

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»**

**Выполнила:**

Студентка группы N32511

Синюта А.А. 

**Проверил:**

Ханов А.Р. \_\_\_\_\_

Санкт-Петербург

2023г.

## Задание:

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

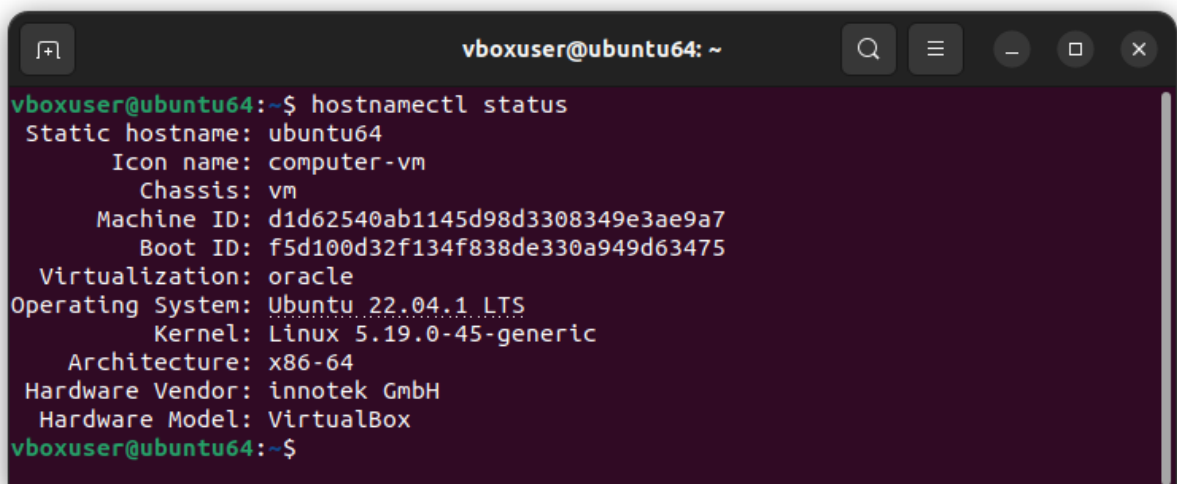
Сложный вариант (или)

1. Привести способ выхода из виртуальной машины
2. На ассемблере

## Ход работы

### Способы обнаружения работы в виртуальной машине

1. Команда `hostnamectl status` используется для получения информации о текущем статусе хостнейма (имени узла) в Linux-системах.



```
vboxuser@ubuntu64: ~  
vboxuser@ubuntu64:~$ hostnamectl status  
Static hostname: ubuntu64  
Icon name: computer-vm  
Chassis: vm  
Machine ID: d1d62540ab1145d98d3308349e3ae9a7  
Boot ID: f5d100d32f134f838de330a949d63475  
Virtualization: oracle  
Operating System: Ubuntu 22.04.1 LTS  
Kernel: Linux 5.19.0-45-generic  
Architecture: x86_64  
Hardware Vendor: innotek GmbH  
Hardware Model: VirtualBox  
vboxuser@ubuntu64:~$
```

Можно заметить, что Chassis (указывает на тип корпуса (физического или виртуального) устройства, на котором работает операционная система) имеет значение "vm", это указывает на то, что устройство является виртуальной машиной.

А также Virtualization (указывает на тип виртуализации, используемой для запуска виртуальной машины) имеет значение "oracle", что указывает на то, что используется гипервизор Oracle VirtualBox.

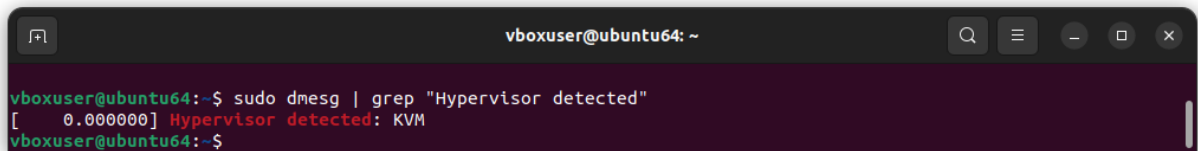
## 2. Использование утилиты dmidecode

```
vboxuser@ubuntu64: ~  
vboxuser@ubuntu64:~$ sudo dmidecode  
# dmidecode 3.3  
Getting SMBIOS data from sysfs.  
SMBIOS 2.5 present.  
10 structures occupying 455 bytes.  
Table at 0x000E1000.  
  
Handle 0x0000, DMI type 0, 20 bytes  
BIOS Information  
    Vendor: innotek GmbH  
    Version: VirtualBox  
    Release Date: 12/01/2006  
    Address: 0xE0000  
    Runtime Size: 128 kB  
    ROM Size: 128 kB  
    Characteristics:  
        ISA is supported  
        PCI is supported  
        Boot from CD is supported  
        Selectable boot is supported  
        8042 keyboard services are supported (int 9h)  
        CGA/mono video services are supported (int 10h)
```

```
vboxuser@ubuntu64: ~  
Handle 0x0001, DMI type 1, 27 bytes  
System Information  
    Manufacturer: innotek GmbH  
    Product Name: VirtualBox  
    Version: 1.2  
    Serial Number: 0  
    UUID: 250f07d6-95ed-8e4c-81e0-8605cfe6e7cd  
    Wake-up Type: Power Switch  
    SKU Number: Not Specified  
    Family: Virtual Machine  
  
Handle 0x0008, DMI type 2, 15 bytes  
Base Board Information  
    Manufacturer: Oracle Corporation  
    Product Name: VirtualBox  
    Version: 1.2  
    Serial Number: 0  
    Asset Tag: Not Specified  
    Features:  
        Board is a hosting board  
    Location In Chassis: Not Specified  
    Chassis Handle: 0x0003
```

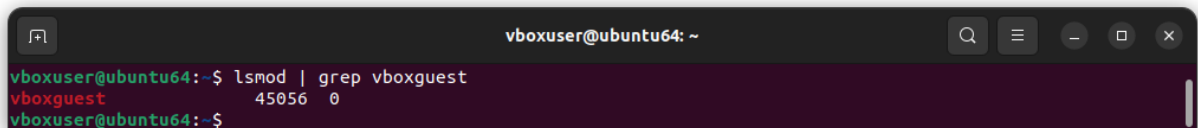
```
vboxuser@ubuntu64: ~  
Handle 0x0001, DMI type 1, 27 bytes  
System Information  
    Manufacturer: innotek GmbH  
    Product Name: VirtualBox  
    Version: 1.2  
    Serial Number: 0  
    UUID: 250f07d6-95ed-8e4c-81e0-8605cfe6e7cd  
    Wake-up Type: Power Switch  
    SKU Number: Not Specified  
    Family: Virtual Machine  
  
Handle 0x0008, DMI type 2, 15 bytes  
Base Board Information  
    Manufacturer: Oracle Corporation  
    Product Name: VirtualBox  
    Version: 1.2  
    Serial Number: 0  
    Asset Tag: Not Specified  
    Features:  
        Board is a hosting board  
    Location In Chassis: Not Specified  
    Chassis Handle: 0x0003
```

3. Команда `sudo dmesg | grep "Hypervisor detected"` будет искать в журналах ядра (dmesg) строку "Hypervisor detected" для проверки обнаружения гипервизора.



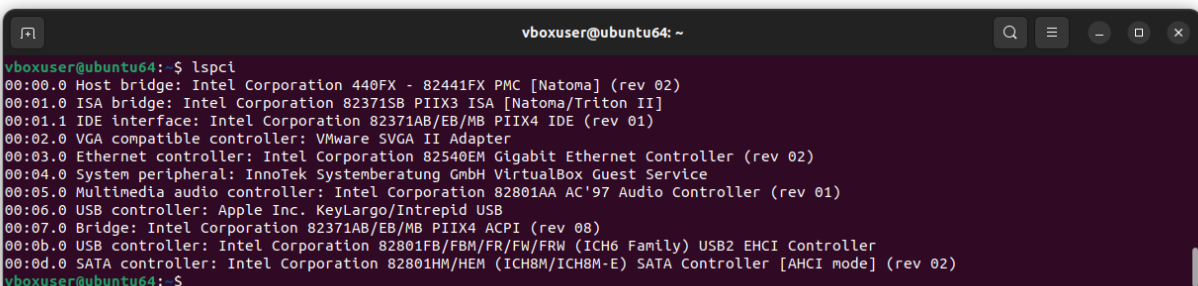
```
vboxuser@ubuntu64: ~  
vboxuser@ubuntu64:~$ sudo dmesg | grep "Hypervisor detected"  
[ 0.000000] Hypervisor detected: KVM  
vboxuser@ubuntu64:~$
```

4. Проверить наличие специальных утилит, таких как VirtualBox Guest Additions. Можно выполнить команду `lsmod | grep vboxguest`, чтобы проверить, загружен ли модуль VBoxGuest в ядро операционной системы. Если результат содержит строку `vboxguest`, это указывает на то, что VirtualBox Guest Additions установлены и загружены, что, в свою очередь, означает, что вы находитесь в виртуальной машине VirtualBox.



```
vboxuser@ubuntu64:~$ lsmod | grep vboxguest  
vboxguest 45056 0  
vboxuser@ubuntu64:~$
```

5. Посмотреть устройства Ubuntu подключенные по шине PCI можно с помощью команды `lspci`.



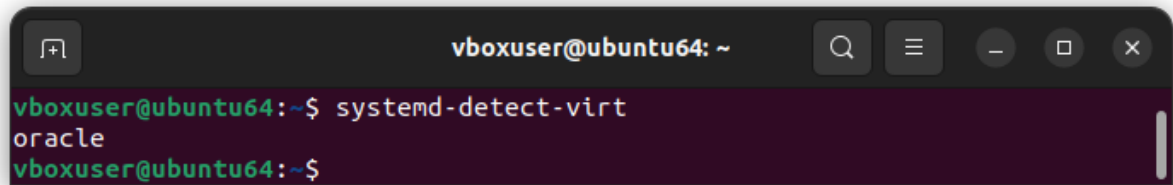
```
vboxuser@ubuntu64:~$ lspci  
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)  
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]  
00:01.1 IDE interface: Intel Corporation 82371AB/EB/MB PIIX4 IDE (rev 01)  
00:02.0 VGA compatible controller: VMware SVGA II Adapter  
00:03.0 Ethernet controller: Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02)  
00:04.0 System peripheral: InnoTek Systemberatung GmbH VirtualBox Guest Service  
00:05.0 Multimedia audio controller: Intel Corporation 82801AA AC'97 Audio Controller (rev 01)  
00:06.0 USB controller: Apple Inc. KeyLargo/Intrepid USB  
00:07.0 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 08)  
00:0b.0 USB controller: Intel Corporation 82801FB/FBM/FR/FW/FRW (ICH6 Family) USB2 EHCI Controller  
00:0d.0 SATA controller: Intel Corporation 82801HM/HEM (ICH8M/ICH8M-E) SATA controller [AHCI mode] (rev 02)  
vboxuser@ubuntu64:~$
```

Из вывода команды `lspci` видно, что виртуальная машина использует гипервизор VirtualBox. Некоторые из строк вывода указывают на наличие компонентов, характерных для VirtualBox:

- **VGA compatible controller: VMware SVGA II Adapter:** Эта строка указывает на использование графического адаптера VMware SVGA II, VirtualBox использует эмуляцию VMware SVGA II для отображения графики в виртуальной машине.
- **System peripheral: InnoTek Systemberatung GmbH VirtualBox Guest Service:** Эта строка указывает на наличие системного устройства VirtualBox Guest Service. Этот компонент является частью VirtualBox Guest Additions, которые обеспечивают дополнительные функции и интеграцию между хост-системой и виртуальной машиной.

Указанные строки указывают на то, что я работаю в виртуальной машине VirtualBox.

6. Команда `systemd-detect-virt` предоставляет информацию о технологии виртуализации, используемой на текущей системе, и может отличить полную виртуализацию машины от аппаратной или контейнерной виртуализации



```
vboxuser@ubuntu64: ~  
vboxuser@ubuntu64:~$ systemd-detect-virt  
oracle  
vboxuser@ubuntu64:~$
```

Если вывод пустой или отсутствует, это может означать, что система не работает в виртуальной машине или не удалось обнаружить используемую технологию виртуализации.

В моем случае — `oracle`.

## Детектирование виртуальной машины на ассемблере

Для детектирования виртуальной машины на ассемблере, обычно используются некоторые характеристики или инструкции, которые могут указывать на присутствие виртуализации. Например, можно проверить значение регистра `EFLAGS` для наличия некоторых битов, связанных с виртуализацией.

*detect\_vm.asm:*

```
section .data  
    not_vm_msg db "Not a virtual machine", 0x0A  
    in_vm_msg db "Virtual Machine", 0x0A  
  
section .text  
    global _start  
  
_start:  
    ; Проверяем значение регистра EFLAGS для определения виртуальной  
    машины  
    mov eax, 1  
    cpuid  
    test ecx, 0x80000000 ; Проверяем бит "Virtual Machine Extensions"  
    jz not_in_vm ; Если бит не установлен, переходим к not_in_vm  
  
    ; Бит установлен, значит, это виртуальная машина  
    mov eax, 4 ; Системный вызов для вывода в терминал  
    mov ebx, 1 ; Файловый дескриптор стандартного вывода (stdout)  
    mov ecx, in_vm_msg ; Указатель на сообщение  
    mov edx, 18 ; Длина сообщения  
    int 0x80 ; Вызов системного вызова  
    jmp exit  
  
not_in_vm:  
    ; Бит не установлен, значит, это не виртуальная машина  
    mov eax, 4  
    mov ebx, 1  
    mov ecx, not_vm_msg
```

```
mov edx, 19  
int 0x80
```

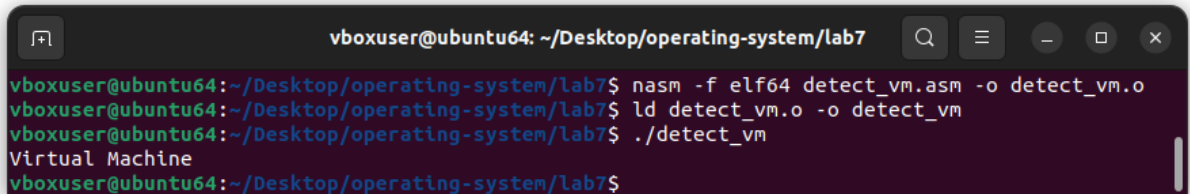
```
exit:
```

```
; Выход из программы
```

```
mov eax, 1 ; Системный вызов для выхода из программы
```

```
xor ebx, ebx
```

```
int 0x80
```



```
vboxuser@ubuntu64: ~/Desktop/operating-system/lab7  
vboxuser@ubuntu64:~/Desktop/operating-system/lab7$ nasm -f elf64 detect_vm.asm -o detect_vm.o  
vboxuser@ubuntu64:~/Desktop/operating-system/lab7$ ld detect_vm.o -o detect_vm  
vboxuser@ubuntu64:~/Desktop/operating-system/lab7$ ./detect_vm  
Virtual Machine  
vboxuser@ubuntu64:~/Desktop/operating-system/lab7$
```

Код проверяет бит "Virtual Machine Extensions" в регистре ECX после выполнения инструкции CPUID. Если бит установлен, то программа выводит сообщение "Virtual Machine". Если бит не установлен, то программа выводит сообщение "Not a virtual machine".