**Experiment No. 13**

# Title: Metasploit Part II - Exploit Heartbleed attack using Beebox

**Roll No.: 16010420075 Experiments No.: 13**

# Aim: To exploit Heartbeat vulnerability using BeeBox.

\

**Resources:** virtual box

**Theory**

**Metasploitable** is a Linux virtual machine that is designed to be vulnerable. This virtual machine can be used for security teaching, tool testing, and typical penetration testing approaches.

A buggy web application, or **bWAPP**, is a free and open-source online application that is purposefully insecure. It assists web security enthusiasts, developers, and students in identifying and preventing web vulnerabilities. The bWAPP training program equips students to execute successful penetration testing and ethical hacking projects.

What distinguishes bWAPP from other apps? It has over 100 web vulnerabilities, to be exact! It covers all significant known web flaws, as well as all OWASP Top 10 project hazards.

bWAPP is a MySQL database-driven PHP application. It runs on Linux/Windows and includes Apache/IIS and MySQL. WAMP or XAMPP can also be used to set it up.

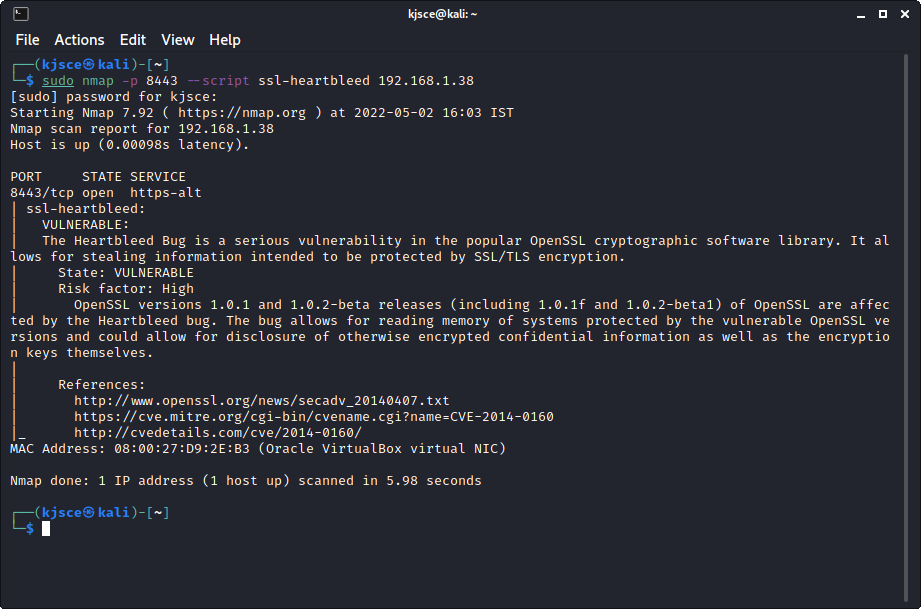
**Heartbleed** is a critical flaw in the widely used OpenSSL cryptographic software library. This flaw allows information to be stolen that is normally secured by the SSL/TLS encryption used to secure the Internet. Web, email, instant messaging, and some VPNs all use SSL/TLS to ensure communication security and privacy over the Internet.

Anyone on the Internet can read the memory of computers protected by vulnerable versions of the OpenSSL software thanks to the Heartbleed issue. The private keys required to identify service providers and encrypt communications, as well as the identities and passwords of users and the actual information, are all at risk. As a result, attackers can listen in on conversations, steal data straight from services and users, and impersonate those services and users.

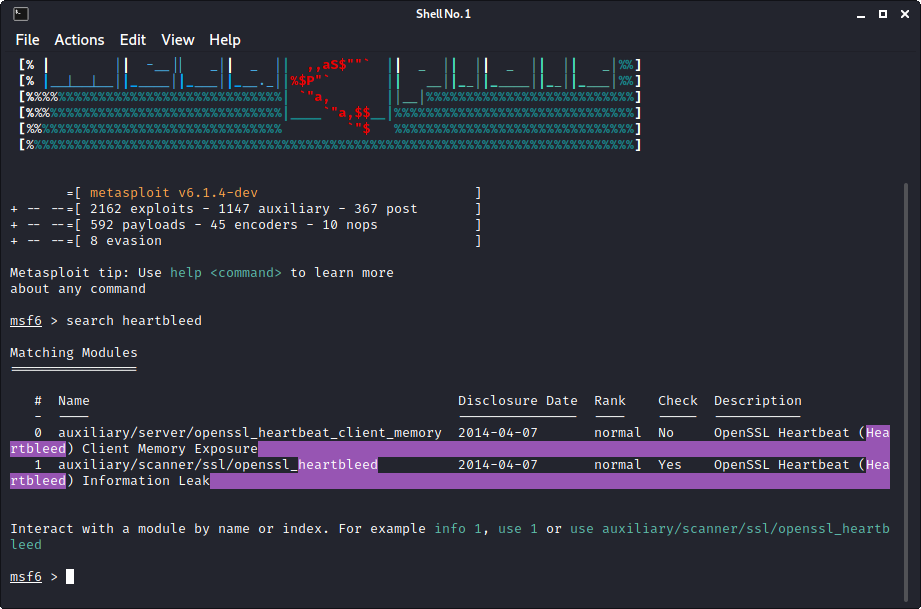
**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**IMPLEMENTATION AND RESULTS:**

Firstly, we open a BeeBox in a machine and login using credentials ‘bee’ as username and ‘bug’ as password (works in most cases). To check the host we enter the following command $ sudo nmap -p 8443 –script ssl-heartbleed 192.168.1.38

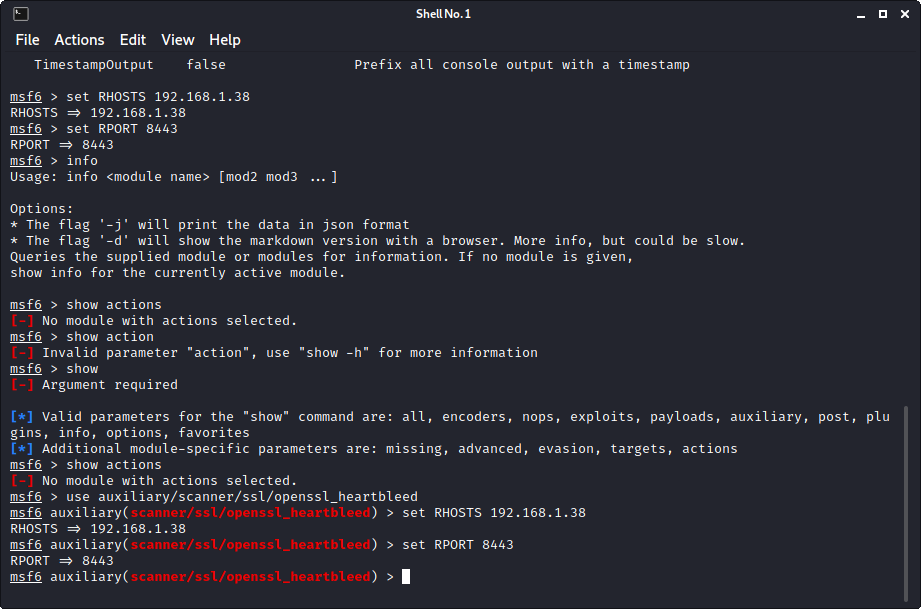


Next, we use Metasploit framework to search for the vulnerability.



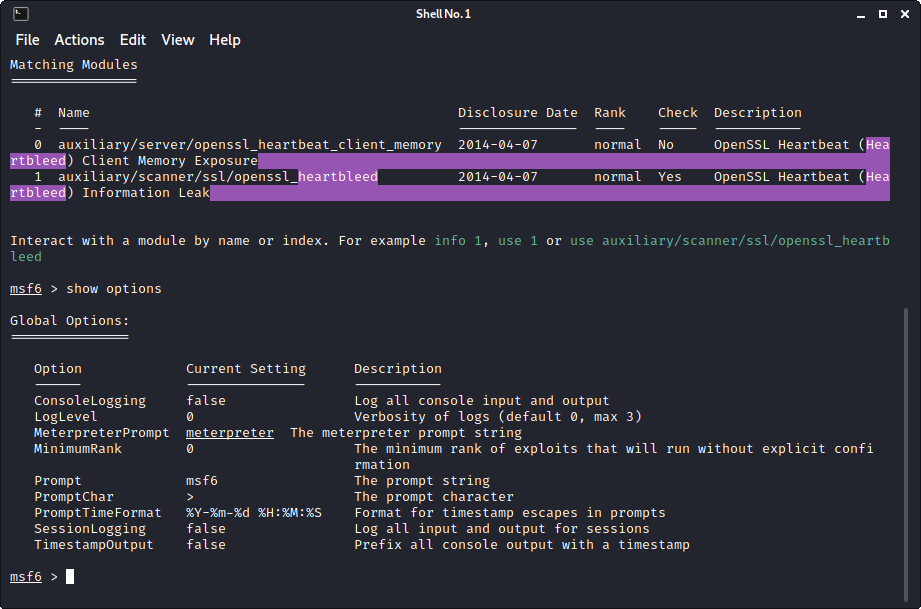
We choose the #1 vulnerability as our option using use command as

$ use <enter name>



The options can be checked to exploit the vulnerability using

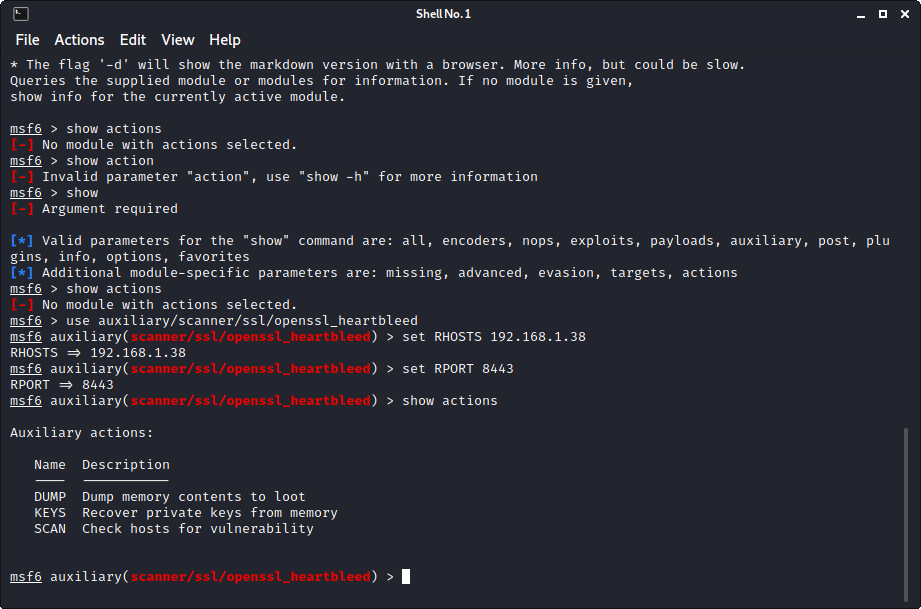
$ show options



Setting the RHOSTS (for attack victim) and RPORT (to exploit Heartbleed) using

$ set RHOSTS <victim IP>

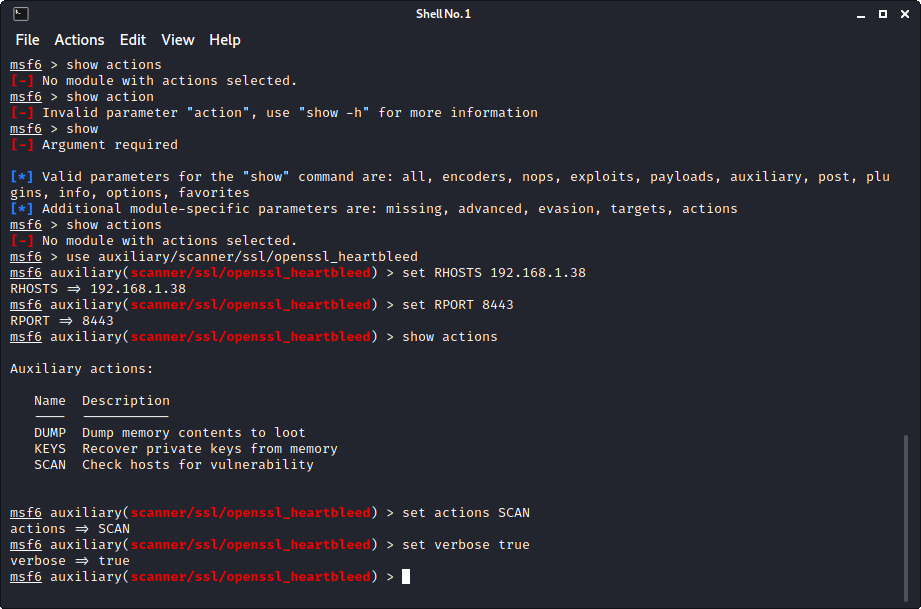
$ set RPORT 8443



We set the actions to scan and set our verbose to true as

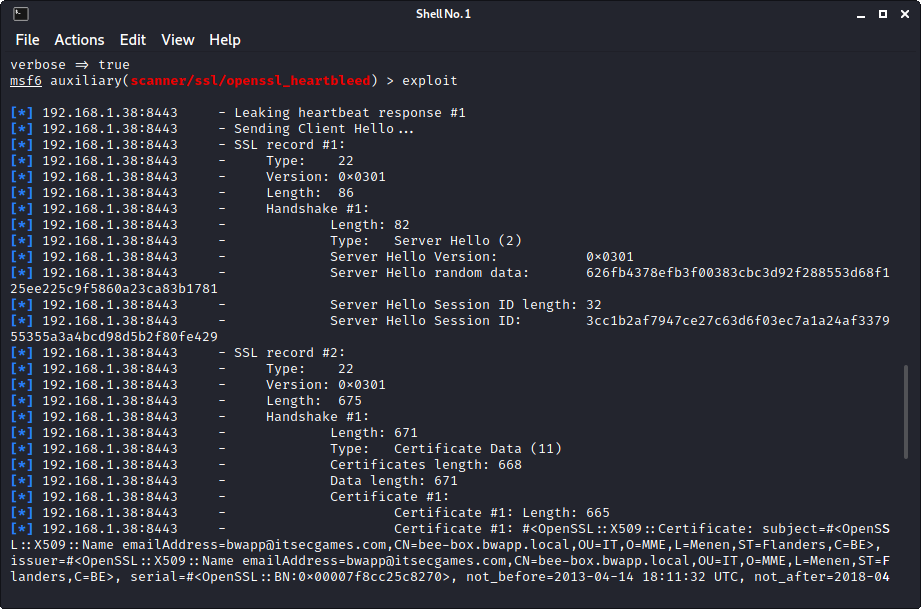
$ set actions SCAN

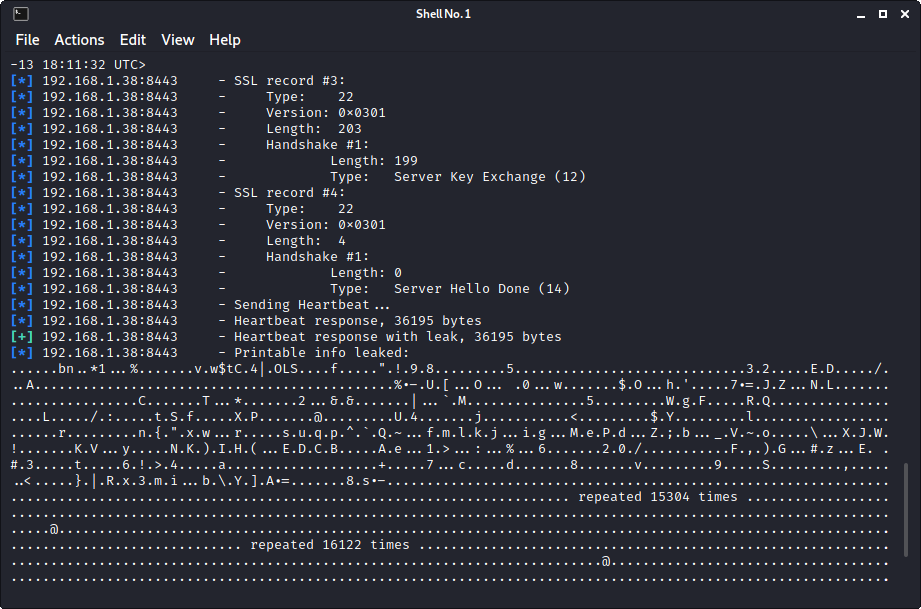
$ set verbose true

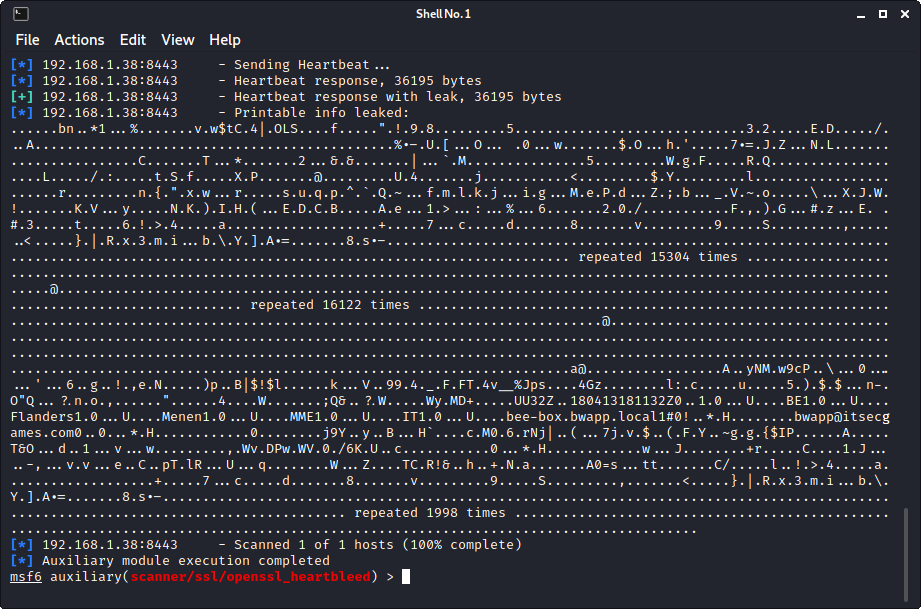


Finally, we exploit.

$ exploit







Looking at the output above, we can finally say that the exploit is successful.

**Outcomes:**

**CO-3:** Comprehend exploitation phase of penetration testing

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Conclusion: (Conclusion to be based on the objectives and outcomes achieved)**

Heartbleed vulnerability was exploited using BeeBox.

**Grade: AA / AB / BB / BC / CC / CD /DD**

**Signature of faculty in-charge with date**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**REFERENCES:**

* [www.kali.org](http://www.kali.org)