LU08.A03 – Logfiles auf eigenem Notebook

Lernziele

1. **Anwenden:** Grundlegende Audit- und Sicherheitsbefehle in der Windows-Kommandozeile anwenden können, um Audit-Policies zu aktivieren und sicherheitsrelevante Ereignisse gezielt auszulösen.
2. **Analysieren:** Exportierte Logdaten analysieren, indem mit Standard-CMD-Befehlen Ereignisse gefiltert werden, zählen und Unterschiede zwischen erfolgreichen und fehlgeschlagenen Anmeldungen herausarbeiten.
3. **Bewerten** der Integrität und Aussagekraft der gesammelten Logdaten, indem Hashwerte erzeugen werden.

Rahmenbedingungen

- Zeitbudget: 50 Minuten
- Sozialform: Einzelarbeit
- Hilfsmittel: Ihr PC
- **Erwartetes Ergebnis:** Arbeitsjournal von 4-5 Seiten, din der die Nachweise der Teilschritte ersichtlich sind.

Ausgangslage

Log-Dateien gibt es nicht nur auf einem Webserver. Auch reguläre Rechner wie Ihr Arbeitsnotebook verfügt über solche Logs. Bei dieser Übung geht es darum diese LogFiles genauer zu analyieren.

Auftrag

Erstelle einen Minireport Inkl. Screenshots), der die nachfolgenden Kennwerte Ihres Notebooks ausgibt:

Abgabe (Mini-Report, max. 1 Seite)

1. **System & Datum/Uhrzeit (inkl. Zeitzone)**
2. **Aktivierte Audit-Subkategorien:**. (Auszug von auditpol).
3. Erzeugte Events (kurzer Ablauf: User angelegt, Sperre/Entsperrung, Fehlversuche).
4. Kernauswertung:
    - Anzahl **4624** (erfolgreich) vs. **4625** (fehlgeschlagen).
    - Zeitpunkte der **4720/4723/4724** (Useranlage/Passwortaenderung).
    - Relevante **System-Events** im gleichen Zeitfenster.
5. **Integritaet:** SHA256-Hashes der Dateien (security_focus.txt, security_last60.txt, system_last60.txt).
6. **Lessons Learned** (brauchbare Event-IDs, Filtersyntax, Grenzen der CMD-Auswertung).

Teilauftrag A: Audit-Policy pruefen & aktivieren (CMD)

```
:: aktuellen Status anzeigen
auditpol /get /category:"Logon/Logoff"
```

```
:: sinnvolle Subkategorien aktivieren (Erfolg+Fehler)
auditpol /set /subcategory:"Logon","Logoff","Account Lockout","User Account Management" /success:enable /failure:enable
```

Teilauftrag B: 2) Ereignisse gezielt erzeugen (CMD)

```
:: Testnutzer anlegen und Passwort setzen
net user TestUser P@ssw0rd! /add
```

```
:: Passwortaenderung erlauben und wechseln
net user TestUser /passwordchg:yes
net user TestUser N3wP@ss!
```

```
:: 1–2 fehlgeschlagene Anmeldungen provozieren (z. B. am Sperrbildschirm)
:: Workstation sperren → entsperren
rundll32 user32.dll,LockWorkStation
```

```
:: optional: Abmelden (erzeugt Logoff/Logon)
shutdown /l
```

Teilauftrag C: Logs sammeln (nur CMD mit wevtutil)

C1: Security-Events (Login/Fehler/Benutzerverwaltung) exportieren

```
:: Export als .evtx (Rohdaten, kompletter Security-Log – optional gross)
wevtutil epl Security .\Security_dump.evtx
```

```
:: Nur relevante Events als Text (max. 500 Eintraege) – IDs: 4624,4625,4634,4720,4723,4724,4725,4726
wevtutil qe Security /q:"*[System[(EventID=4624 or EventID=4625 or EventID=4634 or EventID=4720 or EventID=4723 or EventID=4724 or EventID=4725 or EventID=4726)]]" /f:text /c:500 > .\security_focus.txt
```

C2: Zeitfenster (letzte 60 Minuten) filtern

```
:: XPath-Filter mit Zeitdifferenz in Millisekunden (<= 3.600.000 ms)
wevtutil qe Security /q:"*[System[TimeCreated[timediff(@SystemTime) <= 3600000] and (EventID=4624 or EventID=4625 or EventID=4634 or EventID=4720 or EventID=4723 or EventID=4724 or EventID=4725 or EventID=4726)]]" /f:text > .\security_last60.txt
```

```
:: System-Log der letzten 60 Minuten (z. B. Warnungen rund ums Ereignis)
wevtutil qe System /q:"*[System[TimeCreated[timediff(@SystemTime) <=
3600000]]]" /f:text > .\system_last60.txt
```

Teilauftrag D: Integritaet/Hash der Exportdateien (CMD)

```
certutil -hashfile .\security_focus.txt SHA256
certutil -hashfile .\security_last60.txt SHA256
certutil -hashfile .\system_last60.txt SHA256
```

Hashwerte in den Report uebernehmen.

Teilauftrag E: Quick-Stats (CMD-Einzeiler, einfache Zaehlung)

```
:: erfolgreiche Anmeldungen (4624) zaehlen
find /c "Event ID: 4624" security_last60.txt
```

```
:: fehlgeschlagene Anmeldungen (4625) zaehlen
find /c "Event ID: 4625" security_last60.txt
```

```
:: Benutzeranlage (4720) und Passwortaenderung (4723/4724) zaehlen
find /c "Event ID: 4720" security_last60.txt
find /c "Event ID: 4723" security_last60.txt
find /c "Event ID: 4724" security_last60.txt
```

Tipp: Fuer einen kompakten Ueberblick:

```
echo ---- STATS (letzte 60 Min) ----
for %i in (4624 4625 4634 4720 4723 4724 4725 4726) do @echo ID %i: & find
/c "Event ID: %i" security_last60.txt
```

Teilauftrag F: 6) Stichproben-Anzeige & Kontext (CMD)

```
:: Zeige die letzten ~30 Zeilen rund um einen bestimmten Event-Typ
type security_last60.txt | findstr /n /c:"Event ID: 4625" | more
```

```
:: Nur Zeilen mit Account-/Anmelde-Infos herausfiltern (heuristisch)
findstr /i "Account Name Logon Process Source Network Address Workstation
Name Failure Reason" security_last60.txt > security_login_context.txt
```

Teilauftrag G: Aufraeumen (optional)

```
net user TestUser /delete
```

Solution

Lösung LU08.L03
