Univerzita
Pardubice
Fakulta elektrotechniky
a informatiky

Posudek oponenta diplomové práce

Autor diplomové práce: **Jan Januš, Bc.**

Název diplomové práce: **Problematika Host Intrusion Prevention System**

1. **Zadání odborného problému a použití metod řešení v rámci diplomové práce**

   Cílem diplomové práce bylo popsat principy a možnosti nasazení HIPS v prostředí podnikové sítě včetně návrhu implementace a provedení zátěžových testů. Teoretická část práce by měla být použita na rozšíření wiki upce.

2. **Konkrétní výsledky diplomové práce**

   V teoretické části autor popsal principy fungování systémů IDPS a jejich variant NIDPS, WIDPS, NBA a HIDPS. V praktické části pak autor otestoval dvě vybraná řešení HIDPS: OSSEC a Deep Security. Tato řešení autor nasadil ve dvou různých operačních systémech - Windows a Linux. Autor provedl zátěžové testy zaměřené na ovlivnění operačního systému implementace HIDPS.

3. **Prokázání správnosti navrženého řešení problému**

   Autor popsal principy fungování systémů IDPS dostatečně do hloubky tak, aby se text po určitých úpravách dal použít pro wiki upce. Autor pro zpracování použil dostatečný počet literárních zdrojů, ale převážně čerpal pouze ze dvou hlavních zdrojů (Scarfone, Hudec). V praktické části autor otestoval vybrané produkty HIDPS a změřil jejich průměrný vliv na výkon operačního systému. Autor tento vliv zkoumal při "klidovém stavu", kdy systémy HIDPS nebyly pod žádným útokem, ale mohly provádět aktualizace či naplánované testy. Na základě výsledků autor navrhl nasazení systémů HIDPS v prostředí podnikové sítě.

4. **Splnění cílů diplomové práce**

   Požadované cíle diplomové práce byly splněny.

5. **Kvalita textu diplomové práce**

   Kvalita textu diplomové práce je průměrná. Text obsahuje občasné překlepy ("Sansung", str. 57), chyby způsobené automatickými opravami ("Senzors", str. 19) opakování slov ("se portů se", str. 27) nebo chybějící odkaz ("Chyba! Nenalezen zdroj odkazů", str. 51) a některé další chyby.

6. **Připomínky a dotazy k diplomové práci**

   Na straně 37 autor zmiňuje příklad detekce odlišnosti v šifrování, kdy koncová stanice použije WEP2 místo organizací definovaného WEP. Jedná se opravdu o problém, když stanice použije silnější typ šifrování, než je společností vyžadováno? Jedná se o příklad z praxe (nevhodnost WEP šifrování)?

   Na straně 60 autor popisuje použitý OS Ubuntu 15.04 s tím, že bývá označován jako Kubuntu. Jedná se tedy o distribuci Ubuntu, nebo Kubuntu?

Doporučení práce k obhajobě: **ano**

Navržený klasifikační stupeň: **velmi dobře**

Posudek vypracoval:

Jméno, tituly: Filip Holík, Ing.
Zaměstnavatel: Univerzita Pardubice, FEI

V Pardubicích dne: 3. 9. 2015 Podpis: