Лабораторная работа Iptables,
WEB APPLICATION FIREWALL

Цель: Изучение межсетевых экранов. Приобретение навыков работы с Iptables и WAF.

Часть 1.

сетевые настройки атакующей машины :

```
user@user-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether 00:0c:29:2f:c6:d3 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.21/27 brd 10.10.10.31 scope global dynamic ens33
       valid_lft 1619sec preferred_lft 1619sec
    inet6 fe80::90aa:16a:d3fe:a5b6/64 scope link
       valid_lft forever preferred_lft forever
```

сетевые настройки атакуемой машины :

```
user@user-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether 00:0c:29:b9:64:24 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.22/27 brd 10.10.10.31 scope global dynamic ens33
       valid_lft 1667sec preferred_lft 1667sec
    inet6 fe80::5c9c:99bf:37d8:85a6/64 scope link
       valid_lft forever preferred_lft forever
```

Установка доп. пакетов на атакующую машину :

```
user@user-VirtualBox:~$ sudo apt-get update
[sudo] password for user:
Hit:1 http://ru.archive.ubuntu.com/ubuntu xenial InRelease
Get:2 http://ru.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Hit:3 http://security.ubuntu.com/ubuntu xenial-security InRelease
Get:4 http://ru.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Fetched 216 kB in 1s (187 kB/s)
Reading package lists... Done
user@user-VirtualBox:~$ sudo apt-get install curl
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libcurl3-gnutls
The following NEW packages will be installed:
  curl
```

```
user@user-VirtualBox:~$ sudo apt-get install curl
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libcurl3-gnutls
The following NEW packages will be installed:
  curl
The following packages will be upgraded:
  libcurl3-gnutls
1 upgraded, 1 newly installed, 0 to remove and 91 not upgraded.
Need to get 139 kB/323 kB of archives.
After this operation, 340 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ru.archive.ubuntu.com/ubuntu xenial-updates/main amd64 curl amd64 7
.47.0-1ubuntu2.18 [139 kB]
Fetched 139 kB in 0s (1 120 kB/s)
(Reading database ... 222135 files and directories currently installed.)
Preparing to unpack .../libcurl3-gnutls_7.47.0-1ubuntu2.18_amd64.deb ...
```

Установка доп. пакетов на атакуемую машину :

```
user@user-VirtualBox:~$ sudo apt-get update
[sudo] password for user:
Hit:1 http://security.ubuntu.com/ubuntu xenial-security InRelease
Hit:2 http://ru.archive.ubuntu.com/ubuntu xenial InRelease
Get:3 http://ru.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Get:4 http://ru.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Fetched 216 kB in 2s (101 kB/s)
Reading package lists... 99%
```

```
user@user-VirtualBox:~$ sudo apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-4.15.0-112 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 additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0
0 upgraded, 9 newly installed, 0 to remove and 32 not upgraded.
Need to get 1 542 kB of archives.
After this operation, 6 386 kB of additional disk space will be used.
```

```
user@user-VirtualBox:~$ sudo apt-get install libapache2-mod-security2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-4.15.0-112 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 additional packages will be installed:
  modsecurity-crs
Suggested packages:
  lua geoip-database-contrib ruby
The following NEW packages will be installed:
  libapache2-mod-security2 modsecurity-crs
0 upgraded, 2 newly installed, 0 to remove and 32 not upgraded.
Need to get 524 kB of archives.
After this operation, 3 844 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Выполняю команду sudo apachectl -M | grep --color security2
(Apache не смог найти валидную директиву ServerName в своем конфигурационном файле, поэтому он будет использовать первый обнаруженный IP-адрес. В данном примере это внешний IP-адрес сервера: 127.0.1.1

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

Провожу nmap Xmas сканирование атакуемой машины на порту 80 :

```
user@user-VirtualBox:~$ sudo nmap -sX -p 80 10.10.10.22

Starting Nmap 7.01 ( https://nmap.org ) at 2021-01-30 10:28 MSK
Nmap scan report for 10.10.10.22
Host is up.
PORT   STATE         SERVICE
80/tcp open|filtered http

Nmap done: 1 IP address (1 host up) scanned in 2.39 seconds
```

Список текущих правил iptables таблицы filter :

```
user@user-VirtualBox:~$ 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
```

Данный список можно просмотреть в другом формате, который отражает команды, необходимые для активации правил и политик :

```
user@user-VirtualBox:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
user@user-VirtualBox:~$
```

Сбрасываю текущие правила
Вношу локальный интерфейс в разрешенные
Разрешаю подключения к порту SSH 22
Разрешаю подключения к порту http 80
Так как не будем использовать SSH, удалим ненужное правило
Добавим еще одно правило, которое позволит устанавливать исходящие соединения
Создав все эти правила, можно заблокировать все остальное и разрешить все исходящие соединения

```
user@user-VirtualBox:~$ sudo iptables -F
user@user-VirtualBox:~$ sudo iptables -A INPUT -i lo -j ACCEPT
user@user-VirtualBox:~$ sudo iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEP
T
user@user-VirtualBox:~$ sudo iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEP
T
user@user-VirtualBox:~$ sudo iptables -D INPUT -p tcp -m tcp --dport 22 -j ACCEP
T
user@user-VirtualBox:~$ sudo iptables -I INPUT -m state --state ESTABLISHED,RELA
TED -j ACCEPT
user@user-VirtualBox:~$ sudo iptables -P OUTPUT ACCEPT
user@user-VirtualBox:~$ sudo iptables -P INPUT DROP
```

Ещё раз посмотрим список правил :

```
user@user-VirtualBox:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTA
BLISHED
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

Заблокируем нулевые пакеты
Создадим правило, которое отражает атаки syn-пакетами без состояния NEW
(Теперь фаервол не будет принимать входящих пакетов с tcp-флагами)
Защищаем сервер от разведывательных пакетов XMAS
Загружаем пакет iptables-persistent, теперь текущие правила можно сохранить

```
user@user-VirtualBox:~$ sudo iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DR
OP
user@user-VirtualBox:~$ sudo iptables -A INPUT -p tcp ! --syn -m state --state N
EW -j DROP
user@user-VirtualBox:~$ sudo iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DRO
P
user@user-VirtualBox:~$ sudo apt-get install iptables-persistent
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-4.15.0-112 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 additional packages will be installed:
  netfilter-persistent
The following NEW packages will be installed:
  iptables-persistent netfilter-persistent
0 upgraded, 2 newly installed, 0 to remove and 32 not upgraded.
Need to get 13,3 kB of archives.
After this operation, 79,9 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Со второй виртуальной машины провожу XMAS сканирование :

```
user@user-VirtualBox:~$ sudo nmap -sX 10.10.10.22
[sudo] password for user:

Starting Nmap 7.01 ( https://nmap.org ) at 2021-01-30 10:39 MSK
Nmap scan report for 10.10.10.22
Host is up (0.00047s latency).
All 1000 scanned ports on 10.10.10.22 are open|filtered
MAC Address: 00:0C:29:B9:64:24 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 22.19 seconds
```

Часть 2.

Загрузим пакет правил OWASP на атакуемую машину :

```
user@user-VirtualBox:~$ cd ~
user@user-VirtualBox:~$ git clone https://github.com/SpiderLabs/owasp-modsecurit
y-crs.git
```

И установим их в модуль защиты :

```
Cloning into 'owasp-modsecurity-crs'...
remote: Enumerating objects: 10486, done.
remote: Total 10486 (delta 0), reused 0 (delta 0), pack-reused 10486
Receiving objects: 100% (10486/10486), 3.33 MiB | 902.00 KiB/s, done.
Resolving deltas: 100% (7687/7687), done.
Checking connectivity... done.
user@user-VirtualBox:~$ cd owasp-modsecurity-crs
user@user-VirtualBox:~/owasp-modsecurity-crs$ sudo cp crs-setup.conf.example /et
c/modsecurity/crs-setup.conf
user@user-VirtualBox:~/owasp-modsecurity-crs$ sudo cp -R rules/ /etc/modsecurity
/
user@user-VirtualBox:~/owasp-modsecurity-crs$
```

Переименуем конфигурационный файл :

```
user@user-VirtualBox:~/owasp-modsecurity-crs$ sudo mv /etc/modsecurity/modsecuri
ty.conf-recommended /etc/modsecurity/modsecurity.conf
```

Конфигурационный файл настроен на DetectionOnly, то есть, фаервол только отслеживает логи, при этом ничего не блокируя. Изменим это :

```
  GNU nano 2.5.3      File: /etc/modsecurity/modsecurity.conf         Modified

# -- 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.
#
```

Добавьте несколько правил из каталога /usr/share/modsecurity-crs/ :

```
user@user-VirtualBox:~/owasp-modsecurity-crs$ cd /usr/share/modsecurity-crs/acti
vated_rules/
user@user-VirtualBox:/usr/share/modsecurity-crs/activated_rules$ sudo ln -s /usr
/share/modsecurity-crs/base_rules/modsecurity_crs_30_http_policy.conf
user@user-VirtualBox:/usr/share/modsecurity-crs/activated_rules$ sudo ln -s /usr
/share/modsecurity-crs/base_rules/modsecurity_crs_21_protocol_anomalies.conf
user@user-VirtualBox:/usr/share/modsecurity-crs/activated_rules$
```

Чтобы подгрузить эти готовые правила и правила OWASP, нужно, чтобы веб-сервер Apache читал указанные выше каталоги. Для этого отредактируем файл security2.conf :

```
  GNU nano 2.5.3    File: /etc/apache2/mods-enabled/security2.conf    Modifie

<IfModule security2_module>
        # Default 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>
```

Перезапускаем Apache, чтобы новые правила вступили в силу :

```
user@user-VirtualBox:/usr/share/modsecurity-crs/activated_rules$ sudo service ap
ache2 reload
```

В каталоге логов Apache можно найти новый лог-файл для mod_security :

```
  GNU nano 2.5.3      File: /var/log/apache2/modsec_audit.log
```

Откроем для редактирования дефолтный файл конфигурации сайта 000-default.conf и изменим его таким образом :

```
  GNU nano 2.5.3  File: /etc/apache2/sites-available/000-default.conf Modified

        # 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 info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
SecRuleEngine On
$ test rule has triggered' "
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

(теперь при попытке запроса с параметром «testparam» запрос будет отклонен с кодом 403)

На атакующей машине выполним следующий запрос :

```
user@user-VirtualBox:~$ curl 10.10.10.22/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 10.10.10.22 Port 80</address>
</body></html>
```

(результат «403 Forbidden»)

Выполним сканирование утилитой nmap с опцией детектирования WAF :

```
user@user-VirtualBox:~$ sudo nmap -p 80 -sV --script=http-waf-fingerprint 10.10.
10.22
[sudo] password for user:

Starting Nmap 7.01 ( https://nmap.org ) at 2021-01-30 11:03 MSK
Nmap scan report for 10.10.10.22
Host is up (0.00057s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 00:0C:29:B9:64:24 (VMware)
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 7.44 seconds
```

На атакуемой машине в лог-файле /var/log/apache2/modsec_audit.log данное сканирование будет полностью зафиксировано :

```
  GNU nano 2.5.3      File: /var/log/apache2/modsec_audit.log

--1658d25d-A--
[30/Jan/2021:11:01:30 +0300] YBUSWn8AAQEAAG@yIu0AAAAH 10.10.10.21 35540 10.10.1$
--1658d25d-B--
GET /index.html?testparam=test HTTP/1.1
Host: 10.10.10.22
User-Agent: curl/7.47.0
Accept: */*

--1658d25d-F--
HTTP/1.1 403 Forbidden
Content-Length: 276
Content-Type: text/html; charset=iso-8859-1

--1658d25d-E--
<!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 10.10.10.22 Port 80</address>
</body></html>
```

Вывод : узнал о принцип работы Netfilter, научился работать с утилитой Iptables, научился защищать сервер от некоторых общих атак, научился тестировать модуль защиты WAF, поработал с веб-сервером apache2.