ФЕДЕРАЛЬНОЕ АГЕНТСТВО ОБРАЗОВАНИЯ
ДИМИТРОВГРАДСКИЙ ИНСТИТУТ ТЕХНОЛОГИЙ,
УПРАВЛЕНИЯ И ДИЗАЙНА

Лабораторная работа №5
по курсу: “Усиление защиты ОС Linux в сети”

Выполнил студент гр. ВТ-41:
Потеренко А.Г.
Проверил преподаватель:
Петлинский В.П.

Димитровград 2006г.

Отключение неиспользуемых сетевых сервисов в ОС Linux

Для запуска большинства сетевых сервисов в Unix-системах используется супердемон xinetd.

Чтобы избавить себя от лишних волнений отключите и деинсталлируйте все сервисы, которые вы не используете. Просмотрите файл "/etc/xinetd.conf" и включаемые файлы конфигурации в директории "/etc/xinetd.d" и отключите ненужные сетевые сервисы.

```
[root@DBADOMAIN xinetd.d]# more /etc/xinetd.conf
#
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/

defaults
{
        instances               = 60
        log_type                = SYSLOG authpriv
        log_on_success          = HOST PID
        log_on_failure          = HOST
        cps                     = 25 30
}

includedir /etc/xinetd.d
```

```
[root@DBADOMAIN xinetd.d]# ls /etc/xinetd.d
chargen      daytime      echo-udp  gssftp                    krb5-telnet  tftp
chargen-udp  daytime-udp  eklogin   ion ] [ mode ] files...  kshell       time
cups-lpd     echo         finger    klogin                    rsync        time-udp
```

После чего пошлите демону xinetd сигнал SIGHUP для того, чтобы изменения вступили в силу (Для того, чтобы демон перегрузил файлы конфигурации можно использовать и команду reload в скрипте инициализации /etc/init.d/xinetd). Для этого выполните следующее:

Шаг 1
Смените права доступа к файлу "/etc/xinetd.conf" на 600 для того, чтобы читать и писать в него мог только root. Аналогичные действия рекурсивно предпринять для директории /etc/xinetd.d

```
chmod 600 /etc/xinetd.conf
```

Шаг 2
УБЕДИТЕСЬ, что владельцем файла "/etc/xinetd.conf" является root.

Шаг 3
Отредактируйте файлы в директории /etc/xinetd.d и отключите те сервисы, которые вы не используете.

Шаг 4
Пошлите HUP сигнал демону xinetd

```
killall -HUP xinetd
```

Шаг 5
Сделайте "прививку" файлу "/etc/xinetd.conf", используя команду chattr, чтобы никто не мог модифицировать этот файл. Выполните команду:

```
chattr +i /etc/xinetd.conf
```

Это предотвратит любые изменения файла "xinetd.conf". Только один человек может снять атрибут - это суперпользователь root. Для модификации файла нужно снять immutable-флаг. Это делается следующей командой:

```
chattr -i /etc/xinetd.conf
```

Аналогичные действия рекурсивно предпринять для директории /etc/xinetd.d

Блокировка доступа к сервисам через TCP_WRAPPERS

Инструмент TCP Wrappers играет роль посредника между inetd и целевым сервером. Средства TCP Wrappers применяются для повышения безопасности системы; они позволяют задавать правила установления соединений, защищая тем самым сервер от нежелательного взаимодействия. Передача TCP Wrappers полномочий по управлению соединением повышает гибкость системы, не требуя при этом внесения изменений в программы.

Для управления работой TCP Wrappers используются два файла: **/etc/hosts.allow** и **/etc/hosts.deny**. Эти файлы имеют одинаковый формат, но выполняют противоположные действия. В файле hosts.allow описываются узлы сети, которым разрешено обращаться к данному компьютеру; для всех остальных узлов доступ запрещен. Файл hosts.deny, напротив, содержит описания узлов, доступ с которых запрещен; все остальные узлы могут устанавливать соединение с данным компьютером. Если в системе присутствуют оба файла, **приоритет имеет файл hosts.allow**. Благодаря этому вы имеете возможность задать ограничения в файле hosts.deny, а затем разрешить доступ для отдельных компьютеров. Если сведения о сервере не включены ни в один из файлов (сервер может быть описан либо непосредственно, либо с помощью групповой операции), TCP Wrappers разрешает доступ к нему для всех узлов сети.

Подобно другим конфигурационным файлам, символ # в начале строки означает, что в данной строке содержатся комментарии. Запись в файле hosts.allow или hosts.deny имеет следующий формат:

список_демонов : список_клиентов

В списке демонов указывается один или несколько серверов, к которым применяется данное правило. Если в списке указано несколько серверов, их имена разделяются запятыми или пробелами. Имена серверов должны совпадать с именами, содержащимися в файле **/etc/services**. Кроме имен серверов в этом поле можно также указывать ключевое слово **ALL**, определяющее групповую операцию. Оно означает, что правило применяется ко всем серверам, управляемым TCP Wrappers.

Не все серверы запускаются с помощью TCP Wrappers. Поэтому групповая операция ALL может не включать все серверы, выполняющиеся в системе. Аналогично, указав сервер в списке демонов, вы не защитите его, если для управления им не применяются inetd и TCP Wrappers, либо если он не использует TCP Wrappers непосредственно.

Список клиентов определяет компьютеры, которым разрешен или запрещен доступ к серверу. Подобно списку доменов, в списке серверов может быть указан один узел либо несколько узлов. Идентификаторы узлов разделяются запятыми или пробелами. Описания узлов сети могут быть представлены в перечисленных ниже форматах.

- **IP-адрес**. В списке клиентов можно указать конкретный IP-адрес, например 10.102.201.23. Такое описание определяет только этот адрес.
- **Диапазон IP-адресов**. Задать диапазон IP-адресов можно несколькими способами. Проще всего сделать это, указав в составе адреса меньше четырех десятичных чисел; в этом случае адрес должен заканчиваться точкой. Например, значение 10.102.201. соответствует сети 10.102.201.0/24. Кроме того, можно использовать запись типа IP-адрес/маска. В файлах hosts.allow и hosts.deny также поддерживаются адреса IPv6. Они задаются в виде [n:n:n:n:n:n:n:n]/длина, где n — значения компонентов адреса, а длина — это число битов, используемых для представления диапазона.
- **Имя узла**. Узел можно описывать с помощью его доменного имени. Этим способом определяется только один узел. В этом случае при получении запроса система выполняет преобразование имен, а, следовательно, если сервер DNS работает некорректно, при идентификации компьютера могут быть допущены ошибки.
- **Домен**. Домен можно задавать так же, как вы задается доменное имя одного компьютера. Отличие состоит лишь в том, что в данном случае имя должно начинаться с точки. Если в файле указано имя .threeroomco.com, оно определяет все компьютеры, принадлежащие домену threeroomco.com.
- **Имя группы NIS**. Если последовательность символов начинается со знака @, оно интерпретируется как имя группы NIS (Network Information Services — сетевая информационная служба). Этот метод предполагает, что в сети функционирует сервер NIS. В списке клиентов могут присутствовать ключевые слова, определяющие групповые операции.
- **ALL**. Идентифицирует все компьютеры.
- **LOCAL**. Определяет все локальные компьютеры на основании анализа имени узла. Если в имени отсутствует точка, соответствующий узел считается локальным.
- **UNKNOWN**. Данное ключевое слово задает все компьютеры, чьи доменные имена не могут быть получены средствами преобразования имен.

- **KNOWN**. Идентифицирует компьютеры, доменные имена и IP-адреса которых известны системе.
- **PARANOID**. Определяет компьютеры, имена которых не соответствуют IP-адресам. При использовании последних трех ключевых слов надо соблюдать осторожность, поскольку, если они присутствуют в списке клиентов, компьютер обращается к серверу DNS. Неисправность сетевого оборудования может привести к ненадежной работе сервера DNS. Если сервер DNS недоступен, получить доменное имя компьютера не удастся.

Используя в списке клиентов записи типа **пользователь@компьютер**, можно управлять доступом отдельных пользователей, работающих на удаленных узлах. Для того чтобы это было возможно, на клиентском компьютере должен выполняться сервер ident (в некоторых системах он называется auth), который возвращает имя пользователя, работающего с конкретным сетевым портом. Компьютер, использующий TCP Wrappers, передает запрос клиентской машине и получает имя пользователя. В этом случае соединение устанавливается с некоторой задержкой, а информация о пользователе, полученная из Internet, не всегда заслуживает доверия. Поэтому данную возможность лучше использовать в локальной сети, где вы имеете возможность контролировать конфигурацию всех компьютеров.

В составе правила может присутствовать дополнительное ключевое слово **EXCEPT**. Оно определяет исключения из этого правила. Рассмотрим следующую запись, содержащуюся в файле /etc/hosts.deny:

```
www : badcracker.org EXCEPT goodguy@exception.badcracker.org
```

В данном случае доступ к Web-серверу запрещается для всех компьютеров, принадлежащих домену badcracker.org. Исключением являются лишь запросы, полученные от пользователя goodguy@exception.badcracker.org. Аналогичный результат можно получить, включив правило для goodguy@exception.badcracker.org в файл /etc/hosts.allow.

Если перед вами стоит задача максимально повысить безопасность системы, вы можете начать настройку с создания файла /etc/hosts.deny, содержащего следующую информацию:

```
ALL : ALL
```

Эта запись блокирует доступ ко всем серверам, поддерживаемым TCP Wrappers, с любого компьютера, независимо от его адреса. Затем можно постепенно разрешать доступ к серверам, составляя соответствующие правила и записывая их в файл /etc/hosts.allow. Возможности доступа должны ограничиваться необходимым минимумом. В частности, к серверам, чувствительным к попыткам взлома извне, например к Telnet, следует разрешить доступ только для определенных компьютеров.

Шаг 1
Отредактируйте файл hosts.deny и добавьте такие строки:

```
# Отказать в доступе всем
ALL: ALL@ALL, PARANOID
```

Имеется в виду, что все сервисы и хосты блокируются, если им не разрешён доступ в hosts.allow

Шаг 2
Отредактируйте файл hosts.allow и добавьте в него, например, следующую строку:

```
ftp: 127.0.0.1, 172.16.69.105
```

Клиентской машине с ip-адресом 127.0.0.1 и 172.16.69.105 разрешён доступ к серверу через службу ftp.

Шаг 3

Проверьте изменения для сервисов ftp, telnet, time. Для проверки необходимо использовать в качестве клиента свой и соседний компьютер. Для получения информации о сетевой конфигурации (ip адресе) использовать команду ifconfig (man ifconfig).

Не давайте системе показывать issue-файл

Файлы **issue**, **issue.net** определяют приветствие при попытке регистрации в системе. Файл issue выводится на консоль при локальной регистрации, а issue.net — при регистрации по сети, например, по протоколу telnet.

Не показывайте issue-файл вашей системы при удаленном подключении. Для этого можно изменить опции запуска telnet в файле "/etc/xinetd.d/telnet". Строка в "/etc/xinetd.d/telnet"

```
server = /usr/sbin/telnetd
```

будет выглядеть при этом так:

```
server = /usr/sbin/telnetd -h
```

Добавление флага "-h" в конце заставляет демон выводить приглашение для входа в систему, не показывая никакой системной информации.

Изменения в файле "/etc/host.conf"

Конфигурационный файл /etc/host.conf используется для установки порядка, в котором осуществляются обращения к различным типам ресурсов, используемых для установки соответствия между именами хостов и их IP-адресами. Пример файла /etc/host.conf:

```
# Просматривать имена хостов сперва через DNS, потом в файле /etc/hosts.
order bind, hosts
# Мы имеем машины с несколькими ip-адресами.
multi on
# Проверка ip-адресов на спуфинг.
nospoof on
# С помощью syslogd записывать сообщения об ошибках в системный журнал.
spoofalert on
```

Команда chattr

chattr [-RV] [-v version] [mode] files...

Изменение атрибутов файла. Это специфическая команда файловой системы Linux (Second Extended Filesystem). Работает аналогично символьному варианту chmod с использованием +, - и =. Режим (mode) представляется в виде операция атрибут.

Опции

—R Изменять рекурсивно атрибуты каталогов и их содержимое.
-V Отображать состояние атрибутов после их изменения.
—v version Установить версию файла в version.

Операции

\+ Включить атрибут.
— Выключить атрибут.
= Присвоить атрибуты (выключив те, что не заданы).

Атрибуты

A Не обновлять атрибут времени доступа при изменении файла.
a Разрешить только добавление к содержимому файла. Атрибут может устанавливаться или сниматься только привилегированным пользователем.
c Файл сжат.
d Запретить вывод содержимого программой dump.
i Неизменяемый. Атрибут может устанавливаться или сниматься только привилегированным пользователем.
s Безопасное удаление; содержимое при удалении обнуляется.
u Неудаляемый.
S Синхронное обновление.

"Иммунизация" файла "/etc/services"

Файл /etc/services дает возможность серверу и клиентским программам устанавливать соответствие между названиями служб и номерами (портов). Только суперпользователю root должно быть разрешено вносить изменения в этот файл. Для этого установите запрет на внесение изменений в файл /etc/services:

```
chattr +i /etc/services
```

"Иммунизация" протокольных файлов в директории "/var/log"

Для того чтобы при взломе вашей системы хакер не смог очистить файлы протоколов системы, необходимо сделать прививку этим файлам. Команда chattr +a file, устанавливает атрибут позволяющий только дозаписывать в файл, не очищая его с начала.

Утилиты netstat и nmap

Утилиты netstat и nmap можно использовать для анализа сетевых сервисов, запущенных на вашей машине.

• Запустим утилиту nmap на локальной машине 192.168.50.3 и узнаем версию ОС, работающие сетевые сервисы и их версию:

```
[root@DBADOMAIN xinetd.d]# nmap -sV -O 192.168.50.3

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2006-11-18 07:55 MSK
Interesting ports on 192.168.50.3:
Not shown: 1678 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 3.9p1 (protocol 1.99)
111/tcp open  rpcbind  2 (rpc #100000)
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.5.25 - 2.6.8 or Gentoo 1.2 Linux 2.4.19 rc1-rc7
Uptime 0.673 days (since Fri Nov 17 15:46:15 2006)

Nmap finished: 1 IP address (1 host up) scanned in 21.572 seconds
```

• netstat [options]

Команда TCP/IP. Отображает состояния сетевых соединений. Для всех активных сокетов отображаются протоколы, число байт в очереди приема, число байт в очереди посылки, номер порта, удаленные адрес и порт, а также состояние сокета.

Параметры

—a Отобразить состояние всех сокетов, а не только активных.
—c Отображать информацию постоянно с обновлением раз в секунду.
—i Включать статистику по сетевым устройствам.
—n Отображать численные сетевые адреса.
—o Отображать дополнительную информацию, например, имя пользователя.
—r Отображать таблицы маршрутизации.
—t Перечислять только TCP-сокеты.
—u Перечислять только UDP-сокеты.
—V Вывести номер версии и завершить работу.
—w Перечислять только простые сокеты.
—x Перечислять только доменные гнезда Unix.

```
[root@DBADOMAIN xinetd.d]# netstat -i
Kernel Interface table
Iface       MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500   0    75057      0      0      0   256291      0      0      0 BMRU
lo        16436   0    33913      0      0      0    33913      0      0      0 LRU
```

```
[root@DBADOMAIN xinetd.d]# netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 ::ffff:192.168.50.3:ssh     ::ffff:192.168.50.1:1030    ESTABLISHED
tcp        0      0 ::ffff:192.168.50.3:ssh     ::ffff:192.168.50.1:1067    ESTABLISHED
tcp        0      0 ::ffff:192.168.50.3:ssh     ::ffff:192.168.50.1:1032    ESTABLISHED
tcp        0      0 ::ffff:192.168.50.3:ssh     ::ffff:192.168.50.1:1064    ESTABLISHED
```