Using Exploits a11y.text Using Exploits 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 a11y.text show Using an exploit also adds more options to the show command. MSF Exploit Targets a11y.text 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) MSFÂ ExploitÂ Payloads a11y.text
MSFÂ ExploitÂ 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... MSFÂ ExploitÂ Options a11y.text MSFÂ ExploitÂ 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 a11y.text 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 a11y.text 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)
```

Next Payloads Prev Exploits