**SwagShop walkthrough**

# **Index**

[Index 1](#_Toc179560436)

[List of pictures 1](#_Toc179560437)

[Disclaimer 2](#_Toc179560438)

[Reconnaissance 2](#_Toc179560439)

[Initial foothold 2](#_Toc179560440)

[User flag 3](#_Toc179560441)

[Privilege escalation 4](#_Toc179560442)

[Personal comments 5](#_Toc179560443)

# **List of pictures**

[Figure 1 - nMap scan results 2](#_Toc179560428)

[Figure 2 - ffuf scan results 2](#_Toc179560429)

[Figure 3 - Target vulnerable check 3](#_Toc179560430)

[Figure 4 – Login to the admin dashboard 3](#_Toc179560431)

[Figure 5 - First shell obtained 3](#_Toc179560432)

[Figure 6 - Privilege escalation info 4](#_Toc179560433)

[Figure 7 - How to run vi tool to escalate privileges 4](#_Toc179560434)

[Figure 8 - Privilege escalation and root flag 4](#_Toc179560435)

# **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 as note: 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:

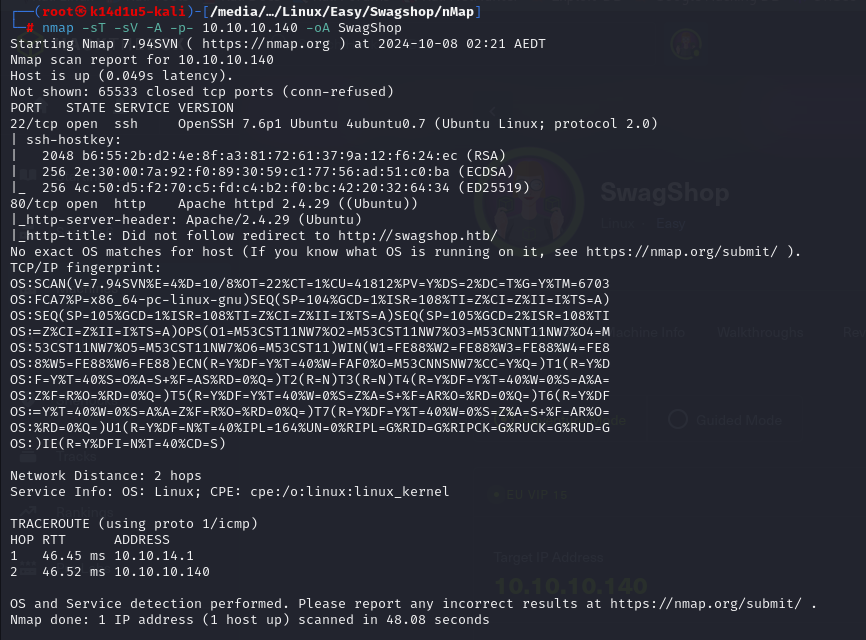


Figure 1 - nMap scan results

Open ports are 22 and 80. This means that the box has SSH service (on port 22) enabled and a web application running on port 80. Also, nMap informed me that OS is Linux, but it didn’t provide any further information.

# **Initial foothold**

Since I just found a web application running on port 80, I tried to access to it. To do it, I needed to add a new entry in my file. Also, I run tool and I found the following hidden contents:

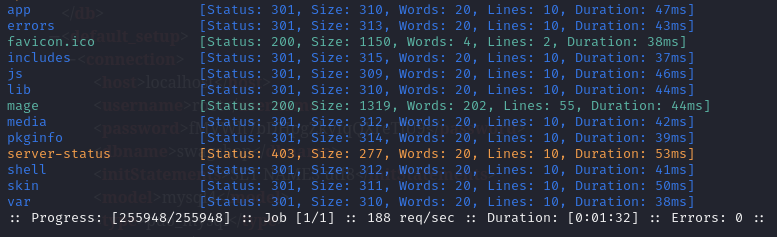


Figure 2 - ffuf scan results

However, I didn’t find any interesting information in this way. I noted that the web application is Magento, so I searched some possible exploit on the Internet. In particular, I found out that the target web application was released in 2014. Looking for some details on the Internet, I found out that the most recent version in 2014 was 1.8.

# **User flag**

At this point, I looked for and I found an interesting exploit. It requires the admin login page. I didn’t find it, so I looked for it on the Internet. Honestly, I don’t remember very well how I found the admin login page. Maybe I found it using the Burp’s Spider functionality. Or maybe when I navigate the paths I found when I run tool. Or maybe just because I noted that all paths of the web application started with <http://swagshop.htb/index.php> and I just tried to look the admin login there. Once I found the admin login, I was able to run the exploit, as shown in the following figure:

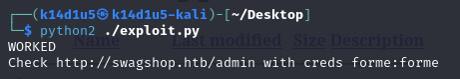


Figure 3 - Target vulnerable check

I verified that everything works properly trying to use the admin credentials:

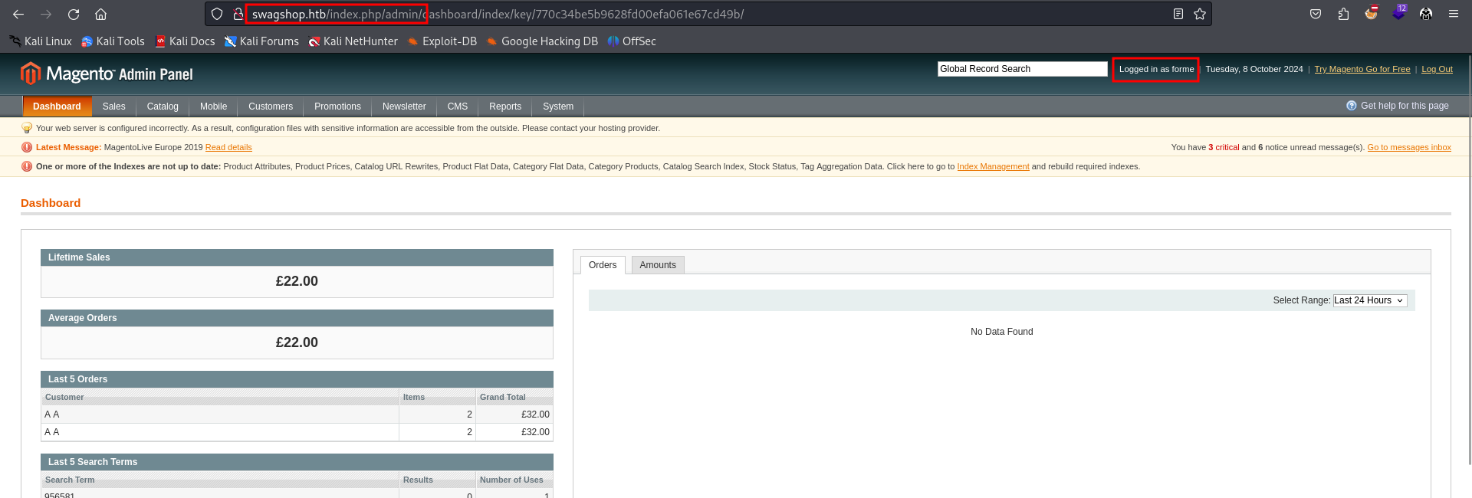


Figure 4 – Login to the admin dashboard

At this point, since I have an admin login, I can execute a different exploit that letting me to obtain RCE. I found it on the Internet too. Using this exploit, I can upload an file and open a new shell:

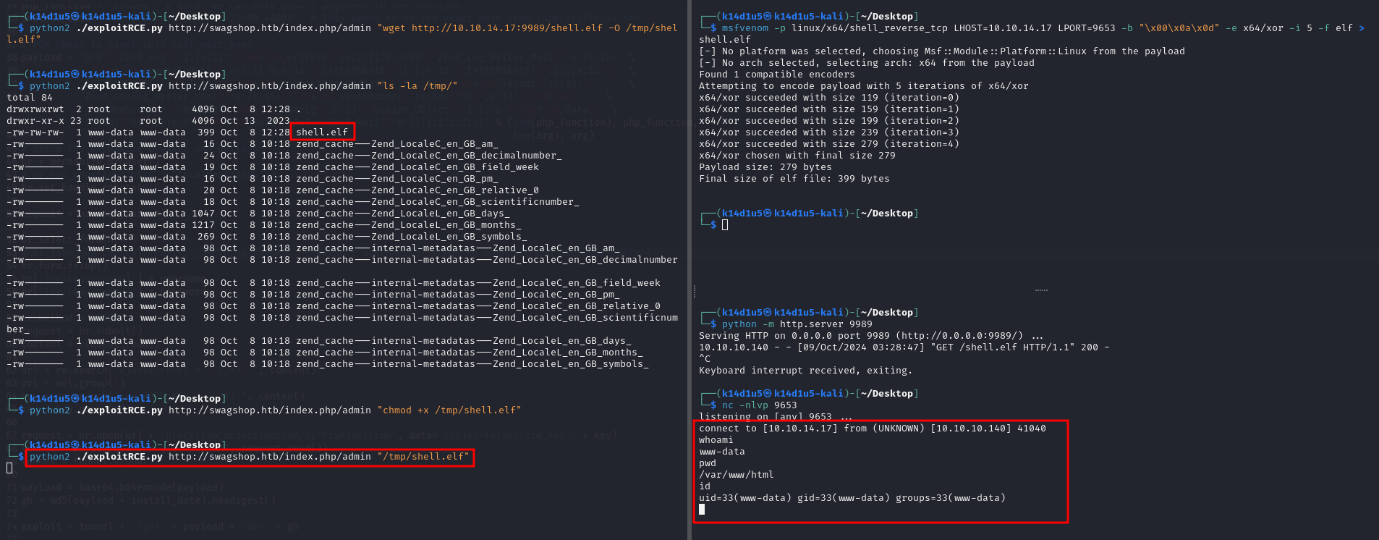


Figure 5 - First shell obtained

Even I am the user, I can read the user flag contained in the home directory of another user (I forgot the screenshot).

# **Privilege escalation**

At this point I need to find a way to escalate my privileges. As usual, one of my first try was checking the sudoers. This time I was lucky. In fact, the user can run tool to modify all file in the web application root directory, as shown in the following figure:

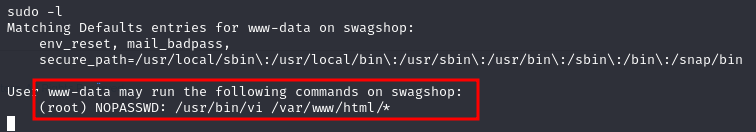


Figure 6 - Privilege escalation info

This means I can run a command in the “interface” and I can obtain a shell as root. To do it, I choose to modify the file:



Figure 7 - How to run vi tool to escalate privileges

At this point, I just need to run the command to spawn a shell as root and retrieve the root flag:

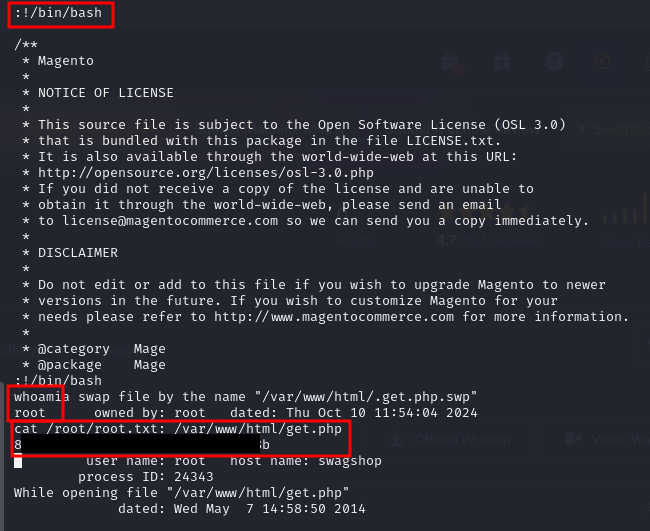


Figure 8 - Privilege escalation and root flag

# **Personal comments**

I was very surprised by this box because it was the first one where I can access to the user flag and escalate my privileges when I was a “service” user as . In my opinion, it was the biggest difficulty for this box. Due to this, I lost a certain amount of time to understand how I can perform a lateral movement, but it was not needed. Also, I consider this box to the easy level, as I rated it on the Hack The Box platform. Also, I am verry sorry because I was not very detailed on some point that I didn’t note and log properly on my personal notes. It can happen, but I always work hard so it will not in the future.