

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет прикладной математики и кибернетики
Кафедра защиты информации и криптографии

Д.Н. Колегов

**ЛАБОРАТОРНЫЙ ПРАКТИКУМ
ПО ОСНОВАМ ПОСТРОЕНИЯ
ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ
СЕТЕЙ**

Томск
2013

УДК 681.322
ББК 32.973.202
К60

Колегов Д.Н.

К60 Лабораторный практикум по основам построения
защищенных компьютерных сетей. Томск :
Томский государственный университет, 2013. – 140 с.

Практикум представляет собой набор лабораторных работ по дисциплине «Основы построения защищенных компьютерных сетей», входящей в образовательную программу по направлению подготовки (специальности) 090301 «Компьютерная безопасность». Для студентов вузов, обучающихся по специальностям в области информационной безопасности, преподавателям и специалистам в области защиты информации.

УДК 681.322
ББК 32.973.202

© Томский государственный университет, 2013
© Колегов Д.Н., 2013

ВВЕДЕНИЕ

В настоящее время компьютерные сети являются ключевой составляющей современных информационно-телекоммуникационных систем. Среди всех задач по построению компьютерных сетей важнейшей является обеспечение их защищенности от угроз конфиденциальности, целостности и доступности. При этом подсистема защиты должна являться полноценной частью компьютерной сети, обеспечивающей ее безопасность, как одно из свойств. При таком подходе к построению архитектуры компьютерных сетей говорят о защищенных компьютерных сетях.

Данный лабораторный практикум представляет набор лабораторных работ по основам построению и инструментальному анализу защищенных компьютерных сетей. Целью лабораторного практикума является развитие научно-образовательного обеспечения в области безопасности информационно-телекоммуникационных технологий. Задачей лабораторного практикума является получение знаний и навыков по следующим направлениям:

- архитектура и методы построения защищенных телекоммуникационных и компьютерных сетей;
- планирование и проектирование подсистем защиты информационных технологий;
- настройка средств защиты сетевой инфраструктуры;
- методы и средства анализа защищенности сетевых информационных инфраструктур;
- методы применения инструментальных средств анализа защищенности информационно-телекоммуникационных систем.

Лабораторный практикум состоит из двух разделов. Первый из них содержит лабораторные работы, ориентированные на построение инфраструктуры защищенных компьютерных сетей и настройку механизмов их корректного функционирования и защиты. Второй раздел содержит лабораторные работы по инструментальному анализу защищенности компьютерных сетей.

Настоящий лабораторный практикум включает следующие лабораторные работы:

1. Настройка операционной системы Cisco IOS.
2. Защита инфраструктуры маршрутизации.
3. Защита инфраструктуры коммутации.
4. Защита ЛВС от петель на канальном уровне.
5. Защита ЛВС от атак канального уровня.
6. Построение маршрутизируемой ЛВС.
7. Защита сетевой инфраструктуры.
8. Защита периметра сети.
9. Криптографическая защита каналов передачи данных.
10. Защита беспроводной ЛВС.
11. Сбор предварительной информации о сети.
12. Идентификация узлов и портов сетевых служб.
13. Идентификация служб и приложений.
14. Идентификация операционных систем.
15. Идентификация уязвимостей сетевых приложений по косвенным признакам.
16. Идентификация уязвимостей на основе тестов.
17. Особенности идентификации уязвимостей Windows.
18. Сканирование уязвимостей СУБД Oracle.

19. Сканирование уязвимостей веб-приложений.

20. Сканирование уязвимостей корпоративной сети.

Описание каждой лабораторной работы включает: название, цель, краткие теоретические сведения, постановку задачи, последовательность действий исполнителя, а также вопросы и задания для самостоятельных исследований.

Для обеспечения условий выполнения лабораторных работ по построению защищенных компьютерных сетей рекомендуется использовать следующее основное программное обеспечение:

- программный эмулятор сетей «Cisco Packet Tracer»;
- систему виртуализации «VMware Player»;
- ОС семейства Microsoft Windows;
- ОС семейства GNU/Linux;
- инструментальное средство анализа защищенности «XSpider»⁴
- дистрибутив для анализа защищенности Backtrack Linux.

Данный набор программного обеспечения позволяет проводить одновременно лабораторный практикум для группы обучающихся численностью до 30 человек. Кроме того, программное обеспечение «Cisco Packet Tracer» позволяет эмулировать все основные процессы функционирования реальных компьютерных сетей и предоставляет в распоряжение обучающегося виртуальную компьютерную сеть, в которой и проводятся все настройки сетевой инфраструктуры, изучаются сетевые технологии и анализируются некоторые из возможных сетевых атак.

При необходимости «Cisco Packet Tracer» может быть заменен на симулятор GNS3 в рамках проведения дополнительных факульт-

тативных занятий или демонстраций. Это позволит наиболее глубоко и подробно изучить возможности современных сетевых технологий, протоколов и маршрутизаторов.

При подготовке второго раздела лабораторного практикума использовались материалы и программное обеспечение, полученные Томским государственным университетом в рамках образовательной программы «Практическая безопасность» ЗАО «Позитив Текнолоджис».

Предполагается, что обучающиеся к моменту начала выполнения учебных задач прослушали курс «Компьютерные сети» или аналогичный ему, а также имеют базовые представления об используемых в современных компьютерных сетях протоколах, криптографических алгоритмах и механизмах защиты.

будет полезно студентам вузов, обучающимся по специальностям в области информационной безопасности, преподавателям и специалистам в области защиты информации.

Основные сокращения и обозначения

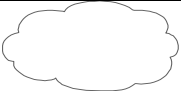
Русскоязычные сокращения

АС	Автоматизированная система
АРМ	Автоматизированное рабочее место
ГВС	Глобальная вычислительная сеть
ДМЗ	Демилитаризованная зона
КС	Компьютерная система
СПД	Сеть передачи данных
ЛВС	Локальная вычислительная сеть
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
СВТ	Средство вычислительной техники
ЭПС	Электронная почтовая система

Англоязычные сокращения

AAA	Аутентификация, авторизация, аудит (Authentication, authorization, audit)
ACL	Списки контроля доступа (Access control list)
DNS	Доменная система имен (Domain name system)
DoS	Отказ в обслуживании (Denial of Service)
NAT	Сетевая трансляция адресов (Network address translation)
VPN	Виртуальная частная сеть (Virtual private network)
VLAN	Виртуальная локальная сеть (Virtual local area network)

Графические обозначения

	Сеть передачи данных
	Оборудование сетей Frame Relay
	Маршрутизатор
	Маршрутизатор с функциями МЭ
	Маршрутизатор беспроводной ЛВС
	Маршрутизирующий коммутатор ЛВС
	Коммутатор ЛВС
	Маршрутизирующий МЭ
	VPN-концентратор
	Сервер
	Рабочая станция
	Мобильная рабочая станция

1. ЛАБОРАТОРНЫЕ РАБОТЫ ПО ПОСТРОЕНИЮ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

1.1. Настройка операционной системы Cisco

Цель работы

Целью лабораторной работы является обучение методам и средствам первоначальной настройки специализированной ОС Cisco IOS, под управлением которой работают маршрутизаторы.

Краткие теоретические сведения

Cisco IOS – это специализированная ОС, обеспечивающая функционирование сетевого оборудования компании «Cisco Systems, Inc». Взаимодействие с данной ОС возможно либо через web-браузер, либо через интерфейс командной строки (CLI-интерфейс). Данная ОС поддерживает удаленный доступ к интерфейсу командной строки по протоколам Telnet или SSH. В Cisco IOS существует несколько режимов.

Пользовательский режим (user mode) – стандартный режим первоначального доступа к ОС. В этот же режим ОС переходит автоматически при продолжительном отсутствии ввода в режиме администратора. В режиме пользователя доступны только простые команды, не влияющие на конфигурацию оборудования. Приглашение командной строки имеет следующий вид:

```
router>
```

Административный режим (privileged mode). Открывается командой *enable*, введенной в режиме пользователя:

```
router> enable
```

В административном режиме доступны команды, позволяющие получить полную информацию о конфигурации оборудования и его состоянии, а также команды перехода в режим конфигурирования, команды сохранения и загрузки конфигурации. Приглашение командной строки имеет следующий вид:

```
router#
```

Обратный переход в пользовательский режим производится по команде *disable* или по истечении установленного времени неактивности. Завершение сессии – команда *exit*.

Глобальный режим конфигурирования (конфигурационный режим). Активируется командой *config terminal*, введенной в административном режиме:

```
router# configure terminal
```

Глобальный режим конфигурирования организован иерархически – он содержит как непосредственно команды конфигурирования оборудования, так и команды перехода в режимы конфигурирования его подсистем (например, интерфейсов, протоколов маршрутизации, механизмов защиты).

Приглашения командной строки в наиболее часто используемых конфигурационных режимах имеют следующий вид:

```
router(config) #
```

```
router(config-if) #
```

```
router(config-router) #
```

```
router(config-ext-nacl) #
```

```
switch(config-line) #
```

```
switch(vlan) #
```

Выход из любого режима конфигурирования в режим верхнего уровня производится командой *exit* или комбинацией клавиш *Ctrl-Z*. Кроме того, команда *end*, поданная в любом из режимов конфигурирования немедленно завершает процесс конфигурирования и возвращает пользователя в администраторский режим.

Любая команда изменения конфигурации вступает в действие немедленно после ввода. Все команды и параметры могут быть сокращены (например, "*enable*" – "*en*", "*configure terminal*" – "*conf t*", "*show running-config*" – "*sh run*").

В любом месте командной строки для получения помощи может быть использован вопросительный знак, например:

```
router#?
```

```
router#co?
```

```
router#conf ?
```

Имена сетевых интерфейсов также могут быть сокращены, например, вместо "*fast ethernet0/1*" достаточно написать "*fa0/1*".

Отмена любой команды (отключение опции или режима, включаемых командой, снятие или удаление параметров, назначаемых командой) производится подачей этой же команды с префиксом "*no*", например:

```
router(config)#int fa0/1
```

```
router(config-if)#shutdown
```

```
router(config-if)#no shutdown
```

При загрузке сетевого оборудования, работающего под управлением Cisco IOS, происходит считывание команд конфигурации из изменяемого постоянного запоминающего устройства (NVRAM), где они хранятся в виде текстового файла, называемого *рабочей*

конфигурацией (running config). Конфигурация, сохраненная в NVRAM, называется *начальной конфигурацией* (startup config). В процессе работы оборудования администратор может вводить дополнительные конфигурационные команды, в результате чего рабочая конфигурация становится отличной от начальной.

Просмотр начальной и рабочей конфигураций маршрутизатора производится в административном режиме:

```
router#show startup-config
```

```
router#show running-config
```

Вывод последней команды позволяет просмотреть текущую конфигурацию. Однако если администратор не менял значения параметров, используемых в ОС по умолчанию, то они при выводе не отобразятся.

При копировании одной конфигурации поверх другой возможны два варианта: перезапись и слияние. При перезаписи старая конфигурация предварительно удаляется. При слиянии команды новой конфигурации добавляются к командам старой, как если бы они вводились вручную.

Ниже приведен список команд копирования конфигурации, первая из которых выполняется в режиме перезаписи, а последняя в режиме слияния:

```
router#copy running-config startup-config
```

```
router#copy startup-config running-config
```

Рассмотрим базовые команды получения информации о работе оборудования и его подсистем.

Просмотр информации об оборудовании (модель, объемы памяти, версия IOS, число и тип интерфейсов) выполняется по следующей команде:

```
router#show version
```

Просмотр содержимого флэш-памяти:

```
router#show flash:
```

Мониторинг загрузки процессора:

```
router#show processes
```

Рассмотрим основные команды первоначальной конфигурации маршрутизатора.

Установить имя маршрутизатора:

```
router(config)#hostname my_router
```

Установить пароль администратора, требуемый при переходе в вводе команды *enable*:

```
router(config)#enable secret my_secret
```

Отключение разрешения DNS-имен:

```
router(config)#no ip domain-lookup
```

Базовая настройка FastEthernet-интерфейса:

```
router#configure terminal
```

```
router(config)#interface fastEthernet 0/1
```

```
router(config-if)#ip          address          192.168.0.1  
255.255.255.0
```

```
router(config-if)#speed 100
```

```
router(config-if)#duplex full
```

```
router(config-if)#no shutdown
```

```
router(config-if)#exit
```

Для последовательного интерфейса устройства, выполняющего роль DCE, необходимо указывать тактовую частоту (пропускную способность), при этом данная команда выполняется только на одной стороне линии связи:

```
router(config) #interface serial0  
router(config-if) #clock rate 125000
```

Если на последовательном интерфейсе необходимо использовать другой протокол 2-го уровня (например, Frame Relay), то это делается с помощью команды:

```
router(config-if) #encapsulation frame-relay
```

Параметры интерфейсов, протоколов 2-го уровня, а также статистика отправленных и полученных кадров может быть просмотрена следующей командой в режиме администратора:

```
router#show interface
```

Подробная информация о параметрах протокола IP доступна в режиме администратора по команде:

```
router#show ip interface interface
```

Краткая сводная таблица состояний IP-интерфейсов:

```
router#show ip interface brief
```

Рассмотрим настройку статической маршрутизации. Маршруты, ведущие в сети, к которым маршрутизатор подключен непосредственно, автоматически добавляются в маршрутную таблицу после конфигурирования интерфейса при условии, что интерфейс корректно функционирует.

Для назначения дополнительных статических маршрутов в режиме глобальной конфигурации вводится команда:

```
router(config) #ip route prefix mask ip_address
```

Маршрут по умолчанию (стандартный маршрут) назначается следующей командой:

```
router(config)#ip route 0.0.0.0 0.0.0.0  
ip_address
```

Просмотреть таблицу маршрутов можно по команде:

```
router#show ip route
```

Постановка задачи

Выполнить первоначальную настройку сетевых параметров ОС Cisco IOS маршрутизатора Cisco 2811 с рабочей станции администратора сети, используя данные в следующей таблице:

Т а б л и ц а 1

Параметры настройки маршрутизатора

Параметр	Значение
IP-адрес интерфейса Fa0/0	10.194.7.1/24
IP-адрес интерфейса Fa0/1	192.168.100.26/30
Стандартный шлюз	192.168.100.25
Имя маршрутизатора	R7
Домен	net.bank
Пароль доступа enable	xkld7Hn434!2&^
Локальный пользователь/пароль	noc/nTefa#51

Последовательность действий

Шаг 1. Подключить к маршрутизатору Cisco 2811 рабочую станцию через консольный шнур и интерфейс RS-232.

Шаг 2. Запустить терминальный клиент и проверить правильность параметров его настройки.

Шаг 3. Просмотреть список команд пользовательского режима.
Выполнить команду:

```
router>show version
```

Шаг 4. Перейти в административный режим, выполнив команду:
router>enable

Шаг 5. Просмотреть уровень доступа в системе и текущую конфигурацию:

```
router#show privilege
```

```
router#show running-config
```

Шаг 6. Просмотреть список доступных команд. Определить и выполнить все возможные информационные команды. Например:

```
router#show flash
```

```
router#show version
```

```
router#show logging
```

Шаг 7. Выполнить настройку маршрутизатора в соответствии с указанными параметрами, выполнив следующие команды:

```
configure terminal
```

```
hostname R7
```

```
interface fastEthernet 0/1
```

```
    ip address 192.168.100.26 255.255.255.252
```

```
    no shutdown
```

```
interface fastEthernet 0/0
```

```
    ip address 10.194.7.1 255.255.255.0
```

```
    no shutdown
```

```
    ip domain-name net.bank
```

```
ip route 0.0.0.0 0.0.0.0 192.168.100.25
```


Шаг 8. Сохранить конфигурацию маршрутизатора, выполнив команду:

```
write memory
```

Шаг 9. Выключить питание маршрутизатора. Установить сетевой модуль NM-ESW161. Включить питание маршрутизатора. Проверить возможность загрузки маршрутизатора с новой конфигурацией.

Шаг 10. Просмотреть список всех портов и их имен:

```
sh ip interface brief
```

Шаг 11. Выполнить следующие команды и посмотреть их результаты:

```
sh processes
```

```
sh file systems
```

Шаг 12. Выключить режим шифрования паролей в конфигурационном файле, создать пользователя и убедиться, что пароль в конфигурационном файле записан в открытом виде, затем включить режим шифрования паролей и убедиться, что теперь пароль представляется в зашифрованном виде:

```
no service password-encryption
```

```
username noc1 secret test
```

```
username noc2 password test
```

```
enable secret test2
```

```
show running-config
```

```
service password-encryption
```

```
show running-config
```

Шаг 13. Удалить всех созданных ранее пользователей, задать стойкие к перебору пароли пользователей и пароли для административных

тивного доступа. Проверить, что для подключения к маршрутизатору и перехода в административный режим требуется пароль:

```
line console 0
  password n&bbR4d21
  login
no username noc1
no username noc2
enable secret xkld7Hn434!2&^
username noc secret nTefa#51
```

Шаг 14. Выполнить настройку механизма ролевого управления доступа к командам маршрутизатора, реализующего следующую политику безопасности.

Существуют следующие роли и соответствующие им уровни безопасности: администратор (15), инженер (5) и оператор (3). Доступ пользователям, авторизованным на роль инженера, может быть предоставлен только через консольную сессию. При этом могут быть выполнены основные команды по диагностике и настройке средств маршрутизации, коммутации и адресации.

Пользователи, авторизованные на роль оператора, могут только просматривать диагностические данные на маршрутизаторе. Роль администратора имеет все привилегии:

```
username admin privilege 15 secret nTefa#51
enable secret 15 secret Rc@sxa&h
username engineer privilege 5 secret LwqndhR5
enable secret 5 secret Jnfbn&gd
username operator privilege 3 secret *mmfjj&D
enable secret 3 secret Mf88MMh1
```

```
privilege exec level 3 show running-config
privilege exec level 3 show startup-config
privilege exec level 3 show
privilege exec level 3 ping
privilege exec level 3 ssh
privilege exec level 3 telnet
privilege exec level 3 exit
privilege exec level 5 configure terminal
privilege exec level 5 configure
privilege configure level 5 ip
privilege configure level 5 no ip
privilege configure level 5 ip route
privilege configure level 5 no ip route
privilege configure level 5 router
privilege configure level 5 no router
privilege configure level 5 interface
line console 0
  privilege 3
```

Вопросы и задания

1. Разработать шаблон конфигурационного файла маршрутизатора для удобства настройки, включить в него основные изученные команды.
2. Предложить набор учетных записей и прав доступа для эксплуатации маршрутизаторов в крупной корпоративной сети.
3. Изучить порядок наименования модулей линейных карт и сетевых интерфейсов на маршрутизаторах и коммутаторах Cisco.

1.2. Защита инфраструктуры маршрутизации

Цель работы

Целью лабораторной работы является обучение методам и средствам проектирования и защиты инфраструктуры маршрутизации отказоустойчивых иерархических компьютерных сетей на основе протокола маршрутизации OSPF.

Краткие теоретические сведения

Маршрутизация является одной из критически важных задач, обеспечивающей корректное функционирование, доступность, надежность и отказоустойчивость компьютерной сети. Выделяют следующие угрозы нарушения безопасности маршрутизации:

- угрозы, направленные на сеансы обмена маршрутной информацией: сброс TCP-сессий, исчерпание ресурсов;
- угрозы, направленные на маршрутизирующие сетевые устройства: отказ в обслуживании, подбор паролей, переполнение буфера, повышение привилегий;
- угрозы, направленные на маршрутную информацию: внедрение ложных маршрутов, создание циклов, удаление корректных маршрутов, чтение маршрутной информации, раскрытие параметров маршрутизации.

Для защиты инфраструктуры маршрутизации СПД используются следующие основные методы:

- управление распространением маршрутной информации с применением фильтров маршрутизации, управление обменом маршрутной информацией между узлами и процессами маршрутизации;

- ограничение множества систем, использующих протоколы маршрутизации, использование методов аутентификации, ограничение сеансов маршрутизации только доверенными узлами;

- регистрация событий маршрутизации, регистрация изменения состояний сеансов маршрутизации со смежными или соседними узлами.

Рассмотрим команды настройки, реализующие базовые методы защиты инфраструктуры маршрутизации.

Настройка аутентификации маршрутизаторов по алгоритму MD5 выполняется следующими командами:

```
interface Ethernet0/1  
ip ospf message-digest-key 10 md5 mysecret  
ip ospf authentication message-digest
```

Назначение интерфейсов маршрутизатора, по которым не распространяется маршрутная информация, выполняется командами:

```
router ospf 10  
passive interface Ethernet 0/0
```

или командами:

```
router ospf 10  
passive interface default  
no passive interface Ethernet 0/0
```

Включение регистрации событий маршрутизации выполняется командами:

```
router ospf 10  
log-adjacency-changes
```

Постановка задачи

На маршрутизаторах СПД выполнить настройки протокола OSPF, обеспечивающие корректную работу сети и защиту инфраструктуры маршрутизации.

Последовательность действий

Шаг 1. Настроить модель коммутаторов Frame Relay, используя элемент Cloud-PT набора WAN Emulation.

Шаг 2. Построить модель компьютерной сети в соответствии со схемой, представленной на рис. 1. Определить уровень каждого маршрутизатора СПД в ее иерархической модели.

Шаг 3. На маршрутизаторе R7 выполнить настройки интерфейсов, а также настройки протокола маршрутизации OSPF для области 120 (полностью тупиковой), обеспечивающие регистрацию событий маршрутизации, аутентификацию соседей и активацию пассивных интерфейсов:

```
router ospf 10
  log-adjacency-changes
  area 120 stub
  passive-interface default
  no passive-interface Se0/0/0
  network 0.0.0.0 255.255.255.255 area 120
interface Se0/0/0
  description Link to R4
  ip address 192.168.100.26 255.255.255.252
  ip ospf message-digest-key 10 md5 H4&hdn3&
  ip ospf authentication message-digest
```

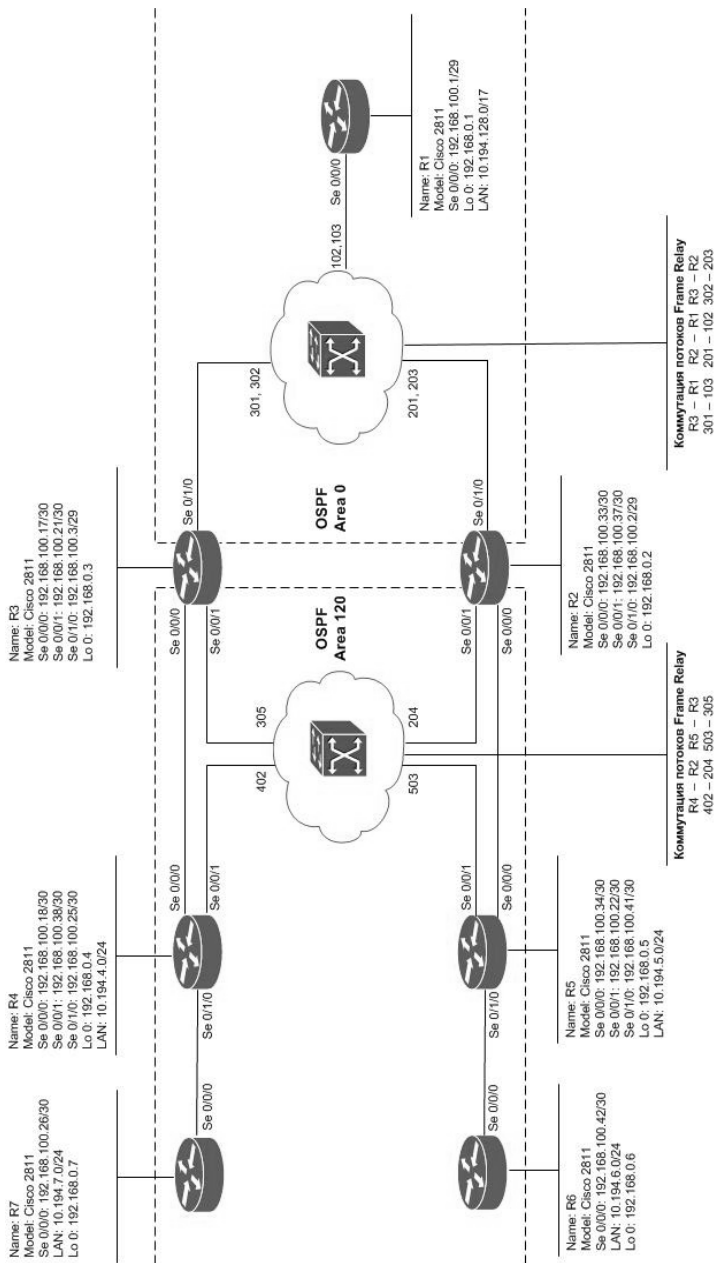


Рис. 1. Схема организации и маршрутизации СПД

```
interface Loopback0
    description Loopback interface
    ip address 192.168.0.7 255.255.255.255
```

Выполнить аналогичные настройки на маршрутизаторе R6.

Шаг 4. На маршрутизаторе R4 выполнить следующие настройки сетевых интерфейсов и протокола маршрутизации OSPF:

```
router ospf 10
    log-adjacency-changes
    area 120 stub
    passive-interface default
    no passive-interface Se0/0/0
    no passive-interface Se0/0/1
    no passive-interface Se0/1/0
    network 192.168.100.0 0.0.0.255 area 120
    network 10.194.0.0 0.0.255.255 area 120
    network 192.168.0.4 0.0.0.0 area 120

interface Se0/0/0
    description Link to R3
    ip address 192.168.100.18 255.255.255.252
    ip ospf message-digest-key 10 md5 H4&hdn3&
    ip ospf authentication message-digest

interface Se0/0/1
    description Frame Relay link to R2
    encapsulation frame-relay
    ip address 192.168.100.38 255.255.255.252
    ip ospf network point-to-point
    ip ospf message-digest-key 10 md5 H4&hdn3&
```



```

ip ospf authentication message-digest
interface Se0/1/0
  description Link to R7
  ip address 192.168.100.25 255.255.255.252
  clock rate 128000
  ip ospf message-digest-key 10 md5 H4&hdn3&
  ip ospf authentication message-digest

```

Выполнить аналогичные настройки на маршрутизаторе R5.

Шаг 5. На маршрутизаторе R3 выполнить следующие настройки сетевых интерфейсов и протокола маршрутизации OSPF:

```

router ospf 10
  log-adjacency-changes
  area 120 stub no-summary
  passive-interface default
  no passive-interface Se0/0/0
  no passive-interface Se0/0/1
  no passive-interface Se0/1/0
  network 192.168.100.17 0.0.0.0 area 120
  network 192.168.100.21 0.0.0.0 area 120
  network 192.168.0.3 0.0.0.0 area 120
  network 192.168.100.3 0.0.0.0 area 0
interface Se0/0/0
  description Link to R4
  clock rate 128000
  ip address 192.168.100.17 255.255.255.252
  ip ospf message-digest-key 10 md5 H4&hdn3&
  ip ospf authentication message-digest

```

```

interface Se0/0/1
    description Frame Relay link to R5
    encapsulation frame-relay
    ip address 192.168.100.21 255.255.255.252
    ip ospf network point-to-point
    ip ospf message-digest-key 10 md5 H4&hdn3&
    ip ospf authentication message-digest
interface Se0/1/0
    description Frame Relay link to R1
    encapsulation frame-relay
    ip address 192.168.100.3 255.255.255.248
    ip ospf message-digest-key 10 md5 H4&hdn3&
    ip ospf authentication message-digest
    ip ospf network broadcast
    ip ospf priority 10

```

Выполнить аналогичные настройки на маршрутизаторе R2, дополнительно назначив ему в рамках протокола OSPF роль BDR .

Шаг 6. На центральном маршрутизаторе R1 выполнить следующие основные настройки:

```

router ospf 10
    log-adjacency-changes
    passive-interface default
    no passive-interface Se0/0/0
    network 192.168.100.0 0.0.0.255 area 0
    network 192.168.0.1 0.0.0.0 area 0
interface Se0/0/0
    description Frame Relay link to R2, R3

```

```
encapsulation frame-relay
clock rate 128000
ip address 192.168.100.1 255.255.255.248
ip ospf network broadcast
ip ospf priority 0
ip ospf message-digest-key 10 md5 H4&hdn3&
ip ospf authentication message-digest
```

Шаг 7. Убедиться в корректности настроек маршрутизаторов, проверить возможность использования резервных маршрутов при разрыве основных каналов связи.

Шаг 8. Внедрить в СПД ложный маршрутизатор. Убедиться в невозможности установки сессий между маршрутизаторами СПД и ложным маршрутизатором, а также внедрения ложной маршрутной информации без знания пароля для алгоритма MD5.

Шаг 9. К маршрутизатору R4 подключить коммутатор ЛВС. Проанализировать сетевые информационные потоки ЛВС и убедиться в отсутствии в ней рассылки пакетов OSPF при активации пассивных интерфейсов.

Вопросы и задания

1. Определить в схеме СПД механизмы и средства обеспечения отказоустойчивости и масштабирования. Перечислить задачи, решаемые на каждом уровне иерархической модели данной СПД.
2. Найти и изучить описание всех команд, используемых для настройки протокола OSPF.
3. Для каждого маршрутизатора определить его характеристики, роли и свойства в рамках протокола OSPF.

1.3. Защита инфраструктуры коммутации

Цель работы

Целью лабораторной работы является обучение методам и средствам защиты инфраструктуры коммутации при использовании технологии виртуальных ЛВС (VLAN), их настройке и маршрутизации.

Краткие теоретические сведения

Виртуальная ЛВС или *VLAN* – широковещательный домен второго уровня. Порты коммутаторов, принадлежащие одной VLAN, могут обмениваться кадрами между собой, но не могут обмениваться кадрами с портами других VLAN.

Для централизованного управления VLAN на коммутаторах может быть использован протокол VTP.

Для передачи кадров нескольких VLAN между коммутаторами используются *магистральные соединения*, или *транки*.

Порты коммутаторов, образующие магистральный канал, называются *магистральными*, или *транковыми* портами. На магистральных портах (в отличие от портов доступа) производится идентификация и инкапсуляция кадров VLAN с помощью протоколов ISL или IEEE 802.1Q.

Для динамического создания магистрального канала между коммутаторами может использоваться протокол DTP. Порты коммутатора, передающие кадры только одной VLAN, называются *портами доступа* (access port). Как правило, по умолчанию все порты коммутаторов являются портами доступа и находятся в

VLAN с номером 1, называемой *собственной* или *стандартной* VLAN (native VLAN). Для собственных VLAN не применяются никакие протоколы инкапсуляции.

Различают статические и динамические VLAN. В *статических* VLAN назначение порта осуществляется администратором на этапе настройки коммутатора. В *динамических* VLAN назначение порта осуществляется по некоторому протоколу и, как правило, на основе MAC-адреса узла сети. В настоящее время в основном используются статические VLAN.

Компьютеры, находящиеся в разных VLAN могут обмениваться данными только через маршрутизатор (или любое другое устройство уровня L3), имеющий интерфейсы в этих VLAN. Такие VLAN называются маршрутизируемыми, иначе – изолированными.

В настоящее время рекомендуется использовать следующие принципы при создании и настройке защищенных коммутируемых ЛВС:

1. Не использовать для распространения информации об используемых VLAN в ЛВС протокол VTP (включать режим transparent).

2. В качестве протокола инкапсуляции использовать протокол IEEE 802.1Q.

3. Запретить передавать кадры собственной VLAN по магистральным каналам. В качестве native VLAN использовать специально для этого выделенную VLAN, не используемую ни для каких других целей.

4. Не использовать стандартную VLAN 1 в ЛВС ни для каких целей, особенно для управления сетевым оборудованием.

5. На магистральных портах использовать только необходимые VLAN – VLAN, которым принадлежат порты коммутаторов на другой стороне. Все другие VLAN запрещать.

6. Не использовать одинаковые VLAN на разных коммутаторах. Наиболее предпочтительный вариант проектирования – один коммутатор, одна VLAN, одна IP-подсеть.

7. Все неиспользуемые порты коммутатора переводить в режим shutdown и назначать их в специально созданную для этого немаршрутизируемую и изолированную VLAN.

8. На портах доступа отключать использование протокола DTP. Для минимизации времени восстановления функционирования системы при подключении канала на магистральных портах устанавливать протокол DTP в режимах On/On и Nonegotiate (отключать согласование).

Постановка задачи

ЛВС филиала банка построена на базе двух коммутаторов уровня доступа филиала Cisco Catalyst 2960 (SW4-2, SW4-3), коммутатора уровня ядра-распределения филиала Cisco Catalyst 3560 (SW4-1) и маршрутизатора доступа Cisco 2811 (R4).

Требуется создать VLAN с номерами для рабочих станций, принтеров и серверов банка в соответствии со схемой, представленной на рис. 2, настроить маршрутизацию между этими VLAN при их подключении к маршрутизатору R4 по магистральному каналу, а также выполнить настройки в соответствии с приведенными выше рекомендациями.

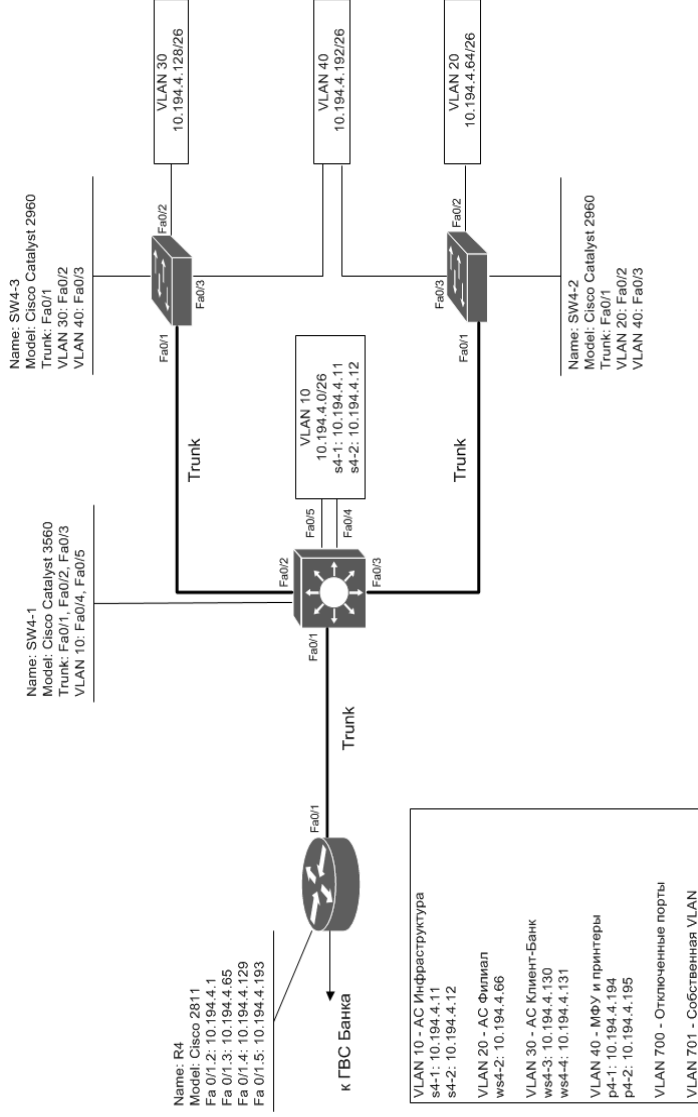


Рис. 2. Схема соединения оборудования ЛВС

Последовательность действий

Шаг 1. На коммутаторе уровня доступа филиала SW4-3 отключить протокол VTP, создать необходимые VLAN, настроить магистральный порт и порты доступа коммутатора:

```
vtp mode transparent
vlan 30
    name AS_Client_Bank
vlan 40
    name Service
vlan 700
    name unused ports
vlan 701
    name native
```

Шаг 2. Настроить используемые магистральные порты и порты доступа коммутатора SW4-3:

```
interface fastEthernet 0/1
    switchport mode trunk
    switchport nonegotiate
    switchport trunk native vlan 701
interface fastEthernet 0/2
    switchport mode access
    switchport nonegotiate
    switchport access vlan 30
```

Шаг 3. Настроить неиспользуемые порты коммутатора SW4-3, используя возможность указания диапазона портов:

```
interface range fastEthernet 0/4-24
    switchport mode access
```



```
switchport nonegotiate
switchport access vlan 700
shutdown
```

Шаг 4. Выполнить аналогичные настройки с учетом требуемых VLAN, на коммутаторе SW4-2.

Шаг 5. На коммутаторе уровня ядра-распределения филиала SW4-1 настроить магистральные порты для соединения с маршрутизатором и коммутаторами доступа по схеме магистрального подключения. Выполнить настройки безопасности согласно приведенным выше рекомендациям:

```
ip routing
interface fa0/1
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport nonegotiate
    switchport trunk native vlan 701
    switchport trunk allowed vlan 10,20,30,40
```

Шаг 6. На маршрутизаторе филиала R4 создать необходимые VLAN, настроить sub-интерфейсы на порту Fa0/1 и включить инкапсуляцию по протоколу IEEE 802.1Q:

```
interface fa0/1
    no shutdown
    no ip address
    interface fa0/1.2
        encapsulation dot1q 10
        ip address 10.194.4.1 255.255.255.192
    interface fa0/1.3
```

```
encapsulation dot1q 20
ip address 10.194.4.65 255.255.255.192
interface fa0/1.4
encapsulation dot1q 30
ip address 10.194.4.129 255.255.255.192
interface fa0/1.5
encapsulation dot1q 40
ip address 10.194.4.193 255.255.255.192
```

Шаг 7. Проверить доступность серверов AC с рабочих станций, исследовать формат кадров, передающихся по магистральному каналу между коммутатором ядра-распределения и маршрутизатором. Убедиться в невозможности взаимодействия с серверами AC из VLAN 700.

Шаг 8. Убедиться, что кадры native VLAN не инкапсулируются протоколом IEEE 802.1q при их передаче по магистральному каналу.

Вопросы и задания

1. Пояснить рекомендации по настройке механизмов защиты виртуальных ЛВС.
2. Реализовать в ЛВС атаку типа «VLAN hopping» при настройке различных собственных VLAN на транковых портах, соединяющих коммутаторы.
3. Настроить распространение базы данных VLAN через протокол VTP в соответствии с рекомендуемыми параметрами.
4. Настроить терминирование и маршрутизацию VLAN на коммутаторе уровня ядра-распределения ЛВС.

1.4. Защита ЛВС от петель на канальном уровне

Цель работы

Целью лабораторной работы является изучение методов и средств построения, защиты и оптимизации отказоустойчивых ЛВС на основе протокола STP.

Краткие теоретические сведения

Протоколы и механизмы оптимизации и защиты семейства STP предназначены для предотвращения петель (циклов) в сетях с множественными маршрутами на канальном уровне ЛВС. За счет обмена служебными BPDU-кадрами коммутаторы, на которых запущен протокол STP, строят топологию, в которой между любыми двумя коммутаторами существует только один активный в данный момент маршрут на канальном уровне.

В настоящее время семейство протоколов STP включает протоколы и механизмы IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, IEEE 802.1t, а также расширение Cisco Spanning Tree Toolkit.

Одним из основных элементов протокола STP является корневой коммутатор. Некорректный выбор корневого коммутатора, вызванный ошибками конфигурирования оборудования или атаками нарушителей, может привести к нарушению штатного функционирования сетевой инфраструктуры или перенаправлению и перехвату информационных потоков на канальном уровне.

В настоящее время используются следующие принципы при проектировании, настройке и оптимизации протоколов семейства STP.

1. Использовать протоколы семейства STP с целью построения отказоустойчивых ЛВС только при необходимости. По возможности для обеспечения отказоустойчивости и высокой доступности ЛВС использовать механизмы и протоколы маршрутизации сетевого уровня.

2. Применение протокола STP является обязательным в случае передачи данных в одной и той же виртуальной ЛВС, организованной на разных коммутаторах, а также для защиты от действий пользователей на портах доступа коммутаторов ЛВС и ошибок обслуживающего персонала.

3. В семействе протоколов STP рекомендуется использовать протокол Rapid-PVST+.

4. Административно определять и назначать корневые коммутаторы. Использовать дополнительные механизмы и средства защиты протокола STP (Root Guard, Loop Guard, UplinkFast, UDLD) для предотвращения получения роли корневого коммутатора другими коммутаторами.

5. На портах доступа коммутаторов ЛВС выполнять настройки по предотвращению возможности появления или фильтрации BPDU-пакетов протокола STP (механизмы BPDU Guard и BPDU Filter соответственно), а также выполнять настройки для быстрого включения и защиты корневого коммутатора (механизмы PortFast и Root Guard соответственно).

Постановка задачи

На коммутаторах ЛВС филиала банка выполнить настройки протокола STP и механизмов его защиты. Построенная ЛВС должна обеспечивать состояние доступности при отказе:

- одного из коммутаторов SW7-1 или SW7-2;
- активного коммутируемого порта маршрутизатора R7;
- одной из линий связи канала EtherChannel;
- активного порта линии связи между коммутатором уровня доступа и коммутатором уровня ядра-распределения.

Последовательность действий

Шаг 1. Построить схему логического соединения коммутаторов ЛВС и найти возможные циклы на канальном уровне (см. рис. 3). Определить оптимальное положение корневого коммутатора в соответствии с маршрутами информационных потоков.

Шаг 2. К маршрутизатору R7 в слот № 3 подключить модуль HWIC-4ESW, обеспечивающий наличие дополнительных четырех коммутируемых Ethernet-портов. Создать на коммутирующем модуле маршрутизатора виртуальные ЛВС и для каждой из них настроить интерфейс SVI, обеспечивающий маршрутизацию виртуальных ЛВС:

```
vlan database  
  vlan 10 name Servers  
  vlan 20 name AS_Filial  
  vlan 30 name AS_Client_Bank  
  vlan 40 name Service
```

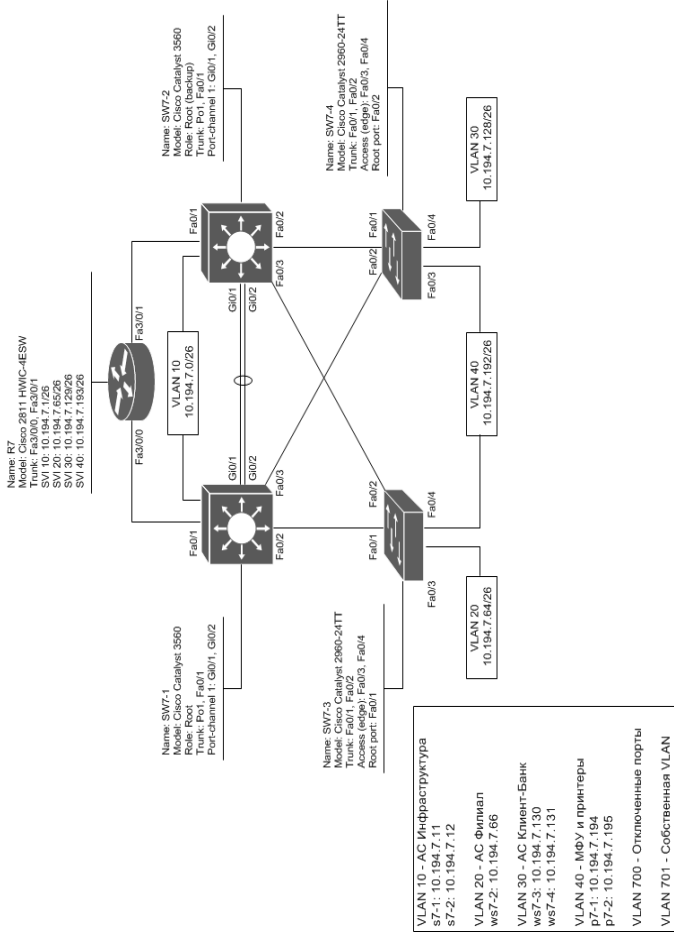


Рис. 3. Схема соединения коммутаторов отказоустойчивой ЛВС

```

interface vlan10
    ip address 10.194.7.1 255.255.255.192
interface vlan20
    ip address 10.194.7.65 255.255.255.192
interface vlan30
    ip address 10.194.7.129 255.255.255.192
interface vlan40
    ip address 10.194.7.193 255.255.255.192
interface fastEthernet 3/0/0
    switchport mode trunk
    switchport trunk allowed vlan 10,20,30,40
    switchport trunk native vlan 701
interface fastEthernet 3/0/1
    switchport mode trunk
    switchport trunk allowed vlan 10,20,30,40
    switchport trunk native vlan 701

```

Шаг 3. На коммутирующем модуле маршрутизатора R7 настроить протокол Rapid-PVST для требуемых VLAN:

```
spanning-tree mode rapid-pvst
```

Шаг 4. Между коммутаторами SW7-1 и SW7-2 настроить агрегирование двух каналов передачи данных по технологии Etherchannel:

```

interface GigabitEthernet0/1
    channel-protocol lacp
    channel-group 1 mode on
interface GigabitEthernet0/2
    channel-protocol lacp
    channel-group 1 mode on

```

```
interface port-channel 1
  no shutdown
  switchport mode trunk
  switchport trunk native vlan 701
  switchport trunk allowed vlan 10,20,30,40
```

Шаг 5. На коммутаторе SW7-1 настроить протокол Rapid-PVST для требуемых виртуальных ЛВС и задать наивысший приоритет коммутатора, обеспечив ему роль корневого моста в указанных VLAN:

```
spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30,40,701 root primary
```

Шаг 6. На коммутаторе SW7-2 настроить протокол Rapid-PVST для требуемых VLAN и задать наивысший приоритет коммутатора, обеспечив ему роль корневого моста в указанных VLAN в случае выхода из строя коммутатора SW7-1:

```
spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30,40,701 root secondary
```

Шаг 7. На коммутаторах SW7-1 и SW7-2 настроить механизм Root Guard:

```
interface range fa0/2-3
  spanning-tree guard root
```

Шаг 8. На коммутаторах SW7-3 и SW7-4 настроить протокол Rapid-PVST для требуемых VLAN:

```
spanning-tree mode rapid-pvst
spanning-tree vlan 20,30,40,701
```


Шаг 9. На портах доступа коммутаторов SW7-3 и SW7-4 настроить протокол STP в режиме portfast, включить механизмы защиты BPDU Guard:

```
interface range fa0/3-4  
switchport mode access  
spanning-tree bpduguard enable  
spanning-tree portfast
```

Шаг 10. Убедиться в корректности настройки протокола STP на коммутаторах ЛВС. Проверить возможность функционирования сети при отключении порта Fa0/0/1 маршрутизатора R7, при отключении порта Gi0/1 коммутатора SW7-1, при отключении коммутатора SW7-1 или при отключении порта Fa0/1 коммутатора SW7-3.

Вопросы и задания

1. Пояснить различия в работе между механизмами BPDU Guard, BPDU Filter и Root Guard. Описать области применения и назначение каждого из этих механизмов защиты.
2. Пояснить выбор портов активации механизма Root Guard на коммутаторах уровня ядра-распределения филиала.
3. Разработать проект внедрения механизма Loop Guard для защиты ЛВС от образования однонаправленных каналов связи.
4. Смоделировать DoS-атаку на сетевую инфраструктуру при подключении к ЛВС коммутатора с наименьшим значением параметра BID.
5. Смоделировать атаку типа BPDU spoofing на протокол STP путем подключения к ЛВС коммутатора нарушителя и получения им роли корневого моста.

1.5. Защита ЛВС от атак канального уровня

Цель работы

Целью лабораторной работы является изучение методов проектирования, развертывания и настройки механизмов защиты в коммутируемых ЛВС от атак канального уровня типа MAC-flooding и MAC-spoofing.

Краткие теоретические сведения

Одним из механизмов защиты ЛВС от атак является механизм *port security*, реализованный на коммутаторах. Механизм *port security* позволяет осуществлять фильтрацию кадров, поступающих на отдельные порты коммутатора ЛВС, на основе MAC-адреса источника.

При активизации данного защитного механизма на порту коммутатора создается список ассоциированных (разрешенных) с ним MAC-адресов. Кадры, поступающие на порт коммутатора с активизированной функцией *port security*, MAC-адреса которых не принадлежат данному списку, уничтожаются. При этом сам порт коммутатора может переходить в режим shutdown.

Существует два метода построения списка разрешенных MAC-адресов – метод статического назначения и метод динамического изучения.

Метод статического назначения разрешенных MAC-адресов применяется на коммутаторах доступа ДМЗ, центров обработки данных и т.д. При этом на порту коммутатора указывается конкретный MAC-адрес.

Метод динамического изучения адресов определяет максимальное количество MAC-адресов, ассоциируемых коммутатором с портом в течение некоторого времени. Такой способ построения таблицы адресов, как правило, применять на уровне доступа ЛВС или в сетях филиалов.

При нарушении безопасности – при поступлении на защищаемый порт коммутатора кадра с запрещенным MAC-адресом – возможно одно из трех событий: порт отключается (режим защиты shutdown), кадр отвергается коммутатором (режим защиты protect), кадр отвергается коммутатором, увеличивается счетчик нарушений порта и генерируется SNMP-сообщение (режим защиты restrict).

В динамически изменяемой сетевой инфраструктуре рекомендуется ограничиваться одним MAC-адресом для порта коммутатора и использовать режим protect, в серверных группах – статически задавать списки MAC-адресов и использовать режим shutdown, в VoIP-сегментах – ограничиваться двумя или тремя MAC-адресами с активизацией режима restrict.

Дополнительным механизмом формирования списка MAC-адресов является механизм sticky. Он позволяет добавить статически заданные или динамически выученные MAC-адреса в конфигурационный файл ОС коммутатора.

Постановка задачи

В сегменте ЛВС филиала (см. рис. 4), построенном на базе двух коммутаторов уровня доступа Cisco Catalyst 2960 и коммутатора уровня ядра-распределения Cisco Catalyst 3560, обеспечить защиту от атак типа MAC-flooding и MAC-spoofing.

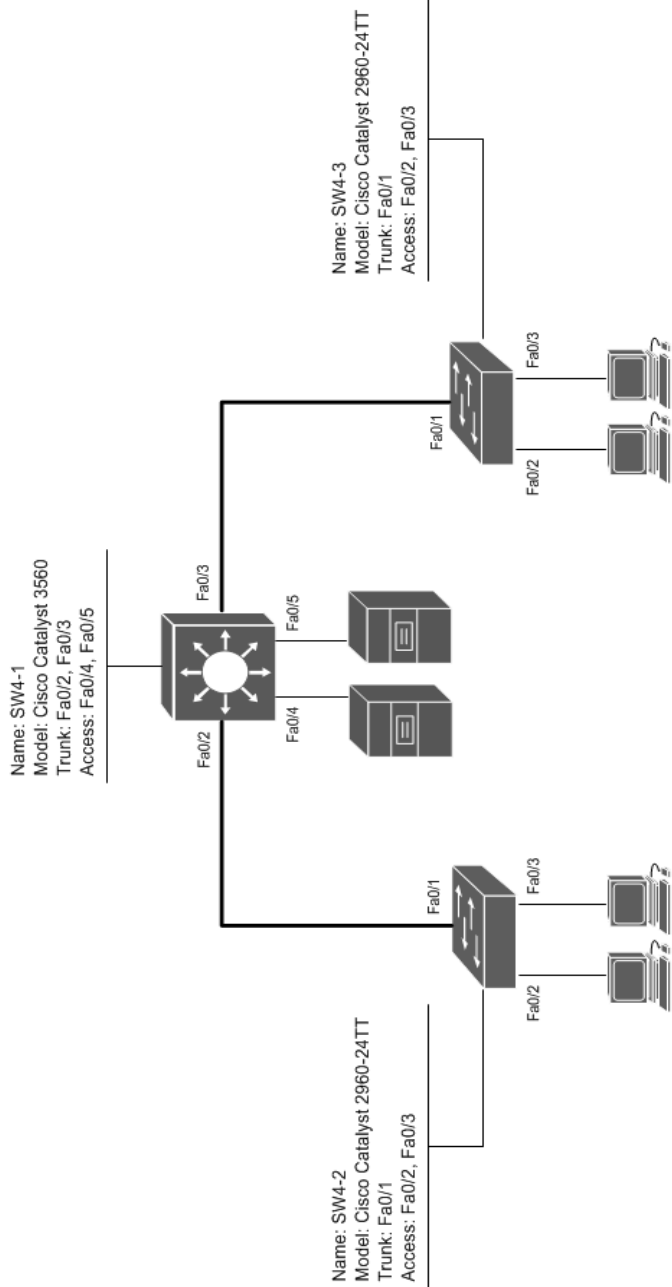


Рис. 4. Схема подключения оборудования к ЛВС филиала банка

Последовательность действий

Шаг 1. На коммутаторе уровня доступа SW4-3 настроить механизм port security в динамическом режиме для рабочих станций:

```
interface range fa0/2-3
    switchport mode access
    switchport port-security
    switchport port-security maximum 1
    switchport port-security violation protect
```

Шаг 2. Выполнить аналогичные настройки механизма port security на коммутаторе SW4-2.

Шаг 3. На коммутаторе уровня ядра-распределения SW4-1 настроить механизм port security в статическом режиме с привязкой к заданному MAC-адресу для порта FastEthernet0/4:

```
interface fa0/4
    switchport mode access
    switchport port-security
    switchport port-security maximum 1
    switchport port-security mac-address
    xxxx.yyyy.zzzz
    switchport port-security violation shutdown
```

Шаг 4. На коммутаторе уровня ядра-распределения SW4-1 настроить механизм port security в статическом режиме с опцией sticky для порта FastEthernet0/5:

```
interface fa0/5
    switchport mode access
    switchport port-security
    switchport port-security maximum 1
```

switchport port-security mac-address sticky

switchport port-security violation shutdown

Шаг 5. Проверить корректность настроек механизма безопасности port security коммутаторов ЛВС путем моделирования атаки типа MAC-spoofing. Задать MAC-адрес рабочей станции, подключенной к порту коммутатора со статическим методом формирования списка MAC-адресов, несоответствующий требованиям политики безопасности. Убедиться в переводе порта коммутатора в режим shutdown или protect.

Шаг 5. Проверить корректность настроек механизма безопасности port security коммутаторов ЛВС путем моделирования атаки типа MAC-flooding. На порт коммутатора с динамическим методом формирования списка разрешенных MAC-адресов подключить коммутатор с несколькими рабочими станциями. Убедиться в переводе порта коммутатора в режим shutdown или protect.

Вопросы и задания

1. Описать назначение и принцип работы механизма port security sticky для статического метода формирования MAC-адресов.

2. Объяснить рекомендацию задания максимального количества MAC-адресов на порту коммутатора с динамическим методом формирования списка из двух или трёх разрешенных MAC-адресов.

3. Возможно ли применение механизма port security для защиты от атак типа ARP spoofing и DHCP spoofing?

1.6. Построение маршрутизируемой ЛВС

Цель работы

Целью лабораторной работы является обучение методам построения и настройки маршрутизируемой ЛВС с высокой доступностью на основе протокола маршрутизации OSPF.

Краткие теоретические сведения

Архитектура современных корпоративных ЛВС должна обладать следующими основными свойствами: иерархичность, модульность, устойчивость и масштабируемость. Классическая иерархическая модель ЛВС состоит из трех уровней – ядра, распределения (агрегирования) и доступа. В современных корпоративных ЛВС, как правило, можно выделить блок распределения и блок сервисов, объединяемых ядром сети. От правильного проектирования блока распределения зависит стабильность и корректность работы всей ЛВС.

В настоящее время основными вариантами архитектуры блока распределения является многозвенная архитектура (multi-tier), архитектура с маршрутизируемым доступом (routed access) и архитектура с виртуальной коммутацией. Подходы различаются в границе между уровнями реализации, используемыми сетевыми технологиями и протоколами уровней L2 и L3, а также возможностями в реализации отказоустойчивости, избыточности и балансировки нагрузки.

Альтернативой традиционному блоку распределения с классической многозвенной архитектурой служит архитектура блока распределения с реализацией функций маршрутизации на уровне доступа,

что позволяет построить полностью маршрутизируемую ЛВС. В такой архитектуре коммутаторы доступа функционируют как устройства третьего уровня, магистральные каналы между коммутаторами уровней доступа и распределения заменены маршрутизируемыми каналами уровня L3.

Таким образом, граница сопряжения сетевых уровней L2 и L3 перемещена в иерархии ЛВС с уровня распределения на уровень доступа. При этом на всех коммутаторах доступа создаются уникальные виртуальные ЛВС, для которых шлюзами являются коммутаторы доступа.

Создание стандартного маршрутизатора для каждой виртуальной ЛВС на коммутаторе доступа выполняется через механизм Switch Virtual Interface (SVI). Для обеспечения высокой доступности используются механизмы маршрутизации, а не специализированные протоколы семейств FHRP и STP.

Данный подход содержит существенные преимущества по сравнению с классическим подходом: простота проектирования и реализации, простота отладки и управления, единые механизмы восстановления и управления.

При проектировании и конфигурировании маршрутизируемой ЛВС на основе протокола OSPF используются следующие основные принципы:

1. Создание двухуровневой модели маршрутизации – магистраль (область 0), реализуемая в ядре сети, и остальные области, реализуемые в сегментах сети, подключенных к магистральной через коммутаторы уровня распределения. Последние выступают в качестве пограничных маршрутизаторов области. Ограничение рассыл-

ки OSPF-сообщений путем определения и настройки пассивных интерфейсов на коммутаторах уровня доступа.

2. Наличие L3-соединения между коммутаторами уровня распределения, а также между коммутаторами уровня доступа и уровня распределения. Использование треугольных топологий между уровнями доступа, распределения и ядра.

3. Уменьшение количества рассылаемых OSPF-сообщений о состоянии связей и размера таблиц маршрутизации путем определения и настройки тупиковых и полностью тупиковых областей, а также путем выполнения суммирования маршрутов на пограничных маршрутизаторах.

Достоинства полностью маршрутизируемых ЛВС:

- простота реализации и сопровождения;
- наличие развитых средств диагностики и устранения неисправностей;
- высокая скорость и предсказуемость восстановления после отказов;
- унификация средств и механизмов построения всех уровней.

Основным требованием для обеспечения возможности построения маршрутизируемой ЛВС является наличие на всех коммутаторах уникальных VLAN.

Постановка задачи

Выполнить настройки коммутаторов ЛВС банка, обеспечивающие реализацию архитектуры полностью маршрутизируемой ЛВС с высокой доступностью.

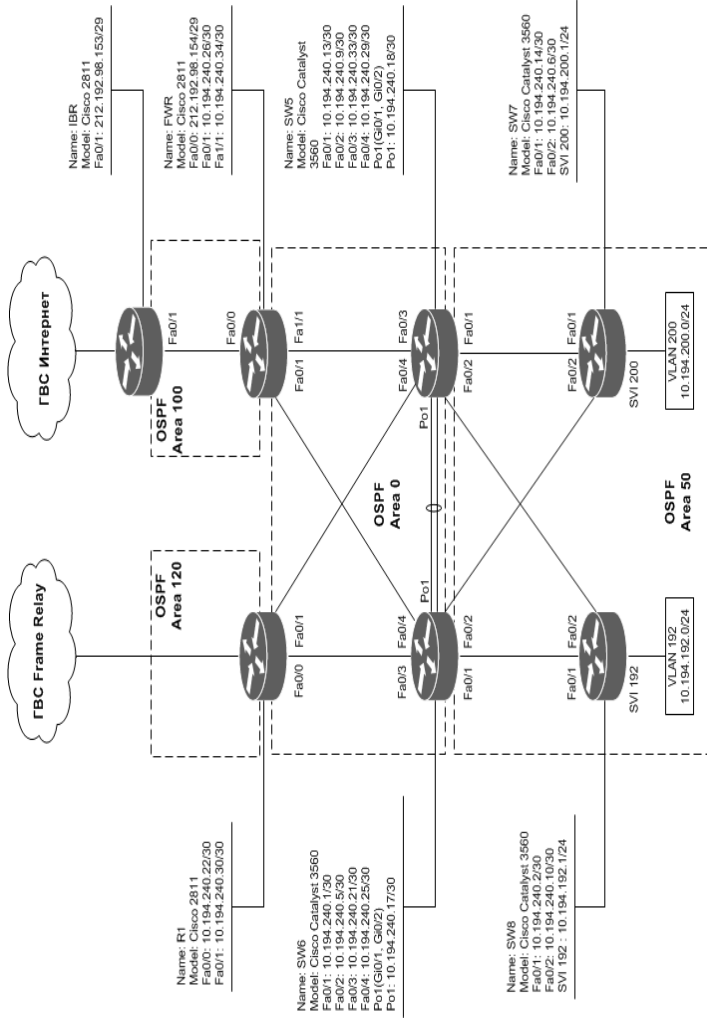


Рис 5. Схема маршрутизации в ЛВС

Последовательность действий

Шаг 1. Построить сеть, в соответствии со схемой маршрутизации, представленной на рис. 5. При необходимости ввести необходимые элементы и включить дополнительные механизмы. Выполнить настройки интерфейса SVI на коммутаторе уровня доступа SW8:

```
vlan 192
interface vlan192
    ip address 10.194.192.1 255.255.255.0
interface fastEthernet 0/10
    switchport access vlan 192
```

Шаг 2. Выполнить настройки протокола маршрутизации OSPF на коммутаторе уровня доступа SW8, обеспечив аутентификацию соседей и инициализацию пассивных интерфейсов:

```
router ospf 10
    log-adjacency-changes
    area 50 stub
    passive-interface default
    no passive-interface fastEthernet 0/1
    no passive-interface fastEthernet 0/2
    network 10.194.0.0 0.0.255.255 area 50
interface fastEthernet 0/1
    no switchport
    ip address 10.194.240.2 255.255.255.252
    ip ospf authentication message-digest
    ip ospf message-digest-key 10 md5 H4&hdn3&
interface fastEthernet 0/2
```

```
no switchport
ip address 10.194.240.10 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 10 md5 H4&hdn3&
```

Шаг 3. Выполнить аналогичные настройки на коммутаторе уровня доступа SW7 согласно схеме, представленной на рис. 5.

Шаг 4. Выполнить настройки протокола маршрутизации OSPF на коммутаторе уровня ядра-распределения SW5, обеспечив аутентификацию соседей, инициализацию пассивных интерфейсов аутентификации соседей и полностью тупиковых областей. Для последней выполняется настройка:

```
router ospf 10
area 50 stub no-summary
```

Шаг 5. Выполнить аналогичные настройки на коммутаторе уровня ядра-распределения SW6.

Шаг 6. Выполнить аналогичные настройки протокола маршрутизации OSPF на маршрутизаторах R1, IBR и FWR. На пограничном маршрутизаторе автономной системы IBR дополнительно настроить объявление внешнего маршрута в OSPF-систему:

```
router ospf 10
network 212.192.98.152 0.0.0.7 area 100
default-information originate
```

Шаг 7. Проверить доступность всех узлов и отказоустойчивость ЛВС.

Шаг 8. Убедиться в прохождении пакетов по разным альтернативным маршрутам (технология ECMP). Выполнить настройки по изменению стоимости интерфейсов коммутаторов так, чтобы все IP-

пакеты проходили только через коммутатор SW5, а при его отказе – через коммутатор SW6. Убедиться в прохождении пакетов по одному маршруту:

```
interface fastEthernet 0/2  
ip ospf cost 2
```

Вопросы и задания

1. Определить в схеме маршрутизации ЛВС механизмы и средства обеспечения отказоустойчивости и масштабирования.
2. Какие сложности могут возникнуть в процессе реализации политик безопасности (межсетевом экранировании, организации VPN) при построении маршрутизируемых ЛВС?
3. Смоделировать процесс асимметричной маршрутизации ЛВС. Каким требованиям должны удовлетворять средства защиты информации при поддержке асимметричной маршрутизации?

1.7. Защита сетевой инфраструктуры

Цель работы

Целью лабораторной работы является изучение методов и средств защиты сетевой инфраструктуры от НСД, а также принципов проектирования сетей управления.

Краткие теоретические сведения

Для защиты устройств сетевой инфраструктуры от НСД, обеспечения ее устойчивости и безотказного функционирования используются следующие основные настройки безопасности:

1. Отключение неиспользуемых протоколов, сетевых служб и механизмов (DNS, CDP, TELNET, DHCP, FINGER, ECHO, маршрутизация от источника, проху-arp, ICMP redirect, ICMP mask-reply и др.).

2. Настройка планировщика задач для обеспечения возможности передачи ресурсов процессам управления.

3. Ограничение доступа к сетевой инфраструктуре только из сети управления или с автоматизированных рабочих мест администраторов.

4. Обеспечение синхронизации времени на всех устройствах для корректного анализа событий (в том числе и событий безопасности). Для этого настраивается синхронизация времени с внешним источником по протоколу NTP с аутентификацией пакетов.

5. Уведомление и сохранение информации о сбоях (SNMP, SYSLOG, автоматическое сохранение файлов crashinfo, создаваемых ОС при фатальных сбоях аппаратного или программного обеспечения).

6. Предупреждение лиц, подключившихся к устройству, о запрете тех или иных действий. Для этого на всех устройствах настраивается выдача предупреждающего сообщения о запрещении НСД к данному устройству. Регистрация и учет для всех видов доступа. Регистрация лиц, осуществляющих доступ к устройству, выполняемых ими действий и времени для последующего аудита.

7. Разрешение управления устройством только по защищенным протоколам типа SSH и SNMP с узлов сети управления и установлением ограничений на продолжительность сессий.

8. Настройка механизмов парольной защиты: использование стойких паролей, включение хэширования и шифрования паролей.

В архитектуре сетей с высоким уровнем безопасности, как правило, выделенная строится сеть управления, выполняющая отдельные функции передачи информационных потоков уровня управления. Сеть управления, использующая физически выделенные каналы, называется сетью внеполосного управления (out-of-band network). Сеть управления, использующая каналы передачи данных, называется сетью внутрисполосного управления (in-band network).

Как правило, сеть внеполосного управления строится в корпоративных ЛВС и ЦОД. При этом используются выделенные, виртуальные коммутаторы и маршрутизаторы.

Сети внутрисполосного управления используются для управления сетями филиалов и внешними устройствами периметра. При построении сетей управления активно используются современные технологии виртуализации сетей – технологии VLAN, VRF, path isolation, механизмы MPLS.

Постановка задачи

Организовать управление сетевым оборудованием филиала из сети внеполосного управления. Выполнить настройки по обеспечению защиты маршрутизаторов СПД. Для централизованного управления доступом администраторов к сетевому оборудованию банка использовать технологию AAA.

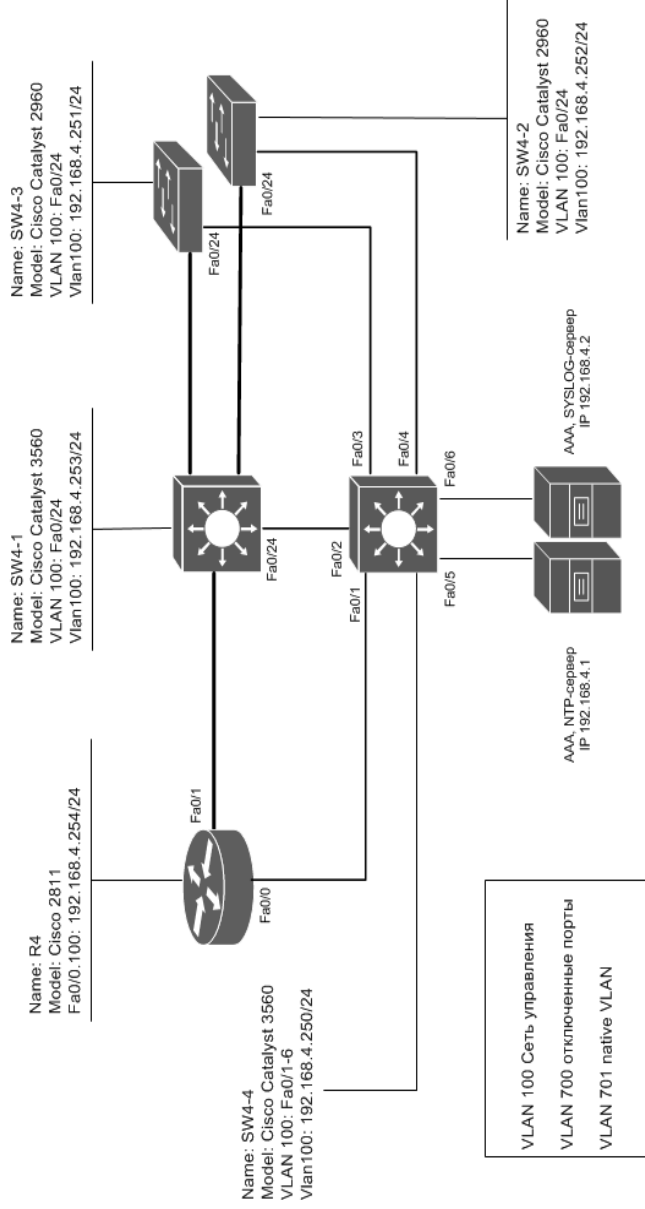


Рис. 6. Сеть внепольного управления ЛВС

Последовательность действий

Шаг 1. Подключиться к маршрутизатору R4 через консольный порт с рабочей станции администратора сети.

Шаг 2. Задать имя маршрутизатора и домен. Сгенерировать криптографические ключи, используемые в криптографическом протоколе SSH, для чего задать имя узла сети и домен:

```
hostname R4
ip domain-name net.bank
crypto key generate rsa
```

Шаг 3. Включить доступ к маршрутизатору по протоколу SSHv2, задать количество попыток аутентификации:

```
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 2
```

Шаг 4. Настроить выдачу предупреждающего сообщения о подключении к сетевому оборудованию:

```
banner login #
*****
*
*                               Bank Router
*
*          UNAUTHORIZED ACCESS IS PROHIBITED          *
*You   have   accessed   network   equipment.   *
*You must have authorized permission to access*
*or configure this device. All activities*
*performed on this device are monitored and*
*logged.                                           *
*****#
```

Шаг 5. Создать локального пользователя и установить пароль на доступ к конфигурационному режиму:

```
username noc secret 5 *jfl(jf33aq  
enable secret Kmme5bb$
```

Шаг 6. Отключить службы DNS и CDP, включить шифрование паролей в конфигурационном файле:

```
no ip domain-lookup  
no cdp run  
service password-encryption
```

Шаг 7. Выполнить настройки доступа к маршрутизатору по технологии AAA на основе протокола TACACS+:

```
tacacs-server host 192.168.4.1 key 8t8Gd2k1;p  
tacacs-server host 192.168.4.2 key r38voa8feq  
aaa new-model  
aaa authentication login default group tacacs+  
local  
aaa authentication enable default group tacacs+  
enable  
aaa authorization exec default group tacacs+  
local
```

Шаг 8. Настроить удаленный доступ к маршрутизатору с разрешенных IP-адресов рабочих станций сети управления филиала:

```
ip access-list extended iacl-vty  
    permit tcp 192.168.4.0 0.0.0.63 any eq 22  
    deny ip any any  
line con 0  
    exec-timeout 5 0
```

```
login authentication default
line vty 0 15
  exec-timeout 10 0
  transport input ssh
  access-class iacl-vty in
```

Шаг 9. Выполнить настройки службы регистрации событий и их отправки на сервер регистрации событий филиала (IP-адрес 192.168.4.2) по протоколу SYSLOG:

```
service timestamps log datetime msec
service timestamps debug datetime msec
logging 192.168.4.2
logging trap debugging
logging buffered 512000
```

Шаг 10. Выполнить настройки протокола SNMP для доступа к маршрутизатору с сервера мониторинга:

```
snmp-server community Hn4bUn3ba ro
snmp-server community mf5FN0d2d rw
```

Шаг 11. Выполнить настройки протокола NTP для синхронизации времени с сервером точного времени (IP-адрес 192.168.4.1):

```
ntp authenticate
ntp authentication-key 1 md5 Yghd6qh2!
ntp trusted-key 1
ntp server 192.168.4.1 key 1
```

Шаг 12. Выполнить настройки коммутаторов ЛВС филиала для подключения к сети внеполосного управления в соответствии со схемой, представленной на рис. 6. На коммутаторах настроить виртуальный интерфейс типа SVI:

```
interface vlan100
  ip address 192.168.4.250 255.255.255.0
  no shutdown
  ip default-gateway 192.168.4.254
```

Шаг 13. На маршрутизаторе R4 выполнить настройки по ограничению доступа к сети управления из ЛВС передачи данных:

```
ip access-list extended iacl-in-management
  permit ip 192.168.4.0 0.0.0.255 192.168.4.0
  0.0.0.255
  deny ip any any
ip access-list extended iacl-out-management
  permit ip 192.168.4.0 0.0.0.255 192.168.4.0
  0.0.0.255
  deny ip any any
```

```
interface fa0/0.100
  encapsulation dot1q 100
  ip access-group iacl-out-management out
  ip access-group iacl-in-management in
```

Шаг 14. Проверить корректность функционирования сети управления, а также регистрацию событий на сервере SYSLOG.

Вопросы и задания

1. В сети одного из филиалов банка построить сеть внутрипольного управления.
2. Убедиться в невозможности доступа в сеть управления из ЛВС передачи данных и наоборот.

1.8. Защита периметра сети

Цель работы

Целью лабораторной работы является изучение основных технологий межсетевого экранирования, методов и средств управления безопасностью информационных потоков на межсетевых экранах и сетевых маршрутизаторах.

Краткие теоретические сведения

Межсетевой экран (далее – МЭ) – аппаратный, программно-аппаратный или программный комплекс, реализующий функции управления, контроля и фильтрации сетевых информационных потоков между двумя и более АС по некоторому набору правил, определяемых политикой безопасности.

МЭ подразделяются на различные типы в зависимости от следующих характеристик:

- обеспечивается соединение между одним узлом и сетью или между двумя или более различными сетями;
- происходит контроль потока данных на сетевом уровне или более высоких уровнях эталонной модели ISO/OSI;
- отслеживаются состояния активных соединений или нет.

В зависимости от охвата контролируемых потоков данных МЭ, как правило, делятся на:

- традиционные МЭ, которые обычно представляют собой специализированное устройство или компьютер, размещённый на границе двух или более сетей. Такие типы экранов контролируют

входящие и исходящие потоки данных в каждой из подключенных сетей;

- персональные МЭ – программные МЭ или модули антивирусного ПО, устанавливаемые на отдельном компьютере и предназначенные для защиты только этого компьютера от несанкционированного доступа.

В зависимости от уровня, на котором происходит управление доступом, существует разделение на:

- МЭ, работающие на сетевом уровне, когда фильтрация происходит на основе сетевых адресов отправителя и получателя пакетов, номеров портов транспортного уровня и статических правил, заданных администратором;

- МЭ, работающие на уровне приложений, осуществляющие контроль за передаваемыми данными на более высоких уровнях модели *OSI*. Такие типы экранов позволяют блокировать передачу нежелательной и потенциально опасной информации в зависимости от принятой администратором политики и настроек устройства. Такие типы МЭ обычно работают в режиме прокси-сервера различных приложений, а не маршрутизации на сетевом уровне.

В зависимости от реализации возможности отслеживания активных соединений МЭ бывают:

- без инспекции состояний – не отслеживают текущие соединения (например, *TCP*), а фильтруют поток данных исключительно на основе статических правил;

- с инспекцией состояний – с отслеживанием текущих соединений и пропуском только таких пакетов, которые удовлетворяют логике и алгоритмам работы соответствующих

протоколов и приложений. Данные МЭ позволяют эффективнее бороться с различными типами *DoS*-атак и уязвимостями некоторых сетевых протоколов. Кроме того, они обеспечивают функционирование таких протоколов, как *H.323*, *SIP*, *FTP* и т.п., использующие сложные схемы передачи данных между узлами, плохо поддающиеся описанию статическими правилами, и зачастую несовместимы со стандартными МЭ без инспекции состояний.

Дополнительными механизмами защиты и управления информационными потоками, реализуемыми, как правило, в МЭ, являются технологии NAT, AAA, VPN и IDPS.

Технология NAT применяется как для обеспечения доступа узлов с немаршрутизируемыми адресами к ГВС Интернет, так и для реализации механизмов защиты сети, например, для изоляции сетей управления или прохождения пакетов через VPN-шлюз.

Существуют следующие виды NAT: динамическая трансляция адресов на уровне портов, динамическая трансляция на уровне портов с выборкой IP-адресов, трансляция с динамической выборкой IP-адресов и статическая трансляция.

Постановка задачи

Настроить правила управления доступом серверов и рабочих станций из ЛВС в сеть Интернет и из нее к серверам АС, расположенным в ДМЗ согласно табл. 2. Реализовать механизм первичной фильтрации пакетов на пограничном маршрутизаторе IBR. Доступ в сеть Интернет из сети 10.194.200.0/24 осуществляется по технологии NAT.

Политика безопасности управления сетевыми потоками информации

№	Источник	Назначение	Правило
1	Сеть 10.194.192.0/24	Интернет	Запретить
2	Сеть 10.194.200.0/24	Интернет	NAT
3	Сеть 10.194.200.0/24	Недоверенные DNS-сервера	Запретить
4	Сеть 10.194.200.0/24	Интернет, протокол HTTP	Разрешить
5	Прокси-сервер IP-адрес 10.194.210.10	Внешний DNS-сервер IP-адрес 212.192.98.162, протокол DNS	Разрешить
6	Терминальный сервер IP-адрес 10.194.210.11	Внешний DNS-сервер IP-адрес 212.192.98.162, протокол DNS	Разрешить
7	Прокси-сервер IP-адрес 10.194.210.10	Интернет, протокол HTTP	Разрешить, через NAT
8	Терминальный сервер IP-адрес 10.194.210.11	Интернет, протокол HTTP	Разрешить через PAT
9	DNS-сервер IP-адрес 212.192.98.162	Интернет, протокол DNS	Разрешить
10	DNS-сервер IP-адрес 212.192.98.162	Интернет	Запретить
11	Веб-сервер IP-адрес 212.192.98.163	Интернет	Запретить
12	Сеть Интернет	IP-адрес 212.192.98.162, протокол DNS	Разрешить
13	Сеть Интернет	IP-адрес 212.192.98.163, протокол HTTP	Разрешить
14	Любая сеть	Любая сеть	Запретить

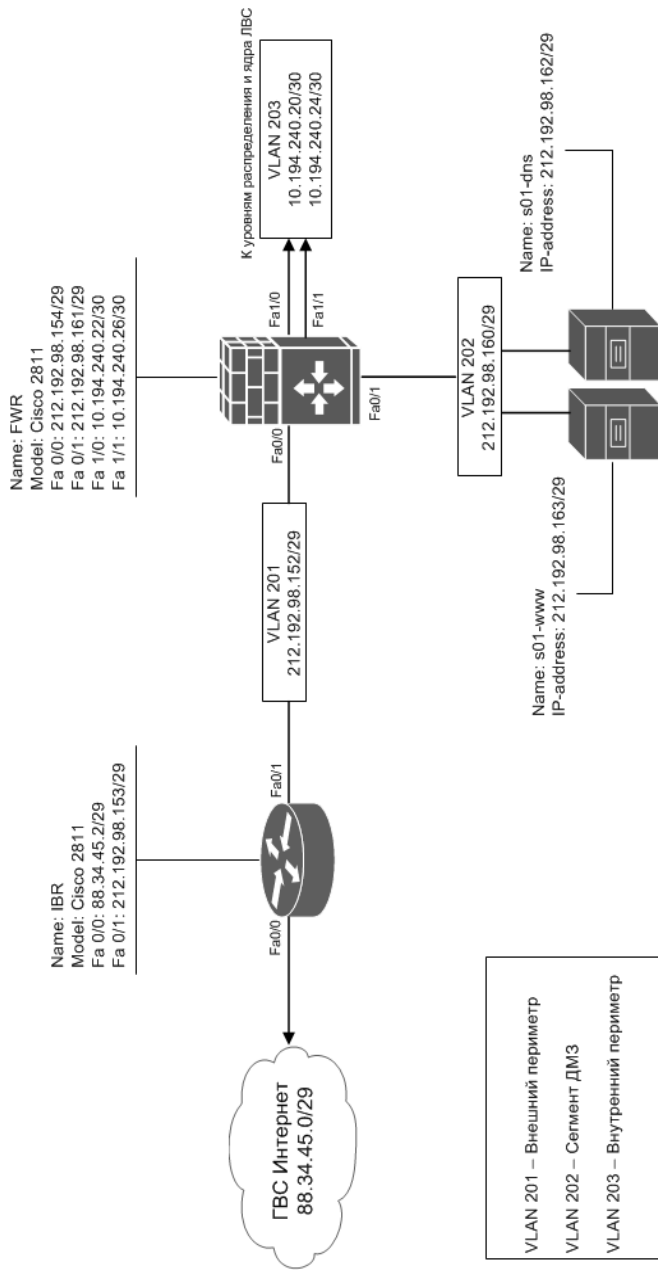


Рис. 7. Схема периметра Интернет

Доступ из сети 10.194.192.0/24 в Интернет запрещен и осуществляется через терминальный сервер s01-term (IP-адрес 10.194.210.11). Дополнительно в ЛВС существует прокси-сервер s01-proxu (IP-адрес 10.194.210.10). Для реализации технологии NAT выделяются IP-сети 212.192.98.168/29 и 212.192.98.154/32 соответственно. В сегменте ДМЗ расположены DNS-сервер s01-dns (IP-адрес 212.192.98.162) и WWW-сервер s01-www (IP-адрес 212.192.98.163). Настроить политику управления доступом к данным серверам на основе порядка функционирования WWW- и DNS-служб.

Последовательность действий

Шаг 1. Построить сегмент периметра Интернет в соответствии со схемой, представленной на рис. 7.

Шаг 2. Настроить IP-интерфейсы, VLAN и маршрутизацию по протоколу OSPF.

Шаг 3. Выполнить настройки технологии трансляции адресов на экранирующем маршрутизаторе FWR:

```
ip nat pool pool-net200 212.192.98.169
212.192.98.174 netmask 255.255.255.248
ip access-list standard acl-nat
 permit 10.194.200.0 0.0.0.255
 permit host 10.194.210.10
ip access-list standard acl-pat
 permit host 10.194.210.11
ip nat inside source list acl-nat pool pool-
net200
ip nat inside source list acl-pat interface fa0/0
```

```

interface fa1/1
    ip nat inside
interface fa1/0
    ip nat inside
interface fa0/0
    ip nat outside

```

Шаг 4. Настроить фильтрацию информационных потоков в соответствии с табл. 2:

```

ip access-list extended acl-LAN
    deny ip 10.194.192.0 0.0.0.255 any
    deny tcp 10.194.200.0 0.0.0.255 any eq 53
    deny udp 10.194.200.0 0.0.0.255 any eq 53
    permit    udp    host    10.194.210.10    host
    212.192.98.162 eq 53
    permit    tcp    host    10.194.210.10    host
    212.192.98.162 eq 53
    permit    udp    host    10.194.210.11    host
    212.192.98.162 eq 53
    permit    tcp    host    10.194.210.11    host
    212.192.98.162 eq 53
    deny tcp host 10.194.210.10 any eq 53
    deny udp host 10.194.210.10 any eq 53
    deny tcp host 10.194.210.11 any eq 53
    deny udp host 10.194.210.11 any eq 53
    permit tcp 10.194.200.0 0.0.0.255 any eq 80
    permit tcp host 10.194.210.11 any eq 80
    deny ip any any

```

```

ip access-list extended acl-DMZ
    permit tcp host 212.192.98.162 any eq 53
    permit udp host 212.192.98.162 any eq 53
    deny ip host 212.192.98.163 any
    deny ip any any
ip access-list extended acl-INTERNET
    permit tcp any host 212.192.98.162 eq 53
    permit udp any host 212.192.98.162 eq 53
    permit tcp any host 212.192.98.163 eq 80
    deny ip any any
interface fa0/0
    ip access-group acl-INTERNET in
interface fa0/1
    ip access-group acl-DMZ in
interface fa1/0
    ip access-group acl-LAN in
interface fa1/1
    ip access-group acl-LAN in

```

Шаг 5. Выполнить настройки механизма инспекции состояний

СВАС на маршрутизаторе FWR:

```

ip inspect audit-trail
ip inspect dns-timeout 15
ip inspect tcp synwait-time 15
ip inspect tcp finwait-time 20
ip inspect tcp idle-time 120
ip inspect udp idle-time 20
ip inspect name cbac-dmz http

```

```

ip inspect name cbac-dmz tcp
ip inspect name cbac-dmz icmp
ip inspect name cbac-dmz udp
ip inspect name cbac-lan http
ip inspect name cbac-lan tcp
ip inspect name cbac-lan icmp
ip inspect name cbac-lan udp
ip inspect name cbac-internet http
ip inspect name cbac-internet tcp
ip inspect name cbac-internet icmp
ip inspect name cbac-internet udp
interface fa0/0
    ip inspect cbac-internet in
interface fa0/1
    ip inspect cbac-dmz in
interface fa1/0
    ip inspect cbac-lan in
interface fa1/1
    ip inspect cbac-lan in

```

Шаг 6. На пограничном маршрутизаторе периметра сети IBR настроить механизм первичной фильтрации пакетов:

```

ip access-list extended iacl-internet
deny ip host 0.0.0.0 any
deny ip 127.0.0.0 0.255.255.255 any
deny ip 192.0.2.0 0.0.0.255 any
deny ip 224.0.0.0 31.255.255.255 any
deny ip 10.0.0.0 0.255.255.255 any

```

```

deny ip 172.16.0.0 0.0.15.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 212.192.98.152 0.0.0.7 any
deny ip 212.192.98.160 0.0.0.7 any
permit ip any any

ip access-list extended iacl-DMZ
    permit ip 212.192.98.152 0.0.0.7 any
    permit ip 212.192.98.160 0.0.0.7 any
    deny ip any any

interface fa0/0
    ip access-group iacl-internet in
interface fa0/1
    ip access-group iacl-DMZ in

```

Шаг 7. Проверить корректность функционирования оборудования периметра Интернет, возможность доступа из сети Интернет к общедоступным сервисам и в сеть Интернет из корпоративной ЛВС.

Вопросы и задания

1. Проанализировать политику безопасности управления информационными потоками, представленную в табл. 2.
2. Дополнить политику безопасности управления информационными потоками правилами для проектируемой вами электронной почтовой системы.
3. Обеспечить доступ к сети Интернет из сетей филиалов через ГВС. При необходимости внести изменения в политику безопасности управления информационными потоками.

1.9. Криптографическая защита каналов передачи данных

Цель работы

Целью лабораторной работы является обучение методам и средствам защиты каналов передачи данных ГВС на основе технологии виртуальных частных сетей.

Краткие теоретические сведения

При организации обмена и передачи информации в ГВС, как правило, исходят из модели нарушителя, в которой последний контролирует каналы передачи данных, а также имеет возможность искажать информацию, передаваемую между абонентами (модель активного нарушителя). Для защиты информации применяют различные специализированные протоколы безопасности, работающие на одном (или нескольких) уровнях модели ISO/OSI. Ниже представлен краткий перечень наиболее распространенных протоколов безопасности. Так, на канальном уровне работают протоколы PPTP, L2TP, L2F, на сетевом уровне работают протоколы IPv6 и IPSec, на транспортном уровне – протокол SSL/TLS и на прикладном – SSH, PGP, S/MIME. Для обмена ключевой информации в рамках одного или нескольких доменов применяют протокол Kerberos, в масштабах ГВС используют инфраструктуры обмена открытыми ключами PKI. Помимо этого, большинство протоколов передачи данных включают в себя возможность проведения аутентификации сторон прежде, чем будет установлен информационный канал связи.

Выбор протокола для защиты передаваемых данных диктуется необходимыми сервисами и возможностями предполагаемого нарушителя. Для защищенного обмена данными между сетями, расположенными удаленно друг от друга, или между абонентами и сетью, как правило, применяется семейство протоколов сетевого уровня IPSec. Защита данных на сетевом уровне обладает тем достоинством, что для транспортных и сеансовых протоколов работа по защите данных становится прозрачной. В этом случае нет необходимости создавать специальное ПО для защиты передаваемых данных протоколами верхних уровней.

Защищенная передача данных, реализуемая на транспортном уровне, используется преимущественно в модели клиент – сервер. Соответственно клиент и сервер должны поддерживать специальный протокол. Примером может служить протокол SSL и его модификация – TLS.

Выбор схемы для распределения ключевой информации зависит от модели нарушителя. Для модели с активным нарушителем подходят только те схемы, в которых участники информационного обмена заранее знают известный только им секрет, или у них есть общий доверенный посредник.

Большое распространение получили способы распределения ключей на основе протокола Kerberos и на основе инфраструктуры открытых ключей. Оба способа предполагают общего доверенного посредника, в роли которого выступает либо контроллер домена, либо удостоверяющий центр. Схема, основанная на предварительном знании общего секрета, предполагает административно-

организационное решение, когда, например, администраторы сети договариваются об используемом пароле или ключе.

Виртуальная частная сеть (VPN) – это технология, использующая криптографические механизмы для защищенной передачи данных по общей или выделенной сетевой инфраструктуре.

В общем случае технология VPN решает следующие задачи: организация связи между филиалами, подключение партнеров и клиентов, а также мобильных сотрудников к корпоративной СПД.

Термин «частная сеть» означает принадлежность оборудования сети предприятия и гарантию конфиденциальности информации, передаваемой по этой сети. Такие сети не очень распространены, гораздо чаще предприятие арендует каналы связи для своих филиалов.

При аренде каналов предприятие делит пропускную способность магистральных каналов с другими абонентами провайдера. Полоса пропускания арендованного канала полностью выделяется предприятию и является его собственностью. Корпоративные данные практически не доступны для абонентов, не являющихся пользователями корпоративной СПД или сети провайдера.

Также возможна организация VPN на базе ГВС Интернет, что, с одной стороны, имеет преимущества в простоте и низкой стоимости реализации, но вместе с тем не гарантирует заданной пропускной способности.

Выделяют следующие виды VPN: внутрикорпоративные (intranet VPN) – для организации связей с филиалами, удаленного доступа (remote access VPN) – для организации доступа к ресурсам компа-

нии сотрудников или клиентов, межкорпоративные (extranet VPN) – для организации связей с партнерами и клиентами.

В VPN для криптографической защиты данных на сетевом уровне предназначено семейство протоколов IPSec, обеспечивающее выполнение следующих задач: шифрование передаваемых данных, обеспечение их аутентичности и целостности, а также разграничение доступа (фильтрация IP-потоков) и защита от повторной передачи IP-дейтаграмм.

В состав семейства IPSec входят протокол аутентификации (AH), протокол шифрования (ESP) и протокол обмена ключами (IKE). Протокол IKE разработан на основе протоколов ISAKMP, Oakley и SKEME и предназначен для согласования используемых алгоритмов, ключей, продолжительности их действия и других параметров. Результатом такого согласования является *однонаправленная безопасная ассоциация* (security association – SA). Работа протокола IKE включает два этапа. Первый – идентификация и аутентификация сторон, установление защищенного канала для согласования параметров (результат – создание IKE SA). Второй – установление защищенного канала передачи данных.

Протоколы семейства IPSec могут работать в транспортном и туннельном режимах. В *транспортном режиме* заголовок исходной дейтаграммы остается неизменным, а в *туннельном режиме* происходит формирование нового IP-заголовка для AH или ESP-пакета.

Выделяют следующие основные варианты применения протокола IPSec: узел – узел, узел – сеть и сеть – сеть. При этом основными схемами включения VPN-шлюзов в сегменте LVP являются параллельная и последовательная.

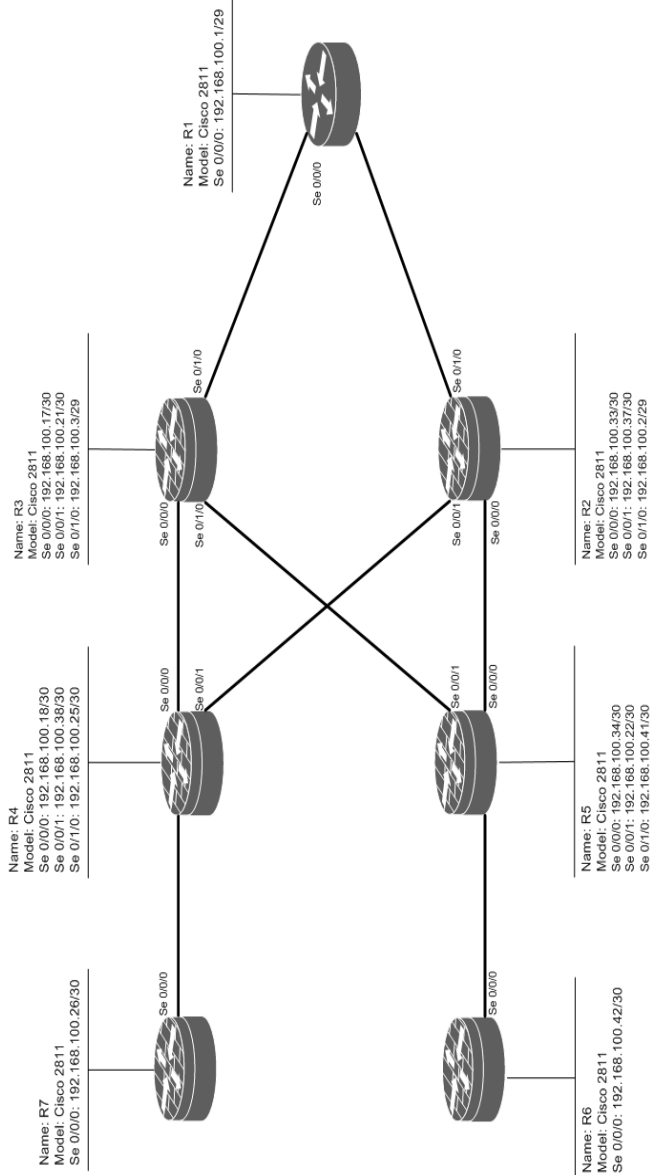


Рис 8. Схема организации виртуальной частной сети

Постановка задачи

Обеспечить криптографически защищенное подключение сетей филиалов к сети центрального офиса по арендуемым каналам передачи данных (рис. 8), а также криптографически защищенный удаленный доступ клиентов через ГВС Интернет к АС «Клиент – Банк» (рис. 9). Для обеспечения гарантий защиты каналов связи для подключения клиентов через ГВС Интернет использовать немаршрутизируемые IP-адреса инфраструктуры АС «Клиент-Банк». Централизованное управление доступом обеспечить путем использования протокола Radius и инфраструктуры AAA.

Последовательность действий

Шаг 1. Создать и настроить политику безопасности протокола ISAKMP со следующими параметрами: метод аутентификации – PSK, алгоритм шифрования – AES, алгоритм хэширования – SHA1, номер группы Диффи-Хеллмана – 5, длина вырабатываемого ключа – 1 536 бит:

```
crypto isakmp policy 10
  authentication pre-share
  encryption aes
  hash sha
  group 5
```

Задать ключи аутентификации маршрутизаторов по методу PSK:

```
crypto isakmp key B4H^3PdQ address Router_IP_address
```

Шаг 2. Создать и настроить политику криптографической защиты каналов передачи данных:

```
crypto ipsec transform-set WAN esp-aes esp-sha-hmac
```

Шаг 3. Определить защищаемые информационные потоки через механизм ACL:

```
ip access-list extended cryptoacl-wan  
permit ip 10.194.0.0 0.0.255.255 10.194.0.0  
0.0.255.255
```

Шаг 4. Настроить криптографическую карту шифрования информационных потоков на канале передачи данных между маршрутизаторами и инициализировать ее на внешнем интерфейсе:

```
crypto map WAN-map 10 ipsec-isakmp  
set peer Router_IP_address  
set transform-set WAN  
match address cryptoacl-wan  
interface se0/0/0  
crypto map WAN-map
```

Шаг 5. Выполнить настройки протокола IPSec на всех маршрутизаторах СПД.

Шаг 6. Выполнить настройки службы AAA и протокол Radius на VPN-концентраторе:

```
aaa new-model  
aaa authentication login ASCB group radius  
aaa authorization network ASCB local  
radius-server host 192.168.20.11 key Fhlewre$
```

Шаг 7. Создать и настроить политику ISAKMP:

```
crypto isakmp policy 10  
authentication pre-share
```

```
encryption aes
```

```
group 5
```

Шаг 8. Выделить диапазон выдаваемых IP-адресов для удаленных клиентов АС «Клиент-Банк»:

```
ip local pool ASCB 192.168.20.100 192.168.20.200
```

Шаг 9. Настроить параметры группы удаленного доступа:

```
crypto isakmp client configuration group ASCB
```

```
key ClientBankKey
```

```
pool ASCB
```

```
netmask 255.255.255.0
```

Шаг 10. Настроить политику криптографической защиты данных:

```
crypto ipsec transform-set CB esp-aes esp-sha-hmac
```

Настроить криптографическую карту шифрования потоков удаленного доступа:

```
crypto dynamic-map d-ASCB 10
```

```
set transform-set CB
```

```
crypto map s-ASCB client authentication list ASCB
```

```
crypto map s-ASCB isakmp authorization list ASCB
```

```
crypto map s-ASCB client configuration address respond
```

```
crypto map s-ASCB 10 ipsec-isakmp dynamic d-ASCB
```

Инициализировать криптографическую карту:

```
interface fa0/0
```

```
crypto map c-ASCB
```

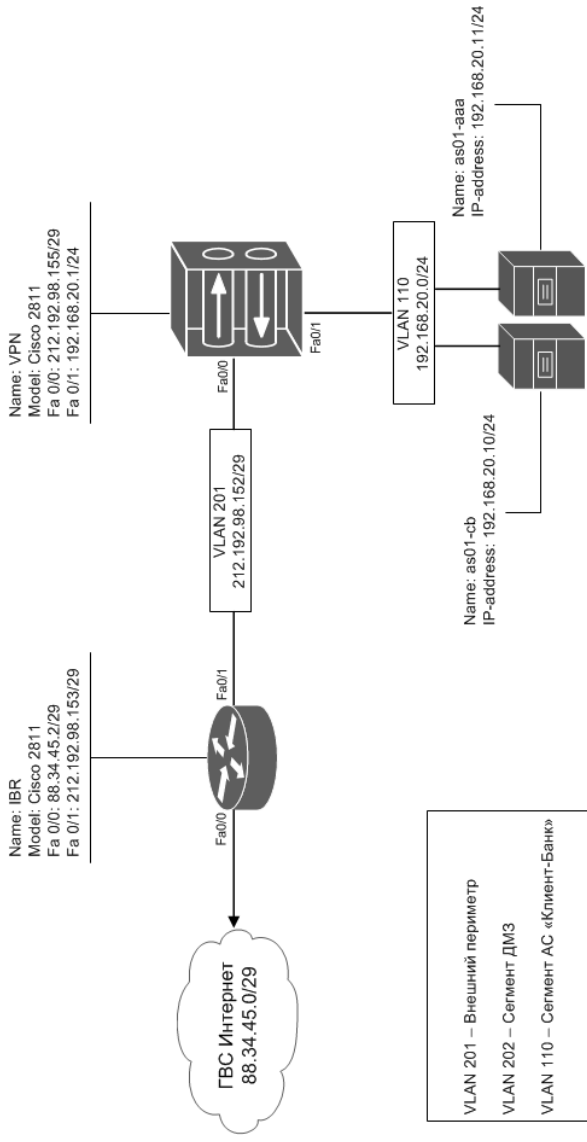


Рис. 9. Схема организации защищенного удаленного подключения к АС «Клиент-Банк»

Шаг 11. Проверить корректность функционирования СПД и доступность служб АС «Клиент-Банк». Изучить структуру зашифрованных сетевых пакетов. Проверить доступность АС центрального офиса при отказе каналов связи или сетевого оборудования.

Вопросы и задания

1. Изучить рекомендации к выбору параметров криптографической защиты протоколов IPSec.
2. Убедиться в невозможности доступа в сегмент АС «Клиент-Банк» из ГВС и корпоративной СПД без знания параметров и ключей криптографической защиты IPSec.

1.10. Защита беспроводной ЛВС

Цель работы

Целью лабораторной работы является иллюстрация применения базовых методов и средств защиты беспроводной ЛВС, являющейся частью корпоративной ЛВС.

Краткие теоретические сведения

В отличие от проводных сетей Ethernet, беспроводные ЛВС семейства стандартов IEEE 802.11 используют общедоступный радиоканал для связи с абонентами. Этот факт лежит в основе целого ряда новых проблем безопасности и приводит к тому, что в настоящее время беспроводные ЛВС в наибольшей степени, по сравнению с другими типами сетей, подвержены атакам.

В корпоративных сетях передачи данных элементы беспроводных ЛВС IEEE 802.11 (точки доступа, маршрутизаторы) используются, как правило, для расширения сетевой инфраструктуры. При анализе безопасности беспроводных ЛВС выделяют следующие основные угрозы:

- несанкционированное подключение к устройствам и сетям;
- неконтролируемое использование инфраструктуры;
- перехват и модификация данных;
- нарушение доступности;
- позиционирование устройства.

Основными механизмами обеспечения безопасности беспроводной ЛВС являются:

- базовые методы защиты и протоколы аутентификации IEEE 802.11i;
- управление доступом в соответствии со стандартом IEEE 802.1x;
- сегментирование сетей с помощью технологии VLAN;
 - управление доступом к сети на основе атрибутов пользователей и средств доступа;
- межсетевое экранирование и VPN;
- обнаружение и предотвращение вторжений на канальном уровне.

Стоит отметить, что все основные механизмы и средства безопасности беспроводных сетей ориентированы, как правило, на защиту канального уровня. Защита на более высоких уровнях сетевой модели реализуется на базе типичных для проводных сетевых КС механизмах.

При организации защищенной беспроводной ЛВС, как правило, отталкиваются от категории информации, передаваемой в сети и обрабатываемой на серверах или рабочих станциях, подключенных к этой сети. В зависимости от нее формируются требования безопасности, которым должна удовлетворять КС. Например, в сети могут быть выделены следующие сегменты беспроводной ЛВС, построенные в соответствии с различными требованиями безопасности: сегмент гостевого доступа к сети Интернет, сегмент доступа к сети Интернет с мобильных устройств сотрудников, сегмент доступа к веб-ресурсам общего назначения и сегмент для соединения двух ЛВС с помощью точек доступа.

Постановка задачи

Построить защищенный беспроводной сегмент ЛВС (см. рис. 10), расширяющий инфраструктуры ЛВС и позволяющий организовать подключение пользователей к ней с использованием механизмов WPA2.

Последовательность действий

Шаг 1. Выполнить подключение беспроводного маршрутизатора к ЛВС филиала.

Шаг 2. Выполнить настройки маршрутизатора WR04-1. Назначить устройству IP-адрес и маску сети из сети управления ЛВС филиала. Назначить SSID – «bank04», метод аутентификации – «WPA2», указать параметры подключения к серверу RADIUS (IP-адрес 192.168.4.1, shared secret – «Nh\$с@vv3», AES).

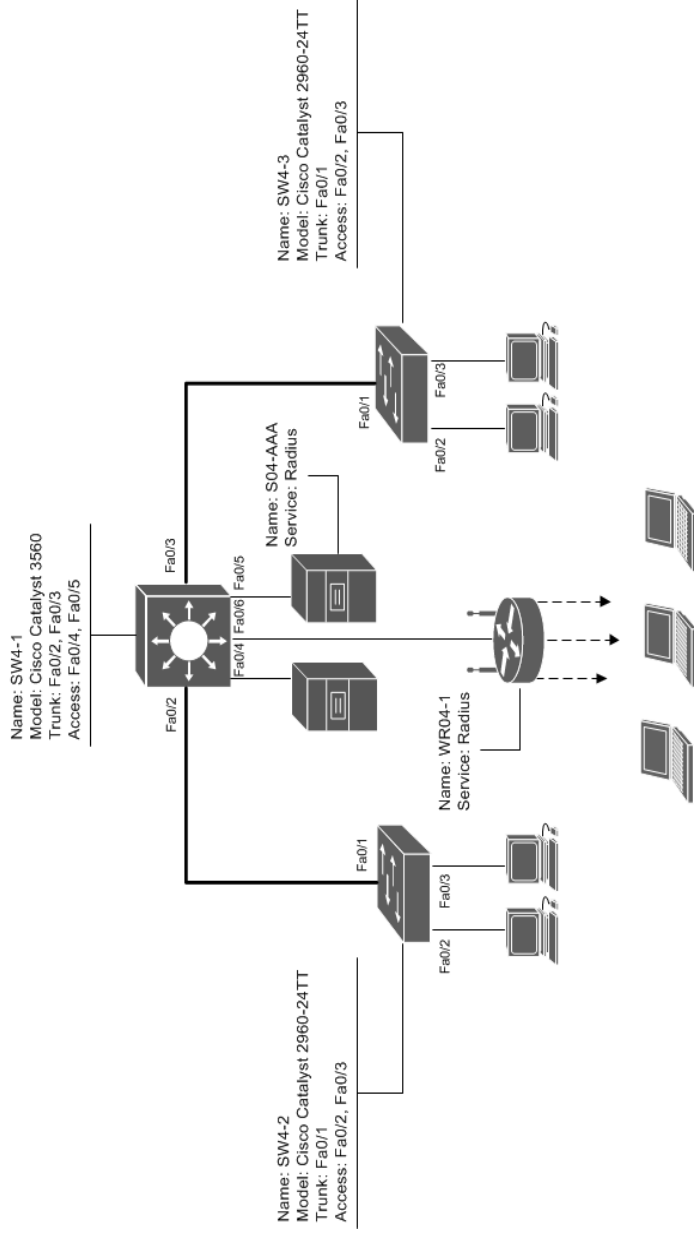


Рис. 10. Схема организации беспроводного сегмента ЛВС филиала

Шаг 3. На сервере S04-AAA создать клиента WR04-1, задать его сетевые параметры. Создать пользователя для подключения: UserName – «user», Password – «Miemnm2».

Шаг 4. На мобильной рабочей станции в параметрах беспроводного подключения указать параметры SSID, метод аутентификации, UserID и Password. Проверить возможность сетевого взаимодействия в ЛВС филиала и доступ к ГВС.

Вопросы и задания

1. Организовать дополнительный беспроводный сегмент ЛВС, предназначенный для гостевого доступа недоверенных пользователей в сеть Интернет. Обеспечить невозможность доступа из недоверенного сегмента в ЛВС филиала.

2. Изучить рекомендации и известные подходы к построению беспроводных ЛВС.

3. Предложить техническое решение (разработать схему) по организации доступа из беспроводного сегмента к ЛВС корпоративной сети с использованием технологий VPN.

2. ЛАБОРАТОРНЫЕ РАБОТЫ

ПО ИНСТРУМЕНТАЛЬНОМУ АНАЛИЗУ

ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

В соответствии с теорией компьютерной безопасности реализация угроз является возможной вследствие наличия уязвимостей в КС. Одним из механизмов защиты КС является анализ защищенности, понимаемый как процесс поиска уязвимостей. Среди множества подходов реализации данного механизма особое место занимает инструментальный анализ защищенности или сканирование уязвимостей, являющееся элементом более сложных методов, таких, как оценка уязвимостей, тестирование возможности проникновения, аудит и пр. В то же время механизмы, используемые при сканировании уязвимостей, могут использоваться как в других средствах защиты, например, в системах обнаружения вторжений, в системах контроля защищенности и соответствия стандартам или в системах управления безопасностью, так и в системах управления информационными технологиями, например, в системах мониторинга или в системах управления конфигурациями.

При инструментальном анализе защищенности, как правило, используются сканеры безопасности, которые позволяют найти известные уязвимости и распространенные ошибки путем моделирования широко известных сценариев атак. Сканером безопасности (сканером уязвимостей) принято называть программное или программно-аппаратное средство защиты информации, реализующее превентивный механизм – автоматизированное выявление уязвимостей.

Для обеспечения условий решения лабораторных работ по инструментальному анализу защищенности сети используется типовая структура учебной виртуальной ЛВС (рис. 11), моделирующая основные конфигурации корпоративных сетей, на базе ПО семейства VMWare и включающая следующие элементы:

- сервер S1 – сервер под управлением ОС Fedora Core Linux;
- сервер S2 – сервер под управлением ОС Microsoft Windows Server 2003;
- APM UWS1 – APM под управлением ОС Microsoft Windows XP;
- APM TWS1 – APM для тестирования безопасности на базе дистрибутива BackTrack Linux;
- APM TWS2 – APM сканирования уязвимостей на базе ПО XSpider.

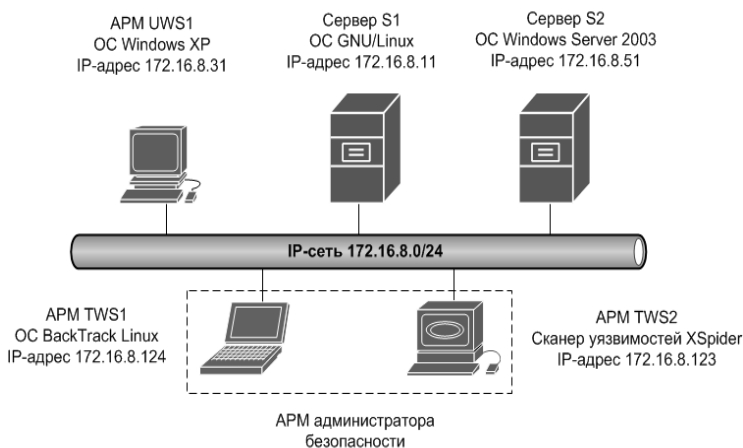


Рис. 11. Схема виртуальной сети

Следующие лабораторные работы ориентированы на изучение и исследование основных принципов, методов и средств инструментального анализа защищенности корпоративных. Работы выполняются с использованием сканера безопасности XSpider. В тоже время в случае отсутствия данного ПО могут быть использованы любые другие сканеры безопасности, например Nessus, Nexpose, Internet Scanner и др. или программные средства, позволяющие выполнить отдельные этапы сканирования: fping, hping, nmap, amap, xprobe, httpprint, smtpscan и т.д. Последние могут быть установлены отдельно на АРМ обучающегося или использованы в составе специализированных дистрибутивов Linux: Backtrack, Pentoo или nUbuntu.

2.1. Сбор предварительной информации

Цель работы

Целью лабораторной работы является обучение методам и средствам сбора предварительной информации в Интернет об анализируемой КС.

Краткие теоретические сведения

Одним из первых этапов анализа защищенности является сбор информации об исследуемой КС. В зависимости от используемой методологии анализа защищенности применяются различные методы сбора информации. Стоит отметить, что сбор предварительной информации о сети, как правило, не характерен для методологий инструментального анализа защищенности.

Методы сбора информации делятся на активные и пассивные. Активные методы требуют отправки запросов в КС и анализа ее ответов, а пассивные используют информацию, добровольно рассылаемую КС.

Активные методы делятся на методы с подключением (например, идентификация узлов) и методы без подключения к КС (например, сбор данных о диапазонах IP-сетей). Технология сбора данных о КС, без явного подключения к последним, носит название предварительное изучение цели (англ. footprinting).

В результате проведения сбора предварительной информации о сети могут быть получены:

- информация о доменах КС;
- данные об используемом системном и прикладном ПО;
- применяемые средства защиты информации;
- адреса электронной почты пользователей;
- адреса IP-сетей и др.

Исходной информацией для получения таких данных могут служить название организации, адреса электронной почты сотрудников, IP-адреса или DNS-имена узлов КС.

Методами получения необходимой информации являются:

- использование функционала поисковых систем (например, Google, Yandex, Bing) и оффлайн-браузеров (например, httrack);
- опрос серверов DNS и SMTP;
- опрос серверов регистраторов Интернет с помощью специализированных средств (например, whois) или веб-приложений сайтов, предоставляющих информацию регистрационного характера (например, www.ripn.net);

- использование веб-средств тестирования и диагностики сетей, предоставляемых операторами связи;
- использование специализированных средств сбора информации (например, SamSpade).

Постановка задачи

Выполнить предварительный сбор информации о домене tsu.ru. Работа выполняется на АРМ, имеющем доступ в сеть Интернет.

Последовательность действий

Шаг 1. Перейти по адресу <http://www.ripn.net/nic/whois>. Указать в строке поиска в базе данных РосНИИРОС домен tsu.ru. Проанализировать полученные данные. Найти DNS-имена и IP-адреса серверов имен. В строке поиска базы данных RIPE задать IP-адреса серверов имен. Определить диапазоны IP-адресов, выделенные организации. Проанализировать данные по администраторам и контактным лицам организации. Найти используемые почтовые адреса.

Шаг 2. Перейти по адресу <http://network-tools.com/nslookup>. Задать параметры: домен – tsu.ru, тип запроса – ANY. Определить почтовый сервер организации.

Шаг 3. Выполнить предыдущие проверки, используя средства nslookup, host и dig.

Шаг 4. Определить DNS-имена и роли узлов из выделенных диапазонов IP-адресов. Использовать веб-средства <http://dnsstuff.com> и <http://dnsreport.com>.

Шаг 5. Проверить наличие узлов найденных сетей в базах данных спам-отправителей и бот-сетях, используя для этого веб-

средства <http://www.spamcop.net>, <http://www.spamcop.net> и <http://rbls.org>.

Шаг 6. Проверить возможность выполнения переноса зоны на первичном и вторичном DNS-серверах:

```
C:\nslookup
>server ns.tsu.ru
>set type=any
>ls -d tsu.ru
```

Шаг 7. Перейти по адресу <http://google.ru>. Задать следующие поисковые запросы и проанализировать результаты:

- «site:tsu.ru filetype:docx для служебного пользования»;
- «site:tsu.ru filetype:doc для служебного пользования»;
- «site:tsu.ru filetype:doc секретно»;
- «site:tsu.ru filetype:doc *ФИО*».

Шаг 8. Выполнить метод анализа *mail bouncing*. Сформировать и отправить некорректные почтовые сообщения: сообщения на несуществующие адреса, сообщения, размер которых превышает допустимый и т.д. Проанализировать полученные ответы.

Шаг 9. Используя веб-инструмент *tracert*, расположенный на веб-ресурсе <http://network-tools.com>, определить маршруты прохождения IP-дейтаграмм до исследуемой сети.

Вопросы и задания

1. Предложить механизмы защиты для противодействия методам предварительного сбора информации о сети.
2. Собрать данные о номерах автономных систем исследуемой сети.

2.2. Идентификация узлов и портов сетевых служб

Цель работы

Целью лабораторной работы является обучение методам и средствам идентификации доступных узлов и сетевых портов в анализируемой КС.

Краткие теоретические сведения

Задача идентификации узлов сводится к тому, чтобы заставить удалённую систему отреагировать на какой-либо запрос. Под реакцией системы понимается генерация какого-либо ответа или сообщения об ошибке. Это и будет доказательством того, что система присутствует в сети. При этом задача состоит именно в доказательстве присутствия системы, а не в определении каких-либо её характеристик (работающие службы, операционная система и т. п.). Для решения этой задачи могут быть использованы различные методы, основанные на разных сетевых протоколах.

Основные методы идентификации:

- ICMP Ping;
- информационные сообщения ICMP;
- UDP Discovery;
- TCP Ping;
- IP probing;
- ARP Scan.

Метод ICMP Ping основан на использовании сообщений ICMP ECHO (Type 8) и ECHO REPLY (Type 0). Сканер отправляет на исследуемый узел сообщения ICMP ECHO (Type 8). Если узел

доступен и отсутствует фильтрация ICMP пакетов данного типа, то в ответ придёт сообщение ICMP типа ECHO REPLY.

В методе TCP Ping производится попытка установки соединения с каждым портом из заданного списка путем отправки сегмента TCP SYN. Если соединение установлено, т.е. в ответ был получен сегмент TCP SYN/ACK, то это означает, что исследуемый узел доступен, при этом соединение тут же разрывается посылкой сегмента TCP RST. Если соединение не установлено, но в ответ получен сегмент TCP RST, то это также означает доступность узла. Отметим, что некоторые сканеры безопасности, например, XSpider и LANGuard, в случае получения сегмента TCP SYN/ACK сначала устанавливают полноценное TCP-соединение, а затем его разрывают. Как правило, возможность использования оптимальной реализации метода TCP Ping связана с наличием генератора пакетов или возможностью использования интерфейса сырых сокетов (англ. raw sockets).

Метод TCP Ping является наиболее эффективным, так как ответ на отправленный сегмент будет получен, даже если исследуемый порт закрыт. Для обхода механизмов фильтрации сегментов TCP целесообразно выбирать часто используемые порты, например:

- SSH (22);
- SMTP (25);
- HTTP (80);
- RPC (135);
- NetBIOS (139).

В методе UDP Discovery на определенный UDP-порт отправляется дейтаграмма, адресованная соответствующей этому порту

службе. Если порт открыт, то будет получен ответ от службы, а если закрыт – сообщение ICMP Destination Unreachable (Port Unreachable). В данном методе могут быть использованы службы:

- DNS (53);
- NetBIOS (137);
- SNMP (161)
- ISAKMP (500).

Особенностью метода UDP Discovery является необходимость использования осмысленных запросов к службе для большей точности идентификации.

Методы группы IP probing представляют научный интерес, но, как правило, редко используются на практике и не реализованы в известных сканерах безопасности. Основная идея данных методов заключается в отправке некорректной IP-дейтаграммы на исследуемый узел КС. Если в ответ будет получено сообщение об ошибке ICMP типа Parameter problem, то устройство доступно. Отсутствие данного ответа не означает недоступность устройства. Достоинство данного метода заключается в том, что он потенциально может быть использован в обход межсетевых экранов.

Метод ARP Scan является самым быстрым, но может быть использован, только в том случае если исследуемый узел и сканер находятся в одном широковещательном домене 2-го уровня (т.е. в одном VLAN). Данный метод заключается в отправке ARP-запроса на получение MAC-адреса исследуемого узла. При этом можно гарантировать, что ответ будет получен тогда и только тогда, когда узел включен. Данный метод реализован в сетевом сканере NMap и средстве перехвата пакетов Caen&Abel.

Следующим этапом после идентификации доступных узлов является идентификация открытых портов. Известны следующие методы решения данной задачи:

- TCP Connect (Vanilla Scan);
- SYN Scan (полусканирование);
- UDP Scan;
- скрытое сканирование (FIN Scan, ACK Scan, XMAS Scan и др.);
- анонимное сканирование класса SSRF.

В методе TCP Connect с каждым TCP-портом штатными средствами ОС устанавливается, а затем разрывается соединение. Данный метод реализован во всех инструментальных средствах анализа.

Метод SYN Scan является оптимизацией предыдущего метода. Идея заключается в том, что полноценное TCP соединение здесь не устанавливается. Если в ответ на отправленный нами сегмент TCP SYN получен сегмент TCP RST, то порт закрыт; если получен сегмент TCP SYN/ACK, то порт открыт и для разрыва соединения требуется отправка сегмента TCP RST удаленной стороне. В результате имеем отправку не более двух TCP сегментов вместо четырех, как в методе TCP Connect.

По результатам сканирования TCP-портов может быть получен один из следующих статусов порта:

- порт открыт (получен TCP SYN/ACK);
- порт закрыт (получен TCP RST);
- порт заблокирован (ничего не получено);
- порт недоступен (порт открыт, но при обращении к сетевой службе этого порта ответы не приходят).

Скрытые методы сканирования портов TCP, заключающиеся в послышке сегментов TCP с нестандартными наборами флагов (например, SYN и FIN одновременно), в настоящее время являются не актуальными по двум причинам:

- применение данных методов легко обнаруживается системами обнаружения вторжений;
- межсетевые экраны с технологией инспекции состояний запрещают ретрансляцию таких сегментов.

Анонимные методы сканирования ориентированы на обеспечение невозможности определения сканирующего субъекта. К данным методам относят:

- сканирование с использованием команд FTP;
- сканирование по полю Identification протокола IP;
- сканирование с использованием анализаторов сетевых пакетов при нахождении сканирующего и сканируемого узлов в одной VLAN.

Задача идентификация открытых портов UDP решается следующим образом. На требуемый порт сканируемого узла отправляется UDP-дейтаграмма с пустым полем данных. Если в ответ было получено ICMP-сообщение «Destination Unreachable», то это означает, что порт закрыт. Неполучение ответной UDP-дейтаграммы говорит о том, что порт открыт. При этом ответ может не быть получен и по другим причинам:

- потеря дейтаграммы в силу отсутствия механизмов гарантированной доставки в протоколе UDP;
- фильтрация дейтаграмм UDP или ICMP.

Всё это приводит к тому, что в случае неполучения ответа от сканируемого узла нельзя быть уверенным в том, что порт открыт. Для снижения вероятности ложной идентификации открытых UDP портов могут использоваться следующие механизмы:

- изменение количества посылаемых UDP-дейтаграмм;
- изменение времени ожидания ответа;
- отправление на порт UDP запроса к соответствующей службе;
- использование портов часто используемых UDP-служб (например, портов 53, 135, 161).

Постановка задачи

Выполнить идентификацию узлов и открытых портов, используя механизмы протоколов ARP, ICMP, IP, TCP и UDP.

Последовательность действий

Шаг 1. Загрузить виртуальную машину TWS1. Войти в систему (логин: root, пароль: toot). Настроить сетевые интерфейсы. Запустить анализатор протоколов tcpdump или wireshark.

Шаг 2. Выполнить идентификацию узлов с помощью средства fping для сети 172.16.8.0/24. Просмотреть трассировку сканирования:

```
fping -g 172.16.8.0/24 -c 1
```

Шаг 3. С помощью сетевого сканера nmap выполнить идентификацию узлов методом ARP Scan. Просмотреть трассировку сканирования:

```
nmap -sn 172.16.8.0/24
```


Шаг 4. С помощью средства hping2 выполнить идентификацию узлов сети, используя ICMP-сообщения Information Request, Time Stamp Request, Address Mask Request. Например:

```
hping2 -C 13 172.16.8.31
```

Просмотреть трассировку сканирования. Сравнить ответы на запросы различных ОС. Составить таблицу.

Шаг 5. С помощью средств hping2 и nmap выполнить идентификацию узлов сети, используя методы UDP Discovery и TCP Ping. Например:

```
hping2 -2 -d 53 172.16.8.31
```

```
hping2 -d 53 172.16.8.31
```

```
nmap -PS -sU -p 111 172.16.8.31
```

Шаг 6. На узле TWS2 запустить сканер безопасности XSpider. Создать новый профиль, выбрав параметры ICMP ping и TCP ping, в секции «Сканер UDP сервисов» отключить опцию «Сканировать UDP порты», в секции «Сканер уязвимостей» отключить опцию «Искать уязвимости». Указать диапазон IP-адресов. Выполнить сканирование сети.

Шаг 7. На узле TWS1 с помощью сетевого сканера nmap выполнить идентификацию открытых TCP и UDP портов найденных узлов IP-сети 172.16.8.0/24, используя основные методы сканирования. Например:

```
nmap -sS -n 172.16.8.11
```

```
nmap -sS -n 172.16.8.51
```

Просмотреть трассировки сканирований. Проанализировать результаты.

Вопросы и задания

1. На серверах S1 и S2 ограничить доступ к некоторым сетевым службам. Повторно выполнить сканирование портов. Убедиться в изменении статусов портов.
2. Определить все возможные методы сканирования, доступные в средстве hping2.
3. Почему метод ARP SCAN не реализован в сканерах безопасности?
4. Выполнить идентификацию узлов методом IP Probing.

2.3. Идентификация служб и приложений

Цель работы

Целью лабораторной работы является обучение методам и средствам идентификации служб и приложений, соответствующих открытым сетевым портам анализируемой КС.

Краткие теоретические сведения

Идентификация служб и приложений является одной из самых важных задач при проведении инструментального анализа защищённости.

Данная задача заключается в определении сетевой службы (протокола), соответствующей найденному открытому порту и идентификации приложения, реализующего серверную часть этой службы. Не корректная, не точная или ошибочная идентификация службы или приложения может привести к ложным срабатываниям сканеров безопасности или систем обнаружения вторжений. Кроме того,

данные, полученные в ходе такого анализа, составляют значительную часть результатов инвентаризации ресурсов компьютерной сети.

Для идентификации служб и приложений, как правило, используются следующие основные методы:

- анализ заголовков («баннеров»);
- использование команд служб прикладного уровня;
- анализ особенностей функционирования служб прикладного уровня.

Первый метод заключается в анализе сообщения, выдаваемого сетевой службой узла при подключении к ней по заданному порту. Часто такие сообщения содержат информацию об используемой службе, вплоть до названия приложения и номера версии, а также могут содержать информацию об установленной на узле ОС. Недостатком метода является возможность ошибочной идентификации службы за счет произвольного изменения приветственных сообщений или их отключения.

Второй метод состоит в использовании команд службы прикладного уровня, ожидаемой на данном порту. Например, если на узле был найден открытый порт TCP с номером 21, то для проверки того, является ли запущенная на этом порту служба сервером FTP необходимо использовать команды, определенные в рамках FTP протокола: например, USER, PASS, PORT, PASV, LIST, HELP и др.

После идентификации службы выполняется определение приложения, реализующего серверную часть этой службы. Например, если на узле был найден открытый порт TCP с номером 25 и было определено, что это протокол SMTP, то далее необходимо опреде-

лить приложение, реализующее этот протокол на стороне сервера. Например, это может быть Sendmail, Postfix или MDAemon.

Идентифицировать приложение также можно по его сообщению, однако, чаще методы идентификации приложений основаны на анализе особенностей реализации той или иной службы.

Суть этих методов состоит в посылке запросов, которые немного отличаются от стандартов и спецификаций, в использовании редких или некорректных команд, опций или параметров и др. Например, работу SMTP-сервера определяют несколько ключевых стандартов: RFC 2821, RFC 1425, RFC 1985. Эти стандарты определяют команды, которые SMTP-клиент может выполнить, подключившись к серверу, обязательные возможности самого сервера, допустимые аргументы и данные.

Однако не все реализации серверов SMTP удовлетворяют этим требованиям. Последнее свойство и позволяет идентифицировать конкретное ПО. Например, программное средство smtpscan использует следующие особенности реализации почтовых служб:

- корректно заданная команда *MAIL FROM* без предварительно переданной команды *HELO*. Некоторые серверы позволяют это (возвращая код ошибки 220), другие запрещают (501 или 503);
- возможность выполнить команду *HELO* без указания имени домена;
- возможность использование команды *MAIL FROM* без постановки знака двоеточия, например, qmail позволяет использование такой записи, хотя стандарт это явно запрещает;

- возможность использования команды *MAIL FROM* с пустым адресом отправителя; все серверы должны это разрешать, но бывают исключения;

- некорректное задание адреса отправителя в команде *MAIL FROM*; некоторые серверы это запрещают, то есть проверяют существование указанного домена.

Другим распространённым методом идентификации почтовых серверов является проверка поддержки некоторых команд: например, *HELP*, *VERFY*, *EXPN*, *TURN*, *EHLO* и др.

Еще одним актуальным методом идентификации ПО серверов SMTP является, уже упоминаемый ранее в рамках сбора предварительной информации о сети, метод mail bouncing. Данный метод заключается в отправке некорректных почтовых сообщений в исследуемую ЭПС, и анализе полученных уведомлений о невозможности доставки писем или сообщений об ошибках. Примерами отправляемых некорректных сообщений являются:

- сообщение для незарегистрированных пользователей ЭПС;
- сообщение от незарегистрированных пользователей ЭПС;
- сообщения с вложенными файлами, размер которых превышает установленные ограничения;
- сообщения, содержащие сигнатуры вредоносного ПО, вложенные файлы, ссылки, почтовые адреса и др.

Постановка задачи

Выполнить идентификацию служб и приложений для открытых портов узлов исследуемой компьютерной сети.

Последовательность действий

Шаг 1. На узле TWS2 перейти в консоль XSpider. Создать новый профиль сканирования.

Шаг 2. Включить опцию ICMP ping, отключить опцию TCP ping, отключить опцию «Сканировать не отвечающие хосты», в секции «Сканер портов» задать параметр «Список портов» 1-200, в секции «Сканер уязвимостей» отключить опцию «Искать уязвимости».

Шаг 3. Запустить сканирование служб и приложений сервера S1. Проверить, что службы FTP, SMTP, HTTP и другие найдены и идентифицированы.

Шаг 4. На сервере S2 сменить номер порта для службы FTP на 25, сменить баннер службы FTP.

Шаг 5. Остановить службу SMTP, сменить номер порта для службы SMTP на 21. Ограничить доступ к службе SMTP со сканирующего узла. Перезапустить службы.

Шаг 6. С помощью средств telnet или netcat проверить состояние портов 21 и 25 на виртуальном узле. Убедиться, что баннер службы FTP изменился.

Шаг 7. Выполнить сканирование узла S2. Убедиться, что служба FTP корректно идентифицирована на 25-м порту. Убедиться, что порт 21 имеет статус «Заблокирован».

Шаг 8. Разрешить доступ к службе SMTP. Повторно выполнить идентификацию служб и приложений.

Шаг 9. На узле TWS1 с помощью сетевых сканеров nmap и amap выполнить идентификацию служб и приложений узлов S1 и S2:

```
nmap -sV 172.16.8.11
```

```
nmap -sV 172.16.8.51
```

```
amap 172.16.8.51 21
```

```
amap 172.16.8.51 25
```

Просмотреть трассировки сканирований. Проанализировать результаты.

Шаг 10. Выполнить идентификацию ЭПС узла S2 с помощью средства `smtpscan`:

```
smtpscan -p 21 172.16.8.51
```

```
smtpscan 172.16.8.51
```

Просмотреть трассировки сканирований. Изучить базу данных параметров ЭПС средства `smtpscan`, хранящуюся в файле *fingerprints*, и набор тестов в файле *tests*.

Шаг 11. Выполнить идентификацию веб-сервера узла S2 с помощью средств `httprecon` и `httpprint`, например:

```
httpprint -h 172.16.8.51
```

Шаг 12. Выполнить идентификацию произвольной службы сервера S1 с помощью средств для идентификации веб-серверов, например:

```
httpprint -h 172.16.8.11
```

Вопросы и задания

1. Изучить и реализовать на практике метод использования служб прикладного уровня для идентификации веб-серверов.

2. Изучить особенности метода анализа параметров повторной передачи для идентификации служб UDP.

3. Изучить особенности реализации механизмов идентификации служб и приложений в сканерах `nmap` и `amap`.

2.4. Идентификация операционных систем

Цель работы

Целью лабораторной работы является обучение современным методам и средствам идентификации ОС анализируемой КС.

Краткие теоретические сведения

Задача определения типа и версии ОС удаленного узла весьма актуальна при проведении анализа защищённости. Чем точнее идентификация ОС исследуемого узла, тем эффективнее может быть выполнена его проверка. Более того, в некоторых сканерах безопасности набор выполняемых проверок зависит от результатов идентификации ОС.

В настоящее время идентификация ОС основана на следующих основных методах:

- анализ заголовков, полей IP-дейтаграмм и набора открытых портов, характерных для каждой ОС;
- опрос стека TCP/IP, впервые реализованный в сканерах queso и nmap;
- анализ ICMP-дейтаграмм, впервые реализованный в сканере xprobe;
- анализ реализации таймеров в механизме повторной передачи протокола TCP;
- анализ значений полей IP- и TCP-пакетов, реализованный в сканере SinFP.

Точность определения ОС существенно зависит от наличия устройств нормализации сетевых пакетов, межсетевых экранов, си-

стем обнаружения вторжений, прокси-серверов и других сетевых средств защиты информации. Кроме того, серьезную задачу представляет собой распознавание ОС одного семейства.

Постановка задачи

Выполнить идентификацию ОС узлов сети и анализ возможностей сетевых сканеров.

Последовательность действий

Шаг 1. Загрузить виртуальную машину TWS1. Войти в систему (логин: root, пароль: toot). Настроить сетевые интерфейсы. Запустить анализатор протоколов tcpdump или wireshark.

Шаг 2. С помощью утилиты hping2 исследовать значения полей TTL в IP-заголовке и Window в TCP-заголовке для ОС семейства GNU/Linux и Windows соответственно:

```
hping2 -S -c 1 -p 80 172.16.8.11
```

```
hping2 -S -c 1 -p 25 172.16.8.51
```

Шаг 3. С помощью сетевого сканера nmap выполнить идентификацию ОС методом опроса стека TCP/IP:

```
nmap -O 172.16.8.51 -vv
```

```
nmap -O 172.16.8.11 -vv
```

Исследовать используемые тесты и механизмы сетевого сканера nmap. Проанализировать результаты.

Шаг 4. С помощью сетевого сканера xprobe выполнить идентификацию ОС с использованием опроса модуля ICMP:

```
xprobe2 172.16.8.11
```

```
xprobe2 -v 172.16.8.51
```

Проанализировать результаты сканирования, сравнить с результатами использования сканера Nmap. Проанализировать трассировки.

Шаг 5. Выполнить шаги 3 и 4, настроив МЭ серверов S1 и S2 на фильтрацию некоторых используемых портов и протоколов.

Шаг 6. На узле TWS2 перейти в консоль XSpider. Обратить внимание на результаты определения ОС в ходе предыдущих сканирований. В используемом профиле сократить диапазон портов до 1–30 и выполнить повторное сканирование. Убедиться, что ОС не определена. Прокомментировать данные результаты.

Шаг 7. В профили сканирования включить опции «Искать уязвимости», «Искать скрытые каталоги». Выполнить сканирование. Убедиться в том, что ОС идентифицирована.

Шаг 8. Определить методы, использованные сканером XSpider для идентификации ОС в процессе сканирования, путем изучения трассировок и файлов регистрации сканирования.

Вопросы и задания

1. Перечислить отличия методов идентификации ОС, реализованные в сетевых сканерах nmap, xprobe, sinfp и сканерах безопасности XSpider, Nessus и Nexpose.

2. Изучить реализацию методов идентификации ОС в сетевых сканерах nmap, xprobe и sinfp.

3. Перечислить методы идентификации ОС, которые могут быть выполнены стандартными сетевыми средствами (командами) ОС (например, telnet, ssh, ping).

2.5. Идентификация уязвимостей сетевых приложений по косвенным признакам

Цель работы

Целью лабораторной работы является обучение методам и средствам идентификации уязвимостей по косвенным признакам в сетевых приложениях КС.

Краткие теоретические сведения

Уязвимостями КС принято называть любые их характеристики и свойства, использование которых нарушителем может привести к реализации угрозы. Существует множество вариантов классификации уязвимостей, например, по уровню инфраструктуры КС, по этапу жизненного цикла КС, по типу уязвимости и т.д.

В настоящее время информация об обнаруженных уязвимостях достаточно систематизирована, существует несколько общеизвестных источников, где эта информация представлена, например:

- <http://xforce.iss.net> – база данных компании IBM Internet Security Systems;
- <http://www.kb.cert.org/vuls> – база данных координационного центра CERT;
- <http://www.securityfocus.com/bid> – информация об обнаруженных уязвимостях с подробными пояснениями;
- <http://www.ptsecurity.ru/lab/advisory> – база данных ЗАО «Позитив Текнолоджис»;
- <http://www.securitylab.ru/vulnerability>;
- <http://www.securitytracker.com>.

Общепринятая система обозначений уязвимостей представлена в двух каталогах:

- <http://cve.mitre.org/cve>;
- <http://nvd.nist.gov>.

Инструментальный анализ защищенности, как правило, включает от автоматизированный поиск уже известных уязвимостей в КС или, иначе, сканирование уязвимостей с помощью проверок, выполняемых сканером безопасности. Все проверки делятся на заключения и тесты.

Заключение (логический вывод) – это алгоритм определения наличия уязвимости в КС без выполнения атаки, использующей данную уязвимость, по косвенным признакам, на основе собранной информации. Иначе говоря, вывод о наличии уязвимости в КС делается на основе каких-либо характерных признаков (номер версии службы, версия ОС, присутствие на узле какого-либо файла и т.п.). При этом используются данные, полученные на этапах идентификации открытых портов, служб, приложений в КС. Среди заключений выделяют локальные и «баннерные» проверки.

Тест – это алгоритм определения наличия уязвимости в КС путём выполнения атаки, использующей данную уязвимость, либо путём специальных запросов в отношении КС, позволяющих с высокой степенью вероятности утверждать о наличии уязвимости.

Таким образом, сканирование уязвимостей – это выполнение набора проверок, состоящих из тестов и заключений.

Сетевые службы и реализующие их приложения являются одним из основных объектов анализа защищённости, выполняемого сетевыми сканерами. После того, как в ходе сбора данных были опреде-

лены открытые порты, соответствующие им службы и реализующие их приложения, начинается этап идентификации уязвимостей. Значительная часть проверок, направленных на выявление уязвимостей сетевых служб, таких, как DNS, HTTP, SSH, FTP – это «баннерные» проверки.

В силу того, что результат «баннерных» проверок зависит от многих факторов, при «верификации» найденных уязвимостей рекомендуется использовать следующие приёмы:

- ручная проверка службы (подключение на заданный порт, анализ баннера, использование команд прикладного уровня);
- поиск информации об уязвимости в различных базах;
- локальная проверка (версия, конфигурационные файлы);
- проверка действительного существования уязвимости.

Данный вариант инструментального анализа защищенности в зарубежной литературе часто называется оценкой защищенности.

Постановка задачи

Выполнить идентификацию уязвимостей сетевых служб DNS, HTTP и SSH по косвенным признакам с помощью сканера XSpider.

Последовательность действий

Шаг 1. Создать профиль сканирования «Сканирование Apache». Перечень сканируемых портов ограничить портом 80. Отключить сканирование служб UDP, в секции «Определение уязвимостей» отключить опции «Использовать финальные проверки», «Проверять на известные DoS-атаки», «Проверять на новые DoS-атаки».

Шаг 2. В секции «HTTP» включить опцию «Включить анализатор директорий», остальные опции отключить. В секции «Анализатор контента» включить опцию «Не выходить за пределы стартовой страницы». В секции «Анализатор сценариев» оставить опцию «Искать уязвимости в GET запросах», отключить остальные опции. В секциях «Типы уязвимостей» и «Методы поиска» отключить все опции. В секции «Подбор учётных записей» отключить опцию «Подбирать учётные записи». Сохранить профиль.

Шаг 3. Создать задачу «Сканирование Linux», добавить в нее узел S1. Запустить на сканирующем узле анализатор протоколов. Выполнить сканирование узла S1. Обратить внимание на уязвимости, найденные на порту 80 веб-сервера Apache, а также на результаты идентификации службы HTTP. Найти результаты работы анализатора каталогов. Проверить наличие найденных уязвимостей вручную. Просмотреть трассировку сканирования в анализаторе протоколов.

Шаг 4. Войти в ОС GNU/Linux сервера S1 (логин: root, пароль: 111111). Открыть для редактирования файл /etc/httpd/conf/httpd.conf. Найти директиву ServerTokens и присвоить ей значение ProductOnly. Перезапустить службу httpd, выполнив команду:

service httpd reload

Шаг 5. Выполнить повторное сканирование сервера S1. Проанализировать результаты. Обратить внимание на результаты идентификации приложения.

Шаг 6. Открыть для редактирования файл /etc/httpd/conf/httpd.conf и закомментировать директиву ServerTo-

kens. Перезапустить службу httpd. Вновь выполнить сканирование, проанализировать результаты.

Шаг 7. Создать копию профиля «Сканирование Apache», задать ему имя «Сканирование сетевых служб». Перечень сканируемых портов ограничить портами 22 и 53. В секции «Сканер UDP-сервисов» отключить все опции, кроме DNS. Сменить профиль для задачи «Сканирование Linux».

Шаг 8. Убедиться, что на сервере S1 служба DNS запущена. Выполнить сканирование сервера S1. Просмотреть результаты, обратить внимание на уязвимость CVE-2008-1657, изучить её описание. Определить версию ПО SSH командой:

```
ssh -v
```

Просмотреть описание уязвимости в базе securityfocus. Сравнить номера версий, сделать вывод о действительном существовании уязвимости.

Шаг 9. Войти в ОС GNU/Linux сервера S1 (логин: user, пароль: abc123). Вывести содержимое какого-либо каталога, например, /tmp. Создать каталог .ssh, в нем создать файл rc и вписать туда команду «ls /tmp». Выполнить команду:

```
ssh localhost
```

Проверить, что при входе выполняется команда, указанная в файле ~/.ssh/rc.

Шаг 10. Выйти из ОС. Войти в ОС с правами учетной записи root. Отредактировать файл /etc/ssh/sshd_config, добавив в конец файла строку ForceCommand ls /usr. Перезапустить службу SSH. Выйти из ОС. Войти в ОС с правами учетной записи user. Выполнить команду:

ssh localhost

Убедиться, что после входа выполняются обе команды, при этом пользовательская команда выполняется первой.

Шаг 10. Проанализировать результаты сканирования службы DNS, обратить внимание на версию BIND. Выполнить ручную проверку наличия уязвимостей, используя средство nslookup:

```
C:>nslookup  
>server 172.16.8.11  
>set class=chaos  
>set test=txt  
>version.bind
```

Выполнить запрос authors.bind:

```
>authors.bind
```

Проверить версию ПО bind, выполнив команду:

```
named -v
```

Проверить установленную версию пакета bind:

```
rpm -q bind
```

В файле /var/named/chroot/named.conf вписать строку version. Перезапустить службу DNS:

```
service named restart
```

Проверить работу команды version.bind. Выполнить повторное сканирование. Просмотреть результаты, обратить внимание на результат определения версии bind.

Вопросы и задания

1. Объяснить отсутствие в результатах последнего сканирования службы DNS ранее найденных уязвимостей.

2.6. Идентификация уязвимостей на основе тестов

Цель работы

Целью лабораторной работы является обучение методам и средствам идентификации уязвимостей на основе тестов.

Краткие теоретические сведения

В случае идентификации уязвимостей на основе тестов в отношении КС запускаются реальные атаки, выполняющиеся при помощи эксплойтов.

Эксплойтом принято называть документированный метод или программу, использующую уязвимость. Во многих известных базах уязвимостей содержатся инструкции или код для использования опубликованных там уязвимостей.

Среди тестов выделяют простые эксплойты, а также тесты проверки возможности запуска кода, исчерпания ресурсов и подбора пароля. К первым относят эксплойты, использующие уязвимости служб КС и позволяющие выполнять произвольные команды ОС через некорректно сформированные запросы. Примером такого эксплойта является использование уязвимости CVE-2000-0886.

Тесты, проверяющие возможность запуска кода, используют уязвимости, делающие возможным создание ситуации переполнения буфера. Ситуация переполнения буфера создаётся путём отправки уязвимой сетевой службе специальным образом сформированных данных. При их обработке происходит изменение хода выполнения программы и передача управления произвольному коду, что может привести:

- к запуску кода, выполняющего какие-либо действия, например, делающего возможным последующие подключения к объекту атаки с получением командной строки ОС;

- к выведению из строя узла или уязвимой сетевой службы.

Как правило, использование теста отличается от запуска настоящего эксплойта тем, что в качестве результата возвращается какой-либо код вместо, например, предоставления командной строки или выполнения произвольных команд ОС. Механизмы проверки на возможность реализации DoS-атаки отправляют на вход тестируемой службы различные значения. Если переданное сканером значение параметра привело к выведению из строя сканируемой службы, проверка заканчивается положительным результатом.

Следующим видом тестов является подбор пароля. Подбор пароля осуществляется путём подключения к соответствующей сетевой службе. Известны следующие методы подбора паролей:

- атака по словарю – наиболее быстрый способ, при котором используются наиболее распространённые слова из словаря;

- гибридная атака – к словам из словаря добавляются подстановки последовательностей букв или цифр (cisco1, cisco2), иногда буквы слова из словаря заменяются цифрами или спецсимволами (c1sc0, r00t).

- атака грубой силы – перебор всех возможных вариантов паролей.

Оценка стойкости паролей может выполняться как на уровне узла, так и на уровне сети. В последнем случае для сканера безопасности эта задача превращается в попытки удалённого подбора паролей, что имеет следующие недостатки:

- низкая скорость перебора;
- возможность блокировки учётных записей пользователей.

Поэтому в сканерах безопасности сетевого уровня подбор паролей обычно ограничивается именами и паролями по умолчанию (наиболее распространёнными комбинациями) и подбором по словарю.

Рассмотрим методы подбора учетных записей и паролей в сканере безопасности XSpider. Соответствующие механизмы сканера реализованы для следующих сетевых служб:

- протоколы ЭПС (SMTP, POP3);
- службы передачи файлов (NetBIOS/SMB, FTP, HTTP);
- протоколы удаленного управления (TELNET, SNMP, SSH, RDP, RADMIN, VNC);
- СУБД (Microsoft SQL, Oracle, MySQL).

Справочники, используемые в ходе подбора учётных записей, могут быть трёх типов:

- пароли;
- логины (имена пользователей);
- комбинированные.

Для большинства сетевых служб подбор учётных записей осуществляется с использованием двух словарей: логинов и паролей. Для некоторых сервисов подбор осуществляется по комбинированному словарю, например, для службы RDP.

В ходе выполнения проверок по подбору пароля, как правило, используется следующая последовательность действий:

1. Обнаружение и идентификация сетевой службы, для которой задействован подбор паролей.
2. Построение списка учётных записей.
3. Выбор механизма аутентификации из числа поддерживаемых объектом сканирования.
4. Подбор пароля.

В ходе идентификации служб и приложений сканер XSpider обнаруживает сетевую службу, для которой необходимо выполнить подбор паролей. Затем строится список учетных записей, для которых будет производиться подбор паролей. Этот список формируется на основе встроенных данных, словарей логинов (если эта опция задействована) и ранее обнаруженных «логинов».

Для сбора учетных записей пользователей могут использоваться различные механизмы, такие, как «нулевой сеанс» в ОС семейства Windows.

Далее сканер определяет поддерживаемый объектом сканирования механизм аутентификации. Если поддерживается несколько методов, то выбирается наиболее эффективный с точки зрения подбора.

Последний этап представляет собой непосредственно подбор пароля. Результаты проверок передаются между модулями сканерами безопасности для различных протоколов. Например, если при работе с NetBIOS был получен список пользователей и подобран пароль для пользователя *user*, то эти данные будут использованы в ходе подбора паролей к службе RDP данного сервера.

Постановка задачи

Выполнить идентификацию уязвимостей и подбор учетных записей с использованием сканера безопасности XSpider.

Последовательность действий

Шаг 1. Добавить новый справочник типа «Логины» и вписать в него только один логин – «administrator». Добавить новый справочник типа «Пароли» и вписать в него несколько паролей, включая «1111». На сервере S2. Включить аутентификацию для службы SMTP.

Шаг 2. Создать новый профиль сканирования с именем «BruteForce». Перечень сканируемых портов ограничить портами служб FTP (21) и SMTP (25). Отключить сканирование служб UDP, в секции «Определение уязвимостей» отключить опции «Использовать финальные проверки», «Проверять на известные DoS-атаки», «Проверять на новые DoS-атаки».

Шаг 3. В секции «Сканер уязвимостей» – «Определение уязвимостей» – «FTP» отключить опцию «Искать скрытые директории». Включить опцию «Подбирать учётные записи», выбрать ранее созданные словари логинов и паролей. Сохранить профиль сканирования.

Шаг 4. Создать новую задачу «Подбор паролей», выбрав созданный ранее профиль сканирования «BruteForce». Выполнить сканирование сервера S2. Проанализировать результаты. Убедиться в подборе пароля к службам FTP и SMTP.

Шаг 5. Создать профиль сканирования «DoS». В список сканируемых портов добавить TCP порты 21 и 25. Отключить сканирова-

ние служб UDP. Включить опции «Искать уязвимости». В секции «Определение уязвимостей» включить опции «Использовать финальные проверки», «Проверять на известные DoS-атаки». Отключить опцию «Подбирать учетные записи».

Шаг 6. Создать задачу «Финальные проверки», используя профиль «DoS». Выполнить сканирование сервера S2. Проанализировать результаты.

Шаг 7. Проверить возможность доступа с сервера S1 к серверу S2. На сервере S2 выполнить команды:

```
cd /root/soft/hack/icmp-reset  
./icmp-reset
```

Шаг 8. С узла TWS2 установить соединение с объектом сканирования, выполнив команду:

```
telnet 172.16.8.51 25
```

Проверить работоспособность службы, набрав несколько команд соответствующего протокола. Запустить ещё один экземпляр командной строки. Вывести параметры текущих соединений и найти среди них сессию с сервером S2. Определить порт клиента (*s*). На сервере S1 запустить программу `icmp-reset` с параметрами:

```
./icmp-reset -c 172.16.8.123:s -s 172.16.8.51:25
```

Перейти в командную строку на узле TWS2. Попытаться набрать команду в установленном с сервером соединении. Убедиться, что соединение разорвано.

Вопросы и задания

1. Изучить и объяснить механизм DoS-атаки, используемой для разрыва соединения с сервером S2.

2.7. Особенности идентификации уязвимостей ОС Windows

Цель работы

Целью лабораторной работы является обучение основным методам и средствам сканирования уязвимостей ОС Windows.

Краткие теоретические сведения

В ОС семейства Windows имеются следующие основные сетевые службы и протоколы:

- RPC (TCP/135, UDP/135);
- разрешения имен NetBIOS (UDP/137);
- дейтаграмм NetBIOS (UDP/138);
- сессий NetBIOS (TCP/139);
- SMB (TCP/445, UDP/445).

Локальные проверки, выполняемые сканером безопасности, используют метод выявления уязвимостей на основе заключений. При этом модуль сканера безопасности устанавливается на исследуемом узле или подключается к нему с использованием учетной записи с административными привилегиями, что в свою очередь позволяет:

- осуществлять мониторинг обновлений ОС Windows;
- реализовать инвентаризацию установленного ПО;
- анализировать настройки ОС и приложений;
- выполнять проверки учетных записей и групп.

В ходе такого сканирования осуществляется доступ к различным объектам ОС и инфраструктуры Microsoft, например:

- системный реестр;
- файловая система;

- системные RPC-функции.

В сканере безопасности XSpider для выполнения данных проверок используются механизмы получения доступа к перечисленным объектам, основанные на сетевых службах и протоколах ОС семейства Windows и называемые транспортом. Транспорт «Использовать реестр через RPC» используется для получения доступа к реестру сканируемого узла через службу «Удаленный реестр».

Транспорт «Использовать файловые проверки через RPC» основан на подключении к административным общим ресурсам (например, C\$, ADMIN\$). При этом сканер безопасности получает доступ к файловой системе и может контролировать наличие необходимых обновлений, а также производить инвентаризацию установленного ПО.

Для выполнения системных проверок требуется обеспечить ряд условий:

- сетевое подключение к узлу на требуемый порт TCP;
- доступ через сетевое подключение к соответствующей службе ОС;
- достаточный уровень привилегий для учётной записи, используемой при подключении.

Для подключения к узлу в режиме аудита используются следующие протоколы прикладного уровня:

- Server Message Block (SMB);
- LDAP;
- протоколы, основанные на RPC.

Наличие обновлений проверяется путём удалённого доступа к реестру и файловой системе сканируемого узла. Следовательно, на сканируемом узле для успешного выполнения этих операций должна работать служба «Удаленный реестр». Кроме того, для получения доступа к файловой системе сканеру необходимо наличие служебных общих ресурсов, в частности, ресурс ADMIN\$ позволяет проверить атрибуты файлов в каталоге %SYSTEMROOT%\System32.

Постановка задачи

Выполнить идентификацию уязвимостей ОС Windows сервера S2 с использованием сканера безопасности XSpider.

Последовательность действий

Шаг 1. Создать профиль «Сканирование Windows». Список портов ограничить значениями 135, 139, 445. В разделе «Сканер UDP-сервисов» выбрать «Сканировать UDP-порты» и указать порты служб NTP, Microsoft RPC и NetBIOS Name. Отключить подбор учетных записей. Запустить анализатор протоколов tcpdump или Wireshark.

Шаг 2. Создать задачу «Сканирование Windows», указать сервер S2 в качестве объекта сканирования. Выполнить сканирование, проанализировать результаты. Просмотреть трассировку сканирования.

Шаг 3. На сервере S2 создать учетную запись «auditor» с паролем «1234567890abcde». Созданного пользователя включить в группу администраторов.

Шаг 4. В консоли сканера XSpider открыть вкладку «Учетные записи». Создать учетную запись «Аудит сервера Windows», указать пароль. Включить в профиле опцию «Расширенная проверка Windows» и выбрать созданную учётную запись. Указать транспорты. Сохранить профиль и выполнить повторное сканирование. Обратить внимание на общее число найденных уязвимостей и статусы транспортов. Проанализировать найденные уязвимости приложений и учетные записи.

Шаг 5. На сервере S2 отключить службу «Remote Registry». Провести повторное сканирование. Проанализировать результаты. Просмотреть статусы транспортов.

Шаг 6. На сервере S2 включить службу «Remote Registry» и отключить административные общие ресурсы C\$ и ADMIN\$. Провести повторное сканирование. Проанализировать результаты, сравнить их с результатами предыдущих сканирований. Просмотреть статусы транспортов.

Вопросы и задания

1. Проанализировать трассировки сканирований и изучить механизмы стека протоколов NetBIOS.
2. Собрать информацию о сети используя стандартные средства ОС семейства Windows.
3. Используя стандартное программное средство nbtstat ОС семейства Windows собрать доступную информацию о MAC-адресах, запущенных службах, пользователях системы.

2.8. Сканирование уязвимостей СУБД Oracle

Цель работы

Целью лабораторной работы является обучение основным методам и средствам сканирования уязвимостей СУБД Oracle.

Краткие теоретические сведения

В сканере безопасности XSpider СУБД рассматривается как сетевая служба, в отношении которой выполняется анализ заголовков.

В СУБД Oracle имеется как минимум одна сетевая служба, которая обеспечивает ее сетевую поддержку и всегда запущена – TNS Listener. Данная служба представляет собой отдельный процесс, принимающий клиентские запросы, передаваемые для обработки соответствующему серверному процессу СУБД.

Сетевой сканер, выполняя анализ защищённости службы Listener, проверяет следующие параметры защиты:

- локальная аутентификация на уровне ОС;
- защита паролем;
- опция ADMIN_RESTRICTIONS.

Локальная аутентификация на уровне ОС включается путём добавления параметра LOCAL_OS_AUTHENTICATION в файл listener.ora. Если значение этого параметра установлено в положение ON, управлять сервисом Listener можно только локально, с консоли сервера.

Начиная с версии СУБД Oracle 10g R1, локальная аутентификация на уровне ОС включена по умолчанию.

Если локальная аутентификация выключена, управлять сервисом Listener можно удалённо. В общем случае удалённо можно выполнить следующие действия:

- получить детальную информацию о системе с помощью команды status;
- остановить службу Listener с помощью команды STOP;
- внести изменения в систему с помощью команды SET.

Опция ADMIN_RESTRICTIONS запрещает удалённое выполнение команды SET, а защита паролем ограничивает получение детальной информации о системе и выполнение команд.

Постановка задачи

Выполнить сканирование уязвимостей СУБД Oracle с помощью сканера безопасности XSpider.

Последовательность действий

Шаг 1. Создать профиль сканирования «СУБД Oracle». Список сканируемых портов ограничить значением 1521. Отключить подбор учетных записей и сканирование служб UDP.

Шаг 2. Запустить сканирование сервера S2 в рамках созданного профиля. Просмотреть результаты. Обратит внимание на статус проверки «Локальная аутентификация на уровне ОС». Объяснить невозможность удаленного сбора информации о службах СУБД Oracle.

Шаг 3. На сервере S2 открыть для редактирования файл listener.ora. Присвоить параметру LOCAL_OS_AUTHENTICATION значение OFF. Перезапустить службу Listener. Запустить повторное

сканирование сервера S2. Проанализировать результаты. Обратить внимание на то, что локальная аутентификация отключена.

Шаг 4. На APM TWS2 установить ПО Oracle Client. Выполнить перезагрузку. В профиле сканирования включить подбор учетных записей. Проверить, что включены опции «Подбирать учётные записи для БД Oracle», «Подбирать пароли для указанных» и указать имя экземпляра testdb. Выполнить повторное сканирование сервера S2. Проанализировать результаты.

Вопросы и задания

1. Предложить перечень мер по устранению найденных уязвимостей СУБД Oracle сервера S2.

2.9. Сканирование уязвимостей веб-приложений

Цель работы

Целью лабораторной работы является изучение основных методов и средств идентификации уязвимостей веб-приложений, реализованных в сканерах безопасности общего назначения.

Краткие теоретические сведения

Как правило, при анализе защищенности веб-приложений сканеры безопасности используются в следующих целях:

- поиск «грубых» ошибок, допущенных разработчиком или администратором приложения;
- поиск хорошо известных уязвимостей;
- проверка пропуска уязвимостей в процессе ручного тестирования.

Специализированные сканеры безопасности способны идентифицировать хорошо известные уязвимости веб-приложений или, по крайней мере, облегчить работу по их поиску. В меньшей мере такой способностью обладают сканеры безопасности общего назначения.

В настоящее время существует несколько классификаций уязвимостей веб-приложений. Наиболее структурированными из них являются классификации сообществ Open Web Application Security Project (OWASP) и Web Application Security Consortium (WASC).

В рамках проекта OWASP предложен список десяти наиболее часто встречающихся проблем безопасности веб-приложений OWASP TOP 10 – 2013:

1. Внедрение кода (Injection).
2. Ошибки в реализации функций аутентификации и управления сессиями (Broken Authentication and Session Management).
3. Межсайтовое выполнение сценариев (Cross-Site Scripting, XSS).
4. Незащищенные прямые ссылки на объекты (Insecure Direct Object Reference).
5. Ошибки в настройке механизмов защиты (Security Misconfiguration).
6. Утечка конфиденциальных данных (Sensitive Data Exposure).
7. Ошибки в управление доступом к функциям (Missing Function Level Access Control).
8. Подделка запросов HTTP (Cross Site Request Forgery, CSRF).
9. Использование компонент с известными уязвимостями (Using Components with Known Vulnerabilities).

10. Непроверенное перенаправление (Unvalidated Redirects and Forwards).

Рассмотрим методы и механизмы сканирования уязвимостей веб-приложений, реализованные в сканере безопасности XSpider.

В рамках анализа защищенности веб-приложений сканер безопасности XSpider имеет следующие основные возможности:

- автоматическое определение веб-приложений на произвольных портах;
- работа с протоколами семейства SSL/TLS;
- автоматическая индексация веб-сайта с поддержкой функции поиска скрытых директорий и резервных копий файлов;
- поддержка аутентификации Basic и нестандартных схем аутентификации;
- автоматическое отслеживание сессий;
- поиск уязвимых и вредоносных сценариев (например, php-shell) по содержимому страницы;
- эвристическое определение основных типов уязвимостей в веб-приложениях;
- определение уязвимостей в полях заголовка запросов HTTP.

Если в ходе идентификации открытых портов и служб на узле обнаружен веб-сервер, то проводится поиск уязвимостей, соответствующих его типу (например, Internet Information Server, Apache и т.д.), а также установленных расширений (FrontPage, OpenSSL и т.п.).

Следующим этапом является аутентификация, авторизация и проверка известных уязвимостей веб-приложений. После этого

включается механизм поиска скрытых директорий и индексации содержимого. В ходе сбора содержимого сканирующее ядро XSpider анализирует на предмет наличия гиперссылок веб-страницы, а также различные служебные и информационные файлы, содержащиеся на сервере (например, robots или readme.txt). После построения карты сайта сканер переходит к режиму поиска уязвимостей, которые отображаются в консоли программы по мере обнаружения.

В настоящее время сканирующее ядро XSpider поддерживает три механизма аутентификации:

- Basic;
- NTLM;
- собственные схемы аутентификации.

Далее рассмотрим две основные атаки на веб-приложения – внедрение операторов SQL (A1) и межсайтовый скриптинг (A3) .

Межсайтовое выполнение сценариев (Cross Site Scripting или, сокращенно, XSS) – атака на веб-приложение, использующая уязвимости неправильной обработки (фильтрации и экранирования) данных, введенных одним пользователем с последующим их выводом другому пользователю веб-приложения. В результате этого данные, выводимые пользователю, могут содержать не только текстовую информацию, но и введенный HTML-код или исполняемые скрипты (например, JavaScript или VBScript). Таким образом, посредством уязвимого веб-приложения нарушитель получает возможность выполнить произвольный JavaScript код у любого пользователя в контексте уязвимого веб-приложения. При этом браузер к этому коду применит политику безопасности, которую он обычно применяет к документам данного веб-приложения.

В некоторых веб-приложениях данные, введенные пользователем, сохраняются в файлах, базе данных или памяти перед выводом другим пользователям системы. Например, сообщения, введенные пользователями, сохраняются на различных Интернет-форумах, и затем их могут просматривать другие пользователи системы. С другой стороны, поисковые веб-приложения не сохраняют запросы пользователей, а отображают для просмотра только результат поиска. В связи с этим принято выделять два основных вида XSS атак – устойчивые (сохраняемые) и неустойчивые (отраженные).

Устойчивая XSS атака – XSS атака, в результате которой введенный нарушителем код сохраняется на веб-сервере. Неустойчивая XSS атака – XSS атака, в результате которой введенный нарушителем код передается пользователю, отправившему запрос к веб-приложению.

В первом случае опасности подвергаются все пользователи веб-приложения, просматривающие данные. Во втором случае – только те пользователи, которые перейдут на уязвимый сервер по ссылке, специально сформированной и переданной нарушителем пользователю под каким-либо предлогом.

Атака внедрение операторов SQL (SQL injection) обозначает атаку на веб-приложение, выполняемую путем обхода его логики работы и получения непосредственного доступа к данным, хранящимся в СУБД, путем внедрения во входные данные, обрабатываемых приложением, операторов SQL.

Постановка задачи

Выполнить сканирование уязвимостей веб-приложения с использованием сканера безопасности XSpider.

Последовательность действий

Шаг 1. Создать профиль сканирования «web scan». Список сканируемых портов ограничить значением 80. Отключить подбор учетных записей и сканирование служб UDP. В разделе «Анализатор контента» отключить использование словарей, поиск старых файлов и поиск вредоносного кода.

Шаг 2. Запустить сканирование сервера S2 с использованием созданного профиля. Просмотреть результаты.

Шаг 3. Проанализировать запросы, отправляемые сканером при выполнении проверки «Внедрение SQL-кода», найти значения полей UserName и Password.

Шаг 4. Подключиться к веб-серверу S2, используя Internet Explorer. Перейти по ссылке «Сервер Nacmebank». Попытаться зарегистрироваться на сайте, используя различные имена и пароли. В ответ должно появляться сообщение «Invalid Login».

Шаг 5. Ввести в поле «Username» символы «'», нажать «Submit». Проанализировать появившееся сообщение об ошибке. Среди результатов сканирования найти уязвимость «Некорректная обработка ошибок». Данная проверка выявляет, что веб-сервер в ответ на запрос возвращает диагностическое сообщение, позволяющее получить дополнительную информацию о веб-приложении.

Шаг 6. Ввести в поле «Username» набор символов «' OR 1=1 --» и нажать «Submit». Убедиться, что был произведён вход в систему под именем Joe Vilella.

Шаг 7. Получить название таблицы и полей с использованием оператора «' HAVING 1=1 --».

Шаг 8. Получить типы полей таблицы с помощью операторов «UNION SELECT SUM (LOGIN_ID) FROM FSB_USERS HAVING 1=1 --» и «UNION SELECT SUM (USER_NAME) FROM FSB_USERS HAVING 1=1 --».

Вопросы и задания

1. Выполнить ручные проверки веб-приложения на наличие уязвимостей приводящих к атакам типа XSS.
2. Построить универсальный текстовый шаблон (XSS-вектор) для тестирования веб-приложения в отношении XSS-атак.
3. Изучить атаку на веб-приложения типа «Подделка межсайтовых запросов» (CSRF). Определить взаимосвязь и влияние друг на друга CSRF- и XSS-атак.

2.10. Сканирование уязвимостей корпоративной сети

Цель работы

Целью лабораторной работы является обучение основным методам организации и проведения сканирования уязвимостей корпоративной сети.

Краткие теоретические сведения

Основным инструментом сканирования уязвимостей является сканер безопасности.

Сканеры безопасности могут быть классифицированы по нескольким признакам. С точки зрения платформы существуют как аппаратно-программные, так и программные сканеры безопасности.

С точки зрения расположения по отношению к объекту сканирования сканеры безопасности делятся на локальные (системные) и сетевые (дистанционные). Локальные сканеры безопасности устанавливаются непосредственно на сканируемом узле, работают от имени учётной записи с максимальными привилегиями и определяют наличие уязвимости только по косвенным признакам (например, по атрибутам файлов или значимым элементам реестра). Сетевые сканеры выполняют проверки по сети и обычно устанавливаются на выделенный узел, предназначенный для целей сканирования. Они могут выявлять уязвимости как по косвенным признакам, так и путем выполнения атак.

По взаимодействию с объектом сканирования выделяют активные и пассивные сканеры. Пассивные сканеры определяют уязвимости на основе анализа сетевых информационных потоков. Они выполняют анализ взаимодействия клиентских и серверных частей сетевых служб, идентифицируют версии используемых приложений и на основе этой информации делают выводы о наличии уязвимостей. Как правило, такие сканеры являются модулями систем обнаружения вторжений, предоставляющими данные для корреляции. Активные сканеры с объектом сканирования взаимодействуют напрямую.

В случае классификации сканеров безопасности по назначению выделяют сканеры общего характера и специализированные сканеры. Сканеры общего характера ориентированы на наиболее распро-

страненные ОС, службы, приложения и наиболее известные уязвимости. Специализированные сканеры ориентированы на конкретные компьютерные системы: WEB-приложения, СУБД (например, Oracle), системы электронного документооборота (например, Lotus Domino), ERP-системы (например, SAP R/3).

Сканирование уязвимостей корпоративной сети является высококритичным мероприятием.

Как правило, в организации разрабатывается специальный нормативный документ, являющийся частью политики безопасности, который определяет порядок сканирования уязвимостей. В некоторых случаях политика сканирования определяется внешними документами (например, стандарт платежных систем PCI DSS).

Рассмотрим типовые положения политики сканирования уязвимостей, применяемые в реальных сетевых КС.

1. К работе с сетевыми сканерами безопасности разрешается допускать только сотрудников, назначенных соответствующим приказом по организации.

2. Установку сканеров безопасности необходимо производить на выделенный АРМ, системные характеристики которого соответствуют требованиям, предъявляемым ПО сканера безопасности. Данное АРМ, как правило, должно находиться в составе центра управления сетью. Допускается установка программного обеспечения сетевых сканеров безопасности на переносной компьютер, предназначенный для проведения мобильных проверок.

3. Сканирование узлов сети (серверов, сетевого активного оборудования, рабочих станций и т.п.) должно производиться в соот-

ветствии с утвержденными внутренними планами (распорядительными документами) организации.

4. Время сканирования серверов критичных АС, ЭПС, а также сетевого активного оборудования центральных узлов связи должно предварительно согласовываться с подразделением, сотрудники которого осуществляют администрирование указанных средств вычислительной техники. Данное подразделение заблаговременно предоставляет список критичных серверов, а также сетевого активного оборудования центрального узла связи с указанием их IP-адресов.

5. При проведении сканирования СВТ, находящихся в промышленной эксплуатации, должны использоваться профили (шаблоны) сканирования, конфигурация которых исключает проведение DoS-атак. При сканировании контроллеров домена, серверов СУБД и ЭПС, а также других СВТ, находящихся в промышленной эксплуатации, должны быть отключены функции подбора паролей. Корректность настроенного профиля перед использованием должна быть проверена на тестовых, либо некритичных серверах/рабочих станциях.

6. Непосредственно по завершении процесса сканирования должны быть сгенерированы отчеты с применением штатных средств ПО сканеров безопасности. Отчеты должны быть незамедлительно переданы сотрудникам, ответственным за администрирование сканируемых устройств в электронном виде для рассмотрения материалов сканирования, проведения анализа и устранения выявленных недостатков.

7. На период рассмотрения материалов сканирования, согласования Акта и устранения выявленных недостатков, доступ к сформированным отчетам и материалам сканирования должен быть строго ограничен. Доступ к данным материалам должен быть разрешен только администраторам сетевых сканеров безопасности, администраторам сканируемых устройств, а также руководителям подразделений информационных технологий и служб информационной безопасности.

8. В течение трех рабочих дней с момента генерации и получения отчетов по сканированию, администраторы сканируемых устройств совместно с подразделением безопасности по сформированным отчетам проводят анализ материалов сканирования. Проводимый анализ должен основываться на реальной конфигурации сетевых устройств, сопоставленной с описанием выявленных уязвимостей и рекомендациями по их устранению, ссылки на которые приведены в отчетах, формируемых сканерами безопасности.

9. По окончании проведения анализа, в течение двух рабочих дней, администраторы сканируемых устройств направляют в подразделение безопасности результаты анализа с предложениями по устранению выявленных недостатков, для включения их в «Акт сканирования». В случае предоставления информации о выявленных «ложных» уязвимостях, в подразделение безопасности также должны быть предоставлены соответствующие подтверждающие материалы (файлы, конфигурации, журналы аудита, протоколы работы и т.п.).

10. Подразделение информационной безопасности на основе информации, предоставленной администраторами сканируемых устройств, формирует двухсторонний «Акт сканирования».

11. Акт направляется в подразделение, ответственное за администрирование сканируемых (проверяемых) устройств, для согласования и утверждения. Срок согласования акта не должен превышать трех рабочих дней.

Постановка задачи

Разработать профиль сканирования уязвимостей серверов корпоративного центра обработки данных для сканера безопасности XSpider.

Последовательность действий

Шаг 1. Создать профиль сканирования «Data Center scan». В разделе «Общие настройки» включить опцию «Не производить сканирование сетевых принтеров». В разделе «Поиск хостов» отключить метод «TCP Ping» и возможность сканирования не отвечающих узлов.

Шаг 2. В разделе «Сканер портов» включить режим «Сканировать весь диапазон TCP-портов». Включить режим «Сканировать UDP порты».

Шаг 3. В разделе «Сканер уязвимостей» отключить «Проверять на известные DoS-атаки», «Проверять на новые DoS-атаки», отключить подбор учетных записей.

Шаг 4. Выполнить тестирование созданного шаблона, выполнив сканирование стенда центра обработки данных (IP-сеть

172.16.8.0/24). Дождаться окончания сканирования. Проанализировать результаты. Убедиться в том, что не выполнялись DoS-атаки и подбор учетных записей.

Шаг 5. Добавить шаблон отчета. Перейти к вкладке «Отчеты», добавить отчет. Указать наименование отчета («Сканирование стенда ЦОД»), выбрать тип отчёта («Информация»), выбрать исходные данные («По скану»), указать тип данных («Pentest»). В параметрах отчета выбрать все опции. Сохранить шаблон отчета.

Шаг 6. Выполнить формирование отчета. Используя созданный шаблон выбрать пункт «Выпустить отчёт», указать задачу и скан. Проанализировать отчет в области «Готовые отчеты».

Шаг 7. Остановить сервер S1 и APM WS1. На сервере S2 остановить службы HTTP и СУБД Oracle. Выполнить повторное сканирование сети стенда. Создать дифференциальный отчет (тип отчета – дифференциальный), название отчета – «Изменения стенда ЦОД», указать два сравниваемых скана. Сгенерировать и просмотреть отчет, найти данные об изменениях в сети стенда.

Вопросы и задания

1. Настроить и выполнить сканирование стенда сети центра обработки данных по расписанию.
2. Настроить запись отладочной информации процесса сканирования в лог-файл.

ЛИТЕРАТУРА

1. Cisco Systems, Inc. Cisco SAFE reference guide [Электронный ресурс]. URL: <http://cisco.com/go/safe>.
2. Cisco Systems, Inc. High availability campus network design – routed access layer using EIGRP or OSPF system assurance guide [Электронный ресурс]. URL: <http://cisco.com/go/srnd>.
3. Cisco Systems, Inc. Network security baseline [Электронный ресурс]. URL: <http://cisco.com/go/safe>.
4. Boyles T, Hucaby D. Cisco CCNP switching exam certification guide. Cisco Press, 2001. 545 p.
5. Convery S. Network security architectures. Cisco Press, 2008. 792 p.
6. Deal R. Cisco router firewall security. Cisco Press, 2004. 912 p.
7. Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. : пер. с англ. М. : Вильямс, 2003. 976 с.
8. Томас М., Томас П. Структура и реализация сетей на основе протокола OSPF. 2-е изд. : пер. с англ. М. : Вильямс, 2004. 816 с.
9. Хилл Б. Полный справочник по Cisco. : пер. с англ. М. : Вильямс, 2004. 1078 с.
10. Хьюкаби Д., Мак-Квери С. Руководство Cisco по конфигурированию коммутаторов Catalyst : пер. с англ. М. : Вильямс, 2004. 560 с.
11. Лепихин В.Б., Гордейчик С.В. Сравнительный анализ сканеров безопасности. Функциональные возможности сканеров безопасности. URL: <http://www.securitylab.ru/analytics/downloads/secscanpt2.pdf>.

12. Herzog P. Open-source Security Testing Methodology Manual.
URL: <http://osstmm.org>.
13. McNab C. Network Security Assessment. Second edition. ISBN-10:0-596-51030-6, 2007. 478 p.
14. ЗАО «Позитив Текнолоджис». Сканер безопасности XSpider.
15. ЗАО «Позитив Текнолоджис». Практические работы по XSpider.
16. The WASC Threat Classification v2.0. URL:
<http://projects.webappsec.org>
17. OWASP. URL: <https://www.owasp.org>
18. Stuttard D., Pinto M. The Web Application Hackers's Handbook: Finding and Exploiting Security Flaws. ISBN-10: 1118026470.

Содержание

Введение.....	3
Основные сокращения и обозначения	7
1. Лабораторные работы по построению защищенных компьютерных сетей.....	9
1.1. Настройка операционной системы Cisco IOS	9
1.2. Защита инфраструктуры маршрутизации.....	20
1.3. Защита инфраструктуры коммутации.....	28
1.4. Защита ЛВС от петель на канальном уровне	35
1.5. Защита ЛВС от атак канального уровня	42
1.6. Построение маршрутизируемой ЛВС.....	47
1.7. Защита сетевой инфраструктуры	53
1.8. Защита периметра сети.....	61
1.9. Криптографическая защита каналов передачи данных.....	71
1.10. Защита беспроводной ЛВС.....	80
2. Лабораторные работы по инструментальному анализу защищенности компьютерных сетей.....	85
2.1. Сбор предварительной информации.....	87
2.2. Идентификация узлов и портов сетевых служб.....	91
2.3. Идентификация служб и приложений	98
2.4. Идентификация операционных систем.....	104
2.5. Идентификация уязвимостей сетевых приложений по косвенным признакам	107
2.6. Идентификация уязвимостей на основе тестов.....	113
2.7. Особенности идентификации уязвимостей ОС Windows ..	119
2.8. Сканирование уязвимостей СУБД Oracle.....	123
2.9. Сканирование уязвимостей веб-приложений.....	125
2.10. Сканирование уязвимостей корпоративной сети	131
Литература	138

Издание вышло в свет в авторской редакции

Отпечатано на участке оперативной полиграфии
редакционно-издательского отдела ТГУ

Заказ № 343 от «21» мая 2013 г. Тираж 50 экз.