Lab Exercise 11 : Creating and Using Workflow Actions

Description

These steps create GET, POST, and Search workflow actions.

Steps

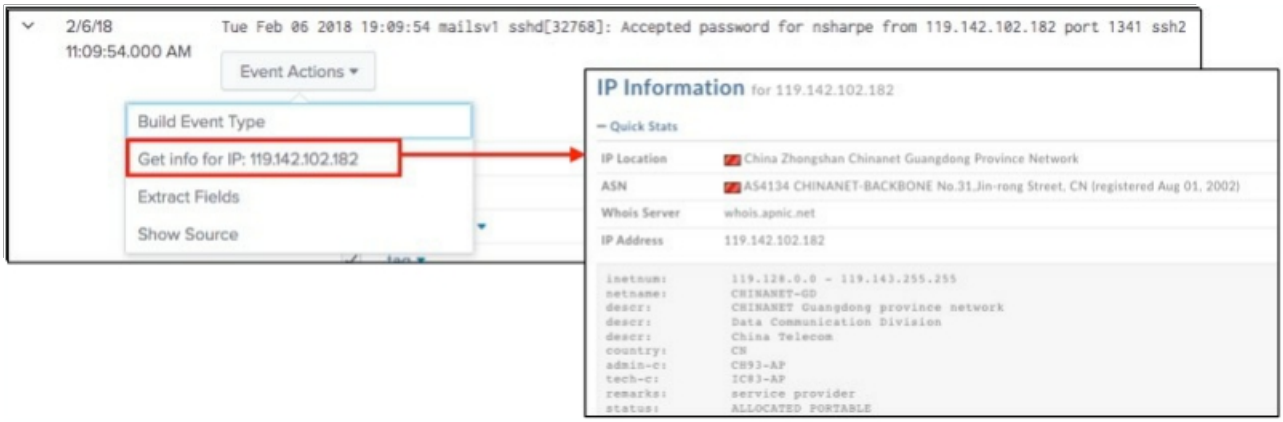
Scenario: **Hackers are continually trying to log into the Linux server. IT Ops analysts need to track ongoing attempts by external sources trying to log in with invalid credentials.**

Task 1: Create a GET workflow action that opens a new browser window with information about the source IP address.

1. Navigate to Settings > Fields > Workflow actions.
2. Click **New Workflow Action** to create a workflow action.
3. For the Destination App, select class_Fund2.
4. For **Name**, type: get_whois_info
5. For **Label**, type: Get info for IP: src_ip
6. For Apply only to the following fields, type: src_ip
7. For **Action type**, make sure link is selected.
8. For **URI**, type: http://who.is/whois-ip/ip-address/src_ip
9. From the **Open link in** dropdown menu, verify New window is selected.
10. From the **Link Method** dropdown menu, verify get is selected.
11. Save your workflow action.
12. Verify your workflow action works as expected. Return to the **CLASS: Intermediate** app and search for `index=security sourcetype=linux_secure src_ip=*` over the **last 24 hours**. (You may need to refresh your browser for the workflow action to appear.)
13. Expand the first event containing a value for `src_ip` and click **Event Actions**.
14. Click **Get info for IP**: {src_ip}. A secondary browser window or tab should open to the URI and display the IP address information.

NOTE: If whois is not behaving as expected, try http://whois.domaintools.com /src.

Results Example:



Task 3: Create a Search workflow action that performs a search for all failed password events associated with a specific IP address.

32. Navigate to Settings > Fields > Workflow actions.
33. Click New Workflow Action.
34. For the Destination App, select **class_Fund2**.
35. For **Name**, type: search_access_by_ipaddress
36. For **Label**, type: Search failed login by IP: src_ip
37. For Apply only to the following fields, type: src_ip
38. From the **Action Type** dropdown menu, select search.
39. In the **Search string** field, type: index=security sourcetype=linux_secure failed src_ip=src_ip
40. From the **Run in app** dropdown, select **class_Fund2**.
41. From the **Run search in** dropdown menu, verify New window is selected.
42. Select the Use the same time range as the search that created the field listing checkbox.
43. Save your workflow action.
44. Verify your workflow action works as expected. Return to the **CLASS: Intermediate** app and search for `index=security sourcetype=linux_secure src_ip=*` over the **last 24 hours**. (You may need to refresh your browser for the workflow action to appear.)
45. Expand an event with an IP address field and click **Event Actions**.
46. Select Search failed login by IP: {src_ip}
47. A secondary search window should open with the search results for the IP address.

Results Example: