УДК 004.056.53
DOI: 10.31673/2409-7292.2024.020009

Щербина Ю. В., Казакова Н. Ф., Логінова Н. І., Фразе-Фразенко О. О., Базаров Д. А.

СУЧАСНІ ПІДХОДИ ДО ЗАХИСТУ ВІД РОЗПОДІЛЕНИХ АТАК НА ВІДМОВУ В ОБСЛУГОВУВАНІ

У статті розглядаються проблеми, пов'язані із захистом від DDoS-атак, що приводять до значних фінансових втрат приватних компаній, які використовують Web-технології для надання своїх послуг у Internet-середовищі. Швидке зростання Internet-залежності бізнесу корпоративного сектора, робить одною з головних його проблем захист від атак типу "відмова в обслуговуванні", складність боротьби з якими пояснюється можливістю їх організаторів приховувати адресу джерела нападу та адреси усіх мережних суб'єктів, задіяних в сценарії атаки. В статті надано аналіз підходів до боротьби з загрозами від розподілених мережних атак і показано, що ефективний захист визначається своєчасним виявленням нападу, аналізом хибного мережного трафіку та його фільтрацією з одночасним блокуванням джерел атаки. Описано задачі, що вирішуються системами виявлення вторгнень IDS та системами запобігання вторгненням IPS, а також їх складові частини та способи використання на основі аналізу стандарту NIST Special Publication 800-94. Додатково описано процедури управління захистом від розподілених мережних атак, та визначення ризиків від реалізації загроз такого типу, на основі галузевих стандартів Open Group, що описують таксономію ризиків (O-PT) та аналіз ризиків (O-RA), орієнтованих на використання методології факторного аналізу інформаційних ризиків FAIR.

Ключові слова: DDoS атака, Web-технології, IDS, IPS, IDPS, FAIR.

Вступ

Протягом кількох останніх десятиріч технології атак на ресурси інформаційно-комунікаційних систем постійно удосконалюються, зростає їх складність і частота нападу, а їх вплив проводить до серйозних економічних втрат. Особливе місце серед різноманіття мережних атак займають, так звані, "атаки на відмову в обслуговувані" (DoS – Denial-of-Service) або "розподілені атаки на відмову в обслуговувані" (DDoS – Distributed Denial-of-Service) [1]. Їх ціллю є припинення обслуговування клієнтів атакованою системою за рахунок вичерпання обчислювальних ресурсів атакованих систем. Причинами таких атак, зазвичай, є недобросовісна конкуренція; здирництво; шпигунство; політичні мотиви або інше. Їх можуть здійснювати як звичайні зловмисники, вимагаючи сплати за припинення атак, так і недобросовісні конкуренти, що намагаються загальмувати розвиток бізнесу компанії-конкурента. Сьогодні, DDoS-атаки є особливо небезпечними в обчислювальних середовищах, які використовують хмарні технології, де вони здатні заблокувати надання послуг клієнтам та суттєво знизити продуктивність роботи обчислювальної мережі.

Постановка проблеми

Проблема боротьби з розподіленими "атаками на відмову в обслуговувані" полягає в тому, що зловмисник використовує ботнети (мережі скомпрометованих пристроїв), з метою перенавантаження мережного трафіку, і це дозволяє йому маскувати джерело атаки. Розглядають два типи таких атак: атаки на рівні додатків та атаки на рівні інфраструктури. На рівні додатків зловмисники використовують слабкі місця у протоколах, а на рівні інфраструктури вони використовують хмарні компоненти, такі як буфери TCP, процесорні компоненти, пропускну здатність каналів, сховища даних та інше [2]. Постійне ускладнення сценаріїв DDoS-атак і, особливо, використання багатовекторних атак такого типу, вимагає пошуку нових методів захисту, які передбачають своєчасне виявлення нападу, аналіз хибного мережного трафіку та його фільтрацію, а також блокування джерел атаки.

Аналіз останніх публікацій

Як показано в роботі [3], особливість DDoS-атак полягає в тому, що вони використовуються для виведення з ладу серверів, а також спотворення роботи системних служб Web-сайтів, що забезпечують управління такими системами, як Mastercard, PayPal, Visa, PSN, тощо [4]. Сучасна розподілена мережна DDoS-атака використовує керовані IRC-боти (Internet Relay Chat bot), розміщені на мережних комп'ютерах, що уявляють собою набори

сценаріїв, протоколи або програми, здатні підключатися до IRC-чату та ідентифікуватися як звичайні користувачі зі своїми власними IP-адресами.

Враховуючи, що DDoS-атаки дедалі більше стають однією з головних загроз мережної безпеки, помітно зростає активність робіт, пов'язаних з розробленням засобів своєчасного їх виявлення та попередження. Як показано в роботі [5], для виявлення зовнішніх вторгнень створюють системи виявлення вторгнень (Intrusion detection system – IDS), що уявляють собою сукупність програмного і апаратного забезпечення для виявлення несанкціонованого трафіку, параметри якого не відповідають вимогам мережної політики безпеки. Робота таких систем заснована або на моніторингу даних аудиту програмного забезпечення та операційних систем на кожному хості контрольованої мережі, або на моніторингу мережного трафіку, що виконується окремим керуючим хостом. Зазвичай, гібридні IDS системи використовують обидва ці способи виявлення нестандартної мережної активності [6].

Відмінність DDoS-атак полягає в тому, що існуючі IDS-системи визначають вторгнення вже після здійснення атаки і тому захиститись від них важко. Задача полягає у зменшенні негативних наслідків від їх реалізації. Враховуючи цей факт, до складу систем захисту додатково вводять системи запобігання вторгненням (Intrusion Prevention System – IPS). Така IPS-система уявляє собою програмне забезпечення, що включає всі можливості системи виявлення вторгнень IDS, а також має засоби для їх зупинки [7].

Роботами, пов'язаними з удосконаленням способів захисту від розподілених мережних атак активно займається лабораторія інформаційних технологій ITL (Information Technology Laboratory) американського національного інституту стандартів і технологій NIST (National Institute of Standards and Technology). У 2007 році цією організацією було випущено стандарт NIST Special Publication 800-94 [8], в якому, на основі накопиченого досвіду, викладено розроблені підходи до організації діяльності щодо забезпечення ефективного захисту від розподілених мережних атак.

Для підтримки належного рівня захисту від DDoS-атак, необхідно постійно слідкувати за відповідністю потужності систем захисту поточному рівню загроз в мережному середовищі. Відкрита група (The Open Group) для вирішення задач, пов'язаних з оцінкою ризиків від реалізації сучасних складних атак, опублікувала у 2021 році галузевий стандарт таксономії ризиків (O-PT) версія 3.01 [9], і додатковий галузевий стандарт аналізу ризиків (O-RA) версія 2.01 [10]. В ці стандарти було закладено методологію факторного аналізу оцінки ризиків FAIR (Factor Analysis of Information Risk), яка передбачає виконання детальної класифікації факторів, що визначають рівень ризиків від реалізації загроз, та взаємозв'язки між такими факторами. Використання FAIR технології дозволяє адекватно оцінювати як частоту реалізації загроз, так і масштаби можливих втрат.

Широка розповсюдженість DDoS-атак свідчить про наявність розриву між розумінням їх природи та успішним захистом від них. Сьогодні ринок пропонує велику кількість технологій, призначених для захисту від розподілених атак типу "відмова в обслуговуванні". Коректний вибір оптимальної з точки зору "ціна – якість" технології захисту вимагає розуміння принципів дії механізмів захисту та способів кількісної і якісної оцінки безпеки.

Мета і задачі дослідження

Зважаючи на те, що основною ціллю управління безпекою розподілених мережних систем є досягнення збалансованості між забезпеченням конфіденційності, цілісності та доступності інформаційних ресурсів і одночасним збереженням ефективності інформаційного обміну, ціллю роботи є обґрунтування рекомендацій, що забезпечують виконання цієї задачі.

Управління виявленням та попередженням DDoS-атак

Розподілені мережні атаки на відмову в обслуговувані найчастіше розділяють у відповідності до рівню OSI, на якому вони здійснюються. На мережному вірні (L3) вони використовують слабкі місця (уразливості) протоколів IP, DVMRP, ICMP, IGMP, PIM-SM, IPsec, IPX, RIP, DDP, OSPF, OSPF. На транспортному рівні (L4) вплив, зазвичай, відбувається

на протоколи TCP та UDP, а також на протоколи DCCP, RUDP, SCTP та UDP Lite. На прикладному рівні (L7), найчастіше, використовують атаки на такі протоколи як HTTP, HTTPS та DNS. Архітектура та принципи організації таких атак описані в [11]. Успішна їх реалізація викликає або переповнення мережного трафіку, або порушення логіки роботи системи великою кількістю некоректних запитів, і, як наслідок, відмову в обслуговуванні клієнтів. Програмні продукти, що реалізують сучасні технології захисту, не містять "чистих" IDS або IPS систем, тому стандартом [8] було введено поняття "Система виявлення та запобігання вторгненням" (Intrusion Detection and Prevention Systems – IDPS). В таких системах склад функцій, призначених для виявлення та запобігання вторгненням можна міняти шляхом відповідних налаштувань.

Склад реальної IDPS-системи захисту, що інтегрується в комп'ютерну систему, залежить від мережного середовища, вимог до захисту та рівню розвитку засобів захисту. В тім, стандарт [8] визначає основні наступні частини їх архітектури:

датчики або агенти, що забезпечують аналіз та контроль мережної активності, при чому термін "датчик" використовується на мережному рівні, а термін "агент" – на рівні хосту;

сервери управління, що аналізують дані про мережні події від датчиків або агентів та їх ідентифікують, у разі, якщо датчики та агенти цього зробити не можуть. Сервери управління можуть бути реалізовані у вигляді апаратного або програмного забезпечення. Іноді у складі IDPS їх може бути декілька;

сервери бази даних, що зберігають інформацію про події, виявлені серверами управління, датчиками або агентами;

консоль, яка уявляє собою програмно реалізований інтерфейс користувачів і адміністраторів IDPS.

Приклад такої архітектури наведено на рис. 1.

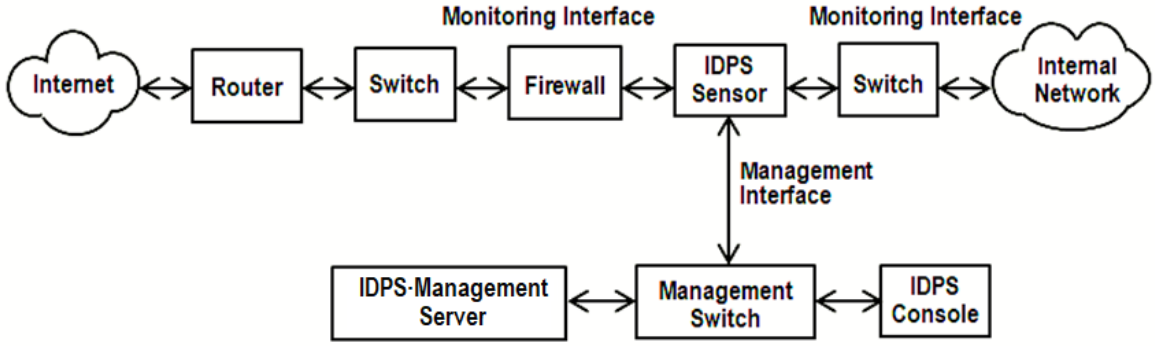

Рис. 1. Приклад вбудованої мережної архітектури IDPS

Захист сегменту мережі від розподілених атак вимагає правильного вибору місць розміщення датчиків IDPS, які можуть бути пасивними або активними. Активні датчики встановлюють так, щоб мережний трафік проходив через них так само, як він проходить через брандмауер. Фактично, деякі датчики такого типу уявляють гібридні міжмережні екрани та IDPS, а інші – просто IDPS. Зазвичай, їх ставлять там, де й інші засоби безпеки – на межі між мережами або між зовнішніми мережами та сегментами мереж, що вимагають захисту. Пасивні датчики відстежують копію фактичного мережного трафіку. Вони використовуються для зв'язку з відповідними портами, фізичним мережним середовищем, балансування навантаження та розподілення трафіку між мережними суб'єктами.

Розділення мережного трафіку між кількома датчиками IDPS може привести до зниження точності виявлення розподілених атак, якщо їх частини фіксуються в різних датчиках. Більшість методів зупинення вторгнень вимагають використання датчиків в активному режимі, оскільки пасивне відстеження трафіку не передбачає надійного способу попередження нападу. Система виявлення вторгнень може бути розміщеною перед фаєрволом з внутрішньої сторони мережі.

© Щербина, Ю. В., Казакова, Н. Ф., Логінова, Н. І., Фразе-Фразенко, О. О., & Базаров, Д. А. (2024). Сучасні підходи до захисту від розподілених атак на відмову в обслуговувані. Сучасний захист інформації, 2(58), 77–83. https://doi.org/10.31673/2409-7292.2024.020009.

В такому випадку IDPS буде аналізувати тільки той трафік, що не був заблокований фаєрволом, і це зменшить навантаження на систему. Такий спосіб підключення (рисунок 2) дозволяє забезпечити ефективний захист внутрішньої мережі від DDoS атак у межах пропускної здатності каналу.

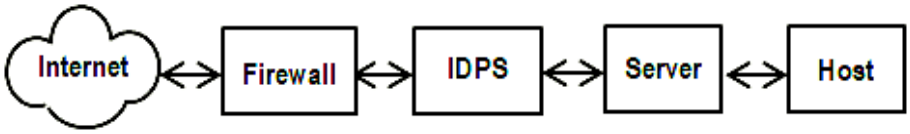

Рис. 2. Розміщення IDPS після фаєрволу

Але IDPS можна, також, поставити і перед фаєрволом. В такому разі, вона буде контролювати мережні рівні з 4-го по 7-й (рис. 3). Тобто, це буде система сигнатурного типу, яка забезпечує менше число хибних рішень. Іноді допускається встановлення кількох копій системи IDPS в різних місцях внутрішньої мережі з урахування пріоритету їх важливості [11]. Остаточно місце розташування IDPS обирається, виходячи із вимог до захисту, наявними ресурсами і конфігурацією мережі.

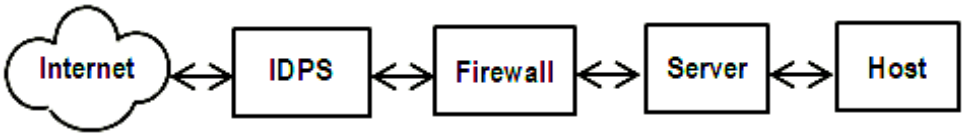

Рис. 3. Розміщення IDPS перед фаєрволом

Такий спосіб підключення передбачає накопичення результатів аналізу трафіку і виявлення факту наявності атаки. Якщо така атака буде виявленою, підключаються засоби видалення із загального мережного потоку його нелегітимної частини.

Останнім часом, для усунення або зменшення наслідків від впливу DDoS-атак, як доповнення до традиційних локальних систем захисту, використовується хмарні технологій. Вони містять ресурси для зупинення великих об'ємних розподілених атак, сформованих мережними ботами, фільтрації мережного трафіку та подальшим перенаправленням його адресатам. Враховуючи динамічний багатовекторний характер DDoS-атак, рекомендується об'єднувати в одну систему як локальні, так і хмарні рішення автоматизованої інтеграції, що забезпечують динамічний адаптивний захист. Прикладом комерційної системи хмарного захисту від DDoS-атак, яка використовує алгоритм адаптивного захисту на основі, як власних дата-центрів, так і на основі хмарних технологій, є система **Arbor Cloud DDoS Protection**. Для великих об'ємів хибного трафіку вона використовує хмарні технології, а для атак низького рівню – власні засоби фільтрації Pravail APS/FW/IPS, як це показано на рис. 4. Послуги захисту такого типу надаються на комерційній основі на певний термін.

Останнім часом, система **Arbor Cloud доповнюється спеціалізованим продуктом** Arbor Network ATLAS, призначеним для раннього визначення нападу та накопичення даних, що збираються в основних мережних вузлах, де визначаються індикатори компрометації (Indicator of Compromise – IOC), необхідні для визначення ризиків від реалізації DDoS-атак, а також, для усунення наслідків від реалізації загроз та зниження втрат.

На рис. 5 наведено приклад використання технології Arbor Network ATLAS в захищеному мережному сегменті.

Сьогодні DDoS-атаки використовують динамічну комбінацію декількох векторів атаки наступних видів [12]:

об'ємні (Volumetric) атаки, що займають широку полосу пропускання, наприклад, UDP-flood атаки для насичення мережних каналів та маршрутизаторів;

атаки з вичерпанням стану TCP (TCP State-Exhaustion), наприклад, TCP-SYN атаки для заповнення таблиць станів TCP у між мережних екранах та IDS/IPS;

атаки на прикладному рівні (Application-Layer), спрямовані на повільне вичерпання ресурсів серверів прикладних додатків, наприклад атаки на HTTP-заголовки або SlowLoris-атаки.

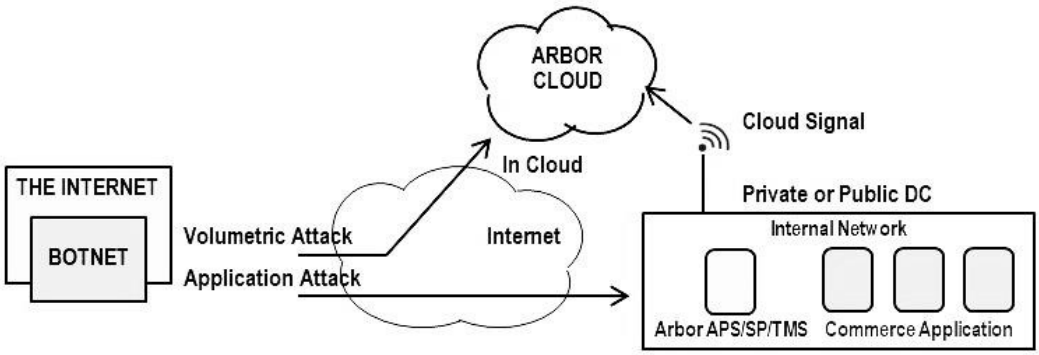

Рис. 4. Система **Arbor Cloud DDoS Protection**

Багатовекторні DDoS-атаки (Multi-vector DDoS attacks) відомі давно і особливо небезпечними їх робить постійний розвиток хмарних технологій та інтернету речей. Зі збільшенням кількості багатовекторних атак стало зрозуміло, що зниження ризиків від їх реалізації, вимагає використання багатоешелонованого захисту. Ефективне управління захистом від DDoS-атак передбачає відповідність обраних засобів захисту, що визначаються налаштуваннями системи Arbor Cloud DDoS Protection і реальним рівнем загроз від атак такого типу та ризиків від їх реалізації. Облік ризиків від розподілених багатовекторних атак, у порівнянні з іншими типами загроз, уявляє собою більш складну задачу, через необхідність урахування великої кількості факторів, зв'язки між якими не завжди очевидні і зрозумілі.

Складність процедури оцінки ризиків визначається тим, що процеси, пов'язані з безпекою, взагалі важко піддаються формалізації і така оцінка, зазвичай, виконується на якісному рівні. Саме для вирішення цієї проблеми, Open Group створила стандарти [9, 10], де викладено правила оцінки ризиків з використанням спеціально розробленої методології факторного аналізу FAIR, яка містить класифікацію факторів, що утворюють ризик, та обумовлюють один-одного.

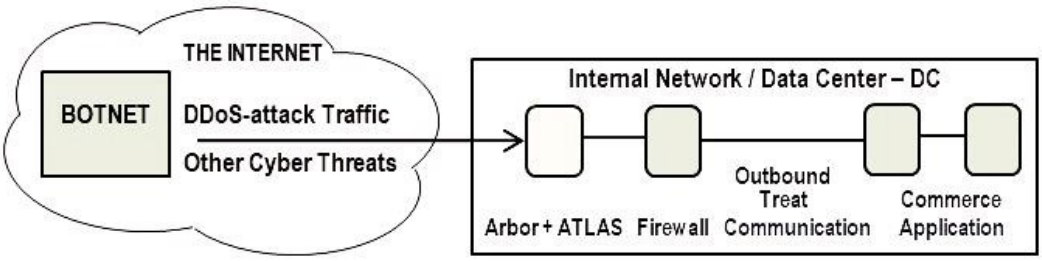

Рис. 5. Втілення Arbor Network ATLAS в систему захисту

Теорія управління безпекою визначає ризик як сукупність частоти реалізації загрози, вразливості системи захисту, цінності активу, а також ймовірності вдалої реалізації атаки. Причому загроза розглядається як потенційно можливі події, направлені на порушення встановленої політики безпеки та приводять до відповідних втрат. Вразливість системи захисту – це слабке місце будь-якої її частини, яка може бути використана у сценарії атаки на інформаційний ресурс. Цінності активу, зазвичай, визначається у грошовому вимірі. Що

стосується ймовірності реалізації атаки, то її важко отримати аналітично і, тому, вона найчастіше визначається експертними методами.

Визначення ризиків від реалізації DDoS-атак, на відміну від атак, що здійснюються з одного джерела нападу, вимагає врахування значно більшої кількості факторів і, таким чином, уявляє собою значно складнішу аналітичну задачу. Саме з цієї причини була розроблена методологія FAIR, яка надає обґрунтовану і логічну основу для оцінки ризиків і складається з наступних складових частин:

класифікація факторів, з яких складається інформаційних ризик, та визначення набору стандартних термінів;

методика оцінки факторів, що приводять до виникнення ризиків, у тому числі частота виникнення, вразливості і втрати;

схема обчислень, що дозволяє виконувати кількісну оцінку ризиків методами математичного моделювання, з урахуванням зв'язків між визначеними факторами;

імітаційна модель, що дозволяє на основі класифікації факторів, методики їх оцінки та схеми обчислень виконувати аналіз ризиків будь-якого ступеня розміру і складності.

Крім стандартів [9, 10], групою Open Group було випущено документ Open FAIR™ Risk Analysis Process Guide [13], в якому викладено послідовність проведення робіт, пов'язаних з оцінкою ризиків. Методика, описана в цьому документі, є універсальною і передбачає виконання наступних семи етапів, ітераційне виконання яких, дозволяє довести рівень ризику до прийнятної величини.

1. Формальне визначення сценарію ризику та з урахуванням активів, що знаходяться під загрозою, типу загрози та її впливу на активи у разі успішної реалізації.
2. Аналіз частоти виникнення загроз та оцінка величини відповідних втрат.
3. Оцінка первинних і вторинних факторів втрат.
4. Визначення вразливостей у системі захисту з урахуванням потужності загрози та рівнем захищеності в поточному стані.
5. Визначення ризиків та створення звіту про поточний стан безпеки.
6. Повторення 4 етапу з визначенням ризиків у наступному стані.
7. Повторення 5 етапу для наступного стану.

Важливо розуміти, що ризик виражається через ймовірність певних втрат за визначений термін. Методологія, описана в стандартах Open FAIR, описує спосіб декомпозиції ризику і надає калібровані інструменти для створення конкретного сценарію його кількісного аналізу. Таксономія ризику Open FAIR включає два його підфактори: частоту нанесення втрат і та їх величину, як це показано на рис. 6.

Рис. 6. Таксономія ризиків методології Open FAIR

Методикою Open FAIR передбачається, що останні два етапи оцінки ризику, ітераційно повторюються допоки остаточний ризик не стане прийнятним.

Висновки

Сьогодні світ поступово наближається до прямої залежності від інформаційних технологій та онлайн доступу до мережних ресурсів. З урахуванням зростання складності інформаційних технологій, що використовуються для надання послуг у відкритому мережному Internet-просторі, з великою швидкістю зростає здатність зловмисників створювати нові ефективні сценарії атак. У боротьбі з DDoS-атаками звичайні мережні екрани виявляються мало ефективними. Особливо небезпечними є багатовекторні комбіновані атаки, що здатні приховувати ідентичність джерела атаки через множинні адреси та механізм хаотичного розповсюдження. Такі атаки включають декілька етапів і використовують більш високий рівень планування та координації суб'єктів, задіяних у нападі. Поступове зростання ефективності технологій нападу вимагає суттєвих зусиль у напрямі розвитку нових стратегій і багатоешелонованого захисту від DDoS-атак. Сучасні рішення Arbor Cloud та Arbor APS, а також наявність стандартів, що описують порядок створення систем IDS та IPS і визначають процес оцінки ризиків, дозволяють знизити економічні втрати від нападу до прийнятних величин.

Перелік посилань

1. Netscout. DDoS Threat Intelligence Report / Findings from 1st half 2023. Internet Traffic and Slipstreamed Threats. DOI:10.30534/ijatcse/2019/12812019. URL: https://www.netscout.com/threatreport/internet-traffic-slipstreamed-threats/

2. Alashhab, Z. R., Anbar, M., Singh, M. M., Alieyan, K. "Detection of HTTP Flooding DDoS Attack using Hadoop with MapReduce: A Survey". February 2019. International Journal of Advanced Trends in Computer Science and Engineering 8(1) URL: https://www.warse.org/IJATCSE/static/pdf/file/ijatcse12812019.pdf

3. Tripathi, S., Gupta, B., Almomani, A., Mishra, A., Veluru, S. "Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks". Journal of Information Security. Vol. 4 No. 3 Article ID: 34629, 2013, 150-164 p. DOI:10.4236/jis.2013.43018. URL: https://www.scirp.org/pdf/JIS_2013071615001745.pdf

4. Prasad, K., Reddy, A. and Rao, K. DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey. Global Journal of Computer Science and Technology, 2014. URL: https://www.researchgate.net/publication/283894681_Detection_of_known_and_unknown_DDoS_attacks_using_Artificial_Neural_Networks

5. Mahajan, D., Sachdeva, M. DDoS attack prevention and mitigation techniques – a review. Int. J. Comput. Appl., 2013, vol. 67, no. 19, 21–24 p. DOI: 10.5120/11504-7221 URL: https://research.ijcaonline.org/volume67/number19/pxc3887221.pdf.

6. Tiwari, M., Kumar, R., Bharti, A., Kishan, J. Intrusion Detection Systems. International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com, Volume 5, Issue 2 (March – April 2017), 38-44 p. URL: https://www.researchgate.net/publication/316599266_INTRUSION_DETECTION_SYSTEM.

7. Abdelkarim, A. A., Nasereddin, H. H. O. Intrusion prevention system. International Journal of Academic Research Vol. 3. No.1. January, 2011, Part II. 432-434 p. URL: https://www.researchgate.net/publication/281120779_INTRUSION_PREVENTION_SYSTEM.

8. Guide to Intrusion Detection and Prevention Systems (IDPS). Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-94. February 2007 URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf

9. The Open Group Risk Taxonomy (O-RT) Standard, Version 3.0.1. https://pubs.opengroup.org/security/o-rt/

10. The Open Group Risk Analysis (O-RA) Standard, Version 2.0.1. URL: https://pubs.opengroup.org/security/o-ra/#:~:text=The%20objective%20of%20the%20Risk,to%20perform%20effective%20risk%20analysis.

11. Sharifi, A., Zad, F. F., Farokhmanesh, F., Noorollahi, A., Sharifi, J. An Overview of Intrusion Detection and Prevention Systems (IDPS) and Security Issues. IOSR Journal of Computer Engineering (IOSR-JCE). e-ISSN: 2278-0661, p-ISSN: 2278-8727. Volume 16, Issue 1, Ver. I (Jan. 2014), 47-52 p. URL: https://www.researchgate.net/publication/273720500_An_Overview_of_Intrusion_Detection_and_Prevention_Systems_IDPS_and_Security_Issues.

12. Rajamannar, K., Paravel, A., Rangasamy, S., Pandi, V. Classifications of DDoS Attack – A Survey. ISSN: 0193-4120 Page No. 12926 – 12932. March-April 2020. URL: https://www.researchgate.net/publication/341190040_Classifications_of_DDoS_Attack_-_A_Survey

13. Open FAIR™ Risk Analysis Process Guide. Document Number: G180. Published by The Open Group, January 2018. URL: https://pubs.opengroup.org/security/openfair-process-guide/

Надійшла 08.05.2024