ООО «КОНТРОЛХАК»
127299, г. Москва, ул. Космонавта Волкова, д.20
+7 (495) 789-7297, info@ctrlhack.ru

www.ctrlhack.ru

«CTRLHACK Base Platform»

Описание функциональных характеристик

Москва, 2021

Оглавление

Аннотация

Настоящий документ является общим описанием системы CTRLHACK Base Platform.
В документе описаны назначение системы, цели ее использования, приведен перечень реализуемых системой функций и требования к программным и аппаратным ресурсам, а также персоналу.

Контактная информация:
ООО «КонтролХак»
Юридический/фактический адрес:
143001, Московская область, г. Одинцово, ул. Чистяковой, д. 6, кв. 63
ОГРН: 1205000049627
ИНН/КПП: 5032318839/503201001
Веб-сайт: https://www.ctrlhack.ru/
Телефон: +7 495 789-72-97
Адрес электронной почты: info@ctrlhack.ru

Перечень терминов, сокращений и обозначений

В документе используются следующие термины, сокращения и обозначения:

Термин/Сокращение/Обозначение	**Определение**
Веб-браузер	Прикладное программное обеспечение для просмотра страниц, содержания веб-документов, компьютерных файлов и их каталогов, управления веб-приложениями.
ГГц	Гигагерц (англ. gigahertz)
ОС	Операционная система
ПО	Программное обеспечение
ЦП	Центральный процессор
API	API (англ. Application Programming Interface — программный интерфейс приложения). Набор методов, с использованием которых, различные программы взаимодействуют друг с другом и передают команды управления и данные.
HTTP	HTTP (англ. HyperText Transfer Protocol) — протокол прикладного уровня передачи данных
HTTPS	HTTPS (англ. HyperText Transfer Protocol Secure) — расширение протокола HTTP для поддержки шифрования в целях повышения безопасности.
SOC	SOC (англ. Security Operation Center) – центр мониторинга и управления информационной безопасностью.

1. Описание системы

1.1. Назначение системы

Система CTRLHACK Base Platform предназначена для проведения симуляций кибератакующих техник хакеров. Использование системы позволяет повысить эффективность выявления кибератак в инфраструктуре организации.

1.2. Вид деятельности, для которой предназначена система

Система предназначена для использования сотрудниками служб информационной безопасности компаний. CTRLHACK Base Platform может использоваться для:

- Оценки качества детектирования атакующих техник.
- Повышения эффективности детектирования кибератакующих техник в SOC.
- Оценки процессов реагирования на инциденты в SOC.
- Оценки работы персонала SOC.
- Проведения киберучений непосредственно в инфраструктуре организации.

1.3. Перечень функций, реализуемых системой

Система CTRLHACK Base Platform позволяет выполнять симуляции различных действий, аналогичных действиям хакеров в реальных кибератаках.

Функции системы разделены на два функциональных модуля:

1. Модуль проверки «Первичный доступ».
2. Модуль проверки «Пост-эксплуатация».

В каждом из модулей включены функции проведения проверок на соответствующих этапах проведения кибератак.

1.3.1. Модуль «Первичный доступ»

В данном модуле представлены функции, обеспечивающие выполнение симуляций действий атакующих на этапе первичного проникновения в инфраструктуру.

Функции указанного модуля позволяют:

- Выполнить попытки соединения с адресами из «черных списков» (адреса командных серверов атакующих, адреса, распространяющие вредоносный контент и т.д.).
- Выполнять попытки скачивания вредоносных файлов с URL.
- Выполнять попытки передачи и получения электронных писем, с вредоносными файлами во вложениях.
- Выполнять попытки сохранения вредоносных файлов в папках файловой системы на рабочих станциях.

В рамках выполнения указанных функций проводится проверка процессов реагирования на актуальные экземпляры вредоносного ПО и попытки соединения с адресами из «черных списков».

Для обновления базы данных актуальными вредоносными файлами и адресами, CTRLHACK Base Platform имеет возможность подключения к ресурсам Threat Intelligence с использованием специализированных API.

Для запуска определенной функции данного модуля пользователь должен создать новое задание. В пошаговом конструкторе нового задания пользователь:

- выбирает набор вредоносных файлов или адресов для выполнения проверки;
- выбирает узлы (с установленными агентами CtrlHack), на которых будет выполняться проверка;
- устанавливает время запуска (или расписание запуска) и время реагирования на выполненные действия.

После этого задание начинает выполняться в соответствии с заданными параметрами.

После выполнения задания пользователь может посмотреть обобщённый результат выполнения задания (в виде цветового сигнала), а также при необходимости открыть детальный отчет с результатами выполненного задания.

Каждое из выполненных заданий можно перезапустить в теми же параметрами в любой время. Для этого нужно нажать соответствующую кнопку в строке задания.

1.3.2. Модуль «Пост-эксплуатация»

В данном модуле представлены функции, обеспечивающие симуляций атакующих техник на разных стадиях выполнения атаки хакером. Действия симулируются для того, чтобы:

- определить какие из атакующих техник не детектируются на разных уровнях системы защиты;
- проверить процесс формирования инцидентов в SOC;
- определить какие из необходимых событий не поступают в SIEM с конечных точек.

На базе полученной информации о проведенных симуляциях возможно разрабатывать новые правила детектирования для SIEM.

Проверки в данном модуле сгруппированы по стадиям выполнения атаки:

- запуск;
- закрепление;
- повышение привилегий;
- обход защиты;
- учетные данные;
- сбор информации;
- перемещение в сети;
- вывод данных;

- урон.

Для запуска определенной функции данного модуля пользователь должен создать новое задание. В пошаговом конструкторе нового задания пользователь:

1. выбирает набор техник определенной стадии атаки для выполнения проверки. Для каждой техники пользователь может посмотреть детальное описание выбранной техники;
2. выбирает узлы (с установленными агентами CtrlHack), на которых будет выполняться проверка;
3. устанавливает время запуска (или расписание запуска) и время реагирования на выполненные действия.

После этого задание начинает выполняться в соответствии с заданными параметрами.

После выполнения задания пользователь может посмотреть обобщённый результат выполнения задания (в виде цветового сигнала), а также при необходимости открыть детальный отчет с результатами выполненного задания.

Каждое из выполненных заданий можно перезапустить в теми же параметрами в любой время. Для этого нужно нажать соответствующую кнопку в строке задания.

2. Условия выполнения программы

2.1. Требования к техническим средствам

Для установки и функционирования сервера управления CtrlHack необходим виртуальный или физический сервер с характеристиками не ниже:

- ЦП: 4 ядра, 2 ГГц.
- Оперативная память: 8Gb.
- Жесткий диск: 50Gb.

Агенты CtrlHack могут устанавливаться и функционировать на рабочих станциях и серверах с характеристиками не ниже:

- ЦП: 1 ядро 2 ГГц.
- Оперативная память: 2Gb.
- Жесткий диск: 20Gb.

2.2. Требования к программным средствам

Сервер управления CtrlHack функционирует на серверах под управлением ОС Ubuntu 18.04.

Агенты CtrlHack могут устанавливаться и функционировать на рабочих станциях и серверах под управлением ОС:

- Microsoft Windows 7 и выше.
- Microsoft Windows 2012 и выше.
- Linux (CentOS, RedHat, Ubuntu, Debian).
- MacOS.

2.3. Требования к сетевому доступу

В таблице представлена матрица сетевого доступа Вариант 1 «Сервер управления CtrlHack в инфраструктуре Компании»:

№	Источник	Назначение	Протокол\Порт
1	Компьютер пользователя CtrlHack	Сервер управления CtrlHack	tcp\443
3	Сервер управления CtrlHack	Глобальная сеть «Интернет»	tcp\443
4	Рабочая станция или сервер с установленным агентом CtrlHack	Сервер управления CtrlHack	tcp\443

3. Требования к персоналу

К эксплуатации CTRLHACK Base Platform допускаются лица, ознакомившиеся с эксплуатационной документацией на ПО «CTRLHACK Base Platform», эксплуатационной документацией на аппаратное обеспечение, которое используется совместно с CTRLHACK Base Platform, и имеющие практические навыки работы с указанным программным и аппаратным обеспечением.

Для эксплуатации CTRLHACK Base Platform может привлекаться штатный персонал Заказчика либо организаций-подрядчиков, предоставляющих услуги по обслуживанию ПО на договорной основе. Рекомендуется, чтобы было обеспечено периодическое обучение персонала на учебных курсах, авторизованных производителем.

Администратор CTRLHACK Base Platform должен иметь навыки:

- Администрирования ОС семейства Linux;
- Администрирования систем контейнеризации Docker Container.