

**ВВЕДЕНИЕ В КИБЕРБЕЗОПАСНОСТЬ
КОМПЬЮТЕРНЫЕ СЕТИ**

**ЛАБОРАТОРНАЯ РАБОТА № 4
Маршрутизация**

**Выполнил:
Мосолков Е.Н.
Преподаватель:
Минченков В.О.**

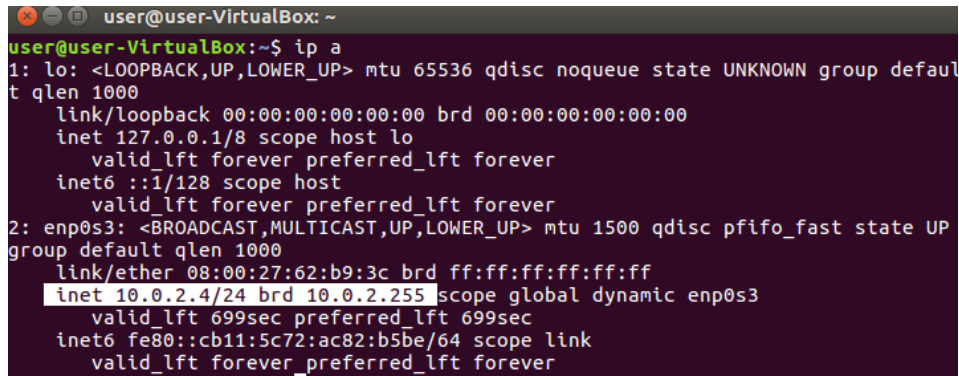
Москва 2020 г.

ЦЕЛЬ РАБОТЫ

Цель работы состоит в изучении iptables и WAF.

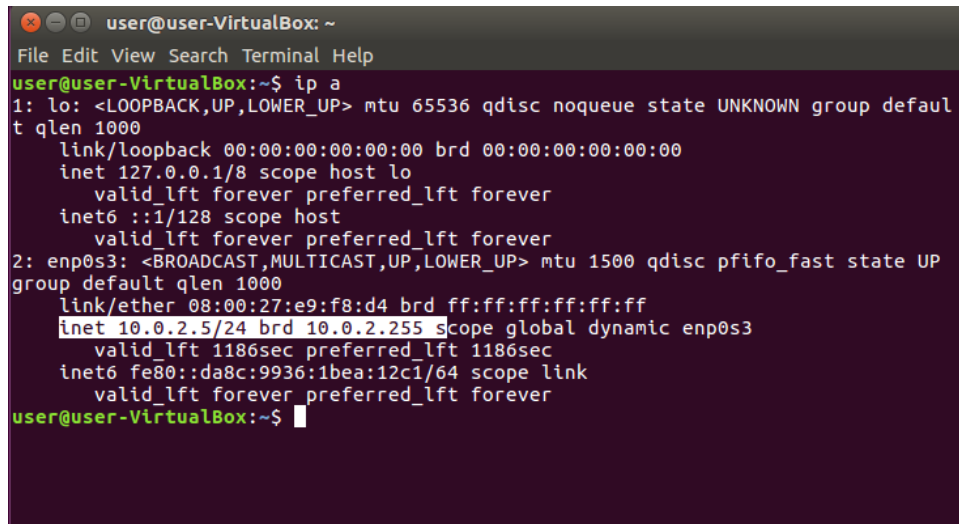
ХОД РАБОТЫ

Iptables



```
user@user-VirtualBox: ~  
user@user-VirtualBox:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP  
    group default qlen 1000  
    link/ether 08:00:27:62:b9:3c brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic enp0s3  
        valid_lft 699sec preferred_lft 699sec  
    inet6 fe80::cb11:5c72:ac82:b5be/64 scope link  
        valid_lft forever preferred_lft forever
```

Рис 1



```
user@user-VirtualBox: ~  
File Edit View Search Terminal Help  
user@user-VirtualBox:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP  
    group default qlen 1000  
    link/ether 08:00:27:e9:f8:d4 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.5/24 brd 10.0.2.255 scope global dynamic enp0s3  
        valid_lft 1186sec preferred_lft 1186sec  
    inet6 fe80::da8c:9936:1bea:12c1/64 scope link  
        valid_lft forever preferred_lft forever  
user@user-VirtualBox:~$
```

Рис 2

Выяснили IP адреса машин (выделенны на скриншотах). Рис 1 – атакуемая машина, рис 2 – атакующая.

Установили curl на атакующей

```

user@user-VirtualBox:~$ sudo apt-get install curl
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  Firefox Web Browser 5.0-112 linux-headers-4.15.0-112-generic
  linux-image-4.15.0-112-generic linux-modules-4.15.0-112-generic
  linux-modules-extra-4.15.0-112-generic
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  curl
0 upgraded, 1 newly installed, 0 to remove and 26 not upgraded.
Need to get 139 kB of archives.
After this operation, 340 kB of additional disk space will be used.
Get:1 http://ru.archive.ubuntu.com/ubuntu xenial-updates/main amd64 curl amd64 7
.47.0-1ubuntu2.16 [139 kB]
Fetched 139 kB in 0s (1 062 kB/s)
Selecting previously unselected package curl.
(Reading database ... 257666 files and directories currently installed.)
Preparing to unpack .../curl_7.47.0-1ubuntu2.16_amd64.deb ...
Unpacking curl (7.47.0-1ubuntu2.16) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up curl (7.47.0-1ubuntu2.16) ...
user@user-VirtualBox:~$

```

Установили apache2 и libapache2-mod-security2 на атакуемой

```

user@user-VirtualBox:~$ sudo apachectl -M | grep --color security2
AH00558: apache2: Could not reliably determine the server's fully qualified domain
name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
security2_module (shared)
user@user-VirtualBox:~$

```

Провели сканирование атакуемой машины

```

user@user-VirtualBox:~$ sudo nmap -sX 10.0.2.4
[sudo] password for user:

Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-09 15:30 MSK
Nmap scan report for 10.0.2.4
Host is up (0.00031s latency).
Not shown: 998 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
80/tcp    open|filtered http
MAC Address: 08:00:27:62:B9:3C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 44.14 seconds
user@user-VirtualBox:~$

```

Порт 80 открыт

Открываем и сбрасываем настройки iptables

```

user@user-VirtualBox:~$ sudo iptables -L
[sudo] password for user:
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
user@user-VirtualBox:~$ sudo iptables -F
user@user-VirtualBox:~$

```

Настраиваем атакуемую машину

```

user@user-VirtualBox: ~
user@user-VirtualBox:~$ sudo iptables -A INPUT -p tcp ! --syn -m state --state ESTABLISHED,RELATED -j DROP
user@user-VirtualBox:~$ sudo iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
user@user-VirtualBox:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination            state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere              anywhere               state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere              anywhere               tcp dpt:http
DROP       tcp  --  anywhere              anywhere               tcp flags:FIN,SYN,RST,PSH,ACK,URG/NONE
DROP       tcp  --  anywhere              anywhere               tcp flags:!FIN,SYN,RST,ACK/SYN state NEW
DROP       tcp  --  anywhere              anywhere               tcp flags:FIN,SYN,RST,PSH,ACK,URG
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
user@user-VirtualBox:~$

```

Повторно сканируем с атакующей машины

```

user@user-VirtualBox:~$ sudo nmap -sX 10.0.2.4
[sudo] password for user:

Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-09 15:46 MSK
Nmap scan report for 10.0.2.4
Host is up (0.00040s latency).
All 1000 scanned ports on 10.0.2.4 are open|filtered
MAC Address: 08:00:27:62:B9:3C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 37.85 seconds
user@user-VirtualBox:~$

```

WAF

Склонировали репозиторий и изменили конфиг файл

```
# -- Rule engine initialization -----
# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
SecRuleEngine On

# -- Request body handling -----

# Allow ModSecurity to access request bodies. If you don't, ModSecurity
# won't be able to see any POST parameters, which opens a large security
# hole for attackers to exploit.
#
SecRequestBodyAccess On

# Enable XML request body parser.

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

Отредактировали apache2.conf файл

```
user@user-VirtualBox: /usr/share/modsecurity-crs/activated_rules
GNU nano 2.5.3 File: /etc/apache2/mods-enabled/security2.conf Modified

<IfModule security2_module>
  Files Fault Debian dir for modsecurity's persistent data
  SecDataDir /var/cache/modsecurity

  # Include all the *.conf files in /etc/modsecurity.
  # Keeping your local configuration in that directory
  # will allow for an easy upgrade of THIS file and
  # make your life easier
  IncludeOptional /etc/modsecurity/*.conf
  Include /usr/share/modsecurity-crs/*.conf
  Include /usr/share/modsecurity-crs/activated_rules/*.conf
  Include /etc/modsecurity/rules/*.conf
</IfModule>

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

```
user@user-VirtualBox: /usr/share/modsecurity-crs/activated_rules
GNU nano 2.5.3 File: /etc/apache2/sites-available/000-default.conf

SecRuleEngine On
SecRule ARGS:testparam "@contains test" "id: 1234,deny,status:403,msg:'Our test'"
<VirtualHost *:80>
  # The ServerName directive sets the request scheme, hostname and port to
  # the server uses to identify itself. This is used when creating
  # redirection URLs. In the context of virtual hosts, the ServerName
  # specifies what hostname must appear in the request's Host: header to
  # match this virtual host. For the default virtual host (this file) this
  # value is not decisive as it is used as a last resort host regardless.
  # However, you must set it for any further virtual host explicitly.
  #ServerName www.example.com

  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html

  # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
  # error, crit, alert, emerg.
  # It is also possible to configure the loglevel for particular
  # modules, e.g.
  #
  #LogLevel warn

  # Read 33 lines
  ^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
  ^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

Донастраиваем сеть и выполняем запрос на атакующей машине

```
user@user-VirtualBox:~$ curl 10.0.2.4/index.html?testparam=test
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at 10.0.2.4 Port 80</address>
</body></html>
user@user-VirtualBox:~$
```

Все верно

Выполняем сканирование nmap с опцией детектирования WAF

```
user@user-VirtualBox:~$ sudo nmap -p 80 -sV --script=http-waf-fingerprint 10.0.2.4
[sudo] password for user:

Starting Nmap 7.01 ( https://nmap.org ) at 2020-12-09 18:03 MSK
Nmap scan report for 10.0.2.4
Host is up (0.00041s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:62:B9:3C (Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.59 seconds
```

```
--8df8fd4d-A--
[09/Dec/2020:18:00:04 +0300] X9DmdH8AAQEAAEvN0EsAAAAAN 10.0.2.5 34286 10.0.2.4 80
--8df8fd4d-B--
GET /index.html?testparam=test HTTP/1.1
Host: 10.0.2.4
User-Agent: curl/7.47.0
Accept: */*
```

Видим что команда сработала

Вопросы к лабораторной работе

1. Программный или программно-аппаратный элемент компьютерной сети
2. Фильтрует и контролирует проходящую через него информацию, защищает от несанкционированного доступа
3. Когда сетевые пакеты попадают в сетевой интерфейс, они после ряда проверок ядром проходят последовательность так называемых цепочек. Пакет обязательно проходит через цепочку PREROUTING, после чего определяется, кому он, собственно, был адресован. Если пакет не адресован локальной системе (в нашем случае серверу), он попадает в цепочку FORWARD, а иначе — в цепочку INPUT, после прохождения которой отдается локальным демонам или процессам. После этого при необходимости формируется ответ, который направляется в цепочку OUTPUT. После цепочек OUTPUT или FORWARD пакет в очередной раз встречается с правилами маршрутизации и направляется в цепочку POSTROUTING. В результате прохождения пакетом цепочек фильтрации несколько раз, проверка его принадлежности определенным критериям осуществляется несколько раз.
4. Таблицы межсетевого экрана Netfilter: raw, filter, nat, mangle

raw – маркирует пакеты, которые не должны обрабатываться системой определения состояний. Содержатся в цепочках PREROUTING и OUTPUT

filter – основная таблица, используется по умолчанию

nat – предназначена для подмены адреса отправителя или получателя. Данную таблицу проходят только первые пакеты из потока - трансляция адресов или маскировка (подмена адреса отправителя или получателя) применяются ко всем последующим пакетам в потоке автоматически. Поддерживает действия DNAT, SNAT, MASQUERADE, REDIRECT. Содержится в цепочках PREROUTING, OUTPUT, и POSTROUTING

mangle – таблица с правилами модификации IP пакетов

5. Правила межсетевых экранов – это ситуации при которых запрещается передача трафика, во избежание взлома устройства
6. Рассмотрим две цепочки, задающие два основных правила Iptables — PREROUTING и FORWARD.

```
- iptables -t nat -A PREROUTING -i eth0 -j DNAT --to-destination 192.168.57.102
```

```
- iptables -A FORWARD -d 192.168.57.102 -j ACCEPT
```

7. Утилита iptables-persistent
8. WAF (Web Application Firewall) - это межсетевые экраны, работающие на прикладном уровне и осуществляющие фильтрацию трафика Web-приложений. Эти средства не требуют изменений в исходном коде Web-приложения и, как правило, защищают Web-сервисы гораздо лучше обычных межсетевых экранов и средств обнаружения вторжений.
9. Изменить конфигурационный файл modsecurity