Azure Kubernetes scan fingerprinting

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 fingerprinting scans from the internet 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
- Azure storage data
- [Splunk Add-on for Microsoft Cloud Services](#)

Example

One of your concerns with using Kubernetes is fingerprinting. You want a search that shows unauthenticated requests via source IP address, user agent, request URI, and response status data against your Kubernetes cluster in Azure.

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

1. Ensure that you have configured Kube-Audit data diagnostics in the Splunk Add-on for Microsoft Cloud Services.
2. Run the following search:

```
sourceType:mscs:storage:blob:json category=kube-audit
| spath input=properties.log
| search responseStatus.code=401
| table sourceIPs{} userAgent verb requestURI responseStatus.reason
```

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.

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.
### Splunk Search

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>category=kube-audit</td>
<td>Search the data source kube-audit from the diagnostic logs in Azure Cloud services.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pull information from this specific Kubernetes audit log.</td>
</tr>
<tr>
<td></td>
<td>Search for HTTP Status 401, an unauthorized request.</td>
</tr>
<tr>
<td></td>
<td>Display the results in a table with columns in the order shown.</td>
</tr>
</tbody>
</table>

### 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](https://github.com/).