**Tabby walkthrough**

# **Index**

[Index 1](#_Toc169442733)

[List of pictures 1](#_Toc169442734)

[Disclaimer 2](#_Toc169442735)

[Reconnaissance 2](#_Toc169442736)

[Initial foothold 2](#_Toc169442737)

[User flag 4](#_Toc169442738)

[Privilege escalation 6](#_Toc169442739)

# **List of pictures**

[Figure 1 - nMap scan results 2](#_Toc169442743)

[Figure 2 - External link 3](#_Toc169442744)

[Figure 3 - Tomcat configuration file with credentials 3](#_Toc169442745)

[Figure 4 - Tomcat host manager GUI 4](#_Toc169442746)

[Figure 5 - Upload malicious war file 4](#_Toc169442747)

[Figure 6 - Reverse shell 4](#_Toc169442748)

[Figure 7 - Interesting file 5](#_Toc169442749)

[Figure 8 - Cracking zip password 5](#_Toc169442750)

[Figure 9 - /etc/passwd file via path traversal 5](#_Toc169442751)

[Figure 10 - Lateral movement 6](#_Toc169442752)

[Figure 11 - Way to privesc 6](#_Toc169442753)

[Figure 12 - Privesc and root flag 6](#_Toc169442754)

# **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:

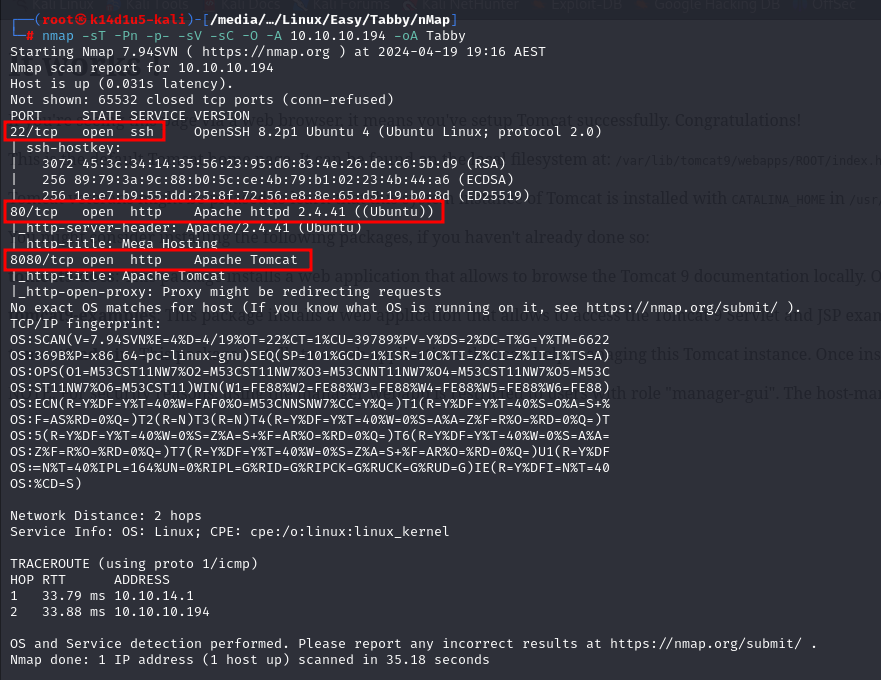


Figure 1 - nMap scan results

Open ports are 22, 80 and 8080. So, this box has the SSH service enabled and two web application, one running on port 80 and the other one running on port 8080. Also, nMap can provide just Linux as operative system.

# **Initial foothold**

Analyzing the web application running on port 80, one of its links (NEWS link) would access to **megahosting.htb**, so I add this entry into my **/etc/hosts** file. When I access to this link, I see that it uses a GET parameter named **file**, as shown in the following figure:

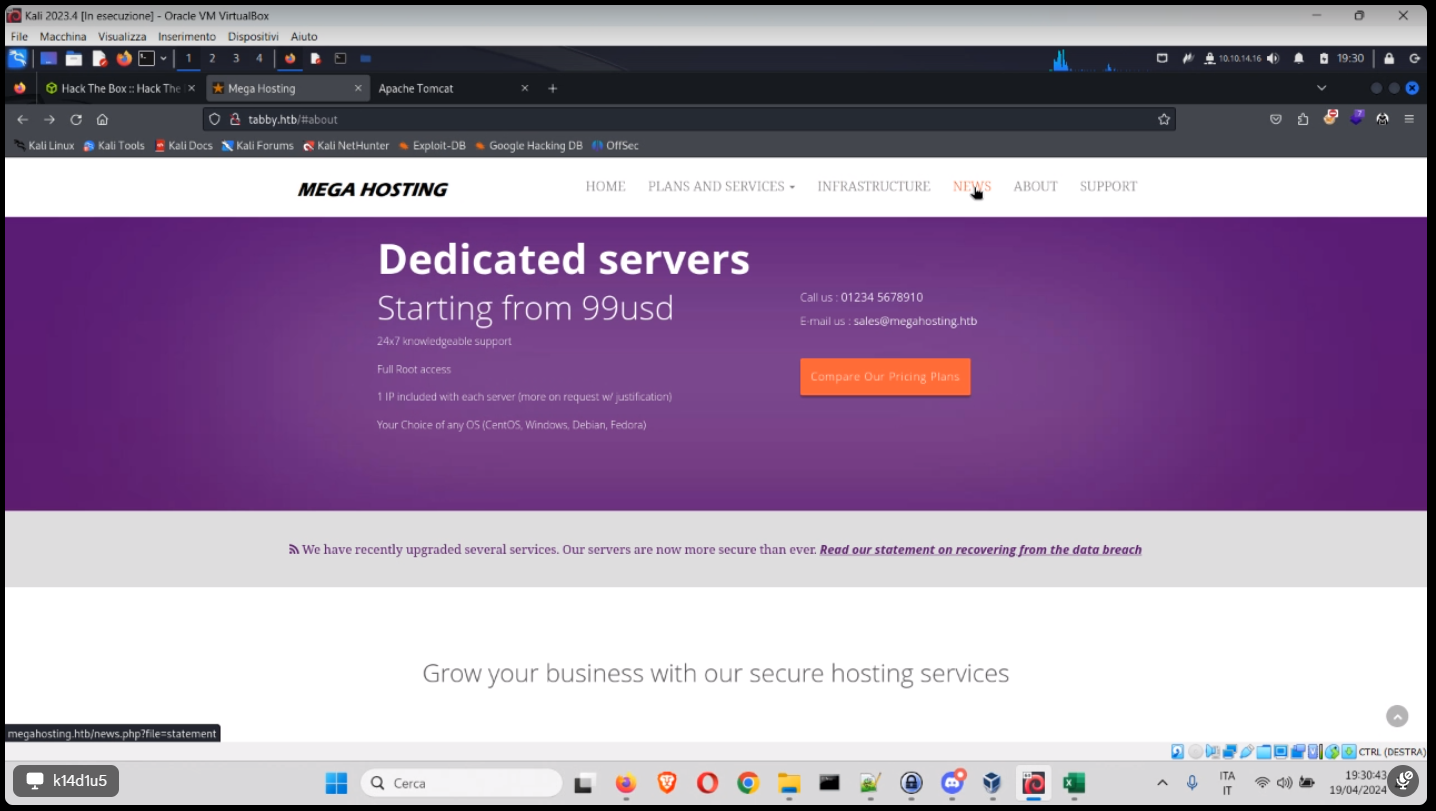


Figure 2 - External link

I can see that **megahosting.htb** is used as email domain too. I can leverage the **file** parameter to perform a directory traversal attack. Looking for the Tomcat documentation on Internet, I found that the **/usr/share/tomcat9/etc/tomcat-users.xml** file can contain some credential. So, I try to access to this file:

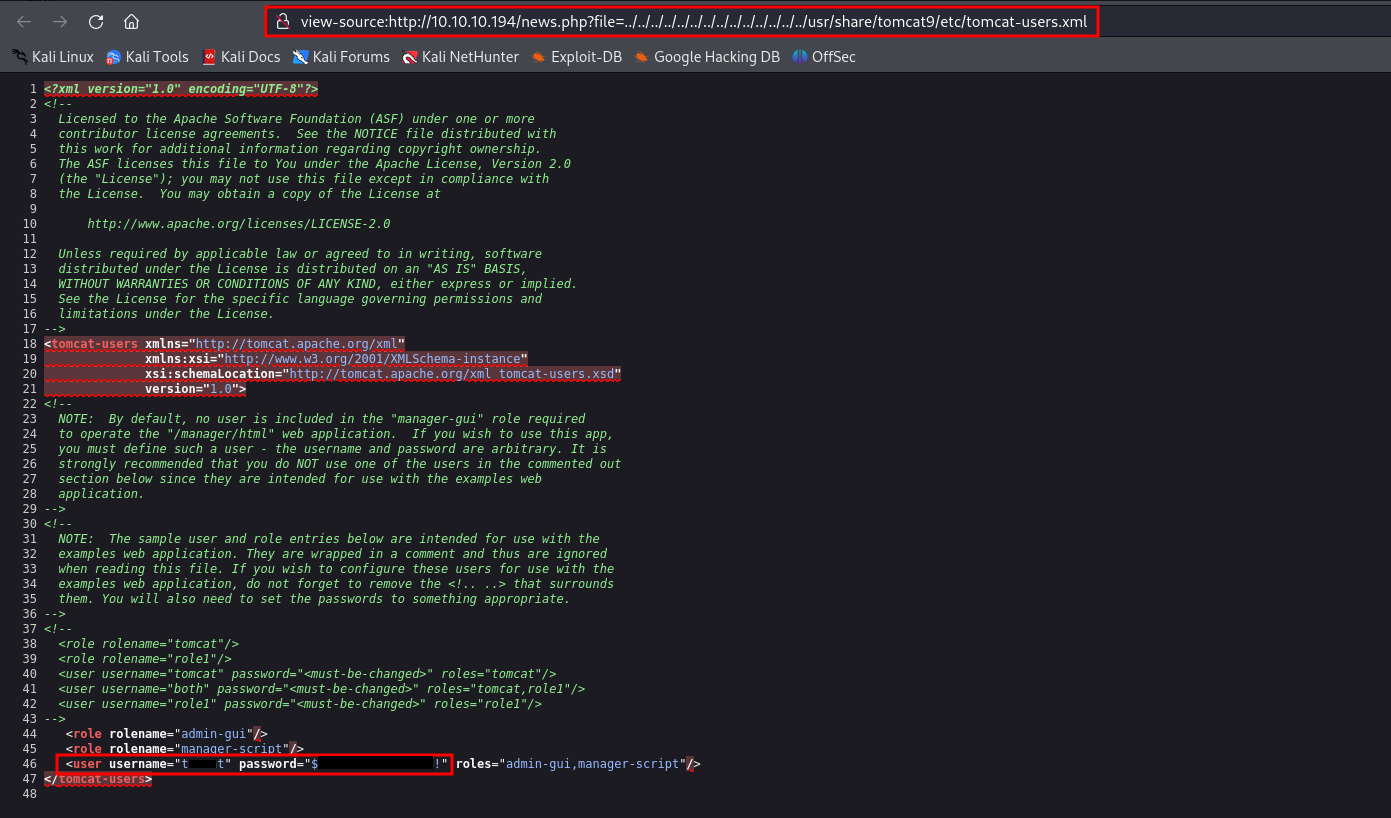


Figure 3 - Tomcat configuration file with credentials

I can use these credentials to access to the host manager at the path:

The host manager looks like the following:

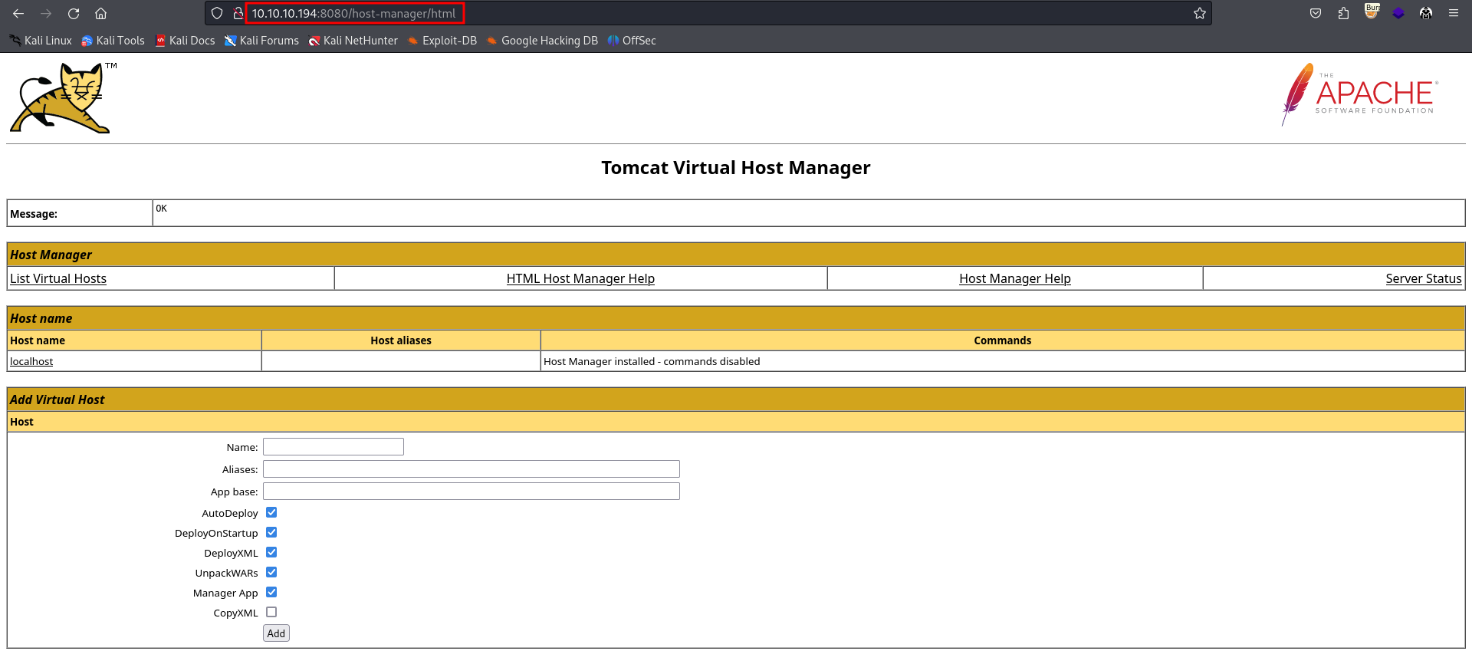


Figure 4 - Tomcat host manager GUI

# **User flag**

Since I am facing Tomcat, I look for a way to upload a malicious war file. I can generate a malicious war file running the following command:

So, I can upload it using curl tool, as shown in the following:



Figure 5 - Upload malicious war file

Obviously, I need an opened listener to receive connection. Also, to let the shell pop up, I just need to visit the [**http://10.10.10.194:8080/tmp**](http://10.10.10.194:8080/tmp) URL, since I uploaded the reverse shell in the **/tmp/** path and I obtain the shell:

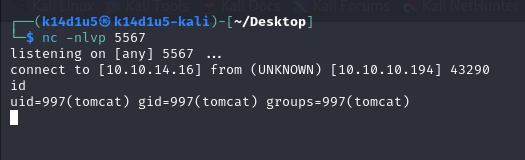


Figure 6 - Reverse shell

However, this is not the user that has the user flag. Looking for some interesting file in the filesystem, I found the **/var/www/html/files/16162020\_backup.zip**:

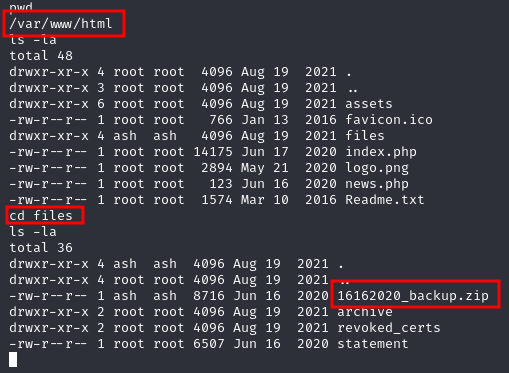


Figure 7 - Interesting file

Since it is a backup file, it looks very interesting. Unlucky, it is protected by a password. So, I downloaded it on my Kali machine and I tried to crack it running the following commands:



Figure 8 - Cracking zip password

Luckly, I cracked the password and I can open the zip! However, the zip itself it was not useful. Maybe this password can be used for something else. I remembered that I found a path traversal vulnerability, so I checked the **/etc/passwd file** to look for some user on the machine:

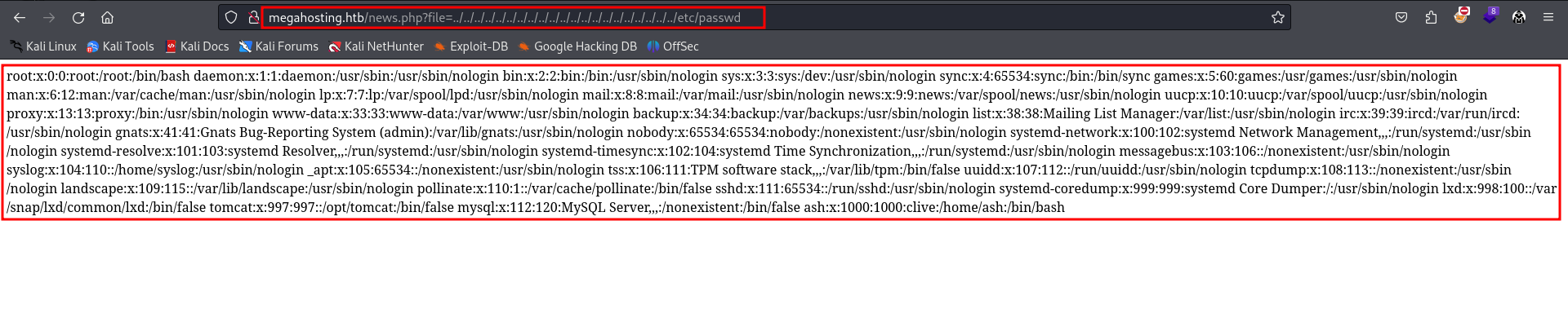


Figure 9 - /etc/passwd file via path traversal

In this way, I found a user called **ash**. So, I tried to became ash using the password I cracked before:

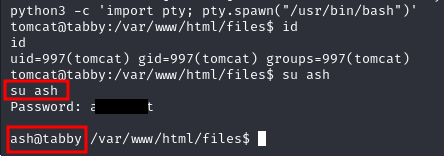


Figure 10 - Lateral movement

Finally, I am a true user on the machine and I can retrieve the flag (I forgot the user flag screenshot).

# **Privilege escalation**

Now it is time to escalate my privileges. To do it, I run Linpeas.sh script and I found that the sudo version is vulnerable:

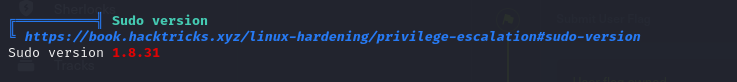


Figure 11 - Way to privesc

So, I download the Pwnkit exploit, run it on the target machine and I obtain a root shell and flag:

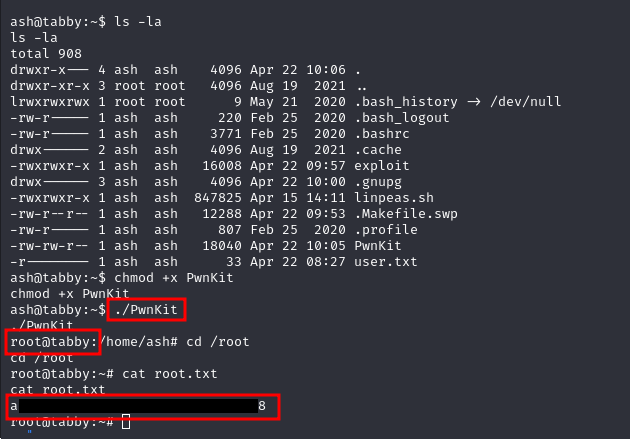


Figure 12 - Privesc and root flag