УДК 004.49

ДІАГНОСТИЧНІ ІНСТРУМЕНТИ СИСТЕМ IPS/IDS

Живило Є.О., канд. держ. упр., доцент кафедри комп'ютерних та інформаційних технологій і систем, zhivilka@i.ua, НУ "ПП ім. Ю. Кондратюка"
Дамян М.Ю., студент, kqmaksym1029@gmail.com, НУ "ПП ім. Ю. Кондратюка"
Топчій Ю.П., студент, ggeasywon@gmail.com, НУ "ПП м. Ю. Кондратюка"

Системи запобігання вторгненням та системи виявлення вторгнень є важливими компонентами системи захисту інформації та кібербезпеки електронно-комунікаційних систем/мереж. Система виявлення та запобігання вторгнень (IDPS) фокусується на виявленні потенційних інцидентів, записує інформацію про них, запобігає їм, реєструє інциденти та повідомлення.

Крім того, організації використовують IDPS для інших цілей, а саме: виявлення проблем в політиці безпеки, документування існуючих загроз і стримування окремих осіб від порушення політики безпеки. Активне впровадження та експлуатація зазначених систем спрямована на виявлення та запобігання несанкціонованому доступу до інформації та ресурсів. У цій публікації розглядаються принципи роботи IDS та IPS, їхні відмінності, аспекти впровадження та сучасні тенденції в цій галузі.

***IPS** (Intrusion Prevention System)* – це програмна або апаратна система запобігання вторгнень призначена для активного захисту комп'ютерних систем, мереж та ресурсів від несанкціонованого доступу та атак. Системи IPS можна розглядати як розширення систем виявлення вторгнень (IDS), бо завдання відстеження атак залишається однаковим.

IPS представляє собою:

- Сенсори (Sensors) – це перша лінія оборони, що розташована на мережевому периметрі, вузлах мережі або на кінцевих точках інфраструктури. Сенсори постійно моніторять задля виявлення небезпечних дій у мережевому трафіку.
- Аналізатор (Analyzer) – відповідає за аналіз даних, отриманих від сенсорів, та визначення, чи є ці дії загрозливими, використовуючи різні методи для виявлення підозрілої або загрозливої активності.
- Реагування (Response) – команди реагування на сенсори, що можуть блокувати мережевий трафік, відмовляти у доступі до ресурсів, сповіщення адміністраторів тощо.
- База знань (Knowledge Base) – це централізована база даних, яка містить інформацію про загрози та методи їх виявлення й блокування.

IPS може використовувати такі методи:

- Блокування Пакетів (Packet Blocking) – відхилення пакетів мережевого трафіку, що містять код.

- Відключення Доступу (Access Denial) – відмова у доступі до ресурсів чи сервісів для користувачів чи пристроїв, які можуть бути загрозливими.

- Застосування Виправлень (Patch Application) - автоматичне застосування заходів забезпечення безпеки до системи або програмного забезпечення з вразливостями.

Популярне програмне забезпечення, яке пов'язане з IPS:

- **Suricata** – це некомерційне IPS-програмне забезпечення з відкритим кодом, що аналізує весь мережевий трафік на брандмауері для пошуку відомих атак та загроз, щоб в реальному часі запобігати їм. Дана програма має велику базу сигнатур (*цифрових відбитків*) та правил.

- **Snort** – це IPS-програмне забезпечення, що комерційно розробляється компанією Cisco. Так само як і Suricata аналізує та захищає мережевий трафік у режимі реального часу

- **Fail2Ban** – це IPS-програмне забезпечення, що також аналізує та захищає мережевий трафік у режимі реального часу. Дана програма спеціалізується на захисті від brute-force attacks (*зловмисник підбирає багато паролів, щоб врешті-решт відгадати правильний*).

IDS (*Intrusion Detection System*) – це програмне або апаратне забезпечення, яке спроектоване для виявлення аномальної або потенційно шкідливої активності в мережі чи системі. Основна мета IDS полягає в реєстрації та сповіщенні про можливі вторгнення чи атаки, але вона не має здатності автоматично блокувати ці атаки. IDS реагує на підозрілу активність, виходячи з попередньо визначених правил чи шаблонів поведінки.

Типи IDS:

- Системи виявлення вторгнень на основі сигнатур – використовують базу даних сигнатур, які описують відомі атаки. Перевіряють трафік на відповідність цим сигнатурам. Швидше реагують на відомі загрози, але менш ефективні проти нових атак.

- Системи виявлення аномалій - базуються на аналізі нормальної поведінки системи чи мережі. Виявляють аномалії або незвичайні патерни, які можуть свідчити про атаку. Менш чутливі до нових атак, але можуть виявляти раніше невідомі загрози.

Етапи роботи IDS:

1. Збір інформації – збирає дані про трафік мережі чи події на рівні системи. Використовує різні джерела, такі як системні журнали, пакети даних тощо.

2. Аналіз – використовує різні методи для визначення, що відбувається в мережі чи системі. У сигнатурних системах порівнює трафік із відомими сигнатурами.

3. Сповіщення – якщо IDS виявляє підозрілу або потенційно шкідливу активність, воно генерує сповіщення або занотовує цю подію.

4. Реагування – адміністратори можуть реагувати на сповіщення IDS, вживаючи заходів для запобігання подальших атак або відновлення безпеки системи.

Програмне забезпечення, яке пов’язане з IDS:

1. Snort:

- Відкрите програмне забезпечення для виявлення вторгнень (IDS) та запобігання вторгненням (IPS). Використовує сигнатури для виявлення відомих атак та аномалій в мережі.

2. Suricata:

- Також IDS з відкритим вихідним кодом. Має широкий функціонал, включаючи виявлення атак на різних рівнях мережі.

3. Zeek:

- Мережевий аналізатор, який може використовуватися для виявлення вторгнень. Спеціалізується на аналізі мережевого трафіку та реєстрації подій.

4. Nessus:

- Програмне забезпечення для виявлення та сканування пристроїв, мереж, операційних систем, програмних забезпечень на наявність потенційних загроз.

Як висновок необхідно зазначити, що системи IDS та IPS є важливими інструментами в галузі кібербезпеки. При цьому сучасні системи захисту інформації та кібербезпеки використовують низку методів реагування. Зокрема – використання декількох методів реагування, таких як зупинка самої атаки, зміна середовища безпеки, переналаштування брандмауерів або зміна змісту атаки.

Компоненти зазначених систем забезпечують цілодобове виявлення та запобігання різноманітних інформаційних (м) та кіберзагроз (ам). Розуміння їхніх особливостей, відмінностей та сучасних тенденцій дозволяє ефективно захищати комунікаційні системи та мережі в умовах постійно зростаючих загроз їх сталому функціонуванню.

Список використаних джерел

1. Penetration Testing: A Hands-On Introduction to Hacking, Georgia Weidman // https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf.
2. Protect your network with the world's most powerful Open Source detection software // https://www.snort.org/.
3. What is Suricata? // https://docs.suricata.io/en/latest/what-is-suricata.html.