**«Администратор Программного Комплекса Efros Defense Operations. Модуль Network Access Control»**

**Цель обучения:**получение теоретических знаний и практических навыков администрирования комплекса Efros Defense Operations (ПК EDO), включая установку, настройку сервисов, добавление объектов защиты и работу с модулем «Разграничение и контроль доступа в сети (NAC)».

**Для кого этот курс?**

- начальники отделов и специалисты служб безопасности (информационной безопасности);

- руководители и сотрудники отделов автоматизации, вычислительных центров, информационно-технических отделов;

- руководители и сотрудники специализированных подразделений по защите конфиденциальной информации;

- администраторы безопасности компьютерных сетей.

**Профессиональный стандарт**: 06.032 Специалист по безопасности компьютерных систем и сетей 14.09.2022

**Срок обучения:**24 академических часов (3 учебных дня)

**Формат**: очный/дистанционный, с отрывом от работы.

**Режим занятий**: 8 академических часов в день

**Структура курса**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №№  п.п. | Наименование разделов и тем | Всего часов | В том числе | | Форма контроля |
|  |  |  | Лекции | Практ. занятия |  |
| **1** | **Назначение и структура программного комплекса Efros Defense Operations (ПК EDO).** | **2** | **2** |  | **Мини-тест** |
| 1.1. | Назначение ПК EDO, основные возможности и преимущества. Структура ПК EDO, функциональные модули, микросервисы. Политика лицензирования | 1 | 1 |  |  |
| 1.2. | Подготовка к установке, предварительные требования. Виды дистрибутивов. | 1 | 1 |  |  |
| **2.** | **Установка и удаление ПК EDO. Настройка и администрирование.** | **6** | **2** | **4** | **Мини-тест** |
| 2.1. | Установка и первоначальная настройка серверной части ПК EDO на ОС Astra Linux. Использование скриптов, работа с контейнерами Docker.  Ознакомление с необходимыми командами для удаления ПК EDO | 2 | 1 | 1 |  |
| 2.2. | Начало работы. Знакомство с веб-интерфейсом, активация лицензии | 1 | 1 |  |  |
| 2.3. | Раздел «Администрирование» (управление учетными записями (УЗ) пользователей, назначение ролей, привилегий; создание групп пользователей; использование настроек безопасности УЗ и парольной политики; предустановленные задачи; настройка оповещений; использование сертификатов)  Раздел «Настройки» (управление сроками и объёмом хранения данных, событий и потокам данных способах; интеграции с почтовым сервером (SMTP, Microsoft Exchange); настройка параметров отправки почтовых сообщений; сервер DNS как источник данных для базы знаний; загрузка модулей, обновления, включения/отключения) | 1 |  | 1 |  |
| 2.4. | Раздел «Объекты сети» (отображение, создание, редактирование, удаление объектов защиты (ОЗ), добавление возможностей; подразделы База знаний, Сканирование; использование автоматизированной возможности формирования списка подключенных устройств.  Раздел «Мониторинг» (использование виджетов для отображения информации о метриках комплекса – работа с вкладками, создание, настройка виджетов).  Раздел «События» (типы событий; работа с событиями, связанными с действиями пользователя при работе с комплексом – фильтрация, экспорт, классы и типы событий; работа со списком событий безопасности, полученных от ОЗ – фильтрация, экспорт, типы событий, важность; экспорт событий) | 2 |  | 2 |  |
| **3.** | **Модуль Network Access Control (NAC).** **Разграничение и контроль доступа в сети.** | **14** | **6** | **8** | **Мини-тест** |
| 3.1. | Вводная часть. Виды сетевого доступа, схема ААА, протоколы доступа в сеть и на оборудование, методы аутентификации. | 1 | 1 |  |  |
| 3.2. | Источники данных: внешние (настройка взаимодействия с серверами служб каталогов, различные типы подключения – AD, LDAP; работа с сертификатами; создание профиля сертификатов, принцип работы); внутренние (работа с локальными хранилищами данных о пользователях и устройствах, особенности использования – сетевые пользователи, разрешенные MAC-адреса, конечные точки; работа с карточкой конечной точки – назначение меток, отправка Change of Authorization (CoA), автоматически формируемые атрибуты, добавление в список разрешенных MAC-адресов.  Словари: системные, псевдословари, пользовательские (предустановленные в комплексе словарей, их использование для настройки доступа по протоколам RADIUS, TACACS; наиболее часто используемые атрибуты) | 3 | 1 | 2 |  |
| 3.3. | Профили оборудования. Словари RADIUS; условия сценариев доступа; разрешения (определение атрибутов для использования устройством при назначении VLAN и ACL механизме работы CoA, настройка параметров для запроса на изменение параметров сеанса аутентификации или авторизации, требования к оборудованию, механизм работы перенаправления, настройка атрибутов для передачи ссылки для переадресации на гостевой портал клиента, запрашивающего доступ к сети).  Сетевое оборудование. Добавление информации об аутентификаторе – особенности создания (конкретное устройство, подсети), алгоритм и пример конфигурации оборудования для взаимодействия с ПК EDO по протоколам RADIUS, TACACS. | 2 | 1 | 1 |  |
| 3.4. | Профили авторизации. Использование предустановленного профиля. Основные настройки: загружаемый ACL, ACL, ACL контроллера точек доступа, Веб-переадресация, VLAN. Типы настроек – Shell, WLC, Nexus, Generic. Перечень доступных параметров для настройки, применимость к оборудованию различных вендоров, описание настраиваемых параметров Наборы команд. Разрешенные протоколы. | 3 | 1 | 2 |  |
| 3.5. | Раздел «Настройки», доступ в сеть. Основные параметры настройки, схема работы TLS, выбор сертификата, настройка протоколов доступа в сеть: PEAP, TTLS, TLS, MD5  Наборы политик.  Доступ в сеть. Обход правил (порядок, правила срабатывания). Использование словарей, атрибутов и значений для разных этапов (правило срабатывания, аутентификация, авторизация). Применение шаблонов условий, примеры настроек типов доступа (по проводной сети, беспроводной, доступ по сертификатам и пр) и различных типов аутентификации (PAP, EAP-MD5, TTLS-PAP, PEAP-EAP-MSCHAPv2 и т.п.). Параметры настройки правила срабатывания, правил аутентификации, правил авторизации – выбор источников данных, действий при отсутствии пользователя или ошибки аутентификации, профиля авторизации.  Доступ на оборудование Обход правил (порядок, правила срабатывания). Использование словарей, атрибутов и значений для разных этапов. Параметры настройки правила срабатывания, правил аутентификации, правил авторизации – выбор источников данных, действий при ошибке аутентификации, профиля авторизации и наборов команд. | 3 | 1 | 2 |  |
| 3.6. | Профилирование Поддерживаемые источники профилирования (RADIUS, DHCP, User-agent), алгоритм работы, настройка источников, использование полученных данных в наборах политик  Гостевой портал. Схема и пример настройки сценария работы гостевого портала. Типы гостевого доступа, гостевые пользователи  События. Отображаемые данные на вкладках: аутентификация, аудит. Фильтрация, экспорт событий | 2 | 1 | 1 |  |
|  | **Всего:** | **22** | **10** | **12** |  |
|  | **Итоговый контроль знаний** | **2** |  | **2** | **Итоговый тест** |
|  | **Итого:** | **24** | **10** | **14** |  |