УДК 004.492.3
Жовток О. – ст. гр. СНмп-51
Тернопільський національний технічний університет імені Івана Пулюя

ВИКОРИСТАННЯ СИСТЕМИ ВИЯВЛЕННЯ АТАК SNORT

Науковий керівник: к.т.н., старший викладач Козак Р.О.

Міжмережеві екрани не можуть забезпечити повний захист через наступні причини: помилки або недоліки проектування; недоліки реалізації; недоліки використання. МЕ є “єдиною точкою”, через яку проходять всі з'єднання. Тому будь-яка помилка МЕ можуть привести до проникнення в захищувану мережу.

Ці причини викликали необхідність ведення журналів аудиту, в результаті аналізу яких спеціалісти роблять висновок про здійсненні проникнення. Проведення подібного аналізу ускладнюється безліччю причин, серед яких основними є: величезний об'єм даних журналів аудиту; складність аналізу даних різних журналів; необхідність високої кваліфікації фахівця, який проводить аналіз.

Тому зусилля дослідників направлені на розробку процесів виявлення вторгнень і автоматизацію процесу виявлення. Подібні системи отримали назву систем виявлення атак (вторгнень) (Intrusion Detection Systems).

Система Snort є класичним продуктом з відкритим кодом. Snort – мережева система виявлення атак. Це означає, що система виявляє атаки виключно на основі аналізу мережевого трафіку. Основним методом виявлення атак, використовуваним в системі, є виявлення зловживань на основі опису сигнатур атак. У системі використовується проста мова опису сигнатур атак, яка повністю описана в документації і дозволяє адміністраторам доповнювати базу своїми сигнатурами. Кожне правило на цій мові складається з двох частин: умова використання і дія.

Приклад правила системи Snort: *alert tcp any any -> 10.1.1.0/24 80 (content: "/cgi-bin/phf"; msg: "PHF probe!";)*. Це правило визначає, що будь-який сегмент TCP, направлений на порт 80 на будь-яку адресу в мережі 10.1.1.0/24 і при цьому має в полі даних рядок “/cgi-bin/phf”, є підозрілим і надісилається повідомлення адміністраторові.

Архітектура системи Snort гранично проста і складається з трьох підсистем: декодер пакетів, ядро виявлення і підсистеми сповіщення і реагування. Декодер пакетів реалізує набір процедур для послідовної декомпозиції пакетів відповідно до рівнів мережевого стека. В даний час підтримуються протоколи канального рівня Ethernet, SLIP, PPP. Ядро вибудовує наявні правила в т.з. ланцюги правил – двовимірні послідовності правил, де правила із загальною частиною умов використання об'єднуються в одну ланку ланцюга, а неспівпадаючі компоненти правил будуються ланцюгом в іншому вимірі від отриманої ланки. Це зроблено для прискорення аналізу мережевого трафіку. Кожен пакет проходить по ланцюжку від кореня, і перше відповідне правило виконує свій блок дій і прохід завершується.

Окрім модуля аналізу трафіку на основі правил, до ядра виявлення можуть підключатися модулі сторонніх розробників. За допомогою таких модулів можна додавати функціональності ядру виявлення атак і реалізовувати різні методи виявлення. Крім того, в останніх версіях з'явився модуль статистичного аналізу, який призначений для виявлення аномалій в мережевому трафіку. Підсистема сповіщення і реагування відповідає за збереження результатів аналізу трафіку в журнали реєстрації самої системи Snort, або виведення цієї інформації через системні служби реєстрації подій ОС. Система Snort має реалізації під безліч UNIX платформ, а також під ОС компанії Microsoft.