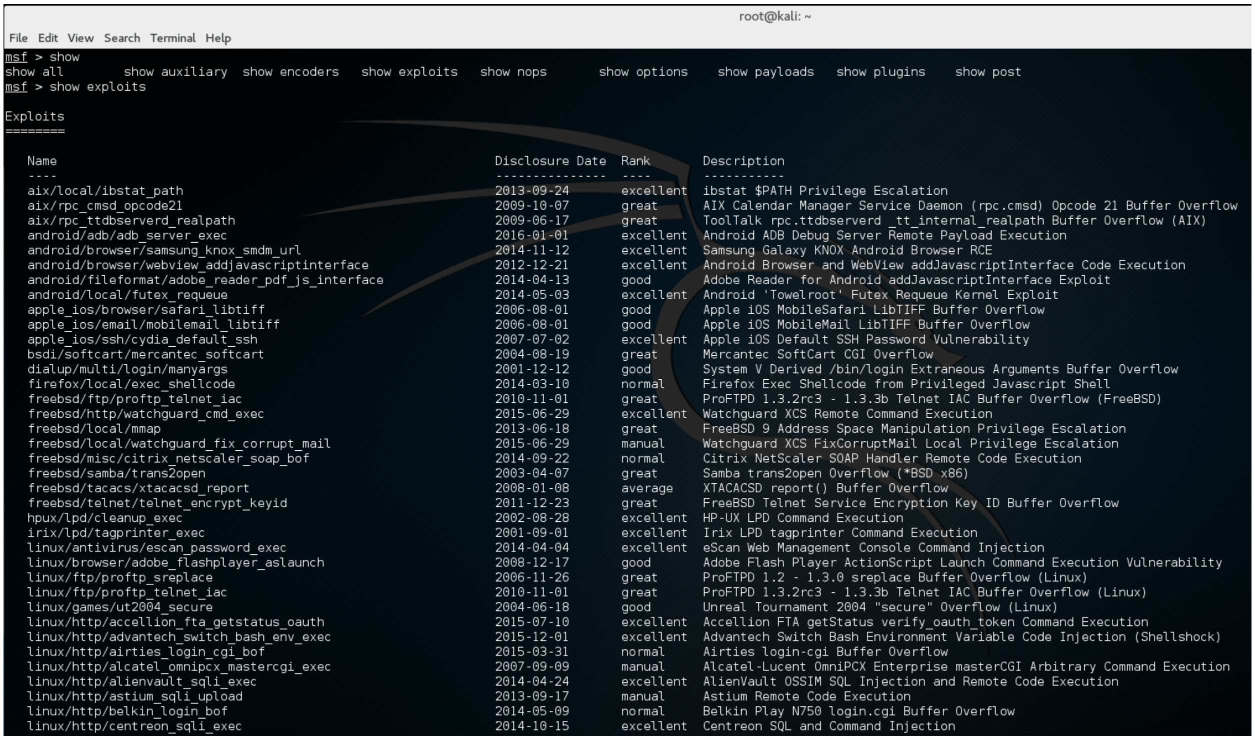
Using Exploits in Metasploit



```
msf > show
show all        show auxiliary  show encoders   show exploits   show nops       show options    show payloads   show plugins    show post
msf > show exploits

Exploits
========

   Name                                                           Disclosure Date  Rank       Description
   ----                                                           ---------------  ----       -----------
   aix/local/ibstat_path                                          2013-09-24       excellent  ibstat $PATH Privilege Escalation
   aix/rpc_cmsd_opcode21                                          2009-10-07       great      AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
   aix/rpc_ttdbserverd_realpath                                   2009-06-17       great      ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
   android/adb/adb_server_exec                                    2016-01-01       excellent  Android ADB Debug Server Remote Payload Execution
   android/browser/samsung_knox_smdm_url                          2014-11-12       excellent  Samsung Galaxy KNOX Android Browser RCE
   android/browser/webview_addjavascriptinterface                 2012-12-21       excellent  Android Browser and WebView addJavascriptInterface Code Execution
   android/fileformat/adobe_reader_pdf_js_interface               2014-04-13       good       Adobe Reader for Android addJavascriptInterface Exploit
   android/local/futex_requeue                                    2014-05-03       excellent  Android 'Towelroot' Futex Requeue Kernel Exploit
   apple_ios/browser/safari_libtiff                               2006-08-01       good       Apple iOS MobileSafari LibTIFF Buffer Overflow
   apple_ios/email/mobilemail_libtiff                             2006-08-01       good       Apple iOS MobileMail LibTIFF Buffer Overflow
   apple_ios/ssh/cydia_default_ssh                                2007-07-02       excellent  Apple iOS Default SSH Password Vulnerability
   bsdi/softcart/mercantec_softcart                               2004-08-19       great      Mercantec SoftCart CGI Overflow
   dialup/multi/login/manyargs                                    2001-12-12       good       System V Derived /bin/login Extraneous Arguments Buffer Overflow
   firefox/local/exec_shellcode                                   2014-03-10       normal     Firefox Exec Shellcode from Privileged Javascript Shell
   freebsd/ftp/proftp_telnet_iac                                  2010-11-01       great      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   freebsd/http/watchguard_cmd_exec                               2015-06-29       excellent  Watchguard XCS Remote Command Execution
   freebsd/local/mmap                                             2013-06-18       great      FreeBSD 9 Address Space Manipulation Privilege Escalation
   freebsd/local/watchguard_fix_corrupt_mail                      2015-06-29       manual     Watchguard XCS FixCorruptMail Local Privilege Escalation
   freebsd/misc/citrix_netscaler_soap_bof                         2014-09-22       normal     Citrix NetScaler SOAP Handler Remote Code Execution
   freebsd/samba/trans2open                                       2003-04-07       great      Samba trans2open Overflow (*BSD x86)
   freebsd/tacacs/xtacacsd_report                                 2008-01-08       average    XTACACSD report() Buffer Overflow
   freebsd/telnet/telnet_encrypt_keyid                            2011-12-23       great      FreeBSD Telnet Service Encryption Key ID Buffer Overflow
   hpux/lpd/cleanup_exec                                          2002-08-28       excellent  HP-UX LPD Command Execution
   irix/lpd/tagprinter_exec                                       2001-09-01       excellent  Irix LPD tagprinter Command Execution
   linux/antivirus/escan_password_exec                            2014-04-04       excellent  eScan Web Management Console Command Injection
   linux/browser/adobe_flashplayer_aslaunch                       2008-12-17       good       Adobe Flash Player ActionScript Launch Command Execution Vulnerability
   linux/ftp/proftp_sreplace                                      2006-11-26       great      ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   linux/ftp/proftp_telnet_iac                                    2010-11-01       great      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   linux/games/ut2004_secure                                      2004-06-18       good       Unreal Tournament 2004 "secure" Overflow (Linux)
   linux/http/accellion_fta_getstatus_oauth                       2015-07-10       excellent  Accellion FTA getStatus verify_oauth_token Command Execution
   linux/http/advantech_switch_bash_env_exec                      2015-12-01       excellent  Advantech Switch Bash Environment Variable Code Injection (Shellshock)
   linux/http/airties_login_cgi_bof                               2015-03-31       normal     Airties login-cgi Buffer Overflow
   linux/http/alcatel_omnipcx_mastercgi_exec                      2007-09-09       manual     Alcatel-Lucent OmniPCX Enterprise masterCGI Arbitrary Command Execution
   linux/http/alienvault_sqli_exec                                2014-04-24       excellent  AlienVault OSSIM SQL Injection and Remote Code Execution
   linux/http/astium_sqli_upload                                  2013-09-17       manual     Astium Remote Code Execution
   linux/http/belkin_login_bof                                    2014-05-09       normal     Belkin Play N750 login.cgi Buffer Overflow
   linux/http/centreon_sqli_exec                                  2014-10-15       excellent  Centreon SQL and Command Injection
```

SHOW EXPLOITS command in MSFCONSOLE | Metasploit Unleashed

Selecting an exploit in Metasploit adds the **exploit** and **check** commands to msfconsole.

```
msf > use  exploit/windows/smb/ms09_050_smb2_negotiate_func_index
msf exploit(ms09_050_smb2_negotiate_func_index) > help
...snip...
Exploit Commands
================

    Command       Description
    -------       -----------
    check         Check to see if a target is vulnerable
    exploit       Launch an exploit attempt
    pry           Open a Pry session on the current module
    rcheck        Reloads the module and checks if the target is vulnerable
    reload        Just reloads the module
    rerun         Alias for rexploit
    rexploit      Reloads the module and launches an exploit attempt
    run           Alias for exploit

msf exploit(ms09_050_smb2_negotiate_func_index) >
```

show

Using an exploit also adds more options to the **show** command.

MSF Exploit Targets

```
msf exploit(ms09_050_smb2_negotiate_func_index) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows Vista SP1/SP2 and Server 2008 (x86)
```

MSF Exploit Payloads

```
msf exploit(ms09_050_smb2_negotiate_func_index) > show payloads

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

   Name                              Disclosure Date  Rank    Description
   ----                              ---------------  ----    -----------
   generic/custom                                     normal  Custom Payload
   generic/debug_trap                                 normal  Generic x86
Debug Trap
   generic/shell_bind_tcp                             normal  Generic Command
Shell, Bind TCP Inline
   generic/shell_reverse_tcp                          normal  Generic Command
Shell, Reverse TCP Inline
   generic/tight_loop                                 normal  Generic x86
Tight Loop
   windows/adduser                                    normal  Windows Execute
net user /ADD
...snip...
```

MSF Exploit Options

```
msf exploit(ms09_050_smb2_negotiate_func_index) > show options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  445              yes       The target port (TCP)
   WAIT   180              yes       The number of seconds to wait for the
attack to complete.


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista SP1/SP2 and Server 2008 (x86)
```

Advanced

```
msf exploit(ms09_050_smb2_negotiate_func_index) > show advanced

Module advanced options
(exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name                     Current Setting    Required  Description
   ----                     ---------------    --------  -----------
   CHOST                                       no        The local client
address
   CPORT                                       no        The local client port
   ConnectTimeout           10                 yes       Maximum number of
seconds to establish a TCP connection
   ContextInformationFile                      no        The information file
that contains context information
   DisablePayloadHandler    false              no        Disable the handler
code for the selected payload
   EnableContextEncoding    false              no        Use transient context
when encoding payloads
...snip...
```

Evasion

```
msf exploit(ms09_050_smb2_negotiate_func_index) > show evasion
Module evasion options:

   Name                            Current Setting  Required  Description
   ----                            ---------------  --------  -----------
   SMB::obscure_trans_pipe_level   0                yes       Obscure PIPE
string in TransNamedPipe (level 0-3)
   SMB::pad_data_level             0                yes       Place extra
padding between headers and data (level 0-3)
   SMB::pad_file_level             0                yes       Obscure path
names used in open/create (level 0-3)
   SMB::pipe_evasion               false            yes       Enable segmented
read/writes for SMB Pipes
   SMB::pipe_read_max_size         1024             yes       Maximum buffer
size for pipe reads
   SMB::pipe_read_min_size         1                yes       Minimum buffer
size for pipe reads
   SMB::pipe_write_max_size        1024             yes       Maximum buffer
size for pipe writes
   SMB::pipe_write_min_size        1                yes       Minimum buffer
size for pipe writes
   TCP::max_send_size              0                no        Maxiumum tcp
segment size.  (0 = disable)
   TCP::send_delay                 0                no        Delays inserted
before every send.  (0 = disable)
```