ОНЛАЙН-ОБРАЗОВАНИЕ

OTUS

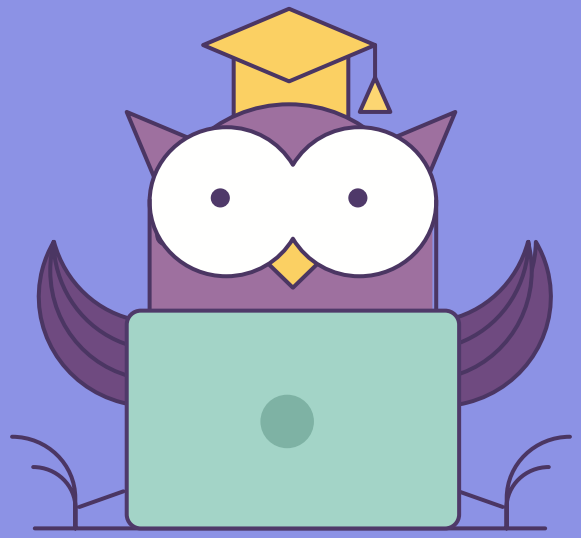
Структура операционной системы Windows

Основные механизмы разграничения доступа.

Часть 1

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

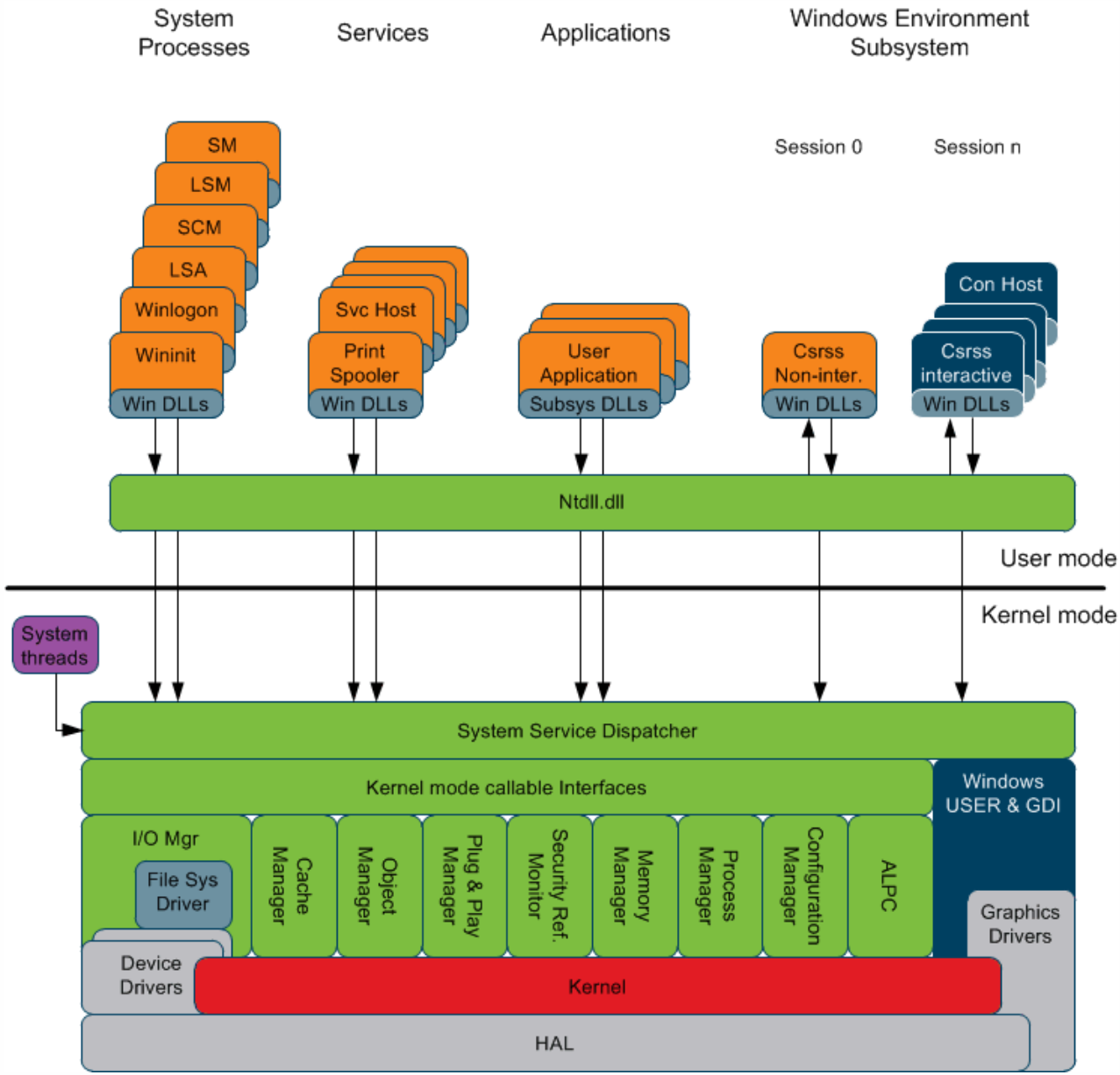
- Операционная система Windows
  - Структура операционной системы
  - Виртуальная память
  - Структура PE
  - Структуры процесса
  - Основные элементы исполняющей подсистемы

- Типы уязвимостей:
  - Классификация (Живых) уязвимостей

01

Операционная система Windows

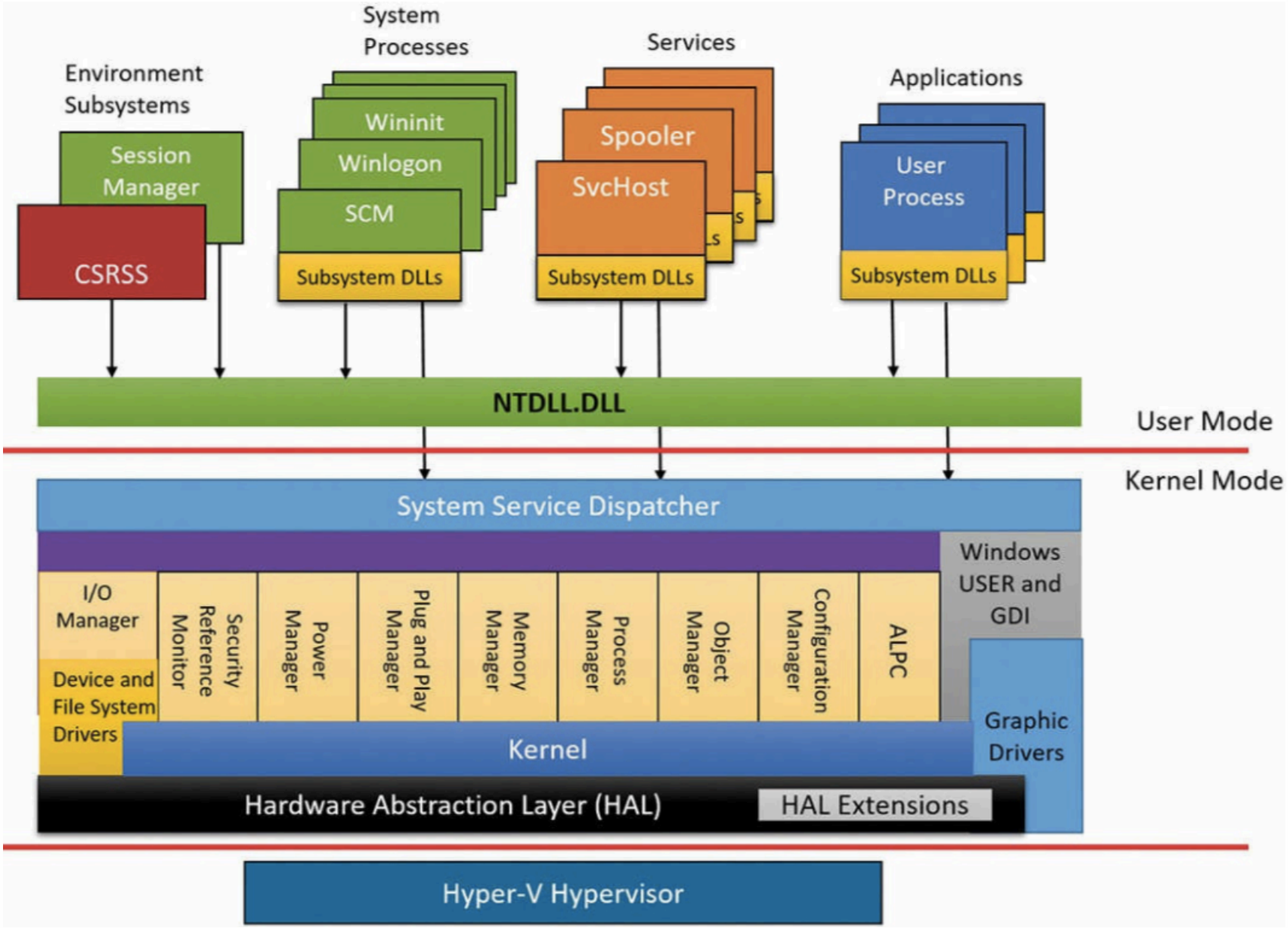
Архитектура Windows (до 10)



Основные особенности WIndows до 10

- Операционная система задумывалась как удобная для использования без навыков в программировании или администрировании.
- Не содержит эффективных механизмов разграничения доступа к ресурсам
- В разных версиях имеет различные системные характеристики, часто завышенные в рекламных целях
- Многоуровневая структура, не имеет четкого логического разделения, многие функции которые выполняют основной функционал одной подсистемы, физически находятся в модулях соседней подсистемы
- Отсутствует полноценный механизм виртуализации
- Архитектура не задумывалась как полностью безопасная, существует множество способов отправки данных напрямую в функции ядра, без дополнительной проверки

Архитектура Windows (10)



Основные особенности Windows 10

Основные отличия от предшествующих версий операционной системы:

- Появление новой прослойки системных функций UWP(United Windows Platform)
- Появление подсистем защиты ядра средствами виртуализации
- Появления контейнеров, которые могут быть использованы системой Docker или ей подобной
- Новая подсистема разграничения доступа (За счет виртуализации)
- Более современные решения для работы с памятью
  - Изменен алгоритм формирования heap
  - Изменен алгоритм высвобождения памяти
- Появление новых системных процессов, которые отвечают за разграничение доступа к ресурсам и операционной системе
- Появление новых типов процессов, которые имеют достаточно размытое описание из-за закрытого исходного кода операционной системы
- Появление новых приложений, которые по структуре напоминают исполняемые файлы операционных систем Android и iOs. (Windows Apps)

02

Организация и работа памяти

Основные понятия

OTUS

В зависимости от разрядности устанавливается объем памяти для процесса:

- 4 Гб для 32-битных процессоров
- 8 Тб для 64-битных процессоров

Каждое выделенное пространство в памяти не позволяет получить доступ к памяти другого процесса. (Если не было произведено разделение памяти)

64-bit register	Lower 32 bits	Lower 16 bits	Lower 8 bits
rax	eax	ax	al
rbx	ebx	bx	bl
rcx	ecx	cx	cl
rdx	edx	dx	dl
rsi	esi	si	sil
rdi	edi	di	dil
rbp	ebp	bp	bpl
rsp	esp	sp	spl
r8	r8d	r8w	r8b
r9	r9d	r9w	r9b
r10	r10d	r10w	r10b
r11	r11d	r11w	r11b
r12	r12d	r12w	r12b
r13	r13d	r13w	r13b
r14	r14d	r14w	r14b
r15	r15d	r15w	r15b

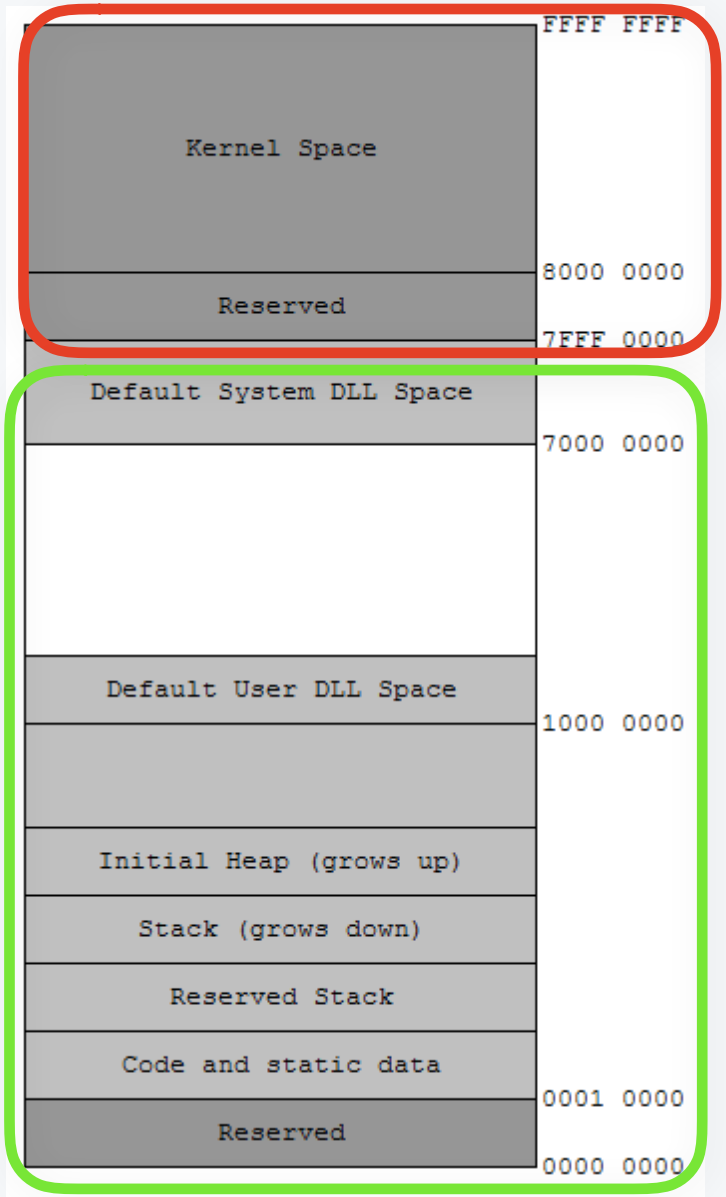
Карта памяти

Виртуальная память != физическая память, которая непрерывна

Виртуальная память организуется в таблицы, которые состоят из страниц.

Виртуальное пространство адресов процесса делится на две части:

- Системная память
- Память пользовательская



Ограничение виртуальной памяти

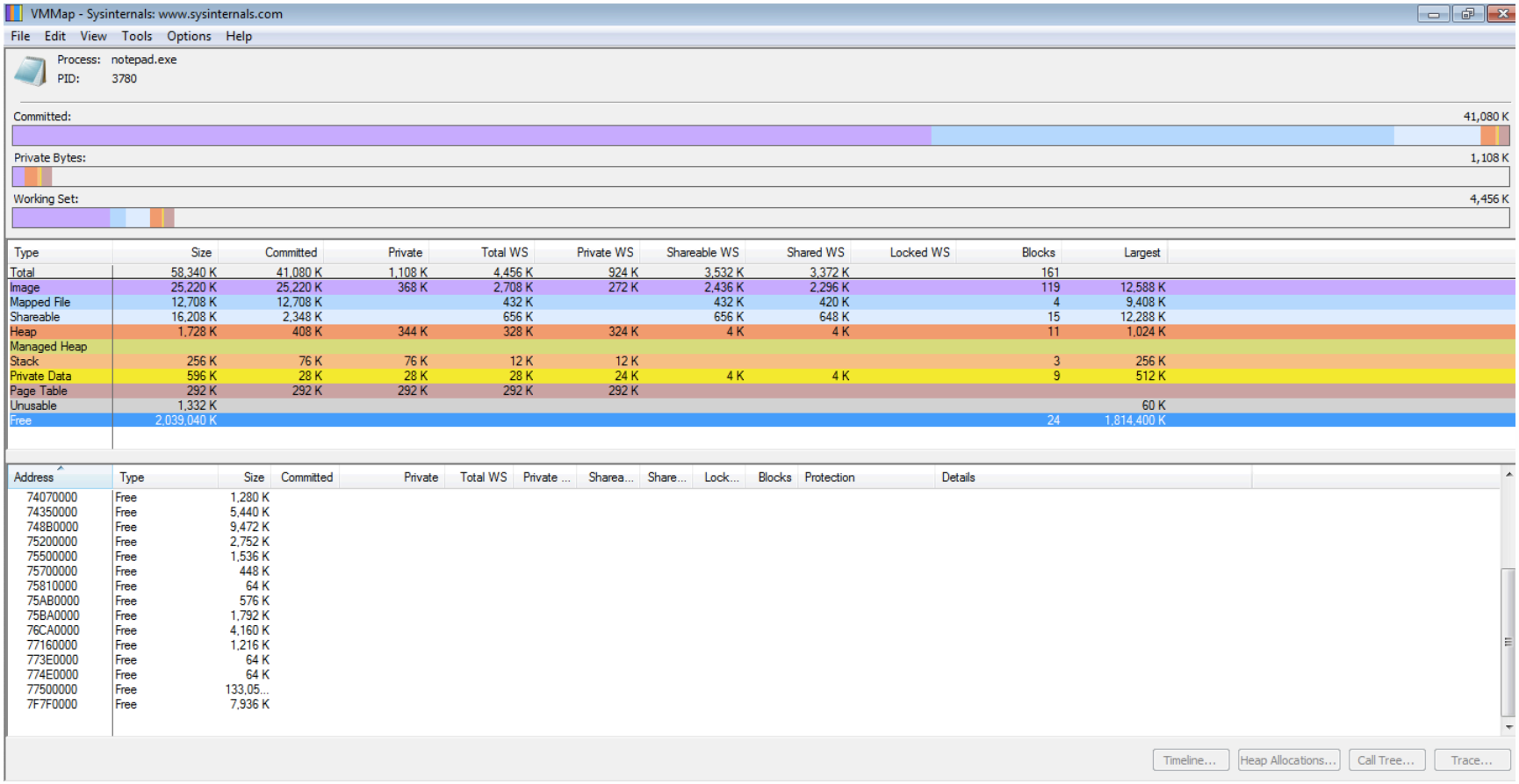
	x86	x64
Пользовательская часть для 32-битных процессов	2 GB (4 GB при расширенной памяти)	2 GB (4 GB при использовании расширения)
Пользовательская часть для 64 - битных процессов	-	8 TB (128 TB при расширение) 2 GB при выключенном расширении
Системная часть	2 GB	8 TB до 128 TB

01

Практика

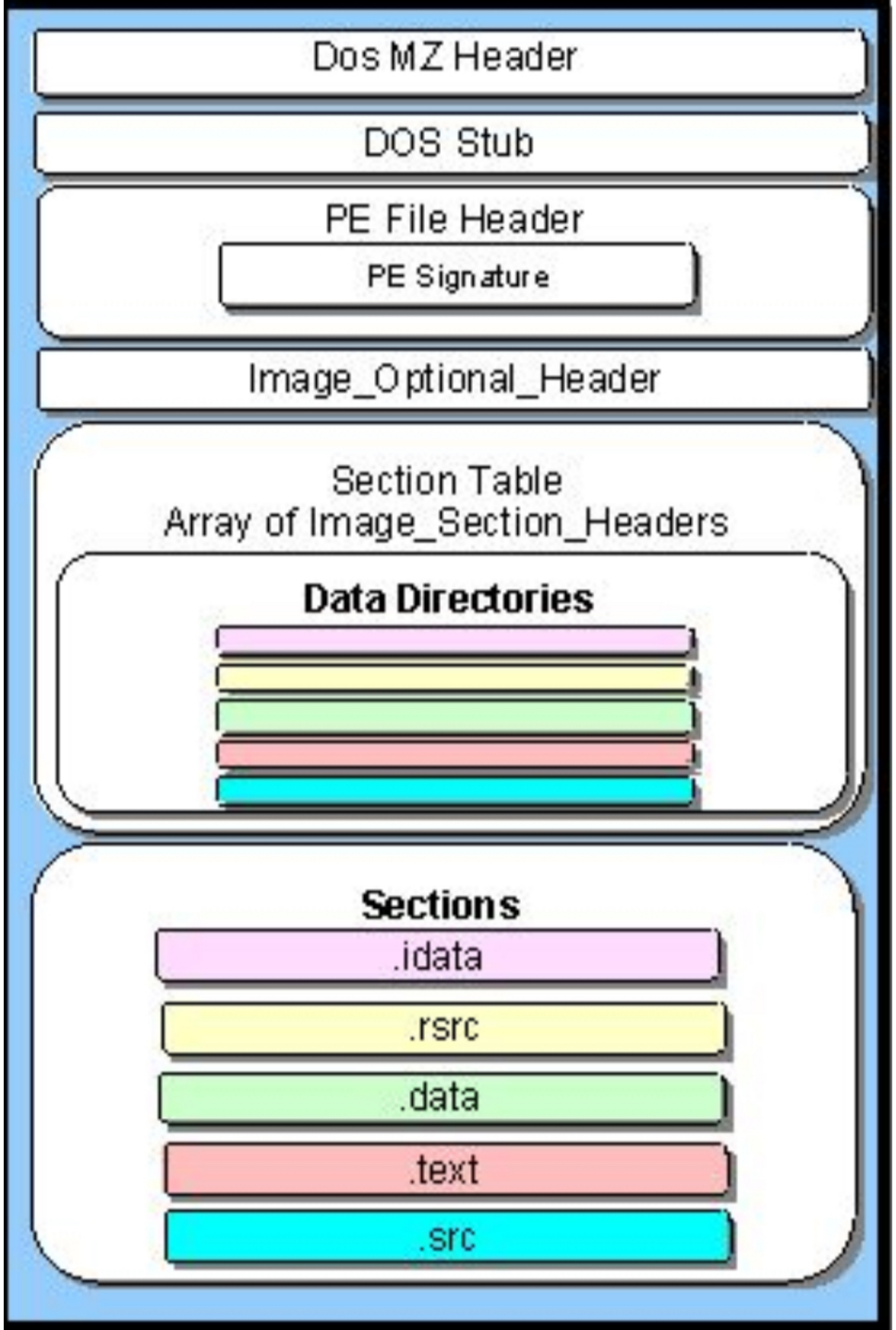
Просмотр пользовательского пространства памяти

Разметка пользовательского адресного пространства



03

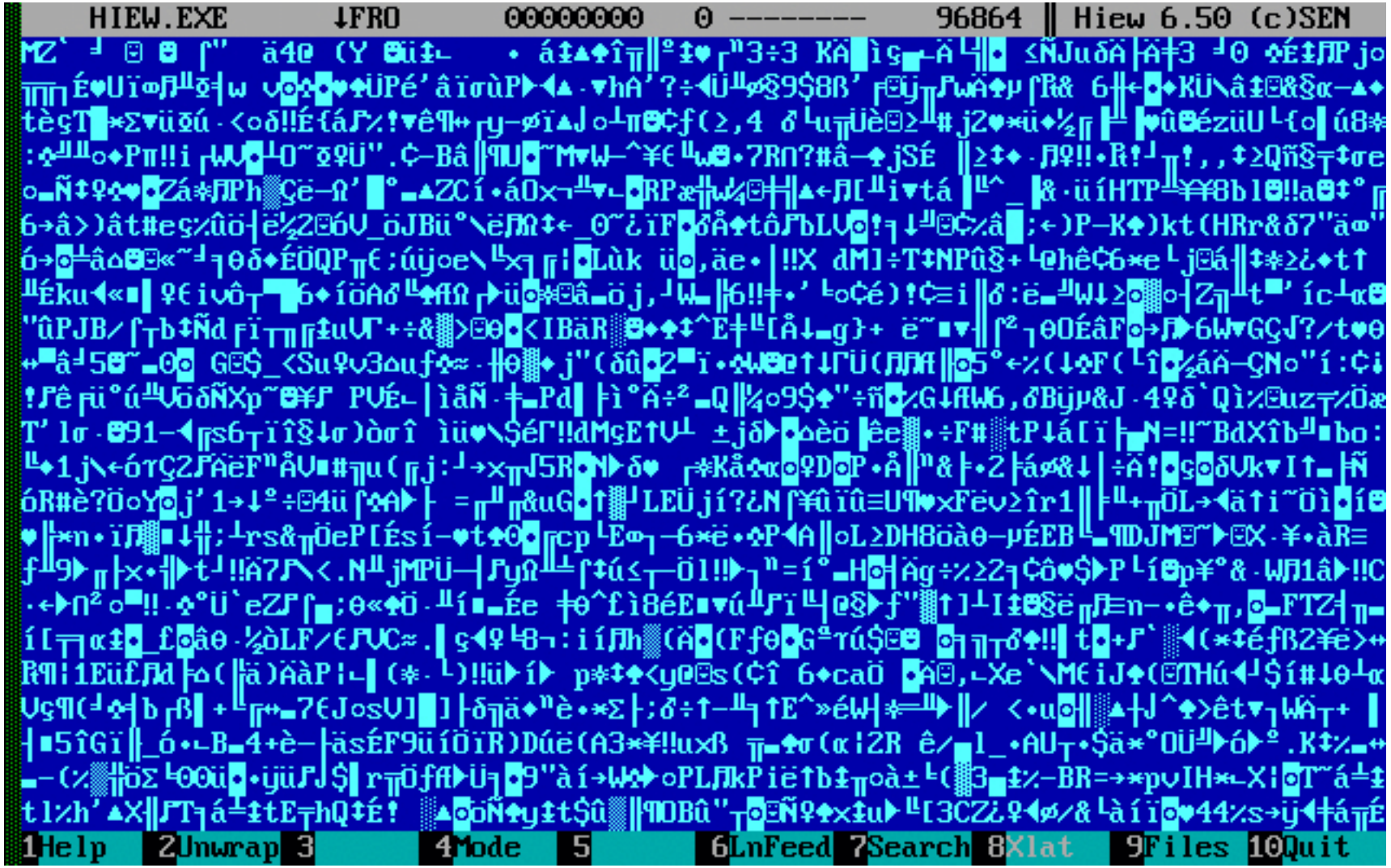
Структура PE файла


Dos MZ Header
DOS Stub
PE File Header
PE Signature
Image_Optional_Header
Section Table
Array of Image_Section_Headers
Data Directories
Sections
.idata
.rsrc
.data
.text
.src

01

Просмотр структуры файла

PE файл в ASCII представлении



Просмотр структур PE в Windbg

Список команд:

- dt _IMAGE_DOS_HEADER 0xaaaaaaaa
- !dh 0xaaaaaaaa -f
- dd 0xaaaaa
- ? 123213
- dc 0xaaaaa

Где найти заголовочные файлы:

https://github.com/Alexpux/mingw-w64/blob/master/mingw-w64-tools/widl/include/winnt.h

04

Структуры процесса

Процесс

Объект исполняющей системы

Может содержать в себе потоки.

Информация о его состоянии и характеристиках хранится в отдельных структурах данных.

Процесс

Ядро:
EPROCESS
ETHREAD
ETHREAD
Пользователь:
PEB
TEB

01

Исследование структур процесса

Исследование структур процесса

- **Чтобы отобразить структуры процесса необходимо:**
  - Запустить операционную систему в режиме отладки
  - Запустить WIndbg в режиме отладки локального ядра

- **Для структуры EPROCESS:** dt nt!_eprocess
- **Основная команда для работы с процессом:** !process
- **Основная команда для ресурсов процесса:** !handle

- **Информация о окружении процесса:** !peb 0xaaaaa - адрес структуры

05

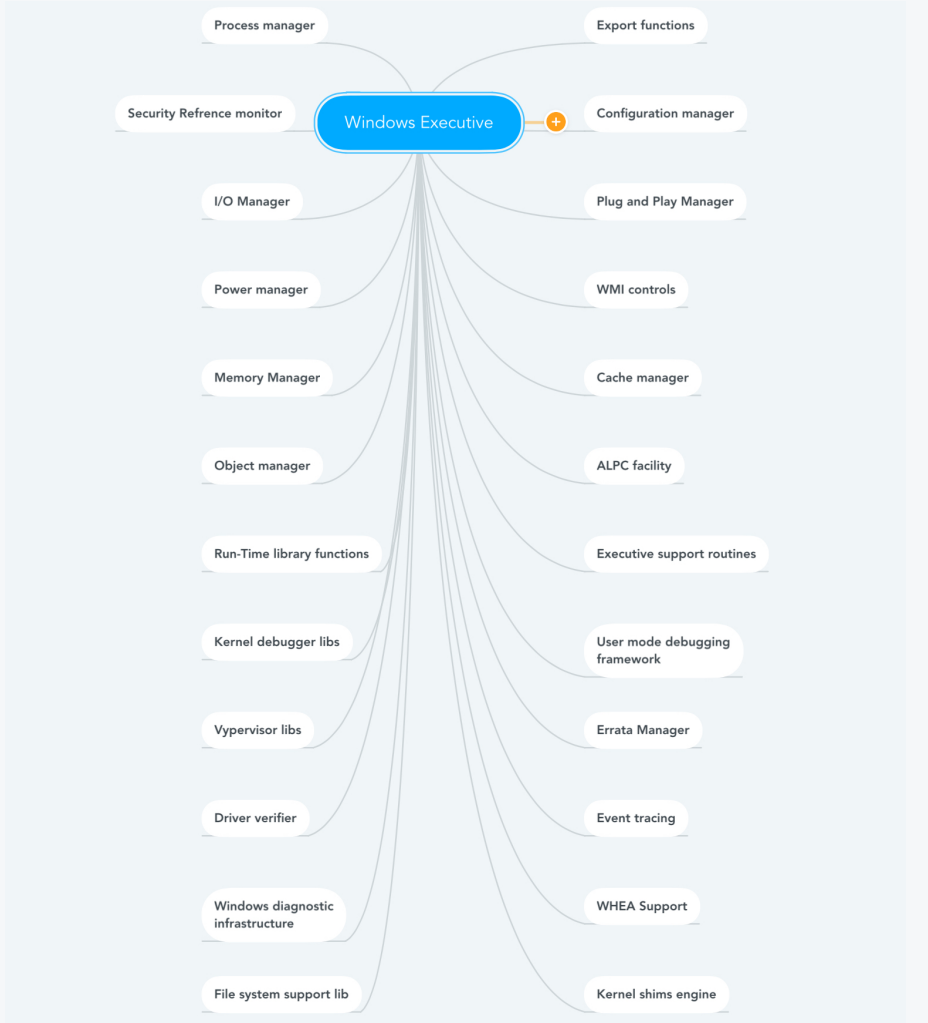
Элементы исполняющей подсистемы

Исполняющая подсистема

Из-за особенности архитектуры это не отдельная подсистема.

Основные функции являются верхней надстройкой над ядром операционной системы.

Включает в себя порядка 24 подсистем.



Подсистемы исполняющей системы важные для курса

Memory Manager - подсистема контроля доступа к памяти и выделения ее по запросу.

Object manager - подсистема, которая хранит информацию об объектах в операционной системе.

Security Reference Monitor - подсистема, которая следит за разграничениями доступа и уровнями ограничений.

01

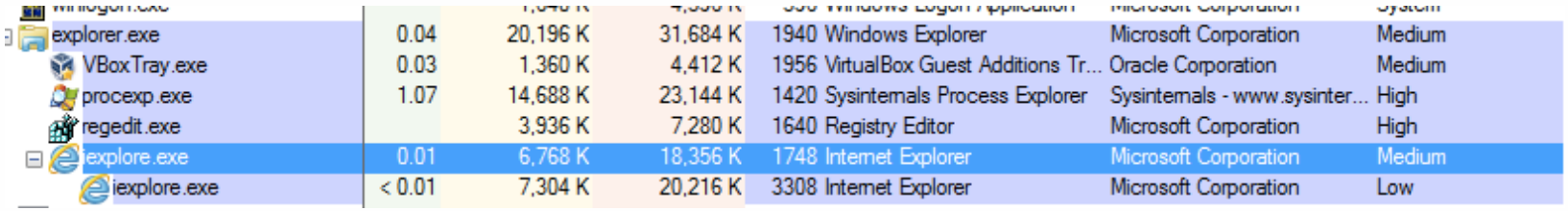
Практика

Просмотр объектов подсистем

Integrity Levels

Чтобы получить настройку, при которой работает опция Internet Settings:

Убедитесь, что в ветке реестра не стоит параметр, запрещающий IE запускать вкладку в песочнице: **HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\TabProcGrowth:0 (Dword)**



explorer.exe	0.04	20,196 K	31,684 K	1940 Windows Explorer	Microsoft Corporation	Medium
VBoxTray.exe	0.03	1,360 K	4,412 K	1956 VirtualBox Guest Additions Tr...	Oracle Corporation	Medium
procexp.exe	1.07	14,688 K	23,144 K	1420 Sysinternals Process Explorer	Sysinternals - www.sysinter...	High
regedit.exe		3,936 K	7,280 K	1640 Registry Editor	Microsoft Corporation	High
iexplore.exe	0.01	6,768 K	18,356 K	1748 Internet Explorer	Microsoft Corporation	Medium
iexplore.exe	< 0.01	7,304 K	20,216 K	3308 Internet Explorer	Microsoft Corporation	Low

Объекты SRM

Объекты, которые позволяют ограничивать доступ к ресурсам системы.

Для пользователей это SID

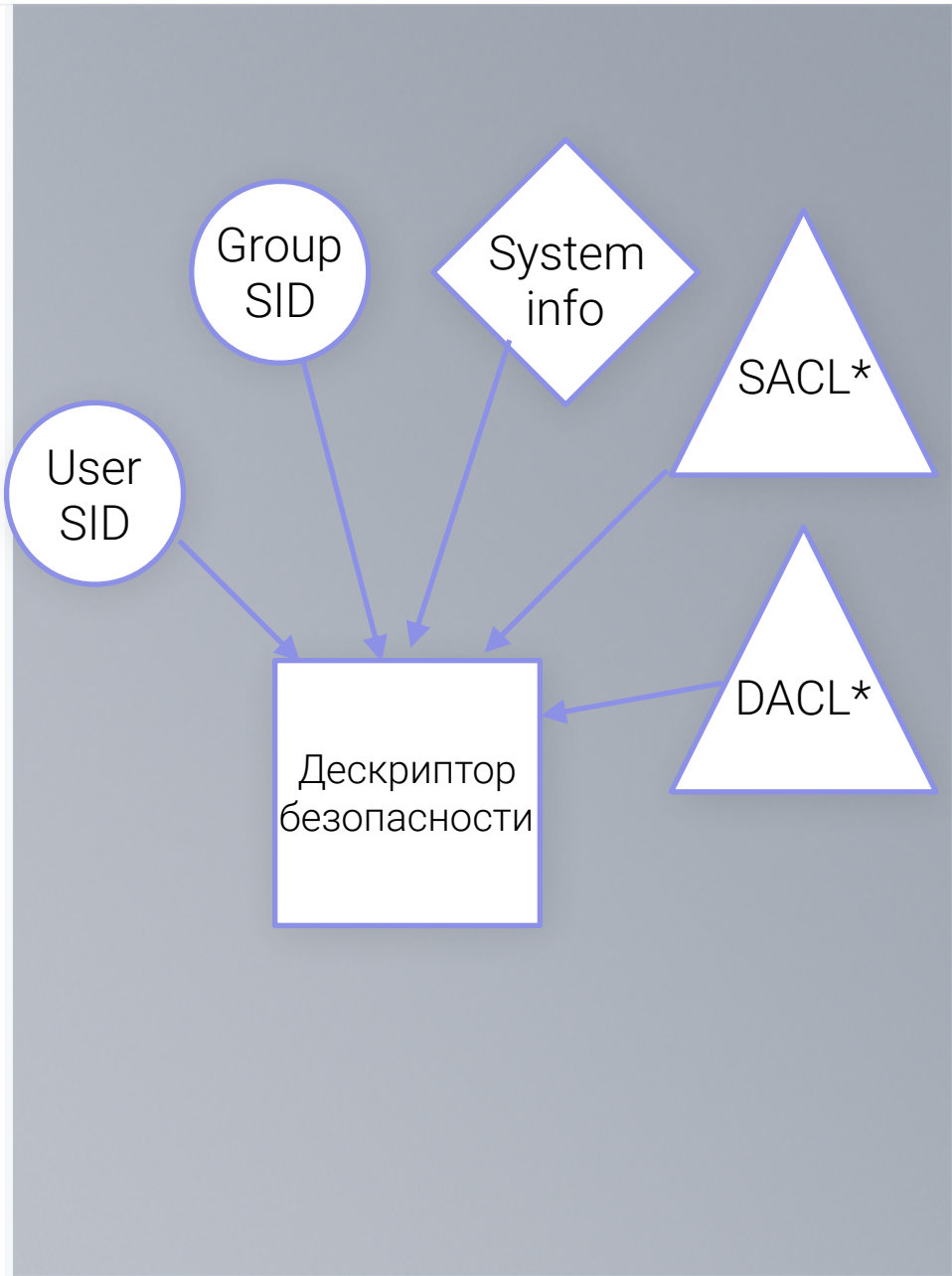
Для процессов - SID уровня целостности

Существует 5 уровней:

- Untrusted
- Low
- Medium
- High
- System

* DACL - Discretionary access list

*SACL - System access control list



Security Descriptor

1) Выполнить команду перевода операционной системы в отладочный режим.

Win7 - bcdedit.exe /debug on.

Задание для самостоятельного выполнения - запустить Win 10 в отладочном режиме.

2) Запустить Windbg - Local kernel debugging

3) Ввести команду: !process 0 0 explorer.exe

4) Ввести команду: !object 0xAAAAAA - адрес объекта из предыдущей команды

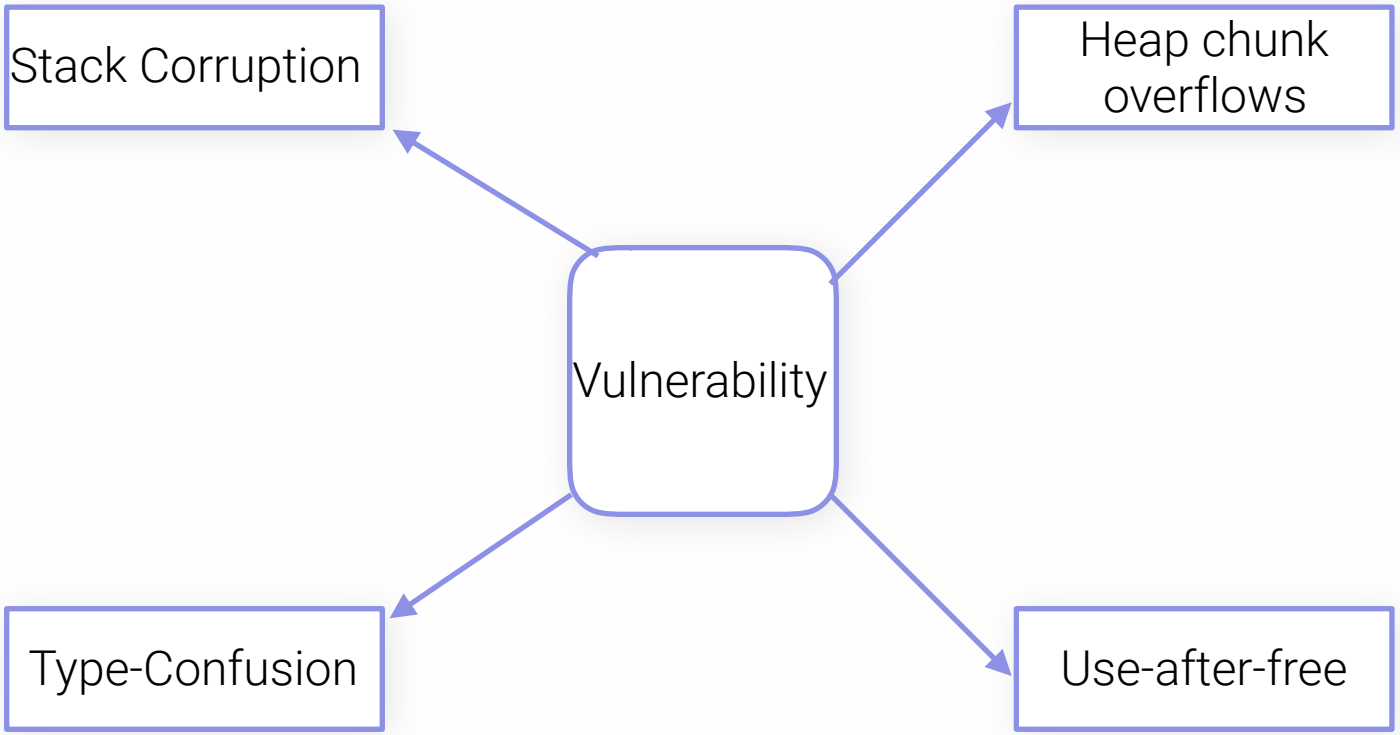
5) Ввести команду: dt _OBJECT_HEADER_ 0xaaaaaa - адрес заголовка объекта

6) Ввести команду: !sd 0xaaaaaa & -8 - (8 - обнуление 3 битов, 10 обнуление 4 битов)

06

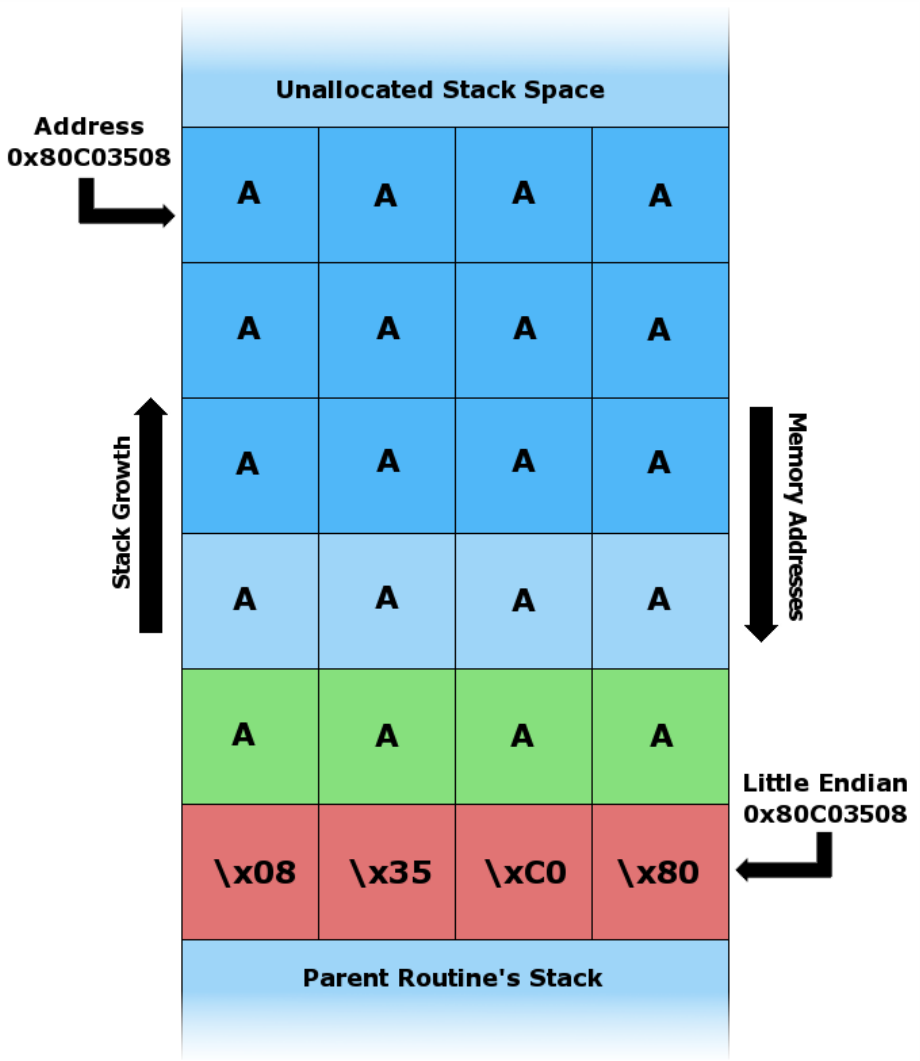
Классификация уязвимостей

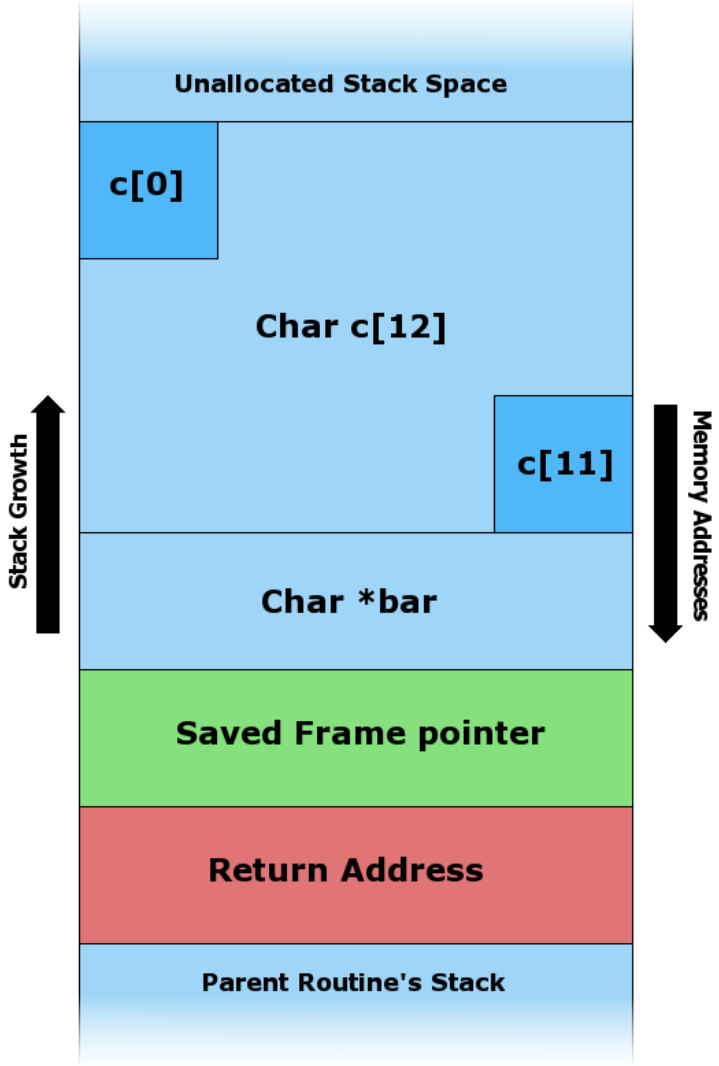
Классификация уязвимостей



Stack Corruption

Повреждение стека или массива данных, которые сохраняются на стеке.

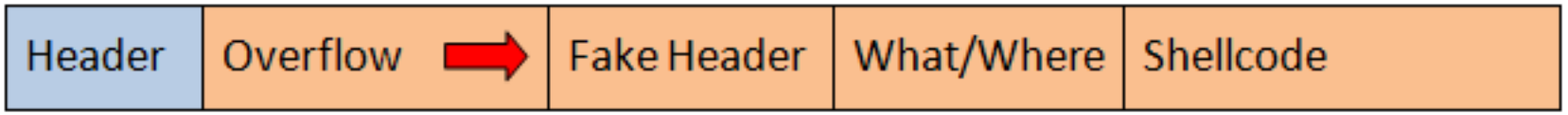




Heap overflow

Переполнение, которое происходит на куче. Сложно диагностируемая ошибка, так как реализация кучи может быть собственной у каждого ПО.

The pool before an overflow



The pool after an overflow

Type Confusion and Use-After-Free

- **Type Confusion** - Уязвимость, которая позволяет вывести приложение из строя или выполнить дополнительные действия. Чаще всего используется для повреждения памяти

- **UAF** - уязвимость при которой процесс может войти в неопределенное состояние. При определенных условиях может быть произведено выполнение команд

Колесников Александр

Спасибо
за внимание!