[Course | SkillFactory](https://apps.skillfactory.ru/learning/course/course-v1:SKILLFACTORY+hack_pentest+2020/block-v1:SKILLFACTORY+hack_pentest+2020+type@sequential+block@192054eb8246455fa5e3800e06af26b8/block-v1:SKILLFACTORY+hack_pentest+2020+type@vertical+block@85760c514cb5435b91fefefad5450a08)

# 30.5 Практика / Модуль 30. Администрирование с помощью Powershell, написание и эксплуатация при проведении пентеста

0

Установка *Empire:*

git clone https://github.com/BC-SECURITY/Empire.git

cd Empire

sudo ./setup/install.sh

1

С помощью *PowerShell Empire* создать *listener*. В отчет включить скриншоты создания *listener*.

2

С помощью *PowerShell Empire* создать *stager* и установить обратное соединение.

В отчет включить скриншоты создания *stager* и успешной установки обратного соединения.

3

Использовать модуль *BloodHound*, чтобы собрать информацию о локальных администраторах и группах.

В отчет включить скриншоты выбора модуля полезной нагрузки и содержимого полученных файлов.

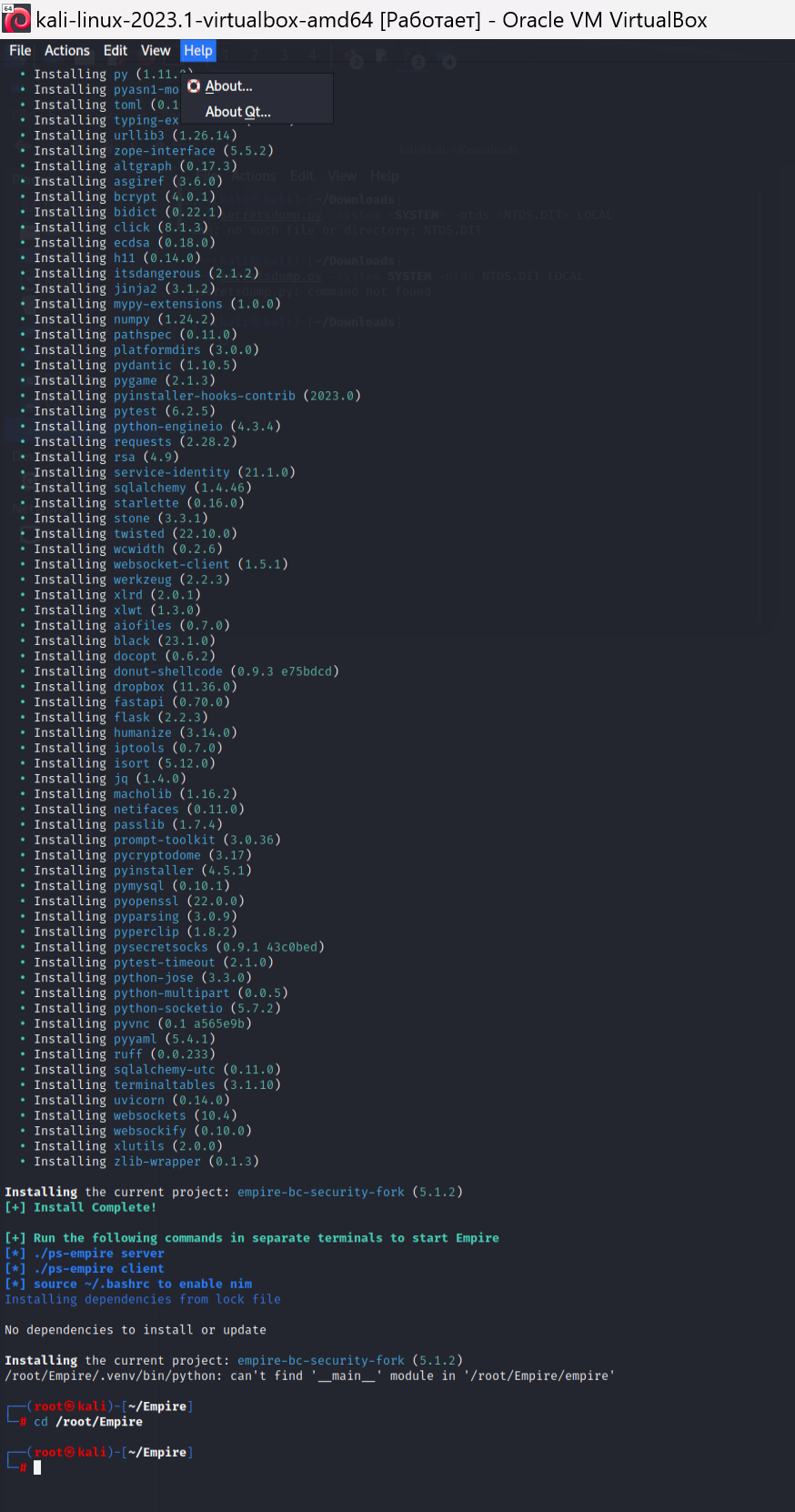
# Решение

Установим Empire.

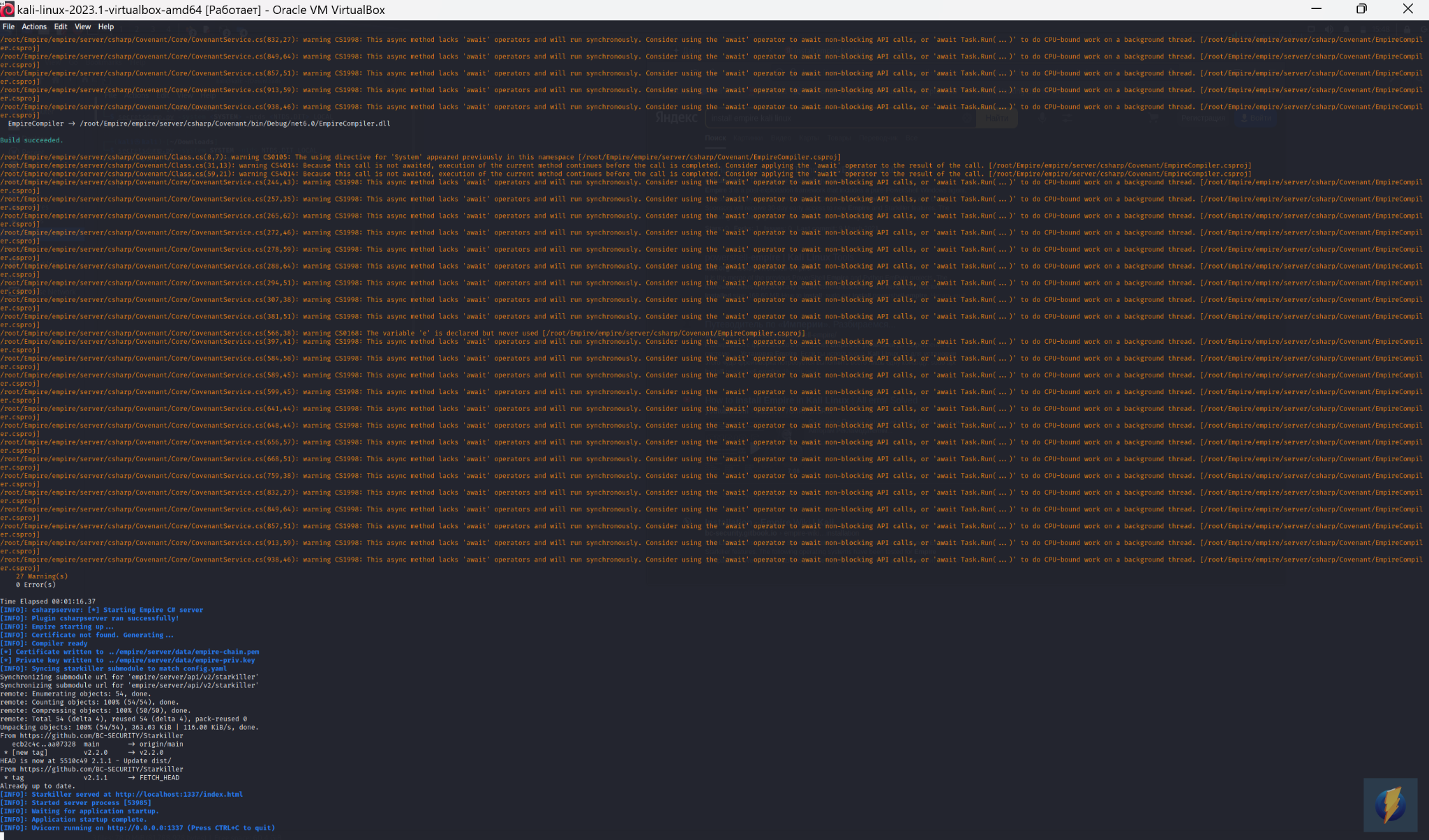
git clone https://github.com/BC-SECURITY/Empire.git

cd Empire

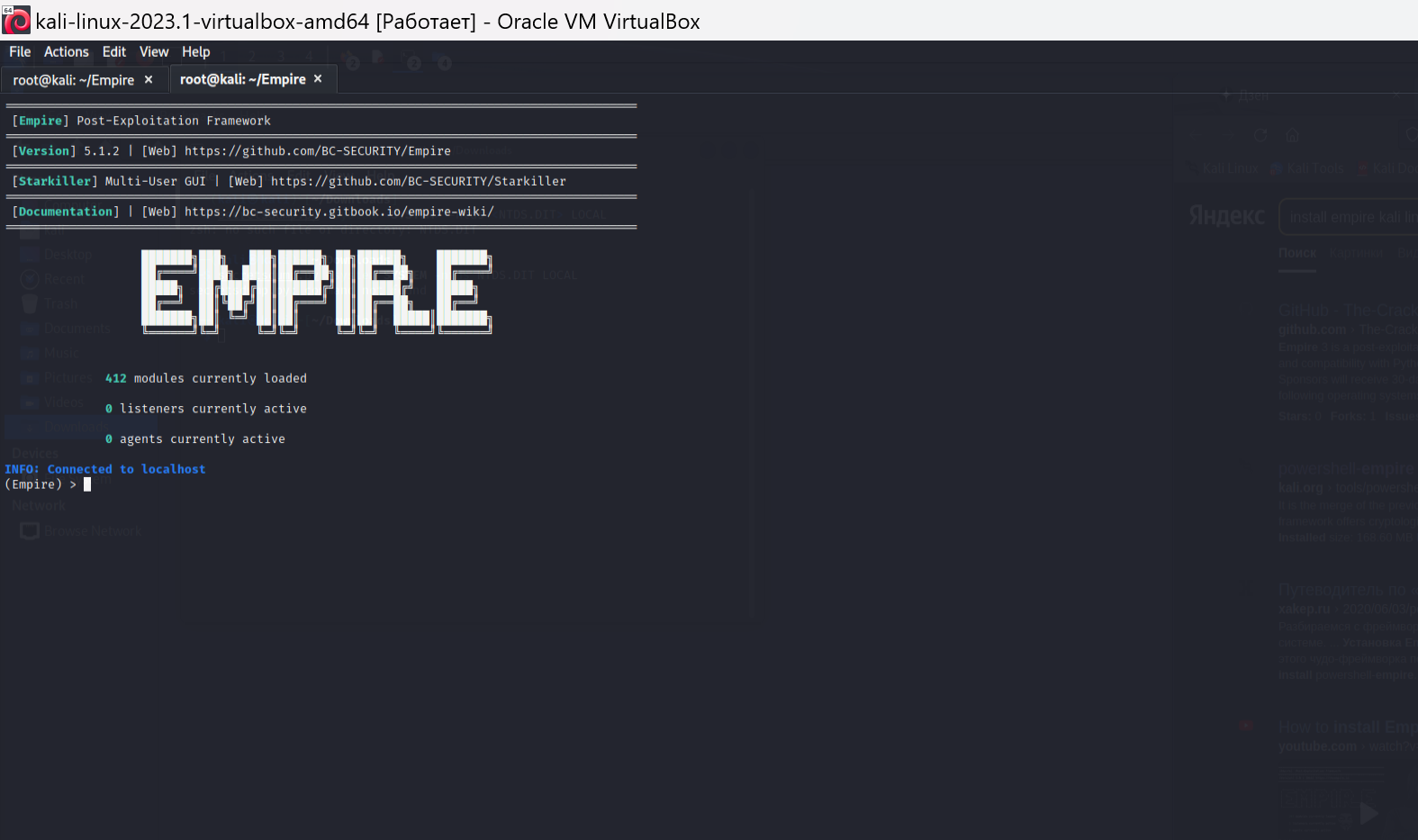
sudo ./setup/install.sh



Запустим ./ps-empire server для установки листенера и стейджа.



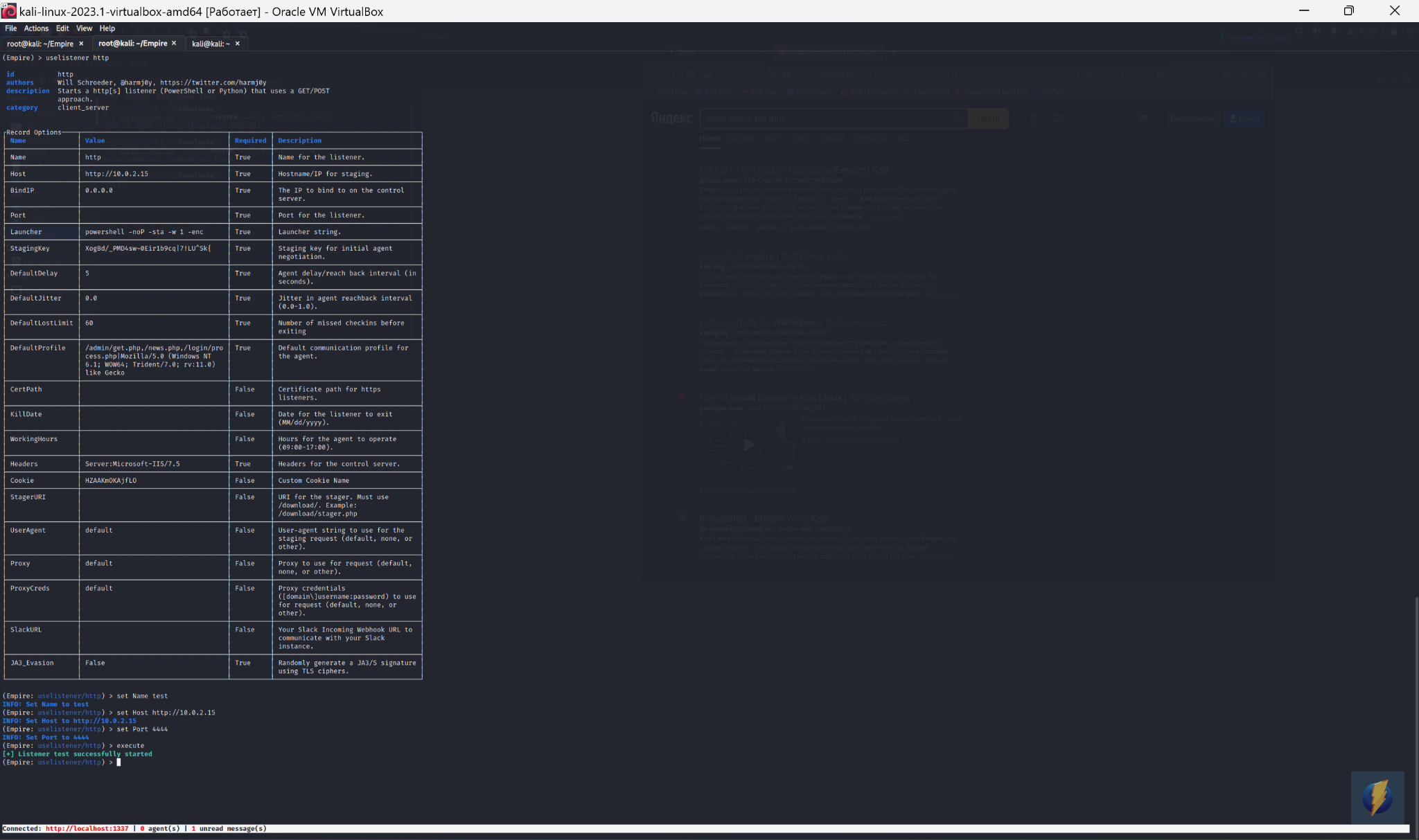
Запустим ./ps-empire client



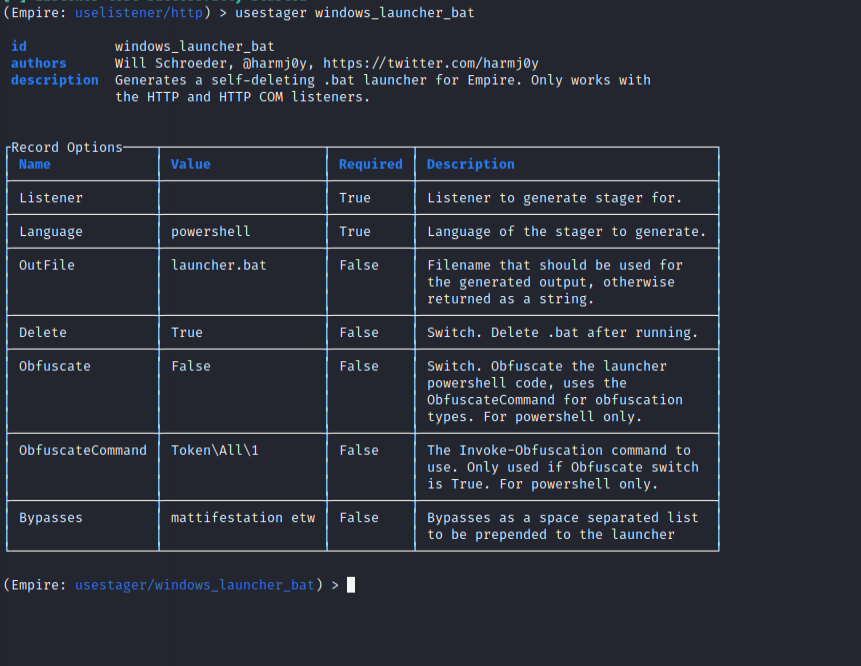
Поднимем listener- напишем команду uselistener http



Укажем хостнейм, айпи, порт, к какой машине стучимся и запускаем.



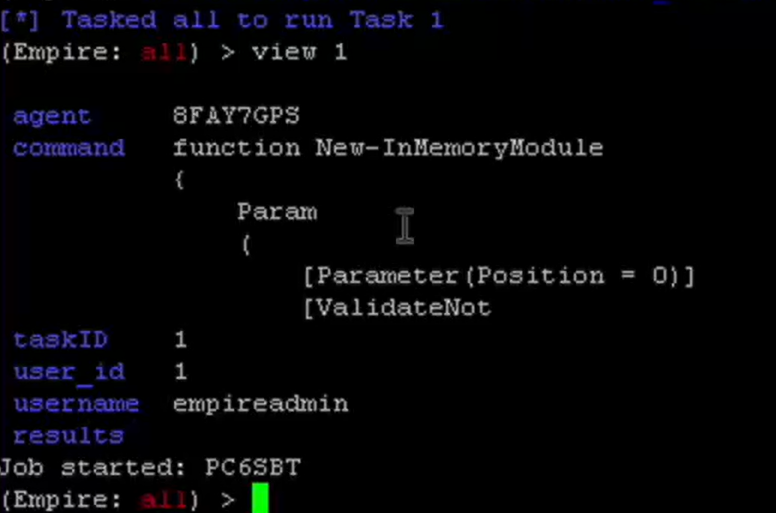
Сделаем полезную нагрузку, например, командой usestager windows\_launcher\_bat



Соберем информацию о локальных администраторах и группах, запустив модуль Bloodhound. Команда usemodule powershell/situational\_awareness\_network\_bloodhound.



Запустим execute и посмотри view.



В действительности можно увидеть на рабочей машине сохраненные файлы. Проверим их содержимое.

