УДК 681.03
Улянюк А. – ст. гр. PI-41
Тернопільський державний технічний університет імені Івана Пулюя

СУЧАСНІ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Науковий керівник: к.т.н. Луцків А. М.

Щодня по корпоративних мережах передаються мільярди пакетів даних. Деякі з них небезпечні; автори таких пакетів здійснюють спеціальні заходи, щоб обійти брандмауери. Руйнівна дія таких атак, як Code Red, Nimda, SQL Slammer і MSBlaster, добре відома. Всі ці шкідливі програми використовують в своїх цілях протоколи, яким здебільшого довіряють (наприклад, HTTP) або мережевий трафік систем Microsoft. Такі протоколи не можна просто взяти і заблокувати, тому адміністратори зазвичай прагнуть якомога швидше виявити небезпечний трафік за допомогою систем виявлення вторгнень, Network Intrusion Detection System (NIDS), щоб вчасно зреагувати на загрозу.

IDS (Intrusion-Detection System) – програмний або апаратний засіб, призначений для виявлення вторгнення в комп'ютерну систему або мережу. Існують вузлові IDS (Host Intrusion Detection System – HIDS) і мережеві IDS (Network Intrusion Detection System – NIDS). Системи HIDS розміщуються прямо на клієнтському комп'ютері, а NIDS зазвичай інтегровані в SPAN-порт свіча.

Можна сформулювати наступні характеристики, яким повинна відповідати сучасна система виявлення вторгнень:

- відкритість системи, тобто знання того що система сама не є одним з методів вторгнень;
- гнучкість – здатність конфігуруватися під різні задачі та наявність засобів, які дозволяють адміністратору розширювати функціональність власноручно, а також самому створювати правила виявлення невідомих до цього часу вторгнень;
- підтримка більшості сучасних операційних систем;
- зручність інформування адміністратора про вторгнення;
- велике покриття для моніторингу і в зв'язку з цим централізоване управління (розгалужена інфраструктура із декількох оптимально розміщених NIDS можуть «переглядати» велику мережу);
- можуть функціонувати в оточені, в якому мережевий трафік зашифрований;
- не потребують додаткової функціональності мережевих пристроїв.

На сьогодні на ринку є ціла низка систем виявлення вторгнень, зокрема ці: PortSentry, Snort, Nidsbench, Iplog, Libnids, Slsnif, а також багато інших.

Зі всіх наведених програм, на мою думку, найкращим варіантом є Snort, який легко встановлюється і налаштовується, має невеликий розмір і системні вимоги, можливість виявлення великої кількості атак завдяки великій базі сигнатур відомих атак. Крім можливості створення власних правил, він також дозволяє підключати додаткові програмні модулі.

Варто звернути увагу й на те, що Snort є чудовим інструментом для навчання, оскільки має відкритий вихідний код.