Installing a vulnerable server

In this section, we will install a vulnerable virtual machine as a target virtual machine. This target will be used in several chapters of the book when we explain particular topics. The reason we chose to set up a vulnerable server in our machine instead of using vulnerable servers available on the Internet is because we don't want you to break any laws. We should emphasize that you should never pen test other servers without written permission. Another purpose of installing another virtual machine would be to improve your skills in a controlled manner. This way, it is easy to fix issues and understand what is going on in the target machine when attacks do not work.

In several countries, even port scanning a machine that you don't own can be considered a criminal act. Also, if something happens to the operating system using a virtual machine, we can repair it easily.

The vulnerable virtual machine that we are going to use is **Metasploitable 2** . This vulnerable system is created by the famous HD Moore of Rapid7.

Note

There are other deliberately vulnerable systems besides Metasploitable 2 that you can use for your penetration testing learning process, as can be seen on the following site: http://www.felipemartins.info/2011/05/pentesting-vulnerable-study-frameworks-complete-list/.

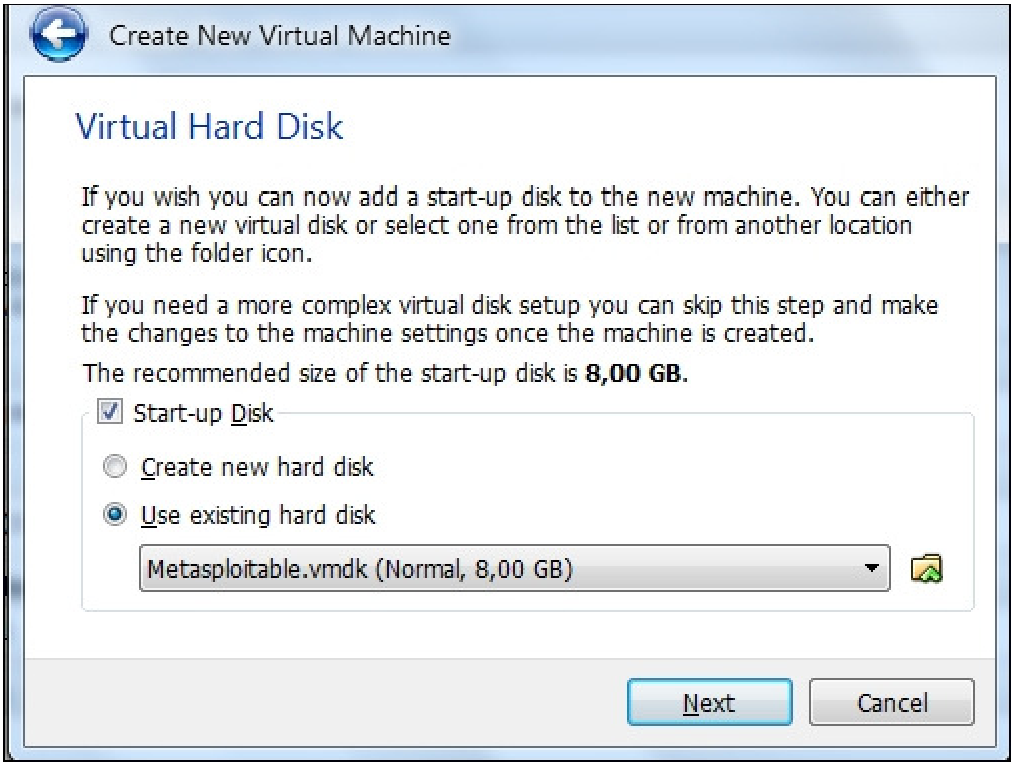
Metasploitable 2 has many vulnerabilities in the operating system, network, and web application layers.

Note

Information about the vulnerabilities contained in Metasploitable 2 can be found on the Rapid7 site at https://community.rapid7.com/docs/DOC-1875.

To install Metasploitable 2 in VirtualBox, you can perform the following steps:

1. Download the Metasploitable 2 file from http://sourceforge.net/projects/metasploitable/files/Metasploitable2/.
2. Extract the Metasploitable 2 ZIP file. After the extraction process is completed successfully, you will find five files:
   - `Metasploitable.nvram`
   - `Metasploitable.vmdk`
   - `Metasploitable.vmsd`
   - `Metasploitable.vmx`
   - `Metasploitable.vmxf`
3. Create a new virtual machine in VirtualBox. Set **Name** to `Metasploitable2` , **Operating System** to **Linux**, and **Version** to **Ubuntu**.
4. Set the memory to **1024MB**.
5. In the **Virtual Hard Disk** setting, select **Use existing hard disk**. Choose the Metasploitable files that we have already extracted in the previous step:



Create New Virtual Machine

Virtual Hard Disk

If you wish you can now add a start-up disk to the new machine. You can either create a new virtual disk or select one from the list or from another location using the folder icon.

If you need a more complex virtual disk setup you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the start-up disk is **8,00 GB.**

☑ Start-up Disk

○ Create new hard disk

● Use existing hard disk

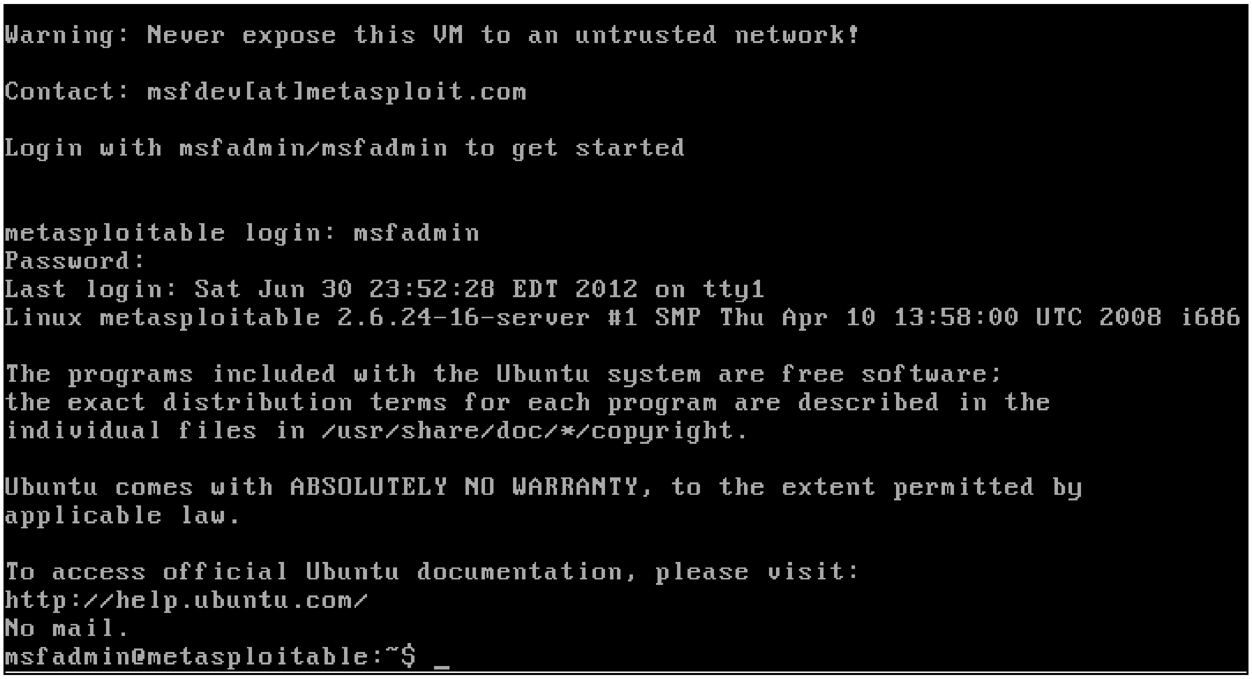
Metasploitable.vmdk (Normal, 8,00 GB)

6. Change the network setting to **Host-only adapter** to make sure that this server is accessible only from the host machine and the Kali Linux virtual machine. The Kali Linux virtual machine's network setting should also be set to **Host-only adapter** for pen-testing local VMs.

7. Start the Metasploitable 2 virtual machine. After the boot process is finished, you can log in to the Metasploitable 2 console using the following credentials:

   - Username: `msfadmin`
   - Password: `msfadmin`

8. The following is the Metasploitable 2 console after you have logged in successfully:



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

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sat Jun 30 23:52:28 EDT 2012 on tty1
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/
No mail.
msfadmin@metasploitable:~$ _
```