УДК 621.396.662.072.078

СКАНУВАННЯ ПОРТІВ МЕРЕЖЕВИХ ОБ'ЄКТІВ

Коростенський А.Б.
Тернопільський національний економічний університет, магістр

II. Вступ

Локальна обчислювальна мережа є незамінним атрибутом інформаційної підтримки будь-якої великої фірми, підприємства чи організації. Незалежно від потужності мережі, що нараховує від декількох комп'ютерів до сотень робочих станцій, вона має потребу в щоденному моніторингу, сервісному обслуговуванні, тестуванні робочих режимів функціонування, діагностуванні виникаючих відмовлень і несправностей. Використання сервісних засобів надає досвідченому адміністратору інформацію для визначення місця, причини і вигляду дефекту, якщо мережа досить проста і містить невелику кількість робочих станцій. Для мереж, що містять десятки і сотні комп'ютерів, з розвиненою структурою і різними технологіями виконання проблема формалізації діагностичного експерименту і його реалізації з метою контролю і пошуку дефектів є досить актуальною [1].

II. Мета роботи

Метою дослідження є розробка програмного засобу для моніторингу мережевого середовища зв'язку для підвищення захисту локальної комп'ютерної мережі.

III. Особливості моніторингу мережевого середовища зв'язку

Одним із засобів моніторингу стану об'єктів мережі є мережевий сканер, який призначений для сканування мереж з будь-якою кількістю об'єктів, визначення стану об'єктів, а також портів і відповідних їм служб. На сьогоднішній день налічується декілька десятків програмних продуктів, які здатні виконувати сканування мережі, однак більшість з них комерційні, що обмежує їх повноцінне використання.

Принцип роботи мережевих сканерів полягає в наступному:

1. Комп'ютер з встановленим на ньому сканером підключається до мережі.

2. В заданому діапазоні IP-адрес проводиться пошук доступних мережевих ресурсів, ідентифікація мережевих сервісів та аналізується їх захищеність.

3. За результатами сканування автоматично формується звіт про стан захищеності кожного мережевого ресурсу, виявлені недоліки в системі захисту та оцінці небезпеки, з точки зору використання цих недоліків для проникнення в систему.

Отримавши звіт від мережевого сканера адміністратор мережевого ресурсу може через мережу Інтернет спробувати знайти необхідні засоби захисту від потенційних загроз. І робити це потрібно негайно, тому що точно також проаналізувати доступність мережевих ресурсів може і зловмисник. А потім визначити, через яку «дірку» і як можна пролізти в систему.

Висновок

У роботі розроблено мережевий сканер портів з відкритим доступом, який дає змогу сканувати відкриті порти мережевих об'єктів та відповідних їм служб. Для цього використовується TCP SYN та ICMP (ping) методи сканування. Результатом роботи програми є список сканованих портів віддаленої машини із зазначенням номера та стану порту, типу використовуваного протоколу а також назви служби, закріпленої за цим портом.

Необхідно відмітити, що наявність інформації про результати сканування мережі істотно полегшують адміністратору вирішення багатьох проблем, включаючи ті, що пов'язані з інформаційною безпекою і продуктивністю, дозволяють визначити потенційні загрози та сформувати індивідуальну політику комп'ютерної безпеки.

Список використаних джерел

1. Камер Д. Разработка приложений типа клиент/сервер / Д. Камер, Л. Стівенс. - Киев: Издательский дом «Вильямс», - 2002. - 592 с.