**Домашнее задание**

|  |  |
| --- | --- |
| Дисциплина | «Защита компьютерных сетей и систем» |
| Тема | Тема 33. «Анализ данных вторжений» |
| Форма проверки | **Проверка преподавателем** |
| Имя преподавателя | Антон Носков |
| Время выполнения | 180 минут |
| Цель задания | Научиться просматривать журналы во время использования задокументированной уязвимости с помощью инструментов Security Onion:   * + просматривать события в Sguil и работать с предупреждениями, оповещениями;   + работать с предупреждениями в Wireshark;   + работать с журналами в Bro;   + использовать ELSA для просмотра извлечённых данных. |
| Инструменты для выполнения ДЗ | Компьютер с оперативной памятью не менее 3 ГБ и 10 ГБ свободного дискового пространства, последняя версия Oracle VirtualBox, одна виртуальная машина с Alternate Security Onion, интернет-подключение. |
| Правила приёма работы | 1. Выполненная работа на виртуальной машине.  2. Ссылка в ЛМС на файл с отчётом. |
| Критерии оценки | **Задание оценивается в 10 баллов:**  - выполнение задания 1 — 2 балла;  - выполнение задания 2 — 2 балла;  - выполнение задания 3 — 1 балл;  - выполнение задания 4 — 1 балл;  - выполнение задания 5 — 2 балла;  - выполнение задания 6 — 2 балла (дополнительные баллы за глубину анализа, оригинальность выводов и представления результатов)  **Задание считается выполненным, если:**  - представлена ссылка на файл с отчётом в свободной форме,  - выполнены все части задания.  **Задание не выполнено, если:**  - файл с отчётом не представлен,  - работа содержит существенные ошибки. |
| Дедлайн | *три недели после вебинара (точную дату см. в ЛМС).* |

**Прежде чем выполнять задание**

Необходимо:

* установить виртуальную машину по инструкции,
* выполнить дополнительные настройки SecurityOnion.

*Инструкция по дополнительной настройке SecurityOnion*

1. Отмените синхронизацию времени с одной из виртуальных машин:

* введите в командной строке от имени администратора основной операционной системы:

**cmd**

**cd c:\Program Files\Oracle\VirtualBox**

* выполните команду:

**VBoxManage.exe setextradata "Security Onion\_3G" "VBoxInternal/Devices/VMMDev/0/Config/GetHostTimeDisabled" 1**

1. Запустите виртуальную машину.
2. В виртуальной машине запустите терминал.
3. В терминале напишите:

**sudo timedatectl set-ntp 0**

и

**sudo timedatectl -- set-time 2020-11-11**

1. Введите **date**.

Если дата *Wed Nov 11 00:00:04 UTC 2020,* то переходите к выполнению практического задания.

**Практическое задание**

**Часть 1. Подготовка виртуальной среды**

1. Загрузите [виртуальную машину Alternate Security Onion](https://disk.yandex.ru/d/nNPmNdK7LSXVSw).
2. Запустите Oracle VirtualBox. Импортируйте виртуальную машину Alternate Security Onion.
3. Запустите ВМ Alternate Security Onion и войдите в систему. Войдите в систему под именем пользователя **analyst** с паролем **cyberops**.
4. На виртуальной машине Alternate Security Onion щёлкните правой кнопкой мыши **Desktop > Open Terminal Here (Рабочий стол > Открыть терминал здесь)**. Введите команду **sudo service nsm status**, чтобы убедиться, что все серверы и датчики готовы к работе. Этот процесс может занять некоторое время. Если какие-то службы отправляют сообщение **FAIL**, повторяйте команду до тех пор, пока все статусы не примут значение **OK**, после чего перейдите к следующей части.

analyst@SecOnion:~/Desktop$ **sudo service nsm status**

Status: securityonion

\* sguil server [ OK ]

Status: HIDS

\* ossec\_agent (sguil) [ OK ]

Status: Bro

Name Type Host Status Pid Started

manager manager localhost running 5577 26 Jun 10:04:27

proxy proxy localhost running 5772 26 Jun 10:04:29

seconion-eth0-1 worker localhost running 6245 26 Jun 10:04:33

seconion-eth1-1 worker localhost running 6247 26 Jun 10:04:33

seconion-eth2-1 worker localhost running 6246 26 Jun 10:04:33

Status: seconion-eth0

\* netsniff-ng (full packet data) [ OK ]

\* pcap\_agent (sguil) [ OK ]

\* snort\_agent-1 (sguil) [ OK ]

\* snort-1 (alert data) [ OK ]

\* barnyard2-1 (spooler, unified2 format) [ OK ]

<output omitted>

**Часть 2. Просмотр журналов**

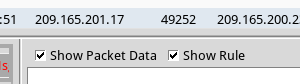
После атаки у пользователей больше нет доступа к файлу с именем **confidential.txt**. Теперь вы сможете посмотреть журналы, чтобы определить, каким образом был скомпрометирован файл.

**Примечание**: если бы это была производственная сеть, нужно было бы рекомендовать пользователям **analyst** и **root** изменить свои пароли, чтобы выполнить требования текущей политики безопасности.

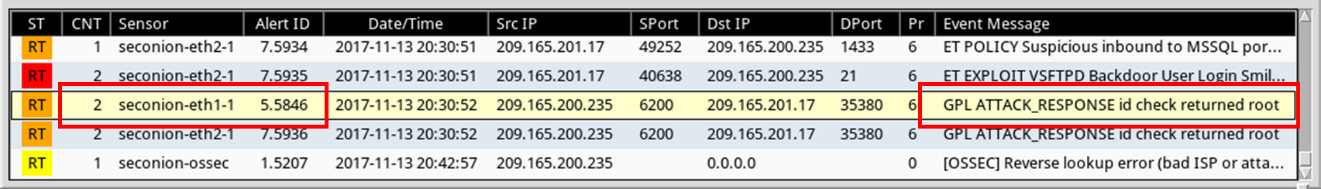
**Шаг 1: изучите оповещения в Sguil:**

a. откройте **Sguil** и выполните вход. Щёлкните **Select All (Выбрать все)** и **запустите Sguil**;

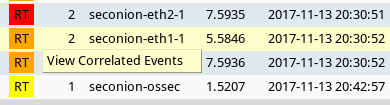
b. просмотрите события в списке столбца сообщений о событии. Там есть два сообщения **GPL ATTACK\_RESPONSE id check returned root**. Эти сообщения указывают, что во время атаки мог быть предоставлен доступ с правами root. Узел 209.165.200.235 по запросу предоставил доступ с правами root узлу 209.165.201.17. Установите флажок **Show Packet Data (Показать пакетные данные)** и **Show Rule (Показать правило)** для подробного просмотра каждого оповещения;



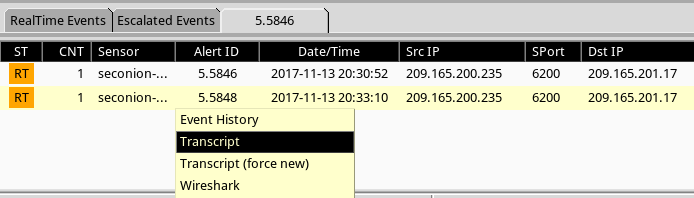
c. выберите возвращённое сообщение root, которое связано с датчиком **seconion-eth1-1**, чтобы проанализировать его подробнее. На рисунке ниже показано оповещение **Alert ID 5.5846** и связанные с ним события;



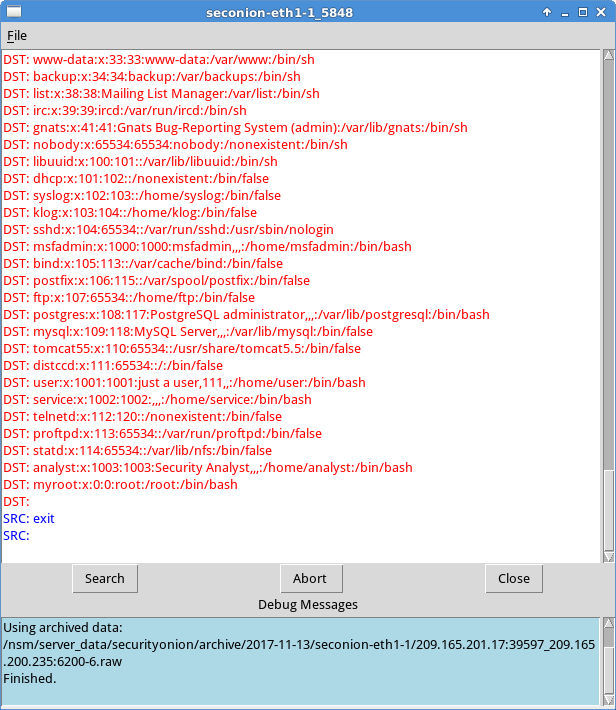
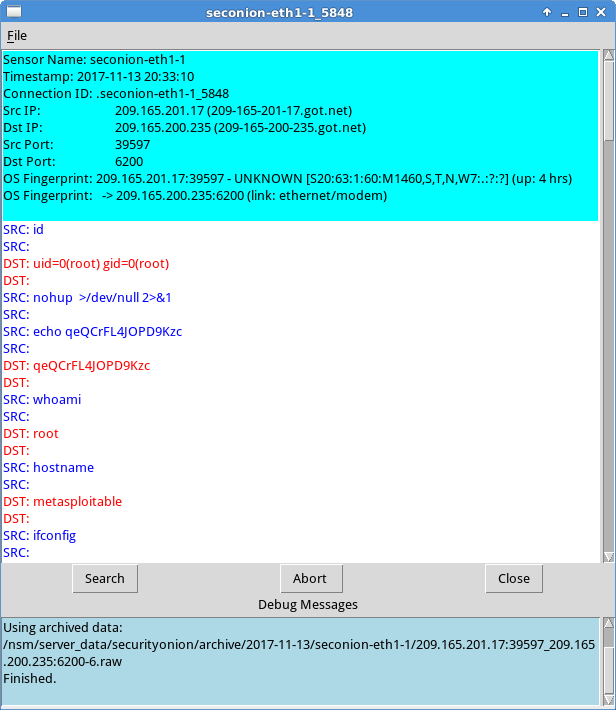
d. щёлкните правой кнопкой мыши по цифре под заголовком CNT и выберите **View Correlated Events (Просмотр связанных событий)**;



e. на новой вкладке щёлкните правой кнопкой мыши **Alert ID (Идентификатор оповещения)** для одного из оповещений **GPL ATTACK\_RESPONSE id check returned root** и выберите **Transcript (Запись)**. В этом примере используется оповещение с идентификатором 5.5848;



f. просмотрите записи для всех таких оповещений. Последующие оповещения на вкладке, вероятнее всего, покажут транзакции между хакером и его целью во время атаки.



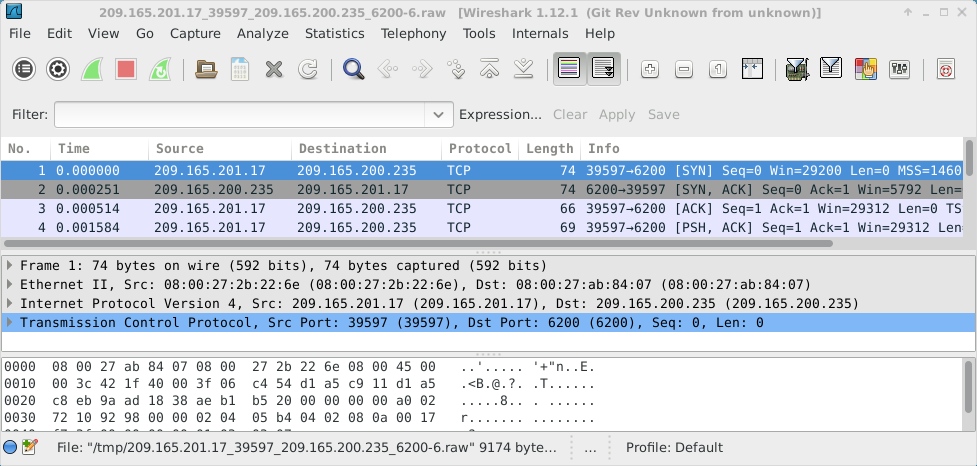
Что произошло во время атаки?

Ответ:

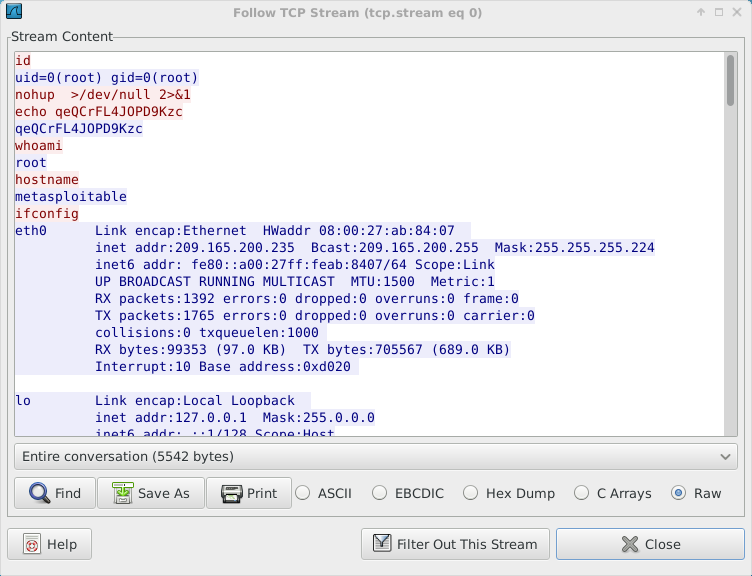
Злоумышленник получил root-доступ, собрал хеши паролей и создал скрытую root-учётку для постоянного доступа. Это Privilege Escalation → Credential Dumping → Persistence. Критический инцидент.

**Шаг 2: перейдите на Wireshark.**

a. выберите оповещение, запись событий которого вы изучали на предыдущем шаге. Щёлкните правой кнопкой мыши по идентификатору оповещения и выберите **Wireshark**;



b. для того чтобы просмотреть все пакеты, объединённые в сеансе TCP, щёлкните правой кнопкой мыши по любому пакету и выберите **Follow TCP stream (Отслеживать поток TCP)**;



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

Ответ:

Полноценный интерактивный сеанс атакующего.

Красный Client → Server. Вводимые злоумышленником команды (SRC)

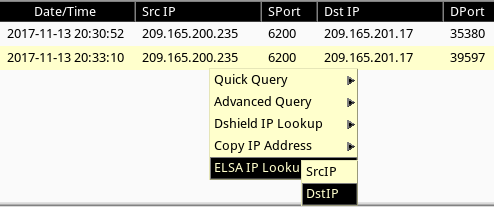
Синий Server → Client. Ответы системы на эти команды (DST)

c. выйдите из окна потока TCP. После просмотра информации **Wireshark** закройте это приложение.

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

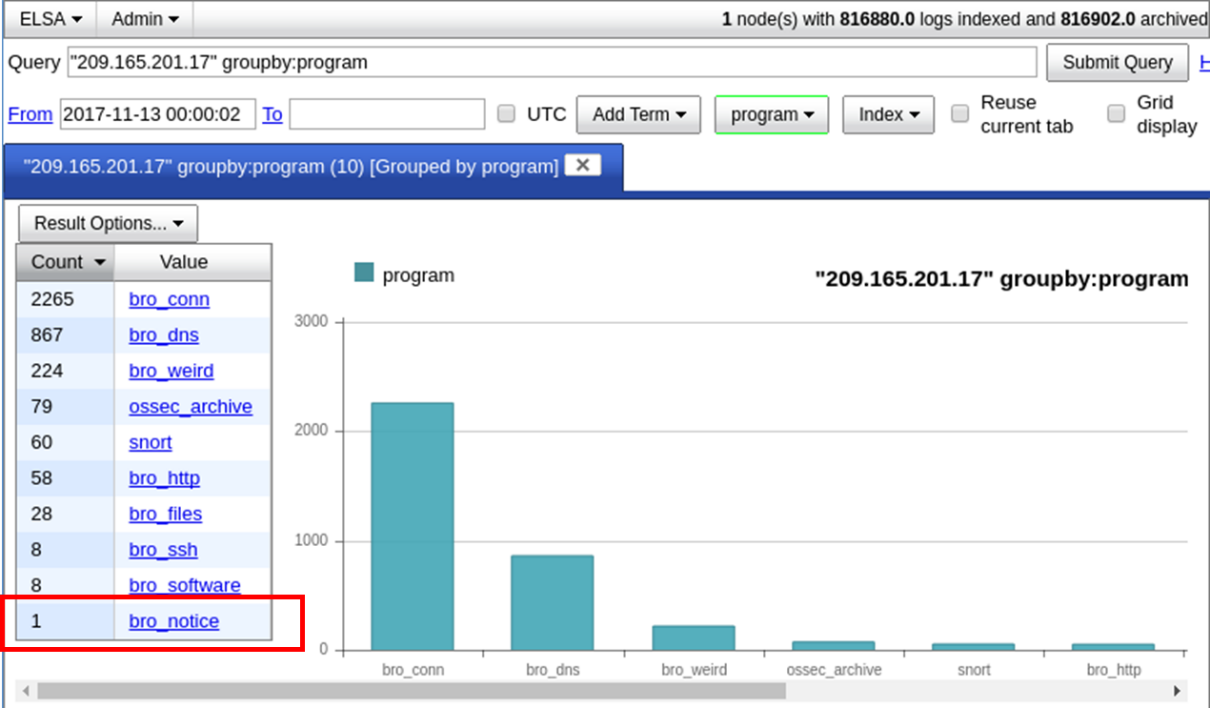
a. вернитесь к Sguil. Щёлкните правой кнопкой мыши по IP-адресу источника или назначения для одинакового оповещения **GPL ATTACK\_RESPONSE id check returned root** и выберите **ELSA IP Lookup** > **DstIP**. По запросу ELSA введите имя пользователя **analyst** и пароль **cyberops**;

**Примечание**: если вы получили сообщение «Your connection is not private» («Ваше подключение не является частным»), то щёлкните **ADVANCED (Дополнительно) > Proceed to localhost (unsafe) (Перейти на локальный хост-компьютер (небезопасно))** для продолжения.



b. измените дату в поле From (От) на предшествующую дате, которая отображается в Sguil. Нажмите **Submit Query (Отправить запрос)**;

c. нажмите **bro\_notice**;



d. результат показывает, что узел 209.165.201.17 сканировал порты на узле 209.165.200.235. Злоумышленник, вероятно, нашёл уязвимости узла 209.165.200.235, позволившие ему получить туда доступ;

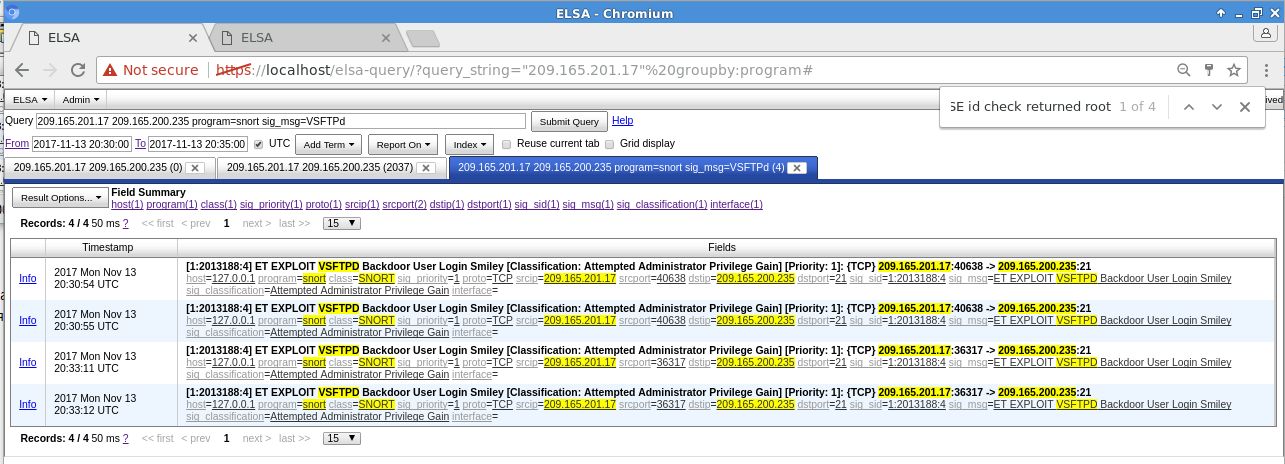


e. если злоумышленник скомпрометировал узел 209.165.200.235, теперь вам нужно определить эксплойт, который был использован и при помощи которого он получил доступ.

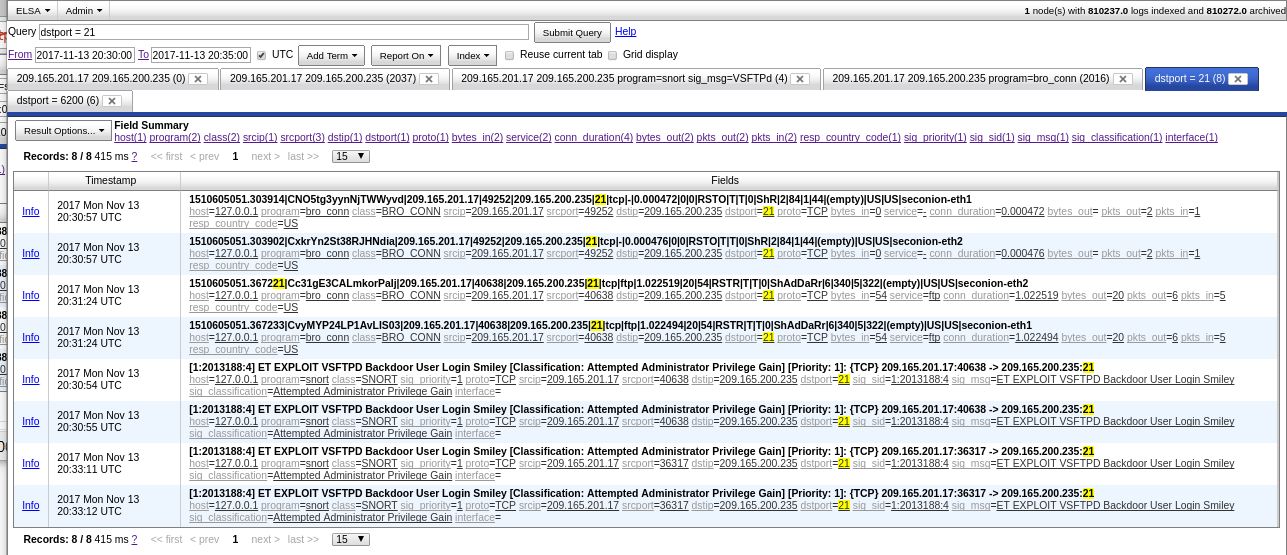
f. Сделайте скриншот для отчета.

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

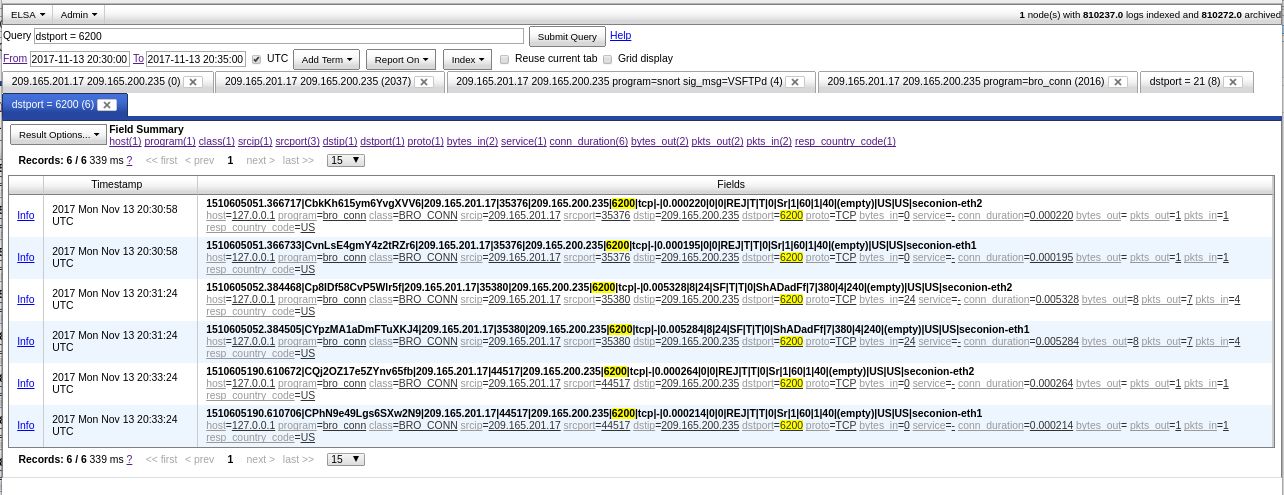




**Короткое TCP-рукопожатие к 21/tcp:**

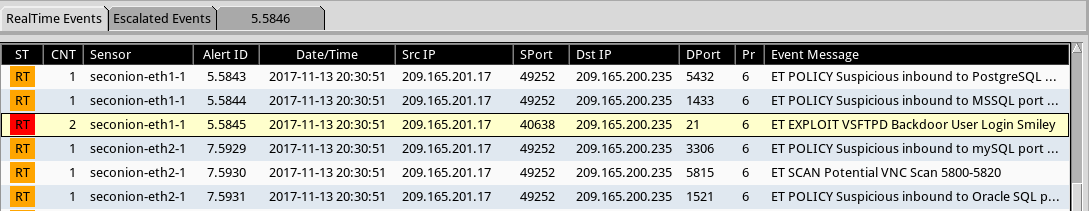


**Входящий connect на 6200/tcp, ответная shell-сессия (root):**



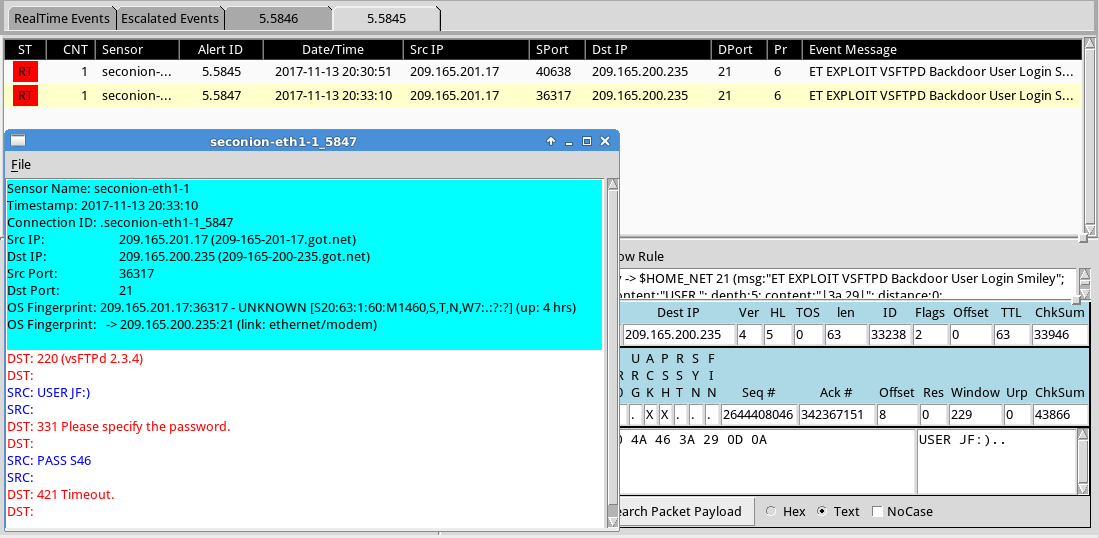
**Шаг 4: вернитесь в Squil для изучения атаки.**

a. перейдите в Sguil и щёлкните вкладку **RealTime Events (События в реальном времени)**. Найдите события **ET EXLOIT VSFTPD Backdoor User Login Smiley**. Эти события являются возможными эксплойтами и произошли во время несанкционированного доступа с правами root;



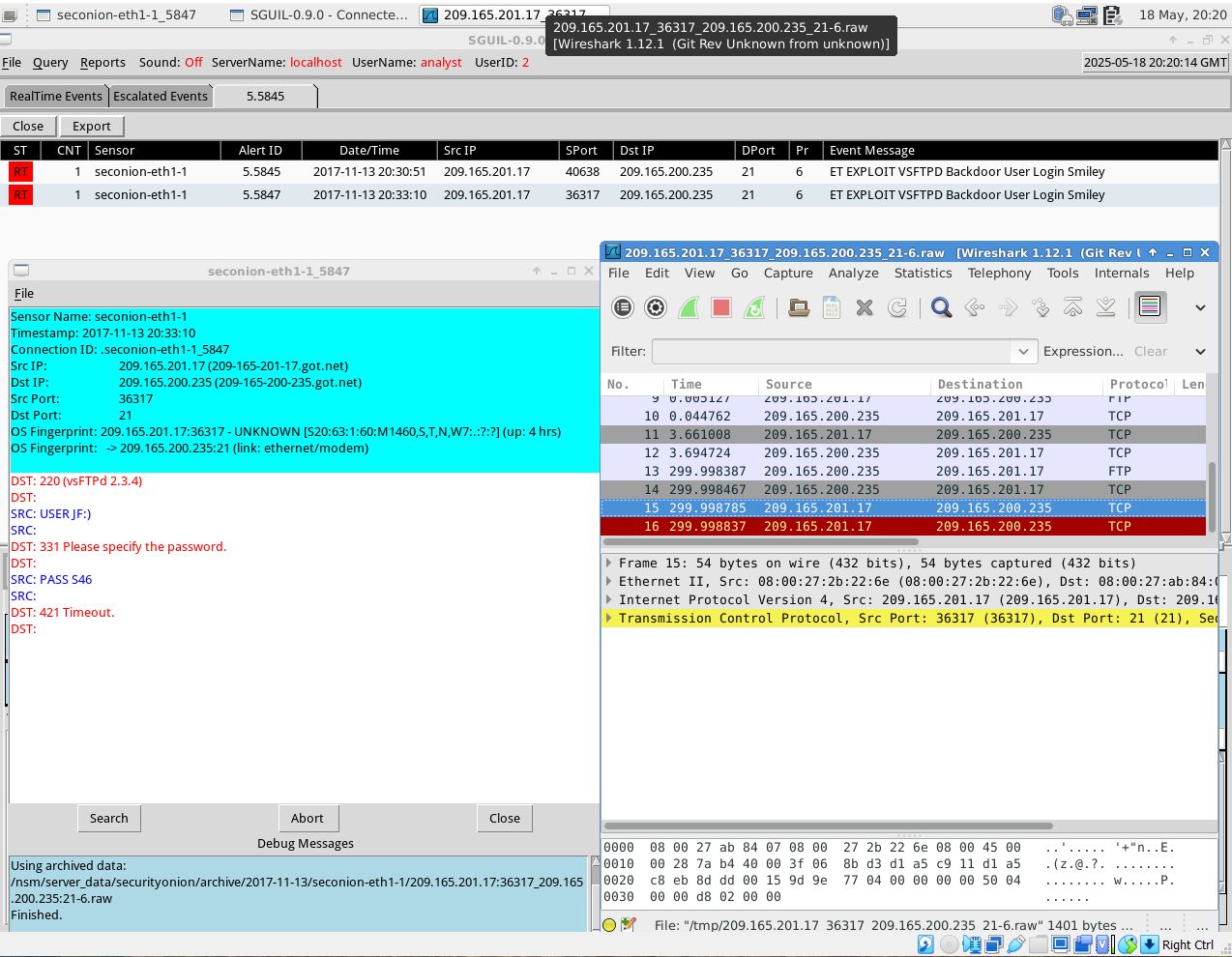
b. щёлкните правой кнопкой мыши по номеру под заголовком CNT и выберите **View Correlated Events (Просмотр связанных событий)**, чтобы просмотреть все связанные события. Выберите оповещение с идентификатором, который начинается с 5. Это оповещение собрало информацию с датчика на интерфейсе seconion-eth1-1;

c. в новой вкладке со всеми связанными событиями щёлкните правой кнопкой мыши идентификатор оповещения и выберите **Transcript (Запись)** для подробного просмотра каждого оповещения. Самые последние, вероятнее всего, будут содержать операции передачи данных по TCP между злоумышленником и жертвой;



d. также можно щёлкнуть правой кнопкой мыши по идентификатору оповещения и выбрать **Wireshark** для просмотра и сохранения файла pcap и потока TCP.

e. Сделайте скриншот для отчета.

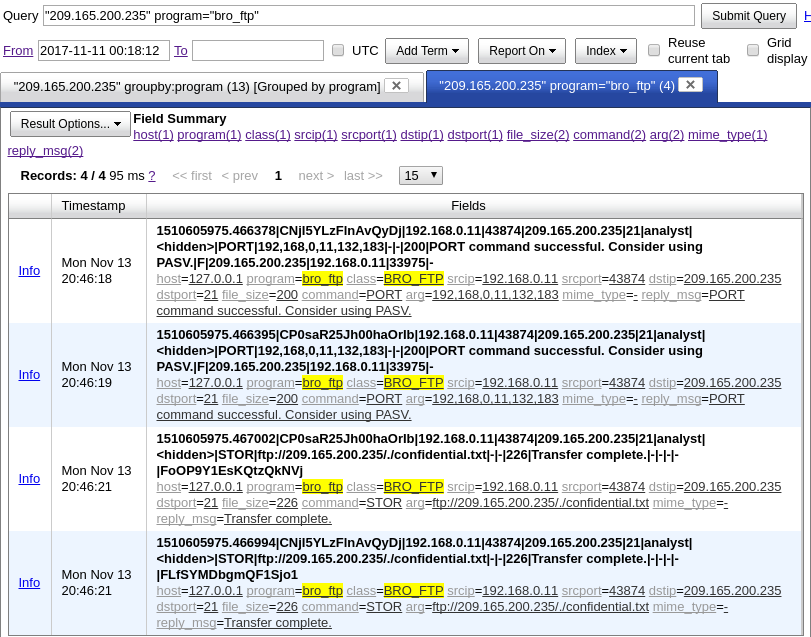


**Шаг 5: используйте ELSA для просмотра извлечённых данных.**

a. для того чтобы использовать ELSA для получения дополнительных сведений о том же оповещении, что и выше, щёлкните правой кнопкой мыши IP-адрес источника или назначения и выберите **ELSA IP Lookup (Поиск IP-адреса ELSA)** > **DstIP**;

b. измените дату в поле From (От) на такую, которая будет предшествовать событию, соответствующему метке времени Sguil;

c. нажмите кнопку **bro\_ftp** для просмотра журналов ELSA, которые относятся к FTP;



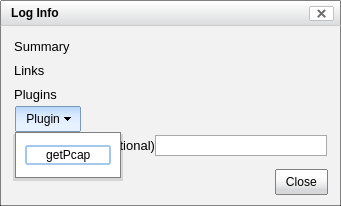
Какой файл был передан по протоколу FTP на адрес 209.165.200.235? Чья учётная запись была использована для передачи файла?

Ответ:

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

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

d. нажмите кнопку **info (Информация)** для просмотра транзакций в последней записи. Поле reply\_msg указывает, что это последняя запись о передаче файла confidential.txt. Выберите **Plugin (Подключаемый модуль)** > **getPcap**. По запросу введите имя пользователя **analyst** и пароль **cyberops**. При необходимости нажмите кнопку **Submit (Отправить)**;



Запись pcap отображается с помощью средства tcpflow, и эта страница также содержит ссылку для доступа к соответствующему файлу pcap.

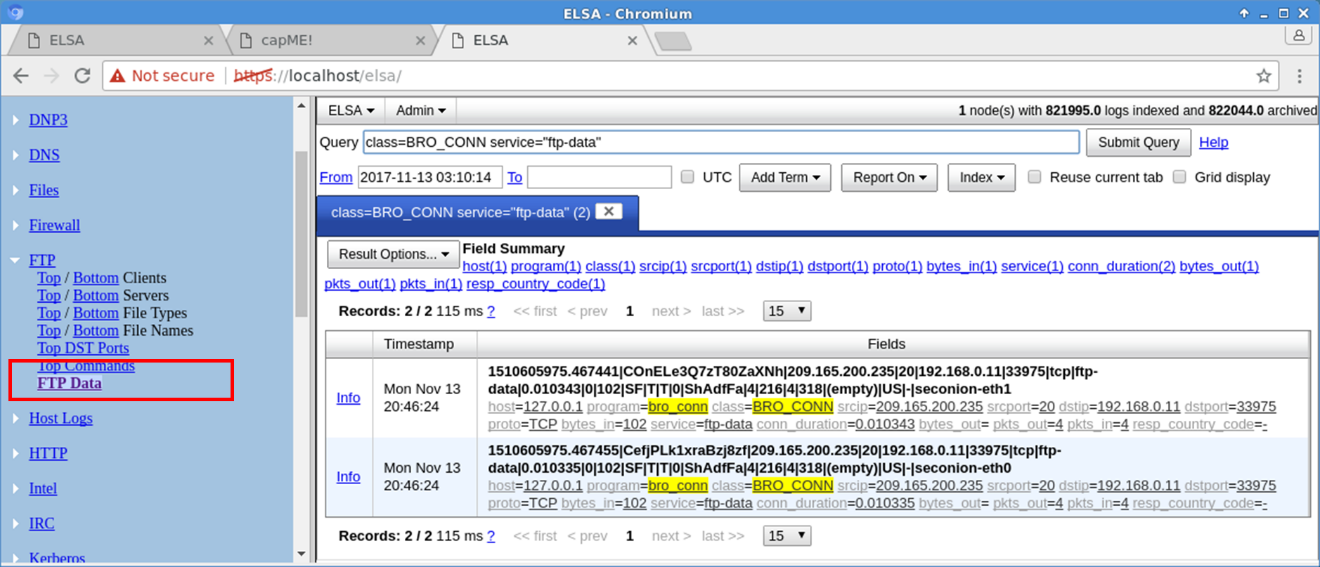


e. для того чтобы определить содержимое файла, который был скомпрометирован, откройте **ELSA**, дважды щёлкнув по значку на рабочем столе, чтобы открыть новую вкладку и выполнить новый поиск;

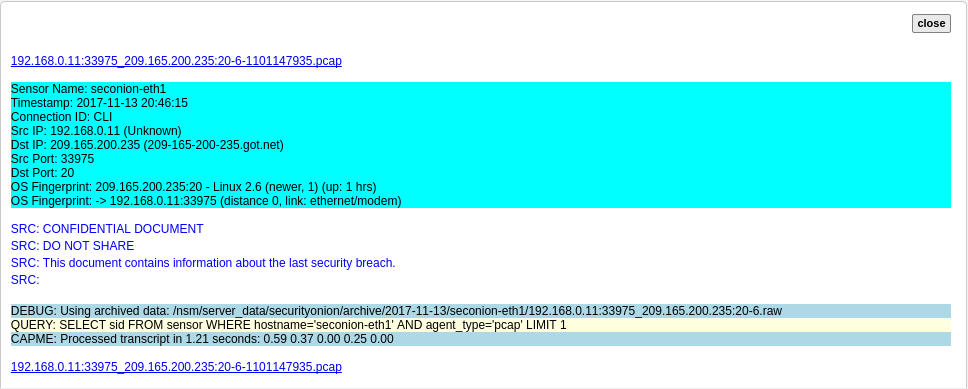
f. разверните раздел **FTP** и нажмите кнопку **FTP Data (Данные FTP)**;

g. измените дату в поле данных From (От), чтобы включить нужный период, и нажмите кнопку **Submit Query (Отправить запрос)**;

h. щёлкните одну из ссылок **Info (Информация)** и выберите в раскрывающемся меню пункт getPcap, чтобы просмотреть содержимое украденного файла;



i. результат отображает содержимое файла с именем **confidential.txt**, который был передан на указанный сервер FTP.



**Шаг 6: удалите конфигурацию.**

Закончив анализ, выключите виртуальную машину.

Итак, вы просмотрели журналы в роли аналитика по кибербезопасности. Теперь изложите свои результаты анализа.

# **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.

**Подготовка отчёта**

По результатам выполнения второй части работы необходимо подготовить отчёт. Он оформляется в свободной форме.

Отчёт по выполненной работе должен включать:

* ответ на вопрос из шага 1,
* ответ на вопрос из шага 2,
* скриншот выполненного пункта в шаге 3,
* скриншот выполненного пункта в шаге 4,
* ответ на вопрос из шага 5,
* ответ на вопрос из шага 6.