FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název:	Automatické rozpoznávání síťových zařízení a jejich závislostí
Student:	Josef Koumar
Vedoucí:	Ing. Tomáš Čejka, Ph.D.
Studijní program:	Informatika
Studijní obor:	Bezpečnost a informační technologie
Katedra:	Katedra počítačových systémů
Platnost zadání:	Do konce letního semestru 2020/21

Pokyny pro vypracování

Seznamte se s problematikou monitorování síťového provozu pomocí tzv. síťových toků (IP Flows).
Seznamte se s open source systémem NEMEA [1,2] pro automatickou analýzu provozu a detekci bezpečnostních událostí.
Navrhněte NEMEA modul pro analýzu rozšířených obousměrných síťových toků (biflow) pro rozpoznání serverů a jejich služeb, případně i dalších informací o zařízeních.
Implementujte navržený NEMEA modul, který bude detekovat servery a udržovat seznam jejich klientů. Výstup modulu, tzn. graf závislostí klientů na službách serverů, zkuste vizualizovat pomocí existujících nástrojů.
Vyvinutý modul otestujte pomocí reálného síťového provozu (dodá vedoucí práce), zaměřte se na vyhodnocení propustnosti modulu a jeho náročnosti na výpočetní a paměťové zdroje.

Seznam odborné literatury

[1] T. Cejka, et al.: "NEMEA: A Framework for Network Traffic Analysis," in *12th International Conference on Network and Service Management (CNSM 2016)*, Montreal, Canada, 2016.
[2] https://nemea.liberouter.org

prof. Ing. Pavel Tvrdík, CSc.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 11. prosince 2019