**Metasploitable 2**

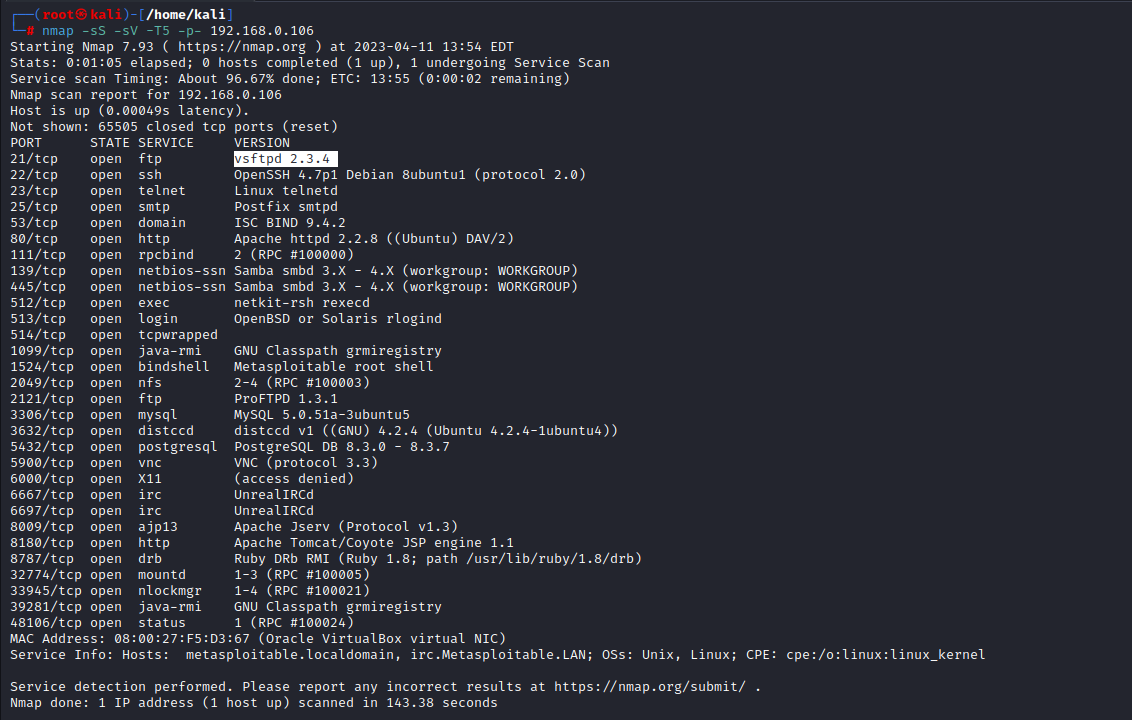
Submitted By:- Binay Chaudhary

Submitted to:- Er. Suman Basnet Sir

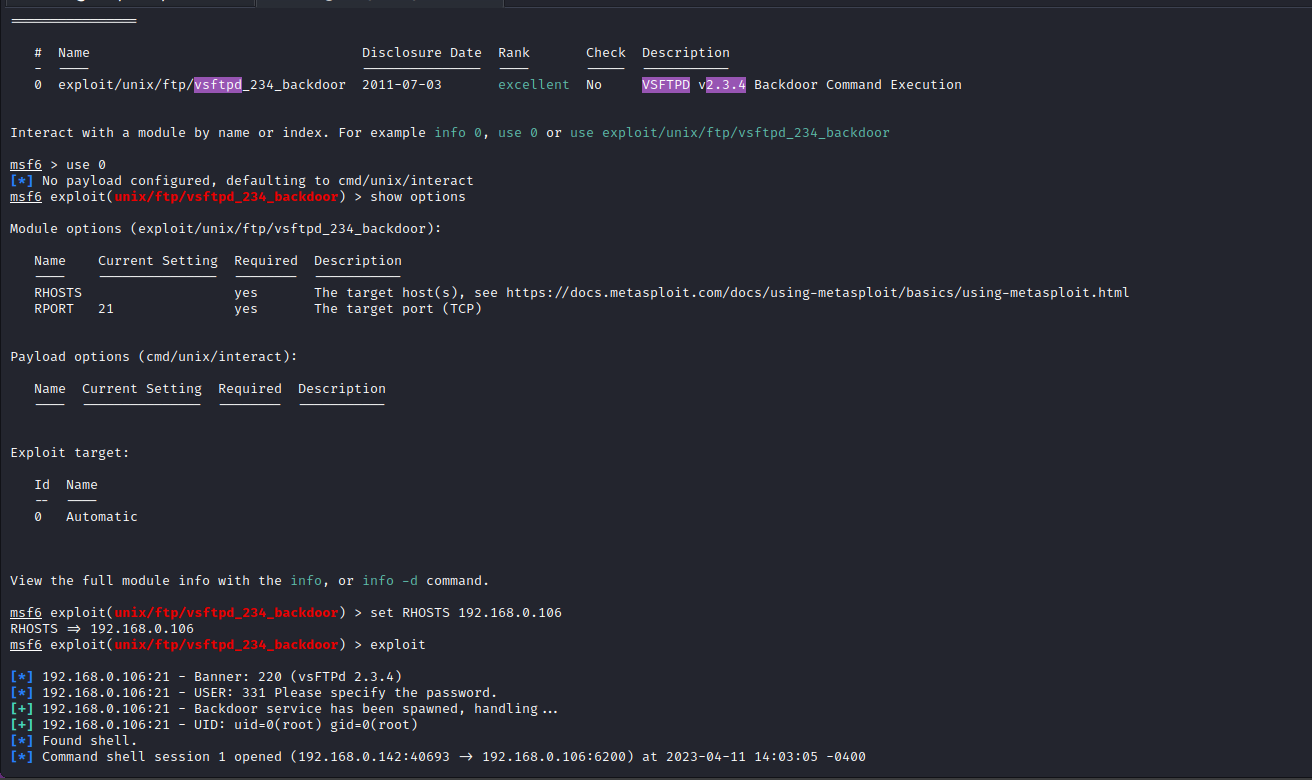
Table of Contents Page no.

**Nmap**

Nmap is a short form of Network Mapper and it's an open-source tool that is used for mapping networks, auditing and security scanning of the networks. The reason behind its development is to quickly find large networks at a specific location. For the discovery of networks, the raw IP packets are used by Nmap.

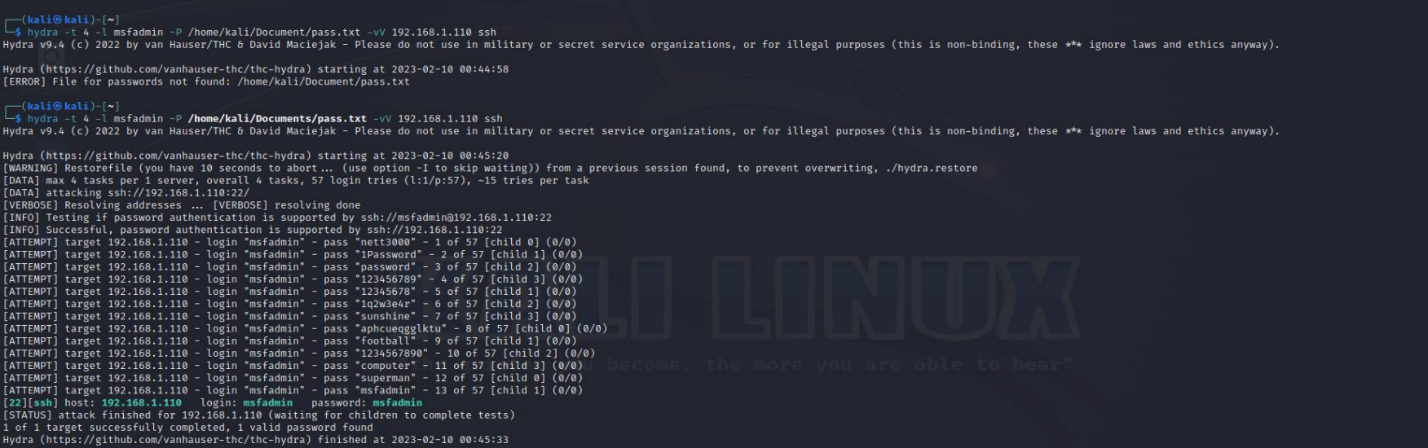


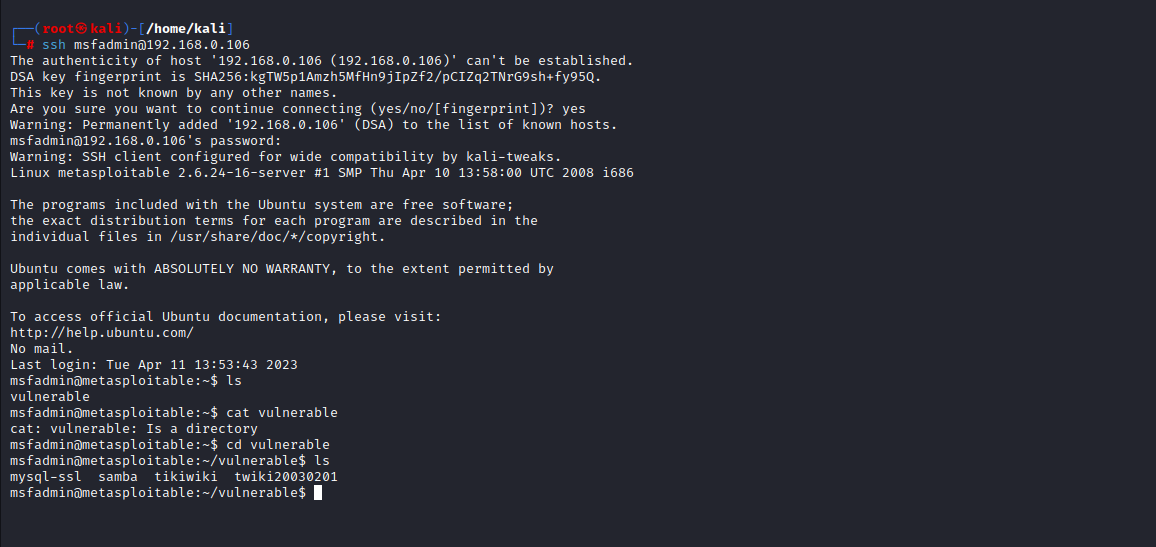
**vsftpd 2.3.4**

Here, we’ve searched for the exploit of the version which is shown on the port 21 i.e. ftp version and after searching the exploit we have found 1 exploit server i.e. in the version of the ftp server.

After that we have exploited the version of ftp i.e. available.

**SSh (secure shell)**

****Here, we’ve done the brute force attack through hydra and we,ve found the password through hydra.

**** Here, in this picture we can see that we’ve logged in the msfadmin accounts through his weak credentials that can be guessable and can login anyone through the ssh.

Here, we’ve found the password and we’ve logged in the msfadmin account.

Linux telnetd

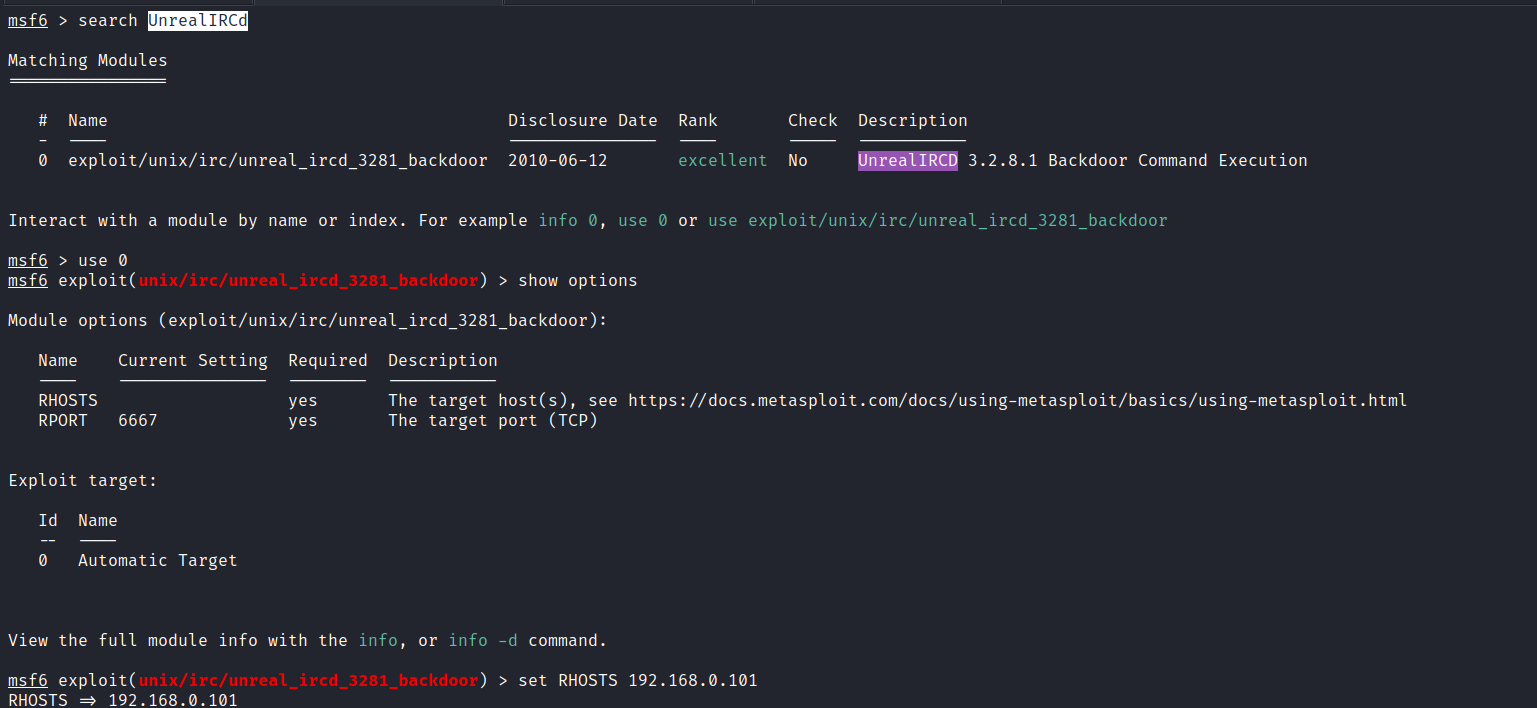
Here, as we know we’ve bruteforced the password with the help of hydra tool i.e. username:- msfadmin and the password is msfadmin.

 Now, we can login through the telnet and through the ip so let’s do login.

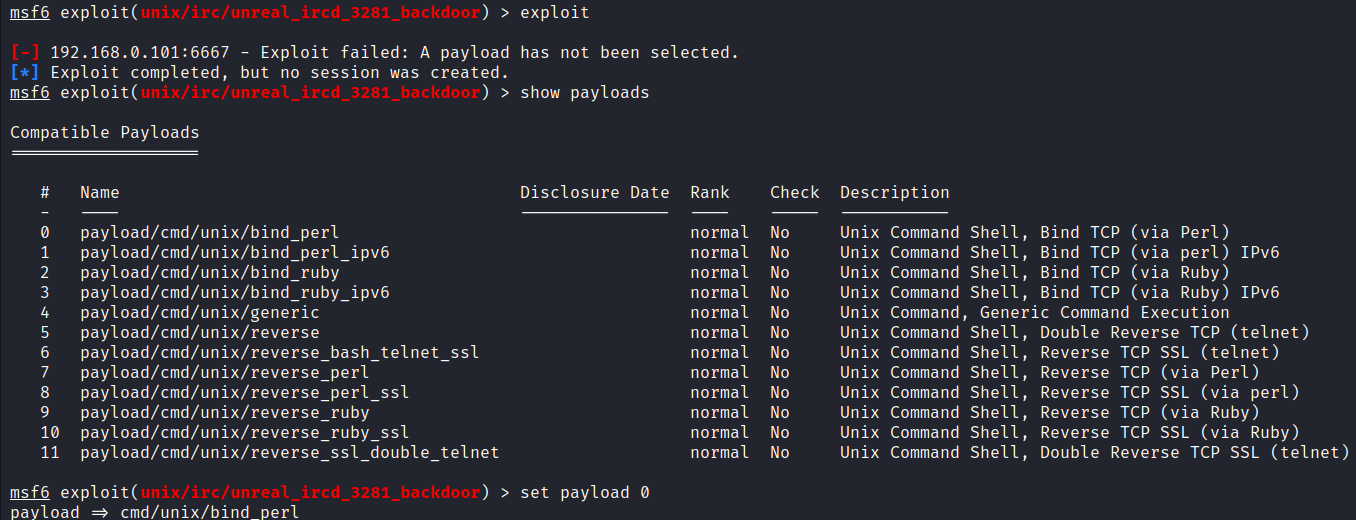
From here above pics, we’ve found that we can easily login through the weak credentials and can access the files on the that port.

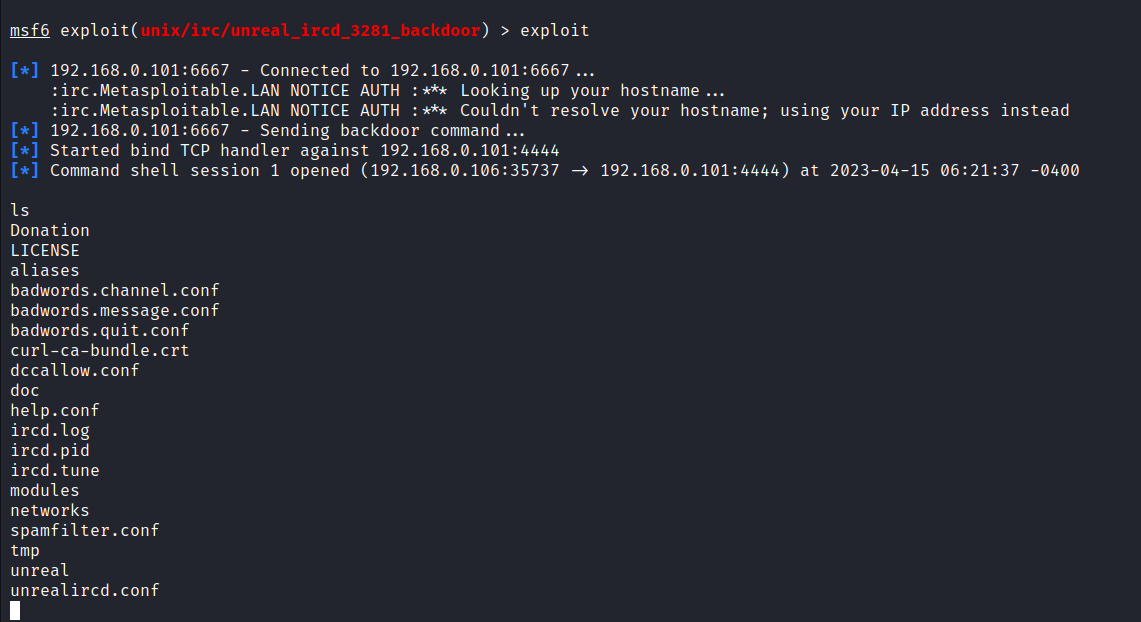
**UnrealIRCd**

Here, in this picture we have found the UnrealIRCd at the port no. 6697. So, we’ve searched for the exploit and found 1 exploit so, let’s begin to exploit if it is possible.



Here, we’ve found that it required for the payloads and we’ve founded the payloads and let’s try with the payload one by one if it exploit or not.



 Here, After we have set the payload we’ve found that we have connected to the server.

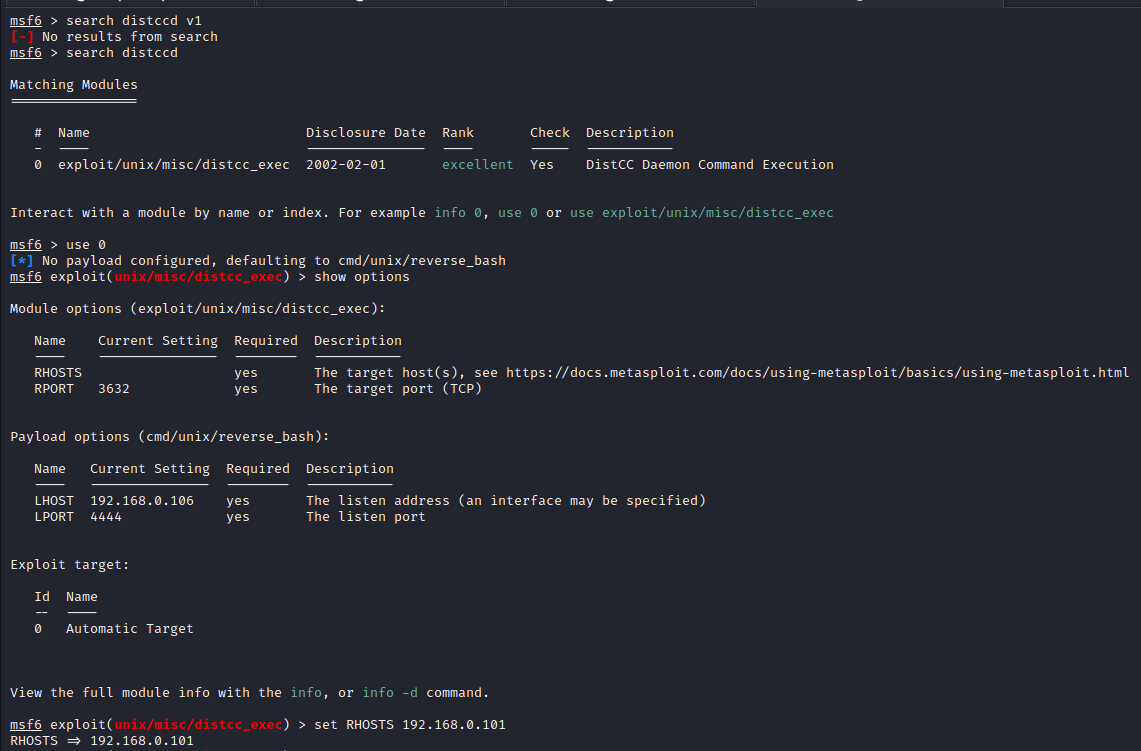
After some time we have connected and now, we can view the files on that port that can be shared and can access by the attacker.

**Apache Tomcat**

Here, this is a service of http at port no. 8180/tcp we’ve tried for the exploitation but this port not. Is not vulnerable tried all the payloads to exploit but dinn’t exploited it, so this port is not vulnerable.

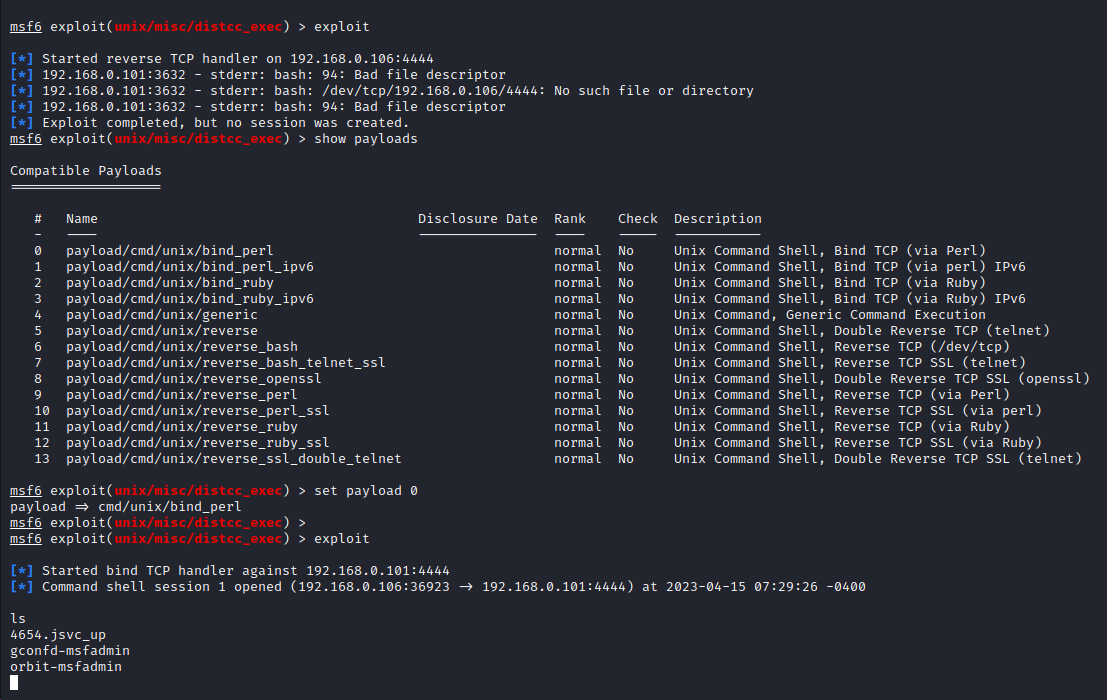
**distccd**

Here, after a time we’ve found the shell i.e. is opened at the port 3632/tcp.



Here, after all we have tried the payloads to exploit it. And we’ve done exploiting it with the payload and we can access the fine in that port that it is

Hackable by the hacker and this port can make a company huge losses.



As we can see that we can see the username and the password. That can an attacker can directly login in the admin page.