Posudek oponenta bakalářské práce

Student: Pisk Jiří
Téma: Detekce bezpečnostních incidentů v počítačové síti nemocnice (id 25055)
Oponent: Ryšavý Ondřej, doc. Ing., Ph.D., UIFS FIT VUT

1. Náročnost zadání **obtížnější zadání**

Projekt se zabývá nasazením honeypotů v komplexní síťové infrastruktuře. Z tohoto důvodu existují další omezení, které je nutné dodržovat. Bezpečnostní politika a organizační pravidla navíc kladou další požadavky na výsledné řešení.

2. Splnění požadavků zadání **zadání splněno**

3. Rozsah technické zprávy **je v obvyklém rozmezí**

4. Prezentační úroveň předložené práce **80 b. (B)**

Práce je vhodně strukturována. Kapitola 2 poskytuje zajímavý přehled existujících honeypotů, ačkoliv jejich charakteristika v 2.1 je slabší. V kapitole 3 jsou informace specifické pro cílové prostředí. Obrázek sítě je dostatečný pro představení nejdůležitějších částí, ale neumožňuje pochopení topologie této infrastruktury (což je možná záměr, neboť konkrétní informace o existující infrastruktuře nebývají veřejně dostupné). Obrázek 3.2 nemá bez dalšího popisu (kdy bylo měřeno, jak dlouho) větší informační hodnotu. Nejasný je důvod uvedení nejaktivnějších sítí. V kapitole 4 je představeno nasazení a testování honeypotů. Zde se v podstatě ověřilo, že tyto systémy dělají to co se od nich očekává.

5. Formální úprava technické zprávy **70 b. (C)**

V práci lze najít pravopisné, gramatické a stylistické prohřešky. Naštěstí je jejich výskyt řídký a výrazně neovlivňují celkovou srozumitelnost textu.

6. Práce s literaturou **80 b. (B)**

Student použil několik zdrojů souvisejících s používáním honeypotů. Ty jsou pro daný problém relevantní. Zbývající zdroje se týkají použitých technologií. Jelikož se jedná o BP, výběr je dostatečný.

7. Realizační výstup **65 b. (D)**

Realizačním výstupem je několik konfiguračních souborů pro nasazení honeypotů formou kontajnerů. Jediným spustitelným kódem je skript pro flask aplikaci zajišťující vytváření incidentů na GitLab.

8. Využitelnost výsledků

Práce přináší praktické informace, které lze využít při nasazení honeypotů. Pro skutečně použitelné nasazení je nutné vyřešit problém se zpracováním výstupů, které bude operátorům poskytovat užitečné informace.

9. Otázky k obhajobě

- Díval jste se na nějaké existující strategie "maskování" honeypotů? Je možné některé z nich využít?
- Proč není možné použít existující SIEM pro zpracování výstupů z honeypotů?

10. Souhrnné hodnocení **75 b. dobře (C)**

Student se zabýval nasazením honeypotů do existující infrastruktury, umožňující sběr bezpečnostních incidentů s cílem posílení kybernetické bezpečnosti komplexního kritického systému. V předložené práci lze kladně hodnotit představený přehled honeypotů a analýzu cílového prostředí, včetně bezpečnostních politik. Zpracování výstup z honeypotů, jejich přizpůsobení reálnému prostředí a automatizované nasazení je hlavním realizačním výstupem předložené práce.

Celkově se jedná o zdařilou a po nezbytných úpravách v praxi použitelnou práci.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 1. června 2022

Ryšavý Ondřej, doc. Ing., Ph.D.
oponent