FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Josef Kokeš, Ph.D.
Student:	Bc. Silvie Němcová
Název práce:	Analýza technik "Lateral movement" v systémech s OS Windows
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	1. června 2024

Hodnotící kritéria

1. Splnění zadání

[1] zadání splněno
[2] zadání splněno s menšími výhradami
[3] zadání splněno s většími výhradami
▸ **[4] zadání nesplněno**

O splnění zadání mám vážné pochybnosti - řekl bych, že se studentka zaměřila výrazně odlišným směrem, než bylo požadováno. Jak zadání rozumím, tak smyslem mělo být nalezení postupů, jak v dříve napadeném systému rozpoznat známky pohybu útočníka mezi počítači (bod 2), tyto postupy ověřit na skutečně napadeném systému (bod 3) a vyhodnotit jejich účinnost (bod 4). Namísto toho se studentka věnovala velmi podrobné teoretické rešerši a v praktické části tomu, jak nastavit detekční pravidla tak, aby zachytila známky jednoho konkrétního způsobu pohybu útočníka v okamžiku, kdy k tomu dochází, a toto ověřila na umělém testovacím případě. Primární cíl, který zadání deklaruje, podle mě není splněn.

2. Písemná část práce

70 / 100 (C)

Písemná část zadání velmi podrobně popisuje obecné principy a techniky pro detekci hrozeb. Tato část je v pořádku a do textu jednoznačně patří, i když její formulace působí dosti "manažerským" dojmem a je velice rozsáhlá. Méně spokojen jsem se samotnými technikami detekce laterálního pohybu útočníka, které vnímám jako poměrně stručné, povrchní a zejména velmi nekonkrétní; líbí se mi kapitoly 1 a 6.1, zbytek je vesměs jen obecným popisem bez hlubšího obsahu, chybí zejména konkrétní rozhodnutí, jejich zdůvodnění a výsledky. Poznatky z analýzy modelu útočníka (kap. 6.1) mi dávají smysl a věřím, že detekce na nich postavené by fungovaly, nevidím však, že by v práci byly skutečně použity. Celkově textová část práce působí jako dobrý teoretický úvod do problematiky, podle zadání jsem však očekával výrazně praktičtější pojetí.

Pochvalu si zaslouží jazyková stránka práce, narazil jsem jen na několik málo chyb (zejm. překlep v titulku sekce 1.2.6). Použití čárek mezi větami je možná příliš rozsáhlé a narážíme na některé typografické prohřešky (špatné uvozovky, přetékající řádky v bibliografii, chybějící úvod v kapitole 2), ale celkově v pořádku. Chybí mi citace u některých obrázků, které patrně pocházejí z externích zdrojů (1.2, 1.3, 3.1, 3.4, 3.5, 4.1, 4.2). Zdroje mají nekonzistentně zapsané autory (srv. [13] a [14]).

3. Nepísemná část, přílohy

50 /100 (E)

Nepísemnou část práce tvoří zejména nástroje pro vytvoření testovacího prostředí, pravidla pro detekci laterálního pohybu útočníka a skripty pro simulaci útočníka. Testovací prostředí nedokážu ověřit kvůli chybějícím prerekvizitám, ale obsah vypadá rozumně, i když velmi jednoduše a není jasné, jaký přínos vlastně má proti pouhému rozkopírovanému virtuálnímu stroji s čistě nainstalovanými Windows. Detekční pravidla považuji za velmi chudá a vedoucí k mnoha falešným detekcím - první detekuje všechna vytvoření souboru na jiném disku než C:, druhé detekuje spuštění utility attrib.exe nebo použití argumentu "+h" nebo výskyt řetězce "[System.IO.FileAttributes]::Hidden" na příkazové řádce. Toto vnímám jako nedostatečné, i když odhlédneme od otázky, zda vůbec plní zadání. Skripty pro simulaci útočníka jsou triviální, bez jakéhokoliv pokusu o zamaskování činnosti (což by skutečný útočník jistě udělal), ale v zásadě funkční v rámci omezení daných tím, co detekční pravidla dokážou rozpoznat.

4. Hodnocení výsledků, jejich využitelnost

30 /100 (F)

Obávám se, že v odevzdané podobě není práce příliš použitelná. Její rešeršní část poskytne čtenáři dobrý náhled do problematiky, ovšem na dosti abstraktní úrovni, čtenář nejspíš bude mít potíže ji aplikovat do praxe. To, co měla práce hlavně přinést, podle mě neplní.

Celkové hodnocení

49 /100 (F)

Mé celkové hodnocení je velmi ovlivněno tím, že práci vnímám jako výrazně se odchylující od zadání. Pokud by bylo cílem, vytvořit materiál pro přiblížení problematiky nováčkovi, asi bych neměl námitky - rešeršní část práce je zpracovaná dobře, je přehledná a dosti ucelená, i když by jí velmi pomohly praktické příklady. Praktické aspekty, které v zadání vnímám jako ty stěžejní, však nejsou uspokojivě řešeny. Experimentální prostředí je zaměřeno na jiný účel, než požaduje zadání, detekční pravidla jsou podle mě nepoužitelná a simulace útočníka je sice v zásadě funkční, ale velmi jednoduchá a prakticky stěží upotřebitelná. Za těchto okolností se přikláním k hodnocení Nedostatečně (F).

Otázky k obhajobě

1) Jak by mělo proběhnout praktické nasazení vašich výsledků?
2) V čem spatřujete hlavní přínosy vašeho testovacího prostředí ve srovnání s čistě nainstalovanými Windows?
3) Dělala jste nějaké testy na falešné poplachy ve vašich detekcích? S jakým výsledkem?

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.