ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	Bezpečnostní nástroj využívající klasifikaci Mitre ATT&CK
Jméno autora:	Harant Filip
Typ práce:	diplomová
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	katedra telekomunikační techniky
Oponent práce:	Ing. Josef Koumar
Pracoviště oponenta práce:	Fakulta informačních technologií (FIT)

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání — **náročnější**

Hodnocení náročnosti zadání závěrečné práce.

Zadání práce si definuje za cíl vytvoření nástroje pro modelování hrozeb pomocí klasifikace MITRE ATT&CK. Jelikož je nutné hluboce porozumět metodám kybernetické bezpečnosti, nastudovat řadu nástrojů kybernetické bezpečnosti, zpracovat velké množství dat a naprogramovat vlastní nástroj, tak práci hodnotím jako náročnější.

Splnění zadání — **splněno**

Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Zadání bylo plně splněno.

Zvolený postup řešení — **správný**

Posuďte, zda student zvolil správný postup nebo metody řešení.

Student zvolil správný postup řešení při řešení teoretické části práce. U praktické části navrhnul správně podobu nástroje a vhodně zvolil programovací jazyk Python. Nicméně praktické provedení implementace je bohužel žalostná. Hodnotím postup jako správný s menšími výhradami.

Odborná úroveň — **C - dobře**

Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

Student nastudoval vhodné prameny a na základě nich navrhnul a naimplementoval nástroj, který by mohlo být bývalo možné použít přímo v praxi. Po odborné stránce teoretická část a text neobsahuje žádné nedokonalosti. Oceňuji zejména navržení vhodných kroků, které musí organizace podniknout, aby provedla adekvátní zlepšení bezpečnosti proti APT hrozbám na základě veřejně dostupných informací.

Nicméně odborná úroveň Python kódu je bohužel na opačné hranici spektra než ta teoretická. V bodech:

- Návrh celého nástroje je chaotický – student například vytvořil samostatný soubor, ve kterém je jedna obrovská nepřehledná funkce
- Student nedodržuje zaběhlý PEP8 coding-style
- Kód neobsahuje téměř žádné komentáře, ani dokumentační stringy, ani dokumentování argumentů funkcí a návratových hodnot
- Student se často zanořuje v jedné funkci třeba až 7 krát
- Potřebné knihovny jsou napsané pouze v README.md a to ještě bez verzí, což znamená, že dle tohoto „návodu na instalaci" nástroj pravděpodobně v budoucnu nebude nikdo moci nainstalovat a spustit.
- Student importuje některé knihovny dvakrát, a řadu knihoven či jejich částí importuje aniž by je v nástroji používal

Úroveň praktického řešení dokresluje například to, že student ve funkci *getTechniques2()* načítá hned dvakrát po sobě soubor *„Techniques_to_mitigate.json"* přičemž používá jen jeden z výstupů. Nebo například ve for cyklu opakovaně vytváří konstanty.

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

Celkově měl student zvolit jiný postup řešení a to formou Python knihovny, která se nainstaluje z PyPI pomocí jednoho příkazu. Jelikož se jedná o nástroj se skvělou myšlenkou a mohl by o něj být ve firmách zájem, tak je škoda, že kód není zabalen do knihovny nebo alespoň zveřejněn na GitHub.

Formální a jazyková úroveň, rozsah práce **B - velmi dobře**

Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.

Z hlediska anglického jazyka by bylo možné práci ještě zlepšovat. Například se v práci většinou používá první osoba jednotného čísla, ale občas se přejde na první osobu množného čísla. Uvítal bych kdyby v práci byla kapitola Implementace, rozdělena na kapitoly Návrh a Implemetace. Bohužel takto napsaná kapitola Implementace je lehce chaotická a mate čtenáře, například poslední obrázek je bez popisku a bylo by vhodné jej umístit na začátek kapitoly Implementace, resp. do kapitoly Návrh.

Kapitola Testování bohužel úplně chybí i přes to, že zadáním je vytvoření nástroje, a tudíž i jeho otestování. Navíc kapitola Implementace obsahuje dvě A4 taktik, které ale do kapitoly nazvané Implementace by vůbec neměli patřit, spíše by měli být v teoretické části práce. Rozsah práce je od úvodu po závěr 39 stran přičemž obsahuje řadu obrázků, proto rozsah práce hodnotím lehce pod průměrem, jelikož od diplomové práce bych očekával 50 A4 stran od úvodu po závěr.

Výběr zdrojů, korektnost citací **A - výborně**

Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Citační etika studenta není v rozporu z běžnou praxí u závěrečných prací.

Další komentáře a hodnocení

Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.

Vložte komentář (nepovinné hodnocení).

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

Celkově jsem byl do kapitoly Implementace tématem, textem a navrženými kroky obrany nadšený. Nicméně kapitola Implementace je lehce chaotická a provedení implementace v jazyce Python je žalostné. Proto jsem se rozhodl dát finální hodnocení horší B (skoro C).

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **B - velmi dobře.**

Otázky k obhajobě:

1. Do nástroje je vložen parametr „geolokace". Co znamená pro organizaci využívající nástroj, pokud útočník použije APT hrozbu z jiného konce světa než bylo původně vybráno v nástroji?
2. Jak jste vytvořený nástroj testoval?
3. Zkusil jste použít nástroj či navržené kroky u řešení kybernetické bezpečnosti v reálné firmě?

Datum: 15.6.2024 Podpis: