АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА ДОПОМОГОЮ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Федюшин О.І., Юхименко В.І., Кожушко Д.Р.
Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день для тестування на проникнення існує безліч інструментів, що можуть бути включені до арсеналу фахівця з аудиту інформаційної безпеки, вибір найефективніших із них, стає досить складною задачею. Окрім завищених заявок постачальників, є мало емпіричних досліджень з метою порівняння, щоб проінформувати практикуючих про те, які інструменти можуть бути найбільш ефективними для їх потреб. Отже, головною метою цієї роботи є дослідити діапазон ефективності інструментів пен тестування з точки зору часу відгуку та охоплення. В роботі розглядається впровадження мережних систем виявлення вторгнень (NIDS) [1, 2] з відкритим кодом для отримання та збереження мережних цифрових доказів («відбитків») при робочих навантаженнях.

Архітектура запропонованої системи складається з двох мереж: перша є модельованою мережею Інтернету, друга – виробничою мережею. Кожна мережа має певні компоненти. Інтернет-мережа включає чотири машини, що виробляють трафік, і одну машину, що виробляє міжсайтові сценарії та атаки SQL-ін'єкцій проти веб-сервера [3]. Виробнича мережа складається з веб-сервера з вразливим веб-додатком для пропонованих атак, брандмауера з NIDS, включаючи Snort, Suricata та Bro-IDS, і, нарешті, Forensic-сервера. Як результат, запропонована система працює для моніторингу та криміналістичного вивчення переданого трафіку між обома мережами.

Отримані дані демонструють, що запропоновані NIDS можна використовувати як джерело цифрових доказів. Захоплені пакети, а також попередження, генеровані цими NIDS, можуть бути використані як сліди доказу відтворених атак. Однак вони мають проблеми доставки пакетів до своїх інтелектуальних аналізаторів. Проблема значною мірою пов’язана з функціями перехоплення, і ці функції потрібно вдосконалити, щоб усунути проблему. У дослідженні були написані сценарії для підвищення продуктивності інструментів та можливості збереження цифрових доказів. Результати експериментів показали, що запропонована конструкція системи може виконати багато завдань, включаючи отримання та збереження мережного трафіку VLAN як цінного джерела цифрових доказів.

Список літератури

1. Khraisat, A., Gondal, I. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur 2, 20(2019). DOI: https://doi.org/10.1186/s42400-019-0038-7.

2. О.В. Сєвєрінов, А.Г. Хрєнов. Аналіз сучасних систем виявлення вторгнень. Системи обробки інформації, 6 (2014): 122-124.

3. О.В. Сєвєрінов, А.Г. Хрєнов. Аналіз сучасних методів атак на електронні ресурси органів військового управління. Наука і техніка Повітряних Сил Збройних Сил України, 3 (2015): 125-128.