UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

NÁZOV FAKULTY

IDENTIFIKÁCIA POSTUPU ÚTOČNÍKA V SIETI PODNÁZOV PRÁCE

2023 **Adam KUNDRACIK**

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
NÁZOV FAKULTY

IDENTIFIKÁCIA POSTUPU ÚTOČNÍKA V SIETI
PODNÁZOV PRÁCE

BAKALÁRSKA PRÁCA**, DIPLOMOVÁ PRÁCA, DIZERTAČNÁ PRÁCA, HABILITAČNÁ PRÁCA**

Študijný program:	Informatika
Pracovisko (katedra/ústav):	Ústav informatiky
Vedúci bakalárskej práce:	RNDr. Tomáš Bajtoš

Košice 2023

Adam KUNDRACIK

Univerzita P. J. Šafárika v Košiciach
Prírodovedecká fakulta

ZADANIE ZÁVEREČNEJ PRÁCE

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

Názov: Identifikácia postupu útočníka v sieti

Názov EN: Identification of a lateral movement

Cieľ: (1) Analýza vybraných techník postupu útočníka v sieti
(2) Spracovanie a porovnanie prístupov k identifikácii postupu útočníka v sieti na základe záznamov z koncových zariadení
(3) Návrh metódy identifikácie postupu útočníka v sieti, otestovanie metódy a zhodnotenie výsledkov

Literatúra:
(1) FAWAZ, Ahmed, et al. Lateral movement detection using distributed data fusion. In: 2016 IEEE 35th Symposium on Reliable Distributed Systems (SRDS). IEEE, 2016. p. 21-30.
(2) TIAN, Zhihong, et al. Real-time lateral movement detection based on evidence reasoning network for edge computing environment. IEEE Transactions on Industrial Informatics, 2019, 15.7: 4285-4294.
(3) HENDLER, Danny; KELS, Shay; RUBIN, Amir. Detecting malicious powershell commands using deep neural networks. In: Proceedings of the 2018 on Asia conference on computer and communications security. 2018. p. 187-197.
(4) BAI, Tim, et al. A machine learning approach for rdp-based lateral movement detection. In: 2019 IEEE 44th Conference on Local Computer Networks (LCN). IEEE, 2019. p. 242-245.

Vedúci: RNDr. Tomáš Bajtoš
Oponent: RNDr. Peter Gurský, PhD.
Ústav : ÚINF - Ústav informatiky
Riaditeľ ústavu: doc. RNDr. Ondrej Krídlo, PhD.
Spôsob sprístupnenia elektronickej verzie práce: bez obmedzenia

Dátum schválenia: 15.05.2023

Poďakovanie

Ďakujem vedúcemu svojej diplomovej práce RNDr. Tomášovi Bajtošovi za cenné pripomienky a za obetavosť počas jej písania. Veľká vďaka patrí aj mojej rodine a blízkym osobám, ktoré mi boli veľkou oporou pri písaní práce a poskytli mi rady a pripomienky.

Abstrakt v štátnom jazyku

Laterálny pohyb je súbor techník ktoré používajú útočníci, po tom ako získajú prvotný prístup, na pohyb v rámci siete. V tejto práci sa venujeme základným pojmom a ich hlbšiemu vysvetleniu, ukazujeme najvyužívanejšie techniky laterálneho pohybu a simulujeme ho nástrojmi, ktoré sa využívajú najviac. Popisujeme fungovanie prostredia v ktorom tieto nástroje budeme používať a akým spôsobmi môžeme následne logy z týchto útokov získavať. V ďalšom kroku popisujeme nami vybraný a implementovaný spôsob na zber logov a nastavenia skupinových politík v systéme. Následne detegujeme laterálny pohyb a hľadáme postupnosť krokov, ktoré danú techniku charakterizujú. Výstupom je súbor postupností pre rôzne techniky laterálneho pohybu ako príručka pre ľudí ktorí danej problematike čelia alebo čeliť môžu.

Kľúčové slová: Laterálny pohyb, útočník, techniky, nástroje, EventCollector, PsExec

Abstrakt v cudzom jazyku

Lateral movement is a set of techniques used by hackers, after gaining initial access, to move within a network. In this work, We deal with the fundamental ideas and their deeper explanation, demonstrating the most popular lateral movement strategies before simulating them using the most popular tools. We are discussing how the environment in which these tools are being utilized operates and how logs may be gathered from these attacks as a result. The approach We chose and put into practice for gathering logs and creating group policies for the system will be covered in the next section. We'll then check for the series of actions that define the specified method and identify any lateral movement.

Key words: Lateral movement, attacker, technics, tools, EventCollector, PsExec

Obsah

OBSAH **6**

ZOZNAM SKRATIEK A ZNAČIEK **8**

ÚVOD **9**

1 LATERÁLNY POHYB (LATERAL MOVEMENT) **10**

TECHNIKY LATERÁLNEHO POHYBU **10**

1.1 VYUŽÍVANIE VZDIALENÝCH SLUŽIEB 11
1.2 INTERNAL SPEARPHISHING 15
1.3 VZDIALENÉ SLUŽBY 15
1.4 LATERÁLNY PRENOS NÁSTROJA 16
1.5 REPLIKÁCIA POMOCOU ODNÍMATEĽNÝCH ZARIADENÍ 20
1.6 NÁSTROJE NA NASADENIE SOFTVÉRU 24
1.7 ZNEHODNOTENIE ZDIEĽANÉHO OBSAHU 24
1.8 ALTERNATÍVNE SPÔSOBY AUTENTIFIKÁCIE 26

2 PODOBNÉ PRÁCE **29**

3 SPÔSOBY ZBERU DÁT **34**

3.1 METODOLÓGIA ZBERU DÁT 36
3.1.1 Vytvorenie lokálneho systému z virtuálnych strojov *37*
3.1.2 Iniciálne nastavenie Windows Server 2019 ..... *38*
3.1.3 Nastavenia skupinových politík *38*
3.1.4 Spôsob zberu dát *43*
3.1.5 Identifikácia relevantných dát *44*

4 DETEKCIA PIATICH NAJVIAC VYUŽÍVANÝCH TECHNÍK LATERÁLNEHO POHYBU **46**

4.1 PSEXEC 46
4.2 WINRS 49
4.3 RDP (REMOTE DESKTOP PROTOCOL) 51
4.4 WMIC (WINDOWS MANAGEMENT INSTRUMENTATION COMMAND-LINE) 55
4.5 NET USE 57

5 DETEKCIA LATERÁLNEHO POHYBU **60**

5.1 PSEXEC 60
5.1.1 Zdrojové zariadenie *60*
5.1.2 Koncové zariadenie *60*
5.2 WINRS 62
5.2.1 Zdrojové zariadenie *62*
5.2.2 Koncové zariadenie *62*

5.3 RDP 64
5.3.1 Zdrojové zariadenie *64*
5.3.2 Koncové zariadenie *64*
5.4 WMIC 66
5.4.1 Zdrojové zariadenie *66*
5.4.2 Koncové zariadenie *66*
5.5 NET USE 66
5.5.1 Zdrojové zariadenie *66*
5.5.2 Koncové zariadenie *67*
5.6 VYHODNOTENIE 68
ZÁVER 69
ZOZNAM POUŽITEJ LITERATÚRY 72
PRÍLOHY 86

Zoznam skratiek a značiek

RDP - **R**emote **D**eskrop **P**rotocol

RDBMS - relational database management system

RAT - Remote Access Tool

SSDP - Simple Service Discovery Protocol

SMB - Server Message Block

HTTP - Hypertext transfer protocol

HTTPS - Hypertext transfer protocol secure

AD FS - Active Directory Federated Services

SSMS - SQL Server Management Studio

WECC - Windows Event Collector klienta

WECS - Windows Event Collector server

WEC - Windows Event Collector

NAT - Network address translation

CEF - Common Event Format

LEEF - Log Event Extended Format

Úvod

V tejto práci budeme analyzovať techniku laterálneho pohybu, ktorou sa páchateľ dokáže pohybovať sieťou a napádať ďalšie zariadenia pomocou rôznych skriptov alebo iných prostriedkov.

Keďže v dnešnom svete je kybernetických útokov čoraz viac a viac, je potrebné zvyšovať povedomie ľudí aj o tejto problematike. Práve preto by sme vďaka tejto práci chceli dopomôcť k tomu, aby ľudia mali možnosť zistiť, aké všelijaké nástrahy na nich vo svete číhajú a ako fungujú.

Prakticky ukážeme, ako sa jednotlivé nástroje prejavujú a ako ich môžeme prostredníctvom zozbieraných logov detegovať. Výsledkom práce budú nielen zistenia priamo použiteľné na zlepšenie porozumenia postupu útočníka, ale aj ako danú skutočnosť zistiť. Získané výsledky povedú k zvýšeniu kybernetickej bezpečnosti v praxi, ako aj prípadnej skorej detekcie, k zrýchlenému konaniu užívateľa, ktorý útokom čelí.

Práca je štruktúrovaná nasledovne. V prvej kapitole popisujeme laterálny pohyb, čo laterálny pohyb je, a aké techniky a nástroje využíva. V druhej kapitole sa venujeme podobným prácam, ktoré sa venujú podobnej problematike. Tretia kapitola popisuje metodológiu nášho výskumu, identifikáciu event logov a iniciálne nastavenia nášho prostredia ktoré je bezprostredne pre funkčnosť nevyhnutné. Vo štvrtej kapitole bližšie popisujeme získané event logy pre päť najviac využívaných nástrojov laterálneho pohybu. V piatej kapitole popisujeme a ukazujeme databázové dopyty, ktorými dokážeme na danom zariadení , po získaní jeho event logov, detegovať laterálny pohyb pre vyššie spomínané konkrétne nástroje. Posledná kapitola sa venuje zhrnutiu nami získaných poznatkov a uzatvára problematiku s reálnymi výsledkami.

1 Laterálny pohyb (Lateral movement)

Laterálny pohyb je technika používaná na prevzatie kontroly nad systémom a získanie prístupu k rôznym iným systémom v rámci siete [12]. V článku ***What Is Lateral Movement? (Čo je laterálny pohyb?)*** [11], laterálny pohyb definujú ako techniku, ktorú útočníci používajú na rozširovanie sa na viacerých zariadeniach v sieti, ktorých cieľom je získať, alebo zničiť citlivé údaje na napadnutom zariadení .

Laterálny pohyb vieme rozdeliť do 3 fáz: **Fáza pozorovania, získania prístupových údajov a eskalácia práv a získania prístupu do zariadenia [1]**.

V prvej fáze útočník pozoruje, skúma a mapuje sieť, jej používateľov a zariadenia v nej. Toto mapovanie mu napomáha pochopiť jej hierarchiu, identifikovať potenciálne zariadenia, ktoré sú objektmi jeho záujmu. Útočníci v sieti nasadzujú rôzne nástroje, aby zistili kde v sieti sa nachádzajú, k čomu môžu získať prístup a aké firewally sa v sieti využívajú.[1]

Vo fáze dva sa útočník snaží nadobudnúť prihlasovacie údaje, ktoré potrebuje aby sa mohol v sieti pohybovať. Jednou z možností ako získať tieto údaje je oklamanie používateľov, napríklad phishingovým útokom. Medzi ďalšie bežné techniky patria napr. **Pass the Hash [55], Pass the Ticket [54] alebo nástroje ako Mimikatz [74].** [1]

V tretej fáze útočník vykonáva laterálny pohyb po sieti a napadá zariadenia kým nedôjde k dátam, ktoré hľadá. [1].

Techniky laterálneho pohybu

Útočníci sa snažia, aby v sieti boli čo najmenej viditeľní. Keďže využívanie externých nástrojov môže byť veľmi ľahko vystopovateľné, snažia sa využívať nástroje, ktoré sú na hostiteľskom zariadení už nainštalované. Môžu to byť napríklad nástroje ako: PowerShell [76], Windows Management Instrumentation (WMI) [77] ale aj PsExec. [11]

V nasledujúcich podkapitolách sa bližšie zaoberáme vybranými technikami, ich popisom, správaním a nástrojmi ktoré sú s nimi spojené.

1.1 Využívanie vzdialených služieb

Využívanie vzdialených služieb je technika, pomocou ktorej sa útočník snaží dostať do siete napríklad pomocou programovej chyby nezabezpečeného softvéru. Následne je útočník schopný na zariadení spustiť kód, ktorý mu dopomôže k jednoduchšiemu postupu po zariadeniach v rámci siete [13]. Túto teóriu rovnako popisuje aj MITRE ATT&CK matica [78], ktorá hovorí, že daná technika slúži na získanie neautorizovaného prístupu k interným systémom v rámci siete prostredníctvom programovej chyby v softvéri [7].

Tabuľka č. 1 – Popis nástrojov využívaných pri technike využívania vzdialených služieb

Nástroj	Popis nástroja
Bad Rabbit [17]	• Ransomvér • Využíva SMB protokol • Prvýkrát použitý v roku 2017
Conficker [18]	• je počítačový malware typu červ • Napáda počítače a počítačové systémy vybavené operačným systémom MS Windows • Prvýkrát objavený v roku 2008 • Využíva SSDP (Simple Service Discovery Protocol) protokol
Emotet [19]	• Malvér • Slúži na získanie prvotného prístupu do systému a následne v ňom povoľuje sťahovanie ďalších potrebných súborov • Prvýkrát objavený v roku 2014
Empire [20]	• Empire je open source, multiplatformný framework pre vzdialenú správu a post-exploatáciu • Využíva SMB protokol • Prvýkrát objavený v roku 2019

Flame [21]	• Môže nahrávať zvuk zo zariadení • Využíva akýkoľvek hardvér na laterálny pohyb a zber dát • Prvýkrát objavený v roku 2017
InvisiMole [89]	• Spyware • môže šíriť v sieti prostredníctvom zraniteľností BlueKeep (CVE-2019-0708) [79] a EternalBlue (CVE-2017-0144) [80] • Využíva protokol RDP a SMB • Prvýkrát objavený v roku 2018
Lucifer [90]	• Softvér na ťažbu kryptomien • Môže využiť protokol Stratum alebo SMB • Prvýkrát objavený v roku 2020
NotPetya [91]	• Malvér • Jeho cieľom bola deštrukcia dát a pevných diskov • Využíva protokol SMB • Prvýkrát objavený v roku 2019
PoshC2 [92]	• je open source framework pre vzdialenú správu a post-exploatáciu • Využíva SMB protokol • Prvýkrát objavený v roku 2019
QakBot [93]	• bankový trójsky kôň • Využíva SMB protokol • Prvýkrát objavený v roku 2021
Stuxnet [48]	• Počítačový červ • zameriava sa na programovateľné logické riadiace jednotky (PLC), ktoré umožňujú automatizáciu elektromechanických procesov • Prvýkrát objavený v roku 2020
TrickBot [94]	• Spyware

	• využíva exploity EternalBlue a EternalRomance na laterálny pohyb v moduloch wormwinDll, wormDll, mwormDll, nwormDll, tabDll • Prvýkrát objavený v roku 2018
WannaCry [95]	• Ransomvér • Využíva protokol SMB • Prvýkrát objavený v roku 2019

Skupiny, ktoré využívali túto techniku, sú napríklad: Fancy Bear (APT28) [22], Dragonfly [23], Fox Kitten [24], menuPass [25] [7].

Spôsoby využitia techniky využívania vzdialených služieb

K bežným terčom útoku patrí napríklad **Remote Desktop Protokol (RDP) [81],** taktiež známy ako vzdialená plocha. Dôvod je jednoduchý. RDP je frekventovane používaný v mnohých veľkých firmách. RDP nám povoľuje vzdialený prístup k zariadeniu [13]. Medzi Ďalšie patria aj **SMB** protokol, **služby web servera** ale aj **MySQL** [7].

RDP je jeden z najviac využívaných nástrojov na vzdialené ovládanie systému. Nachádza sa v každom modernom windowsovom operačnom systéme. RDP môže poskytnúť prenos výstupu obrazovky servera do klienta ako aj prenos vstupu z klávesnice a myši z klienta na server. Tento protokol má viacero nebezpečných zraniteľností. Jednou z nich je BlueKeep. Táto zraniteľnosť vedie k vzdialenému spusteniu náhodného kódu bez toho, aby používateľ čokoľvek urobil. Navyše nevyžadovala ani platné prihlasovacie údaje. Kombinácia týchto skutočností mohla viesť k vzniku škodlivého softvéru, ktorý by sa mohol šíriť medzi zraniteľnými systémami. Ďalšou zo zraniteľností je DejaBlue. DejaBlue je zoznám chýb, ktoré podobne ako BlueKeep umožňujú útočníkom prebrať zraniteľné systémy bez akejkoľvek formy overenia. Medzi bežné úskalia zabezpečenia RDP patria napr. : Slabé prihlasovacie údaje používateľa, Servery, na ktorých sa nezaznamenávajú alebo nemonitorujú prihlásenia RDP alebo Verejne vystavené systémy bez akéhokoľvek sieťového filtrovania. [64]

MySQL **[82]** je Systém riadenia relačných databáz a patrí medzi najpopulárnejšie open-source RDBMS (systém na riadenie relačnej databázy), ktoré sa v súčasnosti používajú. Jeho hlavným účelom je ukladať údaje pre webové servery alebo webové stránky. Nevýhodou je, že ani ten nie je úplne bezpečný a má určité zraniteľnosti. Medzi ne patria napr. :

- **SQL Injection** – Ide o útok na databázu pri ktorej útočník pomocou SQL dopytov získava údaje z databázy, alebo ich vymazuje. Môže to mať za následok následnú krádež prihlasovacích alebo iných citlivých údajov. Obísť zadanie korektných prihlasovacích údajov by bolo možne pomocou jednoduchého SQL dopytu. Ten by vyzeral nasledovne:

  Databázový dopyt č. 13

  ```
  SELECT * FROM utable WHERE username = "UserName001"
  AND password = "*" OR "1" = "1"
  ```

  Teda vždy, keď systém spustí tento dotaz, vždy by dal výsledok „true“ a aplikácia by si myslela, že heslo je správne. V tomto dopyte bude prvá časť hľadať používateľa s používateľským menom "UserName001" s heslom "*" a buď nedá žiadny výsledok, alebo ho vylúči ako nepravdivý. Ďalej prichádza na rad druhá časť dopytu. Tu bude výsledok hesla vždy „true“. Aplikácia nechá dopyt prejsť, a teda útočník bude môcť obísť proces overovania.
- **Nesprávne overenie vstupu** - typ útoku, pri ktorom škodlivý používateľ vykonáva útok na webové servery alebo ich inštancie, ako je napríklad MySQL. V prípade MySQL môže spôsobiť zlyhanie inštancie MySQL, čím sa stane na chvíľu nedostupnou pre všetky služby, ktoré ju používajú ako zdroj údajov.
- **Súbežné vykonávanie pomocou zdieľaných zdrojov s nesprávnou synchronizáciou alebo race condition** - je nežiaduci stav, ku ktorému dochádza, keď sa systém pokúša spustiť dve alebo viac ako dve operácie súčasne. V systéme MySQL to môže viesť k vzniku race condition. Umožňuje to lokálnemu používateľovi získať prístup k databáze. Následne môže využiť eskaláciu privilégií alebo zvýšiť svoje používateľské oprávnenia. Po zmene oprávnení môže vykonať útok.

- **Oprávnenia, privilégiá a kontroly prístupu -** Ide o starú zraniteľnosť, ktorá už bola opravená. Táto zraniteľnosť umožňovala útočníkom prepísať konfiguračný súbor MySQL mnohými nastaveniami. Tieto nastavenia boli následne implementované po jej opätovnom zapnutí. [65]

1.2 Internal Spearphishing

Internal spearphishing je technika slúžiaca na zneužitie účtov v internej sieti ako vstupný bod do nej. Bežným úkazom tohoto podvodu je využitie klamlivého linku ktorý sa používateľovi môže javiť ako skutočný. Ten ho následne presmeruje na nimi vytvorenú webovú službu do ktorej používateľ bez tušenia zadá svoje citlivé údaje ako napr. heslo. [8][16]

Medzi skupiny, ktoré využívali techniku Internal spearphishing patria napríklad: **Hexane** [26], **Gamaredon Group** [27], **Kimsuky** [28], **Lazarus Group** [29] [8].

1.3 Vzdialené služby

Vo väčších sieťach zvyknú byť servery organizované do domén. Keďže na prístup do domény stačí jedna sada prihlasovacích údajov, útočníkovi stačí získať tieto údaje a následne získava prístup do všetkých zariadení pomocou rôznych protokolov ako je SSH alebo RDP.

Tabuľka č. 2 – Popis nástrojov využívaných pri technike vzdialených služieb

Nástroj	Popis nástroja
Kivars [96]	• Nástroj vzdialeného prístupu (RAT - remote access tool) • má schopnosť diaľkovo spúšťať vstupy z klávesnice a kliknutia myšou, spúšťať sťahovanie súborov alebo zaznamenávať snímky obrazovky • Prvýkrát použitý v roku 2020
Stuxnet	• Popísaný v podkapitole 2.1 tabuľka č. 1

Spôsoby využívania vzdialených služieb

SSH (Secure Shell) je kryptografický sieťový protokol, ktorý používa kryptografiu s verejným kľúčom na zabezpečenie prístupu k vzdialeným serverom a zariadeniam cez nezabezpečenú sieť. Má niekoľko zraniteľností:

- **Útoky hrubou silou a malvérom**
- **Krádež relácie SSH a neoprávnený prístup** - Môže k tomu dôjsť buď únosom SSH agenta, alebo získaním neoprávneného prístupu k soketu agenta. V prípade predvolených konfigurácií SSH môže útočník narušiť privilegovaný prístup používateľa a vytvoriť backdoor kľúč manipuláciou s predvolenými nastaveniami.
- **Krádež súkromného kľúča** - Ak je súkromný kľúč kompromitovaný, útočník môže získať prístup ku všetkým účtom, v ktorých je súkromný kľúč platný. Existuje taktiež aj kratšia dĺžka kľúča, čo ale dodáva útočníkovi možnosť jeho rýchlejšieho dohľadania.

1.4 Laterálny prenos nástroja

Laterálny prenos nástroja je technika pri ktorej útočník premiestňuje súbory medzi zariadeniami v sieti v ktorej sa nachádza. Tento nástroj tak môže byť premiestňovaný zo zariadenia na zariadenie hocikde v rámci siete. Zväčša ide o nástroje, ktoré im pomáhajú v laterálnom pohybe a v rozširovaní sa na ďalšie zariadenia. [15]

Tabuľka č. 3 – Popis nástrojov využívaných pri technike laterálneho prenosu nástroja

Nástroj	Popis nástroja
BITSAdmin [33]	• Nástroj vzdialeného prístupu (RAT - remote access tool) • má schopnosť diaľkovo spúšťať vstupy z klávesnice a kliknutia myšou, spúšťať sťahovanie súborov alebo zaznamenávať snímky obrazovky • Prvýkrát použitý v roku 2020
Cmd [97]	• Nástroj systému Windows • Spúšťanie programov, vyhľadávanie súborov
DustSky [98]	• Malvér

	• vyhľadá v systéme súbory, ktoré obsahujú určité kľúčové slová a typy dokumentov vrátane PDF, DOC, DOCX, XLS a XLSX, zo zoznamu získaného z C2 ako textový súbor. Môže ich vymazávať, môže detegovať pripojené USB zariadenia, zbiera dáta o systéme • Prvýkrát použitý v roku 2017
Esentutl [99]	• Nástroj príkazového riadku • poskytuje databázové nástroje pre Windows Extensible Storage Engine, získava dáta o systéme, môže čítať a meniť toky dát, kopírovať súbory atď. • Prvýkrát použitý v roku 2019
Expand [100]	• Nástroj systému Windows • používa sa na rozbalenie jedného alebo viacerých komprimovaných CAB súborov , môže byť použitý na stiahnutie alebo skopírovanie súboru do dátového toku alebo cez zdieľanú sieť • Prvýkrát použitý v roku 2019
ftp [101]	• nástroj bežne dostupný v operačných systémoch na prenos informácií prostredníctvom protokolu FTP (File Transfer Protocol) • môže prenášať nástroje alebo súbory medzi systémami v rámci ohrozeného prostredia.
HermeticWizard [102]	• červ • môže využiť cmd.exe, spustiť príkaz „wevtutil cl system“ na vymazanie logov, kopírovať súbory do iných strojov, skenovať porty atď. • Prvýkrát použitý v roku 2022
LockerGoga [103]	• Ransomvér • Môže meniť heslá používateľom, enkryptovať súbory, vymazať svoj vlastný spustiteľný súbor atď. • Využíva protokol SMB • Prvýkrát použitý v roku 2019

Lucifer	• Popísaný v podkapitole 5.1 tabuľka č. 1
Olympic destroyer [104]	• Malvér • Hlavným cieľom škodlivého softvéru bolo znefunkčniť infikované počítačové systémy • používa natívne nástroje systému Windows vssadmin, wbadmin a bcdedit na odstránenie a vypnutie funkcií obnovy operačného systému, ako je katalóg záloh systému Windows a automatická oprava systému Windows. • Pokúša sa nakopírovať do vzdialených počítačov v sieti. • Prvýkrát použitý v roku 2019
PsExec [105]	• Nástroj spoločnosti Microsoft • Používa sa na spustenie programu na inom počítači • Môže vytvárať nových užívateľov, zvýšiť privilégia v rámci systému, sťahovať alebo nahrávať súbory
Shamoon [106]	• Wiper malvér • Pokúša sa nakopírovať do vzdialených počítačov v sieti. • Prvýkrát použitý v roku 2017
Stuxnet	• Popísaný v podkapitole 2.1 tabuľka č. 1
WannaCry	• Popísaný v podkapitole 2.1 tabuľka č. 1

Skupiny, ktoré využívali túto techniku, sú napríklad: **Aoqin Dragon, GALLIUM, Wizard Spider** a mnohé ďalšie [15].

Spôsoby využívania laterálneho prenosu nástroja

Cmd.exe je shell v operačnom systéme Microsoft Windows, ktorý poskytuje rozhranie príkazového riadka v tomto systéme. Medzi jeho zraniteľnosti patrí možnosť zámeny kódu za iný, tzv. **Cmd Hijack.** Cmd hijack je zámena príkazov/argumentov v súbore cmd.exe, ktorá umožňuje útočníkovi spustiť ľubovoľné spustiteľné súbory systému Windows. Napríklad nasledujúci príkaz:

```
„cmd.exe /c
"ping127.0.0.1/../../../../../../../../../../windows/system32/calc.exe"“
```

spustí calc.exe namiesto ping.exe.

FTP je jednou z najstarších a stále často používaných metód zdieľania údajov je protokol FTP (File Transfer Protocol). Chýba mu ale mnoho kľúčových požiadaviek na bezpečnosť. Medzi najčastejšie zneužitia FTP patria:

- **Anonymné overovanie** - Táto zraniteľnosť umožňuje používateľom prihlásiť sa k FTP serveru pomocou používateľského mena a hesla, alebo anonymne. V mnohých prípadoch sa ako heslo používa e-mailová adresa. Avšak, prihlasovacie údaje používateľa (používateľské meno a heslo) a príkazy použité na serveri FTP sú nešifrované, viditeľné a zraniteľné. Okrem toho sú všetky údaje odoslané pomocou FTP alebo uložené na anonymnom FTP serveri nechránené.
- **Útok cez adresár –** je útok, pri ktorom útok prepíše alebo vytvorí neoprávnené nové súbory, ktoré sú uložené mimo koreňového priečinka webu.
- **Krížové skriptovanie (XSS)** - Útoky typu XSS sa vyskytujú, keď útočník využíva webovú aplikáciu na odoslanie škodlivého kódu, obvykle vo forme skriptu, priamo koncovému používateľovi. Chyby, ktoré umožňujú útoky tohto typu, sú pomerne bežné a môžu sa vyskytnúť všade tam, kde webová aplikácia používa vstup od používateľa v rámci výstupu, ktorý generuje, a to bez toho, aby tento vstup overila alebo zakódovala. Prehliadač koncového používateľa nie je schopný rozpoznať, že skript nie je dôveryhodný, a tak ho spustí. Pretože prehliadač predpokladá, že skript pochádza z dôveryhodného zdroja, škodlivý skript môže získať prístup k všetkým súborom cookie, tokenom relácie a ďalším citlivým informáciám, ktoré prehliadač uchováva a používa v rámci danej stránky.
- **Útok škodlivým softvérom na báze Dridexu** - Dridex je škodlivý softvér zameraný na používateľov systému Windows, ktorí otvárajú prílohy e-mailov vo formáte Word alebo Excel. Tento softvér obsahuje makrá, ktoré sa po otvorení aktivujú a spôsobia infekciu počítača, čím sa používateľ vystavuje riziku bankovej krádeže. V najnovšej verzii Dridexu používajú hackeri stránky FTP a získané poverenia na obchádzanie ochranných opatrení e-mailových brán a sieťových zásad, ktoré dôverujú FTP.

SMB (Server Message Block) protokol je používaný pre zdieľanie súborov, tlačiarní a iných zdrojov v sieťach s operačným systémom Windows. Medzi najznámejšie zraniteľnosti patrí:

- **Remote Code Execution (RCE)** - Útočník môže spustiť škodlivý kód na vzdialenom systéme a získať plnú kontrolu nad ním.
- **Denial of Service (DoS)** - Útočník môže vytvoriť preťaženie siete alebo vzdialeného systému tým, že odosiela špeciálne SMB pakety, čím bráni ostatným používateľom prístup k zdieľaným zdrojom.
- **Man-in-the-Middle (MitM)** - Útočník môže odchytávať komunikáciu medzi dvoma zariadeniami v sieti a získavať citlivé informácie, ako sú heslá alebo citlivé súbory.
- **Information Disclosure -** Útočník môže získať citlivé informácie, ako sú názvy používateľských účtov, zdieľané adresáre a súbory alebo konfiguračné informácie o systéme.
- **SMB Relay Attack** - Útočník môže využiť zraniteľnosť, ktorá umožňuje útočníkovi preposlať autentifikačné údaje používateľa na iný systém a získať prístup k citlivým informáciám.
- **Brute Force** - Útočník môže pokúšať zistiť heslo používateľského účtu pomocou brute force útoku, ktorý spočíva v opakovanej pokuse o prihlásenie sa s rôznymi kombináciami hesiel a používateľských mien.

Tieto zraniteľnosti sa môžu využívať na získanie neoprávnenej prístupu k súborom a zdrojom, získanie citlivých informácií a dokonca aj na prepadnutie celej siete. Preto je dôležité zabezpečiť používanie SMB protokolu, napríklad prostredníctvom šifrovania a autentifikácie, aby sa minimalizovala riziko útoku a ochránila citlivá informácia. [68]

1.5 Replikácia pomocou odnímateľných zariadení

Technika replikácie pomocou odnímateľných zariadení spočíva v šírení škodlivého programu na odnímateľne zariadenie ako je napríklad USB. Toto zariadenie sa následne môže na zariadeniach spúšťať automaticky po tom, čo sa pripojí k systému.

Táto technika zvyčajne zahŕňa kopírovanie súborov alebo úpravu existujúcich súborov uložených na vymeniteľnom médiu. Malvér sa zvyčajne tvári ako neškodný legitímny súbor. [37] [38]

Tabuľka č. 4 – Popis nástrojov využívaných pri technike replikácie pomocou odnímateľných zariadení

Nástroj	Popis nástroja
Agent.btz [107]	• Červ • Šíri sa pomocou odnímateľných zariadení ako napr. USB • Vytvorí na odnímateľnom zariadení samo spúšťací súbor autorun.inf. Po vložení tohoto zariadenia do iného PC sa súbor sám spustí a stiahne do neho malvér • Prvýkrát použitý v roku 2017
CHOPSTICK [108]	• Malvér • Je schopný spustiť kód / skript vzdialene • Monitoruje súbory s koncovkou .doc, .docx, .pgp, .gpg, .m2f, alebo .m2o • Prvýkrát použitý v roku 2017
Conficker	• Popísaný v podkapitole 2.1 tabuľka č. 1
Crimson [109]	• Trójsky kôň so vzdialeným prístupom • Môže využiť HTTP volania, odpočúvať cez mikrofóny, kradnúť heslá z Webových prehliadačov, zbierať informácie o hostiteľskom prostredí • Prvýkrát použitý v roku 2017
DustSky	• Popísaný v podkapitole 2.3 tabuľka č. 3
Flame	• Popísaný v podkapitole 2.1 tabuľka č. 1
H1N1 [110]	• Malvér • Môže získavať heslá z Webových prehliadačov, ukončovať rôzne servisy pomocou cmd.exe, enkryptovať C2 premávku, ukončovať servisy pre Windows Security Center a Windows Defender, spustiť sťahovanie rôznych súborov, nakopírovať sa na akékoľvek zariadenie • Prvýkrát použitý v roku 2017
njRAT [111]	• Nástroj vzdialeného prístupu • zhromažďuje informácie o otvorených oknách, môže spúšťať PowerShell skripty, spúšťať skripty cez príkazový riadok, kradnúť heslá atď.

	• Prvýkrát použitý v roku 2019
QakBot	• Popísaný v podkapitole 2.1 tabuľka č. 1
Ramsay [112]	• Nástroj na krádež dát • dokáže komprimovať a archivovať zhromaždené súbory pomocou programu WinRAR, po zašifrovaní a komprimovaní pomocou RC4 a WinRAR môže zhromaždené dokumenty uložiť do vlastného kontajnera, môže zhromažďovať dokumenty Microsoft Word z cieľového súborového systému, ako aj súbory .txt, .doc a .xls z vyrovnávacej pamäte prehliadača Internet Explorer atď. • Prvýkrát použitý v roku 2020
SHIPSHAPE [113]	• Malvér • Zameriava sa na vymeniteľné disky, aby sa rozšíril do iných systémov úpravou disku tak, aby používal autorun súbor na spúšťanie alebo skryl legitímne súbory dokumentov a skopíroval spustiteľný súbor do priečinka s rovnakým názvom ako legitímny. • Prvýkrát použitý v roku 2017
Stuxnet	• Popísaný v podkapitole 2.1 tabuľka č. 1
Unknown Logger [114]	• Nástroj tajných vchodov • dokáže ukradnúť používateľské mená a heslá z prehliadačov v počítači obete, má funkciu na vypnutie bezpečnostných nástrojov, dokáže sťahovať vzdialené súbory atď. • Prvýkrát použitý v roku 2017
Ursnif [115]	• bankový trójsky kôň • spája sa predovšetkým s krádežou údajov, ale jeho varianty obsahujú aj komponenty (backdoory, spyware, injektory súborov atď.), ktoré sú schopné vykonávať širokú škálu činností. • Prvýkrát použitý v roku 2019

USBferry [116]	• malvér na kradnutie informácií • monitoruje pripojené USB zariadenia, môže sa nakopírovať do pripojených USB zariadení, získava citlivé dáta, dokáže detegovať súbory a dostupné zložky obete • Prvýkrát použitý v roku 2017
USBStealer [117]	• Malvér • Dokáže sa nakopírovať na odnímateľné zariadenie a po následnom pripojení v inom systéme spustiť samo spustiteľný škodlivý autorun súbor • Prvýkrát použitý v roku 2017

Skupiny, ktoré využívali túto techniku, sú napríklad: **Fancy Bear (APT28), Aoqin Dragon , Darkhotel** a mnohé ďalšie[15].

Spôsoby využívania techniky replikácie odnímateľných zariadení

HTTP (Hypertext Transfer Protocol) je protokol používaný na prenos dát na internete. Je to základný protokol používaný pre webové stránky a umožňuje komunikáciu medzi webovým klientom (napr. internetovým prehliadačom) a webovým serverom.

Niektoré z najbežnejších zraniteľností HTTP protokolu sú:

- **Injection útoky** - zraniteľnosti v rámci aplikácií na spracovanie dát, ktoré umožňujú útočníkom vkladať do systému škodlivý kód.
- **Cross-site scripting (XSS)** - umožňuje útočníkom vkladať skripty alebo škodlivý kód do webových stránok a získať tak prístup k citlivým údajom používateľov.
- **Cross-site request forgery (CSRF)** - táto zraniteľnosť umožňuje útočníkom manipulovať s relačnými tokenmi, ktoré sú používané na overenie totožnosti používateľov a umožňuje im vyslať neoprávnené požiadavky v mene používateľa.
- **Request smuggling** - zraniteľnosti v HTTP protokole, ktoré umožňujú útočníkom manipulovať s posielaním HTTP požiadaviek a následne získať neoprávnený prístup k citlivým údajom.
- **Server-side request forgery (SSRF)** - umožňuje útočníkom vytvárať a spracovávať požiadavky zvnútra systému a získať tak prístup k citlivým údajom.

- **Dávkové útoky (Brute Force)** - umožňujú útočníkom zistiť prihlasovacie údaje používateľov alebo heslá prostredníctvom opakovaných neúspešných pokusov o prihlásenie.
- **Zneužitie závislostí (Dependency Injection)** - táto zraniteľnosť umožňuje útočníkom vkladať do systému škodlivý kód prostredníctvom zneužitia závislostí medzi komponentami. [67]

1.6 Nástroje na nasadenie softvéru

Nástroje na nasadenie softvéru je technika pri ktorej je do aplikácie tretej strany vpustený malvér ktorý útočníkom napomáha pri laterálnom pohybe v rámci siete.

Prístup môže byť použitý na laterálny presun do iných systémov, zhromažďovanie informácií alebo vymazanie pevných diskov na všetkých koncových bodoch [39]. Povolenia potrebné na vykonanie tejto akcie sa môžu líšiť v závislosti od nastavenia systému. Niekde môžu postačovať lokálne prihlasovacie údaje, inde sa môžu vyžadovať prihlasovacie údaje domény [40].

Tabuľka č. 5 – Popis nástrojov využívaných pri technike nástroje na nasadenie softvéru

Nástroj	Popis nástroja
Wiper [118]	• malvér • Pravdepodobne bol injektovaný do antivírusových softvérov ktoré boli následne nainštalované na rôznych zariadeniach v rámci mnohých spoločností • Prvýkrát použitý v roku 2017

Skupiny, ktoré využívali túto techniku, sú napríklad: **OceanLostus (APT32)** [42], **Threat Group-1314** [43], **Silence** [44] a mnohé ďalšie. [40]

1.7 Znehodnotenie zdieľaného obsahu

Táto technika spočíva v infikovaní zdieľaného úložiska alebo iného zdieľaného miesta škodlivými súbormi. Tieto súbory po následnom spustení infikujú zariadenie nič

netušiaceho užívateľa, ktorý tieto súbory spúšťa. Tento proces napomáha útočníkom v laterálnom pohybe. [39]

Súbory používajú kamuflovanie pôvodných súborov pomocou .LNK, a tieto nové súbory vyzerajú ako tie pôvodné, legitímne. .LNK súbory obsahujú zabudovaný príkaz, ktorý spustí skrytý súbor . Škodlivé súbory sa tvária ako neškodné a legitímne. Využívajú sa na to .LNK súbory, ktoré tak vyzerajú, no obsahujú v sebe príkaz ktorý spustí skrytý súbor v adresári, no stále vykonáva príkaz zadaný užívateľom, aby to vyzeralo, že všetko je v poriadku. [45]

Tabuľka č. 6 – Popis nástrojov využívaných pri technike znehodnotenia zdieľaného obsahu

Nástroj	Popis nástroja
Conti [119]	• Ransomvér ako služba (Ransomware-as-a-Service) • Slúži na krádež citlivých súborov a informácií z napadnutých sietí a vyhrážanie sa zverejnením týchto údajov, ak nebude zaplatená požadovaná čiastka • Prvýkrát použitý v roku 2021
H1N1	• Popísaný v podkapitole 2.4 tabuľka č. 4
InvisiMole	• Popísaný v podkapitole 2.1 tabuľka č. 1
Miner-C [120]	• Malvér • Na hostiteľskom zariadení ťaží kryptomenu Monero • Využíva FTP protokol • Prvýkrát použitý v roku 2017
Ramsay	• Popísaný v podkapitole 2.4 tabuľka č. 4
Stuxnet	• Popísaný v podkapitole 2.1 tabuľka č. 1
Ursnif	• Popísaný v podkapitole 2.4 tabuľka č. 4

Skupiny, ktoré využívali túto techniku, sú napríklad: **BRONZE BUTLER, Gamaredon Group , Darkhotel** a mnohé ďalšie.

1.8 Alternatívne spôsoby autentifikácie

V systéme sa na pri autentifikácii do medzipamäte alebo na disk ukladajú autentifikačné tokeny, ktoré majú za úlohu overiť, či sa používateľ úspešne autentifikoval, bez toho, aby sa od neho vyžadovalo opätovné prihlásenie. Ich získaním môžu útočníci získať prístup do systému bez potreby poznať prihlasovacie údaje jeho vlastníka. Medzi najčastejšie techniky patria: **pass the hash** alebo **pass the ticket** spoločne s využívaním **webových cookies**. [52]

Tabuľka č. 7 – Popis nástrojov využívaných pri technike alternatívne spôsoby autentifikácie

Nástroj	Popis nástroja
FoggyWeb [121]	• Nástroj tajných vchodov (backdoor) • dokáže na diaľku exfiltrovať citlivé informácie z napadnutého servera Active Directory Federated Services (AD FS), má schopnosť komunikovať so servermi C2 prostredníctvom požiadaviek HTTP GET/POST, môže umožniť zneužitie tokenu SAML • Prvýkrát použitý v roku 2021

Spôsoby techniky alternatívnych spôsobov autentifikácie

Mimikatz je nástroj na získavanie hesiel v operačnom systéme Windows. Tento nástroj je schopný extrahovať heslá uložené v pamäti systému, ktoré môžu byť využité na získanie neoprávnenej prístupu k rôznym systémovým účtom a službám. Dokáže získať heslá uložené v pamäti pre rôzne autentifikačné mechanizmy, ako sú napríklad NTLM (NT LAN Manager), Kerberos a WDigest. Tento nástroj môže byť použitý na získanie hesiel lokálne na počítači, ale aj vzdialene pomocou sieťových protokolov. Mimikatz je často využívaný k útokom na firemné siete a organizácie. Útočníci môžu použiť tento nástroj na získanie hesiel od používateľov a potom sa pokúsiť získať neoprávnený prístup k iným systémovým účtom a službám. V preklade by sme mohli nazvať Mimikatz napríklad "vykradnutie hesiel" a jeho účelom je získavanie hesiel na neoprávnené použitie. [74]

Pass the hash (Odovzdanie hash-u)

Na vykonanie techniky pass the hash je potrebné najskôr aplikovať techniku **Credential Access** (prístup k povereniu) [53], čo je súbor techník určených na krádež prihlasovacích mien a ich hesiel. Najčastejšie ide o **keylogging [50]** alebo **credential dumping [51].** [54]

Útočníci môžu získané hash-e hesiel využívať na prihlásenie do vzdialeného zariadenia bez toho aby vedeli aké heslo mu prislúcha. Po získaní hash-u útočníci tento hash posúvajú serveru, ktorý ich autentifikuje. Po tomto kroku útočník získava prístup do systému a môže vykonávať laterálny pohyb na ďalšie zariadenia v sieti. [53]

Pass the ticket (Odovzdanie lístku)

Ide o techniku autentifikovania sa do systému pomocou kerberos lístkov bez hlbšieho poznania hesiel. Kerberos tikety sú získavané technikou s názvom credential dumping [51].

V závislosti od úrovne prístupu možno získať servisný lístok alebo lístok na udelenie lístku. Servisný lístok nám udeľuje prístup k určitému zdroju, medzitým čo lístok udeľujúci lístky nám poskytuje prístup k akémukoľvek zdroju ku ktorému má používateľ oprávnenia. [54]

Strieborný lístok umožňuje útočníkovi falšovať iba lístky TGS (ticket-granting service) pre konkrétne služby. Vstupenky TGS sú zašifrované hash-om hesla pre službu. Ak teda útočník ukradne hash pre určitú službu, môže pre túto službu falšovať vstupenky TGS. [57]

Zlatý lístok poskytuje držiteľovi neobmedzený prístup. Ak protivník získa hash hesla KRBTGT, vlastní zlatý lístok, ktorý mu dáva právomoc pristupovať k akémukoľvek ľubovoľnému zdroju v systéme. Tento útok je ťažko odhaliteľný. [58]

Využívanie webových cookies

Autentifikačné súbory cookie sa bežne používajú vo webových aplikáciách vrátane cloudových služieb po tom, ako sa používateľ autentifikoval do služby. Slúži k tomu, aby sa užívateľ nemusel mnohokrát autentifikovať po každej návšteve danej služby. Útočník je schopný dané súbory cookies získať a následne ich importovať do prehliadača. Po importovaní získava prístup k aplikácii ako používateľ, až dokiaľ súbor cookie nestratí svoju platnosť. Po prihlásení na web môže útočník získať prístup k

citlivým informáciám, čítať e-maily alebo vykonávať akcie, na ktoré má konto obete oprávnenie. [56]

2 Podobné práce

V tejto kapitole sa budeme venovať prácam, ktoré riešili podobnú problematiku.

Prvou z podobných prác je práca od Nikhila Somashekarappa [12], vypracovaná na National College of Ireland, ktorá sa zaoberá problematikou detekcie laterálneho pohybu v systéme Windows, ktorý predstavuje jednu z najčastejších taktík využívaných útočníkmi na pohyb v sieti, ktorá bola napadnutá. Autor sa v práci podrobne venuje dvom najpoužívanejším technikám - pass-the-hash a pass-the-ticket - a popisuje spôsob, ako tieto techniky detegovať pomocou bezpečnostných logov operačného systému Windows. Jeho prístup k detekcii spočíva v tvorbe bezpečnostnej aplikácie, ktorá monitoruje bezpečnostné logy a upozorňuje administrátora pri výskyte určitých event log ID, ktoré signalizujú potenciálnu hrozbu. Autor sa v práci snažil pomôcť administrátorom sietí a iným bezpečnostným profesionálom identifikovať a zastaviť útoky na ich systémy a tak ich chrániť pred stratou dát a ďalšími bezpečnostnými problémami. Prínosom práce je aj zvýšenie povedomia o problematike laterálneho pohybu a dôležitosti bezpečnostných opatrení v oblasti IT ochrany. Ide o zaujímavú a aktuálnu tému, ktorá je veľmi relevantná pre oblasť IT bezpečnosti a môže byť prínosná pre všetkých, ktorí sa zaoberajú ochranou IT infraštruktúry.

Ďalej sa pozrieme na prácu od Christos Smiliotopoulos et al. [59], v ktorej sa zamerali na identifikáciu a detekciu deviatich najbežnejších techník laterálneho pohybu. Na základe experimentov a testovania na testovacom zariadení vytvorili vlastné pravidlá konfigurácie monitorovacieho systému Sysmon [83], v súbore config.xml. Týmto spôsobom zozbierali viac ako 870 tisíc logov, ktoré následne analyzovali v programovacom jazyku Python pomocou aplikácie s názvom PeX [84], určenej na automatizáciu rozboru a monitorovania týchto objemných súborov. PeX je voľne dostupný a umožňuje širšiu analýzu logov. Ich prístup a aplikácia sú široko používané pri detekcii laterálneho pohybu v systéme Windows a sú obzvlášť užitočné v situáciách, keď je potrebné identifikovať možné hrozby a potenciálne rizikové prvky. Výsledky ich práce sú veľmi pozitívne, pričom miera identifikácie techník laterálneho pohybu dosahuje až 95 %. Tento prístup a aplikácia PeX sú príkladom toho, ako sa technológie dajú využiť na vylepšenie bezpečnosti a ochrany informačných systémov pred možnými hrozbami.

Diplomová práca od Utkarsh Jain [53] sa zaoberá problematikou laterálneho pohybu a spracováva väčšinu nástrojov a techník, ktoré s týmto fenoménom súvisia. V práci je detailne rozobraný nástroj ELK[85] stack, ktorý slúži na spracovanie a analýzu logov a je často využívaný na detekciu laterálneho pohybu. Autor v práci poukazuje na to, ako pomocou ELK stacku a zozbieraných logov môže byť detekcia laterálneho pohybu efektívnejšia a presnejšia. Autor v práci detailne popisuje ako ELK stack funguje, ako sa používa a čo každá z jeho častí vykonáva. Taktiež popisuje ako dané systémové logy do ELK stacku dostáva a aké nástroje pri tom využíva aj s návodom na ich inštaláciu a iniciálne nastavenia. Následne dôsledne popisuje prejavy každej techniky v logoch a logy ktoré s touto technikou priamo súvisia. V závere tieto výsledky popisuje.

Určovanie, aké logy sa zanechávajú na serveri a klientoch pri použití rôznych nástrojov, je kritickou zložkou procesu vyšetrovania bezpečnostných incidentov a môže pomôcť pri identifikácii podozrivých aktivít. V tomto kontexte sa výskumníci JPCERT (Japan Computer Emergency Response Team Coordination Center) et al. [60] zaoberali presne týmto problémom v ich výskume popísanom v článku na webovej stránke. Okrem zisťovania, aké logy sú zanechávané, cieľom výskumu bolo aj nájsť konkrétne nastavenia na konfiguráciu, ktoré by umožnili získanie logov na dokazovanie následného spustenia rôznych nástrojov. V rámci svojej práce JPCERT použili viaceré nástroje a technológie, vrátane zberu logov pomocou nástrojov ako ELK stack a iných. Vďaka týmto nástrojom boli schopní zistiť logy z rôznych fáz útoku, čo im umožnilo rekonštruovať postupnosti udalostí a identifikovať škodlivé aktivity. V kapitole 3 výskumu popisujú výsledky zberu logov a konkrétne sa zaoberajú identifikáciou logov z rôznych nástrojov v závislosti na ich úlohe v rámci útoku. Tieto výsledky umožnili výskumníkom vytvoriť postupnosti spustenia rôznych nástrojov pre rôzne organizácie z celého sveta. Výsledkom je prehľadný súbor, ktorý sa môže použiť ako referenčný materiál pri vyšetrovaní podobných incidentov. Okrem zberu logov sa výskumníci JPCERT zaoberali aj integráciou rôznych nástrojov a technológií pre efektívne vyšetrovanie incidentov. Vo svojej práci popisujú, ako sa ELK stack, LateralStalker a iné nástroje môžu integrovať s ďalšími bezpečnostnými riešeniami pre zlepšenie celkového výkonu a účinnosti vyšetrovania. Ich výsledky a postupy môžu byť preto veľmi užitočné pre bezpečnostné tímy, ktoré sa zaoberajú ochranou sietí a aplikácií pred škodlivými útokmi.

Samostatný výskum v oblasti detekcie laterálneho pohybu v prostredí Edge Computing má veľký potenciál pomôcť v boji proti pokročilým kybernetickým hrozbám. Práve preto bol vytvorený návrh nového modelu detekcie laterálneho pohybu na základe siete Evidence Reasoning Network, ktorý by mohol byť účinnejší a spoľahlivejší v porovnaní s existujúcimi riešeniami. Hlavným cieľom článku od Zhihong Tian et al. [61], bolo navrhnúť a implementovať model detekcie laterálneho pohybu založený na sieti Evidence Reasoning Network, ktorý by bol schopný poskytnúť presné výsledky v reálnom čase v prostredí Edge Computing. Výsledky ukázali, že nový navrhnutý model je účinný v detekcii laterálneho pohybu a poskytuje rýchle a presné výsledky v reálnom čase. Navyše, tento model je schopný pracovať s obmedzenými prostriedkami a počítačovými zdrojmi v prostredí Edge Computing, čo z neho robí vhodné riešenie pre túto oblasť. V budúcnosti by bolo možné tento model ďalej vylepšiť a rozšíriť jeho funkčnosti na základe nových poznatkov a vývoja technológií v oblasti detekcie kybernetických hrozieb v prostredí Edge Computing.

V článku od Martina Husáka et al. [62] z Masarykovej Univerzity sa skupina autorov z tejto univerzity venuje problému laterálneho pohybu v počítačových sieťach. Tento fenomén predstavuje vážne bezpečnostné riziko, keďže útočník dokáže postupne získavať prístup k rôznym častiam siete a následne získať cenné informácie. Autori v článku identifikujú problém s falošnými hláseniami o laterálnom pohybe v logoch, ktoré sa často objavujú a zbytočne vyťažujú systém. Preto sa snažia vyvinúť detekčný nástroj, ktorý by dokázal tieto falošné logy filtrovať a zamerať sa len na tie, ktoré skutočne popisujú laterálny pohyb. Na dosiahnutie tohto cieľa autori používajú kombináciu odborných znalostí a strojového učenia. Konkrétne sa v článku zameriavajú na identifikáciu jedinečných znakov, ktoré poukazujú na skutočný laterálny pohyb. Navyše využívajú štatistickú metódu PCA na nájdenie skutočných znakov laterálneho pohybu a identifikáciu súvisiacich logov. Okrem toho, výskum bol realizovaný na datasete, ktorý obsahuje logy skutočných útokov, čím sa zvyšuje presnosť detekčného nástroja a umožňuje jeho overenie na reálnych útokoch. Autori teda v článku opisujú vývoj nového nástroja na detekciu laterálneho pohybu, ktorý by mal zlepšiť bezpečnosť v počítačových sieťach a zároveň byť efektívnejší pri spracovaní logov.

Ďalší článok z oblasti kybernetickej bezpečnosti zaoberajúci sa detekciou laterálneho pohybu v sieti pochádza od autora Giovanni Apruzzese et al. [63]. V tomto

článku autor popisuje nový typ útoku, ktorý využíva tunelovanie na šírenie príkazov, a ktorý je pre detekciu ťažko vystopovateľný. Tento typ útoku je zložitý na odhalenie pomocou bežných podpisov v systéme, čo útočníkom umožňuje pohybovať sa v sieti bez toho, aby boli odhalení. Na riešenie tohto problému autor navrhuje nový algoritmus na detekciu laterálneho pohybu, ktorý využíva analýzu sieťových tokov a časových grafov. Taktiež sa v článku zavádza algoritmus prioritizácie, ktorý zoraďuje zistené cesty podľa stupňa hrozby. Výsledkom tohto prístupu je integrácia detekcie a prioritizácie hrozieb v rámci pivotných útokov. Navrhovaný algoritmus možno ľahko integrovať s akýmikoľvek inými detekčnými schémami, ktoré využívajú čierne a biele zoznamy hostiteľov, analýzy DNS premávky a premávky medzi internými a externými sieťami. Článok sa tak zaoberá dôležitým problémom v oblasti kybernetickej bezpečnosti a predstavuje nový prístup k detekcii laterálneho pohybu v sieti, ktorý je spoľahlivejší a účinnejší než súčasné riešenia. Výsledky výskumu ukazujú, že navrhovaný algoritmus dosahuje vysokú presnosť a úspešne identifikuje laterálny pohyb v sieti aj v prípade, keď sú útoky maskované tunelovaním. Tento prístup teda môže byť dôležitým nástrojom v boji proti kybernetickým hrozbám a pomôcť organizáciám chrániť sa pred stratami dát, finančnými stratami a inými škodlivými účinkami kybernetických útokov.

Článok od Rafael Salema Marques et al. [75] sa zaoberá nástrojom na detekciu a ochranu pred útokmi na aplikačné rozhrania s názvom APIVADS. Tento nástroj bol vytvorený na ochranu aplikácií pred rôznymi druhmi kybernetických útokov, ktoré môžu byť vykonané na aplikačné rozhrania. Hlavným cieľom APIVADS je poskytnúť ochranu pred útokmi typu DDoS, SQL injection, Cross-Site Scripting a mnohými ďalšími. Nástroj APIVADS využíva rôzne algoritmy pre detekciu a ochranu proti útokom. Medzi tieto algoritmy patrí napríklad: Bayesian Network, Artificial Neural Network, Support Vector Machine, Decision Tree a ďalšie. Tieto algoritmy sú schopné spracovať rôzne druhy údajov, ako sú sieťové pakety, dáta z aplikácie alebo HTTP požiadavky, aby identifikovali potenciálne hrozby a zabezpečili ochranu aplikácií. APIVADS je navrhnutý tak, aby bol agnostický vzhľadom na transportné a aplikačné protokoly, čo znamená, že môže byť použitý pre rôzne typy aplikácií bez ohľadu na to, aké protokoly používajú. Nástroj je tiež schopný pracovať v reálnom čase a poskytuje možnosť ovládať prahy na základe presnosti detekcie a falošných pozitív. Výsledky experimentov ukazujú, že APIVADS je schopný efektívne detegovať a ochrániť aplikácie pred rôznymi typmi útokov. V porovnaní s ostatnými nástrojmi na ochranu, APIVADS

poskytuje vysokú presnosť a nízku falošnú pozitivitu. Tento nástroj by mohol byť použitý v rôznych typoch aplikácií a môže byť účinným riešením na ochranu pred kybernetickými útokmi. V závere článku sa ukazuje, že APIVADS môže byť úspešným nástrojom pre detekciu a ochranu proti rôznym druhom kybernetických útokov na aplikačné rozhrania. Tento nástroj môže byť použitý v rôznych aplikáciách a môže byť efektívnym riešením na ochranu pred kybernetickými hrozbami.

3 Spôsoby zberu dát

Na zber logov je možno využiť viacero rôznych prístupov. Medzi ne patria napríklad: WinCollect [69], WinLogBeat [71], Windows Event Collector (WEC) [73] alebo zber logov do databázy pomocou PowerShell-u prostredníctvom dostupných API pripojení.

WinCollect je nástroj od spoločnosti IBM, ktorý slúži na zbieranie event logov z Windows zariadení a ich prenos pomocou syslog správ. Je bezplatný a pomáha zhromažďovať a poskytovať informácie o bezpečnosti a prevádzke systému, ktoré sú potrebné na identifikáciu hrozieb a detekciu incidentov. Tieto informácie vo forme eventov získava prostredníctvom Windows Event Log API. Môže byť použitý v súvislosti s inými bezpečnostnými softvérovými riešeniami, ako napríklad s nástrojom QRadar, ktorý poskytuje možnosti spracovania a analýzy týchto eventov a výsledných dát. Umožňuje zbierať eventy z rôznych zdrojov, ako sú event logy systému Windows. Podporuje protokoly ako syslog, CEF, LEEF a súčasne umožňuje filtrovať a vylučovať získané eventy na základe definovaných pravidiel. WinCollect je jednoduchý na inštaláciu a konfiguráciu a je schopný pracovať s rôznymi verziami operačných systémov Windows, ako sú Windows 7, 8, 10, Windows Server 2008, 2012, 2016 a 2019. Je užitočný pre firmy a organizácie, ktoré potrebujú zabezpečiť bezpečnosť svojich sietí a systémov a identifikovať potenciálne hrozby a anomálie v prevádzke. [69] [70]

Winlogbeat je open-source nástroj od spoločnosti Elastic, určený na zber a odosielanie Windows event logov. Je postavený na rámci Beats, ktorý tvorí súčasť Elastic Stack. Umožňuje zber logov z rôznych Windows event log kanálov. Ide napríklad o aplikačné, systémové a bezpečnostné logy. Taktiež podporuje filtrovanie a parsovanie udalostí na extrahovanie konkrétnych údajov alebo polí. Zozbierané logy môže Winlogbeat odosielať na rôzne výstupy, ako napríklad Elasticsearch, Logstash alebo Kafka, čím sa umožňuje ďalšia analýza a vizualizácia dát. Celkovo je Winlogbeat mocným nástrojom na zber a odosielanie event logov z Windows. Dokáže centralizovať event logy z celej infraštruktúry organizácie, ktorá používa Windows, čo umožňuje jednoduchšiu analýzu a monitorovanie získaných eventov. [71] [72]

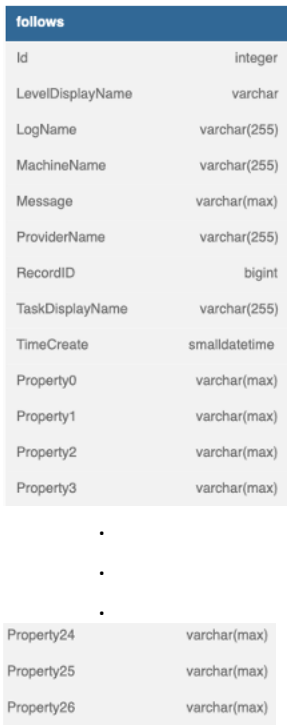
Windows Event Collector (WEC) je služba v systéme Windows, ktorá umožňuje centralizovaný zber logov z viacerých zdrojov a ich odosielanie do jedného

miesta na analýzu a monitorovanie. WEC dokáže zhromažďovať udalosti z rôznych počítačov a serverov v rámci jednej siete, pričom používa protokoly ako WinRM a HTTPS na zabezpečenie prenosu dát.

WEC sa líši od iných nástrojov na zber udalostí, ako sú WinLogBeat a WinCollect, tým, že umožňuje zber udalostí z ľubovoľného zdroja v sieti a zabezpečuje ich prenos do jedného miesta. Na rozdiel od WinLogBeat a WinCollect, ktoré sú primárne určené na zber udalostí z jedného konkrétneho zdroja, ako sú aplikácie a systémové služby. Okrem toho WEC ponúka výkonnejšie a rozšíriteľnejšie možnosti filtrovania udalostí, čo znamená, že môže byť použitý na zber len určitých typov udalostí, ktoré majú väčší význam pre organizáciu. WEC tiež umožňuje správcovi siete vytvárať a upravovať odosielateľov udalostí a nastavovať prístupové práva pre jednotlivých užívateľov a skupiny. Fungovanie WEC je založené na architektúre klient-server, kde Windows Event Collector server (WECS) sa stará o prijímanie udalostí a ich odosielanie do zvolenej cieľovej stanice. Tento server môže byť umiestnený na rôznych miestach v sieti a môže prijímať udalosti z rôznych zdrojov. Na strane klienta je potrebné nakonfigurovať Windows Event Collector klienta (WECC) pre odosielanie udalostí na server. WECC môže byť konfigurovaný pomocou nástrojov v systéme Windows alebo pomocou skriptovania. Celkovo, WEC je užitočným nástrojom pre centralizovaný zber udalostí v rámci siete, ktorý umožňuje správcom siete monitorovať a analýzovať rôzne udalosti v reálnom čase. Jeho schopnosť zberať udalosti z rôznych zdrojov a využívať robustné filtre umožňuje lepšiu kontrolu nad udalosťami, ktoré majú najväčší význam pre organizáciu. [73]

Relačná databáza - Relačná databáza, ako napríklad Microsoft SQL Server, je jednou z možností na zber a ukladanie event logov. Po nainštalovaní a konfigurácii databázového servera sa pripraví nástroj, ktorým budeme k databáze pristupovať, napríklad SQL Server Management Studio (SSMS). Na začiatku sme vytvorili databázu, ktorá slúži na ukladanie event logov. Následne sme vytvorili tabuľky, do ktorých dané event logy ukladáme. Tabuľky obsahujú tieto polia: **ID, LevelDisplayName, LogName, MachineName, Message, ProviderName, RecordID, TaskDisplayName, TimeCreated a Property 0 až 26,** ktoré budú bližšie popisovať event message a jej obsah. Môžeme si jej stavbu všimnúť na obrázku č. 1.

Obrázok č. 1 – Databázová tabuľka a jej názvy stĺpcov



follows	
Id	integer
LevelDisplayName	varchar
LogName	varchar(255)
MachineName	varchar(255)
Message	varchar(max)
ProviderName	varchar(255)
RecordID	bigint
TaskDisplayName	varchar(255)
TimeCreate	smalldatetime
Property0	varchar(max)
Property1	varchar(max)
Property2	varchar(max)
Property3	varchar(max)
.	
.	
.	
Property24	varchar(max)
Property25	varchar(max)
Property26	varchar(max)

Pre prístup k uloženým event logom v systéme a ich odosielanie do pripravených tabuliek na SQL Serveri používame napríklad PowerShell. Pomocou príkazu „Get-EventLog -LogName System“ a príkazu „Get-EventLog -LogName Security“ dokážeme pristupovať k systémovým a bezpečnostným logom systému v ktorom sú dané príkazy spustené. Následne pomocou príkazu z obrázku č. 4 dokážeme logy odosielať do vytvorenej databázovej tabuľky. Po úspešnom odoslaní event logov do relačnej databázy je možné čítať a vyhodnocovať uložené event logy pomocou databázových dopytov, ktoré umožňujú filtrovanie a vyhľadávanie dát na základe určitých kritérií. Tento postup umožňuje získavať cenné informácie a sledovať dianie v sieti, čo môže byť veľmi užitočné pre prevenciu a detekciu bezpečnostných hrozieb.

3.1 Metodológia zberu dát

V tejto podkapitole sa venujeme metodológii nastavenia systému, virtuálnych strojov a ich systémovým nastaveniam a nastaveniam ich prostredia, v ktorom pracujeme. Popisujeme nastavenie skupinových politík pre oba stroje a inštaláciu databázového servera MS SQL 2019, na ktorom ukladáme dáta v tvare systémových a bezpečnostných

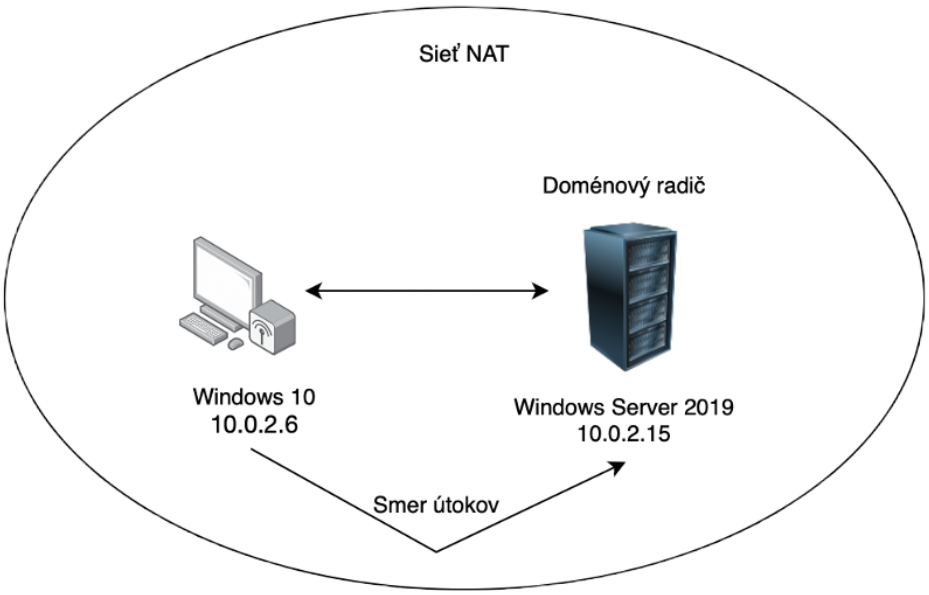
logov. Následne ukazujeme, ako tieto dáta zbierame a identifikujeme pomocou databázových dopytov.

3.1.1 Vytvorenie lokálneho systému z virtuálnych strojov

Na vopred pripravené zariadenie s operačným systémom Windows 10 sme stiahli a nainštalovali multiplatformový virtualižačný nástroj VirtualBox [87] od Oracle. Po jeho inštalácií sme v tomto nástroji vytvorili dva virtuálne stroje. Jeden pod názvom ad-server a druhý ako member-client. Obom virtuálnym zariadeniam sme v jeho nastaveniach nastavili ako hlavnú sieť „sieť NAT“. Z možností výberu vyberieme ponúkanú sieť NAT a tou je „NatNetwork“ (Názvy sa môžu líšiť, niekedy je potrebné pridať novú). Teraz sa oba stroje nachádzajú v tej istej NAT sieti a teda sú schopné spolu komunikovať a sú si navzájom viditeľné. Nachádzajú sa v rovnakej sieti.

Ad-server je stroj s operačným systémom Windows Server 2016. Naopak, na stroji client-member, bol nainštalovaný klientský operačný systém Windows 10. Oba inštalačné súbory boli stiahnuté z oficiálnych stránok Microsoft. Následne spúšťame oba stroje a ich iniciálnu inštaláciu operačných systémov. Toto nastavenie popisuje obrázok č. 2.

Obázok č. 2 – Diagram zobrazujúci prostredie

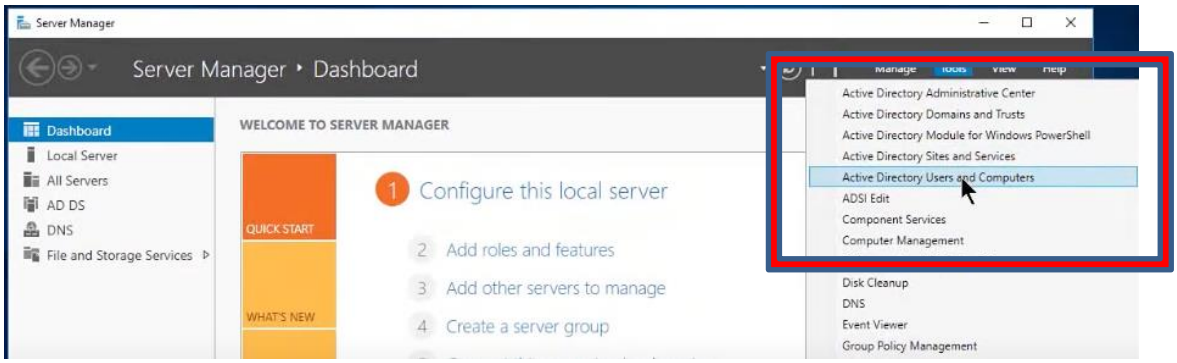


3.1.2 Iniciálne nastavenie Windows Server 2019

Po nainštalovaní Windows Servera a jeho spustení je potrebné vykonať jeho nastavenie. V Aplikácii Server Manager, ktorá sprostredkováva nastavenia servera, sme nastavili nášmu zariadeniu s operačným systémom Windows Server 2019 rolu doménového radiča. Pri vytváraní domény v nasledujúcom kroku, sme zvolili jej názov ako upjs.local.

Ak sme všetko správne nastavili a systém sa reštartoval, na hlavnej stránke Server Manager v záložke "Tools" by sme mali vidieť viacero možností, ako napríklad Active Directory Administrative Center, Active Directory Domains and Trusts alebo Active Directory Users and Computers, ako je ukázané na obrázku č. 3 nižšie.

Obrázok č. 3 – Hlavná stránka Server Managera so záložkou tools s vyššie uvedenými prvkami



3.1.3 Nastavenia skupinových politík

Nastavenie skupinových politík (Group Policy) v systéme Windows umožňuje správcom siete kontrolovať a spravovať rôzne nastavenia a politiky pre používateľov a počítače v rámci danej siete. Niektoré z príkladov, kedy sa používajú skupinové politiky, sú:

- **Bezpečnosť**: Skupinová politika môže byť použitá na zabezpečenie počítačov v sieti tým, že umožňuje správcom nastaviť bezpečnostné politiky pre používateľov a počítače. Napríklad, môže sa nastaviť politika,

ktorá vyžaduje, aby používatelia mali silné heslá, alebo politika, ktorá obmedzuje prístup k citlivým súborom alebo priečinkom.

- **Správa**: Skupinová politika môže byť použitá na spravovanie počítačov v sieti tým, že umožňuje správcom nastaviť rôzne systémové politiky a obmedzenia, ako napríklad zakázať prístup k určitým aplikáciám alebo službám.

- **Konfigurácia aplikácií**: Skupinová politika môže byť použitá na konfiguráciu rôznych aplikácií v sieti, ako napríklad Microsoft Office alebo prehliadača Internet Explorer. Správcovia môžu nastaviť politiky pre tieto aplikácie, ako napríklad predvolené nastavenia a obmedzenia pre používateľov.

Nastavenia:

Na virtuálnom stroji ad-server v systéme Windows Server 2019 sme použili aplikáciu na manažment skupinových politík "Group Policy Management" na vytvorenie dvoch nových objektov v sekcii "Group Policy Objects". Objekt pre klienta bol označený ako "WEF_audit_policy_member", zatiaľ čo objekt pre do bol pomenovaný ako "WEF_audit_policy_controller". Oba boli následne pridané pod doménu – upjs.local.

Každý z týchto objektov má svoje vlastné nastavenia audit politík. V sekcii **Computer Configuration -> Policies -> Administrative Templates -> System -> Audit Process Creation** sme pre "WEF_audit_policy_member" aj "WEF_audit_policy_controller" nastavili **Include command line in process creation events** na **ENABLED**.

V sekcii Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows PowerShell sme nastavili Turn on Module Logging na ENABLED a do hodnoty Module names vložili "*", čím sme umožnili sledovanie modulových akcií. Taktiež sme nastavili Turn on PowerShell Script Block Logging na ENABLED a zapli sme logovanie skriptových blokov.

Ďalej nasleduje nastavenie audit politík pre konkrétne skupiny. Na ich konfiguráciu sa dostaneme následovaním tejto cesty: **Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Configuration**:

Nastavenie audit politík pre skupinu member:

Tabuľka č. 8 - Nastavenie audit politík pre skupinu member

Názov audit politiky	Vybraná hodnota
Audit Credential Validation	Success and Failure
Audit Computer Account Management	Success and Failure
Audit Other Account Management Events	Success and Failure
Audit Security Group Management	Success and Failure
Audit User Account Management	Success and Failure
Audit Process Creation	Success and Failure
Audit Account Lockout	Success and Failure
Audit Logoff	Success and Failure
Audit Logon	Success and Failure
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success and Failure
Audit Detailed File Share	Success and Failure
Audit File Share	Success and Failure
Audit Other Object Access Events	Success and Failure
Audit Removable Storage	Success and Failure
Audit Audit Policy Change	Success and Failure
Audit Authentication Policy Change	Success and Failure
Audit Authorization Policy Change	Success and Failure

Audit MPSSVC Rule-Level Policy Change	Success and Failure
Audit Other Policy Change Events	Success and Failure
Audit Sensitive Privilege Use	Success and Failure
Audit Other System Events	Success and Failure
Audit Security State Change	Success and Failure
Audit Security System Extension	Success and Failure
Audit System Integrity	Success and Failure

Nastavenie audit politík pre skupinu controller:

Tabuľka č. 9 - Nastavenie audit politík pre skupinu controller

Názov audit politiky	Vybraná hodnota
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	Success and Failure
Audit Kerberos Service Ticket Operations	Success and Failure
Audit Other Account Logon Events	Success and Failure
Audit Computer Account Management	Success and Failure
Audit Distribution Group Management	Success and Failure
Audit Other Account Management Events	Success and Failure
Audit Security Group Management	Success and Failure
Audit User Account Management	Success and Failure

Audit DPAPI Activity	Success and Failure
Audit Process Creation	Success and Failure
Audit Process Termination	Success and Failure
Audit Detailed Directory Service Replication	Success and Failure
Audit Directory Service Access	Success and Failure
Audit Directory Service Changes	Success and Failure
Audit Directory Service Replication	Success and Failure
Audit Account Lockout	Success and Failure
Audit User / Device Claims	Success and Failure
Audit Logoff	Success and Failure
Audit Logon	Success and Failure
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success and Failure
Audit Detailed File Share	Success and Failure
Audit File Share	Success and Failure
Audit File System	Success and Failure
Audit Filtering Platform Connection	Success and Failure
Audit Other Object Access Events	Success and Failure
Audit Registry	Success and Failure
Audit Removable Storage	Success and Failure
Audit Audit Policy Change	Success and Failure
Audit Authentication Policy Change	Success and Failure
Audit Authorization Policy Change	Success and Failure

Audit MPSSVC Rule-Level Policy Change	Success and Failure
Audit Other Policy Change Events	Success and Failure
Audit Non Sensitive Privilege Use	Failure
Audit Sensitive Privilege Use	Success and Failure
Audit Other System Events	Success and Failure
Audit Security State Change	Success and Failure
Audit Security System Extension	Success and Failure
Audit System Integrity	Success and Failure

3.1.4 Spôsob zberu dát

Dáta zbierame nasledovne: Ako prvé vymazujeme akékoľvek logy z databázy, alebo zo systémových či bezpečnostných logov zozbieraných na systéme. Vykonávame konkrétnu vybranú techniku laterálneho pohybu. Po úspešnom vykonaní techniky spúšťame skript (Obrázok č. 4) pre systémové aj bezpečnostné logy. Tento príkaz nám parsuje logy zozbierané systémom a posúva ich ďalej do pripravenej databázovej tabuľky ktorú mu v skripte špecifikujeme. Do ľubovoľného editačného prostredia (v našom prípade poznámkový blok) si zapisujeme postupnosť event ID, ktoré sa nám v logoch vyskytli.

Túto metódu opakujeme desaťkrát pre každú zvolenú techniku, aby sme dostali dostatočnú vzorku event logov, ktoré pre danú techniku a jej následnú detekciu môžu byť v budúcnosti dôležité.

Obrázok č. 4 – PowerShell skript na zapisovanie windows logov do SQL databáz

```
$events = Get-WinEvent -LogName Security -MaxEvents 26 |
Select-Object ID, LevelDisplayName, LogName, MachineName,
Message, ProviderName, RecordID, TaskDisplayName, TimeCreated
$events2 = Get-WinEvent -LogName Security -MaxEvents 26

$connectionString = "Server=.;Database=EventCollections;User
Id=sa;Password=Asdf1234;"
$bulkCopy = new-object ("Data.SqlClient.SqlBulkCopy")
$connectionString
$bulkCopy.DestinationTableName = "systemEvents2"
$dt = New-Object "System.Data.DataTable"

$cols = $events | select -first 1 | get-member -MemberType
NoteProperty | select -Expand Name
foreach ($col in $cols)  {$null = $dt.Columns.Add($col)}
for ($i = 0; $i -le 26; $i++) { $null =
$dt.Columns.Add("Property$i") }

foreach ($event in $events2)
{
    $row = $dt.NewRow()
    foreach ($col in $cols) { $row.Item($col) = $event.$col }

    for($i = 0; $i -le 26; $i++) {
     $row.Item("Property$i") =  $event.Properties[$i].value
        Write-Host $event.Properties[$i].Key
        Write-Host '------------------'
    }

   $dt.Rows.Add($row)

}
$bulkCopy.WriteToServer($dt)
```

3.1.5 Identifikácia relevantných dát

Keďže nie všetky dáta poukazujú na využitie niektorej z techník laterálneho pohybu, je potrebné zistiť, ktoré áno. Pre túto skutočnosť musíme kontrolovať viaceré aspekty. Keďže po každom vykonaní laterálneho pohybu premazávame databázu získaných logov, zaručujeme si tým to, že len logy vygenerované spustením jednej z techník, budú po jeho spustení získané. Budú nás zaujímať logy, ktoré sú najviac frekventované, to znamená, že sa vyskytli takmer pri každom spustení. Ďalej nás zaujímajú event logy, ktoré bližšie popisujú, spustenie danej služby (napr. pri spustení PSExec sa na končiacom zariadení zapisuje event log 7036, ktorého správa je „“The

PSEXESVC service entered the running state.“ (PSEXESVC servis vstúpil do bežiaceho stavu) (Obrázok č. 5). Mimo toho, mnohé event logy nám môžu taktiež naznačiť, že došlo k nejakej anomálii. Napríklad môže ísť o správu ktorá nám síce konkrétne nehovorí, že došlo k spusteniu služby, ktorú sme spustili, no napovedá nám to v event logu správou ako napr. 5140, ktorý hovorí: „A network share object was accessed“ a teda, že niekto sa pripojil na naše sieťové zdieľanie.

Keďže určité tímy odborníkov už podobné výskumy vykonali, ich získané dáta môžu byť taktiež skvelým zdrojom informácii, v podobe logov, ktoré sa ku daným technikám viažu. Preto budeme logy získané nami na konci porovnávať a zisťovať, či daný log nemôže byť pre nás prospešný.

Obrázok č. 5 – Event log hovoriaci o spustení PSEXESVC servisy

4 Detekcia piatich najviac využívaných techník laterálneho pohybu

V tejto kapitole analyzujeme a popisujeme päť najpoužívanejších techník laterálneho pohybu. Podľa viacerých podobných prác sme získali tieto techniky: PSExec, WinRS, RDP, WMIC, net use. Každej z týchto techník pridelíme event logy, ktoré jej prislúchajú podľa nami vytvoreného postupu a analýzy, ktorý sme popisovali v predchádzajúcej kapitole.

V prípade, že niektoré logy, ktoré by sa zobrazovať pri danej technike mali, tu nie sú, môže to byť dôsledkom nenastavenia auditovania tohoto eventu v skupinových politikách doménových zariadení. V našom prípade ide napríklad o event logy 4656 a 4663. V našom prostredí sa dané logy nezískavajú z dôvodu, že sme sa nepokúšali pristúpiť k žiadnemu z objektov.

4.1 PSExec

Zdrojový počítač (Tabuľka č. 10):

Po vykonaní techniky pomocou nástroja PSExec sme na zdrojovom zariadení odsledovali nasledovné bezpečnostné event logy: 4688, 4689. Tieto logy priamo dokazujú spustenie PSExec nástroja a to tým, že popisujú zapnutie procesu psexec.exe na zariadení. Tieto logy by mali byť postačujúce pre zistenie, či na danom zariadení došlo k spusteniu tejto služby.

Tabuľka č. 10 – Tabuľka zaznamenávajúca event logy na zdrojovom zariadení pre nástroj PSExec

Systémové logy	Popis	Ak existuje – priamy dôkaz spustenia služby
Žiadne	-	-
Bezpečnostné logy	Popis	Ak existuje – priamy dôkaz spustenia služby

4688	A new process has been created	Spustenie procesu súborom "PsExec.exe“
4689	A proces has exited	Ukončenie procesu súborom "PsExec.exe“

Koncový počítač (Tabuľka č. 11):

Na koncovom zariadení sme odsledovali nasledovné bezpečnostné event logy: Zo systémových to sú 7036 a 7045 a z bezpečnostných to sú 5156, 5158, 4624, 4634, 4672, 4673, 4674, 5140 a 5145. Žiaľ, nie všetky z nich s určitosťou dokazujú spustenie služby PSExec a preto vyberieme len tie, ktoré to priamo dokážu. Medzi nimi sú systémové logy 7036 a 7045, pričom obe obsahujú processName PSEXESVC ktorý dokazuje že tento proces spustený bol. Medzi bezpečnostnými logmi sú:

- 5156 - kde port na koncovom zariadení je väčší než 1024 a port na zdrojovom zariadení je v rozmedzí 135 až 445
- 5140 - V jednom prípade obsahuje admin share „\??\C:\Windows“ a v druhom prípade admin share „*\IPC$“
- 5145 - Obsahuje v share path „\??\C:\Windows“
- 4624 + 4672 – logu 4672 nutne predchádza log 4624 a pri logu 4672 sú pripísané nové privilégia.

Tabuľka č. 11 – Tabuľka zaznamenávajúca event logy na koncovom zariadení pre nástroj PSExec

Systémové logy	Popis	Ak existuje – priamy dôkaz spustenia služby
7036	The PSEXESVC service entered the running state	Service Name: PSEXESVC

7045	A service was installed in the system	Service Name: PSEXESVC
Bezpečnostné logy	Popis	Ak existuje – priamy dôkaz spustenia služby
5156	The Windows Filtering Platform has allowed a connection	Port na koncovom zariadení je väčší než 1024 Port na zdrojovom zariadení je v rozmedzí 135 až 445
5158	The Windows Filtering Platform has permitted a bind to a local port	-
4634	An account was logged off	-
4624 + 4672	„A account was successcfully logged on“ a hneď za ním následuje „Special privileges assigned to new logon“	-
4673	A privileged service was called	-
4674	An operation was attempted on a privileged object	-
5140	A network share object was accessed	V jednom prípade obsahuje admin share „\??\C:\Windows“ a v druhom prípade admin share *\IPC$

		Dátum a čas je skorší ako dátum a čas spustenia PSEXESVC.exe
5145	A network share object was checked to see whether client can be granted desired access	Obsahuje v share path „\??\C:\Windows“

4.2 WinRS

Zdrojový počítač (Tabuľka č. 13):

Po vykonaní techniky pomocou nástroja WinRS sme na zdrojovom zariadení odsledovali nasledovné bezpečnostné event logy: 4688, 4689. Tieto logy priamo dokazujú spustenie WinRS nástroja a to tým, že popisujú zapnutie procesu winrs.exe na zariadení. Tieto logy by mali byť postačujúce pre zistenie, či na danom zariadení došlo k spusteniu tejto služby.

Tabuľka č. 13 – Tabuľka zaznamenávajúca event logy na zdrojovom zariadení pre nástroj WinRS

Systémové logy	Popis	Ak existuje – priamy dôkaz spustenia služby
Žiadne	-	-
Bezpečnostné logy	**Popis**	**Ak existuje – priamy dôkaz spustenia služby**
4688	A new process has been created	Spustenie procesu súborom "winrs.exe“
4689	A proces has exited	Ukončenie procesu súborom "winrs.exe“

Koncový počítač (Tabuľka č. 14):

Na koncovom zariadení sme odsledovali nasledovné bezpečnostné event logy: Z bezpečnostných to sú 5156, 5158, 4624, 4634, 4672, 4673, 4674, 4688, 4689, 5140 a 5145. Žiaľ, nie všetky z nich s určitosťou dokazujú spustenie služby WinRS a preto vyberieme len tie, ktoré to priamo dokážu:

- 5156 – Obsahuje destination adress (adresu koncového zariadenia0 a port zariadenia
- 4688 - Log obsahuje „C:\Windows\System32\winrshost.exe“
- 4689 - Log obsahuje „C:\Windows\System32\winrshost.exe“

Tabuľka č. 14 – Tabuľka zaznamenávajúca event logy na koncovom zariadení pre nástroj WinRS

Systémové logy	Popis	Ak existuje – priamy dôkaz spustenia služby
Žiadne	-	-
Bezpečnostné logy	**Popis**	**Ak existuje – priamy dôkaz spustenia služby**
5156	The Windows Filtering Platform has allowed a connection	obsahuje Destination adress (adresa koncového zariadenia) a source port je 5985 alebo 5986
5158	The Windows Filtering Platform has permitted a bind to a local port	-
4634	An account was logged off	-
4624	„A account was successcfully logged on“	Obsahuje account name MEMBER-CLIENT$

4672	Special privileges assigned to new logon	
4673	A privileged service was called	-
4674	An operation was attempted on a privileged object	-
4688	A new process has been created	Log obsahuje príkaz ktorý bol na zdrojovom zariadení spustený
4689	A proces has exited	Log obsahuje príkaz ktorý bol na zdrojovom zariadení spustený
4688	A new process has been created	Log obsahuje „C:\Windows\System32\ winrshost.exe“
4689	A proces has exited	Log obsahuje „C:\Windows\System32\ winrshost.exe“

4.3 RDP (Remote Desktop Protocol)

Zdrojový počítač (Tabuľka č. 15):

Po vykonaní techniky pomocou nástroja RDP sme na zdrojovom zariadení odsledovali nasledovné bezpečnostné event logy: 4688, 4689, 4648, 4673 a 5379. Väčšina týchto logo priamo dokazuje spustenie služb RDP. Medzi ne patria:

- 4688 - Log obsahuje process name „C:\Windows\System32\mstsc,exe “ a príkaz ktorý na zdrojovom zariadení spustil spustiteľný súbor mstsc.exe

- 4689 - Log obsahuje process name „C:\Windows\System32\mstsc,exe “ a príkaz ktorý na zdrojovom zariadení spustil spustiteľný súbor mstsc.exe

- 4648 - Target info je TERMSRV/adserver (resp. Hostname zariadenia na ktoré sa pripájame)

- 5379 - Target name je TERMSRV/adserver (resp. Hostname zariadenia na ktoré sa pripájame)

Tabuľka č. 15 – Tabuľka zaznamenávajúca event logy na zdrojovom zariadení pre nástroj RDP

Systémové logy	Popis	Ak existuje – priamy dôkaz spustenia služby
Žiadne	-	-
Bezpečnostné logy	**Popis**	**Ak existuje – priamy dôkaz spustenia služby**
4688	A new process has been created	Log obsahuje process name „C:\Windows\System32\mstsc,exe “ a príkaz ktorý na zdrojovom zariadení spustil spustiteľný súbor mstsc.exe
4689	A proces has exited	Log obsahuje process name „C:\Windows\System32\mstsc,exe “ a príkaz ktorý na zdrojovom zariadení spustil spustiteľný súbor mstsc.exe
4648	A logon was attempted using explicit credentials.	Target info je TERMSRV/adserver (resp. Hostname zariadenia na ktoré sa pripájame)
4673	A privileged service was called	-

5379	Credential Manager credentials were read	Target name je TERMSRV/adserver (resp. Hostname zariadenia na ktoré sa pripájame)

Koncový počítač (Tabuľka č. 16):

Na koncovom zariadení sme odsledovali nasledovné bezpečnostné a systémové event logy: Zo systémových logov sem patrí log 7036, ktorý priamo nedokazuje spustenie danej služby a z bezpečnostných to sú 5156, 5158, 4634, 4624, 4672, 4611, 4673, 4688, 4689, 4778, 4779, 4946, 4948, 4670, 4769, 4768, 4800 a 4648 a 5145. Žiaľ, nie všetky z nich s určitosťou dokazujú spustenie služby RDP a preto vyberieme len tie, ktoré to priamo dokážu. Medzi nimi sú:

- 4624 – Obsahuje LogonType 10 ktorý sa vyskytuje iba pri použití RDP
- 4778 - Obsahuje RDP-Tcp#4 a názov zdrojového počítača
- 4779 - Obsahuje RDP-Tcp#4 a názov zdrojového počítača

Tabuľka č. 16 – Tabuľka zaznamenávajúca event logy na koncovom zariadení pre nástroj RDP

Systémové logy	Popis	Ak existuje – priamy dôkaz spustenia služby
7036	Service entered running / stopped state	-
Bezpečnostné logy	**Popis**	**Ak existuje – priamy dôkaz spustenia služby**

5156	The Windows Filtering Platform has allowed a connection	-
5158	The Windows Filtering Platform has permitted a bind to a local port	-
4634	An account was logged off	-
4624	A account was successcfully logged on	Dôkaz je samotný event log s LogonType 10
4672	Special privileges assigned to new logon	-
4611	A trusted logon process has been registered with the Local Security Authority	-
4673	A privilaged service was called	-
4688	A new process has been created	Log obsahuje príkaz ktorý bol na zdrojovom zariadení spustený
4689	A proces has exited	Log obsahuje príkaz ktorý bol na zdrojovom zariadení spustený
4778	A session was reconnected to a Windows Station	Obsahuje RDP-Tcp#4 a názov zdrojového počítača
4779	A session was disconnected to a Windows Station	Obsahuje RDP-Tcp#4 a názov zdrojového počítača
4946	A change has been made to Windows Firewall	-

	exception list. A rule was added	
4948	A change has been made to Windows Firewall exception list. A rule was deleted	-
4670	Permissions on an object were changed	-
4769	A Kerberos service ticket was requested	-
4768	A Kerberos authentication ticket (TGT) was requested	-
4800	The workstation was locked	-
4648	A logon was attempted using explicit credentials	-

4.4 WMIC (Windows Management Instrumentation Command-Line)

Zdrojový počítač (Tabuľka č. 17):

Po vykonaní techniky pomocou nástroja WMIC sme na zdrojovom zariadení odsledovali nasledovné bezpečnostné event logy: 4688, 4689 a 4674. Tieto logy priamo dokazujú spustenie WNIC nástroja a to tým, že popisujú zapnutie procesu winrs.exe na zariadení. Tieto logy by mali byť postačujúce pre zistenie, či na danom zariadení došlo k spusteniu tejto služby.

Tabuľka č. 17 – Tabuľka zaznamenávajúca event logy na zdrojovom zariadení pre nástroj WMIC

Systémové logy	Popis	Ak existuje – priamy dôkaz spustenia služby
Žiadne	-	-
Bezpečnostné logy	**Popis**	**Ak existuje – priamy dôkaz spustenia služby**
4688	A new process has been created	NewProcessName je „C:\Windows\System32\wbem\WMIC.exe“
4689	A proces has exited	ProcessName je „C:\Windows\System32\wbem\WMIC.exe“
4674	A logon was attempted using explicit credentials.	Obsahuje „C:\Windows\System32\wbem\WMIC.exe“

Koncový počíta (Tabuľka č. 18)č:

Na koncovom zariadení sme odsledovali nasledovné bezpečnostné logy a tie sú 4624, 4634, 4672, 4674, 5156, 4688 a 4689. Ani jeden z týchto logov nám nedokáže jednoznačne potvrdiť využitie služby WMIC a teda našou metódou tento nástroj nevieme detegovať.

Na to, aby sme daný nástroj na koncovom zariadení detegovať mohli, potrebovali by sme použiť iný auditovací nástroj napr. Sysmon.

Tabuľka č. 18 – Tabuľka zaznamenávajúca event logy na koncovom zariadení pre nástroj WMIC

Systémové logy	Popis	Ak existuje – priamy dôkaz spustenia služby
Žiadne	-	-

Bezpečnostné logy	Popis	Ak existuje – priamy dôkaz spustenia služby
4634	An account was logged off	-
4624	A account was successcfully logged on	-
4672	Special privileges assigned to new logon	-
4674	An operation was attempted on a privileged object	Log obsahuje aplikáciu ktorú sa pomocou WMIC pokúšame spustiť (napr. cmd.exe)
5156	The Windows Filtering Platform has allowed a connection	-
4688	A new process has been created	Log obsahuje spustený príkaz
4689	A proces has exited	Log obsahuje spustený príkaz

4.5 Net use

Zdrojový počítač (Tabuľka č. 19):

Po vykonaní techniky pomocou nástroja net use sme na zdrojovom zariadení odsledovali nasledovné bezpečnostné event logy: 4688, 4689. Tieto logy priamo dokazujú spustenie net use nástroja a to tým, že popisujú zapnutie procesu net.exe na zariadení. Tieto logy by mali byť postačujúce pre zistenie, či na danom zariadení došlo k spusteniu tejto služby.

Tabuľka č. 19 – Tabuľka zaznamenávajúca event logy na zdrojovom zariadení pre nástroj net use

Systémové logy	Popis	Ak existuje – priamy dôkaz spustenia služby
Žiadne	-	-
Bezpečnostné logy	**Popis**	**Ak existuje – priamy dôkaz spustenia služby**
4688	A new process has been created	NewProcessName je „C:\Windows\System32\wbem\net.exe“ a spustený command v cmd.exe
4689	A proces has exited	ProcessName je „C:\Windows\System32\wbem\net.exe“

Koncový počítač (Tabuľka č. 20):

Na koncovom zariadení sme odsledovali nasledovné bezpečnostné event logy: Zo systémových to sú 7036 a 7045 a z bezpečnostných to sú 5156, 5158, 4624, 4634a 5145. Žiaľ, nie všetky z nich s určitosťou dokazujú spustenie služby PSExec a preto vyberieme len tie, ktoré to priamo dokážu:

- 5156 - Obsahuje source name a jeho IP adresu
- 5145 - Obsahuje názov zdieľaného média ktoré sme pripojili

PRAVDEPODOBNE SA NEDA ZISTIT

Tabuľka č. 20 – Tabuľka zaznamenávajúca event logy na koncovom zariadení pre nástroj net use

Systémové logy	Popis	Ak existuje – priamy dôkaz spustenia služby

Žiadne	-	-
Bezpečnostné logy	Popis	Ak existuje – priamy dôkaz spustenia služby
5158	The Windows Filtering Platform has permitted a bind to a local port	-
5156	The Windows Filtering Platform has allowed a connection	Obsahuje source name a jeho IP adresu -
4624	A account was successcfully logged on	-
4634	An account was logged off	-
5145	A network share object was checked to see whether client can be granted desired access	Obsahuje názov zdieľaného média ktoré sme pripojili

5 Detekcia laterálneho pohybu

V tejto kapitole sa venujeme databázovým dopytom, pomocou ktorých vieme konkrétne techniky z kapitoly 8 detegovať. Postupne ukážeme ako zistiť spustenie nástroja na koncovom aj zdrojovom zariadení aj s popisom ako dopyt funguje a na čo sa zameriava pri prehľadávaní tabuľky. Výsledkom sú databázové dopyty a výsledok, či sa dá daný nástroj detegovať.

5.1 PSExec

5.1.1 Zdrojové zariadenie

Databázový dopyt č. 1 na zdrojovom zariadení vyhľadáva akúkoľvek evidenciu o spustení služby. Tá nám je ponúkaná pri event logu 4688 a 4689. Pre jeden z týchto logov zistíme čas kedy bol daný log zaznamenaný, a uložíme si ho do premennej @TimeCreated. Ďalej prehľadávame tabuľku ale iba v tom časovom intervale, pre ktorý platí že začiatok intervalu je 3 minúty pred zaznamenaním tohoto logu, a 3 minúty po jeho zaznamenaní. Dĺžka intervalu je ľubovoľná, avšak mala by byť vyberaná rozumne, ideálne chvíľu pred spustením a chvíľu po. Následne sme pre získané logy z intervalu pridali podmienky a to také , aby sme zistili, či sa v ňom nachádzajú logy, ktoré by nám potvrdili spustenie tejto služby. V prípade PSExec ide o string „%PsExec.exe“ v oboch prípadoch logov 4688 a 4689.

Databázový dopyt č. 1 – Detekcia PSExec na zdrojovom zariadení

```
DECLARE @TimeCreated DATETIME;
SELECT @TimeCreated = TimeCreated
FROM dbo.SecurityEvents
WHERE (id=4688 AND Property5 LIKE ‘%PsExec.exe')

SELECT ROW_NUMBER() OVER (ORDER BY Id) as 'rows', *
FROM dbo.SecurityEvents
WHERE TimeCreated BETWEEN DATEADD(MINUTE, -3, @TimeCreated) AND DATEADD(MINUTE,5, @TimeCreated) AND
 ((id=4688 AND Property5 LIKE '%PsExec.exe') OR (id=4689 AND Property6 LIKE ‘%PsExec.exe'))
```

5.1.2 Koncové zariadenie

Databázový dopyt č. 2 na koncovom zariadení funguje na princípe zjednotenia systémových a bezpečnostných tabuliek. Následne sa z tejto zjednotenej tabuľky získa čas kedy bol event log potvrdzujúci spustenie služby zaznamenaný. Vytvoríme novú tabuľku, do ktorej pridáme 2 nové stĺpce pre zisťovanie aký event log sa nachádza pred

tým pozorovaným, a aký za ním. (Túto pomocnú tabuľku vytvárame pre identifikáciu event logov 4624 a 4672, ktoré v prípade služby PSExec majú nutné poradie a to také že najprv je zaznamenaný log 4624 a následne po ňom 4672). Tabuľku filtrujeme podľa časového intervalu ako pri zdrojovom zariadení. Následne z tabuľky vyberáme logy, ktoré by sa pri detekcii nástroja PSExec zobraziť mali aj s ich bližšou špecifikáciou popísanou v kapitole 4.

Databázový dopyt č. 2 – Detekcia PSExec na koncovom zariadení

```
DECLARE @TimeCreated DATETIME;

SELECT @TimeCreated = TimeCreated
FROM (
  SELECT *
  FROM dbo.SecurityEvents
  UNION
  SELECT *
  FROM dbo.SystemEvents
) se
WHERE id=7045 AND Property0='PSEXESVC';

WITH AllEvents AS (
  SELECT ROW_NUMBER() OVER (ORDER BY Id) as 'rows', *,
       LAG(id) OVER (ORDER BY TimeCreated) as PreviousEventId,
       LEAD(id) OVER (ORDER BY TimeCreated) as NextEventId
  FROM (
    SELECT *  FROM dbo.SecurityEvents UNION SELECT * FROM dbo.SystemEvents) se
 WHERE TimeCreated BETWEEN DATEADD(MINUTE, -3, @TimeCreated) AND DATEADD(MINUTE, 3, @TimeCreated) AND
((id=5156)
OR (id=4624) OR (id=4672) OR (id=7045 AND Property0='PSEXESVC') OR (id=7036 AND Property0='PSEXESVC'))
OR (id=5140 AND TimeCreated <= @TimeCreated) OR  (id=5145))

SELECT *
FROM AllEvents
WHERE TimeCreated BETWEEN DATEADD(MINUTE, -3, @TimeCreated) AND DATEADD(MINUTE, 3, @TimeCreated) AND
((id=4672 AND NextEventId =4624) OR
(id=4624 AND PreviousEventId=4672) OR ((id=5156 AND (Property6 >= 1024
OR Property6 = 135 OR Property6 = 445)) OR (id=7045 AND Property0='PSEXESVC') OR (id=7036 AND
Property0='PSEXESVC'))
OR (id=5140 AND TimeCreated <= @TimeCreated AND (Property8='\??\C:\Windows' OR Property7='\\*\IPC$')
OR (id=5145 AND (Property8 LIKE '\??\C:\Windows%'))))
```

Na užšiu detekciu, kedy chceme zistiť len IP adresu koncového a zdrojového systému, čas a uživateľa, ktorý útok vykonal, využijeme databázový dopyt č. 10 kde z celkového výseku dát si pýtame len tie, ktoré obsahujú IP adresy vzťahujúce sa k tomuto útoku, čas kedy sa útok vykonal a kto ho započal.

Databázový dopyt č. 10 – Detekcia koncového a zdrojového zariadenia, času a používateľa pri PSExec

```
SELECT TOP(1) 'PSExec' AS Name,
 (SELECT TOP(1) TimeCreated FROM AllEvents WHERE id = 7045) AS 'TimeCreated of log 7045',
 (SELECT TOP(1) Property5 FROM AllEvents WHERE id = 5156) AS 'Source IP',
 (SELECT TOP(1) Property3 FROM AllEvents WHERE id = 5156) AS 'Destination IP',
COALESCE((SELECT TOP(1) Property1 FROM AllEvents WHERE (id=5140 AND (Property1 != 'ADSERVER$' AND Property1 !=
'Administrator'))), '-') AS 'User'
FROM AllEvents
```

5.2 WinRS

5.2.1 Zdrojové zariadenie

Databázový dopyt č. 3 na zdrojovom zariadení vyhľadáva akúkoľvek evidenciu o spustení služby. Tá nám je ponúkaná pri event logu 4688 a 4689. Pre jeden z týchto logov zistíme čas kedy bol daný log zaznamenaný, a uložíme si ho do premennej @TimeCreated. Ďalej prehľadávame tabuľku ale iba v tom časovom intervale, pre ktorý platí že začiatok intervalu je 3 minúty pred zaznamenaním tohoto logu, a 3 minúty po jeho zaznamenaní. Dĺžka intervalu je ľubovoľná, avšak mala by byť vyberaná rozumne, ideálne chvíľu pred spustením a chvíľu po. Následne sme pre získané logy z intervalu pridali podmienky a to také , aby sme zistili, či sa v ňom nachádzajú logy, ktoré by nám potvrdili spustenie tejto služby. V prípade WinRS ide o string „C:\Windows\System32\winrs.exe“ v oboch prípadoch logov 4688 a 4689.

Databázový dopyt č. 3 – Detekcia WinRS na zdrojovom zariadení

```
DECLARE @TimeCreated DATETIME;
SELECT @TimeCreated = TimeCreated
FROM dbo.SecurityEvents
WHERE (id=4688 AND Property5 = 'C:\Windows\System32\winrs.exe');

SELECT *
FROM dbo.SecurityEvents
WHERE TimeCreated BETWEEN DATEADD(MINUTE, -1, @TimeCreated) AND DATEADD(MINUTE, 0, @TimeCreated)
AND ((id=4688 AND Property5 = 'C:\Windows\System32\winrs.exe') OR
(id=4689 AND Property6 = 'C:\Windows\System32\winrs.exe'))
```

5.2.2 Koncové zariadenie

Databázový dopyt č. 4 na koncovom zariadení vyhľadáva akúkoľvek evidenciu o spustení služby. Tá nám je ponúkaná pri event logoch 5156, 5158, 4634, 4624, 4672, 4673, 4674, 4688 ,4689 ,4688 a 4689. Keďže log 4688 so stringom

„C:\Windows\System32\winrshost.exe“ ktorý obsahuje názov spustiteľného súboru winrshost.exe, je priamy dôkaz spustenia WinRS, uložíme si jeho čas zaznamenania do premennej @TimeCreated. Ďalej prehľadávame tabuľku ale iba v tom časovom intervale, pre ktorý platí že začiatok intervalu je 3 minúty pred zaznamenaním tohoto logu, a 3 minúty po jeho zaznamenaní. Dĺžka intervalu je ľubovoľná, avšak mala by byť vyberaná rozumne, ideálne chvíľu pred spustením a chvíľu po. Následne sme pre získané logy z intervalu pridali podmienky a to také , aby sme zistili, či sa v ňom nachádzajú logy, ktoré by nám potvrdili spustenie tejto služby. V prípade WinRS ide o log 4688 s názvom spustiteľného súboru winrshost.exe a log 4689 s názvom spustiteľného súboru winrshost.exe

Databázový dopyt č. 4 – Detekcia WinRS na koncovom zariadení

```
DECLARE @TimeCreated DATETIME;
SELECT @TimeCreated = TimeCreated
FROM dbo.SecurityEvents
WHERE (id=4688 AND Property5 = 'C:\Windows\System32\winrshost.exe');

WITH AllEvents AS (
SELECT *
FROM dbo.SecurityEvents
WHERE TimeCreated BETWEEN DATEADD(MINUTE, -1, @TimeCreated) AND DATEADD(MINUTE, 0, @TimeCreated)
AND ((id=5156 AND Property1='System' AND Property5 = '10.0.2.15 AND Property7='6' AND (Property6='5985' OR
Property6='5986')) OR
(id=4688 AND Property5 = 'C:\Windows\System32\winrshost.exe') OR (id=4689 AND Property6 =
'C:\Windows\System32\winrshost.exe')))

SELECT * FROM AllEvents
```

Na užšiu detekciu, kedy chceme zistiť len IP adresu koncového a zdrojového systému, čas a uživateľa, ktorý útok vykonal, využijeme databázový dopyt č. 11 kde z celkového výseku dát si pýtame len tie, ktoré obsahujú IP adresy vzťahujúce sa k tomuto útoku, čas kedy sa útok vykonal a kto ho započal. V tomto prípade nemáme dostatočné typy logov na to, aby sme dokázali identifikovať názov zariadenia ktorý útok vykonalo.

Databázový dopyt č. 11 – Detekcia koncového a zdrojového zariadenia, času a používateľa pri WinRS

```
SELECT TOP (1) 'WinRS' AS Name,
 (@TimeCreated) AS 'TimeCreated of log 4688',
 (SELECT TOP(1) Property3 FROM AllEvents WHERE id = 5156) AS 'Source IP',
 (SELECT TOP(1) Property5 FROM AllEvents WHERE id = 5156) AS 'Destination IP',
 ('-') AS 'User'
FROM AllEvents
```

5.3 RDP

5.3.1 Zdrojové zariadenie

Databázový dopyt č. 5 na zdrojovom zariadení vyhľadáva akúkoľvek evidenciu o spustení služby. Tá nám je ponúkaná pri event logu 4688, 4689. Pre jeden z týchto logov zistíme čas kedy bol daný log zaznamenaný, a uložíme si ho do premennej @TimeCreated. Ďalej prehľadávame tabuľku ale iba v tom časovom intervale, pre ktorý platí že začiatok intervalu je 3 minúty pred zaznamenaním tohoto logu, a 3 minúty po jeho zaznamenaní. Dĺžka intervalu je ľubovoľná, avšak mala by byť vyberaná rozumne, ideálne chvíľu pred spustením a chvíľu po. Následne sme pre získané logy z intervalu pridali podmienky, a to také , aby sme zistili, či sa v ňom nachádzajú logy, ktoré by nám potvrdili spustenie tejto služby. V prípade RDP ide o string „C:\Windows\System32\mstsc.exe“ v oboch prípadoch logov 4688 a 4689.

Databázový dopyt č. 5 – Detekcia RDP na zdrojovom zariadení

```
DECLARE @TimeCreated DATETIME;
SELECT @TimeCreated = TimeCreated
FROM dbo.SecurityEvents
WHERE (id=4688 AND Property5 = 'C:\Windows\System32\mstsc.exe');

SELECT *
FROM dbo.SecurityEvents
WHERE TimeCreated BETWEEN DATEADD(MINUTE, -0, @TimeCreated) AND DATEADD(MINUTE, 0, @TimeCreated)
AND ((id=4688 AND Property5 = 'C:\Windows\System32\mstsc.exe') OR
(id=4689 AND Property6 = 'C:\Windows\System32\mstsc.exe')
```

5.3.2 Koncové zariadenie

Databázový dopyt č. 6 na koncovom zariadení vyhľadáva akúkoľvek evidenciu o spustení služby. Tá nám je ponúkaná pri event logu 4624, 4778 a 4779. Keďže log 4624 s typom logu 10, je priamy dôkaz spustenia RDP, uložíme si jeho čas zaznamenania do premennej @TimeCreated. Ďalej prehľadávame tabuľku ale iba v tom časovom intervale, pre ktorý platí že začiatok intervalu je 3 minúty pred zaznamenaním tohoto logu, a 3 minúty po jeho zaznamenaní. Dĺžka intervalu je ľubovoľná, avšak mala by byť vyberaná

rozumne, ideálne chvíľu pred spustením a chvíľu po. Následne sme pre získané logy z intervalu pridali podmienky a to také , aby sme zistili, či sa v ňom nachádzajú logy, ktoré by nám potvrdili spustenie tejto služby. V prípade RDP ide o string „RDP-Tcp#%“ v oboch prípadoch logov 4778 a 4778. Log 5156 by mal na mieste IP koncového zariadenia obsahovať IP adresu nášho koncového zariadenia a log 4624 by mal byť typu 10.

Databázový dopyt č. 6 – Detekcia RDP na koncovom zariadení

```
DECLARE @TimeCreated DATETIME;
SELECT @TimeCreated = TimeCreated
FROM dbo.SecurityEvents
WHERE (id = 4624 AND Property8='10');

WITH AllEvents AS (
SELECT *
FROM dbo.SecurityEvents
WHERE TimeCreated BETWEEN DATEADD(MINUTE, -3, @TimeCreated) AND DATEADD(MINUTE, 3, @TimeCreated)
AND ((id=4778 AND Property3 LIKE 'RDP-Tcp#%')
OR (id=4779 AND Property3 LIKE 'RDP-Tcp#%') OR (id=5156 AND Property5 = '10.0.2.15') OR (id = 4624 AND
Property8='10')))

SELECT * FROM AllEvents
```

Na užšiu detekciu, kedy chceme zistiť len IP adresu koncového a zdrojového systému, čas a uživateľa, ktorý útok vykonal, využijeme databázový dopyt č. 12 kde z celkového výseku dát si pýtame len tie, ktoré obsahujú IP adresy vzťahujúce sa k tomuto útoku, čas kedy sa útok vykonal a kto ho započal. V tomto prípade nemáme dostatočné typy logov na to, aby sme dokázali identifikovať názov zariadenia ktorý útok vykonalo.

Databázový dopyt č. 12 – Detekcia koncového a zdrojového zariadenia, času a používateľa pri RDP

```
SELECT TOP(1) 'RDP' AS Name,
 (@TimeCreated) AS 'TimeCreated',
 (SELECT TOP(1) Property5 FROM AllEvents WHERE id = 5156) AS 'Source IP',
 (SELECT TOP(1) Property3 FROM AllEvents WHERE id = 5156) AS 'Destination IP',
 (SELECT TOP(1) Property4 FROM AllEvents WHERE id=4778) AS 'User'
FROM AllEvents
```

5.4 WMIC

5.4.1 Zdrojové zariadenie

Databázový dopyt č. 7 na zdrojovom zariadení vyhľadáva akúkoľvek evidenciu o spustení služby. Tá nám je ponúkaná pri event logu 4688, 4689. Pre jeden z týchto logov zistíme čas kedy bol daný log zaznamenaný, a uložíme si ho do premennej @TimeCreated. Ďalej prehľadávame tabuľku ale iba v tom časovom intervale, pre ktorý platí že začiatok intervalu je 3 minúty pred zaznamenaním tohoto logu, a 3 minúty po jeho zaznamenaní. Dĺžka intervalu je ľubovoľná, avšak mala by byť vyberaná rozumne, ideálne chvíľu pred spustením a chvíľu po. Následne sme pre získané logy z intervalu pridali podmienky a to také , aby sme zistili, či sa v ňom nachádzajú logy, ktoré by nám potvrdili spustenie tejto služby. V prípade WMIC ide o string „'C:\Windows\System32\wbem\WMIC.exe'“ v oboch prípadoch logov 4688 a 4689.

Databázový dopyt č. 7 – Detekcia WMIC na zdrojovom zariadení

```
DECLARE @TimeCreated DATETIME;
SELECT @TimeCreated = TimeCreated
FROM dbo.SecurityEvents
WHERE (id=4688 AND Property5='C:\Windows\System32\wbem\WMIC.exe')

SELECT ROW_NUMBER() OVER (ORDER BY Id) as 'rows', *
FROM dbo.SecurityEvents
WHERE TimeCreated BETWEEN DATEADD(MINUTE, -3, @TimeCreated) AND DATEADD(MINUTE,5, @TimeCreated) AND
((id=4688 AND Property5='C:\Windows\System32\wbem\WMIC.exe') OR (id=4689 AND
Property6='C:\Windows\System32\wbem\WMIC.exe'))
```

5.4.2 Koncové zariadenie

Neexistuje databázový dopyt, ktorý by jednoznačne našiel využitie tejto služby na koncovom zariadení.

5.5 Net use

5.5.1 Zdrojové zariadenie

Databázový dopyt č. 8 na zdrojovom zariadení vyhľadáva akúkoľvek evidenciu o spustení služby. Tá nám je ponúkaná pri event logu 4688, 4689. Pre jeden z týchto logov zistíme čas kedy bol daný log zaznamenaný, a uložíme si ho do premennej @TimeCreated. Ďalej prehľadávame tabuľku ale iba v tom časovom intervale, pre ktorý platí že začiatok intervalu je 3 minúty pred zaznamenaním tohoto logu, a 3 minúty po

jeho zaznamenaní. Dĺžka intervalu je ľubovoľná, avšak mala by byť vyberaná rozumne, ideálne chvíľu pred spustením a chvíľu po. Následne sme pre získané logy z intervalu pridali podmienky a to také , aby sme zistili, či sa v ňom nachádzajú logy, ktoré by nám potvrdili spustenie tejto služby. V prípade Net use ide o string „C:\Windows\System32\net.exe“ v oboch prípadoch logov 4688 a 4689.

Databázový dopyt č. 8 – Detekcia Net use na koncovom zariadení

```
DECLARE @TimeCreated DATETIME;
SELECT @TimeCreated = TimeCreated
FROM dbo.SecurityEvents
WHERE (id=4688 AND Property5='C:\Windows\System32\net.exe')

SELECT ROW_NUMBER() OVER (ORDER BY Id) as 'rows', *
FROM dbo.SecurityEvents
WHERE TimeCreated BETWEEN DATEADD(MINUTE, -3, @TimeCreated) AND DATEADD(MINUTE,3, @TimeCreated) AND
((id=4688 AND Property5='C:\Windows\System32\net.exe') OR (id=4689 AND Property6='C:\Windows\System32\net.exe'))
```

5.5.2 Koncové zariadenie

Databázový dopyt č. 9 na koncovom zariadení vyhľadáva akúkoľvek evidenciu o spustení služby. Tá nám je ponúkaná pri event logoch 4624, 5156, 5158, 4634 a 5145. Keďže ani jeden z logov nie je priamym dôkazom spustenia služby net use, vieme ho detegovať iba vo vyššej miere hodnoty FP. Pre log 5156, s IP koncového zariadenia zhodujúcim sa s IP zariadenia na ktorom detekciu vykonávame a jeho portom 5985, zistíme čas, kedy bol daný log zaznamenaný a uložíme si ho do premennej @TimeCreated. Ďalej prehľadávame tabuľku, ale iba v tom časovom intervale, pre ktorý platí, že začiatok intervalu je 3 minúty pred zaznamenaním tohoto logu, a 3 minúty po jeho zaznamenaní. Dĺžka intervalu je ľubovoľná, avšak mala by byť vyberaná rozumne, ideálne chvíľu pred spustením a chvíľu po. Následne sme pre získané logy z intervalu pridali podmienky a to také , aby sme zistili, či sa v ňom nachádzajú logy, ktoré by nám potvrdili spustenie tejto služby.

Databázový dopyt č. 9 – Detekcia Net use na koncovom zariadení

```
DECLARE @TimeCreated DATETIME;
SELECT @TimeCreated = TimeCreated
FROM dbo.SecurityEvents
WHERE (id=5156 AND Property7 = '6' AND Property5 = '10.0.2.15’ AND Property6='5985');

SELECT *
FROM dbo.SecurityEvents
WHERE TimeCreated BETWEEN DATEADD(MINUTE, -3,  @TimeCreated) AND DATEADD(MINUTE, 3, @TimeCreated)
AND (id=4624 OR (id=5156 AND Property7 = '6' AND Property5 = '10.0.2.15’ AND Property6='5985'))
```

Keďže tento dopyt jednoznačne nevyznačuje miesto, kde bola daná služba spustená, nedá sa ani konkrétne určiť aká je IP koncového ani zdrojového zariadenia, ani kto daný útok započal. Preto je tento databázový dopyt nemožné vykonať a neuvádzame ho tu.

5.6 Vyhodnotenie

Nami navrhnuté databázové dopyty boli otestované na súbore viac ako 15 000 event logov, ktoré sme získali z oboch zariadení vykonávaním všetkých vyššie uvedených nástrojov. Nástroje sme spúšťali zaradom s odstupom cca 8-9 minút. Žiaden z nástrojov nebol spustený paralelne spoločne s iným.

Na tejto vzorke dát sme nakoniec naše databázové dopyty testovali. Dopyty skutočne dokázali detegovať spustenie rôznych služieb. Nástroje, ktoré nebolo možné jednoznačne detegovať sme neuviedli. Napriek tomu, že dokážeme detegovať využitie týchto nástrojov je možné, že detegujeme aj ich legitímne použitie. Pre analýzu laterálneho pohybu je dôležité vyfiltrovať tieto prípady a je na analytikovi aby vyhodnotil ich legitímnosť.

Záver

Laterálny pohyb je v dnešnej dobe počítačov a internetu rozsiahlou technikou, ktorú útočníci pri postupe sieťou využívajú. Jedná sa o súbor techník ktorými sa útočník sieťou pohybuje zo zariadenia na zariadenie a snaží sa identifikovať rôzne typy citlivých dát, ktoré by mohol zneužiť. V tejto práci sme sa venovali detekcii týchto techník pomocou databázových dopytov z tabuľky s bezpečnostnými a systémovými event logmi, ktoré nám dokázali nájsť informácie, nutné pre správnu detekciu útočníka na koncovom a zdrojovom zariadení.

Prvým cieľom tejto práce bolo analyzovať jednotlivé techniky laterálneho pohybu a priblížiť čitateľovi v čom každá z týchto techník spočíva, ako funguje, aké skupiny ju využívali a akými nástrojmi môžeme tieto techniky realizovať. Následne sme popísali, čo tieto nástroje spôsobujú, o aký typ nástroja ide, kedy bol nájdený, prípadne aký typ služby využíva.

Druhým cieľom tejto práce bola interpretácia podobných prác a ich analýza. V prácach sme popísali k akým rôznym prístupom ich výskumom dospeli a aké boli ich výstupy. Z prác sme čerpali informácie, ktoré nám pomohli bližšie a presnejšie detegovať dané techniky.

Ďalším, tretím cieľom bola príprava testovacieho prostredia, ktoré bolo pre nás kľúčovým prostriedkom pri výkone našej práce. V kapitole 3 sme popísali s akými systémami sme pracovali a základné a najmä nutné nastavenia oboch systémov v rámci siete. Následne sme oba systémy nastavili a priradili do nami vytvorených skupín v skupinových politikách operačného systému Windows Server 2019. Následne sme popísali metodológiu zberu dát pomocou PowerShellových skriptov do relačnej databázy Microsoft Server SQL. Ďalej sme popísali ako budeme relevantné dáta selektovať.

Prvým z hlavných cieľov tejto práce v kapitole 4 bola detekcia relevantných event logov zaznamenaných pomocou systému pri spustení každého z nami vybraných piatich najviac využívaných nástrojov. Následne sme vykonali útoky podľa metodológie z kapitoly 3. Výsledky sme zaznamenali a rozanalyzovali. V určitých prípadoch sme dospeli k novým ďalším dosiaľ nezisteným dátam, ktoré taktiež jednoznačne potvrdzujú

spustenie nástroja. Všetky tieto získane dáta boli najväčším vodidlom, potrebnému k detekcii.

Druhým hlavným cieľom a zároveň pridanou hodnotou tejto práce bola samotná detekcia pomocou databázových dopytov, ktorú sme popísali v kapitole 5. Keďže pri veľkom množstve zozbieraných dát je veľmi ťažko možné detegovať vykonanie techniky laterálneho pohybu, zamerali sme sa na riešenie tohoto problému. Náš implementovaný návrh bol zozbierať všetky logy do pripravenej relačnej databázy a následne z výsledkov získaných v kapitole 4 vytvoriť také databázové dopyty, ktoré by dokázali detegovať okrem samotných logov, aj aká bola IP adresa zdrojového a koncového zariadenia, ak je možné aj aký je názov zdrojového zariadenia odkiaľ útok prichádzal ale aj samotný čas, kedy k útoku došlo. To všetko ale len na koncovom zariadení, keďže hľadáme odkiaľ útok prišiel, nie kam smeroval. Hoci sa nám pri majorite nástrojov jeho spustenie nájsť podarilo, zistili sme, že nie vždy je možné daný nástroj detegovať. V určitých prípadoch nami zvolenou metodológiou vôbec, inokedy len čiastočne a nie presne, teda, že nie je zrejmé, kedy tento útok nastal a či získané logy popisujú práve hľadaný nástroj. Na to aby sme dokázali jednoznačné spustenie tohoto nástroja by sme museli využiť ďalšie iné auditovacie nástroje ako napr. Sysmon.

Na základe získaných výsledkov môžeme konštatovať, že nami navrhnutá detekčná technika je efektívna pri identifikácii útokov na koncové zariadenia. V budúcnosti by sme túto metódu radi rozšírili o ďalšie bežne využívané nástroje, ako aj o vyššie spomínané auditovacie nástroje, čo by prispelo k zvýšeniu presnosti našej detekcie.

Naším cieľom je v budúcnosti vyvinúť nástroj, ktorý by bol voľne dostupný pre všetkých užívateľov a s ďalšími úpravami by umožňoval ešte presnejšiu detekciu. Hoci už existujú podobné nástroje, ako je napríklad Hayabusa [88], tieto nástroje detegujú laterálny pohyb iba na základe jednej anomálie (jedného logu, ktorý sa javí ako podozrivý). Naša metodológia však zohľadňuje viacero aspektov súvisiacich so spustením danej služby, čo zabezpečuje vyššiu presnosť detekcie.

Keďže naša metodológia fungovala na princípe vymazávania záznamov zo systému pred opätovným spustením rovnakej služby, dokázali sme eliminovať niektoré logy, ktoré by naznačovali len prvotné spustenie služby a tým pádom sme zovšeobecnili

zisk relevantných dát. To by nebolo možné v prípade, kedy by sme pristúpili k spúšťaniu snímky virtuálneho stroja, s určitými nastaveniami.

Zoznam použitej literatúry

[1] Crowdstrike, "Lateral Movement: What It Is, How Hackers Use It, and How to Stop It," [Online]. Dostupné na: https://www.crowdstrike.com/cybersecurity-101/lateral-movement/. [Cit. 23. apr. 2023].

[2] MITRE, "SilkETW," [Online]. Dostupné na: https://attack.mitre.org/software/S0029/. [Cit. 23. apr. 2023].

[3] PCWDLD, "What Is WinRM and How Does It Work?," [Online]. Dostupné na: https://www.pcwdld.com/what-is-winrm. [Cit. 23. apr. 2023].

[4] Varonis, "What Is Mimikatz?," [Online]. Dostupné na: https://www.varonis.com/blog/what-is-mimikatz. [Cit. 23. apr. 2023].

[5] Netwrix, "CrackMapExec Tutorial: What It Is, How It Works, Best Practices," [Online]. Dostupné na: https://blog.netwrix.com/2022/12/16/crackmapexec_tutorial/. [Cit. 23. apr. 2023].

[6] JPCERT Coordination Center, "Tool Analysis Result Sheet: SilkETW," [Online]. Dostupné na: https://jpcertcc.github.io/ToolAnalysisResultSheet-SilkETW/. [Cit. 23. apr. 2023].

[7] MITRE, "SMB/Windows Admin Shares (T1210)," [Online]. Dostupné na: https://attack.mitre.org/techniques/T1210/. [Cit. 23. apr. 2023].

[8] MITRE, "Service Stop (T1534)," [Online]. Dostupné na: https://attack.mitre.org/techniques/T1534/. [Cit. 23. apr. 2023].

[9] MITRE, "Remote Services (T1021)," [Online]. Dostupné na: https://attack.mitre.org/techniques/T1021/. [Cit. 23. apr. 2023].

[10] Windows Security, "Windows Event Collector," [Online]. Dostupné na: https://www.windows-security.org/windows-service/windows-event-collector. [Cit. 23. apr. 2023].

[11] Palo Alto Networks, "What Is Lateral Movement?," [Online]. Dostupné na: https://www.paloaltonetworks.com/cyberpedia/what-is-lateral-movement. [Cit. 23. apr. 2023].

[12] Somashekarappa, N., "Lateral movement techniques used by advanced persistent threats," 2017. [Online]. Dostupné na: https://norma.ncirl.ie/6063/1/nikhilsomashekarappa.pdf. [Cit. 23. apr. 2023].

[13] ExtraHop, "Detecting Remote Services Exploitation," [Online]. Dostupné na: https://www.extrahop.com/resources/attacks/remote-services-exploitation/. [Cit. 23. apr. 2023].

[14] MITRE, "Remote Services (T1021)," [Online]. Dostupné na: https://attack.mitre.org/techniques/T1021/. [Cit. 23. apr. 2023].

[15] MITRE[15] MITRE ATT&CK. (2021). Lateral Movement. [online] Available at: https://attack.mitre.org/tactics/TA0008/ [Navštívené dňa: 24. apr. 2023].

[16] dmcxblue. (n.d.). Internal Spearphishing. [online] Dostupné na: https://dmcxblue.gitbook.io/red-team-notes/lateral-movement/internal-spearphishing [Navštívené dňa: 24. apr. 2023].

[17] Proofpoint Threat Reference. (n.d.). Bad Rabbit. [online] Dostupné na: https://www.proofpoint.com/us/threat-reference/bad-rabbit [Navštívené dňa: 24. apr. 2023].

[18] Wikipédia. (2022). Conficker. [online] Dostupné na: https://sk.wikipedia.org/wiki/Conficker [Navštívené dňa: 24. apr. 2023].

[19] Wikipédia. (2022). Emotet. [online] Dostupné na: https://en.wikipedia.org/wiki/Emotet [Navštívené dňa: 24. apr. 2023].

[20] Alpine Security. (n.d.). Empire - A PowerShell Post-Exploitation Tool. [online] Dostupné na: https://www.alpinesecurity.com/blog/empire-a-powershell-post-exploitation-tool/ [Navštívené dňa: 24. apr. 2023].

[21] Wikipédia. (2022). Flame (malware). [online] Dostupné na: https://en.wikipedia.org/wiki/Flame_(malware) [Navštívené dňa: 24. apr. 2023].

[22] MITRE ATT&CK. (2021). APT28. [online] Dostupné na: https://attack.mitre.org/groups/G0007/ [Navštívené dňa: 24. apr. 2023].

[23] MITRE ATT&CK. (2021). APT41. [online] Dostupné na: https://attack.mitre.org/groups/G0035/ [Navštívené dňa: 24. apr. 2023].

[24] MITRE ATT&CK. (2021). APT33. [online] Dostupné na: https://attack.mitre.org/groups/G0117/ [Navštívené dňa: 24. apr. 2023].

[25] MITRE ATT&CK. (2021). Magic Hound. [online] Dostupné na: https://attack.mitre.org/groups/G0045/ [Navštívené dňa: 24. apr. 2023].

[26] MITRE ATT&CK. (2021). APT40. [online] Dostupné na: https://attack.mitre.org/groups/G1001/ [Navštívené dňa: 24. apr. 2023].

[27] MITRE ATT&CK. (2021). APT32. [online] Dostupné na: https://attack.mitre.org/groups/G0047/ [Navštívené dňa: 24. apr. 2023].

[28] MITRE ATT&CK, "APT19," [Online]. Dostupné na: https://attack.mitre.org/groups/G0094/. [Cit. 24. apr. 2023].

[29] MITRE ATT&CK, "APT32," [Online]. Dostupné na: https://attack.mitre.org/groups/G0032/. [Cit. 24. apr. 2023].

[30] MITRE ATT&CK, "FIVEHANDS," [Online]. Dostupné na: https://attack.mitre.org/software/S0437/. [Cit. 24. apr. 2023].

[31] MITRE ATT&CK, "Lazarus Group," [Online]. Dostupné na: https://attack.mitre.org/groups/G0079/. [Cit. 24. apr. 2023].

[32] MITRE ATT&CK, "Mimikatz," [Online]. Dostupné na: https://attack.mitre.org/software/S0002/. [Cit. 24. apr. 2023].

[33] Microsoft, "Bitsadmin," [Online]. Dostupné na: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/bitsadmin. [Cit. 24. apr. 2023].

[34] Wikipedia, "Command-line interface," [Online]. Dostupné na: https://en.wikipedia.org/wiki/Command-line_interface. [Cit. 24. apr. 2023].

[35] Wikipédia, "Protokol prenosu súborov," [Online]. Dostupné na: https://sk.wikipedia.org/wiki/Protokol_prenosu_súborov. [Cit. 24. apr. 2023].

[36] Heimdal Security, "Netwalker Ransomware Explained: How It Works and How to Protect Your PC," [Online]. Dostupné na: https://heimdalsecurity.com/blog/netwalker-ransomware-explained/. [Cit. 24. apr. 2023].

[37] Singh, M. (2018), "Understanding Malware Analysis: A Comprehensive Approach," [Online]. Dostupné na: https://www.oreilly.com/library/view/learning-malware-analysis/9781788392501/40ceb597-1319-4eca-8d29-fbff1793f35e.xhtml. [Cit. 24. apr. 2023].

[38] MITRE ATT&CK, "Remote Services: Remote Desktop Protocol," [Online]. Dostupné na: https://attack.mitre.org/techniques/T1091/. [Cit. 24. apr. 2023].

[39] Senseon, "MITRE ATT&CK Lateral Movement Techniques - How Threat Actors Move Within a Network," [Online]. Dostupné na: https://www.senseon.io/resource/mitre-attck-lateral-movement-techniques-how-threat-actors-move-within-a-network/. [Cit. 24. apr. 2023].

[40] MITRE ATT&CK, "SMB/Windows Admin Shares," [Online]. Dostupné na: https://attack.mitre.org/techniques/T1072/. [Cit. 24. apr. 2023].

[41] MITRE ATT&CK, "PoshC2," [Online]. Dostupné na: https://attack.mitre.org/software/S0041/. [Cit. 24. apr. 2023].

[42] MITRE ATT&CK Group G0050, "Soft Cell," [Online]. Dostupné na: https://attack.mitre.org/groups/G0050/. [Cit. 23. apr. 2023].

[43] MITRE ATT&CK Group G0028, "admin@338," [Online]. Dostupné na: https://attack.mitre.org/groups/G0028/. [Cit. 23. apr. 2023].

[44] MITRE ATT&CK Group G0091, "APT40," [Online]. Dostupné na: https://attack.mitre.org/groups/G0091/. [Cit. 23. apr. 2023].

[45] MITRE ATT&CK Technique T1080, "Taint Shared Content," [Online]. Dostupné na: https://attack.mitre.org/techniques/T1080/. [Cit. 23. apr. 2023].

[46] Heimdal Security, "NetWalker Ransomware Explained: In-Depth Analysis," [Online]. Dostupné na: https://heimdalsecurity.com/blog/netwalker-ransomware-explained/. [Cit. 23. apr. 2023].

[47] Cisco, "H1N1 Technical Analysis Reveals New Capabilities," [Online]. Dostupné na: https://blogs.cisco.com/security/h1n1-technical-analysis-reveals-new-capabilities. [Cit. 23. apr. 2023].

[48] Wikipedia, "Stuxnet," [Online]. Dostupné na: https://en.wikipedia.org/wiki/Stuxnet. [Cit. 23. apr. 2023].

[49] Wikipedia, "Ramsay Malware," [Online]. Dostupné na: https://en.wikipedia.org/wiki/Ramsay_Malware. [Cit. 23. apr. 2023].

[50] MITRE ATT&CK Technique T1056.001, "Input Capture: Keylogging," [Online]. Dostupné na: https://attack.mitre.org/techniques/T1056/001/. [Cit. 23. apr. 2023].

[51] MITRE ATT&CK Technique T1003, "Credential Dumping," [Online]. Dostupné na: https://attack.mitre.org/techniques/T1003/. [Cit. 23. apr. 2023].

[52] MITRE ATT&CK Technique T1550, "Use Alternate Authentication Material," [Online]. Dostupné na: https://attack.mitre.org/techniques/T1550/. [Cit. 23. apr. 2023].

[53] Jain, U. (May 2018). "Lateral Movement Detection and Analysis for Enterprise Security," [Online]. Dostupné na: https://uh-ir.tdl.org/bitstream/handle/10657/3109/JAIN-THESIS-2018.pdf?sequence=1&isAllowed=y. [Cit. 23. apr. 2023].

[54] MITRE ATT&CK Technique T1550.003, "Steal Web Session Cookie," [Online]. Dostupné na: https://attack.mitre.org/techniques/T1550/003/. [Cit. 23. apr. 2023].

[55] MITRE ATT&CK Technique T1550.002, "Steal Application Access Token," [Online]. Dostupné na: https://attack.mitre.org/techniques/T1550/002/. [Cit. 23. apr. 2023].

[57] Netwrix. (2021). Silver Ticket Attack: What It Is and How to Defend Against It. [online] Dostupné na: https://www.netwrix.com/silver_ticket_attack_forged_service_tickets.html [Cit. 23 Apr. 2023].

[58] Netwrix. (2021). How a Golden Ticket Attack Works: Mitigation Tips. [online] Dostupné na: https://www.netwrix.com/how_golden_ticket_attack_works.html [Cit. 23 Apr. 2023].

[59] Smiliotopoulos, C., Kambourakis, G., & Kambourakis, G. (2022). Exploring the Effectiveness of an Endpoint Protection Platform in the Detection of Lateral Movement Techniques. Applied Sciences, 12(15), 7746. https://doi.org/10.3390/app12157746

[60] CENTER, JPCERT Coordination. Detecting lateral movement through tracking event logs. JPCERT Coordination Center, 2017. Dostupné na: https://www.jpcert.or.jp/english/pub/sr/ir_research.html [Cit. 23 Apr. 2023].

[61] Zhihong, T., Wei, S., Yuhang, W., Chunsheng, Z., Xiaojiang, D., Shen, S., . . . Nadra, G. (2019). Moving Target Defense for Lateral Movement Detection. In 2019 IEEE International Conference on Communications, Control, and

Computing Technologies for Smart Grids (SmartGridComm) (pp. 1–7). https://doi.org/10.1109/SmartGridComm.2019.8909762

[62] Husák, M., Apruzzese, G., & Shanchieh Jay, Y. (2021). Towards an Efficient Detection of Pivoting Activity. In 2021 IEEE 14th International Conference on Global Security, Safety and Sustainability (ICGS3) (pp. 1–7). https://doi.org/10.1109/ICGS351857.2021.9519405

[63] Apruzzese, G., Pierazzi, F., Colajanni, M., & Marchetti, M. (2017). Detecting Lateral Movement with SSH Honeypots. In 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID) (pp. 652–661). https://doi.org/10.1109/CCGRID.2017.112

[64] Security Intelligence. (2017). Exploiting Remote Desktop Protocol: A Hacker's Perspective. [online] Dostupné na: https://securityintelligence.com/articles/exploiting-remote-desktop-protocol/ [Cit. 23 Apr. 2023].

[65] GeeksforGeeks. (n.d.). MySQL Vulnerabilities. [online] Dostupné na: https://www.geeksforgeeks.org/mysql-vulnerabilities/ [Cit. 23 Apr. 2023].

[66] AppViewX, "Identifying and Mitigating Secure Socket Shell (SSH) Key Security Vulnerabilities," [Online]. Dostupné na: https://www.appviewx.com/blogs/identifying-and-mitigating-secure-socket-shell-ssh-key-security-vulnerabilities. [Cit. 23. apr. 2023].

[67] PureVPN, "How HTTP is Vulnerable to DDos Attacks," [Online]. Dostupné na: https://www.purevpn.com/ddos/http-vulnerability. [Cit. 23. apr. 2023].

[68] HackTricks, "Pentesting SMB," [Online]. Dostupné na: https://book.hacktricks.xyz/network-services-pentesting/pentesting-smb. [Cit. 23. apr. 2023].

[69] IBM, "IBM QRadar WinCollect Guide," [Online]. Dostupné na: https://www.ibm.com/docs/en/SS42VS_SHR/pdf/b_wincollect.pdf. [Cit. 23. apr. 2023].

[70] Juniper Networks, "WinCollect User Guide," [Online]. Dostupné na: https://www.juniper.net/documentation/us/en/software/jsa7.5.0/jsa-wincollect10/jsa-wincollect10.pdf. [Cit. 23. apr. 2023].

[71] Elastic, "Winlogbeat Overview," [Online]. Dostupné na: https://www.elastic.co/guide/en/beats/winlogbeat/current/_winlogbeat_overview.html. [Cit. 23. apr. 2023].

[72] Logz.io, "Windows Event Log Analysis," [Online]. Dostupné na: https://logz.io/blog/windows-event-log-analysis/. [Cit. 23. apr. 2023].

[73] Windows Security, "Windows Event Collector," [Online]. Dostupné na: https://www.windows-security.org/windows-service/windows-event-collector. [Cit. 23. apr. 2023].

[74] Varonis, "What Is Mimikatz?," [Online]. Dostupné na: https://www.varonis.com/blog/what-is-mimikatz. [Cit. 23. apr. 2023].

[75] Marques, R. S., Al-Khateeb, H., Epiphaniou, G., & Maple, C. "Detecting Lateral Movement in Enterprise Networks using Machine Learning Algorithms," IEEExplore, Január 2022. Dostupné na: https://ieeexplore.ieee.org/abstract/document/9690881?casa_token=6CSOIbyh8qMAAAAA:X_V7x64IEjrdmuz0FC-

lClirvtdxNd8H4pmBck2WorOUvLNERThJbRjsjpEjnmPNYDXJD3glYVf7. [Cit. 23. apr. 2023].

[76] MITRE ATT&CK, "Command and Scripting Interpreter: Windows Command Shell - T1059.001," [Online]. Dostupné na: https://attack.mitre.org/techniques/T1059/001/. [Cit. 23. apr. 2023].

[77] MITRE ATT&CK, "Windows Management Instrumentation - T1047," [Online]. Dostupné na: https://attack.mitre.org/techniques/T1047/. [Cit. 23. apr. 2023].

[78] MITRE ATT&CK, "MITRE ATT&CK®," [Online]. Dostupné na: https://attack.mitre.org. [Cit. 23. apr. 2023].

[79] Microsoft Security Response Center, "CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability," [Online]. Dostupné na: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0708. [Cit. 23. apr. 2023].

[80] Rapid7, "CVE-2017-0144 | Microsoft Windows SMB Remote Code Execution Vulnerability," [Online]. Dostupné na: https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-0144/. [Cit. 23. apr. 2023].

[81] MITRE ATT&CK, "Remote Services: SMB/Windows Admin Shares - T1021.001," [Online]. Dostupné na: https://attack.mitre.org/techniques/T1021/001/. [Cit. 23. apr. 2023].

[82] Oracle Corporation, "What is MySQL?," [Online]. Dostupné na: https://dev.mysql.com/doc/refman/8.0/en/what-is-mysql.html. [Cit. 23. apr. 2023].

[83] CrowdStrike, "Lateral Movement: The Basics," [Online]. Dostupné na: https://www.crowdstrike.com/cybersecurity-101/lateral-movement/. [Cit. 23. apr. 2023].

[84] Smiliotopoulos, C., "Python Evtx Analyzer," [Online]. Dostupné na: https://github.com/ChristosSmiliotopoulos/Python_Evtx_Analyzer. [Cit. 23. apr. 2023].

[85] Amazon Web Services, "What is the ELK Stack?," [Online]. Dostupné na: https://aws.amazon.com/what-is/elk-stack/. [Cit. 23. apr. 2023].

[86] JPCERT Coordination Center, "About JPCERT/CC," [Online]. Dostupné na: https://www.jpcert.or.jp/english/about/. [Cit. 23. apr. 2023].

[87] Oracle Corporation, "Oracle VM VirtualBox," [Online]. Dostupné na: https://www.virtualbox.org. [Cit. 23. apr. 2023].

[88] Yamato Security, "Hayabusa," [Online]. Dostupné na: https://github.com/Yamato-Security/hayabusa. [Cit. 14. máj. 2023].

[89] Malpedia, "win.invisimole," [Online]. Dostupné na: https://malpedia.caad.fkie.fraunhofer.de/details/win.invisimole. [Cit. 14. máj. 2023].

[90] KnowBe4, "Heads Up: A New Devilish Malware Worm Called Lucifer Is Targeting Your Windows Workstations," [Online]. Dostupné na: https://blog.knowbe4.com/heads-up-a-new-devilish-malware-worm-called-lucifer-is-targeting-your-windows-workstations. [Cit. 14. máj. 2023].

[91] Trellix, "Petya Ransomware," [Online]. Dostupné na: https://www.trellix.com/en-us/security-awareness/ransomware/petya.html. [Cit. 14. máj. 2023].

[92] Nettitude, "PoshC2," [Online]. Dostupné na: https://github.com/nettitude/PoshC2. [Cit. 14. máj. 2023].

[93] Malpedia, "win.qakbot," [Online]. Dostupné na: https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot. [Cit. 14. máj. 2023].

[94] Malwarebytes, "TrickBot," [Online]. Dostupné na: https://www.malwarebytes.com/trickbot. [Cit. 14. máj. 2023].

[95] Wikipedia (SK), "WannaCry," [Online]. Dostupné na: https://sk.wikipedia.org/wiki/WannaCry. [Cit. 14. máj. 2023].

[96] MITRE ATT&CK, "S0437," [Online]. Dostupné na: https://attack.mitre.org/software/S0437/. [Cit. 14. máj. 2023].

[97] Wikipedia (EN), "Cmd.exe," [Online]. Dostupné na: https://en.wikipedia.org/wiki/Cmd.exe. [Cit. 14. máj. 2023].

[98] Softpedia, "Gaza Cybergang Develops New Malware for Cyberespionage Campaigns," [Online]. Dostupné na: https://news.softpedia.com/news/gaza-cybergang-develops-new-malware-for-cyberespionage-campaigns-499121.shtml. [Cit. 14. máj. 2023].

[99] MITRE ATT&CK, "S0404," [Online]. Dostupné na: https://attack.mitre.org/software/S0404/. [Cit. 14. máj. 2023].

[100] MITRE ATT&CK, "S0361," [Online]. Dostupné na: https://attack.mitre.org/software/S0361/. [Cit. 14. máj. 2023].

[101] MITRE ATT&CK, "S0095," [Online]. Dostupné na: https://attack.mitre.org/software/S0095/. [Cit. 14. máj. 2023].

[102] MITRE ATT&CK, "S0698," [Online]. Dostupné na: https://attack.mitre.org/software/S0698/. [Cit. 14. máj. 2023].

[103] MITRE ATT&CK, "S0372," [Online]. Dostupné na: https://attack.mitre.org/software/S0372/. [Cit. 14. máj. 2023].

[104] MITRE ATT&CK, "S0365," [Online]. Dostupné na: https://attack.mitre.org/software/S0365/. [Cit. 14. máj. 2023].

[105] MITRE ATT&CK, "S0029," [Online]. Dostupné na: https://attack.mitre.org/software/S0029/. [Cit. 14. máj. 2023].

[106] MITRE ATT&CK, "S0140," [Online]. Dostupné na: https://attack.mitre.org/software/S0140/. [Cit. 14. máj. 2023].

[107] MITRE ATT&CK, "S0092," [Online]. Dostupné na: https://attack.mitre.org/software/S0092/. [Cit. 14. máj. 2023].

[108] MITRE ATT&CK, "S0023," [Online]. Dostupné na: https://attack.mitre.org/software/S0023/. [Cit. 14. máj. 2023].

[109] MITRE ATT&CK, "S0115," [Online]. Dostupné na: https://attack.mitre.org/software/S0115/. [Cit. 14. máj. 2023].

[110] MITRE ATT&CK, "S0132," [Online]. Dostupné na: https://attack.mitre.org/software/S0132/. [Cit. 14. máj. 2023].

[111] MITRE ATT&CK, "S0385," [Online]. Dostupné na: https://attack.mitre.org/software/S0385/. [Cit. 14. máj. 2023].

[112] MITRE ATT&CK, "S0458," [Online]. Dostupné na: https://attack.mitre.org/software/S0458/. [Cit. 14. máj. 2023].

[113] MITRE ATT&CK, "S0028," [Online]. Dostupné na: https://attack.mitre.org/software/S0028/. [Cit. 14. máj. 2023].

[114] MITRE ATT&CK, "S0130," [Online]. Dostupné na: https://attack.mitre.org/software/S0130/. [Cit. 14. máj. 2023].

[115] MITRE ATT&CK, "S0386," [Online]. Dostupné na: https://attack.mitre.org/software/S0386/. [Cit. 14. máj. 2023].

[116] MITRE ATT&CK, "S0452," [Online]. Dostupné na: https://attack.mitre.org/software/S0452/. [Cit. 14. máj. 2023].

[117] MITRE ATT&CK, "S0136," [Online]. Dostupné na: https://attack.mitre.org/software/S0136/. [Cit. 14. máj. 2023].

[118] MITRE ATT&CK, "S0041," [Online]. Dostupné na: https://attack.mitre.org/software/S0041/. [Cit. 14. máj. 2023].

[119] MITRE ATT&CK, "S0575," [Online]. Dostupné na: https://attack.mitre.org/software/S0575/. [Cit. 14. máj. 2023].

[120] MITRE ATT&CK, "S0133," [Online]. Dostupné na: https://attack.mitre.org/software/S0133/. [Cit. 14. máj. 2023].

[121] MITRE ATT&CK, "S0661," [Online]. Dostupné na: https://attack.mitre.org/software/S0661/. [Cit. 14. máj. 2023].

Prílohy

Príloha A: Zložka rozdelená do dvoch podadresárov s názvami MEMBER a ADSERVER. Obe obsahujú 5 ďalších adresárov, podľa názvov nástrojov, ktoré sme využívali: PSEXEC, WinRS, RDP, WMIC, NET USE. Každá z nich obsahuje 20 súborov s logmi. Konkrétne system1-10 pre systémové logy a security1-10 pre bezpečnostné logy, získané opakovaným spúšťaním daného nástroja.