Keikaku 企画

PMR Insight Collective Knowledge (PICK)
Use Case Scenario
03/10/2020

Scenario 1: Generate Attack Graphs

Preconditions: A Kali Linux environment is running and a Splunk server has been set up by the analyst, all dependency libraries have been installed, and the analyst has a collection of data/files that have been generated during an adversarial assessment.

Postconditions: The analyst will have created an attack graph of a given vector with its corresponding CSV file with the use of the PICK system.

Actors: Analyst, Lead Analyst, Splunk

Scenario 1: Generate Attack Graphs

1. The analyst provides the event name, event description, event start timestamp, and event end timestamp.
2. The system stores the event name, event description, event start timestamp, and event end timestamp.
3. The analyst creates the vectors for the given session and provides the name and description for them.
4. The system generates unique identification numbers for the vectors.
5. The system will store the unique ID, name, and description for each vector.
6. The analyst enters the lead analysts' IP address (ALT 1).
7. The system stores the provided lead's IP address.
8. The analyst provides the root directory where the adversarial assessment data exists, along with the Red Team, Blue Team, White Team, and Icon subdirectories.
9. The system records the paths of the root directory and Red Team, Blue Team, White Team, and Icon subdirectories.
10. The system begins creating LogFile objects of the scanned files.
11. The system compares the log file to the validation criteria provided by the analyst.
12. The system identifies what sections of the file require attention (ALT 2).
13. The system creates a copy of the validated and cleansed version of the files as LogFile objects.
14. The system sends the cleansed and validated files to Splunk.
15. Splunk converts the log file into indexable log entries.
16. The system retrieves the Splunk-generated log entries.
17. The system begins creating LogEntry objects for every individual retrieved log entry (ALT 3, ALT 4).
18. The analyst chooses which vector each log entry belongs to.
19. The system stores the vector specification of each log entry.
20. The system generates Node objects from log entries with unique identification numbers (ALT 5).
21. The system stores the Node IDs in their respective vector.
22. The analyst sets node visibility by either Node ID, Node Name, Node Timestamp, Node Description, Log Entry Reference, Log Creator, Event Type, Icon Type, or Source (ALT 7, ALT 8).
23. The system stores the analyst-selected node visibility settings.
24. The system renders the nodes based on the selected visibility settings.
25. The analyst manipulates and moves the rendered nodes to event specifications (ALT 9, ALT 10).
26. The analyst adds a new relationship.
27. The system generates and stores a unique relationship ID.
28. The analyst provides the parent, child, and label fields for relationship.
29. The system stores the new relationship ID with corresponding information.
30. The system renders the newly created relationship on graph (ALT 12, ALT 13).
31. Go to step 26 for multiple relationship additions or continue.
32. The analyst wishes to export their graph image, log entry, and node list.
33. The analyst specifies the desired export format for files.

34. The system exports the files.

[*ALT 6 can be executed from steps 6 – 28.]
[* ALT 11A and ALT 11B can be executed from steps 1 – 28.]

ALT 1: The analyst using the system is a lead.
A1-1: The analyst identifies themselves as the lead for the session.
A1-2: The analyst provides their network adapter's IP address
A1-3: The system stores the provided IP address.
A1-4: Use case continues at step 8.

ALT 2: The system detects if a file falls outside of the validation criteria
A2-1: The system provides the items that require attention to the Enforcement Action Report.
A2-2: The analyst corrects items in the Enforcement Action Report or ignores them.
A2-3: Use case continues at step 13.

ALT 3: The analyst wishes to apply filtering to the system generated log entries.
A3-1: The analyst provides filtering criteria, such as keyword, start, or/and end timestamps.
A3-2: The system stores the analyst-provided filtering criteria.
A3-3: The system applies the filtering criteria to the generated log entries.
A3-4: The system displays the filtered log entries.
A3-4: Use case continues at step 18.

ALT 4: The analyst wishes to sort the system generated log entries.
A4-1: The analyst chooses to sort by the list number, timestamp, event, or vector.
A4-2: The system sorts the log entries by analyst specified field.
A4-3: The system displays the sorted log entries.
A4-4: Use case continues at step 18.

ALT 5: The analyst wishes to add/remove independent nodes for a given vector.
A1-1: The user selects a specific vector.
A1-2: The user add/removes a specific node in a particular vector.
A1-3: The system stores the newly added or newly removed node from specified vector.
A1-4: The system displays the updated node list for vector.
A1-5: Use case continues at step 21.

ALT 6: The analyst wishes to commit recent changes to be saved.
A6-1: The analyst provides a brief description list of the changes to be committed.
A6-2: The system stores the brief description change list
A6-3: The system saves the analysts' current work session.
A6-4: Use case continues at step *.

ALT 7: The analyst wishes to apply filtering to the system nodes.
A7-1: The analyst provides filtering criteria, such as keyword, start, or/and end timestamps.
A7-2: The system stores the analyst-provided filtering criteria.
A7-3: The system applies the filtering criteria to the generated nodes
A7-4: The system displays the filtered node list.
A7-4: Use case continues at step 23.

ALT 8: The analyst wishes to sort the system nodes.
A8-1: The analyst chooses to sort by the Node ID, Node Name, Node Timestamp, Node Description, Log Entry Reference, Creator, Event Type, Icon Type, Source, or Node Visibility.
A8-2: The system sorts the nodes by analyst specified field.
A8-3: The system displays the sorted nodes
A8-4: Use case continues at step 23.

ALT 9: The analyst wishes to change the rendered graph's timeline orientation.
A9-1: The analyst selects between horizontal or vertical orientation.
A9-2: The system stores the selected orientation.
A9-3: The analyst chooses the desired interval unit (Days, Hours, Minutes, Seconds).
A9-4: The system stores the selected interval unit.
A9-5: The analyst chooses a specific interval.
A9-4: The system stores the specified interval.
A9-6: The system renders the graph based on user provided settings.
A9-7: Use case continues at step 26.

ALT 10: The analyst wishes to zoom in/ zoom out on the graph.
A11-1: The analyst selects whether to zoom in or zoom out on current graph.
A11-2: The system renders the graph based on analysts' selection.
A11-3: Use case continues at step 26.

ALT 11A: The analyst wishes to send current session to the DB.
A12A-1: The analyst sends request to push/pull current work session to/from the DB.
A12A-2: The lead approves/declines the pushing to DB.
A12A-3: The system pushes /pulls work to/from the DB.
A12A-3: Use case continues at step *.

ALT 11B: The lead approves/declines push requests from clients.
A12B-1: The system displays a list of pending, client push requests.
A12B-2: The lead accepts/declines push request to DB.
A12B-3: The system merges the work to the DB.
A12B-3: Use case continues at step *.

ALT 12: The analyst wishes to apply filtering to the relationships.
A12-1: The analyst provides filtering criteria, such as label and parent/child IDs.
A12-2: The system stores the analyst-provided filtering criteria.
A12-3: The system applies the filtering criteria to the generated relationships.
A12-4: The system displays the filtered relationships.
A12-5: Use case continues at step 32.

ALT 13: The analyst wishes to sort the system relationships.
A13-1: The analyst chooses to sort by parent, child, or label.
A13-2: The system sorts the relationships by analyst specified field.
A13-3: The system displays the sorted relationships.
A13-4: Use case continues at step 32.