ШОУ ПРОФЕССИЙ

СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СЦЕНАРНЫЙ ПЛАН ПРОВЕДЕНИЯ ПРОФОРИЕНТАЦИОННОГО ЗАНЯТИЯ

Содержание

1. Тема занятия .....
1.1. Цель занятия 2
1.2. Задачи занятия 2
1.3. Методическое обеспечение занятия 3

2. Описание занятия 4
2.1. Интервью с преподавателем 4
2.2. Вводная часть занятия 4

3. Практическая часть занятия 5
3.1. Демонстрация профессиональных приемов 5
3.2. Обзор профессиональных образовательных организаций 5
3.3. Выполнение заданий 5

4. Вывод 6

1. Тема занятия

Специалист по информационной безопасности

1.1. Цель занятия

Сформировать представление у обучающихся о процессе ликвидации последствий хакерской атаки на сервер компании. Продемонстрировать устранение «уязвимости в доступе» в онлайн-режиме.

1.2. Задачи занятия

Образовательные:

- продемонстрировать обучающимся признаки хакерской атаки на сайт;
- познакомить обучающихся с процессом определения способа проникновения злоумышленника на сайт компании;
- познакомить обучающихся с методами защиты от хакерской атаки и спецификой каждого метода;
- познакомить с понятийным аппаратом: хакерская атака, сетевой анализатор трафика, запрос на авторизацию, учетная запись, декодер, IP-адрес, файервол (Firewall).

Развивающие:

- познакомить со спецификой профессии «Специалист по информационной безопасности»;
- сформировать навыки работы с высокотехнологичным оборудованием;
- познакомить с образовательными организациями среднего профессионального образования, где обучают данной профессии.

Воспитательные:

- формировать устойчивый интерес к профессии, умение планировать и реализовывать собственное профессиональное и личностное развитие;

- воспитывать эмоционально-нравственные качества, ответственное отношение к труду, положительную мотивацию к выполнению практических задач;
- способствовать развитию коммуникативных способностей, умений для эффективной работы с высокотехнологичным оборудованием;
- формировать у обучающихся сознательное отношение к профессиональному самоопределению с учетом индивидуальных склонностей и интересов, востребованности профессии.

1.3. Методическое обеспечение занятия

Форма организации деятельности на занятии:

- индивидуально-групповая.

Методы и приемы организации занятия:

- наглядный (демонстрация);
- словесный (беседа, объяснение);

Оборудование и оснащение занятия:

- компьютер, клавиатура, мышь

Информация для преподавателя:

- Определение признаков хакерской атаки.
- Демонстрация использования программы-анализатора.
- Демонстрация установки двухфакторной защиты.

2. Описание занятия

2.1. Интервью с преподавателем

Преподаватель специальных дисциплин Сергей Варламов Подмосковного колледжа «Энергия» объясняет признаки хакерской атаки, показывает, как ликвидировать ее последствия в режиме реального времени и защититься от возможных атак в будущем.

2.2. Вводная часть занятия

***Преподаватель*:** Здравствуйте! Сейчас мы с моим помощником продемонстрируем, как можно защититься от хакерской атаки, которая произошла на сервер компании, и попробуем в моменте устранить эту проблему.

***Преподаватель*:** Нам удалось перехватить некоторую часть данных, которая передавалась с компьютера хакера. Как вы думаете, что помогло нам это сделать?

***Студенты*:** выдвигают свои версии.

***Преподаватель*:** Перехватить данные мы смогли с помощью программы анализатора трафика. Какие данные удалось перехватить с помощью этой программы?

***Студенты*:** выдвигают свои версии.

***Преподаватель*:** Совершенно верно, мы нашли IP-адрес злоумышленника, а еще увидели запросы, которые он посылал на наш сервер для того, чтобы проникнуть в нашу систему.

***Преподаватель*:** Наша задача как специалистов по информационной безопасности, найти уязвимость и устранить ее. Давайте начнем.

3. Практическая часть занятия

3.1. Демонстрация профессиональных приемов

В ходе мастер-класса преподаватель:

- оценивает данные, которые удалось перехватить при передаче с компьютера хакера;
- определяет IP-адрес злоумышленника с помощью программы сетевого анализатора трафика;
- изучает запросы, которые посылал хакер на сервер компании для того, чтобы проникнуть в систему;
- блокирует IP-адрес хакера;
- изменяет пароль входа на сервер;
- применяет более надежные методы защиты информации — двухфакторную идентификацию.

3.2. Обзор профессиональных образовательных организаций

Освоить профессию «Специалист по информационной безопасности» можно в профильных учреждениях среднего профессионального образования, а также в учебных центрах дополнительного профессионального образования; например, в колледжах и техникумах ПРОФЕССИОНАЛИТЕТА:

- Уфимский многопрофильный профессиональный колледж
- Омский авиационный колледж имени Н.Е. Жуковского
- Томский индустриальный техникум
- Ногинский колледж (Московская область)

3.3. Выполнение заданий

Чтобы закрепить знания, предлагается ответить на несколько вопросов.

- Для чего нужна программа «анализатор трафика»?
- Что такое IP-адрес?
- Какие действия предпринимает хакер для проникновения в систему?
- Что такое двухфакторная идентификация?

4. Вывод

Данный мастер-класс позволяет получить представление о работе специалистов по информационной безопасности, узнать о процессе анализа действий хакера, способах защиты от хакерской атаки в моменте и надежных методах профилактики уязвимости серверов в будущем.