

УО «Гомельский государственный университет им. Ф. Скорины»
Физический факультет
Кафедра общей физики

ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 5

Идентификация уязвимостей сетевых
приложений по косвенным признакам

Проверил:
Грищенко В.В.

Выполнили:
студент группы МС-42
Гончаров Владислав

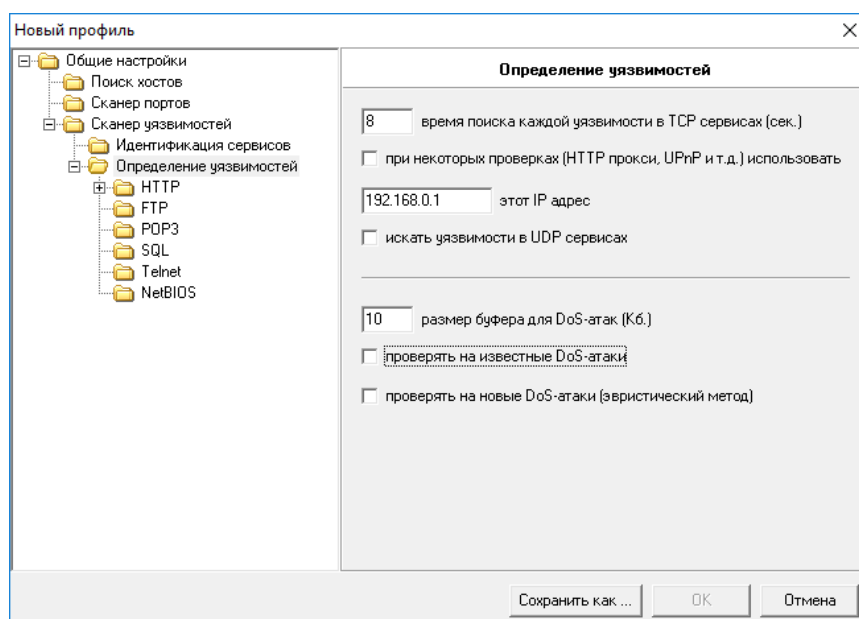
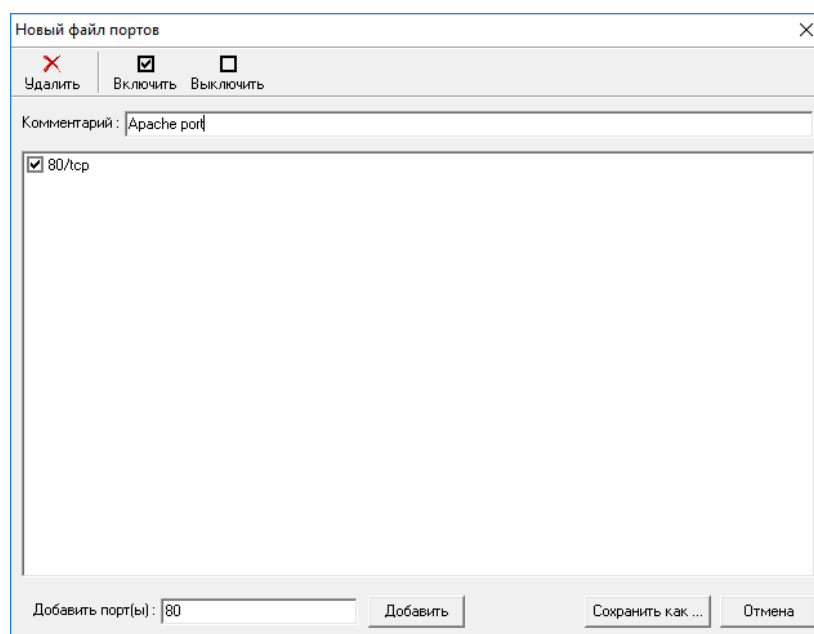
Гомель 2020

Лабораторная работа №5

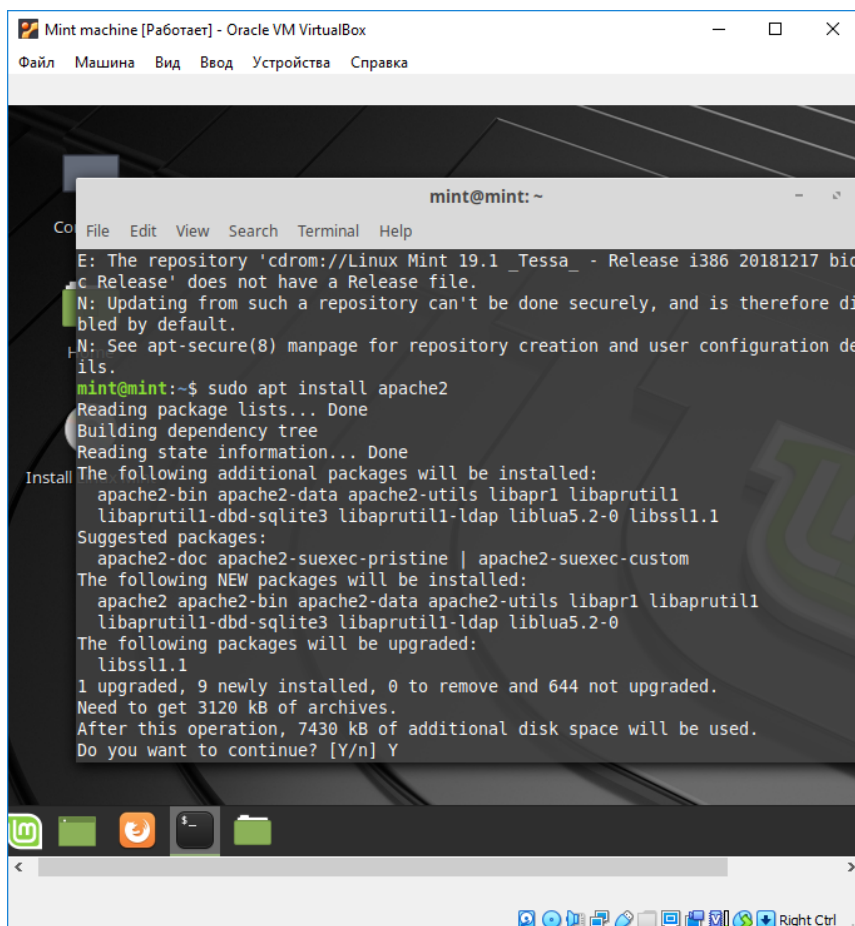
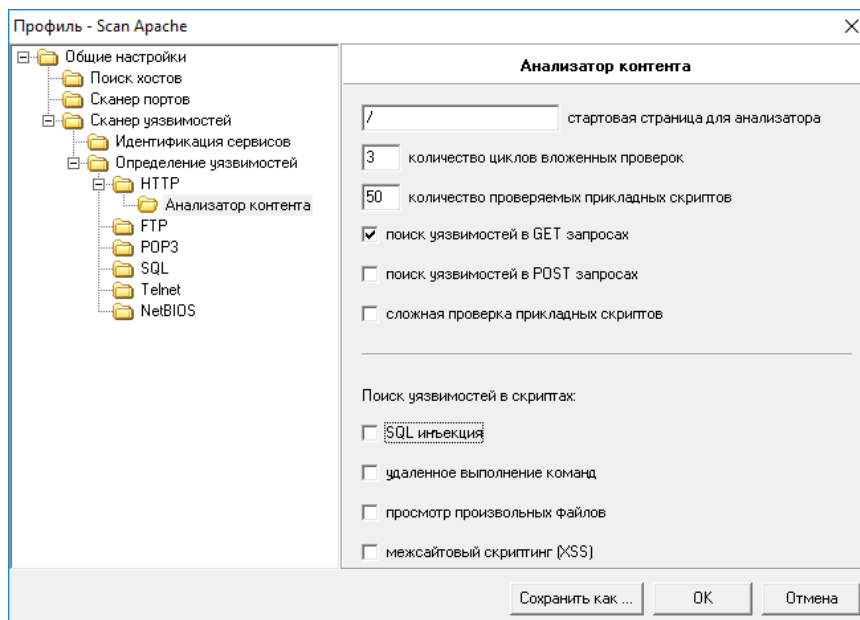
Цель работы: обучение методам и средствам идентификации уязвимостей по косвенным признакам в сетевых приложениях КС.

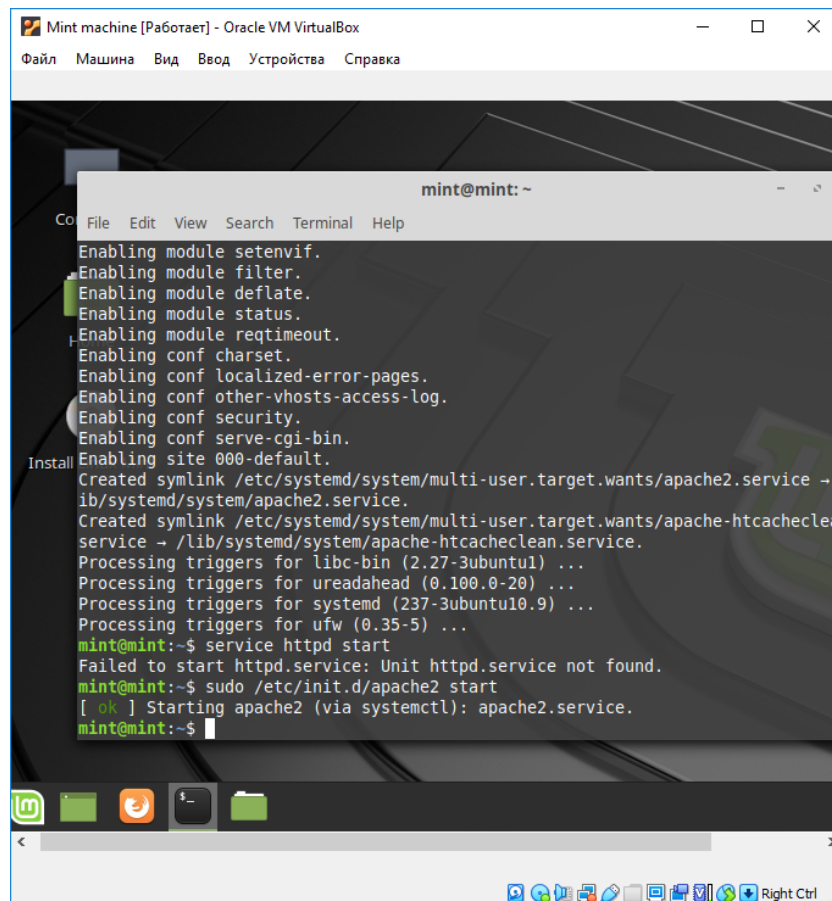
Постановка задачи: выполнить идентификацию уязвимостей сетевых служб DNS, HTTP и SSH по косвенным признакам с помощью сканера XSpider.

Шаг 1. Создать профиль сканирования «Сканирование Apache». Перечень сканируемых портов ограничить портом 80. Отключить сканирование служб UDP, в секции «Определение уязвимостей» отключить опции «Использовать финальные проверки», «Проверять на известные DoS-атаки», «Проверять на новые DoS-атаки».



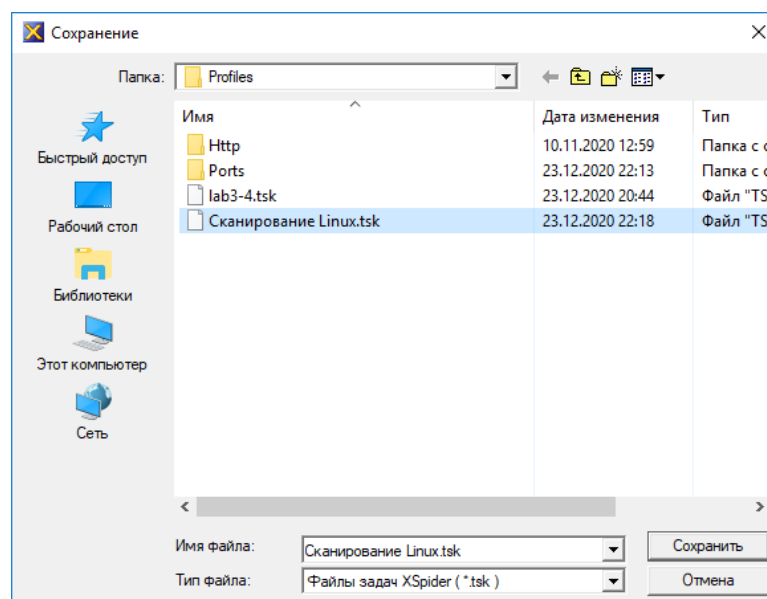
Шаг 2. В секции «HTTP» включить опцию «Включить анализатор директорий», остальные опции отключить. В секции «Анализатор контента» включить опцию «Не выходить за пределы стартовой страницы». В секции «Анализатор сценариев» оставить опцию «Искать уязвимости в GET запросах», отключить остальные опции. В секциях «Типы уязвимостей» и «Методы поиска» отключить все опции. В секции «Подбор учётных записей» отключить опцию «Подбирать учётные записи». Сохранить профиль.

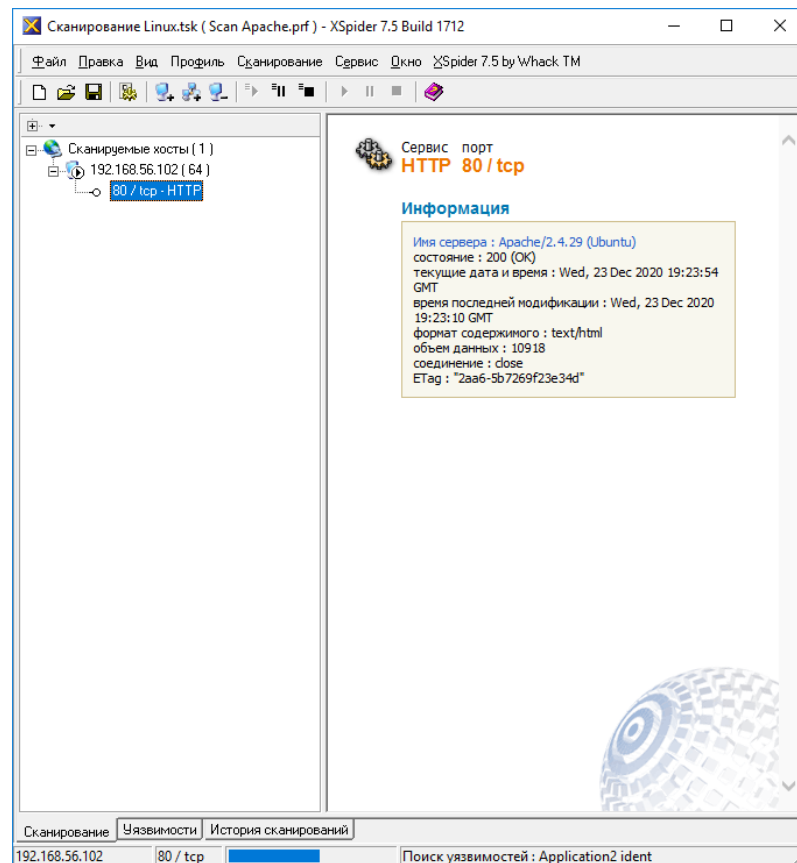




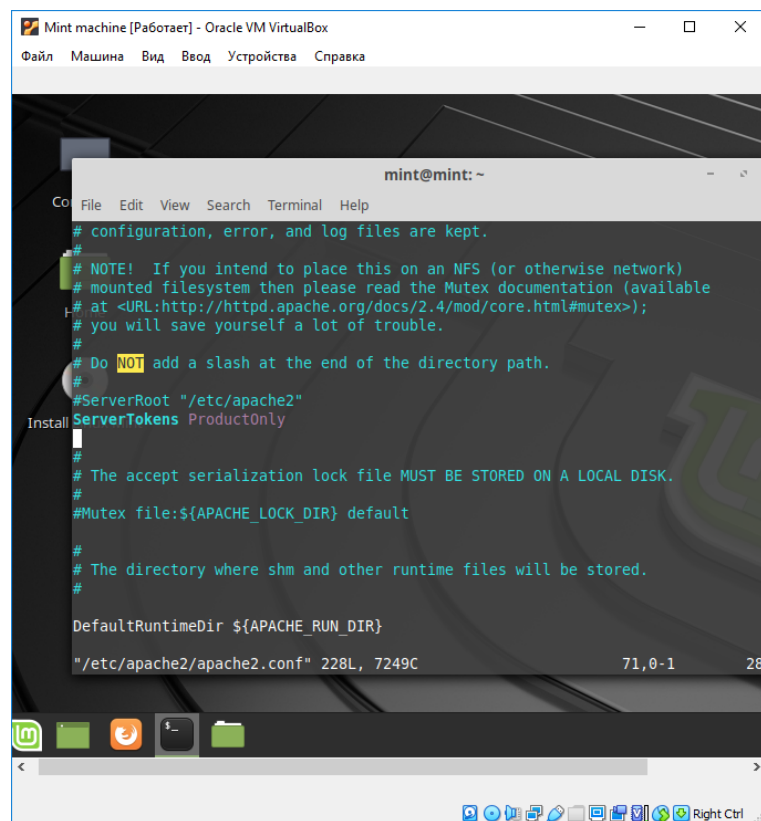
```
mint@mint: ~  
File Edit View Search Terminal Help  
Enabling module setenvif.  
Enabling module filter.  
Enabling module deflate.  
Enabling module status.  
Enabling module reqtimeout.  
Enabling conf charset.  
Enabling conf localized-error-pages.  
Enabling conf other-vhosts-access-log.  
Enabling conf security.  
Enabling conf serve-cgi-bin.  
Enabling site 000-default.  
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service →  
lib/systemd/system/apache2.service.  
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean  
service → /lib/systemd/system/apache-htcacheclean.service.  
Processing triggers for libc-bin (2.27-3ubuntu1) ...  
Processing triggers for ureadahead (0.100.0-20) ...  
Processing triggers for systemd (237-3ubuntu10.9) ...  
Processing triggers for ufw (0.35-5) ...  
mint@mint:~$ service httpd start  
Failed to start httpd.service: Unit httpd.service not found.  
mint@mint:~$ sudo /etc/init.d/apache2 start  
[ OK ] Starting apache2 (via systemctl): apache2.service.  
mint@mint:~$
```

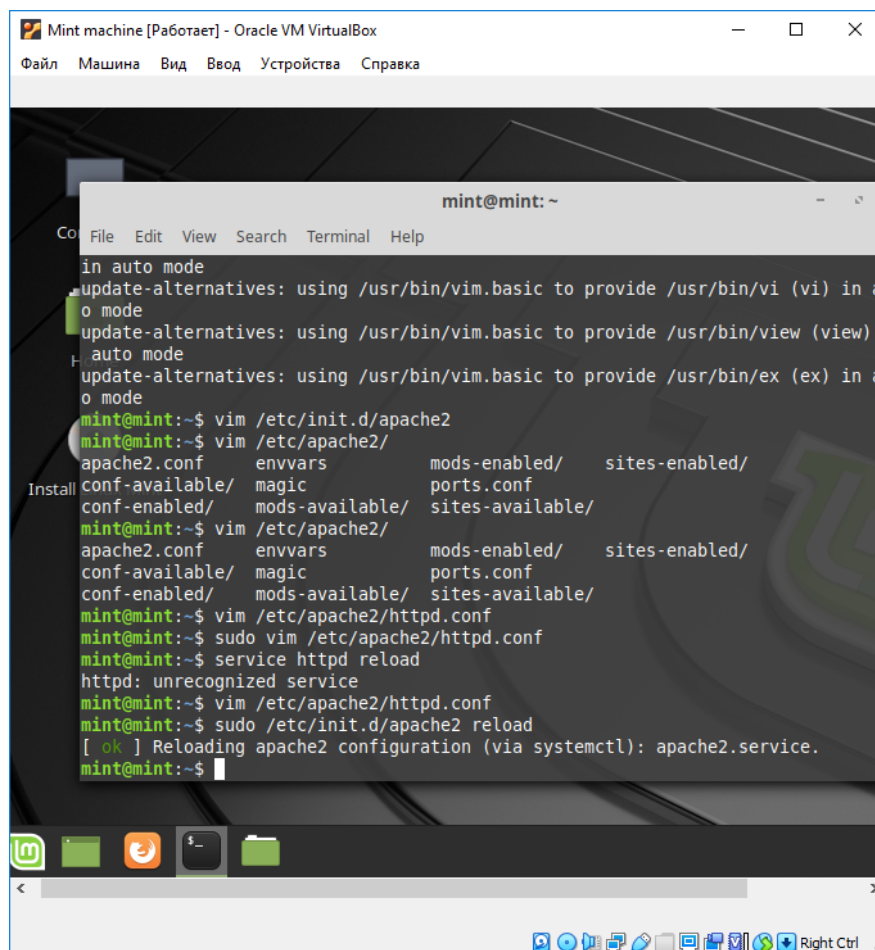
Шаг 3. Создать задачу «Сканирование Linux», добавить в нее узел S1. Запустить на сканирующем узле анализатор протоколов. Выполнить сканирование узла S1. Обратить внимание на уязвимости, найденные на порту 80 веб-сервера Apache, а также на результаты идентификации службы HTTP. Найти результаты работы анализатора каталогов. Проверить наличие найденных уязвимостей вручную. Просмотреть трассировку сканирования в анализаторе протоколов.



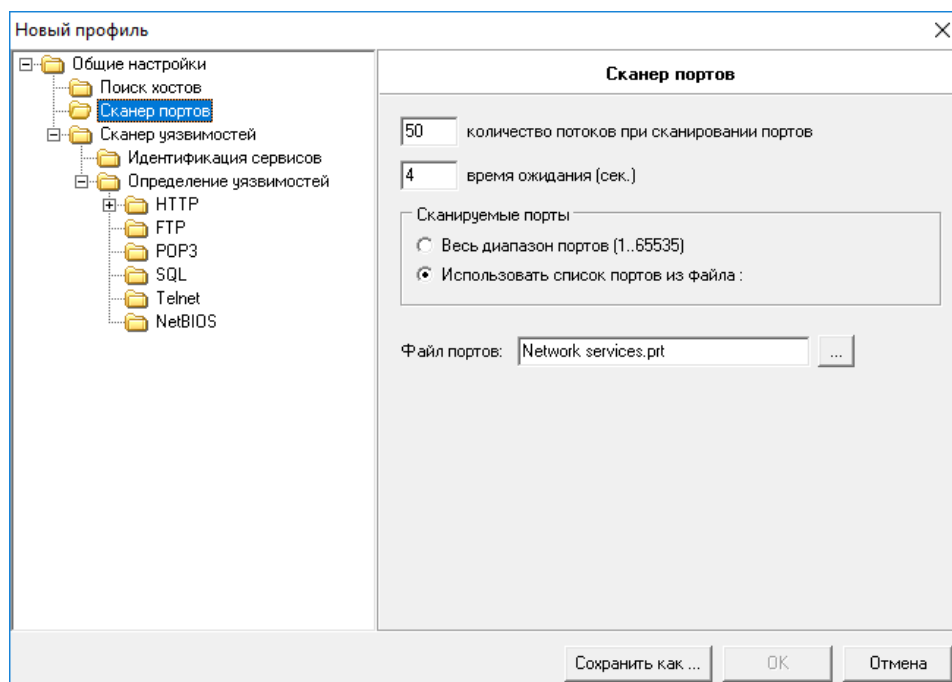


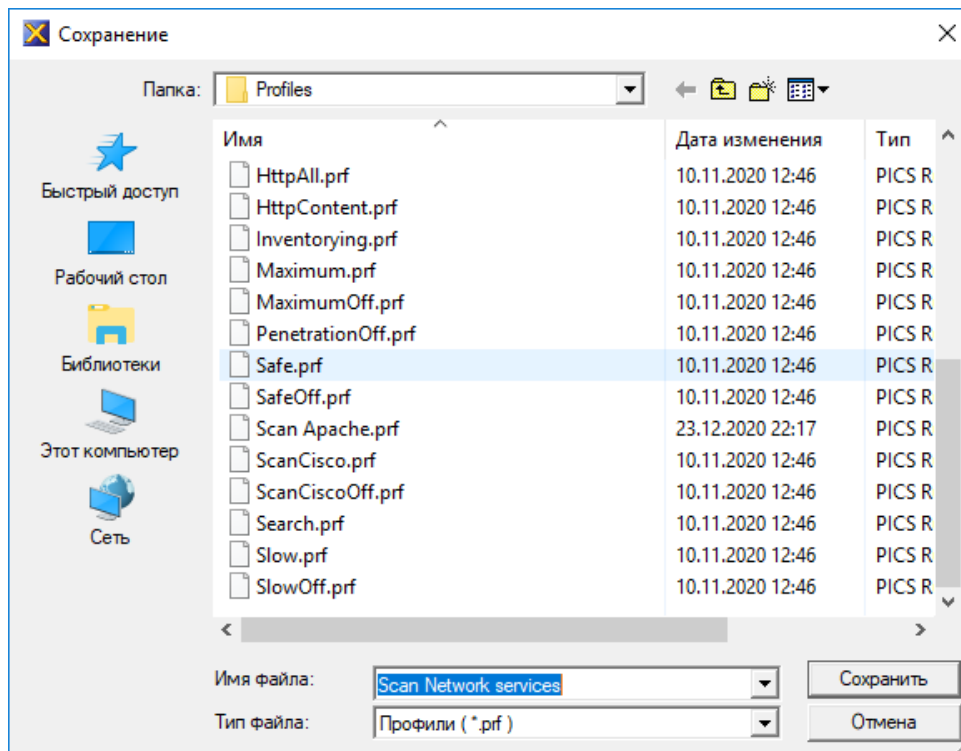
Шаг 4. Открыть для редактирования файл `/etc/httpd/conf/httpd.conf`.
Найти директиву `ServerTokens` и присвоить ей значение `ProductOnly`.
Перезапустить службу `httpd`.



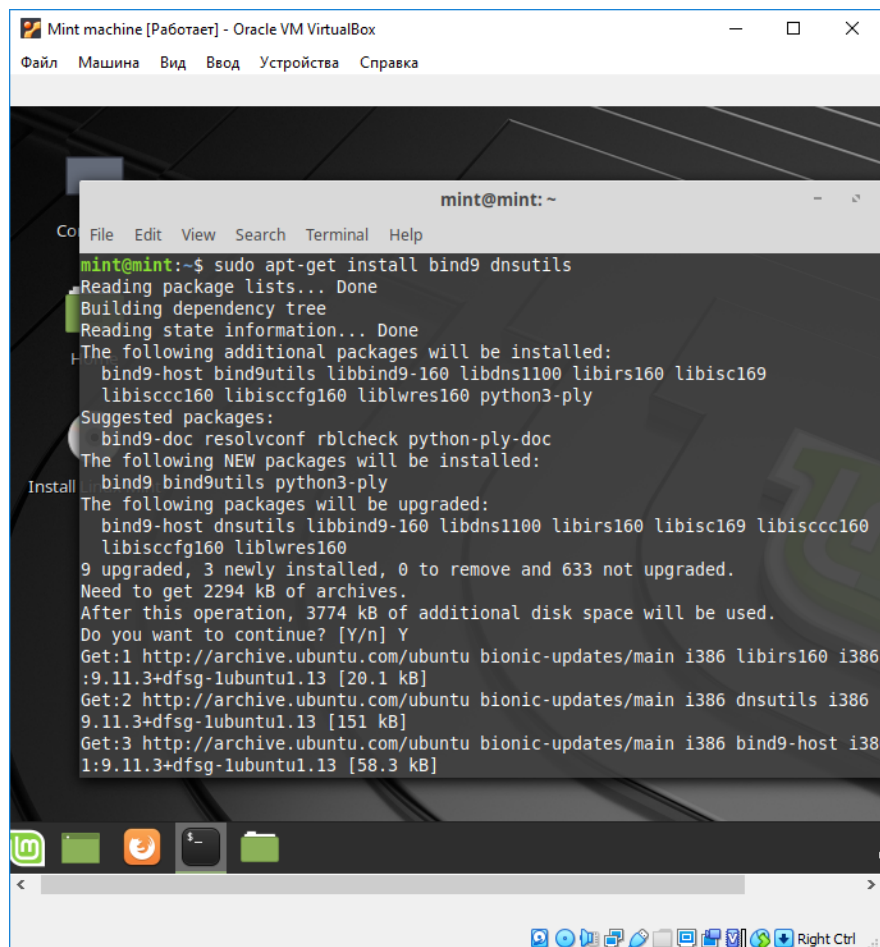


Шаг 5. Создать копию профиля «Сканирование Apache», задать ему имя «Сканирование сетевых служб». Перечень сканируемых портов ограничить портами 22 и 53. В секции «Сканер UDP сервисов» отключить все опции, кроме DNS. Сменить профиль для задачи «Сканирование Linux».





Шаг 6. Убедиться, что на сервере S1 служба DNS запущена. Выполнить сканирование сервера S1.



Mint machine [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

```
mint@mint: ~  
File Edit View Search Terminal Help  
Setting up libbind9-160:i386 (1:9.11.3+dfsg-1ubuntu1.13) ...  
Setting up bind9utils (1:9.11.3+dfsg-1ubuntu1.13) ...  
Setting up bind9-host (1:9.11.3+dfsg-1ubuntu1.13) ...  
Setting up bind9 (1:9.11.3+dfsg-1ubuntu1.13) ...  
Adding group `bind' (GID 128) ...  
Done.  
Adding system user `bind' (UID 121) ...  
Adding new user `bind' (UID 121) with group `bind' ...  
Not creating home directory `/var/cache/bind'.  
wrote key file "/etc/bind/rndc.key"  
Created symlink /etc/systemd/system/multi-user.target.wants/bind9.service → /l  
/systemd/system/bind9.service.  
bind9-pkcs11.service is a disabled or a static unit, not starting it.  
bind9-resolvconf.service is a disabled or a static unit, not starting it.  
Setting up dnsutils (1:9.11.3+dfsg-1ubuntu1.13) ...  
Processing triggers for libc-bin (2.27-3ubuntu1) ...  
Processing triggers for ureadahead (0.100.0-20) ...  
Processing triggers for systemd (237-3ubuntu10.9) ...  
Processing triggers for ufw (0.35-5) ...  
mint@mint:~$ /etc/in  
init/          init.d/          initramfs-tools/ insserv.conf.d/  
mint@mint:~$ /etc/init.d/bind9 start  
[ ok ] Starting bind9 (via systemctl): bind9.service.  
mint@mint:~$
```

Сканирование Linux.tsk (Scan Network services.prf) - XSpider 7.5 Build 1712

Файл Правка Вид Профиль Сканирование Сервис Окно XSpider 7.5 by Whack TM

Сканируемые хосты (1)

- 192.168.56.102 (64)
 - 53 / tcp - DNS

Хост
192.168.56.102

Информация

Время отклика:	< 1 мсек
TTL:	64

Параметры сканирования

Начало сканирования:	23:00:58 23.12.2020
Время сканирования:	00:00:14
Версия:	7.5 Build 1712
Профиль:	Scan Network services.prf

Сканирование Уязвимости История сканиваний

192.168.56.102

Уязвимость				Хост	Порт	Сервис
рекурсия				192.168.56.102	53 / udp	DNS

Шаг 7. Проанализировать результаты сканирования службы DNS, обратить внимание на версию BIND. Выполнить ручную проверку наличия уязвимостей, используя средство nslookup.

```

Mint machine [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

mint@mint: ~
File Edit View Search Terminal Help
Created symlink /etc/systemd/system/multi-user.target.wants/bind9.service → /lib/systemd/system/bind9.service.
bind9-pkcs11.service is a disabled or a static unit, not starting it.
bind9-resolvconf.service is a disabled or a static unit, not starting it.
Setting up dnsutils (1:9.11.3+dfsg-1ubuntu1.13) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for ureadahead (0.100.0-20) ...
Processing triggers for systemd (237-3ubuntu10.9) ...
Processing triggers for ufw (0.35-5) ...
mint@mint:~$ /etc/init
init/ Linux Mint      init.d/                initramfs-tools/ insserv.conf.d/
mint@mint:~$ /etc/init.d/bind9 start
[ ok ] Starting bind9 (via systemctl): bind9.service.
mint@mint:~$ nslookup
> server 192.168.56.102
Default server: 192.168.56.102
Address: 192.168.56.102#53
> set class=chaos
> set -h
> set test=txt
> version.bind
Server:      192.168.56.102
Address:     192.168.56.102#53

```