Технологии обнаружения вторжений

- **Тема**

- **Технология обнаружения атак**

технологии информационной защиты

- криптографическая защита данных для обеспечения конфиденциальности, целостности и подлинности информации;
- технологии аутентификации для проверки подлинности пользователей и объектов сети;
- технологии межсетевых экранов для защиты корпоративной сети от внешних угроз при подключении к общедоступным сетям связи;
- технологии виртуальных защищенных каналов и сетей VPN для защиты информации, передаваемой по открытым каналам связи;

технологии информационной защиты

- гарантированная идентификация пользователей путем применения токенов (смарт-карт, touch-memory, ключей для USB-портов и т. п.) и других средств аутентификации;
- управление доступом на уровне пользователей и защита от несанкционированного доступа к информации;
- поддержка инфраструктуры управления открытыми ключами PKI;
- технологии обнаружения вторжений (Intrusion Detection) для активного исследования защищенности информационных ресурсов;

технологии информационной защиты

- •технологии защиты от вирусов с использованием специализированных комплексов антивирусной профилактики и защиты;
- • централизованное управление СИБ на базе единой политики безопасности предприятия;
- • комплексный подход к обеспечению информационной безопасности, обеспечивающий рациональное сочетание технологий и средств информационной защиты.

Архитектура Информационных Систем (ИС)

- •уровень прикладного программного обеспечения (ПО), отвечающий за взаимодействие с пользователем. Примером элементов ИС, работающих на этом уровне, можно назвать текстовый редактор WinWord, редактор электронных таблиц Excel, почтовую программу Outlook и т. д.
- •уровень системы управления базами данных (СУБД), отвечающий за хранение и обработку данных ИС. Примером элементов ИС, работающих на этом уровне, можно назвать СУБД Oracle, MS SQL Server, Sybase и MS Access.
- •уровень операционной системы (ОС), отвечающий за обслуживание СУБД и прикладного ПО. Примером элементов ИС, работающих на этом уровне, можно назвать ОС Microsoft Windows NT/2000/XP, Sun Solaris, Novell Netware.
- •уровень сети, отвечающий за взаимодействие узлов ИС. Примером элементов ИС, работающих на этом уровне, можно назвать стеки протоколов TCP/IP, IPS/SPX и SMB/NetBIOS.

этапы осуществления атаки на КИС

Концепция атаки . Изучение цели (предпосылки)

- Предварительный сбор данных, заключающийся в скрытом наблюдении за организацией, целью которого является систематизированный сбор открытых сведений о компьютерной информационной системе конкретной организации.
- Сканирование сети организации с целью выявления уязвимостей, позволяющих взломщику проникнуть в компьютерную систему.
- Инвентаризацию общих ресурсов иучетных записей системы, что позволит взломщику получить доступ к информации, хрнимой в атакуемой системе.

Исполнение атаки

- **Проникновение в систему, заключающееся в попытках получения доступа по любой учетной записи.**
- **Расширение прав доступа, состоящее во взломе паролей учетных записей с большими правами, например, администратора системы.**
- **Выполнение цели атаки - извлечение данных, разрушение информации и т.д.**

Цели атаки

- **Любопытство** - это мотив, который обычно приписывают (чаще всего сами себе) хакерам, осуществляющим атаки якобы без преследования какой-либо выгоды. Тем не менее, все это приводит к потере конфиденциальности информации и даже ее целостности, что вряд ли приемлемо для владельцев информации.
- **Шпионаж**, преследующий цель получения информации технического или военно-политического значения. Как правило, такие атаки обходятся без потери целостности информации - ведь шпионы вовсе не хотят, чтобы их деятельность была обнаружена.
- **Финансовая выгода**, которая относится к сфере преступной деятельности (скажем кража номеров кредитных карточек) и приводит к реальным потерям - не только финансовым, но и целостности информации.
- **Вандализм** - взломщик просто разрушает всю систему, нанося убытки атакуемой организации путем, скажем, внедрения вирусов. Ныне этот вид деятельности приобрел угрожающие масштабы - всем известен случай с распространением по почте вирусов, например, Melissa, приводящим к миллиардным убыткам организаций и частных лиц во всем мире.
- **Шантаж и террор** - использование результатов взлома с целью вымогательства, например, путем угрозы раскрытия конфиденциальной информации.

Сокрытие следов атаки

- **Использование** для выполнения атаки чужих компьютеров, что дает злоумышленникам наилучшие возможности для сохранения анонимности.
- **Подмена адреса** источника атаки путем использования промежуточных серверов.
- **Изменение** стандартных номеров портов хакерских программ, оставленных на взломанное компьютере, что затрудняет их выявление.
- **Чистка журналов** регистрации событий безопасности.
- **Скрытие файлов и папок.**
- **Скрытие процессов.**

Классификация атак

- **Атаки**, использующие средства удаленного администрирования системой.
- **Атаки**, направленные на расширение прав доступа. Примером могут служить программы sechole, getadmin, hk.
- **Удаленные атаки DoS**, которые направлены на нарушение функционирования информационной системы путем рассылки пакетов, перегружающих сетевые серверы
- **Локальная атака DoS**, которая сводится к запуску, например, злонамеренного аплета на Web-страничке, загружающего процессор бесконечным циклом отображения диалогов на мониторе компьютера, как описано в главе 8 этой книги.
- **Анализаторы** сетевых уязвимостей, выполняющие, в сущности, поиск брешей в системе безопасности вместе с попытками взлома, что позволяет проверить надежность защиты. Примером служит уже рассмотренное приложение Retina.
- **Взломщики паролей**, выполняющие подбор паролей доступа. Пример - рассмотренная в главе 13 программа LC3, позволяющая взламывать пароли в базе данных SAM и системном реестре компьютера.
- **Сетевые анализаторы**, предназначенные для перехвата сетевого трафика с целью получения конфиденциальных данных.

Атаки могут быть также классифицированы по способам доступа к компьютерной системе

- **Взломщик может воспользоваться физическим проникновением** - попросту выкрасть компонент компьютерной системы, например, жесткий диск.
- **Взломщик может осуществить локальное проникновение в компьютер**, например, зарегистрировавшись с консоли управления сетевого сервера или клиента.
- **Взломщик может осуществить удаленное проникновение в компьютеры локальной сети организации**, действуя в пределах территории самой организации.
- **Взломщик может попытаться подсоединиться к сети организации через телефонную линию связи** с модемом, подключенным к сетевому компьютеру.
- **Если сеть организации подсоединена к Интернету**, то взломщик может проникнуть в локальную сеть через Интернет.

Системы обнаружения атак

- Традиционные системы защиты компьютерной информации опираются на три основных средства (называемых "три А" системы защиты):
- **Аутентификация**
- **Авторизация**
- **Аудит**

Базовые средства выявления атак

- **Накопленная информация о признаках атаки.**
- **Контроль источников информации о признаках атаки.**
- **Накопленные методы анализа информации.**

Системы защиты

- **Сканеры безопасности**, которые действуют как средство анализа защищенности системы путем имитации хакерской атаки на этапе выявления уязвимостей атакуемой системы.
- **Классические средства** выявления вторжений, действующие в режиме реального времени и позволяющие обнаруживать атаки на этапе их реализации.
- **Контроль целостности**, обнаруживающий изменения в контролируемых ресурсах, например, в ресурсах файловой системы, для выявления последствия выполнения атаки.

Классические системы обнаружения атак

- **Сетевые атаки.** Для обнаружения атак на уровне сети классические системы собирают информацию из сетевого трафика, а также анализируют информацию в журналах регистрации событий программно-аппаратного обеспечения сети
- **Захват пакетов** чаще всего выполняется обычной сетевой картой, но иногда применяются и специализированные устройства.
- **Атаки** на операционную систему, приложения и базу данных.
- **Обманные системы** называемые камуфляжем.

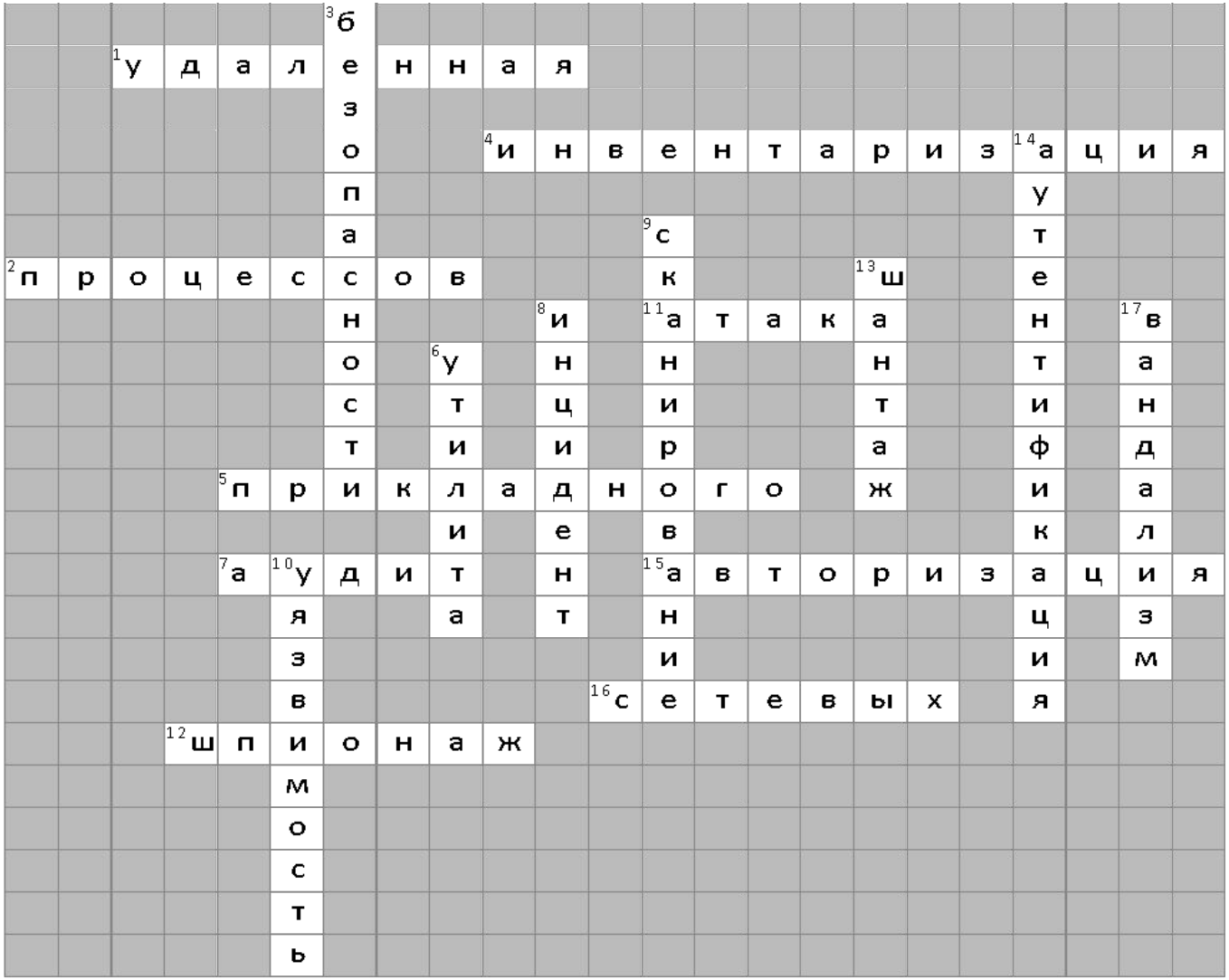
Классические системы обнаружения атак (продолжение)

- **Контроль целостности.**
- **Для защиты файлов**, системы контроля целостности используют специализированные криптографические средства, которые для защиты файлов вычисляют для каждого файла цифровой отпечаток (дайджеста).
- **Управление безопасностью.** Состояние дел в современном компьютерном сообществе ныне таково, что только систематическое применение хорошо продуманных мер по обеспечению безопасности может снизить до приемлемого уровня риск потери информации или ее порчу

Правило безопасности должно содержать:

- **Сведения о конфигурации** локальной сети и сетевых устройств (в частности, брандмауэров).
- **План резервного копирования** системы и восстановления после аварий.
- **Инструкцию о действиях** персонала при прорыве системы защиты.
- **Журнал** с детальным описанием действий системного администратора.
- **Результаты аудита попыток** неавторизованного доступа, вместе с указанием лица, к которому следует обратиться при обнаружении таких попыток.

Кроссворд


1 у д а л е н н а я
2 п р о ц е с с о в
3 б
з
о
п
а
4 и н в е н т а р и з а ц и я
у
т
е
н
т
а
ц
и
я
5 п р и к л а д н о г о
и
е
6 у
н
т
и
н
а
л
7 а
8 и
9 с
10 у д и т
я
з
в
11 а т а к а
н
н
и
12 ш п и о н а ж
м
о
с
т
ь
13 ш
ж
13 а
в
т о р и з а ц и я
ц
з
м
16 с е т е в ы х
ф
д
17 в

Вопросы приветствуются!

ВОПРОСЫ?