Обеспечение безопасности веб-приложений.фип_СПО_н/с

1. На ваш компьютер пришло сообщение о необходимости пройти тест по курсу компьютерных сетей. Укажите, в какой последовательности при декапсуляции данных будут анализироваться заголовки уровней модели OSI?
2. Какое(ие) из перечисленных устройств является(ются) устройством(ами) канального уровня модели OSI? Выберите все верные ответы.
3. Какое(ие) из перечисленных устройств является(ются) устройством(ами) сетевого уровня модели OSI?
4. Какое(ие) из перечисленных устройств является(ются) устройством(ами) транспортного уровня модели OSI?
5. Укажите протоколы транспортного уровня модели OSI. Выберите все верные ответы.
6. В каком(их) из перечисленных протоколов блоки данных имеют не только заголовок, но и концевик?
7. Укажите, какое количество соединений необходимо для построения полносвязанной топологии из 5 устройств?
8. Укажите, какое количество соединений необходимо для построения полносвязанной топологии из 10 устройств?
9. Как называется система, которая в одном месте хранит информацию о том, какие сети для каких целей использованы, какие в этих сетях ресурсы, сколько адресов выдано (какой % утилизации адресного пространства в той или иной подсети)?
10. Клиент отправляет широковещательно сообщение Discover. Наш роутер, на котором настроена функция X, перехватывает это сообщение, сам его не обрабатывает, а отправляет на адрес сервера. Сервер это сообщение обрабатывает, понимает, из какого сегмента пришел запрос, смотрит пул адресов, который соответствует этому сегменту, и отправляет ответ (то есть происходит стандартная процедура получения IP-адреса). Другими словами, роутер «прикидывается» DHCP-сервером, а в реальности пересылает запрос дальше. Укажите, о какой функции протокола DHCP идет речь

11. Может ли роутер (в частности, ваш домашний Wi-Fi роутер) выполнять функции DHCP-сервера? В ответе укажите только да или нет.

12. Как может выглядеть MAC-адрес отправителя широковещательного фрейма? Выберите все верные ответы.

13. Выберете флаг протокола TCP, указывающий на важность = передаются ли в нашем сегменте какие-то важные данные. Если этот флаг поднят, то мы (принимающая сторона) обращаем внимание на поле Urgent point, которое показывает границы важных данных. Если этот флаг опущен, то на поле Urgent point мы, соответственно, смотреть не будем.

14. Выберете флаг протокола TCP, который говорит получателю о том, что принятые данные нужно не хранить в буфере, а как можно быстрее передать приложению.

15. Выберете флаг(и) протокола TCP, который(ые) используется(ют) для того, чтобы закрыть TCP-сессию

16. На рисунке ниже приведен пример статической NAT-трансляции. Узел B решил ответить на сообщение, полученное от узла A. Укажите, какой IP-адрес укажет узел B в качестве адреса получателя пакета.

17. На рисунке ниже приведен пример статической NAT-трансляции. Узел B решил ответить на сообщение, полученное от узла A. Укажите, какой IP-адрес укажет узел B в качестве адреса отправителя пакета.

18. На рисунке ниже приведен пример статической NAT-трансляции. Узел B решил ответить на сообщение, полученное от узла A. Укажите, какой IP-адрес будет в поле «IP-адрес получателя», когда ответ узла B придет на роутер R1.

19. Сопоставьте поля заголовков протоколов и протоколы, в которых они используются

20. Расположите протоколы Ethernet, IP, UDP в порядке возрастания уровня модели OSI, на котором расположен соответствующий протокол?

21. На рисунке ниже приведен пример динамической PAT-трансляции. Сервер 9.9.9.9 решил ответить на сообщение, полученное от узла A. Укажите, какой TCP-порт будет в поле «TCP-порт отправителя», когда ответ узла B окажется в левой части сети (то есть после обработки роутером R1). В ответе укажите только номер порта.

22 Укажите сообщения протокола DHCP в порядке их появления в сети в процессе стандартного получения хостом IP-адреса:

23 Позволяет ли переход от концентраторов к коммутаторам в локальных сетях полностью избавиться от прослушивания сети злоумышленником?

24 Какую информацию может предоставить кабельный тестер?

25 Системный администратор подключила свой ноутбук к сетевому устройству с надписью Switch на лицевой панели с помощью прямого патч-корда и увидела, что с помощью Auto MDI/MDIX у неё определились следующие параметры работы среды: 100 FX. Может ли она утверждать, что устройство, к которому она подключилась, - коммутатор? Что на это указывает?

26 В процессе своей работы коммутатор обучается (learning) на проходящем трафике. Что используется для заполнения мостовой таблицы?

27 Какой механизм позволяет ограничить количество изученных MAC-адресов на порту коммутатора?

28 Какой механизм позволяет защититься от атак с использованием rogue DHCP-сервер?

29 Что такое native-VLAN (выберите максимально подходящий ответ)?

30 На что направлена атака DHCP starvation?

31 В чём смысл атаки ARP spoofing?

32 В чём смысл атаки ARP flooding?

33 С помощью какого механизма DHCP-сервер может узнать, к какому порту какого коммутатора подключен DHCP-клиент?

34 С помощью какого протокола злоумышленник может узнать подробную информацию о коммутаторе, к которому подключен?

35 С помощью какого протокола злоумышленник может удалить всю информацию о виртуальных сетях (VLAN) с коммутаторов?

36 С помощью какого протокола можно провести аутентификацию подключаемого к сети устройства?

37 С помощью какого пассивного устройства можно получить копию трафика, передаваемого через оптический канал?

38 Какое сообщение используется маршрутизатором в протоколе NDP для сообщения о себе, то есть, например, для объявления о том, что данный маршрутизатор можно использовать для выхода из сегмента сети?

39 При проведении атаки DHCP starvation появление какого из перечисленных сообщений протокола DHCP не ожидается: Discover, Offer, Request, Release?

40 Упорядочите уровни модели OSI (снизу вверх):

41 Поставьте в соответствие названия устройств из левого столбца уровням модели OSI из правого столбца.

42 Поставьте понятию из левого столбца в соответствие уровень модели OSI из правого столбца.

43 Какова длина ключа для протокола симметричного шифрования DES (в битах)?

44 Какая длина блока используется при шифровании с помощью протокола DES?

45 В чем содержится «весь секрет» алгоритмов симметричного шифрования?

46 Какой параметр алгоритма шифр Цезаря можно назвать ключом шифрования?

47 Какая суммарная длина ключей в алгоритме шифрования 3DES (в битах)?

48 Какие цели преследует нарушитель, пытаясь взломать алгоритм симметричного шифрования?

49 Как называется статистическая зависимость между исходным и зашифрованным сообщением?

50 Используется ли ключ шифрования при начальной и конечной перестановках (Initial Permission) в алгоритме DES?

51 Как называются алгоритмы, которые разбивают сообщение на блоки определенной длины, и шифруют отдельный блок?

52 Использует ли алгоритм симметричного шифрования DES классическую сеть Фейштеля? (В ответе укажите только да или нет)

53 Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?

54 Укажите количество раундов в алгоритме симметричного шифрования DES (В ответе укажите только число).

55 Что в криптографии называют открытым текстом?

56 Укажите, число S-боксов (блоков), используемых в алгоритме симметричного шифрования DES

57 Укажите длину ключа раунда для протокола DES в битах

58 Сколько ветвей в сети Фейстеля в протоколе DES?

59 Требуется ли при шифровании с помощью алгоритмов, использующих сеть Фейстеля, обратимость функции F в сети Фейстеля? (В ответе укажите только да или нет)

60 До какой длины (в битах) расширяется во время раунда шифрования правая ветка сети Фейстеля в алгоритме DES?

61 Установите соответствие между алгоритмами симметричного шифрования и длинами ключей

62 Расположите алгоритмы симметричного шифрования 3DES, DES, AES в порядке возрастания их криптографической стойкости

63 Изучите структуру функции расширения для алгоритма симметричного шифрования DES. Выпишите номера бит, полученные в первой строке после применения функции расширения (получается таблица из 8 строк, по 6 бит в каждой), если считать, что изначально все биты были занумерованы от 1 до 32. В ответе укажите номера бит без пробелов.

64 Какая может быть длина ключа для протокола симметричного шифрования AES (в битах)? Выберите все правильные варианты

65 Какая длина блока используется при шифровании с помощью протокола AES?

66 В чем содержится «весь секрет» алгоритма симметричного шифрования AES?

67 В какой из 4 приведенных ниже операций раунда вводится понятие S-боксов в рамках алгоритма AES?

68 На какое количество элементов значения в таблице ниже сдвинутся влево в 0 строке при операции ShiftRows алгоритма AES?

69 На какое количество элементов значения в таблице ниже сдвинутся влево в 1 строке при операции ShiftRows алгоритма AES?

70 Как называется статистическая зависимость между исходным и зашифрованным сообщением?

71 На какое количество элементов значения в таблице ниже сдвинутся влево во 2 строке при операции ShiftRows алгоритма AES?

72 Какой блочный режим шифрования иллюстрирует данная схема? (В ответе можно указать аббревиатуру/полное название)

73 Использует ли алгоритм симметричного шифрования AES классическую сеть Фейстеля? (В ответе укажите только да или нет)

74 На какое количество элементов значения в таблице ниже сдвинутся влево в 3 строке при операции ShiftRows алгоритма AES?

75 Укажите количество раундов в алгоритме симметричного шифрования AES при использовании длины ключа и длины блока 128 бит? (В ответе укажите только число).

76 Выберите, какие операции используются в алгоритмах симметричного шифрования?

77 Укажите количество раундов в алгоритме симметричного шифрования AES при использовании длины ключа 192 бита и длины блока 128 бит? (В ответе укажите только число).

78 Укажите количество раундов в алгоритме симметричного шифрования AES при использовании длины ключа 192 бита и длины блока 128 бит? (В ответе укажите только число).

79 Какой блочный режим шифрования иллюстрирует данная схема? (В ответе можно указать аббревиатуру/полное название)

80 Требуется ли обратимость преобразований, выполняемых во время раунда в протоколе симметричного шифрования AES? (В ответе укажите только да или нет)

81 До какой длины (в битах) расширяется во время раунда шифрования правая ветка сети Фейстеля в алгоритме DES?

82 Установите соответствие между алгоритмами симметричного шифрования и длинами ключей

83 Расположите функции раунда, используемые в алгоритме AES – AddRoundKey, MixColomns, ShiftRows, SubBytes, в том порядке, в котором они применяются во время раунда шифрования.

84 Изучите описание, предложенное ниже и определите, о каком режиме шифрования блоков идет речь. В ответе можно указать аббревиатуру/полное название. Преимущество данного режима заключается в том, что в случае потери пакета при транспорте от отправителя к получателю ничего страшного не произойдет – следующий пакет расшифруется. Однако мы теряем в безопасности, потому что в хвост регистра мы фактически помещаем зашифрованный исходный текст, и можно попытаться перебрать ключи

85 Логика работы какой хеш-функции изображена на блок-схеме ниже?

86 Логика работы какой хеш-функции изображена на блок-схеме ниже?

87 Логика работы какой хеш-функции изображена на блок-схеме ниже?

88 Логика работы какой хеш-функции изображена на блок-схеме ниже?

89 Какой сервис безопасности иллюстрирует данное изображение?

90 В какой хеш-функции вычисления циклов происходят с использованием следующих функций?

91 Укажите длину хеш-кода для функции MD5 (в битах).

92 Значения входных регистров какой функции хеширования представлены на изображении ниже?

93 Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции MD5.

94 Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции SHA-2 [256].

95 Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции SHA-2 [512].

96 Какой может быть длина хеш-кода у функции SHA-2? (Выберите все подходящие варианты)

97 Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции SHA-2 [384].

98 Укажите длину хеш-кода для функции SHA-1 (в битах).

99 Какая наименьшая длина длина хеш-кода может быть у функции SHA-3? (в битах)

100 Какая наибольшая длина длина хеш-кода может быть у функции SHA-3? (в битах)

101 Преобразования, применяемые в цикле какой хеш-функции представлены в формуле ниже? (В ответе запишите только название хеш-функции, например SHA-3)

102 Установите соответствие между хеш-функциями и длинами хеш-кодов этих функций

103 Расположите хеш-функции MD5, SHA-1, SHA-2 в порядке возрастания длины хеш-кода

104 Изучите описание, предложенное ниже, и определите, о какой хеш-функции идет речь. В ответе запишите только название хеш-функции, например SHA-1 Алгоритм основан на «принципе губки». Исходное сообщение делится на блоки; используется начальный вектор, который состоит из двух частей r и c. Выполняется XOR r-части с первым блоком, полученный результат и блок с подаются в функцию f и так до тех пор, пока не закончится сообщение. Это так называемая стадия «сжатия». Когда сообщение закончилось, начинается стадия «отжатия»: используется та же функция f, результат выдается до получения хэш-кода нужной длины.

105 Как называется протокол, который позволяет спросить у сервера, истек ли сертификат?

106 Как называется список недействительных сертификатов, который каждый сертификационный центр выпускает через определенные промежутки времени ΔT (должен быть подписан закрытым ключом CA)?

107 Какие значения может принимать поле признак критичности у расширений сертификата X.509?

108 Какая версия сертификатов формата X.509 наиболее распространена на сегодняшний день?

109 Какой сервис безопасности иллюстрирует данное изображение?

110 В какой хеш-функции вычисления циклов происходят с использованием следующих функций?

111 Укажите длину хеш-кода для функции MD5 (в битах).

112 Какой формат сертификатов наиболее распространен на сегодняшний день?

113 Какая оптимизация протокола OSCP изображена на схеме ниже?

114 Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции SHA-2 [256].

115 Значения входных регистров какой функции хеширования представлены на изображении ниже?

116 Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции SHA-2 [512].

117 Какой может быть длина хеш-кода у функции SHA-2? (Выберите все подходящие варианты)

118 Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции SHA-2 [384].

119 Укажите длину хеш-кода для функции SHA-1 (в битах).

120 Какая наименьшая длина длина хеш-кода может быть у функции SHA-3? (в битах)

121 Какая наибольшая длина длина хеш-кода может быть у функции SHA-3? (в битах)

122 Преобразования, применяемые в цикле какой хеш-функции представлены в формуле ниже? (В ответе запишите только название хеш-функции, например SHA-3)

123 Установите соответствие между хеш-функциями и длинами хеш-кодов этих функций

124 Расположите хеш-функции MD5, SHA-1, SHA-2 в порядке возрастания длины хеш-кода

125 Изучите описание, предложенное ниже, и определите, о какой хеш-функции идет речь. В ответе запишите только название хеш-функции, например SHA-1 Алгоритм основан на «принципе губки». Исходное сообщение делится на блоки; используется начальный вектор, который состоит из двух частей r и c. Выполняется XOR r-части с первым блоком, полученный результат и блок с подаются в функцию f и так до тех пор, пока не закончится сообщение. Это так называемая стадия «сжатия». Когда сообщение закончилось, начинается стадия «отжатия»: используется та же функция f, результат выдается до получения хэш-кода нужной длины.

126 Между протоколами каких уровней модели OSI располагается заголовок протокола ESP?

127 Между протоколами каких уровней модели OSI располагается заголовок протокола AH?

128 Целостность каких полей IP-заголовка может проверить протокол AH?

129 Между протоколами каких уровней модели OSI может быть расположен заголовок протокола ESP? Выберите все подходящие варианты.

130 Между протоколами каких уровней модели OSI может быть расположен заголовок протокола ESP? Выберите все подходящие варианты.

131 Целостность каких полей IP-заголовка не может проверить протокол AH?

132 Как называется упорядоченный набор записей, в котором содержится действие Action и параметры трафика? В ответе приведите только аббревиатуру данной базы данных на английском языке

133 Какой формат сертификатов наиболее распространен на сегодняшний день?

134 Какой сервис безопасности может быть обеспечен протоколом ESP и принципиально не обеспечивается протоколом AH?

135 Укажите, Main mode или Aggressive mode используется на схеме ниже при установления соединения в первой фазе. В ответе укажите только Main mode/Aggressive mode

136 Укажите, Pre-shared secret или Сертификат используется на схеме ниже для аутентификации в первой фазе. В ответе укажите только Pre-shared secret/Сертификат

137 Укажите, Main mode или Aggressive mode используется на схеме ниже при установления соединения в первой фазе. В ответе укажите только Main mode/Aggressive mode

138 Укажите, Pre-shared secret или Сертификат используется на схеме ниже для аутентификации в первой фазе. В ответе укажите только Pre-shared secret/Сертификат

139 Укажите, Main mode или Aggressive mode используется на схеме ниже при установления соединения в первой фазе. В ответе укажите только Main mode/Aggressive mode

140 На рисунке ниже приведена последовательность заголовков для решения GRE over IPSec. В каком режиме в данном случае работает IPSec: туннельном или транспортном? В ответе Укажите только режим: туннельный/транспортный.

141 Установите соответствие между хеш-функциями и длинами хеш-кодов этих функций

142 Расположите хеш-функции MD5, SHA-1, SHA-2 в порядке возрастания длины хеш-кода

143 Изучите описание, предложенное ниже, и определите, о каком протоколе семейства IPSec идет речь. В ответе запишите только название протокола, например ESP Данный протокол используется для формирования IPSec SA, проще говоря, согласования работы участников защищенного соединения. Используя этот протокол, участники договариваются, какой алгоритм шифрования будет использоваться, по какому алгоритму будет производиться (и будет ли вообще) проверка целостности, как аутентифицировать друг друга

144 С чем связано ограничение на количество записей IP route records в пакете? Укажите ответ в именительном падеже.

145 Какое максимальное количество IP route records может быть в пакете?

146 Путь, отображаемый утилитой tracert, ограничен тридцатью хопами. Вы можете написать свою собственную утилиту tracert, сняв ограничение в тридцать хопов. Какое максимальное количество хопов могла бы отображать Ваша утилита, работающая по тому же принципу, что и стандартный tracert (traceroute)?

147 Что такое white list?

148 Что лежит в основе атаки Ping of Death?

149 Что лежит в основе атаки TearDrop?

150 Какова наиболее вероятная причина использования злоумышленником маршрутизации от источника?

151 Что может стать узлом ботнет?

152 Какой тип DDoS атак может быть подавлен непосредственно на площадке заказчика с использованием специализированного оборудования, но без привлечения услуг провайдера или иных компаний?

153 В чём суть защиты от атаки SYN flood с помощью SYN cookie?

154 Что означает «DNS amplification»?

155 При какой атаке рассылается сообщение ICMP echo request на широковещательный адрес подсети?

156 При какой атаке злоумышленник отправляет специально подготовленные сегменты TCP, в которых порт отправителя совпадает с портом получателя, а значение IP-адреса получателя совпадает с IP-адресом отправителя?

157 Как называется компьютерная сеть, состоящая из некоторого количества хостов с запущенным автономным программным обеспечением. Чаще всего на узлах находится программа, скрытно установленная на устройство жертвы и позволяющая злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера?

158 Что лежит в основе атак Smurf и Fraggle?

159 Каково максимальное смещение фрагмента допустимо в IPv4-сетях?

160 Как называется механизм, позволяющий запретить принимать пакеты, если маршрут на отправителя этих пакетов лежит не через тот интерфейс, через который они были получены?

161 В заголовке пакета протокола IPv6 отсутствуют опции. Что используется вместо них?

162 Поставьте в соответствие название атаки и её описание.

163 Расположите протоколы динамической маршрутизации в порядке возрастания AD (с точки зрения Cisco):

164 Злоумышленник хочет использовать DNS-amplification, для чего формирует особым образом запросы к DNS-серверам. Вне зависимости от длины запроса ответ, возвращаемый DNS-сервером, имеет фиксированную длину. Расположите домены, для которых злоумышленник отправляет запрос, в порядке увеличения КПД атаки: synergy.ru, mail.ru, yandex.ru.

165 Укажите цель, которую преследует злоумышленник при использовании VLAN ID Enumeration.

166 Как формируется значение BID коммутатора без использования опции Extended System ID? Ответ запишите в виде x/y, где x – длина Bridge Priority в байтах, а y – длина MAC-адреса коммутатора в байтах.

167 Как формируется значение BID коммутатора при использовании опции Extended System ID? Ответ запишите в виде x/y/z, где x – длина Bridge Priority в битах, y – длина Extended System ID в битах, а z – длина MAC-адреса коммутатора в битах.

168 Какой виртуальной сети (VLAN ID) соответствует следующее значение BID коммутатора - 8315?

169 Какую цель преследует злоумышленник при выполнении атаки Eternal Election Attack?

170 Какую цель преследует злоумышленник при выполнении атаки Root Disappearance Attack?

171 Какую цель преследуют злоумышленник при выполнении атаки Merging-splitting of the trees?

172 Злоумышленник подключён к одному порту коммутатора доступа. Что из перечисленного ниже поможет защититься от любых STP-атак с его стороны?

173 Что из перечисленного ниже может помочь против атак, связанных с перевыборами корневого коммутатора?

174 Как называется BPDU, в котором содержится меньшее значение Rood ID?

175 Каково значение таймера forwarding delay по умолчанию в классическом протоколе STP?

176 Как влияет событие изменение топологии в протоколе STP на время жизни записей в таблице коммутации?

177 На таблицы коммутации каких коммутаторов влияет событие изменения топологии в протоколе STP?

178 Какая версия протокола STP позволяет построить несколько деревьев, соответствующих независимым топологиям (обычно больше одного, но меньше количества существующих виртуальных сетей (VLAN))?

179 Какая версия протокола STP строит столько деревьев, сколько используется виртуальных сетей (VLAN)?

180 Какая версия протокола STP всегда строит одно единственное деревно вне зависимости от количества виртуальных сетей (VLAN)?

181 Каково значение hello таймера по умолчанию в классическом протоколе STP?

182 Как называется опция, позволяющая заблокировать интерфейс коммутатора, если через него было получено любое сообщение STP BPDU?

183 Понятиям, технологиям, оптимизациям в левом столбце поставьте в соответствие протоколу, который указан в правом столбце?

184 Ролям портов коммутатора из левого столбца поставьте в соответствие версию протокола STP из правого столбца?

185 Коммутатор работает в режиме классического STP 802.1D. Расставьте статусы интерфейса, через которые пройдёт порт, в соответствующем порядке, если к нему подключают какое-либо устройство: Blocking, Learning, Listening, Forwarding?

186 Какой(ие) сервис(ы) безопасности реализован(ы) на схеме ниже?

187 Какой(ие) сервис(ы) безопасности реализован(ы) на схеме ниже?

188 Какой(ие) сервис(ы) безопасности реализован(ы) на схеме ниже?

189 В каком алгоритме асимметричного шифрование секрет шифруется по схеме, предложенной ниже?

190 В каком алгоритме асимметричного шифрование секрет расшифровывается по схеме, предложенной ниже?

191 В каком алгоритме асимметричного шифрование ключ сессии вырабатывается (передается) по схеме, предложенной ниже?

192 Логика вычисления открытого и закрытого ключа какого протокола асимметричного шифрования представлена ниже?

193 Какой алгоритм асимметричного шифрования основан на задаче факторизации числа?

194 Верно ли утверждение про алгоритмы асимметричного шифрования: легко вычислить пару (KU, KR). В ответе укажите только да или нет

195 Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно легко зашифровать сообщение, используя открытый ключ (KU). В ответе укажите только да или нет

196 Укажите, какой(ие) из предложенных алгоритмов асимметричного шифрования может(гут) использоваться для создания цифровой подписи?

197 Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно легко расшифровать сообщение, используя закрытый ключ (KR). В ответе укажите только да или нет

198 Укажите, какой(ие) из предложенных алгоритмов асимметричного шифрования может(гут) использоваться для обмена общим секретом?

199 Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно трудно, зная открытый ключ (KU), найти соответствующий ему закрытый ключ (KR). В ответе укажите только да или нет

200 Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно трудно, зная зашифрованное сообщение (C) и открытый ключ (KU), найти исходное сообщение (M). В ответе укажите только да или нет

201 Верно ли утверждение про алгоритмы асимметричного шифрования: трудно вычислить пару (KU, KR). В ответе укажите только да или нет

202 Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно трудно зашифровать сообщение, используя открытый ключ (KU). В ответе укажите только да или нет

203 Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно легко, зная открытый ключ (KU), найти соответствующий ему закрытый ключ (KR). В ответе укажите только да или нет

204 Установите соответствие между столбцами слева и справа

205 Расположите алгоритмы симметричного шифрования 3DES, DES, AES в порядке возрастания их криптографической стойкости

206 В алгоритме асимметричного шифрования RSA p = 5, q = 7. Вычислите значение φ(n), n =pq. В ответе укажите только число.

207 Какое количество корневых центров сертификации существует на данный момент?

208 Каким образом операционная система изначально получает список доверенных корневых центров сертификации?

209 Как коротко называется список отозванных сертификатов?

210 В чём состоит основной недостаток использования CRL?

211 Чей сертификат обычно имеет самый длительный период валидности? Укажите ответ в именительном падеже.

212 Может ли сертификат конечного устройства быть заменён раньше окончания срока его действия?

213 Может ли электронный сертификат выдаваться строго для определённых целей? Ответ да/нет.

214 Для чего используются электронные подписи в сертификате (fingerprints)?

215 Может ли маршрутизатор Cisco встраиваться в цепочку доверия с корневым центром сертификации, работающим под управлением операционной системы MS Windows?

216 Для чего может использовать сертификаты site-to-site IPSec VPN?

217 С помощью какой команды клиентский маршрутизатор Cisco (с настроенным trustpoint) устанавливает отношения доверия с PKI-сервером?

218 Какой протокол является альтернативой CRL?

219 Для корректного функционирования PKI инфраструктуры критически важно наличие синхронизации времени. По какому протоколу это можно сделать?

220 При генерации ключей часто используется опция modulus. За что она отвечает?

221 Что выполняет функция grant?

222 Какую длину имеет хэш-сумма MD5?

223 Какую длину имеет хэш-сумма RSA-1?

224 Укажите одну из двух причин, по которой сертификат может быть удален из CRL.

225 Поставьте в соответствие название хэш-суммы в левом столбце и её длину из правого столбца.

226 Запишите в порядке возрастания время жизни следующих сущностей: сертификат ресурса, сертификат промежуточного центра сертификации, сертификат корневого центра сертификации, CRL.

227 Поставьте в соответствие высказывание из правого столбца методу проверки отозванных сертификатов из левого столбца.

228 Над протоколами какого уровня модели TCP/IP располагается протокол Записи технологии SSL/TLS?

229 Между протоколами каких уровней модели TCP/IP располагаются протоколы технологии SSL/TLS?

230 Конфиденциальность какого протокола можно обеспечить средствами технологии SSL/TLS?

231 Конфиденциальность какого протокола можно обеспечить средствами технологии SSL/TLS?

232 Конфиденциальность какого протокола можно обеспечить средствами технологии SSL/TLS?

233 Конфиденциальность какого протокола можно обеспечить средствами технологии SSL/TLS?

234 Как называется упорядоченный набор записей, в котором содержится действие Action и параметры трафика? В ответе приведите только аббревиатуру данной базы данных на английском языке

235 Конфиденциальность какого протокола можно обеспечить средствами технологии SSL/TLS?

236 Какой протокол асимметричного шифрования для формирования pre-master secret был исключен из технологии TLS 1.3 по сравнению с предыдущей версией?

237 С какого сообщения начинается установление соединения между клиентом и сервером по технологии TLS?

238 Является ли предоставление сертификата клиента обязательным при установке соединения по протоколу TLS? В ответе укажите только да или нет

239 Укажите количество раундов в алгоритме симметричного шифрования DES (В ответе укажите только число).

240 Что в криптографии называют открытым текстом?

241 Укажите, число S-боксов (блоков), используемых в алгоритме симметричного шифрования DES

242 Укажите длину ключа раунда для протокола DES в битах

243 Сколько ветвей в сети Фейстеля в протоколе DES?

244 Требуется ли при шифровании с помощью алгоритмов, использующих сеть Фейстеля, обратимость функции F в сети Фейстеля? (В ответе укажите только да или нет)

245 До какой длины (в битах) расширяется во время раунда шифрования правая ветка сети Фейстеля в алгоритме DES?

246 Установите соответствие между версиями протокола TLS и состояниями данных версий

247 Расположите хеш-функции MD5, SHA-1, SHA-2 в порядке возрастания длины хеш-кода

248 Изучите описание, предложенное ниже, и определите, о каком протоколе семейства IPSec идет речь. В ответе запишите только название протокола, например ESP Данный протокол используется для формирования IPSec SA, проще говоря, согласования работы участников защищенного соединения. Используя этот протокол, участники договариваются, какой алгоритм шифрования будет использоваться, по какому алгоритму будет производиться (и будет ли вообще) проверка целостности, как аутентифицировать друг друга

249 Что не является недостатком режима настройки IPSec с использованием криптографических карт?

250 В какой фазе установления IPSec соединения используется протокол ISAKMP? Ответ укажите цифрой

251 Какова минимальная длина заголовка протокола GRE?

252 С помощью параметра transform-set можно выбрать режим работы IPSec-соединения. Какие два режима поддерживаются?

253 Какой алгоритм сжатия данных поддерживается в IPSec?

254 При настройке VTI IPSec как режим работы туннельного интерфейса должен быть выбран?

255 Какой алгоритм шифрования данных не поддерживается в ISAKMP сессии (на том оборудовании, которое используется в курсе)?

256 Для чего в одну криптокарту добавляют несколько записей?

257 Что не является преимуществом подхода GRE over IPSec по сравнению с традиционными криптокартами?

258 В чём особенность настройки списков доступа (ACL) для отбора «интересного» трафика при использовании криптокарт?

259 Чем отличается настройка IPSec VTI от настройки традиционного IPSec с использованием криптокарт?

260 В какой ситуации наиболее вероятно использование сертификата для аутентификации, а в какой разделяемого секрета (pre-shared key)?

261 Что наиболее точно описывает работу группы Диффи-Хэллмана?

262 Что из перечисленного ниже верно описывает разницу между первой и второй версиями протокола IKE?

263 Возможно ли AH использовать в туннельном режиме? Ответ да/нет.

264 Может ли IPSec с ESP передавать данные открытым? Ответ да/нет.

265 Какое минимальное количество байт добавляется к пакету при стандартной GRE инкапсуляции?

266 В какой транспортный протокол может инкапсулироваться IPSec?

267 Поставьте в соответствие характеристику работы протокола из правого столбца протоколу из левого столбца?

268 Запишите алгоритмы шифрования, упорядочив их от самых слабых до наиболее криптостойких: AES, DES, 3DES.

269 Запишите режимы настройки IPSec, упорядочив их по времени появления: VTI, GRE over IPSec и IPSec with crypto-maps.

270 Какой протокол используется для связи между прокси-сервером и сервером антивирусной защиты?

271 Корпоративный пользователь просматривает разнообразные ресурсы в Интернет со своего рабочего места. При посещении большинства страниц браузер отображает предупреждение о проблемах с сертификатом сайта. Какова наиболее вероятная причина появления таких предупреждений?

272 С помощью какого режима работы ICAP прокси-сервер передает идущий от пользователя в Интернет-трафик на модуль антивирусной защиты?

273 С помощью какого режима работы ICAP прокси-сервер передает идущий из сети Интернет в сторону пользователя трафик на модуль антивирусной защиты?

274 Что такое межсайтовый скриптинг (XSS-атаки)?

275 Что такое атака нулевого дня (zero day)?

276 Что из перечисленного ниже является HTTP-запросом?

277 Что такое WAF? Напишите расшифровку аббревиатуры.

278 Что такое IPS? Напишите расшифровку аббревиатуры.

279 Что из перечисленного ниже может рассматриваться в качестве замены (альтернативы) для WAF?

280 Какой компонент присутствует в модели доступа 3 Tire, но отсутствует в модели доступа 2 Tire?

281 Как называется атака, при которой злоумышленник внедряет в страницу код, исполняемый в браузере жертвы?

282 Как называется атака, при которой злоумышленник вводит код на языке баз данных, исполняемый на стороне сервера?

283 Как называется атака, при которой злоумышленник кроме технических средств использует также методы социальной инженерии?

284 В каком виде получает информацию WAF, работающий в режиме аудита?

285 Выберите модель защиты WAF и правильное описание к ней.

286 Что относится к веб-приложениям?

287 Чем централизованная антивирусная проверка веб-трафика лучше использования антивирусного ПО, установленного на компьютерах пользователей?

288 Расположите устройства в порядке прохождения трафика через них по направлению из Интернет к базе данных: граничный маршрутизатор, сервер, NGFW, WAF.

289 Поставьте в соответствие модель защиты WAF и описание.

290 Поставьте в соответствие название атаки и её описание.

291 Какой протокол используется для передачи электронной почты между почтовыми серверами?

292 Какой протокол используется клиентом для получения почты с помощью почтового клиента?

293 Какой протокол используется клиентом для доступа к почте с помощью браузера?

294 Выберите правильное утверждение.

295 Какой тип записи в DNS обычно используется для определения почтовых серверов, отвечающих за домен?

296 С помощью какой команды протокола SMTP современный клиент идентифицирует себя?

297 Как производится проверка существования домена отправителя электронного письма?

298 К DNS записи какого типа необходимо обратиться при выполнении проверки SPF?

299 К DNS записи какого типа необходимо обратиться при выполнении проверки DKIM?

300 На чём основана атака SMTP smuggling?

301 В чём преимущество для компании, если антивирусная (антифишинговая, антиспам и т.д.) проверка почты выполняется централизованно на шлюзе или SMTP-сервере, а не только средствами антивируса на ПК пользователя?

302 Перед вами пример части DKIM-записи из электронного письма сотрудника нашего Университета. С помощью какой команды можно получить открытый ключ для проверки подписи данного письма? DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=synergy.ru; s=default; t=1707573465; x=1709387866.

303 Вы работаете почтовым администратором в компании. Один из сотрудников обратился к Вам с вопросом о том, что у него не работает отправка почты через наши почтовые сервера и он подозревает, что проблема в том, что во время SMTP-сессии сервер возвращает клиенту код 354. В чём может быть источник проблемы?

304 Какой протокол может использоваться для шифрования электронной почты при передаче?

305 Какая из команд протокола SMTP может использоваться несколько раз за время отправки клиентом электронного письма?

306 Какая команда используется в протоколе SMTP для уведомления противоположной стороны об окончании передачи электронного письма.

307 Как называется узел, входящий в цепочку пересылки электронной почты, и не являющийся почтовым сервером?

308 С помощью какой команды протокола SMTP отправитель извещает почтовый сервер о начале передачи тела электронного письма?

309 Расположите следующие команды в порядке, в котором они появляются в рамках SMTP сессии: rcpt to, data, mail from, ehlo.

310 Вы работаете сетевым администратором в нашем ВУЗе. В логах DNS-сервера, авторитетного для зоны synergy.ru Вы видите запросы с некоторого стороннего сервера электронной почты о TXT-записях для самого домена и некоторых поддоменов. Поставьте в соответствие перечисленные в логах домены и технологии защиты электронной почты, в рамках которых с наибольшей вероятностью производилась проверка.

311 Ваш почтовый клиент поддерживает работу нескольких почтовых протоколов. Поставьте в соответствие название протокола и направление передачи почты.

312 Что такое пассивный интерфейс в OSPF?

313 Какой максимально безопасный метод аутентификации в OSPF?

314 В чём суть seq++ атаки на OSPF?

315 Что такое unnumbered-интерфейс?

316 Какой транспортный протокол используется BGP?

317 Что из перечисленного ниже относится к механизмам аутентификации в BGP?

318 Какова основная цель использования механизмов TTL-security в BGP?

319 С какой целью оператор устанавливает ограничение на количество префиксов, принимаемых от клиента по BGP?

320 В чём смысл защиты с использованием IRR?

321 В чём смысл атаки LSA flooding?

322 Вы снимаете разнообразную статистику с маршрутизаторов в сети. В какой-то момент Вы замечаете, что начался резкий рост счётчика OspfSpfRuns и он продолжается в течение длительного времени. В чём может быть наиболее вероятная причина такого роста?

323 С помощью какого механизма можно преодолеть «расщепление горизонта» в BGP?

324 Анатолий пытается разобраться в том, как работает TTL Security в BGP и занимается подсчетами вручную. Между двумя BGP-маршрутизаторами находится четыре L3-устройства. Какое максимальное значение поля TTL могут увидеть указанные маршрутизаторы в сообщениях друг от друга?

325 Что является этапами внедрения RPKI?

326 Укажите номер TCP-порта, который используется для установления соединения.

327 В блоки данных какого протокола помещаются сообщения OSPF?

328 Какой вспомогательный протокол используется протоколами динамической маршрутизации OSPF и BGP для ускорения детектирования непрямых (indirect) отказов?

329 Какие модели внедрения RPKI поддерживает RIPE?

330 Сопоставьте термины из правого столбца с протоколами динамической маршрутизации из левого.

331 Запишите в порядке возрастания значений AD следующие протоколы динамической маршрутизации (значения AD считать по принятым в Cisco): iBGP, eBGP, OSPF.

332 Запишите в порядке возрастания безопасности методы аутентификации в OSPF: plain text, MD5, none.

333 С чем связано ограничение на количество записей IP route records в пакете? Укажите ответ в именительном падеже.

334 Какое максимальное количество IP route records может быть в пакете?

335 Путь, отображаемый утилитой tracert, ограничен тридцатью хопами. Вы можете написать свою собственную утилиту tracert, сняв ограничение в тридцать хопов. Какое максимальное количество хопов могла бы отображать Ваша утилита, работающая по тому же принципу, что и стандартный tracert (traceroute)?

336 Что такое white list?

337 Что лежит в основе атаки Ping of Death?

338 Что лежит в основе атаки TearDrop?

339 Какова наиболее вероятная причина использования злоумышленником маршрутизации от источника?

340 Что может стать узлом ботнет?

341 Какой тип DDoS атак может быть подавлен непосредственно на площадке заказчика с использованием специализированного оборудования, но без привлечения услуг провайдера или иных компаний?

342 В чём суть защиты от атаки SYN flood с помощью SYN cookie?

343 Что означает «DNS amplification»?

344 При какой атаке рассылается сообщение ICMP echo request на широковещательный адрес подсети?

345 При какой атаке злоумышленник отправляет специально подготовленные сегменты TCP, в которых порт отправителя совпадает с портом получателя, а значение IP-адреса получателя совпадает с IP-адресом отправителя?

346 Как называется компьютерная сеть, состоящая из некоторого количества хостов с запущенным автономным программным обеспечением. Чаще всего на узлах находится программа, скрытно установленная на устройство жертвы и позволяющая злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера?

347 Что лежит в основе атак Smurf и Fraggle?

348 Каково максимальное смещение фрагмента допустимо в IPv4-сетях?

349 Как называется механизм, позволяющий запретить принимать пакеты, если маршрут на отправителя этих пакетов лежит не через тот интерфейс, через который они были получены?

350 Для чего брандмауэры выполняют сборку пакетов из фрагментов?

351 Кто такие скрипт-кидди (script kiddie)?

352 В заголовке пакета протокола IPv6 отсутствуют опции. Что используется вместо них?

353 Что такое BGP FlowSpec?

354 Что (как и BGP FlowSpec) используется для фильтрации трафика в сети оператора?

355 Поставьте в соответствие название атаки и ее описание.

356 Расположите протоколы динамической маршрутизации в порядке возрастания AD (с точки зрения Cisco): RIPv2, OSPF, iBGP, eBGP.

357 Злоумышленник хочет использовать DNS-amplification, для чего формирует особым образом запросы к DNS-серверам. Вне зависимости от длины запроса ответ, возвращаемый DNS-сервером, имеет фиксированную длину. Расположите домены, для которых злоумышленник отправляет запрос, в порядке увеличения КПД атаки: synergy.ru, mail.ru, yandex.ru.

358 Что такое пассивный интерфейс в OSPF?

359 Какой максимально безопасный метод аутентификации в OSPF?

360 В чём суть seq++ атаки на OSPF?

361 Что такое unnumbered-интерфейс?

362 Какой транспортный протокол используется BGP?

363 Что из перечисленного ниже относится к механизмам аутентификации в BGP?

364 Какова основная цель использования механизмов TTL-security в BGP?

365 С какой целью оператор устанавливает ограничение на количество префиксов, принимаемых от клиента по BGP?

366 В чём смысл защиты с использованием IRR?

367 В чём смысл атаки LSA flooding?

368 Вы снимаете разнообразную статистику с маршрутизаторов в сети. В какой-то момент Вы замечаете, что начался резкий рост счётчика OspfSpfRuns и он продолжается в течение длительного времени. В чём может быть наиболее вероятная причина такого роста?

369 С помощью какого механизма можно преодолеть «расщепление горизонта» в BGP?

370 Как работает механизм uRPF?

371 В некотором OSPF домене ABR настроен таким образом, что в магистральную зону отдаёт единственный агрегированный префикс (вместо множества мелких). В чём преимущество такого подхода?

372 С какой целью используют списки доступа (ACL), разрешающие подключение к порту TCP-179 только с определённых IP-адресов, если сам BGP-протокол не позволит установить BGP-сессию с произвольным адресом?

373 От каких атак может защитить использование RPKI совместно с BGP?

374 Анатолий пытается разобраться в том, как работает TTL Security в BGP и занимается подсчетами вручную. Между двумя BGP-маршрутизаторами находится четыре L3-устройства. Какое максимальное значение поля TTL могут увидеть указанные маршрутизаторы в сообщениях друг от друга?

375 Укажите номер TCP-порта, который используется для установления соединения.

376 Что из перечисленного ниже должно выполняться при валидации ROA?

377 В каком статусе может оказаться префикс в результате проверки?

378 Сопоставьте термины из левого столбца с протоколами динамической маршрутизации из правого.

379 Запишите в порядке возрастания значений AD следующие протоколы динамической маршрутизации (значения AD считать по принятым в Cisco): iBGP, eBGP, OSPF.

380 Запишите в порядке возрастания безопасности методы аутентификации в OSPF: plain text, MD5, none.

381 Какое количество корневых центров сертификации существует на данный момент?

382 Каким образом операционная система изначально получает список доверенных корневых центров сертификации?

383 Как коротко называется список отозванных сертификатов?

384 В чём состоит основной недостаток использования CRL?

385 Чей сертификат обычно имеет самый длительный период валидности? Укажите ответ в именительном падеже.

386 Может ли сертификат конечного устройства быть заменён раньше окончания срока его действия?

387 Может ли электронный сертификат выдаваться строго для определённых целей? Ответ да/нет.

388 Для чего используются электронные подписи в сертификате (fingerprints)?

389 Может ли маршрутизатор Cisco встраиваться в цепочку доверия с корневым центром сертификации, работающим под управлением операционной системы MS Windows?

390 Для чего может использовать сертификаты site-to-site IPSec VPN?

391 С помощью какой команды клиентский маршрутизатор Cisco (с настроенным trustpoint) устанавливает отношения доверия с PKI-сервером?

392 Какой протокол является альтернативой CRL?

393 Для корректного функционирования PKI инфраструктуры критически важно наличие синхронизации времени. По какому протоколу это можно сделать?

394 При генерации ключей часто используется опция modulus. За что она отвечает?

395 Что выполняет функция grant?

396 Какой вариант детализации при заполнении базы выданных сертификатов отсутствует в настройках PKI-сервера на маршрутизаторе Cisco?

397 Какая информация сохраняется в базе сервера PKI при выборе режима детализации «names»?

398 Вы добавляете новый маршрутизатор (с рекомендованным в данном курсе ПО) в существующую PKI инфраструктуру. При выполнении процедуры authenticate отображаются две контрольные суммы для валидации сервера PKI. Какой из перечисленных ниже алгоритмов расчёта контрольных сумм входит в указанную пару?

399 Какую длину имеет хэш-сумма MD5?

400 Какую длину имеет хэш-сумма RSA-1?

401 Укажите одну из двух причин, по которой сертификат может быть удален из CRL.

402 Поставьте в соответствие название хэш-суммы в левом столбце и её длину из правого столбца.

403 Запишите в порядке возрастания время жизни следующих сущностей: сертификат ресурса, сертификат промежуточного центра сертификации, сертификат корневого центра сертификации, CRL.

404 Поставьте в соответствие высказывание из левого столбца методу проверки отозванных сертификатов из правого столбца.

405 Что не является недостатком режима настройки IPSec с использованием криптографических карт?

406 В какой фазе установления IPSec соединения используется протокол ISAKMP? Ответ укажите цифрой

407 Какова минимальная длина заголовка протокола GRE?

408 С помощью параметра transform-set можно выбрать режим работы IPSec-соединения. Какие два режима поддерживаются?

409 Какой алгоритм сжатия данных поддерживается в IPSec?

410 При настройке VTI IPSec как режим работы туннельного интерфейса должен быть выбран?

411 Какой алгоритм шифрования данных не поддерживается в ISAKMP сессии (на том оборудовании, которое используется в курсе)?

412 Для чего в одну криптокарту добавляют несколько записей?

413 Что не является преимуществом подхода GRE over IPSec по сравнению с традиционными криптокартами?

414 В чём особенность настройки списков доступа (ACL) для отбора «интересного» трафика при использовании криптокарт?

415 Чем отличается настройка IPSec VTI от настройки традиционного IPSec с использованием криптокарт?

416 В какой ситуации наиболее вероятно использование сертификата для аутентификации, а в какой разделяемого секрета (pre-shared key)?

417 Что наиболее точно описывает работу группы Диффи-Хэллмана?

418 Что из перечисленного ниже верно описывает разницу между первой и второй версиями протокола IKE?

419 Что из перечисленного ниже не является компонентом IPSec?

420 Возможно ли AH использовать в туннельном режиме? Ответ да/нет.

421 Может ли IPSec с ESP передавать данные открытым? Ответ да/нет.

422 Какое минимальное количество байт добавляется к пакету при стандартной GRE инкапсуляции?

423 В какой транспортный протокол может инкапсулироваться IPSec?

424 Что относят к недостаткам IPSec?

425 Что из перечисленного ниже не является задачей, решаемой семейством протоколов IPSec?

426 Поставьте в соответствие характеристику работы протокола из левого столбца протоколу из правого столбца?

427 Запишите алгоритмы шифрования, упорядочив их от самых слабых до наиболее криптостойких: AES, DES, 3DES.

428 Запишите режимы настройки IPSec, упорядочив их по времени появления: VTI, GRE over IPSec и IPSec with crypto-maps.

429 Какой протокол используется для связи между прокси-сервером и сервером антивирусной защиты?

430 Корпоративный пользователь просматривает разнообразные ресурсы в Интернет со своего рабочего места. При посещении большинства страниц браузер отображает предупреждение о проблемах с сертификатом сайта. Какова наиболее вероятная причина появления таких предупреждений?

431 С помощью какого режима работы ICAP прокси-сервер передает идущий от пользователя в Интернет-трафик на модуль антивирусной защиты?

432 С помощью какого режима работы ICAP прокси-сервер передает идущий из сети Интернет в сторону пользователя трафик на модуль антивирусной защиты?

433 Что такое межсайтовый скриптинг (XSS-атаки)?

434 Что такое атака нулевого дня (zero day)?

435 Что из перечисленного ниже является HTTP-запросом?

436 Что такое WAF? Напишите расшифровку аббревиатуры.

437 Что такое IPS? Напишите расшифровку аббревиатуры.

438 Что из перечисленного ниже может рассматриваться в качестве замены (альтернативы) для WAF?

439 Какой компонент присутствует в модели доступа 3 Tire, но отсутствует в модели доступа 2 Tire?

440 Как называется атака, при которой злоумышленник внедряет в страницу код, исполняемый в браузере жертвы?

441 Как называется атака, при которой злоумышленник вводит код на языке баз данных, исполняемый на стороне сервера?

442 Как называется атака, при которой злоумышленник кроме технических средств использует также методы социальной инженерии?

443 В каком виде получает информацию WAF, работающий в режиме аудита?

444 Выберите модель защиты WAF и правильное описание к ней.

445 Что относится к веб-приложениям?

446 Чем централизованная антивирусная проверка веб-трафика лучше использования антивирусного ПО, установленного на компьютерах пользователей?

447 Где обычно располагают WAF в корпоративной сети при использовании on-premise подхода?

448 Могут ли функции WAF и балансировщика трафика быть совмещены на одном устройстве?

449 Могут ли функции WAF и SSL decrypt быть совмещены на одном устройстве?

450 Какова основная причина успешности атак SQL injection?

451 Что такое фишинговая ссылка?

452 Что из перечисленного ниже позволит снизить необходимость в использовании WAF?

453 Расположите устройства в порядке прохождения трафика через них по направлению из Интернет к базе данных: граничный маршрутизатор, сервер, NGFW, WAF.

454 Поставьте в соответствие модель защиты WAF и описание.

455 Поставьте в соответствие название атаки и ее описание.

456 Какой протокол используется для передачи электронной почты между почтовыми серверами?

457 Какой протокол используется клиентом для получения почты с помощью почтового клиента?

458 Какой протокол используется клиентом для доступа к почте с помощью браузера?

459 Выберите правильное утверждение.

460 Какой тип записи в DNS обычно используется для определения почтовых серверов, отвечающих за домен?

461 С помощью какой команды протокола SMTP современный клиент идентифицирует себя?

462 Как производится проверка существования домена отправителя электронного письма?

463 К DNS записи какого типа необходимо обратиться при выполнении проверки SPF?

464 К DNS записи какого типа необходимо обратиться при выполнении проверки DKIM?

465 На чём основана атака SMTP smuggling?

466 В чём преимущество для компании, если антивирусная (антифишинговая, антиспам и т.д.) проверка почты выполняется централизованно на шлюзе или SMTP-сервере, а не только средствами антивируса на ПК пользователя?

467 Перед вами пример части DKIM-записи из электронного письма сотрудника нашего Университета. С помощью какой команды можно получить открытый ключ для проверки подписи данного письма? DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=synergy.ru; s=default; t=1707573465; x=1709387866.

468 Вы работаете почтовым администратором в компании. Один из сотрудников обратился к Вам с вопросом о том, что у него не работает отправка почты через наши почтовые сервера и он подозревает, что проблема в том, что во время SMTP-сессии сервер возвращает клиенту код 354. В чём может быть источник проблемы?

469 Какой протокол может использоваться для шифрования электронной почты при передаче?

470 Вы получили письмо от ректора. Какой из перечисленных ниже адресов отправителя вызывает меньше всего доверия как принадлежащий ректору нашего Университета?

471 Для чего используется бесплатный сервис DNSBL?

472 Что из перечисленного ниже не является политикой DMARC?

473 Какая из команд протокола SMTP может использоваться несколько раз за время отправки клиентом электронного письма?

474 В каком виде можно указывать разрешённые сервера в SPF-записи?

475 Системы защиты электронной почты проверяют не только входящие письма, но и исходящие. Какова наиболее вероятная цель такой проверки?

476 Какая команда используется в протоколе SMTP для уведомления противоположной стороны об окончании передачи электронного письма.

477 Как называется узел, входящий в цепочку пересылки электронной почты, и не являющийся почтовым сервером?

478 С помощью какой команды протокола SMTP отправитель извещает почтовый сервер о начале передачи тела электронного письма?

479 Расположите следующие команды в порядке, в котором они появляются в рамках SMTP сессии: rcpt to, data, mail from, ehlo.

480 Вы работаете сетевым администратором в нашем ВУЗе. В логах DNS-сервера, авторитетного для зоны synergy.ru Вы видите запросы с некоторого стороннего сервера электронной почты о TXT-записях для самого домена и некоторых поддоменов. Поставьте в соответствие перечисленные в логах домены и технологии защиты электронной почты, в рамках которых с наибольшей вероятностью производилась проверка.

481 Как формируется значение BID коммутатора без использования опции Extended System ID? Ответ запишите в виде x/y, где x – длина Bridge Priority в байтах, а y – длина MAC-адреса коммутатора в байтах.

482 Как формируется значение BID коммутатора при использовании опции Extended System ID? Ответ запишите в виде x/y/z, где x – длина Bridge Priority в битах, y – длина Extended System ID в битах, а z – длина MAC-адреса коммутатора в битах.

483 Какой виртуальной сети (VLAN ID) соответствует следующее значение BID коммутатора - 8315?

484 Какую цель преследует злоумышленник при выполнении атаки Eternal Election Attack?

485 Какую цель преследует злоумышленник при выполнении атаки Root Disappearance Attack?

486 Какую цель преследует злоумышленник при выполнении атаки Merging-splitting of the trees?

487 Злоумышленник подключен к одному порту коммутатора доступа. Что из перечисленного ниже поможет защититься от любых STP-атак с его стороны?

488 Что из перечисленного ниже может помочь против атак, связанных с перевыборами корневого коммутатора?

489 Как называется BPDU, в котором содержится меньшее значение Rood ID?

490 Каково значение таймера forwarding delay по умолчанию в классическом протоколе STP?

491 Как влияет событие изменение топологии в протоколе STP на время жизни записей в таблице коммутации?

492 На таблицы коммутации каких коммутаторов влияет событие изменения топологии в протоколе STP?

493 Какая версия протокола STP позволяет построить несколько деревьев, соответствующих независимым топологиям (обычно больше одного, но меньше количества существующих виртуальных сетей (VLAN))?

494 Какая версия протокола STP строит столько деревьев, сколько используется виртуальных сетей (VLAN)?

495 Какая версия протокола STP всегда строит одно единственное деревно вне зависимости от количества виртуальных сетей (VLAN)?

496 Каково значение hello таймера по умолчанию в классическом протоколе STP?

497 Как называется опция, позволяющая заблокировать передачу или приём STP BPDU через определённый интерфейс коммутатора?

498 Как называется опция, позволяющая заблокировать интерфейс коммутатора, если через него было получено любое сообщение STP BPDU?

499 Как называется опция, позволяющая заблокировать интерфейс коммутатора, если через него было получено superior сообщение STP BPDU?

500 Понятиям, технологиям, оптимизациям в левом столбце поставьте в соответствие протоколу, который указан в правом столбце?

501 Ролям портов коммутатора из левого столбца поставьте в соответствие версию протокола STP из правого столбца?

502 Коммутатор работает в режиме классического STP 802.1D. Расставьте статусы интерфейса, через которые пройдёт порт, в соответствующем порядке, если к нему подключают какое-либо устройство: Blocking, Learning, Listening, Forwarding?

503 Позволяет ли переход от концентраторов к коммутаторам в локальных сетях полностью избавиться от прослушивания сети злоумышленником?

504 Какую информацию может предоставить кабельный тестер?

505 Системный администратор подключила свой ноутбук к сетевому устройству с надписью Switch на лицевой панели с помощью прямого патч-корда и увидела, что с помощью Auto MDI/MDIX у неё определились следующие параметры работы среды: 100 FX. Может ли она утверждать, что устройство, к которому она подключилась, - коммутатор? Что на это указывает?

506 В процессе своей работы коммутатор обучается (learning) на проходящем трафике. Что используется для заполнения мостовой таблицы?

507 Какой механизм позволяет ограничить количество изученных MAC-адресов на порту коммутатора?

508 Какой механизм позволяет защититься от атак с использованием rogue DHCP-сервер?

509 Что такое native-VLAN (выберите максимально подходящий ответ)?

510 На что направлена атака DHCP starvation?

511 В чём смысл атаки ARP spoofing?

512 В чём смысл атаки ARP flooding?

513 С помощью какого механизма DHCP-сервер может узнать, к какому порту какого коммутатора подключен DHCP-клиент?

514 С помощью какого протокола злоумышленник может узнать подробную информацию о коммутаторе, к которому подключен?

515 С помощью какого протокола злоумышленник может удалить всю информацию о виртуальных сетях (VLAN) с коммутаторов?

516 С помощью какого протокола можно провести аутентификацию подключаемого к сети устройства?

517 С помощью какого пассивного устройства можно получить копию трафика, передаваемого через оптический канал?

518 Какое сообщение используется маршрутизатором в протоколе NDP для сообщения о себе, то есть, например, для объявления о том, что данный маршрутизатор можно использовать для выхода из сегмента сети?

519 При проведении атаки DHCP starvation появление какого из перечисленных сообщений протокола DHCP не ожидается: Discover, Offer, Request, Release?

520 Какой механизм может использоваться для подавления атаки ARP flooding?

521 Для подавления какой атаки может использоваться механизм uRPF?

522 Какое устройство вставляет опцию №82 в сообщение протокола DHCP?

523 Упорядочите уровни модели OSI (снизу вверх): канальный, физический, транспортный, сетевой.

524 Поставьте в соответствие названия устройств из левого столбца уровням модели OSI из правого столбца.

525 Укажите сообщения протокола DHCP в порядке их появления в сети в процессе стандартного получения хостом IP-адреса: Offer, Discover, Ack, Request.

526 Поставьте понятию из левого столбца в соответствие уровень модели OSI из правого столбца.

527 На ваш компьютер пришло сообщение о необходимости пройти тест по курсу компьютерных сетей. Укажите, в какой последовательности при декапсуляции данных будут анализироваться заголовки уровней модели OSI? Ответ приведите для следующего набора уровней: сетевой, канальный, транспортный.

528 Какое(ие) из перечисленных устройств является(ются) устройством(ами) канального уровня модели OSI? Выберите все верные ответы.

529 Какое(ие) из перечисленных устройств является(ются) устройством(ами) сетевого уровня модели OSI? Выберите все верные ответы.

530 Какое(ие) из перечисленных устройств является(ются) устройством(ами) транспортного уровня модели OSI? Выберите все верные ответы.

531 Укажите протоколы транспортного уровня модели OSI. Выберите все верные ответы.

532 В каком(их) из перечисленных протоколов блоки данных имеют не только заголовок, но и концевик?

533 Укажите, какое количество соединений необходимо для построения полносвязанной топологии из 5 устройств?

534 Укажите, какое количество соединений необходимо для построения полносвязанной топологии из 10 устройств?

535 Как называется система, которая в одном месте хранит информацию о том, какие сети для каких целей использованы, какие в этих сетях ресурсы, сколько адресов выдано (какой % утилизации адресного пространства в той или иной подсети)?

536 Клиент отправляет широковещательно сообщение Discover. Наш роутер, на котором настроена функция X, перехватывает это сообщение, сам его не обрабатывает, а отправляет на адрес сервера. Сервер это сообщение обрабатывает, понимает, из какого сегмента пришел запрос, смотрит пул адресов, который соответствует этому сегменту, и отправляет ответ (то есть происходит стандартная процедура получения IP-адреса). Другими словами, роутер «прикидывается» DHCP-сервером, а в реальности пересылает запрос дальше. Укажите, о какой функции протокола DHCP идет речь

537 Может ли роутер (в частности, ваш домашний Wi-Fi роутер) выполнять функции DHCP-сервера? В ответе укажите только да или нет.

538 Как может выглядеть MAC-адрес отправителя широковещательного фрейма? Выберите все верные ответы.

539 Выберете флаг протокола TCP, указывающий на важность = передаются ли в нашем сегменте какие-то важные данные. Если этот флаг поднят, то мы (принимающая сторона) обращаем внимание на поле Urgent point, которое показывает границы важных данных. Если этот флаг опущен, то на поле Urgent point мы, соответственно, смотреть не будем.

540 Выберете флаг протокола TCP, который говорит получателю о том, что принятые данные нужно не хранить в буфере, а как можно быстрее передать приложению.

541 Выберете флаг(и) протокола TCP, который(ые) используется(ют) для того, чтобы закрыть TCP-сессию

542 На рисунке ниже приведен пример статической NAT-трансляции. Узел B решил ответить на сообщение, полученное от узла A. Укажите, какой IP-адрес укажет узел B в качестве адреса получателя пакета.

543 На рисунке ниже приведен пример статической NAT-трансляции. Узел B решил ответить на сообщение, полученное от узла A. Укажите, какой IP-адрес укажет узел B в качестве адреса отправителя пакета.

544 На рисунке ниже приведен пример статической NAT-трансляции. Узел B решил ответить на сообщение, полученное от узла A. Укажите, какой IP-адрес будет в поле «IP-адрес получателя», когда ответ узла B придет на роутер R1.

545 Сопоставьте поля заголовков протоколов и протоколы, в которых они используются

546 Расположите протоколы Ethernet, IP, UDP в порядке возрастания уровня модели OSI, на котором расположен соответствующий протокол?

547 На рисунке ниже приведен пример динамической PAT-трансляции. Сервер 9.9.9.9 решил ответить на сообщение, полученное от узла A. Укажите, какой TCP-порт будет в поле «TCP-порт отправителя», когда ответ узла B окажется в левой части сети (то есть после обработки роутером R1). В ответе укажите только номер порта.

548 Какова длина ключа для протокола симметричного шифрования DES (в битах)?

549 Какая длина блока используется при шифровании с помощью протокола DES?

550 В чем содержится «весь секрет» алгоритмов симметричного шифрования?

551 Какой параметр алгоритма шифр Цезаря можно назвать ключом шифрования?

552 Какая суммарная длина ключей в алгоритме шифрования 3DES (в битах)?

553 Какие цели преследует нарушитель, пытаясь взломать алгоритм симметричного шифрования?

554 Как называется статистическая зависимость между исходным и зашифрованным сообщением?

555 Используется ли ключ шифрования при начальной и конечной перестановках (Initial Permission) в алгоритме DES?

556 Как называются алгоритмы, которые разбивают сообщение на блоки определенной длины, и шифруют отдельный блок?

557 Использует ли алгоритм симметричного шифрования DES классическую сеть Фейштеля? (В ответе укажите только да или нет)

558 Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?

559 Укажите количество раундов в алгоритме симметричного шифрования DES (В ответе укажите только число).

560 Что в криптографии называют открытым текстом?

561 Укажите, число S-боксов (блоков), используемых в алгоритме симметричного шифрования DES

562 Укажите длину ключа раунда для протокола DES в битах

563 Сколько ветвей в сети Фейстеля в протоколе DES?

564 Требуется ли при шифровании с помощью алгоритмов, использующих сеть Фейстеля, обратимость функции F в сети Фейстеля? (В ответе укажите только да или нет)

565 До какой длины (в битах) расширяется во время раунда шифрования правая ветка сети Фейстеля в алгоритме DES?

566 Установите соответствие между алгоритмами симметричного шифрования и длинами ключей

567 Расположите алгоритмы симметричного шифрования 3DES, DES, AES в порядке возрастания их криптографической стойкости

568 Изучите структуру функции расширения для алгоритма симметричного шифрования DES. Выпишите номера бит, полученные в первой строке после применения функции расширения (получается таблица из 8 строк, по 6 бит в каждой), если считать, что изначально все биты были занумерованы от 1 до 32. В ответе укажите номера бит без пробелов.

569 Какая может быть длина ключа для протокола симметричного шифрования AES (в битах)? Выберите все правильные варианты

570 Какая длина блока используется при шифровании с помощью протокола AES?

571 В чем содержится «весь секрет» алгоритма симметричного шифрования AES?

572 В какой из 4 приведенных ниже операций раунда вводится понятие S-боксов в рамках алгоритма AES?

573 На какое количество элементов значения в таблице ниже сдвинутся влево в 0 строке при операции ShiftRows алгоритма AES?

574 На какое количество элементов значения в таблице ниже сдвинутся влево в 1 строке при операции ShiftRows алгоритма AES?

575 На какое количество элементов значения в таблице ниже сдвинутся влево во 2 строке при операции ShiftRows алгоритма AES?

576 Какой блочный режим шифрования иллюстрирует данная схема? (В ответе можно указать аббревиатуру/полное название)

577 Использует ли алгоритм симметричного шифрования AES классическую сеть Фейстеля? (В ответе укажите только да или нет)

578 На какое количество элементов значения в таблице ниже сдвинутся влево в 3 строке при операции ShiftRows алгоритма AES?

579 Укажите количество раундов в алгоритме симметричного шифрования AES при использовании длины ключа и длины блока 128 бит? (В ответе укажите только число).

580 Выберите, какие операции используются в алгоритмах симметричного шифрования?

581 Укажите количество раундов в алгоритме симметричного шифрования AES при использовании длины ключа 192 бита и длины блока 128 бит? (В ответе укажите только число).

582 Укажите количество раундов в алгоритме симметричного шифрования AES при использовании длины ключа 192 бита и длины блока 128 бит? (В ответе укажите только число).

583 Какой блочный режим шифрования иллюстрирует данная схема? (В ответе можно указать аббревиатуру/полное название)

584 Требуется ли обратимость преобразований, выполняемых во время раунда в протоколе симметричного шифрования AES? (В ответе укажите только да или нет)

585 Расположите функции раунда, используемые в алгоритме AES – AddRoundKey, MixColomns, ShiftRows, SubBytes, в том порядке, в котором они применяются во время раунда шифрования.

586 Изучите описание, предложенное ниже и определите, о каком режиме шифрования блоков идет речь. В ответе можно указать аббревиатуру/полное название. Преимущество данного режима заключается в том, что в случае потери пакета при транспорте от отправителя к получателю ничего страшного не произойдет – следующий пакет расшифруется. Однако мы теряем в безопасности, потому что в хвост регистра мы фактически помещаем зашифрованный исходный текст, и можно попытаться перебрать ключи

587 Какой(ие) сервис(ы) безопасности реализован(ы) на схеме ниже?

588 Какой(ие) сервис(ы) безопасности реализован(ы) на схеме ниже?

589 Какой(ие) сервис(ы) безопасности реализован(ы) на схеме ниже?

590 В каком алгоритме асимметричного шифрование секрет шифруется по схеме, предложенной ниже?

591 В каком алгоритме асимметричного шифрование секрет расшифровывается по схеме, предложенной ниже?

592 В каком алгоритме асимметричного шифрование ключ сессии вырабатывается (передается) по схеме, предложенной ниже?

593 Логика вычисления открытого и закрытого ключа какого протокола асимметричного шифрования представлена ниже?

594 Какой алгоритм асимметричного шифрования основан на задаче факторизации числа?

595 Верно ли утверждение про алгоритмы асимметричного шифрования: легко вычислить пару (KU, KR). В ответе укажите только да или нет

596 Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно легко зашифровать сообщение, используя открытый ключ (KU). В ответе укажите только да или нет

597 Укажите, какой(ие) из предложенных алгоритмов асимметричного шифрования может(гут) использоваться для создания цифровой подписи?

598 Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно легко расшифровать сообщение, используя закрытый ключ (KR). В ответе укажите только да или нет

599 Укажите, какой(ие) из предложенных алгоритмов асимметричного шифрования может(гут) использоваться для обмена общим секретом?

600 Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно трудно, зная открытый ключ (KU), найти соответствующий ему закрытый ключ (KR). В ответе укажите только да или нет

601 Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно трудно, зная зашифрованное сообщение (C) и открытый ключ (KU), найти исходное сообщение (M). В ответе укажите только да или нет

602 .Верно ли утверждение про алгоритмы асимметричного шифрования: трудно вычислить пару (KU, KR). В ответе укажите только да или нет

603 Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно трудно зашифровать сообщение, используя открытый ключ (KU). В ответе укажите только да или нет

604 Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно легко, зная открытый ключ (KU), найти соответствующий ему закрытый ключ (KR). В ответе укажите только да или нет

605 Установите соответствие между столбцами слева и справа

606 Расположите алгоритмы симметричного шифрования 3DES, DES, AES в порядке возрастания их криптографической стойкости

607 В алгоритме асимметричного шифрования RSA p = 5, q = 7. Вычислите значение φ(n), n =pq. В ответе укажите только число.

608 Логика работы какой хеш-функции изображена на блок-схеме ниже?

609 Логика работы какой хеш-функции изображена на блок-схеме ниже?

610 Логика работы какой хеш-функции изображена на блок-схеме ниже?

611 Логика работы какой хеш-функции изображена на блок-схеме ниже?

612 Какой сервис безопасности иллюстрирует данное изображение?

613 Укажите хеш-функцию, в которой вычисления циклов происходят с использованием следующих функций?

614 Укажите длину хеш-кода для функции MD5 (в битах).

615 Входные регистры какой хеш-функции изображены на рисунке ниже?

616 Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции MD5.

617 Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции SHA-2 [256].

618 Укажите длины блоков, на которые разбивается сообщение для хеширования с помощью функции SHA-2 [512].

619 Укажите варианты длины хеш-кода для функции SHA-2 (Выберите все подходящие варианты)

620 Укажите длины блоков, на которые разбивается сообщение для хеширования с помощью функции SHA-2 [384].

621 Какая длина хеш-кода у функции SHA-1? (в битах).

622 Укажите наименьшую длину хеш-кода функции SHA-3? (в битах)

623 Укажите наибольшую длину хеш-кода для функции SHA-3 (в битах)

624 В какой хеш-функции используются преобразования, предложенные ниже? (В ответе запишите только название хеш-функции, например SHA-3)

625 Установите соответствие между хеш-функциями и длинами хеш-кодов этих функций

626 Расположите хеш-функции MD5, SHA-1, SHA-2 в порядке возрастания длины хеш-кода

627 Изучите описание, предложенное ниже, и определите, о какой хеш-функции идет речь. В ответе запишите только название хеш-функции, например SHA-1 Алгоритм основан на «принципе губки». Исходное сообщение делится на блоки; используется начальный вектор, который состоит из двух частей r и c. Выполняется XOR r-части с первым блоком, полученный результат и блок с подаются в функцию f и так до тех пор, пока не закончится сообщение. Это так называемая стадия «сжатия». Когда сообщение закончилось, начинается стадия «отжатия»: используется та же функция f, результат выдается до получения хэш-кода нужной длины.

628 Между какими уровнями модели OSI располагается заголовок протокола ESP?

629 Между какими уровнями модели OSI располагается заголовок протокола AH?

630 Целостность каких полей IP-заголовка может проверить протокол AH?

631 Укажите, между какими протоколами может быть расположен заголовок протокола ESP? Выберите все подходящие варианты.

632 Укажите, между какими протоколами может быть расположен заголовок протокола ESP? Выберите все варианты, которые могут быть использованы в разобранных на занятиях ситуациях

633 Укажите поля IP-заголовка, целостность которых не может проверить протокол AH?

634 Как называется упорядоченный набор записей, в котором содержится действие Action и параметры трафика? В ответе приведите только аббревиатуру данной базы данных на английском языке

635 Выберите стандарт формата сертификатов, который наиболее распространен на сегодняшний день?

636 Какой сервис безопасности может быть обеспечен протоколом ESP и принципиально не обеспечивается протоколом AH?

637 Укажите, Main mode или Aggressive mode используется при установления соединения в первой фазе на схеме установления соединения, изображенной ниже. В ответе укажите только Main mode/Aggressive mode

638 Укажите, Pre-shared secret или Сертификат используется для аутентификации в первой фазе на схеме установления соединения, изображенной ниже. В ответе укажите только Pre-shared secret/Сертификат

639 Укажите, Main mode или Aggressive mode при установлении соединения в первой фазе на схеме установления соединения, изображенной ниже. В ответе укажите только Main mode/Aggressive mode

640 Укажите, Pre-shared secret или Сертификат используется для аутентификации в первой фазе на схеме установления соединения, изображенной ниже. В ответе укажите только Pre-shared secret/Сертификат

641 Укажите, Main mode или Aggressive mode используется при установлении соединения в первой фазе на схеме установления соединения, изображенной ниже.. В ответе укажите только Main mode/Aggressive mode

642 Укажите, какой алгоритм (Main mode или Aggressive mode) используется при установлении соединения в первой фазе на схеме ниже. В ответе укажите только Main mode/Aggressive mode

643 Укажите, Pre-shared secret или Сертификат используется для аутентификации в первой фазе на схеме ниже. В ответе укажите только Pre-shared secret/Сертификат

644 На рисунке ниже приведена последовательность заголовков, которая предполагается в технологии GRE over IPSec. В каком режиме в данном случае работает IPSec: туннельном или транспортном? В ответе Укажите только режим: туннельный/транспортный.

645 Изучите описание, предложенное ниже, и определите протокол семейства IPSec, о котором идет речь. В ответе запишите только название протокола, например, ESP. Данный протокол используется для формирования IPSec SA, проще говоря, согласования работы участников защищенного соединения. Используя этот протокол, участники договариваются, какой алгоритм шифрования будет использоваться, по какому алгоритму будет производиться (и будет ли вообще) проверка целостности, как аутентифицировать друг друга

646 Укажите, над протоколами какого уровня модели TCP/IP расположен протокол Записи технологии SSL/TLS?

647 Укажите уровни модели TCP/IP, между которыми располагаются протоколы технологии SSL/TLS?

648 Конфиденциальность какого протокола можно обеспечить средствами технологии SSL/TLS?

649 Конфиденциальность какого протокола можно обеспечить средствами технологии SSL/TLS?

650 Конфиденциальность какого протокола можно обеспечить средствами технологии SSL/TLS?

651 Выберите протокол, конфиденциальность которого можно обеспечить средствами технологии SSL/TLS

652 Как называется упорядоченный набор записей, в котором содержится действие (Action) + параметры трафика? В ответе необходимо привести только аббревиатуру данной базы данных на английском языке

653 Выберите протокол, конфиденциальность которого обеспечить средствами технологии SSL/TLS

654 Укажите протокол асимметричного шифрования для формирования pre-master secret, который был исключен из технологии TLS 1.3 по сравнению с более ранней версией

655 Какое сообщение отправляется первым при установлении соединения между клиентом и сервером по технологии TLS?

656 Обязателен ли сертификат со стороны клиента при установке соединения по протоколу TLS? В ответе укажите только да или нет

657 Сколько раундов шифрования предусмотрено в алгоритме симметричного шифрования DES? (В ответе укажите только число).

658 Что в криптографии понимают под термином «открытый текст»?

659 Какое количество S-боксов (блоков), используется в алгоритме симметричного шифрования DES? (В ответе укажите только число)

660 Какова длина ключа раунда для протокола DES(ответ приведите в битах)

661 Укажите количество ветвей в сети Фейстеля в протоколе DES?

662 Какой размер (в битах) достигает правая половина блока данных в процессе одного раунда шифрования в алгоритме DES, когда она расширяется в сети Фейстеля?

663 Установите соответствие между версиями протокола TLS и состояниями данных версий

664 Что является этапами внедрения RPKI?

665 В блоки данных какого протокола помещаются сообщения OSPF?

666 Какой вспомогательный протокол используется протоколами динамической маршрутизации OSPF и BGP для ускорения детектирования непрямых (indirect) отказов?

667 Какие модели внедрения RPKI поддерживает RIPE?

668 Ваш почтовый клиент поддерживает работу нескольких почтовых протоколов. Поставьте в соответствие название протокола и направление передачи почты.