Vigomar Kim Algador

CSC 154 - 01

Professor Jun Dai

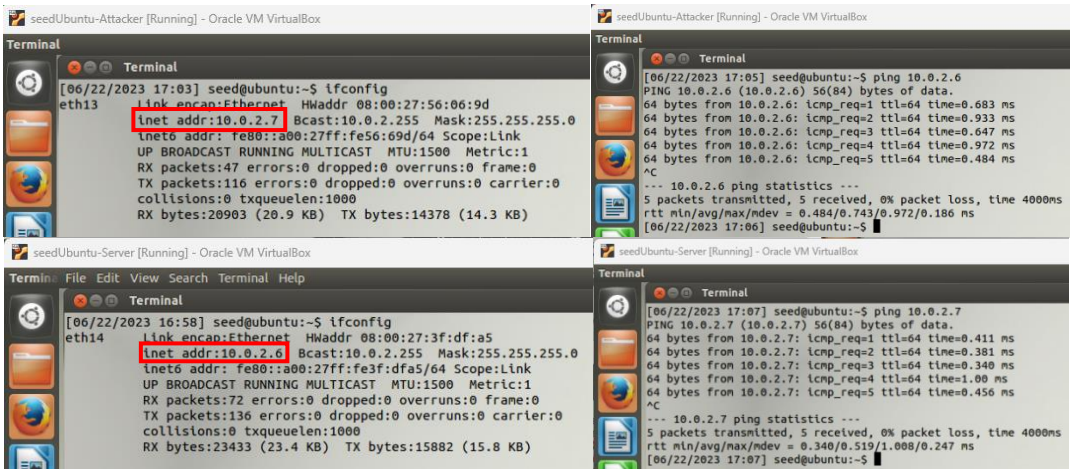
25 June 2023

LAB 4 - HEARTBLEED

The goal of this laboratory is to fully understand the weakness of the implementation of the Heartbeat protocol. This laboratory will show the students on the vulnerability of this attack and how to fix it. Heartbleed bug is a severe implementation flaw in the OpenSSL library, which enables attackers to steal data from the memory of the victim server.

For this laboratory, we need to setup two machines: an attack machine and a victim machine. We will be using SEEDUbuntu for both VMs and test if they both communications. In addition, we named attack machine as seedUbuntu-Attacker and victim machine as seedUbuntu-Server. We grabbed the IP address of both VMs to test if they both communicate with each other.

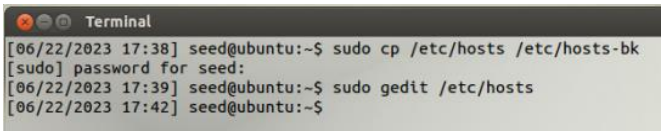
```
Command: ifconfig
         ping <IP address>
```

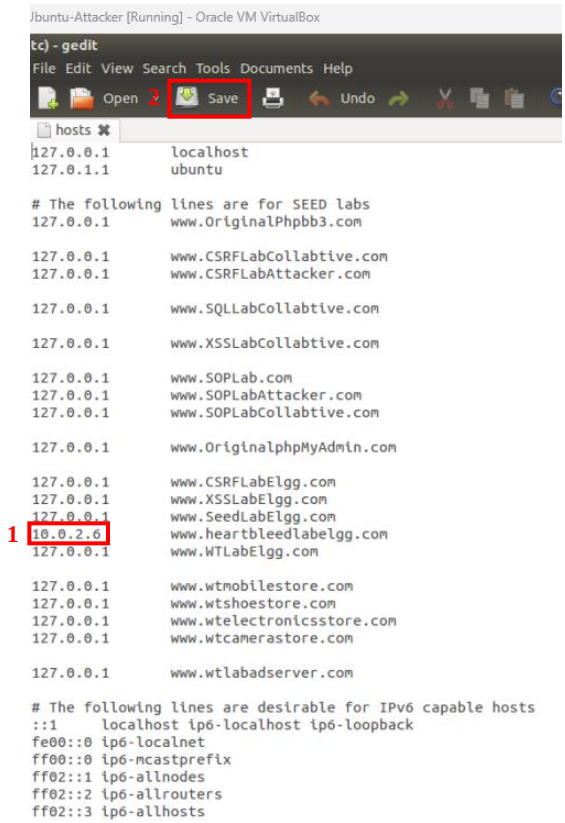


From the screenshots above, we got the IP addresses: 10.0.2.7 (attacker) and 10.0.2.6 (victim). We also use the ping command and confirmed that both machines are able to communicate with each other.

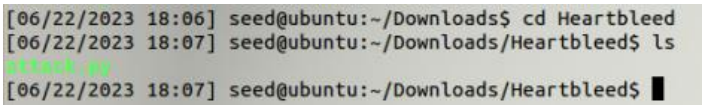
For the next step, we need to modify the `/etc/hosts` file on the attacker machine to map the server name to the IP address of the server VM. To do this, we need to search the following line in `/etc/hosts`, and replace the IP address `127.0.0.1` with the actual IP address of the server VM that hosts the `ELGG` application. For safety, we need to have a copy of `/etc/hosts` file if we doing any changes.

```
Command: sudo cp /etc/hosts /etc/hosts-bk
         sudo gedit /etc/hosts
```



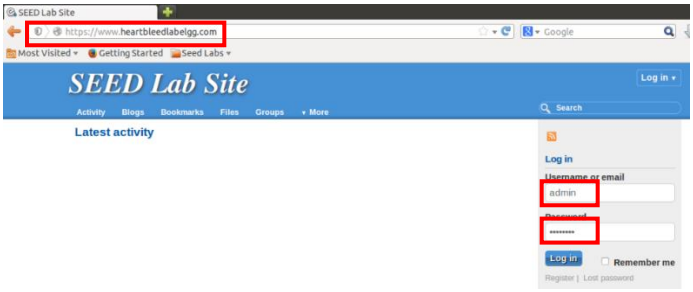


After, we need to confirm that the attack.py file is in the attacker machine. Navigating through our folder, we confirmed that the attack.py file is available under Heartbleed folder and the file is executable. This file will be used later for our attack.

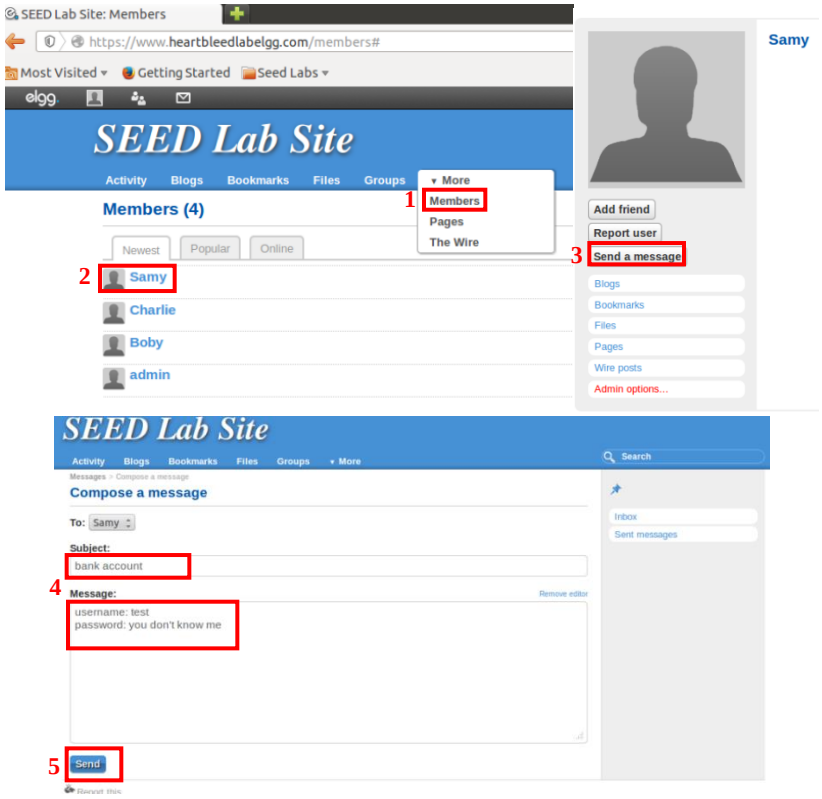


Task 1. Launch the Heartbleed Attack

For this task, we need to launch the Heartbleed attack on our social network site and see what kind of damages can be achieved. The actual damage of the Heartbleed attack depends on what kind of information is stored in the server memory. First step is to visit https://www.heartbleedlabelgg.com from browser and login as the site administrator.



After we login, we need to navigate to “More” tab, then click “Members”, and we can choose any of the members we want to. For this one, we chose Samy and send a message. Then, we need to compose a message with a subject and content of the message, and click send.



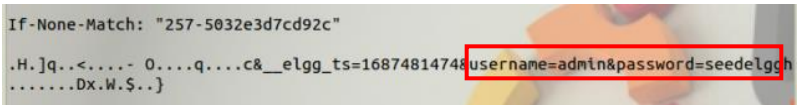
After that, we can start the attack by running the attack.py file. The command is shown below.

```
Command: ./attack.py www.heartbleedlabelgg.com -l 0x4000
```

```
[06/22/2023 18:07] seed@ubuntu:~/Downloads/Heartbleed$ ./attack.py www.heartblee
dlabelgg.com -l 0x4000
```

However, we need to run the attack code multiple times to get useful data.

After running multiple times, we were able to get the information of the message we sent earlier which shows the example bank account username and password.



On the other hand, we were also able to get the admin credentials and would be able to gain administrative control of the website.