**Postman walkthrough**

# **Index**

[Index 1](#_Toc174284857)

[List of pictures 1](#_Toc174284858)

[Disclaimer 2](#_Toc174284859)

[Reconnaissance 2](#_Toc174284860)

[Initial foothold 3](#_Toc174284861)

[User flag 3](#_Toc174284862)

[Privilege escalation 7](#_Toc174284863)

# **List of pictures**

[Figure 1 - nMap scan results 2](#_Toc174284842)

[Figure 2 - Redis home directory 3](#_Toc174284843)

[Figure 3 - Geenrating SSH key pair 3](#_Toc174284844)

[Figure 4 - Public key formatted 3](#_Toc174284845)

[Figure 5 - Public key uploaded on target 4](#_Toc174284846)

[Figure 6 - SSH connection 4](#_Toc174284847)

[Figure 7 - .bash\_history content 5](#_Toc174284848)

[Figure 8 - id\_rsa.bak file 6](#_Toc174284849)

[Figure 9 - Data in John the Ripper tool format 6](#_Toc174284850)

[Figure 10 - Passphrase decoded 6](#_Toc174284851)

[Figure 11 - Matt's SSH login disabled 7](#_Toc174284852)

[Figure 12 - Log in as Matt 7](#_Toc174284853)

[Figure 13 - Privilege escalation exploit 8](#_Toc174284854)

[Figure 14 - Root shell 8](#_Toc174284855)

[Figure 15 - Root flag 8](#_Toc174284856)

# **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’re willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

# **Reconnaissance**

The results of an initial nMap scan are the following:

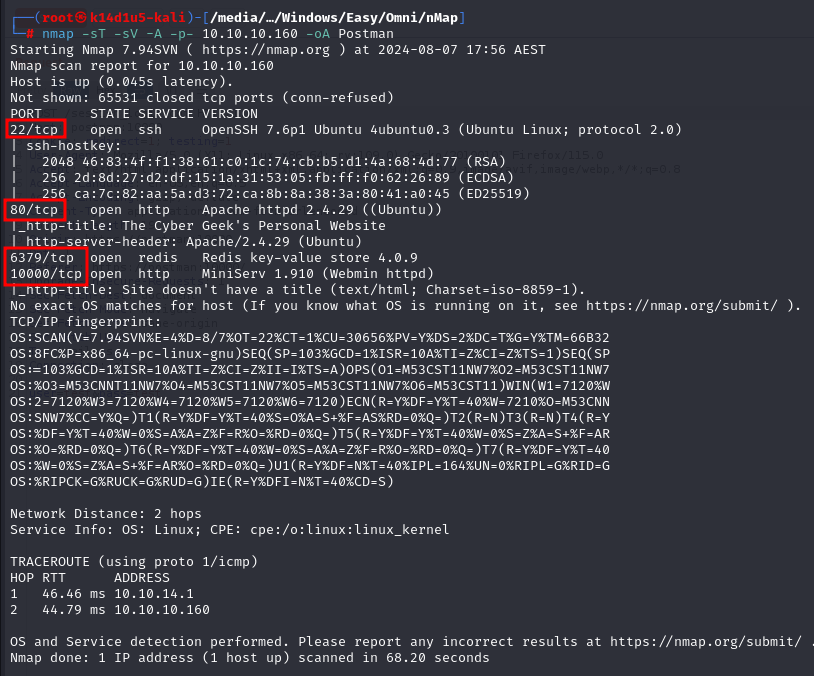


Figure 1 - nMap scan results

Open ports a re 22, 80, 6379 and 10000. So, this box has SSH service enabled on port 22, Redis service enabled on port 6379 and two web application running on ports 80 and 10000. Also, nMap has recognized Linux as operative system.

Web application running on port 10000 can be reached adding a new entry in the file.

# **Initial foothold**

Based on which services I found open via the nMap scan, I tried to interact with the Redis service. Since I can interact with it, I can explore its file system. For example, I found the Redis home directory:



Figure 2 - Redis home directory

Also, I found out that the web application running on port 10000 require credentials.

# **User flag**

Looking for something interesting on the Internet, I found out that I could be able to upload the SSH key. So, I generated a key pair as shown in the following figure:

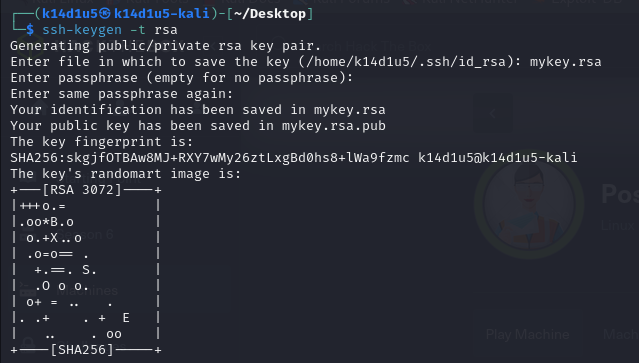


Figure 3 - Generating SSH key pair

The second step was to give the correct format to my public key, adding some new lines:

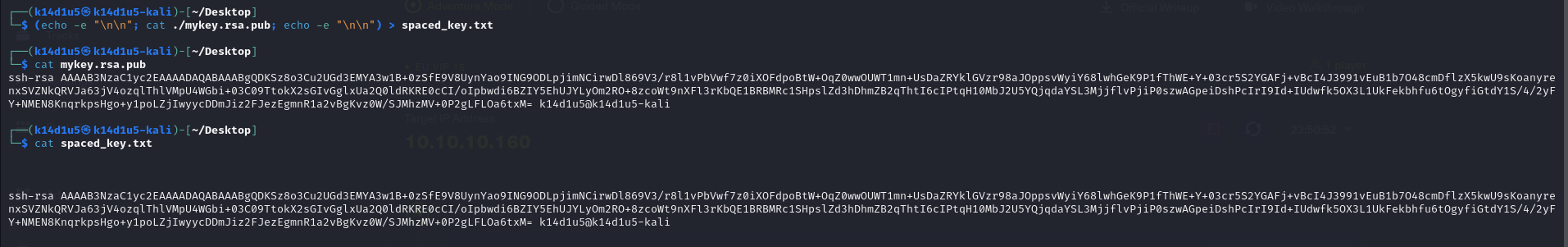


Figure 4 - Public key formatted

Now I am ready to upload the key on the target via Redis. To accomplish this goal, I run the following commands:



Figure 5 - Public key uploaded on target

At this point, I am ready to connect to the target via SSH:

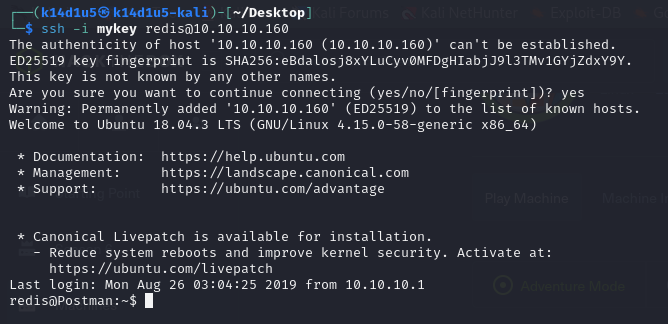


Figure 6 - SSH connection

However, I am not ready to retrieve the user flag. Exploring the file system, I found that the user flag is owned by a user named Matt. So, I started to find something useful to perform lateral movement and became Matt. In the Redis user home directory, I found a very interesting information in the file. In that file I found the following command previously run:

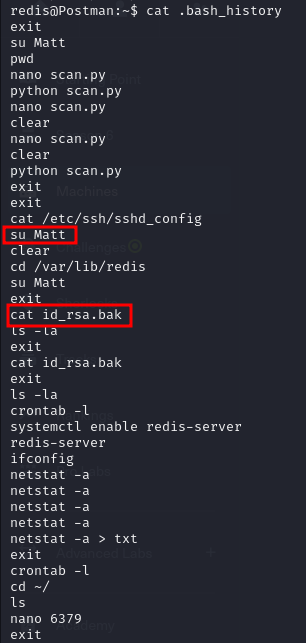


Figure 7 - .bash\_history content

So, I downloaded/copied the file on my Kali machine. This file contains Matt’s private key:

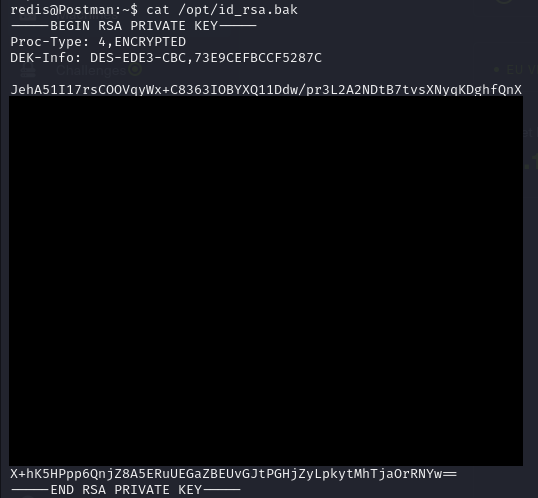


Figure 8 - id\_rsa.bak file

I tried to use it to login to the target via SSH, but I need a passphrase. So, I tried to crack the passphrase using John the Ripper tool. I prepared the data for John running the following command:

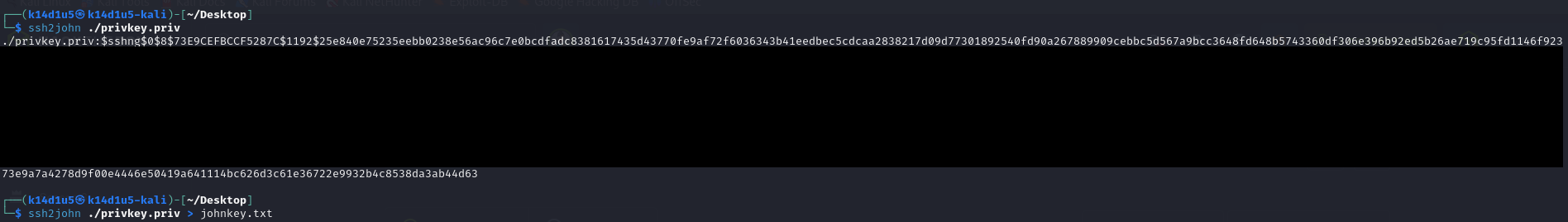


Figure 9 - Data in John the Ripper tool format

Now, I can decode the passphrase running John the Ripper tool, as shown:

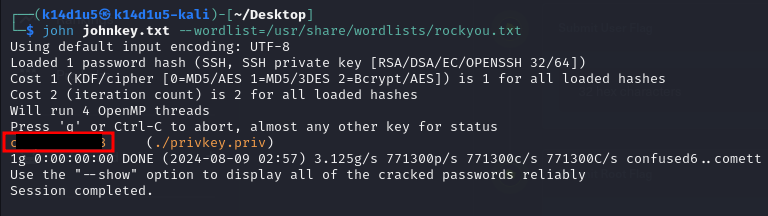


Figure 10 - Passphrase decoded

I tried to use this credential to log in the target via SSH. However, the file set Matt user with SSH disabled:

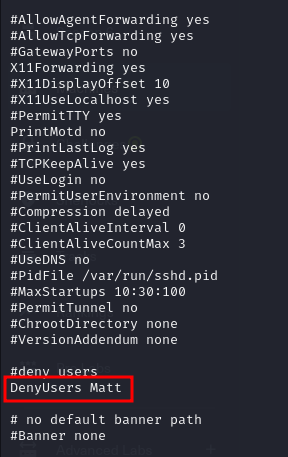


Figure 11 - Matt's SSH login disabled

But I have found credentials. So, I simply tried them to switch user from Redis to Matt:



Figure 12 - Log in as Matt

I just need to retrieve the user flag. However, I forgot the user flag screenshot.

# **Privilege escalation**

Now, I need to escalate my privileges. I remembered that web application running on port 10000 require credentials. For this reason, I tried to use Matt credentials to log in the application and it luckily worked! Also, I tried to intercept the login request and I found that the server is MiniServ 1.910. Also, I noted that the web application is named Webmin. I looked for some exploit on the Internet about it and I found a very interesting one. So, I simply tried it. As first step, I set a listener to receive the shell. After that, I run the exploit as shown in the following picture:

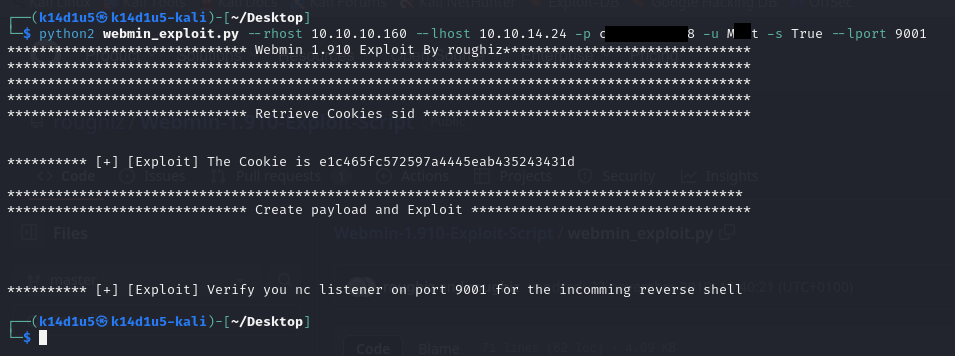


Figure 13 - Privilege escalation exploit

It worked and I received the shell as root:

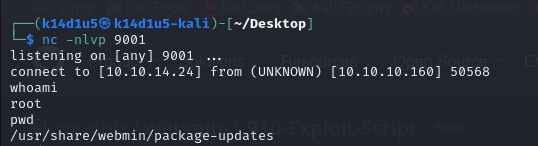


Figure 14 - Root shell

So, the root flag is:



Figure 15 - Root flag