Компьютерная безопасность: Введение

Иртегов Д.В.

НГУ

2024

Почему может случиться что-то плохое?

- Объективные обстоятельства
  - Наводнение, землетрясение, падение метеорита
- Субъективные причины
  - По злобе
  - По глупости
- Промежуточные варианты
  - Техническая неисправность
  - Пожар, обрушение потолка, прорыв водопровода

По злобе или по глупости

- Юристы это называют
  - Умышленное причинение ущерба («по злобе»)
  - Неумышленное («по глупости»)
- Чем категоризация на злобу и глупость лучше?
  - Она допускает промежуточное состояние:
    по сочетанию злобы и глупости
  - E.q. хотел причинить какой-то конкретный ущерб,
    а по глупости причинил другой
    - Не обязательно меньший
    - Но и не обязательно больший

Почему деление на злобу и глупость важно?

- Разная структура угроз и распределение ответственности
- Некоторые вещи можно сделать только по злобе
  - Например, украсть компьютер
  - Ущерб от глупостей может быть не меньше
- От злых людей вашу организацию защищают, кроме вас:
  - Охрана, отдел кадров, скрининг персонала
  - Полиция, юристы
- Глупость может сделать любой сотрудник
  - В том числе вы
- На глупость можно спровоцировать
  это называется *социальная инженерия*

Что плохого можно сделать с компьютером?

- Кража данных
- Несанкционированная модификация данных
- Отказ сервиса, например
  - Сломать компьютер
  - Уронить сервер
  - Уничтожить данные
- Нецелевое использование, например
  - Майнинг биткойнов
  - Рассылка спама
  - Взлом других компьютеров

Комбинированные плохие вещи

- Компьютер рядового сотрудника взламывают
  - Или самого сотрудника инженерят что-то запустить/установить
- Запускают на нем агент для доступа к корпоративной сети
- Взламывают продуктивные сервера (возможно, по цепочке)
- Пример: Aurora attack (когда китайцы ломали гугль)

Еще общих соображений

- Теоретически, модель безопасности современных ОС (как Linux, так и Windows) непробиваема
- Все проблемы с безопасностью, так или иначе, «практические»:
  - Физический доступ к компьютеру
  - «Социальная инженерия» и другой человеческий фактор
  - «Уязвимости»
    - Ошибки в программном коде ОС и приложений
    - Ошибки администратора при развертывании ОС и приложений
    - Логические бомбы или «закладки» (умышленно внедренный вредоносный код)
    - «Задние двери» (отладочные средства, которые неумышленно забыли выключить в релизной/продуктивной версии)

Уязвимости

- Деление на ошибки, «логические бомбы» и «задние двери» условно: мы не знаем, что творилось в голове у человека, который делал ошибку (это к вопросу про злобу и глупость). И наоборот, хорошие логические бомбы могут быть замаскированы под ошибки.
- Наиболее опасные типы ошибок могут приводить к удаленному исполнению кода
  - Срывы буфера в программах на C/C++/Fortran/Rust
  - Инъекция скрипта в языках, где есть оператор eval или эквиваленты (JavaScript, Python, unix shell, да тыщи их)
  - Инъекция SQL
  - Cross-site scripting
- Если вы исполнили чужой код на вашем компьютере, это больше не ваш компьютер

Общие подходы и принципы

- Комплексная («эшелонированная») безопасность
  - Пробив защиту в любом месте, хакер должен оказываться в изолированной среде с ограниченным доступом
  - Ему придется тратить время на пробивание следующих слоев
  - Чем дольше он этим занимается, тем выше шанс что
    - Он где-то застрянет
    - Это обнаружат и прекратят
    - Или даже что его поймают
  - Роботическая атака на этом, скорее всего, и закончится
- Принцип минимума привилегий
  - Помогает и от глупостей со стороны сотрудников
- Чем-то отличаться от других
  - Нам не нужно бежать быстрее Балрога, нам достаточно бежать быстрее тебя
  - Хорошо помогает от автоматических атак («червей», вирусов)
  - От хакеров тоже помогает