[Hack Metasploitable 2 Part 2](https://null-byte.wonderhowto.com/how-to/hack-metasploitable-2-part-2-0164436/)

* BY [**JEREMIAH PAYNE**](https://creator.wonderhowto.com/jeremiahpayne/)
* 09/11/2015 8:11 AM

In this tutorial I am going to look at what services are running on our Metasploitable machine and setup firewalls. This is more basic scanning of our machine to get an idea of how to get in. Obviously in a real engagement you would want to do research on Google and whatnot to find out as much as you can about your target but this series isn't about all of that.

Sidenote: I wanna do a series on how to setup and use the ZUES botnet. Does this sound interesting?

Step 1Finding All Available IPs

First things first. I want to find my machine! this can be done with the **nmap -sP 192.168.1.0/24** command. The IP used it your network IP and the /24 is the [subnet mask bits](http://www.subnet-calculator.com/). You should get an output similar to this.

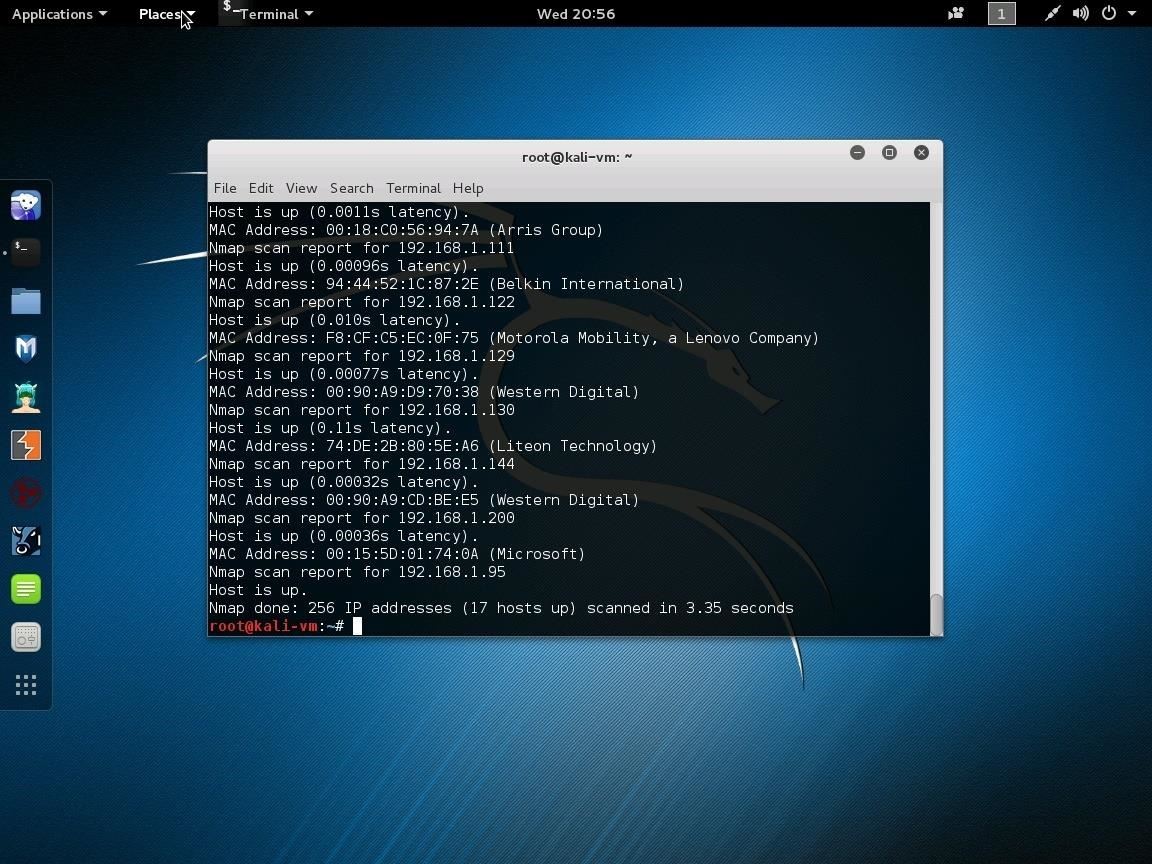
[](https://img.wonderhowto.com/img/original/93/88/63577505304496/0/635775053044969388.jpg)

Image via [imgur.com](http://imgur.com/)

Step 2Scanning Our IP

Once you find the machine you want to test (for me it is 192.168.1.200) we want to find all the services and open ports. Remember that the goal of this series is to keep these ports open but secure the machine. This is to make it so we don't just block all connections and makes the scenario more realistic. This should be very similar to the output you get.

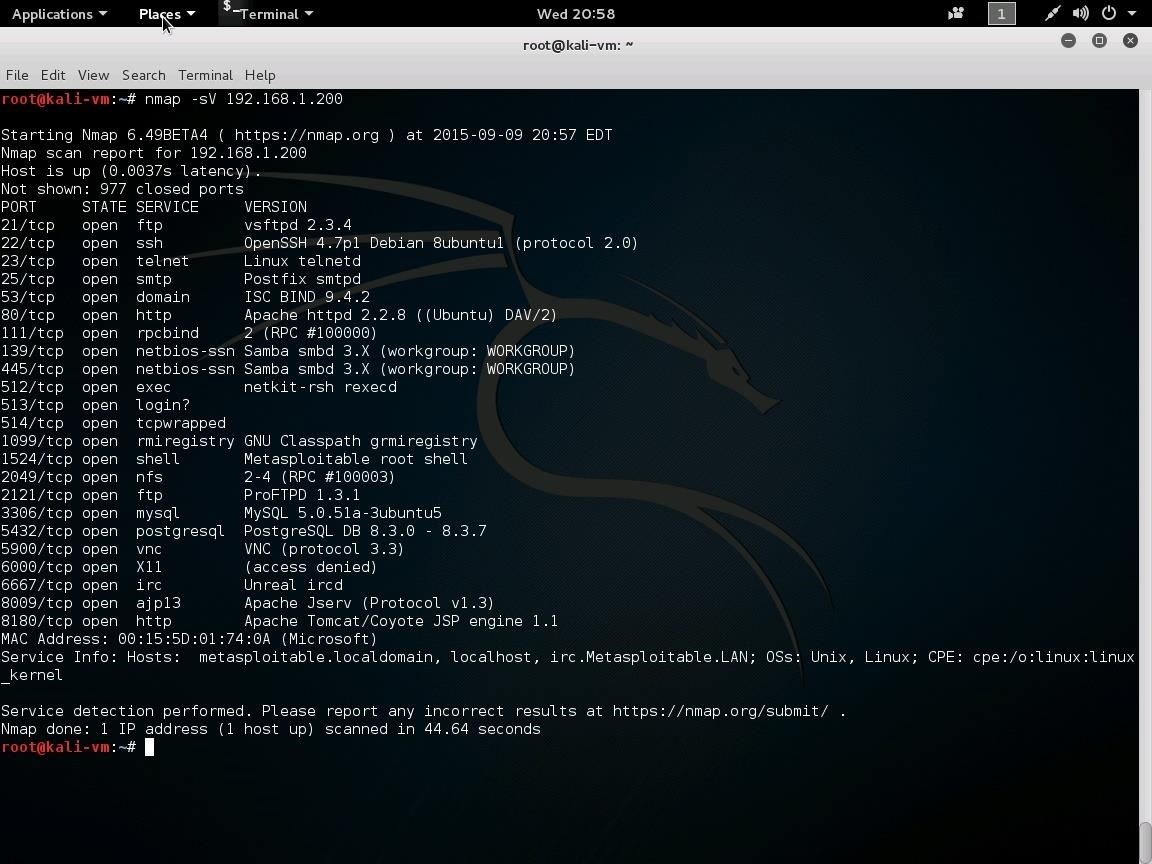
[](https://img.wonderhowto.com/img/original/88/57/63577505320199/0/635775053201998857.jpg)

Image via [imgur.com](http://imgur.com/)

Step 3Setting Up IPtables

Next you will want to connect to your Metasploitable machine using the account we used last time. I use **ssh msfadmin@192.168.1.200** and typed "yes" without quotes to add the key to my SSH cache.

IPtables is a great piece of software that any Linux server admin NEEDS to know so it is worth the Googling ;). I have seen several machines on my college's darknet that have never setup their IPtables and it would help them alot to do so.

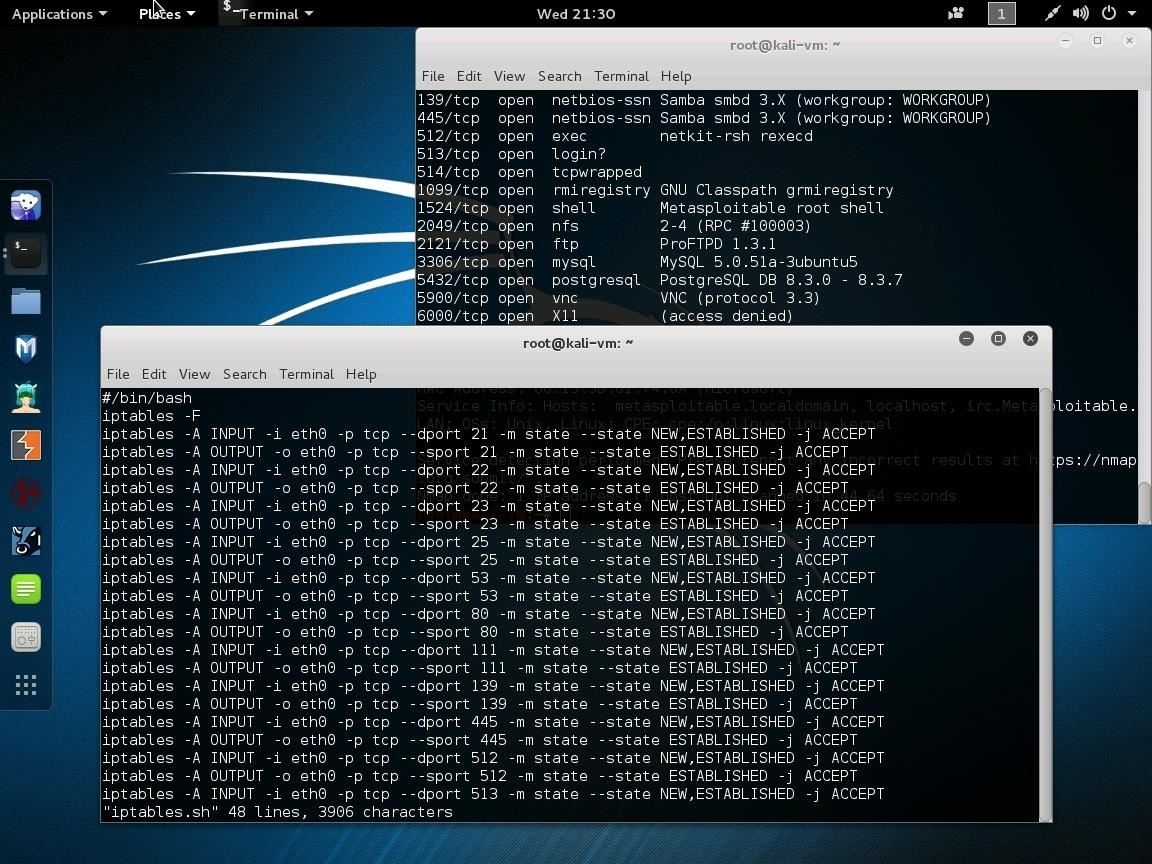
[](https://img.wonderhowto.com/img/original/21/54/63577505341403/0/635775053414032154.jpg)

Image via [imgur.com](http://imgur.com/)

Here I am clearing all previous rules (**iptables -F**)and then defining new ones for all the ports I see are being used. I did this for both the INPUT and OUTPUT chains. This is in a script just so I have the ability to reapply them or even modify and reapply quickly. Remember to save with **iptables-save** once you have finished. I will attach this script to this tutorial (remember to run **chmod +x iptables.sh**). Again some Googling will help you understand these commands alot!

After you run this script type **iptables -L** to view the setup rules. IPtables real each rule from top to bottom for each packet that applies to the chain. Thus why an observant person would notice the last rule drops all remaining packets.

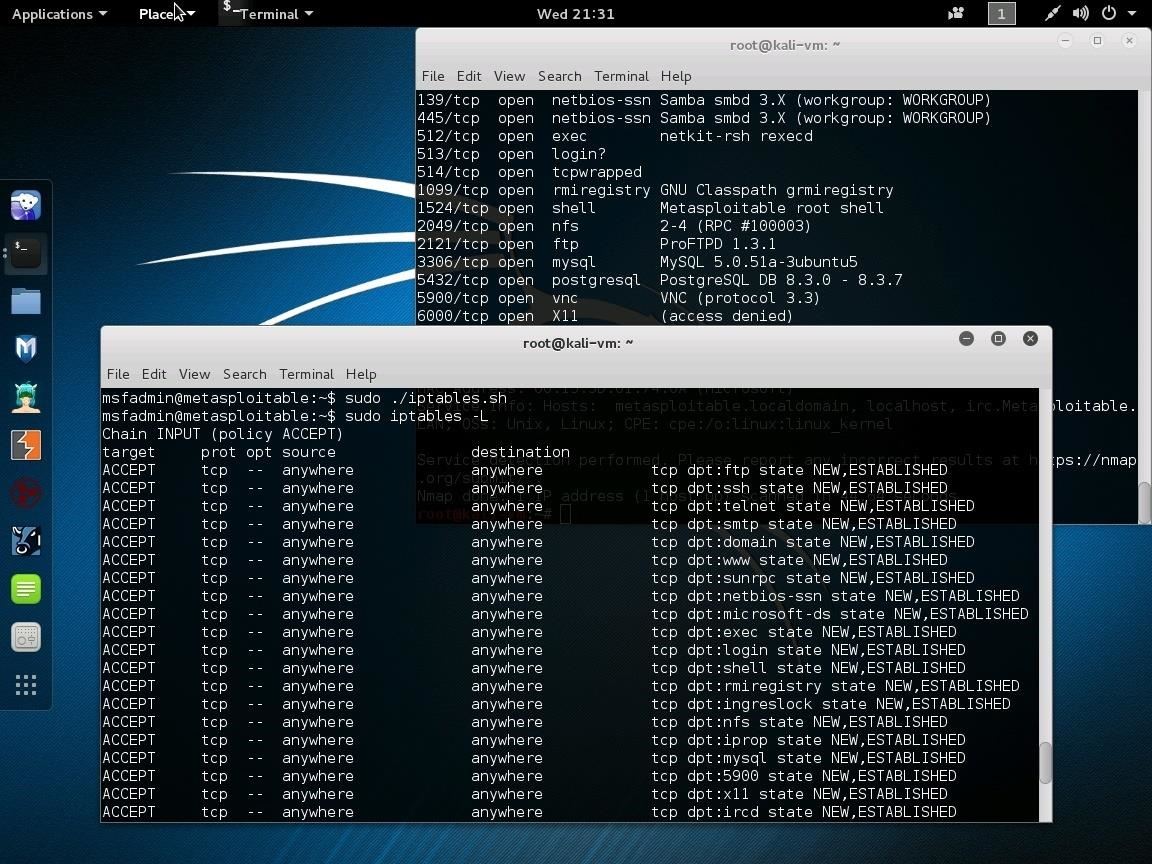
[](https://img.wonderhowto.com/img/original/33/72/63577505415434/0/635775054154343372.jpg)

Image via [imgur.com](http://imgur.com/)

Try scanning your machine with the **nmap -sV** command again and you will see that it appear nothing has changed. Half of the firewalls job is to keep listeners (or really anything the admin wants) from leaving the machine/network or coming in.

Question: Is this tutorial length good or no? I see that most tutorials seem like shorter reads. Or should it just depend on what I wanna teach?