Gain SSH Access to Servers by Brute-Forcing Credentials:

Scan with Nmap:

A screenshot of a computer program

Description automatically generated

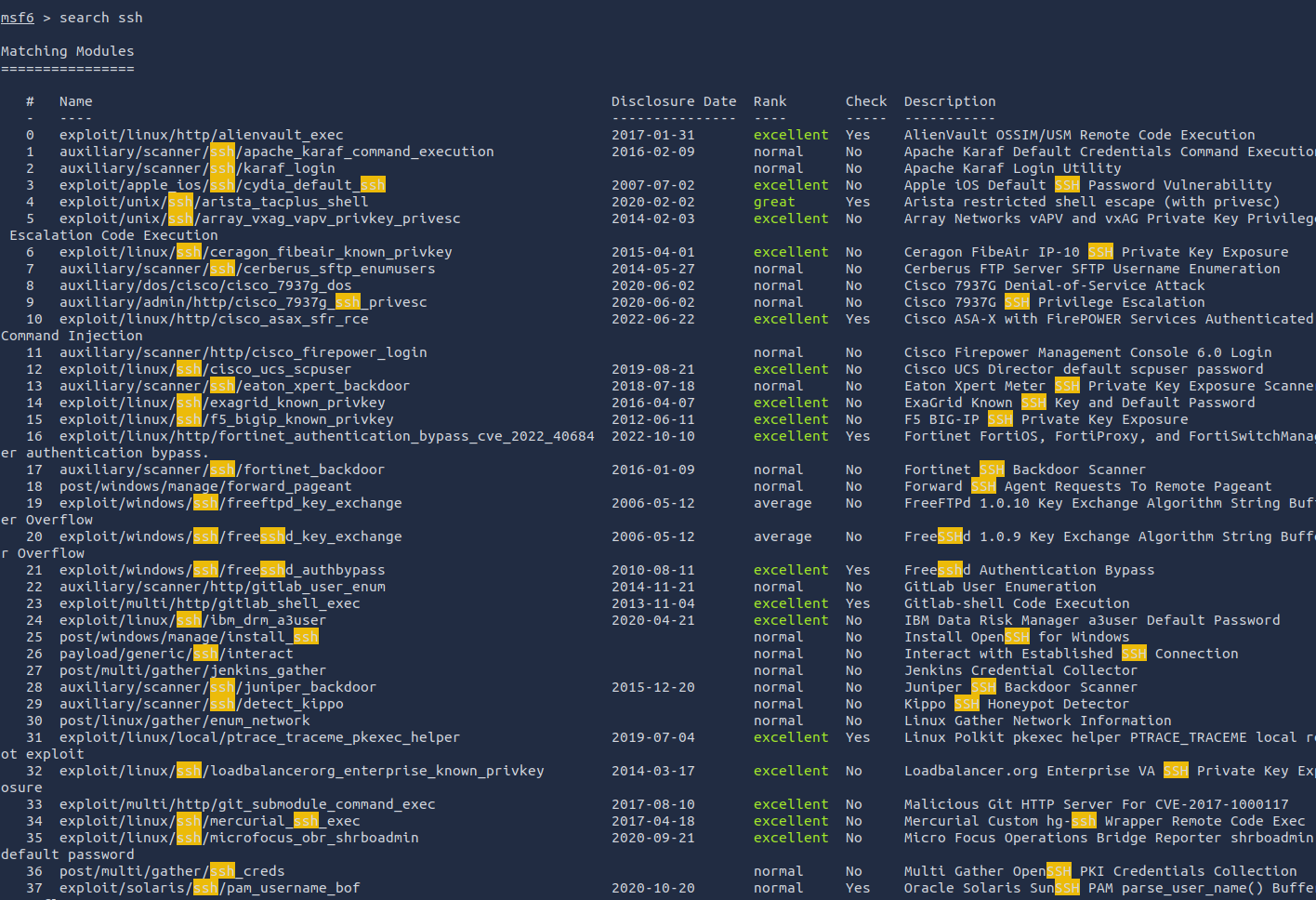
we can see that port 22 is open and the SSH service is running on it. It would be a waste of time if this was closed or not running at all. Now we can start brute-forcing.

Open Metasploit:

A screenshot of a computer program

Description automatically generated

Msf6 > search ssh



A screen shot of a computer

Description automatically generated

Select the aux scanner option for ssh\_login to use to exploit and perform Brute Force



Use command ssh\_login to equip the command



Once its equipped it will show



Type in options to see what the available settings for the scanner

A screenshot of a computer screen

Description automatically generated

We need to set some targets for the brute force to work

First, **RHOSTS** is the ip address of our target

Next, STOP\_ON\_SUCCESS will stop once the scan finds the valid credentials



Then, USER\_FILE is the list of usernames



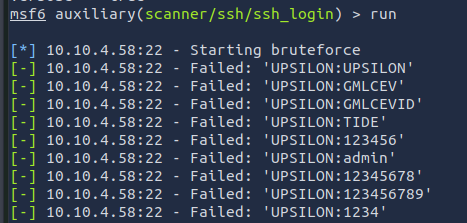
And PASS\_FILE is the list of passwords



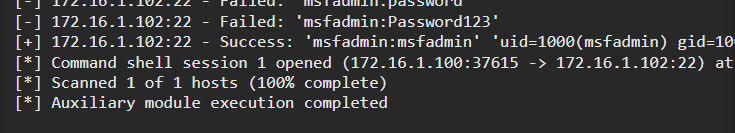
Finally, set the VERBOSE, which will display all of the attempts



Run the brute force



The scan will stop once it finds a success as shown below



When the valid credentials were found we can see the current active session using the session command

A screen shot of a computer

Description automatically generated

To interact with the session, use the -I flag and then you will be connected to the target via SSH and can run commands like normal

A screen shot of a computer

Description automatically generated