



mkantoz1 / study_2024_2025_infosec



<> Code

Issues

Pull requests

Actions

Projects

Wiki

Security



study_2024_2025_infosec / labs / lab01 / presentation / LAB1 report.md



mkantoz1 Update and rename presentation.md to LAB1 report.md

8a7e409 · yesterday



88 lines (25 loc) · 2.35 KB

Preview

Code

Blame



Raw



Презентация по лабораторной работе №1 Основы информационной безопасности

• Mehmet Efe Kantoz

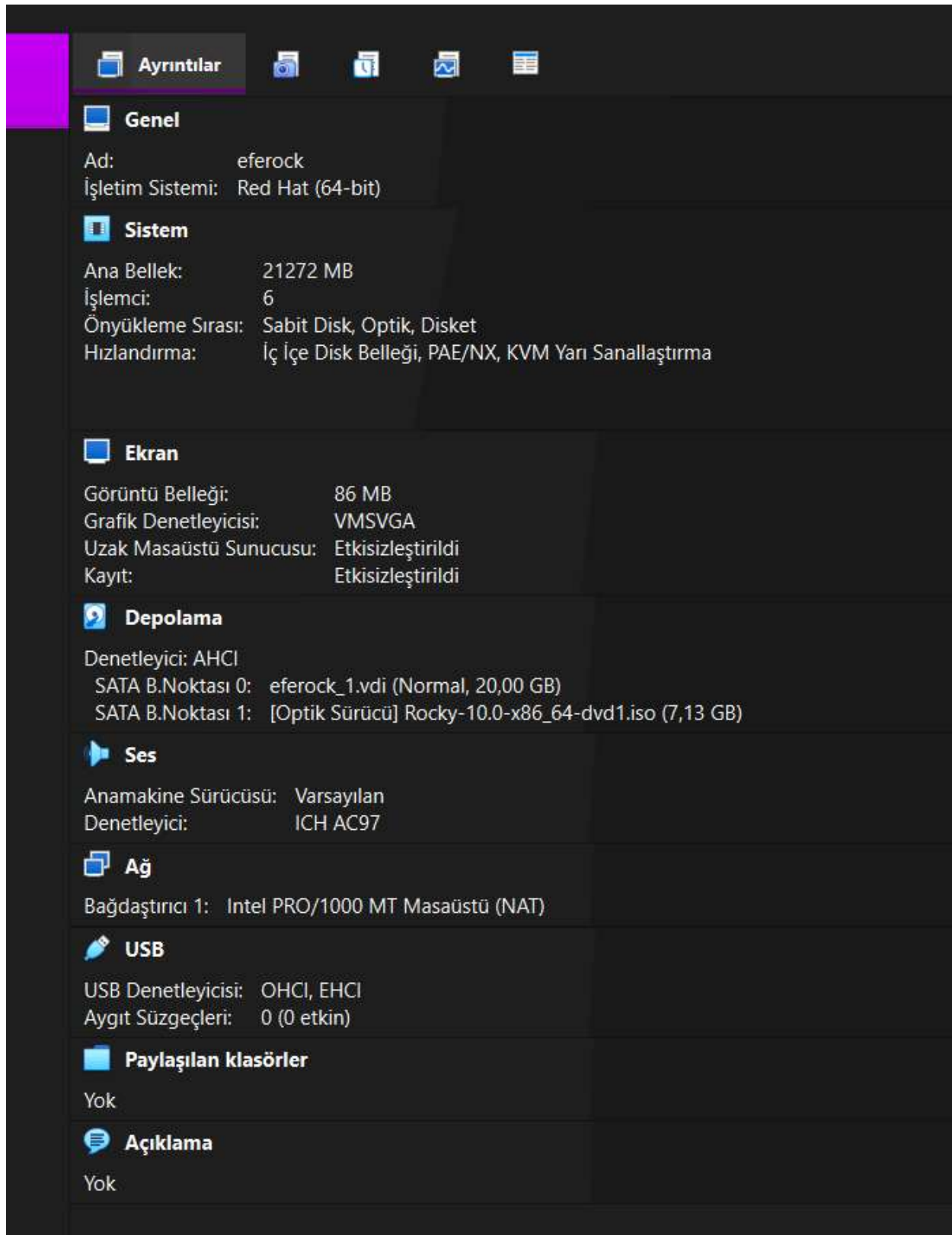
студентка группы НКАбд-01-23 • Российский университет дружбы народов •

Целью данной работы является приобретение практических навыков установки операционной системы на виртуальную машину, настройки минимально необходимых для дальнейшей работы сервисов

Установка и настройка операционной системы

. 2. Найти следующую информацию: 2.1 Версия ядра Linux (Linux version). 2.2 Частота процессора (Detected Mhz processor). 2.3 Модель процессора (CPU0). 2.4 Объем доступной оперативной памяти (Memory available). 2.5 Тип обнаруженного гипервизора (Hypervisor detected). 2.6 Тип файловой системы корневого раздела.

Я выполняю лабораторную работу на домашнем оборудовании, поэтому создаю новую виртуальную машину в VirtualBox, выбираю



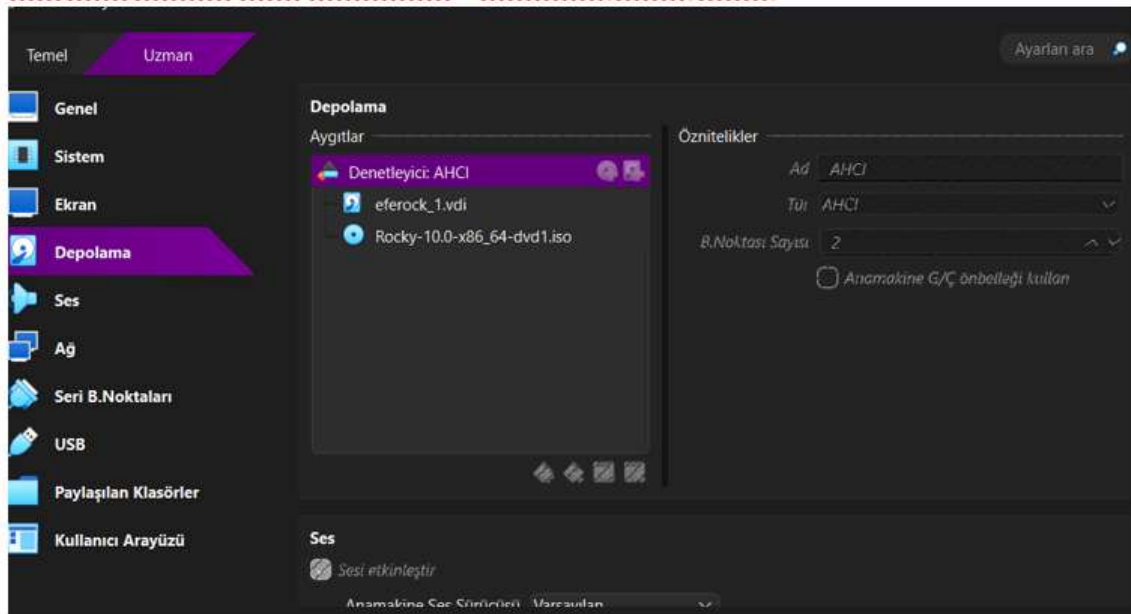
устанавливать будем операционную систему Rocky DVD

Соглашаюсь с предоставленными настройками

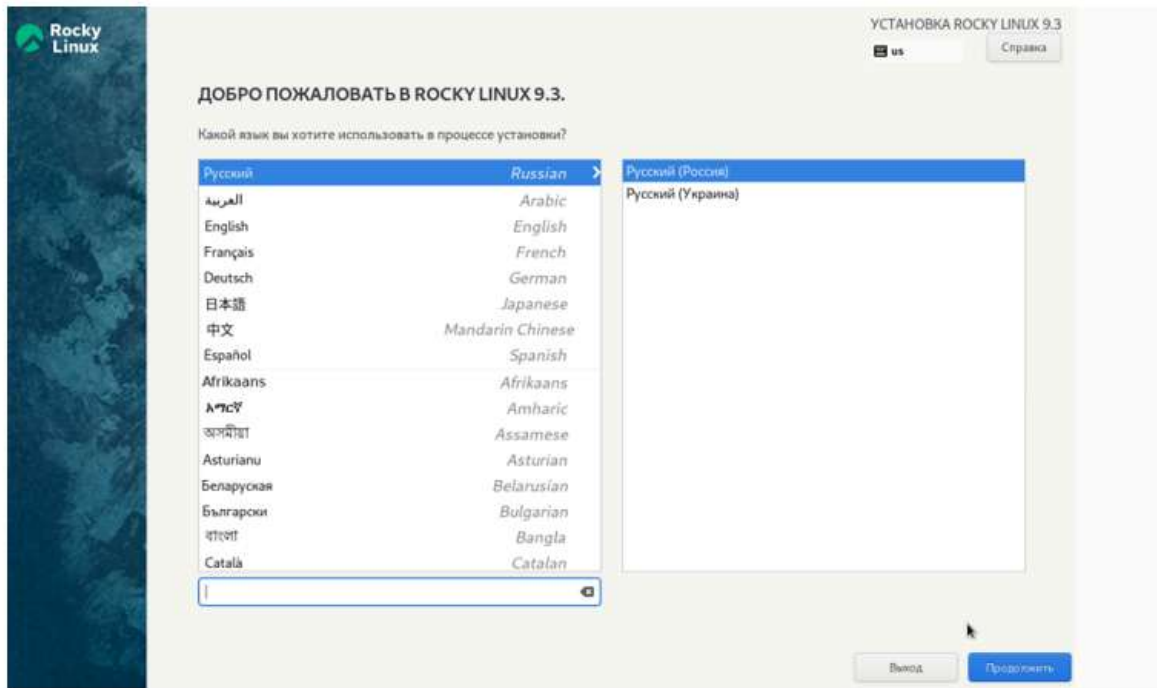
Начинается загрузка операционной системы



При этом должен быть подключен в носителях образ диска



Выбираю язык установки

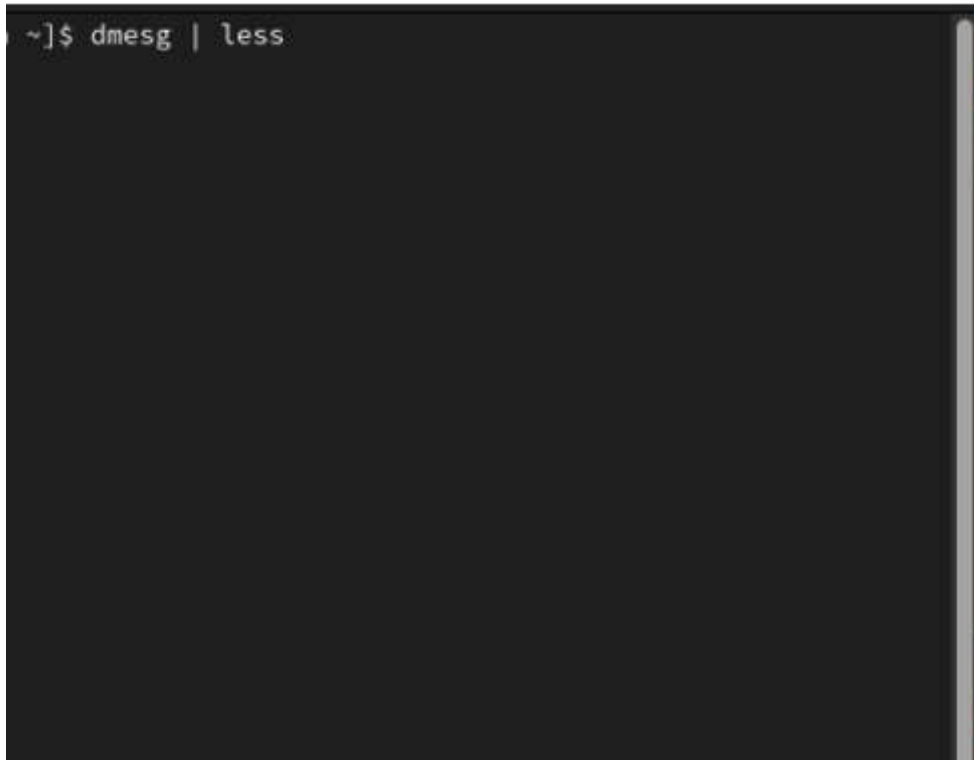


В обзоре установки будем проверять все настройки и менять на нужные



Выполнение дополнительного задания

Открываю терминал, в нем прописываю `dmesg | less`



Версия ядра 5.14.0-362.8.1.el9_3.x86_64

```
[ 0.000000] Linux version 5.14.0-362.8.1.el9_3.x86_64 (mockbuild@iad1-prod-bu
ild001.bld.equ.rockylinux.org) (gcc (GCC) 11.4.1 20230605 (Red Hat 11.4.1-2), GN
U ld version 2.35.2-42.el9) #1 SMP PREEMPT_DYNAMIC Wed Nov 8 17:36:32 UTC 2023
[evdvorkina@evdvorkina ~]$
```

Рис. 11: Версия ядра

```

grep: version: Нет такого файла или каталога
[evdvorkina@evdvorkina ~]$ dmesg | grep -i Linux Version
grep: Version: Нет такого файла или каталога
[evdvorkina@evdvorkina ~]$ dmesg | grep -i "Linux version"
[ 0.000000] Linux version 5.14.0-362.8.1.el9_3.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.4.1 20230605 (Red Hat 11.4.1-2), GNU ld version 2.35.2-42.el9) #1 SMP PREEMPT_DYNAMIC Wed Nov 8 17:36:32 UTC 2023
[evdvorkina@evdvorkina ~]$ dmesg | grep -i "Detected Mhz processor"
[evdvorkina@evdvorkina ~]$ dmesg | grep -i "Detected Mhz"
[evdvorkina@evdvorkina ~]$ dmesg | grep -i "Detected"
[ 0.000000] Hypervisor detected: KVM
[ 0.000010] tsc: Detected 1992.000 MHz processor
[ 0.491415] hub 1-0:1.0: 12 ports detected
[ 0.500150] hub 2-0:1.0: 12 ports detected
[ 1.573999] systemd[1]: Detected virtualization oracle.
[ 1.574005] systemd[1]: Detected architecture x86-64.
[ 2.260568] Warning: Unmaintained hardware is detected: e1000:100E:8086 @ 00:00:00:03.0
[ 4.594918] systemd[1]: Detected virtualization oracle.
[ 4.594923] systemd[1]: Detected architecture x86-64.
[evdvorkina@evdvorkina ~]$

```

Модель процессора Intel Core i7-8550U

```

0.003247] PM: hibernation: Registered nosave memory: [mem 0x00000000-0x0000ffff]
0.003249] PM: hibernation: Registered nosave memory: [mem 0x0009f000-0x0009ffff]
0.003250] PM: hibernation: Registered nosave memory: [mem 0x000a0000-0x000effff]
0.003250] PM: hibernation: Registered nosave memory: [mem 0x000f0000-0x000ffff]
0.015632] Memory: 260860K/2096696K available (16384K kernel code, 5596K rdata, 11444K rodata, 3824K init, 18424K bss, 158276K reserved, 0K cma-reserved)
0.089223] Freeing SMP alternatives memory: 36K
1.203111] Freeing initrd memory: 57244K
1.460019] Freeing unused decrypted memory: 2036K
1.460771] Freeing unused kernel image (initmem) memory: 3824K
1.465494] Freeing unused kernel image (rodata/data gap) memory: 844K

```

Обнаруженный гипервизор типа KVMv


```
[ 0.000000] Hypervisor detected: KVM
[ 0.073694] SRBDS: Unknown: Dependent on hypervisor status
[ 0.073695] GDS: Unknown: Dependent on hypervisor status
```

sudo fdisk -l показывает тип файловой системы, типа Linux, Linux LVM

Мы полагаем, что ваш системный администратор изложил вам основы безопасности. Как правило, всё сводится к трём следующим правилам:

- №1) Уважайте частную жизнь других.
- №2) Думайте, прежде что-то вводить.
- №3) С большой властью приходит большая ответственность.

[sudo] пароль для evdvorkina:

Диск /dev/sda: 40 GiB, 42949672960 байт, 83886080 секторов

Disk model: VBOX HARDDISK

Единицы: секторов по 1 * 512 = 512 байт

Размер сектора (логический/физический): 512 байт / 512 байт

Размер I/O (минимальный/оптимальный): 512 байт / 512 байт

Тип метки диска: dos

Идентификатор диска: 0x00b40096

Устр-во	Загрузочный	начало	Конец	Секторы	Размер	Идентификатор	Тип
/dev/sda1	*	2048	2099199	2097152	1G	83	Linux
/dev/sda2		2099200	83886079	81786880	39G	8e	Linux LVM

Далее показана последовательно монтирования файловых систем

```
[ 0.070880] Mount-cache hash table entries: 4096 (order: 3, 32768 bytes, linear)
[ 0.070886] Mountpoint-cache hash table entries: 4096 (order: 3, 32768 bytes, linear)
[ 3.968701] XFS (dm-0): Mounting V5 Filesystem
[ 3.990946] XFS (dm-0): Ending clean mount
[ 5.087934] systemd[1]: Set up automount Arbitrary Executable File Formats File System Automount Point.
[ 5.103176] systemd[1]: Mounting Huge Pages File System...
[ 5.105646] systemd[1]: Mounting POSIX Message Queue File System...
[ 5.114903] systemd[1]: Mounting Kernel Debug File System...
[ 5.117063] systemd[1]: Mounting Kernel Trace File System...
[ 5.153426] systemd[1]: Starting Remount Root and Kernel File Systems...
[ 5.183994] systemd[1]: Mounted Huge Pages File System.
[ 5.184506] systemd[1]: Mounted POSIX Message Queue File System.
[ 5.184983] systemd[1]: Mounted Kernel Debug File System.
[ 5.185737] systemd[1]: Mounted Kernel Trace File System.
[ 5.196437] systemd[1]: Finished Remount Root and Kernel File Systems.
[ 5.200572] systemd[1]: Mounting FUSE Control File System...
[ 5.203467] systemd[1]: Mounting Kernel Configuration File System...
[ 5.204176] systemd[1]: OSTree Remount OS/ Bind Mounts was skipped because of an unmet condition check (ConditionKernelCommandLine=ostree).
[ 7.229376] XFS (sda1): Mounting V5 Filesystem
[ 7.564957] XFS (sda1): Ending clean mount
```

Я приобрела практические навыки установки операционной системы на виртуальную машину, настройки минимально необходимых для дальнейшей работы сервисов.

...