Кожен район обслуговування визначався виходячи з умови, що час реагування ПРП має не перевищувати 20 хв. [2, 3], причому розрахункова швидкість пожежно-рятувального автомобіля становила 30 км/год. Очевидно, що всі об’єкти підвищеної небезпеки та потенційно небезпечні об’єкти знаходяться в районах обслуговування центрів безпеки.

Висновки. Таким чином, маючи в доступі автоматизовані карти графу доріг з точними геоданими, можливо з меншою похибкою вирішувати задачі геометричного моделювання для покриття заданої області.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Комяк В.М. Моделювання покриття опуклими багатокутниками заданої області з дискретними елементами / В.М. Комяк, О.М. Соболь, С.Я. Кравців, І.А. Чуб // Вісник Херсонського національного технічного університету. – Херсон: ХНТУ, 2018. – № 3(66). – Т. 2. – С. 147–152.

2. ДБН 360-92**. Містобудування планування і забудова міських і сільських поселень [Електронний ресурс]. – Режим доступу: https://dnaop.com/html/29810/doc-%D0%94%D0%91%D0%9D_360-92__.

3. Постанова Кабінету Міністрів України від 27.11.2013 р. № 874 «Про затвердження критеріїв утворення державних пожежно-рятувальних підрозділів (частин) Оперативно-рятувальної служби цивільного захисту в адміністративно-територіальних одиницях та переліку суб’єктів господарювання, де утворюються такі підрозділи (частини)» [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/874-2013-%D0%BF#n10.

УДК 004.056.53

ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ РОБОТИ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

М.А. Лоян, С.І. Войцех
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. У сучасному цифровому світі безпека інформації стала надзвичайно важливою частиною процеса обробки, передачі та зберігання даних. В основі концепції безпеки інформації лежить безпека персональних комп'ютерів та мереж зв'язку між ними. В останні роки системи виявлення вторгнень (IDS) та системи профілактики вторгнень (IPS) життєво важливі для комп'ютерних мереж малих та середніх масштабів, в яких існує потреба в захисті конфіденційних даних. Для того, щоб забезпечити безпеку мережі, потрібно контролювати та аналізувати рух трафіку в ній.

Забезпечення безпеки інформації, особливо в комп'ютерних мережах малих масштабів, потребує суттєвих фінансових витрат. Тому актуальною задачею є розробка недорогих та практичних рішень.

Для реалізації поставленої задачі можуть бути використані малоенергетичні мікропроцесорні системи, які мають повноцінні безпекові характеристики і інструменти. Таким комплексом може стати одноплатний мікрокомп’ютер Raspberry Pi у зв'язці з програмним забезпеченням Snort IDS. Цей комплекс може бути розміщений в мережі і працювати як повноцінна система безпеки.

Raspberry Pi - одноплатний мікрокомп’ютер який має характеристики повноцінного комп'ютера при мінімальних розмірах.

IDS Snort є вільним програмним забезпеченням. Snort - це система, яка використовується для виявлення та запобігання вторгнень і може виконувати аналіз протоколів та аномалій в мережі на основі правил. Правила - основа Snort. Вони являються послідовність байтів, сигнатури нападів і даних інших типів, при виявленні яких, генерується попередження. Також, особливістю цієї системи є те, що користувачі можуть вільно додавати свої власні правила безпеки. За допомогою комплексу побудованого на базі Raspberry Pi і Snort можна зробити мережу більш безпечною аналізуючи мережевий трафік.

Snort працює наступним чином :

1. Відбувається прослуховування мережевого трафіку та прийняття пакетів.
2. Пакети аналізуються, із застосування правил до прийнятих даних. Процес застосування правил зводиться до пошуку в пакеті певних сигнатур, послідовностей, які вказані в правилах. Самі правила складаються з опису трафіку, сигнатури, яка шукається, опису загрози і опису реакції на виявлення.
3. При виявлення атаки до журналу подій заноситься попередження щодо загрози та дані сеансу зв’язку.

При побудові та проведенні дослідження ефективності системи виявлення вторгнень,використовувались наступня програмні та аппаратні засоби:

- коммутатор Cisco 2960x,
- мікрокомпьютер Raspberry Pi 3,
- ноутбук,
- серверний комп’ютер,
- операційні системи Debian, Ubuntu та Windows,
- програмний комплекс виявлення вторгнень IDS Snort,
- программа для роботи з мережевим трафіком hping3,
- програмні засоби для логування подій до журналу.

Дослідження продуктивності комплекса проводилося в локальній мережі. Згідно сценарію користувач атакував сервер у мережі пакетами даних за технологією SYN-flood. SYN-flood - один з різновидів мережевих атак типу "відмова від обслуговування", які полягають у відправці великої кількості SYN-запитів (запитів на підключення по протоколу TCP) в досить короткий термін. В процесі експерименту було проведено вимірювання продуктивності комплексу для різної кількості правил безпеки. В процесі експерименту вимірювалась кількість успішно прийнятих пакетів даних в системі для правил, використаних на момент нападу.

Було задіяно від 500 до 12500 правил при кожній атаці. Проведено 1 мільйон пакетних атак. Результати наведені на рисунку 1.

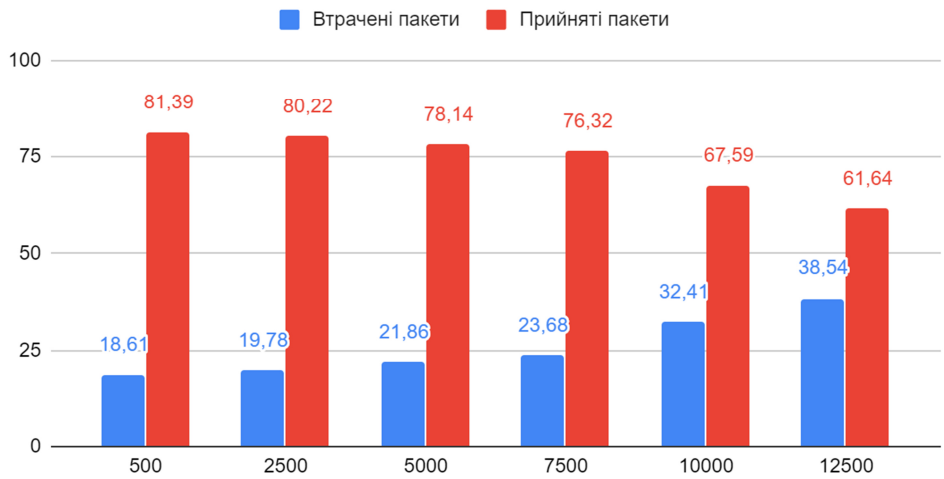

Рис. 1. Відносна кількість успішно прийнятих пакетів даних в системі від кількості правил задіяних на момент нападу

На момент атаки IDS почала працювати з 500 встановленими правилами, при цьому відносна кількість успішно прийнятих пакетів даних була на рівні 82%. При підвищенні кількості правил до 2500 і 5000 продуктивність знизилася на 1% та 3% відповідно. При задіянні 7500 правил продуктивність знизилася на 5%. Нарешті, з реалізацією 12500 правил продуктивність прийняття пакетів знизилась до 61%.

Висновки. Для комплекса, який досліджувався, кількість правил, які задіяні під час роботи, впливає на його продуктивність. При збільшенні кількості правил збільшується час обробки одного пакету даних, що призводить до втрати корисних робочих можливостей прийняття даних та зниження ефективності визначення можливих атак на мережу. Тому для конкретної конфігурації мережі потрібно оцінювати і визначати найвірогідніші атаки і формувати правила для системи на основі цієї оцінки. Намагання захиститися від всіх атак призводить до втрати значної кількості інформації, в тому числі і корисної.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Nabi Z., A $35 Firewall for the Developing World [Електронний ресурс] / Z. Nabi // arXiv. – 2014. – Режим доступу до ресурсу: https://arxiv.org /abs/1405.2517.

2. Ferdoush S. Wireless Sensor Network System Design using Raspberry Pi and Arduino for Environmental Monitoring Applications. The 9th International Conference on Future Networks and Communications / S. Ferdoush, X. Li. // Procedia Computer Science. – 2014. – №34. – С. 103–110.

3. Rolbin M. Early detection of network threats using Software Defined Network (SDN) and virtualization / M. Rolbin. – Ottawa, Canada: Carleton University, 2013. – 43 с.