УДК 004.75

АЛГОРИТМИ СКАНУВАННЯ ПОРТІВ У КОРПОРАТИВНІЙ КОМП'ЮТЕРНІЙ МЕРЕЖІ

Довгий В.В., Небесний І. В.
Тернопільський національний економічний університет, магістранти

І. Постановка задачі

В Інтернеті щодня з'являється нове шкідливе програмне забезпечення. У зв'язку з цим захист персональних комп'ютерів і цифрових активів стає важливою задачею. Першою фазою більшості комп'ютерних атак є розвідка. Одним із механізмів здійснення розвідки є сканування портів, яке дозволяє зловмисникові з'ясувати, які сервіси працюють в цільовій системі, а значить, підготувати і провести цілеспрямовану атаку проти виявлених сервісів і їх вразливостей. Отже, боротися з розвідкою, у вигляді сканування портів, є актуальною задачею.

ІІ. Мета роботи

Метою роботи є аналіз алгоритмів сканування портів у корпоративній комп'ютерній мережі.

ІІІ. Алгоритми сканування портів

Сканування портів - це набір процедур, що дозволяють зловмисникові ідентифікувати вузли мережі, включаючи імена пристроїв, IP-адреси, операційні системи, програмне забезпечення та служби, імена користувачів, групи та відкриті порти і сервіси цільової системи [1]. Сканування звичайно виконують до початку атаки. Існують багато різних підходів до сканування мережевих портів, зокрема: 1) горизонтальне сканування –зловмисник переглядає один і той же порт на декількох комп'ютерах; 2) вертикальне сканування – зловмисник сканує кілька портів на одному комп'ютері; 3) розподілене вертикальне сканування – кілька джерел послідовно сканують кілька портів на одному IP-адресу; 4) розподілене горизонтальне сканування – кілька джерел сканують один і той же порт на декількох IP-адреси послідовним чином.

Механізми сканування портів засновані на спробі пробного підключення до портів TCP і UDP досліджуваного комп'ютера з метою визначення запущених служб і відповідних їм портів, серед таких механізмів найбільш поширені наступні [1]:

– TCP-сканування підключенням (TCP connect scan) – полягає в спробі підключення по протоколу TCP до потрібного порту з проходженням повної процедури узгодження параметрів з'єднання (процедура handshake), що полягає в обміні службовими повідомленнями (SYN, SYN / ACK, ACK) між вузлами мережі;

– TCP-сканування за допомогою повідомлень SYN (TCP SYN scan) – досліджуваному порту надсилається повідомлення SYN, якщо у відповідь приходить повідомлення SYN / ACK, то це означає, що порт знаходиться в режимі прослуховування.

– TCP нуль-сканування (TCP Null scan) – здійснюється відправка пакетів з відключеними прапорцями. Досліджуваний вузол у відповідь повинен відправити повідомлення RST для всіх закритих портів;

– TCP-сканування за допомогою повідомлень ACK (TCP ACK scan) – дозволяє встановити набір правил, використовуваних брандмауером, і з'ясувати, чи виконує брандмауер розширену фільтрацію пакетів;

– UDP-сканування (UDP scan) – полягає у відправці пакетів по протоколу UDP, якщо у відповідь надходить повідомлення, що порт недоступний, то це означає, що порт закритий. При відсутності такої відповіді можна припустити, що порт відкритий.

Для захисту від сканування портів необхідно налаштувати брандмауер і відключити всі невикористовувані служби.

Висновок

У роботі проведено аналіз підходів та методів сканування портів у корпоративній комп'ютерній мережі.

Список використаних джерел

1. Singh, R. R., Tomar, D. S. Port Scanning Attack Analysis with Dempster-Shafer Evidence Theory. International Journal of Applied Engineering Research, *12*(16), 2017, pp.5900-5904