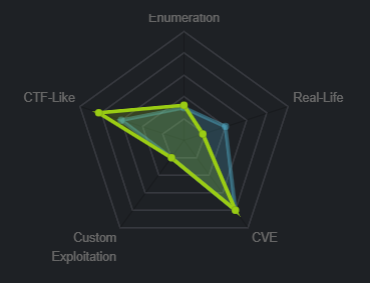
**HACKTHEBOX-SCRIPTKIDDIE**

Machine name : ScriptKiddie

Machine IP : 10.10.10.226

Difficulty : easy

Stats :



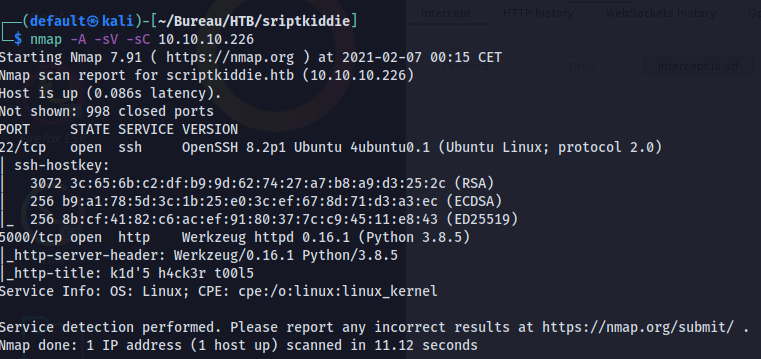
**0x1 : nmap scan**

« nmap -A -sV -sC 10.10.10.226 »

-A : Enables operating system and version detection

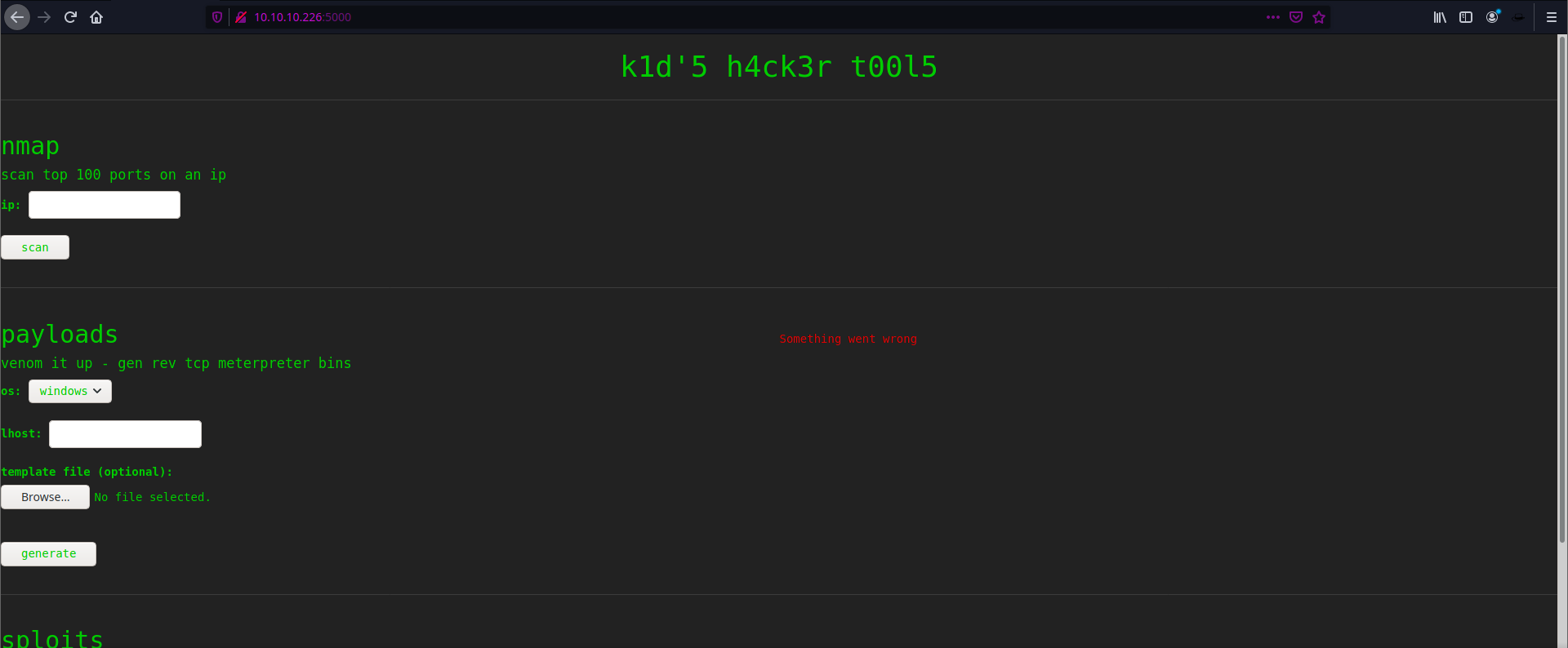
-sV : Tests open ports to determine which service is listening and its version

-sC : -sC: equivalent of --script = safe, intrusive (use default script of nmap)

****

**0x2 : FootHold**

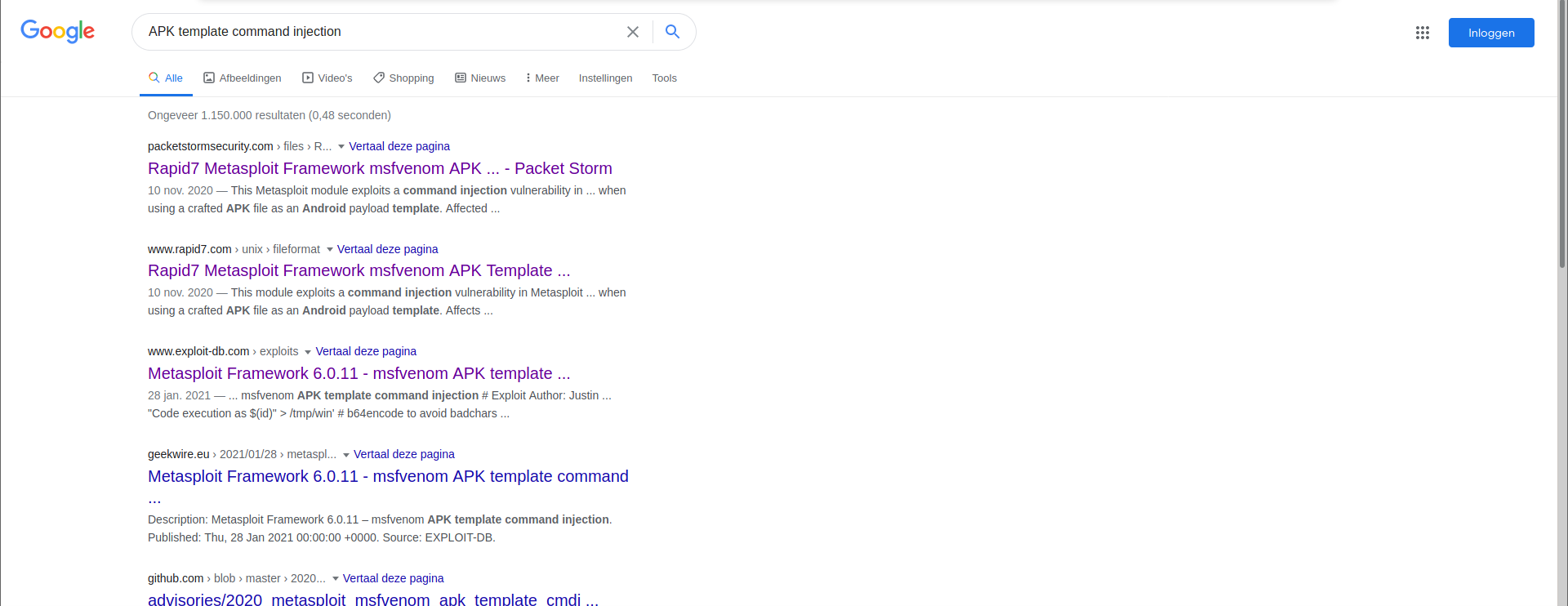
Let’s check web server



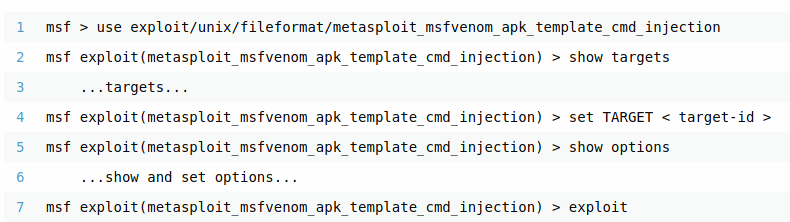
Find us a page that will bring together the kid's hacker tools

After looking for a while I found something interesting

I looked on google for a possible exploitation on the "payload" tool which seems to be metasploit, I found this exploitation on metasploit (apk template injection)

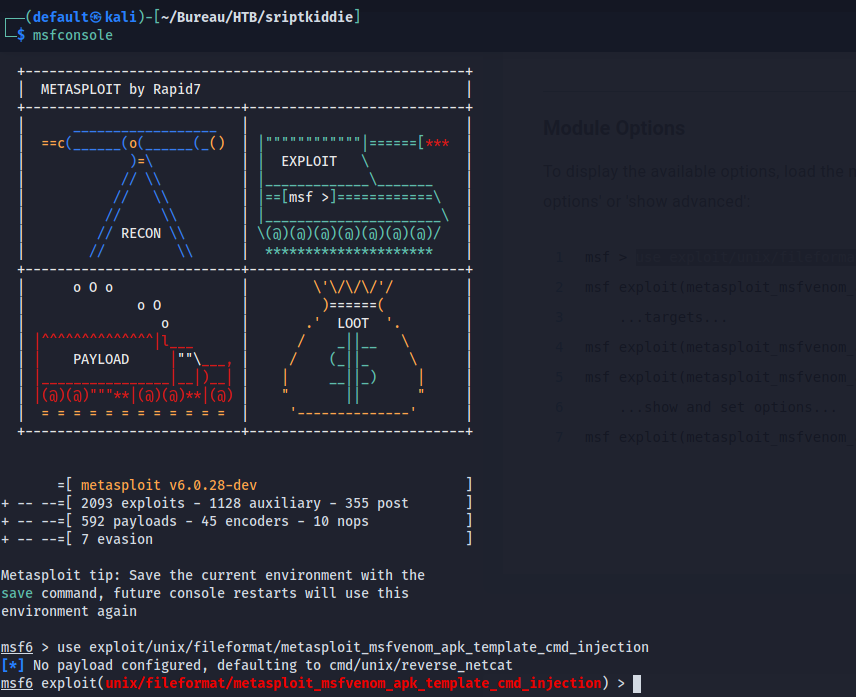


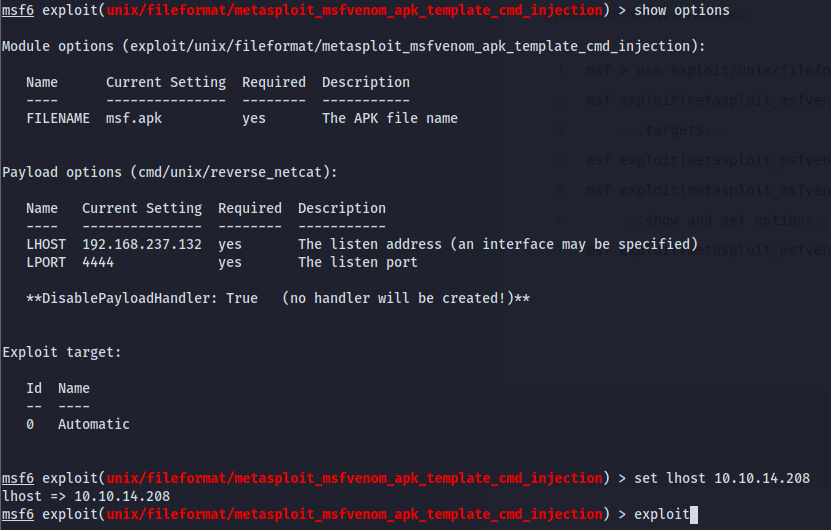
<https://www.rapid7.com/db/modules/exploit/unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection/>



**0x3 : Exploit**

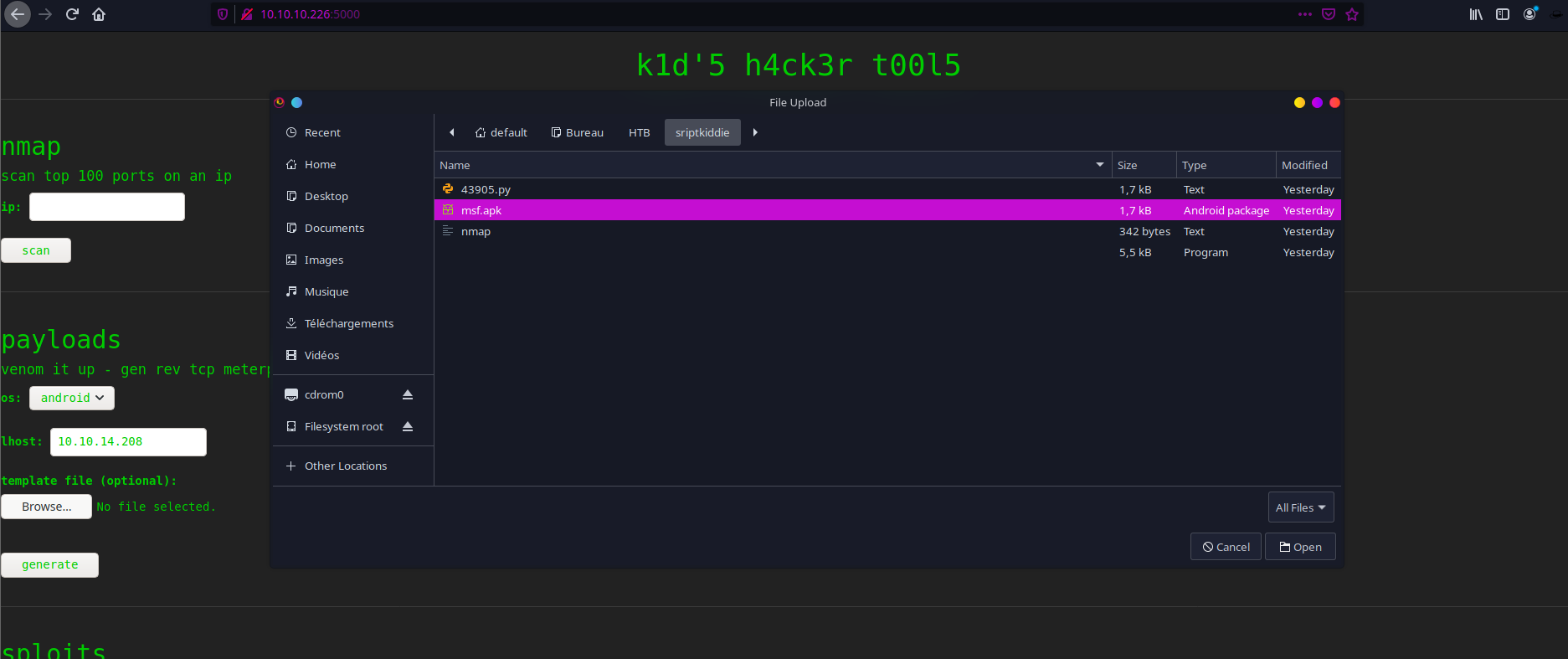
metasploit launch





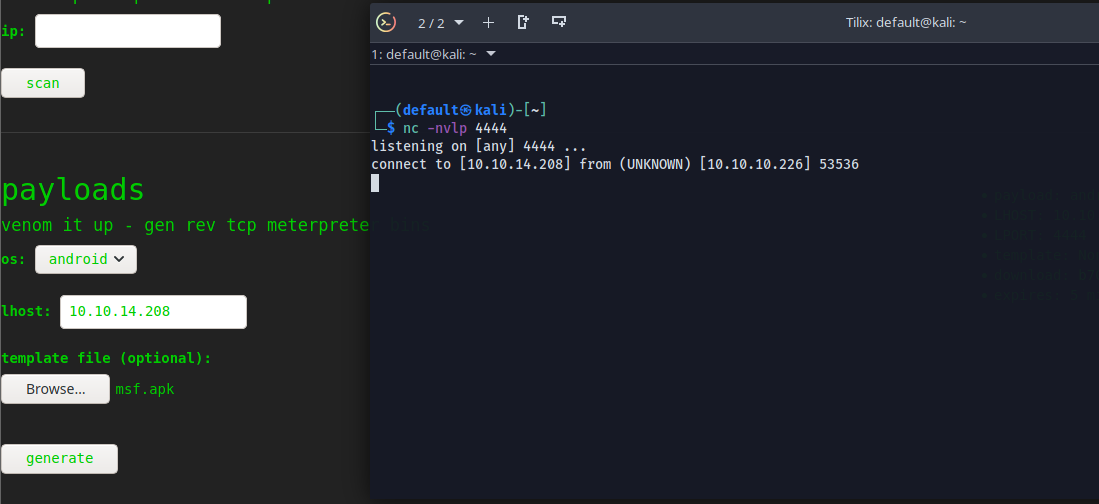




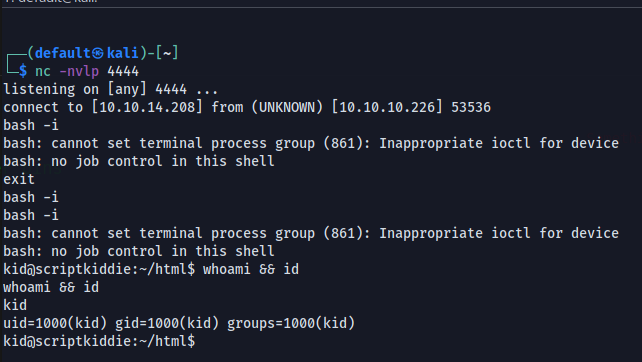


So let’s upload the apk template with our payload

Start your listening on the port put previously and generate from apk file



And we obit a shell on the machine as user "kid"

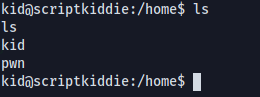


We got the user hash

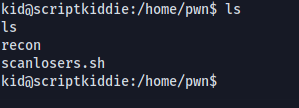


**0x4 : privilege escalation at user « pwn »**

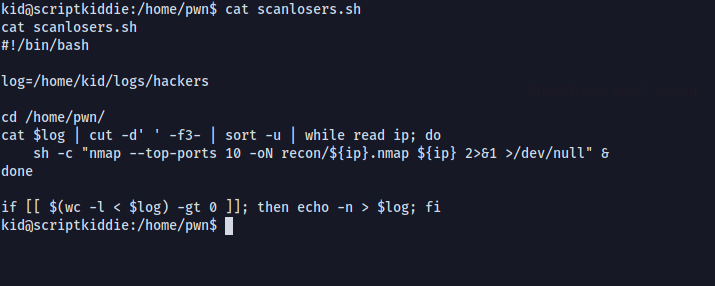
We can see that two user not present "kid" which is the user on which we are connecting and "pwn" another user



Let’s check the « pwn » current directory of user



We find a bash script let’s check it



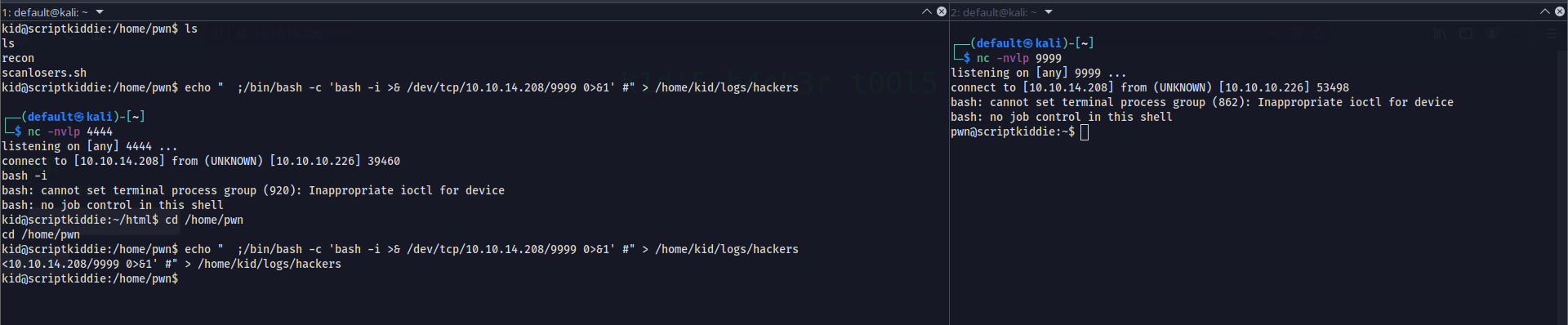
Ok we can try dragging a reverse shell in bash into / home / kid / logs / hackers to become the "pwn" user

Let’s go try this

We are going to use a reverse shell in bash but we are going to make some modification to it

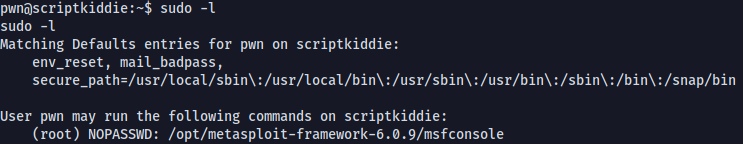
because we can see that the script redirects to the /dev/null redirection which will cancel our command execution and double space and ; to execute our command

We will put our reverse shell in "hackers" and set up our listening on the predefined port previously



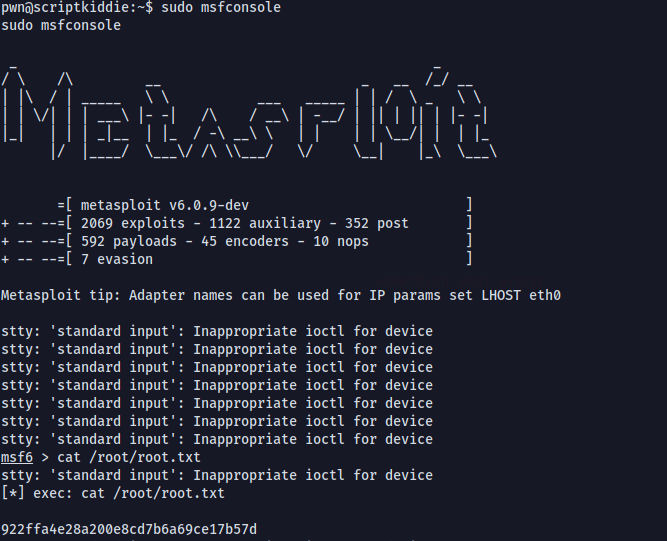
And BOOM !!! we have a reverse shell as user "pwn"

**0x5 : final privilege escalation**

We will look at the permissions of the user pwn

We can see that pwn has all the access on "/opt/metasploit-framework-6.0.9/msfconsole"

the rest is really easy we will run msfconsole as root to become the root of the machine



And GG we are root

ScriptKiddie has been pwned !