УДК 004.77; 004.71
Рак В. – ст. гр. СНс-43
Тернопільський національний технічний університет імені Івана Пулюя

ВИДИ АТАК В ЛОКАЛЬНИХ МЕРЕЖАХ

Науковий керівник: асистент Маєвський О.В.

З розвитком інформаційних технологій і проникненням їх в усі сфери сучасного життя росте число зловмисників, які активно ці технології використовують. Інформація з'являється на основі подій навколишнього світу. Інформація результат двох речей – сприйнятих подій (даних) і команд, необхідних для інтерпретації даних і зв'язування з ними значень. В даний час під словосполученням «атака» розуміється «замах на систему безпеки». Атака в широкому сенсі слова (початковий зміст) - мозковий штурм, спрямований на знаходження шляху вирішення складних завдань. В результаті мозкового штурму можуть бути придумані нетрадиційні методи вирішення проблеми або внесені оптимізуючі коригування у вже існуючі методи. Атака на інформацію – це навмисне порушення правил роботи з інформацією. Атаки настільки ж різноманітні, як різноманітні системи, протии яких вони спрямовані.

Методи атак:

- *Атака листами.* Вважається найстарішим методом атак, хоча суть її проста й примітивна: велика кількість листів унеможливлюють роботу з поштовими скриньками, а іноді і з цілими поштовими серверами. Цій атаці складно запобігти, тому що провайдер може обмежити кількість листів від одного відправника.

- *Rootkit та інші спеціальні програми.* Наступний вид атак є більш витонченим методом отримання доступу до закритої інформації - це використання спеціальних програм для ведення роботи на комп'ютері жертви, а також подальшого поширення (це віруси і черв'яки).

- *Сніффінг пакетів.* Також досить поширений вид атак, в основу якого покладено роботу мережевої карти в режимі promiscuous mode, а також monitor mode для мереж Wi-Fi. У такому режимі всі пакети, отримані мережевою картою, пересилаються на обробку спеціальним додатком, який називається сніффером. У результаті зловмисник може отримати велику кількість службової інформації: хто звідки куди передавав пакети, через які адреси ці пакети проходили.

- *IP-спуфінг.* Також поширений вид атак в недостатньо захищених мережах, коли зловмисник видає себе за санкціонованого користувача, перебуваючи у самій організації, або за її межами. Така атака можлива, якщо система безпеки дозволяє ідентифікацію користувача тільки за IP-адресою і не вимагає додаткових підтверджень.

- *Man-in-the-Middle.* З англ. «Людина посередині». Коли зловмисник перехоплює канал зв'язку між двома системами, і отримує доступ до всієї передаваної інформації. Мета такої атаки - крадіжка або фальсифікація переданої інформації, або ж отримання доступу до ресурсів мережі. Тому в чисто технічному плані убезпечити себе можна лише шляхом криптошифрування переданих даних.