Факультет компьютерных технологий и прикладной математики

Кафедра вычислительных технологий

02.03.02

Информационная безопасность

Лабораторная работа № 10

Тема: NIPS/NIDS: Snort. SIEM.

Цель работы

Получить сведения о том, как осуществляется защита с помощью систем обнаружения и предотвращения вторжений. Научиться использовать SNORT. Получение теоретических и практических навыков работы с SIEM.

Указания к работе

Вначале студенты изучают теоретическую часть. Далее каждый студент должен выполнить задания, а также ответить на вопросы к лабораторной работе. За проделанную работу студент может получить оценку от «неудовлетворительно» до «отлично». Для получения оценки «удовлетворительно» студент должен выполнить ВСЕ задания к лабораторной работе. Оценка «хорошо» ставится, если студент ответил на ВСЕ вопросы к лабораторной работе. Оценку «отлично» студент получает, если подготовлен отчёт по лабораторной работе.

ОЦЕНКУ ЗА ПРОДЕЛАННУЮ РАБОТУ МОЖНО ПОВЫСИТЬ ДО СДАЧИ СЛЕДУЮЩЕЙ ЛАБОРАТОРНОЙ РАБОТЫ.

Теоретическая часть

Часть 1

Система обнаружения вторжений (IDS) – программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет.

Сетевая система обнаружения вторжений (англ. network intrusion detection system, NIDS) – система обнаружения вторжений, которая отслеживает такие виды вредоносной деятельности, как DoS-атаки, сканирование портов или даже попытки проникновения в сеть.

В пассивной IDS при обнаружении нарушения безопасности, информация о нарушении записывается в лог приложения, а также сигналы опасности отправляются на консоль и/или администратору системы по определенному каналу связи. В активной системе, также известной как Система Предотвращения Вторжений (IPS – Intrusion Prevention system (англ.)), IDS ведет ответные действия на нарушение, сбрасывая соединение или перенастраивая межсетевой экран для блокирования трафика от злоумышленника. Ответные действия могут проводиться автоматически либо по команде оператора.

Обнаружение проникновения позволяет организациям защищать свои системы от угроз, которые связаны с возрастанием сетевой активности и важностью информационных систем. При понимании уровня и природы современных угроз сетевой безопасности, вопрос не в том, следует ли использовать системы обнаружения проникновений, а в том, какие возможности и особенности систем обнаружения проникновений следует использовать.

Snort – свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом, способная выполнять регистрацию пакетов и в реальном времени осуществлять анализ трафика в IP-сетях.

Выполняет протоколирование, анализ, поиск по содержимому, а также широко используется для активного блокирования или пассивного обнаружения целого ряда нападений и зондирований, таких как попытки атак на переполнение буфера, скрытое сканирование портов, атаки на веб-приложения, SMB-зондирование и попытки определения операционной

системы. Программное обеспечение в основном используется для предотвращения проникновения, блокирования атак, если они имеют место.

Snort использует правила, написанные простым, но в то же время гибким и достаточно мощным языком. Существует ряд общих принципов написания, запомнить которые достаточно просто.

Большая часть правил Snort умещается в 1 строку. Это следствие того, что до версии 1.8 нельзя было использовать многострочные записи. В более поздних версиях правила можно растягивать на несколько строк, вставляя в конец строки символ “ ” (без кавычек).

Правила Snort состоят из двух частей: заголовка правила и параметров правила. Заголовок содержит описание действия, протокол передачи данных, IP-адреса, сетевые маски и порты источника и назначения. Параметры правила хранят предупреждающее сообщение, а также информацию о том, какую часть обнаруженного пакета нужно обработать в случае срабатывания правила.

Часть 2

SIEM (Security information and event management) – объединение двух терминов, обозначающих область применения ПО: SIM – Security information management – управление информационной безопасностью и SEM – Security event management – управление событиями безопасности. Технология SIEM обеспечивает анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений. SIEM представлено приложениями, приборами или услугами, и используется также для журналирования данных и генерации отчетов в целях совместимости (с прочими бизнес-данными).

Перед системой SIEM ставятся следующие задачи.

1. Агрегация данных: управление журналами данных; данные собираются из различных источников сетевые устройства и сервисы, датчики систем безопасности, серверы, базы данных, приложения; обеспечивается консолидация данных с целью критических событий.

2. Корреляция: поиск общих атрибутов, связывание событий в значимые кластеры. Технология обеспечивает применение различных технических приемов для интеграции данных из различных источников для превращения исходных данных в значащую информацию. Корреляция является типичной функцией подмножества Security Event Management.

3. Оповещение: автоматизированный анализ коррелирующих событий и генерация оповещений (тревог) о текущих проблемах. Оповещение может как выводиться на «приборную» панель самого приложения, так и быть направлено в прочие сторонние каналы: e-mail, GSM-шлюз и т.п.

4. Средства отображения (информационные панели): отображение диаграмм помогающих идентифицировать паттерны, отличные от стандартного поведения.

5. Совместимость (трансформируемость): применение приложений для автоматизации сбора данных, формированию отчётности для адаптации агрегируемых данных к существующим процессам управления информационной безопасностью и аудита.

6. Хранение данных: применение долговременного хранилища данных в историческом порядке для корреляции данных по времени и для обеспечения трансформируемости. Долговременное хранение данных критично для проведения компьютерно-технических экспертиз, поскольку расследование сетевого инцидента вряд ли будет проводиться в сам момент нарушения.

7. Экспертный анализ: возможность поиска по множеству журналов на различных узлах; может выполняться в рамках программно-технической экспертизы.

SIEM способна выявлять:

1) сетевые атаки во внутреннем и внешнем периметрах;

2) вирусные эпидемии или отдельные вирусные заражения, неудалённые вирусы, бэкдоры и трояны;

3) попытки несанкционированного доступа к конфиденциальной информации;

4) фрод и мошенничество;

5) ошибки и сбои в работе информационных систем;

6) уязвимости;

7) ошибки конфигураций в средствах защиты и информационных системах.

Splunk Enterprise – платформа для операционной аналитики. Способна осуществлять мониторинг и анализ всех действий, от посещений веб-сайтов и транзакций до сетевых операций и зарегистрированных вызовов.

Splunk – это мощный инструмент операционной аналитики, отслеживающий логи любых систем и собирающий их в единую базу.

Особенности системы:

1. Сбор данных из удалённых источников

2. Корреляция сложных событий, охватывающих множество разнородных источников данных в среде.

3. Масштабирование для сбора и индексации сотен терабайтов данных в день

4. Возможность комбинирования данных из традиционных реляционных БД и Hadoop для последующего анализа.

5. Ролевая модель доступа к данным.

6. Возможность создавать собственные приложения. Можно создавать панели (dashboard’ы), из которых формировать свое собственное Splunk-приложение. У Splunk есть магазин приложений (хотя большинство из них бесплатны), где есть море уже готовых конфигураций для анализа популярных систем, например, UNIX syslog, логи Apache, Microsoft Exchange и т.д.

Задания к лабораторной работе

Часть 1

Узнайте свой ip адрес командой ifconfig

Установите SNORT <sudo apt-get install snort>

При установке будет нужно указать защищаемую сеть. Введите ..*.0/24 (Где ..* – первые три числа вашего ip-адреса, например это будет

192.168.1.0/24, если вы используете VirtualBox и у вас в настройках сети стоит сетевой мост)

Запустите SNORT <sudo service snort start>

Настройка правил

Перейдите в каталог /etc/snort/rules < cd /etc/snort/rules)

Создайте файл с правилами <sudo nano test.rules>

alert tcp any any -> any any (content:»https://www.google.ru/» ; msg:»Someone open Google website» ; sid: 12312313;)

Перейдите в каталог /etc/snort <cd /etc/snort)

Теперь нужно изменить содержимое конфигурационного файла Snort < sudo nano snort.conf>

Найдите строчки с правилами (они начинаются с include $RULE_PATH, это в части Step 7) и добавьте файл с нашими правилами

include $RULE_PATH/test.tules

В файле snort.conf также укажите домашнюю сеть. В Step 1 измените строчку «ipvar HOME_NET any» , на

ipvar HOME_NET 192.168.1.0/24

Запустите snort <sudo snort -A console -i eth0 -c snort.conf>

Зайдите на https://www.google.ru/ и проверьте в терминале, как работает правило.

Теперь нам понадобиться еще одна виртуальная машина, на ней должен быть установлен nmap.

Со второй ВМ используйте ping, посмотрите, как реагирует SNORT

Используйте различные методы сканирования nmap(используйте -sS, -sT, -sN, -sU, -sX, -sF и посмотрите, как реагирует SNORT;

В файл test.rules добавьте правило обнаружения сканирования nmap -sN (NULL Scan)

alert tcp any any -> any any (msg:»NULL Scan»; flags: 0; sid:322222;)

Запустите snort <sudo snort -A console -i eth0 -c snort.conf>

Со второй виртуальной машины произведите NULL сканирование <sudo nmap -sN>, проверьте, как работает правило.

Часть 2

Загрузите Splunk Enterprise с http://www.splunk.com/ru_ru/download/splunk-enterprise.html. Выберите вашу систему, после чего нужно будет зарегистрироваться.

После загрузки дистрибутива, его необходимо установить. Установка deb пакета выполняется командой <dpkg -i splunk_package_name.deb>. О других типах установки можно прочитать здесь.

Для запуска Splunk выполните </opt/splunk/bin/splunk start>.

Запустите web-интерфейс, при запуске splunk будет указано, как подключиться к нему (что-то похожее на https://sit-VirtualBox:8000), чтобы начать использовать систему.

Учётные данные по умолчанию – admin – changeme. При первом входе Вам будет предложено их изменить.

В левой части окна будут перечислены приложения, установленные в Splunk и доступные для работы. Приложение – это своего рода среда или интерфейс, в котором пользователь работает с событиями, которые собирает Splunk. По умолчанию доступно приложение Search and Reporting. У Splunk есть несколько основных типов расширения функциональности – приложения (Apps) и дополнения (Add-on).

В центральной части экрана будет пустое окно, на котором предполагается размещение главного дашборда. В правой верхней части расположено меню для управления системой Splunk, в том числе всеми источниками данных.

Подключим источник событий. Добавим журнал событий Linux, для мониторинга. В правой верхней части экрана выбирайте меню Settings и переходите в Data Inputs

Перейдите в меню Settings – Data Input - Files & directories. Тип Files & directories позволяет получать события из локальных файлов и директорий.

Нажмите на кнопку «New», введите путь к файлу auth.log (var/log/.auth.log) и выберите continuously monitor.

Нажмите «Next». Выберите тип данных (sourcetype – operating system) из списка, а именно «linux_audit». В открывшемся окне можно ничего не менять. Если всё прошло успешно, то после нажатия на «Start searching» вы увидите перечень событий из журнала аудита.

Перейдите в меню Settings – Data Input - Files & directories. Добавьте домашнюю директорию, в ней создайте и удалите несколько файлов, Просмотрите журнал событий в Splunk.

Добавьте еще несколько файлов, директорий и логов, через меню Settings – Data Input - Files & directories.

Перейдите в приложение «Search and Reporting». Вы попадете на вкладку Search.

Найдите события, которые относятся к файлу var/log/.auth.log , для этого введите «source=var/log/.auth.log». Здесь так же можно выбрать записи который относятся к Sourcetype (sourcetupe=operating system) – это имя типа данных, куда предполагается относить все данные определённого типа, или Host (host=splunk) – это идентификатор источника, от которого приходят события в какой-либо sourcetype (обычно доменное имя или ip-адрес). Можно фильтровать данные, введя в строку поиска определенные параметры, вы получите записи, только с этими параметрами. Можно делать составные запросы. Один запрос может состоять из множества подзапросов разделенных между собой pipe (|), и справа налево каждый следующий запрос оперирует данными полученными в результате выполнения предыдущего.

Сбор логов – это далеко не всё, что необходимо для безопасности. Для SIEM нужно, чтобы система не только собирала логи, но и находила события, связанные с нарушениями безопасности. При слежении за логами, можно автоматически обнаруживать любые угрозы безопасности. Splunk можно использовать вместе с IDS.

В данной лабораторной работе вы уже познакомились IDS Snort. Так что, установите и настройте Snort, так же как в лабораторной работе №14. Запустите Snort с ведением логов <sudo snort -A console -i eth0 -c snort.conf -l /var/log/snort/>. Произведите различные типы сканирования nmap, и проверку правил Snort. И добавьте логи Snort в Splunk. Вы так же можете загрузить приложение Snort для Splunk https://splunkbase.splunk.com/app/340/. Вместо Snort можно так же использовать OSSEC, для OSSEC тоже есть приложение в Splunk.

Вопросы к лабораторной работе

Часть 1

1. Что такое IDS?
2. Что такое сетевая система обнаружения вторжений?
3. Чем отличаются пассивные и активные IDS?
4. Что такое SNORT?
5. Какие задачи выполняет SNORT?
6. Как работают правила SNORT?
7. Как писать правила для SNORT?
8. Зачем писать собственные правила SNORT?
9. Зачем загружать обновление правил SNORT?
10. Как в SNORT создавать логи?

Часть 2

1. Что такое SIEM?
2. Для чего используют SIEM?
3. В чем отличие SIEM от IDS?
4. Где используют SIEM?
5. В чем преимущества SIEM?
6. В чем недостатки SIEM?
7. Какие существуют альтернативы использованию SIEM?