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

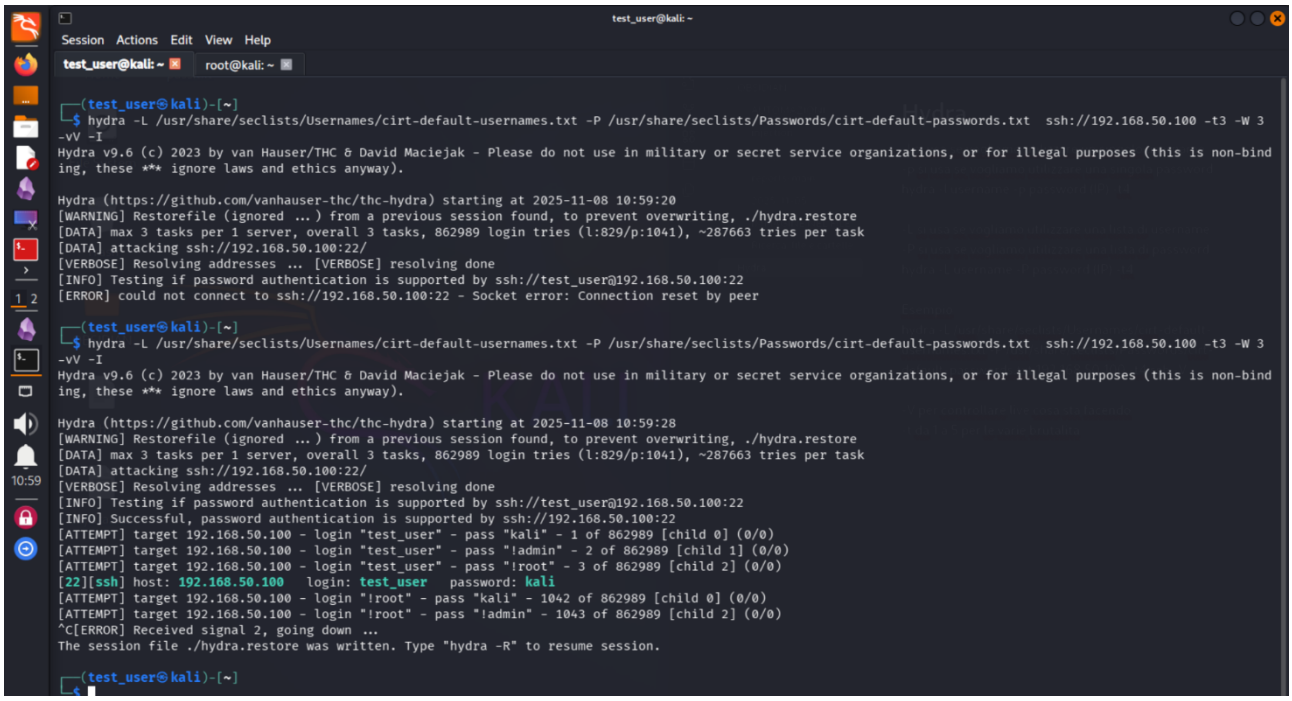
```
┌──(root㉿kali)-[~]
└─# adduser test_user
warn: The home directory `/home/test_user' already exists.  Not touching this directory.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
        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/seclist/Usernames/cirt-default-usernames.txt -P /usr/share/seclist/Passwords/cirt-default-passwords.txt ssh://192.168.50.100 -t3 -W3 -vV -I



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)