POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**DNS tunelling detection**
Jméno autora:	**Jan Karsch**
Typ práce:	bakalářská
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra počítačů
Oponent práce:	Mgr. Jan Kohout
Pracoviště oponenta práce:	FEL ČVUT

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **průměrně náročné**

Hodnocení náročnosti zadání závěrečné práce.

Náročnost zadání odpovídá bakalářské práci.

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 bylo splněno.

Zvolený postup řešení **správný**

Posuďte, zda student zvolil správný postup nebo metody řešení.

Postup řešení byl zvolen správně, jednotlivé kroky na sebe logicky navazují. Metodika experimentů je v zásadě správná, ale v práci chybí důkladnější zhodnocení výsledků klasifikace.

Odborná úroveň **A - výborně**

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

Autor práce se dobře orientuje v dané problematice i v přípravě a návrhu experimentů.

Formální a jazyková úroveň, rozsah práce **B - velmi dobře**

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

Po typografické stránce je práce na dobré úrovni, bohužel jazyková úroveň je horší. Neobratné formulace, popřípadě i jazykově nesprávné, místy až komplikují srozumitelnost textu.

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.

Zdroje jsou správně citovány, dostupné zdroje byly vhodně využity.

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).

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

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 zajímavým tématem detekce DNS tunelů, které mohou být zneužity pro skrytí komunikace malwaru. Existující nástroje pro DNS tunelování jsou v práci dobře popsány, návrh experimentů je také vhodný.

Práci bych vytkl horší jazykovou úroveň, která místy komplikuje čitelnost. Bylo by též vhodné kritičtěji zhodnotit a diskutovat výsledky jednotlivých klasifikátorů, především náhodných lesů, kde vzhledem k velmi vysoké přesnosti na testovacích datech vzniká podezření, zda tak dobrý výsledek klasifikace nebyl dosažen především díky tomu, že pozitivní a negativní vzorky pocházely z různých zdrojů.

Otázky:

Byla v experimentech testována i schopnost klasifikátoru identifikovat DNS tunely, které byly vytvořeny pomocí tunelovacího nástroje, který ale nebyl zastoupen v trénovacích datech klasifikátoru?

Je možné posoudit, jak velký vliv na výsledky experimentů má skutečnost, že pozitivní vzorky byly vytvořeny uměle a do reálného provozu přimíchány?

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

Datum: 31.5.2018 Podpis: