**­­г. Москва**

**МГТУ им Н. Э. Баумана**

**Отчёт**

**по лабораторной работе № 1**

**Работу выполнили:**

**Погребняк Мария, Борисова Мария,**

**Бучака Дарья**

**Группа ИУ10-14**

**2020 г.**

**Оглавление:**

|  |  |
| --- | --- |
| 1. **Постановка задачи………………….** | 3 |
| 1. **Анализ сети…………………………..** | 3 |
| 1. **Выявление злоумышленника и последствия его действий…………..** | 3 |
| 1. **Заключение…………………………..** | 7 |
| 1. **Примечания………………………….** | 7-8 |

**Постановка задачи**

Дан некий FTP сервер организации (10.44.50.150). По имеющейся информации злоумышленник оказывает некое вредоносное воздействие на данный сервер.

**Цель работы:** Подтвердить или опровергнуть информацию о вредоносном воздействии. В случае подтверждения информации принять необходимые меры для информационной безопасности.

**Анализ сети**

Благодаря logfip.rar и Wireshark, узнаем, что к данному FTP серверу организации (10.44.50.150) подключены следующие пользователи:

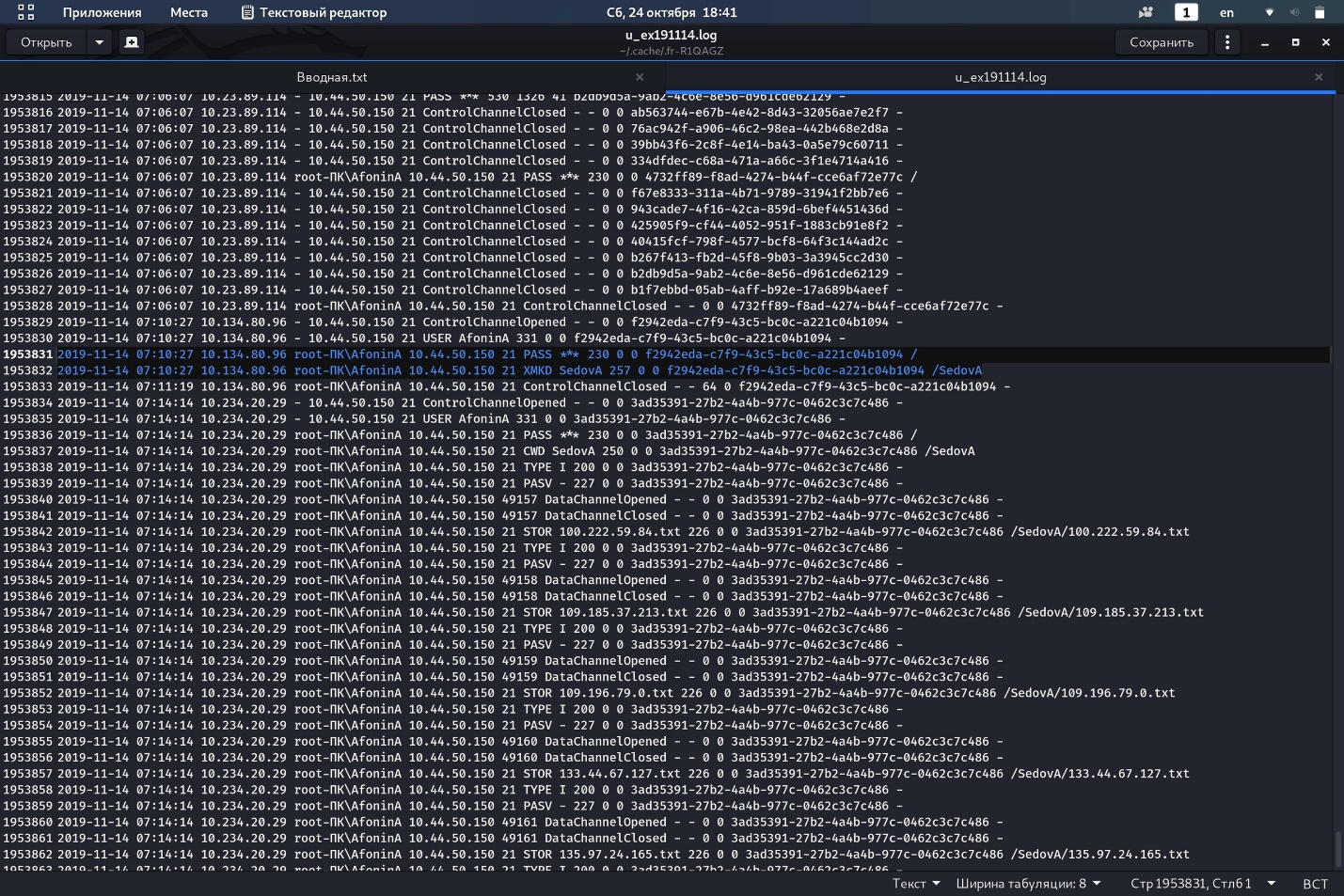
1. DolgalloP
2. EfimkinA
3. GalkaD
4. NaumivD
5. PankinM
6. AfoninA

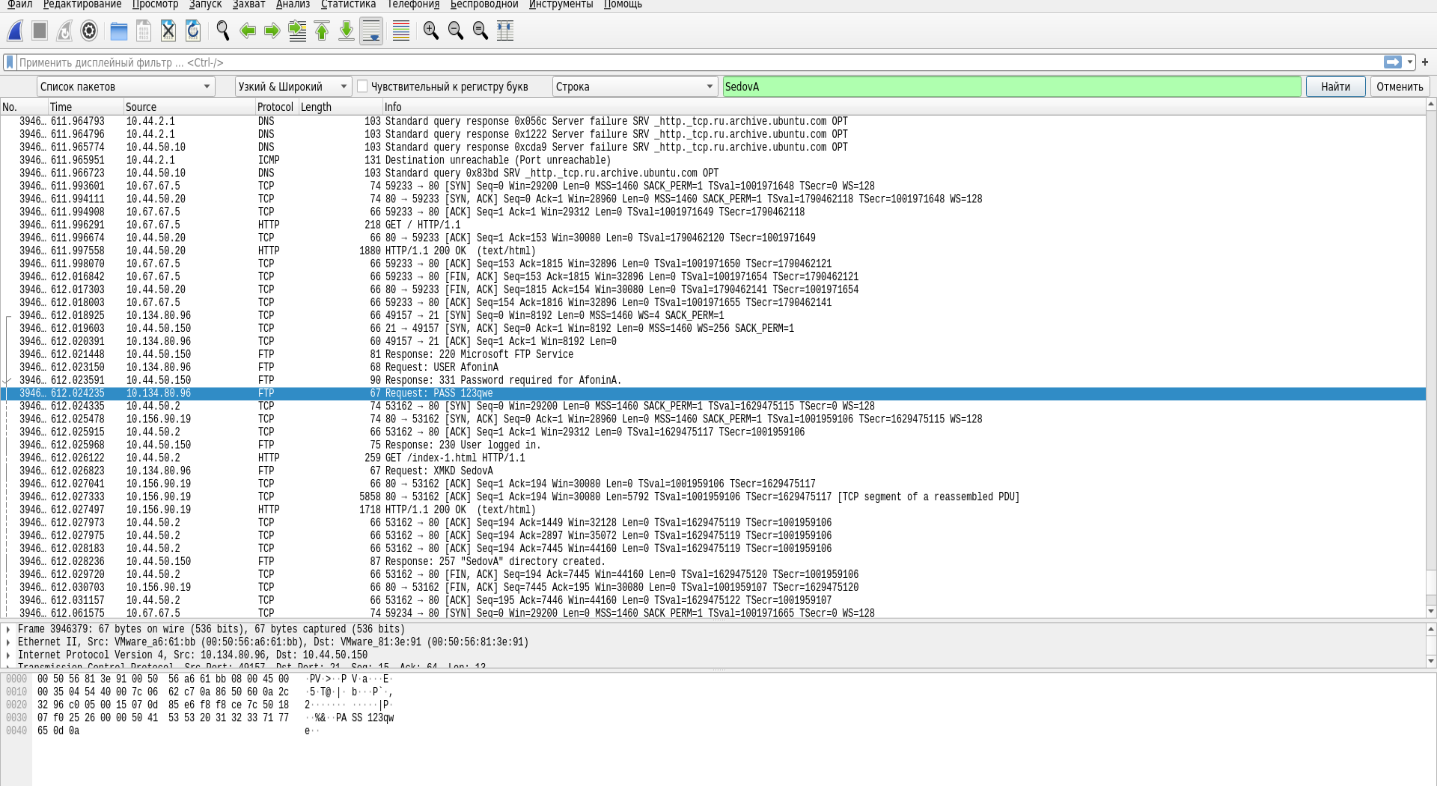
При этом, каждый из данных пользователей имеет свой индивидуальный пароль, благодаря которому он осуществляет вход на сервер.

**Выявление злоумышленника и последствия его действий**

1. В 07.06.07 некий злоумышленник (10.23.89.114) подключается к серверу и пытается подобрать пароли ко всем пользователям, однако ему удается подобрать пароль только для пользователя AfoninA. Поэтому злоумышленник входит на сервер под видом пользователя AfoninA, используя пароль для входа: **123qwe**

(То, что был использован именно этот пароль, узнаем, используя Wireshark):





1. Затем злоумышленник создает каталог SedovA и создает папку SedovA, в которой создает тестовые файлы. В этих файлах содержится украденная информация о именах пользователей и их паролях:
   1. Вход в систему в 07:14:14

Создание файлов и загрузка их в папку SedovA:

100.222.59.84.txt  
109.185.37.213.txt  
109.196.79.0.txt  
133.44.67.127.txt  
135.97.24.165.txt  
145.255.1.47.txt  
176.115.138.170.txt

Выход из системы в 07:14:14

* 1. Вход в систему в 07:18:14

Создание файлов и загрузка их в папку SedovA:

31.135.229.187.txt  
178.252.209.18.txt  
179.127.55.147.txt  
185.17.135.9.txt  
201.53.185.29.txt  
209.149.52.87.txt  
217.118.79.19.txt  
Выход из системы в 07:18:14

* 1. Вход в систему в 07:20:14

Создание файлов и загрузка их в папку SedovA:

5.76.123.181.94.txt  
5.79.225.117.txt  
46.164.131.86.txt  
83.220.236.206.txt  
86.174.200.99.txt  
95.153.186.134.txt

176.126.63.7.txt  
176.215.34.224.txt  
Выход из системы в 07:20:14

* 1. Вход в систему в 07:23:14

Создание файлов и загрузка их в папку SedovA:

5.76.181.94.txt

46.233.193.1.txt

176.222.169.247.txt

178.21.226.200.txt

Выход из системы в 07:23:14

* 1. Вход в систему в 07:27:14

Создание файлов и загрузка их в папку SedovA:

46.34.216.93.txt

46.61.35.103.txt

58.107.44.82.txt

77.40.18.51.txt

178.187.3.67.txt

Выход из системы в 07:27:14

* 1. Вход в систему в 07:30:14

Создание файлов и загрузка их в папку SedovA:

5.138.237.234.txt

46.241.60.61.txt

85.173.135.188.txt

90.143.35.215.txt

92.113.157.127.txt

178.141.133.106.txt

Выход из системы в 07:30:14

* 1. Вход в систему в 07:32:14

Злоумышленник выводит с сервера все созданные текстовые файлы. Затем копии этих файлов он скачивает из каталога SedovA на сервер 10.23.89.114

Выход из системы в 07:32:14

* 1. Вход в систему в 07:32:14

Злоумышленник выводит список файлов из каталога SedovA, при этом выходной размер берётся от первого созданного файла (100.222.59.84.txt).

**Заключение**

Злоумышленнику удалось получить доступ к личной информации пользователей, потому что атакованная сеть была уязвима к атаке с применением программ-анализаторов сетевого трафика. Данный вид атак относится к типу пассивных, поэтому трудно распознаваем.

Однако существует ряд методов, способный ослабить или устранить воздействие такой атаки:

* Криптография
* Аутентификация. Однократные пароли
* Коммутируемая инфраструктура
* ПО для обнаружения снифферов
* Модификация ARP протокола

**Примечания**

Основные команды FTP:

CWD — Сменить каталог

PASS — Пароль

STOR — Закачать файл. Перед STOR должна быть команда PASV или PORT

TYPE — Установить тип передачи файла (бинарный, текстовый).

PWD — Возвращает текущий каталог.

RETR — Скачать файл. Перед RETR должна быть команда PASV или PORT.

**USER** — Имя пользователя для входа на сервер

PASV — Войти в пассивный режим. Сервер вернёт адрес и порт, к которому нужно подключиться, чтобы забрать данные. Передача начнётся при введении следующих команд: RETR, LIST

QUIT — Отключиться

LIST — Возвращает список файлов каталога

SYST — Возвращает тип системы (UNIX, WIN)

MDTM — Возвращает время модификации(изменения) файла

FEAT — Показывает расширенные функции, поддерживаемые сервером

OPTS UTF8 ON — Проверяет, поддерживает ли сервер UTF-8. Аналог команды SYST