FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Lukáš Kotlaba
Oponent práce:	Ing. Miroslav Prágl, MBA
Název práce:	Detection of Active Directory attacks
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 10. 6. 2019

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
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.

Komentář:
Zadání splněno bez výhrad. Rozsahem je práce nadstandardní. Je přehledná, čitelná, bez chyb. V obecném úvodu popisuje problematiku, dále navrhuje vhodné prostředky ke splnění zadaných cílů a realizuje je.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*95 (A)*

Popis kritéria:
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. 26/2017, 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.

Komentář:
Práce je vyvážená, všechny části jsou přiměřeně informačně bohaté. Jednotlivé části na sebe dobře navazují. Hutnost realizační části je dobře vyvážena čtivým obecným úvodem do problematiky. Formálně, jazykově i typograficky je na velmi dobré úrovni, citace jsou bohaté a přehledné. Citované zdroje jsou převážně internetové, což je u tématu pochopitelné.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*100 (A)*

Popis kritéria:
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

Komentář:
Zvolené prostředky / technologie jsou vhodné a odpovídající. Testovací prostředí bylo vybráno tak, aby v maximálně možné míře odpovídalo reálné konfiguraci běžné sítě (AD, různé verze klientských OS, databázový server). Pro testovací útoky byla zvolena distribuce Kali Linux, což je de facto standard pro digitální forenzní analýzu a penetrační testy. Vzhledem ke komplexnosti zpracovávaných logů byly s výhodou nasazeny technologie pokročilého parsování/zpracování logů, založené na SPL (Search Processing Language). Testy jsou dobře popsané a opakovatelné.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*100 (A)*

Popis kritéria:
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.

Komentář:

Práce je komplexní a umožňuje čtenáři seznámení s tématem v obecné rovině, prakticky vyzkoušet běžné techniky útoků a samozřejmě je detekovat, je tedy dobře použitelná jako opora v praxi.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*

5. Otázky k obhajobě

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

Vzhledem k tomu, že je práce věnována detekci, je zde hezký prostor pro rozšíření / pokračování:
- je frekvence / rychlost zpracování logů použitelná na (téměř) okamžitou reakci na útok?
- jaké reakce považujete za vhodné / realizovatelné?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*100 (A)*

Popis kritéria:
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.

Text hodnocení:

Práce je věnována aktuálnímu tématu - bezpečnosti resp. útokům a jejich detekci v reálném a běžném síťovém prostředí Active Directory. Pokrývá běžné scénáře útoků a pomáhá IT odborníkům uvědomit si jejich relativní snadnost a důležitost jejich detekce a samozřejmě ochrany před nimi. Vzhledem k otevřenosti a kvalitě je dobře připravena na případné pokračování do diplomové práce.

Podpis oponenta práce: