Министерство науки и высшего образования Российской Федерации федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»

Факультет инфокоммуникационных технологий

**Основы кибербезопасности**

Практическая работа №4

**Выполнил**:

студент группы K34211

Швалов Даниил Андреевич

**Проверил**:

преподаватель практики, КТН

Назаров Михаил Сергеевич

Санкт-Петербург

2024

# Оглавление

[Введение 3](#__RefHeading___Toc6438_2741830133)

[Содержание отчета 4](#__RefHeading___Toc6442_2741830133)

[1. Работа в лаборатории для тестирования и поиска уязвимостей 4](#__RefHeading___Toc8544_875968271)

[2. Работа с инструментом NMAP 8](#__RefHeading___Toc8689_875968271)

[3. Установка и работа с metasploit 14](#__RefHeading___Toc8691_875968271)

[Вывод по работе 18](#__RefHeading___Toc7412_875968271)

# Введение

**Цель работы**. Изучить типовой алгоритм работы с нарушителя информационных систем. Приобрести практические навыки по использованию инструментов сканирования ИС. Научиться идентифицировать узлы в информационной системы.

# Содержание отчета

## Работа в лаборатории для тестирования и поиска уязвимостей

Для настройки лаборатории для тестирования и поиска уязвимостей были запущены контейнеры «metasploitable1» и «metasploitable2» на основе образа «tleemcjr/metasploitable2». Также был запущен контейнер «kalibox» на основе образа «kalilinux/kali-rolling». Этот процесс показан на рисунках 1-3.



Рисунок 1 — Запуск контейнера «metasploitable1»

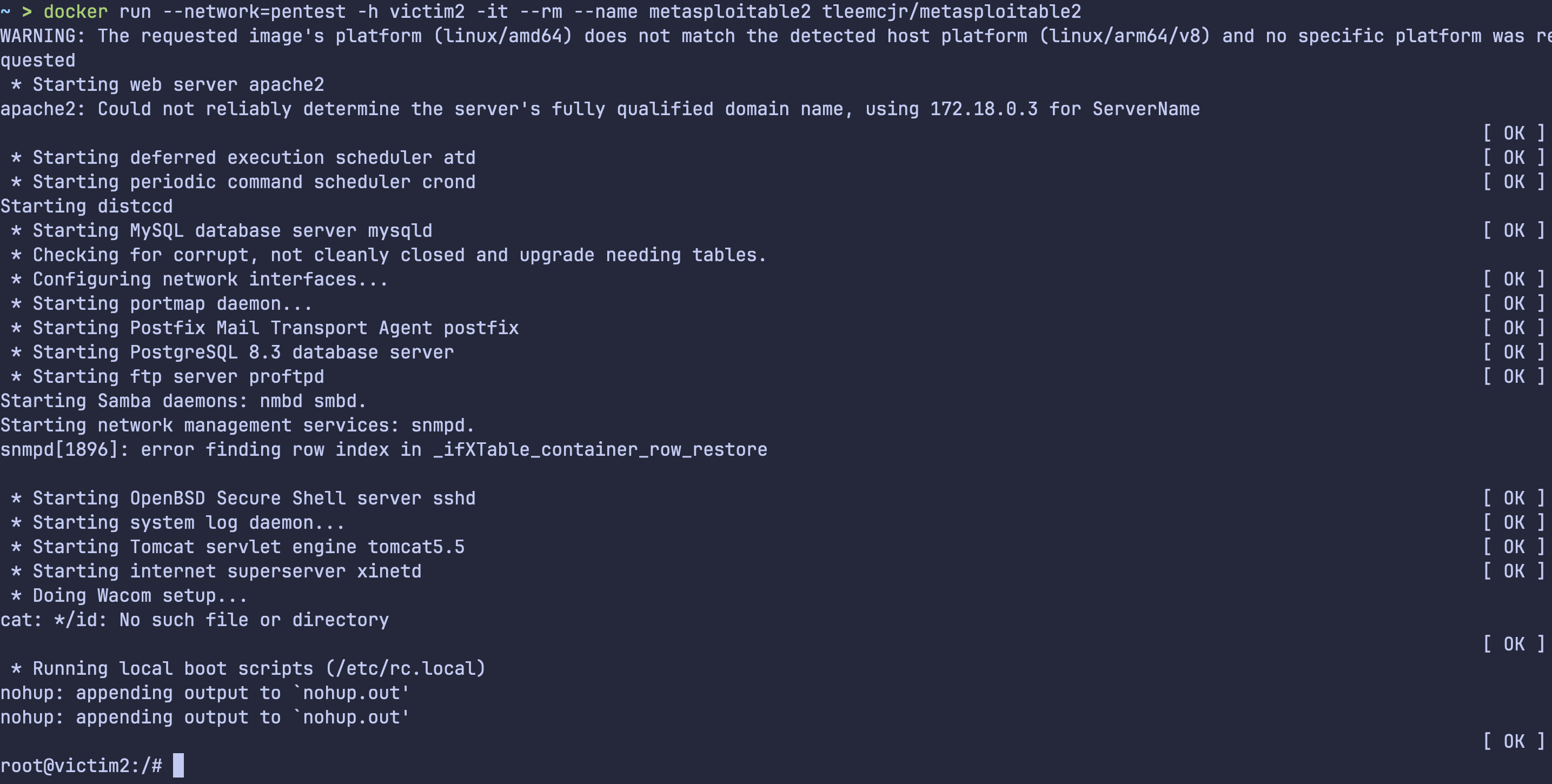


Рисунок 2 — Запуск контейнера «metasploitable2»

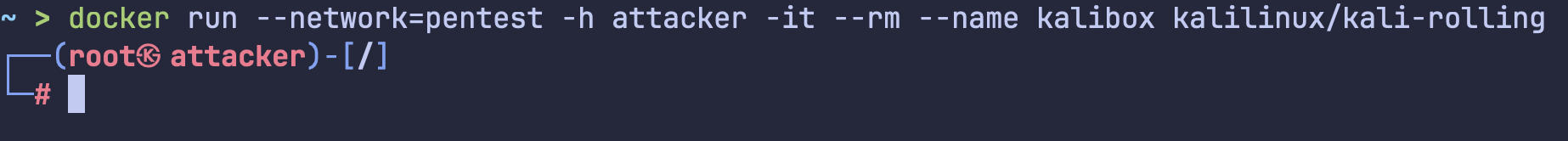


Рисунок 3 — Запуск контейнера «kalibox»

После этого в контейнер «kalibox» была установлена утилита «ping». С ее помощью была проверена сетевая доступность контейнеров «metasploitable1» и «metasploitable2», имеющих адреса 172.18.0.2 и 172.18.0.3 соответственно. После отправки ICMP-запросов были получены ICMP-ответы. Таким образом, было установлено, что контейнер «kalibox» может взаимодействовать с контейнерами «metasploitable1» и «metasploitable2» по сети. Это видно на рисунке 4.

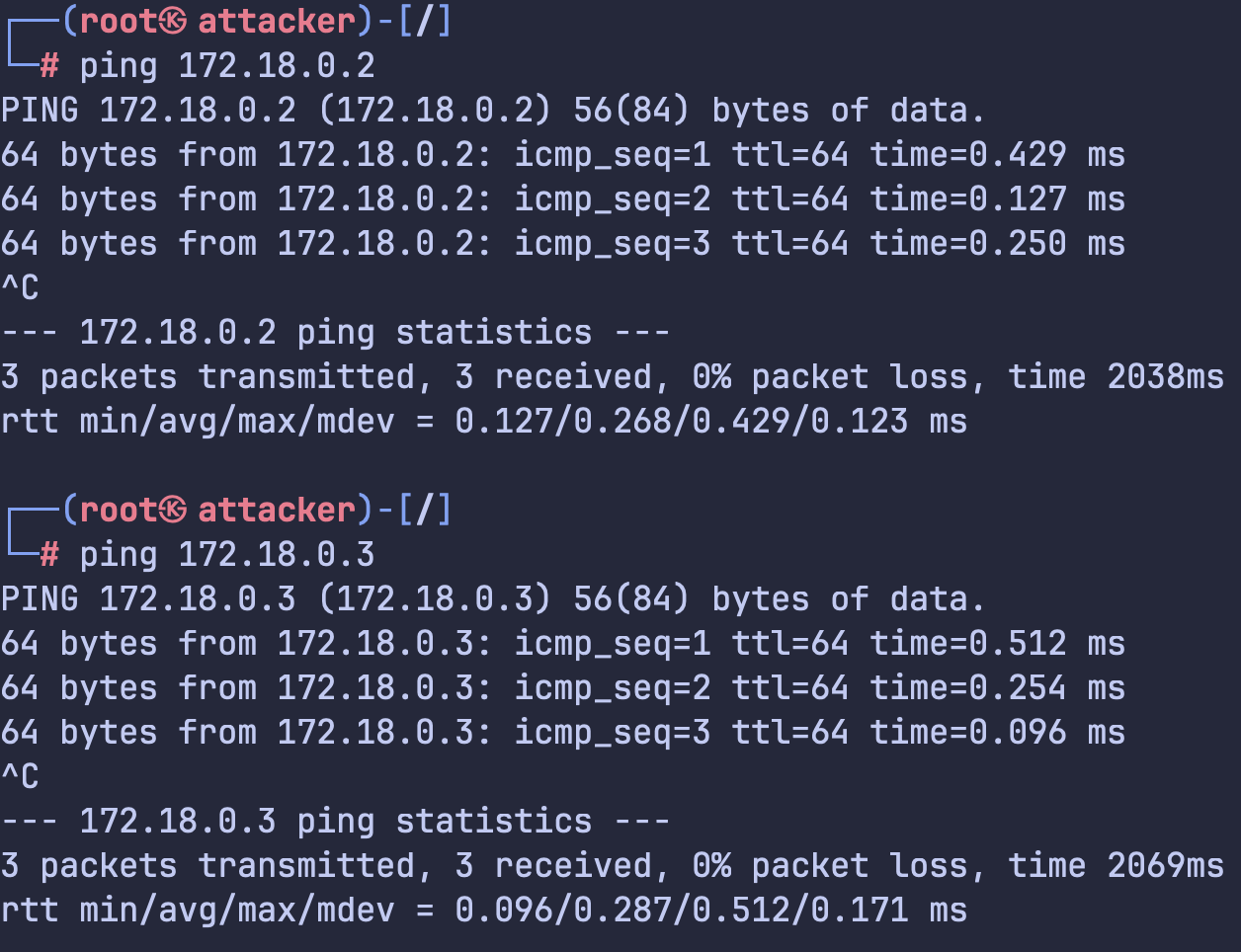


Рисунок 4 — Проверка доступности контейнеров « metasploitable1» и «metasploitable2» из контейнера «kalibox» с помощью утилиты «ping»

Затем была установлена утилита «fping», которая позволяет отправлять ICMP-запросы сразу по нескольким адресам. С ее помощью была повторно проверена доступность адресов 172.18.0.2 и 172.18.0.3. В добавок к этому, был указан IP-адрес, не принадлежащий ни к одному из узлов. После запуска утилиты «fping» было выведено сообщение, что адреса 172.18.0.2 и 172.18.0.3 доступны, а адрес 172.18.0.5 — нет. Этот процесс показан на рисунках 5-6.

Рисунок 5 — Установка утилиты «fping»

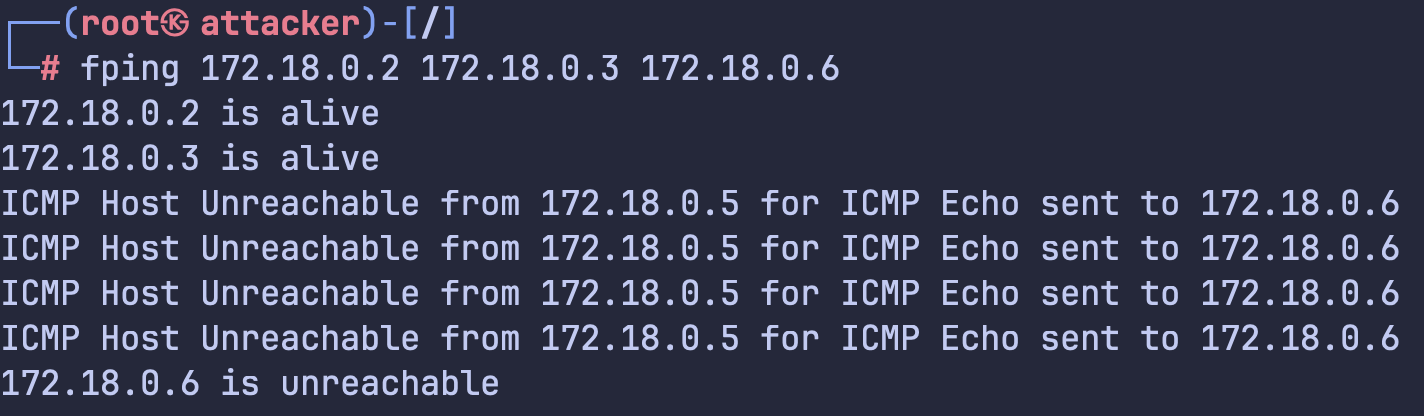
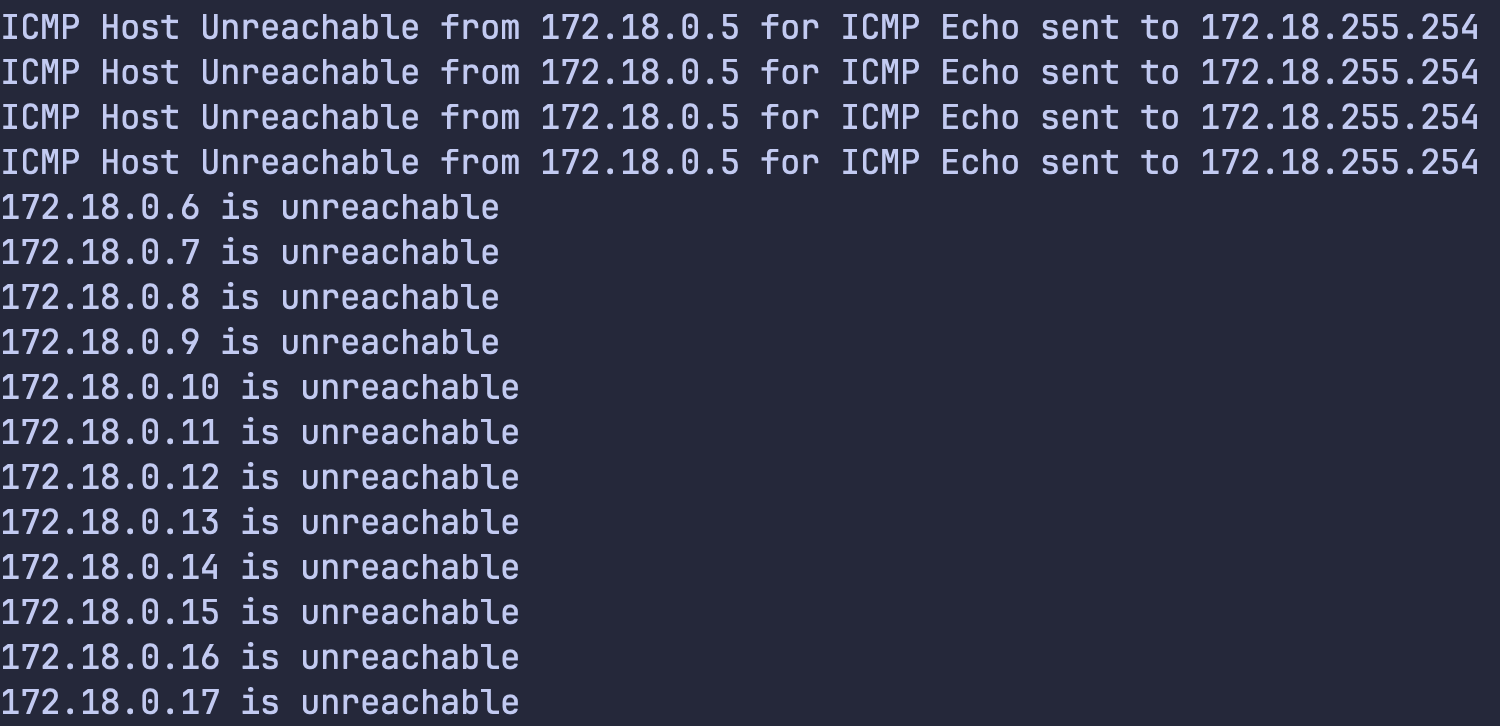


Рисунок 6 — Проверка доступности узлов с помощью утилиты «fping»

После этого была протестирована работы утилиты «fping» с опцией «-g», которая позволяет протестировать доступность списка адресов заданной подсети. В данном случае была указана подсеть 172.18.0.0/16. После запуска утилиты «fping» началась проверка доступности всех хостов из данной подсети. Через некоторое время утилита «fping» вывела информацию о недоступных узлах. Это показано на рисунках 7-8.

Рисунок 7 — Проверка доступности всех узлов в подсети 172.18.0.0/16 с помощью утилиты «fping»

Рисунок 8 — Информация о недоступных узлах

## Работа с инструментом NMAP

При работе с утилитой «nmap» были изучены и протестированы различные опции. Первой из них была опция «-A», которая позволяет просканировать операционную систему, ее версию, наличие различных скриптов, а также определить маршрут так, как это делает утилита «traceroute». Результат запуска утилиты показан на рисунке 9.

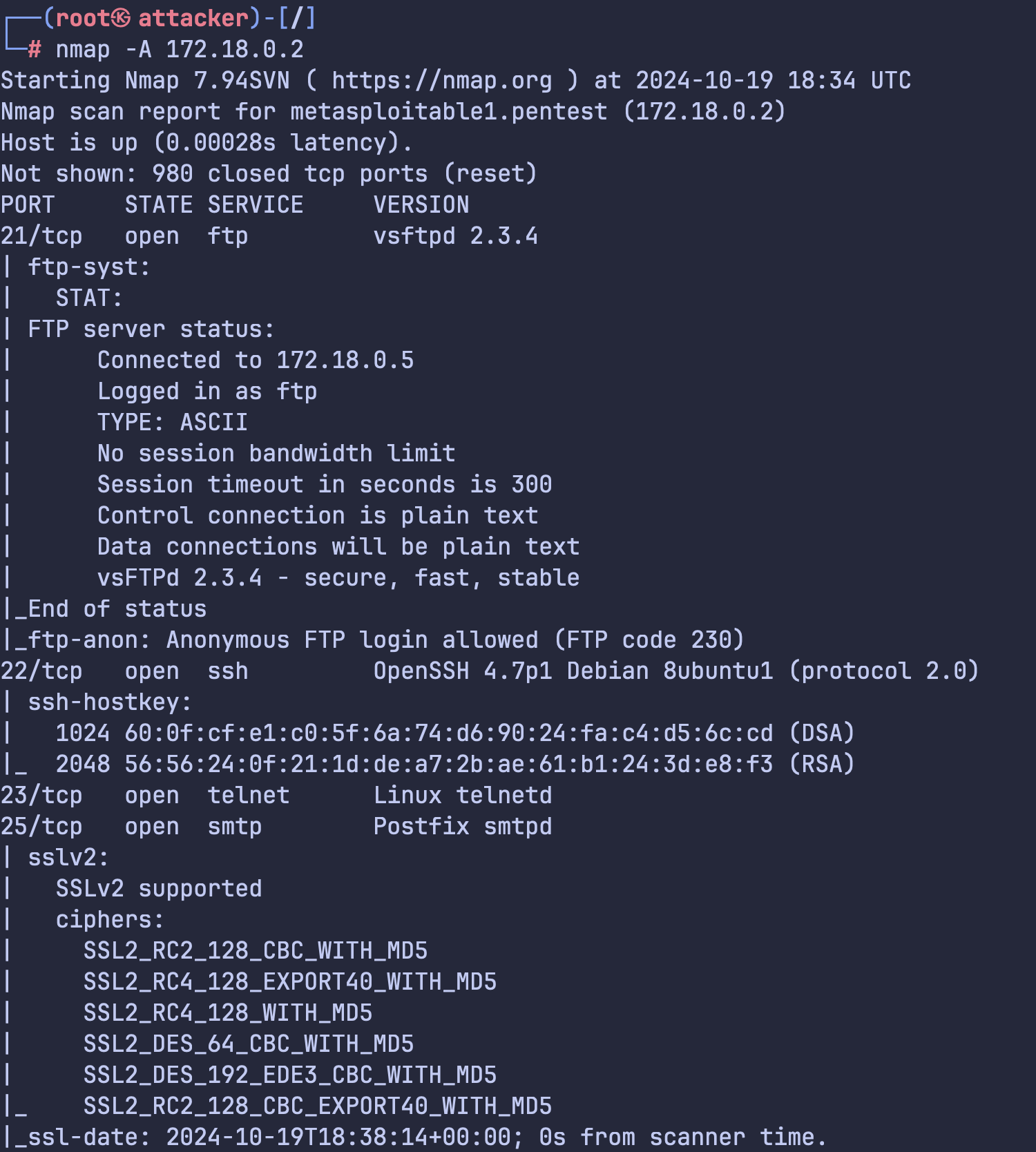


Рисунок 9 — Запуск утилиты «nmap» с опцией «-A»

После этого утилита «nmap» была запущена с опцией «-sT», которая позволяет провести TCP-сканирование подключения с помощью трехстороннего рукопожатия. После запуска сканирования на экран были выведены все открытие TCP-порты. Результат запуска утилиты показан на рисунке 10.

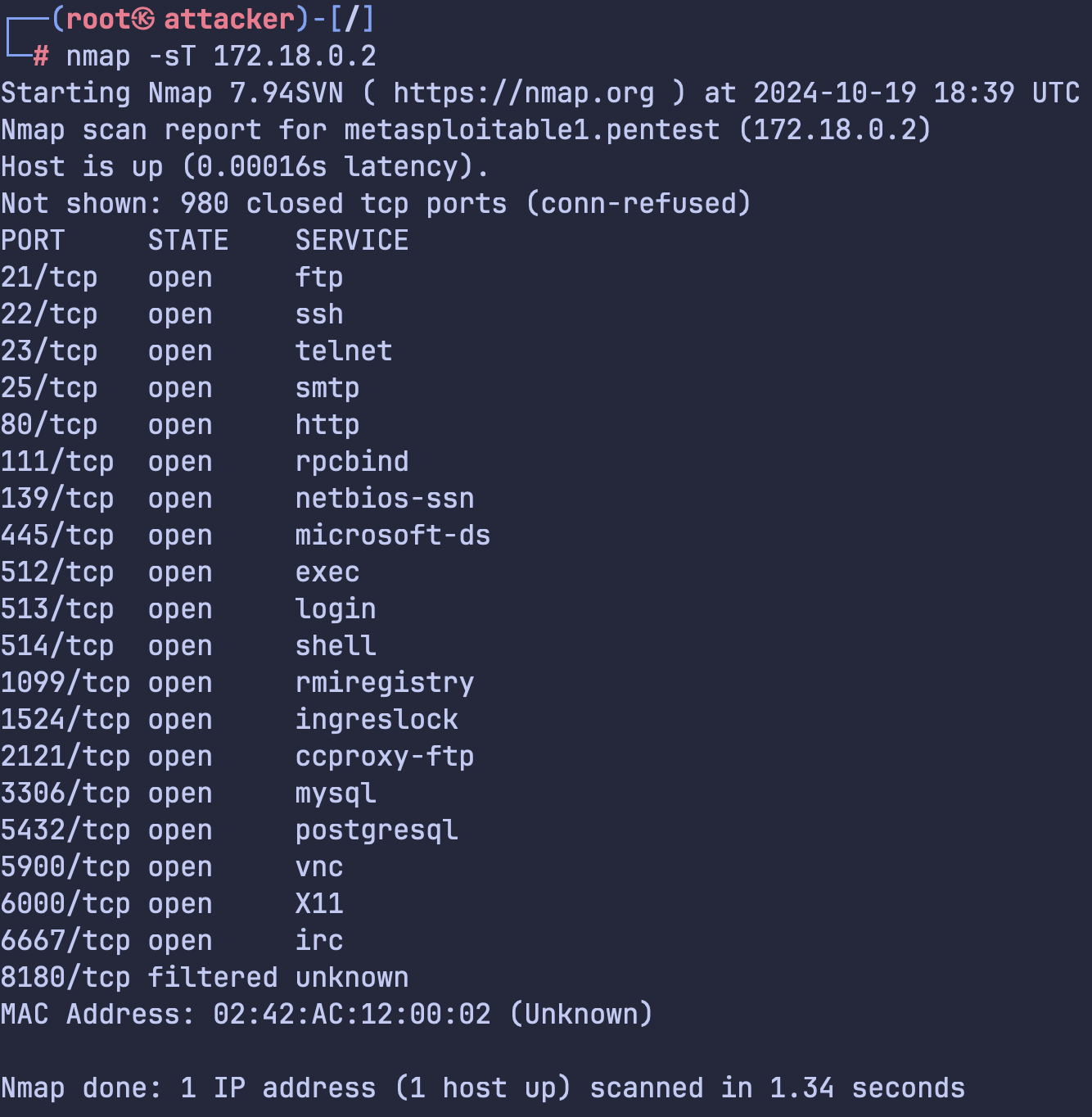


Рисунок 10 — Запуск утилиты «nmap» с опцией «-sT»

Затем утилита «nmap» была запущена с опцией «-sS», которая позволяет провести SYN-сканирование. После запуска сканирования на экран были выведены все открытие TCP-порты. Результат запуска утилиты показан на рисунке 11.

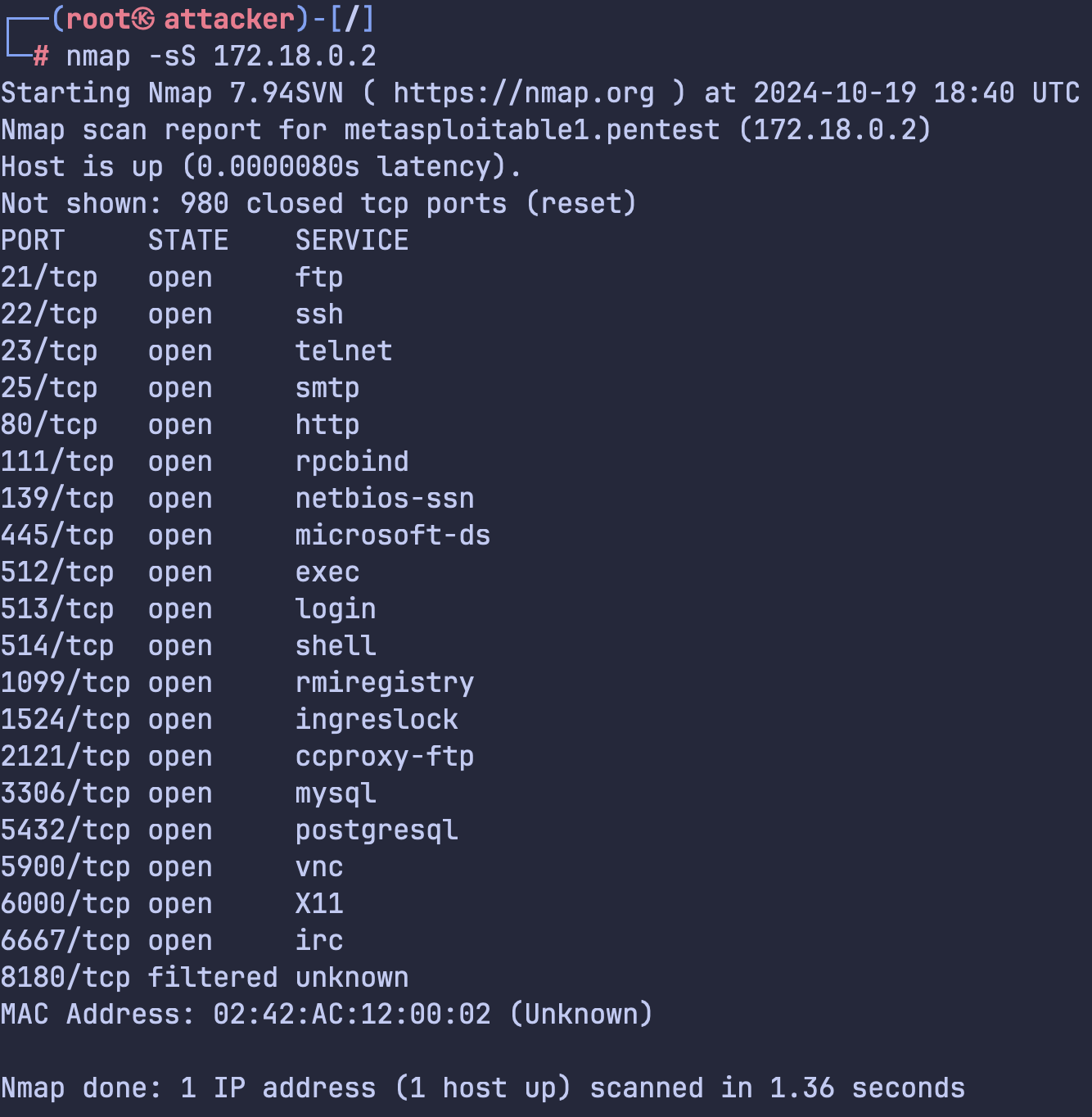


Рисунок 11 — Запуск утилиты «nmap» с опцией «-sS»

После этого утилита «nmap» была запущена с опцией «-sN», которая позволяет провести TCP NULL-сканирование. После запуска сканирования на экран были выведены все открытие и фильтруемые TCP-порты. Результат запуска утилиты показан на рисунке 12.

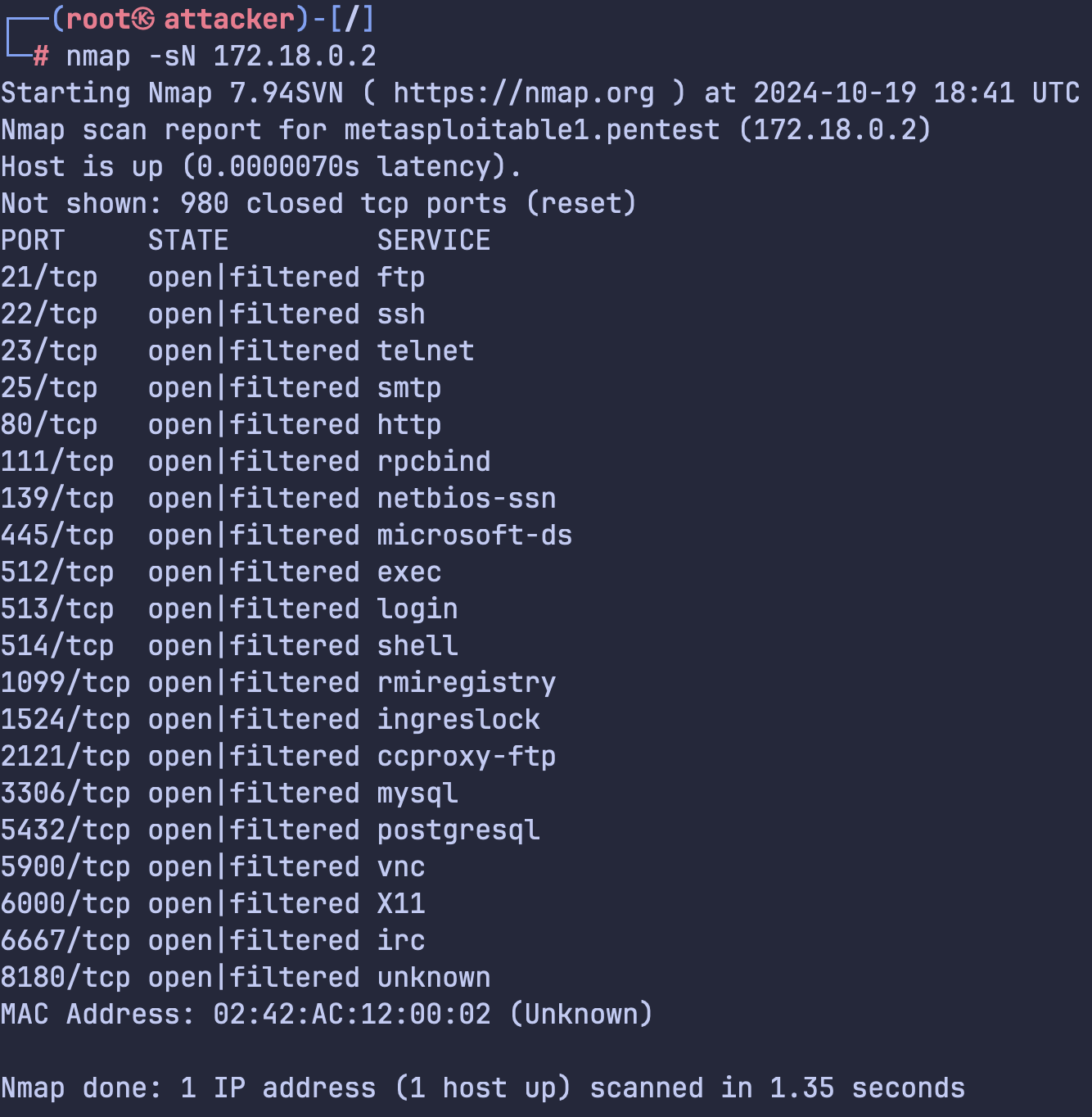


Рисунок 12 — Запуск утилиты «nmap» с опцией «-sN»

Затем утилита «nmap» была запущена с опцией «-sM», которая позволяет провести TCP-сканирование Маймона. После запуска сканирования на экран было выведено сообщение, что все сканируемые порты находятся в состоянии игнорирования. Результат запуска утилиты показан на рисунке 13.

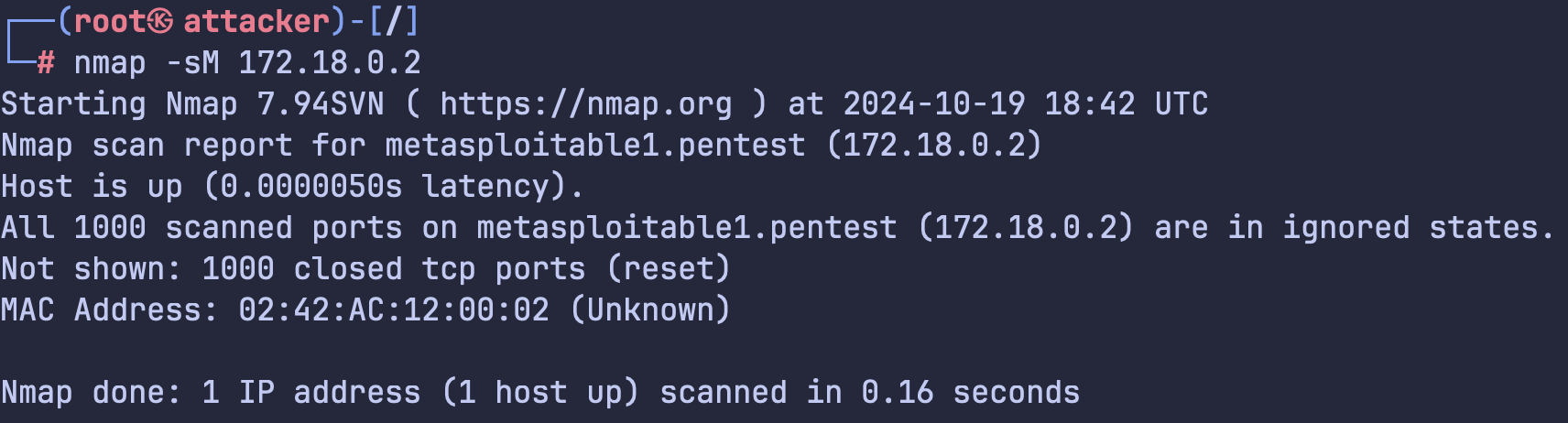


Рисунок 13 — Запуск утилиты «nmap» с опцией «-sM»

После этого утилита «nmap» была запущена с опцией «-sA», которая позволяет провести TCP ACK-сканирование. После запуска сканирования на экран было выведено сообщение, что все сканируемые порты находятся в состоянии игнорирования. Результат запуска утилиты показан на рисунке 14.

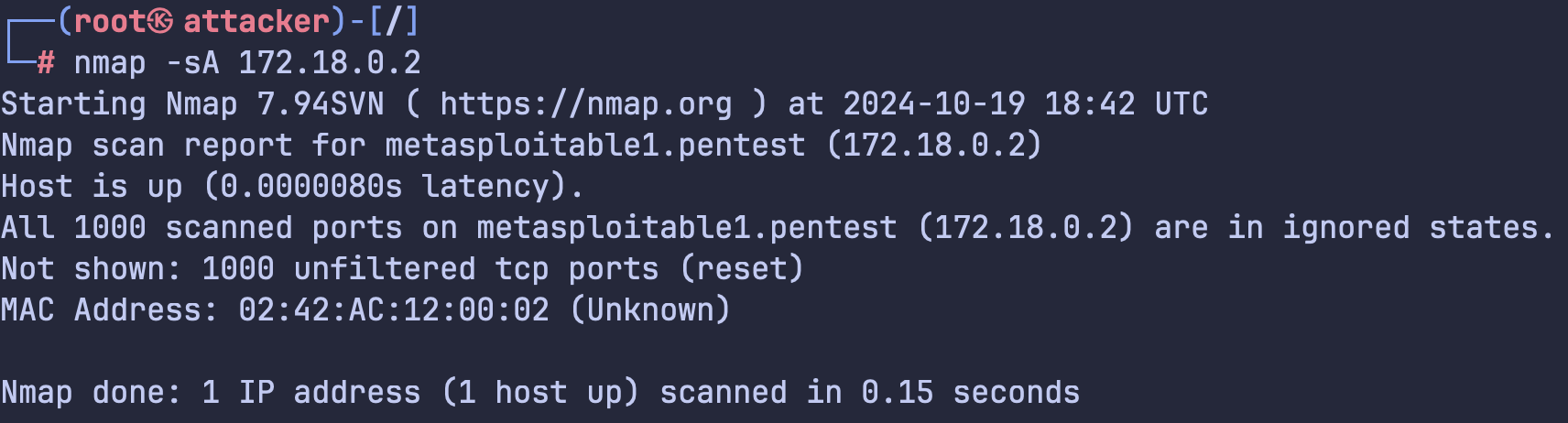


Рисунок 14 — Запуск утилиты «nmap» с опцией «-sA»

Затем утилита «nmap» была запущена с опцией «-sW», которая позволяет провести TCP Window-сканирование. После запуска сканирования на экран было выведено сообщение, что все сканируемые порты находятся в состоянии игнорирования. Результат запуска утилиты показан на рисунке 15.

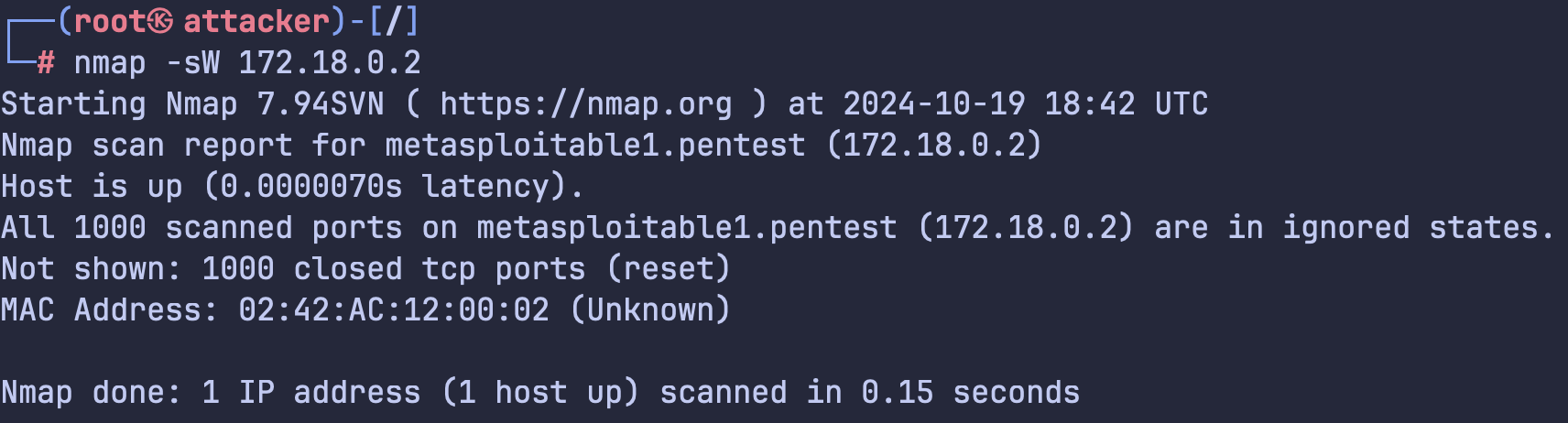


Рисунок 15 — Запуск утилиты «nmap» с опцией «-sW»

После этого утилита «nmap» была запущена с опцией «-sI», которая позволяет провести TCP Idle-сканирование. В качестве зомби-хоста был выбран IP-адрес атакующего. После запуска сканирования на экран было выведено сообщение, что сканируемые порты находятся в состоянии «unknown». Результат запуска утилиты показан на рисунке 16.

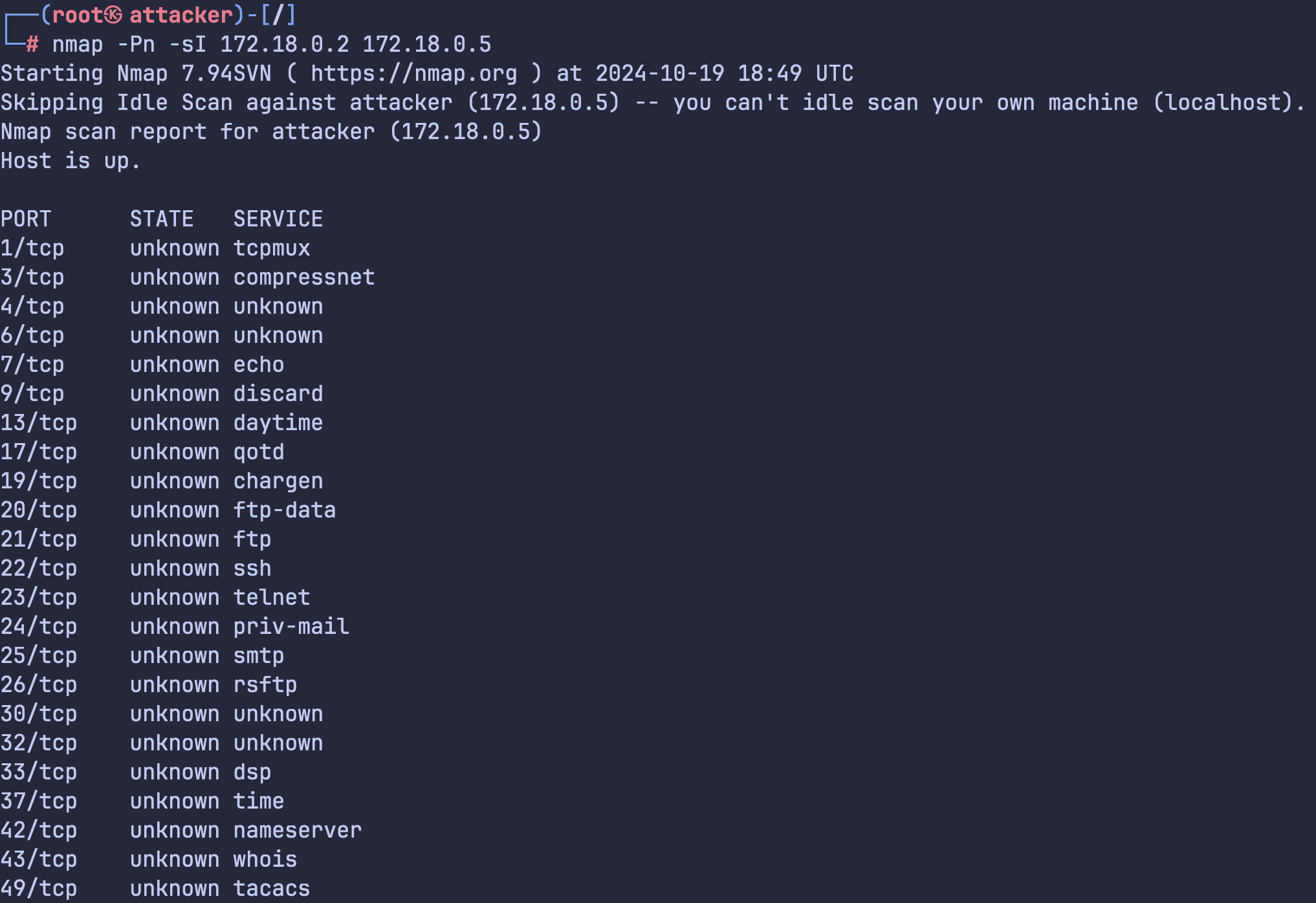


Рисунок 16 — Запуск утилиты «nmap» с опцией «-sI»

Затем утилита «nmap» была запущена с опцией «-O», которая позволяет которая позволяет просканировать операционную систему. После запуска сканирования на экран была выведена информация о стандартных портах, а также об операционной системе. Результат запуска утилиты показан на рисунке 17.

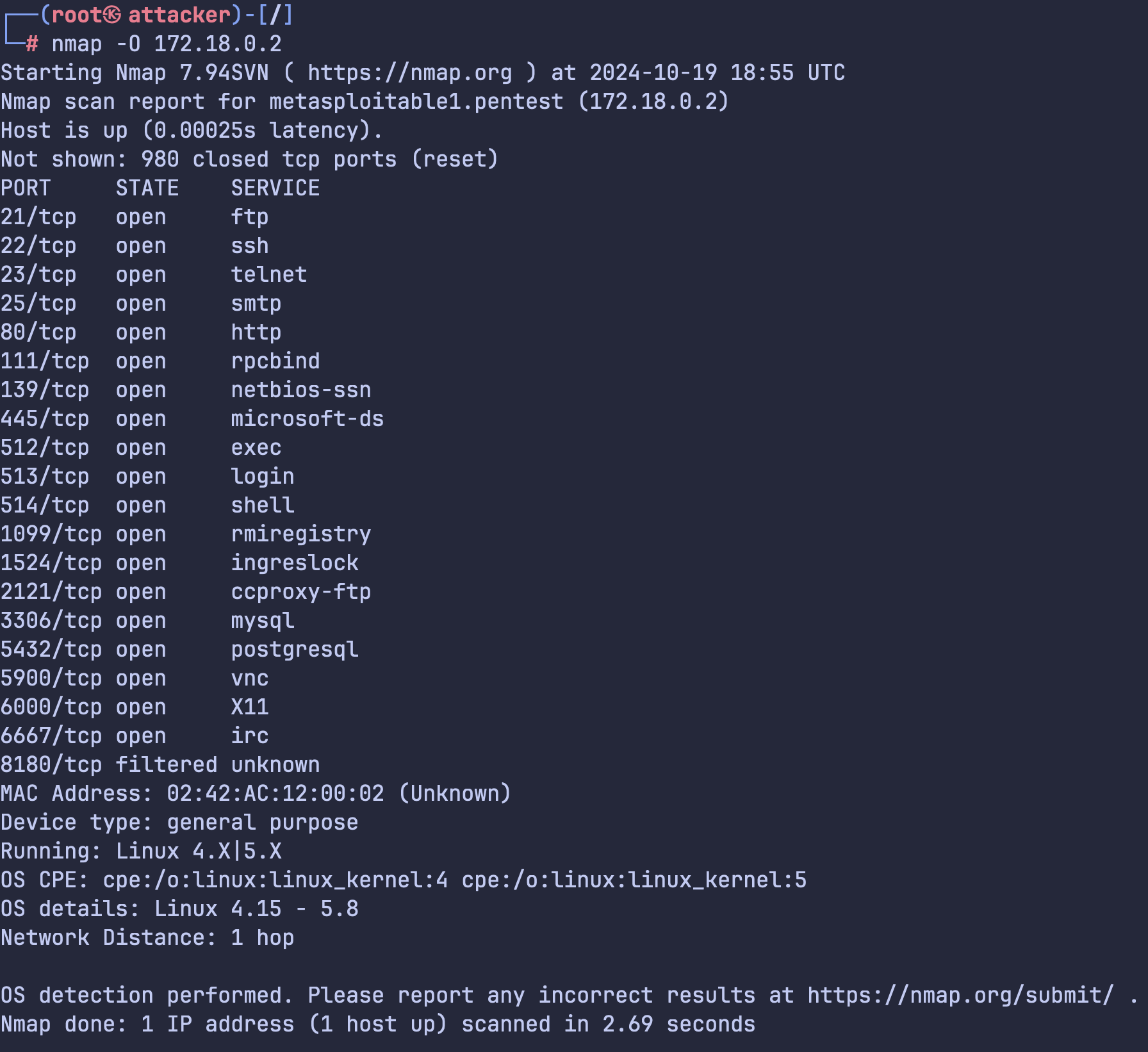


Рисунок 17 — Запуск утилиты «nmap» с опцией «-O»

## Установка и работа с metasploit

Для дополнительного сканирования уязвимостей была установлена утилита «metasploit» с помощью Docker. Эта утилита предоставляет возможности для для создания и отладки эксплойтов.

После загрузки образа «strm/metasploit» и запуска контейнера «metasploit» на его основе на экран было выведено приветственное сообщение. Данное сообщение показано на рисунке 18.

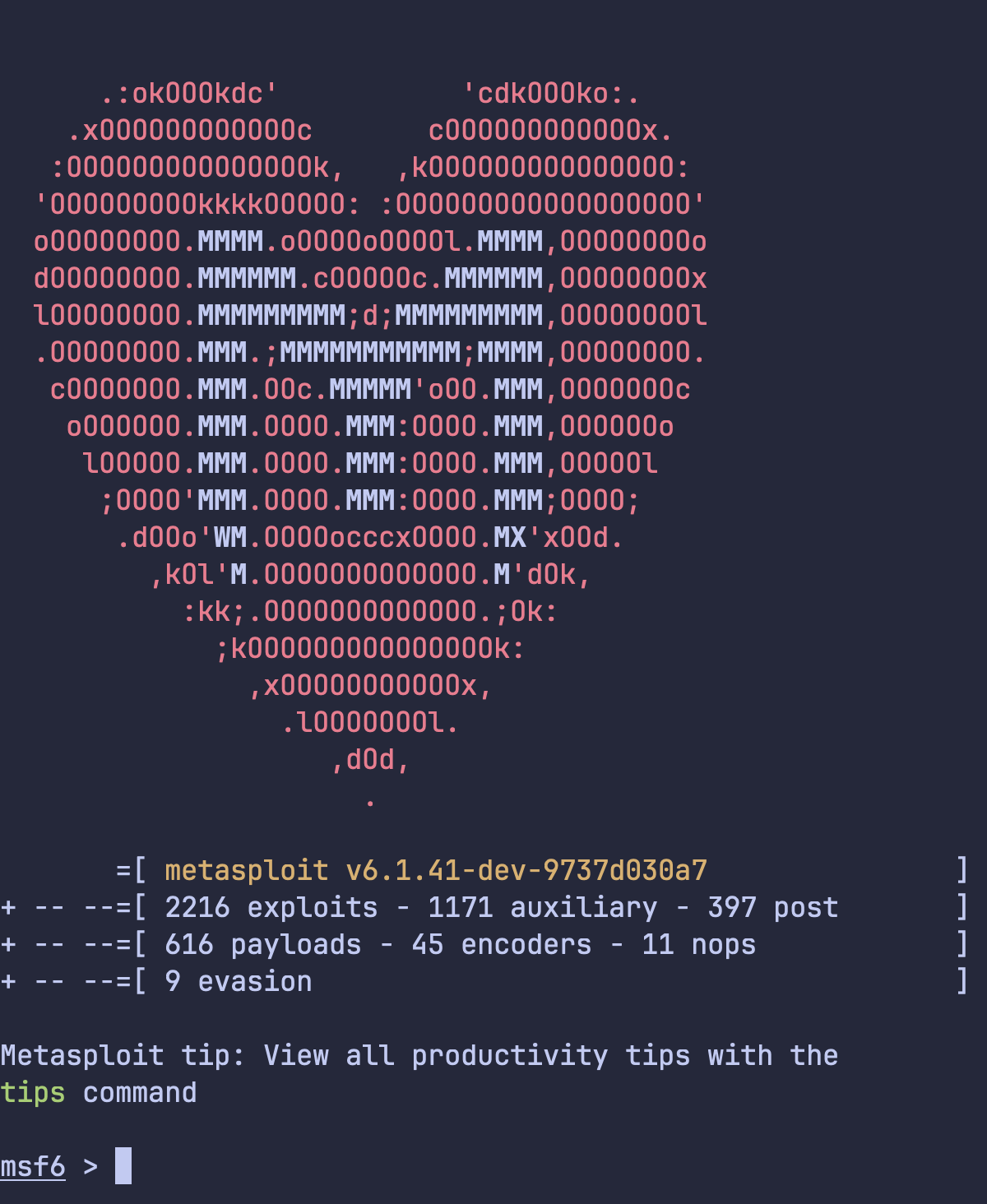


Рисунок 18 — Приветственное сообщение при запуске контейнера «metasploit»

После этого была запущена утилита «db\_nmap», позволяющая просканировать TCP-порты так, как это делает утилита «nmap». В качестве сканируемого адреса был указан адрес контейнера «metasploitable1», т. е. адрес 172.18.0.2. Результат запуска утилиты «db\_nmap» показан на рисунке 19.

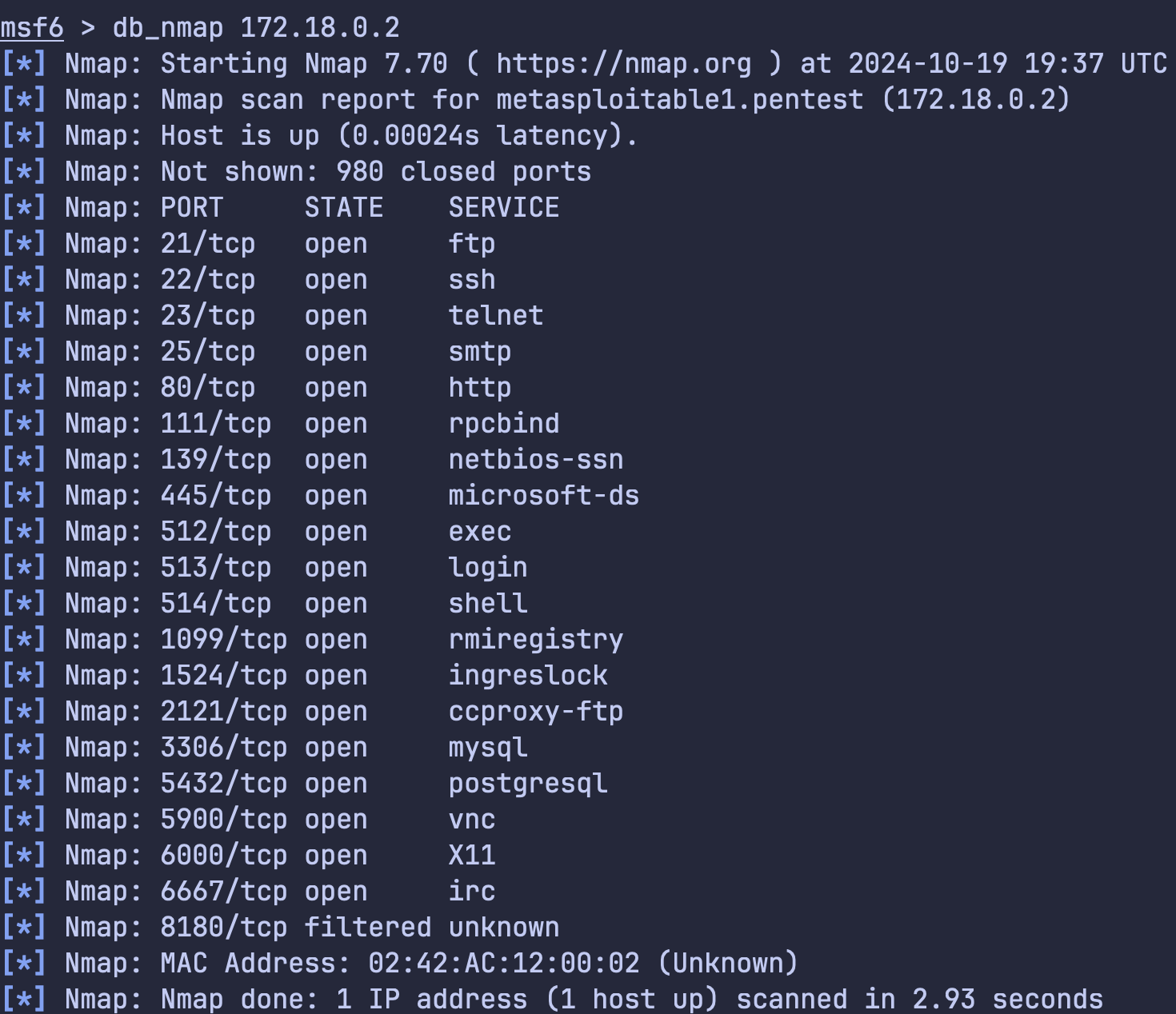


Рисунок 19 — Запуск утилиты «db\_nmap» в контейнере «metasploit»

Затем была протестирована утилита «exploit/unix/http/ xdebug\_unauth\_exec». С помощью команды «options» были выведены все доступные опции утилиты. С помощью команды «set RHOST» был изменен хост цели. После изменения хоста цели в выводе «options» в поле «RHOST» начал отображаться ранее установленный хост. Это видно на рисунках 20-21.

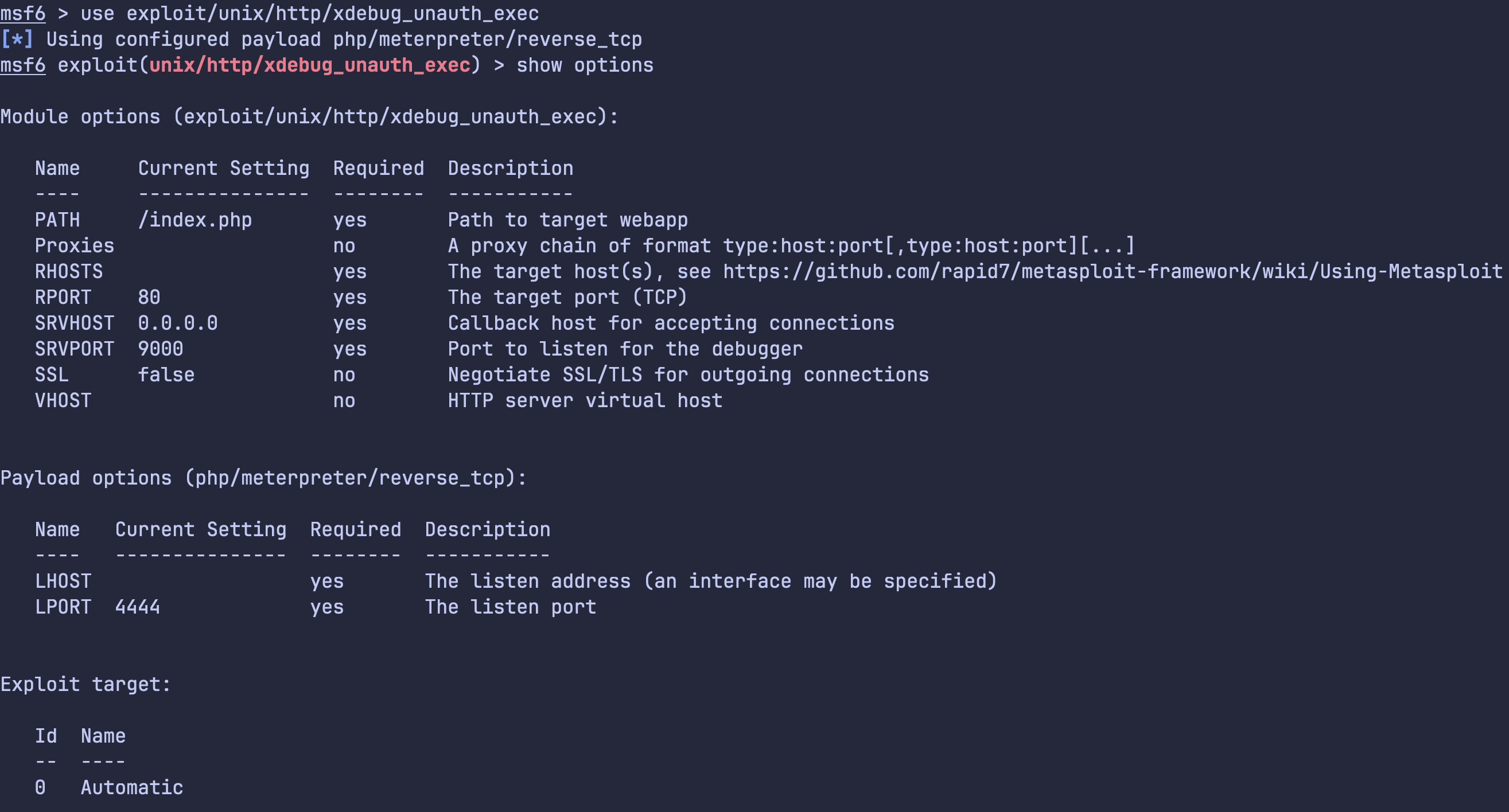


Рисунок 20 — Опции утилиты «exploit/unix/http/xdebug\_unauth\_exec»

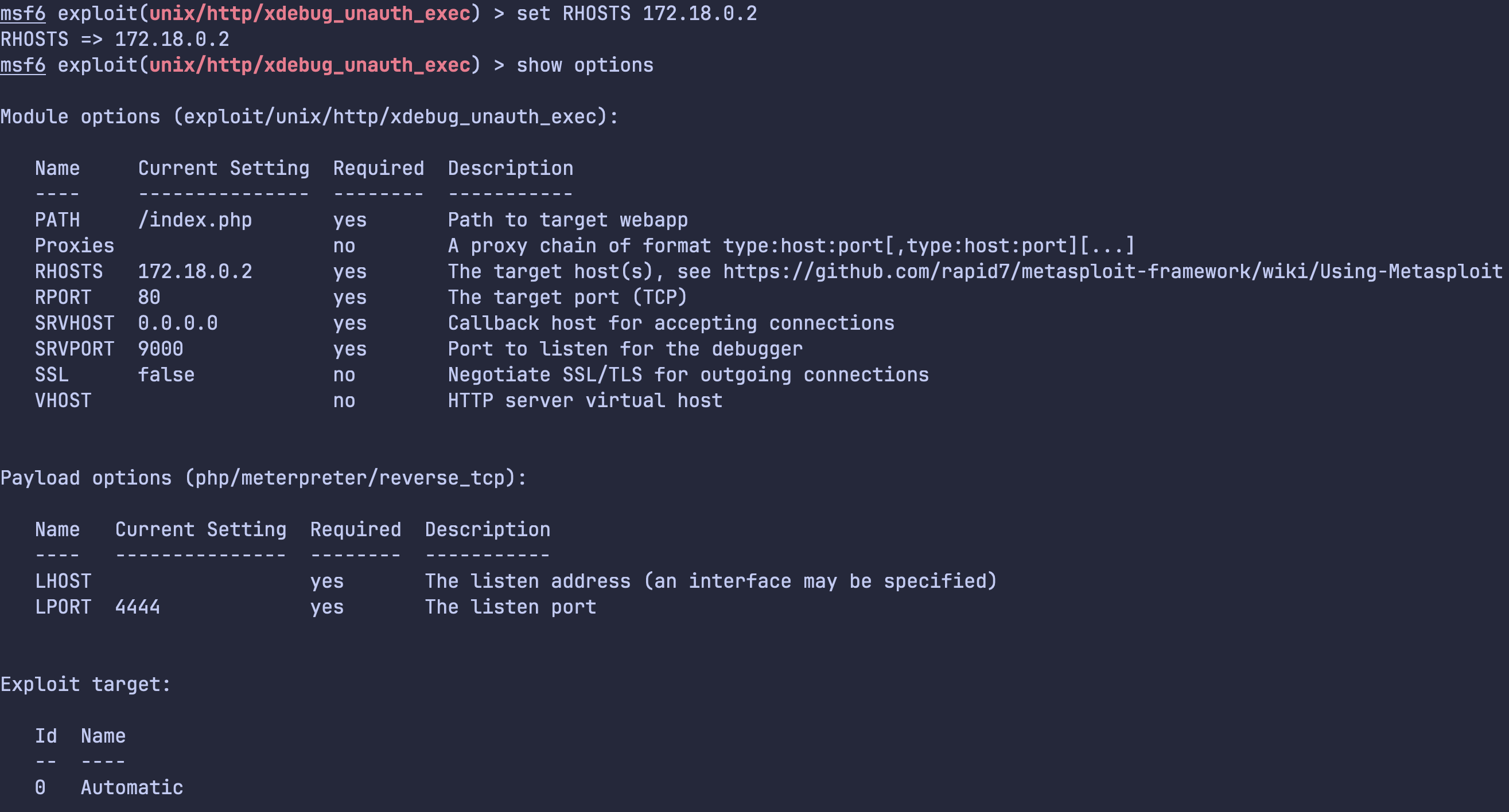


Рисунок 21 — Опции утилиты «exploit/unix/http/xdebug\_unauth\_exec» после настройки RHOST

# Вывод по работе

В результате выполнения данной практической работы был изучен типовой алгоритм работы с нарушителями информационных систем, приобретены практические навыки по использованию инструментов сканирования ИС, получены навыки идентификации узлов в информационной системе.