Game of Active Directory (GOAD), setup the lab in linux machine

mahim-firoj.medium.com/game-of-active-directory-goad-setup-the-lab-in-linux-machine-5e682db516e3

Md. Mahim Bin Firoj 29 мая 2024 г.

Md. Mahim Bin Firoj

Image source:

Here in our esxi server, we have created a vm named GOAD-VM and giving resources of 32 GB ram, 8 core cpu’s and 500 GB hard disk (because if you take snapshots then space will be required more). On that vm we have installed ubuntu 22.04 desktop edition

operating system. If you have a old machine that is unused and the above mentioned resources are available, then you can still use that machine to create GOAD by installing ubuntu on that machine as the base os. Then rest procedure are same.

Now say you have installed ubuntu on esxi vm or your physical old machine. After that you need to use **sudo apt update && apt upgrade** command to update all the packages. We have done that and the ip of the ubuntu vm is i.e. 10.10.11.182

We have also installed the following:

```
sudo apt install -vm-tools-desktopsudo apt install -vm-tools
```

tldr; quick install

- You are on linux, you already got virtualbox, vagrant and docker installed on your host and you know what you are doing, just run :

```
./goad.sh -t check -l GOAD -p virtualbox -m docker
./goad.sh -t install -l GOAD -p virtualbox  -m docker
```

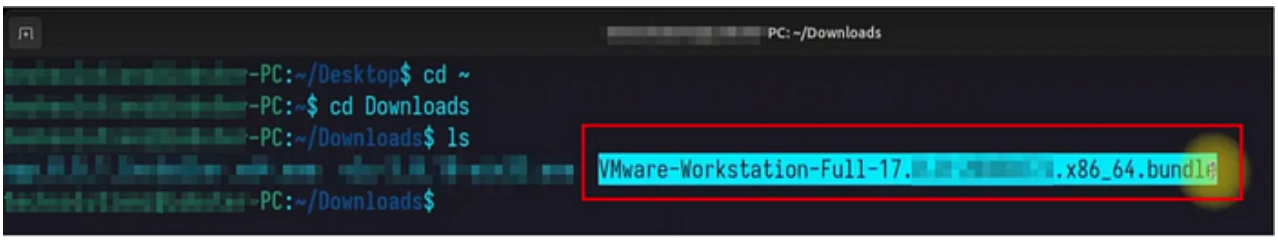
- Now you can grab a coffee ☕ it will take time :)

Now if you want to quick install the whole lab, then you first need to install virtual box, docker and vagrant on the system. Then you just need to clone the repo and utilize the **goad.sh** script. Grab the coffee because it will take time to comple the whole lab.

But we did not follow that approach. We plan to use vmware instead of other providers. So we installed vmware on the ubuntu vm. We also did not provision with docker, instead we used ansible locally.

1. First of all, you need to download the vmware for our ubuntu machine but this has now become tricky as vmware is acquired by Broadcom. Don't worry we will tell you how you can download this (Please reach out to me for this). After you download you will get a file like this ->

If you need this file then let me know please.



Now execute the following command one by one to install vmware on ubuntu.

```
sudo apt sudo apt install buildessential ysudo bash VMwareWrokstation-
x86_64.bundlesudo vmwaremodconfig
```

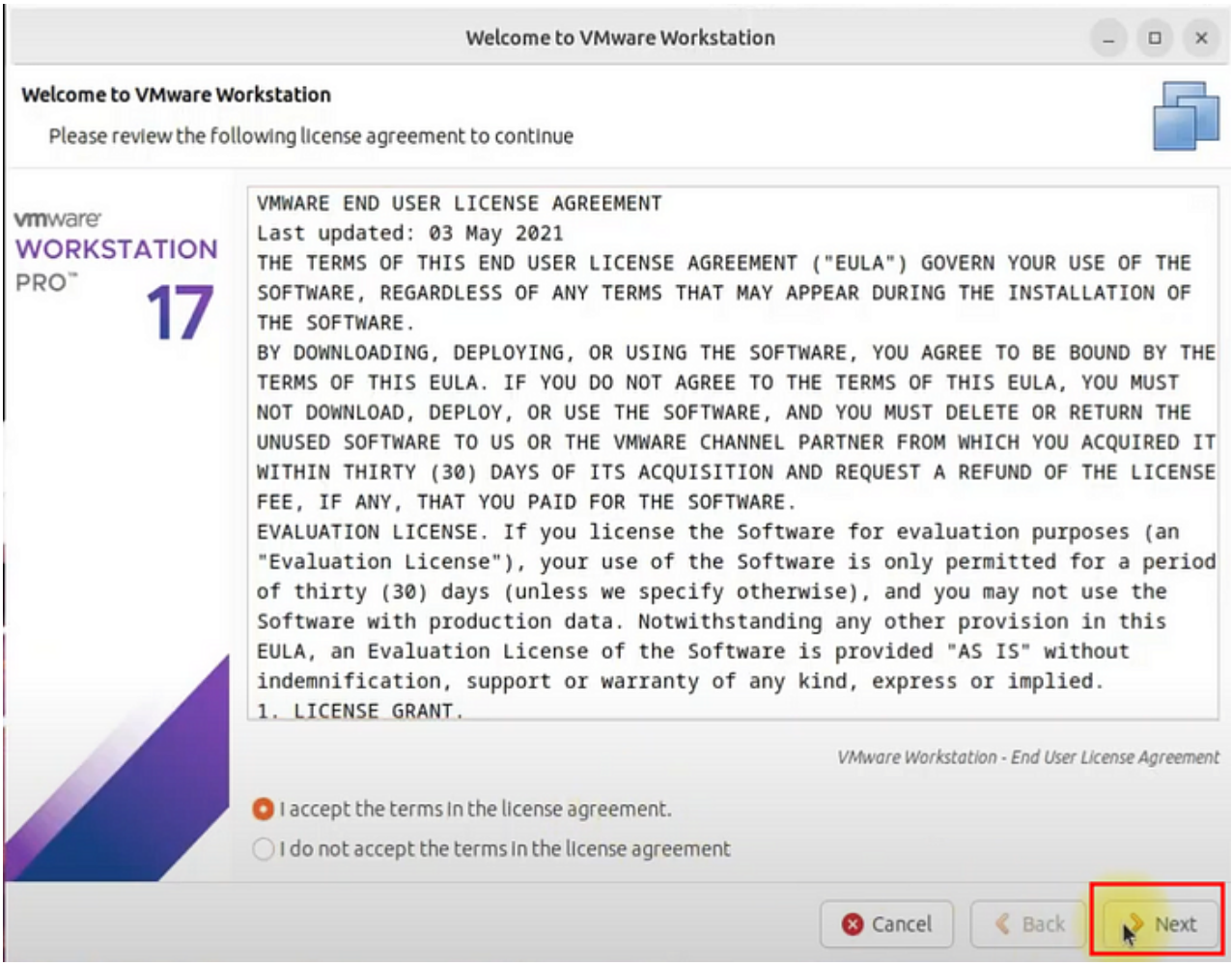
Now you will see that in your linux machine, vmware workstation pro has been installed. Open it.

You will see that its asking for gcc-12 or gcc-12–3.0 something like that. You need to install it using following command:

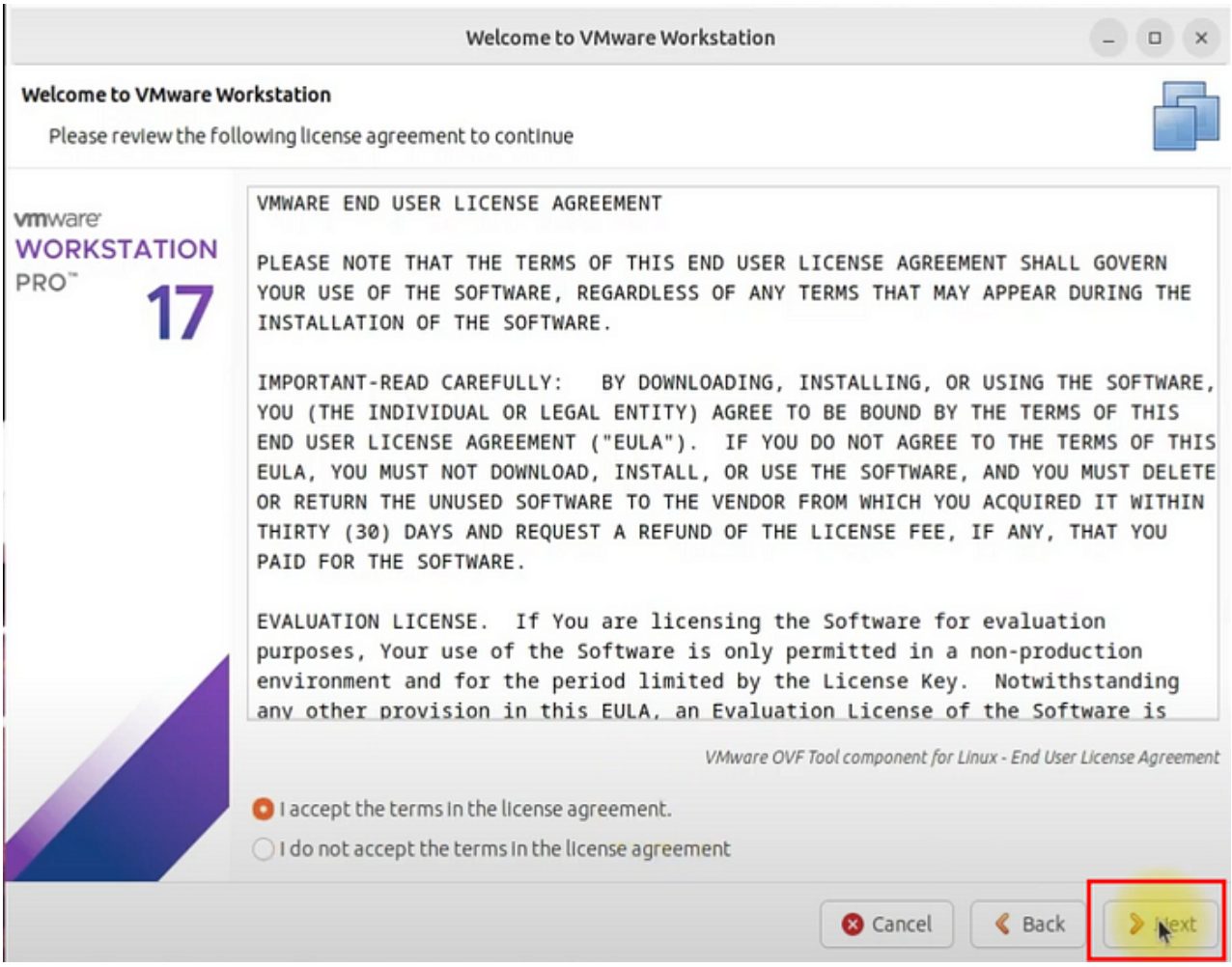
```
sudo apt install gcc- -y
```

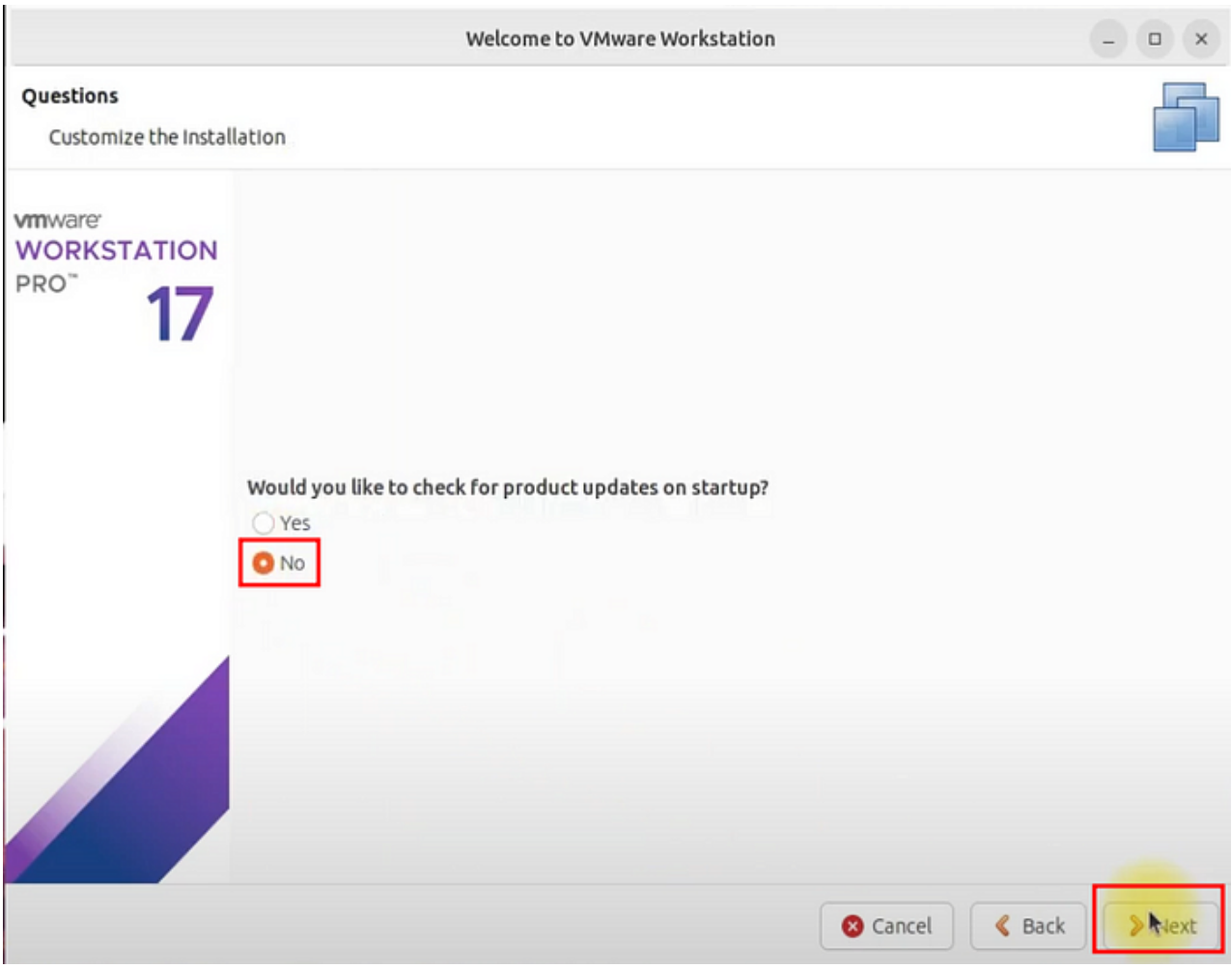
After the install is done, open vmware. Click on browse. The location where gcc file is present is opened by default. Point the gcc-12 and click ok.

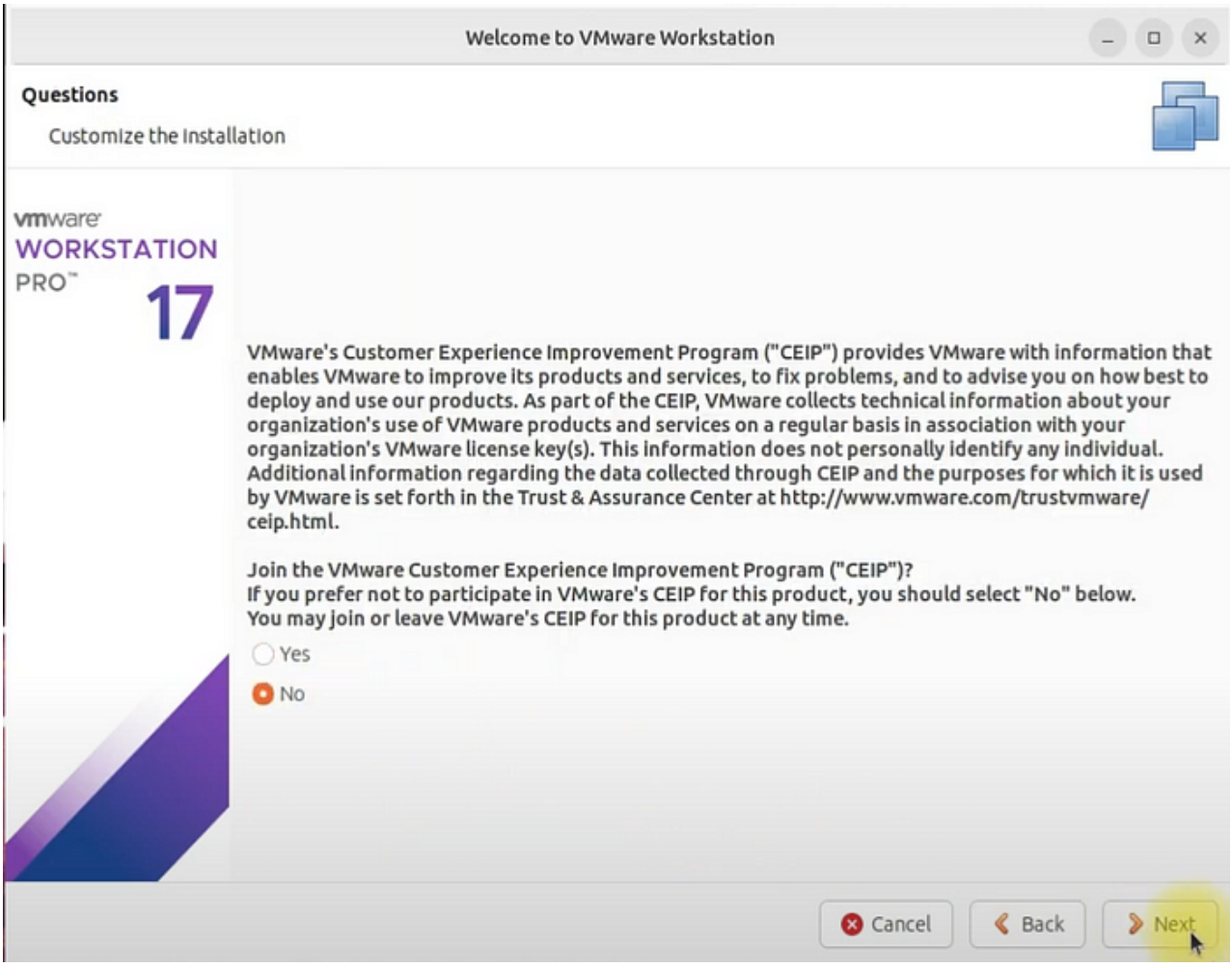
Now follow the on screen instruction (given below) and put the license. Please note, we need vmware pro license version for cloning and snapshot the GOAD vm's. Evaluation mode does not support these features.

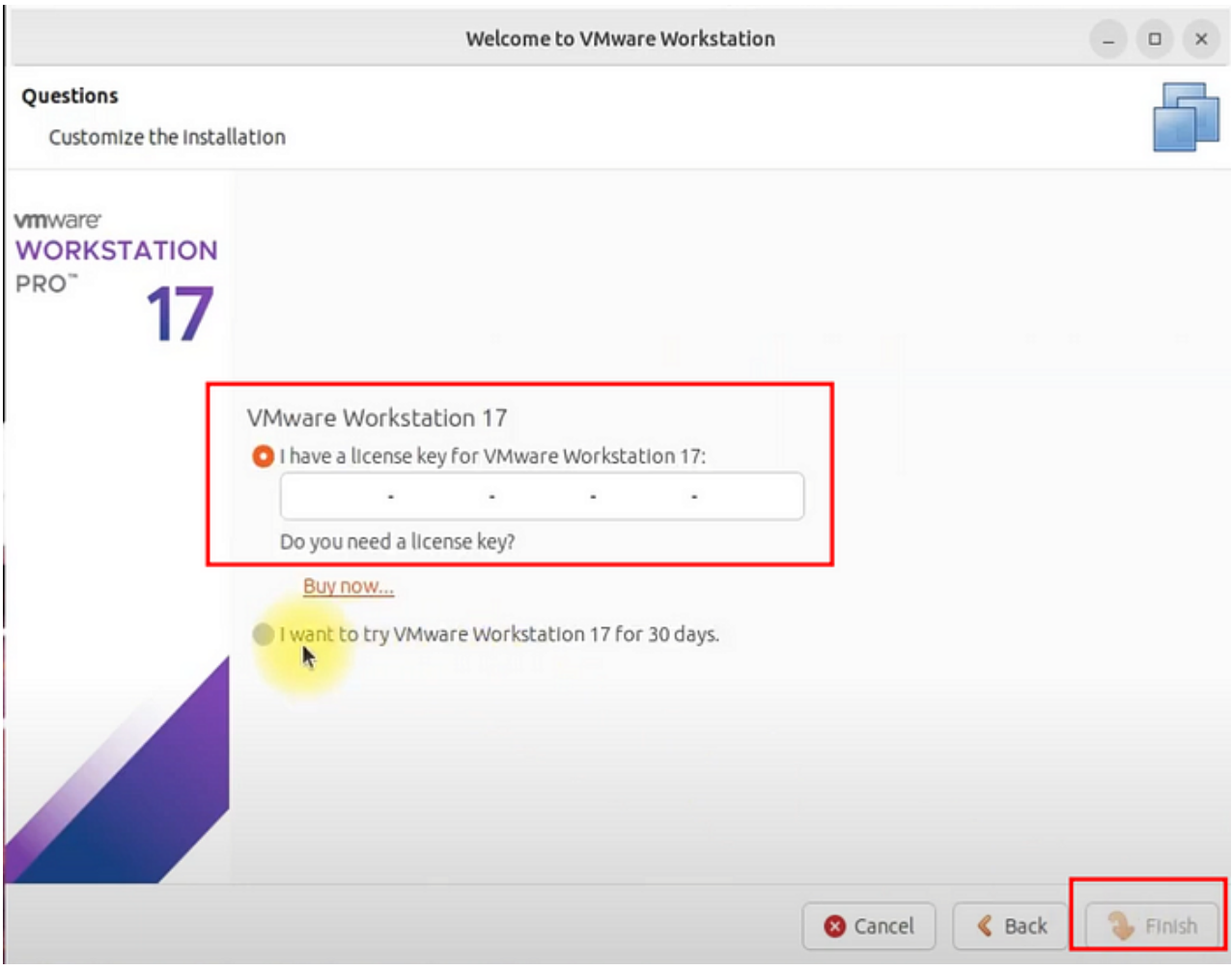


Now open the vmware application from your ubuntu system.


Welcome to VMware Workstation
Welcome to VMware Workstation
Please review the following license agreement to continue
vmware
WORKSTATION
PRO™
17
VMWARE END USER LICENSE AGREEMENT
PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.
IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.
EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is
VMware OVF Tool component for Linux - End User License Agreement
I accept the terms in the license agreement.
I do not accept the terms in the license agreement
Cancel
Back
Next


Welcome to VMware Workstation
Questions
Customize the Installation
vmware
WORKSTATION
PRO™
17
Would you like to check for product updates on startup?
Yes
No
Cancel
Back
Next


Welcome to VMware Workstation
Questions
Customize the Installation
vmware
WORKSTATION
PRO™
17
VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s). This information does not personally identify any individual. Additional information regarding the data collected through CEIP and the purposes for which it is used by VMware is set forth in the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.
Join the VMware Customer Experience Improvement Program ("CEIP")?
If you prefer not to participate in VMware's CEIP for this product, you should select "No" below.
You may join or leave VMware's CEIP for this product at any time.
Yes
No
Cancel
Back
Next


Welcome to VMware Workstation
Questions
Customize the Installation
vmware
WORKSTATION
PRO™
17
VMware Workstation 17
I have a license key for VMware Workstation 17:
Do you need a license key?
Buy now...
I want to try VMware Workstation 17 for 30 days.
Cancel
Back
Finish

Put the license key and click finish.

2. Now we need to install vmware utility vagrant driver.

Install | Vagrant | HashiCorp Developer

Explore Vagrant product documentation, tutorials, and examples.

developer.hashicorp.com

https://releases.hashicorp.com/vagrant-vmware-utility/1.0.22/vagrant-vmware-utility_1.0.22-1_amd64.deb

From this link you can download the **amd64.deb** package and install it by the below command. And we follow this step (not the alternative one).

```
sudo dpkg -i vagrant-vmware-utility_1.0.22-1_amd64.debor apt install ./vagrant-vmware-utility_1.0.22-1_amd64.deb
```

Or alternatively, you can install the package manually by following below commands which is mentioned on orange cyber defense's github page.

```
 /tmpwget https://releases.hashicorp.com/vagrant-vmware-utility/1.0.22/vagrant-vmware-utility_1.0.22_linux_amd64.zipsudo  -p /opt/vagrant-vmware-desktop/binsudo unzip -d /opt/vagrant-vmware-desktop/bin vagrant-vmware-utility_1.0.22_linux_amd64.zipsudo /opt/vagrant-vmware-desktop/bin/vagrant-vmware-utility certificate generatesudo /opt/vagrant-vmware-desktop/bin/vagrant-vmware-utility service install
```

Please note that you will also need to install the vmware-desktop plugin after the vagrant installation, so run the below command:

```
vagrant plugin install vagrant-vmware-desktop
```

3. Now we need to install the Vagrant. Run the below commands one by one.

```
wget -O- https://apt.releases.hashicorp.com/gpg | gpg --dearmor | sudo /usr/share/keyrings/hashicorp-archive-keyring.gpg  | sudo /etc/apt/sources.list.d/hashicorp.listsudo apt update && sudo apt install vagrant
```

On some recent versions (ubuntu 23.04), you should consider run also:

```
sudo apt install ruby-rubygemsgem install winrm winrm-fs winrm-elevated
```

But in ubuntu 22.04 I tried to install the above, but it failed. Then I tried below and got success.

```
vagrant plugin install winrmvagrant plugin install winrm-fsvagrant plugin install winrm-elevated
```

4. Now we will install ansible locally.

```
sudo apt install gitsudo git  https://github.com/Orange-Cyberdefense/GOAD.git
GOADsudo apt install python3-pippip3 --versionsudo apt install python3-venvpython3
-m venv venvGOAD ansible/ ~/venvGOAD/bin/activatepip install ansible-corepip
install pywinrmansible-galaxy install -r requirements.yml
```

5. You can check dependencies using the below command now. (No docker)

```
Desktop/GOAD/./goad.sh -t check -l GOAD -p vmware -m
```

If all ok, then you are good to go.

6. Now navigate to the following path to create all the vm's using **vagrant up** command.

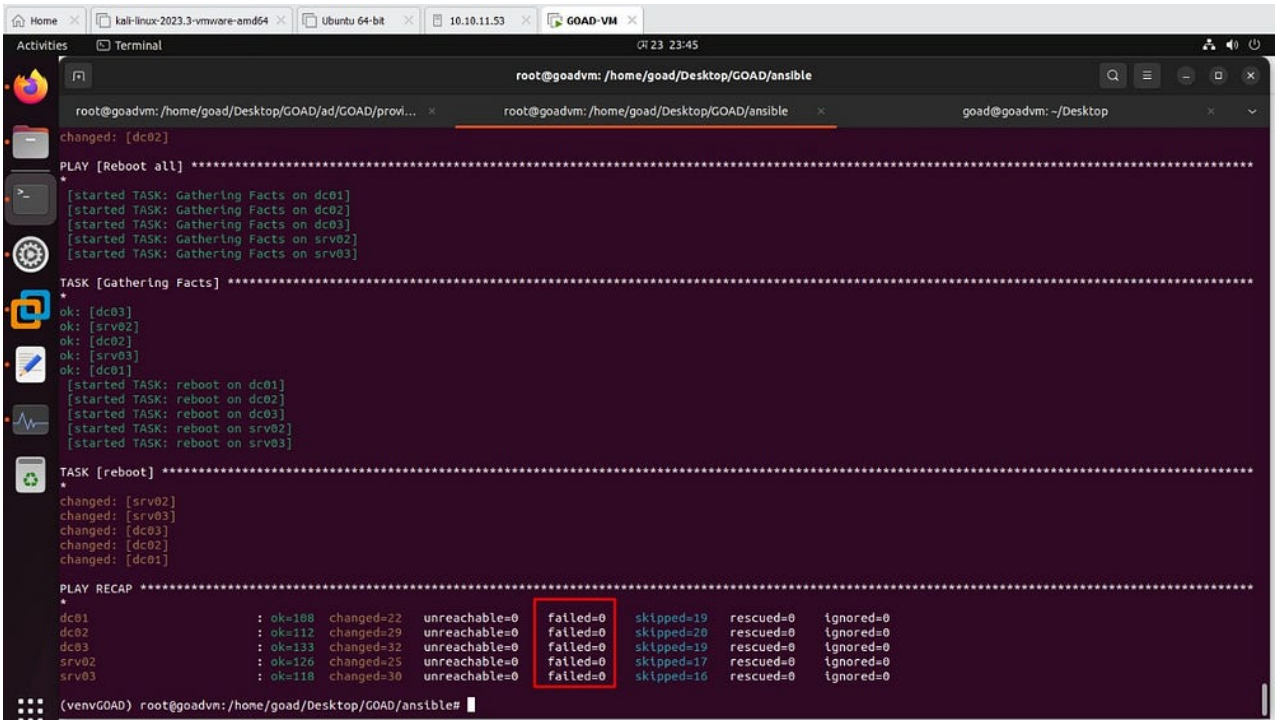
```
Desktop/GOAD/ad/GOAD/providers/vmwarevagrant up
```

Now allow some time. When all your vm's are up and running then you should go for ansible playbook to run.

7. Ansible playbook to run.

```
Desktop/GOAD/ansible/ansible-playbook -i ../ad/GOAD/data/inventory -i
../ad/GOAD/providers/vmware/inventory main.yml
```

In some writeup's, I saw that they recommend to run individual playbooks one by one. Please don't do that. Run directly the **main.yml** playbook file. Give some time. Once done you will see the following.



If you see out of 5, any 1 is failed, then re-run the **main.yml** playbook again. I encountered the similar thing. Then I re-run the playbook again. And guess what !!!! I got success the second time.

Happy AD Pentest :)

If you find the writeup useful, please subscribe below and share it to your social media. I would like to extend my gratidue to my colleague **Mohamed Alamin** for his wonderful co-operation with me regarding the RnD session. Thank you.

LinkedIn:

https://www.linkedin.com/in/md-mahimbin-firoj-7b8a5a113/

YouTube:

https://www.youtube.com/@mahimfiroj1802/videos