Социальная инженерия

Лекция 5

По курсу: Защита информационных ресурсов компьютерных систем и сетей

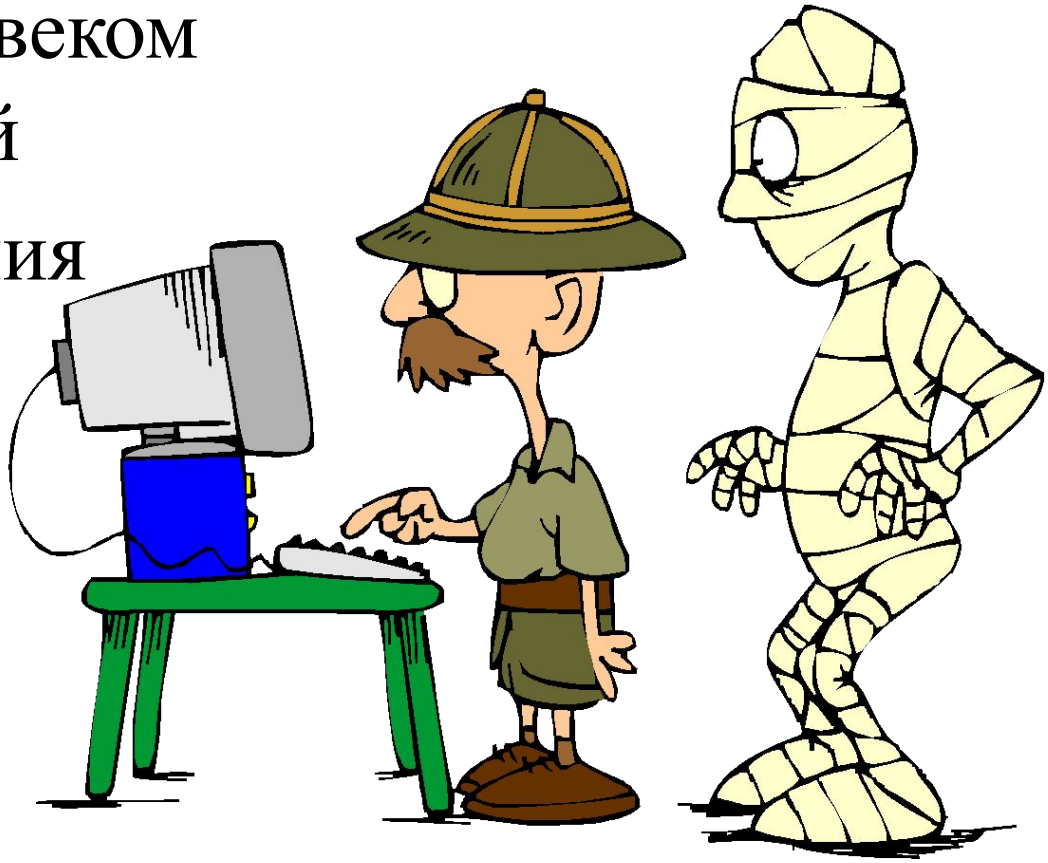
Атаки на автоматизированную систему (пользователь + ЭВМ)

технические методы взлома

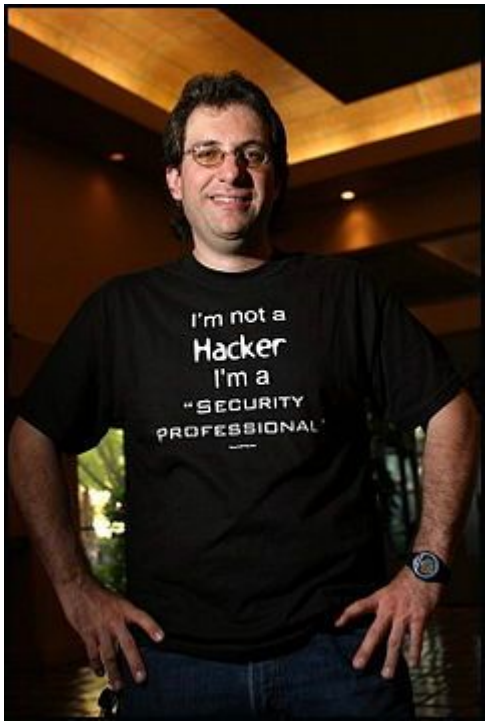
социальная инженерия

Социальная инженерия

- совокупность приемов манипуляции человеком или группой людей
- с целью преодоления систем защиты информации и
- копирования или модификации информации ограниченного доступа



История



Кевин Дэвид Митник — знаковая фигура в сфере информационной безопасности, фактически является именем нарицательным. Ныне является консультантом по компьютерной безопасности, автором и бывшим компьютерным хакером. В конце XX века был признан виновным в различных компьютерных и коммуникационных преступлениях. На момент ареста был наиболее разыскиваемым компьютерным преступником в США.

Области применения социальной инженерии

- Финансовые махинации в организациях.
- Общая дестабилизация работы организации с целью ее дальнейшего разрушения.
- Проникновение в сеть организации для дестабилизации работы основных узлов с какой-либо целью.
- Фишинг и другие способы получения паролей для доступа информации ограниченного доступа.
- Конкурентная разведка.

Конкурентная разведка

- Неправомерное получение чужих баз данных.
- Информация о маркетинговых планах организации.
- Общая информация об организации (используется для рейдерских атак).
- Информация о наиболее перспективных сотрудниках с целью их дальнейшего «переманивания» в свою организацию.

Принципы социальной инженерии

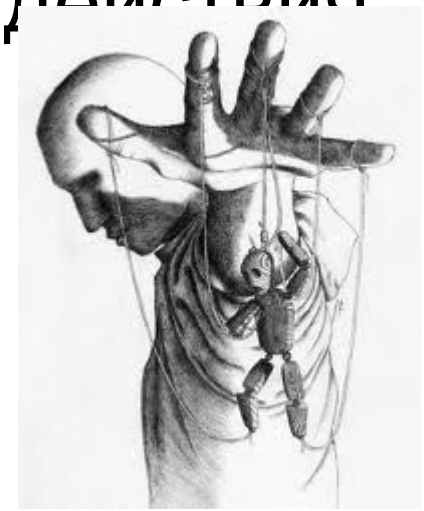
- выдача себя за другое лицо
- отвлечение внимания
- нагнетание психологического напряжения

Выдача себя за другое лицо

Регистрация под ложными персональными данными.

Отвлечение внимания

Для отвлечения внимания злоумышленники часто прибегают к имитации атаки, выполняя различные бессмысленные, но целенаправл
действия



Нагнетание психологического напряжения

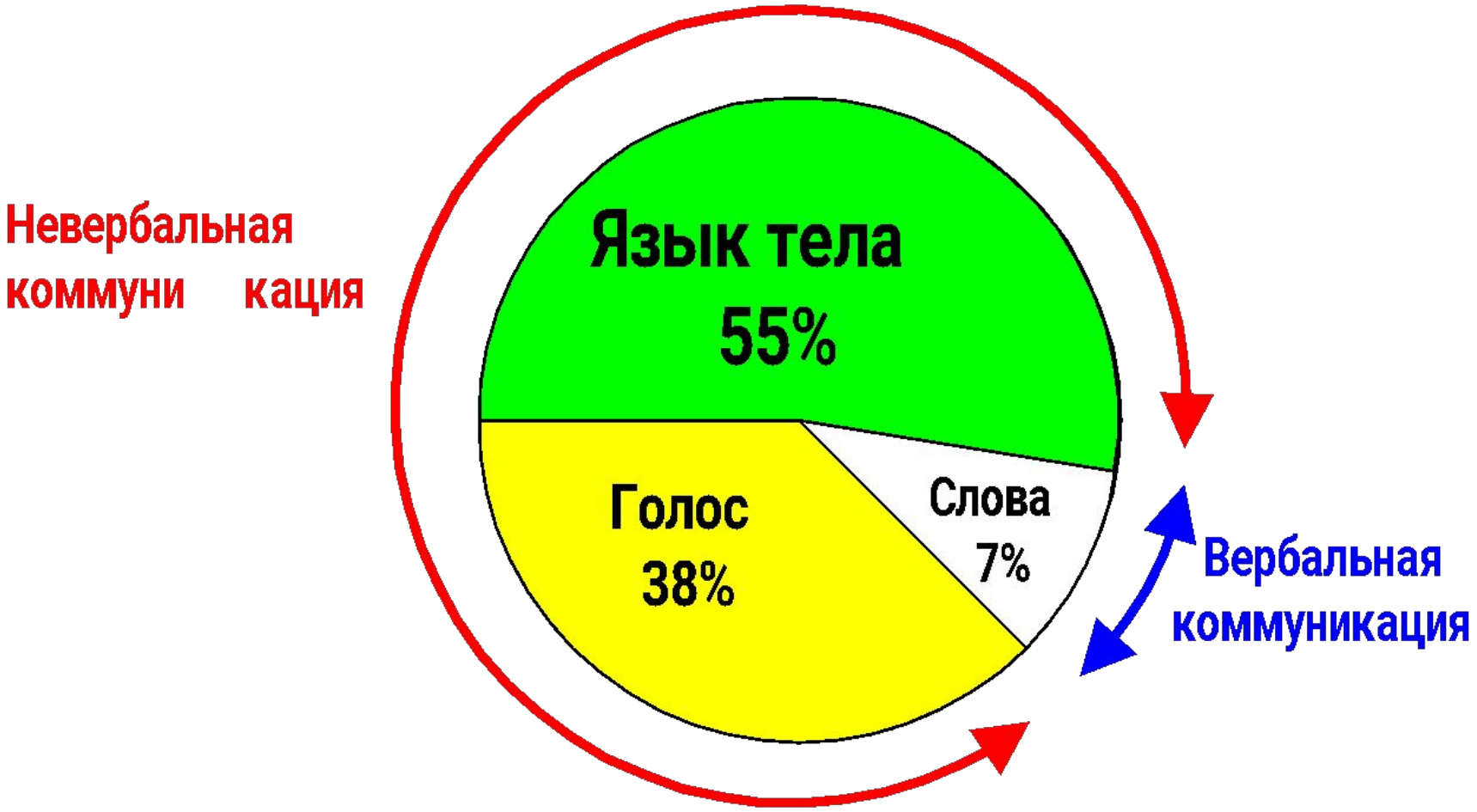
Предоставление компрометирующей информации, с дальнейшим шантажом.

Возможные мишени воздействия

- Обида, месть.
- Корыстные мотивы.
- Компромат.
- Чувство привязанности, влюбленности.

Доверие – основа эффективного общения (коммуникации)

Сознательное и подсознательное доверие



Пользователи ЭВМ

основной источник угроз информационной безопасности

Техники социальной инженерии

- Претекстинг
- Фишинг
- Кви про кво
- Троянский конь
- Дорожное яблоко
- Сбор информации из открытых источников
- Спам

Претекстинг

это набор действий, проведенный по определенному сценарию и заставляющий цель совершить определенное действие или предоставить определенную информацию.

Телефон

Фишинг

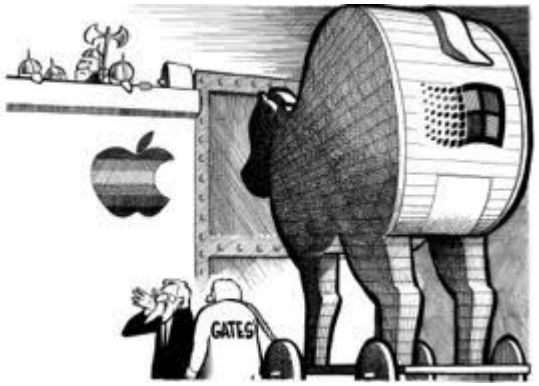
техника, направленная на незаконное получение конфиденциальной информации

Кви про кво

Данный вид атаки подразумевает звонок злоумышленника в компанию по корпоративному телефону.

Троянский конь

Эта техника зачастую эксплуатирует любопытство, либо другие эмоции цели.



Дорожное яблоко

Этот метод атаки представляет собой *адаптацию троянского коня*, и состоит в использовании физических носителей. Злоумышленник может подбросить инфицированный CD, или флэш, в месте, где носитель может быть легко найден (туалет, лифт, парковка).

Сбор информации из открытых источников

Это способом получения информации стал её сбор из открытых источников, главным образом из *социальных сетей*.

Прочее

Злоумышленник получает информацию, например, путем сбора информации о служащих объекта атаки, с помощью обычного телефонного звонка или путем проникновения в организацию под видом ее служащего.

Злоумышленник может позвонить работнику компании (под видом технической службы) и выведать пароль, сославшись на необходимость решения небольшой проблемы в компьютерной системе.

Имена служащих удается узнать после череды звонков и изучения имён руководителей на сайте компании и других источников открытой информации (отчётов, рекламы и т. п.).

Используя реальные имена в разговоре со службой технической поддержки, злоумышленник рассказывает придуманную историю, что не может попасть на важное совещание на сайте со своей учетной записью удаленного доступа.

Другим подспорьем в данном методе являются
исследование мусора организаций, виртуальных мусорных корзин, кража портативного компьютера или носителей информации.

Обратная социальная инженерия

Целью обратной социальной инженерии (*reverse social engineering*) является заставить цель самой рассказать о своих паролях, информацию о компании.

Пример:

При использовании эл. почты многие делают секретным вопросом "девичья фамилия матери" — тогда хакер звонит жертве и представляется сотрудником социальной (опрашиваемой, государственной, муниципальной и др.) службы, проводит опрос о родителях — и одним из вопросов является вопрос о девичьей фамилии матери — жертва её называет и даже не предполагает что только это и нужно было злоумышленнику, т. к. человеческий мозг не смог связать безопасность своей почтовой системы и опрос о родителях.

Этапы воздействия на объект

- Формулирования цели воздействия.
- Сбор информации об объекте.
- Обнаружение наиболее удобных мишеней воздействия.
- Создание нужных условий для воздействия на объект.
- Понуждение к нужному действию.
- Использование результатов воздействия.

Способы защиты от социальной инженерии

Антропогенная защита

- Привлечение внимания людей к вопросам безопасности.
- Изучение и внедрение необходимых методов и действий для повышения защиты информационного обеспечения.
- Осознание пользователями всей серьезности проблемы и принятие политики безопасности системы.

Техническая защита

К технической защите можно отнести средства, мешающие заполучить информацию и средства, мешающие воспользоваться информацией.

Признаки неправомерных действиях злоумышленников

- прямые
- косвенные

Источники данных о неправомерных действиях злоумышленников

- собственные наблюдения;
- показания очевидцев;
- показания технических средств наблюдения (дежурных и специальных).

Версии

- Нет нарушения информационной безопасности (Ошибка оценки поступившей информации)
- Есть нарушение, но оно совершено неумышленно.
- Есть умышленное нарушение.

Виды ответственности за нарушение ЗИ

- Дисциплинарно-материальная
- Гражданско-правовая
- Административная
- Уголовная

Признаки нарушений ЗИ

- Прямые
- Косвенные
- Установленные с помощью аппаратно-программных средств
- Установленные на основании собственных наблюдений
- Установленные на основании информации, полученной из иных источников

Косвенные признаки, указывающие на нарушение ЗИ

- нарушение правил ведения журналов рабочего времени компьютерных систем (журналов ЭВМ) или их полное отсутствие;
- необоснованные манипуляции с данными: производится перезапись (тиражирование, копирование), замена, изменение, либо стирание без серьезных на то причин, либо данные не обновляются своевременно по мере их поступления (накопления);
- появление подложных либо фальсифицированных документов или бланков строгой отчетности;

Косвенные признаки, указывающие на нарушение ЗИ

- сверхурочная работа некоторых сотрудников организации без видимых на то причин, проявление повышенного интереса к сведениям, не относящимся к их функциональным обязанностям, либо посещение других подразделений и служб организации;
- выражение сотрудниками открытого недовольства по поводу осуществления контроля за их деятельностью;
- многочисленные жалобы клиентов.

Тактические особенности следственных действий при расследовании преступлений, совершенных применением ЭВМ