OTUS

Онлайн образование

otus.ru

Проверить, идет ли запись

Меня хорошо видно && слышно?

Основы сетевой безопасности

Андрей Рукин

Инженер ИТ

arukin@m-pr.tv

Правила вебинара

Активно участвуем

Задаем вопросы в чат

Вопросы вижу в чате,
могу ответить не сразу

Условные обозначения

Индивидуально

Время, необходимое на активность

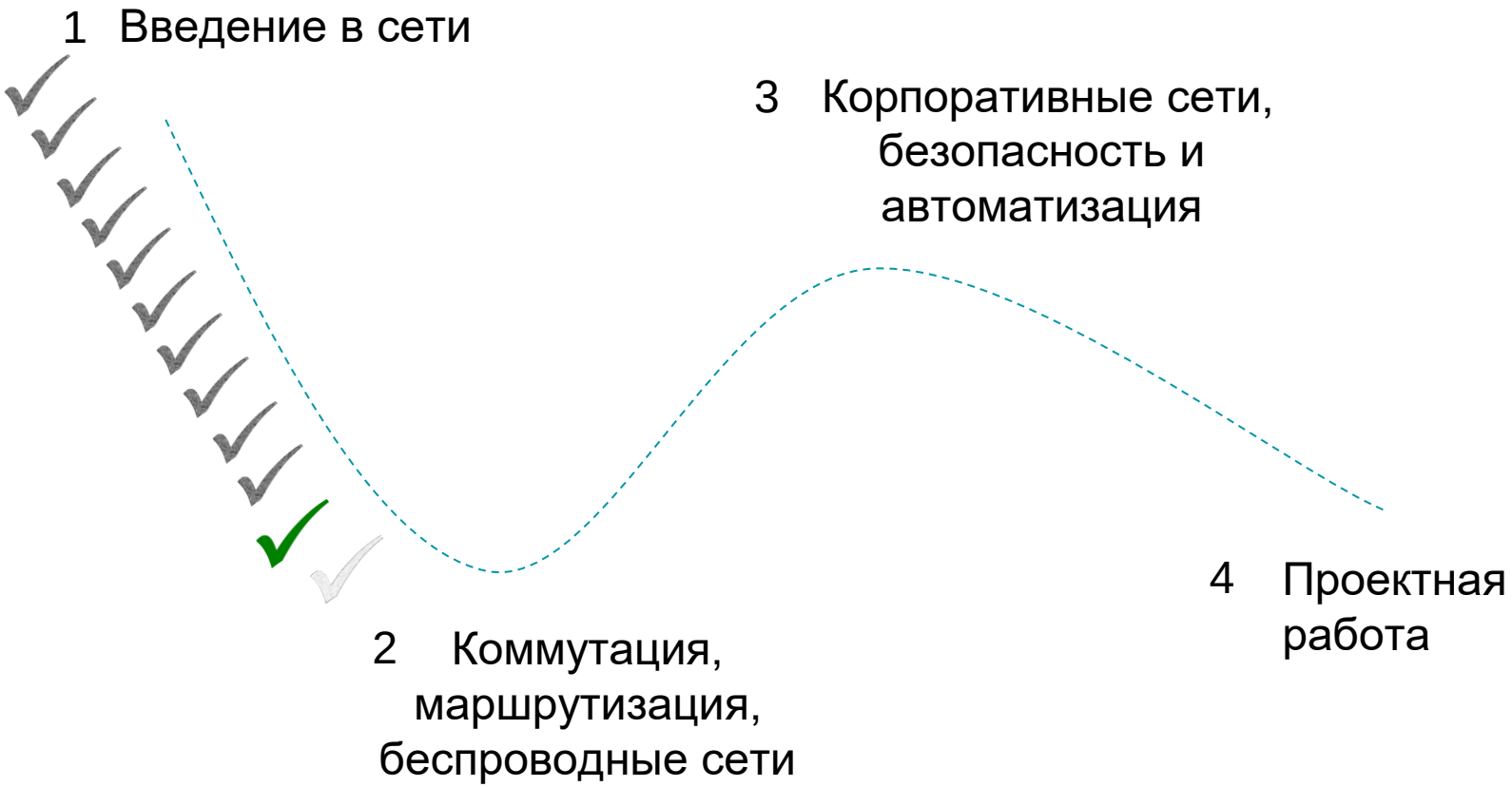
Пишем в чат

Говорим голосом

Документ

Ответьте себе или задайте вопрос

Карта курса


1 Введение в сети
2 Коммутация, маршрутизация, беспроводные сети
3 Корпоративные сети, безопасность и автоматизация
4 Проектная работа

Угрозы и уязвимости безопасности

Типы угроз

Атака на сеть может иметь разрушительные последствия с потерей времени и средств в результате повреждения или хищения важной информации и ресурсов.

Злоумышленники могут получить доступ к сети, используя уязвимости программного обеспечения, атаки на аппаратное обеспечение, подбор имени пользователя и пароля. Злоумышленников, которые получают доступ, внося изменения в ПО или используя его уязвимости, называют хакерами.

Хакер, получивший доступ к сети, сразу становится источником четырех видов угроз.

- Кража информации
- Утечка данных и их неправомерное использование
- Кража персональных данных
- Прекращение обслуживания (DOS)

Типы уязвимостей

Уязвимость — степень незащищенности, свойственная каждой сети и устройству. Некоторая степень уязвимости присуща маршрутизаторам, коммутаторам, настольным компьютерам, серверам и даже устройствам безопасности. Как правило, атакам подвержены такие оконечные устройства, как серверы и настольные компьютеры.

Существует три основных типа уязвимостей:

- Технологические уязвимости могут включать в себя слабости протокола TCP/IP, слабые места операционной системы и слабости сетевого оборудования.
- Уязвимости конфигурации могут включать незащищенные учетные записи пользователей, системные учетные записи с ненадежными паролями, неправильно настроенные интернет-службы, незащищенные параметры по умолчанию и неправильно настроенное сетевое оборудование.
- Уязвимости политики безопасности могут включать в себя отсутствие письменной политики безопасности, политики, отсутствие непрерывности проверки подлинности, неприменение логических элементов управления доступом, установку программного и аппаратного обеспечения и изменения, не соответствующие политике, а также несуществующий план аварийного восстановления.

Все три типа уязвимостей могут быть причиной атак, включая атаки с использованием вредоносного ПО и сетевые атаки.

Физическая безопасность

Злоумышленник может блокировать доступ к сетевым ресурсам, если их можно повредить на физическом уровне. Имеется четыре класса угроз:

- **Угрозы для аппаратного обеспечения** — физическое повреждение серверов, маршрутизаторов, коммутаторов, кабельных линий и рабочих станций.
- **Угрозы со стороны окружающей среды** — предельные температуры (слишком высокие или слишком низкие) или крайние значения влажности (слишком низкая или слишком высокая)
- **Электрические угрозы** — всплески напряжения, недостаточное напряжение в электрической сети (провалы напряжения), колебания напряжения (шум) и полное отключение электропитания
- **Эксплуатационные угрозы** — ненадлежащее обращение с ключевыми электрическими компонентами (электростатический разряд), нехватка важных запасных деталей, неправильная прокладка кабелей и ненадлежащая маркировка.

Для решения этих проблем необходимо разработать и осуществить хороший план обеспечения физической безопасности.

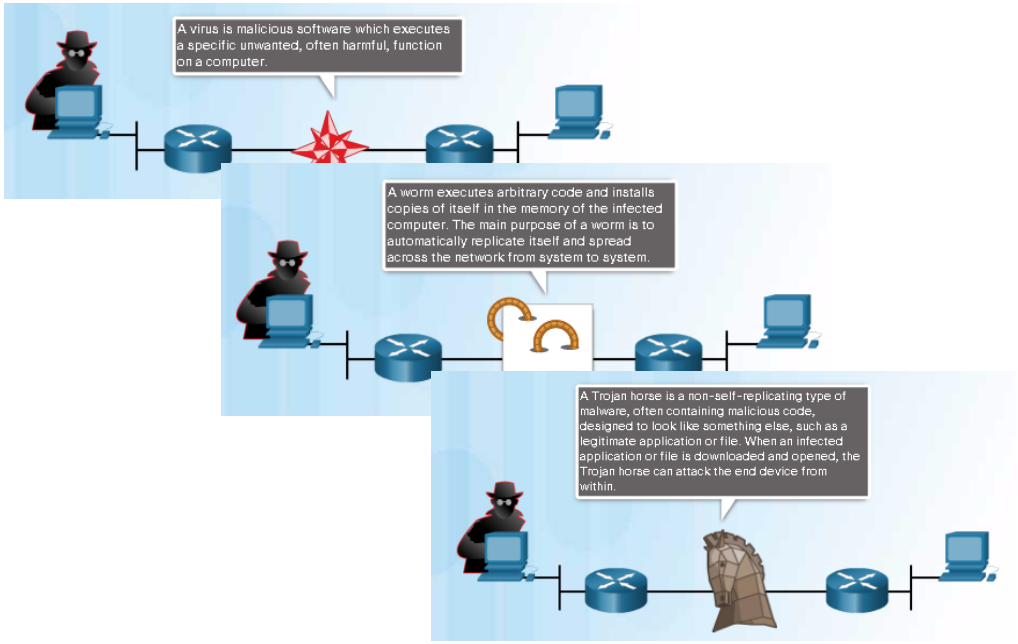
Типы вредоносных программ

Вредоносное ПО - это сокращение от вредоносного программного обеспечения или вредоносного кода. Это код или программное обеспечение, специально предназначенные для повреждения, нарушения работы, кражи или совершения каких-либо других вредоносных или незаконных действий в отношении данных, хостов или сетей.

Конечные устройства особенно подвержены вредоносным атакам.

Три наиболее распространенных типа вредоносных программ:

- вирус
- червь
- троянский конь



Вирусы

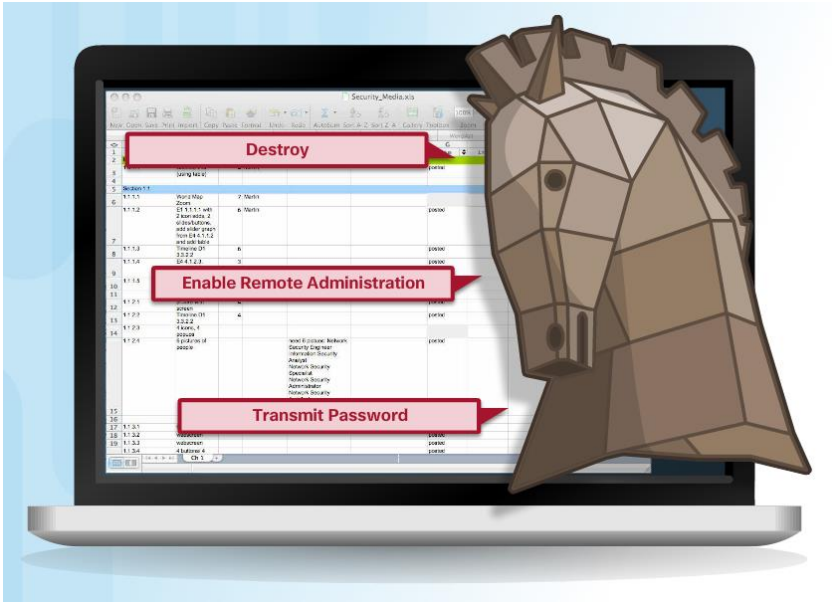
Вирус-это тип вредоносного ПО, которое распространяется, вставляя свою копию в другую программу. После запуска программы вирусы распространяются с одного компьютера на другой, заражая их. Для распространения большинства вирусов требуется действие человека.

Простой вирус может установить себя в первой строке кода исполняемого файла. При активации вирус может проверить диск на наличие других исполняемых файлов, чтобы заразить все файлы, которые он еще не заразил.

Вирусы также могут быть запрограммированы на мутирование, чтобы избежать обнаружения.

Большинство вирусов в настоящее время распространяются с помощью USB-накопителей, компакт-дисков, DVD-дисков, сетевых ресурсов и электронной почты.

Троянские кони



Троянский конь-это программное обеспечение, которое кажется законным, но содержит вредоносный код, который использует привилегии пользователя, который его запускает.

Часто трояны обнаруживаются прикрепленными к онлайн-играм. Пользователи обычно обманом загружают и запускают троянского коня в своих системах. Во время игры пользователь не заметит проблемы. В фоновом режиме троянский конь был установлен в системе пользователя. Вредоносный код от троянского коня продолжает работать даже после закрытия игры.

Концепция троянского коня очень гибка. Это может привести к немедленному повреждению, обеспечить удаленный доступ к системе или загрузку вредоносного кода.
Он также может выполнять удаленные действия в соответствии с инструкциями, например "присылайте мне файл пароля один раз в неделю".

Классификация троянских коней

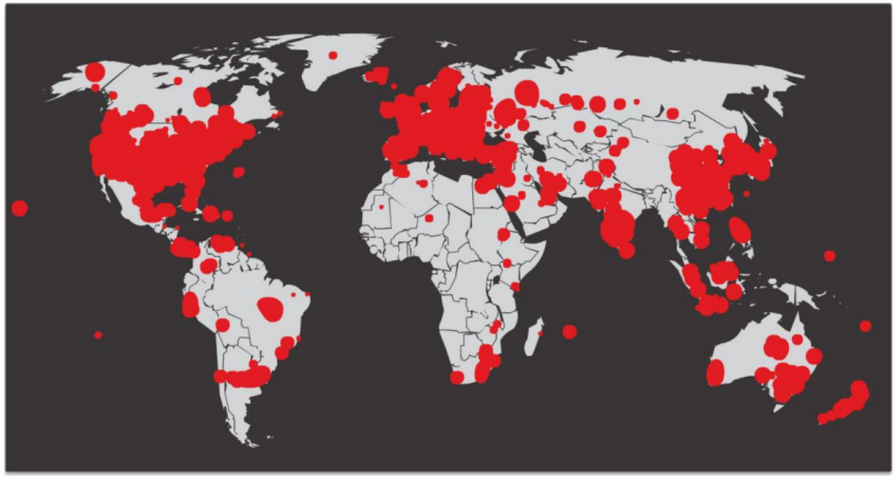
Троянские кони обычно классифицируются в соответствии с ущербом, который они наносят, или способом, которым они нарушают систему, как показано в таблице.

Тип Троянского коня	Описание
Удаленный доступ	Включает несанкционированный удаленный доступ.
Передача данных	Предоставляет субъекту угрозы конфиденциальные данные, такие как пароли.
Разрушительный	Повреждает или удаляет файлы.
Прокси	Использует компьютер жертвы в качестве исходного устройства для запуска атак и выполнения других незаконных действий.
FTP	Включает несанкционированную передачу файлов на конечных устройствах.
Отключение программного обеспечения безопасности	Останавливает работу антивирусных программ или брандмауэров.
Отказ в обслуживании (DoS)	Замедляет или останавливает сетевую активность.
Кейлоггер	Активно пытается украсть конфиденциальную информацию, такую как номера кредитных карт, записывая нажатия клавиш, которые были введены в веб-форму.

Черви

Компьютерные черви похожи на вирусы, потому что они размножаются и могут нанести один и тот же тип ущерба. В частности, черви реплицируют себя, независимо используя уязвимости в сетях. Черви могут замедлять работу сетей по мере их распространения от системы к системе.

SQL Slammer, известный как червь, который «съел» Интернет, был атакой типа "Отказ в обслуживании" (DoS), которая использовала ошибку переполнения буфера в SQL-сервере Microsoft. На пике своего развития количество зараженных серверов удваивалось каждые 8,5 секунды. Он заразил более 250 000 хостов в течение 30 минут, как показано на рисунке.



Компоненты червя

Большинство атак червя состоят из трех компонентов:

•**Использование уязвимости** - Червь устанавливает себя с помощью механизма эксплойта, такого как вложение электронной почты, исполняемый файл или троянский конь, в уязвимую систему.

•**Механизм распространения** - Получив доступ к устройству, червь реплицируется и находит новые цели.

•**Полезная нагрузка** - Любой вредоносный код, который приводит к какому-то действию, является полезной нагрузкой. Чаще всего это используется для создания бэкдора, который позволяет субъекту угрозы получить доступ к зараженному хосту, или для создания DoS-атаки.

Червячные компоненты (продолжение)

Техника размножения, используемая Code Red червем, показана на рисунке.

Вымогатели

В настоящее время наиболее распространенной вредоносной программой является **программа-вымогатель.**

- Вымогатели-это вредоносные программы, которые отказывают в доступе к зараженной компьютерной системе или ее данным. Затем киберпреступники требуют оплаты за освобождение компьютерной системы.
- Вымогатели эволюционировали, чтобы стать самым прибыльным типом вредоносных программ в истории.
- Существуют десятки вариантов вымогателей.
- Вымогатели часто используют алгоритм шифрования для шифрования системных файлов и данных.
- Платежи обычно оплачиваются в биткойнах, потому что пользователи биткойнов могут оставаться анонимными.
- Электронная почта и вредоносная реклама, также известная как вредоносная реклама, являются переносчиками для вымогателей.
- Также используется социальная инженерия.

Другие вредоносные программы

Вот некоторые примеры разновидностей современных вредоносных программ:

Тип вредоносного ПО	Описание
Шпионское ПО	Используется для сбора информации о пользователе и передачи ее другому лицу без согласия пользователя. Шпионское ПО может быть системным монитором, троянским конем, рекламным ПО, отслеживающими файлами cookie и регистраторами ключей.
Реклама	Отображает раздражающие всплывающие окна для получения дохода для своего автора. Вредоносная программа может анализировать интересы пользователей, отслеживая посещенные веб-сайты. Затем он может отправлять всплывающую рекламу, относящуюся к этим сайтам.
Scareware	Включает в себя мошенническое программное обеспечение, которое использует социальную инженерию, чтобы шокировать или вызвать беспокойство, создавая восприятие угрозы. Как правило, он направлен на ничего не подозревающего пользователя и пытается убедить его заразить компьютер, приняв меры по устранению фиктивной угрозы.
Фишинг	Попытки убедить людей разглашать конфиденциальную информацию. Примеры включают получение электронного письма от своего банка с просьбой разгласить свой счет и PIN-коды.
Руткиты	Установлен в скомпрометированной системе. После установки он продолжает скрывать свое вторжение и предоставлять привилегированный доступ субъекту угрозы.

Распространенное вредоносное поведение

Компьютеры, зараженные вредоносными программами, часто проявляют один или несколько из следующих симптомов:

•Появление странных файлов, программ или значков на рабочем столе
•Антивирусные программы и брандмауэры отключаются или перенастраивают свои настройки
•Экран компьютера зависает или система выходит из строя
•Электронные письма спонтанно отправляются по вашему списку контактов без вашего ведома
•Файлы были изменены или удалены
•Увеличение использования процессора и/или памяти
•Проблемы с подключением к сетям
•Низкая скорость работы компьютера или веб-браузера
•Запущенные неизвестные процессы или службы
•Неизвестные TCP или UDP порты открыты
•Подключения к хостам в Интернете осуществляются без каких-либо действий пользователя
•Другое странное поведение компьютера

Вопросы?

Ставим “+”,
если вопросы есть

Ставим “–”,
если вопросов нет

Сетевые атаки

Типы сетевых атак

Чтобы смягчить эффект атаки, полезно сначала классифицировать различные типы атак. Классифицируя сетевые атаки, можно рассматривать типы атак, а не отдельные атаки.

Хотя стандартизированного способа классификации сетевых атак не существует, метод, используемый в этом курсе, классифицирует атаки по трем основным категориям:

- **Разведывательные атаки**
- **Атаки доступа**
- **DoS-атаки**

Разведывательные атаки

Разведка-это сбор информации. Субъекты угроз используют рекогносцировочные (или разведывательные) атаки для несанкционированного обнаружения и картирования систем, служб или уязвимостей. Разведывательные атаки предшествуют атакам доступа или DoS-атакам. Некоторые методы, используемые злоумышленниками для проведения разведывательных атак, описаны в таблице.

Техника	Описание
Выполнение информационного запроса целевого объекта	Субъект угрозы ищет исходную информацию о цели. Можно использовать различные инструменты, включая поиск Google, веб-сайт организаций, whois и многое другое.
Инициировать пинг-проверку целевой сети	Информационный запрос обычно раскрывает сетевой адрес цели. Теперь субъект угрозы может инициировать проверку ping, чтобы определить, какие IP-адреса активны.
Инициировать сканирование портов активных IP - адресов	Он используется для определения доступных портов или служб. Примеры сканеров портов включают Nmap, SuperScan, Angry IP Scanner и NetScanTools.
Запуск сканеров уязвимостей	Это делается для запроса идентифицированных портов, чтобы определить тип и версию приложения и операционной системы, запущенных на хосте. Примеры инструментов включают Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT и Open VAS.
Запустить инструменты эксплуатации уязвимостей	Теперь субъект угрозы пытается обнаружить уязвимые службы, которые могут быть использованы. Существует множество инструментов эксплуатации уязвимостей, включая Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit и Netsparker.

Атаки доступа

Атаки доступа используют известные уязвимости в службах аутентификации, FTP-службах и веб-службах. Цель этого типа атаки-получить доступ к веб-учетным записям, конфиденциальным базам данных и другой конфиденциальной информации.

Техника	Описание
Парольные атаки	При парольной атаке субъект угрозы пытается обнаружить критические системные пароли с помощью различных методов.
Атаки спуфинга	При атаках спуфинга устройство субъекта угрозы пытается выдать себя за другое устройство, фальсифицируя данные. Распространенные атаки спуфинга включают IP-спуфинг, MAC-спуфинг и DHCP-спуфинг.
Эксплуатация доверия	При атаке с использованием доверия субъект угрозы использует несанкционированные привилегии для получения доступа к системе, что может поставить под угрозу цель.
Перенаправление портов	При атаке с перенаправлением портов субъект угрозы использует скомпрометированную систему в качестве базы для атак на другие цели.
Человек посередине	При атаке "человек посередине" субъект угрозы располагается между двумя законными сущностями, чтобы считывать или изменять данные, передаваемые между двумя сторонами.
Атака переполнения буфера	При атаке переполнения буфера субъект угрозы использует буферную память и переполняет ее неожиданными значениями. Это обычно делает систему неработоспособной, что приводит к DoS-атаке.

Атаки социальной инженерии

Социальная инженерия-это атака доступа, которая пытается манипулировать людьми для выполнения действий или разглашения конфиденциальной информации. Информация о методах социальной инженерии приведена в таблице.

Атака	Описание
Предлог	Субъект угрозы делает вид, что ему нужны личные или финансовые данные для подтверждения личности получателя.
Фишинг	Субъект угрозы отправляет мошенническое электронное письмо, замаскированное под законный, надежный источник, чтобы обмануть получателя и заставить его установить вредоносное ПО на свое устройство или поделиться личной или финансовой информацией.
Направленный фишинг	Субъект угрозы создает целевую фишинговую атаку, предназначенную для конкретного человека или организации.
Спам	Также известный как нежелательная почта, это нежелательная почта, которая часто содержит вредоносные ссылки, вредоносные программы или вводящий в заблуждение контент.
Что-то за кое-что	Иногда называемый “Quid pro quo”, это когда субъект угрозы запрашивает личную информацию у какой-либо стороны в обмен на что-то вроде подарка.
Приманка	Субъект угрозы оставляет зараженную вредоносным ПО флешку в общедоступном месте. Жертва находит диск и, ничего не подозревая, вставляет его в свой ноутбук, непреднамеренно устанавливая вредоносное ПО.
Маска	В этом типе атаки субъект угрозы притворяется кем-то другим, чтобы завоевать доверие жертвы.

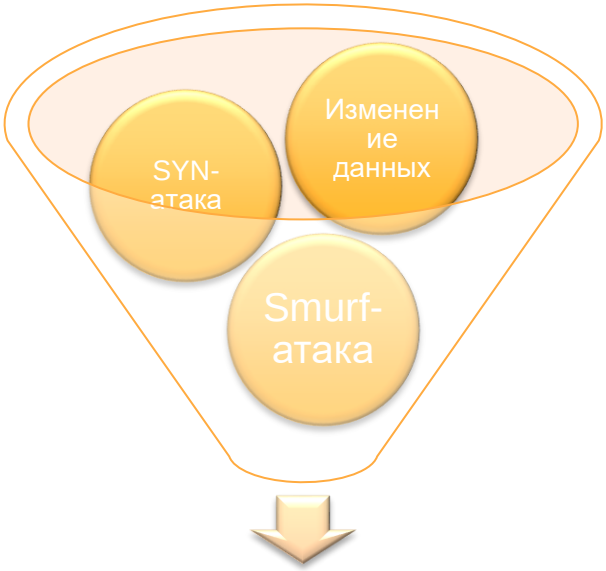
Атаки социальной инженерии (продолжение)

Атака социальной инженерии	Описание
Сесть на хвост	Это когда субъект угрозы быстро следует за уполномоченным лицом в безопасное место, чтобы получить доступ к защищенной зоне.
Плечевой серфинг	Субъект угрозы незаметно заглядывает кому-то через плечо, чтобы украсть его пароли или другую информацию.
Залезть в мусорный контейнер	Здесь субъект угрозы роется в мусоре, чтобы обнаружить конфиденциальные документы.

Укрепление самого слабого звена

Кибербезопасность сильна лишь настолько, насколько ее самое слабое звено. Поскольку компьютеры и другие устройства, подключенные к Интернету, стали неотъемлемой частью нашей жизни, они больше не кажутся чем-то особенным.

Самым слабым звеном в кибербезопасности может быть персонал внутри организации, а социальная инженерия является серьезной угрозой безопасности. Из-за этого одной из наиболее эффективных мер безопасности, которые может принять организация, является обучение ее персонала и создание “культуры безопасности”.



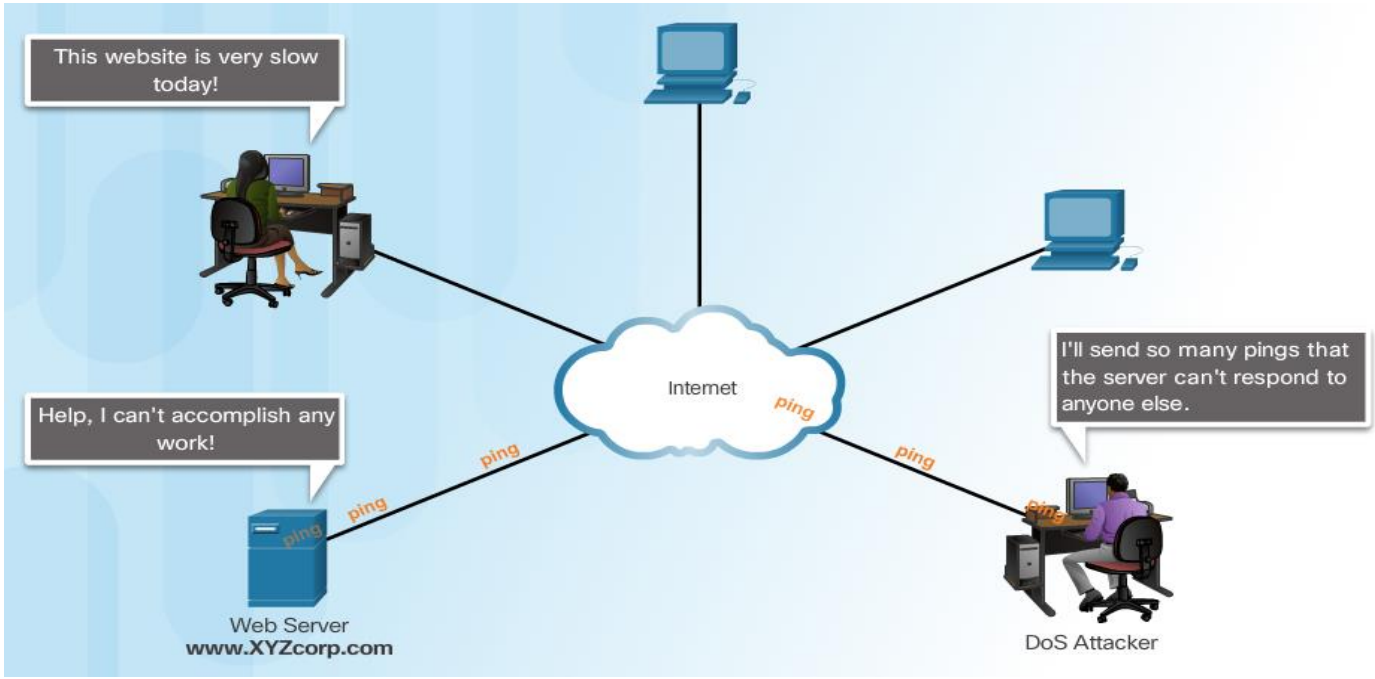
Отказ в обслуживании, переполнение буфера и методы сокрытия

DoS-и DDoS-атаки

Атака типа "Отказ в обслуживании" (DoS) создает своего рода прерывание работы сетевых служб для пользователей, устройств или приложений. Существует два основных типа DoS - атак:

- **Лавинное количество трафика**
- **Умышленно подготовленные пакеты**

Распределенная DoS-атака (DDoS) похожа на DoS-атаку, но она исходит из нескольких скоординированных источников.



Компоненты DDoS-атак

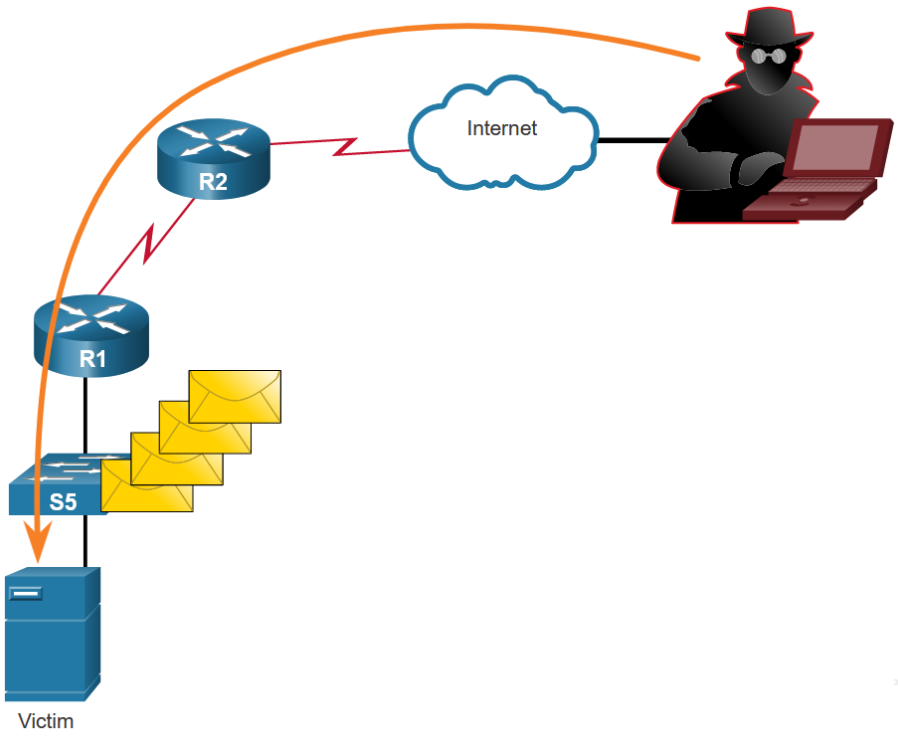
Если субъекты угрозы могут скомпрометировать многие хосты, они могут выполнить распределенную DoS-атаку (DDoS). DDoS-атаки аналогичны по своему замыслу DoS-атакам, за исключением того, что DDoS-атака увеличивается по масштабам и сложнее купируется, поскольку она исходит из нескольких скоординированных источников. Для описания компонентов DDoS-атаки используются следующие термины:

Компонент	Описание
зомби	Это относится к группе скомпрометированных хостов (агентов). Эти хосты запускают вредоносный код, называемый роботами (ботами). Вредоносная программа зомби постоянно пытается самовоспроизводиться, как червь.
боты	Боты-это вредоносное ПО, предназначенное для заражения хоста и связи с обработчиком системы. Боты также могут регистрировать нажатия клавиш, собирать пароли, захватывать и анализировать пакеты и многое другое.
ботнет	Это относится к группе зомби, которые были заражены с помощью самораспространяющихся вредоносных программ (ботов) и контролируются обработчиками.
обработчики	Это относится к главному командно-управляющему серверу (CnC или C2), управляющему группами зомби. Создатель ботнета может использовать Internet Relay Chat (IRC) или веб-сервер на сервере C2 для удаленного управления зомби.
ботмастер	Это субъект угрозы, который контролирует ботнет и обработчики.

Атака переполнения буфера

Цель субъекта угрозы при использовании DoS-атаки с переполнением буфера состоит в том, чтобы найти недостаток системной памяти на сервере и использовать его. Использование буферной памяти путем переполнения ее неожиданными значениями обычно выводит систему из строя, создавая DoS-атаку.

Подсчитано, что одна треть вредоносных атак является результатом переполнения буфера.



Методы сокрытия

Некоторые из методов сокрытия, используемых субъектами угрозы, включают:

Способ	Описание
Шифрование и туннелирование	Этот метод сокрытия использует туннелирование для шифрования вредоносных файлов. Это затрудняет обнаружение и идентификацию вредоносного ПО многими методами обнаружения безопасности. Туннелирование может означать сокрытие украденных данных внутри легитимных пакетов.
Исчерпание ресурсов	Этот метод сокрытия делает целевой хост слишком занятым, чтобы правильно использовать методы обнаружения безопасности.
Фрагментация трафика	Этот метод сокрытия разбивает вредоносную полезную нагрузку на более мелкие пакеты, чтобы обойти обнаружение сетевой безопасности. После того как фрагментированные пакеты обходят систему обнаружения безопасности, вредоносная программа собирается заново и может начать отправлять конфиденциальные данные из сети.
Неверная интерпретация на уровне протокола	Этот метод сокрытия возникает, когда сетевые средства защиты неправильно обрабатывают такие функции PDU, как контрольная сумма или значение TTL. Это может заставить брандмауэр игнорировать пакеты, которые он должен проверить.
Замещение трафика	В этом методе сокрытия субъект угрозы пытается обмануть IP-адрес, запутывая данные в полезной нагрузке. Это делается путем кодирования его в другом формате. Например, субъект угрозы может использовать кодированный трафик в Unicode вместо ASCII. IPS не распознает истинный смысл данных, но целевая конечная система может считывать их.

Методы сокрытия (продолжение)

Способ	Описание
Вставка трафика	Аналогично подмене трафика, но субъект угрозы вставляет дополнительные байты данных в последовательность вредоносных данных. Правила IPS пропускают вредоносные данные, принимая полную последовательность данных.
Поворотный	Этот метод предполагает, что субъект угрозы скомпрометировал внутренний хост и хочет расширить свой доступ в скомпрометированную сеть. Примером может служить субъект угрозы, который получил доступ к паролю администратора на скомпрометированном хосте и пытается войти на другой хост, используя те же учетные данные.
Руткиты	Руткит - это сложный инструмент злоумышленника, используемый опытными участниками угроз. Он интегрируется с самыми низкими уровнями операционной системы. Когда программа пытается перечислить файлы, процессы или сетевые подключения, руткит представляет очищенную версию выходных данных, устраняя любые компрометирующие выходные данные. Цель руткита - полностью скрыть деятельность злоумышленника в локальной системе.
Прокси	Сетевой трафик может быть перенаправлен через промежуточные системы, чтобы скрыть конечный пункт назначения украденных данных. Таким образом, известные команды и средства управления не могут быть заблокированы предприятием, поскольку назначение прокси-сервера выглядит безвредным. Кроме того, если данные украдены, место назначения украденных данных может быть распределено между многими прокси-серверами, таким образом, не привлекая внимания к тому факту, что один неизвестный пункт назначения служит местом назначения для больших объемов сетевого трафика.

Вопросы?

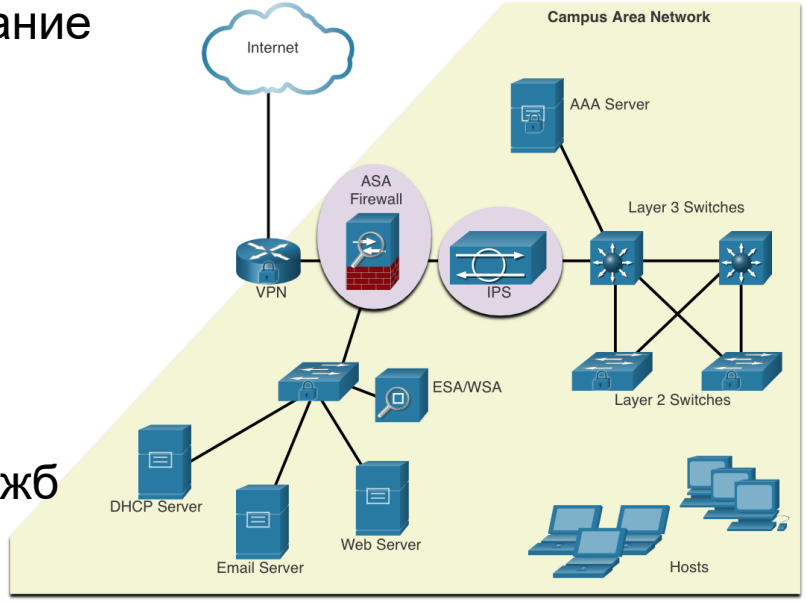
Ставим “+”,
если вопросы есть

Ставим “–”,
если вопросов нет

Защита от сетевых атак

Углубленный подход к защите подход к защите

Чтобы снизить уровень сетевых атак, сначала необходимо обеспечить безопасность устройств, включая маршрутизаторы, коммутаторы, серверы и хосты. Одним из решений является использование углубленного подхода к обеспечению безопасности, также известного как многоуровневый подход. Такой подход предполагает совместную работу сетевых устройств и сервисов.



Для защиты пользователей и активов от угроз TCP/IP реализовано несколько устройств и служб безопасности.

- VPN
- Межсетевой экран ASA
- IPS
- ESA/WSA
- Сервер AAA

Сохранение резервных копий

Резервное копирование данных —эффективный способ защиты данных от потери. Регулярно выполняйте резервное копирование, как определено в политике безопасности. Резервные копии данных обычно хранятся отдельно, чтобы защитить носитель с резервными копиями на случай, если что-либо произойдет в основном помещении.

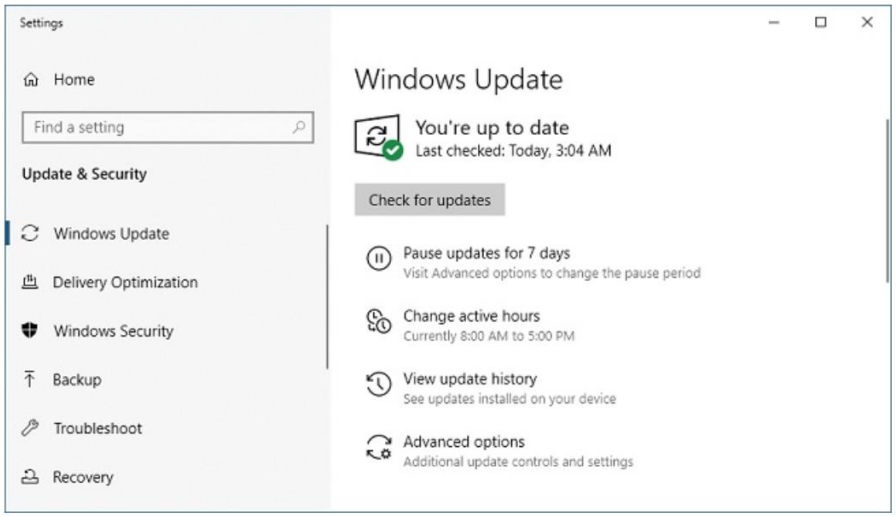
В таблице приведены соображения по резервному копированию и их описания.

Параметр	Описание
Частота	•Регулярно выполняйте резервное копирование, как определено в политике безопасности. •Полное резервное копирование может занять длительное время.
Хранение	•Необходимо переносить резервные копии в автономное хранилище ежедневно, еженедельно или ежемесячно в соответствии с политикой безопасности.
Безопасность	•Резервные копии должны быть защищены с помощью надежных паролей. Пароль необходим для восстановления данных.
Проверка	•Всегда проверяйте резервные копии, чтобы обеспечить целостность данных и проверить процедуры восстановления файлов.

Обновление и установка исправлений

По мере появления нового вредоносного ПО предприятиям рекомендуется постоянно следить за обновлением антивирусного ПО до последних версий.

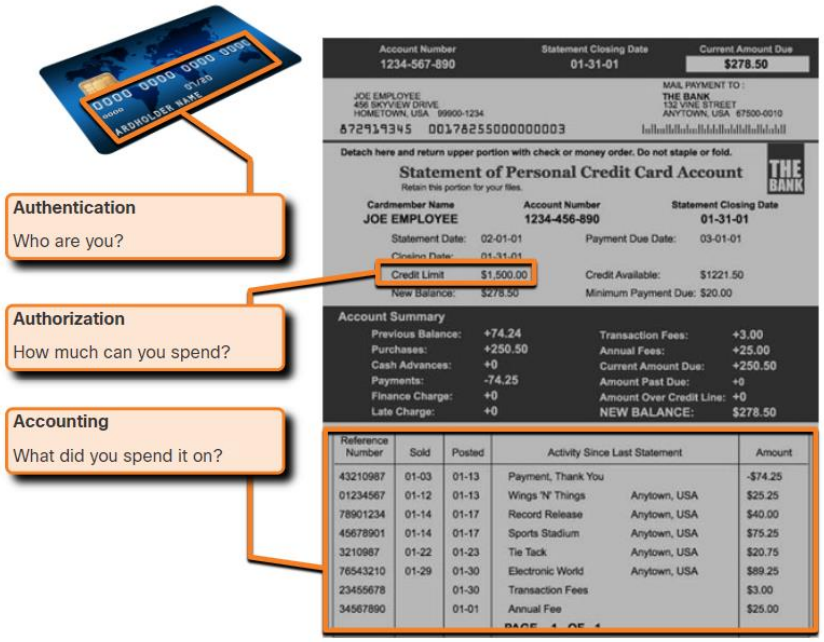
- Наиболее действенный метод минимизации последствий атаки вируса-червя — загрузить обновления для системы безопасности с сайта поставщика ОС и установить соответствующие обновления на все уязвимые копии систем.
- Одно из решений для управления критически важными исправлениями безопасности заключается в том, чтобы убедиться, что все конечные системы автоматически загружают обновления.



Аутентификация, авторизация и учет

Такие службы по обеспечению сетевой безопасности, как аутентификация, авторизация и учет (AAA), являются базовой инфраструктурой, которая устанавливает средства контроля доступа на каком-либо сетевом устройстве.

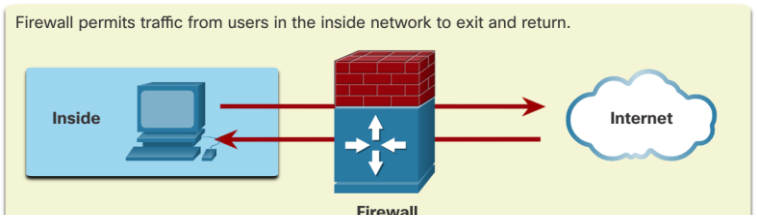
- Сочетание служб аутентификации, авторизации и учета — это метод, позволяющий контролировать вход разрешенных пользователей (аутентификация), какие действия они могут выполнять, находясь в сети (авторизация), а также следить за их действиями во время доступа к сети (учет).
- Концепция служб аутентификации, авторизации и учета (AAA) похожа на использование кредитной карты.

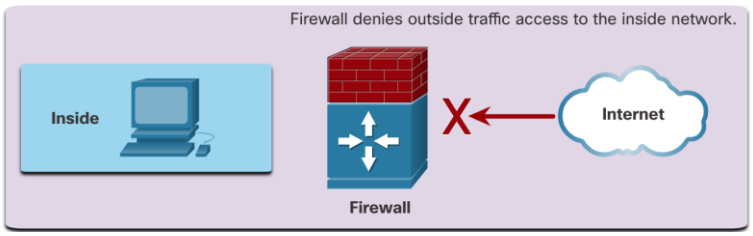


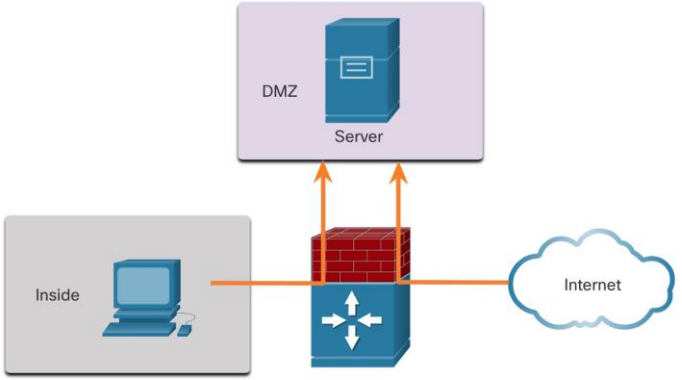
Межсетевые экраны

Межсетевой экран ставится между двумя (или более) сетями и контролирует трафик между ними, а также позволяет предотвратить несанкционированный доступ.

Межсетевой экран может позволить внешним пользователям управлять доступом к определенным службам. Например, серверы, доступные внешним пользователям, обычно размещаются в специальной сети, которая называется демилитаризованной зоной (DMZ). DMZ позволяет администратору применять определенные политики для хостов, подключенных к этой сети.







Типы межсетевых экранов

Решения для межсетевых экранов собраны в различные комплекты. В брандмауэрах используются различные методы для определения разрешения или запрета доступа к сети. В этот список входят следующие продукты:

- **Фильтрация пакетов** — запрет или разрешение доступа на основе IP- или MAC-адресов.
- **Фильтрация по приложениям** — запрет или разрешение доступа для конкретных типов приложений на основе номеров портов.
- **Фильтрация по URL-адресам** — запрет или разрешение доступа к веб-сайтам на основе конкретных URL-адресов или ключевых слов.
- **Анализ пакетов с учетом состояний соединений (SPI)** — входящие пакеты должны представлять собой легитимные отклики на запросы внутренних узлов. Незапрошенные пакеты блокируются, если они не разрешены в явном виде. SPI также предоставляет возможность распознавать и блокировать конкретные типы атак, например атаку типа «отказ в обслуживании» (DoS-атака).

Безопасность оконечных устройств

Оконечное устройство, или узел, представляет собой отдельную компьютерную систему или устройство, которое выступает в роли клиента сети. К наиболее распространенным оконечным устройствам относятся ноутбуки, настольные компьютеры, серверы и смартфоны и планшеты.

Защита оконечных устройств — одна из наиболее сложных задач, входящих в обязанности администратора сети, поскольку в данном случае имеет значение человеческий фактор. Компании необходимо разработать и тщательно задокументировать соответствующие политики и ознакомить с ними сотрудников.

Сотрудников необходимо обучить правильно использовать сеть. Политики зачастую подразумевают использование антивирусного ПО и меры предотвращения несанкционированного вторжения на узел. Комплексные решения для защиты оконечных устройств используют функции контроля доступа к сети.

Безопасность устройств

Базовые шаги

При установке на устройство новой ОС настройки системы безопасности имеют значения по умолчанию. В большинстве случаев этого недостаточно.

Существует ряд простых шагов, которые можно применить для большинства ОС:

- Установленные по умолчанию логины и пароли необходимо немедленно изменить.
- Доступом к системным ресурсам должны обладать только лица, наделенные соответствующими правами.
- Все невостребованные службы и приложения при возможности необходимо отключить или удалить.
- Зачастую устройства, полученные от производителя, до отгрузки хранились на складе в течение определенного периода, и поэтому на них не установлены актуальные обновления. Прежде чем внедрять любое ПО, важно сначала его обновить и установить любые имеющиеся обновления для системы безопасности.

Пароли

Для защиты сетевых устройств необходимо использовать надежные пароли. Ниже приведены стандартные рекомендации по выбору пароля.

- Используйте пароль длиной не менее 10 символов (предпочтительно более 10).
- Выбирайте сложные пароли. Включайте в пароль комбинацию букв в верхнем и нижнем регистре, цифр, специальных символов и пробелов (если допускается их использование).
- Избегайте использования паролей на основе повторений, обычных слов из словаря, последовательностей букв или цифр, имени пользователя, имен родственников и домашних животных, биографических данных (дата рождения, номер паспорта, имена родителей и пр.).
- Допустите в пароле намеренную ошибку. Например, Ivanov = Ivonov = 1vOnov.
- Периодически меняйте пароли.
- Не записывайте пароли на бумаге и не оставляйте их в легко доступных местах.

Маршрутизаторы Cisco игнорируют начальные пробелы в паролях, но пробелы после первого символа учитываются. Таким образом, один из способов создать надежный пароль — использовать пробел в пароле и задать фразу, состоящую из нескольких слов. Это называется парольной фразой. Парольную фразу зачастую проще запомнить, чем обычный пароль. Парольная фраза также имеет большую длину, чем простой пароль, и ее сложнее подобрать.

Расширенная защита пароля

Существует ряд действий, которые можно выполнить, чтобы обеспечить сохранность пароля в тайне на маршрутизаторах и коммутаторах включающих следующее:

- Чтобы зашифровать пароли, используйте команду глобальной конфигурации **service password-encryption**.
- Установите минимально допустимую длину пароля с помощью команды **security password min-length** .
- Предотвратите атаки с использованием пароля грубой силы с помощью **команды login block for # attempts # within #**
- Отключение доступа к неактивному привилегированному режиму EXEC через определенное время (**exec-timeout)** .

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
Router#
```

Активация подключения по SSH

Настройка поддержки протокола SSH выполняется в четыре этапа:

1. **Настройте уникальное имя хоста устройства**.
2. **Настройте доменное имя IP** с помощью команды **ip-domain name**.
3. **Создайте ключ для шифрования SSH-трафика**. SSH шифрует трафик между источником и получателем. Однако для этого уникальный ключ проверки подлинности должен быть создан с помощью команды глобальной конфигурации **crypto key generate rsa general-keys modulus** *bits*. Следует лишь отметить, что модуль определяет размер ключа, который может быть в диапазоне от 360 *бит* до 2048 бит. Чем больше значение бита, тем безопаснее ключ. Однако большие значения битов также требовать больше времени для шифрования и расшифровки информации. Минимальная рекомендуемая длина модуля — 1024 бит.
4. **Проверьте или создайте запись локальной базы данных**. Создайте учетную запись пользователя в локальной базе данных с помощью команды **username**.
5. **Пользователи проходят аутентификацию в локальной базе данных.** Используйте команду конфигурации **login local** для проверки подлинности строки vty в локальной базе данных.
6. **Включите входящие сеансы SSH с использованием vty.** По умолчанию сеанс ввода не разрешен на линиях vty. Можно указать несколько протоколов, включая Telnet и SSH, используя команду **transport input [ssh | telnet].**

Вопросы?

Ставим “+”,
если вопросы есть

Ставим “–”,
если вопросов нет

Заполните, пожалуйста, опрос о занятии

Спасибо за внимание!