**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Операционные системы»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №7**

«Способы обнаружения работы в виртуальной машине»

Содержание

[Введение 3](#_Toc183545424)

[1 Способы обнаружения 4](#_Toc183545425)

[1.1 Задание 4](#_Toc183545426)

[1.2 Ход работы 4](#_Toc183545427)

[1.2.1 Общее 4](#_Toc183545428)

[1.2.2 dmidecode 4](#_Toc183545429)

[1.2.3 virt-what 6](#_Toc183545430)

[1.2.4 cat /sys/class/dmi/id/product\_name 6](#_Toc183545431)

[1.2.5 hostnamectl 6](#_Toc183545432)

[1.2.6 systemd-detect-virt 7](#_Toc183545433)

[1.2.7 imvirt 7](#_Toc183545434)

[2 Обнаружение работы вм с помощью ассемблера 8](#_Toc183545435)

[2.1 Задание 8](#_Toc183545436)

[2.2 Ход работы 8](#_Toc183545437)

[Заключение 10](#_Toc183545438)

[Список использованных источников 11](#_Toc183545439)

Введение

Цель работы – перечислите все известные вам способы обнаружения работы в виртуальной машине (>=5). Привести код на ассемблере.

Для достижения поставленной цели необходимо решить следующие задачи:

* познакомить со способами обнаружения работы в виртуальной машине;
* протестировать не менее 5 способов;
* привести код на ассемблере.

# Способы обнаружения

## Задание

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

## Ход работы

### Общее

Виртуальная машина (ВМ, VM) – это виртуальная среда, работающая как настоящий компьютер, но внутри другого компьютера. Если выражаться проще, то это приложение, которое имитирует компьютер с полноценной операционной системой и аппаратным обеспечением.

Способы обнаружения работы в виртуальной машине нужны для решения следующих задач: мониторинг производительности и ресурсов; выявление инцидентов информационной безопасности; дискаверинг (процесс автоматизированного сбора инвентаризационных и топологических данных об ИТ-инфраструктуре).

Существует много различных способов обнаружения работы в виртуальной машине. Одни из самых часто используемых это: system-detect-virt, dmidecode, virtwhat, cat /sys/class/dmi/id/product\_name, hostnamecl, imvirt.

### Dmidecode

dmidecode — это утилита для получения информации о системе из DMI (Desktop Management Interface) таблиц. Она может предоставить информацию о аппаратном обеспечении, включая производителя, модель материнской платы, серийные номера и другие характеристики. При использовании этой команды можно определить, находится ли система на физическом сервере или в виртуальной машине, основываясь на значениях полей, таких как "Product Name" или "System Information".

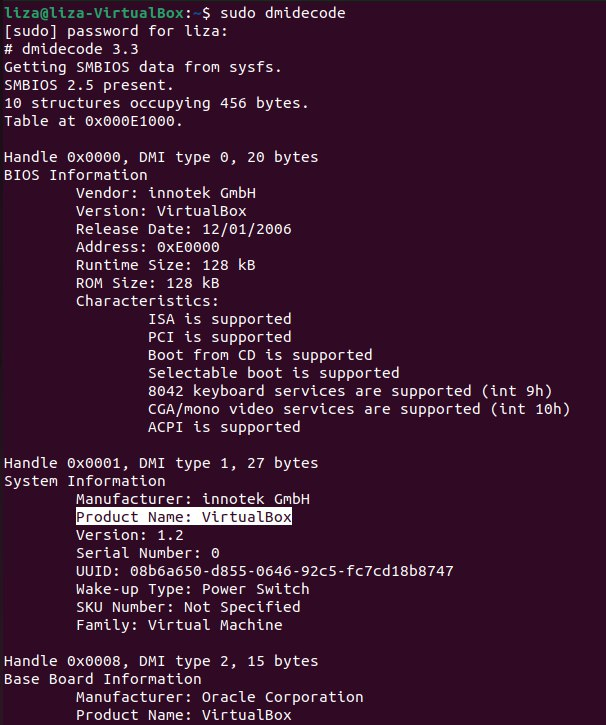


Рисунок 1 – терминал после запуска dmidecode



Рисунок 2 – терминал после запуска dmidecode



Рисунок 3 – терминал после запуска dmidecode

### virt-what

virtwhat — это скрипт для определения виртуальной среды. Он выполняет несколько проверок на наличие специфических для виртуальных машин признаков, таких как наличие гипервизоров или специфических устройств. Результат выполнения команды указывает на тип виртуализации, если таковая имеется.



Рисунок 4 - терминал после запуска virtwhat

### cat /sys/class/dmi/id/product\_name

Эта команда выводит имя продукта системы, полученное из DMI таблиц. Это может быть полезно для определения типа и модели оборудования или гипервизора. В случае виртуальной машины это может вернуть название виртуального оборудования (например, "KVM", "VMware Virtual Platform" и т.д.).



Рисунок 5 - терминал после запуска cat /sys/class/dmi/id/product\_name

### hostnamectl

Команда hostnamectl используется для управления настройками имени хоста системы и может также предоставить информацию о системе, включая ее архитектуру и тип. В некоторых случаях она может помочь определить, работает ли система в виртуальной среде.

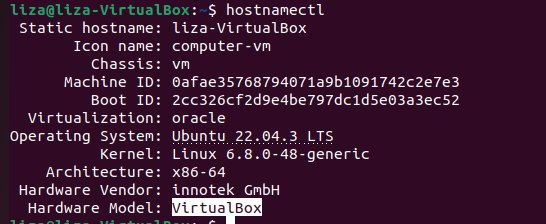


Рисунок 6 - терминал после запуска hostnamectl

### systemd-detect-virt

Утилита systemd-detect-virt является частью пакета virt-what и используется для определения, запущена ли система в виртуальной среде. Она проверяет различные параметры и метаданные, чтобы выявить, работает ли система на гипервизоре (например, KVM, VMware, Xen и т.д.).



Рисунок 7 - терминал после запуска systemd-detect-virt

### imvirt

imvirt — это утилита, которая помогает определить, работает ли система в виртуальной среде. Она проверяет наличие специфических для виртуализации устройств и метаданных и возвращает результаты о том, обнаружена ли виртуализация.



Рисунок 8 - терминал после запуска imvirt

# обнаружение работы вм с помощью ассемблера

## Задание

Привести код для обнаружения работы виртуальной машины на ассемблере.

## Ход работы

Обнаружить работу виртуальной машины можно и с помощью кода на ассемблере.

global \_start

section .data

    virt: db "Virtual box",10

    length1: equ $-virt

    phys: db "Physical machine",10

    length2: equ $-phys

section .text

\_start:

    xor eax, eax

mov eax, 0x40000000

cpuid

cmp ebx, 0x4b4d564b  ; соответствует строке "KVMK"

jne physical

;virtual

mov eax, 4

mov ebx, 1

mov ecx, virt

mov edx, length1

int 0x80

jmp exit

physical:

mov eax, 4

mov ebx, 1

mov ecx, phys

mov edx, length2

int 0x80

exit:

mov ebx, 0

mov eax, 1

int 0x80

Листинг 1 – код на ассемблере.

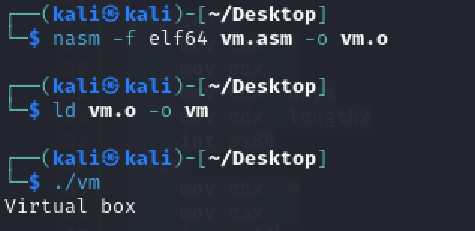


Рисунок 9 – терминал после запуска программы на ассемблере

Заключение

В ходе данной лабораторной работы мы познакомились со способами обнаружения работы в виртуальной машине, а именно system-detect-virt, dmidecode, virtwhat, cat /sys/class/dmi/id/product\_name, hostnamecl, imvirt. Каждый из способов был проверен на наших виртуальных машинах. Кроме того, был написан код на языке ассемблер для обнаружения работы в виртуальной машине. Это позволило закрепить полученные знания и навыки. В ходе выполнения лабораторной работы были выполнены все задачи и достигнуты поставленные цели.

Список использованных источников

1. Эндрю Таненбаум Современные операционные системы. — 4-е изд. — СПб. : Питер, 2015. — 1120 с.