ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	Identifikace skupin útočníků pomocí minimálních honeypotů
Jméno autora:	**Bc. Miroslav Hanák**
Typ práce:	diplomová
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra měření
Oponent práce:	Ing. Tomáš Čejka, Ph.D.
Pracoviště oponenta práce:	KČN, FIT ČVUT v Praze

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání — náročnější

Hodnocení náročnosti zadání závěrečné práce.

Téma práce je rozsáhlé, neboť zahrnuje náročnou problematiku návrhu a vývoje obtížně rozpoznatelných honeypotů. Zároveň se práce věnuje sběru dat z velkého množství honeypotů a způsobům analýzy dat z honeypotů.

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.

Výsledkem práce je sada vyvinutých/rozšířených aplikací, které slouží jako honeypoty a infrastruktura sběru dat z nich. Hlavním přínosem práce je podpora protokolů (HTTP, FTP, SMTP), které nebyly obsaženy v původním řešení, ze kterého autor vychází. Ačkoliv název práce cílí na identifikaci skupin útočníků, této problematice se bohužel autor v textu věnuje pouze teoreticky na konci (rešerší existujících shlukovacích algoritmů). Vzhledem ke značnému rozsahu návrhové a implementační části práce, která byla nezbytná pro sběr potřebných dat, je pochopitelné, že se nepodařilo část analýzy dat více rozpracovat.

Zvolený postup řešení — správný

Posuďte, zda student zvolil správný postup nebo metody řešení.

Zvolený postup řešení vedl ke splnění zadání a k vytvoření rozsáhlých softwarových výsledků, které byly důkladně otestovány a připraveny k praktickému nasazení ve směrovačích Turris. Výsledkem práce je proto výborně zpracované inženýrské dílo.

Odborná úroveň — B - velmi dobře

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

Text práce obsahuje chyby, které mohou vést ke zmatení čtenáře a nebo v horším případě k chybné implementaci (např. Table 4.1, PASS / PASV). Zdá se, že zdrojové kódy jsou v pořádku, doporučoval bych do souborů uvést autora, aby bylo zřejmé i bez textu závěrečné práce, které části byly původní a které jsou nově vytvořené.

Formální a jazyková úroveň, rozsah práce — C - dobře

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

Práce je zpracována v anglickém jazyce, rozsah práce splňuje požadavky. Text práce obsahuje řadu překlepů a gramatických chyb, přičemž řadu z nich by jistě bylo možné opravit pouhou automatickou strojovou kontrolou (spellchecker). Odkazy na sekce/tabulky apod. nejsou řešeny přehledně a v papírové podobě (bez hypertextových odkazů) musí být pro čtenáře často velice obtížné se zorientovat, na co se vlastně autor odkazuje.

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

Výběr zdrojů, korektnost citací C - dobře

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.

Práce obsahuje dostatečné množství citovaných zdrojů, avšak citace nejsou mnohdy použity přehledně a srozumitelně v textu. Zaznamenal jsem duplicitu zdrojů, citace [6] a [9].

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.

Odevzdaná práce je celkově na dobré úrovni, navržené a implementované softwarové části byly dostatečně otestovány a velice kladně hodnotím důraz autora na praktickou nasaditelnost a použitelnost v reálném prostředí. Naproti tomu text práce obsahuje řadu jazykových a typografických nedostatků, které celkový dobrý dojem kazí.

Otázky:
1) Probíhala nějaká kontrola/vyhodnocení IP adres připojujících se k reálným honeypotům, např. pomocí existujících veřejných „blacklistů“? Pokud ano, jaký podíl útočníků nebyl evidován na blacklistech?
2) Na konci Sekce „15.2 Data Analyses“ (str. 79) autor píše, že výsledky shlukovacích algoritmů nad nasbíranými daty vypadají slibně. Jakých výsledků bylo v praxi dosaženo? Podařilo se najít a ověřit nějakou skupinu podobně se chovajících útočníků na základě analýzy dat z honeypotů?

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.

Předloženou závěrečnou práci hodnotím klasifikačním stupněm B - velmi dobře.

Datum: 24.8.2020 Podpis: