

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 02.02.2021 10:00:30
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе

« 1 » 02 2018 г.



ОСНОВЫ МОНИТОРИНГА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Методические указания к самостоятельной работе для
студентов укрупненной группы специальностей и направлений
подготовки 10.00.00 «Информационная безопасность»

Курск 2018

УДК 004

Составитель: М.О. Таныгин

Рецензент

Кандидат технических наук, доцент кафедры
«Информационная безопасность» А.Л. Марухленко

Основы мониторинга безопасности информационных систем [Текст]: методические указания к самостоятельной работе/ Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2018. – 10 с. – Библиогр.: с. 10.

Содержат сведения по вопросам самостоятельной работы на протяжении изучения дисциплины. Указывается порядок выполнения самостоятельных работ, содержание работы.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать *1.02.18* Формат 60x84 1/16.
Усл.печ. л. 0,58. Уч.-изд. л. 0,53. Тираж 100 экз. Заказ. Бесплатно. *ИЧО*
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

Введение	4
Цель работы.....	4
Основные определения	4
Содержание работы	5
Тема самостоятельной работы 1: «Введение. Анализ современного состояния сетевой безопасности»	5
Тема самостоятельной работы 2: «Назначение сетевых пакетов и их структура».....	5
Тема самостоятельной работы 3: «Анализ сетевого трафика»	5
Тема самостоятельной работы 4: «Программные утилиты для мониторинга сети»	5
Тема самостоятельной работы 5: «Контроль трафика с помощью виртуальных частных сетей».....	5
Тема самостоятельной работы 6: «Угрозы информации в беспроводных сетях»	6
Тема самостоятельной работы 7: «Получение информации от сетевых сервисов»	6
Тема самостоятельной работы 8: «Системы мониторинга сетей связи».....	6
Тема самостоятельной работы 9: «Системы обнаружения вторжений. Автоматическая валидация уязвимостей с помощью нечетких множеств и нейронных сетей»	7
Описание курса и методические рекомендации	7
Вопросы для самопроверки	8
Список информационных источников	10

ВВЕДЕНИЕ

Самостоятельная работа важна для каждой дисциплины, так как позволяет на более глубоком уровне усвоить студентам основы мониторинга безопасности информационных систем.

В настоящее время актуальность безопасности ИС резко возросла. Это связано с увеличением зависимости организаций от информации и ИС. Возросла уязвимость ИС за счет сложности элементов ИС, появления новых технологий передачи и хранения данных, увеличения объема ПО.

ЦЕЛЬ РАБОТЫ

Цель самостоятельно работы – получить более полные знания по изучаемой дисциплине.

ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

Информация – сведения о каких-либо событиях, процессах, фактах или предметах;

Информационная система - система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию;

Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации.

СОДЕРЖАНИЕ РАБОТЫ

Тема самостоятельной работы 1:

«Введение. Анализ современного состояния сетевой безопасности»

Эволюция угроз. Сдвиги в потребительском восприятии угроз сетевой безопасности. Актуальность технологий предотвращения утечек. Шифрование и многофакторная аутентификация как наиболее эффективные методы защиты. Амплификация. BGP и утечки информации.

Тема самостоятельной работы 2:

«Назначение сетевых пакетов и их структура»

Необходимость упаковки информации. Заголовки пакетов. Формат данных в пакете. Методы управления обменом данными. Управление обменом данными в системах с различной топологией. Адресация пакетов.

Тема самостоятельной работы 3:

«Анализ сетевого трафика»

АРМ-решения. Признаки комплексного подхода, а анализу трафика. Методы анализа сетевого трафика. Парадигмы сетевого мониторинга. Решения в области анализа трафика.

Тема самостоятельной работы 4:

«Программные утилиты для мониторинга сети»

Назначение, состав, функционал, особенности лицензирования средств мониторинга сети. Состояние рынка средств мониторинга сети. Виды собираемой информации в сетевых мониторах.

Тема самостоятельной работы 5:

«Контроль трафика с помощью виртуальных частных сетей»

Определение виртуальных частных сетей. Принцип действия VPN. Создание туннеля. Процесс инкапсуляции. Туннелирование на уровне 2. Туннелирование IPSec. Поддержка VPN

операционными системами. VPN и коммутируемые сети: преимущества и недостатки. Сценарии VPN. VPN удаленного доступа. Виртуальные частные экстрасети. Протоколы туннелирования. Технология PPTP. Технология L2F. Технология L2TP. Режимы туннелирования. Протоколы шифрования.

Тема самостоятельной работы 6:

«Угрозы информации в беспроводных сетях»

Особенности беспроводных сетей. Периметр беспроводных сетей. Риски для информации в беспроводных сетях. Уязвимости устройств беспроводной связи. Ошибки конфигурации точек беспроводного доступа. Ошибки конфигурации клиентов беспроводных сетей. Уязвимость криптографических протоколов беспроводных сетей. Утечки информации в беспроводных сетях. Физические особенности среды, влияющие на безопасность.

Тема самостоятельной работы 7:

«Получение информации от сетевых сервисов»

Сканирование портов. Получение информации от DNS-сервера. Перебор имен. Перебор обратных записей. Получение информации с использованием SNMP. Получение информации с использованием NetBIOS. Работа с электронной почтой. Анализ баннеров. Получение информации от NTP-сервера.

Тема самостоятельной работы 8:

«Системы мониторинга сетей связи»

Контроль точек взаимодействия сетей. Управление сетью. Возможности современных систем контроля сетей связи. учёт разговорного трафика. Функциональные возможности систем мониторинга сетей связи. Анализ качества функционирования сети. Анализ разговорной нагрузки по каналам.

Тема самостоятельной работы 9:

«Системы обнаружения вторжений. Автоматическая валидация уязвимостей с помощью нечетких множеств и нейронных сетей»

Проверка конфигураций и поиск уязвимости ИС. Принципы работы систем обнаружения вторжений. Состав системы обнаружения вторжений. Классификация систем обнаружения вторжений. Размещение компонентов системы обнаружения вторжений в сети. Постановка задачи нечеткой классификации уязвимостей при использовании нейросетей. Принципы работы систем обнаружения вторжений на основе нейросетей.

Описание курса и методические рекомендации

Во время освоения курса «Основы мониторинга безопасности инфокоммуникационных систем и сетей Основы мониторинга безопасности информационных систем» студент осваивает основные методы и технические средства контроля информационных потоков в телекоммуникационных сетях различного назначения.

Обилие объектов мониторинга порождает широкую номенклатуру программных и аппаратных средств слежения, ознакомиться со всеми в рамках лекционного курса, лабораторных и практических занятий не представляется возможным. Поэтому основным наполнением самостоятельной работы видится, помимо подготовки к аудиторным занятиям, изучение именно технических средств, их установка и ознакомительный запуск. Тем более что многие из них размещены в свободном доступе, бесплатны или условно бесплатны. Это касается в основном программных мониторов сетевой активности и сканеров уязвимостей, тогда как в сетях голосовой связи подобные средства представлены в основном дорогостоящими аппаратными решениями.

Следует отметить, что в большинстве литературных источников даются фундаментальные основы мониторинга безопасности, тогда как сама проблемная область является достаточно быстро меняющейся. Методы, которые были актуальны

5 – 10 лет назад сейчас уже неактуальны, технологии, которые в них задействованы, перестают поддерживаться производителям. Поэтому актуальные материалы целесообразно искать на специализированных ресурсах в сети интернет, таких как, например, <https://habrahabr.ru/> в разделах «информационная безопасность», «сети ЭВМ», «администрирование». Также рекомендуется обращаться в ежегодным и ежеквартальным обзорам компаний, занимающихся проблемой сетевой безопасности. Классическим примером может быть сайт компании Cisco и их корпоративный блог. Также следует отметить сайт Лаборатории Касперского (<https://www.kaspersky.ru/blog/>) и компании Код Безопасности (www.securitycode.ru/documents/analytics)

Вопросы для самопроверки

Тема 1. Введение. Анализ современного состояния сетевой безопасности.

1. Эволюция угроз сетевому взаимодействию
2. Основные тенденции в развитии средств противодействия сетевым угрозам
3. Понятие амплификации.
4. Дайте критерии для оценки эффективности современных средств мониторинга безопасности сетевых ресурсов.
5. Охарактеризуйте проблему утечек информации

Тема 2. Программные утилиты для мониторинга сети.

1. Какие ресурсы могут подлежать контролю при сетевом взаимодействии?
2. Существуют ли стандартные средства операционных систем, позволяющие анализировать угрозы информационной безопасности в сети?
3. Какую информацию агрегируют сетевые мониторы?
4. Назовите бесплатные кроссплатформанные средства сбора информации о сетевом взаимодействии

Тема 3. Контроль трафика с помощью виртуальных частных сетей.

1. Принцип действия VPN.

2. Как происходит создание туннеля?
3. Что такое процесс инкапсуляции и как он происходит?
4. Уровни тунеллирования.
5. Как поддерживается VPN операционными системами?
6. Назовите преимущества и недостатки использования

VPN в коммутируемых сетях

7. Как можно использовать VPN для контроля сетевой активности пользователей?
8. Назовите основные технологии VPN.

Тема 4. Системы обнаружения вторжений. Автоматическая валидация уязвимостей с помощью нечетких множеств и нейронных сетей.

1. Принципы работы систем обнаружения вторжений.
2. Состав системы обнаружения вторжений.
3. Классификация систем обнаружения вторжений.
4. Где эксперты рекомендуют размещать функциональные элементы систем обнаружения вторжений и почему?
5. Что позволяет использование нейросетевого подхода и нечёткой логики в системах обнаружения вторжений?

Список информационных источников

1) Громов Юрий Юрьевич. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. - ТНТ, 2013. - 384 с.

2) Лукьянюк, Сергей Георгиевич. Теория электрической связи. Помехоустойчивость и эффективность систем связи [Текст] : учебное пособие / С. Г. Лукьянюк, А. М. Потапенко. - ЮЗГУ, 2013. - 263 с.

3) Олифер, Виктор Григорьевич. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - Санкт-Петербург : Питер, 2015. - 943 с.

1) Гордиенко В. Н. Многоканальные телекоммуникационные системы [Текст] : учебник / В. Н. Гордиенко, М. С. Тверецкий. - Горячая линия - Телеком, 2007. - 416 с.

2) Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие / М. А. Иванов, И. Чугунков. - Москва : МИФИ, 2012. - 400 с.

3) Крук, Борис Иванович. Телекоммуникационные системы и сети [Текст] : учебное пособие / Б. И. Крук, В. Н. Попантопуло, В. П. Шувалов ; под ред. В. П. Шувалова. - 4-е изд., испр. и доп. - Москва : Горячая линия - Телеком. Т. 1: Современные технологии. - 2013. - 620 с.

4) Крухмалев В. В. Цифровые системы передачи [Текст] : учебное пособие / В. В. Крухмалев, В. Н. Гордиенко, А. Д. Моченов. - Горячая линия - Телеком, 2007. - 352 с.

5) Онокой, Людмила Сергеевна. Компьютерные технологии в науке и образовании [Текст]: учебное пособие / Л. С. Онокой, В. М. Титов. - Москва: ФОРУМ : ИНФРА-М, 2014. — 223 с.

6) Скабцов Н. Аудит безопасности информационных систем. — СПб.: Питер, 2018. — 272 с.: ил.