ОТЧЕТ ПО ПРОХОЖДЕНИЮ ВНЕШНЕГО КУРСА «ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ»

РАЗДЕЛ 1. БЕЗОПАСНОСТЬ СЕТИ

Поляков Глеб Сергеевич

Содержание

# 1 Цель работы

Целью данной работы является изучение безопасности сети и прохождение контрольных мероприятий внешнего курса.

# 2 Выполнение работы

Выполнение работы:

*Как работает интернет: базовые сетевые протоколы*

*Вопрос 1.*

|  |
| --- |
| Название рисунка |

Рис. 1: Название рисунка

HTTPS является протоколом прикладного уровня, так как он функционирует поверх протокола транспортного уровня (обычно TCP) и обеспечивает следующие функции для приложений:

1. **Шифрование**: HTTPS шифрует данные, передаваемые между клиентом и сервером, что обеспечивает конфиденциальность и безопасность передаваемой информации.
2. **Аутентификация**: HTTPS использует цифровые сертификаты для проверки подлинности сервера, что гарантирует пользователям подключение к правильному веб-сайту.
3. **Целостность данных**: HTTPS проверяет целостность передаваемых данных, чтобы убедиться, что они не были подделаны или изменены в процессе передачи.

Эти функции позволяют приложениям, таким как веб-браузеры и веб-серверы, безопасно и надежно обмениваться данными через Интернет.

|  |
| --- |
| Название рисунка |

Рис. 2: Название рисунка

*Вопрос 2.*

Название рисунка TCP работает на транспортном уровне, так как он отвечает за передачу данных между приложениями на разных узлах сети. Этот протокол обеспечивает надежную доставку данных, управляя сегментацией, сборкой и повторной передачей пакетов данных. Название рисунка

*Вопрос 3.*

Название рисунка Адреса 421.0.15.19 и 43.12.256.7 некорректны, потому что:

* **421.0.15.19**: Первый октет должен быть в диапазоне от 0 до 255.
* **43.12.256.7**: Третий октет должен быть в диапазоне от 0 до 255.

Корректный адрес IPv4 состоит из четырех октетов, каждый из которых представляет собой число в диапазоне от 0 до 255, разделенных точками. Название рисунка *Вопрос 4.* Название рисунка DNS-сервер (система доменных имен) сопоставляет доменные имена с соответствующими IP-адресами. Это позволяет пользователям легко получить доступ к веб-сайтам и другим сетевым ресурсам, вводя понятные доменные имена вместо сложных числовых IP-адресов. Название рисунка

*Вопрос 5.* Название рисунка Эта последовательность соответствует стеку протоколов TCP/IP, где:

* **Прикладной уровень**: предоставляет услуги приложениям, таким как передача файлов (FTP), электронная почта (SMTP) и веб-просмотр (HTTP).
* **Транспортный уровень**: обеспечивает надежную передачу данных между хостами, используя протоколы TCP и UDP.
* **Сетевой уровень**: отвечает за адресацию и маршрутизацию данных, используя протокол IP.
* **Канальный уровень**: управляет передачей данных по физическому сетевому интерфейсу, используя протоколы, такие как Ethernet и Wi-Fi. Название рисунка

*Вопрос 6.* Название рисунка Протокол HTTP (Hypertext Transfer Protocol) не шифрует данные, передаваемые между клиентом и сервером. Для безопасной передачи данных используется HTTPS (HTTP Secure), который шифрует данные с помощью протокола SSL/TLS. Название рисунка

*Вопрос 7.* Название рисунка Протокол HTTPS состоит из двух основных фаз:

1. **Фаза рукопожатия**: Клиент и сервер договариваются об используемых криптографических алгоритмах и обмениваются цифровыми сертификатами для аутентификации.
2. **Фаза передачи данных**: После успешного рукопожатия данные шифруются с использованием согласованных алгоритмов и передаются между клиентом и сервером. Название рисунка

*Вопрос 8.* Название рисунка Версия протокола TLS определяется в процессе “переговоров” между клиентом и сервером во время фазы рукопожатия. Клиент отправляет список поддерживаемых версий TLS, а сервер выбирает самую высокую версию, которую они оба поддерживают. Название рисунка

*Вопрос 9.* Название рисунка В фазе “рукопожатия” протокола TLS не предусмотрено шифрование данных. Эта фаза используется для установления безопасного канала связи, включая:

* Выбор версии протокола TLS и криптографических алгоритмов.
* Аутентификацию клиента и/или сервера с использованием цифровых сертификатов.
* Формирование общего секретного ключа.

После успешного рукопожатия данные шифруются и передаются во время фазы передачи данных. Название рисунка

*Персонализация сети* *Вопрос 1.* Название рисунка Куки хранят информацию, которая используется для идентификации пользователя или отслеживания состояния сеанса. Эта информация обычно включает такие данные, как идентификатор сессии, идентификатор пользователя и настройки пользователя. IP-адрес и пароль пользователя обычно не хранятся в куках из соображений безопасности и конфиденциальности. Название рисунка

*Вопрос 2.* Название рисунка Куки в первую очередь используются для хранения информации о состоянии и предпочтениях пользователя. Они не предназначены для улучшения надежности соединения, которое в основном обеспечивается протоколами транспортного уровня, такими как TCP и UDP. Название рисунка

*Вопрос 3.* Название рисунка Куки генерируются веб-сервером и отправляются клиенту в заголовке HTTP-ответа. Клиент хранит куки и отправляет их обратно на сервер каждый раз, когда запрашивает ресурс с того же домена. Название рисунка

*Вопрос 4.* Название рисунка Сессионные куки хранятся в браузере пользователя только во время текущего сеанса просмотра. Они удаляются, когда пользователь закрывает браузер или истекает срок их действия, который обычно задается в секундах и определяется веб-сервером. Название рисунка

*Браузер TOR. Анонимизация* *Вопрос 1.* Название рисунка В луковой сети TOR используется три промежуточных узла для обеспечения анонимности и защиты от сетевого анализа. Эти узлы называются входным узлом, промежуточным узлом и выходным узлом. Название рисунка

*Вопрос 2.* Название рисунка В сети TOR отправитель и выходной узел имеют информацию о IP-адресе получателя, поскольку отправитель напрямую направляет данные получателю через выходной узел. Однако охранный и промежуточные узлы знают только IP-адрес следующего узла в цепочке, что обеспечивает анонимность и защищает конфиденциальность передаваемой информации. Название рисунка

*Вопрос 3.* Название рисунка При внедрении системы обмена ключами с использованием охранных, промежуточных и выходных узлов достигается повышенная надежность и защита. Каждый из этих узлов выполняет определенные функции, направленные на обеспечение безопасности передаваемой информации. Охранный узел отвечает за предотвращение несанкционированного доступа, промежуточный узел может добавлять дополнительные слои защиты или обработки данных, а выходной узел осуществляет передачу уже защищенной информации получателю.

Использование всех трех узлов способствует увеличению сложности системы шифрования и делает её менее уязвимой к атакам. Кроме того, это обеспечивает более эффективную защиту информации в процессе передачи от отправителя к получателю. Название рисунка

*Вопрос 4.* Название рисунка Получателю не нужно использовать браузер Tor или другой браузер, основанный на луковой маршрутизации, для успешного получения пакетов. Луковые маршрутизаторы автоматически расшифровывают и перенаправляют пакеты через цепочку луковых маршрутизаторов, обеспечивая анонимность отправителя, но не получателя. Название рисунка

*Беспроводные сети Wi-fi* *Вопрос 1.* Название рисунка Wi-Fi, сокращение от Wireless Fidelity, представляет собой технологию беспроводной локальной сети (WLAN), которая использует радиоволны для обеспечения сетевого доступа и подключения устройств в ограниченной области действия. Она основана на стандартах, установленных Институтом инженеров по электротехнике и электронике (IEEE), в частности, стандарте IEEE 802.11. Wi-Fi позволяет устройствам подключаться к сети Интернет, обмениваться файлами и совместно использовать ресурсы без необходимости физических кабельных соединений. Название рисунка

*Вопрос 2.* Название рисунка Протокол Wi-Fi функционирует на канальном уровне модели OSI. Этот уровень отвечает за передачу данных между устройствами в пределах одного сегмента сети. Он контролирует доступ к среде передачи, обнаруживает и исправляет ошибки в передаваемых данных, а также обеспечивает физическую адресацию устройств. В контексте Wi-Fi реализация канального уровня осуществляется через стандарты IEEE 802.11, такие как 802.11a, 802.11b, 802.11g, 802.11n и 802.11ac. Эти стандарты определяют различные физические и протокольные характеристики для беспроводной связи. Название рисунка

*Вопрос 3.* Название рисунка WEP (Wired Equivalent Privacy) является небезопасным методом обеспечения шифрования и аутентификации в сети Wi-Fi. Он был разработан в 1997 году как первый протокол безопасности для беспроводных локальных сетей, но из-за серьезных уязвимостей его безопасность была скомпрометирована вскоре после появления. WEP использует слабые механизмы шифрования и аутентификации, что делает его уязвимым для перехвата и взлома данных. Поэтому WEP больше не рекомендуется использовать и должен быть заменен более надежными протоколами безопасности, такими как WPA, WPA2 или WPA3.

*Вопрос 4.* Название рисунка В современных сетях Wi-Fi данные между хостом сети (компьютером или смартфоном) и роутером передаются в зашифрованном виде после того, как устройства успешно пройдут аутентификацию. Это делается для защиты данных от перехвата и несанкционированного доступа. Для шифрования используются протоколы безопасности, такие как WPA2 или WPA3, которые обеспечивают надежное шифрование и аутентификацию. Название рисунка

*Вопрос 5.* Название рисунка Для домашней сети для аутентификации обычно используется метод WPA2 Personal. WPA2 Personal использует предварительный общий ключ (PSK) для аутентификации устройств в сети. PSK - это пароль, который должен быть одинаковым на всех устройствах, подключающихся к сети. WPA2 Personal прост в настройке и обеспечивает надежную защиту для домашних сетей. Название рисунка

# 3 Вывод

В ходе выполнения лабораторной работы были приобретены знания в области безопасности интернет-трафика, а также знания были укреплены прохождением тестовых вопросов.

# Список литературы