**Sunday walkthrough**

# **Index**

[Index 1](#_Toc181994817)

[List of pictures 1](#_Toc181994818)

[Disclaimer 2](#_Toc181994819)

[Reconnaissance 2](#_Toc181994820)

[Initial foothold 3](#_Toc181994821)

[User flag 3](#_Toc181994822)

[Privilege escalation 6](#_Toc181994823)

[Personal comments 7](#_Toc181994824)

# **List of pictures**

[Figure 1 - nMap scan results (part 1) 2](#_Toc181994807)

[Figure 2 - nMap scan results (part 2) 2](#_Toc181994808)

[Figure 3 - Finger user enumeration 3](#_Toc181994809)

[Figure 4 - Credentials found 4](#_Toc181994810)

[Figure 5 - SSH conncetion as sunny user 4](#_Toc181994811)

[Figure 6 - Shadow backup file found 5](#_Toc181994812)

[Figure 7 – Successful cracking 5](#_Toc181994813)

[Figure 8 - User flag 6](#_Toc181994814)

[Figure 9 - Useful information to escalate privileges 6](#_Toc181994815)

[Figure 10 - Privilege escalation and root flag 6](#_Toc181994816)

# **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:

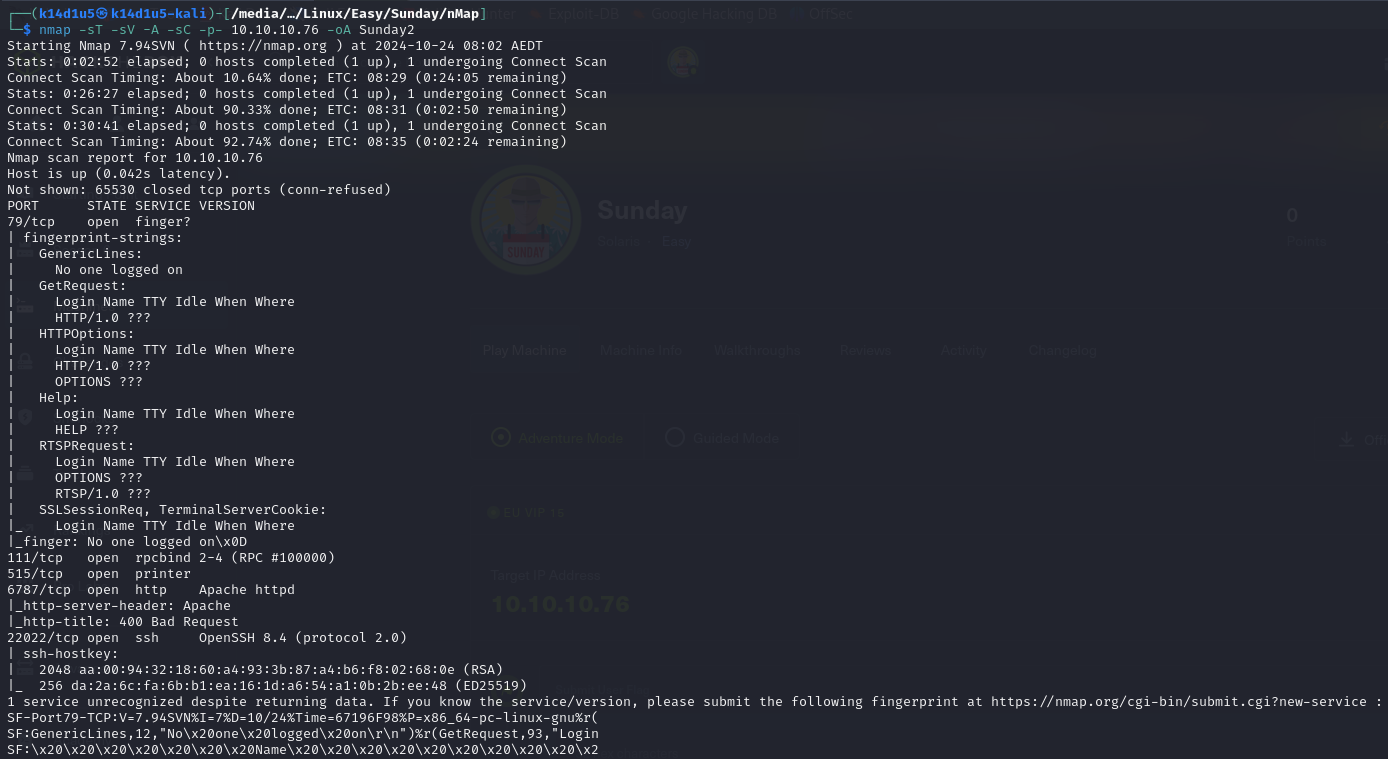


Figure 1 - nMap scan results (part 1)

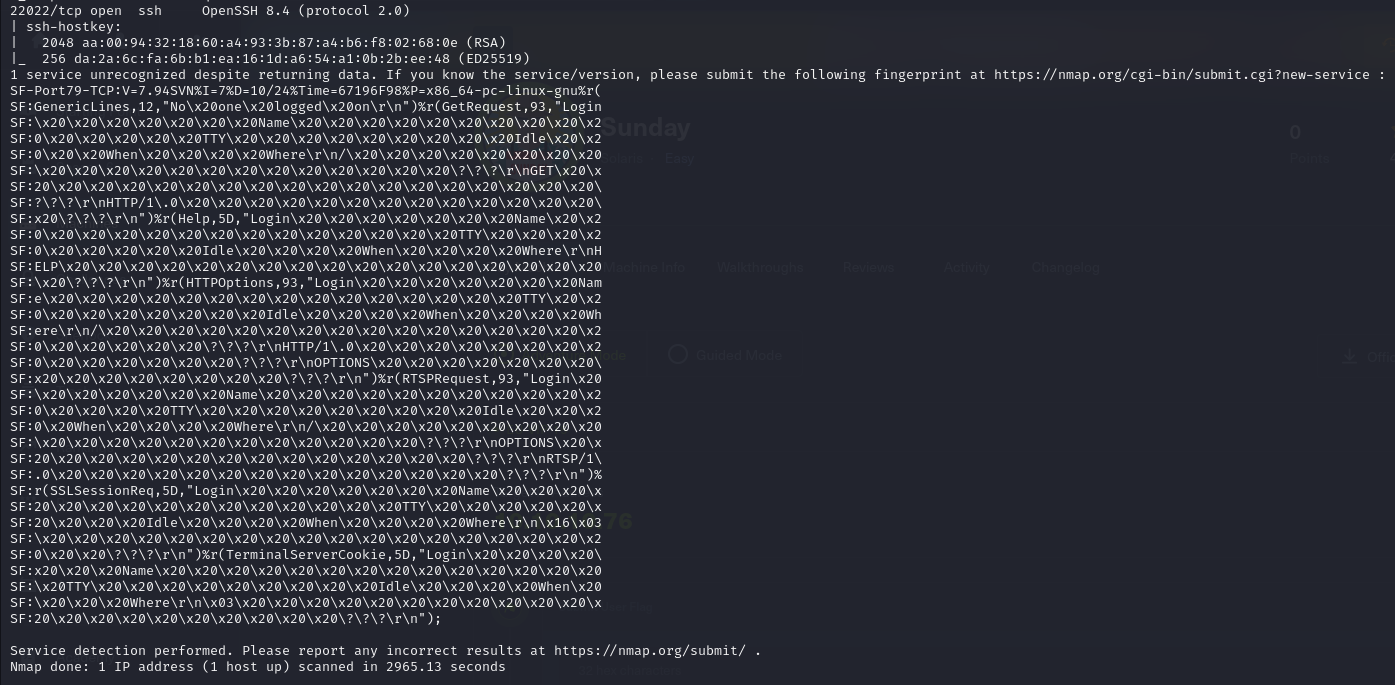


Figure 2 - nMap scan results (part 2)

Open ports are 79, 111, 515, 6787, 22022. It seems a Finger service is running on port 79. In addition, an RPCBind (111), Printer (515) and SSH (22022) services are enabled. Also, a web application is running on port 6787. I already noted that SSH service is running on a non-standard port. Finally, nMap provide Linux as operative system.

# **Initial foothold**

As I usually do, I started to find some clues browsing the web application. In this case I find a page which requires a username, so I thought that probably it is a login page. Since I didn’t find anything useful from the web application, I was curious about the Finger service. I found out from the Internet that this service is useful to find information about accounts on a machine. So, I found a script to enumerate users on the machine via Finger service. I downloaded a usernames list too. At this point, I run the script:

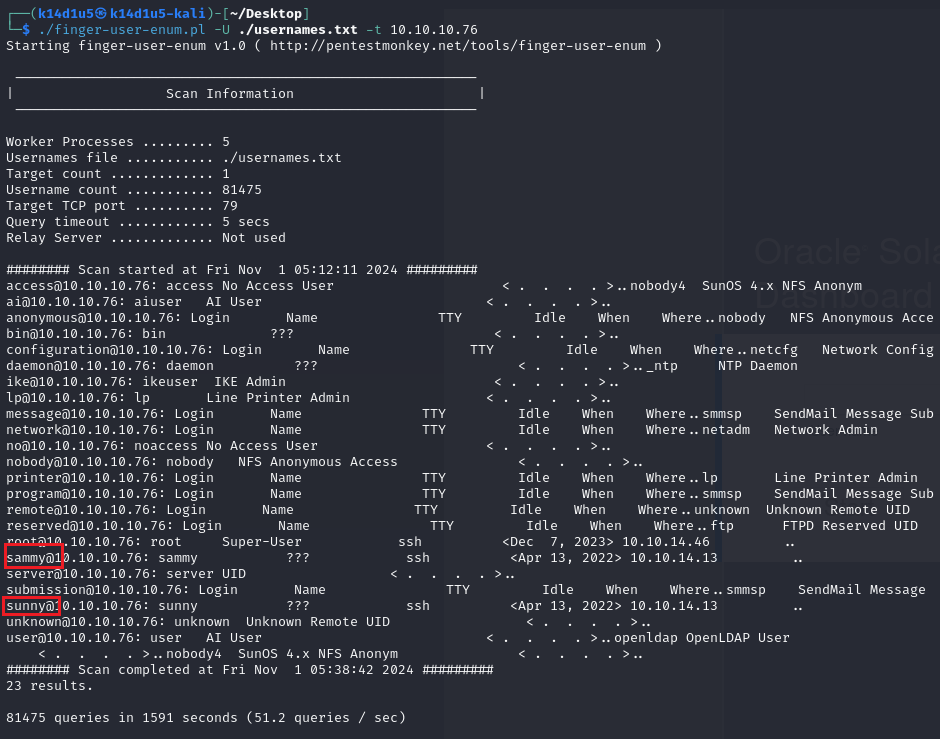


Figure 3 - Finger user enumeration

It was very interesting because I found two users: and .

# **User flag**

Well, I have some usernames and the SSH service enabled. So, I tried to run a brute force attack against the SSH service running hydra tool:

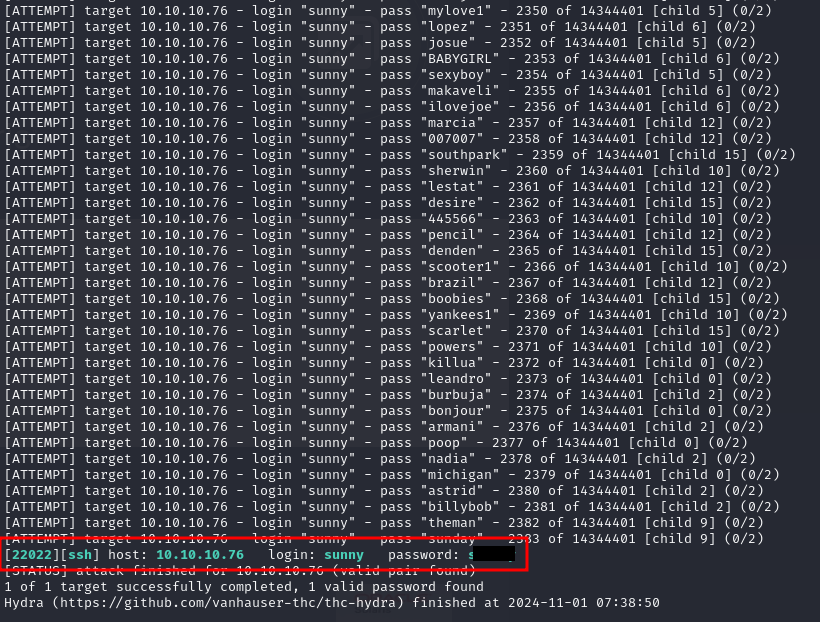


Figure 4 - Credentials found

I was lucky! I found the ’s password. In fact, when I tried to log in via SSH with this user, I had success:

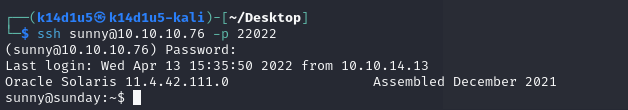


Figure 5 - SSH connection as sunny user

The first thing I did was to search the flag, but, unfortunately, this user didn’t have. What I saw as user was very minimal. I had very few resources which I can work on. So, I tried to check his history:

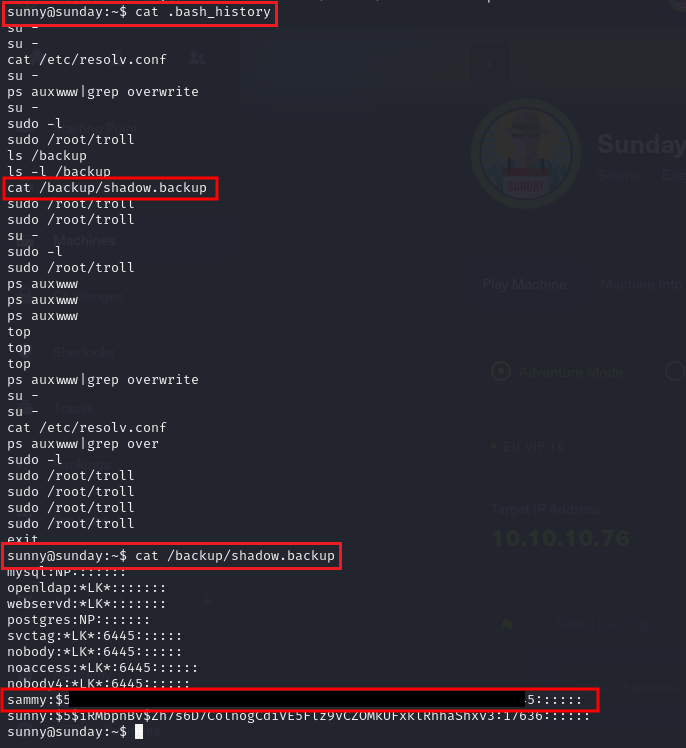


Figure 6 - Shadow backup file found

Luckily, this user read a shadow backup file and I found the ’s hash password. At this point, I just tried to crack this hash, as shown in the following picture:

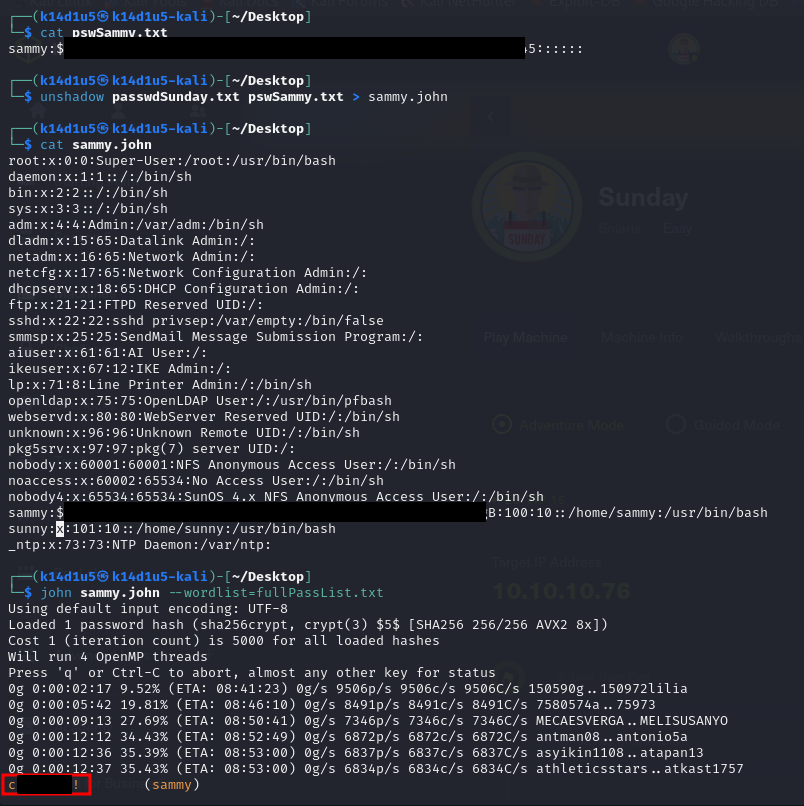


Figure 7 – Successful cracking

All I needed to do was connecting via SSH as and retrieve the user flag:

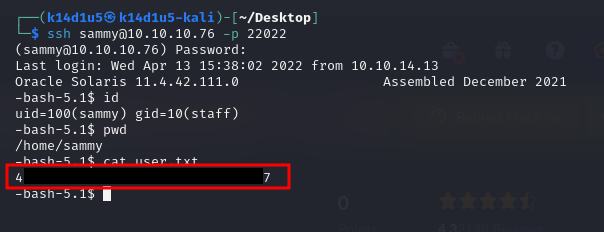


Figure 8 - User flag

# **Privilege escalation**

The first check I always do when I have to escalate my privileges on a Linux machine is checking the sudoers. I was lucky, because this user was able to run as root without providing the password the tool:

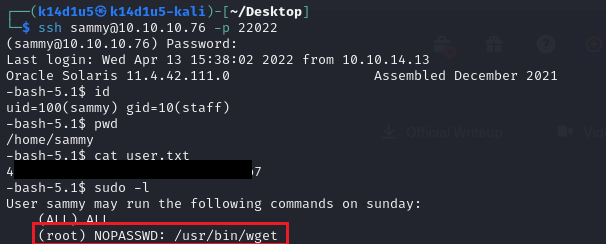


Figure 9 - Useful information to escalate privileges

So, I checked if an exploit exists on GTFObins web site, I run it and I retrieved the root flag:

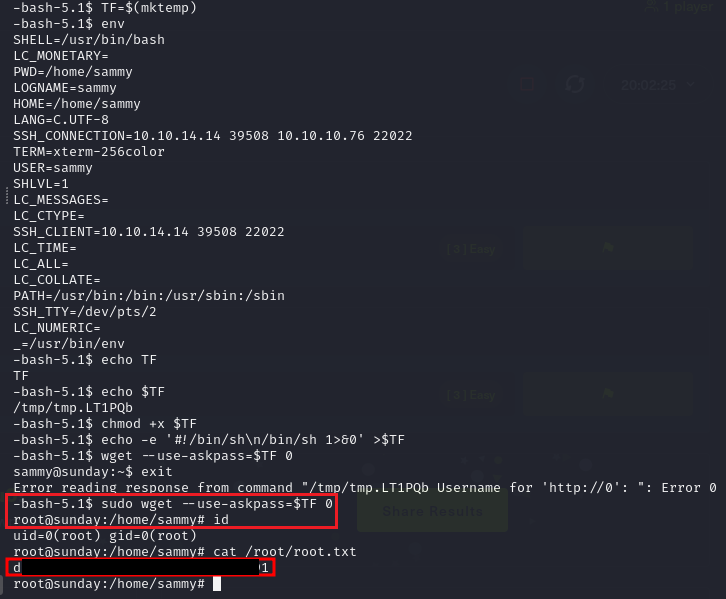


Figure 10 - Privilege escalation and root flag

# **Personal comments**

This box was funny for me. I learnt about the Finger service and I liked I leveraged it to retrieve users’ list. Also, I liked I found some interesting information inside an history file and a shadow backup file. In my opinion, was a good box. However, it was easy to exploit and I rated in this way on the Hack The Box platform.