Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK OPONENTA BAKALÁŘSKÉ PRÁCE

Jméno studenta: Radek Netolický

Název práce: Moderní techniky analýzy malware

Autor posudku: Ing. Lubomír Almer, Ph.D.

Cíl práce: Cílem bakalářské práce je představení problematiky analýzy malware pro zajištění parametrů důvernosti, dostupnosti a integrity dat, tedy základním stavebním kamenům zajištění bezpečnosti. V teoretické části autor představí a podrobně popíše principy bezpečnosti s důrazem na hrozby typu malware a jejich dopad na zajištění bezpečnosti. V praktické části pak autor vytvoří praktická řešení dílčích úloh statické a dynamické analýzy malware dle předem definovaných usecase.

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)					
	A	**B**	**C**	**D**	**E**	**F**
Práce svým zaměřením odpovídá studovanému oboru	☒	☐	☐	☐	☐	☐
Vymezení cíle a jeho naplnění	☐	☒	☐	☐	☐	☐
Zpracování teoretických aspektů tématu	☐	☐	☐	☒	☐	☐
Zpracování praktických aspektů tématu	☐	☒	☐	☐	☐	☐
Adekvátnost použitých metod, způsob jejich použití	☐	☐	☐	☐	☒	☐
Hloubka a správnost provedené analýzy	☐	☐	☐	☒	☐	☐
Práce s literaturou	☐	☐	☒	☐	☐	☐
Logická stavba a členění práce	☐	☒	☐	☐	☐	☐
Jazyková a terminologická úroveň	☐	☒	☐	☐	☐	☐
Formální úprava a náležitosti práce	☐	☒	☐	☐	☐	☐
Vlastní přínos studenta	☐	☒	☐	☐	☐	☐
Využitelnost výsledků práce v teorii (v praxi)	☐	☒	☐	☐	☐	☐

Vyjádření k výsledku anti-plagiátorské kontroly

Antiplagiátorská kontrola identifikovala celkovou podobnost: 6 %.

Dílčí připomínky a náměty:

Autor v práci neuvádí použité metody a způsob jejich použití.

Dále doporučuji v cíli práce, případně v omezeních se vymezit na konkrétní nástroje, které budou pro zpracování práce použity. Rovněž je žádoucí mít soulad mezi cílem práce, který je uveden v zadání a cílem, který je uveden v textaci práce.

Celkové posouzení práce a zdůvodnění výsledné známky:

Autor bakalářské práce v definici cíle práce (kapitola č. 2) použil rozdílný popis cíle vůči zadání,

a to konkrétně: popsat historii a vývoj kybernetické bezpečnosti v České republice, popsat zákon o kybernetické bezpečnosti, popsat základní modely informační bezpečnosti, objasnit základní pojmy z oblasti analýzy rizik, vysvětlit statickou a dynamickou analýzu.

Autor v teoretické části představil a popsal principy bezpečnosti za použití CIA triády. Rovněž je v teoretické části vymezena oblast malware a rozdělena do jednotlivých typů. Teoretická část dále vcelku detailně popisuje techniky analýzy malware.

V praktické části autor popisuje konkrétní úlohy statické a dynamické analýzy malware za použití nástrojů: HashMyFiles, VirusTottal, PEID, UPX, Strings, Wireshark, Process Monitor a Regshot. Řešené úlohy jsou popsány v dostatečném detailu pro naplnění definovaného zadání. Jediným nedostatkem v praktické části je absence popisu metodiky testování.

Na základě uvedeného autor práce naplnil veškeré stanovené cíle uvedené v zadání práce.

Bakalářská práce je dobře logicky členěna a strukturována, stylistická a grafická podoba je rovněž na dobré úrovni.

Otázky k obhajobě:

Zdůvodněte volbu nástrojů pro statickou a dynamickou analýzu malware.
Doplňte otázky k obhajobě.

Práci doporučuji k obhajobě.

Navržená výsledná známka: B

V Hradci Králové**, dne 15. května 2024**

podpis