Ю.Ю. Нізовцев
Український інститут спеціальної техніки та судових експертиз СБУ

КРИМІНАЛІСТИЧНЕ ДОСЛІДЖЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ, ЩО ПІДДАВАЛИСЯ ВІДДАЛЕНІЙ АТАЦІ НА ВІДМОВУ В ОБСЛУГОВУВАННІ: КЛАСИФІКАЦІЯ АТАК НА ВІДМОВУ

У статті наведена класифікація атак на відмову в обслуговуванні. Також розглянуті варіанти організації розподілених атак. Дана класифікація надає можливість краще зрозуміти сутність атаки на відмову в обслуговуванні, способи її реалізації, можливості досягнення атакуючим своєї мети. Знання видів атак на відмову надає експертові можливість більш ефективно досліджувати автоматизовані системи, які були піддані таким атакам.

Одним з різновидів втручання в роботу автоматизованих систем є атака на відмову в обслуговуванні (або просто атака на відмову), яка полягає в заблокуванні доступу користувачів до сервісу, що надається атакованою системою, або у примушуванні атакованої системи функціонувати потрібним зловмисникові чином.

Термін "атака на відмову в обслуговуванні" вперше з'явився в англомовній літературі: **DoS** attack, або Denial-of-Service attack. Так само в англомовній літературі з'явився термін "розподілена атака на відмову в обслуговуванні" (англ. **DDoS** attack, Distributed Denial-of-Service attack), що являє собою таку саму атаку на відмову в обслуговуванні, яка реалізується одночасно багатьма хостами. Тобто, якщо атака відбувається одночасно з великої кількості IP-адрес, то її називають розподіленою (DDoS). У розподіленій атаці на відмову одночасно можуть брати участь від кількох одиниць до кількох сотен тисяч, а іноді — кількох мільйонів хостів.

Атаки на відмову зазвичай здійснюються з наміром зробити недоступними ресурси атакованої системи для легітимних користувачів. Як прогнозований наслідок такої атаки може бути неможливість здійснення розрахунків через Інтернет, втрата іміджу власника атакованого ресурсу або власника хостингу атакованого ресурсу, підміна заблокованого ресурсу іншим ("підробленим") тощо.

Крім того, метою атаки на відмову можуть бути й інші збої у функціонуванні атакованої системи. Наприклад, надмірне перевантаження ресурсів певної системи може призвести до відключення її міжмереже-

вого екрану та зробити можливою іншу атаку на цю систему (наприклад, завантаження шкідливого програмного коду тощо), або атаку на другу систему, яка при нормальному функціонуванні першої атакованої системи була недосяжною для зловмисників.

За ***локалізацією реалізації*** атаки на відмову поділяються на *локальні* та *віддалені*.

Локальні атаки (або атаки *на стороні клієнта*) реалізуються безпосередньо на атакованому хості. До них відносяться різні експлойти: форк-бомби і програми, що відкривають по мільйону файлів або запускають якийсь циклічний алгоритм, який перевантажує пам'ять та процесорні ресурси. Для локальної атаки на відмову необхідно мати, або якимось чином отримати доступ до атакованої машини на рівні, що буде достатнім для захоплення ресурсів. Доступ можна отримати, зокрема, використовуючи вразливості програмного забезпечення (ПЗ) атакованої системи, методи "соціальної інженерії" тощо.

Віддалені атаки на відмову реалізуються ззовні відносно атакованого хоста або атакованої мережі. В залежності від шляхів реалізації вони поділяються на два види:

– віддалена експлуатація уразливостей програмного забезпечення атакованої системи;
– перевантаження атакованої системи з метою вичерпання усіх наявних у атакованої системи ресурсів.

Віддалена експлуатація уразливостей програмного забезпечення представляє собою використання помилок, недоробок чи інших слабкостей у програмному забезпеченні атакованої системи з метою довести його до неробочого стану. Реалізується частіш за все шляхом пересилки спеціально сформованих шкідливих пакетів. Прикладом такої атаки може слугувати так званий "pingofdeath"– тип мереженої атаки, під час якої атакований комп'ютер отримує особливим чином сформований echo-запит (ping), після якого він перестає відповідати на запити взагалі. Ця уразливість була досить широко розповсюджена у середині 1990-х років на різних операційних системах та мережених пристроях, включаючи Unix, Linux, Mac, Windows, мережеві принтери та маршрутизатори.

Перевантаження атакованої системи з метою вичерпання усіх наявних у атакованої системи ресурсів полягає у використанні величезної кількості безглуздих (рідше — осмислених) пакетів для завантаження ресурсів системи, необхідних для обробки запитів легітимних користувачів. Цей вид атаки також має назву ***флуд***, що походить від англомовного терміну *flood* — повінь.

В залежності від напрямку реалізації флуд-атаки бувають:
– спрямовані на ресурси атакованої системи;
– спрямовані на канал зв'язку, що з'єднує атаковану систему з іншою частиною мережі.

Під час флуд-атаки, *спрямованої на ресурси системи*, ці ресурси захоплюються за допомогою багаторазового і дуже частого звернення до якого-небудь сервісу, що виконує складну, ресурсоємну операцію. Це може бути, наприклад, тривале звернення до одного з активних компонентів (скриптів) web-сервера. Сервер витрачає всі ресурси машини на обробку атакуючих запитів, а легітимним користувачам доводиться чекати.

Якщо ж флуд-атака с*прямована на канал зв'язку*, потік флуд-пакетів займає весь пропускний канал. Завдяки цьому більшість легітимних пакетів не досягають цільової системи, що піддається атаці. Крім того, сама атакована система, будучи зайнятою обробкою флуд-пакетів, не має можливості обробляти легальні запити.

Як видно з визначення, грань між двома описаними вище напрямками флуд-атак є досить умовною, оскільки в багатьох випадках величезна кількість трафіку займає як ресурси атакованої системи, так і канал зв'язку.

В залежності від рівня мережевої моделі "TCP/IP", на якому реалізується атака на відмову, виділяють: рівень доступу до середи передачі даних; мережевий рівень; транспортний рівень; прикладний рівень.

В залежності від рівня мережевої моделі "OSI", на якому реалізується атака на відмову, виділяють сім рівнів: перший рівень — фізичний; другий — канальний; третій — мережевий; четвертий — транспортний; п'ятий — сеансовий; шостий — представлення; сьомий рівень — прикладний.

Не є суттєвим, яку з мережевих моделей ("TCP/IP" чи "OSI") обрати задля класифікації мережевих рівнів реалізації атак на відмову, оскільки існує певне співвідношення між цими рівнями в обох моделях. Розширений опис рівнів мережевих моделей та їх співвідношення виходить за рамки даної публікації. Слід лише наголосити, що використання мережевої моделі "TCP/IP" вбачається більш зручним, оскільки ця модель ближче до практичної реалізації основних протоколів Інтернет, а модель "OSI" має більш теоретичний характер.

За ***схемою атаки***, тобто за ***шляхами доставки*** атакуючим зловмисного трафіка жертві виділяють наступні атаки на відмову:

– *пряма*, під час якої пересилка трафіку здійснюється безпосередньо з одного або багатьох хостів;
– *віддзеркалена*, під час якої пересилка трафіка здійснюється через третіх осіб;
– *прихована*, під час якої зловмисний трафік ховається в “законому”.

Як вже зазначалося вище, розподілена атака на відмову характеризується тим, що здійснюється одночасно кількома атакуючими. Існують наступні варіанти організації розподілених атак на відмову:

- ***Ботнет*** — зараження певного числа комп’ютерів програмами, які в певний момент починають здійснювати запити до атакованого сервера;
- ***Флешмоб*** — домовленість великого числа користувачів Інтернету почати здійснювати певні типи запитів до атакованого сервера;
- ***Смурфінг*** — атака з використанням широкомовних адрес та підробки IP-адреси відправника;
- ***Разове завантаження скрипта*** — здійснюється шляхом разового завантаження та виконання скрипта на комп’ютер, що бере участь у розподіленій атаці на відмову.

Ботне́т (англ. *botnet* від *robot* і *network*) — це комп’ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами — автономним програмним забезпеченням. Найчастіше бот у складі ботнета є програмою, яка приховано встановлюється на комп’ютері жертви і дозволяє зловмисникові виконувати певні дії з використанням ресурсів інфікованого комп’ютера. Нерідко ботом називають сам інфікований комп’ютер. Зазвичай боти використовуються для протиправної діяльності — розсилки спаму, перебору паролів на віддаленій системі, атак на відмову в обслуговуванні, отримання персональної інформації про користувачів, крадіжка номерів кредитних карт та паролів доступу. Серед найбільших відомих ботнетів можна виділити BredoLab, що був створений у 2009 році та налічував близько 30 000 000 ботів [1], а також Mariposa, що був створений у 2008 році та налічував 12 000 000 ботів [2].

Комп’ютер може потрапити в мережу ботнету через встановлення певного програмного забезпечення, частіше за все — без відома користувача.

Задля убезпечення від видалення з інфікованого хоста, ПЗ ботнету має механізм самозахисту (механізм маскування). Механізм самозахисту аналогічний для більшості вірусів та руткітів. Крім того, ПЗ ботнету має певні механізми для забезпечення успішного запуску при увімкненні комп’ютера.

Кожен ботнет має механізми керування, завдяки якому всі інфіковані комп'ютери виконують дії, необхідні "власникові" ботнету. Раніше керування передбачало "очікування" певних команд від командного центру на певному порту, або участь в IRC-чаті. При відсутності команд програма "спить", очікуючи на команду від командного центру, можливо намагається саморозмножуватись. При отриманні команди від командного центру ботнету, бот починає виконувати вказану команду. В ряді випадків за командою завантажується виконуваний файл (таким чином, є можливість "оновлювати" програму і завантажувати модулі, які додають функціональність).

Наразі отримали поширення ботнети, які керуються через веб-сайт або по принципу p2p-мереж.

Флешмо́б (також флеш моб і флеш-моб, англ. *flashmob* — "спалахуючий натовп", *flash* — спалах, *mob* — натовп) у контексті атаки на відмову в обслуговуванні — це заздалегідь спланована масова акція, у якій велика кількість людей одночасно направляють запити до певного мережевого ресурсу. Під час такої атаки найчастіше застосовується звичайне (легальне) програмне забезпечення, наприклад, інтернет-оглядач, за допомогою якого відкривається та періодично оновлюється (клавішею "F5") web-сторінка атакованого ресурсу. Але може використовуватись і спеціалізоване програмне забезпечення, призначене для проведення віддаленої атаки на відмову (наприклад — "loic").

На відміну від ботнету, в даному випадку користувачі обізнані про характер своїх дій та свідомо беруть участь в атаці.

Смурфінг (англ. *Smurf*, або *Smurfing*) — атака із застосуванням ефекту віддзеркалення трафіку, полягає у відправленні на широкомовну або групову адресу повідомлення, яке потребує відповіді (наприклад — echo-запит). В якості адреси відправника у повідомленні зазначається адреса атакованого хоста. Як результат, усі вузли мережі, які отримають це повідомлення, надішлють відповідь до атакованого хоста.

Особливість даного варіанту організації розподіленої атаки на відмову полягає в наступному:

– відсутність необхідності встановлення ПЗ ботнету на комп'ютери, що беруть участь в атаці;
– відсутність необхідності підмовлення користувачів комп'ютерів, що беруть участь в атаці.

Слід зазначити, що використання ефекту віддзеркалення трафіку значно ускладнює ідентифікацію джерел атаки.

Разове завантаження скрипта. Даний вид атаки на відмову має деякі спільні риси з ботнетом. Суть його полягає в наступному. На загальнодоступному (бажано — популярному) мережевому ресурсі розміщується скрипт, який при відвідуванні цього ресурсу завантажується на комп'ютер відвідувача та здійснює багаторазову відсилку певних запитів на адресу атакованої системи.

Прикладом даного виду організації розподіленої атаки є розміщення в тілі web-сторінки java-скрипта, яким запрограмовано відсилку певної кількості echo-запитів (ping) на певну адресу. Java-скрипт завантажується інтернет-оглядачем (браузером) разом з web-сторінкою та виконується на стороні (на комп'ютері) відвідувача. Таким чином, комп'ютер відвідувача стає "співучасником" розподіленої атаки на відмову.

На відміну від ботнету, при разовому завантаженні скрипта не відбувається інсталяції шкідливого програмного забезпечення на комп'ютер, що бере участь в розподіленій атаці на відмову. Крім того, відсутній механізм віддаленого керування. Завантажений скрипт працює лише доки він завантажений інтернет-оглядачем та відразу припиняє роботу після закриття web-сторінки або закриття інтернет-оглядача. Таким чином, комп'ютер, до якого було завантажено скрипт, не є підконтрольним зловмисникові.

Як бачимо, класифікувати атаки на відмову в обслуговуванні можна за різними критеріями, кожен з яких характеризує певний бік таких атак. Наведена вище класифікація атак на відмову носить не лише академічний характер. Знання теорії, по-перше, дає змогу краще вивчити та зрозуміти суть конкретної атаки на практиці. По-друге, різні види атак можуть залишити різні "сліди", а отже, знаючи класифікацію атак на відмову, експерту буде легше зрозуміти, що це за "сліди" та де їх шукати.

Список використаної літератури

1. Infosecurity (UK) — BredoLab downed botnet linked with Spamit.com [Електронний ресурс]. — Режим доступу: http://www.infosecurity-magazine.com/view/13620/bredolab-downed-botnet-linked-with-spamitcom/
2. "Suspected 'Mariposa Botnet' creator arrested". [Електронний ресурс]. — Режим доступу: http://www.canada.com/topics/technology/story.html?id=3333655
3. Ігнатенко О. Атаки на відмову: виникнення, проблеми, огляд атак, класифікація. [Електронний ресурс]. — Режим доступу: http://eprints.isofts.kiev.ua/250/1/Атаки_на_відмову.pdf
4. *Уланов А.В., Котенко И.В.* Защита от DDoS-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия / А.В. Уланов, И.В. Котенко // Защита информации. INSIDE. — 2007. — № 1–3.
5. DoS-атака [Електронний ресурс]. — Режим доступу: http://uk.wikipedia.org/wiki/DoS-атака

6. Ботнет [Електронний ресурс]. — Режим доступу: http://uk.wikipedia.org/wiki/Ботнет

Резюме

В статье представлена классификация атак на отказ в обслуживании. Также рассмотрены варианты организации распределенных атак. Данная классификация дает возможность лучше понять суть атаки на отказ в обслуживании, способы ее проведения, возможности достижения атакующим своих целей. Знание видов атак на отказ в обслуживании даст эксперту возможность более эффективно исследовать автоматизированные системы, которые подверглись таким атакам.

Summary

The paper presents the classification of attacks on the denial of service. Also considered options for distributed attacks. This classification makes it possible to better understand the Denial-of-service, methods of implementation, the possibility of reaching an attacking their targets. Knowledge of the types of attacks denial of service will give the expert to explore more efficient automated systems which have undergone such attacks.

Л.Г. Бордюгов, канд. юрид. наук, заст. директора

Донецький НДІ судових експертиз

ПРОЦЕСУАЛЬНА ПРИРОДА І ОСНОВНІ ПОНЯТТЯ СУДОВОЇ ІНЖЕНЕРНО-ЕКОЛОГІЧНОЇ ЕКСПЕРТИЗИ

У статті розглянуті питання щодо процесуальної природи судової інженерно-екологічної експертизи, надано визначення її поняття. Розкрито поняття предмета та об'єкта цієї експертизи, визначено коло розв'язуваних нею завдань.

Підвищення ефективності судової експертизи як основної форми використання спеціальних знань у судочинстві ґрунтується на двох тенденціях: розвитку існуючих і формуванні нових класів (родів, видів) судових експертиз. До останніх належить і судова інженерно-екологічна експертиза, поява та розвиток якої обумовлені потребами слідчої і судової практики при розслідуванні і розгляді екологічних злочинів.

У даний час як в Україні, так і в Росії ведуться наукові дослідження, присвячені питанням теорії судово-екологічної експертизи [1–6].

На жаль, теоретичні питання судової інженерно-екологічної експертизи досліджені недостатньо. Її зміст і деякі загально-методичні положення знайшли відображення в спеціальній літературі, в наукових розробках Донецького та Харківського НДІ судових експертиз, і отримують визнання в експертній, слідчій і судовій практиці. Однак