Posudek práce

předložené na Ústavu aplikované informatiky Přírodovědecké fakulty JU

❑ posudek vedoucího ☑ posudek oponenta
☑ bakalářské práce ❑ diplomové práce

Autor/ka: Dominik Marek

Název práce: Detekce červů a botnetů pomocí volně šiřitelného software

Studijní obor: Aplikovaná Informatika

Datum odevzdání: 29. 4. 2011

Jméno a tituly vedoucího/oponenta: Ing. Rudolf Vohnout

Pracoviště: Ústav aplikované informatiky

Kontaktní e-mail: rudolf.vohnout@prf.jcu.cz

Odborná úroveň práce:
☑ vynikající ❑ velmi dobrá ❑ průměrná ❑ podprůměrná ❑ nevyhovující

Věcné chyby:
☑ téměř žádné ❑ vzhledem k rozsahu přiměřený počet ❑ méně podstatné četné ❑ závažné

Výsledky:
☑ originální ❑ původní i převzaté ❑ netriviální kompilace ❑ citované z literatury ❑ opsané

Rozsah práce:
☑ veliký ❑ standardní ❑ dostatečný ❑ nedostatečný

Grafická, jazyková a formální úroveň:
❑ vynikající ❑ velmi dobrá ☑ průměrná ❑ podprůměrná ❑ nevyhovující

Tiskové chyby:
❑ téměř žádné ☑ vzhledem k rozsahu a tématu přiměřený počet ❑ četné

Celková úroveň práce:
❑ vynikající ☑ velmi dobrá ❑ průměrná ❑ podprůměrná ❑ nevyhovující

Slovní vyjádření, komentáře a připomínky vedoucího/oponenta:

Předložená práce zpracovává jedno ze zásadních témat počítačové bezpečnosti. Autor přistoupil k této problematice velmi ze široka, avšak zodpovědně. V úvodní části jsou autorem popsány možnosti detekce a analýzy síťových útoků a tím pádem také z nich vyplývajícího nutného zabezpečení systémů a aplikací. V praktické části autor nejprve demonstruje instalaci a konfiguraci „honeypotu" a poté analyzuje několika metodami získané výsledky nasbírané za relativně rozumné časové období. Velkým překvapením jsou také zjištěné bezpečnostní chyby v samotné univerzitní síti. Na začátku praktické části je také vidět, že se autor práci, resp. přípravě na ni, opravdu věnoval (viz. kapitoly o zjištěných chybách v programu a jejich řešení se samotnými vývojáři) a časově ji nepodcenil. Výsledky a jejich analýza jsou v této práci zcela zásadním elementem určujícím její nespornou kvalitu.

Výhrady k práci mám pouze k jejímu rozsahu (dle mého názoru 35 stran řádkováním 1 bez toho aby kapitoly začínaly na nových stranách je na BP příliš). V některých pasážích je práce zcela zbytečně natahována (např. postup instalace apod. patří spíše do příloh než do hlavního textu) a spíše než takto obsáhlý úvod do problematiky by bylo vhodnější zvětšit „slovníček pojmů", který na práci takovéhoto rozsahu pojmů opravdu mnoho neobsahuje. Dále práce s literaturou není nejšťastnější a v úvodu zcela chybí metodika! Dále mi v práci chybí nějaký graf (např. časový průběh zachycující jaké dny v týdnu nebo jakou hodinu byly útoky nejčetnější apod.).

I přes výše uvedené výhrady díky originalitě tématu a praktickému přínosu hodnotím práci jako celek stupněm *výborně* a doporučuji ji k obhajobě.

Případné otázky při obhajobě a náměty do diskuze:

1) Proč byl zvolen pro „sběr dat" právě a pouze *honeypot Dionaea* a ne třeba dva různé honeypoty ve dvou různých sítích (na stejně dlouhé časové období) pro následné vzájemné porovnání výsledků?

Práci
☑ doporučuji
☐ nedoporučuji
uznat jako ~~diplomovou~~/bakalářskou.

Navrhuji hodnocení stupněm:
☑ výborně ☐ velmi dobře ☐ dobře ☐ neprospěl/a

Místo, datum a podpis vedoucího/oponenta:

České Budějovice, 18. 5. 2011