МОДЕЛИ АНАЛИЗА ЖУРНАЛОВ БЕЗОПАСНОСТИ СЕТЕВОГО ОБОРУДОВАНИЯ

Бельчик Эдуард Эдуардович
Шапорин В.О., к.т.н., доцент

Комплексная защита компьютерной сети современного уровня требует использования различных средств безопасности, таких как системы обнаружения сетевых атак, системы защиты от спама, антивирусы, межсетевые экраны (firewall), сканеры безопасности и т.д. При этом возрастание количества аппаратных и программных средств защиты сети значительно увеличивает объём анализируемой информации, необходимый для контроля безопасности. Как следствие - администраторы сети должны уделять значительное время анализу рутинной информации, что снижает продуктивность работы и, соответственно, влияет на оперативное принятие решений по поддержке функционирования компьютерной сети. Таким образом, возникает противоречие между увеличением объёма информации, которую целесообразно анализировать для предотвращения угроз, и оперативностью управления сетью. Для данных целей используют системы мониторинга, которые основаны на анализе журналов безопасности [1].

Целью работы является изучение и усовершенствование модели анализа журналов безопасности сетевого оборудования, используемых в системах мониторинга для обеспечения конечного пользователя актуальной и достоверной информацией о функционировании сети.

Основная часть работы. Системы мониторинга, анализирующие журналы безопасности сетевого оборудования (например, ELSA (Enterprise Log Search and Archive) входящая в пакет утилит Security Onion) для сбора и синтаксического анализа журналов безопасности используют syslog-ng. Syslog-ng – реализация протокола syslog для Unix и Unix-подобных систем, расширяющая возможности исходного протокола.

Syslog (англ. *system log* — системный журнал) — стандарт отправки и регистрации сообщений о происходящих в системе событиях (то есть создания логов), использующийся в компьютерных сетях, работающих по протоколу IP. Термином «syslog» называют как ныне стандартизированный сетевой протокол syslog, так и программное обеспечение (приложение, библиотека), которое занимается отправкой/получением системных сообщений. Суть механизма Syslog проста: источники формируют простые текстовые сообщения о происходящих в них событиях и передают их на обработку серверу Syslog (называемому «syslogd», «syslog daemon», либо же, «syslog server»), используя один из сетевых протоколов семейства IP (UDP или TCP). Формирование сообщений о событиях и их передача происходит по определенным правилам, называемым протоколом Syslog. Как правило сообщение имеет небольшой размер (до 1024 байт) и отсылается в открытом виде [2].

Записи журналов безопасности имеют примерно следующий вид: [дата записи с точностью до секунды] : [тип записи] : [текст сообщения]. Под типами записи подразумевается некий набор параметров, каждый из которых определенным образом классифицирует конкретную запись журнала. Типы записи журналов безопасности не имеют четкой стандартизации, в связи с чем различается от одной операционной системы к другой, от одного программного обеспечения к другому, от одного устройства к другому. По этой причине возникает необходимость разработки унифицированной классификации типов записей и ее применение для усовершенствования анализа журналов безопасности.

Определим термин «вид журнала безопасности». Под видом журнала безопасности будет подразумеваться журнал безопасности, принадлежащий определенной операционной системе, определенному программному обеспечению или определенному виду сетевого оборудования.

Стратегия усовершенствования процесса анализа журналов безопасности следующая:

1. Анализ уровней журналирования всех различных видов журналов безопасности, используемых в сети.

2. Разработка унифицированной классификации.

3. Разработка модели оценивания и ее использование для применения унифицированной классификации.

Унифицированная классификация может иметь следующий вид:

1. Критическая ошибка.
2. Ошибка.
3. Предупреждение.
4. Информационное сообщение.
5. Отладочное сообщение.

Первые четыре пункта предложенной классификации повторяют типы записей (уровни приоритета) журнала безопасности операционной системы Windows.

Кратко о каждом типе записи классификации:

1) Критическая ошибка – событие указывает на сбой в приложении или части операционной системы, которое не может быть восстановлено автоматически;

2) ошибка – событие указывает на существенные проблемы, которые обычно приводят к потере функциональности или данных;

3) предупреждение – событие указывает на проблемы, которые не требуют немедленного вмешательства, но могут привести к ошибкам в будущем;

4) информационное сообщение – событие указывает на редкие и важные успешные операции. Записи в этой категории, как правило, отчеты о состоянии;

5) отладочное сообщение – событие, связанное с обращением пользователя к ресурсам, которые могут быть защищены на уровне прав доступа, а также сообщения – связанные с налаживанием работы операционной системы, программного продукта или сетевого оборудования.

Назначение новой классификации записям будет проводиться на основе лингвистического анализа каждой записи каждого журнала безопасности, полученного системой мониторинга. На основе результатов анализа записям будет назначаться цифровой эквивалент (соответствует порядковому номеру), соответствующий типу записи унифицированной классификации. Так как возможно ситуация, при которой одна запись журнала будет содержать несколько типов записей (уровней приоритета) ей будет назначен тип из унифицированной классификации с наименьшим числовым коэффициентом.

В случае, если анализ не дал результатов и новый тип классификации не был назначен – система проанализирует сообщение текущей записи журнала безопасности для определения типа классификации. Если данный анализ также не даст результатов, то записи будет назначен тип «информационное сообщение» с указанием, что система не смогла явно определить тип классификации записи. Данный подход поможет точно определить тип классификации записи журнала безопасности, если это возможно.

Рассмотрены существующие решения по анализу журналов безопасности сетевого оборудования. Определена стратегия усовершенствования. Данная система позволяет проводить непрерывный мониторинг в режиме реального времени и отправлять полученные данные в БД конечного пользователя. Осуществление данной функции позволяет оценивать состояние функционирования сети и может быть использовано для быстрого определения и исправления возникающих сбоев.