Esercitazione W14D4

Authentication Cracking - Hydra

Fabio Benevento - 08/02/2024

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 dell'autenticazione con Hydra
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

Implementazione

Fase 1 - Cracking SSH

Per questa esercitazione ho in primo luogo creato un nuovo utente con credenziali username: `test_user` e password: `testpass` mediante il comando `sudo adduser testuser`.
Ho avviato quindi il servizio con il comando `sudo service ssh start` e verificato la correttezza delle credenziali accedendo in maniera canonica con il comando ssh.

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password for kali:
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 []: utente_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' ...

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

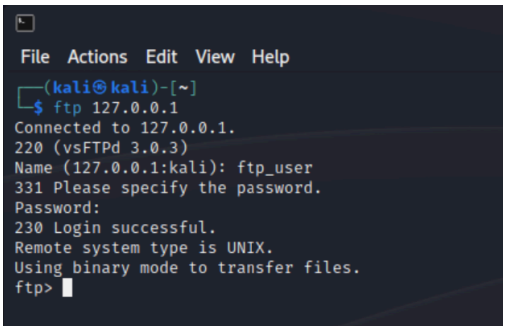
```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@127.0.0.1
test_user@127.0.0.1's password:
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64

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.
Last login: Tue Feb 13 09:21:06 2024 from 127.0.0.1
┌──(test_user㉿kali)-[~]
└─$
```

Ho lanciato quindi l'esecuzione di Hydra utilizzando come dizionario le password salvate nel file `xato-net-10-million-passwords.txt`. Dopo svariati tentativi Hydra è riuscito ad individuare la password impostata in precedenza come mostrato in figura.

```
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "9562876" - 5191 of 5189454 [child 2] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "5656" - 5192 of 5189454 [child 3] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "1945" - 5193 of 5189454 [child 0] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "159632" - 5194 of 5189454 [child 2] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "15151515" - 5195 of 5189454 [child 0] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "123456qw" - 5196 of 5189454 [child 2] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "1234567891" - 5197 of 5189454 [child 0] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "02051983" - 5198 of 5189454 [child 2] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "02041983" - 5199 of 5189454 [child 2] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "02031987" - 5200 of 5189454 [child 1] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "02021989" - 5201 of 5189454 [child 1] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "z1×2c3v4" - 5202 of 5189454 [child 1] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "xing" - 5203 of 5189454 [child 1] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "vSjasnel12" - 5204 of 5189454 [child 1] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "twenty" - 5205 of 5189454 [child 3] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "toolman" - 5206 of 5189454 [child 3] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "thing" - 5207 of 5189454 [child 3] (0/0)
[ATTEMPT] target 192.168.40.100 - login "test_user" - pass "testpass" - 5208 of 5189454 [child 0] (0/0)
[22][ssh] host: 192.168.40.100   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 2024-02-13 14:00:10
```

Fase 2 - Cracking FTP

Per questa esercitazione ho in primo luogo creato un nuovo utente con credenziali username: `ftp_user` e password: `peanut` mediante il comando `sudo adduser ftp_user`.
Ho avviato quindi il servizio con il comando `sudo service vsftp start` e verificato la correttezza delle credenziali accedendo in maniera canonica con il comando `ftp`.



Ho lanciato quindi l'esecuzione di Hydra utilizzando come dizionario le password salvate nel file `xato-net-10-million-passwords.txt`. Dopo svariati tentativi Hydra è riuscito ad individuare la password impostata in precedenza come mostrato in figura.