УДК 004.056
DOI: 10.31673/2409-7292.2021.014757

Касовська І.В., Шаповаленко О.Д., Луценко І.М.

ПРОГРАМНІ КОМПЛЕКСИ МЕРЕЖЕВОГО МОНІТОРИНГУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ МЕРЕЖ

В роботі приведено основні методи та протоколи мережевого моніторингу. Проведений загальний огляд властивостей програмних комплексів мережевого моніторингу. Досліджені наявні у відкритому доступу програмні комплекси моніторингу мережевої безпеки та обґрунтувати вибір інструменту для подальшого дослідження. Розроблені рекомендації щодо заходів забезпечення мережевої безпеки.

Ключові слова: моніторинг мережевої безпеки, NSM, Zabbix, Wireshark, Security Onion, межеві атаки

Вступ

Сучасні комп'ютерні системи побудовані за допомогою мережі Internet, або інтегровані в локальну мережу з подальшим доступом в Internet. З огляду на сучасний стан інформаційних і комунікаційних технологій, виникає проблема моніторингу в комп'ютерних мережах. Бажано створювати програми моніторингу мережі, щоб забезпечити доступ до інформації мережевого контенгенту, топології, обладнання для спеціалістів та користувачів.

Мережевий моніторинг - це система, яка відстежує вашу внутрішню IT-інфраструктуру на предмет потенційних проблем. Система здатна виявляти велику кількість конкретних проблем, які можуть вплинути на загальну продуктивність вашої мережевої інфраструктури. При виявленні будь-яких проблем система мережевого моніторингу повідомить системного адміністратора або організацію IT-обслуговування, а також надасть розширені інструменти для усунення проблем, перш ніж вони стануть серйозною проблемою.

Метою даної статті є дослідити методи мережевого моніторингу та можливості програмних комплексів мережевого моніторингу для підвищення ефективності захисту мереж.

Методи моніторингу, засновані на маршрутизації.

Методи моніторингу засновані на маршрутизаторах - вшиті в роутери і, отже, мають низьку гнучкість. На відміну від оперативного моніторингу мережі, моніторинг мережевої безпеки і аналітики, які його використовують, повинні вміти виявляти вторгнення і всі форми атак, включаючи нові (нульові атаки) і складні загрози, щоб приймати управлінські рішення, засновані на доказах.

Жоден фахівець з безпеки не може гарантувати 100% захист від атак, але технології безперервного моніторингу і аналізу мережі надають можливості, які можуть значно знизити наслідки атаки або злому.

Моніторинг мережної безпеки включає в себе 3 основних завдання, а саме: збір мережних даних; виявлення мережних даних; аналіз мережних даних, пов`язаних з безпекою.

Протокол простого мережевого моніторингу (SNMP). SNMP (Simple Network Management Protocol) – це протокол прикладного рівня, який є частиною протоколу TCP/IP. Він дозволяє адміністраторам управляти продуктивністю мережі, знаходити і усувати проблеми і планувати зростання мережі. Він збирає статистику за трафіком до кінцевого хоста через пасивні датчики, вбудовані в маршрутизатор.

SNMP складається з трьох ключових компонентів (рис. 1.): керовані пристрої (Managed Devices); агенти (Agents); системи управління мережею (Network Management Systems – NMSs).

Керовані пристрої включають в себе SNMP-агента і можуть складатися з маршрутизаторів, комутаторів, концентраторів, персональних комп'ютерів, принтерів тощо. Вони несуть відповідальність за збір інформації та надання її системі управління мережею (NMS). Агенти включають програмне забезпечення, яке має керуючу інформацію, і переводять цю інформацію в форму, сумісну з SNMP. Вони закриті для керуючого пристрою. Системи управління мережею (NMS) виконують додатки, які відстежують і контролюють пристрої управління. Ресурси ЦП і пам'яті, необхідні для управління мережею,

© *І.В. Касовська, О.Д. Шаповаленко, І.М. Луценко, 2021*

надаються NMS. Для будь-якої керованої мережі повинна бути створена хоча б одна система управління. SNMP може діяти виключно як NMS.

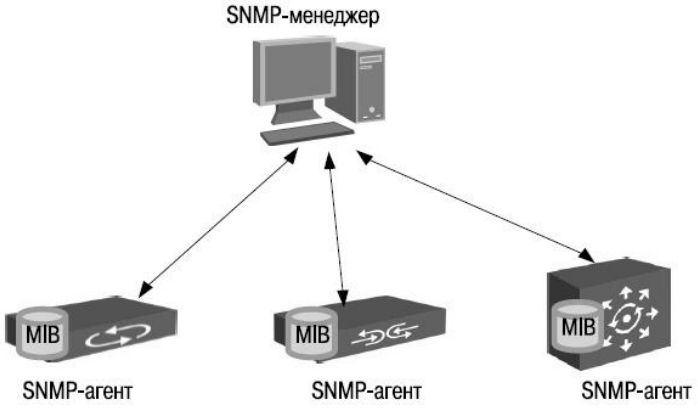

Рис. 1. Компоненти SNMP

Віддалений моніторинг (RMON). RMON включає в себе різні мережеві монітори і консольні системи для зміни даних, отриманих під час моніторингу мережі. Це розширення для бази даних керуючої інформації SNMP. На відміну від SNMP, якому потрібно посилати запити для відправки інформаційних, RMON може налаштовувати сигнали, які будуть «контролювати» мережу на основі певного критерію. RMON дає адміністраторам можливість управляти локальними мережами віддалено з одного певного місця / точки.

Компоненти RMON – це датчик, також відомий як агент або монітор, і клієнт, також відомий як станція управління. На відміну від SNMP, датчик або агент RMON збирає і зберігає мережеву інформацію. Клієнт зазвичай являє собою контрольну станцію, підключену до датчика, який використовує SNMP для прийому і виправлення даних RMON.

Потоковий метод Netflow. Netflow – це розширення, представлене в маршрутизаторах Cisco, яке забезпечує можливість збору мережевого IP-трафіку, якщо це зазначено в інтерфейсі. Аналізуючи дані, надані Netflow, мережевий адміністратор може визначити такі речі, як: джерело і одержувач трафіку, клас обслуговування, причини перевантаження. Netflow включає 3 компоненти:

а) FlowCaching (кешування потоку);
б) FlowCollector (збирач інформації про потоки);
в) Data Analyzer (аналізатор даних).

На рис. 2. показана інфраструктура Netflow.

FlowCaching аналізує і збирає дані про IP-потоки, які входять в інтерфейс, і перетворює дані для експорту.

Безмаршрутизаторні методи моніторингу.

Активний моніторинг. Активний моніторинг повідомляє про мережеві проблеми, збираючи вимірювання між двома кінцевими точками. Активна система вимірювання має справу з такими показниками, як: маршрутизатори / маршрути, затримка пакетів, повторення пакетів, втрата пакетів, нестабільна синхронізація між надходженнями, вимір смуги пропускання.

Основне використання інструментів, таких як команда ping, яка вимірює затримку і втрату пакетів, і traceroute, яка допомагає визначити топологію мережі, є прикладами основних активних інструментів вимірювання. Обидва цих інструменту відправляють пробні пакети ICMP в пункт призначення і чекають, поки ця точка не відповість відправнику. На рис. 3. показаний приклад команди ping, яка використовує активний метод вимірювання для

© *І.В. Касовська, О.Д. Шаповаленко, І.М. Луценко, 2021*

відправки Echo-запиту від джерела по мережі в задану точку. Потім одержувач відправляє Echo-запит назад до джерела, з якого він прийшов.

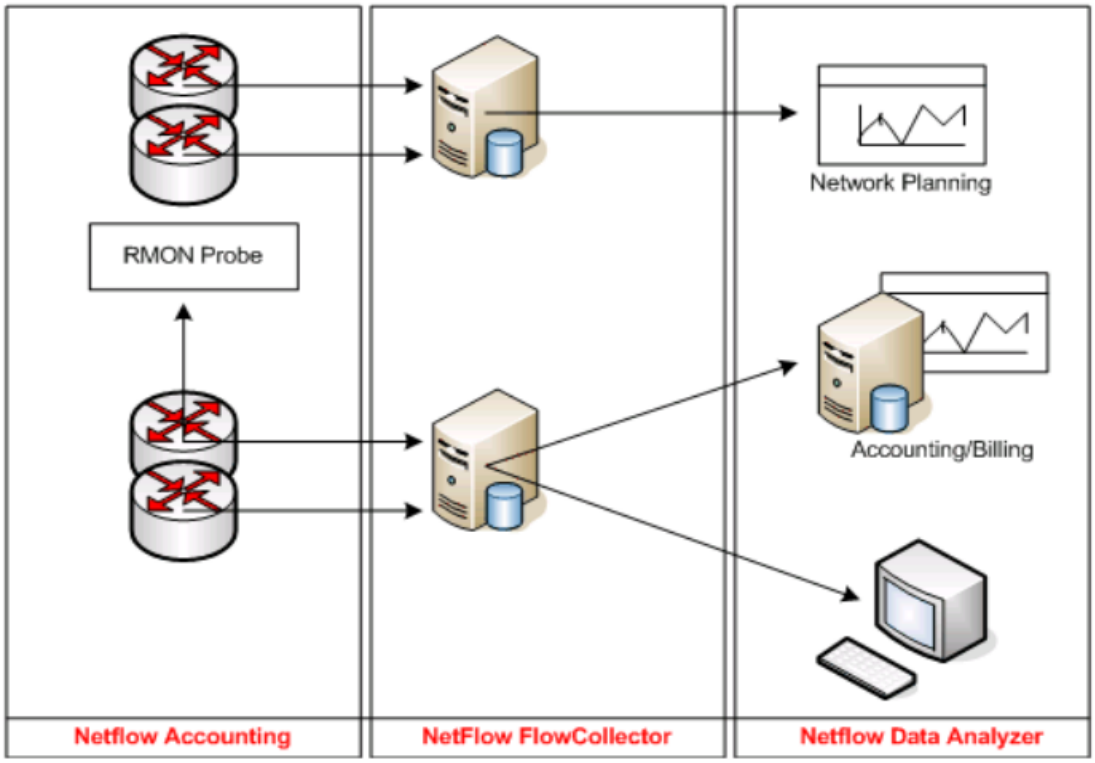

Рис. 2. Інфраструктура NetFlow

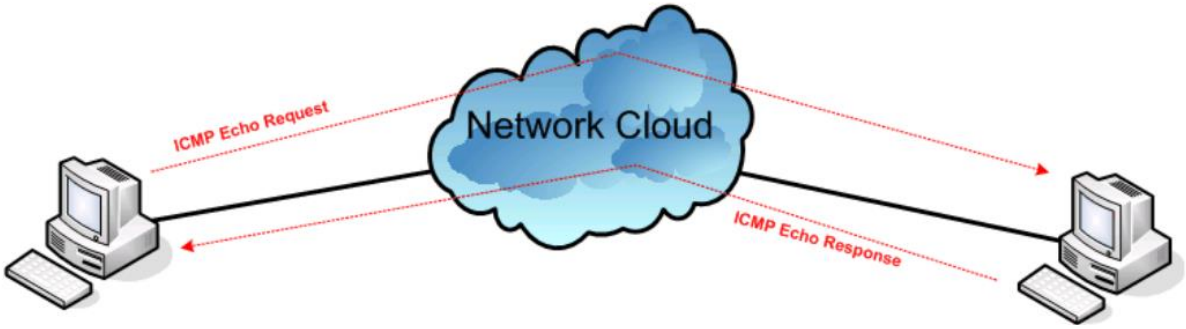

Рис. 3. Команда ping (Активний вимір)

Пасивний моніторинг. Пасивний моніторинг, на відміну від активного, не додає трафіку в мережу і не змінює трафік, який вже існує в мережі. Також, на відміну від активного моніторингу, пасивний моніторинг збирає інформацію тільки про одну точку в мережі. Вимірювання набагато краще, ніж між двома точками, при активному моніторингу. На рис. 4. показана установка системи пасивного моніторингу, в якій монітор розміщується на одному каналі між двома кінцевими точками і відстежує трафік в міру його проходження через канал.

Пасивні вимірювання мають справу з такою інформацією, як: трафік і суміш протоколів, кількість біт (швидкість), синхронізація пакетів і час між прибуттям. Пасивний моніторинг може виконуватися за допомогою будь-якої програми, яка отримує пакети. При пасивному моніторингу вимірювання можна аналізувати тільки в автономному режимі, і вони не являють собою сукупність. Це створює проблему з обробкою великих наборів даних, які збираються під час вимірювання.

© *І.В. Касовська, О.Д. Шаповаленко, І.М. Луценко, 2021*

Рис. 4. Установка пасивного моніторингу

Комбінований моніторинг.

Перегляд ресурсів на кінцях мережі (WREN). WREN використовує комбінацію активних і пасивних методів моніторингу, активно обробляючи дані при низькому трафіку і пасивно обробляючи дані під час інтенсивного трафіку. Він відстежує трафік як від джерела, так і від приймача, що робить можливими більш точні вимірювання. WREN використовує трасування пакетів з трафіку, створюваного додатками, для вимірювання корисної пропускної здатності. WREN розділений на два рівня: базовий рівень швидкої обробки пакетів і аналізатор трасування призначеного для рівня користувача.

Монітор з власною конфігурацією (SCNM). SCNM - це інструмент моніторингу, який використовує комбінацію пасивних і активних вимірювань для збору інформації на трьох рівнях проникнення вихідних маршрутизаторів і інших важливих точок моніторингу мережі. Середа SCNM включає як апаратні, так і програмні компоненти. Устаткування встановлюється в критичних точках мережі. Він відповідає за пасивний збір заголовків пакетів. Програмне забезпечення працює в кінцевій точці мережі.

Програмні комплекси мережевого моніторингу.

Універсальна система моніторингу Zabbix. Zabbix - це інструмент моніторингу серверів з відкритим вихідним кодом, який використовується для моніторингу різних IT-компонентів, таких як сервери, мережі, обладнання, програмне забезпечення, віртуальні машини, хмарні сервіси і багато іншого. Він надає показники моніторингу продуктивності, що стосуються використання дискового простору, використання мережі та завантаження ЦП. Zabbix можна розгорнути для агентів і безагентного моніторингу. Він може відстежувати операції в операційних системах, таких як Hewlett Packard Unix (HP-UX), Linux, Mac OS X і Solaris, без будь-яких агентів. Дані зберігаються на платформах баз даних, таких як MySQL, Oracle, PostgreSQL і SQLite. Зібрана інформація включається в звіти або представляється візуально за допомогою графічного інтерфейсу користувача (GUI) Zabbix. Користувачі можуть переглядати ці докладні звіти у вигляді віджетів, мережевих карт, графіків, слайд-шоу через настроювані інформаційні панелі. Шаблони складаються із спеціально створених надбудов для розширення функціональних можливостей Zabbix. Ці шаблони дозволяють користувачам відстежувати мережеві пристрої від таких постачальників, як Cisco, Juniper, HP і Dell.

Інструмент для моніторингу мережі Wireshark. Wireshark - це популярний інструмент з відкритим вихідним кодом для захоплення мережевих пакетів і їх перетворення в легкий для читання двійковий формат. Він надає кожну деталь мережевої інфраструктури організації. Він складається з пристроїв, призначених для вимірювання входів і виходів мережі. Інформація, зібрана за допомогою Wireshark, може використовуватися для різних цілей, таких як аналіз мережі в режимі реального часу або в автономному режимі, ідентифікація трафіку, що надходить в мережу, його частоту і затримку між конкретними переходами. Це допомагає адміністраторам мережі генерувати статистику на основі даних в реальному часі.

Крім моніторингу мережі, організації використовують Wireshark для налагодження програм, вивчення проблем безпеки і вивчення внутрішніх компонентів мережевих протоколів. Після збору мережевих даних список мережевих пакетів відображається на

© *І.В. Касовська, О.Д. Шаповаленко, І.М. Луценко, 2021*

консолі централізованого управління або приладової панелі. Екран складається з трьох панелей: список пакетів, байти пакета і відомості про пакет.

Монітор продуктивності мережі SolarWinds. Монітор продуктивності мережі SolarWinds (NPM) - це потужне програмне забезпечення для моніторингу мережі, що використовується для виявлення, діагностики та усунення мережевих проблем і збоїв. Інструмент спеціально розроблений для розширеного усунення неполадок в мережі для локальних, гібридних і хмарних сервісів і виявляє проблеми за допомогою поетапного аналізу. Це не тільки допомагає масштабувати мережу, але і забезпечити безпеку.

SolarWinds Response Time Viewer для Wireshark дозволяє користувачам виявляти і аналізувати перехоплення пакетів Wireshark і усувати неполадки в роботі мережі в режимі реального часу. Він може виконувати кілька завдань, таких як ідентифікація більше 1200 додатків, обчислення часу відгуку їх мережі, відображення даних і вартості транзакції, візуалізація критичного шляху за допомогою Netpath, а також моніторинг і управління бездротовою мережею. Оцінка цих параметрів допомагає визначати недоліки і збої в мережі.

Система моніторингу мережевої безпеки Security Onion. Security Onion - комплект інструментів моніторингу безпеки мережі (NSM) з відкритим вихідним кодом, який працює в ОС Ubuntu Linux. Набір Security Onion можна встановити як окрему систему або як платформу типу «датчик і сервер». Деякі компоненти рішення Security Onion є власністю корпорацій, таких як Cisco і Riverbend Technologies, і керуються ними, але їх вихідний код зроблений відкритим.

Рекомендації щодо захисту мереж.

Фахівці в області кібербезпеки знають, що хакери безперервно розробляють нові методи. Постійно з'являються нові загрози, які необхідно виявляти і стримувати з тим, щоб ресурси і зв'язок відновлювалися якомога швидше. Для отримання прибутку багато хакерів використовують такі методи, як вимагання, шахрайство і крадіжка персональних даних. Необхідність постійно захищатися від цих атак привела до створення декількох моделей реагування на інциденти.

Профілювання мережі. Для виявлення серйозних подій безпеки важливо розуміти, кваліфікувати і аналізувати дані про нормальне функціонування мережі. Всі мережі, сервери і хости в кожен даний момент часу поводяться стандартним чином. Профілювання мережі і пристроїв дозволяє сформувати базові показники, які послужать контрольною точкою. Незрозумілі відхилення від базової поведінки можуть вказувати на проникнення. Підвищена інтенсивність використання з'єднань WAN в незвичайний час може вказувати на порушення безпеки мережі і витік даних. Відхилення в поведінці мережі складно виявити, якщо не визначено нормальна поведінка. Такі інструменти, як NetFlow, Wireshark, Zabbix і Security Onion можна використовувати для опису нормальних характеристик мережевого трафіку. Оскільки у організацій вимоги до своїх мереж можуть відрізнятися в залежності від часу доби або дня в році, збір базових показників мережі необхідно виконувати протягом тривалого періоду часу.

Профілювання сервера. Профілювання сервера за допомогою програмних рішень Zabbix та Security Onion використовується для визначення прийнятого робочого стану серверів. Профіль сервера являє собою базові показники безпеки для даного сервера. Він визначає параметри мережі, користувачів і додатків, прийняті для конкретного сервера.

Корпоративне управління виправленнями. Управління виправленнями пов'язано з управлінням уразливостями. Уразливості часто виникають в операційних системах і програмному забезпеченні критично важливих клієнтських, серверних і мережевих пристроїв. У прикладному програмному забезпеченні, особливо в інтернет-додатках і архітектурі, таких як Acrobat, Flash і Java, також часто виявляються вразливості. Управління виправленнями включає всі аспекти патчінга програмного забезпечення, в тому числі визначення необхідних виправлень, отримання, поширення, установку і перевірку установки виправлень на всі необхідні системи. Установка виправлень часто є найбільш ефективним

© І.В. Касовська, О.Д. Шаповаленко, І.М. Луценко, 2021

методом зведення до мінімуму вразливостей програмного забезпечення. А в деяких випадках це і єдиний спосіб.

Повне перехоплення пакетів. Повне перехоплення пакетів є найбільш докладне з зібраних даних про мережу. Через великий обсяг відомостей це також самий ресурсномісткий тип даних, використовуваний в NSM. Повний перехоплення пакетів містить не тільки дані про мережеві сеанси зв'язку, наприклад дані сеансів. У нього також входить фактичний вміст сеансів зв'язку. Повне перехоплення пакетів містить текст електронних повідомлень, HTML-коди веб-сторінок і файли, що надійшли в мережу або відправлені з неї. Витягнутий вміст можна відновити з повного перехоплення пакетів і проаналізувати на наявність шкідливого ПЗ або моделі поведінки користувача, що порушує бізнес-політики і політики безпеки. Відомий інструмент Wireshark широко використовується для перегляда повного перехоплення пакетів і доступу до даних, що належать до мережевих сеансами зв'язку.

Висновки.

Будь-яка корпоративна комп'ютерна мережа, навіть невелика, вимагає постійної уваги. Як би добре вона не була налаштована, як би надійно не було встановлено програмне забезпечення на серверах і клієнтських комп'ютерах - неможливо повністю виключити можливість виходу з ладу або некоректної роботи обладнання, рішення - виявити проблеми на самих ранніх етапах і отримати максимально докладну інформацію про них. Для цього, як правило, використовується різне програмне забезпечення для моніторингу та управління мережею, яке здатне своєчасно повідомляти технічних фахівців про виявлену проблему, а також накопичувати статистику по стабільності і іншим параметрам серверів, сервісів і служб, доступних для детального аналізу.

Перелік посилань.

1. Bejtlich R. The Practice of Network Security Monitoring. Michigan: No Starch Press, 2013. 465 с.
2. Sanders C., Smith J. Applied Network Security Monitoring. USA: Elsevier, 2014. 672 с.
3. Olups R. Zabbix Network Monitoring Second Edition. UK: Packt Publishing Ltd., 2016. 765 с.
4. Далле А. Zabbix. Практическое руководство. Москва: ДМК Пресс, 2017. 356 с.
5. Seagren E., Noonan W. Secure Your Network for Free. MA: Syngress Publishing, Inc., 2007. 536 с.
6. Knapp E. Industrial Network Security. USA: Syngress is an imprint of Elsevier, 2011. 405 с.
7. Lockhart A. Network Security Hacks. USA: O'Reilly Media, Inc, 2007. 508 с.
8. Bullock J., Parker J. Wireshark for Security Professionals. Canada: Indianapolis, 2017. 447 с.
9. Волков И. Разработка рекомендаций по повышению эффективности защиты информации в корпоративной сети передачи данных: дис. ... канд. экон. наук. Москва, 2016. 177 с.
10. Методы мониторинга и обеспечения безопасности для поддержания работоспособности корпоративной сети [Електронний ресурс] – Режим доступу до ресурса: https://www.securitylab.ru/analytics/301808.php
11. A Summary of Network Traffic Monitoring and Analysis Techniques [Електронний ресурс] – Режим доступу до ресурса: https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index.html
12. How to Use Wireshark for Network Monitoring? [Електронний ресурс] – Режим доступу до ресурса: https://www.tek-tools.com/network/how-to-use-wireshark
13. A Comprehensive Guide to Network Monitoring Tools [Електронний ресурс] – Режим доступу до ресурса: https://www.tek-tools.com/network/best-network-monitoring-tools
14. IntroductionToSecurityOnion Tools [Електронний ресурс] – Режим доступу до ресурса: https://github.com/Security-Onion-Solutions/security-onion/wiki/IntroductionToSecurityOnion
15. Cisco Networking Academy CCNA Cybersecurity Operations

Надійшла: 18.02.2021 Рецензент: д.т.н., с.н.с. Лаптєв О.А.

© *І.В. Касовська, О.Д. Шаповаленко, І.М. Луценко, 2021*