FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Jan Luxemburk
Oponent práce:	Ing. Tomáš Čejka, Ph.D.
Název práce:	Detection of HTTPS brute-force attacks in high-speed computer networks
Obor:	Počítačová bezpečnost

Datum vytvoření: 4. 6. 2020

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:
Analýza šifrovaného provozu je aktuální výzkumná oblast, jejíž důležitost identifikuje i nedávná zpráva ENISA. Do této oblasti přirozeně patří i analýza HTTPS provozu, který aktuálně tvoří většinu internetové komunikace. Práce se zaměřuje na detekci útoků hrubou silou proti webovým serverům, konkr. proti často používaným webovým aplikacím-redakčním systémům. Toto téma je v práci výborně zpracováno, obsahuje velmi slibné výsledky experimentálně vyhodnoceného detekčního mechanismu, jež je součástí odevzdané práce.

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:
Text práce je v angličtině, úroveň jazyka, struktura práce i srozumitelnost jsou na špičkové úrovni. V textu jsem našel jen pár drobných typografickým nedostatků a překlepů.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*92 (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:
Součástí práce jsou zdrojové kódy pomocných skriptů a konfiguračních postupů (jako je např. bruteforce-simulator) pro vytvoření testovacího prostředí, dále pak funkční detekční modul založený na analýze rozšířených flow dat z exportéru Cisco Joy. Na některých místech sice chybí podrobnější komentáře, ale celkově vypadá implementace srozumitelně a čitelně.

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:
V současné době platí, že o šifrovaném provozu se dá zjistit na síťové vrstvě pouze minimální množství informací. Bez razantního zásahu do soukromí uživatelů v podobě proxy a dešifrování provozu (MitM) je nemožné spolehlivě analyzovat provoz a detekovat bezpečnostní hrozby. Tato práce ukazuje (a odkazuje se na relevatní existující zdroje), že je možné s vysokou spolehlivostí detekovat některé bezpečnostní hrozby i v šifrovaném provozu. Tím se tato práce a její přínosy stávají extrémně důležité pro praxi. Navíc se jedná o oblast aktuálního intenzivního výzkumu, takže velmi doporučuji tuto práci a postup publikovat na nějaké prestižní konferenci, případně v nějakém vědeckém časopise.

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:
1) Co přesně znamená "interpenetratable" na str. 59?
2) Za předpokladu výchozího nastavení nástrojů pro hádání hesel hrubou silou, je možné kromě samotné detekce bezpečnostní události určit i nástroj, kterým byl útok generován?
3) Vzhledem k tomu, že běžnými prostředky na síťové úrovni není možné podobné útoky na HTTPS detekovat, je úspěšnost cca 84% velmi vysoká. Podle Fig. 52 však není možné detekovat cca 15% útoků. Je možné úspěšnost detekce do budoucna ještě zvýšit, aniž by došlo ke zvýšení falešně pozitivních hlášení?

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

6. Celkové hodnocení

99 (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 na špičkové úrovni, obsahuje přehledný a dostatečně obsáhlý popis stávajícího stavu a na základě analýzy a experimentů prezentuje nově vyvinutý funkční způsob detekce útoků hrubou silou na autentizaci uživatelů pomocí HTTPS komunikace.
Výstupem závěrečné práce je implementovaný detekční modul, který vznikl na základě experimentů popsaných v práci.
Celkově práce obsahuje velmi málo nedostatků.
Vzhledem k vysoké úspěšnosti detekce a kvalitě zpracování se jedná o excelentní závěrečnou práci, kterou by bylo velice vhodné publikovat.

Podpis oponenta práce: