IP address attempting a brute force password attack

The origin of a brute force password attack can be important to know when working on the following use cases:

- Reconstructing a website defacement

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- Web server data

Example

A device on your network was hacked into with a brute force password attempt. You want to find out what IP address the attack originated from.

To optimize the search shown below, you should specify an index and a time range. In addition, this sample search uses Splunk Stream. You can replace this source with any other web server data used in your organization.

1. Run the following search:
   ```sh
   sourcetype=stream:http dest="<IP address receiving the request>" http_method=POST |stats count BY src
   ```
2. Expand any event to see all fields.
3. In the form_data field, look at the format the username and password are provided in. Use that format to write a wildcard search for this field and add it to the search. 
   **Example:** If the log shows `form_data username=admin&passwd=123abc` Then a good search term is: `form_data=*username*passwd*`

Stream requires special configuration. If you do not see the fields referenced in this procedure, see the Splunk Stream Installation and Configuration Manual on the Splunk documentation site.

4. Add the following to the search and rerun it:
   ```sh
   |stats count BY src
   ```

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourcetype=stream:http</td>
<td>Search only Stream http data.</td>
</tr>
<tr>
<td>dest=&lt;IP address receiving the request&gt;</td>
<td>Search data going to this IP address.</td>
</tr>
<tr>
<td>http_method=POST</td>
<td>Search for a request pushed to the server. In this case, the request is a password that was pushed from the source.</td>
</tr>
<tr>
<td>form_data=&lt;wildcard search&gt;</td>
<td>Return results that match your wildcard search.</td>
</tr>
<tr>
<td></td>
<td>stats count BY src</td>
</tr>
</tbody>
</table>

Result

The IP address with the most hits is most likely the one the brute force password attack originated from. You can use open source intelligence (OSINT) to find a domain name and other IP addresses associated with the one you found in the investigation.