**UNICORN VYSOKÁ ŠKOLA S.R.O.**

BAKALÁŘSKÁ PRÁCE

**2022 Vojtěch Šetina**

**UNICORN VYSOKÁ ŠKOLA S.R.O.**

**Softwarový vývoj**

****

**BAKALÁŘSKÁ PRÁCE**

**Profylaxe síťových prvků**

**Autor BP:** Vojtěch Šetina

**Vedoucí BP:** Ing. Radim Roška

*Vzor:* ***ZADÁNÍ ZÁVĚREČNÉ PRÁCE*** *– originál, kopie originálu, naskenovaná podoba – dle jednotlivých forem (originál, 2 x kopie, elektronická verze)*

*Vzor:* ***ČESTNÉ PROHLÁŠENÍ*** *– prohlášení o samostatném vypracování závěrečné práce, datum a vlastnoruční podpis (v každém výtisku práce)*

**Čestné prohlášení**

Prohlašuji, že jsem svou bakalářskou práci na téma ....................... vypracoval/a samostatně pod vedením vedoucího bakalářské práce a s použitím výhradně odborné literatury a dalších informačních zdrojů, které jsou v práci všechny citovány a jsou také uvedeny v seznamu použitých zdrojů.

Jako autor/ka této bakalářské práce dále prohlašuji, že v souvislosti s jejím vytvořením jsem neporušil/a autorská práva třetích osob a jsem si plně vědom/a následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb.

Dále prohlašuji, že odevzdaná tištěná verze bakalářské práce je shodná s verzí, která byla odevzdána elektronicky.

V……………………. dne ……….. …….……………………………

Vojtěch Šetina

*Vzor:* ***PODĚKOVÁNÍ*** *vedoucímu BP, konzultantům, odborníků, spolupracovníkům za poskytnuté rady a podkladové materiály apod.) –* ***není povinné***

**Poděkování**

Např: Děkuji vedoucímu bakalářské práce Jméno Příjmení (i s tituly) za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce…

*Vzor:* ***PRVNÍ ČÍSLOVANÁ STRANA*** *– číslice na první číslované straně se určí podle počtu předchozích stran, počínaje Titulní stranou, tzn. že pokud jsou řazené všechny dané strany – Titulní strana, Zadání (2 strany), Čestné prohlášení a Poděkování – je první číslovaná strana stranou 6.*

**

**Profylaxe síťových prvků**

**Prophylaxis of network devices**

*Vzor: ABSTRAKT A KLÍČOVÁ SLOVA*

**Abstrakt**

Cílem bakalářské práce je vytvoření programu, který výrazně usnadní a zjednoduší dokumentaci síťové infrastruktury a skrz lepší znalost prostředí pomůže zvýšit úroveň zabezpečení. Program bude řešit profylaxi síťových prvků a její automatizaci. Bude rozdělen do dvou částí. První bude mít na starost dokumentaci a vizualizaci síťové topologie. Výsledkem budou tabulky se seznamem prvků – identifikace hardware modelu, nasazená verze operačního systému, používaných IP sítí, aktivních VLAN a IP rozhraní. Součástí bude také seznam všech portů a jejich konfigurace. V další části půjde o kontrolu nastavení zejména v kontextu doporučených bezpečnostních principů dle best-practice. Výsledkem bude report z několika běžně používaných nástrojů. Pomocí NMAP skeneru program zkontroluje otevřené porty, popřípadě vypíše známé zranitelnosti aktivních služeb. Skenem a následnou kontrolou konfigurací bude zjištěno, jaké služby má kontrolovaný síťový prvek zapnuté nebo například počet a jména uživatelů, kteří mají vzdálený přístup. Program vyzkouší defaultní přihlašovací údaje pro vzdálený přístup. Program bude primárně podporovat prvky od výrobce Huawei a Cisco.

Klíčová slova: Počítačové sítě, administrace, automatizace, switch, inventarizace

**Abstract**

The aim of the bachelor thesis is to create a program that will greatly simplify the documentation of the network infrastructure and through better knowledge of the environment will help to increase the level of security. The program will address the prophylaxis of network elements and its automation. It will be divided into two parts. The first will be in charge of the documentation and visualization of the network topology. The result will be tables listing the elements - hardware model identification, deployed operating system version, IP networks in use, active VLANs and IP interfaces. It will also include a list of all ports and their configurations. The next section will be a check of the settings especially in the context of recommended security principles according to best-practice. The result will be a report from several commonly used tools. Using the NMAP scanner, the program will check for open ports, or list known vulnerabilities of active services. The scan and subsequent configuration checks will identify what services are enabled on the network element being scanned or, for example, the number and names of users who have remote access. The program will test the default login credentials for remote access. The program will primarily support elements from Huawei and Cisco.

Keywords: Počítačové sítě, administrace, automatizace, switch, inventarizace

*Vzor:* ***OBSAH*** *– hierarchické uspořádání číslovaných názvů kapitol a podkapitol, včetně všech příloh, spolu s čísly jejich stran. Dále se uvádí Seznam obrázků/tabulek/grafů. Pozn.: počet a názvy kapitol samozřejmě odpovídají charakteru konkrétní práce.*

**Obsah**

[Úvod 11](#_Toc96879554)

[1 Úvod 13](#_Toc96879555)

[1.1 Motivace 13](#_Toc96879556)

[1.2 Struktura 13](#_Toc96879557)

[1.3 Cíl 13](#_Toc96879558)

[2 Rešerše a průzkum trhu 14](#_Toc96879559)

[2.1 Existující komerční řešení 14](#_Toc96879560)

[Závěr 16](#_Toc96879561)

[Seznam použitých zdrojů 17](#_Toc96879562)

[Seznam obrázků (existují-li) 18](#_Toc96879563)

[Seznam grafů (existují-li) 20](#_Toc96879564)

[Seznam příloh (existují-li) 21](#_Toc96879565)

[Příloha A – Název přílohy 22](#_Toc96879566)

[Příloha B – Název přílohy 23](#_Toc96879567)

*Vzor:* ***ÚVOD*** *(cca 5-10 normostran)*

# Úvod

V mé bakalářské práci se převážně věnuji tématu profylaxe síťových prvků a její automatizaci. Ačkoli by se mohlo na první pohled zdát, že síťová dokumentace a administrace nejsou tak tíživé a náročné úlohy, ze své vlastní zkušenosti vím, že se jedná o vcelku komplexní problém. Z několika desítek projektů pro střední a velké firmy, na kterých jsem v rámci své pracovní náplně podílel, jsem si mohl udělat obrázek, jak moc je síťová infrastruktura a její dokumentace podceňovaná. Z jednoduchého průzkumu u zákazníků a síťových specialistů jasně vyplívá, proč je administrace a dokumentace ve firmách na nízké úrovni. Jedná se totiž zpravidla o inventární a repetitivní práci. I když jde o neoblíbenou úlohu, která má na první pohled málo využití, tak hraje obrovskou roli v řešení incidentů a výrazně ovlivňuje bezpečnost celé firmy. Se stále se měnicí topologií a inventářem síťových prvků je časově náročné udržovat aktuální stav celého prostředí. K mému velkému překvapení se většina firem o komplexní dokumentaci vůbec nestará a pokud ano, většinu práce provádí administrátoři ‚ručně‘ – tedy bez použití automatizovaných programů a nástrojů.

*Vzor:* ***VLASTNÍ TEXT*** *závěrečné práce uspořádaný hierarchicky do kapitol a podkapitol, každá kapitola (úrovně 1) musí být vždy na nové straně.*

# Úvod

Autor/autorka uvedou vlastní název kapitoly vztahující se ke konkrétnímu tématu práce

## Motivace

Hlavní motivací ke zvolení tohoto tématu byla především snaha zefektivnit a automatizovat soubor akcí, které se používají k vytvoření takzvané profylaxe. Skládá se zejména z kontroly a získaní dat ze síťových prvků a jejich následné vyhodnocení. Vzhledem k tomu že pracuji ve firmě, která nabízí profylaxi jako jeden z jejich mnoha produktů a dosavadní postup byl tvořen převážně manuálními kroky (přihlášení do síťových prvků a jejich zkontrolování, kopírovaní dat z terminálu) rozhodl jsem se celý tento postup zefektivnit jak časově, tak i z pohledu využití lidských zdrojů.

## Struktura

Struktura bakalářské práce se skládá ze dvou hlavních částí, a to z části teoretické a praktické. Teoretická část obsahuje převážně informace ohledně síťové dokumentace a inventarizace, ale také srovnání dosavadních nástrojů na trhu. Hlavní náplní praktické části je vytvoření skriptu se všemi náležitostmi jako je například diagram, dokumentace a popis hlavních funkcí skriptu.

## Cíl

Hlavním cílem této bakalářské práce je vytvoření programu, který výrazně usnadní a zjednoduší dokumentaci síťové infrastruktury a skrz lepší znalost prostředí pomůže zvýšit úroveň zabezpečení. Největší důraz bude kladen na automatizaci celého řešení profylaxe. Výstupem programu budou tabulky se seznamem prvků a jejich informacemi společně s best-practise principy pro zabezpečení a zvýšení transparentnosti síťové infrastruktury. Program bude mít konfigurační soubor a dokumentaci pomocí které půjde script jednoduše upravit podle toho, co bude dané řešení potřebovat. Script bude primárně podporovat prvky od výrobce Huawei a Cisco.

# Rešerše a průzkum trhu

## Existující komerční řešení

Síťová administrace má celosvětově obrovský trh, a to hned z několika důvodů. Každá firma, ať už se jedná o malou či velkou, má několik síťových prvků, na kterých stojí celý její chod. Z pravidla se jedná o switche a routery, ale také firewally. Těchto zařízení může být ve společnosti vysoký počet a jednoduše se tak může stát, že ztratíme přehled o těchto zařízeních. Se stále narůstajícím rizikem kyberútoků je důležité mít svou infrastrukturu pod kontrolou, mít aplikované nejnovější opravy chyb a dělat pravidelné kontroly zabezpečení.

Jeden z největších hráčů na trhu se síťovou administrací je SolarWinds. SolarWinds nabízí velké množství systému a služeb, které ulehčují práci nejen síťovým administrátorům. Komerční řešení od této společnosti má mnoho skvělých funkcí, jako je například automatické nalezení nových prvků v síti nebo automatickou konfiguraci zařízení. Tento nástroj je velice robustní, avšak relativně drahý, a proto je převážně určen velkým firmám s vysokým počtem vlastních zařízení. Pro menší či střední společnosti s menším počtem síťových zařízení se nástroj nehodí, ať už jde o pokročilé funkce, které menší podniky nevyužijí nebo o samotnou cenu tohoto nástroje.

Další společností, která se specializuje na automatizaci síťové administrace je firma Auvik. Software této firmy, který je designován tak, aby běžel přímo v cloudu, nabízí propracované funkce a širokou podporu zařízení od mnoha výrobců. Auvik klade velký důraz na automatizaci a jednoduchost používaní a nabízí také mnoho integrací do nástrojů třetích stran jako je například komunikační nástroj Slack nebo ticketovací systém Freshdesk.

## Dostupné opensource nastroje

# Analýza

Z

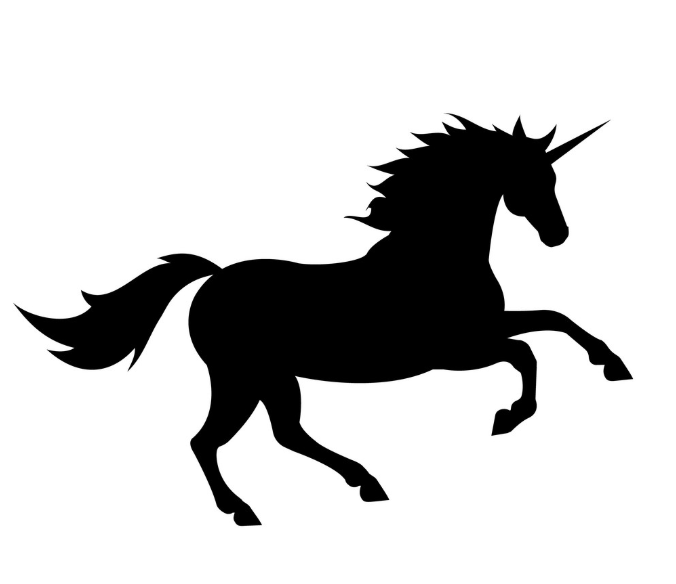
*Obrázek se v textu značí následujícím způsobem: samotný obrázek se označí: „****Obrázek 1: Název obrázku****“ (11 nebo 12 pt, černě, tučně). Obrázky se označují názvem a číslováním nad obrázkem a zdrojovým dokumentem pod obrázkem, příp. informace o vlastním zpracování (11 nebo 12 pt, černě). K popisování doporučujeme využít nástroje textového editoru, který usnadní generování seznamu obrázků na konci práce.*

**Obrázek 1: Logo**



Zdroj: č

**Obrázek 2: Obrázek jednorožce**



Zdroj: Vlastní zpracování

*Tabulky se označují názvem a číslováním nad tabulkou a zdrojovým textem pod tabulkou. Tabulky, obrázky a grafy se číslují zvlášť. Každá tabulka, obrázek nebo graf MUSÍ být v textu okomentován. Je nepřípustné, aby jednotlivé kapitoly (podkapitoly) tvořilo pouze grafické znázornění v podobě tabulek, grafů, obrázků, schémat atp. bez jejich okomentování.*

**Tabulka 1: Statistika vět zachovaných a vyřazených filtr. kritériem *FK1***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sada** | **Celkem** | **Zachováno** | **Vyřazeno** | **Zachováno** |
| **dtest** | 5228 | 2384 | 2844 | 45,6 % |
| **etest** | 5476 | 2419 | 3057 | 44,2 % |
| **train-1** | 4709 | 2204 | 2505 | 46,8 % |

Zdroj: Vlastní zpracování

**Matematické rovnice, vzorce**

*Pokud jsou v práci rovnice, nezapomeňte je správně číslovat. Pro jejich zápis používejte MS Editor rovnic, případně jinou obdobnou aplikaci. Rovnice by měla vypadat například takto (nezapomeňte proměnné popisovat):*

|  |  |
| --- | --- |
|  | (1) |

*kde S je obsah kruhu o poloměru r .*

# Závěr

Tato kapitola se nečísluje. Rozsah je zpravidla 5-10 normostran.

# Seznam použitých zdrojů

V seznamu zdrojů musí být uvedeny všechny v závěrečné práci citované zdroje. Zároveň nesmí seznam obsahovat zdroje, které nejsou v závěrečné práci použity.

Používáme citační normu ČNS ISO 690. Doporučujeme pro tvorbu citací některý z citačních nástrojů, které jsou v základní verzi zpravidla zdarma dostupné.

• HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.

• KUROSE, James F. a Keith W. ROSS. Počítačové sítě. Brno: Computer Press, 2014. ISBN 9788025138250.

• SUMMERFIELD, Mark. Python 3: výukový kurz. 2. vydání. Přeložil Lukáš KREJČÍ. Brno: Computer Press, 2021. ISBN 9788025150306.

• 3.10.1 Documentation. [online]. Copyright © [cit. 30.12.2021]. Dostupné z: https://docs.python.org/3/

• Welcome to NAPALM’s documentation! — NAPALM 3 documentation. [online]. Copyright © Copyright 2021, David Barroso [cit. 30.12.2021]. Dostupné z: https://napalm.readthedocs.io/en/latest/

• What is Network Penetration Testing? - Penetration Testing | aNetworks. Cyber Security, Managed IT, Cloud, & Consulting Services | aNetworks [online]. Copyright © 2021 [cit. 30.12.2021]. Dostupné z: https://www.anetworks.com/what-is-network-penetration-testing/

• Projekty ve firmě Altepro Solutions a.s.

o Rozšíření a profylaxe sítě Nemocnice Pardubického kraje

o Monitoring sítě – Česká televize

• GitHub Documentation. [online]. Copyright © [cit. 30.12.2021]. Dostupné z: https://docs.github.com/en

• Network Management Guide: How To, Best Practices, & Tools - DNSstuff. Software Reviews, Opinions, and Tips - DNSstuff [online]. Copyright © 2021 SolarWinds Worldwide, LLC. All rights reserved. [cit. 30.12.2021]. Dostupné z: https://www.dnsstuff.com/network-management

# Seznam obrázků (existují-li)

Obrázek 1: Logo 11

Obrázek 2: Obrázek jednorožce 12

**Seznam tabulek (existují-li)**

[Tabulka 1: Statistika vět zachovaných a vyřazených filtr. kritériem *FK1* 12](#_bookmark9)

# Seznam grafů (existují-li)

# Seznam příloh (existují-li)

*Každá příloha musí být alespoň jednou odkázána do vlastního textu práce. Přílohy se číslují. Každá příloha začíná na nové stránce.*

# Příloha A – Název přílohy

# Příloha B – Název přílohy