Университет ИТМО
Факультет программной инженерии и компьютерной техники

Лабораторная работа №4
по дисциплине «Информационная безопасность»
«Атака переполнения буфера»

Выполнил:Ларочкин Г.И
Группа: P3400
Преподаватель: Маркина Т.А.

Санкт-Петербург
2021 г.

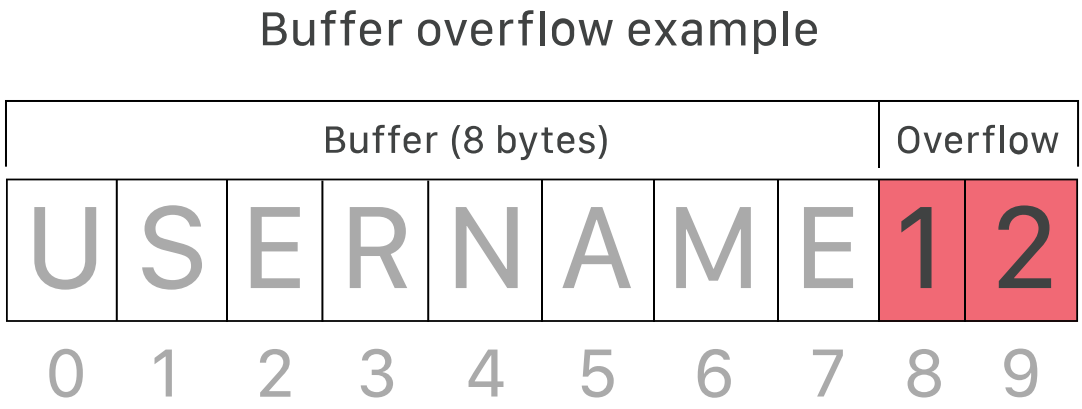
Оглавление

1. Описание

Атака переполнения буфера, или buffer overflow attack – это тип атаки, когда в ходе манипуляции входными данными программа или системный процесс помещает больше данных, чем изначально выделено для буфера и происходит перезапись данных в смежных регионы памяти. Таким образом, взломщик осуществляет вмешательство исполняемую программу, изменяя её поведение.

Цель атаки – изменение данных, используемых программой, для проникновения и дальнейшего исследования атакующим, или же предотвращение её дальнейшего исполнения. Объектами атаки обычно являются популярные библиотеки, используемые большим количеством программных систем, различного рода приложений с, содержащих личные данные, VPN сервисы и даже операционные системы.

Атаки переполнения буфера бывают различных видов. В основном различают два основных вида: stack overflow attack в котором производится манипуляция с данными, локальными для функции, heap overflow attack, где происходит манипуляция с динамически выделяемыми данными, которые в основном глобально видимы для всего приложения. Первый в свою очередь более приоритетный т. к. требует меньше анализа, а также может позволить получить полный доступ к целевой системе за счёт манипуляции с правами.



Общий принцип атаки – злоумышленники идентифицируют уязвимость переполнения буфера, определяет точный размер буфера. Атакующий должен иметь полный контроль над записью в буфер, иначе атака провалена. После буфера должны находиться чувствительные к безопасности данные или же исполняемый регион, иначе атака провалена.

Атакующий может подменить чувствительные к безопасности данные или же записать инструкции в исполняемый регион.

2. Развитие атаки

Атакующий может иметь совершенно различные цели, это может быть как полная остановка системы/приложения, получение полного доступа к системе или же получение полезных данных. Её можно разделить на два отдельных этапа: подготовка и действие.

Подготовка

На этом этапе злоумышленник изучает целевую систему на наличие уязвимостей. Это может быть как изучение исходного кода, ручной поиск или же сторонние утилиты. Также на этом этапе происходит анализ чувствительных к безопасности данных, это также может происходить перебором или анализом исходного кода. Данный этап легче осуществлять именно с stack-based overflow уязвимостью т. к. изучение ограничено лишь областью видимости функции.

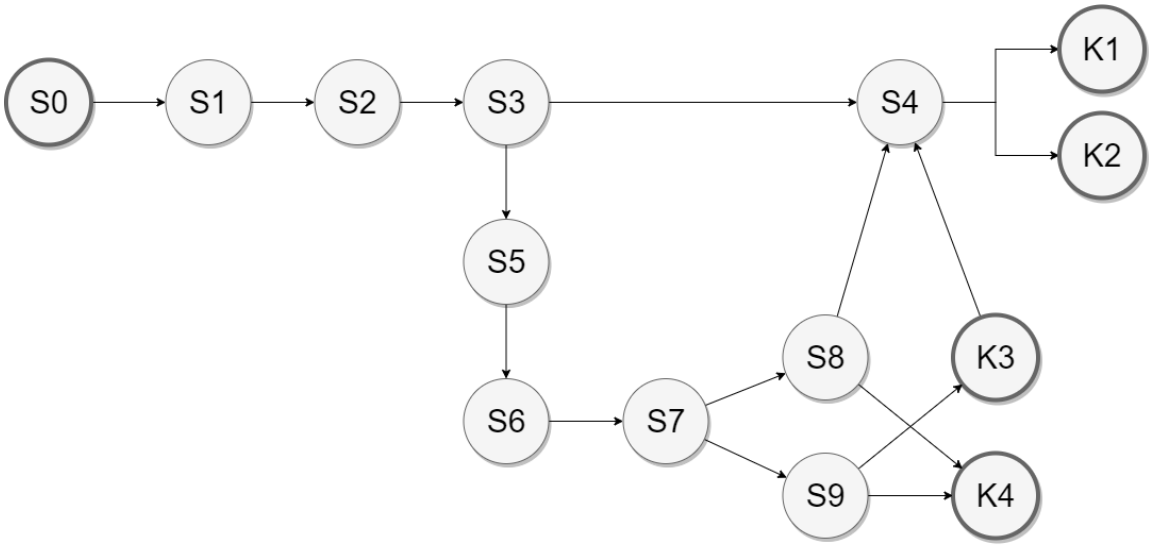
Действие

Если нашлись чувствительные к безопасности данные, то злоумышленник уже на этом этапе может получить полезную для него информацию.
Если таковых нет, то злоумышленник может получить контроль над ходом исполнения программы:

1. С помощью перезаписи адреса возврата
2. Если буфер executable, то с помощь инъекции исполняемых инструкций

Если злоумышленнику удалось получить контроль над исполнением программы, то он может производить манипуляции в операционной системе, например, добавление пользователей/повышение прав. Или же просто завершить исполнение программы.

3. Граф атаки



Действия злоумышленника:
S1 - подготовка: идентификация уязвимости (мануальная исследование реакции системы на входные данные, исследование поведения клиентской программы, использование сторонних средств)
S2 - Идентификация размера буфера
S3 - Исследование чувствительных к безопасности данных
S4 - Подбор подходящих данных (например, пароль)
S5 - Подмена адреса возврата
S6 - Подмена исполняемой программы
S7 - Внедрение бекдор процесса
S8 - Исследование окружения целевой системы
S9 - Повышение привелегий в операционной системе

Возможные исходы:
K1 - Кража информации
K2 - Подмена информации
K3 - Несанкционированное изменение привелегий системы
K4 - Отказ в доступе системы