МЕТОДИ ЗАХИСТУ ВІД СНІФІНГУ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Ковтун Р.О., к.ф-м.н., доц. Черних О.П.
Національний технічний університет «ХПІ», Харків

У сучасних комп'ютерних мережах існує ризик сніфінгу (перехоплення та аналізу мережевого трафіку сторонніми особами). Основними методами захисту від сніфінгу є:

– аутентифікація;
– комутована інфраструктура;
– антисніфери;
– криптографія.

Аутентифікація. Прикладом є система одноразових паролів, де необхідно мати «токен» (апаратний або програмний засіб, що генерує унікальний одноразовий пароль). Якщо хакер дізнається даний пароль за допомогою сніфера, то ця інформація буде марною, оскільки в цей момент пароль вже буде використаний. Цей спосіб боротьби зі сніфінгом ефективний тільки в випадках перехоплення паролів.

Комутована інфраструктура. Ще одним способом боротьби зі сніфінгом пакетів є створення комутованої інфраструктури. Якщо, наприклад, у всій організації використовується комутований Ethernet, хакери можуть отримати доступ тільки до трафіку, що надходить на той порт, до якого вони підключені. Комутована інфраструктура не усуває загрози сніфінгу, але помітно знижує його доцільність.

Антисніфери. Даній спосіб боротьби зі сніфінгом полягає в установці апаратних або програмних засобів, які розпізнають сніфери, що працюють у вашій мережі. Антисніфери вимірюють час реагування хостів і визначають, чи не доводиться хостам обробляти зайвий трафік.

Криптографія. Це найефективніший спосіб боротьби зі сніфінгом пакетів. Хоча він не запобігає перехопленню і не розпізнає роботу сніферів, але робить цю роботу марною. Якщо канал зв'язку є криптографічно захищеним, то хакер перехоплює не вихідне повідомлення, а зашифрований текст (незрозумілу послідовність бітів). Для створення захищеного зв'язку між пристроями використовуються протоколи, IPSec, SSH (Secure Shell) і SSL (Secure Socket Layer).

Для підвищення ефективності захисту від сніфінгу у комп'ютерних мережах можна використовувати перераховані методи разом.