УСТАНОВКА BRO В UBUNTU 16.04

Август 13, 2017 12:37 пп 1 285 views | Комментариев нет
Ubuntu | Amber | 0 Comments

Bro – это открытая система анализа данных и приложение для мониторинга безопасности, которое объединяет лучшие функции OSSEC и osquery в один пакет.

Bro может выполнять анализ поведения и поддерживает сигнатурный метод обнаружения. Bro предлагает следующие функции:

- Обнаружение brute-force атак на сетевые сервисы, например, SSH и FTP.
- Мониторинг и анализ трафика HTTP.
- Обнаружение изменений в установленном программном обеспечении.
- Проверка сертификатов SSL/TLS.
- Обнаружение SQL-инъекций.
- Мониторинг целостности файлов.
- Отправка отчетов и уведомлений по электронной почте.
- Геолокация IP-адресов.
- Поддержка автономного и распределенного режимов.

Bro можно установить из исходного кода и с помощью менеджера пакетов. Компиляция приложения из исходного кода требует больше времени, но это единственный метод, поддерживающий геолокацию IP.

После установки Bro в системе появятся команды bro и broctl. Bro может анализировать файлы трассировки и трафик в реальном времени; broctl — это интерактивная утилита командной строки для управления автономными и распределенными установками Bro.

Данный мануал поможет установить Bro в Ubuntu 16.04 из исходного кода в автономном режиме.

Требования

- Сервер Ubuntu 16.04, пользователь sudo (все инструкции – здесь).
- 1 Гб RAM минимум.
- Postfix только в режиме передачи. Обратитесь к руководству Установка и настройка SMTP-сервера исходящей почты Postfix в Ubuntu 16.04.

1: Установка зависимостей

Обновите индекс пакетов, чтоб избежать ошибок с менеджером пакетов.

```
sudo apt-get update
```

Bro зависит от ряда библиотек и инструментов как Libpcap, OpenSSL и BIND8. BroControl также требует Python 2.6 и выше. При сборке Bro из исходного кода нужны CMake, SWIG, Bison и компилятор C/C++.

Чтобы установить все зависимости, можно ввести:

```
sudo apt-get install bison cmake flex g++ gdb make libmagic-dev
libpcap-dev libgeoip-dev libssl-dev python-dev swig2.0 zlib1g-dev
```

2: Загрузка базы данных GeoIP

Теперь нужно загрузить БД GeoIP, с помощью которой Bro сможет определять геолокацию IP-адресов. Загрузите сжатые файлы для IPv4 и IPv6, распакуйте их и переместите в каталог /usr/share/GeoIP.

> **Примечание**: Загрузить бесплатную базу данных GeoIP можно с MaxMind. Сейчас появился новый формат базы данных IP, но Bro пока не поддерживает его.

Загрузите базы для IPv4 и IPv6.

```
wget
http://geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz
wget http://geolite.maxmind.com/download/geoip/database/GeoLiteCityv6-
beta/GeoLiteCityv6.dat.gz
```

Распакуйте файлы, после чего в рабочем каталоге появятся файлы GeoLiteCity.dat и GeoLiteCityv6.dat.

```
gzip -d GeoLiteCity.dat.gz
gzip -d GeoLiteCityv6.dat.gz
```

Переместите файлы в каталог /usr/share/GeoIP и переименуйте их.

```
sudo mv GeoLiteCity.dat /usr/share/GeoIP/GeoIPCity.dat
sudo mv GeoLiteCityv6.dat /usr/share/GeoIP/GeoIPCityv6.dat
```

3: Установка Bro из исходного кода

Для начала нужно клонировать репозиторий с GitHub.

Git устанавливается в Ubuntu по умолчанию. Для клонирования репозитория используйте следующую команду:

```
git clone --recursive git://git.bro.org/bro
```

Файлы будут помещены в каталог bro.

```
cd bro
```

Запустите конфигурацию Bro, что займет меньше минуты.

```
./configure
```

Затем используйте команду make, чтобы собрать программу. Этот процесс может занять около 20 минут.

```
make
```

В выводе вы увидите, сколько процентов сборки уже обработано.

После сборки можно установить Bro. Установка займет не больше минуты.

```
sudo make install
```

Команда установит Bro в каталог /usr/local/bro.

Добавьте /usr/local/bro/bin в переменную $PATH. Для этого нужно добавить путь в файл в каталоге /etc/profile.d. Назовем этот файл 3rd-party.sh.

Создайте и откройте этот файл:

```
sudo nano /etc/profile.d/3rd-party.sh
```

Затем скопируйте и вставьте в файл следующие строки.

```
# Expand PATH to include the path to Bro's binaries
export PATH=$PATH:/usr/local/bro/bin
```

Сохраните и закройте файл. Чтобы обновить параметры, введите:

```
source /etc/profile.d/3rd-party.sh
```

Также можно выйти из системы и войти снова, чтобы все пути правильно загрузились.

4: Настройка Bro

Теперь нужно отредактировать пару файлов Bro, которые находятся в /usr/local/bro/etc:

- node.cfg содержит настройки отслеживаемых нод.
- networks.cfg содержит список сетей ноды в нотации CIDR.
- broctl.cfg хранит глобальные настройки BroControl.

Настройка отслеживаемых нод

Чтобы настроить ноды, которые будет отслеживать Bro, откройте файл node.cfg.

«Из коробки» Bro работает в автономном режиме. Поскольку в данном случае режим меняться не будет, никаких изменений в этот файл вносить не нужно. Но лучше все же убедиться, что он содержит правильные параметры.

Откройте файл:

```
sudo nano /usr/local/bro/etc/node.cfg
```

В разделе bro найдите параметр interface. По умолчанию он имеет значение etho0. Это значение должно совпадать с публичным интерфейсом сервера Ubuntu 16.04. В случае необходимости откорректируйте его.

```
[bro]
type=standalone
```

```
host=localhost
interface=eth0
```

Сохраните и закройте файл.

Настройка частных сетей ноды

В файле networks.cfg нужно указать, к каким сетям относится нода (то есть какие сети нужно отслеживать).

Откройте файл:

```
sudo nano /usr/local/bro/etc/networks.cfg
```

По умолчанию он содержит три блока Private IP. Используйте их в качестве примера, чтобы добавить свои сети.

```
# List of local networks in CIDR notation, optionally followed by a
# descriptive tag.
# For example, "10.0.0.0/8" or "fe80::/64" are valid prefixes.
10.0.0.0/8          Private IP space
172.16.0.0/12       Private IP space
192.168.0.0/16      Private IP space
```

Удалите эти три записи и добавьте данные о своих сетях. Чтобы проверить сетевой адрес интерфейсов, используйте ip addr show. В результате файл будет выглядеть примерно так (адреса будут отличаться):

```
203.0.113.0/24          Public IP space
198.51.100.0/24         Private IP space
```

Сохраните и закройте файл.

Настройка почты и логирования

Файл broctl.cfg содержит глобальные настройки BroControl, в том числе и параметры почты и логирования. Большую часть параметров по умолчанию менять не нужно. Нужно только указать свой адрес электронной почты.

Откройте файл:

```
sudo nano /usr/local/bro/etc/broctl.cfg
```

В разделе Mail Options найдите параметр MailTo и укажите в нем валидный адрес электронной почты, на который Bro сможет отправлять отчеты и уведомления.

```
. . .
# Mail Options
# Recipient address for all emails sent out by Bro and BroControl.
MailTo = 8host@example.com
. . .
```

Сохраните и закройте файл.

5: Управление Bro с помощью BroControl

BroControl позволяет управлять установками Bro – запуском и остановкой сервиса, развертыванием и т. п. BroControl является одновременно инструментом командной строки и интерактивной оболочкой.

Если broctl вызывается с помощью sudo sudo /usr/local/bro/bin/broctl, инструмент запустит интерактивную оболочку:

```
Welcome to BroControl 1.5-21
Type "help" for help.
[BroControl] >
```

Чтобы закрыть ее, введите exit.

В оболочке вы можете запустить любую валидную команду Bro. Те же команды могут также запускаться непосредственно из командной строки без вызова оболочки. Работа в командной строке часто является более полезным подходом, поскольку позволяет передавать вывод команды broctl стандартной команде Linux.

> **Примечание**: Далее работа с broctl происходит в командной строке.

Чтобы запустить Bro и убедиться, что все файлы BroControl и Bro обновились, введитие broctl deploy:

```
sudo /usr/local/bro/bin/broctl deploy
```

Эту команду нужно запускать после любых изменений в конфигурации или скриптах.

Примечание: Если Bro не запускается, в выводе вы сможете найти подсказки, почему так происходит. К примеру, если у вас нет почтового агента, вы увидите такую ошибку:

```
bro not running (was crashed)
Error: error occurred while trying to send mail: send-mail:
SENDMAIL-NOTFOUND not found
starting ...
starting bro ...
```

Чтобы исправить ошибку, нужно отредактировать файл BroControl /usr/local/bro/etc/broctl.cfg и добавить в него запись для Sendmail в конец раздела Mail Options.

```
. . .
# Added for Sendmail
SendMail = /usr/sbin/sendmail
################################################
# Logging Options
. . .
```

Чтобы повторить развертывание Bro, введите:

```
sudo /usr/local/bro/bin/broctl deploy
```

Проверить состояние Bro можно с помощью команды:

```
sudo /usr/local/bro/bin/broctl status
Name         Type       Host          Status    Pid    Started
bro          standalone localhost     running   6807   12 Apr 05:42:50
```

Кроме running, вывод также поддерживает состояние crashed или stopped.

Чтобы перезапустить Bro, используйте:

```
sudo /usr/local/bro/bin/broctl restart
```

Примечание: Команды broctl restart и broctl deploy – не одно и то же. Первая позволяет остановить и перезапустить весь сервис, а вторая – обновить

конфигурации и сценарии.

6: Настройка cron для Bro

Читайте также: Планирование рутинных задач Linux при помощи Cron и Anacron

У Bro нет файла дескриптора сервиса Systemd, но он поставляется с cron-сценарием, который, если он включен, перезапустит Bro в случае сбоя и выполнит другие задачи (такие как проверка дискового пространства и удаление устаревших файлов).

Bro поддерживает команду cron «из коробки», но вам нужно установить cronjob для запуска сценария. Сначала добавьте файл cron для Bro в /etc/cron.d. По соглашению такой файл должен называться bro.

```
sudo nano /etc/cron.d/bro
```

Затем нужно скопировать и вставить в файл следующую запись. Она будет запускать cron для Bro каждые пять минут. В случае сбоя приложение Bro будет перезапущено.

```
*/5 * * * * root /usr/local/bro/bin/broctl cron
```

Чтобы изменить интервал запуска, замените 5 другим значением.

Сохраните и закройте файл.

После включения cronjob вы получите электронное письмо, в котором сообщается, что каталог для файлов статистики создан в /usr/local/bro/logs/stats. Имейте в виду: чтобы эти файлы начали работать, приложение Bro должно выйти из строя (то есть, некорректно завершить работу). В таком случае команда BroControl stop не поможет.

Чтобы убедиться, что файлы работают, нужно перезапустить компьютер или убить один из процессов Bro. Если вы выберете перезагрузку, приложение Bro будет перезапущено через пять минут после завершения процесса перезагрузки сервера. Чтобы использовать второй подход, сначала получите один из идентификаторов процесса Bro.

```
ps aux | grep bro
```

Теперь прервите один из процессов:

```
sudo kill -9 process_id
```

Проверьте состояние приложения:

```
sudo /usr/local/bro/bin/broctl status
Name         Type       Host          Status    Pid    Started
bro          standalone localhost     crashed
```

Через несколько минут снова запросите состояние. Приложение должно быть запущено.

Система Bro должна отправлять сводные электронные письма о событиях, которые происходят на интерфейсе каждый час. И если она выйдет из строя и перезагрузится, она сообщит вам об этом с помощью письма.

7: Использование bro, bro-cut и сценариев политики Bro

Команды bro и bro-cut – еще две важные утилиты, поставляющиеся вместе с Bro. Команда bro позволяет собирать живой трафик и анализировать файлы трассировки, собранные другими инструментами. Команда bro-cut – это общий инструмент для чтения и сбора данных из логов Bro.

Команда для сбора живого трафика имеет такой формат:

```
sudo /usr/local/bro/bin/bro -ieth0 file...
```

В ней нужно указать, с какого интерфейса собирать трафик. «file…» относится к сценарию политики, который определяет процессы Bro. Их указывать необязательно, потому команда может иметь такой вид:

```
sudo /usr/local/bro/bin/bro -i eth0
```

> **Примечание**: Сценарии, которые Bro использует для работы, находятся в каталоге /usr/local/bro/share/bro. Индивидуальные сценарии сайтов находятся в каталоге /usr/local/bro/share/bro/site/. Не редактируйте никакие файлы в этом каталоге, кроме /usr/local/bro/share/bro/site/local.bro, так как ваши изменения будут перезаписаны при обновлении или переустановке Bro.

Команда bro создает в рабочем каталоге много файлов в рамках одной сессии сбора, потому лучше запускать эту команду в специально отведенном каталоге. Следующая команда ls –l выводит длинный список файлов:

```
total 152
-rw-r--r-- 1 root root   277 Apr 14 09:20 capture_loss.log
-rw-r--r-- 1 root root  4711 Apr 14 09:20 conn.log
-rw-r--r-- 1 root root  2614 Apr 14 04:49 dns.log
-rw-r--r-- 1 root root 25168 Apr 14 09:20 loaded_scripts.log
-rw-r--r-- 1 root root   253 Apr 14 09:20 packet_filter.log
-rw-r--r-- 1 root root   686 Apr 14 09:20 reporter.log
-rw-r--r-- 1 root root   708 Apr 14 04:49 ssh.log
-rw-r--r-- 1 root root   793 Apr 14 09:20 stats.log
-rw-r--r-- 1 root root   373 Apr 14 09:20 weird.log
```

Попробуйте запустить команду для сбора живого трафика, дайте ей немного поработать и остановите ее с помощью CTRL+C. Каждый файл можно прочитать с помощью bro-cut, для этого можно использовать такую команду:

```
cat ssh.log| /usr/local/bro/bin/bro-cut -C –d
```

Заключение

Теперь вы умеете устанавливать Bro из исходного кода и добавлять функцию геолокации адресов IPv4 и IPv6. Также вы ознакомились с основными инструментами Bro.