Product or software accessing web server

You might want to investigate the device behind an IP address when doing the following:

- Reconstructing a defacement of your organization’s website

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 certain IP address made a lot of requests to your web server. You suspect that it is a web vulnerability scanner.

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 under investigation> sourcetype=stream:http
   ```

2. In the field sections on the left, find and click `src_header`.
3. Click the value with the highest count to add it to the search.
4. In the field sections on the left, find and click `src_header`.
5. Examine the headers to find the name of the web vulnerability scanner used.

Research any information in the logs that is unfamiliar to you. The log may not directly call out a web vulnerability scanner, but you don’t want to overlook useful information.

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.
### Splunk Search

- `src=<IP address under investigation>`

### Explanation

Search data coming from this IP address.

Logs vary in the information they contain. Not all logs have hostnames or IP addresses. Sometimes the `src` 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.

**Example:**

```
(src="192.0.2.0" OR src_ip="192.0.2.0")
```

**Example:**

```
(src="192.0.2.0" OR src="example.com")
```

- `sourcetype=stream:http`

Search only Stream http data.

### Result

The product used to scan your web server can be useful in subsequent investigation and prevention efforts. Make a note of it.