Отчет по первому этапу внешнего курса

Дисциплина: основы информационнной безопасности

Казазаев Даниил Михайлович

Содержание

1	Цель работы	4
2	Этап первый	5
3	Выполнение первого этапа внешнего курса. 3.1 Базовые сетевые протоколы	6 12
4	Браузер TOR	17
5	Беспроводные сети Wi-fi	21
6	Вывод	24

Список иллюстраций

3.1	Первыи вопрос	6
3.2	Второй вопрос	7
3.3	Третий вопрос	8
3.4	Четвертый вопрос	9
3.5	Пятый вопрос	10
3.6		10
3.7	Седьмой вопрос	11
3.8	Восьмой вопрос	11
3.9		12
3.10		13
	Второй вопрос	14
	Третий вопрос	15
	Четвертый вопрос	16
4.1	Первый вопрос	17
4.2	Второй вопрос	18
4.3	Третий вопрос	19
4.4	Четвертый вопрос	20
5.1	Первый вопрос	21
5.2		22
5.3		22
5.4		23
5 5	Пятый вопрос	23

1 Цель работы

Внешний кур состоит из трех этапов.

2 Этап первый

Первый этап курса состоит из 4 частей:

- 1. Базовые сетевые протоколы
- 2. Персонализация сети
- 3. Браузер TOR
- 4. Беспроводные сети Wi-fi

3 Выполнение первого этапа внешнего курса.

3.1 Базовые сетевые протоколы

HTTPS является протоколом прикладного уровня. (рис. 3.1)

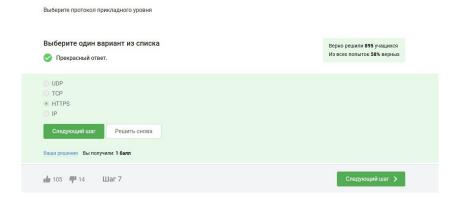


Рис. 3.1: Первый вопрос

Протокол ТСР работает на транспортном уровне. (рис. 3.2)

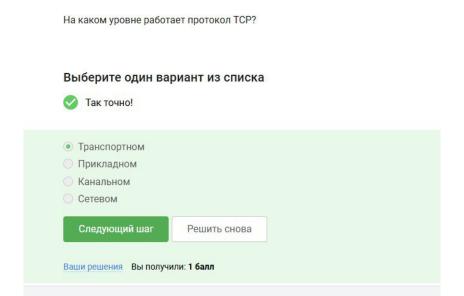


Рис. 3.2: Второй вопрос

Адреса формата IPv4 состоят из 4-х значений от 0 до 255. (рис. 3.3)

Выберите все подходящие ответы из списка

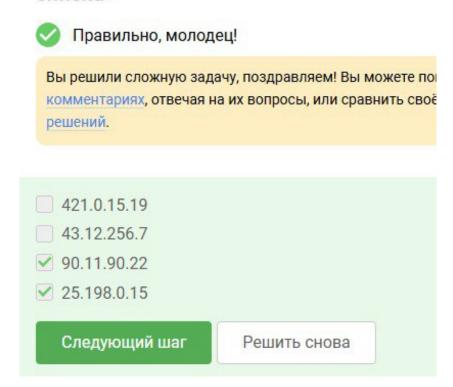


Рис. 3.3: Третий вопрос

DNS сервера необходимы для сопоставления IP адреса с доменным именем при маршрутизации запроса. (рис. 3.4)

Выберите один вариант из списка

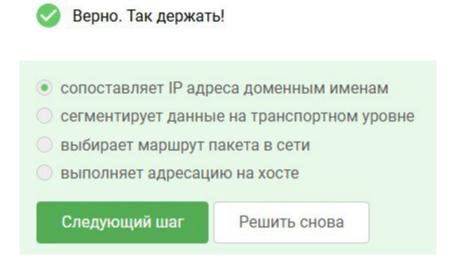


Рис. 3.4: Четвертый вопрос

Корректная последовательность протоколов в модели ТСР/ІР. (рис. 3.5)

Выберите корректную последовательность протоколов в модели TCP/IP

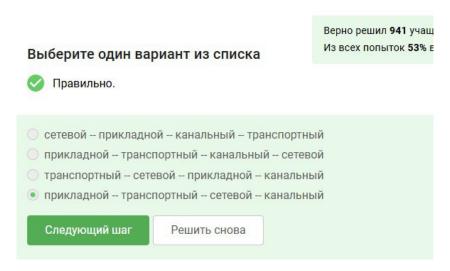


Рис. 3.5: Пятый вопрос

Так как http это незащищенный протокол, он предполагает передачу данных в открытом виде.(рис. 3.6)

Протокол http предполагает

Верно решили 965 у Из всех попыток 78 Отлично!

Отлично!

передачу зашифрованных данных между клиентом и сервером
передачу данных между клиентом и сервером в открытом виде

Следующий шаг

Решить снова

Рис. 3.6: Шестой вопрос

HTTPS протокол состоит из двух фаз: рукопожатия и передачи данных.(рис. 3.7)

Протокол https состоит из

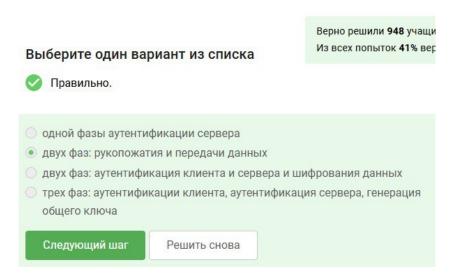


Рис. 3.7: Седьмой вопрос

Версия протокола TLS определяется как клиентом, так и сервером на стадии "переговоров".(рис. 3.8)

Версия протокола TLS определяется

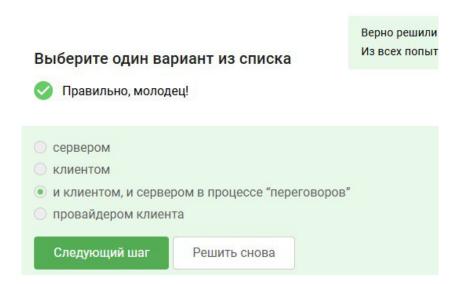


Рис. 3.8: Восьмой вопрос

На фазе рукопожатия протокола TLS не предусмотрено шифрование данных.(рис. 3.9)

В фазе "рукопожатия" протокола TLS не предусмотрено

Верно решил 931 учащи Из всех попыток 44% все Обрание общего секретного ключа между клиентом и сервером аутентификация (как минимум одной из сторон)

выбираются алгоритмы шифрования/аутентификации

шифрование данных

Следующий шаг

Решить снова

Рис. 3.9: Девятый вопрос

3.2 Персонализация сети

Куки-файлы хранят в себе информацию о идентификаторе пользователя и id сессии.(рис. 3.10)

Куки хранят:

Выберите все подходящие ответы из списка

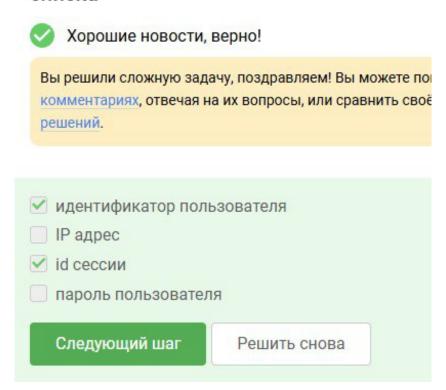


Рис. 3.10: Первый вопрос

Куки-файлы не используются для улучшения надежности соединения. (рис. 3.11)

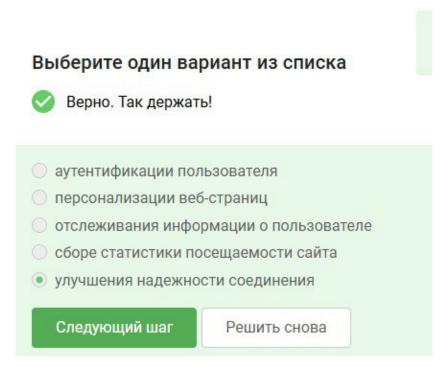


Рис. 3.11: Второй вопрос

Куки-файлы генерируются сервером. (рис. 3.12)

Выберите один вариант из списка

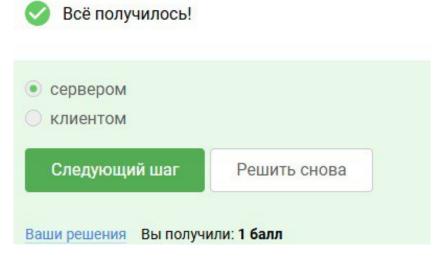


Рис. 3.12: Третий вопрос

Сессионные куки хранятся в браузере на время пользования им. (рис. 3.13)

Сессионные куки хранятся в браузере?

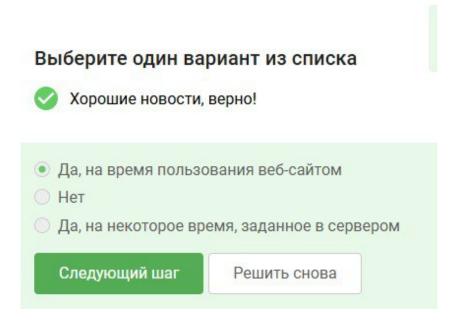


Рис. 3.13: Четвертый вопрос

4 Браузер TOR

В браузере на основе TOR три промежуточных узла: охранный, промежуточный, выходной. (рис. 4.1)

Сколько промежуточных узлов в луковой сети TOR?

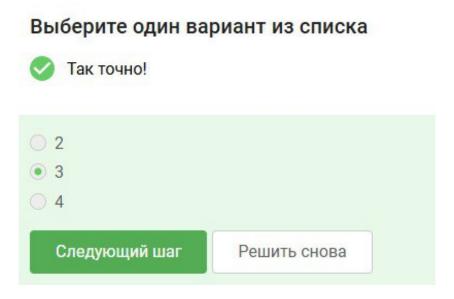


Рис. 4.1: Первый вопрос

IP-адрес получателя в системе TOR изместен только отправителю и выходному узлу. (рис. 4.2)

Выберите все подходящие ответы из списка Отличное решение! Вы решили сложную задачу, поздравляем! Вы можете по комментариях, отвечая на их вопросы, или сравнить сво решений. охранному узлу промежуточному узлу отправителю выходному узлу Следующий шаг Решить снова

Рис. 4.2: Второй вопрос

При запросе через TOR отправитель гененирует общий секрутный ключ со всеми узлами. (рис. 4.3)

Выберите один вариант из списка Верно. только с охранным узлом с охранным и промежуточным узлом о с охранным, промежуточным и выходном узлом с промежуточным и выходным узлом Следующий шаг Решить снова

Рис. 4.3: Третий вопрос

Получатель может использовать любой браузер для принятия запроса из TOR. (рис. 4.4)

Должен ли получатель использовать браузер Tor (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов?

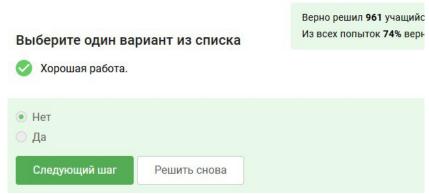


Рис. 4.4: Четвертый вопрос

5 Беспроводные сети Wi-fi

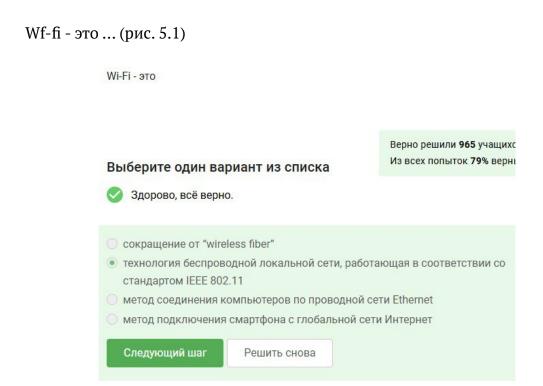


Рис. 5.1: Первый вопрос

Протоколы Wf-fi работают на канальном уровне. (рис. 5.2)

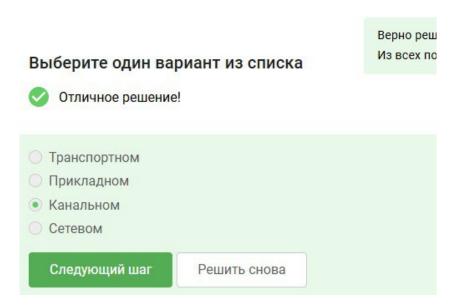


Рис. 5.2: Второй вопрос

Самой небезопасный метод шифрования и аунтификации Wf-fi это WEP, так как он старый и в нем используется малое кольчество бит для шифрования. (рис. 5.3)

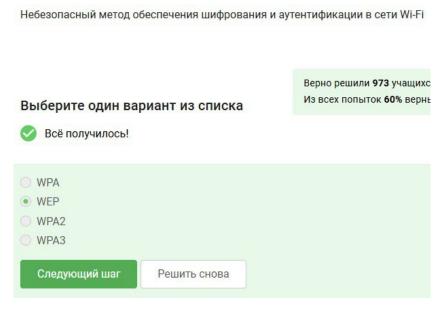


Рис. 5.3: Третий вопрос

Данные шифруются после аунтификации польователя. (рис. 5.4)

Данные между хостом сети (компьютером или смартфоном) и роутером

Верно решили 975 учац
Из всех попыток 53% в

Так точно!

передаются в зашифрованном виде после аутентификации устройств
передаются в открытом виде после аутентификации устройств
передаются в зашифрованном виде
передаются в зашифрованном виде
передаются в открытом виде
Передаются в открытом виде
Передаются в открытом виде
Решить снова

Рис. 5.4: Четвертый вопрос

Для домашних сетей используется аунтификатор Wi-fi Personal. (рис. 5.5)

Для домашней сети для аутентификации обычно используется метод

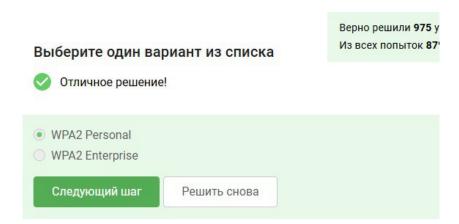


Рис. 5.5: Пятый вопрос

6 Вывод

Выполнен первый этап внешнего курса