

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО  
ОБРАЗОВАНИЯ  
«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
УНИВЕРСИТЕТ ИТМО»**

**Факультет безопасности информационных технологий**

**Дисциплина:  
«Операционные системы»**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 7**  
Способы обнаружения работы в виртуальной машине

**Выполнила:**  
Студентка гр. №N3253  
Пастухова А.А.



**Проверил:**  
Ханов А.Р.

Санкт-Петербург  
2022 г.

## Задачи:

Перечислите все известные вам способы обнаружения работы в виртуальной машине ( $\geq 5$ )

Сложный:

На ассемблере

## Ход работы:

1. Утилита **dmidecode**, позволяющая собирать данные о характеристиках компьютера.

С ключом `baseboard` информация о том, что я работаю в ВМ, в строке `Description (VMware SVGA II)`

```
anastasya@ubuntu:~$ sudo dmidecode -t baseboard
# dmidecode 3.3
Getting SMBIOS data from sysfs.
SMBIOS 2.7 present.

Handle 0x0002, DMI type 2, 15 bytes
Base Board Information
    Manufacturer: Intel Corporation
    Product Name: 440BX Desktop Reference Platform
    Version: None
    Serial Number: None
    Asset Tag: Not Specified
    Features: None
    Location In Chassis: Not Specified
    Chassis Handle: 0x0000
    Type: Unknown
    Contained Object Handles: 0

Handle 0x019F, DMI type 10, 8 bytes
On Board Device 1 Information
    Type: Video
    Status: Disabled
    Description: VMware SVGA II
On Board Device 2 Information
    Type: Sound
    Status: Disabled
    Description: ES1371
```

С ключом `system` информация о том, что я работаю в ВМ, в строке `Product Name (VMware Virtual Platform)`

```

anastasya@ubuntu:~$ sudo dmidecode -t system
# dmidecode 3.3
Getting SMBIOS data from sysfs.
SMBIOS 2.7 present.

Handle 0x0001, DMI type 1, 27 bytes
System Information
    Manufacturer: VMware, Inc.
    Product Name: VMware Virtual Platform
    Version: None
    Serial Number: VMware-56 4d d2 a8 d4 c7 8a 74-0b 78 5d 86 92 f6 13 b3
    UUID: a8d24d56-c7d4-748a-0b78-5d8692f613b3
    Wake-up Type: Power Switch
    SKU Number: Not Specified
    Family: Not Specified

Handle 0x01A1, DMI type 15, 29 bytes
System Event Log
    Area Length: 16 bytes
    Header Start Offset: 0x0000
    Header Length: 16 bytes
    Data Start Offset: 0x0010
    Access Method: General-purpose non-volatile data functions
    Access Address: 0x0000
    Status: Invalid, Full
    Change Token: 0x00000036
    Header Format: Type 1

```

2. Похожий способ, выводит напрямую значение **human-readable dmi**.

```

anastasya@ubuntu:~$ cat /sys/class/dmi/id/product_name
VMware Virtual Platform
anastasya@ubuntu:~$ cat /sys/class/dmi/id/sys_vendor
VMware, Inc.
anastasya@ubuntu:~$

```

3. Утилита **hostnamectl** используется для идентификации машины на базе Linux.

```

anastasya@ubuntu:~$ sudo hostnamectl
Static hostname: ubuntu
    Icon name: computer-vm
    Chassis: vm
    Machine ID: d5db0b76043640829aef6cc628c3415a
    Boot ID: 779d8055b1f54ad5a75b19e6fdcab031
    Virtualization: vmware
Operating System: Ubuntu 21.10
    Kernel: Linux 5.13.0-19-generic
    Architecture: x86-64
Hardware Vendor: VMware, Inc.
Hardware Model: VMware Virtual Platform

```

4. Проверка через сравнение **MAC-адреса**. Поскольку первые три байта MAC-адреса сетевой карты определяют её производителя и по

умолчанию фиксированы, можно легко прочитать это значение с помощью API-функции и сопоставить со списком адресов, соответствующих различным производителям виртуальных машин. Однако такой медот нельзя считать надежным, так как MAC-адрес легко изменить. В моем случае второй адрес 00:0c:29:f6:13:b3 оказался в списке производителя VMware.

```
anastasya@ubuntu:~$ sudo cat /sys/class/net/*/address
02:42:34:6a:27:a4
00:0c:29:f6:13:b3
00:00:00:00:00:00
```


udger

Products Prices Download Resources Support Contact

Resources > MAC address vendors > Detail

Vendors list | TOP Vendors by range count | MAC address lookup

VMware, Inc.

Vendor	VMware, Inc.
Vendor code	vmware_inc
Addresses	3401 Hillview Avenue Palo Alto CA 94304
Country	 United states
Country code	US
Assigned MAC range	format 1 00:05:69:xx:xx:xx 00:0c:29:xx:xx:xx 00:1c:14:xx:xx:xx 00:50:56:xx:xx:xx

Ubuntu 64-bit - VMware Workstation 16 Player (Evaluation license)

Player

Activities Terminal Jun 16 11:17

anastasya@ubuntu: ~

Reset Limit: Unknown  
Timer Interval: Unknown  
Timeout: Unknown

Handle 0x0268, DMI type 32, 20 bytes  
System Boot Information  
Status: No errors detected

```
anastasya@ubuntu:~$ sudo cat /sys/class/net/*/address
02:42:34:6a:27:a4
00:0c:29:f6:13:b3
00:00:00:00:00:00

anastasya@ubuntu:~$ sudo hostnamectl
Static hostname: ubuntu
Icon name: computer-vm
Chassis: vm
Machine ID: d5db0b76043640829aef6cc628c3415a
Boot ID: 779d8055b1f54ad5a75b19e6fdcab031
Virtualization: vmware
```

5. Утилита **lspci** - утилита Unix, которая печатает в стандартный вывод детальную информацию о всех PCI-шинах и устройствах на них. Основана на библиотеке **libpci**, которая предоставляет доступ к конфигурационному адресному пространству PCI на различных операционных системах.

```

anastasya@ubuntu:~$ lspci
00:00.0 Host bridge: Intel Corporation 440BX/ZX/DX - 82443BX/ZX/DX Host bridge (rev 01)
00:01.0 PCI bridge: Intel Corporation 440BX/ZX/DX - 82443BX/ZX/DX AGP bridge (rev 01)
00:07.0 ISA bridge: Intel Corporation 82371AB/EB/MB PIIX4 ISA (rev 08)
00:07.1 IDE interface: Intel Corporation 82371AB/EB/MB PIIX4 IDE (rev 01)
00:07.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 08)
00:07.7 System peripheral: VMware Virtual Machine Communication Interface (rev 10)
00:0f.0 VGA compatible controller: VMware SVGA II Adapter
00:10.0 SCSI storage controller: Broadcom / LSI 53c1030 PCI-X Fusion-MPT Dual Ultra320 SCSI (rev 01)
00:11.0 PCI bridge: VMware PCI bridge (rev 02)
00:15.0 PCI bridge: VMware PCI Express Root Port (rev 01)
00:15.1 PCI bridge: VMware PCI Express Root Port (rev 01)
00:15.2 PCI bridge: VMware PCI Express Root Port (rev 01)
00:15.3 PCI bridge: VMware PCI Express Root Port (rev 01)
00:15.4 PCI bridge: VMware PCI Express Root Port (rev 01)
00:15.5 PCI bridge: VMware PCI Express Root Port (rev 01)
00:15.6 PCI bridge: VMware PCI Express Root Port (rev 01)
00:15.7 PCI bridge: VMware PCI Express Root Port (rev 01)
00:16.0 PCI bridge: VMware PCI Express Root Port (rev 01)
00:16.1 PCI bridge: VMware PCI Express Root Port (rev 01)
00:16.2 PCI bridge: VMware PCI Express Root Port (rev 01)
00:16.3 PCI bridge: VMware PCI Express Root Port (rev 01)
00:16.4 PCI bridge: VMware PCI Express Root Port (rev 01)
00:16.5 PCI bridge: VMware PCI Express Root Port (rev 01)
00:16.6 PCI bridge: VMware PCI Express Root Port (rev 01)
00:16.7 PCI bridge: VMware PCI Express Root Port (rev 01)
00:17.0 PCI bridge: VMware PCI Express Root Port (rev 01)
00:17.1 PCI bridge: VMware PCI Express Root Port (rev 01)
00:17.2 PCI bridge: VMware PCI Express Root Port (rev 01)
00:17.3 PCI bridge: VMware PCI Express Root Port (rev 01)
00:17.4 PCI bridge: VMware PCI Express Root Port (rev 01)
00:17.5 PCI bridge: VMware PCI Express Root Port (rev 01)
00:17.6 PCI bridge: VMware PCI Express Root Port (rev 01)
00:17.7 PCI bridge: VMware PCI Express Root Port (rev 01)
00:18.0 PCI bridge: VMware PCI Express Root Port (rev 01)
00:18.1 PCI bridge: VMware PCI Express Root Port (rev 01)
00:18.2 PCI bridge: VMware PCI Express Root Port (rev 01)
00:18.3 PCI bridge: VMware PCI Express Root Port (rev 01)
00:18.4 PCI bridge: VMware PCI Express Root Port (rev 01)
00:18.5 PCI bridge: VMware PCI Express Root Port (rev 01)
00:18.6 PCI bridge: VMware PCI Express Root Port (rev 01)
00:18.7 PCI bridge: VMware PCI Express Root Port (rev 01)
02:00.0 USB controller: VMware USB1.1 UHCI Controller
02:01.0 Ethernet controller: Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) (rev 01)
02:02.0 Multimedia audio controller: Ensoniq ES1371/ES1373 / Creative Labs CT2518 (rev 02)
02:03.0 USB controller: VMware USB2 EHCI Controller
02:04.0 SATA controller: VMware SATA AHCI controller

```

6. Утилита `systemd-detect-virt` – обнаруживает выполнение в виртуализированной среде. Позволяет отличить полную виртуализацию машины от виртуального контейнера.

```

anastasya@ubuntu:~$ sudo systemd-detect-virt
vmware

```

Еще один способ на ассемблере.

Для обнаружения работы в VMware используется число 0x56D5868, которое на самом деле означает (ASCII 'VMXh'), оно присваивается регистру EAX;

Параметр команды определен в регистре EBX;

Сама команда загружается в ECX (0x0A возвращает версию VM или 0x14 возвращает размер памяти);

С порта 0x5658 считываются данные: если в регистре EBX появляется значение 'VMXh', VMware обнаружена. Это обусловлено тем, что VMware использует нереальный порт 0x5658 для коммуникации с виртуальной машиной.

Код программы на ассемблере:

**Asm\_module.asm**

```
%ifidn __OUTPUT_FORMAT__, elf64
    %define ARG1 rdi
    %define ARG2 rsi
%endif
```

```
global __VM_cmd
```

```
__VM_cmd:
    push rbp
    mov rbp, rsp
    push ARG1
    push ARG2
    mov rax, 0x564D5868;
    mov rcx, ARG2
    mov dx, 0x5658
    in eax, dx
    pop rsi
    pop rdi
    cmp rsi, 0x14
    je ret_rax
    mov [rdi], rbx
    mov rax, rcx
ret_rax:
    pop rbp
    ret
```

Код основной программы на C:

**pros\_test.c**

```
#include <stdio.h>
#include <string.h>

#if defined (__LP64__)
    #define __try bool _HadError = false;
    #define __except(x) ExitJmp:if(!_HadError)
    #include <stdlib.h>
    #include <stdbool.h>
#endif

#define DEBUG 0

extern unsigned long long __VM_cmd (unsigned long long*, unsigned);

int main(){
    unsigned long long x,y;
    __try {
        y = __VM_cmd(&x, 0x0A);
```

```

}__except(EXCEPTION_EXECUTE_HANDLER){ }
#ifdef DEBUG == 1
printf("\n [ x=%x; y=%d] \n\n", x, y);
#endif
if (x == 0x564D5868){
    printf("Result: VMware detected\nVersion : ");
    if (y == 1) printf("Express\n\n");
    else if (y == 2) printf("ESX\n\n");
    else if (y == 3) printf("Workstation\n\n");
    else printf("unknown verion\n\n");
}
else printf("Result : Native OS\n\n");
return 0;
}

```

Запуск программ:

```

anastasya@ubuntu:~/Documents/lab7$ nasm -f elf64 asm_module.asm -o asm_module.o
anastasya@ubuntu:~/Documents/lab7$ gcc pros_test.c asm_module.o -o pros_test.elf
anastasya@ubuntu:~/Documents/lab7$ ./pros_test.elf
Result: VMware detected
Version : unknown verion

anastasya@ubuntu:~/Documents/lab7$

```

Помощь и консультации в выполнении работы оказывал **Шарифуллин И.А.**