ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

*Московский институт электроники и математики им. А.Н.Тихонова*

**Домашнее задание по теме 33. Анализ данных вторжений**

По направлению 10.04.01 – «Информационная безопасность»

Проверил:

преп. Антон Носков

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Выполнил:

Новиков В. С. МКБ 241

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Москва 2025

Оглавление

[Решение 3](#_Toc198505371)

[Шаг 1: изучите оповещения в Sguil: 3](#_Toc198505372)

[Шаг 2: перейдите на Wireshark. 3](#_Toc198505373)

[Шаг 3: используйте ELSA для перехода к журналам Bro. 3](#_Toc198505374)

[Шаг 4: вернитесь в Squil для изучения атаки. 4](#_Toc198505375)

[Шаг 5: используйте ELSA для просмотра извлечённых данных. 5](#_Toc198505376)

[Результаты анализа 5](#_Toc198505377)

[Хронология событий 5](#_Toc198505378)

[Доказательства 5](#_Toc198505379)

[Вывод 6](#_Toc198505380)

[Рекомендации 6](#_Toc198505381)

# Решение

## Шаг 1: изучите оповещения в Sguil:

Что произошло во время атаки?

**Ответ:**

Злоумышленник получил root-доступ, собрал хеши паролей и создал скрытую root-учётку для постоянного доступа. Это Privilege Escalation → Credential Dumping → Persistence. Критический инцидент.

## Шаг 2: перейдите на Wireshark.

Что вы увидели? Что обозначает красный и синий цвет текста?

**Ответ:**

Полноценный интерактивный сеанс атакующего.

Красный Client → Server. Вводимые злоумышленником команды (SRC)

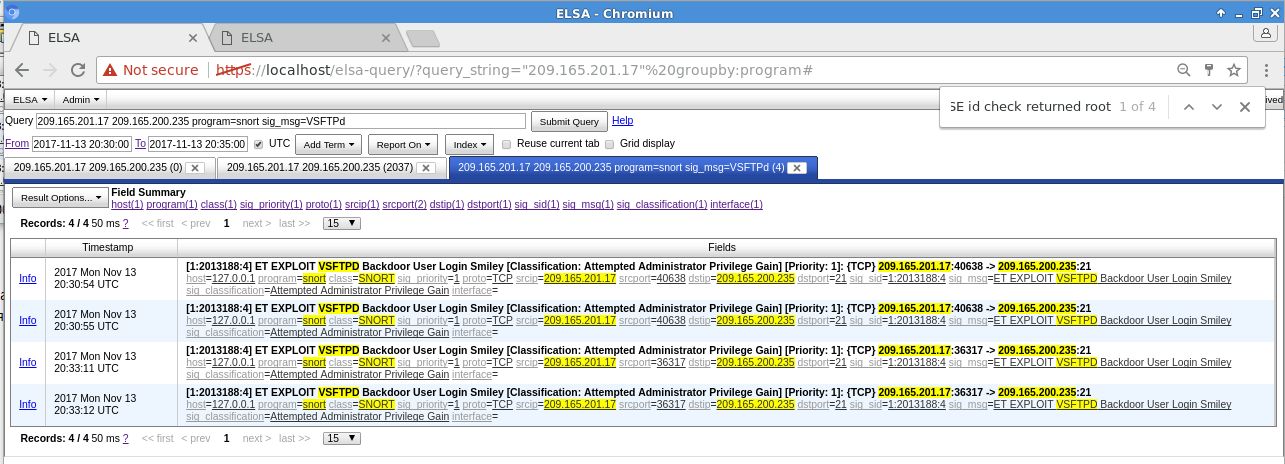
Синий Server → Client. Ответы системы на эти команды (DST)

## Шаг 3: используйте ELSA для перехода к журналам Bro.

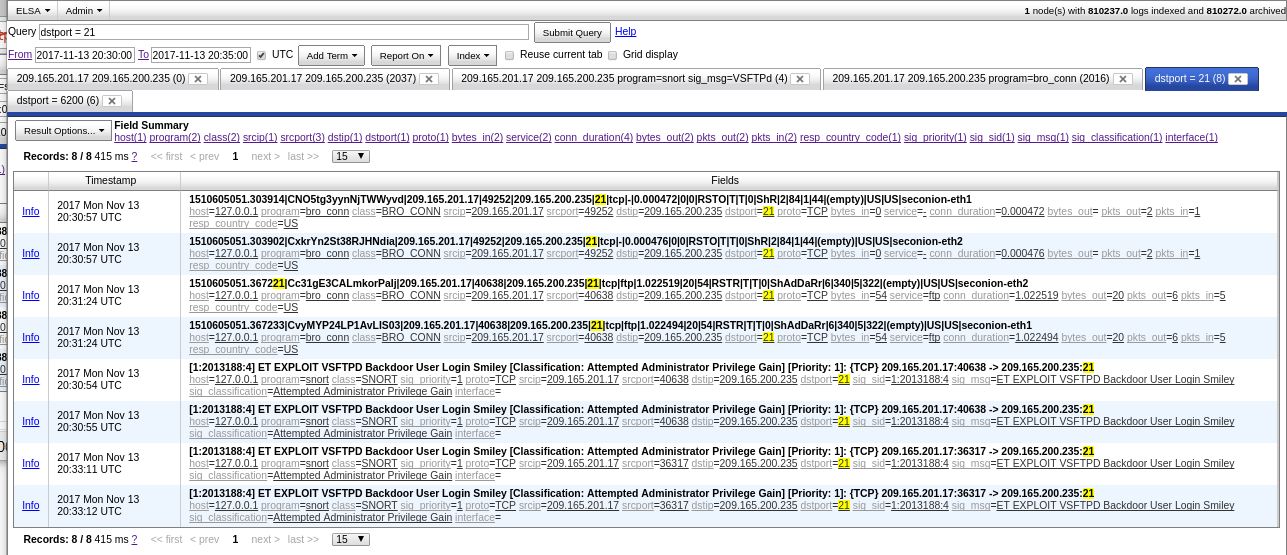
f. Сделайте скриншот для отчета.

backdoor-уязвимости vsftpd 2.3.4 (CVE-2011-2523):

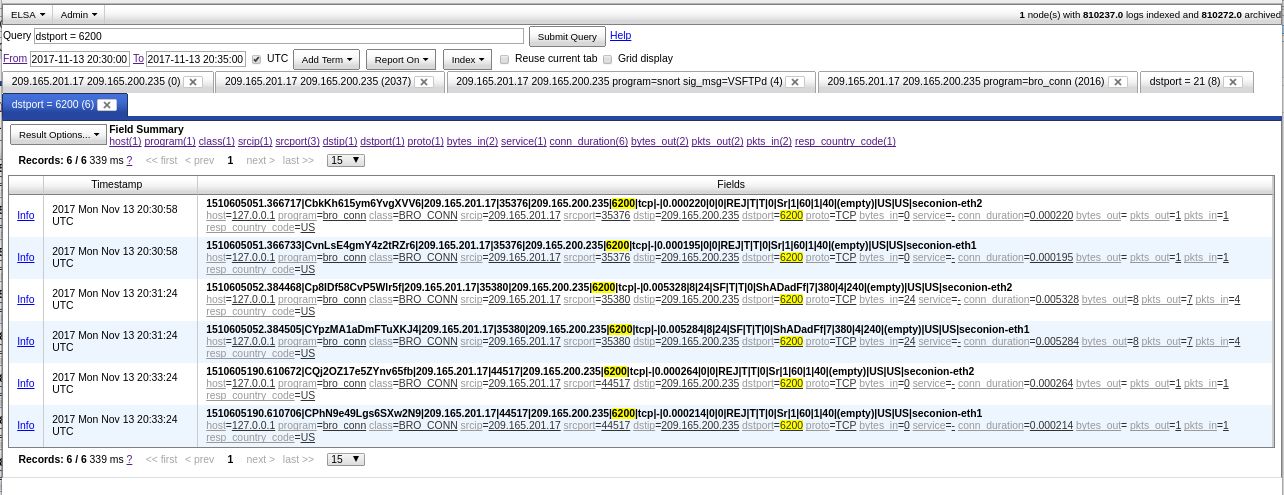




Короткое TCP-рукопожатие к 21/tcp:

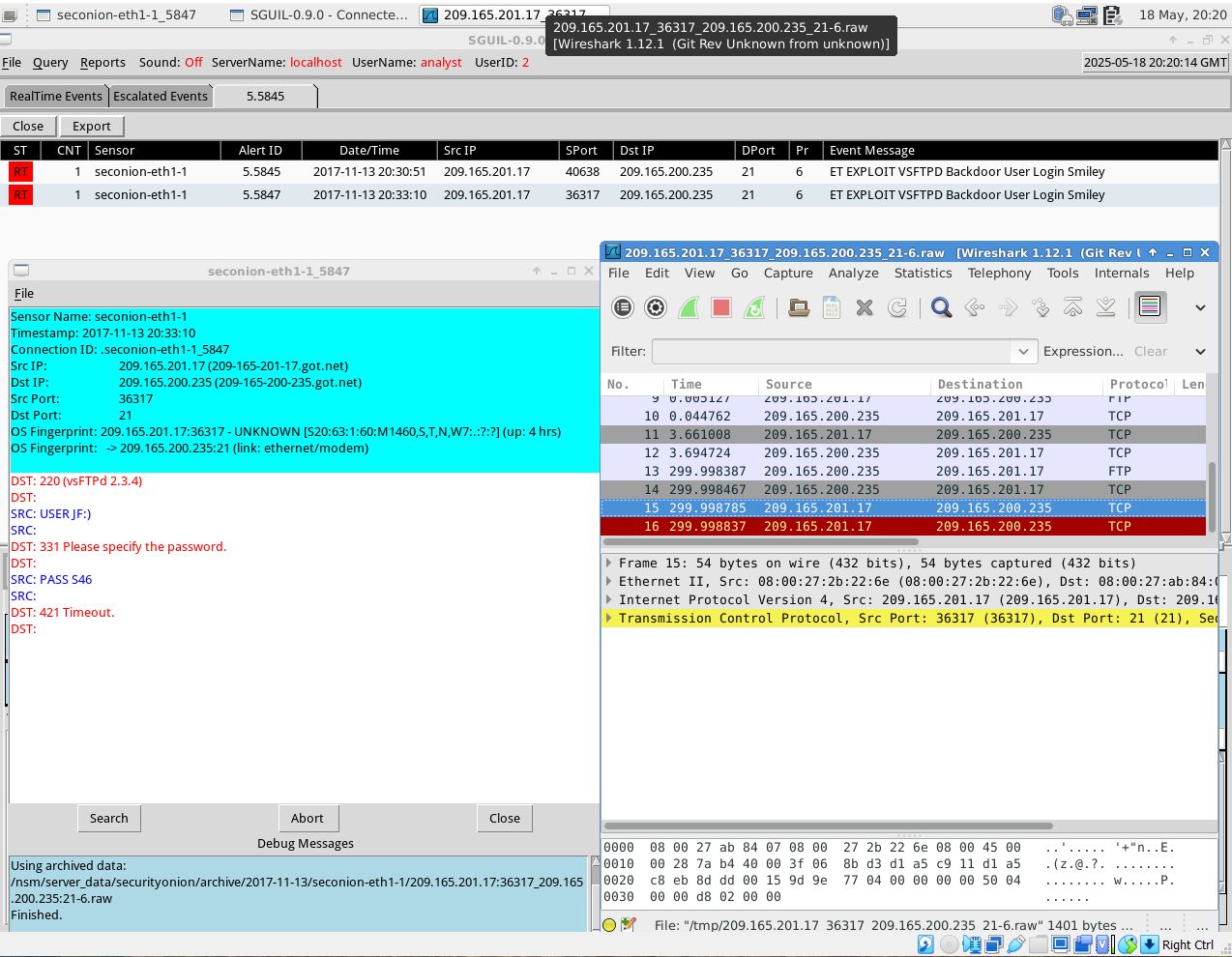


Входящий connect на 6200/tcp, ответная shell-сессия (root):



## Шаг 4: вернитесь в Squil для изучения атаки.

e. Сделайте скриншот для отчета.



## Шаг 5: используйте ELSA для просмотра извлечённых данных.

Какой файл был передан по протоколу FTP на адрес 209.165.200.235? Чья учётная запись была использована для передачи файла?

**Ответ:**

Был передан файл по протоколу FTP: **confidential.txt**

Для передачи файла использовалась УЗ: **analyst (пароль скрыт)**

# Результаты анализа

Жертва 209.165.200.235

Атакующий 209.165.201.17

Дата / время (UTC) 2017-11-13 20:30 – 20:35

Эксплойт Backdoor vsftpd 2.3.4 &nbsp;→&nbsp; USER → root-shell 6200/tcp

Переданный файл /confidential.txt

Учётная запись FTP analyst

Права, полученные злоумышленником uid=0(root)

Техники MITRE ATT&CK:

* T1059 CLI · T1049 Net Discovery
* T1003 OS Credential Dumping
* T1098 Account Manipulation
* T1105 Ingress Tool Transfer

## Хронология событий

20:31:17 Scan::Port\_Scan 209.165.201.17 сканирует ≥18 портов цели `bro\_notice`

20:30:54 FTP-коннект 21/tcp, команда USER `bro\_conn`, `bro\_ftp`

20:30:54 Snort - ET EXPLOIT VSFTPd Backdoor User Login Smiley `snort sig\_msg`

20:30:58 обратный root-shell 6200/tcp (жертва - атакующий) `bro\_conn` dport 6200

20:31-20:33 команды *whoami*, *hostname*, *ifconfig* - подтверждён root-доступ Wireshark / transcript

20:31-20:33 *cat /etc/shadow* - дамп хешей Wireshark

20:31-20:33 добавлена учётка *myroot* (UID 0) в */etc/passwd & /etc/shadow* Wireshark

20:46:21 FTP *STOR /confidential.txt* на 209.165.200.235; user *analyst* `bro\_ftp`, arg=`/confidential.txt`

20:46:22 Snort — GPL ATTACK\_RESPONSE id check returned root (6200/tcp) подтверждение root

20:46:34 сессия закрыта, атакующий выходит `bro\_conn` завершается

## Доказательства

FTP 21/tcp → *USER :)* → vsftpd 2.3.4 backdoor (CVE-2011-2523) → ответный root-shell 6200/tcp.

IDS-сигнатуры:

* ET EXPLOIT VSFTPd Backdoor User Login Smiley
* GPL ATTACK\_RESPONSE id check returned root

Утечка файла *confidential.txt* под пользователем *analyst*.

Создание скрытого пользователя *myroot*, UID 0 — устойчивый доступ.

Дамп */etc/shadow*, последующее сканирование сети (*ifconfig*).

## Вывод

1. причина взлома - публичный сервис vsftpd 2.3.4 с заложенным бэкдором;
2. последствия - полный root-доступ, компрометация учётных данных, загрузка/выгрузка файлов, создание постоянного root-аккаунта;
3. критично - неограниченный контроль над сервером + утечка конфиденциальных данных.

## Рекомендации

1. немедленно вывести хост 209.165.200.235 из сети; сохранить образ диска для форензики.
2. удалить vsftpd 2.3.4 или обновить ≥ 2.3.5 и закрыть порт 21 вовне, разрешить только по VPN;
3. сбросить все пароли; удалить учётку *myroot,* провести аудит UID 0 в */etc/passwd*;
4. включить File-Integrity Monitoring */etc/passwd, /etc/shadow, /usr/sbin/vsftpd*;
5. логировать и блокировать любые внешние подключения к динамическим портам от сервера.