УДК 004.056

Назарій ФЛЯШКО

Західноукраїнський національний університет

КОНТРОЛЬ КІНЦЕВИХ ТОЧОК З ВИКОРИСТАННЯМ АГЕНТА WAZUH

Вступ. Як відомо шкідливе програмне забезпечення широко розповсюдження в кібер просторі. Тому компанії щоб вберегтися та застерегти себе від дії зловмисного програмного забезпечення використовують різноманітні продукти які виявляють, повідомляють або ж усувають їх без участі користувача. Одним із таких ресурсів є платформа Wazuh. Успішне виконання задач та надійний захист програмних ресурсів та активів дозволила їй завоювати схвалення та прихильність сотні тисяч компаній. Крім цього Wazuh наділений багатьма корисними функціями, включаючи легку інтеграцію із моделями SOC, активне реагування на інциденти та шкідливе програмне забезпечення, постійний моніторинг пристроїв, та їх цілісна оцінка безпеки та пошуку вразливих зон, можливість працювати з великими даними локальних чи хмарних середовищах, ідентифікація прихованих процесів. Головним виконавчим механізмом, що забезпечує комунікацію між платформою та серверними, комп'ютерними і мережевими точками є агент. Агент займається збором, аналізом, моніторингом, виявленням, реагуванням шкідливого програмного забезпечення із централізованим управлінням.

Мета: дослідити виявлення шкідливого програмного забезпечення за допомогою агента, що є центральним компонентом платформи Wazuh, а також вивчити його структуру та технічні особливості.

1. Архітектура агента Wazuh

Агент є центральним елементом в структурі Wazuh машини, адже в нього вбудовано багато модулів, без яких дана система не працювала б. Робоча область агента поширена на вузлових точках серверного, користувальницького та мережевого середовища. У процесі встановлення завантажується програмне забезпечення агента, після чого налаштовуються його процеси під певний тип задач, які він має проробити.

За своєю архітектурою агент має модульну будову. Вузька направленість кожного елементу дозволяє ефективно вирішувати певні задачі, тобто кожний метод розробляється під конкретні завдання. Таким чином агент здатний відстежувати дані файлової системи, зчитувати повідомлення із журналів, збирати об'єктивну інформацію про наявність шкідливого програного забезпечення.

На рисунку 1 наведено архітектуру агента Wazuh із його основними модулями.

Модуль збору журналів використовується для зчитування файдів журналів та події що відбуваються в операційних системах. Конфігураційний файл потрібний для зручного редагування системного коду агента, пристосовуючи його під власні потреби.

Комунікаційний модуль сполучає агент із менеджером Wazuh, де отримані

результати роботи агента направляються на сервер Wazuh для подальшого аналізу.

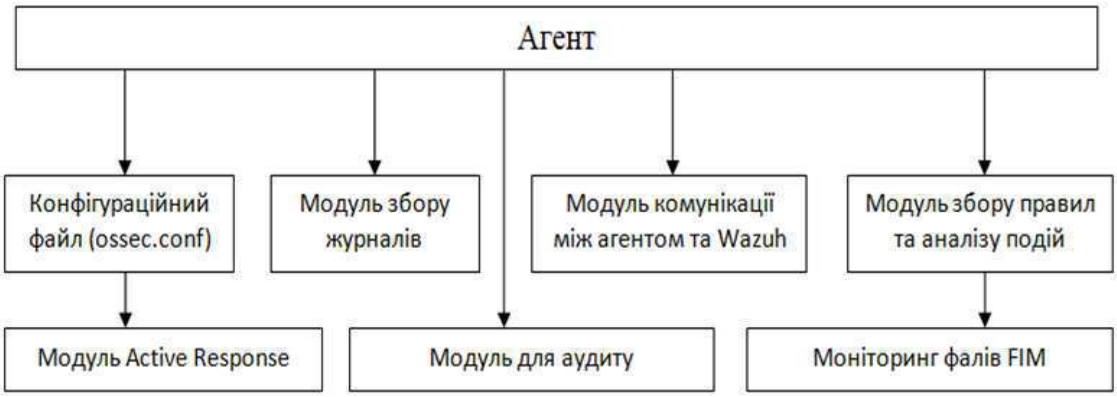

Рисунок 1- Архітектурна схема агента Wazuh

Моніторинг файлової систем більш відомий як FIM розроблений для введення спостереження за файловою системою, що дозволяє в режимі реального часу активно відслідковувати будь які зміни у файлах, а також перевіряти їх попередня стани для віддалених запитів.

Модуль збору правил та аналізу подій займається скануванням та збором даних, включаючи версії операційної системи, інформацію про мережу, відомості про запущені процеси, завантажені програми, а також санують порти що перебувають в активному режимі.

Модуль аудиту використовується для забезпечення цілісного аналізу досліджуваного об'єкту, а саме операційної системи, тобто розробляються усі можливі рішення для виявлення та захисту операційних систем від впливу шкідливого продукту.

Активне реагування розроблене для автоматичного виявлення загроз, що були помічені, блокуючи мережевий трафік, та інші процеси, видаляючи шкідливі файли [2].

Після успішного розгортання інтерфейсу користувача наступним кроком буде відвідування офіційного сайту розробників. Тут ви знайдете детальні інструкції щодо встановлення моделей агентів для певного типу операційної системи. У нашому випадку ми будемо встановлювати програмне забезпечення агента на операційну систему Kali Linux. Існує два способи встановлення агента. Перший спосіб передбачає використання набору команд у терміналі, як зазначено в документації. Другий спосіб передбачає безпосереднє введення інформації про агента та пристрій [1]. Розглянемо обидва способи докладніше.

Якщо ми вирішили налаштувати його через консоль, то після встановлення відкриється інтерфейс агента. Потім нам потрібно призначити агенту IP-адресу менеджера Wazuh (ту саму адресу, що використовується для запуску програмного забезпечення) і ввести ключ для входу.

Крім того, якщо ми вирішимо заповнити форму, доступну за посиланням Додати агента, нам потрібно надати інформацію про агента, як показано на рисунку 2.

Після заповнення форми буде згенеровано команду [1]. Цю команду потрібно виконати в командному рядку, щоб запустити агента з усіма його функціональними можливостями.

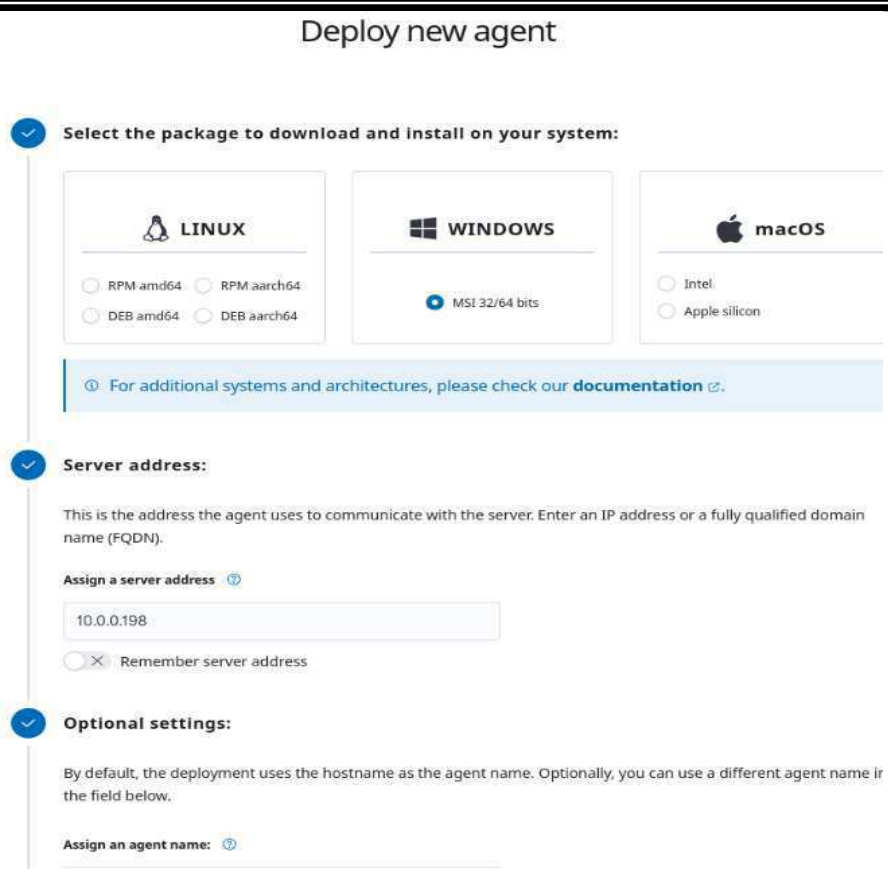

Рисунок 2 - Ручне заповнення форми агента

Тоді коли ми внесли усі необхідні відомості у форму агента, в інтерфейсі користувача з'явиться вкладка активно запущеного агента. Корисним є те що за потреби ми можемо в любий час налаштовувати його параметри, та переглядати інформацію, яку йому вдалося зібрати із системного середовища до якого він прив'язаний за IP адресом.

Як ми бачимо на малюнку показано конфігурацію агента з його важливими даними. Тоді коли ми внесли усі необхідні відомості у форму агента, в інтерфейсі користувача з'явиться вкладка активно запущеного агента. Корисним є те що за потреби ми можемо в любий час налаштовувати його параметри, та переглядати інформацію, яку йому вдалося зібрати із середовища до якого він прив'язаний за IP адресом.

В цю панель можливо підключити велику кількість агентів, а отже користувач зможе активно прив'язуватись до операційних систем та досліджувати їхню поведінку. Від агентів користувач отримує повну звітність активних подій, які виконувались системою вході яких користувач формуватиме висновки щодо посилення безпеки.

Щоб прив'язати агента Wazuh до каталогу Linux, ми повинні спочатку встановити та налаштувати агента Wazuh на основну операційну систему. Після цього необхідно виконати наведені нижче кроки, для того щоб прив'язати агента до конкретного файлу в каталозі Linux:

1. Відкрити оболонку термінал в системі Linux.
2. Перейти до відповідного каталогу, в якому встановлено агент Wazuh.
3. Виконайте команду прив'язки агента до цього каталогу, вказавши необхідні параметри, такі як ім'я сервера або IP-адреса сервера керування Wazuh.

Встановивши зв'язок між агентом і кожним елементом каталогу, користувач зможе отримати вичерпну інформацію про кожен файл у каталозі та визначити всі наявні в ньому вразливості. Дані будуть зібрані та належним чином надіслані на сервер Wazuh.

Для того, щоб проілюструвати поведінку сервера Wazuh у випадку атаки зловмисників, необхідно написати в терміналі наступну функцію: У терміналі слід ввести наступну команду [3]:

python3 wazuh-ransomware-poc.py attack.

Після виконання цієї команди почнеться процес дублювання файлів, в результаті якого існуючі файли будуть видалені, а нові зашифровані [3].

Згодом на інформаційній панелі Wazuh з'явиться повідомлення про виявлення подій, що відбулися під час моделювання цієї атаки. В інтерфейсі користувача показаного на рисунок 3 ми спостерігатимемо за моніторингом файлової системи, який відображатиме зображення перезапису файлів і бачитимемо деякі відмінності із попереднім рисунком, які виділені кольором що сигналізують про додавання "added" та видалення "deleted" оригінальних файлів [3].

full_log	rule.description	syscheck.event
File '/home/vagrant/test/Directory_09/File_18.txt.encrypted' was added.	File added to the system.	added
File '/home/vagrant/test/Directory_09/File_19.txt' was deleted.	File deleted.	deleted
File '/home/vagrant/test/Directory_09/File_17.txt' was deleted.	File deleted.	deleted
File '/home/vagrant/test/Directory_09/File_17.txt.encrypted' was added.	File added to the system.	added
File '/home/vagrant/test/Directory_09/File_16.txt.encrypted' was added.	File added to the system.	added
File '/home/vagrant/test/Directory_09/File_15.txt' was deleted.	File deleted.	deleted
File '/home/vagrant/test/Directory_09/File_14.txt.encrypted' was added.	File added to the system.	added
File '/home/vagrant/test/Directory_09/File_11.txt' was deleted.	File deleted.	deleted
File '/home/vagrant/test/Directory_09/File_11.txt.encrypted' was added.	File added to the system.	added
File '/home/vagrant/test/Directory_09/File_08.txt' was deleted.	File deleted.	deleted
File '/home/vagrant/test/Directory_09/File_07.txt.encrypted' was added.	File added to the system.	added
File '/home/vagrant/test/Directory_09/File_08.txt.encrypted' was added.	File added to the system.	added

Рисунок 3 - Моніторинг файлової системи після атаки програм-вимагачів

Висновок. Проведені дослідження алгоритмів виявлення шкідливого програмного забезпечення показали ефективність агента на платформі Wazuh. Було досліджено архітектуру агента, налаштовано його конфігурацію, а також показано його роботу на ділі.

Перелік використаних джерел.

1. Instalation Wazuh agent [Електронний ресурс]. - Режим доступу: https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html

2. Active response [Електронний ресурс]. - Режим доступу: https://documentation.wazuh.com/current/user-manual/capabilities/active-response/index.html

3. Preventing and detecting ransomware with Wazuh [Електронний ресурс] // Jesus Linares. - 2019. - Режим доступу до ресурсу: https://wazuh.com/blog/preventing-and-detecting-ransomware-with-wazuh/.