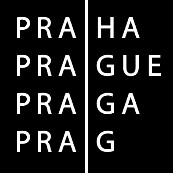
**Střední průmyslová škola elektrotechnická a gymnázium V Úžlabině 320**



**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**

**Keywords**

# Obsah

[1 Obsah 2](#_Toc186325830)

[2 Úvod a cíl práce 4](#_Toc186325831)

[2.1 Cíl a zaměření práce 4](#_Toc186325832)

[2.2 Význam problematiky útoku typu „Denial of Service“ 4](#_Toc186325833)

[2.3 Struktura dokumentu 4](#_Toc186325834)

[3 Název kapitoly – teoretická část práce 4](#_Toc186325835)

[3.1 Princip a funkce útoků typu DoS 4](#_Toc186325836)

[3.2 Základní členění DoS útoků 4](#_Toc186325837)

[3.2.1 Distribuované 4](#_Toc186325838)

[3.2.2 Volumetrické 5](#_Toc186325839)

[3.2.3 Protokolové 5](#_Toc186325840)

[3.2.4 Aplikační 5](#_Toc186325841)

[3.3 Zaměřené útoky – HTTP flood/TCP SYN flood 6](#_Toc186325842)

[3.4 Známé nástroje pro realizaci útoků 6](#_Toc186325843)

[3.4.1 LOIC/HOIC 6](#_Toc186325844)

[3.4.2 Scapy 6](#_Toc186325845)

[3.4.3 Slowloris 6](#_Toc186325846)

[3.5 Prevence a obrana 6](#_Toc186325847)

[3.5.1 Firewally a IPD/IDS systémy 6](#_Toc186325848)

[3.5.2 Load balancery 6](#_Toc186325849)

[3.5.3 Protokoly 6](#_Toc186325850)

[4 Název kapitoly – vlastní práce 7](#_Toc186325851)

[4.1 Přehled a výběr metod útoků 7](#_Toc186325852)

[4.2 Popis virtualizovaného prostředí 7](#_Toc186325853)

[4.3 Scénář – HTTP flood 7](#_Toc186325854)

[4.4 Scénář – SYN flood 7](#_Toc186325855)

[5 Závěr 8](#_Toc186325856)

[6 Seznam použitých zdrojů 9](#_Toc186325857)

[7 Seznam příloh 10](#_Toc186325858)

# Úvod a cíl práce

## Cíl a zaměření práce

## Význam problematiky útoku typu „Denial of Service“

## Struktura dokumentu

Struktura dokumentu se dělí na osnovu, úvod práce, teoretickou a praktickou část práce a její závěr. Teoretická část práce obsahuje základní řazení DoS útoků, nástroje k jejich nasazení a následná prevence. 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 možné obraně proti nim, si první musíme…

## Princip a funkce útoků typu DoS

Než začneme s typy DoS útoků a možné obraně proti nim, si první musíme…

## Základní členění DoS útoků

### Distribuované

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

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

Could but ? <https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture29.pdf>

### Volumetrické

„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 pak složitější rozpoznat legitimní uživatele/požadavky od škodlivého provozu, protože velký objem dat zahlcuje i bezpečnostní prvky v síti tak i na cíli, 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.

### Protokolové

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.

### Aplikační

„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?

x

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

## Zaměřené útoky – HTTP flood/TCP SYN flood

## Známé nástroje pro realizaci útoků

Tato podkapitola se zaměřuje na nejčastěji používané nástroje pro dříve zmíněné útoky.

(Dandotiya et al. 2024)

### LOIC/HOIC

a

### Scapy

A

### Slowloris

a

## Prevence a obrana

a

### Firewally a IPD/IDS systémy

a

### Load balancery

a

### Protokoly

a

# 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

Seznam použité literatury a zdrojů sestavený v souladu s ČSN ISO 690. Pro účely maturitní práce postačí výchozí nástroj textového procesoru MS Word. Doporučujeme styl ISO 690 – první prvek a datum. Dále je možné využít dalších nástrojů (např. citace.com, katalog Národní knihovny v Praze, citační software – např. aplikace Zotero). **Wikipedia není považována za relevantní zdroj při práci s odborným textem.**

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>

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>

# 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.

**Seznam tabulek** Viz seznam obrázků.

**Seznam grafů atd.**

Viz seznam obrázků.