Санкт-Петербургский Политехнический Университет Петра Великого

Кафедра компьютерных систем и программных технологий

Отчёт по лабораторной работе №4

Курс: «Администрирование компьютерных сетей»

Тема: «Устранение уязвимостей»

Выполнил студент:

Бояркин Никита Сергеевич
Группа: 13541/3

Проверил:

Малышев Игорь Алексеевич

Санкт-Петербург
2018 г.

Содержание

Лабораторная работа №4

1.1 Цель работы

Получить навыки работы с Netfilter, используя iptables – утилита для управления межсетевым экраном.

1.2 Устранение уязвимостей

Уязвимости, найденные в предыдущих лабораторных работах связаны в первую очередь с открытыми портами. Утилита iptables позволяет задать правила для входящих/исходящих tcp/udp портов для обеспечения безопасности.

Чтобы показать все правила, необходимо ввести команду:

```
nikita@ubuntu:~$ sudo iptables -L -n
[sudo] password for nikita:
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Рис. 1.1: Правила по-умолчанию

По-умолчанию нет никаких правил, а следовательно все внешние порты закрыты.

Открытие TCP порта 80 производится следующей командой:

```
nikita@ubuntu:~$ sudo iptables -I INPUT -p tcp -m tcp --dport 80 -j ACCEPT
nikita@ubuntu:~$ sudo iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Рис. 1.2: Создание нового правила открытия 80 tcp порта

Удаление правила по его порядковому номеру в таблице производится следующей командой:

```
nikita@ubuntu:~$ sudo iptables -D INPUT 1
nikita@ubuntu:~$ sudo iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Рис. 1.3: Удаление правила по номеру

Удаление всех правил производится следующей командой:

```
nikita@ubuntu:~$ sudo iptables -F
```

Рис. 1.4: Удаление всех правил

Запрет исходящих соединений на конкретный адрес:

```
nikita@ubuntu:~$ sudo iptables -A OUTPUT -d 8.8.8.8 -j DROP
nikita@ubuntu:~$ sudo iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  0.0.0.0/0            8.8.8.8
nikita@ubuntu:~$ ping 8.8.8.8 -c 3
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2038ms
```

Рис. 1.5: Запрет исходящих соединений на конкретный адрес

Также есть возможность сохранить и восстановить правила:

```
nikita@ubuntu:~$ sudo iptables-save > /home/nikita/1
nikita@ubuntu:~$ sudo iptables-restore < /home/nikita/1
```

Рис. 1.6: Сохранение и восстановление правил из файла

1.3 Вывод

Межсетевой экран, встроенный в ядро Linux, называется Netfilter, а iptables – утилита для управления этим межсетевым экраном.

В системе netfilter пакеты пропускаются через цепочки. Цепочка является упорядоченным списком правил, а каждое правило может содержать критерии и действие или переход.

Утилита iptables позволяет легко получить доступ к межсетевому экрану, однако большое количество флагов не всегда позволяет удобно ей пользоваться. В этом плане брандмауэр Windows более интуитивно понятно позволяет задавать правила.