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:	2020

Jméno a tituly vedoucího/oponenta:	Ing. Jiří Jelínek, CSc.
Pracoviště:	Ústav aplikované informatiky
Kontaktní e-mail:	jjelinek@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:

Autor se zaměřuje na oblast bezpečnosti komponentů v počítačové síti a cílem jeho práce je analýza a prezentace dat exportovaných z automatických bezpečnostních skenerů. Oficiální zadání práce není přiloženo.
Druhá kapitola se zaměřuje na použitou metodiku, přičemž výčet použitého softwaru by měl odkazovat na příslušné zdroje. Bohužel tím také kapitola 2 končí a o metodice práce v ní není bohužel nic dalšího.
V třetí kapitole se autor zaměřuje na skenování sítí. Již v úvodu je poněkud nelogicky zmíněno několik softwarových nástrojů použitelných pro skenování sítě bez dalších informací. Proces skenování je popsán až následně a na obecné úrovni. Teprve pak, jsou uvedeny podrobnější informace k některým SW nástrojům, lépe vysvětlen by měl být systém pluginů.
Kapitola 4 se pak zaměřuje na popis CVSS, který však není zcela přesný (např. použití tří metrik). Vysvětlení metrik všech kategorií také chybí, zato je detailně diskutován rozdíl mezi verzemi CVSS. Seznam a význam těchto rozdílů uvedených v tabulce 2 by měl být rovněž vysvětlen. Bližší informace by měly být podány rovněž k obrázku 2. Otázkou je také výpočet výsledného skóre, který není popsán.
Kapitola 5 se zabývá návrhem databáze a importů, přičemž tento návrh není optimální z hlediska dalšího možného rozšiřování aplikace (zahrnutí dalších scannerů), kdy bude nutné strukturu DB upravit. Autor rovněž naznačuje, že v relační databázi ukládá redundantní hodnoty, přičemž není jasné, proč takto činí a vystavuje se tak možným problémům s nekonzistencí dat. Diskutabilní rovněž dvojice tabulek „CVSS_..." , kde by údaje mohly být uloženy i efektivnějším způsobem, zejména v situaci, kdy nebudou vyplněny všechny položky. Nejasně jsou uvedeny informace o tabulkách pro správu aktiv a skupin.
Reálně je import dat do databáze popisován až v kapitole 6. Autor zde otestoval rovněž možnost získání validních informací přímo z internetu, přičemž tuto metodu nakonec nevyužil, což považuji za nepříliš šťastné řešení (získané hodnoty by zaručovaly aktuálnost). V kapitole 6.3 autor rovněž zmiňuje vysokou časovou náročnost výpočtů a absenci vláknového zpracování v PHP, přičemž není zřejmé, proč tedy tuto technologii volil. Doba zpracování reportu 17 minut se jeví jako velmi problematická.
Kapitola 7 se zaměřuje na vytvoření samotné grafické webové aplikace na bázi PHP. Je zřejmé, že při návrhu nebylo postupováno dle obecných zásad návrhu SW aplikací (Use Cases, další požadavky, drátový model, ...). Autor zmiňuje rovněž bezpečnostní aspekt celého návrhu, přičemž se však nezabývá bezpečností použitého frameworku. Problémem je absence grafického rozhraní pro správu uživatelských oprávnění. Autor rovněž popisuje řadu různých reportů, kterými lze získat výpisy informací z aplikace a popsána je i další manipulace s GUI. V kapitole 8 se autor zabývá integrováním dalších programů do rozhraní, přičemž zmiňovány jsou aplikace Pink a Nmap.
Formální úroveň práce je velmi nízká, a to z důvodu existence značného množství pravopisných chyb a často nesrozumitelných formulací. Práce obsahuje také 24 uvedených zdrojů. Autor rovněž slibuje tři přílohy práce, přičemž v rámci Stagu nebyla uvedena ani jedna z nich. Dvě přílohy obsahově pokrývající tři avizované jsou přiloženy pouze v písemné podobě k textu práce. Autor dodal částečně dokumentované zdrojové kódy své aplikace, přičemž její funkční verzi nezpřístupnil (nebo nedodal např. ve formě virtuálního stroje).
Celkově lze konstatovat, že autor zadání práce naplnil s výše uvedenými výhradami a vytvořil nadstavbu nad existujícími skenery pro zpřístupnění a vizualizaci informací, které jsou tyto automatizované skenery schopné poskytnout. Celkově práci doporučuji k obhajobě a navrhuji hodnotit stupněm dobře.

Případné otázky při obhajobě a náměty do diskuze:

1. Předveďte vaši aplikaci v reálném provozu.
2. Popište způsob výpočtu CVSS skóre.

Práci
☑ doporučuji
☐ nedoporučuji
uznat jako diplomovou/bakalářskou.

Navrhuji hodnocení stupněm:
☐ výborně ☐ velmi dobře ☑ dobře ☐ neprospěl/a

Místo, datum a podpis vedoucího/oponenta:

V Českých Budějovicích dne 6. ledna 2020