

Posudek práce

předložené na Přírodovědecké fakultě JU

- | | |
|---|---|
| ☒ posudek vedoucího | ☐ posudek oponenta |
| ☒ bakalářské práce | ☐ diplomové práce |

Autor/ka: Pavel Vodstrčil

Název práce: Analýza dat z automatických bezpečnostních scannerů

Studijní program a obor: Aplikovaná informatika

Rok odevzdání: 2019

Jméno a tituly vedoucího: ing. Petr Břehovský

Pracoviště: ÚAI PŘF Jihočeská univerzita, České Budějovice

Kontaktní e-mail: pbrehovsky@prf.jcu.cz

Odborná úroveň práce:

- ☐ vynikající ☒ velmi dobrá ☐ průměrná ☐ podprůměrná ☐ nevyhovující

Věcné chyby:

- ☐ téměř žádné ☒ vzhledem k rozsahu přiměřený počet ☐ méně podstatné četné ☐ závažné

Výsledky:

- ☒ originální ☐ původní i převzaté ☐ netriviální kompilace ☐ citované z literatury ☐ opsané

Rozsah práce:

- ☐ veliký ☒ standardní ☐ dostatečný ☐ nedostatečný

Grafická, jazyková a formální úroveň:

- ☐ vynikající ☐ velmi dobrá ☒ průměrná ☐ podprůměrná ☐ nevyhovující

Tiskové chyby:

- ☐ téměř žádné ☒ vzhledem k rozsahu a tématu přiměřený počet ☐ četné

Celková úroveň práce:

- ☐ vynikající ☒ velmi dobrá ☐ průměrná ☐ podprůměrná ☐ nevyhovující

Slovní vyjádření, komentáře a připomínky vedoucího/oponenta:

Současné skenery zranitelností poskytují informace, které neberou v úvahu prostředí, ve kterém jsou testované systémy provozovány. Výsledky skenů jsou tak nepřehledné a zobrazené kritičnosti nálezů neodpovídají danému prostředí.

Autor práce vytvořil nástroj, který zpracovává výsledky skenů bezpečnostních nástrojů, v přehledné formě je zobrazuje a obohacuje o hodnotící kritéria CVSS. Uživatel tak získá mnohem přesnější představu o rizicích, která nalezené zranitelnosti pro jeho síť představují.

Nástroj umožňuje doplnění neúplných CVSS vektorů ze skeneru o informace vypovídající o vlastnostech konkrétního prostředí a dovoluje definovat skupiny zařízení, například podle jejich funkčnosti, nebo příslušnosti. Existuje několik způsobů jak nálezy zobrazit.

Sám text práce by však zasloužil lepší logické uspořádání a jasnější vysvětlení popisovaných myšlenek a postupů. V neposlední řadě by byl vhodný i formálnější způsob vyjadřování.

Je však třeba vyzdvihnout autorovu vysoce samostatnou a odpovědnou práci při samotné implementaci nástroje.

Případné otázky při obhajobě a náměty do diskuze:

Jakým způsobem by bylo možné rozšířit aplikaci o import dat z databáze aktiv (jméno aktiva, IP adresa, vlastníci aktiva, kritičnost aktiva atd.)?

Práci

☒ doporučuji

☐ nedoporučuji

uznat jako bakalářskou.

Navrhuji hodnocení stupněm:

☐ výborně ☒ velmi dobře ☐ dobře ☐ neprospěl/a

Místo, datum a podpis vedoucího/oponenta:

V Českých Budějovicích 8.1.2020

