Rozšírené zadanie diplomovej práce

Názov práce: Identifikácia relevantných digitálnych stôp pri forenznom vyšetrovaní

Autor práce: Bc. František Kurimský

Vedúci práce: doc. JUDr. RNDr. Pavol Sokol, PhD.

Konzultant práce: Mgr. Eva Marková

Ciele:

(1) Analyzovať forenzné artefakty v operačnom systéme Windows.
(2) Porovnať existujúce prístupy k identifikácii relevantných digitálnych stôp pri forenznom vyšetrovaní operačného systému Windows.
(3) Navrhnúť model pre identifikáciu relevantných digitálnych stôp pri forenznom vyšetrovaní operačného systému Windows, implementovať model a zhodnotiť efektívnosť tohto modelu.

Popis:

V dnešnej dobe neustále narastá počet kybernetických útokov. Pri forenznom vyšetrovaní je potrebné sa čo najrýchlejšie dopracovať k relevantným dátam, ktoré obsahujú informácie o postupe útočníka. Artefakty získané z napadnutého systému sa z veľkej časti skladajú z artefaktov nerelevantných pre forenzné vyšetrovanie konkrétneho prípadu, resp. bezpečnostného incidentu. Cieľom práce je ušetriť čas forenzného analytika pri hľadaní relevantných dát pre forenznú analýzu. Inými slovami, ide o automatizáciu tohto procesu. Nájdené artefakty poskytujú forenznému analytikovi nadhľad nad bezpečnostným incidentom a umožňujú rýchlejšie stanovenie a následne potvrdenie alebo vyvrátenie forenzných hypotéz o bezpečnostnom incidente a činnosti útočníka.

Prvým cieľom práce je analýza forenzných artefaktov v operačnom systéme Windows. Operačný systém si interne zaznamenáva dôležité udalosti vykonané v určitom čase. Sú to napríklad udalosti ako prihlásenie používateľa, alebo odosielanie emailovej správy. Príklady

forenzných artefaktov sú Recycle Bin, Browsers, Windows Error Reporting Forensics, Remote Desktop Protocol (RDP) Cache, LNK Files, Jump Lists, Prefetch Files a Shellbag. Výsledkom prvého cieľu je analýza týchto artefaktov, analýza ich štruktúry a obsiahnutých informácií. Súčasťou tohto cieľa bude aj identifikácia vhodnej reprezentácie týchto informácií v dátových rámcoch (datafremoch) a transformácia dát do podoby vhodnej pre navrhovaný model v treťom cieli.

Prácou forenzného analytika je identifikácia artefaktov, ktoré mu umožnia odhaliť kroky vykonané útočníkom. Tento krok analýzy je časovo náročný. Druhým cieľom práce je naučiť sa postup práce pri identifikácií relevantných digitálnych stôp pri forenznom vyšetrovaní v operačnom systéme Windows a takisto porovnať existujúce prístupy a nástroje používané pri tomto úkone. Výsledkom druhého cieľa je zistiť, ktoré údaje sú dôležité pre identifikáciu stôp, a na základe získaných informácií hľadať možnosti automatizácie.

Tretím cieľom je príprava modelu, ktorý bude automatizovať identifikáciu relevantných digitálnych stôp. V princípe ide o hľadanie neštandardných udalostí uskutočnených v operačnom systéme. Vstupom pre tento model je obraz disku operačného systému Windows so súborovým systémom NTFS. K danej problematike neexistuje dataset, ktorý obsahuje obrazy diskov s definovanými digitálnymi stopami útočníka. Možnosťou je trénovať model metódou bez učiteľa a overenie jeho efektívnosti nad nami pripravenými obrazmi disku operačného systému, v ktorom sme vykonali útok. Medzi zvažované metódy zaraďujeme samo organizujúce mapy, ktoré sú príkladom použitia neurónových sietí v podobných problémoch odhaľovania anomálií, resp. outlierov.

Najbližšími krokmi práce bude analyzovať jednotlivé forenzné artefakty a informácie v nich obsiahnuté, ako aj identifikovať možnosti vytvorenia dátovej sady forenzných obrazov (imagov) diskov. Pri spoznávaní sa s problematikou použijeme vzorový obraz disku z DFIR Madness portálu, The case of the stolen Szechuan sauce.

Literatúra:

(1) Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer networks, 51(12), 3448-3470.

(2) Alabadi, M., & Celik, Y. (2020, June). Anomaly detection for cyber-security based on convolution neural network: A survey. In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-14). IEEE.

(3) Mohammad, R. M. A., & Alqahtani, M. (2019). A comparison of machine learning techniques for file system forensics analysis. Journal of Information Security and Applications, 46, 53-61.

(4) Grajeda, C., Breitinger, F., & Baggili, I. (2017). Availability of datasets for digital forensics–and what is missing. Digital Investigation, 22, S94-S105.