**ScriptKiddie walkthrough**

# **Index**

[Index 1](#_Toc157500754)

[List of pictures 1](#_Toc157500755)

[Disclaimer 2](#_Toc157500756)

[Reconnaissance 2](#_Toc157500757)

[Initial foothold 2](#_Toc157500758)

[User flag 3](#_Toc157500759)

[Privilege escalation 4](#_Toc157500760)

# **List of pictures**

[Figure 1 - nMap scan results 2](#_Toc157500792)

[Figure 2 - Application running on port 5000 3](#_Toc157500793)

[Figure 3 - Generating malicious APK file 3](#_Toc157500794)

[Figure 4 - Exploit 4](#_Toc157500795)

[Figure 5 - User reverse shell and user flag 4](#_Toc157500796)

[Figure 6 - Useful information for privilege escalation 5](#_Toc157500797)

[Figure 7 - Root flag 5](#_Toc157500798)

# **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:

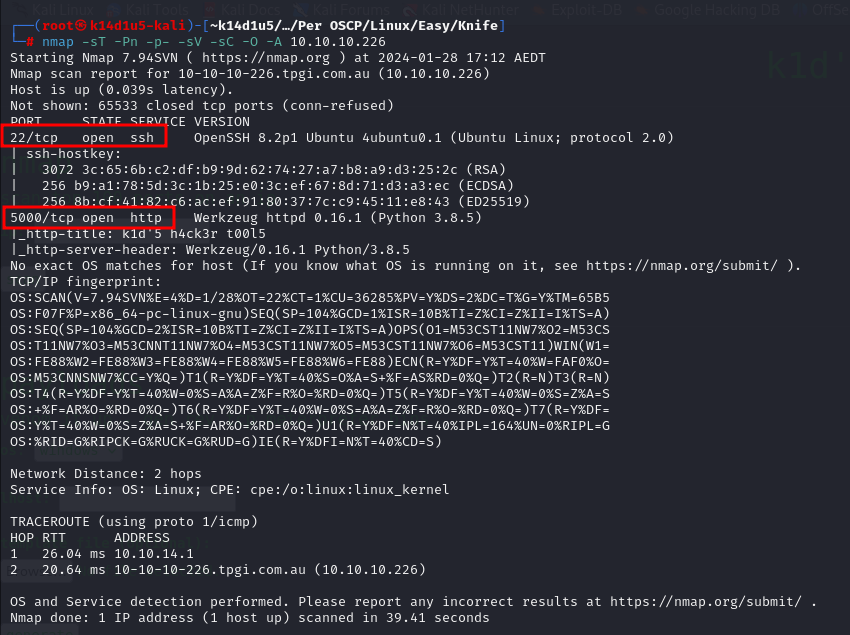


Figure 1 - nMap scan results

Open ports are 22 and 5000. So, the machine had SSH enabled and an application running on port 5000. NMap had recognize Linux as operative system, probably Ubuntu.

# **Initial foothold**

I accessed to the application running on port 5000 and it was:

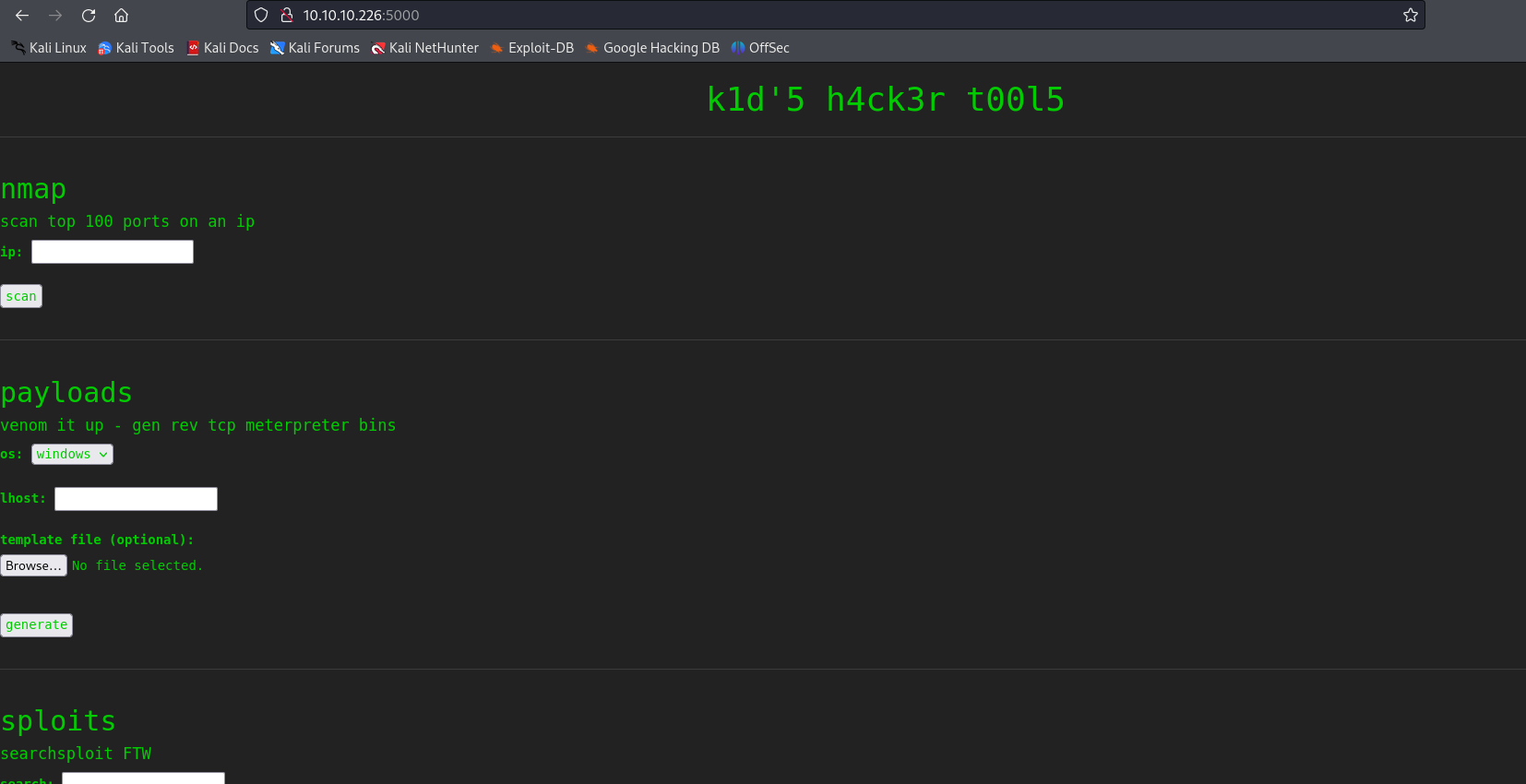


Figure 2 - Application running on port 5000

It provided some penetration test tools as **nMap**, **searchsploit** and **msfvenom**. I searched some possible known vulnerabilities affected these tools and I found [**CVE-2020-7384**](https://nvd.nist.gov/vuln/detail/CVE-2020-7384) that affect some **msfvenom** versions. **Rapid7's Metasploit msfvenom framework** handles APK files in a way that allows for a malicious user to craft and publish a file that would execute arbitrary commands on a victim's machine.

# **User flag**

I found a possible CVE to exploit application, so I tried to use its exploit. I generate a malicious APK file running the script **cve-2020-7384.sh**. I generate this file in the following way:

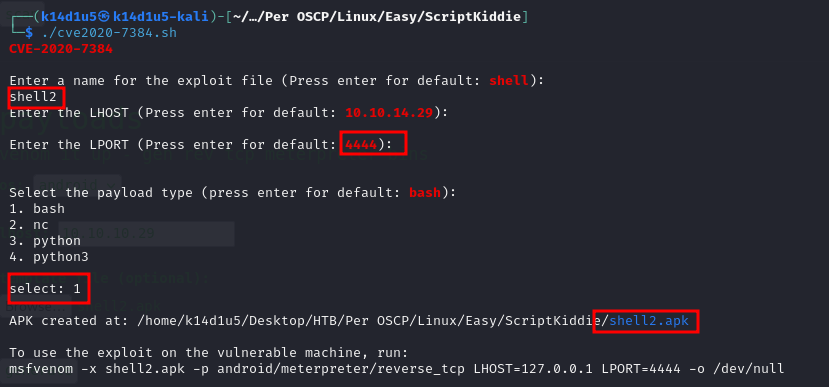


Figure 3 - Generating malicious APK file

At this point I used this malicious APK file in the application:

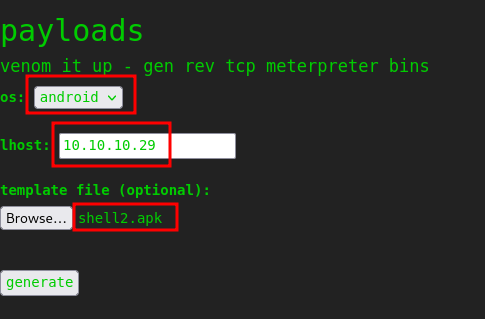


Figure 4 - Exploit

In this way, I obtained a reverse shell and retrieved the user flag:

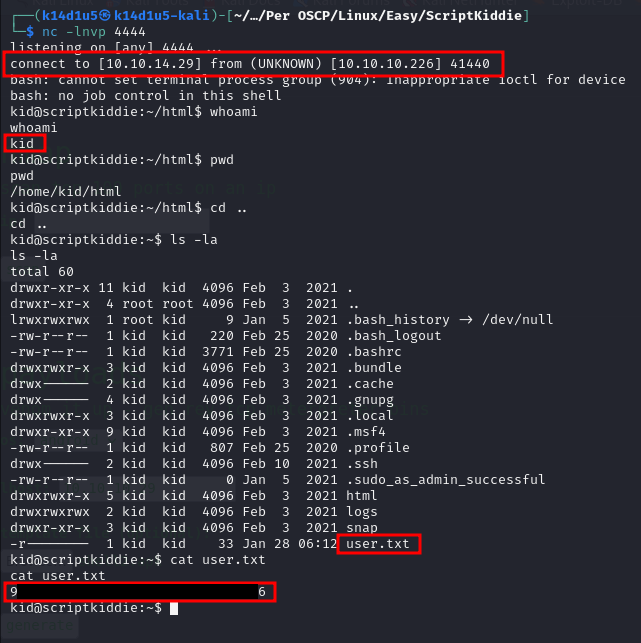


Figure 5 - User reverse shell and user flag

# **Privilege escalation**

To find a way to escalate my privileges, I uploaded **linpeas.sh** script on the target machine and I run it. Among its results, I found some possible interesting vulnerabilities:

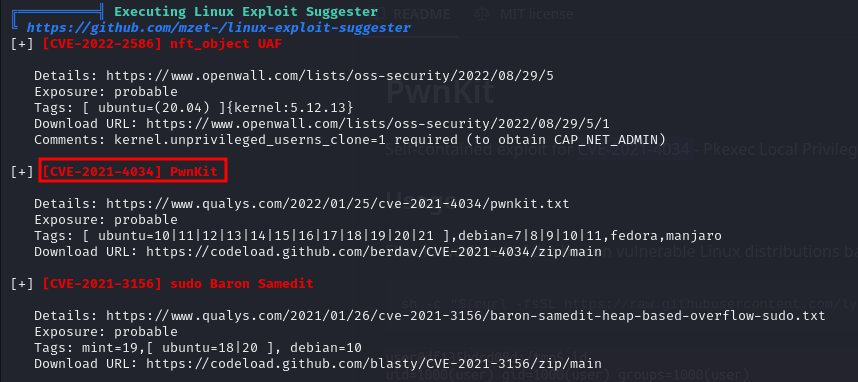


Figure 6 - Useful information for privilege escalation

So, I tried to download an exploit for this vulnerability, I uploaded on the target machine and run it. It worked and I obtained a shell as root. So, I retrieved the root flag:

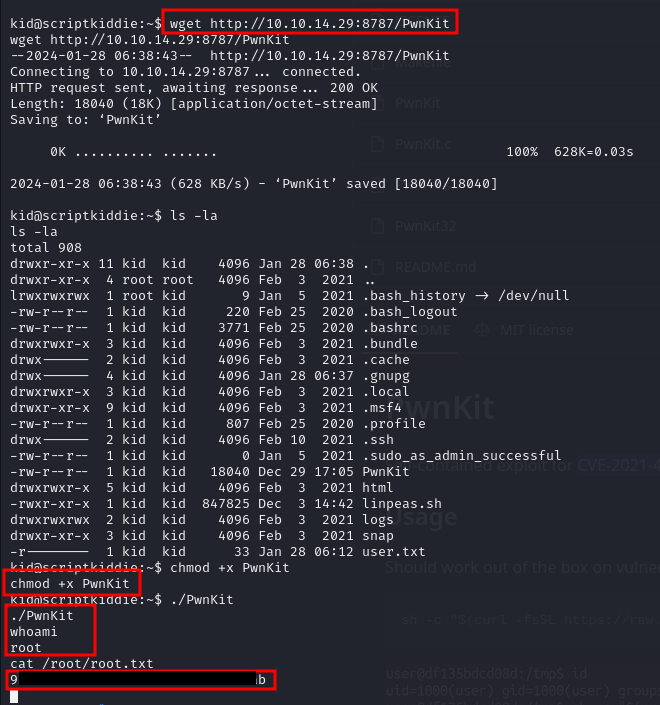


Figure - Root flag