ТиП БИТКС

10 семестр

Темы

1. Мультимедийная подсистема IP (IMS). Назначение. Построение сетей NGN на базе IMS. Архитектура IMS. Состав, функции оборудования. Протоколы. Механизмы обеспечения безопасности в сетях на базе IMS.
2. Сети доступа. Определение. Классификация. Основные технологии сетей доступа (xDSL, PON, Ethernet, Wi-Fi, FTTx и пр.). Эталонная модель сети доступа. Состав оборудования и его функции для различных технологий.
3. Особенности построения сетей доступа. Узлы сети доступа, состав оборудования. Типовые системно-сетевые решения. Примеры архитектуры.
4. Транспортные сети IP/MPLS.
5. Спутниковые системы связи. Навигационные спутниковые системы. Принципы определения местоположения.
6. Транспортные сети IP/MPLS.
7. QoS

Темы

1. Комплексный подход к обеспечению защиты сетей связи. Технологии аутентификации
2. Аутентификация в открытых системах
   - Подсистема аутентификации
   - Аутентификация клиент-сервер (двухзвенная, трехзвенная с имперсонализацией, без имперсонализации)
   - Аутентификация в однородных и гетерогенных системах
   - Типовые модели аутентификации
   - Аппаратные средства аутентификации в сетевой среде
   - Методы аутентификации
   - Протоколы аутентификации (PAP, запрос-ответ, RADIUS, TACACS, EAP, KERBEROS и пр.)
   - Серверы аутентификации и поддерживаемые службы аутентификации
3. Межсетевые экраны
4. Определение виртуальных частных сетей, цели и задачи. Туннелирование в VPN (защищенные каналы, частные каналы, промежуточные каналы). Схема VPN. Политики безопасности VPN. Протоколы VPN.
5. Защита на канальном и сеансовом уровнях
6. Обеспечение защиты на прикладном уровне.

Практическая работа 1:

Исследование сетевых приложений, запущенных на локальном компьютере

- Запустить на компьютере побольше различных сетевых приложений. Если вы в Windows, запустите пакет программ Denver. Запустите Mozill'у и откройте несколько веб-страничек в различных вкладках.
- Выполнить анализ, какие приложения у нас запущены, какие они используют порты и т.п. Откройте командное окно и выполните команду «netstat -anb» для Windows и «netstat -46anep» для Linux. На экране начнет появляться список активных подключений и прослушиваемых портов

Ответьте на вопросы:

- Найдите пакеты, соответствующие тройному рукопожатию TCP (1 – SYN, 2 – SYN и ACK, 3 – ACK)
- Запущен ли у вас на компьютере веб-сервер (его можно узнать, например, по стандартному номеру порта). Какие порты прослушивает данный процесс?
- Найдите все соединения браузера. Укажите IP-адреса и порты серверов, к которым он подключился, а также порты соответствующих подключений на локальном компьютере.
- Запущен ли у вас на компьютере почтовый SMTP-сервер (его тоже можно узнать по стандартному номеру порта).
- Запущен ли у вас на компьютере DNS-сервер? Какие интерфейсы он прослушивает?

Как оформить

- оформите информацию об активных подключениях и прослушиваемых портах в виде таблиц (не более 5 строчек в каждой)
- **Срок выполнения: 01.03.2016**

Поддерживаемые TCP соединения			
Локальный порт	**Процесс**	**Удаленный IP-адрес**	**Удаленный порт**
1183	opera.exe	87.250.251.63	80
1191	opera.exe	64.233.183.127	80
…	…	…	
…	…	…	
…	…	…	
…	…	…	
…	…	…	
…	…	…	

Открытые порты и соответствующие TCP серверы		
Порт	**Интерфейс**	**Процесс**
135	0.0.0.0 - все	svchost.exe
445	0.0.0.0 - все	Система
…	…	…
…	…	…
…	…	…
…	…	…
…	…	…
…	…	…

Открытые UDP-порты		
Порт	**Интерфейс**	**Процесс**
500	0.0.0.0 - все	lsass.exe
1038	0.0.0.0 - все	TrafSvc.exe
…	…	…
…	…	…
…	…	…
…	…	…
…	…	…
…	…	…

Темы докладов по ТиПБТКС

Тема
Протокол SSL
Протокол TLS
GRE — протокол туннелирования сетевых пакетов без шифрования.
Облачная архитектура. Механизмы обеспечения безопасности.
Технология Li-Fi
Спецификация GS NFV-SEC 004 . Безопасность.
IPSEC — позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов.
Протоколы Telnet, SSH.
Протокол SNMP.
Аутентификация в открытых системах. Аутентификация клиент-сервер
Сети 5G
Аппаратные средства аутентификации в сетевой среде
Сенсорные сети
Протоколы аутентификации (PAP, запрос-ответ, RADIUS, TACACS, EAP, KERBEROS и пр.)
Межсетевые экраны. Функции межсетевых экранов. Типы межсетевых экранов. Схемы подключения межсетевых экранов
Экранирующие концентраторы, пакетные фильтры, шлюзы сеансового уровня, прикладного уровня, экспертного уровня, персональные МЭ.
Определение виртуальных частных сетей, цели и задачи. Принципы. Туннелирование в VPN (защищенные каналы, частные каналы, промежуточные каналы)
Принципы и методы обеспечения безопасности Telegram
Протокол RSVP
Организация VPN в сетях IP/|MPLS
Система управления сетями связи. Концепция TMN. OSS/BSS.
Технология DPI.
Биометрические системы аутентификации.
Самоорганизующиеся сети
Программно-определяемые сети.