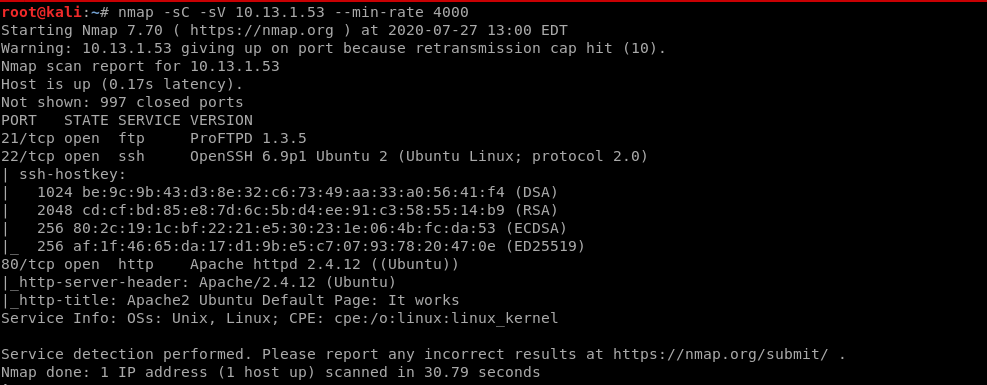
VPS1723(10.13.1.53)-GhostIA

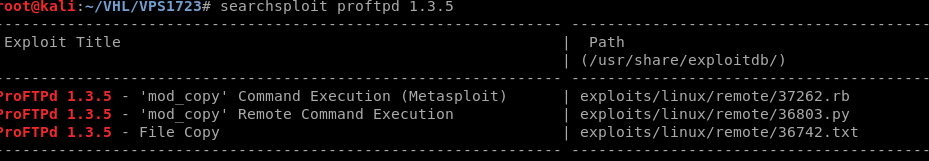
Sarah Ferenczi

Enumeration

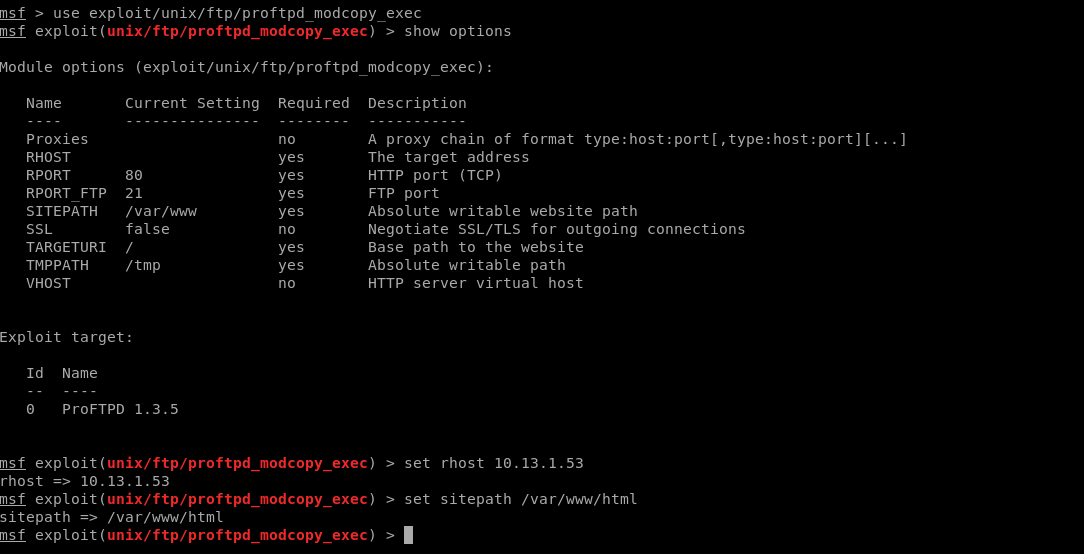


First, run an nmap scan. We immediately notice that port 80 is open. There is nothing on the site, however, with the ftp server, we can see that it may be connected to the apache server.

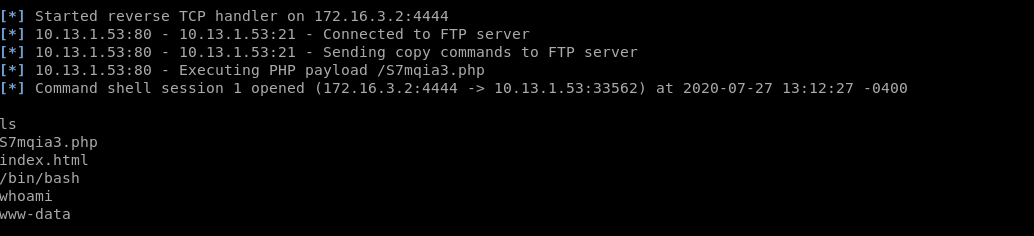
Exploitation



When searching for vulnerabilities, we can find that there is both a Metasploit module and a Python script. Let’s try the Metasploit module.

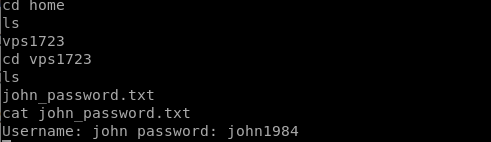


Let’s change some of the settings since the ftp server may be located within the /html file of apache.

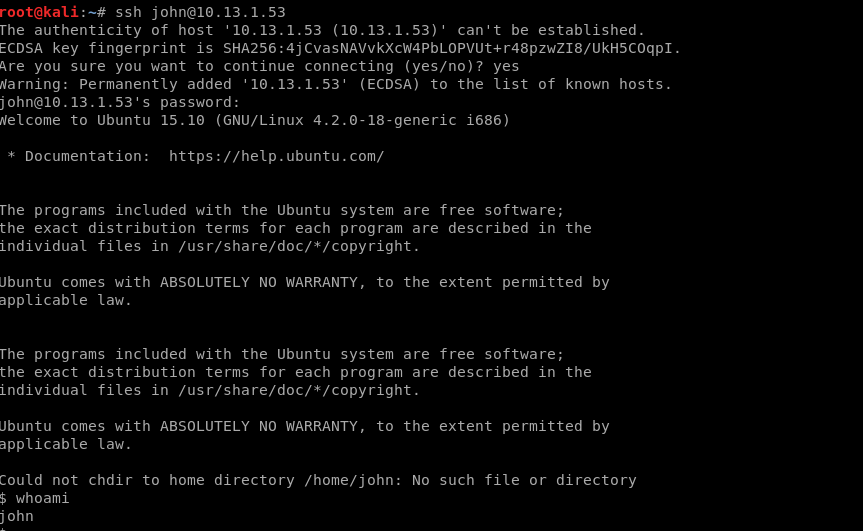


And then we exploit. Currently, we are a low privilege user, so let’s poke around to find some files.

Privilege Escalation



It’s important to type /bin/bash as well otherwise commands will not run. In /home/vps1723, we can find a username and password.

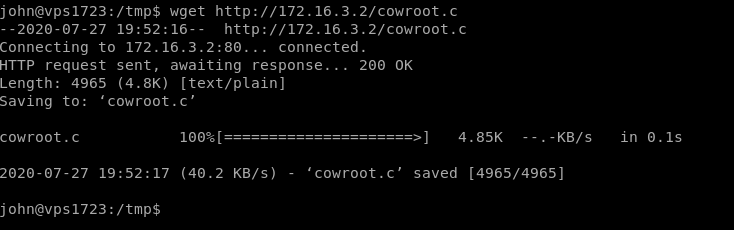


Let’s ssh into this user.

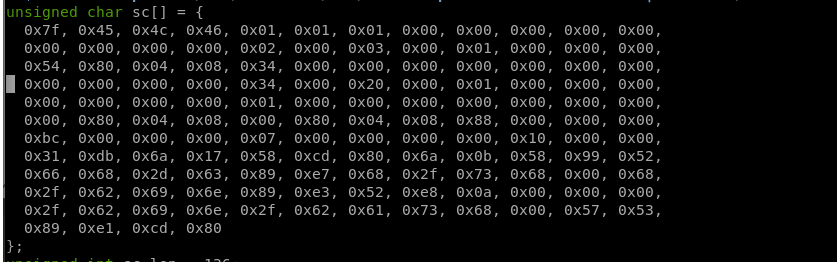


We can see that this version of linux is valid for the cowroot exploit.

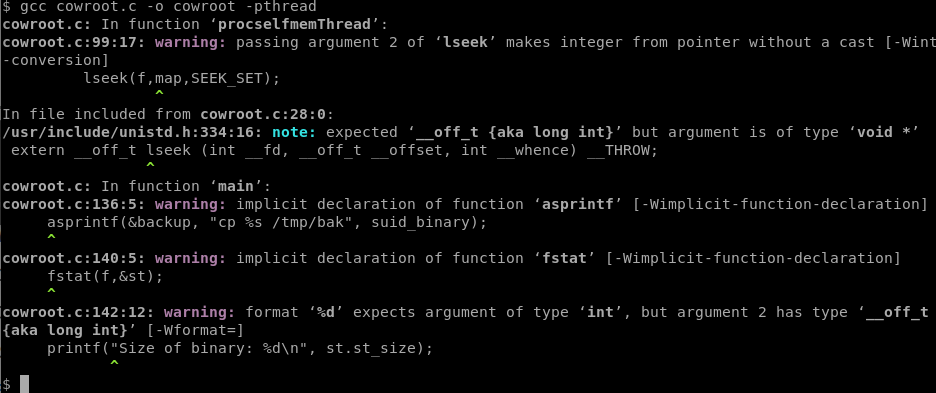


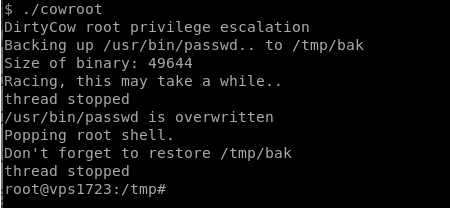


Let’s transfer the exploit onto this machine



Since we know this is a 32-bit machine, let’s uncomment the 32-bit code.





Let’s compile and run the code now.



Then we get out key: w76jooebu9p4yshd9q71