Aim: - Installation of Metaspoitable, Virtual Box and Exploitation of Metaspoitable using Kali Linux.

Software Required: -

Kali Linux, Metaspoitable

Outputs: -

Theory: -

About Kali Linux: -

Kali Linux is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains several hundred tools targeted towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering. Kali Linux is a multi-platform solution, accessible and freely available to information security professionals and hobbyists.

Kali Linux was released on the 13th March 2013 as a complete, top-to-bottom rebuild of Backtrack Linux, adhering completely to Debian development standards.

Wide-ranging wireless device support: A regular sticking point with Linux distributions has been support for wireless interfaces. We have built Kali Linux to support as many wireless devices as we possibly can, allowing it to run properly on a wide variety of hardware and making it compatible with numerous USB and other wireless devices.

Custom kernel, patched for injection: As penetration testers, the development team often needs to do wireless assessments, so our kernel has the latest injection patches included.

Developed in a secure environment: The Kali Linux team is made up of a small group of individuals who are the only ones trusted to commit packages and interact with the repositories, all of which is done using multiple secure protocols.

GPG signed packages and repositories: Every package in Kali Linux is signed by each individual developer who built and committed it, and the repositories subsequently sign the packages as well.

Multi-language support: Although penetration tools tend to be written in English, we have ensured that Kali includes true multilingual support, allowing more users to operate in their native language and locate the tools they need for the job.

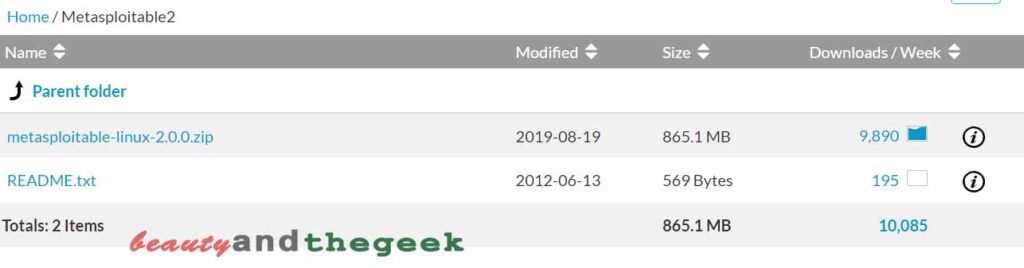
What is Metasploitable?

The basic definition given on the website is “Metasploitable is an intentionally vulnerable Linux virtual machine”. It is used for penetration testing. You are not supposed to connect it to public or unknown network. As defined it is a intentionally vulnerable machine. It can be hacked easily.

Steps to download Metasploitable: -

Whenever you download anything, please make sure you download from legit website. You can download Metasploitable from below mentioned link. It is around 865.1 MB in size. It will be a zipped file. You will have to extract the same. Once you open the below mentioned link you will get something mentioned like in Fig 1. Just click on it and file will start to download.

<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>



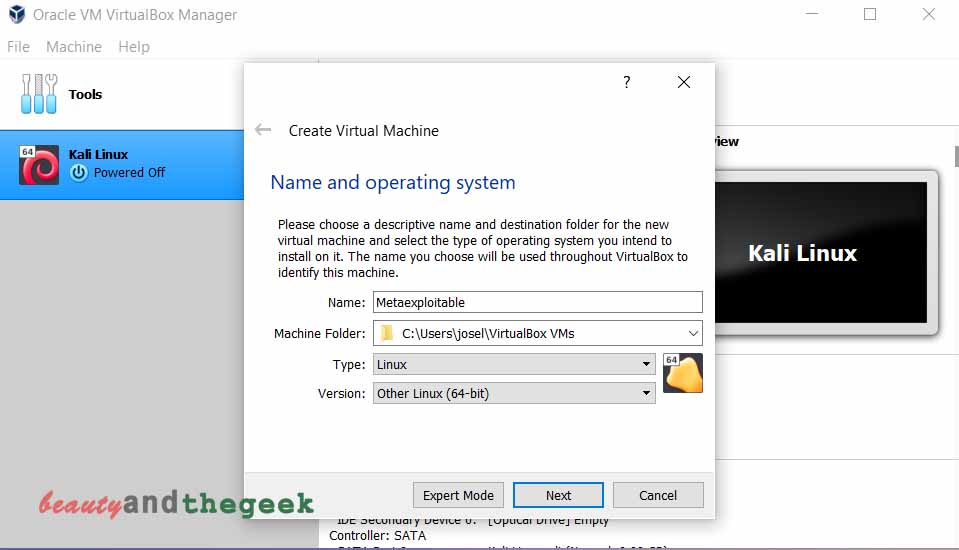
How to install Metasploitable in Virtual Box:

Below are the steps assuming you have Virtual box on your system.

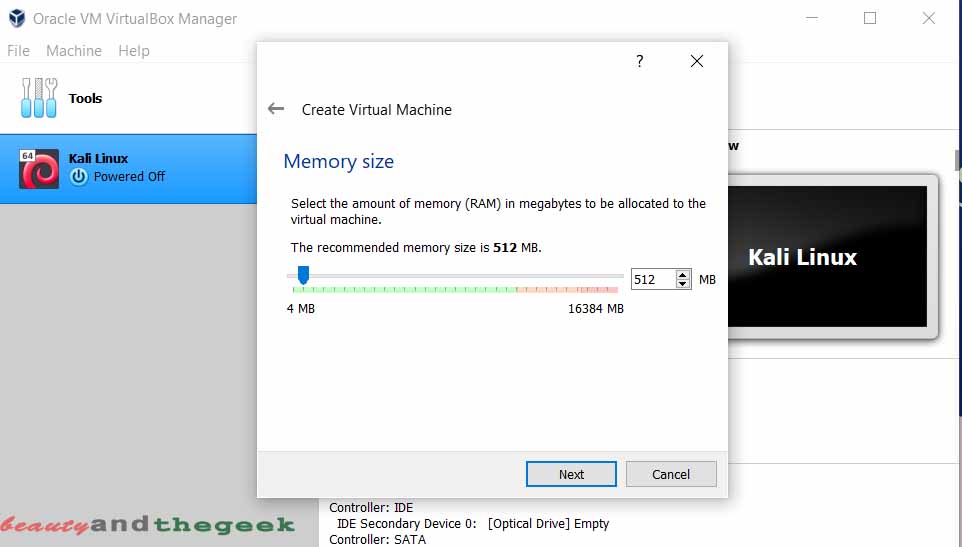
1. Extract the Metasploitable downloaded file: Once you have downloaded the file from the above link. Extract the file. This is a very curial step otherwise the file will not be uploaded in the VM.
2. Click on the “New” Option as shown in the below image.



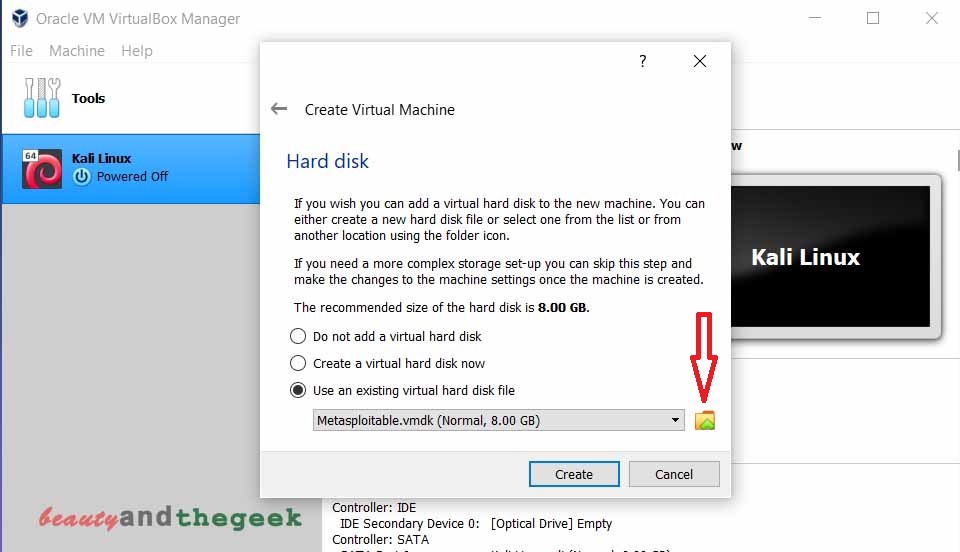
1. Name the System: Once you click on New option, you will have to Name. In this case I put the name as “Metasploitable”, I do not know what I was thinking, I named exploitable. Type: Linux and change Version: Other Linux (64-bit) and click on Next.



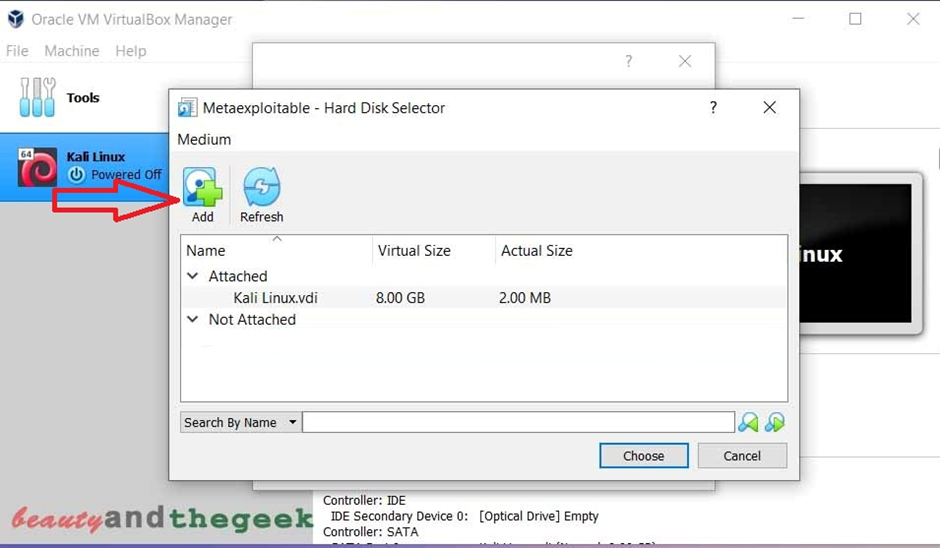
1. Memory size: By default, it chooses the memory size as 512MB. You can keep the default memory. You do not require more since it is command line interface machine. And Click on Next.



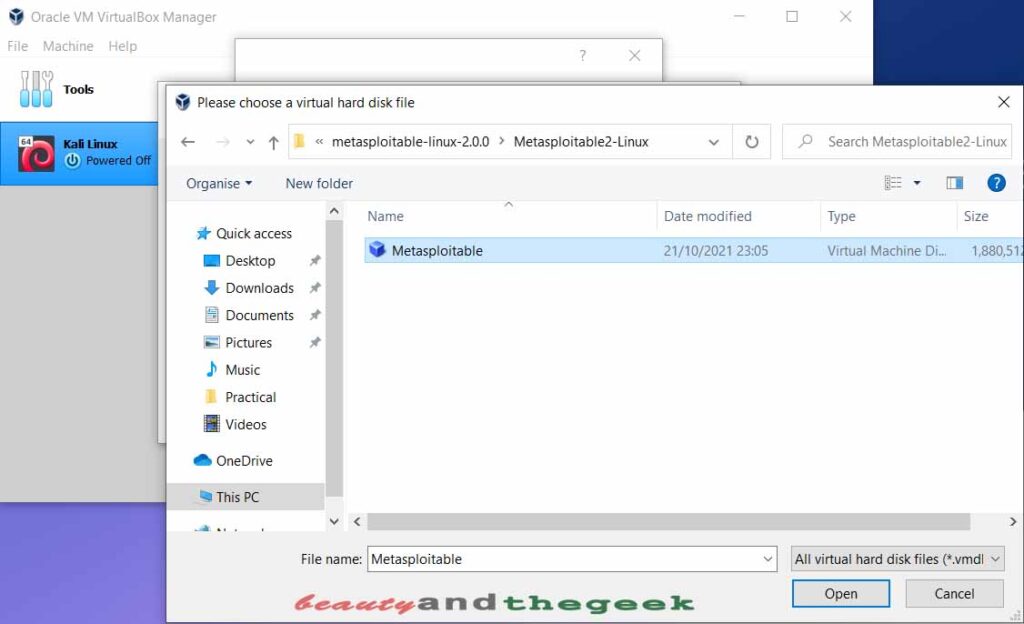
1. Choosing Hard disk: By default, it will be on the second radio button i.e., Create a virtual hard disk now. You will have to select “Use an existing virtual Hard disk file”. And then click on the yellow folder icon (marked with red arrow).



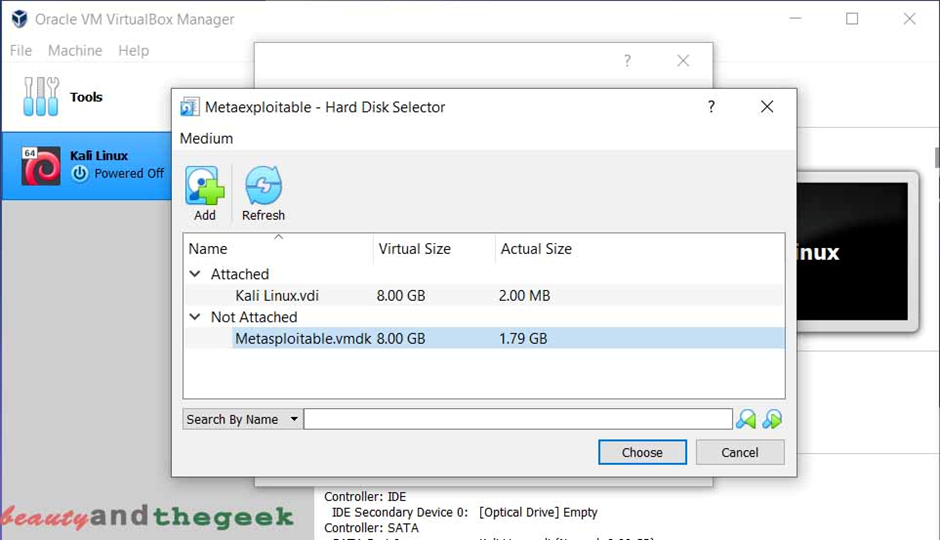
Once you click on the yellow icon, the next page will open up and you will have to click on add.



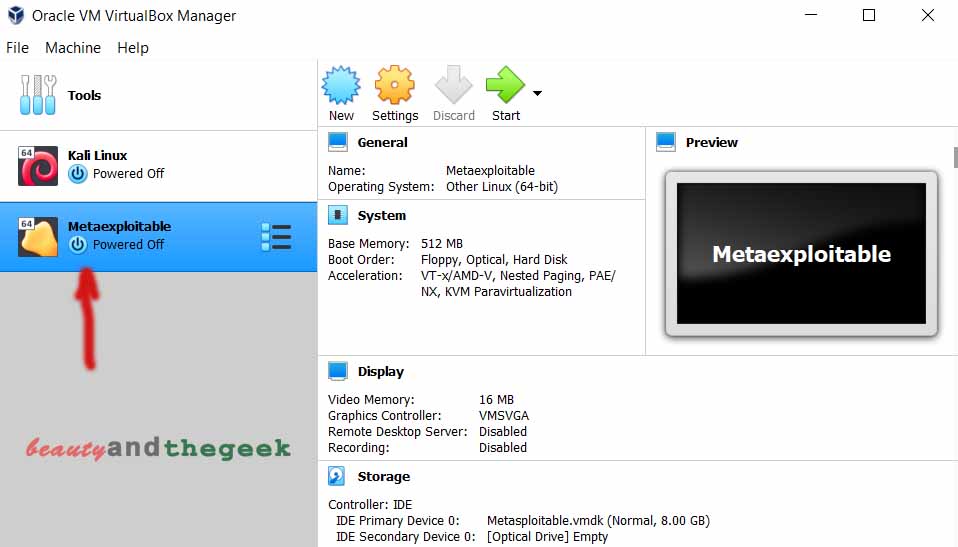
1. Select the Location where you had extracted and stored the file. It is a .vmdk file. Click on it. And then click Open.



It is displayed under “Not Attached”. Click on “Metasploitable.vmdk” file and Hit the Choose button. You are using existing hard disk. That is present in the downloads without creating a new one.



1. The Installation is complete. Metasploitable is displayed on the left-hand side of the Virtual Machine.

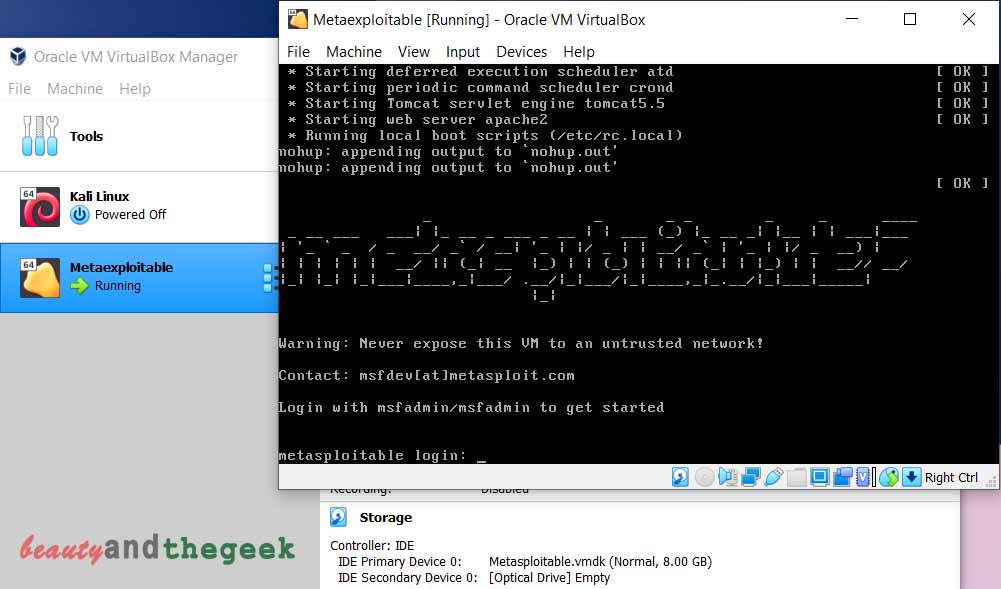


To check if Metasploitable runs successfully, click on the START button. It will take a few seconds to start the machine and you will get Metasploitable login.

The default login username and password is on the website

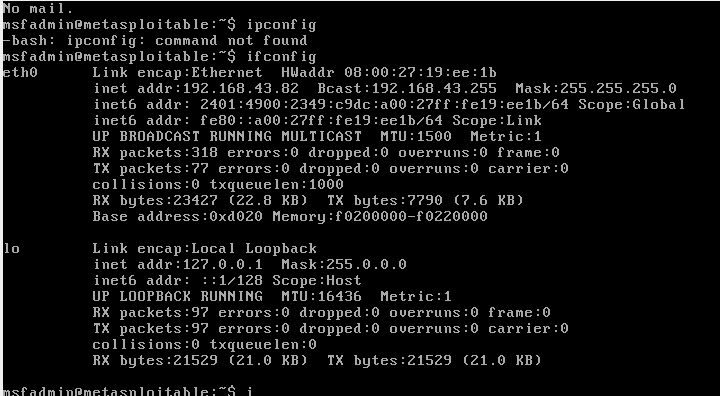
Default login: msfadmin

Default password: msfadmin

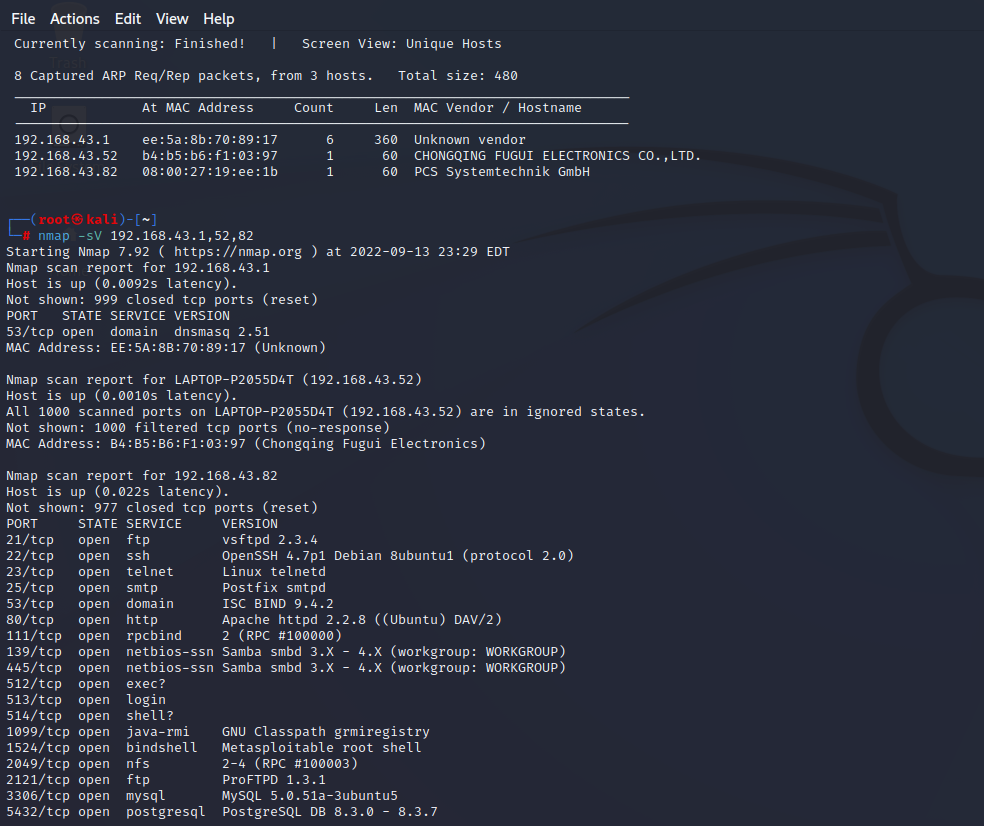


EXPERIMENT STEPS:

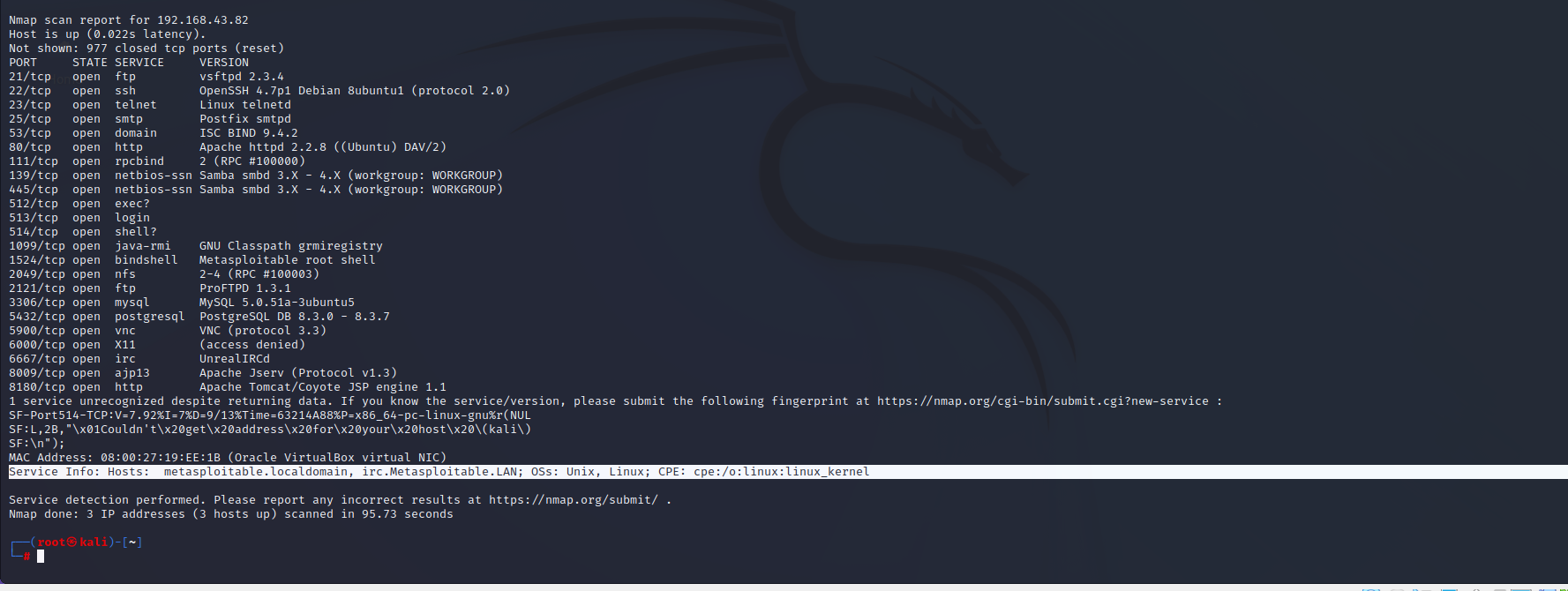
Step 1:



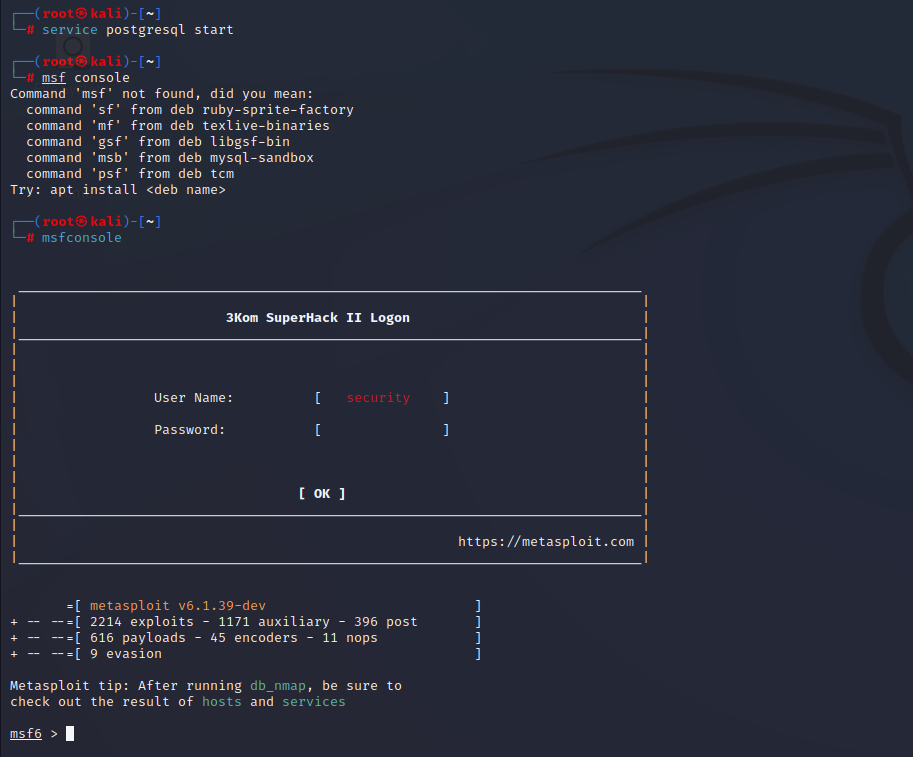
Step 2:



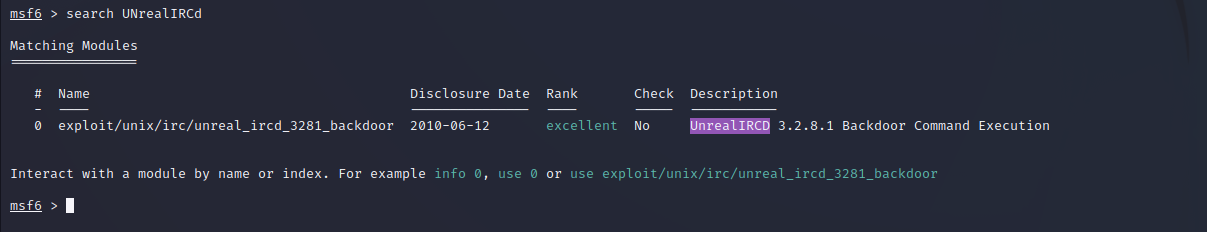
Step 3:



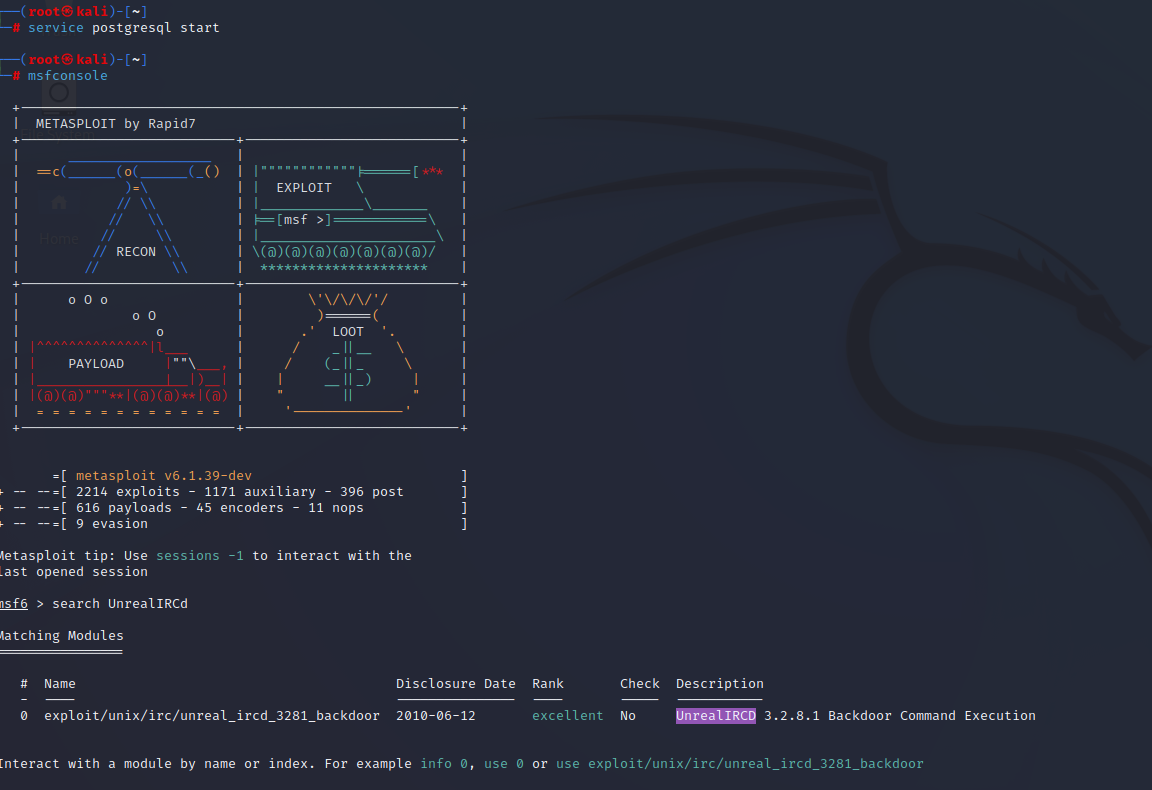
Step 4:



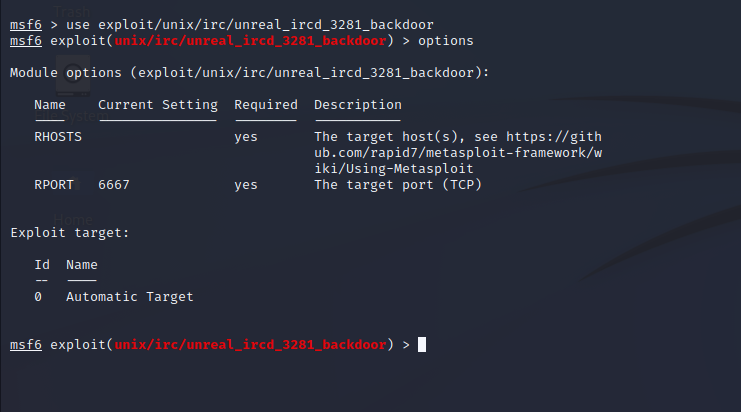
Step 5:



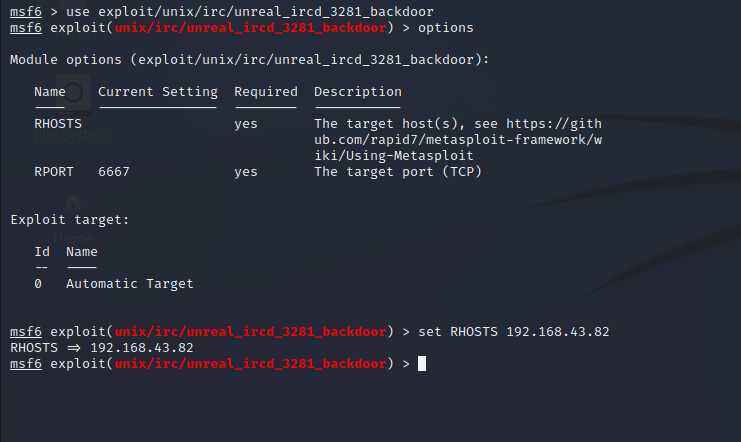
Step 6:



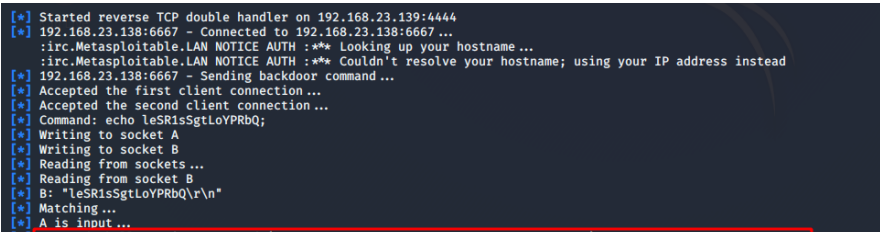
Step 7:



Step 8:



Step 9:



Result:

Therefore, Exploitation of Metasploitable using Kali Linux is performed fully.