УДК 004.6

ВИЯВЛЕННЯ НЕБЕЗПЕЧНИХ ВХОДЖЕНЬ У КОМП'ЮТЕРНУ МЕРЕЖУ ЗА ДОПОМОГОЮ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Боднар О., Лагун А., Ткачук Р.
Львівський державний університет безпеки життєдіяльнсті, м. Львів

В роботі розглядаються вимоги до систем виявлення та запобігання вторгнень, а також описаний вибір методів та критеріїв досліджень IDPS. Проведено аналіз сучасних IDPS-систем, досліджено особливості їх роботи.
***Ключові слова**: IDS/IPS системи, інформаційна безпека, Snort, Suricata.*

The paper considers the requirements for intrusion detection and prevention systems, as well as describes the choice of methods and criteria for IDPS research. The analysis of modern IDPS-systems is carried out, features of their work are investigated.
***Key words:** IDS/IPS systems, information security, Snort, Suricata.*

Найважливішим атрибутом нашого часу є глобальна інформаційна інтеграція, заснована на побудові комп'ютерних мереж масштабу підприємства і їх об'єднання за допомогою Інтернету.

Складність логічної і фізичної організації сучасних мереж призводить до об'єктивних труднощів при вирішенні питань управління та захисту мереж. В процесі експлуатації комп'ютерних мереж адміністраторам доводиться вирішувати дві головні завдання [5]:

– діагностувати роботу мережі і підключених до неї серверів, робочих станцій і відповідного програмного забезпечення;

– захищати інформаційні ресурси мережі від несанкціонованої діяльності хакерів, впливів вірусів, мережевих черв'яків і тп. ті. забезпечувати їх конфіденційність, цілісність і доступність.

При вирішенні завдань, пов'язаних з діагностикою та захистом мережевих ресурсів, центральним питанням є оперативне виявлення станів мережі, що призводять до втрати повної або часткової її працездатності, знищення, перекручення чи витоку інформації, що є наслідком відмов, збоїв випадкового характеру або результатом отримання зловмисником несанкціонованого доступу до мережевих ресурсів, проникнення мережевих черв'яків, вірусів і інших загроз інформаційної безпеки. Раннє виявлення таких станів дозволить своєчасно усунути їх причину, а також попередить можливі катастрофічні наслідки.

Для їх виявлення використовується великий спектр спеціалізованих систем. Так, при вирішенні проблем діагностики мереж застосовуються засоби систем управління, аналізатори мережевих протоколів, системи тестування навантаження, системи моніторингу мережі. Проблеми захисту

інформаційних ресурсів мереж вирішуються за допомогою міжмережевих екранів (firewall), антивірусів, систем виявлення атак (вторгнень) (СВВ) (Intrusion Detection System, IDS), систем контролю цілісності, криптографічних засобів захисту [3, 4].

Характерними особливостями використання цих систем є або їх періодичне і короткочасне застосування для вирішення певної проблеми, або постійне використання, але зі статичними настройками. В результаті методи аналізу, що використовуються в сучасних системах, спрямовані на виявлення відомих і конкретніше згаданих типів впливів, але можуть виявитися не в змозі виявити їх модифікації або нові типи, що робить їх використання малоефективним.

Таким чином, на сьогоднішній день дуже актуальним завданням є пошук більш ефективних методів виявлення неприпустимих подій (аномалій) в роботі мережі, які є наслідком технічних збоїв або несанкціонованих дій. Основною вимогою до цих методів є можливість виявлення довільних типів аномалій, в тому числі нових, а також впливів, розподілених у часі.

Цей напрямок наукових досліджень є дуже молодим. Перші роботи, присвячені даній проблемі, були опубліковані в 90-х роках минулого століття.

На даний момент дослідження в цій області ведуться великими закордонними комерційними компаніями. Загальний підхід, який лежить в основі цих досліджень, полягає в пошуку методів аналізу, що дозволяють виявляти аномальні стани інформаційних ресурсів у вигляді відхилень від звичайного («нормального») стану. Ці відхилення можуть бути результатами збоїв в роботі апаратного і програмного забезпечення, а також причинами мережевих атак хакерів. Такий підхід теоретично дозволить виявляти як відомі, так і нові типи проблем. Від ефективності і точності апарату, що визначає «нормальний» стан і фіксує відхилення, залежить в цілому ефективність рішення питань діагностики та захисту мережевих ресурсів. Особливу важливість на поточний момент становить проблема виявлення аномальних станів в роботі мережі, що мають розподілений у часі характер. Вони можуть бути наслідками спеціально маскуючих мережевих атак зловмисників, прихованих апаратно-програмних збоїв, нових вірусів і т. п.

Системи виявлення та запобігання вторгнень (IDPS) в основному зосереджені на виявленні можливих інцидентів, реєстрації інформації про них, спробі їх зупинити і повідомленні про них адміністраторам безпеки. Існує багато типів технологій IDPS, які диференціюються насамперед за типами подій, які вони можуть розпізнати, та методологіями, які вони використовують для виявлення можливих інцидентів [1, 2].

Типи технологій IDPS:

– Network-Based;
– Host-Based;
– Wireless;

– Application-Protocol-Based;
– Protocol-Based;
– Network Behavior Analysis;
– Hybrid.

Більшість IDPS використовують кілька методологій виявлення, як окремих, так і інтегрованих, для забезпечення більш широкого і точного виявлення. Основними класами методологій виявлення є наступні:

– виявлення на основі підписів;
– виявлення на основі аномалій.

Перш ніж обирати продукцію IDPS, організації повинні спочатку визначити загальні вимоги, яким повинна відповідати продукція. Функції, що надаються продуктами IDPS, та методології, які вони використовують, значно різняться, тому продукт, який найкраще відповідає вимогам однієї організації, може не відповідати вимогам іншої організації. Спочатку оцінювачі повинні зрозуміти характеристики системного та мережевого середовища організації та плани на короткострокові зміни, щоб можна було обрати IDPS, який буде сумісним з ними та матиме змогу контролювати події, що цікавлять системи та / або мережі. Ці знання також необхідні для розробки рішення IDPS. Отримавши розуміння існуючої системи та мережевого середовища, оцінювачі повинні сформулювати цілі та завдання, які вони хочуть досягти, використовуючи IDPS. Оцінювачі також повинні переглянути свої існуючі правила безпеки та інші IT-політики перед вибором продуктів. Ці правила слугують специфікацією для багатьох функцій, які повинні надавати продукти IDPS. Крім того, оцінювачі повинні розуміти, чи підлягає організація нагляду чи перегляду іншою організацією чи ні. Якщо так, вони повинні визначити, чи вимагає цей орган нагляду IDPS або інші конкретні ресурси системи безпеки. Обмежувачі ресурсів також повинні враховуватися оцінювачами. На додаток до визначення загальних вимог, оцінювачі також повинні визначити більш спеціалізовані набори вимог [4, 5]:

– захисні можливості, включаючи збір інформації, реєстрацію, виявлення та запобігання;

– ефективність, включаючи максимальну потужність та характеристики продуктивності;

– управління, включаючи проектування та впровадження, експлуатацію та технічне обслуговування та навчання, документація та технічна підтримка;

– витрати життєвого циклу, як початкові, так і витрати на обслуговування.

Отже, ми можемо зробити висновок, що системи виявлення вторгнень та запобігання вторгнень проводять моніторинг подій, що відбуваються в комп'ютерній системі або мережі, і аналізують їх на наявність ознак мож-

ливих інцидентів, які є порушеннями або неминучими загрозами порушення політик комп'ютерної безпеки, політик допустимого використання або стандартних методів забезпечення безпеки та здійснюють спроби зупинки виявлених можливих інцидентів. Деякі організації використовують IDPS для інших цілей, таких як виявлення проблем з політиками безпеки, документування існуючих загроз і утримання окремих осіб від порушення політик безпеки. IDPS стали необхідним доповненням до інфраструктури безпеки майже кожної організації.

IDPS не можуть забезпечити повністю точне виявлення; всі вони генерують false positivse (невірне визначення доброякісної активності як шкідливої) і false negativse (нездатність ідентифікувати шкідливу активність).

Вибір правильної системи з точки зору компанії залежить від ряду факторів:

– необхідного рівня захисту мережі;
– сфери діяльності компанії;
– підготовки фахівців;
– бюджету організації.

Література

1. Офіційний сайт фірми Snort [Електронний ресурс] // Snort IDPS – 2021 - Режим доступу до ресурсу: https://www.snort.org/.

2. Офіційний сайт фірми Suricata [Електронний ресурс] // Suricata Open Source IDS / IPS / NSM engine – 2021 – Режим доступу до ресурсу: https://suricata-ids.org/.

3. Офіційний сайт фірми OSSEC [Електронний ресурс] // OSSEC HIDS – 2021 – Режим доступу до ресурсу: https://www.ossec.net/.

4. Система обнаружения вторжений на базе IDS Snort [Електронний ресурс] // OpenNET – 2007 – Режим доступу до ресурсу: https://www.opennet.ru/base/sec/snort_ids.txt.html.

5. Системы обнаружения вторжений. Разворачиваем Snort и пишем правила [Електронний ресурс] // Эксплойт – 2018 – Режим доступу до ресурсу: https://telegra.ph/Sistemy-obnaruzheniya-vtorzhenij-Razvorachivaem-Snort-i-pishem-pravila-11-25.