



# Hodnocení vedoucího závěrečné práce

**Student:** Bc. Petr Beneš  
**Vedoucí práce:** Ing. Jiří Chludil  
**Název práce:** Využití softwaru Suricata v cloudovém systému  
**Obor:** Počítačová bezpečnost

**Datum vytvoření:** 8. 6. 2020

<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení – následující škálou 1 až 4:</b>
<b>1. Splnění zadání</b>	<b>1=zadání splněno, 2=zadání splněno s menšími výhradami, 3=zadání splněno s většími výhradami, 4=zadání nesplněno</b>
<b>Popis kritéria:</b> Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.	
<b>Komentář:</b> Zadání práce bylo splněno.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</b>
<b>2. Písemná část práce</b>	<b>90 (A)</b>
<b>Popis kritéria:</b> Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále 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. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.	
<b>Komentář:</b> Text práce je logicky řazen, jednotlivé části na sebe navazují. Úvodní analýza zahrnuje jak souhrn systému pro monitorování a analýzu komunikace po síti, tak i problematiku virtualizace. V návrhové části je stěžejní návrh API, který slouží pro implementaci na straně zadavatele a způsob komunikace se systémem BC. Popis implementace samotného monitorovacího stroje je dostatečný pro další použití. Testování je velmi důležitou částí práce. Zde bych pochválil autora za vytvoření testovacího prostředí složeného z infikovatelných strojů, které sice nebylo otestováno studenty EHA (projekt nebyl studenty vybrán), ale i tak nezůstali nepovšimnuti. Text práce je bez větších prohřešků proti typografii a gramatice. Počet zdrojů odpovídá charakteru práce a nenašel jsem prohřešky proti citačním pravidlům.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</b>
<b>3. Nepísemná část, přílohy</b>	<b>100 (A)</b>
<b>Popis kritéria:</b> Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů	
<b>Komentář:</b> Implementační část práce je zdařilá a navržené řešení je plně integrovatelné do cloudového systému. Realizované části jsou řádně otestované a finálnímu nasazení do produkce brání jen zpoždění částí, které řeší zadavatel.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</b>
<b>4. Hodnocení výsledků, jejich využitelnost</b>	<b>100 (A)</b>
<b>Popis kritéria:</b> Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.	

**Komentář:**

Výsledky práce jsou zadavatel v současné době integrovány do systému (realizuje se API dle návrhu studenta) a finišuje úprava GUI. O prázdninách je plánováno nasazení systému na produkční servery. Tato práce bude i dále rozvíjena v oblasti identifikace hrozeb s využitím neuronových sítí.

*Hodnotící kritérium:*

*Způsob hodnocení – následující škálou 1 až 5:*

**5. Aktivita a samostatnost studenta**

5a:  
**1=výborná aktivita,**  
2=velmi dobrá aktivita,  
3=průměrná aktivita,  
4=slabší, ale ještě dostatečná aktivita,  
5=nedostatečná aktivita

5b:  
**1=výborná samostatnost,**  
2=velmi dobrá samostatnost,  
3=průměrná samostatnost,  
4=slabší, ale ještě dostatečná samostatnost,  
5=nedostatečná samostatnost

*Popis kritéria:*

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (5a). Posuďte schopnost studenta samostatně tvůrčí práce (5b).

**Komentář:**

Student pravidelně konzultoval jak s autory cloudového systému tak i s lidmi z praxe denně řešící různé internetové hrozby.

*Hodnotící kritérium:*

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

**6. Celkové hodnocení**

95 (A)

*Popis kritéria:*

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

**Text hodnocení:**

Celkově je tato diplomová práce ukázkou propojení teorie a praxe při řešení síťových hrozeb. Práci doporučuji k obhajobě a hodnotím stupněm A.

Podpis vedoucího práce: