The Poor Man's Security Lab

www.chimera-security.com

Contents

Introduction

In this paper, we are going to look at building your very own penetration testing playground on the cheap. The hardware you choose to use doesn't really matter, but it must be capable of running at least 2 virtual machines at any one time.

The tools of choice are shown below:

- Virtual Box [https://www.virtualbox.org/]
- Kali Linux [Download: http://cdimage.kali.org/kali-images/kali-linux-1.0-i386-gnome-vm.tar.gz]
- Metasploitable [Download: http://www.offensive-security.com/metasploit-unleashed/Metasploitable]
- Windows XP [This requires a license, but i'll leave that up to you]
- OWASP Bricks [http://sechow.com/bricks/download.html - Download the latest!]

The static addresses we will use (you'll need these later)

Machine	Address	Netmask	Gateway
VM Host Only Adapter	192.168.10.1	255.255.255.0	N/A
Lab - Attacker	192.168.10.110	255.255.255.0	192.168.10.1
Lab - Target (XP)	192.168.10.120	255.255.255.0	192.168.10.1
Lab - Target (Metasploitable)	192.168.10.130	255.255.255.0	192.168.10.1
Lab - Target (OWASP Bricks)	192.168.10.140	255.255.255.0	192.168.10.1

Step 1 - Installing Virtual Box

As Virtual Box is available in three different flavours, I will not go into how to install it on all three available OS's. Installation is a case of simply downloading the appropriate package and going through you usual installation process of your host OS. Download the appropriate package below:

Windows Host	(http://download.virtualbox.org/virtualbox/4.2.16/VirtualBox-4.2.16-86992-Win.exe)
OSX Host	(http://download.virtualbox.org/virtualbox/4.2.16/VirtualBox-4.2.16-86992-OSX.dmg)
Linux Host	(https://www.virtualbox.org/wiki/Linux_Downloads)

We will also need the Virtual Box extensions package, this is platform independent so don't worry about choosing the right one, the download link is shown below. Once Virtual Box is installed and the extensions pack is downloaded, run the extensions package from the download directory. Once executed, Virtual Box will prompt whether to install, follow it through.

Link: http://download.virtualbox.org/virtualbox/4.2.16/Oracle_VM_VirtualBox_Extension_Pack-4.2.16-86992.vbox-extpack

Step 2 - Preparing the attacker

In order to make this setup as painless as possible, we will be using Kali linux as the attacker VM. Kali (previously Backtrack) is a penetration testing distribution from Offensive-Secuirty that contains the most popular tools and resources needed during a penetration test or "just having a look". The download link for Kali can be found above in the tools section. I have opted to use the pre-configured vm package rather than the normal ISO as it is faster to deploy. Download the archive, then continue below.

Once downloaded, open the download directory and extract the virtual appliance. Windows users will have to install a third party app as tar archives are not supported out of the box, 7zip will do the job (and it's free!). Once extracted, you will be presented with a mass of VMDKs (Virtual Machine Disks). Don't worry about the number of files we've just unpacked, they will be consolidated once we import them into Virtual Box.

Now we will import the VM into Virtualbox. To do this, follow the steps below:

> Copy the Kali folder we extracted earlier into the default virtual machine folder, on Windows, this is usually in /My Documents/Virtualbox Vms

> Open Virtual Box

> Select "New"

> Enter a name for the attacker VM, to keep this guide as simple as possible, set it to "Lab – Attacker"

> Change the Type to "Linux" & the Version to "Debian", click next

> Now we need to allocate some ram, depending on your environment you should allocate an ample amount. 512mb should be more than enough for this instance. Click next.

> As we already have a virtual hard drive for Kali, go ahead and select "Use an existing virtual hard drive file"

> Select the folder icon next to the drop down menu, navigate to the Kali folder and open the file named "kali-linux-i386-gnome-vm.vmdk"

> Select "Create"

We have now created the attacker instance of the virtual security lab. Before we jump head first into playing with Kali, we need to ensure that our virtual machines are isolated from the outside world and anything else on the LAN. To do this, we need to make sure that the attacker VM is set to use the host network only (host only network mode enables the VMs to communicate with each other, but nothing else outside of the host).

To do this, do the following:

> Within the VBox window, right click the attacker VM and select "Settings"

> Select the "Network" tab

> Change the drop down box named "attached to:" under Adapter 1 to "Host-only adapter"

One more step, we need to configure the network:

> Inside the kali VM, select Applications, System Tools then Preferences. Click "Network Connections"

> Highlight "Wired connection 1" and select "edit"

> Select the "IPV4" tab, select "Manual" from the drop down and enter the following in the appropriate fields:

Address:	192.168.10.110
Netmask:	255.255.255.0
Gateway:	192.168.10.1

> Go ahead and click save

Now we have isolated the attacker VM, you can go ahead and boot it up. The username and password for Kali is root:toor (username:password). Go ahead and familiarise yourself, watch a few YouTube videos detailing the OS and come back!

Step 3 - Preparing the Windows XP target

Windows XP is one of the most popular Microsoft operating system in use today, even though support has ended for the product. For this target, I am going to use Windows Professional as I have a license laying around. For this VM, you will need to source both a Windows XP ISO & a valid license. I have also opted to use a version that does not come pre-packaged with any service packs, giving me the freedom to update the OS as i see fit (more vulns the older it is!).

I have chosen not to go through the installation process of Windows because if you are comfortable with the command-line sections of this guide then you are probably more than comfortable installing a feeble OS such as XP.

Fast forward to post install! make sure you write down the usernames/passwords of any accounts you create on the VM for future reference.

The only step we need to take with this VM post installation is setting a static address, follow the steps below:

> Launch the target XP VM

> Log in with any credentials you set during the installation process

> Navigate to Start / Control Panel / Network and Internet Connections / Network Connections

> Right click the network interface and select "Properties"

> Under the general tab, highlight "Internet Protocol (TCP/IP)" and select "Properties"

> Select the radial button next to "use the following IP address" and enter the following:

IP address:	192.168.10.120
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.10.1

> Click OK, then Apply

This VM is now ready! move on...

Step 4 - Preparing the Metasploitable target

Metasploitable is another great offering from the guys over at Offensive Security. This virtual machine is a highly vulnerable install of the linux operating system employing a number of vulnerable services and applications. Metasploitable can be used to test penetration testing techniques, security tools and other security related software.

The first step in getting this vm set up is to download the necessary archive. The download link can be found above, but if you're too "in the zone" to scroll up and lose your place, it's here: http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Once the zip is download, extract it to the VM path we discussed earlier (the place where VBox stores the virtual machine folders). Once you've extracted the files, follow these steps and the vulnerable VM will be exposed in no time!

> Extract the Metasploitable archive to the VM folder if you haven't already

> Open Virtual Box

> Select "File", then "New"

> Enter a name for the target VM, as before, we'll keep this consistent. Give it the name "Lab - Target (Metasploitable)"

> Change the type to "linux" and the version to "ubuntu", click next

> Give it some ram, 512mb ought to be enough. Click next

> As we already have the appropriate VMDK in the VBox directory, select "Use an existing virtual hard drive file"

> Select the folder icon next to the drop down menu, navigate to the Metasploitable folder within the VM directory and open the file named "Metasploitable.vmdk"

> Select "Create"

As before with the previous virtual machines, we need to edit to settings to make sure the VM connects to the internal network. To do this, follow these steps:

> Within the VBox window, right click the attacker VM and select "Settings"

> Select the "Network" tab

> Change the drop down box named "attached to:" under Adapter 1 to "Host-only adapter"

Now the Metasploitable VM is close to being ready. The last thing we need to do is give it a static address. To do this, we need to log into the VM & edit the appropriate config file. It's easier than it sounds so if you don't feel comfortable with the command line, don't worry, we've got you covered!

> Open Virtual Box

> Double-click the Metasploitable 2 virtual machine

> Once prompted, enter the username "msfadmin" & the password "msfadmin" (yes they're the same!)

> Enter the following command: { sudo nano /etc/network/interfaces }

> Clear the whole config file and enter the following:

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary interface
auto eth0
iface eth0 inet static
address 192.168.10.130
network 192.168.10.0
netmask 255.255.255.0
broadcast 192.168.10.255
gateway 192.168.10.1
```

Once you've copied the above into the interfaces file, hit CTRL + X and press "Y" when prompted to save, press enter and move on to the next command.
We need to restart the interfaces to bring up eth0 with the correct IP, simply enter the command { sudo /etc/init.d/networking restart }

This VM is ready! Move on...

Step 5 – Preparing the OWASP Bricks target
OWASP Bricks is a set of vulnerable web applications built on PHP & MySQL foundations created by the OWASP foundation. Each brick is a vulnerability in the web application, the object of the framework is to "break the bricks".

The first step of getting this great VM up and running is to set up a virtual machine that will host the platform. I have chosen the LAMP Stack appliance from the great source of free appliances that is turnkeylinux.org. This pre-configured VM enables us to rapidly deploy the platform and spend time breaking things instead of watching loading bars during installations!

Go ahead and download the LAMP Stack VM, the link can be found at the top of this guide.
(It's here if you don't want to lose your place ;) http://www.turnkeylinux.org/download?file=turnkey-lamp-12.1-squeeze-amd64-ovf.zip)

Once the appliance has downloaded, go ahead and extract the files into the Virtual Box machine directory as before. This installation is a little different to the other targets. This time we have a vm in the OVF format, making it a lot easier and faster to get it up and running in Virtual Box. After extraction, simply follow the steps below:

> Open Virtual Box

> Select "File" and "Import Appliance"

> Select "Open Appliance" and navigate to the directory where you extracted the Bricks OVF file, open the OVF.

> Select "Continue"

> Select "Import"

> Once imported, right click the new VM and select "Settings"

> Change the name of the VM to "Lab - Target (Bricks)" to keep things consistent

> Select the "Network" tab and select "NAT" from the drop down menu (we need to download the Bricks package before we isolate it)

> Press OK and start the VM

The best part of using this pre-configured virtual appliance is that there is barely anything we need to do to get it up and running. Once the VM is running, do the following:

> When prompted, enter a password for the root account. Make sure you document it for future reference!

> When prompted, enter a password for the MySQL root account

> Skip the prompt for a TurnKey API key, we don't need this

> Skip the prompt to install security updates, it's gonna be vulnerable for a reason!

> When prompted for the network config, select DHCP

> Select "Apply" then "Reboot"

We now need to download the Bricks package. To do this, we will SSH onto the LAMP vm & take things from there. To do this connect via SSH and log in with the username root & the password you set during installation. As there are a number of ways for you to connect & do this, I will not go into this at this stage. When connected via ssh, simply issue the following commands:

> wget (link to latest version of bricks)

Once downloaded, you need to extract the files into the www directory on the lamp server. There are many guides available online that will guide you through this!

After Bricks is downloaded and placed in the right directory, we need to set the VBox interface back to "Host-only adapter" and assign a static address. To do this, do the following:

> Inside the Lab - Target (Bricks) vm, select "Advanced Menu"

> Select "Networking" and then "Static IP" and enter the following:

IP Address	192.168.10.140
Netmask	255.255.255.0
Default Gateway	192.168.10.1

> Select "Apply" then "Back"

> Select "Reboot"

This VM is now ready!

Other Possible Targets
Here is a list of other possible target instances that you could use. These examples can be set up using the guide above (with minor alterations).

Web Goat
Another vulnerable web application from OWASP
https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

SQLol
SQL Injection Testbed
https://github.com/SpiderLabs/SQLol