Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK VEDOUCÍHO BAKALÁŘSKÉ PRÁCE

Jméno studenta: Jiří Hladík

Název práce: Analýza nástrojů pro automatizovanou analýzu a ošetření operačního systému Windows v případě napadení malware

Autor posudku: Ing. Tomáš Svoboda, Ph.D.

Cíl práce: Cílem práce je představení problematiky analýzy nástrojů pro automatizovanou analýzu a ošetření operačního systému Windows v případě napadení malware

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 eVSKP identifikovala celkovou podobnost: 16 %. Po manuálním přezkoumání uvedených shod je možné konstatovat, že se jedná o shodu ve výpisem logů z praktické části práce, které odpovídají oficiální dokumentaci společnosti Microsoft k testovanému produktu, což bylo zapříčiněno využitím oficiální distribuce operačního systému Microsoft Windows a nejedná se tedy o plagiát.

Dílčí připomínky a náměty:

Vedoucí práce má následující připomínky a náměty k předložené práci:

1. V Úvodu bakalářské práce je uvedena struktura a členění bakalářské práce jako celku, avšak práce postrádá obecný úvod do problematiky. Bylo by vhodné v úvodu bakalářské práce popsat současný stav, hrozby, zranitelnosti a aktuální vývoj v oblasti kybernetické bezpečnosti s ohledem na probíhající a historické kybernetické útoky zneužívající zranitelnosti v operačních systémech a možnosti obrany, resp. odhalení tohoto typu útoků, což je hlavním cílem bakalářské práce.

2. Na základě předchozí připomínky lze konstatovat, že cíle práce nejsou dostatečně vysvětleny ve 2. kapitole, ale jsou součástí Úvodu bakalářské práce, což pro čtenáře působí matoucím dojmem.

Celkové posouzení práce a zdůvodnění výsledné známky:

Předložená práce je rozdělena do pěti kapitol včetně úvodu a závěru. Ve 3. kapitole autor popisuje vývoj operačních systémů s důrazem na platformu Windows a základních funkcionalit tohoto operačního systému, včetně Windows serveru a dotýká se okrajově i operačních systémů rodiny UNIX/LINUX. Dále jsou představeny základní pilíře zajištění informační bezpečnosti s důrazem na CIA triádu a Parkerian Hexad včetně nejznámějších typů hrozeb, které cílí na narušení parametrů informační bezpečnosti v operačních systémech. Autor dále představuje možnosti ochrany operačního systému za využití komerčních a open-source nástrojů ve formě antiviru, antispware, anti-phishingové ochrany a customizovaných skriptů. V této kapitole by bylo vhodné provést analýzu na detailnější úrovni, neboť se jedná pouze o obecný popis možností ochrany operačního systému, ale bez vazby na konkrétní typy hrozeb, které autor představil v kapitole 3.4.
Následuje kapitola 4., kde autor práce představuje vytvoření virtuálního prostředí pro praktickou část bakalářské práce, instalaci Tron skriptu a testování infekce virtuálního stroje prostřednictvím tohoto typu skriptu. Bohužel, práce postrádá logickou návaznost mezi teoretickou a praktickou částí. Není zřejmé, na základě jakých kritérií autor vybral pro praktickou část Tron skript, lze pouze usuzovat, že toto řešení bylo vybráno na základě již existujících zkušenosti autora. Autor měl provést detailní analýzu dostupných řešení custom skritptů pro účely testování Windows v případě napadení malware a na základě předem definovaných kritérií vybrat skript pro praktickou část.
Představení každé jednotlivé fáze využití Tron skriptu je logicky popsáno, avšak je velká škoda, že autor v praktické části práce nedoplnil texty výstupu z testování jednotlivými částmi z log souboru Tron skritpu a celý tento výstup zahrnul pouze do přílohy bakalářské práce.

Závěrem lze konstatovat, že autor práce naplnil vytyčený cíl a práce splňuje požadavky kladené na závěrečnou práci.

Otázky k obhajobě:

1. Z jakého důvodu byl vybrán pro praktickou část bakalářské práce právě Tron skript?
2. Jaké jsou další customizované skripty, které poskytují stejné nebo podobnmé funkcionality jako Tron skript?

Práci doporučuji k obhajobě.

Navržená výsledná známka: C

V Hradci Králové**, dne 30. prosince 2023**

_____

podpis