Sunday walkthrough

Index

List of pictures

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:

```
┌──(k14d1u5㉿k14d1u5-kali)-[/media/…/Linux/Easy/Sunday/nMap]
└─$ nmap -sT -sV -A -sC -p- 10.10.10.76 -oA Sunday2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 08:02 AEDT
Stats: 0:02:52 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 10.64% done; ETC: 08:29 (0:24:05 remaining)
Stats: 0:26:27 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 90.33% done; ETC: 08:31 (0:02:50 remaining)
Stats: 0:30:41 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 92.74% done; ETC: 08:35 (0:02:24 remaining)
Nmap scan report for 10.10.10.76
Host is up (0.042s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
79/tcp    open  finger?
| fingerprint-strings:
|   GenericLines:
|     No one logged on
|   GetRequest:
|     Login Name TTY Idle When Where
|     HTTP/1.0 ???
|   HTTPOptions:
|     Login Name TTY Idle When Where
|     HTTP/1.0 ???
|     OPTIONS ???
|   Help:
|     Login Name TTY Idle When Where
|     HELP ???
|   RTSPRequest:
|     Login Name TTY Idle When Where
|     OPTIONS ???
|     RTSP/1.0 ???
|   SSLSessionReq, TerminalServerCookie:
|     Login Name TTY Idle When Where
|_    Login Name TTY Idle When Where
|_finger: No one logged on\x0D
111/tcp   open  rpcbind 2-4 (RPC #100000)
515/tcp   open  printer
6787/tcp  open  http    Apache httpd
|_http-server-header: Apache
|_http-title: 400 Bad Request
22022/tcp open  ssh     OpenSSH 8.4 (protocol 2.0)
| ssh-hostkey:
|   2048 aa:00:94:32:18:60:a4:93:3b:87:a4:b6:f8:02:68:0e (RSA)
|_  256 da:2a:6c:fa:6b:b1:ea:16:1d:a6:54:a1:0b:2b:ee:48 (ED25519)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port79-TCP:V=7.94SVN%I=7%D=10/24%Time=67196F98%P=x86_64-pc-linux-gnu%r(
SF:GenericLines,12,"No\x20one\x20logged\x20on\r\n")%r(GetRequest,93,"Login
SF:\x20\x20\x20\x20\x20\x20\x20\x20Name\x20\x20\x20\x20\x20\x20\x20\x20\x2
```

Figure 1 - nMap scan results (part 1)

```
22022/tcp open  ssh     OpenSSH 8.4 (protocol 2.0)
| ssh-hostkey:
|   2048 aa:00:94:32:18:60:a4:93:3b:87:a4:b6:f8:02:68:0e (RSA)
|_  256 da:2a:6c:fa:6b:b1:ea:16:1d:a6:54:a1:0b:2b:ee:48 (ED25519)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port79-TCP:V=7.94SVN%I=7%D=10/24%Time=67196F98%P=x86_64-pc-linux-gnu%r(
SF:GenericLines,12,"No\x20one\x20logged\x20on\r\n")%r(GetRequest,93,"Login
SF:\x20\x20\x20\x20\x20\x20\x20\x20Name\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20TTY\x20\x20\x20\x20\x20\x20\x20\x20Idle\x20\x2
SF:0\x20\x20When\x20\x20\x20\x20Where\r\n/\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\nGET\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:?\?\?\r\nHTTP/1\.0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\?\?\?\r\n")%r(Help,5D,"Login\x20\x20\x20\x20\x20\x20\x20Name\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20TTY\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20Idle\x20\x20\x20\x20When\x20\x20\x20\x20Where\r\nH
SF:ELP\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\?\?\?\r\n")%r(HTTPOptions,93,"Login\x20\x20\x20\x20\x20\x20\x20Nam
SF:e\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20TTY\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20Idle\x20\x20\x20\x20When\x20\x20\x20\x20Wh
SF:ere\r\n/\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\?\?\?\r\nHTTP/1\.0\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\nOPTIONS\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\n")%r(RTSPRequest,93,"Login\x20
SF:\x20\x20\x20\x20\x20\x20Name\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20TTY\x20\x20\x20\x20\x20\x20\x20\x20Idle\x20\x20\x2
SF:0\x20When\x20\x20\x20\x20Where\r\n/\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\nOPTIONS\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\nRTSP/1\
SF:.0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\n")%
SF:r(SSLSessionReq,5D,"Login\x20\x20\x20\x20\x20\x20\x20Name\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20TTY\x20\x20\x20\x20\x
SF:20\x20\x20\x20Idle\x20\x20\x20\x20When\x20\x20\x20\x20Where\r\n\x16\x03
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\?\?\?\r\n")%r(TerminalServerCookie,5D,"Login\x20\x20\x20\x20\
SF:x20\x20\x20Name\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20TTY\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20Idle\x20\x20\x20\x20When\x20
SF:\x20\x20\x20Where\r\n\x03\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2965.13 seconds
```

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:

```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ ./finger-user-enum.pl -U ./usernames.txt -t 10.10.10.76
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )

 ------------------------------------------------------
|                   Scan Information                   |
 ------------------------------------------------------

Worker Processes ......... 5
Usernames file ........... ./usernames.txt
Target count ............. 1
Username count ........... 81475
Target TCP port .......... 79
Query timeout ............ 5 secs
Relay Server ............. Not used

######## Scan started at Fri Nov  1 05:12:11 2024 #########
access@10.10.10.76: access No Access User                       < .  .  .  .  . >..nobody4  SunOS 4.x NFS Anonym
ai@10.10.10.76: aiuser   AI User                              < .  .  .  .  . >..
anonymous@10.10.10.76: Login       Name               TTY         Idle    When    Where..nobody   NFS Anonymous Acce
bin@10.10.10.76: bin             ???                          < .  .  .  .  . >..
configuration@10.10.10.76: Login       Name               TTY         Idle    When    Where..netcfg   Network Config
daemon@10.10.10.76: daemon          ???                          < .  .  .  .  . >.._ntp     NTP Daemon
ike@10.10.10.76: ikeuser  IKE Admin                           < .  .  .  .  . >..
lp@10.10.10.76: lp       Line Printer Admin                   < .  .  .  .  . >..
message@10.10.10.76: Login       Name               TTY         Idle    When    Where..smmsp    SendMail Message Sub
network@10.10.10.76: Login       Name               TTY         Idle    When    Where..netadm   Network Admin
no@10.10.10.76: noaccess No Access User                       < .  .  .  .  . >..
nobody@10.10.10.76: nobody   NFS Anonymous Access                 < .  .  .  .  . >..
printer@10.10.10.76: Login       Name               TTY         Idle    When    Where..lp       Line Printer Admin
program@10.10.10.76: Login       Name               TTY         Idle    When    Where..smmsp    SendMail Message Sub
remote@10.10.10.76: Login       Name               TTY         Idle    When    Where..unknown  Unknown Remote UID
reserved@10.10.10.76: Login       Name               TTY         Idle    When    Where..ftp      FTPD Reserved UID
root@10.10.10.76: root     Super-User            ssh          <Dec  7, 2023> 10.10.14.46          ..
sammy@10.10.10.76: sammy          ???            ssh          <Apr 13, 2022> 10.10.14.13          ..
server@10.10.10.76: server UID                 < .  .  .  .  . >..
submission@10.10.10.76: Login       Name               TTY         Idle    When    Where..smmsp    SendMail Message
sunny@10.10.10.76: sunny          ???            ssh          <Apr 13, 2022> 10.10.14.13          ..
unknown@10.10.10.76: unknown  Unknown Remote UID                 < .  .  .  .  . >..
user@10.10.10.76: user   AI User                              < .  .  .  .  . >..openldap OpenLDAP User
    < .  .  .  .  . >..nobody4  SunOS 4.x NFS Anonym            < .  .  .  .  . >..
######## Scan completed at Fri Nov  1 05:38:42 2024 #########
23 results.

81475 queries in 1591 seconds (51.2 queries / sec)
```

Figure 3 - Finger user enumeration

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

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:

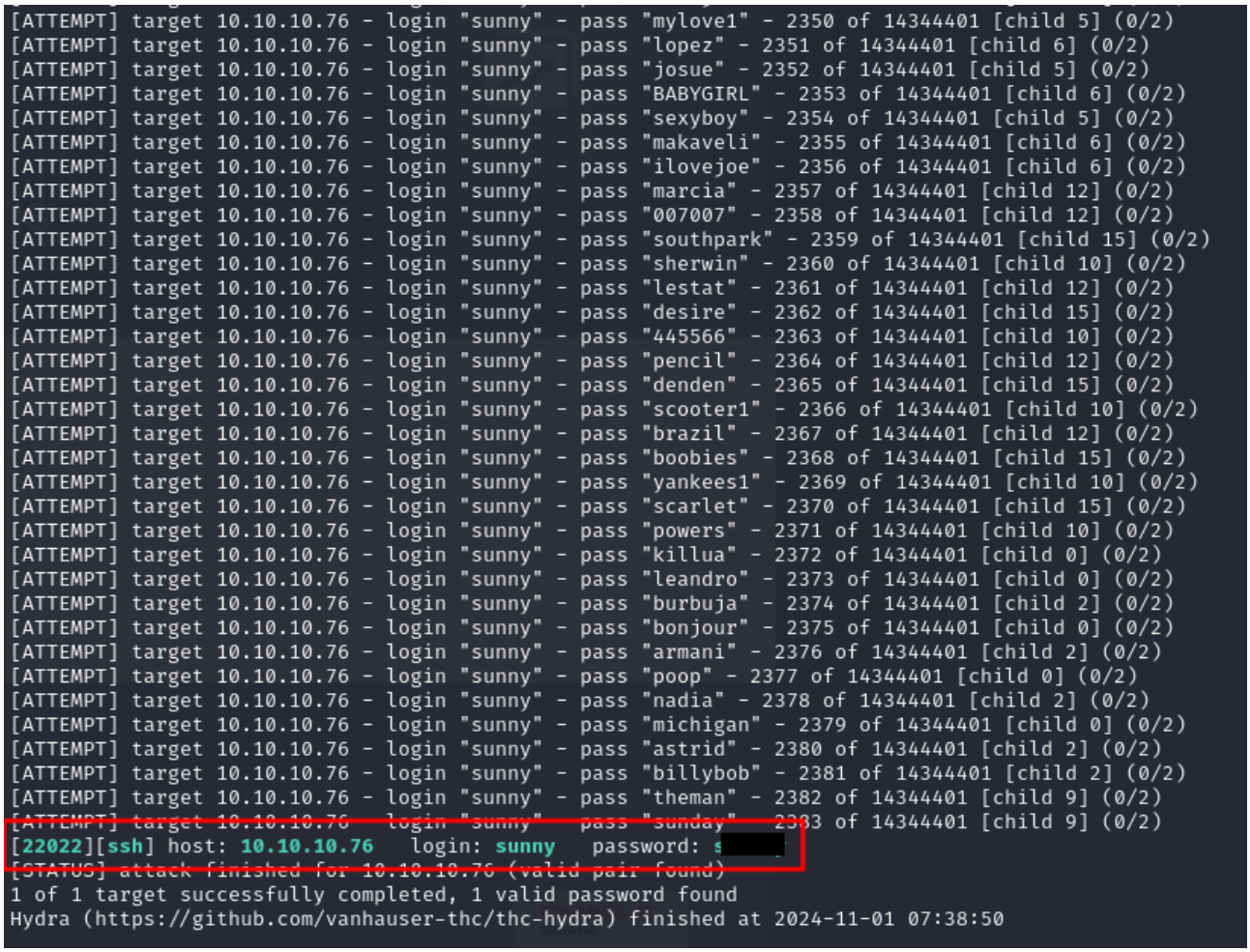

Figure 4 - Credentials found

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

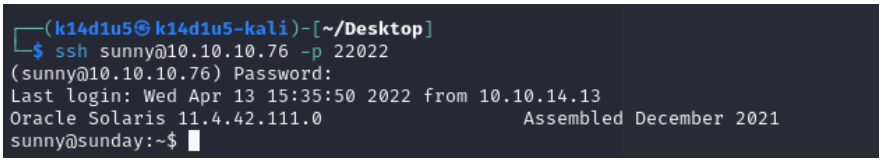

Figure 5 - SSH connection as sunny user

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

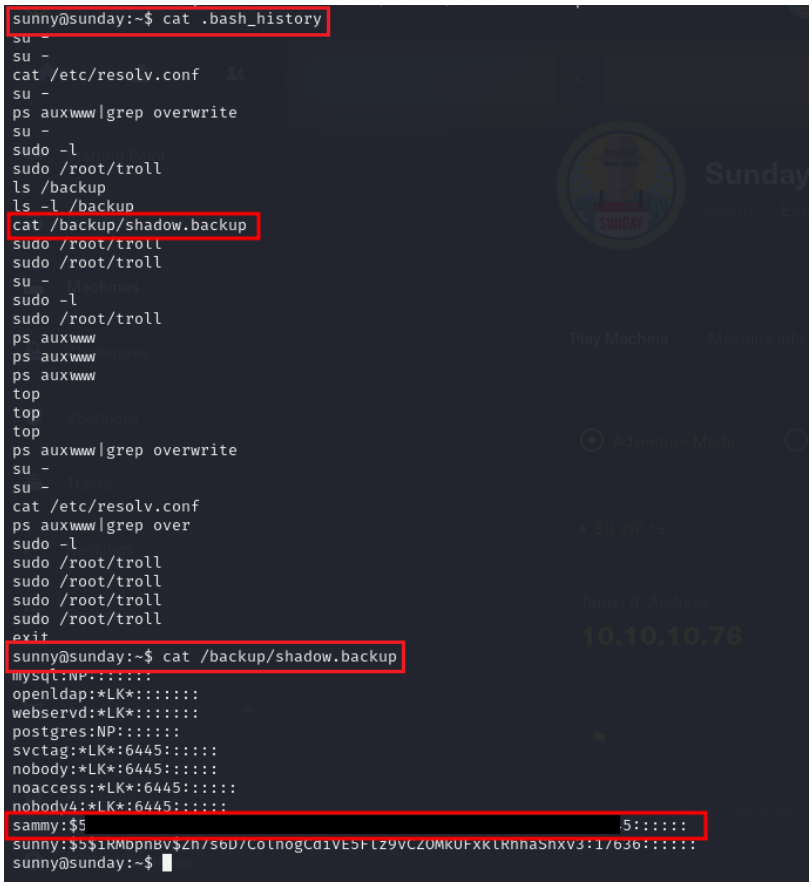

Figure 6 - Shadow backup file found

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

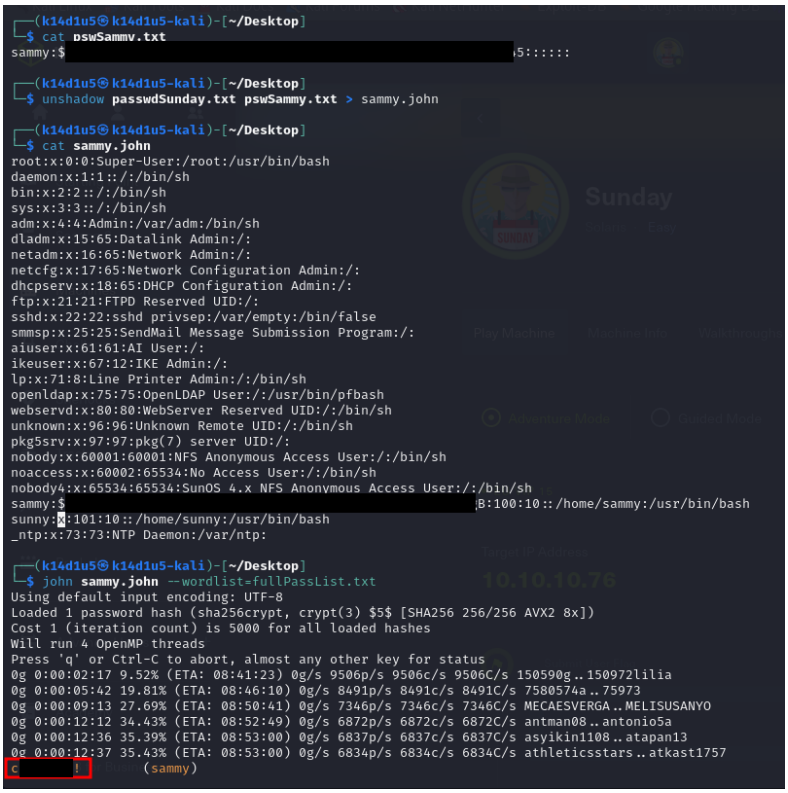

Figure 7 – Successful cracking

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

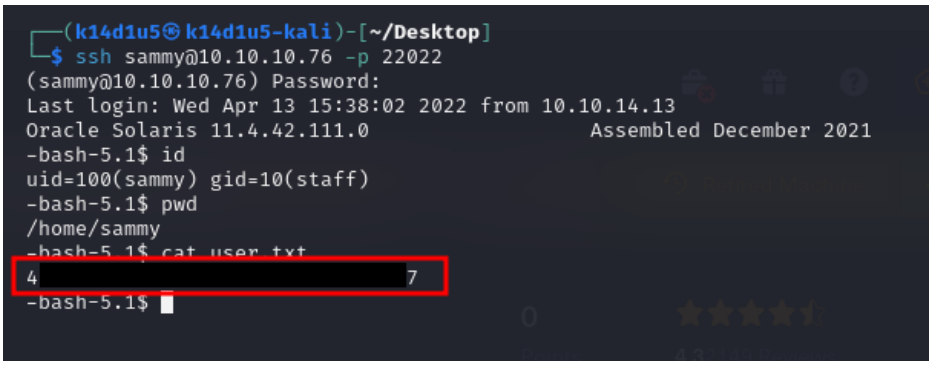

Figure 8 - User flag

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 *wget* tool:

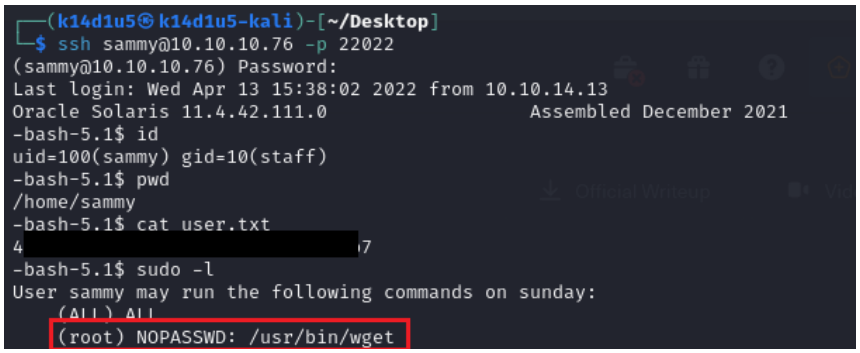

Figure 9 - Useful information to escalate privileges

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

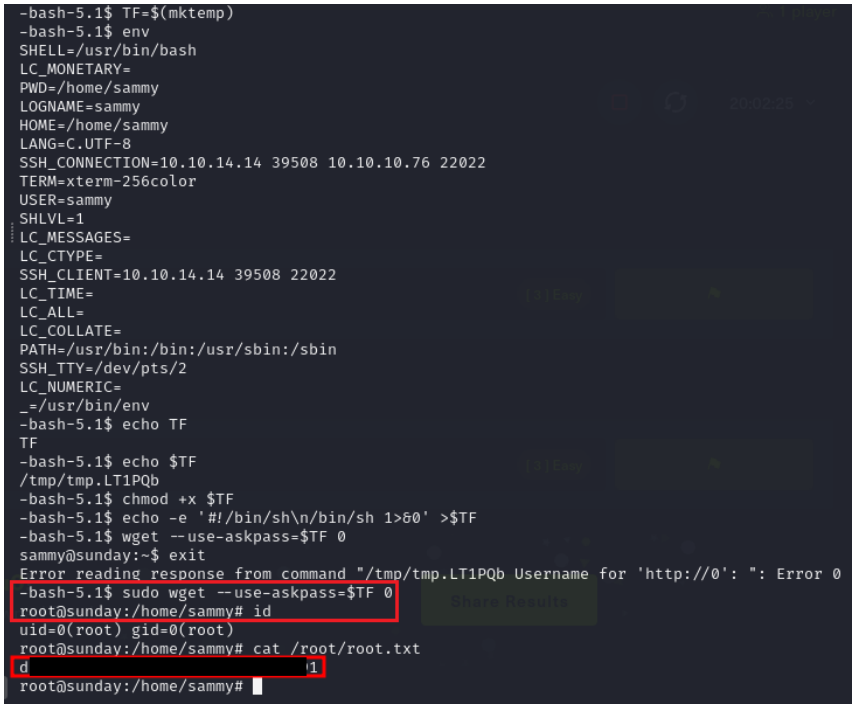

Figure 10 - Privilege escalation and root flag

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.