МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__» _____ 2017 г.

ОСНОВЫ МОНИТОРИНГА БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ

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

Курск 2017

УДК 621.(076.1)

Составитель: М.О. Таныгин

Рецензент

Кандидат технических наук, доцент кафедры
«Информационная безопасность» И.В. Калуцкий

Основы мониторинга безопасности инфокоммуникационных систем и сетей [Текст] : методические указания для самостоятельной работы/ Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2017. – 10 с. – Библиогр.: с. 10.

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

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 24.11.17 Формат 60x84 1/16.
Усл.печ. л. 0,58. Уч.-изд. л. 0,53. Тираж 100 экз. Заказ. Бесплатно 2147
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание курса

№ п/п	Раздел (тема) дисциплины	Краткое содержание
	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
	Назначение сетевых пакетов и их структура	Необходимость упаковки информации. Заголовки пактов. Формат данных в пакте. Методы управления обменом данными. Управление обменом данными в системах с различной топологией. Адресация пакетов.
	Анализ сетевого трафика	APM-решения. Признаки комплексного подхода а анализу трафика. Методы анализа сетевого трафика. Парадигмы сетевого мониторинга. Решения в области анализа трафика.
	Программные утилиты для мониторинга сети	Назначение, состав, функционал, особенности лицензирования средств мониторинга сети. Состояние рынка средств мониторинга сети. Виды собираемой информации в сетевых мониторах
	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 тунеллирования. Протоколы

		шифрования.
	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
	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.
	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.
	Системы обнаружения вторжений. Автоматическая валидация уязвимостей с помощью нечетких	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

	множеств и нейронных сетей	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» студент осваивает основные методы и технические средства контроля информационных потоков в телекоммуникационных сетях различного назначения.

Обилие объектов мониторинга порождет широкую номенклатуру программных и аппаратных средств слежения, ознакомиться со всеми в рамках лекционного курса, лабораторных и практических занятий не представляется возможным. Поэтому основным наполеннием самостоятельной работы видится, помимо подготовки к аудиторным занятиям, изучение именно технических средств, их установка и ознакомительный запуск. Тем более что многие из них размещны 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. Назначение сетевых пакетов и их структура.

1. Опишите структуру сетевого пакета.
2. Как сетевые устройства воспринимают данные в служебных полях пакета?
3. Какая адресная информация содержится в заголовках пакетов?
4. Как топология сети влияет на работу маршрутизаторов и оконечных устройств?

Тема 3. Анализ сетевого трафика.

1. Перечислите проблемы, возникающие при анализе сетевого трафика?
2. Перечислите парадигмы сетевого мониторинга
3. Какие существуют методы анализа сетевого трафика?
4. Назовите существующие на рынке решения в области анализа сетевого трафика

Тема 4. 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 кросплатформанные средства сбора информации о сетевом взаимодействии

Тема 5. 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 6. Угрозы информации в беспроводных сетях.

1. Назовите особенности беспроводных сетей, определяющие специфические для них угрозы информации
2. Какие существуют риски при использовании беспроводных сетей?
3. Назовите уязвимости криптографических протоколов, используемых в беспроводных сетях.
4. Назовите физические особенности среды распространения сигнала, влияющие на безопасность беспроводных сетей

Тема 7. Получение информации от сетевых сервисов.

1. Какую информацию можно получить при сканировании портов?
2. Какую информацию можно получить штатными средствами от DNS-сервера?
3. Как выделить критическую информацию из данных, передаваемых по протоколу SNMP?
4. Как во время аудита безопасности происходит получение информации от NTP-сервера

Тема 8. Системы мониторинга сетей связи.

1. Для чего необходим контроль точек взаимодействия сетей?

2. Перечислите возможности современных систем контроля сетей связи.

3. Что позволяет анализ качества функционирования сети?

4. Для чего нужен анализ разговорной нагрузки в сетях голосовых данных?

Тема 9. 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?

Библиография

Основная литература

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.

Дополнительная литература

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. Попантонопуло, 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.

Перечень ресурсов информационно-телекоммуникационной сети Интернет

1) Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/

2) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/

3) Корпорация Microsoft [официальный сайт]. Режим доступа: http://microsoft.com/

4) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru

5) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru

6) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/

7) База данных "Патенты России"

8) Компания Cisco [официальный сайт] https://www.cisco.com/c/ru_ru/index.html

9) ЗАО «Лаборатория Касперского» [корпоратвный блог] https://www.kaspersky.ru/blog/
10) Аналитический раздел комании «Код Безопасности» https://www.securitycode.ru/documents/analytics/
11) Сайт для IT-специалистов www/habrahabr.ru
Методические