Сетевые атаки

Классификация атак:

По характеру воздействия

- Пассивное
- Активное

По цели воздействия

- Нарушение функционирования системы (доступа к системе)
- Нарушение целостности информационных ресурсов (ИР)
- Нарушение конфиденциальности ИР

По условию начала осуществления воздействия

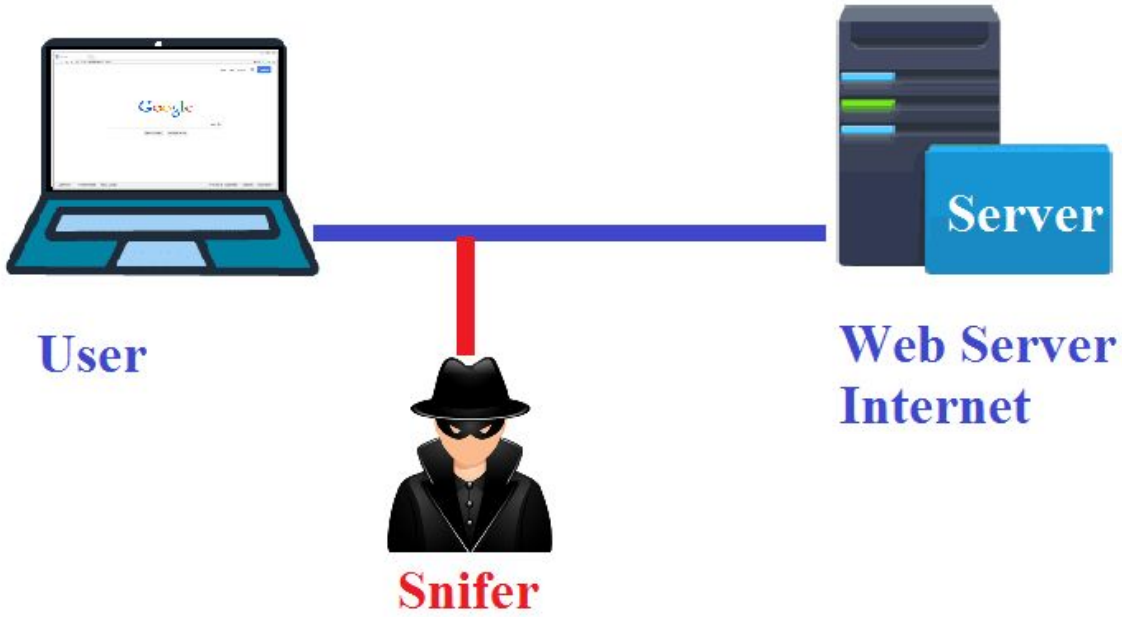
- Атака по запросу от атакуемого объекта
- Атака по наступлению ожидаемого события на атакуемом объекте
- Безусловная атака

Переполнение буфера(buffer overflows)

Основывается на поиске программных или системных уязвимостей, способных вызвать нарушение границ памяти и аварийно завершить приложение или выполнить произвольный бинарный код от имени пользователя, под которым работала уязвимая программа

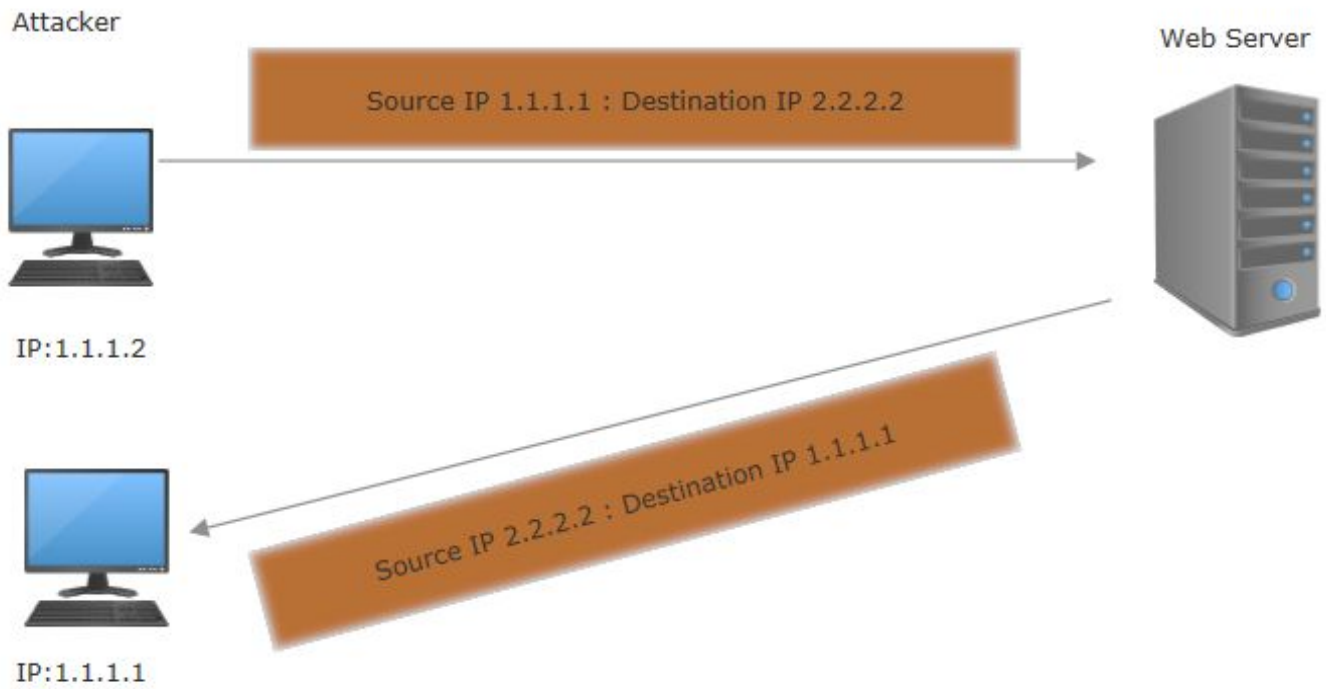
Sniffing

Прослушивание канала



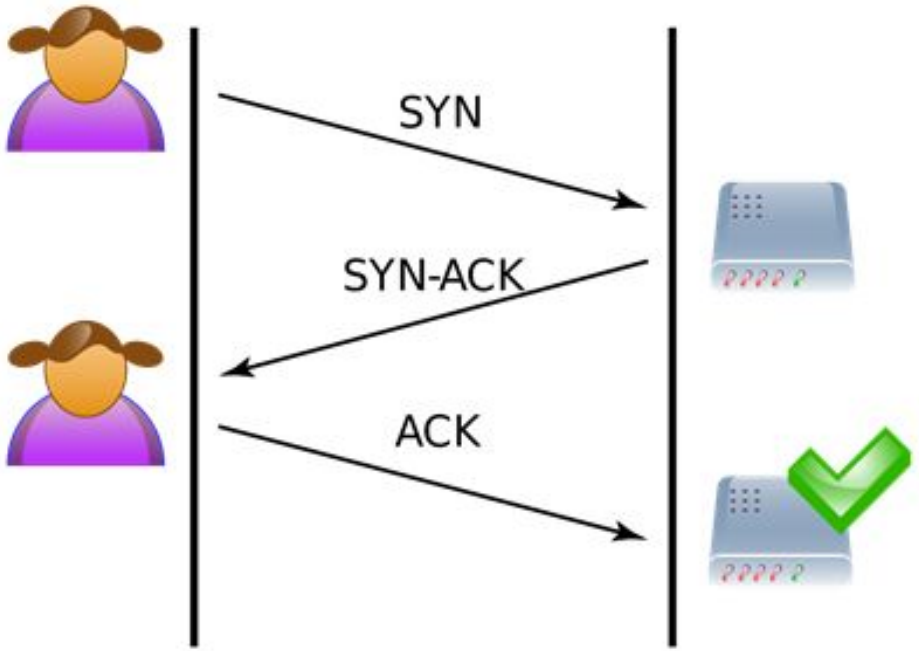
IP spoofing

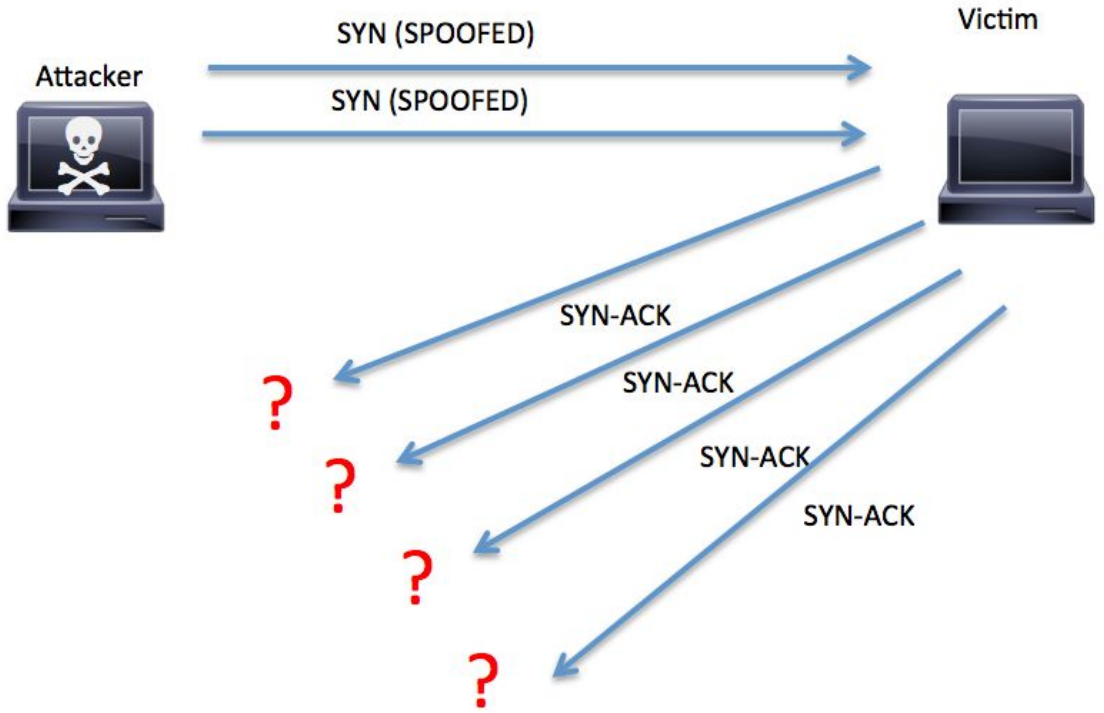
Использование чужого IP-адреса с целью обмана системы безопасности



SYN-flood

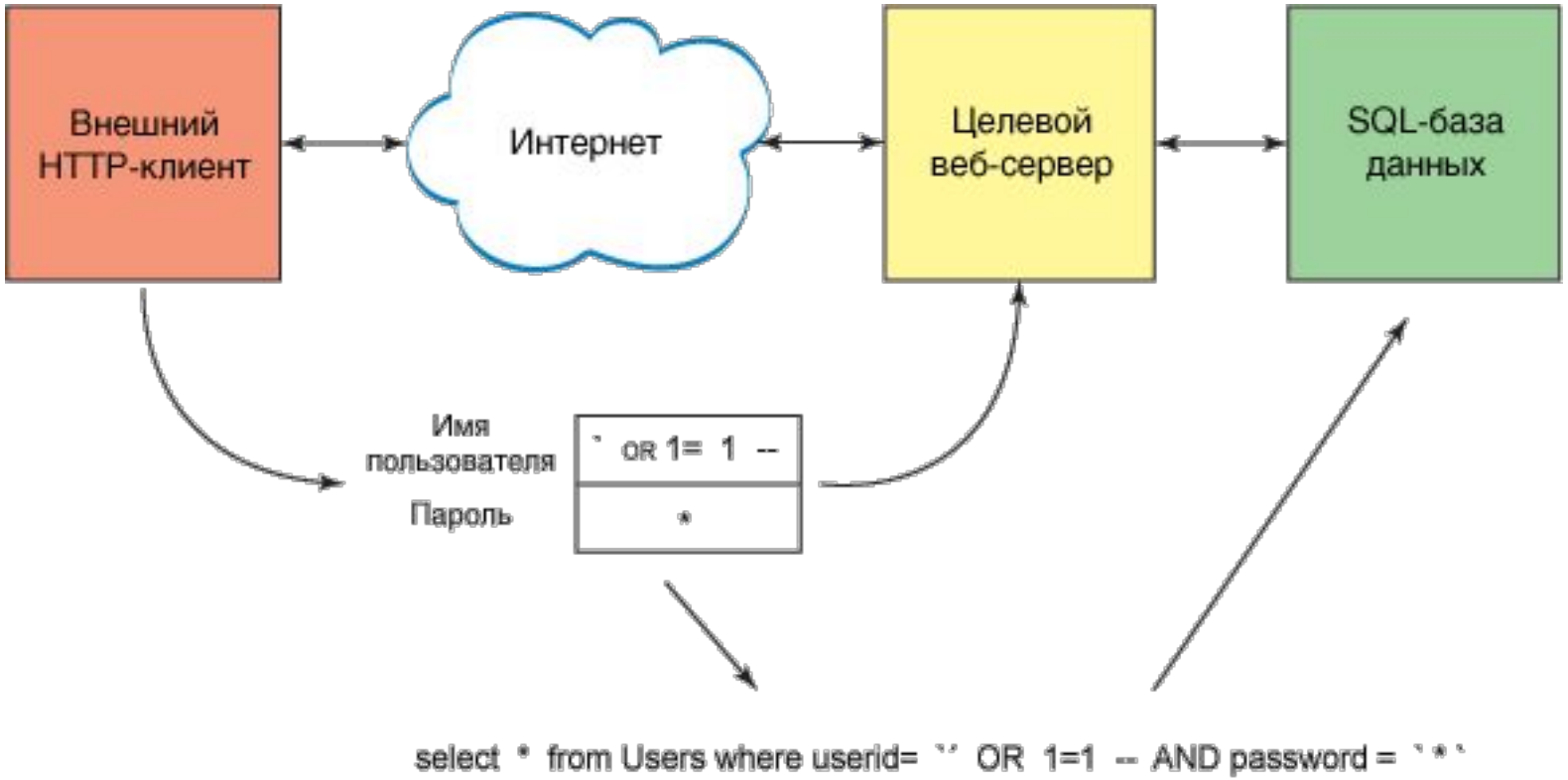
Заключается в отправке большого количества SYN-запросов в достаточно короткий срок





SQL инъекция

Внедрение в данные (передаваемые через GET, POST запросы или значения Cookie) произвольного SQL кода.



Атака SMURF

Имеет эффект усиления, являющийся результатом отправки прямых широковещательных запросов ping к системам, которые обязаны послать ответ