УДК 004.2; 004.7

Є.В. РИНДИЧ[*], В.В. КОНЯШИН[*], С.В. ЗАЙЦЕВ[*], Я.Ю. УСОВ[*]

ОСОБЛИВОСТІ СТВОРЕННЯ МЕРЕЖЕВОЇ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ У КОМП'ЮТЕРНІ СИСТЕМИ

[*]Чернігівський національний технологічний університет, м. Чернігів, Україна

Анотація. *Досліджено існуючі мережеві системи виявлення вторгнень (Intrusion Detection System, IDS) на основі хоста (Host-based intrusion detection system, HIDS) та мережеві системи виявлення вторгнення (Network intrusion detection system, NIDS). Особливу увагу приділено системам з відкритим програмним кодом як таким, що надають можливість провести дослідження не лише роботи, а й архітектури програмного забезпечення та принципів їх реалізації. Досліджено такі системи, як Snort, Suricata, Bro IDS, Security Onion. Система Snort є лідером серед систем із відкритим кодом і отримала широке визнання як ефективне рішення мережевої системи виявлення вторгнень для широкого кола сценаріїв та випадків використання в локальних та корпоративних мережах. Визначено загальні риси мережевих систем виявлення вторгнень, їх позитивні та негативні особливості. Запропонована трирівнева «клієнт-серверна» загальна архітектура мережевої системи виявлення вторгнень із використанням веб-додатку. У порівнянні з дворівневою «клієнт-серверною» архітектурою або «файл-серверною» архітектурою трирівнева архітектура забезпечує, як правило, більшу масштабованість, кращу можливість конфігурування. Базовими шарами запропонованої архітектури є шар веб-додатків або кластер веб-додатків, шар сервера додатків, який може бути масштабовано, та шар баз даних. Визначено особливості побудови мережевих систем виявлення вторгнень на стороні сервера. Вузьким місцем усієї системи є набір підписів і незручний спосіб взаємодії з користувачем. Одна з найважливіших проблем сучасних систем полягає в тому, що даний набір не може відстежувати загрози, які не мали прецедентів у минулому. Тому основним напрямом досліджень є впровадження пошуку вторгнень на основі пошуку аномальної активності. Наступна проблема, що була виявлена та досліджувалась, полягає в розробці дружніх інтерфейсів. Дана проблема вирішується впровадженням веб-додатку, який може ефективно взаємодіяти з сервером і на якому розміщені системи виявлення вторгнень та база даних, що зберігає всю необхідну інформацію. Перспективними напрямами досліджень слід вважати розробку методів пошуку вторгнень на основі пошуку аномальної активності та їх впровадження в реальних комп'ютерних мережах.*

Ключові слова: *мережева система, виявлення вторгнень, підписи, категорії вторгнень, аналіз мережевого трафіка.*

Аннотация. *Исследованы существующие сетевые системы обнаружения вторжений (Intrusion Detection System, IDS) на основе хоста (Host-based intrusion detection system, HIDS) и сетевые системы обнаружения (Network intrusion detection system, NIDS). Особое внимание уделено системам с открытым кодом как таким, которые предоставляют возможность провести исследование не только работы, а и архитектуры программного обеспечения и принципов их реализации. Исследованы такие системы, как Snort, Suricata, Bro IDS, Security Onion. Система Snort является лидером среди систем с открытым кодом и получила широкое признание как эффективное решение сетевой системы обнаружения вторжений для широкого круга сценариев и случаев использования в локальных и корпоративных сетях. Определены общие черты сетевых систем обнаружения вторжений и их положительные и негативные особенности. Предложена обобщенная трехуровневая «клиент-серверная» архитектура сетевой системы обнаружения вторжений с использованием веб-приложения. По сравнению с двухуровневой «клиент-серверной» архитектурой или «файл-серверной» архитектурой, трехуровневая архитектура обеспечивает, как правило, большую масштабируемость, лучшую возможность конфигурирования. Базовыми слоями предложенной архитектуры являются слой веб-приложений и кластер веб-приложений, слой сервера приложений, который может масштабироваться, и слой баз данных. Определены особенности построения сетевых систем обнаружения вторжений на стороне сервера. Узким местом всей системы является набор подписей и неудобство взаимодействия с пользователем. Одной из важнейших проблем современных систем является то, что сейчас данный набор не может отслежи-*

ISSN 1028-9763. Математичні машини і системи, 2018, № 3

вать угрозы, которые не имели прецедентов в прошлом. Поэтому основным направлением исследований является внедрение поиска вторжений на основе поиска аномальной активности. Следующая проблема, которая была обнаружена и исследована, заключается в разработке дружественных интерфейсов. Данная проблема решается внедрением веб-приложения, которое может эффективно взаимодействовать с сервером, на котором размещены системы обнаружения вторжений и база данных, хранящая всю необходимую информацию. Перспективными направлениями исследований следует считать разработку методов поиска вторжений на основе поиска аномальной активности и их внедрение в реальные компьютерные сети.
Ключевые слова: *сетевая система, обнаружение вторжений, подписи, категории вторжений, анализ сетевого трафика.*

Abstract. *The existing network-based Intrusion Detection System (IDS) based host (Host-based intrusion detection system, HIDS) and network detection systems (Network intrusion detection system, NIDS) have been investigated. Special attention is paid to open source systems, as they provide an opportunity to research not only work principles, but the software architecture and the principles of their implementation. Systems such as Snort, Suricata, Bro IDS, Security Onion have been studied. Snort is a leader in open source systems and has been widely recognized as an effective network intrusion detection system solution for a wide range of scenarios and cases of use in local and corporate networks. Determine the general features of network systems to detect invasions and their positive and negative features. A generalized three-level «client-server» architecture of the network intrusion detection system using a web application is proposed. Compared to the two-level «client-server» architecture or «file-server» architecture, the three-tier architecture provides, as a rule, greater scalability, better configuration capability. The underlying layers of the proposed architecture are the web application layer or the web application cluster, the application server layer that can be scaled, and the database layer. Determine the peculiarities of building network systems for detecting server-side intrusions. The bottleneck of the entire system is a set of signatures and inconvenience of interaction with the user. One of the most important problems of modern systems is that this set cannot track threats that have not had precedents in the past. Therefore, the main direction of research is to introduce intrusion searches based on the search for abnormal activity. The next problem that has been discovered and investigated is the development of friendly interfaces. This problem is solved by the introduction of a web application that can efficiently interact with a server hosting intrusion detection systems and a database that stores all the necessary information. Prospective areas of research should be considered the development of methods for searching intruders based on the search for abnormal activity and their implementation into real computer networks.*
Keywords: *network system, intrusion detection, security, signatures, intrusion categories.*

1. Вступ. Актуальність теми дослідження

На сьогодні безпека є однією з найбільших проблем майже для всіх мереж у будь-якій галузі. Існує незліченна кількість шкідливих спроб долучитися до приватної інформації, мереж та веб-служб компаній, тому різні компанії використовували різні методи для забезпечення інструментів, апаратних та програмних компонентів, таких як брандмауери, механізми шифрування та віртуальні приватні мережі для захисту особистої інформації. Масове поширення та фактичне створення багатоелементних і багаторівневих корпоративних мереж призводить до необхідності забезпечувати безпеку й у середині мережі.

2. Постановка проблеми

Зараз існує тенденція мати систему виявлення вторгнень (Intrusion Detection System, IDS) у будь-якій мережі, оскільки атаки та загрози створюють потенційний ризик для мережевої та комп'ютерної систем. IDS може зіткнутися з великою проблемою під час раптової зміни категорій вторгнення, а також при великій обчислювальній потужності. Системи виявлення вторгнень – це «системи, які збирають інформацію з різних системних і мережевих джерел, а потім аналізують інформацію про ознаки вторгнення та зловживання» (Пауль Проктор, 2001) [1].

Найважливішою перевагою використання IDS є те, що IDS надає інформацію, якщо відбувається атака за певною системою. Через користувачів IDS відомо про те, в якому ризику і загрозі вони знаходяться. Багато інструментів може бути використано для захисту певної системи. Це такі, як брандмауери, IDS SNORT, Suricata і т.д. Дана стаття присвячена аналізу таких систем, виявленню особливостей та побудові системи, що буде належати до цього класу систем і яку в подальшому можна буде досліджувати та використовувати на практиці.

3. Аналіз останніх досліджень та публікацій

IDS, як правило, поділяються на два типи рішень: системи виявлення вторгнення на основі хоста (HIDS) та мережеві системи виявлення вторгнення (NIDS). HIDS встановлюються на кожному комп'ютері в мережі, щоб аналізувати та контролювати трафік, що надходить до відповідного вузла. Та з нього HIDS також відстежує та контролює локальні зміни файлів і можливі зміни через несанкціонований доступ та/або компроміс [2].

На відміну від цього, NIDS є стратегічно розташованою у різних точках мережі, щоб стежити за трафіком, що йде до мережевих пристроїв і з них. Рішення NIDS пропонують складні можливості для виявлення вторгнення в реальному часі, що часто складається зі збірки взаємодіючих частин: автономний пристрій, апаратні датчики та програмні компоненти є типовими складовими, що входять до NIDS. Ці компоненти дозволяють більше розширити спектр можливостей виявлення вторгнення в мережі, ніж при використанні HIDS.

Перш ніж перейти до перегляду широко відомих мережевих систем виявлення вторгнень, слід розглянути, як різні типи NIDS виявляють вторгнення.

NIDS може включати один із двох (або обидва) типів виявлення вторгнення у свої рішення: на підпис (Signature-based) і на основі аномалій (Anomaly-based) [3]. NIDS на базі підписів відстежує мережевий трафік на наявність підозрілих патернів у пакетах даних – «підписів» відомих шаблонів вторгнення в мережу – для виявлення та усунення нападів та компромісів. Використовуючи перелік відомих типів вторгнень та їх шаблонів даних, NIDS на основі підпису може швидко визначити вторгнення та розпочати відповідний курс дій.

NIDS на основі аномалій використовує базову лінію системи в нормальному робочому стані для відстеження наявності незвичної або підозрілої діяльності. Хоча для цього методу потрібен час для налаштування, оскільки для базового сценарію потрібно, щоб NIDS дізналася про вашу модель використання системи. Цей органічний евристичний підхід до виявлення вторгнень може бути більш гнучким та потужним, ніж підхід, що вимагає, щоб шаблон із попередньо існуючим типом вторгнень знаходився в переліці відомих типів вторгнень.

Snort є лідером серед систем з відкритим кодом. Незважаючи на відсутність графічного інтерфейсу або простого інтерфейсу адміністратора, цей інструмент отримав широке визнання як ефективне рішення мережевої системи виявлення вторгнень для широкого кола сценаріїв та випадків використання. Крім того, громада створила різні інтерфейси для вирішення проблеми відсутності графічного інтерфейсу. Snort використовує як виявлення вторгнення на основі сигнатур, так і методи, що базуються на аномаліях і можуть покладатися на створені користувачами правила або підписи, отримані з баз даних.

Suricata є прямим конкурентом Snort і використовує методологію, основану на підписах, безпеку, керовану правилами/політикою, та підхід, що базується на аномаліях, для виявлення вторгнень. Для деяких це рішення є сучасною альтернативою галузевому стандартному інструменту – Snort «на стероїди» з багатьма можливостями для потоку, прискоренням графічного процесора та численними моделями виявлення статистичних аномалій.

Bro IDS використовує виявлення вторгнень на основі аномалій і, як правило, застосовується у поєднанні з Snort, оскільки вони дуже добре доповнюють один одного. Слід зазначити, що Bro насправді є спеціальною мовою для мережевих додатків, в яких написано Bro IDS. Ця технологія особливо ефективна при аналізі трафіку і часто застосовується у випадках судової експертизи.

Security Onion [4] насправді є дистрибутивом Linux на базі Ubuntu для IDS та моніторингу мережевої безпеки (NSM) і складається з декількох вищезазначених технологій з відкритим кодом, які працюють у взаємозв'язку між собою. Платформа пропонує комплексне виявлення вторгнень, моніторинг безпеки мережі та управління журналами, об'єднуючи найкраще з Snort, Suricata, Bro, а також інші інструменти, такі як Sguil, Squert, Snorby, ELSA, Xplico та ін. Для випадків, коли необхідно отримати найкраще з вищезазначених інструментів в одному пакеті, варто використовувати Security Onion. У табл. 1 наведено порівняльний аналіз вищезазначених систем.

Таблиця 1 – Порівняльний аналіз існуючих IDS

Назва системи	Переваги	Недоліки
Snort	Дуже простий в установці, запуску та роботі. Велике ком'юніті користувачів, багато підтримуваних ресурсів, доступних в Інтернеті	Поставляється без графічного інтерфейсу, хоча існують додатки, розроблені ком'юніті. Обробка пакетів може бути повільною
Suricata	Може використовувати набори правил Snort. Має розширені функції, такі як багатопоточність і прискорення графічного процесора	Схильні до помилкових спрацьовувань. Системна та мережева ресурсомісткість
Bro IDS	Платформа може бути адаптована до різних випадків використання мережевої безпеки, в доповненні до NIDS	Необхідний певний досвід програмування. Отримання кваліфікації в Bro DSL може потребувати певних зусиль
Security Onion	Комплексний стек безпеки, що складається з декількох провідних рішень із відкритим кодом. Забезпечує простий інструмент налаштування для встановлення всього стеку	Як платформа, що складається з декількох технологій, Security Onion наслідує недоліки кожного компонента

4. Мета статті

Провести аналіз та виявити особливості роботи мережевих систем виявлення вторгнень. Запропонувати узагальнену архітектуру цього класу систем з урахуванням використання ними веб-додатків.

5. Виклад основного матеріалу

Мережеві системи виявлення вторгнень призначені для детектування атак у сегменті мережі, які знаходиться під управлінням одного адміністратора. Таким чином можна визначити IDS як систему, що використовується в корпоративних мережах, які можуть включати в себе територіально віддалені мережі, що використовують єдину політику безпеки. Джерелом інформації для них є мережевий трафік: заголовки і вміст мережевих пакетів.

Сучасні NIDS є розподілені і складаються з декількох компонентів. На рис. 1 наведено архітектуру та особливості роботи NIDS на прикладі Snort, яка складається з таких компонентів:

– аналізатор трафіку (sniffer);
– дешифратор пакетів (preprocessor);
– механізм виявлення (detection engine);
– набір правил (ruleset);
– система реєстрації/оповіщення (logger/alerter).

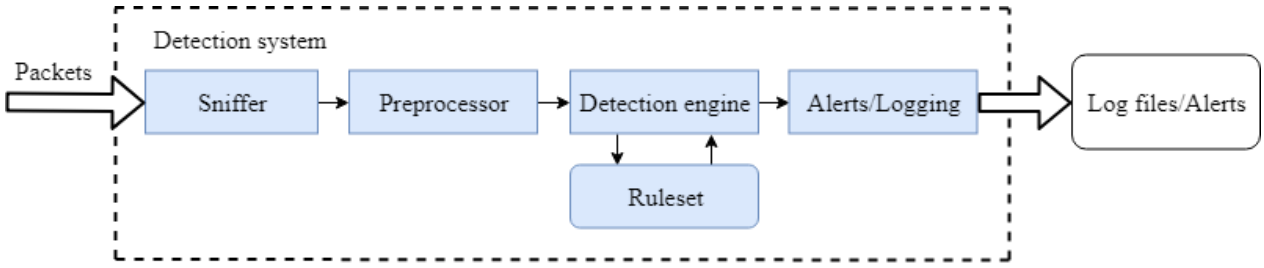

Рисунок 1 – Архітектура Snort

Аналізатор трафіку призначений для перехоплення і подальшого аналізу мережевого трафіку. Перехоплення трафіку здійснюється за допомогою бібліотеки pcap (libpcap – для Linux, WinPcap – для Windows) звичайним «прослуховуванням» мережевого інтерфейсу.

Дешифратор пакетів готує перехоплені пакети в форму типу даних, які потім можуть бути оброблені механізмом виявлення. Дешифратор пакетів може реєструвати Ethernet, SLIP і PPP-пакети.

Механізм виявлення аналізує і обробляє пакети, подані до нього «дешифратором», ґрунтуючись на правилах Snort (так як система виявлення в Snort працює на основі підписів). Змінні модулі можуть бути включені в механізм виявлення, щоб збільшити функціональні можливості Snort.

Набір правил включає в себе низку підписів (правил), на основі яких орієнтується механізм виявлення, і вже потім вирішує, чи є перехоплений трафік вторгненням.

Система реєстрації/оповіщення дозволяє реєструвати інформацію, зібрану дешифратором пакетів у легкому для читання форматі або повідомляти про виявлені загрози. За замовчуванням файли реєстрації збережені в каталозі /var/log/snort.

Snort має три режими роботи [5]:

1. Режим пакетного сніферу. В цьому режимі Snort читає і дешифрує всі мережеві пакети і формує дамп до stdout (ваш екран). Для перекладу Snort в режим сніффер використовуйте ключ –v.

2. Режим реєстрації пакетів. Цей режим записує пакети на диск і декодує їх в ASCII-формат.

3. Режим виявлення вторгнень. У цьому режимі Snort виступає як повноцінна мережева система виявлення вторгнень.

Саме третій режим відповідає принципам роботи NIDS. При правильному налаштуванні Snort можна досягнути досить високого рівня захисту мережі. Головним критерієм правильного налаштування системи є низка правил для виявлення всіх можливих категорій вторгнень. Для того, щоб цього досягти, використовується великий досвід, отриманий довготривалою експлуатацією системи. За тривалий час свого існування Snort накопичив велике ком'юніті, яке поповнювало перелік правил, і на сьогоднішній час число цих правил перевищує величину в 50 000. Оскільки система є гнучкою і орієнтована на кастомізацію

під потреби користувача, то є можливість самостійно розробляти потрібні підписи (правила).

Кожен підпис має поділ на дві частини: заголовок та опції. Заголовок підпису включає дію, протокол, IP-адресу і маски для відправника та отримувача, а також номери портів відправника та отримувача. Опції підпису включають повідомлення та інформацію про те, які частини пакета варто перевірити, аби визначити, чи слід прийняти по відношенню до пакета задану дію.

Нижче наведено приклад підпису:

alert tcp any any –> 192.160.0.0/24 111 \

(content: "| 00 01 86 a5 |"; msg: "mountd access";)

Опції підпису вказуються у круглих дужках, слова, за якими слідує двокрапка, є ключовими.

При дотриманні усіх вказаних у підписі умов по відношенню до пакета виконується задана підписом дія (генерація попередження у наведеному прикладі).

Заголовок правила має вигляд:

<Дія> <Протокол> <Відправник> <Порт> <Напрямок> <Отримувач> <Порт> (ключ: значення)

Заголовок правила містить ключове слово, яке визначає дію, виконувану при співпадінні всіх заданих підписом умов. Дія завжди вказується першою і може бути одним і наведених ключових слів:

1. Alert – сгенерувати сигнал з використанням обраного методу і записати інформацію про пакети в журнальний файл.

2. Log – записати інформацію про пакети в журнальний файл.

3. Pass – ігнорувати пакет.

4. Active – згенерувати сигнал і активізувати інше динамічне правило.

5. Dynamic – правило не виконує жодних дій до його активації за допомогою дії activate в іншому правилі, а при активації виконується як log.

Наступне поле заголовку вказує протокол, який буде відстежуватися.

Після протоколу в підписі вказуються адреси і номери портів для даного підпису. Ключовому слову any будуть відповідати всі адреси IP (0.0.0.0/0).

Номери портів можна задавати у вигляді конкретного значення, діапазону, переліку або ключового слова any (будь-який порт). Для портів також підтримується оператор заперечення. Для задання діапазону вказуються верхня та нижня границі, відокремлені двокрапкою (:).

Оператор напрямку –> вказує напрямок передачі трафіку для даного підпису. Адреси і порт ліворуч від цього оператора відносяться до відправника, а праворуч – до отримувача пакетів. Можна також створювати двонаправлені підписи за допомогою оператора <>. У цьому випадку кожна із пар «адреса-порт» буде трактуватися як відправник і отримувач водночас.

Опції правил є найважливішою частиною роботи системи підписів. Для розділення опцій у підписах використовується крапка з комою (;). Ключові слова опцій відділяються від аргументів двокрапкою (:).

Існує 4 (чотири) основних категорії опцій підписів:

1. Meta-data – інформація про підпис, що не впливає на детектування пакетів і виконувані по відношенню до них операції.

2. Payload – опція перегляду поля даних пакета (packet payload).

3. Non-payload – опція перегляду службових полів пакета.

4. Post-detection – опція, яка вказує, що необхідно зробити після виконання заданих для підпису умов.

Для забезпечення зручного користування NIDS потрібен user-friendly інтерфейс користувача. Цю вимогу можна забезпечити за допомогою веб-додатку, що є поширеною практикою на сьогоднішній день. Проте спочатку потрібно спроектувати архітектуру такої системи.

Для даного випадку слід використовувати трирівневу «клієнт-серверну» архітектуру. Це архітектурна модель програмного комплексу, що передбачає наявність у ньому трьох компонентів: клієнта, сервера додатків (наша система виявлення) і сервера баз даних (з яким працює сервер додатків).

У порівнянні з дворівневою «клієнт-серверною» архітектурою або «файл-серверною» архітектурою, трирівнева архітектура забезпечує, як правило, більшу масштабованість (за рахунок горизонтальної масштабованості сервера додатків і мультиплексування з'єднань), кращу можливість конфігурування (за рахунок ізольованості рівнів один від одного) [6].

Дана архітектура представлена на рис. 2.

Слід зазначити, що для NIDS важливим є розподілена обробка подій. Для цього в наведеній архітектурі запропоновано використати Веб кластер.

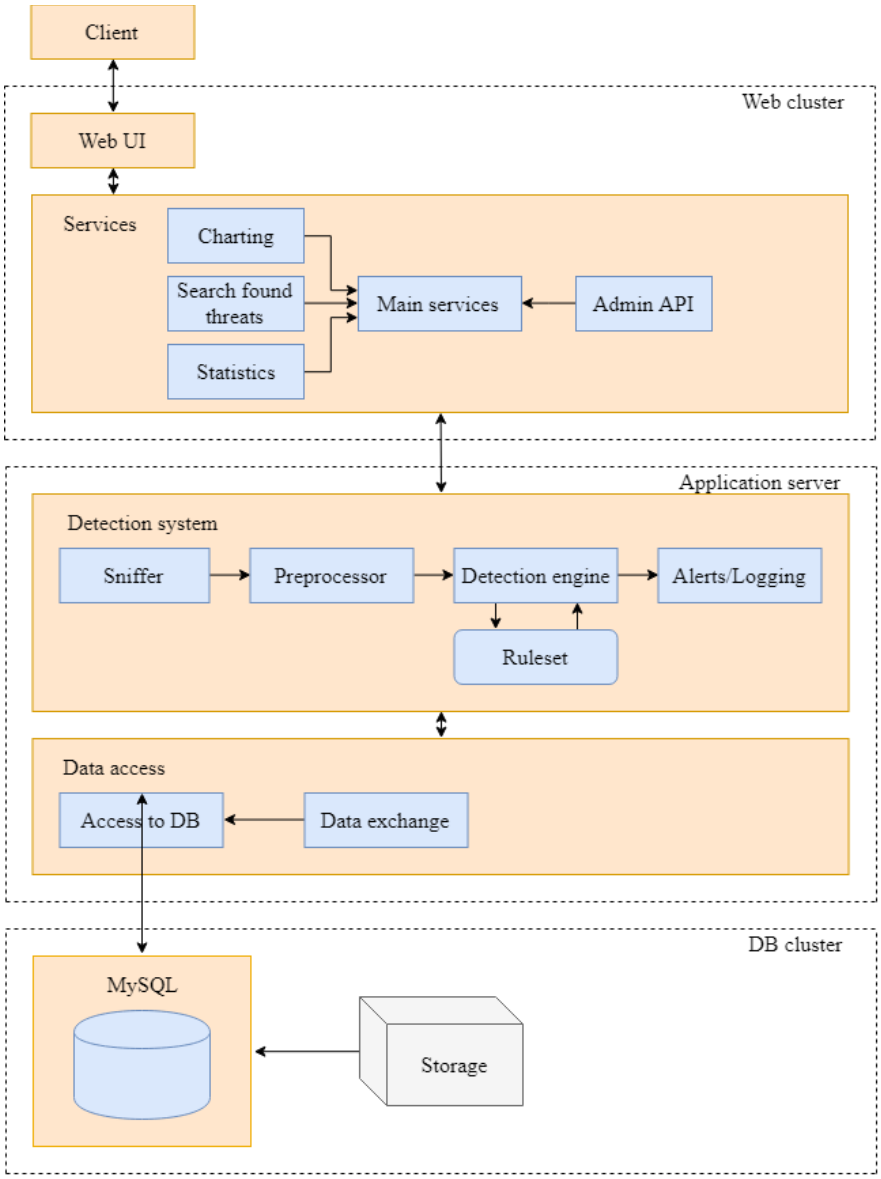

Рисунок 2 – Трирівнева «клієнт-серверна» архітектура мережевої системи виявлення вторгнень

6. Висновки та пропозиції

У роботі проведено аналіз існуючих мережевих систем виявлення вторгнень, який показав необхідність використання user-friendly інтерфейсу користувача та розроблення узагальненої архітектури NIDS з урахуванням використання веб-додатку.

Запропоновано архітектуру мережевої системи виявлення вторгнень на основі трирівневої клінт-серверної моделі. Виділені основні компоненти системи виявлення і описана її робота, що працює на основі підписів.

Як показав аналіз системи, вузьким місцем усієї системи є набір підписів і незручний спосіб взаємодії з користувачем. Одна з найважливіших проблем сучасних систем полягає в тому, що даний набір не може відстежувати загрози, які не мали прецедентів у минулому. Тому основним напрямом досліджень є впровадження пошуку вторгнень на основі пошуку аномальної активності.

Наступна проблема, а саме розробка дружніх інтерфейсів, вирішується впровадженням веб-додатку, який може ефективно взаємодіяти з сервером, на якому розміщені системи виявлення і база даних, що зберігає всю необхідну інформацію.

СПИСОК ДЖЕРЕЛ

1. Dhangar K., Kulhare D., Khan A. A Proposed Intrusion Detection System. *International Journal of Computer Applications*. 2013. Vol. 65, N 23. P. 46–50.
2. Vijayarani S., Sylviaa M. Intrusion Detection System – A Study. *International Journal of Security, Privacy and Trust Management*. 2015. Vol. 4, N 1. P. 31 – 44.
3. Shaker A. Gore S. Intrusion Detection System (IDS): Case Study. *International Conference on Advanced Materials Engineering IPCSIT*. 2011. Vol. 15. P. 6 – 9.
4. Top Free Network-Based Intrusion Detection Systems (IDS) for the Enterprise. URL: https://www.upguard.com/articles/top-free-network-based-intrusion-detection-systems-ids-for-the-enterprise.
5. Open Source Intrusion Detection System using Snort: conf. paper from the 4th International Symposium on Sustainable Development. *International Burch University, Faculty of Engineering and Information Technologies*. Sarajevo: SOC-1441, 2014. 8 p.
6. Риндич Є.В. Сервісно-орієнтована архітектура інформаційних систем у сфері надання транспортних послуг. *Вісник Чернігівського державного технологічного університету*. *Технічні науки*. 2013. № 1. С. 155–160.

Стаття надійшла до редакції 13.06.2018