**Rozšírené zadanie diplomovej práce**

**Názov:** Forenzná analýza pokročilých útokov na Active Directory a vybraných služieb

v infraštruktúre Windows

**Autor:** Bc. Michal Šafranko

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

**Konzultant:** Mgr. Lukáš Hlavička, IstroSec

**Ciele práce:**

1. Analýza pokročilých útokov na Active Directory a identifikácia forenzných artefaktov v rámci identifikovaných útokov.
2. Návrh postupov pre zaistenie zodpovedajúcich digitálnych stôp.
3. Návrh, implementácia a vyhodnotenie nástroja pre zber, triáž a analýzu zachytených digitálnych stôp.

Služba Active Directory je podľa [1] využívaná približne 90% najväčších svetových spoločností. Umožňuje centralizovanú správu počítačov, identít a riadenia prístupu. Toto robí z Active Directory aj lukratívny cieľ pre útočníkov, ktorí kompromitáciou domény získajú prístup k všetkým digitálnym aktívam danej spoločnosti. Už pri kompromitácií jedného servera, ktorý slúži ako doménový radič, a jeho databázy, získava útočník prístup nie len k danej stanici, ale aj k celej doméne a potencionálne aj k celému lesu domén.

Ochrana domény je komplexný proces, ktorý vyžaduje ako správne nastavené procesy, tak aj správne nastavenie domény a ochranu individuálnych staníc a serverov [2]. Dôležité je tiež využívať moderné technológie, ako sú Credential Guard, skupinu s chránenými užívateľmi alebo doménové radiče určené iba na čítanie. No história ukazuje, že útočníci dokážu kompromitovať aj dobre nakonfigurovanú doménu a úspešne obísť aj vyššie zmienené bezpečnostné technológie, vrátane technológií založených na virtualizácií.

Z týchto dôvodov je pri daných typov bezpečnostných incidentov dôležité poznať kroky útočníka v doméne, a teda je nevyhnutné vykonať forenznú analýzu Active Directory. Podľa nám dostupných informácií, aktuálne chýbajú na trhu nástroje, ktoré by dokázali vyextrahovať zo systému a analyzovať všetky relevantné digitálne stopy týkajúce sa domény a útokov na ňu.

Hlavným cieľom práce, ako aj názov napovedá, je analýza útokov na Active Directory s prihliadnutím na ciele reakcie na incidenty a riešenie forenznej analýzy. Tento hlavný cieľ je možné rozdeliť do troch parciálnych otázok.

Prvým parciálnym cieľom je analyzovať pokročilé útoky na Active Directory, ako sú napríklad Kerberoasting alebo Silver Ticket a Golden Ticket.

Následne vypracujeme postup na zaisťovanie digitálnych stôp, ktoré v systéme zostanú po týchto útokoch. Daný postup bude zahŕňať ako typ a umiestnenie digitálnej stopy, tak aj spôsob ich získania.

Tretím, cieľom je vytvorenie nástroja, ktorý by daný proces zautomatizoval, vykonal triáž a na získaných digitálnych stopách vykonať analýzu.

Zdroje:

[1] Frost & Sullivan: Active Directory Holds the Keys to your Kingdom, but is it Secure? [online] [30.11.2021]. Dostupné na: <https://www.frost.com/frost-perspectives/active-directory-holds-the-keys-to-your-kingdom-but-is-it-secure/>

[2] Microsoft Corpotation: Best Practices for Securing Active Directory. [online] [30.11.2021]. Dostupné na: <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>