# Trasovanie a lokalizácia dát v počítačových sieťach

Bc. František Varga

Diplomová práca
2018



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

# ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Bc. František Varga** |
| Osobní číslo: | **A16155** |
| Studijní program: | **N3902 Inženýrská informatika** |
| Studijní obor: | **Bezpečnostní technologie, systémy a management** |
| Forma studia: | **prezenční** |
| Téma práce: | **Trasování a lokalizace dat v počítačových sítích** |
| Téma anglicky: | **Tracing and Locating Data in Computer Networks** |

Zásady pro vypracování:

1. **Specifikujte technologie, které je možné pro trasování dat použít.**
2. **Stanovte omezující podmínky pro trasování komunikace.**
3. **Navrhněte metodologii pro nasazení forenzních nástrojů pro trasování.**
4. **Navrženou metodologii otestujte na technologiích: LAN, WAN, VPN**
5. **Zhodnoťte faktory ovlivňující možnosti lokalizace datových spojení.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:


1. **KOSTOPOULOS, George K. Cyberspace and cybersecurity. Boca Raton, Fl.: CRC Press, c2013. ISBN 978-1-4665-0133-1.**
2. **DONAHUE, Gary A. Kompletní průvodce síťového experta. Brno: Computer Press, 2009. ISBN 9788025122471.**
3. **SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno: Computer Press, 2010. ISBN 9788025133637.**
4. **STUART, Barbara. Forensic analytical techniques. Chichester, West Sussex, United Kingdom: Wiley, A John Wiley & Sons, Ltd., Publication, 2013. ISBN 978-0-470-68727-7.**
5. **LILLARD, Terrence. Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data. Burlington, MA: Syngress, c2010. ISBN 978-1-59749-537-0.**
6. **ALTHEIDE, Cory. a Harlan A. CARVEY. Digital forensics with open source tools. Burlington, MA: Syngress, c2011. ISBN 978-1-59749-586-8.**


Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **8. prosince 2017**

Termín odevzdání diplomové práce: **28. května 2018**

Ve Zlíně dne 8. prosince 2017

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
*děkan*

doc. RNDr. Vojtěch Křesálek, CSc.
*ředitel ústavu*

**Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

**Prohlašuji,**

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne …….

podpis diplomanta

## ABSTRAKT

Práca je zameraná na problematiku trasovania a lokalizácie dátových spojení v počítačových sieťach. Riešená je otázka trasovania v rámci lokálnej sieti, ako aj komunikácie prostredníctvom siete Internet. Pre možnosti trasovania boli zavedené OpenSource forenzné a bezpečnostné nástroje. Výstupom práce je špecifikácia možností trasovania a zhotovenie metodiky pre trasovanie komunikácie v kyberpriestore. V praktickej časti bola metodika aplikovaná na dvoch modelových prípadoch, v ktorých boli použité digitálne forenzné nástroje.



Kľúčové slová: trasovanie, kyberpriestor, log, forenzné nástroje, OpenSource, IDS



## ABSTRACT

The thesis deals with tracing and locating data connections in computer networks. It deals with tracing connections within a local network, as well as created by the Internet connections. For options to trace, were used the OpenSource computer forensics and security tools. The output of thesis is to specify options for tracing and make a methodology for tracing the network communications in a Cyberspace. The practical part applies the methodology for two cases, during which were used also the forensic and security tools.



Keywords: Tracing, Cyberspace, log, Forensics tools, OpenSource, IDS

**Poďakovanie a motto**

Rád by som chcel poďakovať vedúcemu práce Ing. Davidovi Malaníkovi, PhD. za odborné pripomienky a cenné rady poskytnuté pre vypracovanie bakalárskej práce. Najväčšie poďakovanie smeruje mojej rodine za jej podporu a lásku, nie len počas štúdia.

„You never conquer the mountain.
You only conquer yourself. “

Jim Whitaker

# OBSAH

# ÚVOD

Komunikácia na dlhé vzdialenosti bola v histórií vždy obrovskou výhodou, najmä z bezpečnostného a vojenského hľadiska. Práve vďaka týmto motívom sa tvorili prvé počítačové siete, ktoré dokázali umožniť komunikáciu medzi zariadeniami. Počítačové siete sa v modernej histórií rozšírili do enormného pokrytia a tvoria v súčasnosti najväčšiu svetovú sieť Internet. Ten je v súčasnosti využívaný na mnoho účelov prosperujúcich modernej spoločnosti, okrem iného prevod finančných prostriedkov.

Presunom stále väčšieho množstva aktív sa využívajúce informačné technológie začali objavovať aj kybernetické hrozby. Táto práca poukazuje na kybernetické útoky ako hrozbu a stanovuje metodiku pre možnosť trasovania lokalizácie dátového spojenia medzi útočníkom a obeťou v kybernetickom prostredí. Mnohé služby využívajúce Internet sú založené na presnom doručení dát od odosielateľa k príjemcovi. Pre túto funkciu počítačové siete disponujú množstvom protokolov. Práca stanovuje v teoretickej časti, aké technológie sú využívané pre komunikáciu v počítačových sieťach, ďalej opisuje kybernetickú bezpečnosť a špecifikuje technológie použiteľné na trasovanie dát.

Výstupom práce je vytvorená metodika na trasovanie dát, ktorá je súhrnom postupných krokov zberu dát, ich vyhodnotenia a skúmania. Metodika je následne implementovaná na dvoch modelových situáciách, zaoberajúcimi sa trasovaním dátovej komunikácie prostredníctvom LAN a WAN siete. Modelová situácia taktiež poukazuje na možnosti trasovania s použitím služieb VPN a Tor. V závere práce sa zhodnocujú faktory ovplyvňujúce možnosti vyšetrovateľov na lokalizovanie dátového spojenia.

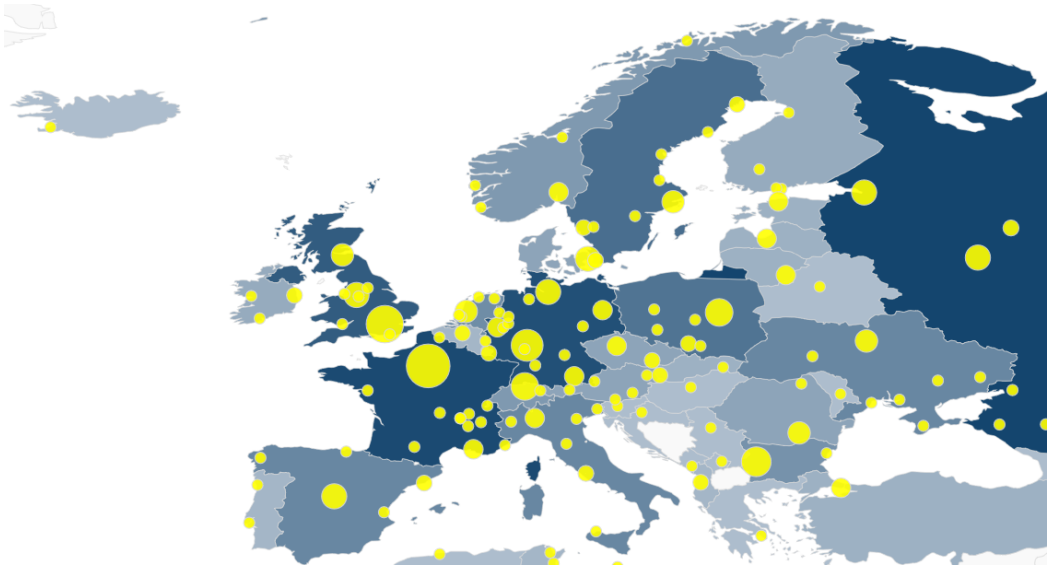
# I. TEORETICKÁ ČÁST

# 1 KYBERNETICKÝ PRIESTOR A KYBERNETICKÁ BEZPEČNOSŤ

Informačné technológie sa od čias ich začiatku vyvíjali sa exponenciálne. Vytvorením ich prepojení a komunikácie sa začali využívať na všestranné účely od prenosu správ po riadenie. S rastúcim počtom informačných systémov sa zväčšoval i tok dát, ktorým jednotlivé systémy komunikujú. Kybernetický priestor v súčasnosti zasahuje do všetkých odvetví modernej spoločnosti a to zvyšuje i potenciál zneužívania príslušných technológií na nezákonnú činnosť. Rovnako ako v prípade fyzických útokov na jedinca, skupinu či majetok, rovnako i kybernetický priestor reaguje pre svoju ochranu zvýšením bezpečnostného riadenia svojich systémov. Štáty, spoločnosti, podniky začali vnímať ohrozenie ich aktív v informačných technológiách, ktoré môže mať negatívny dopad na ich produktivitu, zisk a fungovanie. Už v roku 2001 Európska Rada [1] vyjadrila zjednotený pohľad na kriminalitu a trestnú činnosť prostredníctvom informačných technológií, čím sa začala zjednocovať legislatíva pre chápanie kybernetických trestných činov ako medzinárodný problém. Išlo o jasnú odpoveď na kybernetické útoky, ktorým bol napríklad v roku 1999 vírus Melissa [2]. Škoda bola vyčíslená na viac než 80 miliónov dolárov. Tento vírus infikoval dokumenty Microsoft Word, ktorý ako makrovírus vedel samého seba rozposielať ďalším 50 emailovým adresám, čím v konečnom dôsledku preťažil emailové systémy. V tomto roku sa antivírusové softwary rozšírili mnohonásobne po užívateľoch Internetu. V roku 2009 sa uskutočnil jeden z najväčších Fraudových prípadov – sprenevery – v histórií USA, kedy bol hacker zodpovedný za predaj desiatok miliónov čísiel kreditných a debitných kariet [3]. Hacknutá bola platobná sieť kariet z viacerých spoločnosti, ako i sieť najväčšieho reťazca potravinových samoobslužných obchodov. Hrozby kybernetických útokov môžu byť aj medzinárodného charakteru s politickým motívom, čo sa v modernej histórií už početne zachytilo, a je možné, že väčšie množstvo útokov zachytených nebolo. Začiatkom roka 2009 sa uskutočnil útok DoS (Denial-of-Service) na dvoch najväčších kirgizských poskytovateľov Internetových služieb. Pôvod útoku bol zaznamenaný z Ruska, čo vytvorilo mnohé dohady o možných politických motívoch, kedy by za útokom mohli stáť ruskí sympatizanti, ktorí týmto spôsobom protestujú voči aktuálnemu povoleniu kirgizského vzdušného priestoru pre letectvo Spojeným Štátom. [4] V roku 2011 Čínska armáda obvinila USA z vedenia celosvetovej kybernetickej vojny proti viacerým krajinám v snahe zosadiť vlády. [5] Ten istý rok boli zaznamenané útoky na Ministerstvo financií Francúzska, ktoré potvrdilo cielené útoky na dáta summitu G20, ktorý sa uskutočnil vo februári. [5]

## 1.1 Kybernetický priestor - Internet

Rozsiahla sieť, ako sa prekladá Wide Area Network (WAN), je súborom sietí prepojených prostredníctvom verejne dostupnej služby, prípadne služby pokrývajúcu veľké geografické územie. Celosvetová sieť Internet je prepojenou formou viacerých WAN sietí (tie sú zasa prepojením viacerých LAN sietí), ktoré pokrývajú jednotlivé časti Zeme. Približne 95% protokolov používaných pre transport dát v Internete má charakter TCP/IP (Transmission Control Protocol/Internet Protocol). Pomocou tohto protokolu je možné prepojiť dvoch klientov so sieťovými službami na aplikačnej úrovni. [6] Jednotlivé zariadenia počítačov pracujú ako klienti alebo sú servermi, ktoré poskytujú služby klientom. Zaujímavým aspektom Internetu sú body prepojenia a smerovania jednotlivých WAN sietí. V dnešnej podobe sa nazývajú ako Internetový body výmeny dát (IXP – Internet eXchange Points), ktoré slúžia pre spojenie poskytovateľov služieb s národnými sieťami.



Obrázok 1. Internetové body výmeny dát IXP v Európe. [7]

IXP je prakticky sieťový uzol určený k prepojeniu sietí poskytovateľov internetových služieb. Tam prebieha výmena dát medzi sieťami vďaka vzájomnej párovanej zmluve (mutual pairing agreement). Prepojenie IXP prebieha prostredníctvom vysokorýchlostných optických káblov. Rovnako i v prípade interkontinentálneho spojenia IXP bodov sa používajú pre ich prepojenie podmorské optické káble. Body IXP majú iba funkciu prepájania prevádzky medzi sieťami. Ostatné funkcie ako profilovanie prevádzky, správa smerovania a filtrovania sú na jednotlivých zúčastnených poskytovateľoch Internetového pripojenia. Ak sú dvaja poskytovatelia pripojenia prepojení i priamo, využitie IXP bodov používajú iba ako zálohu v prípade, ak sa priame pripojenie sa preruší. [6]

### 1.1.1 TCP/IP protokoly

Ako bolo spomenuté, najčastejšími protokolmi, ktoré sa využívajú v sieti Internet sú takzvané TCP/IP protokoly. Tie však obsahujú ďalšiu sadu protokolov a štandardov pre zasielanie dát v sieti. Technológia TCP vytvára virtuálne spojenie medzi dvoma koncovými bodmi, riadi prenos dát a zaisťuje ich doručenie. Pakety sa však zasielajú prostredníctvom Internet Protocol – teda IP protokolu. Ten sa používa k zabaleniu dát zasielaných do siete s prepínaním paketových dát a taktiež k adresovaniu systémov v sieti. [6]

**Protokol TCP**

Ide o najpoužívanejší transportný protokol v počítačových sieťach. V TCP sa nachádzajú sady riadiacich príkazov, ktoré majú vplyv na množstvo obsiahnutých dát v jednotlivých paketoch. Týmto protokolom prebieha komunikácia, ktorá umožňuje doručovanie elektronickej pošty, sledovanie webových stránok, či komunikácia s programami pre prenášanie súborov. Ide pritom o vyriešenie hlavného problému niektorých nespoľahlivých protokolov. Dáta sa rozdelia do IP paketov a sú prenesené vo forme sady IP požiadavkov. Musí následne existovať mechanizmus pre riadenie toku týchto paketov. IP paket sa skladá z tela a záhlavia. V záhlaví sa nachádzajú informácie o cieli paketu, prípadne výber trasy pre cestu paketu, veľkosť dát v tele a kontrolný súčet. Nachádza sa v záhlaví aj takzvaný „príznak“ (Flags) paketu – kontrolné bity, ktoré sa používajú pre definovanie štádia pripojenia a pre informatívne účely. TCP umožňuje multiplexovanie, ktoré zaisťuje súbežný tok dát za pomoci paralelných procesov. To slúži k zrýchleniu a optimalizácií dátových procesov. Ide napríklad o možnosť sťahovania cez webový prehliadač viacero súborov súbežne.

**Protokol UDP**

Ako jeden z Internetových protokolov slúži k založeniu nestavových spojení medzi hosťami v sietí IP. Prostredníctvom UDP sa vymieňajú krátke úseky dát – datagramy. Využíva rovnaký typ multiplexovania prostredníctvom princípu portov ako TPC, ale nepodporuje ho mechanizmus pre zaistenie platnosti dát, ktoré zasiela. UDP sa preto používa v prípade, že nie je vyžadovaná spoľahlivosť dát – kratšie správy a redundancia, čo na druhej strane urýchľuje prenos dát. Ako príklad, systém doménových mien DNS využíva UDP, rovnako ako i DHCP protokol pre dynamickú konfiguráciu hostiteľov, ale i SNMP pre rýchlu správu siete. S protokolom TCP sa UDP dopĺňa vo funkciách, kde TCP sa dokáže vysporiadať so zahltením, kým UDP s veľkým množstvom prenosov. V tabuľke 1. sú zobrazené najpoužívanejšie porty.

Tabuľka 1. Najpoužívanejšie Porty v rozsahu 0 až 1023. [6]

| Port | Význam |
|---|---|
| 1 | Multiplexor služieb na TPC portoch |
| 20 | FTP – štandardný port pre dáta |
| 21 | FTP – štandardný port pre príkazy |
| 22 | Protokol SSH pre vzdialené prihlásenie |
| 25 | Protokol SMTP (Simple Mail Transfer Protocol) |
| 43 | Protokol WHOIS |
| 53 | Systém DNS (Domain Name System) |
| 80 | Protokol HTTP (Hypertext Transfer Protocol) |
| 110 | Protokol POP3 (Post Office Protocol 3) |
| 143 | Protokol IMAP (Internet Message Access Protocol) |
| 443/TCP | Protokol HTTP nad TLS/SSL (HTTPS) |
| 514/UDP | Protokol Syslog |
| 993/TCP | Protokol IMAP nad TLS/SSL (IMAPS) |
| 995/TCP | Protokol POP3 nad TLS/SSL (POP3S) |

### 1.1.2 Protokol IP

Hlavnou funkciou IP protokolu je doručovanie paketov medzi koncovými bodmi v TCP/IP sieťach. Ide o nestavový a smerovateľný protokol, tolerantný k výpadkom siete. Existujú dve verzie IP: IPv4, ktorý je stále najrozšírenejším s 32bitovými adresami (v desiatkovom formáte ###.###.###.###); a IPv6, ktorý pomaly nahradzuje staršiu verziu pri stále rozrastajúcom sa Internete, využívajúc adresy s 128 bitmi, zapisujúc v hexadecimálnom formáte (rozdelené do 8 skupín nnnn:nnnn:nnnn:nnnn:hhhh:hhhh:hhhh:hhhh, kde písmena n identifikujú sieť a písmená h identifikujú hostiteľa). [8]

Adresy IPv4 je možné triediť podľa bitov na začiatku adresy – Trieda A, bit 0 (0.x.x.x) ; Trieda B, bity 10 (128.x.x.x) ; Trieda C, bity 110 (192.x.x.x). Sieť následne môžeme rozdeliť na rôzne skupiny podľa veľkosti prefixu /N (masky). Prefix uvádza, aký počet bitov v binárnom zápise je zo sieťového bloku vylúčených. Čím väčšie je číslo prefixu, tým je označený sieťový blok menší. V súčasnosti je Internet rozdelený na niekoľko geografických regiónov. Každý z nich má priradené rozsahy adries. Výsledkom je efektívne smerovanie na kombináciu geografických a adresných informácií. Regionálni internetoví regis-

trátori (RIR) sa zaoberajú blokmi s prefixami /8 (obsahujúcimi 16 777 216 adries). Pre Európu spravuje IP adresy organizácia RIPE Network Coordination Centre (RIPE NCC).


Obrázok 2. RIR organizácie a ich obsadenie vo svete. [18]

V databázach RIR je možné vyhľadávať systémom WHOIS, ktorý poskytuje verejne dostupné informácie o tom, komu boli zadané bloky adries pridelené. Okrem služby WHOIS, RIR poskytuje alokáciu adries IPv4 a IPv6, registráciu autonómnych systémov, reverzné vyhľadávanie v DNS a register smerovania na Internetu. V rámci IPv4 nie sú všetky adresy dostupné. Adresy bývajú rezervované pre konkrétny účel. Organizácia IANA rezervovala adresy pre typy sietí: miestna (0.0.0.0/8), privátne (npr. 10.0.0.0/8 alebo 192.168.0.0/16), spätnej slučke (loopback 127.0.0.0/8), viacsmerové vysielanie (pre multicast a broadcast) a iné. [6] Každá sieť, ktorá má dostatočný rozsah prefixu, sa môže rozdeliť na podsiete prostredníctvom zmenšenia prefixu a vyhradenia počtu adries pre jednotlivé podsiete.

Pod IP protokolmi sa zahŕňa aj ARP protokol (Adress Resolution Protocol) pre automatizáciu procesu prekladania adries a názvov. Umožňuje zobrazenie tabuľky s IP adresami, ich odpovedajúcimi fyzickými (MAC) adresami, index sieťového rozhrania alebo portu a typ priradenia položky (statická, dynamická, neplatný záznam, neexistujúce priradenie). Táto tabuľka sa automaticky upravuje. Zariadenie využívajúce zachytenie tohto protokolu ukladá ARP údaje po dobu nastaveného času. ARP patrí medzi protokoly linkovej vrstvy, preto sa nedá smerovať a je obmedzený len na miestnu sieť alebo podsieť. [6]

## 1.2 Kybernetická bezpečnosť

Počítače môžu byť obeťami, ale rovnako i použité pre tvorbu protiprávnych činností. Počet kybernetických hrozieb ustavične narastá. Riešenia kybernetickej bezpečnosti sa snažia tento trend konvergovať. Pre zvýšenie povedomia o týchto hrozbách sa začali tvoriť skupiny CERT (Computer Emergency Response Team) zaoberajúce sa riešením mimoriadnych udalostí. Pre Českú republiku v súčasnosti túto funkciu zastáva Národní úřad pro kybernetickou a informační bezpečnost, ktorý spolupracuje s medzinárodnými CERT a CSIRT tímami. [9] Kybernetická kriminalita zahŕňa viacero aspektov, ktoré nesúvisia iba s oblasťou bezpečnosti informačných systémov, ale i využívania kybernetického priestoru pre nelegálnu činnosť, ako programové pirátstvo, detská pornografia, nezákonné hazardné hry, propagácia kontextu nenávisti (extrémizmus, terorizmus), vydieranie, intelektuálne kradnutie majetku, e-špionáž a mnoho ďalších. [10] Kybernetické hrozby sa môžu rozdeliť do troch hlavných skupín, menovite nedovolená zmena dát, nedovolený prístup k dátam a nedovolené blokovanie dostupnosti dát. Riziko pre spoločnosť sa tvorí najmä dopustením príležitosti pre nelegálnu činnosť, ktorá by spôsobila spoločnosti škodu. Zdroj rizika môže prameniť z hardwaru, softwaru a ľudí. [5]

Profesionáli v kybernetickej bezpečnosti musia mať široké spektrum zručností a odborností. Jednotlivé špecializácie môžeme deliť do štyroch skupín: [5]

- administrácia systému (údržba serveru, zhoda s politikou - SW, firewall a doplnky).
- penetračné testovanie (prienik do systému, siete, OS, webové aplikácie).
- kybernetický audit a forenzné vyšetrovanie (obnova dát, vyšetrovanie malwaru, zariadenia, sieťové protokoly, detekcia prieniku, reakcia na incident).
- manažment kybernetickej bezpečnosti (zhoda s politikou - ľudia, postupy vyšetrovania, dokumentácia, právne aspekty).

### 1.2.1 Zákon o kybernetickej bezpečnosti, č. 181/2014 Sb.

V súčasnosti moderné krajiny odpovedajú na hrozby počítačovej kriminality zvýšením povedomia a kritérií pre chod informačnej infraštruktúry prostredníctvom zákonov a medzinárodných ustanovení. Medzi takéto krajiny patrí v Európe väčšina západných krajín ako Veľká Británia, Nemecko, od apríla 2018 aj Slovenská republika a od 2014 aj Česká republika. Zákon s vyhláškou č. 316/2014 Sb. (vyhláška o kybernetickej bezpečnosti) [11] vymedzujú, kto je povinný sa zákonom riadiť, kam okrem iných patrí aj poskytovateľ

služby elektronických komunikácií, osoba/orgán zaisťujúcu významnú sieť, správca a prevádzkovateľ informačného a/alebo komunikačného systému kritickej infraštruktúry a poskytovateľ digitálnej služby. Uvádza i kategórie opatrení, ktoré delí na organizačné a technické. Medzi technické opatrenia patria taktiež nástroje pre zber a vyhodnocovanie kybernetických bezpečnostných udalostí, nástroj pre zaistenie úrovne dostupností informácií, prípadne nástroj pre ochranu integrity komunikačných sietí. Úrady sú povinné si viesť evidenciu kybernetických bezpečnostných incidentov, s údajmi o zdroji incidentu.

## 1.3 Trendy kybernetickej bezpečnosti

V súčasnosti kybernetická bezpečnosť zaviedla niekoľko best practice – najlepších riešení odskúšaných praxou. Jednotlivé oblasti kybernetickej bezpečnosti, ktoré boli spomenuté, sa dajú deliť aj podľa ich zavedenia z pohľadu prevencie, reakcie na incident, alebo reakcie po incidente, respektíve vylepšení preventívnych nástrojov a spôsobov.

### 1.3.1 Etický hacking

Etický hacking je inak povedané penetračné testovanie IT systémov a infraštruktúr. Ide o testovanie zraniteľnosti sietí, webových aplikácií, stránok, databázy a ďalších systémov. Pri hľadaní zraniteľnosti sa využívajú dostupné riešenia, ktoré by mohol použiť prípadný útočník – hacker pre prelomenie ochrany systému a zneužitie daných materiálov. Hlavným cieľom etického hackingu je otestovanie systémov, ktorým by ich znehodnotenie mohlo priviesť spoločnosti vysoké finančné straty. Testovanie má predbiehať kybernetických kriminálnikov v odhaľovaní slabých miest a zároveň v nezneužití informácií, ku ktorým etický hacker získa prístup. Ide predovšetkým o preventívne opatrenie.

### 1.3.2 Forenzné vyšetrovanie dát

Pri forenzných vyšetrovaniach ide o reaktívnu činnosť po incidente spáchanom na informačnom systéme. Hlavným cieľom je spätné dohľadanie koreňa problému incidentu, nájdenie a vyselektovanie páchateľov, zistenie motívu, návrh a implementácia bezpečnostného riešenia pre zabránenie opakovateľnosti incidentu. Primárne je potrebné zistiť obmedzenia a vyšetrovateľské požiadavky pre dôkazy, mieru očakávaného súkromia zúčastnených osôb, ako aj mieru očakávania možných ďalších súdnych procesov v prípade vyšetrovania v privátnom sektore. Výsledkom vyšetrovania by mali byť jasne obhájiteľné dôkazy pre prípad vznesenia obvinenia a možného následného súdneho sporu. [10]

Zdroje dát pri kybernetických forenzných vyšetrovaniach môžu byť rôzne schované vo viacerých zariadeniach – počítačoch, pamäti tlačiarne, ale aj na prenosných zariadeniach (notebooky, flash disky, externé hardisky, CD, DVD, pamäťové karty, mobily/tablety) či dokonca na internetových serveroch (sieťových, cloudových, e-mailoch, zvukových správach, serveroch poskytovateľov internetových služieb).

Dáta pre forenzné vyšetrovanie môžu byť delené na tri formy: extrahovateľné digitálne dáta, metadáta a latentné/skryté digitálne dáta. Extrahovateľné dáta môžu byť definované ako „pozorovateľné“ dáta, kedy sa použijú potrebné technológie pre ich načítanie, analýzu, spracovanie a vyvodenie záverov. Je preto nutné mať správne znalosti nástrojov a techník pre lokalizovanie a konvertovanie dát do pozorovateľného štádia pre nájdenie hľadaných informácií. Jedny z takýchto nástrojov sú takzvané datamining, ktoré následne hľadajú v dátach stopy o kriminálnej činnosti. Metadáta sú informácie zachytené v aplikáciách s potenciálnym zdrojom dôležitých informácií alebo dôkazov. Dá sa povedať, že metadáta sú dáta o dátach, ktoré prinášajú základné informácie, napríklad o súboroch – čas ich tvorby, modifikácie, posledného prehliadania, lokácie, mena, konkrétne štatistiky, veľkosť, v prípade digitálnych fotografií i viaceré informácie o fotoaparáte, ktorý ich zachytil. Môže pritom ísť o štruktúrovanú databázu, „vlastnosti“ (properties) konkrétnych súborov, či systémové logy aktivít užívateľov. Pri latentných dátach hovoríme o vyššej obtiažnosti získania dát, ktoré sú neobjaviteľné štandardnými cestami. Môže ísť o dáta vymazané, dočasné dáta, RAM, dočasne stiahnuté dáta pri webovom prehliadaní, neprepísané miesto na disku alebo dáta uložené v dočasných pamätiach zariadení ako skener a tlačiareň. Inak povedané, páchateľ schováva dáta a neočakáva ich odhalenie. Jeden zo spôsobov, ako to docieliť, je použitie stenografie. Čím sofistikovanejší sú páchatelia, o to ťažšie je vystopovanie latentných dát. [10]

Proces vyšetrovania sa pritom riadi veľmi podobným spôsobom ako pri vyšetrovaní nekybernetického incidentu. Špecifikom je hlavne zaistenie originálnych dôkazových dát, ktoré musia byť neporušené. Pri ich zaistení je nutné odobrať HASH-e jednotlivých dôkazov, ktoré sa pred analýzou po transporte overujú, aby ich autenticita bola stopercentná. Samotná analýza sa tvorí na skopírovaných dôkazoch(s rovnakým HASH výsledkom) bez modifikácie originálu. Následne sa postupuje podľa vopred stanoveného plánu práce s dátami pre zachovanie ich autenticity a dáta sa prekonvertujú do podoby vhodné na prezentáciu. Všetky dáta a výsledky sa následne zdokumentujú a vyhodnocujú.

### 1.3.3 Sieťové bezpečnostné prvky

Pre bezpečnosť sietí sa využívajú monitorovacie preventívne opatrenia, ktoré v prítomnom čase reagujú na pripojené zariadenia a tok dát v monitorovanej sieti. Medzi najznámejšie patria firewall, systém detekcie prieniku a systém prevencie prieniku. [8]

Firewall je brána ktorá umožňuje správcovi kontrolovať prístup medzi vonkajšou sieťou a prostriedkami riadených prenos toku dát spravovanej firmy. Firewall tým izoluje vnútornú sieť organizácie od Internetu. Úlohou Firewallu je spravovať a definovať v miestnych zásadách zabezpečenie, aby mohola do siete organizácie prejsť iba autorizovaná prevádzka. Existujú rôzne typy firewallu, jednoduché ale i komplexné. Môžu byť implementované v software, ale existujú aj také, ktoré sú inštalované na vyhradený hardware; niektoré fungujú v rámci prostredia operačného systému, iné ako „čierne skrinky“ so svojím vlastným operačným systémom. Základnými vlastnosťami firewallu sú filtrovanie paketov, vstupné filtry sieťového rozhrania, preklad sieťových adries NAT, stavová kontrola paketov, kontrola okruhu, proxy firewally a aplikačné filtre. [6]

Paketové filtre kontrolujú záhlavie paketov IP, TCP, UDP a ICMP. Následne rozhodujú, ktoré pakety prejdú cez bránu firewall. Pre detekciu útoku je však potrebné previesť hĺbkovú kontrolu paketov, ktorá nesleduje iba záhlavie ale nahliadne aj do skutočných aplikačných dát prenášaných dát. Takéto zariadenie môže vďaka týmto detekčným schopnostiam detekovať podozrivý paket alebo sériu paketov. Následne môže rozhodnúť či daný paket nevpustí do systému. V prípade podozrenia je možné i po vpustení paket ďalej evidovať ako podozrivý s označením upozornenia pre správcu siete, ktorý danú komunikáciu preskúma a prijme vhodné opatrenia. Takémuto zariadeniu, ktoré generuje upozornenia hovoríme Systém detekcie prieniku (IDS – Intrusion Detection System). Ak zariadenie filtruje komunikáciu, hovoríme o Systému prevencie prieniku (IPS – Intrusion Prevention System). [8] Ich princíp zistenia podozrivého prenosu je však totožný, jediný rozdiel nastáva v konaní, ktoré vyústi po detekcií. Keďže IDS sondy monitorujú prevádzku systému, môžu sa vysporiadať nielen s externým, ale aj interným nebezpečenstvom. Pre implementáciu IDS rozoznávame tri základné spôsoby. [12] Prvým je sieťový (Network-based) IDS, ktorý sleduje celé sieťové prostredie a hľadá v ňom signatúry detekcie. Druhým je hosťovský (Host-based) IDS. Ten obraňuje konkrétny systém v sieti, ako napríklad počítač alebo server. Treťou konfiguráciou IDS je distribuovaný (Distributed) IDS založený na systéme rozmiestnenia senzorov po sieti, ktoré posielajú správy riadiacemu systému. V praxi sa používajú najmä kombinácie týchto typov.

IDS sleduje hrozby siete dvojakým spôsobom detekcie. Prvým spôsob je detekcia signatúr, ktorá pracuje podobným spôsobom ako antivírusové programy používajúce vírové signatúry, ktoré následne odhaľujú medzi súbormi, programami, či webovým obsahom vstupujúcim do systému. Detekcia signatúr prebieha monitorovaním sieťovej komunikácie, jej analýzou a následným porovnaním s databázou známych ukazovateľov, ktoré označujú prípadné bezpečnostné riziko. Druhým spôsobom detekcie je detekcia anomálií identifikujúca abnormálne aktivity systému. Používa pravidlá, ktoré definujú koncept „normálu“ a „abnormality“, aby boli odhalené odklony od bežného chovania systému. Následne prebehne potrebné opatrenie, ktorým buď zablokuje komunikáciu alebo informuje správcu systému. Tento spôsob je však náročnejší na čas, personál i financie. [12]

# 2 KOMUNIKÁCIA V SIEŤACH Z POHĽADU TRASOVANIA

Základným pilierom systémov informačných technológií je ich prepojiteľnosť a komunikácia, ktorá spočíva v sieťovaní jednotlivých zariadení. Počítačové siete sa skladajú z rôznych stavebných blokov ako sú počítače, káble, sieťové prepínače a pod.. Každá komunikácia, ktorá sa uskutoční medzi dvoma koncovými bodmi, prechádza danou trasou práve týmito prvkami. „Priama cesta“ medzi nimi je čisto virtuálna a spojená správnym nakonfigurovaním viacerých fyzických medzi-prvkov. Virtuálna cesta môže byť rôzna na základe siete, ktorou komunikuje.

## 2.1 Hardwarové prvky sietí

Ku komunikácii v sieťach dochádza predovšetkým vďaka hardwarovým prvkom, ktoré posielajú, prenášajú, presmerujú alebo prijímajú dáta. Okrem koncových zariadení v podobe počítačov, môžeme hovoriť o serveroch, smerovačoch (router), prepínačoch (switch), mostoch (bridge) a prenosových médiách (káble alebo bezdrôtová komunikácia). Z typov serverov sú pre komunikáciu zaujímavé sieťové servery, ktoré ponúkajú funkcie identifikácie systému, smerovania a pod., kedy môžeme hovoriť napríklad o DHCP alebo DNS serveroch. Prepínač je aktívnym zariadením spájajúci jednotlivé časti siete. Používa sa ako centrálny prvok, podobne ako rozbočovač (hub), ale na rozdiel od neho dokáže rozpoznať zariadenia podľa MAC adresy priradených k jednotlivým portom. [6] Prepínače, ktoré sú bez administrácie (nemanažované), nie je možné konfigurovať a spravovať na diaľku. Prepínače s administráciou využívajú ku konfigurácií agent SNMP, rozhranie CLI na konzole, prípadne aj webové rozhranie. Sieťový most sa používa k prepojeniu dvoch rôznych typov fyzických médií sieťových segmentov v rámci jednej podsiete. Skúmajú cieľovú MAC adresu sieťovej prevádzky. [8] Smerovač je zariadenie, ktoré prepája aspoň dve rôzne siete. Ide o inteligentný prvok, ktorý dokáže filtrovať, blokovať broadcast, zisťuje optimálnu trasu paketov a rozdeľuje kolízne domény. Súčasťou smerovača sú pravidlá, ktoré určujú, či pakety môžu byť vpustené alebo budú zachytené filtrom a zahodené. Analyzuje adresu jednotlivých datagramov, ktoré ním prejdú a podľa toho určuje cieľovú destináciu dát. Smerovače komunikujú a informujú o stave siete prostredníctvom netradičných protokolov ako ICMP. K smerovaniu sa používajú smerovacie protokoly, ktoré priraďujú adresu jednotlivým koncovým bodom. Medzi takéto protokoly patria aj OSPF (skúma stav liniek) a RIP (používa techniku vektorov vzdialeností). [6]

Prechod medzi jednotlivými prvkami sietí sa nazýva sieťové rozhranie. Ide buď o bod stretu či dotyku rôznych sietí, virtuálny objekt operačného systému (software), rozdelenú sieť pripojenú k smerovači, bod pripojeného terminálu alebo ide o sieťovú kartu. Z pohľadu komunikácie je hlavným partnerom práve sieťové rozhranie a jemu priradená sieťová adresa. Sieťová karta sa vyznačuje i tým, že má vlastnú unikátnu pevne viazanú fyzickú MAC adresu uloženú v pamäti určenej len na čítanie (Read Only Memory). Táto adresa slúži k vytvoreniu unikátnej cieľovej destinácie pre komunikáciu. [6]

## 2.2 Typy sietí a ich komunikácia

Pre správne pochopenie komunikácie a následného trasovania, je vhodné pochopiť fungovanie základných typov sietí a ich prepojenie na aplikácie pre prípad spätného trasovania komunikácie.

### 2.2.1 Peer-to-Peer (P2P)

Sieť typu peer-to-peer (P2P) sa vyznačuje tým, že ich uzly môžu mať rolu klienta i serveru. Najväčšou výhodou tejto siete je možnosť rýchleho zdieľania distribuovaných prostriedkov a nie je nutná zbytočná duplikácia zdrojov, čím sú celkové náklady nižšie. Pre hybridné P2P siete sú k dispozícií i centrálne služby a klienti sú tiež v rovnocennými partnermi. Sú rozšírené vo forme distribuovaných internetových aplikácií. Štruktúrované siete tvoria spojenie medzi dvoma uzlami, pričom oba uzly vedia o vzájomnej existencií skôr, než začnú vzájomné spojenie. Ako príklad, toto spojenie využívajú populárne aplikácie ako BitTorrent alebo Napster. [6] Takáto aplikácia umožňuje svojimi centrálnymi službami efektívne vyhľadanie v databázach s miliónmi užívateľov. Klient pre zdieľanie svojich dát vytvorí súbor s príponou .TORRENT, ktorý obsahuje informácie o zdieľaní súboru a serveru, s úlohou zachovať metadáta a ukazovať na súbor. Súbor .TORRENT sa prenesie na Torrent server, odkiaľ si ho iný klient, pátrací po konkrétnych dátach, prevezme. Po prečítaní súboru nový klient zahajuje prenos s prvým klientom – rozsievačom (seeder), a všetci uvedení klienti následne poskytujú kompletnú kópiu súboru ako noví rozsievači. Torrentová služba je v súčasnej dobe chápaná ako nelegálna. To je však omyl, pretože umožňuje rýchlu a efektívnu distribúciu súborov medzi viacerých užívateľov, klientov. Nelegálnym podtextom tejto služby je zdieľaný obsah, ktorý spadá pod ochranu autorských práv, prípadne zdieľanie iného nelegálneho obsahu. [6]

### 2.2.2 Miestna sieť (LAN)

Za miestnu sieť sa považuje sieť v určitej lokálnej oblasti. Ide o lokálne systémy, ktoré majú svojich administrátorov starajúcich sa o sieť. Miestne siete možno využiť súkromným účelom domácností alebo pracovným prostrediam spoločností. Ako bolo spomenuté, pre LAN súkromné siete požívajú IP adresy v rozhraní 10.0.0.0/8 alebo 192.168.0.0/16. Z veľkého čísla prefixu môžeme usúdiť, že pre spoločnosti môže ísť o dostatočný počet možností zapojenia koncových zariadení. Tieto siete k tomu využívajú jednotlivé sieťové prvky, ktoré presmerujú tok dát do cieľovej destinácie. [8]

### 2.2.3 Rozsiahla sieť (WAN)

Sieť WAN je rozsiahlou sieťou, ktorá spája viaceré menšie siete a spája ich pre umožnenie komunikácie. Najznámejšou WAN sieťou je svetová sieť Internet, ktorá je prepojením viacerých WAN sietí po celom svete. Niektoré WAN siete sú súkromné a vybudované pre jednotlivé spoločnosti. Iné WAN siete spájajú určitú väčšiu oblasť ako sú prevádzkovatelia Internetových služieb a prepájajú LAN siete s Internetom. K ich adresovaniu dopomáha hlavne protokol IP, ktorý bol už zmienený a vysvetlený. Každý pripojený server, web, LAN sieť atď., k WAN sieti získa unikátnu verejnú IP adresu, s ktorou môže nadviazať spojenie. [8]

### 2.2.4 Virtuálna privátna sieť (VPN)

Virtuálnu privátnu sieť predstavuje šifrovaný tunel medzi klientom a serverom. Šifrovanie prebieha na koncovým zariadením klienta a zostáva zašifrované po dobu prenosu sieťou až na určený server, ktorý umožňuje dešifrovanie spojenia. Užívateľ VPN služby takto pri kontaktovaní novej siete vystupuje ako užívateľ servera s jeho IP adresou a celá komunikácia klientskeho zariadenia je prenášaná cez šifrovaný tunel do serveru. [6]

### 2.2.5 Sieť Tor

Tor – The Onion Routing – cibuľové smerovanie, využíva takzvané smerovacie vrstvy ako pri cibuli, kedy sa využívajú „vrstvové smerovače“ pre dátový prechod cez sieťové servery Tor siete. Správy cez túto sieť sú mnohonásobne šifrované, pre každú medzistanicu (vrstvu) unikátne šifrovanie, aby správy boli bezpečne prenesené. Dnes tento opensource projekt používa tisíce rôznych severov, ktoré sa využívajú na presmerovanie toku dát. Táto sieť zaisťuje iba účely presmerovania, ktoré sú náhodné medzi Tor servermi. Vstup do

siete je na báze tradičného spojenia, kedy sa nadviaže spojenie s adresárovým serverom Tor a umožní sa prepojenie na jeden zo vstupných serverov siete, následná komunikácia medzi servermi však prebieha v tvare P2P, konkrétne F2F – friend-to-friend spojeniu, [6] a výstupná IP adresa patrí poslednému konečnému serveru, cez ktorý prebieha komunikácia v Tor sieti. Cieľový koncový bod zaznamená tak požiadavku komunikácie práve z tohto serveru. Táto komunikácia robí užívateľov anonymných a častokrát sa využíva aj pri útokoch. Obrana proti útokom z Tor siete môže byť v podobe IDS/IPS systémov a firewallu, ktoré by blokovali zaznamenanú komunikáciu vychádzajú zo serverov podozrivých zo spoluúčasti na Tor siete.

## 2.3 Logy

Pre trasovanie komunikácie je nutné najskôr vedieť čo sa trasuje a ktorým smerom sa vybrať. Tieto informácie nám ponúka záznam logov. Súbor log nám zaznamenáva udalosti, ktoré sa dejú v operačnom systéme, softwari, správach medzi rôznymi užívateľmi cez komunikačné programy, atď. Logovanie je sloveso označujúce činnosť zaznamenávania logov a zachovávania pre neskoršie účely do súborov s koncovkou „ .log “. Logy nám umožňujú zaznamenávať bezpečnostné výstrahy, chyby (error log), prístupy (access log) a iné. [13] Každý záznam v .log je koncipovaný s vlastnosťami, ktoré zodpovedajú základné otázky o udalosti:

- „Kedy?“ – zaznamenáva sa dátum, čas a časová zóna podľa ktorej čas beží, prípadne i deň k danému dátumu.
- „Kde?“ – záznam IP adresy, miesta úložiska, programu a pod.
- „Čo?“ – informácia o udalosti.
- „Kto?“ – prístupový údaj, ID užívateľa, IP adresa prípadne MAC adresa.

Všetky tieto údaje sú evidované podľa relevantnosti konkrétnej udalosti, ktorú zaznamenávajú. Treba uvážiť, že čistá evidencia logov je iný koncept monitoringu bezpečnostných aktivít, na rozdiel od ich aktívneho spracovávania v prostredí spoločnosti. Evidencia logov je užitočná v prípade užitia v nadväzujúcich forenzných vyšetrovaniach. Pokiaľ však zaznamenávanie logov nemá procedúry, ktoré ich aktívne prezerajú a analyzujú, ich úžitok je v ustavičnom chode bezpečnostného manažmentu zanedbateľný. Pre ich plné využitie je pre spoločnosti rozumné, aby zabezpečili ich monitoring a analýzu. Tá by mala vyhodnotiť udalosti čo najrýchlejšie, ako to je len možné za účelom získania výsledkov, detekovať

prípadný útok a stanoviť okamžité bezpečnostné opatrenia. Keďže útočníci (a ich útoky) sú čím ďalej sofistikovanejší a vzdelanejší, takáto nadstavba pre záznam logov je čím ďalej užitočnejšie až nevyhnutná. [16]

Najväčšou výzvou dnešných spoločností je enormný nárast počtu logov na systém a zároveň, pri ich predpokladanom rozrastaní sa, sa bude viac násobne zvyšovať. Hoci sa zdá, že nárast hardwarových prvkov v rámci organizácií je limitovaný, ich kapacita môže byť využitá s rozšírením virtualizačných nástrojov.

### 2.3.1 Odporúčanie pre záznam logov

Český Národní úřad pro kybernetickou a informační bezpečnost vydal v roku 2016 odporúčanie na minimálne požiadavky pre záznam logov, ktoré musia byť zaistené pre spoľahlivú ex-post analýzu kybernetických bezpečnostných incidentov. [14] Toto odporúčanie vychádza z dokumentu NIST800-92 [15].

Pre ex-post analýzu kyberneticko-bezpečnostného incidentu je nutné disponovať záznamami prevádzky z doby jeho výskytu. Zariadení, ktoré záznamy generujú je veľké množstvo, ide o bezpečnostné nástroje (antivirus, IDS/IPS, proxy, smerovač, prepínač, firewall, atď.), operačné systémy (autentizácia, privilegované spúšťanie, systémové udalosti, atď.) a aplikácie (komunikácie medzi klientmi a servermi, užívateľské udalosti, prístupy, atď.). Preto je pre nasadenie log manažmentu kľúčové:

- správne nastavenie časovej značky na všetkých zdrojoch – synchronizácia času v rámci aj časovej zóny a jeho jednotný formát.
- zaistenie dostatočnej kapacity pre logovanie, pravidelné odosielanie logov do centrálneho log manažmentu a ich uchovávanie po určenú dobu.
- pravidelná analýza logov v log manažmente, najlepšie automatizované upozorňovanie na výskyt abnormalít.
- zaistenie bezpečnosti a integrity logovacích záznamov (ochrana pred zneužitím, zmenením alebo vymazaním) naprieč celým log manažment systémom (adekvátne podľa možnej závažnosti zneužitia).
- dostupnosť logov v prípade poruchy systému (zabezpečiť zálohovanie).

Odporúčanie ďalej zmieňuje kategorizáciu logov do rôznych skupín podľa možnej závažnosti a to skupina bezpečnostná (SEC), systémová (OS) a aplikačná (APP).

Skupina bezpečnostná zahrňuje logy z bezpečnostných softwarov a nástrojov ako sú antivírusové/antimalware programy, IPS a IDS systémy, VPN, web proxy, software manažmentu zraniteľnosti, firewally a routery, autentizačné servery a pod.

Skupina systémová (OS) zahrňuje servery, pracovné stanice a sieťové prvky (prepínače a smerovače). Ide predovšetkým o dva typy logov, a to systémové udalosti (spustenie/zastavenie služby, vypnutie a zapnutie systému, porucha služieb, závažné chyby a pod.) a udalosti auditu (pokusy o úspešné a neúspešné prihlásenie, prístupy k súborom, zmeny nastavenia, využitie oprávnenia a pod.)

Aplikačná skupina logov sleduje chod aplikácií. Ide najmä o logy:

- komunikačné (C<>S ... Klient – Server) – klientské požiadavky prijaté serverom a ich odpovede;
- využívanie účtu (ACC = Account info.) – Informácie o prihlásení k aplikácií/službe (i neúspešné pokusy), zmeny v účtoch, zmeny oprávnení a pod.;
- údaje o aktivite užívateľov (Aktivita) – napríklad počty transakcií a ich objem;
- významné prevádzkové akcie (Akce) ako spustenie alebo ukončenie aplikácie, pád aplikácie alebo jeho významné zmeny.

Pre každú skupinu logov je stanovený koeficient času dĺžky (počet dní) ich záznamu. Pre všetky kategórie bezpečnostných logov (SEC) sa odporúča 30 dní, rovnako i pri systémových (OS) logoch, je to 30 dní. U aplikačných je to u komunikácií C<>S a ACC doba 7 dní, u aktivít užívateľov (Aktivita) po dobu 1 dňa a pri prevádzkových akciách (Akce) doba 30 dní. Podľa zákona o kybernetickej bezpečnosti je však stanovené, že pri objektoch významného informačného systému musí požadovaná doba úschovy dát až trojnásobná (do čoho spadajú aj napríklad poskytovatelia internetových služieb) a pri systémoch kritickej informačnej infraštruktúry až šesťnásobná. [14]

## 2.4 Podmienky pre trasovanie

Podmienky pre možné trasovanie vybranej komunikácie sú nastolené na základe komplexnej zhody viacerých zmienených systémov: o akú komunikáciu ide, na akom type siete prebehla, aké služby boli použité, aký hardware administrátori sietí používajú, aké manažment-softwary sa využívajú, a v neposlednom rade i akú detekciu komunikácie (Log manažment, IDS/IPS systémy), ich záznam a možnosti spätnej ex-post analýzy.

# 3 METODIKA PRE TRASOVANIE KOMUNIKÁCIE S FORENZNÝMI NÁSTROJMI

Metodika pre trasovanie komunikácie je využiteľná pri ex-post štádiu incidentu. Ako bolo zmienené, jej nasadenie úzko súvisí s podmienkami a informáciami, ktoré sú dostupné z vyhodnotenia incidentu. Trasovanie tým pádom začína už od samotnej detekcie incidentu, kedy sa dozvedáme prvé stopy, ktoré nás môžu viesť k potenciálnemu páchateľovi útoku, alebo všeobecne povedané, tvorcu komunikačného spojenia so sledovaným systémom.

## 3.1 Detekcia incidentu a komunikácie

Ako prvým bodom postupu pri metodike je detekcia incidentu a komunikácie, ktorá ho zapríčinila. Táto detekcia môže byť vytvorená pasívne – administrátor si všimol pri prechádzaní .log súboru, že je konkrétna komunikácia nebezpečná; alebo aktívne – vďaka upozorneniu z monitoringu a analýzy prevádzky siete.

Cieľom je zistiť, odkiaľ prebiehala komunikácia, ktorá zapríčinila daný incident, čiže sa sledujú záznamy, ktoré korelujú s časom možného uskutočnenia incidentu. V týchto záznamoch sa následne hľadá, čo sa udialo a odkiaľ bol daný príkaz poslaný/prijatý.

### 3.1.1 Pasívna detekcia incidentu

Pri zistení nefunkčnosti systému sa systém diagnostikuje. Môže sa stať, že systém bol pod neoprávneným vplyvom a to zapríčinilo jeho chybu. Keď sa zistí, že ide o bezpečnostný incident až po odhalení poruchy systému, hovoríme o pasívnej detekcií. Následne sa hľadá príčina a vyšetrovanie sa zameriava na zaznamenané súbory logov. Zaznamenávanie logov môže prebiehať v rôznych softwaroch na rôznych sieťových zariadeniach. Bežný log, napríklad služby Apache sa zobrazuje nasledovne:

- 195.178.92.54 - - [04/May/2018:13:49:07 +0200] "GET /mail/ HTTP/1.1" 200 3232

Z uvedeného vieme vyčítať nadviazanie spojenia z IP adresy 195.178.92.54 na náš server, v čase 13:49:07 v časovom pásme GTM +2 s dátumom 4.5.2018 a aplikačné informácie, čo sa udialo. Ak vieme priradiť tomuto logu daný pokus o ohrozenie, vieme následne zahájiť ďalšie operatívne postupy pre trasovanie zdroja útoku prostredníctvom IP adresy.

### 3.1.2 Aktívna detekcia incidentu

Pri použití detekčného systému, ktorý aktívne monitoruje a zaznamenáva komunikáciu na sieti, vieme byť s krátkym časovým oneskorením oboznámení o danej udalosti. To sa dá docieliť pomocou IDS systému. IDS systémy sú dnes vo firmách časté, až samozrejmé. V praxi sa používajú aj nadstavbové systémy ako napríklad DLP (Data Lost Protection – ochrana straty dát), ktoré sú pre svoj charakter aj patrične spoplatnené. Pre jednoduché informačné systémy sú však k dispozícií aj niektoré OpecSource IDS programy, ktoré sú dostupné zdarma, ako napríklad Snort alebo PSAD.

**Snort**

Snort je IDS/IPS systém ponúknutý od firmy Cisco. Je schopný real-time monitoringu a analýzy prevádzky a logovaniu toku paketov siete. Môže analyzovať protokoly, hľadať zhody v kontextoch, detekovať viaceré útoky alebo kryté skenovanie portov, pokus o SMB útok, preťaženie vyrovnávacej pamäte (buffer overflow), a ďalšie. Snort môže byť použitý ako sniffer (odpočúvanie) paketov komunikácií siete [22]. Snort sa najčastejšie používa na serveroch, ktoré využívajú operačný systém Linux. Je však dostupný a plne funkčný aj pre OS Windows. Jediný rozdiel pri konfigurácií je v zmene prepísania funkcií kódu pre daný operačný systém. Pre sniffovanie, v termináli operačného systému sa zadá jednoduchá funkcia:

- *snort -vde*

Kde snort je funkcia pre začiatok programu, pomlčkou vyvoláva konkrétnu funkciu, „v“ pre zobrazovanie záhlavie TCP/IP paketov, „d“ pridanie UDP a ICMP záhlaví, „e“ pre zobrazenie ďalšej vrstvy záhlavia.

Pre logovanie paketov sa pridáva za vyvolávaním funkcie „-l“ pre logging a destinácia kam sa má súbor logu zaznamenať na disk.

- *Snort -vde -l <destination>*

Logy sú však pri sniffovaní v binárnom formáte tcpdump. Dajú sa však prezerať prostredníctvom aplikácie, ktorá dokáže čítať tento formát, ako napríklad Wireshark. Preto sa odporúča doplniť Snort s logovacou aplikáciou, ako je napríklad Syslog. [22]

Pre použitie Snortu ako IDS systému, je potreba ho nakonfigurovať. K tomu slúži konfiguračný súbor *snort.conf* , ktorý používa preddefinované vlastnosti, ktoré IDS systém bude skúmať. Predprogramované konfiguračné súbory sú dostupné i zo stránok snort.org.

K tomuto súboru je vhodné preddefinovať/stiahnuť pridané súbory preprocesorov a pravidiel, na ktorý sa konfiguráčný súbor *snort.conf* odvoláva pri vyvolávaní funkcií. Konfiguračný súbor obsahuje niekoľko základných krokov. Ako prvý, sleduje konfiguráciu adries sietí, ktoré chceme chrániť, siete ktoré považujeme za externé (častokrát negácia chránenej siete pomocou !<chránená sieť>), a zoznam jednotlivých serverov siete (DNS, SMTP, web, atď.). Taktiež sa dajú nastaviť i zoznamy sledovaných portov. V druhom kroku nastavujeme konfiguráciu dekodéru a iných funkcí, ako i nastavenie automatického vytvárania logovacích súborov *config logdir: <destination>*. Tretí krok je konfigurácia základných detekčných mechanizmov. Pri kroku štyri sa konfigurujú dynamické načítavania knižníc (lib). Piaty krok, konfigurácia preprocesorov, ktoré sledujú napríklad fragmentáciu paketov, sledovanie protokolov, skenovanie portov, konfiguráciu blacklistu a whitelistu. Šiesty krok je dôležitý pre využívanie pridaných výstupných programov, ako je napríklad už spomínaný Syslog. Siedmy krok konfiguruje, ktoré súbory pravidiel sa načítajú do programu Snort počas jeho vyskúšania. Krok osem a deväť sú užívateľským nastavením preprocesorov a pravidiel.

Po správnej konfigurácií systému môže IDS plne fungovať a sledovať nakonfigurovanú sieť, prípadne časť siete. Vďaka programovateľnosti určitých pravidiel môže byť nastavené, pri akej detekcii signatúry sa na panele logu zachytí upozornenie o nebezpečnej udalosti. To môžeme nastaviť v priečinku pravidiel, napríklad *local.rules* , kde sa dá efektívne prispôsobiť, ako sa bude upozornenie zobrazovať pre konkrétne udalosti. Príklad:

- Alert TCP any any -> 192.168.0.0/16 any (msg: “Port Scan Alert!”; sid:100001; flags:FPU; class-type:network-scan;)

Kde funkciou „Alert“ vyvoláme poplach, keď akákoľvek adresa s akýmkoľvek vychádzajúcim portom „any any“ chce naviazať komunikáciu so sledovanou adresou na akomkoľvek porte „x.x.x.x/y any“, zobrazí sa nadefinovaná správa a identifikačné číslo udalosti. To, že ide o skenovanie portov, vieme nastaviť pomocou príkazu „flags:FPU“, kedy sa sledujú špecifické príznaky (flags) paketu, konkrétne FPU – FIN, PSH a URG, ktoré nie sú v komunikácií časté.

Skladaním rôznych podobných konfigurácií udalostí môže byť nadefinovaný podrobný IDS systém, ktorý analyzuje, detekuje a zobrazí, o aký konkrétny útok na sieť sa jedná v reálnom čase.

Nakoniec sa celý proces IDS systému a s evidenciou v Syslogu spustí nasledovne:

- *snort -i X -c <destination> -s*

kde funkcia „-i X“ spustí systém cez sieťovú kartu X (číslo sieťovej karty zistíme príkazom s funkciou –W), „-c <destination>“ načítanie konfiguračného súboru s cestou k nemu; a „-s“ pre výstup do programu Syslog. [17] Pri použití programu Syslog je potreba zabezpečiť iný spôsob zaznamenávania MAC adresy počítača k IP adresám, pretože Syslog nie je naprogramovaný pre spracovanie a zobrazovanie tohto údaju.

**PSAD**

Port Scan Attack Detection – PSAD nástroj je IDS software, ktorý detekuje a analyzuje záznamy logov (IPtables) z Linuxových platforiem, aby hlásil pokus o skenovanie portov a iných podozrivých tokov dát na sledovanú sieť. PSAD používa pre svoj chod princípy prevzaté z knižníc signatúr spomínaného Snort IDS systému, konkrétne z balíčkov Snort pravidiel (Snort rule set). Výsledkom, podobne ako u Snort, je detekcia pokusov o rôzne útoky ako backdoor programov, DDoS nástrojov alebo pokročilých skenov portov.

V rámci operačného systému Debian, je možná veľmi rýchla inštaláca PSAD nástroja priamo zo zdrojového kódu alebo zo stránok debian.org. K tomu je potreba iba spravovať operačný systém s aktualizáciami (pomocou *apt-get update* ) a následne stačí inštalovať pomocou *apt-get install psad* v termináli operačného systému. Na distribúcií Debianu je možné priamo nájsť konfiguračné súbory a pravidlá pre jeho chod.

Po začatí používania je potreba umožniť logovanie vstupných a výstupných reťazcov IPtables, aby PSAD dokázal detekovať abnormálne aktivity:

- *iptables –A INPUT –j LOG*
- *iptables –A FORWARD –j LOG*

PSAD sa následne spustí jednoduchým príkazom „ *start* “ a pre zobrazenie detailných výstupov „ *-s* “

- *psad start*
- *psad –s*

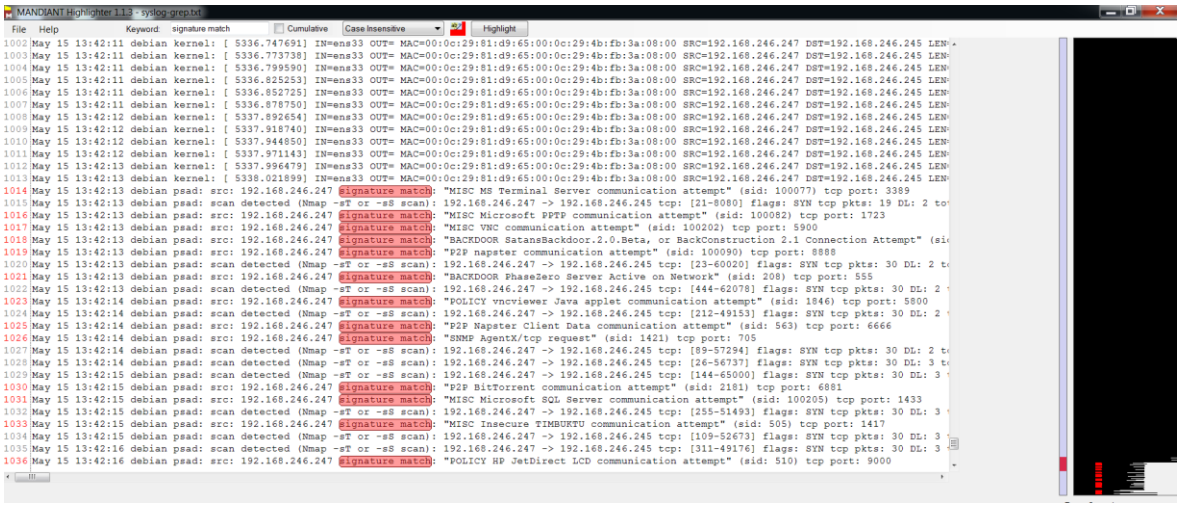
Detail výstupu nám zobrazuje Top 50 zhôd signatúr, IP adresy Top útočníkov s počtom zhôd signatúr, najčastejšie skenované porty a informácie k jednotlivým IP adresám, u ktorých môžeme vidieť aj aké signatúry útokov boli zaznamenané.

Následne môžeme v zázname programových správ syslog nájsť výsledky detekcie s informáciami z PSAD o čase, dátume, čo bolo detekované, aká zhoda signatúry, IP adresu zdroju a IP adresu destinácie nadviazanej komunikácie(útoku), príznak (flags) paketu a port. Pri zachytení niektorých typov komunikácií môže byť zaznamenaná aj MAC adresa zariadenia zdroja a aj destinácie. Ukážka výstupu zo syslog je zobrazená na obrázku 3.

## 3.2 Spracovanie log záznamu a vyhodnotenie detekcie útokov

Po úspešnom zachytení útoku, či podozrivej komunikácie je potreba záznamy logov vhodne spracovať a vyhodnotiť útok pre zavedenie ďalších krokov. Log súbory sú obyčajne v klasickom .txt formáte. Je však vhodné, aby sa používali iné programy pracujúce s textovými súbormi, ktoré „nerozosypú“ text, prípadne rešpektujú riadkovanie, medzery a pod. Ako najzákladnejším doplnkom pre prezeranie textových súborov môže byť Notepad++, ktorý elegantne zachováva štruktúru textového súboru a dokonca i počíta riadky súboru.

Pre lepšiu a efektívnejšiu prácu s logmi, je však k dispozícii zdarma MANDIANT Highlighter. Tento program nielen zachováva štruktúru súboru a počíta riadky, ale i využíva efektívne vyznačovacie prvky pre rýchle hľadanie zhôd výrazu (napríklad konkrétna IP adresa, MAC adresa alebo detekcia signatúr).




Obrázok 3. MANDIANT Highlighter pri vyhľadávaní zhôd „signature match“ v textu syslog – evidencií záznamu programových správ. [Zdroj: autor]

Pri záznamoch o detekcií je pre nás najdôležitejšie zistiť páchateľa. K tomu sa postupuje tým, že sa bude trasovať zdroj útoku. Pre možnosti trasovania sú preto najdôležitejšie informácie, „Čo?“ – stanovenie, ktorý záznam je spojený s útokom, „Kedy?“ – čas a dátum

záznamu s GMT zónou a „Odkiaľ?“ – zdroj komunikácie: IP adresa, prípadne MAC adresa. Následne sa určí, či sa identifikovala LAN sieť, alebo je potrebné trasovať zdroj komunikácie z externej siete cez WAN – Internet.

## 3.3 Trasovanie komunikácie cez WAN sieť

Keď podozrivý záznam z logu ukazuje IP adresu mimo lokálnej siete, znamená že práve daná IP adresa pochádza z WAN siete. Ako už bolo zmienené, Internet sa skladá z viacerých WAN sietí. Každý internetový prevádzkovateľ, server, doména atď., má pridelenú svoju verejnú IP adresu. Lokálny koncový bod – počítač – má v lokálnej sieti lokálnu IP adresu. Pri prechode paketov do WAN siete, pakety preposlané smerovačom do WAN siete nadobudnú zdrojovú adresu poskytovateľa internetovej služby (domény, serveru, atď.). Pre zistenie podrobnejších informácií o podozrivej IP adrese je možné použiť množstvo nástrojov, ktoré využívajú podobný princíp – zber dát z databáz systému WHOIS Regionálnych Internetových Registrov (RIR – Regional Internet registry), ktoré boli spomenuté v prvej kapitole. Väčšina nástrojov však využíva iba časť informácií o danej IP adrese s pomocou pridaných aplikácií, ako napríklad mapu, do ktorej sa vloží lokácia registrovanej spoločnosti, ktorá si vyhradila danú IP adresu.

### 3.3.1 WHOIS

WHOIS protokol je v súčasnosti štandardom pre dopyt informácií o doménach. Existuje veľa rôznych stránok, ktoré poskytujú túto službu, rovnako ako i programy, vďaka ktorým je možné tieto informácie získať od online serverov za pomoci terminálového príkazového riadka CMD. Najbežnejším spôsobom použitia WHOIS klienta je prostredníctvom webového nástroja, ktorý ponúkajú spoločnosti pre poskytovanie hostingu a registrácie domén. Jeden z týchto webov pre Českú republiku je Whois.SmartWeb.cz [20], kde doména SmartWeb spadá pod spoločnosť E4YOU, poskytovateľom zmienených služieb.

Pri zadaní podozrivej IP adresy do vyhľadávača WHOIS sa zobrazia nasledovné informácie (pre príklad použitá náhodná adresa evidovaná pod Univerzitu Tomáše Bati ve Zlíně):

```
IP Address: 195.178.88.60
Netblock: 195/8
Status: ALLOCATED
Detail: RIPE NCC

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
```

```
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '195.178.88.0 - 195.178.95.255'

% Abuse contact for '195.178.88.0 - 195.178.95.255' is 'abuse@utb.cz'

inetnum:        195.178.88.0 - 195.178.95.255
netname:        UTB-T34CZ
descr:          Tomas Bata University
descr:          Zlin
country:        CZ
org:            ORG-TBUi1-RIPE
admin-c:        TBUI1-RIPE
tech-c:         TBUI1-RIPE
status:         ASSIGNED PA
mnt-by:         TENCZ-MNT
remarks:        Please report network abuse -> abuse@utb.cz
created:        1970-01-01T00:00:00Z
last-modified:  2013-10-11T11:51:58Z
source:         RIPE

% Information related to '195.178.64.0/19AS2852'

route:          195.178.64.0/19
descr:          CESNET-T34CZ
origin:         AS2852 - výsledek Whois dotazu">AS2852
mnt-by:         AS2852-MNT
remarks:        Please report abuse -> abuse@cesnet.cz
created:        1970-01-01T00:00:00Z
last-modified:  2006-06-26T14:36:38Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.91.2
(HEREFORD)
```

Informácie nám zobrazujú, že daná IP adresa spadá pod RIR registrátora RIPE NCC, ktorý spravuje IP adresy pre Európu, Rusko a blízky východ a informácie sú zobrazené z RIPE databáz. Taktiež informuje o presnej veľkosti siete, pod ktorú dané informácie spadajú, konkrétne '195.178.88.0 - 195.178.95.255'.Následne sú uvedené informácie pre danú sieť: Názov siete ( UTB-T34CZ ), popis (Tomas Bata University , Zlin), krajinu (CZ), indentifikátory pre organizáciu a administrátora (ORG-TBUi1-RIPE a TBUI1-RIPE), status adresy (zapísaná), kto udržiava danú službu (mnt-by: TENCZ-MNT – po vyhľadaní môžeme zistiť že ide o spoločnosť Cesnet) a najdôležitejším pre nás je kontaktný údaj pre prípad sieťového zneužitia (abuse@utb.cz). Pri vyhľadaní podozrivej IP adresy je dôležité práve získať kontakt na správcu siete.

Pri kontaktovaní správcu siete treba uviesť dôvod písania, ktorým je kybernetický útok zo spravovanej siete, čas útoku spolu s GMT zónou, IP adresa zdroja útoku a IP adresa na ktorý útok bol mierený. Administrátor danej domény následne skontroluje logy pripojenia a komunikácie (ktoré sa zaznamenávajú a spravujú po určitý čas pre danú inštitúciu podľa [15]) v danom čase s GMT zónou, mieriace na konečnú IP adresu a zistí konkrétnu IP adresu z ktorej daná komunikácia pokračovala. V prípade, že ide o policajné vyšetrovanie, pre sprístupnenie informácií sa vydáva súdny príkaz.

Administrátor danej siete následne zistí, či:

- daná komunikácia iba prešla daným serverom, a bola pôvodne vyslaná z inej WAN siete (použitá VPN, prípadne iný typ smerovacích šupiek, zmienených v 2.2.5) – v takomto prípade sa celý proces dopytovania informácií opakuje s novou IP adresou, hľadaním WHOIS a kontaktovaním nového správcu;
- daný útok bol prevedený z lokálnej adresy správcu siete.

Nevýhodou tejto metódy je možné nezabezpečenie logov u správcu podozrivej IP adresy v zahraničnej krajine, kde požiadavky na záznam a ukladanie logov nemusí byť dostatočne dlhý, prípadne žiadny.

### 3.3.2 AbuseIPDP

Webový nástroj AbuseIPDP zaznamenáva do svojej databázy IP adresy a záznamy hrozieb, ktoré boli vytvorené danými IP adresami. Na základe tohto nástroja je možné zhodnotiť, či daná IP adresa je riziková pri komunikácií. Hodnotia sa pritom hlásenia, ktoré jednotliví administrátori serverov zašlú do tejto databázy. Výsledným ukazovateľom je uvedenie k danej IP adrese percento nedôveryhodnosti, ktoré poukazuje na pravdepodobnosť zneužitia. Pri vyhľadanej IP adrese je viditeľný i zoznam zaslaných hlásení s komentármi, o aký pokus o nebezpečnej činnosti išlo a o akú kategóriu. Taktiež ako WHOIS, i tento nástroj zobrazí niektoré základné informácie o adrese, akými je internetový poskytovateľ, krajina a mesto, v ktorom server sídli. [21]

## 3.4 Trasovanie komunikácie na LAN sieti

Pokiaľ trasovanie komunikácie doviedlo stopu na miestnu sieť, hlavnou úlohou je identifikovať zariadenie, ktoré komunikáciu nadviazalo a iniciovalo útok, a následne identifikovať páchateľa, ktorý zariadenie obsluhoval.

Po získaní logu času a IP adresy zariadenia v miestnej sieti, je možné trasovať zariadenie viacerými cestami na základe nástrojov, ktorými daná miestna sieť operuje. Je to buď na základe IDS/IPS systému alebo vďaka softwarovým doplnkom sieťových prvkov, ktoré miestna sieť využíva. Výsledok však musí byť jednoznačný – identifikácia zariadenia. Zariadenie sa identifikuje pomocou unikátnej MAC adresy sieťovej karty, ktorá sa pripojila na sieť v danom čase. Keďže IP adresy sa menia pre zariadenia vďaka DHCP protokolu pre prideľovanie IP adries, je dôležité zaznamenať spojenie IP adries a MAC adries v rovnakom čase. Väčšina kvalitnejších sieťových zariadení umožňuje pomocou webového rozhrania pripojenie a manažovanie zariadenia, ktoré zaznamenáva tieto informácie. V spoločnostiach, ktoré majú vlastnú informačnú infraštruktúru, zvyknú pre svoju internú sieť povoliť prístup do siete iba zariadeniam, ktoré registrujú svoju MAC adresu do smerovača (router) alebo servera. Prepínače (switch) túto funkciu obyčajne nemajú, špeciálne ak sa jedná o lacnejšie verzie. Kvalitné prepínače môžu obsahovať aj konfigurovateľné rozhranie, ktoré udáva MAC adresu a port/zásuvku, na ktorom je zariadenie pripojené. Každý správca siete by mal mať kontrolu nad svojou sieťou, správou zariadení a ich pripojení do siete. Preto keď sa zistí IP adresa lokálnej siete, hľadanie zariadenia už nie je veľkou prekážkou.

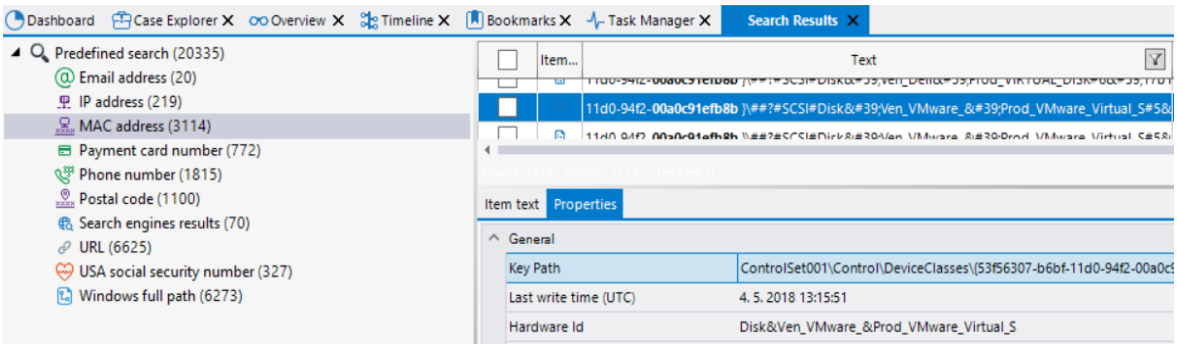
## 3.5 Analýza identifikovaného zariadenia

Pre identifikáciu páchateľa môže byť potrebná aj dodatočná analýza zariadenia, ktoré podozrivý používal. Po identifikácií tohto zariadenia je možné použiť radu forenzných nástrojov, ktoré skúmajú priamo zariadenie, prácu s ním a jeho aktivitu. K tomuto účelu patria napríklad aj nástroje od firmy Belkasoft, konkrétne Belkasoft Acquisition Tool pre zachytávanie obsahu disku s tvorbou jeho obrazu (Image), následne Belkasoft Evidence Center pre spracovanie a prípravu dát z daného Image a Belkasoft Evidence Reader pre jeho čitateľnosť a následnú analýzu. Všetky nástroje musia byť v zhodnej verzií.

Image skúmaného disku je potrebné vytvoriť na pridaný disk tak, aby sa nepoškodili dáta daného skúmaného systému a tým nemanipulovalo s dôkazmi. Vytvorenému obrazu disku vypočítame Hash (MD5 a SHA1), pre jeho dodatočnú verifikáciu pri manipulovaní s ním – prenesením na analytické pracovisko so softwarovým nástrojom Belkasoft Evidence Center, ktorý zanalyzuje obraz disku a vytvorí nám výstup v podobe, ktorý je čitateľný s nástrojom Belkasoft Evidence Reader.

### 3.5.1 Belkasoft Evidence Reader

Prostredníctvom Evidence Reader sa hľadajú dôkazy pre identifikáciu zariadenia a identifikáciu páchateľa, ktoré by mohli dopomôcť k uzavretiu prípadu. Práca s ním je prehľadná, keďže dokáže efektívne spájať dáta podľa kategórie, času a významu. Vďaka tomu sa dá zhromažďovať dôkazy o aktivitách, ktoré boli vykonávané na disku: vytvorené dokumenty, práca s internetovým prehliadačom, rýchle správy v rámci použitia Messengerových softwarov (ICQ, Skype), Emaily, obrázky, ale aj systémové záznamy (Syslog), a vďaka hľadaniu formátu aj IP adresy a MAC adresy. Tieto dáta sa následne môžu filtrovať, prípadne k nim pridať komentáre a následne zaznamenať (bookmark).




Obrázok 4. Príklad vyhľadania MAC adresy v BS Evidence Reader. [Zdroj: autor]

Výhodou tohto programu je, že sa vytvorí spolu s výstupom analýzy daného obrazu disku. Tým je možné celú analýzu presúvať prostredníctvom prenosného disku a zobraziť kdekoľvek, kedykoľvek bude potrebné. Konečné dáta môžu byť aj exportované do .PDF, .HTML alebo iných formátov ako čitateľný výstup a dôkaz pre post-analytické procesy.

## 3.6 Zhrnutie metodiky

Na záver stručné bodové zhrnutie postupu metodiky:

- zabezpečenie evidencie logu komunikácie s časom, časovou zónou, adresou zdroju útoku a adresu cieľa útoku.
- ak išlo o útok z externej siete, zistenie administrátora danej zdrojovej WAN siete, dopyt po ďalších informáciách zdroja útoku.
- ak bola identifikovaná LAN sieť, evidovanie prepojenie IP adresy a MAC adresy zariadenia, identifikovanie zariadení.
- po identifikácií zariadenia sa identifikuje páchateľ. K tomu môžu byť použité aj forenzné analytické nástroje.

# II. PRAKTICKÁ ČÁST

# 4 MODELOVÁ SITUÁCIA Č. 1

Stanovená metodika bola otestovaná na modelových situáciách, ktoré sú predmetom praktickej časti. Prvá modelová situácia bola vytvorená pre prípad útoku v internej sieti LAN, kde páchateľ bol jej užívateľom. Cieľom bolo zachytenie útoku a vypátranie zariadenia, z ktorého daný útok bol uskutočnený.

## 4.1 Informácie o útoku

Pri prvej modelovej situácií boli použité ako detekčné zariadenia virtuálne operačné systémy prostredníctvom virtualizačného nástroja VMware Workstation 12. Použité operačné systémy boli Windows 7 a Debian 9.4 na báze Linuxu. Servery obyčajne využívajú viaceré virtualizačné operačné systémy, ktoré sa navzájom dopĺňajú a spolupracujú pri bezpečnostnej konfigurácií.

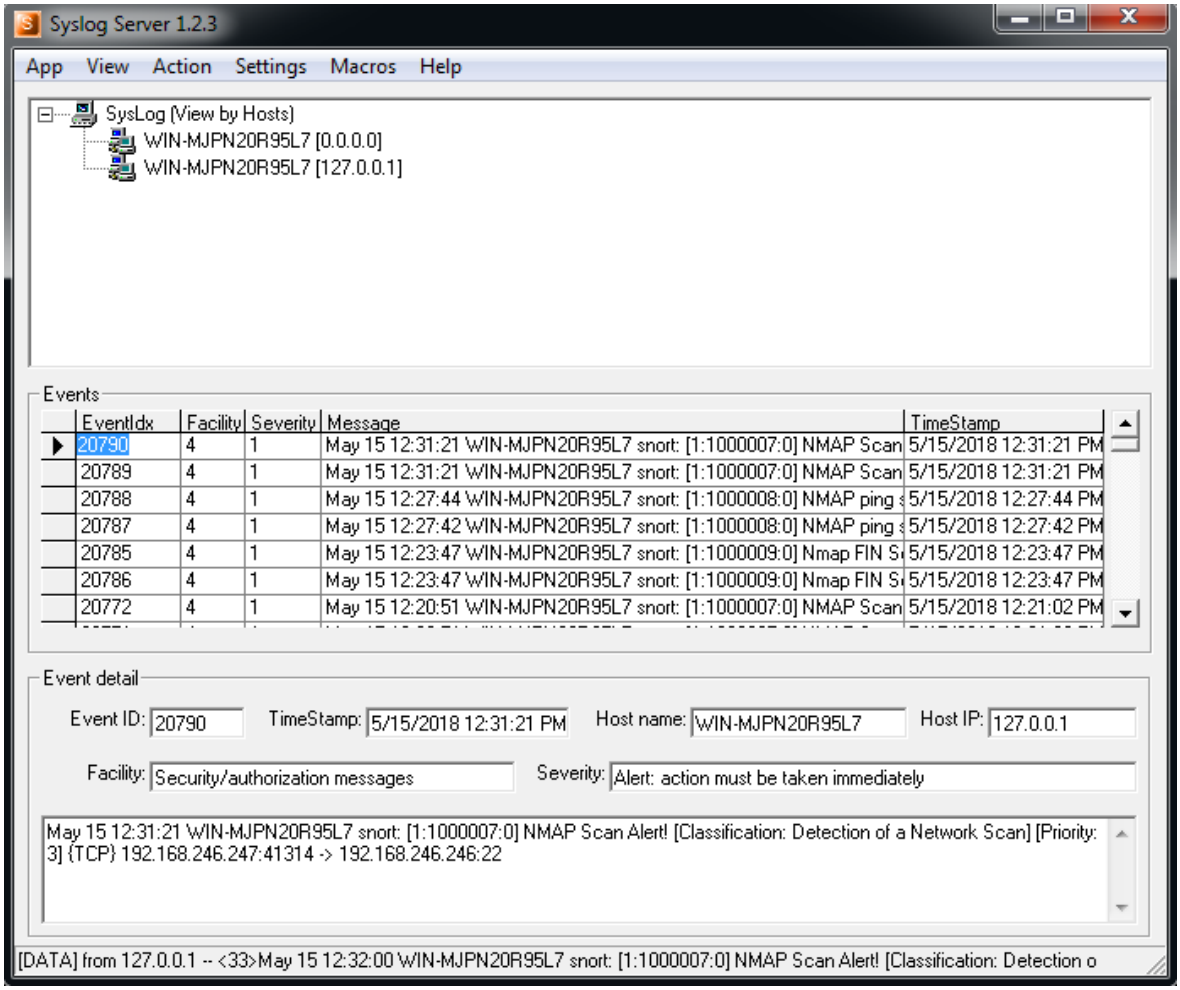
Oba virtuálne OS boli spustené na počítači LAN siete, s lokálnou IP adresou 192.168.246.22 s operačným systémom Windows 10.

VM (Virtual Machine – virtualizačný systém) Windows 7 mal priradenú IP adresu 192.168.246.246. Na tomto operačnom systéme bol sputený detekčný systém IDS Snort, ktorý bol nakonfigurovaný pre Windows systém tak, aby detekoval prípadný utok na túto jednotku. V rámci lokálnych pravidiel (local.rules) boli nastavené detekčné vlastnosti rôznych útokov skenovania portov.

```
18 #-------------
19 # LOCAL RULES
20 #-------------
21 #alert ICMP any any -> any any (msg:"Testing ICMP alert."; sid:1000001;)
22 #alert UDP any any -> any any (msg:"Testing UDP alert."; sid:1000002;)
23 #alert TCP any any -> any any (msg:"Testing TCP alert."; sid:1000003;)
24 alert TCP any any -> $HOME_NET any (msg:"NMAP Scan Alert!"; sid:1000004; flags:FPU; classtype:network-scan;)
25 alert TCP any any -> $HOME_NET any (msg:"Nmap NULL Scan Alert!"; sid:1000005; flags:0;)
26 alert TCP any any -> $HOME_NET any (msg:"Nmap FIN Scan Alert!"; sid:1000006; flags:F;)
27 alert ICMP any any -> $HOME_NET any (msg:"NMAP ping sweep Scan Alert!"; dsize:0; sid:1000007;)
28
```

Obrázok 5. Ukážka local.rules súboru s nastavením upozornení na útoky. [Zdroj: autor]

Zvolená detekčná oblasť siete bola *$HOME_NET* , pričom táto oblasť bola nakonfigurovaná v súbore snort.conf , kde zastupovala oblasť celej lokálnej siete 192.168.246.0/8 . Pri detekcií bol využívaný ako výstupný zobrazovací program software Syslog. Ten zobrazoval dáta z upozornení pri nakonfigurovanej detekcii útoku. Na obrázku 6. je možné pozorovať výsledné dáta zobrazované v programe Syslog.




Obrázok 6. Výstup detekcie útokov z programu Snort zobrazujúci software Syslog. [Zdroj: autor]

Software Syslog nám zobrazil niekoľko pokusov o skenovanie portov. Vyznačená udalosť s identifikačným číslom 20790 zobrazuje:

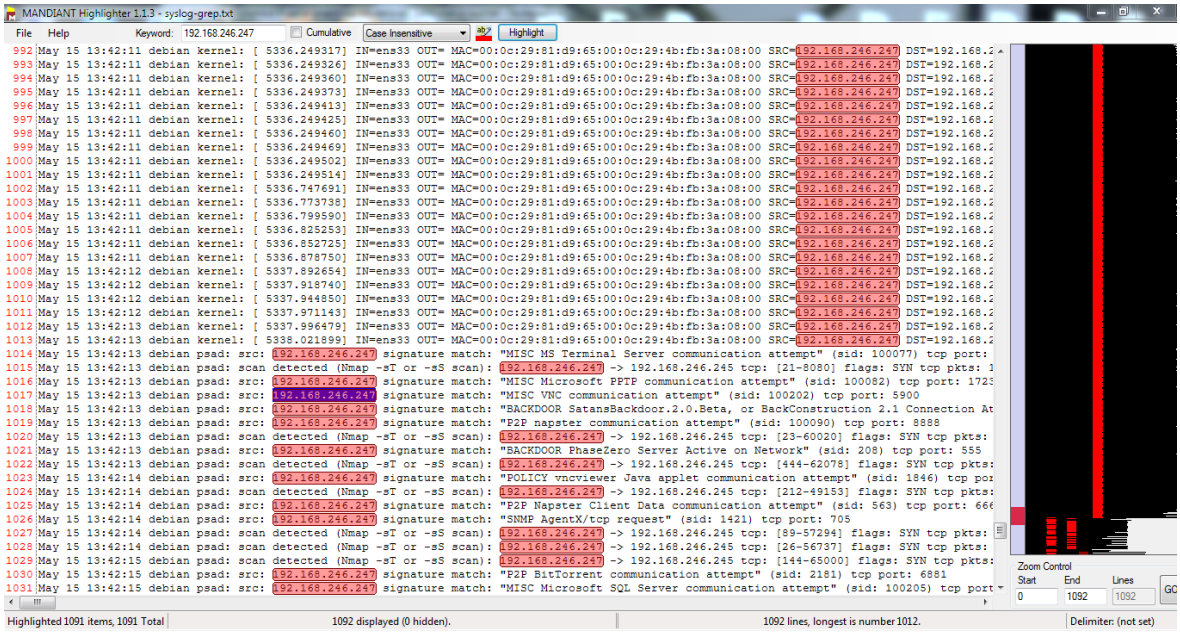
- čas hlásenia: 15.5.2018 12:31:21 PM (doplnkovo vieme, že čas je GMT +2);
- názov hostiteľského detekčného nástroja (na ktorom Snort je spustený);
- IP adresa nástroja – ide o IP adresu služby spustenej na lokálnom serveri (Snort s Syslog sú spustené na rovnakom systéme);
- sekcia upozornenia: Bezpečnostné; Vážnosť akcie – okamžitá;
- ID udalosti so správou: 1000007 NMAP Scan Alert!;
- kasifikácia útoku – Detekcia sieťového skenovania;
- aký protokol bol použitý: TCP;
- IP adresa zdroju útoku s portom: 192.168.246.247 : 41314;
- IP adresa cieľu útoku s portom: 192.168.246.246 : 22;

Z danej detekcie boli zaznamenané všetky potrebné informácie: čas útoku, jeho zdroj útoku i cieľ útoku. Taktiež sa zistilo, že skenovaný port bol číslo 22, ktorý sa používa ako prihlasovací protokol. Ten býva častokrát zneužiteľný rôznymi hackerskými útokmi ako napríklad trojský kôň. Rovnako bol použitý VM Debian 9.4 s priradenou IP adresu 192.168.246.245. Na tomto operačnom systéme bol spustený detekčný IDS systém PSAD. Počas priebehu detekcie boli rovnako zaznamenané viaceré pokusy útokov o skenovanie portov, ako to bolo v prípade Snort detekcie. Po útokoch sa exportoval z PSAD súbor doterajšieho stavu detekcie (Status).

```
111
112  SRC:  192.168.246.247, DL: 3, Dsts: 1, Pkts: 1011, Total protocols: 3, Unique sigs: 3, Email alerts: 35
113
114      DST: 192.168.246.245
115          Scanned ports: UDP 38480, Pkts: 2, Chain: INPUT, Intf: ens33
116          Scanned ports: TCP 1-65389, Pkts: 1005, Chain: INPUT, Intf: ens33
117          Total scanned IP protocols: 3, Chain: INPUT, Intf: ens33
118          Signature match: "SCAN nmap XMAS"
119              TCP, Chain: INPUT, Count: 1, DP: 1, URG PSH FIN, Sid: 1228
120          Signature match: "ICMP PING"
121              ICMP, Chain: INPUT, Count: 1, Sid: 384
122          Signature match: "ICMP PING undefined code"
123              ICMP, Chain: INPUT, Count: 1, Sid: 365
124
```

Obrázok 7. Výstup Status – stavu z IDS systému PSAD. [Zdroj: autor]

Behom detekcie systém PSAD identifikoval niekoľko pokusov o skenovanie portov z IP adresy 192.168.246.247 s cieľom útoku na IP adresu 192.168.246.245, ktorá bola priradená pre VM Debian. Pre viac podrobností bolo potrebné nájsť informácie v systémovom zázname OS, kam zaznamenal PSAD časové informácie k jednotlivým udalostiam.

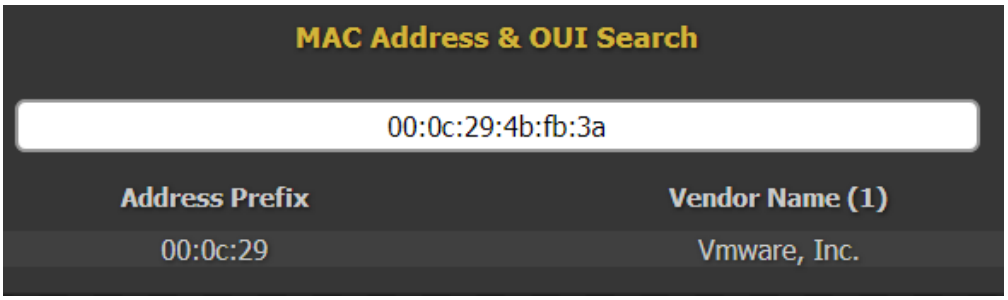



Obrázok 8. Výpis systémového záznamu s údajmi z PSAD systému. [Zdroj: autor]

```
1011 May 15 13:42:12 debian kernel: [ 5337.971143] IN=ens33 OUT= MAC=00:0c:29:81:d9:65:00:0c:29:4b:fb:3a:08:00 SRC=192.168.246.247
1012 May 15 13:42:13 debian kernel: [ 5337.996479] IN=ens33 OUT= MAC=00:0c:29:81:d9:65:00:0c:29:4b:fb:3a:08:00 SRC=192.168.246.247
1013 May 15 13:42:13 debian kernel: [ 5338.021899] IN=ens33 OUT= MAC=00:0c:29:81:d9:65:00:0c:29:4b:fb:3a:08:00 SRC=192.168.246.247
1014 May 15 13:42:13 debian psad: src: 192.168.246.247 signature match: "MISC MS Terminal Server communication attempt" (sid: 1000
1015 May 15 13:42:13 debian psad: scan detected (Nmap -sT or -sS scan): 192.168.246.247 -> 192.168.246.245 tcp: [21-8080] flags: S
```

Obrázok 9. Detail zo systémového záznamu z obrázka 8. [Zdroj: autor]

Ako je možné vidieť na obrázku 8. a detailnejšom zábere obrázka 9., je možné vidieť čas detekcie útoku PSAD systémom (15.5. 13:42:13 GTM +2) z IP adresy 192.168.246.247 na 192.168.246.245, s detekciou Nmap -sT alebo -sS skenovania – TCP pripojenia alebo TCP SYN skenovania. Pri skúmaní celkovej komunikácie bolo možné zachytiť v danom čase pokus o nadviazanie spojenia z podozrivej IP adresy na systém i prostredníctvom iných služieb, pravdepodobne kvôli rozsiahlosti skenovaných portov a protokolov. Vďaka tomu bolo možné zachytiť aj MAC adresu podozrivého zariadenia: 00:0c:29:4b:fb:3a . Na základe MAC adresy môžeme vyhľadať o akého výrobcu sieťovej karty ide a aký systém bol použitý.




Obrázok 10. Vyhľadávanie podrobností o MAC adrese. [19]

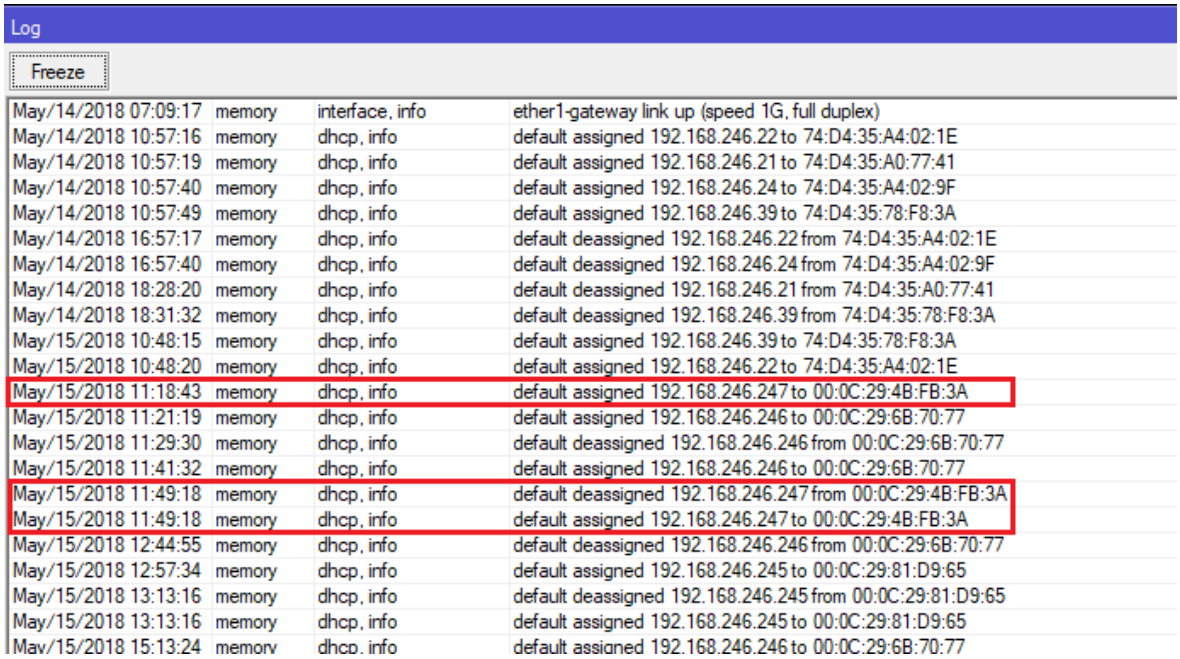
K tomu bol použitý webový nástroj stránky WhatsMyIP.org/MAC-Address-LookUp/, ktorý dokáže nájsť dodatočné informácie o MAC adrese. V tomto prípade bolo zistené, že na útok bol použitý VMware virtualizačný nástroj.

Výsledné informácie o hľadanom zdroji útoku sú po analýze detekčných a logovacích záznamov nasledovné:

- časy útokov: 15.5.2018 12:31:21 GTM +2 ; 15.5. 13:42:13 GTM +2
- IP adresa: 192.168.246.247
    - Zdroj útoku sa nachádza v rámci lokálnej sieti
- MAC adresa: 00:0c:29:4b:fb:3a
    - Použitý virtualizačný nástroj VMware

## 4.2 Identifikácia zariadenia na LAN sieti

Ako správcovia LAN siete, máme týmto prístup k sieťovým zariadeniam na sieti. Keďže sa útok podarilo hneď detekovať prostredníctvom IDS systému, môžeme skúmať aktuálne pripojenia zariadení na sieťové prvky, ako aj ich pripájanie a odpájanie zo siete. Ako prvé bolo skúmané zariadenie MicroTik router (smerovač) s IP adresou 192.168.246.1, ktorý zaznamenával a priraďoval IP adresy jednotlivým zariadeniam. Toto zariadenie si počas svojej funkcie zaznamenáva logy stavu smerovača, ako aj stav distribúcie IP adries zariadeniam, respektíve MAC adresám sieťových kariet.

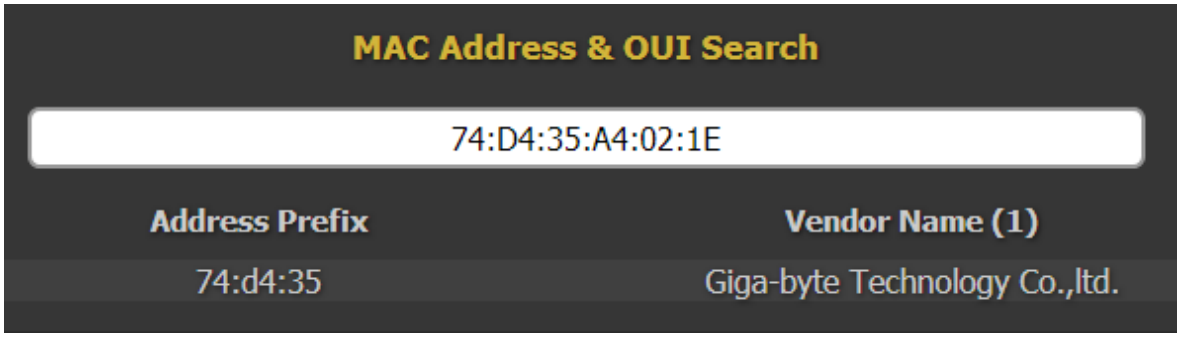

Log

Freeze

| | | | |
|---|---|---|---|
| May/14/2018 07:09:17 | memory | interface, info | ether1-gateway link up (speed 1G, full duplex) |
| May/14/2018 10:57:16 | memory | dhcp, info | default assigned 192.168.246.22 to 74:D4:35:A4:02:1E |
| May/14/2018 10:57:19 | memory | dhcp, info | default assigned 192.168.246.21 to 74:D4:35:A0:77:41 |
| May/14/2018 10:57:40 | memory | dhcp, info | default assigned 192.168.246.24 to 74:D4:35:A4:02:9F |
| May/14/2018 10:57:49 | memory | dhcp, info | default assigned 192.168.246.39 to 74:D4:35:78:F8:3A |
| May/14/2018 16:57:17 | memory | dhcp, info | default deassigned 192.168.246.22 from 74:D4:35:A4:02:1E |
| May/14/2018 16:57:40 | memory | dhcp, info | default deassigned 192.168.246.24 from 74:D4:35:A4:02:9F |
| May/14/2018 18:28:20 | memory | dhcp, info | default deassigned 192.168.246.21 from 74:D4:35:A0:77:41 |
| May/14/2018 18:31:32 | memory | dhcp, info | default deassigned 192.168.246.39 from 74:D4:35:78:F8:3A |
| May/15/2018 10:48:15 | memory | dhcp, info | default assigned 192.168.246.39 to 74:D4:35:78:F8:3A |
| May/15/2018 10:48:20 | memory | dhcp, info | default assigned 192.168.246.22 to 74:D4:35:A4:02:1E |
| May/15/2018 11:18:43 | memory | dhcp, info | default assigned 192.168.246.247 to 00:0C:29:4B:FB:3A |
| May/15/2018 11:21:19 | memory | dhcp, info | default assigned 192.168.246.246 to 00:0C:29:6B:70:77 |
| May/15/2018 11:29:30 | memory | dhcp, info | default deassigned 192.168.246.246 from 00:0C:29:6B:70:77 |
| May/15/2018 11:41:32 | memory | dhcp, info | default assigned 192.168.246.246 to 00:0C:29:6B:70:77 |
| May/15/2018 11:49:18 | memory | dhcp, info | default deassigned 192.168.246.247 from 00:0C:29:4B:FB:3A |
| May/15/2018 11:49:18 | memory | dhcp, info | default assigned 192.168.246.247 to 00:0C:29:4B:FB:3A |
| May/15/2018 12:44:55 | memory | dhcp, info | default deassigned 192.168.246.246 from 00:0C:29:6B:70:77 |
| May/15/2018 12:57:34 | memory | dhcp, info | default assigned 192.168.246.245 to 00:0C:29:81:D9:65 |
| May/15/2018 13:13:16 | memory | dhcp, info | default deassigned 192.168.246.245 from 00:0C:29:81:D9:65 |
| May/15/2018 13:13:16 | memory | dhcp, info | default assigned 192.168.246.245 to 00:0C:29:81:D9:65 |
| May/15/2018 15:13:24 | memory | dhcp, info | default assigned 192.168.246.246 to 00:0C:29:6B:70:77 |

Obrázok 11. Záznam logov na smerovači MiroTik router. [Zdroj: autor]

V rámci detekcie útoku v daný deň 15. mája 2018 môžeme vidieť pridelenie IP adresy 192.168.246.247 pre MAC adresu 00:0C:29:4B:FB:3A. Tieto adresy sa zhodujú identifikácií zdroju útoku. Na základe logu na obrázku 11. môžeme pozorovať priradenie IP adresy, ktoré prebehlo v času 11:18:43 a okrem krátkeho odpísania a spätného pripísania adresy v čase 11:49:18, môžeme evidovať, že zariadenie je stále pripojené na sieti. Rovnako však môžeme vidieť pripojené zariadenie s IP adresou 192.168.246.22, ktoré patrí už spomínanému počítaču, na ktorom prebiehajú virtualizačné nástroje s IDS systémami. Je viditeľná aj jeho MAC adresa 74:D4:35:A4:02:1E, ktorá podľa spomínaného vyhľadávača WhatsMyIP.org, ktorého výsledok je na obrázku 12., patrí fyzickej sieťovej karte, ktorej výroba je Giga-byte Technology. Tým môžeme usudzovať, že ide o fyzický počítač.




Obrázok 12. Vyhľadávanie podrobností o MAC adrese. [19]

Taktiež je vidieť priradenie IP adresy 192.168.246.39 pre MAC adresu sieťovej karty 74:D4:35:78:F8:3A. Z identickej prvej polovice MAC adresy v porovnaní s počítačom vyhľadaným na obrázku 12., môžeme usúdiť, že ide o MAC adresu fyzickej sieťovej karty a teda ďalšieho počítača. Ak sa pozrieme na danú sieť a nie je k nej iný fyzický počítač pripojený, značí to, že jedno z týchto zariadení je zdrojom útoku. Pokiaľ zvážime vylučovacou metódou, že počítač s MAC adresou končiacou A4:02:1E je izolovaný a zabezpečený, keďže na ňom prebiehajú ochranné systémy a zaznamenáva interné bezpečnostné údaje – logy, môžeme usúdiť, že počítač s končiacou MAC adresou 78:F8:3A je počítač, z ktorého útok prebiehal. Kým je daný systém stále pripojený v sieti, je možné páchateľa pristihnúť priamo pri čine.

# 5 MODELOVÁ SITUÁCIA Č. 2

Druhá modelová situácia bola vytvorená pre prípad útoku na server so zdrojom útoku z externej sieti cez WAN. Cieľom bolo zistiť všetky možnosti a informácie dostupné pre administrátora nízkonákladovými OpenSource nástrojmi, dostupnými vďaka Internetu.

## 5.1 Informácie o útoku

Modelový scenár útoku bol uskutočnený na anonymizovaný on-line cloudový server s IP adresou 80.211.x.x ; a URL adresou: *xxx.cloud* . Systém si zaznamenáva údaje logov pri komunikácií so serverom. Počas chodu serveru boli zaznamenané činnosti útoku, ktoré prislúchajú nasledujúcim záznamom z logu:

Logy pri utoku.txt

```
1  195.178.92.54 - - [04/May/2018:13:45:18 +0200]
2  195.178.92.54 - - [04/May/2018:13:45:19 +0200]
3  195.178.92.54 - - [04/May/2018:13:47:02 +0200]
4  195.178.92.54 - - [04/May/2018:13:47:03 +0200]
5  94.242.219.254 - - [04/May/2018:13:48:01 +0200]
6  94.242.219.254 - - [04/May/2018:13:48:02 +0200]
7  94.242.219.254 - - [04/May/2018:13:48:49 +0200]
8  94.242.219.254 - - [04/May/2018:13:48:50 +0200]
9  195.178.92.54 - - [04/May/2018:13:49:07 +0200]
10 79.124.59.194 - - [04/May/2018:14:32:43 +0200]
11 79.124.59.194 - - [04/May/2018:14:32:44 +0200]
12 79.124.59.194 - - [04/May/2018:14:32:45 +0200]
13 79.124.59.194 - - [04/May/2018:14:32:46 +0200]
14 79.124.59.194 - - [04/May/2018:14:32:47 +0200]
15
```

Obrázok 13. Záznam z logu spojení so serverom 80.211.x.x [Zdroj: autor]

Zdroj zaznamenanej komunikácie prichádzal z troch IP adries dňa 4. mája 2018 v čase 13:45:18 až 14:32:47 v časovej zóne GTM +2), ako je možné pozorovať na obrázku 13. záznamom logov spojení so serverom 80.211.x.x. Zachytené IP adresy majú charakter externej siete a preto je evidentné, že útok pochádzal z WAN siete prostredníctvom siete Internet. Možnosti legálneho trasovania komunikácie Internetom sú limitujúce a spoliehajú sa najmä na kooperáciu zainteresovaných strán. O jednotlivých IP adresách boli zisťované podrobnejšie informácie.

## 5.2 Trasovanie komunikácie WAN sieťou

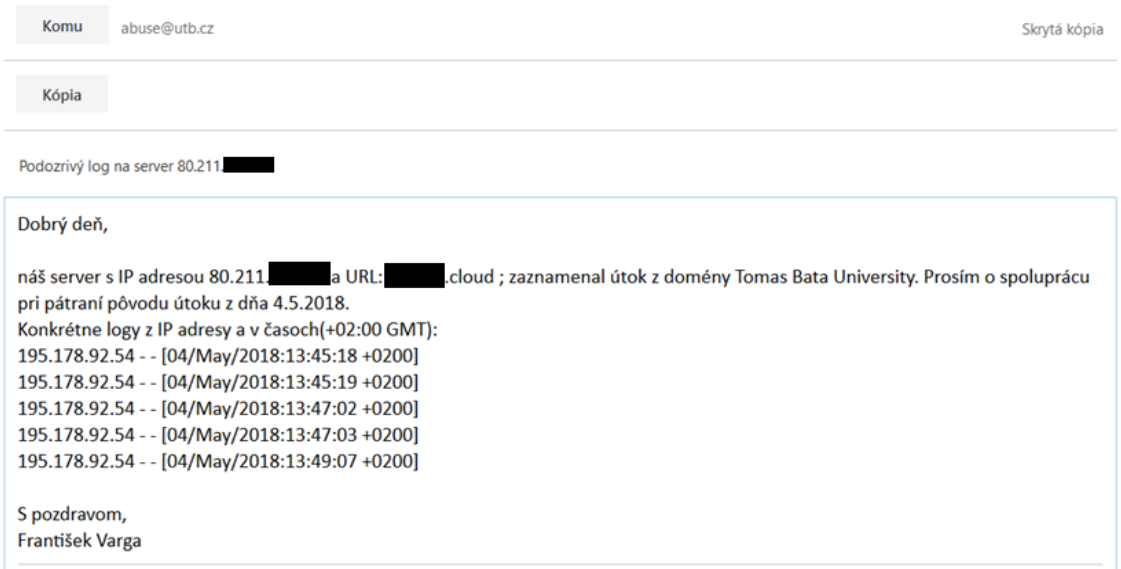
Pre každú IP adresu sa zisťovali všetky dostupné informácie, ktoré sa dali získať. Ako prvá bola podrobená skúmaniu IP adresa 195.178.92.54. Podozrivú IP adresu sa, za účelom získania informácií o správcovi siete, zadala do nástroja WHOIS [20]:

```
IP Address: 195.178.92.54
Netblock: 195/8
Status: ALLOCATED
Detail: RIPE NCC

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '195.178.88.0 - 195.178.95.255'

% Abuse contact for '195.178.88.0 - 195.178.95.255' is 'abuse@utb.cz'

inetnum:        195.178.88.0 - 195.178.95.255
netname:        UTB-T34CZ
descr:          Tomas Bata University
descr:          Zlin
country:        CZ
org:            ORG-TBUi1-RIPE
admin-c:        TBUI1-RIPE
tech-c:         TBUI1-RIPE
status:         ASSIGNED PA
mnt-by:         TENCZ-MNT
remarks:        Please report network abuse -> abuse@utb.cz
created:        1970-01-01T00:00:00Z
last-modified:  2013-10-11T11:51:58Z
source:         RIPE

% Information related to '195.178.64.0/19AS2852'

route:          195.178.64.0/19
descr:          CESNET-T34CZ
origin:         AS2852 - výsledek Whois dotazu">AS2852
mnt-by:         AS2852-MNT
remarks:        Please report abuse -> abuse@cesnet.cz
created:        1970-01-01T00:00:00Z
last-modified:  2006-06-26T14:36:38Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.91.2
(HEREFORD)
```

Zistilo sa, že daný útok využil sieť s doménou Tomas Bata University s lokáciou mesta Zlín v Českej republike. Pre podrobnejšie informácie bolo vyhľadané aj identifikačné značenie administrátorov siete: TBUI1-RIPE:

```
% Information related to 'TBUI1-RIPE'

role:           Tomas Bata University in Zlin Admins
address:        Univerzita Tomase Bati
address:        nam. T. G. Masaryka 5555
address:        Zlin
address:        760 01
address:        The Czech Republic
phone:          +420 576 032 525
fax-no:         +420 576 032 121
org:            ORG-TBUi1-RIPE
admin-c:        PV148-RIPE
tech-c:         PV148-RIPE
nic-hdl:        TBUI1-RIPE
abuse-mailbox:  abuse@utb.cz
mnt-by:         TENCZ-MNT
created:        2013-06-12T13:28:25Z
last-modified:  2013-10-11T11:51:59Z
source:         RIPE # Filtered
```

Identifikátor administrátorov siete zobrazil, že sa jedná o Administrátorov Univerzity Tomáše Bati ve Zlíně, s adresou umiestnenia T. G. Masaryka 5555, Zlín, Česká republika. Daná oblasť IP adries bola priradená v roku 2013 pre danú spoločnosť, čo môže naznačovať o serióznosti administrátorov, ktorí vedú sieť päť rokov. Pre komunikáciu so všetkými podrobnosťami z logov a informáciami o útoku sa odporúča e-mailová komunikácia. Pre abuse@utb.cz bol vyhotovený nasledovný e-mail s údajmi logov zaznamenanej IP adresy a všetkých časov pri zachytenej komunikácií:




Obrázok 14. Ukážka e-mailu s požiadavkou o spoluprácu. [Zdroj: autor]

Výsledkom bola nadviazaná spolupráca s administrátormi Univerzity Tomáše Bati. V rámci sekcie trasovania WAN sieťou však prv analyzujeme všetky podozrivé IP adresy. Ako druhá bola skúmaná IP adresa 94.242.219.254 prostredníctvom nástroja WHOIS:

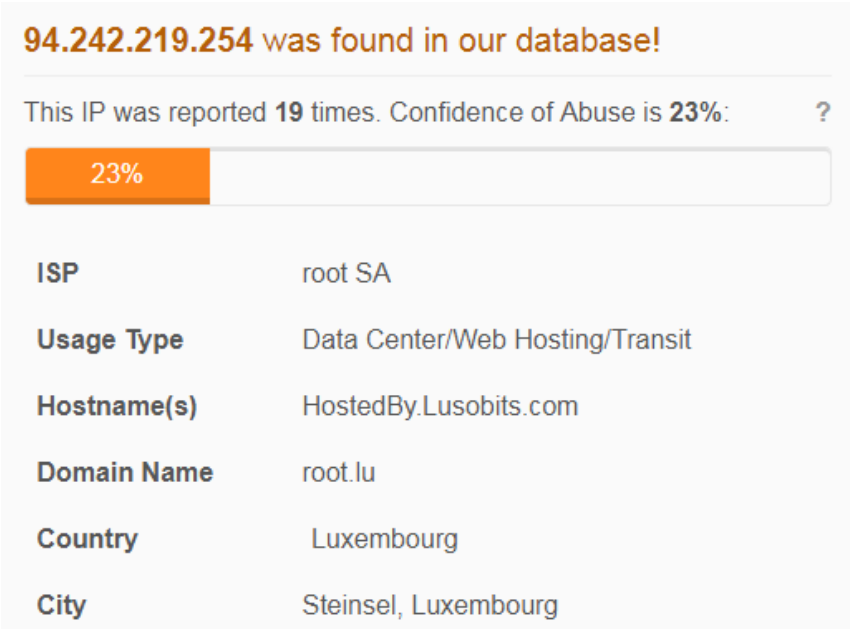
```
IP Address: 94.242.219.254
Netblock: 094/8
Status: ALLOCATED
Detail: RIPE NCC

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '94.242.219.240 - 94.242.219.255'

% Abuse contact for '94.242.219.240 - 94.242.219.255' is
'abuse@lusobits.com'

inetnum:        94.242.219.240 - 94.242.219.255
netname:        Evoluso
country:        LU
admin-c:        GF10682-RIPE
tech-c:         GF10682-RIPE
abuse-c:        EA6202-RIPE
status:         ASSIGNED PA
mnt-by:         ROOT-MNT
created:        2017-11-22T15:45:10Z
last-modified:  2017-11-22T15:45:10Z
source:         RIPE

% Information related to '94.242.192.0/18AS5577'

route:          94.242.192.0/18
descr:          root SA (www.root.lu)
origin:         AS5577 - výsledek Whois dotazu">AS5577
mnt-by:         ROOT-MNT
created:        2009-10-19T07:44:58Z
last-modified:  2016-07-05T12:21:50Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.91.2
(HEREFORD)
```

Zadaná IP adresa má podľa WHOIS databázy lokáciu v Luxembursku. V tomto prípade ide o medzinárodné pripojenie. Názov siete je evidovaný pod Evoluso, čo pri hľadaní internetom našlo poskytovateľa služieb prenájmu serverov. Ten na svojich stránkach (evoluso.com) poskytuje servery v rôznych krajinách: Holandsko, Švajčiarsko, Švédsko a Luxembursko. Pre podrobnejšie informácie o administrátorovi siete bol vyhľadaný prostredníctvom WHOIS identifikátor GF10682-RIPE:

```
% Information related to 'GF10682-RIPE'

person:          Gualter Fernandez
address:         Rua D. António Ferreira Gomes 4250-572 Porto
phone:           +369738827789
nic-hdl:         GF10682-RIPE
mnt-by:          EVOLUSO-MNT
created:         2016-12-06T10:15:01Z
last-modified:   2017-10-30T23:31:55Z
source:          RIPE

LOCATED
Detail: RIPE NCC
```

Informácie o administrátorovi danej siete sú meno a miesto registrácie v Porte - Portugalsko. Kontaktovanie administrátora nebolo neúspešné, preto sa informácie o IP adrese skúmali naďalej. Podozrivá IP adresa bola skontrolovaná v zoznamov blacklistov, ktoré ponúka viacero webov, medzi nimi aj spomínaný Whois.Smart.cz [20]. Výsledkom vyhľadávania bolo nájdenie danej IP adresy v dvoch blacklistoch.

Pre ďalšie analýzy sa použil webový nástroj AbuseIPDB [21] pre skúmanie histórie hlásení nebezpečnej činnosti tvorenej z IP adresy 94.242.219.254:




Obrázok 15. Výstup informácií z AbuseIPDB pre 94.242.219.254. [21]

Podozrivá IP adresa bola už zaznamenaná a hlásená pre možnosti útoku. Taktiež informuje o možnom type používania danej siete: Data centrum/web hosting/Transit – čo opisuje možnosť použitia serveru na presmerovanie komunikácie.

| Reporter | Date | Comment | Categories |
|---|---|---|---|
| Anonymous | 20 May 2018 | | Hacking |
| Anonymous | 18 May 2018 | Attempted to admin login on NAS | Hacking Brute-Force |
| Anonymous | 15 May 2018 | | Hacking |
| Anonymous | 13 May 2018 | | Brute-Force |
| Anonymous | 08 May 2018 | Qnap nas login attempt | Hacking Brute-Force |
| Anonymous | 07 May 2018 | QNAP NAS Login attempt | Hacking Brute-Force |
| Xoto | 06 May 2018 | Attempted to log on to NAS | Port Scan Hacking |
| Anonymous | 05 May 2018 | admin login attempt on QNAP | Hacking Brute-Force |
| Anonymous | 04 May 2018 | | Brute-Force |
| Anonymous | 04 May 2018 | Unauthorized admin login attempt | Port Scan Hacking Brute-Force Web App Attack |

Obrázok 16. Zoznam hlásených útokov z adresy 94.242.219.254. [21]

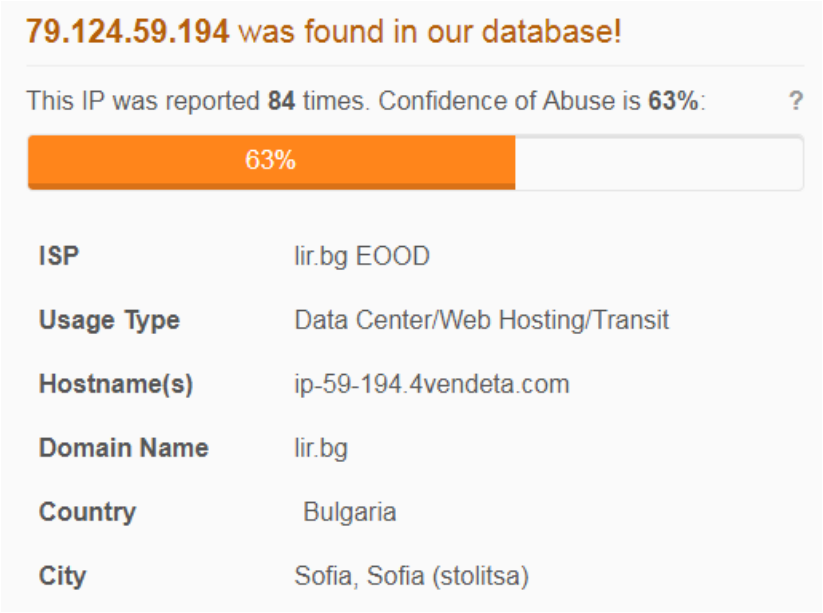
Je evidentné, že útoky z tohto serveru je časté. S použitím informácie o presmerovaní komunikácie vieme konštatovať, že ide o VPN server alebo server Tor siete, ktorý sa využíva na krytie identity útočníka pri jeho nelegálnej činnosti v kyberpriestore. V tomto prípade trasovanie dát za spolupráce administrátorov sietí je veľmi náročné, dokonca až nemožné.

V prípade IP adresy 79.124.59.194 je príbeh veľmi podobný. V tomto prípade WHOIS databáza zobrazila nasledovné informácie o IP adrese a Administrátorovi s identifikátorom PD8817-RiPE:

```
IP Address: 79.124.59.194
Netblock: 079/8
Status: ALLOCATED
Detail: RIPE NCC


% Information related to '79.124.59.0 - 79.124.59.255'

% Abuse contact for '79.124.59.0 - 79.124.59.255' is 'noc@4vendeta.com'

inetnum:        79.124.59.0 - 79.124.59.255
netname:        Tamatiya-EOOD
descr:          Tamatiya EOOD
country:        BG
org:            ORG-IPTL2-RIPE
admin-c:        PD8817-RIPE
tech-c:         PD8817-RIPE
mnt-routes:     TAMATYA-MNT
mnt-domains:    TAMATYA-MNT
status:         SUB-ALLOCATED PA
mnt-by:         AZ39139-MNT
mnt-by:         TAMATYA-MNT
created:        2014-02-04T12:30:51Z
last-modified:  2017-08-23T09:01:11Z
source:         RIPE
```

```
% Information related to '79.124.59.0/24AS50360'

route:          79.124.59.0/24
origin:         AS50360 - výsledek Whois dotazu">AS50360
mnt-by:         TAMATYA-MNT
created:        2014-11-20T08:23:26Z
last-modified:  2017-08-23T08:54:35Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.91.2
(HEREFORD)

% Information related to 'PD8817-RIPE'

person:         Petar Dimov
address:        hostmaster@4vendeta.com
phone:          +359988865442
nic-hdl:        PD8817-RIPE
mnt-by:         TAMATYA-MNT
created:        2016-11-06T19:36:43Z
last-modified:  2017-10-30T23:28:52Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.91.2
(HEREFORD)
```

IP adresa je registrovaná pod Bulharskú spoločnosť TAMATYA pôsobiaca pod doménou 4vendeta.com. Administrátor siete je zapísaný ako Petar Dimov, ktorý podľa stránok spoločnosti 4Vendeta Communications je prezidentom 4 Vendeta. Či administrátor jednej zo sietí, ktorá je zapísaná pod spoločnosťou internetového poskytovateľa, je zároveň aj prezident spoločnosti, je otázna. Preto bola tvorená následná analýza IP adresy pomocou AbuseIPDB, ktorej výstup je nasledovný:




Obrázok 17. Výstup informácií z AbuseIPDB pre 79.124.59.194. [21]

| Reporter | Date | Comment | Categories |
|---|---|---|---|
| ✔ 1reg.online | 07 May 2018 | GET /wp-login.php HTTP/1.1 | Web App Attack |
| ✔ SoManyDesigns | 07 May 2018 | IP address was detected and listed 1433 times in the pa st 28 days -- IP is infected (or NATting for ... show more | Exploited Host |
| ✔ SoManyDesigns | 07 May 2018 | BAD UA -- GET: / -- Mozilla/5.0 (Windows NT 5.1; rv:7.0 .1) Gecko/20100101 Firefox/7.0.1 | Bad Web Bot |
| ✔ louisep | 06 May 2018 | user/register | Web Spam |
| ✔ Anonymous | 06 May 2018 | | Web App Attack |
| Anonymous | 06 May 2018 | Malicious Traffic/Form Submission | Web Spam |
| ✔ www.elinox.de | 05 May 2018 | Referer Spam - Detected by ELinOX-ALM | Web Spam |
| Anonymous | 02 May 2018 | /wp-config.php.bak /wp-config.bak | Web App Attack |
| ✔ nowyouknow | 02 May 2018 | Malicious Traffic/Form Submission | Phishing Web Spam |
| ✔ www.elinox.de | 01 May 2018 | Referer Spam - Detected by ELinOX-ALM | Web Spam |

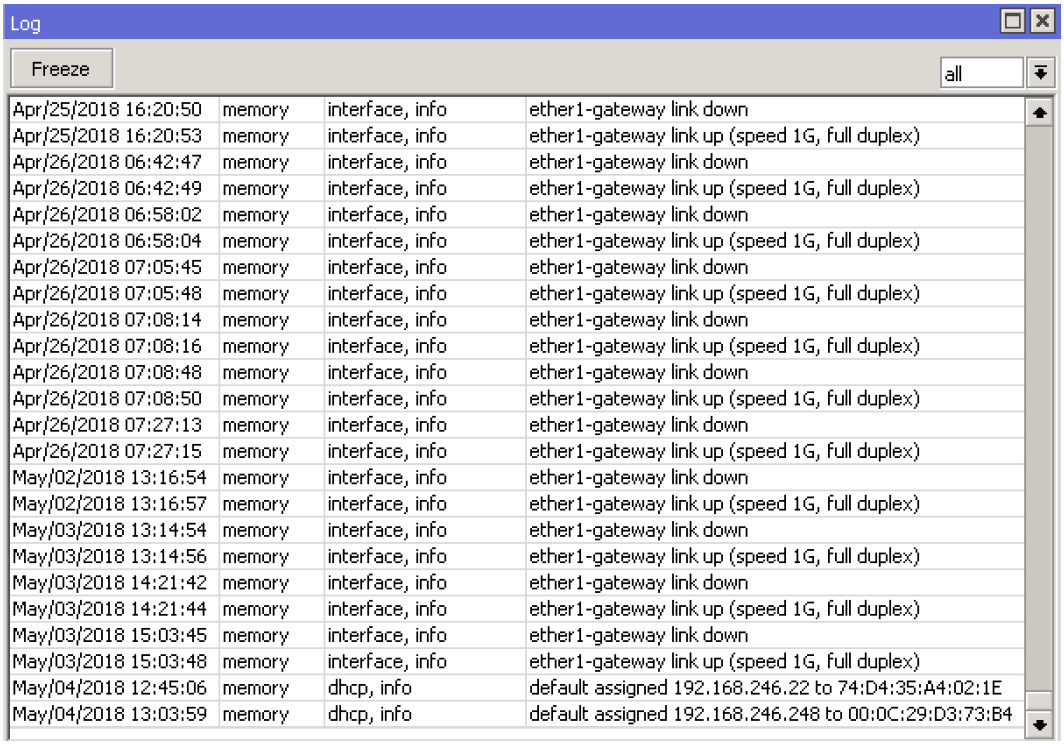
Obrázok 18. Zoznam hlásených útokov z adresy 79.124.59.194 [21]

Webový nástroj AbuseIPDB zobrazil až 84 hlásení z podozrivej IP adresy a 63% vierohodného tvrdenia, že sa IP adresa zneužíva pre nelegálnu činnosť útokov. Je vidieť, že cieľom niekoľkých útokov bolo množstvo registrovaných serverov, ktoré čelili útokom ako phishing, webový spam, použitie exploitov a ďalšie. IP adresa 79.124.59.194 bola zaznamenaná na 7 blacklistoch, čo značne spochybňuje reputáciu adresy. Keďže sa aj tento server využíva ako web hosting/transit, bolo usúdené, že môže ísť s vysokou pravdepodobnosťou o útok prostredníctvom Tor siete.

## 5.3 Identifikácia zariadenia na LAN sieti

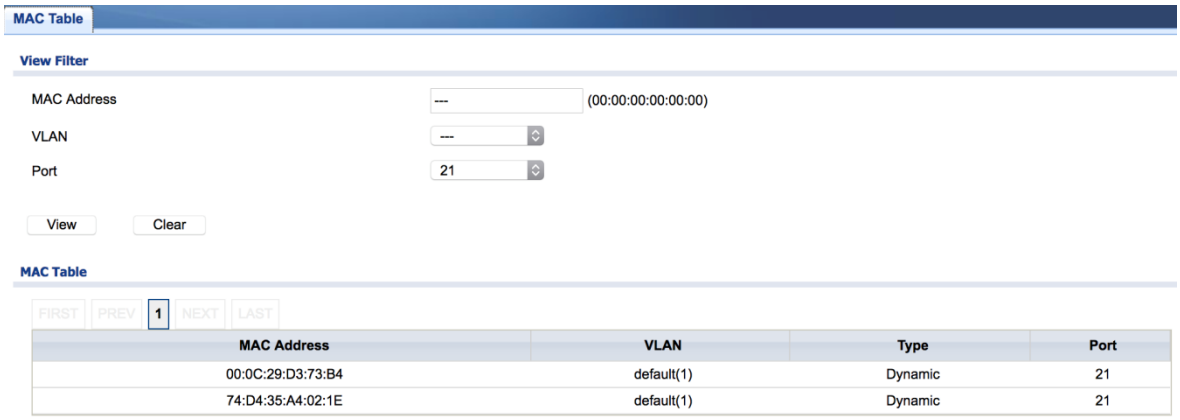
Z podozrivých IP adries bola úspešná komunikácia len s administrátormi siete Univerzity Tomáše Bati ve Zlíně. Tí boli pre zachovanie svojej dobrej reputácie čistých poskytovateľov služieb internetu a spravovania Internetového pripojenia pre univerzitu, veľmi ochotní. Vďaka ich spolupráci bolo možné zistiť, z ktorej podsiete sa útok uskutočnil a ktoré zariadenia boli v daný čas 4.5.2018 13:45:18 až 13:49:07 (GTM +2) pripojené na sieť. Podsieť mala rozsah 192.168.246.0/8 a bola zapojená pod smerovačom MicroTik router so zapojeným prepínačom pre drôtové pripojenie na viaceré počítače na univerzitnej učebni.

Výstup z pripojení na router je možné vidieť na obrázku 19. V Čase 12:45:06 sa pripojilo zariadenie do siete s MAC adresou 74:D435:A4:02:1E a vzápätí druhé zariadenie v čase 13:03:59 s MAC adresou 00:0C:29:D3:73:B4. Obe zariadenia časovo súhlasia s časom útoku.




| | | | |
|---|---|---|---|
| Apr/25/2018 16:20:50 | memory | interface, info | ether1-gateway link down |
| Apr/25/2018 16:20:53 | memory | interface, info | ether1-gateway link up (speed 1G, full duplex) |
| Apr/26/2018 06:42:47 | memory | interface, info | ether1-gateway link down |
| Apr/26/2018 06:42:49 | memory | interface, info | ether1-gateway link up (speed 1G, full duplex) |
| Apr/26/2018 06:58:02 | memory | interface, info | ether1-gateway link down |
| Apr/26/2018 06:58:04 | memory | interface, info | ether1-gateway link up (speed 1G, full duplex) |
| Apr/26/2018 07:05:45 | memory | interface, info | ether1-gateway link down |
| Apr/26/2018 07:05:48 | memory | interface, info | ether1-gateway link up (speed 1G, full duplex) |
| Apr/26/2018 07:08:14 | memory | interface, info | ether1-gateway link down |
| Apr/26/2018 07:08:16 | memory | interface, info | ether1-gateway link up (speed 1G, full duplex) |
| Apr/26/2018 07:08:48 | memory | interface, info | ether1-gateway link down |
| Apr/26/2018 07:08:50 | memory | interface, info | ether1-gateway link up (speed 1G, full duplex) |
| Apr/26/2018 07:27:13 | memory | interface, info | ether1-gateway link down |
| Apr/26/2018 07:27:15 | memory | interface, info | ether1-gateway link up (speed 1G, full duplex) |
| May/02/2018 13:16:54 | memory | interface, info | ether1-gateway link down |
| May/02/2018 13:16:57 | memory | interface, info | ether1-gateway link up (speed 1G, full duplex) |
| May/03/2018 13:14:54 | memory | interface, info | ether1-gateway link down |
| May/03/2018 13:14:56 | memory | interface, info | ether1-gateway link up (speed 1G, full duplex) |
| May/03/2018 14:21:42 | memory | interface, info | ether1-gateway link down |
| May/03/2018 14:21:44 | memory | interface, info | ether1-gateway link up (speed 1G, full duplex) |
| May/03/2018 15:03:45 | memory | interface, info | ether1-gateway link down |
| May/03/2018 15:03:48 | memory | interface, info | ether1-gateway link up (speed 1G, full duplex) |
| May/04/2018 12:45:06 | memory | dhcp, info | default assigned 192.168.246.22 to 74:D4:35:A4:02:1E |
| May/04/2018 13:03:59 | memory | dhcp, info | default assigned 192.168.246.248 to 00:0C:29:D3:73:B4 |

Obrázok 19. Záznam logov zo smerovača MicroTik router na sieti UTB. [Zdroj: autor]

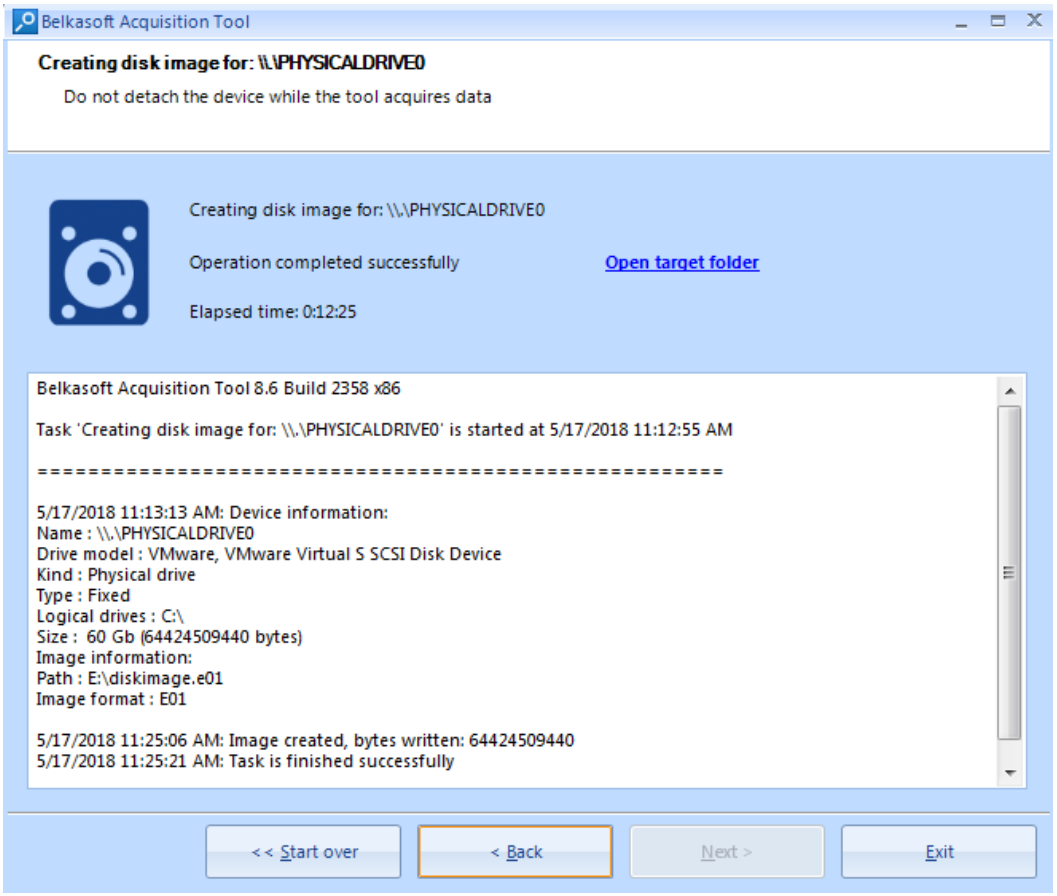



Obrázok 20. Tabuľka MAC adries pripojených na prepínači. [Zdroj: autor]

Vďaka použitiu prepínača s rozhraním jeho obsluhy, môžeme monitorovať aktívne pripojené zariadenia, ich MAC adresu a číslo portu – zásuvky, v ktorom pripojené zariadenie figuruje. S porovnaním s tabuľkou na obrázku 19 zo smerovača a tabuľkou na obrázku 20 z prepínača, bolo zistené, že obe zariadenia sú pripojené na rovnakej zásuvke portu číslo 21. Po vyhľadaní MAC adresy pomocou webového nástroja [19] sa zistilo, že sa jedná v prípade 00:0C:29:D3:73:84 o virtuálny nástroj VMware a v prípade 74:D4:35:A4:02:1E o sieťovú kartu Giga-byte Technology – fyzický počítač. Toto zariadenie sa stalo podozrivým z útoku na server 80.211.x.x. Keďže sa nezaznamenalo priame pripojenie na sieti UTB na tento server, je potrebná dodatočná forenzná analýza podozrivého systému.

## 5.4 Analýza identifikovaného podozrivého zariadenia

Pre analýzu zariadenia, konkrétne podozrivého virtuálneho operačného systému, ktorý bol použitý pri útoku, bol použitý nástroj pre zaznamenanie obrazu disku (disk Image). Pre jeho vyhotovenie sa použil nástroj Belkasoft Acquisition Tool 8.6 x86.




Obrázok 21. Tvorba obrazu disku nástrojom Belkasoft Acquisition. [Zdroj: autor]

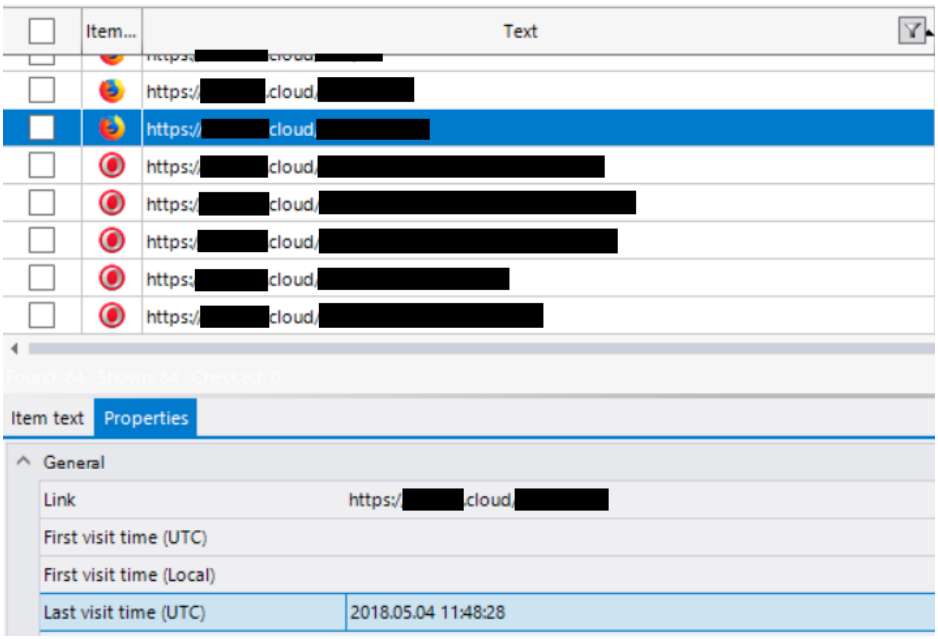
Image – obraz disku sa následne zdokumentoval s vypočítaním otlačku HASH v prípade jeho autentizácie pri analyzovaní po presune na iné úložisko, prípadne pre neskoršie účely.

Tabuľka 2. Informácie o súbore obrazu podozrivého disku. [Zdroj: autor]

| Názov a veľkosť súboru | Hash MD5 | Hash SHA1 | Popis súboru |
|---|---|---|---|
| diskimage.E01<br>14 484 087 507 B | 359366cc3f1977da<br>63228c7c8e39c374 | 05c283191c65d656e5d7<br>b36cc63ae054f594f008 | Obraz podozri-<br>vého disku |

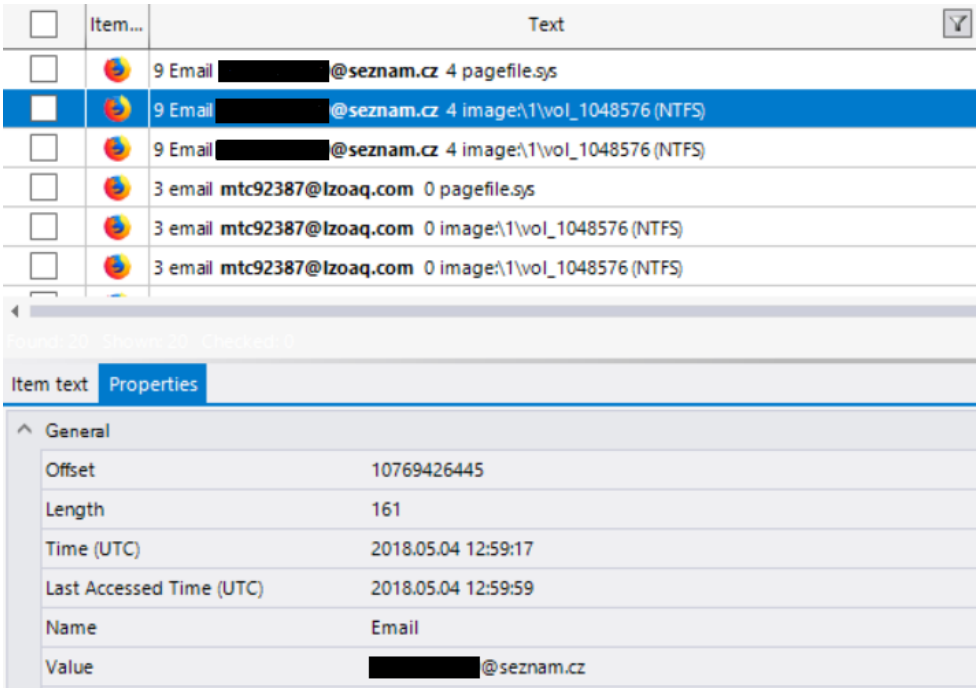
Následne nástrojom Belkasoft Evidence Center bol obraz disku analyzovaný s výstupom akcií, ktoré sa na danom disku odohrávali. Tento výstup je možný prehliadať prostredníctvom Belkasoft Evidence Reader, verzia 9.0.2518.0.

Ako prvé sa vyhľadávala IP adresa cieľu útoku, 80.211.x.x a URL: *xxx.cloud* pre nájdenie prepojenia systému so serverom.



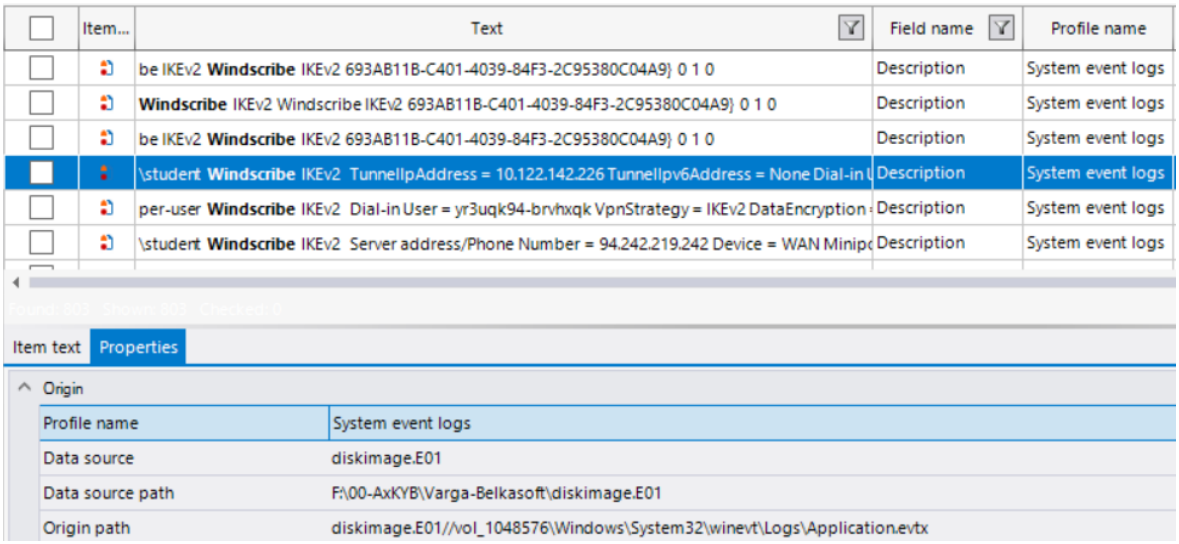

Obrázok 22. Výstup z BER – prepojenie systému so serverom. [Zdroj: autor]

Na skúmanom disku sa našlo 64 zhôd pri vyhľadaní servera. Čas komunikácie so serverom sa zhoduje s časom útoku na server (13:45:18 až 14:32:47 v časovej zóne GTM +2). Tým sa potvrdilo prepojenie so serverom a dané zariadenie je oficiálne klasifikované ako použitý nástroj na útok. Následne bolo potrebné získať dáta o útočníkovi, zber dát bol teda sústredený podľa časovej tabuľky (timeline) jednotlivých udalostí v rozpätí dňa, kedy sa útok uskutočnil. Po filtrovaní bolo nájdených 7364 záznamov. Stanovil sa čas zapnutia a vypnutia operačného systému (zapnutie: 12:43:42 ; vypnutie: 15:18:01). Najrelevantnejšie bolo nájdenie emailovej adresy ****@seznam.cz, ktorá by mohla byť páchateľova a dopomôcť k jeho dolapeniu. Rovnako bolo zachytených niekoľko fiktívnych emailových adries, jedna z nich je viditeľná aj na obrázku 23. Email bol na základe ďalších záznamov vytvorený zo stránky 10minutemail.net. Časová značka vytvorenia záznamov zodpovedá dátumu a približnej dobe útokov a manipulácií s počítačom.

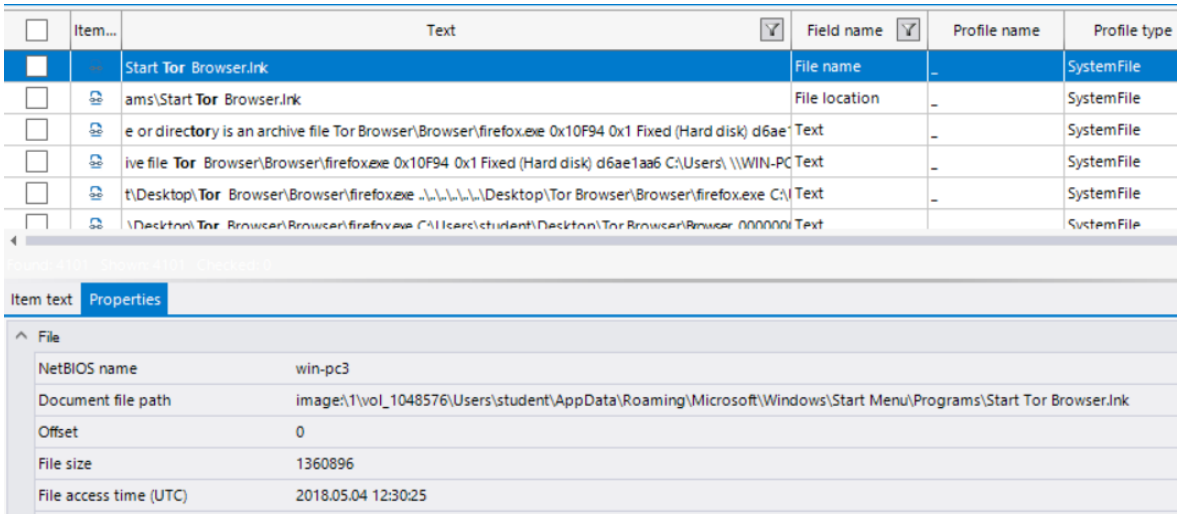



Obrázok 23. Výstup z BER – emailové adresy. [Zdroj: autor]

Ďalšie skúmané záznamy boli nájdené v súvislosti s programom WindScribe, ktorý ponúka služby s tvorbou VPN prenosu. Časy záznamov spustenia prenosu zodpovedajú s časom útoku, ktorý prišiel z Luxemburského serveru s IP adresou 94.242.219.254. Rovnako je možné v záznamoch vidieť aj IP adresu pridelenú serverom pre tento VPN prenos (94.242.219.242).




Obrázok 24. Výstup z BER – VPN software WindScribe. [Zdroj: autor]




Obrázok 25. Výstup z BER – Tor prehliadač. [Zdroj: autor]

Ďalšie nájdené záznamy boli v súvislosti s prehliadačom Tor – jeho inštalácia a spustenie. Časové otlačky záznamov sa približne zhodujú so zaznamenanými logmi incidentu, IP adresy však nie. To sa pri Tor-e dalo očakávať, keďže jeho komunikácia prechádza minimálne tromi náhodnými servermi.

Výsledky získané z analýzy dát počítača sú dostačujúce pre overenie podozrenia zariadenia z jeho použitia pri útoku na server a tým aj nájdenie študenta. Toho sa podarilo vypátrať na základe emailového účtu domény seznam.cz. Študent sa následne priznal a trest mu bol odpustený pod podmienkou, že už podobné delikty nebude opakovať.

# 6 FAKTORY OVPLYVŇUJÚCE LOKALIZOVANIE DÁTOVEJ KOMUNIKÁCIE

Modelové situácie v kapitole 4. a 5. aplikovali navrhnutú metodiku trasovania dátového spojenia. Pre finálne lokalizovanie zariadenia – zdroja komunikácie (kybernetického útoku), bolo potrebné postupovať jednotlivými krokmi vyšetrovania. Vyšetrovanie však môže byť ovplyvnené rôznymi faktormi, ktoré môžu uľahčiť alebo sťažiť samotnú schopnosť trasovať podozrivé dátové spojenie. Na základe modelových situácií bolo možné niektoré z týchto faktorov určiť a spresniť.

Pri prvom kroku detekcie spojenia je dôležité zaznamenávanie komunikácie a zavedenie logovania pri sprístupnení siete jednotlivým koncovým zariadeniam. Kvôli záznamu veľkého množstva dát je potrebné disponovať adekvátnou kapacitou úložiska a výkonnou technikou na spracovávanie dát. Daná sieť je primárne určená na komunikačné spojenie a prenos dát. Jej cieľom je zefektívniť aktíva spoločností, alebo zvýšiť úroveň pohodlia pre domácnosti. Vďaka množstvu dátových spojení, ktoré nemajú nebezpečný charakter, je pri monitoringu významným faktorom otázka zavedenia ich analýzy. Tá ma za úlohu detekovať možné podozrivé dátové spojenia, ktoré by mohli ohroziť počítačovú sieť, jej prvky a koncové zariadenia. Na túto detekciu sa používajú systémy IDS. Dôležité je systém detekcie prieniku do siete neustále aktualizovať, aby mohol zachytiť najnovšie trendy útokov. Pre veľké spoločnosti, ktoré zavádzajú monitoring siete, je potrebné uvážiť, ako dlho budú jednotlivé dáta uchovávať a stanoviť obdobie, po ktorom budú dáta automatický vymazané. Ak je toto obdobie krátke a záznamy nie sú dostupné pri odhalení kriminálnej činnosti, trasovanie takejto činnosti k jeho zdroju nie je možné. Skladovanie dát je však nákladné na systémy, a tým aj na finančné prostriedky. Treba preto nájsť vhodný súlad medzi mierou ohrozenia a uvoľnením finančných prostriedkov na zabezpečenie organizácie. Jednotlivé organizácie a spoločnosti taktiež musia zvážiť, aké všetky typy dát sa budú monitorovať a analyzovať, aby nedošlo k porušeniu ochrany osobných údajov užívateľov siete.

Pre správcu siete je dôležité mať spracovávanie a selekciu informácií z logu vo formáte, z ktorého je možné získať potrebné dáta k ďalšej analýze. Z logu musia byť jasne dohľadateľné odpovede na tri stanovené otázky: „Čo?“ – incident (útok), jemu priradený čas – „Kedy?“ a nájdenie zdroja komunikácie – „Odkiaľ?“. Pri selekcií IP adresy je potrebné vedieť rozpoznať, či sa spojenie nadviazalo s externou WAN sieťou alebo so zariadením v rámci internej LAN sieti.

Ak podozrivé spojenie pochádzalo z externej WAN siete, je potrebné nastaviť proces na trasovanie komunikácie. Ten začína prostredníctvom získania podrobných informácií o IP adrese zdroja komunikácie. Nástrojom WHOIS je možné získať informácie o serveri poskytovateľa internetovej služby, pod ktorú patrí IP adresa. Pri zneužití tejto siete je možné kontaktovať správcu siete a pokračovať vo vyšetrovaní. Ak však správca neodpovedá na žiadosti spolupráce, ktorá nie je jeho povinnosťou (pokiaľ tak neurobia orgány činné v trestnom konaní so súdnym príkazom), stopa po páchateľovi chladne. Rovnako, ako pri lokálnych správcoch siete, i poskytovateľ siete má možnosť logovania jednotlivých spojení. Pre Českú republiku zo Zákona o kybernetickej bezpečnosti č. 181/2014 Sb. [11] je toto logovanie povinnosťou aspoň na dobu troch mesiacov. Ak však páchateľ využíva služby VPN alebo Tor, ktoré šifrovaným tunelom presmerujú komunikáciu cez server inou krajinou, ktorá podobné povinnosti zákonne nevyžaduje, pri dopytovaní informácií o logoch nebude mať poskytovateľ čo ponúknuť a tým sa stopa po páchateľovi stráca. Pokiaľ správca siete spolupracuje a vie poskytnúť požadované informácie o logoch páchateľa, je možné sa týmto dopytovaním dostať až na miestnu sieť LAN, z ktorej bol páchateľ pripojený.

Po identifikácií LAN siete je potrebné kontaktovať miestnych administrátorov pre ďalšiu spoluprácu pri analýze zdroja útoku. Nájdenie zariadenia, ktoré bolo pripojené v čase útoku na sieť vyžaduje ďalšie monitorovacie nástroje, rovnako ako pri monitoringu poškodenej siete. Pre identifikáciu zariadenia sa môžu použiť záznamy pripojenia do siete jednotlivým sieťovým kartám koncových zariadení – priradenie IP adresy MAC adrese. Niektoré sieťové prvky touto možnosťou disponujú, závisí to však od ich ceny a kvality. Iné sieťové prvky využívajú iba monitoring aktuálnych zapojených zariadení.

Miestny správca, po selekcií podozrivých zariadení, môže jednotlivé zariadenia podrobiť vyšetreniu digitálnymi forenznými nástrojmi pre získanie extrahovateľných digitálnych dát, metadát alebo latentných/skrytých digitálnych dát.

Úspešnosť trasovania spočíva v zhode viacerých komplexných faktorov, ktoré sú založené najmä na stanovení vyšetrovateľských postupov, spolupráci zainteresovaných osôb a možnosti použitia forenzných nástrojov.

# ZÁVER

V čase, kedy sa o kybernetickej bezpečnosti sa z médií dozvedáme stále častejšie, je potrebné hľadať riešenia na možné hrozby kybernetických incidentov a útokov. Pri kybernetickom incidente sa v súčasnosti získavajú dáta o type incidentu, útoku, dôsledkoch, motíve a príčiny. Trasovanie a lokalizácia dát v počítačových sieťach je jedným z mnohých krokov, ktoré spolu tvoria súbor digitálneho forenzného vyšetrovania. Cieľom práce bolo zhrnúť teoretické znalosti potrebné pre pochopenie komunikácie na počítačovej sieti, aby bolo možné nadviazať na tému trasovania. Následne sa stanovila metodika vyšetrovania incidentu s možnosťami zapojenia digitálnych forenzných a bezpečnostných nástrojov pre efektívne trasovanie a lokalizovanie dátových spojení.

V praktickej časti boli vytvorené dve modelové situácie, v ktorých metodika bola demonštrovaná a poukázala na podmienky pre úspešné trasovanie dát za pomoci OpenSource programov. Prvá modelová situácia bola tvorená so scenárom interného útoku užívateľa na spoločnej LAN sieti. Pre tieto účely boli spustené detekčné IDS nástroje Snort a PSAD. Zaznamenané údaje boli vyhodnotené a následne sa trasovalo zariadenie zdroja útoku. Pri druhej modelovej situácií bol pod kybernetickým útokom server, ktorý zachytil komunikáciu z externých WAN sietí. Pri trasovaní sa použili prístupné nástroje WHOIS a databáza AbuseIPDB pre vyhodnotenie zaznamenaných IP adries. Pre legálne trasovanie WAN sieťou je nutné dopytovanie informácií od správcov sietí, z ktorých komunikácia bola zachytená. Z troch IP adries sa spolupráca nadviazala iba s jedným. Ostatné IP adresy boli vyhodnotené ako možné sieťové „šupky cibule“ s využitými VPN a Tor sietí. Trasovanie komunikácie WAN sieťou je možné z legislatívneho hľadiska iba za spolupráce jednotlivých poskytovateľov sieťových služieb a administrátorov sietí.

Pre záverečné zhodnotenie faktorov úspešného trasovania komunikácie je potrebné, aby správcovia zaznamenávali údaje logov s identifikačnými prvkami komunikácie (IP adresa a MAC adresa), časový údaj s časovou zónou (GMT) a pre vyšetrovanie samotné aj ostatné údaje spojené s identifikáciou páchateľa. Hlavnými problémami pri trasovaní môžu byť nezavedené logovania komunikácií a nespolupracovanie administrátorov sietí. Otázkou do budúcna je stanoviť, v ktorých inštitúciách je potrené zaviesť obdobné nástroje pre podrobné logovanie, aby nebola porušená miera osobného súkromia.

# ZOZNAM POUŽITEJ LITERATÚRY

[1] *Dohovor o kybernetickej kriminalite: Podrobnosti zmluvy č. 185, Európská rada* [online]. 2001 [cit. 2018-05-16]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[2] Virus:W32/Melissa. *F-Secure* [online]. 2013 [cit. 2018-05-16]. Dostupné z: https://www.f-secure.com/v-descs/melissa.shtml

[3] JONES, David a Jim FINKLE. U.S. indicts hackers in biggest cyber fraud case in history. *Reuters* [online]. 25.7.2013 [cit. 2018-05-16]. Dostupné z: https://www.reuters.com/article/us-usa-hackers-creditcards-idUSBRE96O0RI20130725

[4] LEMOS, Robert. Cyber attacks disrupt Kyrgyzstan's networks. *Security Focus* [online]. 30.01.2009 [cit. 2018-05-16]. Dostupné z: https://www.securityfocus.com/brief/896

[5] KOSTOPOULOS, George K. *Cyberspace and cybersecurity*. Boca Raton, Fl.: CRC Press, c2013. ISBN 978-1-4665-0133-1.

[6] SOSINSKY, Barrie A. *Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]*. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

[7] Internet Exchange Directory. In: Packet Clearing House: PCH [online]. [cit. 2018-05-16]. Dostupné z: https://www.pch.net/ixp/dir#!mt-zoom=%5B4.35275281648062%2C-0.3879190177554041%2C-0.12626890635575722%5D

[8] KUROSE, James F. a Keith W. ROSS. *Počítačové sítě*. Brno: Computer Press, 2014. ISBN 9788025138250.

[9] *NÚKIB: Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2018-05-16]. Dostupné z: https://www.govcert.cz/

[10] SINGLETON, Tommie. a Aaron J. SINGLETON. *Fraud auditing and forensic accounting*. 4th ed. Hoboken, N.J.: John Wiley, c2010. ISBN 978-0-470-56413-4.

[11] *ZoKB a související vyhlášky* [online]. In: . 2014 [cit. 2018-05-17]. Dostupné z: https://www.rac.cz/rac/homepage.nsf/CZ/vyhlasky316317

[12] MAURIC, Jakub. *IDS systém SNORT* [online]. České Budějovice, 2009 [cit. 2018-05-19]. Dostupné z: https://theses.cz/id/4lgemh/downloadPraceContent_adipIdno_12546. Bakalářská práce. JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH. Vedoucí práce Ing. Ladislav Beránek, CSc., MBA.

[13] Log Files. *Apache HTTP Server* [online]. [cit. 2018-05-19]. Dostupné z: https://httpd.apache.org/docs/1.3/logs.html

[14] Doporučení na minimální požadavky pro logy, které musí být zajištěny pro spolehlivou ex-post analýzu kybernetických bezpečnostních incidentů. *NÚKIB* [online]. 2016, 10. 08. 2016 [cit. 2018-05-19]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2485-doporuceni-na-minimalni-pozadavky-pro-logy-ktere-musi-byt-zajisteny-pro-spolehlivou-ex-post-analyzu-kybernetickych-bezpecnostnich-incidentu/

[15] KENT, Karen a Murugiah SOUPPAYA. Guide to Computer Security Log Management. In: *Guide to Computer Security Log Management: Recommendations of the National Institute of Standards and Technology* [online]. 2006, September 2006, s. 72 [cit. 2018-05-19]. Dostupné z: https://csrc.nist.gov/publications/detail/sp/800-92/final

[16] Effective Daily Log Monitoring. In: *Effective Daily Log Monitoring by PCI Security Standards Council* [online]. 2016, May 2016, s. 43 [cit. 2018-05-19]. Dostupné z: https://www.pcisecuritystandards.org/documents/Effective-Daily-Log-Monitoring-Guidance.pdf

[17] SNORT Users Manual 2.9.11. In: *Snort Setup Guides* [online]. August 31, 2017 [cit. 2018-05-20]. Dostupné z: https://www.snort.org/documents

[18] Regional Internet Registries. In: *American Registry for Internet Numbers* [online]. [cit. 2018-05-20]. Dostupné z: https://arin.net/knowledge/rirs.html

[19] WhatsMyIP: MAC Address Lookup. In: *WhatsMyIP* [online]. [cit. 2018-05-20]. Dostupné z: http://www.whatsmyip.org/mac-address-lookup/

[20] Whois.SmartWeb.CZ. In: *WhatsMyIP* [online]. [cit. 2018-05-20]. Dostupné z: https://whois.smartweb.cz/

[21] AbuseIPDP. In: *AbuseIPDP* [online]. [cit. 2018-05-20]. Dostupné z: https://www.abuseipdb.com/

[22] LILLARD, Terrence. *Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data*. Burlington, MA: Syngress, c2010. ISBN 978-1-59749-537-0.

# ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

| | |
|---|---|
| ARP | Sieťový protokol zisťujúci MAC adresy – Address Resolution Protocol |
| BER | Belkasoft Evidence Reader |
| CERT | Bezpečnostný tým – Computer Emergency Response Team |
| CLI | Príkazový riadok |
| CMD | Príkazový riadok |
| CSIRT | Bezpečnostný tým – Computer Security Incident Response Team |
| DDoS | Distribuovaný DoS |
| DHCP | Protokol dynamickej konfigurácie hosťov |
| DLP | Prevencia straty dát – Data Loss Prevention |
| DNS | Systém názvov domén – Domain Name System |
| DoS | Zamedzenie služby – Denial of Service |
| F2F | Typ P2P siete, priateľ-priateľ – Friend to Friend |
| FTP | Protokol prenosu súborov – File Transfer Protocol |
| GMT/UTC | Koordinovaný svetový čas |
| HASH | Hašovacia funkcia – kontrolný otlačok |
| HTTP | Hypertextový prenosový protokol |
| IANA | Autorita pre pridelovanie adries IP – Internet Assigned Numbers Authority |
| ICMP | Internet Control Message Protocol |
| ID | Identifikácia |
| IDS | Systém detekcie prieniku – Intrusion Detection System |
| IMAP | Internet Message Access Protocol |
| IP | Internet Protocol |
| IPS | Systém prevencie prieniku – Intrusion Prevention System |
| IT | Informačné technológie |

| | |
|---|---|
| IXP | Internetový bod výmeny dát |
| LAN | Miestna sieť – Local Address Network |
| MAC | Riadenie prístupu k médiu – Media Access Control |
| MD5 | Hašovací algoritmus 128 bitov – Message-Digest algorithm |
| NAT | Preklad sieťových adries – Network Address Translation |
| OS | Operačný systém |
| OSPF | Smerovací protokol – Open shortest Path First |
| P2P | Typ počítačovej siete klient-klient – Peer to Peer |
| POP3 | Post Office Protocol 3 |
| PSAD | Detektor útoku skenovania portov – Port Scan Attack Detector |
| RAM | Pamäť s priamym prístupom – Random Access Memory |
| RIP | Routing Information Protocol |
| RIR | Regionálni internetoví registrátori |
| SHA1 | Hašovací algoritmus 160 bitov – Secure Hash Algorithm |
| SMTP | Jednoduchý protokol na prenos pošty – Simple Mail Transfer Protocol |
| SNMP | Jednoduchý manažérsky protokol siete – Simple Network Management P. |
| SSH | Secure shell |
| SSL | Secure Sockets Layer |
| SW | Software |
| TCP | Protokol riadenia prenosu – Transmission Control Protocol |
| TLS | Transport Layer Security |
| Tor | Cibuľový smerovač – The Onion Router – Tor sieť |
| UDP | Používateľský datagramový protokol – User Datagram Protocol |
| VM | Virtuálne zariadenia – Virtuál Machine |
| VPN | Súkromná virtuálna sieť – Virtual Private Network |
| WAN | Rozľahlá sieť – Wide Area Network |

# ZOZNAM OBRÁZKOV

# ZOZNAM TABULIEK