GCP Kubernetes cluster scan detection

A Kubernetes cluster is a set of worker machines, called nodes, that run containerized applications. A cluster usually runs multiple nodes to provide fault-tolerance and high availability. The cluster master runs the Kubernetes API server, scheduler, and core resource controllers. You might want to look for unauthenticated requests via user agent and authentication data against a GCP Kubernetes cluster when doing the following:

- Detecting Kubernetes scanning activity

Prerequisites

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

- Splunk Enterprise or Splunk Cloud Platform
- Kubernetes
- Pub/Sub message data
- Cloud infrastructure data model
- Splunk Add-on for Google Cloud Platform

Example

One of your concerns with using Kubernetes is unauthenticated requests. You want to know if attackers are targeting your clusters, and, if so, to get suspicious request details, such as IP address, user agent, request URI, and response status data.

To optimize the search shown below, you should specify an index and a time range.

1. Ensure that you have configured stackdriver and set a Pub/Sub subscription to be imported to Splunk.
2. Run the following search:

```splunk
sourcetype="google:gcp:pubsub:message" data.protoPayload.requestMetadata.callerIp!=<valid IP address> data.protoPayload.requestMetadata.callerIp!::1 "data.labels.authorization.k8s.io/decision"=forbid "data.protoPayload.status.message"=PERMISSION_DENIED data.protoPayload.authenticationInfo.principalEmail="system:anonymous"
| rename data.protoPayload.requestMetadata.callerIp AS src_ip
| stats count min(_time) AS firstTime max(_time) AS lastTime values(data.protoPayload.methodName) AS method_name values(data.protoPayload.resourceName) AS resource_name values(data.protoPayload.requestMetadata.callerSuppliedUserAgent) AS http_user_agent BY src_ip data.resource.labels.cluster_name
| rename data.resource.labels.cluster_name AS cluster_name
| convert timeformat="%m/%d/%Y %H:%M:%S" ctime(lastTime)
| convert timeformat="%m/%d/%Y %H:%M:%S" ctime(firstTime)
```

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=&quot;google:gcp:pubsub:message&quot;</td>
<td>Search only GCP Pub/Sub messages.</td>
</tr>
<tr>
<td>data.protoPayload.requestMetadata.callerIp!=&lt;valid IP address&gt;</td>
<td>Exclude a legitimate IP address or range of addresses from the search.</td>
</tr>
<tr>
<td>data.protoPayload.requestMetadata.callerIp!=::1</td>
<td></td>
</tr>
<tr>
<td>&quot;data.labels.authorization.k8s.io/decision&quot;=forbid</td>
<td>Search for an authorization status of forbid.</td>
</tr>
<tr>
<td>&quot;data.protoPayload.status.message&quot;=PERMISSION_DENIED</td>
<td>Search for an authentication status of PERMISSION_DENIED.</td>
</tr>
<tr>
<td>data.protoPayload.authenticationInfo.principalEmail=&quot;system:anonymous&quot;</td>
<td>Search for anonymous users.</td>
</tr>
<tr>
<td></td>
<td>rename data.protoPayload.requestMetadata.callerIp AS src_ip</td>
</tr>
<tr>
<td></td>
<td>stats count min(_time) AS firstTime max(_time) AS lastTime values(data.protoPayload.methodName) AS method_name</td>
</tr>
<tr>
<td></td>
<td>values(data.protoPayload.resourceName) AS resource_name</td>
</tr>
<tr>
<td></td>
<td>values(data.protoPayload.requestMetadata.callerSuppliedUserAgent)AS http_user_agent AS http_user_agent BY src_ip</td>
</tr>
<tr>
<td>data.resource.labels.cluster_name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rename data.resource.labels.cluster_name AS cluster_name</td>
</tr>
</tbody>
</table>
| convert timeformat="%m/%d/%Y %H:%M:%S" ctime(lastTime)
| convert timeformat="%m/%d/%Y %H:%M:%S" ctime(firstTime)

Convert these times into readable strings.

Result

Not all unauthenticated requests are malicious, but the strings provided in this search provide context. Analyze the following to determine what needs further investigation:

- Source IP address reputation, geolocation, and access policy
- Banners in the user agent for scanning tools, such as Zgrab or Nmap
- Targeted files, directories or command strings in the request URI field
- A high number of forbidden, unauthorized, or failure responses

For additional information about this search, such as its applicability to common frameworks and standards, see this project on GitHub.