FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student: Bc. Martin Gajdoš
Oponent práce: Ing. Simona Buchovecká
Název práce: Výběr IDS řešení do firemního prostředí
Obor: Počítačové systémy a sítě

Datum vytvoření: 20. 5. 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:
Diplomová práce splňuje základní požadavky, avšak zejména část testování, která by měla byt těžištěm práce mohla obsahovat více testovacích scénařů; rovněž chybí formálnější a systematičtější přístup pro výběr testovací množiny útoků - ty jsou vybrány spíš náhodně. Minimum pozornosti je věnováno i porovnání efektivity detekcí založených na signaturách a detekci anomálií - ač student tyto možnosti zmiňuje u jednotlivých řešení.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*60 (D)*

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:
Rozsah práce je 59 stran, po odečtení obrázků či tabulek (napr. tab. 4.1; obr 1.1., 1.2) zbytečně umístěných na samostatnou stranu se však rozsah práce blíží spodní hranici počtu stran doporučených pro DP. Text práce by ještě zasloužil revize - jazyk práce je místy neformální, některá tvrzení v práci jsou značně zjednodušená a neberou v úvahu různé možnosti nasazení, topologii a možnosti segmentace sítě (napr. kap. 2.1.1 “Firewall … nijakým spôsobom neobmedzuje dianie v intranete” či “IDS naopak kontroluje aj vnútornú siet’”). Rovněž některé části práce nejsou zcela logicky řazeny (napr. části “OSI sieťový model” a “Program nmap” v kapitole 1.1).

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*80 (B)*

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:
Práce v rámci nepísemné části obsahuje pouze .pcap soubory provedených útoků - vzhledem k charakteru práce to považuji za dostatečné.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*70 (C)*

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:

Na základě výsledku testování bylo implementováno vybrané řešení ve firmě Ataccama Software, práce tedy nalezla praktické uplatnění. Pro širší využití by ale bylo nutno odstranit výše zmíněných nedostatků - zejména výrazně zvětšit testovací množinu útoků a k jejich výběru přistoupit více systematicky - tak aby byly rovnoměrně pokryty různé protokoly a fázy útoků (od skenování přes exploitaci až po exfiltraci dat).

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:

Na základě jakých kritérií byla vybíráná testovací množina útoků?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*65 (D)*

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:

Práci doporučuji k obhajobě a vzhledem k výše zmíněným nedostatkům hodnotím známkou D.

Podpis oponenta práce: