ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Факультет безопасности информационных технологий

Дисциплина: «Операционные системы»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №7

Выполнил:
Студент группы N3249
Чан Нгок Хуан

Проверил:
Савков Сергей Витальевич

Санкт-Петербург
2022г.

ЗАДАНИЕ

Лаб 7.
Перечислите все известные вам способы обнаружения работы в виртуальной машине. (>=5)

Сложный вариант (или)

1. Привести способ выхода из виртуальной машины
2. На ассемблере

I. **Известные вам способы обнаружения работы в виртуальной машине**.

1. **Hostnamectl**

Это выделенная утилита для управления системным именем хоста. Чтобы просмотреть текущее имя хоста, введите следующую команду: **hostnamectl**

```
tran@tran-virtual-machine:~$ hostnamectl
   Static hostname: tran-virtual-machine
         Icon name: computer-vm
           Chassis: vm
        Machine ID: cebd0c0c43e74372a11e7e3b1ee073e2
           Boot ID: 40020ca1a4f844ae9a0d5728a6d45623
    Virtualization: vmware
  Operating System: Ubuntu 20.04.4 LTS
            Kernel: Linux 5.13.0-40-generic
      Architecture: x86-64
```

2. **Dmidecode**

Dmidecode, декодер таблиц DMI, используется для поиска аппаратных компонентов вашей системы, а также другой полезной информации, такой как серийные номера и версия BIOS. С помощью этой утилиты можно несколькими способами обнаружить работу на виртуальной машине:

```
tran@tran-virtual-machine:~$ sudo dmidecode -s system-product-name
VMware Virtual Platform
```

```
tran@tran-virtual-machine:~$ sudo dmidecode|grep -i product
[sudo] password for tran:
        Product Name: VMware Virtual Platform
        Product Name: 440BX Desktop Reference Platform
```

3. **Dmesg**

Команда для вывода буфера сообщений ядра в стандартный поток вывода.

```
tran@tran-virtual-machine:~$ sudo dmesg | grep "Hypervisor detected"
[    0.000000] Hypervisor detected: VMware
```

4. **Virt-what**

Virt-what – это небольшой скрит оболочки, разработанный Red Hat, чтобы определить, работаем ли мы на виртуальной или физической машине. Установить virt-what по комманду:

```
sudo apt-get update -y
sudo apt-get install -y virt-what
```

После установки выполните следующую команду, чтобы отобразить, является ли ваша система физической или виртуальной:

sudo virt-what

Если ничего не выводится и скрит завершается с кодом 0 (без ошибок), это означает, что либо система является физической, либо является типом виртуальной машины, о которой мы не знаем или не можем обнаружить. Если ваша система виртуальная, вы увидите результат:

```
tran@tran-virtual-machine:~$ sudo apt-get update -y
Hit:1 http://ru.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://ru.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://ru.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu focal-security InRelease
Reading package lists... Done
tran@tran-virtual-machine:~$ sudo apt-get install -y virt-what
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfwupdplugin1
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  virt-what
0 upgraded, 1 newly installed, 0 to remove and 24 not upgraded.
Need to get 15,3 kB of archives.
After this operation, 49,2 kB of additional disk space will be used.
Get:1 http://ru.archive.ubuntu.com/ubuntu focal/universe amd64 virt-what amd64 1.19-1 [15,3 kB]
Fetched 15,3 kB in 0s (99,6 kB/s)
Selecting previously unselected package virt-what.
(Reading database ... 182268 files and directories currently installed.)
Preparing to unpack .../virt-what_1.19-1_amd64.deb ...
Unpacking virt-what (1.19-1) ...
Setting up virt-what (1.19-1) ...
Processing triggers for man-db (2.9.1-1) ...
tran@tran-virtual-machine:~$ sudo virt-what
vmware
```

5. **systemd-detect-virt**

Обнаруживает выполнение в виртуализированной среде. Он идентифицирует технологию виртуализации и может отличить полную виртуализацию машины от виртуализации контейнера.

```
tran@tran-virtual-machine:~$ systemd-detect-virt
vmware
```

6. **lshw**

Утилита lshw – это небольшая утилита командной строки, которая отображает подробную информацию об оборудовании Unix-подобной системы. Она отображает все детали оборудования, включая конфигурацию памяти, версию прошивки, конфигурацию материнской платы, версию и скорость процессора, конфигурацию кеша, скорость шины и т. д. Выполните следующую команду, чтобы узнать, является ли ваша система физической или виртуальной:

sudo lshw -class system

```
tran@tran-virtual-machine:~$ sudo lshw -class system
tran-virtual-machine
    description: Computer
    product: VMware Virtual Platform
    vendor: VMware, Inc.
    version: None
    serial: VMware-56 4d 59 55 f6 b0 6e 2c-01 d8 c6 a5 c9 95 c9 d4
    width: 64 bits
    capabilities: smbios-2.7 dmi-2.7 smp vsyscall32
    configuration: administrator_password=enabled boot=normal frontpanel_password=unknown keyboard_password=unknown power-on_password=disabled
 uuid=564D5955-F6B0-6E2C-01D8-C6A5C995C9D4
  *-pnp00:00
       product: PnP device PNP0c02
       physical id: 3
       capabilities: pnp
       configuration: driver=system
  *-pnp00:01
       product: PnP device PNP0b00
       physical id: 4
       capabilities: pnp
       configuration: driver=rtc_cmos
  *-pnp00:04
       product: PnP device PNP0103
       physical id: 85
       capabilities: pnp
       configuration: driver=system
  *-pnp00:07
       product: PnP device PNP0c02
       physical id: 88
       capabilities: pnp
       configuration: driver=system
  *-remoteaccess UNCLAIMED
       vendor: Intel
       physical id: 1
       capabilities: inbound
```

7. Imvirt

Imvirt — это еще один небольшой Perl-скрипт, который помогает определить, работаем ли мы на виртуальной машине.

Установить virt-what по комманд: sudo apt-get install imvirt

```
tran@tran-virtual-machine:~$ sudo imvirt
VMware Workstation
```

II. **Сложный вариант:**

Обнаружение виртуальной машины с помощью Assembler кода

CPUID (CPU Identification) — ассемблерная мнемоника инструкции процессоров x86, используется для получения информации о процессоре. Используя её, программа может определить тип процессора и его возможности. Вид выдаваемой этой командой информации зависит от содержимого регистра EAX. Результат работы команды записывается в регистры EBX, ECX и EDX. Для наших целей мы будем использовать эту инструкцию, предварительно положив в регистр EAX значение 0x40000000:

```
SECTION .data
res1: db "Virtual machine", 10
len1: equ $-res1
res2: db "None", 10
len2: equ $-res2

section .text
    global _start
_start:
    xor eax, eax
    mov eax, 0x40000000
    cpuid
    cmp ecx, 0x4D566572     ;Mver
    jne None
    cmp edx, 0x65726177      ;eraw
    jne None
    mov edx, len1          ;длина сообщения
    mov ecx, res1          ; сообщение для написания
    mov ebx,1              ;файловый дескриптор
    mov eax,4              ;номер системного вызова
    int 0x80               ;вызов ядра (kernel)
    jmp finish
None:
    mov edx, len2
    mov ecx, res2
    mov ebx,1
    mov eax,4
    int 0x80
finish:
    xor ebx, ebx
    mov eax,1
    int 0x80
```

When the leaf at `0x40000000` is queried, the hypervisor will return information that provides the maximum hypervisor CPUID leaf number and a vendor ID signature.

Register	Information Provided
EAX	The maximum input value for hypervisor CPUID information
EBX	Hypervisor Vendor ID Signature
ECX	Hypervisor Vendor ID Signature
EDX	Hypervisor Vendor ID Signature

Leaf	Information Provided	
0x40000000	Hypervisor CPUID leaf range and vendor ID signature.	
	EAX	The maximum input value for hypervisor CPUID information. On Microsoft hypervisors, this will be at least 0x40000005. The vendor ID signature should be used only for reporting and diagnostic purposes.
	EBX	0x7263694D—“Micr”
	ECX	0x666F736F—“osof”
	EDX	0x76482074—“t Hv”

- Результат работы:

на реальной системе:

```
chudoan@chudoan-Latitude-5510:~/Downloads$ nasm -f elf64 lab7.asm -o lab7.o
chudoan@chudoan-Latitude-5510:~/Downloads$ ld lab7.o -o lab7
chudoan@chudoan-Latitude-5510:~/Downloads$ ./lab7
None
```

на виртуальной машине:

```
tran@tran-virtual-machine:~/OS/LAB7$ nasm -f elf64 lab7.asm -o lab7.o
tran@tran-virtual-machine:~/OS/LAB7$ ld lab7.o -o lab7
tran@tran-virtual-machine:~/OS/LAB7$ ./lab7
Virtual Machine
```

III. Вывод

После выполнения этой лабораторной работы, я научился разные способы обнаружения работы в виртуальной машине.