УДК 004.77
Гамеляк Й. – ст. гр. СНм-51
Тернопільський національний технічний університет імені Івана Пулюя

ОСНОВНІ МІРИ ПРОТИДІЇ DOS- І DDOS-АТАКАМ

Науковий керівник: асистент Маєвський О.В.

Міри протидії DDOS-атакам можна розділити на пасивні та активні, а також на превентивні та реакційні. Розглянемо основні методи.

Запобігання. Профілактика причин, що спонукують тих або інших осіб організовувати DDOS-атаки. Дуже часто атаки є наслідками особистої образи, політичних, релігійних розбіжностей, що провокує поводження жертви.

Розосередження. Побудова розподілених і резервних систем, які не припинять обслуговувати користувачів навіть, якщо деякі їхні елементи стануть недоступні.

Відхилення. Відвести безпосередню ціль атаки подалі від інших ресурсів, які часто піддаються впливу разом із безпосередньою мішенню.

Фільтрація трафіку на маршрутизаторах найпоширеніший метод протидії. Фільтри варто вводити ближче до джерела flood. Міжмережеві екрани та спеціалізовані antiflood засоби фільтрації найбільш ефективна міра, але й найбільш дорога. Знизити витрати можна, розділяючи такі системи між багатьма клієнтами (фільтрація на вимогу).

Нарощування. Якщо flood спрямований на вичерпання ресурсів, найпримітивніший спосіб протидії flood – нарощування своїх ресурсів, щоб супротивник не зміг їх вичерпати.

Сучасні засоби захисту від DDOS-атак дозволяють із досить високим ступенем ефективності виявити атаку та зменшити або запобігти втратам ресурсів операторів та їхніх клієнтів. Компанія "NVisionGroup" пропонує комплексне рішення для захисту від DDOS-атак на основі технології CiscoCleanPipes, що забезпечує оперативну реакцію на DDOS-атаки, легко масштабується, має високу надійність і швидкодією.

Технологія CiscoCleanPipes дозволяє використання модулів CiscoAnomalyDetector і CiscoGuard, а також різні системи статистичного аналізу мережевого трафіку, в основу яких покладені дані, які одержуються із маршрутизаторів за протоколом CiscoNetflow. При цьому AnomalyDetector і системи статистичного аналізу трафіку виступають як системи виявлення DDOS-атак, а CiscoGuard як засіб протидії вже виявленій атаці. У загальному випадку технологія CleanPipes припускає наявність етапу тестування (навчання), що проводиться в період відсутності DDOS-атак. На цьому етапі пристрої виявлення визначають і запам'ятовують, який трафік для захищуваного ресурсу є нормальним. Ситуація, при якій поточний трафік на захищуваний ресурс різко відрізняється від нормального, вважається DDOS-атакою. При виявленні DDOS, система виявлення повідомляє оператору та активує підсистему захисту CiscoGuard.

DDOS-атаку дуже складно виявити та запобігти, оскільки "шкідливі" пакети не відрізняються від "легітимних". Мережеві пристрої та традиційні технічні рішення для забезпечення безпеки мережевого периметру, такі як міжмережеві екрани та системи виявлення вторгнень (IDS), є важливими компонентами загальної стратегії мережевої безпеки, однак самі ці пристрої не забезпечують повного захисту від DDOS-атак. Міжмережеві екрани дозволяють або забороняють проходження мережевого трафіку на підставі аналізу різних полів мережевих пакетів. Але DDOS-атака може бути успішно реалізована в рамках дозволених міжмережевим екраном потоків трафіку.