**POSUDEK OPONENTA DIPLOMOVÉ PRÁCE**

|  |  |  |  |
| --- | --- | --- | --- |
| **Student:** | **Bc. Jan Bobák** | **Oponent:** | **Ing. Martin Spurný** |
|  |  |  |  |
| Studijní program: |  |
| Studijní obor: |  |
| Akademický rok: |  |  |  |
|  |  |  |  |
| Téma diplomové práce: | **Implementace aktivních protiopatření pro honeypoty** |

**Hodnocení práce:**

Cílem diplomové práce Bc. Jana BOBÁKA na téma „Implementace aktivních protiopatření pro honeypoty“ bylo navrhnout možnosti nasazení prvků pro detekci a lokalizaci útočníků v IT infrastruktuře s využitím honeypotů, implementovat firewall, charakterizovat varianty útoků s analýzou možností získání informací o nich a vytvořit protiopatření s popisem pro jejich odvrácení.

Diplomová práce se v teoretické části práce zabývá základním popisem honeypotů s vhodností použití v praxi a popisem bezpečnosti linuxových serverů formou různých forem útoku s uvedením jednotlivých druhů útočníků. Dále se zabývá penetračním nástrojem BeEF a návrhem implementace firewallu. Teoretická část diplomové práce je zpracována srozumitelně.

Praktická část diplomové práce se věnuje tvorbě firewallu s použitím nástroje iptables a jeho nasazením mezi jednotlivé segmenty sítě, včetně provedení testu konfigurace. Dále se zabývá implementací nástrojů pro honeypot, umožňující vystopování útočníka s možností znemožnit mu další přístup. Nakonec se zabývá názorným provedením testu útoku na honeypot s ověřením, zda navržené systémy fungují a následným vyhodnocením získaných informací. Tato část diplomové práce je zpracována důkladně.

Po formální stránce je práce na velmi dobré úrovni, s minimálním obsahem pravopisných chyb a s přiměřeným množstvím překlepů. Práce je zpracována přehledně s logicky navazujícími kapitolami. V závěru práce autor srozumitelně shrnuje zjištěné poznatky. V diplomové práci autor uvádí přiměřené množství obrázků k objasnění popisované problematiky. Seznam literatury zahrnuje odpovídající množství relevantních zdrojů. Všechny body zadání práce byly splněny.

Diplomant prokázal velmi dobré znalosti daného tématu a orientaci v prostředí linuxových operačních systémů. Práce přináší cenné rady v oblasti využití vybraných aktivních protiopatření, majících za úkol ochránit webové servery proti všem typům útočníků.

Při obhajobě prosím o zodpovězení následující otázky:

Ve své diplomové práci často používáte pojmy „hacker“, „hackeři“. Definujte prosím pojem „cracker“ a vysvětlete rozdíl mezi tímto pojmem a pojmem „hacker“.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Celkové hodnocení práce:** |  |  |  |  |  |  |

Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

|  |
| --- |
| **Předloženou diplomovou práci**  **k obhajobě a navrhuji hodnocení****.****V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.** |

Datum 27.5.2014 Podpis oponenta diplomové práce