Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Marek Cigánek** **Oponent:** **Ing. Petr Mrázek, Ph.D.**

Studijní program: **Bezpečnostní technologie, systémy a management**
Studijní obor/Specializace: **Bezpečnostní technologie**
Akademický rok: **2023/2024**

Téma diplomové práce: **Systém detekce průniku v Linuxovém serveru**

Hodnocení práce:
V teoretické části se autor věnuje historii vzniku detekčních systémů, jejich komponentám, technikám a obecnému rozdělení. Další kapitola je věnována návrhu pravidel detekce a poslední kapitola vede k výběru detekčního systému.
Praktická část nejprve popisuje architekturu použitého testovacího prostředí, operační systém Linux a jeho části. Dále je popsán samotný systém HIDS, pro nějž byl použit projekt Wazuh. Dále je dopodrobna popsáno samotné penetrační testování a v poslední kapitole praktické části pak vyhodnocení včetně návrhů řešení odhalených zranitelností.

Práce beze zbytku splnila zadání a po formální stránce je také bezchybná.

Při obhajobě by mohl diplomant zmínit, je-li reálné nasadit systém kdekoli v produkčním prostředí a pokusit se odhadnout hardwarové nároky na server, který by měl obsluhovat např. vyšší desítky klientských stanic.

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

A - výborně.

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

Datum 30.05.2024 Podpis oponenta diplomové práce