

# Hodnocení vedoucího závěrečné práce

České vysoké učení technické v Praze

Fakulta informačních technologií

**Student:** Otto Hollmann  
**Vedoucí práce:** Ing. Tomáš Čejka  
**Název práce:** Detekce síťových útoků typu Denial of Service  
**Obor:** Teoretická informatika

**Datum vytvoření:** 12. 6. 2017

<b>Hodnotící kritérium:</b> <b>1. Náročnost a další komentář k zadání</b>	<b>Způsob hodnocení - následující škálou 1 až 5:</b> 1=mimořádně náročné zadání, 2=náročnější zadání, <b>3=průměrně náročné zadání,</b> 4=lehčí, ale ještě dostatečně náročné zadání, 5=nedostatečně náročné zadání
<b>Popis kritéria:</b> Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.) <b>Komentář:</b> Cílem práce bylo vytvořit detekční modul implementující jednoduchý algoritmus pro detekci zvýšení objemu provozu v čase. Tento modul je určen k detekování volumetrických útoků DDoS.	
<b>Hodnotící kritérium:</b> <b>2. Splnění zadání</b>	<b>Způsob hodnocení - následující škálou 1 až 4:</b> <b>1=zadání splněno,</b> 2=zadání splněno s menšími výhradami, 3=zadání splněno s většími výhradami, 4=zadání nesplněno
<b>Popis kritéria:</b> Posuďte, zda předložená ZP splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků. <b>Komentář:</b> Výsledkem práce je funkční prototyp detekčního modulu.	
<b>Hodnotící kritérium:</b> <b>3. Rozsah písemné zprávy</b>	<b>Způsob hodnocení - následující škálou 1 až 4:</b> 1=splňuje požadavky, <b>2=splňuje požadavky s menšími výhradami,</b> 3=splňuje požadavky s většími výhradami, 4=nesplňuje požadavky
<b>Popis kritéria:</b> Zhodněte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. <b>Komentář:</b> Rozsah předložené práce je přiměřený. Slabou částí práce je nedostatečný popis implementovaného algoritmu.	
<b>Hodnotící kritérium:</b> <b>4. Věcná a logická úroveň práce</b>	<b>Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):</b> 85 (B)
<b>Popis kritéria:</b> Posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. <b>Komentář:</b> Práce je víceméně v pořádku. Struktura textu by se dala vylepšit, místo informačně bohatého teoretického úvodu by bylo vhodné zaměřit se na podrobnější popis vlastní práce a výsledků.	
<b>Hodnotící kritérium:</b> <b>5. Formální úroveň práce</b>	<b>Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):</b> 90 (A)
<b>Popis kritéria:</b> Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3. <b>Komentář:</b> Po jazykové a typografické stránce se práce zdá být v pořádku.	
<b>Hodnotící kritérium:</b> <b>6. Práce se zdroji</b>	<b>Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):</b> 90 (A)
<b>Popis kritéria:</b> Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.	

Komentář:

Práce obsahuje dostatečné množství relevantních zdrojů.

Hodnotící kritérium:

Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):

### 7. Hodnocení výsledků, publikační výstupy a ocenění

85 (B)

Popis kritéria:

Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:

Téma práce patří mezi aktuální oblasti výzkumu a vývoje. Výsledkem práce je funkční modul schopný zpracovat data z páteřní sítě a zaměřuje se na detekci specifického typu útoků. Pro publikaci výsledků je nezbytné podrobněji popsat implementovaný algoritmus a provést rozsáhlejší experimenty.

Hodnotící kritérium:

Způsob hodnocení - nehodnotí se

### 8. Komentář o využitelnosti výsledků

Popis kritéria:

Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:

Výsledky práce jsou využitelné v praxi. V současné době je modul nasazený na produkčním kolektoru, který analyzuje provoz hraničních linek sítě CESNET2.

Hodnotící kritérium:

Způsob hodnocení - následující škálou 1 až 5:

### 9. Aktivita a samostatnost studenta v průběhu řešení

9a:

1=výborná aktivita,

**2=velmi dobrá aktivita,**

3=průměrná aktivita,

4=slabší, ale ještě dostatečná aktivita,

5=nedostatečná aktivita

9b:

1=výborná samostatnost,

**2=velmi dobrá samostatnost,**

3=průměrná samostatnost,

4=slabší, ale ještě dostatečná samostatnost,

5=nedostatečná samostatnost

Popis kritéria:

Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (9a). Posuďte schopnost studenta samostatně tvůrčí práce (9b).

Komentář:

Student pracoval aktivně, samostatně a průběžně.

Hodnotící kritérium:

Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):

### 10. Celkové hodnocení

85 (B)

Popis kritéria:

Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:

Výsledkem této práce je open source detekční modul, který je dostupný celosvětové komunitě v repozitáři github.com.

Vyvinutý modul je součástí systému NEMEA pro analýzu síťového provozu a detekci anomálií. Předložený text práce by bylo vhodné doplnit o podrobnější popis implementovaného algoritmu.

Podpis vedoucího práce: