Категории атак

РЕПОЗИТОРИЙ ГГУ ИМЕНИ ФРАНЦИСКА СКОРИНЫ

Системы обнаружения атак

- Существует три этапа осуществления атаки. Первый, подготовительный, этап заключается в поиске предпосылок для осуществления той или иной атаки. На этом этапе ищутся уязвимости, использование которых приводит к реализации атаки, т.е. ко второму этапу. На третьем этапе завершается атака, "заметаются" следы и т.д. При этом первый этап, поиск уязвимостей при помощи сканеров безопасности считается атакой.
- Существующие механизмы защиты, реализованные в межсетевых экранах, серверах аутентификации, системах разграничения доступа и т.д. работают только на втором этапе.

Системы обнаружения атак

- Эти механизмы являются средствами блокирующими, а не упреждающими атаки. В абсолютном большинстве случаев они защищают от атак, которые уже находятся в процессе осуществления. И даже если они смогли предотвратить ту или иную атаку, то намного более эффективным было бы упреждение атак, т.е. устранение самих предпосылок реализации вторжений. Комплексная система обеспечения информационной безопасности должна работать на всех трех этапах осуществления атаки.

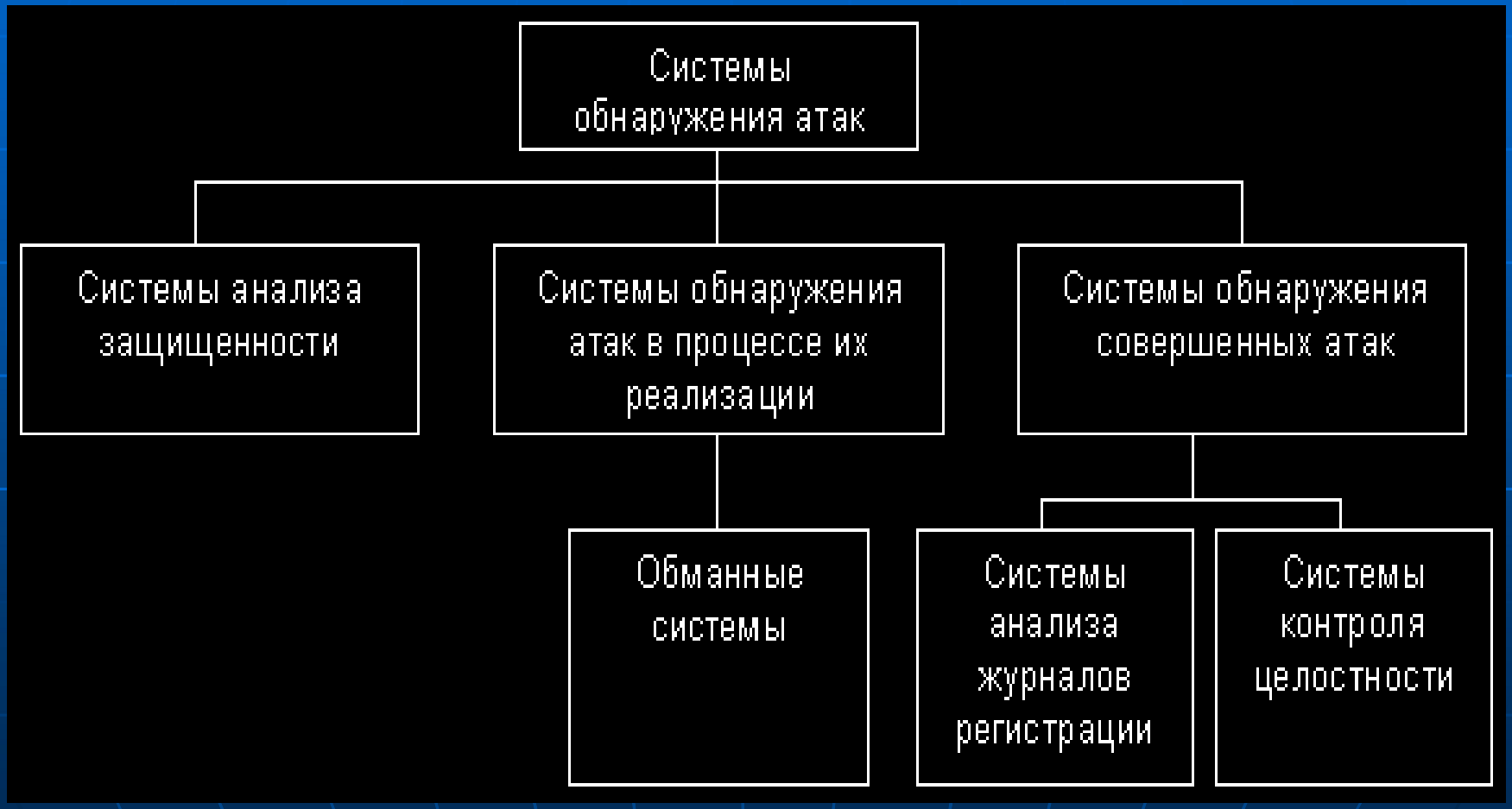
Системы обнаружения атак

- Обнаруживать, блокировать и предотвращать атаки можно несколькими путями. Первый, и самый распространенный, способ - это обнаружение уже реализуемых атак. Этот способ применяется в "классических" системах обнаружения атак (например, RealSecure компании Internet Security Systems), межсетевых экранах и т.п. Однако, "недостаток" средств данного класса в том, что атаки могут быть реализованы повторно. Второй путь - предотвратить атаки еще до их реализации. Осуществляется это путем поиска уязвимостей, которые могут быть использованы для реализации атаки.

Системы обнаружения атак

- И, наконец, третий путь - обнаружение уже совершенных атак и предотвращение их повторного осуществления. Таким образом, системы обнаружения атак могут быть классифицированы по этапам осуществления атаки (см. рис.).

Системы обнаружения атак



Системы обнаружения атак

- Системы, функционирующие на первом этапе осуществления атак и позволяющие обнаружить уязвимости информационной системы, используемые нарушителем для реализации атаки. Иначе средства этой категории называются системами анализа защищенности (security assessment systems) или сканерами безопасности (security scanners). Обычно системы анализа защищенности не принято относить к классу средств обнаружения атак, однако, если следовать описанным выше этапам осуществления атаки, то такое отнесение вполне логично.

Системы обнаружения атак

- Системы, функционирующие на втором этапе осуществления атаки и позволяющие обнаружить атаки в процессе их реализации, т.е. в режиме реального (или близкого к реальному) времени. Именно эти средства и принято считать системами обнаружения атак в классическом понимании. Помимо этого можно выделить такой класс средств обнаружения атак как обманные системы.
- Системы, функционирующие на третьем этапе осуществления атаки и позволяющие обнаружить уже совершенные атаки. Эти системы делятся на два класса - системы контроля целостности, обнаруживающие изменения контролируемых ресурсов, и системы анализа журналов регистрации.

Системы обнаружения атак

- Помимо этого, существует еще одна распространенная классификация систем обнаружения нарушения политики безопасности - по принципу реализации: host-based, т.е. обнаруживающие атаки, направленные на конкретный узел сети, и network-based, направленные на всю сеть или сегмент сети. Обычно на этом дальнейшая классификация останавливается. Однако системы класса host-based можно разделить еще на три подуровня:
  - Application IDS (Intrusion Detection System), обнаруживающие атаки на конкретные приложения;

Системы обнаружения атак

- OS IDS, обнаруживающие атаки на операционные системы;
- DBMS IDS, обнаруживающие атаки на системы управления базами данных.

- Выделение обнаружения атак СУБД в отдельную категорию связано с тем, что современные СУБД уже вышли из разряда обычных приложений и по многим своим характеристикам приближаются к операционным системам.
- Классификация систем обнаружения атак по уровню реализации выглядит следующим образом (см. рис.). Можно заметить, что это деление соответствует уровням информационной системы предприятия.

Системы обнаружения атак

Системы контроля целостности

- Системы контроля целостности работают по замкнутому циклу, обрабатывая файлы, системные объекты и атрибуты системных объектов с целью получения контрольных сумм; затем они сравнивают их с предыдущими контрольными суммами, отыскивая изменения. Когда изменение обнаружено, система посылает сообщение администратору, фиксируя время, соответствующее вероятному времени изменения. Если вновь вернуться к этапам реализации атаки, то системы этого класса функционируют на третьем этапе, т.е. они могут однозначно сказать, происходила атака (точнее изменение контролируемого объекта) или нет.

Обманные системы

- Когда речь заходит об обмане в области информационной безопасности, то здесь используются методы, которые применяют злоумышленники, т.е. лазейки для обхода используемых средств защиты, будь то кража паролей и работа от имени авторизованного пользователя. Обман может сослужить хорошую службу не только для злоумышленников, но и для защиты корпоративных ресурсов. Существует множество различных вариантов использования обмана в благих целях:
  - Сокрытие
  - Камуфляж
  - Дезинформация

Обманные системы

- В области информационной безопасности наибольшее распространение получил первый метод - сокрытие. Примером использования этого метода можно назвать сокрытие сетевой топологии при помощи межсетевого экрана. Пример камуфляжа: каждая операционная система обладает присущим только ей представлением механизма идентификации пользователя, отличающимся цветом и типом шрифта, которым выдается приглашение, текстом приглашения и местом его расположения. Примером дезинформации можно назвать использование заголовков, которые бы давали понять злоумышленнику, что атакуемая им система якобы уязвима.

Обманные системы

- Работа систем вида 2 и 3 заключается в том, что эти системы эмулируют те или иные известные уязвимости, которых в реальности не существует. Использование средств (deception systems), реализующих камуфляж и дезинформацию, приводит к следующему:
- 1.Увеличение числа выполняемых нарушителем операций и действий. Например, попытка запустить программу подбора паролей (например, Crack для Unix или L0phtCrack(LC) для Windows) на сфальсифицированный и несуществующий в реальности файл, приведет к бесполезной трате времени. Нападающий будет думать, что он не смог подобрать пароли, в то время как на самом деле программа "взлома" была просто обманута.

Обманные системы

- 2.Получение возможности отследить нападающих. За тот период времени, когда нападающие пытаются проверить все обнаруженные уязвимости, в т.ч. и фиктивные, администраторы безопасности могут проследить весь путь до нарушителя и предпринять соответствующие меры.
- Например, в информационной системе используются от 5 до 10 зарезервированных портов (с номерами от 1 до 1024). Если обманные системы (например, RealSecure компании ISS) эмулируют использование еще 100 и более портов, то работа нападающего резко увеличивается и злоумышленник обнаружит не 5-10, а 100 открытых портов.
-

Обманные системы

- При этом мало обнаружить открытый порт, надо еще попытаться использовать уязвимости, связанные с этим портом. И даже если нападающий автоматизирует эту работу путем использования соответствующих программных средств (Nmap, SATAN и т.д.), то число выполняемых им операций все равно существенно увеличивается, что приводит к быстрому снижению производительности его работы.

Средства анализа уязвимостей

- Обнаружением уязвимостей занимаются системы анализа защищенности - сканеры безопасности или системы поиска уязвимостей. Они проводят всесторонние исследования заданных систем с целью обнаружения уязвимостей, которые могут привести к нарушениям политики безопасности. Результаты, полученные от средств анализа защищенности, представляют "мгновенный снимок" состояния защиты системы в данный момент времени. Несмотря на то, что эти системы не могут обнаруживать атаку в процессе ее развития, они могут определить потенциальную возможность реализации атак.

Средства анализа уязвимостей

- Технология анализа защищенности является действенным методом реализации политики сетевой безопасности прежде, чем осуществится попытка ее нарушения снаружи или изнутри организации.
- Одним из вариантов классификации уязвимостей может служить классификация, отражающая этапы жизненного цикла информационной системы (см. таблицу).
- Наиболее опасны уязвимости проектирования. В этом случае, уязвимость свойственна проекту или алгоритму и, следовательно, даже совершенная его реализация не избавит от заложенной в нем уязвимости. Например, уязвимость стека протоколов TCP/IP.

Средства анализа уязвимостей

Этапы жизненного цикла ИС	**Категории уязвимостей ИС**
Проектирование ИС	Уязвимости проектирования
Реализация ИС	Уязвимости реализации
Эксплуатация ИС	Уязвимости конфигурации

Средства анализа уязвимостей

- Смысл уязвимостей реализации заключается в появлении ошибки на этапе реализации в программном или аппаратном обеспечении корректного с точки зрения безопасности проекта или алгоритма. Обнаруживаются и устраняются уязвимости относительно легко - путем обновления исполняемого кода или изменения исходного текста уязвимого ПО.
- К ошибкам конфигурации программного или аппаратного обеспечения можно отнести, например, доступный, но не используемый на узле сервис Telnet, использование "слабых" паролей менее 6 символов, учетные записи и пароли, остановленные по умолчанию, и т.д. Обнаружить и исправить такие уязвимости проще всего.

Средства анализа уязвимостей

Средства анализа уязвимостей

- Системы анализа защищенности второго и третьего типов получили наибольшее распространение среди конечных пользователей. Существует несколько дополнительных классификаций этих систем. Например, системы анализа исходного текста и исполняемого кода тестируемого программно-аппаратного обеспечения и т.д. Большой интерес вызывают системы поиска уязвимостей в исполняемом коде, самым распространенным подклассом которых являются системы имитации атак, которые моделируют различные несанкционированные воздействия на компоненты информационной системы.

Средства анализа уязвимостей

- Именно эти системы получили широкую известность во всем мире ввиду своей относительной простоты и дешевизны. Посредством таких имитаторов обнаруживаются уязвимости еще до того, как они будут использованы нарушителями для реализации атак. К числу систем данного класса можно отнести SATAN, Internet Scanner, Cisco Secure Scanner и т.д.
- Системы имитации атак с одинаковым успехом обнаруживают не только уязвимости реализации, но и уязвимости эксплуатации. Функционировать они могут на уровне сети, операционной системы, СУБД и прикладного программного обеспечения.

Средства анализа уязвимостей

- Наибольшее распространение получили средства анализа защищенности сетевых сервисов и протоколов. Связано это с универсальностью используемых протоколов. Изученность и повсеместное использование таких стеков протоколов, как TCP/IP и т.п. позволяют с высокой степенью эффективности проверять защищенность корпоративной сети, работающей в данном сетевом окружении, независимо от того, какое программное обеспечение функционирует на более высоких уровнях. Примером такой системы является Internet Scanner компании ISS.

Средства анализа уязвимостей

- Вторыми по распространенности являются средства анализа защищенности операционных систем. Связано это также с универсальностью и распространенностью некоторых операционных систем (например, UNIX и Windows). Однако, из-за того, что каждый производитель вносит в операционную систему свои изменения (ярким примером является множество разновидностей ОС UNIX), средства анализа защищенности ОС анализируют в первую очередь параметры, характерные для всего семейства одной ОС. И лишь для некоторых систем анализируются специфичные для нее параметры.

Средства анализа уязвимостей

- При проведении анализа защищенности реализуются две стратегии. Первая - пассивная, - реализуемая на уровне операционной системы, СУБД и приложений, при которой осуществляется анализ конфигурационных файлов и системного реестра на наличие неправильных параметров, файлов паролей на наличие легко угадываемых паролей, а также других системных объектов на нарушения политики безопасности. Вторая стратегия, - активная, - осуществляемая в большинстве случаев на сетевом уровне, позволяющая воспроизводить наиболее распространенные сценарии атак, и анализировать реакции системы на эти сценарии.

Средства анализа уязвимостей

- Системы анализа защищенности могут быть использованы:
- для оценки уровня безопасности организации;
- для контроля эффективности настройки сетевого, системного и прикладного программно-аппаратного обеспечения;
- внешними аудиторскими и консалтинговыми компаниями, осуществляющими информационные обследования сетей заказчиков;
- для тестирования и сертификации того или иного программно-аппаратного обеспечения.

Средства анализа уязвимостей

Название	Производитель	Категория	Примечание
Internet Scanner	Internet Security Systems	На уровне сети	Имеет сертификат ГТК.
System Scanner	Internet Security Systems	На уровне ОС	
Database Scanner	Internet Security Systems	На уровне СУБД	

Средства анализа уязвимостей

Название	Производитель	Категория	Примечание
Cisco Secure Scanner	Cisco Systems	На уровне сети	
CyberCop Scanner	Network Associates	На уровне сети	
WebTrends Security Analyzer	WebTrends Corporation	На уровне сети	

Средства анализа уязвимостей

Название	Производитель	Категория	Примечание
Enterprise Security Manager	Symantec	На уровне ОС	
SFProtect	Hewlett Packard	На уровне сети, ОС, СУБД	
Nessus	Свободно распространяет-ся	На уровне сети	Имеет сертификат ГТК.

Средства анализа уязвимостей

- Поскольку постоянно появляются новые уязвимости, то для их эффективного обнаружения необходимо постоянно обновлять базу данных системы анализа защищенности. В идеале разрыв между появлением информации об уязвимости в различных "хакерских" источниках и появлением сигнатуры в базе данных системы обнаружения должен отсутствовать. Но как бы часто не обновлялась база данных уязвимостей, существует временной промежуток между сообщением о новой уязвимости и появлением проверки для нее.

Средства анализа уязвимостей

- Существует два основных механизма, при помощи которых сканер проверяет наличие уязвимости - сканирование (**scan**) и зондирование (**probe**).
- ***Сканирование*** - механизм пассивного анализа, с помощью которого сканер пытается определить наличие уязвимости без фактического подтверждения ее наличия - по косвенным признакам. Этот метод является наиболее быстрым и простым для реализации. Согласно компании Cisco этот процесс идентифицирует открытые порты, найденные на каждом сетевом устройстве, и собирает связанные с портами заголовки (banner), найденные при сканировании каждого порта.

Средства анализа уязвимостей

- Каждый полученный заголовок сравнивается с таблицей правил определения сетевых устройств, операционных систем и потенциальных уязвимостей. На основе проведенного сравнения делается вывод о наличии или отсутствии уязвимости.
- ***Зондирование*** - механизм активного анализа, который позволяет убедиться, присутствует или нет на анализируемом узле уязвимость. Зондирование выполняется путем имитации атаки, использующей проверяемую уязвимость. Этот метод более медленный, чем "сканирование", но более точный, чем он. Этот процесс использует информацию, полученную в процессе сканирования для детального анализа каждого сетевого устройства.

Средства анализа уязвимостей

- Этот процесс также использует известные методы реализации атак для того, чтобы полностью подтвердить предполагаемые уязвимости и обнаружить другие уязвимости, которые не могут быть обнаружены пассивными методами, например подверженность атакам типа "отказ в обслуживании" ("denial of service").
- На практике указанные механизмы реализуются несколькими методами.
- **"Проверка заголовков" (banner check)**
- Представляет собой ряд проверок типа "сканирование" и позволяет делать вывод об уязвимости, опираясь на информацию в заголовке ответа на запрос сканера.

Средства анализа уязвимостей

- Типичный пример такой проверки - анализ заголовков программы Sendmail или FTP-сервера, позволяющий узнать их версию и на основе этой информации сделать вывод о наличии в них уязвимости. Однако администратор может изменить текст заголовков, возвращаемых на внешние запросы.
- **"Активные зондирующие проверки" (active probing check)**
- Относятся к механизму "сканирования". Основаны на сравнении "цифрового слепка" (fingerprint) фрагмента программного обеспечения со слепком известной уязвимости.

Средства анализа уязвимостей

- Аналогичным образом поступают антивирусные системы, сравнивая фрагменты сканируемого программного обеспечения с сигнатурами вирусов, хранящимися в специализированной базе данных. Разновидностью этого метода являются проверки контрольных сумм или даты сканируемого программного обеспечения, которые реализуются в сканерах, работающих на уровне операционной системы.
- Этот метод также достаточно быстр, но реализуется труднее, чем "проверка заголовков".

Средства анализа уязвимостей

- **"Имитация атак" (exploit check)**
- Некоторые уязвимости не обнаруживают себя, пока их не "подтолкнут". Для этого против подозрительного сервиса или узла запускаются реальные атаки. Проверки методом "exploit check" позволяет имитировать реальные атаки, тем самым с большей эффективностью (но меньшей скоростью) обнаруживая уязвимости на сканируемых узлах. Имитация атак является более надежным способом анализа защищенности, чем проверки заголовков, и обычно более надежны, чем активные зондирующие проверки.

Средства анализа уязвимостей

- Однако существуют случаи, когда имитация атак не может быть реализована: ситуации, в которых тест приводит к "отказу в обслуживании" анализируемого узла (сети), и ситуации, при которых уязвимость в принципе не годна для реализации атаки на сеть.
- В некоторых случаях нежелательно использовать имитацию атак, т.к. это может привести к большим затратам на восстановление работоспособности выведенных из строя элементов корпоративной сети. В этих случаях желательно применить другие проверки, например, активное зондирование или проверки заголовков.

Этапы сканирования

- Практически любой сканер проводит анализ защищенности в несколько этапов:
- *Сбор информации о сети*. Идентифицируются все активные устройства в сети и определяются запущенные на них сервисы. В случае использования систем анализа защищенности на уровне операционной системы данный этап пропускается, поскольку на каждом анализируемом узле установлены соответствующие агенты системного сканера.
- *Обнаружение потенциальных уязвимостей*. Сканер использует базу данных для сравнения собранных данных с известными уязвимостями при помощи проверки заголовков или активных зондирующих проверок.

Этапы сканирования

- *Подтверждение выбранных уязвимостей*. Сканер использует специальные методы и моделирует (имитирует) определенные атаки для подтверждения факта наличия уязвимостей на выбранных узлах сети.
- *Генерация отчетов*.
- *Автоматическое устранение уязвимостей*. Широко применяется в системных сканерах. Создается специальный сценарий (fix script) для устранения уязвимости. Одновременно создается и второй сценарий, отменяющий произведенные изменения. Это необходимо в том случае, если после устранения проблемы, нормальное функционирование узла будет нарушено.

Этапы сканирования

- У администратора есть несколько вариантов использования системы анализа защищенности:
- Запуск сканирования только с проверками на потенциальные уязвимости (этапы 1,2 и 4). Это дает предварительное ознакомление с системами в сети. Этот метод является гораздо менее разрушительным по сравнению с другими и также является самым быстрым.
- Запуск сканирования с проверками на потенциальные и подтвержденные уязвимости. Этот метод может вызвать нарушение работы узлов сети во время реализации проверок типа "exploit check".

Этапы сканирования

- Запуск сканирования с пользовательскими правилами для нахождения конкретной проблемы.
- Комбинации вышеперечисленного.
- Подсистема генерации отчетов - немаловажный элемент системы анализа защищенности. Без нее трудно составить мнение о том, каков уровень защищенности сегментов корпоративной сети. На основе созданных отчетов администратор безопасности строит всю свою дальнейшую деятельность - изменяет политику безопасности, устраняет обнаруженные уязвимости, реконфигурирует средства защиты, готовит отчеты руководству и т.д.

Этапы сканирования

- Хорошая подсистема генерации отчетов должна обладать следующими свойствами:
- Наличие в отчетах как текстовой информации, так и графических данных.
- Наличие информации об обнаруженной уязвимости, вариантах ложного обнаружения, наличие рекомендаций по устранению обнаруженных проблем, ссылках на сервера производителей, дополнительной информации.
- Возможность выборки из всей собранной информации только нужных данных по заданным критериям (интервал времени, название уязвимости, степень риска, операционная система, тип уязвимости и т.д.).

Этапы сканирования

- Возможность сортировки данных в создаваемых отчетах по различным параметрам (по имени, по дате, по степени риска и т.д.).
- Возможность создания отчетов для различных категорий специалистов. Как минимум можно выделить три таких категории: руководство компании, руководство среднего звена и технические специалисты. В отчетах первой категории содержится описание общего состояния защищенности корпоративной сети. Отчеты второй категории могут содержать описание обнаруженных уязвимостей или атак, но без указания мер по их устранению.

Этапы сканирования

- К данной категории также относятся так называемые сравнительные отчеты (trend analysis), которые показывают тенденции в изменении уровня защищенности заданных узлов корпоративной сети. К последней категории отчетов можно отнести технические отчеты, содержащие не только подробное описание каждой из обнаруженных проблем, но и рекомендации по их устранению, а также ссылки на дополнительные источники информации. Такие категории отчетов приняты, например, в Internet Scanner и Cisco Secure Scanner.
- Поддержка различных форматов создаваемых отчетов.

Особенности применения

- Если сканер не находит уязвимостей на тестируемом узле это не значит, что их нет. Просто это зависит не только от сканера, но и от его окружения. Различные реализации одного и того же сервиса по-разному реагируют на системы анализа защищенности. Очень часто на практике можно увидеть, что сканер показывает уязвимости, которых на анализируемом узле нет. Это относится к сетевым сканерам, которые проводят дистанционный анализ узлов сети. В этом случае можно порекомендовать использовать систему анализа защищенности на уровне операционной системы, агенты которой устанавливаются на каждый контролируемый узел и проводят все проверки локально.

Особенности применения

- В некоторых случаях имеются уязвимости, с трудом обнаруживаемые или совсем не обнаруживаемые через сеть. Например, проверка "слабости" паролей, используемых пользователями и другими учетными записями. В случае использования сетевого сканера вам потребуется затратить очень много времени на удаленную проверку каждой учетной записи. В то же время, аналогичная проверка, осуществляемая на локальном узле, проводится на несколько порядков быстрее. Другим примером может служить проверка файловой системы сканируемого узла. Во многих случаях ее нельзя осуществить дистанционно.

Особенности применения

- Достоинства сканирования на уровне ОС кроются в прямом доступе к низкоуровневым возможностям ОС хоста, конкретным сервисам и деталям конфигурации. Тогда как сканер сетевого уровня имитирует ситуацию, которую мог бы иметь внешний злоумышленник, сканер системного уровня может рассматривать систему со стороны пользователя, уже имеющего доступ к анализируемой системе и имеющего в ней учетную запись. Это является наиболее важным отличием, поскольку сетевой сканер по определению не может предоставить эффективного анализа возможных рисков деятельности пользователя.

Меры безопасности при использовании TCP/IP

- **1.Фильтрация на маршрутизаторе**
- Фильтры на маршрутизаторе, соединяющем сеть предприятия с Интернетом, применяются для запрета пропуска датаграмм, которые могут быть использованы для атак как на сеть организации из Интернета, так и на внешние сети злоумышленником, находящимся внутри организации.
- Более безопасным и управляемым решением, чем фильтрация того или иного TCP-трафика следующего от или к компьютеру пользователя, является работа пользователей через прокси-серверы. Прокси-сервер берет на себя функции предоставления пользователю требуемого сервиса и сам связывается с необходимыми хостами Интернета.

Меры безопасности при использовании TCP/IP

- Хост пользователя взаимодействует только с прокси-сервером и не нуждается в коннективности с Интернетом. Таким образом, фильтрующий маршрутизатор разрешает прохождение TCP-сегментов определенного типа только от или к прокси-серверу. Преимущества этого решения следующие:
- Прокси-сервер находится под контролем администратора предприятия, что позволяет реализовывать различные политики для дифференцированного управления доступом пользователей к сервисам и ресурсам Интернета, фильтрации передаваемых данных (защита от вирусов, цензура и т.п.), кэширования (там, где это применимо).

Меры безопасности при использовании TCP/IP

- С точки зрения Интернета от имени всех пользовательских хостов предприятия действует один прокси-сервер, то есть имеется только один потенциальный объект для атаки из Интернета, а безопасность одного прокси-сервера, легче обеспечить, чем безопасность множества пользовательских компьютеров.
- **2. Анализ сетевого трафика**
- Анализ сетевого трафика проводится для обнаружения атак, предпринятых злоумышленниками, находящимися как в сети организации, так и в Интернете.

Меры безопасности при использовании TCP/IP

- **3. Защита маршрутизатора**
- Мероприятия по защите маршрутизатора проводятся с целью предотвращения атак, направленных на нарушение схемы маршрутизации датаграмм или на захват маршрутизатора злоумышленником.
- **4. Защита хоста**
- Мероприятия по защите хоста проводятся для предотвращения атак, цель которых — перехват данных, отказ в обслуживании, или проникновение злоумышленника в операционную систему.

Меры безопасности при использовании TCP/IP

- **5. Превентивное сканирование**
- Администратор сети должен знать и использовать методы и инструменты злоумышленника и проводить превентивное сканирование сети организации для обнаружения слабых мест в безопасности до того, как это сделает злоумышленник. Для этой цели имеется также специальное программное обеспечение — сканеры безопасности.

Общие меры по повышению безопасности сети

- 1. **Оперативная установка исправлений для программ (Patching)**. Системные администраторы должны защищать самые важные свои системы, оперативно устанавливая исправления для программ на них. Тем не менее, установить исправления для программ на всех хостах в сети трудно, так как исправления могут появляться достаточно часто. В этом случае надо обязательно вносить исправления в программы на самых важных хостах.

Общие меры по повышению безопасности сети

- 2. **Обнаружение вирусов и троянских коней.** Для максимальной эффективности они должны быть установлены на всех компьютерах в сети. Пользователей следует учить, как им самим делать эти обновления, но при этом нельзя полностью полагаться на них. Помимо обычной антивирусной программы на каждом компьютере необходимо сканирование приложений к электронным письмам на почтовом сервере. Таким образом можно обнаружить большинство вирусов до того, как они достигнут машин пользователей.

Общие меры по повышению безопасности сети

- 3. **Межсетевые экраны** Межсетевые экраны - самое важное средство защиты сети организации. Они контролируют сетевой трафик, входящий в сеть и выходящий из нее. Межсетевой экран может блокировать передачу в сеть какого-либо вида трафика или выполнять те или иные проверки другого вида трафика. Хорошо сконфигуированный межсетевой экран в состоянии остановить большинство известных компьютерных атак.

Общие меры по повышению безопасности сети

- 4. **Вскрыватели паролей (Password Crackers)** Хакеры часто используют малоизвестные уязвимые места в компьютерах для того, чтобы украсть файлы с зашифрованными паролями. Затем они используют специальные программы для вскрытия паролей, которые могут обнаружить слабые пароли в этих зашифрованных файлах. Хотя это средство используются злоумышленниками, оно будет также полезно и системным администраторам, чтобы своевременно обнаружить слабые пароли.

Общие меры по повышению безопасности сети

- 5. **Шифрование.** Атакующие часто проникают в сети с помощью прослушивания сетевого трафика в наиболее важных местах и выделения из него имен пользователей и их паролей. Поэтому соединения с удаленными машинами, защищаемые с помощью пароля, должны быть зашифрованы. Это особенно важно в тех случаях, если соединение осуществляется по Интернет или с важным сервером. Имеется ряд коммерческих и бесплатных программ для шифрования трафика TCP/IP (наиболее известен SSH).

Общие меры по повышению безопасности сети

- 6. **Сканеры уязвимых мест.** Это программы, которые сканируют сеть в поисках компьютеров, уязвимых к определенным видам атак. Сканеры имеют большую базу данных уязвимых мест, которую они используют при проверке того или иного компьютера на наличие у него уязвимых мест.
- 7. **Грамотное конфигурирование компьютеров в отношении безопасности.**
- 8. **Средства для поиска подключенных модемов.** Для поиска подключенных модемов атакующие могут использовать программы обзвонки большого числа телефонных номеров.

Общие меры по повышению безопасности сети

- 9. **Рекомендации по безопасности (security advisories)** Рекомендации по безопасности - это предупреждения, публикуемые группами по борьбе с компьютерными преступлениями и производителями программ о недавно обнаруженных уязвимых местах. Рекомендации обычно описывают самые серьезные угрозы, возникающие из-за этих уязвимых мест и поэтому являются занимающими мало времени на чтение, но очень полезными. Они описывают угрозу и дают довольно конкретные советы о том, что нужно сделать для устранения данного уязвимого места. Двумя самыми полезными являются рекомендации, которые публикует группа по борьбе с компьютерными преступлениями **CIAC** и **CERT.**

Общие меры по повышению безопасности сети

- 10. **Средства обнаружения атак (Intrusion Detection)** Системы обнаружения атак оперативно обнаруживают компьютерные атаки. Они могут быть установлены за межсетевым экраном, чтобы обнаруживать атаки, организуемые изнутри сети. Или они могут быть установлены перед межсетевым экраном, чтобы обнаруживать атаки на межсетевой экран. Средства этого типа могут иметь разнообразные возможности.
- 11. **Средства выявления топологии сети и сканеры портов**. Эти программы позволяют составить полную картину того, как устроена ваша сеть и какие компьютеры в ней работают, а также выявить все сервисы, которые работают на каждой машине.

Общие меры по повышению безопасности сети

- 12. **Инструкции по действию в критических ситуациях.** В каждой сети, независимо от того, насколько она безопасна, происходят какие-либо события, связанные с безопасностью (может быть даже ложные тревоги). Сотрудники организации должны заранее знать, что нужно делать в том или ином случае.
- 13. **Политики безопасности.** Организации должны написать политику безопасности, в которой определялся бы ожидаемый уровень защиты, который должен быть везде единообразно реализован. Самым важным аспектом политики является выработка единых требований к тому, какой трафик должен пропускаться через межсетевые экраны сети.

Общие меры по повышению безопасности сети

- 14. **Тестирование межсетевых экранов и WWW-серверов на устойчивость к попыткам их блокирования.** Атаки на блокирование компьютера распространены в Интернет. Атакующие постоянно выводят из строя WWW-сайты, перегружают компьютеры или переполняют сети бессмысленными пакетами. Сети, заботящиеся о безопасности, могут организовать атаки против себя сами, чтобы определить, какой ущерб может быть нанесен им.