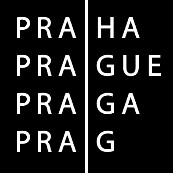
**Střední průmyslová škola elektrotechnická a gymnázium V Úžlabině 320**



**Maturitní práce z odborných předmětů**

**Název práce v českém jazyce**

**Jméno a příjmení autora/autorky práce Vyberte vaši třídu**

Vedoucí práce: **Ing. David Čepička** Studijní obor: **Informační technologie**

Rok odevzdání: **2025**

**Čestné prohlášení**

Odevzdáním této maturitní práce na téma **Útoky typu DoS** potvrzuji, že jsem ji vypracoval/a pod vedením vedoucího samostatně za použití v práci uvedených pramenů a literatury. Dále potvrzuji, že odevzdaná vytištěná verze písemné zprávy (protokolu) a plakátu se plně shoduje s odevzdanou elektronickou verzí.

V Praze dne ..................................... ...................................................

Podpis autora/autorky práce

**Anotace**

**Klíčová slova**

Kyberbezpečnost, DoS, HTTP, TCP,

**Keywords**

Cybersecurity, DoS, HTTP, TCP,

**Obsah**

[1 Úvod a cíl práce 4](#_Toc186658143)

[1.1 Cíl a zaměření práce (smazat?) 4](#_Toc186658144)

[1.2 Význam problematiky útoku typu „Denial of Service“ (smazat?) 4](#_Toc186658145)

[1.3 Struktura dokumentu (smazat?) 4](#_Toc186658146)

[2 Název kapitoly – teoretická část práce 4](#_Toc186658147)

[2.1 Princip a funkce útoků typu DoS 4](#_Toc186658148)

[2.2 Základní členění DoS útoků 5](#_Toc186658149)

[2.2.1 Distribuované útoky 5](#_Toc186658150)

[2.2.2 Volumetrické útoky 5](#_Toc186658151)

[2.2.3 Protokolové útoky 6](#_Toc186658152)

[2.2.4 Aplikační útoky 6](#_Toc186658153)

[2.3 Zaměřené útoky – HTTP flood/TCP SYN flood a další? 6](#_Toc186658154)

[2.4 Známé nástroje pro realizaci útoků 6](#_Toc186658155)

[2.4.1 LOIC 6](#_Toc186658156)

[2.4.2 Hping3 7](#_Toc186658157)

[2.4.3 HULK 7](#_Toc186658158)

[2.5 Prevence a obrana 8](#_Toc186658159)

[2.5.1 Firewally a IPD/IDS systémy 8](#_Toc186658160)

[2.5.2 Load balancery 9](#_Toc186658161)

[2.5.3 Protokoly 9](#_Toc186658162)

[3 Název kapitoly – vlastní práce 9](#_Toc186658163)

[3.1 Přehled a výběr metod útoků 9](#_Toc186658164)

[3.2 Popis virtualizovaného prostředí 9](#_Toc186658165)

[3.3 Scénář – HTTP flood 9](#_Toc186658166)

[3.4 Scénář – SYN flood 9](#_Toc186658167)

[4 Závěr 10](#_Toc186658168)

# Úvod a cíl práce

## Cíl a zaměření práce (smazat?)

## Význam problematiky útoku typu „Denial of Service“ (smazat?)

## Struktura dokumentu (smazat?)

Struktura dokumentu se dělí na úvod práce, teoretickou a praktickou část práce a její závěr. Teoretická část práce obsahuje základní řazení DoS útoků, nástroje k jejich nasazení a následnou prevenci. Praktická část se naopak zaobírá realizací dvou scénářů, jejich topologii a útoky, které byly použity.

# Název kapitoly – teoretická část práce

Než začneme s typy DoS útoků a možnou obranou proti nim, je třeba nejprve pochopit principy těchto útoků a jejich fungování. Dále si ukážeme jaké nástroje se používají pro jejich realizaci a jaké jsou možné varianty obrany proti nim.

## Princip a funkce útoků typu DoS

Útoky typu DoS (Denial of Service) jsou zaměřeny na znepřístupnění online služeb prostřednictvím přetížení cílového systému nadměrným množstvím síťového provozu. Tento nápor vede k vyčerpání zdrojů, což způsobí, že systém pak není schopen obsloužit legitimní požadavky uživatelů.

Většinou se u DoS útoků setkáváme se zaplavováním (flooding), což je odesílání velkého množství dat nebo požadavků s cílem přetížit šířku pásma (bandwidth) nebo výpočetní kapacitu cílového zařízení. Anebo také s využitím nějaké slabiny (exploit) v síťových protokolech nebo aplikacích.

Důsledkem útoků DoS jsou finanční ztráty, narušení reputace anebo ztráta důvěry zákazníků. S rostoucím počtem těchto útoků je stále naléhavější potřeba implementovat robustnější bezpečnostní strategie. (example růstů <https://www.researchgate.net/publication/378952021_Evolving_Malware_DDoS_Attacks_Decadal_Longitudinal_Study>, nebo <https://nukib.gov.cz/download/publications_en/2023_Report_on_the_State_of_Cybersecurity_in_the_Czech_Republic.pdf>)

## Základní členění DoS útoků

### Distribuované útoky

Distribuované útoky typu Denial of service, se liší od normálních DoS útoků tím, že odcházejí z více lokací najednou, a tak účinnost útoků je vyšší. DDoS útoky svým velikým počtem dat maskují útočníka a také rychlost jakou mohou cíl vyřadit z provozu je mnohonásobně větší.

Pro lepší zdůraznění si můžeme ukázat základní popis sítě DDoS útoku na figuře 1.

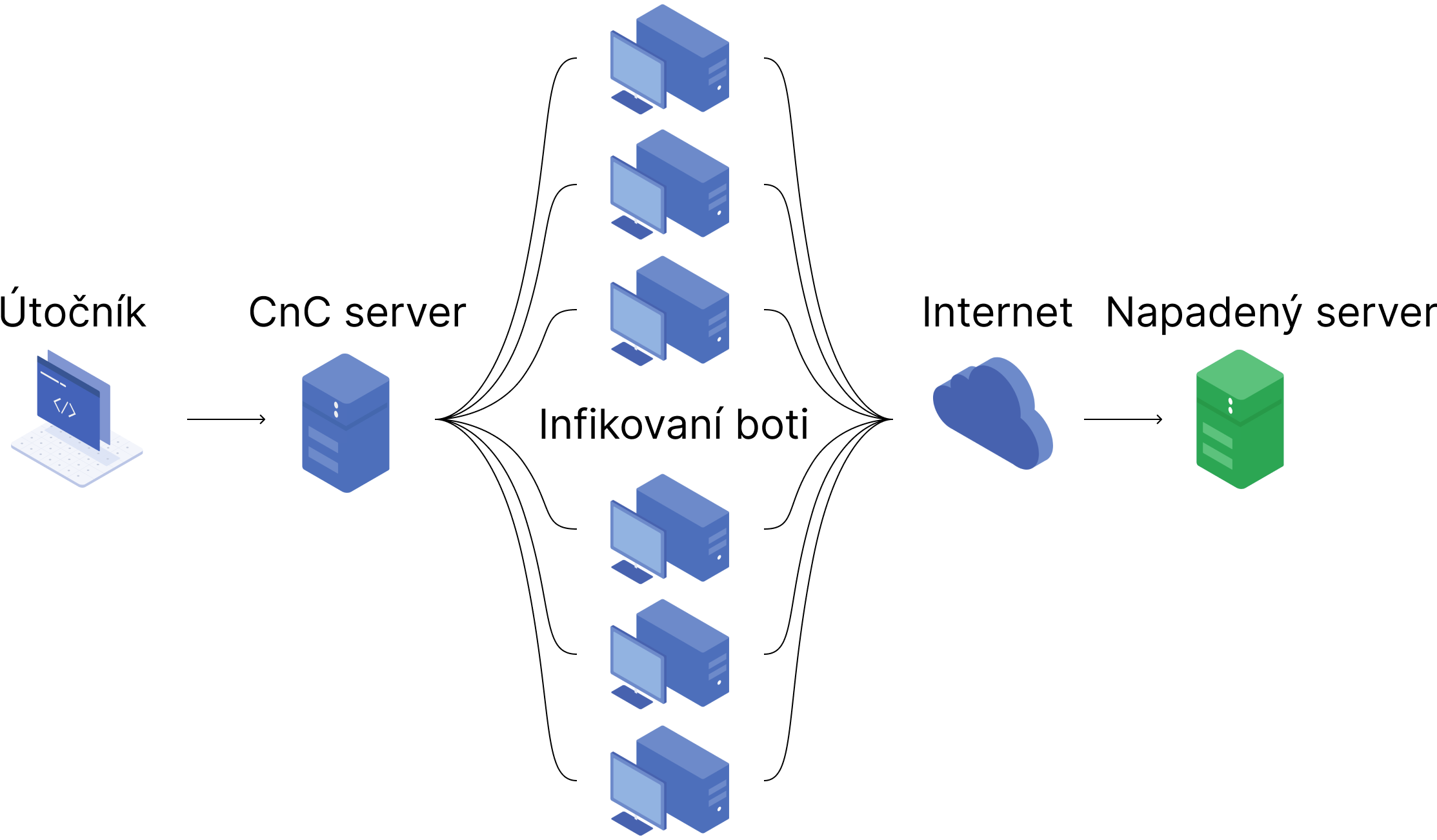


Figura Schéma základního DDoS útoku

Na figuře 1 vidíme použití strategie botnetu, což je kolekce botů (infikovaných počítačů), kteří jsou většinou pod hierarchickou kontrolou. Na konci této kontroly se většinou vyskytuje také Command-and-Control (CnC) Server, který rozesílá útočníkovi instrukce svým botům.

Dokazují to i tyto informce…/Další informace k tomuto tématu lze nalézt v dokumentu Lecture 29, Purdue University. ? <https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture29.pdf>

### Volumetrické útoky

„Volumterické útoky jsou nejčastějším typem DDoS útoků. Jejich cílem je přesycení šířky pásma cíle, což způsobí nedostupnost služby. Tyto útoky zahlcují cíl obrovským množstvím dat, které se často měří v bitech za sekundu (Bps) nebo gigabitech za sekundu (Gbps).“ (Merkebaiuly, 2024) Citace?

U volumetrických útoků je i složitější rozpoznat legitimní uživatele/požadavky od škodlivého provozu, protože velký objem dat zahlcuje nejen bezpečnostní prvky v síti, ale i prvky na napadeném zařízení, které by je mohli rozlišit.

Volumetrické útoky se pohybují primárně ve třetí a čtvrté vrstvě ISO/OSI modelu. Do těchto útoků spadá například UDP flood, SYN flood, ICMP flood nebo DNS reflection flood útoky.

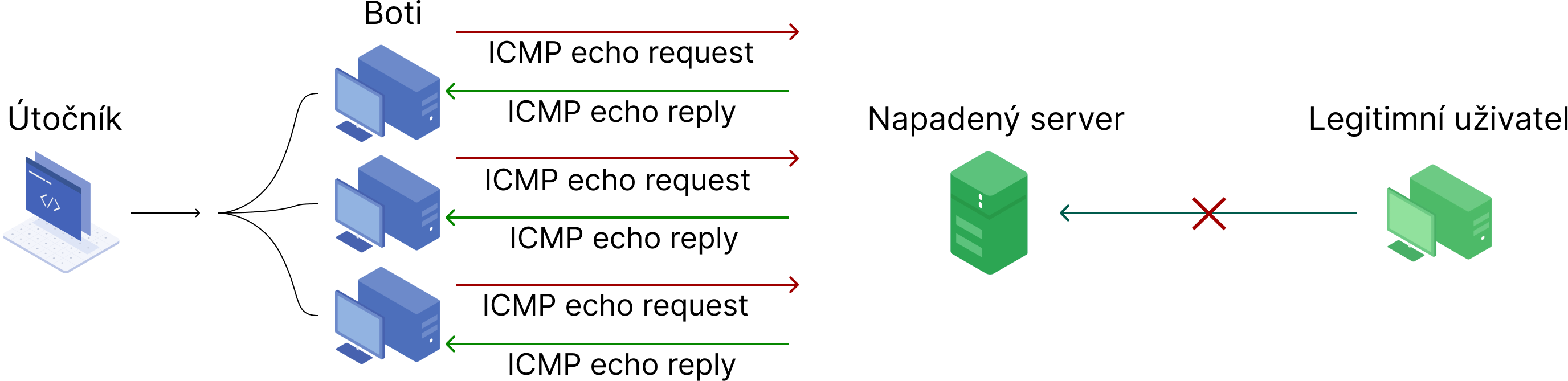


Figura Schéma ICMP flood útoku

Na levé straně figury 2, která znázorňuje ICMP flood útok, můžeme vidět útočníka řídící botnet a samotnou záplavu ICMP echo požadavky. Napadený server odpovídá a útok tak vyplýtvá jeho šířku pásma (bandwidth). Na pravé straně je zase legitimní uživatel, který není schopen komunikovat s přetíženým serverem.

### Protokolové útoky

Protokolové útoky se také pohybují ve třetí a čtvrté vrstvě ISO/OSI modelu, ale na rozdíl od volumetrických se zaměřují na využití slabin v protokolu, například v handshake procesu nebo navázání relace. (Merkebaiuly, 2024) Parafráze?

Nejčastěji se tyto útoky měří v (Pbs) paktetech za sekundu. Do těchto útoků pak spadá TCP SYN flood, Smurf útoky nebo útok ping of death.

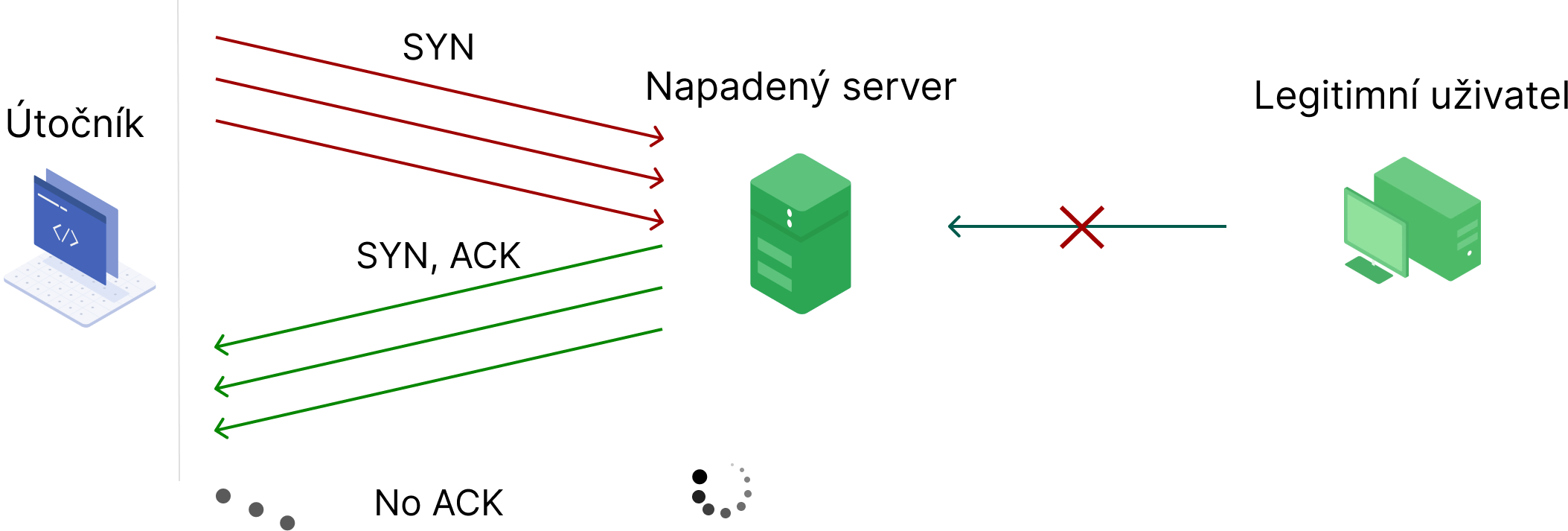
**

Figura Schéma TCP SYN flood útoku

TCP SYN flood funguje na základě operace „three-way handshake“, která se používá k navázání TCP komunikace. Normální průběh této operace probíhá tak, že klient pošle synchronizační zprávu (SYN), server odpoví také synchronizační zprávou (SYN) a ještě uznáním klientovi zprávy (ACK) a nakonec klient nazpět uzná serveru jeho zprávu (ACK).

Trik ve TCP SYN flood útoku je ten, že pokud klient neodpoví poslední zprávou (ACK), tak instance navázání komunikace bude stále otevřená. Nakonec server může dojít až do kritického bodu (viz. Figura 3) kdy bude přetížen a nebude schopen odpovídat na další TCP SYN zprávy.

### Aplikační útoky

„Aplikační útoky se zaměřují na nejvyšší vrstvu ISO/OSI modelu. Jejich cílem je vyčerpat zdroje konkrétní aplikace. Tyto útoky je často obtížnější odhalit, protože napodobují legitimní požadavky a provoz.“ (Merkebaiuly, 2024) Citace?

Nicméně, tyto útoky budou mít podobný dopad na služby, protože cílí na specifické charakteristiky aplikací, jako jsou HTTP, DNS nebo protokoly pro inicializaci relací (SIP). (Zargar, 2013)

Mezi tyto útoky patří HTTP GET/POST flood útoky, BGP hijacking nebo Slowloris útoky.

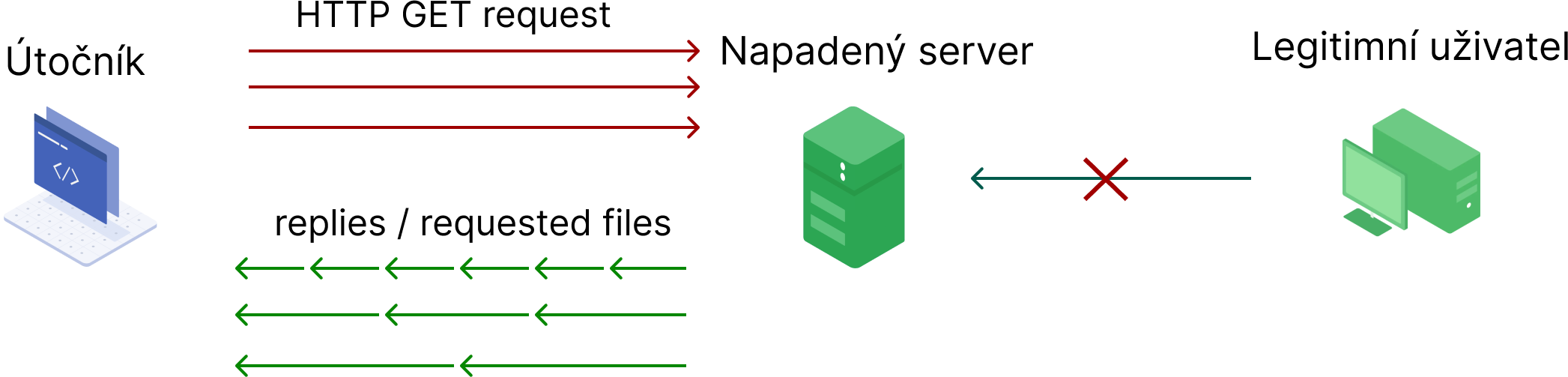


Figura Schéma HTTP GET flood útoku

Na figuře 4 je znázorněn právě HTTP GET flood útok, kde útočník posílá velké množství GET požadavků, například na stáhnutí obrázků či scriptů. Tím zapříčiní přetížení serveru, protože server musí odpovídat většinou i objemnými daty. Útočníci také kombinují různé parametry nebo i celkovou strukturu útoku pro co nevyšší poškození.

## Známé nástroje pro realizaci útoků

(Dandotiya et al. 2024)

### LOIC

Jeden z nejznámějších nástrojů k provádění DoS a DDoS útoků. Původně byl vyvinut společností Praetox Technology jako aplikace pro testování zatížení sítí, ale později se stal open-source softwarem a nyní se používá i pro škodlivé účely. LOIC je známý svou jednoduchostí a dostupností, což ho činí oblíbeným i mezi lidmi s minimálními technickými znalostmi. Proslavil se použitím skupinou Anonymous a uživateli online fór.

Nástroj umožňuje zaplavovat cílové servery s TCP, UDP nebo http pakety. Pro rozsáhlé útoky vyžadující spolupráci tisíce uživatelů je k dispozici mód „Hivemind“, kdy jeden hlavní uživatel řídí více připojených zařízení (dobrovalný botnet) prostřednictvím IRC chatovacích kanálů. Účastníci tak můžou tvrdit, že jejich zařízení byla oběťmi botnetu.

Mezi významné incidenty s využitím LOIC patří útoky Anonymous na weby Church of Scientology v roce 2008 a útoky podporovatelů WikiLeaks na weby Visa a MasterCard v roce 2010 poté, co tyto společnosti zablokovaly platby směrem k WikiLeaks. (Cloudflare, 2024)

### Hping3

Hping3 je síťový CLI nástroj, který dokáže odesílat vlastní ICMP/UDP/TCP pakety a zobrazovat odpovědi cíle podobně jako ping zobrazuje ICMP odpovědi. Podporuje fragmentaci, libovolné tělo a velikost paketů a lze jej použít k přenosu souborů prostřednictvím podporovaných protokolů.

Pomocí hping3 můžeme testovat pravidla firewallu, provádět (falšované) skenování portů, testovat výkon sítě s použitím různých protokolů, provádět objevování MTU cesty, provádět operace podobné traceroute s různými protokoly, identifikovat vzdálené operační systémy, nebo auditovat TCP/IP stacky. (Kali Hping3, 2024)

### HULK

HULK (HTTP Unbearable Load King) byl primárně navržen pro výzkumné účely a měl pomáhat penetračním testerům ověřovat efektivitu serverů. Důvod vzniku byl za vylepšení dřívějších penetračních nástrojů, jelikož většina generovala předvídatelné pakety nebo http SYN požadavky, což bránilo efektivně testovat obrany sítí.

HULK se tak liší od běžných nástrojů pro penetrační testování, skriptů nebo metod exploitace. Generuje množství unikátních požadavků v nepravidelných intervalech z jednoho hostitele. Nejenže spouští DDoS útok, ale zároveň ztěžuje obranným mechanismům sítě odhalit vzor útoku, což komplikuje filtrování provozu.

Nástroj nabízí také funkce, jako je maskování referenčních požadavků a skrytí identity útočníka. (Beschokov, 2024)

## Prevence a obrana

Obvykle, když je útok DDoS typu flooding detekován pozdě, nelze udělat nic jiného než odpojit oběť od sítě a ručně problém vyřešit. Útoky DDoS typu flooding plýtvají značným množstvím zdrojů (například výpočetním časem atd.) na cestách vedoucích k cílovému zařízení. Proto je hlavním cílem jakéhokoli mechanismu obrany proti DDoS detekovat tyto útoky co nejdříve a zastavit je co nejblíže jejich zdrojům. (Zargar, 2013)

Avšak pro dokonalou obrobnu by se muselo synchronizovaně kontrolovat na každém kroku po internetu, kvůli rozsáhlosti DDoS útoků. A díky tomu, že implementace širokého nasazení obrany se nemůže vnutit na všechny uživatele internetu <https://www.princeton.edu/~rblee/ELE572Papers/Fall04Readings/DDoSmirkovic.pdf> str47

### Firewally a IPD/IDS systémy

Firewally a systémy pro detekci a prevenci průniků (IDS/IPS) představují základní vrstvu obrany proti DDoS útokům.

Firewally umožňují blokovat podezřelý síťový provoz na základě předem nastavených pravidel, jako je filtrování podle IP adres, portů nebo protokolů, a tak zabraňují před neautorizovaným přístupem. (Netacad, 2024)

IDS/IPS systémy přidávají schopnost detekovat a automaticky reagovat na škodlivý provoz. IDS systémy analyzují síťovou komunikaci a upozorňují na možné hrozby, zatímco IPS systémy dokáží aktivně blokovat škodlivé pakety v reálném čase. Tyto technologie jsou však limitovány svou schopností zvládat vysoké objemy provozu, které větší DDoS útoky generují. (Scarfone, 2007)

### Load balancery

Load balancery představují účinnou metodu pro distribuci síťového provozu mezi více servery. Tím se snižuje riziko přetížení jednoho zařízení a umožňuje lepší odolnost vůči DDoS útokům. V případě útoku může load balancer přesměrovat provoz na méně vytížené servery nebo na speciálně navržené servery pro absorpci DDoS útoků. Moderní load balancery mohou navíc využívat metody analýzy provozu k identifikaci a filtrování škodlivého provozu. (f5, 2023)

### Protokoly

Nastavení, optimalizace a analýza síťových protokolů také hrají klíčovou roli v obraně proti DDoS útokům. Například protokol TCP může být nakonfigurován tak, aby omezoval počet současných spojení nebo minimalizoval dobu čekání na odpověď. Podobně lze využít metody jako rate limiting, které kontrolují počet požadavků z jedné IP adresy v určitém čase.

x

Také jak píše Mirkovic et al. (2004), pokud se filtruje pomocí mechanismu, který ověřuje například TCP připojení, tak podle jeho definice může odhalit polootevřené spojení odpojit je a tím zabránit jejich hromadění.

# Název kapitoly – vlastní práce

## Přehled a výběr metod útoků

## Popis virtualizovaného prostředí

## Scénář – HTTP flood

## Scénář – SYN flood

# Závěr

**V prvním odstavci závěru autor znovu uvede cíl práce** (bude shodný s cílem práce, který je uveden v úvodu).

I u závěru platí, že není zpravidla napsána na první pokus. Závěr je kapitolou, která by měla obsahovat zejména zhodnocení dosažených výsledků, hodnocení splnění cíle práce (nikoliv pouze konstatováním, že cíl práce byl/nebyl splněn; to skutečně nestačí), uvádí se také možnost uplatnění řešení v praxi apod.

V závěru by měl být stručně shrnut výsledek práce. Nejedná se však o konkrétní výsledky, které mají prostor v praktické části práce. Jedná se o výsledek shrnující v pár větách dosažení stanovených cílů. Autor při zadání práce čelí problému, který má vyřešit. Snadno se může stát, že během práce přijde na nové skutečnosti, se kterými na začátku nemusel počítat. Proto může uvést jisté odůvodnění, proč a jak v práci postupoval. Samozřejmě se nesmí autor od stanoveného cíle odchýlit výrazně. Jde o rozumnou toleranci přímo související s celou problematikou.

**Závěr představuje minimálně 1 normostranu textu (což odpovídá přibližně rozsahu tohoto obecného textu)**. Kromě výše uvedeného (zejména zhodnocení cílů práce) má obsahovat také shrnutí a zhodnocení teoretických poznatků (pokud jsou součástí práce), shrnutí a zhodnocení praktické části práce včetně přínosu pro praxi. Závěr také může obsahovat zdůvodnění nesplnění zadání práce, cíle práce apod.

Závěr se člení do odstavců. Nepatří sem nadpisy, obrázky, citáty (zvláště pak doslovné), číselné výsledky apod. Mělo by se jednat o čtivý a zajímavý text.

Osoby, které předem nebudou znát podrobnosti o práci (například stálí členové zkušební maturitní komise) by měli získat jasnou představu o práci po pročtení těchto kapitol: Úvod a cíl práce, Závěr. V kapitole Úvod a cíle práce čtenář načerpá obecné poznatky o dané práci. Po pročtení kapitoly Závěr by měl mít jasnou představu o tom, čím se měla práce zabývat, jak se podařilo cíle práce dosáhnout, jaký je přínos pro praxi apod.

**Seznam použitých zdrojů**

NOVÁK, Ondřej. *DoS útoky a jejich analýza*. Bakalářská práce. Slezská univerzita v Opavě, Filozoficko-přírodovědecká fakulta v Opavě. [online] 2023 [cit. 2024-12-28]. Dostupné z: https://is.slu.cz/th/uhwyf/.

Merkebaiuly, Medet. Overview of Distributed Denial of Service (DDoS) attack types and mitigation methods. InterConf. 10.51582/interconf.19-20.03.2024.048. 2024 [cit. 2024-12-14]. Dostupné také z: <https://www.researchgate.net/publication/379284307_Overview_of_Distributed_Denial_of_Service_DDoS_attack_types_and_mitigation_methods>.

Zargar, ST & Joshi, J & Tipper, D, A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks. IEEE Communications Surveys and Tutorials, 15 (4). 2046 – 2069. 2013 [cit. 2024-12-31]. Dostupné také z: <https://d-scholarship.pitt.edu/19225/1/FinalVersion.pdf>

Obaid, Hadeel. Denial of Service Attacks: Tools and Categories. International Journal of Engineering Research and. V9. 10.17577/IJERTV9IS030289. (2020). Dostupné také z: <https://www.researchgate.net/publication/341875337_Denial_of_Service_Attacks_Tools_and_Categories>.

Dandotiya, Abhinandan & Sharma, Palash & gole, Bharti & Dubey, Shruti & Dandotiya, Nidhi. An Empirical Analysis of DDoS Attack Detection and Mitigation Techniques: A Comparative Review of Tools and Methods. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 10. 1099-1108. 10.32628/CSEIT2410462. (2024). ISSN: 2456-3307 Dostupné také z: <https://www.researchgate.net/publication/386447490_An_Empirical_Analysis_of_DDoS_Attack_Detection_and_Mitigation_Techniques_A_Comparative_Review_of_Tools_and_Methods>.

What is the low orbit ion cannon (LOIC)? Cloudflare. [online] 2024 [cit. 2024-12-27]. Dostupné také z: <https://www.cloudflare.com/en-gb/learning/ddos/ddos-attack-tools/low-orbit-ion-cannon-loic/>

Hping3 Kali. [online] 2024 [cit. 2024-12-27]. Dostupné také z: <https://www.kali.org/tools/hping3/>

Mukhadin Beschokov, What is HULK - HTTP Unbearable Load King?, wallarm [online] 2024 [cit. 2024-12-28]. Dostupné z: <https://www.wallarm.com/what/what-is-hulk-http-unbearable-load-king>

Netacad, CCNA: Enterprise Networking, Security, and Automation. [online] [Paywall] 2024 [cit. 2024-12-31]. Dostupné také z: <https://www.netacad.com/trainings/ccna-enterprise-networking-security-automation?courseLang=en-US>

Scarfone, K., & Mell, P. *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST Special Publication 800-94. National Institute of Standards and Technology. [online] (2007) [cit. 2024-12-31]. Dostupné také z: <https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50951>

F5, What Is a Load Balancer?. [online] 2023 [cit. 2024-12-31]. Dostupné také z: <https://www.f5.com/glossary/load-balancer>

Mirkovic, J., & Reiher, P. *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms*. [online] (2004) [cit. 2024-12-31]. Dostupné také z: <https://www.princeton.edu/~rblee/ELE572Papers/Fall04Readings/DDoSmirkovic.pdf>

**Seznam příloh**

**Příloha č. 1: Název přílohy**

Samotná příloha. Nejčastěji se do příloh dávají např. návrhy plošných spojů, další obrazová dokumentace, ukázky kódu ve formě printscreenů apod. Pokud přílohy v práci nebudou, tuto kapitolu smažte.

**Příloha č. 2: Název přílohy**

**Seznam obrázků**

Seznamy obrázků uvedených ve vlastní práci. Autor práce zde pracuje s titulky a s automaticky generovaným seznamem otitulkovaných objektů. Pokud tyto seznamy v práci nebudou, tyto kapitoly smažte.

<https://www.svgrepo.com/collection/servers-isometric-icons/>

[Figura 1 Schéma základního DDoS útoku 5](#_Toc186749581)

[Figura 2 Schéma ICMP flood útoku 6](#_Toc186749582)

[Figura 3 Schéma TCP SYN flood útoku 7](#_Toc186749583)

[Figura 4 Schéma HTTP GET flood útoku 8](#_Toc186749584)

**Seznam tabulek** Viz seznam obrázků.

**Seznam grafů atd.**

Viz seznam obrázků.