УДК 504.064.36

МОНИТОРИНГ IT-СИСТЕМ И СЕТЕВЫХ УСТРОЙСТВ

И.М.Шамин

студент института приоритетных технологий кафедры информационной безопасности

Волгоградский государственный университет

goldenchildivan@gmail.com

Аннтотация: Мониторинг IT-систем и сетевых устройств является неотъемлемой частью своевременного реагирования как на ошибки сети, пользователей, операционной системы, так и на инциденты информационной безопасности (ИБ), которые могут указывать как на аномальное поведение, так и на атаки.

До появления автоматизированных систем мониторинга администратору безопасности приходилось собирать сведения от сетевых устройств и от рабочих станций пользователей вручную. Например, когда пользователи не могут обмениваться файлами через FTP (File Transfer Protocol), они пишут в поддержку, сообщая о своей проблеме. Поддержка довольно долго будет искать в чем проблема, если нет системы мониторинга. При наличии же такой системы администратор сразу увидит в списки событий, что много запросов на FTP поступало снаружи и были заблокированы каким-нибудь прокси-сервером, межсетевым экраном.

В статье дается понятие о мониторинге, приводится классификация по источникам событий. Рассматриваются требования, которые должны быть в программном обеспечении (ПО) по мониторингу сети. Поднимается вопрос о важности проведения мониторинга для организаций, у которых стоят требования: минимальные затраты за максимальный функционал. В связи с этим, является актуальным рассмотрение 10 наиболее функциональных и популярных бесплатных программ для мониторинга и анализа событий.

Ключевые слова: мониторинг систем, анализ событий, источники событий.

MONITORING IT-SYSTEMS AND NETWORK DEVICES

I.M. Shamin

Student of the Institute of Priority Technologies of the Information Security Department

Volgograd State University

goldenchildivan@gmail.com

Annotation: Monitoring of IT systems and network devices is an integral part of timely response to network errors, users, the operating system, and information security (IS) incidents, which can indicate both abnormal behavior and attacks.

Before the advent of automated monitoring systems, a security administrator had to collect information from network devices and from user workstations manually. For example, when users cannot share files via FTP (File Transfer Protocol), they write in support, reporting their problem. Support for a long time will look for what the problem is, if there is no monitoring system. If there is such a system, the administrator will immediately see in the event lists that many requests for FTP have been received outside and have been blocked by some proxy server, a firewall.

The article gives the concept of monitoring, provides a classification by event sources. Considers the requirements that should be in the software (software) for network monitoring. The question of the importance of monitoring for organizations that have requirements is raised: minimum costs for maximum functionality. In this regard, it is relevant to consider the 5 most functional and popular free programs for monitoring and analyzing events.

Key words: system monitoring, event analysis, event sources.

Понятие мониторинга, классификация систем мониторинга по источникам.

Система мониторинга [5] – это совокупность технических средств, осуществляющих непрерывное наблюдение и сбор информации в локальной вычислительной сети (ЛВС), рабочих станциях пользователя на основе анализа статистических данных, происходящих в системе с целью выявления неисправных или некорректно работающих узлов и оповещения администраторов безопасности.

Существует большое количество систем мониторинга. Они могут быть собирать данные от [1]:

1. **Сетевые источники событий** – это так называемые анализаторы протоколов, они нужны для контроля сетевого трафика. Примерами таких источников могут быть:

— *Syslog (system log – системный журнал)* является стандартным средством для журналирования в системах семейства Unix и Linux, а позже стал использоваться и на других операционных системах. Этот термин также употребляется в качестве протокола syslog. Этот протокол использует порт UDP 514 для отправки сообщений с уведомлением о сетевых событиях по сетям IP. Работает с многими сетевыми устройствами, например, маршрутизаторы, коммутаторы, межсетевые экраны и т.д. Для приема таких сетевых уведомлений иногда разворачивают специальную выделенную сеть. Основные задачи, которые решает данный протокол это: сбор информации для мониторинга и отладки, выбор типа собираемой информации, а также получателей этой информации. Сообщения, которые можно получить от сетевых устройств делятся на 7 уровней важности (таблица 1)

Название уровня важности	Пояснение
Уровень 0 – чрезвычайная ситуация	Невозможно дальнейшее использование системы. Описываются события, содержащие данные о сервисах.
Уровень 1 – предупреждение	Необходимо срочно принять меры.
Уровень 2 – критический	Критическое состояние вторичной системы.
Уровень 3 – ошибка	Ошибки, которые не требуют незамедлительного вмешательства
Уровень 4 – предупреждение	Предупреждают о возможных проблемах. При этом, если игнорировать такие сообщения, то это может привести к возникновению проблем
Уровень 5 – уведомление	События, которые возникают при необычном поведении системы.
Уровень 6 – информационные	Полезны при составлении отчетов.
Уровень 7 – отладка	Информация для разработчиков программного обеспечения (ПО).

2. **Системные источники событий** – содержат в себе щирокий спектр информации от операционных систем (ОС), рабочих станций пользователя. Содержит в себе операции, которые выполняются компонентами ОС и рабочими станциями.

- *Журналы событий.*

Примером является события, которые регистрируются в ОС Windows. В этой ОС есть встроенные журналы:

- журнал установки журнал приложений;
- журнал системы;
- журнал операций;
- журнал пересылаемых событий;
- административный журнал;
- аналитический журнал;
- отладочный журнал;
- журнал безопасности.

Перечисленные журналы позволяют обычным пользователям или системным администраторам разобраться в причинах сбоя того или иного оборудования. Но т.к. этих

сведений много, создаются специализированные ПО, системы мониторинга и анализа событий.

Программное обеспечение, системы и инструменты для мониторинга. Обзор рынка.

Выделяются основные требования, которые должны быть в программном обеспечении (ПО) по мониторингу сети [4]:

1. Поддержка всех видов сетевых подключений, в том числе wifi сети.
2. Слежка за сетевой активностью.
3. Определение детальности системных и сетевых служб.
4. Анализ удаленных компьютеров и веб серверов.

Системы мониторинга должны предоставлять отчеты про события за определенные временные периоды. Важно сохранять весь листинг активности и архивировать его в соответствующем журнале.

Требуется различать средства, которые обеспечивают контроль внешнего доступа сети и программного обеспечения, что важно для контроля за внутри сетевыми процессами.

Мониторинг активности сети определяется так:

1. Приложение с определенным периодом отправляет запросы по необходимым ip адресам сети.
2. При некорректном или неудачном результате подобного запроса, отправляется сигнал администратору безопасности.
3. Автоматическое определение действия, которые регламентированы сетевым протоколом.

В организации всегда встает материальный вопрос: реализация максимальных мер по мониторингу и анализу при минимальных затратах. Поэтому целесообразно рассмотреть бесплатные, но не менее функциональные решения [2,3]:

1. Zabbix 4.0 - открытое ПО для мониторинга и отслеживания статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования, используется для получения данных о нагрузке процессора, использования сети, дисковом пространстве и тому подобного.
2. SCOM (part of Microsoft System Center) - System Center — представляет собой полный набор инструментов для управления IT-инфраструктурой, с помощью которых Вы

сможете управлять, развертывать, мониторить, производить настройку программного обеспечения Microsoft (Windows, IIS, SQLServer, Exchange, и так далее). Увы, MSC не является бесплатным. SCOM используется для проактивного мониторинга ключевых объектов IT-инфраструктуры.

3. Nagios - является самым популярным инструментом мониторинга инфраструктуры в течение нескольких лет (для Linux и Windows). Если Вы рассматриваете Nagios для Windows, то установите и настройте агент NSClient ++ на Windows сервер. NSClient ++ мониторит систему в реальном времени и предоставляет выводы с удаленного сервера мониторинга и не только.

4. Enigma - приложение, которое поможет Вам следить за всеми важных показателями прямо с рабочего стола для ОС семейства Windows

5. Nixstats - это сервис для отслеживания статистики, различных маркетинговых метрик, и доступности удаленных серверов и сайтов. Платформа имеет удобный веб-интерфейс. Присутствует бесплатная версия, оповещения через смс и мессенджеры. Сервис основан одноименной компанией из Амстердама в 2017 году. За это время сайтом успели воспользоваться более 15 000 клиентов.

6. Zenoss - гибкий комплексный сервис для мониторинга событий, производительности и доступности

7. SpiceWorks - полностью бесплатная (даже поддержка) система мониторинга с богатыми возможностями.

8. Reliability Monitor – монитор стабильности системы, позволяет отслеживать любые изменения в производительности компьютера, найти монитор стабильности можно в Windows 7, 8, 10: Control Panel > System and Security > Action Center. С помощью Reliability Monitor можно вести учет изменений и сбоев на компьютере, данные будут выводиться в удобном графическом виде, что позволит Вам отследить, какое приложение и когда вызвало ошибку или зависло, отследить появление синего экрана смерти Windows, причину его появления (очередное обновлением Windows или установка программы).

9. Microsoft SysInternals - это полный набор программ для администрирования и мониторинга компьютеров под управлением ОС Windows. Вы можете скачать их себе бесплатно на сайте Microsoft. Сервисные программы Sysinternals помогают управлять, находить и устранять неисправности, выполнять диагностику приложений и операционных систем Windows.

10. Task Manager - всем известный диспетчер задач Windows — утилита для вывода на экран списка запущенных процессов и потребляемых ими ресурсов. Но знаете ли Вы, как использовать его весь потенциал? Как правило, с его помощью контролируют

состояние процессора и памяти, но можно же пойти гораздо дальше. Это приложение предварительно на всех операционных системах компании Microsoft.

Заключение

Внедрение системы мониторинга – это важный шаг на пути к полной автоматизации ИТ-инфраструктуры, который ведет к повышению эффективности ее использования. Необязательно использовать большие системы мониторинга, например, SIEM (Security information and event management), которые в основном платные и содержат в себе большой функционал, вплоть до обнаружения и предупреждения атак. Если организация небольшая, то администратору может хватить бесплатных инструментов для эффективного проведения мониторинга и анализа.

Литература

1. А. Астахов: "Мониторинг действий пользователей корпоративной сети". - Мир и безопасность №1, 2008.
2. Электронный ресурс: 51 инструмент для АРМ и мониторинга серверов https://habr.com/company/pc-administrator/blog/304356/
3. Электронный ресурс: 7 бесплатных программ для мониторинга сети и серверов https://steptosleep.ru/ что-такое-мониторинг-сети/#i-7
4. Электронный ресурс: СИСТЕМА МОНИТОРИНГА СЕТИ https://wiki.merionet.ru/servernye-resheniya/sistema-monitoringa-seti/
5. Электронный ресурс: Что такое мониторинг в IT или почему админы стали больше спать? https://habr.com/company/croc/blog/144941/