Cloud Security Scanner & Windows Containers on Google Compute Engine

Presented By:
Sai Amal Ankem

Google Account

- Login to Google Cloud Console using the Qwiklabs Username and password.
- Accept the terms and conditions.

Agenda

- Introduction
- An overview of Cloud Security Scanner
- An overview of Windows Containers
- Labs on Cloud Security Scanner and Windows Containers
- Conclusion

Introduction: Cloud Security Scanner

- The Cloud Security Scanner identifies security vulnerabilities in your Google App Engine web applications.
- Checks the applications for two common types of vulnerabilities: Cross-Site Scripting(XSS) and mixed content.

How it works?

- To access Google Cloud Security Scanner, navigate to Google Developers Console, select Compute, choose App Engine, and then Security.
- The scanner works by first making a high-speed pass, crawling and parsing the HTML, and then executing a slow and thorough full-page render to find the more complex sections of a site.

Approaches

Google notes that there are two typical approaches to security scans:

- Parse the HTML and emulate a browser. This is fast; however, it comes at the cost of missing site actions that require a full DOM or complex JavaScript operations.
- Use a real browser. This approach avoids the parser coverage gap and most closely simulates the site experience. However, it can be slow due to event firing, dynamic execution, and time needed for the DOM to settle.

Security Command Center

- Helps security teams gather data , identify threats, and act on them before they result in business damage or loss.
- Gives enterprises consolidated visibility into their cloud assets across App Engine, Compute Engine, Cloud Storage, and Datastore.
- Integrates with Google Cloud Platform security tools like Cloud Security Scanner, the Cloud Data Loss Prevention (DLP) API and third-party security solutions from Cloudflare, CrowdStrike, Dome9, Palo Alto Networks, Qualys, and RedLock.
- The DLP API, will let teams identify and redact any piece of sensitive information that may be in applications running on GCP.

Contd..

- The key differentiator for Google is the fact that DLP API for GCP is an extension of DLP for Gmail, and DLP for Drive.
- Google is providing enterprises with security tools to protect the data on applications running within the cloud.
- Amazon, while it has invested in data protection, has focused on the server and block storage level.

Introduction: Running Windows Containers on Compute Engine.

- Container virtualization is a rapidly evolving technology that can simplify how you deploy and manage distributed applications.
- Containers are an isolated, resource controlled, and portable runtime environment which runs on a host machine or virtual machine.
- An application or process which runs in a container is packaged with all the required dependencies and configuration files.
- Gives the illusion that there are no other processes running outside of its container.

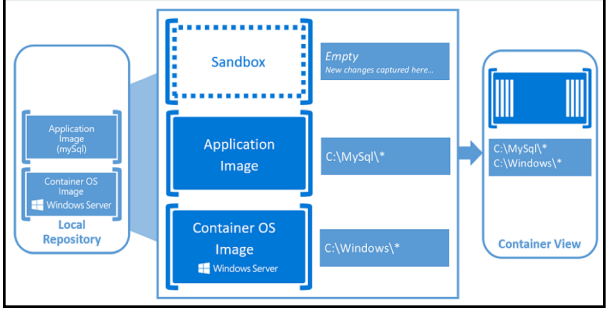
Contd..

- The container's host provisions a set of resources for the container and the container will use only these resources.
- As far as the container knows, no other resources exist outside of what it has been given and therefore cannot touch resources which may have been provisioned for a neighboring container.

Creating Windows Containers

The following key concepts will be helpful as you begin creating and working with Windows Containers.

- Container Host
- Container Image
- Sandbox
- Container OS Image
- Container Repository



Windows Container Types

Windows Containers include two different container types, or runtimes.

Windows Server Containers

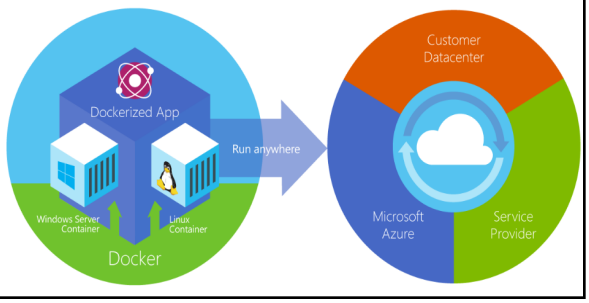
- Provide application isolation through process and namespace isolation technology
- Shares a kernel with the container host and all containers running on the host.
- Do not provide a hostile security boundary and should not be used to isolate untrusted code.

Hyper-V Isolation

- Expands on the isolation provided by Windows Server Containers by running each container in a highly optimized virtual machine.
- The kernel of the container host is not shared with other containers on the same host.
- These containers are designed for hostile multitenant hosting with the same security assurances of a virtual machine.

What is Docker?

- Docker is the vessel by which container images are packaged and delivered.
- This automated process produces images which may then be run anywhere—on premises, in the cloud, or on a personal machine—as a container.



Cloud Security Scanner Lab

- Setup and requirements
- Test App
- Deploy App
- View App
- Run the scan

Running Windows Containers on Compute Engine Lab

- Setup and requirements
- Create a Windows VM for Containers
- Create a Windows Password
- RDP into Windows VM
- Create a HelloWorld PowerShell script
- Create a modified image from the container.
- Run the Windows Container
- Cleanup

References

- https://cloudplatform.googleblog.com/2018/04/how-to-run-Windows-Containers-on-Compute-Engine.html
- https://cloud.google.com/security-scanner/
- https://cloud.google.com/security-command-center/
- https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/


Thank
You For
Listening
Any
Questions?