

Домашнее задание (модуль 18)

18.5 Практическая работа

Задание 1

Цель задания

Попрактиковаться в настройке подключения по SSH к хосту.

Что нужно сделать

1. Настройте подключение по SSH с аутентификацией по ключам к вашей виртуальной машине, как было показано на уроке.
2. Ответьте, как будет выглядеть сгенерённый fingerprint вашей виртуальной машины?

Что оценивается

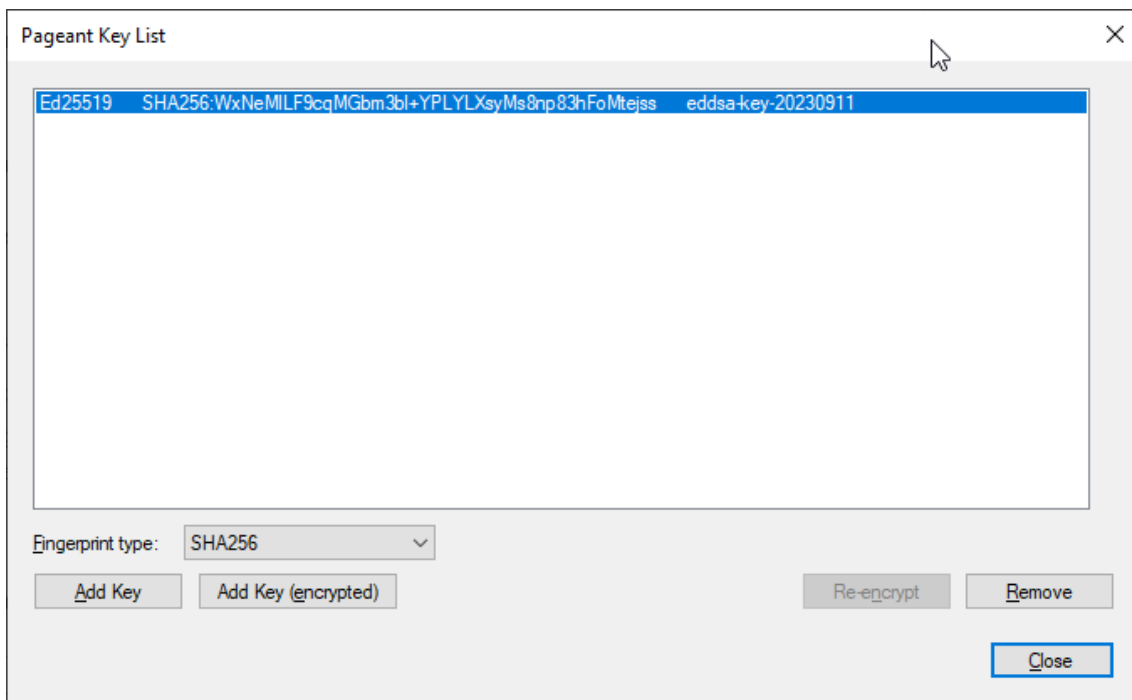
Успешное подключение к виртуальной машине.

Как отправить задание на проверку

Пришлите через форму ниже скриншот консоли, на котором видно содержимое домашней директории виртуальной машины, и ответ на вопрос.

Ответ:

1. Настройте подключение по SSH с аутентификацией по ключам к вашей виртуальной машине, как было показано на уроке.



2. Содержимое домашней директории

```

vgusev2007@skillbox-vgusev2007: ~/skillbox
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

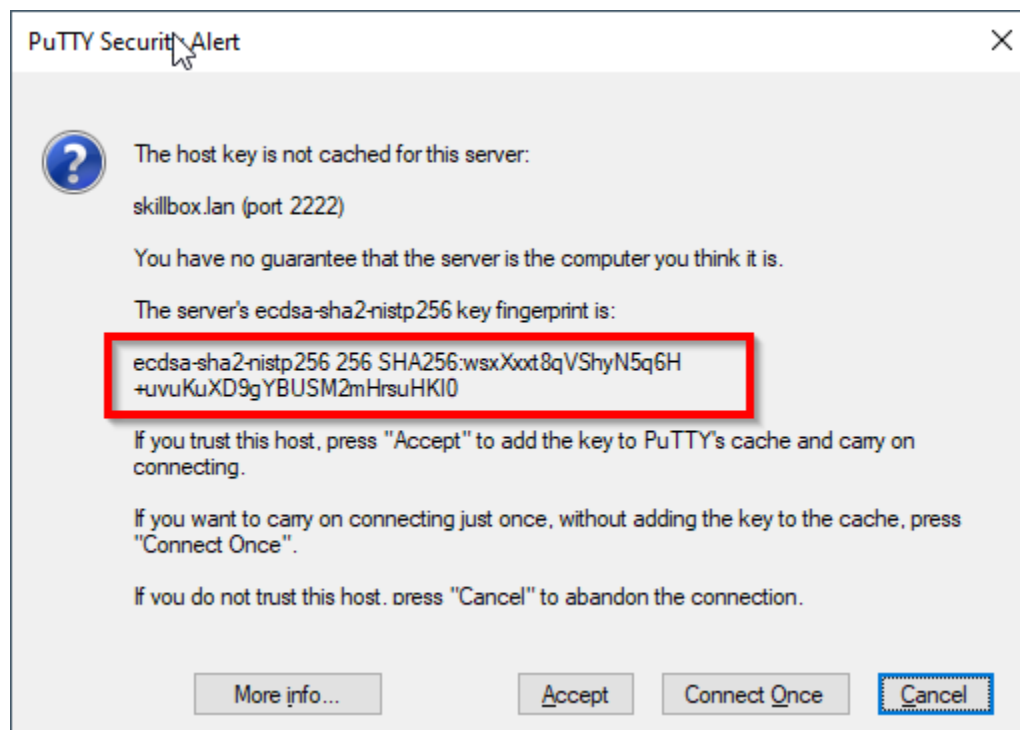
/ \  В наших тюрьмах все сидячие места  \
 \  заняты.                             /
-----
 \
  \
   .--.
  |o_o|
  |: / |
 / \ / \
(| | | |)
/ \ / \
(| | | |)
 \ / \ /
  ( )
  ( )
  ( )

vgusev2007@skillbox-vgusev2007:~/skillbox$ ls ~
bar.file  Documents/  foo.file  Pictures/  scripts/  Templates/  Videos/
Desktop/  Downloads/  Music/    Public/    skillbox/  TRASH/

vgusev2007@skillbox-vgusev2007:~/skillbox$

```

3. Ответьте, как будет выглядеть сгенерённый fingerprint вашей виртуальной машины?



Задание 2

Цель задания

Попрактиковаться в настройке сервера SSH.

Что нужно сделать

Настройте SSH-сервер на работу по 2222 порту.

Что оценивается

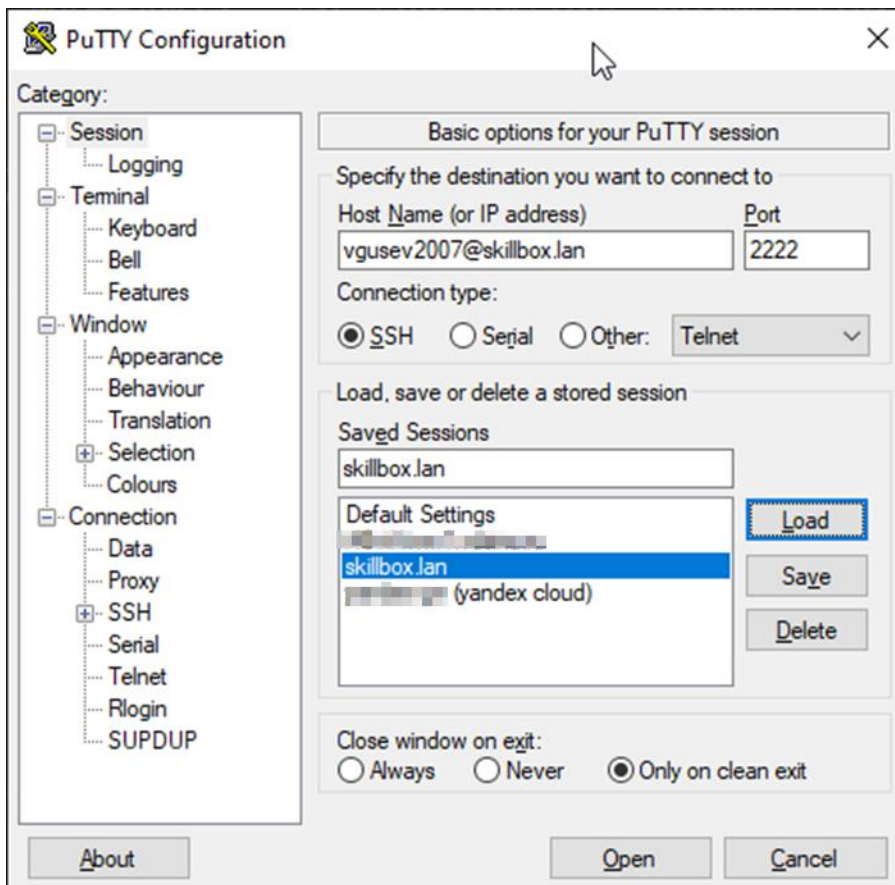
SSH-клиент успешно подключается к виртуальной машине по 2222 порту.

Как отправить задание на проверку

Пришлите через форму ниже скриншот консоли, на котором показано успешное подключение к виртуальной машине по 2222 порту.

Ответ:

Через putty:



PuTTY Security Alert



The host key is not cached for this server:

skillbox.lan (port 2222)

You have no guarantee that the server is the computer you think it is.

The server's ecdsa-sha2-nistp256 key fingerprint is:

ecdsa-sha2-nistp256 256 SHA256:wsxXxt8qVShyN5q6H
+uvuKuXD9gYBUSM2mHrsuHKI0

If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.

If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".

If you do not trust this host, press "Cancel" to abandon the connection.

More info...

Accept

Connect Once

Cancel

Через Apache Guacamole:

EDIT CONNECTION

Name:

Location:

Protocol:

CONCURRENCY LIMITS

Maximum number of connections:

Maximum number of connections per user:

GUACAMOLE PROXY PARAMETERS (GUACD)

Hostname:

Port:

Encryption:

PARAMETERS

Network

Hostname:

Port:

1

Authentication

Username:

Password:

Private key:

2

Задание 3

Цель задания

Попрактиковаться в работе с Wireshark.

Что нужно сделать

1. Перехватите трафик, который генерируется при запросе `curl google.com`.
2. Отфильтруйте только запросы протокола DNS.
3. Ответьте:
 - На каком уровне в стеке протоколов TCP/IP располагается DNS?
 - Какой протокол транспортного уровня используется для DNS? Как вы думаете, почему?

Что оценивается

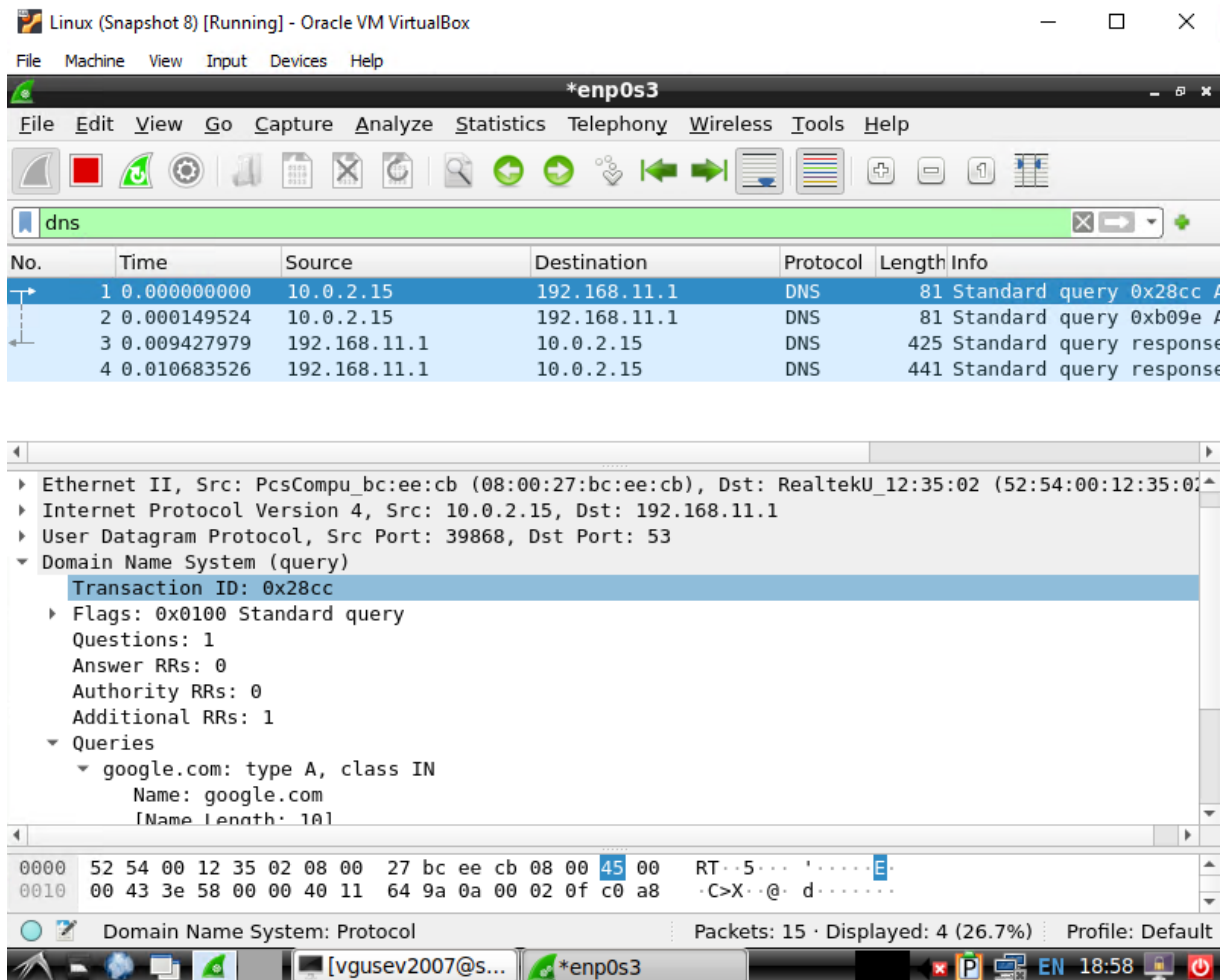
Работа с интерфейсом Wireshark.

Как отправить задание на проверку

Через форму ниже приложите скриншоты Wireshark и ответы на вопросы.

Ответ:

скриншоты Wireshark



*enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

vgusev2007@skillbox-vgusev2007: ~/skillbox

File Edit Tabs Help

vgusev2007... x vgusev2007... x

No. 14 15 16 17 18 19

/ Я красивый, я сильный, я умный, я \
/ добрый. И я сам все это открыл! /

o o
: /
()
()
() = ()

vgusev2007@skillbox-vgusev2007:~/skillbox\$ curl google.com

Quest<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
Answ<TITLE>301 Moved</TITLE></HEAD><BODY>
Aut<H1>301 Moved</H1>
AddThe document has moved
Questhere.
g</BODY></HTML>

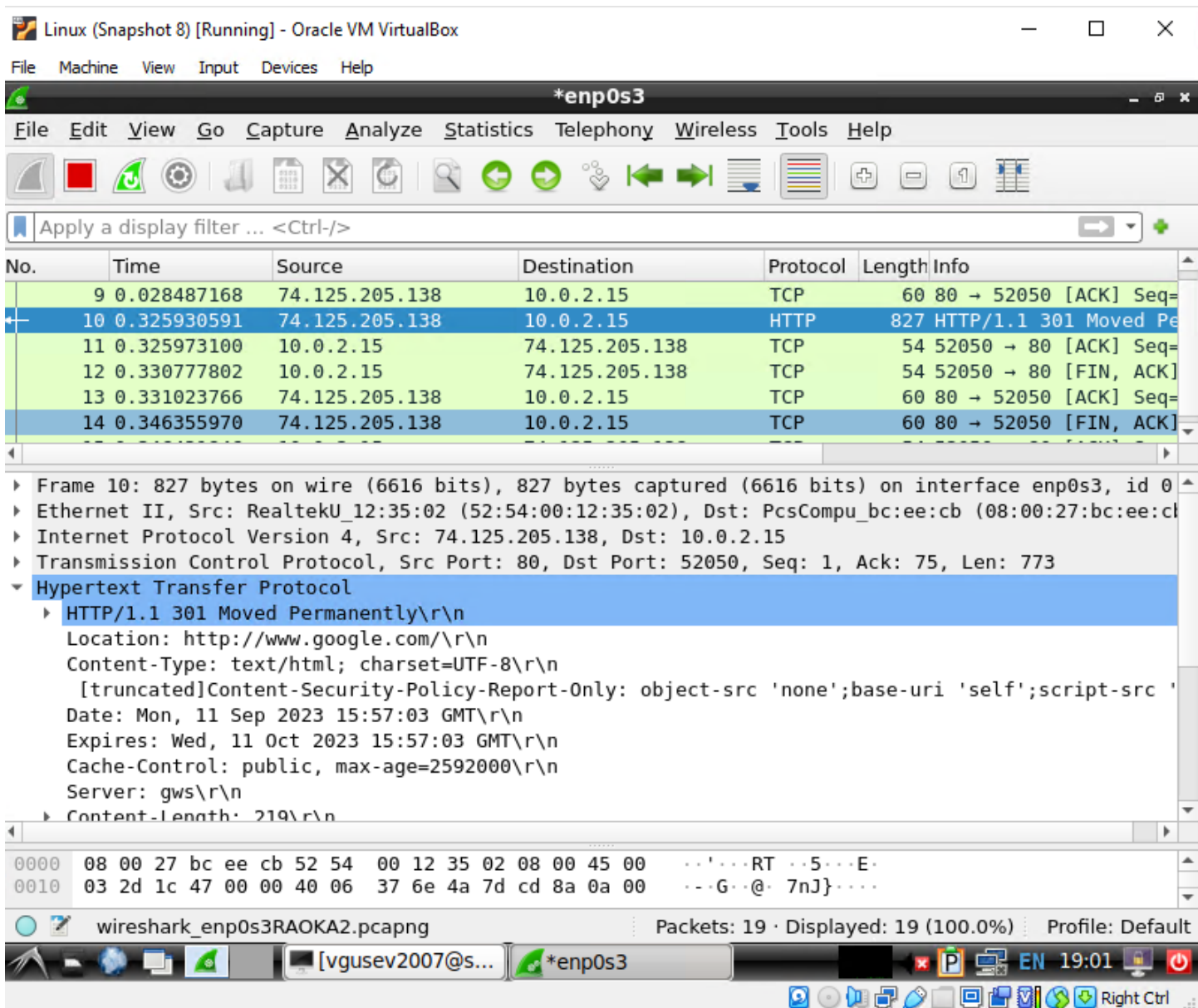
vgusev2007@skillbox-vgusev2007:~/skillbox\$

0000 52 54 00 12 35 02 08 00 27 bc ee cb 08 00 45 00 RT..5... '.....E.
0010 00 43 3e 58 00 00 40 11 64 9a 0a 00 02 0f c0 a8 .C>X..@. d.....

wireshark_enp0s3RAOKA2.pcapng Packets: 19 · Displayed: 19 (100.0%) Profile: Default

vgusev2007@sk... *enp0s3

EN 19:01



Ответы на доп. вопросы:

1. На каком уровне в стеке протоколов TCP/IP располагается DNS?

Ответ: уровень приложения.

2. Какой протокол транспортного уровня используется для DNS? Как вы думаете, почему?

Ответ: как правило (но не всегда), для DNS используется протокол транспортного уровня UDP.

Потому что:

1. UDP в сравнении с TCP, гораздо более быстрый, за счет того, что не требуется «тройного рукопожатия» для установки сессии.

2. DNS работает по схеме, запрос-ответ. Нет нужды поддерживать соединение. Следовательно, нет и нужды в протоколе поддерживающим сессионность.
3. Запрос DNS небольшой, и может уместиться буквально в один пакет.
4. Недостаток UDP, может быть достаточно легко компенсирован тем, что приложение, в том случае, если не получило ответа за определенный промежуток времени, просто повторяет запрос и всё.