ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK VEDOUCÍHO ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Detekce DNS tunelování**
Jméno autora:	**Jan Karsch**
Typ práce:	bakalářská
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra počítačů
Vedoucí práce:	Ivan Nikolaev
Pracoviště vedoucího práce:	Cisco Systems

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **průměrně náročné**

Hodnocení náročnosti zadání závěrečné práce.

Práce se zabývá detekcí DNS tunelů, které mohou být útočníkem využity ke skrytému přenosu dat nebo komunikaci s Command and Control (C&C) serverem.

Splnění zadání **splněno**

Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Zadání práce splněno v plném rozsahu.

Zvolený postup řešení **správný**

Posuďte, zda student zvolil správný postup nebo metody řešení.

V první fázi práce student provedl řadu experimentů, ve kterých vytvořil různé typy DNS tunelů pomocí stávajících programů pro DNS tunely. Poté student použil data z experimentů a data z reálného provozu pro vytvoření simulované sítě, kde řada uživatelů provozuje DNS tunely. Tato simulovaná síť byla následně použita pro trénování a evaluaci klasifikátorů pomocí příznaků navržených studentem.

Odborná úroveň **A - výborně**

Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

Student se seznámil s existujícími metodami pro detekci DNS tunelů a kriticky zhodnotil jejich výhody a nevýhody. Data získaná z experimentů byly využity účelným způsobem pro vývoj detekčního algoritmu.

Formální a jazyková úroveň, rozsah práce **C - dobře**

Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.

Práce je dobře typograficky zpracována. Tabulky a grafy jsou použité vhodným způsobem, který přidává k celkovému obsahu na srozumitelnosti. Bohužel nižší úroveň angličtiny snižuje celkový dojem z práce. Text obsahuje velké množství gramatických chyb a nesprávných formulací, což citelně zhoršuje čitelnost a srozumitelnost obsahu.

Výběr zdrojů, korektnost citací **A - výborně**

Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. 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.

Student provedl obsáhlou rešerši, ve které zjistil a kriticky zhodnotil existující metody pro detekci DNS tunelů. Student také prozkoumal existující software pro tvorbu DNS tunelů a použil je ve svých experimentech. Veškeré zdroje jsou v práci důkladně citované.

Další komentáře a hodnocení
Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.
Vložte komentář (nepovinné hodnocení).

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

Práce se zabývá návrhem detekční metody pro DNS tunely, které mohou být útočníkem využity ke skrytému přenosu dat nebo komunikaci s Command and Control (C&C) serverem. V práci byla provedena rešerše ohledně existujících metod pro detekci DNS tunelů a jejich výhody a nevýhody jsou dobře zhodnoceny. Dále byla provedena řada experimentů se softwarem pro DNS tunely, které byly následně využity při vytváření detekční metody. Student zvolil správný postup, který v experimentální části vykazuje výborné výsledky.

Práce je dobře typograficky zpracována. Bohužel nižší úroveň anglického jazyka ubírá na srozumitelnosti. I přesto je navrhovaná metoda detekce dobře popsaná s prokazatelným přínosem do oblasti síťové bezpečnosti.

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **B - velmi dobře.**

Datum: 4.6.2018 Podpis: