Автор:
Баранов Сергій Сергійович,
студент 31ІА І групи
Науковий керівник:
Франчук Василь Михайлович,
кандидат педагогічних наук,
доцент кафедри комп'ютерної інженерії

ПЕРЕХОПЛЕННЯ МЕРЕЖЕВОГО ТРАФІКА. МЕРЕЖЕВИЙ СНІФІНГ

Анотація. Метою дослідження є вивчення способів перехоплення мережевого трафіка зловмисником на прикладі використання мережевого сніфінгу. Завданням дослідження є аналіз способів повного чи часткового уникнення перехоплення мережевого трафіку. Методом дослідження є огляд відомостей на основі досвіду вчених у галузі захисту комп'ютерних систем. Об'єкт дослідження: комп'ютерні мережі. Предметом дослідження є процес перехоплення пакетів даних у мережі та стратегії застосування мережевого сніфінгу. Результатом дослідження є методи захисту від дій зловмисника направлених на перехоплення пакетів даних.

Ключові слова: Мережевий захист, перехоплення мережевого трафіку, сніфінг, сніфер, аналіз трафіку, сніфінг пакетів.

Вступ. З розповсюдженням використання комп'ютерних мереж та входженням їх у наше життя виникає небезпека перехоплення персональних даних, що передаються каналами зв'язку, зловмисником для власних цілей.

Постановка задачі. Щодня користувачі мереж передають велику кількість даних, серед яких і персональні дані, доступ до яких може бути отриманих зловмисником для здійснення шкідливих операцій з ними. Тому існує проблема інформування людей про можливість перехоплення повідомлень та методи профілактики, для уникнення таких ситуацій.

Мета роботи. Метою дослідження є методи перехоплення мережевого трафіка на прикладі мережевого сніфінгу.

Основна частина.

Перехоплення мережевих даних являє собою найбільш ефективний метод мережевого шпигунства, що дозволяє ініціатору мережевого дослідження отримати практично всі дані, що передають каналами зв'язку.

Найбільший практичний розвиток отримали засоби сніфінга, тобто прослуховування мереж; однак не можна обійти увагою і методи перехоплення мережевих даних, що виконуються за допомогою втручання в нормальне функціонування мережі з метою перенаправлення трафіка на адресу зловмисника, в особливості методи перехоплення TCP-з'єднань[1].

Класифікувати методи перехоплення мережевих даних можна за наступною схемою. (рис.1).

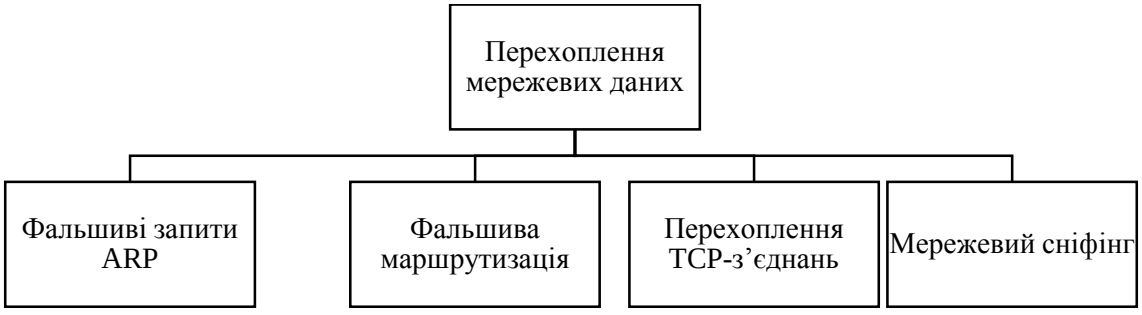

Рис.1.Методи перехоплення мережевих даних

Фальшиві запити ARP (Address Resolution Protocol - Протокол дозволу адрес). Для перехоплення мережевого трафіка між вузлами А і В перехоплювач задає цим вузлам свою IP-адресу, щоб А і В використовували цю фальсифіковану IP-адресу при обміні повідомленнями.

Фальшива маршрутизація. Для перехоплення мережевого трафіка між вузлами А і В перехоплювач задає цим вузлам свою IP-адресу, щоб А і В використовували цю фальсифіковану IP-адресу при обміні повідомленнями.

Перехоплення TCP-з'єднання. Перехоплювач, шляхом генерації і відсилання на атакований вузол TCP-пакетів, перериває поточний сеанс зв'язку з вузлом. Далі, користуючись можливостями протоколу TCP з відновленням перерваного TCP-з'єднання, він перехоплює перерваний сеанс зв'язку і продовжує його замість відключеного клієнта.

Мережевий сніфінг. Для сніфінга мереж, зазвичай, використовуються мережеві карти, що переведені в режим прослуховування. Прослуховування мережі вимагає підключення комп'ютера із запущеною програмою-сніфером до сегмента мережі, після чого ініціатору інформаційного дослідження стає доступним весь мережевий трафік, що відправляється і отримується комп'ютерами в даному мережевому сегменті. Ще простіше виконати перехоплення трафіка радіо-мереж, що використовують бездротові мережні посередники, – в цьому випадку не потрібно навіть шукати місце для підключення до кабелю.

Сніфер – програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережного трафіку, призначеного для інших вузлів[1].

Перехоплення трафіку може здійснюватися:

- звичайним «прослуховуванням» мережевого інтерфейсу (метод ефективний при використанні в сегменті концентраторів (хабів) замість комутаторів (світчей);
- підключенням сніфера в розрив каналу;
- відгалуженням (програмним або апаратним) трафіку і спрямуванням його копії на сніфер;
- через аналіз побічних електромагнітних випромінювань і відновлення трафіку, що таким чином прослуховується;

Організація «прослуховування» каналу передачі даних може бути виконана за наступною схемою (рис.2).

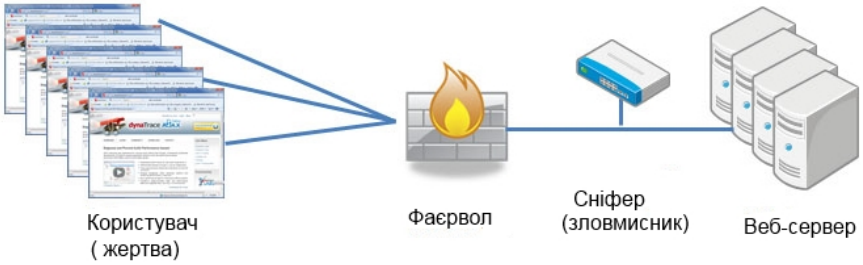

Рис.2.Схема організації підключення сніфера до мережі

При використанні такого методу використання захисту не впливає на перехоплення пакетів даних від користувача до серверу, адже зловмисник має змогу підключити пристрій безпосередньо до каналу передачі даних. Але головним мінусом такого методу є те, що зловмисник повинен мати фізичний доступ до каналу зв'язку (підключення сніфера в розрив каналу).

Існує інший спосіб організації «прослуховування» каналу за наступною схемою (рис.3).

Рис.3.Схема бездротової організації підключення сніфера

Використання такого методу є найнебезпечнішим для користувачів, адже за допомогою мережевої карти у режимі сніфера, використовуючи додаткове програмне забезпечення, перехоплюються усі пакети даних, що надсилаються для подальшого опрацювання wi-fi роутером.

Дослідивши схеми організації підключення сніфера, легко бачити, що обмін даними клієнта з сервером має ряд загроз перехоплення мережевого трафіку. Але отримання пакетів з даними користувачів не означає, що зловмисник зможе отримати усі дані що передавались у розшифрованому вигляді. Тому слід звернути увагу на такі методи захисту перехоплення мережевого трафіку:

1. Основним методом захисту даних є їх шифрування, тобто використання криптографічних методів захисту. Адже перехоплення пакетів зловмисником за допомогою додаткових засобів відносно просто, а їх інтерпретація (огляд вмісту) може бути складним процесом.
2. Використання VPN (Virtual Private Network, Віртуальна приватна мережа) мережі. VPN - це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж. Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну даними.
3. Використання захищених протоколів передачі даних (наприклад HTTPS).

Висновок. Кожна мережа не може бути абсолютно захищеною, адже завжди існує ризик перехоплення даних. Сніфінг є дуже небезпечним методом «прослуховування» мережі, адже у перехоплених пакетах даних можуть міститися конфіденційні відомості, якими може скористуватися зловмисник. Тому при організації мережі, важливо використовувати усі доступні методи захисту, особливу увагу слід приділити використанню криптографічних методів, адже навіть отримавши пакети даних користувача, зловмиснику буде потрібно більше часу для їх розшифрування.

Список використаних джерел.

1. Любарський С.В. Місце та роль мережевої розвідки в моделях інформаційного протиборства / Збірник наукових праць ВІТІ НТУУ „КПІ” № 1 – 2013
2. Перехват сетевых данных [Electronic resource] / alex-shtilev.narod.ru /. – 2014. – Mode of access : http://alex-shtilev.narod.ru/diplom/glava16.html
3. Захист інформаційних ресурсів / Василь Франчук. – К.: Редакції газет природничо-математичного циклу, 2012. – 112с. – (Бібліотека «Шкільного світу»).