УДК 621.396 **doi: 10.26906/SUNZ.2022.1.098**

А. С. Янко, А. М. Мартиненко, В. В. Трикоз

Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Украина

МЕРЕЖНІ СЕНСОРИ ТА ДЕТЕКТОРИ ЯК ЕФЕКТИВНИЙ ІНСТРУМЕНТ МОНІТОРИНГУ ДАНИХ

Анотація. Дана стаття присвячена збору даних та аналізу мережі з метою розуміння принципів їх використання та запобігання хакерських зловмисних дій. Особлива увага приділяється аналізу – процес збору даних про безпеку та вжиття рішучих заходів на їх основі. В даній статті було сконцентровано увагу на механізмах виявлення вторгнень за рахунок використання мережних сенсорів та детекторів. У результаті були сформовані рекомендації щодо забезпечення ефективної інформаційної безпеки сучасної комп'ютерної мережі на основі застосування мережних сенсорів та детекторів. Також розглядалися заходи інформаційної безпеки для запобігання подальшим зловмисним діям.

Ключові слова: інформаційна безпека, комп'ютерна мережа, мережний детектор, мережний сенсор, політика безпеки, система виявлень вторгнень, сканування даних.

Вступ

Ефективний аналіз безпеки вимагає збору даних з безлічі різних джерел, кожен із яких лише частково відбиває стан справ у мережі. Найскладніше завдання у проведенні аналізу з урахуванням даних – це збір достатньої кількості даних відтворення рідкісних подій. Достатнього, але не надлишкового, інакше буде неможливо виконати пошуковий запит. Збір даних напрочуд простий, але осмислення отриманих даних набагато складніше. У безпеці ця проблема ускладнюється рідкісним виникненням реальних загроз. Більшість мережного трафіку не несе жодної загрози і часто повторюється: масове розсилання листів або одночасний перегляд відео на YouTube великою кількістю користувачів, доступ до файлів. Багато з невеликої кількості фактичних атак будуть дійсно невинними, наприклад сліпе сканування порожніх IP-адрес

Ефективний моніторинг інформації будується на даних, зібраних з численних сенсорів, які генерують різні види даних та створюються різними людьми для різних цілей. Сенсором може бути все, що завгодно, від мережного відведення до журналу файрвола – тим, що здійснює збір інформації про вашу мережу та може бути використане для оцінки інформаційної безпеки. Побудова ефективної системи сенсорів вимагає досягнення балансу між її укомплектованістю та надмірністю. Ідеальна система сенсорів укомплектована, але не надмірна. Під укомплектованістю розуміється те, що кожна подія ретельно описана, а під відсутністю надмірності – те, що сенсори не дублюють інформацію про події. Ці, можливо, недосяжні цілі є ідеальною моделлю для побудови рішення щодо моніторингу [1, 2].

Процес аналізу даних, описаний у цій роботі, спрямовано розвиток знань у сфері безпеки з метою прийняття ефективних рішень у цій сфері. Це можуть бути експертні рішення: реконструкція подій постфактум з метою визначити, чому відбулася атака і що сприяло її здійсненню, або оцінити завдану шкоду. Також можна вдатися до профілактичних заходів: встановлення обмежувачів швидкості передачі, встановлення систем виявлення вторгнень або розробка стратегій, які можуть обмежити вплив хакера на мережу.

Аналіз останніх досліджень і публікацій. Першим поштовхом для розвитку мережних сенсорів став розвиток бездротових сенсорних мереж. Наприклад, у 1970-1980 роках у американських військово-технічних системах розпочали використовувати прототипи сучасних мережних сенсорів у системі SOSUS – SOund SUrveillance System. Ця глобальна система звукового спостереження призначається для виявлення та ідентифікації радянських підводних човнів і передачі стану спостережень в центр обробки інформації по радіоканалам. Своєрідним рубежем в історії створення бездротових сенсорних мереж та мережних сенсорів та детекторів став 2003 рік, коли була опублікована перша версія стандарту IEEE 802.15.4 [3-5].

У даний час проблема інформаційної безпеки мереж є досить важливою та актуальною, це питання обговорюється на різноманітних конференціях та самітах, друкуються різні цікаві матеріали в даній області. Michael Collins у своїй книзі під назвою «Network Security Through Data Analysis: From Data to Action» значну увагу звернув на введення в загальний процес розпізнавання даних мережними сенсорами, а також ввів терміни для опису взаємодії сенсорів між собою. Наведені сучасні сенсори, такі як *tcpdump* та NetFlow, які здійснюють збір даних із мережних інтерфейсів. Значну увагу присвячено хост-сенсорам і сервісним сенсорам, які здійснюють збір даних про різні процеси, що відбуваються, наприклад, в серверах та операційних системах.

Метою статті є підвищення інформаційної безпеки комп'ютерних мереж підприємств на основі мережних сенсорів та детекторів, а також розгляду процесу розпізнавання даних мережними сенсорами та їх збору, як ефективного інструменту системи виявлень вторгнень.

Виклад основного матеріалу

Мережний детектор збирає дані безпосередньо з мережного трафіку без допомоги посередницького

додатка, що і відрізняє його від хост-сенсорів. Прикладом можна навести NetFlow сенсори на роутері та сенсори, які використовують для збору даних трафіку такі інструменти моніторингу, як *tcpdump*.

При роботі з мережним трафіком ми стикаємося з проблемою, аналогічною тій, що виникає при роботі з усіма даними журналів: фактичні події безпеки відбуваються рідко, тоді як робота з даними вимагає часу та місця для зберігання. Перевага надається, по можливості, даними журналів, оскільки вони достовірні (у даних журналу фіксуються події високого рівня) і компактні. Те саме явище в мережному трафіку довелося б витягувати з безлічі пакетів, які часто дублюються, зашифровані або просто незчитувані. У той же час зловмиснику не важко маніпулювати мережним трафіком і запускати в мережі нешкідливі на перший погляд, але досить шкідливі сесії. Подія, що відображається в 300-байтному журналі, може запросто являти собою мегабайти пакетних даних, з яких лише перші 10 пакетів мають аналітичну цінність [6, 7].

Жоден із сенсорів не може виконувати всі функції поодинці. Мережні сенсори дійсно виконують багато роботи, але їх легко спантеличити в процесі управління потоками трафіку, вони неефективні щодо зашифрованого трафіку і можуть лише припустити наявність активності в хості. Хост-сенсори надають більш вичерпну та точну інформацію щодо явлень, для опису яких вони мають достатній інструментарій. З метою ефективного комбінування сенсорів їх класифікую у трьох площинах:

Область огляду (Vantage). Розташування сенсорів усередині мережі. Сенсори, розташовані у різних точках, бачитимуть різні сторони однієї події.

Рівень (Domain). Інформація, що надається сенсором, незалежно від місцезнаходження (хост, сервіс хоста чи мережу). Сенсори з однаковою областю огляду, але різного рівня доповнюють один одного в процесі надання даних про одну і ту саму подію. Інформацію про деякі події можна отримати лише на одному з рівнів. Наприклад, моніторинг хоста – це єдиний спосіб визначити, чи мав місце фізичний доступ до цього хоста.

Дія сенсора (Action). Як сенсор ухвалює рішення про створення інформаційного звіту. Він може просто записувати дані, надавати інформацію про події або обробляти трафік, який надає дані. Сенсори різної дії можуть потенційно заважати роботі один одного [1].

Область огляду сенсора дає уявлення, які пакети сенсор зможе вивчати. Область огляду визначається взаємозалежністю між розташуванням сенсора та інфраструктурою маршрутизації мережі. Щоб зрозуміти, як процеси впливають на область огляду, погляньте на рис. 1. На цьому рисунку показані унікальні потенційні сенсори, позначені великими літерами.

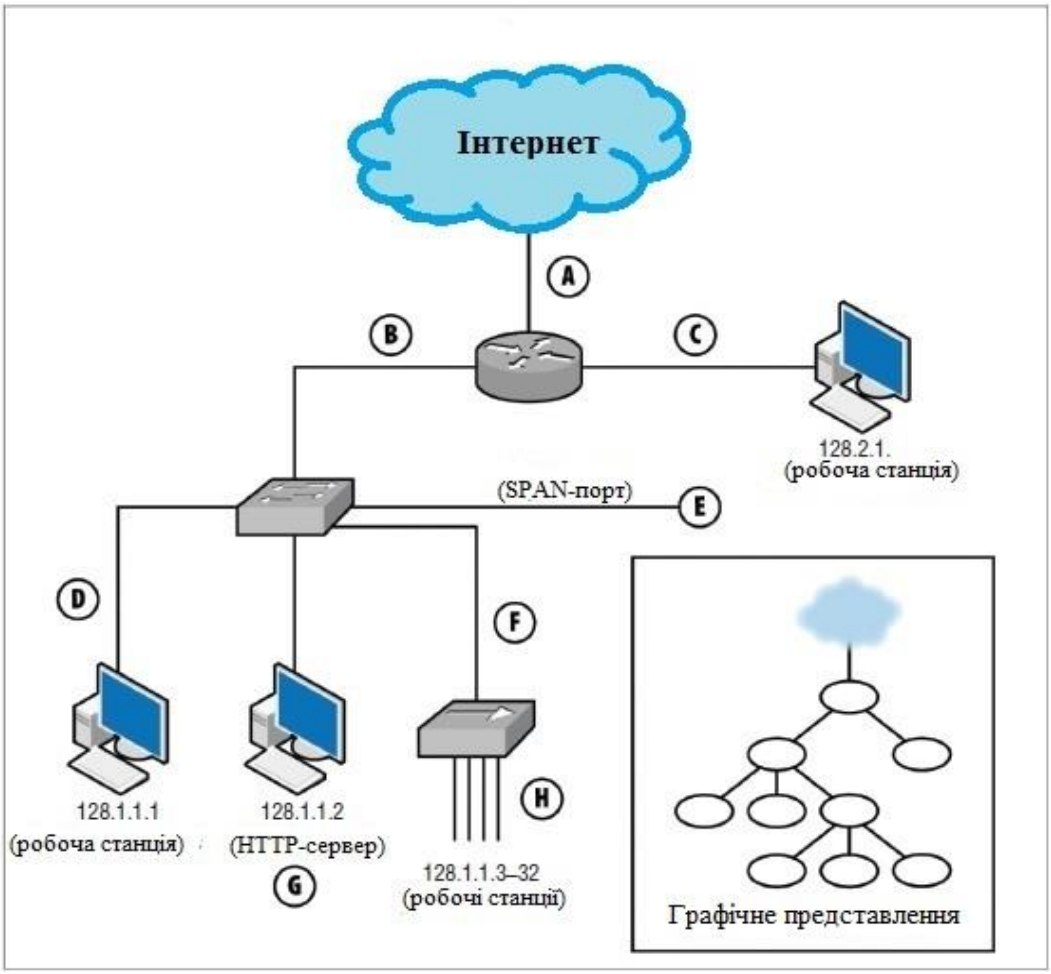

Рис. 1. Позиціонування сенсорів у простій мережі та графічне подання

У порядку черговості ці сенсори мають таке розташування:

A – перевіряє інтерфейс, що з'єднує роутер із Інтернетом;

B – перевіряє інтерфейс, що з'єднує роутер із мережним комутатором;

C – перевіряє інтерфейс, що з'єднує роутер і хост з IP-адресою 128.2.1.1;

D – перевіряє хост із адресою 128.1.1.1;

E – перевіряє SPAN-порт мережного комутатора (цей порт записує весь трафік, що проходить через комутатор);

F – перевіряє інтерфейс, що з'єднує мережний комутатор та мережний концентратор (хаб);

G – здійснює збір даних журналу HTTP у хості з адресою 128.1.1.2;

H – аналізує весь трафік протоколу TCP у мережному концентраторі.

Кожен із цих сенсорів має різну область огляду, тому бачитиме різні ділянки трафіку. Ви можете приблизно розрахувати область огляду сенсорів всередині мережі за допомогою простого графа, що складається з вершин і ребер, як показано в нижньому правому куті рис.1, а потім простежити, які з ребер перетинаються між вершинами. Сенсор, позначений рубом, реєструватиме весь трафік, що перетинає це ребро на шляху до точки призначення. Наприклад, згідно з рис.1:

- сенсор у точці *A* бачитиме лише трафік між мережею та Інтернетом, але не бачитиме, наприклад, трафік між адресами 128.1.1.1 та 128.2.1.1;
- сенсор у точці *B* бачить весь трафік між однією з адрес, розташованих нижче за нього на схемі, та адресою 128.2.1.1 або Інтернетом;
- сенсор *C* бачить тільки вихідний та вхідний трафік 128.2.1.1;
- сенсор *D*, як і *C*, бачить лише трафік, що виходить від адреси 128.1.1.1 або передається їм;
- сенсор *E* бачить весь трафік, що циркулює між портами комутатора: трафік від адреси 128.1.1.1 кудись ще, трафік від адреси 128.1.1.2 кудись ще, а також трафік з 128.1.1.3 в 128.1.1.32, що взаємодіє з чимось ще за межами даного концентратора;
- сенсор *F* бачить частину трафіку, видимого сенсором *E*, а саме ту його частину, яка передається від 128.1.1.3 до 128.1.1.32, що взаємодіє з чимось ще за межами даного концентратора;
- сенсор *G* – особливий випадок, оскільки є журналом HTTP. Він бачить лише трафік протоколу HTTP (порти 80 та 443), де 128.1.1.2 – це адреса сервера;
- і нарешті, сенсор *H* бачить будь-який трафік, що відправляється або одержується будь-якою з адрес діапазону 128.1.1.3–128.1.1.32, а також трафік між цими хостами [1].

Жоден із сенсорів не охоплює всю мережу повністю. Крім того, у процесі роботи доведеться зіткнутися з надлишковим трафіком. Наприклад, якщо використовувати сенсори *H* і *E*, то побачимо трафік від 128.1.1.3 до 128.1.1.1 двічі. При виборі місця встановлення сенсора необхідно прагнути охопити мережу повністю, не блукаючи у надлишкових даних.

Оснащуючи мережу, необхідно визначати правильні місця встановлення сенсорів у три етапи: створення карти мережі, визначення потенційних точок встановлення сенсорів та визначення оптимального охоплення мережі.

Перший етап передбачає розробку карти мережі, розуміння того, як її елементи з'єднані один з одним, а також визначення потенційних точок встановлення сенсорів. Рис.1 є спрощеною схемою такої мережі.

На другому етапі, при оцінці області огляду, необхідно знайти потенційно прийнятні точки установки сенсорів мережі та визначити область, видиму з цих точок. Це значення може бути виражене у вигляді переліку комбінацій IP-адреси/порту.

Таблиця 1 показує приклад звіту для рис. 1. Побудови графа достатньо, щоб припустити, яке охоплення мережі забезпечуватиметься з точок встановлення сенсорів, але побудова більш точної моделі потребує більше інформації про маршрутизатори та мережне обладнання [8].

Таблиця 1 – **Область видимості з точок встановлення сенсорів на рис. 1**

Точка встановлення	IP-адреса джерела	IP-адреса пункту призначення
A	Інтернет	128.1, 2.1.1-32
	128.1, 2.1.1-32	Інтернет
B	128.1.1.1-32	128.2.1.1, Інтернет
	128.2.1.1, Інтернет	128.1.1.1-32
C	128.2.1.1	128.1.1.1-32, Інтернет
	128.1.1.1-32, Інтернет	128.2.1.1
D	128.1.1.1	128.1.1.2-32, 128.2.1.1, Інтернет
	128.1.1.2-32, 128.2.1.1, Інтернет	128.1.1.1
E	128.1.1.1	128.1.1.2-32, 128.2.1.1, Інтернет
	128.1.1.2	128.1.1.1, 128.1.1.3-32, 128.2.1.1, Інтернет
	128.1.1.3-32	128.1.1.1-2,128.2.1.1, Інтернет
F	128.1.1.3-32	128.1.1.1-2,128.2.1.1, Інтернет
	128.1.1.1-32, 128.2.1.1, Інтернет	128.1.1.3-32
G	128.1,2.1.1-32, Інтернет	128.1.1.2:tcp/80
	128.1.1.2:tcp/80	128.1,2.1.1-32
H	128.1.1.3-32	128.1.1.1-32, 128.2.1.1, Інтернет
	128.1.1.1-32, 128.2.1.1, Інтернет	128.1.1.3-32

Наприклад, при роботі з роутерами ми можемо виявити, що огляд з точки установки сенсора асиметричний (зверніть увагу, що трафік, показаний на рис.1, завжди симетричний).

Третій етап передбачає вибір оптимальних точок установки, показаних у цій таблиці. Мета – вибрати точки, які забезпечують моніторинг мережі за найменшої надмірності трафіку. Наприклад, сенсор *E*, крім інших, бачить усі дані сенсора *F*, тому немає сенсу вибирати обидві точки. При виборі точок установки практично завжди доводиться мати справу з надмірністю трафіку.

У цій ситуації допоможе застосування правил фільтрації. Наприклад, щоб обробити трафік між хостами 128.1.1.3–32, у точці *H* необхідно встановити сенсор, і цей трафік спливатиме знову і знову в точках *E, F, B* та *A*. Якщо налаштувати сенсори в цих точках таким чином, щоб вони не були звітували про трафік, що надходить з адрес 128.1.1.3–32, проблема дублювання стає неактуальною.

Сенсор *G* дуже відрізняється від інших сенсорів, показаних на рис. 1.

Поки інші сенсори фіксують весь трафік мережі, *G* фіксує лише трафік протоколу HTTP (tcp/80).

Поки інші сенсори здійснюють збір даних трафіку в межах мережі, *G* збирає дані з іншого рівня. Рівень сенсора дає уявлення про інформацію, що він збирає.

Висновки

Сенсори збирають інформацію про мережний трафік. Приклади таких сенсорів включають VPN, більшість систем виявлення вторгнень (IDSes), програми збору даних протоколу NetFlow, такі як YAF (Yet Another Flowmeter є еталонною реалізацією для стандарту IETF IPFIX і стандартним програмним забезпеченням захоплення пакетів потоку для інструментарію SiLK, YAF може зчитати *pcap* дані з файлів або отримати пакети безпосередньо, які він потім збирає в запису потоку і експортує на диск), а також програми збору даних протоколу TCP, такі як Snort, і сирі дані *tcpdump*. Мережуі сенсори дають більше інформації, ніж хост-сенсори, не тільки тому, що вони бачать безліч хостів, але і тому, що хост може не реагувати на трафік, що відправляється по всій мережі. У той самий час якщо брати до уваги обсяг мережних даних, їх цінність невелика: доводиться аналізувати більшу кількість записів для розуміння події, і часто складно визначити, чи хост відреагував на мережний трафік. Мережні сенсори можуть допомогти в розслідуванні та лужити підмогою для хост-сенсорів, коли ця інформація недоступна [9]. Використання мережних сенсорів та детекторів є ефективним інструментом систем виявлення вторгнень (IDSes) для впровадження дієвої політики безпеки сучасних комп'ютерних мереж.

Список літератури

1. Michael Collins. Network Security Through Data Analysis: From Data to Action 2nd Edition, 2017. – 428 p.
2. Зиков І. С., Кучук Н. Г., Шматков С. І. Синтез архітектури комп'ютерної системи управління транзакціями e-learning. *Сучасні інформаційні системи*. 2018. Т. 2, № 3. С. 60–66. DOI: https://doi.org/10.20998/2522-9052.2018.3.10.
3. Катренко А. Особливості інформаційної безпеки за міжнародними стандартами // Альманах економічної безпеки. – 1999. – №2. – С. 15–17.
4. Кучук Н.Г., Гавриленко С.Ю., Лукова-Чуйко Н.В., Собчук В.В. Перерозподіл інформаційних потоків у гіперконвергентній системі / С.Ю. Гавриленко. *Сучасні інформаційні системи*. 2019. Т. 3, № 2. С. 116-121. DOI: https://doi.org/10.20998/2522-9052.2019.2.20.
5. Nechausov A., Mamusuĉ I., Kuchuk N. Synthesis of the air pollution level control system on the basis of hyperconvergent infrastructures. Сучасні інформаційні системи. 2017. Т. 1, № 2. С. 21 – 26. DOI: https://doi.org/10.20998/2522-9052.2017.2.04.
6. Bonabeau Eric. Swarm Intelligence: From Natural to Artificial Systems / Eric Bonabeau, Marco Dorigo, Guy Therauaz. – NY: Oxford University Press Inc. – 1999. – 306 p.
7. Кучук Г.А. Метод мінімізації середньої затримки пакетів у віртуальних з'єднаннях мережі підтримки хмарного сервісу / Г.А. Кучук, А.А. Коваленко, Н.В. Лукова-Чуйко // Системи управління, навігації та зв'язку. – Полтава . ПНТУ, 2017. – Вип. 2(42). – С. 117-120.
8. Haykin S. Neural Networks and Learning Machines / S. Haykin. - Prentice Hall. – 2009. – 906 p.
9. Кузьменко Б.В., Чайковська О.О. «Захист інформації. Частина 2. Програмно-технічні засоби забезпечення інформаційної безпеки». – 2009.

Received (Надійшла) 21.10.2021
Accepted for publication (Прийнята до друку) 05.01.2022

Network sensors and detectors as an effective data monitoring tool

A. Yanko, A. Martynenko, V. Trykoz

Abstract. This article is devoted to data collection and network analysis in order to understand the principles of their use and prevent hacker malware. The main considerations for security measures are considered. An in-depth understanding of the areas of information security is provided. For each attack scenario, the most effective scenarios for protection and formation of an effective information security policy were selected and developed. Developing the right structure requires an understanding of how different sensors collect data, how they complement, duplicate, and interact with each other, and an understanding of the principles of efficient data storage to enable analysis. It is these problems that are emphasized in this paper. Particular attention is paid to analysis - the process of collecting safety data and taking decisive action based on them. This article focuses on the mechanisms of intrusion detection through the use of network sensors and detectors. As a result, recommendations were made to ensure effective information security of a modern computer network based on the use of network sensors and detectors. Information security measures to prevent further malicious actions were also considered.

Keywords: information security, computer network, network detector, network sensor, security policy, intrusion detection system, data scanning.