

Posudek oponenta diplomové práce

Student: Procházka Jiří, Bc.
Téma: Sběr indikátorů kompromitace z operačních systémů (id 22188)
Oponent: Ryšavý Ondřej, doc. Ing., Ph.D., UIFS FIT VUT

- 1. Náročnost zadání** průměrně obtížné zadání
Jedná se o vytvoření nástroje, který je schopen identifikovat zda se na cílovém operačním systému objevují příznaky možné kompromitace.
- 2. Splnění požadavků zadání** zadání splněno
Zadání bylo splněno. Místo testování v produkční síti bylo použito síťové prostředí dostupné v rámci kybernetického cvičení, jenž poskytuje z pohledu testování vhodnou alternativu.
- 3. Rozsah technické zprávy** je v obvyklém rozmezí
- 4. Prezentační úroveň předložené práce** 85 b. (B)
Práce je srozumitelná a text obsahuje nezbytné informace. Mimo popisu principů realizace samotného nástroje, je v práci uveden také přehled existujících systémů vhodných pro detekci loC a formátů pro výměnu informací o incidentech. Přestože žádných z uvedených systémů ani formátů nakonec nebyl v práci použit, obojí přináší cenné informace v řešené oblasti. V práci je také uvedeno vyhodnocení systému v testovacím prostředí a v prostředí kybernetického cvičení, včetně uvedení výkonnostních parametrů.
- 5. Formální úprava technické zprávy** 75 b. (C)
Práce je srozumitelná a psána na dobré jazykové úrovni. V textu lze nalézt drobné jazykové nedostatky, například nesprávný tvar slovesa, výrazy neobvyklé v technickém textu a překlepy.
- 6. Práce s literaturou** 75 b. (C)
Z použité literatury má většina charakter internetových zdrojů. Ty jsou tvořeny specifikacemi nebo blogy. Přestože jsou tyto zdroje relevantní k řešenému tématu, očekával bych více zdrojů, jenž se problematikou loC systematicky zabývají.
- 7. Realizační výstup** 90 b. (A)
Výstupem je skript, který provádí automatickou identifikaci možných kompromitací operačních systémů. Tento systém je poměrně jednoduchý, avšak funkční a představuje vhodné řešení zadaného problému. Bylo také provedeno důkladné testování pomocí virtualizovaných prostředí a v téměř reálném prostředí, což dostatečně demonstrovalo použitelnost systému.
- 8. Využitelnost výsledků**
Systém byl vytvářen pro NÚKIB a dá se předpokládat, že bude příjemcem využit a dále rozvíjen.
- 9. Otázky k obhajobě**
 - Na základě čeho jste určil množinu podporovaný loC entit?
 - Jaké další loC informace by bylo vhodné sbírat a proč?
 - Z povahy řešení se zdá, že platforma OS Windows není podporována. Z jakého důvodu?
- 10. Souhrnné hodnocení** 80 b. velmi dobře (B)
Celkově se jedná o kvalitní práci, která má praktický potenciál. Text práce je srozumitelný a dobře vysvětluje řešenou problematiku. Realizační část má velmi dobrou úroveň. Přestože se jedná o poměrně jednoduché řešení jeho praktická použitelnost byla demonstrována při kybernetickém cvičení a dá se předpokládat, že nástroj bude uvažovaným příjemcem využíván.

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

V Brně dne: 28. května 2019

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