ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ - ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»

Факультет безопасности информационных технологий

Кафедра проектирования и безопасности компьютерных систем

Дисциплина:

«Операционные системы»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 7

Выполнил:

Студент группы N3248

Назаров Максим Вячеславович

Проверил:

Савков Алексей Витальевич

Санкт - Петербург 2022г.

Лаб 7.

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

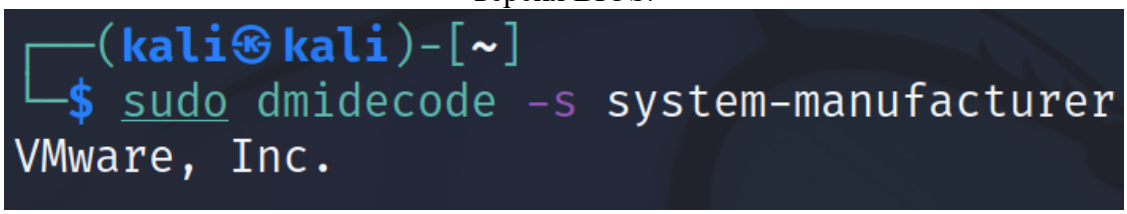
Сложный вариант (или)

- Привести способ выхода из виртуальной машины
- На ассемблере

Все дальнейшие действия производились в виртуальной машине с ОС kali linux на VMware последней версии.

Обнаружение виртуальной машины

Dmidecode - декодер таблиц DMI, используется для поиска аппаратных компонентов вашей системы, а также другой полезной информации, такой как серийные номера и версия BIOS.



1) Facter - это утилита командной строки для сбора и отображения информации о системе.

```
┌──(kali㉿kali)-[~/facter]
└─$ sudo facter | grep virtual
is_virtual ⇒ true
virtual ⇒ vmware
```

2) virt - what - сценарий командной оболочки, с помощью которого можно определить запущен ли он на виртуальной машине. Программа выводит список «фактов» о виртуальной машине, получаемых эвристическим методом.

```
┌──(kali㉿kali)-[~/facter]
└─$ sudo virt-what
vmware
```

3) Утилита lspci - С помощью утилиты lspci можно просмотреть информацию обо всех шинах PCI и подключенных к ним устройствах. Она входит в пакет pciutils, включенный в большинство современных дистрибутивов Linux; если он по каким - либо причинам отсутствует, его можно установить при помощи стандартного менеджера пакетов.

```
┌──(kali㉿kali)-[~/facter]
└─$ lspci | grep VMware | tail -1
02:03.0 USB controller: VMware USB2 EHCI Controller
```

4) 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.

```
┌──(kali㉿kali)-[~/facter]
└─$ sudo lshw | grep -i virtual
    product: VMware Virtual Platform
             product: Virtual Machine Communication Interface
                product: VMware Virtual S
                      product: VMware VMware Virtual USB Mouse
                      product: VMware Virtual USB Hub
       product: VirtualPS/2 VMware VMMouse
       product: VirtualPS/2 VMware VMMouse
```

5) Псевдофайлы /proc

hypervisor - указывается, если ОС запущена под гипервизором;

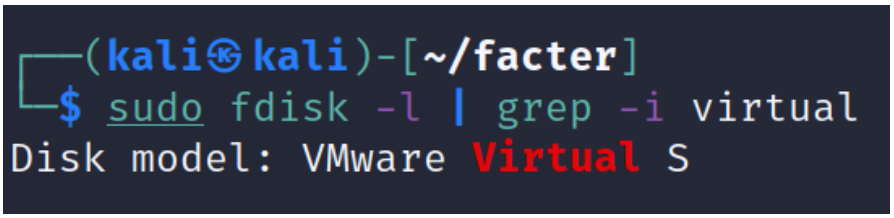
```
┌──(kali㉿kali)-[~/facter]
└─$ cat /proc/cpuinfo | grep hypervisor
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pg
e mca cmov pat pse36 clflush mmx fxsr sse sse2 ht syscall nx mmxext f
xsr_opt rdtscp lm constant_tsc rep_good nopl tsc_reliable nonstop_tsc
 cpuid extd_apicid tsc_known_freq pni pclmulqdq ssse3 fma cx16 sse4_1
 sse4_2 movbe popcnt aes xsave avx hypervisor lahf_lm extapic abm sse
4a misalignsse 3dnowprefetch osvw ssbd vmmcall arat overflow_recov su
ccor
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pg
e mca cmov pat pse36 clflush mmx fxsr sse sse2 ht syscall nx mmxext f
xsr_opt rdtscp lm constant_tsc rep_good nopl tsc_reliable nonstop_tsc
 cpuid extd_apicid tsc_known_freq pni pclmulqdq ssse3 fma cx16 sse4_1
 sse4_2 movbe popcnt aes xsave avx hypervisor lahf_lm extapic abm sse
4a misalignsse 3dnowprefetch osvw ssbd vmmcall arat overflow_recov su
ccor
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pg
e mca cmov pat pse36 clflush mmx fxsr sse sse2 ht syscall nx mmxext f
xsr_opt rdtscp lm constant_tsc rep_good nopl tsc_reliable nonstop_tsc
 cpuid extd_apicid tsc_known_freq pni pclmulqdq ssse3 fma cx16 sse4_1
 sse4_2 movbe popcnt aes xsave avx hypervisor lahf_lm extapic abm sse
4a misalignsse 3dnowprefetch osvw ssbd vmmcall arat overflow_recov su
ccor
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pg
e mca cmov pat pse36 clflush mmx fxsr sse sse2 ht syscall nx mmxext f
xsr_opt rdtscp lm constant_tsc rep_good nopl tsc_reliable nonstop_tsc
 cpuid extd_apicid tsc_known_freq pni pclmulqdq ssse3 fma cx16 sse4_1
 sse4_2 movbe popcnt aes xsave avx hypervisor lahf_lm extapic abm sse
4a misalignsse 3dnowprefetch osvw ssbd vmmcall arat overflow_recov su
ccor
```

6) Узнать тип системы можно с помощью утилиты dmesg. Dmesg используется для проверки кольцевого буфера ядра или управления им. Моя ОС:

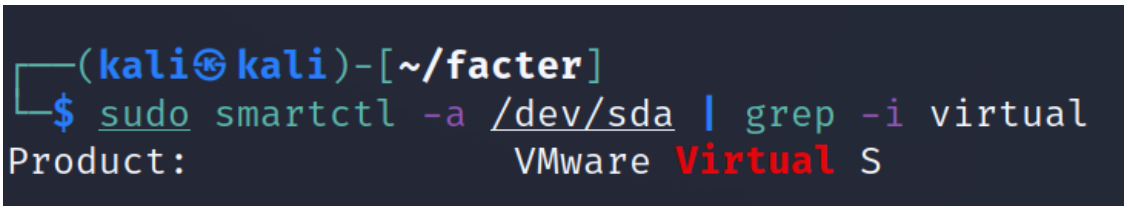
```
┌──(kali㉿kali)-[~]
└─$ sudo dmesg | grep "Hypervisor detected"
[    0.000000] Hypervisor detected: VMware
```

Как мы видим, ничего не выводится, так как гипервизор не был найден, а значит машина физическая Виртуальная машина:

7) fdisk - fdisk обозначает "fixed disk" или "format disk". Это утилита командной строки, которая позволяет пользователям выполнять различные действия с дисками. Она позволяет нам просматривать, создавать, изменять размеры, удалять, перемещать и копировать разделы.



8) smartctl - Просмотреть подробную информацию о состоянии жесткого диска можно при помощи утилиты smartctl, включенной в официальные репозитории большинства современных дистрибутивов Linux. Для просмотра полной информации нужно ввести команду:



9) lscpu -это небольшая и быстрая команда, не требующая никаких опций. Она просто выводит информацию об аппаратном обеспечении CPU в удобном для пользователя формате.

```
┌──(kali㉿kali)-[~/facter]
└─$ lscpu | grep -i vmware
Hypervisor vendor:                    VMware
```

10)

```
┌──(kali㉿kali)-[~/facter]
└─$ ls /dev/disk/by-id/
ata-VMware_Virtual_IDE_CDROM_Drive_10000000000000000001
```

11) Мы можем узнать, является ли наша система виртуальной или физической, используя команду hostnamectl.

```
┌──(kali㉿kali)-[~]
└─$ hostnamectl status
 Static hostname: kali
       Icon name: computer-vm
         Chassis: vm 
      Machine ID: 0e5f878f6b6c4f04867b3ee69ad14862
         Boot ID: 70bc8082229940d2ba0aa30c73642286
  Virtualization: vmware
Operating System: Kali GNU/Linux Rolling
          Kernel: Linux 5.15.0-kali3-amd64
    Architecture: x86-64
 Hardware Vendor: VMware, Inc.
  Hardware Model: VMware Virtual Platform
```

12) hwinfo - мощная утилита, с помощью которой можно получить детальную информацию об аппаратных компонентах вашего персонального компьютера (например, температуре жесткого диска и данные S.M.A.R.T., показания датчиков и т.д.) . Присутствуют индикаторы в системном трее, мониторинг в режиме реального времени, уведомления, генерация и импорт отчетов и прочие полезные инструменты и функции.

```
┌──(kali㉿kali)-[~/facter]
└─$ sudo hwinfo | grep -i virtual | wc -l
549
```

13) lsscsi - список устройств scsi.

Выдается список устройств scsi/sata, например, жестких дисков и оптических приводов.

```
┌──(kali㉿kali)-[~/facter]
└─$ sudo lsscsi
[1:0:0:0]    cd/dvd  NECVMWar VMware IDE CDR10 1.00  /dev/sr0
[2:0:0:0]    disk    VMware,  VMware Virtual S 1.0   /dev/sda
```

14) lsusb - подробный список шин и устройств usb

Эта команда показывает информацию о контроллерах usb и подробные сведения о подключенных к ним устройствах. По умолчанию выдается краткая информация. Для того, чтобы о каждом порте usb получить подробную информацию, используйте параметр " - v".

```
┌──(kali㉿kali)-[~/facter]
└─$ sudo hwinfo | grep -i virtual | wc -l
549
```

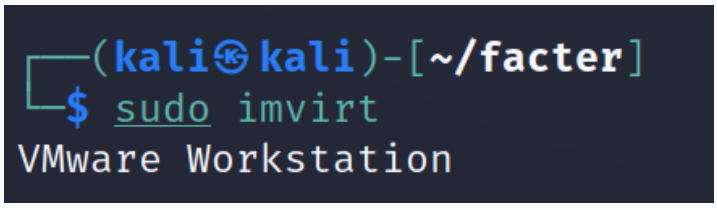
15) Inxi - мега скрипт bash, состоящий из 10000 строк кода, с помощью которого из разных источников и команд системы будет получена подробная информация об аппаратном обеспечении и будет создан отчет в виде, позволяющим его читать пользователям, которые не являются техническими специалистами.

```
┌──(kali㉿kali)-[~/facter]
└─$ inxi -Fx | grep -i virtual
  Type: Vmware System: VMware product: VMware Virtual Platform
    vendor: VMware Virtual Machine type: network bridge driver: N/A
  ID-1: /dev/sda vendor: VMware model: Virtual S size: 80 GiB
```

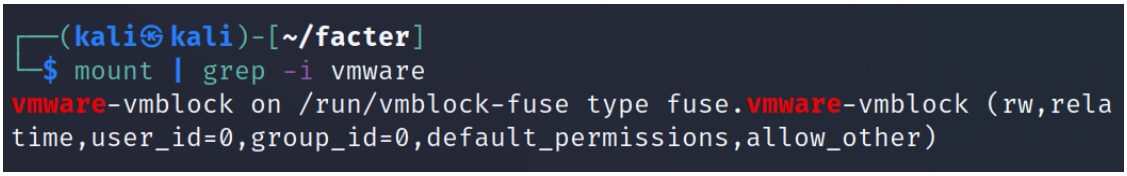
16) Инструмент systemd - detect - virt обнаруживает технологию виртуализации и может отличить полную виртуализацию машины от аппаратной или контейнерной виртуализации.

```
┌──(kali㉿kali)-[~/facter]
└─$ systemd-detect-virt
vmware
```

17) Imvirt - это небольшой скрипт Perl, который помогает вам определить, работает ли мы на виртуальной машине.



18) Mount - Команда mount используется для монтирования/демонтирования, а также для просмотра смонтированных файловых систем.



Обнаружение виртуальной машины с помощью Assembler кода.

Идентификатор процессора определяется с помощью команды cpuid. Благодаря ей можно получить много всякой полезной информации об установленном процессоре. Вид выдаваемой этой командой информации зависит от содержимого регистра EAX. Результат работы команды записывается в регистры EBX, ECX и EDX. Подробно про эту команду можно почитать в любой книге по программированию на ассемблере. Для наших целей мы будем использовать эту инструкцию, предварительно положив в регистр EAX значение 0x40000000:

```
SECTION .data
res1:   db "VM",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
    jne None
    cmp edx,0x65726177
    jne None
    mov edx,len1
    mov ecx,res1
    mov ebx,1
    mov eax,4
    int 0x80
    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
```

Результат работы: