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

Выполнение.

Часть 1. Iptables

1) На атакующую машину необходимо установить дополнительные пакеты. Выполним в терминале следующие команды:
sudo apt-get update
sudo apt-get install curl

```
root@user-VirtualBox:/home/user# apt-get update
Hit:1 http://ru.archive.ubuntu.com/ubuntu xenial InRelease
Hit:2 http://ru.archive.ubuntu.com/ubuntu xenial-updates InRelease
Hit:3 http://ru.archive.ubuntu.com/ubuntu xenial-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu xenial-security InRelease
Reading package lists... Done
root@user-VirtualBox:/home/user# 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 159 not upgraded.
Need to get 139 kB/328 kB of archives.
After this operation, 352 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
```

2) Установив веб-сервер: sudo apt-get install apache2

```
root@user-VirtualBox:/home/user# apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.18-2ubuntu3.17).
0 upgraded, 0 newly installed, 0 to remove and 160 not upgraded.
root@user-VirtualBox:/home/user# apt-get install libapache2-mod-security2
Reading package lists... Done
Building dependency tree
Reading state information... Done
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 160 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]
```

3) Выполним команду <sudo apachectl -M l grep --color security2>. Если на экране появился модуль по имени security2_module (shared), значит, все прошло успешн

```
root@user-VirtualBox:/home/user# 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)
root@user-VirtualBox:/home/user#
```

4) Проведем сканирование на порту 80

```
root@user-VirtualBox:/home/user# nmap -sX -p 80 192.168.1.10

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-22 10:30 MSK
Nmap scan report for 192.168.1.10
Host is up (0.00073s latency).
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 08:00:27:A2:13:50 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
```

5) Далее настроим защиту атакуемой машины: Просмотрим список текущих правил iptables таблицы filter
sudo iptables -L

```
root@user-VirtualBox:/home/user# 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
```

6) Чтобы заблокировать весь исходящий трафик, кроме портов для SSH и веб-сервера, нужно сначала разрешить подключения к этим портам. В цепочку ACCEPT добавим два порта (порт SSH 22 и порт http 80), что разрешит трафик на эти порты.
sudo iptables -A INPUT -p tcp -m tcp –dport 22 -j ACCEPT
sudo iptables -A INPUT -p tcp -m tcp –dport 80 -j ACCEPT

```
root@user-VirtualBox:/home/user# iptables -A INPUT -i lo -j ACCEPT
root@user-VirtualBox:/home/user# iptables -I INPUR -m state --state ESTABLISHED,
RELATED -j ACCEPT
iptables: No chain/target/match by that name.
root@user-VirtualBox:/home/user# iptables -I INPUT -m state --state ESTABLISHED,
RELATED -j ACCEPT
root@user-VirtualBox:/home/user#
```

7) Создав все эти правила, можно заблокировать все остальное и разрешить все исходящие соединения.
sudo iptables -P OUTPUT ACCEPT
sudo iptables -P INPUT DROP

```
root@user-VirtualBox:/home/user# iptables -P OUTPUT ACCEPT
root@user-VirtualBox:/home/user# iptables -P INPUT DROP
root@user-VirtualBox:/home/user# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTA
BLISHED
ACCEPT     all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@user-VirtualBox:/home/user#
```

8) Добавим еще несколько правил для блокировки наиболее распространенных атак
Для начала нужно заблокировать нулевые пакеты
sudo iptables -A INPUT -p tcp –tcp-flags ALL NONE -j DROP. Следующее правило отражает атаки syn-пакетами без состояния NEW
sudo iptables -A INPUT -p tcp ! –syn -m state –state NEW -j DROP

```
root@user-VirtualBox: /home/user
root@user-VirtualBox:/home/user# iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
root@user-VirtualBox:/home/user# iptables -A INPIT -p tcp ! --syn -m state --state NEW -j
DROP
iptables: No chain/target/match by that name.
root@user-VirtualBox:/home/user# iptables -A INPuT -p tcp ! --syn -m state --state NEW -j
DROP
iptables: No chain/target/match by that name.
root@user-VirtualBox:/home/user# iptables -A INPUT -p tcp ! --syn -m state --state NEW -j
DROP
root@user-VirtualBox:/home/user# iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
root@user-VirtualBox:/home/user#
```

9) Установим пакеты.

```
root@user-VirtualBox: /home/user
root@user-VirtualBox:/home/user# apt-get install iptables-persistent
Reading package lists... Done
Building dependency tree
Reading state information... Done
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 159 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] y
```

10) Со второй виртуальной машины, проведем XMAS сканирование и зафиксируем результат в отчете
sudo nmap -sX

```
root@user-VirtualBox:/home/user# nmap -sX -p 80 192.168.1.10

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-22 10:37 MSK
Nmap scan report for 192.168.1.10
Host is up (0.00077s latency).
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 08:00:27:A2:13:50 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

Часть 2. WAF

1) Загрузим пакеты на атакуемую машину

```
root@user-VirtualBox:/home/user# cd ~
root@user-VirtualBox:~# git clone https://github.com/coreruleset/coreruleset.git
Cloning into 'coreruleset'...
remote: Enumerating objects: 35273, done.
remote: Counting objects: 100% (245/245), done.
remote: Compressing objects: 100% (128/128), done.
remote: Total 35273 (delta 215), reused 118 (delta 117), pack-reused 35028 (from 4)
Receiving objects: 100% (35273/35273), 10.23 MiB | 4.62 MiB/s, done.
Resolving deltas: 100% (27898/27898), done.
Checking connectivity... done.
```

2) Установим модуль защиты

```
root@user-VirtualBox: ~/coreruleset
root@user-VirtualBox:~/coreruleset# cp -R rules/ /etc/modsecurity/
root@user-VirtualBox:~/coreruleset# rm /etc/modsecurity/rules/REQUEST-922-MULTIPART-ATTACK
.conf
root@user-VirtualBox:~/coreruleset#
```

3) Установка ModSecurity включает в себя конфигурационный файл, который нужно переименовать:
sudo mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf

```
root@user-VirtualBox:~/coreruleset# mv /etc/modsecurity/modsecurity.conf-recomme
nded /etc/modsecurity/modsecurity.conf
root@user-VirtualBox:~/coreruleset#
```

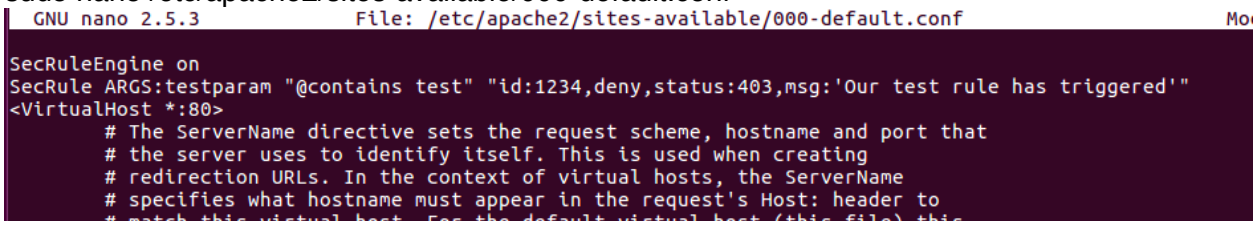
4) Стандартный конфигурационный файл настроен на DetectionOnly, то есть, фаервол только отслеживает логи, при этом ничего не блокируя. Чтобы изменить это поведение, отредактируйте файл modsecurity.conf:
sudo nano /etc/modsecurity/modsecurity.conf

```
# -- Rule engine initialization ----------------------------------------

# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installatio
# 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.
```

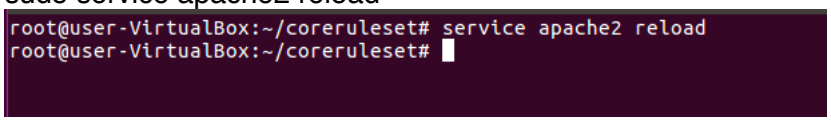
5) Чтобы подгрузить эти готовые правила и правила OWASP, нужно, чтобы веб-сервер Apache читал указанные выше каталоги. Для этого отредактируйте файл security2.conf:
sudo nano /etc/apache2/mods-enabled/security2.conf

```
<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
        IncludeOptional /etc/modsecurity/rules/*.conf
</IfModule>
```

6) Откройте для редактирования дефолтный файл конфигурации сайта 000-default.conf
sudo nano /etc/apache2/sites-available/000-default.conf

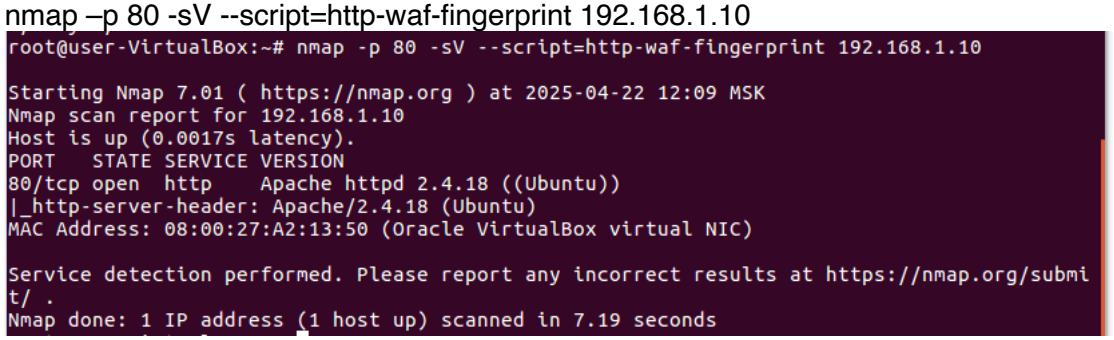


7) Чтобы новые правила вступили в исполнение, нужно перезапустить Apache
sudo service apache2 reload

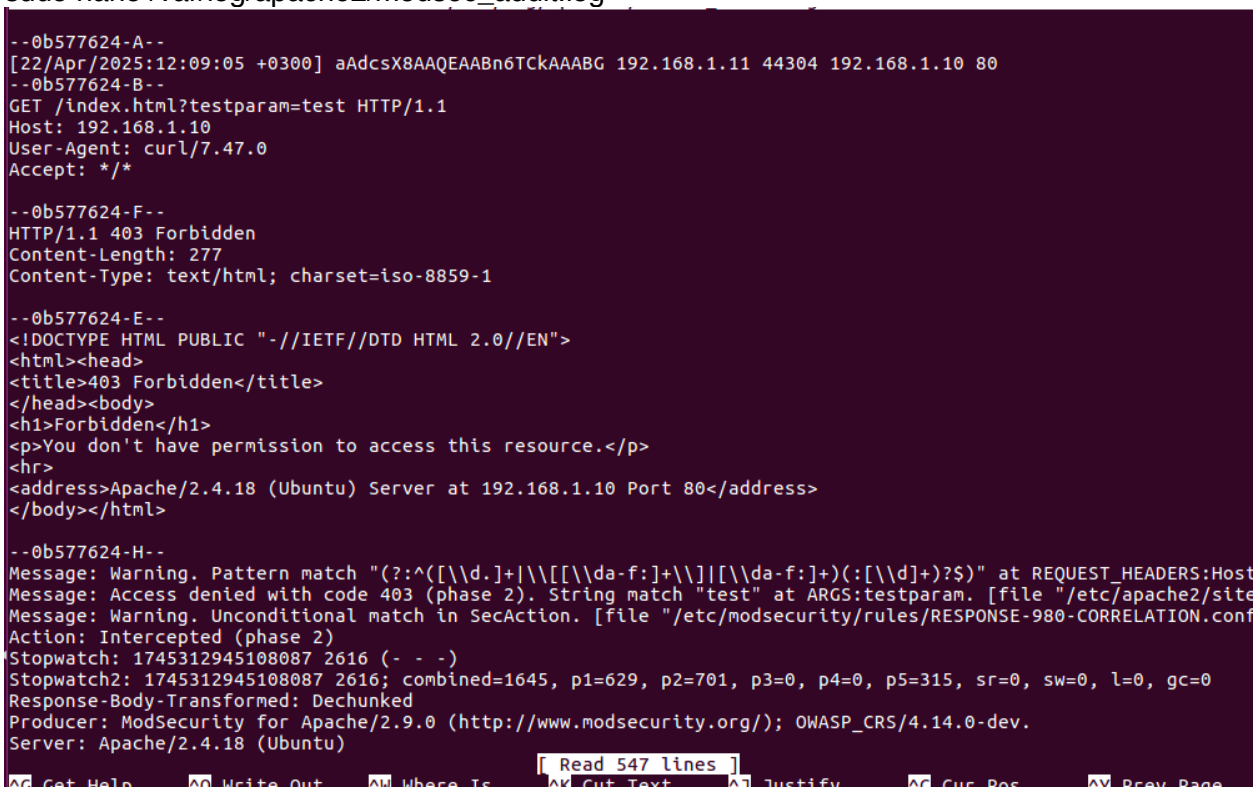


8) На атакующей машине выполните следующий запрос curl IP_атакуемой_ машины/index.html?testparam=test

9) Для закрепления результата выполните сканирование утилитой nmap с опцией детектирования WAF. Выполните на атакующей машине:
nmap –p 80 -sV --script=http-waf-fingerprint 192.168.1.10



10)К сожалению данное сканирование не даст наглядного результата, но на атакуемой машине в лог-файле /var/log/apache2/modsec_audit.log данное сканирование будет полностью зафиксировано. Просмотрите данный файл:
sudo nano /var/log/apache2/modsec_audit.log



Вопросы к лабораторной работе

1. Что такое межсетевой экран?

Межсетевой экран (firewall) — это программное или аппаратное средство, которое контролирует и фильтрует сетевой трафик между различными сегментами сети на основе заданных правил безопасности.

2. Для чего используется межсетевой экран?

Он используется для защиты компьютеров и сетей от несанкционированного доступа, вредоносного трафика и атак, таких как сканирование портов, DDoS-атаки, и для ограничения доступа к определённым ресурсам.

3. Принцип работы Netfilter.

Netfilter — это подсистема ядра Linux, обрабатывающая сетевые пакеты. Она анализирует пакеты по определённым цепочкам и таблицам и применяет к ним заданные правила, определяя: разрешить, отклонить или изменить пакет.

4. Таблицы межсетевого экрана Netfilter. Для чего они используются?

Таблица filter используется для фильтрации пакетов (основная).
Таблица nat применяется для трансляции сетевых адресов.
Таблица mangle служит для изменения заголовков пакетов.
Таблица raw используется для предварительной обработки до применения остальных таблиц.
Таблица security используется совместно с SELinux.

5. Что такое правила межсетевого экрана?

Это инструкции, определяющие действия над пакетами на основе их параметров (IP, порт, протокол и т.д.). Они указывают, пропускать ли трафик, блокировать или изменять.

6. Как создавать правила для межсетевого экрана утилитой Iptables?

Для этого используется команда `iptables` с параметрами. Например, чтобы разрешить входящие подключения на порт 80 (HTTP):

`iptables -A INPUT -p tcp --dport 80 -j ACCEPT`

7. Как сохранить правила для последующей автозагрузки?

На Debian/Ubuntu можно сохранить с помощью команды `iptables-save > /etc/iptables/rules.v4`.
На CentOS/RHEL — через `service iptables save`.
Также можно использовать пакет `iptables-persistent`.

8. Что такое Web Application Firewall?

WAF — это межсетевой экран, фильтрующий HTTP-запросы и защищающий веб-приложения от атак, таких как SQL-инъекции, XSS и другие уязвимости уровня приложений.

9. Как настроить правила в WAF mod_security?

mod_security использует набор правил в конфигурационных файлах. Пример правила: запрет доступа к адресу `/admin`

SecRule REQUEST_URI "@contains /admin" "id:1001,deny,status:403,msg:'Запрещён доступ к /admin'"

Файлы правил обычно находятся в `/etc/modsecurity/`.

Вывод: В ходе ЛР мы изучили межсетевые экраны. Приобрели навыки работы с Iptables и WAF.