Практическое задание № 07. Межсетевые экраны. Iptables

Опубликовано **14.11.2023**

Дедлайн **28.11.2023**

Лабораторная работа посвящена настройке межсетевого экрана в Linux. Для выполнения работы понадобятся две виртуальные машины с Linux.

1 Задания

1.1 Блокирование определённого хоста по IP-адресу

В общем виде правило для фильтрации трафика по критерию «отправитель» можно создать следующим образом:

```
iptables -A INPUT -s source_addr_or_name -j {DROP/REJECT} [--reject-with reject_type]
```

Здесь в квадратные скобки заключен необязательный параметр.

1. составить правила для фильтрации входящего трафика с лабораторных машин с действиями DROP и REJECT
2. проверить защищенность машины с помощью утилиты ping и nmap
3. при использовании действия REJECT проверить влияние параметра --reject-with на результаты сканирования
4. в чем различия при фильтрации трафика целями DROP и REJECT?

Для просмотра текущего списка правил используйте:

```
iptables -L
```

Для сброса используйте:

```
iptables -F
```

1.2 Фильтрация по протоколу

В общем виде правило для фильтрации трафика по критерию «протокол» можно создать следующим образом:

```
iptables -A INPUT -p {tcp/udp/icmp/all} -j {DROP/REJECT} [--reject-with reject_type]
```

1. составить правила для фильтрации входящего трафика с лабораторных машин с целями DROP и REJECT по протоколам tcp, udp и icmp
2. проверить защищенность с помощью ping и nmap
3. при использовании цели REJECT проверить влияние параметра –reject-with на результаты сканирования.
4. показать различия при фильтрации трафика целями DROP и REJECT

1.3 Фильтрация по порту назначения

В общем виде правило для фильтрации трафика по критерию "порт назначения"можно создать следующим образом:

```
iptables -A INPUT -p {tcp/udp/all} --dport port -j {DROP/REJECT/ACCEPT} [--reject-with type]
```

1. запустить несколько сервисов на машине (ssh, mysql, postgresql, nginx и т.п)
2. выбрать какие из сервисов должны быть доступны извне, а какие – нет
3. составить правила так, чтобы попытка доступа к неразрешенному извне сервису записывалась в лог
4. проверить защищенность машины с помощью nmap
5. попытки доступа должны быть записаны в /var/log/syslog

1.4 Маскировка машины путем блокирования ICMP-пакетов

В общем виде правило для фильтрации трафика по icmp может быть создано следующим образом:

```
iptables -A INPUT -p icmp -icmp-type type -j {DROP/REJECT} [--reject-with reject_type]
```

1. составить правила для фильтрации входящего icmp-трафика с лабораторных машин с действиями DROP и REJECT
2. для получения возможных аргументов ключа --icmp-type использовать команду iptables -p icmp -h
3. при проверке маскировки машины использовать утилиту nmap

1.5 Разрешение только исходящих соединений

Используется, когда нужен доступ в интернет, но входящие соединения, открытые по инициативе внешнего хоста, нежелательны. Такую политику можно реализовать следующим образом:

1. поменять политику по умолчанию на блокирование всех пакетов для цепочек INPUT, OUTPUT (команда -P)
2. разрешить входящие пакеты, которые относятся к соединению (RELATED, ESTABLISHED - использовать модуль conntrack)
3. разрешить все исходящие пакеты (цепочка OUTPUT)
4. проверить способность подключаться к удаленным компьютерам
5. проверить защищенность машины с помощью nmap