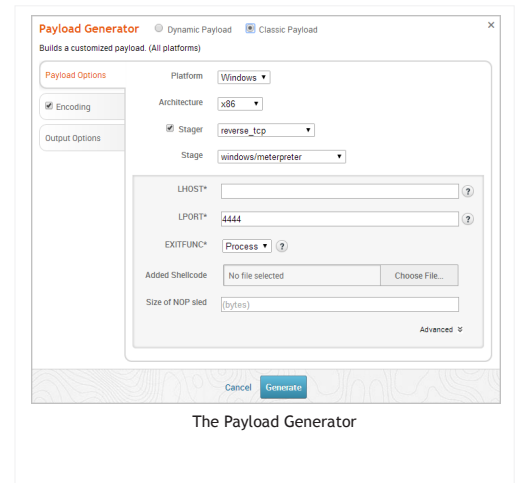


With Metasploit Pro, you can build payloads with the Payload Generator. The Payload Generator provides a guided interface that you can use to quickly build a standalone binary file that executes a payload. Binary files, such as .exe and .bin files, are typically delivered through client-side exploits, such as phishing e-mails or social engineering attacks.

You can use the Payload Generator to build a dynamic payload or a classic payload. Depending on the type of payload you choose to build, the Payload Generator will display the applicable options that you can use to customize the payload. All payloads are generated on the fly and are available for a one time download.

This tutorial will show you how to generate executables for two common payloads: Windows Meterpreter reverse TCP and Linux Meterpreter reverse TCP.



Tutorial Objectives

- Set up persistent listeners for Windows and Java payloads
- Generate a windows/meterpreter/reverse_tcp executable payload
- Generate a linux/meterpreter/reverse_tcp executable payload

Payload Terminology

Listener	The component that waits for an incoming connection from an exploited system.
Payload	The shellcode that executes on the target system.
Payload Generator	A Metasploit feature that you use to build payloads.
Stager	The component that sets up the network connection between the target machine and the payload handler running on the Metasploit server. It enables you to use a smaller payload to load and inject a larger, more complex payload called the stage.
Stage	The payload that is delivered by the stager.
Staged Payload	A payload that is used to deliver larger, more complex payloads to the target when there are space constraints in the exploit. It consists of the stager and stage.

Before You Begin

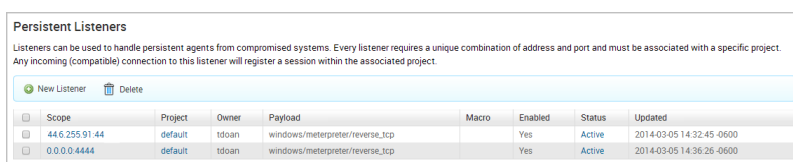
Clear your browser's cache	<p>After you install or update Metasploit, you must clear your browser's cache to ensure that all user interface elements load properly.</p> <p>To learn how to clear the browser cache, visit the documentation for your web browser.</p>
-----------------------------------	--

Windows Meterpreter Reverse TCP Payloads

Step 1: Set Up a Persistent Listener for Windows Meterpreter Payloads

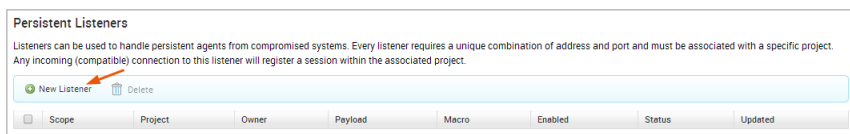
Before you build the Windows Meterpreter payload, you will need to set up a listener for it. A listener is the component that waits for an incoming connection from an exploited system and enables you to establish a connection between your Metasploit server and the exploited machine.

1. Open a web browser and go to <https://localhost:3790> if Metasploit Pro runs on your local machine. If Metasploit Pro isn't installed locally, replace localhost with the address of the remote machine.
2. Log in to the Metasploit Pro web interface.
3. Select **Administration > Global Settings** from the main tool bar.
4. Find the Persistent Listeners section.

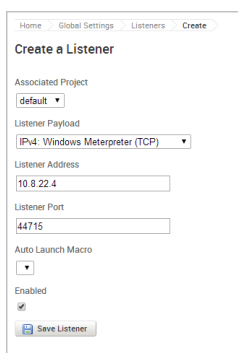


Scope	Project	Owner	Payload	Macro	Enabled	Status	Updated
44.6.255.91:44	default	tdoan	windows/meterpreter/reverse_tcp		Yes	Active	2014-03-05 14:32:45 -0600
0.0.0.4444	default	tdoan	windows/meterpreter/reverse_tcp		Yes	Active	2014-03-05 14:36:26 -0600

3. Click the **New Listener** button.



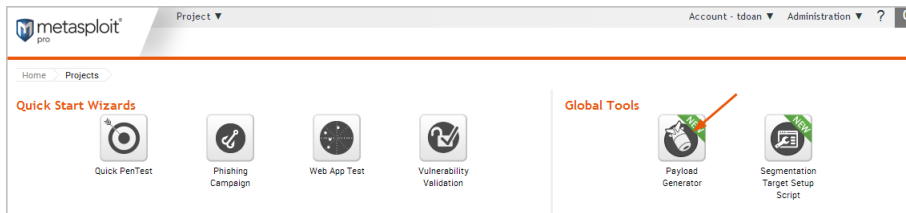
4. When the Create a Listener form appears, specify the following:



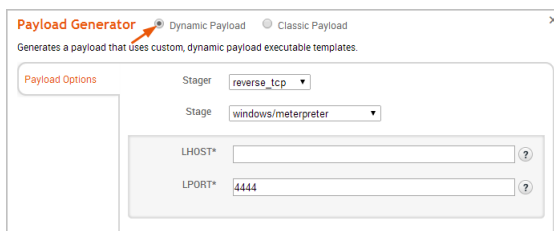
- **Associated project** - Choose the project you want to use to access and manage open sessions.
 - **Listener payload** - Choose **IPv4: Windows Meterpreter (TCP)**.
 - **Listener Address** - Specify the IP address that you want the payload to connect back to (e.g., the IP address of the Metasploit server).
 - **Listener Port** - Specify the port you've set up for the handler when you generated the Windows Meterpreter Reverse TCP payload (e.g., 4444).
5. Save the listener.

Step 2: Generate a Windows Meterpreter Reverse TCP Payload

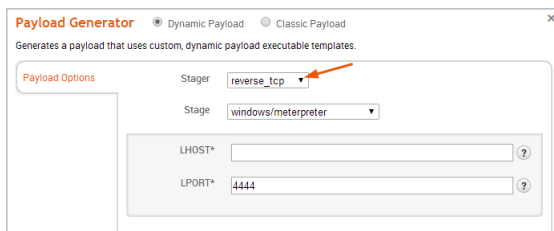
1. Select **Project > Show Projects** from the main menu to view the Projects List.
2. When the Projects List appears, launch the Payload Generator. It is located under the Global Tools.



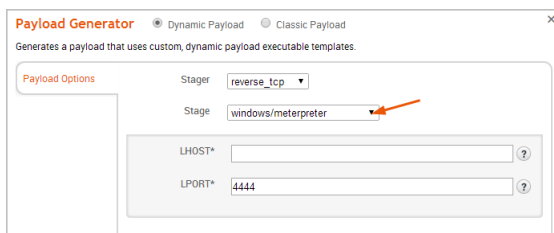
3. Select the **Dynamic Payload** option.



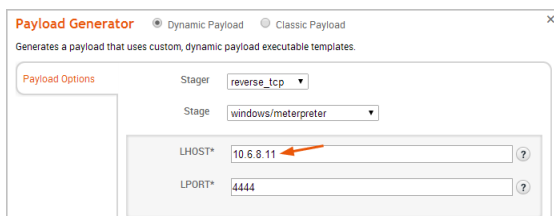
4. Click the **Stager** dropdown and choose **reverse_tcp**.



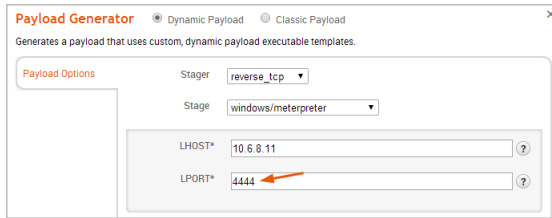
5. Click the **Stage** dropdown and choose **windows/meterpreter**.



6. Enter the IP address of the listener you set up earlier in the **LHOST** field.



7. Enter the port of the listener you set up earlier in the **LPORT** field.



Dynamic Payload

Generates a payload that uses custom, dynamic payload executable templates.

Stager: reverse_tcp

Stage: windows/meterpreter

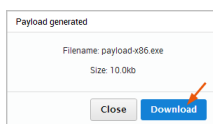
LHOST*: 10.6.8.11

LPORT*: 4444

8. Generate the payload.

A progress bar appears and shows you the status of the payload generation. When the payload has been generated, a Download button appears.

9. Click the **Download** button to save the payload.



The download process will automatically start. If your browser is not configured to automatically download files, a dialog window will appear and prompt you to save the file.

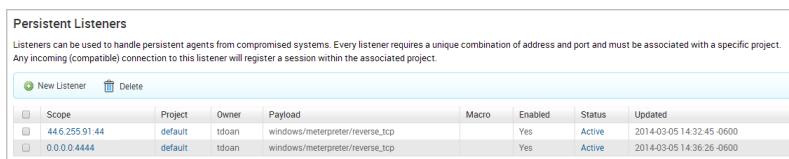
Step 3: Deliver the Executable and Wait for a Connection

Now that you have an executable, you'll need to deliver it to a Windows target host using a method such as a USB drop or e-mail. After you deliver the executable to the target, you'll need to check the project that you set up for your listener to wait for open sessions.

Linux Meterpreter Reverse TCP Payloads

Step 1: Set Up a Persistent Listener for Linux Meterpreter Payloads

1. Select **Administration > Global Settings**.
2. Find the Persistent Listeners section.

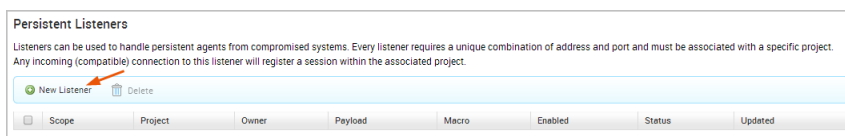


Persistent Listeners

Listeners can be used to handle persistent agents from compromised systems. Every listener requires a unique combination of address and port and must be associated with a specific project. Any incoming (compatible) connection to this listener will register a session within the associated project.

Scope	Project	Owner	Payload	Macro	Enabled	Status	Updated
44.6.255.91.44	default	tdoan	windows/meterpreter/reverse_tcp	Yes	Active	2014-03-05 14:32:45 -0600	
0.0.0.4444	default	tdoan	windows/meterpreter/reverse_tcp	Yes	Active	2014-03-05 14:36:26 -0600	

3. Click the **New Listener** button.



Persistent Listeners

Listeners can be used to handle persistent agents from compromised systems. Every listener requires a unique combination of address and port and must be associated with a specific project. Any incoming (compatible) connection to this listener will register a session within the associated project.

New Listener Delete

Scope	Project	Owner	Payload	Macro	Enabled	Status	Updated
-------	---------	-------	---------	-------	---------	--------	---------

- When the Create a Listener form appears, specify the following:

Create a Listener

Associated Project
default

Listener Payload
IPv4: Java Meterpreter (TCP)

Listener Address
10.8.22.4

Listener Port
19236

Auto Launch Macro
Enabled

Save Listener

- Associated project** - Choose the project you want to use to access and manage open sessions.
- Listener payload** - Choose **IPv4: Java Meterpreter (TCP)**.
- Listener Address** - Specify the IP address that you want the payload to connect back to (e.g., the IP address of the Metasploit server).
- Listener Port** - Specify the port you set up for the handler when you generated the Windows Meterpreter Reverse TCP payload (e.g., 4444).

- Save the listener.

Step 2: Generate a Linux Meterpreter Reverse TCP Payload

- Select **Project > Show Projects** from the main menu to view the Projects List.
- When the Projects List appears, launch the Payload Generator. It is located under the Global Tools.
- Select the **Classic Payload** option.

Payload Generator Dynamic Payload Classic Payload

Builds a customized payload. (All platforms)

Platform Windows

Architecture x86

Stager reverse_tcp

Stage windows/meterpreter

- Click the **Platform** dropdown and choose **Linux**.

Payload Generator Dynamic Payload Classic Payload

Builds a customized payload. (All platforms)

Platform Linux

Architecture x86

Stager reverse_tcp

Stage linux/x86/meterpreter

- Click the **Architecture** dropdown and choose **x86**.

Payload Generator Dynamic Payload Classic Payload

Builds a customized payload. (All platforms)

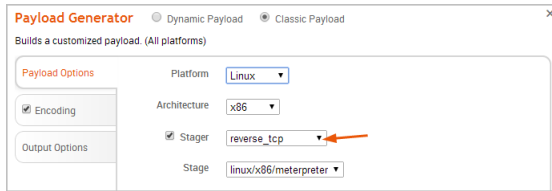
Platform Linux

Architecture x86

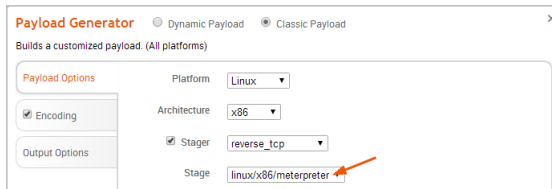
Stager reverse_tcp

Stage linux/x86/meterpreter

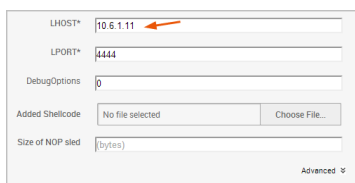
- Click the **Stager** dropdown and choose **reverse_tcp**.



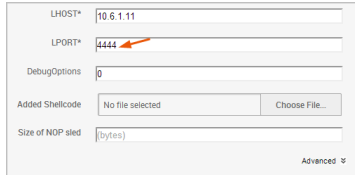
- Click the **Stage** dropdown and choose **linux/x86/meterpreter**.



- Enter the IP address of the listener you set up earlier in the **LHOST** field.



- Enter the port of the listener you set up earlier in the **LPORT** field.



- If you want to add shellcode to the payload, click the **Choose File** button and navigate to the binary file that you want to use.

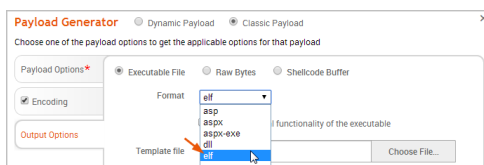
What does the added shellcode do? It adds a wrapper that spawns a separate thread that executes the added bytes in parallel with the main thread. For example, if you want to set the privileges or the user ID, you can add shellcode to the generated payload to perform those tasks.

- Enter the length of the NOP sled that you want to prepend to the payload. (Optional)

What does the NOP sled do? A NOP sled is a series of no operation commands that are added to the payload and do nothing until they hit the execution function.

- Click the **Output Options** tab.

- Click the **Format** dropdown and select **elf**.



15. Generate the payload.

A progress bar appears and shows you the status of the payload generation. When the payload has been generated, a Download button appears.

16. Click the **Download** button to save the payload.

The download process will automatically start. If your browser is not configured to automatically download files, a dialog window will appear and prompt you to save the file.

The next thing you need to do is set up a persistent listener to wait for incoming connections.

Step 3: Deliver the Executable and Wait for a Connection

Now that you have an executable, you'll need to deliver it to a Linux target via USB drop or e-mail. After you deliver the executable to the target, you'll need to check the project that you set up for your listener to look at open sessions.

Support

If you experience any issues with Metasploit Pro, please send an e-mail to support@rapid7.com. Provide a detailed description of the issue you are encountering and describe the steps to reproduce the issue. You may be asked to provide the production log, which is located in `/path/to/Metasploit/apps/pro/ui/log`.