Week 9 - Supplementary Materials

Markdown | PDF | MS Word DOCX | Libre ODT | HTML

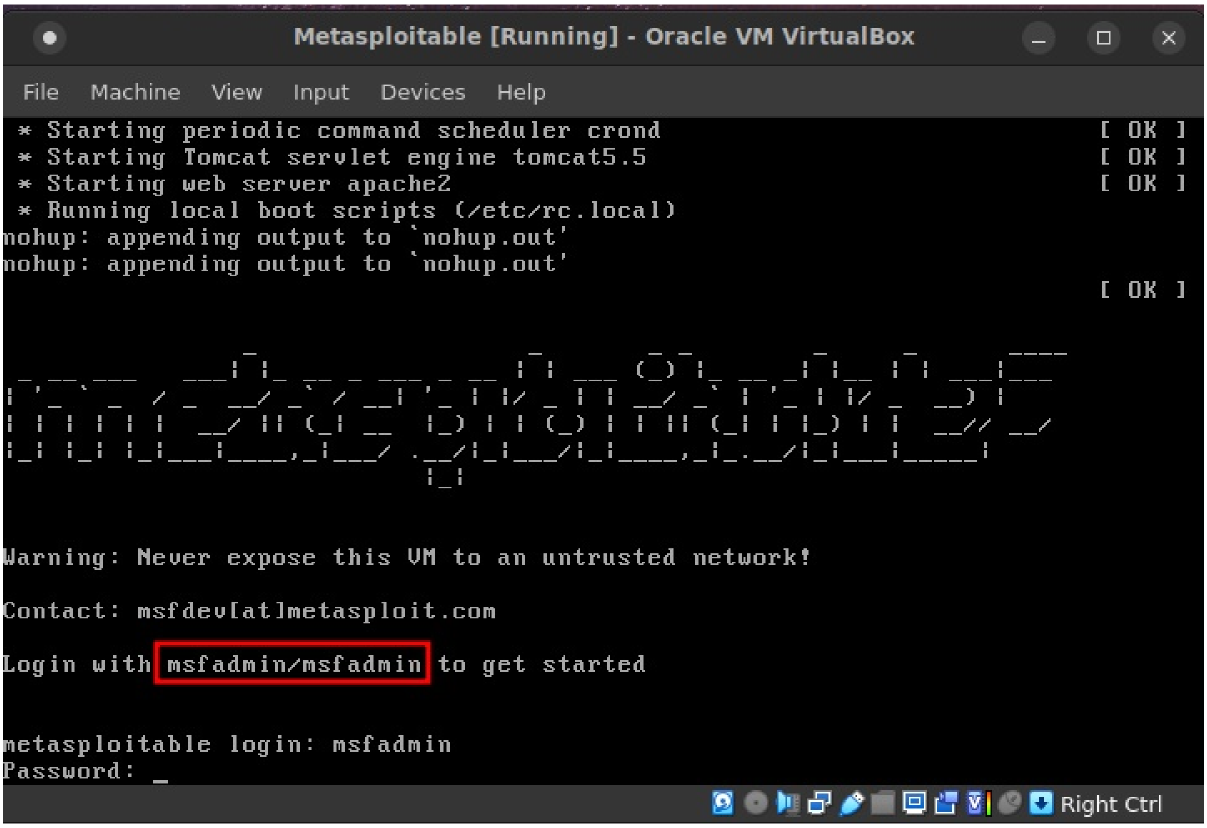
Metasploit & Metasploitable

Metasploit is a suite of exploits and penetration testing tools that is installed by default on Kali Linux. We demonstrate Metasploit via the `msfconsole` command throughout this course and it's one of the most important tools at your displosal as an ethical hacker. Real-world exploits such as EternalBlue, the exploit behind waves of ransomware, are merged into Metasploit as they become well-known and utilized in-the-wild.

Metasploitable (Metasploitable-2) is a purposefully vulnerable operating system. It is a secure place to perform penetration testing and security research, notably by attacking it with Metasploit. To follow along with our live hacks in class, this virtual machine will be required. Additionally, it provides a good basis for your final hacks (though it is not required for your final project).

Download & Install Metasploitable

CLICK HERE and download a 64-bit pre-built virtual machine (VM) image of Metasploitable. You will add this VM image to VirtualBox to boot into Metasploitable inside your host operating system.



```
 * 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: msfadmin
Password: _
```

Metasploitable setup tutorials:

- Video 01
- Video 02
- Video 03

Extracting the Zip File

The Metasploitable VM is distributed in a compressed Zip .zip format. All modern desktop operating systems (Windows, macOS, and most GNU/Linux variants) will extract Zip files. Please make sure you extract the VM image somewhere that you can find it. Though it is in VMware .vmdk format, you will be able to import it into VirtualBox.

Log In to Metasploitable

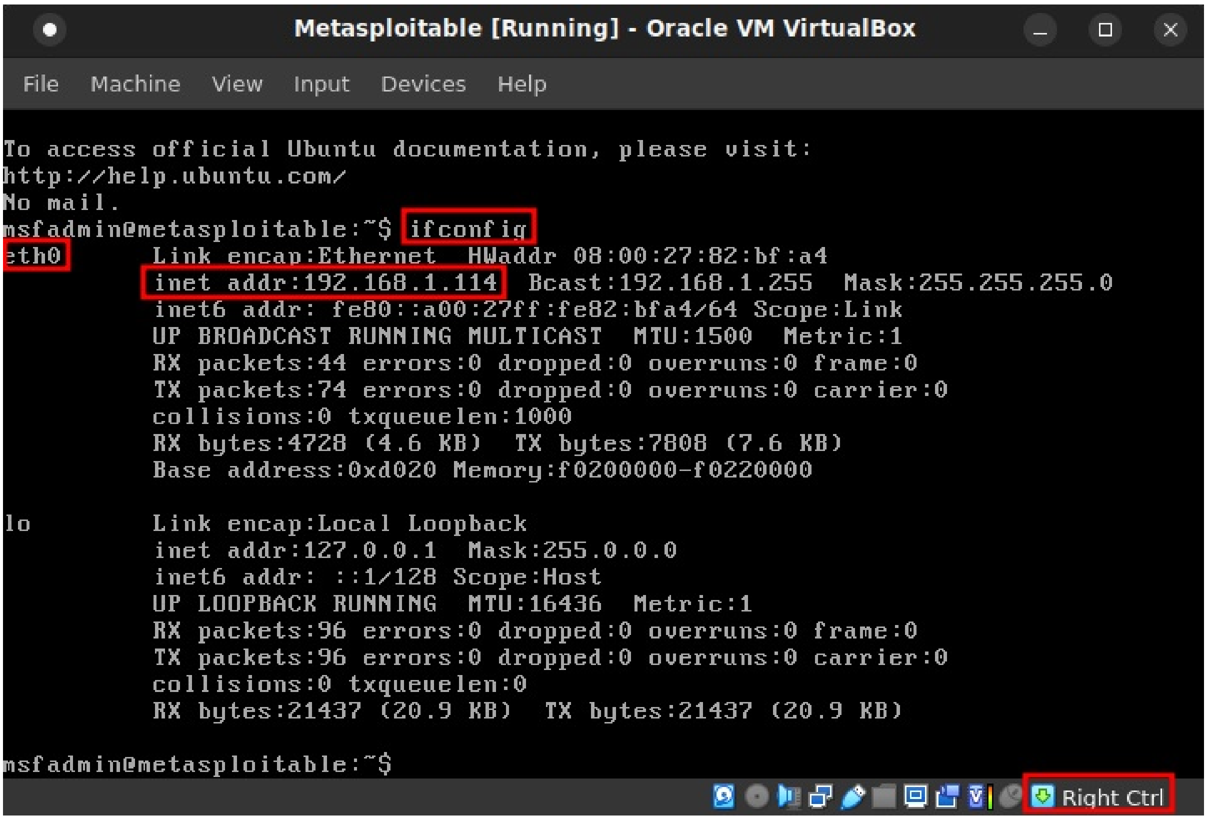
Once you can boot Metasploitable, the default credentials are:

- username: `msfadmin`
- password: `msfadmin`

You don't have to change this password even though it is very weak because Metasploitable is *supposed* to be insecure.

Find the Metasploitable Network Address

Use the `ifconfig` command to find the IP address for the Metasploitable VM. Remember this address because it will be the one that you attack with Kali Linux using Metasploit `msfconsole`.



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:82:bf:a4
          inet addr:192.168.1.114  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe82:bfa4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:44 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4728 (4.6 KB)  TX bytes:7808 (7.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$
```

Starting Metasploit

Metasploit utilizes a database of exploits that must be initialized the first time `msfconsole` is run.

- Restart the PostgreSQL database service:

```
sudo service postgresql restart
```

- Initialize the Metasploit database:

```
sudo msfdb init
```

- Start `msfconsole`:

```
sudo msfconsole
```

Now you can follow along with our hacks using Metasploit and try some of your own. Here are some examples you can try online:

- Step-By-Step Getting Started with Metasploit
- SMB/Samba EternalBlue exploit
- FTP exploit
- Delivering a Payload

Meterpreter

Metasploit is not limited to `msfconsole` and we will also demonstrate the Meterpreter command to, for example, capture microphone audio on a vulnerable machine.

- Get started with Meterpreter