**Valentine walkthrough**

# **Index**

[Index 1](#_Toc181999119)

[List of pictures 1](#_Toc181999120)

[Disclaimer 2](#_Toc181999121)

[Reconnaissance 2](#_Toc181999122)

[Initial foothold 2](#_Toc181999123)

[User flag 3](#_Toc181999124)

[Privilege escalation 4](#_Toc181999125)

[Personal comments 4](#_Toc181999126)

[Appendix A – CVE-2014-0160 (HeartBleed) 5](#_Toc181999127)

[References 5](#_Toc181999128)

# **List of pictures**

[Figure 1 - nMap scan results 2](#_Toc181999111)

[Figure 2 - Vulnerabilities checked by nMap vuln script 2](#_Toc181999112)

[Figure 3 - HeartBleed exploit 3](#_Toc181999113)

[Figure 4 - Base64 from the HeartBleed exploit results 3](#_Toc181999114)

[Figure 5 - Hidden content found running ffuf tool 3](#_Toc181999115)

[Figure 6 - User shell and flag 4](#_Toc181999116)

[Figure 7 - tmux session information and privilege escalation 4](#_Toc181999117)

[Figure 8 - Root flag 4](#_Toc181999118)

# **Disclaimer**

I do this box to learn things and challenge myself. I’m not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who are willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Just to say: I am not an English native person, so sorry if I did some grammatical and syntax mistakes.

# **Reconnaissance**

The results of an initial nMap scan are the following:

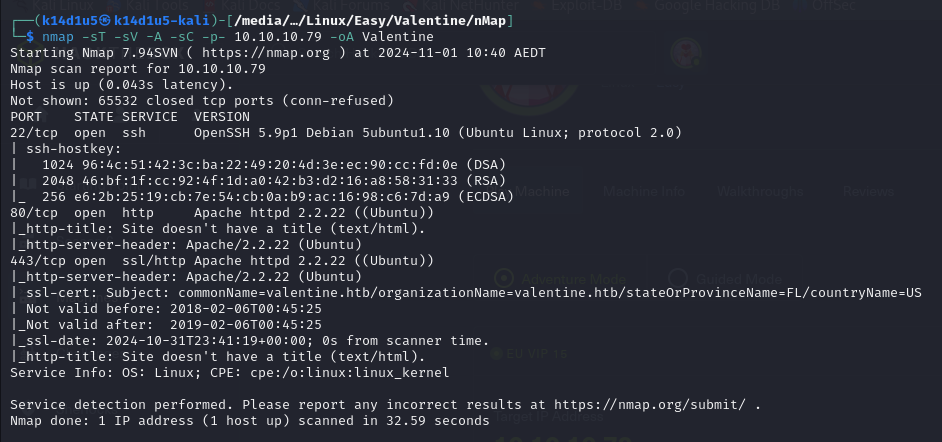


Figure 1 - nMap scan results

Open ports are 22, 80 and 443. So SSH service is enabled (port 22) and the box has a web application running on port 80 and 443. Also, nMap provide Linux as Operative System, but it didn’t provide further information about it.

# **Initial foothold**

In my opinion, one very important thing to do is run again nMap on the only ports found to check if the box is susceptible to some known vulnerabilities. In this case, I found out that the box is vulnerable to HeartBleed and POODLE, as shown in the following figure:

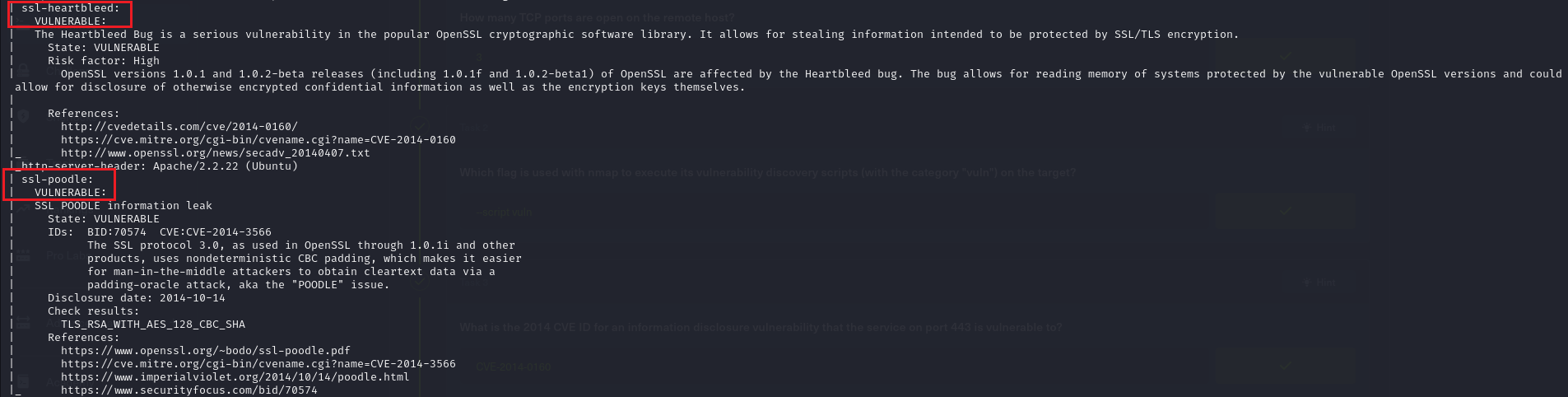


Figure 2 - Vulnerabilities checked by nMap vuln script

# **User flag**

Since I found out that the box is vulnerable to HeartBleed, I looked for an exploit on the Internet. I run it as shown in the following:

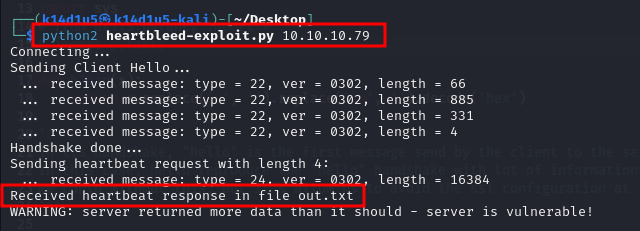


Figure 3 - HeartBleed exploit

Due to the HeartBleed vulnerability nature, it could be needed to run this exploit more than one time to retrieve some interesting information. All I found in this way was the following base64 value:

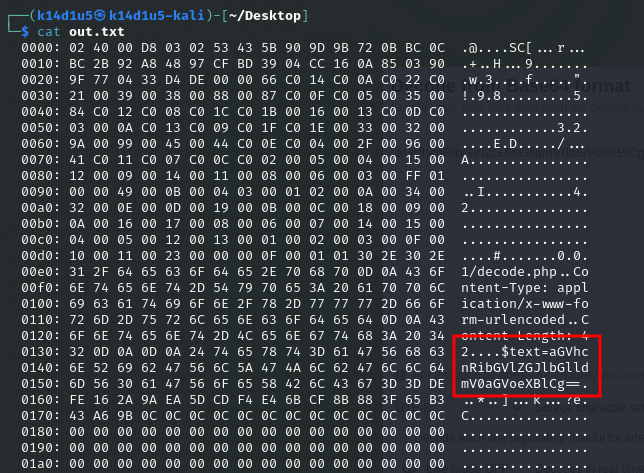


Figure 4 - Base64 from the HeartBleed exploit results

Of course, I decoded it and stored to have it ready if I need it (I don’t insert what it means because of it is a very simple task and this value will be useful after). At this point I need some other information. So, I searched other resources on the web site:

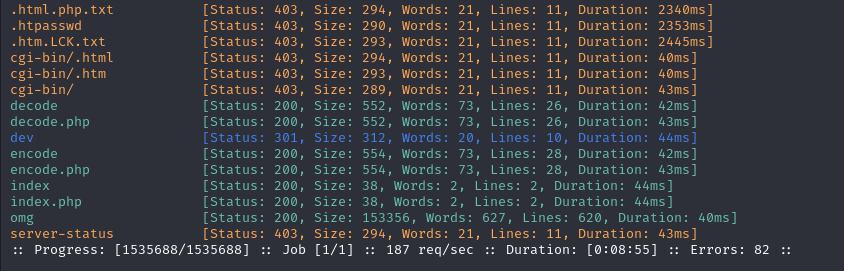


Figure 5 - Hidden content found running ffuf tool

In particular, I found a base64 encoder and decoder and a very interesting directory. In this directory, I found a note and an RSA key (sorry, I forgot to take the screenshot). I download the RSA key, which original name was (I named it ). Based on the information I had now, I can suppose that the box had a user and I can try to connect via SSH as this user. To do so, I need to provide a passphrase to use the RSA key. Luckily, I found something before, and I tried to use the base64 decoded value found previously. I was successful to login via SSH in this way and I retrieved the user flag, as shown in the following:

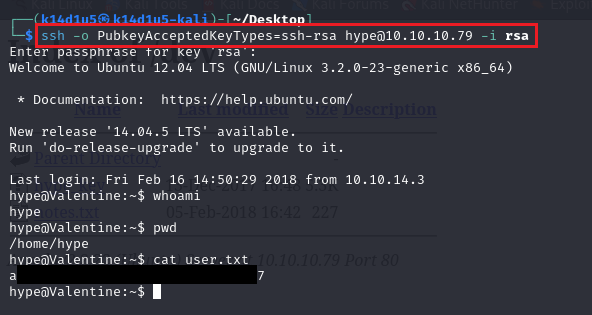


Figure 6 - User shell and flag

# **Privilege escalation**

At this point I needed to find a way to escalate my privileges. All basic methods didn’t work, so I uploaded on the target machine Linpeas tool and I run it. In this way I found out an interesting process named . I looked for some exploit against it on the Internet and I checked if it was useful:

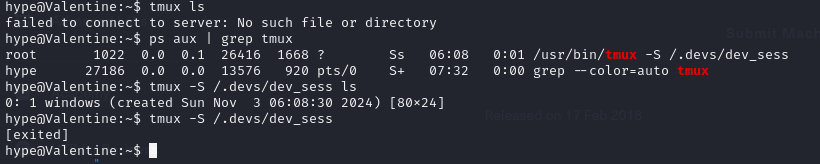


Figure 7 - tmux session information and privilege escalation

Since process handled a session, I tried to connect to it running the last command in the previous screenshot and I obtained a root shell. From there, I retrieved the root flag:

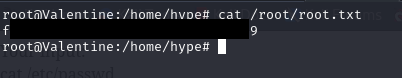


Figure 8 - Root flag

# **Personal comments**

For the first time in my life, I exploited the HeartBleed vulnerability. I never thought I achieve this goal! Anyway, I liked this box very much and I learnt a new possible flag to connect via SSH. I rated this box as easy on the Hack The Box platform.

# **Appendix A – CVE-2014-0160 (HeartBleed)**

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

It could leak X.509 certificates, user names and passwords, instant messages, emails and business critical documents and communication.

As long as the vulnerable version of OpenSSL is in use it can be abused. Fixed OpenSSL has been released and now it has to be deployed. Operating system vendors and distribution, appliance vendors, independent software vendors have to adopt the fix and notify their users. Service providers and users have to install the fix as it becomes available for the operating systems, networked appliances and software they use.

# **References**

<https://heartbleed.com/> -> HeartBleed Bug

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-shell-sessions> -> Hacktricks privilege escalation leveraging

<https://confluence.atlassian.com/bitbucketserverkb/ssh-rsa-key-rejected-with-message-no-mutual-signature-algorithm-1026057701.html> -> SSH connection issue