

Posudek oponenta bakalářské práce

Student: Zítka Radim
Téma: Analýza aplikačních firewallů sociálních sítí (id 24019)
Oponent: Malinka Kamil, Mgr., Ph.D., UITS FIT VUT

1. **Náročnost zadání** průměrně obtížné zadání
2. **Splnění požadavků zadání** zadání splněno s drobnými výhradami

Všechny body zadání byly splněny. Nicméně body týkající se nastudování existujících aktuálních metod jsou zpracovány na velmi základní úrovni. Chybí např. porovnání existujících aplikačních FW a jejich schopností detekovat boty. Obdobně pak část týkající se analýzy aplikačních sociálních sítí obsahuje pouze empirické měření. Chybí analýza dostupné dokumentace a literatury. Výhrady mám i k návrhu opatření, kdy některé podle mě nepatří na úroveň aplikačních FW nebo jsou velmi základní.
3. **Rozsah technické zprávy** je v obvyklém rozmezí

Rozsah technické zprávy odpovídá požadavkům na bakalářskou práci.
4. **Prezentační úroveň předložené práce** 75 b. (C)

V úvodních kapitolách práce chybí lepší vysvětlení motivace celé práce a specifikace cílů práce. Dlouho tak není jasné, na čem chce autor pracovat. Kapitola 3 mi nepřijde relevantní k tématu. Kapitola 4 poskytuje přehled různých oblastí zranitelností, ale je extrémně obecná. Chybí větší zaměření na téma. Naopak kapitola 5 solidně představuje relevantní technologie a přístupy automatického přístupu. Kapitola 6 prezentuje poměrně zdařilé testování existujících sociálních sítí. Autor testuje jejich chování, ale nikde není zmíněno, zda se student podíval do dokumentace a dalších relevantních materiálů. Drobnou výtku mám k metodice testování - občas nedošlo k detekci problému s odůvodněním na nedostatečný výkon stanice. Student měl použít dostupné výkonnější zdroje. Prezentovaný návrh opatření není podložen teorií - je opravdu problém stejné chování (chovaly by se boty takto)? Jaký je model útočníka? Závěrečné kapitoly nicméně dobře prezentují realizované výsledky. Autor se v práci občas opakuje.
5. **Formální úprava technické zprávy** 75 b. (C)

Práce obsahuje menší množství jazykových a typografických chyb. Nicméně jazyková a stylistická stránka práce je na dobré úrovni.
6. **Práce s literaturou** 65 b. (D)

Odkazované zdroje jsou relevantní tématu a až na výjimky vhodně vybrány, nicméně by jich mělo být více. Tou výjimkou je reference na Wikipedii. Některé oblasti nejsou literaturou vůbec podloženy, nejvíce to chybí v části týkající se nastudování aktuálních aplikačních firewallů. V práci také nejsou popsány existující best practices ochran, OWASP, již existující řešení apod.
7. **Realizační výstup** 65 b. (D)

Realizační výstup se skládá z několika částí: zprovoznění simulované sociální sítě, implementace vybraných ochranných opatření a implementace testů jejich funkčnosti. Implementace je na dobré úrovni. Student naimplementoval vše, co si navrhnul. Hlavní výtku mám ovšem k vlastnímu návrhu: navržené ochrany jsou poměrně naivní. Např. hodnota user-agent se dá jednoduše podvrhnout, počet neúspěšných přihlášení spíše patří do autentizačních a autentizačních mechanismů než na úroveň aplikačních FW, test na opakované zadání hesla zablokuje pouze prohlížeč, což je neefektivní, atd.
8. **Využitelnost výsledků**

Práce se snaží přinést informace pro zkvalitnění implementace aplikačních FW, nicméně výsledky nepovažuji za dále využitelné.
9. **Otázky k obhajobě**
 1. Můžete uvést, jaké metody ochran proti automatickému přístupu používají aktuální dostupné aplikační FW?
 2. Jste si vědom toho, že v jednom opatření děláte profilaci uživatele? Jak by se na to dívalo GDPR
10. **Souhrnné hodnocení** 70 b. dobře (C)

Hlavním problémem práce je nedostatečné nastudování řešené problematiky. Student většinu věcí řeší pouze na základě svého aktuálního povědomí o problematice, které dále nerozšiřoval. Podle toho pak vypadá i kvalita návrhu opatření, které jsou velmi základní, některé navíc podle mě spadají do jiné oblasti. Nicméně autor svůj návrh solidně implementovat a otestoval, textová část je dobře zpracovaná. Autor dále sliboval doporučení pro tvorbu aplikačních FW na základě analýz aktuálních sociálních sítí, nicméně výsledky testování dále nijak

nerozvíjí.

Práci navrhuji uznat jako bakalářskou a hodnotím ji "C".

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

V Brně dne: 2. června 2021

Malinka Kamil, Mgr., Ph.D.
oponent