

## HODNOCENÍ OPONENTA DIPLOMOVÉ PRÁCE

|                  |                                              |
|------------------|----------------------------------------------|
| Autor práce      | Matěj Fusek                                  |
| Studijní program | Bezpečnost společnosti                       |
| Specializace     | Rizikové inženýrství                         |
| Forma studia     | kombinovaná                                  |
| Akademický rok   | 2024/2025                                    |
| Téma práce       | Flowmon jako aktivní ochrana počítačové sítě |
| Autor posudku    | Jakub Trojan                                 |

|   | Kritéria hodnocení                                                                      | Váha        | Hodnocení       |
|---|-----------------------------------------------------------------------------------------|-------------|-----------------|
| 1 | Formulace cílů práce a použité metody                                                   | 0,07        | D               |
| 2 | Úroveň teoretické části práce                                                           | 0,15        | E               |
| 3 | Úroveň analyticko-empirické části práce                                                 | 0,25        | E               |
| 4 | Úroveň aplikační části práce                                                            | 0,10        | D               |
| 5 | Výstavba textu a jeho logická provázanost, kvalitativní a kvantitativní parametry práce | 0,08        | D               |
| 6 | Splnění cílů práce a relevance závěrů                                                   | 0,15        | C               |
| 7 | Odborný přínos práce a její praktické využití                                           | 0,10        | E               |
| 8 | Jazyková úroveň práce                                                                   | 0,05        | D               |
| 9 | Formální náležitosti práce (včetně citací a užití šablony)                              | 0,05        | E               |
|   | <b>Návrh hodnocení dle váženého průměru</b>                                             | <b>1,00</b> | <b>E (2,70)</b> |

Diplomová práce M. Fuska zaměřená na Flowmon je reakcí na relativně známé a poměrně zaběhlé řešení pro monitorování a analýzu síťového provozu v oblasti detekce provozních, výkonnostních a bezpečnostních problémů. Teoretická část práce je velmi popisná s absencí analytického myšlení. Výběr zdrojů je poměrně úzký a často se opírá o firemní dokumentaci výrobce Flowmonu či jiných webových stránek (a to vč. problematických – např. Kaspersky Lab, kterou autor ani neuvedl v seznamu použité literatury). Chybí zapojení nezávislých vědeckých článků, případových studií z praxe nebo srovnávacích recenzí. V práci není patrné, že by autor sledoval aktuální vývoj v oblasti síťové bezpečnosti na mezinárodní úrovni. Některé pasáže jsou téměř doslovně převzaté z dokumentace nebo webových stránek bez dostatečné míry parafráze. Citace sice formálně nechybí, ale způsob práce s literaturou je pasivní a místy na hraně akceptovatelnosti pro diplomovou práci. Chybí jasné oddělení vlastních myšlenek od převzatých informací. Nestandardní je také uvádění zdroje u tabulek a obrázků jako „vlastní“ bez indikace původu dat/obsahu.

Praktická část je z mého pohledu také komplikovaná. Již autorem zmíněna jediná metoda – „analýza“ není nijak dále rozvíjena. O jaký typ analýzy se jedná? Kvalitativní či kvantitativní metody? Na úrovni diplomové práce je toto neakceptovatelné. Praktická část práce dále popisuje nasazení Flowmonu v konkrétní síti, ale je de facto založena jen na prostém popisu

funkcionality nástroje a návrzích vylepšení bez jednoznačné opory v robustním experimentu či na základě rešerše literatury či testování user experience. Autor v provozu testuje pouze základní scénáře, chybí simulace složitějších útoků, testování robustnosti systému nebo porovnání s jinými nástroji v reálném provozu. Výsledky jsou prezentovány bez hlubší interpretace. Autor nekriticky přijímá možnosti Flowmonu, nevěnuje se jeho slabinám (např. detekce v šifrovaném provozu, nároky na správu, riziko falešných poplachů). Chybí diskuse o tom, jak by se systém choval v prostředí s vyšší zátěží nebo v případě cíleného útoku. Inspirací mohla být série závěrečných prací zpracovaných na podobné téma na FI MU (již někdy před 10 lety). V diplomové práci absentuje i standardní kapitola „Diskuse“, která by výsledky dávala do kontextu s již dříve vydanými studiemi.

Styl psaní práce je místy neobratný, autor často používá dlouhé, složité věty, které ztěžují porozumění. Odborná terminologie je používána ne vždy konzistentně, některé pojmy nejsou vůbec vysvětleny. Práce obsahuje i pravopisné a stylistické chyby.

I přes výše uvedenou kritiku považuji diplomovou práci za obhajitelnou a rámcově splňující požadavky kladené na tento typ závěrečných prací na FLKŘ UTB.

#### **Otázky k obhajobě:**

1. Jaká jsou hlavní rizika a omezení nasazení Flowmonu v prostředí s vysokým podílem šifrovaného provozu a jak byste je řešil?
2. Jak byste řešil situaci, kdy by Flowmon generoval vysoké množství falešných poplachů – jaký by to mělo dopad na provoz a jak byste tento problém minimalizoval?

**V Uherském Hradišti dne 13.05.2025**

**Podpis:**

Hodnocení odpovídá následující stupnici:

A = 1,00-1,24    B = 1,25-1,50    C = 1,51-2,00    D = 2,01-2,50    E = 2,51-3,00    F = 3,01-...