

# Posudek práce

předložené na Přírodovědecké fakultě JU

- posudek vedoucího  
 bakalářské práce
- posudek oponenta  
 diplomové práce

Autor/ka: **Tomáš Rýc**  
Název práce: **Analýza Darknetu se zaměřením na forenzní zkoumání**  
Studijní program a obor: Aplikovaná informatika  
Rok odevzdání: 2020

Jméno a tituly vedoucího/opponenta: Ing. Marta Vohnoutová  
Pracoviště: Ústav aplikované informatiky  
Kontaktní e-mail: mvohnoutova@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/oponenta:

V bakalářské práci ofocené zadání obsahovalo požadavek vytvoření metodiky řešení kybernetické kriminality, identifikace trestného jednání, monitoring trestného jednání.

V práci jsem však, odpovídající metodiku (kromě dvou stránek v závěru práce), nenašla. Do strany 14 jsem pročetla pouze sebrané informace. Postrádala jsem vlastní schémata, obrázky, většina byla obrázky převzaté z internetu, kde ani nebylo vyznačené, že byly převzaty nebo jejich zdroj. Celý text je jakoby posbíráán na jednu haldu, postrádala jsem přehlednost. Autor práce si navíc libuje ve zkratkách, kterých je v práci tolik, že práce ztrácí přehlednost a čtivost. Tabulka zkratek nebo něco obdobného v práci není.

Rozsah práce je, vzhledem k tomu, jaká část je pouze převzatá, nedostatečný. Určitá tvrzení nejsou v textu jasně popsána, např. není jasné, jak může autor odposlechem získat IP adresu serveru, když celý Darknet je stavěn tak, aby toto možné nebylo. Prosím studenta o vysvětlení, které tedy víme, ale v práci popsáno není.

To, co považuji za klíčové, v práci popsáno není nebo nedostatečně – např. „Kapitola 4. Způsob identifikace trestné činnosti v Darknetu“ má o identifikaci trestné činnosti v Darknetu tři podkapitoly, každou o několika větách, zbytek je technický popis fungování Darknetu.

Podle mého názoru však práce neobsahuje požadovanou metodiku, resp. Na konci jsou dvě stránky nazvané Metodika, což není dostatečné.

Kladem práce je, že autor vytvořil vlastní simulaci Darknetu pomocí simulátoru sítě Shadow a Tor Pluginu. Popis sítě, její schéma a výstupy nejsou v práci popsány dostatečně. Očekávala bych přílohu k práci nebo možnost přístupu do simulovaného prostředí, které autor vytvořil.

## Případné otázky při obhajobě a náměty do diskuze:

1. Korelační útok – popište princip a řekněte, jak se dozvíte, který server v Darknetu je ten příslušný, kde máte odposlouchávat.
2. Replay útok – popište, jak na rozsáhlé Darknet síti zjistíte správný výstupní uzel, kde můžete očekávat vámi vyvolanou chybu?
3. Jakým způsobem byste prováděl analýzu informací získaných ze serveru v Darknetu. Srovnajte jednotlivé, vámi zmíněné, nástroje a porovnejte je. Jaký z nich byste použil vy a proč?

## Práci

doporučuji

nedoporučuji

uznat jako ~~diplomovou~~/bakalářskou.

## Navrhuji hodnocení stupněm:

výborně  velmi dobře  dobře  neprospěl/a

## Místo, datum a podpis vedoucího/oponenta:

V Českých Budějovicích dne 24. června 2020