

LAB 10 - HEARTBLEED ATTACK LAB

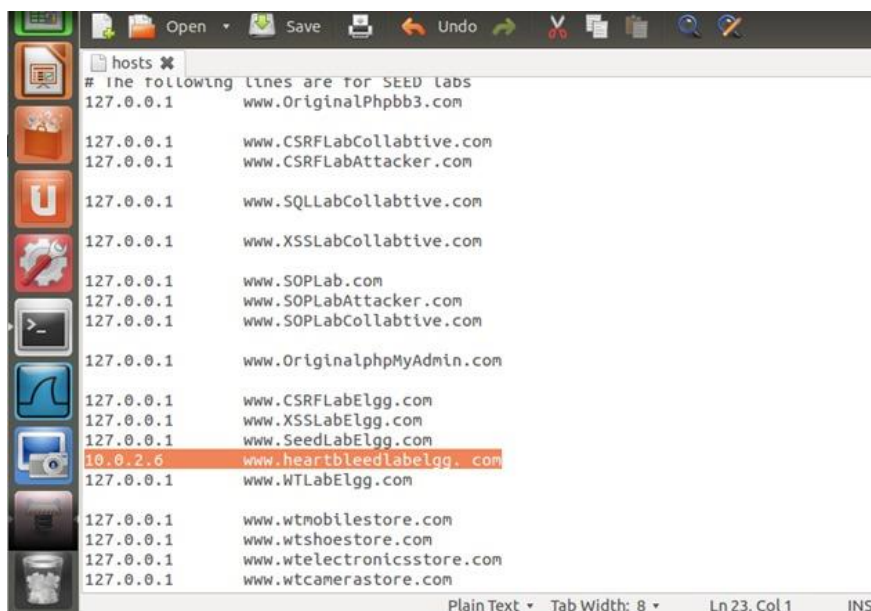
NAME: NAVYA PERAM

SRN: PES1UG21CS924

Step 1

In the given process, we have used the `sudo gedit /etc/hosts` command to open and modify `/etc/hosts` on the attacker's machine. We have changed the ip address of the heartbleed website to that of the victim's web server's ip, which is 10.0.2.6. We have done so, to make them believe that the website is on the server machine. Hence the change in ip.

```
PES1UG21CS924:navya:/w/n/$>sudo gedit /etc/hosts
PES1UG21CS924:navya:/w/n/$>
```



Step 2

We make `attack.py` executable by using the below command. We used `sudo chmod 777` to change the permissions of the file to give anyone full read, write, and execute permissions.

```
PES1UG21CS924:navya:/w/n/$>cd Downloads/
PES1UG21CS924:navya:/w/n/$>sudo chmod 777 attack.py
PES1UG21CS924:navya:/w/n/$>ls -l
total 20
-rwxrwxrwx 1 seed seed 19100 Nov 18 23:15 attack.py
PES1UG21CS924:navya:/w/n/$>
```

After giving the permissions to the `attack.py` file, we ran the file. We used this program to send a malicious heartbeat request to the website on the server. The website then send random data from the server. This vulnerability allows attackers to steal sensitive data, such as usernames, passwords, and encryption keys, from affected servers. This occurs through a vulnerability present in the OpenSSL crypto library. The vulnerability is caused by a flaw in the implementation of the TLS

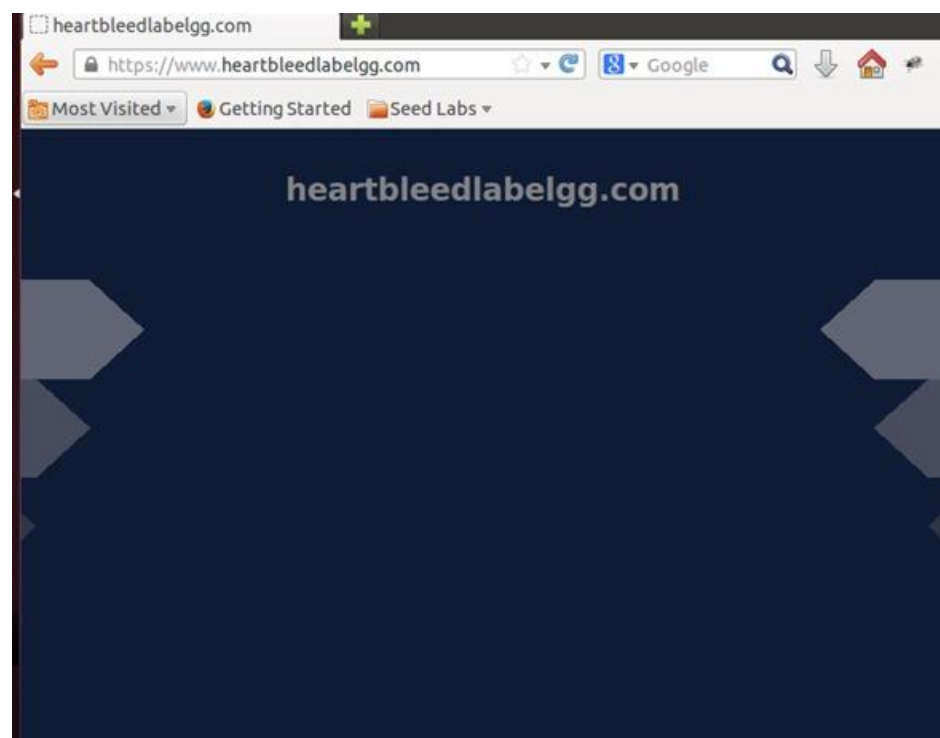
heartbeat extension. The heartbeat extension is used to keep a secure connection alive by periodically sending a small piece of data (a heartbeat) from one end of the connection to the other. Essentially, a malformed heartbeat request sent by an attacker can trick the server into responding with more data from it's memory than required, therefore giving out more sensitive information. Here, we have sent a heartbeat request to the server which is accepted and then we are able to view the website.

```
PES1UG21CS924:navya:/w/n/$>python attack.py www.heartbleedlabelgg.com

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result...
Analyze the result...
Analyze the result...
Analyze the result...
Received Server Hello for TLSv1.0
Analyze the result...
Received alert:
Please wait... connection attempt 1 of 1
#####
.
```

We were able to view the website.



I was unable to log in as admin in the website. Hence, I couldn't do the further steps.