FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Bc. Jan Luxemburk
Vedoucí: práce:	Ing. Karel Hynek
Název práce:	Detection of HTTPS brute-force attacks in high-speed computer networks
Obor:	Počítačová bezpečnost

Datum vytvoření: 1. 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:

Zadání práce bylo splněno v celém rozsahu. Student nad rámec zadání doplnil program Joy o možnost exportování rozšířených IP toků, čímž značným způsobem ulehčil předpokládané nasazení v síti CESNET2.

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

Písemná část je nadprůměrně rozsáhlá a obsahuje všechny potřebné části. Práce je přehledně a logicky strukturovaná a v průběhu jejího čtení jsem nezaznamenal žádné nedostatky.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*90 (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:

Nepísemná část je velice obsáhlá. Skládá se z nástroje pro tvorbu datové sady, detekčního modulu pro systém Nemea, datové sady a v neposlední řadě upravený exportér IP toků Joy. Drobným nedostatkem je absence podrobnější dokumentace a komentářů přímo v kódu, nicméně spoustu informací je možné vyčíst z přiložených README.

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:

Nejdůležitějším výsledkem práce je modul, který dokáže detekovat útok hrubou silou s vysokou přesností. Předpokládáme jeho nasazení v síti CESNET2. Vytvořená metodika detekce je unikátní a ve své přesnosti převyšuje ostatní relevantní práce. Z toho důvodu je také plánováno ji odpublikovat na odborné konferenci.

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 5:*
5. Aktivita a samostatnost studenta	5a: ***1=výborná aktivita,*** *2=velmi dobrá aktivita,* *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 5b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
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 (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:

Student byl velice samostatný a aktivní. Na konzultace přicházel vždy perfektně připraven.

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 na mě působí velice dobrým dojmem. Student pečlivě nastudoval předchozí práce zabývající se detekcí HTTPS útoků hrubou silou na síťové úrovni. Na základě získaných informací navrhl metodu, která veškeré předchozí práce překonává. Student tuto metodu implementoval ve formě modulu pro systém NEMEA. Text práce perfektně dokumentuje vytvořenou metodu a poslouží jako základ k napsání vědecké publikace. Jako vedoucí práce jsem byl nad míru spokojen. Z výše popsaných důvodů hodnotím práci velmi vysoko a doporučuji komisi, aby tuto práci navrhla na cenu děkana.

Podpis vedoucího práce: