FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Tomáš Ďuračka
Oponent práce:	Ing. Václav Bartoš
Název práce:	Detekce útoků využívajících aplikační protokol HTTP
Obor:	Počítačová bezpečnost

Datum vytvoření: 4. 6. 2018

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	*1=mimořádně náročné zadání,* *2=náročnější zadání,* ***3=průměrně náročné zadání,*** *4=lehčí, ale ještě dostatečně náročné zadání,* *5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Práce se zabývá rešerší nástrojů pro testování (či zneužívání) zranitelností webových aplikací a vývojem modulu pro systém NEMEA, který je schopen takový síťový provoz detekovat. Náročnost práce spočívá především ve studiu množství útoků a dostupných nástrojů a v získání sady detekčních pravidel, implementace modulu je relativně snazší (i když nikoliv triviální). Celkově je tedy zadání středně obtížné.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. 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 splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Zadání bylo v plném rozsahu splněno.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	*1=splňuje požadavky,* ***2=splňuje požadavky s menšími výhradami,*** *3=splňuje požadavky s většími výhradami,* *4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Analýze problému a rešerši útoků a dostupných nástrojů je věnován dostatečně velký prostor a všechny související kapitoly jsou informačně bohaté. Jen kapitola Realizace je až příliš stručná. Modul je sice poměrně jednoduchý a detailní popis kódu není nutný, přesto však mohlo být věnováno více prostoru např. zvolenému formátu souborů s pravidly a jejich reprezentaci v programu.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*100 (A)*

Popis kritéria:
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.

Komentář:
Po věcné stránce je práce zcela v pořádku. Členění do kapitol je logické, text je snadno pochopitelný a celkově se práce dobře čte.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*

5. Formální úroveň práce *95 (A)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3.

Komentář:
Po formální i jazykové stránce mohu vytknout jen několik nepodstatných drobností a překlepů, jinak je práce zcela v pořádku.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*99 (A)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. 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.

Komentář:
Výběr i zpracování studijních materiálů je zcela ukázkový. To se týká jak nejen rešerše a studia problematiky, což bylo jádrem zadání, ale také motivace, v níž student uvádí konkrétní čísla o počtech útoků podložená různými publikovanými zprávami. Dále si také všiml a cituje vědeckou práci, která představuje velmi podobný způsob detekce aplikačních útoků, a byla zveřejněna krátce před termínem odevzdání ZP.
Celkový dojem kazí jen drobná chyba ve formátování citací - některá slova v názvech organizací jsou systémem BibTeX zkrácena, jako by to byla křestní jména autorů.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*85 (B)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Implementovaný modul je plně funkční a pravděpodobně i dostatečně výkonný. Některé části by však přesto šlo velmi jednoduše optimalizovat a získat tak větší propustnost. Dále chybí možnost nastavit cestu k adresáři s pravidly, což aktuálně znemožňuje instalaci modulu do standardních cest (oprava však bude triviální).

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Detekční pravidla vycházejí především z veřejně dostupné databáze, hlavním přínosem je však možnost použití těchto pravidel při analýze toků, což dosud nebylo možné. Z hlediska systému NEMEA je tento modul také velkým přínosem, protože umožní detekovat zcela novou kategorii útoků.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
9. Otázky k obhajobě	

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

Otázky:
* Je propustnost modulu dostatečná pro analýzu veškerého HTTP provozu ze sítě CESNET v reálném čase? (Dle vzorku dat, který jste dostal, by mělo jít určit obvyklé množství HTTP požadavků za sekundu v této síti)

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*95 (A)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Kvalita implementace modulu je spíše průměrná, jádrem práce však byla rešerše útoků a dostupných nástrojů a vytvoření algoritmu a sady pravidel pro jejich detekci - a tato část byla provedena velmi dobře. Navíc výběr studijních materiálů i kvalita výsledného textu jsou vysoce nadprůměrné.

Podpis oponenta práce: