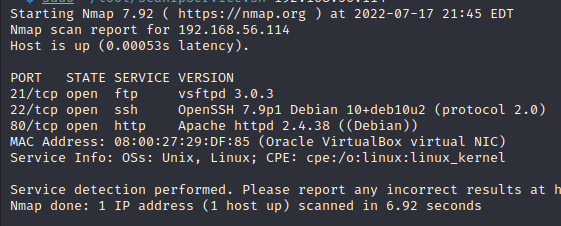
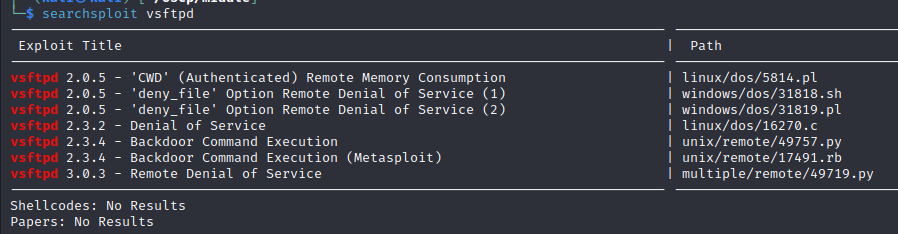
target: 192.168.56.114

host: 192.168.56.112

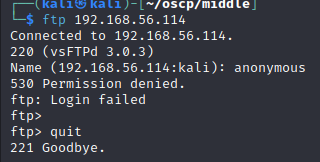
1. nmap -p- 192.168.56.114 --open scan the open port on the target, and then scan the server info on the special ports. nmap -p21,22,80 -sV 192.168.56.114



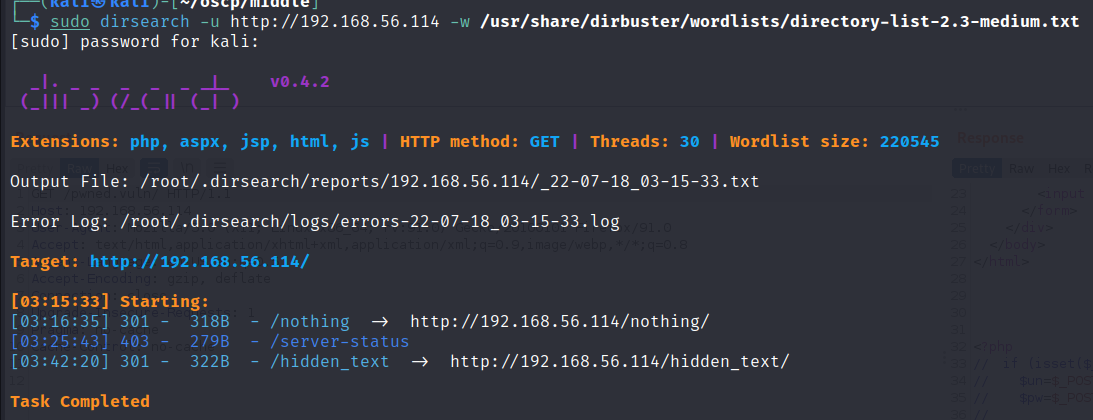
2.search the exploit info for vsftpd, no useful info.



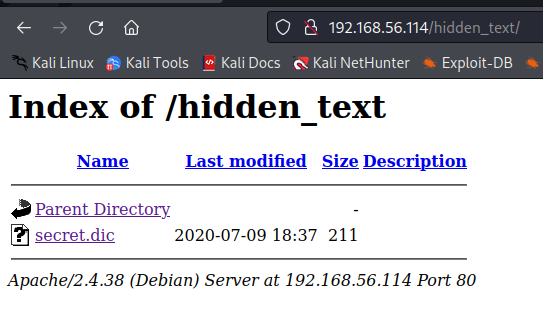
3.try to login ftp with anonymous, failed

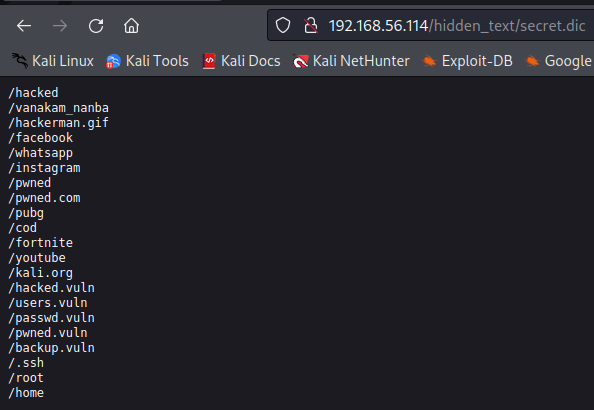


4.use dirsearch to scan the path of servers, found the hidden path /nothing and /hidden/text directory

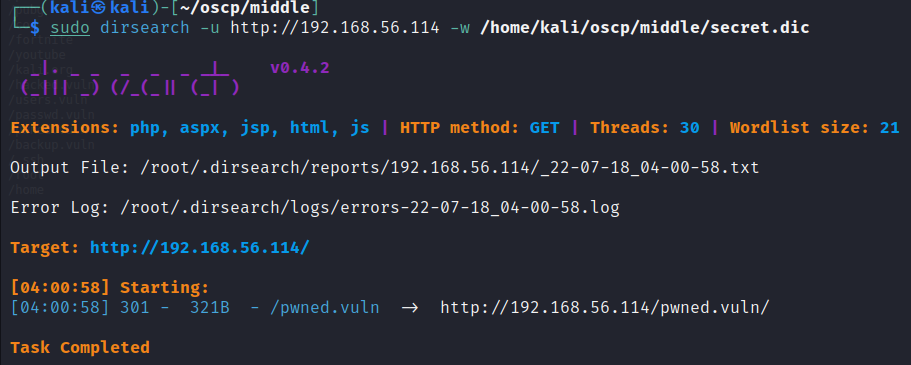


5.visit hidden page <http://192.168.56.114/hidden_text/>, found a secret.dic file, check the file’s content, it looks like a directory list

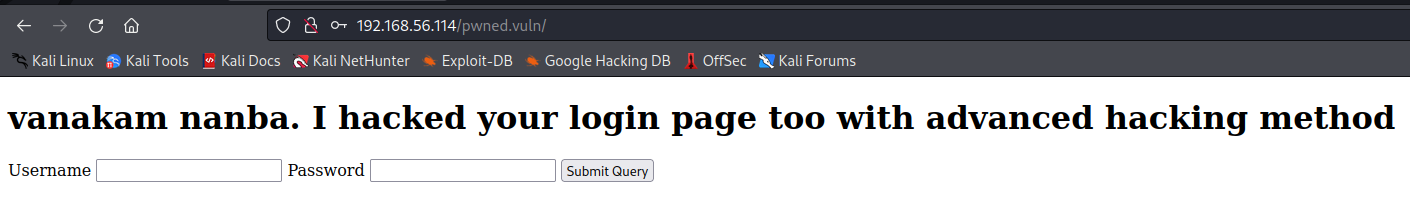




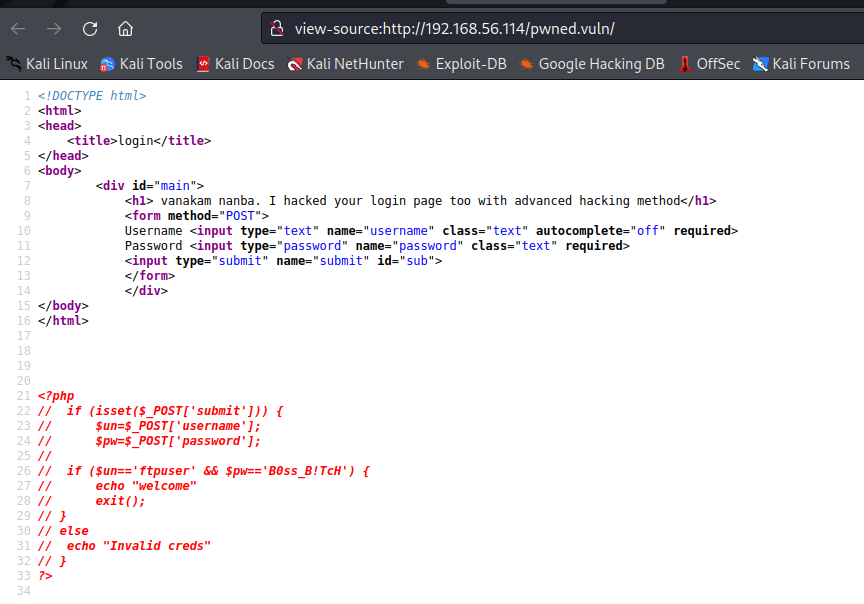
6.Use the dirsearch tool with secret.dic to scan the path of target, found a hidden directory



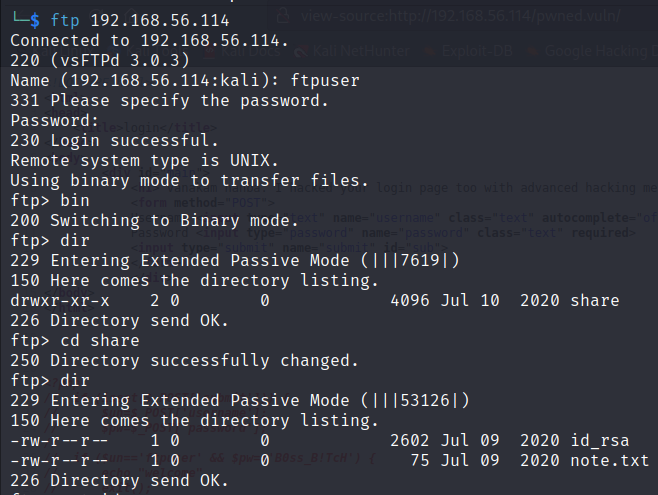
7.access the hidden directory, found a login page



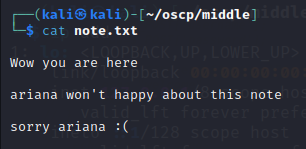
8.checking the source code of the page, found an account and password in comments , it looks like a ftp user



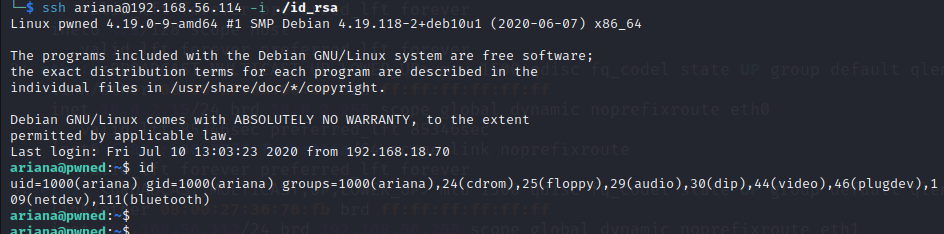
9.login the ftp server with found user and password, login success and found a file with file name similar to the private key. download all files to kali



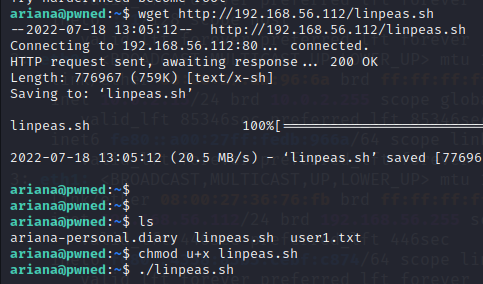
10.checking the content of note.txt, found a use name



11.try to use the user and private key to login the target server’s SSH server.login success with normal user



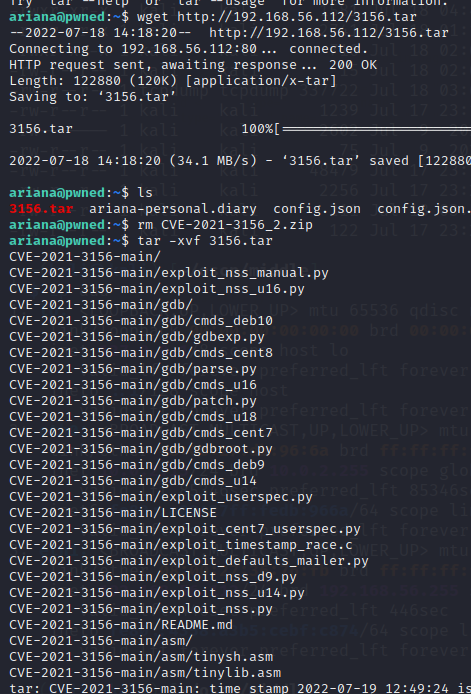
12.use wget to download the shell scrip linpeas.sh from kali host.Add execution permission and then execute the script



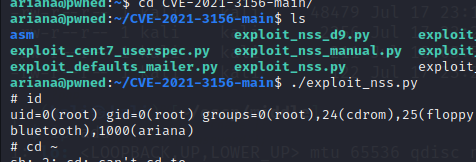
13.checking the result and found some exploits



14.download the exploit script from kali host,



15.execute the exploit script to get root privilege.



16.Get the flag file content

