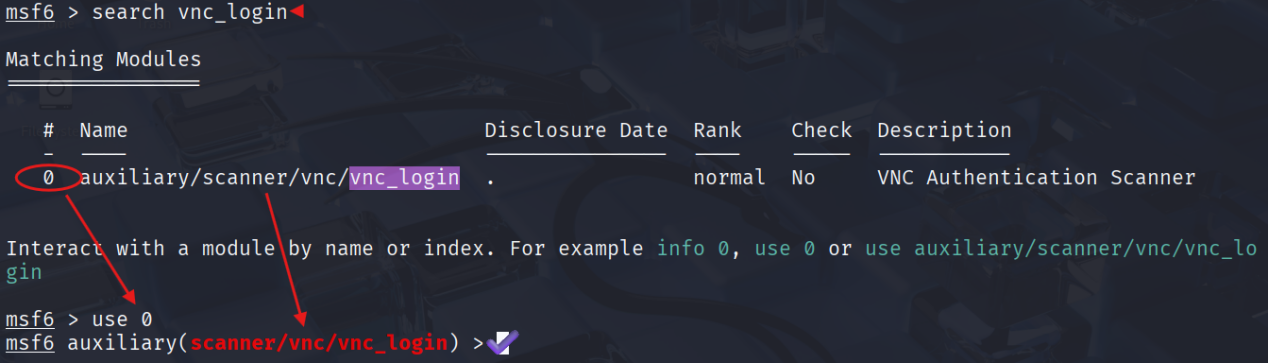
Auxiliary modules are tools that perform actions other than directly exploiting a vulnerability to gain access. They are used to gather information about the target system, scan for vulnerabilities, conduct denial-of-service attacks, or perform other supporting tasks that are not directly related to exploitation.

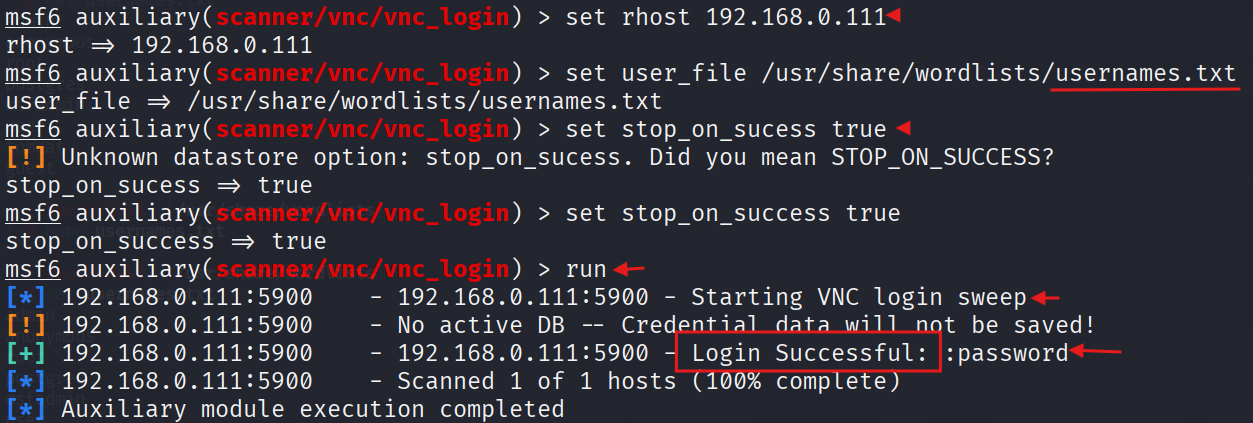
Using auxiliary we are breaking into VNC : Attacker system : Kali

Target system : Metasploitable 2

We running msfconsole to use the auxiliary on attacker system, we need to search the auxiliary using a specific pattern. “search service type” example : Search ftp\_login. Similarly we can change the service as per your need and run the attack.



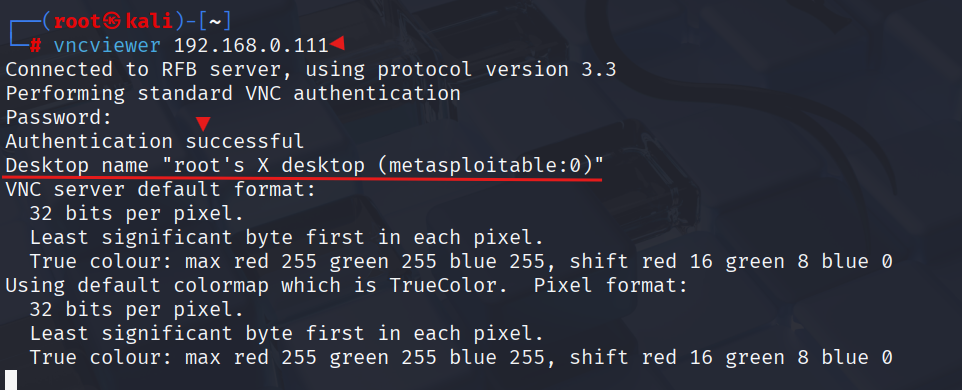
Now we will set the rhosts, set to stop the attack once it got the correct username and password , we can also set to print output for all attempts. And we need to set username and password files as well to the auxiliary.



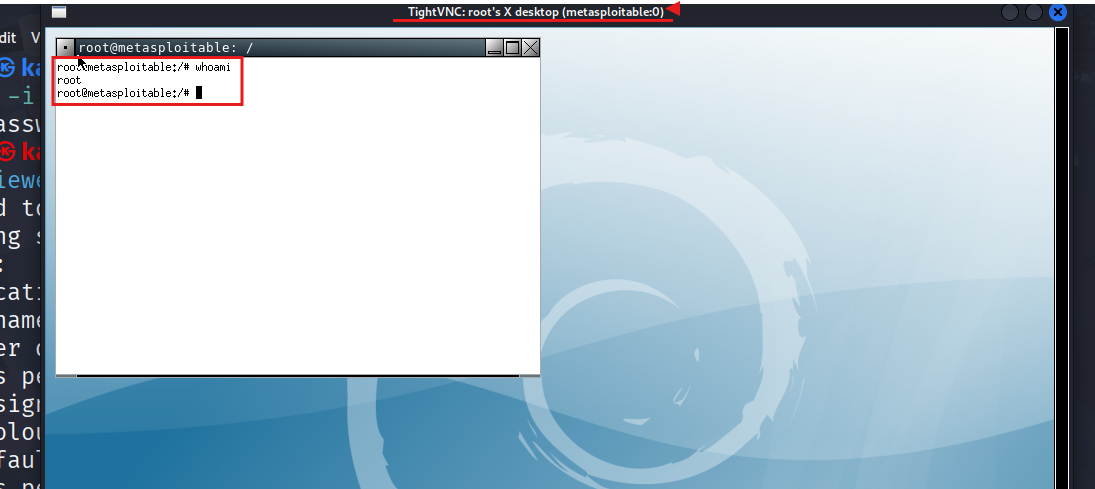
What is happening above is that the module is trying to login using the default credentials on its list against 192.168.0.111 : 5900

# **EXPLOITATION :**

Now let us try to connect remotely to the target. Opening up a terminal and running the command vncviewer 192.168.0.111



a graphical user interface of the vnc connection will pop up as shown below



we can see that we logged in as root. effectively here, we have access to the system. As a root user, we can do whatever we want to the system. Here Metasploitable 2 was exploited because of using a poor password.