

# Posudek práce

předložené na Přírodovědecké fakultě JU

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> posudek vedoucího | <input type="checkbox"/> posudek oponenta |
| <input checked="" type="checkbox"/> bakalářské práce  | <input type="checkbox"/> diplomové práce  |

Autor/ka: **Jan Soubusta**  
Název práce: **Vizualizace síťového provozu s ohledem na bezpečnostní události**  
Studijní program a obor: Aplikovaná informatika  
Rok odevzdání: 2020

Jméno a tituly vedoucího: Ing. Petr Břehovský  
Pracoviště: Ústav aplikované informatiky  
Kontaktní e-mail: PBrehovsky@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:**

Nosnou myšlenkou této práce bylo ověřit, zda je možné použít relativně levné metody vizualizace vybraných síťových a provozních parametrů k detekci útoku.

Detekce v tomto případě nespočívá ve složitých automatizovaných metodách, ale ve vizuálním vyhodnocení grafických reprezentací hodnot relevantních parametrů. Autor vytvořil prostředí, které umožňuje provádět útoky, monitorovat a vizualizovat provozní parametry, na které mohou mít útoky vliv. Bylo ověřeno, že některé útoky lze detekovat spolehlivě, ale některé se projevují v parametrech, jejichž sběr dané řešení nepodporuje. Autor se musel seznámit s řadou síťových útoků, musel identifikovat jejich projevy, útoky prakticky realizovat a navrhnout a implementovat řešení pro generování, sběr a vizualizaci relevantních parametrů. Oceňuji vysoce samostatnou práci autora ve všech fázích projektu.

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

Myslíte si, že použité metody mohou prakticky sloužit k identifikaci útoků na výpočetní systémy?

Jak by bylo nutné systém dále rozvíjet, aby umožňoval identifikovat i ve stávající práci neodhalené útoky?

### **Práci**

doporučuji

nedoporučuji

uznat jako bakalářskou.

### **Navrhuji hodnocení stupněm:**

výborně  velmi dobře  dobře  neprospěl/a

### **Místo, datum a podpis vedoucího/oponenta:**

V Českých Budějovicích dne 3. července 2020

.....