ATTACK DEFENSE

by PentesterAcademy

Name	System Backdoor
URL	https://attackdefense.com/challengedetails?cid=1454
Type	Docker Security : Docker Forensics

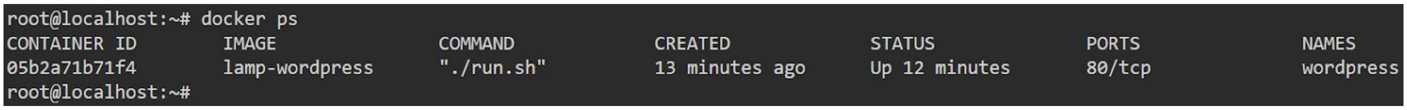
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: **Study the changes made by the attacker and find the backdoor?**

Solution:

Step 1: Check running containers

Command: docker ps

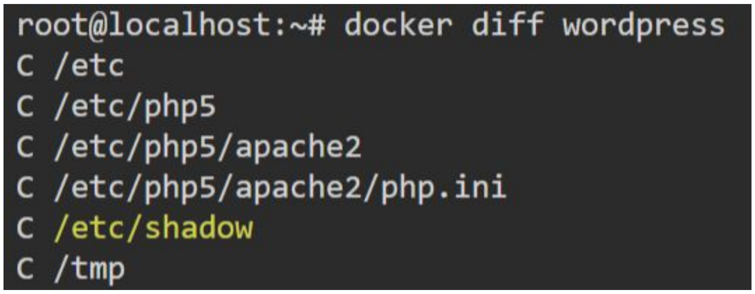


```
root@localhost:~# docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS              PORTS               NAMES
05b2a71b71f4        lamp-wordpress      "./run.sh"          13 minutes ago      Up 12 minutes       80/tcp              wordpress
root@localhost:~#
```

A wordpress container is running on the host.

Step 2: Check the changes made to the container after starting. Docker diff command can take container_name or container_id

Command: docker diff wordpress

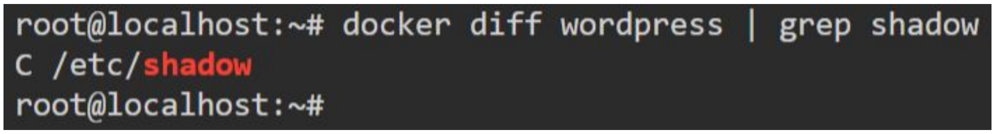


```
root@localhost:~# docker diff wordpress
C /etc
C /etc/php5
C /etc/php5/apache2
C /etc/php5/apache2/php.ini
C /etc/shadow
C /tmp
```

.

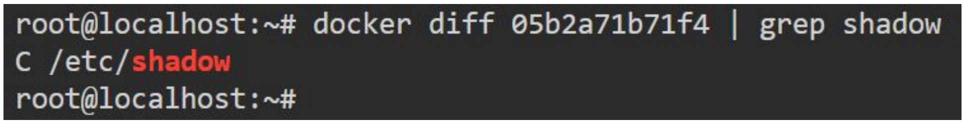
Step 3: One can observe that shadow file is changed. One can also use grep to see the results.

Commands: docker diff wordpress | grep shadow



```
root@localhost:~# docker diff wordpress | grep shadow
C /etc/shadow
root@localhost:~#
```

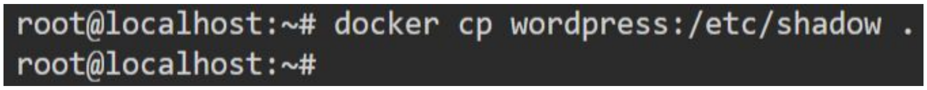
Commands: docker diff 05b2a71b71f4 | grep shadow



```
root@localhost:~# docker diff 05b2a71b71f4 | grep shadow
C /etc/shadow
root@localhost:~#
```

Step 4: Copy the shadow file from the container to the host machine.

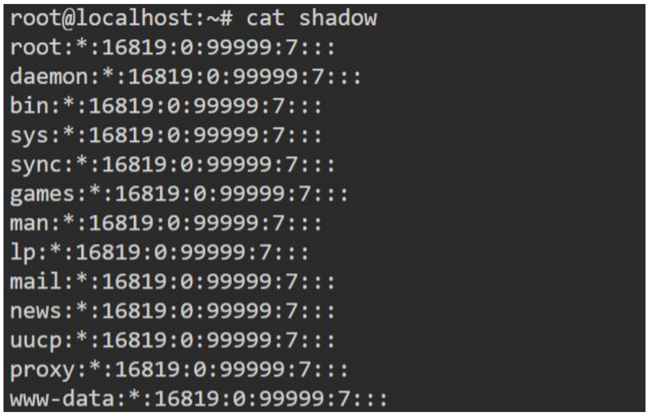
Command: docker cp wordpress:/etc/shadow .



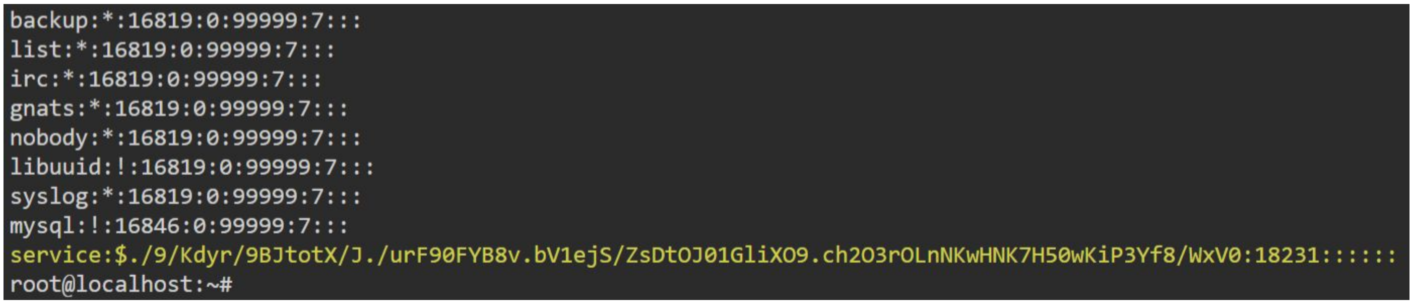
```
root@localhost:~# docker cp wordpress:/etc/shadow .
root@localhost:~#
```

Step 5: Check the contents of the copied shadow file.

Command: cat shadow



```
root@localhost:~# cat shadow
root:*:16819:0:99999:7:::
daemon:*:16819:0:99999:7:::
bin:*:16819:0:99999:7:::
sys:*:16819:0:99999:7:::
sync:*:16819:0:99999:7:::
games:*:16819:0:99999:7:::
man:*:16819:0:99999:7:::
lp:*:16819:0:99999:7:::
mail:*:16819:0:99999:7:::
news:*:16819:0:99999:7:::
uucp:*:16819:0:99999:7:::
proxy:*:16819:0:99999:7:::
www-data:*:16819:0:99999:7:::
```

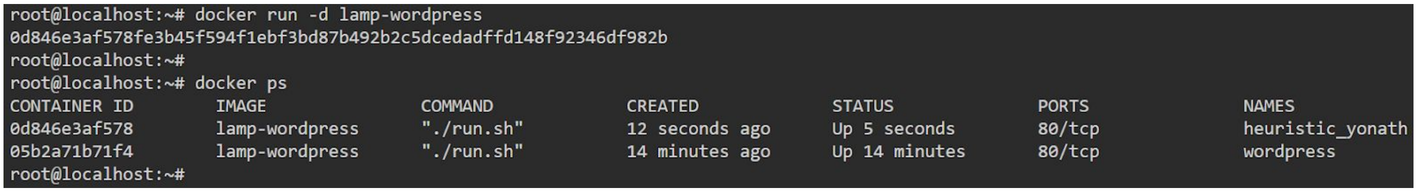


```
backup:*:16819:0:99999:7:::
list:*:16819:0:99999:7:::
irc:*:16819:0:99999:7:::
gnats:*:16819:0:99999:7:::
nobody:*:16819:0:99999:7:::
libuuid:!:16819:0:99999:7:::
syslog:*:16819:0:99999:7:::
mysql:!:16846:0:99999:7:::
service:$./9/Kdyr/9BJtotX/J./urF90FYB8v.bV1ejS/ZsDtOJ01GliXO9.ch2O3rOLnNKwHNK7H50wKiP3Yf8/WxV0:18231:::::
root@localhost:~#
```

The last line seems to be appended. The same can be verified by starting another container from the lamp-wordpress image and checking the /etc/shadow

Step 6: Start a new container from "lamp-wordpress" docker image

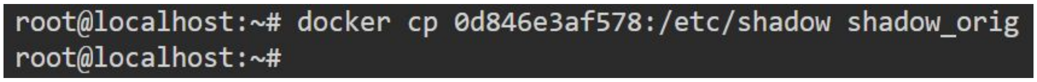
Commands:
docker run -d lamp-wordpress
docker ps



```
root@localhost:~# docker run -d lamp-wordpress
0d846e3af578fe3b45f594f1ebf3bd87b492b2c5dcedadffd148f92346df982b
root@localhost:~#
root@localhost:~# docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS              PORTS               NAMES
0d846e3af578        lamp-wordpress      "./run.sh"          12 seconds ago      Up 5 seconds        80/tcp              heuristic_yonath
05b2a71b71f4        lamp-wordpress      "./run.sh"          14 minutes ago      Up 14 minutes       80/tcp              wordpress
root@localhost:~#
```

Step 7: Copy shadow file out from the newly created container. Save it as shadow_orig so to make sure it doesn't overwrite the other shadow file.

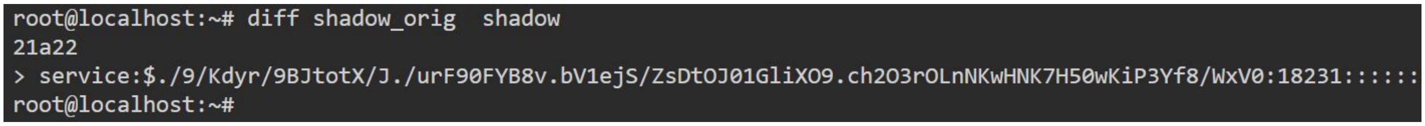
Command: docker cp 0d846e3af578:/etc/shadow shadow_orig



```
root@localhost:~# docker cp 0d846e3af578:/etc/shadow shadow_orig
root@localhost:~#
```

Step 8: Use diff tool to check the modification

Command: diff shadow_orig shadow



```
root@localhost:~# diff shadow_orig  shadow
21a22
> service:$./9/Kdyr/9BJtotX/J./urF90FYB8v.bV1ejS/ZsDtOJ01GliXO9.ch2O3rOLnNKwHNK7H50wKiP3Yf8/WxV0:18231::::::
root@localhost:~#
```

Added user: service