

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií



Diplomová práce

Možnosti zabezpečení počítačových sítí

Bc. Ladislav Nepomucký

© 2024 ČZU v Praze

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Ladislav Nepomucký

Informatika

Název práce

Možnosti zabezpečení počítačových sítí

Název anglicky

Security options for computer networks

Cíle práce

Cílem práce je zpracování problematiky zabezpečení počítačových sítí se zaměřením na vybrané kybernetické útoky a obranou před nimi.

Díličími cíli je

- přehled a analýza jednotlivých útoků
- výběr vhodných postupů k jejich prevenci
- provedení testovacích útoků a implementace ochrany
- diskuse, formulace závěrů a doporučení.

Metodika

Teoretická část práce je založena na studiu a analýze odborných a vědeckých informačních zdrojů. Obsahuje přehled a analýzu vybraných kybernetických útoků a nástrojů k jejich provedení. Důraz je kladen na typické problémové situace.

Následně jsou navrženy postupy k odvrácení útoků či prevenci.

V praktické části jsou vybrané útoky provedeny na modelových příkladech s využitím zařízení různých výrobců.

K obraně proti těmto útokům jsou navrženy konfigurace síťových prvků.

Na základě syntézy poznatků teoretické části a vyhodnocení výsledků praktické části budou formulovány závěry práce a doporučení.

Doporučený rozsah práce

60 – 70 stran

Klíčová slova

počítačové sítě, bezpečnost, útok, zabezpečení, kybernetický útok

Doporučené zdroje informací

MCNAB, Chris. Network security assessment. Second Edition. Cambridge: O'Reilly, 2007. ISBN 0-596-51030-6.

OCCUPYTHEWEB. Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali. San Francisco: No Starch Press, 2018. ISBN 978-1593278557.

PENGELLY, James. The Official CompTIA Security+ Student Guide: Exam SY0-601 [online]. Illinois: CompTIA, c2020. ISBN 978-1-64274-328-9. Dostupné také z: learn.comptia.org

SAPP, S Arthur. Infinity Ethical Hacking: Learn basic to advance hacks. c2020. ISBN 979-8662888128.

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

doc. Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 25. 6. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 31. 03. 2024

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Možnosti zabezpečení počítačových sítí" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31.3.2024

Poděkování

Rád bych touto cestou poděkoval panu doc. Ing. Jiřímu Vaňkovi, Ph.D. za jeho pomoc, rady a postřehy během vypracování této diplomové práce. Poděkování také patří Petru Procházkovi, Lukáši Hájkovi a dalším kolegům ze Střední průmyslové školy na Proseku za cenné rady a poskytnuté vybavení. Děkuji rovněž své rodině za podporu při psaní.

Možnosti zabezpečení počítačových sítí

Abstrakt

Diplomová práce se zabývá kybernetickou bezpečností s důrazem na identifikaci a obranu proti specifickým kybernetickým útokům. V teoretické části práce je prozkoumána motivace a techniky útočníků a jsou představeny obranné strategie a nástroje pro ochranu počítačových sítí. V praktické části byl realizován útočný scénář v nezabezpečené infrastruktuře, kde byly demonstrativně použity různé útočné techniky, odhalující slabá místa v zabezpečení. Pro obranu byly navrženy a testovány konfigurace na zařízeních Cisco a Mikrotik, doplněné o využití systému pro detekci průniků Security Onion. Práce poskytuje srovnání implementace bezpečnostních opatření mezi oběma typy zařízení a demonstruje účinnost různých obranných mechanismů. Výsledky této práce mohou sloužit jako vzdělávací materiál pro studenty a jako praktický průvodce pro správce sítí, zaměřený na posílení bezpečnostních postupů v síťové infrastruktuře.

Klíčová slova: počítačové sítě, bezpečnost, útok, zabezpečení, kybernetický útok

Security options for computer networks

Abstract

The thesis deals with cyber security with emphasis on identification and defense against specific cyber attacks. The theoretical part of the thesis explores the motivations and techniques of attackers and presents defensive strategies and tools for protecting computer networks. In the practical part, an attack scenario was implemented in an insecure infrastructure, where different attack techniques were demonstrated, revealing security weaknesses. For defense, configurations on Cisco and Mikrotik devices were designed and tested, complemented by the use of the Security Onion intrusion detection system. The paper provides a comparison of the security implementation between the two types of devices and demonstrates the effectiveness of the different defense mechanisms. The results of this work can serve as educational material for students and as a practical guide for network administrators, aimed at strengthening security practices in network infrastructure.

Keywords: computer networks, security, attack, security procedures, cyber attack

Obsah

1 Úvod.....	10
2 Cíl práce a metodika	11
2.1 Cíl práce	11
2.2 Metodika	11
3 Teoretická východiska	12
3.1 Útoky a útočníci	12
3.2 Motivace útočníků.....	14
3.3 Nástroje útočníků	15
3.3.1 Kali Linux	15
3.3.2 Parrot Security	18
3.4 Postupy a útoky	19
3.4.1 Analýza síťové komunikace	19
3.4.2 Skenování sítě	24
3.4.3 Útoky na heslo	28
3.4.4 Social engineering.....	30
3.4.5 Keylogging.....	32
3.4.6 Útoky na zařízení a služby.....	32
3.5 Bezpečnostní postupy a nástroje	35
3.5.1 Fyzické zabezpečení	35
3.5.2 Bezpečnost hesel.....	36
3.5.3 Řízení přístupu.....	37
3.5.4 Aktualizace softwaru	37
3.5.5 Firewall	38
3.5.6 Access Control Lists	39
3.5.7 Port Security	41
3.5.8 Honeypot.....	41
3.5.9 Systémy odhalení a prevence průniku	42
4 Vlastní práce	46

4.1	Přístup do sítě.....	46
4.1.1	Obrana.....	46
4.2	Skenování sítě	53
4.2.1	Obrana.....	54
4.3	Útok na heslo přes protokol SSH.....	57
4.3.1	Ochrana Linux serveru.....	59
4.3.2	Ochrana routeru Mikrotik	61
4.3.3	Ochrana L3 přepínače Cisco.....	62
4.4	Parazitní DHCP server	64
4.4.1	Obrana.....	64
4.5	Neighbor discovery Attack	68
4.5.1	Obrana.....	72
4.6	Nasazení IDS řešení Security Onion.....	75
5	Výsledky a diskuse	78
5.1	Kybernetické útoky	78
5.2	Mechanismy obrany	78
	Závěr	80
6	Seznam použitých zdrojů	81
6.1	Seznam obrázků	89
	Přílohy.....	91

Příloha A – Skript pro generování pravidel filtrování MAC adres na porty pro RouterOS

1 Úvod

Počítačové sítě jsou podstatnou součástí fungování dnešního světa. Obsahují obrovské množství důležitých informací, které je třeba nejen úspěšně přenést, ale také chránit před zneužitím. Kvůli neustálému vývoji je nutné vyvíjet opatření a způsoby ochrany před kybernetickými útočníky.

Historie zabezpečení počítačových sítí sahá až do doby samotného vzniku počítačových sítí. V počátcích, kdy sloužily k vojenským a akademickým účelům, stačila bezpečnostní opatření na úrovni fyzického zabezpečení a jednoduché řízení přístupu, kdo může zařízení obsluhovat. S expanzí internetu a možností jeho využívání běžnými uživateli však bylo třeba rychle aplikovat komplexnější bezpečnostní mechanismy.

V současnosti je zabezpečení počítačových sítí komplexní problematika, která zahrnuje množství technologií, postupů a způsobů, jak k ní přistupovat. Základním stavebním kamenem je šifrování dat, filtrování komunikace, implementace systémů pro detekci útoků podle chování a přenesených dat, řízení přístupů a v neposlední řadě zabezpečení koncových stanic.

Výrobci síťových prvků přistupují k implementaci bezpečnosti s velkou vážností, jelikož zabezpečení síťové infrastruktury je klíčové pro ochranu dat a zajištění kontinuity podnikání. Bezpečnostní opatření jsou integrována na různých úrovních síťového designu a provozu, od hardwaru po software a od fyzické až po logickou bezpečnost.

Při chápání hrozeb nestačí řešit, co hrozí. Důležité je také znát následky jednotlivých bezpečnostních hrozeb. Například v případě narušení dostupnosti webového serveru je třeba vědět, jaké to bude mít dopady, jak to ovlivní zaměstnance a zákazníky a kolik bude stát náprava. S tím souvisí i četnost takové hrozby.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je zpracování problematiky zabezpečení počítačových sítí se zaměřením na vybrané kybernetické útoky a obranou před nimi. Dílčími cíli je přehled a analýza jednotlivých útoků, výběr vhodných postupů k jejich prevenci, provedení testovacích útoků a implementace ochrany, diskuse, formulace závěrů a doporučení.

2.2 Metodika

Teoretická část práce je založena na studiu a analýze odborných a vědeckých informačních zdrojů. Obsahuje přehled a analýzu vybraných kybernetických útoků a nástrojů k jejich provedení. Důraz je kladen na typické problémové situace.

Následně jsou navrženy postupy k odvrácení útoků či prevenci.

V praktické části jsou vybrané útoky provedeny na modelových příkladech s využitím zařízení různých výrobců.

K obraně proti těmto útokům jsou navrženy konfigurace síťových prvků.

Na základě syntézy poznatků teoretické části a vyhodnocení výsledků praktické části budou formulovány závěry práce a doporučení.

3 Teoretická východiska

Téma kybernetické bezpečnosti je aktuální a týká se všech – firem, státních organizací, nemocnic, škol i jednotlivců. Uživatelé sociálních sítí se pravidelně setkávají s pokusy o prolomení jejich účtů. Servery přístupné z internetu jsou útočníky pravidelně skenovány a napadány. Obětí může být kdokoliv. Proto je důležité být připraven těmto útokům odolat.

3.1 Útoky a útočníci

Díky nástrojům a návodům dostupným na internetu je možnost stát se hackerem dostupná komukoliv. Není třeba umět programovat, chápat fungování operačních systémů nebo počítačových sítí. Průměrný uživatel počítače se tak snadno může stát kybernetickým útočníkem. Zároveň však riskuje snadné odhalení, protože se nedokáže správně maskovat. Automatizované nástroje stačí spustit a bez další útočnickovy interakce naleznou slabiny v cílovém systému, které poté zneužijí. Takoví amatéři, kteří se v oblasti kybernetické bezpečnosti neorientují a používají jen metody nalezené na internetu, se nejčastěji označují jako *Script Kiddies*. Ti si častokrát ani neuvědomují následky svých činů. [1]

Ne všechny hackerské aktivity však mají špatný záměr. Etičtí hackeři naopak pracují na ochraně počítačových sítí a systémů v nich. Jejich cílem je objevit všechny zranitelnosti dříve, než to udělá někdo jiný. Operují v mezích zákona a při provádění útoků spolupracují s firmami, pro které vyhodnocují bezpečnostní rizika. Na základě toho navrhují nebo i implementují ochranné mechanismy. Označují se také jako *white hat* hackeři. [2] [85]

Opakem etického hackera je takzvaný *black hat* hacker. Ten napadá cizí systémy a praktikuje nelegální aktivity. Škodí v cizích systémech, zneužívá zranitelnosti, narušuje fungování počítačových sítí nebo krade data. Takový hacker může operovat jako jednotlivec nebo v organizované skupině. [2] [85]

Grey hat hackeři se pohybují na pomezí etického a *black hat* hackingu. Operují bez povolení správce systému a provádí testy bez předchozí spolupráce. Zároveň ale nemají nekalé úmysly, nezneužívají odhalené zranitelnosti a hlásí je správcům. I přesto je takové jednání považováno za protiprávní. [2] [85]

Všechny známé zranitelnosti se zapisují do veřejného katalogu *Common Vulnerabilities and Exposures* (CVE). Každý záznam má vlastní unikátní identifikátor (CVE ID) a popis, který obsahuje všechny důležité informace o zranitelnosti a který odkazuje na konkrétní relevantní zdroje. [3]

Vulnerability Details : CVE-2024-20338

A vulnerability in the ISE Posture (System Scan) module of Cisco Secure Client for Linux could allow an authenticated, local attacker to elevate privileges on an affected device.

This vulnerability is due to the use of an uncontrolled search path element. An attacker could exploit this vulnerability by copying a malicious library file to a specific directory in the filesystem and persuading an administrator to restart a specific process. A successful exploit could allow the attacker to execute arbitrary code on an affected device with root privileges.

Published 2024-03-06 17:15:10 Updated 2024-03-07 13:52:27 Source [Cisco Systems, Inc.](#) View at [NVD](#), [CVE.org](#)

Vulnerability category: [Execute code](#)

Exploit prediction scoring system (EPSS) score for CVE-2024-20338

Probability of exploitation activity in the next 30 days: 0.04%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 7% [EPSS Score History](#) [EPSS FAQ](#)

CVSS scores for CVE-2024-20338

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
7.3	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H	N/A	N/A	Cisco:cisco-sa-secure-privesc-sYxQ06ds
7.3	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H	1.3	5.9	Cisco Systems, Inc.

CWE ids for CVE-2024-20338

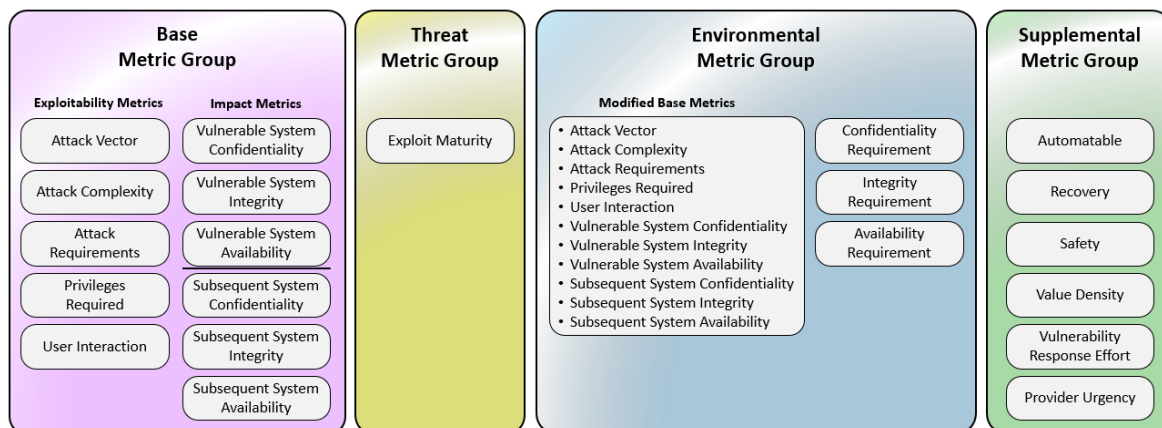
[CWE-427 Uncontrolled Search Path Element](#)
The product uses a fixed or controlled search path to find resources, but one or more locations in that path can be under the control of unintended actors.
Assigned by: ykramarz@cisco.com (Secondary)

References for CVE-2024-20338

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-privesc-sYxQ06ds>
Cisco Secure Client for Linux with ISE Posture Module Privilege Escalation Vulnerability

Obrázek 1 – Ukázka CVE záznamu Zdroj: [4]

Pomocí systému skórování (CVSS) je každá zranitelnost bodově hodnocena na základě její závažnosti. Aktuální verzi skórovacího systému je CVSS 4.0 a obsahuje komplexnější metriku pro relevantnější výsledky oproti předešlé verzi. Zahrnuje složitost zneužití zranitelnosti, dopady na systém, složitost opravy, využitelnost ve skutečném prostředí a další kritéria. Výsledkem je hodnota od 0 do 10, přičemž čím vyšší skóre je, tím závažnější je zranitelnosti. Konkrétní zkoumané parametry jsou vidět na obrázku 2. [5]



Obrázek 2 – Skórovací systém CVSS 4.0 Zdroj: [5]

3.2 Motivace útočníků

Motivace útočníků mohou být různé a mění se v závislosti na konkrétních jedincích nebo skupinách. Některé z hlavních motivací mohou zahrnovat:

Testování

Někteří hackeři cílí na počítačové sítě a systémy, aby upozornili na jejich slabiny. Jedná se o příklady *white hat* a *gray hat* hackingu.

Finanční zisk

Útoky prováděné za účelem získání vlastního zisku cílí většinou na platební či osobní údaje, následné vydírání nebo krádeže kryptoměn.

Konkurence a špionáž

Vidina získání výhody na trhu může útočníky motivovat ke krádeži obchodních tajemství konkurence.

Touha někoho poškodit

Cílem útočníka nemusí být jen něco získat, někteří chtějí jen někoho poškodit. Oběť může být předem vybrána, ale může být i náhodná.

Zábava nebo výzva

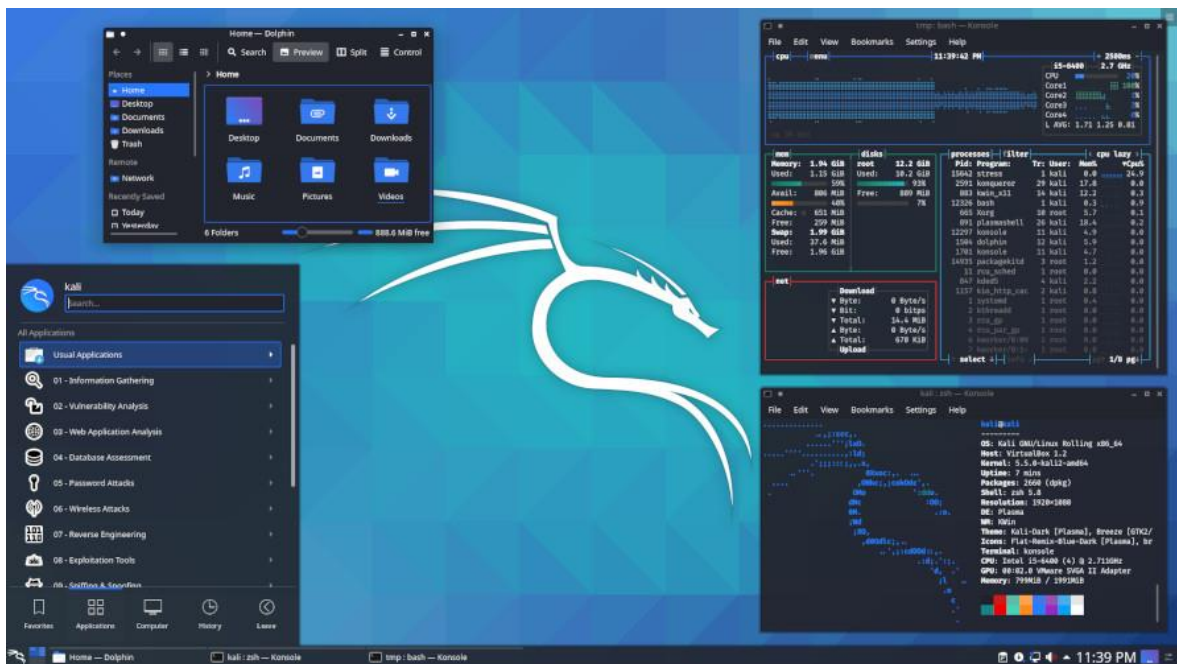
Někteří hackeři útočí ze zvědavosti. I když jejich úmysly nemusí být špatné, jejich aktivita může mít negativní následky.

3.3 Nástroje útočníků

Hackeři nejsou odkázáni na vlastní znalosti a nemusí malware a penetrační nástroje sami vyvíjet. Existuje celá řada dostupných aplikací obsahující vše potřebné pro provádění různých útoků. Tyto nástroje jsou určeny pro použití *white hat* hackery na vlastních systémech a sítích, ale mohou být úplně stejně využity i při nelegálních aktivitách. Jsou dostupné a jejich použití může být tak jednoduché, že se útočníkem může stát úplně běžný uživatel počítače.

3.3.1 Kali Linux

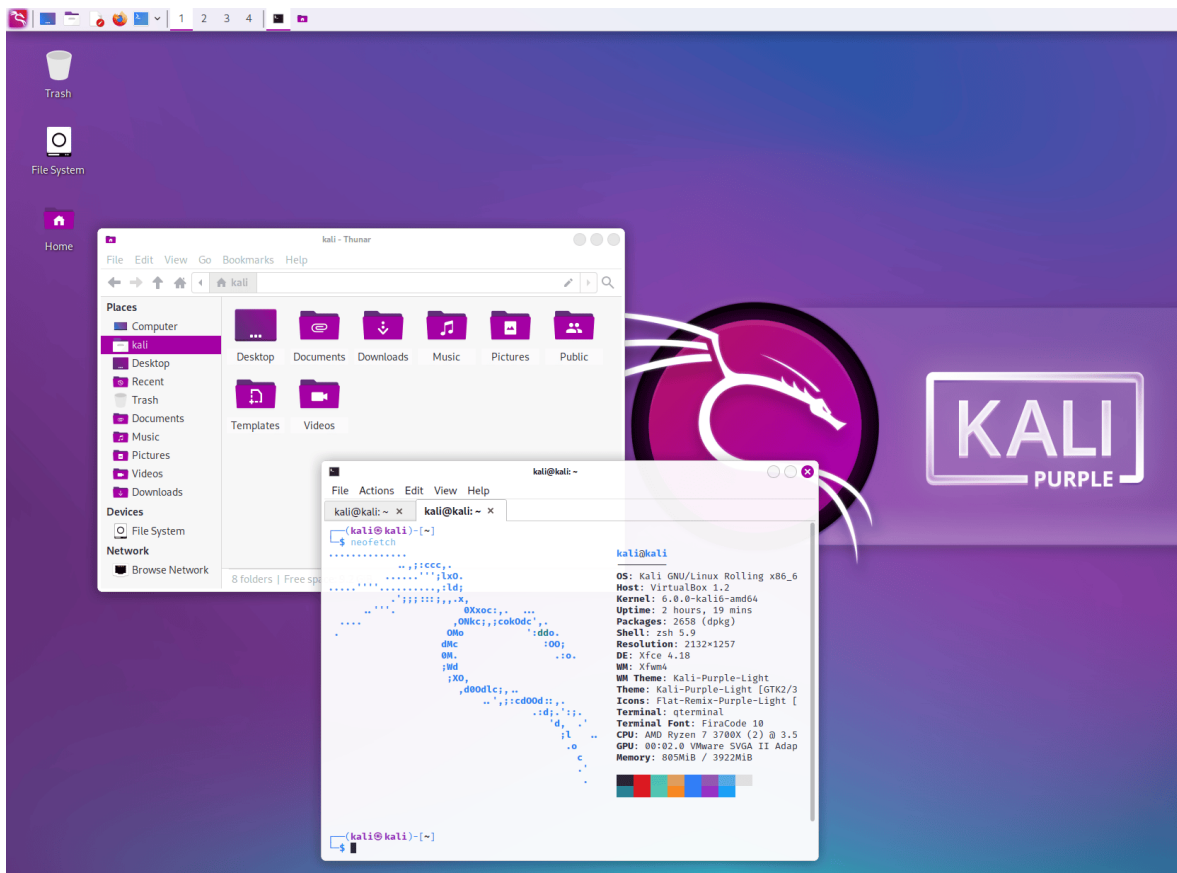
Kali Linux, původně známý jako BackTrack Linux, je specializovaný operační systém založený na distribuci Debian. Zaměřuje se na potřeby penetračního testování a bezpečnostní analýzy. S více než 600 předinstalovanými nástroji pro kybernetickou bezpečnost nabízí uživatelům komplexní prostředí pro testování zranitelností a průniků do počítačových sítí, digitální forenzní analýzu a další bezpečnostní úkoly. Bezplatnost a otevřený zdrojový kód poskytují uživatelům plnou kontrolu a možnost přizpůsobení systému dle svých potřeb. S flexibilitou, rozsáhlou podporou bezdrátových zařízení a schopností pracovat na zařízeních s architekturou ARM poskytuje Kali Linux komplexní a výkonné prostředí pro profesionály v oblasti kybernetické bezpečnosti, což je klíčovým prvkem pro úspěšné provádění etického hackingu a penetračních testů. [6] [7]



Obrázek 3 – Rozhraní Kali Linux Zdroj: [7]

Kali Purple

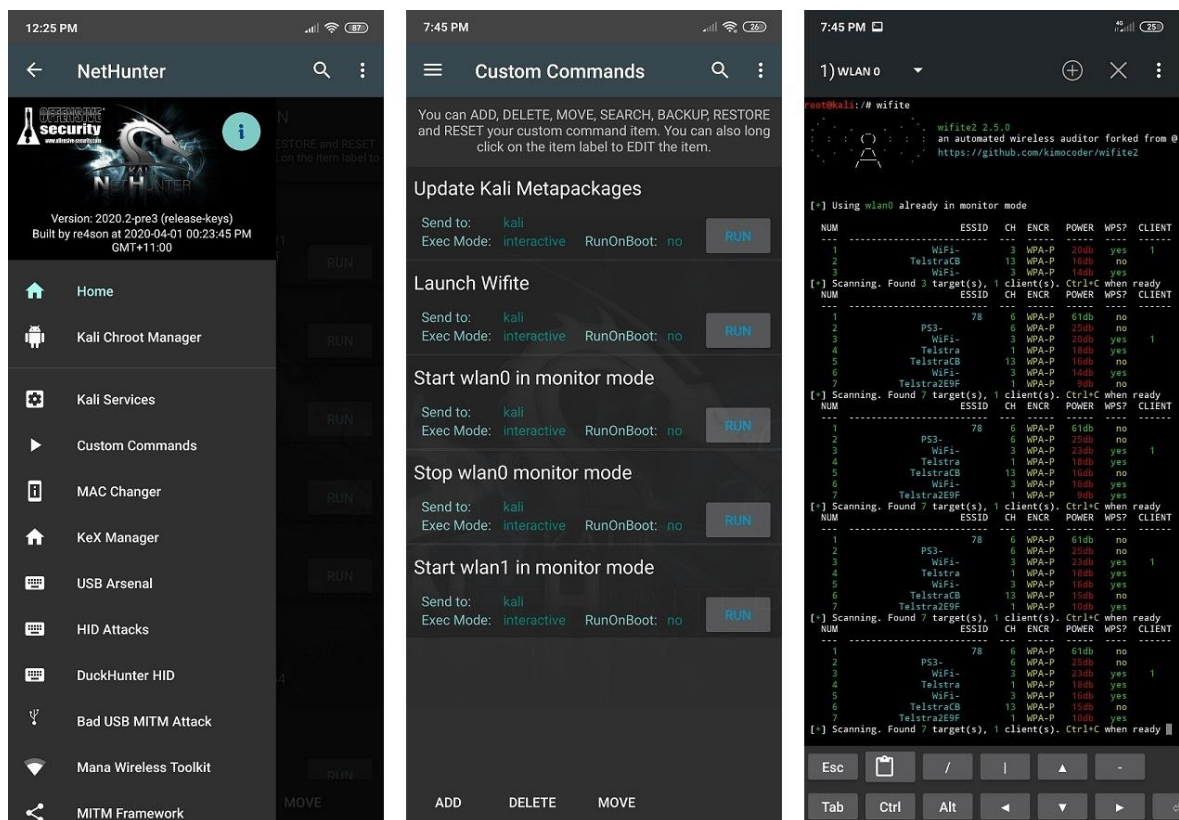
Distribuce Kali Purple, představená v první polovině roku 2023, se zaměřuje na obranu před kybernetickými útoky. Obsahuje více než 100 defenzivních nástrojů – například *Arkime* pro zachytávání paketů, *CyberChef* pro šifrování, *Elasticsearch* SIEM, *GVM* skener zranitelností, IDS *Suricata* a *Zeek* a mnoho dalších. Tento inovativní design integruje rozmanitou sadu komponent bezpečnostního operačního centra (SOC) do modulární propojené platformy. Nabízí efektivní, centralizované řešení pro správu bezpečnostních operací a odezvy na incidenty. [8]



Obrázek 4 – Rozhraní Kali Purple Zdroj: [9]

Kali NetHunter

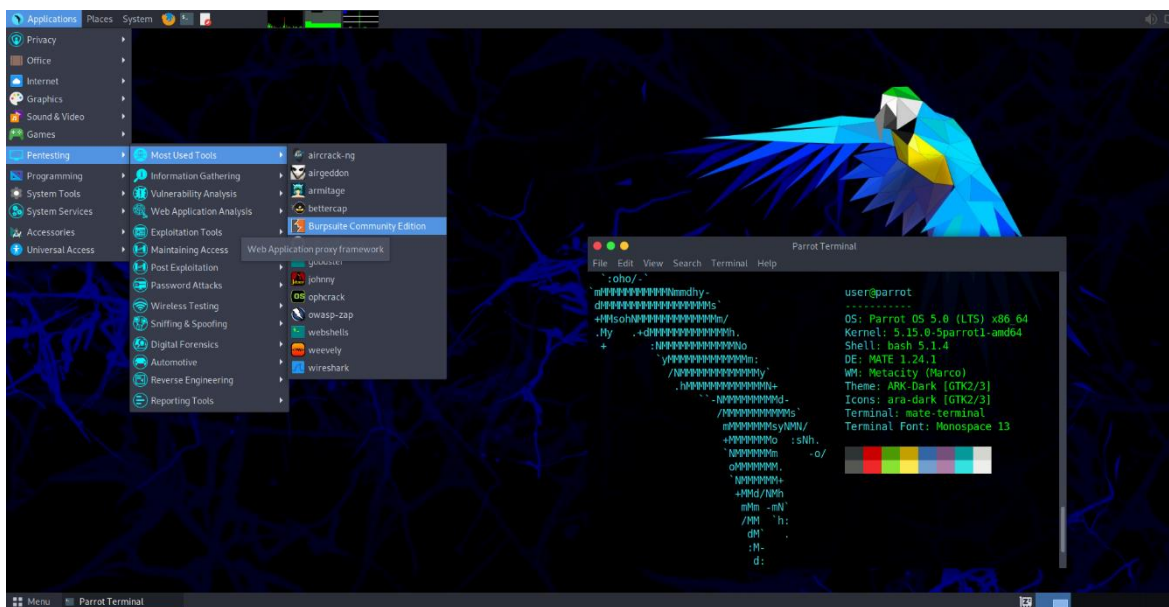
Kali NetHunter je oficiální mobilní verze Kali Linuxu. Je dostupná ve třech variantách. První verze je určena pro mobilní telefony bez modifikace původního systému, druhá pro systémy s vyšším oprávněním (root) bez upraveného kernelu a třetí verze obsahuje vlastní kernel. Jednotlivé varianty se liší ve funkcích, které podporují. Mezi ně patří nástroje pro penetrační testování (*Metasploit Framework*, *SQLMap*), pro průzkum sítí (*Nmap*, *Wireshark*) a pro útoky na bezdrátové sítě (*Fluxion*, *Aircrack-ng*). Právě pro provádění útoků na WiFi sítě je však nutná nejvyšší verze, která je ale dostupná jen pro vybraná podporovaná zařízení. [10] [11]



Obrázek 5 – Rozhraní Kali NetHunter Zdroj: [11]

3.3.2 Parrot Security

Parrot OS ve verzi security je, stejně jako Kali Linux, operační systém založený na distribuci Debian. Stejně jako Kali Linux se zaměřuje na potřeby penetračního testování a bezpečnostní analýzy. Nezaostává ani v množství nástrojů, také obsahuje více než 600 předinstalovaných nástrojů. Tato sada má podobný základ, ale navíc obsahuje aplikace, které napomáhají anonymitě při prohlížení internetu. [12] [13]



Obrázek 6 – Rozhraní Parrot Security Zdroj: [14]

3.4 Postupy a útoky

Útočníci mají k dispozici celou řadu postupů a nástrojů, které mohou ve vybraných situacích využívat. Liší se v podmínkách, které pro útoky potřebují, v oprávněních, v přístupech, v potřebných znalostech a hardwaru. Různé jsou i následky takových akcí.

3.4.1 Analýza síťové komunikace

Už samotné připojení do počítačové sítě umožní klientovi nahlížet do komunikace ostatních zařízení. Šifrovaná komunikace znemožňuje čtení obsahu zpráv, ale i z hlavičky je možné vytěžit určitá data, jako například zdrojové a cílové adresy nebo o jaký protokol se jedná. Naopak protokoly, které nepoužívají šifrování, umožňují čtení obsahu zpráv i ostatním zařízením v síti. Tyto informace mohou být užitečné pro administrátory při hledání problémů, ale mohou být zneužity potencionálními útočníky, kterým stačí jen přístup do sítě. Takovéto pasivní sledování nevyžaduje žádné vysílání, takže není snadno detekovatelné. [84]

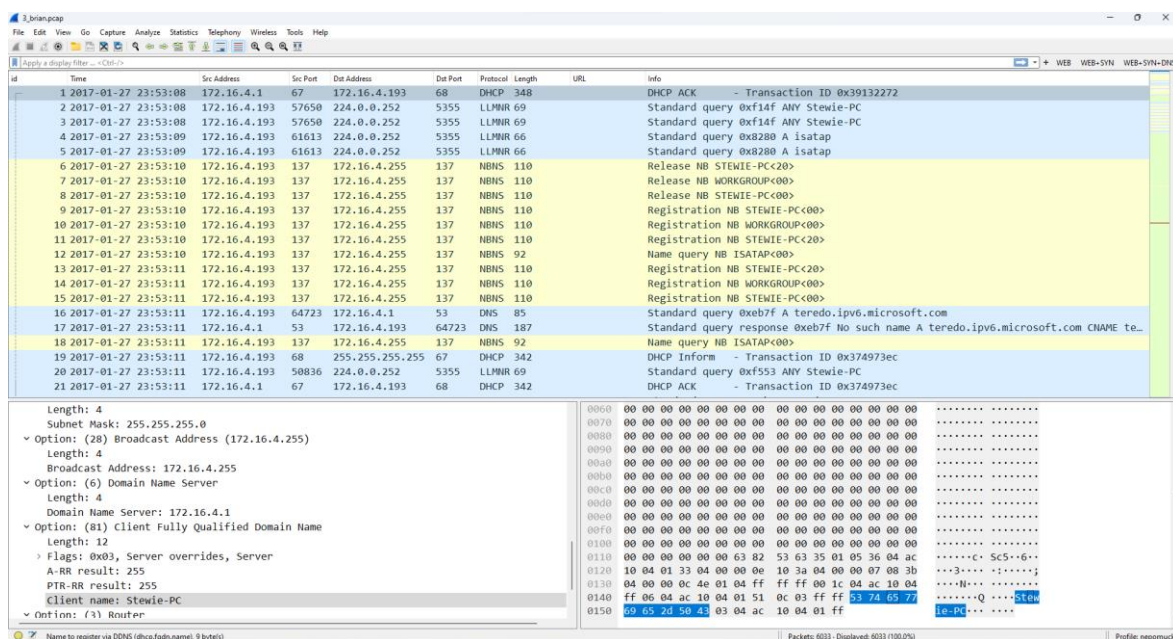
I proto je důležitým postupem při zabezpečování počítačové sítě ověřování připojených zařízení a povolování pouze známých a bezpečných koncových stanic. Veřejnou síť je vhodné oddělovat od interní sítě s klíčovou infrastrukturou, jako jsou

servery. Toho je možné docílit například používáním virtuálních sítí VLAN a správným nastavením firewallu.

Na základě zkoumání síťové komunikace fungují systémy pro detekci a prevenci průniků, které jsou podstatným prvkem síťové bezpečnosti. Tyto systémy jsou blíže popsány v kapitole 3.5.9.

Wireshark

Jedním z nejrozšířenějších programů pro analýzu síťové komunikace je Wireshark. Umožňuje sledovat pakety ze síťových karet včetně těch bezdrátových. Zobrazuje data v reálném čase a umožňuje uložení přenosů pro následnou offline analýzu. Využití filtrů usnadňuje vyhledávání i ve velkém množství paketů. Grafické rozhraní, které lze přizpůsobit dle preferencí uživatele, dělá z programu přehledný a intuitivní nástroj.



Obrázek 7 – Rozhraní programu Wireshark Zdroj: [vlastní zpracování]

Pokročilé funkce jako sledování TCP toků umožňuje zobrazení celého toku komunikace mezi dvěma zařízeními. To se hodí například při diagnostice problémů s připojením nebo analýze síťové komunikace po bezpečnostním incidentu. [15] [16]

Přenesená data je možné zkoumat na různých vrstvách síťového modelu. A to i na těch vyšších, což umožňuje uživatelům vidět obsah komunikace na protokolech jako HTTP, FTP, DNS a dalších. Takové informace může využít administrátor při identifikaci

problémů, ale i útočník s cílem získaná data zneužít například pro průnik do interních systémů. [15] [16]

Wireshark rovněž poskytuje řadu statistických výstupů, které umožňují uživatelům získat přehled o charakteristikách síťového provozu. Vlastnosti prohlíženého souboru obsahují informace o souboru samotném, době sběru dat, sledovaných portech a základní statistiky jako počet paketů, jejich velikosti, rychlosti a průměry těchto hodnot. Hierarchie protokolů umožňuje zkoumání statistických dat na úrovni konkrétních protokolů. Konverzace zobrazují údaje o přenesených datech mezi jednotlivými uzly, kdy je výsledky možné opět filtrovat dle vrstev a používaných protokolů. [17]

Grafické rozhraní nabízí vysokou míru přizpůsobení pro lepší čitelnost a zobrazování potřebných relevantních dat dle specifických potřeb. Uživatelé si mohou změnit barvy a styl rozhraní i jednotlivých řádků podle definovaných pravidel pro snadnější orientaci ve velkém množství dat. Sloupce se zobrazovanými informacemi je možné libovolně přidávat, odebírat nebo jen dočasně skrývat a zobrazovat. Mimo předdefinovaných hodnot je možné přidat i vlastní cesty k datům ve struktuře paketů, což ušetří čas při hledání potřebných informací ze síťové komunikace. Filtry a jejich kombinace usnadňují vyhledávání paketů nebo specifických typů provozu. Pro rychlou aplikaci často používaných filtrů je možné jejich přidání do rozhraní formou tlačítka.

TShark

Nástroj TShark je příkazová verze síťového analyzátoru Wireshark. Spouští se v příkazové řádce a najde tak uplatnění v systémech, kde chybí grafické rozhraní. Stejně jako jeho grafická varianta umožňuje uživatelům zachytávat síťový provoz na jednom nebo více rozhraních a procházet soubory s dříve zachycenou komunikací.


```
asf@ass1-nepomucky-alma:~$ tshark -r Downloads/3_brian.pcap
1 0.000000 172.16.4.1 → 172.16.4.193 DHCP 348 DHCP ACK - Transaction ID 0x39132272
2 0.008974 172.16.4.193 → 224.0.0.252 LLNMR 69 Standard query 0xf14f ANY Stewie-PC
3 0.107795 172.16.4.193 → 224.0.0.252 LLNMR 69 Standard query 0xf14f ANY Stewie-PC
4 1.528070 172.16.4.193 → 224.0.0.252 LLNMR 66 Standard query 0x8280 A isatap
5 1.636618 172.16.4.193 → 224.0.0.252 LLNMR 66 Standard query 0x8280 A isatap
6 2.060191 172.16.4.193 → 172.16.4.255 NBNS 110 Release NB STEWIE-PC<20>
7 2.060388 172.16.4.193 → 172.16.4.255 NBNS 110 Release NB WORKGROUP<00>
8 2.060396 172.16.4.193 → 172.16.4.255 NBNS 110 Release NB STEWIE-PC<00>
9 2.136179 172.16.4.193 → 172.16.4.255 NBNS 110 Registration NB STEWIE-PC<00>
10 2.136377 172.16.4.193 → 172.16.4.255 NBNS 110 Registration NB WORKGROUP<00>
11 2.136383 172.16.4.193 → 172.16.4.255 NBNS 110 Registration NB STEWIE-PC<20>
12 2.603784 172.16.4.193 → 172.16.4.255 NBNS 92 Name query NB ISATAP<00>
13 2.900156 172.16.4.193 → 172.16.4.255 NBNS 110 Registration NB STEWIE-PC<20>
14 2.900175 172.16.4.193 → 172.16.4.255 NBNS 110 Registration NB WORKGROUP<00>
15 2.900180 172.16.4.193 → 172.16.4.255 NBNS 110 Registration NB STEWIE-PC<00>
16 3.060350 172.16.4.193 → 172.16.4.1 DNS 85 Standard query 0xeb7f A teredo.ipv6.microsoft.com
17 3.250308 172.16.4.1 → 172.16.4.193 DNS 187 Standard query response 0xeb7f No such name A teredo.ipv6.microsoft.com CNAME teredo.ipv6.microsoft.com.nsatsc.net SOA admin.nsatsc.net
18 3.368166 172.16.4.193 → 172.16.4.255 NBNS 92 Name query NB ISATAP<00>
19 3.419891 172.16.4.193 → 255.255.255.255 DHCP 342 DHCP Inform - Transaction ID 0x374973ec
20 3.419917 172.16.4.193 → 224.0.0.252 LLNMR 69 Standard query 0xf553 ANY Stewie-PC
21 3.420105 172.16.4.1 → 172.16.4.193 DHCP 342 DHCP ACK - Transaction ID 0x374973ec
22 3.423435 172.16.4.193 → 224.0.0.252 LLNMR 64 Standard query 0x41b6 A wpad
23 3.524231 172.16.4.193 → 224.0.0.252 LLNMR 64 Standard query 0x41b6 A wpad
24 3.524418 172.16.4.193 → 224.0.0.252 LLNMR 69 Standard query 0xf553 ANY Stewie-PC
25 3.664572 172.16.4.193 → 172.16.4.255 NBNS 110 Registration NB STEWIE-PC<00>
26 3.664591 172.16.4.193 → 172.16.4.255 NBNS 110 Registration NB WORKGROUP<00>
27 3.664596 172.16.4.193 → 172.16.4.255 NBNS 110 Registration NB STEWIE-PC<20>
28 3.727235 172.16.4.193 → 172.16.4.255 NBNS 92 Name query NB WPAD<00>
29 4.133497 172.16.4.193 → 224.0.0.252 LLNMR 66 Standard query 0xf4fd A isatap
30 4.241846 172.16.4.193 → 224.0.0.252 LLNMR 66 Standard query 0xf4fd A isatap
31 4.429000 172.16.4.193 → 172.16.4.255 NBNS 110 Registration NB STEWIE-PC<20>
32 4.429021 172.16.4.193 → 172.16.4.255 NBNS 110 Registration NB WORKGROUP<00>
```

Obrázek 8 – TShark Zdroj: [vlastní zpracování]

K pokročilé inspekci paketů je možné použít přepínače a filtry, díky kterým je možné využívat funkce Wiresharku i bez GUI. V případě potřeby je možné data uložit do souboru a později analyzovat v grafické verzi, která může být pro běžné uživatele přívětivější. [18]

Tcpdump

Tcpdump je nástroj fungující na principu zachytávání paketů procházející síťovým rozhraním. Využívá příkazovou řádku, a tak je používán zejména v linuxových systémech. Díky tomu se hodí například na serverech, které nemají grafické uživatelské rozhraní.

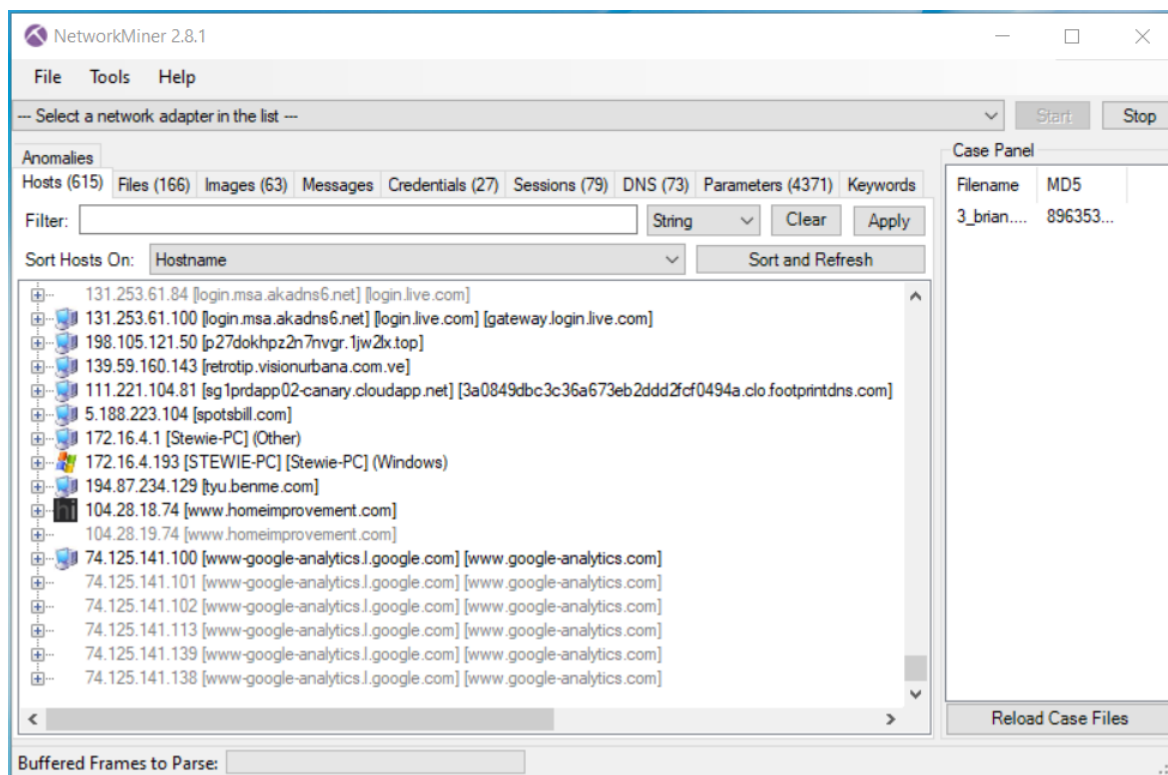
```
asd@ass1-nepomucky-alma:~$ sudo tcpdump -r Downloads/3_brian.pcap
reading from file Downloads/3_brian.pcap, link-type EN10MB (Ethernet), snapshot length 65535
dropped privs to tcpdump
23:53:08.210137 IP 172.16.4.1.bootpc > 172.16.4.193.bootpc: BOOTP/DHCP, Reply, length 306
23:53:08.219111 IP 172.16.4.193.57650 > 224.0.0.252.hostmon: UDP, length 27
23:53:08.317932 IP 172.16.4.193.57650 > 224.0.0.252.hostmon: UDP, length 27
23:53:09.738207 IP 172.16.4.193.61613 > 224.0.0.252.hostmon: UDP, length 24
23:53:09.846755 IP 172.16.4.193.61613 > 224.0.0.252.hostmon: UDP, length 24
23:53:10.270328 IP 172.16.4.193.netbios-ns > 172.16.4.255.netbios-ns: UDP, length 68
23:53:10.270525 IP 172.16.4.193.netbios-ns > 172.16.4.255.netbios-ns: UDP, length 68
23:53:10.270533 IP 172.16.4.193.netbios-ns > 172.16.4.255.netbios-ns: UDP, length 68
23:53:10.346316 IP 172.16.4.193.netbios-ns > 172.16.4.255.netbios-ns: UDP, length 68
23:53:10.346514 IP 172.16.4.193.netbios-ns > 172.16.4.255.netbios-ns: UDP, length 68
23:53:10.346520 IP 172.16.4.193.netbios-ns > 172.16.4.255.netbios-ns: UDP, length 68
23:53:10.813921 IP 172.16.4.193.netbios-ns > 172.16.4.255.netbios-ns: UDP, length 50
23:53:11.110293 IP 172.16.4.193.netbios-ns > 172.16.4.255.netbios-ns: UDP, length 68
23:53:11.110312 IP 172.16.4.193.netbios-ns > 172.16.4.255.netbios-ns: UDP, length 68
23:53:11.110317 IP 172.16.4.193.netbios-ns > 172.16.4.255.netbios-ns: UDP, length 68
23:53:11.270487 IP 172.16.4.193.64723 > 172.16.4.1.domain: 60287+ A? teredo.ipv6.microsoft.com. (43)
23:53:11.460445 IP 172.16.4.1.domain > 172.16.4.193.64723: 60287 NXDomain 1/1/0 CNAME teredo.ipv6.microsoft.com
.nsatc.net. (145)
23:53:11.578303 IP 172.16.4.193.netbios-ns > 172.16.4.255.netbios-ns: UDP, length 50
23:53:11.630028 IP 172.16.4.193.bootpc > 255.255.255.255.bootpc: BOOTP/DHCP, Request from 5c:26:0a:02:a8:e4 (ou
t Unknown), length 300
23:53:11.630054 IP 172.16.4.193.50836 > 224.0.0.252.hostmon: UDP, length 27
23:53:11.630242 IP 172.16.4.1.bootpc > 172.16.4.193.bootpc: BOOTP/DHCP, Reply, length 300
23:53:11.633572 IP 172.16.4.193.60128 > 224.0.0.252.hostmon: UDP, length 22
23:53:11.734368 IP 172.16.4.193.60128 > 224.0.0.252.hostmon: UDP, length 22
23:53:11.734555 IP 172.16.4.193.50836 > 224.0.0.252.hostmon: UDP, length 27
23:53:11.874709 IP 172.16.4.193.netbios-ns > 172.16.4.255.netbios-ns: UDP, length 68
23:53:11.874728 IP 172.16.4.193.netbios-ns > 172.16.4.255.netbios-ns: UDP, length 68
23:53:11.874733 IP 172.16.4.193.netbios-ns > 172.16.4.255.netbios-ns: UDP, length 68
23:53:11.937372 IP 172.16.4.193.netbios-ns > 172.16.4.255.netbios-ns: UDP, length 50
23:53:12.343634 IP 172.16.4.193.54622 > 224.0.0.252.hostmon: UDP, length 24
```

Obrázek 9 – Tcpdump Zdroj: [vlastní zpracování]

Výstup tcpdump je typicky textový a zobrazuje detaily každého paketu, včetně časového razítka, zdrojové a cílové IP adresy, protokolu a dalších informací specifických pro daný protokol. K přehlednosti pomáhají přepínače, které umožňují filtrování získaných paketů například na základě IP adres nebo portů a protokolů. Takový výstup lze i exportovat do souboru a dále zpracovávat a analyzovat pomocí různých nástrojů, jako třeba v grafickém analyzátoru sítě Wireshark. [19] [20]

Network miner

Program Network miner je určený pro forenzní analýzu síťové komunikace. Extrahuje artefakty jako například soubory, obrázky, emaily a hesla získané ze získaného síťového přenosu ve formátu PCAP. Umožňuje i živé odposlouchání komunikace na síťové kartě. Získané informace jsou agregovány do přehledného grafického rozhraní obsahující seznam zařízení, které spolu komunikují. [21]



Obrázek 10 – Network miner Zdroj: [vlastní zpracování]

Network miner je primárně určen pro operační systém Windows, ale je možné ho spustit i v Linuxu. [21]

3.4.2 Skenování sítě

Když útočníkům nestačí jen zkoumat přenášená data a chtějí zjistit více informací o zařízeních v síti, mohou síť skenovat. Skenování sítě mapuje cílové prostředí. Blíže identifikuje uzly, jejich propojení a běžící služby. Aktivní skenování na rozdíl od pasivního sledování komunikace ostatních uzlů již vyžaduje vysílání dat do sítě. Kvůli tomu je i snadnější detekce takové aktivity administrátorem. [82] [83] [85]

Útočníci používají různé druhy skenů, které se od sebe liší ve způsobu detekce otevřených služeb. Rozdíly jsou v rychlosti, spolehlivosti a schopnosti obejít firewallů nebo IDS systémů. Některé provádějí běžné navázání TCP komunikace, jiné používají nestandardní kombinace TCP vlajek.

TCP SYN Sken

TCP SYN sken je výchozí a nejčastěji používaný způsob, který umožňuje skenovat velké množství portů za krátký čas. Odesílá se SYN paket jako při běžném navázání spojení a následně se čeká na odpověď. Vlajka odpovědi SYN/ACK znamená, že port naslouchá (je otevřený), zatímco RST (reset) znamená, že port nenaslouchá. Pokud po několika opakovaných odeslání nepříjde žádná odpověď, je port označený jako filtrovaný (filtered). Port je také označený jako filtrovaný, pokud je přijata ICMP chyba. Tato technika se často označuje jako *half-open scanning*, protože se při ní neotevřívá celé TCP spojení. [22]

TCP Connect Sken

V případě, že uživatel nemá dostatečná oprávnění pro práci s raw pakety, je možné navázat celé TCP spojení. To ale zabere více času i přenesených dat a může být snadněji detekovatelné IDS systémy. [22]

UDP Sken

UDP skeny posílají UDP pakety na cílené porty. Na základě odpovědi nebo její absence se portům přidělí jeden ze čtyř stavů:

- open – když přijde jakákoliv odpověď
- open | filtered – když nepříjde žádná odpověď
- closed – když přijde ICMP unreachable error (type 3, code 3)
- filtered – když přijde jiný ICMP unreachable error (type 3, code 1, 2, 9, 10 nebo 13)

Problémem při skenování UDP je rychlost. Otevřené a filtrované porty zřídka odešlou nějakou odpověď, proto dochází k čekání, a u uzavřených portů se odesílá velké množství chybových ICMP zpráv, které bývají rychlostně omezené. [22]

TCP NULL, FIN, Xmas a podobné skeny

Specifické typy skenů využívají charakteristik protokolu TCP, který je definován v RFC 793. Používají například nestandardní vlajky v paketech, díky čemuž mohou obejít méně sofistikované firewally nebo systémy pro detekci průniku. [22] [23]

NULL sken posílá pakety bez nastavených TCP vlajek. Pokud je cílový port otevřen, zařízení neodpoví, jelikož je paket neplatný a nevyvolá reakci. Naopak když je uzavřený, přijde odpověď RST. [22]

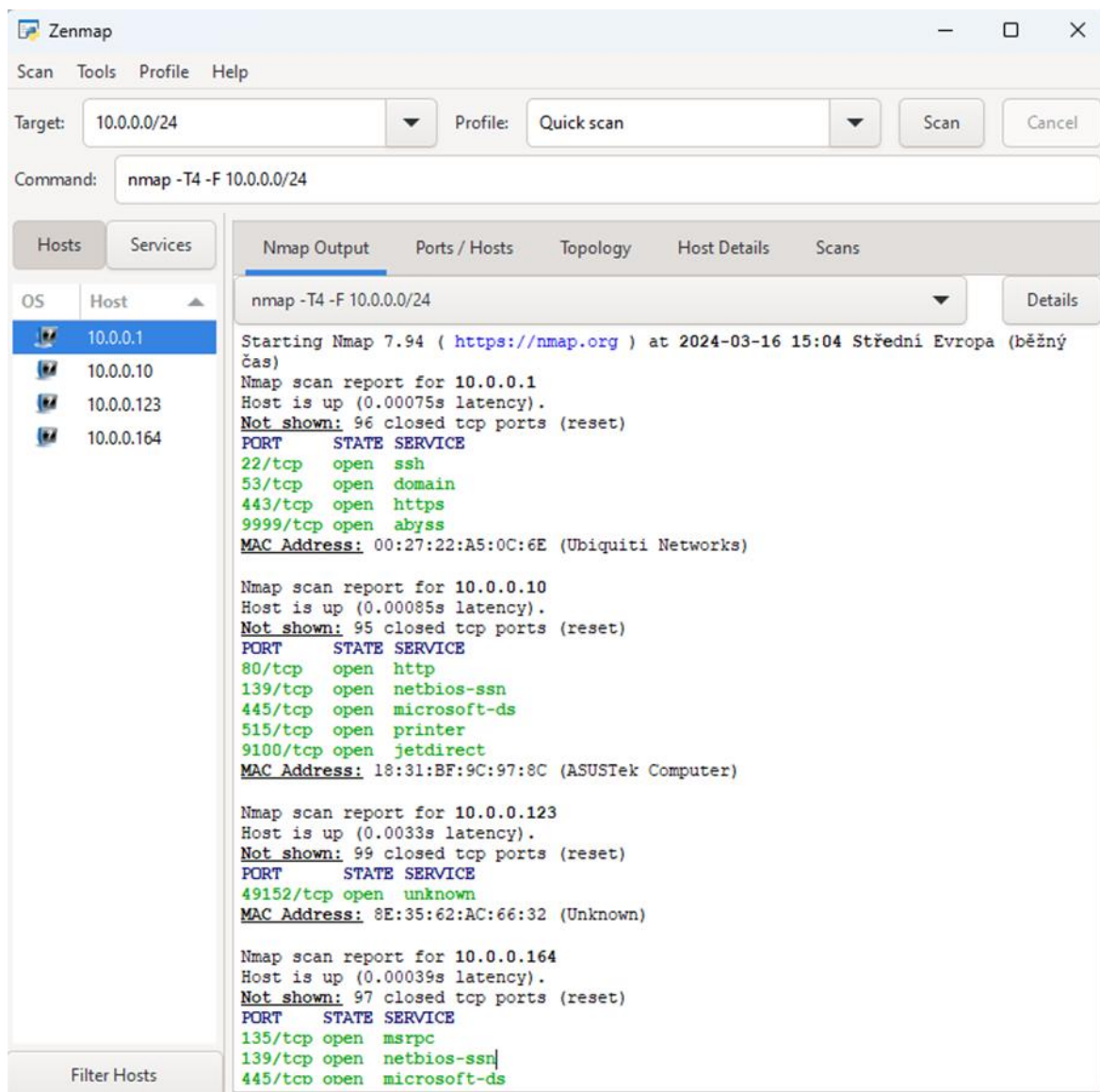

```
nepomucky@bit8-nepomucky-kali-v2: ~
File Actions Edit View Help
(nepomucky@bit8-nepomucky-kali-v2)-[~]
$ nmap -h
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
```

Obrázek 12 – Nmap Zdroj: [vlastní zpracování]

S programem se pracuje v příkazovém řádku, ve kterém je výsledek skenování uživateli zobrazován. Výstup je rovněž možné exportovat do souboru, který je možné následně zpracovávat dalšími programy.

Zenmap

Oficiální grafické rozhraní nástroje Nmap usnadňuje skenování sítě nováčkům a zároveň obsahuje všechny nástroje terminálové varianty. Profily umožňují ukládání často používaných skenů pro jejich snadné opakované spouštění. Slouží i jako generátor konkrétních Nmap příkazů. Ve výsledcích skenů lze vyhledávat a dají se uložit pro vzájemné porovnání. [25]



Obrázek 13 – rozhraní Zenmap Zdroj: [vlastní zpracování]

3.4.3 Útoky na heslo

Pro většinu přístupů se dnes používají kombinace uživatelských jmen a hesel. Výjimkou není ani prostor počítačových sítí, kdy se takovým způsobem ověřuje přístup do síťových prvků, serverů a koncových stanic. Útočníci proto zkusí tento mechanismus prolomit.

Dictionary attack

Mezi nejběžnější postupy je možné zařadit slovníkové útoky. Slovníky představují různě dlouhé seznamy často používaných hesel. Ty se následně používají při pokusu o prolomení ochrany.

Tyto slovníky si útočník může vytvořit sám na míru pro svůj cíl nebo využít některý z mnoha veřejně dostupných. Nejznámějším je *RockYou.txt*, který vznikl z velkého úniku dat v roce 2009. Při něm bylo odhaleno více než 32 milionů uživatelských hesel, která nebyla nijak šifrovaná. V Kali Linuxu je tento seznam zmenšen a obsahuje přibližně 14 milionů hesel. [26] [27]

Mezi nejpoužívanější nástroje pro provedení útoku s využitím slovníků patří *Hydra*. Umožňuje cílit na běžné protokoly a služby jako HTTP, HTTPS, LDAP, MySQL, RDP, SNMP nebo SSH. [28]

```
(nepomucky@bit8-nepomucky-kali-v2)-[~]
└─$ hydra -h
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
rvic organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics
 anyway).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-
M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [
-m MODULE_OPT] [service://server[:PORT][/OPT]]

Options:
-R          restore a previous aborted/crashed session
-I          ignore an existing restore file (don't wait 10 seconds)
-S          perform an SSL connect
-s PORT    if the service is on a different default port, define it here
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-x MIN:MAX:CHARSET password bruteforce generation, type "-x -h" to get help
-y          disable use of symbols in bruteforce, see above
-r          use a non-random shuffling method for option -x
-e nsr     try "n" null password, "s" login as pass and/or "r" reversed login
-u         loop around users, not passwords (effective! implied with -x)
-C FILE    colon separated "login:pass" format, instead of -L/-P options
-M FILE    list of servers to attack, one entry per line, ':' to specify port
-o FILE    write found login/password pairs to FILE instead of stdout
-b FORMAT specify the format for the -o FILE: text(default), json, jsonv1
-f / -F    exit when a login/pass pair is found (-M: -f per host, -F global)
-t TASKS   run TASKS number of connects in parallel per target (default: 16)
-T TASKS   run TASKS connects in parallel overall (for -M, default: 64)
-w / -W TIME wait time for a response (32) / between connects per thread (0)
-c TIME    wait time per login attempt over all threads (enforces -t 1)
-4 / -6    use IPv4 (default) / IPv6 addresses (put always in [] also in -M)
```

Obrázek 14 – Hydra Zdroj: [vlastní zpracování]

Credential stuffing

Credential stuffing je kybernetický útok, při kterém útočníci používají uživatelská jména a hesla z uniklých databází. Ta zkouší používat do různých online služeb. Tento útok je založen na tom, že lidé často používají stejné nebo podobné přihlašovací údaje na více webových stránkách a aplikacích. [29]

3.4.4 Social engineering

Sociální inženýrství je technika, kterou využívají útočníci k manipulaci jednotlivců, aby vyzradili důvěrné informace, provedli akce nebo poskytli přístup k zabezpečeným systémům. Na rozdíl od jiným hackerských metod, které využívají technické zranitelnosti, se sociální inženýrství zaměřuje na lidský faktor a využívá psychologické a behaviorální faktory.

Protože člověk je nejslabším článkem kybernetické bezpečnosti, je nutné tomu přizpůsobit postupy při nastavování bezpečnostní politiky. Ta zahrnuje mimo jiné řízení přístupu blíže popsané v kapitole 3.5.3. Stejně důležitá jsou i pravidelná školení uživatelů, které je třeba informovat o aktuálních hrozbách. [30] [31] [32] [33]

Phishing

Phishing je typ kybernetického útoku, při kterém se útočníci snaží získat citlivé údaje – hesla, údaje z kreditních karet a podobně. Během toho se vydávají za důvěryhodné organizace – banky, velké známé společnosti nebo technické oddělení firmy, ve které oběť pracuje. Komunikují prostřednictvím emailů nebo zpráv, kdy oběť přesměrují na webovou stránku, která má stejný vzhled jako reálná předloha. Zadané údaje jsou ale odeslány přímo útočnickovi, který je následně může zneužít. [34]

Nástroj *Blackeye* umožňuje automatické generování přihlašovacích stránek desítek populárních webových stránek jako jsou Instagram, Facebook nebo Netflix. Po vybrání požadované služby se zobrazí vlastní URL adresa, na které běží vytvořená phishingová stránka. Zadané přihlašovací údaje jsou ihned zachytávány, zobrazovány v rozhraní útočníka a dají se snadno zneužít. [35]

Vishing

Mezi aktuální trendy patří vishing, který je založen na principu telefonních hovorů. Volající se představí jako pracovník banky, který zjistil napadení účtu. Fiktivní bankovní úředník za využití autority a vytvoření strachu přiměje oběť přesunout peníze na jiný účet, který ale patří útočnickovi. Tato metoda je efektivní na všechny věkové kategorie. [36]

Cílení na jednotlivce a jejich bankovní účty je aktuálně velice rozšířené, protože je pro útočníky nejjednodušší pro jejich obohacení. Podobný postup ale lze využít i při útoku proti konkrétní organizaci, kdy cílem může být nejen převedení finančních prostředků, ale i vyzrazení obchodních tajemství, přístupu do infrastruktury, krádež nebo zašifrování dat a

následné vydírání. Takový únik dat může znamenat ztrátu důvěry klientů firmy a mít za následek její celkový krach. [36]

The image shows a Google search interface with the query "falešný bankéř". The search results are as follows:

- policie.cz**
https://www.policie.cz › falesny-banker-opet-v-akci
Falešný bankéř opět v akci!
21. 8. 2023 — **Falešný bankéř** opět v akci! LIBEREC – Žena z Liberce na poslední chvíli uchránila své úspory ve výši 306.000 korun. V minulém týdnu byla ...
- policie.cz**
https://www.policie.cz › clanek › falesny-banker-pripr...
Falešný bankéř připravil ženu o 299 tisíc korun
před 1 dnem — **Falešný bankéř** připravil ženu o 299 tisíc korun. ZLÍNSKO: Uvěřila, že je její účet napaden. Kriminalisté se od včerejška zabývají dalším ...
- idnes.cz**
https://www.idnes.cz › jihlava › zpravy › policie-fales...
Gang falešných bankéřů obral stovky lidí o 195 milionů ...
16. 11. 2023
- lupa.cz**
https://www.lupa.cz › aktuality › akce-falesny-banker-...
Akce falešný bankéř: Policie odhalila největší případ ...
před 5 dny
- denik.cz**
https://melnicky.denik.cz › ... › Krimi › Zločiny a soudy
Falešný bankéř připravil ženu z Mělnicka o 240 tisíc korun
16. 11. 2023
- denik.cz**
https://hradecky.denik.cz › ... › Krimi › Zločiny a soudy
Falešný bankéř řádí v Hradci Králové. Lidé své úspory už ...
31. 7. 2023
- ceskatelevize.cz**
https://ct24.ceskatelevize.cz › domaci › 3618718-repo...
Reportéři ČT: Falešní bankéři jako nová mafie. Oběti ... - ČT24

Obrázek 15 – Úspěšnost sociálního inženýrství Zdroj: [vlastní zpracování]

3.4.5 Keylogging

Keylogger je zkratkou pro „Keystroke Logger“. Jedná se o škodlivý software nebo hardwarové zařízení, které má za úkol zaznamenávat stisknuté klávesy uživatele. Cílem je opět získání citlivých dat.

Softwarová varianta může být do počítače stažena jako jakýkoliv jiný malware – z emailu nebo škodlivé webové stránky. Následně běží na pozadí počítače a získané uživatelské vstupy jsou uloženy v souboru nebo odeslány na vzdálený server. Infikování bývá odhaleno antivirovým programem. [37]

Hardwarová varianta se umísťuje mezi klávesnici a USB vstup počítače. Nejčastěji zezadu do základní desky, kde zařízení není na první pohled vidět. Data se ukládají do integrované paměti nebo odesílají za použití bezdrátového připojení. Jelikož se nejedná o software, antivirus ho nemůže detekovat. Odhalení je možné pouze fyzickou kontrolou. [38]

AirDrive Pro USB Keylogger

★★★★★



AirDrive Pro USB keylogger s kapacitou 16 MB, kompletní WiFi konektivitou, možností přizpůsobení národní klávesnice, možností zaslání emailových reportů, záznamem data a času a živým streamováním je aktuálně nejlepším keyloggerem na trhu v poměru výkon / cena. [více](#)

Cena za 1 ks vč. DPH:	4 295 Kč
Cena za 1 ks bez DPH:	3 550 Kč

🎁 Dárek

Více než 5ks skladem

1

Expediční doba: do 24 hodin

Obrázek 16 – USB Keylogger Zdroj: [39]

3.4.6 Útoky na zařízení a služby

Útok může cílit i na samotná zařízení v síti. Tím je útočník schopen narušit dostupnost zdrojů, rychlost i stabilitu sítě. K tomu lze mimo jiné využít útoky typu Denial of Service (DoS) a Distributed Denial of Service (DDoS), které mají za cíl přetížit klíčové

prvky a servery tak, aby nebyly schopny správně plnit svoji funkci. DDoS útoky jsou oproti DoS útokům prováděny z více zdrojů, a tak dokáží generovat více dat a cíl efektivněji zahltit. [40]

Z napadených zařízení mohou útočníci ukrást data, know-how nebo je mohou využít jako zdroj dalších útoků a cílit na další zařízení v lokální síti i mimo ni. Servery pak lze využít k rozesílání nevyžádané pošty, hostování phishingových stránek, podvodných e-shopů nebo jako botnet pro provádění DDoS útoků. [41] [42]

DHCP starvation attack

V počítačových sítích jsou častokrát IP adresy přidělovány DHCP serverem. Ty je propůjčují klientům z dostupného rozsahu na zvolenou dobu. Útočník může tohoto mechanismu zneužít a server takzvaně vyhladovět. Útok provede tak, že ze svého zařízení zažádá o tolik IP adres, že vyčerpá celý dostupný rozsah a pro další legitimní zařízení žádné nezbudou.

Nástroj umožňující provedení takového útoku se nazývá *Yersinia*. Je navržen tak, aby využil slabiny v různých protokolech druhé vrstvy. Jsou v něm implementovány útoky pro protokoly Dynamic Host Configuration Protocol (DHCP), Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP) a další. Použití je možné jak v příkazové řádce, tak v grafickém prostředí. [43]

```
nepomucky@bit8-nepomucky-kali: ~
File Actions Edit View Help

(nepomucky@bit8-nepomucky-kali)-[~]
$ sudo yersinia -h
Yersinia ...
The Black Death for nowadays networks
by Slay & tomac
http://www.yersinia.net
yersinia@yersinia.net
Prune your MSTP, RSTP, STP trees!!!!

Usage: yersinia [-hVGI-D-d] [-l logfile] [-c conffile] protocol [protocol_options]
-V Program version.
-h This help screen.
-G Graphical mode (GTK).
-I Interactive mode (ncurses).
-D Daemon mode.
-d Debug.
-l logfile Select logfile.
-c conffile Select config file.
protocol One of the following: cdp, dhcp, dot1q, dot1x, dtp, hsrp, isl, mpls, stp, vtp.

Try 'yersinia protocol -h' to see protocol_options help

Please, see the man page for a full list of options and many examples.
Send your bugs & suggestions to the Yersinia developers <yersinia@yersinia.net>

MOTD: M4t30 31337 M4t30 31337 M4t30 31337 M4t30 31337 M4t30 31337
```

Obrázek 17 – Nástroj Yersinia Zdroj: [vlastní zpracování]

Rogue DHCP

Mimo přímého útoku na DHCP server lze tento protokol využít i k jinému typu útoku. Útočník při něm do sítě nasadí svůj vlastní DHCP server s cílem rozdávat IP adresy, výchozí bránu, DNS server a další parametry poskytované tímto protokolem. Díky tomu je schopen ovlivnit komunikaci z koncových zařízení, odposlouchávat ji nebo ji blokovat a tím znemožnit komunikaci s ostatními prvky a internetem.

Neighbor discovery attack

Neighbor Discovery protokoly (NDP) umožňují najít zařízení kompatibilní s MNDP (MikroTik Neighbor Discovery Protocol), CDP (Cisco Discovery Protocol) nebo LLDP (Link Layer Discovery Protocol) na druhé vrstvě celé broadcastové domény. Vytvořený seznam zařízení obsahuje všechny zjištěné sousedy včetně jejich IP a MAC adresy a dalších parametrů. [44]

```
[admin@MikroTik] /ip neighbor print
# INTERFACE ADDRESS MAC-ADDRESS IDENTITY VERSION BOARD
0 ether13 192.168.33.2 00:0C:42:00:38:9F MikroTik 5.99 RB1100AHx2
1 ether11 1.1.1.4 00:0C:42:40:94:25 test-host 5.8 RB1000
2 Local 10.0.11.203 00:02:B9:3E:AD:E0 c2611-r1 Cisco I...
3 Local 10.0.11.47 00:0C:42:84:25:BA 11.47-750 5.7 RB750
4 Local 10.0.11.254 00:0C:42:70:04:83 tsys-sw1 5.8 RB750G
5 Local 10.0.11.202 00:17:5A:90:66:08 c7200 Cisco I...
```

Obrázek 18 – Neighbor list Zdroj: [44]

Jeden z útoků, který využívá tyto protokoly, může spočívat v přetížení zařízení a přeplnění NDP tabulky. Útočník při něm zasílá velké množství falešných NDP zpráv, které se síťový prvek snaží zaznamenat a uložit do paměti. Mívá to za následek vysoké vytížení procesoru, úložiště i šířky přenosového pásma. Zařízení poté nemusí být schopné směřovat a přepínat zbytek komunikace a celkově plnit svoji funkci. K provedení tohoto útoku je opět možné použít nástroj *Yersinia*, stejně jako pro vyhledování DHCP serveru. [43]

3.5 Bezpečnostní postupy a nástroje

Bezpečnostní experti mají k dispozici celou řadu nástrojů, které zajišťují bezpečnost počítačových sítí a systémů v nich. Jejich široké spektrum pomáhá odolat útokům různých druhů i zdrojů.

3.5.1 Fyzické zabezpečení

Stavebním kamenem zabezpečené počítačové sítě je ochrana přístupu k síťovým prvkům. Přístup do rozvodů a serverových místností by měl být omezen směrnicí firmy a monitorován. Evidence přístupu může ztížit pokus o narušení a identifikovat útočníka po incidentu. S tím souvisí i zabezpečení síťových zásuvek, které mohou být přístupovým bodem do sítě stejně jako připojení bezdrátové.

Přístup do prostor organizace by měl být také omezen. Útočník by mohl v nestřežených okamžicích použít něčí počítač a nakazit ho malwarem nebo ho využít k útoku na síťovou infrastrukturu. Pro přístup ke stisknutým klávesám by mohl nainstalovat hardwarový keylogger, který nelze systémově detekovat.

3.5.2 Bezpečnost hesel

Síťové prvky většinou používají pro přístup ke konfiguraci přihlašovací jména a hesla. Ta bývají pro zjednodušení práce běžným uživatelem předdefinována na jednoduché kombinace jako například uživatel *admin* s heslem *admin*. Jednotlivec provede prvotní nastavení a výzvu o změně hesla častokrát ignoruje. Tím vzniká obrovské bezpečnostní riziko, které může útočnickovi získat přístup k celé síti a všem přenášeným datům bez toho, aby uživatel toto jednání odhalil.

Proto je nutné mít nastavenou bezpečnou politiku hesel. Nejen ve firmě, ale i v osobním životě. Takové heslo by mělo být dostatečně dlouhé. Policie ve své kampani doporučuje minimálně 8 znaků [45], zatímco antivirová společnost Avast nedoporučuje používat žádné heslo kratší než 15 znaků [46]. Je důležité se vyvarovat běžným kombinacím (např. „123456789“, „qwertz“, „password“), využívat nejen velká a malá písmena, ale i čísla a speciální znaky. Takto vytvořená hesla by měla být pro každou službu unikátní. Tím se eliminuje riziko zneužití ukradených přihlašovacích údajů z jedné služby na některé z ostatních. Bezpečné heslo může vycházet z fráze nebo věty. Ta se snáze pamatuje a je dostatečně dlouhá.

Velké množství přihlašovacích údajů je možné ukládat i do správce hesel. Ty ukládají hesla od jednotlivých služeb a uživateli odpadá nutnost si je pamatovat. Díky tomu je snazší používat rozdílná hesla pro různé služby. Bezpečnost všech hesel ale závisí na jedné službě, a tak je třeba zvolit vhodné řešení a dbát na její zabezpečení. Zneužití takové služby by totiž představovalo únik všech uložených hesel.

Ve firmě může nastat problém, kdy je vyžadována tak vysoká bezpečnost, že administrátor vynucuje tak silná hesla nebo jejich pravidelné změny, že si je uživatelé nebudou schopni pamatovat a začnou si je například psát na papírek vedle počítače. Tím vznikne obrovské bezpečnostní riziko. Proto je důležité bezpečnostní politiku hesel nastavovat s rozumem a s ohledem na zaměstnance firmy.

Pro zvýšení zabezpečení je rozšířeno používání dvoufázového ověření. To mimo znalosti přihlašovacích údajů vyžaduje zadání kódu z mobilní aplikace, ověření pomocí hardwarového klíče (čipové karty, USB, Bluetooth, NFC zařízení) nebo biometrie. [47]

3.5.3 Řízení přístupu

Řízení přístupu určuje, kdo má povolení k provedení určitých akcí, přístupu k vybraným datům, aplikacím a prostředkům. Chrání důvěrné informace firmy před neoprávněnými uživateli a snižují riziko exfiltrace (vynesení) dat zaměstnanci.

Každý zaměstnanec by měl mít přístupy a oprávnění potřebné pro jeho druh práce. Zbytečně vysoká oprávnění uživatelských účtů zvyšují riziko zneužití v případě jejich odcizení. Proto se administrátorům nedoporučuje nepoužívat na běžné akce účty s nejvyšším oprávněním. [48]

3.5.4 Aktualizace softwaru

Často opomíjená, ale velmi významná součást zabezpečené sítě je pravidelná aktualizace firmwaru a softwaru používaných zařízení. Nové verze totiž mimo oprav chyb nebo přidání dalších funkcí obsahují i důležité bezpečnostní změny. Neaktuální verze mohou představovat bezpečnostní riziko.



The image shows a screenshot of a website article. At the top is a dark navigation bar with the 'MSSPAlert' logo and links for NEWS, WEBCASTS, PODCAST, RESOURCES, ABOUT, CONTACT, MANAGE, Log In, and a red 'Create Account' button. Below the navigation bar, the article title is 'Kaspersky: Enterprises Running Old Software Lose 47% More Money in Data Breach' by D. Howard Kass, dated December 29, 2020. The main image is a teal-tinted close-up of US dollar bills. Below the image, a text snippet reads: 'More than four in 10 organizations in North America use out-of-date technology and lose nearly 50 percent more money in a data breach than companies running updated software and hardware, a new Kaspersky report said.'

Obrázek 19 – Úniky dat způsobené neaktuálním softwarem Zdroj: [49]

3.5.5 Firewall

Firewall je prvek určený pro zabezpečení počítačové sítě. Monitoruje příchozí a odchozí síťový provoz a podle definované sady bezpečnostních pravidel rozhoduje, zda danou komunikaci povolí či zablokuje. Jeho hlavním účelem je chránit zařízení v síti před neautorizovaným přístupem, útoky a hrozbami z internetu nebo z jiných sítí.

Pracuje na různých úrovních síťového modelu, zakazuje nežádoucí provoz a povoluje provoz legitimní. Může filtrovat provoz na základě IP adres, portů, protokolů, aplikací a mnoha dalších kritérií dle konkrétní implementace daného výrobce. [51] [53]

Hardware firewall

Firewall může být samostatné fyzické zařízení umístěné nejčastěji na hranici mezi interní a externí částí počítačové sítě, aby blokoval nežádoucí provoz a chránil lokální síť před hrozbami z internetu. [53]

Software firewall

Implementace je možná i jako software na úrovni operačního systému. V takovém případě běží jako aplikace nebo součást operačního systému na serveru, síťovém prvku nebo koncovém zařízení. [53]

Nestavový firewall

Nestavový firewall zpracovává každý paket samostatně a rozhoduje se pouze na základě obsažených informací a definovaných pravidel. Nezohledňuje historii ani kontext daného síťového připojení. [53] [54]

Stavový firewall

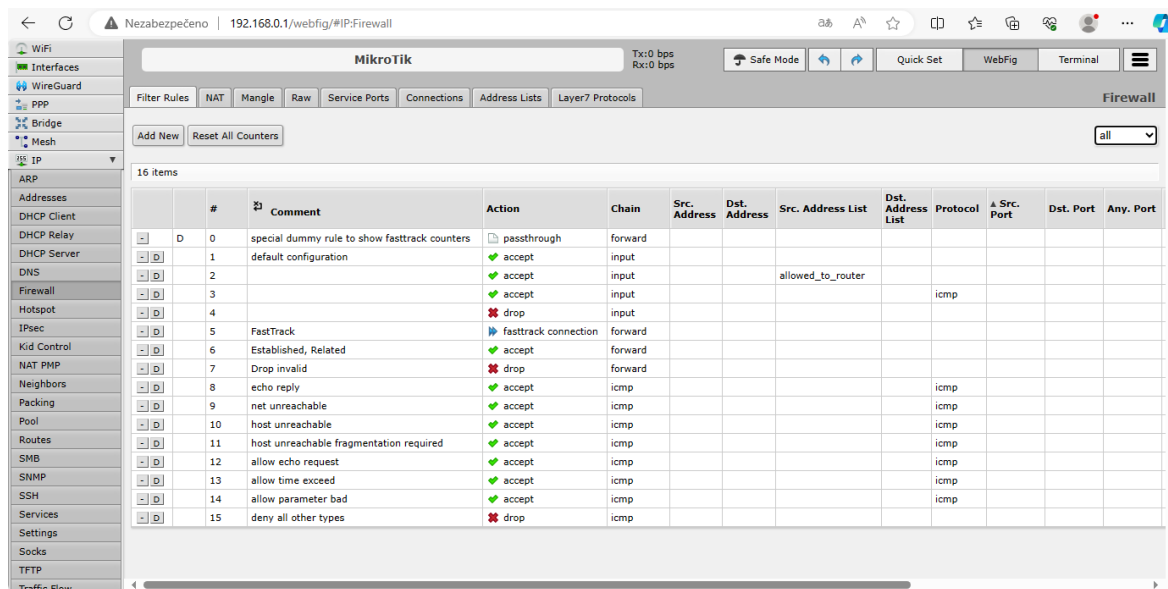
Stavový firewall monitoruje stav aktivních spojení, čímž přidává připojením kontext. Tato metoda umožňuje firewallu analyzovat komunikaci jako celek, nejen jako jednotlivé pakety bez ohledu na jejich historii a návaznost. [52] [53] [54]

Aplikační firewall

Aplikační firewall může filtrovat komunikaci nejen dle protokolu, ale i aplikace, která ho využívá. Například v případě webové komunikace odhaluje jeho obsah, který je uložen v sedmé vrstvě. [51]

Next Generation Firewall

Next Generation Firewall (NGFW) umí navíc oproti běžnému firewallu blokovat známé útoky, provádět hloubkovou inspekci paketů a fungovat jako systém pro prevenci průniků (IPS). [50] [52] [53]



The screenshot shows the Mikrotik RouterOS Firewall configuration page. The left sidebar contains various system settings like WiFi, Interfaces, WireGuard, PPP, Bridge, Mesh, IP, ARP, Addresses, DHCP Client, DHCP Relay, DHCP Server, DNS, Firewall, Hotspot, IPsec, Kid Control, NAT PMP, Neighbors, Packing, Pool, Routes, SMB, SNMP, SSH, Services, Settings, Socks, and TFTP. The main content area is titled 'Firewall' and shows a list of 16 items. The table below represents the data shown in the screenshot.

#	Comment	Action	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Address List	Protocol	Src. Port	Dst. Port	Any. Port
0	special dummy rule to show fasttrack counters	passthrough	forward								
1	default configuration	accept	input								
2		accept	input			allowed_to_router					
3		accept	input					icmp			
4		drop	input								
5	FastTrack	fasttrack connection	forward								
6	Established, Related	accept	forward								
7	Drop invalid	drop	forward								
8	echo reply	accept	icmp					icmp			
9	net unreachable	accept	icmp					icmp			
10	host unreachable	accept	icmp					icmp			
11	host unreachable fragmentation required	accept	icmp					icmp			
12	allow echo request	accept	icmp					icmp			
13	allow time exceed	accept	icmp					icmp			
14	allow parameter bad	accept	icmp					icmp			
15	deny all other types	drop	icmp					icmp			

Obrázek 20 – Firewall v RouterOS Zdroj: [vlastní zpracování]

3.5.6 Access Control Lists

Na aktivních prvcích společnosti Cisco jsou Access Control Lists (ACL) vlastností operačního systému. Umožňují filtrování síťového provozu podle definovaných pravidel. Seznamy pravidel jsou kontrolovány sekvenčně za sebou a pokud dojde ke splnění podmínek, provede se akce a dále se nepokračuje. Používají se akce *permit* pro povolení a *deny* pro zakázání komunikace. Na konci každého seznamu je výchozí pravidlo, které zakazuje všechnu ostatní komunikaci. ACL se aplikují na síťové porty, kde se rovněž určuje směr, ve kterém má působit – *in* v případě omezení paketů, které vstupují přes vybraný interface do síťového prvku, nebo *out*, kdy se filtruje komunikace na výstupu ze zařízení. [55] [58] [59]

Standard ACL

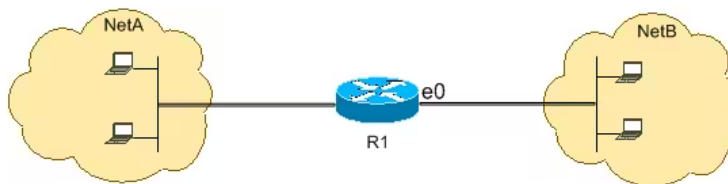
Základní pravidla podporují filtrování pouze na základě zdrojové IP adresy. Zakázání nebo povolení komunikace se týká všech protokolů. Označují se čísly od 1 do 99 a od 1300 do 1999, nebo pomocí názvu. Většinou se používají blíže k cíli právě kvůli chybějící možnosti nastavit v pravidle cílovou IP adresu. [55] [56] [58]

Extended ACL

Rozšířená pravidla umožňují filtrování provozu podle více parametrů – lze definovat zdrojové i cílové IP adresy a čísla portů. Rovněž podporují filtrování na základě MAC adresy. Označují se čísly od 100 do 199 a od 2000 do 2699, nebo pomocí názvu. Oproti standardním ACL se používají blíže ke zdrojovým zařízením. [56] [57] [58]

Allow Pings (ICMP)

This image shows that ICMP sourced from NetA destined to NetB is permitted, and pings sourced from NetB destined to NetA are denied.



This configuration permits only echo-reply (ping response) packets to come in on interface Ethernet 0 from NetB towards NetA. However, the configuration blocks all echo-request ICMP packets when pings are sourced in NetB and destined to NetA. Therefore, hosts in NetA can ping hosts in NetB, but hosts in NetB cannot ping hosts in NetA.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit icmp any any echo-reply
```

Obrázek 21 – Ukázka použití ACL Zdroj: [56]

3.5.7 Port Security

Ethernetové zásuvky jsou vstupní bránou do počítačové sítě. Jsou důležitým pasivním síťovým prvkem, který umožňuje připojovat koncová zařízení, a proto jsou většinou situovány v jejich blízkosti. Kvůli jejich snadné dostupnosti je nutné zajistit ochranu před jejich zneužitím útočníky. Fyzický přístup je možné zneužít k odposlouchávání síťové komunikace, skenování sítě a zařízení v ní a následně k útokům na klíčové prvky infrastruktury. [60]

Základem zabezpečení je vypínání nepoužívaných portů na přepínačích. Pokud síťová zásuvka není využívána, je zbytečné, aby umožňovala přístup do sítě. Riziko zneužití je ale i u těch používaných. Útočníkovi by stačilo odpojit počítač zaměstnance firmy a připojit svůj. Pro tyto případy je vhodné kontrolovat MAC adresy zařízení připojených do daného portu a povolit konkrétně jen ty ověřené. Při detekci připojení jakéhokoliv jiného zařízení je možné port úplně vypnout nebo komunikaci blokovat a dál do sítě neposílat. Dalším způsobem je ověřování koncových zařízení na úrovni sítě. Pomocí přihlašovacích údajů nebo certifikátů lze nejen zařízení povolit nebo blokovat, ale také přiřazovat porty do různých VLAN – zaměstnanecké počítače do lokální firemní sítě a vše ostatní do sítě pro hosty, ze které nejsou zařízení firemní sítě dostupné. [60] [61]

3.5.8 Honeypot

Honeypot je záměrně zranitelný systém, který slouží jako past na útočníky. Jeho účelem je lákat potenciální hackery, díky čemuž je rychle odhaluje a zároveň odvrací pozornost od jiných prvků síťové infrastruktury. Honeypot sbírá data o provedených útocích, čímž poskytuje cenné informace o postupech a nástrojích útočníků. Ty mohou využít bezpečnostní experti při optimalizaci a vylepšení zabezpečení. [62]

Jednotlivé varianty se liší zejména v míře interakce. Honeypoty s nízkou interakcí obsahují jen základní prostředí, ve kterém může útočník pracovat. Naopak honeypoty s vysokou interakcí používají propracované prostředí, ve kterém může útočník provádět velké množství akcí, čímž poskytuje mnohem více dat o jeho postupech. [62]

3.5.9 Systémy odhalení a prevence průniku

Systémy pro odhalení a prevence průniku jsou důležitými prvky zabezpečení počítačových sítí. Detekují útoky a chrání infrastrukturu organizace před útočníky.

Intrusion Detection System

Systém pro odhalení průniku (IDS) monitoruje síťový provoz. Detekuje známé škodlivé a podezřelé aktivity nebo porušení bezpečnostních zásad. Na základě těchto upozornění mohou pracovníci bezpečnostního operačního centra (SOC) reagovat na incidenty, daný problém prošetřit a přijmout vhodná opatření k nápravě hrozby. Jedná se o spíše pasivní nástroje, jelikož průnik jen detekují a předávají informaci správci sítě, který na incident reaguje. [63]

Network intrusion detection systems

NIDS je systém navržený k monitorování a analýze síťového provozu s cílem detekovat bezpečnostní hrozby v reálném čase. Zkoumá různé aspekty paketů a hledá vzorce spojené se známými útoky.

Host intrusion detection systems

HIDS monitorují procesy a aplikace spouštěné na koncových zařízeních. Sledují změny v systémové konfiguraci, registrech, prochází logy a upozorňují na nestandardní aktivitu. [64]

Intrusion Prevention System

Systém pro prevenci průniku (IPS) na rozdíl od systémů pro odhalení průniku na aktuální hrozbu aktivně reaguje. Škodlivou komunikaci odhaluje a následně blokuje, čímž útok zastaví dříve, než naruší koncové stanice v síťové infrastruktuře. Může se stát, že zablokuje i legitimní komunikaci, proto je v některých sítích preferováno mít pouze IDS.

Security onion

Security Onion je pokročilá platforma pro ochranu síťové bezpečnosti, která poskytuje komplexní soubor nástrojů pro monitorování a analýzu síťového provozu a chování hostitelů. Využívá mnoho bezpečnostních nástrojů, které jako celek poskytují komplexní systém pro zabezpečení počítačové sítě.

Pro generování NIDS výstrah používá systémy *Suricata* a *Zeek*, které monitorují síťový provoz a identifikují potenciální pokusy o průnik. Pro ukládání přenesených paketů pro pozdější offline analýzu používá *Stenographer*. Intrusion Detection Honeypot (IDH), který je založen na *OpenCanary*, láká útočníky a získává o něm důležité informace, které je možné využít k dalšímu vyšetřování a budoucímu vylepšení zabezpečení. Pro získávání dat z koncových zařízení je možné využít *Elastic Agent* a *Sysmon*. Používané nástroje nejsou ve všech verzích stejné, starší vydání používaly například systém *Wazuh*, který je v aktuální verzi nahrazen. [65]

Společnost nabízí i oficiální hardware v různých variantách, který je optimalizován pro nasazení systému Security Onion. Jednotlivé verze se liší ve výkonu, úložišti, datové propustnosti a ceně. [66]

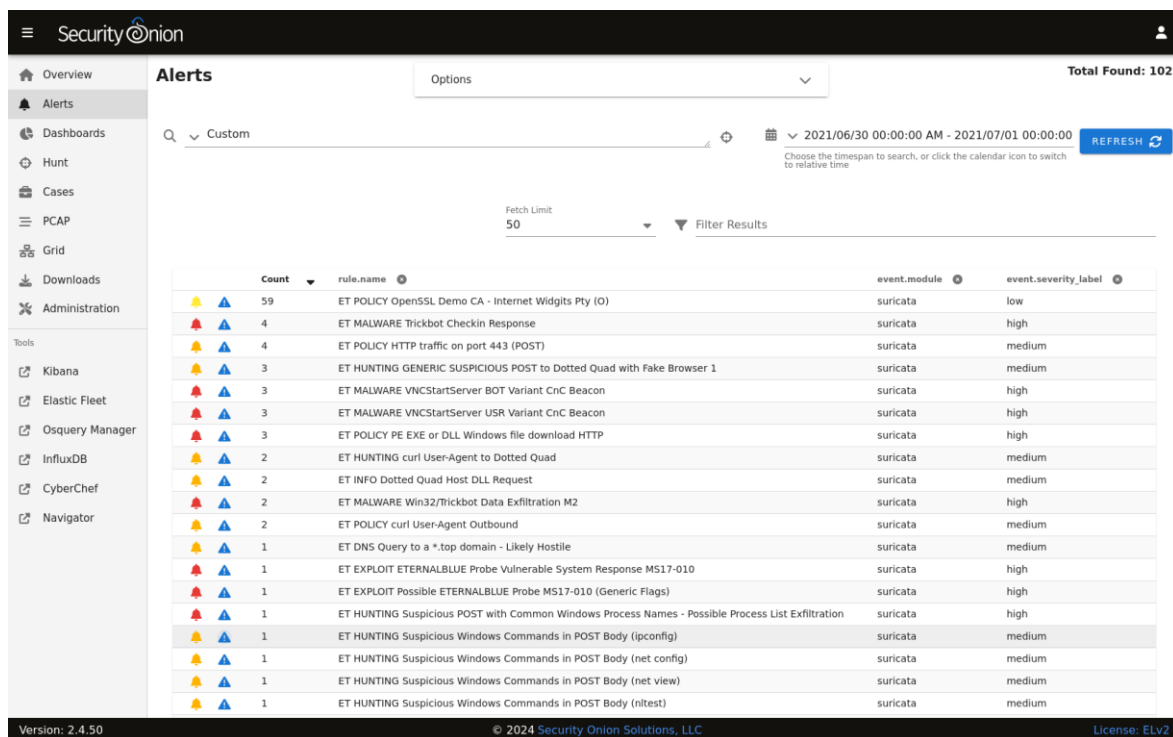


Obrázek 22 - SOS 1000F Zdroj: [67]

Suricata

Suricata funguje jako detekční (IDS) i prevenční (IPS) systém. Funguje tak, že v reálném čase monitoruje síťový provoz, ze kterého identifikuje potenciální hrozby a útoky. Komunikaci porovnává se známými útoky a hledá odchylky od běžného chování. K tomu využívá sadu pravidel, která je pravidelně aktualizována. Díky analýze aplikační vrstvy je schopen detekovat protokoly i na nestandardních portech. [68] [69]

Suricatu používá například Security Onion a je součástí dalších ucelených řešení pro zabezpečení počítačových sítí. Příklad výstupu je vidět na obrázku 23. [70]



The screenshot shows the Security Onion Alerts dashboard. The interface includes a sidebar with navigation options like Overview, Alerts, Dashboards, Hunt, Cases, PCAP, Grid, Downloads, and Administration. The main area displays a table of alerts with the following columns: Count, rule.name, event.module, and event.severity_label. The table contains 20 rows of alert data, each with a count, a rule name, the event module (all 'suricata'), and a severity label (low, high, or medium). The interface also shows a search bar, a date range selector (2021/06/30 00:00:00 AM - 2021/07/01 00:00:00), a refresh button, and a filter results button.

Count	rule.name	event.module	event.severity_label
59	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)	suricata	low
4	ET MALWARE Trickbot Checkin Response	suricata	high
4	ET POLICY HTTP traffic on port 443 (POST)	suricata	medium
3	ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1	suricata	medium
3	ET MALWARE VNCStartServer BOT Variant CnC Beacon	suricata	high
3	ET MALWARE VNCStartServer USR Variant CnC Beacon	suricata	high
3	ET POLICY PE EXE or DLL Windows file download HTTP	suricata	high
2	ET HUNTING curl User-Agent to Dotted Quad	suricata	medium
2	ET INFO Dotted Quad Host DLL Request	suricata	medium
2	ET MALWARE Win32/Trickbot Data Exfiltration M2	suricata	high
2	ET POLICY curl User-Agent Outbound	suricata	medium
1	ET DNS Query to a *.top domain - Likely Hostile	suricata	medium
1	ET EXPLOIT ETERNALBLUE Probe Vulnerable System Response MS17-010	suricata	high
1	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	suricata	high
1	ET HUNTING Suspicious POST with Common Windows Process Names - Possible Process List Exfiltration	suricata	high
1	ET HUNTING Suspicious Windows Commands in POST Body (ipconfig)	suricata	medium
1	ET HUNTING Suspicious Windows Commands in POST Body (net config)	suricata	medium
1	ET HUNTING Suspicious Windows Commands in POST Body (net view)	suricata	medium
1	ET HUNTING Suspicious Windows Commands in POST Body (nlist)	suricata	medium

Obrázek 23 – Upozornění v systému Security Onion Zdroj: [70]

Snort

Snort, stejně jako Suricata, funguje jako detekční (IDS) i prevenční (IPS) systém. Analyzuje v reálném čase síťovou komunikaci a porovnává ji s databází signatur známých útoků. Odhaluje pokusy o průnik a generuje upozornění nebo na základě pravidel automaticky provádí akce k jejich blokování. [71] [72]

Snort může fungovat ve třech režimech. První jen zachytává síťovou komunikaci a zobrazuje ji. Druhý ji ukládá pro možnost pozdější offline analýzy. Třetím režimem je samotný Network Intrusion Detection System. [71] [72]

Databáze pravidel je distribuována ve dvou sadách. Placená verze je vyvíjena společností *Cisco Talos*, která spadá pod *Cisco Systems Inc.* Bezplatná verze je tvořena komunitou. [71] [73]

Fail2Ban

Fail2Ban je IPS nástroj navržený k ochraně Linuxových serverů před útoky cílenými na heslo. Jeho hlavní funkcí je sledování logů protokolů jako SSH, FTP nebo HTTP, kdy detekuje opakované neúspěšné pokusy o přihlášení a následně blokuje zdrojovou IP adresu, aby zamezil potenciálně škodlivým aktivitám útočníka. [74]

4 Vlastní práce

Praktická část diplomové práce se věnuje provedení konkrétních kybernetických útoků a implementace ochrany na reálných příkladech. Pro ukázkou možného postupu útočníka je navržen scénář, který obsahuje jednotlivé kroky útočníka, jeho možné postupy a provedené útoky. Proti těmto krokům jsou následně navrženy postupy a konfigurace za využití různých systémů a síťových prvků.

4.1 Přístup do sítě

K přístupu do počítačové sítě může útočník využít volně dostupnou síťovou zásuvku nebo odpojit některé zařízení a využít jeho připojení. Už jen samotné připojení mu může poskytnout důležité informace o infrastruktuře. Analýza síťové komunikace mu napoví, jaké zařízení v síti jsou a jaké jsou jejich role.

4.1.1 Obrana

Identifikace cizích zařízení je možná například na druhé vrstvě podle MAC adres. Povoláním pouze známých legitimních zařízení lze automaticky blokovat ty potenciálně nebezpečné.

Zařízení Cisco

Cisco ve svých zařízeních umožňuje nastavení zabezpečení portů na základě MAC adres standardně. Konfigurace se provádí na konkrétních portech a stačí k ní jen několik málo kroků, které jsou provedeny v následujícím příkladu. Použitým hardwarem je L3 switch Cisco Catalyst 3650 24 PoE+ 4X1G.

V konfiguračním režimu je třeba vybrat interface, na který se zabezpečení má aplikovat.

```
Switch(config)# interface gigabitEthernet 1/0/24
```

Port je nutné mít v módu access, který je určený pro koncová zařízení (počítače, servery, IP telefony apod.). U běžných L2 switchů je tento mód výchozí, ale v případě L3 switchu je nutné tento mód zvolit místo výchozího dynamického.

```
Switch(config-if)# switchport mode access
```

Zabezpečení portu je nutné zapnout.

```
Switch(config-if)# switchport port-security
```

Počet povolených MAC adres je možné zvolit různě. U sítí, kde je k přepínači připojen pouze koncový počítač, stačí povolit jednu adresu. Naopak v případě použití IP telefonu a počítače na jednom portu je nutné povolit adresy dvě. V tomto příkladu je povoleno pouze jedno zařízení.

```
Switch(config-if)# switchport port-security maximum 1
```

Nastavení, které MAC adresy mají být povolené, je možné několika způsoby. Prvním je ruční definování.

```
Switch(config-if)# switchport port-security mac-address 0001.1617.322a
```

Cisco zařízení také podporují automatické nastavení právě připojeného zařízení jako toho povoleného.

```
Switch(config-if)# switchport port-security mac-address sticky
```

Akci, která má nastat při porušení pravidla, si uživatel může vybrat ze tří možností.

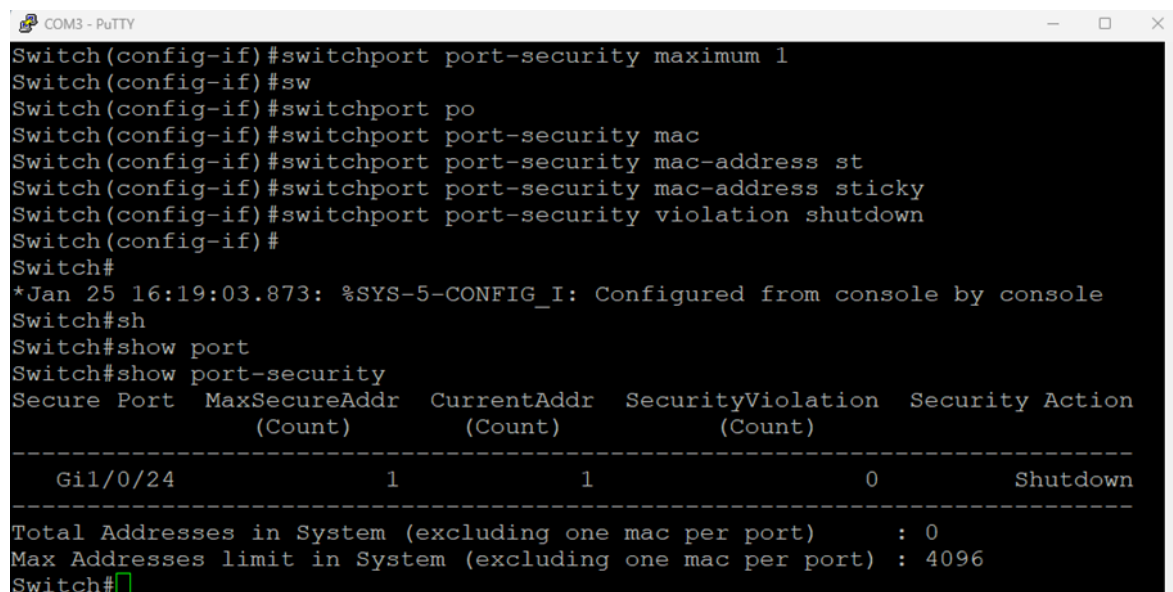
- shutdown – kompletně vypne daný port, výchozí stav
- restrict – port zůstává zapnutý, blokuje komunikaci a posílá SNMP zprávu
- protect – port zůstává zapnutý, blokuje komunikaci a neposílá SNMP zprávu

V tomto příkladě můžeme port vypnout a zamezit tak i dalším pokusům útočníka toto pravidlo obejít.

```
Switch(config-if)# switchport port-security violation shutdown
```

Kompletní výpis konfigurace port-security je dostupný pomocí příkazu

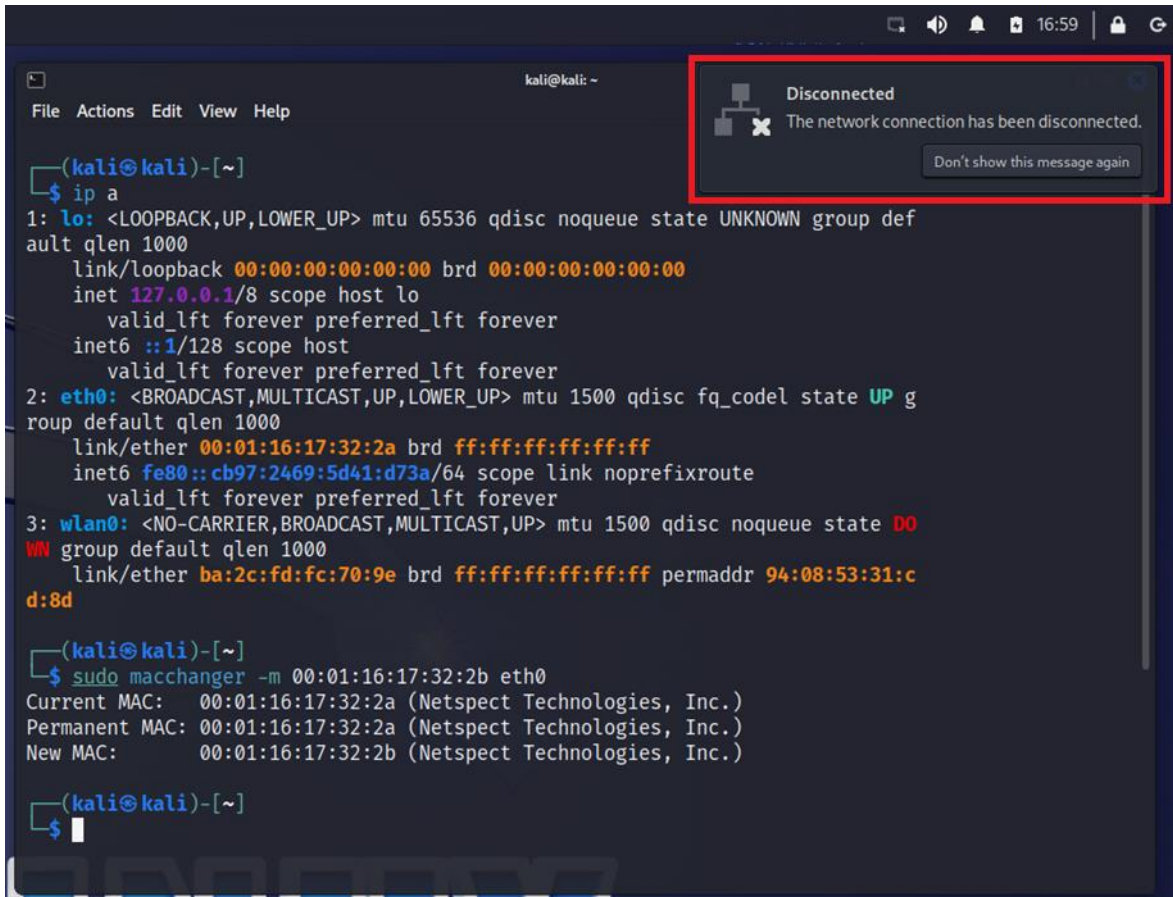
```
Switch# show port-security
```



```
COM3 - PuTTY
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#sw
Switch(config-if)#switchport po
Switch(config-if)#switchport port-security mac
Switch(config-if)#switchport port-security mac-address st
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#
Switch#
*Jan 25 16:19:03.873: %SYS-5-CONFIG_I: Configured from console by console
Switch#sh
Switch#show port
Switch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
          (Count)             (Count)             (Count)
-----
    Gi1/0/24             1             1             0             Shutdown
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

Obrázek 24 – Zobrazení konfigurace port-security Zdroj: [vlastní zpracování]

Připojení útočníka je možné simulovat změnou MAC adresy pomocí nástroje *macchanger*. Změna je ihned detekována a operační systém informuje o odpojení ze sítě.



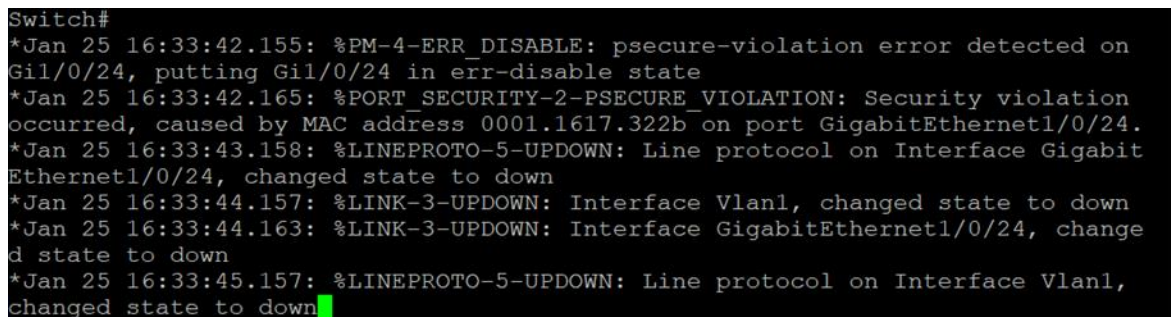
```
(kali@kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:01:16:17:32:2a brd ff:ff:ff:ff:ff:ff
    inet6 fe80::cb97:2469:5d41:d73a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DO
WN group default qlen 1000
    link/ether ba:2c:fd:fc:70:9e brd ff:ff:ff:ff:ff:ff permaddr 94:08:53:31:c
d:8d

(kali@kali)-[~]
└─$ sudo macchanger -m 00:01:16:17:32:2b eth0
Current MAC: 00:01:16:17:32:2a (Netspect Technologies, Inc.)
Permanent MAC: 00:01:16:17:32:2a (Netspect Technologies, Inc.)
New MAC: 00:01:16:17:32:2b (Netspect Technologies, Inc.)

(kali@kali)-[~]
└─$
```

Obrázek 25 – Změna MAC adresy Zdroj: [vlastní zpracování]

V logu přepínače je vidět informace o porušení pravidla a o vypnutí daného portu.



```
Switch#
*Jan 25 16:33:42.155: %PM-4-ERR_DISABLE: psecure-violation error detected on
Gil/0/24, putting Gil/0/24 in err-disable state
*Jan 25 16:33:42.165: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address 0001.1617.322b on port GigabitEthernet1/0/24.
*Jan 25 16:33:43.158: %LINEPROTO-5-UPDOWN: Line protocol on Interface Gigabit
Ethernet1/0/24, changed state to down
*Jan 25 16:33:44.157: %LINK-3-UPDOWN: Interface Vlan1, changed state to down
*Jan 25 16:33:44.163: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, change
d state to down
*Jan 25 16:33:45.157: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to down
```

Obrázek 26 – Log při porušení port-security pravidla Zdroj: [vlastní zpracování]

Bližší informace je možné zobrazit ve stavu port-security na vybraném portu, kde je vidět stav portu jako *Secure-shutdown*.


```

Switch#show port-security interface g1/0/24
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0001.1617.322b:1
Security Violation Count : 1

```

Obrázek 27 – Stav port-security po porušení pravidla Zdroj: [vlastní zpracování]

Status portu se liší oproti běžnému manuálnímu vypnutí.

```

Switch#show interfaces g1/0/24 status

```

Port	Name	Status	Vlan	Duplex	Speed	Type
Gil/0/24		err-disabled	1	auto	auto	10/100/1000BaseTX

```

Switch#

```

Obrázek 28 – Status portu po porušení pravidla Zdroj: [vlastní zpracování]

Po opětovném připojení zařízení se správnou MAC adresou nedojde k obnovení komunikace. Port je zablokován a je třeba ho restartovat následujícími příkazy:

```
Switch(config-if)# shutdown
```

```
Switch(config-if)# no shutdown
```

Až poté může původní zařízení komunikovat v síti. Nutnost odblokování portu administrátorem zamezí situacím, kdy by za sebou chtěl útočník zamést stopy.

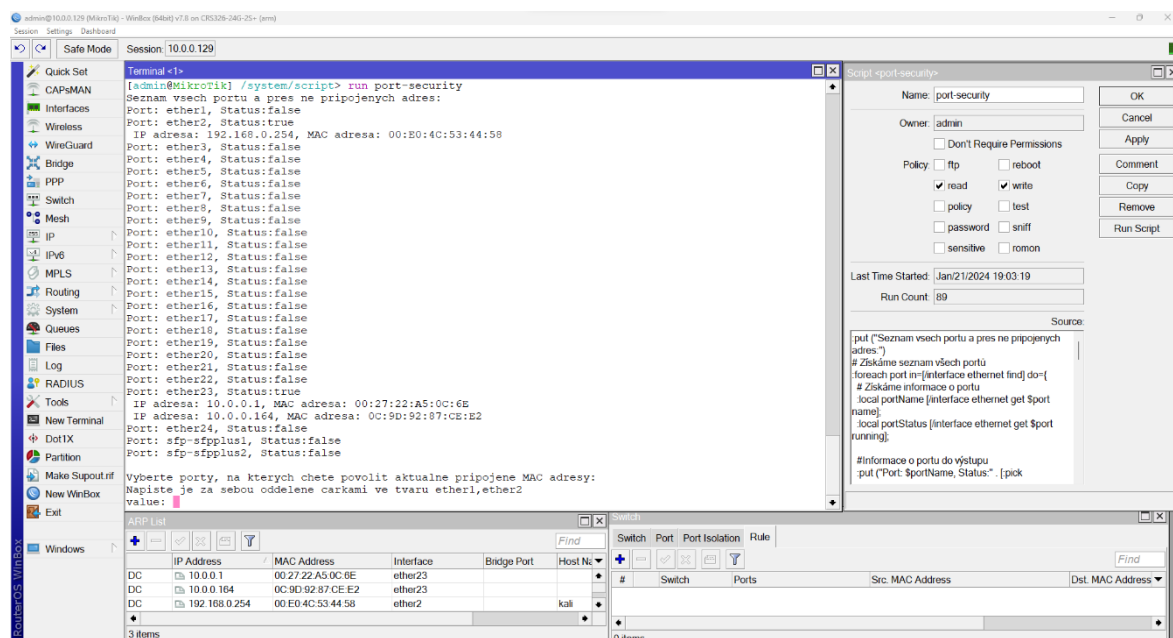
Tato část je zpracována dle [75].

Zařízení Mikrotik

Na zařízeních Mikrotik je filtrování MAC adres možné v záložce *Rule* položky *Switch*. V této části je možné nastavit různá pravidla přepínání na jednotlivých portech.

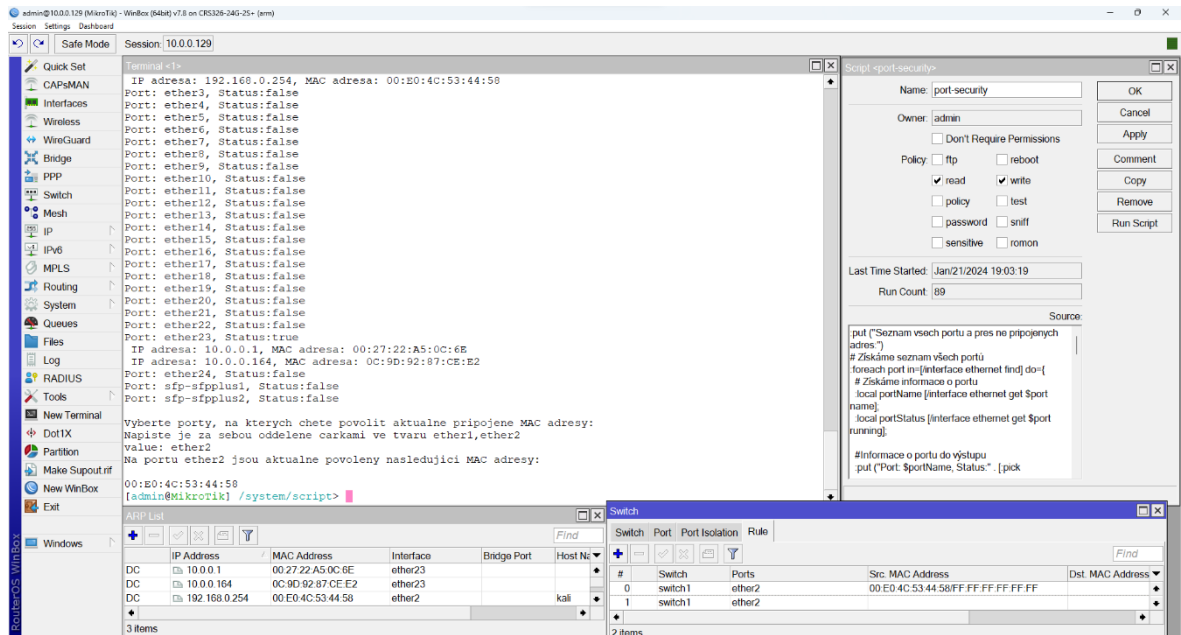
Oproti systému Cisco IOS neumožňuje automatické načtení MAC adresy zařízení připojené přes daný interface. Tu je nutné ručně zapsat do pravidel. Pro účely automatizace této operace byl navržen skript, který proces zjednodušuje. Skript je součástí této práci

jako Příloha A – Skript pro generování pravidel filtrování MAC adres na porty pro RouterOS.

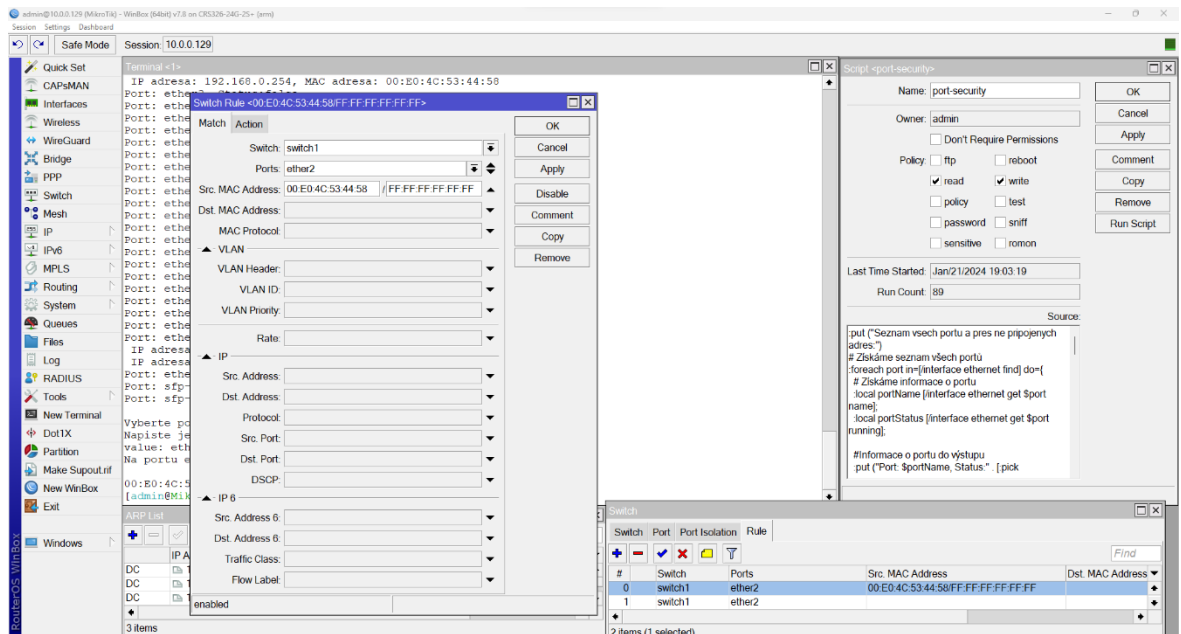


Obrázek 29 – Výpis portů a připojených zařízení Zdroj: [vlastní zpracování]

Skript vypíše všechny porty a k nim připojená zařízení a následně vyzve uživatele, aby zadal názvy portů, na kterých chce povolit pouze aktuálně připojené MAC adresy. Ty skript automaticky načte z ARP tabulky a vytvoří potřebná pravidla. Poté přidá pravidlo, které všechny ostatní zařízení zakáže.

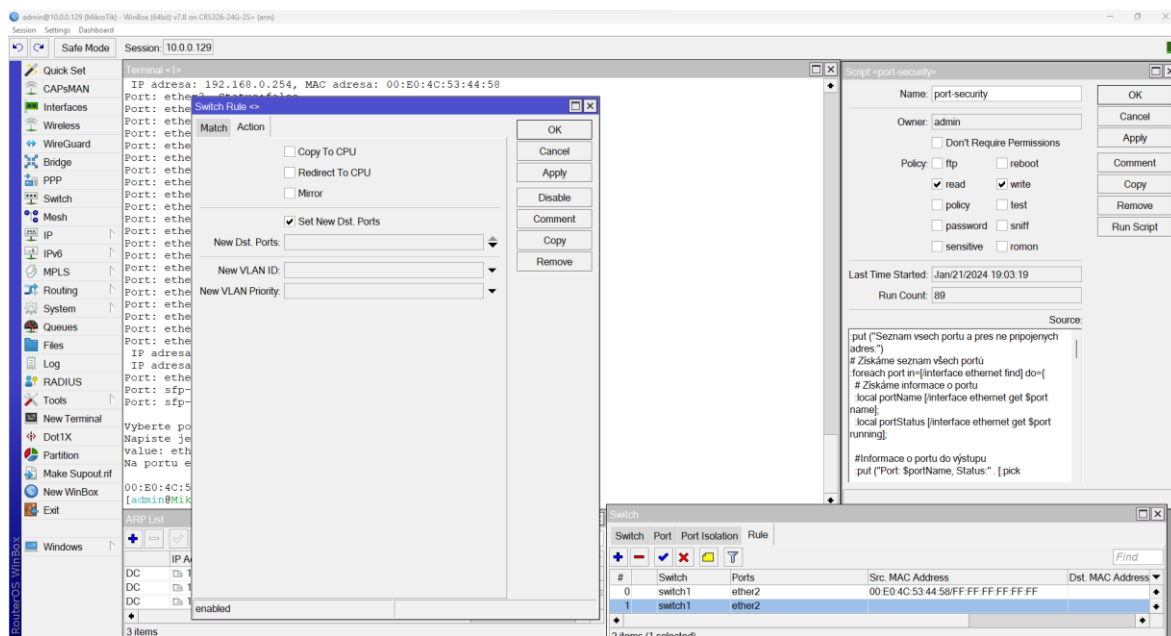


Obrázek 30 – Vytvoření pravidel pro vybraný port Zdroj: [vlastní zpracování]



Obrázek 31 – Detail pravidla pro povolení MAC adresy Zdroj: [vlastní zpracování]

První pravidlo povoluje komunikaci ze zdrojové MAC adresy vybraného zařízení.



Obrázek 32 – Pravidlo zakazující ostatní MAC adresy Zdroj: [vlastní zpracování]

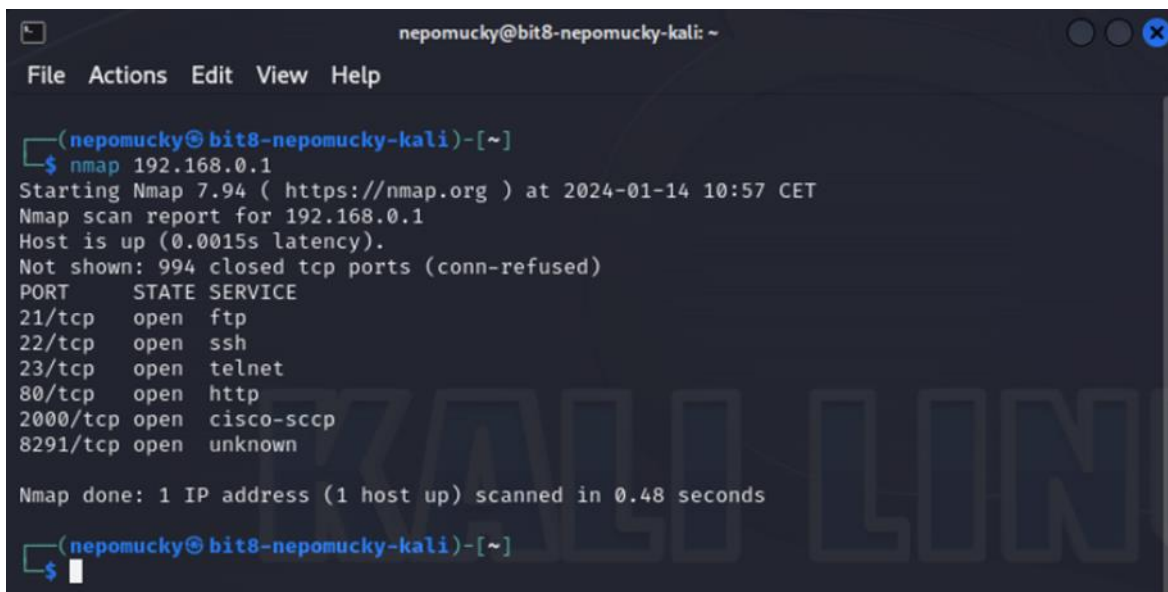
Druhé pravidlo neobsahuje definovanou zdrojovou adresu. Díky principu procházení First Fit se akce provede pro všechny ostatní adresy, které nejsou předchozími pravidly povoleny. Akcí je v tomto případě nastavení nového cílového portu, který není definován. Tím dojde k zablokování komunikace.

Díky cyklům umožňuje skript povolit více MAC adres na jednom portu. To se hodí například v případě používání IP telefonů, kdy je internetový kabel připojen z přepínače do telefonu a z něj následně do počítače zaměstnance. V takovém případě jsou přes jeden port připojena dvě zařízení – každé s jinou adresou.

Tento způsob implementace zabezpečení portů je samozřejmě možné provádět i ručně. Použití vytvořeného skriptu tento proces automatizuje, urychluje a pomáhá předejít chybám v konfiguracích, které mohou mít za následek i zablokování přístupu ke konfigurovanému zařízení. Skript byl otestován na zařízeních Cloud Router Switch model CRS326-24G-2S+IN se systémem RouterOS verze 7.8 a CRS328-4C-20S+RM se systémem RouterOS verze 6.49.

4.2 Skenování sítě

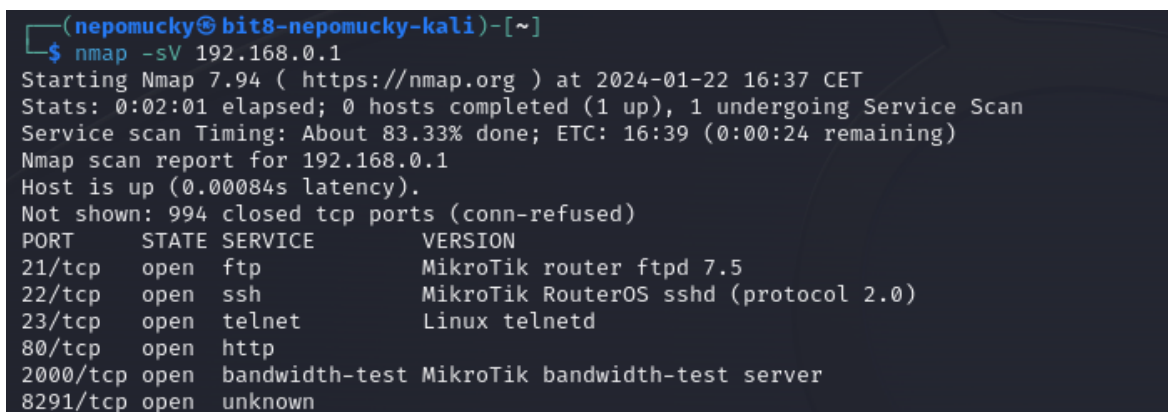
Aby útočník zjistil podrobnější informace o zařízeních v síti, jako například používané operační systémy, poskytované služby a jejich verze je nutné provést aktivní skenování sítě. K tomu může využít nástroj *Nmap*. Výsledkem je seznam portů a služeb, které na cílovém zařízení běží.



```
nepomucky@bit8-nepomucky-kali: ~  
File Actions Edit View Help  
  
(nepomucky@bit8-nepomucky-kali)-[~]  
$ nmap 192.168.0.1  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-14 10:57 CET  
Nmap scan report for 192.168.0.1  
Host is up (0.0015s latency).  
Not shown: 994 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
80/tcp    open  http  
2000/tcp  open  cisco-sccp  
8291/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds  
  
(nepomucky@bit8-nepomucky-kali)-[~]  
$
```

Obrázek 33 – Skenování služeb bez ochrany FW Zdroj: [vlastní zpracování]

Přidáním přepínače `-sV` je útočník schopen zjistit i verze těchto služeb. Takovou informaci může využít při hledání a zneužívání zranitelností.

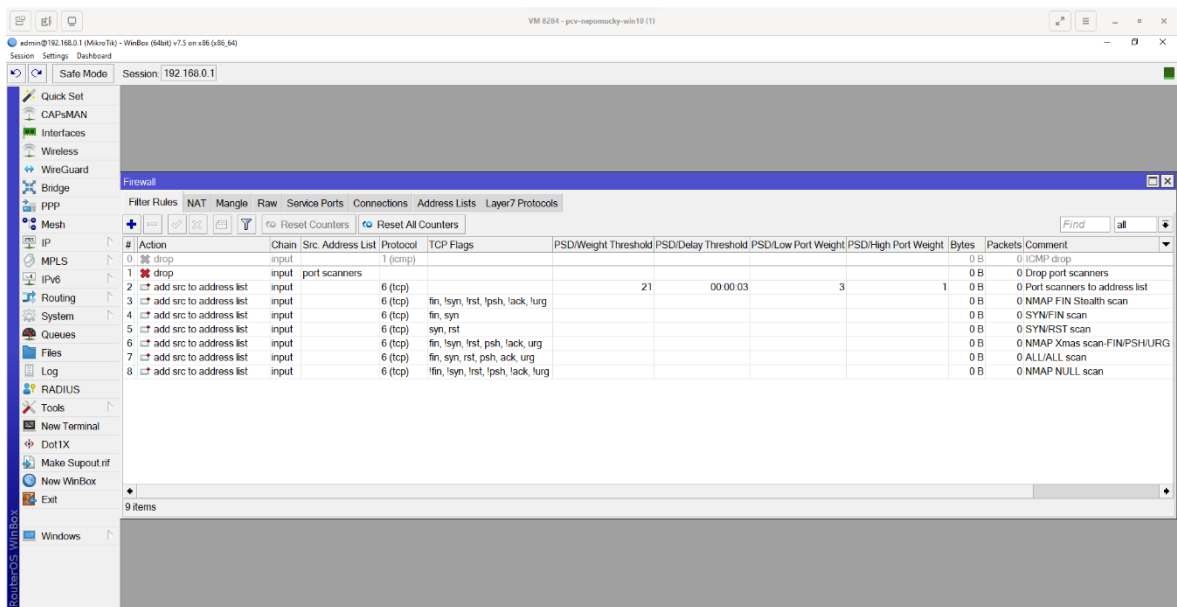


```
(nepomucky@bit8-nepomucky-kali)-[~]  
$ nmap -sV 192.168.0.1  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 16:37 CET  
Stats: 0:02:01 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 83.33% done; ETC: 16:39 (0:00:24 remaining)  
Nmap scan report for 192.168.0.1  
Host is up (0.00084s latency).  
Not shown: 994 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          MikroTik router ftpd 7.5  
22/tcp    open  ssh         MikroTik RouterOS sshd (protocol 2.0)  
23/tcp    open  telnet      Linux telnetd  
80/tcp    open  http  
2000/tcp  open  bandwidth-test MikroTik bandwidth-test server  
8291/tcp  open  unknown
```

Obrázek 34 – Detekce verzí služeb bez ochrany FW Zdroj: [vlastní zpracování]

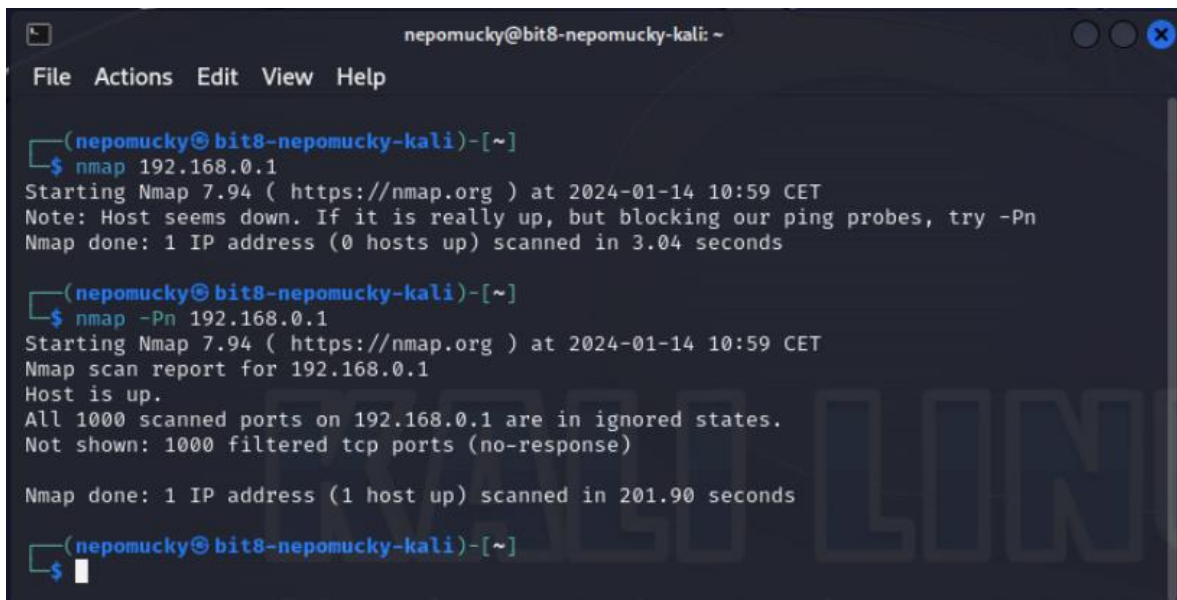
2. Pokud během tří sekund uživatel vytvoří spojení s celkovým skóre 21, přičemž se při každém novém spojení na portu menším než 1024 přičte číslo 3 a při portu 1024 a vyšším přičte číslo 1, přidá se jeho IP adresa na seznam blokových. Toto pravidlo odhalí většinu běžných skenů.
3. Detekce FIN skenu
4. Detekce SYN/FIN skenu
5. Detekce SYN/RST skenu
6. Detekce NMAP Xmas skenu
7. Detekce ALL/ALL skenu
8. Detekce NMAP NULL skenu

IP adresa útočníka se do seznamu přidává na 14 dnů.



Obrázek 36 – Konfigurace firewallu Zdroj: [vlastní zpracování]

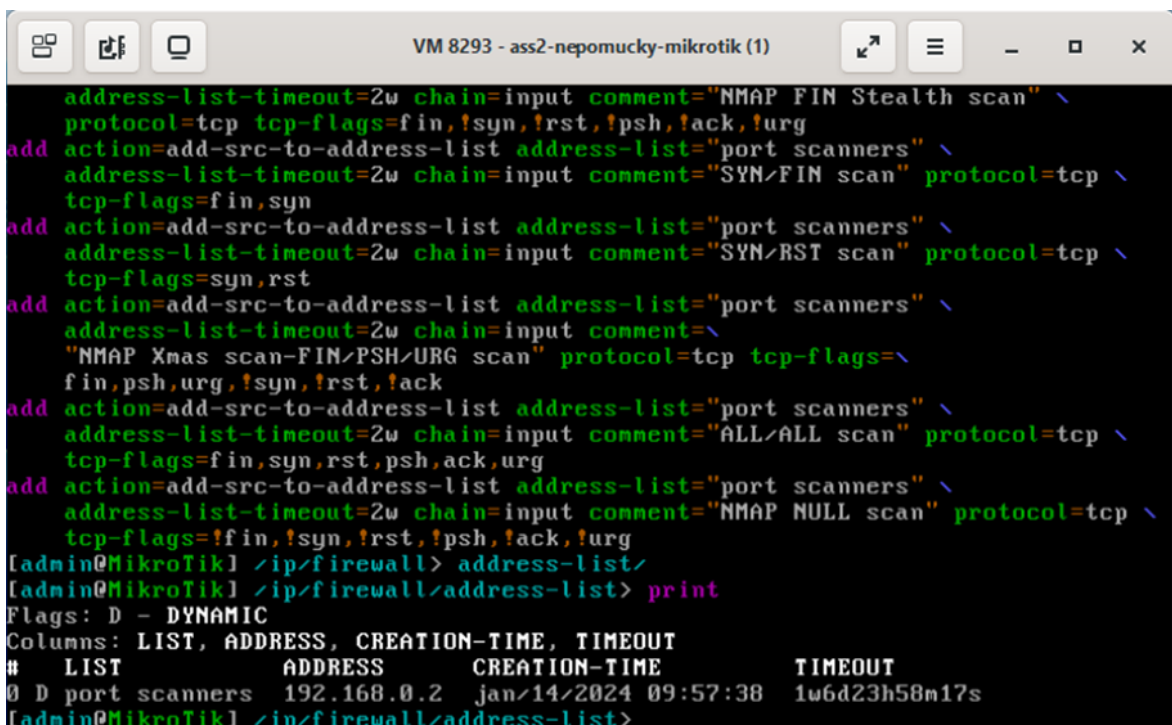
Při opětovném provedení skenu je vidět, že útočník žádné informace o cílovém zařízení nezíská.



```
nepomucky@bit8-nepomucky-kali: ~  
File Actions Edit View Help  
  
(nepomucky@bit8-nepomucky-kali)-[~]  
$ nmap 192.168.0.1  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-14 10:59 CET  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds  
  
(nepomucky@bit8-nepomucky-kali)-[~]  
$ nmap -Pn 192.168.0.1  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-14 10:59 CET  
Nmap scan report for 192.168.0.1  
Host is up.  
All 1000 scanned ports on 192.168.0.1 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
  
Nmap done: 1 IP address (1 host up) scanned in 201.90 seconds  
  
(nepomucky@bit8-nepomucky-kali)-[~]  
$
```

Obrázek 37 – Pokus o útok s ochranou FW Zdroj: [vlastní zpracování]

V seznamu adres je vidět IP adresa útočníka, která na něm zůstane dva týdny. Po tuto dobu bude veškerá jeho komunikace zablokována tak, jak je nastaveno ve firewall pravidle.



```
VM 8293 - ass2-nepomucky-mikrotik (1)  
address-list-timeout=2w chain=input comment="NMAP FIN Stealth scan" \  
protocol=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg  
add action=add-src-to-address-list address-list="port scanners" \  
address-list-timeout=2w chain=input comment="SYN/FIN scan" protocol=tcp \  
tcp-flags=fin,syn  
add action=add-src-to-address-list address-list="port scanners" \  
address-list-timeout=2w chain=input comment="SYN/RST scan" protocol=tcp \  
tcp-flags=syn,rst  
add action=add-src-to-address-list address-list="port scanners" \  
address-list-timeout=2w chain=input comment=\  
"NMAP Xmas scan-FIN/PSH/URG scan" protocol=tcp tcp-flags=\  
fin,psh,urg,!syn,!rst,!ack  
add action=add-src-to-address-list address-list="port scanners" \  
address-list-timeout=2w chain=input comment="ALL/ALL scan" protocol=tcp \  
tcp-flags=fin,syn,rst,psh,ack,urg  
add action=add-src-to-address-list address-list="port scanners" \  
address-list-timeout=2w chain=input comment="NMAP NULL scan" protocol=tcp \  
tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg  
[admin@MikroTik] /ip/firewall> address-list/  
[admin@MikroTik] /ip/firewall/address-list> print  
Flags: D - DYNAMIC  
Columns: LIST, ADDRESS, CREATION-TIME, TIMEOUT  
# LIST ADDRESS CREATION-TIME TIMEOUT  
0 D port scanners 192.168.0.2 jan/14/2024 09:57:38 1w6d23h58m17s  
[admin@MikroTik] /ip/firewall/address-list>
```

Obrázek 38 – Zablokováná IP adresa útočníka Zdroj: [vlastní zpracování]

Ochrana úspěšně zablokovala skenování sítě za využití různých typů skenů.

Směrovače společnosti Cisco nativně neobsahují mechanismy, které by skenování detekovaly a blokovaly. Výrobce tuto funkci implementoval do firewallů, které se do sítě nasazují zvlášť. [76]

4.3 Útok na heslo přes protokol SSH

Když útočník zjistí, jaké zařízení v síti jsou, může zkusit prolomit jejich zabezpečení. Změnou konfigurace by ovlivnil fungování sítě a převzal nad ní kontrolu. Pro prolomení vzdáleného přístupu přes protokol SSH lze využít například slovníkový útok.

K jeho provedení byl použit nástroj *Hydra*. Cílem bylo zjištění hesla pro vzdálený přístup protokolem SSH. Uživatelské jméno bylo definováno jako *root*. Soubor *wordlist-ssh* obsahuje slovník s často používanými hesly, ve kterém je pro tento příklad obsaženo i heslo používané – *Abcdef0*. Útok je postupně proveden na server s OS AlmaLinux, router Mikrotik a L3 switch Cisco.

Na všech zařízeních je nakonfigurována služba SSH umožňující vzdálený přístup. Parametrem útoku je přihlašovací jméno, slovník hesel, cílová IP adresa a protokol. Na obrázku 39 je vidět celý průběh útoku včetně úspěšně zjištěného hesla. Útok byl úspěšně proveden na všech vybraných prvcích.

```
nepomucky@bit8-nepomucky-kali: ~
File Actions Edit View Help

(nepomucky@bit8-nepomucky-kali)-[~]
$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.953 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.483 ms
^C
— 192.168.0.1 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.483/0.718/0.953/0.235 ms

(nepomucky@bit8-nepomucky-kali)-[~]
$ nano wordlist-ssh

(nepomucky@bit8-nepomucky-kali)-[~]
$ hydra -l root -P wordlist-ssh 192.168.0.1 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not
use in military or secret service organizations, or for illegal pur
poses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-0
1-23 01:13:52
[WARNING] Many SSH configurations limit the number of parallel tasks,
it is recommended to reduce the tasks: use -t 4
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l
:1/p:12), ~1 try per task
[DATA] attacking ssh://192.168.0.1:22/
[22][ssh] host: 192.168.0.1 login: root password: Abcdef0
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-0
1-23 01:13:57

(nepomucky@bit8-nepomucky-kali)-[~]
$
```

Obrázek 39 – Provedení slovníkového útoku bez ochrany Zdroj: [vlastní zpracování]

4.3.1 Ochrana Linux serveru

Jedním ze způsobů obrany před slovníkovým útokem je omezení počtu pokusů. K tomu je vhodný například IPS nástroj *Fail2Ban*, který útočníka po několika neúspěšných pokusech zablokuje.

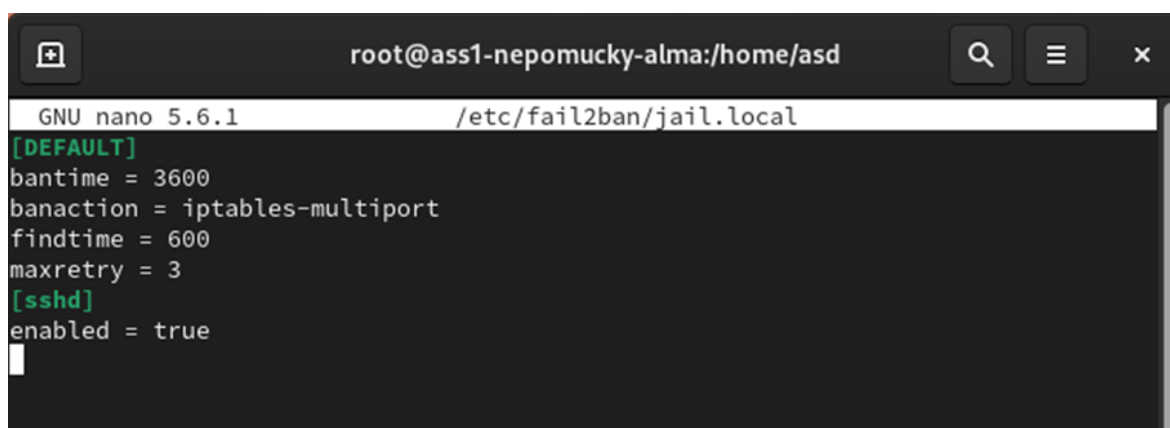
Instalace a konfigurace je jednoduchá, nejprve je nutné stáhnout potřebné balíčky následujícím příkazem:

```
yum install epel-release
```

Poté je možné stáhnout samotný Fail2Ban:

```
yum install fail2ban
```

Konfigurace se provádí v souboru */etc/fail2ban/jail.local*.



```
root@ass1-nepomucky-almal:/home/asd
GNU nano 5.6.1 /etc/fail2ban/jail.local
[DEFAULT]
bantime = 3600
banaction = iptables-multiport
findtime = 600
maxretry = 3
[sshd]
enabled = true
```

Obrázek 40 – Konfigurace Fail2Ban Zdroj: [vlastní zpracování]

Na obrázku 40 je vidět konfigurace, která zablokuje uživatele na 1 hodinu po třetím neúspěšném pokusu o přihlášení přes SSH, který provedl během 10 minut.

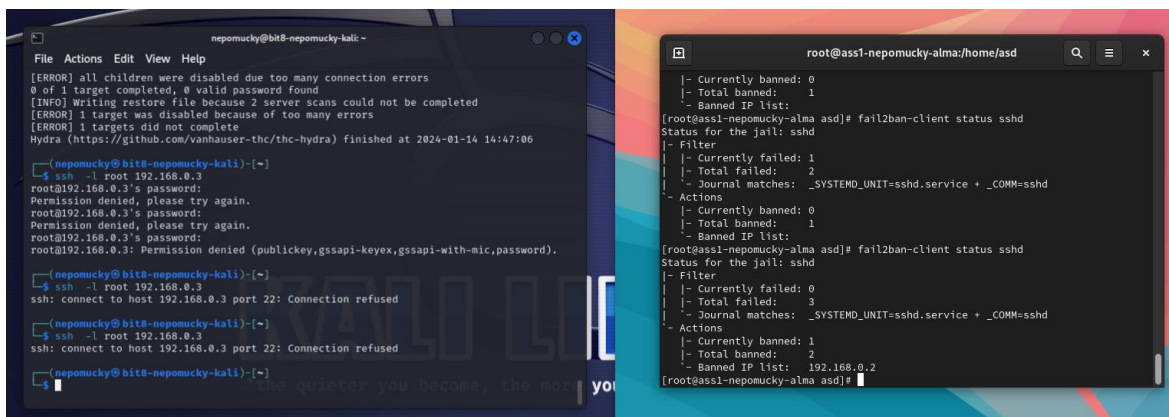
Po změně nastavení je nutné službu restartovat, aby se projevil změny, příkazem

```
systemctl restart fail2ban
```

Službu je vhodné nastavit tak, aby se spouštěla automaticky při startu systému.

```
systemctl enable fail2ban
```

Na obrázku 41 je vidět zablokování IP adresy po neúspěšných pokusech. Stejný proces by následoval i při slovníkovém útoku, který jen pokusy provádí automaticky.



Obrázek 41 – Zablokování IP po neúspěšných pokusech Zdroj: [vlastní zpracování]

Pravidlo firewallu, které komunikaci blokuje, je možné vidět například příkazem

iptables -L



Obrázek 42 – Zablokování IP adresy v iptables Zdroj: [vlastní zpracování]

4.3.2 Ochrana routeru Mikrotik

V systému RouterOS je ochrana před útokem implementována pomocí následujících pěti firewallových pravidel:

```
add chain=input protocol=tcp dst-port=22  
src-address-list=ssh_blacklist action=drop
```

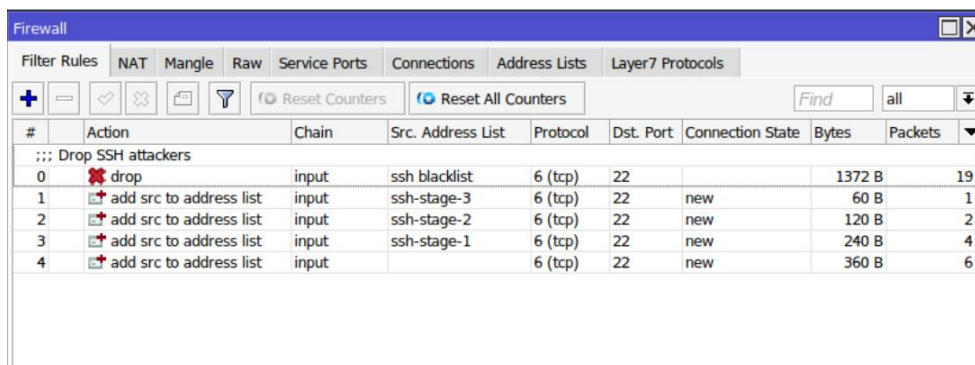
```
add chain=input protocol=tcp dst-port=22 connection-state=new  
src-address-list=ssh_stage_3 action=add-src-to-address-list  
address-list=ssh_blacklist address-list-timeout=14d
```

```
add chain=input protocol=tcp dst-port=22 connection-state=new  
src-address-list=ssh_stage_2 action=add-src-to-address-list  
address-list=ssh_stage_3 address-list-timeout=1m
```

```
add chain=input protocol=tcp dst-port=22 connection-state=new  
src-address-list=ssh_stage_1 action=add-src-to-address-list  
address-list=ssh_stage_2 address-list-timeout=1m
```

```
add chain=input protocol=tcp dst-port=22 connection-state=new  
action=add-src-to-address-list address-list=ssh_stage_1  
address-list-timeout=1m
```

Princip je založen na faktu, že pro pokus o přihlášení je nutné navázat spojení. Poté má uživatel tři pokusy na heslo, které když nezadá správně, je následně odpojen. Pro další pokusy je nutné proces opakovat a navazovat další spojení. Pravidla je v tomto případě vhodné vysvětlit od posledního, protože jimi uživatel v takovém pořadí prochází.



#	Action	Chain	Src. Address List	Protocol	Dst. Port	Connection State	Bytes	Packets
;;; Drop SSH attackers								
0	drop	input	ssh_blacklist	6 (tcp)	22		1372 B	19
1	add src to address list	input	ssh-stage-3	6 (tcp)	22	new	60 B	1
2	add src to address list	input	ssh-stage-2	6 (tcp)	22	new	120 B	2
3	add src to address list	input	ssh-stage-1	6 (tcp)	22	new	240 B	4
4	add src to address list	input		6 (tcp)	22	new	360 B	6

Obrázek 43 – Firewall pravidla pro ochranu před slovníkovým útokem na SSH Zdroj: [vlastní zpracování]

Poslední pravidlo detekuje první pokus o připojení pomocí SSH. Zdrojová IP adresa je na jednu minutu uložena na seznam „ssh_stage_1“. Pokud uživatel během této minuty naváže další spojení, je podle adresy na seznamu detekováno, že se jedná o další pokus a jeho IP adresa se přidá na seznam „ssh_stage_2“. Stejný principem se detekuje i další pokus, kdy je využit seznam „ssh_stage_3“. Pokud i po devíti pokusech, které jsou rozděleny do tří fází, klient znovu vytvoří během minuty další spojení, je na dva týdny přidán na blacklist a komunikace na SSH portu 22 je blokována. Alternativní akcí může být zablokování veškeré komunikace, která by útočnickovi zablokovala další útoky na zařízení nebo další prvky v síti.

Pořadí je úmyslně zvoleno od nejvyšší úrovně kvůli principu procházení pravidel od prvního s provedením akce v případě splnění podmínek. V opačném pořadí by se útočník nikdy nedostal do dalších fází. Tímto stylem je možné pracovat s libovolným časovým úsekem a trojicích pokusů o spojení a přihlášení.

Tato část je zpracována dle [77].

4.3.3 Ochrana L3 přepínače Cisco

Síťové prvky společnosti Cisco umožňují automatické zablokování dalších pokusů o přihlášení po několika chybných přihlášeních. Zařízení se na zvolenou dobu přepne do stavu *Quiet-Mode*. Během něho se aplikují Access Control List pravidla blokující vybranou komunikaci. Po uplynutí této doby se prvek přepne zpět do standardního režimu, který je označen jako *Normal-Mode*.

Konfigurace se provádí následujícím příkazem:

```
CiscoL3(config)# login block-for 600 attempts 3 within 60
```

Tento příklad blokuje danou komunikaci na 10 minut, pokud dojde ke 3 neúspěšným pokusům během jedné minuty. Pokud není nastaveno jinak, zařízení automaticky vytvoří ACL blokující komunikaci na port 23 (telnet), 80 (HTTP) a 22 (SSH).

```
CiscoL3#show ip access-lists | section sl_def_acl
Extended IP access list sl_def_acl
 10 deny tcp any any eq telnet
 20 deny tcp any any eq www
 30 deny tcp any any eq 22
 40 permit ip any any
```

Obrázek 44 – ACL pravidla aplikovaná během stavu *Quiet-Mode* Zdroj: [vlastní zpracování]

Na obrázku 44 je vidět, že spojení je blokováno ze všech zdrojů, nejen z toho, odkud byly provedeny neúspěšné pokusy. Ovlivnění jsou tedy i ostatní klienti, nejen potenciální útočník. Pravidla je možné upravit nebo zvolit vlastní seznam následujícím příkazem:

```
CiscoL3(config)# login quiet-mode access-class myacl
```

V tomto případě je „myacl“ název seznamu pravidel ACL.

Příkazem *show login* je možné zobrazit aktuální stav omezení přihlášení. Výchozí zpoždění pokusů o přihlášení je nastaveno na jednu sekundu. Není nastaven vlastní ACL pro stav *Quiet-Mode* a je zobrazena informace o aktuálním nastavení omezení pokusů o přihlášení. Ve spodní části je vidět aktuální režim, ve kterém se zařízení nachází, čas, který zbývá v daném cyklu, a počet neúspěšných pokusů o přihlášení.

```
CiscoL3#show login
  A default login delay of 1 seconds is applied.
  No Quiet-Mode access list has been configured.

  Router enabled to watch for login Attacks.
  If more than 3 login failures occur in 60 seconds or less,
  logins will be disabled for 600 seconds.

  Router presently in Normal-Mode.
  Current Watch Window remaining time 58 seconds.
  Present login failure count 0.
```

Obrázek 45 – Informace o omezení přihlášení Zdroj: [vlastní zpracování]

Pro otestování ochrany je navázáno připojení z klienta s OS Windows na IP adresu L3 přepínače. Následně je třikrát zadáno špatné heslo.

```
C:\Users\Ladislav Nepomucký>ssh -l root 192.168.0.1
Password:
Password:
Password:
Connection closed by 192.168.0.1 port 22

C:\Users\Ladislav Nepomucký>ssh -l root 192.168.0.1
ssh: connect to host 192.168.0.1 port 22: Connection refused
```

Obrázek 46 – Připojení pomocí SSH Zdroj: [vlastní zpracování]

Pokusu o navázání dalšího spojení Cisco switch ihned zablokuje.


```
*Feb 4 14:29:51.664: %SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for watching failure  
s is 5 secs, [user: root] [Source: 192.168.0.2] [localport: 22] [Reason: Login Authen  
tication Failed] [ACL: sl_def_acl] at 14:29:51 UTC Sun Feb 4 2024
```

Obrázek 47 – Log zpráva o přepnutí do režimu *Quiet-Mode* Zdroj: [vlastní zpracování]

Informace o přepnutí do stavu *Quiet-Mode* je zobrazena v logu konzole zařízení. Obsahuje i zdrojovou IP adresu, port a čas. Po vložení příkazu *show login* je vidět mimo stavu i doba, po kterou bude komunikace dle nastaveného ACL blokována.

```
CiscoL3#show login  
A default login delay of 1 seconds is applied.  
No Quiet-Mode access list has been configured.  
  
Router enabled to watch for login Attacks.  
If more than 3 login failures occur in 60 seconds or less,  
logins will be disabled for 600 seconds.  
  
Router presently in Quiet-Mode.  
Will remain in Quiet-Mode for 555 seconds.  
Denying logins from all sources.
```

Obrázek 48 – Informace o omezení přihlášení po neúspěšných pokusech Zdroj: [vlastní zpracování]

Administrátor má volnost v nastavování počtů pokusů, časů vyhrazených na ně, délky blokování a pravidel, která mají být aplikována. Nevýhodou může být blokování všech a zařízení a nejen toho, ze kterého neúspěšné pokusy šly. Vhodné je i nastavit zpoždění mezi pokusy o přihlášení, což pokusy o prolomení hesla ještě zpomalí. Tato část je zpracována dle [78].

4.4 Parazitní DHCP server

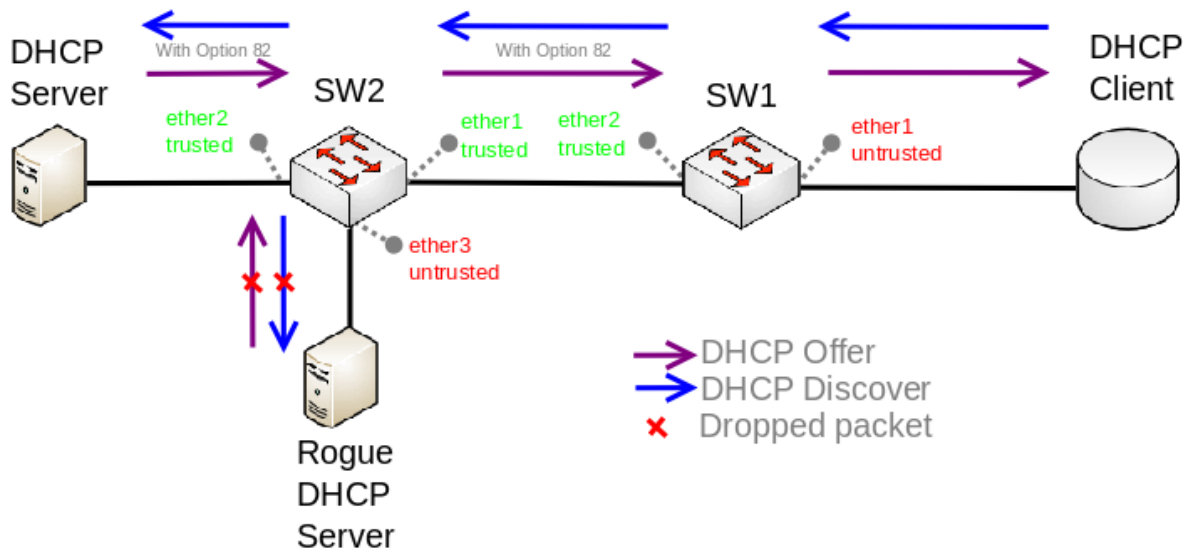
Pro převzetí kontroly nad koncovými body v síti jim může útočník nabídnout IP adresu, výchozí bránu a DNS server prostřednictvím svého parazitního (rouge) DHCP serveru, který stačí připojit do sítě. Díky tomu je schopen ovlivnit způsob komunikace a být prostředníkem mezi klientem a cílovým zařízením.

4.4.1 Obrana

DHCP Snooping funguje na druhé vrstvě jako ochrana před parazitními DHCP servery. Povoluje DHCP nabídky pouze od legitimních DHCP serverů a útočníka tím aktivně blokuje.

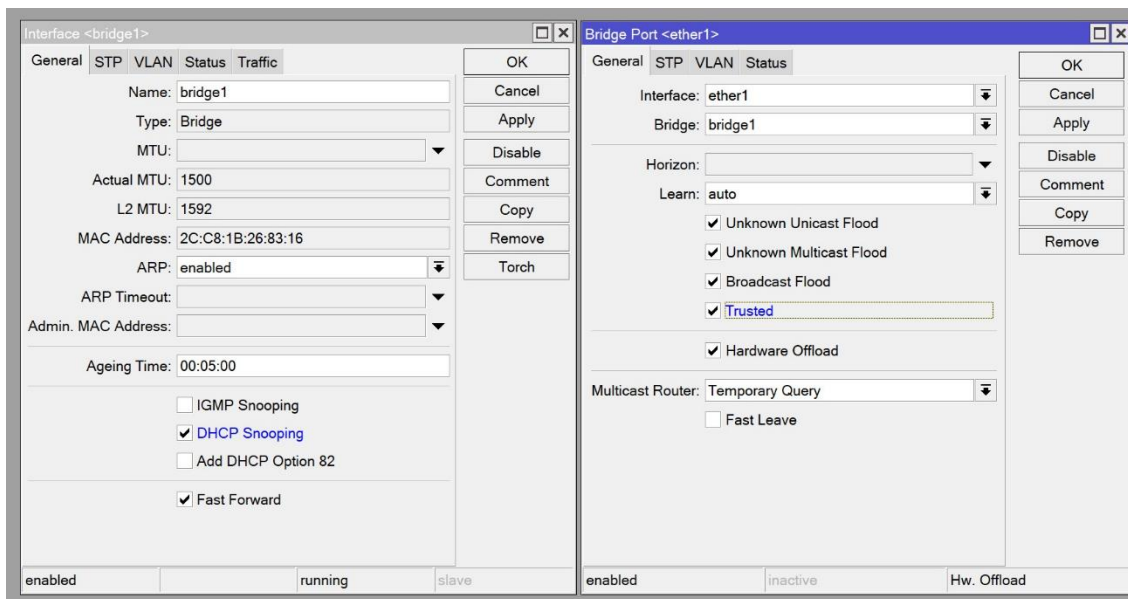
Mikrotik

RouterOS od verze 6.43 podporuje DHCP Snooping. Příklad nasazení je vidět na obrázku 49.



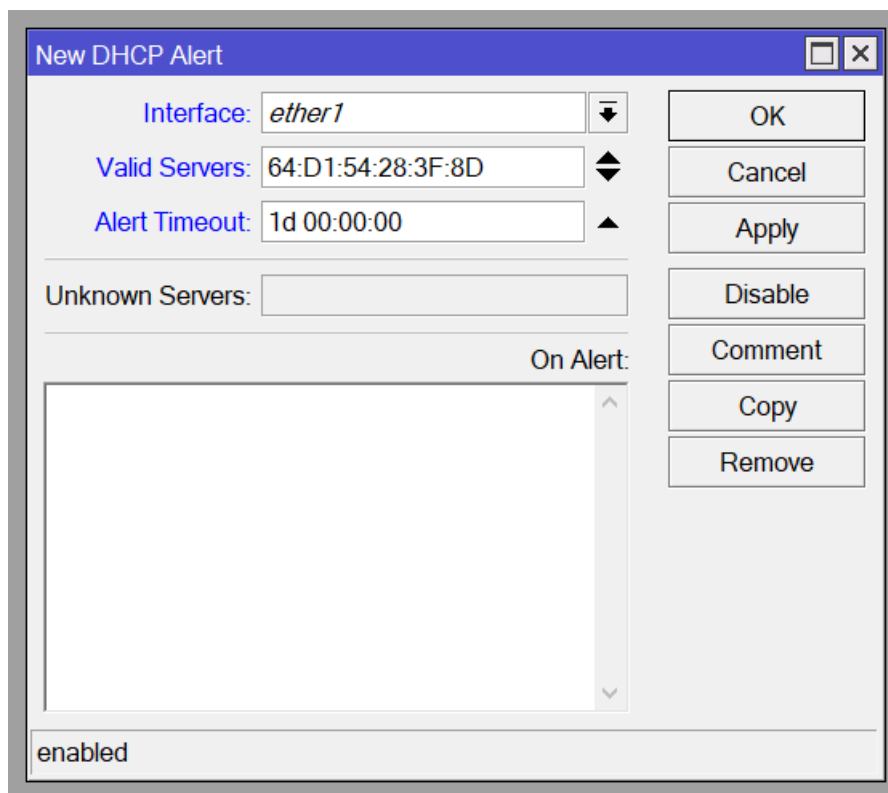
Obrázek 49 – DHCP Snooping a DHCP Option 82 Zdroj: [79]

Konfigurace se provádí v nastavení bridge. Po jeho rozkliknutí je možné ve spodní části zapnout *DHCP Snooping*. Poté je třeba ještě vybrat *Trusted* port, na kterým se DHCP server nachází nebo přes které porty je přístupný.



Obrázek 50 – Konfigurace DHCP Snooping Zdroj: [vlastní zpracování]

Pro rychlou detekci podvodných DHCP serverů lze využít i nástroj *DHCP Alert*. Ten umí monitorovat porty a v případě, že detekuje nový nebo neznámý DHCP server, se vytvoří výstraha (alert). Rovněž je možné automaticky spouštět další akce pomocí skriptů. Pole *Valid Servers* obsahuje MAC adresy známých a legitimních serverů. Tato možnost je nepovinná a umožňuje detekovat všechny nové servery na vybraném portu (pole *Interface*).



Obrázek 51 – DHCP Alert Zdroj: [vlastní zpracování]

Tato část je zpracována dle [79] a [80].

Cisco

Na zařízeních Cisco se DHCP Snooping nastavuje podobně jako u předchozího příkladu. Stejně jako u ostatních služeb se musí následujícím příkazem globálně zapnout.

Switch(config)# ip dhcp snooping

Poté se volí, pro jaké VLANy se ochrana uplatňuje. V případě, že nejsou používány, aplikují se na výchozí VLAN 1.

Switch(config)# ip dhcp snooping vlan 1

Jako poslední je nutné vybrat důvěryhodné porty, přes které jsou dostupné legitimní DHCP servery.

Switch (config-if)# ip dhcp snooping trust

Stav konfigurace je možné zobrazit show příkazem.

Switch (config-if)# show ip dhcp snooping

```

Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
1
DHCP snooping is operational on following VLANs:
1
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: 00ea.bdfe.1e00 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                Trusted    Allow option    Rate limit (pps)
-----                -
GigabitEthernet1/0/10    yes       yes             unlimited
  Custom circuit-ids:

```

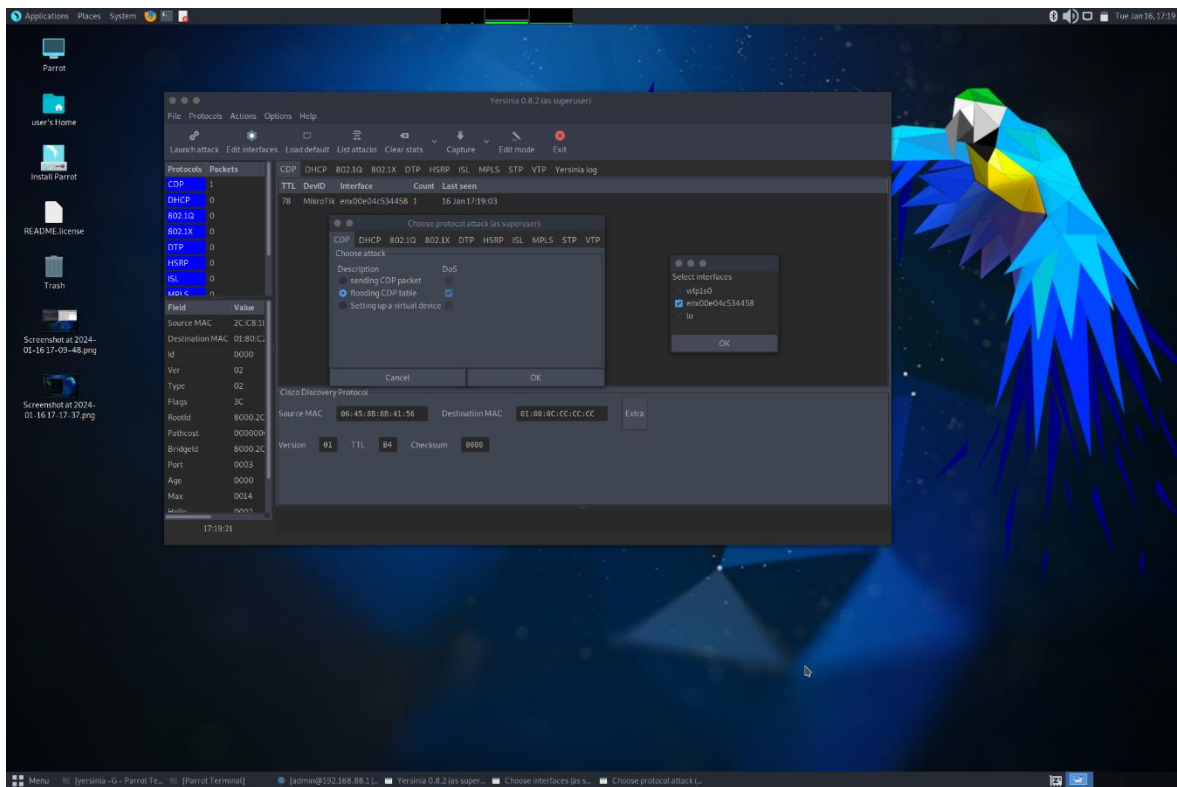
Obrázek 52 - Konfigurace DHCP Snoopingu – Cisco Zdroj: [vlastní zpracování]

Option 82 je standardně zapnutý, na rozdíl od Mikrotiku, kde se povoluje explicitně.

4.5 Neighbor discovery Attack

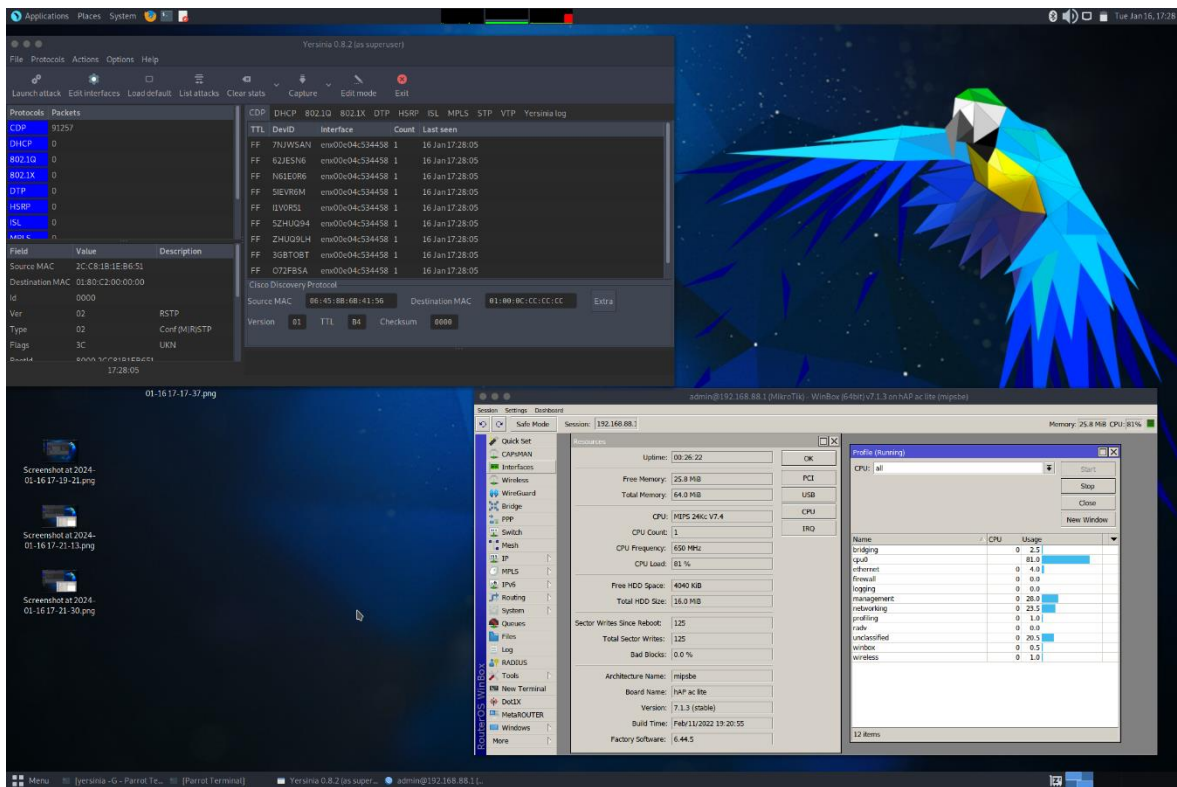
Útočník může rovněž přetížit některý z prvků sítě. Tím může ovlivnit stabilitu sítě nebo některý prvek úplně vyřadit tak, že není schopen obsloužit požadavky klientů. Pro přetížení síťových prvků může využít mimo jiné Neighbor discovery Attack.

Pomocí nástroje *Yersinia* může útočník zahltit zařízení stovkami záznamů do NDP tabulky. V grafickém rozhraní stačí vybrat typ útoku a interface, na který se mají pakety posílat. Cílový síťový prvek je Routerboard MikroTik hAP ac lite, který je schopen přijímat CDP pakety o sousedních zařízeních. Proto je vybraný útok „flooding CDP table“.



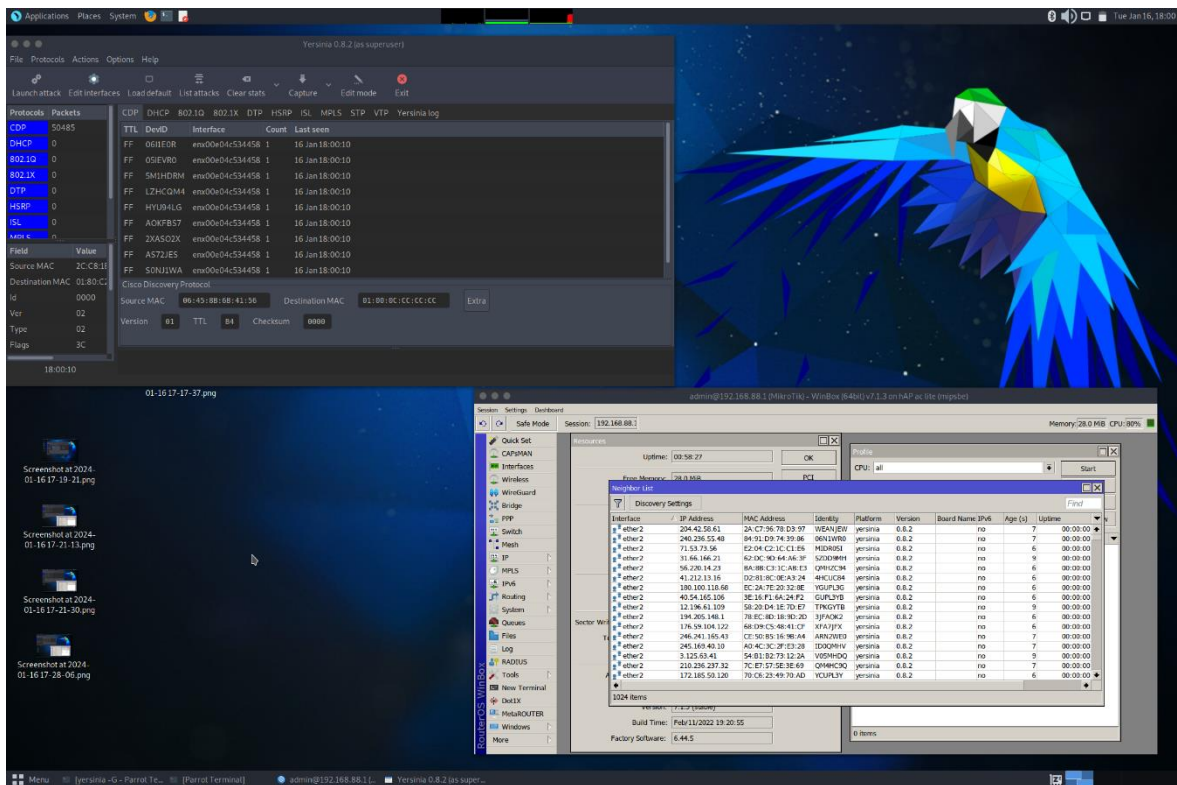
Obrázek 53 – Nastavení NDP útoku Zdroj: [vlastní zpracování]

Po spuštění útočnick vidí průběh útoku. Během krátké doby jsou vygenerovány tisíce paketů, které zahltí cílové zařízení. Vytížení procesoru je vidět na obrázku 54. Dosahuje hodnot více než 80 % i v případě, kdy na jiných portech neprobíhá žádná jiná komunikace. Tím je schopen zařízení vytižít natolik, že nebude schopné zpracovávat požadavky ostatních klientů a celá síť může být nestabilní nebo úplně přestat plnit svoji funkci a vypadnout.



Obrázek 54 – Vytížení CPU při NDP útoku (Mikrotik) Zdroj: [vlastní zpracování]

Všechny falešné sousedy si zařízení samozřejmě rovněž ukládá do seznamu, který je přehlcen obrovským množstvím neexistujících zařízení.



Obrázek 55 – Tabulka sousedů po NDP útoku (Mikrotik) Zdroj: [vlastní zpracování]

U Cisco L3 přepínače je výsledek podobný. Při útoku se tabulka sousedů plní falešnými záznamy a využití CPU dosahuje hodnot okolo 85 %

```

CPU utilization for five seconds: 84%/53%; one minute: 43%; five minutes: 12%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
184 5817 1286 4523 11.61% 6.17% 1.61% 0 CDP Protocol
94 5478 998 5488 10.57% 5.86% 1.55% 0 NGWC Learning Pr
72 8769 8638 1015 5.60% 3.07% 0.86% 0 IOSD ipc task
9 7609 471 16154 1.76% 0.31% 0.29% 0 Check heaps
118 2091 118 17720 1.20% 0.14% 0.07% 0 Per-minute Jobs
1 52 426 122 0.16% 0.06% 0.01% 0 Chunk Manager
142 163 1048 155 0.16% 0.17% 0.04% 0 EEM ED ND
67 1036 7267 142 0.08% 0.05% 0.04% 0 Net Background
  
```

Obrázek 56 - Využití CPU při NDP útoku (Cisco) Zdroj: [vlastní zpracování]

```

Switch#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID         Local Intrfce   Holdtme    Capability   Platform   Port ID
T7OKKXT          Gig 1/0/24     16         R H          yersinia   Eth 0
L4GC8P4          Gig 1/0/24     14         R T I r      yersinia   Eth 0
5ZHVQ99         Gig 1/0/24     14         R B S I      yersinia   Eth 0
XASNN2X          Gig 1/0/24     14         B S H r      yersinia   Eth 0
VQ995HZ         Gig 1/0/24     52         R T B S I    yersinia   Eth 0
1EAAR06         Gig 1/0/24     11         B H I r      yersinia   Eth 0
EAASN2J          Gig 1/0/24     10         T S H I      yersinia   Eth 0
N2JWSSA         Gig 1/0/24     41         R T B S      yersinia   Eth 0
OR61IIE         Gig 1/0/24     6          R H          yersinia   Eth 0
QMM1VDR          Gig 1/0/24     17         T B S        yersinia   Eth 0
FXB7OOK         Gig 1/0/24     22         R T B S H    yersinia   Eth 0
XASOO2X         Gig 1/0/24     0          S H I        yersinia   Eth 0
TBPk3FX         Gig 1/0/24     52         R B I        yersinia   Eth 0

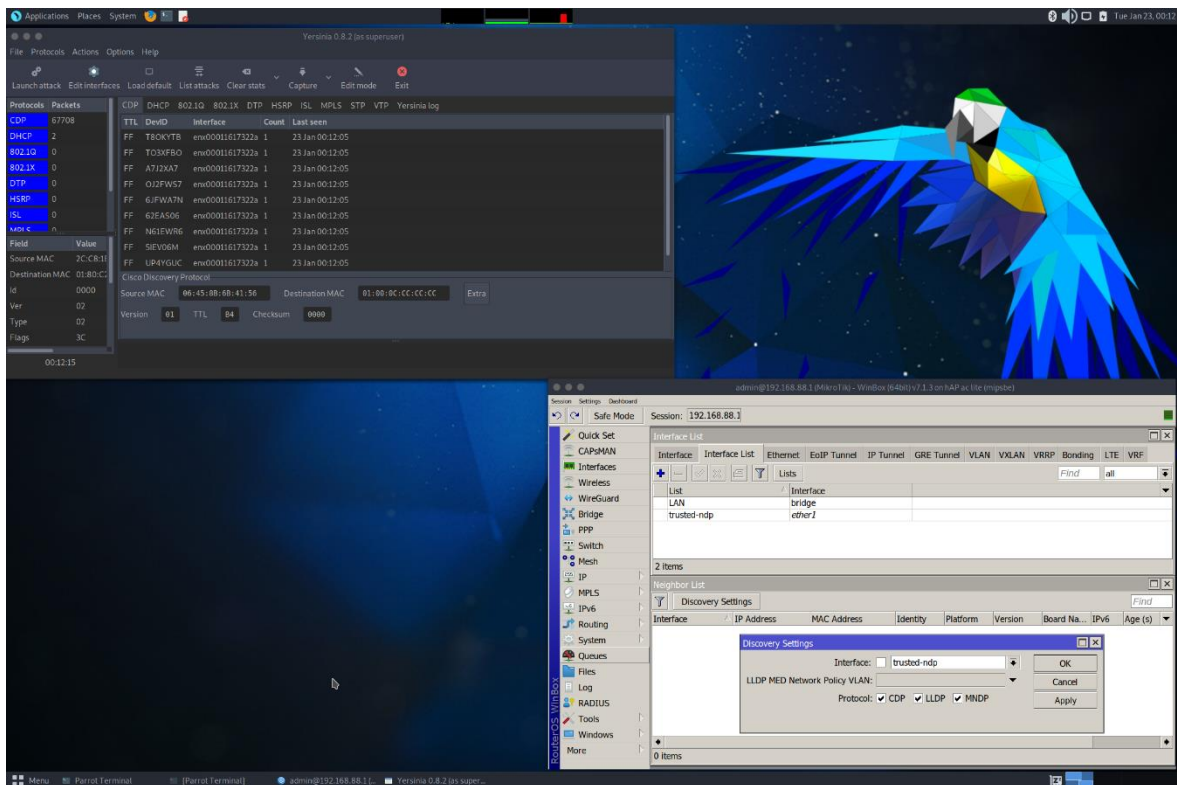
Total cdp entries displayed : 12000

```

Obrázek 57 - Tabulka sousedů po NDP útoku (Cisco) Zdroj: [vlastní zpracování]

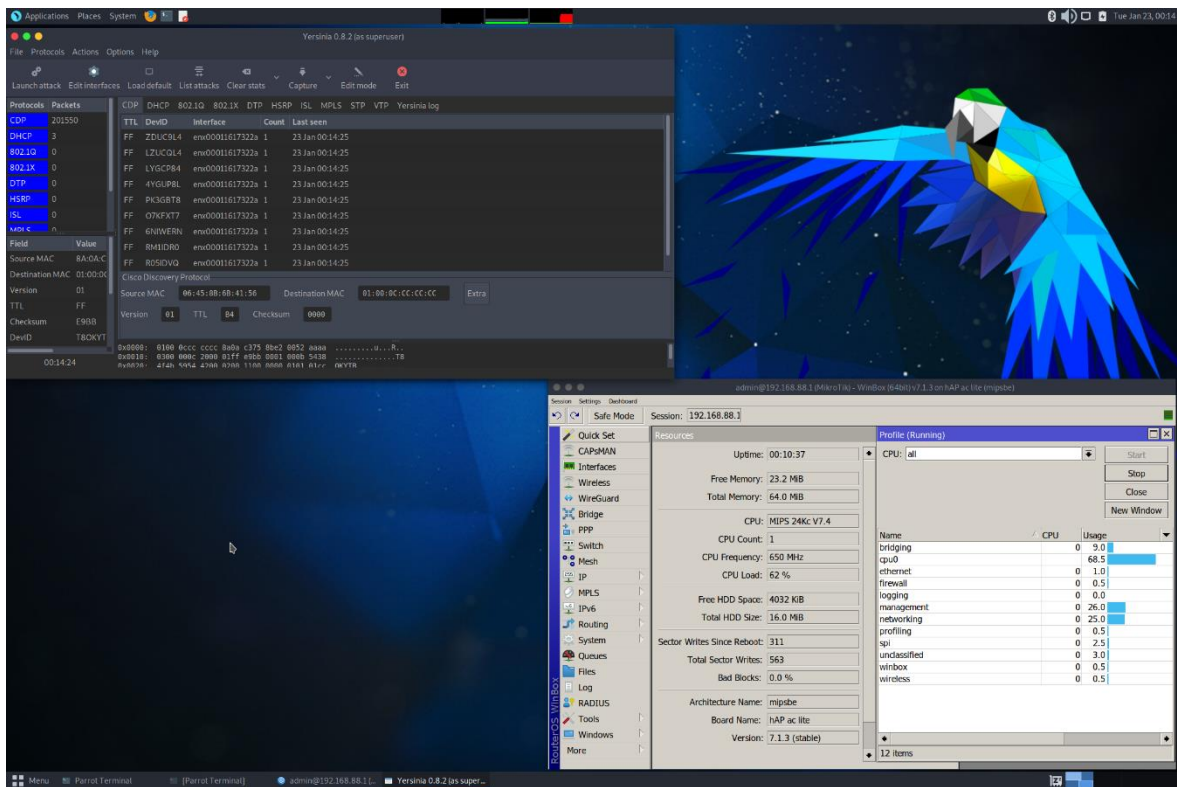
4.5.1 Obrana

Obranou před tímto druhem útoku je možnost přijímat tyto pakety pouze z ověřených portů. Pro ty je možné vytvořit speciální seznam, který se následně aplikuje v nastavení zjišťování sousedů. Díky tomu není na přijaté pakety brán ohled a tabulka se nepřehltí.



Obrázek 58 – Nastavení portů pro příjem NDP paketů Zdroj: [vlastní zpracování]

Tímto způsobem se ošetří situace, kdy útočník zneužije síťovou zásuvku určenou pro koncové zařízení. Stále ale dochází k zahlcování zařízení velkým množstvím falešných paketů. Vytížení procesoru se během útoku snižuje a hodnota dosahuje maximálně necelých 70 %.



Obrázek 59 – Vytížení CPU při NDP útoku s ochranou (Mikrotik) Zdroj: [vlastní zpracování]

Cisco zařízení rovněž podporuje zakázání příjmu CDP paketů na zvolených portech. Provádí se následujícím příkazem:

Switch(config-if)# no cdp enable

Výsledkem je snížení vytížení CPU na necelých 70 %. Do tabulky sousedů se falešné záznamy nepřidávají.

```

CPU utilization for five seconds: 69%/28%; one minute: 35%; five minutes: 14%
PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min  TTY Process
 94      30551      11360      2689  32.87% 16.65% 4.71% 0 NGWC Learning Pr
 72      16839      30738       547   7.59%  3.93% 1.33% 0 IOSD ipc task
 9        10293         648  15884   2.00%  0.45% 0.32% 0 Check heaps
175         295         3142    93   0.07%  0.00% 0.00% 0 FHRP Main thread
179        3463      48712    71   0.07%  0.10% 0.09% 0 VRRS Main thread
285         250         6067    41   0.07%  0.00% 0.00% 0 Timer Library
323         364         4562    79   0.07%  0.00% 0.00% 0 Crypto IKEv2
127        1411        3995   353   0.07%  0.04% 0.05% 0 PLFM-MGR IPC pro
  
```

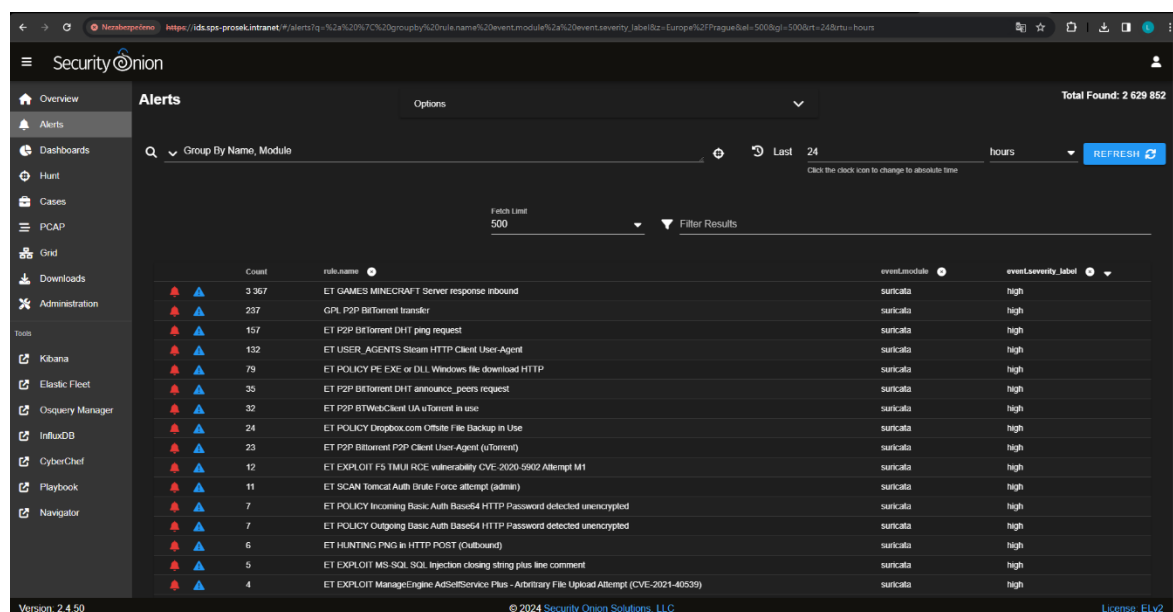
Obrázek 60 - Vytížení CPU při NDP útoku s ochranou (Cisco)

4.6 Nasazení IDS řešení Security Onion

Pro komplexní detekci průniků je vhodné do sítě nasadit IDS systém, který na základě síťové komunikace odhalí různé útoky na infrastrukturu a koncové stanice. V této kapitole jsou představeny vybrané funkce platformy *Security Onion* verze 2.4.50.

Po provedení instalace a nasazení systému do sítě je nutné do něj nahrávat síťový provoz. Toho lze docílit zrcadlením portů na páteřním přepínači nebo přístupového bodu do internetu. Systém následně provádí analýzu a na základě pravidel a znaků detekuje podezřelou komunikaci.

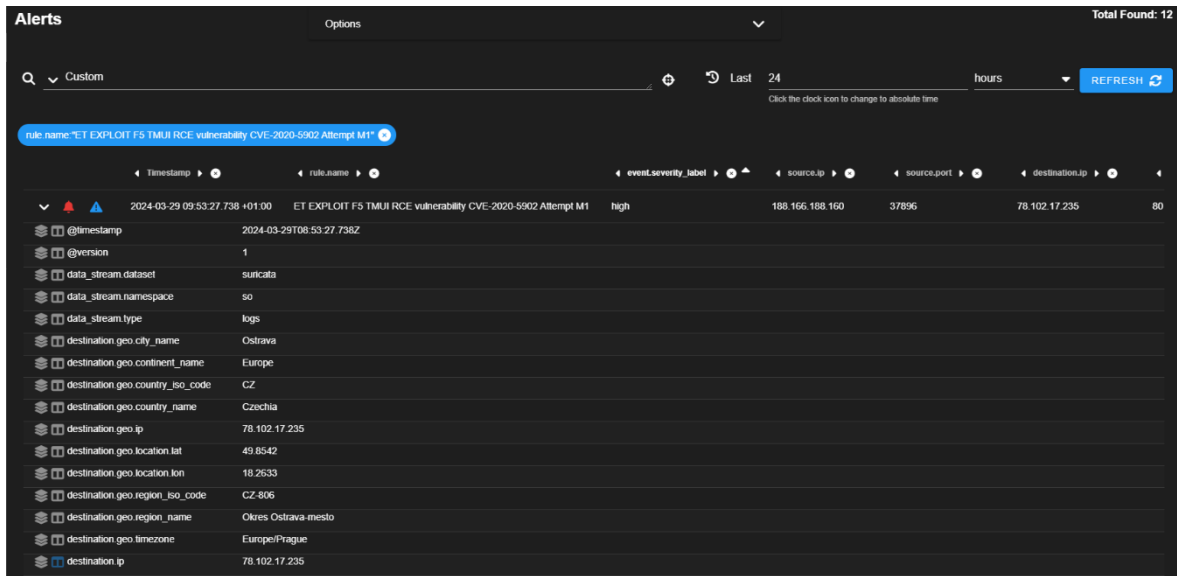
Pro testování v reálném prostředí byl nasazen do sítě školy. Výsledkem jsou upozornění (alerts) obsahující záznamy jednotlivých podezřelých aktivit. Ty jsou generovány systémem *Suricata*, který je blíže popsán v kapitole 3.5.9 Systémy odhalení a prevence průniku.



Count	rule.name	event.module	event.severity_label
3 367	ET GAMES MINECRAFT Server response inbound	suricata	high
237	GPL P2P BitTorrent transfer	suricata	high
157	ET P2P BitTorrent DHT ping request	suricata	high
132	ET USER_AGENTS Steam HTTP Client User-Agent	suricata	high
79	ET POLICY PE_EXE or DLL Windows file download HTTP	suricata	high
35	ET P2P BitTorrent DHT announce_peers request	suricata	high
32	ET P2P BitWebClient UA vTorrent in use	suricata	high
24	ET POLICY Dropbox.com Offsite File Backup in Use	suricata	high
23	ET P2P BitTorrent P2P Client User-Agent (vTorrent)	suricata	high
12	ET EXPLOIT FS_TMUII RCE vulnerability CVE-2020-5902 Attempt M1	suricata	high
11	ET SCAN Tomcat Auth Brute Force attempt (admin)	suricata	high
7	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	suricata	high
7	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted	suricata	high
6	ET HUNTING PNG in HTTP POST (Outbound)	suricata	high
5	ET EXPLOIT MS_SQL_SQL Injection closing string plus line comment	suricata	high
4	ET EXPLOIT ManageEngine AdService.Plus - Arbitrary File Upload Attempt (CVE-2021-40539)	suricata	high

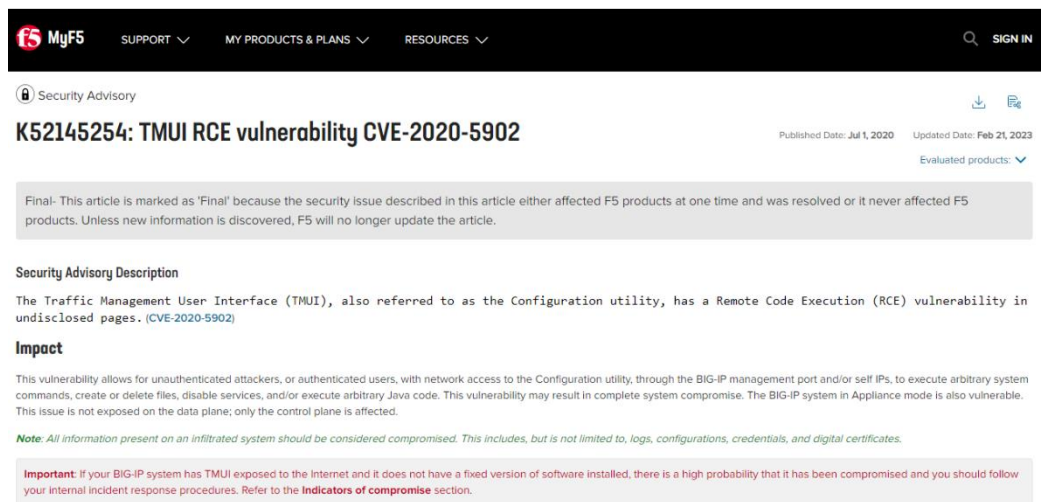
Obrázek 61 - Seznam upozornění v platformě Security Onion Zdroj: [vlastní zpracování]

Detaily obsahují všechny získané podrobnosti – IP adresy, čísla portů a pravidla, která vedla k vytvoření záznamu. Ty mohou i odkazovat na relevantní reference obsahující podrobnější popis útoku nebo zranitelnosti.



Obrázek 62 - Detail upozornění v platformě Security Onion Zdroj: [vlastní zpracování]

System *Suricata* v jednom ze záznamů upozorňuje na zranitelnost *CVE-2020-5902*. V tomto případě se jedná o uživatelské rozhraní správy provozu (TMUI), označované také jako konfigurační nástroj, které má na nezveřejněných stránkách chybu zabezpečení RCE (Remote Code Execution). [81]

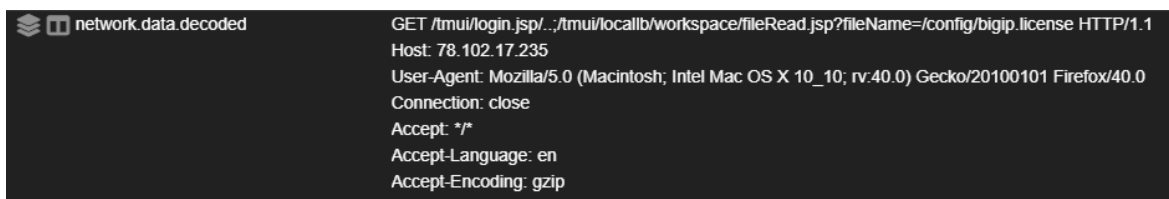


Obrázek 63 - Detail zranitelnosti CVE-2020-5902 Zdroj: [81]

Bezpečnostní pravidlo systému Suricata má následující podobu:

```
alert http any any -> any any (msg:"ET EXPLOIT F5 TMUI RCE vulnerability
CVE-2020-5902 Attempt M1"; flow:established,to_server; http.uri;
content: "/tmui/login.jsp"; depth:15; fast_pattern; content:"|3b|";
distance:0; reference:cve,2020-5902;
reference:url,support.f5.com/csp/article/K52145254; classtype:attempted-
admin; sid:2030469; rev:5; metadata:affected_product
Web_Server_Applications, attack_target Networking_Equipment, created_at
2020_07_05, cve CVE_2020_5902, deployment Perimeter, deployment
SSLDecrypt, former_category EXPLOIT, signature_severity Critical,
updated_at 2020_07_08;)
```

Odchycená síťová komunikace je vidět na obrázku 64.



```
network.data.decoded GET /tmui/login.jsp/./tmui/locallb/workspace/fileRead.jsp?fileName=/config/bigip.license HTTP/1.1
Host: 78.102.17.235
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10; rv:40.0) Gecko/20100101 Firefox/40.0
Connection: close
Accept: */*
Accept-Language: en
Accept-Encoding: gzip
```

Obrázek 64 - odchycená síťová komunikace Zdroj: [vlastní zpracování]

5 Výsledky a diskuse

Oblast kybernetické bezpečnosti je komplexní problematika. Útočníci mají odlišné motivace k napadání počítačových sítí a k dosažení svých cílů využívají různé techniky. Absence bezpečnostních mechanismů může mít za následek narušení provozu a služeb, finanční ztrátu, ztrátu dat nebo zneužití systémů k provádění dalších útoků.

5.1 Kybernetické útoky

Provedení kybernetických útoků není obtížné díky dostupným internetovým zdrojům a intuitivním nástrojům. Tyto nástroje byly v praktické části využity v nezabezpečené infrastruktuře, efektivně identifikovaly zařízení a služby v síti a pomocí slovníkovému útoku uhodly hesla do síťových prvků a Linuxového serveru. K nasazení parazitního DHCP serveru ho stačilo připojit do sítě a zahlcení routerů mělo za následek vysoké vytížení CPU. Tyto útoky nebyly nijak detekovány ani blokovány.

5.2 Mechanismy obrany

Pro efektivní detekci a blokování aktivit útočníka je třeba využít více postupů a nástrojů. Komplexní bezpečnostní politika musí správně identifikovat zdroj a typ útoku. Základem je zabezpečit koncové stanice a síťové prvky. Cizí zařízení je vhodné blokovat nebo oddělit od kritické infrastruktury. I přes zabezpečení přístupu je nutné implementovat ochranu za využití firewallů, access control listů a systémů pro detekci a prevenci průniků.

Na zařízeních výrobců Cisco i Mikrotik lze dosáhnout stejné úrovně zabezpečení, avšak způsob implementace se v některých případech liší. Rozdíly byly znatelné již při blokování přístupu útočníka do sítě. Zatímco Cisco umožňuje jednoduchou intuitivní konfiguraci povolených MAC adres na portech, systém RouterOS neumožňuje detekci a povolení právě připojených zařízení. Proto byl vytvořen skript, který tento postup automatizuje. Směrovače Cisco nativně neobsahují mechanismy pro detekci a blokování skenování portů. Tuto roli by muselo zastoupit zvláštní zařízení – Cisco firewall. Mikrotik má tuto funkci implementovanou v systémovém firewallu. Blokování útoků na protokol SSH se liší v principu, kdy Cisco zařízení přepne do stavu *Quiet-Mode*, ve kterém blokuje

další připojení od všech, zatímco u Mikrotiku lze opět využít firewall a blokovat pouze útočníka na základě jeho IP adresy. Pro ukázkou nasazení IPS na server byl použit nástroj *Fail2Ban*. Konfigurace DHCP Snooping, který blokuje parazitní servery se provádí téměř totožně. Obrana před zahlcením tabulek sousedních zařízení přes protokoly CDP a MNDP se také provádí obdobně.

Pro detekování podezřelé aktivity v síti je možné využít systém *Suricata*, který analyzuje provoz a na základě vzorců vytváří upozornění, které administrátorům pomáhají identifikovat napadená zařízení, pokusy o průnik a slabá místa infrastruktury. Výstupy jsou dostupné v rozhraní platformy *Security Onion*.

Závěr

Cílem práce bylo zpracovat problematiku zabezpečení počítačových sítí se zaměřením na vybrané kybernetické útoky a obranou před nimi. Diplomová práce v teoretické části zkoumá útočníky, jejich motivace, nástroje a konkrétní kybernetické útoky. Dále představuje bezpečnostní postupy a nástroje, které chrání počítačové sítě a zařízení v nich před hackery.

V praktické části byl vytvořen scénář útoku, který obsahuje typické problémové situace zabezpečení firemní sítě. Jsou v něm provedeny útočnickovy postupy a kybernetické útoky na konkrétní síťová zařízení. Tyto techniky odhalují slabá místa v různých oblastech zabezpečení počítačových sítí. Příklady zahrnují přístup do sítě, skenování zařízení v síti, útok na hesla pro získání přístupu, ovlivnění klientů a jejich komunikace i zahlcení klíčových síťových prvků. Záměrně byly zvoleny útoky z různých oblastí s cílem využít různé mechanismy obrany a související nástroje.

Pro obranu před hackerskou aktivitou byly navrženy postupy a konfigurace síťových prvků. Využity byly různé mechanismy – firewall, access control listy, pravidla přepínaných portů i systémy pro detekci a prevenci průniků. Pro srovnání byla obrana prováděna na zařízeních Cisco a Mikrotik, které představují určitý standard řešení síťové infrastruktury. Do počítačové sítě byl rovněž nasazen systém pro detekci průniků Security Onion, který na základě síťové komunikace odhaluje podezřelou aktivitu. Zhodnocení bylo provedeno v páté kapitole.

Cíle práce byly splněny. Práce může sloužit studentům a vzdělávacím institucím jako zdroj informací při výuce kybernetické bezpečnosti, zejména pokud se zabývají praktickou implementací obranných technik na konkrétních zařízeních. Správci sítí mohou využít konfigurace bezpečnostních mechanismů k posílení ochrany infrastruktury, a to jak při použití zařízení od výrobce Cisco, tak od výrobce Mikrotik.

6 Seznam použitých zdrojů

- [1] LUTKEVICH, Ben, 2021. What is a Script Kiddie? - Definition from SearchSecurity. In: techtarget.com [online]. [cit. 14.10.2023]. Dostupné z: <https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie>
- [2] DVOŘÁKOVÁ, Lucie, 2023. Co je to etický hacking? Poznejte rozdíl mezi White Hat a Black Hat. In: l-a-b-a.cz [online]. [cit. 14.10.2023]. Dostupné z: <https://l-a-b-a.cz/blog/565-co-je-to-eticky-hacking-poznejte-rozdil-mezi-white-hat-a-black-hat>
- [3] AWATI, Rahul, 2023. Common Vulnerabilities and Exposures (CVE). In: techtarget.com [online]. [cit. 15.10.2023]. Dostupné z: <https://www.techtarget.com/searchsecurity/definition/Common-Vulnerabilities-and-Exposures-CVE>
- [4] Cvedetails.com, 2024. Vulnerability Details : CVE-2024-20338. In: cvedetails.com [online]. [cit. 15.3.2024]. Dostupné z: <https://www.cvedetails.com/cve/CVE-2024-20338/>
- [5] First.org, 2023. Common Vulnerability Scoring System version 4.0: Specification Document. In: first.org [online]. [cit. 15.3.2024]. Dostupné z: <https://www.first.org/cvss/v4.0/specification-document>
- [6] Kali.org, 2023. What is Kali Linux?. In: kali.org [online]. [cit. 25.11.2023]. Dostupné z: <https://www.kali.org/docs/introduction/what-is-kali-linux/>
- [7] Kali.org, 2023. Kali Linux. In: kali.org [online]. [cit. 25.11.2023]. Dostupné z: <https://www.kali.org/docs/introduction/what-is-kali-linux/>
- [8] DEVITO, Andrew, 2023. The Ultimate Kali Purple Guide: Everything You Need to Know. In: stationx.net [online]. [cit. 25.11.2023]. Dostupné z: <https://www.stationx.net/kali-purple-guide/>
- [9] Kali.org, 2023. Kali Linux 2023.1 Release. In: kali.org [online]. [cit. 25.11.2023]. Dostupné z: <https://www.kali.org/blog/kali-linux-2023-1-release/>
- [10] Kali.org, 2024. Get Kali. In: kali.org [online]. [cit. 25.11.2023]. Dostupné z: <https://www.kali.org/get-kali/#kali-mobile>
- [11] Kali.org, 2024. Kali NetHunter. In: kali.org [online]. [cit. 26.11.2023]. Dostupné z: <https://www.kali.org/docs/nethunter/>

- [12] Parrotsec.org, 2023. Parrot Security. In: parrotsec.org [online]. [cit. 4.12.2023]. Dostupné z: <https://www.parrotsec.org/>
- [13] Parrotsec.org, 2023. What is ParrotOS?. In: parrotsec.org [online]. [cit. 4.12.2023]. Dostupné z: <https://www.parrotsec.org/docs/introduction/what-is-parrot/>
- [14] Parrotsec.org, 2023. Parrot Security Download. In: parrotsec.org [online]. [cit. 4.12.2023]. Dostupné z: <https://www.parrotsec.org/download/>
- [15] Wireshark.org, 2023. Wireshark Frequently Asked Questions. In: wireshark.org [online]. [cit. 10.12.2023]. Dostupné z: <https://www.wireshark.org/faq.html>
- [16] Comptia.org, 2023. What Is Wireshark and How Is It Used?. In: comptia.org [online]. [cit. 10.12.2023]. Dostupné z: <https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it>
- [17] BORICHA, Vijin, 2018. Using statistical tools in Wireshark for packet analysis [Tutorial]. In: packtpub.com [online]. [cit. 28.12.2023]. Dostupné z: <https://hub.packtpub.com/statistical-tools-in-wireshark-for-packet-analysis/>
- [18] Wireshark.org, 2023. tshark(1) Manual Page. In: wireshark.org [online]. [cit. 10.12.2023]. Dostupné z: <https://www.wireshark.org/docs/man-pages/tshark.html>
- [19] Tcpdump.org, 2024. TCPDUMP & LIBPCAP. In: tcpdump.org [online]. [cit. 8.1.2024]. Dostupné z: <https://www.tcpdump.org/>
- [20] Tcpdump.org, 2024. TCPDUMP(1) MAN PAGE. In: tcpdump.org [online]. [cit. 8.1.2024]. Dostupné z: <https://www.tcpdump.org/manpages/tcpdump.1.html>
- [21] Netresec.com, 2023. NetworkMiner. In: netresec.com [online]. [cit. 11.1.2024]. Dostupné z: <https://www.netresec.com/?page=networkminer>
- [22] LYON, Gordon. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning [online]. Nmap Software, 2022 [cit. 11.1.2024]. ISBN 978-0-9799587-1-7. Dostupné z: <https://nmap.org/book/toc.html>
- [23] Information Sciences Institute, University of Southern California, 1981. Transmission Control Protocol. RFC 793. In: rfc-editor.org [online]. [cit. 11.1.2024]. Dostupné z: <https://www.rfc-editor.org/rfc/rfc793>

- [24] Nmap.org, 2024. Nmap: the Network Mapper - Free Security Scanner. In: nmap.org [online]. [cit. 11.1.2024]. Dostupné z: <https://nmap.org>
- [25] Nmap.org, 2024. Zenmap - Official cross-platform Nmap Security Scanner GUI. In: nmap.org [online]. [cit. 14.1.2024]. Dostupné z: <https://nmap.org/zenmap/>
- [26] JESTER, Timothy, 2023. Understanding RockYou.txt: A Tool for Security and a Weapon for Hackers. In: keepersecurity.com [online]. [cit. 14.1.2024]. Dostupné z: <https://www.keepersecurity.com/blog/2023/08/04/understanding-rockyou-txt-a-tool-for-security-and-a-weapon-for-hackers/>
- [27] SEVEN LAYERS, 2023. Pentesting 101: Passwords and Wordlists. In: sevenlayers.com [online]. [cit. 14.1.2024]. Dostupné z: <https://www.sevenlayers.com/index.php/202-pentesting-101-passwords-and-wordlists>
- [28] Kali.org, 2024. hydra | Kali Linux Tools. In: kali.org [online]. [cit. 16.1.2024]. Dostupné z: <https://www.kali.org/tools/hydra/>
- [29] ESET software, 2024. 6 nejčastějších kyberútoků na uživatelská hesla. In: dvojklik.cz [online]. [cit. 16.1.2024]. Dostupné z: <https://www.dvojklik.cz/6-nejcastejsich-kyberutoku-na-uzivatelska-hesla/>
- [30] DOSTALOVÁ, Helena, 2023. V bezpečnosti nejde jen o boj systémů, nejslabším článkem je člověk. In: hn.cz [online]. [cit. 21.1.2024]. Dostupné z: <https://hn.cz/c1-67257330-v-bezpecnosti-nejde-jen-o-boj-systemu-nejslabsim-clankem-je-clovek>
- [31] PIVOŇKA, Michal, 2021. Karel Řehka: Nejslabší článek kybernetické bezpečnosti je vždycky nepoučený uživatel. In: czdefence.cz [online]. [cit. 21.1.2024]. Dostupné z: <https://www.czdefence.cz/clanek/karel-rehka>
- [32] BALÝOVÁ, Lucie, 2022. Nejslabším článkem kybernetické bezpečnosti firmy jsou její zaměstnanci. In: hn.cz [online]. [cit. 21.1.2024]. Dostupné z: <https://archiv.hn.cz/c1-67062560-nejslabsim-clankem-kyberneticke-bezpecnosti-firmy-jsou-jeji-zamestnanci>
- [33] KRČMÁŘ, Petr, 2022. Nejslabším článkem je nepoučený či nezodpovědný uživatel, tvrdí bezpečáči. In: root.cz [online]. [cit. 21.1.2024]. Dostupné z: <https://www.root.cz/clanky/nejslabsim-clankem-je-nepouceny-ci-nezodpovedny-uzivatel-tvrdi-bezpecaci/>

- [34] ESET software, 2023. Co je phishing? | ESET. In: eset.com [online]. [cit. 22.1.2024]. Dostupné z: <https://www.eset.com/cz/phishing/>
- [35] Geeksforgeeks.org, 2021. Blackeye Phishing Tool in Kali Linux. In: geeksforgeeks.org [online]. [cit. 22.1.2024]. Dostupné z: <https://www.geeksforgeeks.org/blackeye-phishing-tool-in-kali-linux/>
- [36] Policejní prezidium ČR, 2021. Vishing a spoofing. In: policie.cz [online]. [cit. 22.1.2024]. Dostupné z: <https://www.policie.cz/clanek/vishing-a-spoofing.aspx>
- [37] You connected, 2017. Keylogger - INTERNETEM BEZPEČNĚ. In: internetembezpecne.cz [online]. [cit. 25.1.2024]. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/malware/keylogger/>
- [38] Keelog, 2023. Keylogger - KeyGrabber - stealthy hardware keylogger. In: keelog.com [online]. [cit. 25.1.2024]. Dostupné z: <https://www.keelog.com/keylogger/>
- [39] SHX Trading, 2023. AirDrive Pro USB Keylogger. In: spyobchod.cz [online]. [cit. 25.1.2024]. Dostupné z: <https://www.spyobchod.cz/airdrive-pro-usb-keylogger-e124105.htm>
- [40] Fortinet, 2023. DoS Attack vs. DDoS Attack. In: fortinet.com [online]. [cit. 2.2.2024]. Dostupné z: <https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos>
- [41] ESET, 2023. Co je botnet? | ESET. In: eset.com [online]. [cit. 2.2.2024]. Dostupné z: <https://www.eset.com/cz/botnet/>
- [42] Policejní prezidium, 2017. Jednotlivé druhy kyberkriminality - Policie České republiky. In: policie.cz [online]. [cit. 2.2.2024]. Dostupné z: <https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx>
- [43] Kali.org, 2024. yersinia | Kali Linux Tools. In: kali.org [online]. [cit. 4.2.2024]. Dostupné z: <https://www.kali.org/tools/yersinia/>
- [44] Mikrotik, 2023. Neighbor discovery - RouterOS - MikroTik Documentation. In: mikrotik.com [online]. [cit. 4.2.2024]. Dostupné z: <https://help.mikrotik.com/docs/display/ROS/Neighbor+discovery>

- [45] Policejní prezidium, 2016. Bezpečné heslo - zásady tvorby bezpečného hesla. In: policie.cz [online]. [cit. 11.2.2024]. Dostupné z: <https://www.policie.cz/soubor/05-bezpecne-heslo-pdf.aspx>
- [46] EMPEY, Charlotte, 2019. Jak si nastavit silné heslo. In: avast.com [online]. [cit. 11.2.2024]. Dostupné z: <https://blog.avast.com/cs/jak-si-nastavit-silne-heslo>
- [47] Google, 2023. Jak funguje dvoufázové ověření - Centrum bezpečnosti Google. In: safety.google [online]. [cit. 11.2.2024]. Dostupné z: <https://safety.google/intl/cs/stories/password/>
- [48] Microsoft, 2023. Co je řízení přístupu Access Control? | Zabezpečení od Microsoftu. In: microsoft.com [online]. [cit. 11.2.2024]. Dostupné z: <https://www.microsoft.com/cs-cz/security/business/security-101/what-is-access-control>
- [49] KASS, Howard, 2020. Kaspersky: Enterprises Running Old Software Lose 47% More Money in Data Breach. In: msspalert.com [online]. [cit. 11.2.2024]. Dostupné z: <https://www.msspalert.com/news/kaspersky-enterprises-running-old-software-lose-47-more-money-in-data-breach>
- [50] Cisco Systems, 2023. What Is a Next-Generation Firewall?. In: cisco.com [online]. [cit. 13.2.2024]. Dostupné z: https://www.cisco.com/c/en_in/products/security/firewalls/what-is-a-next-generation-firewall.html
- [51] W3Schools, 2023. Cyber Security Firewalls. In: w3schools.com [online]. [cit. 13.2.2024]. Dostupné z: https://www.w3schools.com/cybersecurity/cybersecurity_firewalls.php
- [52] Cisco Systems, 2023. What Is a Firewall?. In: cisco.com [online]. [cit. 13.2.2024]. Dostupné z: <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>
- [53] YASAR, Kinza, 2023. What is a Firewall and Why Do I Need One? | Definition from TechTarget. In: techtarget.com [online]. [cit. 13.2.2024]. Dostupné z: <https://www.techtarget.com/searchsecurity/definition/firewall>
- [54] Fortinet, 2022. What Is a Stateful Firewall?. In: fortinet.com [online]. [cit. 13.2.2024]. Dostupné z: <https://www.fortinet.com/resources/cyberglossary/stateful-firewall>

- [55] Geeksforgeeks.org, 2022. Standard Access-List. In: geeksforgeeks.org [online]. [cit. 20.2.2024]. Dostupné z: <https://www.geeksforgeeks.org/standard-access-list/>
- [56] Cisco Systems, 2023. Configure Commonly Used IP ACLs - Cisco. In: cisco.com [online]. [cit. 20.2.2024]. Dostupné z: <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html>
- [57] Geeksforgeeks.org, 2022. Extended Access-List. In: geeksforgeeks.org [online]. [cit. 20.2.2024]. Dostupné z: <https://www.geeksforgeeks.org/extended-access-list/>
- [58] BOUŠKA, Petr, 2009. Cisco IOS 8 - ACL - Access Control List. In: samuraj-cz.com [online]. [cit. 20.2.2024]. Dostupné z: <https://www.samuraj-cz.com/clanek/cisco-ios-8-access-control-list/>
- [59] Cisco Systems, 2023. Configure and Filter IP Access Lists - Cisco. In: cisco.com [online]. [cit. 20.2.2024]. Dostupné z: <https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html>
- [60] BOUŠKA, Petr, 2016. Cisco IOS 24 - zabezpečení komunikace na portech. In: samuraj-cz.com [online]. [cit. 20.2.2024]. Dostupné z: <https://www.samuraj-cz.com/clanek/cisco-ios-24-zabezpeceni-komunikace-na-portech/>
- [61] YUE, Zhu, 2023. What Is 802.1X? How Does It Work? - Huawei. In: huawei.com [online]. [cit. 20.2.2024]. Dostupné z: <https://info.support.huawei.com/info-finder/encyclopedia/en/802.1X.html>
- [62] Kaspersky, 2023. What is a honeypot? How honeypots help security. In: kaspersky.com [online]. [cit. 26.2.2024]. Dostupné z: <https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot>
- [63] IBM, 2023. What is an Intrusion Detection System (IDS)? | IBM. In: ibm.com [online]. [cit. 26.2.2024]. Dostupné z: <https://www.ibm.com/topics/intrusion-detection-system>
- [64] Geeksforgeeks.org, 2022. Difference between HIDs and NIDs - GeeksforGeeks. In: geeksforgeeks.org [online]. [cit. 26.2.2024]. Dostupné z: <https://www.geeksforgeeks.org/difference-between-hids-and-nids/>

- [65] Security Onion Solutions, 2024. Introduction | Security Onion Documentation 2.4 documentation. In: securityonion.net [online]. [cit. 26.2.2024]. Dostupné z: <https://docs.securityonion.net/en/2.4/introduction.html>
- [66] Security Onion Solutions, 2024. Security Onion Solutions | Hardware. In: securityonion.net [online]. [cit. 26.2.2024]. Dostupné z: <https://securityonionsolutions.com/hardware>
- [67] Security Onion Solutions, 2024. Security Onion Solutions | SOS 1000F. In: securityonion.net [online]. [cit. 26.2.2024]. Dostupné z: <https://securityonionsolutions.com/hardware/1000F>
- [68] Open Information Security Foundation, 2024. 1. What is Suricata | Suricata 8.0.0-dev documentation. In: suricata.io [online]. [cit. 3.3.2024]. Dostupné z: <https://docs.suricata.io/en/latest/what-is-suricata.html>
- [69] Open Information Security Foundation, 2024. 8.1. Rules Format | Suricata 8.0.0-dev documentation. In: suricata.io [online]. [cit. 3.3.2024]. Dostupné z: <https://docs.suricata.io/en/latest/rules/intro.html>
- [70] Security Onion Solutions, 2024. Suricata | Security Onion Documentation 2.4 documentation. In: securityonion.net [online]. [cit. 26.2.2024]. Dostupné z: <https://docs.securityonion.net/en/2.4/suricata.html#suricata>
- [71] Cisco Systems, 2023. Snort - Network Intrusion Detection & Prevention System. In: snort.org [online]. [cit. 3.3.2024]. Dostupné z: <https://www.snort.org/>
- [72] Cisco Systems, 2023. Snort 3 Rule Writing Guide - Snort 3 Rule Writing Guide. In: snort.org [online]. [cit. 3.3.2024]. Dostupné z: <https://docs.snort.org/>
- [73] Cisco Systems, 2023. What is the relationship between Snort and Cisco?. In: snort.org [online]. [cit. 3.3.2024]. Dostupné z: <https://www.snort.org/faq/what-is-the-relationship-between-snort-and-cisco>
- [74] KRČMÁŘ, Petr, 2013. Fail2ban: konec hádání hesel na serveru. In: root.cz [online]. [cit. 6.3.2024]. Dostupné z: <https://www.root.cz/clanky/fail2ban-konec-hadani-hesel-na-serveru/>
- [75] EMPSON, Scott. CCNA kompletní přehled příkazů: autorizovaný výukový průvodce. Brno: Computer Press, 2009. ISBN 978-80-251-2286-0.

- [76] Cisco Systems, 2023. Cisco Secure Firewall Port Scan Detection. In: cisco.com [online]. [cit. 14.1.2024]. Dostupné z: <https://secure.cisco.com/secure-firewall/docs/port-scan-detection>
- [77] SIA Mikrotīkls, 2013. Bruteforce login prevention - MikroTik Wiki. In: mikrotik.com [online]. [cit. 23.1.2024]. Dostupné z: https://wiki.mikrotik.com/wiki/Bruteforce_login_prevention
- [78] Cisco Systems, 2016. User Security Configuration Guide - Cisco IOS Login Enhancements-Login Block [Cisco Cloud Services Router 1000V Series] - Cisco. In: cisco.com [online]. [cit. 4.2.2024]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/xen-16/sec-usr-cfg-xe-16-book/sec-login-enhance.html
- [79] SIA Mikrotīkls, 2024. Manual:Interface/Bridge - MikroTik Wiki. In: mikrotik.com [online]. [cit. 5.2.2024]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:Interface/Bridge#DHCP_Snooping_and_DHCP_Option_82
- [80] SIA Mikrotīkls, 2024. Manual:IP/DHCP Server - MikroTik Wiki. In: mikrotik.com [online]. [cit. 5.2.2024]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:IP/DHCP_Server#Alerts
- [81] F5, 2023. K52145254: TMUI RCE vulnerability CVE-2020-5902. In: f5.com [online]. [cit. 30.3.2024]. Dostupné z: <https://my.f5.com/manage/s/article/K52145254>
- [82] MCNAB, Chris. Network security assessment. Second Edition. Cambridge: O'Reilly, 2007. ISBN 0-596-51030-6.
- [83] OCCUPYTHEWEB. Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali. San Francisco: No Starch Press, 2018. ISBN 978-1593278557.
- [84] PENGELLY, James. The Official CompTIA Security+ Student Guide: Exam SY0-601 [online]. Illinois: CompTIA, c2020. ISBN 978-1-64274-328-9. Dostupné také z: learn.comptia.org
- [85] SAPP, S Arthur. Infinity Ethical Hacking: Learn basic to advance hacks. c2020. ISBN 979-8662888128.

6.1 Seznam obrázků

Obrázek 1 – Ukázka CVE záznamu Zdroj: [4].....	13
Obrázek 2 – Skórovací systém CVSS 4.0 Zdroj: [5].....	14
Obrázek 3 – Rozhraní Kali Linux Zdroj: [7].....	16
Obrázek 4 – Rozhraní Kali Purple Zdroj: [9].....	17
Obrázek 5 – Rozhraní Kali NetHunter Zdroj: [11].....	18
Obrázek 6 – Rozhraní Parrot Security Zdroj: [14].....	19
Obrázek 7 – Rozhraní programu Wireshark Zdroj: [vlastní zpracování].....	20
Obrázek 8 – TShark Zdroj: [vlastní zpracování].....	22
Obrázek 9 – Tcpdump Zdroj: [vlastní zpracování].....	23
Obrázek 10 – Network miner Zdroj: [vlastní zpracování].....	24
Obrázek 11 – Xmas sken v analyzátoru Wireshark.....	26
Obrázek 12 – Nmap Zdroj: [vlastní zpracování].....	27
Obrázek 13 – rozhraní Zenmap Zdroj: [vlastní zpracování].....	28
Obrázek 14 – Hydra Zdroj: [vlastní zpracování].....	29
Obrázek 15 – Úspěšnost sociálního inženýrství Zdroj: [vlastní zpracování].....	31
Obrázek 16 – USB Keylogger Zdroj: [39].....	32
Obrázek 17 – Nástroj Yersinia Zdroj: [vlastní zpracování].....	34
Obrázek 18 – Neighbor list Zdroj: [44].....	35
Obrázek 19 – Úniky dat způsobené neaktuálním softwarem Zdroj: [49].....	37
Obrázek 20 – Firewall v RouterOS Zdroj: [vlastní zpracování].....	39
Obrázek 21 – Ukázka použití ACL Zdroj: [56].....	40
Obrázek 22 - SOS 1000F Zdroj: [67].....	43
Obrázek 23 – Upozornění v systému Security Onion Zdroj: [70].....	44
Obrázek 24 – Zobrazení konfigurace port-security Zdroj: [vlastní zpracování].....	47
Obrázek 25 – Změna MAC adresy Zdroj: [vlastní zpracování].....	48
Obrázek 26 – Log při porušení port-security pravidla Zdroj: [vlastní zpracování].....	48
Obrázek 27 – Stav port-security po porušení pravidla Zdroj: [vlastní zpracování].....	49
Obrázek 28 – Status portu po porušení pravidla Zdroj: [vlastní zpracování].....	49
Obrázek 29 – Výpis portů a připojených zařízení Zdroj: [vlastní zpracování].....	50
Obrázek 30 – Vytvoření pravidel pro vybraný port Zdroj: [vlastní zpracování].....	51
Obrázek 31 – Detail pravidla pro povolení MAC adresy Zdroj: [vlastní zpracování].....	51
Obrázek 32 – Pravidlo zakazující ostatní MAC adresy Zdroj: [vlastní zpracování].....	52
Obrázek 33 – Skenování služeb bez ochrany FW Zdroj: [vlastní zpracování].....	53
Obrázek 34 – Detekce verzí služeb bez ochrany FW Zdroj: [vlastní zpracování].....	53
Obrázek 35 – Port Scan Detection v RouterOS Zdroj: [vlastní zpracování].....	54
Obrázek 36 – Konfigurace firewallu Zdroj: [vlastní zpracování].....	55
Obrázek 37 – Pokus o útok s ochranou FW Zdroj: [vlastní zpracování].....	56
Obrázek 38 – Zablokovaná IP adresa útočníka Zdroj: [vlastní zpracování].....	56
Obrázek 39 – Provedení slovníkového útoku bez ochrany Zdroj: [vlastní zpracování].....	58

Obrázek 40 – Konfigurace Fail2Ban Zdroj: [vlastní zpracování]	59
Obrázek 41 – Zablokování IP po neúspěšných pokusech Zdroj: [vlastní zpracování].....	60
Obrázek 42 – Zablokování IP adresy v iptables Zdroj: [vlastní zpracování]	60
Obrázek 43 – Firewall pravidla pro ochranu před slovníkovým útokem na SSH Zdroj: [vlastní zpracování].....	61
Obrázek 44 – ACL pravidla aplikovaná během stavu Quiet-Mode Zdroj: [vlastní zpracování].....	62
Obrázek 45 – Informace o omezení přihlášení Zdroj: [vlastní zpracování]	63
Obrázek 46 – Připojení pomocí SSH Zdroj: [vlastní zpracování]	63
Obrázek 47 – Log zpráva o přepnutí do režimu Quiet-Mode Zdroj: [vlastní zpracování] ..	64
Obrázek 48 – Informace o omezení přihlášení po neúspěšných pokusech Zdroj: [vlastní zpracování].....	64
Obrázek 49 – DHCP Snooping a DHCP Option 82 Zdroj: [79].....	65
Obrázek 50 – Konfigurace DHCP Snooping Zdroj: [vlastní zpracování]	66
Obrázek 51 – DHCP Alert Zdroj: [vlastní zpracování]	67
Obrázek 52 - Konfigurace DHCP Snoopingu – Cisco Zdroj: [vlastní zpracování].....	68
Obrázek 53 – Nastavení NDP útoku Zdroj: [vlastní zpracování]	69
Obrázek 54 – Vytížení CPU při NDP útoku (Mikrotik) Zdroj: [vlastní zpracování]	70
Obrázek 55 – Tabulka sousedů po NDP útoku (Mikrotik) Zdroj: [vlastní zpracování]	71
Obrázek 56 - Vytížení CPU při NDP útoku (Cisco) Zdroj: [vlastní zpracování].....	71
Obrázek 57 - Tabulka sousedů po NDP útoku (Cisco) Zdroj: [vlastní zpracování].....	72
Obrázek 58 – Nastavení portů pro příjem NDP paketů Zdroj: [vlastní zpracování]	73
Obrázek 59 – Vytížení CPU při NDP útoku s ochranou (Mikrotik) Zdroj: [vlastní zpracování].....	74
Obrázek 60 - Vytížení CPU při NDP útoku s ochranou (Cisco)	74
Obrázek 61 - Seznam upozornění v platformě Security Onion Zdroj: [vlastní zpracování]	75
Obrázek 62 - Detail upozornění v platformě Security Onion Zdroj: [vlastní zpracování] ..	76
Obrázek 63 - Detail zranitelnosti CVE-2020-5902 Zdroj: [81].....	76
Obrázek 64 - odchycená síťová komunikace Zdroj: [vlastní zpracování]	77

Přílohy

Příloha A – Skript pro generování pravidel filtrování MAC adres na porty pro RouterOS

Příloha A – Skript pro generování pravidel filtrování MAC adres na porty pro RouterOS

```
#Skript pro automatizaci port-security pravidel
#Testovano na:
# Mikrotik Cloud Router Switch CRS326-24G-2S+IN (RouterOS verze 7.8)
# Mikrotik Cloud Router Switch CRS328-4C-20S+RM (RouterOS verze 6.49)
#Autor: Ladislav Nepomucky

:put ("Seznam vseh portu a pres ne pripojenych adres:")
#ziskani vseh portu
:foreach port in=[/interface ethernet find] do={
    #navez a stav portu
    :local portName [/interface ethernet get $port name];
    :local portStatus [/interface ethernet get $port running];

    #vypis nazvu a stavu
    :put ("Port: $portName, Status:" . [:pick $portStatus 0 5]);

    #pokud je port aktivni
    :if ([:pick $portStatus 0 5] = true) do={

        :local arpEntries [/ip arp find interface=$portName]

        #prochazeni ARP zaznamu a vypis IP a MAC adres
        :foreach arpEntry in=$arpEntries do={
            :local ipAddress [/ip arp get $arpEntry address]
            :local macAddress [/ip arp get $arpEntry mac-address]
            :put (" IP adresa: " . $ipAddress . ", MAC adresa: " .
$macAddress)
        }
    }
}
```

```

:put ("\nVyberte porty, na kterych chete povolit aktualne pripojene MAC
adresy:")
:put ("Napiste je za sebou oddelene carkami ve tvaru ether1,ether2")
#uzivatelsky vstup
:global read do={:return}
#ulozeni vstupu do promenne
:local userInput [$read]

:foreach port in=$userinput do={
  #nazev a stav portu
  :local portName [/interface ethernet get $port name];
  :local portStatus [/interface ethernet get $port running];

  #pokud je port aktivni
  :if ([:pick $portStatus 0 5] = true) do={
    :local arpEntries [/ip arp find interface=$portName]

    #prochazeni ARP zaznamu a pridani MAC adres na seznam povolenych
    :foreach arpEntry in=$arpEntries do={
      :local macAddress [/ip arp get $arpEntry mac-address]
      :if ([:len $macAddress] > 0) do={
        /interface ethernet switch rule
        add ports=$portName src-mac-
address="$macAddress/FF:FF:FF:FF:FF:FF" switch=switch1;
        :put ("\n".$macAddress)
      }
    }
    #zakazani ostatnich MAC adres
    /interface ethernet switch rule
    add new-dst-ports="" ports=$portName switch=switch1;
  } else={
    :put ("Port ".$portName." neni aktivni")
  }
}

```