**Документация автоматизированной системы сканирования ресурсов Дочерних Обществ, расположенных в сети Интернет (АССРДО).**

**Общие сведения.**

В соответствии с договором от 18.06.2014 № 816-СКЗ в 2014 году ЗАО «Позитив Технолоджиз» проведена работа по инвентаризации и оценке защищенности информационных ресурсов ОАО «Газпром» и ряда дочерних обществ, опубликованных в сети Интернет.

Защищенность периметра Компаний Группы Газпром была оценена исполнителем удовлетворительно. Вместе с тем ЗАО «Позитив Технолоджиз» был выявлен ряд уязвимостей в информационных системах, которые впоследствии оперативно устранялись Управлением информационной безопасности совместно с дочерними обществами.

В целях организации таких работ на постоянной основе Управлением информационной безопасности в соответствии с запросом, направленным в дочерние общества и организации письмом от 14.01.2015 № СКЗ-8/КТ, сформирован уточненный перечень оборудования и информационных ресурсов Общества, подключенных к сети Интернет. Для выполнения проверок состояния защищенности этих ресурсов работниками отдела защиты информационных систем Управления информационной безопасности (далее – ОЗИС УИБ) разработан аппаратно-программный комплекс (далее – АПК), осуществляющий в автоматическом режиме их регулярное сканирование на предмет выявления доступных сервисов и служб.

АПК реализован на базе свободно-распространяемого программного обеспечения: операционной системы FreeBSD, базы данных MariaDB, веб-сервера Apache, скриптов PHP и сканера сети Nmap. С мая 2015 г. АПК подключен к сети Интернет и проходит опытную эксплуатацию.

**Настройка и установка системы.**

**Требования к системе:**

* 1. **Структура меню:**

1. Полный отчет;
2. Нелегитимные порты;
3. Новые порты;
4. Сканирование – появляется только для пользователей с ролью «ADMIN».

**Описание страниц:**

* 1. **Страница «Полный отчет».**

Функциональные элементы:

Фильтр по дочерним обществам. Отображает все дочерние общества. Для подбора используется контекстный поиск. Данные в таблице фильтруются по выбранному значению.

В правом верхнем углу иконка с изображением pdf документа, при нажатии на которую весь выводимый список из приведенной таблице выгружается в документ pdf.

Таблица всех портов, структура таблицы:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование колонки | Описание | Возможность редактирования |
| 1 | host\_id | Идентификатор хоста. Таблица hosts->host\_id | --- |
| 2 | do\_id | Идентификатор дочернего общества. Таблица do->do\_id | + |
| 3 | Дочернее Общество | Наименование дочернего общества. Таблица do->do\_id |
| 4 | Описание ресурса | Описание хоста. Таблица hosts->description | + |
| 5 | IP адрес | IP адрес хоста. Таблица hosts->ipaddr | + |
| 6 | Порт | Таблица ports->portnum | + |
| 7 | Протокол | tcp/udp. Таблица ports->prot | + |
| 8 | Статус | Только записи со статусом «Открыт». Таблица ports->status | + |
| 9 | Лигитимность | Да/Нет. Таблица ports->ligitim | + |
| 10 | Дата обновления | Таблица ports->scan\_data | --- |

Пользователь с ролью «ADMIN» поможет редактировать реквизиты.

* 1. **Страница «Нелегитимные порты».**

В правом верхнем углу иконка с изображением pdf документа, при нажатии на которую весь выводимый список из приведенной таблице выгружается в документ pdf.

Таблица нелегитимных портов отображает порты, у которых реквизит «Легитимность» равен «Нет». Структура таблицы:

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование колонки | Описание |
| 1 | host\_id | Идентификатор хоста. Таблица hosts->host\_id |
| 2 | do\_id | Идентификатор дочернего общества. Таблица do->do\_id |
| 3 | Дочернее Общество | Наименование дочернего общества. Таблица do->do\_id |
| 4 | Описание ресурса | Описание хоста. Таблица hosts->description |
| 5 | IP адрес | IP адрес хоста. Таблица hosts->ipaddr |
| 6 | Порт | Таблица ports->portnum |
| 7 | Протокол | tcp/udp. Таблица ports->prot |
| 8 | Статус | Только записи со статусом «Открыт». Таблица ports->status |
| 9 | Лигитимность | Да/Нет. Таблица ports->ligitim |
| 10 | Дата обновления | Таблица ports->scan\_data |

* 1. **Страница «Новые порты».**

В правом верхнем углу иконка с изображением pdf документа, при нажатии на которую весь выводимый список из приведенной таблице выгружается в документ pdf.

Таблица новых портов отображает порыт, у которых реквизит не определен реквизит «Легитимность». Структура таблицы:

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование колонки | Описание |
| 1 | host\_id | Идентификатор хоста. Таблица hosts->host\_id |
| 2 | do\_id | Идентификатор дочернего общества. Таблица do->do\_id |
| 3 | Дочернее Общество | Наименование дочернего общества. Таблица do->do\_id |
| 4 | Описание ресурса | Описание хоста. Таблица hosts->description |
| 5 | IP адрес | IP адрес хоста. Таблица hosts->ipaddr |
| 6 | Порт | Таблица ports->portnum |
| 7 | Протокол | tcp/udp. Таблица ports->prot |
| 8 | Статус | Только записи со статусом «Открыт». Таблица ports->status |
| 9 | Лигитимность | Да/Нет. Таблица ports->ligitim |
| 10 | Дата обновления | Таблица ports->scan\_data |

* 1. **Страница «Сканирование».**

На отдельной странице текстовое поле ввода IP-адреса сканируемого объекта, поле ввода номера порта. Также ниже расположен контекстный поиск по ДО и IP адресу необходимого хоста.

При контекстном выборе выводится таблица:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование колонки | Описание | Возможность редактирования |
| 1 | Выбор | Элемент радио-кнопка для выбора сканируемого хоста. | --- |
| 1 | host\_id | Идентификатор хоста. Таблица hosts->host\_id | --- |
| 2 | do\_id | Идентификатор дочернего общества. Таблица do->do\_id | --- |
| 3 | Дочернее Общество | Наименование дочернего общества. Таблица do->do\_id |
| 4 | Описание ресурса | Описание хоста. Таблица hosts->description | --- |
| 5 | IP адрес | IP адрес хоста. Таблица hosts->ipaddr | --- |

Возможно выбрать только один ресурс для сканирования. И при нажатии кнопки «Сканировать» выводить в режиме онлайн в том же окне результат работы утилиты сканирования. Также предусмотреть возможность выгрузки отчета по сканированию в документе формата pdf.

Параметры запуска программы сканирования следующие:

nmap -sS -sU -P0 IP-адрес\_хоста

* 1. **Безопасность:**

Роли: USER, ADMIN