УДК 004.056.53:004.77

Ю.В. Стасєв[1]
Кіровоградський національний технічний університет

Дослідження систем виявлення та попередження вторгнень у комп'ютерні мережі

Сучасні комп'ютерні мережі потребують високого рівня захищеності від вторгнень (неавторизованого доступу або мережної атаки). Як правило для цього використовуються системи виявлення та попередження вторгнень (IDS/IPS).

Система виявлення вторгнень (СВВ) (Intrusion Detection System) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу (вторгнення або мережевої атаки) в комп'ютерну систему або мережу.

Система запобігання вторгненням (СЗВ) (Intrusion Prevention System)) – програмний або апаратний засіб, який здійснює моніторинг комп'ютерної системи в реальному часі з метою виявлення, запобігання або блокування шкідливої активності.

Проведені дослідження виявили, що IDS все частіше стають необхідним доповненням інфраструктури мережевої безпеки. На додаток до міжмережевих екранів (firewall), робота яких відбувається на основі політики безпеки, IDS служать механізмами моніторингу та спостереження підозрілої активності. Вони можуть виявити атакуючих, які обійшли Firewall, і видати звіт про це адміністратору, який, у свою чергу, зробить подальші кроки щодо запобігання атаки. Технології виявлення проникнень не роблять систему абсолютно безпечною. Проте практична користь від IDS існує і не маленька.

Зазвичай IDS включає: Сенсорну підсистему, призначену для збору подій, пов'язаних з безпекою мережі або системи, що захищається; Підсистему аналізу, призначену для виявлення мережевих атак і підозрілих дій; Сховище, в якому накопичуються первинні події і результати аналізу; Консоль управління, що дозволяє конфігурувати IDS, спостерігати за станом системи, що захищається і IDS, переглядати виявлення підсистемою аналізу інцидентів. За способами моніторингу IDS системи підрозділяються на network-based (NIDS) і host-based (HIDS). Що ж стосується IPS, то вони щодо класифікації та за своїми функціями є аналогічними IDS. Головна їхня відмінність полягає в тому, що вони функціонують в реальному часі і можуть в автоматичному режимі блокувати мережеві атаки. Кожна IPS включає в себе модуль IDS.

Таким чином, розвиток систем виявлення та попередження вторгнень у комп'ютерні мережі є актуальною задачею, яка потребує відповідних програмних та апаратних реалізацій, які можуть модифікуватися з появою нових загроз.

---

[1] доктор технічних наук, професор кафедри програмного забезпечення