XLVIII INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE
INTERACTION OF ART AND SCIENCE: CREATIVE APPROACHES IN RESEARCH

Section name – Information Technology & Cybersecurity

АНАЛІЗ ІСНУЮЧИХ IDS ДЛЯ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ

Рихва Володимир,
Аспірант кафедри кібербезпеки та інформаційних технологій
volodymyr.rykhva@hneu.net
Харківський національний економічний
університет імені Семена Кузнеця, Україна

Фахівці спільно з дослідниками з різних сфер працюють над створенням ефективних систем кіберзахисту. Ці системи забезпечують конфіденційність, цілісність та доступність інформації [1], захищаючи комп'ютери та мережі від хакерських атак.

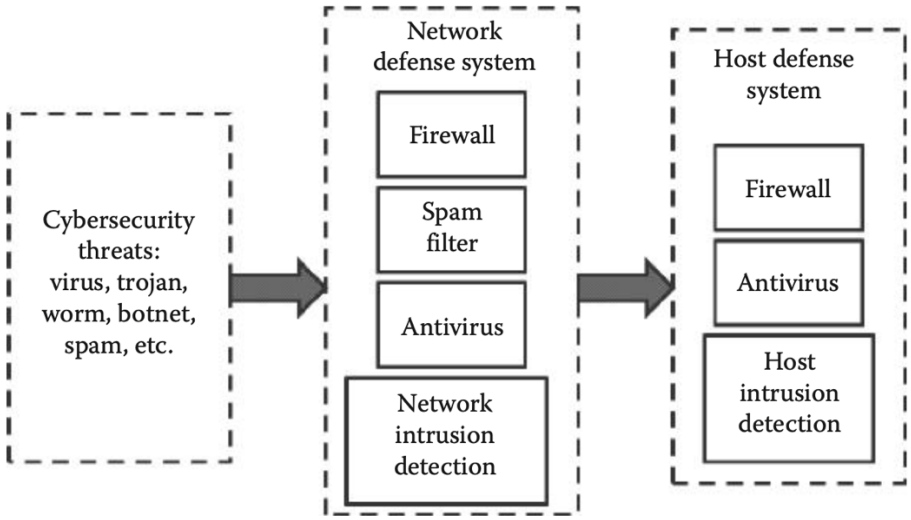

Рис.1. Традиційна система кібербезпеки

Як показано на Рис.1, звичайні системи кібербезпеки вирішують різні загрози, включаючи віруси, трояни, червяки, спам і мережі ботів. Ці системи кібербезпеки борються із загрозами на двох рівнях: мережі та хоста. Мережеві системи захисту контролюють мережевий потік за допомогою мережевого брандмауера, спам-фільтра, антивірусу та методів виявлення мережевих вторгнень. Системи захисту на основі хоста контролюють майбутні дані на робочій станції за допомогою брандмауера, антивірусу та методів виявлення вторгнень, встановлених на хостах.

На обох рівнях присутній додатковий шар захисту Network-based intrusion detection (NIDS) [2] і Host-based intrusion detection (HIDS), що є головними видами Intrusion Detection System (IDS). Основною метою IDS є виявлення та сповіщення адміністраторів безпеки про потенційні інциденти безпеки, такі як спроби несанкціонованого доступу, зараження зловмисним програмним забезпеченням або підозрілі моделі мережевого трафіку. Аналізуючи мережеві пакети, файли журналів, системну діяльність та інші відповідні дані, IDS може допомогти виявити загрози безпеці та реагувати на них у реальному часі.

Найбільш поширені на сьогодні IDS:

Система ***Zeek***, раніше відома як Bro, є результатом багаторічних досліджень та розробок у галузі мережевої безпеки [3]. Розпочата в 1995 році в Національній лабораторії Лоуренса в Берклі, США, вона стала одним із найпотужніших інструментів для аналізу мережевого трафіку та виявлення аномалій. Основним методом, що використовується в Zeek, є глибокий аналіз протоколів і подій на різних рівнях мережевої моделі. Система не просто шукає відомі сигнатури атак, а моделює поведінку мережевих з'єднань, дозволяючи виявляти складні та нові загрози.

Snort – це відкрита система виявлення та запобігання вторгнень (IDS/IPS) [4], розроблена Мартіном Роешем у 1998 році. З моменту свого створення Snort стала однією з найпоширеніших систем IDS у світі, завдяки своїй гнучкості, продуктивності та підтримці спільноти. Основним методом, що використовується в Snort, є сигнатурний аналіз мережевого трафіку з використанням правил, які описують характерні ознаки відомих атак. Система також підтримує аналіз на основі аномалій через використання препроцесорів та модулів розширення.

Suricata – це високопродуктивна система виявлення вторгнень та запобігання атак (IDS/IPS), розроблена Open Information Security Foundation (OISF) [5]. Проект розпочато в 2009 році з метою створення сучасної та гнучкої IDS з відкритим кодом. Основний метод, що використовується в Suricata, - це сигнатурний аналіз мережевого трафіку з використанням правил, подібних до правил Snort. Однак Suricata також підтримує розширені функції, такі як глибокий аналіз пакетів та розпізнавання протоколів на основі контексту.

Security Onion – це інтегрована платформа з відкритим кодом для моніторингу мережевої безпеки, яка поєднує в собі кілька інструментів для виявлення вторгнень, аналізу журналів та реагування на інциденти [6]. Проект розпочато в 2008 році та активно розвивається спільнотою спеціалістів з безпеки. Основний метод роботи Security Onion полягає в комбінуванні різних інструментів та технологій для створення комплексного рішення з моніторингу та аналізу безпеки.

Wazuh – це платформа з відкритим кодом для виявлення вторгнень на основі агентів, моніторингу безпеки та відповідності вимогам [7]. Вона є розвитком проекту OSSEC, розпочатого в 2008 році. Основний метод роботи Wazuh — це збір та аналіз даних з кінцевих вузлів за допомогою встановлених агентів, що дозволяє контролювати цілісність файлів, аналізувати журнали та виявляти аномалії.

Cisco Secure IDS – це комерційна система виявлення та запобігання вторгнень, розроблена компанією Cisco Systems [8]. Вона інтегрується з іншими продуктами Cisco та надає розширені можливості для забезпечення безпеки мережевої інфраструктури. Основний метод роботи Cisco Secure IDS — це аналіз мережевого трафіку з використанням сигнатур та поведінкових моделей для виявлення відомих та нових загроз.

IBM QRadar – це комплексна платформа для управління інформаційною безпекою та подіями (SIEM), яка включає функціональність системи виявлення вторгнень [9]. Розроблена компанією IBM, вона забезпечує централізований моніторинг, аналіз та реагування на загрози. Основний метод роботи QRadar – це кореляція подій з різних джерел та виявлення аномалій на основі поведінкового аналізу та правил безпеки.

Порівняння різних IDS систем:

Критерій	**Zeek**	**Suricata**	**Security Onion**	**Wazuh**	**Cisco Secure IDS**	**IBM QRadar**	**Snort**
Метод виявлення	Поведінковий, аналіз подій	Сигнатурний та поведінковий аналіз	Комбінований	Агентський аналіз, контроль цілісності файлів	Сигнатурний та поведінковий аналіз	Кореляція подій, поведінковий аналіз, AI	Сигнатурний та поведінковий аналіз
Архітектура	Мережна IDS	Мережна IDS/IPS	Гібридна платформа	Агентська IDS	Мережна IDS/IPS	SIEM-платформа з функціями IDS	Мережна IDS/IPS
Масштабованість	Висока (розподілена, паралельна обробка)	Висока (багатопотоковість, апаратне прискорення)	Висока (розподілена архітектура)	Висока (підтримка багатьох агентів)	Висока (особливо з обладнанням Cisco)	Дуже висока (для великих організацій)	Помірна (потребує оптимізації)
Розширюваність	Дуже висока (скриптова мова, модульність)	Висока (правила Snort, Lua-скрипти)	Висока (додавання інструментів)	Висока (налаштування правил, інтеграція з Elastic Stack)	Обмежена (власні стандарти Cisco)	Висока (модулі, інтеграція з іншими системами)	Висока (відкритий код, власні правила)
Простота налаштування	Складна (потрібні знання скриптової мови)	Помірна (налаштування правил, оптимізація)	Складна (багато компонентів)	Відносно проста (шаблони та політики)	Помірна (спрощено для обладнання Cisco)	Складна (потрібні експертні знання)	Відносно проста (налаштування правил)

Підтримка та спільнота	Активна (оновлення, документація)	Активна (OISF, оновлення)	Активна (спільнота фахівців з безпеки)	Активна (оновлення, інтеграція)	Професійна підтримка від Cisco	Професійна підтримка від IBM	Активна (спільнота, оновлення правил)
Вартість	Безкоштовно	Безкоштовно	Безкоштовно	Безкоштовно	Комерційна (вартість ліцензій та обладнання)	Комерційна (висока вартість ліцензій)	Безкоштовно

Табл.1. Зведена порівняльна таблиця IDS

References

1. Столяр А. Л. Аналіз сучасних методів виявлення аномалій в комп'ютерних мережах. 2023, URL: https://doi.org/10.18372/2073-4751.74.17888.
2. Kumar KN, Sukumaran S. A survey on network intrusion detection system techniques. International Journal of Advanced Technology and Engineering Exploration. 2018;5(47):385-393
3. Zeek. URL: https://github.com/zeek/zeek (дата звернення 12.11.2024)
4. Snort URL: https://www.snort.org (дата звернення 12.11.2024)
5. Suricata URL: https://suricata.io (дата звернення 12.11.2024)
6. Security Onion URL: https://securityonionsolutions.com/software (дата звернення 12.11.2024)
7. Wazuh. URL: https://github.com/wazuh/wazuh (дата звернення 12.11.2024)
8. Intrusion Detection: Cisco IDS Overview. URL: https://www.ciscopress.com/articles/article.asp?p=24696 (дата звернення 12.11.2024)
9. IBM QRadar URL: https://www.ibm.com/qradar (дата звернення 12.11.2024)