

# БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

## МОДУЛЬ 4. АДМИНИСТРИРОВАНИЕ ВСТРОЕННЫХ СРЕДСТВ ЗАЩИТЫ LINUX

### ПРАКТИЧЕСКАЯ РАБОТА С ПРОВЕРКОЙ МЕНТОРОМ

#### ЗАДАНИЕ "YOU SHALL NOT PASS".

Выполнил: Андрей Степаненко (MIFIIB/2-й поток)

1. Подключитесь к виртуальной машине по SSH и введите команду “iptables -L”

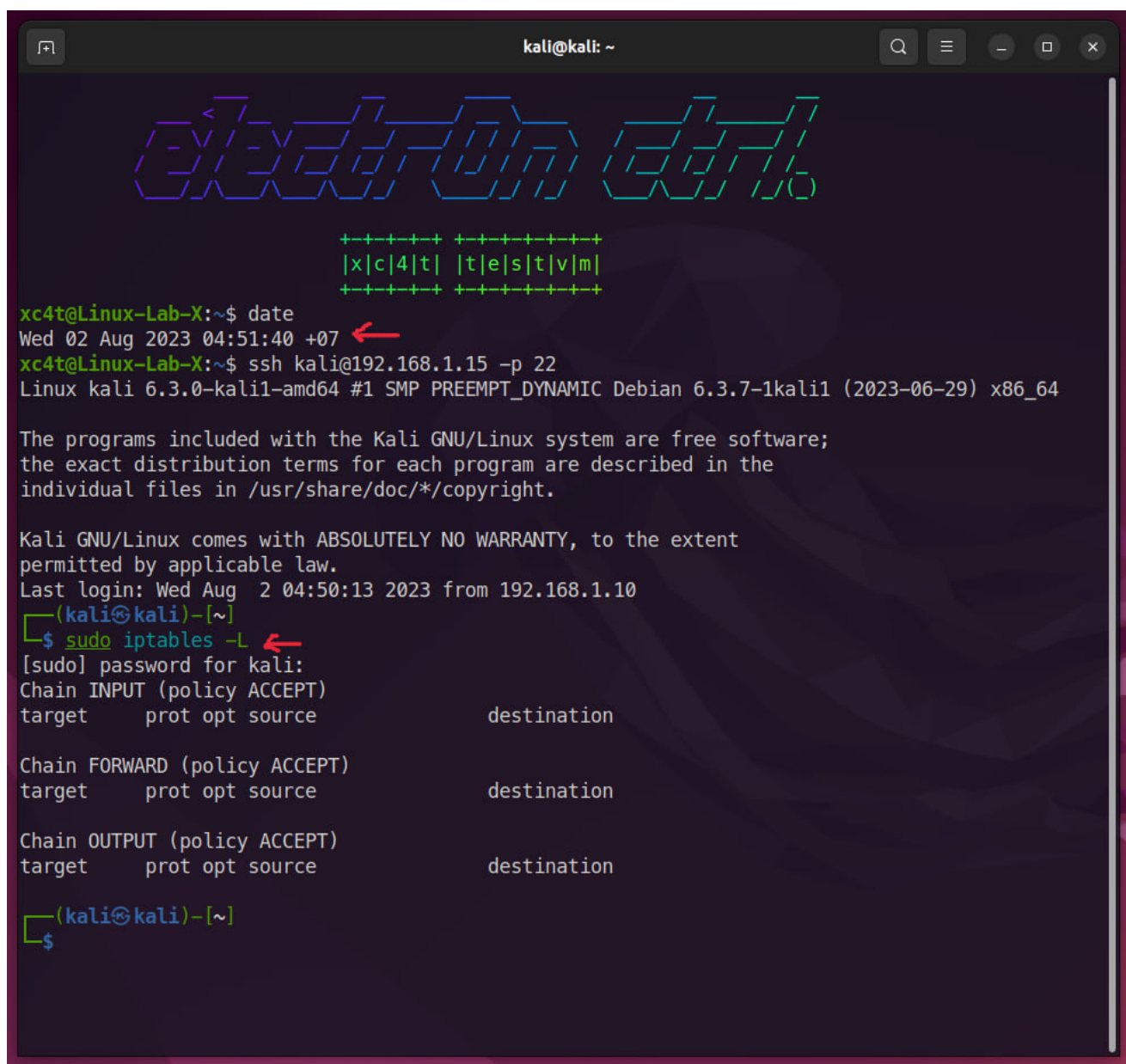
Последовательность выполнения в терминале:

# Выведем текущую дату командой “date”

# (На всех скриншотах должно быть хорошо видно текущее время вашей локальной машины.)

# Подключаемся к удалённой виртуальной машине по SSH: `ssh kali@192.168.1.15 -p 22`

# Выводим текущие настройки командой “`sudo iptables -L`”



```
kali@kali: ~  
date  
Wed 02 Aug 2023 04:51:40 +07  
ssh kali@192.168.1.15 -p 22  
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64  
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Wed Aug 2 04:50:13 2023 from 192.168.1.10  
(kali@kali)~  
$ sudo iptables -L  
[sudo] password for kali:  
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  
(kali@kali)~  
$
```

2. Напишите правило, которое будет запрещать входящие ICMP echo запросы к серверу. После чего заскриньте вывод цепочки так, чтобы новое правило попало в скриншот, а также в скриншотах должна быть команда, которую использовали.

#### Последовательность выполнения в терминале:

# Добавляем правило, запрещающее входящие ICMP echo запросы к серверу командой:

**#sudo iptables -A INPUT -p icmp -j DROP**

```
(kali㉿kali)-[~]
$ date
Wed Aug  2 04:52:31 +07 2023 ←

(kali㉿kali)-[~]
$ sudo iptables -A INPUT -p icmp -j DROP ←

(kali㉿kali)-[~]
$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      icmp -- anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

(kali㉿kali)-[~]
$ date
Wed Aug  2 04:52:47 +07 2023 ←

(kali㉿kali)-[~]
$
```

3. Попробуйте попинговать виртуальную машину с хоста.

4. Сфотографируйте неудачную попытку пинга.

```
(kali㉿kali)-[~]
$ exit
Connection to 192.168.1.15 closed.
xc4t@Linux-Lab-X:~$ ping 192.168.1.15
PING 192.168.1.15 (192.168.1.15) 56(84) bytes of data.
^C
--- 192.168.1.15 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4073ms

xc4t@Linux-Lab-X:~$ date
Wed 02 Aug 2023 04:55:13 +07
xc4t@Linux-Lab-X:~$
```

**5. Верните исходные настройки iptables любым удобным способом и заскриньте вывод цепочки без вашего правила.**

**Последовательность выполнения в терминале:**

**# Удаляем правило командой:**

**# sudo iptables -D INPUT 1**

**# Подтверждаем, что наши настройки вернулись в исходное состояние:**

```
kali@kali: ~  
  
(kali@kali)-[~]  
$ date  
Wed Aug 2 04:57:47 +07 2023 ←  
  
(kali@kali)-[~]  
$ sudo iptables -L  
Chain INPUT (policy ACCEPT)  
target      prot opt source                destination  
DROP        icmp -- anywhere             anywhere  
  
Chain FORWARD (policy ACCEPT)  
target      prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source                destination  
  
(kali@kali)-[~]  
$ sudo iptables -D INPUT 1  
  
(kali@kali)-[~]  
$ sudo iptables -L  
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  
  
(kali@kali)-[~]  
$ date  
Wed Aug 2 04:58:02 +07 2023 ←  
  
(kali@kali)-[~]  
$
```

















