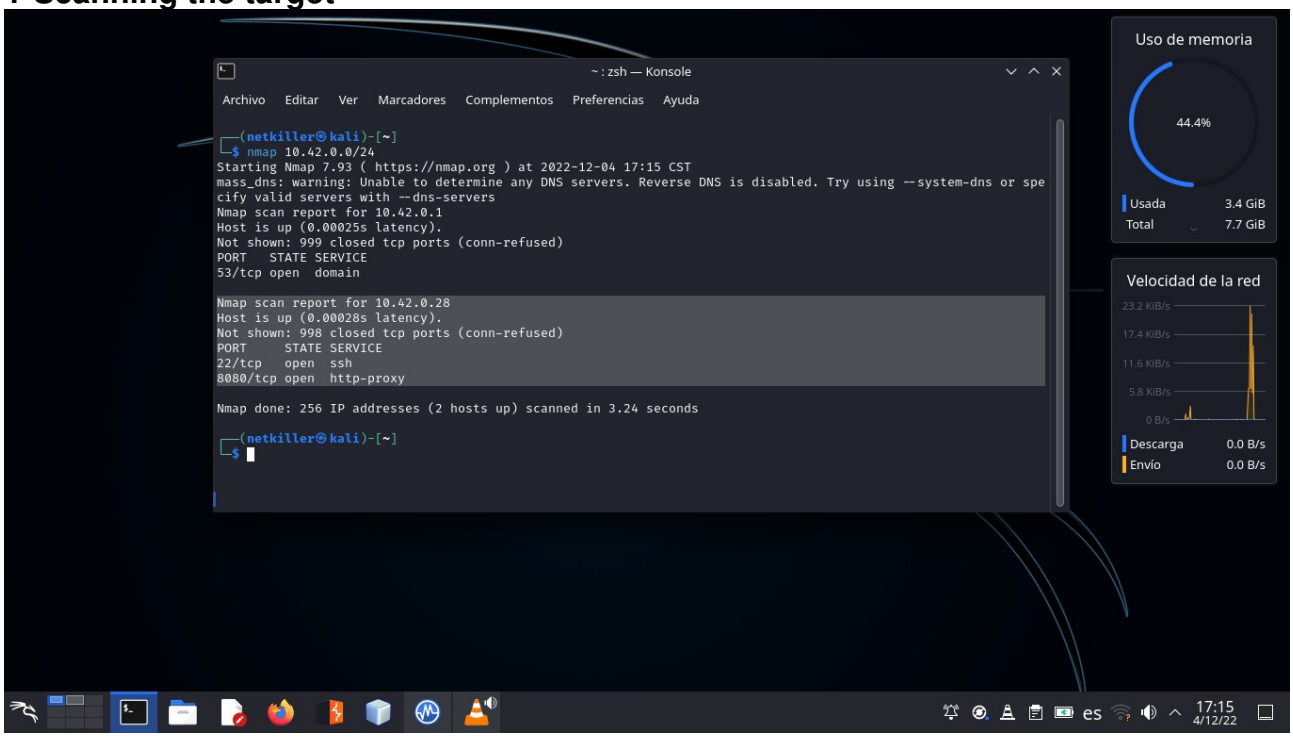
Thales Writeup

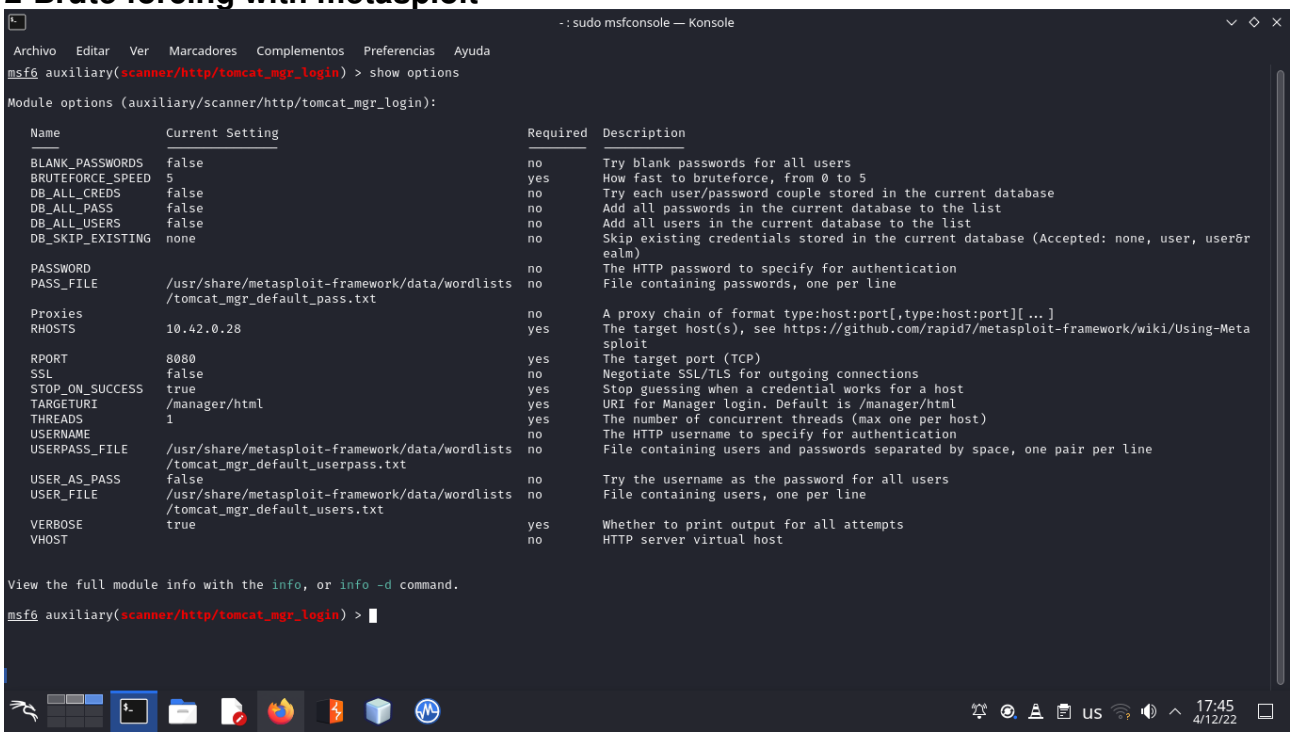
by: Netkiller

1-Scanning the target

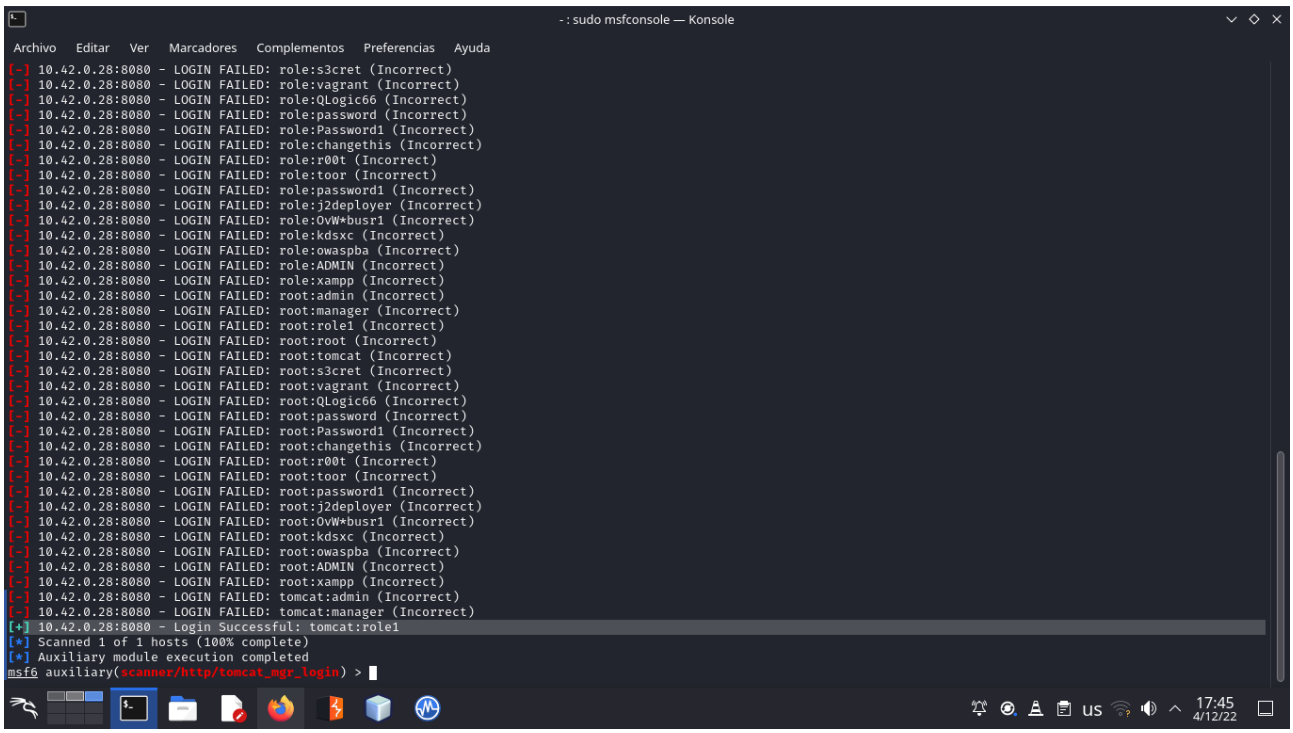


We found an open http-proxy
Exploring the web, we found that there is a tomcat server

2-Brute forcing with metasploit

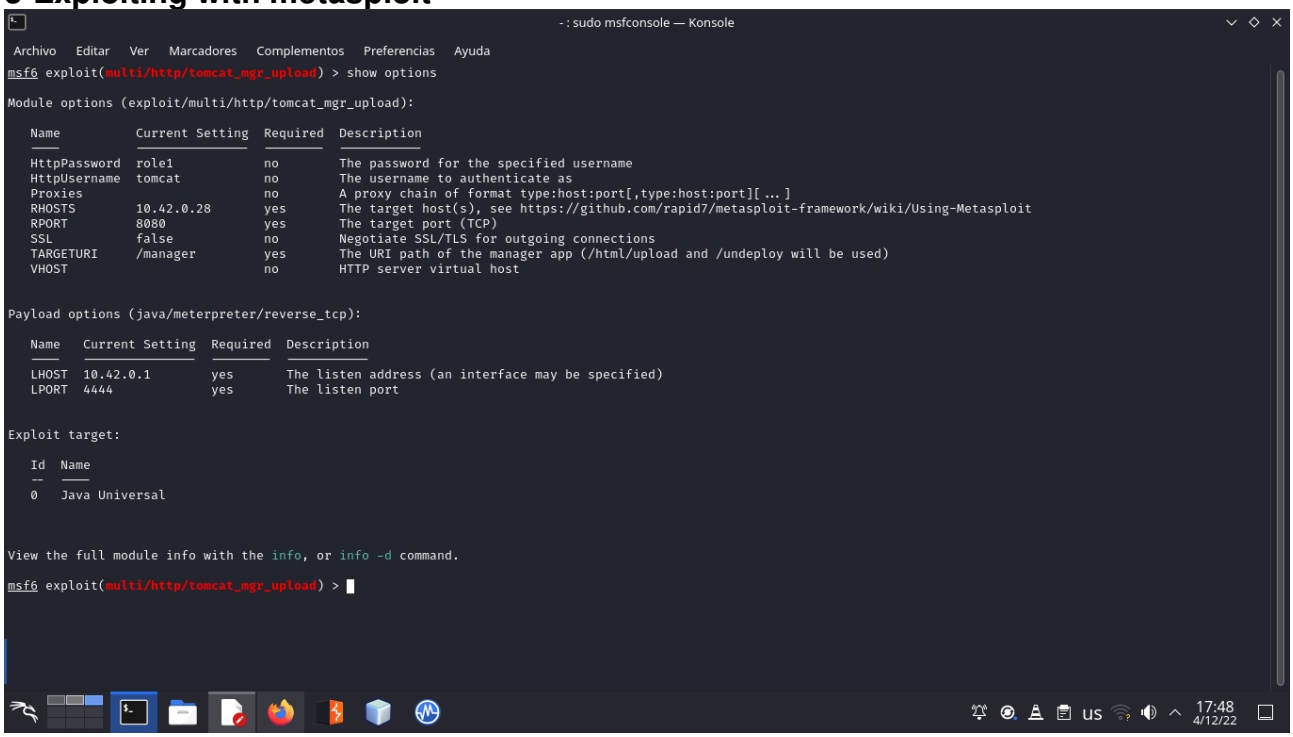


We can use the “scanner/http/tomcat_mgr_login” to search a default login credentials for the tomcat manager.

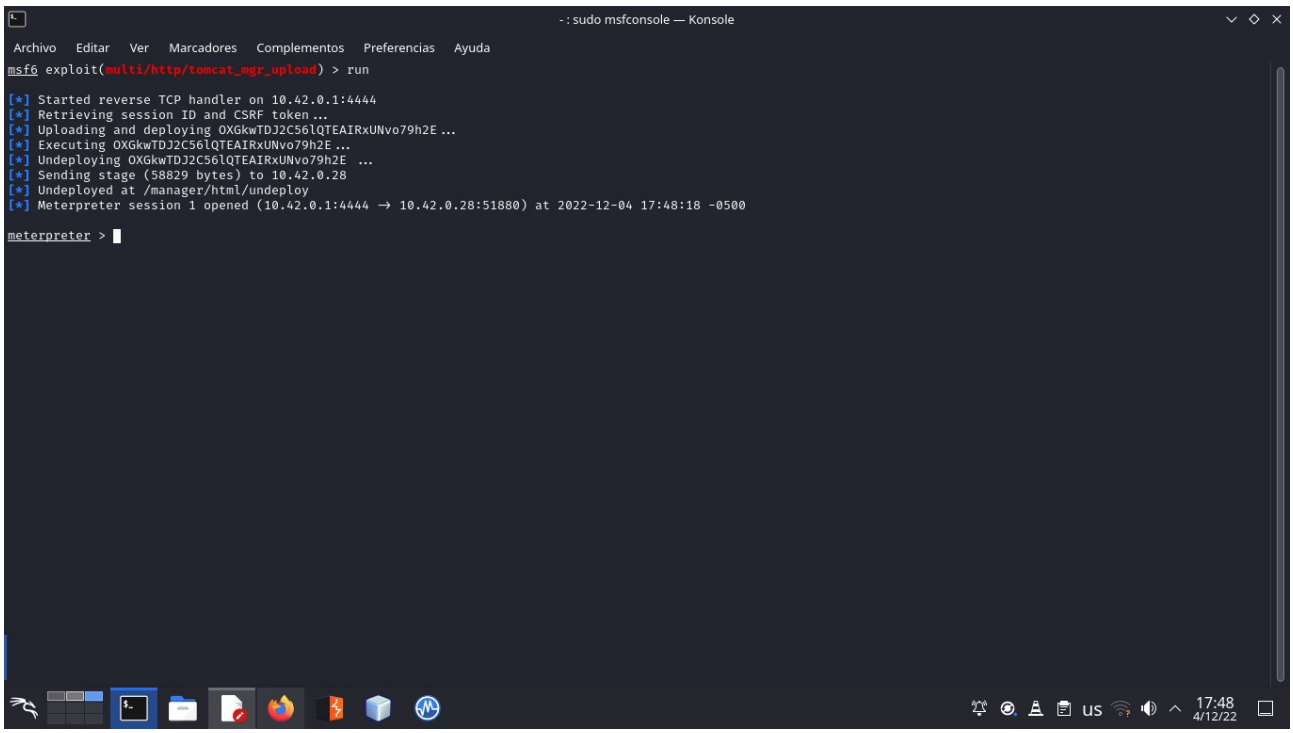


And there it is !

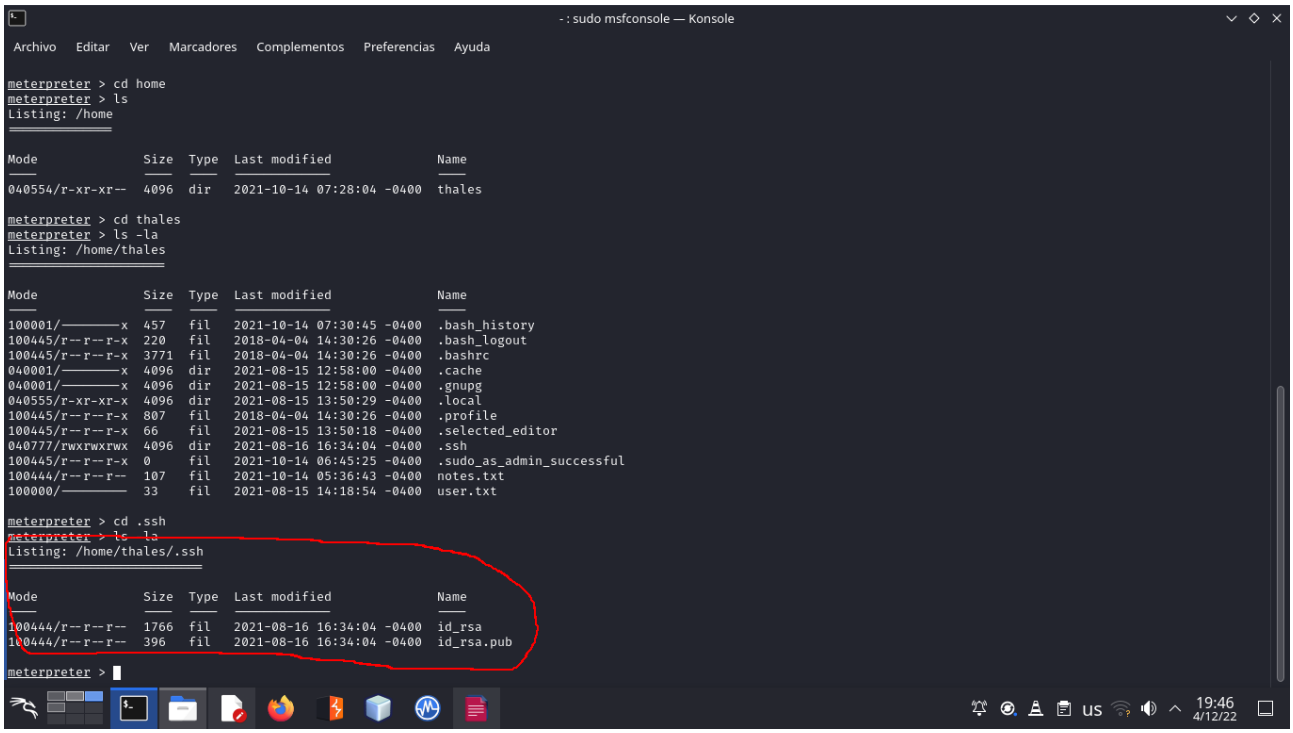
3-Exploiting with metasploit



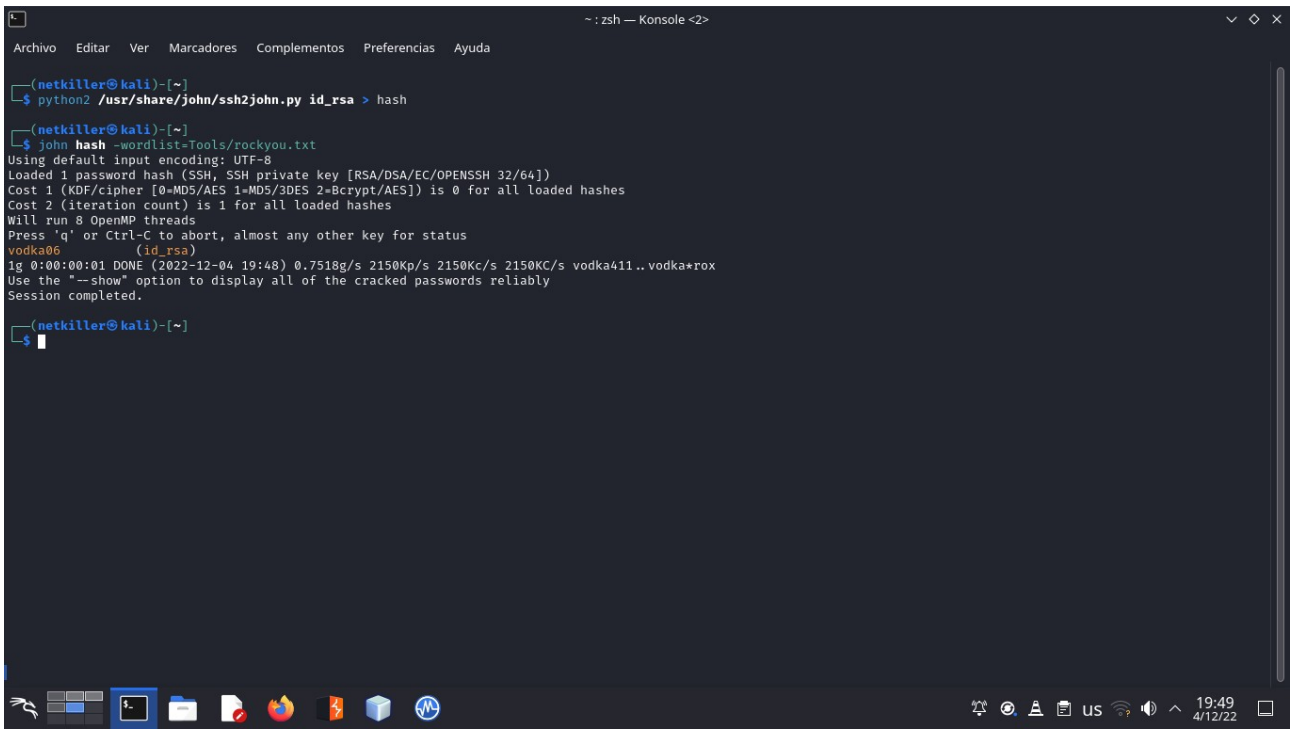
Now that we have a manager login, we can config the “/multi/http/tomcat_mgr_upload” in order to get a reverse (or bind) shell.



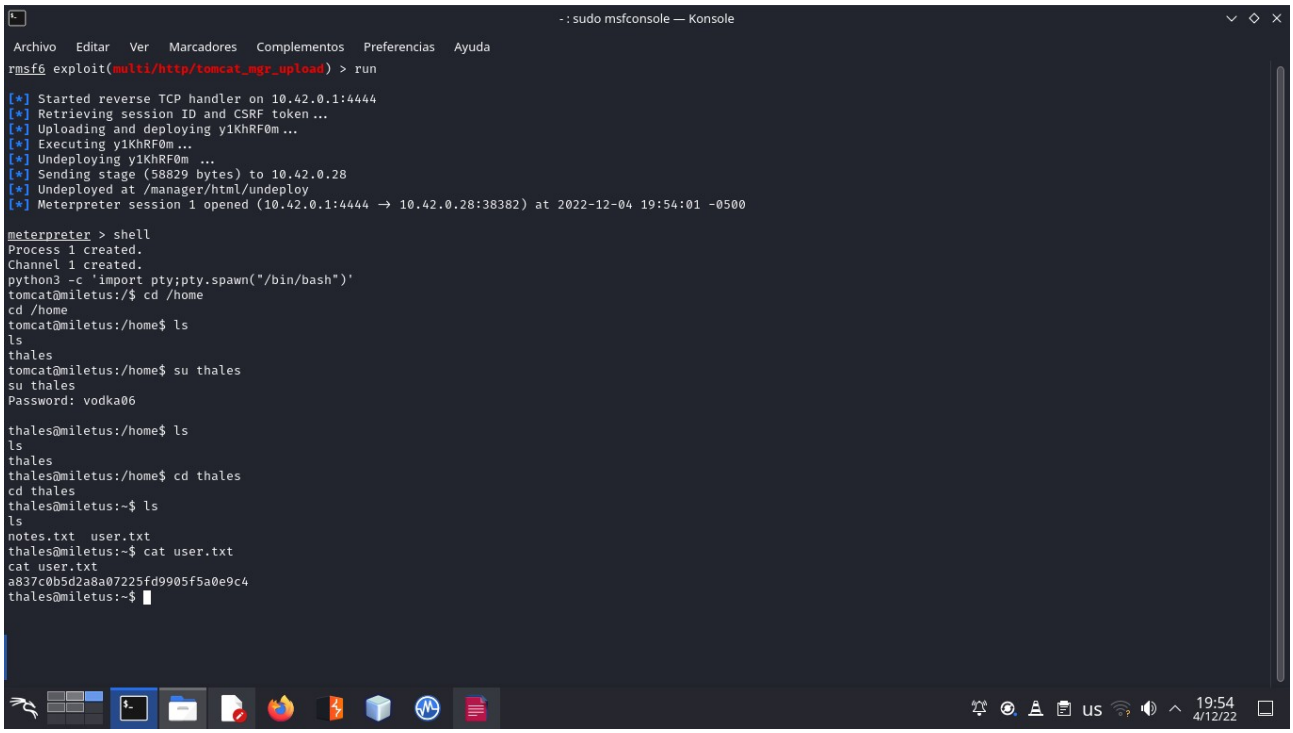
4-Privilege Escalation



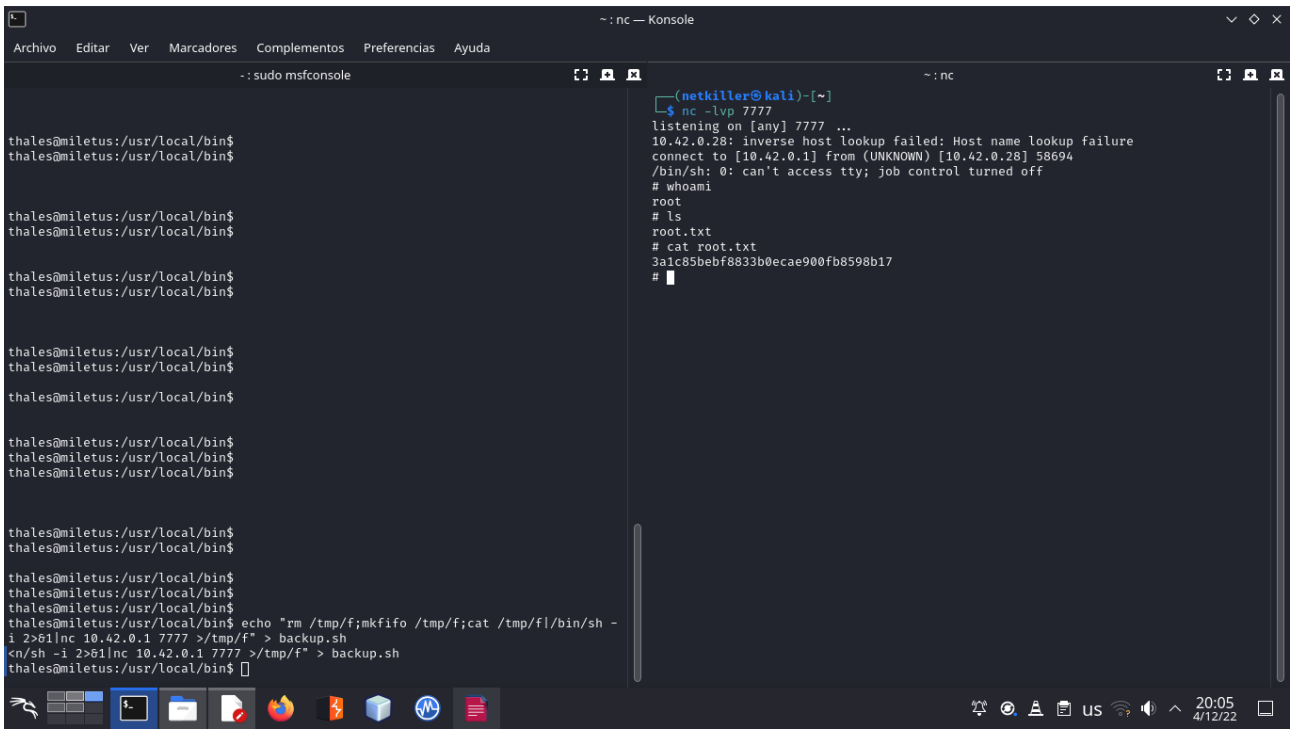
After a lot of time searching a misconfiguration or something like that, we found (there are always here) a .ssh folder with the ssh private key.



We can now turning it into a readable format for john (using ssh2john.py) and get the login using john and rockyou wordlist.



We have now acces to the user thales and can read the user.txt (first flag)



The note.txt file hint tell us that there are a script runhing by the root user (backup things) and, sorprise, we can write on it, now we can set a script for reverse shell with root privileges (we need to wait a few minutes for the server run the script).