

Analýza vzťahov medzi forenznými artefaktami s využitím teórie grafov

Študent: Sophia Petra Krišáková

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

Konzultant: RNDr. Eva Marková

V digitálnom svete je bezpečnosť dát a sietí kľúčovým záujmom pre organizácie všetkých veľkostí a odvetví. S nárastom kybernetických útokov a ich stále sa meniacou povahou sa organizácie musia neustále prispôbovať, aby ochránili svoje aktíva a zabezpečili bezpečnosť svojich informácií. Kybernetickí útočníci sa neustále vyvíjajú a prichádzajú s novými spôsobmi, ako preniknúť do systémov a získať neoprávnený prístup k citlivým údajom. Tieto útoky sa stávajú nielen sofistikovanejšími a preto je pre organizácie výzvou identifikovať tieto útoky čo najrýchlejšie a zareagovať na ne adekvátne.

Jedným z hlavných problémov je čas medzi výskytom bezpečnostného incidentu a jeho identifikáciou a následnou reakciou. Tento čas môže byť netriviálny, často sa meria v stovkách dní, čo dáva útočníkom dostatok času na spôsobenie škôd a uniknutie bez toho, aby boli odhalené. Okrem toho, aj po identifikácii incidentu organizácia potrebuje určitý čas na jeho vyriešenie a obnovenie normálneho fungovania.

Naším cieľom je zredukovať tento časový interval a umožniť organizáciám rýchlejšiu a efektívnejšiu reakciu na kybernetické útoky. V práci sa zameriavame na využitie teórie grafov v procese forenznej analýzy v operačnom systéme Windows. Grafová analýza nám umožňuje identifikovať vzťahy medzi rôznymi digitálnymi stopami a ich atribútmi, čím lepšie porozumieme povahe útoku a jeho šíreniu v sieti.

Pracujeme s rôznymi dátovými sadami, ktoré boli vytvorené na účely rôznych súťaží typu Capture the Flag (CTF). Tieto dáta obsahujú rôzne typy útokov a digitálnych stôp, ktoré nám umožňujú simulovať reálne kybernetické incidenty a testovať naše metódy analýzy.

Výsledkom našej práce je identifikácia anomálií, cyklov a najkratších ciest v grafoch digitálnych stôp. Tieto poznatky môžu poskytnúť organizáciám komplexnejší a hlbší pohľad na ich bezpečnostné postupy a pomôcť im lepšie sa chrániť pred kybernetickými hrozbami.