Кушнір І. В., магістрант,
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ СИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕНЬ SURICATA

Корпоративні комп'ютерні мережі стали невід'ємною частиною сучасних компаній, однак погано захищені мережі є легкою ціллю для зловмисників. Зміна, видалення, крадіжка конфіденційних даних організації можуть призвести до серйозних наслідків, тому питання захисту інформаційних мереж є досить актуальним в наш час.

Для мінімізації загроз доцільне комплексне впровадження підсистем захисту в мережі, що може включати міжмережевий екран, антивірусне програмне забезпечення, VPN тощо. І не менш важливою складовою є система виявлення та запобігання вторгнень, яка дозволяє запобігати виникненню багатьох інцидентів безпеки виявивши та заблокувавши загрози на ранніх етапах появі в мережі.

Система виявлення вторгнень (Intrusion Detection System, IDS) – програмний або апаратний засіб, який аналізує мережевий трафік з метою виявлення атак або шкідливих дій. В залежності від методології IDS перевіряє сигнатури атак, аномальну або нетипову поведінку мережевого трафіку. При виявленні загрози додається відповідний запис в журнал подій для того, щоб вже адміністратор мережі прийняв необхідні заходи для усунення небезпеки. Система запобігання вторгнень (Intrusion Prevention System, IPS) має ті самі можливості IDS і може самостійно приймати активні заходи для блокування або відхилення підозрілого трафіку. Якщо IPS виявляє підозрілу активність, то автоматично застосовуються задані адміністратором правила блокування або відхилення трафіку.

IDS і IPS можуть відрізнятись у способі підключення в інфраструктурі мережі. IDS системи, як правило, встановлюють паралельно мережевому потоку обробляючи копію трафіку, а IPS має бути безпосередньо на шляху проходження трафіку. На практиці ж IPS можна використовувати як IDS, тому часто їх об'єднують в одну назву – IDPS(IDS/IPS). Сучасний ринок може запропонувати ряд популярних некомерційних систем таких як Zeek, Snort та Suricata. Остання система має ряд важливих нововведень та перевага, тому далі мова буде про неї.

Suricata – безкоштовна реалізація мережевої системи виявлення і запобігання вторгнень з відкритим вихідним кодом, яка аналізує і блокує трафік спираючись на набір визначених правил (сигнатур). Підтримується всіма відомими операційними системами і може бути встановлена як на фізичному обладнанні, так і на віртуальних машинах. Перша версія Suricata була представлена в 2010 році, що робить її наймолодшою в порівнянні з іншими конкурентами (Snort – 1998, Zeek – 1995).

Метою початку роботи над Suricata була ціль усунути обмеження пропускної здатності аналізу трафіку. Коли апаратне забезпечення IDPS перевантажене кількістю трафіку система починає пропускати перевірку деяких пакетів, що робить можливим проходження зловмисного трафіку, особливо при DoS-атаках. Тому під час розробки Suricata була використана нова архітектура побудови, яка дозволила використовувати графічний процесор в режимі IDS і багатопоточність при аналізі пакетів, що значно пришвидшило роботу системи. І попри нову архітектуру Suricata все ж може використовувати більшість розроблених правил для Snort.

Крім основних функцій виявлення та блокування загроз даний програмний продукт також надає можливості повноцінною мережевої системи моніторингу, що містить в собі інструменти перехоплення і логування будь-якого трафіку, що буде досить корисним, якщо в мережі наявні платформи для аналізу і візуалізації даних (Splunk, Kibana, Wazuh тощо).

Тож основними перевагами Suricata є: безкоштовна реалізація, відкритий вихідний код, кросплатформеність, висока продуктивність, вбудовані можливості мережевої системи моніторингу, зручна інтеграція з платформами аналізу і візуалізації даних, підтримка автоматичного визначення протоколів (ICMP, HTTP, FTP тощо), готові безкоштовні списки правил.

В доповіді буде представлено використання технології захисту типової корпоративної мережі на основі мережевої системи виявлення та запобігання вторгнень Suricata.

Список використаних джерел

1. All features – Suricata. URL: https://suricata.io/features/all-features/
2. The Other Side of Suricata URL: https://www.stamus-networks.com/blog/the-other-side-of-suricata
3. Suricata User Guide. URL: https://docs.suricata.io