**Lab - Heartbleed OpenSSL Exploit Vulnerability**

**Overview**

In this lab, you will learn about the Heartbleed vulnerability. Heartbleed is a vulnerability that came to light in April of 2014; it allowed attackers unprecedented access to sensitive information and was present on thousands of web servers, including those running major sites like Yahoo.

Heartbleed was caused by a flaw in OpenSSL, an open-source code library that implemented the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. In short, a malicious user could easily trick a vulnerable web server into sending sensitive information, including usernames and passwords.

**OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable**

During communication, OpenSSL uses a “heartbeat” message that echoes back data to verify that it was received correctly. In OpenSSL 1.0.1 to 1.0.1f, a hacker can trick OpenSSL by sending a single byte of information telling the server that it sent up to 64K bytes of data that needs to be checked and echoed back.

Heartbleed can be used to capture secret keys used for X.509 certificates, usernames and passwords, instant messages, emails, and business-critical documents and communication. Leaked secret keys allow the attacker to decrypt any past and future traffic and to impersonate the service at will. Any protection given by the encryption and the signatures in the X.509 certificates can be bypassed.

Though this vulnerability has been patched, this material is still testable on the CompTIA Pentest+ exam.

**Lab Requirements**

* One virtual install of Kali Linux
* One virtual install of SEED Ubuntu 12.04

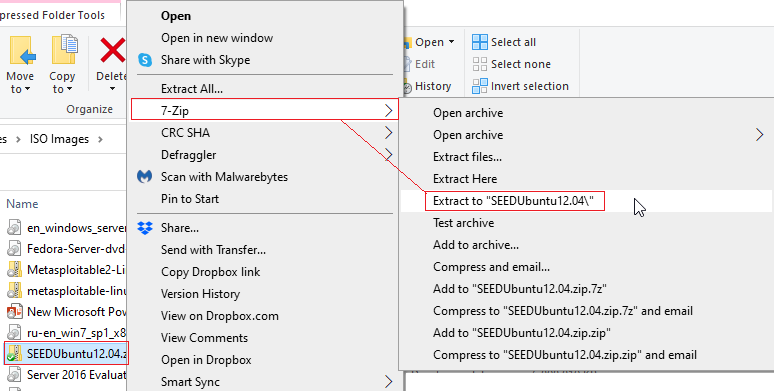
Download SEED Ubuntu 12.04

Use the following link to download your target image for this lab. This is a specially created image of Ubuntu deliberately made vulnerable for the Heartbleed vulnerability.

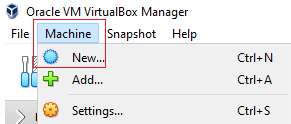
Download SEED Ubuntu 12.04 using one of the following links.

* Syracuse University: [SEEDUbuntu12.04.zip](http://www.cis.syr.edu/~wedu/SEEDUbuntu12.04.zip)
* DigitalOcean: [SEEDUbuntu12.04.zip](https://seed.nyc3.cdn.digitaloceanspaces.com/SEEDUbuntu12.04.zip)
* Zhejiang University: [SEEDUbuntu12.04.zip](https://pan.zju.edu.cn/share/f2a4d37206eee87798702b3cc2)

Once you have downloaded the target machine, you will need to extract the contents.



Open your VirtualBox Management Console. Click on **Machine,** and from the context menu, select **New**.

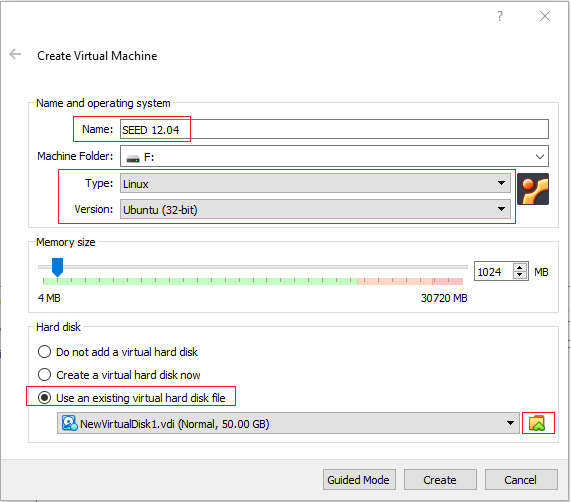


This launches the **Create a Virtual Machine** wizard. Give your target a user-friendly name

For the type, select **Linux**.

For the version, select **Ubuntu (32-bit)**.

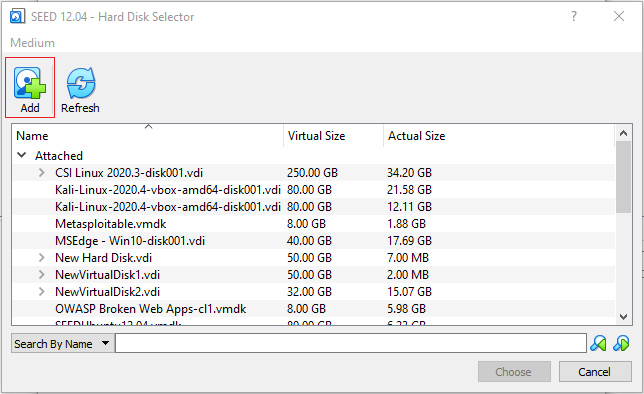
Under **Hard Disk**, select the radio button to **Use an existing virtual hard disk file**.



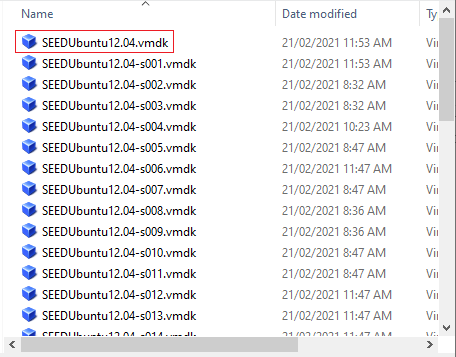
Click on the folder icon to browse to the location of your extracted target folder.



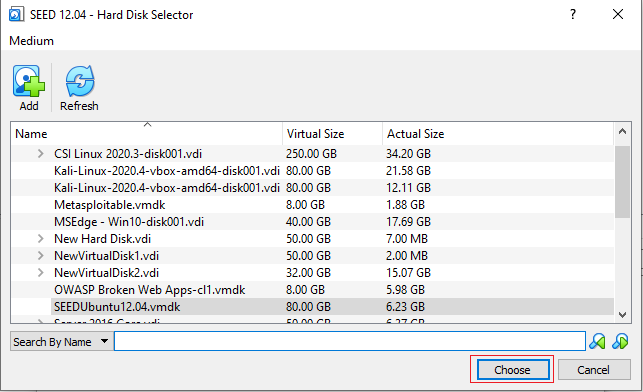
On the next screen, click the **Add** button.



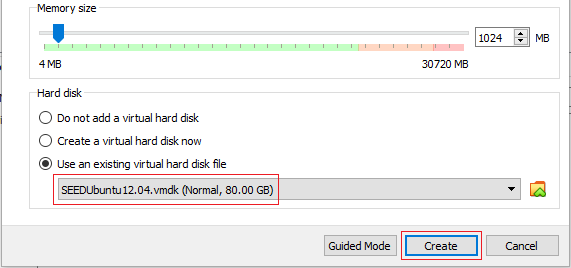
Select the top vmdk file from the list of available files—2X click.



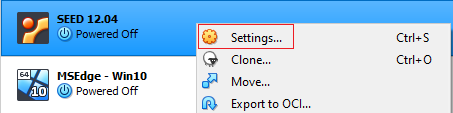
Back at the Hard Disk Selector screen, click the choose button. The correct file has already been chosen.



On the last screen, click the **Create** button.

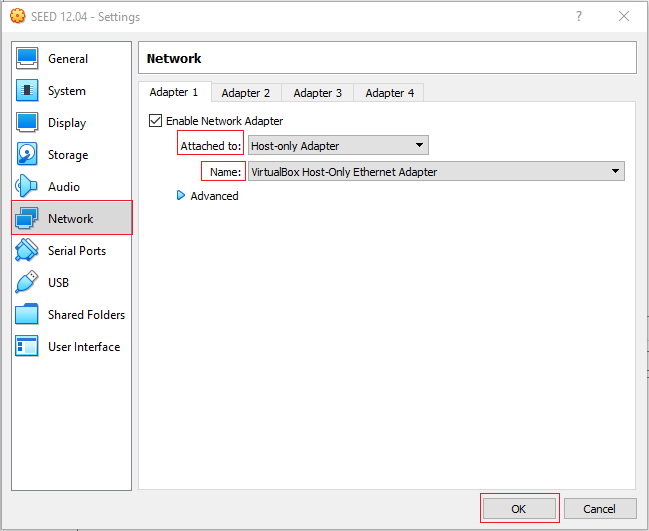


From your VirtualBox manager’s left windowpane, right-click your target VM and from the context menu, select **Settings**.



In the left windowpane of your settings properties, click on **Network**.

In the right windows pane under **Attached to**, select **Host-only Adapter**. In the **Name** dialog box, select the **VirtualBox Host-only Ethernet Adapter**.

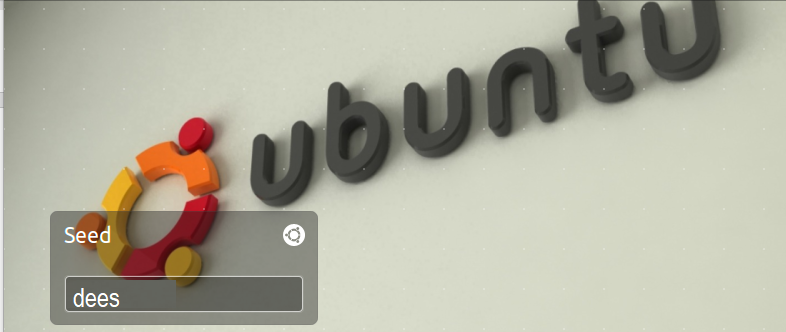


From the left windowpane of your VirtualBox manager, find your target VM and 2X click to launch.



Ensure your Kali machine uses the Host-only adapter for its networking and uses the same adapter name as the target. Launch your Kali machine.

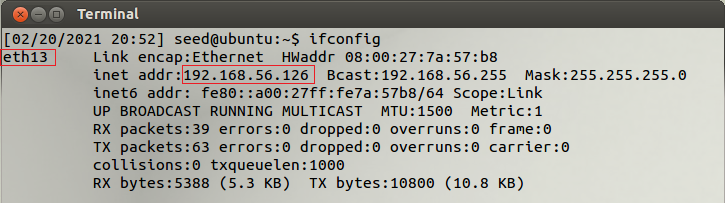
At the login screen, type in the password, **dees**



Wait for the desktop to load, and from the quick launch bar on the left, scroll down, find the terminal shortcut, and launch.



At the terminal prompt type, **ifconfig**. Find your IP address assigned to your eth adapter. Take note, as this will be your target IP. (This is my IP address, yours will differ!)

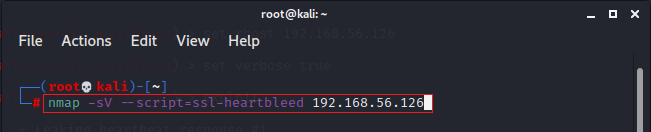


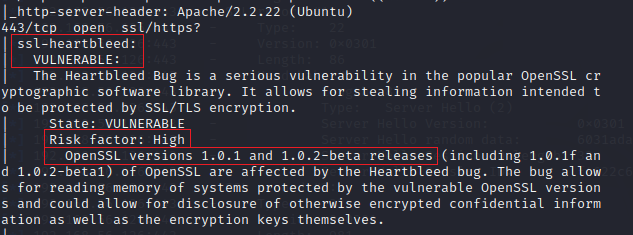
Leave your target machine up and running. From the desktop of your Kali machine, launch a new terminal.

**Check for Heartbleed Using Nmap**

We can use the following Nmap script to check to see if a server is vulnerable to Heartbleed.

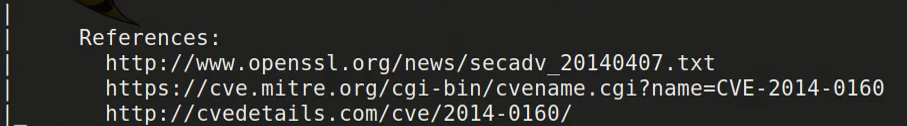
nmap -sV --script=ssl-heartbleed 192.168.56.126





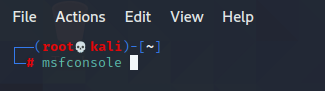
We have confirmed our target is vulnerable to the Heartbleed vulnerability, and with a high-risk factor, we mean we have a high probability of exploiting this server. Further down, you can see the versions of OpenSSL that are present and vulnerable on the target server.

Under references, you are provided with linked resources you can use to learn more about the vulnerability.



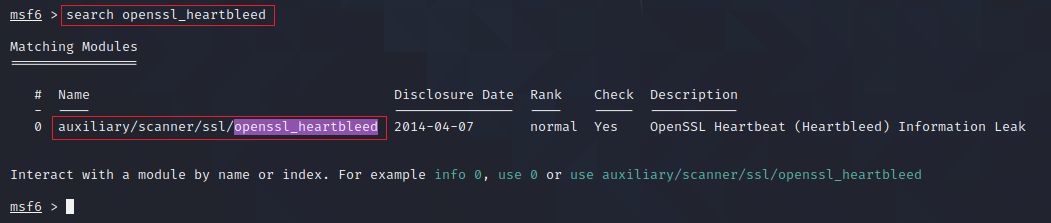
**Check for Heartbleed using Metasploit**

Metasploit will allow us to scan and then test for the vulnerability.



Open a new terminal and at the prompt type, **msfconsole**. At the msf prompt, search the heartbleed module using the following query.

**search openssl\_heartbleed**

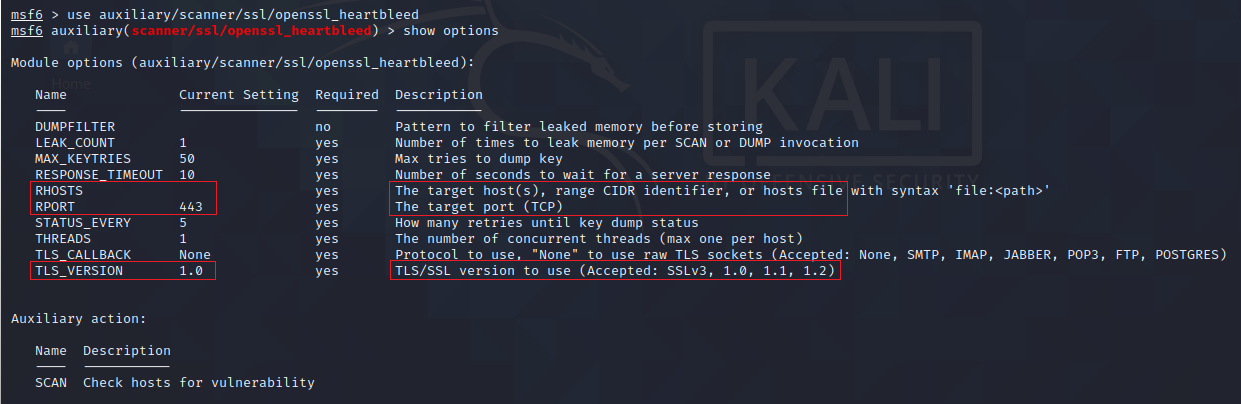


Highlight and copy the full name of the module. At the **msf** prompt, type the word, **use** and paste by the module’s name—press enter.



At the next prompt, type, **show options**.

From the options, you can choose your version of SSL to scan for, but we need to worry about supplying the IP address of the remote host or target. By default, SSL runs on port 443, and that is already set for us.

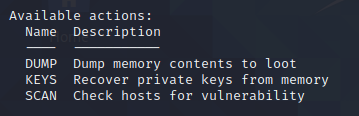


Set the rhost using the IP address of your target machine.

**set rhost 192.168.56.126** (This is my target’s IP address, your will differ)



No need to set the rport as we already know SSL is running on port 443. At the prompt, if we type, **show info,** we see how we can expand on this module’s functionality.Under actions, we have additional options we can perform.



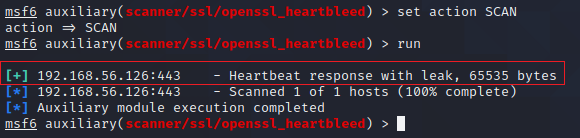
We can also set the module to scan for additional information using the following command.

To check for the presence of the vulnerability, we can use the scan option.

**set action SCAN**

At the prompt type, **run**.

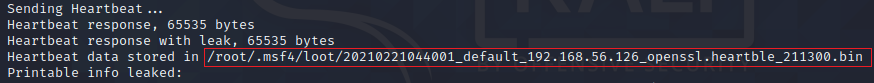
From the response, you can confirm that we have a heartbleed response of 65,535 bytes, and we are shown the data captured. This confirms the server is vulnerable.

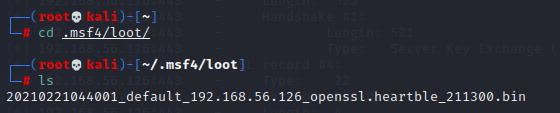


We can also use the DUMP action to capture a memory dump from the server.



The information captured looks the same, but you will see that it does differ if you look closely. If the admin had logged on recently, we would see their username and password for the administrator account. Another feature of the DUMP action is that the memory dump file is saved to your local machine.

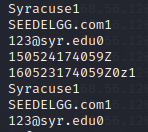




We can open a new prompt and use strings to examine the dump file. Copy the path of the dump file starting just after the /root. Open a new terminal and at the prompt type strings followed by the memory dump file’s path.

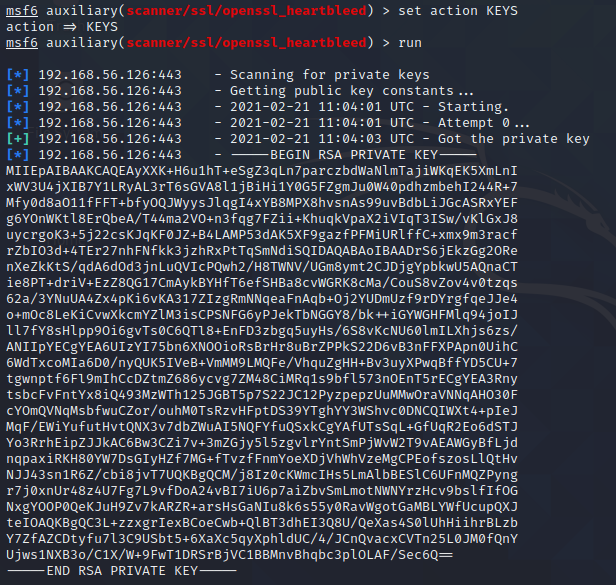


As we scan through the strings, we find some email addresses and a session key. If any username and password were used during the session to log onto one of the affected programs using SSL, this too would have been captured in the dump

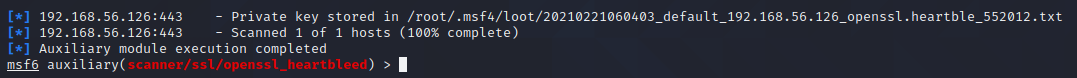
 

The next action we can scan for is to try and capture any keys present on the server.

**Set action KEYS**



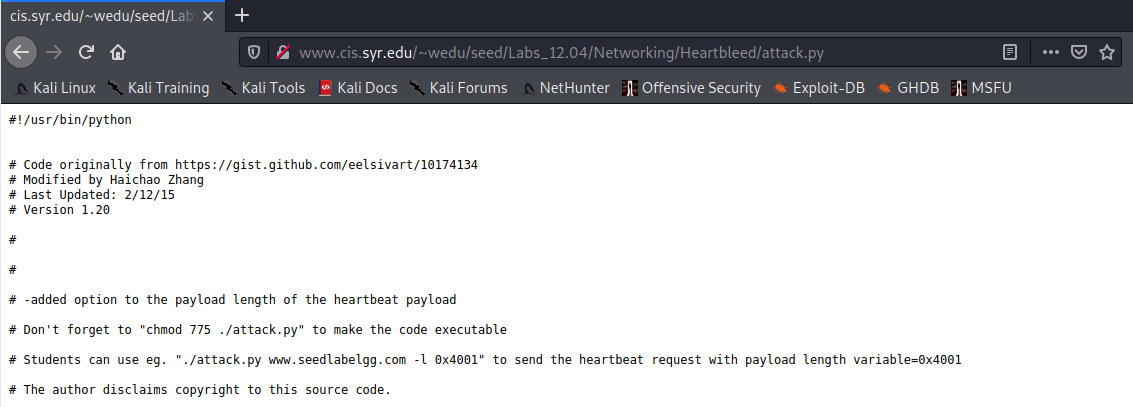
The key is conveniently saved as a text file to your local machine.



**Check for Heartbleed Using a Script**

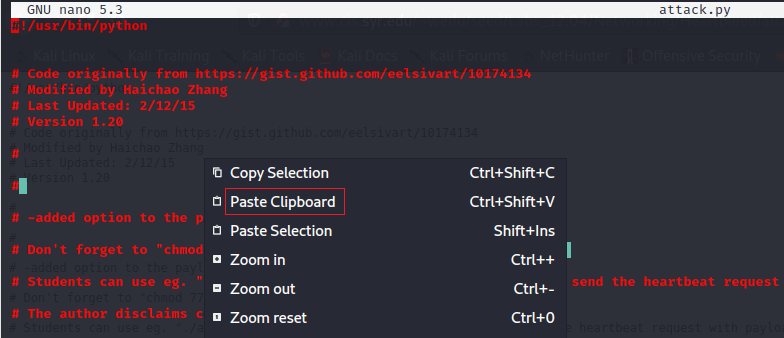
The third way we can check for the Heartbleed vulnerability is to use a python script. These scripts are readily available on the Internet. From your Kali desktop, open a browser. The script used in this lab can be found using the following link.

<http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Networking/Heartbleed/attack.py>



Highlight and copy the entire script.

From your Kali machine, open a new terminal. At the prompt type, **nano attack.py.** Place your mouse inside the empty text file, right-click, and select **Paste Clipboard** from the context menu**.**

****

Press **Ctrl+x** to save the file. When asked to save the changes to the buffer, press ‘**y**’ for yes. Press **enter** to close the text editor.

****

**Make the script executable.**

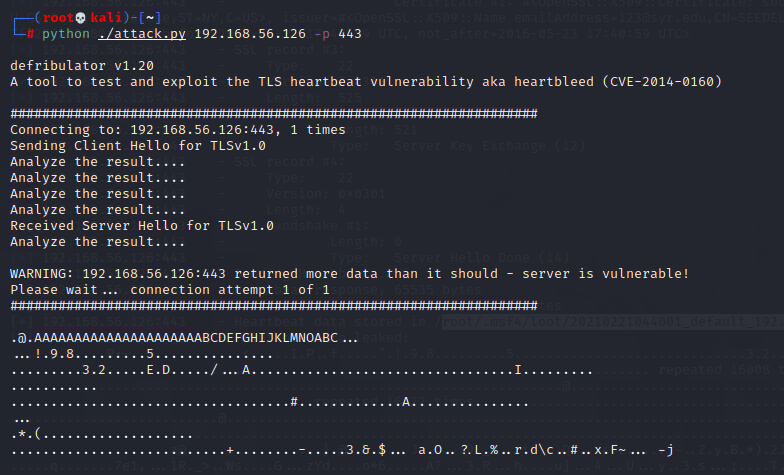
At the terminal prompt, type **chmod 775 ./attack.py** to make the script executable.

**Launch the script**

At the terminal prompt, type

**python .attack.py <target IP> -p 443**

The target is quickly scanned.



**Summary –**

The Heartbleed vulnerability was introduced into the OpenSSL crypto library in 2012. It was discovered and fixed in 2014, yet today—7 years later—there are still unpatched systems. Perhaps that is why you find the exploit still being testable on some of the more popular cybersecurity exams, such as the CompTIA Pentest+.

This is worth learning because the tools and methods are the same as those used by bug bounty hunters. Heartbleed was discovered by bounty bug hunter Neel Mehta, who received a $15,000 reward from [Hackerone](https://www.hackerone.com/) for the discovery.