Forensische Übungsaufgabe: Operation "Harald und Daniels geheimer Plan"

Vorfallbeschreibung

Alarmstufe Rot: Unser Active Directory (AD) ist in den Fängen der berüchtigten Hackergruppe "Harald und Daniel Gesellschaft mit beschränkter Haltung". Dieser Vorfall hat unsere IT-Infrastruktur schwer getroffen, und es ist unerlässlich, sofort zu handeln, um die Sicherheit unserer Daten wiederherzustellen und die Verantwortlichen zur Rechenschaft zu ziehen.

Ziel der Übung

Deine Aufgabe besteht darin, die sicherheitsrelevanten Ereignisse zu rekonstruieren, die zu diesem Sicherheitsvorfall geführt haben. Du wirst Zugang zu den gesammelten Beweismitteln auf der Maschine "SMPVWINCL01" erhalten und sollst analysieren, welche Veränderungen vorgenommen wurden und welche Spuren die Täter hinterlassen haben.

Technische Details

- **Kompromittierter Client:** SMPVWINCL01 (10.0.6.6)
- **Analyse-Plattform:** Flare-VM (10.0.1.125)
    - **Pfad zu den Beweismitteln:** `C:\Users\forensik\Desktop\Übungsaufgabe`
    - **Benutzername/Passwort:** forensik / forensik

Aufgabenstellung

1. **Beweisanalyse:** Untersuche die bereitgestellten Daten auf der Flare-VM. Achte besonders auf Dinge, die du im CDC Bootcamp gelernt hast.
2. **Netzwerkverkehr:** Analysiere etwaige Netzwerklogs, um festzustellen, ob Daten abgeflossen sind oder ungewöhnliche externe Verbindungen bestanden haben.
3. **Arbeitsspeicher:** Analysiere etwaige Memeory Dumps, um festzustellen, ob ein C2 Framework installiert wurde.
4. **HDD Analyse:** Analysiere etwaige HDD Images, um festzustellen, was die beiden bösen Hacker getan haben.

5. **Erstellung eines Berichts:** Dokumentiere deine Erkenntnisse in einem detaillierten Bericht. Deine Analyse sollte klare Beweise und Indizien enthalten, die die Aktivitäten von "Harald und Daniel" belegen.

Zielsetzung

Das ultimative Ziel dieser Übung ist es, durch deine forensische Analyse die verantwortlichen Angreifer "Harald" und "Daniel" zu identifizieren, damit diese endlich in den wohlverdienten Urlaub geschickt werden können.

Viel Erfolg bei deiner Ermittlung!