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

Abstrakt

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

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 to je, a aké techniky a nástroje ho sprevádzajú. V druhej kapitole sa venujeme podobných 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 SQL selekty, 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	• Ransomvér • Využíva SMB protokol • Prvýkrát použitý v roku 2017
Conficker	• 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	• Malvér • Slúži na získanie prvotného prístupu do systému a následne v ňom povoľuje sťahovanie ďalších potrebných súborov • Prvýkrát objavený v roku 2014
Empire	• Empire je open source, multiplatformný framework pre vzdialenú správu a post-exploatáciu • Využíva SMB protokol • Prvýkrát objavený v roku 2019
Flame	• Môže nahrávať zvuk zo zariadení • Využíva akýkoľvek hardvér na laterálny pohyb a zber dát • Prvýkrát objavený v roku 2017
InvisiMole	• 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	• Softvér na ťažbu kryptomien • Môže využiť protokol Stratum alebo SMB • Prvýkrát objavený v roku 2020
NotPetya	• Malvér • Jeho cieľom bola deštrukcia dát a pevných diskov • Využíva protokol SMB • Prvýkrát objavený v roku 2019
PoshC2	• je open source framework pre vzdialenú správu a post-exploatáciu • Využíva SMB protokol • Prvýkrát objavený v roku 2019
QakBot	• bankový trójsky kôň • Využíva SMB protokol • Prvýkrát objavený v roku 2021
Stuxnet	• Počítačový červ • zameriava sa na programovateľné logické riadiace jednotky (PLC), ktoré umožňujú automatizáciu elektromechanických procesov • Prvýkrát objavený v roku 2020
TrickBot	• Spyware • využíva exploity EternalBlue a EternalRomance na laterálny pohyb v moduloch wormwinDll, wormDll, mwormDll, nwormDll, tabDll • Prvýkrát objavený v roku 2018
WannaCry	• 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:

  ```
  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	• 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	• 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	• Nástroj systému Windows • Spúšťanie programov, vyhľadávanie súborov
DustSky	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• Ransomvér ako služba (Ransomware-as-a-Service) • Slúži na kradnež 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	• 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	• 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 Záver

V tomto článku sme si ukázali a vysvetlili čo je to laterálny pohyb a aké sú jeho techniky. Popísali sme sa ako dané techniky fungujú, na čo sa zameriavajú a aké skupiny ich využívali. Taktiež sme si popísali aké nástroje sú s danými technikami spojené, kedy boli objavené a na akom princípe fungujú.

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] JPCERT Coordination Center. (2017). Detecting Lateral Movement through Tracking Event Logs. [online] 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].