Министерство образования Пензенской области
Государственное автономное профессиональное образовательное учреждение
Пензенской области
«Пензенский колледж информационных и промышленных технологий (ИТ-колледж)»
(ГАПОУ ПО ПКИПТ)

УТВЕРЖДАЮ
Директор ГАПОУ ПО ПКИПТ
_____А.Н. Фетисов
«__» 11 2019г.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

«Анализ защищенности сетей»

Пенза – 2019

Организация – разработчик: ГАПОУ ПО «Пензенский колледж информационных и промышленных технологий (ИТ-колледж)»

Разработчики: Д.А. Ручкин, преподаватель первой категории

Дополнительная общеразвивающая программа рассмотрена на заседании МЦК профессиональных дисциплин по укрупненной группе специальности 10.00.00 «Информационная безопасность»

Протокол № 3 от 05.11.19 г.

Председатель МЦК _____ А.Ю. Сазонова

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель программы: Курс посвящён одному из защитных механизмов, который относится к категории превентивных, - мониторингу защищённости. В курсе детально рассматриваются основные типы уязвимостей компьютерных систем и сетей, причины их возникновения и методы выявления. Рассматриваются приёмы и инструменты как удалённого, так и локального анализа систем, приводятся примеры использования современных систем управления уязвимостями, представлена информация по методологии анализа защищённости.

Курс содержит сведения, необходимые для эффективного проведения обследования корпоративной сети с точки зрения защищенности. В программе анализируется архитектура и принципы работы сканеров сетевого уровня, в т. ч. методы сбора информации о сети и методы идентификации уязвимостей. Также рассматриваются вопросы внедрения технологии анализа защищенности в корпоративной сети и методология Penetration Testing (Ethical hacking).

Значительная часть курса отведена практической работе с различными средствами поиска уязвимостей, как свободно распространяемыми, так и коммерческими

1.2. Образовательные результаты программы

В результате освоения программы слушатель должен **иметь навыки**:

- размещения средств анализа защищенности в корпоративной сети;
- выявления уязвимостей с использованием различных средств анализа защищенности, в т.ч. Nessus, XSpider, Internet Scanner;
- написания собственных проверок на языке NASL;
- анализа защищенности приложений;
- анализа результатов работы сканеров уязвимостей

В результате освоения программы слушатель должен **знать**:

- архитектуру и принципы работы сканеров сетевого уровня;
- методы сбора информации о сети;
- методы поиска уязвимостей, используемых в сканерах безопасности;
- методологию внедрения механизма анализа защищенности в корпоративной сети.

1.3. Трудоемкость обучения: 36 часов

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Рабочий учебный план

Министерство образования Пензенской области
Государственное автономное профессиональное образовательное учреждение
Пензенской области
«Пензенский колледж информационных и промышленных технологий (ИТ-колледж)»
(ГАПОУ ПО ПКИПТ (ИТ-колледж))

УТВЕРЖДАЮ
Директор ГАПОУ ПО ПКИПТ
_____А.Н. Фетисов
«12» 11 2019 г.

РАБОЧИЙ УЧЕБНЫЙ ПЛАН
дополнительной общеразвивающей программы

«Анализ защищенности сетей»

Категория слушателей

- Системные и сетевые администраторы, ответственные за безопасность компьютерных сетей, эффективную эксплуатацию средств защиты и средств анализа защищенности сетей.
- Администраторы информационной безопасности.
- Эксперты и аналитики по вопросам компьютерной безопасности, ответственные за анализ состояния информационной безопасности и определение требований к защищенности сетевых ресурсов.

Трудоемкость обучения 36 часов
Срок обучения 1 неделя
Форма обучения очно-заочная

№	Наименование модулей	Всего, ак. час	В том числе			Форма контроля
			лекции	практ. занятия	промеж. и итог. контроль	
1	*2*	*3*	*4*	*5*	*6*	*7*
1	Терминология. Методы выявления уязвимостей. Системы анализа защищенности. Сетевые сканеры безопасности.	2	2	0	0	-
2	Методы сбора информации о сети. Идентификация сетевых объектов. Определение топологии сети.	10	5	4	1	Зачет
3	Идентификация статуса порта. Идентификация сервисов и приложений. Идентификация операционных систем. Идентификация уязвимостей по косвенным признакам.	10	5	4	1	Зачет
4	Методы и задачи Passive fingerprinting. Выявление уязвимостей с помощью тестов. Сетевой сканер Nessus.	8	5	2	1	Зачет

5	Язык описания атак NASL. Примеры средств анализа защищенности. Анализ защищенности уровня узла. Методология анализа защищенности. Централизованное управление уязвимостями.	6	3	2	1	Зачет
ИТОГО:		36	20	12	4	

Согласовано

Заместитель директора по работе с социальными партнерами _____ Чистякова Н.В.

Председатель методической цикловой комиссии _____ А.Ю. Сазонова

2.2. Содержание программы

2.2.1. Тематический план дополнительной общеразвивающей программы «Анализ защищенности сетей»

№	Наименование модулей	Всего, ак. час	В том числе			Форма контроля
			лекции	практ. занятия	промеж. и итог. контроль	
1	*2*	*3*	*4*	*5*	*1*	*2*
1	**Терминология. Методы выявления уязвимостей. Системы анализа защищенности. Сетевые сканеры безопасности.**	**2**	**2**	**0**	**0**	**-**
1.1	Понятие уязвимости. Классификация. Источники информации. Архитектура и принципы работы сканеров сетевого уровня. Методы сканирования на уровне сети.	2	2			
2	**Методы сбора информации о сети. Идентификация сетевых объектов. Определение топологии сети.**	**10**	**5**	**4**	**1**	**Зачет**
2.1	Информация, доступная через Интернет. Программа HTTrack. Foot Printing	5	5			
2.2	Использование протокола TCP. Использование протокола IP. Идентификация узлов с помощью протокола ARP. Использование протокола ICMP. Использование протокола UDP. Отслеживание маршрутов. Определение топологии сети за пакетным фильтром.	4		4		
2.3	Зачетная работа	1			1	зачет
3	**Идентификация статуса порта. Идентификация сервисов и приложений. Идентификация операционных систем. Идентификация уязвимостей по косвенным признакам.**	**10**	**5**	**4**	**1**	**Зачет**

3.1	Способы сканирования портов. Простейшие методы определения ОС. Опрос стека TCP/IP. Инструменты. SinFP. Использование протокола ICMP для идентификации ОС.	5	5			
3.2	Сканирование портов TCP. Сканирование портов UDP. Идентификация TCP-служб. Идентификация UDP-служб. Сканирование протоколов.	4		4		
3.3	Зачетная работа	1			1	зачет
4	**Методы и задачи Passive fingerprinting. Выявление уязвимостей с помощью тестов. Сетевой сканер Nessus.**	**8**	**5**	**2**	**1**	**Зачет**
4.1	Анализ сетевого трафика. Анализ запросов от сканируемого узла. «Эксплойты» и их разновидности. Проблема «отказа в обслуживании». Методы анализа результатов тестирования.	5	5			
4.2	Получение, установка и работа со сканером	2		2		
4.3	Зачетная работа	1			1	зачет
5	**Язык описания атак NASL. Примеры средств анализа защищенности. Анализ защищенности уровня узла. Методология анализа защищенности. Централизованное управление уязвимостями.**	**6**	**3**	**2**	**1**	**Зачет**
5.1	Структура сценария. Синтаксис языка. Подключаемые библиотеки. Сетевой сканер XSpider. Программа Internet Scanner. Задачи и инструменты локального сканирования. Контроль целостности. Оценка стойкости паролей. Программа Assuria Auditor.	3	3			
5.2	Написание пользовательских проверок. Инвентаризация информационных активов. Мониторинг состояния защищённости. Устранение уязвимостей. Контроль.	2		2		
5.3	Зачетная работа	1			1	зачет
ИТОГО:		**36**	**12**	**19**	**5**	

2.2.1.1. Содержание дополнительной общеразвивающей программы «Анализ защищенности сетей»

Тема 1 Терминология. Методы выявления уязвимостей. Системы анализа защищенности. Сетевые сканеры безопасности.

Понятие уязвимости. Классификация. Источники информации. Каталог уязвимостей CVE. Основные приёмы выявления уязвимостей. Обзор средств анализа защищенности. Варианты классификации. Примеры.

Архитектура и принципы работы сканеров сетевого уровня. Методы сканирования на уровне сети.

Тема 2 Методы сбора информации о сети. Идентификация сетевых объектов. Определение топологии сети.

Информация, доступная через Интернет. Программа HTTrack. Foot Printing.

Практическая работа Использование протокола TCP. Использование протокола IP.

Идентификация узлов с помощью протокола ARP.

Практическая работа Использование протокола ICMP. Использование протокола UDP.

Практическая работа Отслеживание маршрутов. Определение топологии сети за пакетным фильтром.

Тема 3 Идентификация статуса порта. Идентификация сервисов и приложений. Идентификация операционных систем. Идентификация уязвимостей по косвенным признакам.

Способы сканирования портов.

Простейшие методы определения ОС. Опрос стека TCP/IP. Инструменты. SinFP.

Использование протокола ICMP для идентификации ОС.

Методы идентификации уязвимостей по косвенным признакам. Баннерные проверки.

Сетевые сервисы как объект сканирования. «Локальные» проверки. Сбор информации о Windows-системах.

Практическая работа Сканирование портов TCP. Сканирование портов UDP.

Практическая работа Идентификация TCP-служб. Идентификация UDP-служб.

Сканирование протоколов.

Тема 4 Методы и задачи Passive fingerprinting. Выявление уязвимостей с помощью тестов. Сетевой сканер Nessus.

Анализ сетевого трафика. Анализ запросов от сканируемого узла.

«Эксплойты» и их разновидности. Проблема «отказа в обслуживании». Методы анализа результатов тестирования.

Обзор возможностей. Архитектура сканера.

Практическая работа Получение, установка и работа со сканером.

Тема 5 Язык описания атак NASL. Примеры средств анализа защищенности. Анализ защищенности уровня узла. Методология анализа защищенности. Централизованное управление уязвимостями.

Структура сценария. Синтаксис языка. Подключаемые библиотеки. Сетевой сканер XSpider.

Программа Internet Scanner.

Задачи и инструменты локального сканирования. Контроль целостности. Оценка стойкости паролей. Программа Assuria Auditor.

Ethical hacking (Penetration Testing). Разновидности Penetration Testing. Схема Penetration Testing.

Практическая работа Написание пользовательских проверок.

Практическая работа Инвентаризация информационных активов. Мониторинг состояния защищённости. Устранение уязвимостей. Контроль.

III. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по дополнительной общеразвивающей программе: Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по теоретическому обучению: обеспечивается педагогическими кадрами, имеющими высшее образование, соответствующее профилю преподаваемой дисциплины, а также имеющими документ на право проведения регионального чемпионата Ворлдскиллс Россия, оценивания демонстрационного экзамена по стандартам Ворлдскиллс Россия. Требования к квалификации педагогических кадров, осуществляющих руководство практикой мастера производственного обучения и преподаватели, имеющие высшее техническое профессиональное образование по профилю подготовки с квалификацией первой и высшей категории.

3.2. Информационно – методические условия реализации программы

Наименование учебной дисциплины	Перечень литератур, Интернет-ресурсов
«Анализ защищенности сетей»	– печатные раздаточные материалы для слушателей – электронные ресурсы – официальный сайт оператора международного некоммерческого движения WorldSkills International - Союз «Молодые профессионалы (Ворлдскиллс Россия)» (электронный ресурс) режим доступа: https://worldskills.ru; – единая система актуальных требований Ворлдскиллс (электронный ресурс) режим доступа: https://esat.worldskills.ru

3.3. Материально-технические условия реализации программы

Наименование аудиторий	Вид занятий	Наименование оборудования, программного обеспечения
Мастерская «Корпоративная защита от внутренних угроз информационной безопасности»	все занятия	Компьютеры и программное обеспечение по количеству слушателей мультимедийный проектор, экран, доска, флипчарт Оборудование, оснащение рабочих мест, инструменты и расходные материалы – в соответствии с инфраструктурным листом по компетенции Ворлдскиллс

IV. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

4.1. Контрольно – измерительный материал по дополнительной общеразвивающей программе «Анализ защищенности сетей»

Выполнение зачетных и практических работ, а также умение сформулировать ответы на вопросы:

- Каким способом можно провести интеграцию IDS/IPS в единую систему?
- Приведите примеры корреляции данных, полученных из различных источников, для обнаружения атак.
- Перечислите угрозы безопасности по отношению к беспроводным сетям.
- В чем заключается несанкционированное использование беспроводных устройств?
- Какие задачи решаются в ходе мониторинга безопасности беспроводной сети?
- Каковы особенности обнаружения атак в беспроводных сетях?
- Сформулируйте перечень атак, специфичных для беспроводных сетей.
- Приведите примеры систем обнаружения атак в беспроводных сетях.
- Опишите достоинства и недостатки метода обнаружения «злоупотреблений».
- В чем заключается алгоритм обнаружения атак метода обнаружения аномалий? Назовите его достоинства и недостатки.
- Перечислите составляющие технологии обнаружения атак.
- Опишите архитектуру сетевой IDS, ее достоинства и недостатки.
- В чем заключается специфика обнаружения атак на уровне узла? Опишите ее
- достоинства и недостатки.
- Как использовать особенности архитектуры Network Flow для обнаружения атак?
- Чем вызвана необходимость централизованного управления уязвимостями?
- Раскройте суть инвентаризации информационных активов.
- Перечислите задачи и способы мониторинга состояния защищенности.
- К чему сводится устранение уязвимостей?
- Какими способами осуществляется контроль правильности устранения уязвимостей?
- Обоснуйте необходимость методологии анализа защищенности.
- Что входит в понятие «Penetration Testing»?
- Перечислите особенности Penetration Testing изнутри и снаружи.
- Перечислите этапы Penetration Testing. Дайте характеристику каждому этапу.
- По каким причинам применение методологии Penetration Testing может быть ограничено?
- Перечислите задачи локального сканирования. Дайте характеристику каждой
- задаче.
- Каковы особенности архитектуры сканеров уровня узла?
- Каким образом осуществляется идентификация уязвимостей?
- Перечислите источники данных для сканеров уровня узла.
- Что такое сканер Assuria Auditor?