Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. František Sedláček** **Oponent:** **RNDr. Vlasta Šťavová, Ph.d.**

Studijní program: N3902 Inženýrská informatika
Studijní obor: Bezpečnostní technologie, systémy a management
Akademický rok: **2020/2021**

Téma diplomové práce: **Zajišťování důkazních materiálů v kybernetických systémech**

Hodnocení práce:
Diplomová práce se zabývá velmi aktuálním tématem a to akvizici dat z inteligentních zařízení a využití těchto dat pro další práci kriminalistů.
První kapitoly se věnují legislativní stránce zajištění důkazu a klasifikaci IOT zařízení. Popisují možné scénáře využití těchto zařízení v kriminalistickém šetření. Zde bych jen podotkla, že scénář 2.6.2.2. popisující útočníka zvyšující zmetkovitost na výrobních zařízeních je možný, ale reálnější mi připadá scénář, kdy útočník vyřadí linku z provozu, případně ovlivní parametry linky tak, aby došlo k co největšímu poškození výroby.
Třetí kapitola je obecný metodologický postup zajištení dat pro jednotlivé kategorie zařízení. Autor zde správně zdůrazňuje důležitost autenticity sebraných dat a zdokumentování celého procesu.
Čtvrtá kapitola je metodologie pro jednotlivé kategorie zařízení. Tady bych měla připomínku k sekci 4.2 SCADA zařízení. Bylo by vhodné zmínit, že takové firmy mívají svuj CIRT tým, který je vhodné kontaktovat a využít ho pro poskytnutí logů a spolupráci na jejich analýze. Lokální bezpečnostní tým bude mít lepší přehled, co je v prostředí běžné a co naopak anomálie.
Kapitola 5 se zabývá praktickou analýzou. Metodologii, kterou autor napsal v předcházejících kapitolách aplikoval na možné scénáře z kriminalistické praxe.

Pokud výsledkem měl být postup “krok za krokem”, mám drobné výhrady k formulaci textu. Nejsem si jistá, zda by člověk bez většího IT povědomí byl schopen popsaný postup replikovat. Dokážu si představit, že by pomohla příloha, kde by autor detailněji popsal zmíněné postupy například, jak správně vytěžit router. Praktický scénář pro skupinu E - otočená Wifi kamera bych rozšířila o zjištění ovládacího rozhraní kamery, přihlašovacích údajů a verze použitého firmware. Pokud vlastník kamery nezměnil defaultní adminské heslo nebo firmware obsahuje známou zranitelnost, může to indikovat možný způsob zneužití. Praktický scénář 6.4. obsahuji prakticky experiment dokládající, že různé hodinky měří kroky různým způsobem. Pokud se experiment odehrál pouze jednou a na jedné trase, je výsledek spíše anekdotické povahy. V sekci 7.1 by se ještě dalo zmínit, že může být zajímavou informací, zda se pachatel připojil do sítě (nové připojení zařízení těsně před zločinem). V pachatelově zařízení se pak dají dohledat “Saved Networks”, atd.
Práce obsahuje rozsáhlé přílohy. Vyzdvihla bych znalecké posudky pokrývající scénáře zmíněné v práci.

Z mého úhlu pohledu se téma diplomové práce ukazuje jako velmi široké. Autor pokrývá několik vzájemně rozdílných kategorii, například SCADA systémy, C-ITS systémy nebo wearables. Práci by prospělo užší zaměření, tak aby se autor mohl zaměřit pouze na danou kategorii, pokrýt několik scénářů pouze v rámci ní, vytvořit detailnější manuál, atd.

Práce je po stránce gramatické na vysoké úrovni, jediný překlep jsem objevila v příloze na str. 109.

Otázky na autora:

- V rámci znaleckých posudků zmiňujete kontaktování cloudového providera Samsung za účelem získání dat. Máte s tímto postupem zkušenost? Je reálné od cloudového providera data získat?
- Jak se bude výsledek práce dále využívat?

Práci doporučuji k obhajobě a hodnotím známkou B.

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 k obhajobě a navrhuji hodnocení
B – velmi dobře

•

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

Datum 1. 6. 2021 Vlasta Šťavová