**Sense walkthrough**

# **Index**

[Index 1](#_Toc184482663)

[List of pictures 1](#_Toc184482664)

[Disclaimer 2](#_Toc184482665)

[Reconnaissance 2](#_Toc184482666)

[Initial foothold 2](#_Toc184482667)

[Privilege escalation 3](#_Toc184482668)

[Personal comments 3](#_Toc184482669)

[References 3](#_Toc184482670)

# **List of pictures**

[Figure 1 - nMap scan results 2](#_Toc184482645)

[Figure 2 - Interesting file found 2](#_Toc184482646)

[Figure 3 - Partial credentials found 3](#_Toc184482647)

[Figure 4 - Shell as root user 3](#_Toc184482648)

# **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:

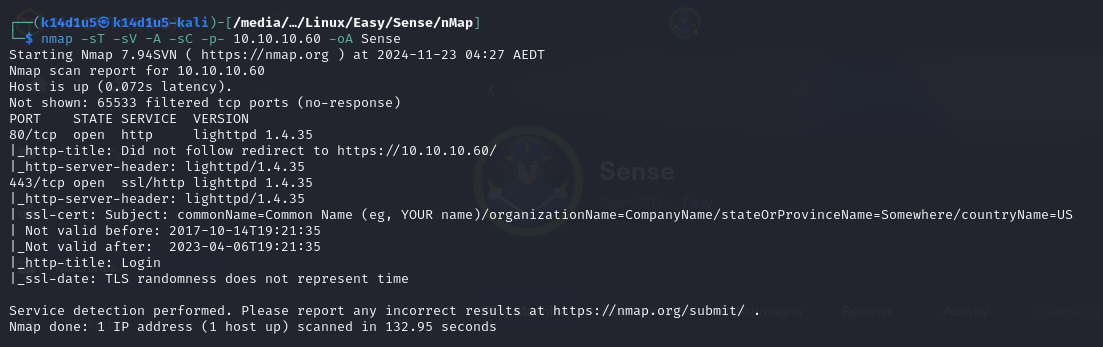


Figure 1 - nMap scan results

Open ports are just 80 and 443. So, we have just a web application running on port 443. When I tried to connect to port 80 via browser, I was redirected to the application on port 443. Also, I didn’t see any information about OS (or I cut them off from the screenshot).

# **Initial foothold**

Since I had just a web application, I tried to access to it via browser. In this way I found a PFSense application. Also, as usual I run a discovery content tool as ffuf. Its results are the following:

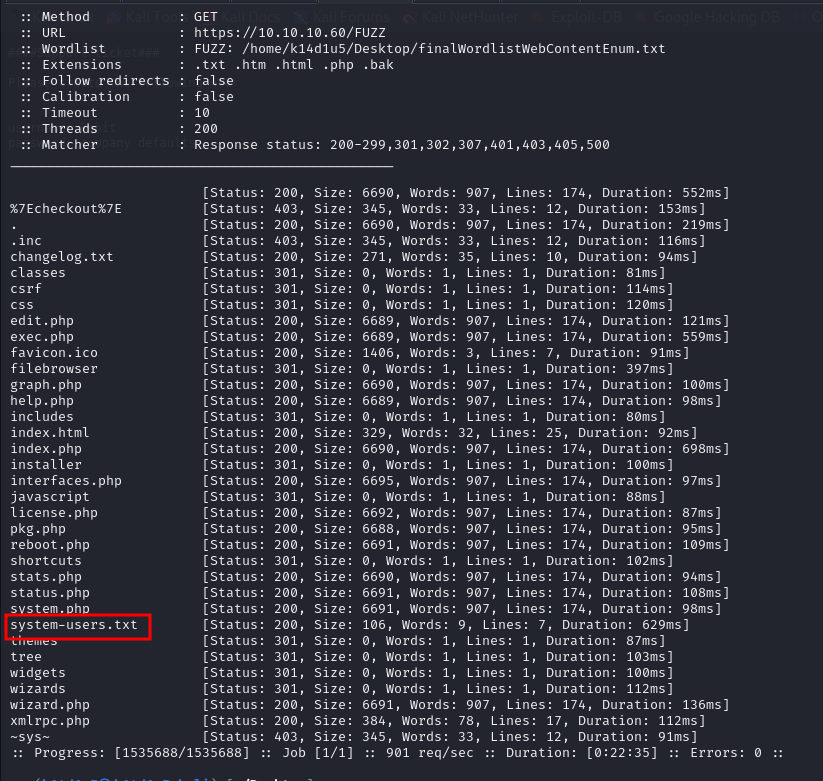


Figure 2 - Interesting file found

So, I found an interesting file named . I browsed to it and I found some partial credentials:

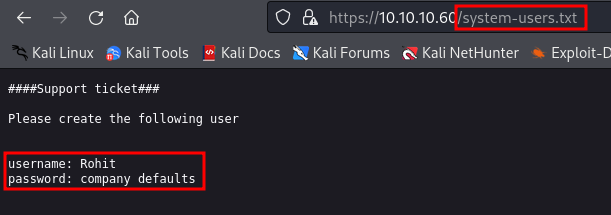


Figure 3 - Partial credentials found

# **Privilege escalation**

I worked a bit on these credentials and I found a valid one to log in in the web application. Also, I found an interesting exploit on the Internet. This exploit is relative to the CVE-2014-4688. I run this authenticated exploit and I obtained a shell as root:

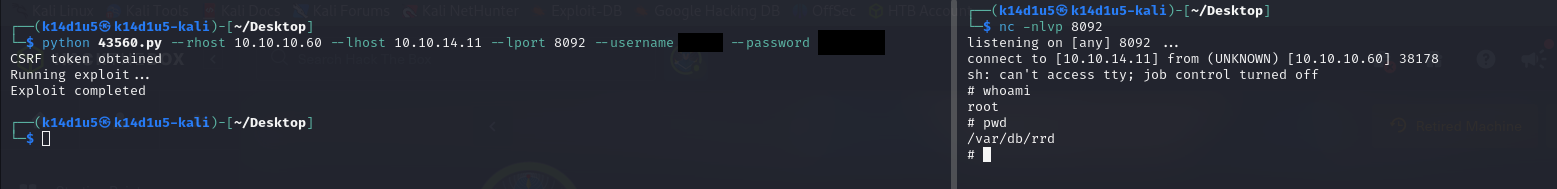


Figure 4 - Shell as root user

At this point, I retrieved both user and root flags (I forgot the screenshot about the flags, sorry).

# **Personal comments**

This box was very easy, in my opinion. You just need to do the very basic tasks and a simple search on the Internet. I was a little bit disappointed about this box because it was too easy.

**CVE-2014-4688**

This critical vulnerability concerns an unknown sequence of the file. An extended rights vulnerability can be exploited by manipulating the file with an unknown input. This vulnerability leads an authenticated users to execute arbitrary commands via:

1. the value to in a action;
2. the value to ;
3. or the database value to .

It is considered easy to exploit. The attack can be launched via the network. In order to enforce exploitation, simple authentication must be implemented. Technical details and a public exploit for the vulnerability are known.

# **References**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4688>