FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Simona Buchovecká
Student:	Bc. Lukáš Kotlaba
Název práce:	Využití technik strojového učení pro detekci útoků v prostředí Active Directory
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	30. května 2021

Hodnotící kritéria

1. Splnění zadání

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

Zadání bylo ve všech bodech bez výhrad splněno.

2. Písemná část práce 95 /100 (A)

Písemná část práce je informačně bohatá a čtivá. V teoretické části student věnuje pozornost všem aspektům nutným k porozumění finálních výsledků - a to jak pozadí fungování Active Directory, popisu vybraných útoků (Password Spraying a Kerberoasting), ale i teorii využití Machine Learning metod pro detekci bezpečnostních incidentů . Následuje praktická část realizace a vyhodnocení, kde student srovnává výsledky diplomové práce a efektivitu machine learning algoritmů, a to i vůči "klasickému" přístupu založeném na signaturách/treshholdu, kterému se student věnoval ve své bakalářské práci.

3. Nepísemná část, přílohy 95 /100 (A)

Přílohy obsahují praktickou implementaci ve formě jupyter notebooků - to je vzhledem k zadání práce adekvátní a odpovídající.

4. Hodnocení výsledků, jejich využitelnost 100 /100 (A)

Zpracovávané téma je aktuální a ukazuje nové možnosti aplikace machine learning technik při detekci incidentů v prostředí Active Directory a možnosti zefektivnění dosud používaných technik. Část výsledků diplomové práce již byla publikovaná (Lukás Kotlaba,

Simona Buchovecká, Róbert Lórencz: Active Directory Kerberoasting Attack: Detection using Machine Learning Techniques. ICISSP 2021: 376-383).

5. Aktivita studenta

▸ [1] **výborná aktivita**
[2] velmi dobrá aktivita
[3] průměrná aktivita
[4] slabší, ale ještě dostatečná aktivita
[5] nedostatečná aktivita

Student byl aktivní a dílčí výsledky průběžně konzultoval.

6. Samostatnost studenta

▸ [1] **výborná samostatnost**
[2] velmi dobrá samostatnost
[3] průměrná samostatnost
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Student pracoval mezi konzultacemi samostatně a přicházel s vlastními nápady k řešení.

Celkové hodnocení 95 /100 (A)

Vzhledem ke komplexnosti zpracovávaného tématu a nutnosti porozumět jak fungování prostředí Active Directory a jednotlivých technik útoků, porozumění logování v prostředí Active Directory, ale i samotným implementovaným machine learning technikám a algoritmům, práci doporučuji k obhajobě. Jelikož téma je zpracováno kvalitně a přináší nové poznatky, což potvrzuje i konferenční publikace dílčích výsledků práce, navrhuji hodnocení výborně - A.

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. 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.

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.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

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.