Použitie honeytokenov v operačnom systéme Windows

Vedúci: RNDr. Tomáš Bajtoš, PhD.

Študent: Jakub Nižník

Honeytokeny v systéme Windows

- **Honeytoken vs. Honeypot**
  - Honeytoken narozdiel od honeypotu nenapodobňuje celý systém, sú to nejaké dáta alebo entita, ktorá je vložená priamo do systému
- **Prečo Windows?**
  - Najpoužívanjší operačný sýstem
  - Veľké množštvo útokov
- **Spôsob zaznamenávanie/logovania**
  - windows event logs

Ciele práce

1. Preskúmať možnosti natívnych komponentov operačného systému Windows pre použitie ako honeytokeny
2. Vytvoriť nástroj na nasadenie a prípady použitia pre honeytokeny v operačnom systéme Windows
3. Otestovať honeytokeny v laboratórnom prostredí s využitím emulovaných útokov

Postup

- **Analýza**
  - Spracovanie už existujúcich honeytokenov v systéme windows
  - Vytvorenie nových honeytokenov podľa analýzy správania útočníka/používateľa
  - Popísanie účelu a využitia nájdených honeytokenov
- **Implementácia**
  - Implementácia honeytokenov v PowerShell
  - Logovanie dát o interakcii s honeytokenmi vo windows event logs
  - Získavanie logov
  - Vytvorenie scriptov na vytvorenie honeytokenov a vygenerovanie xpath
- **Testovanie**

Materiály

- Sanders, C. (2020) Intrusion detection honeypots: Detection Through Deception.
- Swift, N. (2023). Deceptive defense: best practices for identity based honeytokens in Microsoft Defender for Identity. [online] TECHCOMMUNITY.MICROSOFT.COM.
- https://canarytokens.org/

Ďakujem za pozornosť