УДК 004.77: 004.491
Дацер С. – ст. гр. СНм-51
Тернопільський національний технічний університет імені Івана Пулюя

АНАЛІЗ МЕРЕЖ ЗА ДОПОМОГОЮ СКАНУЮЧИХ ПРОГРАМ

Науковий керівник: асистент Маєвський О.В.

За допомогою скануючої програми зловмисник може визначити структуру захищуваної програми: IP-адреси (комп'ютерні системи), користувачів і служби.

Аналіз мереж і комп'ютерних систем.

Існує декілька типів скануючих програм для збору інформації про систему, що є потенційними цілями для майбутніх атак. Скануюче програмне забезпечення використовується для пошуку потенційно слабких місць в системах безпеки систем:

– Комп'ютерні системи. Аналізуються активні IP-адреси (наприклад, за допомогою команди ping). Зловмисник розсилає команди ping на всі IP-адреси в певному діапазоні. В мережах класу С це означає, що команда ping відсилається на IP - адреси в діапазоні від A.B.C.1 до A.B.C.254. З отриманих відповідей, зловимсник визначає, яка IP-адреса відповідає підключеній комп'ютерній системі.

– Активні користувачі. За допомогою команди finger зловмисник може визначити, які користувачі активні в комп'ютерній системі в заданий час, чи прочитали вони вже отриману пошту і так далі.

– Активні служби. Адресуючись до окремих портів, зловмисник може аналізувати, які служби встановлені у відповідній комп'ютерній системі.

Аналіз уразливості окремих комп'ютерних систем.

За допомогою додаткових засобів аналізу, таких як пакети ISS або SATAN, зловмисники можуть провести цільовий аналіз уразливості. Цей аналіз включає перевірку можливості атаки на комп'ютерну систему, наприклад, внаслідок помилок налаштування процесів-демонів активних служб за рахунок використання старих версій програмного забезпечення, що містять помилки.

Використання виявлених вузьких місць.

Наступною дією, виконаною зловмисником, є використання виявлених ним вузьких місць.

Як допомагає брандмауер-система?

Оскільки брандмауер контролює обмін даними по мережі, він теж може бути підданий перевіркам скануючого програмного забезпечення. Більшість брандмауерів розпізнає операції сканування і автоматично блокує будь-який доступ до мережі для джерела сканування. Це блокування ускладнює зловмисникові виявлення вузьких місць. Існують технології, такі як NAT і прикладні проксі-агенти, що дозволяють надавати зловмисникові помилкову інформацію.

Якщо працює брандмауер-система, що приховує структуру внутрішньої мережі, можливості аналізу захищеної мережі зменшуються. Зловмисник може аналізувати тільки IP-адресу брандмауер-системи і визначати, які служби проходять через брандмауер-систему після аутентифікації.

В цьому випадку визначення кількості комп'ютерних систем, підключених до захищеної мережі (1, 10, 100 або 1000), і активізованих служб на цих комп’ютерних системах сильно ускладнюється. Сповільнюється процес збору інформації, що, у свою чергу, надає більше можливостей для адекватної реакції на активність зловмисника.