一、介绍

1、简介

CobalStrike是一款渗透测试神器，被业界人称为CS神器。CobaltStrike分为客户端与服务端，服务端只有一个，客户端可以有多个，可悲团队进行分布式协同操作。

2、功能

CobaltStrike集成了端口转发、服务扫描、自动化溢出、多模式端口监听、Windows exe木马生成、Windows dll木马生成、Java木马生成、Office宏病毒生成、木马捆绑。

钓鱼攻击包括：站点克隆、目标信息获取、Java执行、浏览器自动攻击等强大功能。

3、安装（Kali）

```
# jdk
    1、上传jdk压缩包到Kali中，解压
        tar -xzvf jdk-8u191-linux-x64.tar.gz
    2、移动到opt目录
        mv jdk1.8.0_191/ /opt/
    3、进入jdk目录
        cd  /opt/jdk1.8.0_191
    4、添加文件内容
        vim  ~/.bashrc
            # install JAVA JDK
            export JAVA_HOME=/opt/jdk1.8.0_191
            export CLASSPATH=.:${JAVA_HOME}/lib
            export PATH=${JAVA_HOME}/bin:$PATH
            :wq保存并退出
        source ~/.bashrc
    5、执行
        update-alternatives --install /usr/bin/java java
/opt/jdk1.8.0_191/bin/java 1
        update-alternatives --install /usr/bin/javac javac
/opt/jdk1.8.0_191/bin/javac 1
        update-alternatives --set java /opt/jdk1.8.0_191/bin/java
        update-alternatives --set javac /opt/jdk1.8.0_191/bin/javac
    6、查看结果
        update-alternatives --config java
        update-alternatives --config javac
```

```
# CobalStrike
    1、上传CobalStrike压缩包到Kali，解压
        unzip cobaltstrike-linux.zip
    2、进入CobalStrike目录
        cd cobaltstrike-linux/
```

二、基本功能

1、启动

1.1、服务端

```
# 命令
# 1、正常启动
    ./teamserver 192.168.174.137 1234            # 192.168.174.137为ip，1234为密码
# 2、后台运行启动
    nohup ./teamserver 192.168.174.137 1234 &
# 3、修改默认端口
    默认端口为50050，打开teamserveer文件，将其中的50050修改成任意端口号即可。
```

```
# 文件
    agscript                扩展应用文件
    c2lint                  用于检查profile的错误和异常
    teamserver              服务器端启动程序
    cobaltstrike.jar         CobaltStrike核心程序
    cobaltstrike.auth        用于客户端和服务器端认证的文件
    cobaltstrike.store       密钥证书存放文件
```

```
# 目录
    data                    用于保存当前TeamServer的数据
    download                用于保存目标服务器下载的数据
    upload                  上传文件的目录
    logs                    日志文件
    third-party              第三方工具目录
```

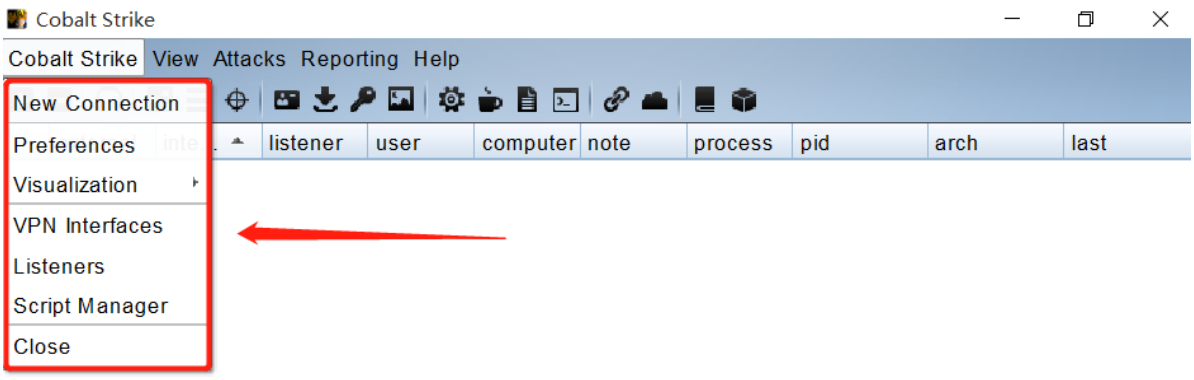
1.2、客户端

```
# Linux
    ./cabalstrike
```

```
# Windows
    直接点击cobaltstrike.exe 或 .bat文件，不同版本启动方式可能存在差异。
```

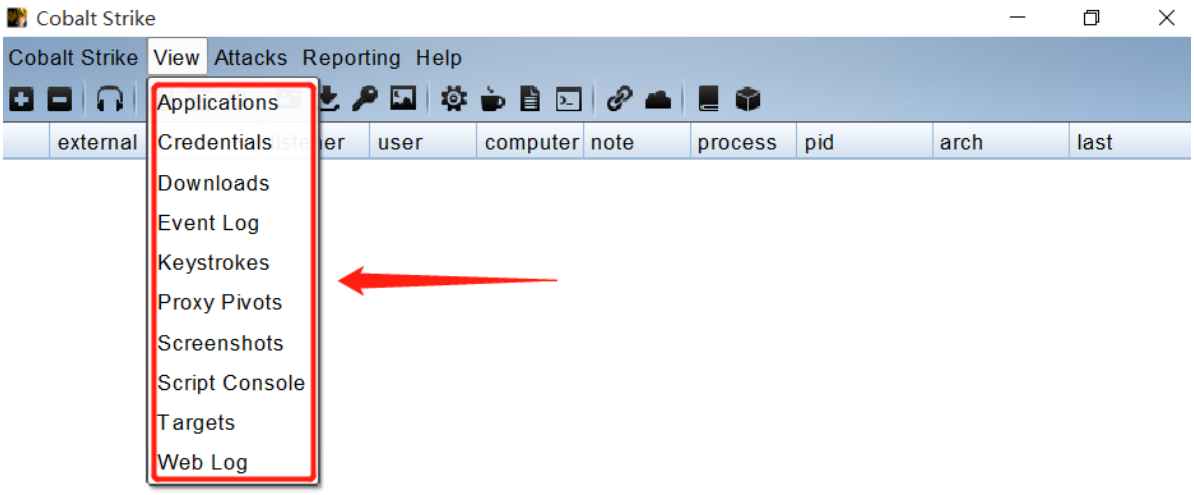
2、参数详解

2.1、Cobalt Strike



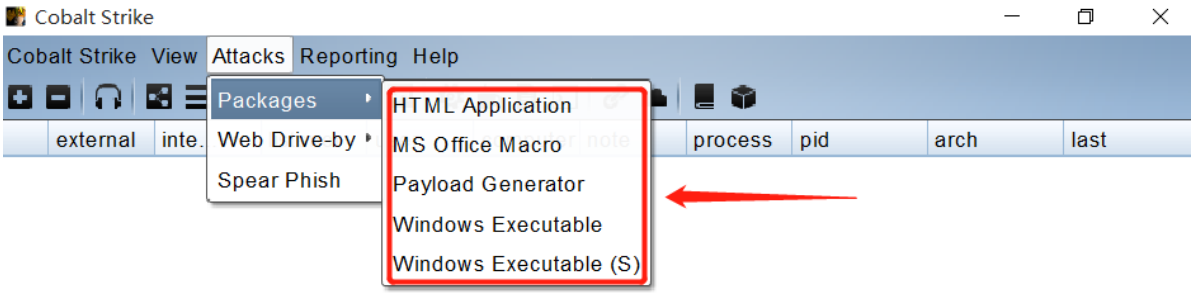
```
New Connection      # 新的连接
Preferences         # 偏好设置
Visualization       # 窗口视图模式
VPN Interfaces      # VPN接入
Listeners           # 监听器
Script Manager      # 脚本管理
Close               # 关闭
```

2.2、View

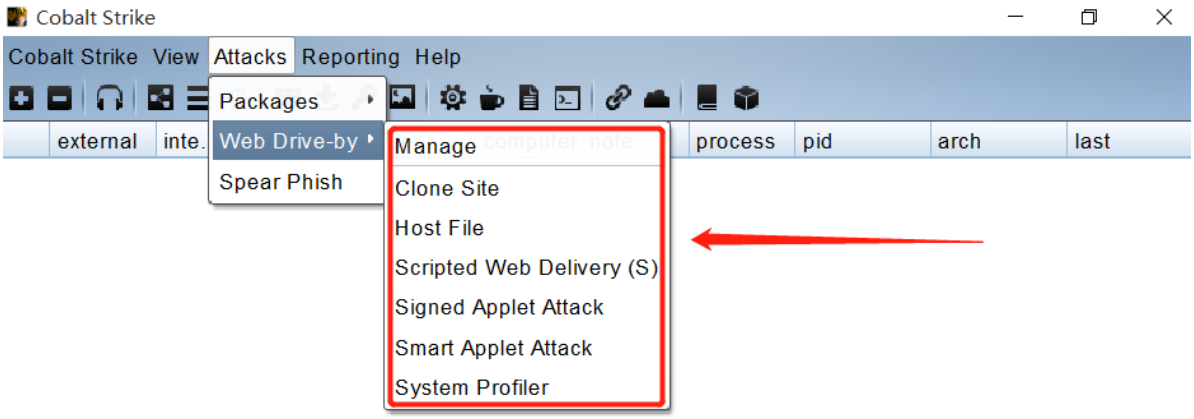



```
Applications        # 应用
Credentials         # 凭证
Downloads           # 下载文件
Event Log           # 事件日志
Keystrokes          # 键盘记录
Proxy Pivots        # 代理模块
Screenshots         # 截图
Script Console      # 脚本控制台
Targets             # 显示目标主机
Web Log             # Web日志
```

2.3、Attacks

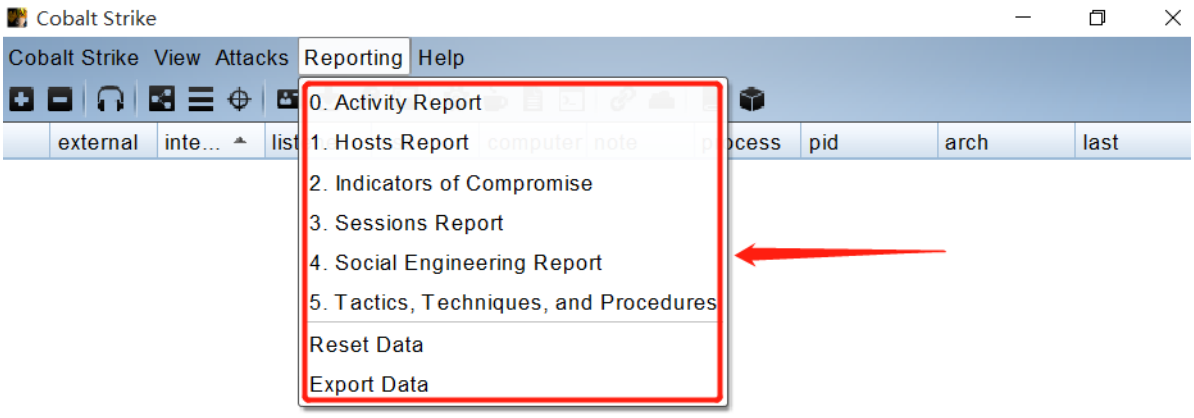


```
# Packages
    HTML Application        # 生成恶意的HTA木马文件
    MS Office Macro         # 生成Office宏病毒文件
    Payload Generator       # 生成各种语言版本的Payload
    USB/CD AutoPlay         # 生成利用自动播放运行的木马文件
    Windows Dropper         # 捆绑器，能够对文档类进行捆绑
    Windows Executable      # 生成可执行Payload
    Windows Executable(s)   # 把包含Payload、Stageless生成可执行文件（包含多数功能）
```



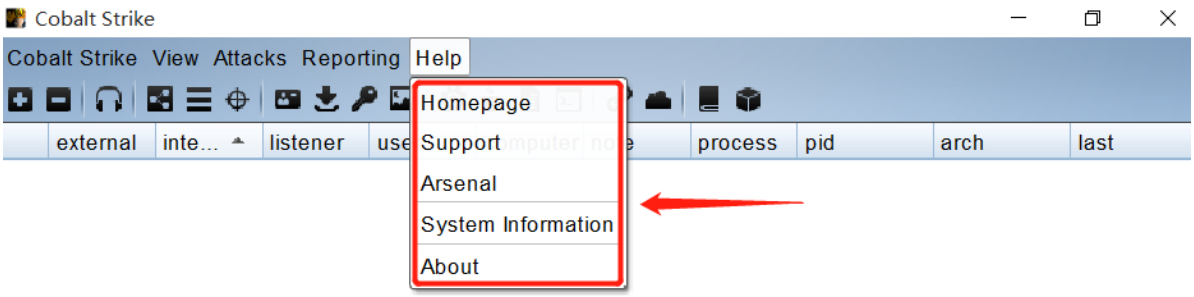

```
# Web Drive-by
    Manage                  # 对开启的Web服务进行管理
    Clone Site              # 克隆网站（可记录受害者提交的数据）
    Host File               # 提供Web以供下载某文件
    Scriptd Web Delivery(s)  # 提供Web服务，便于下载和执行PowerShell Payload
    Signed Applet Attack     # 启动一个Web服务以提供自签名Java Applet的运行环境
    Smart Applet Attack      # 自动检测Java版本并利用已知的Exploits绕过security
    System Profiler          # 获取系统信息，如系统版本、Flash版本、浏览器版本等
```

2.4、Reporting




```
    0.Activity Report                   # 活动报告
    1.Hosts Report                      # 主机报告
    2.Indicators of Compromise           # 威胁报告
    3.Sessions Report                   # 会话报告
    4.Social Engineering Report          # 社会工程学报告
    5.Tactics,Techniques,and Procedures  # 策略、技巧和程序
    Reset Data                          # 重置数据
    Export Data                         # 导出数据
```

2.5、Help




```
Homepage                # 官网主页
Support                 # 技术支持
Arsenal                 # 开发者
System Information       # 版本信息
About                   # 关于
```

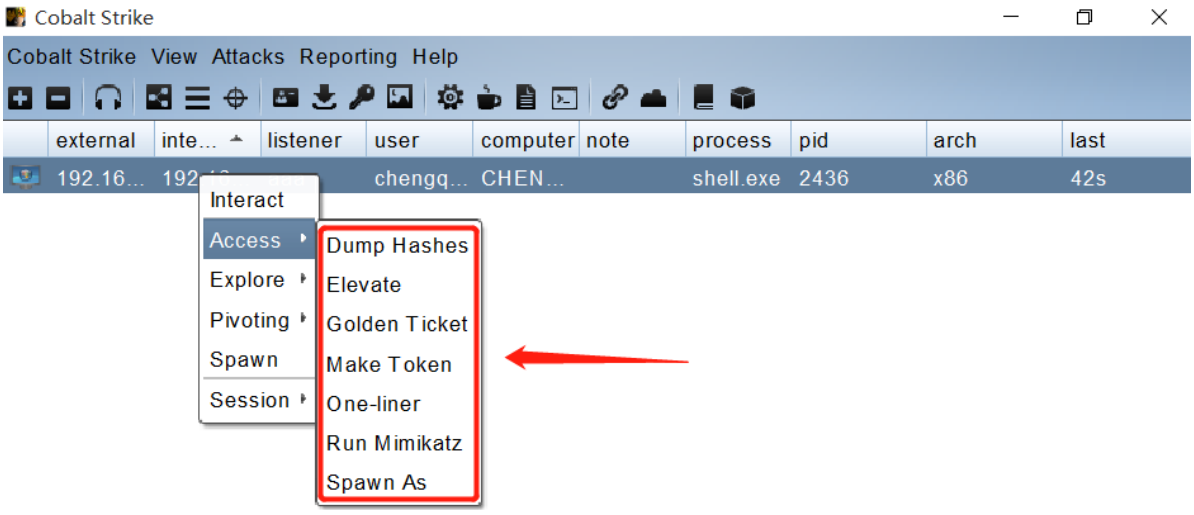
3、右键菜单

3.1、Interact

```
argue                   # 进程参数欺骗
blockdlls               # 阻止子进程加载非Microsoft DLL
browserpivot            # 注入受害者浏览器进程
bypassuac               # 绕过UAC提升权限
cancel                  # 取消正在进行的下载
cd                      # 切换目录
checkin                 # 强制让被控端回连一次
clear                   # 清除beacon内部的任务队列
connect                 # Connect to a Beacon peer over TCP
covertvpn               # 部署Covert VPN客户端
cp                      # 复制文件
dcsync                  # 从DC中提取密码哈希
desktop                 # 远程桌面(VNC)
dllinject               # 反射DLL注入进程
dllload                 # 使用LoadLibrary将DLL加载到进程中
download                # 下载文件
downloads               # 列出正在进行的文件下载
drives                  # 列出目标盘符
elevate                 # 使用exp
execute                 # 在目标上执行程序(无输出)
execute-assembly        # 在目标上内存中执行本地.NET程序
exit                    # 终止beacon会话
getprivs                # Enable system privileges on current token
getsystem               # 尝试获取SYSTEM权限
getuid                  # 获取用户ID
hashdump                # 转储密码哈希值
help                    # 帮助
inject                  # 在注入进程生成会话
jobkill                 # 结束一个后台任务
jobs                    # 列出后台任务
```

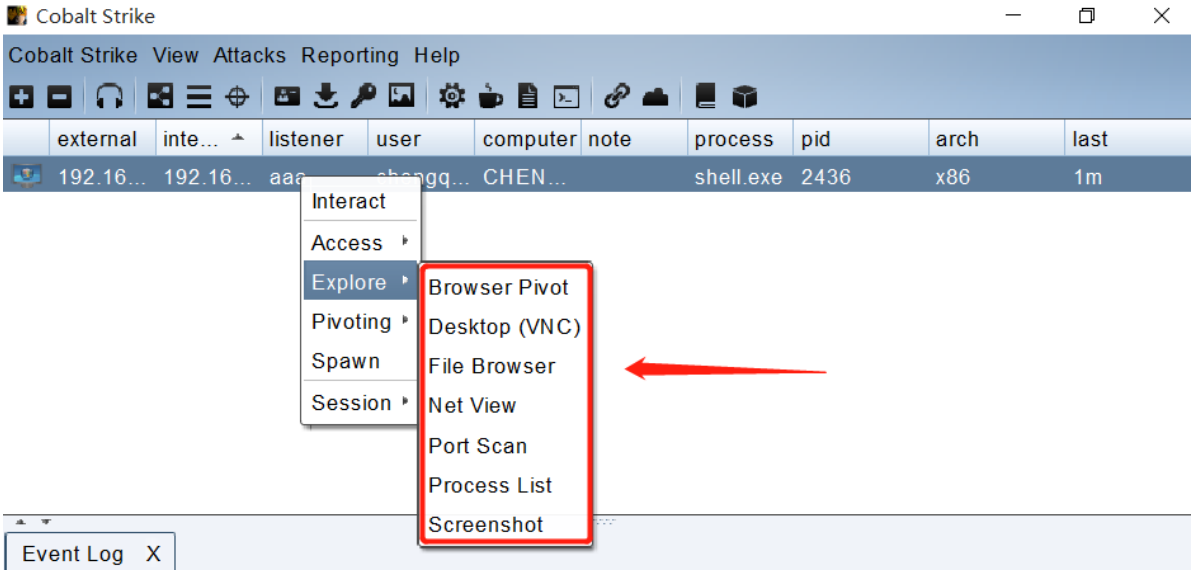
```
kerberos_ccache_use         # 从ccache文件中导入票据应用于此会话
kerberos_ticket_purge       # 清除当前会话的票据
kerberos_ticket_use         # Apply 从ticket文件中导入票据应用于此会话
keylogger                   # 键盘记录
kill                        # 结束进程
link                        # Connect to a Beacon peer over a named pipe
logonpasswords              # 使用mimikatz转储凭据和哈希值
ls                          # 列出文件
make_token                  # 创建令牌以传递凭据
mimikatz                    # 运行mimikatz
mkdir                       # 创建一个目录
mode dns                    # 使用DNS A作为通信通道(仅限DNS beacon)
mode dns-txt                # 使用DNS TXT作为通信通道(仅限D beacon)
mode dns6                   # 使用DNS AAAA作为通信通道(仅限DNS beacon)
mode http                   # 使用HTTP作为通信通道
mv                          # 移动文件
net                         # net命令
note                        # 备注
portscan                    # 进行端口扫描
powerpick                   # 通过Unmanaged PowerShell执行命令
powershell                  # 通过powershell.exe执行命令
powershell-import           # 导入powershell脚本
ppid                        # Set parent PID for spawned post-ex jobs
ps                          # 显示进程列表
psexec                      # Use a service to spawn a session on a host
psexec_psh                  # Use PowerShell to spawn a session on a host
psinject                    # 在特定进程中执行PowerShell命令
pth                         # 使用Mimikatz进行传递哈希
pwd                         # 当前目录位置
reg                         # Query the registry
rev2self                    # 恢复原始令牌
rm                          # 删除文件或文件夹
rportfwd                    # 端口转发
run                         # 在目标上执行程序(返回输出)
runas                       # 以其他用户权限执行程序
runasadmin                  # 在高权限下执行程序
runu                        # Execute a program under another PID
screenshot                  # 屏幕截图
setenv                      # 设置环境变量
shell                       # 执行cmd命令
shinject                    # 将shellcode注入进程
shspawn                     # 启动一个进程并将shellcode注入其中
sleep                       # 设置睡眠延迟时间
socks                       # 启动SOCKS4代理
socks stop                  # 停止SOCKS4
spawn                       # Spawn a session
spawnas                     # Spawn a session as another user
spawnto                     # Set executable to spawn processes into
spawnu                      # Spawn a session under another PID
ssh                         # 使用ssh连接远程主机
ssh-key                     # 使用密钥连接远程主机
steal_token                 # 从进程中窃取令牌
timestomp                   # 将一个文件的时间戳应用到另一个文件
unlink                      # Disconnect from parent Beacon
upload                      # 上传文件
wdigest                     # 使用mimikatz转储明文凭据
winrm                       # 使用WinRM横向渗透
wmi                         # 使用WMI横向渗透
```

3.2、Access



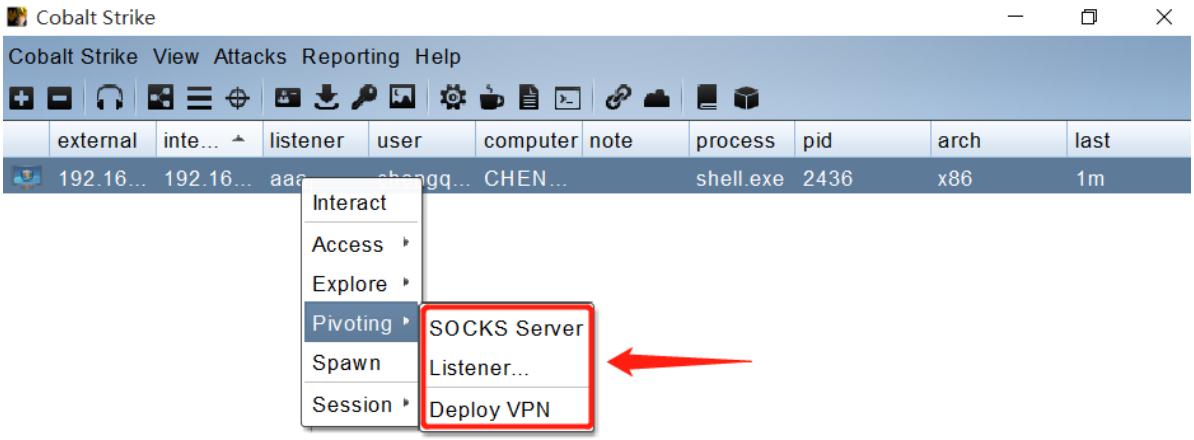

```
Dump Hashes          # 获取hash
Elevate              # 提权
Golden Ticket        # 生成黄金票据注入当前会话
Make Token           # 凭证转换
One-liner
Run Mimikatz         # 运行 Mimikatz
Spawn As             # 用其他用户生成Cobalt Strike监听器
```

3.3、Explore



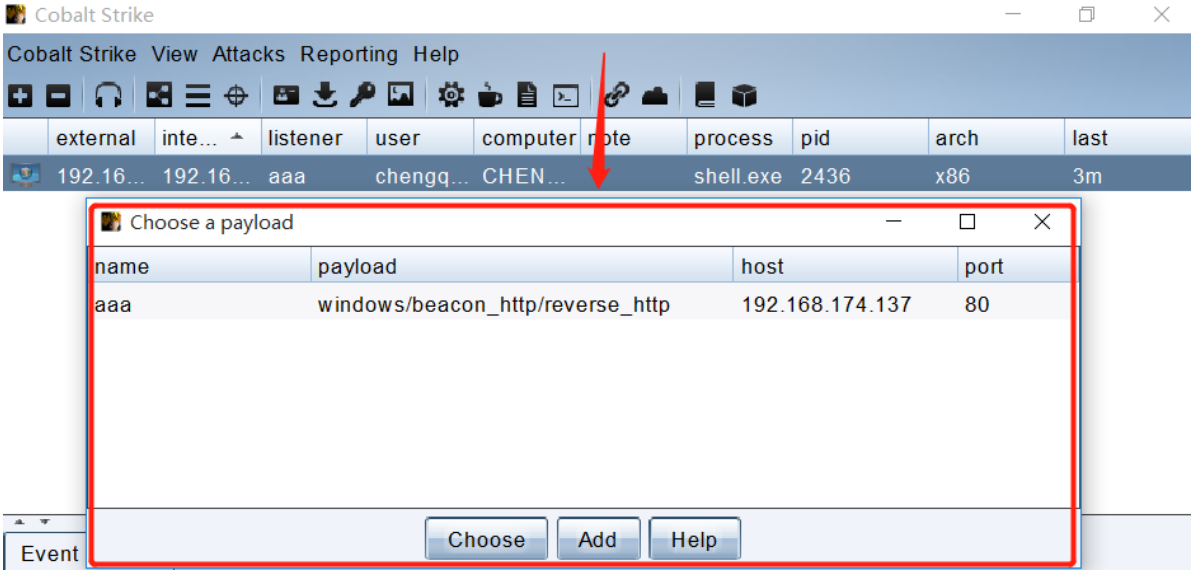

```
Browser Pivot        # 劫持目标浏览器进程
Desktop (VNC)        # 桌面交互
File Browser         # 文件浏览器
Net View             # 命令Net View
Port Scan            # 端口扫描
Process List         # 进程列表
Screenshot           # 截图
```

3.4、Pivoting



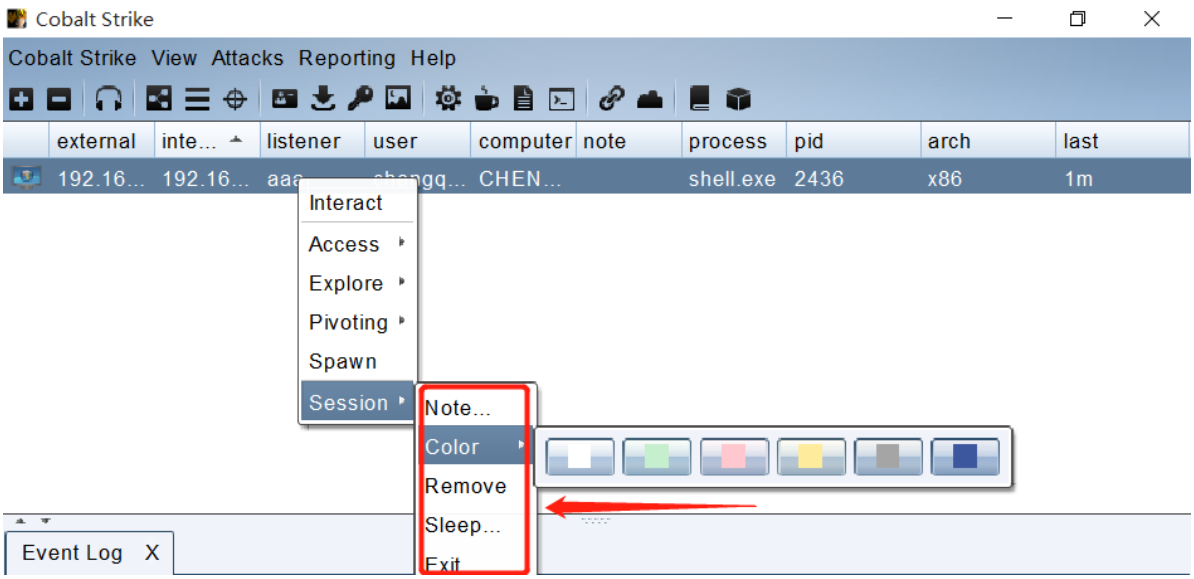

```
SOCKS Server          # 代理服务
Listener...           # 反向端口转发
Deploy VPN            # 部署VPN
```

3.5、Spawn




```
# 外部监听器
```

3.6、Session




```
Note...             # 备注
Color               # 颜色
Remove              # 删除
Sleep               # 指定被控端休眠时间，默认60秒一次回传
Exit                # 退出
```

4、图标按钮


连接到另一个团队服务器。


断开从当前的团队服务器的连接。


新建和编辑 Cobalt Strike 的监听器。


切换为「服务器节点图」的可视化形式。


切换为「会话列表」的可视化形式。


切换为「目标列表」的可视化形式。


查看凭据。


查看下载的文件。


查看键盘记录。


查看屏幕截图。


生成一个无阶段的 Cobalt Strike 可执行文件或 DLL。


设定 Java 签名的 Applet 攻击。


生成一个恶意的 Miscrosoft Office 宏。


建立一个无阶段的脚本的 Web 传送攻击。


在 Cobalt Strike 的 web 服务器上托管一个文件。


管理托管在 Cobalt Strike 的 web 服务器上的文件和应用。


访问 Cobalt Strike 的支持页面。


关于 Cobalt Strike。