

Программный  
«SimuStrike»

комплекс

## Аннотация

Настоящий документ содержит описание функциональных характеристик программного комплекса по защите системно-технической инфраструктуры «SimuStrike» (далее – ПК «SimuStrike», комплекс).

## Содержание

|     |   |    |
|-----|---|----|
| 1   | Общие сведения .....  | 4  |
| 1.1 | Назначение ПК «SimuStrike» .....  | 4  |
| 1.2 | Задачи ПК .....   | 4  |
| 2   | Функциональные характеристики .....                                     | 6  |
| 2.1 | Функциональные возможности ПК .....                                     | 6  |
| 2.2 | Программная структура комплекса .....                                   | 14 |
| 2.3 | Входные и выходные ресурсы функциональных модулей ПК «SimuStrike» ..... | 14 |
| 2.4 | Свойства ПК «SimuStrike» .....  | 15 |
| 3   | Масштабирование .....   | 16 |
|     | Перечень сокращений .....   | 17 |

# 1 Общие сведения

## 1.1 Назначение ПК «SimuStrike»

ПК предназначен для использования в составе программно-технических средств (ПТС) защиты информации, подсистем обеспечения информационной безопасности, а также как отдельное средство для автоматизации тестирования существующих процессов с целью выявления уязвимостей в ИТ-инфраструктуре организации. Решение обеспечивает последовательную и непрерывную проверку защищенности, имитируя различные варианты атак и позволяет осуществлять наблюдение за реагированием ИТ-инфраструктуры организации на угрозы.

ПК расширяет классическое представление о системах симуляции атак, предоставляя не только инструменты для оценки уязвимости инфраструктуры, но также и систему сбора обратной связи от средств защиты, обеспечивая непрерывную информационную поддержку для инженеров ИБ и операторов «Центров Мониторинга».

ПК «SimuStrike» служит для:

- специалистов по информационной безопасности. Использование ПК для регулярного тестирования устойчивости информационной инфраструктуры и проверки наличия уязвимостей;
- специалистов центра мониторинга и реагирования на киберугрозы, которые занимаются обеспечением кибербезопасности. Использование ПК для проверки того, что центр действительно видит все атаки на инфраструктуру, а также для оценки реакции установленных продуктов информационной безопасности на угрозы;
- групп инженеров на исследование на проникновение. Использование ПК для автоматизации проверки инфраструктуры, что позволяет повысить эффективность тестирования.

## 1.2 Задачи ПК

ПК «SimuStrike» расширяет классическое представление о системах симуляции атак, предлагая инструменты для оценки уязвимости инфраструктуры и систему сбора обратной связи от систем защиты, что обеспечивает непрерывную поддержку для инженеров ИБ и операторов SOC.

ПК решает следующие задачи в области информационной безопасности (ИБ):

- 1) Оценка уязвимостей. Программный комплекс помогает IT-специалистам и администраторам выявлять уязвимости и слабые места в сетевой инфраструктуре, что позволяет своевременно принимать меры по их устранению.
- 2) Проведение атак. Программный комплекс предоставляет обширный набор инструментов для симуляции различных типов атак, что позволяет пользователям оценивать уровень безопасности своей системы.

- 3) Анализ эффективности. Программный комплекс позволяет анализировать эффективность проведенных атак в реальном времени, что помогает в выявлении недостатков в защите и в планировании дальнейших действий.
- 4) Тестирование защитных мер. Программный комплекс дает возможность эффективно тестировать существующие защитные меры и планы реагирования на кибератаки, обеспечивая уверенность в их работоспособности и эффективности.
- 5) Улучшение реагирования на инциденты. Программный комплекс способствует улучшению процессов реагирования на кибератаки, позволяя организациям адаптировать свои стратегии безопасности на основе полученных данных и результатов тестирования.

Эти задачи помогают организациям повысить уровень безопасности своей сетевой инфраструктуры и подготовленность к потенциальным киберугрозам.

## 2 Функциональные характеристики

### 2.1 Функциональные возможности ПК

ПК реализует следующие функциональные возможности:

- сбор данных об информационных ресурсах сетевой ИТ-инфраструктуры организации;
- выявление информации о возможных уязвимостях и векторах возможных атак;
- проверка срабатывания средств защиты информации (СрЗИ) ИТ-инфраструктуры организации на генерируемые инциденты;
- проверка времени отклика СрЗИ объекта оценки на генерируемые инциденты;
- формирование отчетов и рекомендаций по результатам выполненных проверок.

Программная структура комплекса включает программные модули, представленные в таблице 1.

Таблица 1 – Описание модулей и их функциональных возможностей

| Название       | Описание  | Функциональные возможности  |
|----------------|---|---|
| Модуль Фишинга | Метод, заключающийся в рассылке фишинговых писем целевым группам пользователей. Цель — фиксация реакции пользователей и анализ результатов фишинговых кампаний. Данный подход позволяет получить первоначальный доступ к инфраструктуре или завладеть учётными данными. Модуль включает функции создания целевых страниц, имитирующих легитимные веб-ресурсы. | <ul style="list-style-type: none"> <li>• Создание и настройка фишинговых кампаний.</li> <li>• Просмотр и редактирование параметров заданий.</li> <li>• Управление статусом заданий.</li> <li>• Организация повторной отправки недоставленных писем.</li> <li>• Запуск атак в ручном и автоматическом режимах.</li> <li>• Настройка IMAP-профиля для мониторинга ответов.</li> <li>• Конфигурация SMTP-профиля для ретрансляции.</li> <li>• Визуализация результатов кампаний на дашборде.</li> <li>• Анализ эффективности по метрикам: доставка, открытия, переходы, ввод данных.</li> <li>• Мониторинг выполнения</li> </ul> |

| Название                 | Описание  | Функциональные возможности   |
|--------------------------|---|--|
|                          |   | заданий в реальном времени.  |
| Модуль сканирования сети | Модуль для обеспечения безопасности информационной инфраструктуры предприятия. Позволяет выявлять уязвимости во внутрисетевой инфраструктуре, сетевых устройствах, рабочих станциях и серверах.   | <ul style="list-style-type: none"> <li>• Создание заданий для сканирования сетевой инфраструктуры.</li> <li>• Просмотр и редактирование параметров заданий.</li> <li>• Управление статусом заданий.</li> <li>• Запуск и остановка процессов сканирования.</li> <li>• Выявление уязвимостей в сетевой инфраструктуре.</li> <li>• Обследование устройств, рабочих станций и серверов.</li> <li>• Анализ защищенности внутренней сетевой среды.</li> <li>• Формирование и экспорт результатов сканирования.</li> <li>• Обеспечение безопасности через регулярное обследование.</li> </ul> |
| Модуль веб-сканирования  | Процесс поиска уязвимостей веб-серверов, сервисов и приложений. Необходим для выявления уязвимостей для последующей эксплуатации, а также сбора информации (например, email-адресов для фишинга). | <ul style="list-style-type: none"> <li>• Поиск уязвимостей веб-серверов, сервисов и приложений.</li> <li>• Создание и настройка заданий для сканирования веб-ресурсов.</li> <li>• Клонирование и редактирование существующих заданий.</li> <li>• Управление жизненным циклом заданий.</li> <li>• Поиск и фильтрация созданных заданий.</li> <li>• Выявление уязвимостей для эксплуатации.</li> <li>• Сбор дополнительной информации (например, email-адресов).</li> </ul>  |

| Название                           | Описание   | Функциональные возможности   |
|------------------------------------|--|--|
| Модуль сканирования инфраструктуры | Инструмент для комплексной проверки безопасности Active Directory (AD). Выполняет аудит конфигураций, обнаружение хостов и учетных данных, поиск хеш-сумм и паролей, а также выявление уязвимостей в доменной среде. | <ul style="list-style-type: none"> <li>• Формирование отчетов и выгрузка результатов.</li> <li>• Проверка безопасности AD.</li> <li>• Выявление ошибочных конфигураций (misconfigurations).</li> <li>• Поиск и анализ учетных данных пользователей.</li> <li>• Обнаружение хостов домена.</li> <li>• Сбор хеш-сумм и паролей.</li> <li>• Поиск уязвимостей в инфраструктуре AD.</li> <li>• Комплексный анализ защищенности AD.</li> <li>• Идентификация слабых мест в настройках доменной среды.</li> <li>• Обнаружение потенциальных векторов атаки.</li> </ul> |
| Модуль первоначального доступа     | Процесс запуска скрипта, использующего уязвимость ПО без внедрения вредоносной нагрузки. Позволяет исследовать уязвимость без нанесения вреда и подтвердить её наличие для дальнейшего тестирования безопасности.    | <ul style="list-style-type: none"> <li>• Эксплуатация уязвимостей ПО без внедрения вредоносной нагрузки.</li> <li>• Подтверждение наличия уязвимостей.</li> <li>• Автоматический подбор эксплойтов на основе данных о версиях ПО.</li> <li>• Поддержка сценариев внутреннего и внешнего нарушителя.</li> <li>• Создание заданий с настройкой списков хостов и режима работы.</li> <li>• Управление уведомлениями о возможности запуска.</li> <li>• Запуск и остановка заданий.</li> <li>• Разграничение прав</li> </ul>  |

| Название                    | Описание   | Функциональные возможности   |
|-----------------------------|--|--|
|                             |  | доступа.<br>• Автоматическое построение и выгрузка отчётов.<br>• Визуализация результатов эксплуатации.  |
| Модуль перемещения в сети   | Процесс поиска уязвимостей внутри инфраструктуры с использованием ранее заражённого хоста для дальнейшего перемещения и установки агента на другие хосты в сети. Позволяет оценить максимальный потенциальный ущерб от внутреннего нарушителя. | • Поиск уязвимостей внутри инфраструктуры с зараженного хоста.<br>• Перемещение между хостами через эксплуатацию уязвимостей.<br>• Установка агента на уязвимые хосты.<br>• Оценка потенциального ущерба.<br>• Поддержка разных режимов работы.<br>• Визуализация хостов с агентами на карте сети.<br>• Логирование всех действий перемещения.<br>• Автоматический переход к фазе поиска и эксфильтрации данных.<br>• Разграничение прав доступа.<br>• Управление заданиями. |
| Модуль эксфильтрации данных | Обнаружение конфиденциальной информации внутри инфраструктуры компании и её отправка во внешнее хранилище в зашифрованном виде.  | • Обнаружение конфиденциальной информации во всей инфраструктуре.<br>• Поиск чувствительных данных на всех доступных носителях.<br>• Выявление архивов, репозиториев, БД, резервных копий и документов.<br>• Настройка типов и расширений файлов для поиска.<br>• Шифрование данных  |

| Название                            | Описание   | Функциональные возможности   |
|-------------------------------------|--|--|
|                                     |  | перед эксфильтрацией. <ul style="list-style-type: none"> <li>• Создание и клонирование заданий поиска и выгрузки.</li> <li>• Настройка параметров заданий (типы файлов, хранилище, расписание).</li> <li>• Запуск заданий в ручном режиме или по расписанию.</li> <li>• Управление статусом заданий.</li> <li>• Автоматическое построение и выгрузка отчётов.</li> <li>• Визуализация результатов (найденные файлы, репозитории, адреса).</li> </ul>   |
| Модуль удаления и шифрования данных | Проверка доступов к разделам и прав перезаписи файлов на указанных хостах. При наличии прав фиксируется событие о возможности шифрования хоста. Имитирует шифрование различных типов данных. | <ul style="list-style-type: none"> <li>• Проверка прав доступа к разделам и права перезаписи файлов.</li> <li>• Фиксация события о возможности шифрования хостов.</li> <li>• Имитация шифрования различных типов данных (архивы, БД, документы).</li> <li>• Создание заданий с выбором типов файлов для шифрования.</li> <li>• Настройка белых и черных списков активов.</li> <li>• Просмотр и редактирование параметров заданий.</li> <li>• Управление статусом заданий.</li> <li>• Запуск заданий в ручном или отложенном режиме.</li> <li>• Построение и выгрузка отчётов.</li> <li>• Фиксация результатов шифрования.</li> </ul> |

| Название                  | Описание  | Функциональные возможности  |
|---------------------------|---|---|
|                           |   | <ul style="list-style-type: none"> <li>• Разграничение прав доступа.</li> </ul>   |
| Модуль перебора хешей     | Метод перебора паролей, пользователей или извлечения паролей из хеш-сумм. Используется для получения первоначального доступа к серверам, оборудованию и рабочим станциям. | <ul style="list-style-type: none"> <li>• Автоматическое построение отчёта по результатам каждой итерации задания.</li> <li>• Отображение метаданных задания (название, автор, дата создания и запуска, статус).</li> <li>• Представление результатов выполнения: подобранные пароли, хеши с неудачными попытками.</li> <li>• Просмотр и выгрузка отчёта.</li> </ul>   |
| Модуль локальной разведки | Функциональный компонент тонкого агента, выполняющий сканирование внутреннего состояния хоста.  | <ul style="list-style-type: none"> <li>• Анализ ОС, прав доступа и привилегий.</li> <li>• Поиск чувствительных данных в файлах Linux и Windows.</li> <li>• Проверка прав доступа к системным файлам (/etc/shadow).</li> <li>• Инвентаризация установленного ПО и служб.</li> <li>• Сбор учетных данных и хешей паролей.</li> <li>• Обнаружение систем защиты и антивирусов.</li> <li>• Поиск векторов для эскалации привилегий.</li> <li>• Анализ автозагрузки и механизмов постоянства.</li> <li>• Выявление уязвимых конфигураций и служб.</li> <li>• Поиск возможностей для перемещения в сети.</li> </ul> |
| Модуль перебора УЗ        | Компонент для автоматизированного обнаружения рабочих пар (логин/пароль) к  | <ul style="list-style-type: none"> <li>• Активный брутфорс учетных данных по SSH.</li> </ul>  |

| Название           | Описание   | Функциональные возможности   |
|--------------------|--|--|
|                    | внутренним сервисам методом комбинированного перебора и пассивного анализа.  | <ul style="list-style-type: none"> <li>• Пассивный сбор валидных логинов и паролей FTP через NXC.</li> <li>• Тихий сбор учетных данных SSH в режиме NXC.</li> <li>• Обнаружение паролей в открытом виде при FTP/SSH-аутентификации.</li> <li>• Анализ чистого текста в сетевых протоколах.</li> <li>• Поиск учетных данных в конфигурационных файлах.</li> <li>• Регулировка скорости перебора.</li> <li>• Приоритизация целей по критичности.</li> <li>• Комбинирование активных и пассивных методов.</li> <li>• Формирование базы валидных учетных записей.</li> <li>• Обеспечение скрытности операций.</li> <li>• Подготовка данных для горизонтального перемещения.</li> </ul> |
| Модуль закрепления | Обеспечение автоматического запуска агента после перезагрузки системы или ключевых служб для поддержания постоянного присутствия в инфраструктуре. | <ul style="list-style-type: none"> <li>• Создание автозагрузочных записей в реестре Windows.</li> <li>• Настройка заданий в планировщике задач Windows.</li> <li>• Регистрация в папке автозагрузки пользователя.</li> <li>• Установка в качестве системной службы (Windows/Linux).</li> <li>• Настройка планировщика заданий в Linux.</li> <li>• Создание файлов</li> </ul>   |

| Название                    | Описание  | Функциональные возможности  |
|-----------------------------|---|---|
|                             |   | сервисов для systemd.<br>• Добавление в автозагрузку через системные скрипты.<br>• Изменение профилей оболочки.<br>• Реализация множественных механизмов.<br>• Обеспечение скрытности записей.<br>• Автоматическое восстановление при сбое.<br>• Адаптация под текущий уровень привилегий.<br>• Кросс-платформенная поддержка.<br>• Обход стандартных методов обнаружения.  |
| Модуль повышения привилегий | Функциональный компонент локального агента для эскалации прав доступа с пользовательского уровня до администраторского (root/sudo/system) на целевом хосте. | • Повышение привилегий через эксплуатацию уязвимостей.<br>• Обход механизмов sudo.<br>• Поиск и использование уязвимостей ядра ОС.<br>• Использование слабых разрешений файловой системы.<br>• Эксплуатация уязвимостей в планировщике заданий ОС.<br>• Обход механизмов защиты.<br>• Автоматический подбор и проверка эксплойтов.<br>• Подтверждение полученных привилегий администратора.<br>• Кросс-платформенная поддержка. |

## 2.2 Программная структура комплекса

Структура комплекса включает следующие основные подсистемы:

- 1) Подсистема хранения данных СУБД. Обеспечивает хранение служебных данных ПК, а также состояния модулей и ядра системы (задания, агенты, библиотека и т.д.) в соответствующей базе данных.
- 2) Подсистема авторизации и аутентификации. Обеспечивает аутентификацию и авторизацию пользователей, контроль и разграничение прав доступа пользователей к функциям ПК.
- 3) Интеграционная подсистема. Обеспечивает возможности лицензирования, обновления, доставки необходимых данных для работы ПК.
- 4) Клиентское веб-приложение. Обеспечивает веб-интерфейс пользователя для управления и запуска атак.

**Примечание.** По результатам атак в веб-интерфейсе отображаются успешность, затрагиваемые и зараженные узлы, а также оценка. По результатам проведения атак формируется отчет, содержащий информацию об используемых эксплойтах, адресах узлов и эксплуатируемое ПО, в котором были выявлены уязвимости.

## 2.3 Входные и выходные ресурсы функциональных модулей ПК «SimuStrike»

Входные и выходные ресурсы функциональных модулей ПК «SimuStrike» приведены в таблице 2.

Таблица 2 – Входные и выходные ресурсы

| Название                            | Входные ресурсы                     | Выходные ресурсы   |
|-------------------------------------|-------------------------------------|--|
| Модуль горизонтального перемещения  | Сетевой сервис, IP                  | Агент, пара пользователь и пароль, пара логин и пароль, пара пользователь и хеш, пара хост и пароль                                      |
| Модуль сканирования Web             | Сетевой сервис, URI, FQDN           | URI, e-mail, телефон, сетевой сервис, пара ПО и хост, пара ПО и URI  |
| Модуль удаления и шифрования данных | Сетевой сервис                      | Файл   |
| Модуль эксфильтрации данных         | Директория, агент, файл             | Файл, пользователь, хеш, пара пользователь и хеш   |
| Модуль первоначального доступа      | Сетевой сервис, пара логин и пароль | Сетевой сервис, пара хост и пароль, пара логин и пароль, пара пользователь и пароль  |
| Модуль сканирования AD              | Сеть, IP, сетевой сервис,           | Сеть, сетевой сервис, IP, пользователь, пароль, пара пользователь и пароль, пара хост и хеш, пара пароль и хост, пара пользователь и хеш |
| Модуль сетевого                     | IP, FQDN, сервис                    | IP, сетевой сервис, пара ПО и хост, пара ПО и  |

| Название     | Входные ресурсы | Выходные ресурсы |
|--------------|-----------------|------------------|
| сканирования |                 | URI              |

## 2.4 Свойства ПК «SimuStrike»

Свойства ПК «SimuStrike» приведены в таблице 3.

Таблица 3 – Свойства комплекса

| Название                                    | Описание  |
|---|---|
| Доступ к обновлению сценариев               | Загрузка и актуализация новых исполняемых сценариев |
| Доступ к обновлению словарей                | Загрузка и актуализация новых версий словарей       |
| Доступ к обновлению базы данных уязвимостей | Загрузка и актуализация базы данных уязвимостей     |
| Доступ к шаблонам кампаний                  | Использование готовых шаблонов кампаний             |
| Доступ к шаблонам фишинга                   | Использование готовых шаблонов фишинга              |

### 3 Масштабирование

Производительность решения в контексте скорости обработки и полноты охвата сетевой инфраструктуры заказчика может быть масштабирована путем развертывания дополнительных агентов. Установка новых агентов позволяет увеличить параллелизм выполнения задач, что способствует более эффективному мониторингу и управлению сетевыми ресурсами. Это также обеспечивает гибкость в адаптации к изменяющимся требованиям инфраструктуры и позволяет оптимизировать распределение нагрузки между компонентами системы.

Ёмкость решения с точки зрения скорости и полноты охвата сетевой инфраструктуры заказчика может регулироваться установкой новых агентов.

## Перечень сокращений

|       |   |                                       |
|-------|---|---------------------------------------|
| AD    | – | Active Directory                      |
| API   | – | Application Programming Interface     |
| CVE   | – | Common Vulnerabilities and Exposures  |
| HTTP  | – | HyperText Transfer Protocol           |
| HTTPS | – | HyperText Transfer Protocol Secure    |
| IP    | – | Internet Protocol                     |
| LDAP  | – | Lightweight Directory Access Protocol |
| MAC   | – | Media Access Control                  |
| NA    | – | Network Address                       |
| SNMP  | – | Simple Network Management Protocol    |
| SQL   | – | Structured Query Language             |
| SSH   | – | Secure Shell                          |
| TI    | – | Threat Intellegence                   |
| TTP   | – | Tactics Technics Protocols            |
| TLS   | – | Transport Layer Security              |
| БД    | – | База данных                           |
| БДУ   | – | База данных уязвимостей               |
| ИБ    | – | Информационная безопасность           |
| КО    | – | Клиентское оборудование               |
| МЭ    | – | Межсетевой экран                      |
| ОС    | – | Операционная система                  |
| ПК    | – | Программный комплекс                  |
| ПО    | – | Программное обеспечение               |
| ПТС   | – | Программно-технические средства       |
| СрЗИ  | – | Средства защиты информации            |
| СЗИ   | – | Система защиты информации             |
| ТУ    | – | Технические условия                   |
| ИБ    | – | Информационная безопасность           |