Владивостокский государственный университет экономики и сервиса
Институт информатики инноваций и бизнес систем

Предмет:
«Технологии Интернет»

Руководитель: Сачко Максим Анатольевич, старший преподаватель

Тема 8

Обеспечение безопасности в корпоративной сети

Содержание:

1) Задача обеспечения безопасности в корпоративной сети
2) Демон оболочек сервисов (TCP wrapper)
3) Списки доступа на маршрутизаторе
4) Расширенные списки доступа
5) Общие правила составления списков доступа на маршрутизаторе

Задачи обеспечения безопасности

Защита сети и данных - важная часть работы системного и сетевого администратора.

Простые методы защиты строятся на создании фильтров, анализирующих поступающие или исходящие данные с целью принятия решения о пропуске или блокировании трафика. Фильтры могут защищать целую сеть или отдельные сетевые сервисы какого-либо узла.

Демон оболочек сервисов (TCP wrapper)

Простым средством защиты Unix-хоста от несанкционированного доступа является установка оболочек сервисов (**TCP wrappers**). Принцип действия оболочек следующий: при поступлении запроса на соединение с каким-либо сетевым сервисом на хосте запускается не демон, обслуживающий этот сервис, а программа-оболочка, которая проверяет, разрешен ли сеанс с удаленным хостом, запросившим соединение, и в случае положительного результата запускает собственно требуемый демон.

Для запуска оболочек для тех или иных сервисов следует модифицировать файл **inetd.conf** так, чтобы при обращении на порты указанных сервисов вместо стандартного демона запускался демон оболочки, а в качестве параметра ему передавался путь к стандартному демону.

finger stream tcp nowait nobody /usr/sbin/tcpd in.fingerd

/usr/sbin/tcpd контролирует доступ к сервису finger

Списки доступа в TCP wrappers

Списки доступа, которыми пользуется демон оболочки, содержатся в файлах /etc/hosts.allow, /etc/hosts.deny. При возникновении попытки соединения адрес хоста ищется сначала в файле hosts.allow, если он найден, то соединение разрешается, иначе производится поиск в hosts.deny. В случае успешного поиска соединение запрещается, иначе разрешается.

Формат файлов *hosts.allow* и *hosts.deny* одинаков, строка в файле имеет вид:

сервисы:хосты[:действие]

действие - действие, выполняемое, в случае совпадения адреса хоста и требуемого сервиса с данной строкой (например, послать сообщение администратору); поле действие может отсутствовать.

В поле хосты допускаются регулярное выражение *, операторы *ALL* и *EXCEPT*.

Пример

hosts.allow:

telnetd:194.84.124.0/255.255.255.0, 193.124.169.58
ftpd:ALL EXCEPT 1.0.0.0/255.0.0.0

hosts.deny:

ALL:ALL

Списки доступа на маршрутизаторе

Списки досутпа позволяют фильтровать входящий и исходящий трафик в сети в зависимости от адресов источника и приемника, номеров портов, протоколов и т.п.

Для защиты целой сети от несанкционированных соединений можно подключить списки доступа на входном маршрутизаторе (шлюзе). Параметры любой входящей или исходящей дейтаграммы (адрес источника, места назначения, номера портов и т.п.) проверяется по списку и в зависимости от результата дейтаграмма либо пропускается маршрутизатором, либо уничтожается.

Списков доступа маршрутизаторов Cisco

Списки доступа строятся командой **access-list** в режиме глобальной конфигурации (режим доступен через команды *enable*, затем *configure terminal*), каждый список определяется номером - числом в диапазоне 0-99. Синтаксис команды для ввода строки в список:

access-list номер_списка {deny | permit} адрес_источника [маска]

Для аннулирования списка доступа следует ввести команду

no access-list номер_списка

Для применения списка доступа к дейтаграммам, проходящим через определенный интерфейс, нужно в режиме конфигурации этого интерфейса ввести команду

ip access_group номер_списка {in | out}

Расширенные списки доступа

Расширенные *(extended)* списки доступа, имеющие большее количество параметров и предлагающие более богатые возможности для контроля трафика.

Расширенные списки доступа создаются также с помощью команды **access-list** в режиме глобальной конфигурации, но номера этих списков лежат в диапазоне 100-199.

Расширенный списокок для контроля TCP-соединений:

access-list номер_списка {deny | permit} tcp адрес_источника маска [оператор порт [порт]] адрес_назначения маска [оператор порт [порт]] [established]

Маски для адреса источника и хоста назначения определяются так же, как и в стандартных списках. Оператор должен иметь одно из следующих значений:

lt (строго меньше), gt (строго больше), eq (равно), neq (не равно), range (диапазон включительно).

Пример

Запретить установление соединений с помощью протокола telnet со всеми хостами сети 172.16.252.0 netmask 255.255.252.0 со стороны всех хостов Интернет, причем в обратном направлении все соединения должны устанавливаться

```
access-list 100 permit tcp any 172.16.252.0 0.0.3.255 eq 23 established
access-list 100 deny tcp any 172.16.252.0 0.0.3.255 eq 23
access-list 100 permit tcp any any
```

Контроль за ICMP сообщениями

access-list *номер_списка* {deny | permit} icmp *адрес_источника* маска *адрес_назначения маска* [icmp-тип [icmp-код]]

где *icmp-тип* и, если требуется уточнение, *icmp-код* определяют ICMP-сообщение. Обычно в целях безопасности не пропускаются ICMP-сообщения типа Redirect (Изменить маршрут), т. е. сообщения типа 5.

Правила составления списков доступа на маршрутизаторе

- Запретить source-routing - использование опции протокола IP, позволяющей фиксировать маршрут дейтаграммы (опасность подстановки ложных адресов отправителя).
- Создать окна для пропуска необходимого TCP-трафика, например, разрешить доступ из Интернет к WWW, email, FTP серверам предприятия, разрешить любой доступ в Интернет из сети предприятия.
- Доступ извне по порту 53/TCP (передача зоны вторичному серверу DNS) разрешить только вторичным серверам DNS.

Правила составления списков доступа на маршрутизаторе

- Весь остальной TCP-трафик запретить.
- Запретить пропуск любых пакетов, приходящих извне с адресом отправителя, принадлежащим внутренней сети (такие пакеты либо ошибочны, либо отправлены злоумышленником).
- Запретить все соединения по UDP кроме порта 53 (DNS) (UDP - протокол без установления соединения, поэтому его сложнее контролировать).
- Запретить передачу ICMP-сообщений типа Redirect.

Вопросы для самопроверки:

1. Опишите, что происходит при подключении клиента к серверу удаленного доступа на базе Unix (протокол PPP). Какие программы запускаются, в какой последовательности, что они делают?
2. Опишите принцип работы демона оболочек сервисов TCP wrapper?
3. Сформулируйте основные угрозы безопасности корпоративной IP-сети.
4. Дайте сравнительные характеристики различных типов брандмауэров.
5. Чем отличаются стандартные и расширенные списки доступа на маршрутизаторах CICSO?

Рекомендуемая литература:

1. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник. – СПб: "Питер", 2005.
2. К. Хант. Персональные компьютеры в сетях TCP/IP: Руководство администратора сети/ Пер. с англ. – СПб.: ЗАО "ЭлектроникаБизнесИнформатика", Киев: "BHV", 2003.
3. UNIX для системных администраторов: Энциклопедия пользователя/ Пер.с англ. – Киев: ДиаСофт, 2008.
4. Chapman and Zwicky. Building Internet Firewalls. – O'Reily and Associates, Inc.Huitema C. Routing in the Internet. – Prentice-Hall PTR, 2003.

- **Использование материалов презентации**

- Использование данной презентации, может осуществляться только при условии соблюдения требований законов РФ об авторском праве и интеллектуальной собственности, а также с учетом требований настоящего Заявления.

- Презентация является собственностью авторов. Разрешается распечатывать копию любой части презентации для личного некоммерческого использования, однако не допускается распечатывать какую-либо часть презентации с любой иной целью или по каким-либо причинам вносить изменения в любую часть презентации. Использование любой части презентации в другом произведении, как в печатной, электронной, так и иной форме, а также использование любой части презентации в другой презентации посредством ссылки или иным образом допускается только после получения письменного согласия авторов.