

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

Факультет безопасности информационных технологий

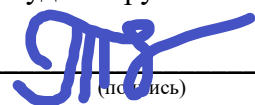
Дисциплина:
«Операционные системы»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №7

«Обнаружение работы в виртуальной машине»

Выполнил:

Рядовой Т.С., студент группы N3252



(подпись)

Проверил:

Чебунин Константин Олегович

(отметка о выполнении)

(подпись)

Санкт-Петербург
2023 г.

СОДЕРЖАНИЕ

Введение.....	4
1 Обычный вариант лабораторной	5
1.1 Задание.....	5
1.1.1 Первый способ – dmidecode.....	5
1.1.2 Второй способ – facter.....	6
1.1.3 Третий способ – hostnamectl	7
1.1.4 Четвертый способ – lshw.....	8
1.1.5 Пятый способ – neofetch	9
1.1.6 Шестой способ - systemd-detect-virt.....	10
1.1.7 Седьмой способ – virt-what	10
2 Усиленный вариант лабораторной	11
2.1 Задание.....	11
2.2 Задание на ассемблере.....	12
Заключение.....	14
Список использованных источников	15

ВВЕДЕНИЕ

Цель работы – познакомиться с работой в виртуальной машине.

В обычном варианте:

- Перечислить способы обнаружения работы в виртуальной машине.

В усложненном варианте:

- Написать способ выхода из виртуальной машины;
- На ассемблере.

1 ОБЫЧНЫЙ ВАРИАНТ ЛАБОРАТОРНОЙ

1.1 Задание

Перечислить способы обнаружения работы в виртуальной машине.

1.1.1 Первый способ – dmidecode

```
fedora > tryadovoi ~/Desktop/itmo/3сем/операционные_системы/lab7/data
sudo dmidecode
[sudo] password for tryadovoi:
# dmidecode 3.5
Getting SMBIOS data from sysfs.
SMBIOS 3.11.1 present.
# SMBIOS implementations newer than version 3.5.0 are not
# fully supported by this version of dmidecode.
Table at 0xAE2DD000.

Handle 0x0000, DMI type 0, 26 bytes
BIOS Information
    Vendor: HUAWEI
    Version: 1.18
    Release Date: 03/30/2022
    Address: 0xE0000
    Runtime Size: 128 kB
    ROM Size: 8 MB
    Characteristics:
        PCI is supported
        PNP is supported
        BIOS is upgradeable
        BIOS shadowing is allowed
        Boot from CD is supported
        Selectable boot is supported
        EDD is supported
        ACPI is supported
        USB legacy is supported
        Smart battery is supported
        BIOS boot specification is supported
        Targeted content distribution is supported
        UEFI is supported
    BIOS Revision: 1.18
    Firmware Revision: 1.18
```

Рисунок 1 – Dmidecode на настольном ПК

```

root@projectoneubuntu:~/folder# dmidecode
# dmidecode 3.2
Getting SMBIOS data from sysfs.
SMBIOS 2.8 present.
10 structures occupying 453 bytes.
Table at 0x000F5A90.

Handle 0x0000, DMI type 0, 24 bytes
BIOS Information
    Vendor: DigitalOcean
    Version: 20171212
    Release Date: 12/12/2017
    Address: 0xE8000
    Runtime Size: 96 kB
    ROM Size: 64 kB
    Characteristics:
        BIOS characteristics not supported
        Targeted content distribution is supported
        System is a virtual machine
    BIOS Revision: 0.0

Handle 0x0100, DMI type 1, 27 bytes
System Information
    Manufacturer: DigitalOcean
    Product Name: Droplet
    Version: 20171212
    Serial Number: 368298340
    UUID: 9a4271f2-c09a-40d4-b22f-5bb7b2cb85c4
    Wake-up Type: Power Switch
    SKU Number: Not Specified
    Family: DigitalOcean_Droplet

```

Рисунок 2 – Dmidecode на виртуальной машине

Так как мы работаем с сервером, в графе Manufacturer и Product Name, Family можно отследить эти признаки.

1.1.2 Второй способ – facter

```

fedora > tryadovoi ~/Desktop/itmo/3сем/операционные_системы/lab7/data
facter 2> /dev/null | grep virtual
is_virtual => false
virtual => physical

```

Рисунок 3 – Facter на настольном ПК

```

root@projectoneubuntu:~/folder# facter 2> /dev/null | grep virtual
is_virtual => true
virtual => kvm

```

Рисунок 4 – Facter на виртуальной машине

1.1.3 Третий способ – hostnamectl

```
fedora > tryadovoi ~/Desktop/itmo/3сем/операционные_системы/lab7/data
hostnamectl status
  Static hostname: (unset)
  Transient hostname: fedora
    Icon name: computer-laptop
    Chassis: laptop
    Machine ID: 79b79a73feba453087c4379392412468
    Boot ID: a3eadc345bba4c3cb2344ff3a58d59a8
  Operating System: Fedora Linux 39 (KDE Plasma)
    CPE OS Name: cpe:/o:fedoraproject:fedora:39
    OS Support End: Tue 2024-05-14
  OS Support Remaining: 5month 1w
    Kernel: Linux 6.5.12-300.fc39.x86_64
    Architecture: x86-64
  Hardware Vendor: HUAWEI
  Hardware Model: NBLK-WAX9X
  Firmware Version: 1.18
  Firmware Date: Wed 2022-03-30
  Firmware Age: 1y 8month 1w
```

Рисунок 5 – hostnamectl на настольном ПК

```
root@projectoneubuntu:~/folder# hostnamectl status
  Static hostname: projectoneubuntu
    Icon name: computer-vm
    Chassis: vm
    Machine ID: 6d5ef7584ab371bf2d25087d64cbc85b
    Boot ID: 8b5baf95143f4f9e9c2a04daafc132ef
  Virtualization: kvm
  Operating System: Ubuntu 20.04.6 LTS
    Kernel: Linux 5.4.0-155-generic
    Architecture: x86-64
root@projectoneubuntu:~/folder#
```

Рисунок 6 – hostnamectl на виртуальной машине

На физической и виртуальной машине разный вывод. В последнем есть графа Virtualization.

1.1.4 Четвертый способ – lshw

```
fedora > tryadovoi ~/Desktop/itmo/3сем/операционные_системы/lab7/data 96% (0:14) 01:41:51
sudo lshw -class system

[sudo] password for tryadovoi:
fedora
  description: Notebook
  product: NBLK-WAX9X (C170)
  vendor: HUAWEI
  version: M1020
  serial: M6TPM20527002069
  width: 64 bits
  capabilities: smbios-3.11.1 dmi-3.11.1 smp vsyscall32
  configuration: chassis=notebook family=MateBook D sku=C170 uuid=28f27a0d-dc86-42c5-bc01-892f5ade680d
*-pnnp00:00
  product: PnP device PNP0c02
  physical id: 0
  capabilities: pnp
  configuration: driver=system
*-pnnp00:01
  product: PnP device PNP0b00
  physical id: 1
  capabilities: pnp
  configuration: driver=rtc_cmos
*-pnnp00:03
  product: PnP device PNP0c02
  physical id: 3
  capabilities: pnp
  configuration: driver=system
*-pnnp00:04
  product: PnP device PNP0c01
  physical id: 4
  capabilities: pnp
  configuration: driver=system
```

Рисунок 7 – lshw на настольном ПК

```
root@projectoneubuntu:~/folder# lshw -class system
projectoneubuntu
  description: Computer
  product: Droplet
  vendor: DigitalOcean
  version: 20171212
  serial: 368298340
  width: 64 bits
  capabilities: smbios-2.8 dmi-2.8 vsyscall32
  configuration: boot=normal family=DigitalOcean_Droplet uuid=F271429A-9AC0-D440-B22F-5BB7B2CB85C4
*-pnnp00:03
  product: PnP device PNP0b00
  physical id: 4
  capabilities: pnp
  configuration: driver=rtc_cmos
root@projectoneubuntu:~/folder#
```

Рисунок 8 – lshw на виртуальной машине

Данные есть в графах product, vendor.

1.1.5 Пятый способ – neofetch

```
fedora > tryadovoi ~/Desktop/itmo/3сем/операционные_системы/lab7/data
neofetch

      .',;:::;,'.
      .':cccccccccc;,.
      .;cccccccccccccccccccc;.
      .:cccccccccccccccccccc;.
      .;cccccccccccc;.ddd1:.;cccccc;.
      .:cccccccccccc;OwMKOOXMd;cccccc;.
      .:cccccccccccc;KMMc;cc;xMMc;cccccc;.
      .;cccccccccccc;MMM.;cc;WW::cccccc;.
      .:cccccccccccc;MMM.;cccccccccccc;.
      .:cccccc;ox000o;MMM000k;cccccccc;.
      .:cccccc;0MMKxdd;MMMkddc.;cccccccc;.
      .:cccc;XM0';cccc;MMM.;cccccccccccc'
      .:cccc;MMo;cccc;MMW.;cccccccccccc;.
      .:cccc;0Mnc.ccc.xMMd;cccccccccccc;.
      .:cccccc;dNMWXXWM0:;cccccccccccc;.
      .:cccccc;.odl:.;cccccccccccc;.
      .:cccccccccccccccccccccccc;'.
      .:cccccccccccccccccccccc;,.
      .':cccccccccccccc;,.

      tryadovoi@fedora
      -----
      OS: Fedora Linux 39 (KDE Plasma) x86_64
      Host: NBLK-WAX9X M1020
      Kernel: 6.5.12-300.fc39.x86_64
      Uptime: 1 hour, 4 mins
      Packages: 2293 (rpm), 17 (flatpak)
      Shell: zsh 5.9
      Resolution: 1920x1080
      DE: Plasma 5.27.9
      WM: kwin
      Theme: [Plasma], Breeze [GTK2/3]
      Icons: [Plasma], breeze-dark [GTK2/3]
      Terminal: konsole
      CPU: AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx (8) @ 2.100GHz
      GPU: AMD ATI Radeon Vega Series / Radeon Vega Mobile Series
      Memory: 4495MiB / 6851MiB
```

Рисунок 9 – neofetch на настольном ПК

```
root@projectoneubuntu:~/folder# neofetch

      .-/+oosssso+/-.
      `:+ssssssssssssssss+:`
      -+ssssssssssssssssyyssss+-
      .ossssssssssssssssdMMMNysssos.
      /ssssssssssshdmmNNmmyNMMMMhssssss/
      +ssssssssshmydMMMMMMMMddddyssssssss+
      /ssssssssshNMMMyhhyyyyhmNMMMMhssssssss/
      .ssssssssdMMMNhssssssssshNMMMdssssssss.
      +sssshhhyNMMNysssssssssssyNMMMyssssssss+
      ossyNMMMNyMMhssssssssssssshmmhssssssso
      ossyNMMMNyMMhssssssssssssshmmhssssssso
      +sssshhhyNMMNysssssssssssyNMMMyssssssss+
      .ssssssssdMMMNhssssssssshNMMMdssssssss.
      /ssssssssshNMMMyhhyyyyhdNMMMMhssssssss/
      +sssssssssdmydMMMMMMMMddddyssssssss+
      /ssssssssssshdmmNNNmyNMMMMhssssss/
      .ossssssssssssssssdMMMNysssos.
      -+ssssssssssssssssyyssss+-
      `:+ssssssssssssssss+:`
      .-/+oosssso+/-.

      root@projectoneubuntu
      -----
      OS: Ubuntu 20.04.6 LTS x86_64
      Host: Droplet 20171212
      Kernel: 5.4.0-155-generic
      Uptime: 123 days, 10 hours, 29 mins
      Packages: 707 (dpkg), 4 (snap)
      Shell: bash 5.0.17
      Resolution: 1024x768
      Terminal: /dev/pts/0
      CPU: D0-Regular (1) @ 1.995GHz
      GPU: 00:02.0 Red Hat, Inc. Virtio GPU
      Memory: 179MiB / 964MiB
```

Рисунок 10 – neofetch на виртуальной машине

Помимо данных в GPU, CPU и Host, можно заметить, что разрешение экрана другое.

1.1.6 Шестой способ - systemd-detect-virt

```
fedora > tryadovoi ~/Desktop/itmo/3сем/операционные_системы/lab7/data
systemd-detect-virt
none
fedora > tryadovoi ~/Desktop/itmo/3сем/операционные_системы/lab7/data
```

Рисунок 11 – systemd-detect-virt на настольном ПК

```
root@projectoneubuntu:~/folder# systemd-detect-virt
kvm
root@projectoneubuntu:~/folder#
```

Рисунок 12 – systemd-detect-virt на виртуальной машине

1.1.7 Седьмой способ – virt-what

```
fedora > tryadovoi ~/Desktop/itmo/3сем/операционные_системы/lab7/data 1 97% (0:11) 01:44:38
sudo virt-what
fedora > tryadovoi ~/Desktop/itmo/3сем/операционные_системы/lab7/data ✓ < 97% (0:12) 01:44:48
```

Рисунок 13 – virt-what на настольном ПК

```
root@projectoneubuntu:~/folder# virt-what
kvm
root@projectoneubuntu:~/folder#
```

Рисунок 14 – virt-what на виртуальной машине

В утилите virt-what, если мы работаем на физической машине, вывод будет пустым.

2 УСИЛЕННЫЙ ВАРИАНТ ЛАБОРАТОРНОЙ

2.1 Задание

Написать способ выхода из виртуальной машины

```
fedora > tryadovoi ~  
sudo docker run -it --privileged ubuntu bash  
Unable to find image 'ubuntu:latest' locally  
latest: Pulling from library/ubuntu  
5e8117c0bd28: Pull complete  
Digest: sha256:8eab65df33a6de2844c9aefd19efe8ddb87b7df5e9185a4ab73af936225685bb  
Status: Downloaded newer image for ubuntu:latest  
root@89cc7d1cd77d:/# mkdir /escape
```

Рисунок 15 – Запуск контейнера с ubuntu

```
root@89cc7d1cd77d:/# mount /dev/nvme0n1p8 /escape  
root@89cc7d1cd77d:/# cd /escape/home/linux/Desktop/  
bash: cd: /escape/home/linux/Desktop/: No such file or directory  
root@89cc7d1cd77d:/# cd /escape/home/tryadovoi/Desktop/  
root@89cc7d1cd77d:/escape/home/tryadovoi/Desktop# touch escaped  
root@89cc7d1cd77d:/escape/home/tryadovoi/Desktop#
```

Рисунок 16 – Создание пустого файла на рабочем столе

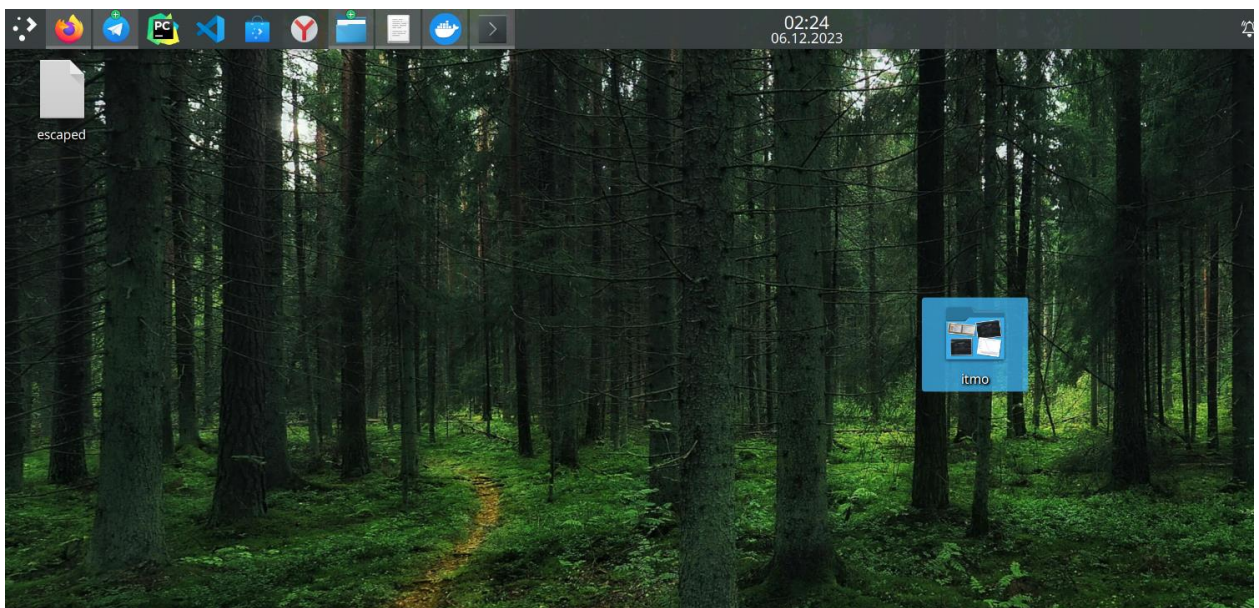


Рисунок 17 – Результат

2.2 Задание на ассемблере

Здесь необходимо использовать инструкцию `cpuid`. Данный код измеряет время выполнения инструкции `cpuid` с использованием Time Stamp Counter (TSC). Если это время превышает 4000 тактов процессора, то программа считается выполняющейся в виртуальной машине, и выводится строка "vm". В противном случае выводится строка "not vm".

Листинг 1 – Код на ассемблере

```
bits 64
section .data
    vm: db "vm", 10
    not_vm: db "not vm", 10

section .text
    global _start

_start:
    rdtscp
    mov r10, rax

    cpuid

    rdtscp
    sub r10, rax
    neg r10

    mov rax, 1

    cmp r10, 4000
    jge is_vm      ; Если больше или равно 4000, переходим к is_vm

    mov rdi, 1
    mov rsi, not_vm
    mov rdx, 7
    jmp _exit      ; Переходим к выходу из программы (_exit)

is_vm:
    mov rdi, 1
    mov rsi, vm
    mov rdx, 4

_exit:
    syscall
    mov eax, 60
    mov rdi, 0
    syscall
```

```
fedora > tryadovoi ~/Desktop/itmo/3сем/операционные_системы/lab7/data ✓ < 93% (0:19) 01:33:49
nasm -f elf64 -o check_vm.o check_vm.asm

fedora > tryadovoi ~/Desktop/itmo/3сем/операционные_системы/lab7/data ✓ < 94% (0:16) 01:34:00
ld -m elf_x86_64 -o check_vm check_vm.o

fedora > tryadovoi ~/Desktop/itmo/3сем/операционные_системы/lab7/data ✓ < 94% (0:16) 01:34:02
./check_vm

not vm
fedora > tryadovoi ~/Desktop/itmo/3сем/операционные_системы/lab7/data ✓ < 94% (0:16) 01:34:05
```

Рисунок 18 – Проверка на физической машине

```
data:zsh × (root) 209.97.137.211 ×
root@projectoneubuntu:~/folder# vim check_vm.asm
root@projectoneubuntu:~/folder# nasm -f elf64 -o check_vm.o check_vm.asm
root@projectoneubuntu:~/folder# ld -m elf_x86_64 -o check_vm check_vm.o
root@projectoneubuntu:~/folder# ./check_vm
vm
nroot@projectoneubuntu:~/folder#
```

Рисунок 19 – Проверка на сервере

ЗАКЛЮЧЕНИЕ

В ходе выполнения лабораторной работы мне удалось достигнуть поставленных целей:

Обычного варианта:

- Перечислить способы обнаружения работы в виртуальной машине;

Усложненного варианта:

- Написать способ выхода из виртуальной машины;
- На ассемблере.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. <https://itsecforu.ru/2020/08/07>
2. <https://xakep.ru/2013/11/08/61563/>
3. <https://forum.ixbt.com/topic.cgi?id=26:42386>