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

Усложнение: способ обнаружения работы в виртуальной машине на ассемблере.

Task: List all methods known to you to detect work in a virtual machine (>=5).

Complication: a way to detect work in a virtual machine in assembler.

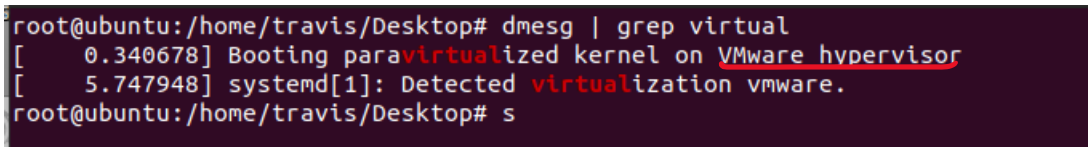
Ход работы

Способы обнаружения работы в виртуальной машине:

1. Чтение системных логов с помощью dmesg.

Вводится следующая команда:

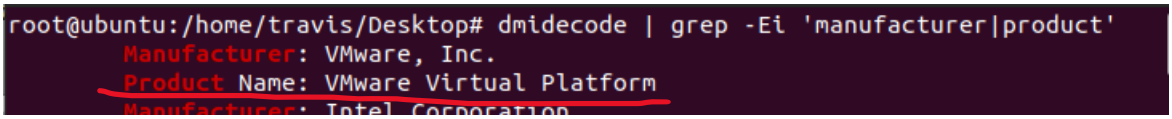
dmesg | grep virtual



Данный способ работает не на всех виртуальных машинах, поскольку не все гипервизоры заносят информацию в системные логи.

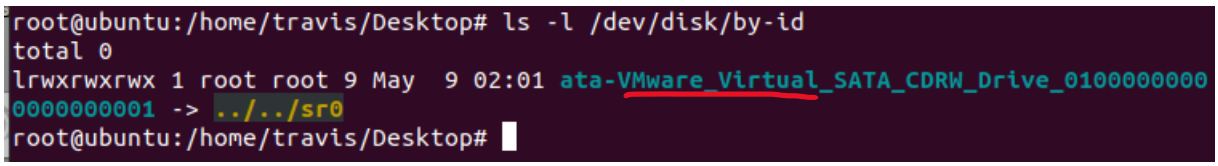
2. Анализ информации об оборудовании и BIOS с помощью dmidecode.

dmidecode | grep -Ei 'manufacturer|product'



3. Листинг каталога /dev/disk/by-id.

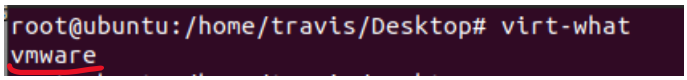
ls -l /dev/disk/by-id



Виртуальные машины должны иметь аппаратную эмуляцию с хоста. Например, эмуляция диска с хоста. Таким образом, перечисляя файлы в данном каталоге, можно легко определить, какой эмулятор используется гипервизором.

4. Использование пакета virt-what.

virt-what



virt-what - это скрипт оболочки, который можно использовать для определения того, запущена ли программа на виртуальной машине.

5. Использование утилиты lshw.

lshw -class system

```
root@ubuntu:/home/travis/Desktop# lshw -class system
ubuntu
    description: Computer
    product: VMware Virtual Platform
    vendor: VMware, Inc.
    version: None
    serial: VMware-56 4d fb 5d 11 20 8b 20-06 c6 73 bb 9a 7c f9 e4
    width: 64 bits
    capabilities: smbios-2.7 dmi-2.7 smp vsyscall32
```

lshw – это инструмент для извлечения подробной информации об аппаратной конфигурации машины.

6. Использование утилиты lspci.

lspci

```
root@ubuntu:/home/travis/Desktop# 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
root@ubuntu:/home/travis/Desktop#
```

lspci – это утилита для отображения информации о шинах PCI в системе и подключенных к ним устройствах.

Способ обнаружения виртуализации VMware в ОС Windows с помощью языка ассемблера:

```
#include <stdio.h>
#include <windows.h>
#define OOPS_PRIVILEGED_INSTRUCTION 0xC0000096
int
main(int argc, char* argv[])
{
unsigned int vm_flag = 1;

/* The check will set the VM Flag to ZERO if successful */

__try
{
__asm
{
mov eax, 0x564D5868 ; ascii: VMXh
mov edx, 0x5658 ; ascii: VX (port)
in eax, dx ; input from Port
cmp ebx, 0x564D5868 ; ascii: VMXh
setz ecx ; if successful -> flag = 0
mov vm_flag, ecx
}

if(vm_flag == 0)
printf("Inside VMWARE!!! 8-X\n");
}
__except(GetExceptionCode() == OOPS_PRIVILEGED_INSTRUCTION ?
EXCEPTION_EXECUTE_HANDLER : EXCEPTION_CONTINUE_SEARCH)
{
printf("VMWARE environment NOT detected\n");
}
return 0;
}
```