УДК 004.942:004.772

В. Кордяк, І. Дронюк, О. Федевич
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ МОНІТОРИНГУ ТА АНАЛІЗУ ТРАФІКУ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Проаналізовано методи моніторингу трафіку комп'ютерних мереж. Розглянуто методи моніторингу, орієнтовані на маршрутизатори та активні і пасивні методи моніторингу, які не орієнтовані на маршрутизатори. Описано розроблену інформаційну технологію моніторингу трафіку. Здійснено класифікацію DDoS-атак, а також запропоновано методи запобігання їм. Ефективність запропонованих методів доведено експериментально, на основі моделювання DDoS-атак та моніторингу мережі за допомогою розробленої інформаційної технології аналізу трафіку. Показано, що завдяки застосуванню запропонованих алгоритмів запобігання хакерським атакам досягають значного зменшення (приблизно у 4 рази) шкідливого трафіку на мережевому обладнанні. Експерименти проілюстровано рисунками та графіками.

Ключові слова: трафік, комп'ютерна мережа, моніторинг мережі, швидкість передавання даних, DDoS-атаки.

This article analyzes the methods of monitoring traffic of computer networks. The methods of monitoring, focused on routers, and active and passive monitoring techniques that are not focused on routers were reviewed. Developed information technology for traffic monitoring is described. Classification of DDoS-attacks, as well as the methods to preventing them were made. The effectiveness of the proposed methods was proved experimentally, by modeling of DDoS-attacks and network monitoring, with the help of developed information technology for traffic analysis. It is shown, that using of the proposed hack preventing algorithms, a significant reduction (approximately in 4 times) of harmful traffic on the network equipment is achieved. The experiments are illustrated with figures and graphics.

Key words: traffic, computer network, network monitoring, bit rate, DDoS-attacks.

Вступ

Кількість великих і малих комп'ютерних мереж неухильно збільшується. Для якісної та безперебійної роботи мережі адміністраторам доводиться невпинно за нею стежити. Моніторинг мережі – це складне завдання, яке потребує великих витрат сил та є життєво важливою частиною роботи мережевих адміністраторів. Моніторинг та аналіз трафіку необхідні для того, щоб ефективніше діагностувати та вирішувати проблеми, не доводячи мережеві сервіси до простою протягом тривалого часу. Сьогодні відомі [1] методи моніторингу, орієнтовані на маршрутизатори і методи моніторингу, які не орієнтовані на маршрутизатори; останні поділяються на активні і пасивні. Моніторинг, який вбудований в маршрутизатори і не вимагає додаткового встановлення програмного або апаратного забезпечення, називають методами, основаними на маршрутизаторах. На противагу їм є методи, що не ґрунтуються на маршрутизаторах, але вимагають встановлення спеціального апаратного та програмного забезпечення. Методи моніторингу тісно пов'язані зі завданнями забезпечення ефективного завантаження обладнання, безперебійної роботи мережі та запобігання несанкціонованим атакам на мережу.

Постановка проблеми

Моніторинг мережі – важливе практичне завдання. Адміністратори постійно прагнуть підтримувати безперебійну роботу своєї мережі. Якщо мережа "впаде" хоча б на короткий період

часу, продуктивність компанії скоротиться і (у випадках організацій, які надають державні послуги) сама можливість надання основних послуг буде поставлена під загрозу. Тому адміністратори мають стежити за рухом мережевого трафіку і продуктивністю на всій мережі, перевіряти та знаходити прогалини в мережевій безпеці.

Одне зі завдань моніторингу – це своєчасне знешкодження DDoS-атак. Проблема боротьби з DDoS-атаками є актуальною, оскільки глобальна мережа Інтернет дедалі ширше використовується у діяльності людини. Розвиток IT-індустрії, розширення комп'ютерних мереж та зростання їх швидкостей спричинили збільшення кількості комп'ютерних атак, зокрема DDoS атак. Із суто інформаційної мережі, призначеної для обміну інформацією електронною поштою і забезпечення доступу до різноманітних віддалених файлових архівів, Інтернет стрімко перетворюється на серйозний ринок послуг, в який інвестуються великі суми грошей. В результаті атаки порушується або повністю блокується обслуговування законних користувачів, мереж, систем та інших ресурсів. Більшість DDoS-атак використовують уразливості в основному протоколі Internet (TCP / IP), а саме спосіб обробки системами запиту, що здійснюється від користувачів.

Аналіз публікацій

Розглянемо моніторинг мережі у поєднанні з запобіганням DDoS-атакам. Моніторинг трафіку розглянуто у [1, 3, 4]. Методи моніторингу засновані на маршрутизаторі – жорстко задані (вшиті) в маршрутизаторах і, отже, мають низьку гнучкість. Стислий опис методів такого моніторингу наведено нижче. Кожен метод розвивався багато років, перш ніж стати стандартизованим способом моніторингу.

Одним з найпоширеніших є протокол простого мережевого моніторингу Simple Network Management Protocol (SNMP), RFC 1157. SNMP – протокол прикладного рівня, який є частиною протоколу TCP / IP. Він дозволяє адміністраторам керувати продуктивністю мережі, знаходити і усувати мережеві проблеми, планувати зростання мережі. Він збирає статистику по трафіку до кінцевого хоста через пасивні датчики, які реалізуються разом з маршрутизатором.

Іншим методом є віддалений моніторинг Remote Network MONitoring (RMON), RFS 1757. RMON містить різні мережеві монітори та консольні системи для зміни даних, отриманих під час моніторингу мережі. Це розширення для SNMP інформаційної бази даних з управління (MIB). На відміну від SNMP, який повинен посилати запити про надання інформації, RMON може настроювати сигнали, які будуть "моніторити" мережу, основану на певному критерії. RMON надає адміністраторам можливості управляти локальними мережами так само добре, як віддаленими. RMON використовує 9 різних груп моніторингу для отримання інформації про мережу, а саме: Statistics – статистика, виміряна датчиком для кожного інтерфейсу моніторингу для цього пристрою; History – облік періодичних статистичних вибірок з мережі і зберігання їх для пошуку; Alarm – періодично бере статистичні зразки і порівнює їх з набором порогових значень для генерації події; Host – містить статистичні дані, пов'язані з кожним хостом, що є в мережі; HostTopN – готує таблиці, які описують головний хост; Filters – передбачає фільтрацію пакетів, ґрунтуючись на фільтровому рівнянні для захоплення подій; Packet capture – захоплення пакетів після їх проходження через канал; Events – контроль генерації та реєстрація подій від пристрою; Token ring – підтримка кільцевих лексем.

Хоча RMON будується на протоколі SNMP, моніторинг трафіку виконаний за допомогою цих методів, дані, отримані SNMP і RMON, мають низьку продуктивність. Набагато продуктивнішою є утиліта Netflow, яка представлена в маршрутизаторах Cisco. Утиліта Netflow дає можливість збирати мережевий IP трафік, працює успішно з багатьма пакетами аналітичного програмного забезпечення, щоб зробити моніторинг трафіку набагато простішим. Netflow міститьбе 3 компоненти: FlowCaching (кеш потоку), FlowCollector (збирач інформації про потоки) і Data Analyzer (аналізатор даних). З Netflow-пакетів можна отримати таку інформацію: адресу джерела і одержувача; адресу вхідного і вихідного пристрою; номер порту джерела і приймача; Протокол 4-го рівня; кількість пакетів в потоці; кількість байтів у потоці; номер автономної системи джерела і приймача.

Перевага Netflow порівняно з іншими способами моніторингу, такими як SNMP і RMON, в тому, що в ньому є програмний пакет Netflow Analyzer, призначений для різного аналізу трафіку, отримання даних від Netflow-пакетів та подання їх у більш зрозумілому для користувача вигляді. Найбільша перевага використання Netflow у можливості побудови численних графіків, що описують активність мережі в будь-який момент часу.

Тепер опишемо методи, що не ґрунтуються на маршрутизаторах. Хоча технології, не вбудовані в маршрутизатор, все ж обмежені у своїх можливостях, вони пропонують більшу гнучкість, ніж технології вбудовані. Ці методи класифікуються як активні і пасивні [1].

Активним моніторингом повідомляють про проблеми в мережі, збираючи вимірювання між двома кінцевими точками. Система активного вимірювання має справу з такими метриками, як: корисність, маршрутизатори або маршрути, затримка пакетів, повтор пакетів, втрати пакетів, вимірювання пропускної здатності. Для вимірювань використовуються інструменти: команда ping, яка вимірює затримку і втрати пакетів, і traceroute, яка допомагає визначити топологію мережі. Ці команди є прикладом основних активних інструментів вимірювання.

На відміну від активного моніторингу, за допомогою пасивного збирають інформацію тільки про одну точку в мережі. Пасивні вимірювання мають справу з такою інформацією, як: трафік і кількість протоколів, кількість бітів, синхронізація пакетів і час між прибуттям. Хоча пасивний моніторинг не має часових витрат, які має активний моніторинг, він має свої недоліки. З пасивним моніторингом вимірювання можуть бути проаналізовані тільки оф-лайн. Створюється проблема, пов'язана з обробкою великих наборів даних, які зібрані під час вимірювання.

Пасивний моніторинг може бути кращим за активний тим, що дані службових сигналів не додаються в мережу, але пост-обробка може викликати велику кількість тимчасових витрат. Тому на практиці використовують комбінацію цих двох методів моніторингу – так званий комбінований моніторинг. У комбінованих технологіях використано переваги пасивного, і активного моніторингу середовищ. Ці засоби можуть бути використані для захисту від DDoS-атак.

Аналіз DDoS-атак зроблено у роботах [5, 6]. Всі DDoS-атаки можна поділити на три великі групи[5]:

Атаки, спрямовані на обсяг

Ця категорія атак спрямована на насичення смуги пропускання, відповідно, силу атаки вимірюють у бітах на секунду. До цієї категорії належать різні види флуд-атак: UDP, ICMP та інші потоки сфальсифікованих пакетів. Сила атаки зростає з кожним роком, і якщо в далекому 2000 році 400 Мбіт/с здавалося чимось незвичайним, то зараз окремі атаки перевищують 100 Гбіт/с і здатні "покласти" навіть деякі дата-центри. Єдиний спосіб боротьби з такими атаками – фільтрація на рівні дата-центру (якщо він надає таку послугу) або спеціалізованих сервісів захисту. Вони володіють достатніми канальними потужностями і обчислювальними ресурсами, щоб поглинути обсяг сфальсифікованих пакетів і передати на сервер користувача вже відфільтрований трафік.

• *Атаки на рівні протоколів*

Ця категорія спрямована на обмеження устаткування або уразливості різних протоколів. Такі атаки забивають ресурси сервера або проміжного обладнання (фаєрволи, балансувальник навантаження і т.п.) паразитними пакетами, в результаті чого системи не здатні обробляти корисні запити. Сила атаки вимірюється в пакетах в секунду. До цієї категорії належать SYN та ICMP флуд, атаки з фрагментованими пакетами та інші. На цьому рівні апаратний захист стає відчутно ефективніший. Спеціально розроблені виробниками таких пристроїв алгоритми допомагають впорядкувати і відфільтрувати трафік. Природно, будь-які алгоритми недосконалі, і якась частина паразитного трафіку все-таки прорветься, а якась частина корисного може бути втрачена.

• *Атаки на рівні додатків*

Як можна зрозуміти з назви, атаки спрямовані на уразливості в додатках і операційних системах (Apache, Windows OpenBSD і т.п.).Вони призводять до непрацездатності будь-якої програми або ОС загалом. Серед таких атак: Slowloris, атаки нульового дня та інші. Як правило, складаються з цілком невинних запитів і блокують роботу веб-сервера. Інтенсивність вимірюється в

запитах на секунду. Цей тип атак найбільш “вбивчий”. Вони надзвичайно вузько спрямовані, завдяки чому можуть створити вельми серйозні проблеми для жертви за малих витрат ресурсів атакуючого. Останні 3–4 роки цей тип атак переважає. До арсеналу боротьби з цією категорією атак, крім згаданих вище зовнішніх сервісів і апаратного захисту, можна також зарахувати вбудовані програмні алгоритми, що аналізують запити і створюють правила для фаєрвола за результатами такого аналізу.

Отже, існує чимало видів DDoS-атак – у кожної свій почерк і способи подолання. Не всі атаки можна послабити або побороти. Іноді навіть немає сенсу намагатися, і простіше перечекати, поки атака закінчиться. Викласти детально механізми протистояння кожному типу неможливо, оскільки атак і методів боротьби з ними є чимало. Розглянемо найпоширеніші.

UDP флуд [7] – це один з найбільш дієвих і водночас простих видів атак. Використовується UDP протокол, де не потрібно встановлення сесії з відправкою відповіді. У випадковому порядку зловмисник атакує порти сервера, відсилаючи величезну кількість пакетів даних. У результаті машина починає перевіряти, чи використовується порт, на який приходить пакет, яким-небудь додатком. А оскільки таких пакетів маса, то машина будь-якої потужності просто не справляється із завданням. У результаті всі ресурси машини використано, і сервер перестає працювати. Найпростіший спосіб захисту від такого типу атак – це блокування UDP трафіку (звісно, якщо програмне забезпечення не використовує цей протокол).

MAC флуд [8] – це незвичайний тип атаки, в якому об’єктом стає мережеве обладнання багатьох типів. Зловмисник починає відправляти велику кількість Ethernet-пакетів з абсолютно різними MAC-адресами. У результаті світч починає резервувати під кожен з пакетів певну кількість ресурсів, і якщо пакетів багато, то світч виділяє всю доступну пам’ять і перестає працювати. Найгірший варіант – збій таблиці маршрутизації.

ICMP флуд [9] – це тип атаки, коли зловмисник постійно пінгує сервер жертви, у результаті чого останній постійно віддає відповіді. Пінгів величезна кількість, отже у результаті результат – з’їдаються ресурси сервера, і машина стає недоступною. Які запобіжний захист можна використовувати блокування ICMP-запитів на рівні брандмауера. Відбити такого роду атаку можна лише заміною обладнання на інше, в якому цю проблему вирішено. Сьогодні більшість виробників включили фільтр у програмне забезпечення свого обладнання.

PING OF DEATH – це атака, сенс якої – переповнення буфера пам’яті через перевищення максимально доступного розміру IP-пакета, результатом чого є відмова сервера і мережевого устаткування від обслуговування будь-якого типу пакетів. Зараз цей тип атак не є серйозною проблемою, хоча раніше це був поширений варіант атаки.

SLOWLORIS – атака, яка дозволяє малими силами домогтися великих результатів. Інакше кажучи, використовуючи не найпотужніший сервер, можна поламати набагато продуктивніше обладнання. При цьому не потрібно задіювати інші протоколи. При такому типі атак сервер зловмисника відкриває максимальну кількість HTTP-з’єднань і намагається тримати їх відкритими якомога довше. Кількість підключень на сервері закінчується, і корисні запити перестають прийматися і оброблятися. Атака ефективна лише на сервери, що обслуговують веб-сайти або ПЗ, що використовує HTTP протокол.

ДЕГРАДАЦІЯ – це такий тип атаки, коли сервер зловмисника симулює дії реальної людини або цілої аудиторії. Як приклад найпростішого варіанта: можна відсилати запити до однієї і тієї самої сторінки ресурсу, причому робити це тисячі разів. Найпростіший спосіб вирішення проблеми – тимчасове повідомлення про помилки з блокуванням сторінки, що піддається атаці. Також можна обмежити доступ до сторінки лише певною аудиторією користувачів (наприклад лише зареєстрованим). Складніший тип атаки – запит великої кількості різних ресурсів сервера, враховуючи мультимедійні дані, сторінки тощо, в результаті чого сервер-жертва перестає працювати. Складні атаки такого типу доволі складно відфільтрувати, отже, доводиться використовувати спеціалізовані програми та сервіси.

Формулювання цілі статті

Метою роботи є експериментальне дослідження, моніторинг і аналіз трафіку та аналіз типів DDoS атак й методів боротьби з ними. У публікації розглянемо типові види DDoS атак, покажемо, як їх моделювати і викривати та розробимо методи захисту від них, відобразимо візуально навантаження на кінцевому обладнанні.

Під час виконання роботи буде використано такі інструменти:

- hping3 – програма для генерації DoS та DDoS атак різних типів.
- Wireshark – програмне забезпечення для аналізу мережевих пакетів Ethernet та інших мереж (сніфер) із вільним вихідним кодом.
- iptraf – невелика програма, яка вміє моніторити всю мережеву активність комп'ютера.
- iptables – утиліта для командного рядка, стандартизований інтерфейс керування роботою міжмережевного екрана (брандмауеру) Netfilter для ядер Linux від версії 2.4.
- netfilter – це міжмережевий екран (брандмауер), вбудований в ядро Linux з версії 2.4.

Аналізувати навантаження мережевого інтерфейсу планується для перевірки достовірності розроблених методів математичного моделювання мережі.

Основна частина

Створено аналізатор роботи комп'ютерної мережі, який призначений для автоматизованого збирання інформації з мережевих пристроїв та контролю роботи каналів зв'язку. Він передбачає автоматизацію процесів збирання та аналізу характеристик мережі та їх відображення у зручному для адміністратора форматі.

Використання системи моніторингу комп'ютерної мережі дає змогу:

а) значно економити час;

б) автоматично і цілодобово збирати дані (джитер, затримка, швидкість) з пристроїв мережі;

в) у режимі реального часу слідкувати за роботою мережі.

Мережевий аналізатор складається із серверної (PHP, HTML, CSS, JS) та клієнтської (C++/QT) частин. Серверна частина займається аналізом даних та відображенням результатів. В свою чергу клієнська – збором, обробкою даних мережі. Цей програмний продукт створено на C++ і розповсюджується за ліцензією GNU GPL.

Змоделюємо UDP флуд за допомогою програми hping3, виконавши команду у терміналі (bash) Linux (див. рис. 1):

sudo hping3 --udp --rand-source -p 10000 --destport 10000 --flood 192.168.1.151,

де UDP – протокол; rand-source – випадкова IP-адреса відправника; destport – порт, який атакується, flood – режим флуду.

Для захисту від таких атак (рис. 2) скористаємося iptables та заблокуємо UDP пакети на всіх портах сервера (маршрутизатора), попередньо дозволивши DNS (що знаходиться на 53 порту). Для цього напишемо спеціальні правила блокування, використовуючи стандарти netfilter [2]:

iptables -A INPUT -p udp --sport 53 -j ACCEPT
iptables -A INPUT -p udp --dport 53 -j ACCEPT
iptables -A OUTPUT -p udp --sport 53 -j ACCEPT
iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
iptables -A INPUT -p udp -j DROP
iptables -A OUTPUT -p udp -j DROP,

де INPUT, OUTPUT – вхідний та вихідний трафік, ACCEPT, DROP – дозволяє або забороняє проходження трафіку, sport, dport – порт джерела і призначення.

Аналогічно проведемо моніторинг мережевого порту сервера за допомогою Wireshark та поглянемо, чи проходять UDP пакети через наше з'єднання (рис. 4). Як можна побачити з програми, на комп'ютер проходить TCP, ICMP та інший трафік, окрім UDP.

Повторимо моделювання UDP флуду та поглянемо на результат iptraf (рис. 3).

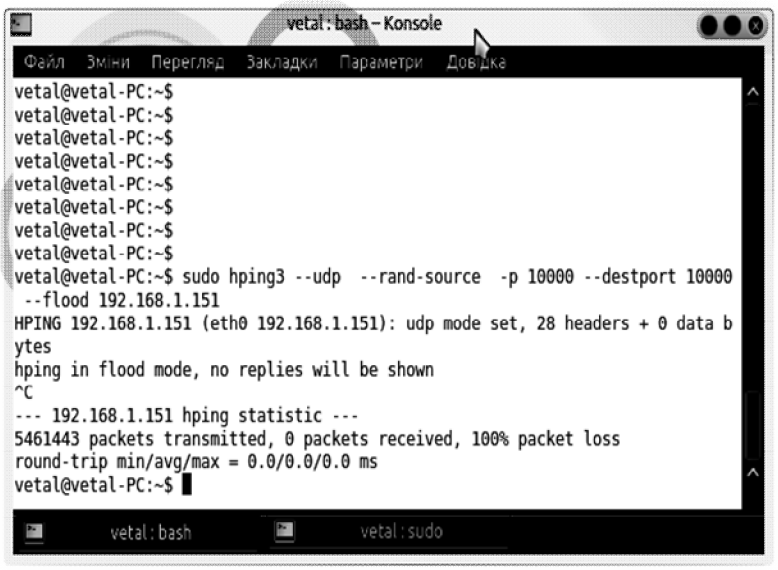


Рис. 1. Виконання програми hping3

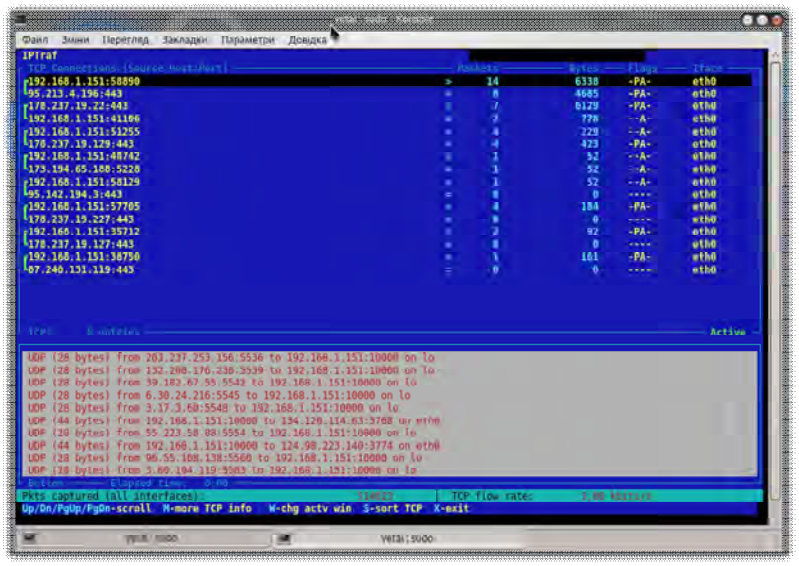


Рис. 2. Виконання програми iptraf

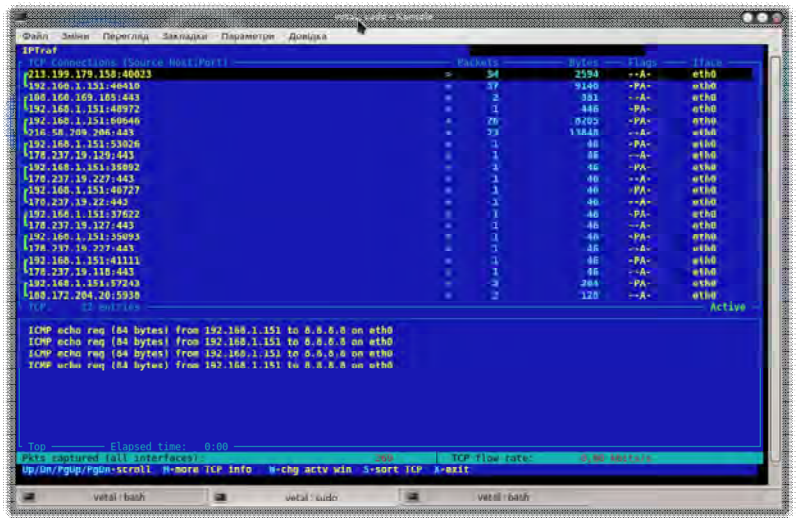


Рис.3. Виконання програми iptraf після ввімкнення фільтру UDP

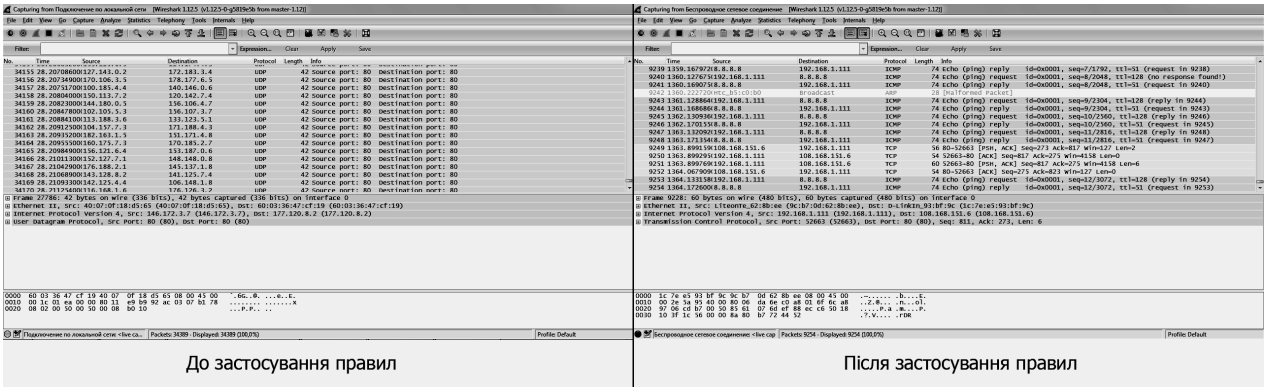
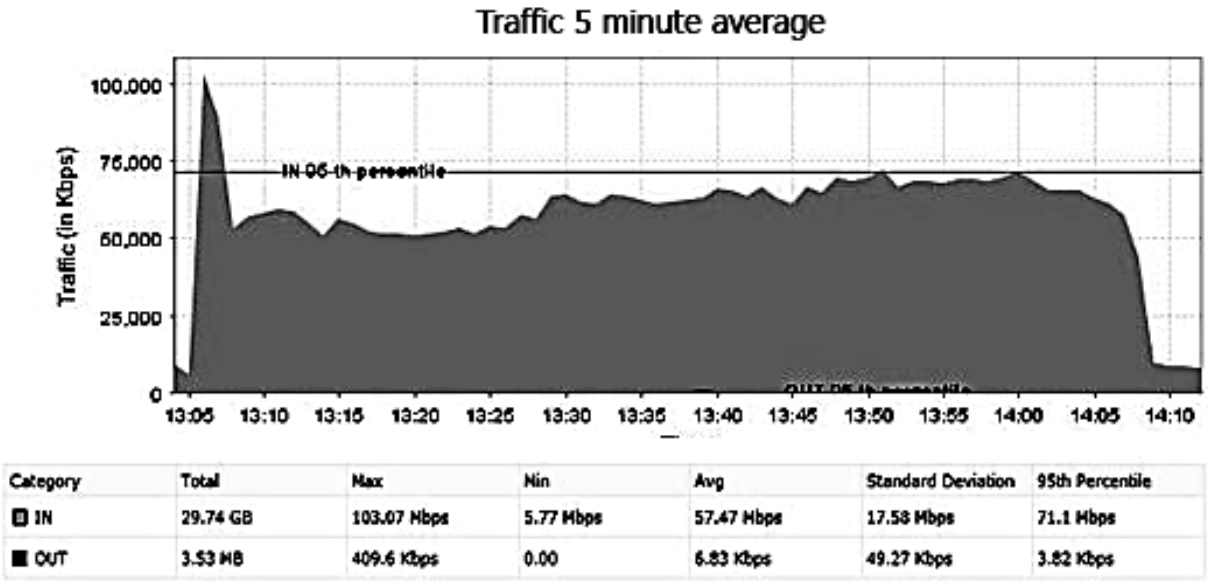


Рис. 4. Моніторинг трафіку до і після застосування правил

Отже, пакети UDP більше не доходять до сервера, тобто не можуть заподіяти шкоди програмному забезпеченню, що там працює, а навантаження мережі на кінцевому обладнанні значно зменшилось (рис. 5).



Category	Total	Max	Min	Avg	Standard Deviation	95th Percentile
IN	29.74 GB	103.07 Mbps	5.77 Mbps	57.47 Mbps	17.58 Mbps	71.1 Mbps
OUT	3.53 MB	409.6 Kbps	0.00	6.83 Kbps	49.27 Kbps	3.82 Kbps

Рис. 5. Візуалізація навантаження на мережевий порт кінцевого обладнання (веб-сервер у внутрішній мережі)

SYN флуд – це тип атаки, коли використовується відправка SYN-пакета серверу жертви. Згідно з процесом з'єднання за протоколом TCP, клієнт посилає пакет зі встановленим прапором SYN (synchronize). На нього сервер повинен відповісти комбінацією прапорів SYN + ACK (acknowledges). Після цього клієнт повинен відповісти пакетом з прапором ACK, після чого з'єднання вважається встановленим

У результаті під час атаки сервер відповідає пакетом SYN-ACK, а машина зловмисника повинна відправити ACK-відповідь, але не відправляє. Результат: відкриття і підвисання величезної кількості активних з'єднань, які закриваються тільки після закінчення таймаута. При перевищенні граничної кількості запитів / відповідей сервер жертви перестає приймати пакети будь-якого типу і стає недоступним. Цей тип DDoS атаки важко відфільтрувати, оскільки не зрозуміло, яке із з'єднань потрібно розірвати, щоб не нашкодити реальним користувачам. У більшості випадків ефективно відбити таку атаку можна лише за допомогою спеціального обладнання CISCO, Mikrotik або спеціально налаштованого кластера. Однак можна спробувати зменшити атаку за допомогою iptables. Наприклад, виконати правило:

iptables -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst 3 -j RETURN,

де --limit 1/s: максимальна кількість з'єднань в секунду; --limit-burst 3: максимальна початкова кількість пакетів для відповіді.

Так ми обмежимо кількість спроб з'єднань для одного бота мережі, що використовуються для атаки.

Як і у випадку з SYN-флудом таку атаку важко відбити, якщо вона здійснюється за допомогою ботнет мережі. Зменшити силу атаки можна аналогічно, обмеживши кількість нових з'єднань на секунду. Так обладнання працюватиме з обмеженою кількістю користувачів. Все ж менша кількість користувачів (які достукаються до сервера) краще, ніж ніхто. Обмежити можна також iptables правилом:

iptables -A INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above 20 -j REJECT --reject-with tcp-reset

Сучасні програми для роботи веб-сервера (nginx, apache) мають влаштований фільтр від такого роду атаки, який працює за принципом: лімітування кількості з'єднань на хвилину чи для одного ip- з'єднання.

Висновки

Описано та проаналізовано основні сучасні способи моніторингу та аналізу трафіку комп'ютерних мереж. Для ефективного моніторингу мережі створено власний аналізатор роботи комп'ютерної мережі, який призначений для автоматизованого збирання інформації з мережевих пристроїв та забезпеченню процесу контролю роботи каналів зв'язку. Розглянуто та проаналізовано види DDoS атак, методи їх моделювання та вивчено проблеми, що виникають у разі їх використання. Проведено моніторинг мережевого обладнання та розроблені правила для боротьби з DDoS атаками. В результаті роботи дані кінцевого обладнання візуально зображено на графіку, де можемо спостерігати значне зменшення (більше ніж у 4 рази) трафіку після його фільтрування сервером (маршрутизатором) з налаштованим фаєрволом згідно з розробленими правилами. На основі аналізу трафіку безкоштовного програмного забезпечення показано, як боротися та моніторити деякі види атак DDoS'у. Не існує універсальної панацеї від усіх видів атак, а тому насамперед ефективніше ліквідувати причину атаки, а не її результат.

Класифіковано та описано види DDoS атак та показано, як звести до мінімуму простої та збитки, завдані таким втручанням в мережу. Запропоновано декілька алгоритмів, які допоможуть вберегтися від атак або значно знизити їх негативний вплив. Ефективність запропонованих методів підтверджено експериментальними дослідженнями на основі розробленої інформаційної технології.

1. Alisha Cecil, "A summary of Network Traffic Monitoring and Analysis Techniques Whitepaper", 2006, [Електронний ресурс]. – Режим доступу: http://www.cs.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index.html 2. Jan Engelhardt and Nicolas Bouliane. Writing Netfilter modules. Revised, February 07, 2011. 3. Ed Wilson, "Network Monitoring and Analysis: A Protocol Approach to Troubleshooting", Prentice Hall PTR, 2013. 4. Laura Chappell. "Wireshark (R) 101: Essential Skills for Network Analysis". Laura Chappell University, 2013. 5. Shui Yu, "Distributed Denial of Service Attack and Defense" (SpringerBriefs in Computer Science), Springer–Verlag New York, 2014. 6. Tee Huu, "Evaluation of a Multi-Agent System for Simulation and Analysis of Distributed Denial-of-Service Attacks. New edition", 2013, [Електронний ресурс]. – Режим доступу: http://www.dtic.mil/dtic/tr/fulltext/u2/a420448.pdf 7. Lysenko S. Botnet detection technique for corporate area network / Lysenko S., Savenko O., Kryshchuk A., Kljots Y. Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), Berlin, DE, IEEE. – 2013. – P. 315-320. 8. Pomorova O. Multi-agent based approach for botnet detectionin a corporate area network using fuzzy logic / Pomorova O., Savenko O., Lysenko S., Kryshchuk A. // Computer Networks 20th International Conference, CN 2013, Lwówek Śląski, Poland, June 17–21. – 2013. – P. 243–254 9. Juniper Official Website, [Електронний ресурс]. – Режим доступу: http://www.juniper.net/techpubs/software/junos-es/junos-es93/junos-es-swconfig-security/understanding-icmp-flood-attacks.html.