Устранение уязвимостей

КУРС: АДМИНИСТРИРОВАНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ

СТУДЕНТ: ВОЛКОВА М.Д.

ГРУППА: 13541/2

Цель работы

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

Вывод всех правил

```
[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
```

Создание нового павила открытия TCP порта 80

```
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
```

Удаление правил из цепочки

```
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
```

```
iptables -F
```

Запрет исходящих соединений на конкретный адрес

```
iptables -A OUTPUT -d 8.8.8.8 -j DROP
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
```

```
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
```

Выводы

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.