ВИКОРИСТАННЯ СНІФЕРУ ДЛЯ «ПРОСЛУХОВУВАННЯ» МЕРЕЖЕВОГО ІНТЕРФЕЙСУ

Ковтун Р.О., Черних О.П.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Комп'ютерні мережі – це невід'ємна складова сьогоденного життя. Ледве не всі комп'ютери та інша обчислювальна техніка контактують між собою за допомогою об'єднання в мережі, передаючи велику кількість інформації, як корисної користувачеві, так і службової. Нажаль, іноді виникають проблеми перенавантаження або некоректної роботи мережі. Для пошуку джерела цієї проблеми дуже зручно використовувати сніфери.

Сніфер – це програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу трафіку, призначеного для інших вузлів.

Перехоплення трафіку може здійснюватися:

– «прослуховуванням» мережевого інтерфейсу;

– підключенням сніфера в розрив каналу;

– відгалуженням (програмним або апаратним) трафіку і спрямуванням його копії на сніфер;

– через аналіз побічних електромагнітних випромінювань;

– через атаку на канальному або мережевому рівні, що приводить до перенаправлення трафіку на сніфер з подальшим поверненням трафіку в належну адресу.

«Прослуховування» мережевого інтерфейсу (наприклад, мережевої карті) є найпростішим і найдоступнішим методом перехоплення трафіку.

Програмний сніфер перехоплює і відображає усі пакети, що проходять через обраний інтерфейс. Це і є «прослуховуванням». Прикладами таких сніферів для Windows є програми Cain & Abel, Wireshark, Windump та ін.

Сніфер зчитує і виводить "службову інформацію" з перехоплених пакетів, таку як: протокол, джерело відправки, отримувача, TTL та ін. Аналіз цієї інформації (автоматичний або ручний) дозволяє:

– виявити паразитний, вірусний і закільцьований трафік, наявність якого збільшує завантаження мережного устаткування і каналів зв'язку;

– виявити в мережі шкідливе і несанкціоноване ПЗ, наприклад, мережеві сканери, флудери, троянські програми, клієнти пірінгових мереж та інші;

– локалізувати несправність мережі або помилку конфігурації мережевих налаштувань.

Подальший аналіз та систематизація отриманих результатів дозволяє користувачеві або системному адміністратору вжити необхідних заходів для оптимізації роботи мережі (наприклад, зменшити обсяг службової інформації, використавши спуфінг) або виявлення та знешкодження шкідливого ПЗ.