
ATTACK
DEFENSE
by PentesterAcademy

Name	Flag File Forensic Recovery I
URL	https://www.attackdefense.com/challengedetails?cid=1036
Type	DevSecOps : Docker Image Forensics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

Step 1: Run container-diff tool on given exported image tar archive to see the image history.

Command: container-diff analyze -t history challenge-image.tar

```
root@attackdefense:~# container-diff analyze -t history challenge-image.tar

-----History-----

Analysis for challenge-image.tar:
-/bin/sh -c #(nop) ADD file:1d7cb45c4e196a6a84319b976b95ce1a9037c40b085e88350c071bf27ff59166 in /
-/bin/sh -c set -xe                && echo '#!/bin/sh' > /usr/sbin/policy-rc.d         && echo 'exit 101' >> /usr/sbin/policy-rc.d         &&
chmod +x /usr/sbin/policy-rc.d                && dpkg-divert --local --rename --add /sbin/initctl         && cp -a /usr/sbin/policy-rc.d /sbin
/initctl         && sed -i 's/^exit.*/exit 0/' /sbin/initctl                && echo 'force-unsafe-io' > /etc/dpkg/dpkg.cfg.d/docker-apt-speedu
p                && echo 'DPkg::Post-Invoke { "rm -f /var/cache/apt/archives/*.deb /var/cache/apt/archives/partial/*.deb /var/cache/apt/*.bin
|| true"; };' > /etc/apt/apt.conf.d/docker-clean         && echo 'APT::Update::Post-Invoke { "rm -f /var/cache/apt/archives/*.deb /var/cache/ap
t/archives/partial/*.deb /var/cache/apt/*.bin || true"; };' >> /etc/apt/apt.conf.d/docker-clean         && echo 'Dir::Cache::pkgcache ""; Dir::
Cache::srcpkgcache "";' >> /etc/apt/apt.conf.d/docker-clean                && echo 'Acquire::Languages "none";' > /etc/apt/apt.conf.d/docker-n
o-languages                && echo 'Acquire::GzipIndexes "true"; Acquire::CompressionTypes::Order:: "gz";' > /etc/apt/apt.conf.d/docker-gzip-i
ndexes                && echo 'Apt::AutoRemove::SuggestsImportant "false";' > /etc/apt/apt.conf.d/docker-autoremove-suggests
-/bin/sh -c rm -rf /var/lib/apt/lists/*
-/bin/sh -c mkdir -p /run/systemd && echo 'docker' > /run/systemd/container
-/bin/sh -c #(nop)  CMD ["/bin/bash"]
-/bin/sh -c #(nop)  ENV name=docker-forensics-challenges
-/bin/sh -c apt-get update
-/bin/sh -c apt-get install -y git vim curl
-/bin/sh -c apt-get install -y python python-pip
-/bin/sh -c cd /tmp/      && echo -e "C H E C K S U M  I S  F L A G" | md5sum > /var/log/system     && echo -e "C H E C K S U M  I S  F L A G"
 > /var/log/system     && md5sum /bin/bash >> /var/log/system     && rm -rf /tmp/*     && cd /var/log     && mv system /bin/shell     && chmod
+x /bin/shell
-/bin/sh -c #(nop) COPY file:39255a7bef4f40baa69ce1885aa878dd2197916a81898269c4b1fefca161123d in /root/
-/bin/sh -c apt-get install -y python python-pip
-/bin/sh -c cd /bin/     && echo "" > shell     && export Message="Work done"
-/bin/sh -c #(nop)  CMD ["/bin/bash"]
```

Step 2: In the last step, we can observe that a checksum based flag is being stored in /bin/shell file but then it is overwritten in another step. Hence, to get the intermediate layer files, extract the tar.

Command: tar -xf challenge-image.tar

```
root@attackdefense:~#
root@attackdefense:~# tar -xf challenge-image.tar
root@attackdefense:~#
root@attackdefense:~# ls -l
total 547312
drwxr-xr-x 2 root root      4096 May 16 08:34 0c2700e1746632deae7692e58f5520c58a1801ab96594af4778d2e31e1e9b98c
drwxr-xr-x 2 root root      4096 May 16 08:34 104db4e0ff6a882a2324da90077a7dfa8675c49a56bda96768f7e28a5f6fa2a4
drwxr-xr-x 2 root root      4096 May 16 08:34 265e3bda6270bd8e644df9ac4846066370a79b85a49ab3632253e74986439990
-rw-r--r-- 1 root root      5429 May 16 08:34 34aa96f7c288ef570e69b53c82d79b8e6d64d488276424933bd81c7bade7929a.json
drwxr-xr-x 2 root root      4096 May 16 08:34 4b9741f7bf29a86bab634f792ca6993c4d81a3b884e15e999a10c2b10027d209
drwxr-xr-x 2 root root      4096 May 16 08:34 55f08f99dfd3ba11cdf9db2ab10176018657bf058f2c0f55febb10f498c887df
drwxr-xr-x 2 root root      4096 May 16 08:34 5fcfe5b5c9e569ded9792636cac9d7ba67bccef4f3d1c38a964bccd01b089f50
drwxr-xr-x 2 root root      4096 May 16 08:34 7001fa465b500162f585a14507474f46afaf424d4e9af13f04b8ff370c90e957
drwxr-xr-x 2 root root      4096 May 16 08:34 70b8c620a0c5a11ba0334324524b1456d3454df23f0413ff61a4f8a60b751958
drwxr-xr-x 2 root root      4096 May 16 08:34 a7571220d942ea41ecb3c1e8b74fb690de817ea02b127e23df74f1be7eeb5f3f
-rw------- 1 root root 560378880 May 16 08:34 challenge-image.tar
drwxr-xr-x 2 root root      4096 May 16 08:34 d38b836a492ad9adfe0e97b58d0f894d0ae3f7a381d561e86d7d588b20da864a
drwxr-xr-x 2 root root      4096 May 16 08:34 fb2d4623281f3a75ee458900ddb41a7e706cef3bdd0dbf80c4b91a6dfe1304a7
-rw-r--r-- 1 root root       981 Jan  1  1970 manifest.json
-rw-r--r-- 1 root root        98 Jan  1  1970 repositories
root@attackdefense:~#
```

Step 3: Check manifest file to know about the ordering of the layers.

Command: cat manifest.json | python -m json.tool

```
root@attackdefense:~#
root@attackdefense:~# cat manifest.json | python -m json.tool
[
    {
        "Config": "34aa96f7c288ef570e69b53c82d79b8e6d64d488276424933bd81c7bade7929a.json",
        "Layers": [
            "70b8c620a0c5a11ba0334324524b1456d3454df23f0413ff61a4f8a60b751958/layer.tar",
            "55f08f99dfd3ba11cdf9db2ab10176018657bf058f2c0f55febb10f498c887df/layer.tar",
            "fb2d4623281f3a75ee458900ddb41a7e706cef3bdd0dbf80c4b91a6dfe1304a7/layer.tar",
            "5fcfe5b5c9e569ded9792636cac9d7ba67bccef4f3d1c38a964bccd01b089f50/layer.tar",
            "0c2700e1746632deae7692e58f5520c58a1801ab96594af4778d2e31e1e9b98c/layer.tar",
            "7001fa465b500162f585a14507474f46afaf424d4e9af13f04b8ff370c90e957/layer.tar",
            "265e3bda6270bd8e644df9ac4846066370a79b85a49ab3632253e74986439990/layer.tar",
            "4b9741f7bf29a86bab634f792ca6993c4d81a3b884e15e999a10c2b10027d209/layer.tar",
            "a7571220d942ea41ecb3c1e8b74fb690de817ea02b127e23df74f1be7eeb5f3f/layer.tar",
            "104db4e0ff6a882a2324da90077a7dfa8675c49a56bda96768f7e28a5f6fa2a4/layer.tar",
            "d38b836a492ad9adfe0e97b58d0f894d0ae3f7a381d561e86d7d588b20da864a/layer.tar"
        ],
        "RepoTags": [
            "challenge-image:latest"
        ]
    }
]
root@attackdefense:~#
```

Step 4: On correlating the output of history command (step 1) with manifest file, the layer of interest seems to be 4th from the bottom (in manifest file listing). Change to the layer directory and extract the layer.

```
root@attackdefense:~#
root@attackdefense:~# cd 4b9741f7bf29a86bab634f792ca6993c4d81a3b884e15e999a10c2b10027d209
root@attackdefense:~/4b9741f7bf29a86bab634f792ca6993c4d81a3b884e15e999a10c2b10027d209# ls -l
total 12
-rw-r--r-- 1 root root    3 May 16 08:34 VERSION
-rw-r--r-- 1 root root  477 May 16 08:34 json
-rw-r--r-- 1 root root 3584 May 16 08:34 layer.tar
root@attackdefense:~/4b9741f7bf29a86bab634f792ca6993c4d81a3b884e15e999a10c2b10027d209# tar -xf layer.tar
root@attackdefense:~/4b9741f7bf29a86bab634f792ca6993c4d81a3b884e15e999a10c2b10027d209# ls -l
total 20
-rw-r--r-- 1 root root    3 May 16 08:34 VERSION
drwxr-xr-x 2 root root 4096 May 16 08:34 bin
-rw-r--r-- 1 root root  477 May 16 08:34 json
-rw-r--r-- 1 root root 3584 May 16 08:34 layer.tar
drwxr-xr-x 3 root root 4096 Mar  7 21:01 var
root@attackdefense:~/4b9741f7bf29a86bab634f792ca6993c4d81a3b884e15e999a10c2b10027d209#
```

Step 5: Check the content of bin/shell file to retrieve the flag.

Command: cat bin/shell

```
root@attackdefense:~/4b9741f7bf29a86bab634f792ca6993c4d81a3b884e15e999a10c2b10027d209#
root@attackdefense:~/4b9741f7bf29a86bab634f792ca6993c4d81a3b884e15e999a10c2b10027d209# cat bin/shell
-e C H E C K S U M  I S  F L A G
5b62133afdcb9e96015f8679888f4434  /bin/bash
root@attackdefense:~/4b9741f7bf29a86bab634f792ca6993c4d81a3b884e15e999a10c2b10027d209#
```

Flag: 5b62133afdcb9e96015f8679888f4434

References:

1. Docker (https://www.docker.com/)
2. Container-diff (https://github.com/GoogleContainerTools/container-diff)