Lab – Creating a Virtual Install of OWASP Using VirtualBox

Overview

The Open Web Application Security Project (OWASP) Broken Web Applications Project is a collection of vulnerable web applications distributed on a Virtual Machine. The installation and the running of OWSAP are much the same as installing and running Metesploitable2.

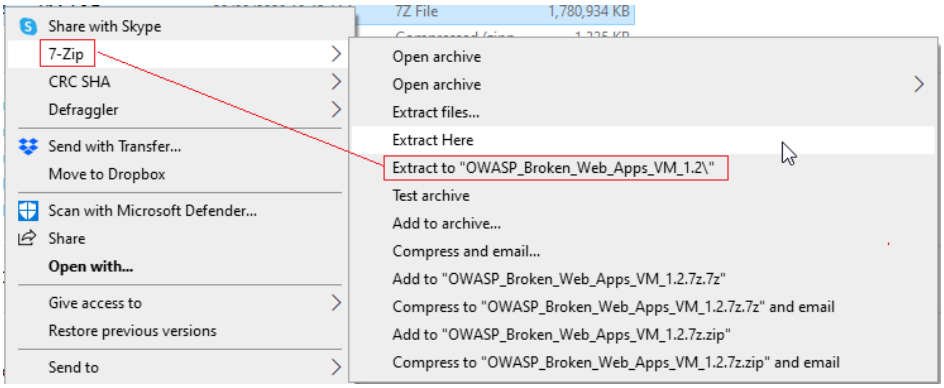
Lab Requirements

- Installation of VirtualBox (If you already have VirtualBox installed, you do not need to reinstall it)
- Download and extract an archive of the OWASP Web Applications Project.
- Installation of 7-zip archive utility.

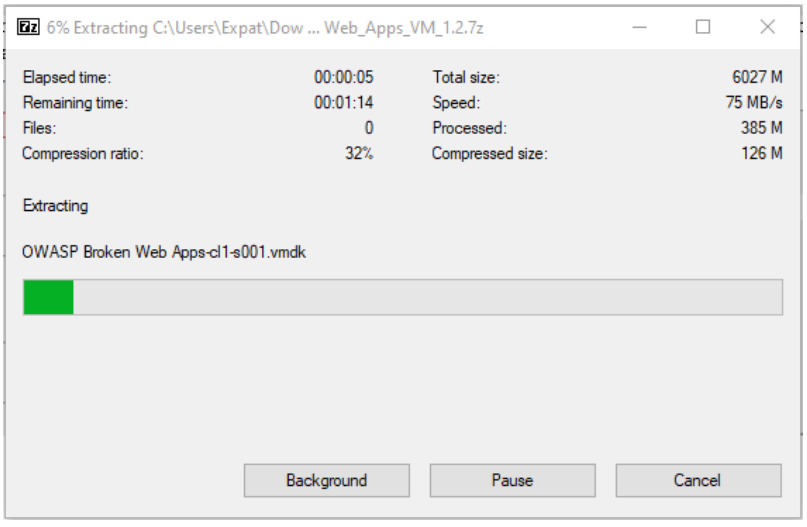
Begin the lab

Download the OWASP Web Applications Project for the SourceForge

Extract the contents using 7-zip. Right-click on the download, and for the context menu, select 7-zip and then select **Extract to** a folder using the same name as the downloaded archive



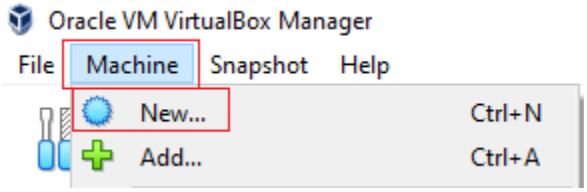
Package being extracted.



Back at the download location, find the extracted folder. Remember the location.

Open VirtualBox.

From the taskbar, click on Machine, and from the context menu, click New.



This launched the Create Virtual Machine Wizard.

Give the new machine a user-friendly name.

Select a location for the machine folder.

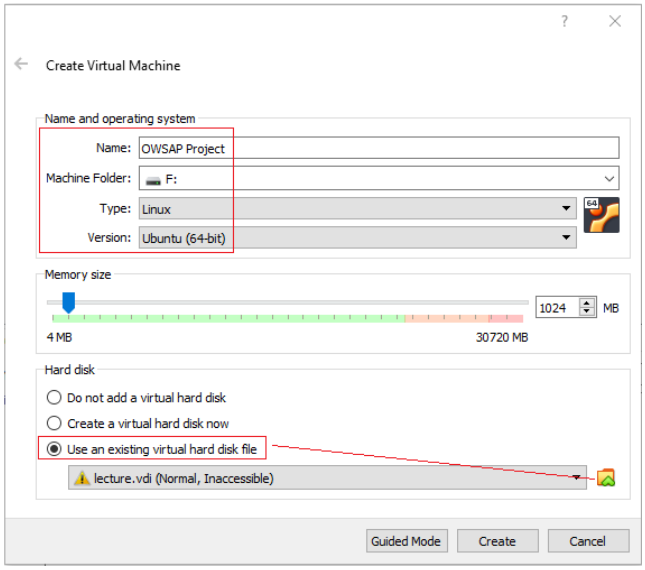
For the Type, select Linux.

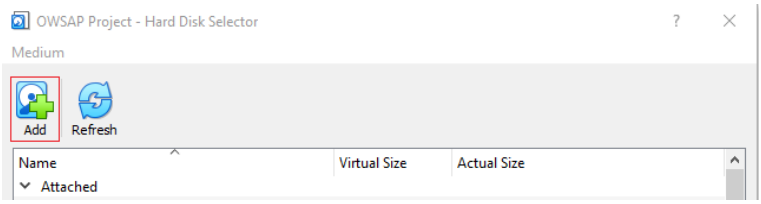
For the version, select Ubuntu (64 -bit)

At the bottom of the window, select the radio Button to Use an existing virtual hard disk file.

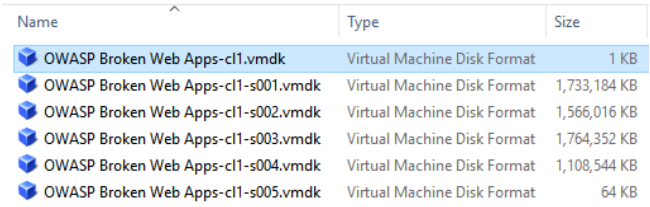
Over to the right of the screen, click on the folder icon to browse to the extracted folder location.

On the next screen, click the add button.

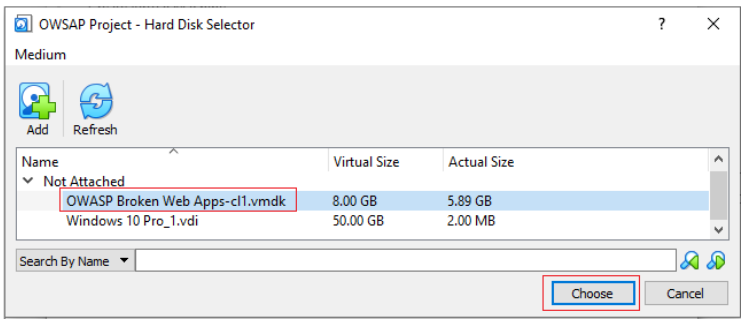




Select the file shown in the following image.

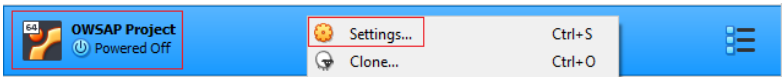


Back at the hard disk selector page, ensure that your disk is selected and click on, **Choose**.



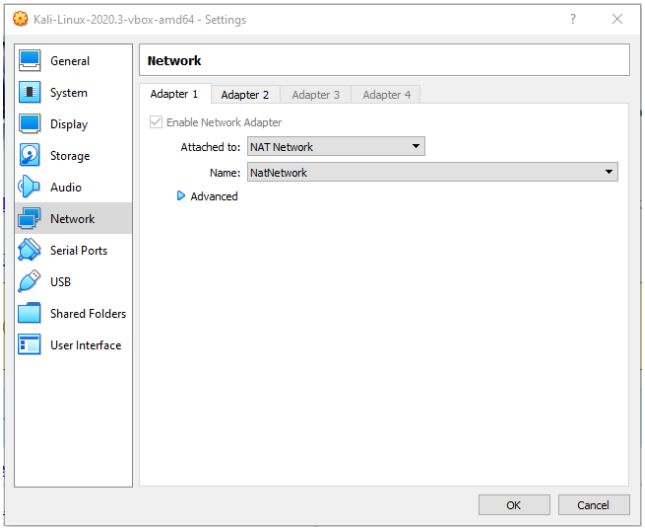
At the next screen, click on Create.

From the left Windows pane, find your newly created virtual install of OWSAP. Right-click on the machine's name, and from the context menu, select Settings.



Caveat!

I could not get OWSAP and Kali to communicate until I configured both with their NAT Network network setting. I tried Host-only and NAT, but they could not see each other until I configured both with NAT Networking.



Click OK

Back at the left windowpane, x2 click your newly created virtual install of OWSAP.

Once fully booted, log in as **`root`** with the password **`owaspbwa`**.

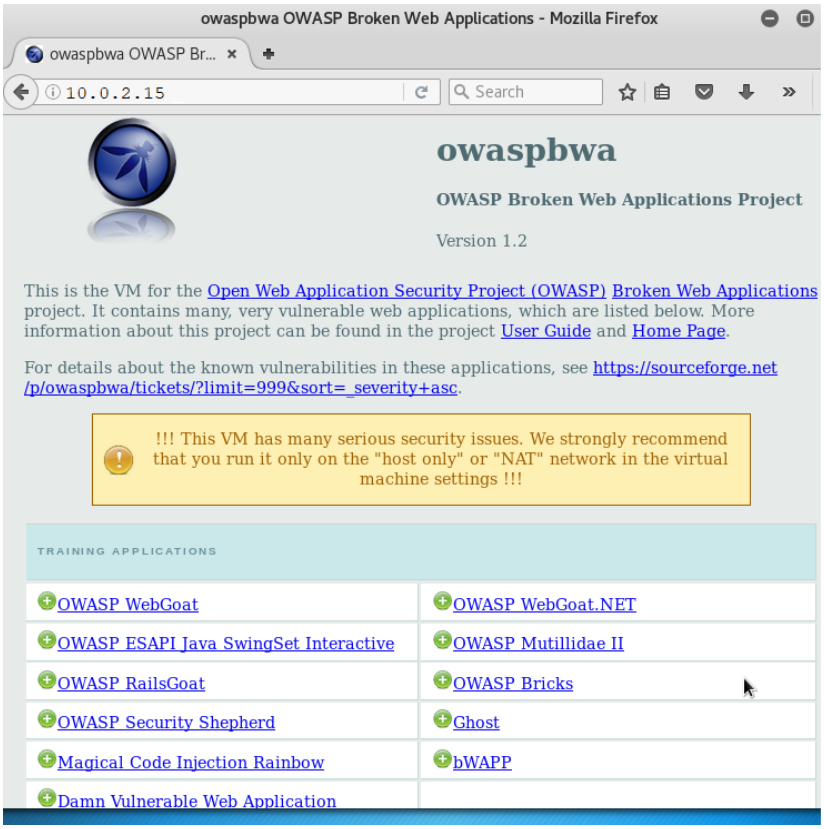
Ensure that you are receiving an IP address from DHCP by issuing ifconfig eth0 from the command line.

```
owaspbwa login: root
Password:
Login timed out after 60 seconds.


OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login: root
Password:
Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://10.0.2.15/

You can administer / configure this machine through the console here, by SSHing
to 10.0.2.15, via Samba at \\10.0.2.15\, or via phpmyadmin at
http://10.0.2.15/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# _
```

Results for ifconfig.

```
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://10.0.2.15/

You can administer / configure this machine through the console here, by SSHing
to 10.0.2.15, via Samba at \\10.0.2.15\, or via phpmyadmin at
http://10.0.2.15/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7a:1a:2a
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7a:1a2a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:103 errors:0 dropped:0 overruns:0 frame:0
          TX packets:199 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12086 (12.0 KB)  TX bytes:137993 (137.9 KB)
```

Open your Kali browser and type the IP address assigned to your OWASP machine at the address bar. You should see the following page.



End of the lab!