**DDoS útoky a obrana proti nim**

**Simulace DDoS útoku a nalezení nejlepší možnosti obrany**

**DDoS attacks and protection against them**

**Simulation of DDoS attack and finding the best defend**

**option**

Projekt 1.

Studijní program: Informatika a kybernetika ve zdravotnictví

Autor práce: Šimon Kochánek

Vedoucí práce: Ing. Jan Mužík, Ph.D.

**Zadání práce**

Vyberte vhodný nástroj na simulaci DDoS útoků. Otestujte, jaký RPS vydrží web server, který vám určí vedoucí práce. Následně webserver ochraňte pomocí vhodného nástroje (např. CloudFlare DDoS Protection for Web Applications) a opět pomocí simulace ověřte odolnost vůči DDoS.

**PROHLÁŠENÍ**

Prohlašuji, že jsem práci s názvem „DDoS útoky a obrana proti nim“ vypracoval samostatně a použil k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k práci.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu §60 Zákona č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Kladně 24.1.2022 …...….………...………………...

Šimon Kochánek

**PODĚKOVÁNÍ**

Rád bych poděkoval Ing. Janu Mužikovi za vedení mé práce a příležitost se něco naučit v poli kybernetické bezpečnosti a vyzkoušet si DDoS útok ve větším měřítku.

**ABSTRAKT**

DDoS útoky a obrana proti nim: Simulace DDoS útoku a nalezení nejlepší možnosti

obrany

Na začátku jsem musel zjistit, jak funguje DoS, DDoS útok a zjistit jejich typy. Dále najít vhodný prostředek na simulaci útoku a simulovat útok na web server a zjistit kolik vydrží. Poté vybrat vhodný ochranný prostředek, kterým ho ochráním. Na konec následoval druhý útok tentokrát překažen ochranou.

**Klíčová slova**

DDoS útok, DoS, DDoS, obrana DDoS, ochrana DoS

**ABSTRACT**

DDoS attacks and protection against them: Simulation of DDoS attack and finding the best defend option

In the beginning of my work I needed to research on how Dos,DDoS attack works and their types.Then I needed to find the most suitable tool for simulating attacks.I tried simulating the attack on web server with estimating how much RPS it can handle. After first attack I needed to find the best protection.When I deployed the protection I initiated the second attack and it was unsucessful.

**Keywords**

DDoS útok, DoS, DDoS, obrana DDoS, ochrana DoS

Obsah

[Seznam symbolů a zkratek 8](#_Toc476327912)

[1 Úvod 9](#_Toc476327913)

[1.1 Přehled současného stavu 9](#_Toc476327914)

[1.1.1 Základ počítačové sítě](#_Toc476327916) 9

[1.1.2 DoS útok](#_Toc476327916) 10

[1.1.3 DDoS útok](#_Toc476327916) 10

[1.1.4 Typy útoků](#_Toc476327916) 11

[1.1.5 Ochrana proti DDoS útokům](#_Toc476327916) 12

[1.2 Cíle práce 1](#_Toc476327915)3

[2 Metody 1](#_Toc476327917)4

[2.1 Způsob výběru a testování softwarů na simulaci útoku 14](#_Toc476327914)

[2.2 Simulování útoku a vytváření testovacího prostředí 1](#_Toc476327914)5

[2.3 Kritéria výběru nástroje na ochranu proti DDoS 1](#_Toc476327914)5

[2.4 Ochrana proti druhému DDoS útoku 1](#_Toc476327914)6

[3 Výsledky 1](#_Toc476327918)8

[4 Diskuse](#_Toc476327919) 20

[5 Závěr](#_Toc476327920) 21

[Seznam použité literatury](#_Toc476327921) 22

# Seznam symbolů a zkratek

#### Seznam zkratek

|  |  |
| --- | --- |
| Zkratka | Význam |
| DoS  DDoS | Denial of Service (odmítnutí služby)  Distributed Denial of Service (distribuované odmítnutí služby) |
| *TCP*  Bandwidth  P2P  ICMP  HTTP  HW  SW  LOIC  RPS | Transmission Control Protocol  Šířka přenosového pásma  Peer to peer (komunikace v počítačové sítí každý s každým)  Internet Control Message Protocol  Hyper Text Transfer Protocol  Hardware (fyzicky existující technické prvky)  Software (Programové vybavení, nehmatatelné programy, aplikace)  Low Orbit Ion Cannon (nástroj na simulaci DoS útoku)  Requests per second(Počet požadavků za vteřinu) |
|  |  |

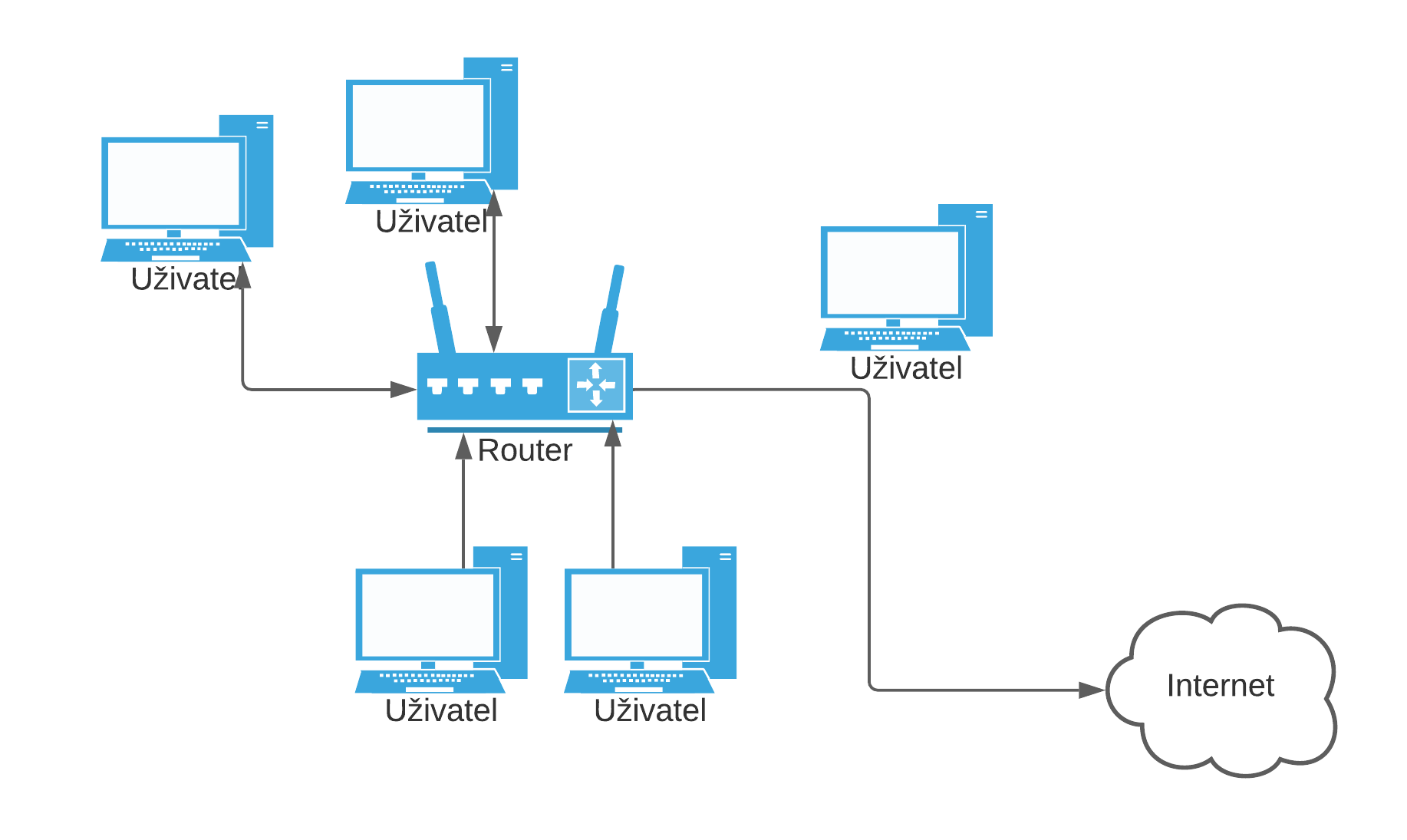
# Úvod

Moje práce se zaměřuje na běžný problém každého síťového prvku přístupného z internetu, ale také klidně v rámci lokální sítě. Každý den můžeme na vlastní oči vidět nebo slyšet o DDoS útoku a jak nějaká služba nebo firma nemůže poskytovat fungovat normálně, protože na ně někdo útočí.

Zaujala mě tato problematika vzhledem k faktu, že jsem se několikrát stal přímo nebo nepřímo oběti DDoS útoku a tato příležitost se nedala odmítnout. Celkově mě zaujímá téma kybernetické bezpečnosti a jsem přesvědčen, že v budoucnu se každá zkušenost se zabezpečováním počítačových systémů náležitě vyplatí.

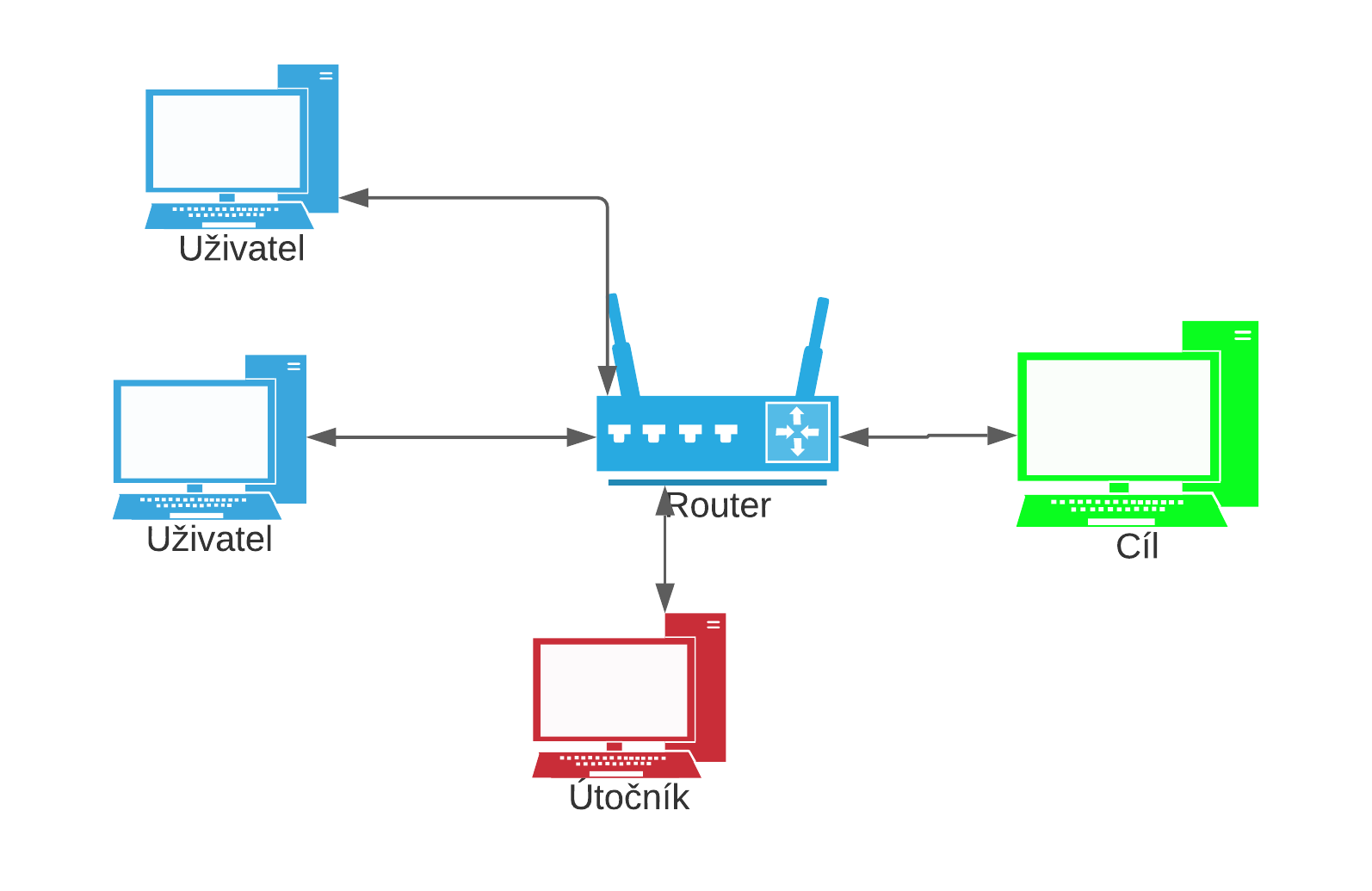
## Přehled současného stavu

### Základ počítačové sítě

Úplně na úvod musíme definovat co je počítačová síť. Počítačovou síť si můžeme představit jako několik počítačů nebo síťových zařízeních propojených do sebe ve tvaru hvězdy (viz. obrázek 1.1). Vždy musí být prostřední bod, který spojuje zařízení. V tomto propojení má pak každý aktivní prvek (kromě např switche, hubu atd.) svou vlastní adresu. V obrázku 1.1 jsou všechny zařízení připojeny do směrovače, který má nejen schopnost propojovat, ale zároveň rozřazovat sítě a adresovat do jiné. Pokud jakýkoliv prvek chce komunikovat musí získat tuto adresu a následně začít komunikaci podle zvoleného protokolu. Tato síť se pak může připojit k internetu a je důležité ji směrovat přes router neboli směrovač.

**Obr. 1.1:** Počítačová síť. Model: autor.

### DoS útok

Když přeskočíme adresování a routování počítačových sítí. Můžeme se ponořit do problematiky útoku DoS. Pro každého uživatele existuje např. jeden kabel, a to ten má maximální šířku pásma, které může komunikace obsáhnout tzv. bandwidth. A tady přichází na scénu hlavní myšlenka DoS útoku. Klade si za cíl zaplnit bandwith odesílán enormního počtu požadavků, a zahltit komunikační kanál zařízení.

**Obr. 1.2:** Počítačová síť s DoS útočníkem. Model: autor.

Jak je vidět na obrázku 1.2 útočník je jeden. Útočník si vybere, jaký přesně útok chce použít a pak vytíží připojení k cíli a tím může shodit, zamezit, či zahltit službu nebo síťový adaptér jako takový. Často se tato myšlenka vysvětluje na dálnici, kdy jeden útočník zastaví svým autem všechny pruhy, takže ostatní neprojedou.

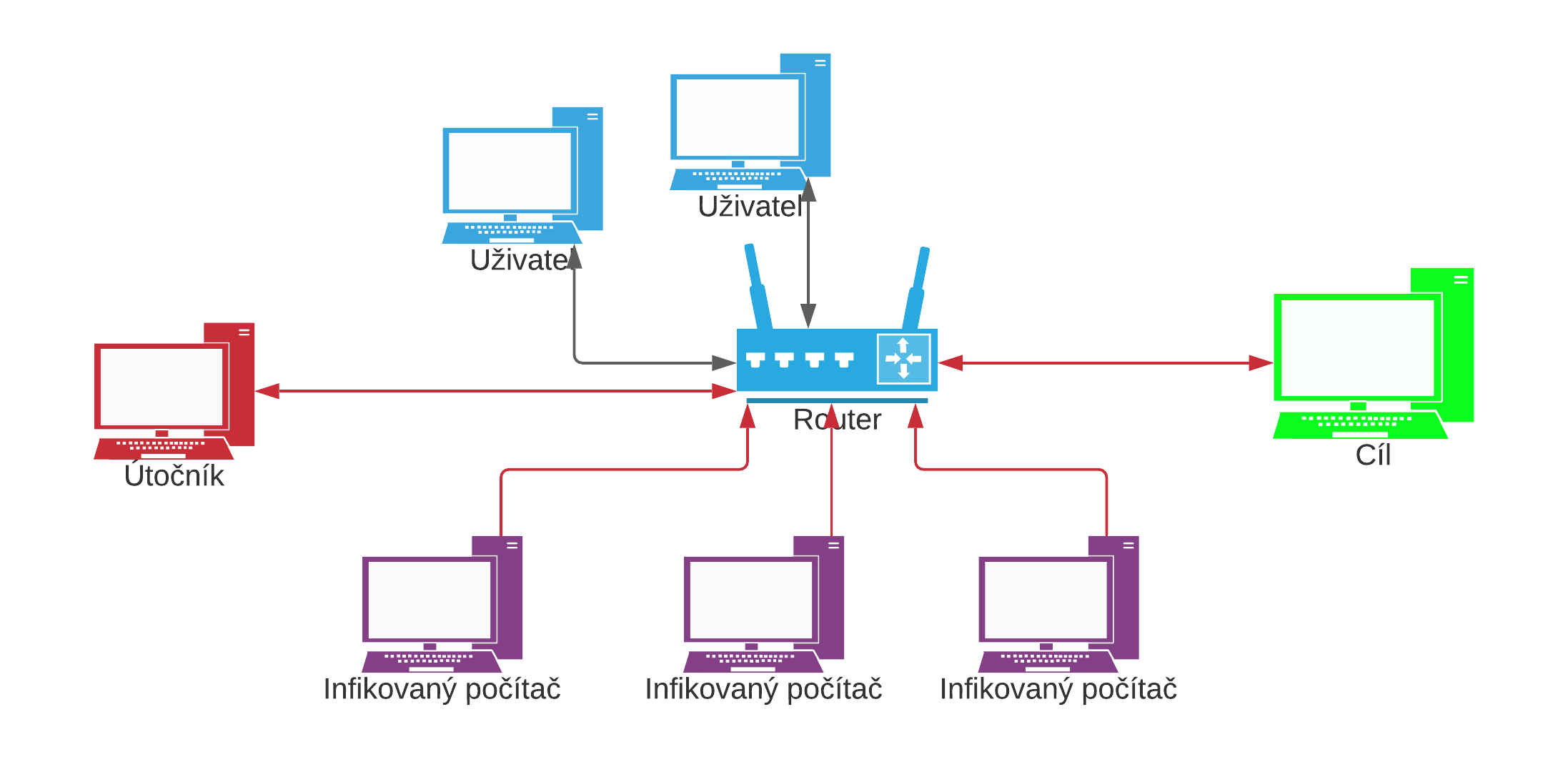
### DDoS útok

Koncept DDoS je po pochopení DoS útoků analogický. Další D ve zkratce DDoS nám říká, že je útok distribuovaný. Z to si zas můžeme na té dálnici představit tak, že útočník není jen jeden, ale skupina se dohodne na zastavení všech pruhů a bude tam stát a tím tvořit větší bariéru, než kdyby byl samostatný.

Tento útok se provádí přes tzv. botnet. Tedy síť infikovaných počítačů, které poslouchají hlavního útočníka. Na obrázku 1.3 vidíme botnet, který útočí na cíl. Jsou dvě hlavní možnosti ovládání botnetu.[1]

U té první se každý infikovaný útočník připojí k útočníkovi a poslouchá ho případně, si stáhne plán útoků. Plán pak v přesně stanovený čas dodrží a s dalšími infikovanými počítači DoSují cíl. Jedná se tedy o architekturu klient-server.[1]

U té druhé pomocí způsobu P2P komunikují nakažené počítače mezi sebou a útočník se může mezi nimi schovat a vydat příkaz o útoku. Při tomto způsobu je těžké určit přímo útočníka, protože se tváří jako nakažený počítač. Když všichni opakují plán útoku je těžké nalézt toho prvního co začal tuto informaci šířit.[1]

**Obr. 1.3:** Počítačová síť s botnetem. Model: autor.

### Typy útoků

Jak už jsem nastínil je několik typů útoku. Začneme od nejjednodušších.

ICMP flood – Zatížení útočníka pomocí ICMP echo requestů. Protokol ICMP je pouze na test konektivity sítě a při tomto útoku je u pingu nastaven co největší možný bandwidth kvůli zahlcení bandwidthu sítě.[2]

UDP flood – Přetížení cíle pomocí UDP protokolu. Cíl útoku je útočit na otevřené porty, což způsobí, aby cíl kontroloval aplikace, které na nich naslouchají a musí využívat prostředky na kontrolu těchto portů což cíl zahltí.[3]

SYN flood – Využívá slabosti v TCP protokolu. TCP uplatňuje tzv. three-way-handshake kdy se začíná komunikace tzv. SYN požadavkem jako žádost o synchronizaci. Protějšek na to odpoví SYN-ACK. Útočník vysílá stále SYN requesty, ale neodpovídá na SYN-ACK, tudíž server stále vysílá tyto odpovědi a zas využívá zdroje na tuto komunikaci.[3]

HTTP flood – Útočník posílá legitimní HTTP GET a POST požadavky, aby útočil na cílový web server nebo aplikaci. A vyžaduje menší bandwith aby shodil cíl. Nejefektivnější útok je, když cíl alokuje maximální množství prostředků na každý požadavek [3] Následovala otázka, jak se bránit proti těmto útoků.

### Ochrana proti DDoS útokům

Ochrana proti DDoS útokům existuje a je na velmi pokročilé úrovni, ale je složitější, než je tento jednoduchý útok. Nejdříve jsem musel zjistit, jak se rozděluje. S ochranou počítačových sítí už jsem měl předchozí zkušenosti a typy se jsou dosti analogické.

Jako první je samozřejmě hardware ochrana ve smyslu routeru nebo firewallu který dáte buď před váš cíl nebo rovnou před prvotní vstup do sítě. Toto zařízení pak může rovnou filtrovat vstup do sítě, blacklistovat IP adresy, omezit počet připojení z jedné adresy a nastavit timeout připojení po kterém se připojení ukončí. Také mnoho dnešních domácích routerů už umožňuje nastavení ochrany DoS (Například domácí router TP-Link Archer C7 1750 nabízí tuto ochranu). Tato ochrana je asi nejlepší, jelikož ji máme plně pod kontrolou a zároveň není SW část daného cíle.

Když nemůžeme nebo nechceme řešit ochranu pomocí hardwaru přichází software. Na našem cíli můžeme nastavit firewall na příchozí komunikaci a omezit v ní parametry podobně jako v HW řešení. Například ve Windows je zabudovaná systémová aplikace Windows Firewall, která umožňuje všechny tyto parametry nastavit. Pro Linux je možnost nainstalovat firewall balíček např. iptables.[4]

Jako další řešení je hybridně či kompletně přenést cíl do Cloudu. Cloud provider nám ručí za bezpečnost a ochranu dat a je často velice jednoduché nastavit DDoS ochranu. Např. u Microsoft Azure nám stačí zadat plán na ochranu naší architektury a Microsoft se postará o zbytek.[5]

## Cíle práce

Práce byla rozdělena na mnoho cílů, a to jak teoretické, tak praktické. Jako první cíl nepsaný v zadání bylo provést obsáhlou rešerši ve které jsem musel proniknout vůbec do problematiky. Úplně prvním cílem bylo zjistit, jak přesně DoS útok funguje. To znamená, na jakých vrstvách OSI modelu počítačové sítě probíhá, jak funguje, a hlavně co přesně si klade za cíl. Když jsem pochopil toto dalo se to aplikovat na DDoS kde se mění jenom počet útočníka z jednoho na několik. Když jsem tuto rešerši udělal, začal jsem vyhledávat nástroj na simulaci útoku.

Další cíl představovalo najít ideální nástroj. Musel jsem vyhodnotit kritéria pro takový nástroj, jak by se měl chovat a ideální vlastnosti. Pak následoval výběr nástroje splňující požadovaná kritéria. Po vybrání několika programů či skriptů jsem zahájil simulaci útoku. Pro svůj jsem musel navrhnout několik scénářů. Poté jsem začal prozkoumávat nabídku ochrany proti DDoS a vybírat co by se hodilo přesně pro zadání.

Pak jsem aplikoval vybranou ochranu na cíl a opakoval útok, jehož cílem bylo zjištěné, jestli ochrana funguje. Následně vyvodit závěry a práci uzavřít.

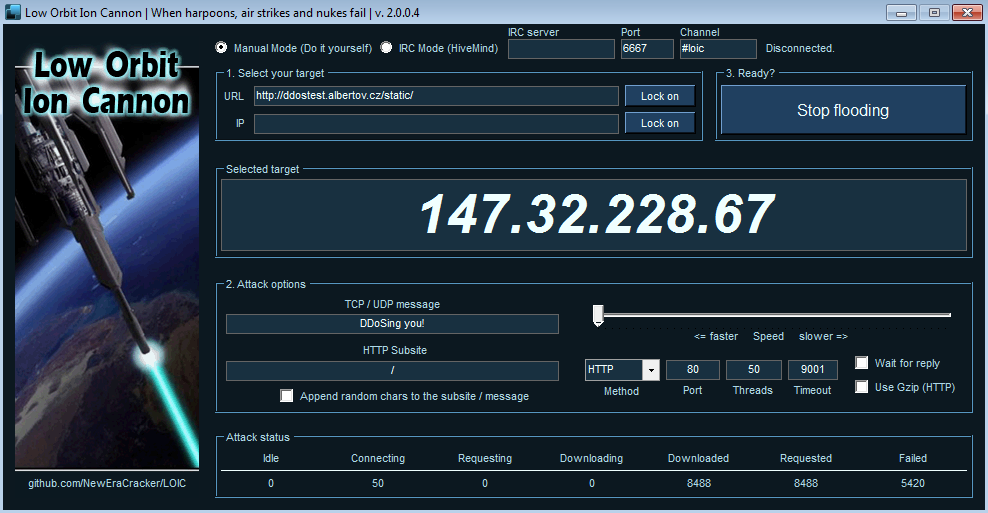
# Metody

## Způsob výběru a testování softwarů na simulaci útoku

Podle zadání jsem měl vybrat nástroj na simulaci DDoS útoku.

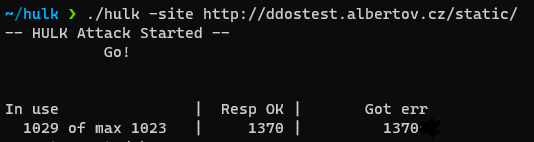
Bylo několik kritérií, podle kterých jsem vybíral software:

* Pro operační systém Windows a nejlépe i pro Linux
* Vyžadován open source, tedy volně dostupný zdrojový kód
* Ovládání jak v grafickém uživatelském rozhraní, tak v příkazové řádce
* Možnost měnit počet vláken, typ a rychlost útoku.
* Statistika o počtu připojení, provedených požadavků a počtu nepovedených
* Možnost zabudované možnosti ovládání pomocí botnetů výhodou

Po uvážení těchto kritérii jsem se vydal hledat ideální nástroj. Hned po několika dotazů na nejlepší útočný nástroj mě zaujala open source verze LOIC [6]. Na obrázku 2.1 je vidět, jak vypadá grafické uživatelské rozhraní. Na tomto snímku zrovna útočí na jeden dovolený web server

**Obr. 2.1:** LOIC při útoku. Snímek: autor.

Tento program je napsán v programovacím jazyce C# a je bohužel určena jen primárně pro Windows. Na Linux vyžaduje použití aplikace Wine, nebo Mono. Na druhou stranu dovoluje jak příkazovou řádku, tak graficky uživatelské rozhraní. Funguje velmi krásně a dovoluje uživateli všechny zmíněné požadavky. Dokonce dovolí se připojit na botnet pomocí IRC, což je služba na chatování kde tento program poslouchá a vykonává příkazy.

Pro Linux jsem našel nástroj Hulk [7]. Na obrázku 2.2 můžeme vidět mnou upravený výstup z toho skriptu při útoku. Tento nástroj pro příkazovou řádku je v napsán ve skriptovacím jazyce Go a Python. Používá jen HTTP Request flood. Tento program se mi zdál nejlepší, jelikož se dá snadno upravit, je spolehlivý a hlavně efektivní.

**Obr. 2.2:** Hulk při útoku. Snímek: autor.

## Simulování útoku a vytváření testovacího prostředí

Jako první jsem si vytvořil pomocí Oracle VirtualBox několik virtuálních strojů s operačním systémem Windows 7.Následně jsem vytvořil virtuální stroj s Debianem, na který jsem nainstaloval apache2 jako web server. Poté jsem simuloval DDoS útok na web server. Tento útok jsem poté vylepšil tím, že jsem každému virtuálnímu stroji nastavil síťový most, takže existoval každý v mé sítí a veškerý provoz, a tedy i útok šel přes router v mé sítí. Pomocí tohoto jsem docílil docela věrnou simulaci a eliminoval jsem virtuální síťové prostředí, které VirtualBox nabízí.

Když jsem skončil tuto simulaci, vyhodil jsem virtuální stroj s Debian web serverem a začal útočit na web server ze zadání fhir.cz/aspnet. Útok jsem stupňoval po jednom počítači a měřil zatíženost a latenci. Vydržel průměrně 240 000 RPS. Poté začal web server házet HTTP 503 error Service Unavailable a kompletně přestal odpovídat po síti.

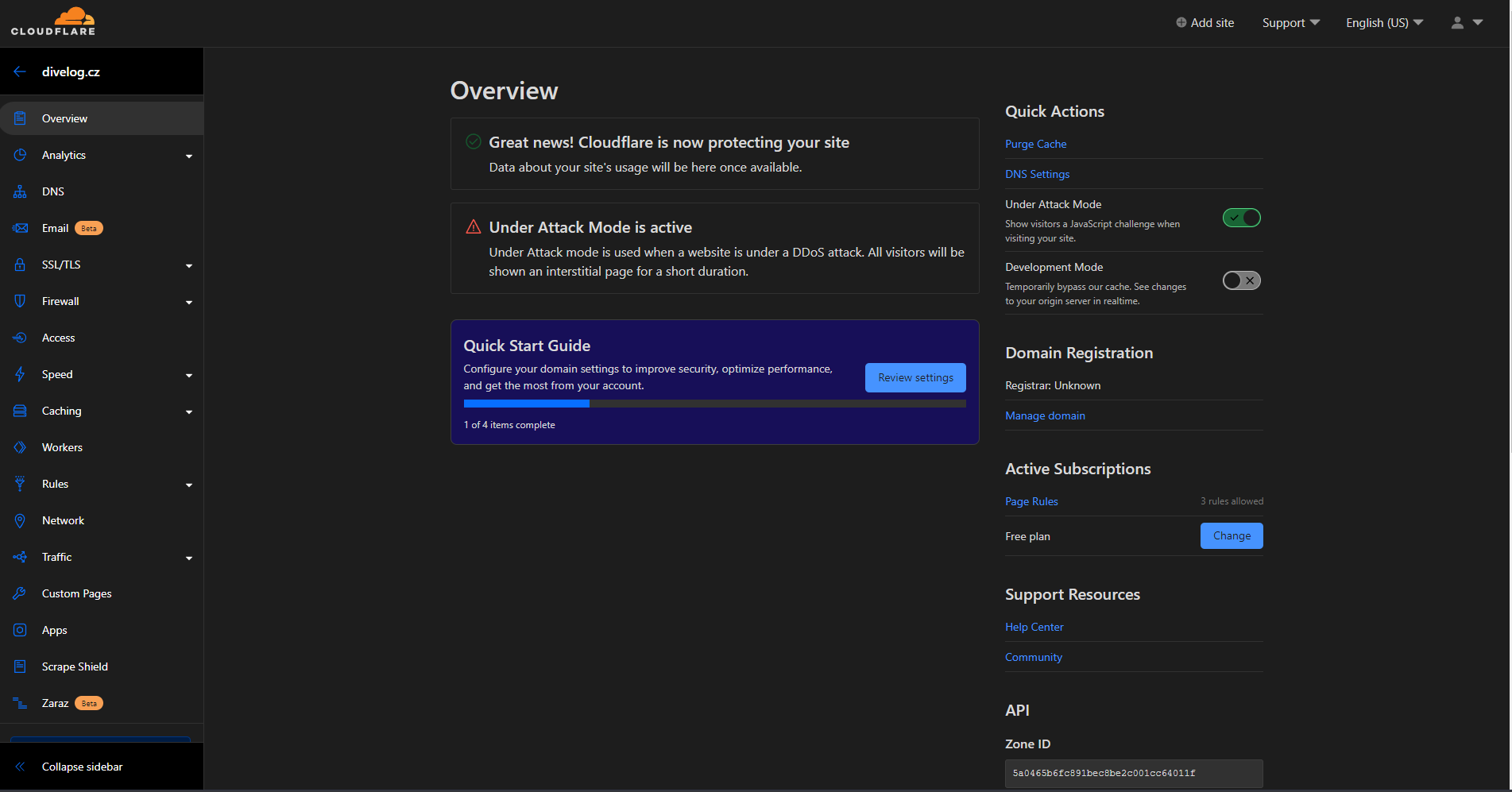
## Kritéria výběru nástroje na ochranu proti DDoS

Vybíral jsem na základě ceny, možností nastavení, rozšíření, a hodnocení.

V konkrétním případě a podle kritérií mi vychází ze zadání už nastíněná cloudová služba

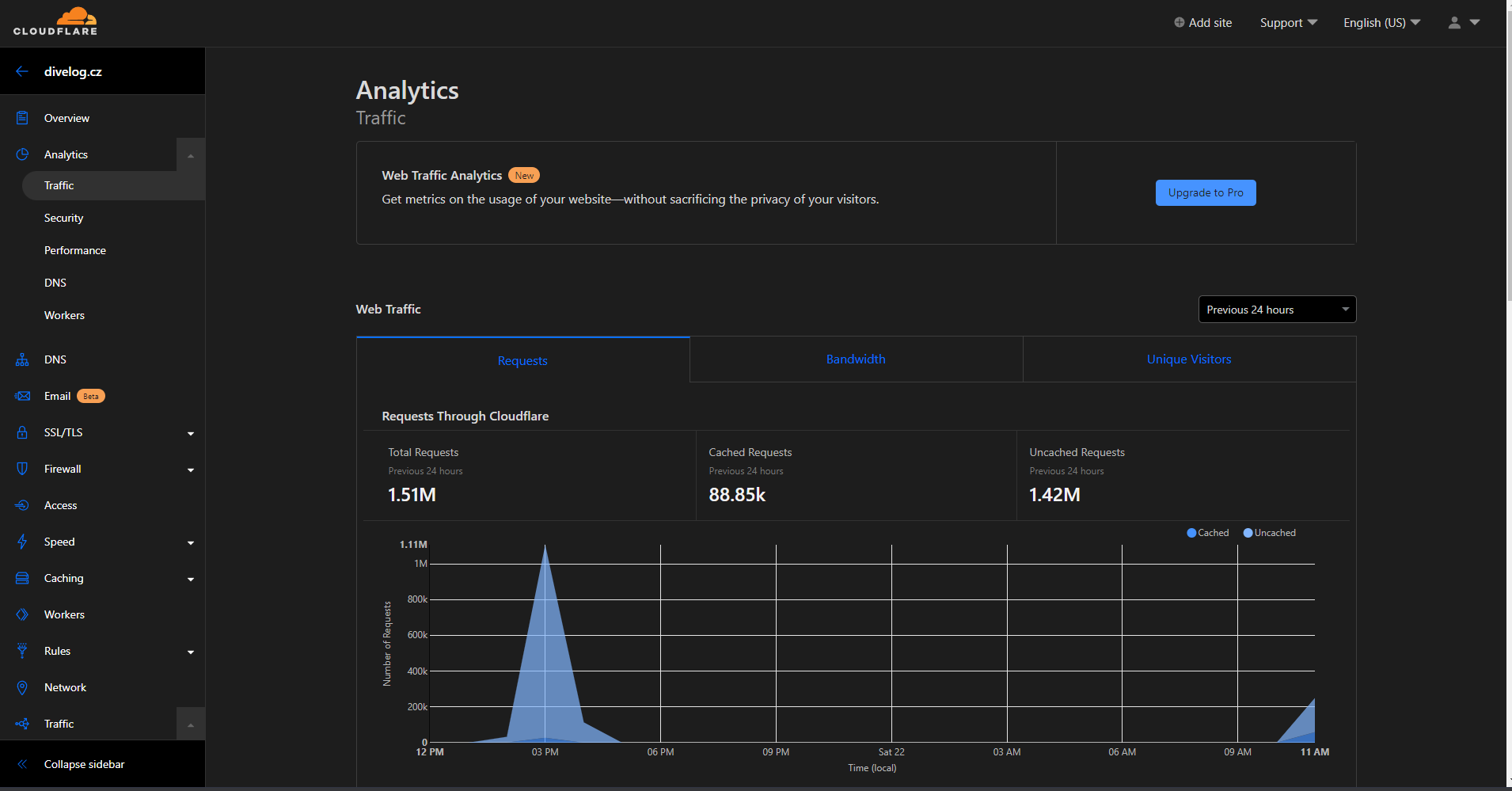
CloudFlare DDoS Protection for Web Applications [8]. Tato služba nabízí proxy server, který má možnost schovat web server a jeho IP adresu. Tento proxy server pak přijímá veškerý provoz a filtruje jen ty, které splňují bezpečnostní pravidla (např. povolená IP atd.). Tento přefiltrovaný provoz pak dostane odpověď od našeho serveru, ale přes Cloudflare proxy, takže náš server je relativně v bezpečí.

## Ochrana proti druhému DDoS útoku

Na obrázku 2.3 můžeme vidět, jak vypadá dashboard, který nás uvítá při přístupu do Cloudflare služby kde jsem si přihlásil svou doménu.

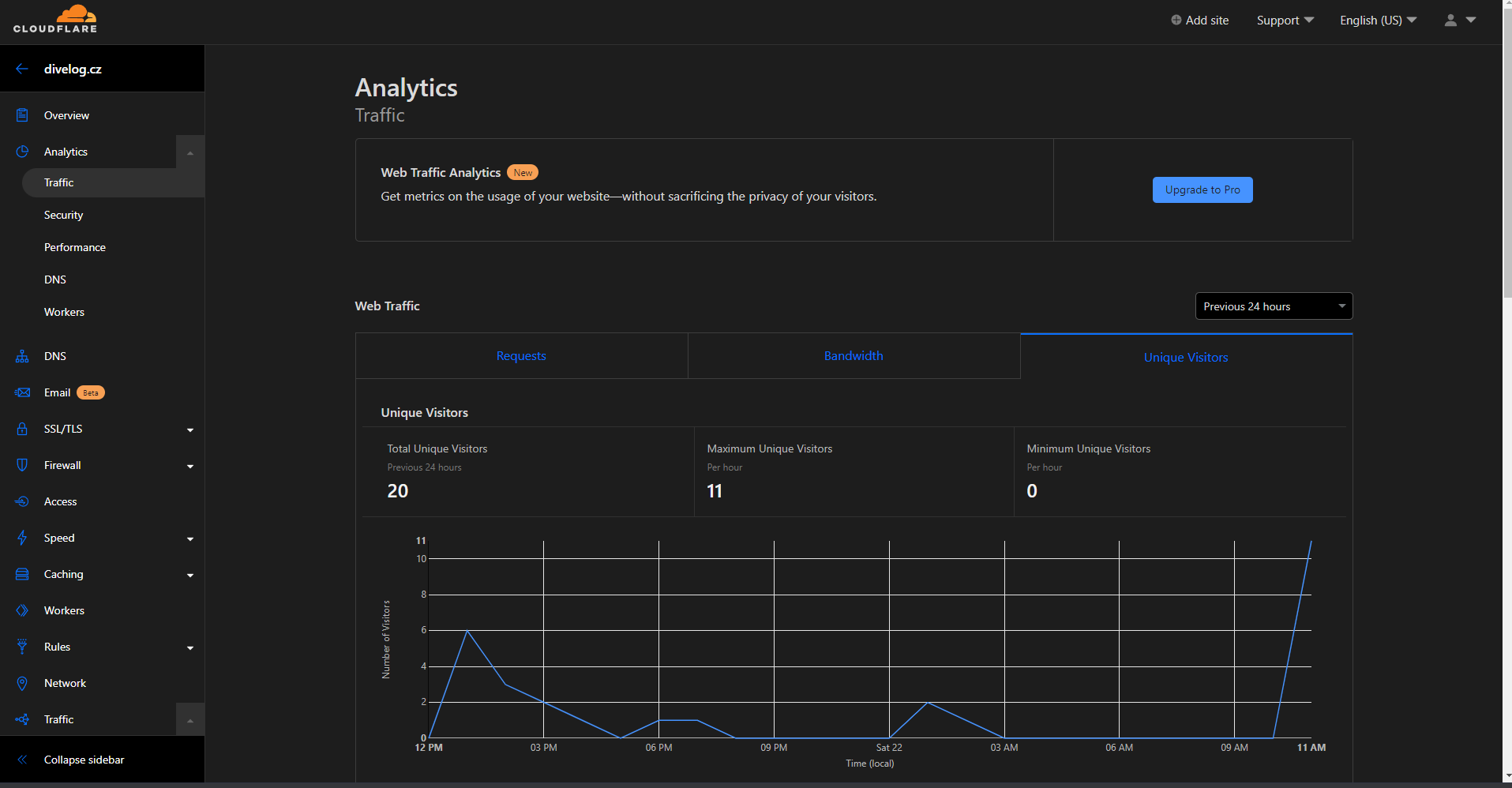
**Obr. 2.3:** Cloudflare dashboard Snímek: autor.

Tlačítko Under Attack Mode, které je na snímku zapnuté, uvádí, že je na webu ochrana DDoS ochrana zapnutá a každý HTTP request bude nejdříve prezentován s javascript captcha testem. Pokud projde dostane se požadavek vůbec k serveru, pokud ne, tak se požadavek přijde jen k serveru cloudflare.

Dále je pak i bez Under Attack Módu možné nastavovat pravidla firewallu cloudflare jako whitelist, blacklist atd.

**Obr. 2.4:** Cloudflare analytika 1 Snímek: autor.

Jak je patrné na obrázcích 2.4 a 2.5 Cloudflare nám ukáže analytiku síťového provozu a ukáže kolik požadavků za hodinu proběhlo a kolik unikátních navštívení stránky proběhlo. A velký počet požadavků, jak je vidět na obrázku 2.4 ukazuje DDoS útok.

 **Obr. 2.5:** Cloudflare analytika 2 Snímek: autor.

Cloudflare nám, jak už bylo řečeno filtruje kompletně všechen provoz a schovává IP adresu web serveru čímž dobře ochraňuje už v základu proti TCP SYN flood útokům. Samozřejmě může filtrovat i HTTP requesty, ale vyžaduje to zapnutí under attack modu nebo nastavení firewallu v dashboardu CloudFlare a pokročilá verze tohoto firewallu je už placená. Další útok byl tedy neúspěšný, jelikož se útok nedostal přes Cloudflare servery.

# Výsledky

Vybral jsem vhodné nástroje na simulaci DDoS útoku, které většinově splňovali požadavky. První vybraný LOIC splňuje všechna kritéria. Daný nástroj je velmi výkonný a má dokonce možnost připojit se na botnet. Tento nástroj jsem úspěšně pak používal ve všech virtuálních strojích. Druhý vybraný Hulk jsem používal na svých fyzických Linux serverech a

Při první simulaci útoku jsem provedl úspěšný DDoS útok a shodil kompletně web server a přetížil síťovou kartu daného web serveru. Útok jsem stupňoval po jednom počítači, aby bylo vidět jak latence a zatížení serveru narůstá s prostředky jak vyplývá z tabulky 3.1. Tato data jsou pak na obr 3.2 graficky znázorněna jako závislost počtu požadavků a počtu počítačů kdy při šesti počítačích je server shozen a útok tak úspěšný-

**Tabulka 3.1:** Tabulka ukazující, jak přidávání útočící kapacity prodlužuje zpoždění a jak postupně přispívá ke shození web serveru

Počet počítačů Latence(s) Zatížení procesoru (%) Síťová karta(Mbps) RPS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0  1 | 0.08  0.15 | 5  20 | 0.2  5 | 0  40000 |
| 2 | 0.4 | 44 | 7 | 80000 |
| 3 | 0.8 | 80 | 11 | 120 000 |
| 4  5  6 | 2.5  4.37  Service Unavaible 503 | 99  100  100 | 14  16  18 | 160 000  200 000  240 000 |

Pro tento útok byla používána učebna AL:001, tudíž tyto počítače byly použity pro útok a na každém bylo spuštěno 15 instancí LOIC s 99 vlákny a kombinací HTTP A TCP floodu. U šestého počítače stačil zaútočit a server byl shozen, web server neodpovídal a serverem nešla navázat síťová komunikace, jelikož byl přehlcen RPS je počet požadavků za vteřinu, který byly útočící nástroje schopné vyvinout a je počítán aritmetickým průměrem. Zpoždění pak odpovídá odezvě na webserveru. Zpoždění bylo počítáno s vypnutým cachováním stránky v prohlížeči a byly odstraněni maximální a minimální hodnoty, aby zpoždění bylo více relevantní. Síťová karta pak odpovídá odchozímu datovému toku v Mb za sekundu.

**Obr. 3.2:** Závislost počtu požadavků na počtu útočících počítačů Graf: autor.

Provedl jsem analýzu a výběr nejlepší ochrany pro daný případ. Po vyhledání možností jsem se uchýlil ke cloudové možnosti zdarma Cloudflare. Tuto možnost jsem řádně prozkoumal a zvolil ji jako ochranný prostředek webového serveru přístupného z internetu. Tuto ochranu jsem nakonfiguroval jako proxy server před mým webovým serverem. Zapnul jsem Under attack, který pak všechno nechal projít Javascript ověřením a tím ověřil a dosáhl ochrany proti DDoS.

Následně jsem provedl druhý útok a zjistil, že ochrana funguje a požadavky končí u Cloudflare serverů a k mému webovému serveru se ani nedostanou. Útočící programy vyžadují úpravu, aby rozpoznali, kdy DDoSují danou stránku a kdy se jejich útok zastaví na Cloudflare serverech. TCP SYN flood se zastaví rovnou u CloudFlare IP adres a není ani rozlišován jako útok na danou stránku kvůli své podstatě. U HTTP floodu nabízí CloudFlare i analytiku požadavků, originálních návštěvníku atd..

# Diskuse

Dle mého názoru jsem vybral ty nejlepší nástroje plnící účel zadání. Věřím, že kdybych měl více času mohl jsem ve svém testovacím prostředí postavit fyzické útočníky, a ne virtuální stroje. Testovací prostředí by pak bylo více realistické. Další možnost je využít cloudu a v něm udělat virtuální stroje co by po internetu útočily.

Můj webserver je hodně starý fyzický počítač, takže byl hodně limitován, a to mi usnadnilo zadání.

Ochrana se v tomto případě zdá jako nejlepší. Problém je při testovaní v lokální sítí tam musí nastoupit HW nebo SW ochrana sice to nebylo součástí zadání, ale pro testovací prostředí bych zvolil jinou.

# Závěr

V tomto projektu jsem měl šanci zjistit, jak funguje DDoS útok, kterého jsem byl už několikrát obětí a umožnilo mi to pochopit, jak funguje. Byla obtíž sehnat nejlepší ochranu, jelikož většina cloudů počítá s tím, že u nich budete i mít ten web server.

Daný projekt byl zajímavý vstup do vytváření projektů a pracování v akademickém prostředí. Moje současné zaměření aspiruje ke kybernetické bezpečnosti, ke které bych chtěl dělat další projekty. Zajímají mě různé typy kybernetických útoků a taky bych se chtěl podívat na kryptografii a prolamování hesel. Případně bych se chtěl dále podílet na bezpečnosti počítačových sítí a vytváření bezpečných počítačových síťí.

# Seznam použité literatury

[1] What is a Botnet? [online]. Kalifornie: CrowdStrike, 2022 [cit. 2022-01-23]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/botnets/

[2] *Ping flood (ICMP flood)* [online]. Kalifornie: Imperva, © 2021 Imperva [cit. 2022-01-23]. Dostupné z: https://www.imperva.com/learn/ddos/ping-icmp-flood/

[3] *DDoS Attacks* [online]. Kalifornie: Imperva, © 2021 Imperva [cit. 2022-01-23]. Dostupné z: https://www.imperva.com/learn/ddos/ddos-attacks/

[4] *Iptables* [online]. Netfilter, © 1991-2021 The Netfilter's webmasters [cit. 2022-01-23]. Dostupné z: https://www.imperva.com/learn/ddos/ddos-attacks/

[5] *Microsoft Azure DDoS protection* [online]. Microsoft, © 2022 Microsoft [cit. 2022-01-23]. Dostupné z: https://www.imperva.com/learn/ddos/ddos-attacks/

[6] *LOIC* [online]. NewEraCracker, 2019 [cit. 2022-01-23]. Dostupné z: https://github.com/NewEraCracker/LOIC

[7] *Hulk* [online]. grafov, 2021 [cit. 2022-01-23]. Dostupné z: https://github.com/grafov/hulk

[8] *Cloudflare DdoS protection* [online]. © 2022 Cloudflare, 2022 [cit. 2022-01-24]. Dostupné z: https://www.cloudflare.com/ddos/