HeartBleed

SSL issues are still lurking in the wild! Can you exploit this web servers OpenSSL?

Introduction to Heartbleed and SSL/TLS

On the internet today, most web servers are configured to use SSL/TLS.

SSL(**secure socket layer**) is a predecessor to TLS (transport layer security). The most common version are TLS 1.2 and TLS 1.3(recently released). Configuring a web server to use TLS means that all communication from that particular server to a client will be encrypted; any malicious third party that has access to this traffic will not be able to understand.decrypt the traffic, and they also will not be ablt to modify the traffic.

Heartbleed is a bug due to the implementation in the OpenSSL library from version 1.0.1 to 1.0.1f(which is widely used)**. it allows a user to access memory on the server(**which they usually worldn't have access to). **this in turn allows a malicious user to access different kinds of information Including:**

- server private key
- confidential data like usernames, passwords, and other personal infromation

Analysing the BUG

The implementation errors occurs in the heartbeat message that OpenSSL uses to keep a connection alive even when no data is sent, A mechanism like this is important because if a connection dies/resets quite often, it would be expensive to set up the TLS

aspect of the connection again; this affects the latency across the internet, and it would make using services slow for users, A heartbeat message sent by one end of the connection, when the server retrieves this message from the client, here's what it does:

- The server constructs a pointer(memory location) to the heartbeat record
- It then copies the length of the data sent by a user into a variable(called payload)
    - The length of this data is unchecked
- The server then allocates memory in the form of:
- 1 + 2 + payload + padding(this can be maximum of 1 + 2 + 65535 + 16)
- The server then creates another pointer(bp) to access this memory
- The server then copies the payload number of bytes from data sent by the user to the bp pointer
- The server sends the data contained in the bp pointers to the user.

Remediation

To ensure that arbitrary data from the server isn't copied and sent to a user, the server needs to check the length of the heartbeat message:

- Ther server needs to check that the length of the heartbeat message sent by the user isn't 0
- The server needs to check the length doesn't exceed the specified length of the variable that holds the data

References:

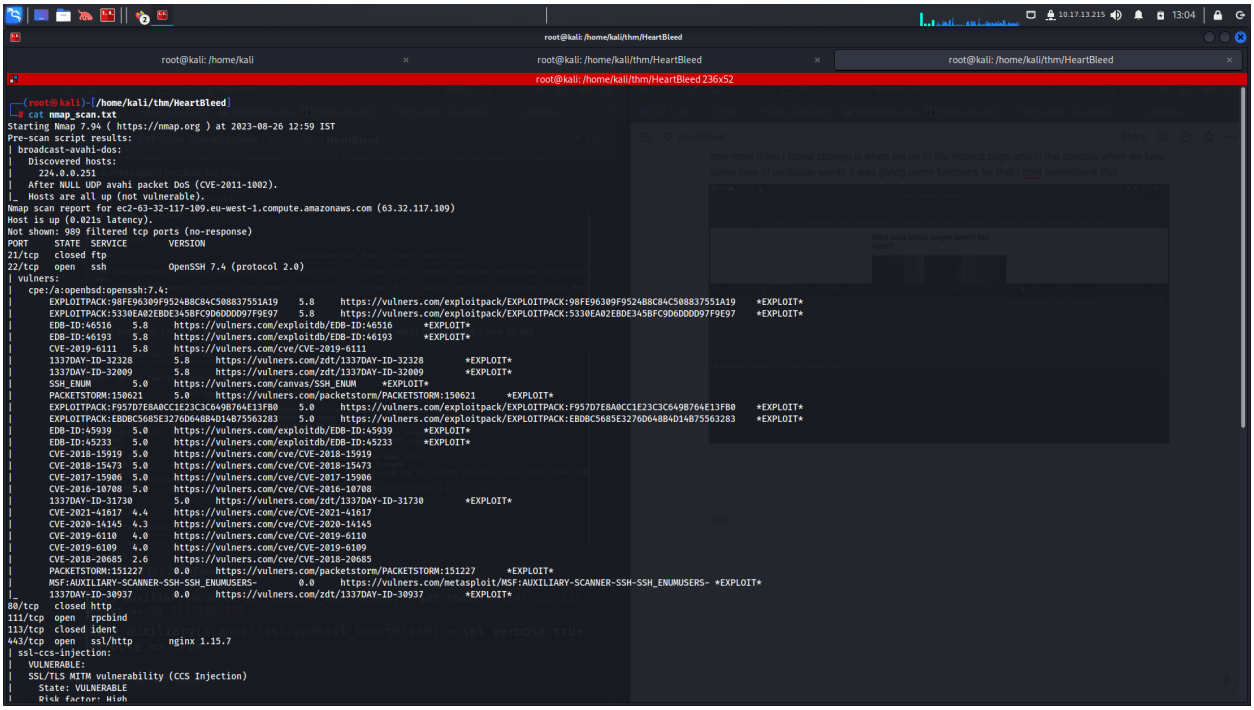
- **http://heartbleed.com/**
- **https://www.seancassidy.me/diagnosis-of-the-openssl-heartbleed-bug.html**
- **https://stackabuse.com/heartbleed-bug-explained/**

1. **what is the flag?**

lets start with nmap scan and it is not as usual scan

we should use —script vuln here

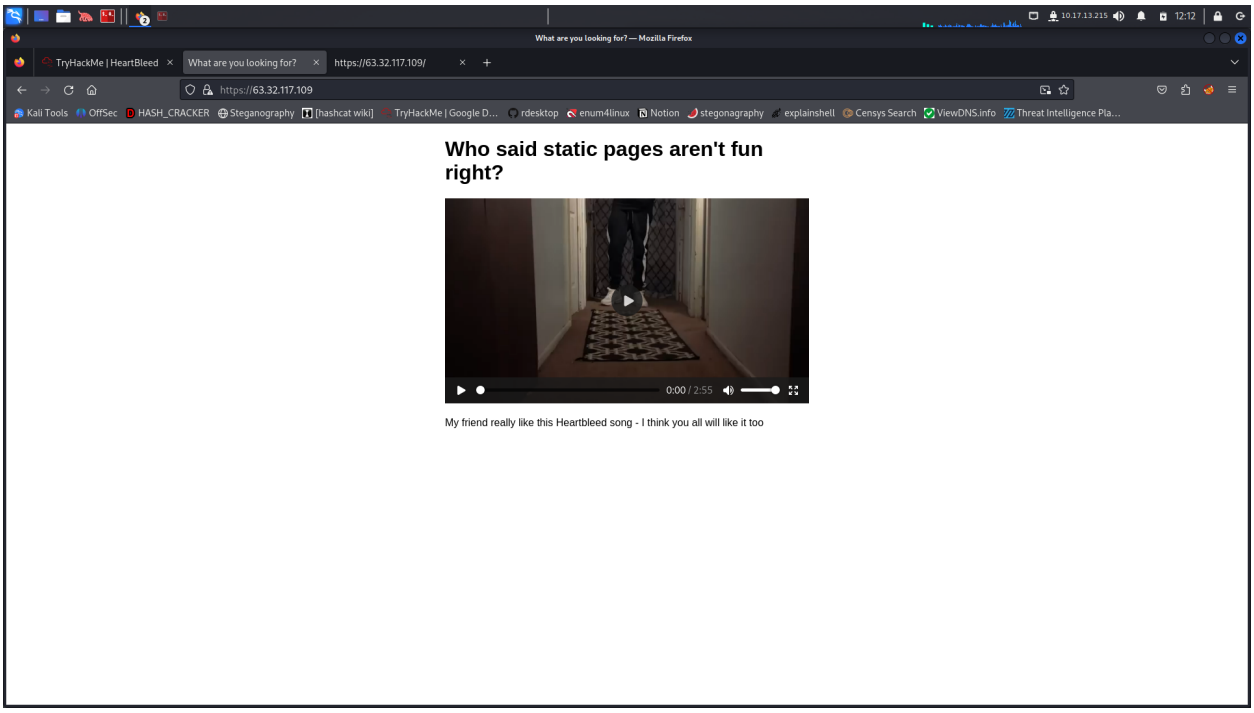
With the --script vuln option, Nmap will then run scripts from the "vuln" category against the open ports and services to identify potential vulnerabilities. These scripts might perform tests or checks that are known to expose vulnerabilities in certain services or configurations.



nmap_scan.txt

the hint given was use the <IP> in the browser

lets do it

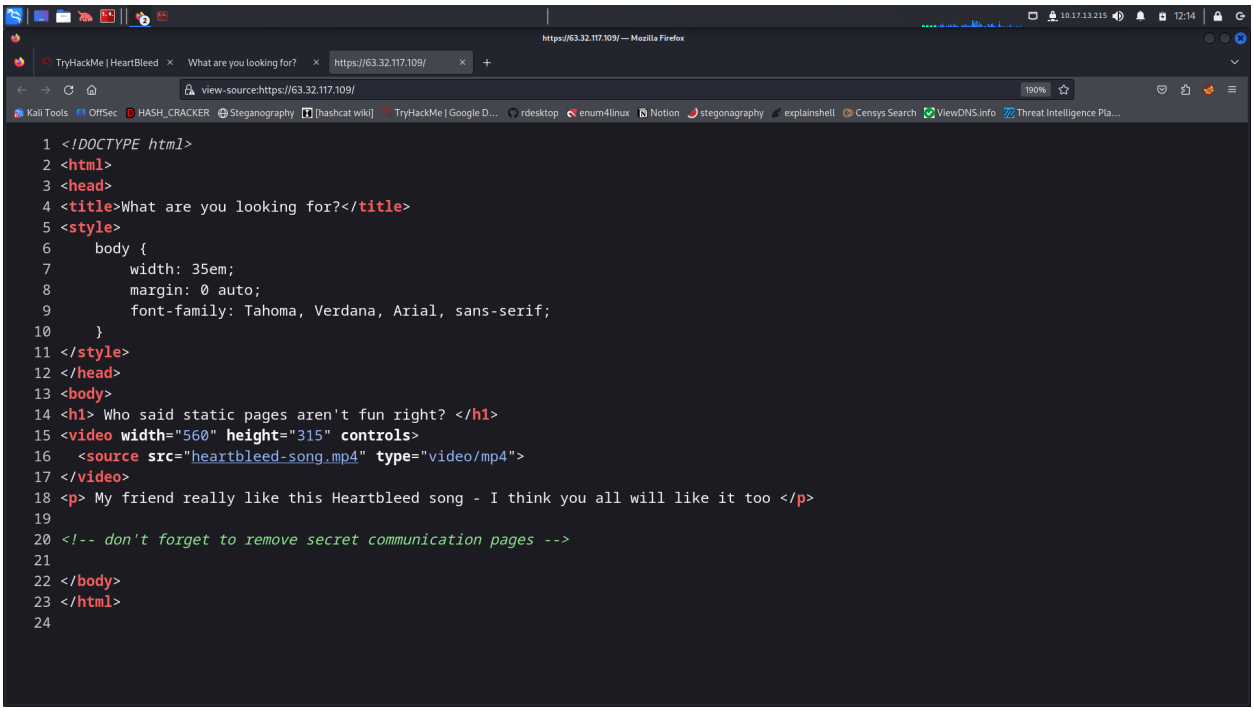


some video was there in the website but it before getting the page i got the security issue that it was not safe

i proceed cause it was virtual machine and trusted platform

and below the video i can see some text “My friend really like this Heartbleed song - I think you all will like it too”

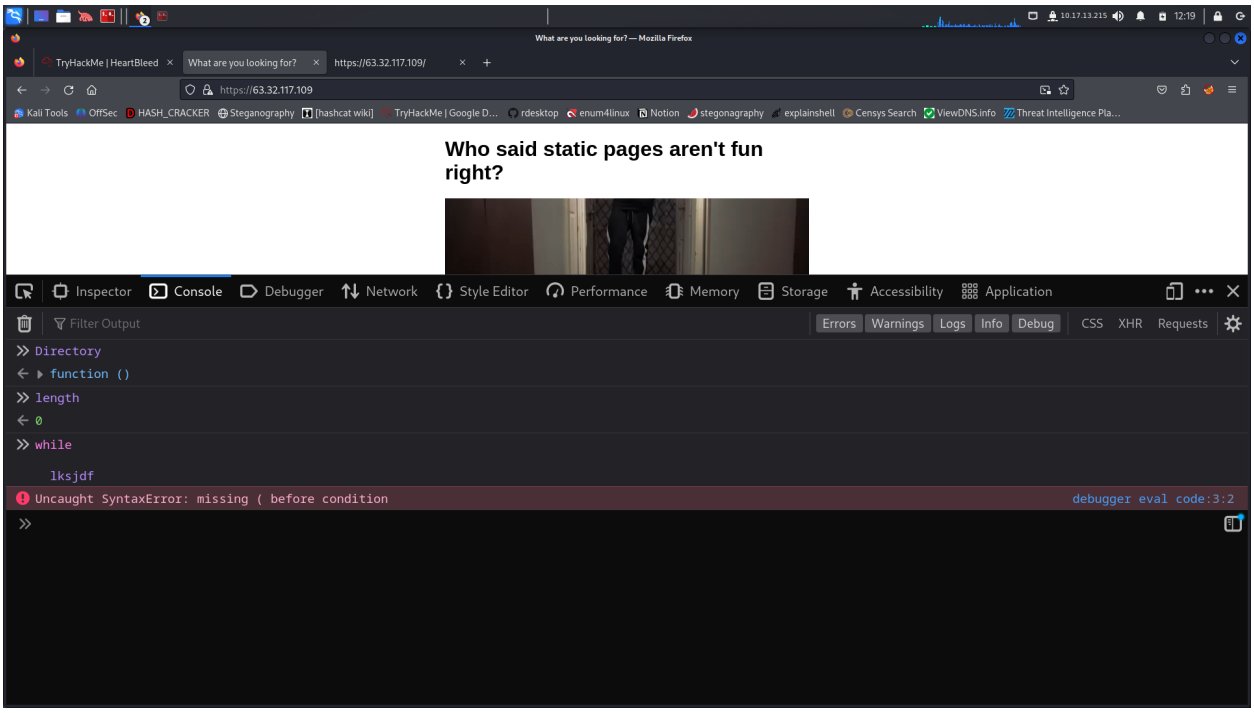
lets see the source page whats there



one thing we should focus on is, when ever we go to the source page we should not see any comments, but here it is there it may give some hints to go forward

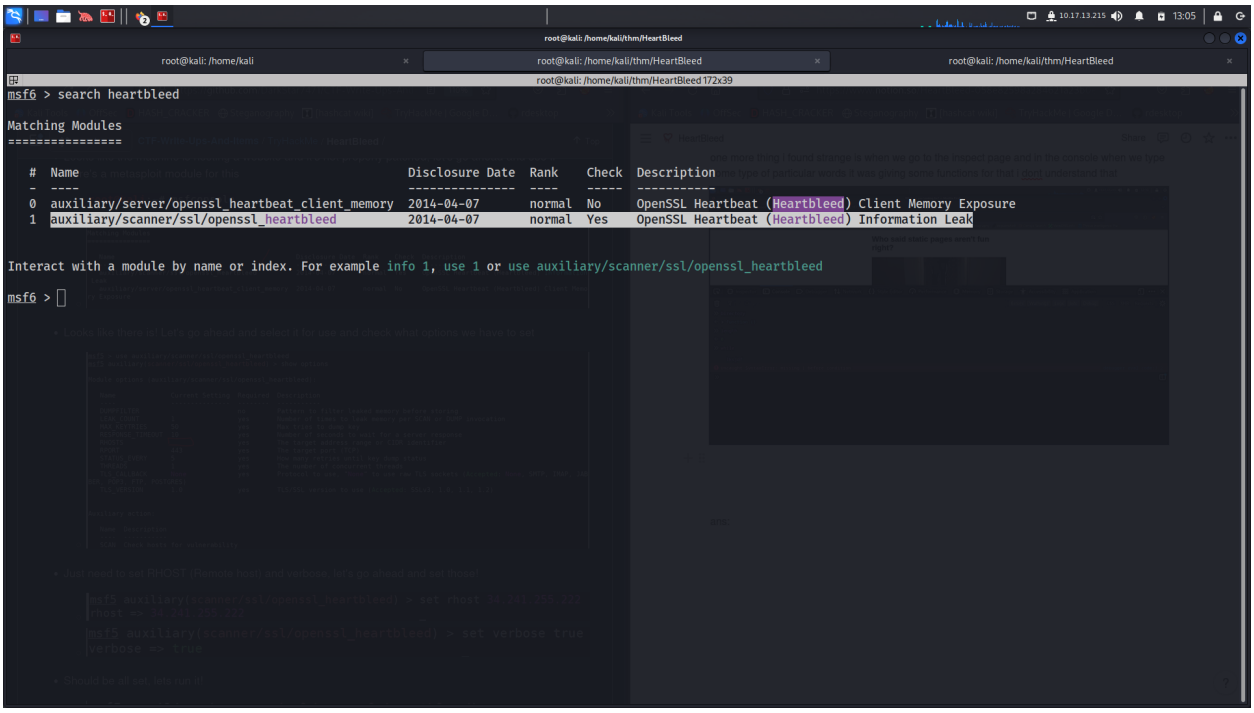
[what i feel is nothing is much important expect the comment in the source page]

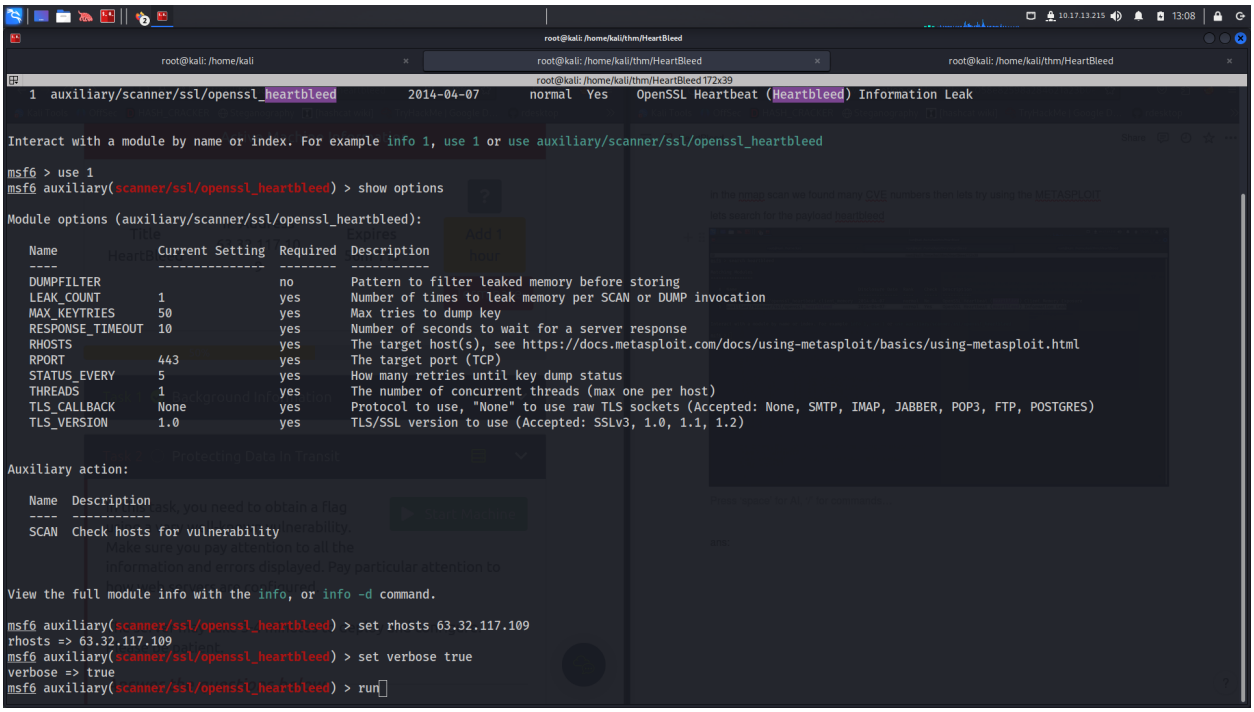
one more thing i found strange is when we go to the inspect page and in the console when we type some type of particular words it was giving some functions for that i dont understand that



in the nmap scan we found many CVE numbers then lets try using the METASPLOIT

lets search for the payload heartbleed





lets run the exploit

it should work but its not working in my case [like flag was not getting]

ans: **THM{sSl-Is-BaD}**