Лабораторная работа №5

СТУДЕНТ: САХНО

ГРУППА: НФИБД-02-23

Цель

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

Задания

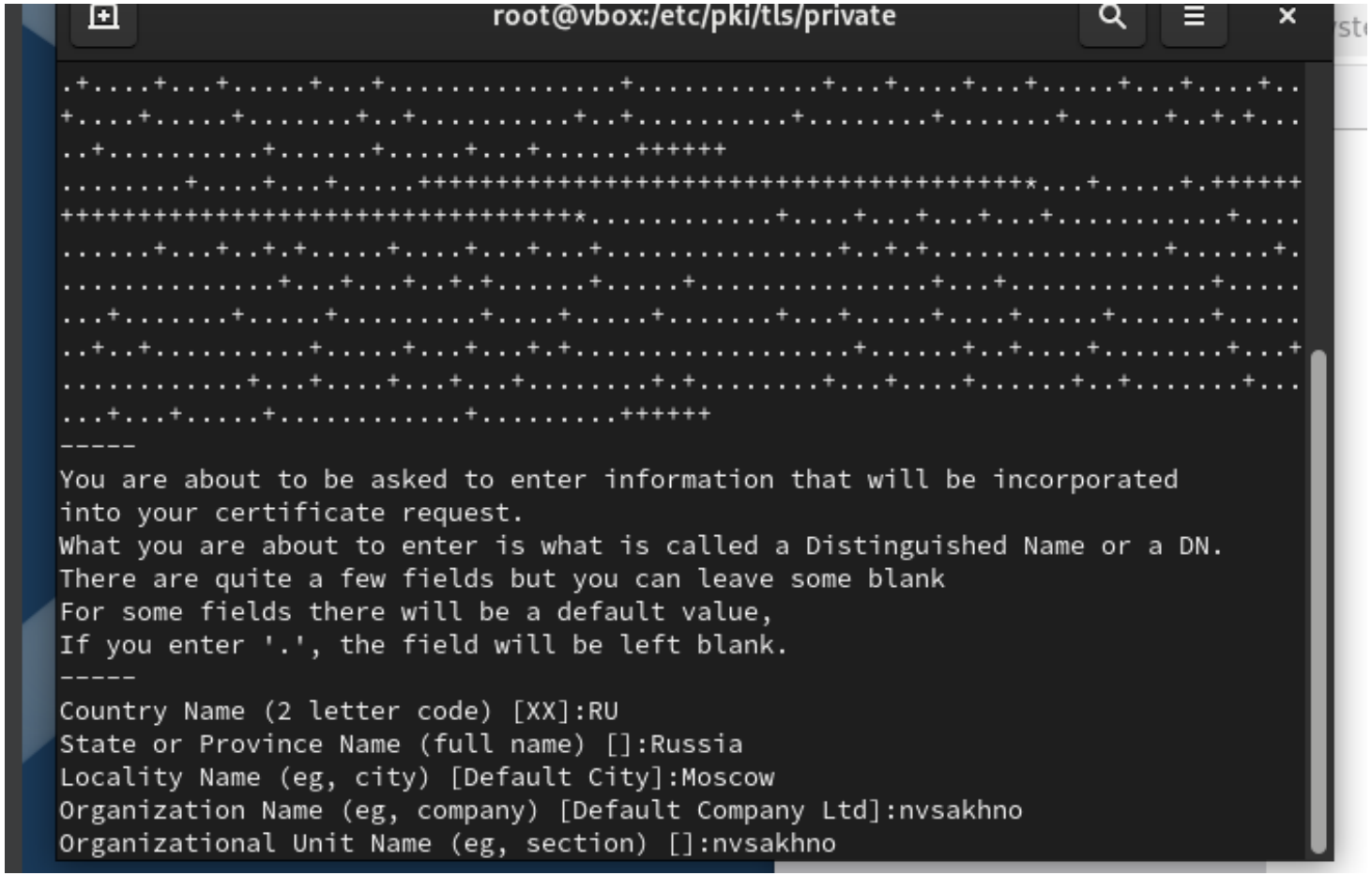
Сгенерировать криптографический ключ и самоподписанный сертификат безопасности для возможности перехода веб-сервера от работы через протокол HTTP к работе через протокол HTTPS;

Настроить веб-сервер для работы с PHP;

Написать скрипт для Vagrant, фиксирующий действия по расширенной настройке HTTP-сервера во внутреннем окружении виртуальной машины server.

```
# mkdir -p /etc/pki/tls/private
# ln - s /etc/pki/tls/private /etc/ssl/private
No such file or directory
# ln -s /etc/pki/tls/private /etc/ssl/private
# cd /etc/pki/tls/private
```

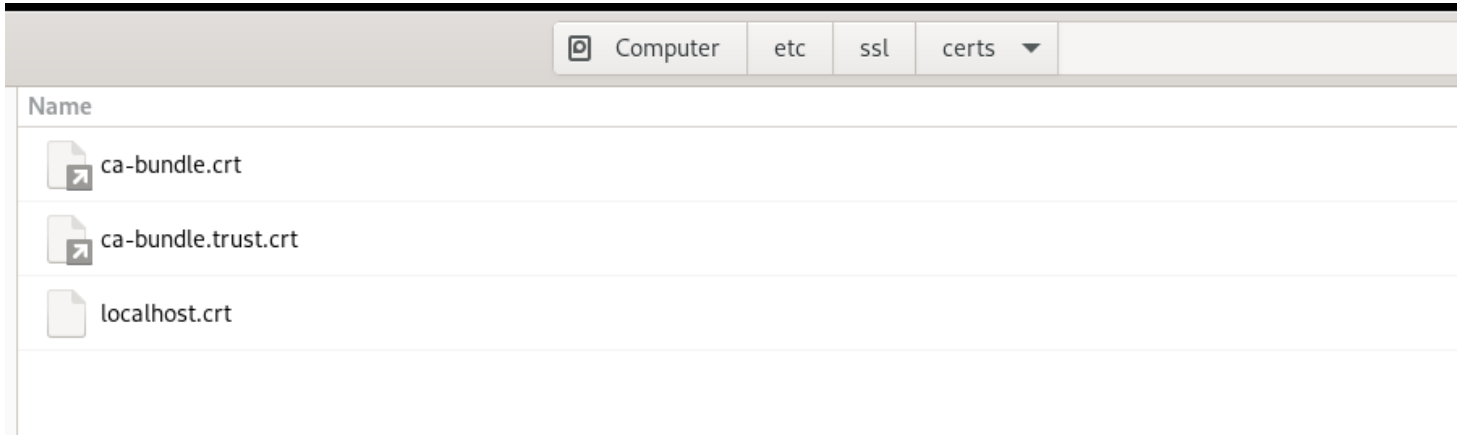
Задание №1


root@vbox:/etc/pki/tls/private

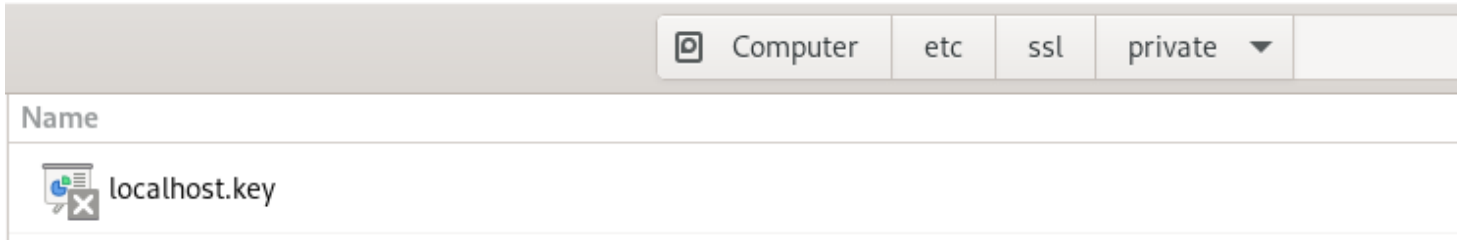
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [XX]:RU
State or Province Name (full name) []:Russia
Locality Name (eg, city) [Default City]:Moscow
Organization Name (eg, company) [Default Company Ltd]:nvsakhno
Organizational Unit Name (eg, section) []:nvsakhno

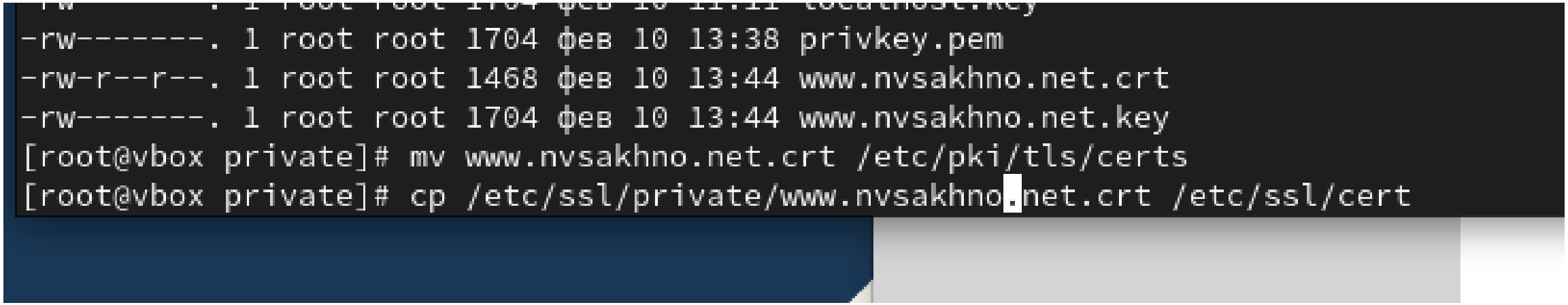
Задание №1


Computer
etc
ssl
certs
Name
ca-bundle.crt
ca-bundle.trust.crt
localhost.crt

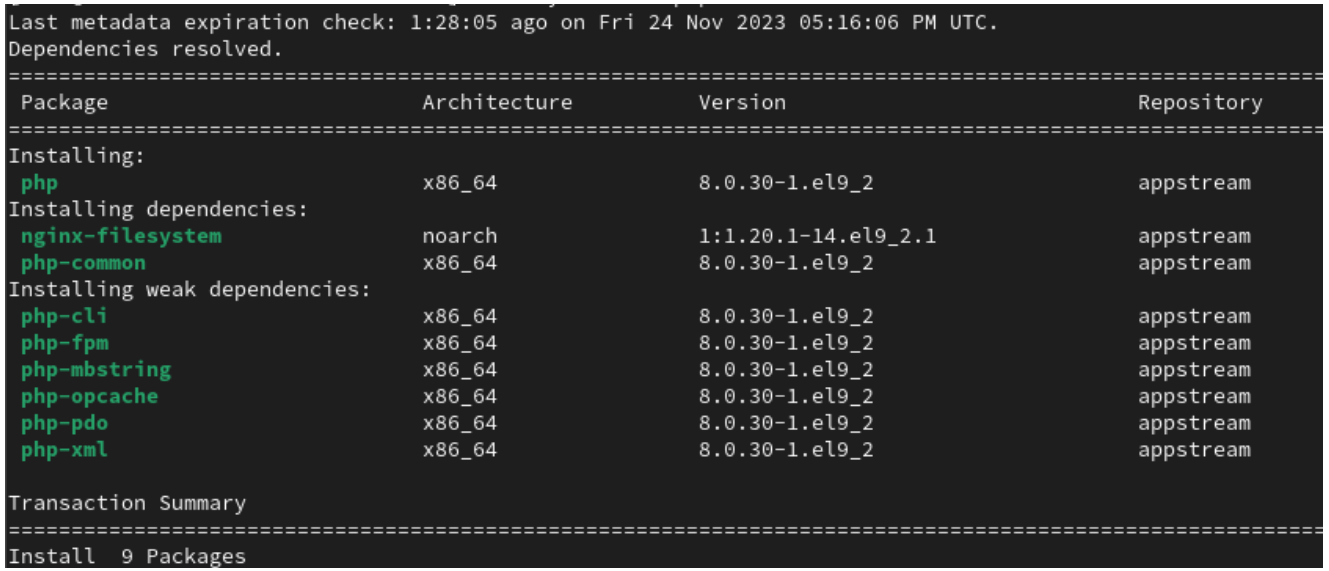
Задание №1



Задание №1


-rw-------. 1 root root 1704 фев 10 13:38 privkey.pem
-rw-r--r--. 1 root root 1468 фев 10 13:44 www.nvsakhno.net.crt
-rw-------. 1 root root 1704 фев 10 13:44 www.nvsakhno.net.key
[root@vbox private]# mv www.nvsakhno.net.crt /etc/pki/tls/certs
[root@vbox private]# cp /etc/ssl/private/www.nvsakhno.net.crt /etc/ssl/cert

Задание №1



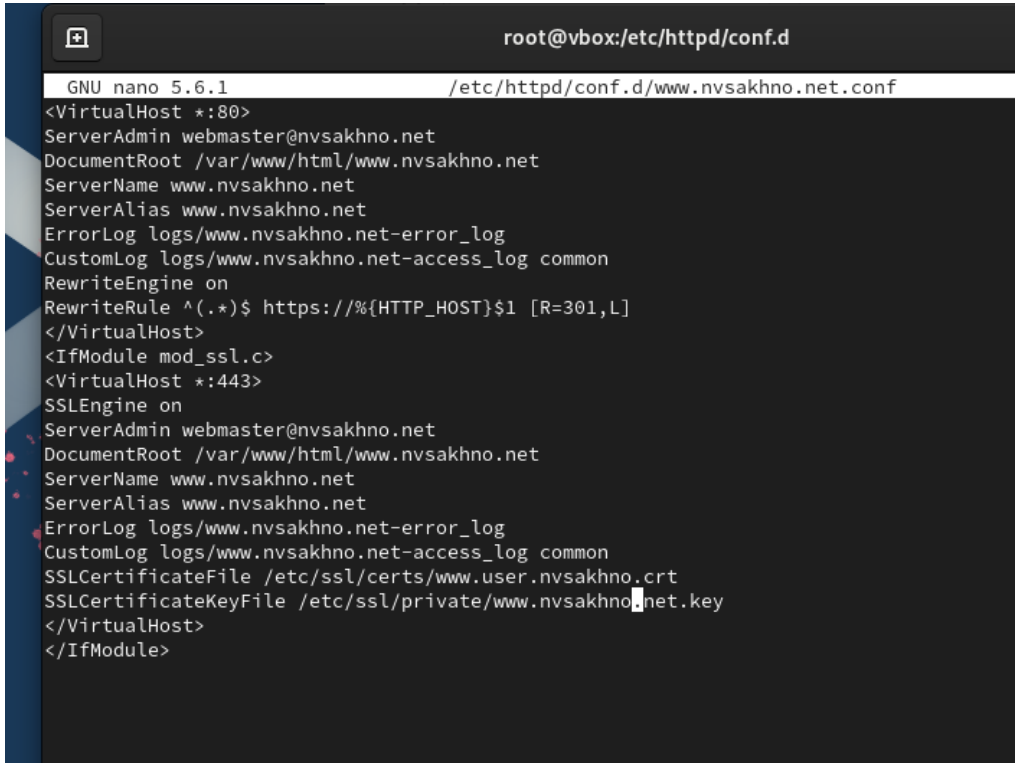
```
Last metadata expiration check: 1:28:05 ago on Fri 24 Nov 2023 05:16:06 PM UTC.
Dependencies resolved.
================================================================================
 Package                Architecture          Version                  Repository
================================================================================
Installing:
 php                    x86_64                8.0.30-1.el9_2           appstream
Installing dependencies:
 nginx-filesystem       noarch                1:1.20.1-14.el9_2.1      appstream
 php-common             x86_64                8.0.30-1.el9_2           appstream
Installing weak dependencies:
 php-cli                x86_64                8.0.30-1.el9_2           appstream
 php-fpm                x86_64                8.0.30-1.el9_2           appstream
 php-mbstring           x86_64                8.0.30-1.el9_2           appstream
 php-opcache            x86_64                8.0.30-1.el9_2           appstream
 php-pdo                x86_64                8.0.30-1.el9_2           appstream
 php-xml                x86_64                8.0.30-1.el9_2           appstream

Transaction Summary
================================================================================
Install  9 Packages
```

Задание №2

```
  GNU nano 5.6.1                                          index.php
<?php
phpinfo();
?>
```

Задание №2


root@vbox:/etc/httpd/conf.d
GNU nano 5.6.1 /etc/httpd/conf.d/www.nvsakhno.net.conf
<VirtualHost *:80>
ServerAdmin webmaster@nvsakhno.net
DocumentRoot /var/www/html/www.nvsakhno.net
ServerName www.nvsakhno.net
ServerAlias www.nvsakhno.net
ErrorLog logs/www.nvsakhno.net-error_log
CustomLog logs/www.nvsakhno.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@nvsakhno.net
DocumentRoot /var/www/html/www.nvsakhno.net
ServerName www.nvsakhno.net
ServerAlias www.nvsakhno.net
ErrorLog logs/www.nvsakhno.net-error_log
CustomLog logs/www.nvsakhno.net-access_log common
SSLCertificateFile /etc/ssl/certs/www.user.nvsakhno.crt
SSLCertificateKeyFile /etc/ssl/private/www.nvsakhno.net.key
</VirtualHost>
</IfModule>

Задание №2

Контрольные вопросы

В чём отличие HTTP от HTTPS?

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

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.

Что такое сертификационный центр? Приведите пример.

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

Вывод:

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