PowerShell

IT Forensics – Log Analysis

Task 1

Log in as administrator and create users *otto* with password *o* and *hans* with password *h*. Log out.

Try logging in as *hans* and intentionally use an incorrect password. After that, log in successfully as *otto* and log out again.

Log in as an administrator and open Event Viewer either from *Tools → Event Viewer* or by typing *eventvwr* in the search box or command prompt.

In the tree structure on the right, navigate to *Windows Logs → Security* and load the log in the middle window.

In the log, identify the following events. If necessary, filter the log by using the *Filter Current Log* action (Actions in the right pane) by entering *Microsoft Windows security auditing* at Source and *4600-4799* at Event ID . For each of the events, write down the timestamp as well as the associated event ID:

1) Failed login attempt *hans*

2) Registration *otto*

3) Unsubscribe *otto*

4) Login Administrator

Task 2

Start a PowerShell as an administrator.

a. Have the first 100 entries of the Windows PowerShell, *System*, *Security* and *Application* logs output to a file with the same name as the corresponding Log. Use the *.log* extension for the files.

b. Find out which three logs on your system have the most entries and specify the total number of logs on your system.

Task 3

Open Event *Viewer* and navigate to the Windows *Security* log.

Clear the log of the appropriate action and save the backup under the name *security-log-backup.txt* in the Downloads folder. Close the Event Viewer.

Open the *Local Security Policy* and set the maximum number of false logins before an account lockout to 2 via the appropriate policy.

Create the user *bernd* with password b via the user administration (graphical interface) and log out as administrator.

Try logging in as *bernd* and intentionally enter incorrect passwords until you see a message that your account is locked. Now log back in as an administrator.

Open the Event Viewer and filter the security log by the source *Microsoft Windows security auditing* and the *User Account Management* task category.

Identify the associated entry that logs user *bernd's* lockout and note the timestamp and event ID.

Unblock *bernd's* account via the user management.

In the log, find the two entries that show the change of a user account and the unlock, and note the timestamp and event ID of each.

Verify that the block has been lifted by logging in as *bernd* and then logging out again.

Log in as an administrator and look for the event in the log that logs *bernd's* successful login.

Finally, restore the *Local Security policy* to its initial state.

Task 4

Open Event *Viewer* and download the Windows *Security* log.

In the actions, select *Open saved* log file and load the *security-log.evtx* file in the center pane.

Filter the log appropriately and answer the following questions. (It may be helpful to write down the filter settings so that the results can be better presented and understood later.)

1) How often were there logins by the administrator?

2) Apart from the administrator, which users have logged in (successfully)?

3) How many logins failed?

4) How many entries are there in the entire log file?

5) Which accounts have been suspended?

6) Which of these accounts have already been unblocked by the administrator?

7) What does Event ID 4798 mean?

8) Which user account has just been newly created by the administrator?

Task 5

Start a PowerShell as an administrator.

a. Load the *security-log.evtx* file using the *Get-WinEvent* cmdlet and view all events in the log.

b. Redirect the output, i.e. the events in the log, to a text file *security-log-events.txt* .

c. (Bonus) Find a cmdlet that allows you to complete the first two subtasks in one step, i.e. the events should be both output to stdout and redirected to a file.

d. Group the entries by event ID and see the five most common event IDs.

e. Create a list of all events with event ID 4624 and ask them to output the timestamp, ID, and text of the event formatted as a list.

Task 6

Open the *Event Viewer*, [1] and then load the *security-log-deletedobjects.evtx log* file.

Use the log file to answer the following questions using appropriate filters. In addition to the user you are looking for, write down the event ID and time.

a. Who deleted the *topsecret.txt* file?

b. Who deleted the *Confidential* folder?

c. Who was denied permission to delete the *topsecret.txt* file ?

[1] Alternatively, you can use PowerShell instead of the Event Viewer and solve the task without a graphical user interface.