HOMEWORK 1

Answer all of the questions from the practical assignment.

Sections:

Get KeePass

Question: Do the checksums match?
Answer: Yes they do, as they should.

Run Some Useful Commands

Question: Look also at disks **sdb** to **sdg**. What do you think these are used for?
Answer: These are the devices that are connected to the machine.

Question: Do you find a pattern in the disk naming notation?
Answer: Yes. Refer to the **Bonus** section for a better answer.

Look at the system logs (the old way)

Question: Do you see anything suspicious?
Answer: Yes! Upon further investigation, it turns out that there are some remote servers that are constantly trying to break into the machine, trying to guess that password for login. Usually these attacks are coming somewhere form China.

Run a security scan of your system

Question: Did **lynis** find any problems with your system?
Answer: Yes. 3 Warnings were issued. 1 was that GRUB2 wasn't set up with password protection (such is life). The other two were because some account names were not set up.

Bonus

Why are the Linux Hard Disk names called sdX?

Answer:
Under Linux systems, the kernel is the one that handles external *Hard Drives*, *SSDs*, *USB* sticks, *DVDs*, *Floppy Disks*, etc. And because these hardware devices need a place to connect to, through which the user and system can access them, a naming convention was developed in order for the user to understand what is connected to the machine. This naming convetion relies on the different types of devices and more importantly, on their interface for connection. In general we have several types of device interfaces, device names, protocols, packages and so on - IDE, SATA, PATA, SCSI, ATAPI, ESDI, etc. With so many different technologies and names, it's kind of easy to get lost in the naming conventions, so lets take a step back and take a detour through history to see how storage interfaces developed through the years (and to also untangle all of these names).

April 23, 1970, Western Digital opened its doors as a new comer to the computer chip manufacturing world. Making calculator chips and earning the trust of other major companies, *WDC* managed to rise as one of the most famous IT companies in the late 20th century. The turning point for them though, was when they managed to create a very specific hardware part called *FD1771*, a floppy disk controller. This was their entrance to the world of data storage and interfaces. By the early 1980s, with the success of the *FD1771*, they managed to score a contract with **IBM** and started producing hard disk controllers for IMBs famous PC/AT machine. Under the name **I**ntegrated **D**rive **E**lectronics (or IDEs for short), these devices were special, because, in addition to their connector and interface, they had a drive controller directly integrated into the drive itself. This alleviated the motherboard from these low-level mechanical operations, which were now performed by the controller. In comparison during the same time, another type of interfaces were popular, namely - the **E**nhanced **S**mall **D**isk **I**nterface (ESMDI), but they soon fell out due to the advantages of IDEs. That specific controller (*WD1003* for the PC/AT - *PC/Advanced Technology*) paved the way for the famous interface standard for hard drives - **ATA** (Advanced Technology Attachment). Thus IDE was renamed to ATA. After that, the company, going through its ups and downs, continued making different controllers, moving to SCSI ones and so on.

Then in 1994 Enhanced IDEs (EIDE) (also called *ATA2*) were developed, bringing performance enhancements.

In 1998 a new protocol was made for the ATA, called the **ATAPI** (ATA Packet Interface). Until now ATA was only useful for the connection of hard disks and floppies to computers, but with this shiny new protocol, a great variety of devices became elagable to be connected to computers. ATA did not have commands like *"eject device"* or *"is there a device connected to my machine right now?"*, but *ATAPI* brought the answers to those problems. It carried instructions for SCSI through the ATA interface. Thus ATAPI was both compatible with ATA and SCSI. This allowed for the connectivity of CD-ROMs, DVD-ROMs, tape drives, magneto-optical drives, and bigger floppy disks.

After that *UDMA*, *ATA-3*, *ATA/ATAPI-4/5/6/7/8*, and *Ultra ATA* came to be. Then in 2003 a new **Serial ATA** (SATA) was introduced, thus replcaing the name ATA/IDE to **P**arallel **ATA** (PATA). SATA brought hot swapping, lower prices, and better data transfer performance to its predecessor.

On the other side, we also have **S**mall **C**omputer **S**ystem **I**nterface (or SCSI for short, also pronounced "**scuzzy**"). This is another set of standards for the connection of physical devices to computers and the data transfer between them. The first standard was developed in 1982, standardized in 1986 called SCSI-1, and the second one emerged in 1990 with the name SCSI-2.

There are several differences between *SCSI* and *ATA*. ATA/IDE devices are cheaper and easier to make in comparison to the more technically advanced SCSI ones. On the other hand, because of this technical advantage, SCSI can connect from **7** to **15** devices at a time, while ATA/IDE can do maximum of **2** (Well not exactly 2, but for the sake of argument lets leave it at that). Also modern hard disks with fast rotating speeds only have SCSI controller, while slower ones have both ATA/IDE and SCSI connections. Another difference is that SCSI requires an additional expansion card to the motherboard that will allow for the connection to be established, while ATA/IDE can be directly plugged in. As a final note, modern hard drives are moving form ATA/IDE and SCSI to SATA.

So after that quick review of technological history, what is up with the naming conventions of disk names under Linux distros?

Linux used to handle peripheral devices like this - `/dev/` holds special device files, that correspond to the physical devices, `/media/` is the place where we mount removable devices, and `/mnt/` is the place where we mount permanent devices. ATA/IDE and ATAPI devices used to be connected under the `/dev/hdX` convention, thus indicating that an ATA/IDE controller was used. SCSI and SATA devices were under the `/dev/sdX` convention, indicating a SCSI controller. But at some point, and more precisely, at Linux Kernel version **2.6.20** (current one being 4.15.13 at time of writing this), a new libATA system was released, that changed these naming standards. Now all ATA/IDE, SCSI, and SATA devices will be found under the `/dev/sdX` name. This means that if we run `ls /dev | grep '[s|h]d[a-z]'` we would see if the machine is using this system.

Note - not *all* Linux distributions are defaulting to this system. There are some that like to be rebels (like Kubuntu Gutsy/Feisty).

So when I check what my system uses, I get this:

```
$ ls /dev | grep '[s|h]d[a-z]'
sda
sda1
sda2
sda3
sdb
sdb1
sdb2
sdb3
sdb4
sdb5
sdc
sdc1
sdc2
sdc5
```

sdc6

It seems that I have the libATA system enabled. If we have CD/DVD devices however, they will not be shown. In order to locate them (if there are any), we need to run `ls /dev | grep sr`. We can also check what are our currently mounted devices with `mount | grep ^'/dev'`.

```
$ mount | grep ^'/dev'
/dev/sdc6 on / type ext4 (rw,relatime,errors=remount-ro,data=ordered)
/dev/sdb2 on /boot/efi type vfat (rw,relatime,fmask=0077,dmask=0077. . .
/dev/sda2 on /media/mdn/**** type fuseblk (rw,nosuid,nodev,relatime. . .
```

Also if we want to correlate a specific device found in the `/dev/` directory, we can use `ls -ld /sys/block/sd*/device` to see where each device is connected to.

```
$ ls -ld /sys/block/sd*/device
lrwxrwxrwx 1 root root 0 Mar 29 14:23 /sys/block/sda/device -> ../../../2:0:0:0
lrwxrwxrwx 1 root root 0 Mar 29 14:23 /sys/block/sdb/device -> ../../../4:0:0:0
lrwxrwxrwx 1 root root 0 Mar 29 14:23 /sys/block/sdc/device -> ../../../5:0:0:0
```

So what is this libATA system exactly. Well, for one, it was developed by Jeff Garzik and currently maintained by Lukasz Kosewski. Directly taking from the dev guide:

"libATA is a library used inside the Linux kernel to support ATA host controllers and devices. libATA provides an ATA driver API, class transports for ATA and ATAPI devices, and SCSI<->ATA translation for ATA devices according to the T10 SAT specification. Features include power management, S.M.A.R.T., PATA/SATA, ATAPI, port multiplier, hot swapping and NCQ."

Couldn't have said it better myself. But there is a limitation though. The old ATA/IDE systems allowed a user to have up to *64* partitions on a disk, while with the libATA system, that number is brought down to *15*. Unless of course we try an experimental patch by Carl-Daniel Hailfinger that allows us to have **127** partitions).

Now only one thing is left to untangle. The suffixes of the devices, why are they `a, b, c` etc. For ATA/IDE the *abc's* have special meaning. **a** is the master drive on the first bus, **b** is the slave drive on the second bus, **c** is the master drive on the third bus. For the SCSI convention of *abc*'s is this - since each drive has an ID, it depends on the order of that ID what letter will the drive receive. That is - if we have 3 SCSI drives with IDs 0, 1, and 3, they would be called **sda**, **sdb**, and **sdc**. At this point, if we introduce a new drive with an ID of 2, it then will get the name **sdc**, and the previous *sdc* will be pushed to **sdd**. The numbers at the end of each device just indicate the particular partition of that device. If you don't like this naming convention e2label is here to help!

Extra References:
libATA hotswap
libATA wiki
Role of dev, media, and mnt
Difference between dev, media, and mnt
Advantages of SATA over PATA
Difference between SATA and PATA
Linux Hard Disk Names
Partition Definitions
Linux Drive Naming Scheme
Difference between hdc and sr0
Linux naming convention for disks
Correlate dev devices to hardware
What is PATA 1
What is PATA 2
What is SATA
What is Scuzzy
IDE vs SATA

Martin Nestorov