### **Урок 4. Разведка 2.0**

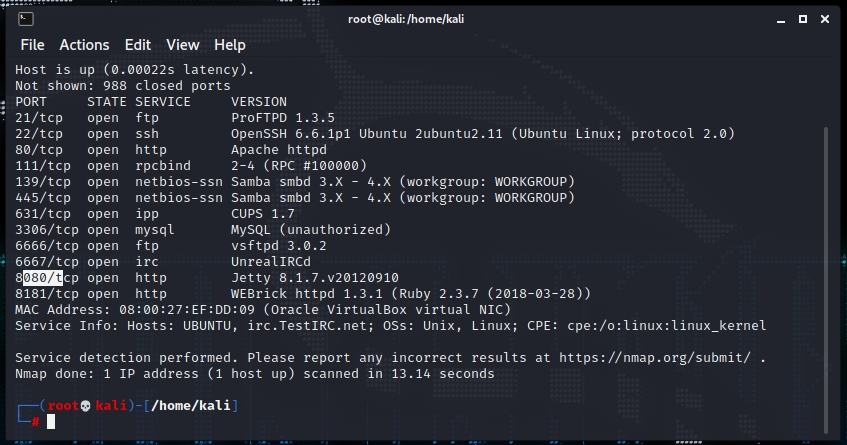
Задание 1:

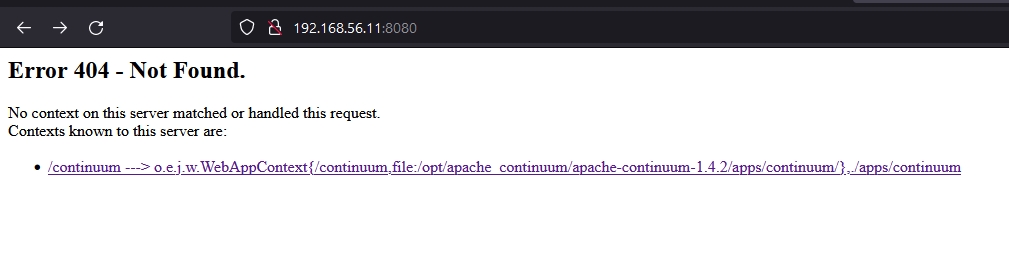
Найдите в ВМ Metasploitable 3 (Linux) адрес страницы Login Page проекта Continuum.

(предварительно отключите межсетевой экран командой iptables -F, затем перезапустите continuum командой service continuum restart), который запущен на одном из кастомных портов. В ответе укажите адрес страницы.

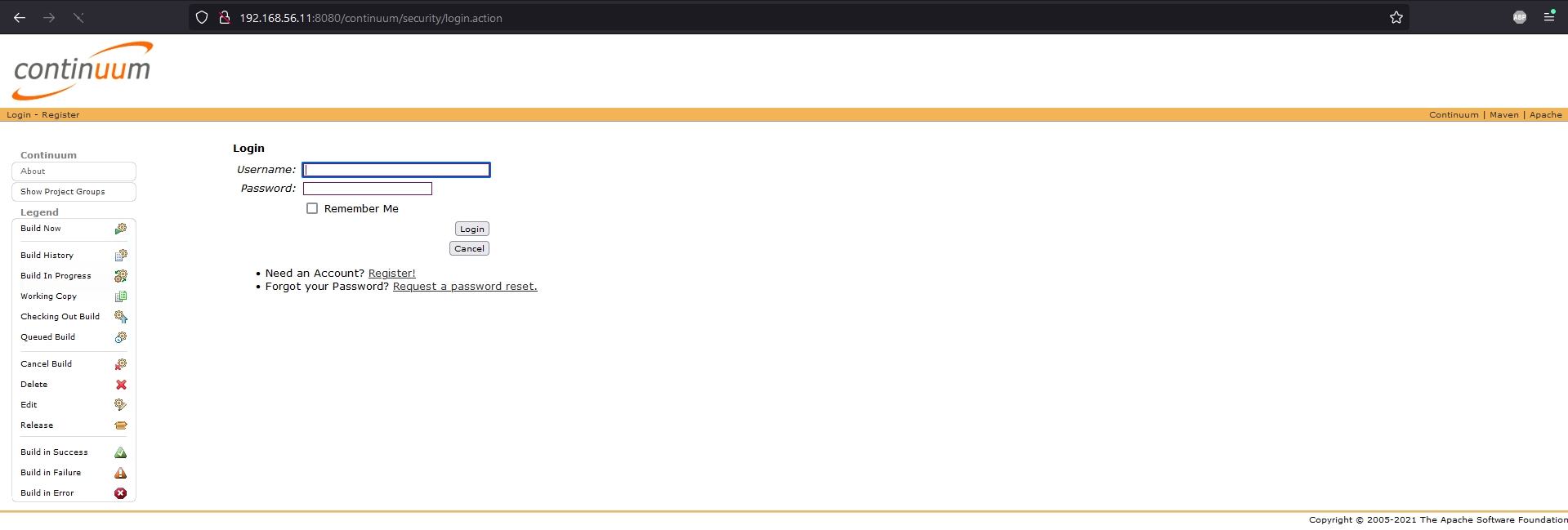
Решение:

Прошёлся утилитой Nmap по серверу и нашёл несколько открытых портов (6697 не нашёл сразу почему-то).

Через браузер зашёл на порт 8080 и увидел следующую страницу:



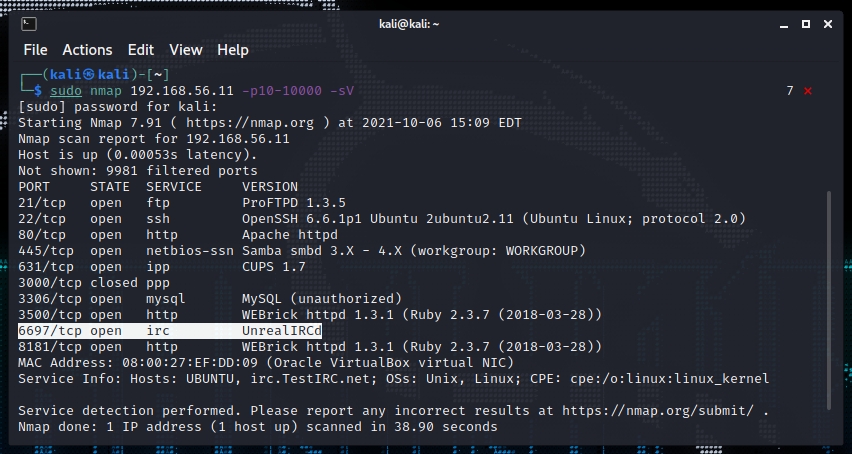
Ссылка на этой странице как раз ведет на страницу авторизации Login Page проекта Continuum.



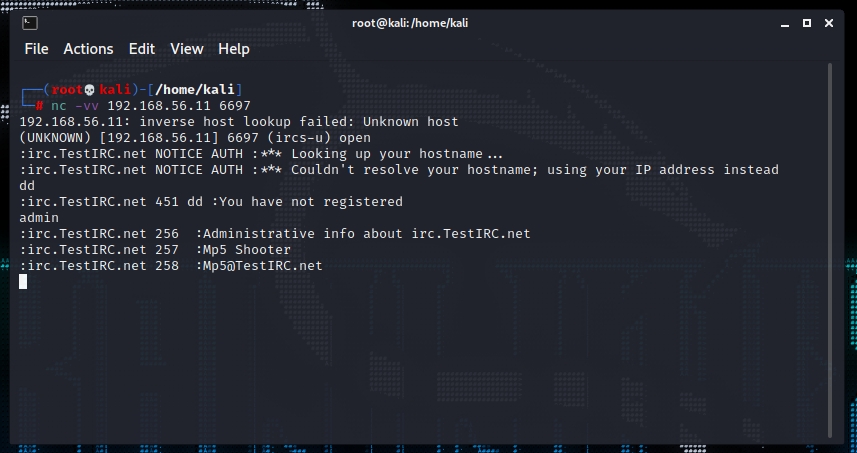
Задание 2:  
 Какой сервис запущен на порту 6697 в ВМ Metasploitable 3 (Linux)?

Решение:

Прошёлся Nmap по серверу, обнаружил порт 6697,



На этом порту работает IRC чат, на сколько я понял.



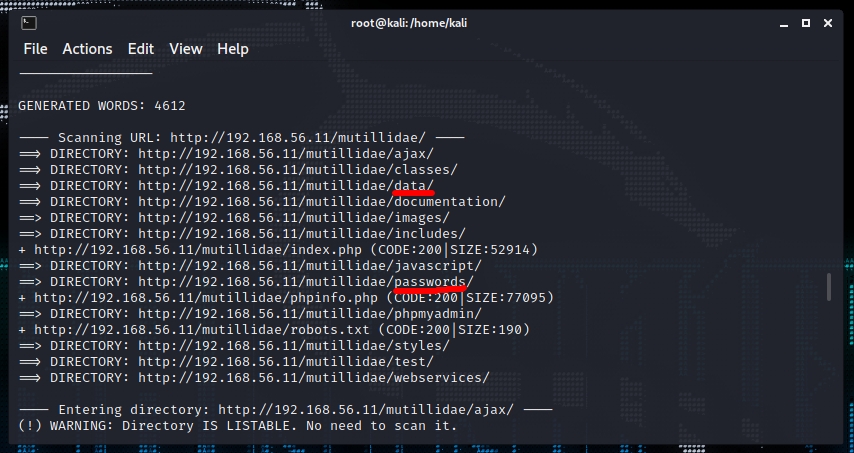
А понял я это из этой статьи:

[*https://russianblogs.com/article/4156850345/*](https://russianblogs.com/article/4156850345/)

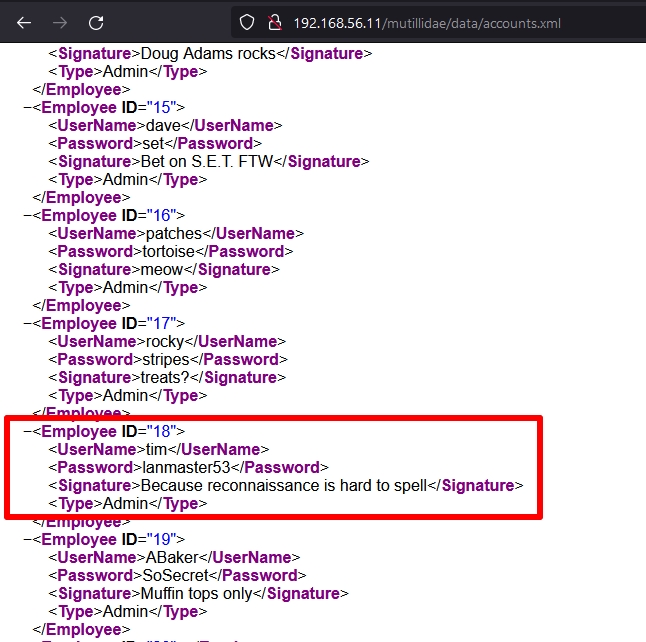
Задание 3:  
 Какой пароль пользователя tim из проекта mutillidae? В каком файле он содержится?

Решение:

Утилитой dirb нашёл несколько интересных каталогов:



Содержимое каталога **data:**



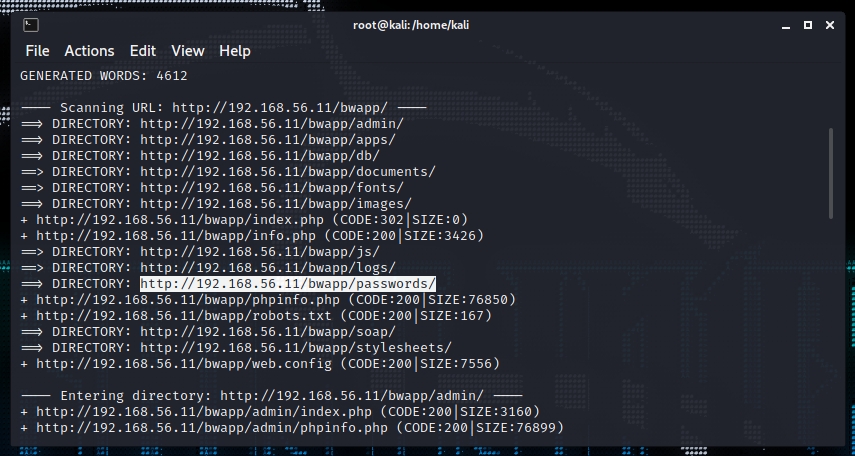
И содержимое каталога **paswords**:



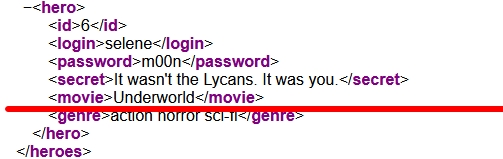
Задание 4:  
 \* В каком файле можно найти информацию о том, какой любимый фильм у юзера с именем selene (не является УЗ в bwapp)?

Решение:

Всё там же dirb прошёлся по bwapp и нашёл каталог passwords:



Зашёл в него через браузер и нашёл там файл heroes.xml, в котором и была найдена нужная информация:



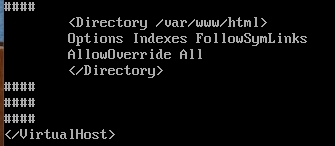
Задание 5:  
 \* Составьте правило (или набор правил) для mod\_rewrite, при помощи которого можно

заблокировать доступ утилиты curl на веб сервер ВМ.

Решение:

Настроил дефолтный конфигурационный файл в директории:

/etc/apache2/sites-available/000-default.conf



Далее командой **a2enmod rewrite** включил mod\_rewrite, чтобы apache читал файл .htaccess.

Далее в директории /var/www/html я создал файл .htaccess и наполнил его следующим содержимым:



Теперь при попытке утилитой curl постучаться на сервер — будет 403 код ответа

