

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”

Лабораторная работа №6
“Virtual Machine detection”

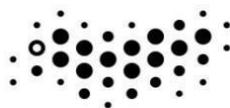
Выполнил:

ст. группы N3246 Цыдыпов А.О.



Проверил:

Ханов А.Р.



УНИВЕРСИТЕТ ИТМО

Санкт-Петербург

2022 г.

Задание:

Перечислите все известные вам способы обнаружения работы в виртуальной машине.

Ход работы:

Работа выполняется на виртуальной машине Ubuntu 22.04 LTS на virtualbox.

1. **virt-what** - shell-скрипт, который используется для детекта работы в виртуальной машине.

```
mertz@mertz-VirtualBox: ~  
mertz@mertz-VirtualBox:~$ sudo virt-what  
virtualbox  
kvm  
mertz@mertz-VirtualBox:~$
```

2. **host** в **neofetch** (или в любой другой утилите, дающий имя хоста)

```
mertz@mertz-VirtualBox: ~  
      .-/+00ssssso+/-.  
      `:+ssssssssssssssss+`  
    -+ssssssssssssssssyyss+-  
  .ossssssssssssssssdMMNysso.  
 /ssssssssssshdmmNNmyNMMMMhsssss/  
+ssssssssshmydMMMMMMNdddysssss+  
/ssssssshNMMMyhhyyyhNMMMNhsssss/  
.sssssssdMMMNhssssssshNMMMdssssss.  
+ssshhhyNMMNysssssssssyNMMMyssss+  
osssyNMMNymMhssssssssshmmhssssso  
osssyNMMNymMhssssssssshmmhssssso  
+ssshhhyNMMNysssssssssyNMMMyssss+  
.sssssssdMMMNhssssssshNMMMdssssss.  
/ssssssshNMMMyhhyyyhdNMMMNhsssss/  
+sssssssdmydMMMMMMNdddysssss+  
/ssssssssshdmmNNNmyNMMMMhsssss/  
.ossssssssssssssssdMMNysso.  
 -+ssssssssssssssssyyss+-  
  `:+ssssssssssssssss+`  
    .-/+00ssssso+/-.  
      mertz@mertz-VirtualBox  
      -----  
      OS: Ubuntu 22.04 LTS x86_64  
      Host: VirtualBox 1.2  
      Kernel: 5.15.0-40-generic  
      Uptime: 7 mins  
      Packages: 1575 (dpkg), 9 (snap)  
      Shell: bash 5.1.16  
      Resolution: 800x600  
      DE: GNOME 42.0  
      WM: Mutter  
      WM Theme: Adwaita  
      Theme: Yaru [GTK2/3]  
      Icons: Yaru [GTK2/3]  
      Terminal: gnome-terminal  
      CPU: AMD Ryzen 5 3600 (4) @ 3.593GHz  
      GPU: 00:02.0 VMware SVGA II Adapter  
      Memory: 788MiB / 8329MiB  
      ██████████
```

3. **dmidecode** - innotek GmbH = virtualbox devs

```
mertz@mertz-VirtualBox:~$ sudo dmidecode | grep Manufacturer  
Manufacturer: innotek GmbH  
Manufacturer: Oracle Corporation  
Manufacturer: Oracle Corporation  
mertz@mertz-VirtualBox:~$
```

4. **dmesg** - напишет "Hypervisor detected" в виртуалке

```
mertz@mertz-VirtualBox:~$ sudo dmesg | grep Hypervisor
[    0.000000] Hypervisor detected: KVM
mertz@mertz-VirtualBox:~$
```

5. **lscpu** - пишет KVM в поле Hypervisor vendor

```
mertz@mertz-VirtualBox:~$ lscpu | grep Hypervisor
Hypervisor vendor:                KVM
mertz@mertz-VirtualBox:~$
```

Усложненный вариант:

Метод детекта: запуская ассемблерную команду `cpuid` с единицей в младшем бите регистра `eax` и тогда на 31 бите в ВМ будет единица, а не в ВМ - ноль.

CPUID (CPU Identification) — [ассемблерная](#) мнемоника [инструкции процессоров x86](#), используется для получения информации о процессоре.

Позаимствуем код из интернета:

`./asm.s:`

```
section .data
    vm: db 'Inside VM',10
    nvm: db 'Not Inside VM',10

section .text
global _start
_start:
    xor eax, eax
    inc eax
    cpuid
    bt ecx, 0x1f
    jc invm
    mov eax, 4
    mov ebx, 1
    mov ecx, nvm
    mov edx, 14
    int 80h
    jmp exit

invm:
    mov eax, 4
    mov ebx, 1
    mov ecx, vm
    mov edx, 10
    int 80h
    jmp exit
```

```
exit:
    mov eax,1
    mov ebx,0
    int 80h
```

```
[mertz@arch 7_lab]$ nasm -f elf asm.s
```

```
[mertz@arch 7_lab]$ ld -m elf_i386 asm.o -o asm
```

```
[mertz@arch 7_lab]$ ./asm
Not Inside VM
```

```
mertz@mertz-VirtualBox:~/Desktop$ ./asm
Inside VM
```

Вывод: существуют огромное количество способов понять, выполняется ли программа в виртуальной машине или нет. В этой лабораторной работе я познакомился с несколькими из них, а также запустил ассемблерный код, позволяющий проверить это с помощью процессорной команды *cpuid*.