МОДУЛЬ 3. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕТИ

КАФЕДРА ТЕЛЕКОММУНИКАЦИЙ

3.1 ТЕКУЩИЙ УРОВЕНЬ КИБЕРБЕЗОПАСНОСТИ

3.1.1 ЗАЯВЛЕНИЕ ОБ ЭТИЧНОМ ХАКЕРСТВЕ

В этом модуле учащиеся могут познакомиться с инструментами и методами в “песочнице”, виртуальной машине с изолированной программной средой, чтобы продемонстрировать различные типы кибератак. Экспериментирование с этими с инструментами, методами и ресурсами осуществляются на усмотрение инструктора и учебного заведения. Если учащийся рассматривает возможность использования инструментов атаки в образовательных целях, он должен связаться со своим инструктором до начала любых экспериментов.

Несанкционированный доступ к данным, компьютерным и сетевым системам является преступлением в большинстве юрисдикций и обычно имеет серьезные последствия, независимо от мотивации правонарушителя. Студенты, пользующиеся этими материалами, несут ответственность за ознакомление с законами об использовании вычислительной техники и их соблюдение.

3.1.2 ТЕКУЩЕЕ СОСТОЯНИЕ ДЕЛ

Киберпреступники теперь обладают опытом и инструментами, необходимыми для уничтожения критически важной инфраструктуры и систем. Их инструменты и методы продолжают развиваться.

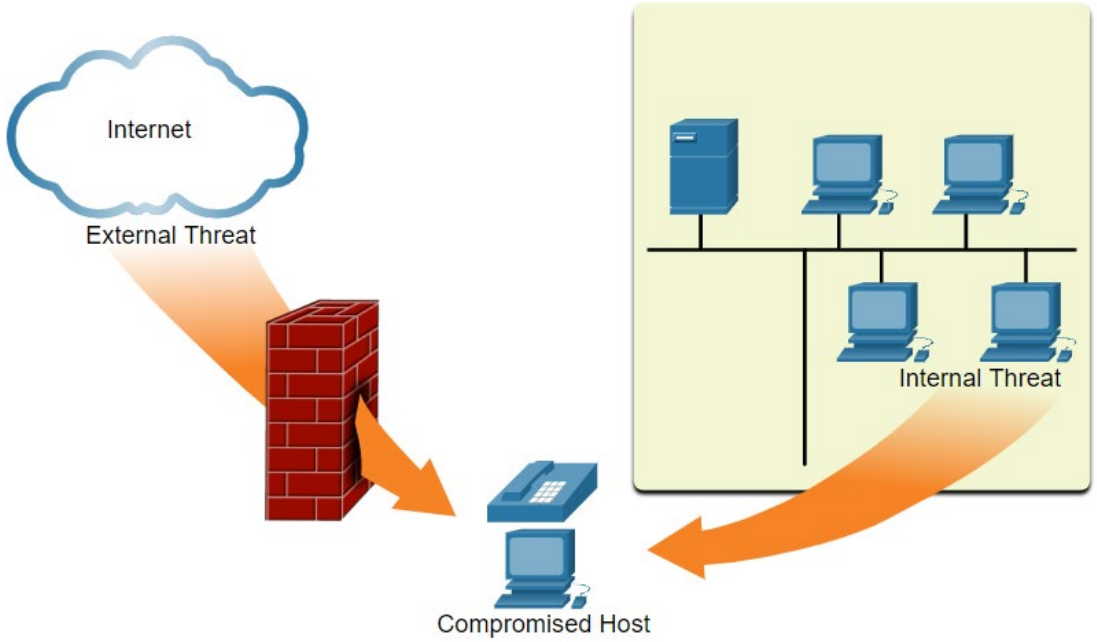
Поддержание сетевой безопасности обеспечивает защиту пользователей сети и коммерческих интересов. Все пользователи должны знать термины безопасности, представленные в таблице.

Термины в сфере безопасности	Описание
Ресурсы	Ресурс - это что-то ценное для организации. Он включает людей, оборудование и данные.
Уязвимость	Уязвимость - это слабое место в системе или ее архитектуре, которое может быть использовано злоумышленниками.
Угроза	Угроза - это потенциальная опасность для ресурсов, данных или сетевых функций компании.
Эксплойт	Эксплойт - механизм для использования уязвимости в целях взлома ресурса.
Устранение	Устранение является контрмерой, которая уменьшает вероятность или серьезность потенциальной угрозы или риска. Сетевая безопасность включает в себя несколько методов устранения.
Риски	Риск - вероятность угрозы использования уязвимости ресурсов с целью негативного воздействия на организацию. Риск определяет вероятность возникновения события и его последствия.

3.1.3 ВЕКТОРЫ СЕТЕВЫХ АТАК

Вектор атаки – это путь (или какой-либо другой способ), по которому злоумышленник проникает на сервер, хост или в сеть. Большинство векторов атак идут извне корпоративной сети, как показано на рисунке.

Ущерб, вызванный действиями внутренних пользователей, обладающих прямым доступом к зданию и его инфраструктуре, может оказаться значительно выше, чем от внешних угроз.



3.1.4 ПОТЕРЯ ДАННЫХ

Под потерей или утечкой данных подразумевается намеренная или ненамеренная потеря, кража или утечка данных во внешний мир. Потеря данных может привести к следующим последствиям:

- ущерб для бренда и репутации;

- потеря конкурентного преимущества;

- потеря заказчиков;

- потеря прибыли;

- разбирательства в суде/юридические последствия, которые могут привести к штрафам и административным санкциям;

- значительные затраты и усилия по уведомлению пострадавших сторон и восстановлению после утечки.

Специалисты по сетевой безопасности должны защищать данные организации. Необходимо внедрять различные техники предотвращения потери данных (Data Loss Prevention, DLP), которые бы включали в себя стратегические, операционные и тактические задачи.

3.1.4 ПОТЕРЯ ДАННЫХ

Векторы потери данных	Описание
Электронная почта/социальные сети	Из перехваченных сообщений электронной почты или мгновенных сообщений может быть извлечена конфиденциальная информация.
Незашифрованные устройства	Если для хранения данных не используется алгоритм шифрования, то злоумышленник получить ценные конфиденциальные данные.
Устройства облачного хранения данных	Конфиденциальные данные могут быть потеряны, если доступ к облаку будет скомпрометирован из-за слабых настроек безопасности.
Съемные носители	Одним из рисков также является то, что сотрудник может несанкционированным образом скопировать на USB-накопитель. Другой риск заключается в том, что USB-накопитель, содержащий ценные корпоративные данные, может быть потерян.
Бумажные носители	Конфиденциальные данные должны быть уничтожены, когда они больше не нужны.
Некорректное управление доступом	Украденные или ненадежные пароли, которые были скомпрометированы, могут предоставить злоумышленнику легкий доступ к корпоративным данным.

3.2 ЗЛОУМЫШЛЕННИКИ
3.2.1 ХАКЕР

Хакер - это общий термин, используемый для обозначения субъекта угрозы, злоумышленника.

Тип хакера	Описание
«Белые» хакеры	Это «белые» хакеры, которые используют свои навыки программирования в хороших, этических и законных целях. Они сообщают об уязвимостях системы обеспечения безопасности разработчикам, чтобы те исправили их, прежде чем кто-то мог бы ими воспользоваться.
«Серые» хакеры	«Серые» хакеры совершают преступления и, возможно, неэтичные поступки, но не в целях личной выгоды или в стремлении причинить ущерб. После проникновения в сеть организации «серые» хакеры могут сообщить пострадавшей организации об уязвимостях ее сетевой инфраструктуры.
«Черные» хакеры	«Черные» хакеры являются неэтичными преступниками, которые нарушают компьютерную и сетевую безопасность в целях личной выгоды или для нанесения вреда, например во время сетевых атак.

3.2.2 ЭВОЛЮЦИЯ ХАКЕРОВ

Таблица показывает современные хакерские термины и краткое описание каждого из них.

Типы хакеров	Описание
Хакеры-дилетанты	Этот термин относится к подросткам или неопытным хакерам, которые используют существующие сценарии, инструменты и эксплойты для нанесения вреда, но обычно не для получения прибыли.
Брокер уязвимостей	Брокерами уязвимостей являются обычно «серые» хакеры, которые пытаются обнаружить эксплойты и сообщить о них продавцам, иногда за вознаграждение.
Хактивисты	Это «серые» хакеры, которые публично протестуют против организаций или правительств, публикуя статьи, выпуская видеоролики, организуя утечки конфиденциальной информации и совершая распределенные атаки типа «отказ в обслуживании».
Киберпреступники	Это «черные» хакеры, которые работают либо на себя, либо на большую киберпреступную организацию.
Спонсируемые государством	Это «белые» или «черные» хакеры, которые крадут правительственные секреты, собирают разведывательные данные и саботируют сети. Их целью являются иностранные правительства, террористические группы и корпорации. Большинство стран мира в той или иной степени участвуют в хакерских атаках, спонсируемых государством.

3.2.3 КИБЕРПРЕСТУПНИКИ, ХАКТИВИСТЫ И СПОНСИРУЕМЫЕ ГОСУДАРСТВОМ ХАКЕРЫ

Предполагается, что в глобальном масштабе киберпреступники ежегодно крадут у потребителей и предприятий миллиарды долларов. Киберпреступники действуют в рамках теневой экономики, где они покупают, продают и обменивают эксплойты и инструменты. Они также покупают и продают личную информацию и интеллектуальную собственность, украденную у жертв. Целью киберпреступников являются малые предприятия и потребители, а также крупные предприятия и целые отрасли.

Два примера хактивистских групп - Анонимус и Сирийская Электронная Армия. Хотя большинство хактивистских групп недостаточно хорошо организованы, они могут вызвать серьезные проблемы для правительств и предприятий. Хактивисты склонны полагаться на довольно простые, свободно доступные инструменты.

Спонсируемые государством хакеры создают расширенный, настраиваемый код атаки, часто используя ранее обнаруженные уязвимости программного обеспечения, называемые уязвимостями нулевого дня. Примером спонсируемой государством атаки является вредоносное ПО Stuxnet, созданное для того, чтобы нанести ущерб возможностям обогащения ядерного топлива в Иране.

3.3 ИНСТРУМЕНТЫ ЗЛОУМЫШЛЕННИКОВ

3.3.1 ЗНАКОМСТВО С ИНСТРУМЕНТАМИ АТАК

Для того чтобы использовать уязвимость, хакеру необходим соответствующий метод или инструмент. За прошедшие годы инструменты атаки стали более сложными и высоко автоматизированными. Сейчас эти новые инструменты требуют все меньше технических знаний для их реализации.

В таблице на следующих слайдах представлены категории распространенных инструментов тестирования на возможность проникновения в сеть. Обратите внимание на то, что некоторые из указанных инструментов используются и «белыми» и «черными» хакерами.

3.3.2 ЭВОЛЮЦИЯ РЕШЕНИЙ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Инструменты тестирования на возможность проникновения.	**Описание**
Взломщики паролей	Инструменты взлома паролей часто рассматриваются как инструменты для восстановления пароля. С их помощью пароли можно взламывать или восстанавливать. Взломщики паролей используют циклический подбор для взлома паролей. В качестве примеров инструментов для взлома паролей можно привести John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack и Medusa.
Беспроводные средства взлома	Инструменты взлома беспроводных сетей используются для взлома беспроводных сетей с целью выявления уязвимостей системы безопасности. Примеры инструментов взлома беспроводных сетей: Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep и NetStumbler.
Инструменты сканирования и взлома сетей	Инструменты сканирования сети используются для проверки сетевых устройств, серверов и хостов на наличие открытых портов TCP или UDP. Примеры инструментов сканирования: SuperScan, Angry IP Scanner и NetScanTools.
Инструменты создания пакетов	Эти инструменты используются для исследования и тестирования отказоустойчивости межсетевого экрана с помощью специально подготовленных поддельных пакетов. Примеры таких инструментов включают Hping, Scapy, Socat, Yersinia, Netcat, Nping и Nemesis.
Анализаторы пакетов	Эти инструменты используются для сбора и анализа пакетов в традиционных проводных и беспроводных локальных сетях Ethernet. Примерами являются Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy и SSLstrip.

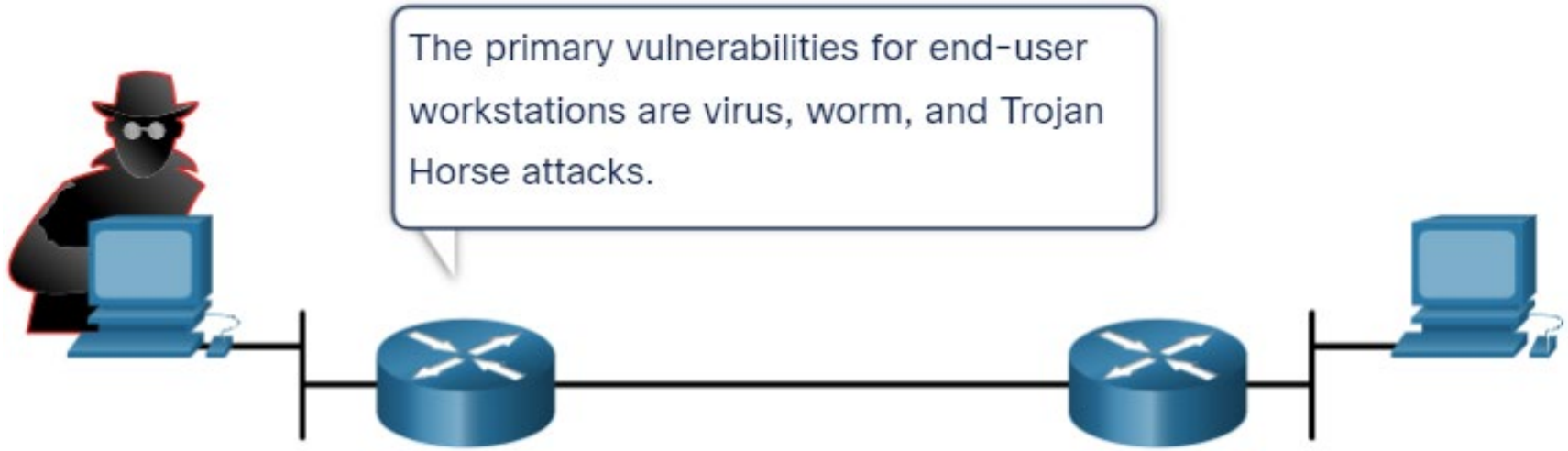
Инструменты тестирования на возможность проникновения.	Описание
Детекторы руткитов	Это инструменты проверки целостности каталогов и файлов, используемые «белыми» хакерами для выявления установленных руткитов. Примерами таких инструментов являются AIDE, Netfilter и PF: OpenBSD Packet Filter.
Фаззеры для поиска уязвимостей	Фаззеры — это инструменты, используемые злоумышленниками при поиске уязвимостей безопасности компьютерной системы. Примеры фаззеров — Skipfish, Wapiti и W3af.
Инструменты технической экспертизы	Эти инструменты используются «белыми» хакерами для выявления следов улик в конкретной компьютерной системе. Примерами таких инструментов являются Sleuth Kit, Helix, Maltego и Encase.
Отладчики	Эти инструменты используются «черными» хакерами для декомпиляции двоичных файлов при программировании эксплойтов. Они также используются «белыми» хакерами при анализе вредоносного ПО. К числу инструментов отладки относятся GDB, WinDbg, IDA Pro и Immunity Debugger.
Хакерские операционные системы	Это специально разработанные операционные системы с предварительно загруженными инструментами и технологиями, предназначенными для взлома. Примерами специальных хакерских операционных систем являются Kali Linux, BackBox Linux.
Средства шифрования	Средства шифрования с помощью алгоритмических схем кодируют данные для предотвращения несанкционированного доступа к зашифрованным данным. Примерами являются VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN и Stunnel.
Средства эксплуатации уязвимостей	Эти средства определяют, является ли удаленный хост уязвимым к атакам на систему безопасности. Примерами средств эксплуатации уязвимостей являются Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit и Netsparker.
Сканеры уязвимостей	Эти инструменты сканируют сети или системы для определения открытых портов. Они также могут использоваться для сканирования на наличие известных уязвимостей и сканирования виртуальных машин, устройств BYOD и баз данных клиентов. Среди этих инструментов — Nipper, Core Impact, Nessus v6, SAINT и Open VAS.

Тип атаки	Описание
Подслушивание	Злоумышленник перехватывает и прослушивает сетевой трафик. Такая атака также называется анализом трафика или снупингом.
Атака с изменением данных	Если злоумышленник перехватывает трафик предприятия, он затем может изменить данные в пакете без ведома отправителя или получателя.
Атака с подменой IP-адреса	Злоумышленник создает IP-пакет, который выглядит как исходящий из допустимого адреса в корпоративной интрасети.
Атаки на основе пароля	Если злоумышленник обнаруживает действительную учетную запись пользователя, он получает такие же права, как и этот настоящий пользователь. Злоумышленник могут использовать эту действительную учетную запись для получения списков других пользователей, информации о сети, изменения конфигурации сервера и сети, а также для изменения, перенаправления или удаления данных.
Атака типа «отказ в обслуживании» (DoS-атака)	DoS-атака лишает законных пользователей возможности нормально использовать компьютер или сеть. DoS-атака может насыщать компьютер или всю сеть трафиком, пока не произойдет отключение из-за перегрузки. DoS-атака также может блокировать трафик, что приводит к потере доступа авторизованных пользователей к сетевым ресурсам.
Атака с перехватом	Такая атака происходит, когда злоумышленник внедряется между источником и получателем. После этого он может активно отслеживать, перехватывать и контролировать обмен данными прозрачным образом.
Атака с подбором ключа	Если злоумышленник получает секретный ключ, этот ключ называется скомпрометированным или раскрытым. Раскрытый ключ позволяет получить доступ к защищенному обмену данными, при этом отправитель или получатель не подозревает о проводящейся атаке.
Атака с перехватом пакетов	Анализатор трафика — это приложение или устройство, которое может выполнять чтение, мониторинг и захват данных, передаваемых по сети, а также чтение сетевых пакетов. Если пакеты не зашифрованы, анализатор трафика позволяет видеть все данные, находящиеся внутри пакета.

3.4 ВРЕДОНОСНОЕ ПО
3.4.1 ОБЗОР ВРЕДОНОСНОГО ПО

Теперь, когда вы узнали об инструментах, которые используют хакеры, этот раздел знакомит вас с различными типами вредоносных программ, которые используют злоумышленники для получения доступа к конечным устройствам.

Оконечные устройства в частности уязвимы перед атаками с использованием вредоносного ПО. Важно знать о вредоносном ПО, поскольку хакеры часто пытаются обманом заставить пользователей установить вредоносное ПО для использования брешей в системе безопасности.



3.4.2 ВИРУСЫ И ТРОЯНЫ

Первым и наиболее распространенным типом вредоносного ПО являются компьютерные вирусы. Вирусы требуют от человека принять участие в распространении и заражении других компьютеров.

Вирус скрывается путем прикрепления себя к компьютерному коду, программному обеспечению или документам на компьютере. При открытии файла вирус выполняется и заражает компьютер.

Вирусы могут:

1. Изменить, повредить, удалить файлы или удалить целые диски.

2. Вызывать проблемы с загрузкой компьютера и повреждение приложений.

3. Выполнять захват и отправку конфиденциальной информации злоумышленникам.

4. Получать доступ и использовать учетные записи электронной почты для распространения.

5. Бездействовать, пока их не активирует хакер.

3.4.2 ВИРУСЫ И ТРОЯНЫ

Современные вирусы разрабатываются для определенных целей, их виды перечислены в таблице.

Виды вирусов	Описание
Вирус загрузочного сектора	Вирусные атаки на загрузочный сектор, таблицу разделов файлов или файловую систему.
Вирусы встроенного ПО	Вирусные атаки на микропрограммное обеспечение устройства.
Макровирус	Вирус использует макрос MS Office вредоносно.
Программные вирусы	Вирус вставляется в другую исполняемую программу.
Сценарий — вирусы	Вирусные атаки с использованием интерпретатора ОС, который используется для выполнения сценариев.

3.4.2 ВИРУСЫ И ТРОЯНЫ

Злоумышленники используют «троянских коней» для того, чтобы скомпрометировать хосты. «Троянский конь», или троян, обычно замаскирован под полезную программу, которая, однако, содержит вредоносный код. Троянские кони часто предоставляются в бесплатных онлайн-программах, таких как компьютерные игры. В таблице перечислены некоторые типы троянов.

Виды действий троянов	Описание
Удаленный доступ	Троян делает возможным несанкционированный удаленный доступ.
Отправка данных	Троян предоставляет злоумышленнику конфиденциальные данные, например пароли.
Разрушение данных	Троян повреждает файлы или удаляет их.
Прокси-сервер	Троян использует компьютер жертвы как источник для новых атак и противоправных действий.
FTP	Троян делает возможным несанкционированный обмен файлами на конечных устройствах.
Вывод из строя защитного ПО	Троян останавливает работу антивирусных программ или брандмауэров.
Отказ в обслуживании (DoS-атака)	Троян замедляет обмен данными по сети или полностью блокирует его.
Кейлогер	Троян активно пытается украсть конфиденциальную информацию, такую как номера кредитных карт, записывая нажатия клавиш, введенные в веб-форму.

3.4.3 ТИПЫ ВРЕДОНОСНОГО ПО

Вредоносное ПО	Описание
Рекламные программы	Рекламное ПО обычно распространяется путем загрузки программного обеспечения онлайн. Рекламное ПО может отображать нежелательную рекламу с помощью всплывающих окон веб-браузера, новых панелей инструментов или неожиданно перенаправлять веб-страницу на другой веб-сайт. Всплывающие окна могут быть сложными для управления, так как новые окна могут быть раскрыты быстрее, чем пользователь может закрыть их.
Вирусы-вымогатели,	Вирус-вымогатель обычно запрещает пользователю доступ к своим файлам, шифруя файлы и затем отображая сообщение, требующее выкуп за ключ дешифрования. Пользователи, не имеющие актуальных резервных копий, должны заплатить выкуп за расшифровку. Оплата обычно производится с помощью банковского перевода или криптовалюты, такие как Биткоин.
Руткит	Руткиты используются злоумышленниками для получения доступа к компьютеру. Их очень трудно обнаружить, потому что они могут изменить брандмауэр, антивирусную защиту, системные файлы и даже команды ОС, чтобы скрыть свое присутствие. Они могут предоставить бэкдор злоумышленникам, предоставляя им доступ к ПК и позволяя им загружать файлы и устанавливать новое программное обеспечение для использования при DDoS-атаке. Для их удаления необходимо использовать специальные инструменты для удаления руткитов, либо может потребоваться полная переустановка ОС.
Шпионское ПО	Аналогично рекламному ПО, но предназначено для сбора информации о пользователе и отправки полученных сведений другой стороне без ведома пользователя. Шпионское ПО может представлять собой незначительную угрозу, собирая только данные о посещенных веб-страницах, или достаточно серьезную опасность, если его целью является сбор личной или финансовой информации.
Червь	Червь — это программа саморепликации, автоматически распространяющаяся без действий пользователя путем использования уязвимостей в легальном программном обеспечении. Он использует сеть для поиска других жертв с такой же уязвимостью. Целью червя обычно является замедление или нарушение работы сети.

3.5 РАСПРОСТРАНЕННЫЕ СЕТЕВЫЕ АТАКИ

3.5.1 ОБЗОР РАСПРОСТРАНЕННЫХ СЕТЕВЫХ АТАК

Когда вредоносное ПО доставляется и устанавливается, его информационное наполнение может использоваться для различных сетевых атак.

Для того чтобы минимизировать последствия атак, полезно сначала классифицировать их различные виды. Распределив сетевые атаки по категориям, можно рассматривать типы атак, а не отдельные атаки.

Сети подвержены следующим типам атак:

1. Разведывательные атаки.

2. Атаки доступа.

3. Атаки типа «отказ в обслуживании» (DoS-атаки).

3.5.2 РАЗВЕДЫВАТЕЛЬНЫЕ АТАКИ

Некоторые техники, используемые злоумышленниками для проведения разведывательных атак, описаны в таблице.

Техника	Описание
Выполнить информационный запрос цели	Хакер ищет исходную информацию о целевом объекте. Можно использовать различные инструменты, в том числе поиск Google, веб-сайт организаций, Whois и многое другое.
Инициация эхо-запроса целевой сети	Информационный запрос обычно показывает сетевой адрес цели. Злоумышленник теперь может инициировать проверку связи, чтобы определить, какие IP-адреса являются активными.
Инициация сканирования портов активных IP-адресов	Используется для определения доступных портов или сервисов. Примеры инструментов сканирования портов: SuperScan, Angry IP Scanner и NetScanTools.
Запуск сканеров уязвимостей	Это делается для запроса идентифицированных портов, чтобы определить тип и версию приложения и операционной системы, которая работает на хосте. Среди этих инструментов — Nipper, Core Impact, Nessus v6, SAINT и Open VAS.
Запуск эксплойтов	Теперь злоумышленник пытается обнаружить уязвимые сервисы, которые могут быть использованы. Примерами средств эксплуатации уязвимостей являются Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit и Netsparker.

3.5.3 АТАКИ ДОСТУПА

Атаки доступа используют известные уязвимости в службах аутентификации, FTP- и веб-сервисах. Цель таких атак - получить доступ к учетным записям в Интернете, конфиденциальным базам данных и другой секретной информации.

Злоумышленники используют атаки доступа на сетевые устройства и компьютеры для получения данных, получения доступа или для расширения прав доступа до статуса администратора.

Атака с подбором пароля: при атаке с подбором пароля злоумышленник пытается обнаружить критические системные пароли, используя различные методы. Такие атаки очень распространены и могут быть запущены с использованием различных инструментов взлома паролей.

Спуфинг-атака: при спуфинг-атаке устройство злоумышленника пытается выдать себя за другое путем фальсификации данных. Обычные спуфинговые атаки включают IP-спуфинг, MAC-спуфинг и DHCP-спуфинг. Такие спуфинговые атаки еще будут более подробно обсуждаться в этом модуле.

Другие атаки доступа включают в себя:

- злоупотребление доверием;

- переадресация портов;

- атака через посредника;

- атака с переполнением буфера.

3.5.4 ПСИХОЛОГИЧЕСКИЕ АТАКИ

Социальная инженерия – это атака, которая пытается заставить человека выполнить определенные действия или раскрыть конфиденциальную информацию. Некоторые методы социальной инженерии подразумевают личное обращение к человеку, в то время как другие могут быть использованы через телефон или интернет.

Социальные инженеры часто полагаются на готовность людей помочь. Они также используют человеческие слабости.

3.5.4 РАСПРОСТРАНЕННЫЕ СЕТЕВЫЕ АТАКИ

Атаки методами социальной инженерии	Описание
Вымышленный предлог	Злоумышленник притворяется, что ему необходимы личные или финансовые данные для подтверждения подлинности получателя.
Фишинг	Злоумышленник отправляет мошенническое электронное письмо, которое замаскировано как из законного надежного источника, чтобы обмануть получателя в установке вредоносного ПО на его устройстве или для обмена личной или финансовой информацией.
Прицельный фишинг	Злоумышленник подготавливает фишинговую атаку, направленную на определенного человека или организацию.
Спам	Нежелательная электронная почта, которая часто содержит опасные каналы, вредоносное ПО или мошенническое содержимое.
Услуга за услугу (взаимовыгодный обмен)	Иногда называется “Quid pro quo”, злоумышленник запрашивает личную информацию в обмен на что-то, например, на подарок.
Приманка	Злоумышленник оставляет зараженное вредоносным ПО физическое устройство, например USB-накопитель, в общественном месте. Жертва находит его и ничего не подозревает, вставляет его в свой ноутбук, непреднамеренно устанавливая вредоносное ПО.
Имперсонификация	Это тип атаки, где злоумышленник притворяется тем, кем он не является, чтобы завоевать доверие к жертве.
Несанкционированное проникновение	Это когда злоумышленник быстро следует за уполномоченным лицом в безопасное место, чтобы получить доступ к безопасной зоне.
Визуальное хакерство (Взгляд через плечо)	Это когда злоумышленники незаметно смотрит через чье-то плечо, чтобы украсть его пароли или другую информацию.
Исследование содержимого мусорных корзин	Когда злоумышленник роется в мусорных корзинах, чтобы найти конфиденциальные документы.

3.5.5 АТАКИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Компанией TrustedSec был разработан набор инструментов социальной инженерии (Social Engineering Toolkit, SET), чтобы помочь «белым» хакерам и другим специалистам по сетевой безопасности организовывать атаки методами социальной инженерии для проверки своих собственных сетей.

Предприятия должны информировать своих пользователей о рисках социальной инженерии и разрабатывать стратегии для подтверждения личности по телефону, электронной почте или лично.

На рисунке показаны рекомендуемые методы защиты, которым должны следовать все пользователи.

3.5.5 DOS И DDOS-АТАКИ

DoS-атака («отказ в обслуживании») влечет за собой перебои в сетевых службах для пользователей, устройств или приложений. Существует два типа DoS-атак.

Огромные объемы трафика - киберпреступник отправляет огромное количество данных с такой скоростью, что сеть, хост или приложение не успевает их обрабатывать. Это приводит к замедлению передачи и времени отклика. Это также может привести к сбою работы устройства или службы.

Пакеты с неправильным форматированием - киберпреступник посылает пакет данных с неправильным форматированием на хост или в приложение. Это замедлит его работу или приведет к сбою.

DoS-атаки представляют высокий риск, поскольку могут легко нарушить обмен информацией и вести к крупным потерям времени и средств. Проводить такие атаки относительно несложно, это под силу даже неопытным злоумышленникам.

Распределенные атаки типа «Отказ в обслуживании» (DDoS) похожи на DoS-атаки, но проводятся скоординировано из нескольких источников.

3.6 УЯЗВИМОСТИ IP И УГРОЗЫ

3.6.1 IPV4 И IPV6

IP не проверяет, действительно ли указанный в пакете IP-адрес источника поступил из этого источника. Поэтому злоумышленники могут отправлять пакеты, используя поддельный IP-адрес источника. Поэтому аналитикам по вопросам безопасности важно понимать суть различных полей в заголовках IPv4 и IPv6.

В таблице приведены некоторые наиболее распространенные атаки, связанные с IP.

Методы IP-атак	Описание
Атаки на основе ICMP	Злоумышленники используют пакеты эхо-запросов (ping) протокола ICMP для обнаружения подсетей и хостов в защищенной сети, чтобы создавать лавинные DoS-атаки, а также изменять таблицы маршрутизации хоста.
Атаки с усилением и отражением	Злоумышленники пытаются лишить законных пользователей доступа к информации или службам.
Атаки с подменой адреса	Злоумышленники подменяют IP-адрес источника в IP-пакете для выполнения открытой подмены или подмены вслепую.
Атака через посредника (MITM)	Злоумышленники внедряются между источником и назначением для прозрачного мониторинга, захвата и контроля обмена данными. Они могут прослушивать, проверяя собранные пакеты, или изменять пакеты и пересылать по первоначальному целевому адресу.
Перехват сеанса	Злоумышленники получают доступ к физической сети, а затем используют атаку через посредника для перехвата сеанса.

3.6.2 АТАКИ НА ОСНОВЕ ICMP

Злоумышленники используют ICMP для разведывательных атак и сканирования в сети. Они могут запустить атаку для сбора информации, чтобы определить топологию сети, узнать, какие хосты активны (доступны), определить операционную систему хоста (создание цифрового отпечатка ОС), а также определить состояние межсетевого экрана. Злоумышленники также используют ICMP для DoS-атак.

Примечание. ICMP для IPv4 (ICMPv4) и ICMP для IPv6 (ICMPv6) подвергаются атакам аналогичных типов.

В сетях должна применяться строгая фильтрация на основе списков контроля доступа (ACL) ICMP на границе сети, чтобы избежать зондирования ICMP из Интернета. В крупных сетях устройства обеспечения безопасности, например, межсетевые экраны и системы обнаружения вторжений (IDS), должны обнаруживать такие атаки и выдавать предупреждения для аналитиков по безопасности.

3.6.2 АТАКИ НА ОСНОВЕ ICMP

В таблице представлены сообщения ICMP, которыми обычно интересуются злоумышленники.

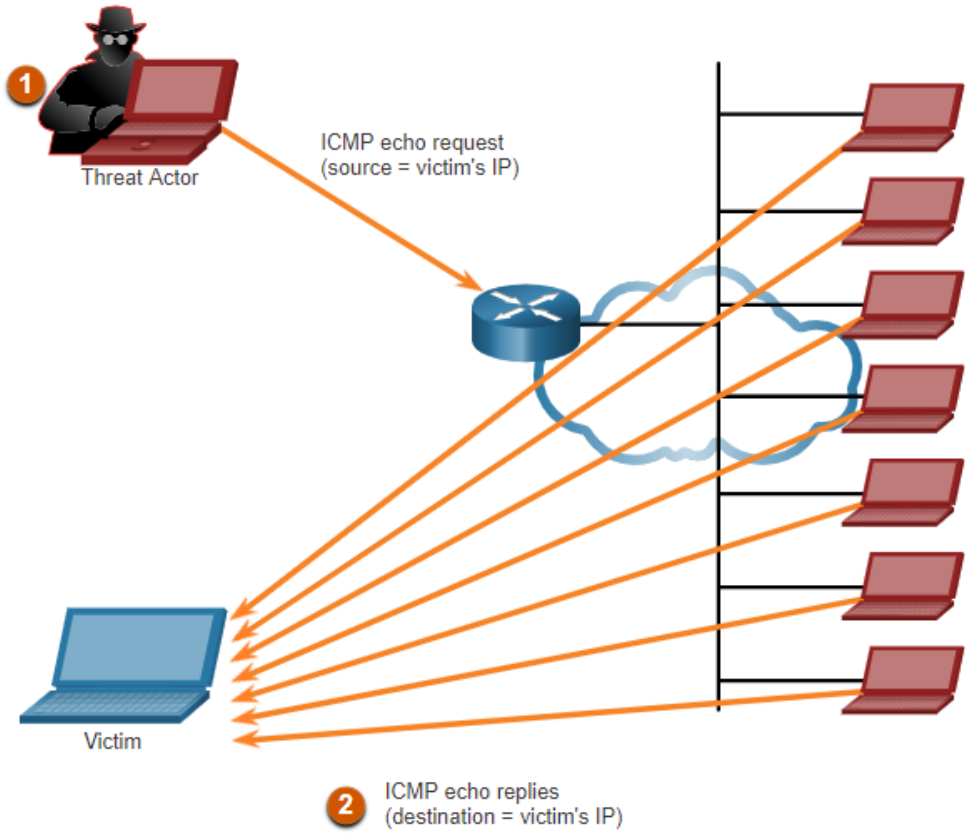
ICMP сообщения, которые используют злоумышленники	Описание
Эхозапрос и эхоответ ICMP	Используются для выполнения проверки хостов и DoS-атак.
Сообщение ICMP о недостижимости	Используется для выполнения разведывательных атак и сканирования сети.
Ответ ICMP с маской.	Используется для составления карты внутренней IP-сети.
Перенаправления ICMP.	Используются, чтобы спровоцировать целевой хост на отправку всего трафика через взломанное устройство и провести атаку через посредника (MITM).
Обнаружение маршрутизатора ICMP	Используется для вставки фиктивных записей маршрута в таблицу маршрутизации целевого хоста.

3.6.3 АТАКИ С ЛАВИНООБРАЗНЫМ УМНОЖЕНИЕМ ДАННЫХ И ОТРАЖЕНИЕМ

Хакеры часто используют методы лавинообразного умножения данных и отражения для создания DoS-атак. В примере на рисунке показано использование Smurf-атаки для перегрузки целевого хоста.

Примечание. В настоящее время используются более новые формы атак по методу умножения и отражения, например, атаки на основе DNS и атаки по NTP с умножением данных.

Злоумышленники также используют атаки с исчерпанием ресурсов, чтобы перегрузить ресурсы целевого хоста и вызвать его сбой или загрузить ресурсы сети.



3.6.4 АТАКИ С ПОДМЕНОЙ АДРЕСА

Атаки с подменой IP-адреса происходят, когда злоумышленник создает пакеты с ложной информацией об IP-адресе источника, чтобы скрыть личность отправителя или выдать себя за легитимного пользователя. Подмена адресов обычно применяется в рамках других атак, например, в smurf-атаках.

Атаки с подменой могут быть с открытой подменой или вслепую.

Открытая подмена - злоумышленник может видеть трафик, который передается между хостом и целевым объектом. Целью открытой подмены может быть определение состояния межсетевого экрана, прогнозирование порядкового номера, а также перехват авторизованного сеанса.

Подмена вслепую - злоумышленник не видит трафик, который передается между хостом и целевым объектом. Подмена вслепую используется в DoS-атаках.

Атаки с подменой MAC-адресов используются, когда у злоумышленника есть доступ к внутренней сети. Злоумышленники изменяют MAC-адрес своего хоста в соответствии с другим известным MAC-адресом целевого хоста.

3.7 УЯЗВИМОСТИ TCP И UDP
3.7.1 IPV4 И IPV6

Информация сегмента TCP находится сразу после заголовка IP. На рисунке изображены поля сегмента TCP и флаги для поля управляющих битов.

Ниже приведены шесть управляющих битов сегмента TCP:

URG - флаг «Указатель важности».

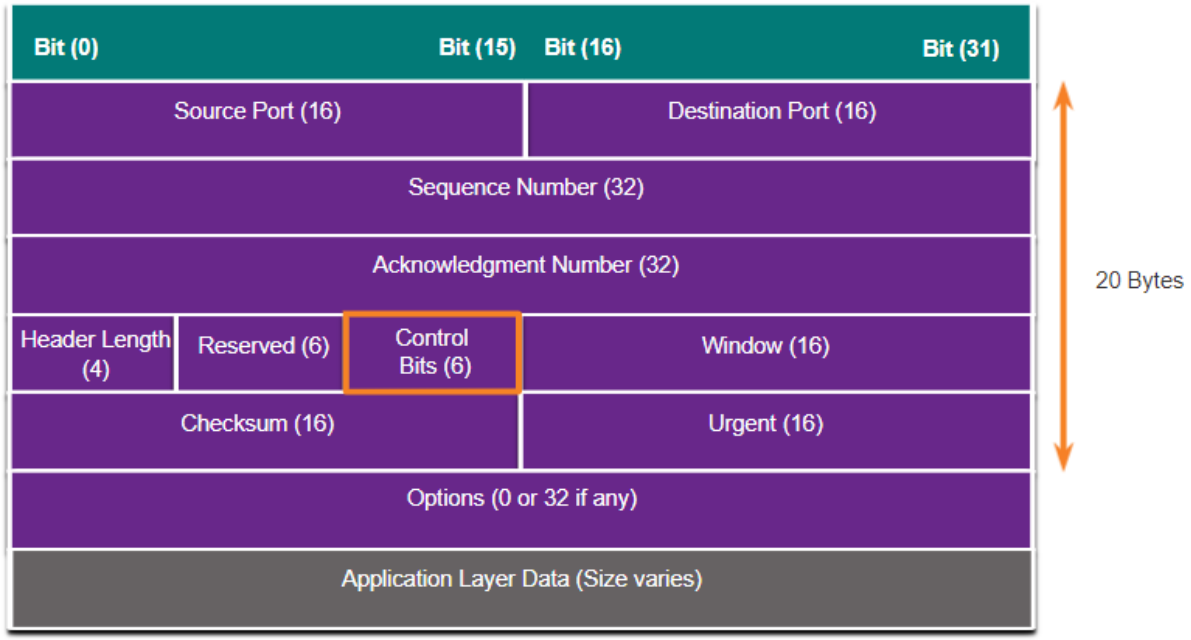
ACK - флаг «Номер подтверждения».

PSH - флаг «Push».

RST- флаг сброса соединения.

SYN - флаг «Номер последовательности».

FIN - флаг «Больше нет данных от отправителя».



3.7.2 СЕРВИСЫ TCP

TCP также обеспечивает следующие возможности:

Надежная доставка - TCP включает подтверждения для гарантированной доставки. Если своевременное подтверждение не получено, отправитель передает данные повторно. Однако необходимость подтверждать получение данных может приводить к существенным задержкам. К примерам протоколов уровня приложений, использующих надежность протокола TCP, относятся SSL/TLS, HTTP, FTP, зонные переносы DNS и др.

Управление потоком - для решения этой проблемы в TCP реализуется управление потоком. Для того чтобы не подтверждать сегменты по одному, с помощью одного сегмента подтверждения можно сообщить о получении сразу нескольких сегментов.

Обмен данными с отслеживанием состояния - обмен данными с отслеживанием состояния по протоколу TCP между двумя сторонами происходит посредством трехстороннего квитирования TCP.

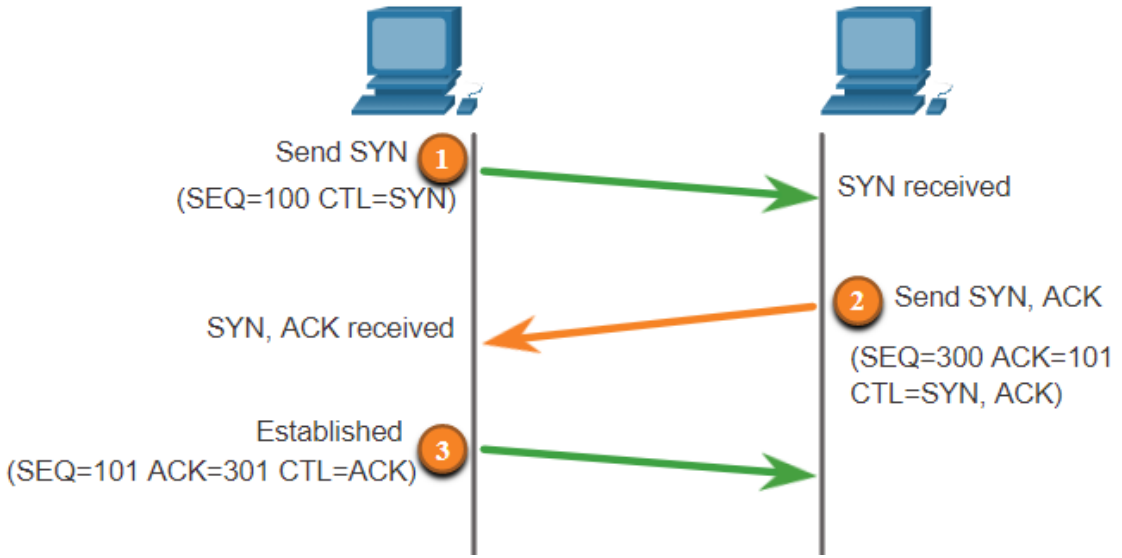
3.7.2 СЕРВИСЫ TCP

Установление соединения по протоколу TCP осуществляется в три этапа.

Инициирующий клиент запрашивает сеанс связи типа «клиент-сервер» с сервером.

Сервер подтверждает сеанс обмена данными «клиент-сервер» и запрашивает сеанс обмена данными «сервер-клиент».

Начальный клиент подтверждает сеанс связи между клиентом и сервером.



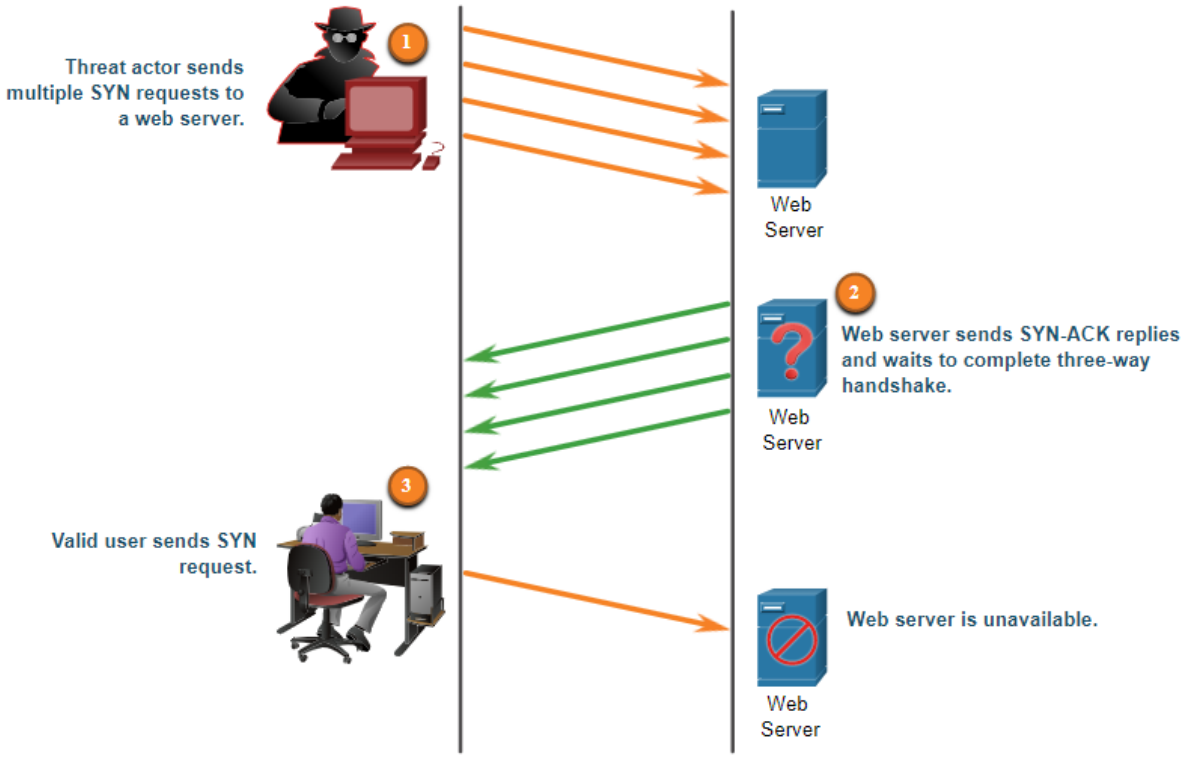
3.7.3 АТАКИ TCP

Лавинная атака SYN-flood TCP

1. Злоумышленник отправляет веб-серверу множество запросов SYN.

2. Веб-сервер отвечает SYN-ACK для каждого запроса SYN и ожидает завершения трехстороннего квитирования. Злоумышленник не отвечает на SYN-ACK.

3. Легитимный пользователь не может получить доступ к веб-серверу, поскольку веб-сервер имеет слишком много полуоткрытых TCP-соединений.



3.7.3 АТАКИ TCP

Для завершения сеанса TCP используется следующий процесс четырехстороннего обмена:

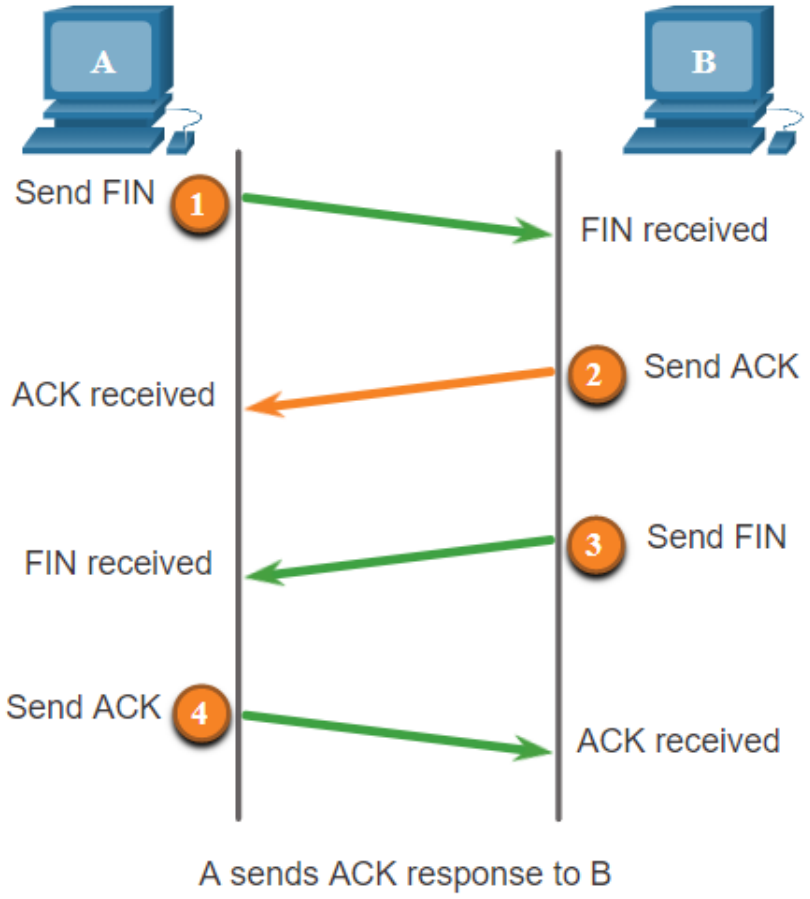
1. Когда у клиента больше нет данных для отправки в потоке, он отправляет сегмент с установленным флагом FIN

2. Сервер отправляет подтверждение ACK, чтобы подтвердить получение FIN для завершения сеанса связи «клиент-сервер»

3. Сервер отправляет клиенту флаг FIN для завершения сеанса связи между сервером и клиентом.

4. Клиент отправляет в ответ флаг ACK, чтобы подтвердить получение флага FIN от сервера.

Злоумышленник может выполнить атаку со сбросом TCP и отправить поддельный пакет, содержащий сегмент TCP RST, на одно или оба оконечных устройства.



3.7.3 АТАКИ TCP

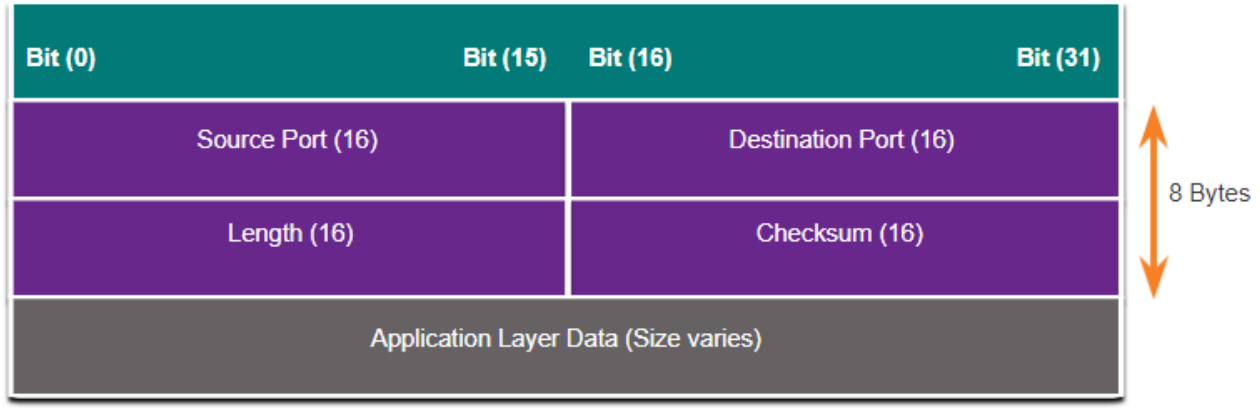
Перехват сеанса TCP представляет собой еще одну уязвимость TCP. Несмотря на сложность реализации, такой перехват позволяет хакеру взять под контроль уже аутентифицированный хост при обмене данными с целевым объектом. Злоумышленнику пришлось бы подменить IP-адрес одного хоста, спрогнозировать следующий порядковый номер и отправить подтверждение (ACK) на другой хост. В случае успеха злоумышленник сможет отправлять, но не получать данные от целевого устройства.

3.7.4 ЗАГОЛОВОК СЕГМЕНТА TCP И ЕГО РАБОТА

UDP обычно используется DNS, TFTP, NFS и SNMP. Он также используется с приложениями реального времени, такими как потоковая передача мультимедиа или передача голоса по IP. UDP — протокол транспортного уровня без установки соединения. Он связан с существенно меньшими накладными расходами в сравнении с TCP, поскольку не устанавливает соединение и не поддерживает сложные механизмы повторной отправки, упорядочения и управления процессами, которые обеспечивают надежность.

Функции обеспечения надежности не обеспечиваются протоколом транспортного уровня и при необходимости должны быть реализованы на других уровнях.

Низкие накладные расходы, свойственные UDP, делают его просто незаменимым в случаях, когда требуется протокол, осуществляющий лишь транзакции по отправке запросов и получению ответов.



3.7.4 АТАКИ UDP

Протокол UDP не защищается шифрованием. В протокол UDP можно добавить функции шифрования, но по умолчанию они недоступны. Отсутствие шифрования позволяет злоумышленнику просмотреть трафик, изменить его и отправить по назначению.

UDP Flood атаки: для этого злоумышленнику необходимо использовать такой инструмент, как UDP Unicorn или Low Orbit Ion Cannon. Такой инструмент отправляет лавину пакетов UDP, часто с ложного хоста, на сервер в подсети. Программа пройдется по всем известным портам в попытке найти закрытые. Это приведет к тому, что сервер отправит в ответ сообщение о недоступности порта ICMP. Поскольку на сервере существует множество закрытых портов, в результате в сегменте оказывается настолько большой объем трафика, что используется почти вся полоса пропускания. Результат очень похож на DoS-атаку.

3.8 IP СЕРВИСЫ
3.8.1 УЯЗВИМОСТИ ARP

Хосты передают ARP-запрос в широковещательном режиме другим хостам в сегменте, чтобы определить MAC-адрес хоста с конкретным IP-адресом. Хост с IP-адресом, соответствующим ARP-запросу, отправляет ARP-ответ.

Любой клиент может отправить незапрашиваемый ARP-ответ, который называется gratuitous ARP (самообращенный ARP). Когда хост отправляет самообращенный ARP, другие хосты в подсети сохраняют в своих ARP-таблицах MAC-адрес и IP-адрес, содержащиеся в этом ответе.

Однако эта функция ARP также означает, что любой хост может объявить себя владельцем любого выбранного IP или MAC-адреса. Злоумышленник может подделать записи кеша ARP устройств в локальной сети, организуя атаку через посредника для перенаправления трафика.

3.8.2 ПОДДЕЛКА ЗАПИСЕЙ КЕША ARP

Подделка записей кеша ARP может использоваться для запуска различных атак «через посредника».

Компьютер PC-A запрашивает MAC-адрес своего шлюза по умолчанию (R1), отправляя ARP-запрос на получение MAC-адреса для IP-адреса 192.168.10.1.

Маршрутизатор R1 вносит в свой кеш ARP IP- и MAC-адрес компьютера PC-A и отправляет ARP-ответ компьютеру PC-A, который затем вносит в свой кеш ARP IP- и MAC-адрес маршрутизатора R1.

Злоумышленник отправляет два поддельных самообращенных ARP-ответа, используя свой собственный MAC-адрес для указанных IP-адресов назначения. Компьютер PC-A обновляет сведения о шлюзе по умолчанию в своем кеше ARP, которые теперь указывают на MAC-адрес хоста злоумышленника. Маршрутизатор R1 также обновляет свой кеш ARP, внося в него IP-адрес компьютера PC-A, указывающий на MAC-адрес злоумышленника.

Атаки с подделкой записей кеша ARP могут быть пассивными или активными. Пассивные - когда злоумышленники крадут конфиденциальную информацию. Активные - злоумышленники изменяют передаваемые данные или внедряют вредоносные данные.

3.8.3 АТАКИ DNS

Протокол системы доменных имен (Domain Name Service, DNS) определяет автоматизированную службу, которая сопоставляет имена ресурсов с соответствующими числовыми сетевыми адресами, такими как IPv4 или IPv6. Он включает в себя формат для запросов, ответов и самих данных и использует записи ресурсов (RR), чтобы определить тип DNS-ответа.

Обеспечением безопасности DNS часто пренебрегают. Однако этот протокол имеет решающее значение для работы сети и должен быть соответствующим образом защищен.

DNS атаки включают в себя:

1. Открытые преобразователи имен DNS.

2. Скрытые атаки DNS.

3. Атаки с теневым управлением DNS.

4. Атаки туннелирования DNS.

3.8.3 АТАКИ DNS

Открытый преобразователь имен DNS отвечает на запросы от клиентов, находящихся за пределами его административного домена. Открытые преобразователи имен DNS уязвимы для различных вредоносных действий, включая следующие.

Уязвимости преобразователей DNS	Описание
Подделка записей кеша DNS	Злоумышленники отправляют поддельную информацию записей ресурсов (RR) в преобразователь имен DNS, чтобы перенаправить пользователей с законных сайтов на вредоносные. Атаки с подделкой записей кеша DNS могут использоваться, чтобы заставить преобразователь имен DNS использовать вредоносный сервер имен, который предоставляет информацию о записях ресурсов (RR) для выполнения вредоносных действий.
Атаки по методу умножения и отражения на основе DNS	Злоумышленники используют открытые преобразователи имен DNS, чтобы увеличить объем атаки и скрыть ее настоящий источник. Злоумышленники отправляют DNS-сообщения открытым преобразователям имен, используя IP-адрес целевого хоста. Эти атаки возможны, поскольку открытый преобразователь имен будет отвечать на запросы от любого объекта.
Атаки с использованием ресурсов DNS.	DoS-атака, использующая ресурсы открытых преобразователей DNS-имен. Эта DoS-атака потребляет все доступные ресурсы, отрицательно влияя на работу преобразователя имен DNS. В результате этой DoS-атаки может потребоваться перезапуск преобразователя имен DNS или остановка и перезапуск служб.

3.8.3 АТАКИ DNS

Скрытые атаки DNS. Для того чтобы скрыть информацию, по которой их можно определить, хакеры применяют для проведения атак следующие скрытые методы использования DNS.

При теневом копировании доменов злоумышленник взламывает родительский домен и создает несколько субдоменов для использования во время атаки. Эти субдомены обычно указывают на вредоносные серверы без предупреждения фактического владельца родительского домена.

Техники скрытых атак DNS	Описание
Метод Fast flux	Злоумышленники используют этот метод, чтобы скрыть фишинговые сайты и сайты, распространяющие вредоносное ПО, внутри быстро меняющейся сети взломанных хостов DNS. IP-адреса DNS постоянно изменяются в течение считаных минут. Ботнеты часто используют методы Fast Flux, чтобы эффективно скрыть от обнаружения вредоносные серверы.
Метод double IP flux (fast flux с частой сменой IP-адресов)	Злоумышленники используют этот метод, чтобы быстро изменять сопоставления имен хостов и IP-адресов, а также изменять доверенный сервер имен. В результате повышается сложность определения источника атаки.
Алгоритмы создания доменов	Злоумышленники используют этот метод во вредоносном ПО, чтобы случайным образом генерировать доменные имена, которые можно использовать как точки встречи для серверов управления и контроля (C&C).

3.8.4 ТУННЕЛИРОВАНИЕ DNS

Хакеры, использующие туннелирование DNS, помещают в трафик DNS трафик, не относящийся к DNS. Этот метод часто позволяет обойти решения по обеспечению безопасности, когда злоумышленник хочет связаться с ботами внутри защищенной сети или отфильтровать данные из организации. Вот как работает туннелирование DNS для команд CnC, отправляемых в ботнет:

1. Данные разбиваются на несколько закодированных фрагментов.

2. Каждый фрагмент помещается в метку доменного имени нижнего уровня в DNS-запросе.

3. Так как ответ локального или сетевого DNS-сервера на этот запрос отсутствует, запрос отправляется на рекурсивные DNS-серверы интернет-провайдера.

4. Рекурсивная служба DNS перенаправляет запрос на доверенный сервер доменных имен злоумышленника.

3.8.4 ТУННЕЛИРОВАНИЕ DNS

5. Этот процесс повторяется, пока не будут отправлены все запросы, содержащие фрагменты данных.

6. Когда доверенный сервер доменных имен злоумышленника получает DNS-запросы от зараженных устройств, он отправляет ответ на каждый запрос, содержащий инкапсулированные, зашифрованные команды.

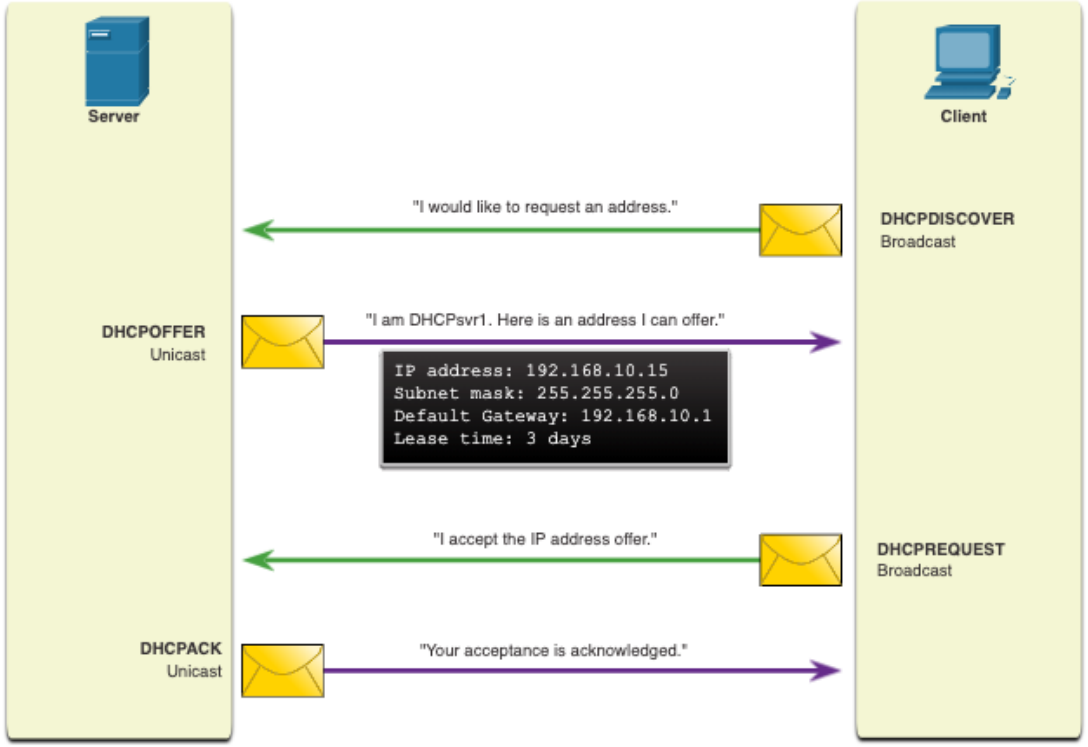
7. Вредоносное ПО, находящееся на скомпрометированном хосте, собирает фрагменты данных и выполняет скрытые в них команды.

Для того чтобы иметь возможность остановить туннелирование DNS, необходимо использовать фильтр, который проверяет DNS-трафик. Обратите особое внимание на DNS-запросы, длина которых превышает среднее значение, а также запросы, содержащие подозрительное доменное имя.

3.8.5 DHCP

Серверы DHCP предоставляют клиентским устройствам сведения о конфигурации динамических IP-адресов.

На рисунке клиент делает широковещательную рассылку сообщений об обнаружении DHCP. DHCP отвечает одноадресной рассылкой с предложением адреса, который клиент может использовать. Клиент широковещательной рассылкой сообщает DHCP серверу, что клиент принимает предложенное. Сервер отвечает одноадресной рассылкой, что он подтверждает прием клиентом адреса.



3.8.6 АТАКИ, СВЯЗАННЫЕ С DHCP

Атака типа «DHCP-спуфинг» состоит в том, что к сети подключается мошеннический DHCP-сервер и предоставляет ложные параметры настройки IP легитимным клиентам. Подставной сервер может предоставлять различные неправильные сведения.

Неправильный шлюз по умолчанию. Злоумышленник предоставляет неправильный шлюз или IP-адрес своего хоста для создания атаки через посредника. Это может пройти полностью незамеченным, поскольку злоумышленник перехватывает поток данных в сети.

Неправильный DNS-сервер. Хакер предоставляет неправильный адрес DNS-сервера, направляя пользователя на вредоносный веб-сайт.

Неправильный IP-адрес. Злоумышленник предоставляет неправильный IP-адрес и/или IP-адрес шлюза по умолчанию. Затем злоумышленник создает DoS-атаку на DHCP-клиента.

3.8.6 АТАКИ, СВЯЗАННЫЕ С DHCP

Предположим, что злоумышленник уже успешно подключил мошеннический сервер DHCP к порту коммутатора в той же подсети, в которой находятся целевые клиенты. Цель подставного сервера — предоставить клиентам неправильную информацию о настройке IP.

1. Для этого клиент отправляет широковещательный запрос обнаружения DHCP, ожидая ответа от DHCP-сервера. Оба сервера получают сообщение.

2. Законный и подставной DHCP-серверы отправляют ответ с допустимыми параметрами настройки IP. Клиент ответит на первое полученное предложение.

3. Клиент первым получает предложение от подставного сервера. Он выполняет широковещательную рассылку DHCP-запроса, принимая параметры от подставного сервера. Запрос получат и законный и подставной серверы.

4. Подставной сервер направляет клиенту индивидуальный ответ с подтверждением запроса. Законный сервер прекращает общение с клиентом, потому что запрос был уже подтвержден.

3.9 ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ СЕТЕВОЙ БЕЗОПАСНОСТИ

3.9.1 КОНФИДЕНЦИАЛЬНОСТЬ, ДОСТУПНОСТЬ И ЦЕЛОСТНОСТЬ

Информационная безопасность занимается защитой информации и информационных систем от несанкционированного доступа, использования, раскрытия, повреждения, изменения или уничтожения.

Большинство организаций придерживается триады КЦД, состоящей из трех компонентов информационной безопасности.

Конфиденциальность — только авторизованные лица, объекты или процессы могут получить доступ к конфиденциальной информации. Для шифрования и дешифрования данных может потребоваться использование алгоритмов криптографического шифрования, таких как AES.

Целостность — защита данных от несанкционированного изменения. Это требует использования криптографических алгоритмов хеширования, таких как SHA.

Доступность — авторизованные пользователи должны иметь непрерывный доступ к важным ресурсам и данным. Это требует внедрения резервных сервисов, шлюзов и каналов связи.

3.9.2 УГЛУБЛЕННЫЙ ПОДХОД К ЗАЩИТЕ

Для безопасного обмена данными через общедоступные и частные сети в первую очередь необходимо обеспечить защиту устройств, включая маршрутизаторы, коммутаторы, серверы и хосты. Организации используют углубленный подход к защите сети. Такой подход предполагает совместную работу сетевых устройств и сервисов.

Внедряется несколько устройств и служб безопасности:

VPN

Межсетевой экран ASA

IPS

ESA/WSA

Сервер AAA

Защита всех сетевых устройств, включая маршрутизатор и коммутаторы.

Далее необходимо обеспечить защиту данных, пересылаемых по различным каналам.

3.9.3 МЕЖСЕТЕВОЙ ЭКРАН (МСЭ)

Межсетевой экран — это система или группа систем, реализующая политику управления доступом между сетями.

Allow traffic from any external address to the web server.

Allow traffic to FTP server.

Allow traffic to SMTP server.

Allow traffic to internal IMAP server.

Deny all inbound traffic with network addresses matching internal-registered IP addresses.

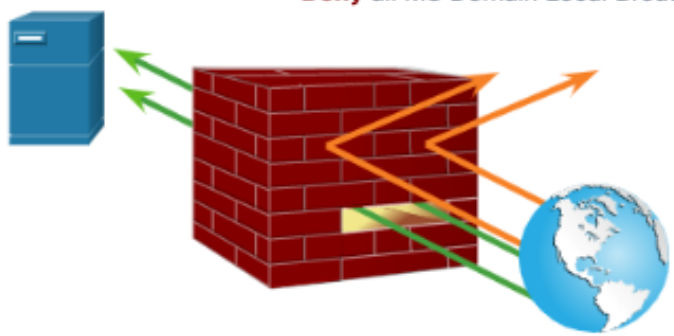
Deny all inbound traffic to server from external addresses.

Deny all inbound ICMP echo request traffic.

Deny all inbound MS Active Directory queries.

Deny all inbound traffic to MS SQL server queries.

Deny all MS Domain Local Broadcasts.



3.9.4 IPS

Для защиты от быстро развивающихся атак вам могут потребоваться экономически эффективные системы обнаружения и предотвращения, интегрированные в точки входа и выхода в сети.

Технологии IDS и IPS имеют несколько общих характеристик. Технологии IDS и IPS реализуются в сети посредством сенсоров. Сенсорами IDS или IPS могут быть разные устройства:

- маршрутизатор, на который установлено программное обеспечение IPS Cisco IOS;

- специализированное устройство, выполняющее функции IDS или IPS;

- сетевой модуль, установленный в многофункциональном устройстве обеспечения безопасности (ASA), коммутаторе или маршрутизаторе.

Для обнаружения вредоносных действий IPS использует набор правил, называемый сигнатурами, с целью выявления шаблонов в сетевом трафике. Технологии IDS и IPS могут обнаруживать атомарные шаблоны сигнатур (один пакет) или составные шаблоны сигнатур (несколько пакетов).

3.9.4 IPS

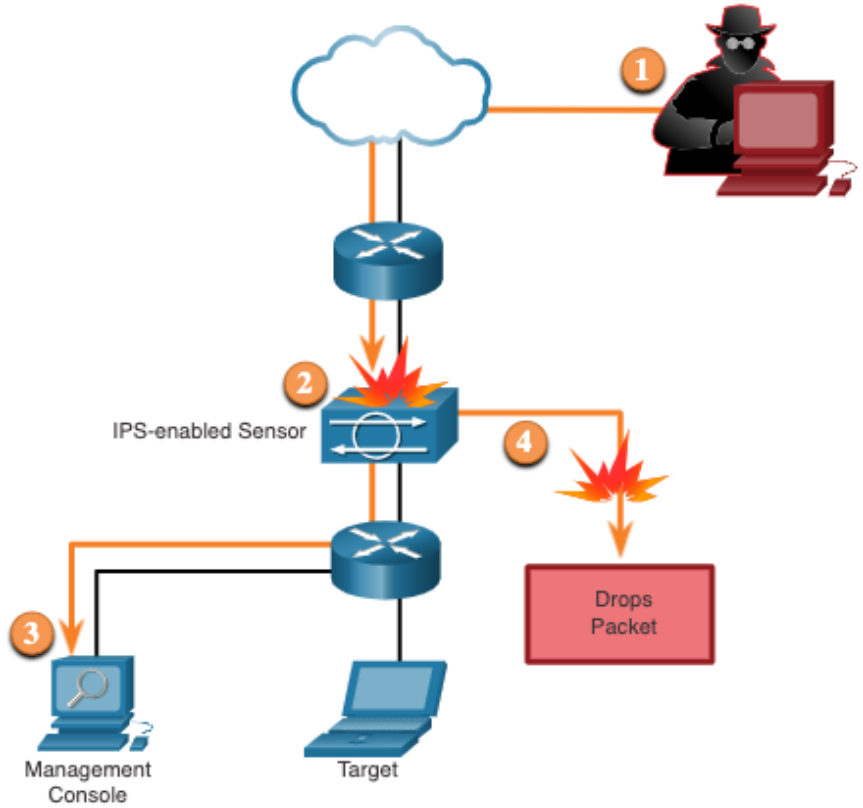
На рисунке показано, как IPS управляет запрещенным трафиком.

1. Злоумышленник посылает пакет, предназначенный целевому хосту.

2. IPS перехватывает трафик и оценивает его относительно угроз и сконфигурированных политик.

3. IPS пересылает сообщения журнала на консоль управления.

4. IPS отбрасывает пакет.



3.9.5 УСТРОЙСТВА ЗАЩИТЫ КОНТЕНТА

Cisco ESA - это устройство, предназначенное для мониторинга SMTP-протокола. Cisco ESA постоянно обновляется в режиме реального времени из каналов Cisco Talos. Эти данные об угрозах извлекаются устройствами Cisco ESA каждые три-пять минут.

Устройство защиты веб-трафика Cisco (WSA) - это технология нейтрализации веб-угроз. WSA предоставляет защиту от вредоносного ПО, мониторинг и контроль функционирования приложений, а также средства управления политиками допустимого использования, создания отчетов.

Cisco WSA обеспечивает полный контроль над доступом пользователей к сети Интернет. WSA может выполнять внесение в черный список URL-адресов, фильтрацию URL-адресов, сканирование на наличие вредоносных программ, категоризацию URL-адресов, фильтрацию веб-приложений, а также шифрование и дешифрование веб-трафика.

3.10 КРИПТОГРАФИЯ
3.10.1 ЗАЩИТА КОММУНИКАЦИЙ

Организации должны обеспечивать безопасность данных, проходящих через каналы передачи информации. К таким данным может относиться внутренний трафик, но более важной задачей является защита данных, которые передаются за пределами организации.

Существует четыре элемента защищенной связи

Целостность данных гарантирует, что данное сообщение не было изменено. Целостность обеспечивается с помощью алгоритмов хеширования Message Digest 5 (MD5) или Secure Hash Algorithm (SHA).

Аутентификация источника гарантирует, что сообщение не является поддельным и действительно поступает с заявленного адреса. Многие современные сети обеспечивают аутентификацию с помощью протоколов, таких как код аутентификации сообщений на основе хеша (HMAC).

3.10.1 ЗАЩИТА КОММУНИКАЦИЙ

Конфиденциальность данных гарантирует, что только авторизованные пользователи могут прочитать сообщение. Конфиденциальность данных реализуется с помощью алгоритмов симметричного и асимметричного шифрования.

Невозможность отказа от данных гарантирует, что отправитель не может отказаться от отправленного сообщения или опровергнуть его достоверность. При реализации невозможности отказа используется тот факт, что только у отправителя есть уникальные характеристики или подпись, указывающие, как следует обрабатывать данное сообщение.

Криптографию можно использовать практически везде, где имеет место передача данных. На самом деле сегодня очевидна тенденция к тому, что шифроваться будут все передаваемые данные.

3.10.2 ЦЕЛОСТНОСТЬ ДАННЫХ

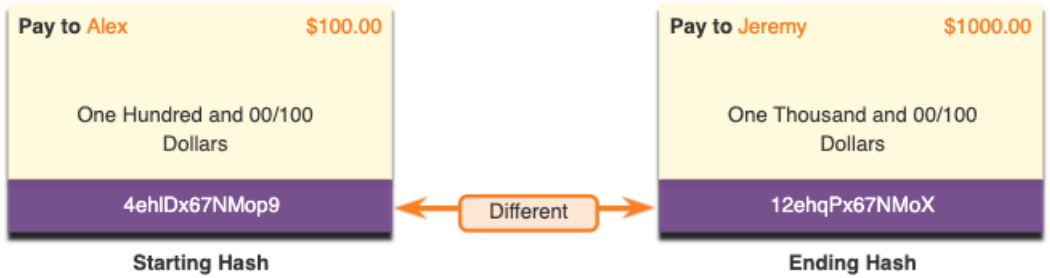
Хеш-функции используются для обеспечения целостности сообщений. Они гарантируют, что данные не были изменены ни случайно, ни преднамеренно.

На рисунке отправитель переводит 100 долл. США Алексу. Отправитель хочет гарантировать, что сообщение не будет изменено на пути к получателю.

Для этого отправляющее устройство использует алгоритм хеширования и рассчитывает хеш-сумму сообщения фиксированной длины 4ehiDx67NMop9.

Затем эта хеш-сумма вкладывается в сообщение и отправляется получателю. Сообщение и хеш-сумма представлены в виде простого текста.

Принимающее устройство удаляет хеш-сумму из сообщения и вводит сообщение в тот же алгоритм хеширования. Если вычисленная хеш-сумма совпадает с хеш-суммой, прикрепленной к сообщению, значит, сообщение не было изменено во время передачи. Если хеш-суммы не равны, целостность сообщения находится под сомнением.



3.10.3 ХЕШ-ФУНКЦИИ

Есть три самые известные хеш-функции.

MD5 с 128-разрядным хешем — односторонняя функция, создающая сообщение с хешем (профилем) длиной 128 бит. MD5 считается устаревшим алгоритмом, который следует использовать только в отсутствии лучших вариантов. Вместо этого используйте SHA-2.

SHA — алгоритм с функциями хеширования, очень похожими на MD5. SHA-1 создает сообщение с 160-разрядным хешем и работает несколько медленнее, чем MD5. Изъяны SHA-1 хорошо известны, и этот алгоритм тоже уже не используется. Используйте SHA-2, когда это возможно.

SHA-2 — включает функции SHA-224 (224 bit), SHA-256 (256 bit), SHA-384 (384 bit), and SHA-512 (512 bit). SHA-256, SHA-384 и SHA-512 — это алгоритмы следующего поколения, которые рекомендуется использовать всегда, когда это возможно.

Хеширование позволяет выявить случайные изменения, но не защищает от намеренного изменения данных. Соответственно, любой, кто имеет доступ к соответствующей хеш-функции, может рассчитать с ее помощью корректную хеш-сумму для любых данных.

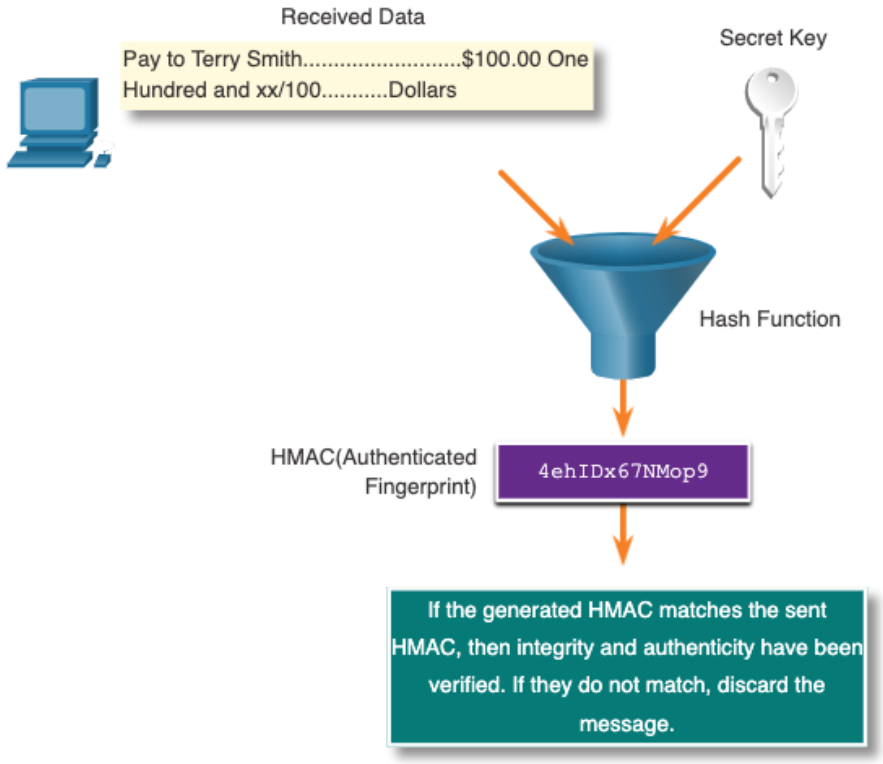
Таким образом, метод хеширования уязвим к атаке через посредника и не защищает передаваемые данные.

3.10.4 АУТЕНТИФИКАЦИЯ ИСТОЧНИКА

Для того чтобы добавить аутентификацию в обеспечение целостности, используется код аутентификации сообщений на основе хеша (**HMAC**).

В вычислении механизма HMAC используется криптографический алгоритм, объединяющий криптографическую хеш-функцию с секретным ключом.

Таким образом, вычислить верную хеш-сумму HMAC может только обладатель секретного ключа. Это свойство позволяет исключить атаку через посредника и аутентифицировать источник данных.

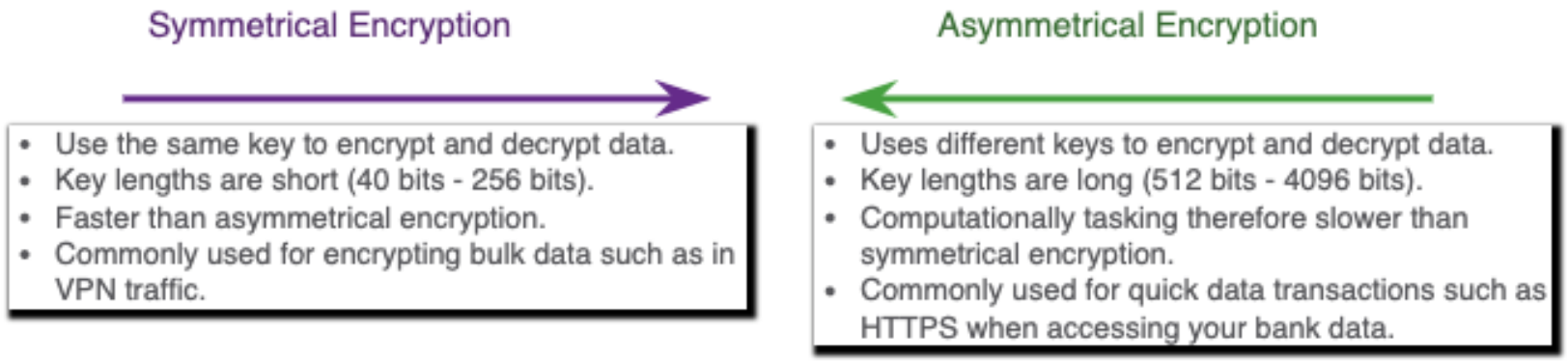


3.10.5 КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ

Для обеспечения конфиденциальности данных существует два класса шифрования. Эти два класса отличаются способом использования ключей.

Симметричные алгоритмы шифрования, такие как (DES), 3DES, и Advanced Encryption Standard (AES) основаны на предположении, что каждой стороне обмена данными известен предварительно согласованный общий ключ. Конфиденциальность данных может также обеспечиваться асимметричными алгоритмами, например алгоритмами Ривеста, Шамира и Адлемана (RSA, Rivest, Shamir, Adleman) и инфраструктурой открытых ключей (PKI, public key infrastructure).

На рисунке показаны некоторые различия между этими алгоритмами шифрования.

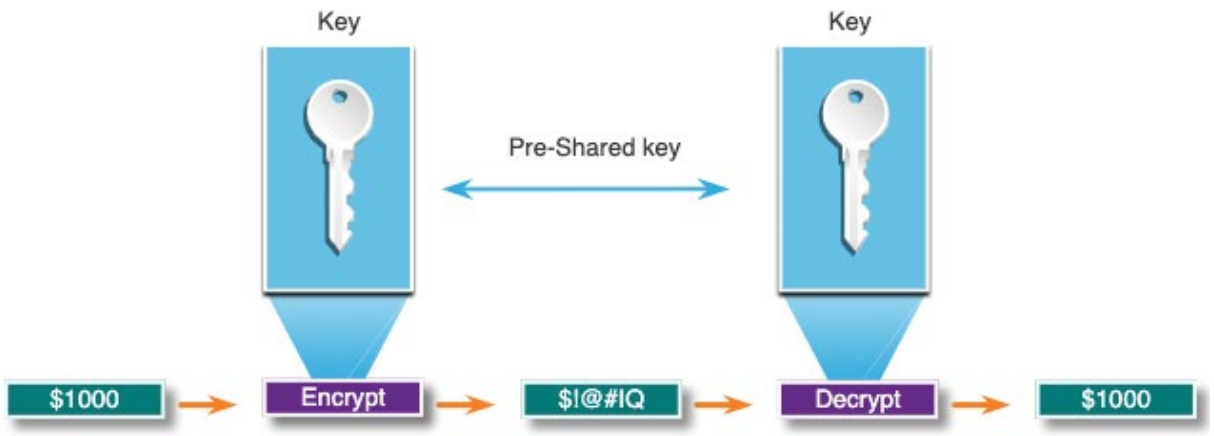


3.10.6 СИММЕТРИЧНОЕ ШИФРОВАНИЕ

Симметричные алгоритмы используют тот же предварительный общий ключ, также называемый секретным ключом, для шифрования и дешифрования данных. Общий ключ известен отправителю и получателю до отправки любых зашифрованных сообщений.

Алгоритмы симметричного шифрования обычно используются с трафиком VPN, потому что они используют меньше ресурсов ЦП, чем алгоритмы асимметричного шифрования.

В алгоритмах симметричного шифрования чем длиннее ключ, тем больше времени займет раскрытие этого ключа. Для того чтобы гарантировать надежность шифрования, следует использовать ключ длиной не менее 128 бит.



3.10.6 СИММЕТРИЧНОЕ ШИФРОВАНИЕ

Симметричные алгоритмы шифрования	Описание
Data Encryption Algorithm (DES)	Это старый алгоритм симметричного шифрования. Его можно использовать в режиме поточного шифрования, но обычно этот алгоритм применяет блочный режим с 64-битными блоками. Потоковый шифр шифрует один байт или один бит за раз.
3DES (Triple DES)	Это более новая версия алгоритма DES, в которой процесс DES повторяется трижды. Он считается очень надежным, если реализация алгоритма предполагает очень малое время жизни ключа.
Advanced Encryption Standard (AES)	Алгоритм AES является надежным и более эффективным по сравнению с 3DES. Это популярный и рекомендованный симметричный алгоритм шифрования. Он предоставляет девять комбинаций длины ключа и блока, используя ключ переменной длины (128, 192 или 256 бит) для шифрования блоков данных длиной 128, 192 или 256 бит.
Алгоритм SEAL (Software-Optimized Encryption Algorithm)	SEAL - быстрый алгоритм симметричного шифрования, являющийся альтернативой алгоритмам DES, 3DES и AES. Оказывает меньшее влияние на производительность ЦП по сравнению с другими программными алгоритмами.
Rivest ciphers (RC) набор алгоритмов	Этот алгоритм был разработан Роном Ривестом. Разработано несколько разновидностей этих алгоритмов, но чаще всего используется RC4. RC4 — это поточный шифр, который используется для обеспечения безопасности веб-трафика в протоколах SSL и TLS.

3.10.7 АСИММЕТРИЧНОЕ ШИФРОВАНИЕ

Алгоритмы асимметричного шифрования, также называемые алгоритмами шифрования с общим ключом, разработаны таким образом, чтобы ключ, который используется для шифрования, отличался от ключа, который используется для расшифровки.
Алгоритмы асимметричного шифрования используют общий ключ и частный ключ. Дополнительный парный ключ необходим для расшифровки. Потому что для расшифровки данных, зашифрованных общим ключом, требуется частный ключ. Этот процесс позволяет с помощью асимметричных алгоритмов обеспечить конфиденциальность, аутентификацию и целостность.
Так как ни у одной из сторон нет общего секретного ключа, необходимо использовать ключи очень большой длины. В асимметричном шифровании используются ключи длиной от 512 до 4096 бит. Ключи длиной 1024 бита и более могут быть надежными, а вот ключи меньшей длины уже считаются ненадежными.

3.10.7 АСИММЕТРИЧНОЕ ШИФРОВАНИЕ

Далее приведены примеры протоколов, в которых используются алгоритмы с асимметричным ключом.

Internet Key Exchange (IKE). Это основной компонент сетей VPN, использующих протокол IPsec.

Secure Socket Layer (SSL). В настоящее время реализуется как TLS стандарта IETF.

Secure Shell (SSH). Этот протокол обеспечивает безопасное, удаленное подключение к сетевым устройствам.

Pretty Good Privacy (PGP). Это компьютерная программа, обеспечивающая криптографическую конфиденциальность и аутентификацию. Она часто используется для повышения безопасности электронной почты.

Асимметричные алгоритмы работают значительно медленнее по сравнению с симметричными. Их работа основана на вычислительных задачах, например на расчете факториалов или дискретных логарифмов очень больших чисел.

Из-за низкой скорости асимметричные алгоритмы обычно используются в механизмах шифрования небольших объемов данных, например, цифровых подписей и обмена ключами.

Алгоритм асимметричного шифрования	Длина ключа	Описание
Алгоритм Диффи — Хеллмана (Diffie-Hellman, DH)	512, 1024, 2048, 3072, 4096	Алгоритм Диффи-Хеллмана позволяет двум сторонам согласовать ключ, который они могут использовать для шифрования отправляемых друг другу сообщений. Безопасность этого алгоритма основывается на предположении, что, хотя любое число можно легко возвести в определенную степень, сложно вычислить, какая степень была использована, на основе данного числа и результата.
Стандарт цифровой подписи (DSS) и алгоритм цифровой подписи (DSA)	512–1024	Стандарт DSS описывает DSA как алгоритм для цифровых подписей. DSA - это алгоритм с общим ключом, основанный на схеме получения цифровой подписи ElGamal. Скорость создания сигнатур аналогична RSA, однако в 10–40 раз ниже для подтверждения.
Алгоритмы шифрования Rivest, Shamir, и Adleman (RSA)	От 512 до 2048	RSA - алгоритм шифрования с открытым ключом, который основан на текущей сложности факторизации больших чисел. Это первый известный алгоритм, подходящий как для подписи, так и для шифрования. Он широко используется в протоколах электронной коммерции и считается надежным при условии использования достаточно длинных ключей и современных реализаций алгоритма.
Алгоритм Эль-Гамаля	512–1024	Алгоритм шифрования с асимметричным ключом для криптографии с открытым ключом, который основывается на согласовании ключей Диффи-Хеллмана. Недостатком системы Эль-Гамаля является существенное увеличение размера зашифрованного сообщения (примерно вдвое по сравнению с исходным сообщением), и по этой причине она используется только для небольших сообщений, таких как секретные ключи.
Методы с использованием эллиптических кривых	160	Метод с использованием эллиптических кривых может использоваться для адаптации многих криптографических алгоритмов, например алгоритмов Диффи-Хеллмана или Эль-Гамаля. Основным преимуществом криптографии на основе эллиптических кривых является существенно меньший размер ключей.

3.10.8 АЛГОРИТМ ДИФФИ-ХЕЛЛМАНА

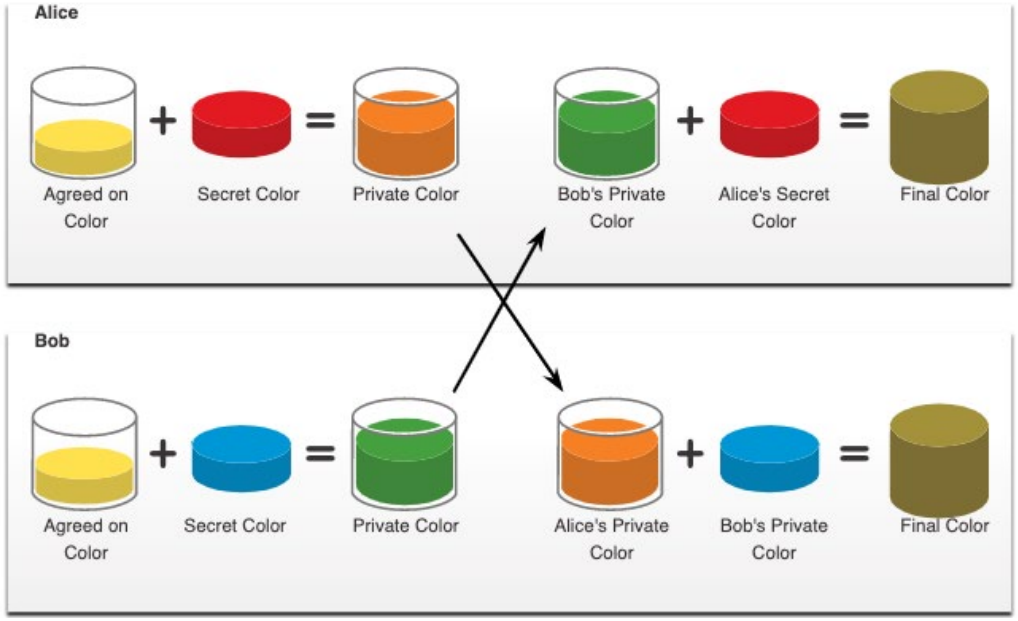
Алгоритм Диффи-Хеллмана (DH) — это математический асимметричный алгоритм, который позволяет двум компьютерам создать одинаковый общий секретный ключ без предварительного взаимодействия. Отправитель и получатель в действительности никогда не обмениваются этим новым общим ключом.

Ниже приведены три стандартных примера использования алгоритма DH.
1. Обмен данными по сети VPN на основе IPsec.
2. Шифрование данных в Интернете с помощью протокола SSL или TLS.
3. Обмен данными по протоколу SSH.

Безопасность алгоритма DH основана на том факте, что в своих расчетах он использует невероятно большие числа.
К сожалению, системы с асимметричными ключами работают слишком медленно и не могут применяться для шифрования больших объемов данных. Именно поэтому стандартной практикой является шифрование большого объема трафика с помощью симметричного алгоритма, например 3DES или AES, и применение алгоритма Диффи-Хеллмана для создания ключей, которые будут использоваться алгоритмом шифрования.

3.10.8 АЛГОРИТМ ДИФФИ-ХЕЛЛМАНА

1. Вместо сложных длинных чисел на рисунке используются цвета, чтобы упростить представление процесса согласования ключей Диффи-Хеллмана. Обмен ключами DH начинается с того, что Алиса и Боб согласуют произвольный общий цвет, который не нужно хранить в секрете. В нашем примере это желтый цвет.
2. Далее Алиса и Боб выбирают свой секретный цвет. Алиса выбрала красный, а Боб — синий. Они не должны сообщать эти цвета никому. Секретный цвет представляет выбранный секретный частный ключ каждой стороны.
3. Алиса и Боб теперь смешивают общий цвет (желтый) со своим соответствующим секретным цветом, создавая частный цвет. Таким образом, Алиса смешает свой желтый цвет с красным и получит частный оранжевый цвет. Боб смешает желтый и синий и получит частный зеленый цвет.



3.10.8 АЛГОРИТМ ДИФФИ-ХЕЛЛМАНА

4. Алиса отправляет Бобу свой частный цвет (оранжевый), а Боб отправляет Алисе свой частный цвет (зеленый).
5. Алиса и Боб смешивают полученный ими цвет с собственным, исходным секретным цветом (красным для Алисы и синим для Боба). В результате получается окончательный коричневый цвет смеси, такой как окончательный цвет смеси у партнера. Коричневый цвет представляет итоговый общий секретный ключ Алисы и Боба.