# Posudek oponenta bakalářské práce

**Student:** Lazárek Zbyněk, Bc.
**Téma:** Automatizovaná detekce transportního protokolu v zachycené síťové komunikaci (id 17384)
**Oponent:** Kmeť Martin, Ing., UIFS FIT VUT

**1. Náročnost zadání** **obtížnější zadání**

V priebehu práce sa študent musel zoznámiť s viacerými normami, týkajúcimi sa viacerých protokolov. V priebehu riešenia musel navrhnúť nielen metódu analýzy zvolených tunelovacích protokolov, ale aj metódu detekcie transportných protokolov z pomerne malej množiny opakujúcich sa hodnôt. Študent sa v implementačnej fáze taktiež musel zoznámiť s pomerne komplexným prostredím Netfox Framework.

**2. Splnění požadavků zadání** **zadání splněno**

Všetky body zadania boli splnené. V bode 2 boli zvolené protokoly GRE, Teredo a 6in4.

**3. Rozsah technické zprávy** **je v obvyklém rozmezí**

Práca je v obvyklom rozsahu.

**4. Prezentační úroveň předložené práce** **60 b. (D)**

Jednotlivé kapitoly na seba nadväzujú a práca je členená pomerne logicky, je písaná veľmi strohým jazykom, miestami až heslovite. Hneď na začiatku práce mi z časti vadil nekorešpondujúci názov a obsah kapitoly 2, v ktorej sa naviac objavujú časté nepresnosti (napr. chyba v popise hlavičky IP, nepresný popis sieťovej vrstvy). V ďalších kapitolách sa taktiež miestami vyskytujú menšie chyby a redundantné informácie. Naopak musím vyzdvihnúť kvalitu kapitoly 6, kde je fáza testovania spracovaná naozaj kvalitne a prehľadne.

**5. Formální úprava technické zprávy** **80 b. (B)**

Práca bola vysádzaná za použitia fakultnej šablóny pre systém LaTeX. Z tohto dôvodu bola správa z typografického hľadiska na vysokej úrovni. Miestami sa však vyskytli chyby v podobe zle rozdeleného slova alebo zle zvoleného tvaru slova. Tieto problémy však neboli príliš časté.

**6. Práce s literaturou** **80 b. (B)**

Študent pracoval väčšinou s dokumentami RFC. Vzhľadom na charakter práce je toto pochopiteľné a všetky použité zdroje boli relevantné k téme práce. V práci sa však nikde nevyskytovali citácie na zdroje 12 a 13.

**7. Realizační výstup** **90 b. (A)**

Riešenie dodané študentom bolo testované ako na syntetických dátach s rôznymi tunelovacími protokolmi, tak na reálnych dátach bez použitia tunelovacieho protokolu. V oboch prípadoch sa riešenie ukázalo ako plne funkčné. Kód dodaný študentom je prehľadný a štruktúrovaný.

**8. Využitelnost výsledků**

Študent rozšíril existujúce riešenie parsovania rámcov v aplikácií Netfox Detective, ktorý je vyvíjaný v rámci projektu MV VG20102015022. Toto rozšírenie umožňuje spracovávanie tunelovanej komunikácie a pridáva možnosť spracovávania rámcov s neznámym zapuzdrením, vďaka pridaniu automatizovanej detekcie transportného protokolu.

**9. Otázky k obhajobě**

- Porovnávali ste schopnosti detekcie pripraveného modulu s inými aplikáciami slúžiacimi na analýzu sieťovej komunikácie (napr. Wireshark, MS NetworkMonitor)? Aká je ich podpora v oblasti tunelovacích protokolov? Umožňujú detekciu transportného protokolu v neznámych tunelovacích protokoloch?

**10. Souhrnné hodnocení** **80 b. velmi dobře (B)**

Študent navrhol plne funkčné riešenie a splnil všetky body zadania. V technickej správe sa však miestami vyskytujú chyby, ktoré síce nie sú zásadného rázu, avšak znižujú dobrý pocit z celkového riešenia (mierne faktické chyby, redundantné informácie). Z implementačného hľadiska je však práca veľmi vydarená a jej výsledky sú prakticky využiteľné. Kapitola popisujúca testovanie riešenia je taktiež spracovaná veľmi precízne a prehľadne. Z toho dôvodu navrhujem hodnotenie B.

V Brně dne: 3. června 2015

.....
podpis