|  |  |
| --- | --- |
| **К Г Э У** | МИНИСТЕРСТВО ВЫСШЕГО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  **Федеральное государственное бюджетное образовательное учреждение**  **высшего образования**  **«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»**  (ФГБОУ ВО «КГЭУ») |

Отчет по лабораторной работе №2

по дисциплине «Информационная безопасность»

**«Разработка сценария кибератаки для моделирования угроз безопасности информации»**

**Выполнил:**

студент Тазеев Р.Р.

**Группа:**

ТРП-1-23

**Проверил:**

Доцент ИТИС  
Хуснутдинов Рамиль Миннегаязович

Казань, 2024 г.

**Цель работы:** обучить учащихся использованию российских и международных баз данных, содержащих тактики и техники злоумышленников, для моделирования угроз информационной безопасности.

**Задание для выполнения**

1. Перечислить, к каким негативным последствиям и ущербу может привести нарушение технологического процесса после реализации угроз безопасности информации в АСУ ТП ТУ.

1. **Технические повреждения оборудования:** Поломка механизмов и устройств вследствие несоответствующих параметров работы.
2. **Простои производства:** Время, необходимое для восстановления нормальной работы системы.
3. **Финансовые потери:** Убытки, вызванные невыпуском продукции или простоями.
4. **Угроза безопасности:** Возможные аварии, представляющие опасность для жизни и здоровья работников.
5. **Нанесение ущерба окружающей среде:** Потенциальные утечки материалов или загрязнение окружающей среды.
6. **Потеря данных:** Уничтожение или изменение критически важной информации.
7. **Убытки репутации:** Отрицательное влияние на имидж компании и доверие со стороны клиентов.

2. Перечислить возможные векторы кибератак на АСУ ТП ТУ. При выборе векторов атак учитывать как внешних, так и внутренних нарушителей, а также различные виды интерфейсов воздействия на компоненты АСУ ТП.

**Внешние нарушители:**

1. **Фишинг:** Применение поддельных писем и веб-сайтов для похищения учетных данных.
2. **Вредоносные программы:** Установка через уязвимости в сетевой инфраструктуре.
3. **DDoS-атаки:** Перегрузка сетевых ресурсов для нарушения их доступности.
4. **Удаленные уязвимости:** Использование уязвимостей в протоколах связи для атаки.

**Внутренние нарушители:**

1. **Неправомерный доступ:** Использование служебных учетных записей для выполнения несанкционированных действий.
2. **Ошибки по неосторожности:** Неправильные действия сотрудников, не знакомых с установленными процессами.
3. **Внутренние угрозы:** Сотрудники, испытывающие недовольство, которые могут намеренно нанести ущерб.

3. Отдельно для каждого из перечисленных векторов кибератак составить Kill chain с помощью тактик и техник матриц MITRE ATT&CK Enterprise, MITRE ATT&CK for ICS. Целевой объект Kill chain необходимо выбирать исходя из того, что нарушитель преследует основную цель – нарушить технологический процесс.

**Внешние нарушители:  
Шаг 1**

1. **Узел-инициатор**: Хакер
2. **Узел-жертва:** Элементы сети
3. **Тактика:** Получение начального доступа
4. **Техника:** Фишинговая атака

**Шаг 2**

1. **Узел-инициатор:** Зараженный компьютер
2. **Узел-жертва:** Оборудование АСУ ТП
3. **Тактика:** Взаимодействие с целью
4. **Техника:** Эксплуатация уязвимостей

**Шаг 3**

1. **Узел-инициатор:** Хакер
2. **Узел-жертва:** Оборудование АСУ ТП
3. **Тактика:** Изменение данных
4. **Техника:** Манипуляция технологическими параметрами

**Внутренние нарушители:  
Шаг 1**

1. **Узел-инициатор:** Служебный сотрудник
2. **Узел-жертва:** Информационная система АСУ ТП
3. **Тактика:** Несанкционированный доступ
4. **Техника:** Использование служебных учетных записей

**Шаг 2**

1. **Узел-инициатор:** Служебный сотрудник
2. **Узел-жертва:** Оборудование АСУ ТП
3. **Тактика:** Изменение данных
4. **Техника:** Использование внутренних полномочий

**Шаг 3**

1. **Узел-инициатор:** Служебный сотрудник
2. **Узел-жертва:** Процесс в АСУ ТП
3. **Тактика:** Завершение процесса
4. **Техника:** Нарушение рабочих процедур

**4. Kill chain оформляется схематично в виде последовательности шагов атаки от узла к узлу. Для каждого шага атаки показать:**

* Порядковый номер шага атаки;
* Узел-инициатор атаки;
* Узел-жертва атаки;
* Тактика;
* Техника(-и).

**Внешние нарушители**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Шаг атаки** | **Узел-инициатор** | **Узел-жертва** | **Тактика** | **Техника** | **Используемые инструменты уязвимости** | **УБИ БДУ ФСТЭК** | **Способы обнаружения** | **Способы противодействия** |
| 1 | *Хакер* | *Элементы сети* | *Начальная точка доступа* | *Фишинг* | *Фальшивые сайты/письма* | *УБИ 3.13,3.14* | *Логи входа, мониторинг трафика* | *Обучение персонала, антивирусы* |
| 2 | *Зараженный компьютер* | *Оборудование АСУ ТП* | *Устное взаимодействие* | *Использование уязвимости* | *Уязвимость ПО* | *УБИ 3.17* | *Мониторинг активности* | *Обновление ПО, система IDS* |
| 3 | *Хакер* | *Оборудование АСУ ТП* | *Изменение данных* | *Манипуляции с параметром* | *Скрипты, вирусы* | *УБИ 3.12, 3.13* | *Аудит действий* |  |

**Внутренние нарушители**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Шаг атаки** | **Узел-инициатор** | **Узел-жертва** | **Тактика** | **Техника** | **Используемые инструменты уязвимости** | **УБИ БДУ ФСТЭК** | **Способы обнаружения** | **Способы противодействия** |
| *1* | *Служебный сотрудник* | *Информационная система АСУ ТП* | *Неправомерный доступ* | *Использование служебных учетных записей* | *Слабые пароли* | *УБИ 3.15* | *Аудит доступов, мониторинг* | *Политика паролей, двухфакторная аунтефикация* |
| *2* | *Служебный сотрудник* | *Оборудование АСУ ТП* | *Изменение данных* | *Внутренние средства* | *Доступ к базам данных* | *УБИ 3.21* | *Логи систем* | *Обучение, внутренние аудиты* |
| *3* | *Служебный сотрудник* | *Процесс в АСУ ТП* | *Завершение процесса* | *Нарушение рабочих процессов* | *Устройства конроля доступа* | *УБИ 3.12* | *Мониторинг работы* | *Меры по контролю, аудит действий* |

5. Для внешнего и внутреннего нарушителей должны быть разные Kill chain (конечные стадии Kill chain обычно совпадают, но векторы атак должны быть разные)

6. Отдельно в табличном виде для каждого шага атаки указать:

* Используемые инструменты/ уязвимости/ эксплойты;
* УБИ БДУ ФСТЭК, реализуемые на данном шаге атаки;
* Способы обнаружения атаки;
* Способы и средства противодействия атаке (меры защиты).

**Внешние нарушители**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Шаг атаки** | **Используемые инструменты/уязвимости/эксплойты** | **УБИ БДУ ФСТЭК** | **Способы обнаружения атаки** | **Способы и средства противодействия атаке (меры защиты)** |
| *1* | *Фальшивые сайты, фишинговые письма* | *УБИ 3.13, 3.14* | *Логи входа, мониторинг трафика* | *Обучение персонала, системы фильтрации email, антивирусы* |
| *2* | *Уязвимость ПО* | *УБИ 3.17* | *Мониторинг активности, IDS/IPS* | *Регулярные обновления и патчи, сетевые экраны* |
| *3* | *Вредоносные скрипты, эксплойты на уровне ОС* | *УБИ 3.12, 3.13* | *Аудит изменений, анализ логов* | *Мониторинг поведения, антивирусные решения, бэкапы* |

**Внутренние нарушители**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Шаг атаки** | **Используемые инструменты/уязвимости/эксплойты** | **УБИ БДУ ФСТЭК** | **Способы обнаружения атаки** | **Способы и средства противодействия атаке (меры защиты)** |
| *1* | *Слабые пароли, доступ через служебные учетные записи* | *УБИ 3.15* | *Аудит доступов, смена паролей* | *Политика паролей, двухфакторная аутентификация* |
| *2* | *Внутренние средства доступа (например, VPN)* | *УБИ 3.21* | *Логи систем, мониторинг действий пользователей* | *Внедрение контроля доступа, регулярные внутренние аудиты* |
| *3* | *Использование стандартных утилит для завершения процессов* | *УБИ 3.12* | *Наблюдение за аномальной активностью* | *Установление строгих процедур для доступа к системам и данным* |