Srdnlen 2023 - Spwnzati

sardCastle

@pc98

Description

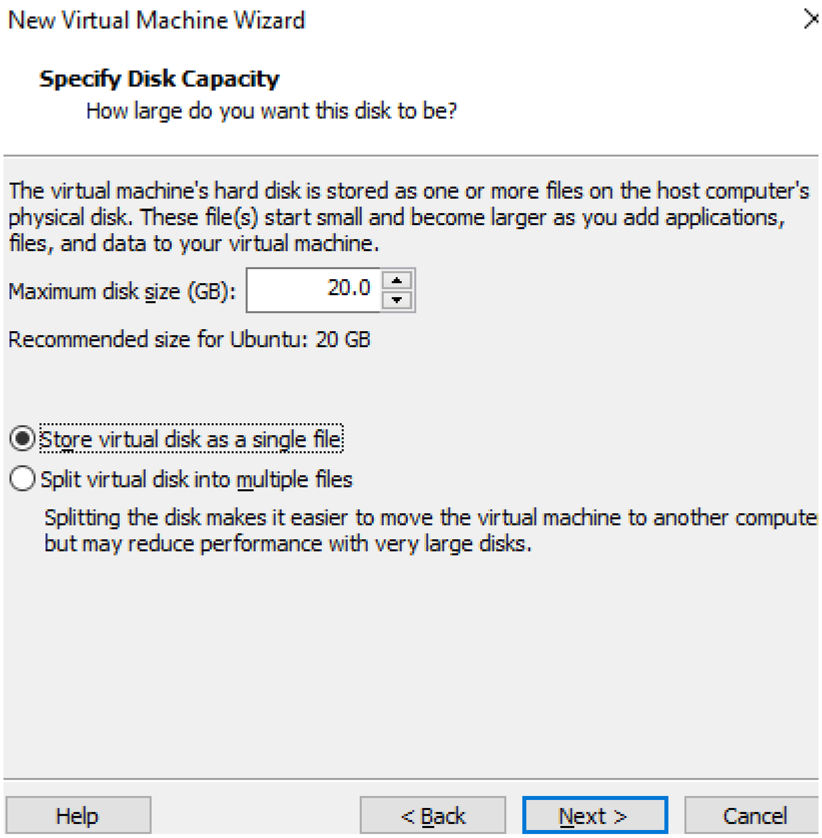
`I really want to build a sandcastle..`

`https://drive.google.com/file/d/17fnrZkRQb83qBgzO61SkpVbtn_tIk5lh/view?usp=sharing`

Solution

In the attachments we find `pc98.vmdk`, from this `website` we find out it's a `virtual machine disk`.

Not knowing the OS of the system we created a VM on VMware with Ubuntu selecting `Store virtual disk as a single file`.



New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 20.0

Recommended size for Ubuntu: 20 GB

● Store virtual disk as a single file

○ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another compute but may reduce performance with very large disks.

Then we replace the file `.vmdk` of this new VM with our `pc98.vmdk`. Booting it up we notice that the only user, `pc-98`, is protected by a password. After some `research` on the web discover that it is possible to change the password.

1. Enter recovery by pressing ESC at boot
2. Select Advance options for Ubuntu
3. Select the option with (recovey mode)
4. Select root to drop the root shell and press ENTER

Now we have root access to the machine, but we need write permission to ovverride the password, we can type `mount -rw -o remount /` to remount the filesystem with read and write permissions.

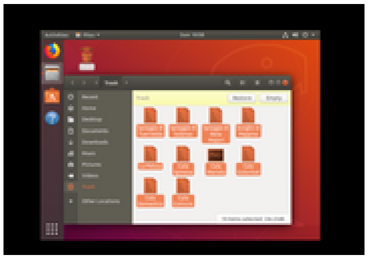
To change the password for the user `pc-98` we use `passwd`:

```
passwd pc-98
```

It will ask for a new UNIX password, we set it and type it again to confirm it.

Now that we changed the password we can reboot the VM and this time access with user: `pc-98` and password: `that one we set earlier`.

In the desktop we notice that the recycle bin is full, so we restore the files and then take them out from the virtual machine to analyze them.



The file names are from famous beaches in Sardinia, all the files weigh 4kb apart from one file that is 1kb, only one file has a preview and upon uploading it on hexed.it we can see that the `magic bytes` matches with .png file extension, we suppose that the files are scrambles chunks from an image and then we confirmit by analayzing the 1kb file and noticing that it ends with IEND that signal the end of a png file.

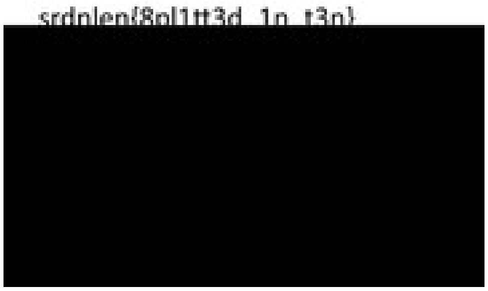
We wrote a python script to order the images:

```
import os

def read(file):
    with open(file,"rb") as f:
        a= f.read()
    return a

data=dict()

start=read("Cala Mariolu.png") # first part of the image
end=read("Cala Domestica") # last part of the image

files=os.listdir()
files.remove("order.py")
files.remove("Cala Mariolu.png")
files.remove("Cala Domestica")
files.remove("images")

for file in files:
    data[file]=read(file)
stream=start
for e in data.keys():
    with open("images/1"+e+".png","wb") as f:
        f.write(stream+data[e]+end)
```

From the output files we can see wich is the correct one because it shows part of the flag, we edit the script adding the next image which is the only one of the combination generated that adds something useful to the image.

```
import os

def read(file):
    with open(file,"rb") as f:
        a= f.read()
    return a

data=dict()

start=read("Cala Mariolu.png")
end=read("Cala Domestica")
spin=read("Cala Spinosa")
cotic=read("Cala Coticcio")
tuar=read("Spiaggia di Tuerredda")
pel=read("La Pelosa")

files=os.listdir()
files.remove("order.py")

files.remove("Cala Mariolu.png")
files.remove("Cala Domestica")
files.remove("Cala Spinosa")
files.remove("Spiaggia di Tuerredda")
files.remove("Cala Coticcio")
files.remove("La Pelosa")

files.remove("images")

for file in files:
    data[file]=read(file)
stream=start+spin+cotic+tuar+pel
for e in data.keys():
    with open("images/5"+e+".png","wb") as f:
        f.write(stream+data[e]+end)
```

Finally among the output files we see the image with the `flag`. We could alse have continued to complete the image but this was enough.



srdnlen{8pl1tt3d 1n t3n}

Flag

srdnlen{8pl1tt3d_1n_t3n}