УДК 004.56

Очеретний С. О., здобувач вищої освіти;
Крижановський В. Г., д-р техн. наук., професор,
професор кафедри прикладної математики та кібербезпеки,
Донецький національний університет імені Василя Стуса

СИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕНЬ, НАЙБІЛЬШ УСПІШНІ ПРАКТИКИ

Ключові слова: система виявлення вторгнень, система запобігання вторгнень, захист комп'ютерних мереж, атака, мережева активність, брандмауер, фаєрвол.

Вступ. Сьогодні проблема зростання кіберзагроз є нагальною. Системи виявлення та запобігання вторгнень є центральними інструментами для забезпечення цифрової безпеки суспільства чи організації.

Актуальність. Системи виявлення та запобігання вторгнень (IDPS) є актуальними інструментами для забезпечення безпеки комп'ютерних мереж. Вони аналізують, відстежують і блокують зловмисні або підозрілі дії, що можуть загрожувати конфіденційності, цілісності та доступності даних. Проте для того, щоб ці складники працювали в належний спосіб, потрібно регулярно налаштовувати і поновлювати правила та підписи IDPS.

Системи виявлення вторгнення (IDS) – це засоби, які слідкують за мережевою активністю і виявляють спроби несанкціонованого або шкідливого доступу до комп'ютерних систем або мереж. Вони можуть бути програмними або апаратними, мережевими або хостовими, пасивними або активними. Використовуються різні методи аналізу трафіку, як-от сигнатурний, протокольний, аномальний, поведінковий тощо [1]. Вони мають на меті виявити різні види мережевих атак. Також збирається інформація про події безпеки і сповіщають адміністраторів або інші системи про виявлені загрози.

Одними з найефективніших та найпоширеніших методів виявлення вторгнень (IDS) є такі:

1. Визначення типу системи, яке відповідає потребам організації під час впровадження IDS. Існує два основні типи систем виявлення вторгнень – мережеві (NIDS) та хостові (HIDS).

2. Встановлення чіткого набору цілей. Вони повинні бути узгоджені із загальною стратегією безпеки організації і можуть включати завдання виявлення конкретних типів атак, виявлення спроб несанкціонованого доступу або моніторингу певних сегментів мережі.

3. Вибір відповідного апаратного та програмного забезпечення. Це включає в себе вибір правильних датчиків, які відповідають за моніторинг мережевого трафіку або активності хостів, і консолі управління, яка використовується для аналізу і реагування на попередження, що генеруються датчиками.

4. Контроль та підтримка системи виявлення вторгнень. Це включає перегляд системних журналів і сповіщень, оновлення програмного та апаратного

забезпечення за необхідності, а також проведення регулярних аудитів для виявлення потенційних вразливостей і сфер, що потребують вдосконалення [2].

Запобігання вторгненням – це протидія небезпечному або незаконному доступу до вашої системи. Система запобігання вторгненням контролює та управляє мережевим потоком, щоб забезпечити належне функціонування мережевих пристроїв.

Системи запобігання вторгненням – це додатковий рівень захисту після фаєрволу. Вони призначені для блокування або усунення (залежно від налаштувань після сканування) виявленого вторгнення. Методи їх запобігання:

1. Складення профілю нормальної мережевої активності, оскільки системи запобігання вторгненням працюють на основі виявлення аномального трафіку [3].

2. Розгортання за брандмауером на межі мережі, щоб зменшити навантаження на вашу систему запобігання вторгненням (брандмауер захищає від несанкціонованого трафіку, що надходить у мережу).

3. Налаштування ваших установок на основі звичайного мережевого трафіку (потрібно точно налаштовувати кількість трафіку, дозволеного без сигналізації про подію безпеки) [4].

4. Встановлення кількох систем для захисту внутрішнього трафіку (оскільки не всі загрози є зовнішніми, встановлення внутрішньомережевих пристроїв або програмного забезпечення для запобігання вторгненням є важливою частиною вашого профілю безпеки) [5].

Інструменти IDPS займають важливе місце в мережевій безпеці. Досліджуючи питання IDPS, можна навести приклад інструменту *Snort* з відкритим вихідним кодом. *Snort* використовується для моніторингу мережі на наявність аномалій та потенційних загроз безпеці. Для використання системи необхідне відповідне обладнання, а також установлення та коригування правил, що визначають, як саме вона буде виявляти та реагувати на загрозу.

Snort за замовчуванням є системою виявлення вторгнень (IDS), тому не має великих можливостей для блокування трафіку. Цей інструмент буде найбільш ефективним як частина комплексної системи безпеки [6].

Ще один інструмент IDPS – *Suricata*. Подібно до *Snort, Suricata* – безкоштовний та відкритий вихідний код, швидкий і надійний механізм виявлення мережевих загроз. Ядро *Suricata* може виявляти вторгнення в реальному часі (IDS), має вбудоване запобігання вторгненням (IPS) та моніторинг мережевої безпеки. *Suricata* перевіряє мережевий трафік, використовуючи потужну і велику мову правил та сигнатур, а також потужну підтримку сценаріїв *Lua* для виявлення складних загроз [7].

Security Onion – інтегрована платформа, яка в собі вже містить інструменти *Suricata, Snort, Zeek* та інші. Платформа використовується для виявлення та запобігання вторгненням, моніторингу безпеки та керування журналами. У *Security Onion* можна інтегрувати інші інструменти, завдяки чому можна створити комплексну систему захисту мережі [8].

Висновки

Системи виявлення та запобігання вторгнень (IDS/IPS) є необхідними складниками сучасного інформаційного захисту, сприяючи вчасному виявленню та блокуванню потенційно шкідливої мережевої активності. Впровадження та належна підтримка систем *Snort* та *Suricata* вимагають обґрунтованого підходу, зокрема вибору відповідного типу системи, формулювання конкретних цілей та правил, належний вибір апаратного та програмного забезпечення, а також постійного контролю й аудиту для забезпечення надійного захисту мережі та комп'ютерних систем від можливих загроз. Використання систем IDS та IPS у поєднанні, як у дистрибутиві *Security Onion,* допомагає створити ефективний бар'єр для запобігання атакам та забезпечення безпеки інформаційних ресурсів.

Список використаних джерел

1. Довбешко С. В., Толюпа С. В., Шестак Я. В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. *Сучасний захист інформації.* 2019. № 1(37). С. 6–15. URL: Перегляд Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак (dut.edu.ua)

2. Implementing Intrusion Detection Systems: Best Practices and Tips. URL: https://ts2.space/en/implementing-intrusion-detection-systems-best-practices-and-tips/

3. Where should you implement intrusion prevention systems in your IT infrastructure? URL: https://www.quora.com/Where-should-you-implement-intrusion-prevention-systems-in-your-IT-infrastructure

4. Intrusion Prevention System. URL: https://foresite.com/blog/intrusion-prevention-system/

5. Network intrusion protection system. URL: https://www.techtarget.com/whatis/definition/network-intrusion-protection-system-NIPS

6. Top 10 Intrusion Detection and Prevention System Software in 2022. URL: https://www.spiceworks.com/it-security/vulnerability-management/articles/best-idps-software/

7. Система виявлення вторгнень у комп'ютерну мережу. URL: https://ela.kpi.ua/bitstream/123456789/40953/1/Sokirko_magistr.pdf

8. What is Security Onion, an Open Source Intrusion Detection System (IDS) Tool. URL: https://cybersecuritynews.com/security-onion/