УДК 004.664

МОНИТОРИНГ И АНАЛИЗ ТРАФИКА ЛОКАЛЬНЫХ СЕТЕЙ

С. Г. САЕВИЧ
(Представлено: канд. пед. наук, доц. П. П. МАТЕЛЕНОК)

Статья посвящена проблемам построения контроля, анализа и управления трафиком локальной сети. Представлена смоделированная экспериментальная сетевая среда. Которая представляет собой типичный сегмент локальной вычислительной сети и включает все необходимые компоненты для демонстрации процесса обнаружения аномальной активности с использованием протокола SNMP.

Обеспечение непрерывной работоспособности сетевой локальной инфраструктуры предполагает систематический контроль за ее операционной деятельностью. Применение специализированных систем мониторинга и анализа предоставляет администратору возможность идентифицировать и ликвидировать любые факторы, представляющие угрозу для штатного функционирования сети. Процесс контроля работы сети делится на два этапа – мониторинг и анализ.

На этапе мониторинга выполняется более простая процедура – процедура сбора первичных данных о работе сети: статистики по циркулирующим в сети пакетам различных протоколов, состоянии портов коммуникационных устройств и т.п. Благодаря ему можно провести анализ трафика локальных сетей для выявления проблем с безопасностью, оптимизации производительности и отладки сети.

В предлагаемой к рассмотрению статье, мы поговорим об одной из ключевых проблем современной IT-инфраструктуры – обеспечении безопасности и стабильности локальных сетей. Сложная структура корпоративных сетей создает значительные трудности в их управлении и защите от постоянно растущего числа киберугроз.

Центральной задачей становится оперативное обнаружение аномальной сетевой активности, которая может привести к сбоям в работе, утечке или потере данных. Традиционные средства защиты, такие как антивирусы и межсетевые экраны, имеют свои ограничения: они потребляют много ресурсов и зачастую неспособны выявлять новые или модифицированные типы атак.

В нашем докладе мы рассмотрим эффективный метод выявления аномалий в сетевом трафике с помощью протокола SNMP (Simple Network Management Protocol). Мы покажем, как этот, на первый взгляд, простой инструмент мониторинга позволяет не только отслеживать состояние сетевых устройств, но и своевременно обнаруживать подозрительную активность.

SNMP предоставляет ценные данные для анализа, помогая выявлять отклонения от нормального поведения сети, которые могут указывать на технические сбои или целенаправленные атаки.Важно понимать, что SNMP сам по себе не является средством борьбы с угрозами, но он служит ключевым инструментом для их обнаружения и сбора информации, необходимой для принятия оперативных мер.

Цель работы – продемонстрировать, как с помощью SNMP можно построить эффективную систему мониторинга для раннего выявления аномального трафика и повышения общего уровня защищенности локальной сети."

Для проведения исследования была смоделирована экспериментальная сетевая среда. Эта среда представляет собой типичный сегмент локальной вычислительной сети и включает все необходимые компоненты для демонстрации процесса обнаружения аномальной активности с использованием протокола SNMP.

Ключевые элементы стенда:

1. **Сервер мониторинга (IP: 192.168.6.164):** Центральным элементом является сервер, функционирующий под управлением ОС Kali Linux. На нем развернута система сетевого мониторинга Observium. Данная система сконфигурирована для автоматического обнаружения сетевых устройств в заданном сегменте, периодического сбора метрик их производительности и состояния по протоколу SNMP, а также для визуализации полученных данных в виде графиков в реальном времени.
2. **Сетевые маршрутизаторы (R1 и R2):** В качестве объектов мониторинга выступают два маршрутизатора: R1 (IP: 192.168.6.175) и R2 (IP: 192.168.6.172). На обоих устройствах была выполнена базовая конфигурация и активированы SNMP-агенты. Это позволяет системе Observium осуществлять их опрос для сбора ключевых параметров, таких как загрузка и ошибки на интерфейсах, использование ресурсов процессора и памяти, а также состояние таблиц маршрутизации.
3. **Компьютер атакующего (IP: 192.168.6.174):** Для имитации несанкционированного воздействия и генерации аномального трафика используется отдельная рабочая станция под управлением ОС Kali Linux. Данный узел предназначен для проведения контролируемого тестирования безопасности, в рамках которого будет осуществлена атака типа UDP Flood.

Цель и начальные условия эксперимента. Целью эксперимента является демонстрация фиксации аномального роста трафика на интерфейсе fa0/0 маршрутизатора R2 (192.168.6.172) средствами системы Observium в момент проведения атаки.

Зафиксировано исходное состояние сети до начала атаки, которое можно охарактеризовать как "мирное время". Система мониторинга успешно подключилась к устройствам и начала сбор данных. Мы наблюдаем незначительную фоновую сетевую активность на целевом интерфейсе, соответствующую нормальному обмену служебным трафиком (например, ARP-запросы, протоколы маршрутизации). Эти данные служат эталонным показателем, с которым будут сравниваться метрики во время атаки."

На данном этапе нашего исследования мы переходим к практической реализации атаки с целью демонстрации возможностей системы мониторинга.

Инициация атаки: С рабочей станции атакующего (IP: 192.168.6.174) была инициирована атака типа **UDP Flood**, направленная на интерфейс FastEthernet0/0 маршрутизатора R2 (IP: 192.168.6.172). Для этого была использована специализированная утилита hping3 с командой, представленной на экране:

sudo hping3 --flood --rand-source -p 80 --udp 192.168.6.172

Механизм атаки: Суть данного воздействия заключается в генерации непрерывного потока UDP-пакетов на целевое устройство с максимально возможной скоростью (--flood). Поскольку протокол UDP является транспортным протоколом без установления соединения, он не требует подтверждения доставки пакетов. Это позволяет злоумышленнику генерировать критический объем трафика с минимальными затратами собственных вычислительных ресурсов. Использование опции --rand-source приводит к подмене IP-адреса отправителя в каждом пакете, что значительно усложняет идентификацию истинного источника атаки.

Целью атаки является исчерпание пропускной способности сетевого канала и перегрузка системных ресурсов целевого устройства (центрального процессора, памяти) за счет необходимости обработки лавинообразного потока входящих пакетов. Это приводит к деградации или полному отказу в обслуживании легитимных пользователей.

Как видно из терминального вывода, в ходе атаки было отправлено **более 24 миллионов пакетов**. Отсутствие ответных пакетов является характерным признаком успешного проведения флуд-атаки."

Реакция системы мониторинга Observium, взаимодействующей с сетевым оборудованием по протоколу SNMP, была незамедлительной.

1. Всплеск трафика (График слева): На детализированном графике трафика для интерфейса FastEthernet0/0 мы наблюдаем резкий, практически вертикальный скачок входящего (зеленая область) и исходящего (синяя область) трафика. Этот всплеск является прямым визуальным подтверждением UDP Flood атаки. Именно благодаря регулярным SNMP-опросам счетчиков интерфейса, система Observium смогла в реальном времени зафиксировать эту аномальную активность, ее интенсивность и точное время начала.

2. Критическая нагрузка и ее последствия (Панель справа): На информационной панели устройства видны не только мини-графики трафика, подтверждающие аномалию, но и показатели критического использования системных ресурсов — памяти и центрального процессора маршрутизатора.

SNMP позволил системе мониторинга зафиксировать полный цикл инцидента, который не виден из простого анализа трафика:

- **Фиксация перегрузки:** Система получила данные о 100% загрузке процессора, что предшествовало отказу.
- **Обнаружение отказа:** Когда маршрутизатор перестал отвечать на SNMP-запросы и ICMP-проверки, Observium изменил его статус на **"Down"**.
- **Регистрация перезагрузки:** В журнале событий (Eventlog) было зафиксировано, что устройство было перезагружено. Это определяется через SNMP-переменную sysUpTime, которая сбрасывается при перезагрузке.
- **Восстановление:** После перезагрузки устройство вновь стало доступно, и его статус изменился на **"Up"**.

Поэтапно рассмотрим жизненный цикл инцидента, зафиксированный системой мониторинга, и увидим, как менялось состояние устройства от нормальной работы до полного восстановления.

- **Нормальная работа:** До инцидента система Observium, используя SNMP, фиксировала минимальный фоновый трафик и стабильную загрузку ресурсов маршрутизатора. Устройство регулярно и корректно отвечало на SNMP-запросы, подтверждая свою штатную работоспособность.
- **Начало атаки:**В момент инициации UDP Flood произошел резкий, экспоненциальный скачок трафика на интерфейсе FastEthernet0/0. Одновременно SNMP-данные показали критический всплеск загрузки центрального процессора и оперативной памяти, что свидетельствует о перегрузке аппаратных ресурсов.

- **Отказ устройства:** Под воздействием лавинообразного потока пакетов маршрутизатор R2 исчерпал свои ресурсы. Он перестал отвечать не только на диагностические ICMP-запросы (ping), но и на SNMP-запросы от системы мониторинга. Observium незамедлительно зафиксировал это, изменив статус устройства на **"Down"**. Не справившись с нагрузкой, устройство аварийно перезагрузилось.
- **Восстановление:**

Спустя некоторое время после отказа, устройство завершило перезагрузку. Его статус изменился на **"Up"**, что было подтверждено возобновлением успешных SNMP-ответов. С этого момента система мониторинга восстановила сбор метрик, регистрируя возвращение устройства в рабочий режим

Проведенное исследование наглядно демонстрирует критически важную роль протокола SNMP для многоуровневого анализа сетевых инцидентов. SNMP — это не просто протокол, а фундаментальный механизм, обеспечивающий "зрение" для системы мониторинга.

- **Визуализация данных:** Именно SNMP позволил построить наглядные графики трафика, которые четко продемонстрировали момент начала, интенсивность и продолжительность атаки. Без данных со счетчиков интерфейсов, полученных по SNMP, система мониторинга была бы "слепой" к происходящему и не смогла бы зафиксировать аномалию на сетевом уровне.
- **Диагностика состояния:** SNMP предоставил ключевую информацию о жизненном цикле устройства. Изменение значения sysUpTime (время непрерывной работы), полученное по SNMP, однозначно указывает на факт перезагрузки. Это позволило зафиксировать не только саму атаку, но и её тяжелые последствия для оборудования.
- **Детализированный мониторинг:** Даже сообщения об ошибках при сборе специфических метрик, как в случае с CISCO-ENVMON-MIB, являются ценной диагностической информацией. Они указывают на сбои в работе конкретных подсистем устройства, которые произошли во время атаки, и подтверждают глубину её воздействия.
- **Триггеры для действий:** Данные, получаемые по SNMP, могут служить основой для проактивных систем защиты. При достижении критических порогов (например, загрузка ЦП или трафик), можно автоматически инициировать защитные действия: временную блокировку портов, применение ACL-правил или отправку мгновенных SNMP-трапов администратору для немедленного реагирования."

Проведенное исследование наглядно демонстрирует, что протокол SNMP является не просто инструментом для мониторинга, а фундаментальным компонентом для обеспечения безопасности и стабильности современных локальных сетей. Его ценность выходит далеко за рамки простого построения графиков трафика.

Как показал эксперимент, SNMP позволил не только визуализировать аномальный всплеск трафика во время UDP Flood атаки, но и получить полную картину инцидента. Именно благодаря SNMP система мониторинга смогла:

1. **Диагностировать причину сбоя:** Зафиксировать критическую перегрузку процессора и памяти маршрутизатора, которая предшествовала отказу.
2. **Определить последствия:** Обнаружить факт отказа устройства (статус "Down") и его последующую аварийную перезагрузку, что было однозначно подтверждено изменением значения uptime.
3. **Оценить состояние подсистем:** Даже ошибки при сборе специфических данных (как в случае с CISCO-ENVMON-MIB) послужили важным диагностическим маркером, указывающим на глубину сбоя в работе оборудования.

Таким образом, SNMP выступает в роли незаменимых **"глаз и ушей"** для любой системы сетевого администрирования. Без него мониторинг остается "слепым", способным видеть лишь симптомы (например, недоступность устройства по ping), но не саму причину и масштаб проблемы.

В перспективе, потенциал SNMP раскрывается в создании проактивных систем защиты, где данные о состоянии сети служат триггерами для автоматических контрмер, предотвращая отказ оборудования еще до его наступления. В конечном счете, грамотное использование SNMP позволяет перейти от реакции на уже случившиеся инциденты к их своевременному предотвращению.