РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет экономический

Кафедра экономико-математического моделирования

**Лабораторная Работа №1**

на тему

**«Защита данных файлового сервера»**

38.03.05 — Кибербезопасность в экономике

Выполнили

Студенты группы НБИбд-02-22

Студенческий билет №: 1132229056

Д.Д. Панченко

*(подпись)*

Студенческий билет №: 1132222827

П.А. Савурская

*(подпись)*

Студенческий билет №: 1132221541

Н.Р. Кочарян

*(подпись)*

Студенческий билет №: 1132220820

Д.В. Чистякова

*(подпись)*

Студенческий билет №: 1132229527

А.В. Захаренко

*(подпись)*

Студенческий билет №: 1132220826

В.В. Щербакова

*(подпись)*

Студенческий билет №: 1032228104

Е. Кроитору

*(подпись)*

« » 2024 г.

Проверил

к.ф.-м.н., доцент кафедры теории вероятностей и кибербезопасности,

В.А. Бесчастный

*(подпись)*

Москва 2024

**Оглавление**

Список сокращений 3

Введение 4

Ход работы 5

1. Простой пароль пользователя веб-приложения предприятия 5

2.1. Служба RDP на порту установлена по умолчанию 9

2.2. Последствие Manager meterpreter 11

3.1. Служба RDP на порту установлена по умолчанию 13

3.2. Последствие FS Backdoorу 17

Вывод 19

# Список сокращений

**Русскоязычные сокращения**

|  |  |
| --- | --- |
| БД | База данных |
| ПО | Программное обеспечение |

**Англоязычные сокращения**

|  |  |
| --- | --- |
| CVE | Demilitarized Zone |
| DMZ | Demilitarized Zone |
| OWA | Outlook Web Access |
| RDP | Remote Desktop Protocol |

# Введение

Внешний злоумышленник находит в интернете сайт Компании и решает провести атаку на него с целью получения доступа к внутренним ресурсам. На сайте был обнаружен раздел для входа в личный кабинет, который не содержит защитных механизмов от атаки перебора учетных данных. Нарушитель смог успешно подобрать параметры входа для одного из пользователей.

Использование одинаковых паролей для различных сервисов позволило нарушителю получить доступ к почтовому ящику сотрудника и далее успешно подключиться к его рабочей станции, с которой он атаковал внутренний файловый сервис с помощью уязвимости в windows-реализации SMB-протокола.

Квалификация нарушителя средняя. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

# Ход работы

## Простой пароль пользователя веб-приложения предприятия

На узле Web Server PHP обслуживается веб-сайт предприятия. В веб-приложении существует механизм аутентификации пользователей.

С помощью ViPNet IDS NS детектируем инструмент перебора паролей hydra, атака происходит на порт 10.10.1.20 (Рисунок 1).

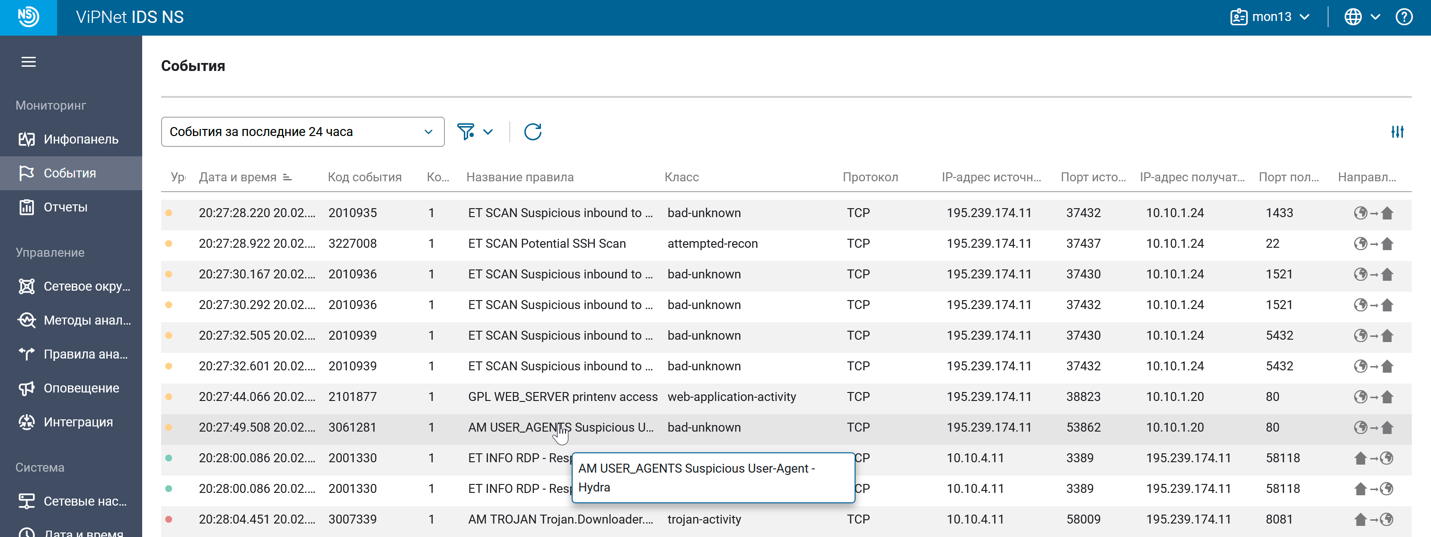


Рисунок . Сканирование серверов из Интернета

Передаем данные группе реагирование (Рисунок 2).

Изображение выглядит как текст, программное обеспечение, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 2. Передача данных

Аутентифицируемся на узле Web Server PHP, воспользовавшись учетной записью user и SSH 10.10.1.20 (Рисунок 3), через Bitvise SSH Client (Рисунок 4).

Изображение выглядит как текст, чек, число, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 3. Данные для входа в виртуальные среды

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 4. Переход в учетную запись user через клиент SSH

Авторизуемся в MySQL, используя логин и пароль. Для вывода всех таблиц БД выполним команды show databases;, use toppro;, show tables; (Рисунок 5).

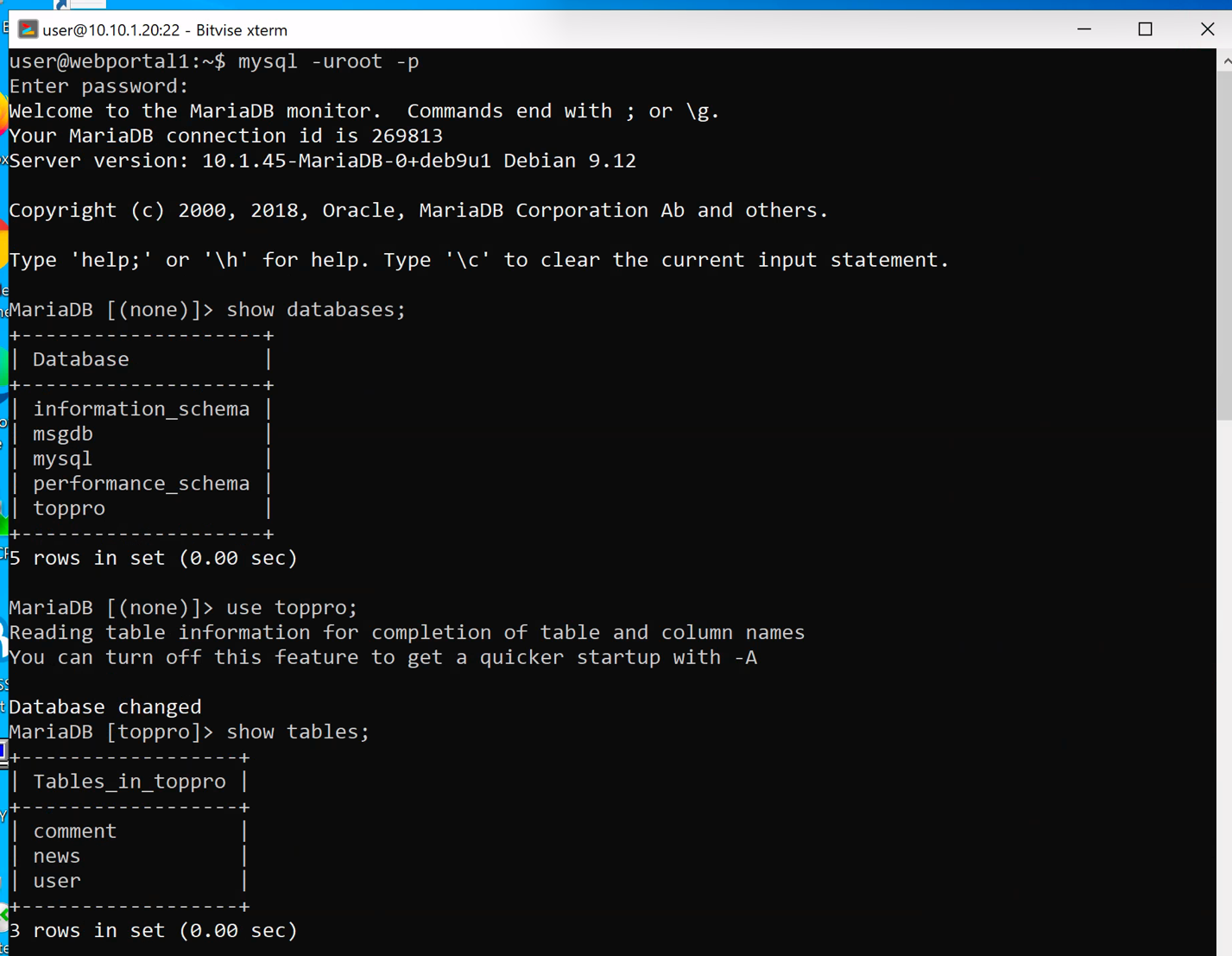


Рисунок 5. Авторизация и вывод таблиц БД «toppro»

Для вывода всех данных в таблице воспользуемся командой SELECT \* FROM user;. В конце таблицы мы видим скомпрометированный пароль пользователя «Manager1» (Рисунок 6).

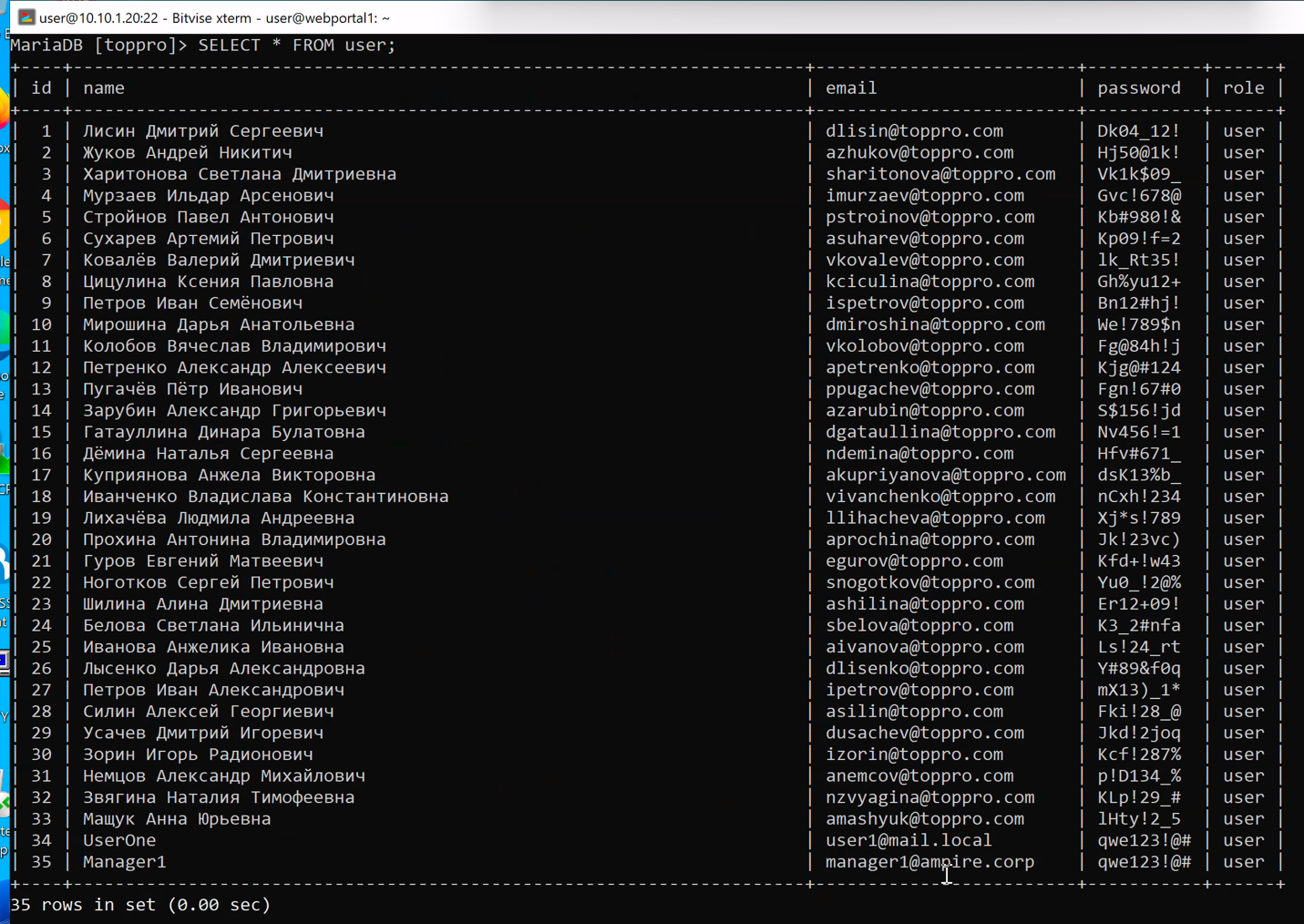


Рисунок 6. Вывод таблицы user

Выполним команду update user set password = ‘YOUR PASSWORD’ where name = ‘Manager1’ и сменим пароль для пользователя (Рисунок 7).

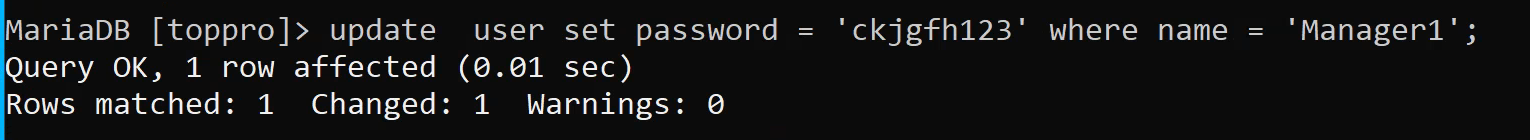


Рисунок 7. Успешное изменение пароля пользователя

Перейдём в Ampire и убедимся в успешном устранении уязвимости (Рисунок 8).

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 8. Успешное устранение уязвимости Web1 MySQL Password

## Служба RDP на порту установлена по умолчанию

На узле менеджера Manager Workstation 1 для внешней сети открыт порт 3389, обслуживающий соединения по протоколу RDP.

С помощью ViPNet IDS NS детектируем этап атаки на внутренний хост 10.10.4.11 (Рисунок 9).

Изображение выглядит как текст, снимок экрана, чек, дизайн

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 9. События атаки на внутренний хост

Передаем данные группе реагирование (Рисунок 10).

Изображение выглядит как текст, программное обеспечение, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 10. Передача данных

Для закрытия уязвимости отключим доступ по RDP для узла Manager Workstation 1.

Для этого подключимся к узлу менеджера Manager Workstation 1, находящейся во внутренней сети, по протоколу RDP (Рисунок 11).

Изображение выглядит как текст, программное обеспечение, веб-страница, Значок на компьютере

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 11. Подключение к узлу Manager Workstation 1

Зайдем на EdgeGW (WEB: https://10.10.1.254). Введем данные и нажмем sign in (Рисунок 12).

Изображение выглядит как текст, программное обеспечение, снимок экрана, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 12. EdgeGW

Отключим доступ по RDP для виртуальной машины менеджера Manager1 (Рисунок 13).

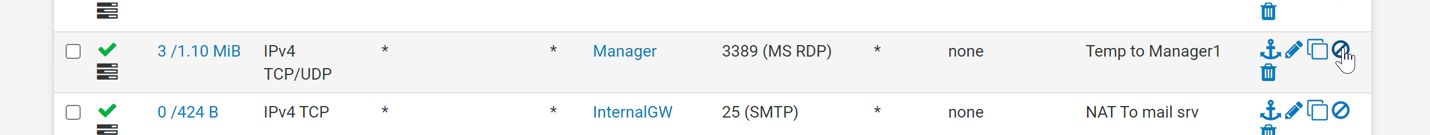


Рисунок 13. Отключение правил проброса RDP портов

Перейдём в Ampire и убедимся в успешном устранении уязвимости (Рисунок 14).

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 14. Успешное устранение уязвимости RDP Checker

## Последствие Manager meterpreter

Нарушитель устанавливает shell соединение с машиной Manager1.

Подключимся к узлу администратора Administrator Workstation, находящейся во внутренней сети, по протоколу RDP (Рисунок 15).

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 15. Подключение к узлу Administrator Workstation

Установленную сессию с нарушителем и имя процесса обнаруживаем с помощью утилиты netstat с ключами -bno (Рисунок 16).

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 16. Список установленных соединений

Мы видим активное соединение веб-портала с IP-адресом нарушителя (195.239.174.11). Для устранения завершаем соединение с помощью команды taskkill /f /pid <PID> (Рисунок 17).

Изображение выглядит как текст, снимок экрана, Шрифт, дизайн

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 17. Остановка процесса

Последствие Manager meterpreter успешно устранено, meterpreter-сессия с нарушителем (195.239.174.11) завершена. Перейдём в Ampire и убедимся в успешном устранении последствия (Рисунок 18).

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 18. Успешное устранение последствия Manager meterpreter

## Служба RDP на порту установлена по умолчанию

Узел MS FileServer является файловым сервером сети предприятия. Файловый сервер предоставляет центральный ресурс в сети для хранения и обеспечения совместного доступа к файлам пользователям сети.

С помощью ViPNet IDS NS детектируем эксплуатацию уязвимости MS17-010 по 445 порту (наиболее распространенный SMB порт) с помощью Metasploit Framework. Обнаруживается анализатором сетевых пакетов (Рисунок 19).

Изображение выглядит как текст, снимок экрана, число

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 19. Факт эксплуатации Eternalblue

Изучив цепочку атак, обнаруживаем, что атака адресована файловому серверу (ip: 10.10.2.12). Это подтверждает анализ событий в ViPNet TIAS (Рисунок 18).



Рисунок 20. Атака на узел 10.10.2.12

Передаем данные группе реагирование (Рисунок 21).

Изображение выглядит как текст, программное обеспечение, Мультимедийное программное обеспечение, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 21. Передача данных

Для устранения данной уязвимости для начала подключимся к RDP файлового сервера (Рисунок 22).

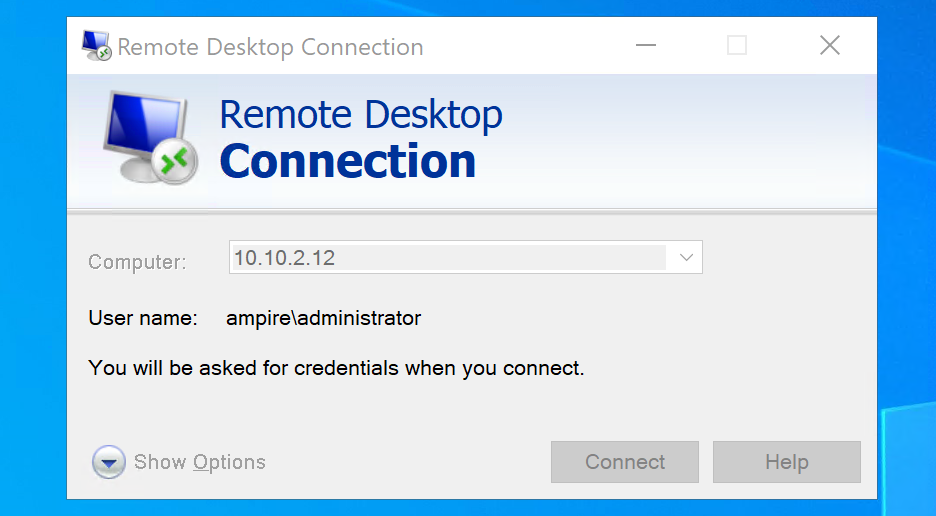


Рисунок 22. Подключение к RDP файлового сервера

Для закрытия уязвимости отключим SMB (Server Message Block) – сетевой протокол для удаленного доступа к файлам и принтерам (Рисунок 23).

Изображение выглядит как текст, снимок экрана, программное обеспечение, Операционная система

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 23. Подключение к RDP файлового сервера

Для его отключения выполним команду Set-SmbServerConfiguration -EnableSMB1Protocol $false в Windows PowerShell (Рисунок 24).

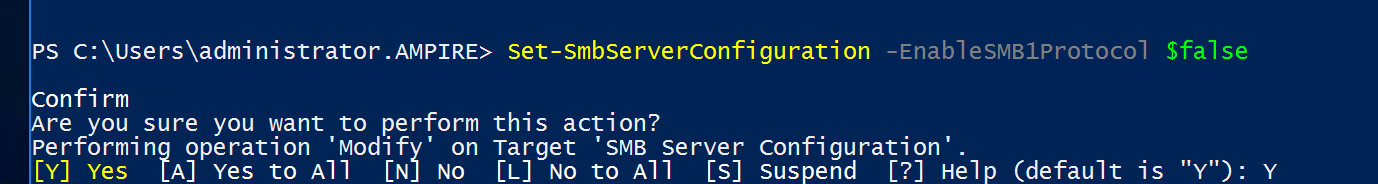


Рисунок 24. Отключение протокола SMBv1

Проверим отключение данного протокола (Рисунок 25).

Изображение выглядит как текст, снимок экрана, программное обеспечение, Операционная система

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 25. Проверка статуса на сервере

Уязвимость MS17-010 файлового сервера успешно устранена (Рисунок 26).

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 26. Успешное устранение уязвимости MS1710

## Последствие FS Backdoorу

Частым способом закрепления в скомпрометированной системе является создание вредоносного сервиса. Нарушитель может создать сервис, автоматически запускающий исполняемый файл, который устанавливает reverse shell подключение.

Установленную сессию файлового сервера с IP-адресом нарушителя (195.239.174.11) и имя запущенного процесса детектируем с помощью утилиты netstat с ключами -bno (Рисунок 27).

Изображение выглядит как текст, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 27. Соединения, вызванные backdoor в netstat

В диспетчере задач детектируем имя процесса и узнаём расположение исполняемого файла (Рисунок 28).

Изображение выглядит как текст, снимок экрана, Шрифт, число

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 28. Исполняемый файл в диспетчере задач

Для устранения полезной нагрузки завершим работу исполняемого файла в диспетчере задач, удалим данный файл из директории C:\Windows\Temp (Рисунок 29).

Изображение выглядит как снимок экрана, текст, программное обеспечение, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 29. Расположение AM\_backdoor.exe

После удаления исполняемого файла и остановки процесса последствие FS Backdoor успешно устранено (Рисунок 30).

Изображение выглядит как снимок экрана, текст, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 30. Успешное устранение последствия FS Backdoor

# Вывод

В данной лабораторной работе мы успешно устранили три уязвимости и два последствия (Рисунок 31–32):

1. Уязвимость 1. Простой пароль пользователя веб-приложения предприятия.
2. Уязвимость 2. Служба RDP на порту установлена по умолчанию.  
   Последствие. Meterpreter-сессия.
3. Уязвимость 3. MS17-010 файлового сервера (CVE-2017–0144).  
   Последствие. FS backdoor.

Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 31. Успешное устранение уязвимостей и последствий

Изображение выглядит как текст, Мультимедийное программное обеспечение, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 32. Успешное устранение уязвимостей и последствий

Кроме этого, мы выстроили примерную схему атаки, где красными линиями обозначены вредоносные действия нарушителя (Рисунок 33).

Изображение выглядит как снимок экрана, текст, диаграмма

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 33. Схема атаки