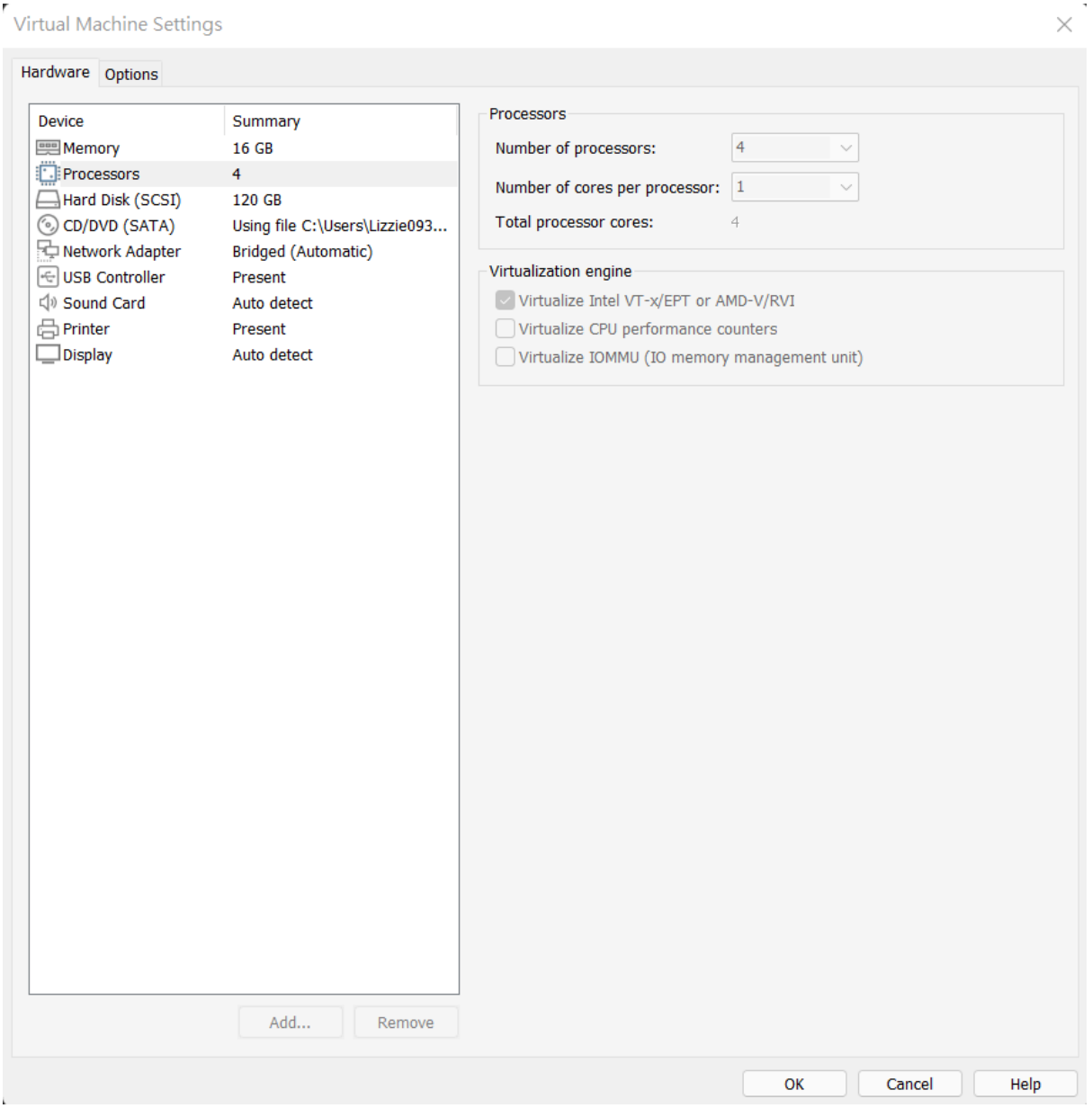
Cuckoo Sandbox Installation Steps

1. Install Vmware
2. Disable Hyper-V:https://www.makeuseof.com/windows-11-disable-hyper-v/
3. Download Ubuntu 18.04 iso

---------- 以下在Vmware上操作 ----------

4. Set up a Ubuntu 64 bit 18.04 virtual machine on Vmware, settings are as follow:



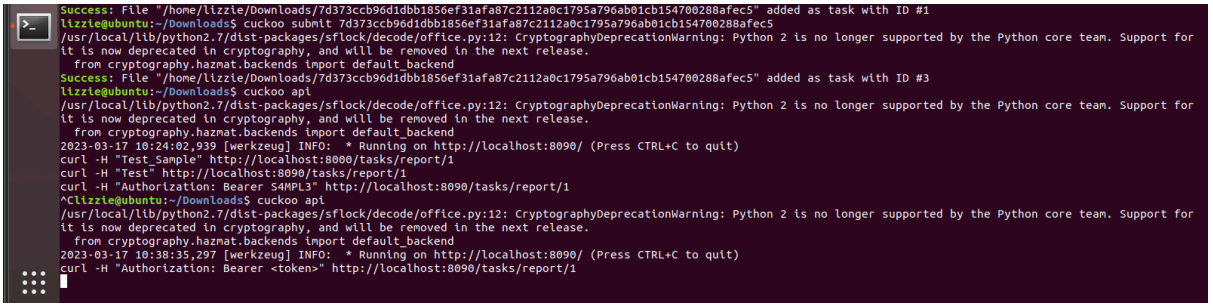
5. Create a shared file, and make it visible: https://communities.vmware.com/t5/VMware-Fusion-Discussions/shared-folders-are-not-visible-after-reboot/td-p/2913852
6. Download Agent.ova in shared file (在Host Computer上下載，透過shared file分享給Vmware) from:https://0x0c.cc/2020/03/19/Install-a-Cuckoo-Sandbox-in-12-steps/
7. Move Agent.ova to Downloads
8. **sudo apt update && sudo apt upgrade**

9. Install curl in terminal (sudo apt install curl or https://www.cyberciti.biz/faq/how-to-install-curl-command-on-a-ubuntu-linux/)
10. Install cuckoo in terminal: https://github.com/S4kur4/AutoDeployCuckoo
11. Connect to 127.0.0.1:8000
12. Download malware from VirusShare.com,
    excel:https://docs.google.com/spreadsheets/d/1EoZkq0ZtM0yBnwrtTtoENw-h1lwzTW1Eb1FtWm-WGD0/edit?usp=sharing (labeled data list)
    paper: https://arxiv.org/pdf/2111.15031v1.pdf
    github: https://github.com/boozallen/MOTIF

13. Install unzip: https://www.hostinger.com/tutorials/how-to-unzip-files-linux/
14. Unzip the malware, password: infected
15. Upload unzipped malware to cuckoo and get the report
16. Download json file of the report

Reference

1. https://www.runoob.com/python/os-listdir.html
2. https://www.runoob.com/python/python-func-enumerate.html
3. https://www.runoob.com/python/python-os-path.html
4. https://www.geeksforgeeks.org/how-to-use-glob-function-to-find-files-recursively-in-python/
5. https://www.runoob.com/python/att-string-format.html
6. https://note.nkmk.me/en/python-random-choice-sample-choices/
7. https://www.tensorflow.org/install/pip?hl=zh-tw#system-install



vim ~/.cuckoo/conf/cuckoo.conf

cuckoo submit path

cuckoo api
curl -o 1.json -H "Authorization: Bearer api_token" http://localhost:8090/tasks/report/1