**UNIVERZITA OBRANY**

**Fakulta vojenských technologií**

Akademický rok: 2024/2025

Studijní program: Kybernetická bezpečnost

Forma studia: Prezenční

Studijní obor/modul/specializace: Kybernetická bezpečnost

Katedra: Katedra informatiky a kybernetických operací

Garant studijního programu: plk. gšt. doc. Ing. Petr Františ, Ph.D.

**ZADÁNÍ DIPLOMOVÉ PRÁCE**

Hodnost, jméno a příjmení studenta: rtn. Tomáš Hujňák

Téma (česky): Nástroj pro testování a zvyšování odolnosti organizací proti phishingu

Téma (anglicky): Tool for testing and increasing phishing resilience in organizations

|  |  |
| --- | --- |
| Vedoucí závěrečné práce: | mjr. Ing. Tomáš Šlajs |
| Konzultanti: | npor. Ing. Tomáš Ráčil |
| Datum zadání: | 1.6. 2024 |
| Termín odevzdání: | 31. 5. 2025 |
| Podpis studenta: | ……………………………………………………….. |

**I. Upřesnění podmínek zpracování závěrečné práce**

V souvislosti se zpracováním závěrečné práce NEBUDE studentem nakládáno s utajovanými informacemi.

V souvislosti se zpracováním závěrečné práce NEBUDE studentem nakládáno s informacemi pro služební potřebu.

Závěrečná práce NEBUDE obsahovat utajené informace.

Závěrečná práce NEBUDE obsahovat informace pro služební potřebu.

Při zpracování závěrečné práce NEBUDOU zpracovávány osobní údaje.

**II. Úkoly a pokyny pro zpracování závěrečné práce**

Práce bude zpracována v českém jazyce. Hlavním úkolem práce je navrhnout a implementovat nástroj, který bude simulovat phishingové kampaně a vyhodnocovat je. Tento nástroj by měl být schopen poskytovat zpětnou vazbu a vzdělávat uživatele na základě jejich chování. Součástí práce bude také implementace mechanismů pro monitorování a analýzu chování uživatelů, což umožní dynamicky přizpůsobovat obtížnost a sofistikovanost phishingových útoků. Cílem práce je vytvořit nástroj, který umožní vyhodnotit odolnost organizace vůči phishingu a identifikovat slabá místa v rámci kybernetické bezpečnosti.

Dílčí úkoly: Analýza stávajících phishingových technik a nástrojů.

Návrh architektury a funkcionalit nástroje.

Výběr vhodných technologií a programovacích jazyků.

Vytvoření prototypu nástroje a jeho testování.

**III. Doporučená literatura**

[1] HADNAGY, Christopher. Social Engineering: The Science of Human Hacking. 1st ed. Indianapolis: Wiley Publishing, 2010. ISBN 978-0-470-63953-5.

[2] MITNICK, Kevin D., William L. SIMON a Steve WOZNIAK. The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers. 1st ed. Indianapolis: Wiley Publishing, 2005. ISBN 0-7645-6959-7.

[3] TUNSTALL, Lewis, Leandro VON WERRA a Thomas WOLF. Natural Language Processing with Transformers. Sebastopol: O'Reilly Media, 2022. ISBN 978-1-492-04113-8.

[4] BENDER, Emily M. a Alexander KOLLER. *Climbing towards NLU: On Meaning, Form, and Understanding in the Age of Data*. In *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*. Online: Association for Computational Linguistics, 2020, s. 5185-5198. ISBN 978-1-950737-66-9.

[5] POLČÁK, Radim. Ochrana osobních údajů podle GDPR v informačních systémech. Brno: Computer Press, 2018. ISBN 978-80-251-4641-1.

V Brně dne ……………………………… ………………………………………………………….……

Vedoucí závěrečné práce

V Brně dne ……………………………… ………………………………………………………….……

Vedoucí odborné katedry

V Brně dne ……………………………… ………………………………………………………….……

Garant studijního programu