Пример атаки на IP - сеть:
«Переполнение буфера»

Цель

Получение контроля над объектом атаки

Механизм реализации

Запуск кода на атакуемом узле

Местонахождение атакующего

В разных сегментах с объектом атаки

Используемые уязвимости

Ошибки реализации

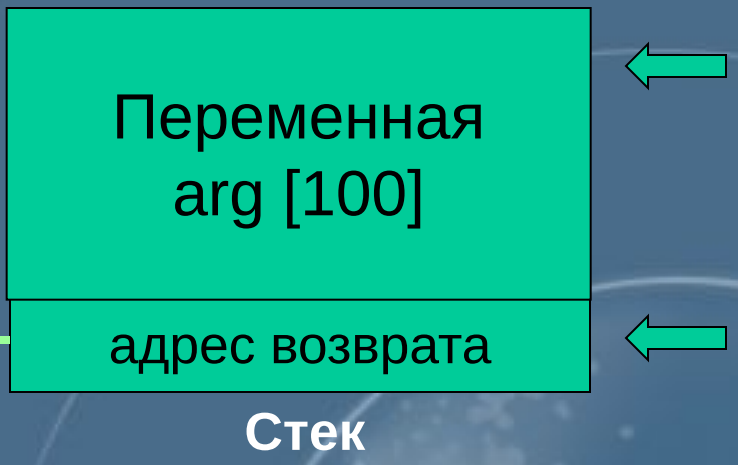
Степень риска ***Высокая***

Пример атаки на IP - сеть:
«Переполнение буфера»

```
int f_vulner (char arg)
{
    char local[100]
    //обработка
    return 0
}
void main()
{
    char arg[200]
    gets (arg)
      .
      .
    f_vulner (arg)
    printf(arg)
    return 0
}
```

strcpy(local, arg)

Обычный ход выполнения программы



Пример атаки на IP - сеть:
«Переполнение буфера»

```
int f_vulner (char arg)
{
    char local[100]
    //обработка
    return 0
}
void main()
{
    char arg[200]
    gets (arg)
      .
      .
    f_vulner (arg)
    printf(arg)
    return 0
}
```

strcpy(local, arg)
Ошибка !

Переполнение стека

Этапы проведения атаки «Переполнение буфера»

Подготовка враждебного кода

Под видом команд или параметров уязвимого приложения

В адресном пространстве уязвимого приложения (без параметров)

В адресном пространстве уязвимого приложения (с параметрами)

Передача управления враждебному коду

Методы защиты

Установка пакетов исправления

Исправление исходного кода с перекомпиляцией

Тестирование программ специальными утилитами

Пример атаки на IP - сеть:
«Троянский конь»

Цель

Получение контроля над объектом атаки

Механизм реализации

Запуск кода (приложения) на объекте атаки

Местонахождение атакующего

В разных сегментах с объектом атаки

Используемые уязвимости

Ошибки эксплуатации (особенности психологии)

Степень риска ***Высокая***

Пример атаки на IP - сеть:
«Троянский конь»

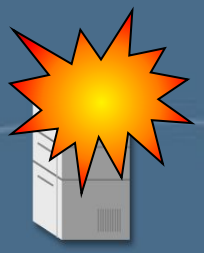
1)

Patch.exe

E-mail from: support@microsoft.com

2)

C:\windows> Patch.exe
C:\windows>



NetBus сервер

3)

Выполнение команд

NetBus клиент