PowerShell

IT Forensik – Log Analyse

Aufgabe 1

Melden Sie sich als Administrator an und erstellen Sie Benutzer *otto* mit Kennwort *o* und *hans* mit Kennwort *h*. Melden Sie sich ab.

Versuchen Sie sich als *hans* anzumelden und verwenden Sie absichtlich ein falsches Kennwort. Melden Sie sich danach erfolgreich als *otto* an und wieder ab.

Melden Sie sich als Administrator an und öffnen Sie die Ereignisanzeige entweder über *Tools* → *Ereignisanzeige* oder durch Eingabe von *eventvwr* im Suchfeld oder der Eingabeaufforderung.

Navigieren Sie in der Baumstruktur rechts zu *Windows-Protokolle* → *Sicherheit* und laden Sie das Protokoll (engl. Log) im mittleren Fenster.

Identifizieren Sie im Log die folgenden Ereignisse. Gegebenenfalls filtern Sie Log mithilfe der Aktion *Aktuelles Protokoll filtern* (Aktionen im rechten Fensterbereich), indem Sie bei Quelle *Microsoft Windows security auditing* und bei Ereignis-ID *4600-4799* eintragen. Notieren Sie zu jedem der Ereignisse den Zeitstempel sowie die zugehörige Ereignis-ID:

1) Fehlgeschlagener Anmeldeversuch *hans*

2) Anmeldung *otto*

3) Abmeldung *otto*

4) Anmeldung Administrator

Aufgabe 2

Starten Sie eine PowerShell als Administrator.

a. Lassen Sie sich jeweils die ersten 100 Einträge der Logs Windows PowerShell, *System*, *Security* und *Application* in eine Datei ausgeben, die wie das entsprechende Log heißt. Verwenden Sie die Endung *.log* für die Dateien.

b. Finden Sie heraus, welche drei Logs auf Ihrem System die meisten Einträge besitzen und geben Sie die Gesamtzahl von Logs auf Ihrem System an.

Aufgabe 3

Öffnen Sie die *Ereignisanzeige* und navigieren Sie zum Windows-Protokoll *Sicherheit*.

Löschen Sie das Protokoll über die entsprechende Aktion und speichern Sie das Backup unter dem Namen *security-log-backup.txt* im Downloads-Ordner. Schließen Sie die Ereignisanzeige.

Öffnen Sie die *Lokale Sicherheitsrichtlinie* und setzen Sie die maximale Anzahl Fehlanmeldungen vor einer Kontosperrung über die entsprechende Richtlinie auf den Wert 2.

Legen Sie den Benutzer *bernd* mit Kennwort b über die Benutzerverwaltung (graphische Oberfläche) an und melden Sie sich als Administrator ab.

Versuchen Sie sich als *bernd* anzumelden und geben Sie absichtlich solange falsche Kennwörter ein, bis der Hinweis erscheint, dass das Konto gesperrt ist. Melden Sie sich nun wieder als Administrator an.

Öffnen Sie die Ereignisanzeige und filtern Sie das Sicherheitsprotokoll nach der Quelle *Microsoft Windows security auditing* und der Aufgabenkategorie *User Account Management*.

Identifizieren Sie den zugehörigen Eintrag, der die Sperrung von Benutzer *bernd* protokolliert und notieren Sie Zeitstempel und Ereignis-ID.

Entsperren Sie das Konto von *bernd* über die Benutzerverwaltung wieder.

Suchen Sie im Log die beiden Einträge, die die Änderung eines Benutzerkontos und die Entsperrung anzeigen und notieren Sie jeweils Zeitstempel und Ereignis-ID.

Verifizieren Sie, dass die Sperrung aufgehoben ist, indem Sie sich als *bernd* anmelden und anschließend wieder abmelden.

Melden Sie sich als Administrator an und suchen Sie im Log nach dem Ereignis, das die erfolgreiche Anmeldung von *bernd* protokolliert.

Versetzen Sie abschließend die *Lokale Sicherheitsrichtlinie* wieder in den Ausgangszustand.

Aufgabe 4

Öffnen Sie die *Ereignisanzeige* und laden Sie das Windows-Protokoll *Sicherheit*.

Wählen Sie bei den Aktionen *Gespeicherte Protokolldatei öffnen* und laden Sie die Datei *security-log.evtx* im mittleren Fensterbereich.

Filtern Sie das Log geeignet und beantworten Sie die folgenden Fragen. (Es kann hilfreich sein, sich die Filtereinstellungen aufzuschreiben, damit die Ergebnisse später besser präsentiert bzw. nachvollzogen werden können.)

1) Wie oft gab es Anmeldungen durch den Administrator?

2) Welche Benutzer haben sich außer dem Administrator (erfolgreich) angemeldet?

3) Wie viele Anmeldevorgänge sind fehlgeschlagen?

4) Wie viele Einträge gibt es im gesamten Log File?

5) Welche Konten wurden gesperrt?

6) Welche dieser Konten wurden durch den Administrator bereits wieder entsperrt?

7) Was bedeutet die Ereignis-ID 4798?

8) Welches Benutzerkonto wurde gerade durch den Administrator neu erstellt?

Aufgabe 5

Starten Sie eine PowerShell als Administrator.

a. Laden Sie die Datei *security-log.evtx* mit dem Cmdlet *Get-WinEvent* und lassen Sie sich alle Ereignisse im Log anzeigen.

b. Leiten Sie den Output, d.h. die Ereignisse im Log in eine Textdatei *security-log-events.txt* um.

c. (Bonus) Finden Sie ein Cmdlet, mit dem Sie die ersten beiden Teilaufgaben in einem Schritt erledigen können, d.h. die Ereignisse sollen sowohl auf stdout ausgegeben werden als auch in eine Datei umgeleitet werden.

d. Gruppieren Sie die Einträge nach der Ereignis-ID und lassen Sie sich die fünf häufigsten Ereignis-IDs anzeigen.

e. Erstellen Sie eine Liste aller Ereignisse mit der Ereignis-ID 4624. Lassen Sie sich von diesen den Zeitstempel, die ID und den Text des Ereignisses als Liste formatiert ausgeben.

Aufgabe 6

Öffnen Sie die *Ereignisanzeige*[1] und laden Sie anschließend die Protokolldatei *security-log-deletedobjects.evtx*.

Beantworten Sie mithilfe des Log Files die folgenden Fragen, indem Sie geeignete Filter verwenden. Notieren Sie neben dem gesuchten Benutzer auch die Ereignis-ID und die Uhrzeit.

a. Wer löschte die Datei *topsecret.txt*?

b. Wer löschte den Ordner *Confidential*?

c. Wem wurde das Löschen der Datei *topsecret.txt* verweigert?

[1] Alternativ können Sie statt der Ereignisanzeige auch die PowerShell verwenden und die Aufgabe ohne graphische Oberfläche lösen.