## Lab 4b installation and configuration Metasploitable 2

Overview

The Metasploitable2 virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. This virtual machine is compatible with VMWare, VirtualBox, and other common virtualization platforms. By default, Metasploitable's network interfaces are bound to the NAT and Host-only network adapters.

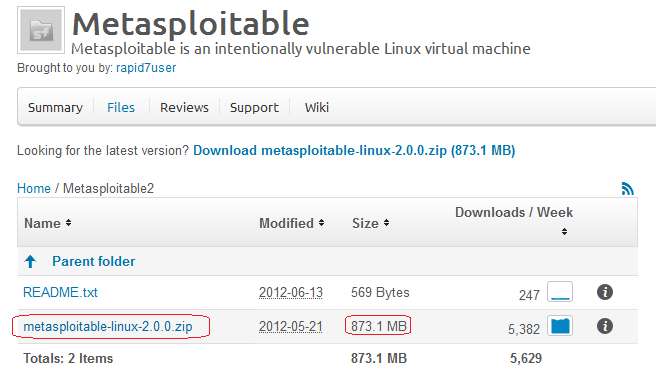
Here is a listing of the vulnerabilities in Metasploitable 2-

1. Misconfigured Services - A lot of services have been misconfigured and provide direct entry into the operating system.
2. Backdoors - A few programs and services have been backdoored. These backdoors can be used to gain access to the OS.
3. Weak Passwords - These are vulnerable to bruteforce attacks.
4. Vulnerable Web Services- A few web services pre-installed into Metasploitable have known vulnerabilities which can be exploited.
5. Web Application Vulnerabilities - Some vulnerable web applications can be exploited to gain entry to the system.

Downloading Metasploitable2

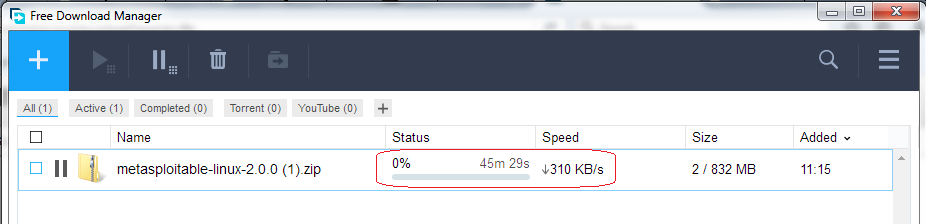
This a small download as far as Linux is concerned, at just over 873 MB. The great thing about this download it is built the same was as our Kali download, as a ready built image so all we must do is import the image into either VirtualBox, VMware of whatever hypervisor we are using. It could not be any easier!

[Download link for Metasploitable2](https://sourceforge.net/projects/metasploitable/files/Metasploitable2/)



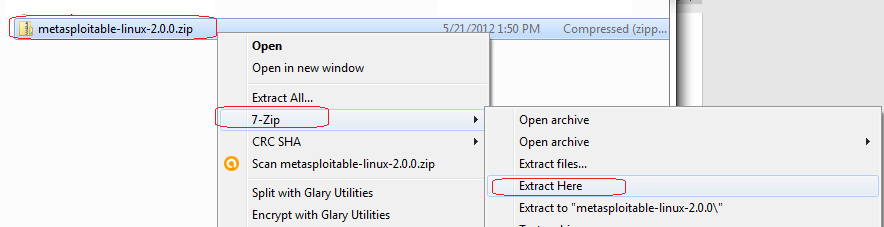
From our previous lab for downloading and installing Kali, we used a download manager to help quicken the download process. If the download manager is still up and running Metasploitable will take but a few minutes to download.

Once the download manager kicks in, the download should take less than an hour, depending on your Internet connection. Using a straight download can take as long as 11 hours.



So once we have Metasploitable downloaded, we will need to extract the images from within the archived folder. For this we will our 7-zip utility.

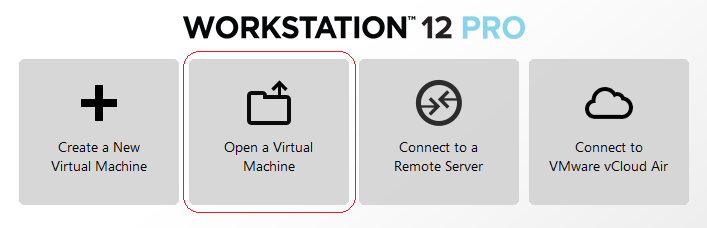
Open the download directory or where ever you saved the file and find the zip folder containing Metasploitable. Right click on the archive, select 7-zip or whatever archive utility you have installed and select extract here.



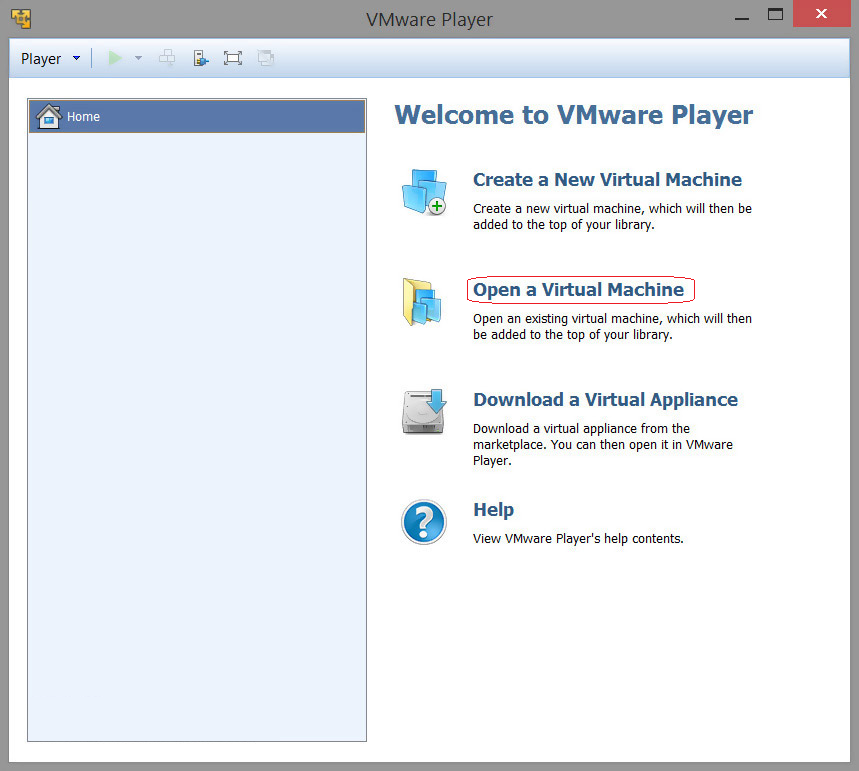
Once the have been extracted, inside you will find all the different image formats for a variety of hypervisors. Don’t worry about trying to figure out which image is yours, the hypervisor will only see the format pertaining to it.

We open our VMware management console and from the right window pane we select Open a Virtual Machine.

For the pro version, it looks like this:



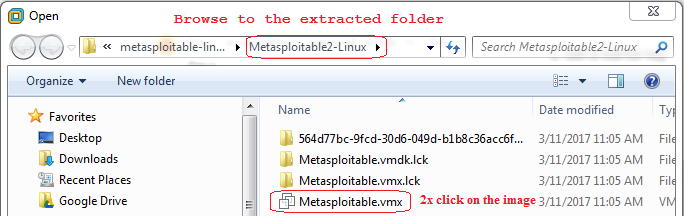
For the free version, it looks like this:



From here on out, the installation process is the same for both.

When we click on the either tile or the link for Open a Virtual Machine, we are asked for the location of the image. Since this VMware, it only sees the VMWare formatted image.

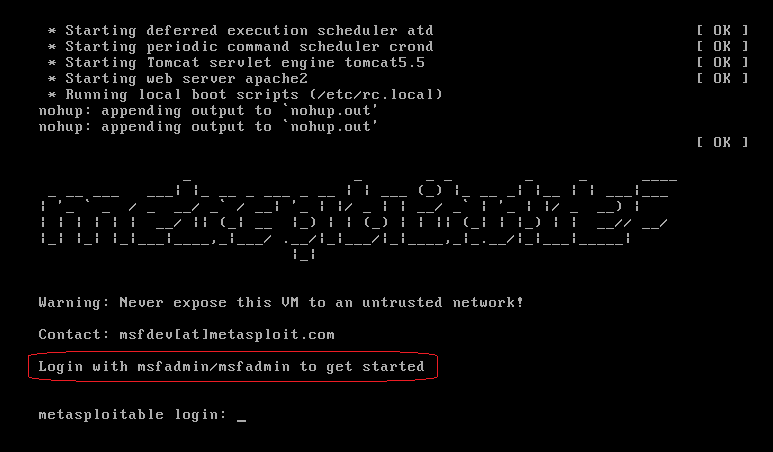
We browse to the extracted folder location and once inside, we 2x click on the VMWare image.



That’s it! If you’re asked where the image came from, select you copied it.

You’re now ready to play the virtual machine. Once you start the image, it boots quickly to terminal screen.

You must read what is written in the terminal for the username and password.



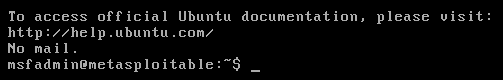
User is: msfadmin



Password is: msfadmin

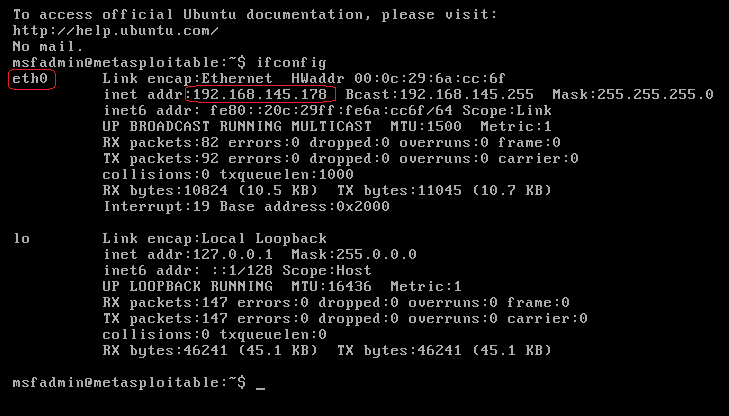
You cannot see the password being typed in any Linux terminal.

You are now logged in as admin.



Check your assigned IP address using either ifconfig or ip addr

This is my IP address! Yours will differ!



Remember the IP address!

Keeping your instance of Metasploitable open, launch a second instance of your VMWare player and start your Kali machine.

Let’s do a couple a quick exploit

First, we need to do a port scan of Metasploitable. For this we can use Nmap.

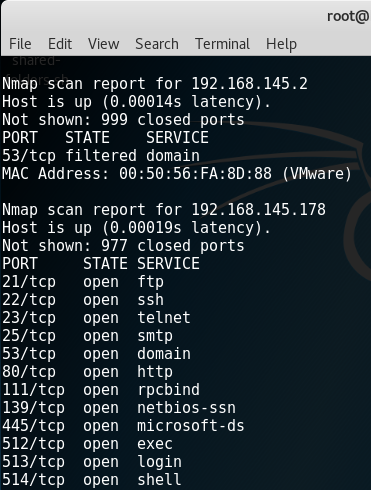
From your Kali terminal, type the following but remember to use your IP address for Metasploitable, not mine!

We can do a full network scan using nmap -sS 192.168.145.0/24 (this is my network IP, not your!)

We can also just scan the IP assigned to our newest victim, Metasploitable2 (insert diabolical laugh here)

nmap -sS 192.168.145.178/24 (This is my victim’s IP, not yours!)

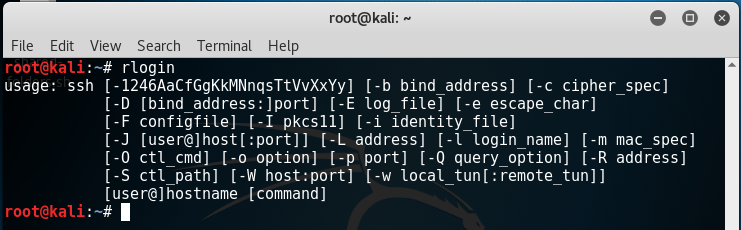
You can see from my Nmap results there is maximum target opportunity. Let’s belly up to the free buffet and exploit a couple of the services.



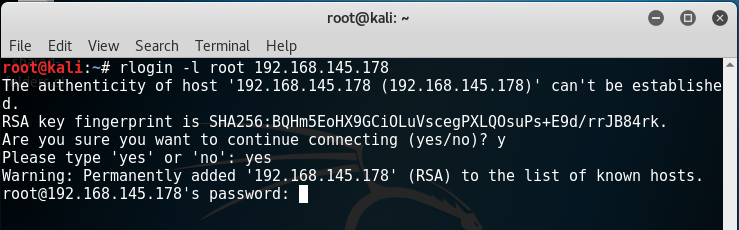
Remote access vulnerability – Rlogin

Ports 512,513 and 514 ports are there for remotely accessing Unix machines. These three have been misconfigured in such a way that anyone can set up a remote connection without proper authentication. Using rlogin, we will attempt to remotely login to Metasploitable 2.

Type rlogin to see the details about the command structure.



If we try and login as root using rlogin, we end up with this:



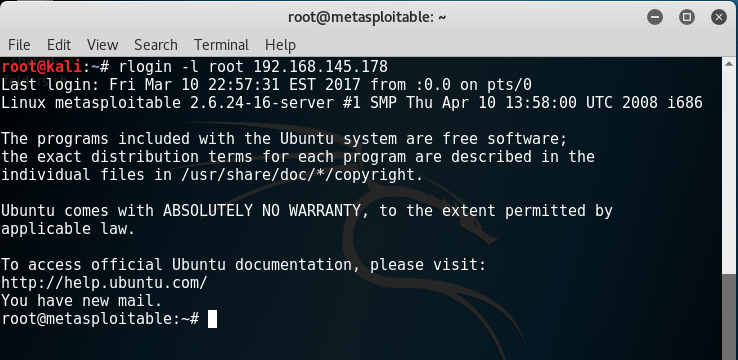
It wants a password! Reason being rlogin uses SSH but we do not have an SSH client installed in our Kali….yet!

Get back to a terminal prompt by just hitting enter. At the prompt type:

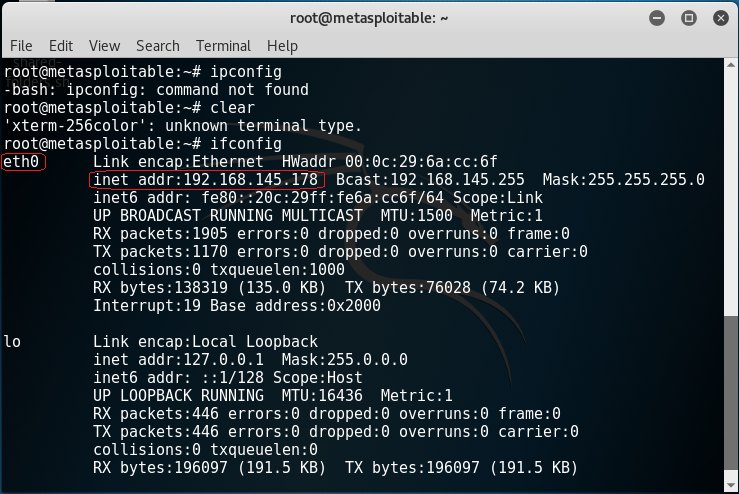
apt-get install rsh-client

This installs the SSH client will need to communicate.

Run the rlogin as root with your victims IP again. Boom goes the dynamite! We are in as root and we have complete run of Metasploitable.



At the prompt type ifconfig to get the remote machines IP address.



Now imagine you are a Pentester. You arrive on site, you scan the network and find several Unix machines running ports 512, 513, and 514. You attempt to log in to the Unix machine using rlogin and you’re successful. All you had to do was capture the images of your logon prompt, and running a couple of harmless commands on the machines such as ifconfig for proof.

Let’s do one more! Type exit at the remote victim’s prompt. This closes the connection. We also have port 21 opened. Metasploitable 2 runs VSFTPD, a popular FTP server. The version that is installed on Metasploitable2 contains a backdoor.

One thing I have learned from pentesting, start with the easiest hacks and work your way up.

I know that FTP comes out of the box with an anonymous user account with the password anonymous. It’s the default found on just about every FTP server.

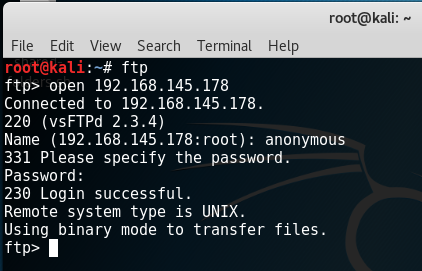
At the Kali terminal, start the FTP client by typing: ftp

The command to connect to a remote FTP server is, open.

Type open followed by the IP address for the victim.

When prompted for the user name, type: anonymous.

When prompted for the password, type: anonymous (remember, you cannot see the password being typed!)



Summary

Be careful how you use your new powers. You can get someone unintentionally fired. This is especially true in government contracting sites and banks. Back in 2010 I hacked a bank in Phoenix to its very foundation. Routers, switches, servers, clients; you name it and I was in it! The president of the bank called me and my manger into his boardroom with the board members present asking we leave most of my finding out the final report. I knew I wasn’t coming back there again.

Problem is, you don’t get credit for the pentesting unless it’s in the report. You get paid, just no bragging rights. When you work in an office with pentesters, they behave much like a hacker, you get bragging rights for performing an awesome pentest.

An awesome pentest only happens once, when you return in two years, they’ll be ready for you.

We have plenty more hacks coming your way for both Windows XP and Metasploitable. Enjoy the ride!

End of the lab!