УДК 009.4

А.Т. Кобевко [1],
О.В. Тимченко [1, 2]

НЕЧІТКЕ ДЕРЕВО РІШЕНЬ ДЛЯ МЕРЕЖЕВОГО ЗАХИСТУ ВІД DoS-АТАК

Abstract. An Intrusion Detection System is a tool that can detect intrusions into a host, network, and application. DoS attack is one of the most common network attacks. During this time, the host sends a huge number of packets per machine and thus slows down the network and the host. There are a number of algorithms for detecting DoS attacks, and most of these solutions generate a high number of false alarms. The paper considers a new method of constructing a fuzzy solution tree for monitoring network flow in case of Smurf, Mail-Bomb and Ping-of-Death attacks.

Постановка проблеми. Швидке зростання кількості DoS-атак на хости, мережі або додатки спонукає дослідників створити ефективний спосіб їх зупинення. Очевидним рішенням є створення системи, яка виявить вторгнення з найменшою похибкою та достатньо швидко. Частота виявлення помилкових результатів не задовольняє користувачів, особливо для систем виявлення в основі яких лежить аналіз аномалій.

Мета статті. Побудувати нечітке дерево рішень для моніторингу мережевого потоку у випаду атак Smurf, Mail-Bomb та Ping-of-Death.

Основна частина

Різке збільшенням кількості користувачів та постачальників послуг Інтернету призводить до зменшення мережевої безпеки, тому постачальники послуг завжди шукають рішення для моніторингу та перевірки пакетів, що надходять з клієнтської сторони, щоб уникнути будь-яких атак.

Механізми безпеки, які використовуються в мережі, мусить запобігати будь-якій атаці. Оскільки він не може повністю перешкоджати атакам, необхідний новий рівень безпеки, мета якого виявити та припинити атаку якнайшвидше.

Система виявлення вторгнень IDS (Intrusion Detection System) динамічно контролює дії, що здійснюються в заданому середовищі, наприклад хості і мережі. Вона вирішує, чи є ці дії симптомами нападу або ж вони представляють законне використання оточення. Два найпоширеніші методи виявлення, які можна застосувати в IDS, - це виявлення на основі сигнатур та виявлення на основі аномалії.

Техніка виявлення на основі сигнатури в IDS шукає характеристики

[1] Українська академія друкарства
[2] University of Warmia and Mazury Olsztyn, Poland

відомих атак, і намагається знайти схожість між попередньою поведінкою системи або мережі з характеристиками відомої атаки в базі даних сигнатур. Однак, ця техніка не може виявити нові атаки.

Техніка виявлення аномалій приймає нормальний стан мережевого трафіку або поведінку хоста як критерії аномалії. Таким підходом можна виявити невідомі напади, проте створює відсоток помилок через труднощі у визначенні нормального стану мережевого трафіку.

DoS-атака використовує ресурси хоста та мережі так, щоб звичайний користувач не міг отримати доступ до сервера.

Для виявлення вторгнення ряд дослідників використовують штучний інтелект, обмін даними та нечіткі методи кластеризації. Останнім часом нечіткі системи виявлення вторгнень довели стійкість до шуму, здатність до самонавчання та здатність будувати початкові правила без необхідності апріорних знань.

Хоча існують різноманітні підходи для виявлення DoS-атак, практика виявлення вимагає вищої точності та ефективності. Тому фахівці з інформаційної безпеки намагаються покращити механізм виявлення DoS-атак різними алгоритмами.

Рішення та методологія

Процес розв'язання поставленої проблеми поділяється на етапи проектування та аналізу. Після визначення цілей вивчаються попередні дослідження та методи, які використовуються різними дослідниками. Потім розробляється система, яка базується на цих дослідженнях, з метою поліпшення захисту. На другому етапі, який називається аналізом, визначається наслідок проектування та його вплив на вдосконалення системи.

В розробленому алгоритмі нечітка логіка обробляє дані, отримані з мережевого потоку, щоб знайти вторгнення. Даними для дослідження є накопичена інформація після виявлення атак. Збирається основна та загальна інформація про IDS, а потім робиться висновок про DoS-атаки та їх поведінку. Ці дослідження показують дві важливі проблеми в IDS - це низька швидкість і повільне виявлення DoS-атак.

Запропоноване рішення - це моніторинг потоку мережі за допомогою нечіткої системи для збільшення швидкості та якості виявлення DoS-атаки.

Проектування

На цьому етапі робиться дослідження суміжних робіт та докладно аналізується механізм подібних систем, щоб з'ясувати, який механізм слід використовувати для виявлення DoS-атак. Більшість DoS-атак мають власну сигнатуру, тому швидкість виявлення за цією ознакою є вищою.

Систему налаштовують таким чином, щоб досягти цілей, які були поставлені на етапі визначення проблеми, а також враховувати інформацію із зібраних даних. Зауважимо, що сконструйований компонент, має мати правильний вихід з кожного модуля та всієї системи (звіт про атаку).

Аналіз

Система стежить за мережевим трафіком і розглядає всі пакети в потоці. Нечіткий алгоритм знаходить підозрілий пакет і зберігає ці потоки в масиві. Зрештою, нечітке дерево рішень перевіряє заголовки підозрілого потоку та у випадку нападу система генерує помилку.

Перевірити показники швидкості та ефективності застосування нечіткої системи можна на вибірці трафіку, який надає Агентство прогресивних науково-дослідних проектів оборони (DARPA) з Лінкольнської лабораторії Массачусетського технологічного інституту (MIT). Результатом цієї фази буде розробки нечіткого алгоритму для виявлення DoS-атак.

Розробка системи

Розглянемо рішення детальніше, щоб показати всі процеси та вплив на продуктивність і точність системи. Спочатку опишемо архітектуру системи, потім - нечіткий алгоритм та мережеві потоки. Детальний опис застосування нечіткого алгоритму та мережевого потоку на IDS, супроводжується аналізом покращення виявлення DoS-атак та швидкості.

Архітектура

На рис. 1 показана структура системи. IDS збирає всі пакети зі зразка трафіку і розміщує їх всередині потоків, щоб зберегти всередині пам'яті. Нечіткий алгоритм збирає будь-які підозрілі пакети і відносить їх до підозрілого потоку. Щоразу, коли підозрілий потік закінчується, нечіткий алгоритм перевірятиме його на остаточний звіт про атаку.

Дані попередньої обробки

TCP та ICMP-пакети з мережі калібруються, а мережеві потоки будуються мережевим обробником. Ідентифікація потоків для пакетів TCP базується на кількості пакетів з одного джерела, призначення, порту джерела та порту призначення. Процес починається з пакета SYN і закінчується, коли приходить FIN-пакет. З іншого боку, для протоколу ICMP, можна визначати два типи пакетів. Перший пакет містить запит від однієї машини до іншої, а другий пакет - відповідь на запит. Обробник мережевого потоку перевіряє мережеві потоки на наявність будь-яких аномалій. Найпоширеніші проблеми IDS - помилка хибного виявлення та помилка пропуску атаки, швидкість виявлення, продуктивність та швидкість роботи загалом. Використовуючи мережевий потік для вхідного сигналу та застосовуючи нечітке дерево рішень для виявлення вторгнень, результат може мати меншу кількість хибнопозитивних помилок та кращу швидкість виявлення.

Основні сигнатури

Як було зазначено раніше, метою даної роботи було виявити 4 типи DOS-атак у вибірці трафіку DARPA. Опис кожної атаки наведено нижче.

1. Land атака

Якщо TCP - протокол вхідного пакета, а вихідний IP і цільовий IP однакові між собою, вихідний порт дорівнює порту призначення, відбувається Land-атака.

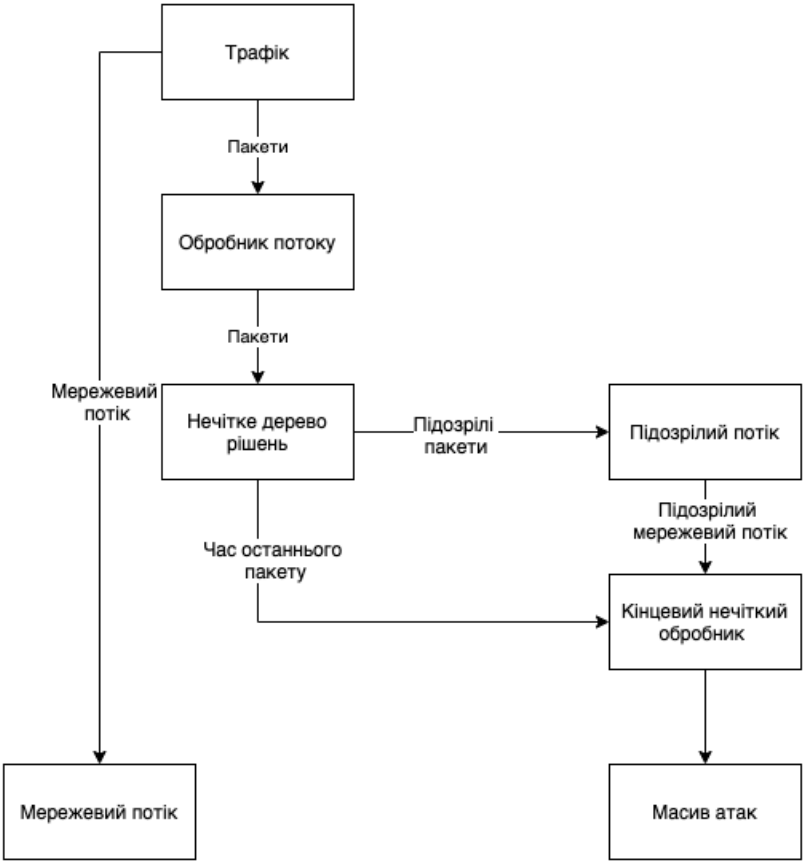

Рис. 1. Структурна схема системи

2. Mail Bomb атака

Атака відбувається за допомогою встановлення одного TCP-з'єднання між двома комп'ютерами. У цьому потоці SMTP-порт використовується для надсилання електронної пошти, але кількість пакетів в одному потоці становить близько 10000 пакетів, а розмір кожного пакету - близько 1000 байт. Таким чином розмір потоку становитиме близько 10 Мбайт.

3. Smurf атака

Атака відбувається за допомогою потоку ICMP. Кількість пакетів в одному потоці невелика, але розмір кожного пакету становить приблизно 1000 байт. Однак потік буде масштабним, оскільки кілька комп'ютерів надсилають великий пакет на один комп'ютер. Пакет містить повідомлення відповіді, але запит повідомлення не надсилається жертвою.

4. Атака за допомогою пінг-пакетів

В одному потоці з одного комп'ютера на інший надсилається велика кількість IP-пакетів великого розміру. Кожен пакет має близько 1000 байт і розмір потоку атаки близько 64 000 байт. Він знаходиться за протоколом ICMP, що викликає перезавантаження, заморожування та збій машини жертви.

5. Нечіткі множини

Нечіткі множини складаються з 0 і 1, тому може бути лише два варіанти відповіді. Але в нечіткій логіці при поєднанні декількох нечітких множин може бути кілька відповідей.

Нечіткий обробник шукає підозрілі пакети, щоб змінити стан потоку з нормального на підозрілий для швидкого виявлення. Цей підпроцес буде підозрілим для пакетів, які мають такий атрибут (форма псевдокоду):

Для Land атаки використовуються правила:
ЯКЩО flowprtcl дорівнює TCP
ЯКЩО flowrc дорівнює flowdest
Запис у масив Land атаки
Для Mail Bomb атаки застосовується правило:
ЯКЩО flowprtc дорівнює TCP
ЯКЩО flowdestPort дорівнює SMTP
ЯКЩО потоки > 10 Мб
Запис у масив атаки Mail Bomb
Для атаки Smurf застосовується правило:
ЯКЩО flowprtc дорівнює ICMP
ЯКЩО інформація містить відповідь
ДЛЯ Пакет з останньої хвилини, до цього Пакету, йдіть один за одним
ЯКЩО інформація не містить Запит від тієї ж машини
Записати до масиву атаки Smurf
Для атаки за допомогою пінг-пакетів застосовується правило:
ЯКЩО flowprtc дорівнює IP
Якщо інформація містить ICMP
Запис у масив Ping of Death

Висновки

Описана конструкція нечіткого дерева рішень, яка може виявити чотири типи DoS-атак шляхом аналізу мережевого потоку. Запропонована архітектура є орієнтиром для розроблення і впровадження системи. Експерименти проводилися з використанням набору даних DARPA.

Попередні рішення щодо IDS базувалися на методі виявлення, який використовував дані пакетів і призводив до хибних помилок. У цьому дослідженні дизайн IDS був зосереджений на розв'язання проблеми, застосовуючи нечітке дерево рішень як процесор і мережевий потік як вхід

системи.

У цій системі спочатку обробляються всі пакети, а згодом будуються мережеві потоки. Під час цього процесу нечіткий обробник збереже всі підозрілі пакети в пам’ять. Коли генерується заголовок потоку, підозрілий потік ще раз перевірятиметься нечітким обробником та виявлятимуться атаки.

1. Denial of Service (DoS) Attack Detection by Using Fuzzy Logic over Network Flows, https://www.researchgate.net/publication/26877049
2. SPADE, Silicon Defense, http://www.silicondefense.com/software/spice/.
3. Intrusion detection system, https://en.wikipedia.org/wiki/Intrusion_detection_system
4. https://www.networkworld.com/article/3073481/darpa-extreme-ddos-project-transforming-network-attack-mitigation.html

http://doi.org/10.5281/zenodo.3859687

Поступила 3.10.2019р.

УДК 621.3

О.Б. Полусин, Львів

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ МУЛЬТИМЕДІЙНИХ ДАНИХ НАНЕСЕННЯМ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ

Abstract. An analysis of steganography methods was performed, which showed that broadband and statistical methods are more effective for the protection of multimedia objects. The use of other methods requires a lot of time or resources, so their introduction can be considered impractical.

Keywords: multimedia protection, digital watermark.

Вступ

Сучасне суспільство користується великою кількістю послуг, що стали більш доступніші за допомогою сучасних комп’ютерних мереж та інформаційних технологій. Сьогодні уся інформація представлена в цифровому вигляді, тому доступ до будь-якої інформації необхідно захистити від багатьох загроз: несанкціонованого доступу та використання, знищення, підробки, витоку, порушення ліцензійних угод, відмови відавторства та ін.

Захист інформації являється вкрай важливим завданням для усіх сфер діяльності, від комерційних до державних. Серед загроз для інформаційної сфери можна виділити: комп'ютерну злочинність; розголошення таємної чи

