Лабораторная работа № 5

Укрепление защиты сети

В этой работе требуется вступить в одну двух из команд («синюю» или «красную»), выполнить настройки сети и сетевых сервисов для обеспечения улучшенной (эшелонированной) защиты и попытаться проникнуть во «вражеский стан».

Задание 1. Сегментация сети

Перед выполнением задания не забудьте сделать снимок виртуальной машины.
Используя первый сетевой адаптер, выполните следующие действия:

1. Проверьте `тип подключения` первого сетевого адаптера, — должен быть установлен `Сетевой мост`.
2. Выберите себе внутренний сетевой адрес в своей подсети: у «синих» — 10.0.1.0; у «красных» — 10.0.100.0.
3. Создайте каталог `/home/public` и сделайте его общедоступным.
4. Проверьте связь со «своими» и «чужими». Проверьте доступность сетевых сервисов («своих» и «чужих»).
5. Добавьте в отчёт конфигурацию сетевых настроек своего компьютера.

Задание 2. Настройка файервола с помощью iptables

Перед выполнением задания не забудьте сделать снимок виртуальной машины.
Файервол, встроенный в ядро Linux, называется «Netfilter», а «iptables» — утилита для управления этим файерволом. С помощью «Netfilter» можно:

- Разрешать/запрещать входящий/исходящий трафик на определенные порты по определенным протоколам (IPv4/IPv6, TCP/UDP) с указанных адресов (IP, MAC) или подсетей.
- Настраивать NAT и OpenVPN.
- Настраивать защиту от DDoS и брутфорса, ограничивать доступ в сеть конкретным приложениям, пользователям или группам.

1. Показать все правила:
   `iptables -L -n`

   В «Netfilter» есть «цепочки» (chains) типа `INPUT`, `OUTPUT` и `FORWARD`.
2. Рассмотрите следующие примеры.

   Удалить все правила:

   ```
   iptables -F
   ```

   Изменить политику (поведение по умолчанию) цепочки:

   ```
   iptables -P INPUT DROP
   iptables -P INPUT ACCEPT
   ```

   Запретить доступ с хоста/подсети:

   ```
   iptables -A INPUT -s 123.45.67.89 -j DROP
   iptables -A INPUT -s 123.45.0.0/16 -j DROP
   ```

   Также можно использовать доменные имена:

   ```
   iptables -A INPUT -s example.ru -j DROP
   ```

Запрет исходящих соединений:

```
iptables -A OUTPUT -d 123.45.67.89 -j DROP
```

В правилах можно использовать отрицания:

```
iptables -A INPUT ! -s 123.45.67.89 -j DROP
```

Удаление правила по его номеру в цепочке:

```
iptables -D INPUT 1
```

Удаление правила на основе того, что оно делает:

```
iptables -D INPUT -s 123.45.67.89 -j DROP
```

Опция `-p` указывает на протокол. Можно использовать `all`, `icmp`, `tcp`, `udp` или номер протокола из `/etc/protocols`.

Флаг `-sport` указывает порт, с которого был прислан пакет, а `-dport` указывает порт назначения:

```
iptables -A INPUT -p tcp --sport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Вставка (insert) правила в начало цепочки:

```
iptables -I INPUT ...
```

Или можно указать конкретную позицию:

```
iptables -I INPUT 3 ...
```

Сохранить правила:

```
iptables-save > /etc/iptables.rules
```

Восстановить правила:

```
iptables-restore < /etc/iptables.rules
```

Восстановление происходит точно так же, только флаг `-A` заменяется на флаг `-D`.

3. Создайте правила для защиты Вашего узла от чужих проникновений, оставив доступ для «своих».

Есть и более удобные инструменты для работы с «iptables», например, есть модуль к системе «Webmin» для настроек «iptables» через веб-интерфейс (`https://localhost:10000/firewall/`).

Проверьте, что всё работает. Если да, то сохраните правила:

```
iptables-save > /etc/iptables.rules
```

4. Чтобы правила подхватывались при загрузке системы, следует создать новый файл `/etc/rc.d/init.d/iptables` (в Rosa, Red Hat, Fedora) или `/etc/network/if-pre-up.d/iptables` (в Ubuntu, Debian), записать в него:

```
#!/bin/sh
iptables-restore < /etc/iptables.rules
exit 0
```

и сделать его исполняемым:

```
chmod +x iptables
```

5. Добавьте в отчёт правила `iptables`.

Задание 3. Настройка файервола с помощью shorewall

«Shorewall» (Shoreline Firewall) — инструмент для настройки файервола в Linux. Технически он является надстройкой над файерволом «Netfilter» ядра Linux и обеспечивает упрощённые методы конфигурирования данной подсистемы. Он предоставляет более высокий уровень абстракции для описания правил работы файервола.

«Shorewall» не является демоном. Правила хранятся в текстовых файлах (в каталоге `/etc/shorewall`), при запуске «shorewall» считывает свои файлы конфигурации и преобразует их в настройки, понятные «ipchains»/«iptables», после чего данные настройки файрвола могут действовать до перезапуска операционной системы.

«Shorewall» не имеет GUI для конфигурирования, правка конфигурационных файлов может быть произведена в любом текстовом редакторе. Есть, например, модуль к системе «Webmin» для настроек «shorewall» через веб-интерфейс (`https://localhost:10000/shorewall/`).

Ваша задача — доработать настройки файервола «Netfilter».

Добавьте в отчёт Ваши настройки «shorewall».