4 lab Knyazev

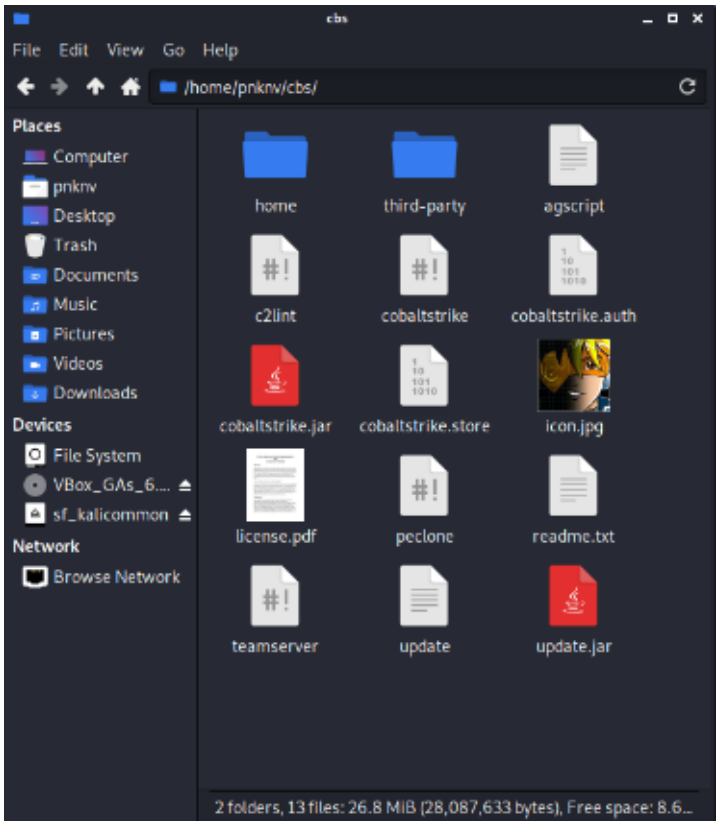
COBALT STRIKE

cobalt strike - это - платный продукт для тестирования на проникновение (пентест), который позволяет злоумышленнику развернуть агент с именем Beacon на машине жертвы. Beacon включает в себя множество функций для злоумышленника, включая, помимо прочего, выполнение команд, регистрацию ключей, передачу файлов, проксирование SOCKS, повышение привилегий, mimikatz, сканирование портов и проникновение в обход защиты.

Beacon находится в памяти / без файлов, так как состоит из безэтапного или многоступенчатого шелл-кода, который после загрузки с использованием уязвимости или выполнения загрузчика шелл-кода загружается в память процесса, не касаясь диска. Он поддерживает промежуточную передачу по HTTP, HTTPS, DNS, SMB, а также прямой и обратный TCP. Cobalt Strike поставляется с набором инструментов для разработки загрузчиков шелл-кода, который называется Artifact Kit.

cobalt strike - уникальна сложная к скачиванию утилита – я перепробовал 5 различных ее версий в течении 7 часов, ломал виртуалку и голову, а потом нашел гайд.

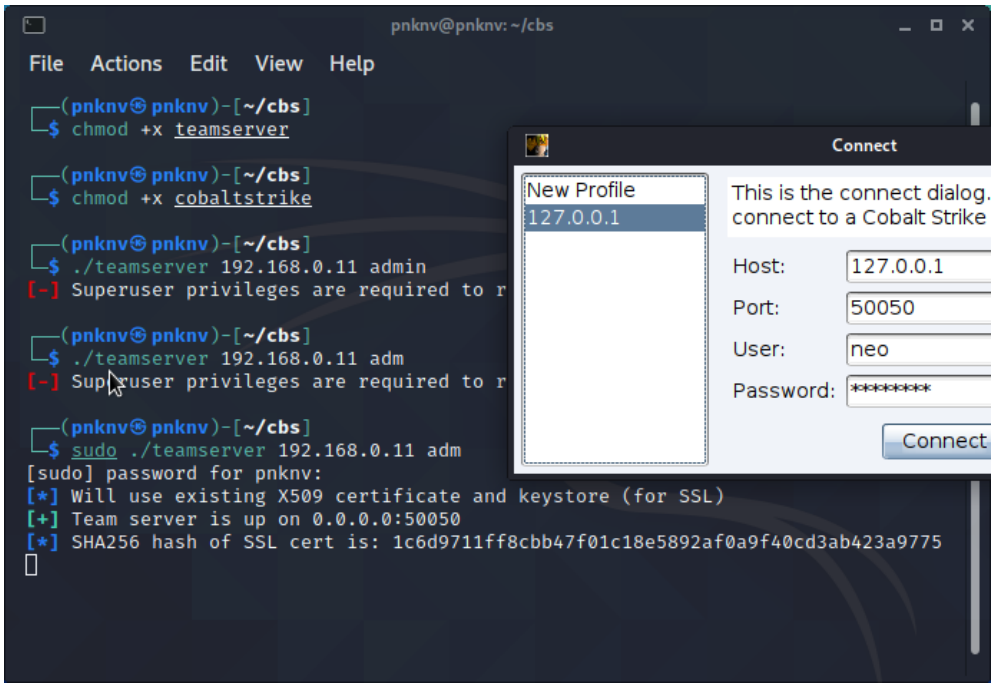
В своем отчете я использовал 4 версию CS. Соержимое папки (рисунок 1):



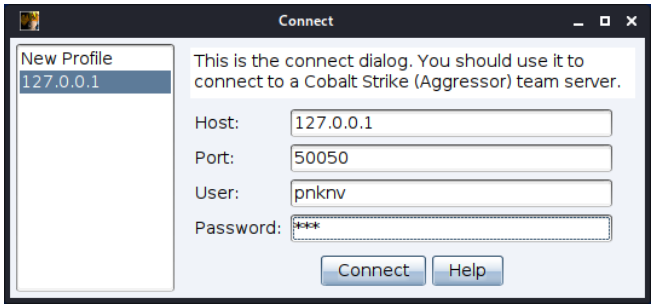
Надо было удалить одну строку из файла cobaltstrike без расширения (рисунок 2):

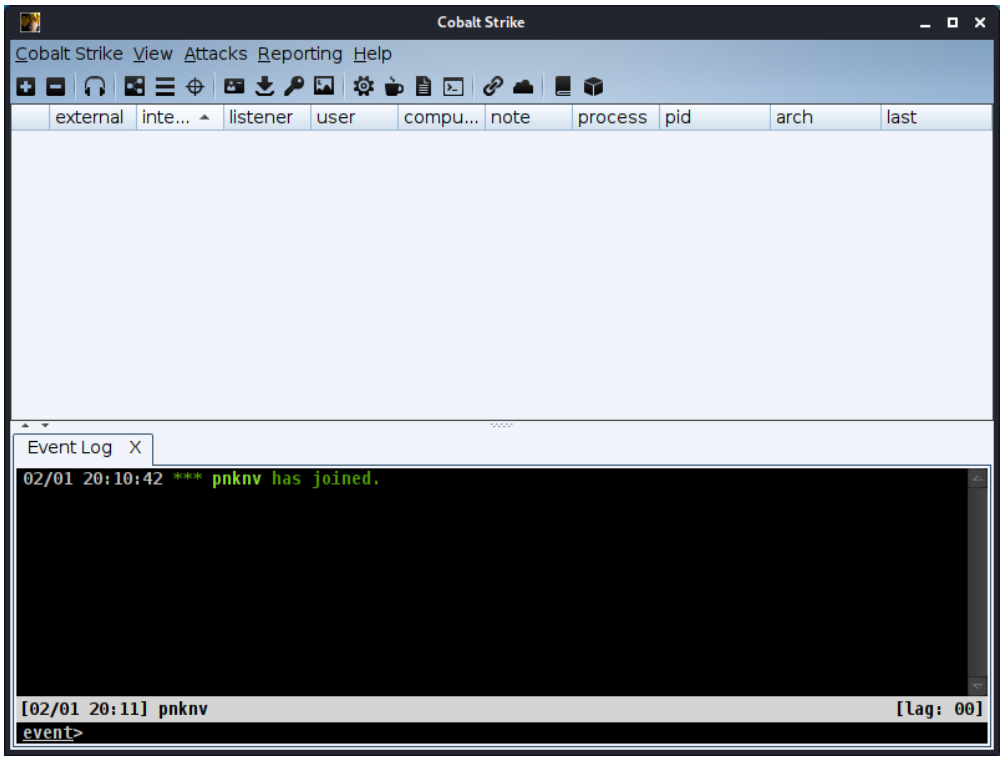
```
#!/bin/bash
export HOME=$PWD/home
mkdir -p "$HOME"
export _JAVA_OPTIONS="$_JAVA_OPTIONS"
java -XX:ParallelGCThreads=4 -XX:+AggressiveHeap -XX:+UseParallelGC -jar cobalts
trike.jar $*
```

После – надо изменить права доступа к файлам CS, teamserver и запустить их с указанными параметрами (рисунок 3): (кобальтстрайк – без параметров: ‘./cobaltstrike’)

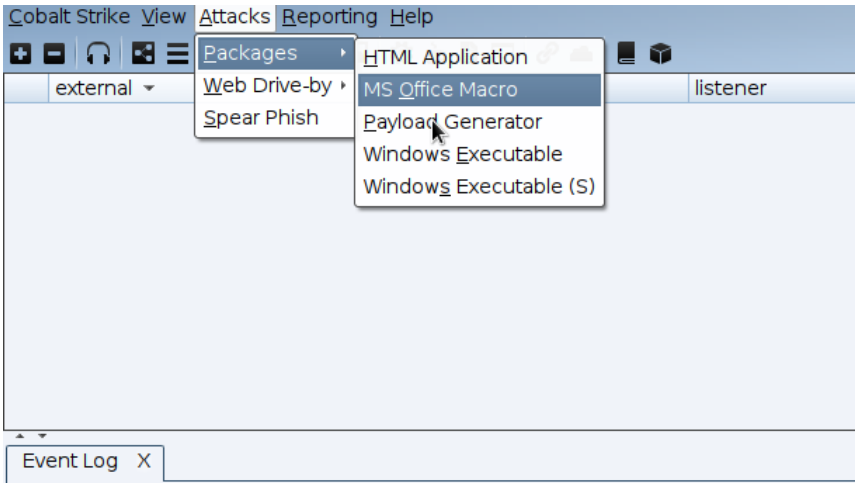


Входим в GUI программы (скриншоты 4, 5):

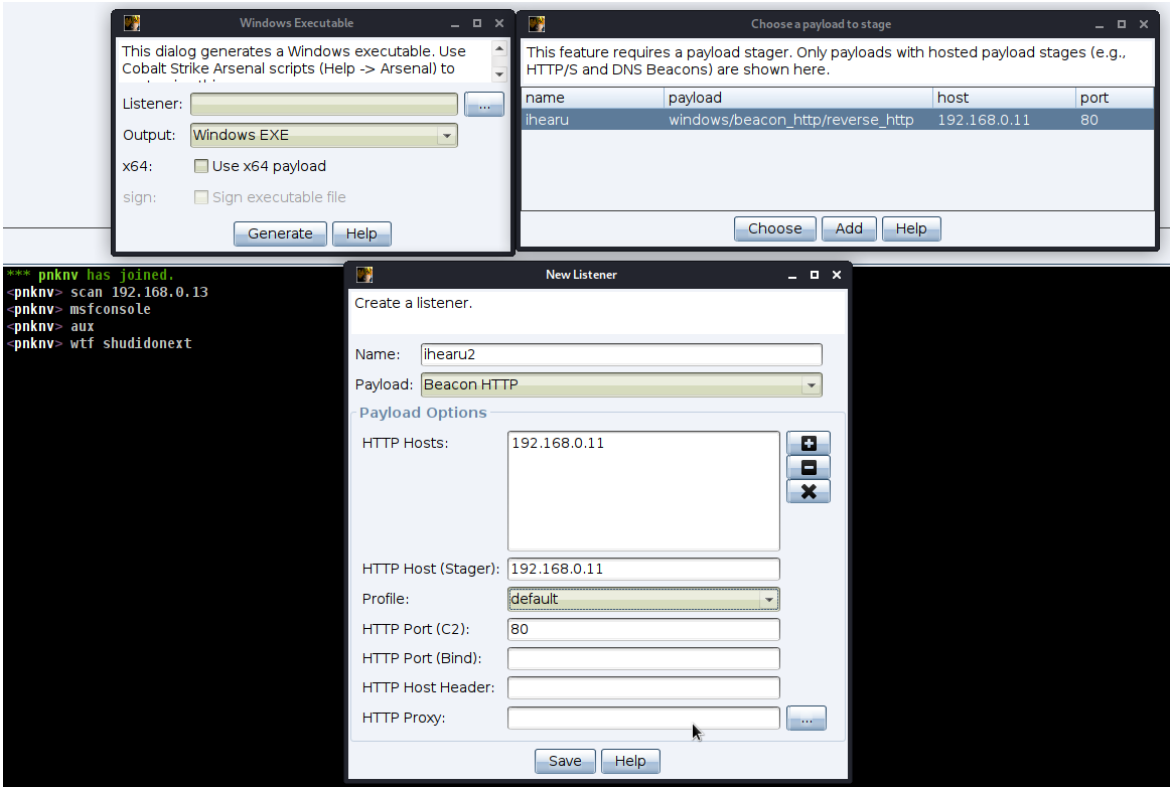




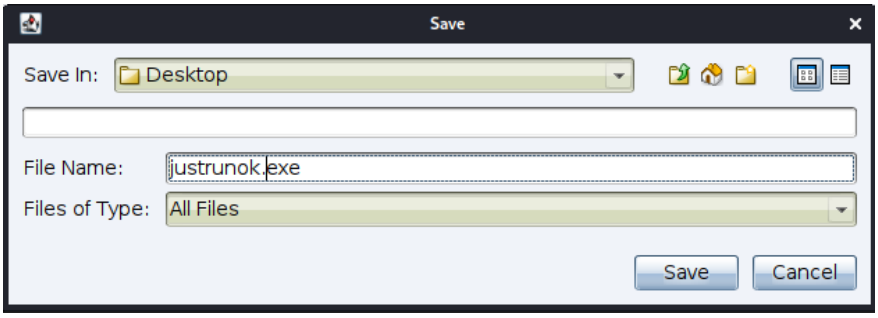
У программ есть много различных возможностей – не зря она так сложно ставится! Используем из всех опций ту, с помощью которой сможем получить .exe пейлоад для винды (скриншоты 6, 7)



Настраиваем listener – из него мы поймем, когда компьютер цели будет инфецирован и сможем выполнять команды на нем, просматривать содержимое, сохранять к себе на устройство:

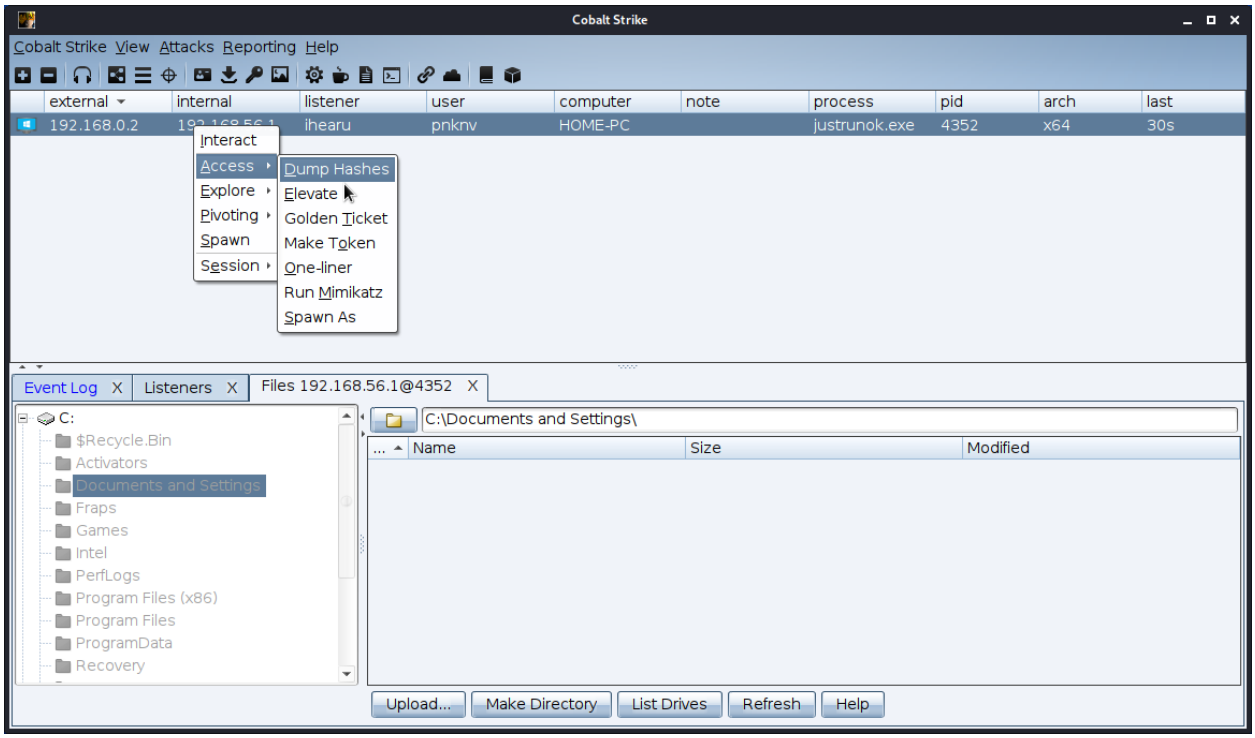


Сохраним .exe, дав ему название justronok.exe (рисунок 8):



Дело за малым – заставить пользователя открыть файл.

После этих действий, окно программы обновляется и мы видим подключенного пользователя. Можем сделать многое – сдампить хеши паролей, повысить привилегии и прочее, что может быть использовано в целях сбора информации о клиенте (рисунок 9)



Так же в графичкском интерфейсе есть красивая визуализация подключенных компов (скрин 10):