



Автономная некоммерческая организация
дополнительного профессионального образования
(АНО ДПО «Инфосфера»)
Центр профессиональной подготовки
ИНСТИТУТ ПРОГРАММНЫХ СИСТЕМ

Рабочая программа дисциплины
«Сетевая безопасность»

Разработал:
преподаватель ИПС
АНО ДПО «Инфосфера»
А.А. Ильин

Йошкар-Ола, 2017

Пояснительная записка

Курс «Сетевая безопасность» рассматривает наиболее широко используемые протоколы сетевой безопасности прикладного и сетевого уровней, вопросы обеспечения безопасности при подключении корпоративной сети к интернету. Основное внимание уделяется классификации межсетевых экранов, систем обнаружения проникновений, обеспечению безопасности сервисов DNS и web-серверов, классификации и способам борьбы с вредоносным программным обеспечением.

Планируемые результаты обучения

Осуществляется предварительная самостоятельная или под руководством разработка алгоритмов с использованием графических средств (блок-схемы, UML-диаграммы и др.). Не требуется взаимодействие с другими программистами, системным аналитиком и архитектором программного обеспечения. Осуществляется решение типовых задач. Полученные результаты представляются руководителю разработки программного обеспечения.

Выполняются самостоятельная разработка процедур сборки модулей и компонент программного обеспечения и верификация выпусков программного продукта. Производится разработка процедур развертывания и обновления программного обеспечения, процедур миграции и преобразования (конвертации) данных и программных интерфейсов с использованием выбранных программных средств, технологий создания открытых систем. Осуществляется решение различных типов задач проектирования программных комплексов различной сложности, выбор способов реализации взаимодействия программных компонент/модулей. Требуется взаимодействие с программистами-разработчиками модулей, архитектором программного обеспечения. Полученные результаты представляются руководителю разработки программного обеспечения.

В процессе интеграции программных модулей и компонент и верификации выпусков программного продукта осуществляется сборка модулей и компонент программного обеспечения, производится интеграция с внешней средой. Обеспечивается согласованное функционирование и требуемый уровень качества.

Проведение интеграции программных модулей и компонент и верификация выпусков программного продукта предполагают определение задач программной интеграции, распределение задач между подчиненными, обеспечение взаимодействия подчиненных сотрудников.

Программист несет ответственность за результат выполнения работ на уровне группы программистов. В процессе интеграции требуется взаимодействие с архитектором программного обеспечения. Полученные результаты представляются руководителю разработки программного обеспечения.

Учебно-тематический план

№	Название темы	Аудиторные занятия
---	---------------	--------------------

		Лекции	Практика	Всего
1	Безопасное сетевое взаимодействие	8	8	16
2	Классификация и определение политик межсетевых экранов (Firewall)	6	4	10
3	Классификация и способы борьбы с вредоносным программным обеспечением	4	6	10
4	Системы обнаружения проникновений (Intrusion Detection Systems - IDS)	4	4	8
5	Принципы безопасного развертывания сервисов DNS	4	2	6
6	Обеспечения безопасности web-серверов	8	10	18
		36	36	72

Содержание курса

1. Безопасное сетевое взаимодействие

Протокол Kerberos. Аутентификационный сервис Kerberos. Требования, которым должен удовлетворять Kerberos, описание протокола Kerberos, функций AS и TGS, структура билета (ticket) и аутентификатора. Вводится понятие области (realm) Kerberos. Описание протокола версии 5.

Протокол TLS/SSL. Описание протокола Записи и протокола Рукопожатия, вводится понятие "состояние соединения". Описание используемых криптографических операций и PRF. Расширения, которые могут использоваться для добавления функциональностей в протокол TLS.

Протокол SSH. Описание протокола удаленного безопасного входа SSH. Определяется понятие ключа хоста, описание алгоритма транспортного уровня, способа аутентификации сервера и вычисления разделяемого секрета. Описание методов аутентификации пользователя и механизма канала, обеспечивающего интерактивные входные сессии, удаленное выполнение команд, перенаправление TCP/IP-соединений, перенаправление X11-соединений.

Протоколы безопасности на уровне IP. Рассматривается архитектура семейства протоколов IPsec. Рассматриваются протоколы безопасности - Authentication Header (AH) и Encapsulating Security Payload (ESP), Безопасные Ассоциации (SA), управление ключом - ручное и автоматическое (Internet Key Exchange - IKE), а также алгоритмы, используемые для аутентификации участников и шифрования трафика. Рассматривается Протокол Управления Ключом (ISAKMP), который определяет общие процедуры и форматы пакетов для ведения переговоров об установлении, изменении и удалении SA. В качестве протокола аутентификации и обмена ключа рассмотрен протокол IKE.

2. Классификация и определение политик межсетевых экранов (Firewall)

Классификация межсетевых экранов. Исследуются существующие технологии межсетевых экранов: пакетные фильтры, stateful inspection firewall'ы, прокси прикладного уровня. Рассматривается сервис NAT. Приводятся примеры использования firewall'ов различного типа: выделенные прокси серверы, host-based firewall'ы, персональные firewall'ы.

Различные типы окружений firewall'a. Рассматриваются различные типы окружений, в которых может функционировать firewall. Приведены основные принципы построения окружения firewall'a. Дается определение DMZ сети. Исследуются различные топологии DMZ сетей с использованием firewall'ов разного типа. Разбирается взаимное расположение конечных точек VPN и firewall'ов. Вводятся понятия интранет, экстранет. Задаются принципы создания политики firewall'a.

Пример пакетных фильтров в ОС FreeBSD 6.0. Рассматриваются пакетные фильтры, реализованные в ОС FreeBSD 6.0: IPF и IPFW. Приводится синтаксис каждого из этих пакетных фильтров и возможности поддержки состояния TCP соединения в них. Приводится порядок прохождения пакета через правила пакетного фильтра. Изучается применение функции трансляции сетевых адресов (NAT). Приведены примеры набора правил в IPF и IPFW.

3. Классификация и способы борьбы с вредоносным программным обеспечением

Классификация вредоносного программного обеспечения: классические вирусы, троянские кони, сетевые черви, хакерские утилиты. Способы обнаружения, идентификации и обезвреживания вредоносного ПО. Принципы работы и классификация антивирусного программного обеспечения.

4. Системы обнаружения проникновений (Intrusion Detection Systems)

Определение понятия Intrusion Detection Systems (IDS). Рассматриваются причины, по которым следует использовать IDS. Приводятся различные подходы к классификации IDS. Сравниваются возможности network-based, host-based и application-based IDS. Оцениваются преимущества и недостатки IDS, основанных на определении злоупотреблений и на определении аномалий. Перечисляются возможные ответные действия IDS.

Дополнительные инструментальные средства. Системы анализа и оценки уязвимостей и проверки целостности файлов. Рассматривается еще одна смежная IDS технология - создание Honey Pot и Padded Cell. Приводятся различные способы развертывания IDS разного типа. Исследуются возможные комбинации использования network-based и host-based IDS. Даются способы обработки выходной информации IDS. Перечисляются типы компьютерных атак, обычно определяемых IDS.

5. Принципы безопасного развертывания сервисов DNS

Свойства инфраструктуры DNS. Основное назначение сервисов DNS, компоненты DNS, такие, как зонный файл, name сервера и resolver'ы. Вводятся различные типы DNS транзакций: запрос / ответ DNS, зонная пересылка, динамические обновления, DNS NOTIFY. Исследуются возможные угрозы сервисам и компонентам DNS. Обсуждается понятие безопасности для сервисов и компонентов DNS. Рассматриваются транзакции DNS и угрозы и цели безопасности для различных типов транзакций. Описывается создание безопасного окружения для сервисов DNS: безопасность платформы, безопасность ПО DNS, управление содержимым зонного файла. Приводятся подходы к обеспечению защиты на основе спецификации TSIG. Рассматривается способ, которым DNSSEC обеспечивает защиту транзакций DNS Query/Response с помощью аутентификации источника,

проверки целостности данных и аутентифицированного отказа при отсутствии запрошенных данных. Описываются механизмы, используемые DNSSEC, операции, с помощью которых эти механизмы реализуются, и способы обеспечения безопасности этих операций. Задаются принципы безопасного развертывания DNSSEC.

6. Обеспечения безопасности web-серверов

Причины уязвимости web-сервера. Рассматриваются проблемы безопасности, связанные с web-серверами. Обсуждаются проблемы, связанные с безопасностью ОС, на которой выполняется ПО web-сервера. Изучаются альтернативные платформы для web-сервера. Приводится способ безопасного инсталлирования ПО web-сервера. Исследуется управление доступом на уровне ОС для приложения web-сервера.

Безопасность web-одержимого. Рассматриваются принципы обеспечения безопасности содержимого web-сервера. Перечислены различные технологии создания активного содержимого на стороне клиента и сравнивается создаваемая ими степень риска. Изучаются различные технологии создания динамических страниц на стороне сервера и связанные с ними уязвимости.

Технологии аутентификации и шифрования. Рассматриваются существующие технологии аутентификации и шифрования в web: BASIC аутентификация, DIGEST аутентификация, TLS/SSL аутентификация.

Firewall прикладного уровня для web ModSecurity: понятие регулярных выражений, основные возможности конфигурирования, способы задания правил (rules), действий (actions). Дается решение основных проблем безопасности. Приводится примерная минимальная конфигурация.

Безопасная сетевая инфраструктура для web-сервера. Топология сети, использование firewall'ов, сетевых коммутаторов и концентраторов, IDS. Формулируются принципы администрирования web-сервера: создание логов, процедуры создания backup web-сервера, восстановление при компрометации безопасности, тестирование безопасности и удаленное администрирование web-сервера.

Пособия по изучению курса

1. Мельников В.П. Информационная безопасность: 3е издание – М: Издательский центр «Академия», 2008
2. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие – СПб: Питер, 2008
3. Мельников В.П. Информационная безопасность и защита информации: учебное пособие – М: Издательский центр «Академия», 2007
4. Галатенко В.А. Основы информационной безопасности: курс лекций - М: Интернет – Университет Информационных технологий, 2006
5. Филин С.А. Информационная безопасность: учебное пособие – М: Альфа-Пресс, 2006
6. Ярочкин В.И., Бузанова Я.В. Теория безопасности – М: Академический проект, 2005

7. Байбурин В.Б., Бровков М.Б., Пластун И.Л. Введение в защиту информации: учебное пособие – М: Инфра-М, 2004
8. Галатенко В.А. Стандарты информационной безопасности – М: ИНТУИТ.РУ, 2004
9. Мельников В.В. Безопасность информации в автоматизированных системах – М: Финансы и статистика, 2003
10. Приходько А.Я. Информационная безопасность в событиях и фактах – Б.м.: СИНТЕГ, 2001
11. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: учебное пособие – М: Инфра-М, 2001
12. Ярочкин В.И. Информационная безопасность: учебное пособие – М: Международные отношения, 2000
13. Устинов Г.Н. Основы информационной безопасности систем передачи данных: учебное пособие – Б.м. СИНТЕГ, 2000