Web requests to a specific system in your environment

You might need to investigate your own company’s servers and related traffic when doing the following:

- Reconstructing a website defacement

If you need even more basic information about your systems than this procedure provides, learning how to monitor for network traffic outliers might be useful.

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

Your website has suffered a cyber attack and you are investigating. You’ve already identified a suspicious source IP address that may be responsible for the attack, but you aren’t sure which of your web servers is under attack and what suspicious requests to that server were made. You need to investigate.

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:

   src=<IP address sending the request> sourcetype=stream:http

2. In the field sections on the left, find and click dest.

3. Click the value with the highest count to add it to the search.

4. Remove the src field from the search and add the following:

   status=200
   |stats count BY uri
   |sort - count
## 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>src=&lt;IP address sending the request&gt;</td>
<td>Search data coming from this IP address. Logs vary in the information they contain. Not all logs have hostnames or IP addresses. Sometimes the dest field will have a hostname in it but sometimes it will have an IP address. Parentheses and OR statements will broaden your search so you don’t miss anything.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> (src=&quot;192.0.2.0&quot; OR src_ip=&quot;192.0.2.0&quot;)</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> (src=&quot;192.0.2.0&quot; OR src=&quot;example.com&quot;)</td>
</tr>
<tr>
<td>sourcetype=stream:http</td>
<td>Search only Stream http data.</td>
</tr>
<tr>
<td>status=200</td>
<td>Search successful page loads.</td>
</tr>
<tr>
<td></td>
<td>stats count BY uri</td>
</tr>
<tr>
<td></td>
<td>sort - count</td>
</tr>
</tbody>
</table>

## Result

The URI with the most hits is most likely the system that was the target of the attack or that had vulnerabilities the attacker was able to leverage. However, you might need to look into other destination servers that were available in step 2 of this task to investigate the attack thoroughly.