**Love walkthrough**

# **Index**

[Index 1](#_Toc184491961)

[List of pictures 1](#_Toc184491962)

[Disclaimer 2](#_Toc184491963)

[Reconnaissance 2](#_Toc184491964)

[Initial foothold 3](#_Toc184491965)

[User flag 4](#_Toc184491966)

[Privilege escalation 4](#_Toc184491967)

[Personal comments 5](#_Toc184491968)

[References 5](#_Toc184491969)

# **List of pictures**

[Figure 1 - nMap scan results (part 1) 2](#_Toc184491951)

[Figure 2 - nMap scan results (part 2) 2](#_Toc184491952)

[Figure 3 - Subdomain and possible username found 3](#_Toc184491953)

[Figure 4 - Credentials found 4](#_Toc184491954)

[Figure 5 - Exploit and user flag 4](#_Toc184491955)

[Figure 6 - Info for privilege escalation (using WinPeas) 4](#_Toc184491956)

[Figure 7 - Info for privilege escalation manually found 5](#_Toc184491957)

[Figure 8 - Privilege escalation and root flag 5](#_Toc184491958)

# **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:

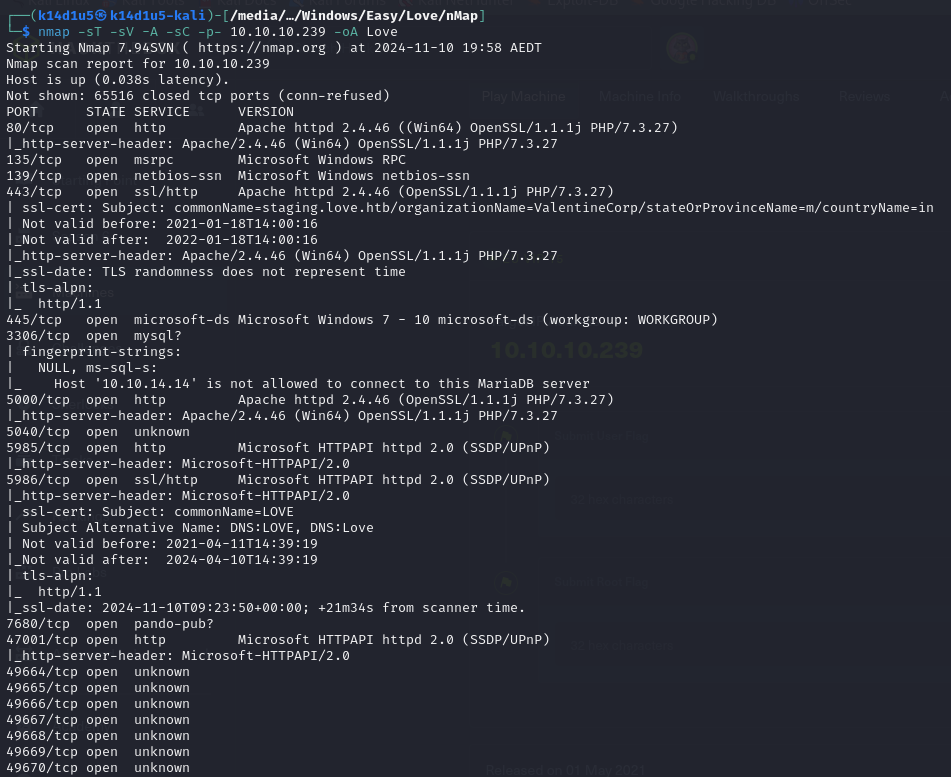


Figure 1 - nMap scan results (part 1)

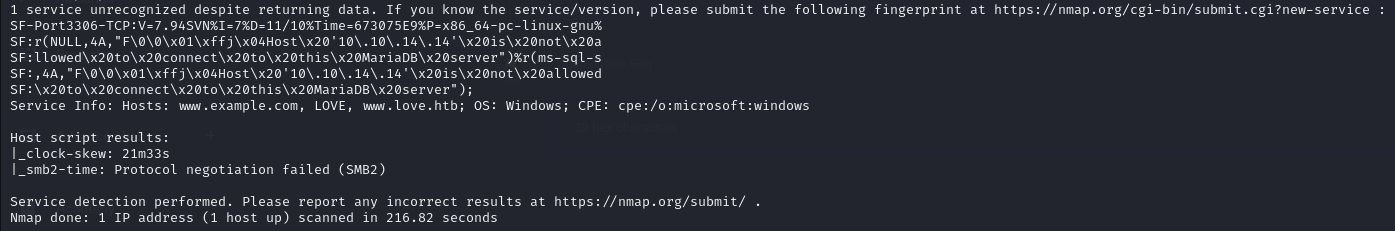


Figure 2 - nMap scan results (part 2)

Open ports are 80, 135, 139, 443, 445, 3306, 5000, 5040, 5985, 5986, 7680, 47001, 49664, 49665, 49666, 49667, 49668, 49669 and 49670. So, this box has a web application running on ports 80, 443, 5000, 5985, 5986 and 47001, MSRPC (port 135) service enabled, NetBIOS (port 139) service enabled, MySQL (port 3306) service enabled, Panda-pub (7680) service enabled and unknown services on ports 5040, 49664, 49665, 49666, 49667, 49668, 49669 and 49670. Also, this box seems to be a Windows target.

# **Initial foothold**

Since I had a Windows target, I tried to run the script and I found an interesting named pipe I can leverage to exploit the box. However, it requires some valid credentials, so I can’t do it now. I tried to use the script, but I have the same “issue”. Also, I have a database exposed. So, I navigate the web application running on port 80 and tried to exploit an SQL injection vulnerability. This seems possible. I run SQLMap, and I accessed to the data contained. I found a hashed password and I tried to crack it, but it seems to be not possible. At this point, I browsed to the web application running on port 443 and I checked his certificate. There, I found a new subdomain and a possible username:

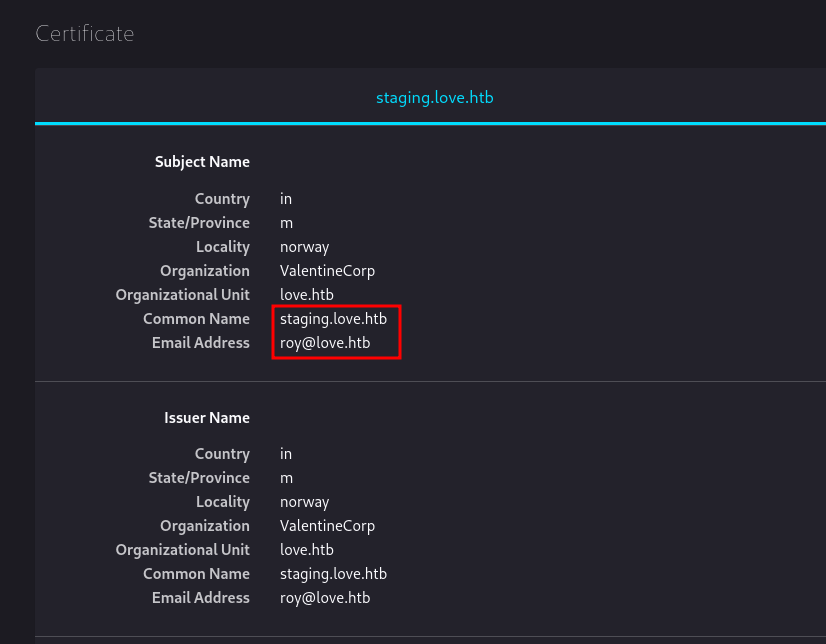


Figure 3 - Subdomain and possible username found

So, I added the subdomain in the file and I browsed to this URL. I found a site where I can upload a file. This application provides an analysis feature. I had to insert a file URL and it includes this file in the page. Since I have some other web server where I didn’t find anything, or I wasn’t able to access via browser, I tried to use those addresses. When I used <http://127.0.0.1:5000>, as URL to the web server running on port 5000, I found some credentials:

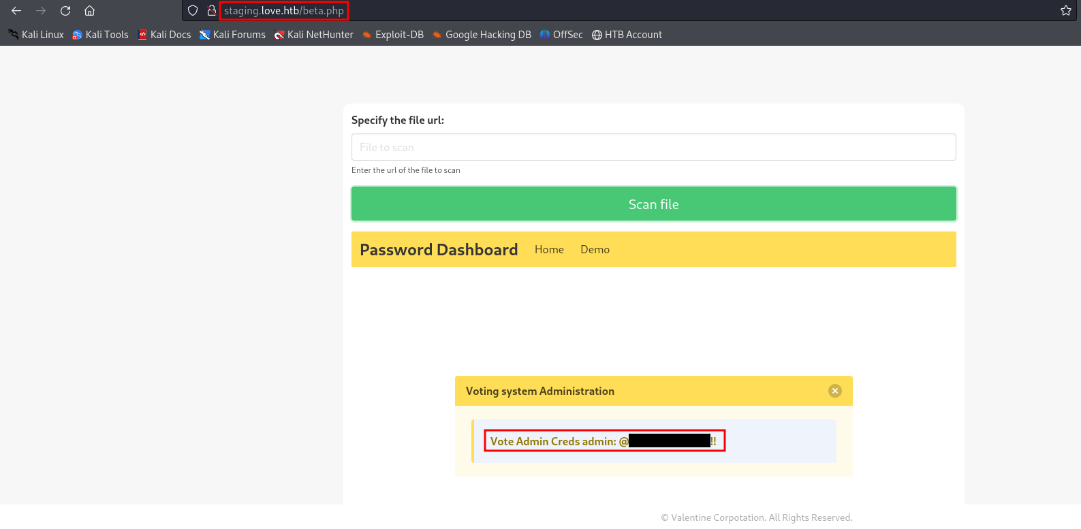


Figure 4 - Credentials found

# **User flag**

I tried to use these credentials and I obtained access to the voting portal running on port 80. At this point, I searched an exploit on the Internet against the and I run it:

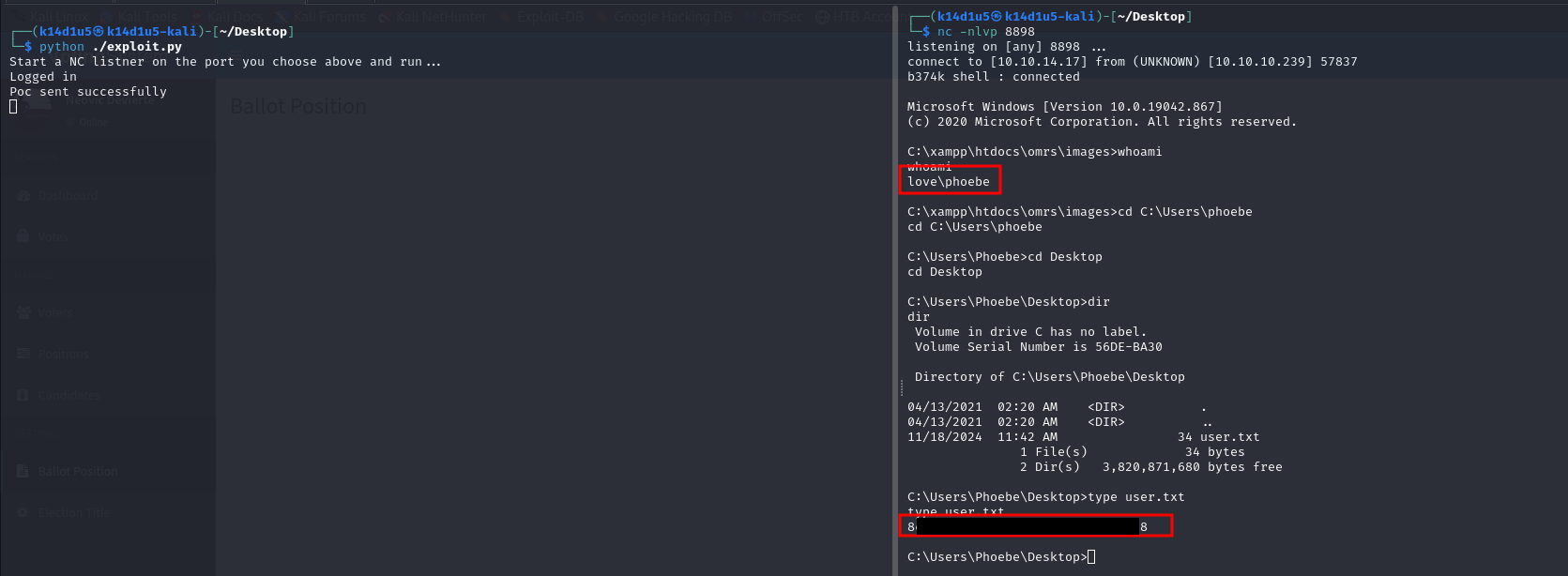


Figure 5 - Exploit and user flag

Of course, it was needed to insert credentials, IP target and listening IP and port inside the script code. In this way, I obtained a shell and the user flag.

# **Privilege escalation**

At this point I needed to escalate my privileges. I run WinPeas tool and I found two interesting permission set. I was able to manually find the same information too, so I inserted in this walkthrough both screenshots:

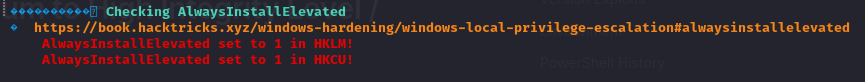


Figure 6 - Info for privilege escalation (using WinPeas)

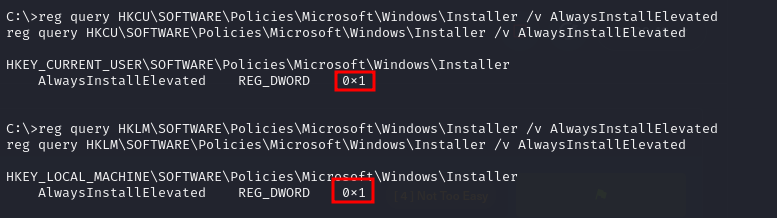


Figure 7 - Info for privilege escalation manually found

Since these permissions let me to install programs as , I simply created a payload with MSFVenom running the command: . I uploaded it on the target and executed it running the command: . In this way I obtained a shell as and I retrieved the root flag:

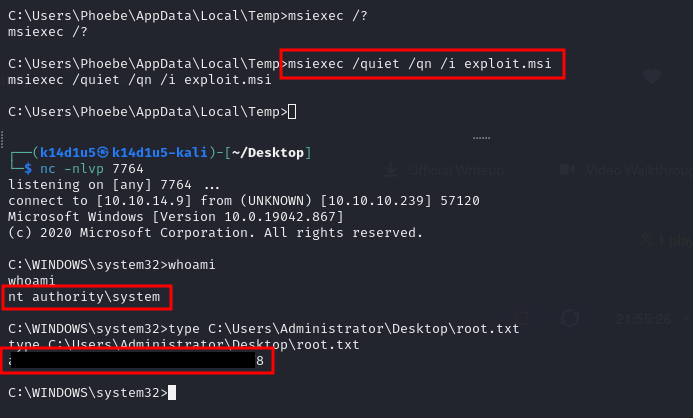


Figure 8 - Privilege escalation and root flag

# **Personal comments**

I really enjoyed this box because has some interesting points. It was very interesting to find a subdomain and a possible username (but it was useless) in the SSL certificate. I could find the subdomain reading better the nMap scan results too. So, I learnt a different place where to search useful information. Also, it was very interesting the way to escalate privileges. It was the first time I found this path and it is in my know-how now. So, as I said, I enjoyed this box which teach me something new. I rated it as Easy on Hack The Box platform.

# **References**

<https://book.hacktricks.xyz/network-services-pentesting/135-pentesting-msrpc>

<https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#basic-uac-bypass-full-file-system-access>