Univerzita Hradec Králové
Fakulta informatiky a managementu

# POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

**Jméno studenta:** Bc. Ondřej Líbal

**Název práce:** Principy honeypotů a jejich využití pro zabezpečení síťového provozu

**Autor posudku:** Ing. Tomáš Svoboda, Ph.D.

**Cíl práce:** Cílem práce je podrobně představit principy fungování honeypotů, jejich rozdělení a využití pro zabezpečení síťového provozu.

| **Povinná kritéria hodnocení práce** | **Stupeň hodnocení** (známka) | | | | | |
|---|---|---|---|---|---|---|
| | **A** | **B** | **C** | **D** | **E** | **F** |
| Práce svým zaměřením odpovídá studovanému oboru | ☒ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Vymezení cíle a jeho naplnění | ☐ | ☐ | ☐ | ☒ | ☐ | ☐ |
| Zpracování teoretických aspektů tématu | ☐ | ☐ | ☒ | ☐ | ☐ | ☐ |
| Zpracování praktických aspektů tématu | ☐ | ☐ | ☒ | ☐ | ☐ | ☐ |
| Adekvátnost použitých metod, způsob jejich použití | ☐ | ☐ | ☐ | ☒ | ☐ | ☐ |
| Hloubka a správnost provedené analýzy | ☐ | ☐ | ☐ | ☒ | ☐ | ☐ |
| Práce s literaturou | ☐ | ☐ | ☒ | ☐ | ☐ | ☐ |
| Logická stavba a členění práce | ☐ | ☐ | ☐ | ☒ | ☐ | ☐ |
| Jazyková a terminologická úroveň | ☐ | ☐ | ☐ | ☒ | ☐ | ☐ |
| Formální úprava a náležitosti práce | ☐ | ☐ | ☒ | ☐ | ☐ | ☐ |
| Vlastní přínos studenta | ☐ | ☐ | ☒ | ☐ | ☐ | ☐ |
| Využitelnost výsledků práce v teorii (v praxi) | ☐ | ☐ | ☒ | ☐ | ☐ | ☐ |

**Vyjádření k výsledku anti-plagiátorské kontroly**

Antiplagiátorská kontrola eVSKP identifikovala celkovou podobnost: 0 %.

**Dílčí připomínky a náměty:**

Oponent práce má následující připomínky a náměty k předložené práci:

1. Cíle práce na str. 2 jsou velice nevhodně formulovány. Jsou využity formulace typu: „*Práce by měla ukázat…, práce by měla být rozdělena do dvou kapitol…*“. Práce fakticky není rozdělena pouze do 2 kapitol. Nelze tedy jednoznačně říci, že práce splnila definované cíle.
2. Z předložené práce není v anotaci, úvodu ani cílů práce v kapitole 2 zřejmé, proč autor popisuje v dalších kapitolách referenční model ISO/OSI, zabezpečení síťového provozu, IDS a IPS systémy. Autor v textu nereflektoval vazbu na zadání, tedy „*podrobně představit principy fungování honeypotů, jejich rozdělení a využití pro zabezpečení síťového provozu*“.
3. Autor v předložené práci používá zavádějící a neověřená tvrzení, např. str. 11 (*Tento pojem není až zas tak starý, takže přesný pojem, co obnáší je těžko specifikovatelné.*), str. 6. *(Je důležité pro mnoho firem, aby byli v bezpečí proti různým útokům, ať už se jedná o útoky na data společnosti nebo útoky na zdroje, jako jsou různá síťová zařízení.*), str. 21 (*Přesná definice honypotu je jasně stanovena, ale přesto se trochu od sebe liší jejich formou*), str. 23 (*Zde si zkusíme obecně říci v čem spočívá výhoda honeypotů a na co naopak honeypoty trpí,*

*co je jejich slabinou*) , str. 27 (*Honeyfarmy a honeynety jsou v podstatě to samé, akorát honeyfarmy bývají více centralizované*).

4. Práce obsahuje kapitoly textu, u kterých není uveden zdroj, např. kapitola 7.2.

**Celkové posouzení práce a zdůvodnění výsledné známky:**

Předložená práce je rozdělena do 14ti kapitol včetně úvodu a závěru. V kapitolách 1 až 8 autor z teoretického úhlu pohledu popisuje principy počítačových sítí a metody, resp. nástroje využívané pro zabezpečení síťového provozu a ochranu vnějšího perimetru se zaměřením na technologie VPN, DLP, IDS, IPS a AMP.
Představení hlavní technologie, tedy honeypotů, se autor věnuje z teoretického hlediska v kapitole 7. Kladně lze hodnotit strukturu kapitoly 7, kde autor systematicky a přehledně popisuje historii, výhody a nevýhody těchto řešení a zároveň detailně představuje jednotlivé typy honeypotů.

V kapitole 8 se autor věnuje právním problémům, které souvisí s nasazením technologie honeypotů. Celý text kapitoly bohužel působí velice nevyváženě a reflektuje v obecné rovině pouze oblast ochrany osobních údajů. Autor měl v této části z mého pohledu provést detailnější analýzu legislativních a normativních požadavků, které souvisí s nasazením honeypotů a výsledky analýzy prezentovat v této kapitole.

V následujících kapitolách 9, 10 a 11 autor přechází k praktické části práce. Nejprve jsou popsány technologie honeypotů, následuje stanovení hypotéz, podrobný přehled konfigurace zvolených honeypot řešení a shrnutí získaných výsledků. Zde je patrná erudice autora v oblasti instalace uvedených řešení. Bohužel prezentace získaných výsledků jednotlivých řešení působí velice nesourodě, vzhledem k jejich reflektování napříč 11. kapitolou. Pro přehlednost a možnosti porovnání získaných výsledků by bylo vhodné tyto spojit do separátní kapitoly.

V kapitole 13 autor prezentuje závěry a doporučení. Závěry a doporučení se týkají pouze praktické části, nikoli předložené práce jako celku.

Závěrem lze obecně konstatovat, že předložená práce naplnila stanovené cíle, které lze bohužel v práci vysledovat až po důkladné analýze textu, a současně práce odpovídá požadavků kladeným na diplomovou práci.

**Otázky k obhajobě:**

V kapitole 7.4 uvádíte, že „*Honeyfarmy a honeynety jsou v podstatě to samé, akorát honeyfarmy bývají více centralizované*“. Vysvětlete detailně rozdíly mezi honeyfarmami a honeynety.
Jakými legislativní předpisy ČR je z vašeho pohledu relevantní se zabývat při nasazení honeypotů do firemního prostředí.

**Práci doporučuji k obhajobě.**

**Navržená výsledná známka: D**

**V** Hradci Králové**, dne 28. prosince 2020**

_____

**podpis**