



# Hodnocení vedoucího závěrečné práce

**Student:** Bc. Tomáš Ďuračka  
**Vedoucí práce:** Ing. Tomáš Čejka  
**Název práce:** Detekce útoků využívajících aplikační protokol HTTP  
**Obor:** Počítačová bezpečnost

**Datum vytvoření:** 5. 6. 2018

<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> Tato práce obsahuje stručný popis problematiky penetračního testování a zaměřuje se na testy zranitelnosti aplikací postavených nad protokolem HTTP. Na základě nastudovaných informací a studentových pracovních zkušeností byl navržen a implementován detekční modul, který je schopný detekovat vybrané penetrační testy v rozšířených datech o provozu počítačové sítě.	
<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> Písemná část práce je na dobré úrovni. Práce obsahuje drobné typografické chyby, které ale nebrání čitelnosti a pochopení obsahu. Práce obsahuje informačně bohaté části, neobsahuje zbytečné části. Text obsahuje užitečné ukázky dat, která jsou generována během penetračních testů a na základě kterých byla navržena detekce. Práce obsahuje dostatečné množství relevantních citovaných zdrojů, které byly v textu použity správně.	
<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>90 (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> Výsledkem práce je softwarová implementace detekčního modulu. Zdrojové kódy jsou napsány pečlivě, jsou dostatečně zdokumentovány.	
<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>90 (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:*

Výsledný detekční modul je využitelný v praxi, bude nasazen na kolektoru síťových toků v infrastruktuře CESNET2. Zdrojové kódy budou přidány do veřejného repozitáře projektu NEMEA, kde budou dostupné spolu s ostatními detekčními moduly komunitě.

*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 pracoval samostatně a vytvořil fungující detekční modul. Konzultace byly potřeba pouze minimálně. Je škoda, že se student nestihl problematice věnovat delší čas.

*Hodnotící kritérium:*

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

**6. Celkové hodnocení**

90 (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:*

Výsledky práce jsou použitelné v praxi, kvalita výsledků je na vysoké úrovni. Text práce neobsahuje žádné závažné problémy. Celkově je tato práce užitečným přínosem a může do budoucna sloužit i pro výukové účely v oblasti síťové bezpečnosti a detekce podezřelého síťového provozu.

Podpis vedoucího práce: