Posudek práce

předložené na Ústavu aplikované informatiky Přírodovědecké fakulty JU

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

Autor/ka: Jan Houška

Název práce: Reakce na incidenty a forenzní analýza

Studijní obor: Aplikovaná informatika

Datum odevzdání: 9. 12. 2012

Jméno a tituly vedoucího/oponenta: Ing. Jiří Jelínek, CSc.

Pracoviště: Ústav aplikované informatiky

Kontaktní e-mail: jjelinek@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:
V první části se autor zabývá teoretickými východisky reakce na incidenty. Zde měl autor v souladu s cíli práce věnovat pozornost i možnostem řešení různých typů útoků, což provedl pouze částečně. V dalších částech je popsána obecně používaná a známá metodika reakce na incident a je charakterizován pojem digitální forenzní analýza.
Autor se dále věnuje postupu zajištění stop, přičemž již v této části (a v částech následujících) se omezuje pouze na jeden operační systém napadeného počítače (Linux), který však není tím nejrozšířenějším. Popsány jsou i vybrané nástroje pro forenzní analýzu.
V kapitole 8 autor navrhuje vlastní metodiku reakce na incident pro konkrétní OS, přičemž obecná metodika je dána a jde pouze o její upřesnění.
V kapitole 9 autor popisuje jednoduchý simulovaný útok (prolomení slabého hesla pomocí SSH přístupu) na zvolený stroj a způsob reakce na něj podle výše uvedené vlastní metodiky. V části věnované vyšetřování incidentu jsou některé body popsány jen velmi stručně a práce se v souladu s cíli zaměřuje především na získání dat a ne na jejich analýzu. V závěru kapitoly je nutno s autorem polemizovat, zda uvedená metodika skutečně může sloužit k odhalování základních druhů útoků.
Závěr práce je velmi stručný a v textu je řada formálních chyb. Náplň práce rámcově odpovídá cílům v ní uvedeným, přičemž některé je nutno považovat za splněné pouze částečně (řešení útoků, úzké zaměření na jeden OS).

Případné otázky při obhajobě a náměty do diskuze:

1. **Proč se autor zaměřil právě na OS Linux a jeho konkrétní verzi, jestliže nejrozšířenějším systémem je MS Windows?**
2. **Jaké další možnosti průniku do systému přicházejí v úvahu kromě prolomení hesla?**
3. **V čem autor vidí svůj osobní přínos k dané problematice?**

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

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

Místo, datum a podpis vedoucího/oponenta: České Budějovice 14. ledna 2013