Лабораторная работа №5

Расширенная настройка HTTP-сервера Apache

Мантуров Татархан Бесланович

Содержание

Цель работы

Приобрести практические навыки по расширенному конфигурированию HTTP-сервера Apache в части безопасности и возможности использования PHP.

Задание

1. Сгенерировать криптографический ключ и самоподписанный сертификат безопасности для возможности перехода веб-сервера от работы через протокол HTTP к работе через протокол HTTPS;
2. Настроить веб-сервер для работы с PHP;
3. Написать скрипт для Vagrant, фиксирующий действия по расширенной настройке HTTP-сервера во внутреннем окружении виртуальной машины server.

Выполнение лабораторной работы

Конфигурирование HTTP-сервера для работы через протокол HTTPS

Загрузим вашу операционную систему и перейдем в рабочий каталог с проектом: cd C:\Users\dasha\work\study\tbmanturov\vagrant

Запустим виртуальную машину server: make server-up

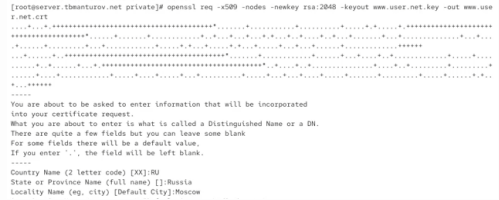
На виртуальной машине server войдем под своим пользователем и откроем терминал. Перейдем в режим суперпользователя: sudo -i

В каталоге /etc/ssl создадим каталог private.

```
[root@server.tbmanturov.net server]# mkdir -p /etc/pki/tls/private
[root@server.tbmanturov.net server]# ln -s /etc/pki/tls/private /etc/ssl/private
[root@server.tbmanturov.net server]# cd /etc/pki/tls/private
[root@server.tbmanturov.net private]#
```

Создание каталога private

Сгенерируем ключ и сертификат:



Генерация ключа и сертификата

- req -x509 означает, что используется запрос подписи сертификата x509 (CSR);
- параметр -nodes указывает OpenSSL, что нужно пропустить шифрование сертификата SSL с использованием парольной фразы, т.е. позволить Apache читать файл без какого-либо вмешательства пользователя (без ввода пароля при попытке доступа к странице, в частности);
- параметр -newkey rsa: 2048 указывает, что одновременно создаются новый ключ и новый сертификат, причём используется 2048-битный ключ RSA;
- параметр -keyout указывает, где хранить сгенерированный файл закрытого ключа при создании;
- параметр -out указывает, где разместить созданный сертификат SSL. Далее требуется заполнить сертификат:

Сгенерированные ключ и сертификат появявились в соответствующем каталогах /etc/ssl/private и /etc/ssl/certs.

Для перехода веб-сервера www.tbmanturov.net на функционирование через протокол HTTPS требуется изменить его конфигурационный файл. Перейдем в каталог с конфигурационными файлами: cd /etc/httpd/conf.d

Откроем на редактирование файл /etc/httpd/conf.d/www.tbmanturov.net.conf и заменим его содержимое на следующее:

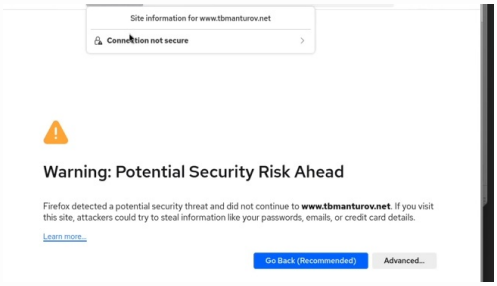
```
<VirtualHost *:80>
  ServerAdmin webmaster@tbmanturov.net
  DocumentRoot /var/www/html/www.tbmanturov.net
  ServerName www.tbmanturov.net
  ServerAlias www.tbmanturov.net
  ErrorLog logs/www.tbmanturov.net-error_log
  CustomLog logs/www.tbmanturov.net-access_log common
  RewriteEngine on
  RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=301,L]
</VirtualHost>

<IfModule mod_ssl.c>
<VirtualHost *:443>
  SSLEngine on
  ServerAdmin webmaster@tbmanturov.net
  DocumentRoot /var/www/html/www.tbmanturov.net
  ServerName www.tbmanturov.net
  ServerAlias www.tbmanturov.net
  ErrorLog logs/www.tbmanturov.net-error_log
  CustomLog logs/www.tbmanturov.net-access_log common
  SSLCertificateFile /etc/ssl/certs/www.tbmanturov.net.crt
  SSLCertificateKeyFile /etc/ssl/private/www.tbmanturov.net.key
</VirtualHost>
</IfModule>
```

Редактирование файла

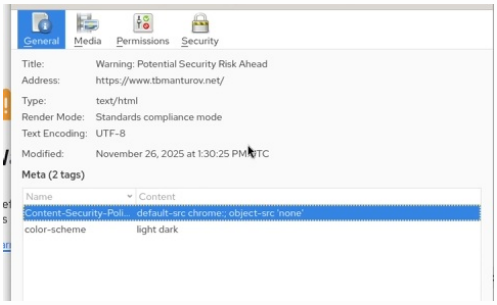
Внесем изменения в настройки межсетевого экрана на сервере, разрешив работу с https. Перезапустим веб-сервер: systemctl restart httpd.

Настройка межсетевого экрана на сервере

На виртуальной машине client в строке браузера введем название веб-сервера www.user.net и убедимся, что произойдёт автоматическое переключение на работу по протоколу HTTPS. На открывшейся странице с сообщением о незащищённости соединения нажмем кнопку «Дополнительно», затем добавим адрес сервера в постоянные исключения. Затем просмотрим содержание сертификата.



Сообщение о незащищенности на сайте



Добавление адреса сервера в исключения

Конфигурирование HTTP-сервера для работы с PHP

Установим пакеты для работы с PHP: dnf -y install php

Установка пакетов для работыы с php

В каталоге /var/www/html/www.tbmanturov.net заменим файл index.html на index.php следующего содержания:

```
<?php
phpinfo();
?>
```

Редактирование файла index.php

Скорректируем права доступа в каталог с веб-контентом: chown -R apache:apache /var/www

Восстановим контекст безопасности в SELinux:

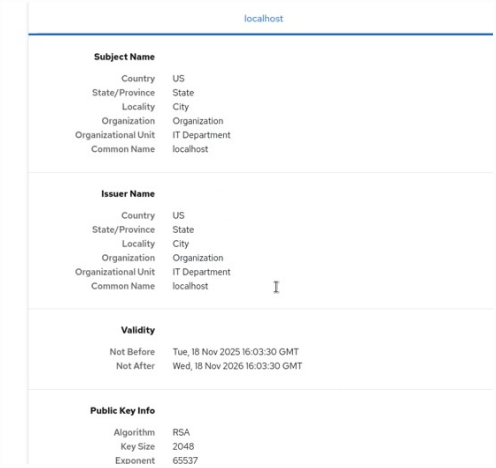
restorecon -vR /etc
restorecon -vR /var/www

Перезапустим HTTP-сервер: systemctl restart httpd

```
[root@server.tbmanturov.net www.tbmanturov.net]# restorecon -vR /etc
[root@server.tbmanturov.net www.tbmanturov.net]# restorecon -vR /var/www
[root@server.tbmanturov.net www.tbmanturov.net]# systemctl restart
```

Права доступа и контекст безопасности в SELinux

На виртуальной машине client в строке браузера введием название веб-сервера www.tbmanturov.net и убедимся, что будет выведена страница с информацией об используемой на веб-сервере версии PHP.



Содержание сайта

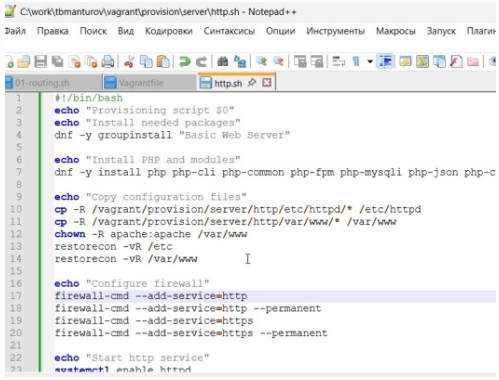
Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/http и в соответствующие каталоги скопируйте конфигурационные файлы:

```
[root@server.tbmanturov.net www.tbmanturov.net]# cp -R /var/www/html/* /vagrant/
provision/server/http/var/www/html
cp: overwrite '/vagrant/provision/server/http/var/www/html/www.tbmanturov.net/in
dex.php'? yes
[root@server.tbmanturov.net www.tbmanturov.net]# mkdir -p /vagrant/provision/ser
ver/http/etc/pki/tls/private
[root@server.tbmanturov.net www.tbmanturov.net]# mkdir -p /vagrant/provision/ser
ver/http/etc/pki/tls/certs
[root@server.tbmanturov.net www.tbmanturov.net]# ^C
[root@server.tbmanturov.net www.tbmanturov.net]# cp -R /etc/pki/tls/private/www.
user.net.key /vagrant/provision/server/http/etc/pki/tls/private
[root@server.tbmanturov.net www.tbmanturov.net]# cp -R /etc/pki/tls/certs/www.us
er.net.crt /vagrant/provision/server/http/etc/pki/tls/certs
cp: cannot stat '/etc/pki/tls/certs/www.user.net.crt': No such file or directory
[root@server.tbmanturov.net www.tbmanturov.net]# cp -R /etc/pki/tls/certs/www.us
er.net.crt /vagrant/provision/server/http/etc/pki/tls/certs
```

Внесения изменений в настройки внутреннего окружения

В имеющийся скрипт /vagrant/provision/server/http.sh внесем изменения, добавив установку PHP и настройку межсетевого экрана, разрешающую работать с https.



Редактирование скрипта

Выводы

в процессе выполнения данной лабораторной работы я приобрела практические навыки по расширенному конфигурированию HTTP-сервера Apache в части безопасности и возможности использования PHP.

Контрольные вопросы

1. В чём отличие HTTP от HTTPS?

Отличие состоит в том, что HTTPS — расширение протокола HTTP для поддержки шифрования в целях повышения безопасности.

2. Каким образом обеспечивается безопасность контента веб-сервера при работе через HTTPS?

Улучшение безопасности при использовании HTTPS вместо HTTP достигается за счёт использования криптографических протоколов при организации HTTP-соединения и передачи по нему данных. Для шифрования может применяться протокол SSL (Secure Sockets Layer) или протокол TLC (Transport Layer Security). Оба протокола используют асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

3. Что такое сертификационный центр? Приведите пример.

Сертификационный центр (Certification authority, CA) представляет собой компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей.

Пример: IdenTrust, DigiCert.