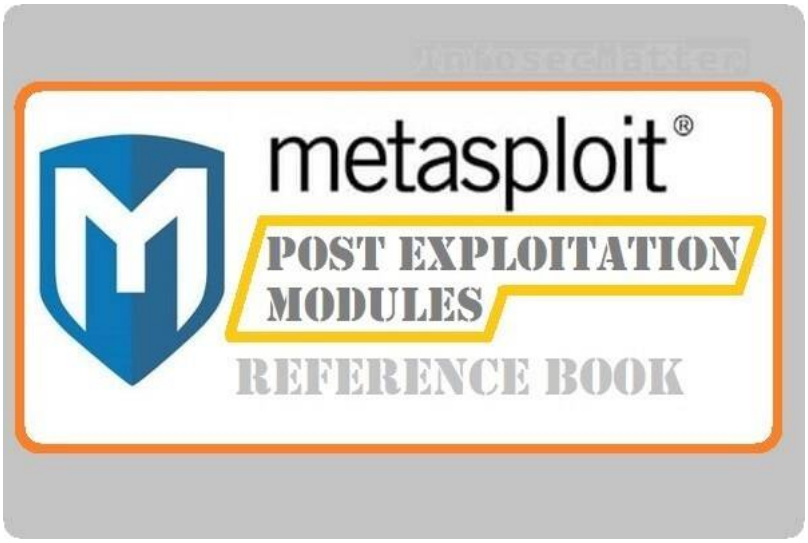
Post Exploitation Metasploit Modules (Reference)

infosecmatter.com/post-exploitation-metasploit-modules-reference

October 8, 2020



Did you know that there are over 350 post exploitation modules in the current Metasploit Framework version that comes pre-installed on the Kali Linux? How many of them do you use during your penetration testing activities?

If you are like me, chances are that you might be using only a handful of them. Well, hopefully this Metasploit post exploitation reference list will change that from now on!

Introduction

Although I have been using Metasploit Framework for many years now, I can't honestly say that I would have somewhat thorough overall knowledge about all the existing post exploitation modules that are available in the Metasploit.

To explore all those hundreds of modules has always been a seemingly difficult thing to do, requiring a fair amount of typing in the msfconsole. Even though I can type with all 10 fingers, it's just been always inconvenient to really spend the time and effort to check each and every module.

That's one of the reasons why I created this page listing all Metasploit post exploitation modules in one place, grouped logically, with details and links conveniently available about each module, ultimately hoping that it will provide somewhat better overview.

How to use this reference list

Every Metasploit post exploitation module listed here is primarily categorized based on the operating system (platform) and then based on its function, e.g. Windows -> Privilege escalation.

Additionally, there are relevant resource links added to each module whenever available, namely:

- Source code of the module
- Official documentation with usage examples
- Any referenced links listed in the module

When looking for a module, I suggest the following approach. Let's say you have exploited a Linux operating system and you are looking for modules that you could use to enumerate the system:

1. First look on the Multiplatform modules, e.g.: Multiplatform -> Information gathering
2. Then look also on the Linux modules, e.g.: Linux -> Information gathering

That would be somewhat equivalent to running:

```
msf5 > search type:post platform:linux name:gather
```

Except that here you don't have to type anything – you have detailed information listed conveniently at hand with additional details available just a mouse click away.

Enough talk, just give it a try and see if it suits you!

Go back to menu.

Multiplatform post exploitation modules

Metasploit module	Description
post/multi/gather/aws_keys	**UNIX Gather AWS Keys** This module will attempt to read AWS configuration files (.aws/config, .aws//credentials and .s3cfg) for users discovered on the session'd system and extract AWS keys from within. Platforms: unix (source, docs, ref1, ref2)
post/multi/gather/dbvis_enum	**Multi Gather DbVisualizer Connections Settings** DbVisualizer stores the user database configuration in dbvis.xml. This module retrieves the connections settings from this file and decrypts the encrypted passwords. Platforms: linux, win (source)
post/multi/gather/docker_creds	**Multi Gather Docker Credentials Collection** This module will collect the contents of all users' .docker directories on the targeted machine. If the user has already push to docker hub, chances are that the password was saved in base64 (default behavior). Platforms: bsd, linux, osx, unix (source)
post/multi/gather/fetchmailrc_creds	**UNIX Gather .fetchmailrc Credentials** Post Module to obtain credentials saved for IMAP, POP and other mail retrieval protocols in fetchmail's .fetchmailrc. Platforms: bsd, linux, osx, unix (source)
post/multi/gather/filezilla_client_cred	**Multi Gather FileZilla FTP Client Credential Collection** This module will collect credentials from the FileZilla FTP client if it is installed. Platforms: bsd, linux, osx, unix, win (source)
post/multi/gather/gpg_creds	**Multi Gather GnuPG Credentials Collection** This module will collect the contents of all users' .gnupg directories on the targeted machine. Password protected secret keyrings can be cracked with John the Ripper (JtR). Platforms: bsd, linux, osx, unix (source)
post/multi/gather/grub_creds	**Gather GRUB Password** This module gathers GRUB passwords from GRUB bootloader config files. Platforms: linux, osx, unix, solaris, bsd (source, docs, ref1)
post/multi/gather/irssi_creds	**Multi Gather IRSSI IRC Password(s)** This module grabs IRSSI IRC credentials. Platforms: bsd, linux, osx, unix (source, docs)
post/multi/gather/jboss_gather	**Jboss Credential Collector** This module can be used to extract the Jboss admin passwords for version 4,5 and 6. Platforms: linux, win (source, docs)
post/multi/gather/jenkins_gather	**Jenkins Credential Collector** This module can be used to extract saved Jenkins credentials, user tokens, SSH keys, and secrets. Interesting files will be stored in loot along with combined csv output. Platforms: linux, win (source, docs)
post/multi/gather/lastpass_creds	**LastPass Vault Decryptor** This module extracts and decrypts LastPass master login accounts and passwords, encryption keys, 2FA tokens and all the vault passwords. Platforms: linux, osx, unix, win (source, ref1)
post/multi/gather/maven_creds	**Multi Gather Maven Credentials Collection** This module will collect the contents of all users' settings.xml (Apache Maven configuration file) on the targeted machine. Platforms: bsd, linux, osx, unix, win (source, docs)
post/multi/gather/netrc_creds	**UNIX Gather .netrc Credentials** This module obtains credentials for FTP and other services saved in the .netrc for each user. Platforms: bsd, linux, osx, unix (source)
post/multi/gather/pgpass_creds	**Multi Gather pgpass Credentials** This module will collect the contents of all users' .pgpass or pgpass.conf file and parse them for credentials. Platforms: linux, bsd, unix, osx, win (source)

Metasploit module	Description
post/multi/gather/pidgin_cred	**Multi Gather Pidgin Instant Messenger Credential Collection** This module will collect credentials from the Pidgin IM client if it is installed. Platforms: bsd, linux, osx, unix, win (source)
post/multi/gather/remmina_creds	**UNIX Gather Remmina Credentials** Post module to obtain credentials saved for RDP and VNC from Remmina's configuration files. Platforms: bsd, linux, osx, unix (source)
post/multi/gather/rsyncd_creds	**UNIX Gather RSYNC Credentials** Post Module to obtain credentials saved for RSYNC in various locations. Platforms: linux, osx, unix, solaris, bsd (source)
post/multi/gather/rubygems_api_key	**Multi Gather RubyGems API Key** This module obtains a user's RubyGems API key from ~/.gem/credentials. Platforms: bsd, linux, osx, unix (source)
post/multi/gather/ssh_creds	**Multi Gather OpenSSH PKI Credentials Collection** This module will collect the contents of all users' .ssh directories on the targeted machine. Additionally, known_hosts and authorized_keys files are also downloaded. Platforms: bsd, linux, osx, unix (source)
post/multi/gather/thunderbird_creds	**Multi Gather Mozilla Thunderbird Signon Credential Collection** This module will collect credentials from Mozilla Thunderbird by downloading the necessary files such as 'signons.sqlite', 'key3.db', and 'cert8.db' for offline decryption with third party tools. Platforms: linux, osx, win (source)
post/multi/gather/tomcat_gather	**Gather Tomcat Credentials** This module will attempt to collect credentials from Tomcat services running on the machine. Platforms: win, linux (source, docs)

Go back to menu.

Multiplatform privilege escalation modules

Metasploit module	Description
post/multi/escalate/aws_create_iam_user	**Create an AWS IAM User** This module will attempt to create an AWS (Amazon Web Services) IAM (Identity and Access Management) user with Admin privileges. Platforms: unix (source, docs, ref1)
post/multi/escalate/cups_root_file_read	**CUPS 1.6.1 Root File Read** This module exploits the CVE-2012-5519 vulnerability in CUPS < 1.6.2, an open source printing system. The vulnerability allows to read arbitrary files (as root) on the system. Platforms: linux, osx (source, ref1)
post/multi/escalate/metasploit_pcaplog	**Multi Escalate Metasploit pcap_log Local Privilege Escalation** Metasploit < 4.4 contains a vulnerable 'pcap_log' plugin which, when used with the default settings, creates pcap files in /tmp with predictable file names. A successful exploitation results in the creation of a new superuser account. Platforms: bsd, linux, unix (source, ref1, ref2)
post/multi/recon/local_exploit_suggester	**Multi Recon Local Exploit Suggester** This module suggests local meterpreter exploits that can be used. The exploits are suggested based on the architecture, session type and the platform of the target. Platforms: all_platforms (source, docs)
post/multi/recon/multiport_egress_traffic	**Generate TCP/UDP Outbound Traffic On Multiple Ports** This module generates TCP or UDP traffic across a sequence of ports, and is useful for finding firewall holes and egress filtering. Platforms: linux, osx, unix, solaris, bsd, windows (source, docs)
post/multi/recon/sudo_commands	**Sudo Commands** This module examines the sudoers configuration for the session user and lists the commands executable via sudo. It also inspects each command and reports potential avenues for privileged code execution due to poor file system permissions or permitting execution of executables known to be useful for privesc. Platforms: bsd, linux, osx, solaris, unix (source, docs)

Go back to menu.

Information gathering (Multiplatform)

Metasploit module	Description
post/multi/gather/apple_ios_backup	**Windows Gather Apple iOS MobileSync Backup File Collection** This module will collect sensitive files from any on-disk iOS device backups. Platforms: osx, win (source)
post/multi/gather/aws_ec2_instance_metadata	**Gather AWS EC2 Instance Metadata** This module will attempt to connect to the AWS EC2 instance metadata service and crawl and collect all metadata known about the session'd host. Platforms: unix (source, docs, ref1)
post/multi/gather/check_malware	**Multi Gather Malware Verifier** This module will check a file for malware on VirusTotal based on the checksum. Platforms: osx, win, linux (source)
post/multi/gather/dns_bruteforce	**Multi Gather DNS Forward Lookup Bruteforce** Brute force subdomains and hostnames via wordlist. Platforms: bsd, linux, osx, solaris, win (source)
post/multi/gather/dns_reverse_lookup	**Multi Gather DNS Reverse Lookup Scan** Performs DNS reverse lookup using the OS included DNS query command. Platforms: bsd, linux, osx, solaris, win (source)
post/multi/gather/dns_srv_lookup	**Multi Gather DNS Service Record Lookup Scan** Enumerates known SRV Records for a given domain using target host DNS query tool. Platforms: bsd, linux, osx, solaris, win (source)
post/multi/gather/enum_hexchat	**Linux Gather HexChat/XChat Enumeration** This module will collect HexChat and XChat's config files and chat logs from the victim's machine, including channel settings, channel/server passwords, etc. Platforms: linux (source, docs, ref1)
post/multi/gather/enum_software_versions	**Multiplatform Installed Software Version Enumerator** This module will gather details on all installed software, including their versions and if available, when they were installed, and will save it into a loot file for later use. This can be used to determine what additional vulnerabilites may affect the target machine. Platforms: win, linux, osx, bsd, solaris, android (source, docs)
post/multi/gather/enum_vbox	**Multi Gather VirtualBox VM Enumeration** This module will attempt to enumerate any VirtualBox VMs on the target machine belonging to the current user. Platforms: bsd, linux, osx, unix, win (source)
post/multi/gather/env	**Multi Gather Generic Operating System Environment Settings** This module prints out the operating system environment variables. Platforms: linux, win (source)
post/multi/gather/find_vmx	**Multi Gather VMWare VM Identification** This module will attempt to find any VMWare virtual machines stored on the target. Platforms: bsd, linux, osx, unix, win (source)
post/multi/gather/multi_command	**Multi Gather Run Shell Command Resource File** This module will read shell commands from a resource file and execute the commands in the specified meterpreter or shell session. Platforms: bsd, linux, osx, unix, win (source)
post/multi/gather/ping_sweep	**Multi Gather Ping Sweep** Performs IPv4 ping sweep using the OS included ping command. Platforms: bsd, linux, osx, solaris, win (source)
post/multi/gather/resolve_hosts	**Multi Gather Resolve Hosts** Resolves hostnames to either IPv4 or IPv6 addresses from the perspective of the remote host. Platforms: win, python (source)

Metasploit module	Description
post/multi/gather/run_console_rc_file	**Multi Gather Run Console Resource File** This module will read console commands from a resource file and execute the commands in the specified Meterpreter session. Platforms: win (source)
post/multi/gather/skype_enum	**Multi Gather Skype User Data Enumeration** This module will enumerate Skype account settings, contact list, call history, chat logs, file transfer history, and voicemail logs, saving all the data to CSV files for analysis. Platforms: osx, win (source)
post/multi/gather/ubiquiti_unifi_backup	**Multi Gather Ubiquiti UniFi Controller Backup** On an Ubiquiti UniFi controller, reads the system.properties configuration file and downloads the backup and autobackup files. The files are then decrypted using a known encryption key, then attempted to be repaired by zip. Platforms: linux, win, osx (source, docs, ref1, ref2, ref3, ref4)
post/multi/gather/wlan_geolocate	**Multiplatform WLAN Enumeration and Geolocation** Enumerate wireless networks visible to the target device. Optionally geolocate the target by gathering local wireless networks and performing a lookup against Google APIs. Platforms: android, osx, win, linux, bsd, solaris (source, docs)

Go back to menu.

Spy / Capture (Multiplatform)

Metasploit module	Description
post/multi/manage/record_mic	**Multi Manage Record Microphone** This module will enable and record your target's microphone. For non-Windows targets, use the Java meterpreter to be able to use this feature. Platforms: linux, osx, win (source)

Go back to menu.

General / Other (Multiplatform)

Metasploit module	Description
post/multi/general/close	**Multi Generic Operating System Session Close** This module closes the specified session. This can be useful as a finisher for automation tasks. Platforms: linux, osx, unix, win (source)
post/multi/general/execute	**Multi Generic Operating System Session Command Execution** This module executes an arbitrary command line. Platforms: linux, osx, unix, win (source)
post/multi/general/wall	**Write Messages to Users** This module utilizes the wall(1) or write(1) utilities, as appropriate, to send messages to users on the target system. Platforms: linux, osx, unix (source)
post/multi/manage/autoroute	**Multi Manage Network Route via Meterpreter Session** This module enables network routing via an existing meterpreter session. It enables other modules to 'pivot' through a compromised host. Autoadd will search a session for valid subnets from the routing table and interface list and then automatically add routes to them. Platforms: (source, docs)
post/multi/manage/dbvis_add_db_admin	**Multi Manage DbVisualizer Add Db Admin** This modules creates an administrator account in the database accessed via the DbVisualizer management and analysis tool. Note: This module currently only supports MySQL. Platforms: linux, win (source, ref1)
post/multi/manage/dbvis_query	**Multi Manage DbVisualizer Query** This modules allows to execute SQL queries in the database accessed via the DbVisualizer management and analysis tool. Platforms: linux, win (source, ref1)
post/multi/manage/multi_post	**Multi Manage Post Module Macro Execution** This module will execute a list of modules given in a macro file in the format of <module> <opt=val,opt=val> against the select meterpreter or shell session. Platforms: linux, osx, solaris, unix, win (source)
post/multi/manage/open	**Open a file or URL on the target computer** This module will open any file or URL specified with the URI format on the target computer via the embedded commands such as 'open' or 'xdg-open'. Platforms: osx, linux, win (source, docs)
post/multi/manage/play_youtube	**Multi Manage YouTube Broadcast** This module will broadcast a YouTube video on specified compromised systems. It will play the video in the target machine's native browser. Platforms: win, osx, linux, android, unix (source, docs)
post/multi/manage/screensaver	**Multi Manage the screensaver of the target computer** This module allows you to turn on or off the screensaver of the target computer and also lock the current session. Platforms: linux, osx, win (source, docs)
post/multi/manage/screenshare	**Multi Manage the screen of the target meterpreter session** This module allows you to view and control the screen of the target computer via a local browser window. The module continually screenshots the target screen and also relays all mouse and keyboard events to session. Platforms: linux, win, osx (source, docs)
post/multi/manage/set_wallpaper	**Multi Manage Set Wallpaper** This module will set the desktop wallpaper background on the specified session. Platforms: win, osx, linux, android (source)
post/multi/manage/shell_to_meterpreter	**Shell to Meterpreter Upgrade** This module attempts to upgrade a command shell to meterpreter. The shell platform is automatically detected and the best version of meterpreter for the target is selected. Platforms: linux, osx, unix, solaris, bsd, windows (source, docs)

Metasploit module	Description
post/multi/manage/sudo	**Multiple Linux / Unix Post Sudo Upgrade Shell** This module attempts to upgrade a shell account to UID 0 by reusing the given password and passing it to sudo. Platforms: aix, linux, osx, solaris, unix (source, ref1)
post/multi/manage/system_session	**Multi Manage System Remote TCP Shell Session** This module will create a Reverse TCP Shell on the target system using the system's own scripting environments installed on the target. Platforms: linux, osx, unix (source)
post/multi/manage/upload_exec	**Upload and Execute** This modules allows to push a file on the remote system and execute it. Platforms: win, unix, linux, osx, bsd, solaris (source, docs)
post/multi/manage/zip	**Multi Manage File Compressor** This module zips a file or a directory on the remote system. Platforms: win, linux (source)

Go back to menu.

Windows post exploitation modules

Extract credentials (Windows)

Metasploit module	Description
post/windows/capture/lockout_keylogger	**Windows Capture Winlogon Lockout Credential Keylogger** This module migrates and logs Microsoft Windows user's passwords via Winlogon.exe using idle time and natural system changes to give a false sense of security to the user. (source, ref1)
post/windows/gather/bitlocker_fvek	**Bitlocker Master Key (FVEK) Extraction** This module enumerates ways to decrypt Bitlocker volume and if a recovery key is stored locally or can be generated, dump the Bitlocker master key (FVEK). (source, docs, ref1, ref2)
post/windows/gather/cachedump	**Windows Gather Credential Cache Dump** This module uses the registry to extract the stored domain hashes that have been cached as a result of a GPO setting. The default setting on Windows is to store the last ten successful logins. (source, docs, ref1)
post/windows/gather/credentials/credential_collector	**Windows Gather Credential Collector** This module harvests credentials (hashes and access tokens) found on the host and stores them in the database. (source)
post/windows/gather/credentials/enum_cred_store	**Windows Gather Credential Store Enumeration and Decryption Module** This module will enumerate the Microsoft Credential Store and decrypt the credentials. This module can only access credentials created by the user the process is running as. It cannot decrypt Domain Network Passwords, but will display the username and location. (source)
post/windows/gather/credentials/mssql_local_hashdump	**Windows Gather Local SQL Server Hash Dump** This module extracts the usernames and password hashes from an MSSQL server and stores them as loot. It uses the same technique in mssql_local_auth_bypass. (source, ref1)
post/windows/gather/credentials/outlook	**Windows Gather Microsoft Outlook Saved Password Extraction** This module extracts and decrypts saved Microsoft Outlook (versions 2002-2010) passwords from the Windows Registry for POP3/IMAP/SMTP/HTTP accounts. (source)
post/windows/gather/credentials/rdc_manager_creds	**Windows Gather Remote Desktop Connection Manager Saved Password Extraction** This module extracts and decrypts saved Microsoft Remote Desktop Connection Manager (RDCMan) passwords the .RDG files of users. The module will attempt to find the files configured for all users on the target system. (source)
post/windows/gather/credentials/skype	**Windows Gather Skype Saved Password Hash Extraction** This module finds saved login credentials for the Windows Skype client found in the Config.xml file. (source, ref1, ref2, ref3)
post/windows/gather/credentials/sso	**Windows Single Sign On Credential Collector (Mimikatz)** This module will collect cleartext Single Sign On credentials from the Local Security Authority using the Kiwi (Mimikatz) extension. Blank passwords will not be stored in the database. (source)
post/windows/gather/credentials/windows_autologin	**Windows Gather AutoLogin User Credential Extractor** This module extracts plain-text Windows AutoLogin passwords from Registry stored in the HKLM\Software\Microsoft\Windows NT\WinLogon location, which is readable by all users. (source, ref1, ref2)
post/windows/gather/enum_snmp	**Windows Gather SNMP Settings Enumeration (Registry)** This module will enumerate the SNMP service configuration, including stored community strings (SNMP authentication). (source)
post/windows/gather/enum_unattend	**Windows Gather Unattended Answer File Enumeration** This module will check the file system for a copy of unattend.xml and/or autounattend.xml found in Windows Vista, or newer Windows systems. And then extract sensitive information such as usernames and decoded passwords. (source, ref1, ref2, ref3)

Metasploit module	Description
post/windows/gather/hashdump	**Windows Gather Local User Account Password Hashes (Registry)** This module will dump the local user accounts from the SAM database using the registry. (source, docs)
post/windows/gather/lsa_secrets	**Windows Enumerate LSA Secrets** This module will attempt to enumerate the LSA Secrets keys found in the registry under the HKEY_LOCAL_MACHINE\Security\Policy\Secrets\ location. (source)
post/windows/gather/netlm_downgrade	**Windows NetLM Downgrade Attack** This module will change a registry value to enable the sending of LM challenge hashes and then initiate a SMB connection to the SMBHOST datastore. If an SMB server is listening, it will receive the NetLM hashes. (source, ref1)
post/windows/gather/phish_windows_credentials	**Windows Gather User Credentials (phishing)** This module is able to perform a phishing attack on the target by popping up a loginprompt. When the user fills credentials in the loginprompt, the credentials will be sent to the attacker. (source, docs, ref1)
post/windows/gather/smart_hashdump	**Windows Gather Local and Domain Controller Account Password Hashes** This will dump local accounts from the SAM Database. If the target host is a Domain Controller, it will dump the Domain Account Database using the proper technique depending on privilege level, OS and role of the host. (source)
post/windows/gather/word_unc_injector	**Windows Gather Microsoft Office Word UNC Path Injector** This module modifies a remote .docx file that will, upon opening, submit stored netNTLM credentials to a remote host. Verified to work with Microsoft Word 2003, 2007, 2010, and 2013. In order to get the hashes the auxiliary/server/capture/smb module can be used. (source, ref1)
post/windows/manage/wdigest_caching	**Windows Post Manage WDigest Credential Caching** On Windows 8/2012 or higher, the Digest Security Provider (WDIGEST) is disabled by default. This module enables/disables credential caching by adding/changing the value of the UseLogonCredential DWORD under the WDIGEST provider's Registry key. Any subsequent logins will allow mimikatz to recover the plain text passwords from the system's memory. (source)

Go back to menu.

Extract credentials (3rd party applications)

Metasploit module	Description
post/windows/gather/credentials/purevpn_cred_collector	**Windows Gather PureVPN Client Credential Collector** Finds the password stored for the PureVPN Client. (source, docs, ref1, ref2)
post/windows/gather/credentials/avira_password	**Windows Gather Avira Password Extraction** This module extracts password from the Avira Antivirus (≤ 15.0.17.273). (source)
post/windows/gather/credentials/bulletproof_ftp	**Windows Gather BulletProof FTP Client Saved Password Extraction** This module extracts information from the BulletProof FTP client including bookmarks and credentials and saves them in the database. (source)
post/windows/gather/credentials/coreftp	**Windows Gather CoreFTP Saved Password Extraction** This module extracts saved passwords from the CoreFTP FTP client from registry. (source)
post/windows/gather/credentials/dynazip_log	**Windows Gather DynaZIP Saved Password Extraction** This module extracts clear text credentials from dynazip.log file, which contains passwords used to encrypt compressed zip files in Microsoft Plus! 98 and Windows Me. (source, docs, ref1)
post/windows/gather/credentials/dyndns	**Windows Gather DynDNS Client Password Extractor** This module extracts the username, password, and hosts for DynDNS version 4.1.8. (source)
post/windows/gather/credentials/enum_picasa_pwds	**Windows Gather Google Picasa Password Extractor** This module extracts and decrypts the login passwords stored by Google Picasa. (source)
post/windows/gather/credentials/epo_sql	**Windows Gather McAfee ePO 4.6 Config SQL Credentials** This module extracts connection details and decrypts the saved password for the SQL database in use by a McAfee ePO 4.6 server. (source)
post/windows/gather/credentials/filezilla_server	**Windows Gather FileZilla FTP Server Credential Collection** This module will collect credentials from the installed FileZilla FTP server. (source)
post/windows/gather/credentials/flashfxp	**Windows Gather FlashFXP Saved Password Extraction** This module extracts saved FTP passwords from the FlashFXP client and its Sites.dat file. (source)
post/windows/gather/credentials/ftpnavigator	**Windows Gather FTP Navigator Saved Password Extraction** This module extracts saved passwords from the FTP Navigator FTP client. It will decode the saved passwords and store them in the database. (source)
post/windows/gather/credentials/ftpx	**Windows Gather FTP Explorer (FTPX) Credential Extraction** This module finds saved login credentials in profiles.xml configuration file of the FTP Explorer (FTPx) client. (source)
post/windows/gather/credentials/heidisql	**Windows Gather HeidiSQL Saved Password Extraction** This module extracts saved passwords from the HeidiSQL client from the registry. (source)
post/windows/gather/credentials/idm	**Windows Gather Internet Download Manager (IDM) Password Extractor** This module recovers premium download account passwords from the Internet Download Manager (IDM) stored in registry. (source)
post/windows/gather/credentials/imail	**Windows Gather IPSwitch iMail User Data Enumeration** This module will collect iMail user data such as the username, domain, full name, e-mail, and the decoded password. (source)
post/windows/gather/credentials/imvu	**Windows Gather Credentials IMVU Game Client** This module extracts account username & password from the IMVU game client and stores it as loot. (source)

Metasploit module	Description
post/windows/gather/credentials/mcafee_vse_hashdump	**McAfee Virus Scan Enterprise Password Hashes Dump** This module extracts the password hash from McAfee Virus Scan Enterprise (VSE) used to lock down the user interface. (source, ref1)
post/windows/gather/credentials/mdaemon_cred_collector	**Windows Gather MDaemonEmailServer Credential Cracking** This module extracts passwords of the MDaemon Email Server. (source, docs)
post/windows/gather/credentials/meebo	**Windows Gather Meebo Password Extractor** This module extracts login password of the Meebo Notifier, a desktop version of the Meebo's Online Messenger. (source)
post/windows/gather/credentials/mremote	**Windows Gather mRemote Saved Password Extraction** This module extracts saved passwords from mRemote connection manager. The mRemote stores connections for RDP, VNC, SSH, Telnet, rlogin and other protocols. (source)
post/windows/gather/credentials/nimbuzz	**Windows Gather Nimbuzz Instant Messenger Password Extractor** This module extracts account passwords saved by the Nimbuzz Instant Messenger. (source)
post/windows/gather/credentials/razer_synapse	**Windows Gather Razer Synapse Password Extraction** This module will enumerate passwords stored by the Razer Synapse client. (source, ref1, ref2)
post/windows/gather/credentials/razorsql	**Windows Gather RazorSQL Credentials** This module extracts credentials and other information from the RazorSQL db client, stored in the profiles.txt configuration file. (source)
post/windows/gather/credentials/securecrt	**Windows SecureCRT Session Information Enumeration** This module will extract credentials from the SecureCRT SSH and Telnet client configuration files. (source, docs, ref1)
post/windows/gather/credentials/smartermail	**Windows Gather SmarterMail Password Extraction** This module extracts and decrypts the sysadmin password from the SmarterMail 'mailConfig.xml' configuration file. (source, ref1)
post/windows/gather/credentials/smartftp	**Windows Gather SmartFTP Saved Password Extraction** This module finds saved login credentials in the SmartFTP FTP client configuration files. (source)
post/windows/gather/credentials/spark_im	**Windows Gather Spark IM Password Extraction** This module will enumerate passwords stored by the Spark IM client. (source, ref1)
post/windows/gather/credentials/steam	**Windows Gather Steam Client Session Collector.** This module will collect Steam session information from an account set to autologin. (source)
post/windows/gather/credentials/teamviewer_passwords	**Windows Gather TeamViewer Passwords** This module will find and decrypt stored TeamViewer passwords. (source, docs, ref1, ref2)
post/windows/gather/credentials/tortoisesvn	**Windows Gather TortoiseSVN Saved Password Extraction** This module extracts and decrypts saved TortoiseSVN passwords. (source)
post/windows/gather/credentials/total_commander	**Windows Gather Total Commander Saved Password Extraction** This module extracts weakly encrypted saved FTP Passwords from Total Commander, stored in the wcx_ftp.ini configuration file. (source)
post/windows/gather/credentials/trillian	**Windows Gather Trillian Password Extractor** This module extracts account password from Trillian & Trillian Astra v4.x-5.x instant messenger. (source)
post/windows/gather/credentials/vnc	**Windows Gather VNC Password Extraction** This module extracts DES encrypted passwords for VNC servers (UltraVNC, RealVNC, WinVNC, TightVNC etc.) from known registry locations. (source)

Metasploit module	Description
post/windows/gather/credentials/winscp	**Windows Gather WinSCP Saved Password Extraction** This module extracts weakly encrypted saved passwords from the WinSCP client, stored in registry and in the WinSCP.ini configuration file. Note that it cannot decrypt passwords if a master password is used. (source)
post/windows/gather/credentials/wsftp_client	**Windows Gather WS_FTP Saved Password Extraction** This module extracts weakly encrypted saved FTP Passwords from the WS_FTP client, stored in the ws_ftp.ini file. (source)
post/windows/gather/credentials/xshell_xftp_password	**Windows Gather Xshell and Xftp Passwords** This module can decrypt stored (remembered) passwords from Xshell and Xftp – SSH, FTP and Telnet clients. (source, docs, ref1)
post/windows/gather/enum_putty_saved_sessions	**Name** This module will identify whether Pageant (PuTTY Agent) is running and obtain saved session information from the registry, including credentials. (source)
post/windows/gather/enum_tomcat	**Windows Gather Apache Tomcat Enumeration** This module will collect information from a Windows-based Apache Tomcat, including the installation path, version, port, deployed web applications, users, passwords, roles, etc. (source)

Go back to menu.

Information gathering (Windows)

Metasploit module	Description
post/windows/gather/enum_emet	**Windows Gather EMET Protected Paths** This module will enumerate the EMET protected paths on the target host. (source)
post/windows/gather/arp_scanner	**Windows Gather ARP Scanner** This module will perform an ARP scan for a given IP range through a Meterpreter Session. (source, docs)
post/windows/gather/bitcoin_jacker	**Windows Gather Bitcoin Wallet** This module downloads any Bitcoin wallet files from the target system. It currently supports both the classic Satoshi wallet and the more recent Armory wallets. (source)
post/windows/gather/checkvm	**Windows Gather Virtual Environment Detection** This module attempts to determine whether the system is running inside of a virtual environment and if so, which one. This module supports detection of Hyper-V, VMWare, Virtual PC, VirtualBox, Xen, and QEMU. (source, docs)
post/windows/gather/dnscache_dump	**Windows Gather DNS Cache** This module displays the records stored in the DNS cache. (source, docs)
post/windows/gather/enum_applications	**Windows Gather Installed Application Enumeration** This module will enumerate all installed applications on a Windows system. (source, docs)
post/windows/gather/enum_artifacts	**Windows Gather File and Registry Artifacts Enumeration** This module will check the file system and registry for particular artifacts. The list of artifacts is read from data/post/enum_artifacts_list.txt or a user specified file. Any matches are written to the loot. (source)
post/windows/gather/enum_av_excluded	**Windows Antivirus Exclusions Enumeration** This module will enumerate the file, directory, process and extension-based exclusions from supported AV products, which currently includes Microsoft Defender, Microsoft Security Essentials/Antimalware, and Symantec Endpoint Protection. (source)
post/windows/gather/enum_computers	**Windows Gather Enumerate Computers** This module will enumerate computers included in the primary Domain. (source)
post/windows/gather/enum_db	**Windows Gather Database Instance Enumeration** This module will enumerate a windows system for installed database instances. (source)
post/windows/gather/enum_devices	**Windows Gather Hardware Enumeration** Enumerate PCI hardware information from the registry. Please note this script will run through registry subkeys such as: 'PCI', 'ACPI', 'ACPI_HAL', 'FDC', 'HID 'HTREE', 'IDE', 'ISAPNP', 'LEGACY", LPTENUM', 'PCIIDE', 'SCSI', 'STORAGE', 'SW and 'USB'. It is recommended to run this module as a background job. (source, docs)
post/windows/gather/enum_dirperms	**Windows Gather Directory Permissions Enumeration** This module enumerates directories and lists the permissions set on found directories. Note that if the PATH option isn't specified, then the module will start enumerate whatever is in the target machine's %PATH% variable. (source)
post/windows/gather/enum_files	**Windows Gather Generic File Collection** This module downloads files recursively based on the FILE_GLOBS option. (source)
post/windows/gather/enum_hostfile	**Windows Gather Windows Host File Enumeration** This module returns a list of entries in the target system's hosts file. (source)
post/windows/gather/enum_hyperv_vms	**Windows Hyper-V VM Enumeration** This module will check if the target machine is a Hyper-V host and, if it is, will return a list of all of the VMs running on the host, as well as stats such as their state, version, CPU Usage, uptime, and status. (source, docs)
post/windows/gather/enum_logged_on_users	**Windows Gather Logged On User Enumeration (Registry)** This module will enumerate current and recently logged on Windows users. (source, docs)

Metasploit module	Description
post/windows/gather/enum_ms_product_keys	**Windows Gather Product Key** This module will enumerate the OS license key. (source)
post/windows/gather/enum_patches	**Windows Gather Applied Patches** This module will attempt to enumerate which patches are applied to a windows system based on the result of the WMI query: SELECT HotFixID, InstalledOn FROM Win32_QuickFixEngineering. (source, docs, ref1)
post/windows/gather/enum_powershell_env	**Windows Gather Powershell Environment Setting Enumeration** This module will enumerate Microsoft Powershell settings. (source)
post/windows/gather/enum_proxy	**Windows Gather Proxy Setting** This module pulls a user's proxy settings from the current computer. It can also pull proxy settings from a specific SID (user) from another remote host. (source)
post/windows/gather/enum_services	**Windows Gather Service Info Enumeration** This module will query the system for services and display name and configuration info for each returned service. It allows you to optionally search the credentials, path, or start type for a string and only return the results that match. (source)
post/windows/gather/enum_shares	**Windows Gather SMB Share Enumeration via Registry** This module will enumerate configured and recently used file shares. (source)
post/windows/gather/enum_termserv	**Windows Gather Terminal Server Client Connection Information Dumper** This module dumps MRU and connection data for RDP sessions. (source)
post/windows/gather/enum_trusted_locations	**Windows Gather Microsoft Office Trusted Locations** This module will enumerate the Microsoft Office trusted locations on the target host. (source)
post/windows/gather/make_csv_orgchart	**Generate CSV Organizational Chart Data Using Manager Information** This module will generate a CSV file containing all users and their managers, which can be imported into Visio which will render it. (source, docs)
post/windows/gather/memory_grep	**Windows Gather Process Memory Grep** This module allows for searching the memory space of a process for potentially sensitive data. Please note: When the HEAP option is enabled, the module will have to migrate to the process you are grepping. (source)
post/windows/gather/outlook	**Windows Gather Outlook Email Messages** This module allows reading and searching email messages from the local Outlook installation using PowerShell. Please note that this module is manipulating the victims keyboard/mouse. If a victim is active on the target system, he/she may notice it. (source, ref1)
post/windows/gather/psreadline_history	**Windows Gather PSReadline History** Gathers Power Shell history data from the target machine. (source, docs, ref1, ref2, ref3)
post/windows/gather/resolve_sid	**Windows Gather Local User Account SID Lookup** This module prints information about a given SID from the perspective of this session. (source)
post/windows/gather/reverse_lookup	**Windows Gather IP Range Reverse Lookup** This module uses Railgun, calling the gethostbyaddr function to resolve a hostname to an IP. (source)
post/windows/gather/tcpnetstat	**Windows Gather TCP Netstat** This module lists current TCP sessions. (source, docs)
post/windows/gather/usb_history	**Windows Gather USB Drive History** This module will enumerate USB Drive history on a target host. (source)

Metasploit module	Description
post/windows/gather/win_privs	**Windows Gather Privileges Enumeration** This module will print if UAC is enabled, and if the current account is ADMIN enabled. It will also print UID, foreground SESSION ID, is SYSTEM status and current process PRIVILEGES. (source)
post/windows/gather/wmic_command	**Windows Gather Run Specified WMIC Command** This module will execute a given WMIC command options or read WMIC commands options from a resource file and execute the commands. (source)
post/windows/recon/computer_browser_discovery	**Windows Recon Computer Browser Discovery** This module uses railgun to discover hostnames and IPs on the network. (source)
post/windows/recon/outbound_ports	**Windows Outbound-Filtering Rules** This module implements TCP traceroute to a public IP address in order to obtain understanding of outbound-filtering rules in the environment. (source, ref1)
post/windows/recon/resolve_ip	**Windows Recon Resolve IP** This module reverse resolves a range or IP to a hostname. (source)
post/windows/wlan/wlan_bss_list	**Windows Gather Wireless BSS Info** This module gathers information about the wireless Basic Service Sets available to the victim machine. (source)
post/windows/wlan/wlan_current_connection	**Windows Gather Wireless Current Connection Info** This module gathers information about the current connection on each wireless lan interface on the target machine. (source)
post/windows/wlan/wlan_disconnect	**Windows Disconnect Wireless Connection** This module disconnects the current wireless network connection on the specified interface. (source)
post/windows/wlan/wlan_probe_request	**Windows Send Probe Request Packets** This module send probe requests through the wlan interface. The ESSID field will be use to set a custom message. (source, docs)
post/windows/wlan/wlan_profile	**Windows Gather Wireless Profile** This module extracts saved Wireless LAN profiles. It will also try to decrypt the network key material. Behavior is slightly different between OS versions. (source)

Go back to menu.

Windows privilege escalation modules

Metasploit module	Description
post/windows/escalate/droplnk	**Windows Escalate SMB Icon LNK Dropper** This module drops a shortcut (LNK file) that has a ICON reference existing on the specified remote host, causing SMB and WebDAV connections to be initiated from any user that views the shortcut. (source)
post/windows/escalate/getsystem	**Windows Escalate Get System via Administrator** This module uses the builtin 'getsystem' command to escalate the current session to the SYSTEM account from an administrator user account. (source)
post/windows/escalate/golden_ticket	**Windows Escalate Golden Ticket** This module will create a Golden Kerberos Ticket using the Mimikatz Kiwi Extension. If no options are applied it will attempt to identify the current domain, the domain administrator account, the target domain SID, and retrieve the krbtgt NTLM hash from the database. By default the well-known Administrator's groups 512, 513, 518, 519, and 520 will be applied to the ticket. (source, ref1)
post/windows/escalate/ms10_073_kbdlayout	**Windows Escalate NtUserLoadKeyboardLayoutEx Privilege Escalation** This module exploits the keyboard layout vulnerability exploited by Stuxnet. When processing specially crafted keyboard layout files (DLLs), the Windows kernel fails to validate that an array index is within the bounds of the array. By loading a specially crafted keyboard layout, an attacker can execute code in Ring 0. (source, ref1)
post/windows/escalate/screen_unlock	**Windows Escalate Locked Desktop Unlocker** This module unlocks a locked Windows desktop by patching the respective code inside the LSASS.exe process. This patching process can result in the target system hanging or even rebooting, so be careful when using this module on production systems. (source)
post/windows/escalate/unmarshal_cmd_exec	**Windows unmarshal post exploitation** This module exploits a local privilege escalation bug which exists in microsoft COM for windows when it fails to properly handle serialized objects. (source, docs, ref1, ref2)

Go back to menu.

Spy / Capture (Windows)

Metasploit module	Description
post/windows/capture/keylog_recorder	**Windows Capture Keystroke Recorder** This module can be used to capture keystrokes. It is recommended to run this module as a job, otherwise it will tie up your framework user interface. (source, docs)
post/windows/gather/screen_spy	**Windows Gather Screen Spy** This module will incrementally take desktop screenshots from the host. This allows for screen spying which can be useful to determine if there is an active user on a machine, or to record the screen for later data extraction. (source, docs)
post/windows/manage/rpcapd_start	**Windows Manage Remote Packet Capture Service Starter** This module enables the Remote Packet Capture System (rpcapd service) included in the default installation of Winpcap. The module allows you to set up the service in passive or active mode (useful if the client is behind a firewall). (source)
post/windows/manage/webcam	**Windows Manage Webcam** This module will allow the user to detect installed webcams (with the LIST action) or take a snapshot (with the SNAPSHOT) action. (source)

Go back to menu.

Forensics (Windows)

Metasploit module	Description
post/windows/gather/dumplinks	**Windows Gather Dump Recent Files lnk Info** The dumplinks module is a modified port of Harlan Carvey's lslnk.pl Perl script. This module will parse .lnk files from a user's Recent Documents folder and Microsoft Office's Recent Documents folder, if present. Windows creates these link files automatically for many common file types. The .lnk files contain time stamps, file locations, including share names, volume serial numbers, and more. (source, docs)
post/windows/gather/enum_muicache	**Windows Gather Enum User MUICache** This module gathers information from MUICache about the files and file paths that logged on users have executed on the system. It will also check if the files still exist on the system or not. This module works by gathering information stored under the MUICache registry key or in the NTUSER.DAT/UsrClass.dat files. (source)
post/windows/gather/enum_prefetch	**Windows Gather Prefetch File Information** This module gathers prefetch file information from WinXP, Win2k3 and Win7 systems and current values of related registry keys. From each prefetch file it will collect filetime of the last execution, file path hash, run count, filename and the execution path. (source)
post/windows/gather/file_from_raw_ntfs	**Windows File Gather File from Raw NTFS** This module gathers a file using the raw NTFS device, bypassing some Windows restrictions such as open file with write lock. Because it avoids the usual file locking issues, it can be used to retrieve files such as NTDS.dit. (source, ref1)
post/windows/gather/forensics/duqu_check	**Windows Gather Forensics Duqu Registry Check** This module searches for CVE-2011-3402 (Duqu) related registry artifacts. (source, ref1)
post/windows/gather/forensics/enum_drives	**Windows Gather Physical Drives and Logical Volumes** This module will list physical drives and logical volumes. (source)
post/windows/gather/forensics/imager	**Windows Gather Forensic Imaging** This module will perform byte-for-byte imaging of remote disks and volumes. (source)
post/windows/gather/forensics/nbd_server	**Windows Gather Local NBD Server** Maps remote disks and logical volumes to a local Network Block Device server. Allows for forensic tools to be executed on the remote disk directly. (source)
post/windows/gather/forensics/recovery_files	**Windows Gather Deleted Files Enumeration and Recovering** This module lists and attempts to recover deleted files from NTFS file systems. Use the FILES option to adjust the recovery process. (source, ref1)
post/windows/manage/nbd_server	**Windows Manage Local NBD Server for Remote Disks** Maps remote disks and logical volumes to a local Network Block Device server. Allows for forensic tools to be executed on the remote disk directly. (source)

Go back to menu.

Generic / Other (Windows)

Metasploit module	Description
post/windows/manage/killav	**Windows Post Kill Antivirus and Hips** This module attempts to locate and terminate any processes that are identified as being Antivirus or Host-based IPS related. (source)
post/windows/manage/archmigrate	**Architecture Migrate** This module checks if the meterpreter architecture is the same as the OS architecture and if it's incompatible it spawns a new process with the correct architecture and migrates into that process. (source, docs)
post/windows/manage/change_password	**Windows Manage Change Password** This module will attempt to change the password of the target account. The typical usage is to change password of a newly created account. (source)
post/windows/manage/clone_proxy_settings	**Windows Manage Proxy Setting Cloner** This module copies the proxy settings from the current user to the targeted user SID, supports remote hosts as well if remote registry is allowed. (source)
post/windows/manage/delete_user	**Windows Manage Local User Account Deletion** This module deletes a local user account from the specified server, or the local machine if no server is given. (source)
post/windows/manage/download_exec	**Windows Manage Download and/or Execute** This module will download a file by importing urlmon via railgun. The user may also choose to execute the file with arguments via exec_string. (source)
post/windows/manage/driver_loader	**Windows Manage Driver Loader** This module loads a KMD (Kernel Mode Driver) using the Windows Service API. (source)
post/windows/manage/enable_rdp	**Windows Manage Enable Remote Desktop** This module enables the Remote Desktop Service (RDP). It provides the options to create an account and configure it to be a member of the Local Administrators and Remote Desktop Users group. It can also forward the target's port 3389/tcp. (source)
post/windows/manage/enable_support_account	**Windows Manage Trojanize Support Account** This module enables alternative access to servers and workstations by modifying the support account's (support_388945a0) properties. It will enable the account for remote access as the administrator. (source)
post/windows/manage/execute_dotnet_assembly	**Execute .NET Assembly (x64 only)** This module executes a .NET assembly in memory. It reflectively loads a dll that will host CLR, then it copies the assembly to be executed into memory. (source, docs, ref1)
post/windows/manage/exec_powershell	**Windows Powershell Execution Post Module** This module will execute a powershell script in a meterpreter session. The user may also enter text substitutions to be made in memory before execution. (source)
post/windows/manage/forward_pageant	**Forward SSH Agent Requests To Remote Pageant** This module forwards SSH agent requests from a local socket to a remote Pageant instance. If a target Windows machine is compromised and is running Pageant, this will allow the attacker to run normal OpenSSH commands (e.g. ssh-add -l) against the Pageant host which are tunneled through the meterpreter session. This could therefore be used to authenticate with a remote host using a private key which is loaded into a remote user's Pageant instance, without ever having knowledge of the private key itself. (source)
post/windows/manage/hashcarve	**Windows Local User Account Hash Carver** This module will change a local user's password directly in the registry. (source, docs)
post/windows/manage/inject_ca	**Windows Manage Certificate Authority Injection** This module allows the attacker to insert an arbitrary CA certificate into the victim's Trusted Root store. (source)
post/windows/manage/inject_host	**Windows Manage Hosts File Injection** This module allows the attacker to insert a new entry into the target system's hosts file. (source)

Metasploit module	Description
post/windows/manage/install_python	**Install Python for Windows** This module places an embeddable Python3 distribution onto the target file system, granting pentesters access to a lightweight Python interpreter. (source, docs, ref1, ref2)
post/windows/manage/install_ssh	**Install OpenSSH for Windows** This module installs OpenSSH server and client for Windows using PowerShell. SSH on Windows can provide pentesters persistent access to a secure interactive terminal, interactive filesystem access, and port forwarding over SSH. (source, docs, ref1, ref2)
post/windows/manage/migrate	**Windows Manage Process Migration** This module will migrate a Meterpreter session from one process to another. A given process PID to migrate to or the module can spawn one and migrate to that newly spawned process. (source)
post/windows/manage/mssql_local_auth_bypass	**Windows Manage Local Microsoft SQL Server Authorization Bypass** When this module is executed, it can be used to add a sysadmin to local SQL Server instances. It first attempts to gain LocalSystem privileges using the “getsystem” escalation methods. If those privileges are not sufficient to add a sysadmin, then it will migrate to the SQL Server service process associated with the target instance. (source, docs)
post/windows/manage/multi_meterpreter_inject	**Windows Manage Inject in Memory Multiple Payloads** This module will inject in to several processes a given payload and connecting to a given list of IP Addresses. (source)
post/windows/manage/peinjector	**Peinjector** This module will inject a specified windows payload into a target executable. (source, docs)
post/windows/manage/persistence_exe	**Windows Manage Persistent EXE Payload Installer** This module will upload an executable to a remote host and make it persistent. It can be installed as USER, SYSTEM, or SERVICE. (source)
post/windows/manage/portproxy	**Windows Manage Set Port Forwarding With PortProxy** This module uses the PortProxy interface from netsh to set up port forwarding persistently (even after reboot). PortProxy supports TCP IPv4 and IPv6 connections. (source)
post/windows/manage/powershell/build_net_code	**Powershell .NET Compiler** This module will build a .NET source file using powershell. The compiler builds the executable or library in memory and produces a binary. After compilation the PowerShell session can also sign the executable if provided a path the a .pfx formatted certificate. (source, docs)
post/windows/manage/powershell/exec_powershell	**Windows Manage PowerShell Download and/or Execute** This module will download and execute a PowerShell script over a meterpreter session. The user may also enter text substitutions to be made in memory before execution. (source)
post/windows/manage/powershell/load_script	**Load Scripts Into PowerShell Session** This module will download and execute one or more PowerShell script s over a present powershell session. (source)
post/windows/manage/pptp_tunnel	**Windows Manage Remote Point-to-Point Tunneling Protocol** This module initiates a PPTP connection to a remote machine (VPN server). Once the tunnel is created we can use it to force the victim traffic to go through the server getting a man in the middle attack. (source, ref1)
post/windows/manage/priv_migrate	**Windows Manage Privilege Based Process Migration** This module will migrate a meterpreter session based on session privileges. It will do everything it can to migrate, including spawning a new User level process. For sessions with Admin rights: It will try to migrate into a System level process in the following order: ANAME (if specified), services.exe, wininit.exe, svchost.exe, lsm.exe, lsass.exe, and winlogon.exe. (source, docs)

Metasploit module	Description
post/windows/manage/pxeexploit	**Windows Manage PXE Exploit Server** This module provides a PXE server, running a DHCP and TFTP server. The default configuration loads a linux kernel and initrd into memory that reads the hard drive; placing a payload to install metsvc, disable the firewall, and add a new user metasploit on any Windows partition seen, and add a uid 0 user with username and password metasploit to any linux partition seen. The windows user will have the password p@SSw0rd!123456 (in case of complexity requirements) and will be added to the administrators group. (source)
post/windows/manage/reflective_dll_inject	**Windows Manage Reflective DLL Injection Module** This module will inject a specified reflective DLL into the memory of a process, new or existing. If arguments are specified, they are passed to the DllMain entry point as the lpvReserved (3rd) parameter. (source, ref1)
post/windows/manage/remove_ca	**Windows Manage Certificate Authority Removal** This module allows the attacker to remove an arbitrary CA certificate from the victim's Trusted Root store. (source)
post/windows/manage/remove_host	**Windows Manage Host File Entry Removal** This module allows the attacker to remove an entry from the Windows hosts file. (source)
post/windows/manage/rid_hijack	**Windows Manage RID Hijacking** This module will create an entry on the target by modifying some properties of an existing account. It will change the account attributes by setting a Relative Identifier (RID), which should be owned by one existing account on the destination machine. (source, docs, ref1)
post/windows/manage/rollback_defender_signatures	**Disable Windows Defender Signatures** This module with appropriate rights let to use the Windows Defender command-line utility a run and automation tool (mpcmdrun.exe) in order to disable all the signatures available installed for the compromised machine. (source, docs)
post/windows/manage/run_as	**Windows Manage Run Command As User** This module will login with the specified username/password and execute the supplied command as a hidden process. (source)
post/windows/manage/run_as_psh	**Windows "Run As" Using Powershell** This module will start a process as another user using powershell. (source, docs)
post/windows/manage/sdel	**Windows Manage Safe Delete** The goal of the module is to hinder the recovery of deleted files by overwriting its contents. This could be useful when you need to download some file on the victim machine and then delete it without leaving clues about its contents. (source)
post/windows/manage/shellcode_inject	**Windows Manage Memory Shellcode Injection Module** This module will inject into the memory of a process a specified shellcode. (source)
post/windows/manage/sshkey_persistence	**SSH Key Persistence** This module will add an SSH key to a specified user (or all), to allow remote login via SSH at any time. The target Windows system has to have OpenSSH server installed. (source, docs)
post/windows/manage/sticky_keys	**Sticky Keys Persistance Module** This module makes it possible to apply the 'sticky keys' hack to a session with appropriate rights. The hack provides a means to get a SYSTEM shell using UI-level interaction at an RDP login screen or via a UAC confirmation dialog. The module modifies the Debug registry setting for certain executables (sethc.exe, utilman.exe, osk.exe or displayswitch.exe). (source, ref1, ref2)
post/windows/manage/vmdk_mount	**Windows Manage VMDK Mount Drive** This module mounts a vmdk file (Virtual Machine Disk) on a drive provided by the user by taking advantage of the vstor2 device driver (VMware). (source, ref1)
post/windows/manage/vss_create	**Windows Manage Create Shadow Copy** This module will attempt to create a new volume shadow copy. (source, ref1)

Metasploit module	Description
post/windows/manage/vss_list	**Windows Manage List Shadow Copies** This module will attempt to list any Volume Shadow Copies on the system. (source, ref1)
post/windows/manage/vss_mount	**Windows Manage Mount Shadow Copy** This module will attempt to mount a Volume Shadow Copy on the system. (source, ref1)
post/windows/manage/vss_set_storage	**Windows Manage Set Shadow Copy Storage Space** This module will attempt to change the amount of space for volume shadow copy storage. (source, ref1)
post/windows/manage/vss_storage	**Windows Manage Get Shadow Copy Storage Info** This module will attempt to get volume shadow copy storage info. (source, ref1)

Go back to menu.

Active Directory post exploitation modules

Extract credentials (Active Directory)

Metasploit module	Description
post/windows/gather/credentials/domain_hashdump	**Windows Domain Controller Hashdump** This module attempts to copy the NTDS.dit database from a live Domain Controller and then parse out all of the User Accounts. It saves all of the captured password hashes, including historical ones. (source)
post/windows/gather/credentials/enum_laps	**Windows Gather Credentials Local Administrator Password Solution** This module will recover the LAPS (Local Administrator Password Solution) passwords, configured in Active Directory, which is usually only accessible by privileged users. (source)
post/windows/gather/credentials/gpp	**Windows Gather Group Policy Preference Saved Passwords** This module enumerates the victim machine's domain controller and connects to it via SMB. It then looks for Group Policy Preference XML files containing local user accounts and passwords (cPassword) and decrypts them using the publicly known AES key. (source, ref1, ref2, ref3, ref4)
post/windows/gather/enum_ad_bitlocker	**Windows Gather Active Directory BitLocker Recovery** This module will enumerate BitLocker recovery passwords in the default AD directory. This module does require Domain Admin or other delegated privileges. (source, ref1)
post/windows/gather/enum_ad_user_comments	**Windows Gather Active Directory User Comments** This module will enumerate user accounts in the default Active Domain (AD) directory which contain 'pass' in their description or comment (case-insensitive) by default. In some cases, such users have their passwords specified in these fields. (source, ref1)
post/windows/gather/ntds_grabber	**NTDS Grabber** This module uses a powershell script to obtain a copy of the ntds.dit SAM and SYSTEM files on a domain controller. It compresses all these files in a cabinet file called All.cab. (source, docs)
post/windows/gather/ntds_location	**Post Windows Gather NTDS.DIT Location** This module will find the location of the NTDS.DIT file (from the Registry check that it exists, and display its location on the screen, which is useful if you wish to manually acquire the file using ntdsutil or vss. (source)

Go back to menu.

Information gathering (Active Directory)

Metasploit module	Description
post/windows/gather/ad_to_sqlite	**AD Computer, Group and Recursive User Membership to Local SQLite DB** This module will gather a list of AD groups, identify the users (taking into account recursion) and write this to a SQLite database for offline analysis and query using normal SQL syntax. (source, docs)
post/windows/gather/bloodhound	**BloodHound Ingestor** This module will execute the BloodHound C# Ingestor (aka SharpHound) to gather sessions, local admin, domain trusts and more. With this information BloodHound will be able to identify attack paths that could lead to compromise of the Active Directory environment. (source, docs, ref1)
post/windows/gather/enum_ad_computers	**Windows Gather Active Directory Computers** This module will enumerate computers in the default AD directory. It allows fine grained enumeration to identify e.g. only domain controllers or only servers. It is also possible to define which information (attributes) should be retrieved. (source, ref1)
post/windows/gather/enum_ad_groups	**Windows Gather Active Directory Groups** This module will enumerate AD groups on the specified domain. (source)
post/windows/gather/enum_ad_managedby_groups	**Windows Gather Active Directory Managed Groups** This module will enumerate AD groups on the specified domain which are specifically managed and list of the managers. This can identify privilege escalation opportunities or persistence mechanisms without having domain admi privileges. (source)
post/windows/gather/enum_ad_service_principal_names	**Windows Gather Active Directory Service Principal Names** This module will enumerate servicePrincipalName in the default AD directory where the user is a member of the Domain Admins group. (source, ref1)
post/windows/gather/enum_ad_to_wordlist	**Windows Active Directory Wordlist Builder** This module will gather information from the default Active Domain (AD) directory and use these words to seed a wordlist. By default it enumerates user accounts t build the wordlist. (source)
post/windows/gather/enum_ad_users	**Windows Gather Active Directory Users** This module will enumerate user accounts in the default Active Domain (AD) directory and stores them in the database. (source)
post/windows/gather/enum_domain	**Windows Gather Enumerate Domain** This module identifies the primary domain via the registry. The registry value use is: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Grou Policy\History\DCName. (source)
post/windows/gather/enum_domains	**Windows Gather Domain Enumeration** This module enumerates currently the domains a host can see and the domain controllers for that domain. (source)
post/windows/gather/enum_domain_group_users	**Windows Gather Enumerate Domain Group** This module extracts user accounts from specified group and stores the results ir the loot. It will also verify if session account is in the group. This module should b run over as session with domain credentials. (source)
post/windows/gather/enum_domain_tokens	**Windows Gather Enumerate Domain Tokens** This module will enumerate tokens present on a system that are part of the domain the target host is part of. It will also enumerate users in the local Administrators, Users and Backup Operator groups to identify Domain members. Processes will be also enumerated and checked if they are running under a Domain account, on all checks the accounts, processes and tokens will be checked if they are part of the Domain Admin group of the domain the machine is a member of. (source)
post/windows/gather/enum_domain_users	**Windows Gather Enumerate Active Domain Users** This module will enumerate all domain computers and check whether the target user has session on them. It is also possible to list which users are logged in on which computers using this module. (source)

Metasploit module	Description
post/windows/gather/enum_tokens	**Windows Gather Enumerate Domain Admin Tokens (Token Hunter)** This module will identify systems that have a Domain Admin (delegation) token o them. The module will first check if sufficient privileges are present for certain actions, and run getprivs for system. If you elevated privs to system, the SeAssignPrimaryTokenPrivilege will not be assigned, in that case try migrating to another process that is running as system. (source)
post/windows/gather/local_admin_search_enum	**Windows Gather Local Admin Search** This module will identify systems in a given range that the supplied domain user (should migrate into a user pid) has administrative access to. It uses the Windows OpenSCManagerA API function. (source)

Go back to menu.

Generic / Other (Active Directory)

Metasploit module	Description
post/windows/manage/add_user	**Windows Manage Add User to the Domain and/or to a Domain Group** This module adds a user to the Domain and/or to a Domain group. It will check if sufficient privileges are present and run getprivs for system, if needed. (source)

Go back to menu.

Linux post exploitation modules

Extract credentials (Linux)

Metasploit module	Description
post/linux/gather/ecryptfs_creds	**Gather eCryptfs Metadata** This module will collect the contents of all users' .ecrypts directories on the targeted machine. Collected "wrapped-passphrase" files can be cracked with John the Ripper (JtR) to recover the "mount passphrases". (source)
post/linux/gather/enum_nagios_xi	**Nagios XI Enumeration** NagiosXI may store credentials of the hosts it monitors. This module extracts these credentials, creating opportunities for lateral movement. (source, docs)
post/linux/gather/enum_psk	**Linux Gather 802-11-Wireless-Security Credentials** This module collects 802-11-Wireless-Security credentials such as Access-Point name and Pre-Shared-Key from your target CLIENT Linux machine using /etc/NetworkManager/system-connections/ files. The module gathers NetworkManager's plaintext "psk" information. (source)
post/linux/gather/gnome_commander_creds	**Linux Gather Gnome-Commander Creds** This module collects clear text passwords stored by Gnome-commander, a GUI file explorer for GNOME. Typically, these passwords are stored in the user's home directory, at ~/.gnome-commander/connections. (source)
post/linux/gather/gnome_keyring_dump	**Gnome-Keyring Dump** This module extracts network passwords for the current user stored in the GNOME Keyring. No need root privileges. (source)
post/linux/gather/hashdump	**Linux Gather Dump Password Hashes for Linux Systems** Post module to dump the password hashes for all users on a Linux System. (source, docs)
post/linux/gather/mount_cifs_creds	**Linux Gather Saved mount.cifs/mount.smbfs Credentials** Post module to obtain credentials saved for mount.cifs/mount.smbfs in the /etc/fstab file on a Linux system. (source)
post/linux/gather/openvpn_credentials	**OpenVPN Gather Credentials** This module grabs OpenVPN credentials from a process listing on Linux. Note: –auth-nocache must not be set in the OpenVPN command line. (source, ref1)
post/linux/gather/phpmyadmin_credsteal	**Phpmyadmin credentials stealer** This module gathers PhpMyAdmin creds from the target linux machine. (source, docs)
post/linux/gather/pptpd_chap_secrets	**Linux Gather PPTP VPN chap-secrets Credentials** This module collects PPTP VPN information such as client, server, password, and IP from your target server's chap-secrets file. (source)

Go back to menu.

Information gathering (Linux)

Metasploit module	Description
post/linux/gather/checkcontainer	**Linux Gather Container Detection** This module attempts to determine whether the system is running inside of a container. It supports detection of Docker, LXC, and systemd nspawn. (source, docs)
post/linux/gather/checkvm	**Linux Gather Virtual Environment Detection** This module attempts to determine whether the system is running inside of a virtual environment. It supports detection of Hyper-V, VMWare, VirtualBox, Xen, and QEMU/KVM. (source, docs)
post/linux/gather/enum_commands	**Testing commands needed in a function** This module will list available commands on the target system, e.g. in the /bin/, /usr/bin, /sbin, /usr/sbin directories etc. (source)
post/linux/gather/enum_configs	**Linux Gather Configurations** This module collects configuration files found on commonly installed applications and services, such as Apache, MySQL, Samba, Sendmail, etc. (source)
post/linux/gather/enum_containers	**Linux Container Enumeration** This module attempts to enumerate containers on the target machine and optionally run a command on each active container found. Currently it supports Docker, LXC and RKT. (source, docs)
post/linux/gather/enum_network	**Linux Gather Network Information** This module gathers network information from the target system IPTables rules, interfaces, wireless information, open and listening ports, active network connections, DNS information and SSH information. (source)
post/linux/gather/enum_protections	**Linux Gather Protection Enumeration** This module checks whether popular system hardening mechanisms are in place, such as SMEP, SMAP, SELinux, PaX and grsecurity. It also tries to find installed applications that can be used to hinder, prevent, or detect attacks, such as tripwire, snort, and apparmor. This module is meant to identify Linux Secure Modules (LSM) in addition to various antivirus, IDS/IPS, firewalls, sandboxes and other security related software. (source)
post/linux/gather/enum_system	**Linux Gather System and User Information** This module gathers system information. Ir collects installed packages, installed services, mount information, user list, user bash history and cron jobs. (source)
post/linux/gather/enum_users_history	**Linux Gather User History** This module gathers the following user-specific information: shell history, MySQL history, PostgreSQL history, MongoDB history, Vim history, lastlog, and sudoers. (source)
post/linux/gather/tor_hiddenservices	**Linux Gather TOR Hidden Services** This module collects the hostnames and private keys of any TOR Hidden Services running on the target machine. Root permissions are required to read all Hidden Service directories, which are usually owned by a separate account. (source)

Go back to menu.

Busybox related (Linux)

These modules will be applied on a session connected to a BusyBox shell.

Metasploit module	Description
post/linux/busybox/enum_connections	**BusyBox Enumerate Connections** This module will be applied on a session connected to a BusyBox shell. It will enumerate the connections established with the router or device executing BusyBox. (source)
post/linux/busybox/enum_hosts	**BusyBox Enumerate Host Names** This module will be applied on a session connected to a BusyBox shell. It will enumerate host names related to the device executing BusyBox. (source)
post/linux/busybox/jailbreak	**BusyBox Jailbreak** This module will send a set of commands to an open session that is connected to a BusyBox limited shell (i.e. a router limited shell). It will try different known tricks to jailbreak the limited shell and get a full BusyBox shell. (source)
post/linux/busybox/ping_net	**BusyBox Ping Network Enumeration** This module will be applied on a session connected to a BusyBox shell. It will ping a range of IP addresses from the router or device executing BusyBox. (source)
post/linux/busybox/set_dmz	**BusyBox DMZ Configuration** This module will be applied on a session connected to a BusyBox shell. It allows to manage traffic forwarding to a target host through the BusyBox device. (source)
post/linux/busybox/set_dns	**BusyBox DNS Configuration** This module will be applied on a session connected to a BusyBox shell. It allows to set the DNS server on the device executing BusyBox so it will be sent by the DHCP server to network hosts. (source)
post/linux/busybox/smb_share_root	**BusyBox SMB Sharing** This module will be applied on a session connected to a BusyBox shell. It will modify the SMB configuration of the device executing BusyBox to share the root directory of the device. (source)
post/linux/busybox/wget_exec	**BusyBox Download and Execute** This module will be applied on a session connected to a BusyBox shell. It will use wget to download and execute a file from the device running BusyBox. (source)

Go back to menu.

Generic / Other (Linux)

Metasploit module	Description
post/linux/dos/xen_420_dos	**Linux DoS Xen 4.2.0 2012-5525** This module causes a hypervisor crash in Xen 4.2.0 when invoked from a paravirtualized VM, including from dom0. (source, docs)
post/linux/manage/dns_spoofing	**Native DNS Spoofing module** This module will redirect all DNS requests on the target Linux system to an arbitrary remote DNS server. (source)
post/linux/manage/download_exec	**Linux Manage Download and Execute** This module downloads and runs a file with bash. It first tries to uses curl as its HTTP client and then wget if it's not found. (source)
post/linux/manage/iptables_removal	**IPTABLES rules removal** This module will completely remove all IPTABLES rules on the target system, including NAT rules. (source)
post/linux/manage/pseudo_shell	**Pseudo-Shell Post-Exploitation Module** This module will run a Pseudo-Shell. (source)
post/linux/manage/sshkey_persistence	**SSH Key Persistence** This module will add an SSH key to a specified user (or all), to allow remote login via SSH at any time. (source, docs)

Go back to menu.

Mac OS X post exploitation Metasploit modules

Extract credentials (Mac OS X)

Metasploit module	Description
post/osx/gather/apfs_encrypted_volume_passwd	**Mac OS X APFS Encrypted Volume Password Disclosure** This module exploits a flaw in OSX 10.13 through 10.13.3 that discloses the passwords of encrypted APFS volumes. (source, docs, ref1, ref2)
post/osx/gather/autologin_password	**OSX Gather Autologin Password as Root** This module will steal the plaintext password of any user on the machine with autologin enabled. Root access is required. (source, ref1)
post/osx/gather/enum_keychain	**OS X Gather Keychain Enumeration** This module presents a way to quickly go through the current user's keychains and collect data such as email accounts, servers, passwords and other data. (source)
post/osx/gather/hashdump	**OS X Gather Mac OS X Password Hash Collector** This module dumps SHA-1, LM, NT, and SHA-512 Hashes on OSX. Supports versions 10.3 to 10.14. (source, docs)
post/osx/gather/password_prompt_spoof	**OSX Password Prompt Spoof** Presents a password prompt dialog to a logged-in OSX user. (source, docs, ref1)
post/osx/gather/vnc_password_osx	**OS X Display Apple VNC Password** This module shows Apple VNC Password from Mac OS X High Sierra. (source, docs)

Go back to menu.

Information gathering (Mac OS X)

Metasploit module	Description
post/osx/gather/enum_adium	**OS X Gather Adium Enumeration** This module will collect Adium's account plist files and chat logs from the victim's machine. It also allows to search for pattern to look for in the chat logs. (source)
post/osx/gather/enum_airport	**OS X Gather Airport Wireless Preferences** This module will download OS X Airport Wireless preferences from the victim machine. The preferences file (which is a plist) contains information such as: SSID, Channels, Security Type, Password ID, etc. (source)
post/osx/gather/enum_chicken_vnc_profile	**OS X Gather Chicken of the VNC Profile** This module will download the "Chicken of the VNC" client application's profile file, which is used to store other VNC servers' information such as the IP and password. (source)
post/osx/gather/enum_colloquy	**OS X Gather Colloquy Enumeration** This module will collect Colloquy's info plist file and chat logs from the victim's machine. It also allows to search for a specific patterns in the chat logs. (source)
post/osx/gather/enum_messages	**OS X Gather Messages** This module will collect the Messages sqlite3 database files and chat logs from the victim's machine. There are four actions you may choose: DBFILE, READABLE, LATEST, and ALL. DBFILE and READABLE will retrieve all messages, and LATEST will retrieve the last X number of messages (useful with 2FA). (source)
post/osx/gather/enum_osx	**OS X Gather Mac OS X System Information Enumeration** This module gathers basic system information from Mac OS X Tiger (10.4), through Mojave (10.14). (source, docs)
post/osx/gather/safari_lastsession	**OSX Gather Safari LastSession.plist** This module downloads the LastSession.plist file from the target machine. LastSession.plist is used by Safari to track active websites in the current session, and sometimes contains sensitive information such as usernames and passwords. This module will first download the original LastSession.plist, and then attempt to find the credential for Gmail. The Gmail's last session state may contain the user's credential if his/her first login attempt failed (likely due to a typo and then the page got refreshed or another login attempt was made. This also means the stolen credential might contain typos. (source, ref1)

Go back to menu.

Spy / Capture (Mac OS X)

Metasploit module	Description
post/osx/capture/keylog_recorder	**OSX Capture Userspace Keylogger** Logs all keyboard events except cmd-keys and GUI password input. Keylogs are transferred between client/server in chunks every SYNCWAIT seconds for reliability. (source)
post/osx/capture/screen	**OSX Screen Capture** This module takes screenshots of target desktop and automatically downloads them. (source, docs)
post/osx/manage/record_mic	**OSX Manage Record Microphone** This module will allow the user to detect (with the LIST action) and capture (with the RECORD action) audio inputs on a remote OSX machine. (source)
post/osx/manage/webcam	**OSX Manage Webcam** This module will allow the user to detect installed webcams (with the LIST action), take a snapshot (with the SNAPSHOT action), or record a webcam and mic (with the RECORD action). (source)

Go back to menu.

Generic / Other (Mac OS X)

Metasploit module	Description
post/osx/admin/say	**OS X Text to Speech Utility** This module will speak whatever is in the 'TEXT' option on the victim machine. (source, docs, ref1)
post/osx/escalate/tccbypass	**Bypass the macOS TCC Framework** This module exploits a vulnerability in the TCC daemon on macOS Catalina (≤ 10.15.5) in order to grant TCC entitlements. The TCC daemon can be manipulated (by setting the HOME environment variable) to use a new user controlled location as the TCC database. We can then grant ourselves entitlements by inserting them into this new database. (source, docs, ref1, ref2)
post/osx/manage/mount_share	**OSX Network Share Mounter** This module lists saved network shares and tries to connect to them using stored credentials. This does not require root privileges. (source)
post/osx/manage/sonic_pi	**OS X Manage Sonic Pi** This module controls Sonic Pi via its local OSC server. The server runs on 127.0.0.1:4557 and receives OSC messages over UDP. Yes, this is RCE, but it's local. I suggest playing music 🙂 (source, docs, ref1, ref2, ref3)
post/osx/manage/vpn	**OSX VPN Manager** This module lists VPN connections and tries to connect to them using stored credentials. (source)

Go back to menu.

UNIX post exploitation modules

AIX post exploitation modules

Metasploit module	Description
post/aix/hashdump	**AIX Gather Dump Password Hashes** Post module to dump the password hashes for all users on an AIX System. (source)

BSD post exploitation modules

Metasploit module	Description
post/bsd/gather/hashdump	**BSD Dump Password Hashes** Post module to dump the password hashes for all users on a BSD system. (source, docs)

Solaris post exploitation modules

Metasploit module	Description
post/solaris/escalate/pfexec	**Solaris pfexec Upgrade Shell** This module attempts to upgrade a shell session to UID 0 using pfexec. (source, docs, ref1, ref2, ref3)
post/solaris/escalate/srsexec_readline	**Solaris srsexec Arbitrary File Reader** This module exploits a vulnerability in NetCommander 3.2.3 and 3.2.5. The most widely accepted exploitation vector is reading /etc/shadow, which will reveal root's hash for cracking. (source, docs, ref1, ref2)
post/solaris/gather/checkvm	**Solaris Gather Virtual Environment Detection** This module attempts to determine whether the system is running inside of a virtual environment and if so, which one. This module supports detection of Solaris Zone, VMWare, VirtualBox, Xen, and QEMU/KVM. (source)
post/solaris/gather/enum_packages	**Solaris Gather Installed Packages** Post module to enumerate installed packages on a Solaris System. (source)
post/solaris/gather/enum_services	**Solaris Gather Configured Services** Post module to enumerate services on a Solaris System. (source)
post/solaris/gather/hashdump	**Solaris Gather Dump Password Hashes for Solaris Systems** Post module to dump the password hashes for all users on a Solaris System. (source)

Go back to menu.

Browser post exploitation modules

Mozilla Firefox post exploitation modules

Metasploit module	Description
post/firefox/gather/cookies	**Firefox Gather Cookies from Privileged Javascript Shell** This module allows collection of cookies from a Firefox Privileged Javascript Shell. (source)
post/firefox/gather/history	**Firefox Gather History from Privileged Javascript Shell** This module allows collection of the entire browser history from a Firefox Privileged Javascript Shell. (source)
post/firefox/gather/passwords	**Firefox Gather Passwords from Privileged Javascript Shell** This module allows collection of passwords from a Firefox Privileged Javascript Shell. (source, docs)
post/firefox/gather/xss	**Firefox XSS** This module runs the provided SCRIPT as JavaScript in the origin of the provided URL. It works by navigating to a hidden ChromeWindow to the URL, then injecting the SCRIPT with Function(). The callback “send(result)” is used to send data back to the listener. (source)
post/firefox/manage/webcam_chat	**Firefox Webcam Chat on Privileged Javascript Shell** This module allows streaming a webcam from a privileged Firefox Javascript shell. (source, ref1)
post/multi/gather/firefox_creds	**Multi Gather Firefox Signon Credential Collection** This module will collect credentials and cookies from the Firefox web browser found on the system. Firefox stores passwords within the signons.sqlite database file. There is also a keys3.db file which contains the key for decrypting these passwords. In cases where a Master Password has not been set, the passwords can easily be decrypted using the referenced 3rd party tools or by setting the DECRYPT option to true. Platforms: bsd, linux, osx, unix, win (source, ref1, ref2)

Google Chrome post exploitation modules

Metasploit module	Description
post/multi/gather/chrome_cookies	**Chrome Gather Cookies** Read all cookies from the Default Chrome profile of the target user. Platforms: linux, unix, bsd, osx, windows (source, docs)
post/windows/gather/enum_chrome	**Windows Gather Google Chrome User Data Enumeration** This module will collect user data from Google Chrome and attempt to decrypt sensitive information. (source, docs)

Internet Explorer post exploitation modules

Metasploit module	Description
post/windows/gather/enum_ie	**Windows Gather Internet Explorer User Data Enumeration** This module will collect history, cookies, and credentials (from either HTTP auth passwords, or saved form passwords found in auto-complete) in Internet Explorer. The ability to gather credentials is only supported for versions of IE ≥7, while history and cookies can be extracted for all versions. (source, docs)
post/windows/manage/ie_proxypac	**Windows Manage Proxy PAC File** This module configures Internet Explorer to use a PAC proxy file. By using the LOCAL_PAC option, a PAC file will be created on the victim host. It’s also possible to provide a remote PAC file (REMOTE_PAC option) by providing the full URL. (source, ref1, ref2)

Multi browser post exploitation modules

Metasploit module	Description
post/multi/manage/hsts_eraser	**Web browsers HSTS entries eraser** This module removes the HSTS (HTTP Strict Transport Security) database of the following tools and web browsers: Mozilla Firefox, Google Chrome, Opera, Safari and wget. Platforms: linux, osx, unix, win (source, docs, ref1, ref2)
post/windows/gather/forensics/browser_history	**Windows Gather Skype, Firefox, and Chrome Artifacts** Gathers Skype chat logs, Firefox history, and Chrome history data from the target machine. (source)

Go back to menu.

Hardware post exploitation modules

Automotive post exploitation modules

Metasploit module	Description
post/hardware/automotive/canprobe	**Module to Probe Different Data Points in a CAN Packet** Scans between two CAN IDs and writes data at each byte position. It will either write a set byte value (Default 0xFF) or iterate through all possible values of that byte position (takes much longer). Does not check for responses and is basically a simple blind fuzzer. (source, docs)
post/hardware/automotive/can_flood	**CAN Flood** This module floods a CAN interface with supplied frames. (source, docs)
post/hardware/automotive/getvinfo	**Get the Vehicle Information Such as the VIN from the Target Module** Post module to query DTCs, Some common engine info and Vehicle Info. It returns such things as engine speed, coolant temp, Diagnostic Trouble Codes as well as All info stored by Mode $09 Vehicle Info, VIN, etc. (source, docs)
post/hardware/automotive/identifymodules	**Scan CAN Bus for Diagnostic Modules** Post module to scan the CAN bus for any modules that can respond to UDS DSC queries. (source, docs)
post/hardware/automotive/malibu_overheat	**Sample Module to Flood Temp Gauge on 2006 Malibu** Simple sample temp flood for the 2006 Chevrolet Malibu. (source)
post/hardware/automotive/mazda_ic_mover	**Mazda 2 Instrument Cluster Accelorometer Mover** This module moves the needle of the accelorometer and speedometer of the Mazda 2 instrument cluster. (source, docs)
post/hardware/automotive/pdt	**Check For and Prep the Pyrotechnic Devices (Airbags, Battery Clamps, etc.)** Acting in the role of a Pyrotechnical Device Deployment Tool (PDT), this module will first query all Pyrotechnic Control Units (PCUs) in the target vehicle to discover how many pyrotechnic devices are present, then attempt to validate the security access token using the default simplified algorithm. On success, the vehicle will be in a state that is prepped to deploy its pyrotechnic devices (e.g. airbags, battery clamps, etc.) via the service routine. (ISO 26021). (source, docs, ref1)

Go back to menu.

Networking equipment post exploitation

Metasploit module	Description
post/hardware/zigbee/zstumbler	**Sends Beacons to Scan for Active ZigBee Networks** Post module to send beacon signals to the broadcast address while channel hopping. (source, docs)
post/networking/gather/enum_brocade	**Brocade Gather Device General Information** This module collects Brocade device information and configuration. It has been tested against an icx6430 running 08.0.20T311. (source, docs)
post/networking/gather/enum_cisco	**Cisco Gather Device General Information** This module collects a Cisco IOS or NXOS device information and configuration. (source, docs)
post/networking/gather/enum_f5	**F5 Gather Device General Information** This module collects a F5's device information and configuration. (source, docs)
post/networking/gather/enum_juniper	**Juniper Gather Device General Information** This module collects a Juniper ScreenOS and JunOS device information and configuration. (source, docs)
post/networking/gather/enum_mikrotik	**Mikrotik Gather Device General Information** This module collects Mikrotik device information and configuration. It has been tested against RouterOS 6.45.9. (source, docs)
post/networking/gather/enum_vyos	**VyOS Gather Device General Information** This module collects VyOS device information and configuration. (source, docs)

Go back to menu.

Radio-frequency devices post exploitation modules

Metasploit module	Description
post/hardware/rftransceiver/rfpwnon	**Brute Force AM/OOK (ie: Garage Doors)** Post module for HWBridge RFTranscievers. Brute forces AM OOK or raw binary signals. This is a port of the rfpwnon tool by Corey Harding. (source, docs, ref1)
post/hardware/rftransceiver/transmitter	**RF Transceiver Transmitter** This module powers an HWBridge-connected radio transceiver, effectively transmitting on the frequency set by the FREQ option. NOTE: Users of this module should be aware of their local laws, regulations, and licensing requirements for transmitting on any given radio frequency. (source, docs, ref1)

Go back to menu.

Mobile devices post exploitation modules

Android post exploitation modules

Metasploit module	Description
post/android/capture/screen	**Android Screen Capture** This module takes a screenshot of the target phone display screen. (source, docs)
post/android/gather/hashdump	**Android Gather Dump Password Hashes for Android Systems** Post module to dump the password hashes for Android System. Root is required. (source, docs, ref1, ref2)
post/android/gather/sub_info	**Extracts subscriber info from target device** This module displays the subscriber info stored on the target phone. It uses call service to get values of each transaction code like imei etc. (source, docs)
post/android/gather/wireless_ap	**Displays wireless SSIDs and PSKs** This module displays all wireless AP creds saved on the target device. (source, docs)
post/android/manage/remove_lock	**Android Settings Remove Device Locks (4.0-4.3)** This module exploits a bug in the Android 4.0 to 4.3 com.android.settings.ChooseLockGeneric class. Any unprivileged app can exploit this vulnerability to remove the lockscreen and the device will be unlocked by a swipe. This vulnerability was patched in Android 4.4. (source, ref1, ref2)
post/android/manage/remove_lock_root	**Android Root Remove Device Locks (root)** This module uses root privileges to remove the device lock. In some cases the original lock method will still be present but any key/gesture will unlock the device. (source, docs)

Go back to menu.

Apple iOS post exploitation modules

Metasploit module	Description
post/apple_ios/gather/ios_image_gather	**iOS Image Gatherer** This module collects images from iPhones. Module was tested on iOS 10.3.3 on an iPhone 5. (source, docs)
post/apple_ios/gather/ios_text_gather	**iOS Text Gatherer** This module collects text messages from iPhones. Tested on iOS 10.3.3 on an iPhone 5. (source, docs)

Go back to menu.

Conclusion

Thank you for checking this list, hope it can help you in your work and please let me know your thoughts in the comment section below!

If you find this reference list useful and you would like more content like it, please subscribe to our mailing list and follow InfosecMatter on Twitter and Facebook and you will get notifications about new additions. You can also support this website through a donation.

See also

- Metasploit Auxiliary Modules (Detailed Spreadsheet)
- Metasploit Windows Exploits (Detailed Spreadsheet)
- Metasploit Linux Exploits (Detailed Spreadsheet)
- Metasploit Payloads (Detailed Spreadsheet)
- Metasploit Android Modules
- Metasploit Module Library