Posudek oponenta diplomové práce

Student: Štěrba Ondřej, Bc.
Téma: Obfuskace anomálií a bezpečnostních incidentů při provozu DNS (id 18979)
Oponent: Kováčik Michal, Ing., UPSY FIT VUT

1. **Náročnost zadání** — **obtížnější zadání**
   Zadání je obtížnějšího charakteru. V prvém radě musel student nastudovat problematiku detekce síťových anomálií v DNS provozu a zanalyzovat jednotlivé přístupy k detekci. Součástí výsledného řešení je také navržení protokolu botnetu pro potřeby práce a navržení samostatných obfuskačních technik.
2. **Splnění požadavků zadání** — **zadání splněno**
   Implementace vlastního botnetu může být považována za práci nad rámec zadání, jelikož zadání s ní nepočítá.
3. **Rozsah technické zprávy** — **je v obvyklém rozmezí**
   Rozsah technické správy je v obvyklém rozmezí.
4. **Prezentační úroveň předložené práce** — **85 b. (B)**
   Práce je dobře strukturovaná. Členění jednotlivých kapitol je logické a dobře na sebe navazují. Výsledný text je dobře čitelný a logicky na sebe navazuje. Práce je velmi dobře pochopitelná a názorná.
5. **Formální úprava technické zprávy** — **85 b. (B)**
   Práce je typograficky na velmi dobré úrovni. Neobsahuje téměř žádné chyby a působí velmi odladěně. Student vhodně využívá prostředky sázení textu a zvýrazňování.
6. **Práce s literaturou** — **90 b. (A)**
   Práce s literaturou je nadstandardní. Student využil velké množství zdrojů, menší část je elektronického charakteru. Použitá literatura byla vhodně zvolena.
7. **Realizační výstup** — **90 b. (A)**
   Výslední aplikace je dobré úrovni, no vzhledem na složitější problematiku a konstrukce by zdrojovému kódu pomohlo vhodnější komentování. Implementace zahrnuje řešení obfuskace nelegitimního provozu pomocí DNS a také C&C server pro komunikaci.
8. **Využitelnost výsledků**
   Práce je přínosem do vědecké sféry. Představuje dobrý základ pro její další pokračování a po úpravách je publikovatelná.
9. **Otázky k obhajobě**
   Uvažovali jste nad generováním další komunikace mezi serverem a klientem, která by neměla žádnou komunikační hodnotu pro dvojici, no samotnou komunikaci by ještě blíže posunula reálnému provozu a ještě víc by tak znemožnila detekci? Bylo by tohle řešení reálné? Přineslo by nějaké komplikace?
10. **Souhrnné hodnocení** — **90 b. výborně (A)**
    Student vykonal velké množství práce už při analýze problematiky a návrhu celého výsledného systému. Výsledné řešení je funkční a demonstruje možnost obfuskace nelegitimní DNS komunikace. Z mého pohledu se jedná o nadprůměrnou práci zejména z pohledu rozsahu práce, kvality výstupu i technické zprávy a také prezentovaných výsledků. Vzhledem k náročnosti zadání navrhuji hodnocení A (výborně).

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 7. června 2016

.....
podpis