Talal Jawaid

11/24/2019

Lab 4

Heartbleed

1. This lab is a demo of the Heartbleed exploit which went famous last year.
2. You need to set up two VMs and then make sure there is cross communication

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

You then want to make sure you have permissions to run attack.py

A screenshot of a cell phone screen with text

Description automatically generated

You also want to make sure to edit hosts file

A screenshot of a cell phone

Description automatically generated

After adding Bobby as a friend and sending him a message, you can then run the attack.py on the website

A close up of text on a white background

Description automatically generated

This will dump server memory for exploitation purposes.

You can use countermeasures such as updating to latest openssl

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

There are bugs in this code, but one that I see of the bat is that there is buffer overflow due to buffersize not being large enough for the memory attempted to place in it.