УДК 004.75:004.056

АНАЛИЗ АНОМАЛЬНОГО ТРАФИКА В ЛОКАЛЬНОЙ СЕТИ ПРИ ПОМОЩИ ПРОТОКОЛА SNMP

С. Г. Саевич, И. О. Петроченко, А. П. Мателенок

Полоцкий государственный университет имени Евфросинии Полоцкой, Новополоцк, Беларусь, a.matelenok@psu.by

Рассмотрены фундаментальные вопросы диагностики и защиты сетевых ресурсов от аномальных воздействий, приводящих к полной или частичной потере работоспособности, уничтожению, искажению, утечке информации, или несанкционированному доступу к сетевым ресурсам. Показано, как SNMP позволяет обнаруживать аномальную сетевую активность и предоставляет данные, на основе которых можно принять меры. SNMP сам по себе «не борется», но является ключевым инструментом для обнаружения и сбора информации, необходимой для борьбы.

Ключевые слова: аномальный трафик; протокол SNMP; информационные риски; анализ защищенности.

ANALYSIS OF ANOMALOUS TRAFFIC IN A LOCAL NETWORK USING SNMP PROTOCOL

S. G. Saevich, I. O. Petrochenko, A. P. Matelenok

Polotsk State University named after Euphrosyne of Polotsk, Novopolotsk, Belarus, a.matelenok@psu.by

The fundamental issues of diagnostics and protection of network resources from abnormal impacts leading to full or partial loss of functionality, destruction, distortion, information leakage, or unauthorized access to network resources are considered. It is shown how SNMP allows detecting abnormal network activity and provides data on the basis of which measures can be taken. SNMP itself “does not fight”, but is a key tool for detection and collection of information necessary for the fight.

Keywords: abnormal traffic; SNMP protocol; information risks; security analysis.

1. Введение

Конгломерат различных компьютерных сетей, систем и их объединения посредством Интернета составляют информационную структура современной компании. Сложность логической и физической организации локальной сети приводит к объективным трудностям при решении вопросов об ее управлении и защиты [1]. Соответственно центральный вопрос –

оперативное обнаружение ее состояния, приводящего к потере полной или частичной ее работоспособности, уничтожению, искажению или утечки информации в результате несанкционированной деятельности хакеров, вирусов и т.д. Раннее обнаружение таких состояний позволит своевременно устранить их причину, а также предотвратить возможные нежелательные последствия. Для диагностики таких состояний применяется значительный спектр специализированных систем [2]: межсетевые экраны, антивирусы, система обнаружения атак (Instrusion Detection System) система контроля целостности, криптографические средства защиты. Однако, указанные системы обнаружения имеют ряд недостатков [3]:

- периодическое применение при наличии признаков вмешательства, так как постоянное их использование приводит к избыточному потреблению ресурсов системы;
- методы анализа специализированных систем направлены на обнаружение известных типов воздействия, но за частую не в состоянии обнаружить их модификации.

Таким образом, в настоящее время является актуальным вопрос поиска более эффективных методов выявления недопустимых аномалий в работе сети, являющихся следствием технических сбоев или несанкционированного воздействия. Основным требованием к этим методам является возможность обнаружения произвольных типов аномалий, в том числе новых, а также воздействий, распределенных во времени. Одним из таких методов, на наш взгляд, является выявление аномальной активности с помощью протокола SNMP.

Целью работы является показать, как SNMP позволяет обнаруживать аномальную сетевую активность и предоставляет данные, на основе которых можно принять меры. SNMP сам по себе «не борется», но является ключевым инструментом для обнаружения и сбора информации, необходимой для борьбы.

2. Проведение атаки и демонстрация

В рамках данного исследования была проведена демонстрация возможностей SNMP для обнаружения аномальной сетевой активности. Была смоделирована типичная ЛВС, включающая сетевые устройства, поддерживающие SNMP, и систему мониторинга, агрегирующую данные, полученные по этому протоколу (рис. 1).

Основные выполненные настройки.

Конфигурация сервера: на сервере под управлением ОС Kali Linux (IP-адрес 192.168.6.164) произведена настройка сетевого интерфейса e0, обеспечивающего его подключение к центральному коммутатору (SW) и

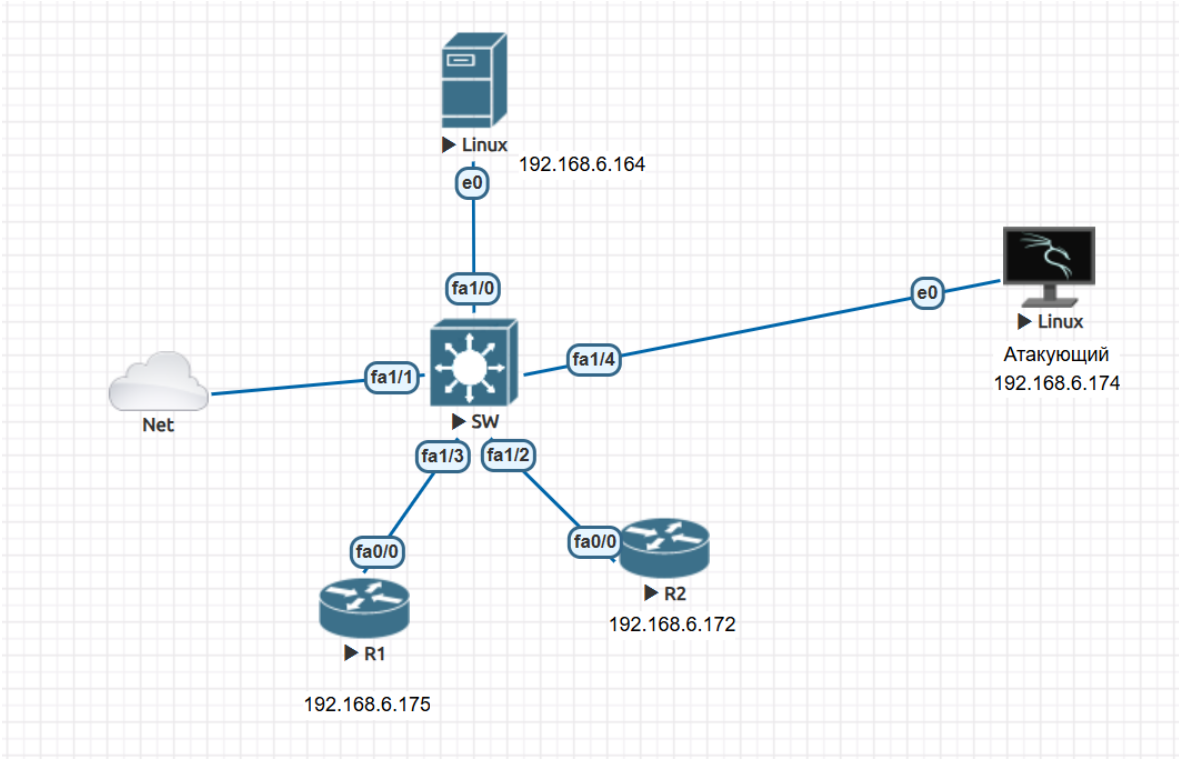

Рис. 1. Локальная сеть

доступность в локальной сети. Ключевым элементом конфигурации сервера стало развертывание системы сетевого мониторинга Observium. Данная система предназначена для автоматического обнаружения сетевых устройств, сбора данных об их состоянии и производительности, а также визуализации полученной информации непосредственно с данного сервера.

Конфигурация атакующего компьютера: компьютер под управлением ОС Kali Linux, обозначенный как «Атакующий» (IP-адрес 192.168.6.174). Для него выполнена базовая настройка сетевого интерфейса e0 для обеспечения взаимодействия в рамках локальной сети. Данный узел используется для осуществления атаки на локальную сеть путём UDP Flood.

Настройка протокола SNMP на маршрутизаторах: на маршрутизаторах R1 (IP-адрес 192.168.6.175) и R2 (IP-адрес 192.168.6.172) была выполнена базовая конфигурация протокола SNMP. Активация SNMP-агентов на данных устройствах позволяет системе Observium осуществлять опрос маршрутизаторов для сбора ключевых метрик, таких как загрузка интерфейсов, состояние устройства, таблицы маршрутизации и другие параметры, необходимые для анализа работы сети.

Таким образом, созданная конфигурация представляет собой функциональный сегмент сети, где ключевые устройства (сервер и

маршрутизаторы) подготовлены для внешнего мониторинга с использованием стандартных протоколов и специализированного программного обеспечения.

Покажем, как Observium фиксирует аномальный рост трафика на интерфейсе одного из роутеров. Будем атаковать R2 (IP: 192.168.6.172) на его интерфейс fa0/0 (рис. 2–3).

На представленных скриншотах из системы Observium для маршрутизатора R2 (с IP-адресом 192.168.6.172) видно, что система мониторинга успешно подключилась к устройству и начала процесс сбора данных.

Текущие графики трафика показывают небольшую сетевую активность на интерфейсе FastEthernet0/0. Эта активность соответствует фоновому обмену данными (например, служебный трафик протоколов маршрутизации, ARP-запросы). Долгосрочные графики пока не информативны, так как сбор данных только начался.

Реализация атаки UDP Flood с компьютера атакующего (IP-адрес 192.168.6.174) на интерфейс FastEthernet0/0 роутера R2 представлена на рис. 4.

С помощью команды sudo hping3 --flood --rand-source -p 80 --udp 192.168.6.172 была инициирована сетевая атака. Программа hping3 используется для отправки специально сформированных сетевых пакетов, а ключ sudo предоставляет ей необходимые права администратора. Опция --flood указывает программе отправлять пакеты максимально быстро, не дожидаясь ответов. Ключ --rand-source заставляет программу

«мирное время»

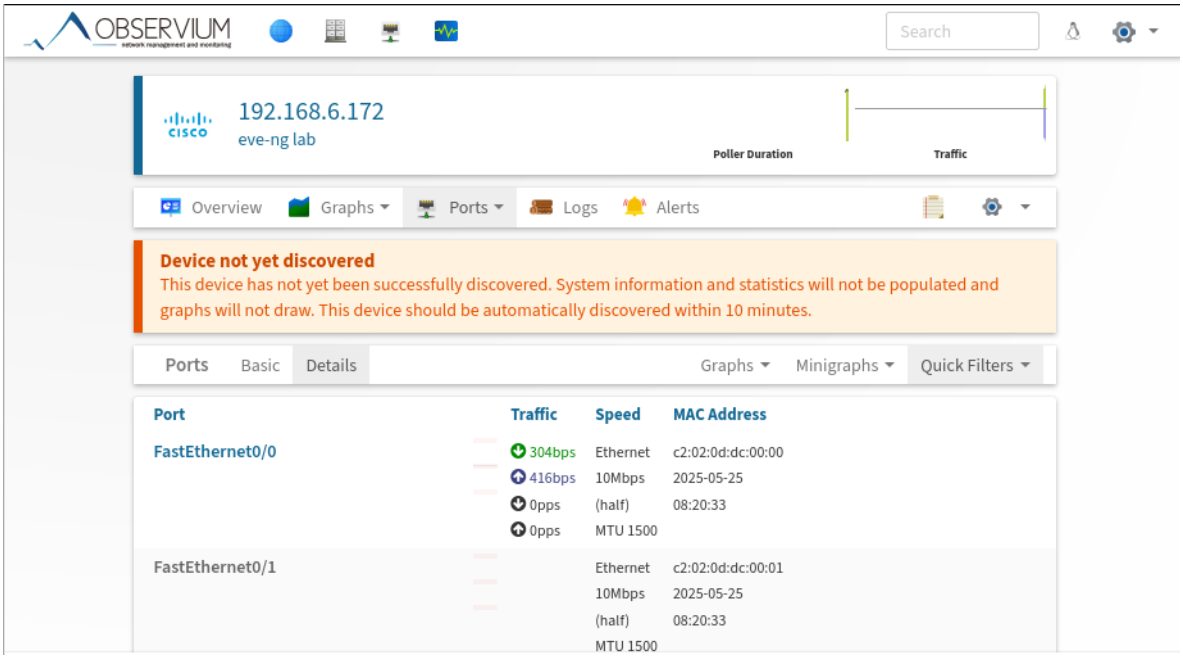

Рис. 2. Общий вид устройства (R2)

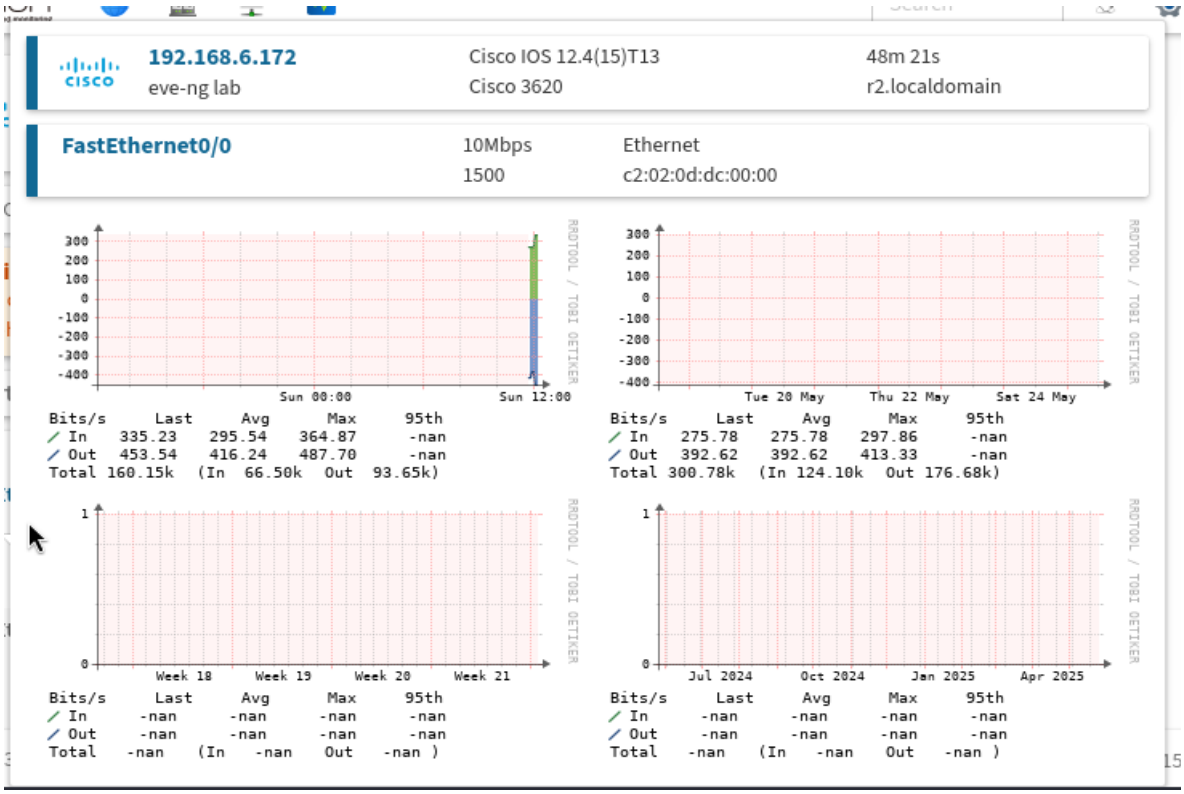

Рис. 3. Детальные графики для порта FastEthernet0/0

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --flood --rand-source -p 80 --udp 192.168.6.172
HPING 192.168.6.172 (eth0 192.168.6.172): udp mode set, 28 headers + 0 data b
ytes
hping in flood mode, no replies will be shown
^C
── 192.168.6.172 hping statistic ──
24443437 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Рис. 4. Окно терминала на атакующем компьютере

использовать случайные (поддельные) IP-адреса отправителя для каждого пакета, что затрудняет идентификацию источника атаки. Параметр -p 80 задает в качестве целевого порта на атакуемом устройстве порт 80, который обычно используется для веб-трафика (HTTP), а --udp определяет, что будут отправляться пакеты протокола UDP. Адрес 192.168.6.172 является IP-адресом цели атаки, в данном случае это маршрутизатор R2.

Таким образом, была проведена атака типа UDP Flood. Суть этой атаки заключается в отправке огромного количества UDP-пакетов на целевое устройство. Поскольку UDP – это протокол без установления соединения, он не требует подтверждения доставки, что позволяет атакующему генерировать очень большой объем трафика с минимальными затратами собственных ресурсов.

Цель атаки – исчерпать пропускную способность сетевого канала к атакуемому устройству или перегрузить его ресурсы (процессор, память) обработкой входящего потока пакетов, что может привести к отказу в обслуживании.

Из вывода команды видно, что было передано более 24 миллионов пакетов, при этом ни одного ответа получено не было, что характерно для данного типа атаки, особенно при использовании опции.

После начала атаки мы сразу замечаем изменения выводимых данных Observium (рис. 5).

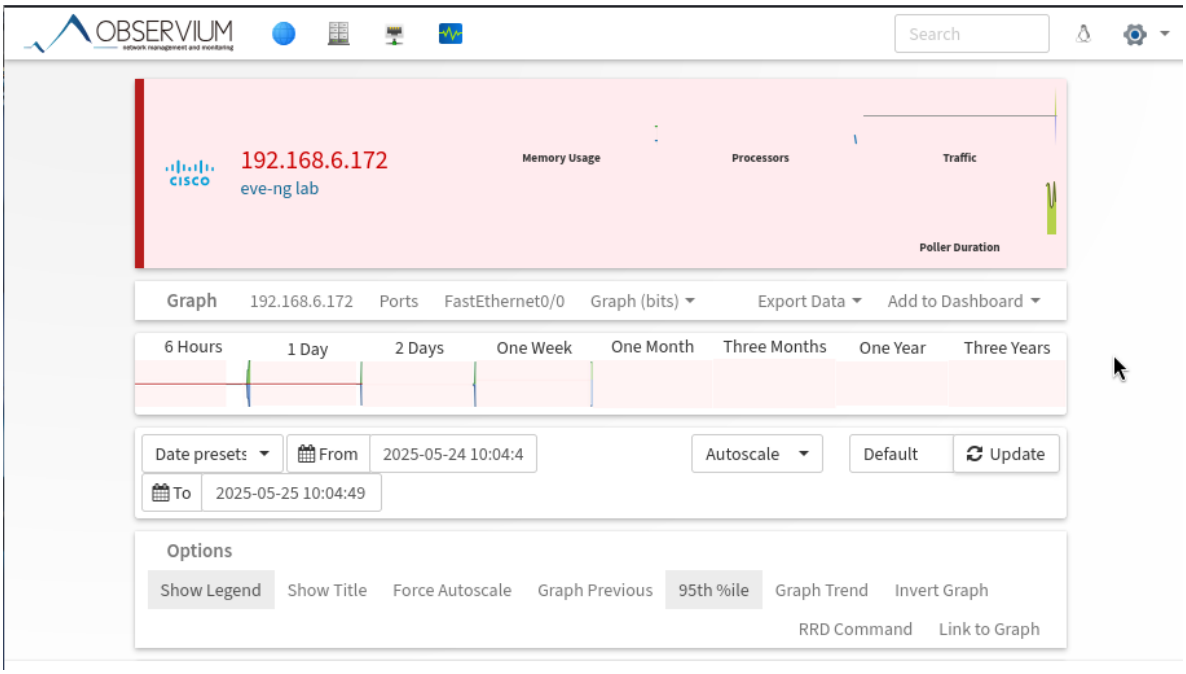

Рис. 5. Общий вид графика трафика и элементы управления

Верхняя часть: мы видим информационную панель для устройства 192.168.6.172. Справа есть мини-графики: Memory Usage (Использование памяти), Processors (Загрузка процессоров) и Traffic (Трафик). На мини-графике Traffic отчетливо виден огромный вертикальный всплеск, указывающий на резкое и значительное увеличение сетевого трафика. Это прямое следствие UDP Flood атаки, когда атакующий компьютер завалил маршрутизатор пакетами.

Главное здесь – подтверждение системой мониторинга факта аномально высокого трафика на атакованное устройство (рис. 6).

Это увеличенный график трафика для интерфейса FastEthernet0/0 роутера R2 за определенный период.

Ключевой момент: Правее отметки “Sun 12:00” (Воскресенье, 12:00) виден резкий, почти вертикальный скачок трафика (зеленая и синяя

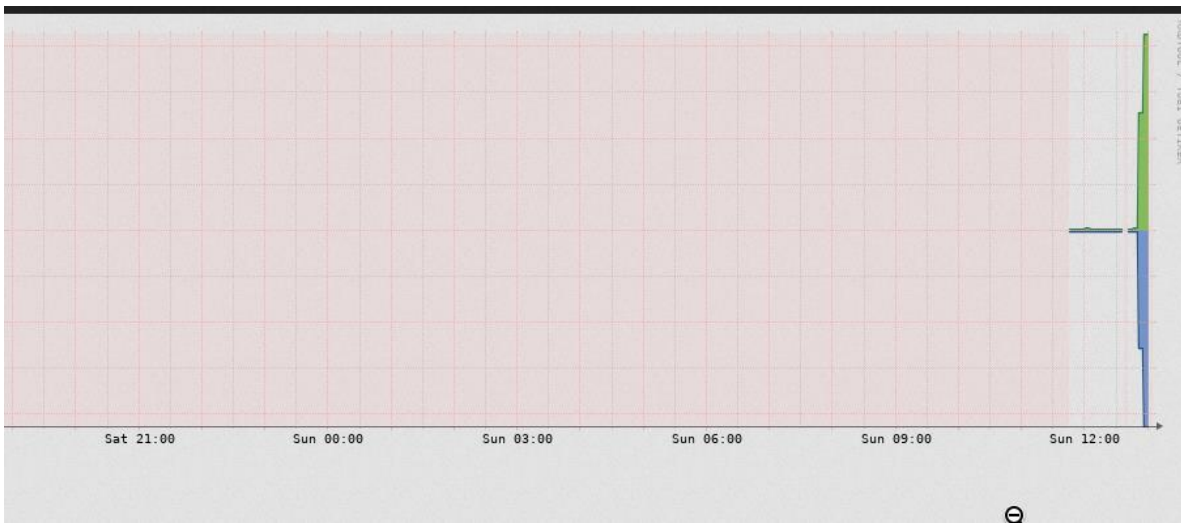

Рис. 6. Детальный график трафика

области). Это и есть визуализация UDP Flood атаки. Зеленая область, входящий трафик, синяя – исходящий. Высота этого пика показывает интенсивность потока данных во время атаки. До и после этого пика трафик был минимальным.

График на рис. 7 наглядно демонстрирует момент начала и окончания атаки, а также ее интенсивность.

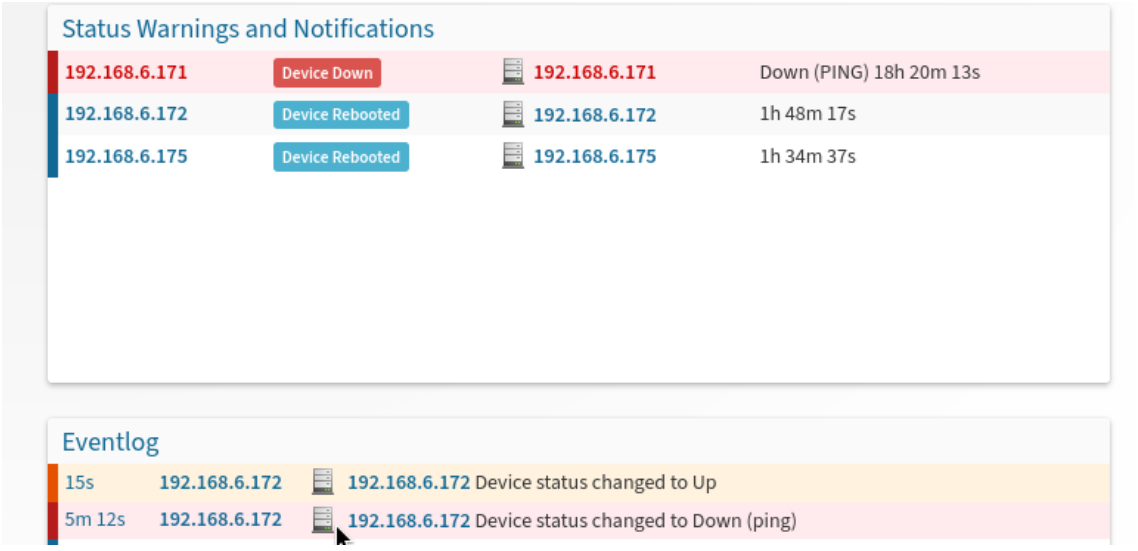

Рис. 7. Status Warnings and Notifications + Eventlog (журнал событий)

Верхний блок "Status Warnings and Notifications" (Предупреждения и Уведомления о состоянии).

192.168.6.172 Device Rebooted 1h 48m 17s: очень важное сообщение! Атакованный маршрутизатор 192.168.6.172 был перезагружен 1 час 48

минут назад. Это следствие успешной атаки. Устройство не справилось с нагрузкой и «пало».

Нижний блок "Eventlog" (продолжение Журнала событий).

15s 192.168.6.172 Device status changed to Up: 15 секунд назад атакованный R2 снова стал доступен (вернулся в состояние "Up") после перезагрузки.

5m 12s 192.168.6.172 Device status changed to Down (ping): это то же событие, что мы видели на предыдущем скриншоте лога – когда R2 «упал» из-за атаки.

Эти логи показывают полный цикл: атака -> устройство недоступно -> устройство перезагружается -> устройство снова доступно. Это классический сценарий последствий атаки UDP Flood.

Ошибки, возникшие после атаки и перезагрузки устройства R2, представлены на рис. 8.

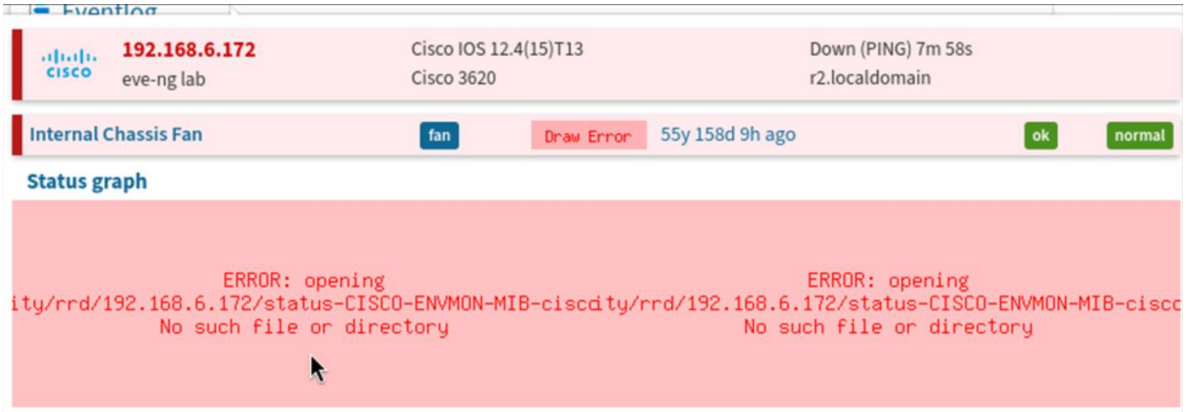

Рис. 8. Страница устройства R2 с ошибками

ERROR: opening /var/lib/observium/rrd/192.168.6.172/status-CISCO-ENVMON-MIB-ciscosity.rrd: No such file or directory. Эти ошибки говорят о том, что Observium не может найти или открыть файлы RRD (Round Robin Database), в которых хранятся исторические данные для некоторых сенсоров (в данном случае, относящихся к CISCO-ENVMON-MIB – MIB для мониторинга окружающей среды Cisco, например, температуры, состояния вентиляторов).

Когда устройство аварийно перезагружается или SNMP-сервис на нем перестает отвечать корректно из-за высокой нагрузки, сбор некоторых данных может прерваться. В результате файлы RRD для этих метрик могут не создаться, повредиться или Observium потеряет к ним доступ на время.

Скриншот на рис. 8 показывает остаточные проблемы после атаки и перезагрузки: Observium не может получить или отобразить некоторые специфические данные мониторинга для R2, вероятно, из-за сбоя в их сборе во время или сразу после инцидента.

3. Общие выводы

Проведенная UDP Flood атака была достаточно мощной, чтобы вызвать значительный всплеск трафика на маршрутизаторе R2 (192.168.6.172). Это привело к тому, что маршрутизатор перестал отвечать (стал “Down”), а затем аварийно перезагрузился. После перезагрузки он снова стал доступен. Система Observium успешно зафиксировала как атаку (всплеск трафика).

Протокол SNMP сыграл ключевую роль в том, что система мониторинга Observium смогла обнаружить, отобразить и зарегистрировать как саму UDP Flood атаку, так и ее последствия для маршрутизатора R2 (192.168.6.172). Вот как это проявилось на каждом этапе.

1. Обнаружение всплеска трафика (см. рис. 5–6).

Именно благодаря SNMP-запросам к маршрутизатору R2 Observium смог получить данные со счетчиков трафика на его интерфейсе FastEthernet0/0. SNMP позволяет системе мониторинга регулярно опрашивать устройство и узнавать, сколько байт/пакетов прошло через каждый порт. Без SNMP Observium не смог бы построить график, наглядно демонстрирующий аномальный скачок трафика во время атаки. Он бы просто не знал, что происходит на сетевом уровне устройства.

2. Определение состояния устройства (см. рис. 7 – “Down”, “Up”, “Rebooted”).

Хотя сообщение “Down (ping)” указывает на отказ ICMP (ping) запросов, SNMP предоставляет гораздо больше информации о состоянии устройства.

До атаки: SNMP позволял Observium регулярно проверять работоспособность SNMP-агента на R2, собирать данные о времени его непрерывной работы (uptime), загрузке процессора, использовании памяти и т.д.

Во время атаки: когда R2 был перегружен, его SNMP-агент, скорее всего, также перестал отвечать или отвечал с огромными задержками. Это является дополнительным сильным индикатором серьезных проблем для Observium.

Обнаружение перезагрузки: изменение значения uptime устройства (которое Observium получает по SNMP) является прямым указанием на то, что устройство было перезагружено. Сообщение “Device Rebooted” генерируется именно на основе этой информации.

Восстановление: когда R2 снова стал доступен (“Device status changed to Up”), Observium смог возобновить успешные SNMP-запросы, подтвердив восстановление работоспособности и начав заново собирать метрики.

3. Сбор детальной информации и ошибки (см. рис. 8 – ошибки ENVMON-MIB).

Сообщения об ошибках ERROR: opening ... status-CISCO-ENVMON-MIB-ciscosity.rrd напрямую связаны с SNMP. CISCO-ENVMON-MIB – это специальный набор объектов (MIB – Management Information Base), который устройства Cisco предоставляют по SNMP для мониторинга параметров окружающей среды (температура, состояние вентиляторов, напряжение и т.д.).

Observium пытался по SNMP запросить эти данные у R2.

Сразу после атаки/перезагрузки SNMP-агент на R2 мог быть недоступен, или конкретно эти данные были недоступны. В результате Observium не смог получить значения, и файлы RRD (где хранятся исторические данные) для этих метрик не были обновлены или созданы корректно, что и вызвало ошибку при попытке их отобразить. Это также свидетельствует о сбое в работе устройства, зафиксированном благодаря попыткам SNMP-опроса.

Таким образом, достоинства SNMP заключается в следующем:

– **предоставление данных для визуализации:** SNMP позволил «увидеть» атаку в виде всплеска трафика на графиках;

– **Диагностика состояния:** SNMP дал Observium возможность отслеживать работоспособность R2, фиксировать его недоступность, перезагрузку и последующее восстановление;

– **детализированный мониторинг:** даже ошибки при сборе специфических данных (как с CISCO-ENVMON-MIB) через SNMP являются важной диагностической информацией, указывающей на проблемы с определенными подсистемами или службами на устройстве.

Без SNMP система Observium была бы значительно «слепее» и не смогла бы предоставить такой подробной картины произошедшего инцидента и его влияния на сетевое оборудование. SNMP – это «глаза и уши» системы мониторинга в сети.

Наше исследование доказывает ценность SNMP как инструмента для постфактум анализа и обнаружения аномалий. Однако истинный потенциал протокола раскрывается, когда он становится частью проактивной системы реагирования. Вместо того чтобы маршрутизатор пассивно «принимал удар» до полного отказа, можно разработать механизмы, где данные SNMP служат триггером для автоматических контрмер. Например, можно было бы сконфигурировать маршрутизатор таким образом, чтобы при достижении критических порогов загрузки интерфейса (значения которых Observium получает по SNMP) не просто регистрировалось событие, а инициировались защитные действия. Это могла бы быть временная блокировка порта, с которого идет аномальный трафик, или применение заранее подготовленных списков контроля доступа (ACL), отсекающих подозрительные пакеты. SNMP в этом сценарии не только сигнализирует

администратору через Observium (например, с помощью SNMP-трапов, отправляемых маршрутизатором немедленно при событии, а не ожидая опроса), но и может служить каналом для получения команды на изменение конфигурации от управляющей системы.

4. Заключение

Таким образом, в данном исследовании была продемонстрирована базовая конфигурация SNMP и её применение для мониторинга самых очевидных метрик, таких как загрузка интерфейса и общее состояние устройства. Современные реализации SNMP (особенно SNMPv3 с его улучшенной безопасностью) и обширные MIB-базы (Management Information Bases), открывают доступ к огромному количеству детализированной информации. SNMP способен предоставлять данные о загрузке каждого процессорного ядра, количестве ошибок на интерфейсах, состоянии таблиц маршрутизации, очередях пакетов, параметрах QoS, специфических для вендора показателях производительности и даже данных о попытках несанкционированного доступа. Это позволяет строить гораздо более сложные и тонкие профили нормального поведения сети и с большей точностью и на более ранних стадиях выявлять аномалии.

Библиографические ссылки

1. *Рябенко Б. Я., Фионов А. Н.* Криптографические методы защиты информации: учеб. пособие. М. : Горячая линия – Телеком, 2013.

2. *Олифер В., Олифер Н.* Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. Учебник для ВУЗов. 6-е изд. СПб. : Питер, 2020.

3. *Костенко Е. Ю., Дуйсенгалиев Р. Р., Барабанова Е. А.* Система мониторинга для контроля трафика технологических сетей передачи данных // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. 2015. № 4. С. 101–109. URL: https://cyberleninka.ru/article/n/sistema-monitoringa-dlya-kontrolya-trafika-tehnologicheskih-setey-peredachi-dannyh (дата обращения: 02.10.2025).