УДК 004.728.3.057
Карнаухов А.К. – ст. гр. СНмс-61
*Тернопільський національний технічний університет імені Івана Пулюя*

## ОСНОВНІ ПРИНЦИПИ СКАНЕРІВ БЕЗПЕКИ

Науковий керівник: асистент Маєвський О.В.

Сканер безпеки — це програмний або програмно-апаратний засіб, призначений для автоматизації процедури виявлення уразливостей комп'ютерних систем. Його головною функцією є з'ясування версій встановленого програмного забезпечення і помилок конфігурації, у тому числі в політиці паролів. Для цього сканер безпеки виявляє доступні на вузлі мережеві служби, намагається підключитися до них, а після цього — провести відповідний набір тестів.

Алгоритм роботи сканера безпеки полягає в наступному: оператор задає деякий набір IP-адрес або DNS-імен вузлів, які необхідно просканувати. Після цього сканер проводить перевірку доступності цього вузла, потім ідентифікує відкриті порти і визначає запущені мережеві сервіси.

Основним компонентом сканера безпеки є база уразливостей. Використовуючи її, сканер намагається перевірити вразливості мережевих сервісів, по черзі застосовуючи тести, які відповідають для цього вибраного сервісу. Сканери безпеки можуть проводити виявлення уразливостей не лише в мережевих сервісах, але і в ОС, в локальних сервісах і застосуваннях. Після завершения сканування всі зібрані дані об'єднуються в звіти різної форми. Аудитор може включати ці звіти в документи, які описують результати інструментальної перевірки.

При використанні сканерів безпеки аудитор повинен дотримуватися підвищеної безпеки, оскільки при тестуванні вони можуть реалізувати атаки на вразливі системи, що може спровокувати порушення нормальної працездатності системи.

Сканер безпеки не намагається «зламати» обстежуваний вузол, проте здійснювані тести можуть бути небезпечними в тому плані, що здатні викликати відмову в обслуговуванні. Крім того, деякі сканери, такі як LANguard Network Security Scanner, дозволяють виконувати атаку «віддалений підбір пароля» для доступу до спільних файлів і папок (в ОС сімейства Windows NTxxx це еквівалентно атаці на обліковий запис користувача).

Проаналізуємо роботу сканера Nessus. Програмна частина Nessus є вільно поширюваною, проте має ряд обмежень. Безкоштовна версія може застосовуватися лише для сканування вузлів в підмережах класу С.

Структурно Nessus складається із серверної частини, клієнтської частини і набору модулів. Серверна частина забезпечує взаємодію з мережевим середовищем, запуск вибраних тестів, а також отримання і первинну обробку їх результатів. Під'єднувані модулі — це сценарії тестів, написані на мові NASL (Nessus Attack Scripting Language). Клієнтська частина забезпечує взаємодію користувача з сервером, вибір і налаштування тестів, а також генерацію звітів. Обмін між клієнтською і серверною частинами ведеться по прикладному протоколу NTP (Nessus Transport Protocol) і може бути як відкритим (без шифрування трафіка), так і закритим (з шифруванням по протоколу SSL або TLS).

Головною особливістю сканера безпеки Nessus є відкритість сценаріїв тестування і можливість написання користувачем своїх власних сценаріїв або доопрацювання існуючих. Цим Nessus кардинально відрізняється від переважної більшості комерційних сканерів, програмний код яких являється на 100 % закритим.