

# 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. Jaroslav Kothánek, Ph.D.

Pracoviště:                                  Ústav aplikované informatiky

Kontaktní e-mail:                          jkothanek@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:**

Autor se zabývá ve své práci řešením reakce na bezpečnostní incidenty a na následnou forenzní analýzu některých známých druhů incidentů. Autor ve své práci volí logický postup. Ve své práci se zabývá popisem nejznámějších bezpečnostních incidentů, vytváří metodologii reakce na incidenty a v poslední řadě se zabývá forenzní analýzou dat za účelem vypátrání útočníka. Autor ve své práci ukazuje svou vysokou odbornou znalost nejen na úseku bezpečnostních incidentů OS Linux, ale též schopnost řešit celou záležitost v celém kontextu tedy forenzní analýzy. Práce má vysokou odbornou úroveň a to i vzhledem k tomu, že se jedná o bakalářskou práci. Ve své práci se však autor, patrně omylem, autor dopouští malé nepřesnost, kde uvádí, že se nedoporučuje využívat tzv. Hardwarových blokátorů při zajišťování dat. Autor splnil veškeré zadání a vzhledem k vysoké odborné úrovni hodnotím práci výborně.

**Případné otázky při obhajobě a náměty do diskuze:**

1. Ve své práci uvádíte, že se nedoporučuje využívat hardwarové blokátory, můžete říci z jakých důvodů

**Práci** doporučuji nedoporučuji

uznat jako diplomovou/bakalářskou.

**Navrhuji hodnocení stupněm:** výborně  velmi dobře  dobře  neprospěl/a

Místo, datum a podpis vedoucího/oponenta:

České Budějovice, 4.1.2013, Ing. Jaroslav Kothánek, Ph.D.