



Posudek oponenta na bakalářskou práci

Student: **Marek Timr**

Název: **Framework for Proof of Concept Implementations of C&C Channels**

Oponent: **Jan Kubr, Ing.**

1 Náročnost a další komentář k zadání

Hodnocení: 3 – průměrně náročné

Zadání hodnotím jako průměrně náročné. Zadání je zaměřené na řešení existujících botnetů a analýzu C&C kanálů v nich používaných. Dále se práce zaměřuje na návrh a implementaci frameworku, který usnadňuje vytváření C&C kanálů pro jejich snazší zkoumání. V závěru by měl autor posoudit zneužitelnost vybraných služeb pro vytváření C&C kanálů.

2 Splnění zadání

Hodnocení: 2 – splněno s menšími výhradami

Zadání bylo splněno. Jedinou výhradu mám k slabšímu posouzení zneužitelnosti vybraných služeb pro vytváření C&C kanálů.

3 Rozsah písemné zprávy

Hodnocení: 1 – splňuje požadavky

Písemná zpráva splňuje požadavky na bakalářskou práci. Všechny části písemné zprávy jsou pro práci nezbytné a informačně bohaté.

4 Věcná a logická úroveň práce

Hodnocení: 90 bodů A

Práce je přehledná a dobře čitelná. Práce neobsahuje věcné a logické chyby.

5 Formální úroveň práce

Hodnocení: 90 bodů A

V práci jsem našel minimální množství překlepů a chyb.

6 Práce se zdroji

Hodnocení: 85 bodů B

Překvapivě mezi zdroji chybí kniha doporučená vedoucím práce (Bloch Joshua; Effective Java).

7 Hodnocení výsledků, publikační výstupy a ocenění

Hodnocení: 85 bodů B

Text je poměrně čtivý. Navržený a implementovaný framework bude přínosný pro studium některých C&C kanálů. Je škoda, že autor neprovedl důkladnější zhodnocení C&C kanálů.

8 Komentář o využitelnosti výsledků

Největší přínos práce je v její praktické části, tedy implementaci frameworku. Velmi zajímavý je návrh hybridního C&C kanálu.

9 Celkové hodnocení

Práce splňuje zadání. Návrh a implementace frameworku je přínosná pro další výzkum C&C kanálů. Jediným nedostatkem práce je slabší zhodnocení C&C kanálů a absence naměřených výsledků pomocí frameworku.

Práci hodnotím **90 body (A – výborně)**.

10 Otázky k obhajobě

- Byla provedena nějaká měření pomocí implementovaného frameworku? S jakými výsledky?
- Jaké byly použity postupy pro otestování implementace frameworku?
- Proč autor nepoužil literaturu doporučenou vedoucím práce?