# PROPOSAL OF CYBER THREAT DETECTOR USING RASPBERRY PI

**David Hirš**
Master Degree Programme (2), FEEC BUT
E-mail: xhirsd00@stud.feec.vutbr.cz

Supervised by: Zdeněk Martinásek
E-mail: martinasek@feec.vutbr.cz

**Abstract**: Nowadays, the number of discovered vulnerabilities increases rapidly. In 2019, the 20, 362 vulnerabilities were discovered. Therefore, the probability of cyber-attacks realization and their economic impact are real. Currently, it is necessary to propose and implement automated and low-cost Intrusion Prevention Systems (IPS) that is applicable for home use or small corporate networks. The main goal of the system is to mitigate cyber-attack impact as fast as possible. In this article, we propose IPS based on Raspberry Pi that can detect and prevent many various cyber-attacks.

**Keywords**: Raspberry Pi, IDS, IPS, Suricata, Kismet, arpwatch

## 1 ÚVOD

Přínos výpočetní techniky pro společnost je bezpochyby nepopiratelný, avšak přináší i rizika v podobě kybernetických útoků. Tyto útoky mohou cílit na odepření služeb, odposlouchávání dat, jejich úprava, nebo i ovládnutí uživatelova zařízení. Tato skutečnost představuje velkou hrozbu pro zařízení komunikující uvnitř sítě. Ať už se jedná o domácí, pracovní či veřejnou síť. Žádoucím je ochránit svá aktiva před zneužitím. Současná situace zaznamenala růst rizik nejen ze zdravotního hlediska, ale i toho kybernetického [1]. Vzrůstá tedy potřeba chránit svá aktiva, avšak použití běžných prostředků je v některých případech nedostačující. Při pohledu na automatizované spuštění kybernetických útoků je vhodné přikročit i k systémům automatizované detekce hrozeb.

Článek neobsahuje popis útoků a možnosti jejich mitigace, avšak o této problematice pojednává publikace [2]. Hlavním přínosem článku je teoretický návrh nízkonákladového detektoru kybernetických útoků. Zařízení Raspberry Pi 4 typ B bylo vybráno jako vhodné pro implementaci detektoru. Zaměření detektoru je závislé na použitých nástrojích a je téměř všestranné. Vhodnými nástroji pro realizaci detektoru jsou IDS (Intrusion Detection System) a IPS (Intrusion Prevention System) zařízení [3]. Detekce kybernetických útoků probíhá na základě anomálií či signatur ze zachyceného síťového provozu [4]. Čtenář získá náhled na problematiku tvorby detektoru zaměřeného na útoky řazené do vrstev L2 až L3 modelu OSI/ISO. Detektor musí poskytnout dostatečnou ochranu před možnými hrozbami tak, jak si uživatel zvolí a nastaví.

## 2 VÝZKUM DOSTUPNOSTI NÁSTROJŮ PRO NÍZKO NÁKLADOVOU SONDU

Tato sekce popisuje IDS/IPS systémy, které byly otestovány a vybrány jako vhodné pro splnění cílů nízkonákladového detektoru. Jedná se o nástroje: **Arpwatch** - sledování ARP dotazů a zjištění nových zařízení v síti, **Kismet** - IDS systém pro bezdrátové komunikace a **Suricata/Snort** - systémy nabízí funkce IDS i IPS pro přímo připojená zařízení.

Systémy Suricata a Snort byly testovány na detekci útoku záplavou ICMP paketů. Testování hardwarového vytížení systémy Suricata a Snort probíhalo při monitorování sítě a zachycení útočníkem

generovaného útoku. Oba systémy pracovaly v režimu IPS. Využitá pravidla pro monitorování sítě byla volně poskytována samotnými organizacemi. Na základě těchto výsledků a subjektivního ohodnocení uživatelské přívětivosti byl vybrán systém Suricata verze 6.0.0.0. Následně byl testován IDS systém Kismet při monitorování bezdrátové sítě a oznamování zjištěných změn. Dále byl testován nástroj Arpwatch. Tento nástroj oznámil připojení nových zařízení do sítě a odhalil probíhající útok ARP spoofing. Nelze opomenout možnost užití vlastních skriptů psaných v programovacím jazyce Python. Programovací jazyk Python byl vybrán na základě obliby širokou veřejností a pozitivního ohlasu při jeho užití. Vlastní skripty představují nutný doplněk celého detektoru. Nedílnou součást představuje menu, které uživatele provede kompletním nastavením, více v kapitole4. Během testování použitelnosti jednotlivých systémů byly zaznamenány nároky na procesor (CPU) a operační paměť (RAM) zařízení Raspberry Pi. Výsledky měření těchto dvou systémů obsahuje Tabulka 1, kde jsou zapsaný hodnoty i zbylých vybraných systémů. Hodnoty v tabulce představují průměr z naměřených hodnot linuxovým softwarem *top*.

**Table 1:** Hardwarové nároky vybraných systémů

| Systém a verze | Vytížení CPU [%] | Vytížení RAM [%] |
|---|---|---|
| Suricata 6.0.0.0 | 23,7 | 1,2 |
| Snort 2.9.7.0 GRE | 28,3 | 2,7 |
| arpwatch 2.1a15 | 0,7 | 1,3 |
| KISMET 2020-00-GIT | 4,1 | 0,5 |
| KISMET chromium web browser | 42,9 | 5,4 |

## 3 REALIZACE EXPERIMENTÁLNÍHO PRACOVIŠTĚ

Nízkonákladový detektor bude realizován na zařízení Raspberry Pi 4 typ B. Jedná se o zařízení drobných rozměrů na které budou instalovány vybrané IDS/IPS systémy. Monitorovaný provoz zde bude vyhodnocován a na základě vyhodnocení budou provedeny příslušné akce. Uvnitř topologie se také nachází přístupový bod Mikrotik, ze kterého bude zrcadlený veškerý provoz na detektor. Zrcadlení provozu je zde nastaveno z důvodu, kdy bude sám Mikrotik vystaven útokům a i tato situace musí být monitorována. Diagram experimentálního pracoviště zobrazuje Obrázek 1. Zde je naznačen směr komunikace mezi jednotlivými uzly realizované topologie a jejich IP adresy. V diagramu jsou stanice útočníka i uživatele vyobrazeny jako dva odlišné stroje, avšak jedná se o dva virtuální stroje uvnitř jednoho fyzického zařízení. Raspberry Pi disponuje Wi-Fi přijímačem, který dovoluje bezdrátové připojení k zařízení Mikrotik. Doplněním popisu realizovaného experimentálního pracoviště je fotka reálného vzhledu pracoviště, viz Obrázek 1. Jak lze z fotky určit, Raspberry Pi je rozšířeno o USB síťový adaptér, skrze který je spojený jedním metalickým kabelem k přístupovému bodu Mikrotik. Rozšíření bylo přidáno z důvodu, kdy by bylo nutné připojit Raspberry Pi zároveň skrze metalický kabel i Wi-Fi. Mikrotik je dále spojený dalším metalickým kabelem k osobnímu počítači, na kterém je spuštěný systém útočníka Kali Linux, spolu s uživatelem Ubuntu Linux.

## 4 NÁVRH PROGRAMOVÉHO VYBAVENÍ DETEKTORU

Navržený detektor umožní uživateli vybrat použité systémy, funkce a zabezpečovanou síť. Významnou roli bude zastupovat IPS systém Surikata, který bude zaměřen na metalické spojení v síti. Uživatel by měl být schopný vybrat soubor pravidel, který Surikata bude následovat. Samozřejmostí je výběr rozhraní, na kterém bude Surikata naslouchat a definice dalších parametrů, se kterými systém Surikata může být spuštěn. Pro bezdrátové sítě bude sloužit jako detekční mechanismus systém Kismet. Umožněný musí být i výběr pravidel, které nesmí být porušeny komunikujícími zařízeními. Pro komunikaci na druhé vrstvě ISO/OSI bude sloužit nástroj Arpwatch. Konkrétně bude zaměřený na ARP protokol a jeho užití v síti. Situaci, kdy nebudou využité systémy dostatečné, bude pokrývat

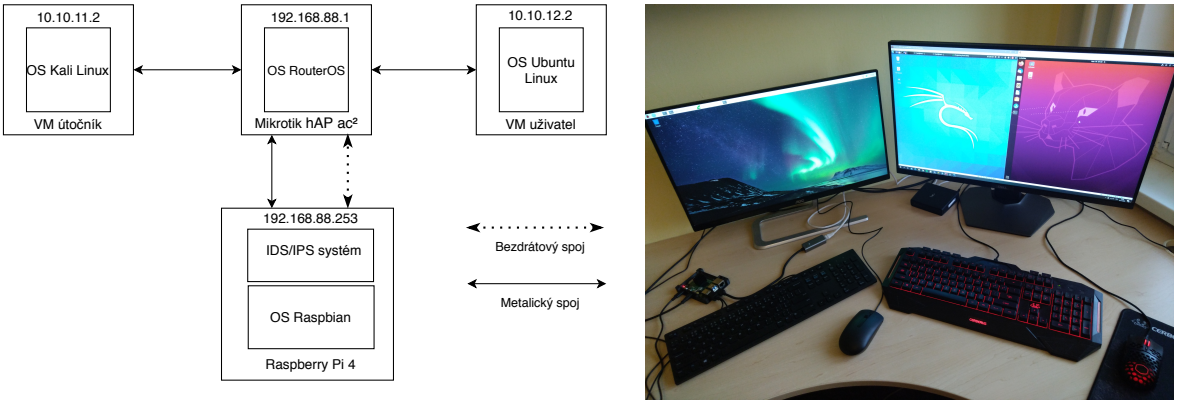


**Figure 1:** Realizované experimentální pracoviště.

tvorba vlastního skriptu, který bude zaměřený na daný incident. V případě většího počtu skriptů je nutné umožnit jejich výběr. Očekávaným výsledkem tedy bude jeden program, který bude ovládat zmíněné systémy. Reakce může probíhat na základě výpisu do logu od IDS systémů či výpisu do konzole. Grafické rozhraní není předpokládáno, což znamená ovládání jen z příkazové řádky. Tato skutečnost však nesmí záporně ovlivnit uživatelskou přívětivost programu. Veškerá menu a tištěné texty musí uživatele provést celým nastavením tak, aby výsledkem byl IPS systém dle jeho představ a požadavků. Po spuštění programu dojde k vytištění uvítacího textu a následně úvodního menu.

Toto menu obsahuje list dostupných systémů a skriptů, které uživatel může použít. Tištění textu do terminálu je rozdělené do dvou procesů kvůli situacím, které vrátí uživatele na začátek programu, ale již není žádoucí tisknout uvítání. Program čeká na interakci uživatele, který nyní může ukončit program, zvolit systém/skript a jejich nastavení, výpis aktivních systémů a skriptů, uvést do režimu Stand-By a nechat detektor pracovat. Uvedení programu do Stand-By vypíše aktivní systémy a skripty, následně čeká na ukončení celého programu od uživatele. Program v první fázi vypne jednotlivé systémy či skripty a následně ukončí sám sebe. Volba konkrétního systému či skriptu dále vede k vytištění informací o očekávaných parametrech a jejich hodnotách. Volba parametru následně poskytuje prostor pro zadání hodnoty vybranému parametru. Po zadání hodnoty dojde k opětovnému vytištění dostupných parametrů. Tímto způsobem uživatel definuje tolik parametrů, kolik bude potřebovat. Pokud jsou některé parametry vyžadované či chybně zadané, bude o této skutečnosti informován. Tato konfigurace bude obdobná každému z dostupných systémů i skriptů. Bude-li uživatel se spuštěnými systémy/skripty spokojený, musí se vrátit o krok zpět do úvodního menu. V tomto menu vybere uvedení programu do režimu Stand-By a nechá program pracovat tak dlouho, dokud uzná za vhodné. Vhodnou funkcionalitou se jeví možnost importu a exportu vybraných systémů, spolu s jejich nastavením. Grafický návrh programu pro nízkonákladový detektor představuje Obrázek 2.

## 5 ZÁVĚR

Efektivní obranu proti kybernetickým útokům nelze realizovat manuálně. Záměrem tohoto článku bylo popsat programové vybavení vhodné pro realizaci detektoru kybernetických hrozeb. Detektor není nutné vybudovat na vysoce výkonném zařízení. Dostačující je i rozměrově menší a výpočetně omezené zařízení, jakým je například Raspberry Pi 4 B. Takto realizovaný detektor je možné snadno přenášet a umístit jej takřka kamkoliv. Hlavním přínosem však je návrh samotného programu, který automatizuje proces nastavení a spuštění všech prvků detektoru. Praktická realizace navrženého programu pro detektor je do budoucna předpokládána, avšak nyní se jedná pouze o teoretický návrh.

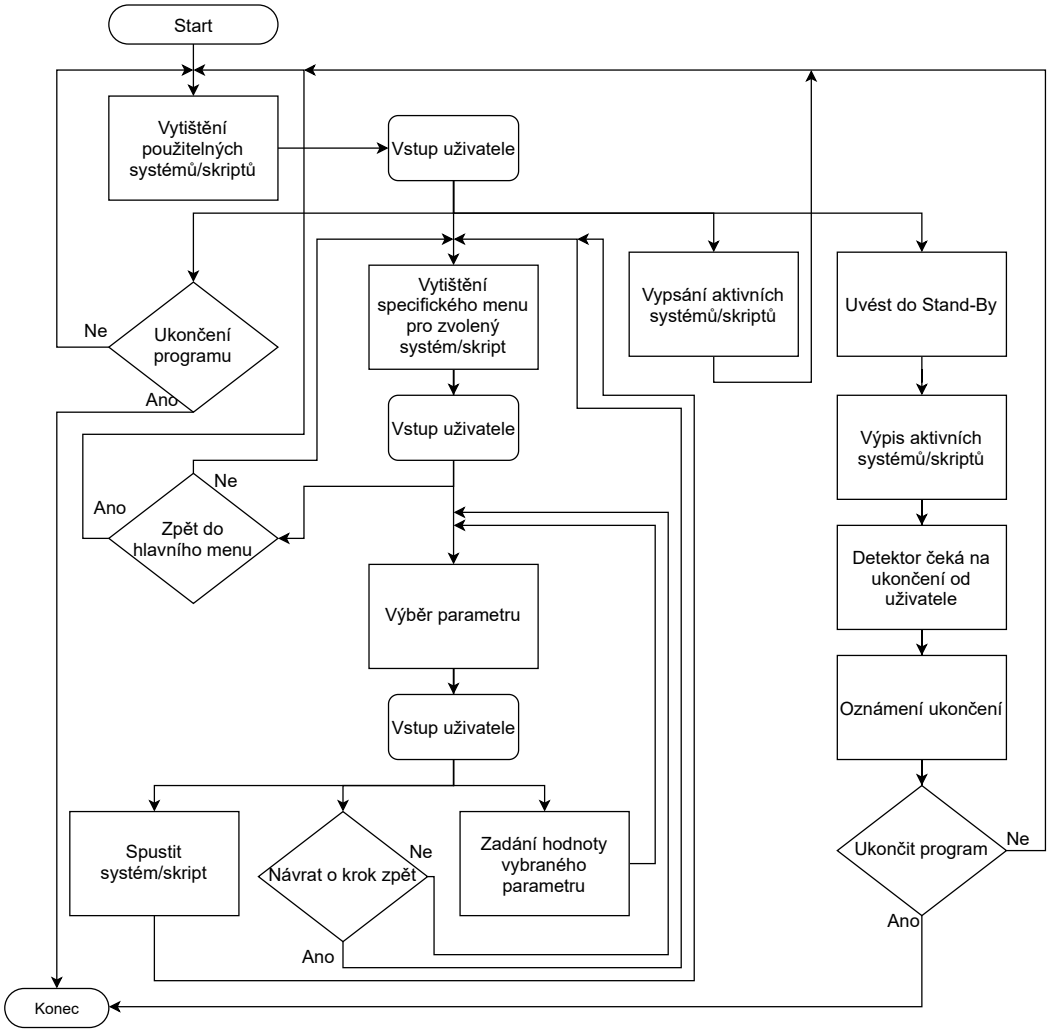


**Figure 2:** Diagram výsledného programu pro nízkonákladový detektor.

## PODĚKOVÁNÍ

Výzkum byl podpořen projektem MVČR s reg.č. VI20192022149.

## REFERENCES

[1] LALLIE, H. S., SHEPHERD, L. A., NURSE, J. R.C., EROLA, A., EPIPHANIOU, G., MAPLE, C., BELLEKENS, X.: Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. Computers & Security, 2021.

[2] HIRŠ, D., MARTINÁSEK, Z.: Přehled kybernetických útoků na linkové a transportnívrstvě. Elektrorevue - Internetový časopis (http://www.elektrorevue.cz), 2020, roč. 22, č. 1, s. 1-15. ISSN: 1213-1539

[3] SCARFONE, K., MELL, P.: Guide to Intrusion Detection and Prevention Systems (IDPS). In: NIST Special Publication (SP), 2012, 800-94 [online]. Gaithersburg, MD: National Institute of Standards and Technology, p. 1-111.

[4] NASEER, S., SALEEM, Y., KHALID, S., BASHIR M., HAN J., IQBAL, M., HAN, K.: Enhanced Network Anomaly Detection Based on Deep Neural Networks. IEEE Access [online]. 2018. 6, 48231-48246.