

Posudek práce

předložené na Přírodovědecké fakultě JU

☒ posudek vedoucího
☐ bakalářské práce

☐ posudek oponenta
☒ diplomové práce

Autor/ka:

Bc. Tomáš Starý

Název práce:

Výzkum a implementace IDS/IPS systému jako ochranu proti aktuálně probíhajícím hrozbám v prostředí velkého poskytovatele internetových služeb

Studijní program a obor:

Aplikovaná informatika

Rok odevzdání:

2019

Jméno a tituly vedoucího/opponenta: Ing. Rudolf Vohnout, Ph.D.

Pracoviště:

ÚAI

Kontaktní e-mail:

rudolf.vohnout@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:

☐ velký ☒ 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:

Předložená práce představuje komplexní celek řešení jedné z aktuálních hrozeb nejen v prostředí internetových poskytovatelů služeb, ale kohokoliv, kdo nemá zabezpečené webové formuláře, ať už využitím některých dostupných free CMS (Joomla, Wordpress, Prestashop atd.) nebo jiným proprietárním řešením. Na rozdíl od nevyžádané pošty posílané přes klasické SMTP servery a spoléhání se na anti-spam filtry je využívání webových formulářů mnohem sofistikovanější.

Práce obsahuje menší množství překlepů („lswh“, „Wordpress“ atd.), ale jinak je z gramatického a interpretačního hlediska nadprůměrná a citace jsou excelentní (až na úsměvnou citaci [41]). Práce je logicky členěna, začíná nezbytným teoretickým úvodem včetně popisu jednotlivých IDS/IPS systémů a stanovení kritérií pro výběr vhodného řešení pro dané infrastrukturní prostředí. Práce dále pokračuje přes základní popis problematiky a způsobů odesílání nevyžádané pošty přes nezabezpečené webové formuláře až dostává ke své stěžejní praktické části (kapitoly 8, 9, 10 a 11).

Praktická část ovšem z větší části popisuje postup instalace Dockeru, přechody na nové releases IDS/IPS Suricata (a problémy s tím spojené), verzování souboru „test_vx.sh“ (kde se čtenář dovídá, jak nová verze byla lepší než verze předchozí) a úpravu stávajících pravidel. V závěru (kapitola 10 a především pak kapitola 11) je náznak stěžejní části práce, tj. nasazení systému a vyhodnocení jeho přínosů. Na samotné práci je vidět množství odpracovaných hodin a velmi hezky se čte. Jako manuál či dokumentace pro instalaci Open Source IDS/IPS řešení v Dockeru pro konkrétní prostředí je vynikající, stejně tak by mohla sloužit jako podklad výkaz práce za posledního půl roku.

„A“ tedy máme, ovšem toto je práce diplomová a chybí jí „B“. Část, kde bude využit sběr dat pro vyhodnocení formou pokročilých metod např. statistické analýzy? Protože se jedná o diplomovou práci, očekával bych implementaci samoučícího se mechanismu, který bude sám navrhovat nová pravidla, či anomálie, přiřazovat jim na základě četností vážnost pro doporučení jejich nasazení. Proč nebyl nasazen také nějaký alternativní (v teoretické části zmíněný) IDS/IPS systém pro provedení komparativní analýzy? Kde jsou časové řady interpretující změnu reputace domény či IP rozsahů firmy WEDOS Internet, a.s. po nasazení řešení? Atd...

Jsem ochoten přimhouřit oči, protože znám okolnosti vypracovávání práce, ovšem po zjištění, že nebyla provedena ani jedna konzultace s povinným konzultantem z praxe, Ing. Břehovským zmíněným v zadávacím protokolu, práci nemohu práci jako celek hodnotit lépe než *dobře*.

Případné otázky při obhajobě a náměty do diskuze:

Proč jste neprobíral průběh práce s konzultantem?

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

8.7. 2020

