**УДК 004**

**ГРНТИ 81.93.29**

**А.А. Громов (студент группы ИКТЗ-83, СПБГУТ)**

# ОБНАРУЖЕНИЕ КОМПЬЮТЕРНЫХ АТАК ПРИ ПОМОЩИ ELK-SIEM

*Работа посвящена изучению способов обнаружения компьютерных атак. Актуальность работы обоснована ростом количества атак на сетевую/серверную инфраструктуру. Столь бурный рост связан с упрощением эксплуатации уязвимостей. В рамках данной работы будет рассмотрено решение от компании Elastic. Главный фактор, по которому было выбрано данное решение - бесплатность. В рамках данной работы был разработан docker-compose файл, который позволяет быстро разворачивать рабочую инфраструктуру,а также были созданы собственные правила корреляции для обнаружения атак*

*Elastic, Kibana, Beats, компьютерные атаки, безопасность, SIEM*

В настоящее время все больше компаний используют цифровые технологии для эффективного функционирования, например, прием и обработка заказов или отслеживание загруженности складских помещений или логистических цепочек. Такие данные являются целью злоумышленников, в связи с этим количество компьютерных атак возрастает.

Атаки бывают разных типов, например, с целью парализовать бизнес конкурента, тем самым переманивая к себе его клиентов; с целью украсть конфиденциальные данные клиентов компании, для дальнешей перепродажи на черном рынеке; или с целью требования выкупа за неразглашение украденной информации. Так же компания, подвергшаяся нападению, несет репутационные потери.

Одна из мер уменьшения потерь при потенциальном взломе - своевременное обнаружение злоумышленников и остановки атаки на ранних этапах. Для этих целей есть множество средств, одно из них - Security information and event management (SIEM), оно и будет рассмотрено в данной работе.

Основными задачами SIEM систем являются сбор и объединение событий из множества источников, аналитика и оповещение сотрудников Security Operations Center (SOC) об инцидентах информационной безопасности.

Есть несколько готовых решений от вендоров, представленных следующими компаниями: HP, RT Solar, PT, IBM, McAfee, КОМРАД. В зависимости от размеров компании, SIEM-системы могут стоить десятки миллионов рублей. По этой причине не каждая компания может себе позволить столь большие траты. Однако есть и бесплатные варианты на основе которых можно построить SIEM-систему.

В данной работе будет рассмотрено решение от компании Elastic. Для хранения событий используется Elasticsearch. Это современная поисковая и аналитическая система, основанная на Apache Lucene, совмещенная с NoSQL базой данных. Для представления и визуализации этих событий использует ся Kibana. События, которые хранит Elasticsearch, приходят от различных утилит для клиентских ПК. В статье будут рассмотрены следующие программы: Filebeat, Winlogbeat, Packetbeat.

Beats - это программы, которые запускаются на клиентских устройствах, после чего отправляют соответствующие данные на сервер.

Изначально данный набор приложений позволяет лишь собирать логи/события, просматривать их в текстовом формате или визуализировать их с помощью диаграмм. Однако добавив проверку приходящих данных по определенным правилам, появляется возможность обнаруживать неправомерные действия на устройствах сотрудников или серверах компании. Таким образом мы получаем SIEM систему из бесплатных компонентов[1].

Развертывание SIEM-системы на основе Elastic и Kibana (EK) может происходить как на сервере под управлением ОС Linux, так и в Docker контейнерах. Далее будет рассмотрен второй вариант.

В ходе данной работы были созданы конфигурационные файлы Elasticsearch и Kibana, а также docker-compose файл с помощью которого можно одной командой развернуть SIEM-систему на любой инфраструктуре. При этом все необходимые параметры для совместной работы Elasticsearch и Kibana будут заданы.

Также на сервере под управлением операционной системы Centos была установлена утилита FileBeat для отслеживания изменения в файлах(логах). На клиентском ПК с ОС Windows установлены Winlogbeat, Packetbeat. Winlogbeat - собирает события, записанные системой Windows, Packetbeat - отправляет данные о сетевой активности устройства. Также созданы конфигурационные файлы для этих программ. В них указаны необходимые параметры для работы с Elasticsearch[1], а также другие детали, для более точной настройки их работы. Пример инфраструктуры представлен на Рисунке 1.

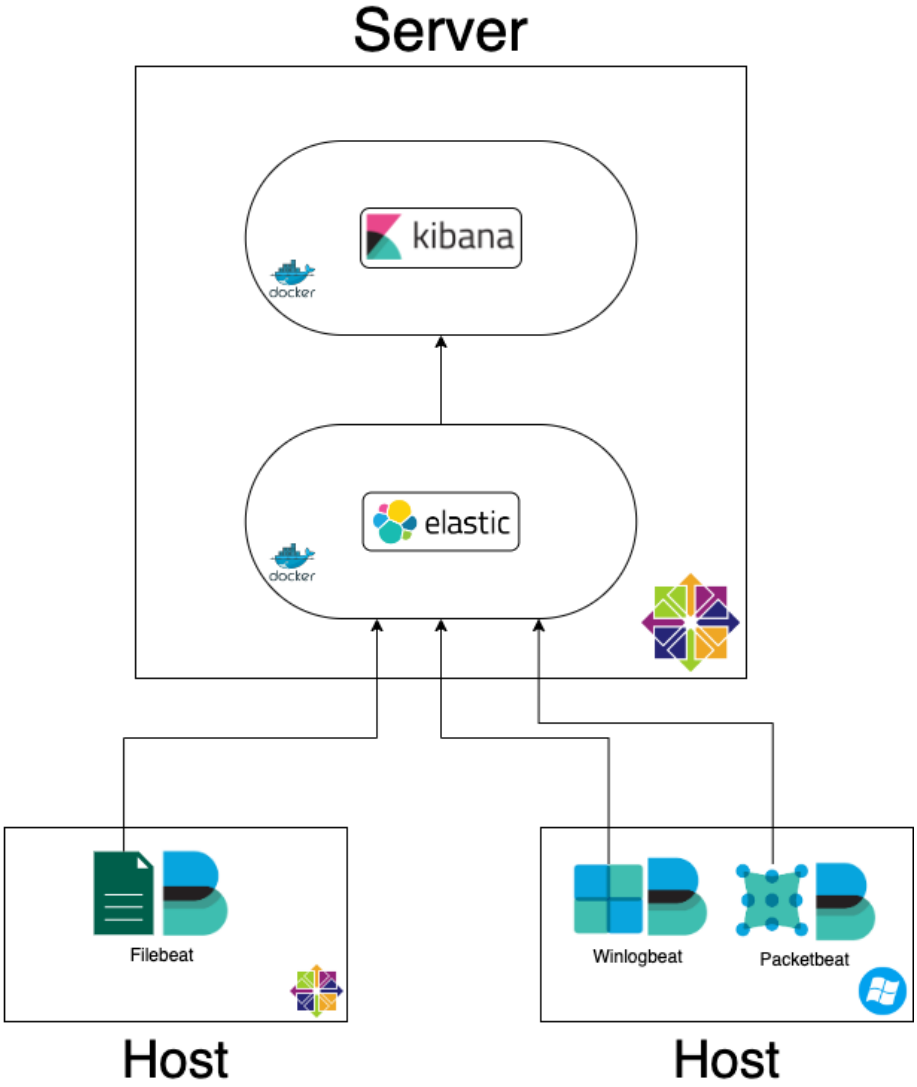


Рис. 1. Схема инфраструктуры

Для демонстрации возможностей данной системы было выбрано 2 популярных типа атак: bruteforce - грубый подбор пары логин - пароль, например, для доступа по протоколу Remote Desktop Protocol (RDP)[2] или Windows Remote Management (WinRM)[3], и атаку использующую уязвимость Eternal Blue[4].

Атаки проводятся с помощью специализированной ОС для тестирований на проникновение - Kali Linux, с использованием скриптов на языке программировании Python, и таких утилит, как Crowbar и Metasploit Framework[5]. Все атаки будут происходить на ПК под управлением Windows 7.

Любые действия, направленные на взлом инфраструктуры, оставляют следы. Благодаря этому, у сотрудников отдела информационной безопасности появляется возможность обнаруживать атаки и пресекать их до утечки конфиденциальной информации.

Первостепенно будем пытаться подобрать пароль к учетной записи пользователя для подключения по RDP. Отследить такие действия не составляет труда, это связано с тем, что при подборе пароля появляется множество событий с Windows event ID 4625, которые в операционной системе означают ложную авторизацию.

Таким образом для выявления успешной атаки подбора пароля для RDP мы будем отслеживать следующую цепочку событий:

1. Большое количество событий с event ID 4625,
2. Одно событие с event ID 4624, которое означает успешный вход в систему
3. Событие с event ID 1149 - подключение по протоколу RDP.

Добавляя условие множественной ложной авторизации удается минимизировать количество ложных срабатываний, например, когда пользователь случайно ввел неверный пароль несколько раз.

При попытке подбора пароля для входа по WinRM в событии event ID 4625 указывается имя процесса - svchost.exe. Таким образом мы можем создать фильтр, в котором ищем события с event ID 4625, но при этом чтобы в записи присутствовал процесс svchost.exe. Далее задаем планку срабатывания правила, например, если неудачных попыток входа было больше 100 шт.

Эксплуатацию уязвимости Eternal Blue обнаружить сложнее, однако при использовании данной уязвимости создается одно событие с event ID 4625 (неуспешная попытка авторизации), которое передается на сервер с помощью Winlogbeat. Далее с помощью утилиты Packetbeat мы можем отследить подключение по 445 порту, который является портом samba протокола. Таким образом собирая события из разных источников удается выявить атаку.

На рисунке ниже представлены алерты, по сработавшим правилам:

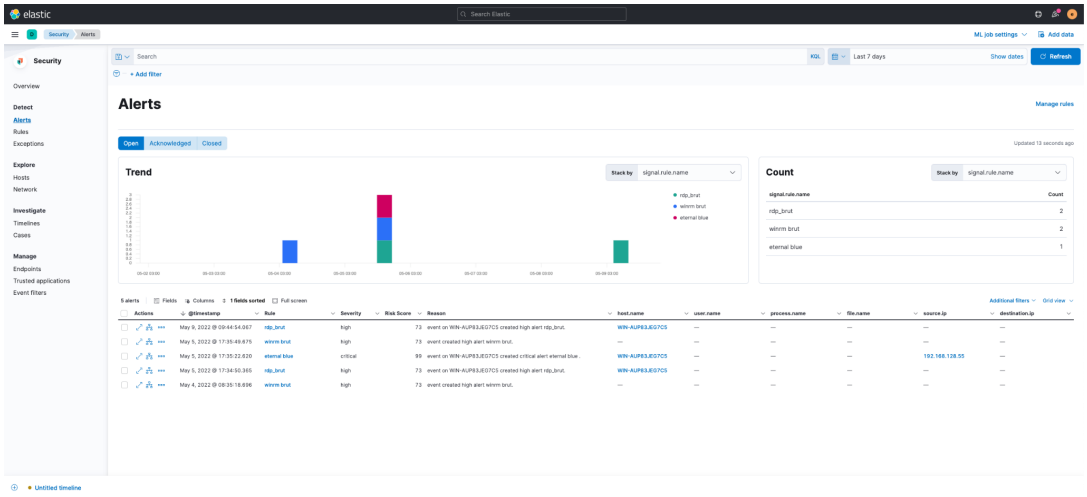


Рисунок 2 - Пример работы правил EK SIEM

В дальнейшем автор данной работы планирует создать комплекс лабораторных работ, в которых студенты научатся запускать Elastic и Kibana с помощью Docker-compose. Также учащиеся ознакомятся с интерфейсом Kibana, после чего настроят клиентский устройства и активируют EK SIEM. Изучив типы атак, описанных в данной статье, студенты попробуют написать правила для их обнаружения. Заключительной лабораторной работой в данном комплексе будет проведение вышеописанных атак для проверки работы правил.

**Список используемых источников**

1. Документация Elastic для Elasticsearch и Kibana. 2022. URL: https://www.elastic.co/guide/index.html (дата обращения 29.04.2022)

2. Объяснение bruteforce на протокол RDP. 2021. URL: https://medium.com/@idan_malihi/remote-desktop-rdp-brute-force-attack-f5484d8cf6a3 (дата обращения 04.05.2022).

3. Инструкция по активации WinRM. 2022. URL: https://winitpro.ru/index.php/2012/01/31/kak-aktivirovat-windows-remote-management-s-pomoshhyu-gruppovoj-politiki/ (дата обращения 08.05.2022)

4.Описание уязвимости Eternal Blue. 2019. URL: https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/ (дата обращения 03.05.2022)

5.Объяснение эксплуатации уязвимости Eternal Blue. 2019. URL: https://null-byte.wonderhowto.com/how-to/exploit-eternalblue-windows-server-with-metasploit-0195413/ (дата обращения 08.05.2022)

Статья представлена научным руководителем, ассистент кафедры ЗСС Скорых М.А., СПБГУТ