FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student: Maxmilián Tomáš
Vedoucí: práce: Ing. Tomáš Čejka
Název práce: Rozšíření reputační databáze o informace z Passive DNS
Obor: Bezpečnost a informační technologie

Datum vytvoření: 6. 6. 2018

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:
Cílem práce bylo vytvořit systém pro ukládání historie informací z DNS zón, které se posílají v rámci síťového provozu. V rámci práce byl tento systém vytvořen a podařilo se ho napojit na existující systém, který vyhodnocuje nahlášené bezpečnostní události.

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:
Písemná část práce není v dobrém stavu. Text obsahuje značné množství překlepů, z nichž mnohé by bylo možné odstranit použitím spellcheckeru. Dále text obsahuje gramatické chyby. Po typografické stránce jsou v práci mnohé nedokonalosti.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*85 (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:
Výsledkem práce je funkční a otestovaná softwarová implementace systému Passive DNS. Zdrojové kódy jsou napsané přehledně, avšak chybí v nich komentáře a licence. Součástí odevzdané práce je instalační skript, který umožňuje zprovoznit systému na distribuci Debian.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*99 (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:

Výsledky práce jsou využitelné v praxi pro ukládání historického mapování IP adres a doménových jmen. Vytvořený systém je nasazen na serveru sdružení CESNET, kde v současné době zpracovává a ukládá data z rekurzivních DNS serverů, které jsou sdružením rovněž provozované. Během práce se podařilo propojit systém Passive DNS a systém NERD (reputační databáze). Na základě toho jsou informace z Passive DNS již využívány jako součást informací o evidovaných potenciálně škodlivých entitách.

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 se aktivně zapojil do týmu, který působí na fakultě, a v rámci své bakalářské práce navázal kontakty se specialisty ze sdružení CESNET, kteří se starají o provoz DNS serverů a monitorování vnitřní infrastruktury. Student se pravidelně účastnil schůzí týmu, na které vždy přišel připraven.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*75 (C)*

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:

Výsledkem této bakalářské práce je vytvořený funkční a otestovaný systém Passive DNS, který již byl nasazen na produkčním serveru sdružení CESNET. Ukládané informace obohacují výsledky systému Reputační databáze (tzv. NERD), která se ve sdružení CESNET rovněž vyvíjí. Aktuální verze systému Passive DNS umožňuje do budoucna výzkum například v oblasti detekce podezřelých doménových jmen. Celkový dojem práce bohužel kazí nedostatky v písemné části práce, která by potřebovala jazykovou korekturu.

Podpis vedoucího práce: