

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: BC. JAN DLUHOŠ

Oponent: Ing. Ladislav Vyskočil

Studijní program: **Informační technologie**
Specializace: **Kybernetická bezpečnost**
Akademický rok: **2024/2025**

Téma diplomové práce: Analýza detekčních enginů antivirových programů

Hodnocení práce:

Cílem diplomové práce bylo popsat problematiku analýzy detekčních enginů antivirových programů, k jehož dosažení bylo třeba naplnit několik bodů, jejichž přesná specifikace byla součástí zásad uvedených v zadání práce. Všechny body zadání diplomové práce byly splněny v plném rozsahu. Diplomant popisované problematice rozumí. Diplomová práce je na vysoké odborné úrovni, je přehledně strukturována a jednotlivé části na sebe logicky navazují. Text práce je zpracován odborně a srozumitelně. Po jazykové stránce nebyly nalezeny žádné pravopisné, nebo stylistické chyby. Po formální stránce je práce vhodným způsobem řazena do logických celků a doplněna upřesňujícími komentáři i odkazy na odpovídající literární či elektronické zdroje. V diplomové práci autor uvádí přiměřené množství obrázků, tabulek a příloh.

V teoretické části byla popsána antivirová řešení a jejich detekční mechanismy, zahrnující přehled základních typů malware, přehled současných AV řešení a popis používaných detekčních mechanismů AV programů. Byla popsána statická, dynamická a behaviorální detekční analýza i mechanismy založené na strojovém učení. Další kapitola teoretické části popisuje metody stěžující detekci malware AV enginem. Zde byly popsány metody obfuskace kódu, šifrování, anti-debugging a anti-sandbox techniky, fileless malware, rezidentní kód a proces injection techniky.

Praktická část obsahuje přípravu testovacího prostředí a vývoj testovacích vzorků malware. Bylo vytvořeno několik typových vzorků malware, které byly použity pro analýzu detekčních enginů AV programů. Následně bylo v další kapitole provedeno experimentální ověření detekce vytvořených vzorků malware a porovnání efektivity detekčních mechanismů. Byla popsána metrika a metodický postup při analýze, velmi podrobně prezentovány výsledky analýzy pro jednotlivé AV enginy a popsány omezení a slabiny detekčních mechanismů jednotlivých AV řešení. Poslední kapitola praktické části se zabývá návrhy na zlepšení ochrany před malware a doporučení pro koncové uživatele a organizace.

Přínos práce vidím v odborném popisu této problematiky, včetně použitých kódů, kdy diplomová práce může sloužit jako zdroj užitečných informací pro další výzkum. Diplomová práce se jeví jako velmi zdařilá a splňující svůj cíl, a proto ji doporučuji předložit k obhajobě.

Celkové hodnocení práce:

Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:

A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně, F – nedostatečně.

Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 30. 5. 2025

Podpis oponenta diplomové práce