**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Операционные системы»

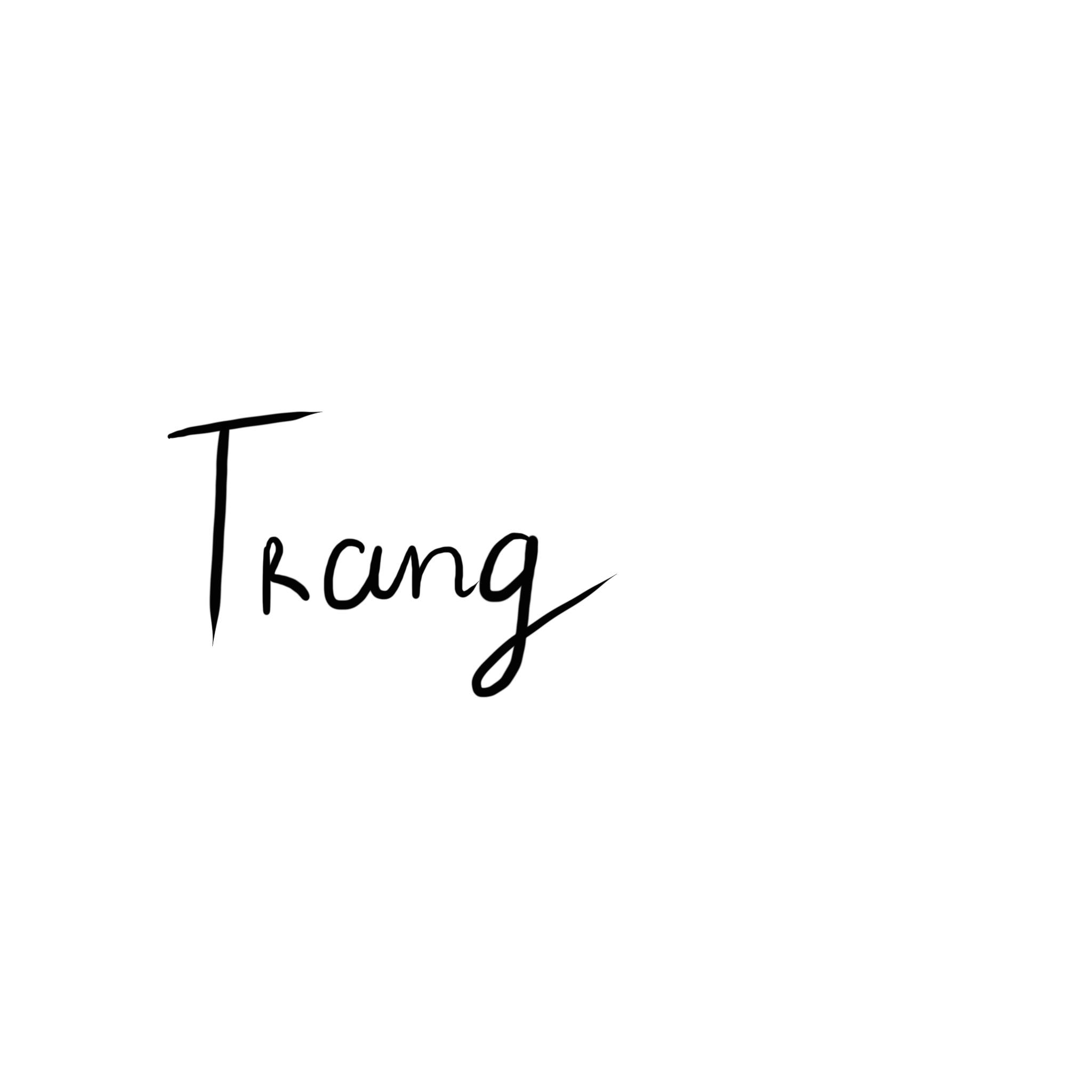
**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №7**

«Виртуальная машина»

# **Выполнил:**

Ву Тхи Тунг Транг

Группа:N3249





(подпись)

Нгуен Тхи Маи

Группа:N3245





(подпись)

# **Проверил:**

Савков Сергей Витальевич



(подпись)

**Задание**

1. Простой вариант:

1. Перечислите все известные вам способы обнаружения работы в виртуальной машине. (>=5)

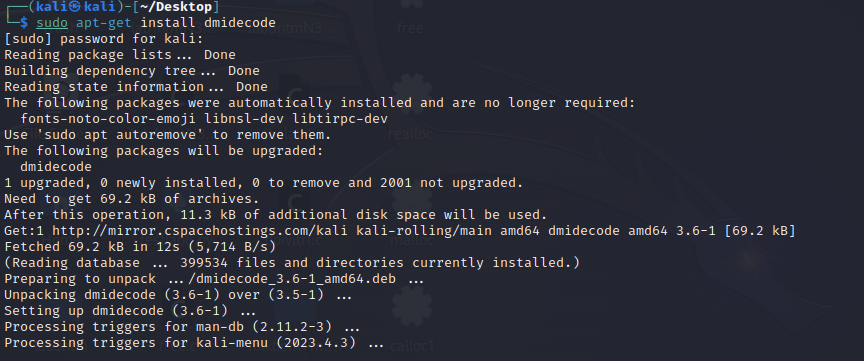
1. Сложный вариант (или)
2. Привести способ выхода из виртуальной машины
3. На ассемблере

**Ход работы**

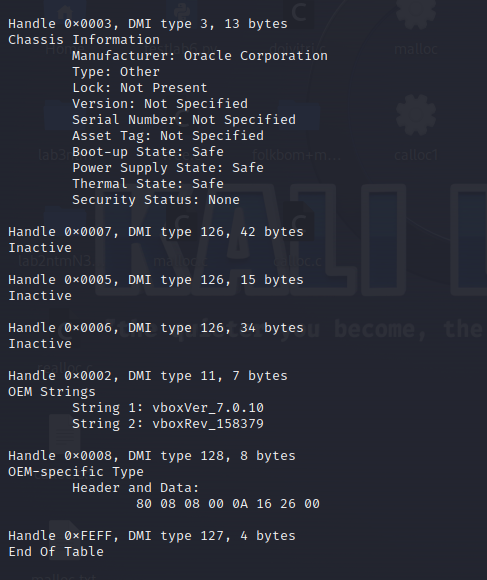
**I) Простой вариант: Перечислите все известные вам способы обнаружения работы в виртуальной машине**

**1. Dmidecode utility**

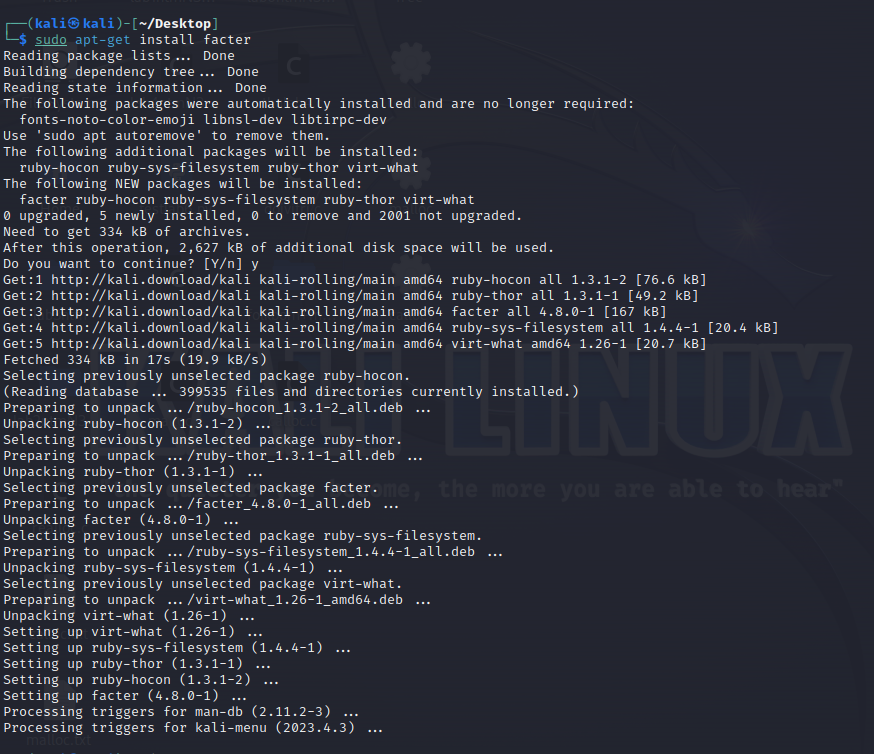
Dmidecode, декодер таблиц DMI, используется для поиска аппаратных компонентов вашей системы, а также для получения другой полезной информации, такой как серийные номера и версия BIOS.  
 Установил и выполнил:





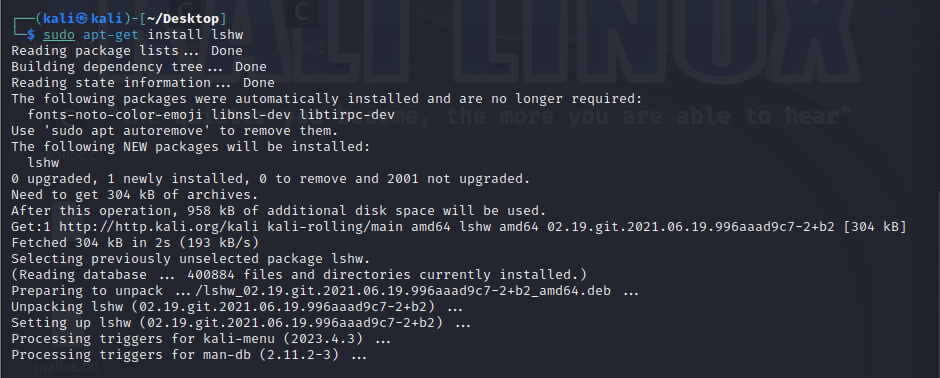


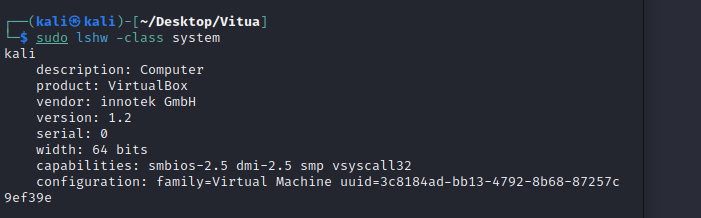
**2. Facter utility:**Facter — это утилита командной строки для сбора и отображения системной информации. В отличие от Dmidecode, Facter не предустанавливается по умолчанию. Вам может потребоваться установить его, как показано ниже, в зависимости от используемого вами дистрибутива Linux.

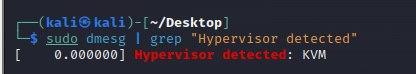
Установил Facter: 

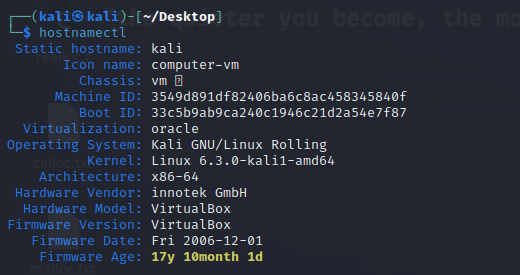
Проверил виртуальную машину: ****

**3. lshw utility**Утилита lshw — это небольшая утилита командной строки, которая отображает подробную информацию об оборудовании Unix-подобной системы. Он отображает все детали оборудования, включая конфигурацию памяти, версию прошивки, конфигурацию материнской платы, версию и скорость процессора, конфигурацию кэша, скорость шины и т. д.

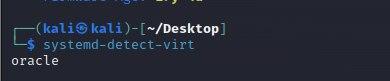
Установил и выполнил команду: Проверил виртуальную машину:

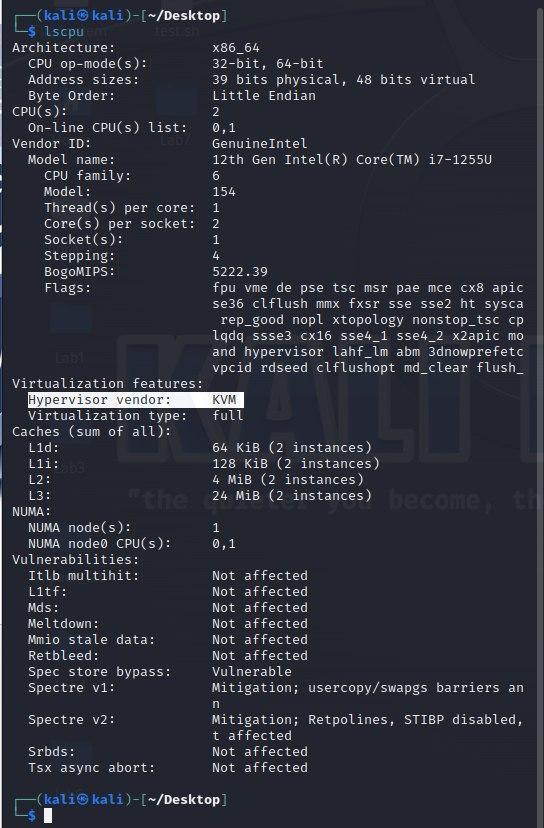


**4. dmesg utility** dmesg используется для проверки или управления кольцевым буфером ядра.

**5. hostnamectl command**Мы можем узнать, является ли наша система виртуальной или физической, используя команду hostnamectl. Для работы требуется systemd. 

**6. systemd-detect-virt**Инструмент systemd-detect-virt определяет технологию виртуализации и может отличить полную виртуализацию машины от аппаратной или контейнерной виртуализации.

****

**7. lscpu **

**II) Сложный вариант: На ассемблере**Существует множество способов обнаружения VMware. Эта короткая версия основана на том факте, что VMware перехватывает инструкции IN для порта 0x5658 с магическим значением 0x564D5868 в EAX.

**global \_start**

**section .data**

**VM: db 'Virtual Machine',0xA**

**VM\_l: equ $-VM**

**PM: db 'Physical Machine',0xA**

**PM\_l: equ $-PM**

**section .bss**

**section .text**

**\_start:**

**xor eax, eax ; eax = 0**

**mov eax, 1 ; eax = 1**

**cpuid ; вызов cpuid**

**bt ecx, 0x1f ; проверка ecx[31]**

**jc .VM ; если ecx[31] = 1, значит присутствия гипервизора**

**jnc .PM ; если ecx[31] = 0, то это физическая машина**

**.VM:**

**mov edx, VM\_l ; длина строк**

**mov ecx, VM ; адрес строк**

**call .print**

**.PM:**

**mov edx, PM\_l**

**mov ecx, PM**

**.print:**

**mov ebx, 1 ; файловый дескриптор 1 - с потоком стандартного вывода**

**mov eax, 4 ; Номер системного вызова (write())**

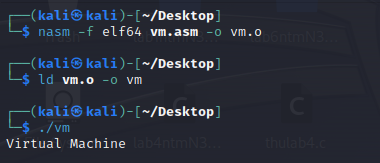
**int 0x80 ; вывод результата**

**mov ebx, 0 ;**

**mov eax, 1 ; Номер системного вызова (exit())**

**int 0x80 ; вызов exit()**

**Запускаем и получим результат:**

****

**III. Вывод**

* После работы получите навыки обнаружения виртуальных сред различными методами.
* Информация о работе виртуальной машины записывается в регистр ЦП. Эту информацию можно получить с помощью программ, написанных на языке ассемблера.