Docker Image

Nimbusec Server Agent Docker Image

This docker image is intended for use with the Website Security Monitor by KSV1870 Nimbusec (https://nimbusec.com). Use of this image requires an active subscription to Website Security Monitor.

This image is published under https://hub.docker.com/r/ksv1870nimbusec/server-agent

What is Nimbusec Server Agent Docker Image?

Let's answer this question step by step.

Nimbusec Website Security Monitor is a cloud-based monitoring solution to check for malicious malipulations on websites.

Nimbusec Server Agent is the server side component of Website Security Monitor. It checks PHP code that is interpreted on the server and therefore cannot be analysed through http requests (as it is interpreted before being sent to the client).

Nimbusec Server Agent Docker Image is a convenient method of distributing the Server Agent to Nimbusec Customers. Its sole purpose is to run the contained server agent.

Basic Assumptions

The server agent runs unprivileged. Per default it runs with the user id 1000. You can supply any user ID if you need to match the permissions of your scan target. While you can run the container

privileged or as user root, this is strongly discouraged.

Configuration

Nimbusec Server Agent uses a config file to read instructions. This config file adheres to the following structure.

```
{
  "key": "$KEY",
  "secret": "$SECRET",
  "domains": {
    "$DOMAIN": "$TARGET_DIR"
  },
  "tmpfile": "/tmp/nimbusagent-hashes.txt",
  "excludeDir": [],
  "excludeRegexp": [],
  "includeDir": [],
  "includeRegexp": [],
  "apiserver": "$API_SERVER"
}
```

All $-Placeholders need to be provided except for $TARGET_DIR and $API_SERVER. For these two this docker image can fall back on the following default values:

- $TARGET_DIR: /app/scan
- $API_SERVER: https://api.nimbusec.com

In addition to the configuration options listed above there is one setting that can only be enabled via Environment Variable in this image. Adding the env `YARA=true` will enable the optional support for yara scan rules. The ruleset is downloaded from the API Server when the server agent is executed.

For additional Information please refer to the Knowledge Base.

Mount your own agent.conf

The most flexible way to provide a configuration is to mount to the container-path /app/agent.config (please note, this path and filename is mandatory). This mount can be read-only

You need to replace the $KEY an $SECRET placeholders from the above example with the corresponding values provided by KSV1870 Nimbusec. For $DOMAIN you can select any Domain that you have configured in your Nimbusec Website Security Monitor Account. Please note, you have to use the correct Style of the domain, i.e. example.com and www.example.com are treated as different domains.

```
docker run -v /local_path_to_config/agent.conf:/app/agent.conf:ro -v /var/www/html:/app/scan:ro <dockerimage>
```

This example mounts a local config file and the scan dir of /var/www/html into the container, both read-only.

Pass Environment Variables

If you don't want to provide a custom config file you can pass the Placeholder values (KEY, SECRET, DOMAIN and optionally TARGET_DIR) as environment variables (docker via -e, docker-compose via environment).

```
docker run -v /var/www/html:/app/scan:ro -e KEY=api-key -e SECRET=api-secret -e DOMAIN=example.com <dockerimage>
```

This example mounts the target /var/www/html into the container and provides key, secret and domain via enviroment variable.

What gets scanned?

The directory to scan needs to be mounted into the container, either into the default location /app/scan or in a custom directory which is specified via your agent.conf or the TARGET_DIR environement variable. This mount should be read-only. The server agent will not write into this directory.

```
docker run -v /local_path_to_config/agent.conf:/app/agent.conf:ro -v /var/www/html:/mnt/html:ro -e TARGET_DIR=/mnt/html -e YARA=true <dockerimage>
```

This example mounts the local config file and the target dir into the container. As the target dir in the container is different from /app/scan we have to specify the container directory to scan as /mnt/html. In addition the YARA env variable enables yara support and downloads the scan rules form the api server.

Recommendations

- It is recommended that you prefer mounting your own agent.conf file over environment variables. It is easier for you to check what the agent is doing where. Additionally you can scan multiple domains with one config. This is not possible with the env variables.
- It is recommended to mount the scan directory under /app/scan. Fallbacks will assume this directory if there is misconfiguration.
- It is recommended to mount all files and directories mentioned so far as read-only. There is one optional exception which is explained in the following "Advanced" section.

Advanced

If you want additional insight into the workings of the server agent you can mount the container tmp dir to a local directory. This mount has to be read/write and has to have these permissions for the User ID that runs the agent (either 1000 or a value that you can set via the -u/--user flag).

```
docker run -v /local_path_to_config/agent.conf:/app/agent.conf:ro -v /var/www/html:/app/scan:ro -u 1234 <dockerimage>
```

Assuming that the data in the local directory /var/www/html is only readable to user ID 1234, you can provide this ID to the docker container. The server agent in the container is executed with the user ID 1234.

Revision #2
Created 2023-01-23 14:47:41 UTC by Christof Horschitz
Updated 2023-02-01 13:17:34 UTC by Christof Horschitz