Отчёт по Внешнему Курсу - Этап 1

Основы информационной безопасности

Чистов Даниил Максимович

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Выводы	16
4	Список литературы	17

Список иллюстраций

2.1	Задание 1																		5
2.2	Задание 002																		6
2.3	Задание 003																		6
2.4	Задание 004																		7
2.5	Задание 005																		8
2.6	Задание 006																		8
2.7	Задание 007																		9
2.8	Задание 008																		9
2.9	Задание 009																		10
2.10	Задание 010																		10
2.11	Задание 011																		11
2.12	Задание 012																		11
2.13	Задание 013																		12
2.14	Задание 014																		12
2.15	Задание 015																		13
2.16	Задание 016																		13
2.17	Задание 017																		13
2.18	Задание 018																		14
2.19	Задание 019																		14
2.20	Задание 020																		15
2.21	Задание 021																		15
2.22	Задание 022																		15

1 Цель работы

Пройти внешний курс - Этап 1

2 Выполнение лабораторной работы

В лекционных материалах было сказано, что в протоколы прикладного уровня включён HTTPS (рис. 2.1).



Рис. 2.1: Задание 1

TCP работает на транспортном уровне, IP - на сетевом (рис. 2.2).

На каком уровне работает протокол ТСР?

Выберите один вариант из списка Верно. Так держать! Транспортном Прикладном Канальном Сетевом Следующий шаг Решить снова Ваши решения Вы получили: 1 балл

Рис. 2.2: Задание 002

Т.к. IPv4 - набор цифр от 0 до 255, следовательно исключаем варианты, которые содержат числа больше/меньше этого набора (рис. 2.3).

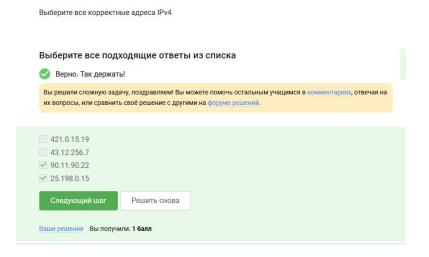


Рис. 2.3: Задание 003

DNS сопоставляет доменное имя соответствующий ему IP (рис. 2.4).

DNS сервер

Выберите один вариант из списка





Рис. 2.4: Задание 004

Порядок такой (рис. 2.5).

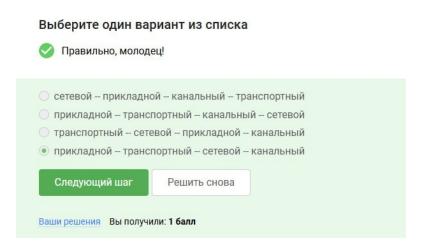


Рис. 2.5: Задание 005

http - предоставляет в открытом виде, именно эту проблему решает https, он работает также, только в этот раз данные шифруются (рис. 2.6).

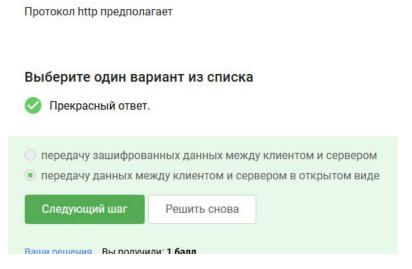


Рис. 2.6: Задание 006

Рукопожатие и передача данных, аутентификации не входит (рис. 2.7).

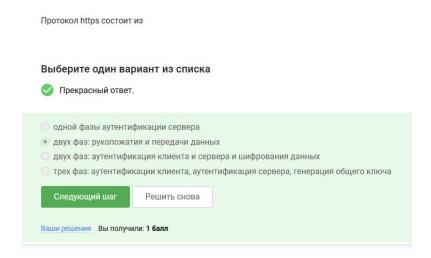


Рис. 2.7: Задание 007

Обязательно версия протокола определяется обоими (рис. 2.8).

Версия протокола TLS определяется

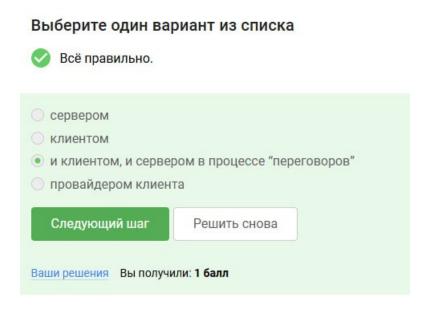


Рис. 2.8: Задание 008

Шифрование данных не происходит в фазе рукопожатия, только после неё (рис. 2.9).

В фазе "рукопожатия" протокола TLS не предусмотрено

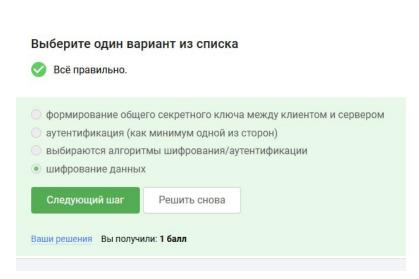


Рис. 2.9: Задание 009

Куки не хранят пароль пользователя или его IP адрес (рис. 2.10).



Рис. 2.10: Задание 010

Куки не сильно влияют на безопасность, скорее упрощают работу пользователям (рис. 2.11).



Рис. 2.11: Задание 011

Куки генерируются сервером и отправляются клиенту, а не наоборот (рис. 2.12).

Куки генерируются

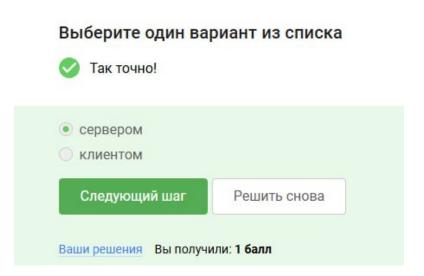


Рис. 2.12: Задание 012

Сессионные куки исчезнут, как только мы закроем окно с веб-сайтом (рис. 2.13).

Сессионные куки хранятся в браузере?

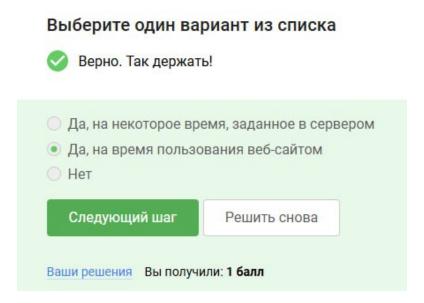


Рис. 2.13: Задание 013

3, т.к. больше узлов анонимности не прибавляют, а при меньших узлах теряется смысл всего алгоритма маршрутизации TOR (рис. 2.14).



Рис. 2.14: Задание 014

При шифровании так получается, что охранный узел и промежуточный узел не знают по итогу IP адрес получателя данных (рис. 2.15).

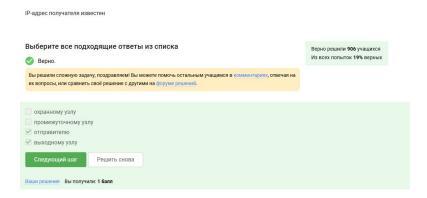


Рис. 2.15: Задание 015

Отправитель генерирует общий секретный ключ со всеми тремя узлами (рис. 2.16).

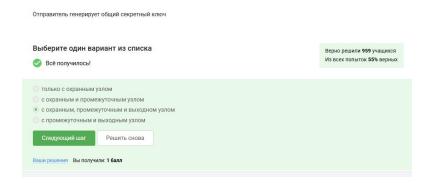


Рис. 2.16: Задание 016

Нет, не должен, далее возвращение данных происходит как обычно (рис. 2.17).

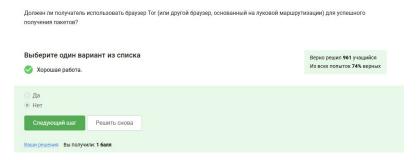


Рис. 2.17: Задание 017

У Wi-fi нет расшифроки, вообще это была такая пометка от компании, которая

проверяла поддерживает ли устройство беспроводную сеть, а так это технология беспроводной сети (рис. 2.18).

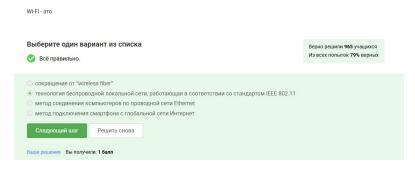


Рис. 2.18: Задание 018

На канальном уровне, т.к. речь всё-таки идёт о физическом излучении и приёме сигнала (рис. 2.19).



Рис. 2.19: Задание 019

WEP самый первый, но и к сожалению, небезопасный, на данный момент самый безопасный - WPA3 (рис. 2.20).



Рис. 2.20: Задание 020

На новых версиях беспроводных сетей происходит шифрование, но перед этим обязательно аутентификация (рис. 2.21).

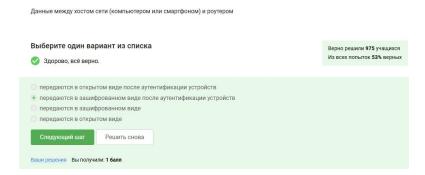


Рис. 2.21: Задание 021

Для домашней сети - personal, для Корпоративных сетей используют Enterprise, т.к. есть база данных её пользователей. Это усиливает безопасность корпорации. (рис. 2.22).

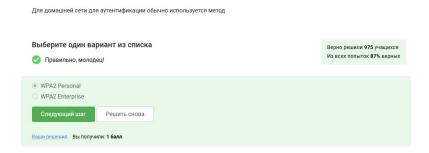


Рис. 2.22: Задание 022

3 Выводы

Этап 1 пройден успешно на максимальный балл.

4 Список литературы

Курс "Основы Кибербезопасности" на платформе Stepik