ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ПЕРЕХОПЛЕННЯ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ З РОЗРОБКОЮ БЛОКУ ЗАХИСТУ

Власенко Т.О., Радіонов Р.О.
Харківський національний університет внутрішніх справ, Харків, Україна

На сьогоднішній день методи перехоплення інформації набули вдосконалення та розширення [1, 2]. Однією з таких загроз є перехоплення даних за допомогою проксі-серверів. Проксі-сервери можуть бути налаштовані для прослуховування мережевого трафіку, і в разі недостатнього захисту можуть надати можливість зловмиснику отримати доступ до конфіденційних даних. Ще однією загрозою є перехоплення даних через використання підписаного сертифікату браузера. Це може виникнути внаслідок компрометації самого сертифікату або атак на центри видачі сертифікатів. Атаки цього типу дозволяють зловмисникам встановити довіру до шкідливого сертифікату та отримати доступ до зашифрованого трафіку. Важливо ретельно аналізувати ці методи перехоплення, оскільки вони можуть мати серйозні наслідки для безпеки конфіденційної інформації.

Ефективний захист від перехоплення інформації вимагає комплексного підходу та використання передових технологій та засобів безпеки. Однією з ключових технологій є шифрування даних. Використання сучасних алгоритмів шифрування, таких як AES (Advanced Encryption Standard), гарантує, що дані залишаються конфіденційними під час передачі по мережі. Важливим компонентом є використання віртуальних приватних мереж (VPN), які створюють шифровану тунель для безпечної передачі даних. Крім того, важливо мати механізми для перевірки аутентичності сертифікатів SSL/TLS та виявлення можливих атак з використанням підписаних сертифікатів браузера. Системи моніторингу та аналізу трафіку можуть виявити надзвичайні події.

Розробка надійного блоку захисту від перехоплення інформації є невід'ємним кроком у забезпеченні безпеки мережевого оточення.

Висновок. Дослідження методів та засобів перехоплення інформації та розробка блоку захисту є ключовими аспектами для забезпечення безпеки мережі та захисту конфіденційної інформації. У світі, де обмін даними відіграє критичну роль, ефективні засоби та технології захисту є невід'ємними для забезпечення безпеки та довіри.

Продовжуючи дослідження та впровадження нових заходів безпеки, ми зможемо створити мережеве середовище, яке залишається надійним та захищеним у цифровій епохі.

Список літератури

1. Комп'ютерні мережі. Таненбаум Е. С., Уезеролл Д. С.792–793.
2. Куперштейн Л. М., Кренцін М. Д. Аналіз тенденцій розвитку пірингових мереж. Вісник Хмельницького національного університету. 2021. № 4. С. 25–29.