, lepšímu řízení zákaznických vztahů a nižším provozním nákladům. Nemalá závislost také existuje mezi modely strojového učení nebo umělé inteligence, které jsou přímo závislé na správných vstupních datech. Je proto dobré uvědomovat si hrozby, které cílí na zdroje dat s cílem získat k nim neoprávněný přístup. Poté můžeme rozlišovat dva hlavní cíle, které vysvětlují chování útočníků při zisku přístupu k datům. Prvním cílem jsou úniky a krádeže

dat, kdy dochází ke zveřejnění nebo ztrátě citlivých informací. Do této kategorie spadá průmyslová špionáž ale také ransomwarové útoky. Druhým je manipulace, aby se zasáhlo do chování systému závislého na datech. Příkladem je šíření dezinformace nebo takzvané *otravování dat**[Data poisoning]***, kde účelná manipulace dat znehodnotí výsledky umělé inteligence nebo strojového učení. Je dobré připomenout, že do této sekce spadají i chybné modifikace dat a neúmyslné úniky informací. To je právě rozlišení mezi porušením bezpečnosti dat (vždy útok) a únikem dat (neúmyslná chyba). Samozřejmě je v mnoha případech těžké nastavit přesnou hranici. Příkladem může být chybná konfigurace bezpečnosti serveru, která vedla ke krádeži dat útočníkem. Z reportu od společnosti ENISA je vidět, že zhruba 80 % útoků s cílem kompromitovat data pochází z vnějšku cílové organizace, zatímco zhruba 20 % vzniká přímo uvnitř organizace. Motivací pro tyto útoky je stále převážně finanční zisk (asi 90 % útoků) a špionáž (méně než 10 %).[2]

5.3.1 Krádež identity

V důsledku nárůstu úniků dat jsou osobní a citlivá data snadno dostupná útočníkům na *dark webu*. Nemůže tak být překvapením kaskádový efekt, který tato skutečnost měla na krádeže identity. Krádež identity znamená, že útočníci používají odcizená osobní údaje k tomu, aby se vydávali za uživatele, nejčastěji s cílem provedení bankovního podvodu. Za zmínku stojí skutečnost, že více jak polovina útoků zaměřených na supply-chain v roce 2021 měla jako koncový cíl právě osobní údaje o uživatelích.

5.3.2 Otravování dat [Data poisoning]

Důvěryhodná data jsou nejdůležitějším předpokladem pro implementaci bezpečných autonomních a adaptivních systémů. Možná nejvíce zasaženými kategoriemi jsou tvorba umělé inteligence a strojové učení. I malá chyba v prvotních učících datech má velkou šanci absolutně zničit celý systém. S možnostmi zpracování dat však narůstá také možnost data cíleně měnit. Dříve byl televizní přenos nebo video téměř nepopíratelný důkaz událostí, dnes pomocí deepfake možné vytvořit cokoli. V době psaní tohoto textu jsou například velmi oblíbená deepfake videa prezidentů USA, kteří v nich hrají počítačové hry. To se nikdy nestalo, proto je použití deepfake očividné a vtipné. Co když ale útočník použije deepfake hlasového hovoru pro podvodný bankovní převod ve výši téměř 35 milionů? Je nutné se připravit na budoucnost, kde je stále obtížnější rozpoznat fikci od skutečnosti.[2]

5.3.3 SQL injection

Možná nejznámějším příkladem lidské chyby je útok SQL (Structured Query Language) injection. Tento známý útok využívá špatného nastavení databáze pro provádění za normálních okolností nepovolených operací. Pokud útočník nalezne špatně zabezpečený vstup, například vyhledávací box, může do databáze zadávat vlastní příkazy. To je možné pomocí

řetězení příkazů, kdy útočník vytvoří specifický řetězec, který mu dovolí vyvolat nejen očekávané chování ale i další chování, které je na původní chování přidané. Nejčastěji takto útočník získává výpis celé databáze.[15]

5.4 Threat against availability

Útoky ohrožující dostupnost dat a systémů jsou používané již více jak 20 let a stále hrají významnou roli v repertoáru útočníků. Je samozřejmé, že přesné postupy byly během let vyvíjeny, ale základní myšlenka je stále stejná, zajistit, aby uživatelé nemohli získat přístup k datům nebo službám. Tohp může být dosaženo vyčerpáním služby a jejích zdrojů nebo zahlcením komponenty síťové infrastruktury. Zajímavé je, že tento typ útoku lze provést i nechtěně. Když známá osoba například náhodně zmíní malý internetový obchod, velké množství fanoušků může svým přístupem vyřadit webové stránky obchodu z provozu, není to však zcela běžné. Ve většině příkladů je tento typ útoku využíván cíleně a s drtivou efektivitou. Dokonce se o těchto typech útoků mluví jako o pátém rozměru války, po bojích ve vzduchu, na moři, na souši a dokonce i ve vesmíru. Většinou se jedná o útoky typu DoS (Denial-of-Service), DDoS (Distributed Denial-of-Service) nebo RDoS (Ransomware Denial-of-Service). Znepokojivá je současná situace právě ve spojení s válkou na Ukrajině. Hrozby a úrovně vydírání se celkově zvýšily a bohužel stále více útoků je vedeno státem podporovanými skupinami. Nepříjemné je také zaměření útočníků na IoT, kde mají senzory a zařízení často nedostatečnou ochranu. Atraktivní jsou tyto cíle pro zisk informací nebo jako část botnetu. Jednou z příčin slabého zabezpečení jsou velmi často slabé přihlašovací údaje, například **admin** (uživatelské jméno) a **1234** (heslo), které uživatelé využívají. Také aktualizace jsou mnohdy problém, například botnet Mozi stále k šíření využívá zranitelností objevených před osmi lety a je odhadováno, že úspěšně napadl až stovky tisíc zařízení.[2]

5.4.1 Denial of service

Denial-of-service, také znám jako DoS, je útok zaměřený na kolaps infrastruktury tím. Útok se snaží vyčerpat zdroje služby množstvím zasílaných požadavků nebo získat přístup k ovládnutí služby a vyřadit ji tak z provozu. Přístup k ovládání dané služby je prováděn s využitím známe zranitelnosti nebo ziskem přístupových údajů administrátora.[15]

5.4.2 Distributed denial of service

Známější a více používaná je však podkategorie tohoto útoku zvaná DDoS. Hlavní změnou je využívání mnoha zařízení, takzvaného *Botnetu*, která na příkaz zahltí službu množstvím požadavků. Problematika tohoto útoku spočívá v 2 hlavních bodech. Při útoku DoS je možné příchozí požadavky z jednoho zařízení snadno zablokovat pomocí *blacklistu* daného zařízení, není to však proveditelné, pokud tyto požadavky přichází z tisíců nebo i statisíců zařízení. S tím souvisí i druhý problém -rozsah celého útoku. Jedno zařízení může jen

těžce konkurovat statisícím v množství požadavků, které je schopné odeslat. A to i za předpokladu, že je mnohem výkonnější. Proto jsou do *botnetů* často přidávána jakákoli možná zařízení s přístupem k internetu, jako smart televize, pračky, ledničky nebo i kamery a jiné typy IoT zařízení.[15]

5.4.3 Ransomware denial of service

Jako nová forma útoků se objevilo RDoS. Jedná se o útok DoS nebo i DDoS, kde však primárním cílem není vyřazení služby z provozu. Výpadek provozu je však efektivní prostředek pro získání pravé motivace – peněz. Stejně jako jiné již zmíněné formy ransomwaru, i RDoS existuje ve dvou hlavních podobách v závislosti na tom, zda nejdříve nastane útok, nebo výhružka. První možnost je, že nejdříve nastane útok. Po jeho pozastavení je poslána výhružka, v níž je požadováno výkupné, jinak útok znovu začne. Druhou možností je zaslání výhružky rovnou a pouze při nezaplacení nebo nutnosti prokázání možností útočníka je proveden skutečný útok. Začíná zde s cílem útoku psychologická hra, protože útočník mnohdy nemá možnosti pro silný a dlouhodobý útok, to však cíl při rozhodování, zda zaplatí výkupné, neví. RDoS často cílí na poskytovatele internetových služeb, finanční instituce a malé až střední podniky. Možná nejpřekvapivější je návrat plateb za *ochranu*, tedy každodenních plateb, například v hodnotě 1 BTC denně, za nenapadnutí společnosti.[2]

5.5 Ostatní útoky

Tato kategorie se skládá z útoků, hrozeb a technik, které nelze zařadit samostatně do jedné kategorie. Často jsou však využívány v kombinaci s jinými kategoriemi útoků pro dosažení lepších výsledků. Je nutné je v tomto výčtu zmínit kvůli jejich nebezpečnosti, rozšířenosti a nízkému veřejnému povědomí.

5.5.1 Man-in-the-middle

Při útoku *Man-in-the-middle*,také zvaném odposlouchávací útoky, se útočník dostává doprostřed komunikace dvou subjektů. Hlavním cílem je filtrování, kradení a nahrazování dat proudících v komunikaci. Mezi nejčastější implementace tohoto útoku patří napodobování veřejné *Wi-Fi*. Útočník se představuje jako vstupní bod na tuto veřejnou Wi-Fi, kam posléze odesílá veškerou komunikaci. Lidé si tak nemusí uvědomit, že útočník existuje, a nedávají si tak pozor na svoji činnost na takto odposlouchávané síti. Další oblíbenou implementací útoku je použití malwaru. Ten po nainstalování přesměrovává komunikaci nebo pouze odposlouchává činnost na daném stroji. Zajímavým trendem poslední doby je použití QR kódů. V lednu 2022 dokonce FBI vydalo varování ohledně zločinců, kteří používají QR kódy k přesměrování obětí na podvodné weby a kradou tak přihlašovací informace. Není to však jen otázka USA, podobné metodologie útoků využívali i útočníci v Německu. QR kódy jsou pro útočníky výhodné, protože člověk není schopen rozeznat pravdivý od škodlivého. Pokud

tedy útočník zamíchá mezi legitimní kódy své podvodné, je pro běžného člověka nemožné je odhalit.[2, 15]

5.5.2 Zero day exploit

Zero day exploit je zranitelnost systému, na niž ještě neexistuje patch. Tato situace může nastat, pokud byla zranitelnost nahlášena a výrobce systému ji ještě nestihl opravit. Mnohem častější je případ, kdy zranitelnost našel sám útočník. Ten ji ale bude chtít využít, rozhodně ne nahlásit. Tyto zranitelnosti se také snaží získat státní složky zaměřené na špehování. Nemůže tak být divu, že s těmito zranitelnostmi existuje černý trh[26], na němž se prodávají až za miliony dolarů. Ani výzkum zranitelností není levná záležitost a vyžaduje velké množství zdrojů. Částečně je to z důvodů lepší bezpečnosti a lepších technologií, částečně je to faktor kompetice, kde první nálezce má ze zranitelnosti největší nebo i jediný zisk. To je jeden z důvodů, proč se skupiny útočníků začaly zaměřovat na napadání bezpečnostních výzkumníků. Proč investovat zdroje, když je možné nechat to na někom jiném. Z podobného důvodu je i samotný fakt veřejného nahlášení zranitelnosti nebezpečný, protože vede k pokusům o zneužití ze strany útočníků, kteří výzkumníky dlouhodobě sledují. Bohužel však existují společnosti, které ignorují nahlášené zranitelnosti právě do chvíle, než jsou upozorněni na veřejné nahlášení v rámci následujících dnů či měsíců. Časová lhůta existuje právě kvůli nutnému času na opravu, je však nutné, aby tuto výhrůžku nahlašovatel dodržel, jinak přestane být efektivní.[2]

5.5.3 DNS tunneling

DNS tunneling je možné použít pro legitimní účely, tato práce však zkoumá jeho zneužití. Není to samotný útok, ale podpora útoku založená na DNS (Domain Name System). Tento protokol je využíván prakticky neustále pro běžné účely a je velmi flexibilní, to však dovoluje jeho zneužití. DNS je používán tak často, že malé navýšení není poznat. Mnoho společností ho navíc nekontroluje dostatečně, aby mohlo tento typ útoku možné odhalit. Útočník v DNS requestech a responsech zakódovává vlastní komunikaci za účelem jejího skrytí. Odchozí komunikace může být použita pro exfiltraci kritických dat nebo přijímání odpovědí od nainstalovaného malwaru, příchozí komunikace naopak pro posílání příkazů již nainstalovanému malwaru nebo dokonce stahování dalšího malwaru.[15, 27]

5.5.4 Supply-chain útoky

Supply-chain útoky využívají vztahy mezi organizacemi. V dnešní době je provázanost nevyhnutelná, bohužel to však představuje značnou bezpečnostní slabinu. ENISA uvádí, že se tyto útoky skládají z kombinace alespoň dvou útoků, jeden na dodavatele a další na spotřebitele. První útok na dodavatele je použit primárně k útoku na skutečný cíl, tedy spotřebitele. To však neznamená, že spotřebitel jedné služby nemůže být dodavatelem další.

Útočník mnohdy může útoky řetězit a mít až překvapivý dosah. Efektivita plyne v malých možnostech přípravy na tento typ útoku ze strany spotřebitele. Velmi nepříjemnou verzí supply-chain útoků jsou útoky na open-source knihovny. Reálné knihovny bývají nakaženy skrytým malwarem s cílem nakazit kohokoli, kdo knihovnu bude využívat. Tento proces by měli zastavit udržovatelé knihoven, kteří kontrolují přidávané změny, bohužel však mohou udělat chybu. Další možností pro útočníky je napodobit jména a funkcionalitu legitimních knihoven. Je pak šance, že vývojáři omylem použijí tuto podvodnou knihovnu, aniž by si to uvědomili. Například v červnu 2022 bylo zjištěno, že knihovny pygrata a loglib extrahují AWS klíče. Za speciální zmínku stojí útok skupiny provozující ransomware LockBit oproti společnosti Abiom. To byl velice závažný útok protože Abiom dodává komunikační technologii pro nizozemskou záchrannou síť C2000, Nizozemské ministerstvo obrany, národní policii a bezpečnostní služby. Situace okolo supply-chain útoků je natolik vážná, že vedla ke vzniku evropské směrnice **NIS2**, která by měla řešit bezpečnost dodavatelských řetězců. Představuje kybernetickou strategii s návrhy na posílení obrany a zlepšení reakcí proti zákeřným aktivitám. Jedinou obranou proti supply-chain útokům je posílení obrany všech článků řetězce.[2]

6 Kategorie útočníků

Pro kompletnost je při bezpečnostním zkoumání nutné uvažovat i typ útočníka, který útok uskutečňuje. Různé typy se chovají během útoku různě, mají jiné cíle, možnosti a motivace. Pokud je cílem komplexní ochrana, je nutné zvážit, se kterými typy útočníků bude nejčastější konflikt. Pro zjednodušení je možné útočníky zařadit do několika skupin. Stejně jako u útoků mezi skupinami existují návaznosti a překrývání, je nutné skupiny brát pouze jako hrubé zařazení a ne definitivní výčet. Skupinami jsou:

- Příležitostný útočník,
- Script kiddie,
- Hacktivista,
- Hacker na objednávku,
- Kyberkriminálník,
- Státem podporovaný útočník,
- Insider (vnitřní osoba).

[2, 28]

6.1 Příležitostný útočník

Tento typ útočníka by bylo možné nazývat také hobby útočník. Mají omezené zdroje a bývají velmi specifičtí v rámci postupů a zranitelností, které využívají k dosažení svého záměru. Tito útočníci nejsou plně zaměřeni na hackování, je to pro ně spíše zábava a zpestření života. Z toho také vyplývají hlavní motivace těchto útočníků – získat proslulost. Existují fóra dedikovaná těmto útočníkům, kde se navzájem chlubí svými útoky ostatním. Můžeme tak očekávat, že útoky budou směřovány k jasně viditelným, avšak málo destruktivním typům.

6.2 Script kiddie

Ve většině případů jsou script kiddies nejméně schopní útočníci. Jsou to amatéři, kteří používají volně dostupné nebo zakoupené nástroje bez hlubších znalostí systémů a hackování. Většinou bývají neškodní, teprve se učí a mají omezené znalosti a možnosti útoku, a proto jsou jejich útoky málokdy úspěšné. V případě úspěchu často ani nevědí, jak v útoku pokračovat. Lze tak u útoků předpokládat nízkou úroveň poškození, snadno odhalitelné útoky a nízkou sofistikovanost. Jediným výrazným rizikem jsou zakoupené nástroje pro specifické účely. Ve výjimečných případech, u nichž bývá motivací pomsta, zakupují script kiddies

na černém trhu nástroje pro konkrétní devastující útok. Ve většině případů se však jedná o nováčky, kteří hledají výzvy a adrenalin. Pokud má nicméně skript kiddie pro hackování talent, může se díky zisku zkušeností a znalostí stát v průběhu času profesionálním hackerem.

6.3 Hacktivista

Útočníci motivovaní politickými nebo ideologickými názory jsou nazýváni hacktivisti. Provádějí škodlivé útoky pro zviditelnění a prosazení své agendy. Možná nejznámějším příslušníkem je skupina Anonymous. S velikostí skupiny je očekávaná jistá fragmentace, a tak se Anonymous hlásí k množství incidentů s různými agendami. Za speciální zmínku stojí jejich kybernetické útoky proti Rusku v souvislosti s válkou na Ukrajině[29]. Motivací hacktivistů není zisk, ale snaha bojovat za spravedlnost. Jejich útoky tak bývají ve vážnosti v rozmezí od neškodných, jako je změna webové stránky, po drastické, kde vede k poškození infrastruktury a zničení nebo vyzrazení citlivých dat. Také není neobvyklá spolupráce s Insidery, kteří sdílí jejich přesvědčení nebo je upozornili na objekt jejich zájmu. Lze tedy říci, že hacktivisté mohou dle svého přesvědčení být kvalifikování jako síla dobra i zla.

6.4 Hacker na objednávku

Skupina schopných hackerů, kteří své vědomosti a znalosti propůjčují jiným osobám či organizacím, jsou hackeři na objednávku. Nemůže být překvapením, že velká většina hackerů více či méně spadá do této skupiny. Skupina se totiž navíc dle motivace,metodologie a záměru dělí na podskupiny, zvané *White hat, Gray hat* a *Black hat* hackeři.

White hat hackeři

White hat hackeři využívají své schopnosti ve spolupráci s organizacemi k určení jejich slabých míst v zabezpečení. Tito hackeři se řídí silným etickým kompasem, který je jasně zřetelný z jejich činnosti a zaměření pro zlepšení zabezpečení. Pracují se svolením organizace a v jasně vymezených hranicích, což však může limitovat jejich schopnost odhalit veškeré zranitelnosti.

Black hat hackeři

Black hat hackeři jsou neetický opak white hat hackerů. Jejich primární metodikou je prolamování obrany systémů a sítí bez vědomí organizace. Cílem těchto hackerů je vždy svůj vlastní prospěch. Existuje mnoho možností, jak tohoto prospěchu dosáhnou. Někteří napadají společnosti a exfiltrují data uživatelů, která pak prodávají na černém trhu. Jiní využívají tato data k bankovním podvodům, kampaním sociálního inženýrství nebo kradení účtů. Další možností je pouze vyhledávání zranitelností a jejich následný prodej na trhu zranitelností. Státní organizace jsou za takzvané *zero day zranitelnosti* ochotné za-

platit i statisíce dolarů[26]. Tam, kde by zranitelnost etický hacker ohlásil, aby mohla být napravena, ji neetický hacker prodá za značnou sumu peněz.

Gray hat hackeři

Gray hat hackeři jsou na pomezí předchozích kategorií. Jestli boudou klasifikování blíže k white hat hackerovi nebo black hat hackerovi závisí na situaci. Mnohdy využívají metodologii black hat hackerů k odhalení zranitelností, ale místo prodeje nebo zneužití zranitelnosti ji dané organizaci nahlásí. Nesnaží se tak způsobovat škodu, ale odhalit slabá místa zabezpečení, které by mohlo být nemožné odhalit pro white hat hackera. To však bohužel stále znamená napadení organizace či osoby, které nemusí reagovat kladně na pozdější oznámení útoku. Také občasné požadavky platby za napravení zranitelnosti nebo její nevyzrazení jim nedělá nejlepší jméno. Asi nejlepším příkladem tohoto fenoménu je kauza okolo Twitteru Donalda Trumpa, jeho hesel a hackerů nazývaných *The Guild of the Grumpy Old Hackers*[30]. Této skupině hackerů se povedlo několikrát získat přístup ke Twitter účtu Donalda Trumpa, a to v letech 2016 a 2020. Pro kontext, Donald Trump byl v roce 2016 kandidát na prezidenta Spojených států amerických a v roce 2020 prezident. Po obou těchto úspěšných útocích to sami hackeři nahlásili, avšak i tak se nevyhnuli soudnímu řízení. Naštěstí byl jejich postup zcela legální a byli tak zproštěni viny.

6.5 Kyberkriminálník

Tento druh útočníků působí jako jednotlivci nebo dokonce organizované skupiny zaměřené na finanční zisk pomocí kriminální aktivity. Mezi jejich činnosti patří ransomware, těžba kryptoměn, krádež kryptoměn nebo krádež přihlašovacích údajů, které posléze využívají pro další trestnou činnost. Množství těchto útočníků stoupá také díky stále nižším vstupním nárokům díky Malware as a Service (MaaS)[31] a RaaS[32]. Zajímavým trendem posledních let je navíc neustálé přejmenovávání a 'odcházení do důchodu' kriminálních skupin. Cílem je vyhýbání se zákonnému stíhání a sankcím, jelikož je na tyto skupiny kladena stále větší pozornost.

6.6 Státem podporovaný útočník

Útočníci úzce spojeni s určitým státem, jejichž motivace a cíle jsou vždy v zájmu jejich státu. Útoky jsou tedy často zaměřené na posílení státu v politické nebo vojenské sféře. Je jasné, že tito útočníci mají téměř neomezené zdroje, vyspělé technologie a prvotřídní znalosti. Proto jsou od nich časté sofistikované a rozsáhlé útoky. Lze tedy očekávat průmyslovou špionáž, úniky státních tajemství, cílené kybernetické útoky na infrastrukturu ale také rozsáhlé ransomwarové kampaně a podvody s kryptoměnou. Není neobvyklé, že státy rekrutují úspěšné hackery ze všech možných zdrojů. Existují dokonce doměnky o rekrutování i mezi kriminálníky. Mnoho spekulací koluje například kolem skupiny REvil, kterou

Rusko zatklo na začátku roku 2022[33]. Bohužel již o pár měsíců později se znovu začaly objevovat známky jejich aktivity. Jak je však u státem sponzorovaných akcí trendem, daný stát jakoukoli vazbu popírá a tento fakt lze jen těžko vyvrátit. Přesto bylo identifikováno hned několik skupin, kde je návaznost na stát téměř jistá. Příkladem je *Lazarus Group* pro Severní Koreu, *Sandworm Team* pro Rusko nebo *APT41* spojený s Čínou[34].

6.7 Insider (vnitřní osoba)

Insider je osoba pocházející z organizace, která způsobila chtěně nebo nechtěně bezpečnostní incident, představuje proto značnou hrozbu pro bezpečnost celé organizace. Většina bezpečnosti je nastavena na venkovní hrozby. Nebezpečí insidera je právě v naprosté neefektivitě takto postavené obrany vůči němu. Systém totiž nemůže být nikdy stejně chráněný z venku jako zevnitř. Insider takto nastavenou ochranu obejde a dostane se přímo ke zranitelným místům. Velmi často jsou těmito insidery nespokojení zaměstnanci, bývalí zaměstnanci, dočasní pracovníci nebo dokonce zákazníci. Je proto velmi důležité správně nastavit přístupy do systému a při odchodu zaměstnanců jim přístup včasně odebrat. Insidery můžeme dle úmyslu dělit na tři hlavní kategorie, kterými jsou *Úmyslný insider*, *Nechtěný insider* a *Nedbalý insider*.

Úmyslný insider

Úmyslný insider je ten, kdo vědomě způsobí své organizaci újmu. Mezi příklady se řadí krádeže dat, úmyslné poškození infrastruktury nebo vydání přístupu třetí neoprávněné osobě. Cílem těchto insiderů bývá často pomsta nebo jen peněžní zisk. Speciálním případem této kategorie je takzvaný *whistleblowing*, což termín označující situaci, při níž současný nebo bývalý zaměstnanec upozorní na trestné, neetické nebo podezřelé jednání firmy či státní instituce. Tohoto zaměstnance lze tedy také považovat za úmyslného insidera, který však vyzrazuje informace v dobré víře a nejedná ve vlastní prospěch. Velice známým zástupcem je Edward Snowden, který v roce 2013 veřejnosti odhalil existenci rozsáhlých programů na sběr informací fungujících pod záštitou NSA (National Security Agency)[35].

Nechtěný insider

Může se stát, že insiderem se stane běžný zaměstnanec, který se shodou okolností dopustil nějaké chyby a poškodil firmu. To však nebylo úmyslem a ani tato situace nenastala v rámci zanedbání povinností. Může se například jednat o náhodné smazání nebo modifikace důležitých souborů, nechtěné vypojení zařízení ze zásuvky.

Nedbalý insider

Některé hrozby vznikly kvůli nedbalosti zaměstnance, Ten pak figuruje jako nedbalý insider. Situace nastane, když zaměstnanec nedodržuje správné postupy, politiky nebo metodologie,

které organizace stanovila. Tyto postupy vznikly právě pro ochranu důvěrnosti, integrity a dostupnost dat. Jejich nedodržování je proto značný bezpečnostní problém. Je však nutné zkoumat, zda toto nedodržování plyne z nerealisticky nastavených politik nebo pouze chyb zaměstnance. Další možností jsou také nedostatečné znalosti a zaškolování zaměstnanců pro vykonávání možné činnosti. Je jasné, že v mnoha případech může být obtížné rozeznat, zda se jedná o nedbalého nebo pouze o nechtěného insidera

7 Testování

Smyslem testování je simulovat útok na infrastrukturu systému. Ve většině případů to znamená, že se specialista na bezpečnost snaží provádět stejné kroky jako potencionální útočník. Ideální postup vylučuje nejen nepředvídatelnost útočníka, ale ve výjimečných případech i jeho neschopnost nebo neznalost. Stejně jako v každém odvětví existují i mezi útočníky sféry kompetence a znalostí. Existuje mnoho útočníků, kteří se touto činností nejen živí, ale je to také jejich vášeň. Takovýto útočník bude disponovat znalostmi a technikami které nejsou běžné. Při útoku bude postupovat co možná nejoptimálněji za účelem dosažení výsledků. Je možné od něj očekávat pozorné zkoumání cíle a vytrvalost, díky nimž si cíl zvolí. Tiše hledá slabiny v obraně a proniká do střežených systémů bez povšimnutí. Ne každý útočník je však takto nebezpečný. Drtivá většina útoků je prováděna nadšenci nebo útočníky bez obsáhlých znalostí a technik útoku. Není tak vyloučeno použití snadno detekovatelných *hlučných* technik nebo prostých chyb, kterými na sebe při útoku upozorní. Nebezpečnost této skupiny v posledních letech vzrostla díky propagaci MaaS (Malware as a Service)[31] a RaaS (Ransomware as a Service)[32]. Existence nástrojů, které dovolují provézt úspěšný útok za pomocí znalostí zkušenějšího útočníka, znamená, že ani nezkušené útočníky není možné podceňovat.

Testování je jedna z nejlepších možností, jak zlepšit obranyschopnost organizace. Nemilou samozřejmostí je, že největší změny v ochraně přichází po bezpečnostním incidentu. Ztráta dat, poškození reputace organizace nebo i finanční postihy jsou výbornou motivací, proč věnovat zabezpečení větší úsilí, nejen pro obránce, ale i pro management organizace. Pokud se útočníkovi podařilo prolomit ochranu organizace, jasně to ukazuje na nedostatky, které je nutné napravit. Bezpečnostní incident tak kromě mnoha nepříjemností ukazuje, jak dobře byla organizace připravena. Dle reakce obránců lze zkoumat jejich celkovou připravenost. Dobře připravení obránci mohou nebezpečný incident zaznamenat včas a pokud jeho následku nejde zabránit, mohou ho alespoň omezit. Nepřipravení obránci nemusejí zaznamenat incident ani měsíce po jeho uskutečnění a několikanásobném zopakování. Organizace a její obránci musí vědět, jak postupovat v případě incidentu. Testování je simulace bezpečnostního incidentu ale bez většiny jeho negativ. V závislosti na druhu testování je možné vyzkoušet připravenost obránců, jejich obezřetnost a postupy v případě detekce podezřelé činnosti. Můžeme testovat robustnost infrastruktury, zda je kvalitně navržena a správně nastavena. Můžeme testovat zařízení, zda fungují správně a nelze je zneužít. Můžeme testovat technologie, zda jsou správně využívány, popřípadě zda je jejich využívání nutno omezit nebo naopak rozšířit. Důvodů, proč by mělo být testování součástí zlepšování obranyschopnosti každé organizace je tedy mnoho. Testování přináší tolik benefitů, protože to není prostá reakce na událost, ale především příprava. Cílem organizace je zajistit, aby žádný bezpečnostní incident nebylo možné stejně uskutečnit dvakrát. Čím více je poprvé

uskutečněno pomocí testování, tím více jich bude zaznamenáno a zastaveno při skutečném útoku.

7.1 Rozsah testování

Obránci se musí přizpůsobovat a testovat nejen nejběžnější a nejefektivnější útoky ale i krajní scénáře. Takovéto přizpůsobování vedlo nejen k různým testovacím metodikám, jako *Red teaming* a *Penetration testing*, ale také k testování různých scénářů a hlavně rozsahů. Mezi nejznámější patří *celkový pokus o kompromitaci*, *specifický pokus o kompromitaci* nebo *předpokládaný kompromis*. Je samozřejmé, že každá tato kategorie obsahuje další podkategorie. Toto základní rozdělení je však vhodné pro rozpoznání hlavních výzev, složitostí ale i přínosů testování. Nelze říci, zda je jeden scénář lepší nežli jiné, naopak se doplňují a každý slouží pro určitou situaci.[36]

7.1.1 Celkový pokus o kompromitaci

Základní situací je *celkový pokus o kompromitaci obrany*, který lze definovat jako snahu *red teamu* napadnout celou infrastrukturu organizace a pokusit se kompromitovat co možná největší možnou část. Tato strategie je vhodná pro celkové testování infrastruktury, jedná se totiž o emulaci skutečného útoku. Testování ve většině případů začíná ze stejného bodu, který je běžně dostupný veřejnosti a tím pádem i útočníkům. Lze takto testovat správnou segmentaci infrastruktury a rezistivitu jednotlivých segmentů. Z velkého a otevřeného rozsahu však vyplývá jen omezená možnost testování do hloubky, není možné zaměřit se na specifické části infrastruktury. *Red team* má pouze omezený čas a prostředky, proto nachází pouze nejčastější zranitelnosti na celém rozsahu testování, je nerealistické předpokládat, že by mohl testovat jednotlivé části infrastruktury do hloubky nebo pro všechny možné hrozby. Při nesprávném provedení nebo nepochopení cíle tohoto testování může vznikat falešný pocit bezpečnosti, který je pro zabezpečení nebezpečný. Cílem tohoto testu je získat celkové povědomí o ochraně a poté pokračovat s podrobnějším testováním.

7.1.2 Specifický pokus o kompromitaci

Pro testování omezené části infrastruktury se využívá *specifický pokus o kompromitaci*. Cílem je důkladně otestovat omezenou část infrastruktury bez využití, zásahu nebo omezení částí infrastruktury nacházející se mimo testovaný rozsah. *Red team* provádí podrobné testování, které při korektním provedení vede k nalezení všech zranitelností. Výhodou tohoto testování je jeho specificita, je možné testovat určitou oblast infrastruktury nebo jen určité zařízení, kde bývá výhodné testovat za určitých podmínek. Příkladem může být testování za použití specifického účtu a s ním spojených pravomocí přístupu. Další výhodou je možnost testování v běžném provozu. Krátkodobě vyřadit a testovat část infrastruktury je proveditelnější než celkové vyřazení nebo testování za běžného provozu. V takovém případě je

však nutné dávat pozor na správný výběr rozsahu. Při důkladném testování není neobvyklé vyřazení testovacího zařízení z běžného provozu nebo jeho zhroucení. Je proto důležité, aby nebyl testován systém, který je kriticky důležitý nebo zrovna používaný.

7.1.3 Předpokládaná kompromitace

Z názvu je jasné, že toto testování zkoumá, jakou škodu může útočník napáchat při úspěšném útoku. Počáteční bod tohoto testování je založen na předpokladu úspěšné infiltrace útočníkem. Přístup k takto identifikovanému bodu je s příslušnými právy poskytnut *red teamu*, který nemusí prolamovat obranu systému. *Red team* se tak může plně soustředit na zkoumání dopadu úspěšného útoku. Důvod, proč toto testování není pouze součástí předchozích testování, je úspora času a prostředků. Vhodným příkladem jsou útoky sociálního inženýrství a phishing. Jsou to často testované útoky právě díky jejich četnosti ale jejich výsledeky nejsou okamžité, a tak není možné vytvořit rychlou zpětnou vazbu. Může totiž trvat i týdny než uživatel otevře e-mail a nainstaluje malware.[36] Z důvodu efektivity je tedy lepší předpokládat úspěch útoku a začít testovat z bodu malwarem nakaženého uživatelského stroje. Tento typ testování je výhodný pro ukázku dopadu úspěšného útoku. Častým problémem bezpečnosti je její nedocenění, dokud funguje správně, specialisti se zdají být nepotřební. Ve chvíli, kdy nastane problém, je však většinou pozdě. Proto tento typ testování představuje nástroj k prokázání důležitosti kvalitní obrany ukázkou důsledků jejího selhání.

7.2 Metodologie testování

Důležitým aspektem testování je již zmíněný rozsah, ještě důležitější je však správný výběr způsobu testování. Mezi nejznámější testovací metodologie patří: *Penetration testování*, *Red team vyhodnocení* a *Purple team testování*, také známé jako *kontrolní cvičení*. Stejně jako u rozsahu testování, tak i u těchto metodologií existuje určitý přesah. Z tohoto důvodu jsou tyto metodologie nepřesně definovány, někdy zaměňovány nebo dokonce považovány za jedinou metodologii s několik různými názvy. Je proto nutné si je představit v kontextu tohoto textu. K tomu slouží následující sekce.[37]

7.2.1 Penetration testování

Penetration testování, často také zkracován na Pen testing, je metodologie s cílem vyhledání co nejvíce možných zranitelností testovaného systému. Takto důkladné hledání je omezeno pouze na zadaný rozsah, neboli část testovaného systému. Aby bylo dosaženo co největší efektivity, tento typ testování se svoji činnost nesnaží schovávat, naopak bývá velmi snadné ho detekovat. To však nevadí, protože ochrana daného systému by o jeho provádění měla být předem informována a může tak zkoušet, zda i detekce funguje optimálně. Tento typ testování může být také z části automatizován, což vede k dalšímu zlepšení efektivnosti na

úkor flexibility. V neposlední řadě Penetration testování vyžaduje menší množství zdrojů než Red team vyhodnocení, ať už v podobě času, lidí či kapitálu.

7.2.2 Red team vyhodnocení

Red team vyhodnocení, také referovaný jako Red teaming, je na rozdíl od Penetration testování zaměřen na dosažení zadaných cílů, například získání přístupu k citlivým datům, nebo testování všímavosti ochranných systémů. To také znamená, že Red teaming není omezen oblastí, kterou může v rámci dosažení svého cíle využít. Obrana systému není ze zřejmých důvodů seznámena s nadcházejícím testováním, proto tato metodika vyžaduje maskování a opatrný přístup, aby,v rámci možností, co nejvíce simulovala skutečný útok. Výhodou je, že za předpokladu detekce bude obrana systému postupovat stejně, jako kdyby se jednalo o skutečnou hrozbu a získají tak cenná data a zpětnou vazbu pro zlepšení budoucí obrany. Je jasné, že pro správné provedení Red teamingu je potřeba více zdrojů než v případě Pen testingu, ať už se jedná o čas nebo lidskou práci,. Také automatizace zde bývá složitá, jedná se totiž o specifickou strategii pro každé testování, při němž je nutné reagovat na všechny události vzniklé při testování.[37, 38, 39]

7.2.3 Purple team testování/Kontrolní cvičení

Specifickou situací je blízká spolupráce útočníků (Red team) a obránců (Blue Team). Hlavní výhodou tohoto postupu je zpětná vazba mezi útočníky a obránci, díky níž se dá testovat detekce a následná odezva obránců při testování specifických technik obsažených v MITRE ATT&CK frameworku. Další výhodou je seznámení s postupy druhé strany pro tvorbu efektivnější strategie obrany, ať už se jedná o útočníky nebo obránce. Tato cvičení lze uskutečňovat pro vyzkoušení techniky jednou, lepší však bývá opakované testování. Částečná automatizace za použití open-source nástrojů, které mají v této práci vlastní kapitolu, je také jednou z možností. Výhodou opakovaného testování s automatizací je možnost měřit a porovnávat výsledky za vstejných stupních podmínek, což vede k jasně viditelnému zlepšení obranné strategie.[37, 40]

8 Zavedené nástroje v problematice Testování

Pro účely testování je dobré využívat stávající technologie. Je jasné, že každé testování prostředí je jedinečné, to však neznamená, že není možné těžit z poznatku ostatních obránců. Vzniklo mnoho nástrojů, jejichž cílem je pomoci nejen s rozeznáváním útoků, ale i se samotným testováním. Asi nejznámějším frameworkem pro kolekci útoků a jejich rozeznávání je MITRE ATT&CK[41]. Tento framework je open-source, volně dostupný a obsáhlý. Existuje množství testovacích frameworků, které jsou s MITRE ATT&CK kompatibilní[42]. Příkladem RTA (Red Team Automation), Caldera nebo Atomic Red. Tyto frameworky jsou na rozdíl od jiných zdarma, a proto se hodí pro začátek testování, kdy je dobré si nejdříve vymezit testovanou oblast a nutné nástroje. Všechny tyto frameworky budou více probrány a porovnány v následujících kapitolách.

8.1 MITRE ATT&CK

Obrázek 6: Mitre ATT@CK Navigátor Zdroj: [41]

MITRE ATT&CK je bezplatná otevřená znalostní databáze popisující chování útočníků a techniky, které tyto útočníci využívají. Tato znalostní báze je založená na pozorování v rámci reálného světa, data pochází z veřejného zpravodajství a hlášených bezpečnostních incidentů. Samozřejmě jsou začleněny i veřejné výzkumy technik útočníků. Je aktivně udržována, nové informace jsou přidávány dvakrát do roka[43]. Hlavním přínosem tohoto projektu však není pouze mapování útočníků, ale celková klasifikace útoků do jednotlivých *taktik, technik a sub-technik*. Framework tak obráncům nabízí možnost rozložit složitý útok

na jeho jednotlivé stavební kameny. ATT&CK je velmi podrobný, a dokonce u jednotlivých technik útočníků nabízí možnosti detekce a obrany. Obránci proto mohou snáze porozumět stylu práce útočníků, technikám, které používají, ale nejdůležitěji, jak tyto informace využít k vytvoření lepší obrany. Všechny tyto informace jsou navíc přehledně dostupné v interaktivní formě pomocí ATT&CK navigátoru[44]. V něm je možné provádět vizualizaci a porovnávání útoků. Je tedy snadné prezentovat rozbor útoku dalším osobám, díky exportování a importování studovat již popsané útoky a sledovat nejpoužívanější taktiky a techniky. Není proto divu, že je MITRE ATT&CK v době psaní tohoto textu považován jako jeden z nejvýznamnějších standardů pro popis technik používaných útočníky při kybernetických útocích.[41]

8.1.1 Členění

Díky popularitě ATT&CK došlo k jeho velkému růstu. Je jasné, že s přidáváním taktik a technik vzrůstá nepřehlednost. Také rozšiřování zaměření nakonec vedlo k nutnosti rozdělení, aby byla zachována přehlednost a funkcionalita. Proto existují specifikace pro určitá odvětví[44]:

- **Enterprise** – síťové a cloudové technologie,
- **ICS** – průmyslové řídící systémy,
- **Mobile** – mobilní zařízení.

Samozřejmě i jednotlivá odvětví jsou dále rozdělena na domény dle zaměření útočníků. U Enterprise je rozlišování pro Windows, macOS nebo Linux a také cloud, network a containers. Mobilní platforma obsahuje techniky pro Android a iOS. Toto rozdělení dává smysl, stejná technika bude jinak aplikována na různých systémech a díky tomuto rozdělení je možné zamířit se právě na jeden určitý use-case útoku.

8.1.2 Taktika

Taktika představuje nejvyšší úroveň abstrakce modelu ATT&CK. Představuje cíl útočníka, ne však jak se tohoto cíle útočník snaží dosáhnout. Jako příklad je možné zmínit taktiku *Impact(Dopad)*, která je zaměřená na způsobení škody v podobě ohrožení integrity nebo dostupnosti dat. Rozdělení na taktiky není ojedinělé, naopak na této abstraktní úrovni ATT&CK těsně připomíná další modely hrozeb zaměřené na postup útoku a útočníka. Důvod, proč je ATT&CK preferován před jinými modely, je jeho rozsah, provázanost a modelování namapované na proces navigace útočníka v napadaném systému. Další výhodou je jasná rozlišitelnost taktik. Jsou označené jedinečným řetězcem ve tvaru **TA0XXX**, kde je XXX nahrazeno číslem jednotlivé taktiky. Pozor na fakt, že taktika se stejným názvem,

například *Initial access(Počáteční přístup)*, bude označena jiným řetězcem v závislosti na odvětví, do něhož spadá. Pro enterprise je to **TA0001**, pro mobile **TA0027** a pro ICS se tato taktika značí **TA0108**. Nemůže proto dojít k záměně a nahlížet na techniky, které nejsou aplikovatelné na dané odvětví.[45, 41]

8.1.3 Technika a sub-technika

Techniky jsou způsob, kterým útočník dosahuje svého taktického cíle. To znamená, že v rámci každé taktiky existuje konečný počet popsaných akcí, jejichž provedením útočník dosáhne svého cíle. Je jasné, že použité techniky se mění v závislosti na znalostech i možnostech útočníka. Také je nutné brát v potaz prostředí, v němž útok probíhá. Popis taktik je však od těchto specifik oproštěn. Důvodem je opět nutnost klasifikace, kdy není možné vytvořit téměř nekonečné množství technik pro jednotlivé útoky. Jsou proto klasifikovány do kategorií technik, v nichž jsou změny v metodologii nebo jednotlivé kroky přidány pomocí sub-technik. Tento postup umožňuje popsat nejdůležitější kroky chování útočníka aniž by se obránce ztratil v detailech. Další výhodou je izolace od neustále vyvíjejícího kódu. Základní metodika zůstává zachována, avšak jednotlivé implementace se v čase rapidně mění. Stejně jako taktiky jsou i techniky označeny jedinečným řetězcem, který je ve tvaru **TXXXX**, kde je XXXX nahrazeno číslem jednotlivé techniky. Pokud pro tuto techniku existují sub-techniky, připojuje se na konec řetězce **.XXX**, dde XXX reprezentuje jednotlivou sub-techniku. Za příklad je možno uvézt techniku *Phishing*, identifikovanou řetězcem **T1566**. Technika *Phishing* má také 3 sub-techniky, kterými jsou *Spearphishing attachment **[T1566.001]***, *Spearphishing link **[T1566.002]*** a *Spearphishing via service **[T1566.003]***

Techniky se jen málokdy vyskytují v izolaci, většinou na sebe, stejně jako celé taktiky, navazují. Vytvářejí tak sled událostí, které vedou k úspěšnému útoku. Schopnost identifikovat a propojit navazující druhy událostí je důležitou součástí obrany, cílem modelu ATT&CK je to co možná nejvíce usnadnit. Data získaná z každého kroku v sekvenci pak nejen vypovídají o tom, zda se jedná o útok, ale také obránci dovolují lépe vyhledávat další postup útočníka. Je také možné, že podle cíle techniky je daná technika zařazena do více taktik zároveň. Jedním takovýmto příkladem může být technika *Input capture (Zachycení vstupu)*. Ta spadá ve stejnou chvíli do taktik *Collection (Sběr dat)* a *Credential access (Pověření k přístupu)*. Je jasné, že framework ATT&CK nevypisuje všechny existující techniky útoku z dané taktiky. Jeho založení na informacích získaných z opravdových bezpečnostních incidentů a komunity výzkumníků však vede k upřednostnění nejznámějších a nejpoužívanějších technik. Zdá se to být nejlepší způsob, jak shromažďovat účinné informace o použití technik útočníka a jak je propojovat do užitečného analytického nástroje.[45, 41]

8.1.4 Další přínos

V neposlední řadě ATT&CK také sleduje původ útoků, využitý software a zařazuje útoky do předpokládaných kampaní. Tyto záložky jsou na hlavní stránce, specificky se jedná o *Groups, Software* a *Campaigns*.

Groups – skupiny

Skupiny označují shluky útočníků, kteří operují se stejným cílem, je proto logické se domnívat, že jsou mezi sebou v kontaktu. Analytici sledují skupiny pomocí různých metodologií a termínů. Je tedy možné, že různé skupiny analytiků nazývají jistou skupinu různými jmény, proto jsou u skupin zaznamenávány i alternativní názvy. ATT&CK se snaží tato různá pojmenování respektovat. Také mezi jednotlivými skupinami dochází k částečnému překrytí, a to z důvodu pohybu útočníků a složitosti sledování skupin. U kriminálních skupin je častý takzvaný *rebranding*, kdy skupina změní své oficiální jméno nebo identifikační rysy za účelem zmatení autorit. Pro zmatení je také časté použití identifikačních rysů jiných skupin, i z toho důvodu je zaznamenávání a sledování skupin obtížné. Hlavním přínosem sledování skupin jsou informace o postupech a metodologiích útoku, které daná skupina preferuje. Tyto informace jsou získány mapováním na veřejně oznámené útoky a jsou uvedeny původní odkazy. Je důležité zmínit, že informace nezobrazují všechna možná použití technik skupin, ale pouze podmnožinu, která byla zaznamenána. I tak je to pro obránce značný přínos. Při identifikaci metodologie útoku na určitou skupinu je možné předpovídat další kroky z předchozích záznamů a zmírnit tak dopad útoku.[34]

Software

Software je termín pro vlastní nebo komerční kód a nástroje používané útočníky pro provádění technik nebo taktik. Stejně jako u skupin můžeme u softwaru najít alternativní názvy právě díky sledování několika skupin. Překrývání je sledováno týmem ATT&CK a tyto názvy jsou označeny jako *Associated Software*. Informace o softwaru pochází z veřejně oznámených technik a často bývají mapované na skupiny, které tento software využívají. Je tedy opět nutné zmínit, že použití určitého softwaru neznamená, že se jedná o související skupinu. Pouze to znamená, že daná skupina tento software v minulosti použila.[46]

Campaigns – kampaně

Pojem kampaň označuje rozsáhlou intruzivní aktivitu, která proběhla během určitého období s obecnými cíli a úkoly a byla značnou kybernetickou hrozbou. Jedná se například o dlouhodobou průmyslovou špionáž nebo špionáž proti vládě určité země. Není neobvyklé, že do složité kybernetické operace je zapojeno několik přidružených skupin, přičemž každá hraje jedinečnou roli. Například může být jedna skupina zodpovědná za počáteční průnik do systému a jiná za exfiltraci dat Kampaň je označována názvem uvedeným ve veřejných

zprávách nebo jedinečným identifikátorem ATT&CK, pokud kampaň ještě nebyla pojmenována. Zaznamenání a sledování kampaní je obtížné. Různé organizace zaznamenávající útok patřící do kampaně ho mohou oznámit pod různými jmény a stejný útok navíc může být popsán z různých úhlů pohledu. Tým ATT&CK pro jednotlivé kampaně činí nejlepší úsilí o sledování překrývajících se jmen, která jsou označena jako 'Přidružené kampaně'. Toto sledování je výhodné, protože poskytuje informace nejen o existenci kampaně, ale také informace o technikách, které jsou využívány. Pro referenci jsou tak kampaně mapovány na veřejně uváděné techniky a jsou v nich zahrnuty původní reference.[47]

8.2 Nástroje

Open-source ATT&CK test tools

PRODUCT	MAIN PURPOSE	STRUCTURE	INSTALLATION*	ENDPOINTS SUPPORTED
Endgame Red Team Automation	Testing EDR products	Python scripts	Minimal	Windows only
Mitre Caldera	State preservation of attack origins	Python scripts, agents and Linux/Win server	Detailed instructions	Windows 64-bit only
Red Canary Atomic Red	Wiki, testing resources reference	No scripts	None	Windows, Mac, Linux
Uber Metta	Playbooks for adversary simulation and testing EDR products	Python, Redis, Celery, Vagrant, VirtualBox	Complex with lots of config file editing	Windows, Mac, Linux

Obrázek 7: Porovnání vybraných nástrojů Zdroj: [42]

Než je zvolen finální framework pro testování, je nutné si nejdříve připravit co možná nejvíce informací týkajících se testování. Je jasné, že každý z vybraných frameworků má své silné a slabé stránky. Jak je vidět v tabulce 7, jedním z ovlivňujících parametrů je například testovaný operační systém. S atomic red je možné testovat na všech třech hlavních platformách, RTA je přizpůsobené pouze pro Windows. Specializace sama o sobě není špatná vlastnost, naopak většinou bývá přínosem. Pokud však potřebujeme testovat Linux, je jasné že nemůžeme použít nástroj, který toho není schopen. Žádný z frameworků také nepokrývá

celou MITRE ATT&CK matici. Proto lze předpokládat použití více nástrojů právě podle okruhu testování, na který je testování zaměřeno.

8.2.1 Red Canary Atomic Red

Ze všech uváděných příkladů je *Atomic Red* nejvíce přívětivý rychlému začátku. Pro jeho funkčnost není potřeba nic stahovat ani nastavovat, lze ho jednoduše použít z příkazové řádky[48]. Další odlišností je jeho ovládání. Většina ostatních frameworků je založena na jazyku Python, popřípadě jiném skriptovacím jazyku. Atomic Red je ale spíše sada instrukcí odpovídajících jednotlivým taktikám a technikám Mitre ATT&CK. Atomic Red tedy není testovací software ale instrukce, pro testování jednotlivých ATT&CK taktik s nástroji, které jsou již pravděpodobně nainstalované v počítači. Je tedy vhodný pro naučení testovacích postupů, ne však pro automatizované testování. Uživatel při testování vždy musí provézt kroky útoku a sledovat výsledek. To neznamená, že není možné simulovat složité útoky využívající hned několik technik. Atomic Red dovoluje techniky za sebou řetězit a vytvářet složité sekvence útoků. Výborným příkladem přímo od tvůrců je kód zvaný *Dragons tail*[49]. Tento příklad se snaží napodobit chování skutečných útočníků. Samozřejmě napodobení není dokonalé, ale dobře ukazuje možnosti Atomic Red pro složitější testování.[42]

Nevýhody

Hlavní nedokonalostí tohoto přístupu je nutnost vytvářet nebo najít vlastní pomůcky. Atomic Red je nástroj pro obránce a nechce dát útočníkům všechny potřebné prostředky pro provedení útoku. To znamená že pomocné nástroje pro útok si musí obránce připravit sám. Příkladem může být malware vložený v Microsoft Word dokumentu. Atomic Red se snaží ukázat, jak malware operuje a jak ho útočníci využívají bez toho, aby ho útočníkům poskytl. Dalším problémem je generace výstupních reportů. Na rozdíl od dalších přístupů Atomic Red nevytváří automaticky stručný report o technikách zkoumaných v útoku. Tato funkcionalita je bohužel až v pokročilejším placeném softwaru, který Red Canary nabízí.[42]

8.2.2 Endgame RTA

RTA v tomto kontextu znamená RTA (Red Team Automation). Z představených nástrojů je to stále jednodušší, třebaže mocný nástroj. Jediný povinný požadavek je Python verze 2.7, kde pro instalaci stačí rozbalit repozitář, který je volně dostupný na GitHubu. Pro plnou funkcionalitu je však doporučeno navíc do podadresáře *bin* vložit **Sysinternals Suite** a **MsXsl**. Stále je to však jednoduchá instalace a celý návod se nachází přímo v GitHub repozitáři.[50]

Schopnosti

RTA je složení téměř 50 různých skriptů simulujících útoky. Bohužel jména těchto skriptů

neodpovídají přesně Mitre ATT&CK, i když jsou na ní založené. Také zde neexistuje hyperlinkuvá navigace, jako například u Atomic Red. Práce se skripty proto vyžaduje více úsilí a určitou známost matice ATT&CK. Naštěstí jsou přesná označení technik, jako **T1107**, snadno dohledatelná přímo ve skriptu. Pro složitější testování je možné spouštět všechny skripty najednou nebo vybrat některé pomocí podmíněného příkazu *IF* přímo v kódu. Pro základní automatizaci stačí, pro hlubší testovaní je tento nástroj však omezen.[42]

8.2.3 Mitre Caldera

Caldera je od stejných vývojářů jako ATT&CK, tedy Mitre. Lze tak očekávat dobrou integraci a kompatibilitu mezi těmito nástroji. Na rozdíl od dříve představených nástrojů je Mitre Caldera komparativně náročnější nástroj, což se projeví i v instalaci. Ani tak není instalace náročná, a to hlavně díky přípravě tvůrců a dobré dokumentaci[51].

Framework caldera lze rozdělit na 2 hlavní části: *jádro systému* a *pluginy. Jádro systému* je dostupné v GitHub repozitáři, zahrnuje asynchronní server pro řízení příkazů a kontrolu (command-and-control, C2) s REST API a webovým rozhraním. *Pluginy* jsou rozšíření možností jádra frameworku, které poskytují dodatečnou funkcionalitu. Ve většině případů se nachází ve vlastních repozitářích, jsou však v hlavním repozitáři referencovány. Jako příklady je dobré uvézt agenty, hlášení, nebo techniky z Atomic Red teamu.[52]

Systémové požadavky

Autoři se snaží podporovat široké spektrum cílových systémů. Proto existují 2 typy požadavků: povinné a doporučené. Povinné požadavky určují minimální prostředí, kde může být Caldera připravena. Jádro frameworku může být nainstalováno na operačních systémech Linux nebo MacOS. Pro fungování je vyžadován Python verze 3.7, 3.8, nebo 3.9, samozřejmě s rozhraním pip3. Pip3 je vyžadován pro instalaci podpůrných balíčků uvedených v souboru *requirements* přímo v repozitáři Caldery. Ke správnému ovládání je vyžadován moderní prohlížeč, doporučený je Google Chrome. Doporučené požadavky se týkají vývoje a správného fungování Caldery. Je doporučený hardware s 8GB+ RAM a 2+ CPU. Dále je pro správnou kompilaci a funkčnost GoLang agentů doporučen GoLang 1.17+. Za zmínku stojí také možnost instalovat a pracovat s Calderou v Docker kontejneru.[51]

Možnosti

Caldera je oproti dříve představeným nástrojům složitý framework. To je však více nežli dostatečně vyváženo dobrou dokumentací a hlavně možnostmi, které zkušenému uživateli Caldera nabízí. Caldera dovoluje nastavení autonomních red-team nebo blue-team operací, a to plnohodnotně včetně závěrečného výpisu a exportování logů. Existuje také možnost manuálních red-team operací, hlavně v případech nahrazování a testování pomocí vlastních nástrojů.[51]

9 Příprava praktické části práce

Praktická část této práce je zaměřená na zjišťování možností testování. Cílem je vytvořit jednoduché a srozumitelné testovací prostředí a návod, jak provádět základní testování taktik a technik MITRE ATT&CK. Za tímto účelem jsou představeny vybrané testovací nástroje založené na MITRE ATT&CK nebo s ním kompatibilní. Je popsáno testovací prostředí, instalace vybraných nástrojů, možné problémy, které při přípravě mohou nastat, a také jak tyto problémy vyřešit. Dále je ukázáno a vysvětleno, jak tyto nástroje používat k docílení testování, a také jak testovat vybrané taktiky a techniky. Výsledná práce by tedy měla stačit k tomu, aby i neznalý uživatel byl schopen nastavit testovací prostředí a otestovat základní vlastnosti své infrastruktury nebo zařízení.

9.1 Popis testovacího prostředí

Jako testovací prostředí bylo zvoleno Kali Linux, které bude spouštěno v Oracle VM VirtualBox. Kali Linux je operační systém založený na Debianu, jenž je od základu navržen pro testování zabezpečení a penetrační testování. Jedná se o možná nejznámější a nejrozšířenější distribuci Linuxu s tímto zaměřením, oblíbeným mezi profesionály i nadšenci. Obsahuje množství specializovaných nástrojů pro testování zabezpečení, odhalování zranitelností nebo monitorování sítě. Velkou výhodou je zaměření na open-source nástroje, často vytvářené profesionály pro své specifické potřeby. Lze tak jednoduše využít jejich znalosti ke zjednodušení práce ostatních uživatelů. V případě potřeby se však stále jedná o distribuci Linuxu a proto je v rámci kmenové distribuce jednoduché nainstalovat jakýkoli nástroj, který by mohl uživatel potřebovat. Repozitáře Kali Linuxu však zjednodušují instalaci právě testovacích nástrojů.[53] Menší změna od původního plánu využít Kali nastala při 10. výročí této distribuce[54]. Vývojáři představili Kali Purple, kterou je možné vidět na obrázku 8. Tato verze Kali Linuxu je oproti klasické ofenzivně zaměřené Kali více orientována na defenzivní testování. Proto byl původní plán pozměněn a pro implementaci prostředí byla použita právě Kali Purple. Dalšími faktory vědoucími k této změně byla i zvědavost a možnost testování nové distribuce. S tímto rozhodnutím se však váže i menší problém – Kali nabízí na svých stránkách ke stáhnutí mnoho různých verzí *image*, mezi nimiž je i specifická verze připravená pro VirtualBox. Kali Purple je v době psaní tohoto textu dostupná pouze v podobě klasického instalačního *image*. Prvotní příprava je proto o instalační krok ztížena, to však není zásadní problém.

Obrázek 8: Spuštěná Kali Purple ve virtuálním prostředí Zdroj: Vlastní

9.1.1 Caldera

Po přípravě operačního systému ve virtuálním prostředí je čas nainstalovat nástroj Mitre Caldera. Při samotné instalaci Caldery však nastal další problém, nejnovější verze Caldery v době psaní je 4.1.0, která vyšla 19. 9. 2022 a v době testování tato verze Caldery nejde na nové verzi Kali Purple zkompilovat. Tento fakt je vidět na obrázku 9.

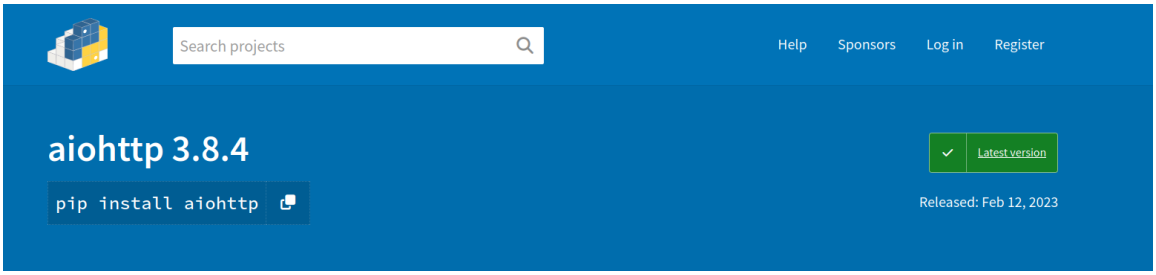
```
    /usr/include/python3.11/cpython/unicodeobject.h:685:27: note: declared here
      685 | static inline Py_UNICODE* PyUnicode_AS_UNICODE(PyObject *op)
          |                           ^~~~~~~~~~~~~~~~~~~~
    error: command '/usr/bin/x86_64-linux-gnu-gcc' failed with exit code 1
    [end of output]

  note: This error originates from a subprocess, and is likely not a problem with pip.
  ERROR: Failed building wheel for reportlab
  Running setup.py clean for reportlab
  Building wheel for pyminizip (setup.py) ... done
  Created wheel for pyminizip: filename=pyminizip-0.2.6-cp311-cp311-linux_x86_64.whl size=203209 sha
256=732d89a585ca502b9e375658a78b02d2e25bb9265ca424a04f159d53e098c9b9
  Stored in directory: /home/kali/.cache/pip/wheels/50/c4/3c/6fb797c8b35d61411c595e7b2074dc657e4395a
7ff525bbace
Successfully built pyminizip
Failed to build aiohttp reportlab
ERROR: Could not build wheels for aiohttp, which is required to install pyproject.toml-based project
s
```

Obrázek 9: Chyba kompilace Caldera frameworku Zdroj: Vlastní

Problém vyplývá ze starších balíčků, které Caldera vyžaduje pro svoji funkčnost. Je zřejmé, že nejnovější verze pip3 a python3 je již plně nepodporují, což vede k chybám kompilace. Nabízí se několik řešení, jak problém vyřešit. Prvním a velmi líným řešením je oznámit problém a počkat na vydání nové verze. Toto řešení zachovává stabilitu systému a frameworku, je to však na úkor času. Autoři Caldery mají nejlepší znalosti a možnosti otestovat, zda změny v závislostech neovlivnily správnou funkčnost frameworku. Z časových důvodů to však není pro tuto práci možné. Dalším možným řešením je změna verze pythonu pro celý systém. To je však velmi drastický zásah do celého systému a mohl by vézt ke ztrátě stability aplikací nebo dokonce celého systému. Realističtější možností je vytvořit virtualizaci pythonu a využívat nižší verzi pythonu pouze pro specifické aplikace, v tomto případě pro Calderu. Caldera je však složitá aplikace využívající nestandardní serverovou strukturu. Není tak zajištěno, že se při zkompilování pod určitým pythonem aplikace nepokusí využívat systémovou vyšší verzi. Posledním řešením je zkusit identifikovat problematické balíčky a najít, zda existují novější kompatibilní verze. Problémem tohoto řešení je možná nefunkčnost aplikace v závislosti na tom, jak velký rozdíl je mezi verzemi balíčků. Lze však očekávat, že novější balíčky mají zpětnou kompatibilitu, není ale neomezená.

Výsledné řešení

Po porovnání přístupů se jako nejlepší řešení jeví využití novějších verzí balíčků. Virtualizace pythonu je druhé nejlepší řešení. Zde je však větší šance problémů, a tak slouží jako záloha v případě, že první řešení nebude fungovat. Identifikace problémových balíčků je jednoduchá přímo ze zpětné vazby při kompilování, jak je možné vidět na obrázku 9. Prvním problémovým balíčkem je **aiohttp**, který je ve verzi 3.8.1. V repozitáři balíčků je možné najít nejnovější **aiohttp** ve verzi 3.8.4. To je možné vidět na obrázku 10



Obrázek 10: Nejnovější verze balíčku aiohttp v repozitáři Pypi Zdroj: Vlastní

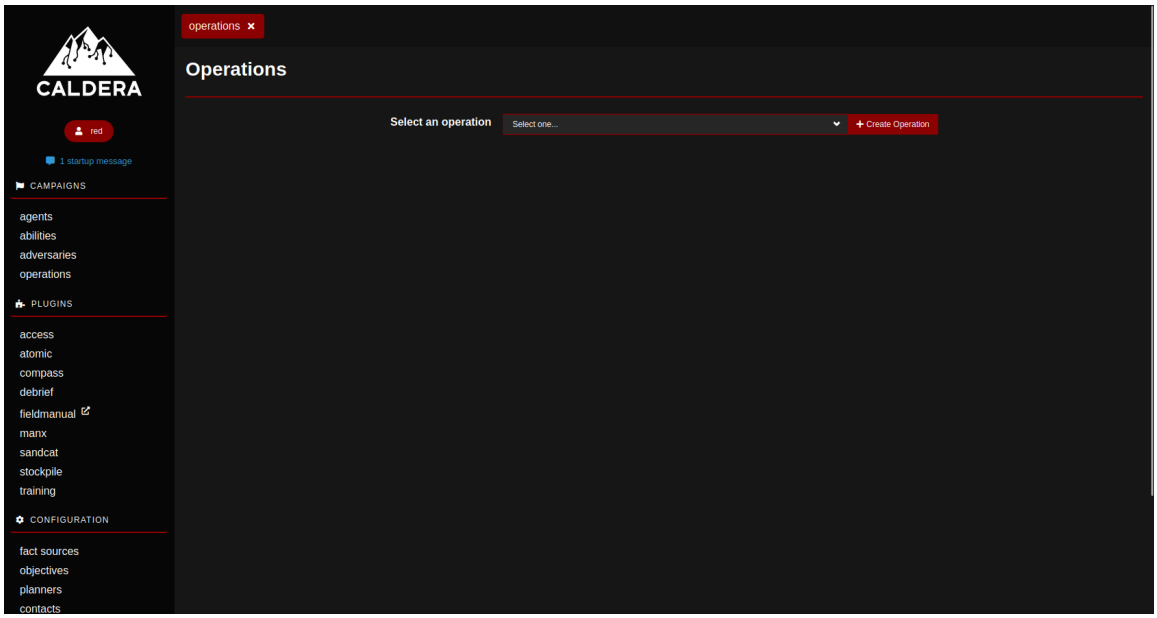
Po změně na tuto novou verzí byl identifikován další problémový balíček. Je jím **reportlab** ve verzi 3.5.67, ten je ale opět možné nahradit novější verzí 3.6.12. Následný pokus o zkompilování proběhl úspěšně. Upravený soubor s požadovanými balíčky je vidět na obrázku 11.

requirements.txt

```
aiohttp-jinja2==1.5.0
aiohttp==3.8.4
aiohttp_session==2.9.0
aiohttp-security==0.4.0
aiohttp-apispec==2.2.3
jinja2==3.0.3
pyyaml >= 5.1
cryptography >= 3.2,<37.0.0; python_version <= '3.7'
cryptography >= 3.2; python_version > '3.7'
websockets >= 10.3
Sphinx==5.1.1
docutils==0.16 # Broken bullet lists in sphinx_rtd_theme https://github.com/readthedocs/sphinx_rtd_theme/issues/1115
sphinx_rtd_theme==0.4.3
myst-parser==0.18.0
marshmallow==3.5.1
dirhash==0.2.0
docker==4.2.0
donut-shellcode==0.9.2
marshmallow-enum==1.5.1
ldap3==2.8.1
lxml~=4.9.1  # debrief
reportlab==3.6.12  # debrief
svglib==1.0.1  # debrief
Markdown==3.3.3  # training
dnspython==2.1.0
asyncssh==2.11.0
aioftp~=0.20.0; python_version >= '3.7'
aioftp==0.16.1; python_version < '3.7'
pyminizip==0.2.6
```

Obrázek 11: Nová podoba souboru requirements.txt Zdroj: Vlastní

Po spuštění serveru existuje propojení přes **localhost:8888**. I přihlášení pomocí základního uživatele **red** s heslem **admin** proběhlo úspěšně a tak lze předpokládat, že Caldera je funkční a připravena pro testování, viz 12.



Obrázek 12: Caldera framework po úvodním přihlášení Zdroj: Vlastní

9.1.2 Recon-ng

Zajímavým nástrojem, který byl připraven, ale nakonec nebyl využit, je *Recon-ng*. Jedná se o open-source OSINT nástroj v příkazové řádce. Díky volbě Kali Purple jako testovacího prostředí je jeho instalace opravdu snadná, stačí v příkazové řádce vykonat příkaz:

```
$ sudo apt-get install recon-ng
```

Ukázka kódu 1: Ukázka příkazu pro instalaci nástroje Recon-ng Zdroj: [Vlastní]

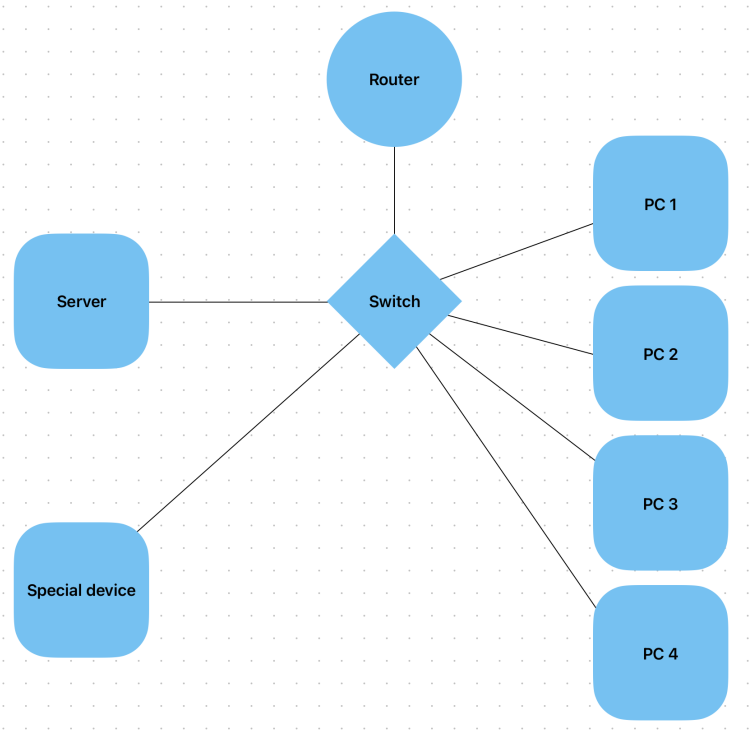
Zajímavějším a důležitějším krokem je však instalace modulů. Po zapnutí nástroje příkazem **recon-ng** je možné instalovat jednotlivé moduly přes marketplace. Všechny moduly je možné zobrazit příkazem **marketplace search**. Vybrané moduly jsou nainstalovány příkazem **marketplace install *"jméno_modulu"***. Při testování však byla zjištěna zastaralost a nefunkčnost důležitých modulů. Také ovládání tohoto nástroje je zvláštní a po otestování bylo od použití tohoto nástroje v testovaných scénářích odstoupeno. Recon-ng je totiž možné nahradit specializovanými nástroji a technikami, jako je například *Nmap*.

9.1.3 Nmap

Zde je důležitá právě volba Kali Purple jako testovacího prostředí. Nástroj Nmap je připraven již s instalací této distribuce a proto nebylo pro jeho používání nutné provádět žádné další kroky.

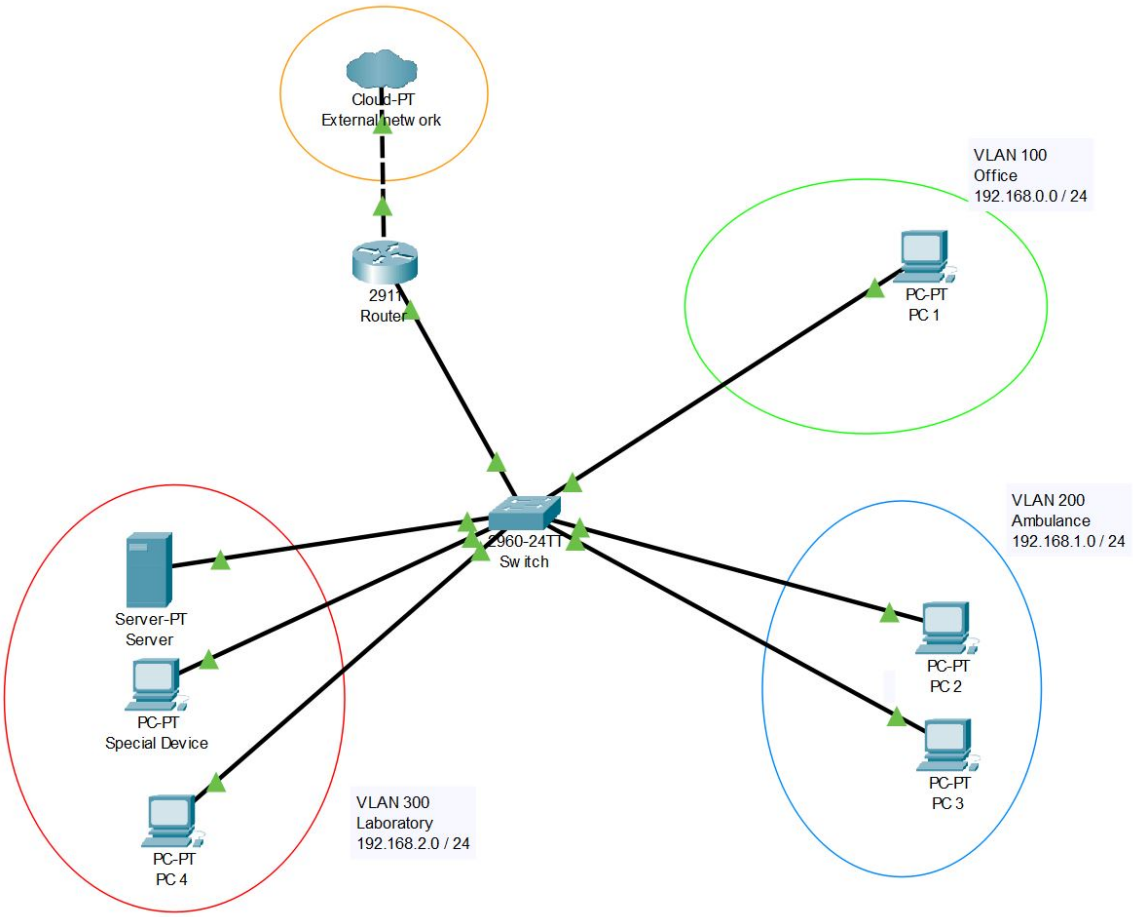
9.2 Popis testované infrastruktury

V rámci pokusu o simulování co možná nejreálnějšího testování bylo i testované prostředí vytvářeno na základě reálného. Vzniklo na základě dotazníku a po rozhovoru s odborníkem, který reálné prostředí udržuje. Je jasné, že simulované prostředí podléhá simplifikaci, byla však snaha zachovat všechny nejdůležitější prvky. Prvotní návrh topologie byl jednoduchý a reflektoval získaná data, viz obrázek 13.



Obrázek 13: Prvotní návrh testovaného prostředí Zdroj: Vlastní

Posléze byl vymodelován v programu Cisco Packet Tracer do použitelného návrhu prostředí. Je jasně vidět zachování základní myšlenky, byly ale přesně definované prvky topologie a jejich vlastnosti jako IP adresy koncových stanic, rozsahy jednotlivých sítí a zařazení do VLAN (Virtual Local Area Network) skupin. V rámci programu Packet Tracer byla také na prvcích provedena potřebná konfigurace a otestování funkčnosti. Model prostředí je na obrázku 14.

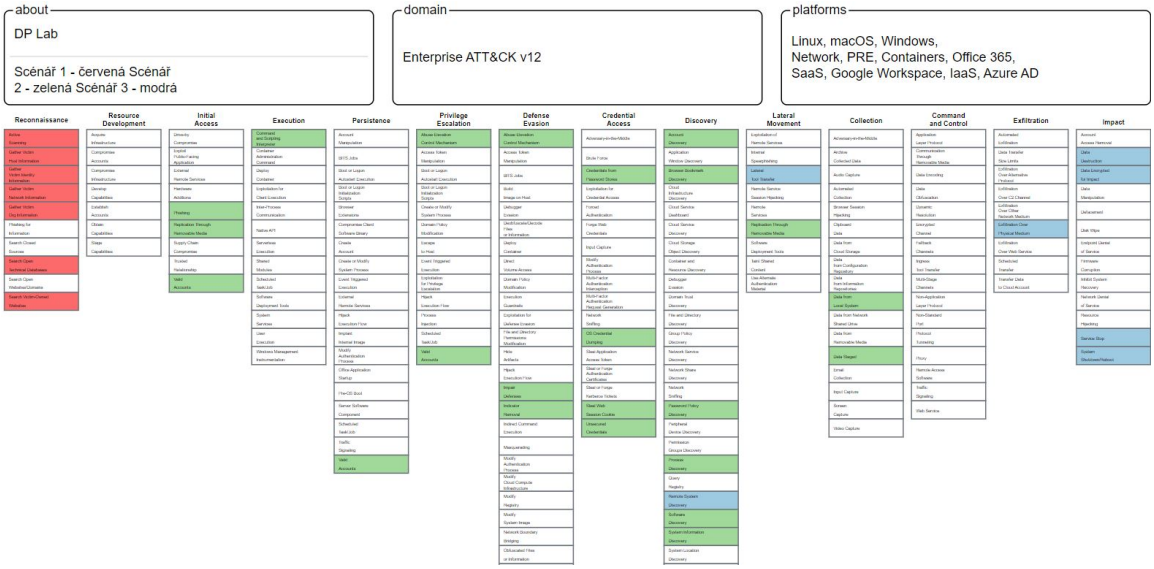


Obrázek 14: Návrh prostředí v Cisco Packet Tracer Zdroj: Vlastní

Posledním krokem je implementace infrastruktury na skutečných zařízeních. Za tímto účelem byla využita síťová laboratoř J-5 Univerzity Hradec Králové. Specificky bylo využito 6 počítačů v učebně, router Cisco 2911 a switch Catalyst 2960. Jeden z počítačů funguje jako simulační server, kde jsou ve virtuálním prostředí nasazeny 2 samostatné serverové implementace – *Windows Server 2012 R2* a *Ubuntu Server 20.04.4 Focal Fossa*. Nasazení infrastruktury s použitím fyzických zařízení opět vyžaduje otestování správného propojení všech komponentů. Důležitým bodem je hlavně možnost komunikovat se servery ve virtuálních prostředích. Proto bylo otestováno u každého zařízení postupně připojení sama na sebe, připojení na switch a router, připojení na ostatní prvky v daném VLAN a nakonec komunikace s prvky v ostatních VLAN. Po úspěšném otestování všech zařízení je možné považovat infrastrukturu za připravenou pro testování v labech.

10 Testované scénáře

Cílem této kapitoly je představit práci s nástroji a simulovat útok na vybranou organizaci. Byly za tímto účelem vybrány hrozby a vytvořeny scénáře, které na sebe volně navazují a představují možné kroky útočníka. Je však nutné podotknout, že každý útok je jedinečný, a proto není možné vytvořit jeden testovací, který reprezentuje všechny možnosti. Je však možné ukázat nejčastější kroky, poukázat na jejich návaznost a připravit potencionální obránce tak, aby byli schopni s pomocí již zmíněných nástrojů vytvořit vlastní scénáře pro jejich specifické potřeby a testování. Na obrázku 15 je možné vidět barevné znázornění reprezentace jednotlivých scénářů.



Obrázek 15: Barevné označení jednotlivých scénářů Zdroj: Vlastní

10.1 Scénář 1 – *Recon*

První scénář je zaměřen na práci s informacemi. Jen velmi malé množství útoků probíhá bez prvotní fáze získávání informací a drtivá většina z nich je neúspěšná právě kvůli tomu, že útočníci podcenili tento první krok. Sběr informací lze provádět mnoha způsoby. V dnešní moderní době není problém informace získat, je však problém určit, která informace je důležitá a která ne. Nejjednodušší řešení je zakoupit informace na černém trhu, dokonce existují balíčky informací setříděné právě pro přípravu útoků. To však není cílem tohoto scénáře. Cílem je ukázat vybrané techniky a nástroje, pomocí kterých získávají útočníci OSINT, neboli volně dostupné informace. Sběr informací je prováděn na již zmíněném reálném cíli, podle něhož je i modelováno testovací prostředí. Z důvodu zachování anonymity vybraného cíle nebudou v práci zveřejňována specifická data, ale pouze typ nalezeného údaje nebo záznam, který není identifikovatelný. Příkladem je nalezení webového serveru.

Je možné říci, že byla nalezena IP adresa a specifický operační systém serveru. Je také možné říci, o jaký operační systém se jedná. Je však nežádoucí zmínit přesnou verzi systému nebo již zmíněnou IP adresu.

10.1.1 Internet

Je překvapivé, kolik dat o cíli může útočník získat čistě pomocí vyhledávání na internetu. Nejen, že cíl provozuje webové stránky, dokonce v porovnání s dalšími stránkami podobných organizací vyplynulo, že mají jiného jednotného správce a jsou pouze upravovány z jednotné šablony. Lze tedy očekávat, že problémy nalezené na jedné implementaci šablony budou platit pro všechny. Bylo proto využito veřejných databázových repozitářů **WHOIS** a **CenSys** pro zjištění více informací. V technických databázích byly o doméně organizace zjištěny následující údaje:

- zkrácená jména administrátorů domény,
- datum registrace domény,
- kontakt na administrátory systému – jméno, adresa, název organizace,
- název organizace, pod kterou je doména zaregistrována.

To jsou informace, které sice nevedou přímo k útoku, ale ukazují na osoby a organizace, na než je dobré se více zaměřit. Není nutné tedy hledat slepě, ale je pro potencionálního útočníka jasné, jakým směrem se vydat. Zde lze například při využití běžného vyhledávače DuckDuckGo a sociálních sítí LinkedIn a Facebook údaje o administrátorovi. Například bylo možné nalézt osobní i pracovní emailovou adresu (vhodné pro phishing), místo bydliště a pracovní i osobní telefonní číslo (Vishing). Třešničkou na pomyslném dortu však byla anonymizovaná smlouva podepsaná daným administrátorem. To by samo o sobě nebyl problém, pokud by nestačilo začernalý text označit a překopírovat do editoru, kde je již vidět ten stejný obsah v plaintextové formě.

10.1.2 Censys

Pro kontrolu a doplnění informací bylo využito platformy Censys. Tato platforma je schopná po zadání doménového jména nebo IP adresy serveru najít informace o službách a portech, na kterých služba komunikuje. Je jasné, že tato platforma nemůže nahradit plnohodnotný nástroj jako Nmap, je však dostupná online a není nutné instalovat další nástroje. Pomocí platformy Censys byly nalezeny 2 důležité záznamy – *webový server* a *emailový server*. Záznam o *webovém serveru* poskytuje informace o IP adrese, provozovaném operačním systému (Ubuntu) a veřejných portech. Na portech 80 a 443 je již zmíněná internetová stránka, zajímavější jsou však porty 500, kde je protokol IKE (Internet Key Exchange), a 10443,

kde se nachází webová služba. Při zadání adresy do prohlížeče je uživatel přesměrován na přihlášení do systému od společnosti Sophos. Tato společnost se zabývá vytvářením bezpečnostního software a monitorováním bezpečnosti klientů. Lze tedy očekávat, že na portu 10443 je vzdálený přístup právě pro tyto účely. Záznam o *emailovém serveru* také obsahuje zajímavé informace, jako například reverzní DNS záznam, operační systém serveru (FortiOS) a také port 10443, jehož prozkoumání vede do přihlašovacího formuláře společnosti fortinet. Jedná se tedy opět o možnost vzdáleného přístupu a u obou serverů je tedy možné získat přístup pomocí supply-chain útoků.

10.1.3 Nmap

Nástroj pro aktivní skenování portů *Nmap* je dlouhodobě využívaný nástroj mnoha útočníků i obránců, a tak je dobré vědět, co s ním jde o daném cíli zjistit. Pro zahájení skenování je nutné zadat potřebné vlastnosti skenu a definovat cíl. Cílem je samozřejmě již zmíněná organizace, Nmap přijímá informace o doméně, jedné nebo i skupině adres, což jsou informace nalezené v předchozím kroku. Nutné je specifikovat možnosti skenování portů, je například možné získat informace o aktivních portech, protokolech, spuštěných službách a jejich verzích. V rámci sbírání přehledných dat bylo také nastaveno, aby po ukončení práce Nmap vyexportoval výsledek do textového souboru.

```
# nmap -v -A -p- -sV -version-all -O -oN vysledek.txt "cíl_útoku"
```

Ukázka kódu 2: Ukázka příkazu pro Nmap Zdroj: [Vlastní]

Výše ukázaný příkaz byl proveden a výsledek byl vypsán do souboru **vysledek.txt**, což je nastaveno přízviskem **-oN**. Příznak **-v** označuje vyšší level podrobnosti, takzvané verbosity. Pro detekci operačního systému a detekci verzí je využito příznaku **-A** a příznaku **-O**. K detekci portů slouží **-sV -version-all**, v němž -version-all znamená testování všech možností. Pro skenování portů slouží **-p-**, což je zkratka pro explicitní skenování všech portů. Výsledek tohoto scanu potvrdil již nalezené informace, ale také tyto znalosti rozšířil o nové poznatky. Obzvláště zajímavá je verze webového serveru, na které je spuštěn internetový portál. Jedná se o totiž o starší verzi serveru Apache vydanou v roce 2017. Tato informace dává útočníkovi možnost nalézt zranitelnosti pro tuto specifickou verzi a je to tedy značným bezpečnostním rizikem. Posledním zajímavým poznatkem bylo nalezení portu 5060 s protokolem SIP a port 8443 se službou OpenVPN.

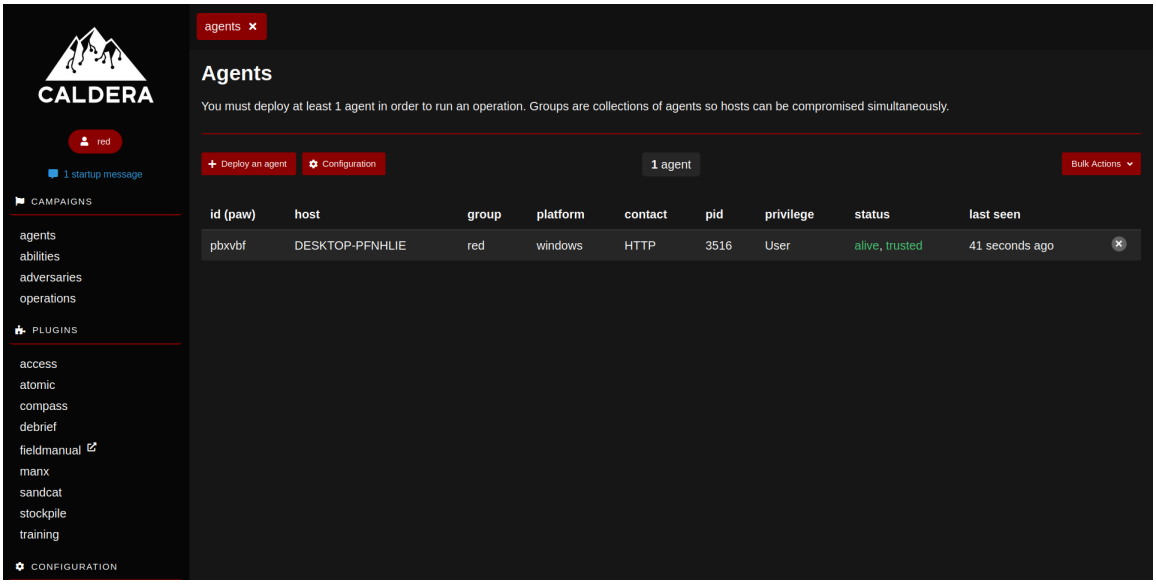
10.2 Scénář 2 – *Discovery* a *Elevate-privileges*

Scénář 2 navazuje na scénář 1. Snahou je simulovat možné kroky útočníka poté, co provedl sběr informací o cíli. Cílem útočníka je tedy využít získaná data ve svůj prospěch a provést kompromitaci systému. Jak již bylo zmíněno v teoretické části textu, jedním z

nejpoužívanějších vektorů pro prvotní kompromitaci systému je *phishing*. Útočník využije již získaných dat ze scénáře 1 pro vytvoření *phishingové kampaně*, jejímž cílem je kompromitovat zařízení. Pro účely scénáře 2 uvažujeme, že se útočníkovi tímto vektorem povedlo získat prvotní vstup, je totiž velmi obtížné simulovat phishing v laboratoři. Jeho založení na psychologii a zranitelnostech lidského chování lze sice jednoduše napodobit, nemá však velký vypovídající význam. Pro účely testování tedy uvažujeme, že běžný uživatel klikl na podvodný email, který útočníkovi poskytl vzdálený přístup k jeho zařízení. Důležité je, že se jedná o běžného uživatele. V pozdějších částech tohoto labu je ukázáno, jaký je rozdíl v možnostech útočníka v případě, že by se jednalo o privilegovaného uživatele. Tento scénář bude simulován na již popsané testovací infrastruktuře. V roli útočníka bude působit Caldera, jakožto nástroj pro testování. Za zmínku stojí fakt, že většina infrastruktury obsahuje nejnovější operační systémy. Výjimkou jsou servery, kde lze očekávat dlouhodobě podporovanou starší verzi operačního systému. Pozor však na fakt, že na všechna zařízení byly, v rozumné míře, uplatněny bezpečnostní aktualizace. To znamená, že tato infrastruktura je proti útokům stejně odolná, jako nejlepší možná varianta skutečné infrastruktury. Pokud však správce skutečné infrastruktury podcenil aktualizace zařízení, lze očekávat, že bude na útoky náchylnější. Výsledkem je tedy nelichotivá komparace testovací a skutečné infrastruktury. Pokud se útok povede na testovací infrastruktuře, zcela jistě ho bude možné provézt i na skutečné. I nevydařený útok na testovacím prostředí má však šanci na skutečné infrastruktuře uspět. Tento fakt pouze svědčí o tom, že je nutné aktualizovat zařízení z důvodu optimální bezpečnosti.

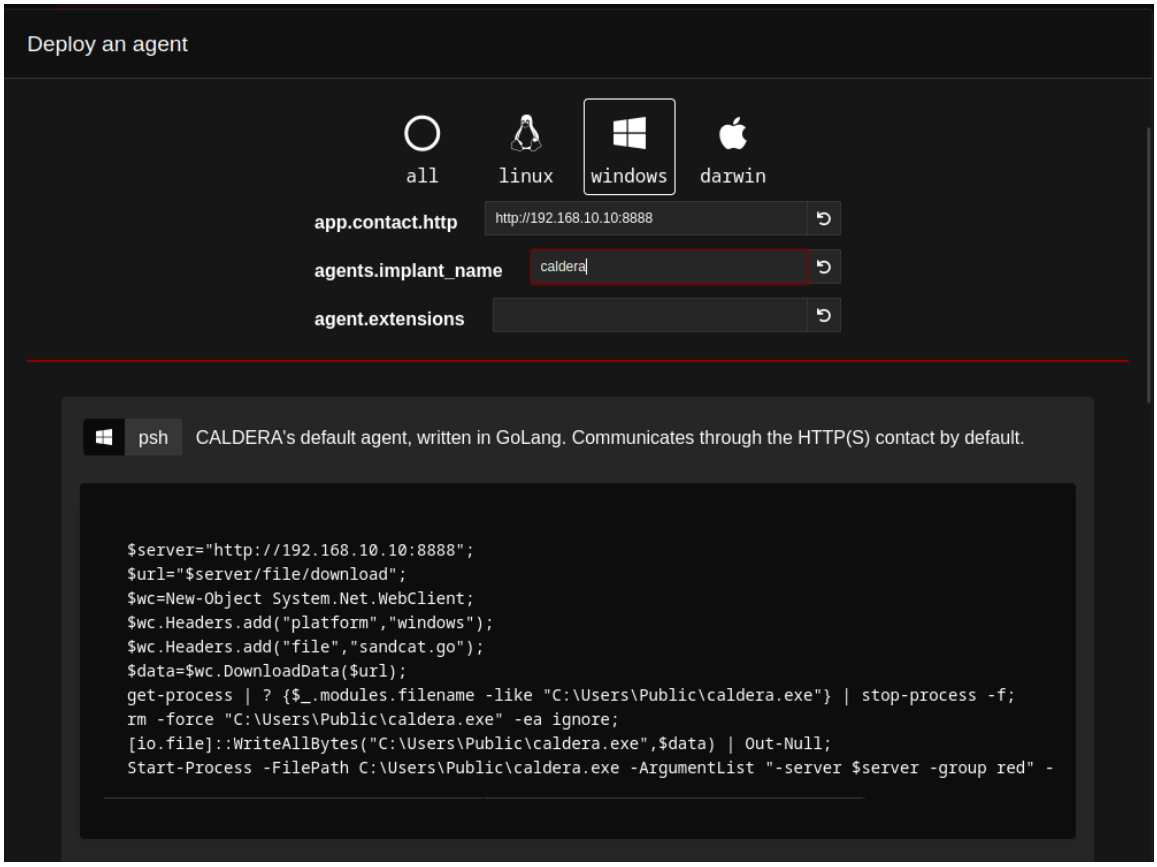
10.2.1 Příprava scénáře

Pro simulaci scénáře je nutné připravit agenta v testovacím nástroji Caldera. Tento agent pak simuluje kompromitování zařízení a provádí testování, které mu nastavíme. V Caldeře je možné sledovat a vytvářet agenty v záložce agents, viz obrázek 16.



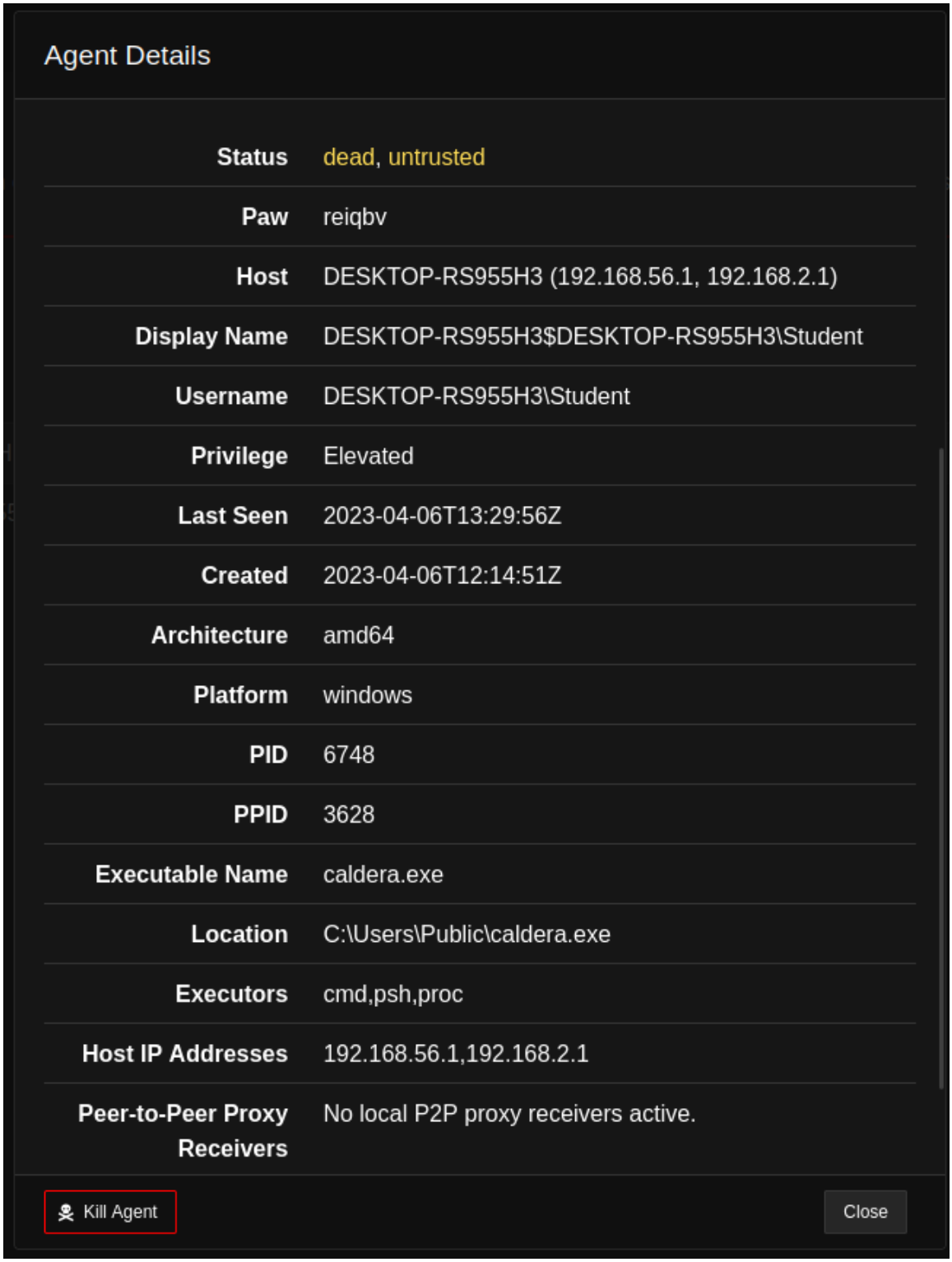
Obrázek 16: Stránka pro ovládání agentů Zdroj: Vlastní

Agenta lze vytvořit stiskem tlačítka *deploy an agent*. Po stisknutí je uživateli představen formulář pro bližší specifikaci agenta, viz obrázek 17. V tomto formuláři je nutné nastavit platformu a kontaktní adresu Caldera serveru. Vhodné je také změnit *implant_name*, což je název, pod nímž bude agent vidět na infikovaném stroji. V rámci testování bylo použito jasně rozeznatelné jméno **caldera**. Pro složitější testování, kde se snaží útočníci red teamu vyhnout detekci členy obrany v blue teamu by mohlo být zvoleno méně nápadné jméno, jako například **svchost**. Na obrázku jsou pak také vidět příkazy, které je nutné spustit na simulovaném napadeném zařízení pro instalaci a nastavení agenta. Existuje několik verzí příkazů, pro tuto práci jsou však aplikovatelné příkazy na obrázku 17, které jsou určené pro windows powershell. Po provedení příkazů agent sám naváže komunikaci se serverem Caldera. Agent navíc pravidelně ohlašuje svoje informace serveru, a to až do doby svého ukončení. Caldera naopak o agentovi vede záznam a může mu posílat instrukce.



Obrázek 17: Formulář pro vytvoření agenta Zdroj: Vlastní

Na obrázku 16 je možné vidět již vytvořeného agenta připraveného pro další testování. Za povšimnutí stojí všechny údaje, které jsou s agentem spojené. Základní údaje jsou *id* a *host*, které agenta jednoznačně identifikují. *Platform* identifikuje, na jaké platformě je agent spuštěn. Nejdůležitější údaje jsou však *group* a *privilege*. *Group* označuje pracovní skupinu, do níž agent patří. To je důležité pro spouštění operací, kde právě pomocí *group* určujeme, kteří agenti mají operace vykonávat. *Privilege* určuje, jaká práva má agent na daném zařízení. **User** znamená, že tento agent byl spuštěn běžným uživatelem a zdědil tak jeho základní práva. Pokud by agenta spustil privilegovaný uživatel, v této kolonce by bylo označení **elevated**, jak je možné vidět na pozdějším obrázku 18. Je také možné identifikovat, jak s Caldera serverem agent komunikuje pomocí atributu *contact*. Poslední důležité údaje vypovídají o stavu agenta [*status*] a informací o čase posledního kontaktu agenta se serverem [*last seen*]. Samozřejmě existuje i podrobnější výpis přímo po rozkliknutí agenta, viz obrázek 18. Za povšimnutí zde stojí informace, které mohou být využitelné pro útočníka. Jsou jimi *host IP addresses, architecture* a primárně *executors*. Důležité je tlačítko *kill agent*, kterým se zastaví funkčnost agenta. Černý křížek na hlavní stránce agentů, viz obrázek 16, nezpůsobí ukončení agenta, ale pouze ho odstraní ze seznamu agentů. Stále fungující agent se proto v tomto seznamu znovu objeví při jeho další komunikaci se serverem.

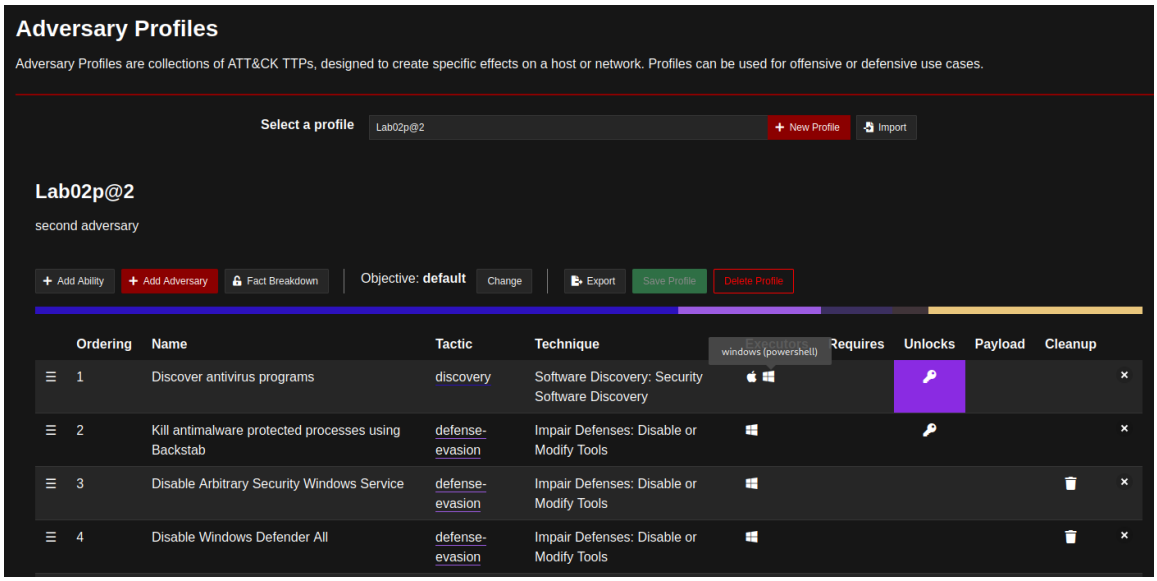


Obrázek 18: Detaily specifického agenta Zdroj: Vlastní

Výběr chování při útoku – *Adversary*

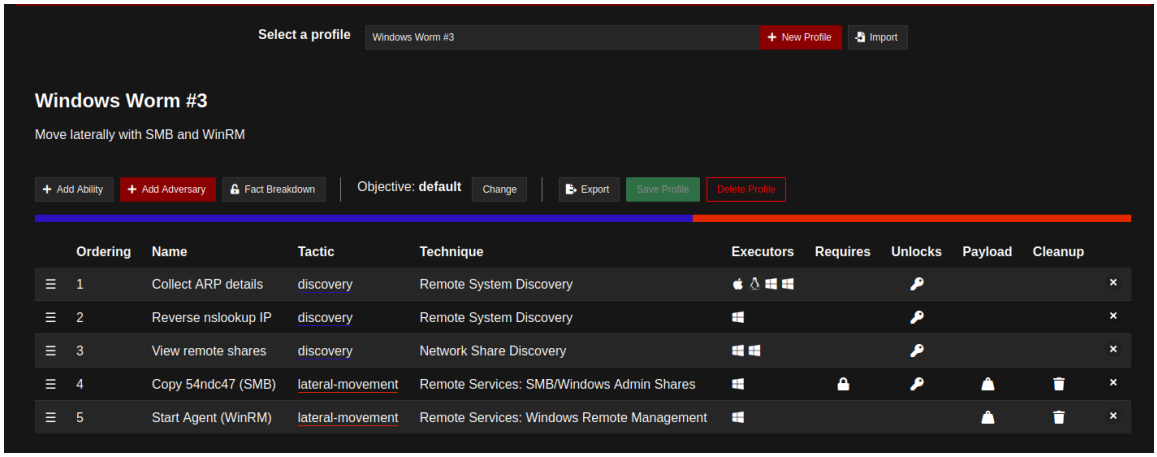
Dalším důležitým krokem je příprava chování útočníka. To je v Caldeře simulované pomocí

takzvaných *adversaries*. *Adversary* je simulovaný útočník, kterému je možné vybrat techniky, které bude v operaci provádět. To je možné vidět na obrázku 19. Jak již bylo zmíněno, Caldera je založena na frameworku Mitre ATT&CK, proto je možno u *adversaries* vybírat techniky podle taktik z Mitre ATT&CK.



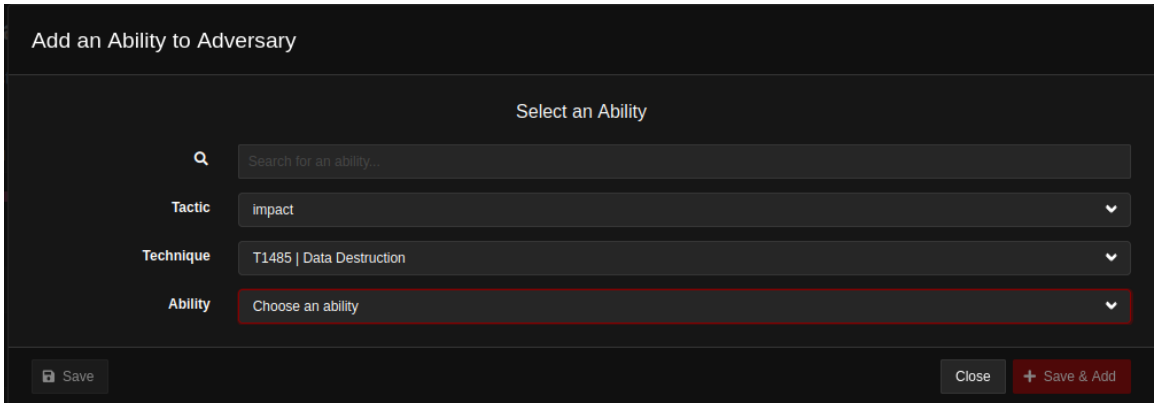
Obrázek 19: Ukázka technik u simulovaného útočníka Zdroj: Vlastní

Nový *adversary* je vytvořen pomocí tlačítka *new profile*. To otevře formulář pro vyplnění názvu a popisu tohoto profilu útočníka. Poté je nutné přidat techniky, které bude tento útočník provádět. To lze udělat dvěma způsoby. Prvním je přidání technik jiného profilu pomocí tlačítka *add adversary*. Samozřejmostí je výběr technik, které lze z jiného profilu přidat. Pokud tedy existuje profil z velké části odpovídající potřebám testování, toto je nejrychlejší volba, jak bez úpravy původního profilu lze vytvořit nový. V Caldeře existuje mnoho před-připravených profilů útočníka, příkladem může být worm, viz obrázek 20, který dokonce existuje v několika podobách s minimálními úpravami. Je tak na zvážení, zda vytvářet nového útočníka zcela od začátku nebo využít jednu z před-připravených šablon a na ní dále stavět.



Obrázek 20: Příklad předpřipraveného adversary Zdroj: Vlastní

Druhým způsobem přidávání technik je tlačítko *add ability*, kde přidáváme jednotlivé požadované techniky. Jak je vidět na obrázku 21, vyhledávání technik lze provádět dvěma způsoby. Pokud je známo jméno techniky nebo alespoň přibližné zaměření, lze použít přímé vyhledávání technik. Naopak pokud je vyžadováno využití určité taktiky, je možné vyhledávat selektivně podle nich. Volba taktiky pak vede k volbě technik vedoucím na volbu sub-technik nebo specifických provedení dané techniky. Tímto způsobem může dále upravovat chování útočníka na bázi jednotlivých technik.



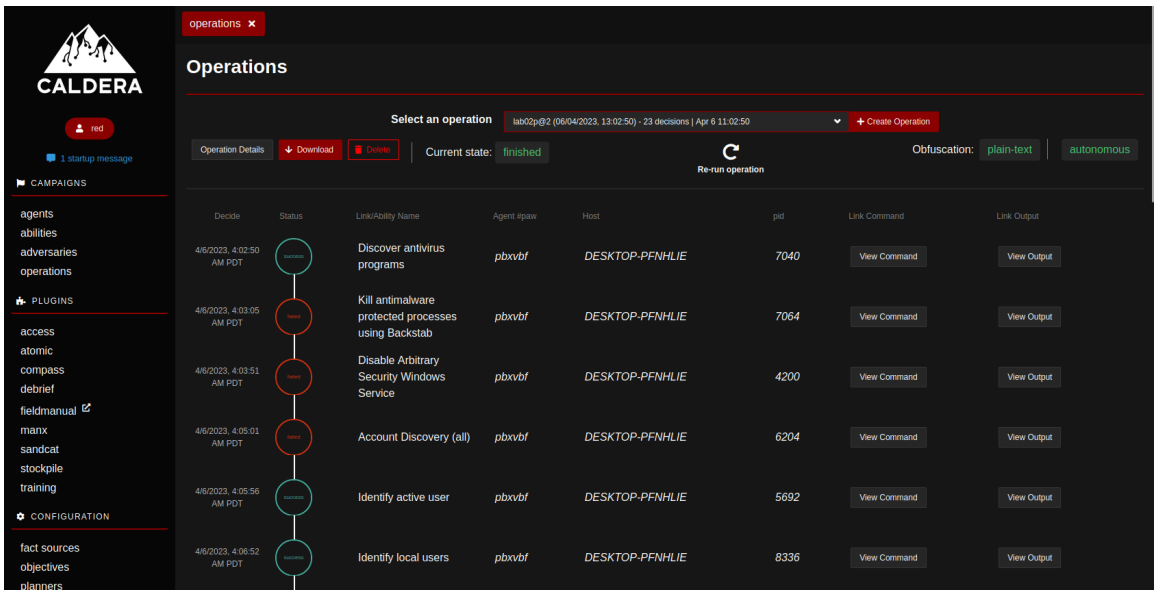
Obrázek 21: Ukázka výběru technik Zdroj: Vlastní

Adversary pro scénář 2

Pro scénář 2 byli vyzkoušeni 2 hlavní profily útočníků, které byly pojmenovány *Lab02* a *Lab02v2*. Pro přehlednost budou i operace pojmenované podle *adversary*, který v nich figuruje. Operace *Lab02* je zaměřena na rozsáhlé testování. Předpokládáme útočníka, který nezná vnitřní prostředí a jeho cílem je získat co nejvíce informací a vyzkoušet základní a pro útočníka přínosné taktiky. *Adversary* pro tuto operaci obsahuje 74 technik. Útočník v operaci *Lab02v2* využije znalosti z předchozí operace a pokusí se dosáhnout specifických

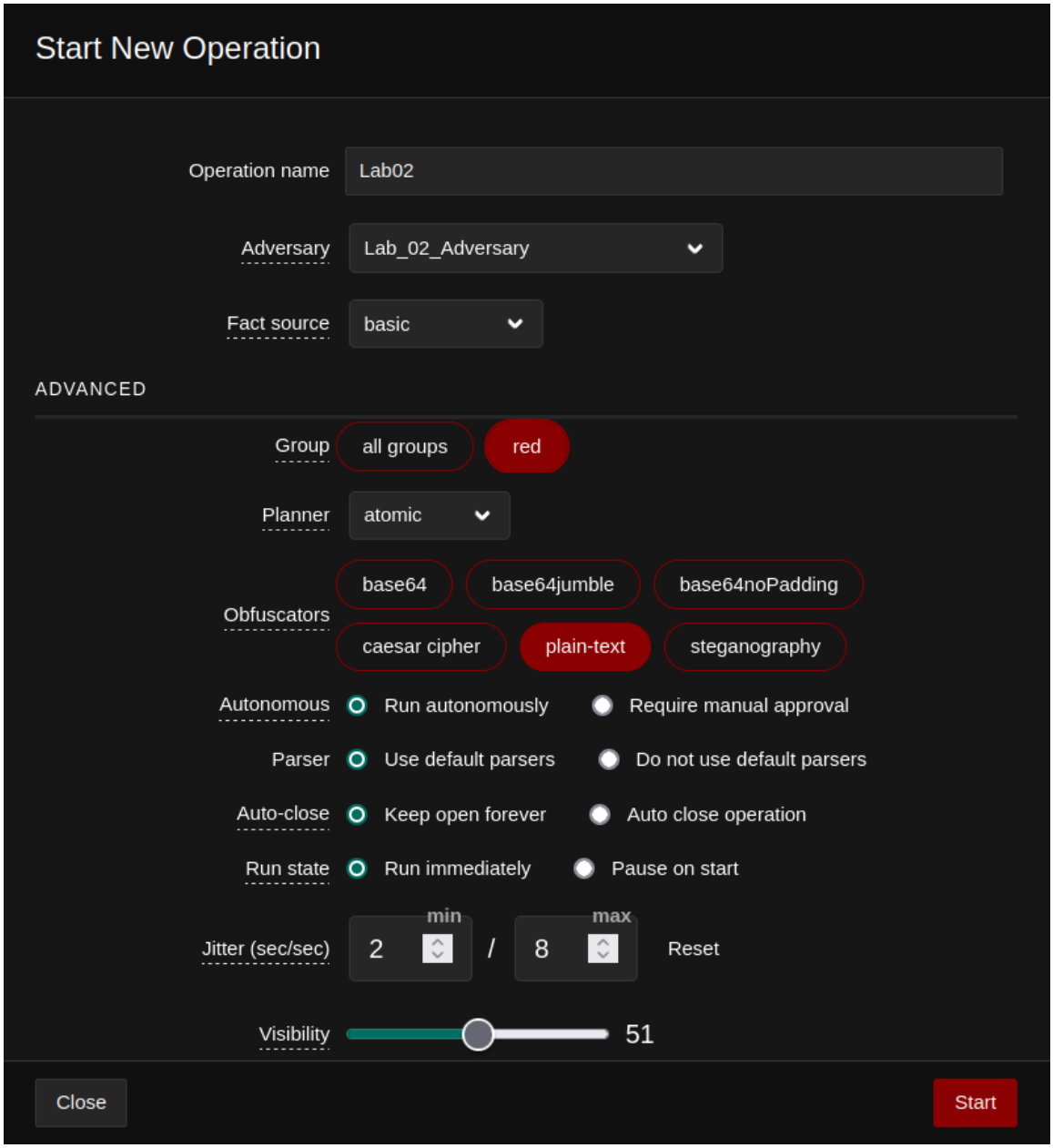
cílů. V tomto případě se jedná specificky o získání privilegií administrátora a vypnutí monitorování. Tento útočník proto obsahuje 31 technik zaměřených právě k tomuto záměru.

10.2.2 Spuštění operace



Obrázek 22: Ukázka správy operací Zdroj: Vlastní

Finálním krokem testování je spuštění operace. K tomuto účelu v Caldeře slouží záložka *operations*, viz obrázek 22. Zde je možné spouštět nebo vytvářet nové operace, ale zároveň tato záložka slouží pro správu již uskutečněných operací. Zachovávají se zde informace o průběhu operace a případných výstupech z daných technik. Jelikož již bylo připraveno vše pro správnou činnost operace, je na čase kliknout na tlačítko *create operation*, čímž je vyvolán formulář pro tvorbu nové operace, viz obrázek 23. Je zde několik důležitých nastavení. Jméno operace a nastavení požadovaného *adversary* je přímočaré. *Fact source* je zajímavější, jedná se o před-připravené poznatky, například o testovaném zařízení, které lze přímo zadat nebo použít zjištěné z předchozích operací. V rozšířené sekci se pak nachází složitější nastavení. Jsou zde nastavení pro cílovou skupinu[*group*], tedy určení, kteří agenti mají provádět úkony útoku zadané v *adversary*. *Planner* určuje, jak budou operace prováděny. Základním je **atomic**, který posílá jednotlivé příkazy jeden po druhém ve stejném pořadí, v jakém se nachází v *adversary*. Lze však vytvořit vlastní *planner* s rozdílným chováním[51]. V neposlední řadě se zde nachází přepínače pro řízení chodu operací a možnosti zakódovaní a skrytí operace.



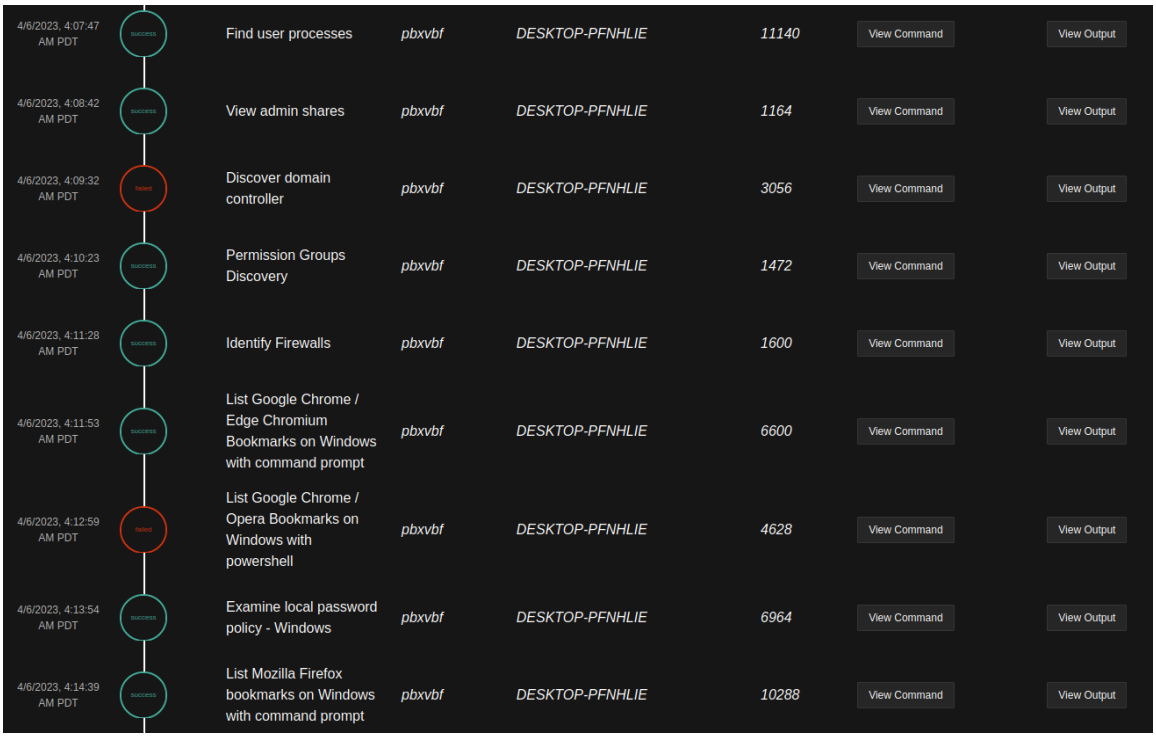
Obrázek 23: Ukázka tvorby operace Zdroj: Vlastní

Pro účely této práce jsou všechny operace nastaveny na automatické spuštění při vytvoření a také automatické uzavření a kolekci dat. Automatické spuštění je zřejmé, již máme připraveny všechny stavební bloky pro vykonání operace, a tak není třeba nic dalšího připravovat a čekat. Automatické uzavření a kolekce vyplývá z faktu, že se jedná o kompletní operace, nechceme v běhu operace přidávat další kroky ani přistupovat k napadenému zařízení na přímo a vykonávat vlastní příkazy. V rámci automatizace je tedy výhodnější zvolit možnosti automatického uzavření a kolekce dat, protože není nutné hlídat, zda se již provedly všechny požadované kroky operace a je nutné zadat příkaz pro uzavření operace. Z

pohledu efektivity to také uvolňuje čas testovatele, který může během průběhu jedné operace vytvářet jinou nebo zkoumat data z jiné operace. Pro referenci, operace může běžet i několik hodin, a pokud tedy není dozor nutný, je dobré se mu vyhnout.

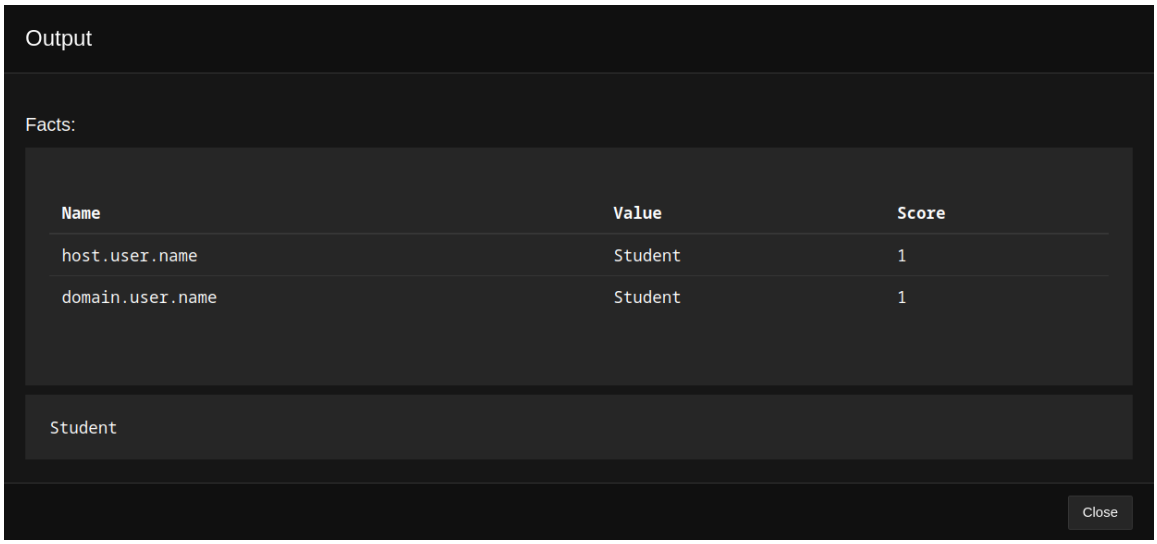
10.2.3 Lab02

První z připravených operací má název *Lab02*. Jak již bylo zmíněno, cílem je simulovat prvotní kroky útočníka v nově infikovaném systému. Útočník má v tuto chvíli o systému pouze minimální informace. Proto lze předpokládat, že se pokusí co nejvíce informací získat. Důvod, proč byla vybrána pro první scénář tato situace, je vyzkoušení možností samotné Caldery. Z tohoto důvodu operace pro *lab02* provádí 74 technik zaměřených na zisk dat, která by běžného útočníka zajímala. Cílem je vyhodnotit, jaká data je pro útočníka jednoduché získat a kde je naopak jeho snaha zastavena. Výhodou pro testovatele je zde barevné značení technik Caldery, jak je vidět na obrázku 24. Rozlišuje 3 barevné stavy techniky, červená barva pro neúspěch, zelená pro úspěch a žlutá pro právě provádějící operaci. Je však nutné dávat pozor na fakt, že úspěšná operace nemusí vždy vracet očekávaná data. Také definice úspěšnosti může být u některých technik pro nezkušeného operátora Caldery zvláštní. Například se stalo, že Caldera vyhodnotila techniku o kontaktování DNS jako úspěšnou, i když celá infrastruktura DNS nevyužívá. Tyto případy jsou však ojedinělé a není problém je nalézt, pokud nastanou.



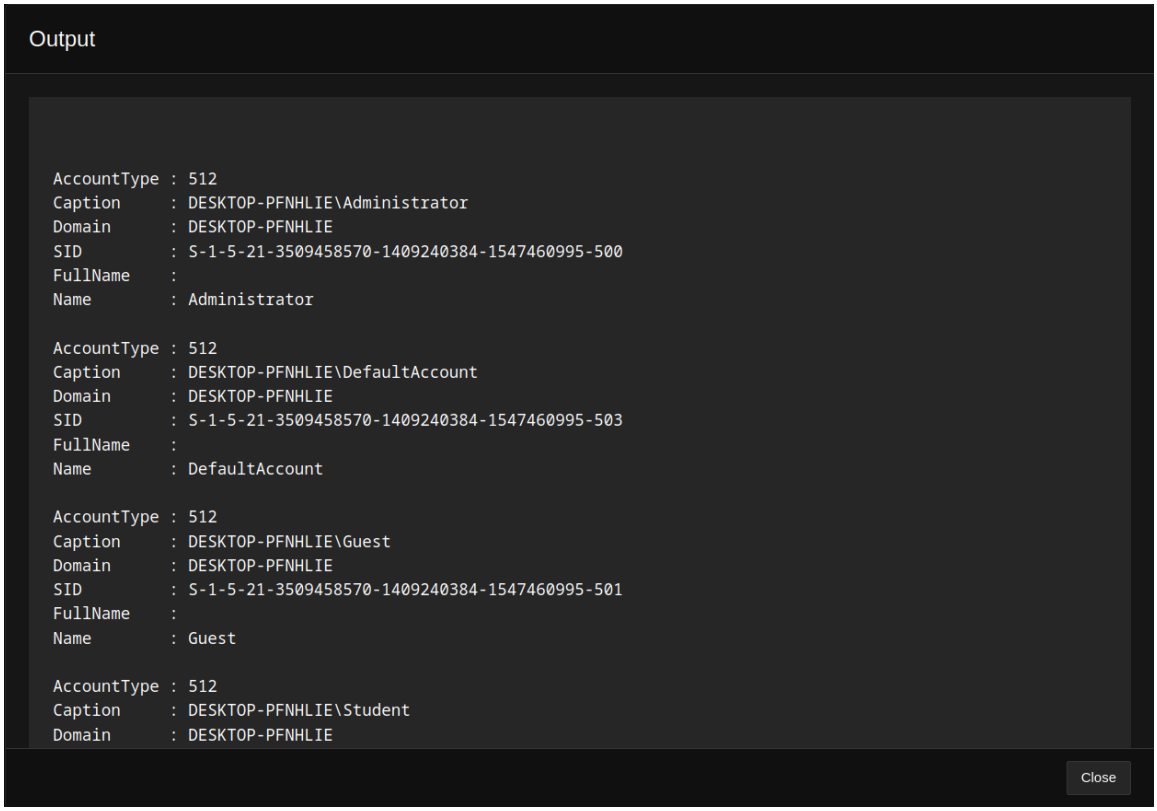
Obrázek 24: Ukázka probíhající operace Zdroj: Vlastní

Je jasné, že pro útočníka existují úrovně dat, jenž jsou řazené podle složitosti zjištění, složitosti pochopení nebo důležitosti. Proto i v simulované operaci můžeme vidět, že útočník se nejdříve zaměřil na snadno zjistitelná data s nízkým rizikem odhalení. Příkladem je jméno uživatele a jeho doména, viz obrázek 25.



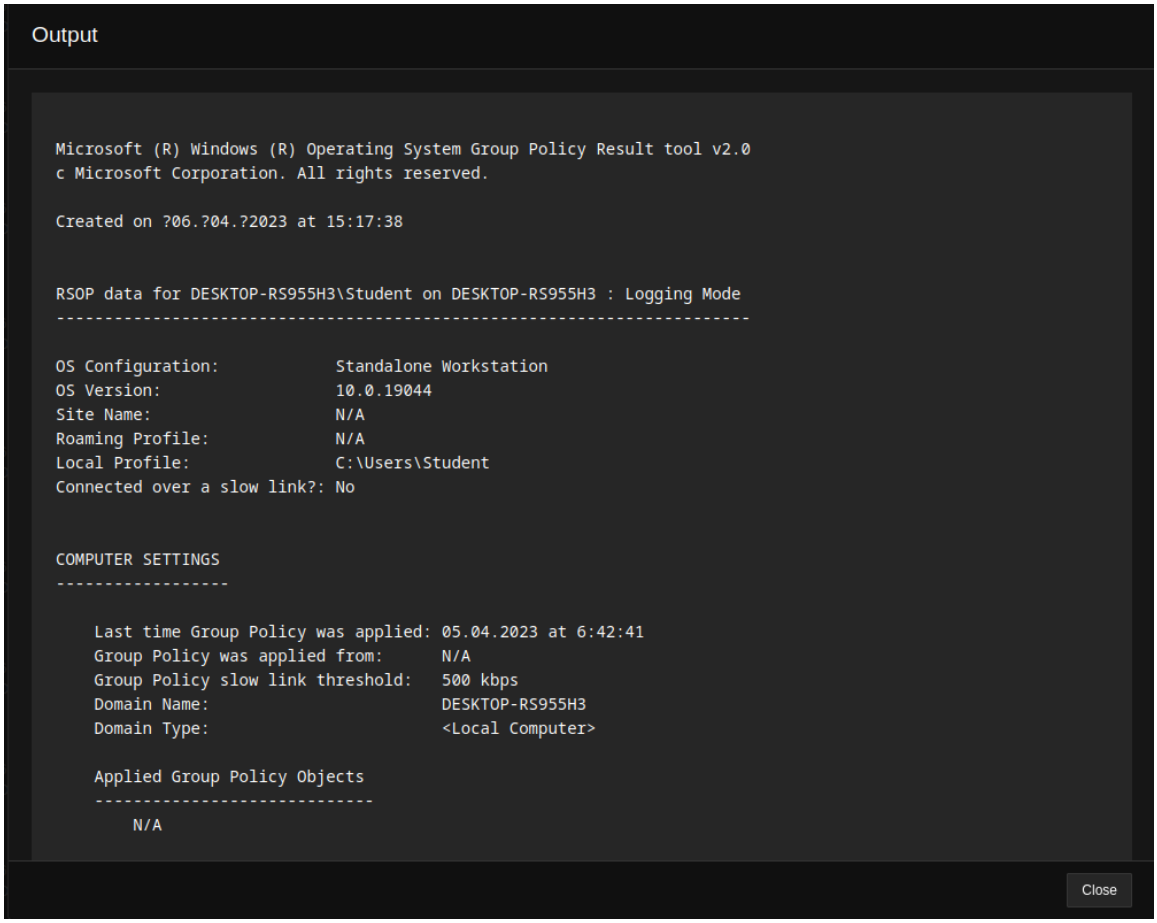
Obrázek 25: Výstup taktiky pro zjištění uživatele a jemu příslušné domény Zdroj: Vlastní

Dalším krokem může být zjištění všech účtů na daném zařízení. Tato informace může vypovídat o počtu uživatelů, kteří se k zařízení běžně přihlašují, ale i jestli v organizaci existuje striktní metodologie vytváření přihlašovacích jmen. Třešničkou na pomyslném dortu jsou účty typu *Admin* nebo *Guest*, kde velmi často dochází k porušení praktik dobrých hesel. Není neobvyklé, že tyto účty mají hesla stejná jako jméno, nebo v případě účtů Admin je stejné heslo pro všechna zařízení. Kompromitace jediného Admin účtu by tak kompromitovala všechna zařízení s tímto účtem. Výstup z techniky pro zjištění bude vypadat jako výstup na obrázku 26.

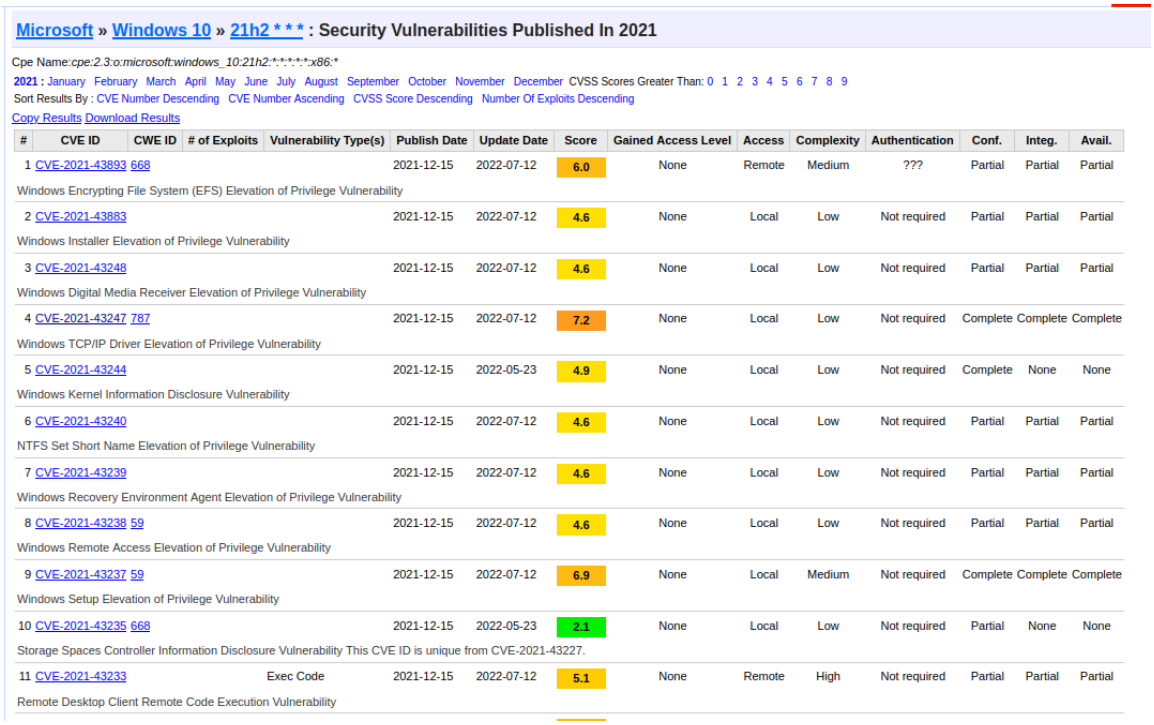


Obrázek 26: Výstup taktiky pro zjištění všech uživatelských účtů Zdroj: Vlastní

Také je možné zjistit přesné informace o operačním systému, viz obrázek 27. Tato data o zařízení jsou pro útočníka zajímavá v kontextu hledání využitelných zranitelností. Na obrázku je vidět *OS Version*, tedy přesná verze operačního systému. Podle tohoto údaje lze z otevřených databází jednoduše vyhledat nejen o kterou aktualizaci se jedná, ale také zda existují novější verze. Největším nebezpečím jsou však databáze zranitelností, existující nejen na dark webu, ale i na klasickém internetu. Stačí velmi jednoduše z databáze verzí získat oficiální označení verze, pro tento scénář se jedná o 21H2[55]. S tímto kódem je pak možné z některé z mnoha přístupných databází nalézt příslušné kódy zranitelností, viz obrázek 28. V tuto chvíli není nic jednoduššího než nalézt aplikovatelnou zranitelnost a využít ji.



Obrázek 27: Ukázka zjištění specifické verze operačního systému Zdroj: Vlastní



Microsoft » Windows 10 » 21h2 * * * : Security Vulnerabilities Published In 2021

Cpe Name:*cpe:2.3:o:microsoft:windows_10:21h2:*:*:*:*:*:x86:**

2021 : January February March April May June July August September October November December CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

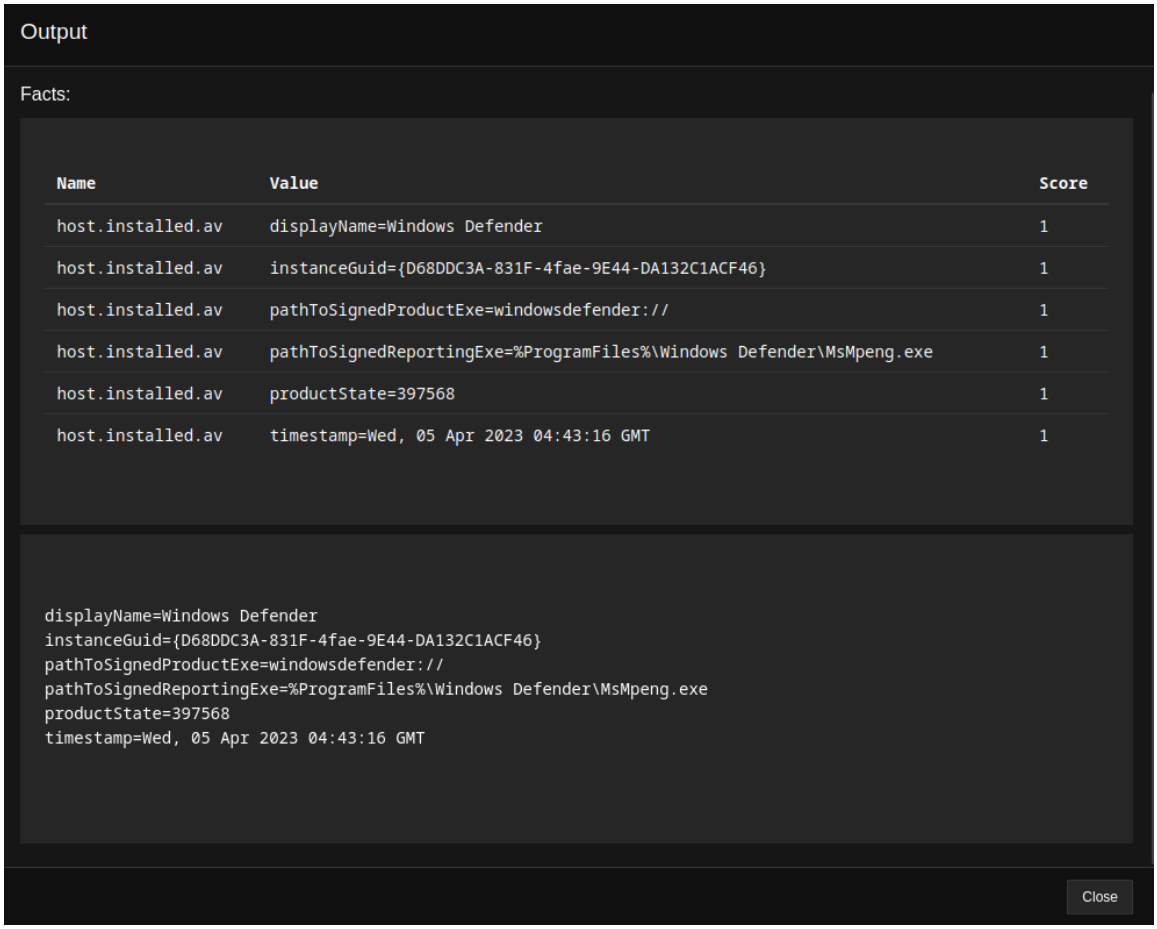
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

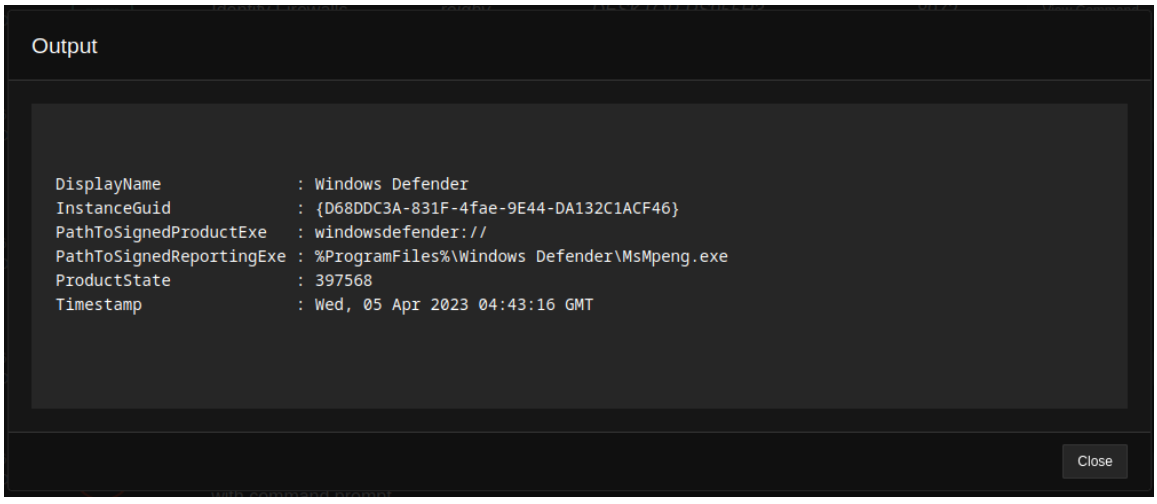
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2021-43893	668			2021-12-15	2022-07-12	6.0	None	Remote	Medium	???	Partial	Partial	Partial
	Windows Encrypting File System (EFS) Elevation of Privilege Vulnerability													
2	CVE-2021-43883				2021-12-15	2022-07-12	4.6	None	Local	Low	Not required	Partial	Partial	Partial
	Windows Installer Elevation of Privilege Vulnerability													
3	CVE-2021-43248				2021-12-15	2022-07-12	4.6	None	Local	Low	Not required	Partial	Partial	Partial
	Windows Digital Media Receiver Elevation of Privilege Vulnerability													
4	CVE-2021-43247	787			2021-12-15	2022-07-12	7.2	None	Local	Low	Not required	Complete	Complete	Complete
	Windows TCP/IP Driver Elevation of Privilege Vulnerability													
5	CVE-2021-43244				2021-12-15	2022-05-23	4.9	None	Local	Low	Not required	Complete	None	None
	Windows Kernel Information Disclosure Vulnerability													
6	CVE-2021-43240				2021-12-15	2022-07-12	4.6	None	Local	Low	Not required	Partial	Partial	Partial
	NTFS Set Short Name Elevation of Privilege Vulnerability													
7	CVE-2021-43239				2021-12-15	2022-07-12	4.6	None	Local	Low	Not required	Partial	Partial	Partial
	Windows Recovery Environment Agent Elevation of Privilege Vulnerability													
8	CVE-2021-43238	59			2021-12-15	2022-07-12	4.6	None	Local	Low	Not required	Partial	Partial	Partial
	Windows Remote Access Elevation of Privilege Vulnerability													
9	CVE-2021-43237	59			2021-12-15	2022-07-12	6.9	None	Local	Medium	Not required	Complete	Complete	Complete
	Windows Setup Elevation of Privilege Vulnerability													
10	CVE-2021-43235	668			2021-12-15	2022-05-23	2.1	None	Local	Low	Not required	Partial	None	None
	Storage Spaces Controller Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-43227.													
11	CVE-2021-43233			Exec Code	2021-12-15	2022-07-12	5.1	None	Remote	High	Not required	Partial	Partial	Partial
	Remote Desktop Client Remote Code Execution Vulnerability													

Obrázek 28: Ukázka zjištění specifické verze operačního systému Zdroj: [56]

Dalším důležitým poznáním z této operace je nejen zjištění přítomnosti firewallu a antiviru na testovaném zařízení, ale dokonce i jejich identifikace. Výstupy zkoumající tyto fakty je možné vidět na obrázcích 29 a 30. Stejně jako u operačních systémů, i u zabezpečení existují zranitelnosti a způsoby obcházení jejich činnosti. Znalost ochranných prostředků proto útočníkovi nabízí podstatnou výhodu.



Obrázek 29: Nalezené informace o antiviry na testovaném zařízení Zdroj: Vlastní



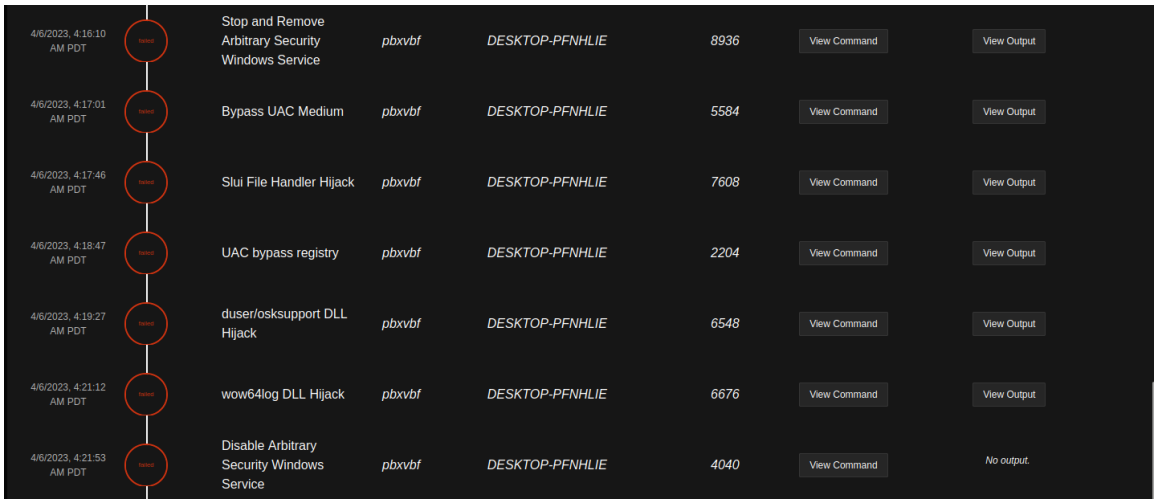
Obrázek 30: Nalezené informace o firewall na testovaném zařízení Zdroj: Vlastní

V neposlední řadě se útočník může pokusit získat data z prohlížeče. Informace, na které se v tomto kontextu útočník zaměřuje, jsou cookies, záložky, historie prohlížení nebo uložená

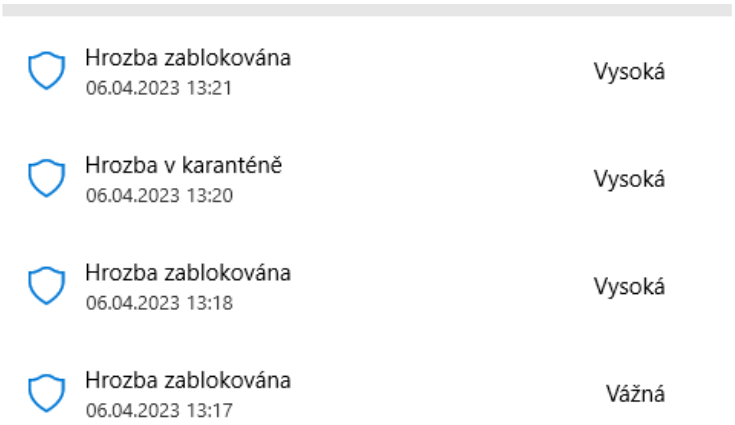
hesla. Oproti předchozím případům se zde primárně nejedná o data, která může útočník použít k dalším útokům na dané zařízení. Stejně se ale jedná o cenná data, která může v mnoha případech útočník prodat nebo použít k jiným typům útoků.

10.2.4 Lab02v2

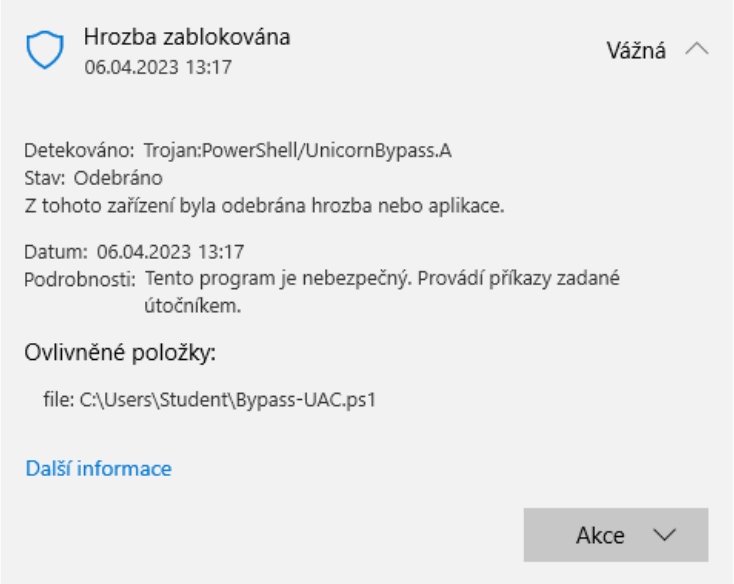
Tato operace a adversary využívají již zjištěných dat k upřesnění specifických cílů. Simulujeme zde situaci, kdy útočník získal základní data o napadeném zařízení. Jeho cílem je teď nejen získat vyšší práva nad tímto zařízením ale také získat informace vhodné pro zajištění dlouhodobého přístupu k zařízení. Prvním krokem je zlepšení šancí na dosažení těchto cílů, za tímto účelem se simulovaný útočník pokusí vypnout antivirová opatření, na než narazil v předchozí operaci, viz obrázek 29. To však není zcela úspěšné, jak již bylo psáno, nacházíme se na novější verzi operačního systému Windows, která je adekvátně aktualizovaná. Nemůže tak být překvapením, že se tato taktika nezdařila. Důležité je však poznamenat, že tento krok operace v systému Windows nevyvolal žádné hlášení. Hlášení nastala až ve chvíli, kdy se simulovaný útočník pokoušel získat administrátorská práva. V rámci testování se tato práva snažil získat všemi možnostmi, které Caldera nabízí. Tento fakt a vyvolané poplašné hlášení je možné vidět na obrázcích 31,32 a 33.



Obrázek 31: Probíhající operace zaměřená na získání administrátorských privilegií Zdroj: Vlastní



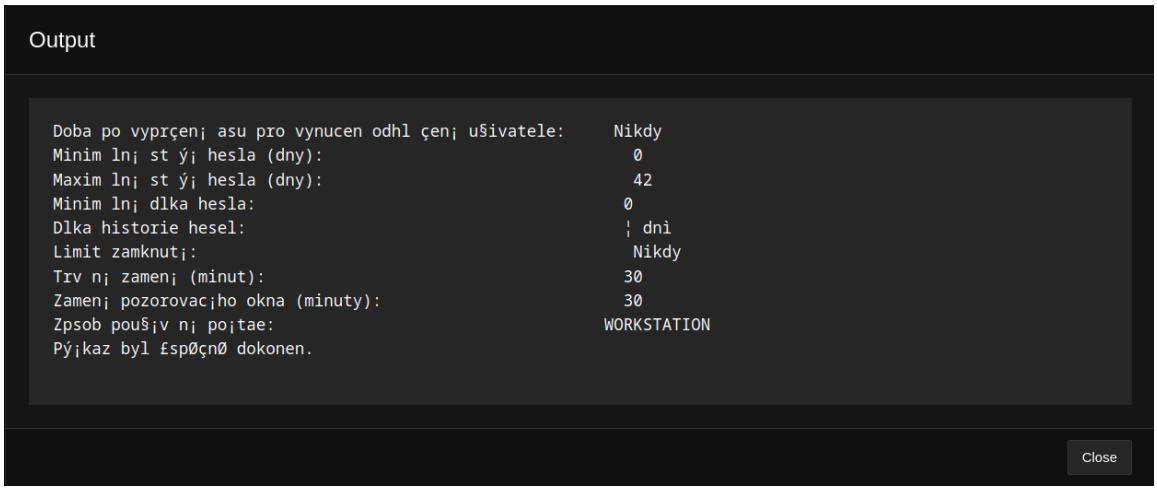
Obrázek 32: Záznamy o vyvolaných hrozbách Zdroj: Vlastní



Obrázek 33: Specifika náhodně vybrané hrozby Zdroj: Vlastní

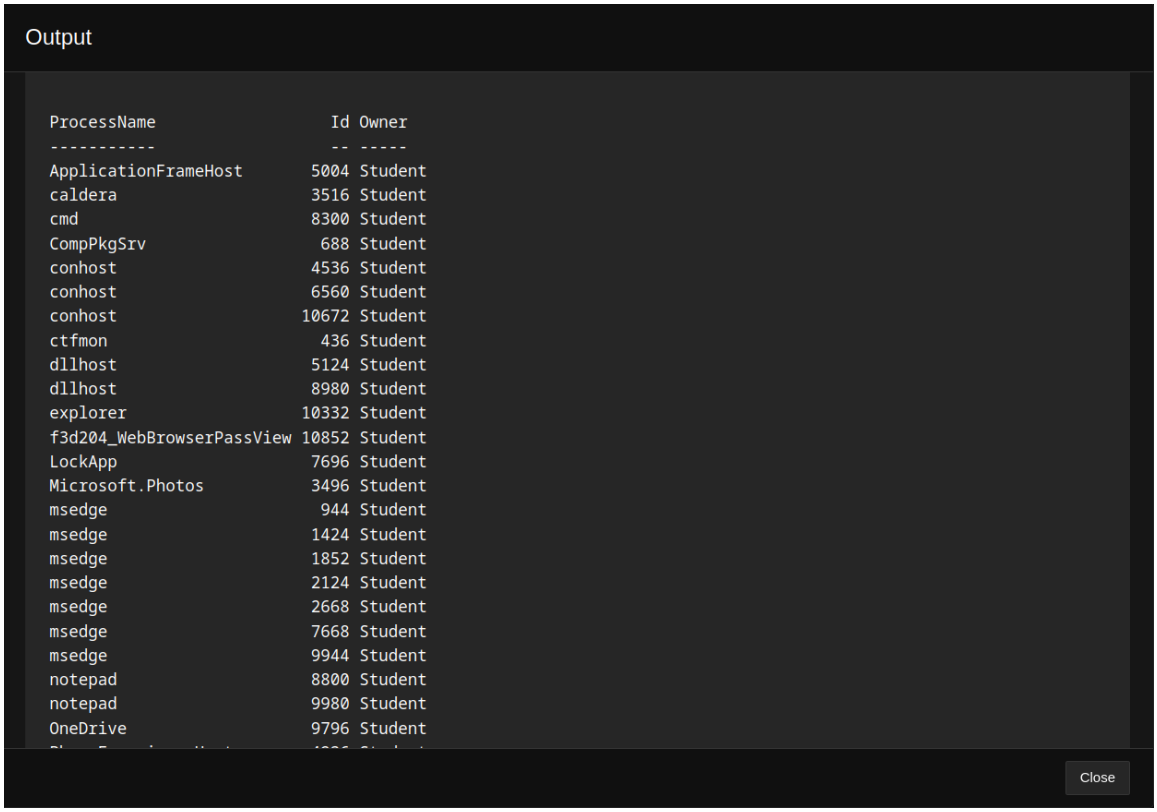
Jak je vidět z obrázků, všechny pokusy o získání administrátorských práv byly zastaveny a oznámeny uživateli. Je tedy zřejmé, že testování systému opravu provádí nebezpečné operace, o nichž je nutné uživatele informovat. Již při vytváření operace bylo jasné, že šance úspěchu předchozích operací je malá. Proto jejich neúspěch není překvapením, ale očekávaným a správným výsledkem. Naopak by bylo nemilým překvapením, kdyby se nám takto jednoduchým způsobem povedlo administrátorská práva získat. Poslední částí této operace jsou pokusy o získání dalších důležitých dat, která by útočníkovi mohla pomoci získat administrátorský přístup. Příkladem je například politika hesel, která existuje na daném zařízení. Jak je patrné na obrázku 34, Caldera si plně nerozumí s českou lokalizací

systému. To pouze znamená, že není možné sběr dat plně zautomatizovat, nejdůležitější poznatky lze stále přečíst, i když se zvýšeným úsilím.



Obrázek 34: Nalezená politika hesel Zdroj: Vlastní

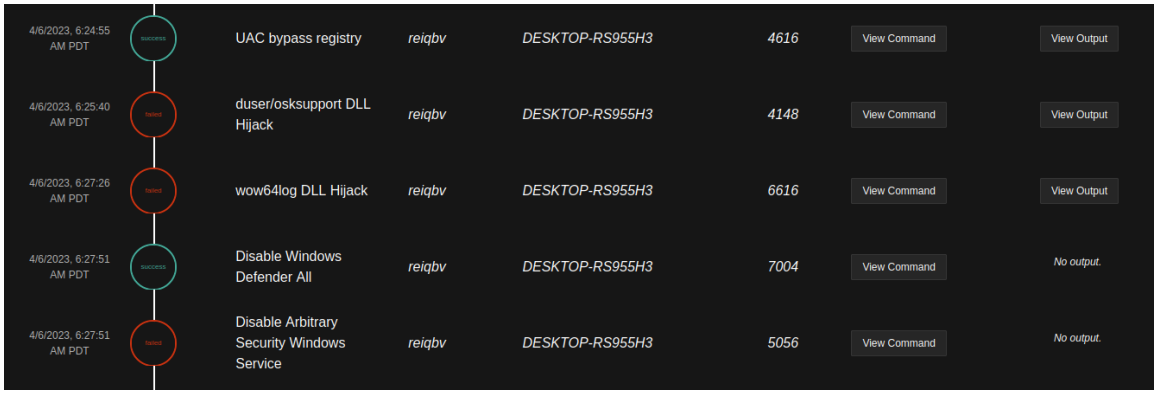
Poslední technikou v této operaci, která stojí za zvláštní zmínku, je zobrazení všech procesů daného uživatele. Jak je vidět na obrázku 35, pro útočníka je možné zjistit všechny procesy daného uživatele. To je důležité hned z několika důvodů. Znalost procesů dovoluje útočníkovi napodobit jména často používaných procesů a tak je před uživatelem chovat. Ještě důležitější je pro útočníka tato znalost z důvodu hledání zranitelností. Znalost procesů omezuje množinu programů, které musí útočník zkontrolovat pro využitelné zranitelnosti. Navíc nemusí řešit dodatečnou instalaci nástrojů nebo hledat zranitelnosti přímo v operačním systému, pokud může využít zranitelností již nainstalovaných programů se stejným výsledkem. Tato možnost není uplatnitelná vždy, ale je dobré mít ji na paměti. Posledním důvodem, proč procesy uživatele útočníka zajímají, jsou data, která z těchto procesů může útočník vytěžit. Pokud narazí na proces, který ho zajímá, může na něj zaměřit další fáze útoku. Například už jen zjištění, jaký prohlížeč uživatel preferuje, zjednodušuje následující útoky na data. Nebo fakt, že uživatel využívá nějaké cloudové uložiště, jak je například vidět na obrázku 35.



Obrázek 35: Ukázka všech procesů uživatele Zdroj: Vlastní

10.2.5 Změny s privilegovaným uživatelem

V rámci kompletnosti testování byly stejné operace, tedy *Lab02* a *Lab02v2*, pouštěny na jiném zařízení v infrastruktuře, tentokrát s privilegovaným přístupem. Získaná data byla až na pár operací stejná. To potvrzuje domněnku robustního systému, kde celková stabilita a dostatečné zabezpečení v podobě antiviru odbouralo alespoň část hrozby. Zajímavá jsou však data z operace *Lab02v2*. Operace *Lab02* byla primárně pro zjištění dat, proto tam nevznikly významné odchylky. *Lab02v2* byl na získání vyšších uživatelských práv, což popravdě nedává s administrátorským účtem smysl, viz obrázek 36. Zajímavé je, že se podařilo částečně vyřadit fungování antivirového programu. Další překvapivé zjištění také nastalo, když se místo selhání všech hrozeb pro zisk privilegií jedna technika vydařila. Tento poznatek nemá velký smysl, ale je to zajímavé a úsměvné zjištění.



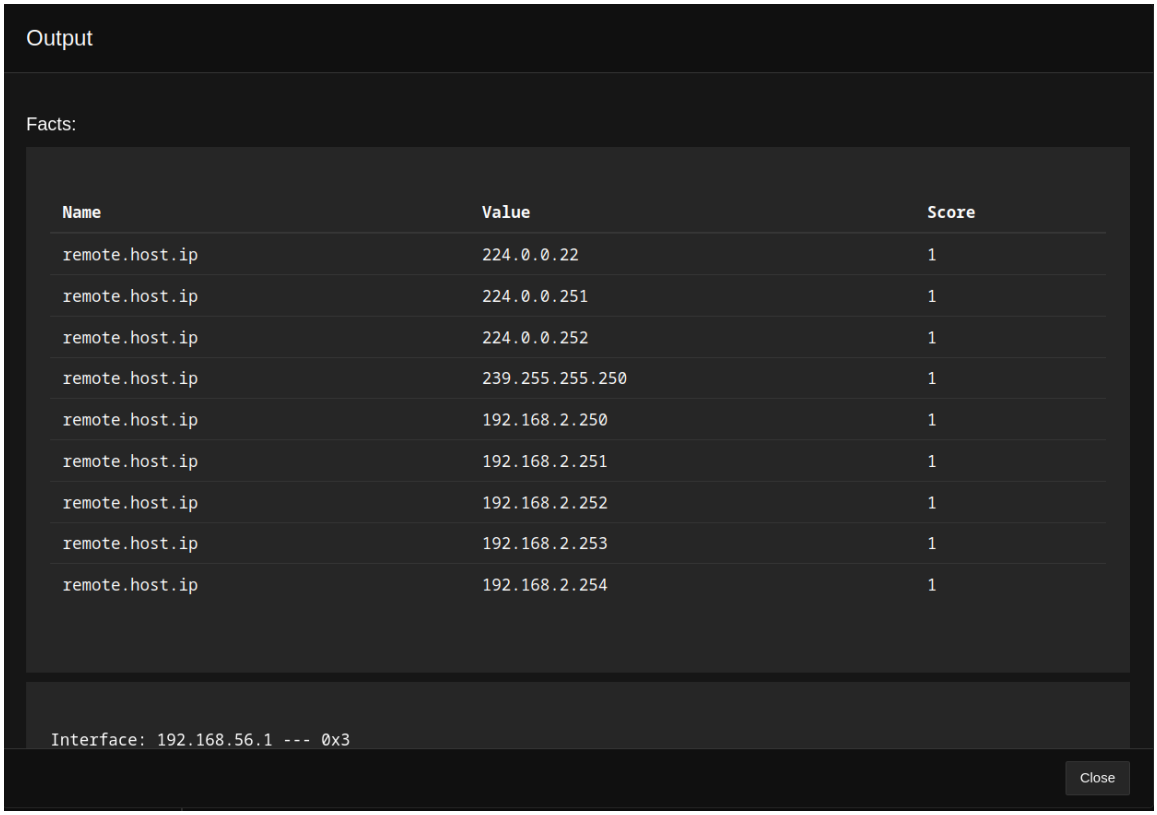
Obrázek 36: Ukázka technik s privilegovaným uživatelem Zdroj: Vlastní

10.3 Scénář 3 – *Discovery, Impact* a *Lateral movement*

Zaměřením tohoto scénáře je otestování možností šíření útočníkova dosahu v infrastruktuře a dopad jeho činnosti. Scénář 2 byl primárně zaměřen na jedno zařízení a zisk informací, scénář 3 je zaměřen na infrastrukturu a dopad na uživatele a společnost. Předpokladem je, že útočník již zjistil minimální potřebná data ze scénáře 2, již ho nezajímá být tak skrytý, ale naopak chce napadenému cíli uškodit. V rámci možností Caldery proto budou simulovány možné techniky, které jsou v souladu s cíli útočníka.

10.3.1 Lab03

Operace na šíření po infrastruktuře má název *Lab03*, jako *adversary* je využit základní útočník **Worm**. Tento útočník v Caldeře existuje hned v několika verzích s malými rozdíly, zajímavou myšlenkou proto bylo použít několik verzí a porovnat jejich výsledky. Specificky byla tato operace testována s útočníky **Worm, Worm2** a **Worm 3**. Pro ukázku je možné techniky útočníka **Worm 3** vidět na obrázku 20. Při testování vybraných útočníků typu worm však nebyly rozeznatelné rozdíly v jejich účinnosti. Proto bude v dalším textu popisována pouze generická operace s útočníkem worm zahrnující všechny specifické iterace. Jak je z obrázku 20 jasné, cílem útočníka worm je rozšířit se v infrastruktuře. Prvním krokem tohoto útočníka je proto zjištění dalších připojených zařízení. Výsledek tohoto kroku je vidět na obrázku 37.



Obrázek 37: Ukázka nalezených IP adres Zdroj: Vlastní

Je zřejmé, že útočník tímto krokem nenalezl všechna zařízení v síti, ale pouze zařízení v jeho VLAN. Tento fakt potvrzuje nutnost dobré segmentace infrastruktury za cílem její obrany. Dalším krokem útočníka je provézt *reverse IP nslookup* pro všechny nalezené IP adresy. Tento krok však selže, protože v síti není využívané DNS, implementace totiž z důvodu velikosti a bezpečnosti nedávala smysl. Překvapivé je, že neexistence DNS nejen že zastavila další šíření útočníka worm, ale navíc byly techniky provádějící tuto operaci chybně označeny za úspěšné. Tento fakt je možný vidět na obrázcích 38 a 39 .

Obrázek 38: Ukázka špatně označených technik Zdroj: Vlastní

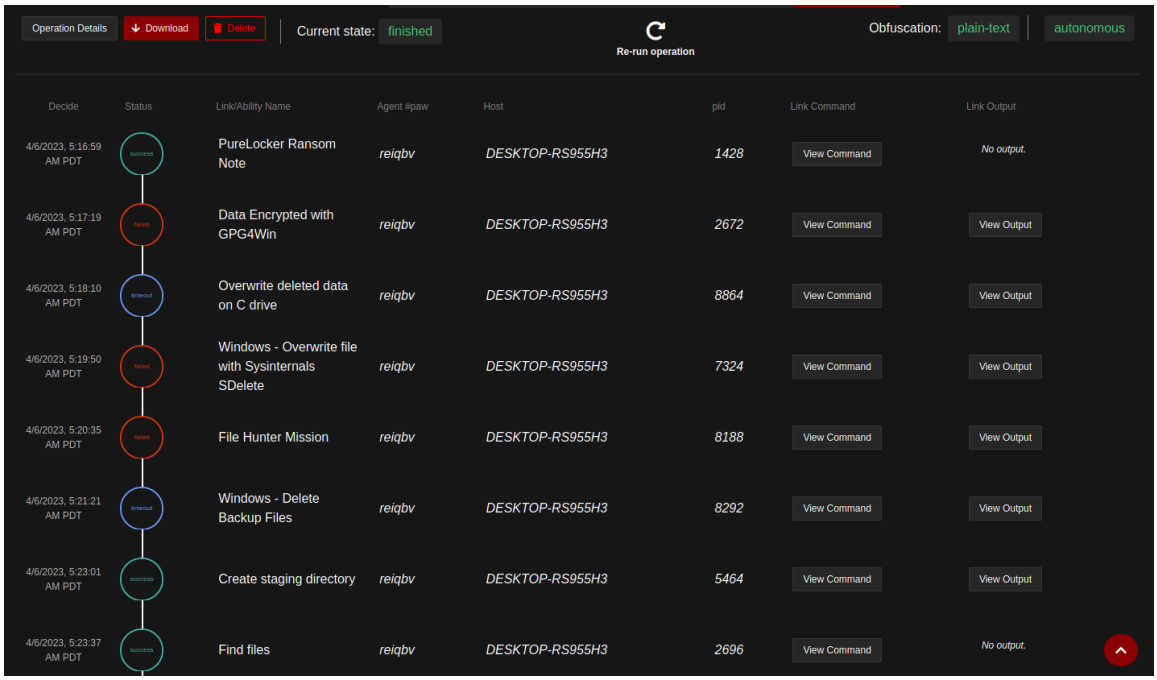
Obrázek 39: Ukázka výstupu špatně označené techniky Zdroj: Vlastní

Z výsledků je jasné, že testovaný infrastruktura je vůči tomuto útoku velmi odolná. Nejen že správně nastavená infrastruktura omezila zisk informací útočníka, ale také kompletně zamezila jeho dalšímu šíření.

10.3.2 Lab03v2

Druhá část scénáře 3 je zaměřena na testování taktiky *Impact*, jenž je zaměřena na manipulaci, přerušení nebo destrukci systémů a dat. V Caldeře byl proto vytvořen *adversary*, který obsahuje techniky s tímto zaměřením. Průběh operace s tímto útočníkem je vidět na obrázku 40. V první části je simulován ransomwarový útok, protože to je nejčastější a nejzávažnější typ hrozby. Dává proto smysl zjistit, zda je možné pomocí Caldery testovat bezpečnost zařízení vůči tomuto útoku. Jak je vidět z obrázku 40, úspěšně se povedlo na ploše uživateli vytvořit textový soubor *ransomware note*. Naštěstí pokus o zakódování dat byl obranou systému úspěšně zastaven. Také přepisování souborů bylo zastaveno. Naopak práce se *staging directory* byla úspěšná, povedlo se nejen vytvořit, ale při ukončování operace po sobě i smazat, tento adresář. Je tedy nutné podotknout, že pokud je i volně dostupný testovací framework chopen provést tyto operace, je na zvážení, co vše je schopen udělat specifický software zaměřený přímo pro tyto úkony. Takových softwarů je hned

řada, velká část je samozřejmě nelegální, existují však i legálně dostupné softwary. Možná nejznámějším příkladem je *Metasploit*[57].



Obrázek 40: Ukázka operace pro Lab03v2 Zdroj: Vlastní

11 Závěry a doporučení

Diplomová práce je zaměřena na zkoumání oblasti kybernetické bezpečnosti s cílem obeznámit čtenáře s nejzákladnějšími termíny kybernetické bezpečnosti a připravit pro něj jednoduché a srozumitelné testovací prostředí. Na závěr je nutné zhodnotit, zda bylo cílů práce dosaženo a zda byly ověřeny všechny předložené hypotézy.

V teoretické části práce byly předány základní znalosti o kybernetické bezpečnosti a také byl čtenář seznámen se současným stavem této tématiky. Především je zde ukázána relevantnost, pomocí rešerše jsou představeny nejdůležitější znalosti, jenž čtenář potřebuje znát, jako rozpoznání útoků nebo znalost útočníků. Na závěr jsou pro lepší pochopení praktické části předány znalosti ohledně testování a k testování využívaných nástrojů. Informace jsou čerpány z kvalitních zdrojů a nemůže tak být pochyb o jejich aplikovatelnosti a korektnosti.

V praktické části práce bylo cílem vytvořit jednoduché a srozumitelné testovací prostředí spolu s návodem k jeho použití. Zabývá se tím i první představená hypotéza, tedy zda je možné vytvořit takto popsané prostředí a adekvátně seznámit s jeho používáním nového uživatele. Odpověď zde není jasná a hypotézu nelze potvrdit ani vyvrátit bez dodatečného testování. Samozřejmě, že testovací prostředí vytvořit lze, bohužel každá osoba bude jinak vnímat, zda je prostředí "jednoduché a srozumitelné". Autor však věří, že popsané postupy jsou natolik podrobné, aby i v případě nepochopení bylo možné dojít k cílenému výsledku. Dále byly ukázány základy testování a uvedeny příklady a připomínky, které je možné aplikovat i na skutečnou infrastrukturu, z niž testování vycházelo. Výborným příkladem je kapitola 10.1, zabývající se zjišťováním informací o organizaci, které lze využít k útokům Sociálního inženýrství. Také kapitola 10.2, jež ukazuje získání specifické verze operačního systému a jak tuto informaci může útočník zneužít, ukazuje reálný dopad na skutečnou infrastrukturu. Lze tedy říci, že druhá představená hypotéza, zabývající se aplikací výsledků testování pro zlepšení bezpečnosti reálného prostředí, byla potvrzena.

Výsledky testování jsou ve většině příkladů očekávány, vždy existují povrchní data, která může útočník získat – například bylo snadné získat data o uživateli, síti nebo o politice hesel. Dle očekávání také dopadly části útoků hlouběji zasahující do systému, ty byly zastaveny obranou systému a ve většině případů nahlášeny uživateli. Nepříjemným zjištěním však bylo, které informace jsou považovány za povrchní, a tedy jednoduše přístupné. Například nalezení přesné verze operačního systému vede po jednoduchém vyhledávání na internetu k jeho známým zranitelnostem, a dokonce i připravenému malwaru, který danou zranitelnost zneužívá. Tento údaj je však útočníkovi jednoduše přístupný, nehledě na závažnost jeho zjištění. Velkým zklamáním bylo také množství a typ informací, jež se povedlo získat o vybrané organizaci. Byly také zjištěny informace, které lze využít k několika typům útoků a představují tak bezpečnostní riziko.

Je přínosné zmínit další možnosti výzkumu související s touto prací. První možné zkoumání závisí na úzké spolupráci s organizací. V rámci možností by bylo zajímavé vytvořit scénáře přímo podle již uskutečněných útoků, které dané organizaci již hrozily, a zjistit, zda je organizace stále připravena takovému útoku čelit. Také opravdové testování infrastruktury by mohlo přinést významná data pro zlepšení bezpečnosti organizace. Problémem těchto zkoumání je však důvěra mezi potencionálním autorem a testovanou organizací. Dalším možným zkoumaným tématem v souvislosti s touto prací by bylo větší zaměření na jednu specifickou oblast útoku. Z důvodu pokrytí mnoha taktik, technik a nástrojů není možné, aby se autor práce každému z nich věnoval do hloubky a připravil jejich zhodnocení a možné návrhy na vylepšení. Autor si například dokáže představit práci založenou pouze na zkoumání taktiky *Reconnaissance*, kde by byly zkoumány využívané nástroje, shromažďována nalezená data a představena nejčastější místa, u nichž je u organizací nutné zlepšit práci s daty. Tato práce by mohla zkoumat několik vybraných organizací, aby bylo poukázáno na nejčastější slabá místa. Cíleně by bylo možné ukázat, kde je nutné omezit sdílení informací, nebo naopak ukázat, jaká data nelze schovat, a tak s nimi nakládat právě jako s daty, která jsou veřejně známá a tedy zneužitelná.

Literatura

[1] Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, volume 7, 2021: pp. 8176–8186, ISSN 2352-4847, doi:https://doi.org/10.1016/j.egyr.2021.08.126. Dostupné z: https://www.sciencedirect.com/science/article/pii/S2352484721007289

[2] European Union Agency for Cybersecurity; Svetozarov Naydenov, R.; Malatras, A.; et al. *ENISA threat landscape 2022 : July 2021 to July 2022*. 2022, ISBN 978-92-9204-588-3, doi:10.2824/764318.

[3] Abrams, L. Ransomware gang apologizes, gives SickKids hospital free decryptor. Dostupné z: https://www.bleepingcomputer.com/news/security/ransomware-gang-apologizes-gives-sickkids-hospital-free-decryptor

[4] Kumar, R.; Sharma, S.; Vachhani, C.; et al. What changed in the cyber-security after COVID-19? *Computers & Security*, volume 120, 2022: p. 102821, ISSN 0167-4048, doi:https://doi.org/10.1016/j.cose.2022.102821. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0167404822002152

[5] Lewis, J. A. Cyber War and Ukraine. Dostupné z: https://www.csis.org/analysis/cyber-war-and-ukraine

[6] on Foreign Relations, C. NotPetya. Dostupné z: https://www.cfr.org/cyber-operations/notpetya

[7] news, B. Tokyo Olympics: Russian hackers targeted Games, UK says. Dostupné z: https://www.bbc.com/news/technology-54600098

[8] Brumfield, C. Russia-linked cyberattacks on Ukraine: A timeline. Dostupné z: https://www.csoonline.com/article/3647072/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html

[9] Dvilyanski, M.; Agranovich, D.; Gleicher, N. Threat Report on the Surveillance-for-Hire Industry. Dostupné z: https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

[10] Bönsch, J. Sociální inženýrství [online]. 2021 [cit. 2023-01-22]. Dostupné z: https://theses.cz/id/r5nl5v/

[11] Stone, M. 4 Most Common Cyberattack Patterns from 2022. Dostupné z: https://securityintelligence.com/articles/most-common-cyberattack-patterns-2022

[12] Accenture. From disruption to reinvention: The future of supply chains in Europe. Dostupné z: https://www.accenture.com/us-en/insights/strategy/ukraine-future-supply-chains-europe

[13] Beck, K. Hackers exploit casino's smart thermometer to steal database info. Dostupné z: https://mashable.com/article/casino-smart-thermometer-hacked

[14] CISA. ICS Advisory (ICSA-22-200-01). Dostupné z: https://www.cisa.gov/uscert/ics/advisories/icsa-22-200-01

[15] Cisco Systems, I. What Is a Cyberattack? Dostupné z: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

[16] of Standards, N. I.; Technology. Cybersecurity Risks. Dostupné z: https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/cybersecurity-risks

[17] Díaz, V. Deception at a scale. Dostupné z: https://blog.virustotal.com/2022/08/deception-at-scale.html

[18] Díaz, V. Deception at scale: How attackers abuse governmental infrastructure. Dostupné z: https://blog.virustotal.com/2022/11/deception-at-scale-how-attackers-abuse.html

[19] USBKILL. USBKILL mainpage. Dostupné z: https://usbkill.com/

[20] ReliaQuest. Five things we learned from the Conti chat logs. Dostupné z: https://www.reliaquest.com/blog/five-things-we-learned-from-the-Conti-chat-logs/

[21] Microsoft. The many lives of BlackCat ransomware. Dostupné z: https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

[22] Sequin, P. What Is Spyware, Who Can Be Attacked, and How to Prevent It. Dostupné z: https://www.avast.com/c-spyware#topic-1

[23] Fortinet. What is Spyware? Dostupné z: https://www.fortinet.com/resources/cyberglossary/spyware

[24] Faife, C. New analysis further links Pegasus spyware to Jamal Khashoggi murder. Dostupné z: https://www.theverge.com/2021/12/21/22848485/pegasus-spyware-jamal-khashoggi-murder-nso-hanan-elatr-new-analysis

[25] Diaries, D. EP 100: NSO. Dostupné z: https://darknetdiaries.com/episode/100/

[26] Perlroth, N. *This is how they tell me the world ends: The cyberweapons arms race.* Bloomsbury Publishing, 2021, ISBN 9781635576054.

[27] Security, B. DNS Tunneling: How it Works, Detection and Prevention. Dostupné z: https://brightsec.com/blog/dns-tunneling/

[28] Flair, D. Most Common Types of Cyber Attackers. Dostupné z: https://data-flair.training/blogs/most-common-types-of-cyber-attackers/

[29] News, B. Anonymous: How hackers are trying to undermine Putin. Dostupné z: https://www.bbc.com/news/technology-60784526

[30] Diaries, D. EP 87: Guild of the Grumpy Old Hackers. Dostupné z: https://darknetdiaries.com/episode/87/

[31] Mladenovska, M. Understanding Malware-as-a-Service (MaaS): The future Of cyber attack accessibility. Dostupné z: https://cybersecurity.att.com/blogs/security-essentials/understanding-malware-as-a-service-maas-the-future-of-cyber-attack-accessibility

[32] Intelligence, M. D. T. Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself. Dostupné z: https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

[33] Ali, F. It's Back: REvil Ransomware Makes a Return, Here's What to Do. Dostupné z: https://www.makeuseof.com/revil-ransomware-attacks-return-what-to-do/

[34] Mitre. ATT&CK Groups. Dostupné z: https://attack.mitre.org/groups/

[35] Ray, M. Edward Snowden. Dostupné z: https://www.britannica.com/biography/Edward-Snowden

[36] Oakley, J. G. *Professional Red Teaming: Conducting Successful Cybersecurity engagements.* Apress, 2019.

[37] Thompson, C. Penetration Testing Versus Red Teaming: Clearing the Confusion. Dostupné z: https://securityintelligence.com/posts/penetration-testing-versus-red-teaming-clearing-the-confusion/

[38] Lootsec. Red Team Assessment Vs Penetration Test. Dostupné z: https://lootsec.io/red-team-assessment-vs-penetration-test/

[39] Keshri, A. Red Teaming vs Penetration Testing – Which One to Choose and Why? Dostupné z: https://www.getastra.com/blog/security-audit/red-teaming-vs-penetration-testing/

[40] Team, T. R. What is purple teaming and how can it strengthen your cyber security? Dostupné z: https://www.redscan.com/news/purple-teaming-can-strengthen-cyber-security/

[41] Corporation, T. M. ATT&CK Matrix. Dostupné z: https://attack.mitre.org

[42] Strom, D. 4 open-source Mitre ATT&CK test tools compared. Dostupné z: https://www.csoonline.com/article/3268545/4-open-source-mitre-attandck-test-tools-compared.html

[43] Corporation, T. M. ATT&CK Frequently Asked Questions. Dostupné z: https://attack.mitre.org/resources/faq/

[44] Corporation, T. M. ATT&CK navigator. Dostupné z: https://mitre-attack.github.io/attack-navigator/

[45] Strom, B. E.; Battaglia, J. A.; Kemmerer, M. S.; et al. Finding Cyber Threats with ATT&CK-Based Analytics. Dostupné z: https://www.mitre.org/sites/default/files/2021-11/16-3713-finding-cyber-threats-with-attack-based-analytics.pdf

[46] Mitre. ATT&CK Software. Dostupné z: https://attack.mitre.org/software/

[47] Mitre. ATT&CK Campaigns. Dostupné z: https://attack.mitre.org/campaigns/

[48] Team, A. R. Atomic Red Team Github page. Dostupné z: https://github.com/redcanaryco/atomic-red-team

[49] Casey Smith, M. H. Atomic Red Team Tests: Catching the Dragon by the Tail. Dostupné z: https://redcanary.com/blog/atomic-red-team-tests-catching-dragon-tail

[50] Endgame. Red Team Automation Github page. Dostupné z: https://github.com/endgameinc/RTA

[51] Mitre. Caldera Dokumentace. Dostupné z: https://caldera.readthedocs.io/en/latest/

[52] Mitre. Caldera Github page. Dostupné z: https://github.com/mitre/caldera

[53] Limited, O. S. Kali mainpage. Dostupné z: https://www.kali.org/

[54] Limited, O. S. Kali Linux 2023.1 Release (Kali Purple & Python Changes). Dostupné z: https://www.kali.org/blog/kali-linux-2023-1-release/#kali-purple

[55] Foundation, W. Windows 10 version history. Dostupné z: https://en.wikipedia.org/wiki/Windows_10_version_history

[56] SecurityScorecard. CVE Details. Dostupné z: https://www.cvedetails.com/

[57] Rapid7. Matasploit mainpage. Dostupné z: https://www.metasploit.com/

Seznam zkratek

DDoS Distributed Denial-of-Service

DNS Domain Name System

DoS Denial-of-Service

ENISA European Union Agency for Cybersecurity

EU Evropská unie

IKE Internet Key Exchange

IoT Internet of Things

MaaS Malware as a Service

MFA Multifactor Authentication

NIST National Institute of Standards and Technology

NSA National Security Agency

OSINT Open Source Inteligence

PhaaS Phishing as a Service

RaaS Ransomware as a Service

RDoS Ransomware Denial-of-Service

RDP Remote Desktop Protocol

RTA Red Team Automation

SIM Subscriber Identity Module

SMS Short Message Service

SQL Structured Query Language

USB Universal Serial Bus

VLAN Virtual Local Area Network

Seznam obrázků

1 Primární hrozby identifikované agenturou ENISA 7
2 Entity identifikované společností Meta 8
3 Nejvíce napadené sektory (v období červenec 2021 – červen 2022) 9
4 Zneužití státní infrastruktury 12
5 Počet zaznamenaných Ransomware incidentů a velikost ukradených dat ve sledovaném období květen 2021 až červen 2022 14
6 Mitre ATT@CK Navigátor 37
7 Porovnání vybraných nástrojů 41
8 Spuštěná Kali Purple ve virtuálním prostředí 45
9 Chyba kompilace Caldera frameworku 45
10 Nejnovější verze balíčku aiohttp v repozitáři Pypi 46
11 Nová podoba souboru requirements.txt 47
12 Caldera framework po úvodním přihlášení 47
13 Prvotní návrh testovaného prostředí 49
14 Návrh prostředí v Cisco Packet Tracer 50
15 Barevné označení jednotlivých scénářů 51
16 Stránka pro ovládání agentů 55
17 Formulář pro vytvoření agenta 56
18 Detaily specifického agenta 57
19 Ukázka technik u simulovaného útočníka 58
20 Příklad předpřipraveného adversary 59
21 Ukázka výběru technik 59
22 Ukázka správy operací 60
23 Ukázka tvorby operace 61
24 Ukázka probíhající operace 62
25 Výstup taktiky pro zjištění uživatele a jemu příslušné domény 63
26 Výstup taktiky pro zjištění všech uživatelských účtů 64
27 Ukázka zjištění specifické verze operačního systému 65
28 Ukázka zjištění specifické verze operačního systému 66
29 Nalezené informace o antiviry na testovaném zařízení 67
30 Nalezené informace o firewall na testovaném zařízení 67
31 Probíhající operace zaměřená na získání administrátorských privilegií . . . 68
32 Záznamy o vyvolaných hrozbách 69
33 Specifika náhodně vybrané hrozby 69
34 Nalezená politika hesel 70
35 Ukázka všech procesů uživatele 71

36 Ukázka technik s privilegovaným uživatelem 72
37 Ukázka nalezených IP adres 73
38 Ukázka špatně označených technik 74
39 Ukázka výstupu špatně označené techniky 74
40 Ukázka operace pro Lab03v2 75

Seznam ukázek kódů

1 Ukázka příkazu pro instalaci nástroje Recon-ng 48
2 Ukázka příkazu pro Nmap 53

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání diplomové práce

Autor:	**Bc. Jiří Bönsch**
Studium:	I2100054
Studijní program:	N1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název diplomové práce:	**Návrh testovacího prostředí za využití nástrojů ATT&CK**
Název diplomové práce AJ:	Design of test environment using ATT&CK tools

Cíl, metody, literatura, předpoklady:

Cílem diplomové práce je navrhnout komplexní prostředí pro testování kybernetické bezpečnosti za využití nástrojů ATT&CK a ověřit jeho implementaci na testovací scénářích.

V teoretické části autor provede literární rešerši zaměřenou na design kybernetických testovacích polygonů. Dále autor provede komparativní analýzu nástrojů od ATT&CK pro oblast testování s důrazem na jejich využití v rámci školního testovacího prostředí. Na základě této analýzy autor vybere jeden či více vhodných nástrojů a navrhne prostředí pro testování kybernetické bezpečnosti. V praktické části autor podrobně představí postup realizace testovacího prostředí a jeho oživení. Následně navrhne minimálně tři testovací scénáře, které prakticky ověří v rámci navrženého a oživeného testovacího prostředí.

Cybersecurity and Infrastructure Security Agency | CISA. Best Practices for MITRE ATT&CK® Mapping [online]. Dostupné z: https://www.cisa.gov/uscert/best-practices-mitre-attckr-mapping

MITRE ATT&CK. Working with ATT&CK. MITRE ATT&CK® [online]. Dostupné z: https://attack.mitre.org/resources/working-withattack/

STROM, David. 4 open-source Mitre ATT&CK test tools compared. CSO [online]. 2018. Dostupné z: https://www.csoonline.com/article/3268545/4-open-source-mitre-attandcktest-tools-compared.html

MITRE. CALDERATM. MITRE Corporation [online]. 2018; Dostupné z: https://www.mitre.org/research/technology-transfer/open-sourcesoftware/caldera%E2%84%A2

https://medium.com/mitre-attack

Zadávající pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	Mgr. Josef Horálek, Ph.D.
Datum zadání závěrečné práce:	15.10.2021