https://doi.org/10.31891/2219-9365-2023-74-1
УДК 004.056

МОСТОВИЙ Сергій
Хмельницький національний університет
https://orcid.org/0000-0002-9505-3206
e-mail: serhii.mostovyi@khmnu.edu.ua
ПЕТЛЯК Наталія
npetlyak@khmnu.edu.ua
Хмельницький національний університет
ГОЛОТА Ірина
holota@khmnu.edu.ua

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ІНСТРУМЕНТІВ ВИЯВЛЕННЯ І ЗАПОБІГАННЯ ВТОРГНЕНЬ НА ВУЗЛИ В КОРПОРАТИВНИХ МЕРЕЖАХ

В роботі наведено результати досліджень ефективності систем виявлення вторгнень в корпоративну мережу при різній інтенсивності трафіка та для різних типів атак.
Ключові слова: корпоративна мережа, виявлення вторгнень, ефективність виявлення та запобігання вторгненням.

MOSTOVYI Serhii, PETLYAK Nataliia, HOLOTA Iryna
Khmelnytskyi National University

RESEARCH OF TOOLS EFFICIENCY FOR DETECTION AND PREVENTION OF INTRUSIONS ON CORPORATE NETWORKS NODES

The increase in the number of various methods of intrusions and their implementation in the form of attacks requires the need to improve existing technologies and means of data protection in corporate computer networks. Among the conditions that have a serious impact on the suitability of various methods, it is possible to single out a rapid increase in the volume of traffic and bandwidth of the communication channel. This means that there is a need to find an algorithm that reduces the amount of calculations. The mechanism for detecting intrusions into the system is based on the assumption of stationarity of network traffic, that is, any deviation from the stationary characteristics of network traffic is understood as an attack. It follows that the problem of traffic analysis and detection of intrusions into the corporate network requires further research.

Despite the large number of methods, they all work in real time and are based on signature analysis, which makes them unsuitable for detecting new, previously unknown types of attacks. Most of the free software systems for detecting and preventing attacks available today use signature analysis.

The paper presents the results of research into the effectiveness of systems for detecting intrusions into the corporate network at different traffic intensities and for different types of attacks.

The effectiveness of the most common systems for detecting intrusions into the corporate network was investigated experimentally. The results showed that these systems give a stable result with a small amount of traffic and only for known types of attacks, since they are based on signature analysis. When the amount and intensity of traffic increases, these systems show rather poor results: they have a lot of packet loss and heavily load server resources. In order to increase the reliability of information security of corporate networks, there is a need to improve approaches to attack detection and traffic analysis.
Keywords: corporate network, intrusion detection, intrusion detection and prevention effectiveness.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Стрімкий та активний розвиток мережних технологій призводить до появи нових типів атак на корпоративні комп'ютерні мережі [1]. Зростання кількості різноманітних методів вторгнень та їх реалізацій у вигляді атак вимагає необхідності удосконалення наявних технологій та засобів захисту даних у корпоративних комп'ютерних мережах. Серед умов, що мають серйозний вплив на придатність різних методів, можна виділити швидке збільшення обсягу трафіку та смуги пропускання каналу зв'язку. Це означає, що виникає необхідність у пошуку алгоритму, який скорочує обсяг обчислень. В основі механізму виявлення вторгнень в систему лежить припущення про стаціонарність мережного трафіку, тобто під атакою розуміють будь-які відхилення від стаціонарних характеристик мережного трафіку. Звідси випливає, що проблема аналізу трафіку та виявлення вторгнень в корпоративну мережу потребує подальших досліджень.

Аналіз досліджень та публікацій

В роботі [2] проаналізовано сучасні підходи до виявлення та прогнозування атак на корпоративні мережі. Проте, незважаючи на велику кількість методів, вони всі працюють в реальному режимі часу та грунтуються на синатурному аналізі, що робить їх непридатними до виявлення нових, раніше невідомих типів атак. Більшість безкоштовних програмних систем для виявлення та запобігання атакам, що доступні на сьогодні, використовують саме сигнатурний аналіз.

Формулювання цілей статті

Метою роботи є: дослідження ефективності таких систем для подальшого вдосконалення інформаційної безпеки в корпоративних мережах.

Виклад основного матеріалу

Критичне порівняння проводиться між системами виявлення та запобігання вторгненням Suricata та Snort [3,6].

Показниками, що використовуються для вимірювання ефективності систем є: швидкість виявлення атак, помилкові спрацьовування [4].

Для кількісної оцінки метрик, що використовуються для оцінки точності системи виявлення та запобігання вторгненню, можна використати наступні: охоплення (кількість атак, які можна виявити), ймовірність помилкових спрацьовувань, ймовірність виявлення резистивних атак, здатність обслуговувати канал з високою пропускною здатністю і ємністю [4]. Що стосується продуктивності, вона має ряд компонентів, і тому не є метрикою. У табл. 1 наведено деякі показники, що відображають ємність.

Необхідно реєструвати такі показники: байти в секунду, пакети в секунду та кількість мережевих атак. Крім того, для кожної системи виявлення та запобігання вторгненню в мережу зменшено кількість втрачених пакетів, також були записані фактичні тригери, помилкові спрацьовування, негативні тригери та загальна кількість тривог. Нарешті, хост відстежує використання центрального процесора та пам'яті, постійне зберігання, пропускну здатність інтерфейсу та статистику файлів підкачки.

Тестовий стенд налаштований у віртуальному середовищі, що сприяє мобільності та безпеці експерименту. Це було необхідно для частого повторення та реконфігурації експериментальних випробувань.

VMware Workstation 15 була використана як платформа для віртуалізації, багато в чому завдяки хорошій продуктивності вводу-виводу та жорсткого диска порівняно з іншими засобами віртуалізації. В якості операційної системи було обрано 32-розрядну Ubuntu 18.04 LTS. Ubuntu регулярно оновлюється і має хорошу базу спільнот. Це також найпопулярніша операційна система Linux.

Таблиця 1

Оцінка потенціалу

Показник, що перевіряється	Використання ресурсів
Пакетів в секунду	Цикли CPU, пропускна здатність інтерфейсів, пропускна здатність шини
Байт в секунду (середній розмір пакета)	Цикли CPU, пропускна здатність інтерфейсів, пропускна здатність шини
Протоколи	Цикли CPU і пропускна здатність шини
Кількість унікальних хостів	Розмір пам'яті, цикли CPU, пропускна здатність шини
Кількість нових з'єднань в секунду	Цикли CPU і пропускна здатність шини
Кількість одночасних з'єднань	Розмір пам'яті, цикли CPU, пропускна здатність шини
Попередження в секунду	Розмір пам'яті, цикли CPU, пропускна здатність шини

За замовчуванням апаратна конфігурація для системи виявлення та запобігання вторгнень в мережу становила 2,8 ГГц чотирьохядерним процесором Intel Xeon (E5462) з 4-ядерною 3 ГБ DDR2 800 МГц повністю буферованою пам'яттю. Кожна система також мала максимальний об’єм жорсткого диска 20 ГБ. Мережевий трафік передавався окремо для кожної системи. Система, що використовується для відтворення мережевого трафіку, використовує одне ядро та 1 Гб оперативної пам'яті. VMware хост операційної системи, що використовує 2 Гб оперативної пам'яті і 1 ядро, що перешкоджає хосту з якого виробляє на випробувальному стенді.

Snort і Suricata були налаштовані на роботу з однаковими правилами. Suricata використовує різні класифікації конфігурації Snort, яка використовує 134 декодери та 174 правила препроцесора. Ідентичні методи реєстрації, які називаються Barnyard, MySQL та AcidBase, використовувались як для систем виявлення вторгнень в мережі, так і для систем запобігання. Версії Snort та Suricata були v2.9.8.3 та v4.1.2 відповідно.

Обидві системи використовували набір правил VRT Snort v2.9.8.3 у поєднанні з набором правил для нових загроз.

Для тестування було використано реальний мережевий трафік у фоновому режимі [5]. Однак повторення експериментів із трафіком у реальному часі було б непередбачуваним через його динаміку. Було обрано використання трафіку, захопленого з файлу pcap. Це сприяло їх обробці системою виявлення та попередження вторгнення мережі в автономному режимі, дозволяючи відтворювати в мережі з різною швидкістю, використовуючи TCPReplay. Крім того, усунуто всі ризики для критично важливих мереж. Використовуваний трафік було зафіксовано для запуску атак Metasploit на комп'ютері під керуванням Microsoft Windows 2000. Windows 2000 було обрано як найбільш підходящий Metasploit для цієї операційної системи порівняно з іншими.

Атаки, перелічені в таблиці 2, реєструються за допомогою Wireshark [7]. Частина програми

Wireshark, Edicap, була використана для зміни часової позначки використовуваного трафіку та співвіднесення її з трафіком у фоновому режимі. У цій дії вони були об’єднані в хронологічному порядку, щоб атакуючий трафік перемістився на другий план.

Відстежувались такі ресурси: використання центрального процесора, використання пам’яті, опір пропускної здатності пам'яті та пропускна здатність мережі. Це було зроблено за допомогою інструмента командного рядка Linux dstat. Кожного разу, коли запускалося тестування, реєструвались початок і кінець трафіку запуску NIDPS. Трафік проходив через хости 192.168.16.2 та 192.168.16.128, але був позначений як небажаний трафік.

Таблиця 2

Вивчення атак

Код	Ім’я	Опис
ms03_026_dcom	Microsoft RPCDCOM Interface Overflow	Модуль використовуваного стеку переповнення буфера в службі RPCSS
ms05_039_pnp	Microsoft Server Service NetpwPathCanonicalize Overflow	Стек переповнення буфера в службі Windows Plug and Play
ms05_047_pnp	Microsoft Plug and Play Service Registry Overflow	Стек переповнення буфера в службі Windows PnP. Причина перезавантажень.
ms06_040_netapi	Microsoft Server Service NetpwPathCanonicalize Overflow	Стек переповнення буфера в NetApi32 CanonicalizePathName () використовуючи функцію NetpwPathCanonicalize RPC виклик служби Server
ms05_017_msmq	Microsoft Message Queueing Service Path Overflow	Використовуваний стек переповнення буфера в RPC інтерфейсі в службі Microsoft Message Queueing
ms01_033_idq	Microsoft IIS5.0 IDQ Path Overflow	Використовуваний стек переповнення буфера в IDQ ISAPI обслуговування для Microsoft Index Server

Для визначення точності використаний контроль попереджень. Ці попередження, отримані без системи стресів, використовувались як еталон. Відхилення від базової лінії в умовах стресу показувало зміни в точності виявлення. У табл. 3 наведено кількість типів попередження, що генеруються під час нападу на кожну NIDPS.

Таблиця 3

Попередження згенеровані Snort і Suricata

Попередження	Snort	Suricata
ms05_040_pnp	4	4
ms05_047_pnp	1	1
ms05_039_pnp	1	6
ms03_026_dcom	1	2
ms01_033_1dq	2	4
ms05_017_msmq	2	3

На рис. 1 показані попередження Suricata на кожен експлоїт у всіх конфігураціях, але деякі попередження втрачені, що призводить до зменшення діапазону виявлення.

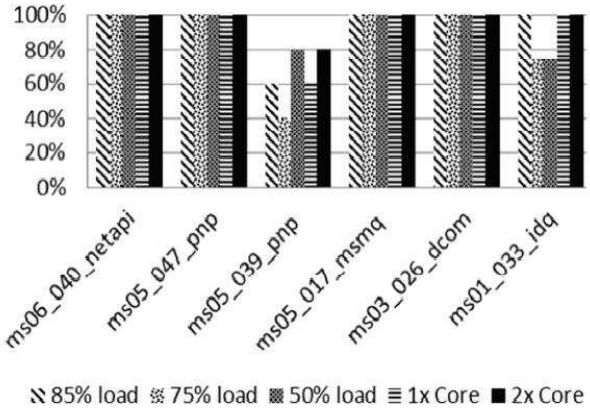

Рис 1 – Попередження у Suricata

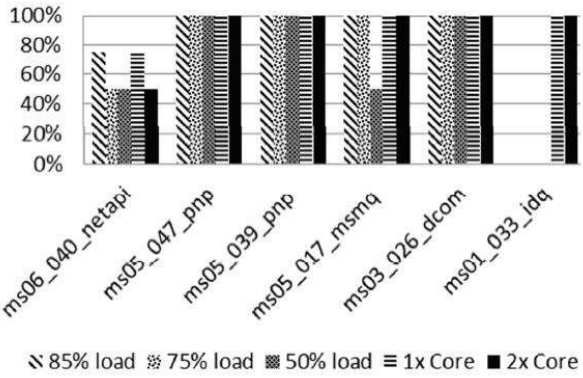

Рис 2 – Попередження у Snort

На рис. 2 показано провальні попередження Snort на ms01_033_idq. Ці помилкові негативні результати обумовлені надмірним навантаженням.

У Suricata спостерігається більша точність, ніж у Snort Частково це пов'язано з тим, що Snort менше

контролює функціонування оповіщень під час атаки, ніж Suricata (два проти чотирьох). Snort не зміг попередити ms01_033_idq двома правилами з набору правил VRT, ідентифікаторами 1245 та 1244. Suricata був успішним, і ці сповіщення спрацьовували. Suricata має високі вимоги до обробки, саме тому він досягає більших експлуатаційних можливостей, ніж Snort. Snort має набагато нижчі системні вимоги, тому він не може працювати з втратою пакетів при максимальному навантаженні системи. При роботі в багатоядерній конфігурації Suricata показує менше втрат пакетів, ніж Snort. Suricata використовує наявні ядра більш рівномірно. Тести в автономному режимі показують, що Suricata набагато повільніша за Snort. Хоча Suricata використовує багатоядерну систему більш чітко, ніж Snort. З огляду на це, можна сказати, що Suricata має кращу масштабованість. Однак, якщо Snort отримує хороші результати пропускної здатності, рекомендується запускати кілька екземплярів Snort на декількох ядрах. Це може запропонувати таку ж масштабованість, як Suricata, але з додатковими витратами на обробку однопотокових додатків на декількох ядрах.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Експериментальним шляхом було досліджено ефективність роботи найбільш поширених систем виявлення вторгнень в корпоративну мережу. Результати показали, що дані системи дають стабільний результат при невеликому обсязі трафіка та лише для відомих типів атак, оскільки базуються на сигнатурному аналізі. При зростанні кількості та інтенсивності трафіка дані системи показують досить низькі результати: мають багато втрат пакетів та сильно навантажують ресурси сервера. З метою підвищення надійності інформаційної безпеки корпоративних мереж є необхідність в удосконаленні підходів до виявлення атак та аналізу трафіка.

Література

1. Методи проникнення в корпоративні мережі [Інтернет-ресурс]. – Режим доступу: https://www.kitgsm.com.ua/stati/bezpeka/metodi-proniknennya-v-korporativni-merezhi.html, вільний.

2. Husák M., Komárková J., Bou-Harb E., Čeleda P.Survey of Attack Projection, Prediction, and Forecasting in Cyber 5. Security. IEEE Communications Surveys Tutorials. September 2018. Vol. 21, No. 1. P. 640-660

3. Обзор систем обнаружения вторжений [Інтернет-ресурс]. Режим доступу: http://www.connect.ru вільний.

4. Критерии сравнения систем обнаружения атак [Інтернет-ресурс]. – Режим доступу: http://inf-bez.ru/?p=480, вільний.

5. Paxon V., Floyd S. Wide-area traffic: The failure of Poisson modeling. / V. Paxon, S. Floyd // IEEE/ACM Transactions on Networking. – 1995. – Vol. 3. – p. 226 – 244.

6. Snort [Інтернет-ресурс] / Web-сайт: snort; Режим доступу http://www.snort.org, вільний.

7. Wireshark [Інтернет-ресурс] / Web-сайт: wireshark; Режим доступу http://www.wireshark.org, вільний.

References

1. Metody pronyknennia v korporatyvni merezhi [Internet-resurs]. – Rezhym dostupu: https://www.kitgsm.com.ua/stati/bezpeka/metodi-proniknennya-v-korporativni-merezhi.html, vilnyi.

2. Husák M., Komárková J., Bou-Harb E., Čeleda P.Survey of Attack Projection, Prediction, and Forecasting in Cyber 5. Security. IEEE Communications Surveys Tutorials. September 2018. Vol. 21, No. 1. P. 640-660

3. Obzor sistem obnaruzheniya vtorzhenij [Internet-resurs]. Rezhym dostupu: http://www.connect.ru vilnyi.

4. Kriterii sravneniya sistem obnaruzheniya atak [Internet-resurs]. – Rezhym dostupu: http://inf-bez.ru/?p=480, vilnyi.

5. Paxon V., Floyd S. Wide-area traffic: The failure of Poisson modeling. / V. Paxon, S. Floyd // IEEE/ACM Transactions on Networking. – 1995. – Vol. 3. – p. 226 – 244.

6. Snort [Internet-resurs]./ Web-сайт: snort; Rezhym dostupu http://www.snort.org, vilnyi.

7. Wireshark [Internet-resurs]./ Web-сайт: wireshark; Rezhym dostupu http://www.wireshark.org, vilnyi.