Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Lukáš Doležel** **Oponent:** **Ing. Jaromír Švejda, Ph.D.**

Studijní program: **Informační technologie**
Studijní obor/Specializace: **Kybernetická bezpečnost**
Akademický rok: **2023/2024**

Téma diplomové práce: **Systém pro rychlou detekci a ověření zranitelností infrastruktury**

Hodnocení práce:
Diplomová práce se zabývá vývojem systému pro rychlou detekci a ověření zranitelnosti infrastruktury. Text práce je psán velmi dobře srozumitelnou formou a věnuje podobně jednotlivým částem vyvíjeného systému. Sporadicky se vyskytují překlepy, které ale nijak výrazně nesnižují kvalitu předloženého textu (např. „lidksými analitiky“, „sytému“, „programagle“ apod.).
Celkově bych v teoretické části práce uvítal výrazně častější citování použitých zdrojů, protože jsem zde objevil i úseky, které nějakou citaci zcela postrádají. Jako příklad zde lze zmínit například to, že první odkaz na použitý zdroj se nachází až na čtvrté stránce teoretické části (str. 16).
Praktická část popisuje architekturu systému využívajícího podpůrná data. Jsou popsány i jednotlivé kroky, které autor provedl za účelem implementace navrženého systému. Co v této části však nepůsobí příliš vhodně, je autorovo časté překlopení popisu do teoretické roviny. Zde jako příklad může posloužit např. kapitola *6.1 Faktory ovlivňující nasazení detekčních systémů*. Nezpochybňují důležitost její přítomnosti v práci, ale svou povahou se hodí spíše zařadit do části teoretické, neboť seznamuje čtenáře s jednotlivými faktory, které je třeba zvážit při nasazení detekčních systémů. Stejný případ je i kapitola *7.3 Pyramida bolesti* a některé další. Zkrátka, při čtení praktické části jsem měl občas pocit, že jsem se začetl spíše do teorie než do popisu praktického výstupu diplomové práce.
Argumentace použitá v kapitola 6.3.1. pro nasazení nástroje Suricata na mě nepůsobí příliš přesvědčivě. Neexistuje sice mnoho systémů, které lze k danému účelu použít, nicméně tento fakt nijak nevylučuje konkurenční nástroj Snort, o němž je rovněž zmínka v teoretické části (kapitola 4.1.5).
Jako poslední výtku bych měl k naplnění posledního bodu zadání: *5. Otestujte funčknost implementovaného systému.* Testování funkčnosti implementovaného systému se explicitně věnuje snad pouze třetí odstavec v závěru. Bylo by však mnohem vhodnější uvést konkrétní výstupy z onoho testování a věnovat jim zvláštní kapitolu.
Celkově je práce napsána velmi solidně, shrnuje přehledně jednotlivé aspekty zabezpečení infrastruktury a uvádí i jak k této problematice z praktického hlediska přistoupit.

Otázky k obhajobě:

1. Mohl byste uvést konkrétnější důvod, proč jste dal přednost nástroji Suricata před nástrojem Snort?
2. Jak probíhalo testování funkčnosti implementovaného systému?

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Celkové hodnocení práce:
Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně, F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

D - uspokojivě.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 23.5.2024 Podpis oponenta diplomové práce