Vplyv anti-forenzných techník na digitálne forenzné vyšetrovanie

MOTIVÁCIA

Študentka: Zuzana Hennelová

Vedúca práce: Mgr. Eva Marková

Konzultant: RNDr. JUDr. Pavol Sokol, PhD.

Pri výbere témy na bakalársku prácu som sa sústredila na oblasť informačnej bezpečnosti, pretože ma táto oblasť zaujíma a chcela by som sa ňou zaoberať aj v budúcnosti. Okrem toho považujem informačnú bezpečnosť za dôležitú v súvislosti s technologickými pokrokmi, s ktorými sa spájajú aj nové riziká ohrozujúce spoločnosť či jednotlivcov.

Z vypísaných tém na bakalársku prácu ma hneď oslovila práca na tému *Vplyv anti-forenzných techník na digitálne forenzné vyšetrovanie* pod vedením Mgr. Evy Markovej. Táto téma ma zaujala, pretože v súčasnej dobe je digitálna kriminalita bežná ale zaisťovanie stôp a dôkazov v digitálnom priestore a následné zisťovanie postupu útočníka môže byť náročné. Práve preto vznikla forenzná analýza, ktorá sa zaoberá zaisťovaním digitálnych dát a ich analýzou. Útočníci sú si však vedomí jej existencie a existencie mnohých postupov a nástrojov, ktoré využíva. Preto po vzniku forenznej analýzy vznikli aj anti-forenzné techniky, ktoré útočníci využívajú s cieľom spomaliť alebo ideálne znemožniť analytikom získanie relevantných informácií o vykonanom alebo ešte prebiehajúcom útoku.

Anti-forenzné techniky sú aj v súčasnosti pomerne málo preskúmané (ich prvé detailnejšie popísanie bolo v roku 2002), čo považujem za jeden z dôvodov prečo je potrebné sa nimi zaoberať. Popularita anti-forenzných techník rastie a útočníci prichádzajú s novými a komplexnejšími technikami. Myslím si, že ich lepšie preskúmanie a pochopenie by mohlo viesť k účinnejšej detekcii použitia takýchto techník, k zníženiu ich efektivity a prípadne aj k ich eliminácii.

Mojim prvým cieľom pri písaní tejto bakalárskej práce bude teda oboznámenie sa s metódami forenznej analýzy a s vplyvom známych anti-forenzných techník používaných proti nim. Ďalej je v pláne urobiť na základe zistených informácií porovnanie vplyvov týchto techník. Potom bude mojou úlohou získavať artefakty z pripravených testovacích dát (obraz disku) a porovnávať ich s dátami, ktoré získam po aplikovaní anti-forenzných techník na dataset.