Todd Wenker

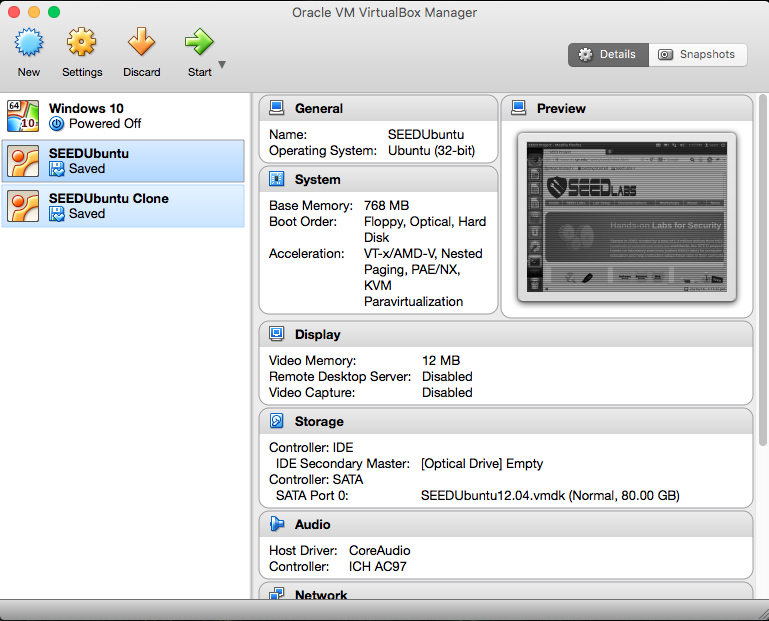
ASU ID: 1206233882

Lab Assignment 7

HeatBleed Lab

**Summary:** The goal of the lab is to conduct the Heartbleed exploit on a basic social media website. The website will be hosted on a on one of two virtual machines, with the other one running a script that will conduct the exploit.

**Network Setup:**



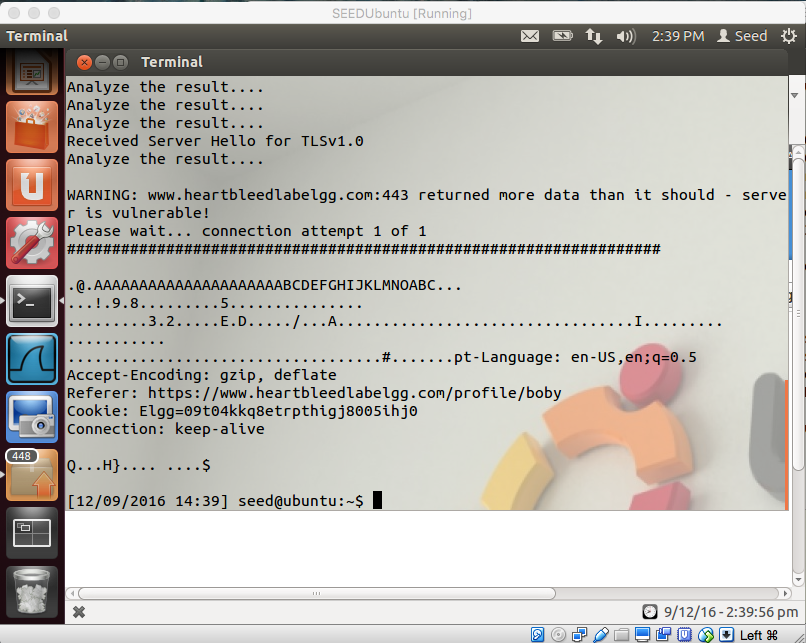
The network is comprised of two virtual machines, with SEEDUbuntu (designated VM1 from here on) the attacker virtual machine and SEEDUbuntu Clone (designated VM2) being the host of the website.

**Software Packages Used:**

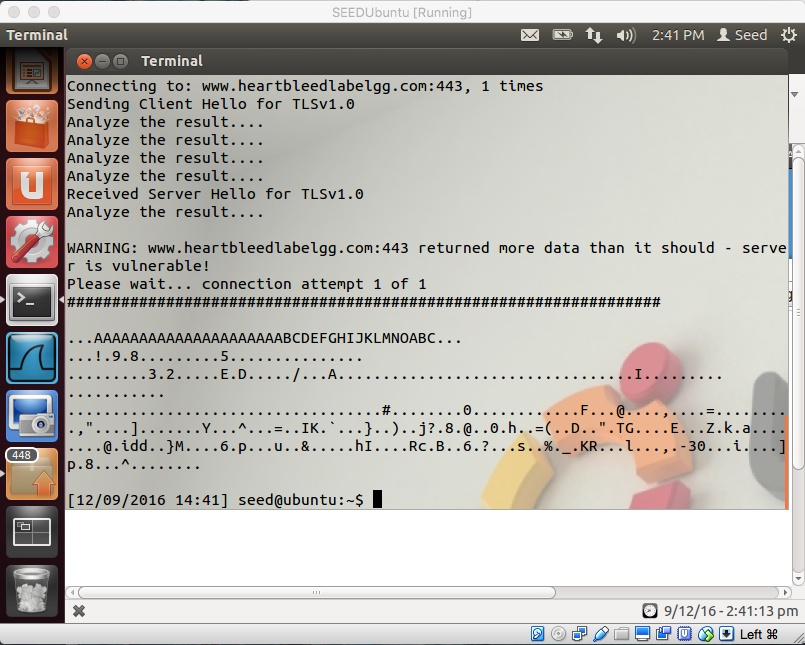
* A python script that will conduct the HeartBleed exploit.

**Lab Task:**

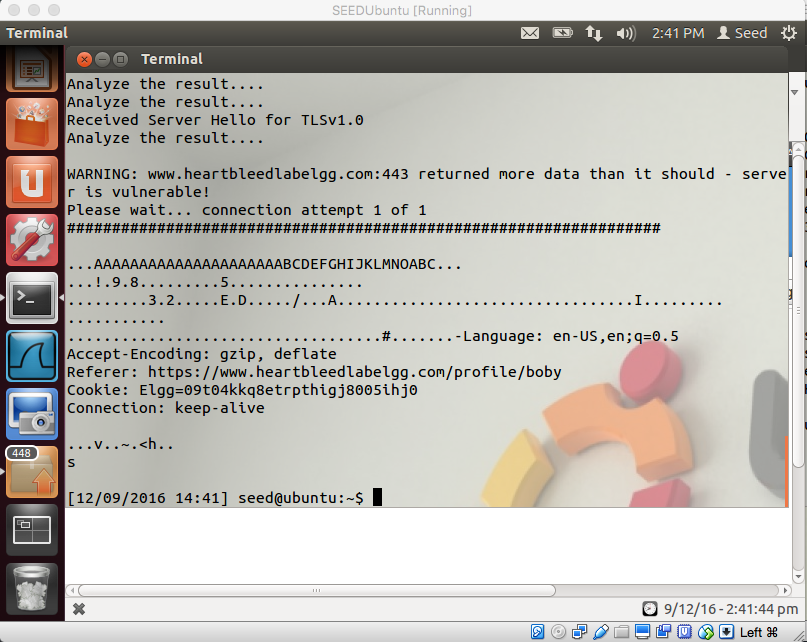
First, the website ‘www.heartbleedlabelgg.com’ needs to assigned to VM2. This is done by editing VM1’s hosts file by using the command *vim /etc/hosts* and changing the line *127.0.0.1 www.heartbleedlabelgg.com* to *10.0.2.5 www.heartbleedlabelgg.com* with 10.0.2.5 being the IP address of VM2. Next, VM1 access the website and logins as admin, adds Bob as a friend and sends them message (just a series of the letter A). Then, VM1 uses the command *chmod +x attack.py* to allow attack.py to be executed and then runs the script using *./attack.py www.heartbleedlabelgg.com.* Below are the results of the script.



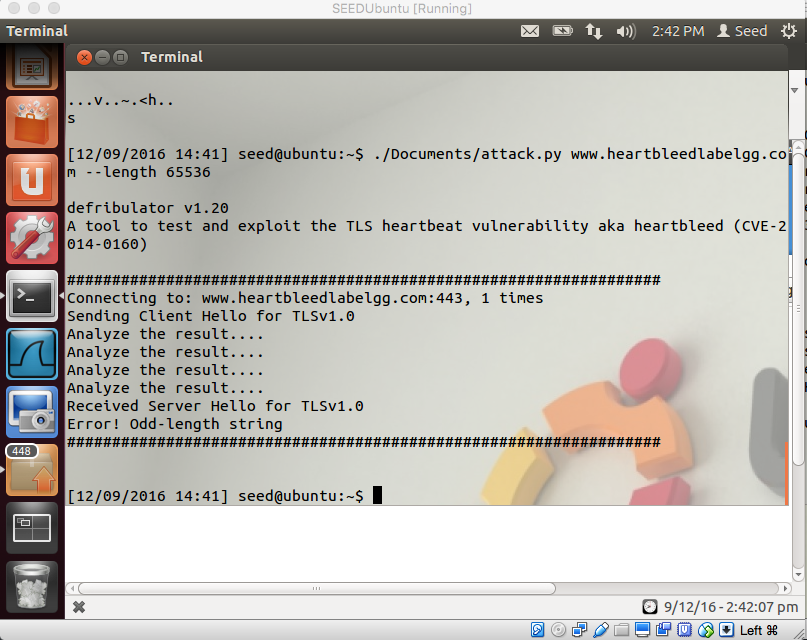
After running the exploit, the VM2 sent a portion of its memory back to VM1. It includes the cookie data and other information.



Above is the result of running the command *./attack.py* [*www.heartbleedlabelgg.com*](http://www.heartbleedlabelgg.com) *--length 4096.*



Above is the result of the command *./attack.py* [*www.heartbleedlabelgg.com*](http://www.heartbleedlabelgg.com) *-length 65535.*



Above is the result of the command *./attack.py* [*www.heartbleedlabelgg.com*](http://www.heartbleedlabelgg.com) *--length65536.*