

## Функциональные характеристики системы для проведения киберучений Nuke «Command and Control Server»

## Оглавление

|                                         |          |
|-----------------------------------------|----------|
| 1. ВВЕДЕНИЕ                             | 3        |
| 1.1. НАЗНАЧЕНИЕ СИСТЕМЫ.                | 3        |
| 1.2. ВВЕДЕНИЕ В СТРУКТУРУ КОМПЛЕКСА.    | 3        |
| 2. АРХИТЕКТУРА ПРОГРАММНОГО КОМПЛЕКСА   | 3        |
| 3. ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ.          | 4        |
| 3.1 . ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ.       | 4        |
| 3.2. КАТЕГОРИИ ПОЛЬЗОВАТЕЛЕЙ КОМПЛЕКСА. | 4        |
| <b>3.3. Функционирование системы</b>    | <b>4</b> |
| <b>3.3. Язык программирования.</b>      | <b>4</b> |

## 1. Введение

### 1.1. Назначение системы.

Система для проведения киберучений Nuke «Command and Control Server» (далее ПО, программное обеспечение) - средство автоматизации процесса тестирования на проникновения и управлениями конечными устройствами.

### 1.2. Введение в структуру комплекса.

Основными компонентами программного обеспечения являются:

- Командный центр ПО (далее - КЦ)
- Прокси сервер (далее – ПС)
- Сервер сборки полезной нагрузки (далее – СС)
- Агент (далее – АГ)

## 2. Архитектура программного комплекса

Визуальное представление архитектуры программного комплекса зафиксировано на рисунке 2.1.

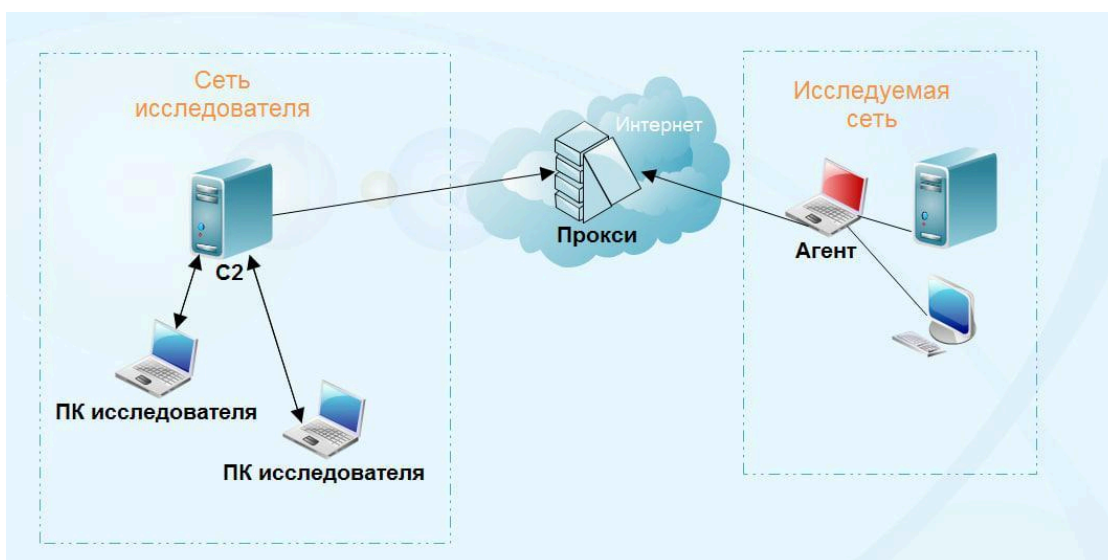


Рисунок 2.1. – Архитектура программного комплекса

Программный комплекс состоит из следующих логических модулей:

- Web Клиент Сервера ПО
- Консольный Клиент Сервера С2
- Сервер ПО
- Прокси
- Агент

- Нагрузка
- Билдсервер

### 3. Технические характеристики.

#### 3.1. Функциональные возможности.

Программное обеспечение поддерживает работу во всех современных браузерах: Google Chrome, Яндекс Браузер, Opera, Microsoft Edge, Firefox, Safari.

Задачами работы комплекса С2 являются:

- Проверка доступности ресурсов
- Инвентаризация ИТ активов
- Возможность выполнения команд и управления конечными станциями
- Возможность взаимодействия с другими сетевыми ресурсами посредством одного узла.
- Получение информации о ресурсах в сети

#### 3.2. Категории пользователей комплекса.

Авторизованный пользователь, с полным доступом обладает правами:

- Просмотр всех доступных разделов и справочных материалов.
- Создание моделей проникновения и управления конечными устройствами.
- Назначение ролей и прав доступа для остальных пользователей ПО.

Авторизованный пользователь, с неполным доступом обладает правами просмотра только тех разделов ПО, которые установил для него, пользователь с полными правами.

Для неавторизованного пользователя доступ в ПО невозможен, но он имеет возможность скачать консольный клиент для необходимой ему операционной системы.

#### 3.3. Функционирование системы

Так как ПО работает на арендованных серверах дата-центра Rucloud, 141070, Московская область, Королев, ул Пионерская, д4, отдельных требований к персональным компьютерам конечного пользователя не предъявляется. Для работы с системой пользователю необходим выход в Интернет и любой современный браузер.

#### 3.3. Язык программирования.

Языками программирования для программного комплекса С2 являются: Golang, JavaScript, Python.