УДК 681.3

А.З. Піскозуб
Національний університет "Львівська політехніка",
кафедра автоматики та телемеханіки

DoS-АТАКИ (АТАКИ ТИПУ "ВІДМОВА ВІД ОБСЛУГОВУВАННЯ") ТА DDoS-АТАКИ (РОЗПОДІЛЕНІ АТАКИ ТИПУ "ВІДМОВА ВІД ОБСЛУГОВУВАННЯ")

У статті розглядаються основні види DoS-атак, що насичують смугу пропускання каналу зв'язку системи-жертви, проводиться їх аналіз і пропонуються способи захисту від них.

In the article there are considered main types of DoS-attacks which flood victim's communication channel bandwidth, carried out their analysis and offered methods of protection from these attacks.

Питання безпеки завжди стояло перед комп'ютерними мережами, але сьогодні як ніколи зростає усвідомлення того, наскільки важлива безпека комп'ютерних мереж в корпоративній інфраструктурі. У цей час для кожної корпоративної мережі необхідно мати чітку політику в галузі безпеки. Ця політика розробляється на основі аналізу ризиків, визначення критично важливих ресурсів і можливих загроз.

Існує декілька основних типів загроз, що представляють велику небезпеку: *маскарад* (користувач видає себе за іншого), *підслуховування* даних під час передачі по незахищених каналах, *маніпулювання* даними (несанкціонована зміна даних, які зберігаються на будь-яких носіях чи передаються по каналах зв'язку) та *відмова від обслуговування* (Denial of Service- DoS). Останньому типу загроз і присвячена ця стаття.

DoS-атаки займають одне з чільних місць в сучасних атаках на комп'ютерні системи – щорічно збитки від них для різних компаній коштують мільйони доларів збитків внаслідок довготривалого простою систем, втраченими прибутками і великим обсягом робіт по ідентифікації і підготовці адекватних заходів у відповідь. По суті, DoS-атака порушує чи повністю блокує обслуговування легітимних користувачів, мереж, систем та інших ресурсів. Жертвами останніх DoS-атак, які відбулися в лютому 2000 року, стали декілька відомих Web-вузлів, таких як Yahoo, eBay, Buy.com, CNN.com, E*TRADE та ZDNet. Більше того, з моменту появи нового напрямку ведення війни під назвою "infowar" ("інформаційна війна") (в 1993 році в директиві комітету начальників штабів міністерства оборони США були викладені основні принципи ведення інформаційної війни), DoS-атаки вважаються чи не одним з основних засобів виведення інформаційних систем супротивника з ладу.

Тому розглянемо основні види DoS-атак, спробуємо їх проаналізувати і запропонувати способи захисту від них.

Відомі такі види DoS-атак: насичення смуги пропускання; атаки, що приводять до нестачі ресурсів; атаки, які використовують помилки програмування; атаки на маршрутизацію та DNS.

Атаки, що призводять до нестачі ресурсів, спрямовані на захоплення системних ресурсів, таких як процесор, пам'ять, дискові квоти чи інші системні процеси. Наприклад,

д) використати шлюз прикладного рівня. Proxy-механізми ефективно блокують увесь TFN2K трафік. Якщо для певного сервісу використання proxy-механізму не прийнятне, то постаратись звести до мінімуму такі сервіси;

е) використати властивість Unicast RPF маршрутизаторів Cisco для запобігання DoS-атак з використанням підроблених вихідних адрес;

є) встановити допустиму частоту звертання CAR для ICMP- та TCP SYN-пакетів на маршрутизаторах Cisco;

ж) використати властивість TCP Intercept маршрутизаторів Cisco для запобігання SYN flood-атак.

- встановити на вашій мережі систему виявлення втручання.

Для виявлення компонентів Trinoo, TFN, TFN2K, Stacheldraht на комп'ютерах необхідно використати сканер *DDoSPing* v2.0 Робіна Кейра [11, 12], утиліту *Zombie Zapper* групи Razor [11, 13], яка робить спробу послати віддаленому DDoS-агенту команду зупинити атаку, і програму-сканер *find_ddos* , розроблену центром NIPC [11, 14]. Сканер *find_ddos* в своїй роботі чимось подібний до антивірусу, оскільки сканує ресурси локальної системи на наявність вказаних вище програм.

Узагальнюючи матеріал по DoS- та DDoS-атаках, зазначимо, що 100-процентного захисту від них не існує. Захист від них потребує комплексних заходів, які часом є не просто реалізувати. Причому декотрі заходи, такі як рекомендації "вхідного фільтрування" ("Ingress Filtering") та "вихідного фільтрування" ("Egress Filtering") мають першочергове значення для захисту від DoS-атак, але потребують часу для їх реалізації на всіх системах Інтернет.

1. [RFC2827] P. Ferguson, D. Senie., Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing., RFC2827, Cisco Systems, Inc., May 2000. 2. [RFC1918] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot & E. Lear. "Address Allocation for Private Internets", RFC1918. February 1996. 3. Microsoft Knowledge Base. Q142641. Internet Server Unavailable Because of Malicious SYN Attacks. Microsoft Corporation. July 4, 2000. 4. Cisco. Configuring TCP Intercept (Prevent Denial-of-Service Attacks). http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/scdenial.htm 5. Cisco. IOS Essential Features http://www.cisco.com/public/cons/isp/documents/IOSEssentialsPDF.zip 6. CERT Distributed System Intruder Tools Workshop report http://www.cert.org/reports/dsit_workshop.pdf 7. Dittrich, Dave. The "Tribe Flood Network" distributed denial of service attack tool http://staff.washington.edu/dittrich/misc/tfn.analysis 8. Dittrich, Dave. The DoS Project's "trinoo" distributed denial of service attack tool http://staff.washington.edu/dittrich/misc/trinoo.analysis 9. Dittrich, Dave. The "stacheldraht" distributed denial of service attack tool http://staff.washington.edu/dittrich/misc/stacheldraht_analysis 10. Barlow, Jason, Thrower, Woody. TFN2K - An Analysis. AXENT Security Team. March 7, 2000. http://packetstorm.decepticons.org/distributed/tfn.analysis.txt 11. Packet Storm Security. Distributed denial of service attack tools http://packetstorm.securify.com/distributed/ 12. DDoSPing. http://www.keir.net 13. Zombie Zapper. http://razor.bindview.com 14 find_ddos. http://www.nipc.gov