УДК 004.77
Рак А.К. – ст. гр. СНм-51
Тернопільський національний технічний університет імені Івана Пулюя

ОСОБЛИВОСТІ DOS- і DDOS-АТАК

Науковий керівник: асистент Маєвський О.В.

DOS-атака ("відмова в обслуговуванні") і DDOS-атака ("розподілена відмова обслуговування") – це різновиди атак зловмисників на комп'ютерні системи. Мета – створення таких умов, при яких користувачі системи не зможуть отримати доступ до ресурсів системи, або цей доступ ускладнений.

DDOS-атака виглядає так: на обраний в якості жертви сервер поступає велика кількість помилкових запитів з комп'ютерів з різних кінців світу. В результаті сервер витрачає всі свої ресурси на обслуговування цих запитів і стає практично недоступним для звичайних користувачів. Програми, які встановлені зловмисниками на цих комп'ютерах, прийнято називати "зомбі". Відома велика кількість шляхів "зомбіювання" комп'ютерів.

Найчастіше зловмисники при проведенні DDOS-атак використовують трирівневу архітектуру, яку називають "кластер DDOS ". Така структура містить:

– консоль керування (їх може бути декілька), – комп'ютер, з якого зловмисник подає сигнал про початок атаки;

– головні комп'ютери – це ті машини, які одержують сигнал про атаку з консолі керування та передають його агентам – "зомбі". На одну керуючу консоль залежно від масштабності атаки може припадати до декількох сотень головних комп'ютерів;

– агенти – безпосередньо "зомбі"-комп'ютери.

Простежити таку структуру у зворотньому напрямку практично неможливо. Комп'ютери-агенти і головні комп'ютери є також потерпілими в даній ситуації та називаються "скомпроментованими". Така структура робить практично неможливим відстеження адреси вузла, що організував атаку.

Інша небезпека DDOS полягає в тому, що зловмисникам не потрібно мати спеціальні знання та ресурси. Програми для проведення атак вільно поширюються в мережі. Виділяють наступні види DDOS-атак:

- UDP flood – відправлення на адресу системи-мішені великої кількості пакетів UDP. Цей метод найменш небезпечний. Програми, що використовують цей тип атак, легко виявляються, оскільки при "зомбуванні" використовуються нешифровані протоколи TCP і UDP.
- TCP flood - відправлення на адресу мішені великої кількості TCP-пакетів, що також приводить до "зв'язування" мережевих ресурсів.
- TCP SYN flood – відправлення великої кількості запитів на ініціалізацію TCP-з'єднань із вузлом-мішенню, якому в результаті доводиться витрачати всі свої ресурси на те, щоб відслідковувати ці частково відкриті з'єднання.
- Smurf-атака - ping-запити ICMP за адресою спрямованої широкомовної розсилки з використанням а пакетах цього запиту фальшивої адреси джерела, яка в результаті виявляється мішенню атаки.
- ICMP flood - атака, аналогічна Smurf, але без використання розсилки.

Найнебезпечнішими є програми, що використовують одночасно кілька видів описаних атак – TFN і TFN2K, і вимагають від зловмисника високого рівня підготовки.