Posudek práce

předložené na Přírodovědecké fakultě JU

❑posudek vedoucího ✓posudek oponenta
❑ bakalářské práce ❑ diplomové práce

Autor/ka: Bc. Tomáš Starý
Název práce: Výzkum a implementace open-source řešení 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/oponenta: Josef Grill
Pracoviště: WEDOS Internet, a.s.
Kontaktní e-mail: josef.grill@wedos.com

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:
Úvodní témata popisovaná v první části textu, která je čistě teoretická, přímo souvisí s cílem diplomové práce. Autor je má zpracované vhodným způsobem. Zařazení první kapitoly, v níž autor definuje důležité pojmy související s diplomovou prací hodnotím jako přínosné a podstatné pro správnou orientaci v dalším textu.

V další části autor popisuje výhody a nevýhody jednotlivých řešení a dostává se tak plynule k rozhodnutí o výběru řešení, které je dále použito v diplomové práci.

Významná část práce se věnuje již praktickým postupům při vývoji, nasazení a testování celého prostředí IDS/IPS ochrany.

V diplomové práci jsou jasně uvedené nejen postupy, kterými autor došel ke svému cíli, ale i výsledky jasně vyjádřené čísly a podložené statistikami. Domnívám se, že je uvedena jen malá část možných statistických výsledků a pohledů na celý problém a to jen ta, kterou se autor přímo zabýval. Určitě bychom našli další možnosti jak hodnotit získaná data, ale autor se rozhodl správně a považuji to za dostačující.

Je vidět, že autor celou práci zpracovával postupně sám, jednotlivými postupnými kroky. Každý krok si nejen musel vymyslet, ale také zároveň vyhodnotit to, zda je zvolený postup správný.

Velmi oceňuji praktické využití celé práce. Nejedná se tak čistě o práci teoretickou, ale o práci, která zpracovává a vyhodnocuje jednotlivé teoretické postupy a umožňuje jejich aplikaci přímo v praxi.

Případné otázky při obhajobě a náměty do diskuze:

- Setkal se autor při vývoji s některými „slepými uličkami“?
- Jaké jsou další možnosti rozšiřování a vylepšování podobných řešení do budoucna?
- Co si autor myslí o plošném nasazení podobných IDS/IPS systémů nejen v prostředí poskytovatelů hostingu, ale i v prostředí ISP? Myslíte si, že je to reálné a užitečné?
- Nakolik je omezující tvorba různých pravidel pro případné plošné nasazení.
- Je reálné nabízet podobnou IDS/IPS ochranu jako službu například na vstupu do jednotlivých firemních sítí? Pokud autor myslí, že ano, tak jak by navrhl podobné řešení? Může být založené na stejné technologii nebo by muselo jít o zcela jinou koncepci?
- Nad rámec práce je určitě ekonomická stránka celého problému. Zamýšlel se autor nad tím někdy a jaký na to má autor názor? Komplexně vzato od rozhodnutí mezi opensource a placenými řešeními, přes samostatný (a časově a ekonomický nákladný) vývoj až po samotnou realizaci a udržování systému během provozu.

Práci
✓ doporučuji
☐ nedoporučuji
uznat jako diplomovou/~~bakalářskou~~.

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

Místo, datum a podpis vedoucího/oponenta:
V Hluboké nad Vltavou dne 5. ledna 2020