

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение   
высшего образования

**«Дальневосточный федеральный университет»**

(ДВФУ)

**ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ**

**Департамент программной инженерии и искусственного интеллекта**

ВОРОБЬЕВА КРИСТИНА ВИТАЛЬЕВНА

**ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3**

по дисциплине «Защита информации»

по образовательной программе подготовки бакалавров по направлению

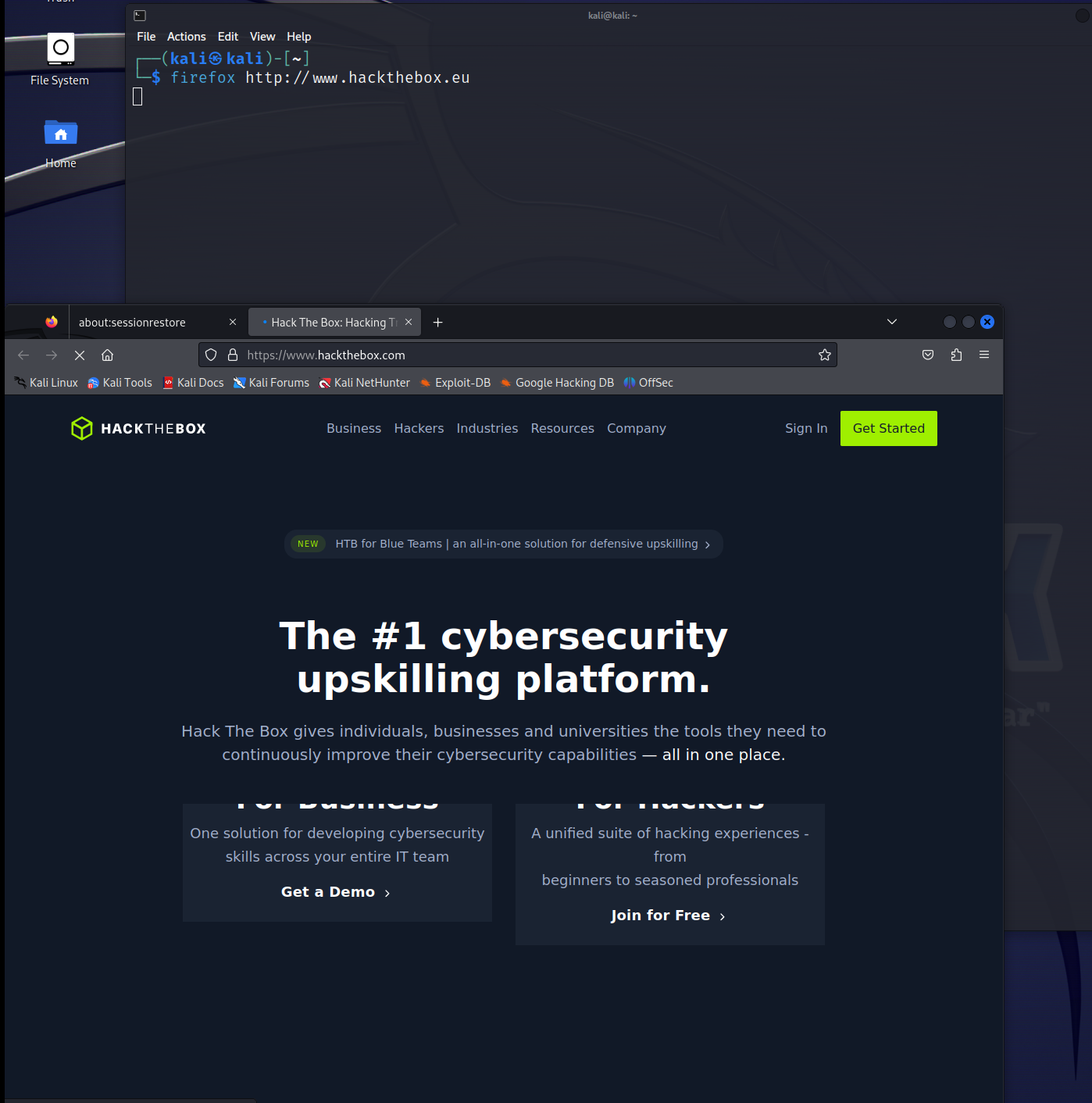
09.03.04 - Программная инженерия

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |  |  | Студент гр. Б9120-09.03.04прогин |
|  |  | К.В. Воробьева |
|  | | | | | | |  |  | ( И.О. Фамилия ) |
|  | | | | | | | | | |
|  | | | | | | |  |  |  |
|  | | | | | | |  |  |  |
|  | | | |  |  | |  |  |  |
|  | | | |  |  | |  |  |  |
|  |  |  |  | | |  |  |  |  |
|  | | | | | | | | | |

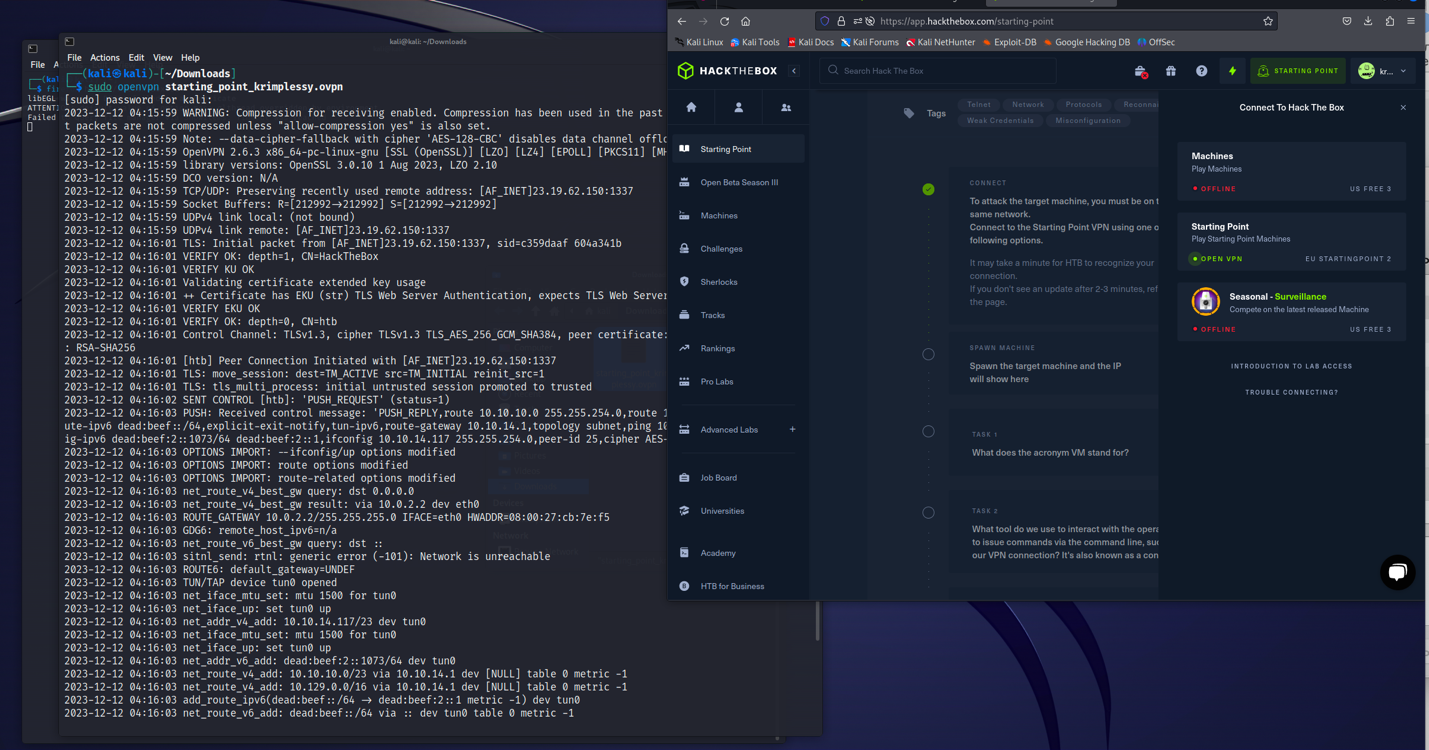
г. Владивосток

2023

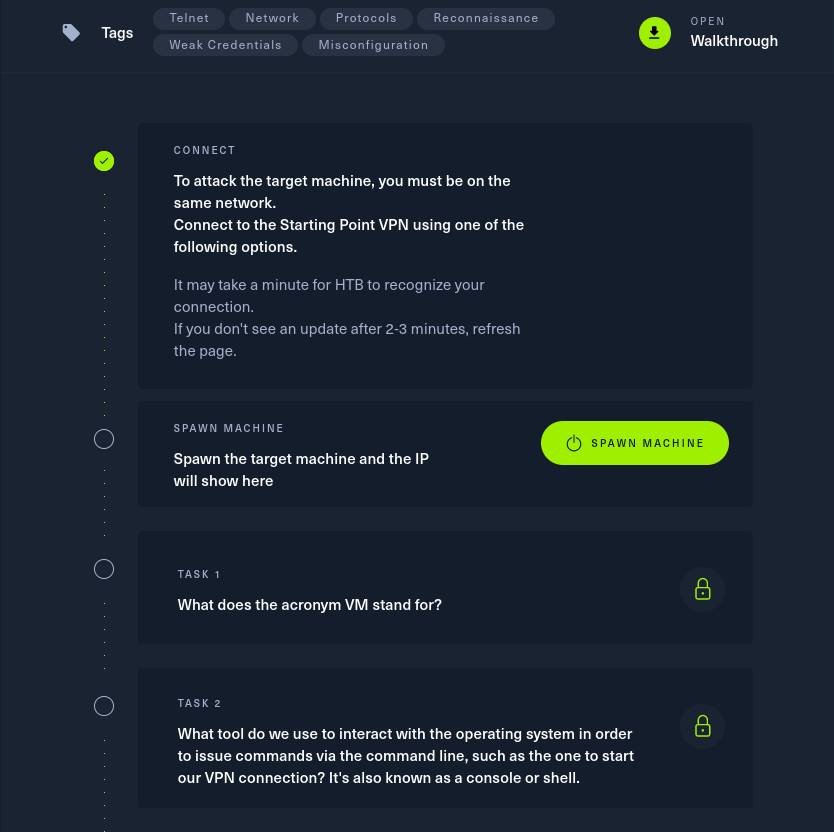
Сначала подключаем HackTheBox к нашей виртуальной машине.



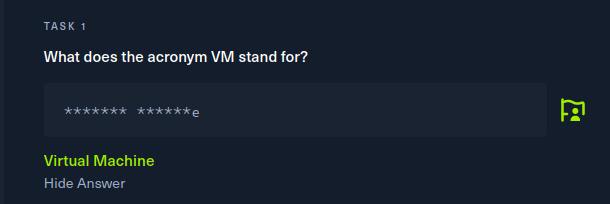
Командой firefox <http://hackthebox.eu> мы открываем браузер firefox на сайте HackTheBox.



**MEOW**

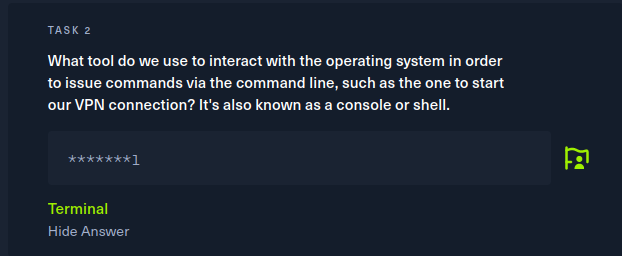


**Task1:** Что означает аббревиатура VM?



Virtual Machine (VM) – виртуальная машина, виртуальная среда, работающая как настоящий компьютер, но внутри другого компьютера. Запускается такая машина на изолированном разделе жесткого диска, установленного в компьютере-хосте.

**Task 2:** Какой инструмент вы используете для взаимодействия с операционной системой, чтобы запустить наше VPN-соединение? Оно также известно, как консоль или shell.

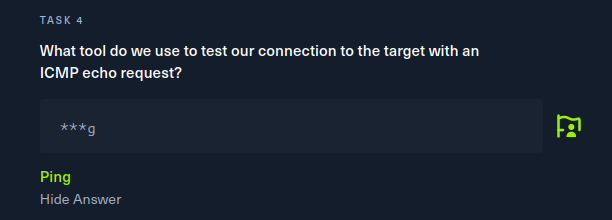


**Task 3**: Какой сервис вы используете для формирования нашего VPN-соединения?



Это VPN, который мы использовали при запуске и подключении starting point.

**Task 4**: Какой инструмент вы используете для проверки соединения с целью с помощью ICMP-эхо-запроса?



Команда **ping** позволяет проверять собственную связь и состояние удаленных хостов, тестировать качество сетей.

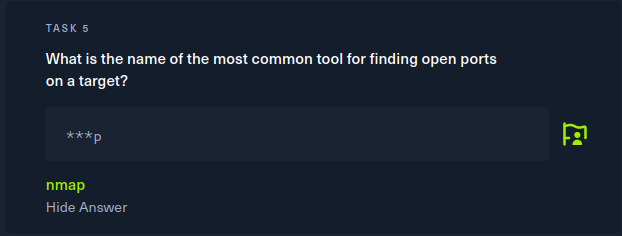
**ICMP**, который расшифровывается как **Internet Control Message Protocol** это сетевой протокол, который используется для диагностики проблем со связностью в сети. Говоря простым языком, ICMP помогает определить может ли достичь пакет адреса назначения в установленные временные рамки.

Основная цель ICMP это отчетность об ошибках. При соединении двух девайсов в сети, если часть данных не доходит до адреса назначения, теряется или превышает допустимые таймауты - ICMP генерирует ошибки.

Второе, и, пожалуй, одно из самых популярных применений ICMP это утилита ping. Термин “пинговать" как - раз связан с протоколом ICMP и “пинговать" хост - означает отправлять ICMP пакеты с целью понять, отвечает ли на них целевое устройство.

Эхо-запрос ICMP означает, что хост, которому адресовано сообщение, должен ответить непосредственно на пакет, используя эхо-ответ.

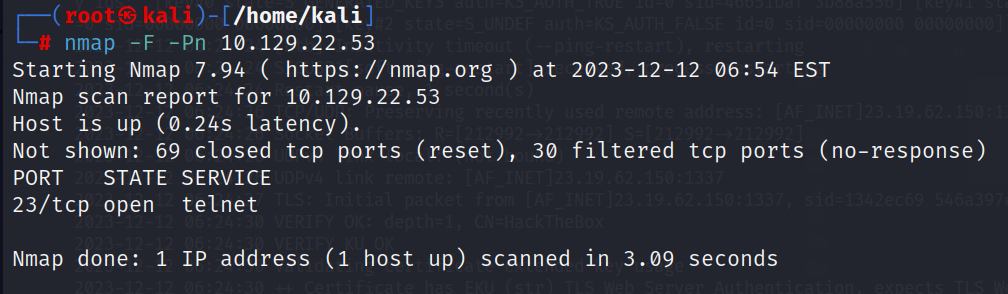
**Task 5**: Как называется наиболее распространенный инструмент для поиска открытых портов на цели?



**Nmap** («**Network Mapper**») — это утилита с открытым исходным кодом для исследования сети и проверки безопасности (для сканирования хоста и сети, чтобы определить уязвимые точки).

**Task 6**: Какую службу вы идентифицировали на порту 23/tcp во время вашего сканирования?



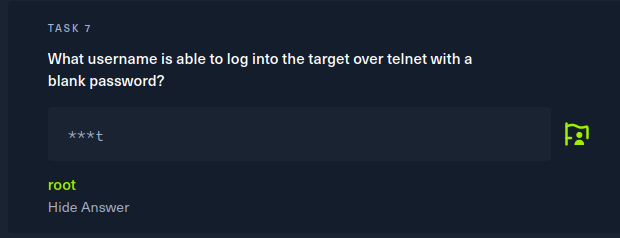


**Telnet** — это традиционный протокол для удалённого подключения к консоли через TCP. Telnet использует незашифрованное соединение, что небезопасно, поскольку соединения можно легко перехватить и даже манипулировать ими. При подключении через недоверенные сети используйте VPN для защиты соединения.

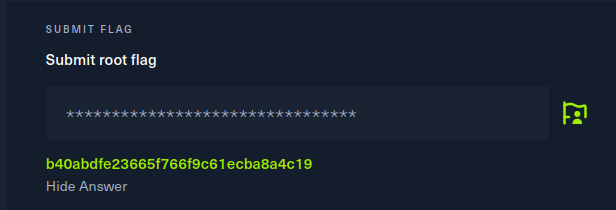
Уязвимости **Telnet**: аутентификация на базе открытого текста.

**TCP-порт 23** использует протокол управления передачей данных (TCP), который является одним из основных протоколов в сетях TCP.

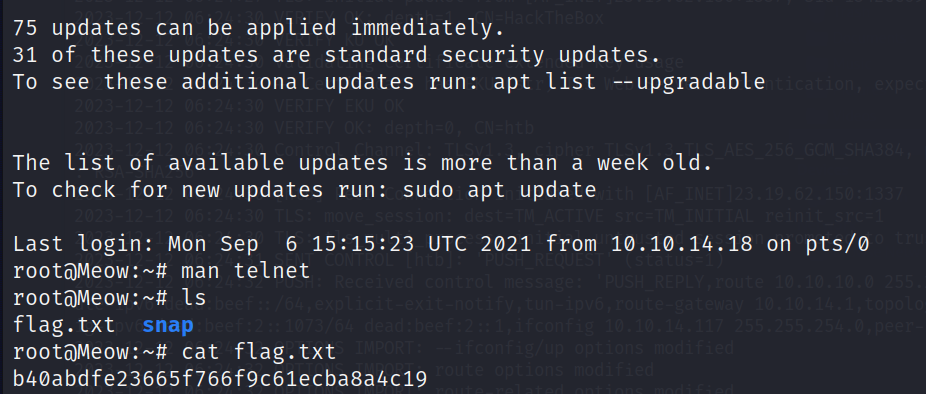
**Task 7**: Какое имя пользователя (логин) может войти в цель через telnet с пустым паролем?



**Task:** Отправить корневой флаг.







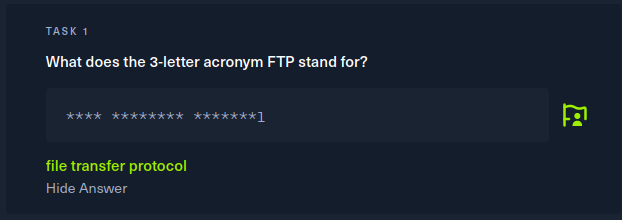
Флаг лежал в домашней директории. Полный доступ к системе был успешно получен.

Уязвимость данной машины заключается в открытом протоколе telnet.

**FAWN**



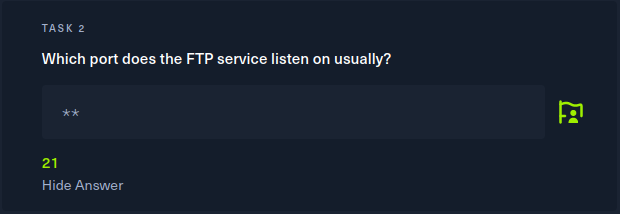
**Task 1:** Что означает трехбуквенная аббревиатура FTP?



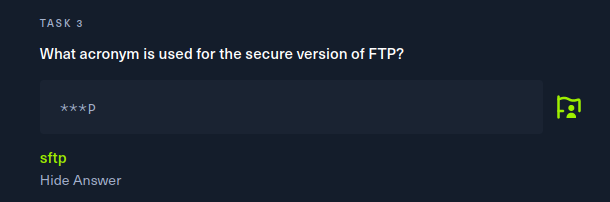
**FTP** – это протокол для передачи данных через интернет. Аббревиатура расшифровывается как **File Transfer Protocol**, в переводе — «протокол передачи данных».

Уязвимости FTP: аутентификация на базе открытого текста, доступ по умолчанию.

**Task 2:** Какой порт обычно прослушивает FTP?



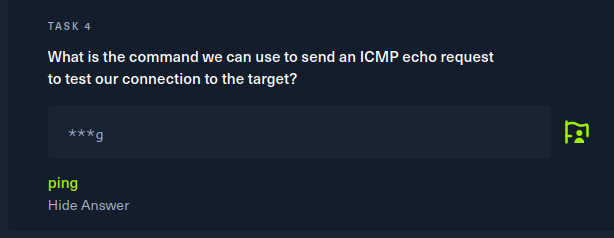
**Task 3:** Какая аббревиатура используется для обозначения защищенной версии FTP?



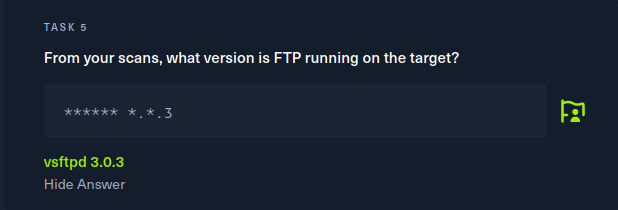
Протокол FTP очень небезопасный протокол, потому что он передает информацию в виде открытого текста.

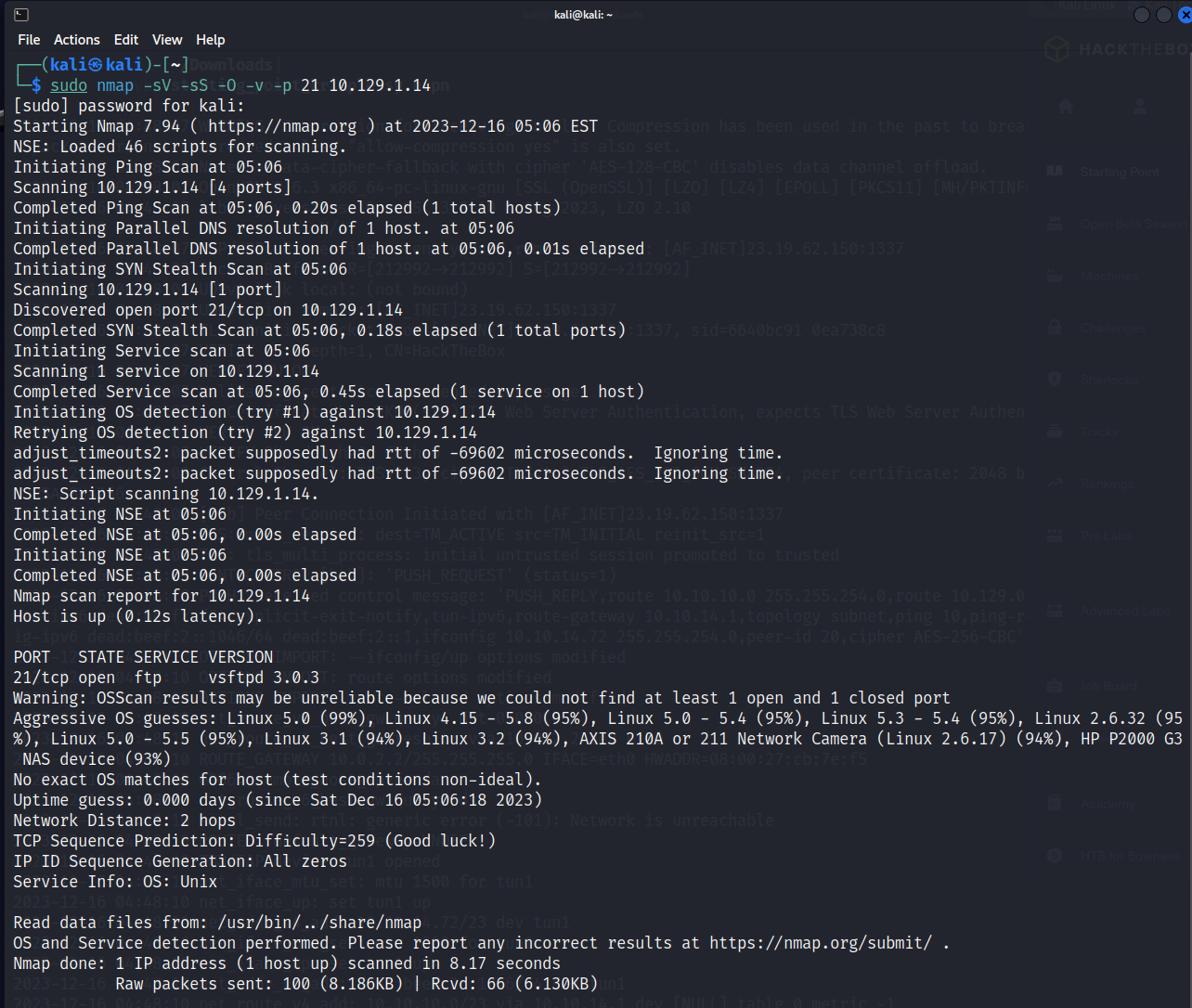
**SFTP** расшифровывается как **Secure File Transfer Protocol**. Самое очевидное преимущество SFTP – это, конечно же, безопасность и конфиденциальность. Нельзя сказать, что данные, передаваемые с использованием протокола SFTP, невозможно украсть, но сделать это очень сложно.

**Task 4:** Какую команду мы можем использовать для отправки эхо-запроса ICMP для проверки нашего соединения с целью?

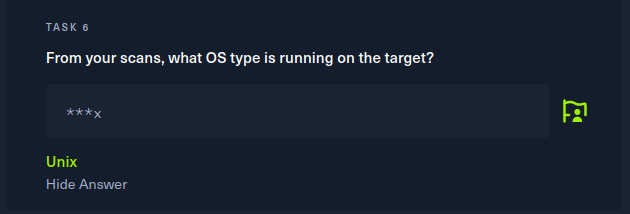


**Task 5:** Судя по вашим сканам, какая версия FTP работает на целевой системе?



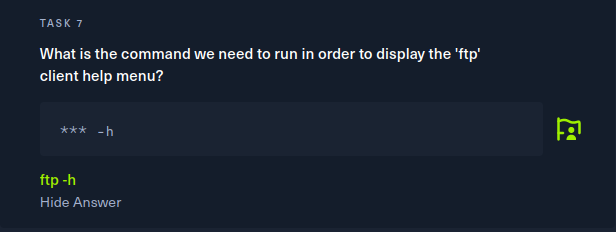


**Task 6:** Судя по вашим сканам, какой тип ОС работает на целевой системе?



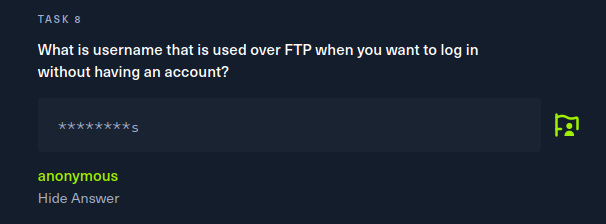
**UNIX** (**Uniplexed Information and Computing Service** (единый информационно-вычислительный сервис) – многопользовательская операционная система. Со стороны пользователя кажется, что весь сервер в его распоряжении, но на самом деле сервером могут пользоваться одновременно десятки человек и не знать о том, что сервер выполняет что-то ещё.

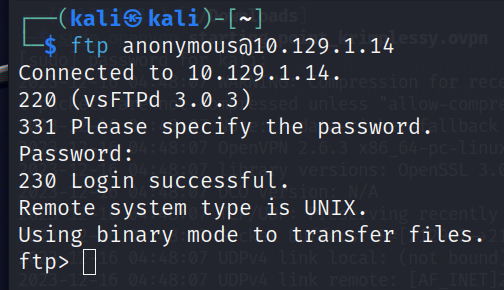
**Task 7:** Какую команду нам нужно выполнить, чтобы отобразить «FTP» меню помощи клиенту?



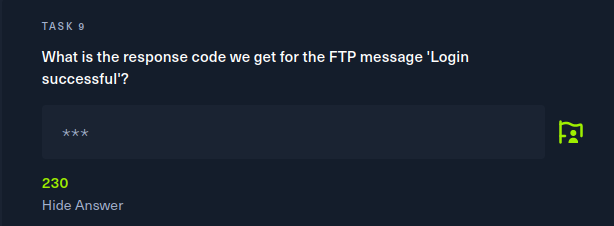


**Task 8:** Какое имя пользователя используется через FTP, когда вы хотите войти в систему без учетной записи?

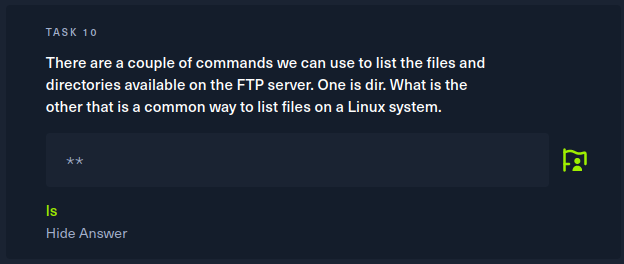


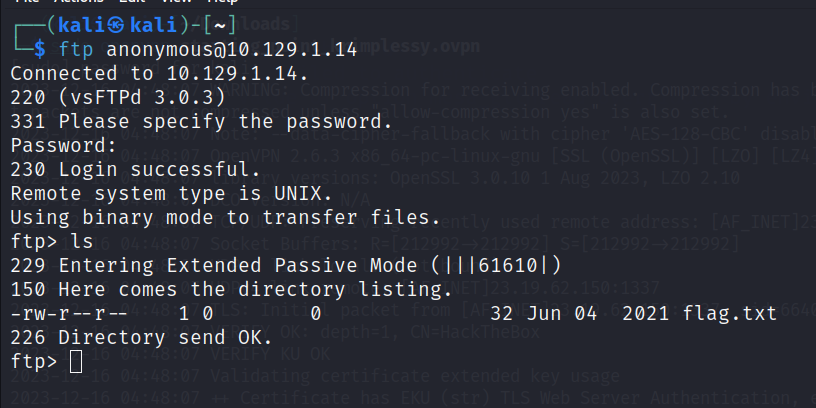


**Task 9:** Какой код ответа мы получаем на FTP-сообщение «Login successful»?

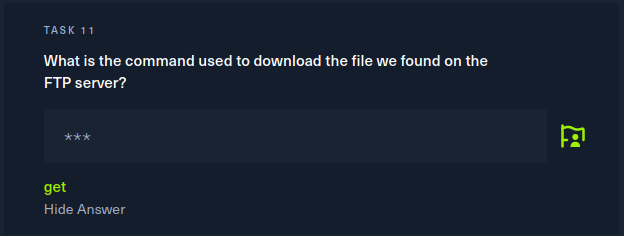


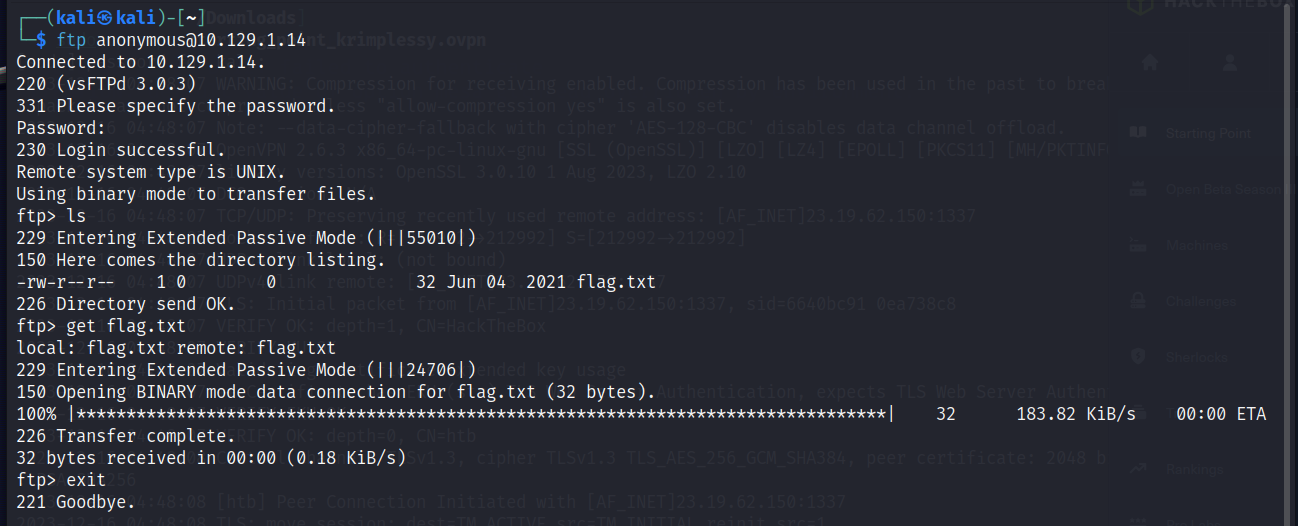
**Task 10:** Есть несколько команд, которые мы можем использовать для вывода списка файлов и каталогов, доступных на FTP-сервере.





**Task 11:** Какая команда используется для загрузки файла, который мы нашли на FTP-сервере?

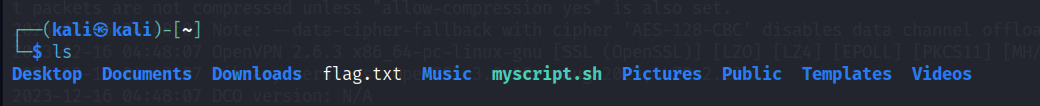


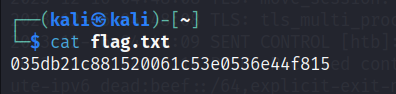


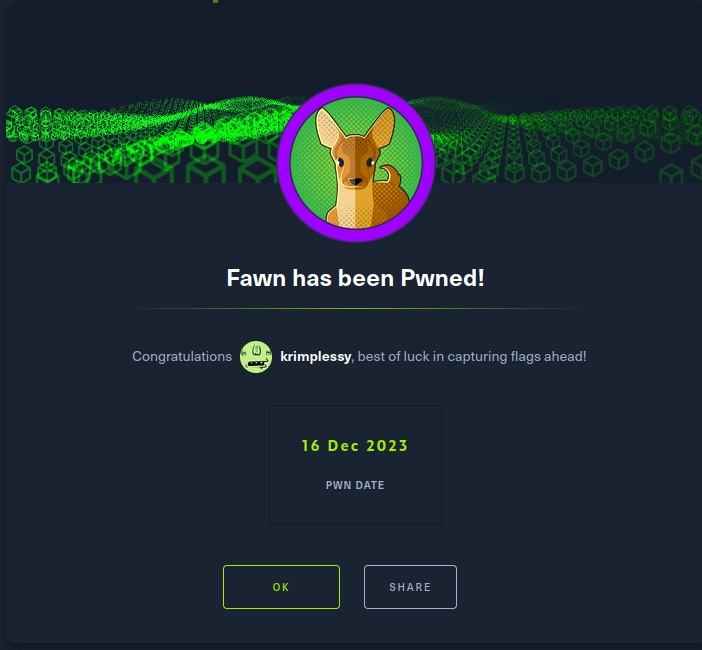
Команда **GET** используется для загрузки файлов с сервера на ваш компьютер.

**Task 12:** Отправить корневой флаг.

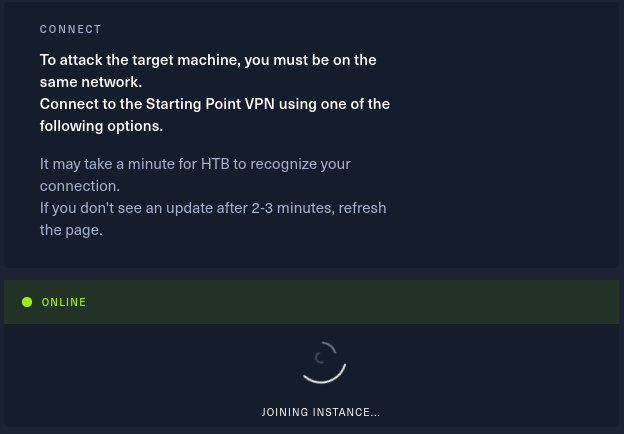




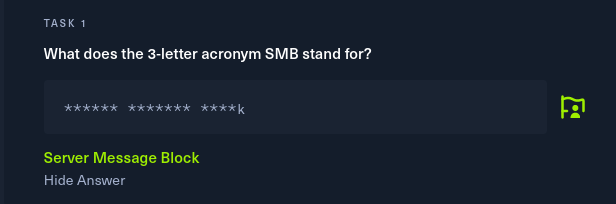




**DANCING**

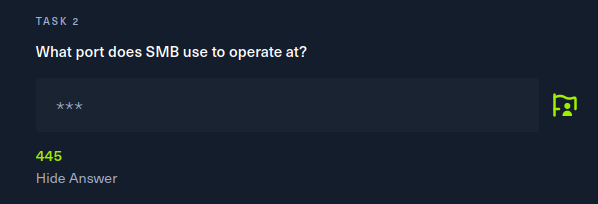


**Task 1:** Что означает трехбуквенная аббревиатура SMB?



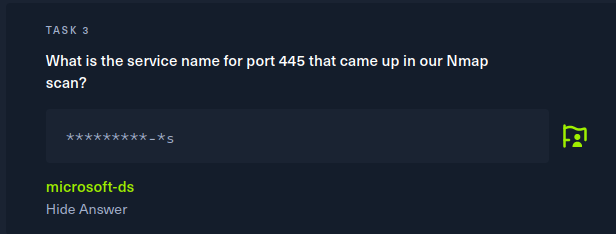
Протокол **SMB (Server Message Block)** – это сетевой протокол для общего доступа к файлам, который позволяет приложениям компьютера читать и записывать файлы, а также запрашивать службы серверных программ в компьютерной сети.

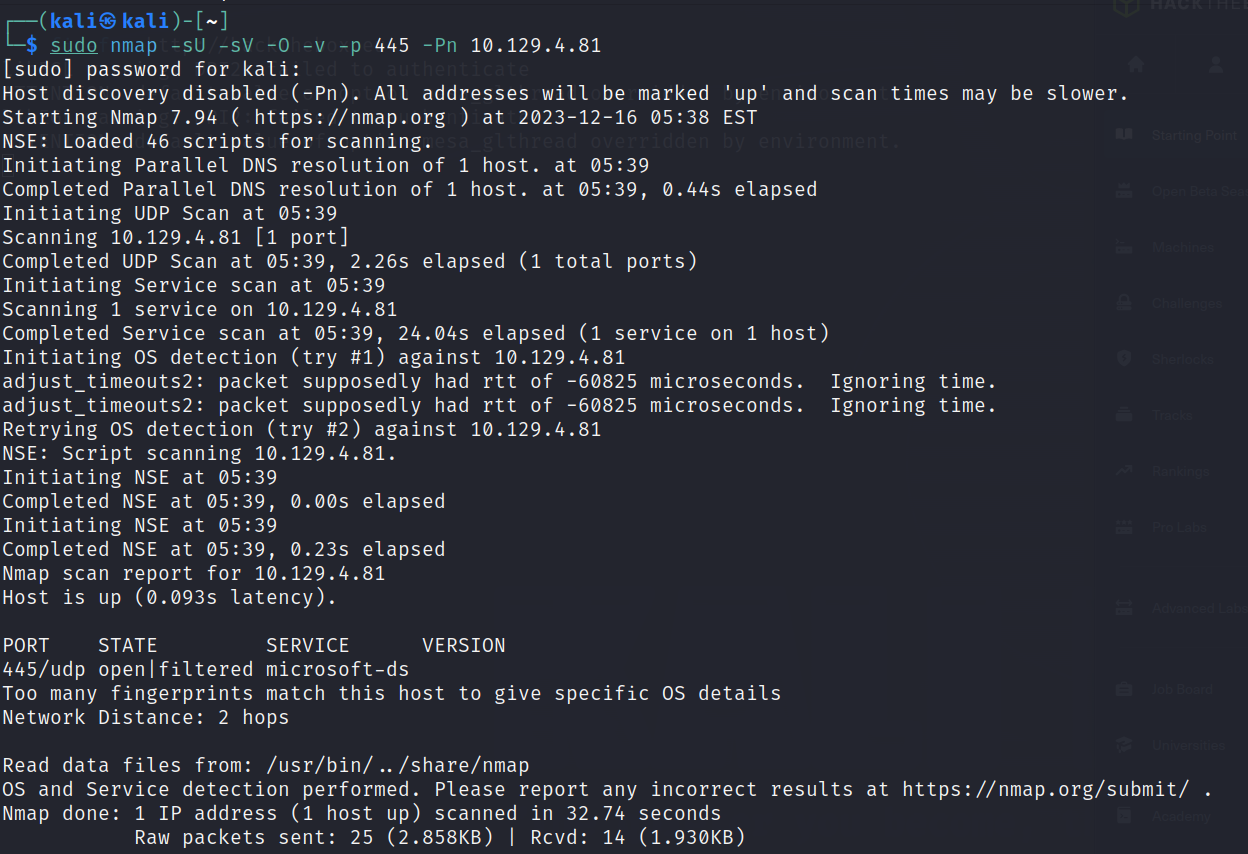
**Task 2:** Какой порт использует SMB для работы?



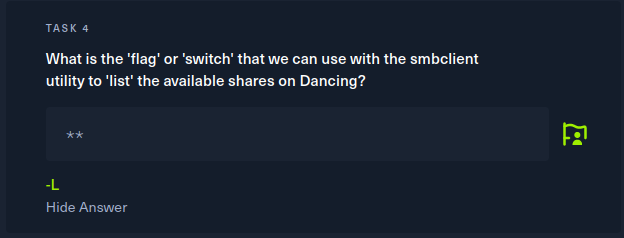
Порт 445 – это порт, который отвечает за передачу данных по протоколу SMB. Порт 445 используется для подключения и передачи данных между клиентами и серверами в сети Windows. Однако, поскольку этот порт открыт по умолчанию, злоумышленники могут использовать его для проведения атак на систему.

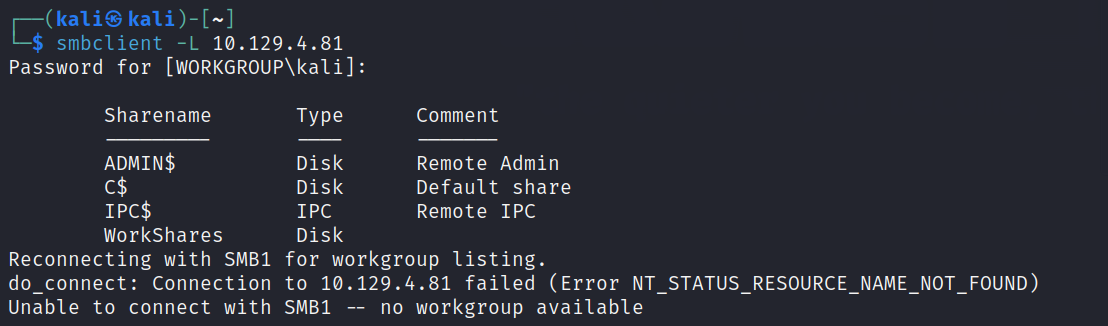
**Task 3:** Какое имя службы для порта 445, которое появилось в нашем Nmap сканировании?



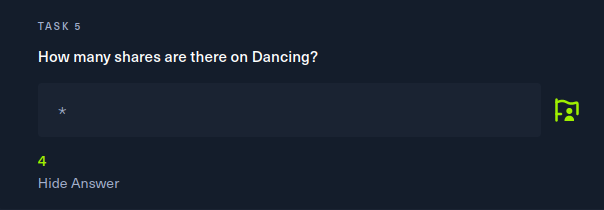


**Task 4:** Какой «флаг» или «переключатель» мы можем использовать с утилитой smbclient для «списка» доступных общих ресурсов на Dancing?

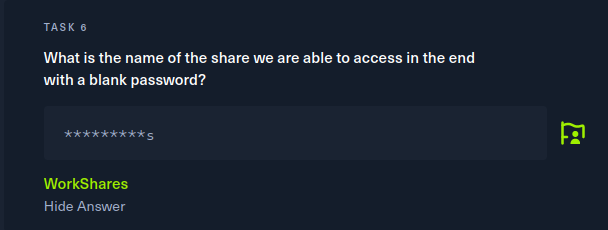


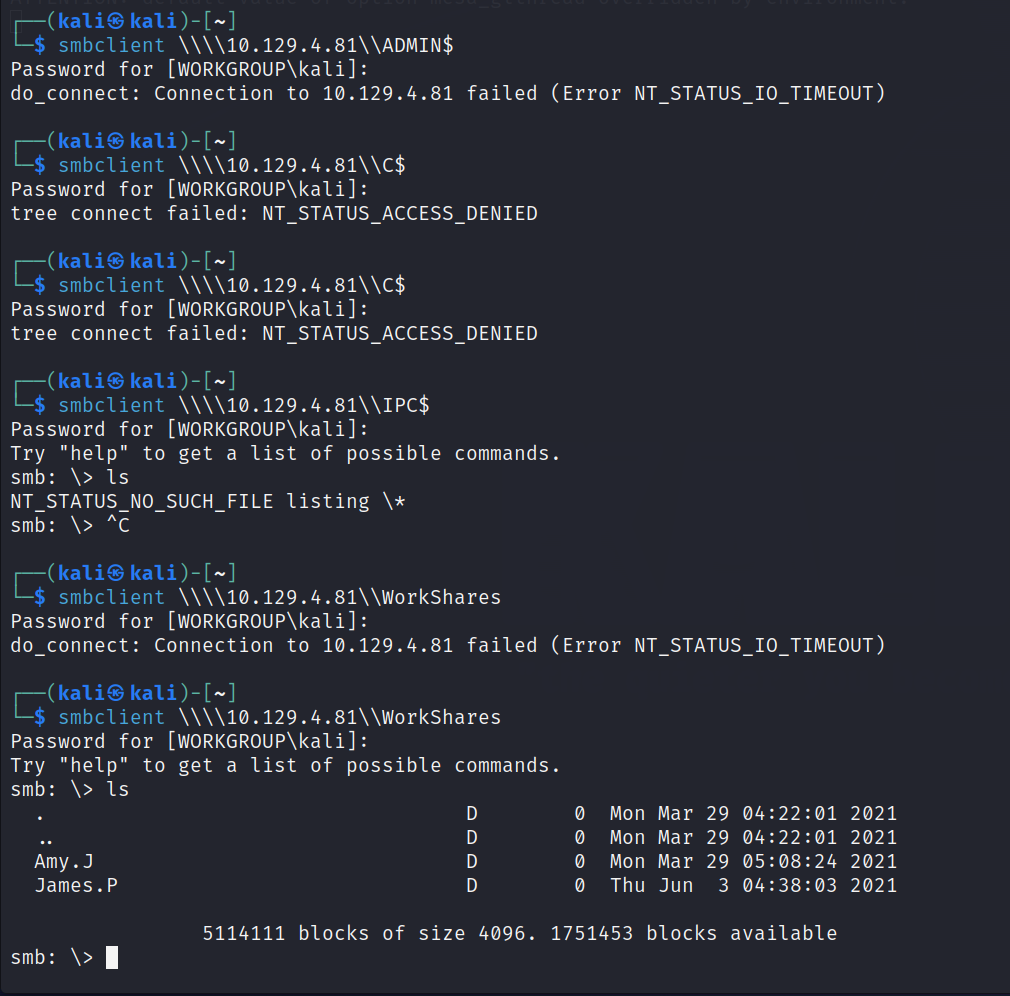


**Task 5:** Как много shares в Dancing?

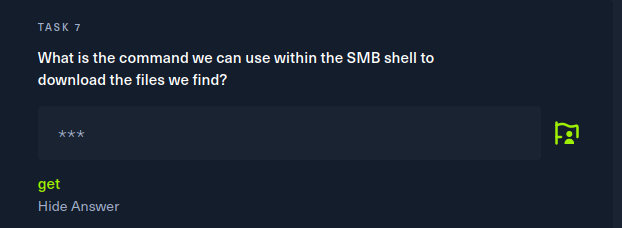


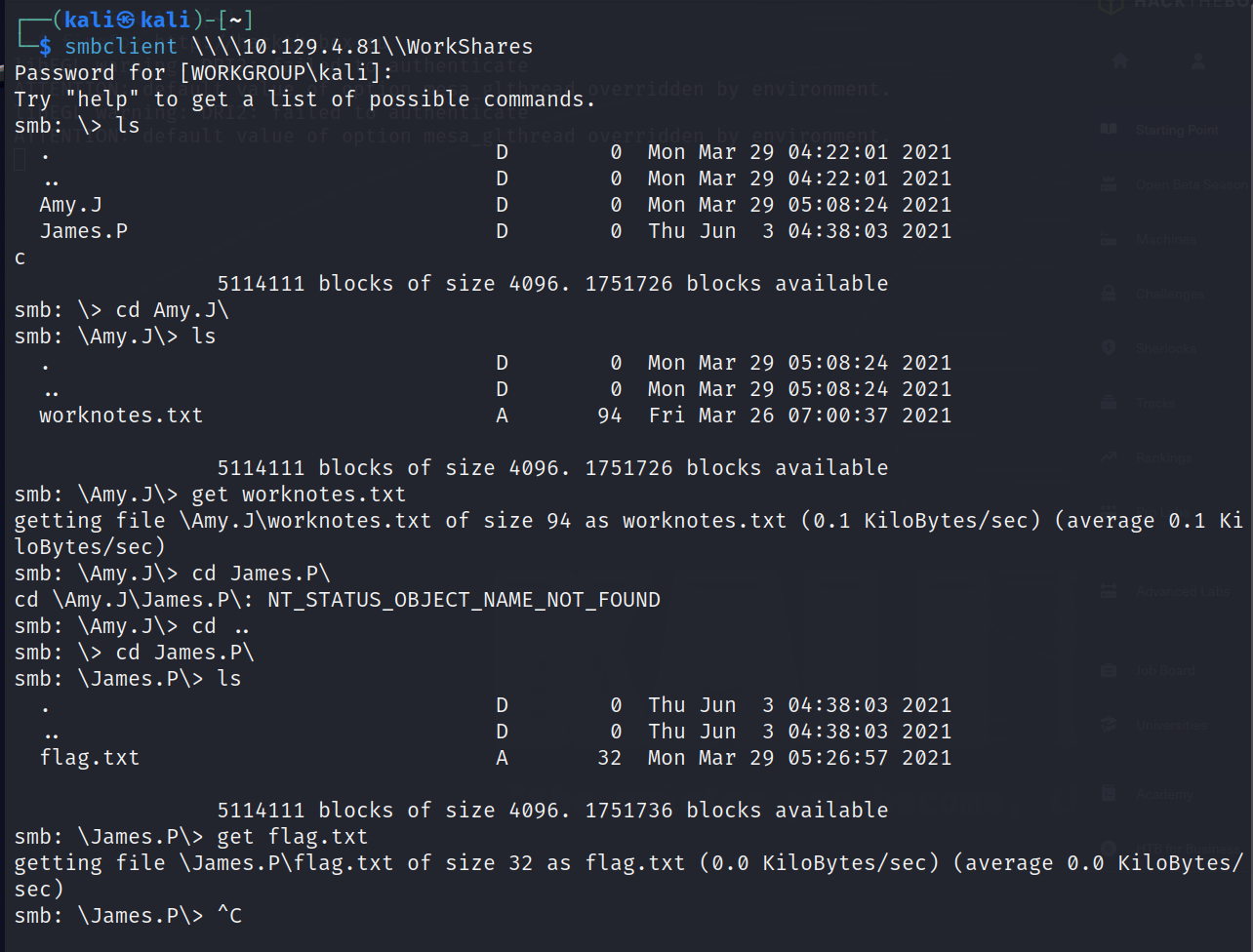
**Task 6:** Как называется общий ресурс, к которому мы можем получить доступ с пустым паролем?



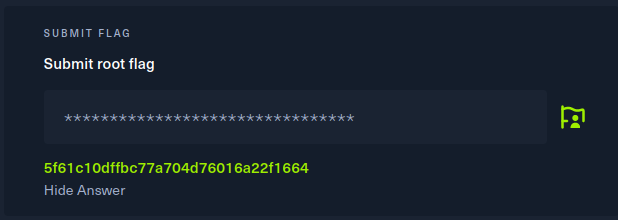


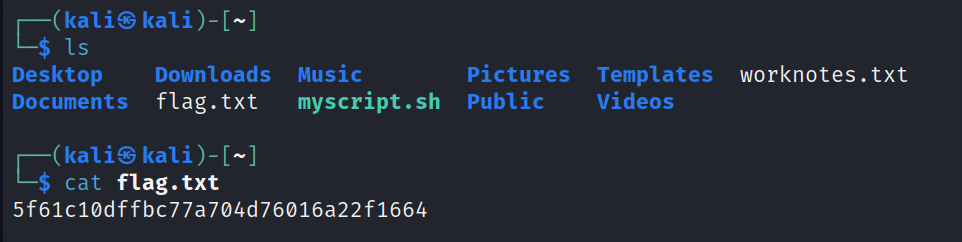
**Task 7:** Какую команду мы можем использовать в оболочке SMB для загрузки найденных файлов?

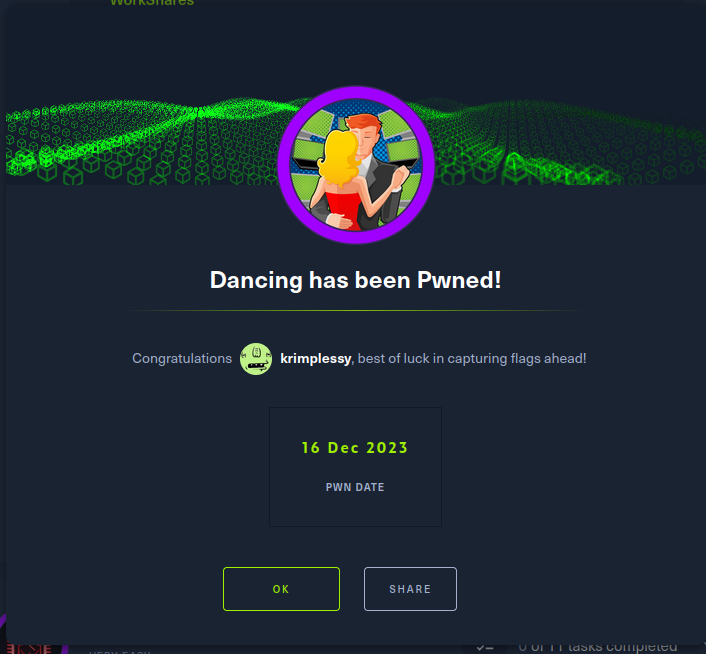




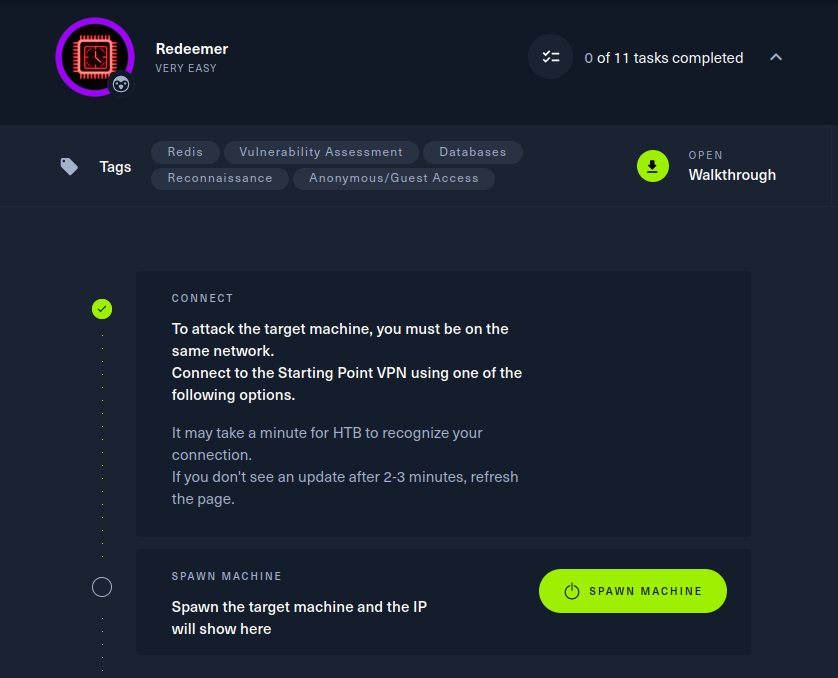
**Task 8:** Отправить корневой флаг.



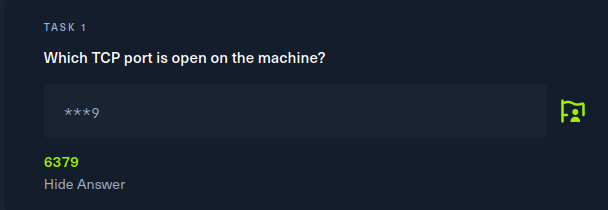


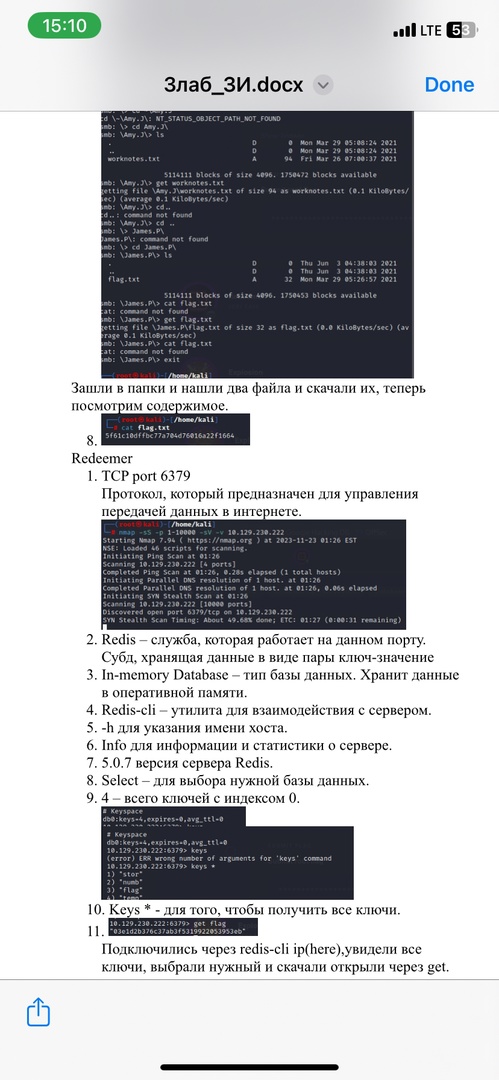


**REDEEMER**

****

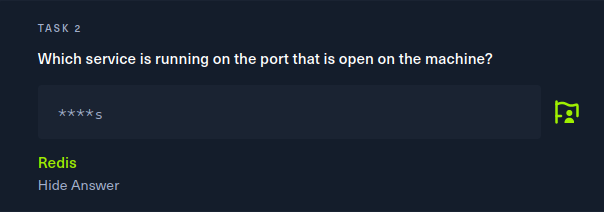
**Task 1:** Какой TCP-порт открыт на компьютере?

****



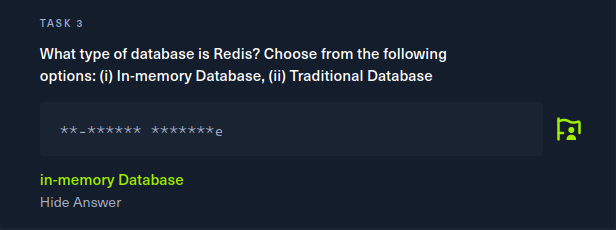
**TCP-порты** используются для установления надежных соединений, которые гарантируют доставку данных без потерь и повторов.

**Task 2:** Какая служба работает на порту, открытом на машине?

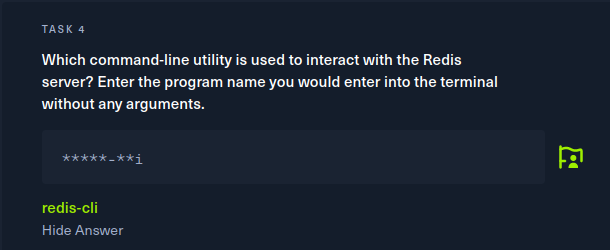
****

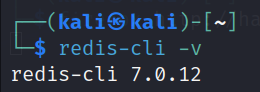
**Redis** – это система управления базами данных, которая хранит информацию в виде пар ключ-значение. Ключ — это название какого-то поля, а значение — его содержание. Это хранилище данных в памяти с открытым исходным кодом.

**Task 3:** Какой тип базы данных представляет собой Redis? 1) База данных в памяти. 2) Традиционная база данных.

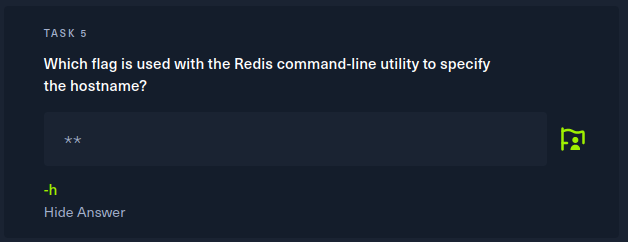
****

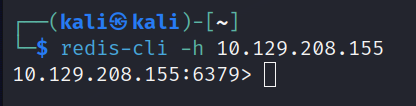
**Task 4:** Какая утилита командной строки используется для взаимодействия с сервером Redis? Введите имя программы, которое вы вводите в терминал без каких-либо аргументов.

****

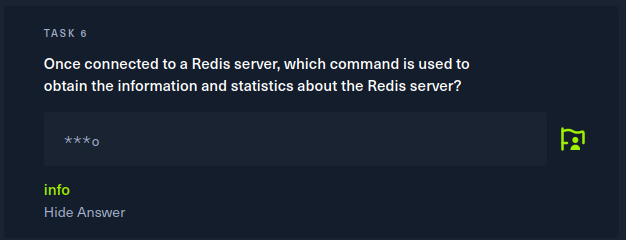
****

**Task 5:** Какой флаг используется утилитой командной строки Redis для указания имени хоста?

****

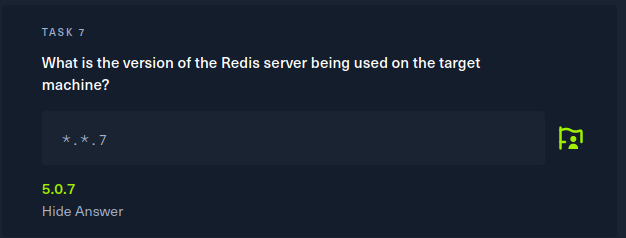
****

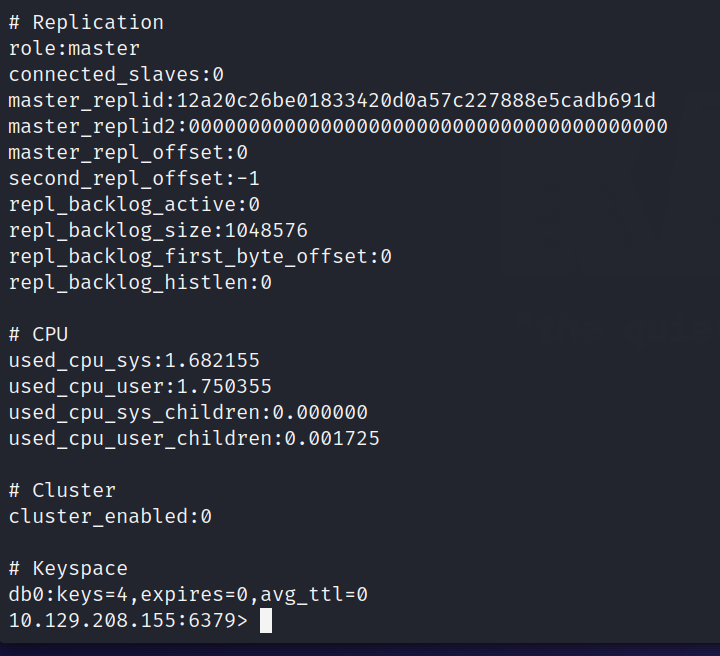
**Task 6:** Какая команда используется после подключения к серверу Redis для получения информации и статистики о сервере Redis?

****

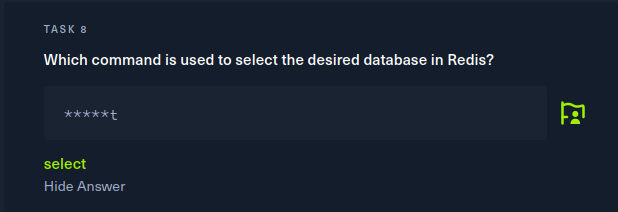
****

**Task 7:** Какая версия сервера Redis используется целевой машине?

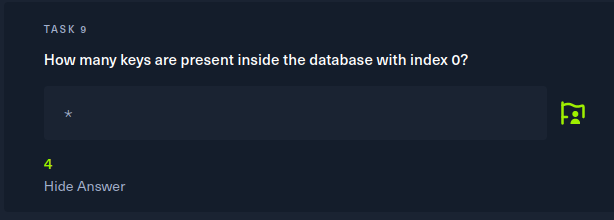
****

****

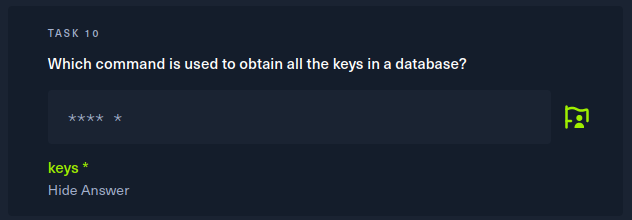
**Task 8:** Какая команда используется для выбора нужной базы данных в Redis?

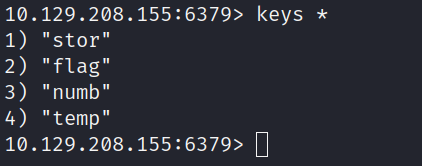
****

**Task 9:** Сколько ключей присутствует в базе данных с индексом 0?

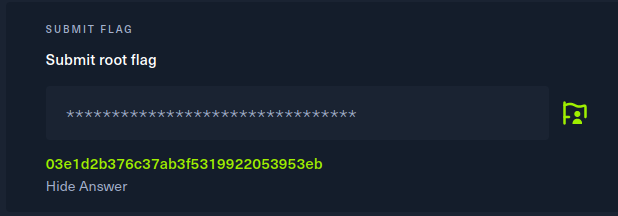
****

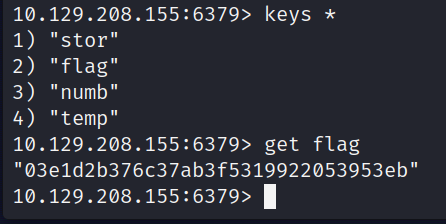
**Task 10:** Какая командаиспользуется для получения всех ключей в базе данных?

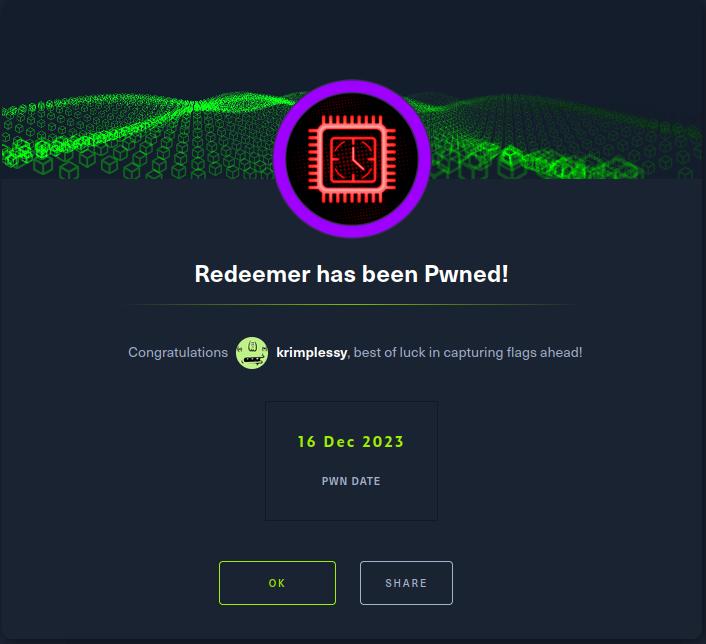
****

****

**Task 11:** Отправить корневой флаг.

****

****

****

**Итог:**

****