**Traverxec walkthrough**

# **Index**

[Index 1](#_Toc177657476)

[List of pictures 1](#_Toc177657477)

[Disclaimer 2](#_Toc177657478)

[Reconnaissance 2](#_Toc177657479)

[Initial foothold 2](#_Toc177657480)

[User flag 2](#_Toc177657481)

[Privilege escalation 5](#_Toc177657482)

[Personal comments 6](#_Toc177657483)

[Appendix A – CVE-2019-16278 6](#_Toc177657484)

[Appendix B – Double check about privesc method (after I became root) 6](#_Toc177657485)

[References 6](#_Toc177657486)

# **List of pictures**

[Figure 1 - nMap scan results 2](#_Toc177657438)

[Figure 2 - Nostromo exploit 3](#_Toc177657439)

[Figure 3 - Web server configuration 3](#_Toc177657440)

[Figure 4 - Access to the server's public home directory 4](#_Toc177657441)

[Figure 5 - Interesting backup file 4](#_Toc177657442)

[Figure 6 - Passphrase cracked 4](#_Toc177657443)

[Figure 7 - SSH Login and user flag 5](#_Toc177657444)

[Figure 8 - Privesc information 5](#_Toc177657445)

[Figure 9 - Root shell and flag 5](#_Toc177657446)

[Figure 10 - Double check about privesc post root flag 6](#_Toc177657447)

# **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:

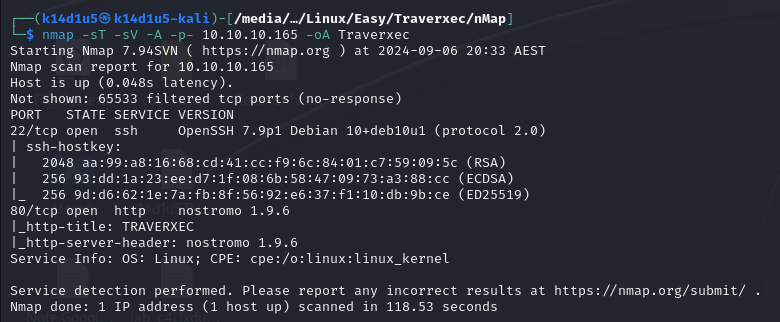


Figure - nMap scan results

Open ports are 22 and 80. So, this box has SSH service enabled (port 22) and a web application running on port 80. Also, nMap recognized Linux as operative system and Nostromo as web server. However, nMap didn’t provide any other information about it.

# **Initial foothold**

Since I have nothing but a web application running on port 80 based on a Nostromo web server, I looked for some information and exploit about Nostromo. I found out the CVE-2019-16278, so I downloaded an exploit.

# **User flag**

I run it to obtain a shell on the target, as shown in the following picture:

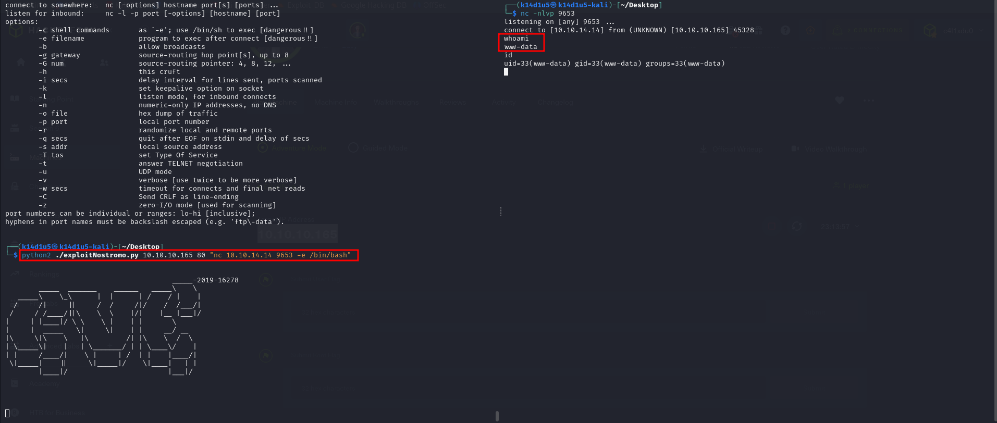


Figure 2 - Nostromo exploit

Once I was on the target machine, I searched some interesting information. In the path I found the file. It contained a user and a hash. I cracked it and tried to use to log in via SSH, but it didn’t work. I kept to search other interesting files and information. I found a backup, but it wasn’t useful too. After some time, I noted that in the path the interesting file was . This file contains some web server configuration. In particular, the web server has set a public home directory, as shown in the following picture:

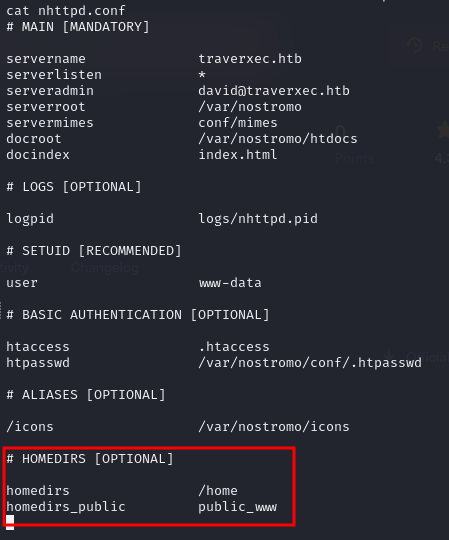


Figure 3 - Web server configuration

Due to this configuration, a user can access to the other user home directories via browser using an URL like . Regarding this box, I can browse the David home directory using the URL. Obviously, I can’t see anything via browser because I still don’t have the right permission to read this folder. However, as I previously found out, I can read and access to the public home directory. I just need to navigate to the right path using the shell:

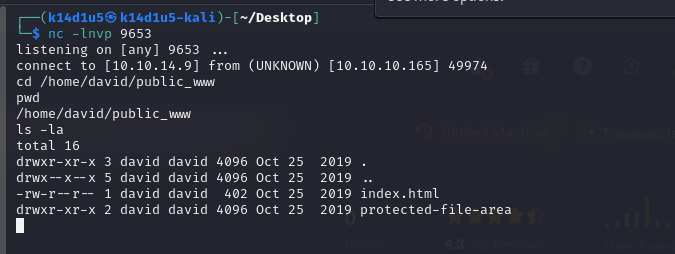


Figure 4 - Access to the server's public home directory

At this point I explored this directory and I found a very interesting file:

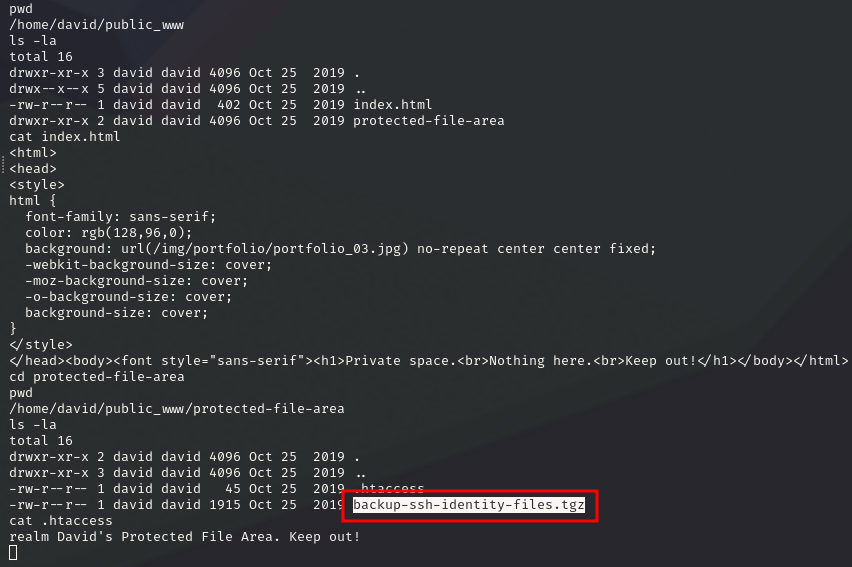


Figure 5 - Interesting backup file

So, I transferred it on my Kali machine and I found the David’s RSA key. I tried to use it to log in via SSH, but I need a passphrase. So, I cracked it using John The Ripper tool as shown in the following:

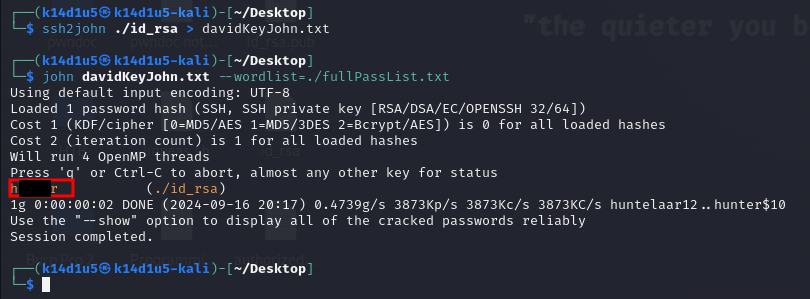


Figure 6 - Passphrase cracked

Since I cracked it, I tried to log in via SSH, as I did previously, and I retrieved the user flag:

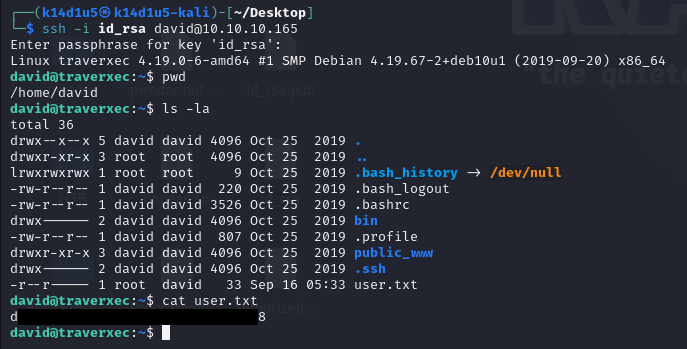


Figure 7 - SSH Login and user flag

# **Privilege escalation**

Finally, I can escalate my privileges. Looking for some interesting file in the David home directory, I found an interesting shell script. It executes a command as , as shown in the following picture:

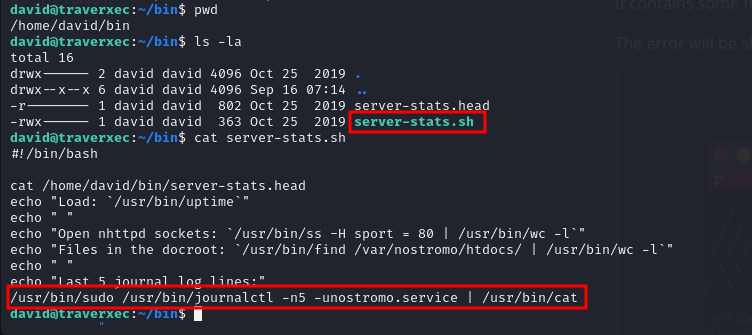


Figure - Privesc information

So, I looked the manual from the shell and I found out it is used to print log entries stored in the journal. Also, I found out it uses the command to achieve its goal. This means I was able to use the same command I found in the shell script (except the pipe to the tool) to open a shell as root and retrieve the root flag:

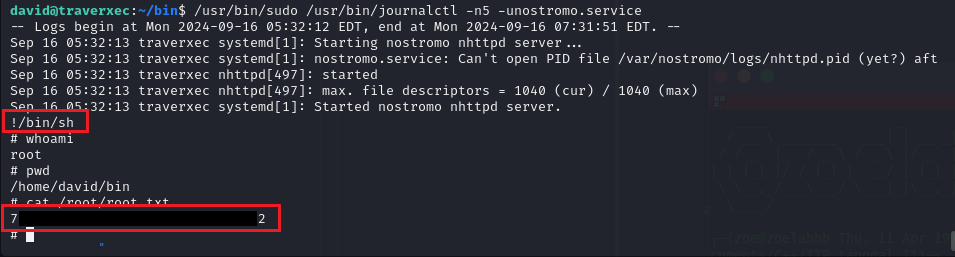


Figure 9 - Root shell and flag

# **Personal comments**

I consider this box very funny and quite basic. It was very interesting the privilege escalation task because I was not able to check the sudoers file (I don’t have the David password to use the command). Also, I learned something new about web servers. I found out I can leverage a public home directory and I understood better how it works. In conclusion, I rated this box as easy.

# **Appendix A – CVE-2019-16278**

This CVE is about the Nostromo web server, aka nhttpd, an open-source web server that is very popular on Unix system like FreeBSD, OpenBSD, etc. Nostromo fails to verify a URL that leads to path traversal to any file in the system. This issue is caused by a directory traversal in the function in nostromo nhttpd. So, an unauthenticated attacker can force the server points to a shell file like and execute arbitrary commands. It's critical due to all Nostromo's versions, include the lasted release 1.9.6, are vulnerable.

# **Appendix B – Double check about privesc method (after I became root)**

After I gain the root flag, I was very curios about why the privilege escalation method I used effectively worked. I imagined the scenario allowed the David user to run that command using and without providing the password. So, I checked it and I was right. In fact, when I completed the box, I changed the David password (when I was root) and I looked the sudoers file for David. As I said, I was right and the information I found out were the following:

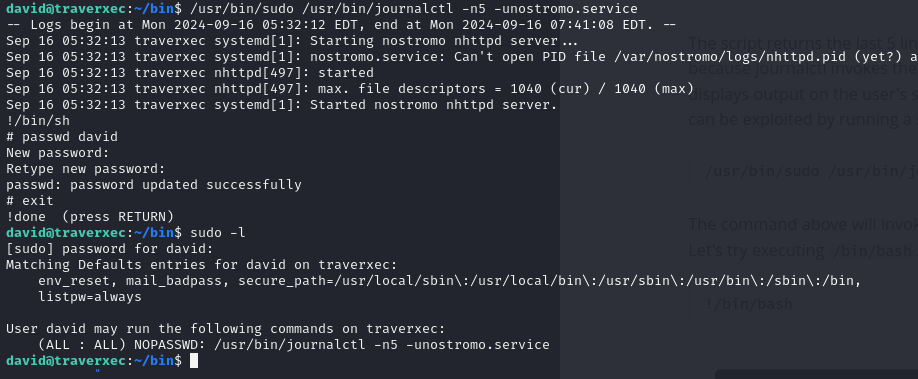


Figure 10 - Double check about privesc post root flag

I obviously reset the box before I stopped the machine, so I recovered its initial state.

# **References**

<https://github.com/aN0mad/CVE-2019-16278-Nostromo_1.9.6-RCE>

<https://www.exploit-db.com/exploits/47837>

<https://www.sudokaikan.com/2019/10/cve-2019-16278-unauthenticated-remote.html>

<https://www.rapid7.com/db/modules/exploit/multi/http/nostromo_code_exec/>