Mastering Enterprise Networks

Step-by-step labs to create, attack, and defend enterprize networks

Mastering Enterprise Networks

STEP-BY-STEP LABS TO CREATE, ATTACK AND DEFEND ENTERPRISE NETWORKS

MATHEW J. HEATH VAN HORN, PHD AND SLARTY BARDFARST

JACOB CHRISTENSEN; BERNARD CORREA; RAECHEL FERGUSON; SAWYER HANSEN; JUSTIN LA ZARE; JULIAN ROMANO; AND DANTE ROCCA

Embry-Riddle Aeronautical University
Prescott

<!–a=1–>

Contents

Introduction

MATHEW J. HEATH VAN HORN, PHD

Hello friend,

We have written this book to help anyone, even you, learn fundamental enterprise network principles through hands-on activities. The book starts by providing you with step-by-step instructions to create your own virtual environment on any modest PC or laptop running Windows. After setting up your own learning space, we will walk you through many real-world networking concepts that culminate with you building your own enterprise network. Once you are comfortable with creating computer networks, we will then show you how to attack your own network and then how to defend your network against those attacks.

The projects in this book are not advanced networking techniques. The projects are designed for anyone to learn more about computer networks. We found that many websites and helpful guides spoke to those who already knew much about computers and computer networks. This book is intended to remove the mystery of computer networks and put the fundamentals right into the hands of people like you. People who have a desire to learn but are unsure they can learn this stuff. Believe me, you can.

This book does not go deep into theory. You can learn the theory from any Wikipedia page or a textbook from the library. Theory abounds us, but what is missing are the fundamentals of putting the theory to use. The focus of this book is having you do the things that other authors talk about. You won't have to read pages of theory, analyze best practices, answer questions, or read case studies. After this introduction, you will be getting your hands dirty and start to make things happen. And you are going to be great at it!

I am Mathew J. Heath Van Horn. I am a military veteran, a church leader, a husband, and a father of five. I am also a kutte-wearing Harley rider and gratefully serve as a professor of cyber security. I'm no genius; I just work hard and learned through my many failures. I grew up in a farming town in rural Minnesota. I didn't want to be a farmer so I joined the Air Force where I spent the next 23 years learning everything I could. I then turned around and taught recent high school graduates the fundamentals of electronics repair, establishing voice and data communications, computer programming, and the theoretical principles of cyberspace. These fundamentals included building computer networks, attacking them as a hacker, and defending them.

Upon retiring as a Cyber Operations Officer, I taught underprivileged New York City college students for five years in upstate NY. Many of the students I encountered did not enroll in college to pursue a career. In fact, their number one answer to my new student poll about why they were attending college was "I have nothing else to do." When I asked why they wanted to learn cyber technologies, the common response was "I like to play games on my phone." Not exactly the highly motivated students desired by professors. However, I firmly believe that anyone can learn these concepts, and I will do anything I can to teach them.

These students opened my eyes that there are people who believe they 'can't' instead of believing they 'can'. Lecturing these students with theory was not going to make much progress in their success. So I flipped teaching on its head and focused on developing as many hands-on learning labs as possible. "Learn by doing" became my mantra. I taught students who initially couldn't write a term paper or even perform basic mathematical functions a wide variety of cyber skills. Microsoft Office was our starting point, and from there, I taught students how to

build and repair computers and use Windows and Linux operating systems. I then developed classes to teach them programming languages, wired and wireless networking, computer hacking, and defense. Students who first stepped into my class believing they couldn't do anything were now graduating from my classes and getting jobs earning $65,000-$90,000 annually. Oftentimes earning more than their parent's combined income!

I wish I could say every student was a success, but some students just held onto that defeatist attitude, and I couldn't break them of it. However, I can say that every student who put in the effort required by hands-on learning mastered the material and found great work opportunities. I teach my students how to 'Karate chop' a board on the first day of class. No student has failed to break the board. However, some students took 2 failures before they succeeded, and others took 30 failures before they did it. Learning involves a lot of trying and failure before you see success.

True failure involves only one factor: giving up trying.

You will fail in completing the labs in this book. However, you will try them again (sometimes again, again, and yet again...) and you will find what you did wrong, fix it, and get it to work. All of these labs were tested by networking novices. Our youngest tester was 12 years old and did nothing more on a computer than play Roblox. He started doing the labs because he wanted to see what everyone else was doing so he said, "I want to try!"

I recruited college students to help build these labs. Most of these students had vague notions of networking theory, but some had no idea when they started. My fellow professors asked why I wasn't using graduate students to help with this book. Remember, I have doing this for nearly 40 years. This means that even though I think I am explaining something, I skip over fundamental concepts the students don't have and the explanations fall flat. I call this 'speeding', but there is probably some fancy pedagogical term for my actions. I hate it when I speed and I encourage my learners to call me on it. Anyway, for this effort, I specifically chose students for their enthusiasm and their abilities were largely secondary.

The student's unique perspectives helped make these labs into what you see, and they deserve all the credit I can give them. Take note of the names of the writers and testers of each lab. These students are simply great. I hope you get to meet them someday.

Keep the following in mind as you read this book:

- This book does not focus on theory. As our younger testers pointed out, "We can Google anything we want, just help us do stuff!" However, we recognize that the labs in this book can be a mystery without the theory. So we recommend you pair this book with any Introduction to Networking website or textbook that caters to your learning style.
- We used many testers and the labs worked great. We used various desktops and laptops in our tests. However, GNS3 can be tricky depending on the hardware in the machine. If you are encountering problems, it could be a hardware problem, but that should be your last thought. When we first started building these labs, we formatted our hard drives often, but now it is a rare occurrence. Now major problems are usually because we tried something new and pushed the limits of GNS3 and issues were not due to lab complexity.
- We found that people with the least experience should start with a fresh install of Windows. This gave learners the best results in completing the labs.
- We do not use punctuation at the end of the lab steps. This is because punctuation could cause confusion among new learners. In these labs, we focus on command-line interface (CLI) typing. However, CLI commands rely on spaces, periods, and other symbols used by sentences. By removing the ending punctuation, clarity emerged and learners were more successful.
- RTFQ is an oft-used acronym that means "Read The 'Full' Question". It indicates that you probably missed something because you didn't read slowly and carefully. My kids have heard this so often that they apply it in their own lives. On my daughter's first day of high school, the teacher gave the class a

pretest similar to this one and my daughter was the only one who got it right. All because of RTFQ.

- Occasionally you will see notes in the labs. These were inserted because some lab testers had problems and others didn't or there was a snippet of theory that helps explains the "why" of the lab at that time.
- New learners found that 7-Zip worked the best in unzipping the files. Windows Zip worked sometimes, so we suggest you download and install 7-Zip for work on these labs.
- Other teachers wanted homework and grading recommendations for the labs. We made these inclusions, but people need to keep in mind that cyber is a 1 or 0 profession. I grade my student's work based on a binary grading scale. The student either got the lab to work or not. There is no such thing as being "almost", "mostly", or "kind of" pregnant. Networks are the same way, there is no such thing as "Computer A can nearly communicate with Computer B". They either communicate or not. Therefore, the deliverables and homework are written with this all-or-nothing idea.
- We used many screenshots to communicate the steps at the beginning of the book. We first embedded the screenshots in the text, but our testers said frequent figures slowed down what they were doing. So we moved most of them to a link that you can click on as you need them. As the labs progressed, we used fewer screenshots since much of the material had already been covered.
- Speaking of which, we generally do not repeat material. Since this is an e-book, the learner can have more than one lab open at a time to refer back to other labs as often as you need to.
- We want learners to learn a wide variety of skills. Therefore, we deliberately used different techniques to satisfy common tasks. This way learners gain topical networking experience and various tools and techniques in virtual and physical machines.
- This book is intended to be a living document. We are sure that both learners and teachers will be sending us feedback on things we missed or just general suggestions of material they think should be included. Also, cyber changes rapidly, and these labs will not stay static as written; they just can't. We welcome comments and suggestions. Furthermore, if anyone wants to submit a complete lab, we will evaluate its applicability and gladly incorporate it into the textbook and give the submitter full credit.

In conclusion, we used professional and novice inputs in building learning labs to reach the widest learner audience possible. We want people to enjoy learning networking principles by doing rather than reading. We hope you enjoy this textbook, and we know you can do it!

Sincerely,

Mathew J. Heath Van Horn, PhD

Jacob Christensen, Student

Julian Romano, Student

Raechel Ferguson, Student

Dante Rocca, Student

About Our Student Editors

MATHEW J. HEATH VAN HORN, PHD

Each chapter lists the students who contributed to that lab, but I would like to bring recognition to the student editors specifically. We started

Jake Christensen (2023-Present) – Jake is new to cybersecurity. He spent 2 years as an aerospace engineering major before making the change. Jake used his college experience to contribute to this textbook's overall pace by sharing his fellow students' observations as they learned these complex materials. He also spent many evenings in the cyber lab ensuring all of the labs worked in a teaching environment, not just on student personal PCs. Jake also became our self-taught subject matter expert in developing the Linux labs.

Dante Rocca (2023-Present) – Dante became a surprise editor. Once I gave them access to the textbook, they completed the first 16 chapters over a weekend! Dante is amazing and right now they pull double duty as the cleanup editor and the copy editor for Part II. They kept the rest of us on track and caught what we missed. They polished the formatting of the labs and led our efforts to make sure the printed version of this ebook looked sharp. They also volunteered for the herculean effort of completing the 2,800-item checklist for publishing.

Julian Romano (2023-Present) – Julian is our jack of all trades. Not only has he tested most of the labs in this book, but Julian uses his experience as a lead help desk technician to ensure the instructions are clear and easy to follow. Julian presented this effort to various industry and educational groups. He became the slide and poster master and easily answered expert and layman questions about this book. Furthermore, he is busy writing undergraduate grants so our students can focus on cyber-related activities instead of working other jobs.

Raechel Ferguson (2023-Present) – Raechel first approached me with an idea. She wanted to learn Windows Server and she felt that having an objective of developing labs would help her do that. Raechel's many extracurricular activities limit her time availability to this effort, but her Windows labs have proven invaluable. She will continue to develop more as she has time. Raechel partners with Julian in presenting our textbook writing effort and assists in preparing the grant.

Kyle Wheaton (2024) – He dominated in his enthusiasm for this project. He became involved when I used this book in class and he had so many great ideas. We brought him on board to turn those ideas into reality. His contributions resulted in making good learning activities into ones that are fun and exciting. A couple of labs would not exist past the idea stage without Kyle putting in the effort.

Justin La Zare (2024) – Is our resident Capture the Flag Expert. He has traveled the world to provide aeronautical-based CTF events to industry and academia. He had a break from his busy schedule and volunteered his time and expertise to develop Part IV of this book. He turned brainstormed ideas into tangible learning activities.

Sincerely,

Dr. HVH

PART I

SETTING UP THE GNS3 ENVIRONMENT

CHAPTER 1

Introduction to Part I

MATHEW J. HEATH VAN HORN, PHD

JUST A QUICK NOTE BEFORE THE LABS BEGIN

The labs in this section are designed for users to set up their own devices so they can complete the learning labs. The labs in this section are not designed to be homework assignments. We didn't list means of evidence to show completion of the lab or suggested extensions of the lab as we do in the later parts of the book.

These setup labs have been tested on various devices and by experts and novices alike. They were tested a lot. Most of the testers had to start from scratch several times. This is both a good and bad thing. Good: because the steps are practiced, the links are tried, the screenshots are accurate, and the processes are tested. Bad: because many of the testers had wiped and reinstalled so many times that they memorized the processes. Memorization means that their brain would fill in gaps in the instructions. A phenomenon I call 'speeding'. If you encounter a lab where speeding occurred, you should be pretty safe in just accepting the default settings and hitting the 'Next' button.

We also used this section to build the student learning lab environment for Embry-Riddle Aeronautical University – Prescott. After this, Deep Freeze was employed so that if a student screwed things up, they could return to start without having to reinstall, rebuild, or reconfigure GNS3 and the associated VMs. This worked out well for our lab environment.

Furthermore, the labs are a mixed bag when using Apple devices. We didn't have Apple devices to test the labs on, but some students got them working on their devices and some students were unable. We tested on various instances of Windows and Linux desktops and laptops.

Finally, here is a list of the software versions that were used for these labs:

- GNS3 – ver 2.2.46 (Note: the GNS3 and GNS3 VM versions must be the same)
- GNS3VM – ver 2.2.46
- MikroTik Cloud Hosted Router – ver 7.11.2
- Windows 11 evaluation
- Windows Server 2019 evaluation
- TinyCore – ver 6.6.8
- Ubuntu – ver 24.04
- Ubuntu Server – ver 24.04

- Kali – ver 2024.1 Rolling

Sincerely,
Mathew J. Heath Van Horn, PhD

CHAPTER 2

Setting Up a GNS3 Environment

MATHEW J. HEATH VAN HORN, PHD

I've been teaching the learning of networking principles for many years. In my experience, one of the biggest obstacles to learning networks and associated applications is the lack of a lab for learners to play. Graphical Network Simulator 3 (GNS3) solves many of those problems. GNS3 uses few hardware resources and can emulate complex networks using real images. Students no longer require access to a dedicated lab or to spend money on cloud architectures. GNS3 can be installed and used on most laptops on the market. A better processor and more RAM on the host machine will improve the GNS3 experience, but this is true with every application.

LEARNING OBJECTIVES

- Create a working GNS3 Learning Environment on a PC or laptop

PREREQUISITES

- Install Oracle VirtualBox

DELIVERABLES

- None – This is for student needs

RESOURCES

- GNS3 Documentation, https://docs.gns3.com/docs/

CONTRIBUTORS AND TESTERS

Testers:

- Quinton D. Heath Van Horn, 7th Grade
- David Reese, Mathematics Student, SUNY Brockport
- Cody Shinkyu Park, Honeywell Software Engineer, ERAU-Prescott Alumni
- Salvador Morales, Safety Management System Analyst, ERAU-Prescott Alumni

- Evan Paddock, Cybersecurity Student, ERAU-Prescott
- Dante Rocca, Cybersecurity Student, ERAU-Prescott
- Sawyer Hansen, Cybersecurity Student, ERAU-Prescott
- Bernard Correa, Cybersecurity Student, ERAU-Prescott
- Justin La Zare, Cybersecurity Professional, ERAU-Prescott

Phase I – Install GNS3 Environment

There are two parts to GNS3: the GNS3 Working Environment and the GNS3 Virtual Machine (VM). This section covers the installation of the GNS3 environment.

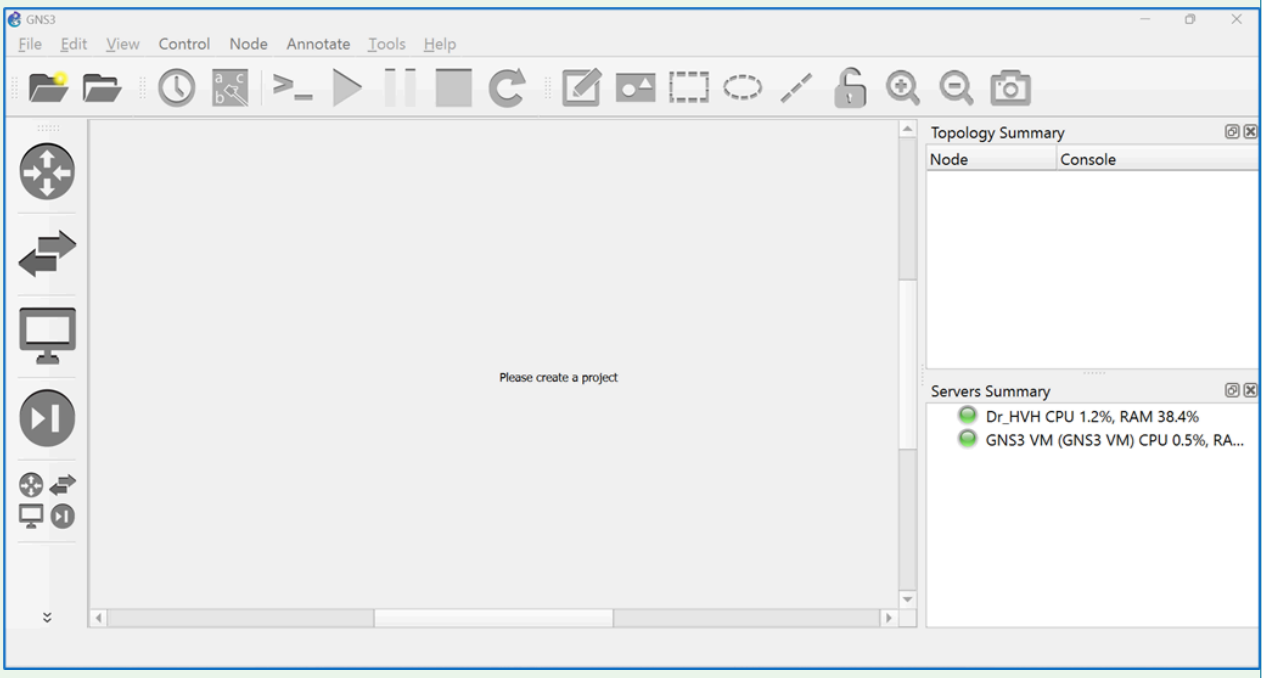


Figure 14 – GNS3 Workspace

1. Navigate to GNS3 at https://www.gns3.com/
2. Click on the ***Free Download*** button
3. Select Windows, Mac, or Linux as appropriate, and then ***Download***
4. Create your GNS3 Community Account as prompted, login, and then return to the download page

> **NOTE:** No one has reported spam from this registration.

5. Run the installer you downloaded and accept the default options. If prompted:

- Permit uBridge to run as root to capture packets
- Do not accept the free offers
- Do **NOT** start GNS automatically! Doing so can distract new learners due to the errors that will pop up

Phase II – Install the GNS3 VM (Virtual Machine)

This is where you will install the GNS3 VM. Remember, the GNS3 Working Environment and the GNS3 VM **must be** the same version.

1. Navigate to the GNS3 VM download page at https://www.gns3.com/software/download-vm
2. Select the image for ***VirtualBox***
3. Extract (unzip) the .zip file

NOTE: You may get 2 errors while unzipping the file and it will show 99% completion. This happens on occasion and does not affect the extracted file.

4. Download and launch https://www.virtualbox.org/wiki/Downloads
5. Select ***File*** → ***Import Appliance*** → ***Import*** (Figure 1) and navigate to the .ova file ("GNS3 VM.ova") that you just downloaded and unzipped. In this example, our .ova file is named "GNS3 VM.ova"(Figure 2)
6. Click ***Next*** (Figure 3)
7. Click ***Finish*** to accept the default appliance settings (Figure 4)
8. Adjust the network settings of the GNS3 VM by selecting the VM and then selecting settings (Figure 5)
9. In the network settings, under Network Adapter 1, select the name of the host-only adapter drop-down arrow. **YES,** even if the right name is already in the box. Just do it, and click ***OK***. If you don't do this, you will get a network error when you start the virtual machine (Figure 6)

NOTE: If no Host-only adapter is available, your VirtualBox version may need to be updated or reinstalled. If the VM still will not launch properly, then open Device Manager -> Network adapaters -> Virtualbox Host-Only Ethernet Adapter -> Disable Device. Re-enable the device again and restart VirtualBox.

10. Finally, start the GNS3 VM you installed to ensure it runs properly. This is a very lightweight version

of Linux (Figure 7)

11. Stop the GNS3 VM

Phase III – Configure GNS3

Now we are going to configure the GNS3 working environment for first-time use. You may encounter many errors when it first starts. This is normal because the GNS3 default settings use VMWare, and we are using VirtualBox. We tried using the free version of VMWare, and it does not have the features installed to be used with GNS3. We are trying to keep things free for learners to learn and not make them spend money.

Also, if you mess up the configuration, you can always re-run the setup wizard. On the GNS3 toolbar, click ***Help*** –> ***Setup*** Wizard.

1. Launch GNS3

NOTE: Sometimes VPNs will interfere with GNS3 working properly. It is recommended that they be disabled before launching GNS3.

NOTE: You may see the prompt "uBridge requires root permissions to interact with network interfaces." Say ***YES***. This allows you to connect GNS3 with the real network if desired.

NOTE: Sometimes GNS3 asks you to name a new project. If so, just pick any name and click ***OK***.

2. Next, choose how to run your GNS3 network simulations by selecting ***Run appliances in a virtual machine*** (Figure 8)

3. Accept the defaults for the Local Server Configuration and click ***Next*** (Figure 9)

4. You should get a successful message. Click ***Next*** (Figure 10)

5. The GNS3 default setting is to use VMWare by default so you will get an error. Select ***OK*** and choose ***VirtualBox*** (Figure 11)

6. When you change the radio button, the GNS3 VM you imported and started in VirtualBox earlier should auto-populate. Use the default settings and click ***Next*** (Figure 12)

7. Then select ***Finish*** (Figure 13)

8. You should have a screen like the one in Figure 14. The windows are adjustable, but the window to take note of is the "Servers Summary". You should see your bare metal machine (In Figure 14 it is Dr. HVH) and the GNS3 VM both show green lights and details of how many resources are being used. If the

server indicator light is still grey, power off the GNS3 VM and restart the GNS3 Working Environment

9. When you start GNS3 it can take a minute or two while the GNS3 VM launches. The indicator will remain grey until it is fully running

Phase IV Final note – Disabling KVM

Depending on the hardware of your bare-metal machine, you may get an error stating that KVM acceleration cannot be used. Simply turn off KVM support in the gns3_server.conf by adding enable_kvm = false to the [Qemu] section. Follow the steps below.

9.1. Open the GNS3 VM (Figure 15)

9.2. Use the cursor keys to navigate to configure

9.3. Add the following line to the bottom (Figure 16): [Qemu] enable_kvm = false

9.4. Press <*ctrl*> *O* to write out the file (e.g. save the file)

9.5. Accept the path by pressing <*enter*>

9.6. Press <*ctrl*> *X* to exit

9.7. Restart the GNS3 VM

End of Lab

List of Figures for Printing Purposes

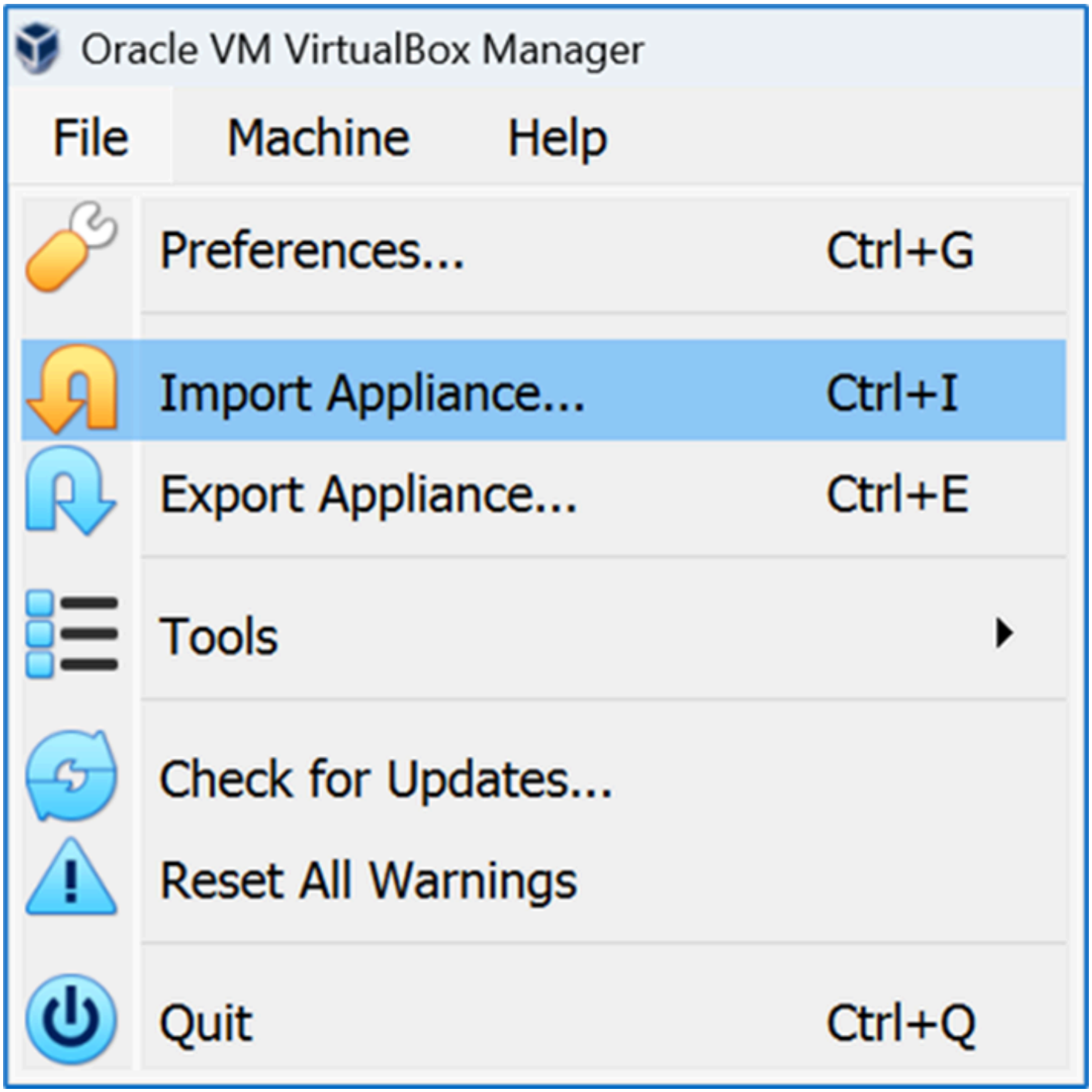


Figure 1 – Import appliance

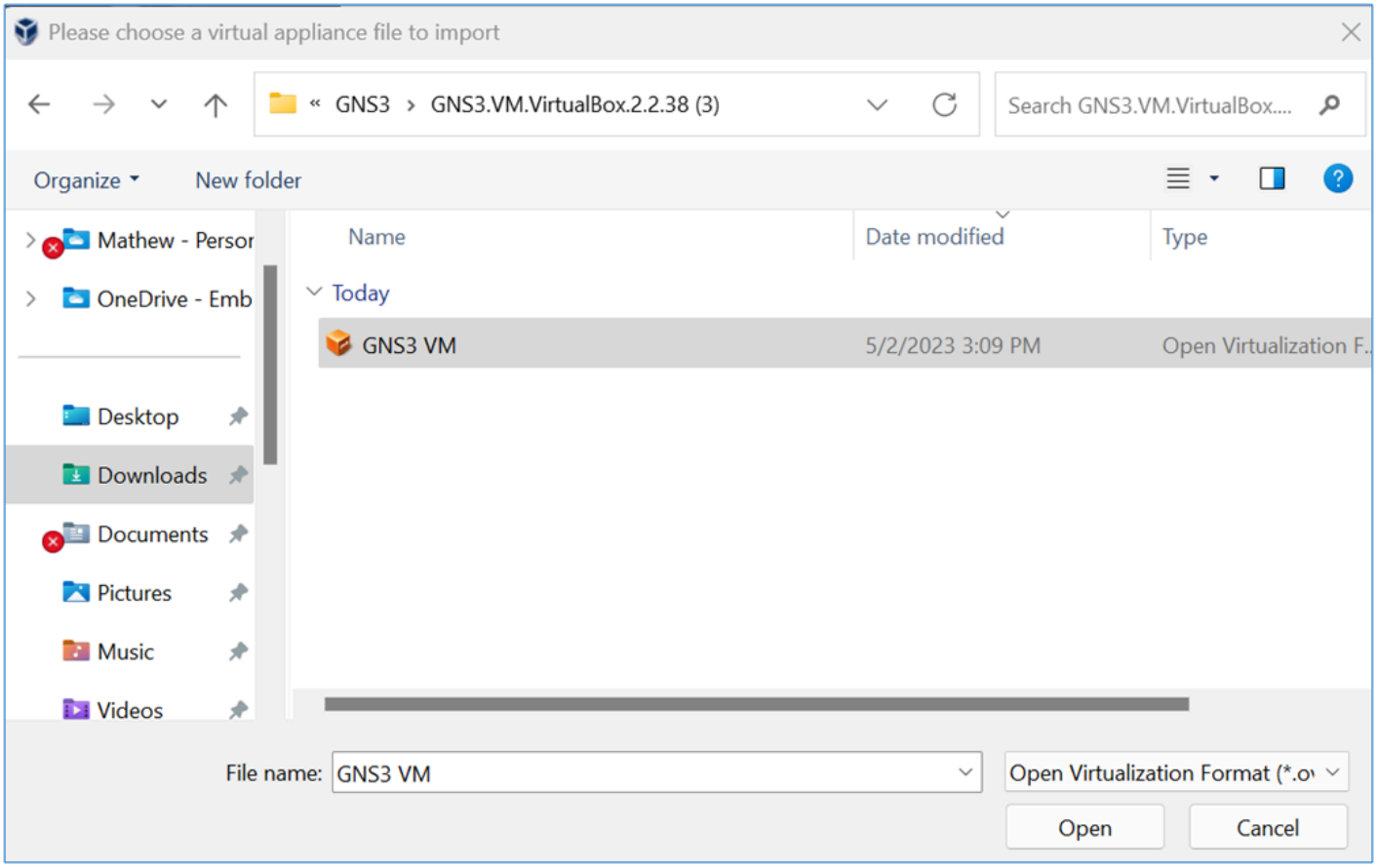


Figure 2 – Importing GNS3 VM

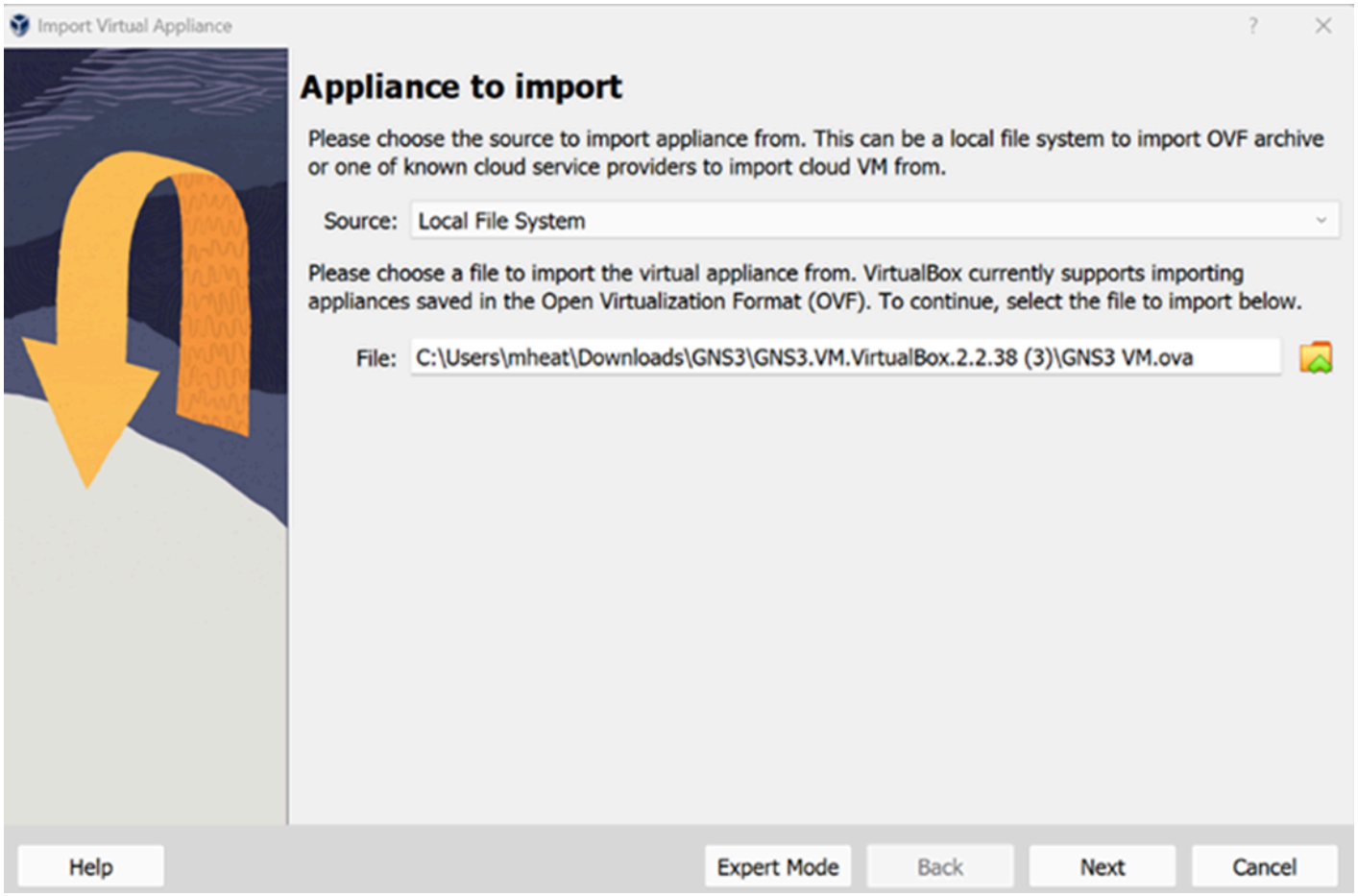


Figure 3 – Importing an appliance

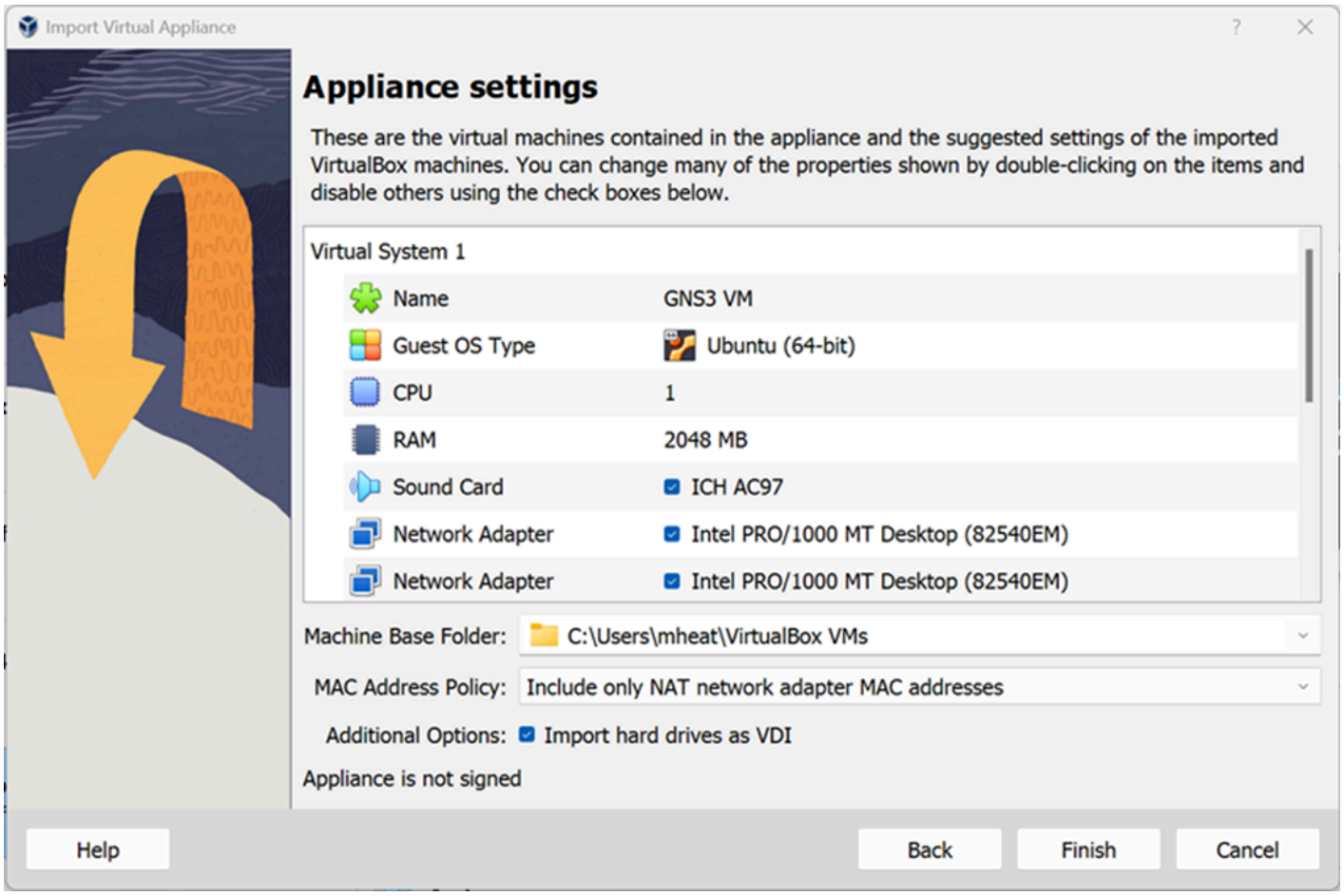


Figure 4 – Appliance settings in VirtualBox

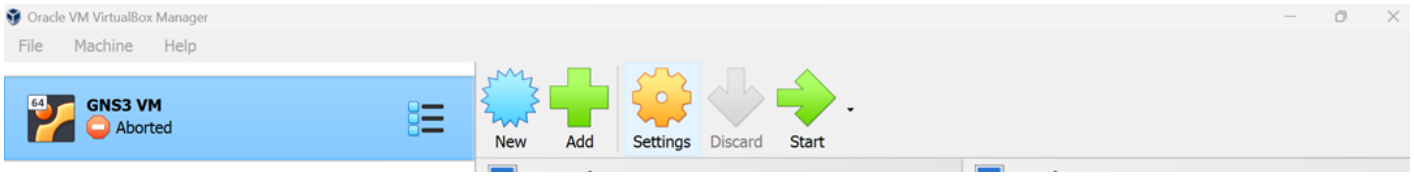


Figure 5 – Clicking on settings in VirtualBox

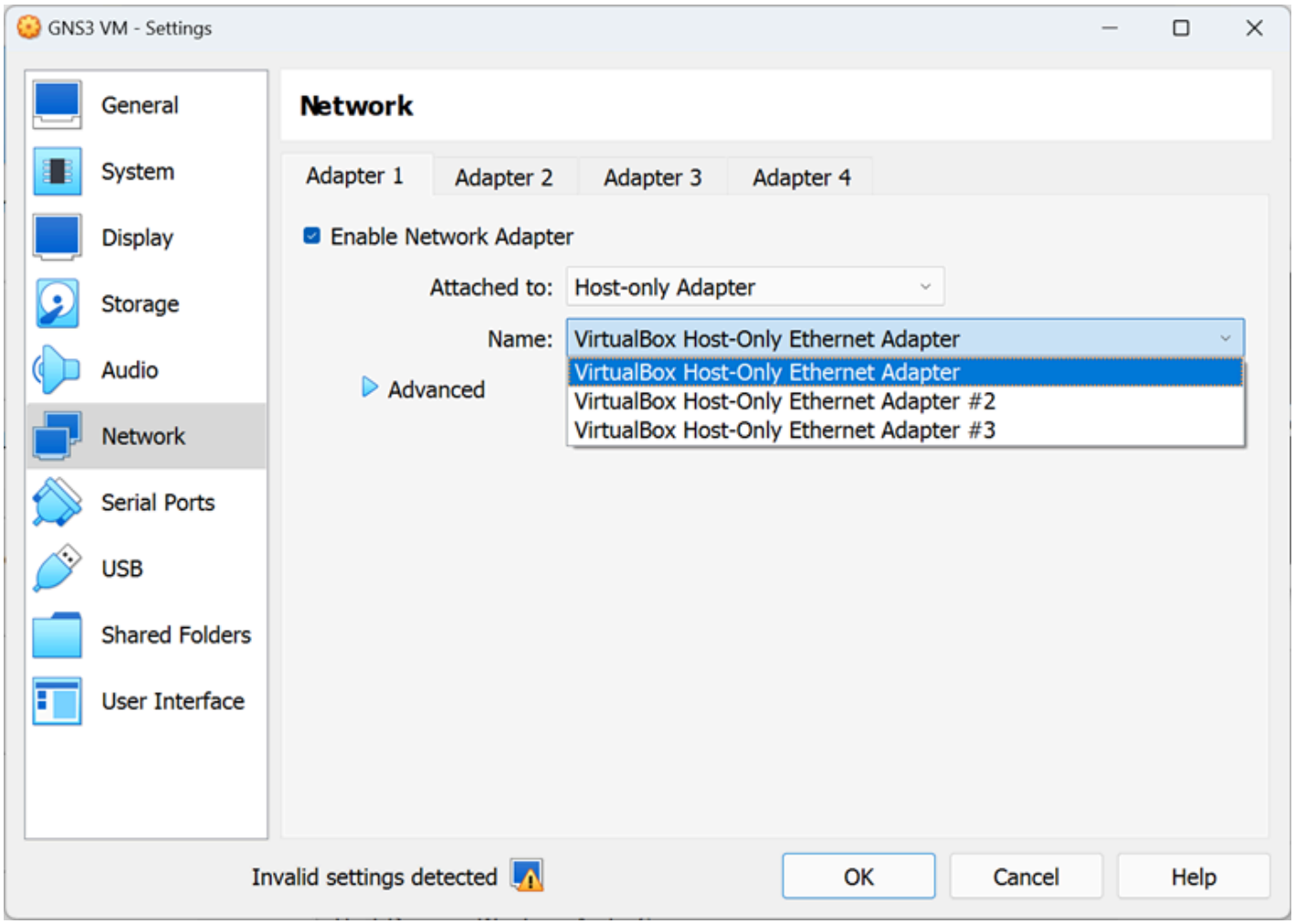


Figure 6 – Selecting the network adapter in VirtualBox

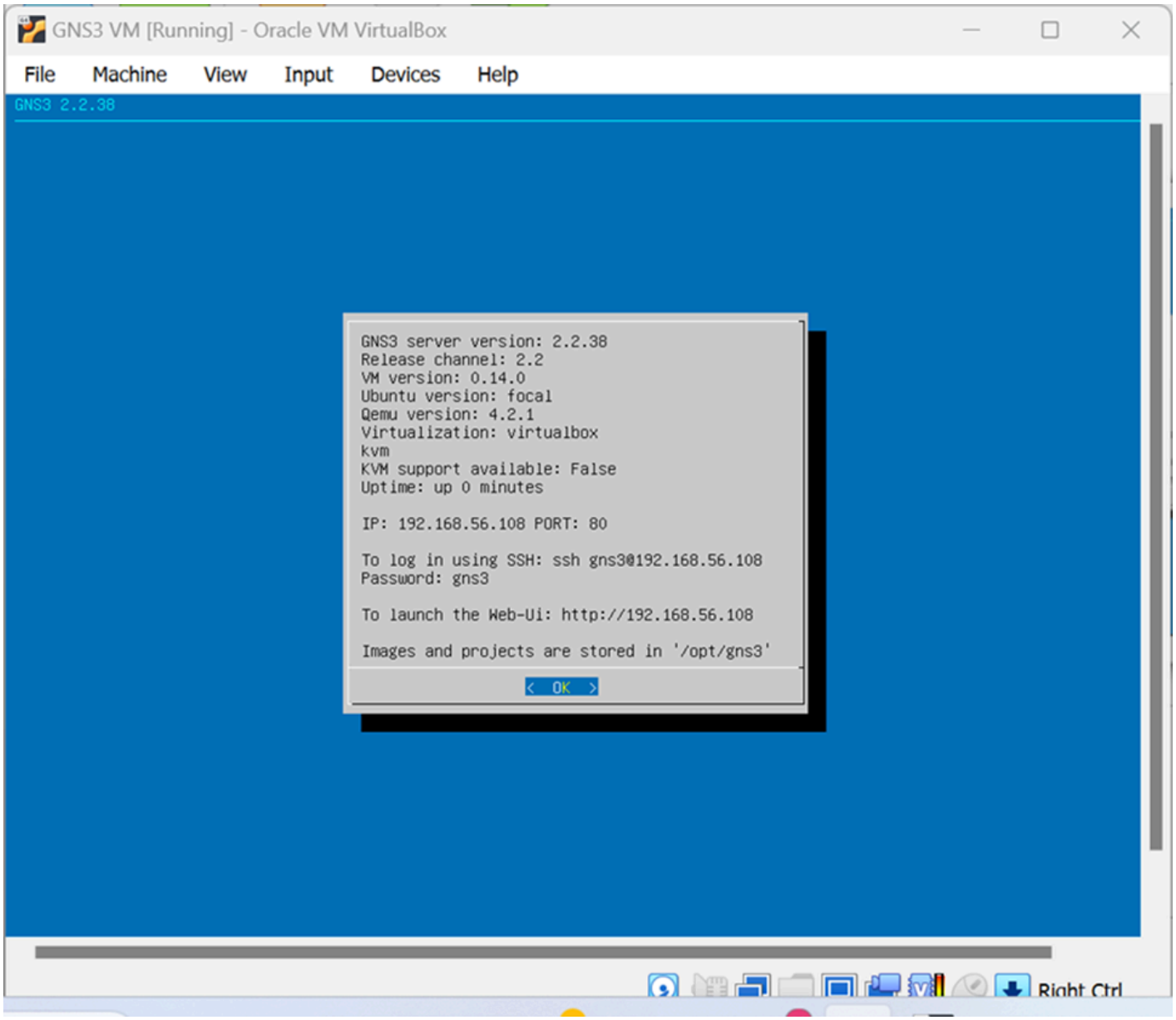


Figure 7 – GNS3 VM settings

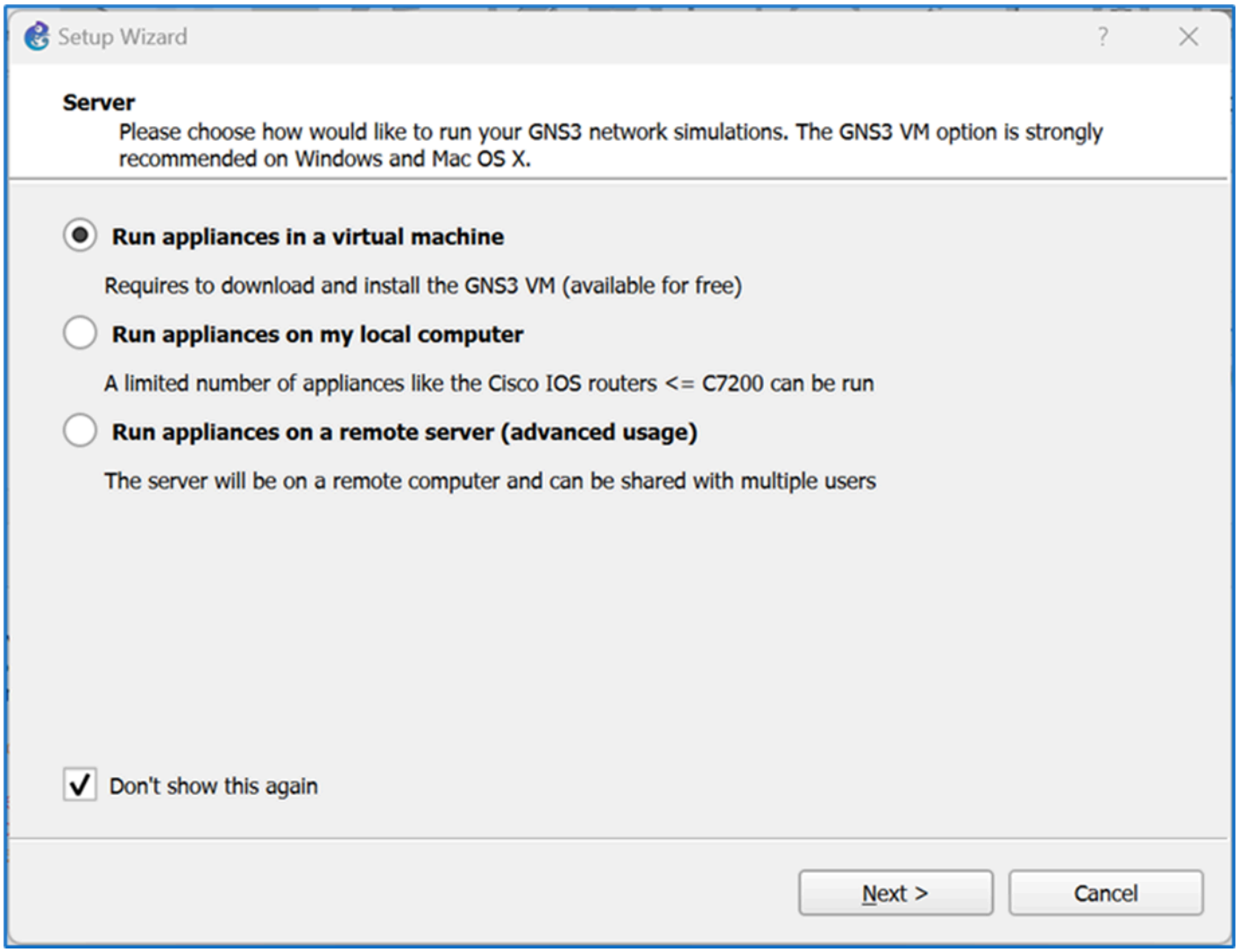


Figure 8 – GNS3 working environment setup wizard

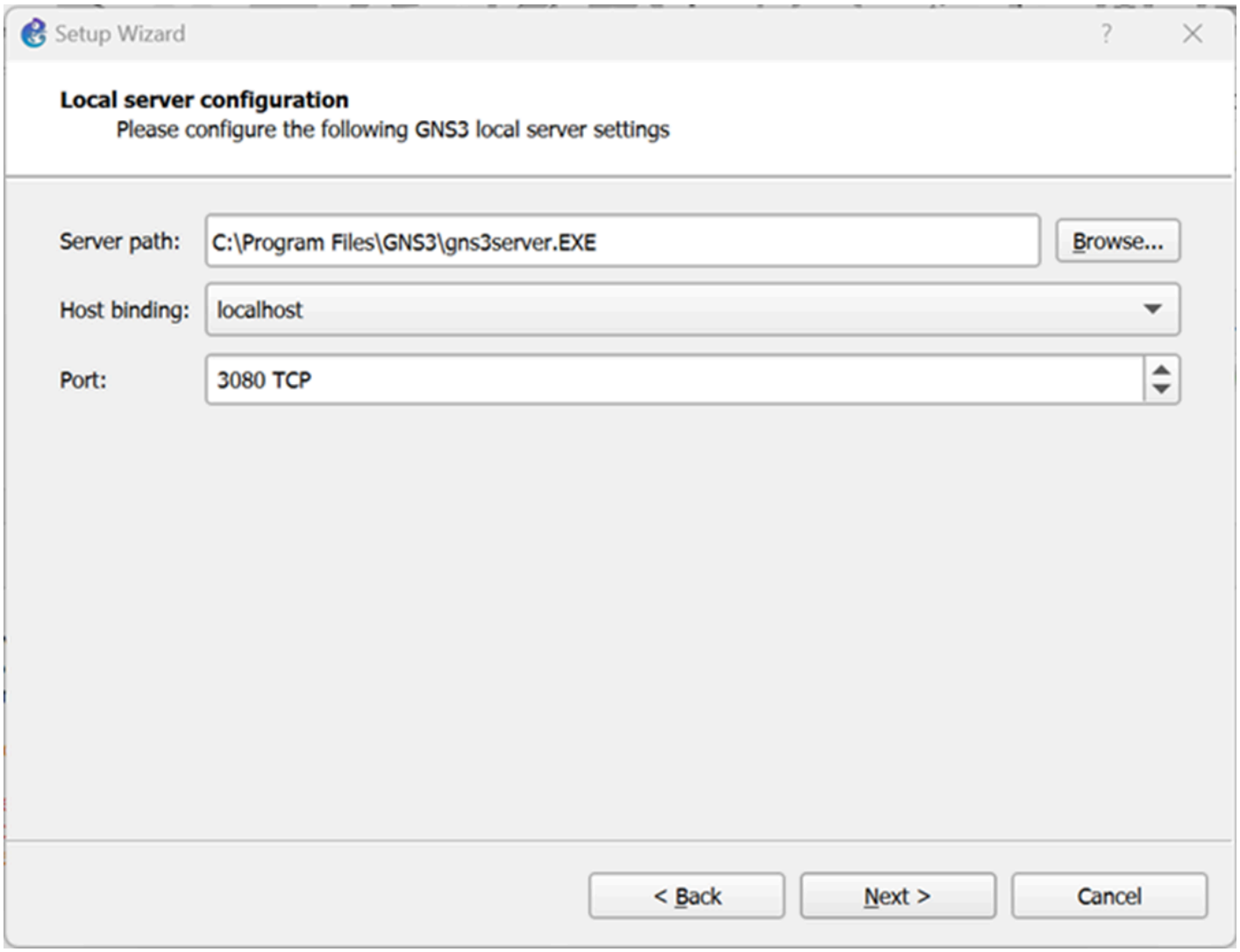


Figure 9 – GNS3 Setup Wizard – Local Server Configuration

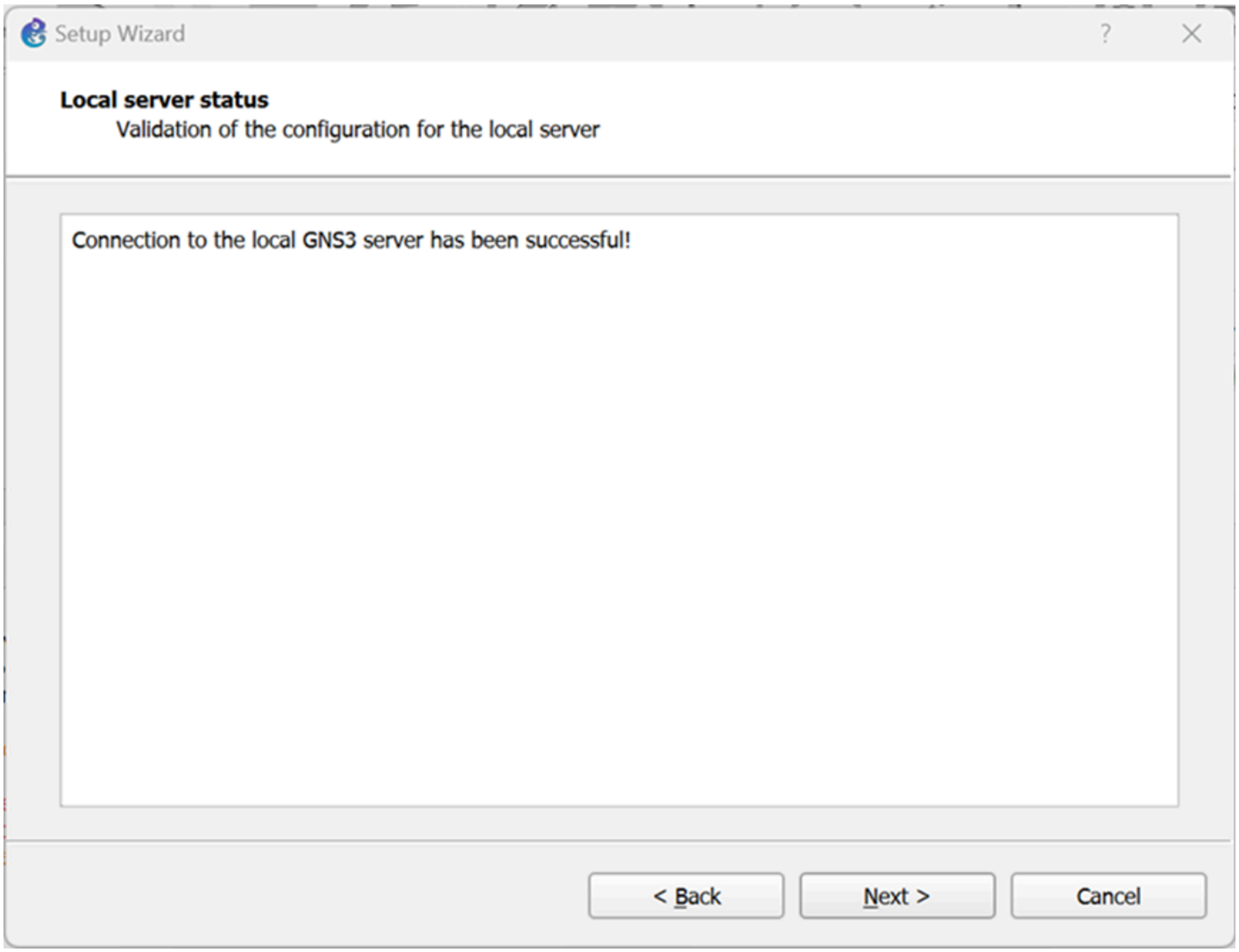


Figure 10 – GNS3 Setup Wizard – Local Server Status

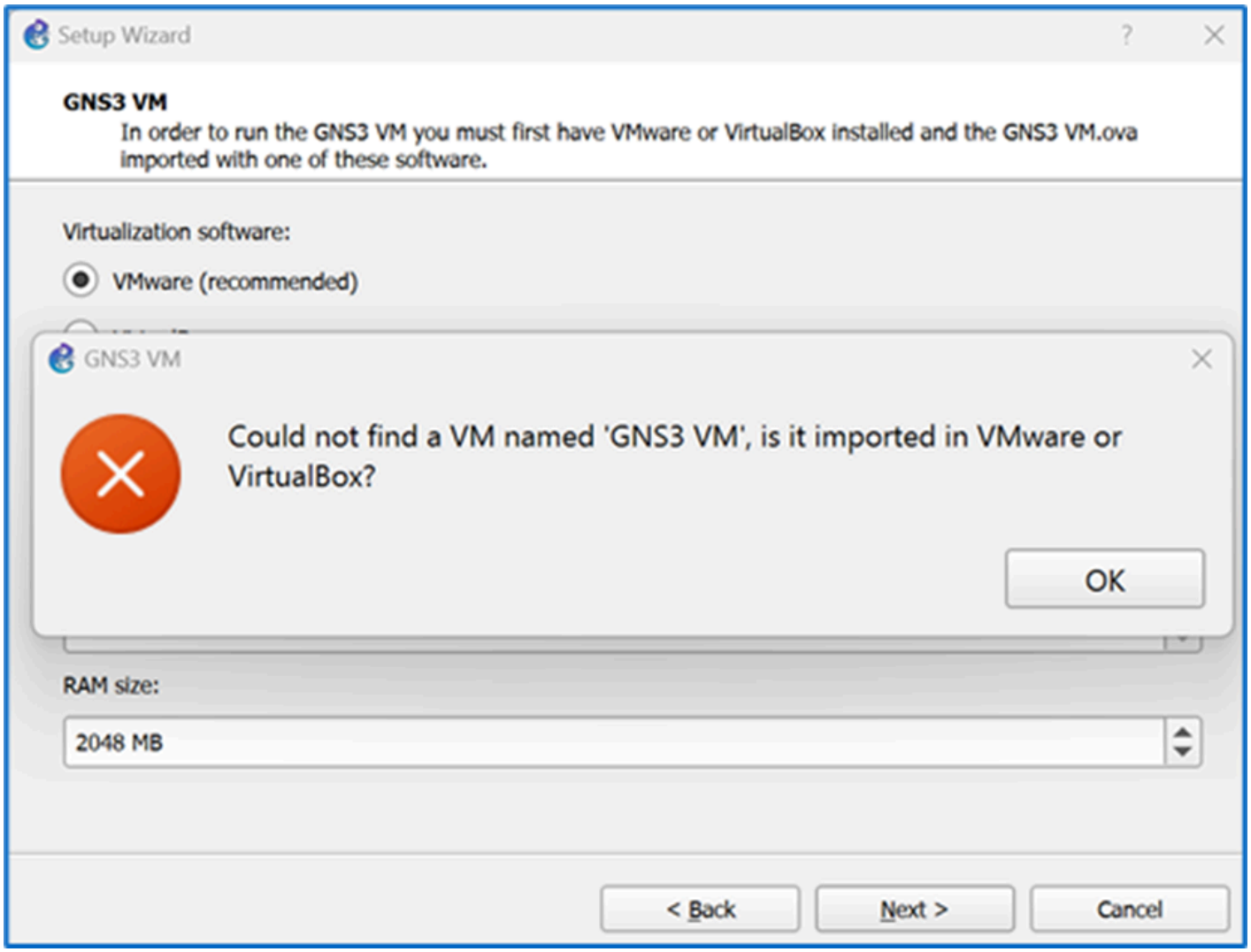


Figure 11 – GNS3 Error, cannot find GNS3 VM in VMware

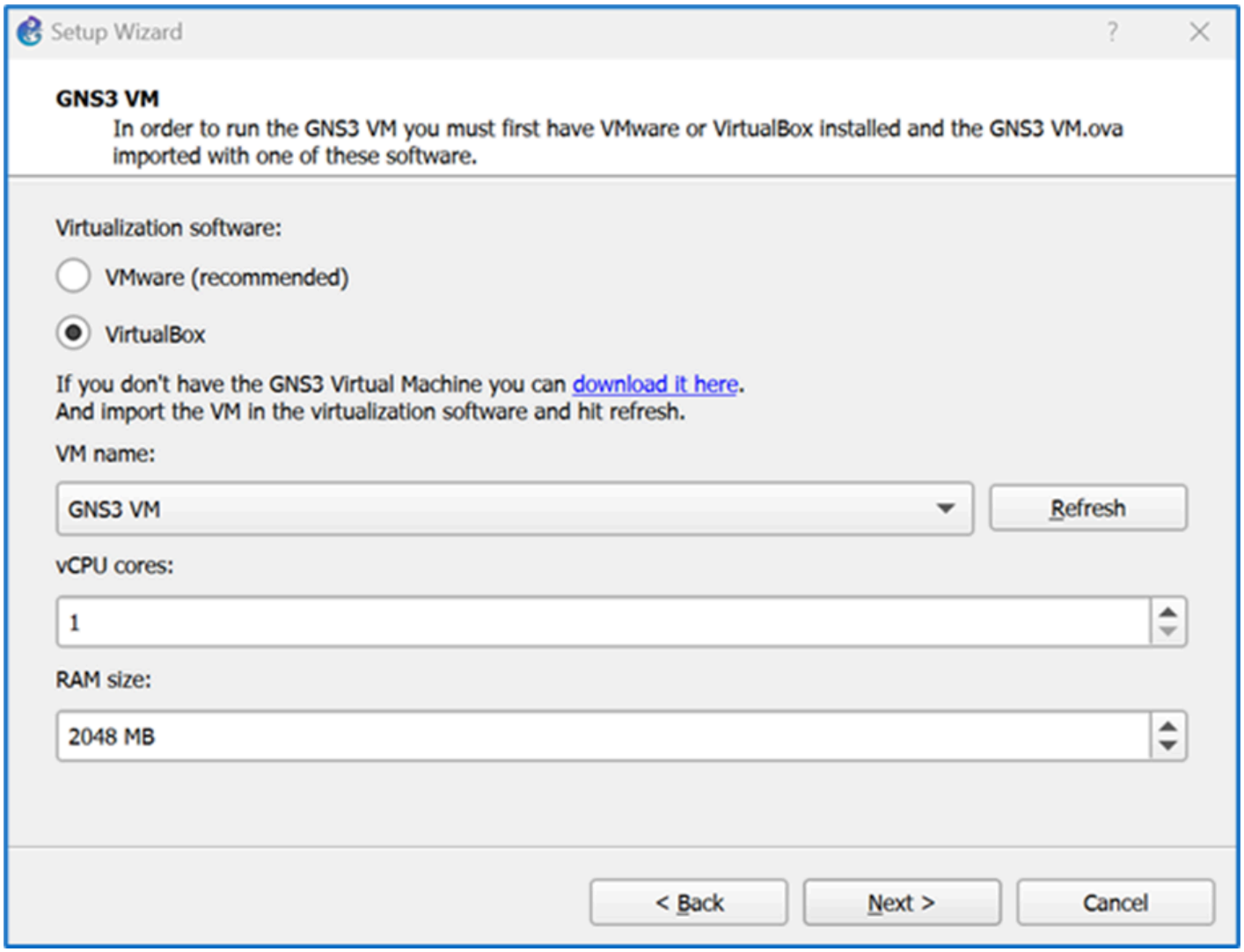


Figure 12 – GNS3 VM Setup Wizard Changing to VirtualBox

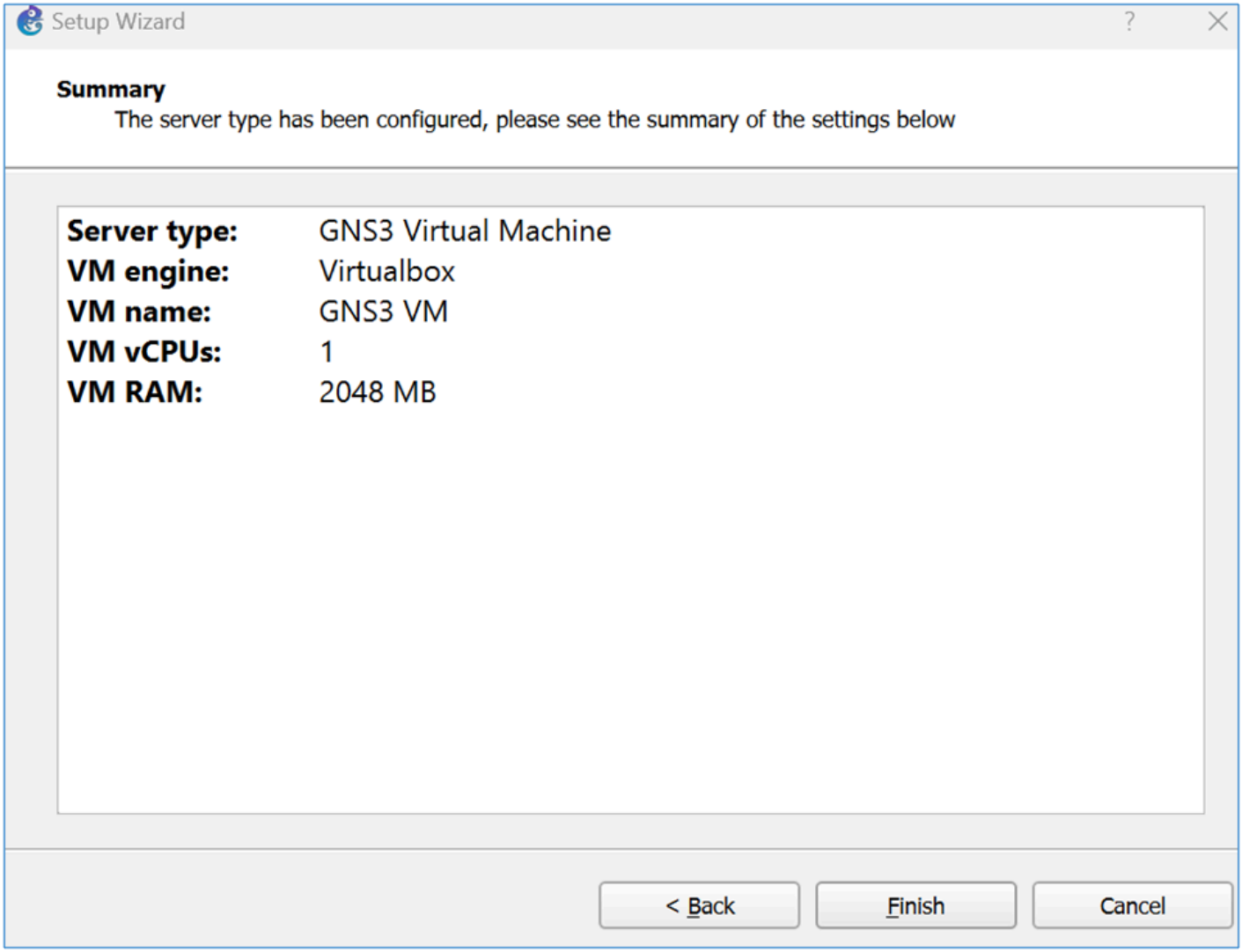


Figure 13 – Finish Setup Wizard

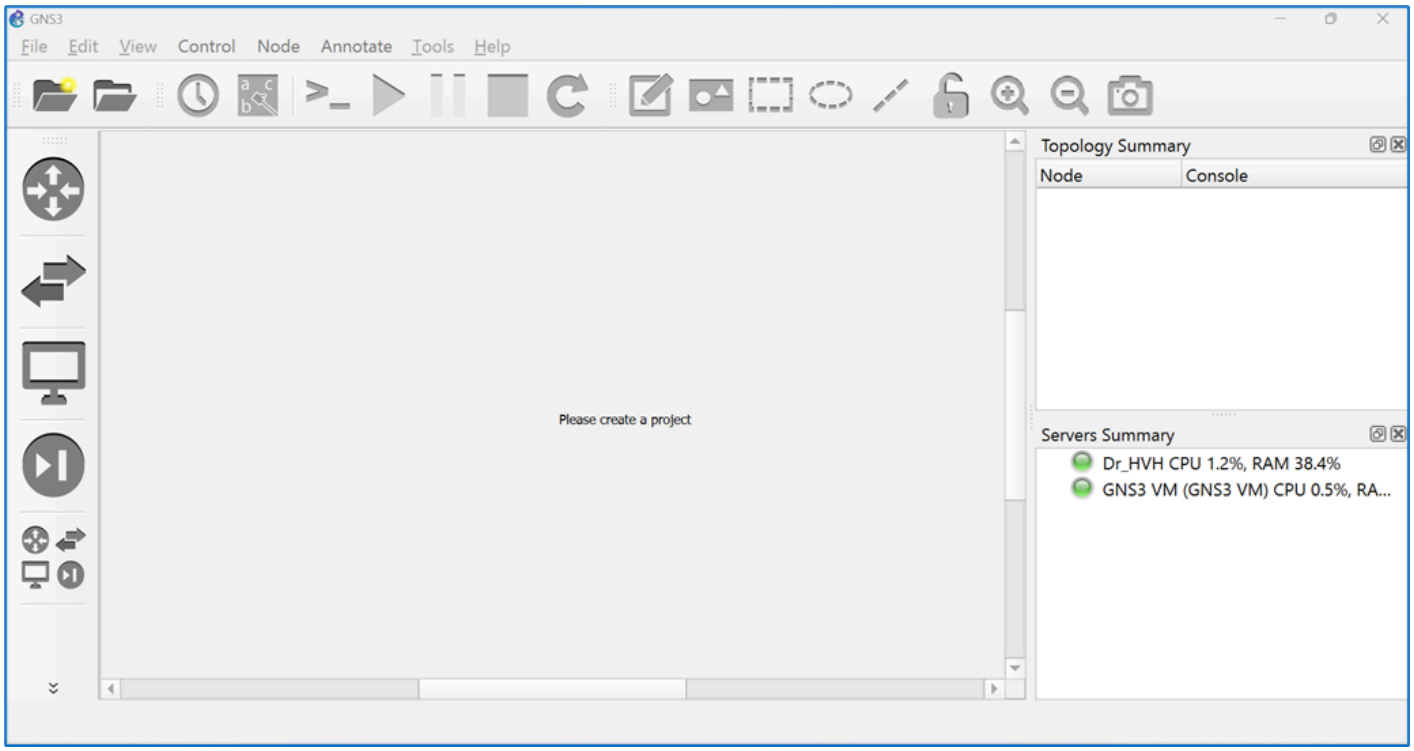


Figure 14 – this is what your screen should look like after finishing the Setup Wizard

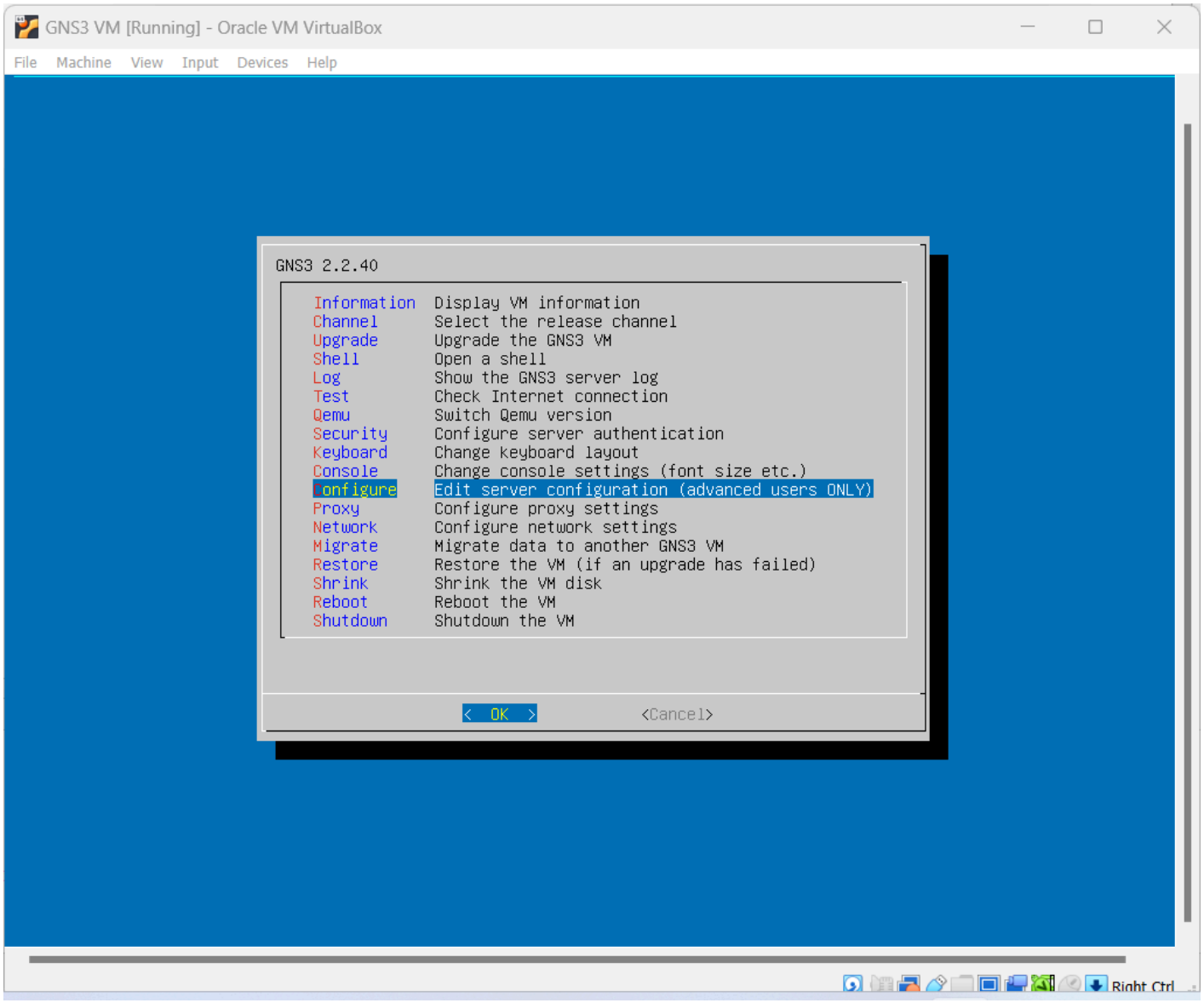


Figure 15 – Disabling Qemu settings in the GNS VM

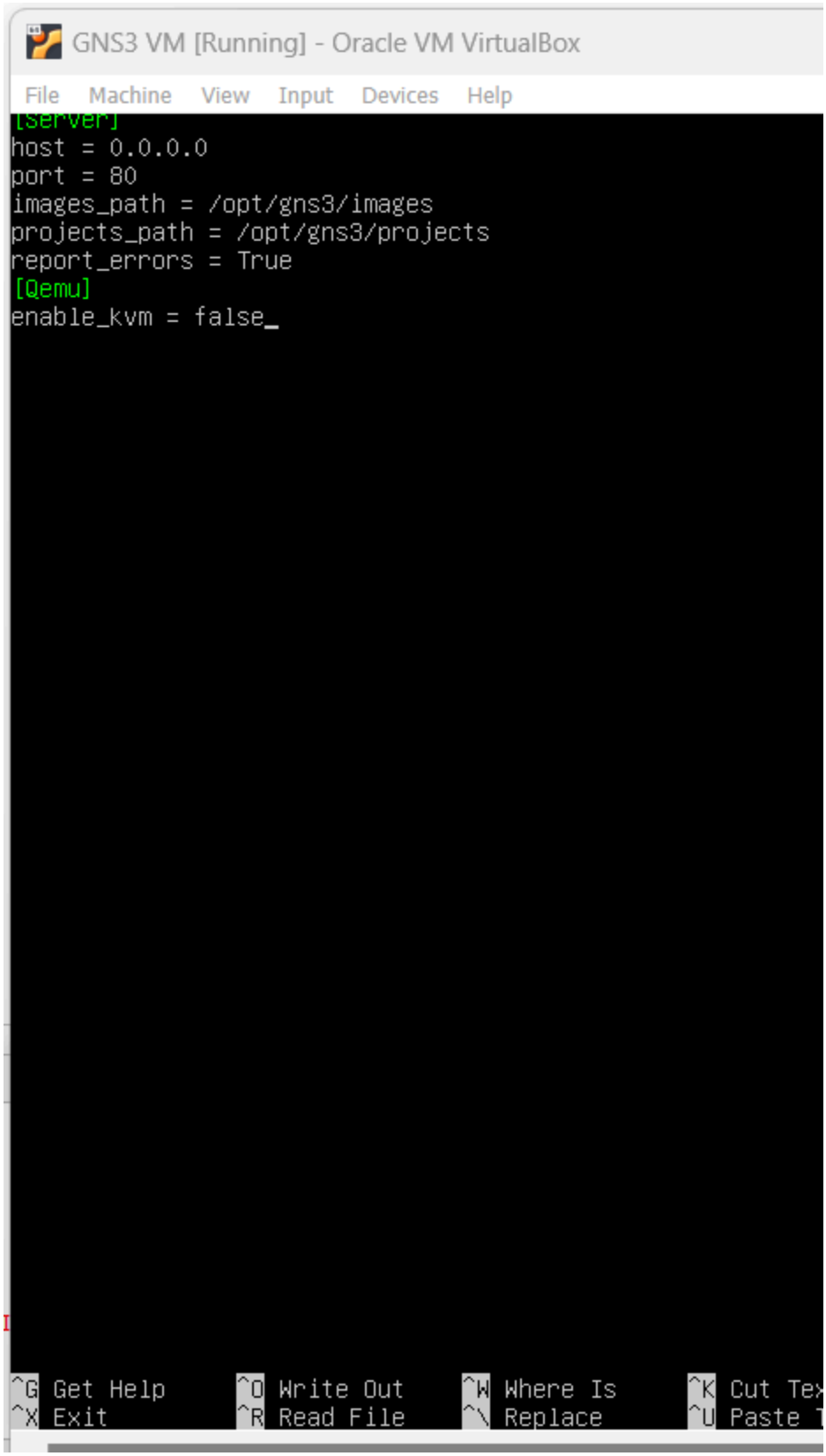


Figure 16 – Disabling Qemu for the GNS3 VM

CHAPTER 3

Adding a MikroTik Appliance in GNS3

MATHEW J. HEATH VAN HORN, PHD

MikroTik is a Latvian enterprise network equipment manufacturer. Their network hardware is used in enterprise networks throughout the world. Their router operating system software is free to use for non-commercial purposes. We use the MikroTik Cloud Hosted Router (CHR) router operating system throughout this book because we have found that it has many of the same features as other commercial products while also being very reliable while running in the GNS3 working environment.

LEARNING OBJECTIVES

- Successfully download, install, and run MikroTik Cloud Hosted Router appliance in a GNS3 environment

PREREQUISITES

- Chapter 2 – Setting Up a GNS3 Environment

DELIVERABLES

- None – this is a preparatory lab that supports other labs in this book

RESOURCES

- GNS3 Documentation – https://docs.gns3.com/docs
- MikroTik Documentation – https://help.mikrotik.com/docs/display/ROS/Getting+started

CONTRIBUTORS AND TESTERS

Testers:

- Quinton D. Heath Van Horn, 7th Grade
- David Reese, Mathematics Student, SUNY Brockport
- Cody Shinkyu Park, Honeywell Software Engineer, ERAU-Prescott Alumni

- Salvador Morales, Safety Management System Analyst, ERAU-Prescott Alumni
- Evan Paddock, Cybersecurity Student, ERAU-Prescott
- Dante Rocca, Cybersecurity Student, ERAU-Prescott
- Sawyer Hansen, Cybersecurity Student, ERAU-Prescott

Phase I – Installing a MikroTik router

Many learners use MikroTik routers to learn enterprise networking principles. You will find many instruction sites on the internet using MikroTik in GNS3.

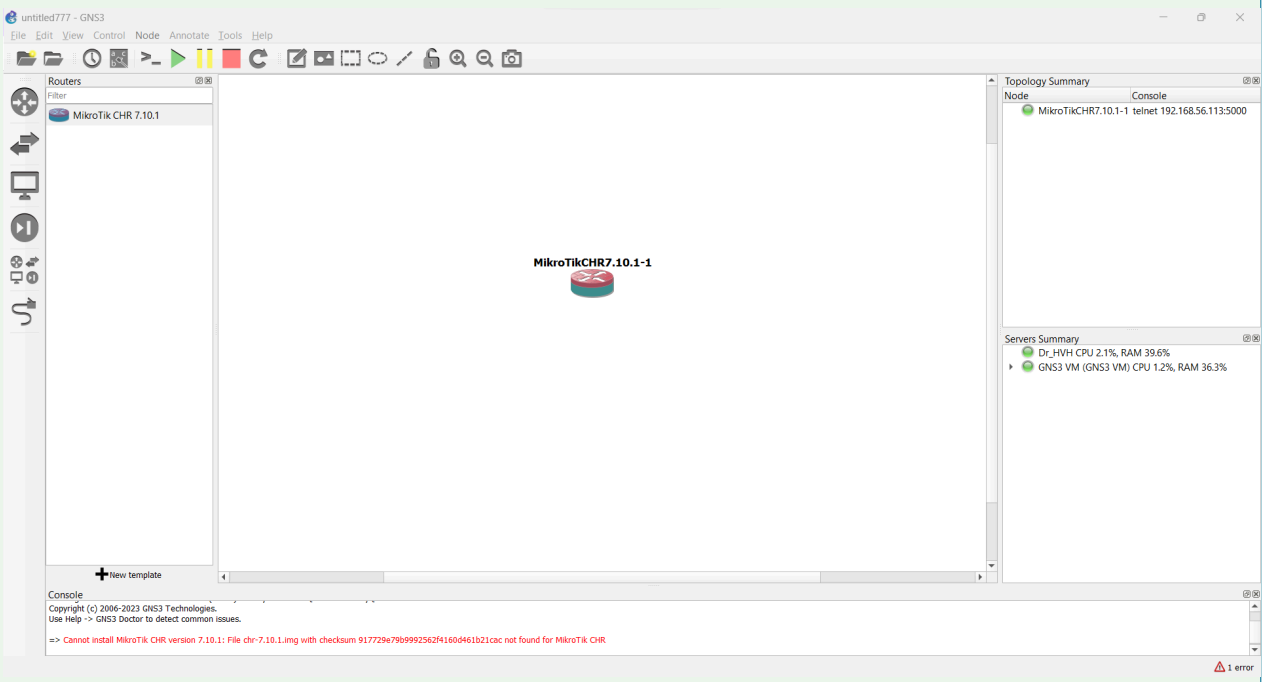


Figure 12 – MikroTik Router successfully installed to the GNS3 Working Environment

1. Visit the GNS3 Marketplace at https://www.gns3.com/marketplace/appliances

2. In the search appliances field, type “MikroTik” (Figure 1)

3. Navigate to the MikroTik CHR appliance and click on it (Figure 2)

4. Download the appliance by hitting the ***Download*** button

5. Scroll down to the most recent version of the image and click on the ***Download*** link. In this case, we are using the chr-7.7.img (Figure 3)

6. Navigate to your downloads folder (or wherever you download the files) and unzip the image file

7. Start GNS3 Workspace

8. At the GNS Workspace top ribbon bar, go to ***File*** and on the submenu click on ***Import Appliance*** (Figure 4)

9. Select the appliance file that you downloaded (Figure 5)

10. Press the ***Open*** button

11. Select the server type Install the appliance on the GNS3 VM (recommended) and press the ***Next*** button (Figure 6)

12. Accept the default QEMU settings and press the ***Next*** button (Figure 7)

13. Highlight the Appliance Version (in this case we are using version 7.10.1) and you will see the status Missing Files. To fix this, click on ***Import*** (Figure 8)

14. Navigate to where you unzipped the image file from Step 6 (Figure 9)

15. Now the status has changed to Ready to Install. Highlight the Ready to Install and click on ***Next*** (Figure 10)

16. Confirm the installation by pressing ***Yes***

17. Read the notes, and press ***Finish*** (Figure 11)

18. You will now see the MikroTik router in the Routers Menu. You can drag it to the workspace and start it to make sure it runs (Figure 12)

End of Lab

List of Figures

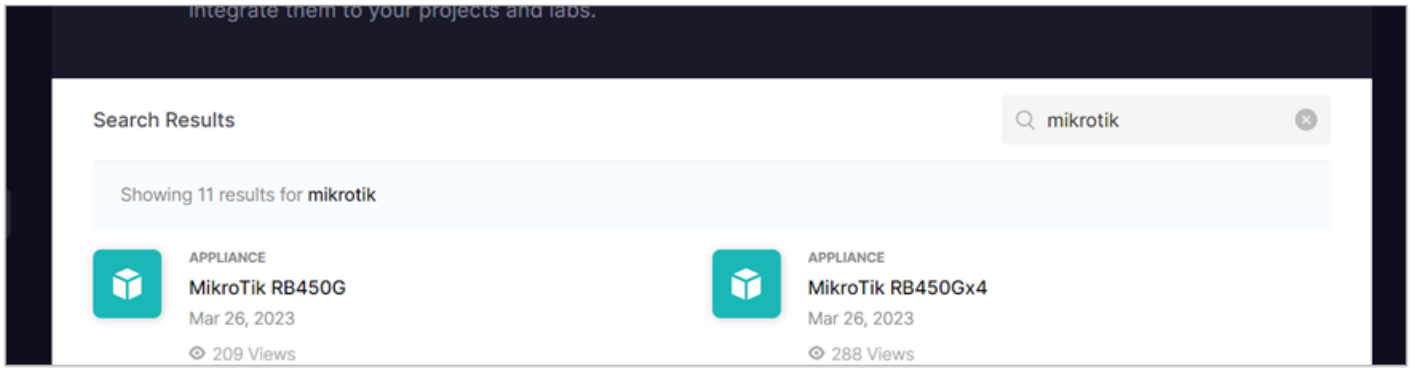


Figure 1 – Searching GNS3 marketplace for MikroTik appliances

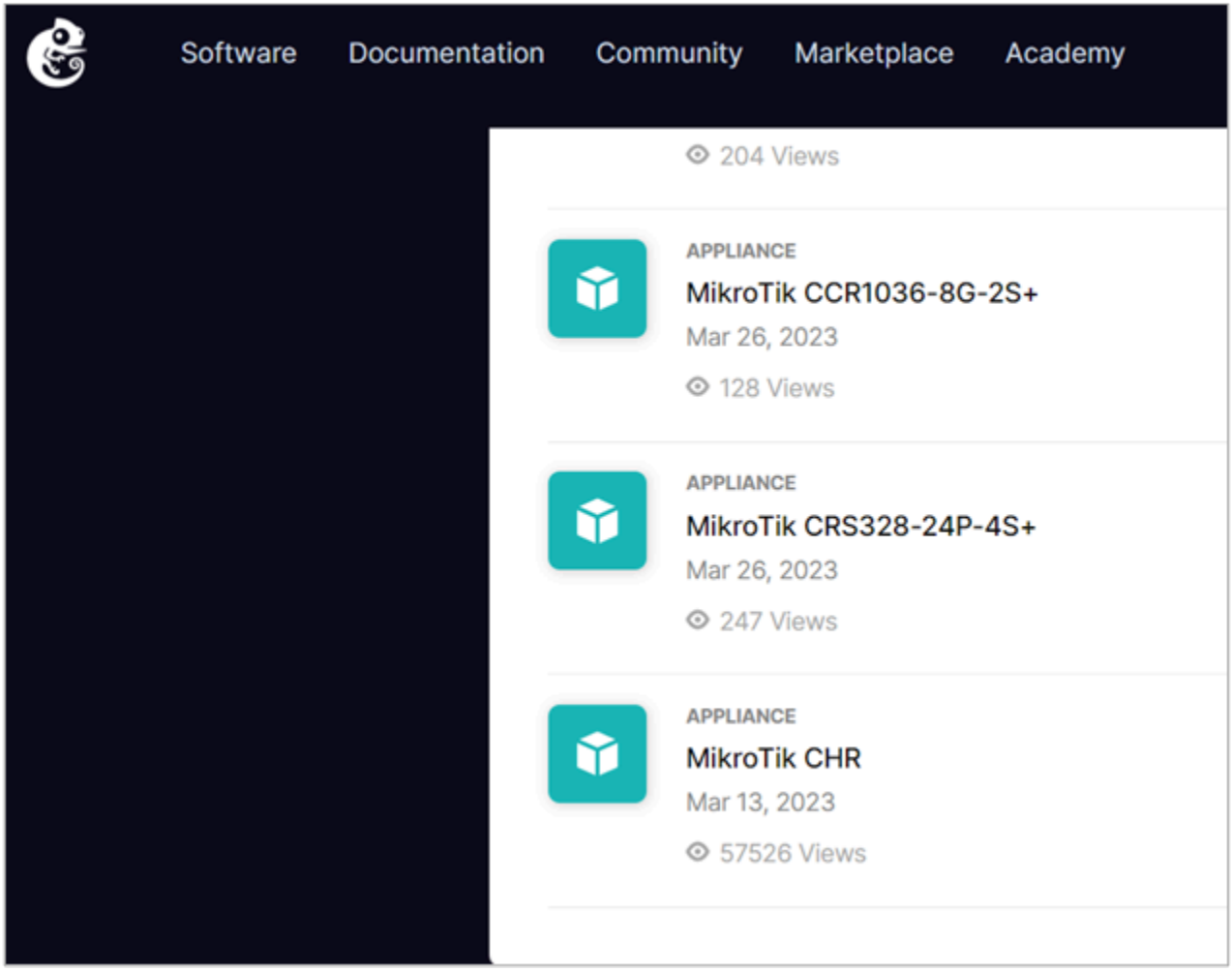


Figure 2 – Showing the MikroTik CHR appliance on GNS3 marketplace

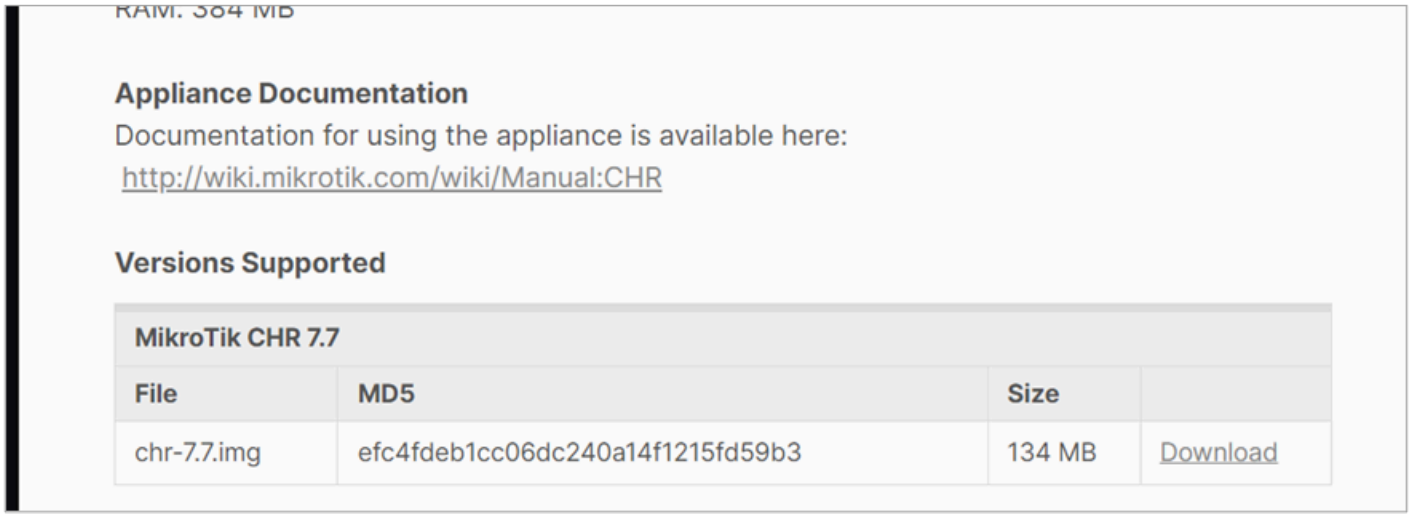


Figure 3 – Downloading the MikroTik router image from GNS3 marketplace

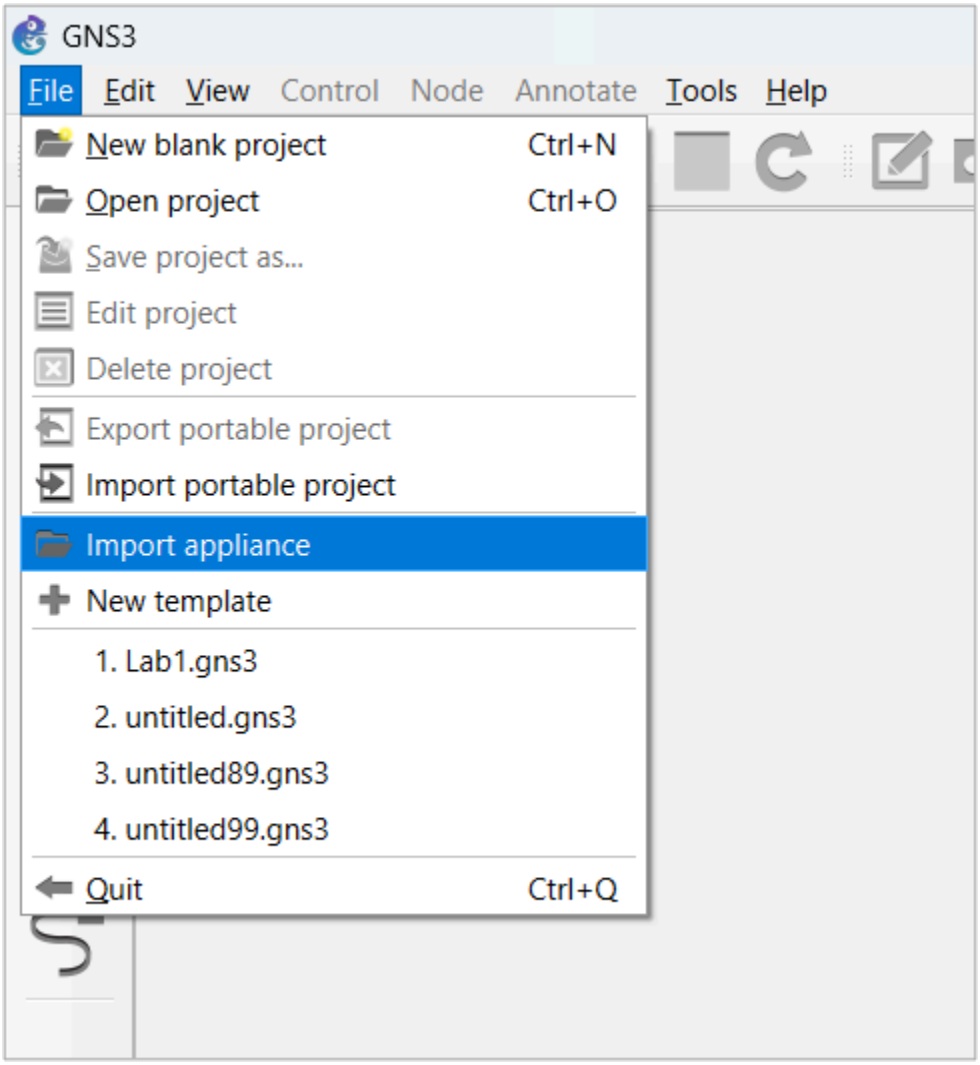


Figure 4 – Screenshot of GNS3 Workspace menu selection

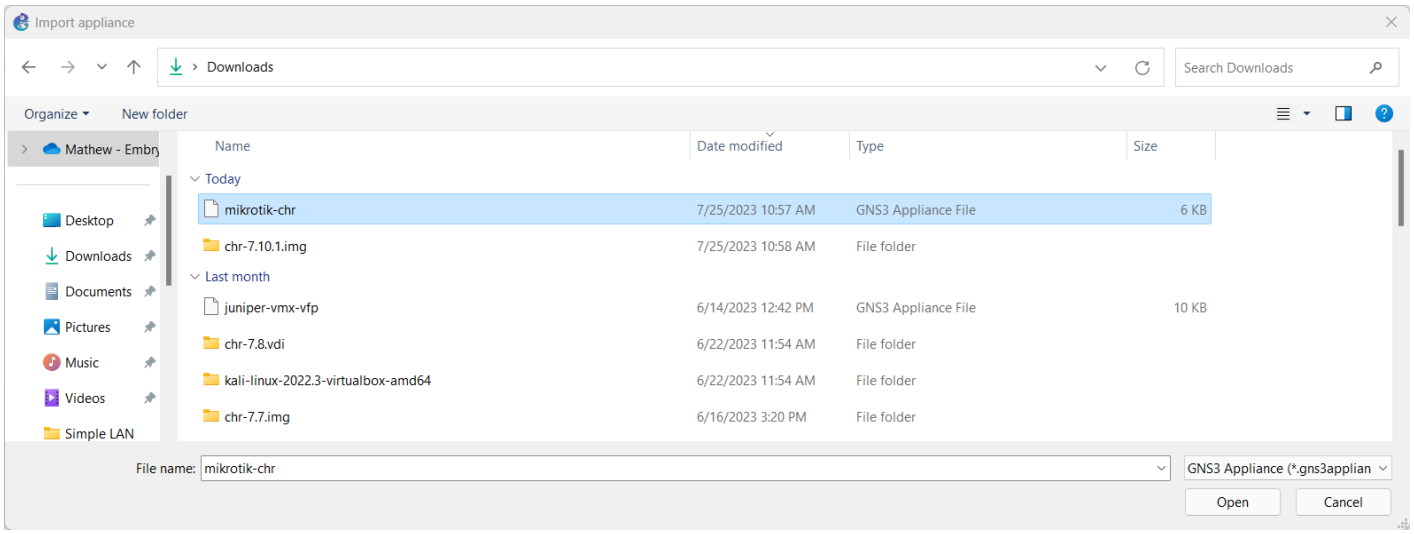


Figure 5 – Selecting the appliance to import into GNS3 Workspace

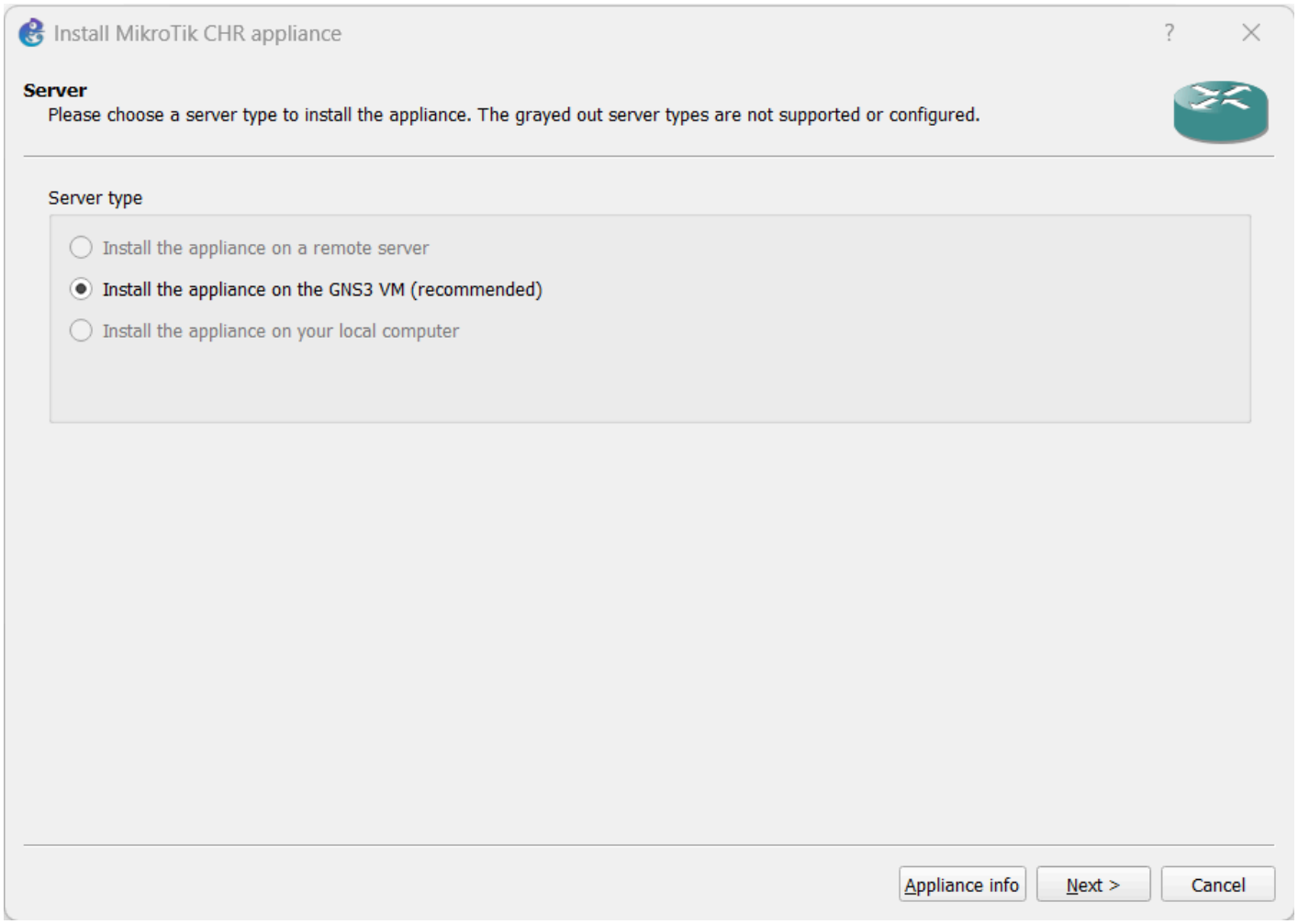


Figure 6 – Configuring the GNS3 Workspace with a MikroTik appliance

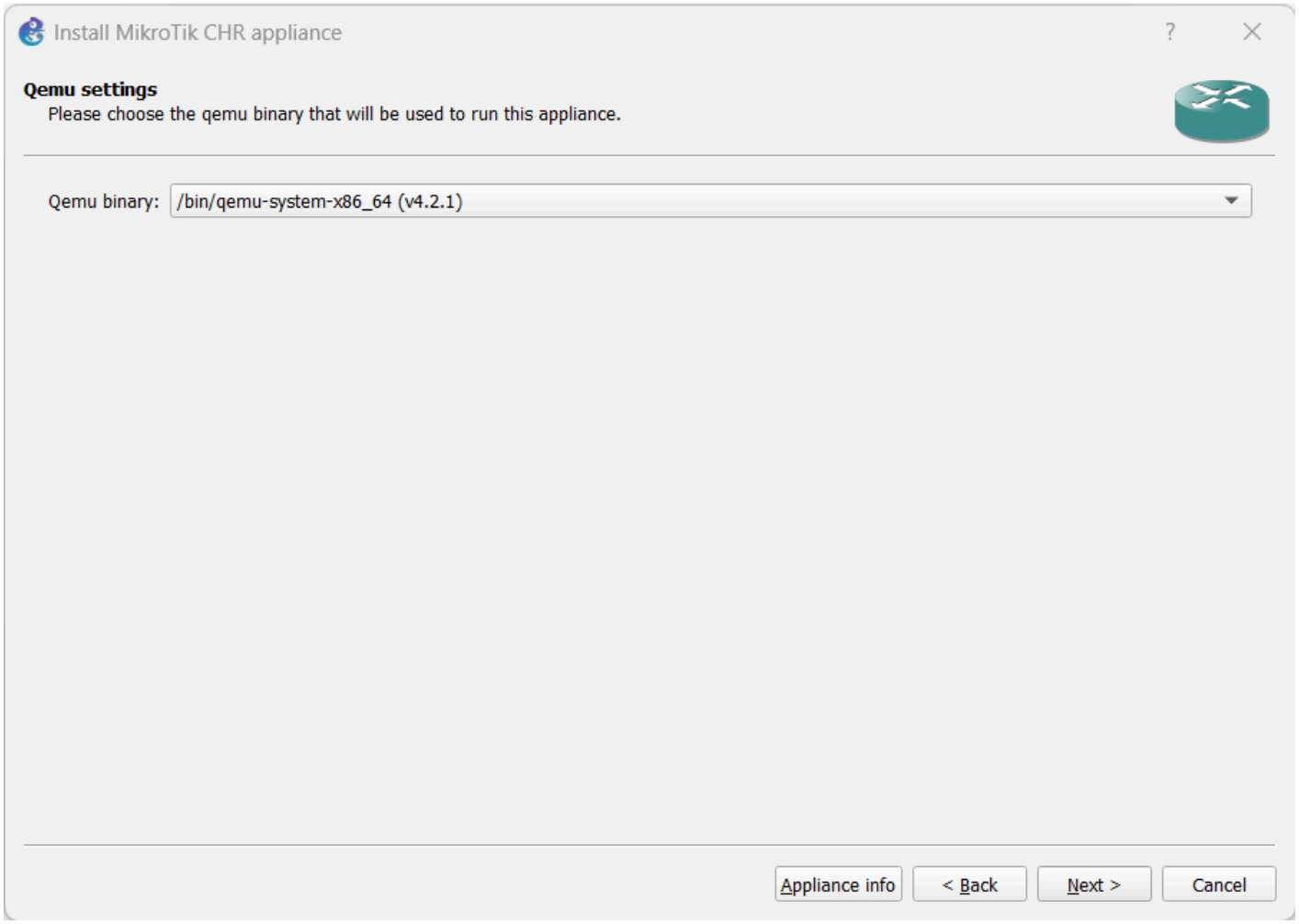


Figure 7 – Accept the QEMU settings

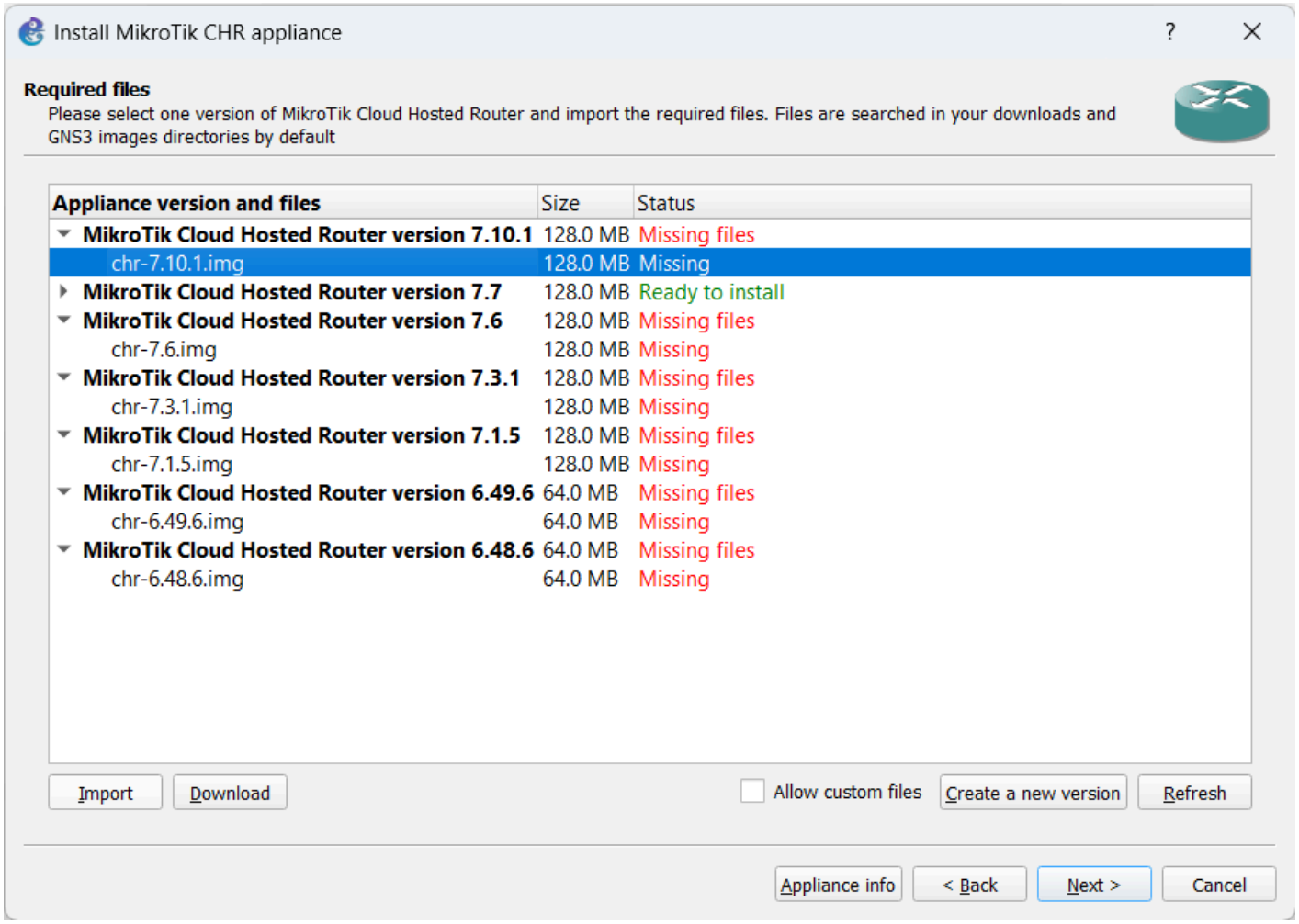


Figure 8 – Correct the missing files for the MikroTik router

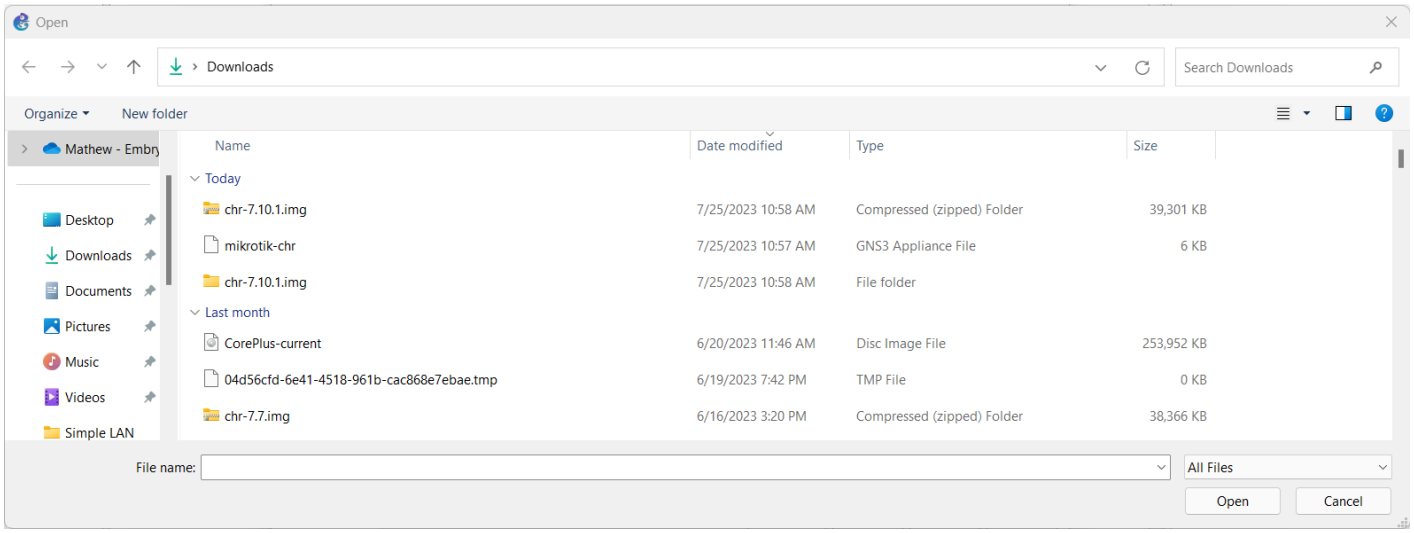


Figure 9 – Navigate to where the image file was saved after unzipping

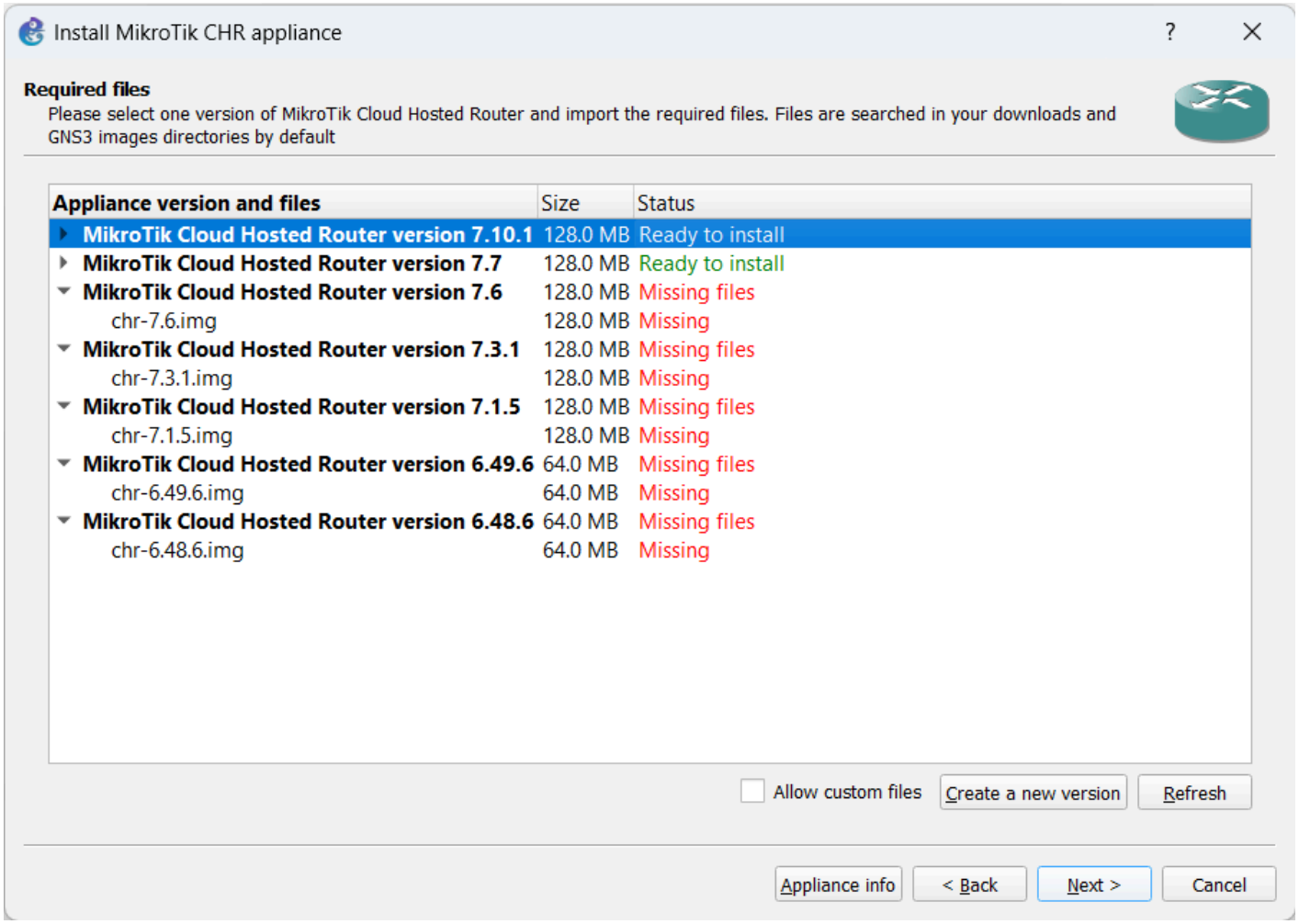


Figure 10 – Installing the MikroTik CHR router

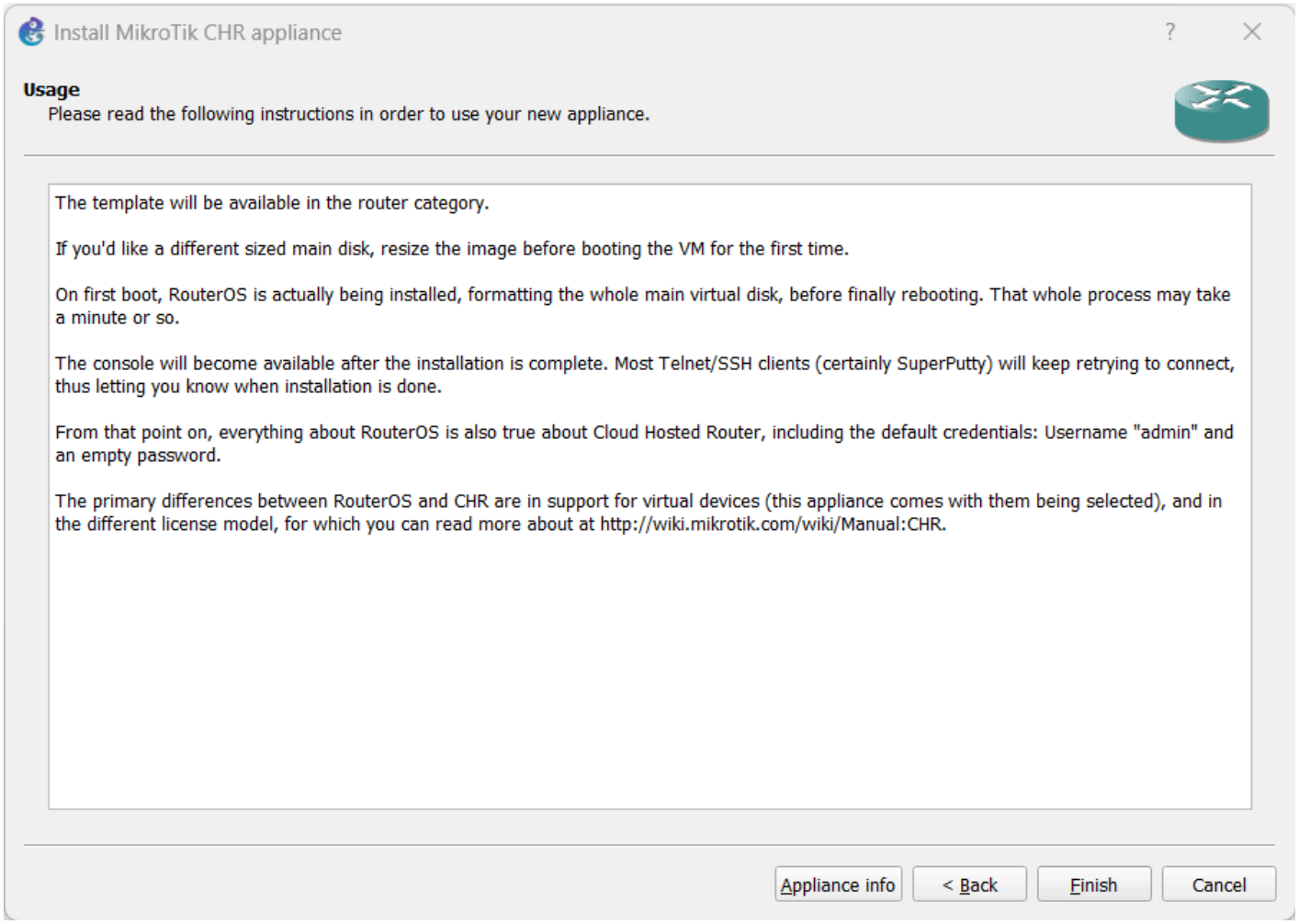


Figure 11 – Finish the addition of a MikroTik router to the GNS3 environment

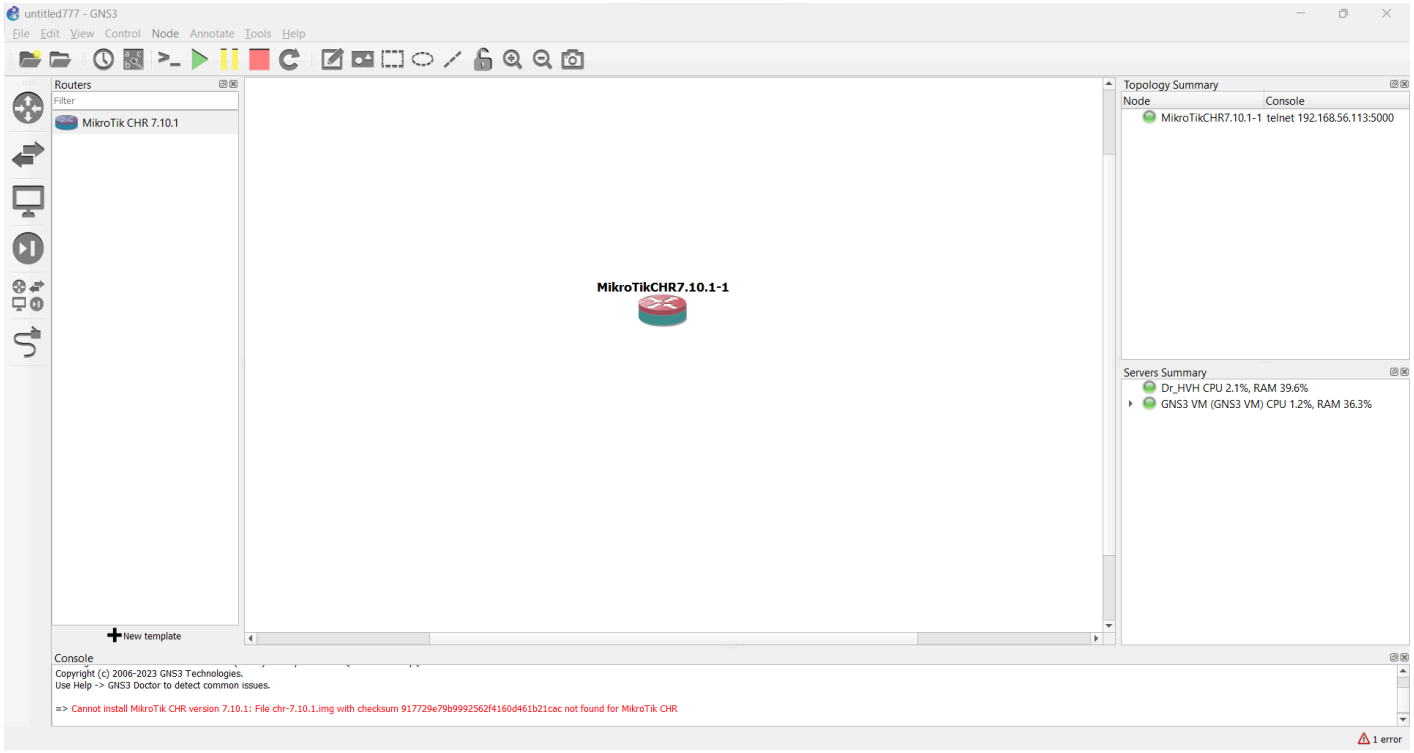


Figure 12 – MikroTik Router successfully installed to the GNS3 Working Environment

CHAPTER 4

Installing an OpenWRT Router in GNS3

MATHEW J. HEATH VAN HORN, PHD

OpenWrt (Open Wireless Router) is an open-source router software developed by Linksys. This free software best mimics the typical home router found in most residences.

LEARNING OBJECTIVES

- Successfully download, install, and run OpenWrt in a GNS3 environment

PREREQUISITES

- Chapter 2 – Setting up a GNS3 Environment

DELIVERABLES

- None – this is a preparatory lab that supports other labs in this book

RESOURCES

- GNS3 Documentation – https://docs.gns3.com/docs
- OpenWrt Download – https://openwrt.org/downloads
- OpenWrt Documentation – https://openwrt.org/docs/start

CONTRIBUTORS AND TESTERS

- Quinton D. Heath Van Horn, 7th Grade
- David Reese, Mathematics Student, SUNY Brockport
- Cody Shinkyu Park, Honeywell Software Engineer, ERAU-Prescott Alumni
- Salvador Morales, Safety Management System Analyst, ERAU-Prescott Alumni
- Evan Paddock, Cybersecurity Student, ERAU-Prescott
- Dante Rocca, Cybersecurity Student, ERAU-Prescott

- Sawyer Hansen, Cybersecurity Student, ERAU-Prescott

Phase I – Installing OpenWrt

This is an abbreviated installation walkthrough. This lab is used to support other labs in this text. This portion covers the download and installation of OpenWrt in the GNS3 environment. This lab is very similar to Chapter 3 – Installing a MikroTik router.

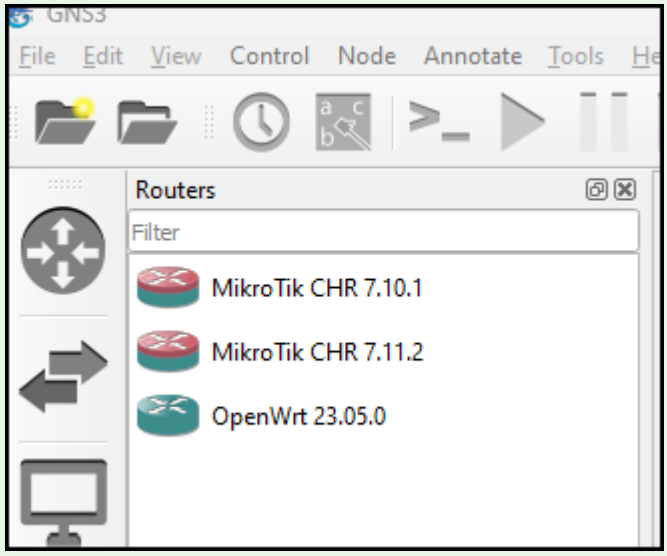


Figure 9 – OpenWrt appears in the router appliance menu

1. Visit https://www.gns3.com/marketplace/appliances and log in (Figure 1)

2. Go to Marketplace

3. Select Appliances on the left

4. Search for OpenWrt

5. Click on the OpenWrt Appliance (**not** the OpenWrt Realview) and then click the ***download*** button (Figure 2)

6. On the same download screen, scroll down to download the most recent image file. Once downloaded, unzip it (Figure 3)

7. Start the GNS3 Workspace. Once the lights are green, select ***File*** → ***Import Appliance*** (Figure 4)

8. Select the OpenWrt appliance you downloaded earlier and select ***open*** (Figure 5)

9. Install the appliance on the GNS3 VM. Use the default Qemu Settings (Figure 6)

10. Select the ***Missing Files*** for the version of OpenWrt you downloaded earlier and select ***Import*** (Figure 7)

11. Select the image file you unzipped earlier and click ***Open*** (Figure 7)

12. It should now say Ready to install. Click on the file and click ***Next*** (Figure 8)

13. Once it finishes, then it will appear in the router appliance menu (Figure 9)

End of Lab

List of Figures

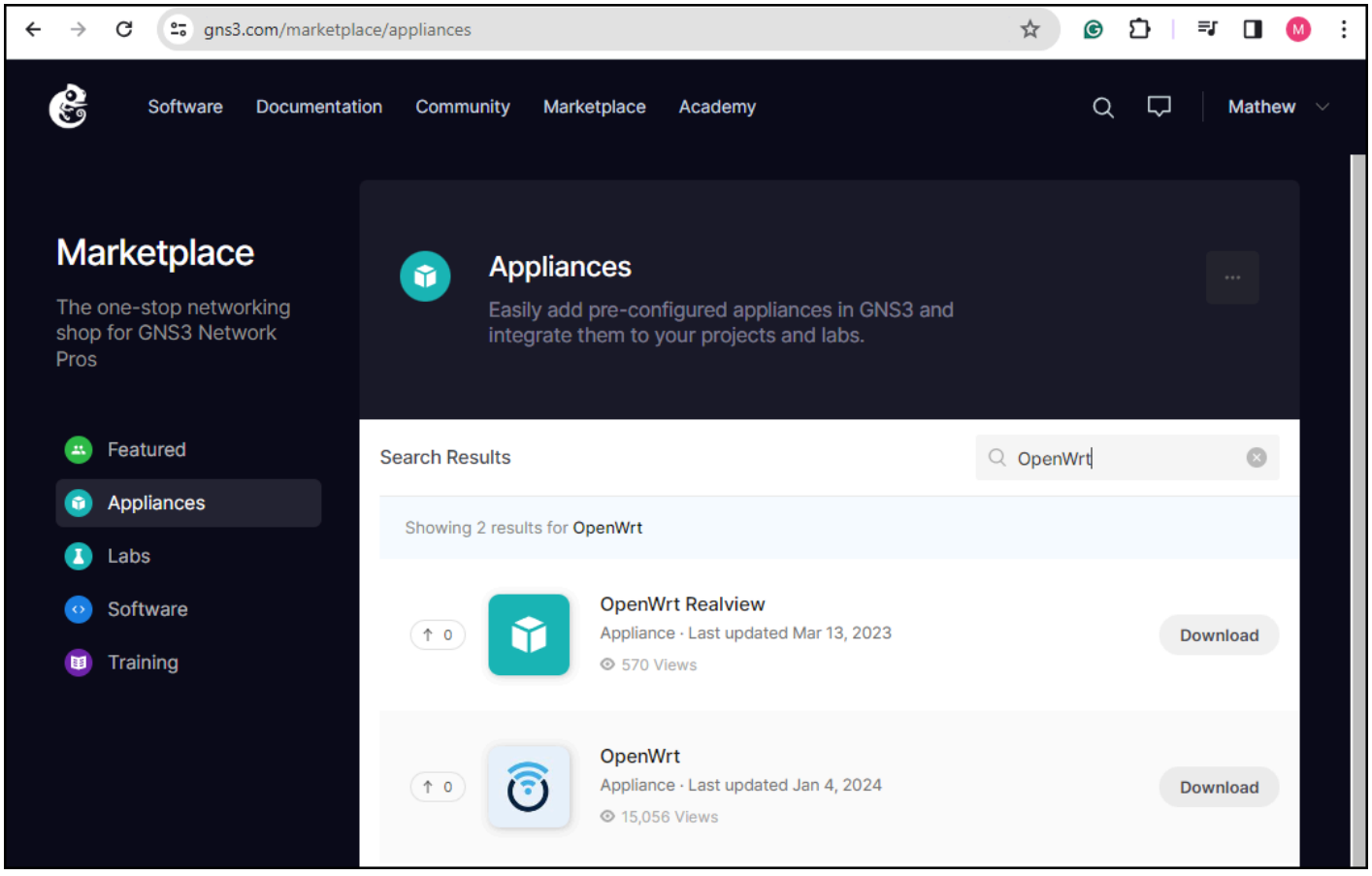


Figure 1 – Downloading OpenWrt

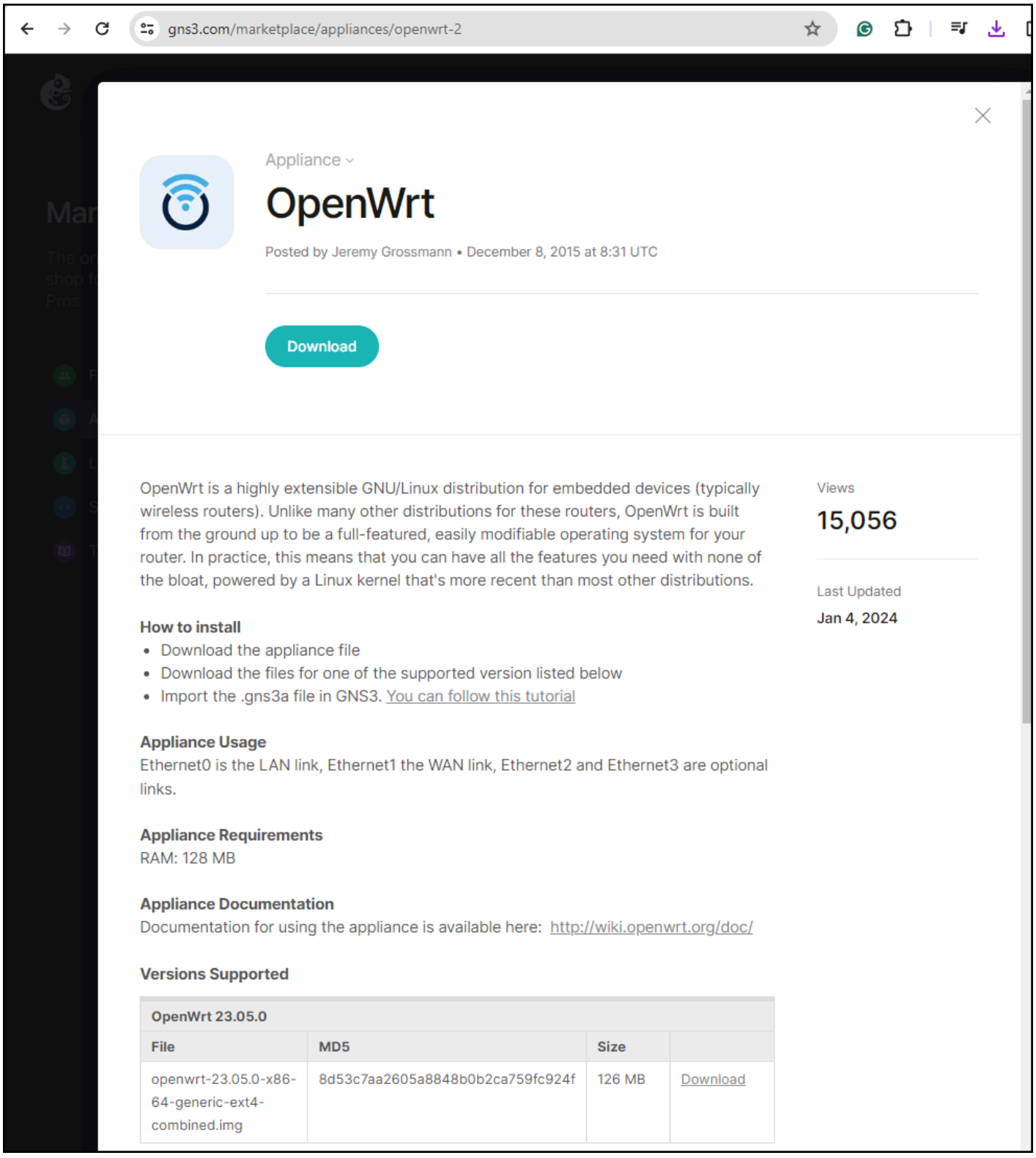


Figure 2 – Download OpenWrt

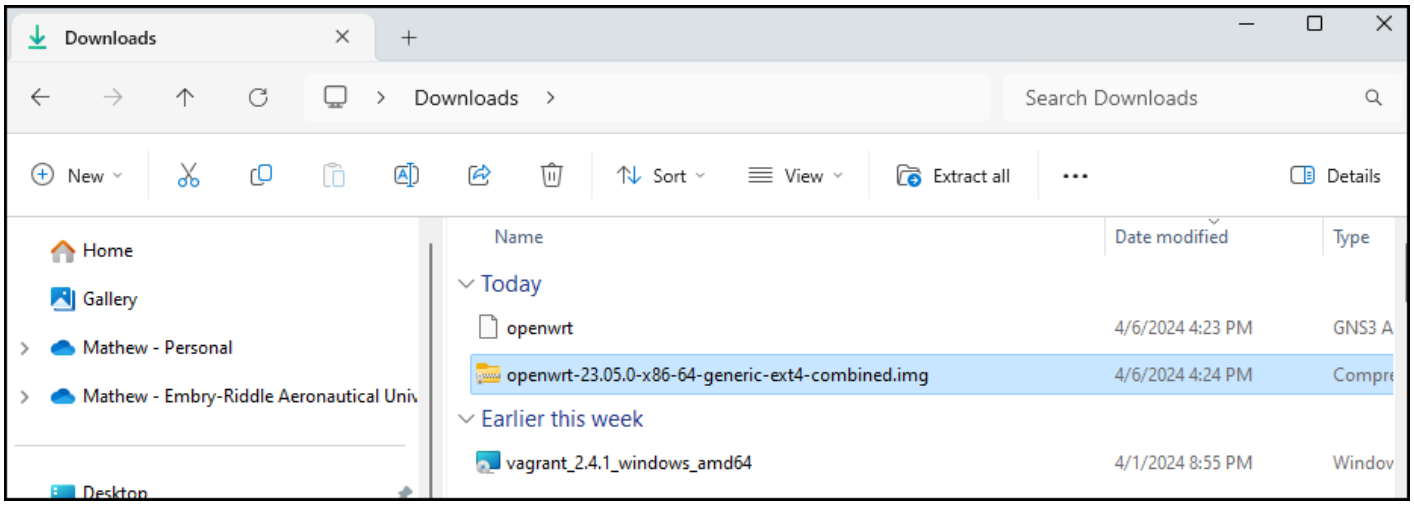


Figure 3 – Unzip the OpenWrt file

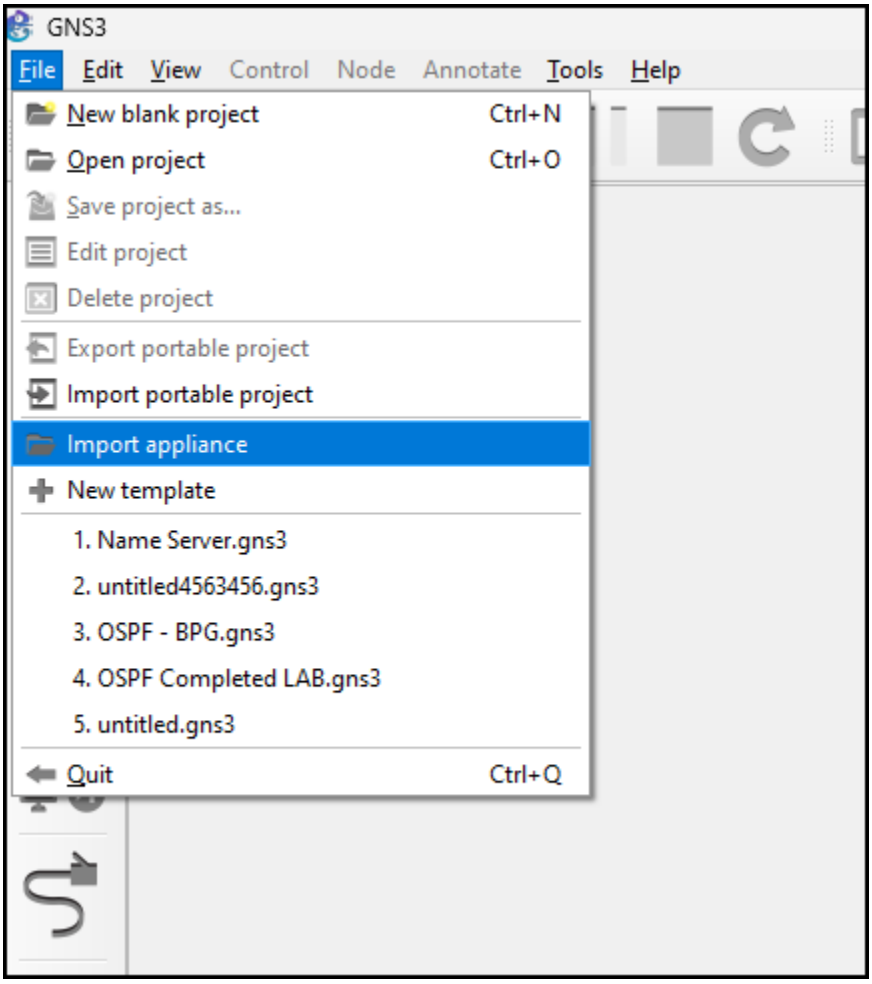


Figure 4 – Import the OpenWrt appliance

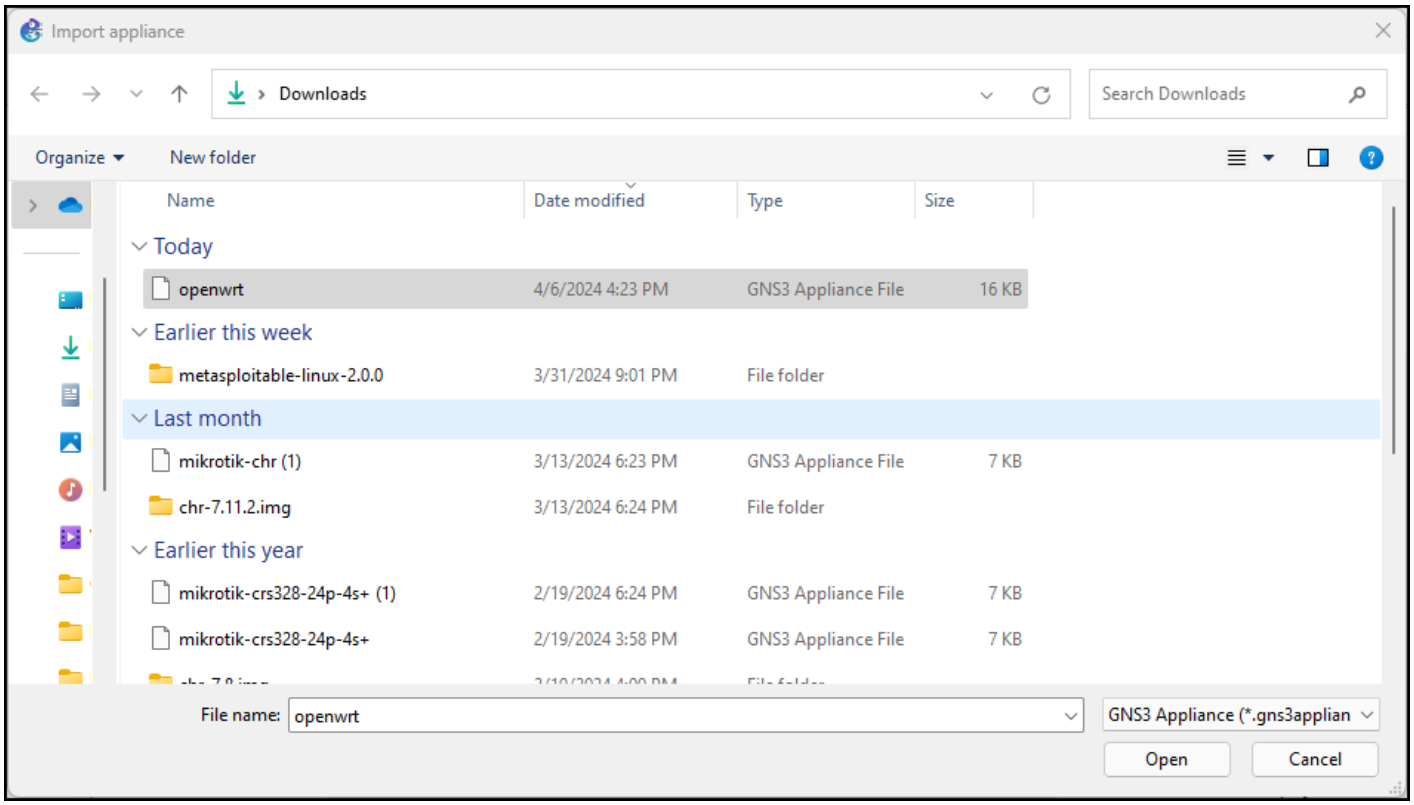


Figure 5 – Select the OpenWrt appliance

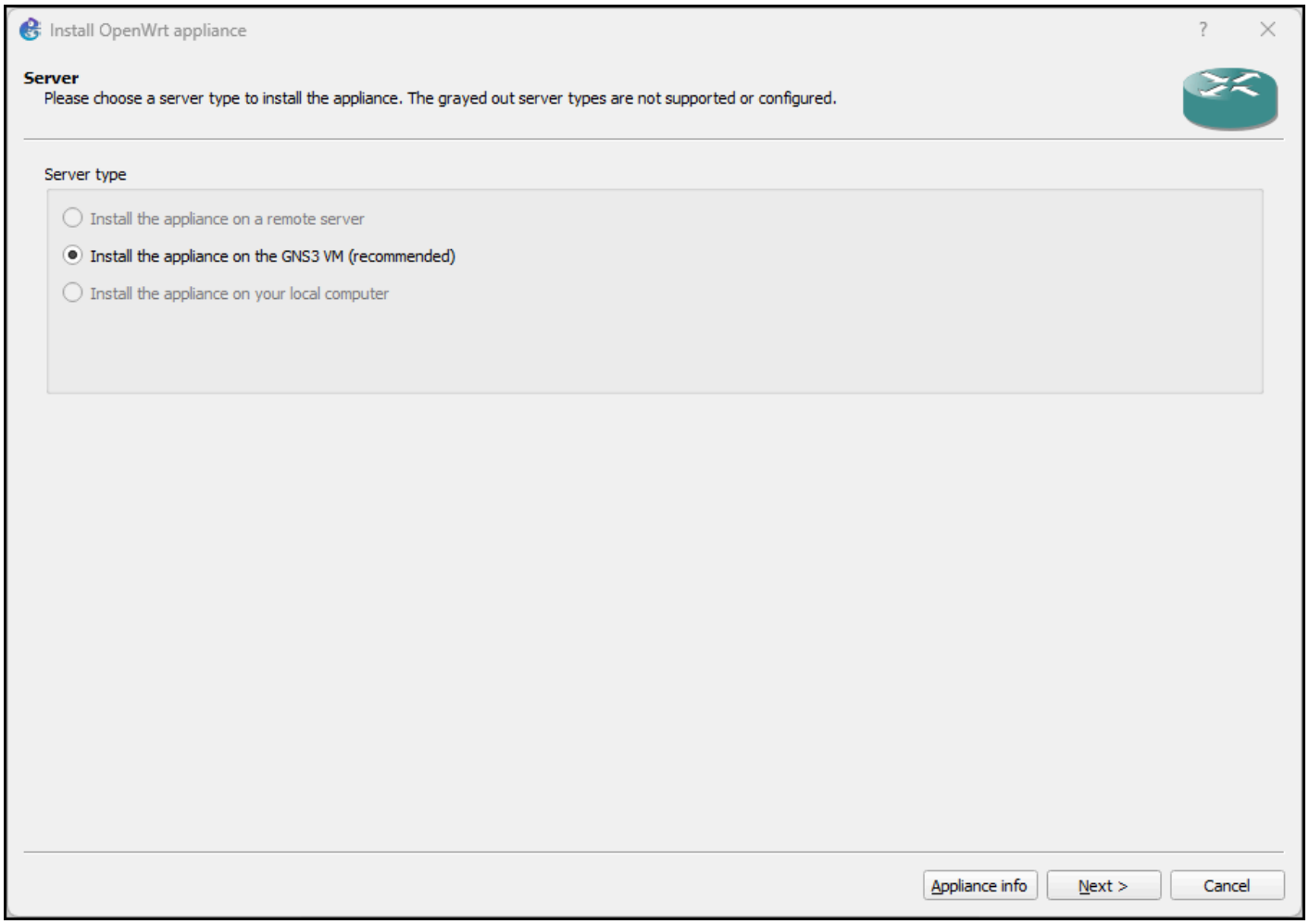


Figure 6 – Install the OpenWrt appliance

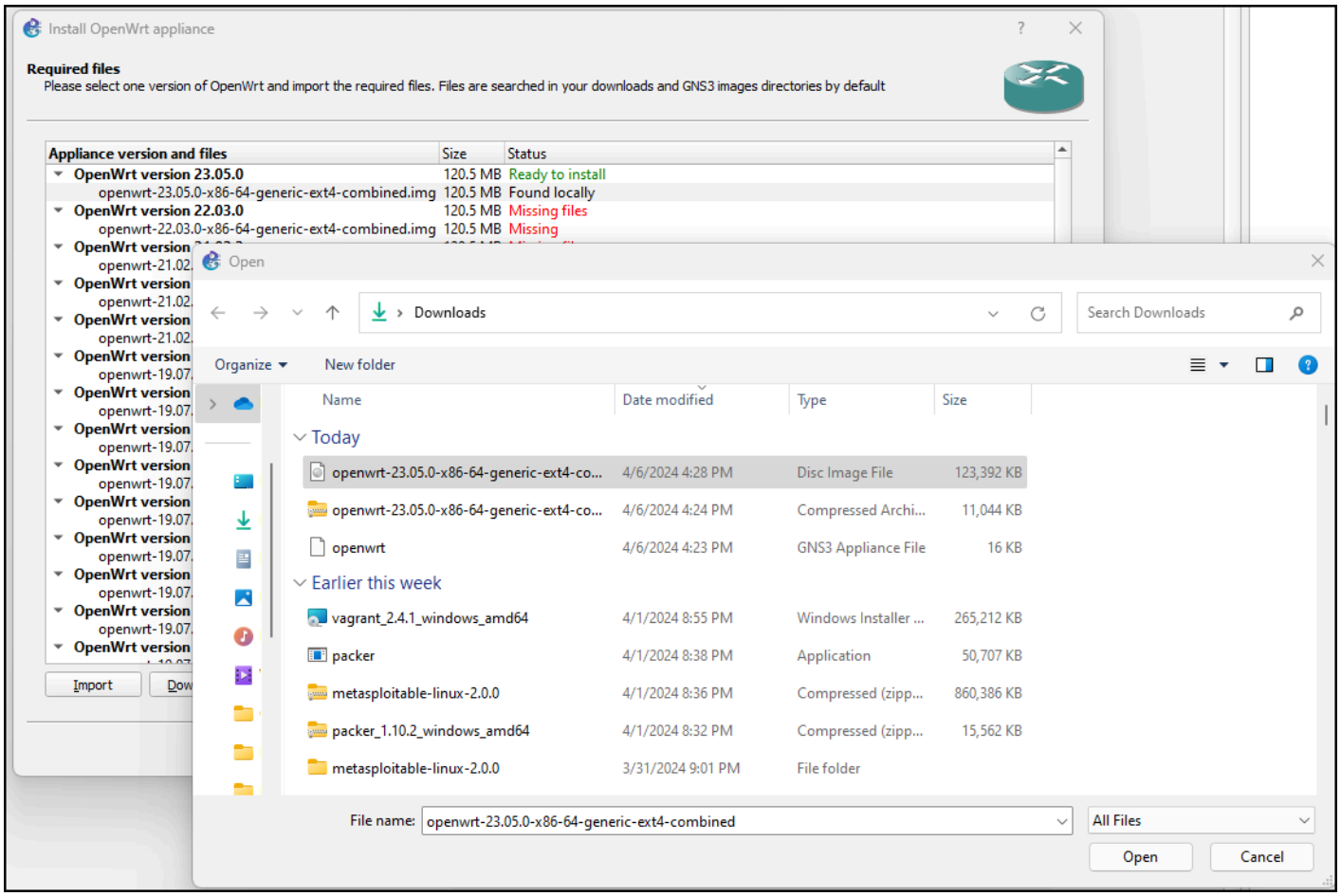


Figure 7 – Select the missing files and open them

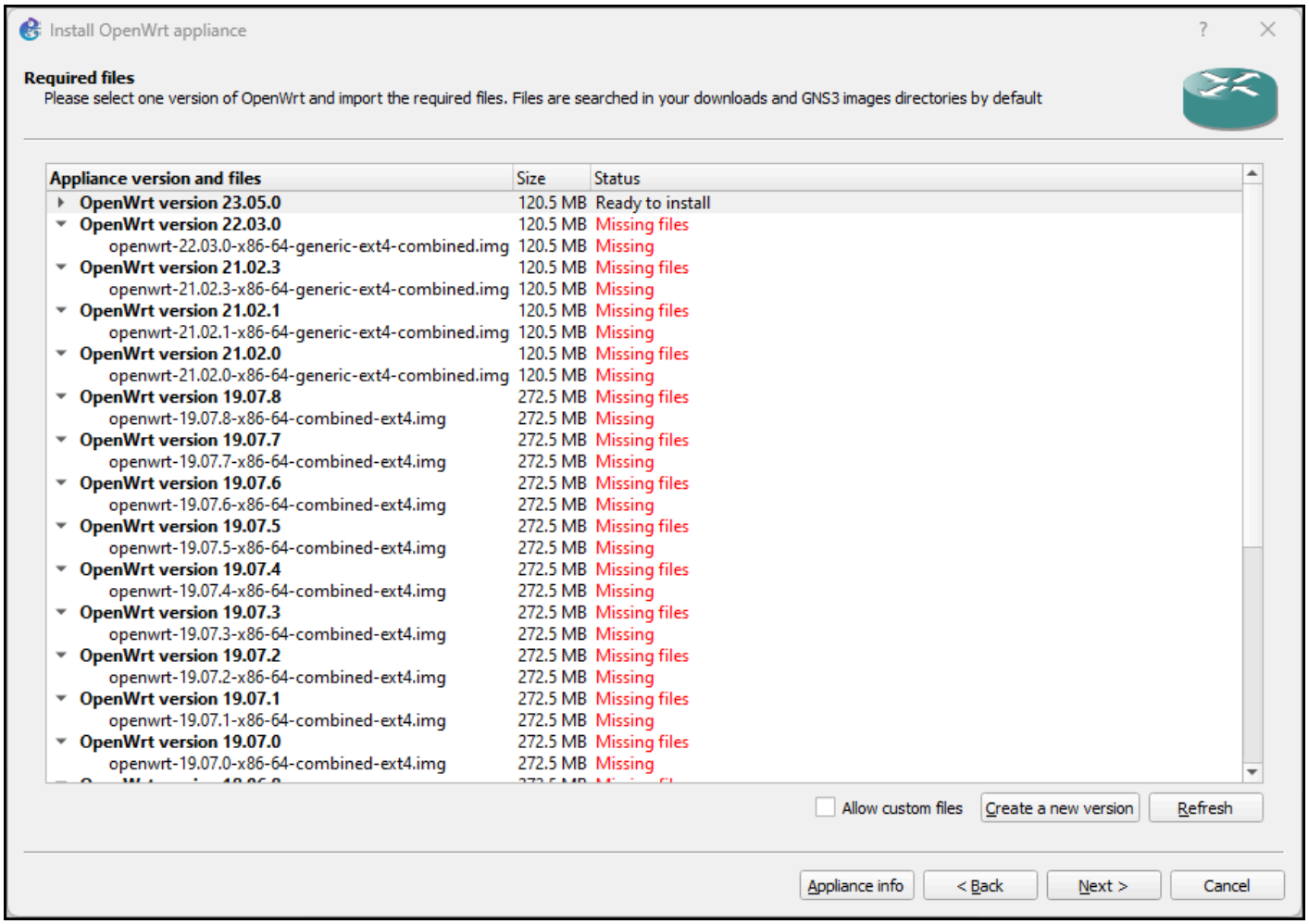


Figure 8 – Finish the install

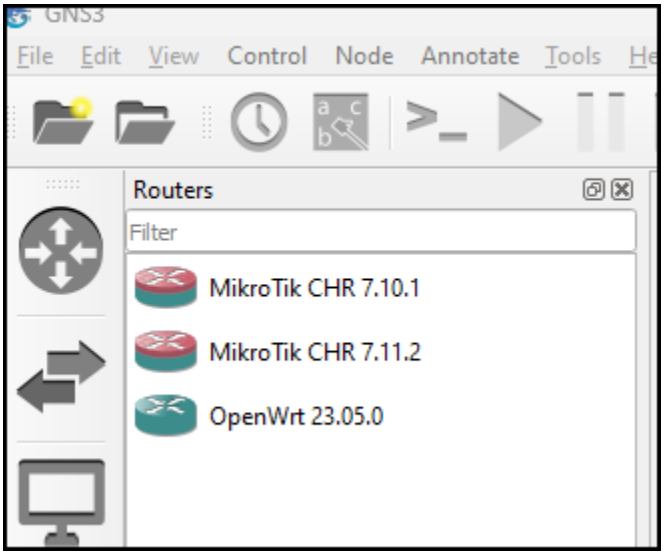


Figure 9 – OpenWrt appears in the router appliance menu

CHAPTER 5

Installing Tiny Core Linux

MATHEW J. HEATH VAN HORN, PHD

Tiny Core Linux is a very lightweight operating system (OS) that is easily configurable to meet a wide variety of needs. Unlike other OSs that require gigabytes (GB) of hard drive space and RAM, Tiny Core Linux requires less than 250 megabytes (MB) of hard drive space and only 23 MB of RAM. This makes it uniquely suited for us to use in this textbook to emulate an enterprise network architecture.

Tiny Core Linux uses a lot of command line interface (CLI) commands, so please pay attention to detail when following these instructions.

LEARNING OBJECTIVES

- Install Tiny Core Linux in VirtualBox
- Add Tiny Core Linux to the GNS3 appliance repository

PREREQUISITES

- Chapter 2 – Setting Up a GNS3 Environment

DELIVERABLES

- None – this is a preparatory lab for other labs

RESOURCES

- Tiny Core Linux Main Website – http://tinycorelinux.net/

CONTRIBUTORS AND TESTERS

- Jacob M. Christensen, C.I.S. Student, ERAU-Prescott
- Julian Romano, C.I.S. Student, ERAU-Prescott
- Cody Shinkyu Park, Honeywell Software Engineer, ERAU-Prescott Alumni
- Evan Paddock, Cybersecurity Student, ERAU-Prescott

- Dante Rocca, Cybersecurity Student, ERAU-Prescott
- Sawyer Hansen, Cybersecurity Student, ERAU-Prescott

Phase I – Download and Install in VirtualBox

Tiny Core Linux is very lightweight. It primarily runs in RAM to increase its operating speed.

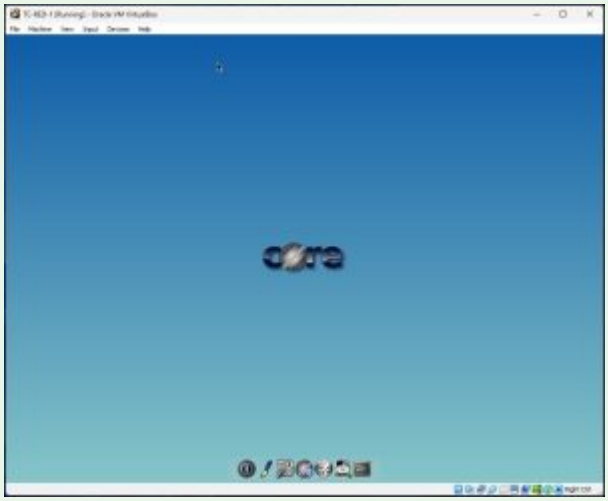


Figure 0.5 – Tiny Core Linux running in VirtualBox

1. Download the Tiny Core Linux iso file named "CorePlus" from http://tinycorelinux.net/downloads.html

> Note: iso is used as a nickname for an optical disk image adhering to the ISO 9660 file system.

2. The file is so small it isn't zipped
3. Open The Oracle VirtualBox Manager and click on ***New*** (Figure 1)
4. Complete the VM form (Figure 2)
    - 4.1. Choose a name – In this lab, we called it "TinyCoreLinux"
    - 4.2. Use the ISO dropdown menu to select the CorePlus-current.iso you downloaded in Step 1
    - 4.3. Use the Type drop-down menu to select ***Linux***
    - 4.4. Use the Version drop-down menu to select ***Other Linux (64-bit)***
    - 4.5. Press ***Next***

5. Decrease the Base Memory to ***256 MB*** and press ***Next*** (Figure 3)

6. Decrease the Virtual Hard Disk to ***500 MB*** and press ***Next*** (Figure 4)

7. At the summary screen, press ***Finish*** (Figure 5)

8. Start the TinyCoreLinux VM

> NOTE: Some testers had to explicitly tell the VM to capture their mouse commands. To do this, navigate to the VM menu at the top of the VM window and under ***Input*** open the drop-down menu and select ***Mouse Integration*** (Figure 6)

> NOTE: Remember – to release the mouse from a VirtualBox VM – press the right-side ***ctrl*** key

9. Use the arrow keys to select ***Boot Core with X/GUI (TinyCore) + Installation Extension*** (Figure 7)

10. Press ***enter*** to start the boot process in this mode

11. Once it starts (takes a few seconds), you will see the main screen. At the bottom of the screen, you can hover your mouse over the icons and right-click the ***Install*** icon (Figure 8)

12. Manage the settings in the Tiny Core Installation menu (Figure 9)

    12.1. Select ***Whole Disk***

    12.2. Highlight ***sda*** as the disk

    12.3. Select ***Install boot loader***

    12.4. Press the ***right arrow*** at the bottom of the settings to go to the next menu

13. Leave the formatting options at their default and press the ***right arrow*** (Figure 10)

14. In the boot options reference list, type the following in the blank field at the bottom (Figure 11)

```
home=sda1 opt=sda1
```

15. Press the ***right arrow***

16. On the Install Type menu, leave the defaults and press the ***right arrow*** (Figure 12)

17. Review the installation information and press ***Proceed*** (Figure 13)

18. When the installation has finished (Figure 14), shut down the VM (Figure 15)

19. Return to the VM VirtualBox manager and adjust the settings for the TinyCoreLinux VM by clicking on ***settings*** (Figure 16)

20. In settings, navigate to ***Storage***, right-click the iso, and click ***Remove Attachment*** (Figure 17). This forces the VM to boot from the virtual hard disk instead of the iso

21. Click ***OK***

22. Start the TinyCoreLinux VM to ensure it boots from the virtual hard drive. Notice that the ***Install icon*** no longer appears (Figure 18)

Phase II – Creating persistance in Tiny Core Linux

Tiny Core Linux discards all changes made when it shuts down. This is great for getting a fresh start but can be a pain when we want to keep something. To persistently save material when the VM shuts down, we need to use the backup feature. In this section, we will create a test file and use the backup feature to keep the information.

1. Start the TinyCore Linux or resume from the install

2. On the main page, click on the third icon ***Control Panel*** (Figure 19)

3. Under the maintenance section, click ***Backup/Restore*** and another window will open. Click on ***Included for Backup (.filetool.lst)*** and you can see which directories and files are saved automatically on shutdown with backup (Figure 20)

4. According to this information, files saved in the ***opt*** and ***home*** directories will be backed up

5. Close the windows

6. Open a blank text file by clicking on the ***editor icon*** (Figure 21)

7. Type in anything in the textbox and then use the mouse to select ***File –> Save File As…*** (Figure 22)

8. In the ***File Save As*** window, leave the default settings and add the file name ***test.txt*** (Figure 23), and click ***ok***

9. Now click on the ***Exit icon*** at the bottom, and on the ***exit options***, select ***Reboot*** and backup options ***Backup*** and then press ***ok*** (Figure 24)

10. After the VM restarts, open the editor again, and this time click ***File –> Open File***. In the new window, you should see the file you saved earlier (Figure 25)

11. You can open it again if you want, but seeing it listed is good enough to know that data persistence via backup is working

End of Lab

List of Figures

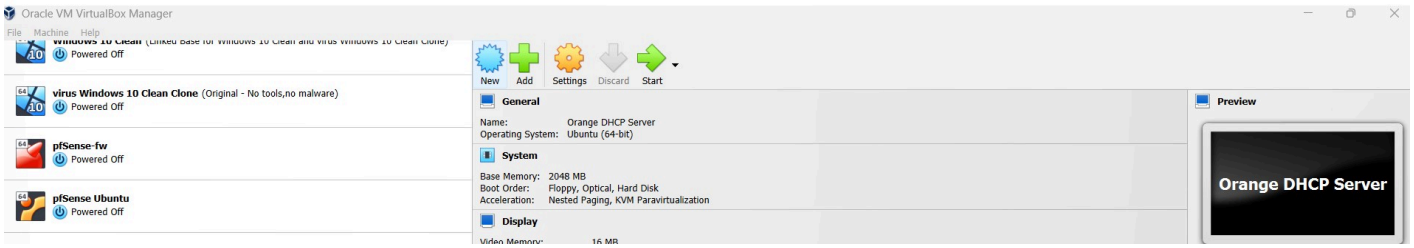


Figure 1 – Create a new VM

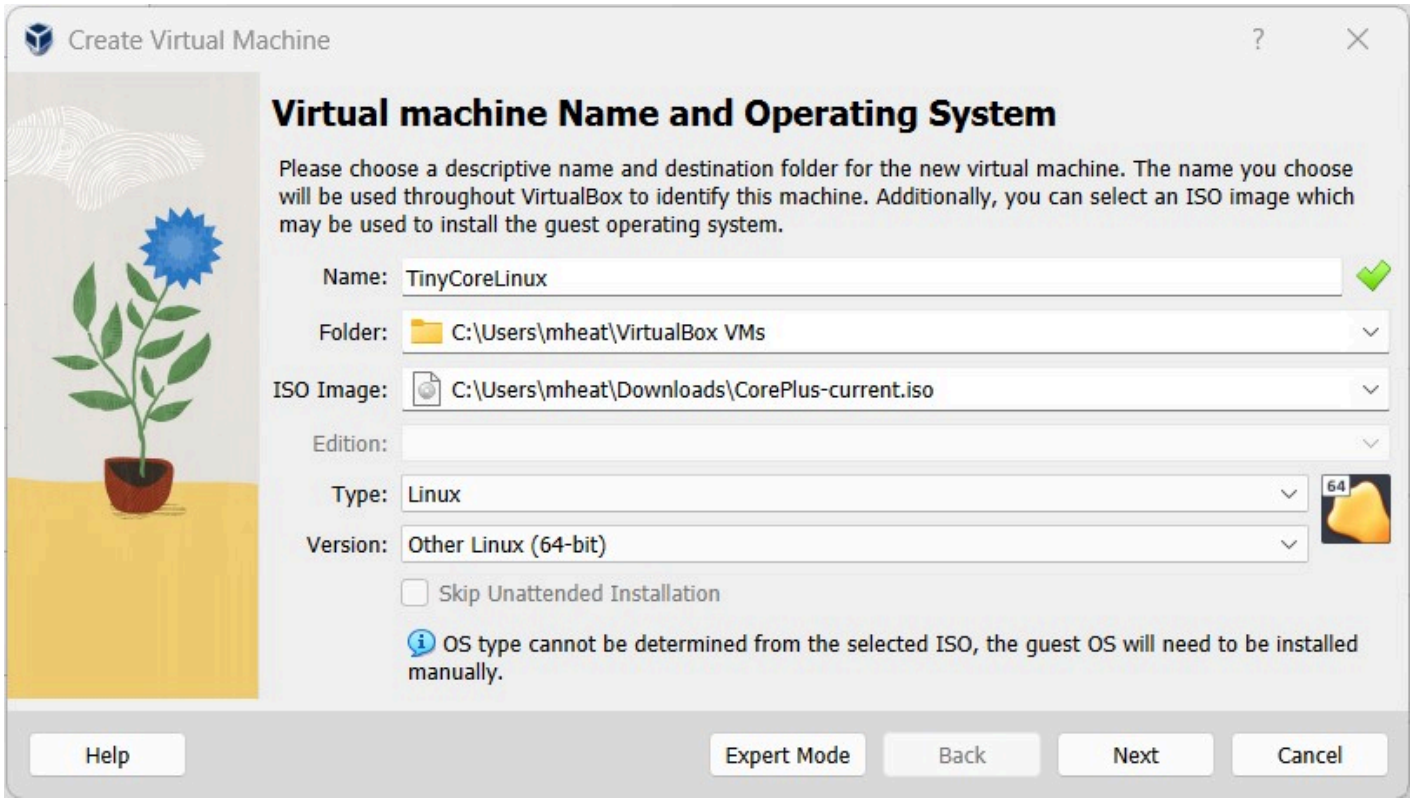


Figure 2 – Completing the VirtualBox VM form

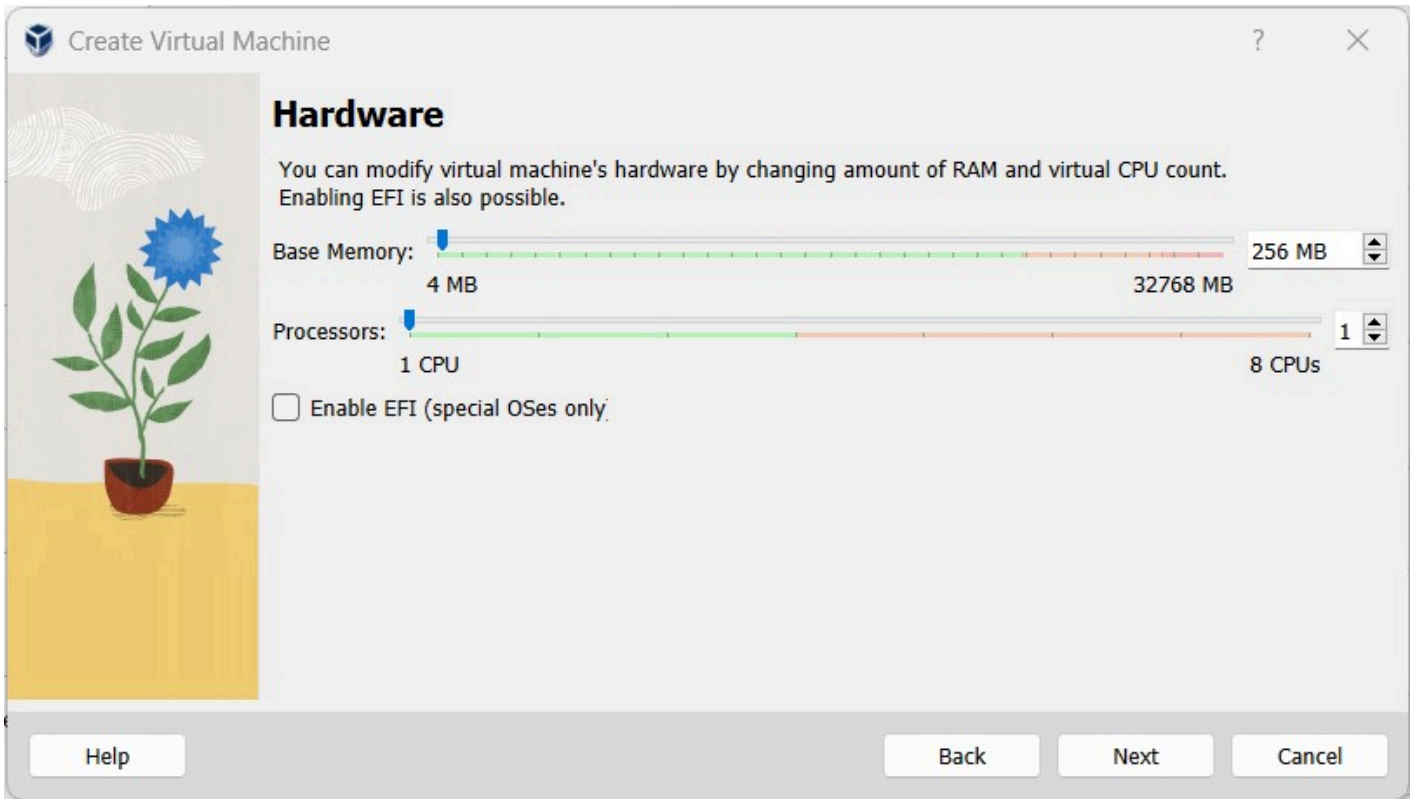


Figure 3 – decrease the memory to 256MB

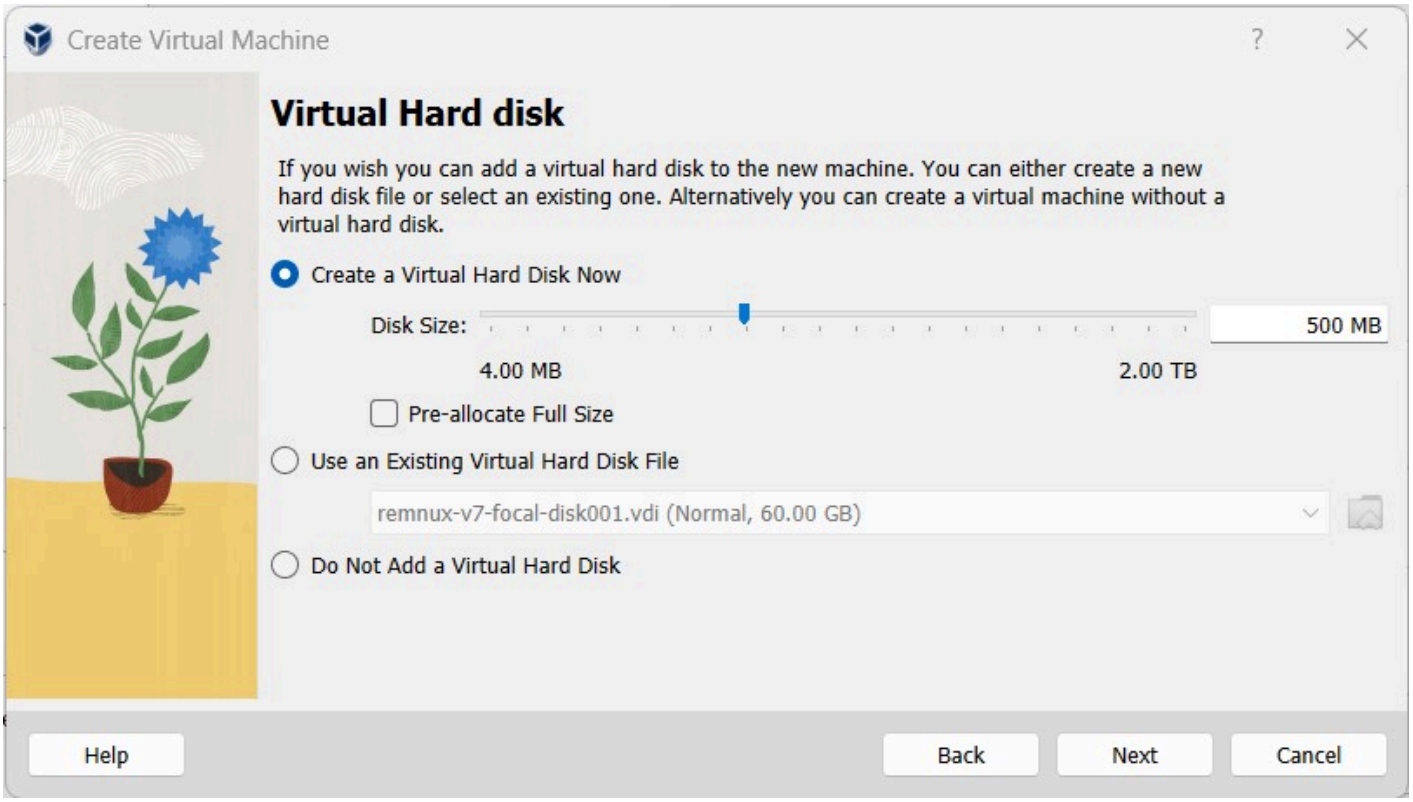


Figure 4 – Decrease the Virtual Hard Disk to 500 MB

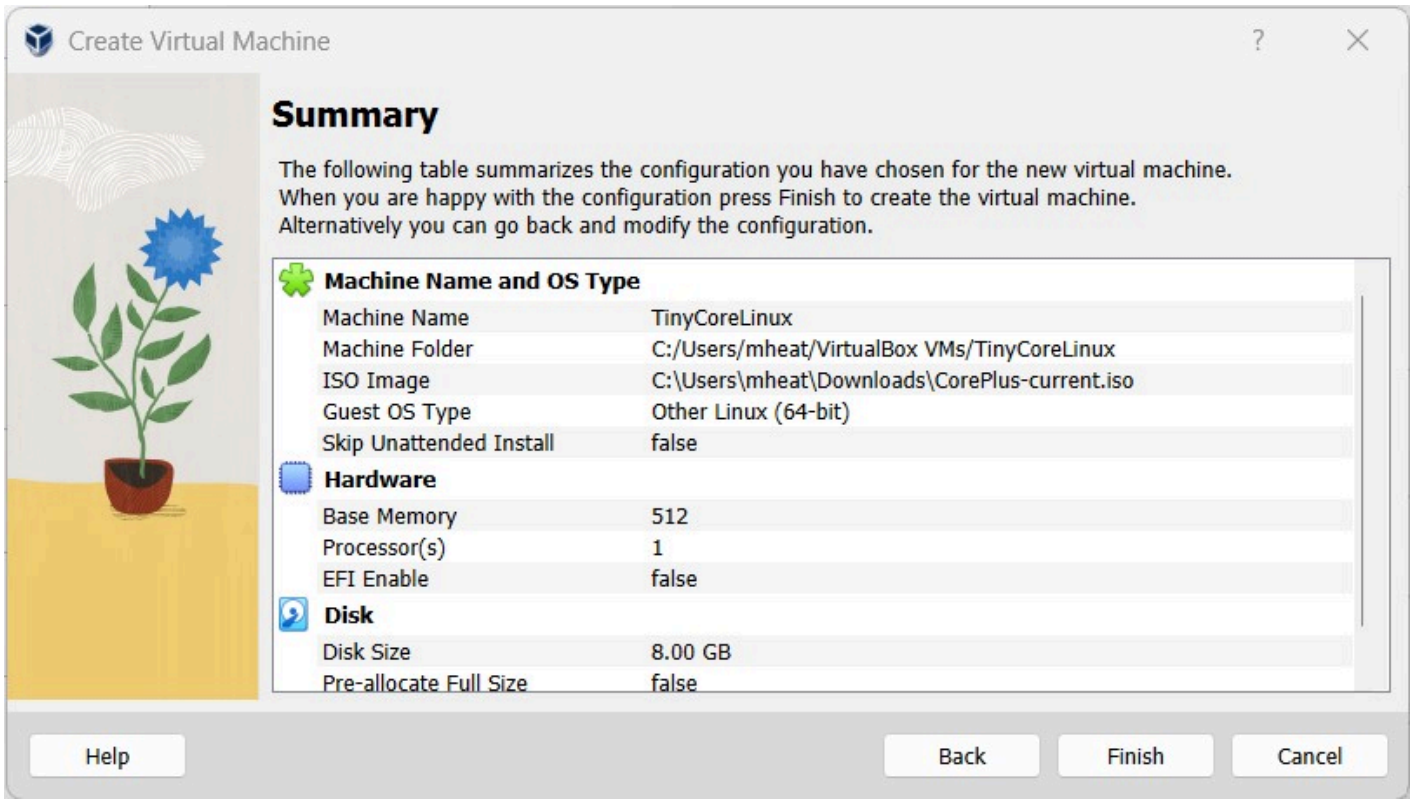


Figure 5 – Finish the VM changes

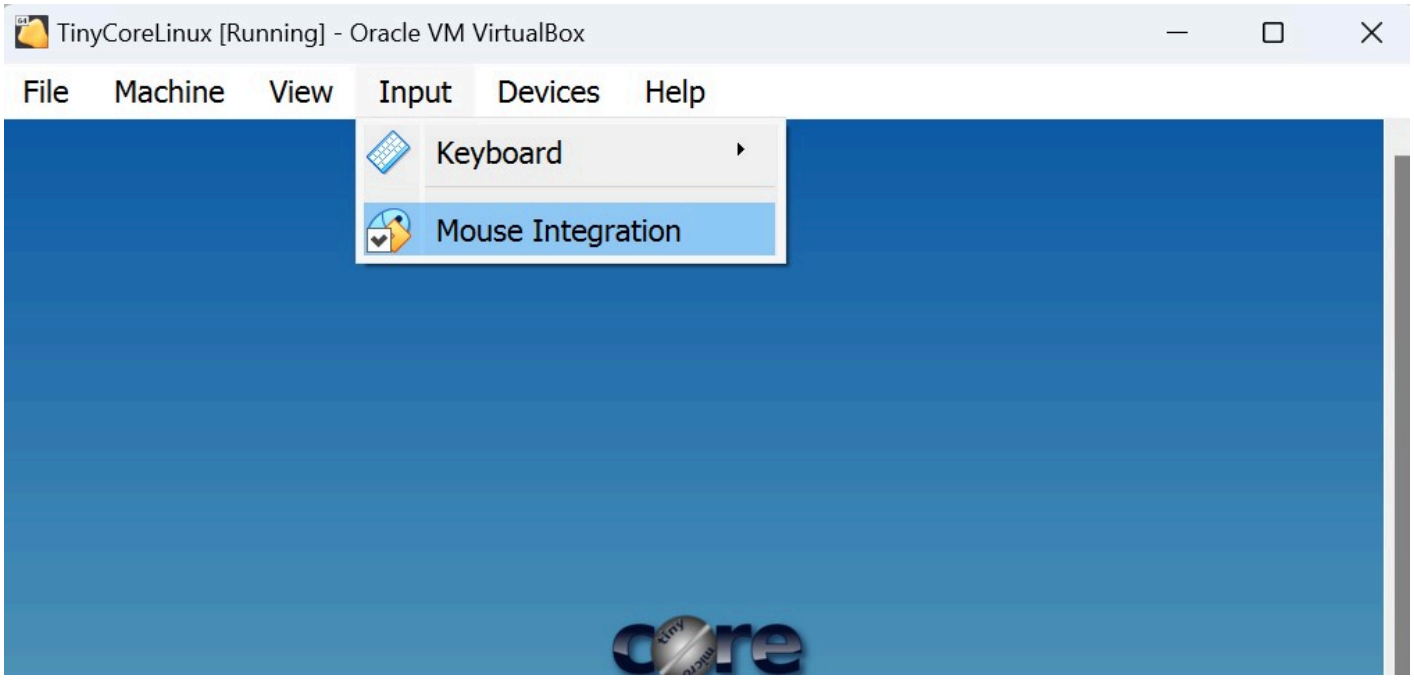


Figure 6 – Mouse integration in VirtualBox VMs

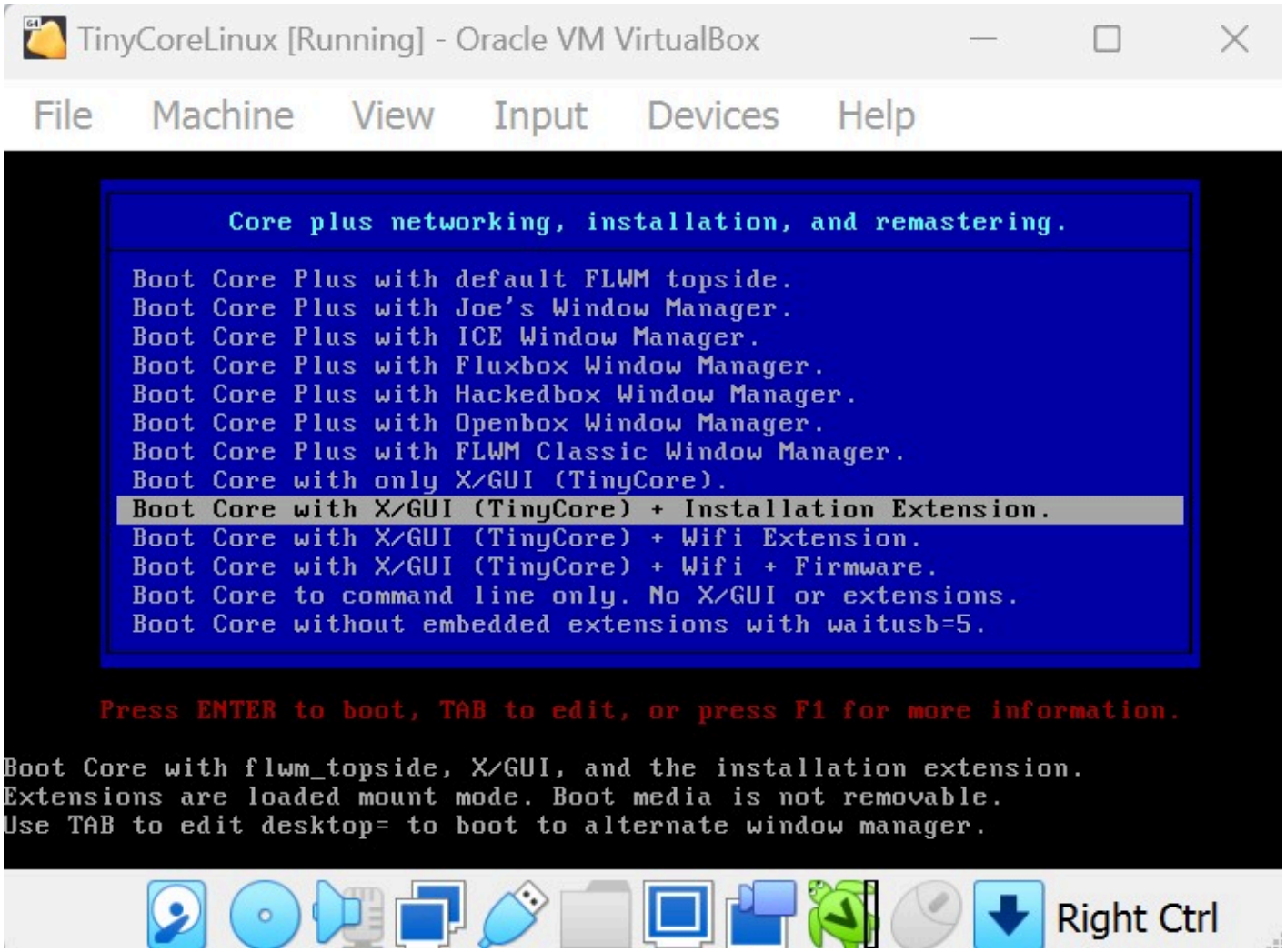


Figure 7 – First time boot instructions for TinyCore Linux

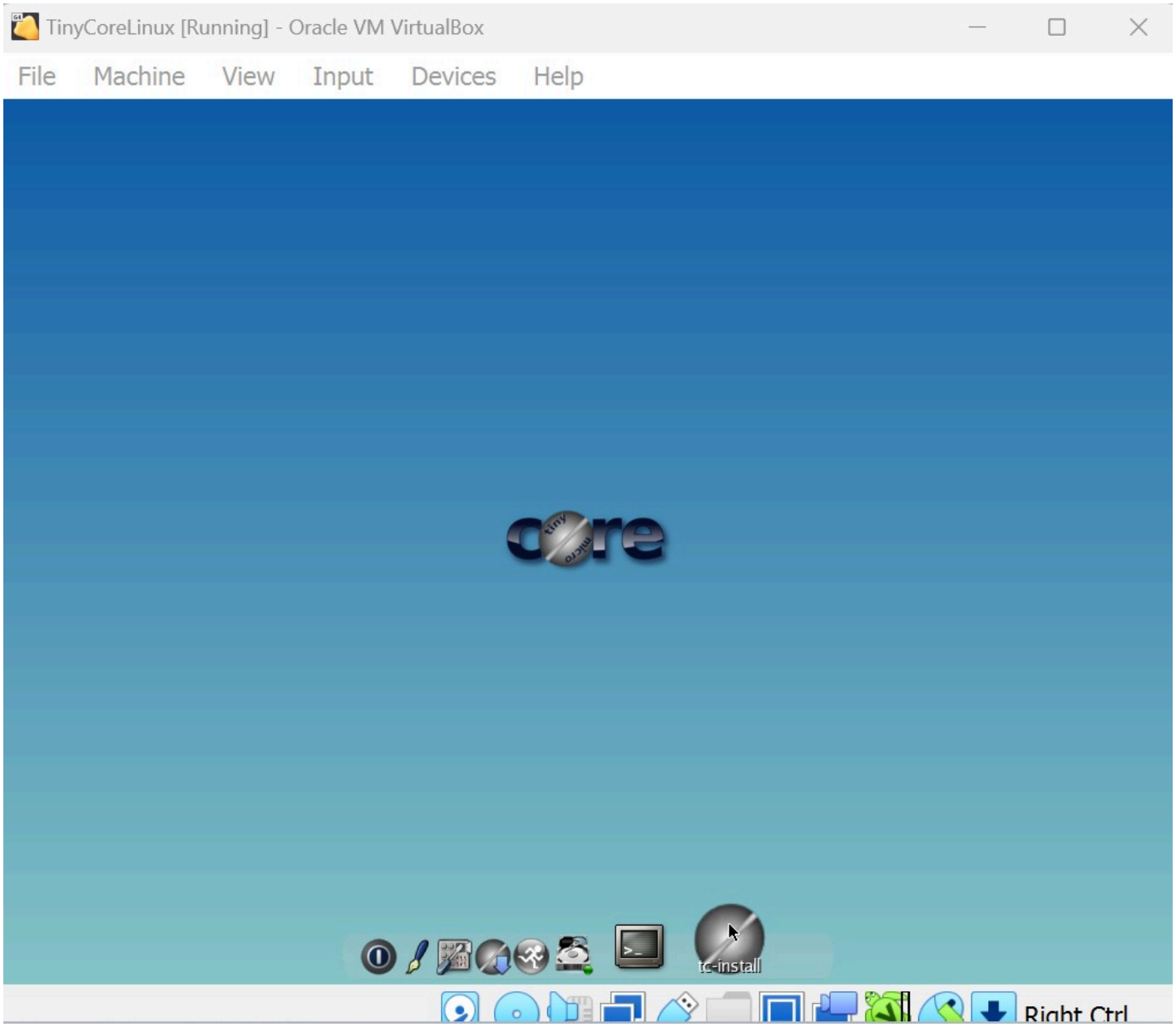


Figure 8 – Install TinyCore Linux

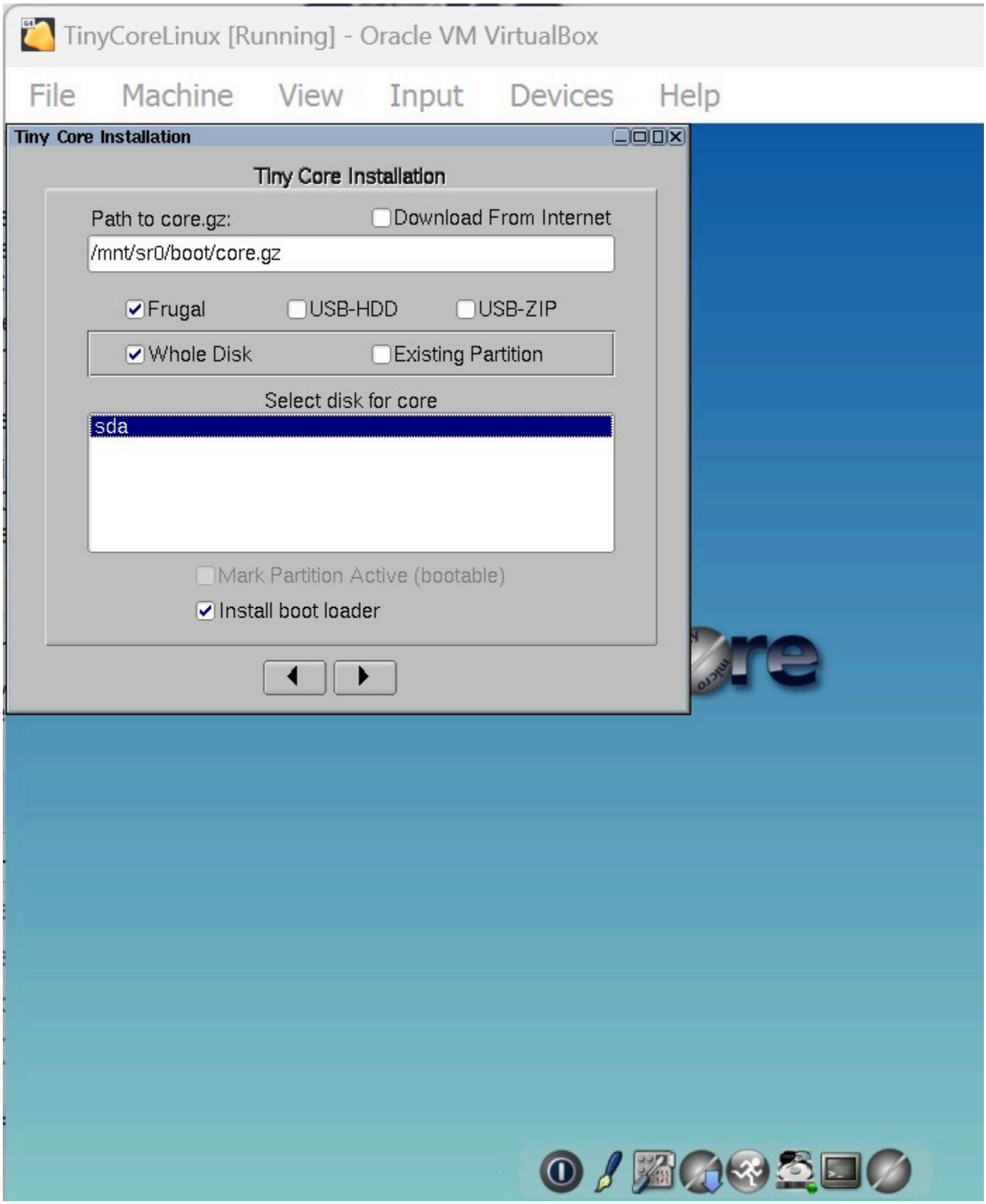


Figure 9 – Managing the settings in TinyCore installation menu

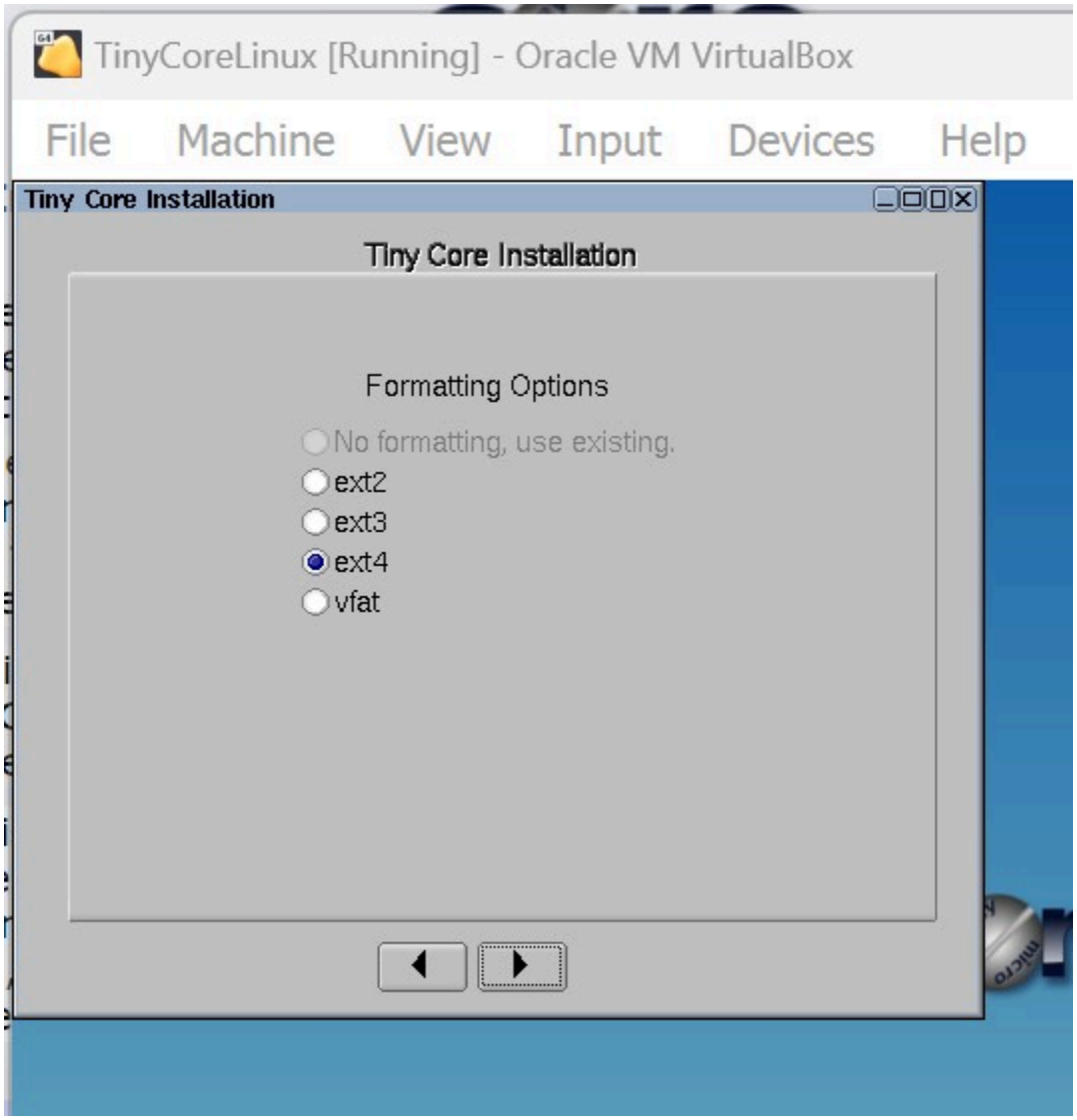


Figure 10 – Leave the formatting options alone

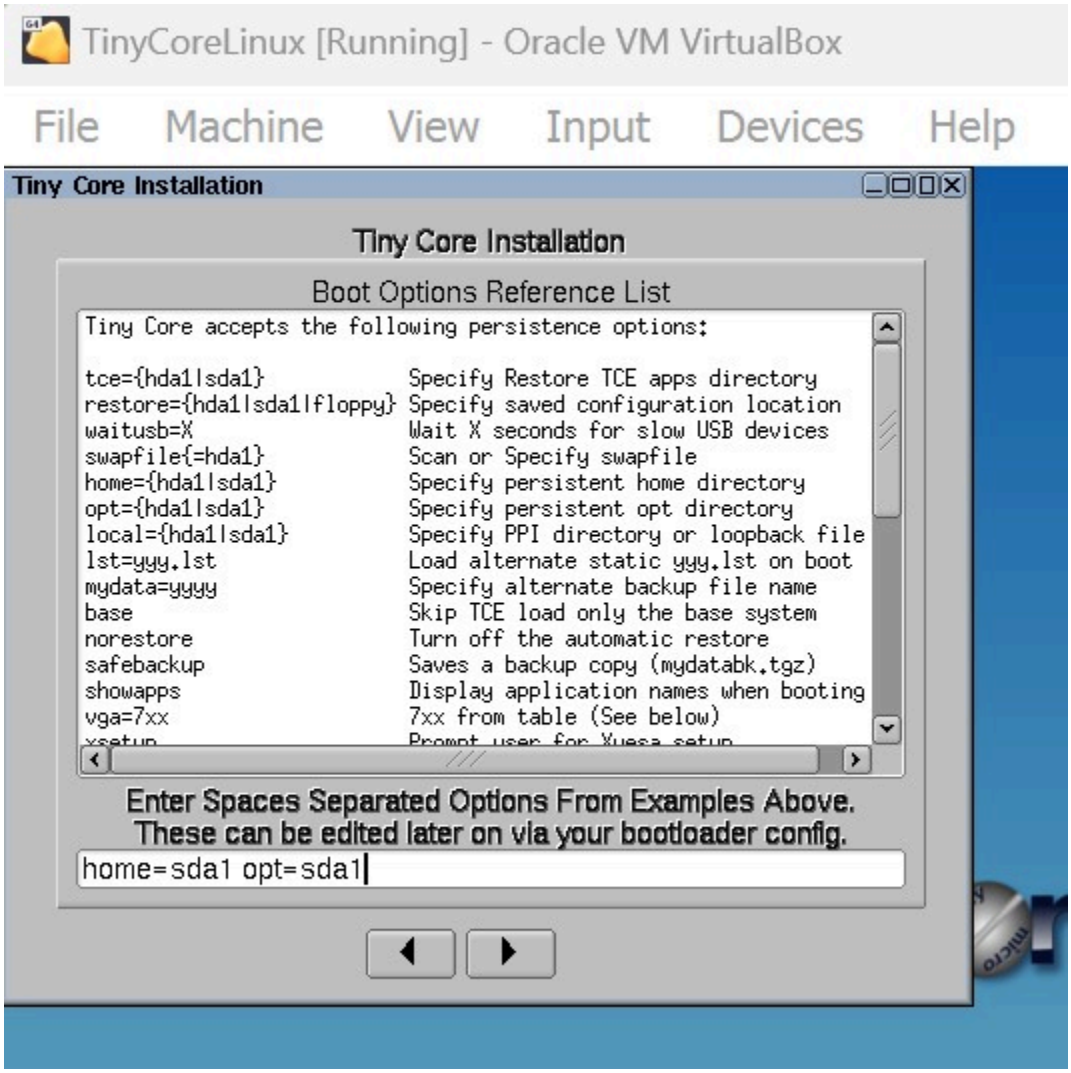


Figure 11 – Set the home and optional drives to use by default

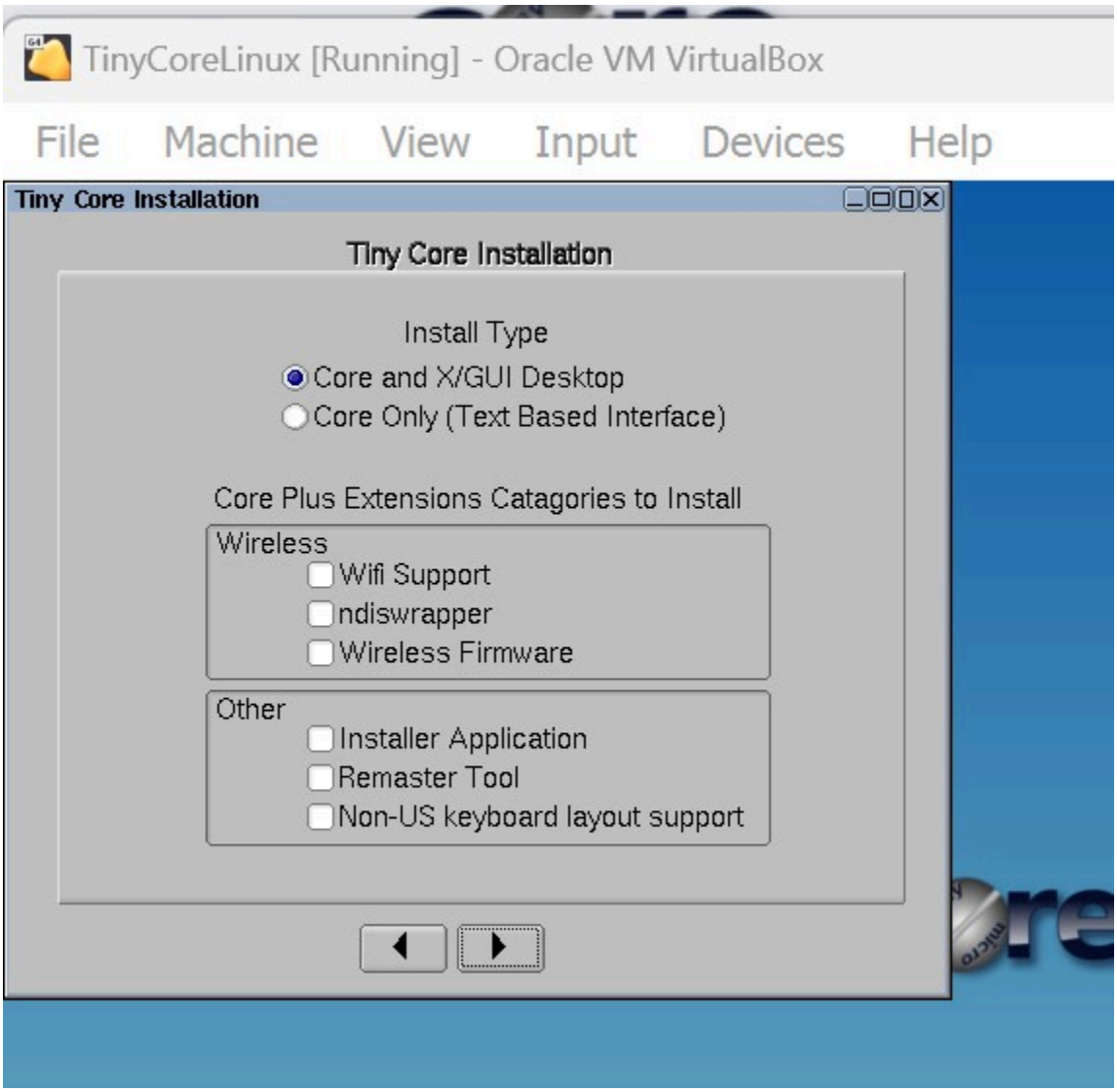


Figure 12 – Leave the install type defaults

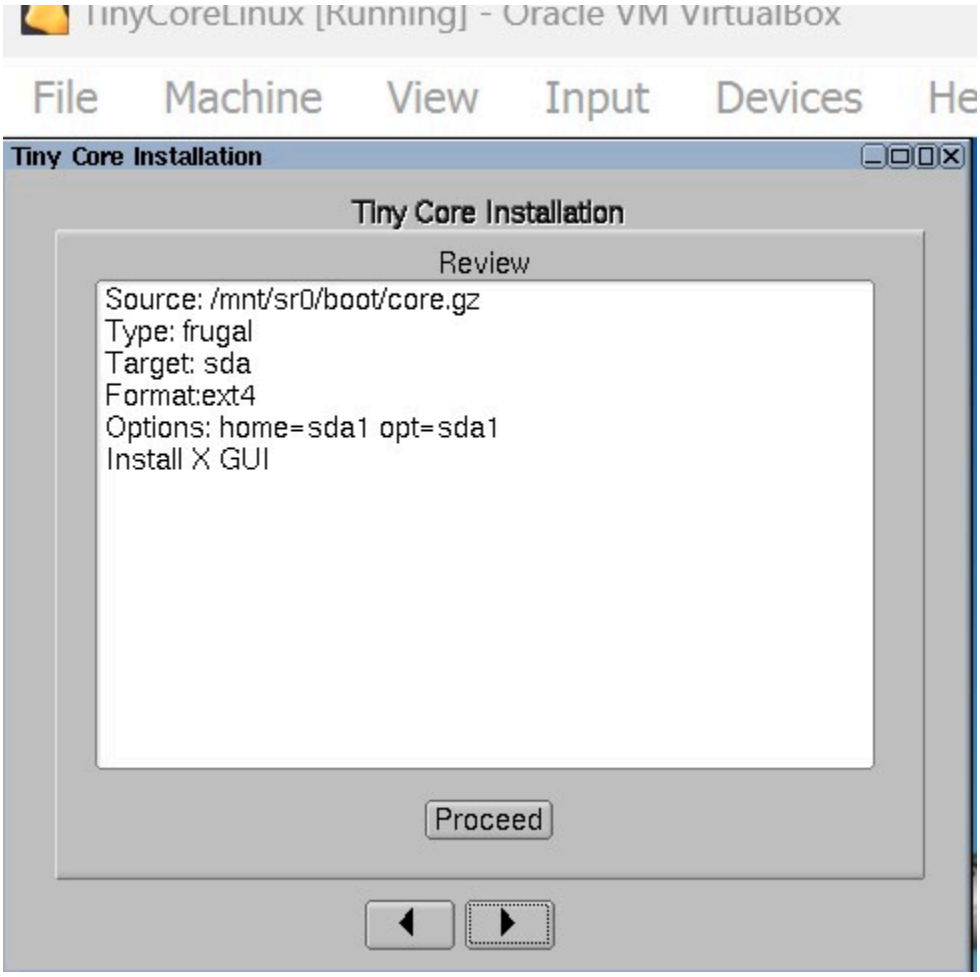


Figure 13 – Review the installation information before proceeding

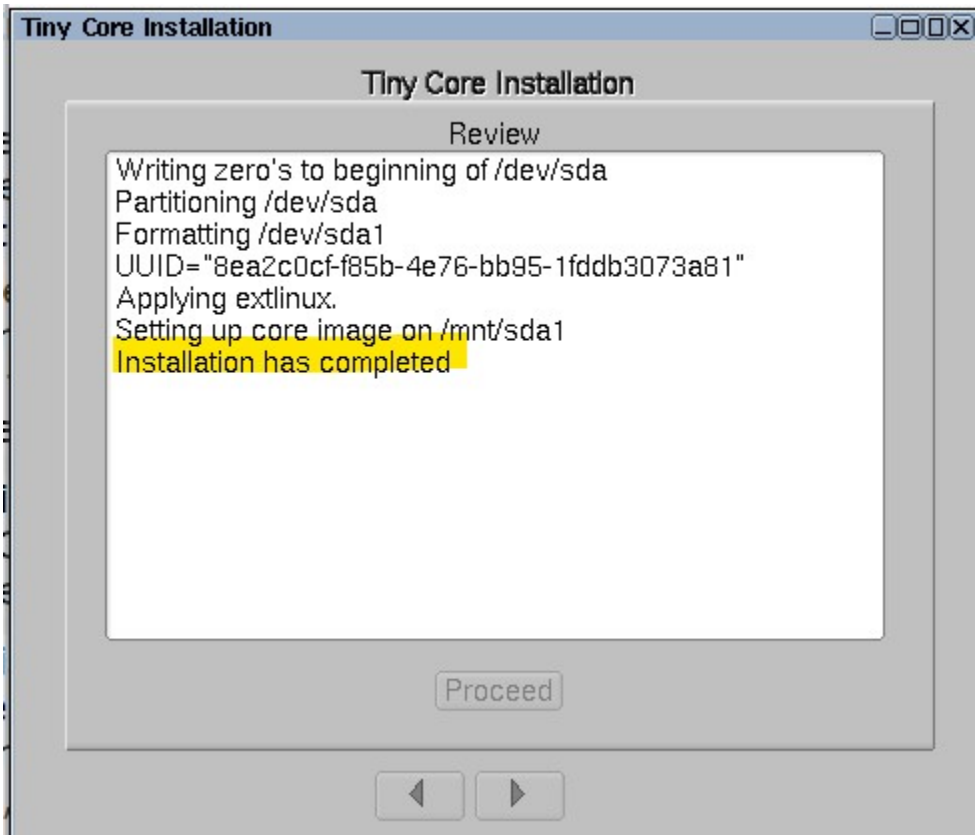


Figure 14 – Installation indicates finished

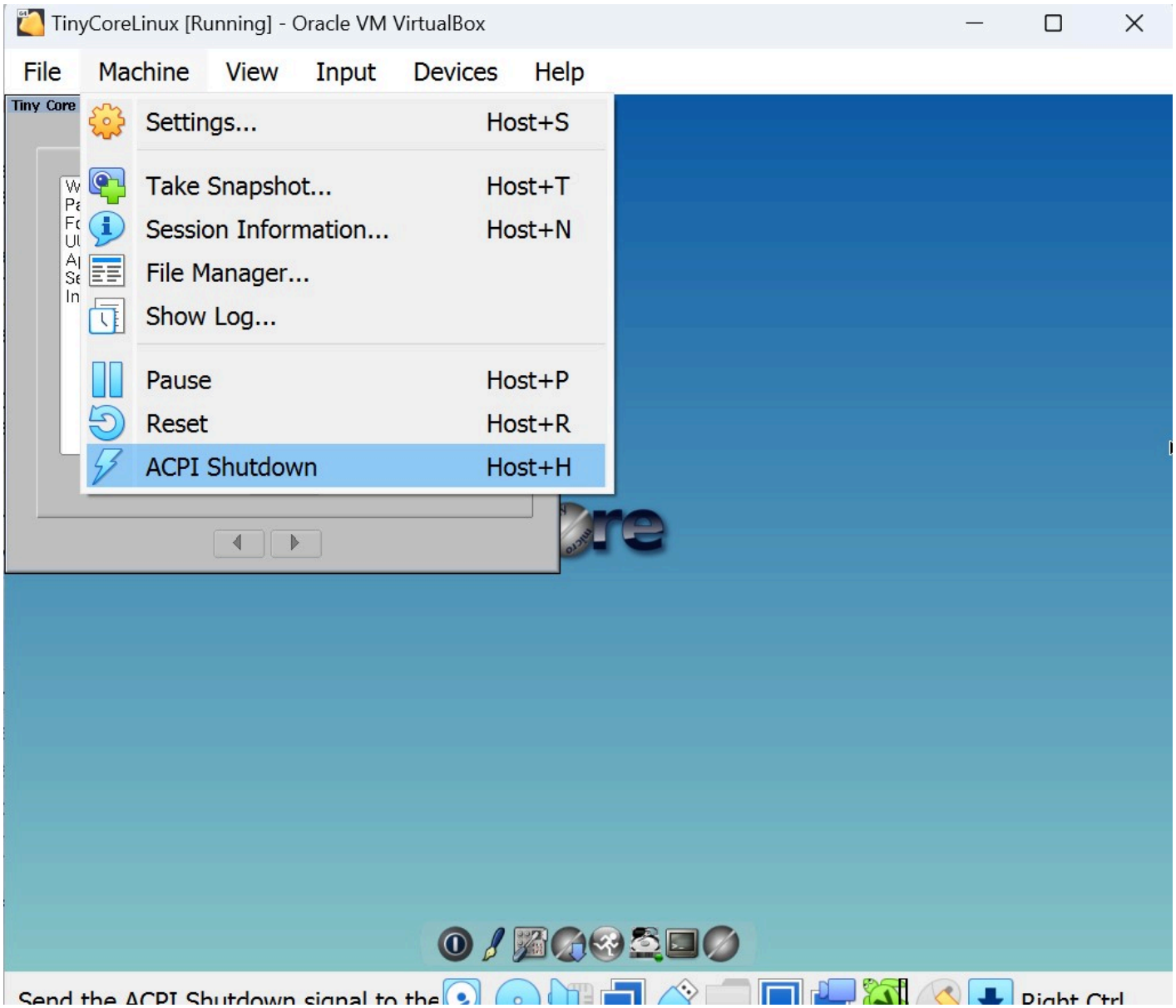


Figure 15 – Shut down the VM from within the VM

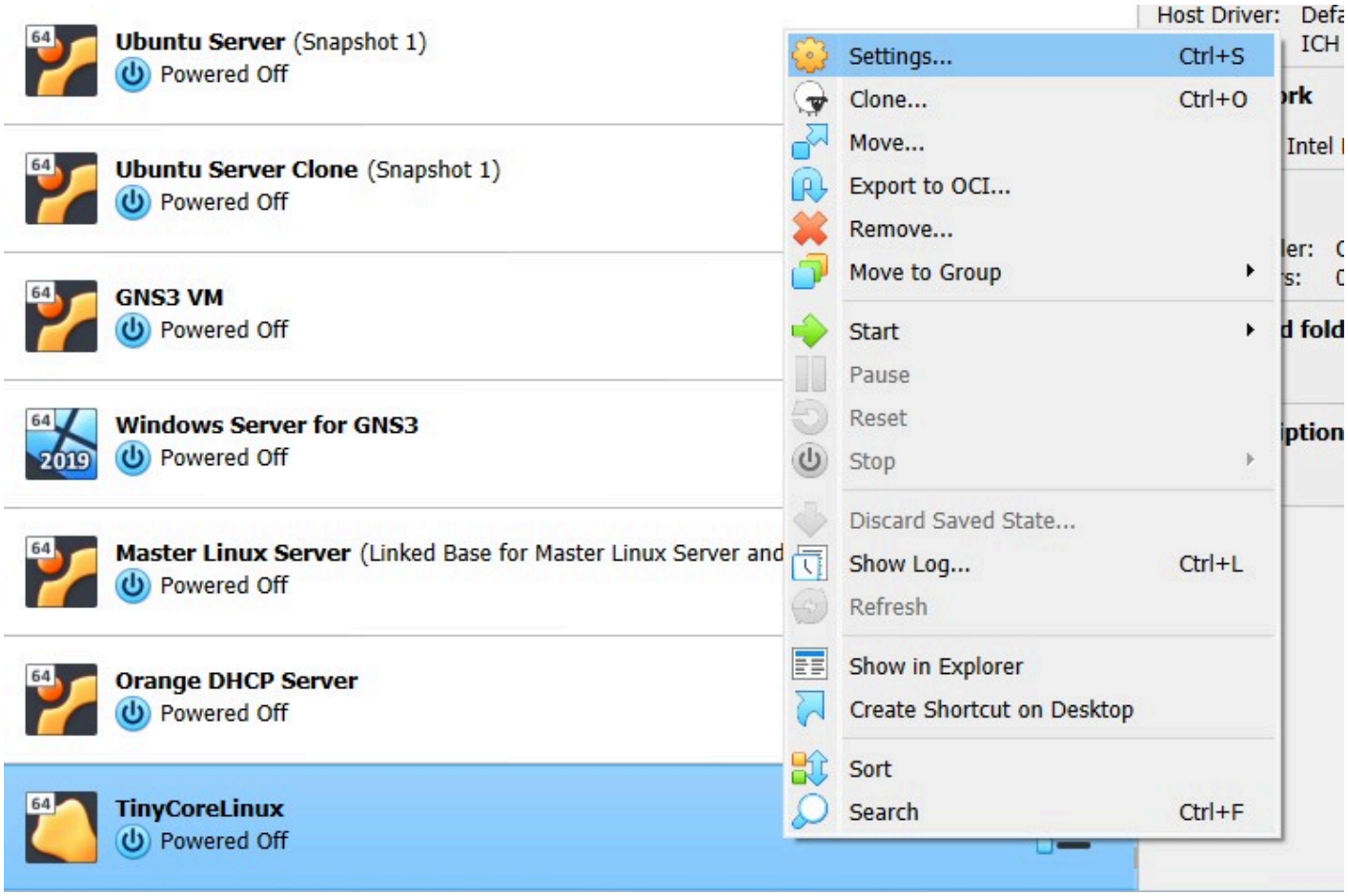


Figure 16 – Configuring the VM again

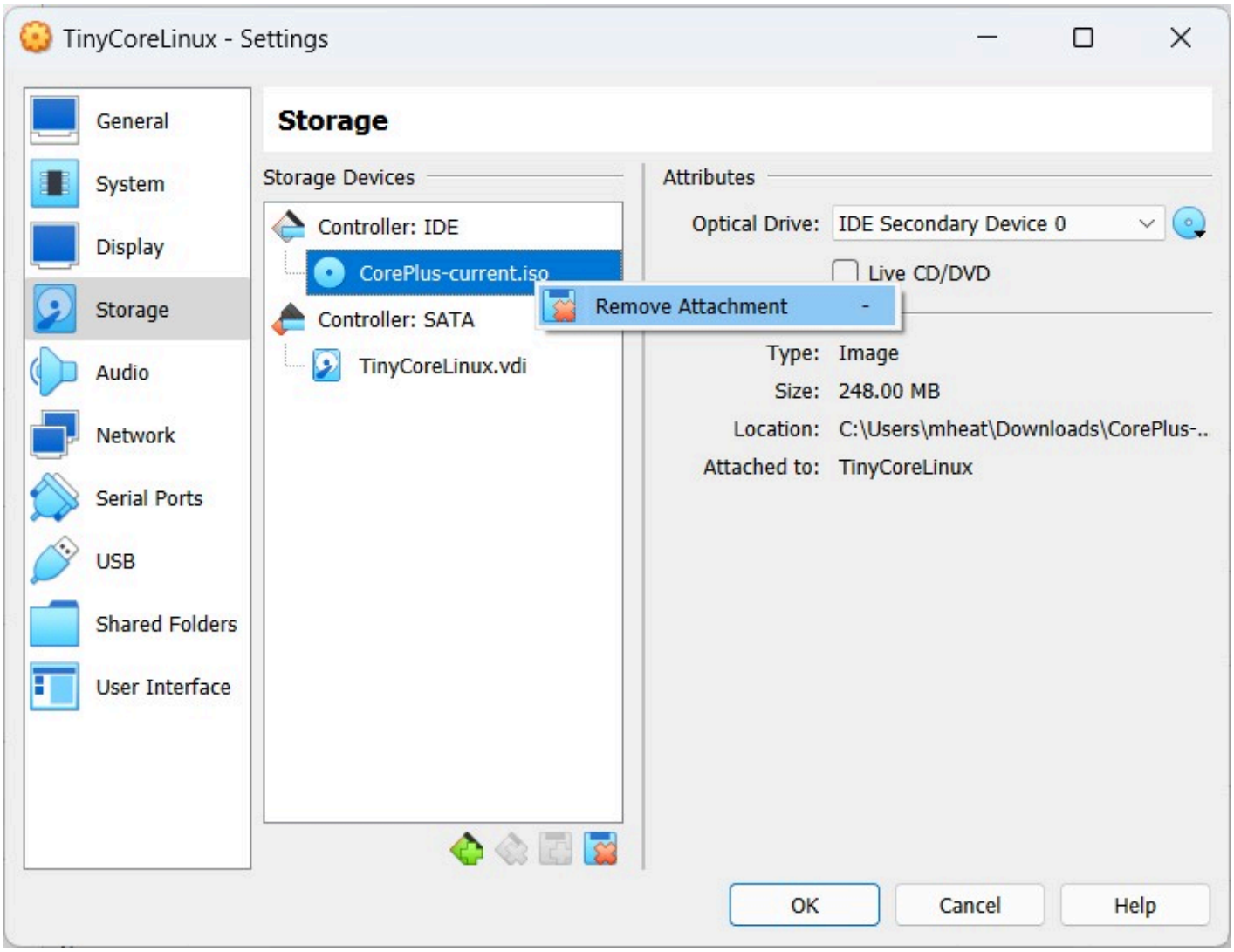


Figure 17 – Remove the booting iso image

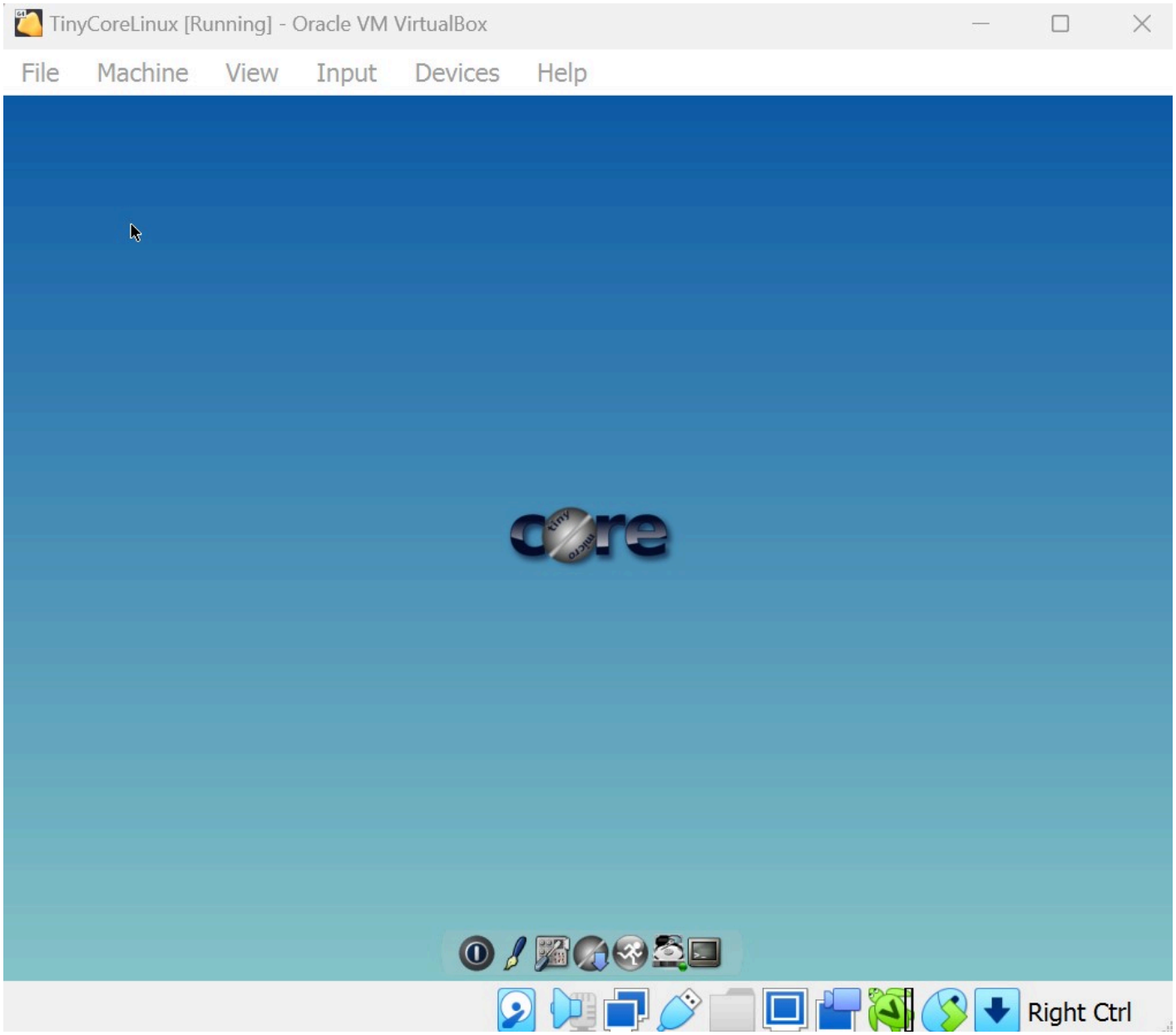


Figure 18 – The install icon no longer appears which means it is booting from the virtual drive instead of the iso

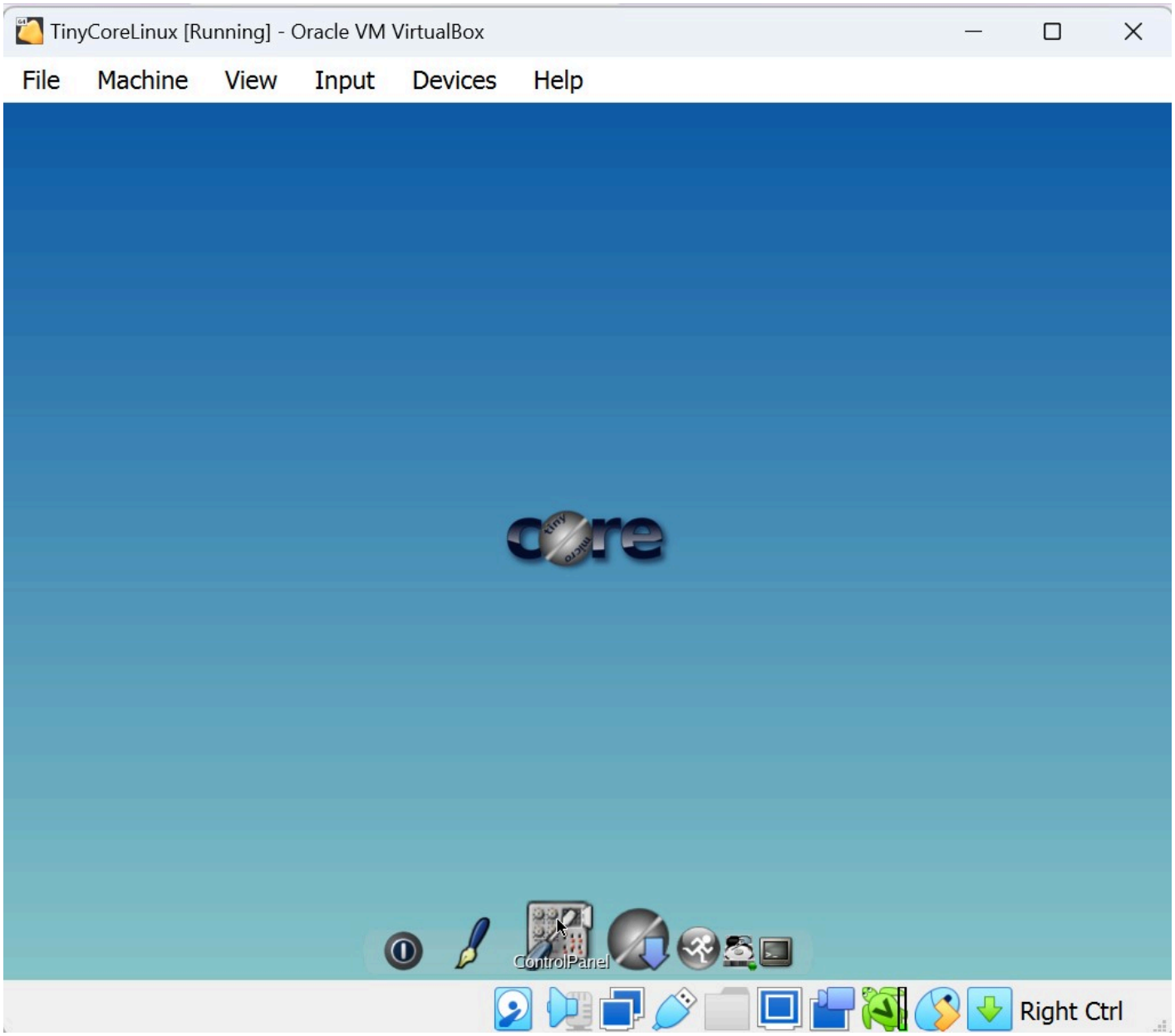


Figure 19 – Configure the TinyCore VM for persistence

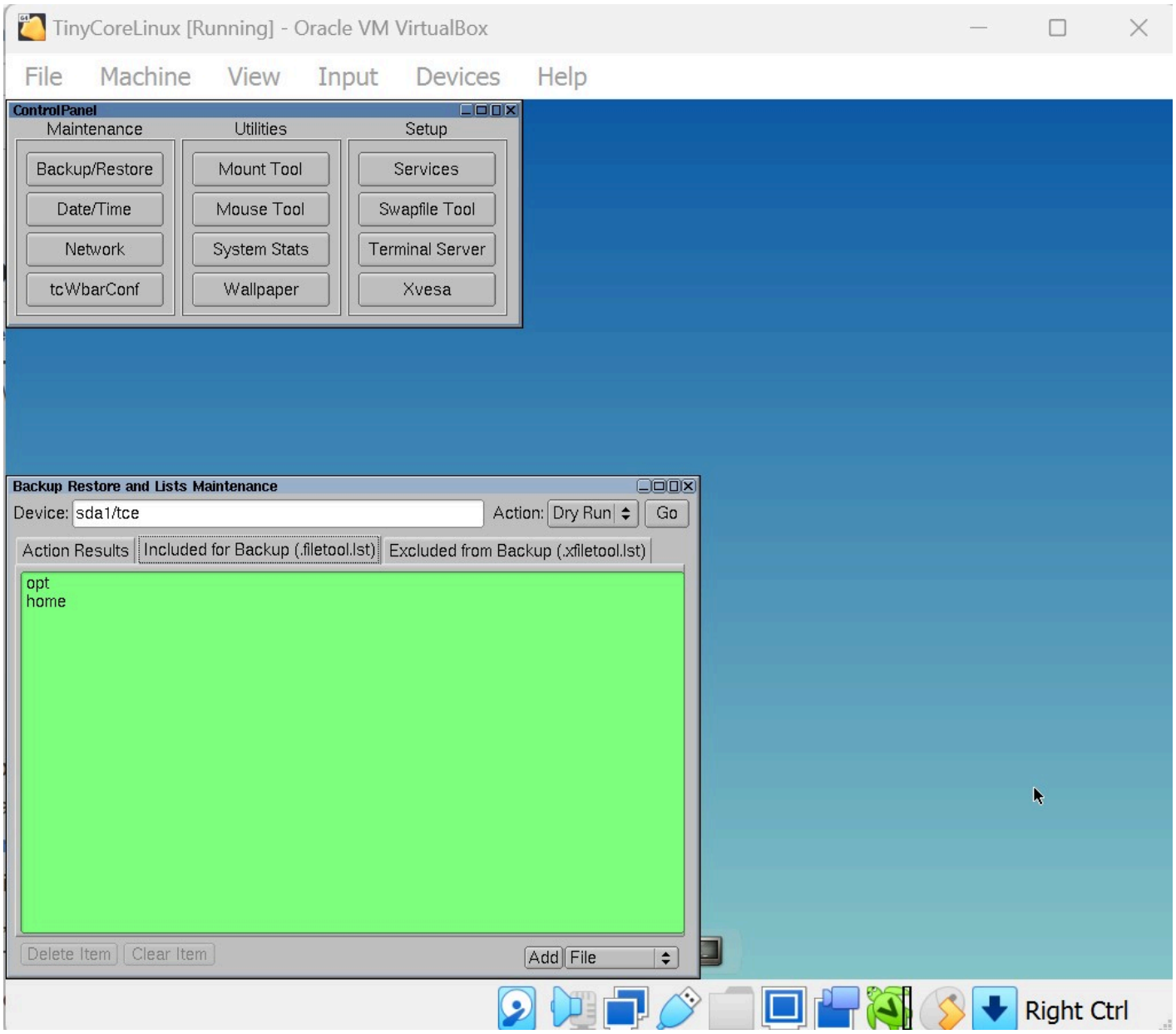


Figure 20 – Changing the backup/restore settings

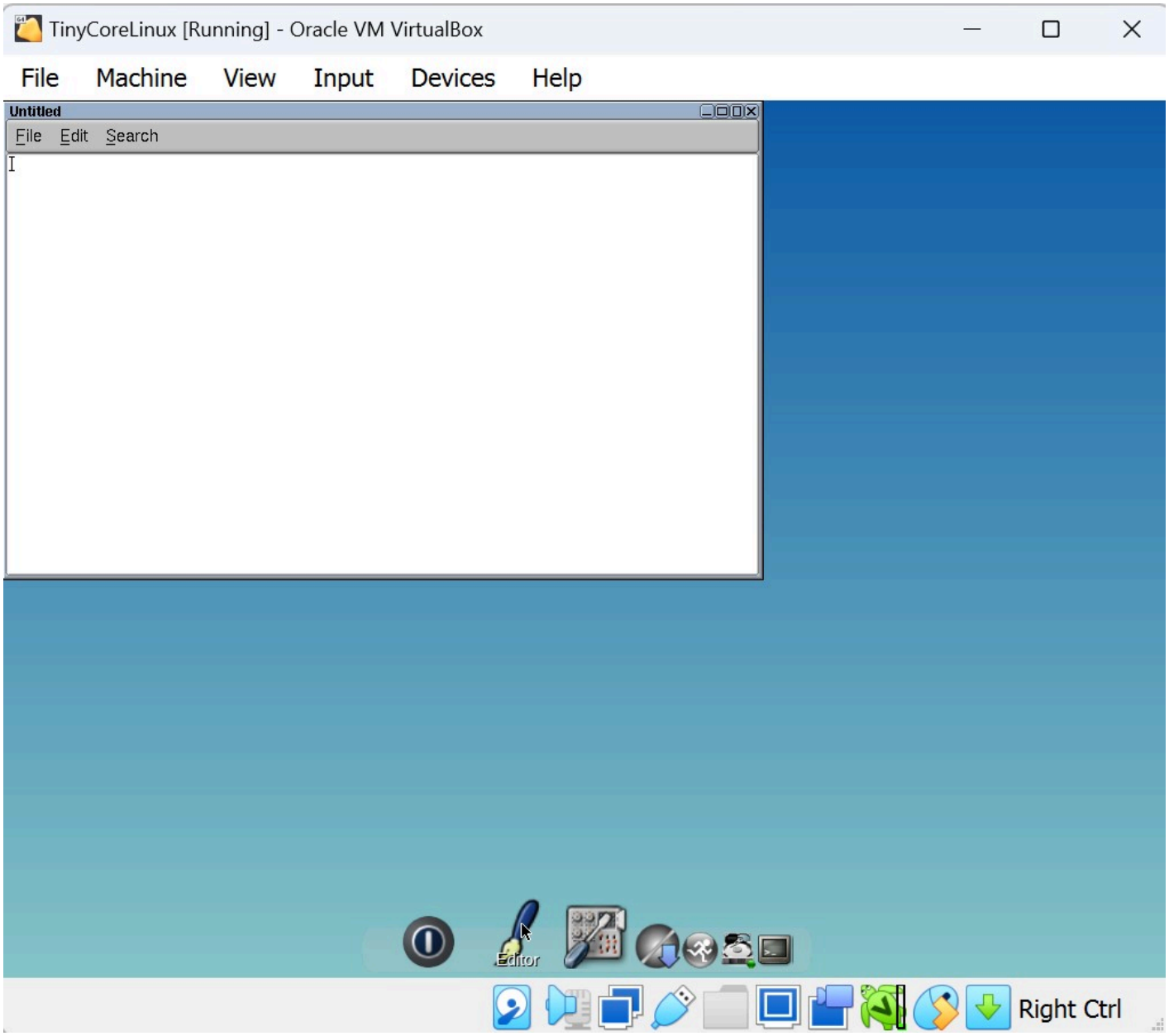


Figure 21 – Open a blank text file

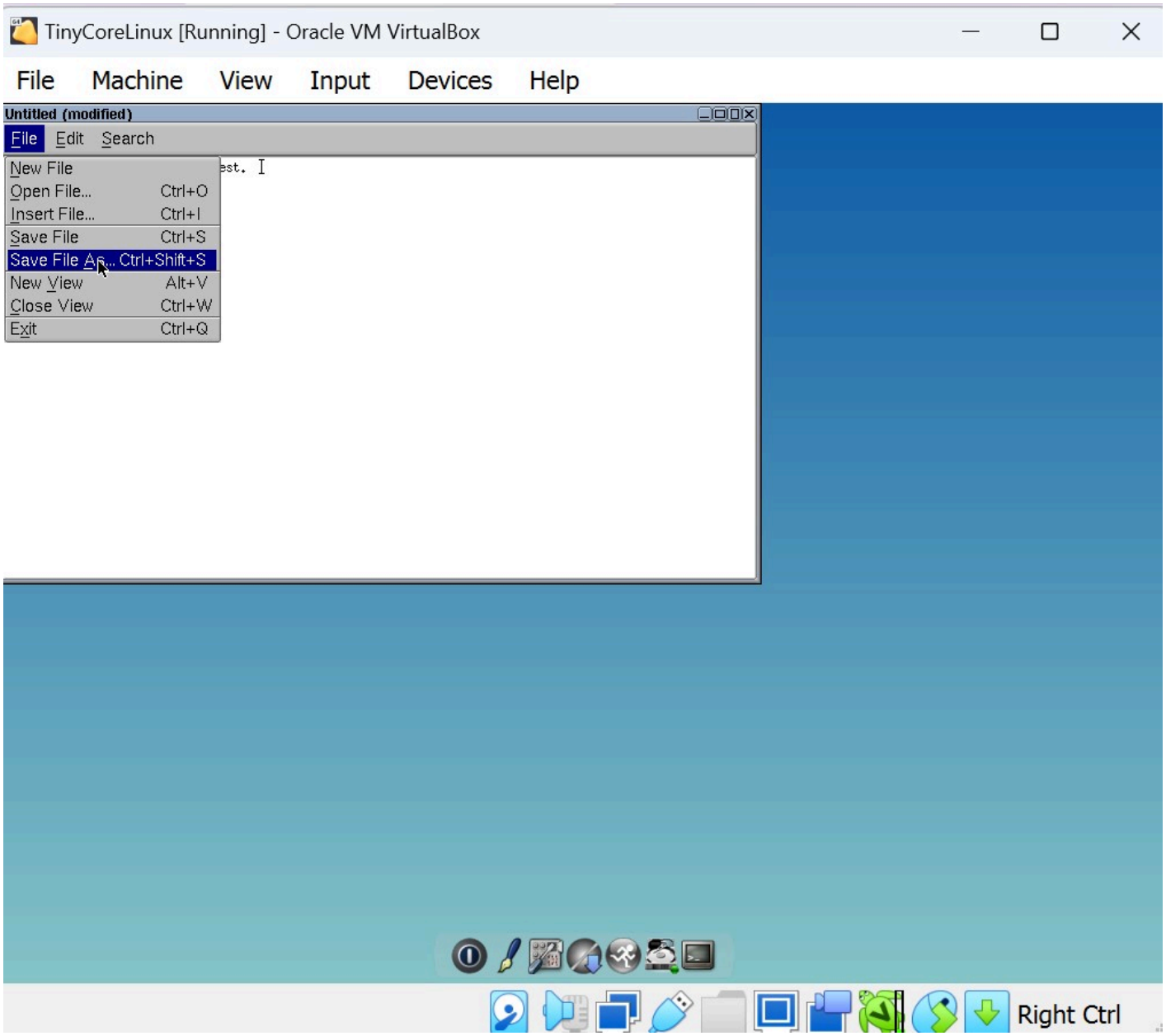


Figure 22 – Type anything and save the document

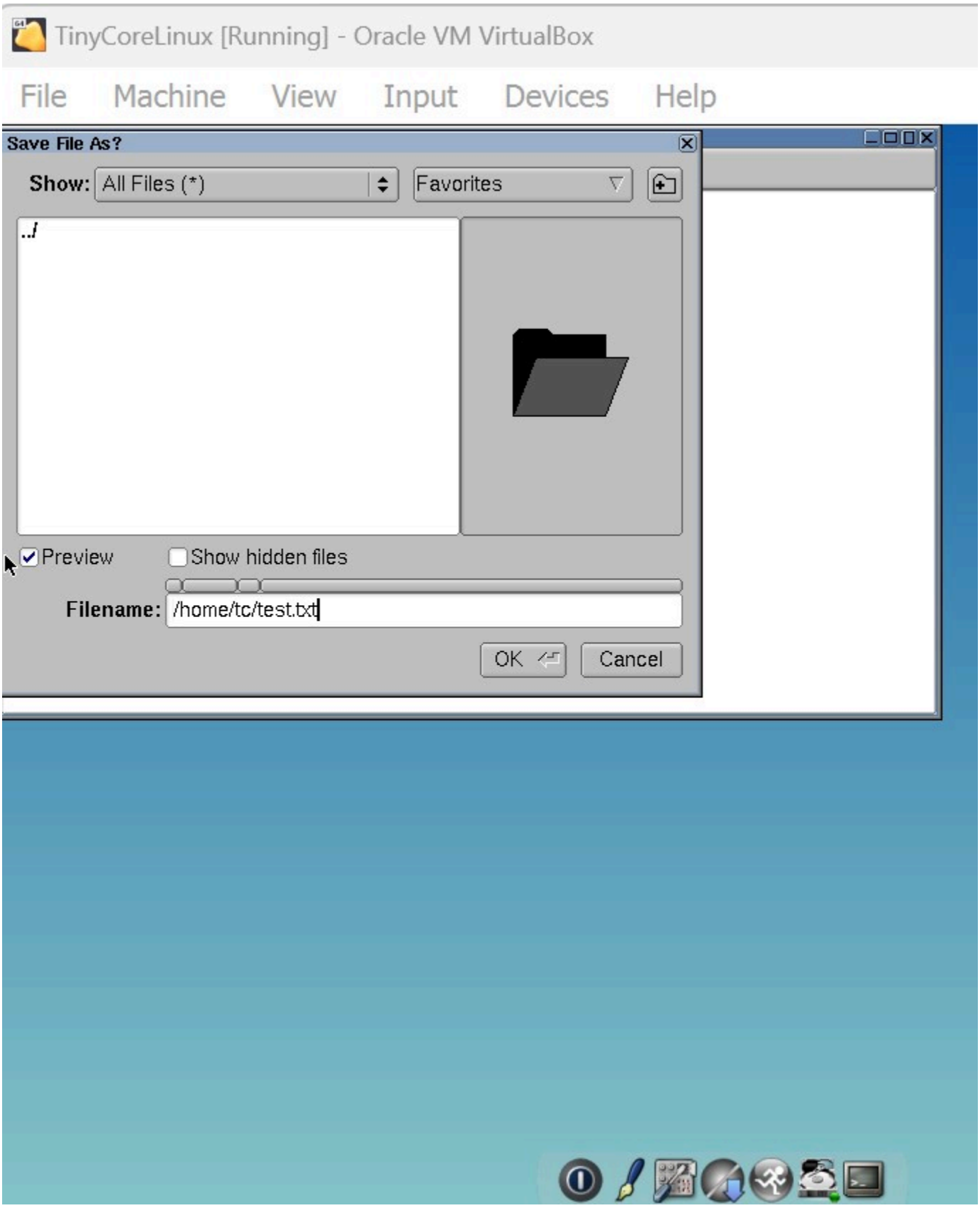


Figure 23 – Save the text file

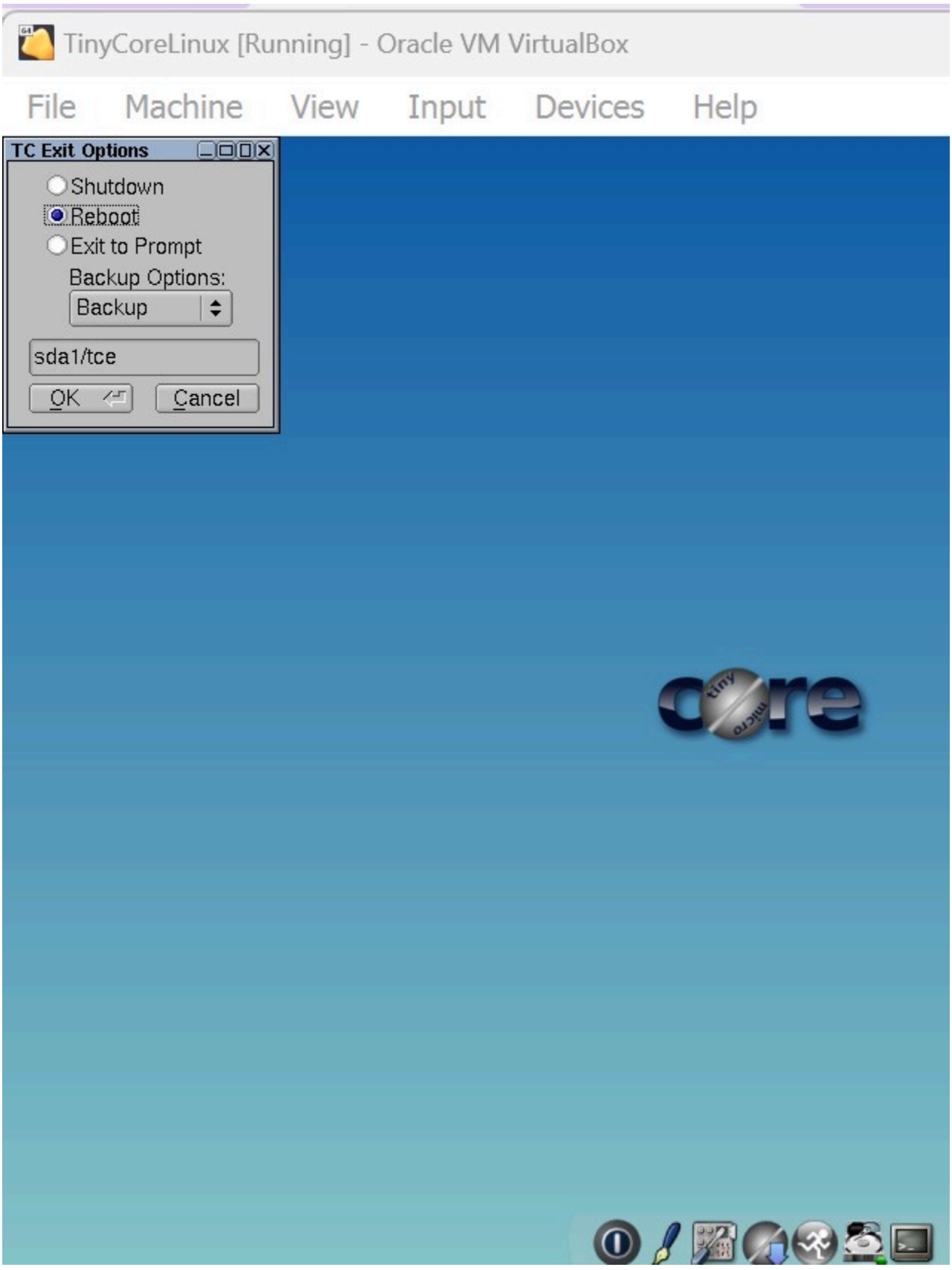


Figure 24 – Reboot and Backup

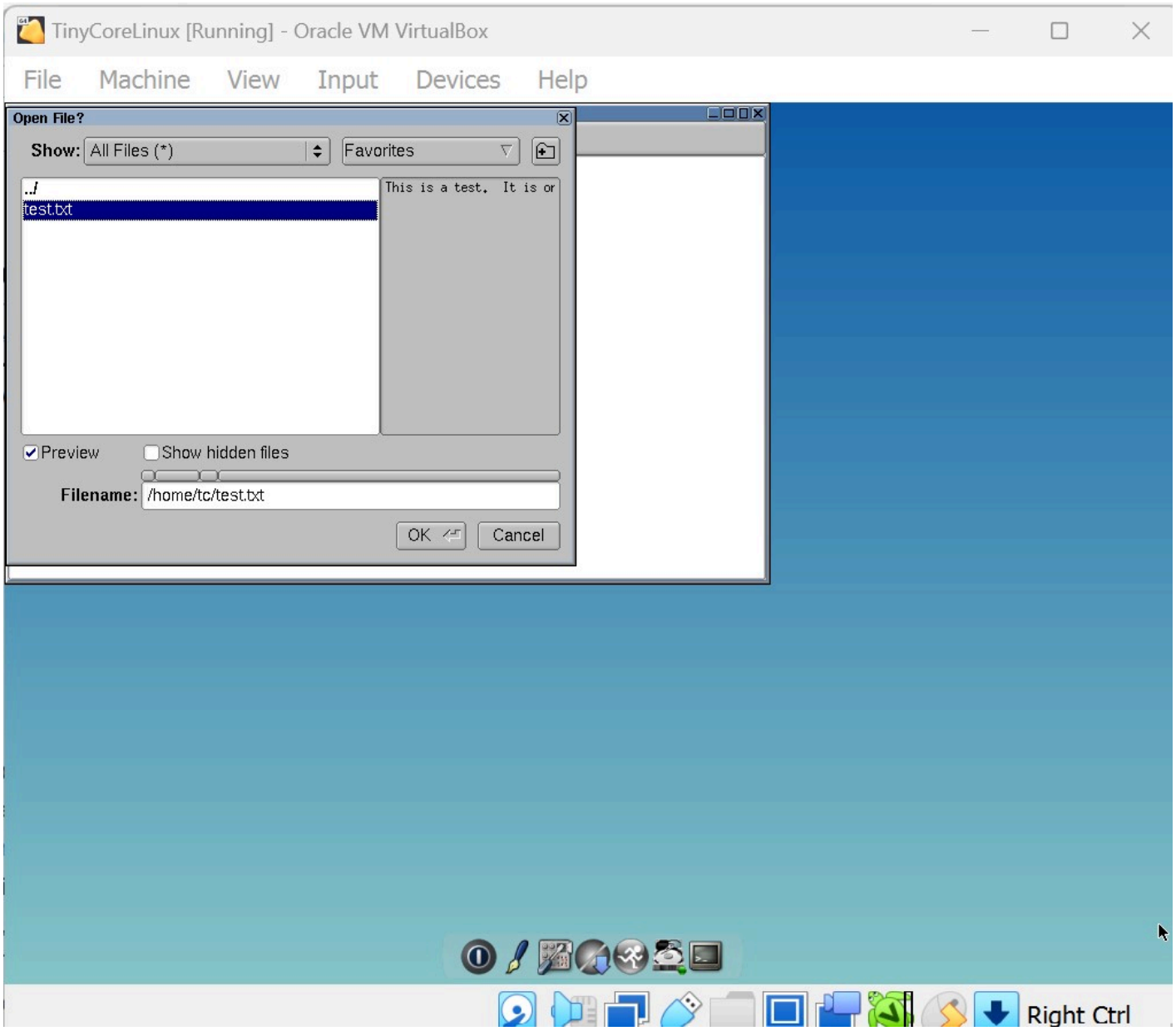


Figure 25 – Checking to see the file was retained after reboot

CHAPTER 6

Adding a Virtual Machine to GNS3

MATHEW J. HEATH VAN HORN, PHD

GNS3 is unique from other simulators such as Cisco's Packet Tracer. With GNS3, you can add any VM you create in VirtualBox and use it within the GNS3 environment. The purpose of this lab is to give you experience in creating GNS3 appliances using VMs

LEARNING OBJECTIVES

- Create GNS3 appliances using VirtualBox VMs

PREREQUISITES

- Oracle VirtualBox installed with at least one functional VM
- Chapter 2 – Setting up a GNS3 environment

DELIVERABLES

- None – this is a preparatory lab for other labs

RESOURCES

- GNS3 Documentation – https://docs.gns3.com/docs/

CONTRIBUTORS AND TESTERS

- Jacob M. Christensen, C.I.S. Student, ERAU-Prescott
- Cody Shinkyu Park, Honeywell Software Engineer, ERAU-Prescott Alumni
- Evan Paddock, Cybersecurity Student, ERAU-Prescott
- Dante Rocca, Cybersecurity Student, ERAU-Prescott
- Sawyer Hansen, Cybersecurity Student, ERAU-Prescott

Phase I – All the steps required

This is pretty straightforward. In this lab, we are using Windows server VM as the example, but any VM in VirtualBox can be used.

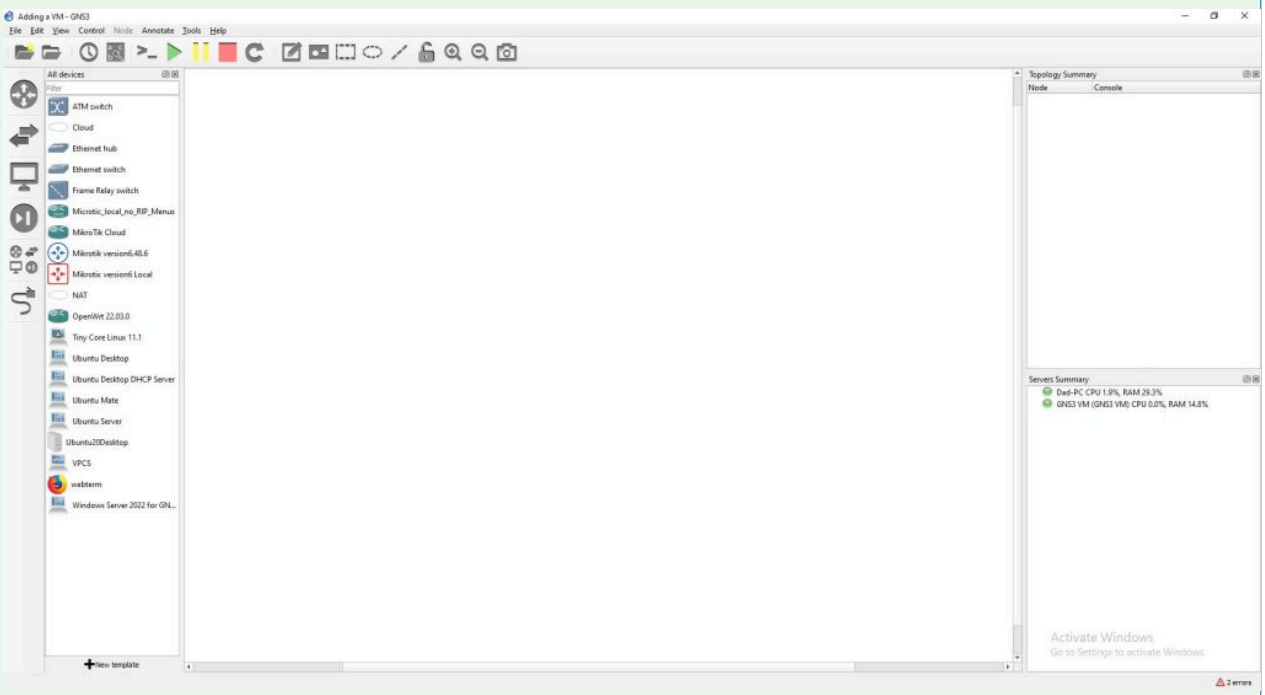


Figure 5 – Screenshot of the VM showing in GNS3 Workspace

1. Open Virtual Box and choose a VM you want to import into GNS3

2. Start GNS3

3. Create a new lab

4. On the GNS3 menu, navigate to ***Edit*** and then ***Preferences*** (Figure 1)

5. Select ***VirtualBox VM***s and you will see the VirtualBox VMs already added to GNS3

6. Select ***new*** at the bottom of the window (Figure 2)

7. Make sure the radio button for running the VM on my local computer is selected and click on ***Next*** (Figure 3)

8. You will now see a window with a drop-down box to select any of the VMs that are loaded in VirtualBox; in this example, we will select ***Windows Server 2022*** for GNS3 (Figure 4)

9. Click ***Finish***

10. To edit the properties of the VM, click ***edit*** on the bottom left of the window

    10.1. Here you can change things such as the default symbol, device name, RAM, etc

    10.2. In the ***Network*** tab, make sure to check the ***Allow GNS3 to use any configured VirtualBox adapter*** option box

    10.3. When you are finished, make sure you click ***Apply*** or risk the VM not being added

11. Click ***OK***

12. Click on the ***all devices*** button and you can now see our VM added to the appliance list (Figure 5)

13. You can drag the recently added VM to the GNS3 Workspace and start it (Figure 6)

14. When the VM starts it will run outside of GNS3, so look for it on your toolbar as a VM (Figure 7)

15. That's it. Remember you can do this for any functional VM in VirtualBox. However, VMs use much more resources than the emulated devices within GNS3. So if you add 10, Windows 11 VMs, you will overload your host machine's processor pretty fast

End of Lab

List of Figures

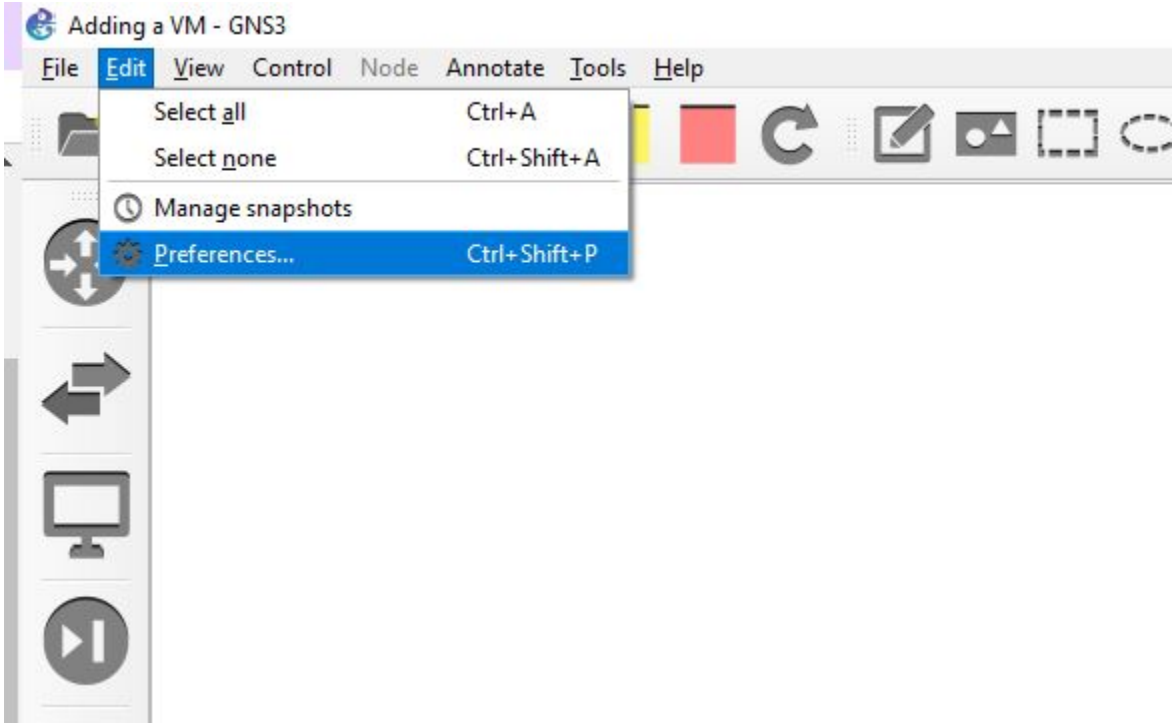


Figure 1 – Adding VirtualBox VMs to GNS3

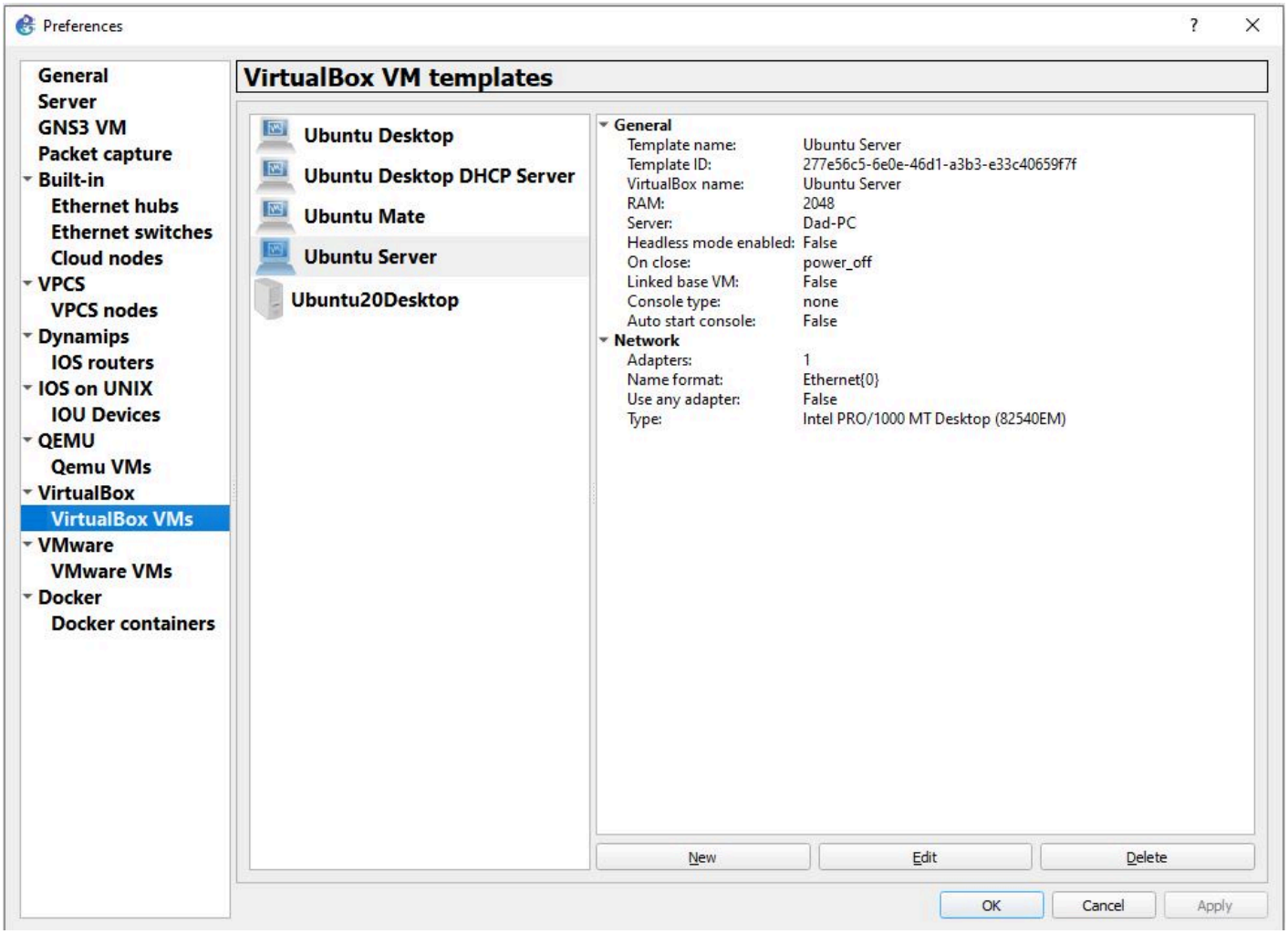


Figure 2 – Adding new VirtualBox VMs to GNS3

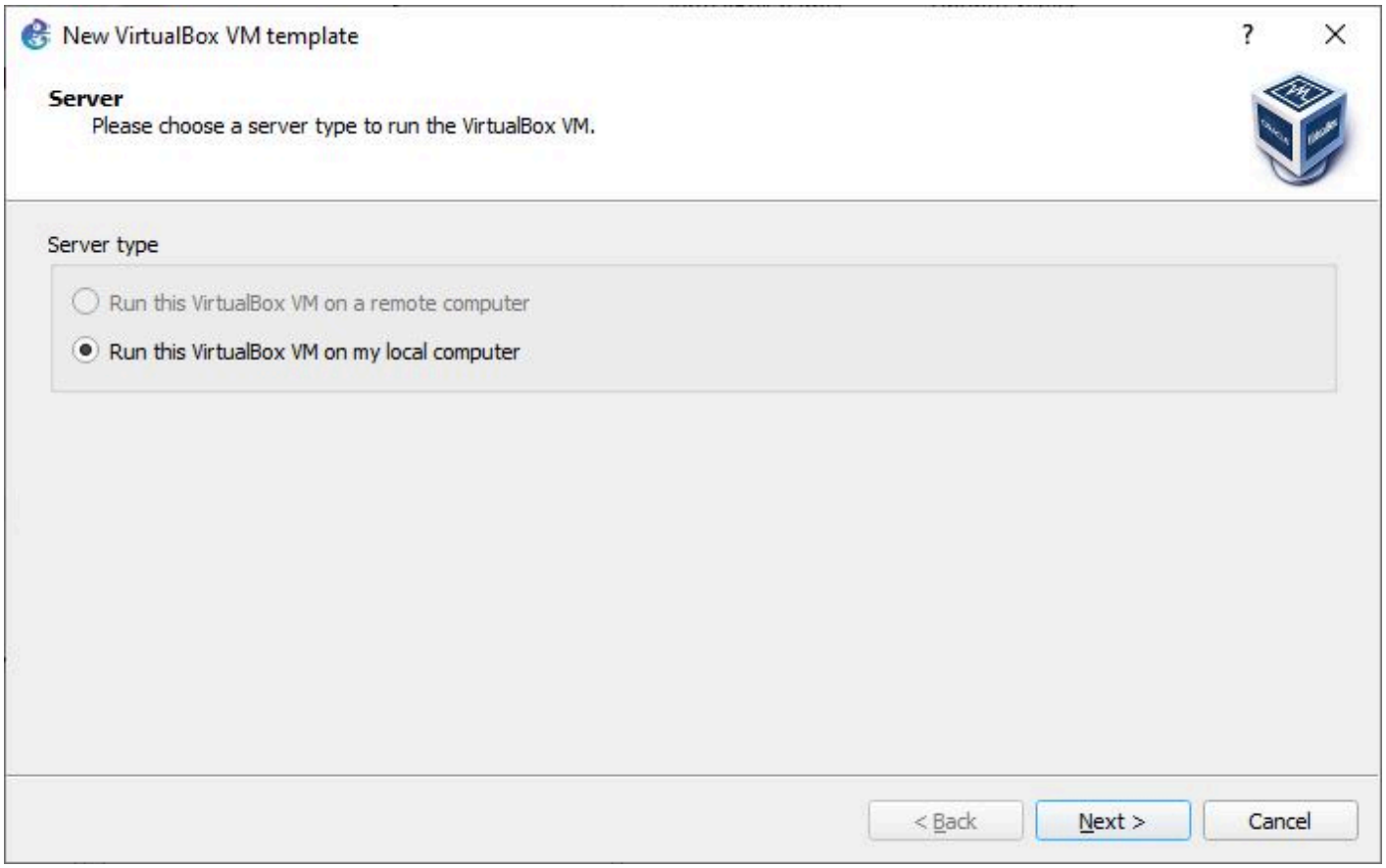


Figure 3 – Radio button selected

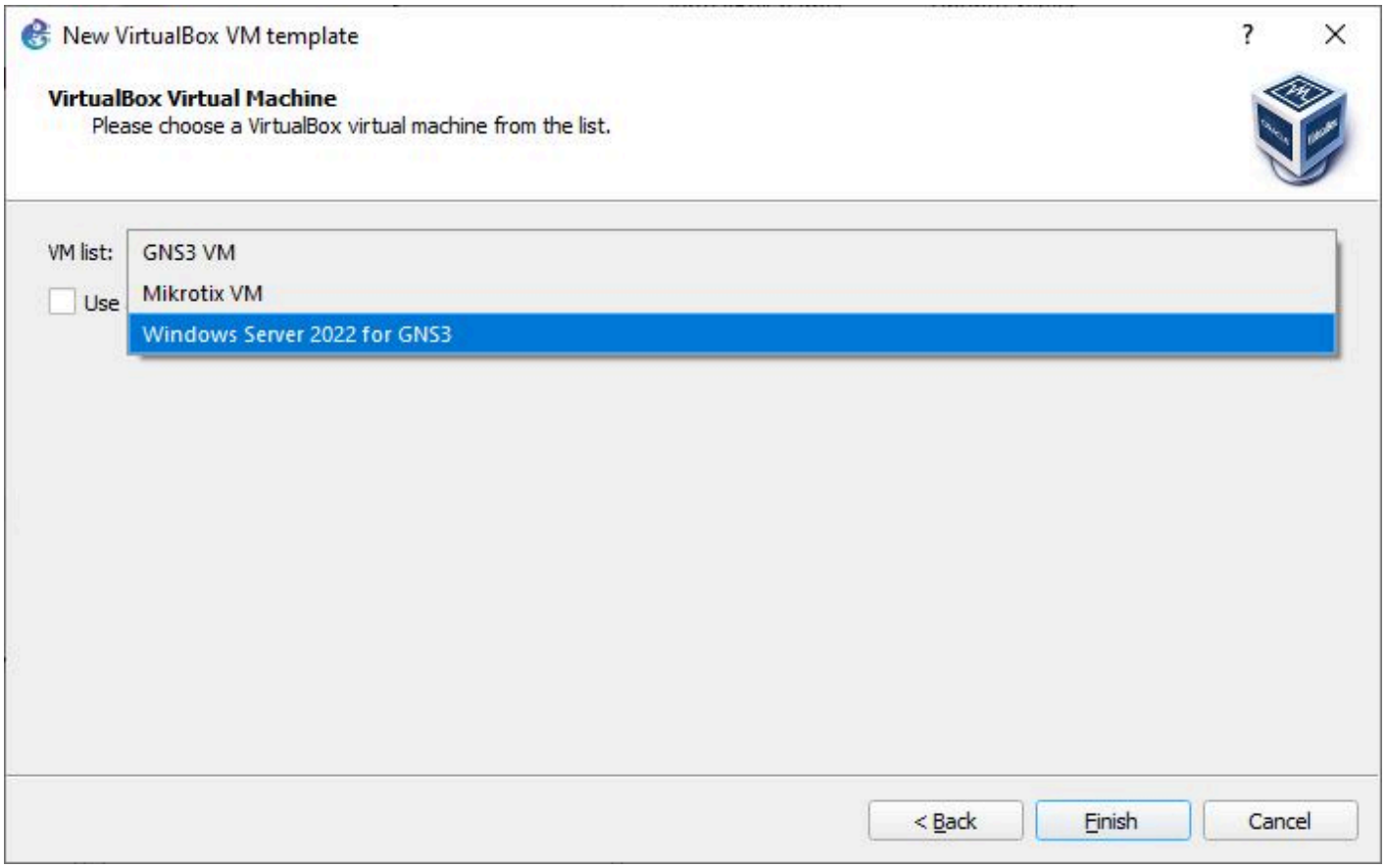


Figure 4 – Adding Windows Server 2022

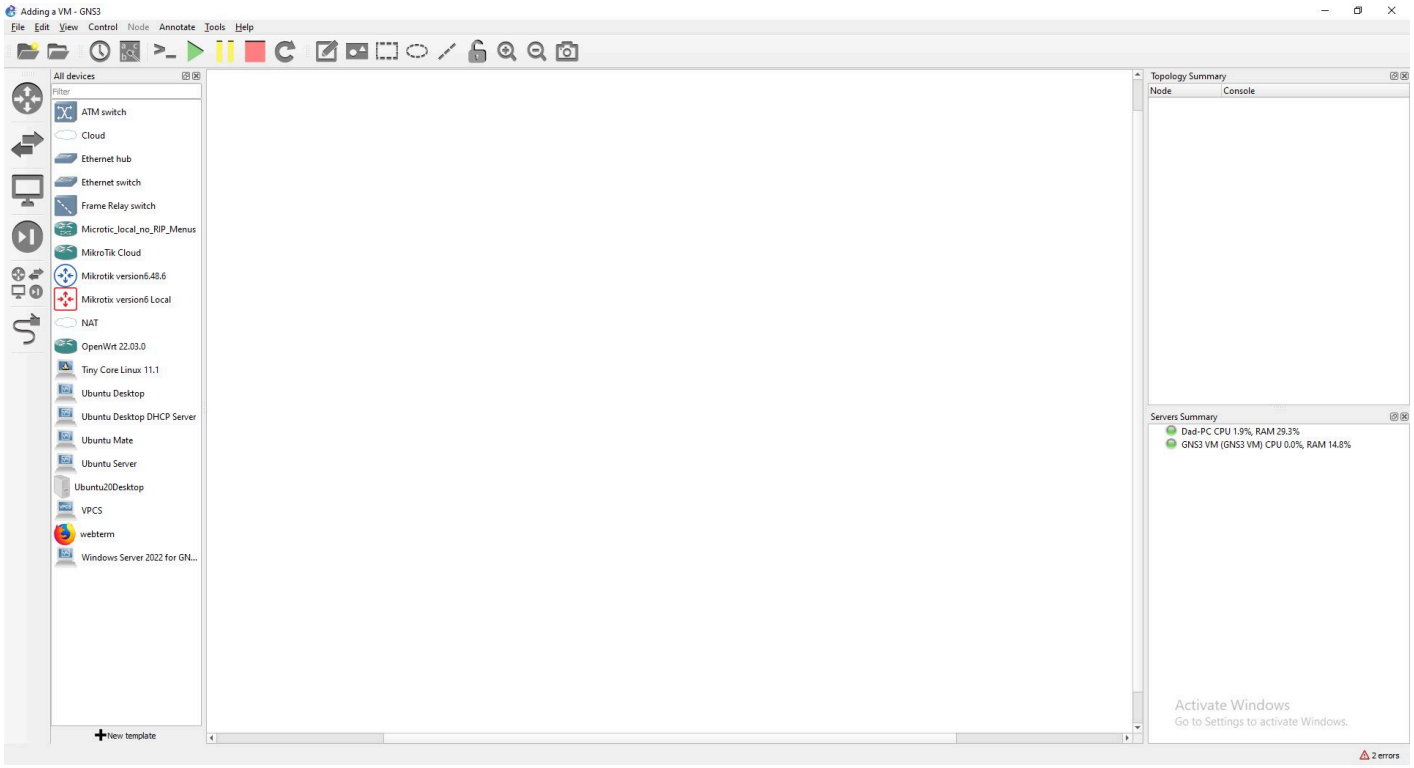


Figure 5 – Screenshot of the VM showing in GNS3 Workspace

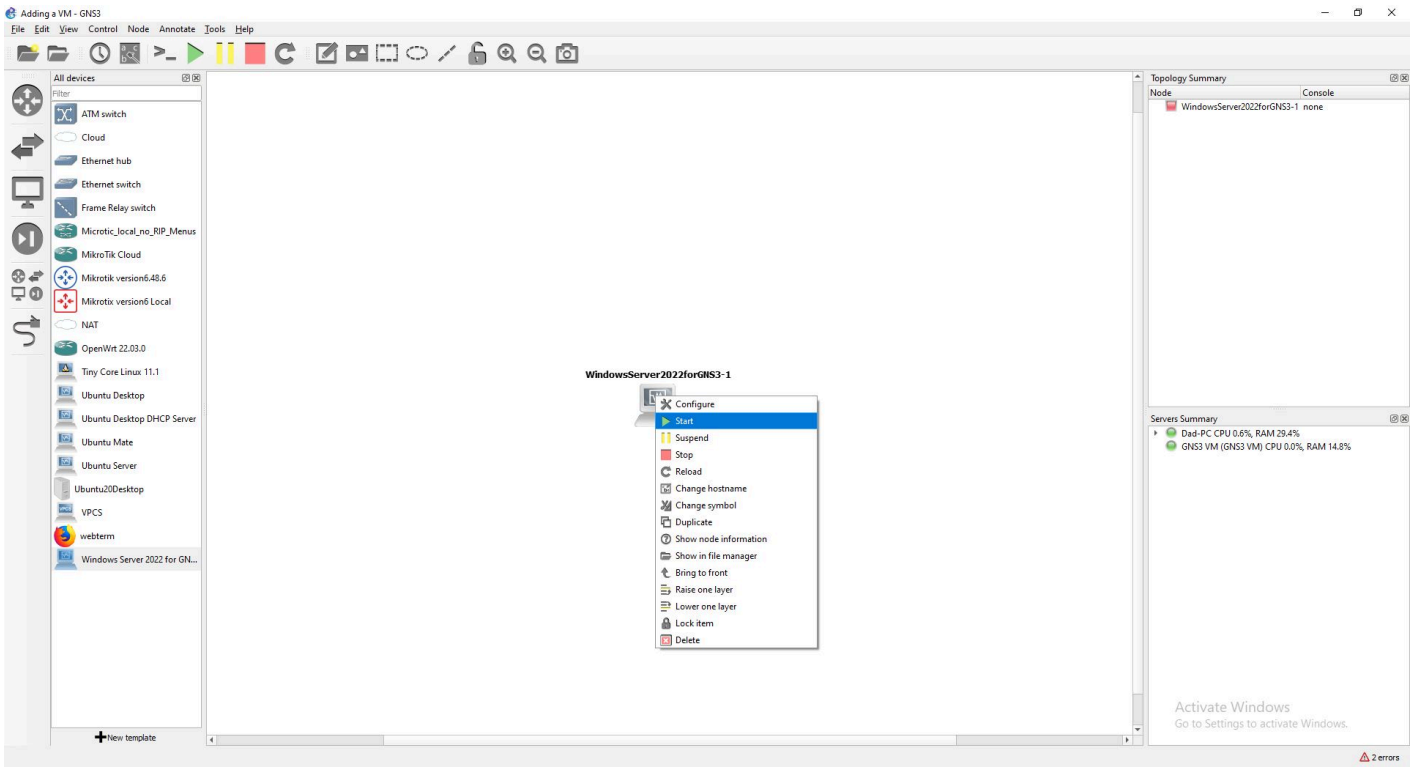


Figure 6 – Drag the new VirtualBox object to the GNS3 Workspace

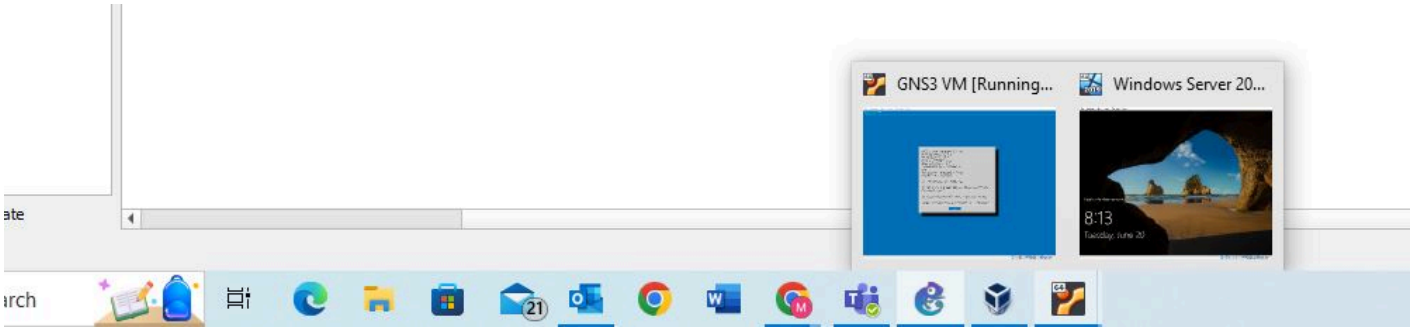


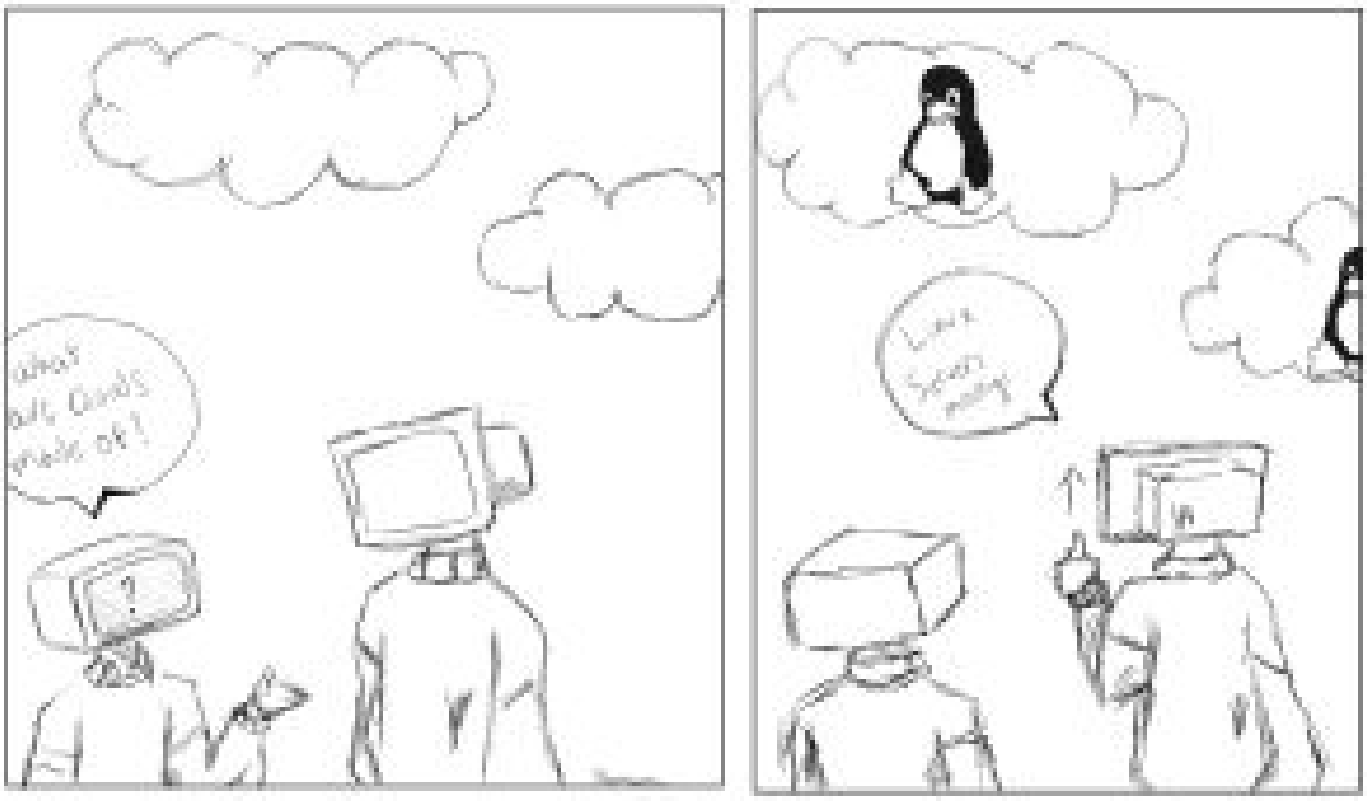
Figure 7 – Looking at the toolbar for the VM

CHAPTER 7

Create a Linux Server

JACOB CHRISTENSEN AND MATHEW J. HEATH VAN HORN, PHD

The Linux operating system has been increasing in popularity for many reasons. Most Linux platforms are free and open-source with very active development communities. Linux is also very reliable in that it often does not require reboots when something goes wrong. Furthermore, Linux is very customizable so only the features that are required are installed. A bare-bones Linux distribution can run on as little as 58MB of RAM! Finally, most applications on Linux are free and open-source.



Used with permission by the artist – Romana A. Heath Van Horn

Many people are reluctant to use Linux because it generally uses a command line interface (CLI) instead of a graphical user interface (GUI) like Windows or Apple. However, all those easy-to-use images require a lot of

RAM and CPU power, so using CLI allows the operating system to focus on the essentials. We use Linux in the GNS3 environment because it requires very little in the way of hardware resources. This allows us to build complex enterprise networks without overloading our hosting machine. This lab will help you download, install, and configure a Ubuntu Linux Server for use in a GNS3 environment.

LEARNING OBJECTIVES

- Successfully download, install, and run Ubuntu Server in a GNS3 environment
- Optional installs for later labs
    - Phase II – DHCP Server – KIA
    - Phase III – DHCP Server – isc-dhcp-server
    - Phase IV – DNS Server – BIND9
    - Phase V – Text-Based Web Browser – w3m
    - Phase VI – GUI – Ubuntu Desktop
    - Phase VII – Web Hosting Service – Apache2

PREREQUISITES

- Chapter 2 – Setting up a GNS3 environment
- Chapter 6 – Adding a VM to GNS3

DELIVERABLES

- None – this is a preparatory lab that supports other labs in this book

RESOURCES

- Download Ubuntu Server https://ubuntu.com/download/server

CONTRIBUTORS AND TESTERS

- Quinton D. Heath Van Horn, 7th Grade
- David Reese, Mathematics Student, SUNY Brockport
- Cody Shinkyu Park, Honeywell Software Engineer, ERAU-Prescott Alumni
- Evan Paddock, Cybersecurity Student, ERAU-Prescott
- Dante Rocca, Cybersecurity Student, ERAU-Prescott
- Sawyer Hansen, Cybersecurity Student, ERAU-Prescott

Phase I – Download and Installation

Installing Linux Server is pretty straightforward. We will use the Ubuntu distribution of Linux due to its expansive documentation and support structure. However, learners will find that other Linux distributions follow similar processes prescribed here.

Furthermore, various tools on the Ubuntu server will be used in part 2 of this book. It is highly recommended that you install all of the optional tools in case you need them later.

1. Download Ubuntu Server from https://ubuntu.com/download/server
2. Start Oracle Virtual Box Manager
3. Click on ***New*** (Figure 1)
    - 3.1. Pick a name, for this example, we use something clever like “Ubuntu Server”
    - 3.2. Use the dropdown menu to select the Ubuntu Server ISO that you downloaded
    - 3.3. Click ***Skip Unattended Installation*** IMPORTANT!
    - 3.4. Click ***Next***
    - 3.5. You can leave the hardware on its defaults –> click ***next*** (Figure 2)

    NOTE: If you are planning on installing the GUI interface you will need at least **50GB** of hard disk storage in the next step.

    - 3.6. Leave the default Virtual Hard Disk settings –> click ***next*** (Figure 3)
    - 3.7. Review the summary and click on ***Finish***
4. Start the Ubuntu Server VM
5. Use the arrow keys to ***Install Ubuntu Server*** (Figure 4)
6. Use the arrow keys to select your language (Figure 5) and your keyboard
7. Use the arrow keys to select ***Ubuntu Server*** and press ***done*** (Figure 6)
8. Accept the default network connections and select***Done*** (Figure 7)
9. Enter a proxy address if you need one select ***Done*** (Figure 8)
10. Enter an alternative Mirror if you know you have one, otherwise, just select ***Done*** (Figure 9)

11. Use the default storage configurations and select ***Done*** for both screens (Figure 10)

12. Confirm the action and select ***Continue*** (Figure 11)

    12.1. For the profile information, the following is recommended (Figure 12)
    Your Name: ***student***
    Your Servers Name: ***ubuntu_server***
    Pick a username: ***student***
    Chose a password: ***Security1***

13. There is no need to update to Ubuntu Pro, so skip it for now (Figure 13) and continue

14. Select ***Install OpenSSH Server*** and continue (Figure 14)

15. No snaps are needed – select ***done*** (Figure 15)

16. Allow the installation and update to complete, then select ***Reboot Now*** (Figure 16)

17. You might have to hit enter a couple of times depending on the way your VirtualBox is configured

18. Login using the credentials you created earlier

NOTE: If you are new to Linux, you should know that the password cursor does not move. This is a security feature to mask how many characters the password is. Anyone shoulder surfing can accelerate their password brute force efforts by knowing the length of the password.

Phase II – Install DHCP Server – Kea (Optional)

These are the instructions to install Kea as the DHCP server because it is replacing isc-dhcp which is no longer supported. We found documentation limited, so for new learners, we recommend installing the isc-dhcp-server which has expansive examples on the web that new learners can refer to as needed.

1. At the terminal prompt, type

```
sudo apt install kea
```

2. Kea can be configured by typing

```
sudo vi /etc/kea/kea-dhcp4.conf
```

3. The instructions to configure Kea are included in the file
4. You can also use this guide to configure Kea
5. Use this guide to add the Ubuntu Server to the GNS3 Working Environment

Phase III – Install DHCP Server – isc-dhcp-server

The isc-dhcp-server is no longer supported as of October 2022. However, it was in use for a long time and there are many writeups on the web on different configurations. We felt it best to continue to have this option for learners at this time.

1. To install type

```
sudo apt install isc-dhcp-server
```

2. Some shortcut commands for future reference include:

2.1. To bind the DHCP server to an interface type

```
vi /etc/default/isc-dhcp-server
```

2.2. To configure type

```
sudo vi /etc/dhcp/dhcpd.conf
```

2.3. To test the configuration file type

```
dhcpd -t
```

2.4. To start the DHCP server type

```
sudo systemctl start isc-dhcp-server.service
```

2.5. To enable the DHCP service to start on boot type

```
sudo systemctl enable isc-dhcp-server.service
```

2.6. To restart the DHCP server type

```
sudo systemctl restart isc-dhcp-server.service
```

2.7. To check the status of the DHCP server type

```
sudo systemctl status isc-dhcp-server.service
```

Phase IV – Install DNS Server – BIND9

Berkley Internet Name Domain (BIND) is the most popular software suite for DNS implementation on Linux systems.

1. Install software and additional utilities

```
sudo apt install -y bind9 dnsutils bind9-utils
```

2. Modify configurations file

```
sudo nano /etc/bind/named.conf.options
```

3. Configure master zone declarations

```
sudo nano /etc/bind/named.conf.local
```

4. Start DNS daemon

```
sudo systemctl start named
```

5. To restart

```
sudo systemctl restart named
```

6. To check status

```
sudo systemctl status named
```

Phase V – Install a Text-Based Web Browser (Optional)

Occasionally you may want to visit the web from the Ubuntu Server that does not have a GUI. This is how you install w3m.

1. Install by typing

```
sudo apt install w3m
```

2. Run by typing

```
w3m -v http://www.google.com
```

3. Exit the browser by pressing *Ctrl-z*

Phase VI – Install a GUI (Optional)

There could be times when you want a graphical user interface (GUI). Make sure your Linux VM has at least 50GB available on the hard drive. Use the default settings whenever prompted.

1. To install the GUI type

```
sudo apt install ubuntu-desktop
```

2. Install the display manager by typing

```
sudo apt install lightdm
```

3. Enable the LightDM service by typing

```
sudo systemctl start lightdm.service
```

4. To make sure it starts on boot type

```
sudo service lightdm start
```

5. You may have to restart the Ubuntu VM

```
sudo shutdown now -r
```

Phase VII – Install a web hosting service

Creating a web hosting service isn't that complicated, but there are a lot of steps. A web server requires a platform, a database, and an interface. Follow these steps to create a local web hosting service and create a test website that can be accessed.

1. Install a GUI on the Ubuntu Server by following the steps in Phase 6
2. Install Apache HTTP Server
    2.1. Install Apache by typing

```
sudo apt install apache2
```

    2.2. Restart the Apache Server by typing

```
sudo service apache2 restart
```

    2.3. Test that it is running by opening Firefox and typing 127.0.0.1 in the address bar
    2.4. Check that it says it works (Figure 17)
3. Install MySQL database management system
    3.1. From a terminal install mySQL by typing

```
sudo apt install mysql-server
```

3.2. Verify it was installed by typing

```
sudo mysql -v
```

3.3. Set the password validation by typing

```
sudo mysql_secure_installation
```

3.3.1. Press ***y*** and set the password strength according to your needs

3.3.2. Press ***y*** to remove anonymous users

3.3.3. Press ***y*** to disallow remote root login

3.3.4. Keep the test database by pressing ***n***

3.3.5. Reload the privilege tables by pressing ***y***

3.4. Test the operability of mysql

3.4.1. Start mysql by typing

```
sudo mysql -u root
```

3.4.2. Create a database by typing

```
create database <name>;
```

3.4.3. List all the databases by typing

```
show databases;
```

3.5. You should have a screen that looks like (Figure 18)

3.6. To leave mysql and return back to the Ubuntu Server console, type

```
exit
```

4. Install PHP web-server scripting language module

4.1. From the terminal, install PHP by typing

```
sudo apt install php
```

4.2. View the version by typing

```
php -v
```

4.3. Make a check file by typing

```
sudo vi /var/www/html/info.php
```

4.3.1. Type *i* and add the following information

```
<?php
phpinfo();
?>
```

4.3.2. Save the file by pressing the escape key followed by

```
:wq
```

4.4. Restart the Apache service by typing

```
sudo service apache2 restart
```

4.5. Test PHP by opening Firefox and typing the following into the web browser address bar 127.0.0.1/info.php

4.6. You should get the following screen (Figure 19)

NOTE: if a service fails to start and you do not know why, try the following commands:

```
systemctl status <service>
```

Record the service's process ID (PID) number.

```
journalctl _PID=<pid_number>
```

Look at the error logs closely, they often help locate the root of most issues!

End of Lab

Figures for Print Version

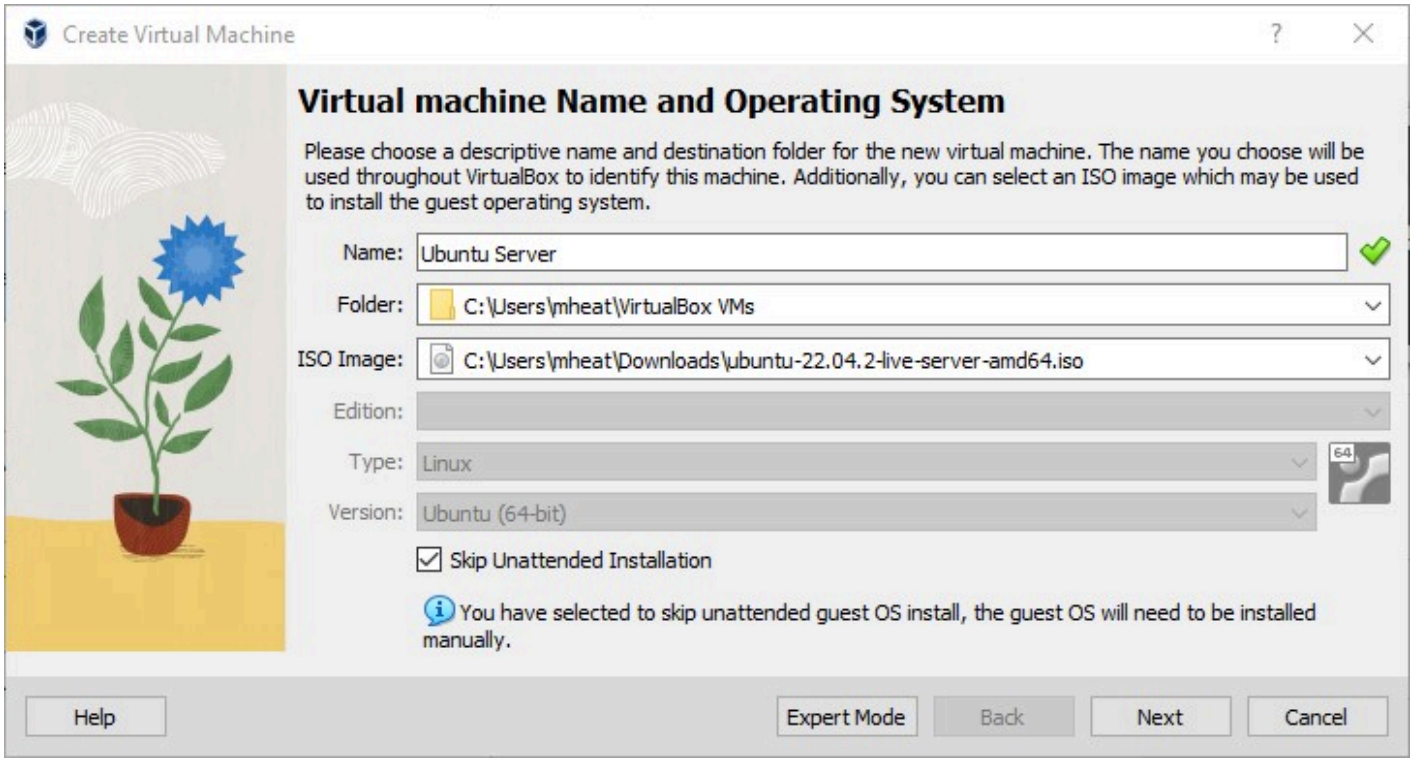


Figure 1 – Create a new VM

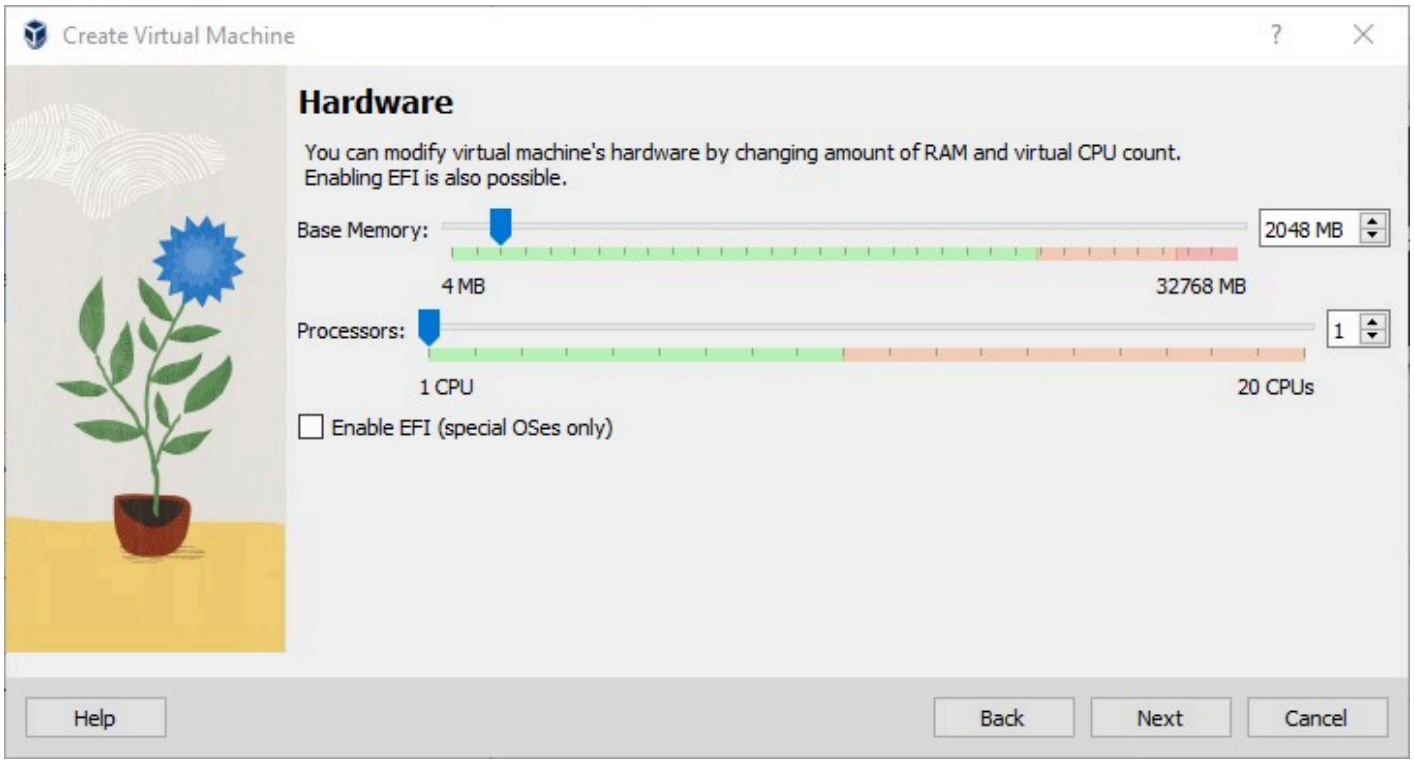


Figure 2 – VM resource settings

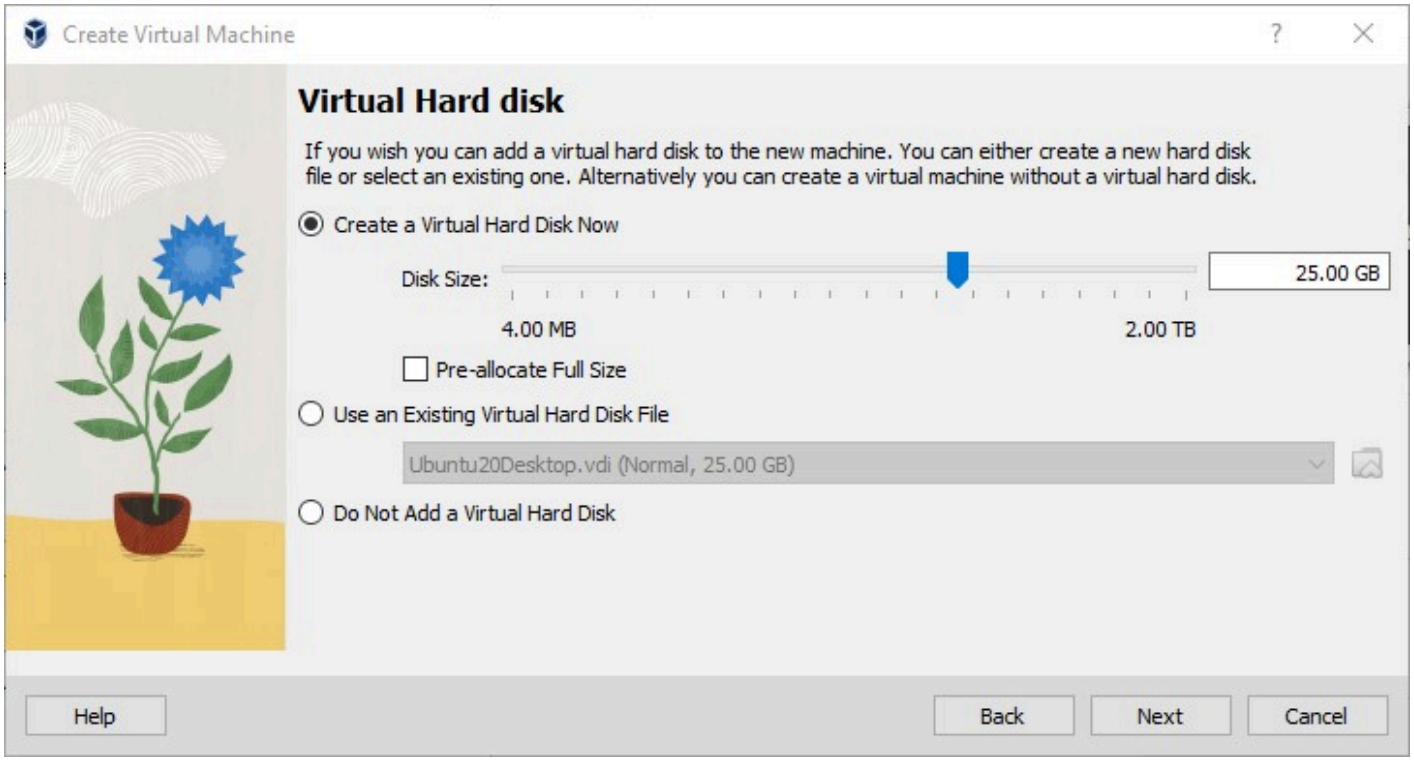


Figure 3 – Hard disk settings

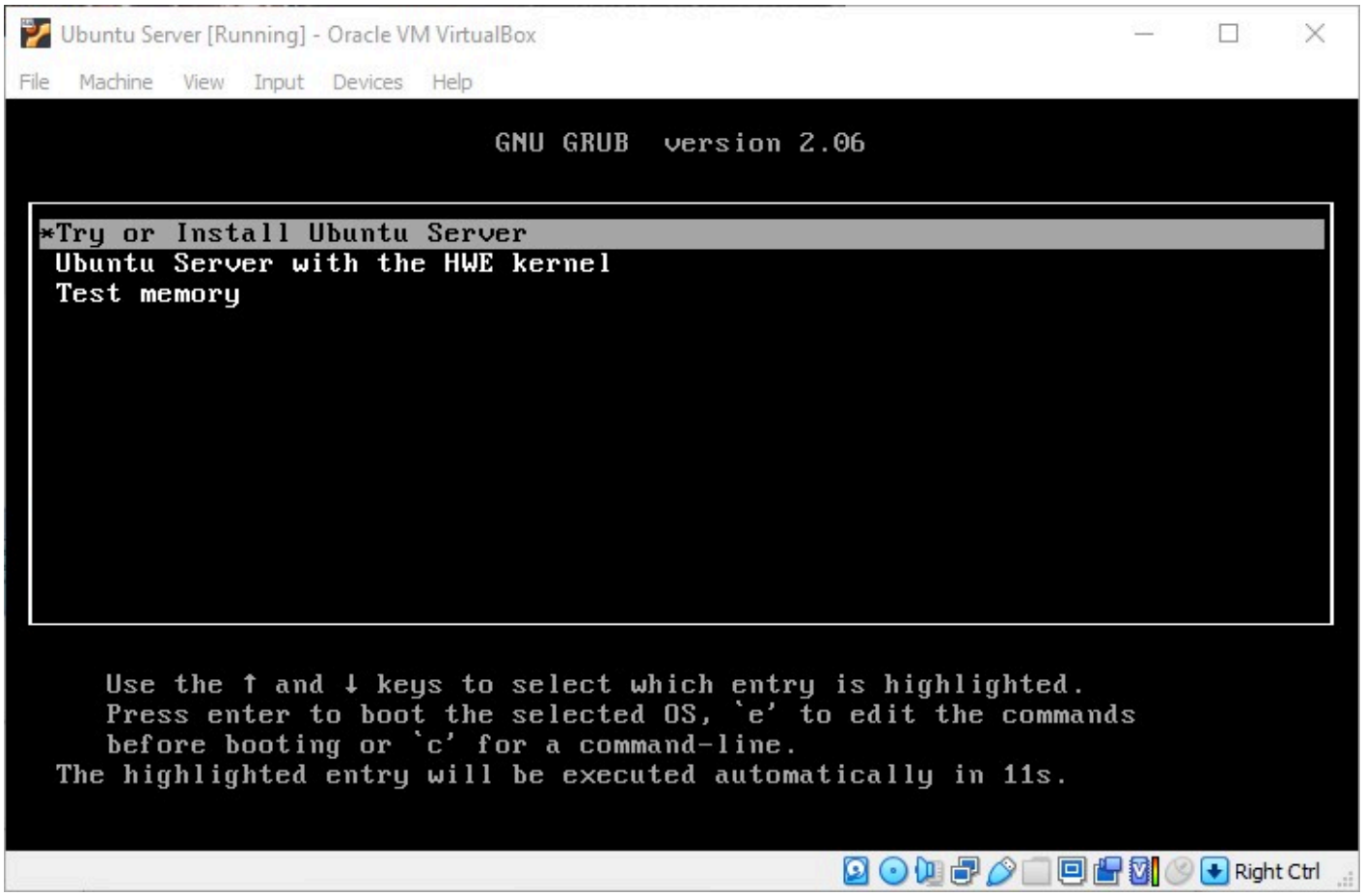


Figure 4 – Install Ubuntu Server

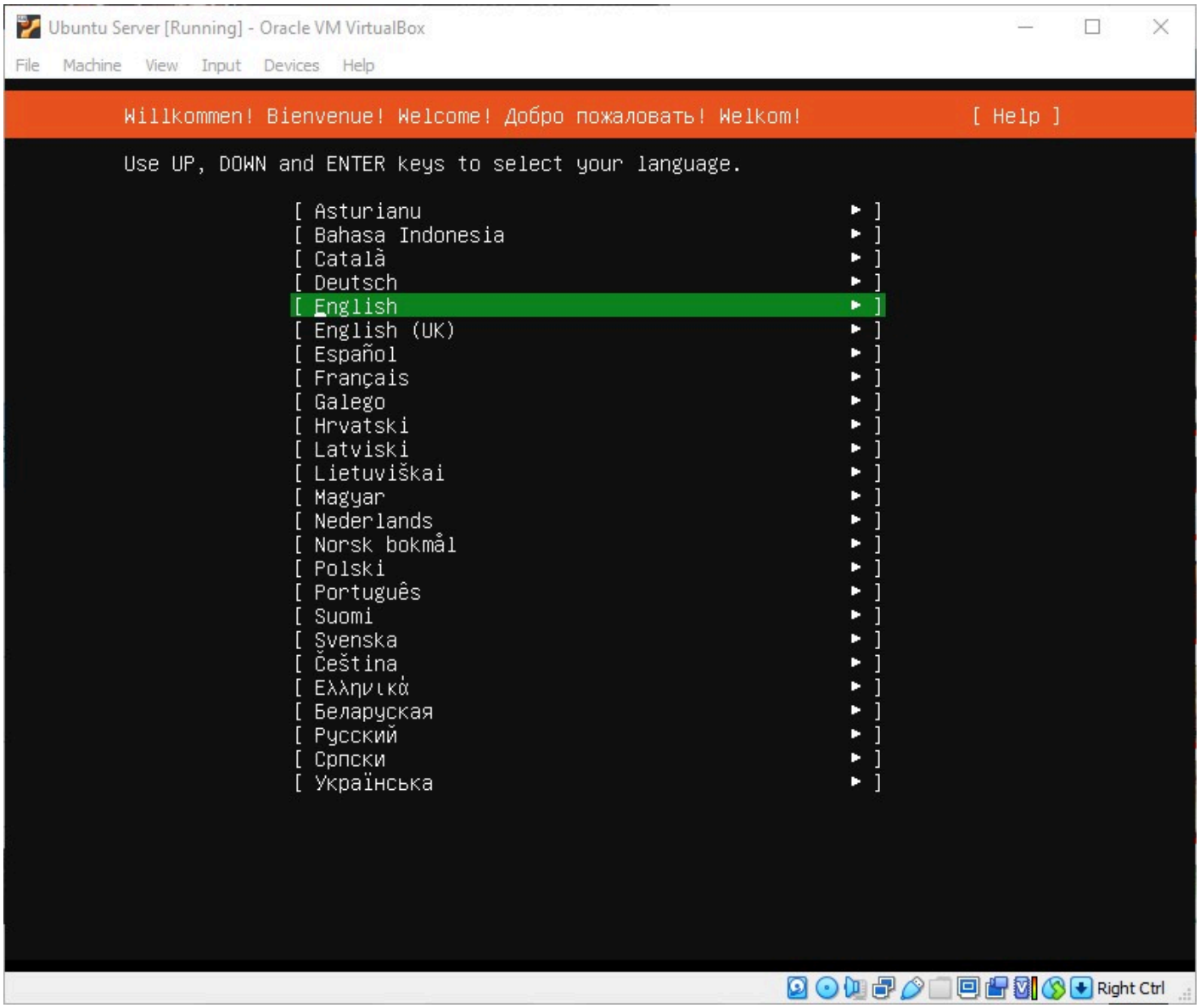


Figure 5 – Select your language

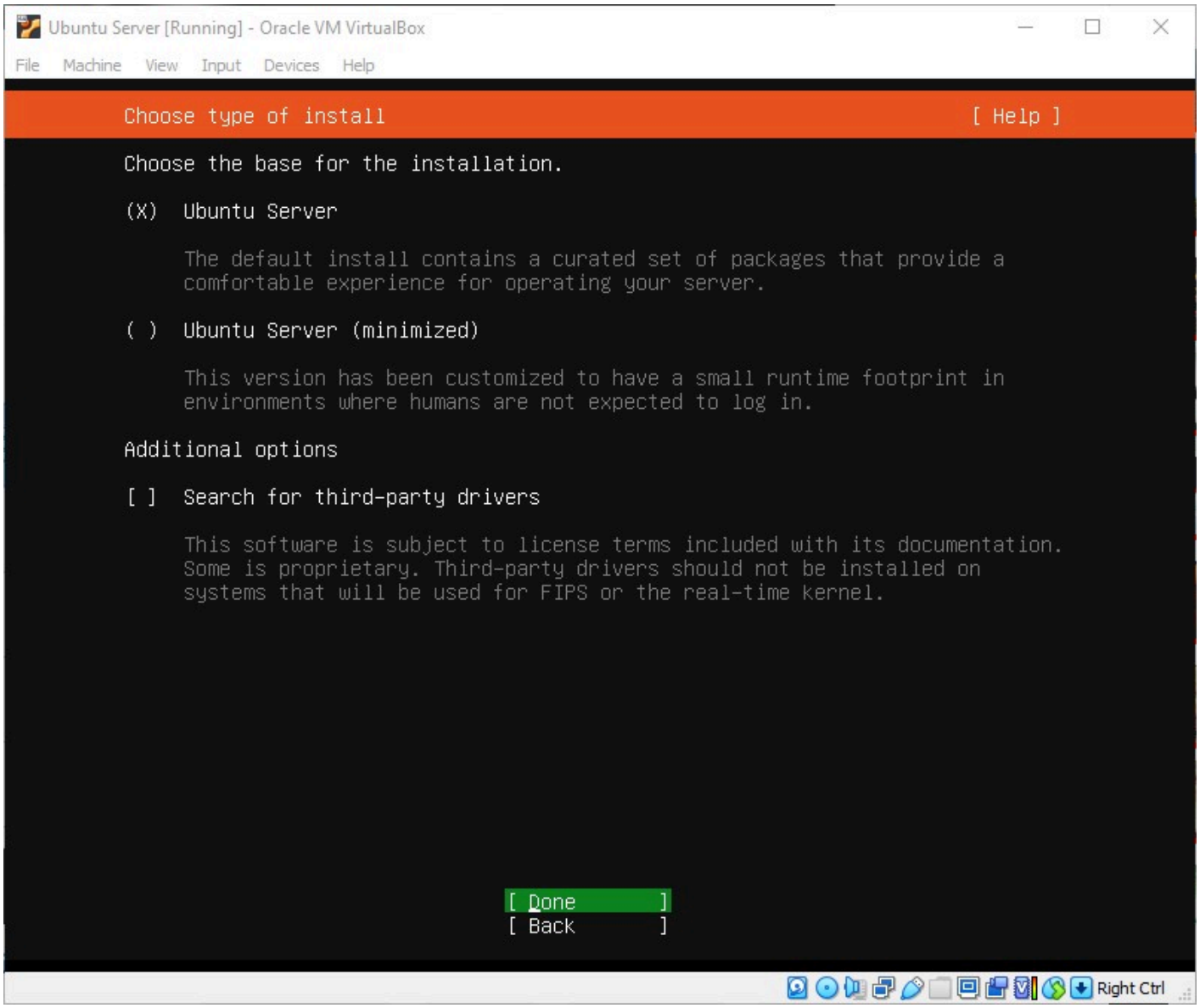


Figure 6 – Ubuntu Server

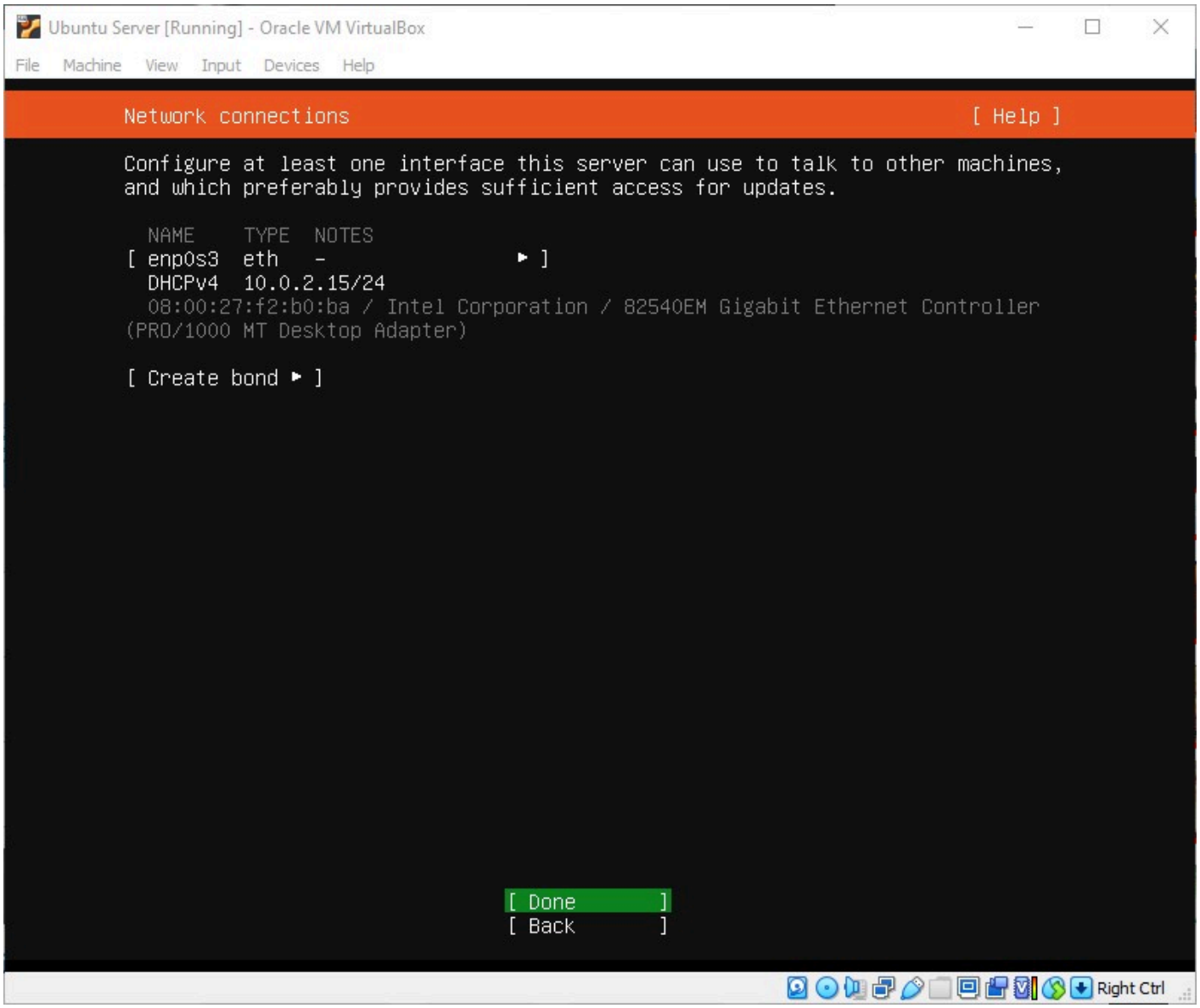


Figure 7 – Accept default network connections

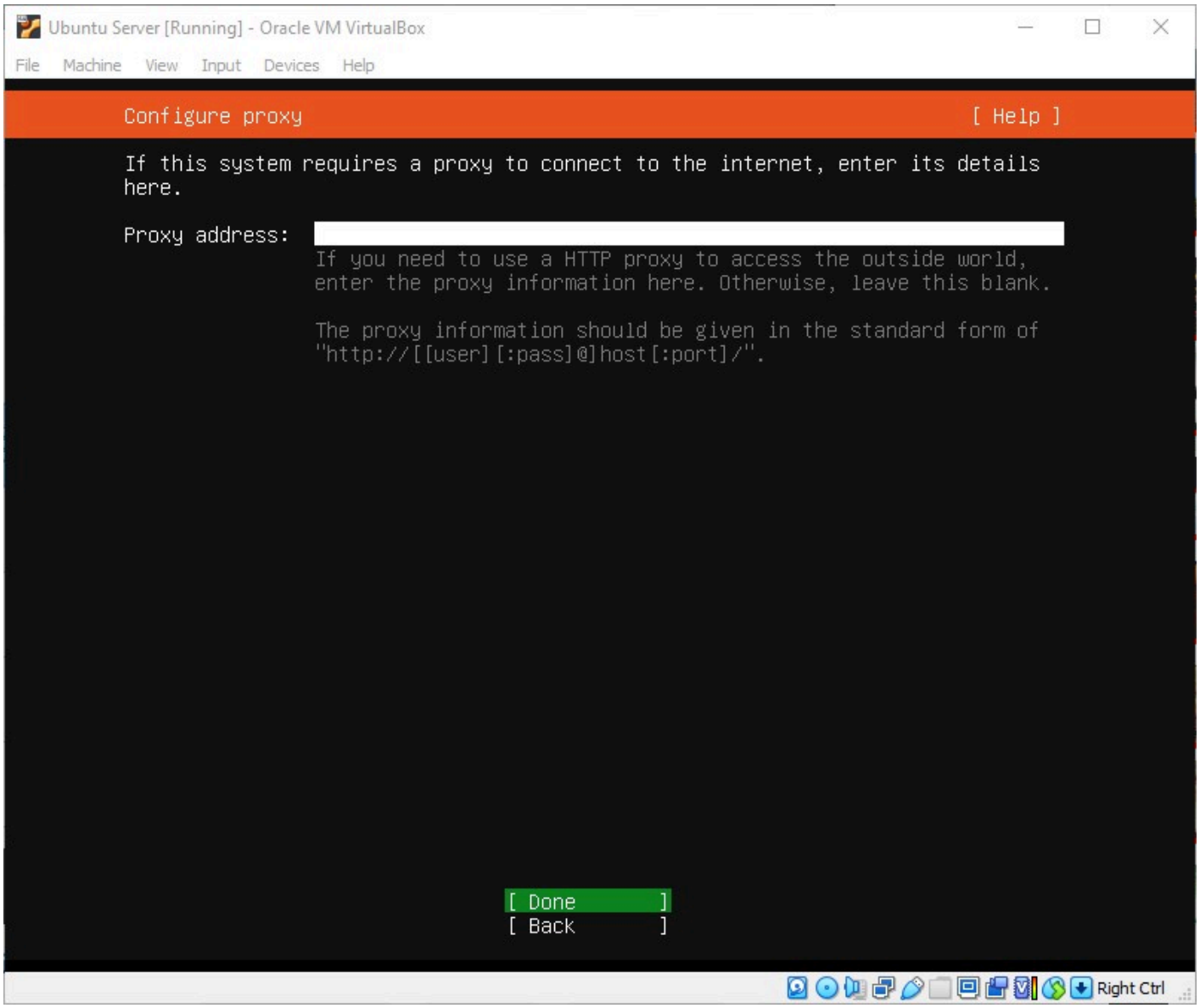


Figure 8 – Proxy address if needed

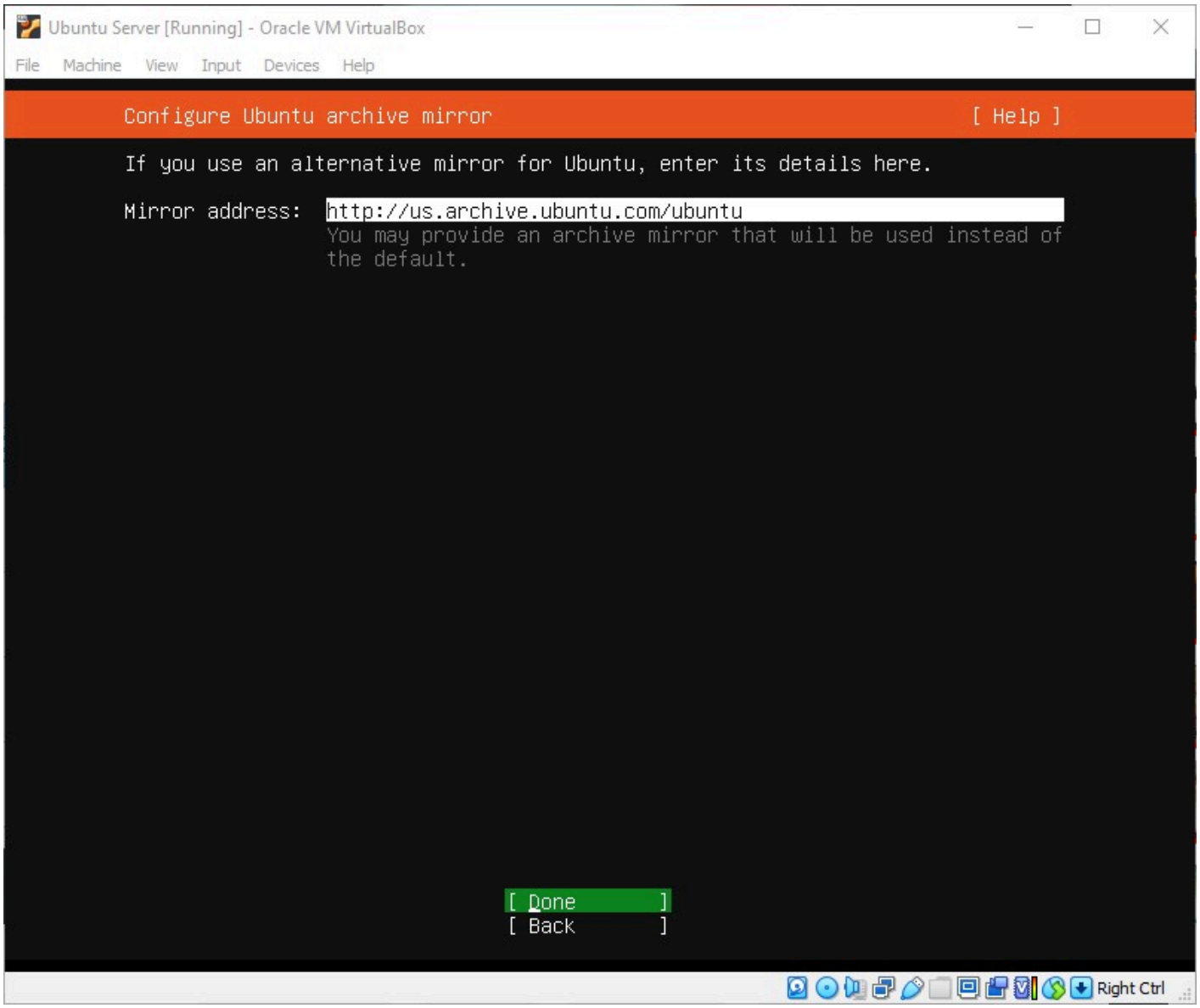


Figure 9 – Alternative mirror if needed

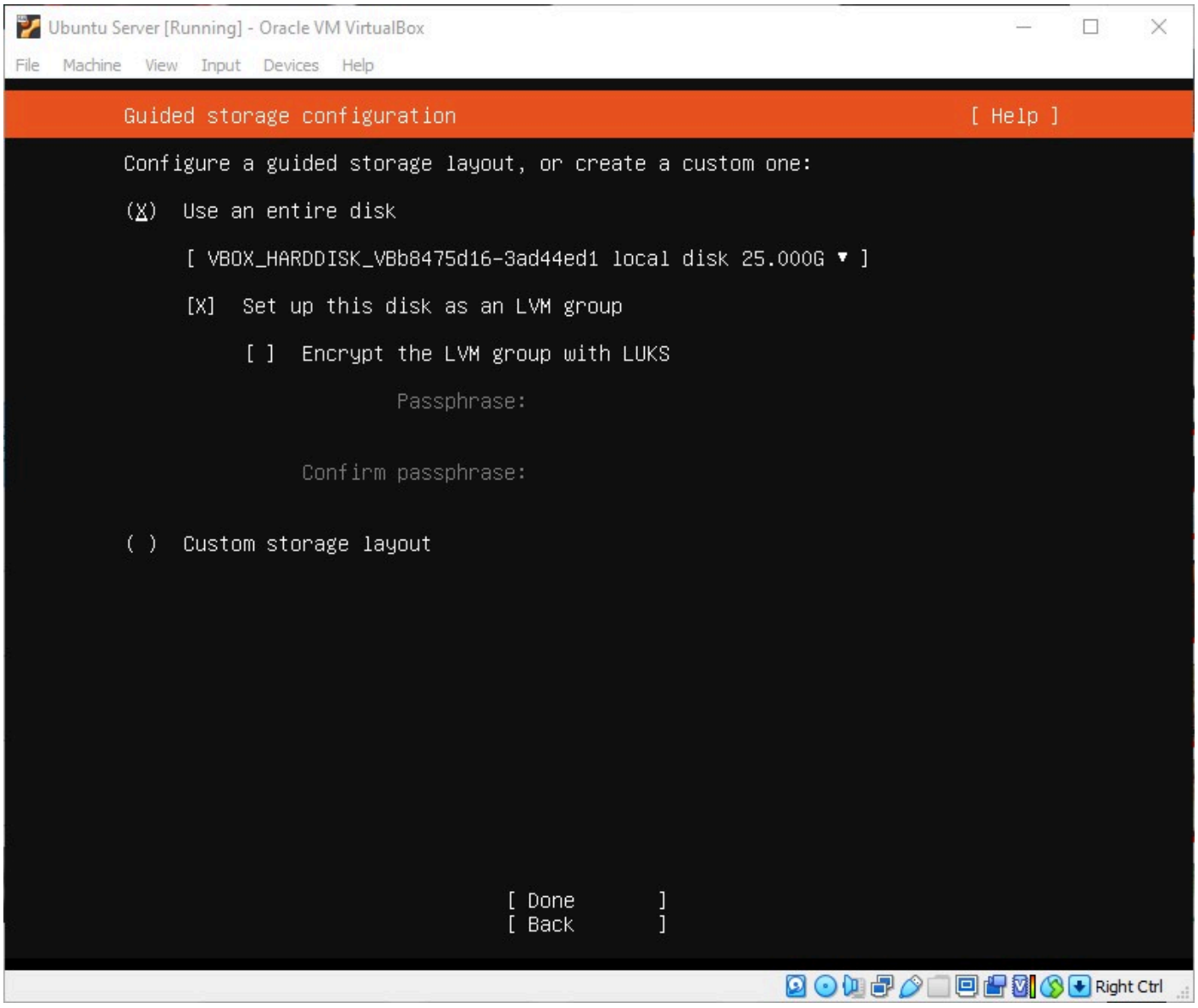


Figure 10 – Use the default storage configurations

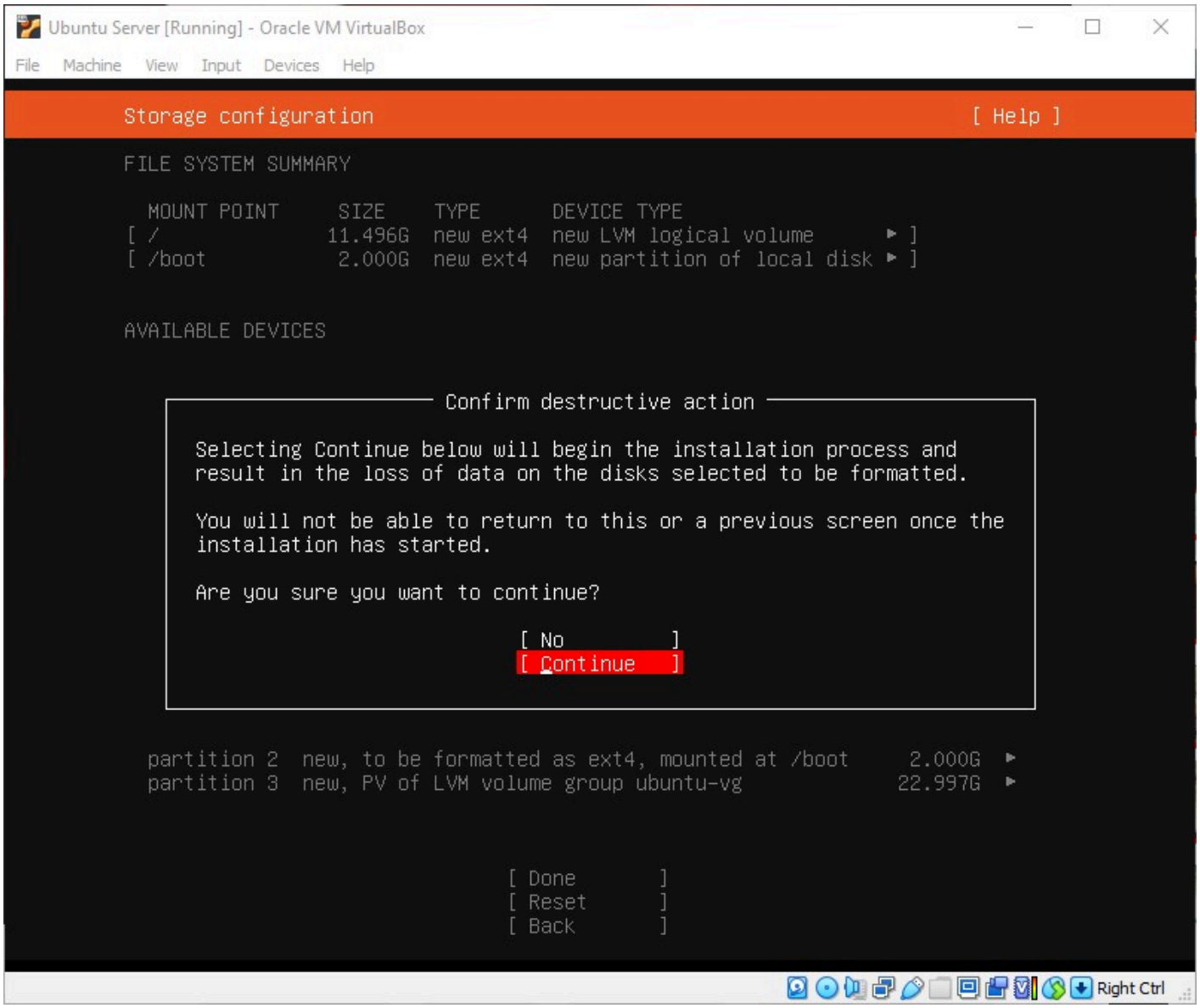


Figure 11 – Confirm and continue

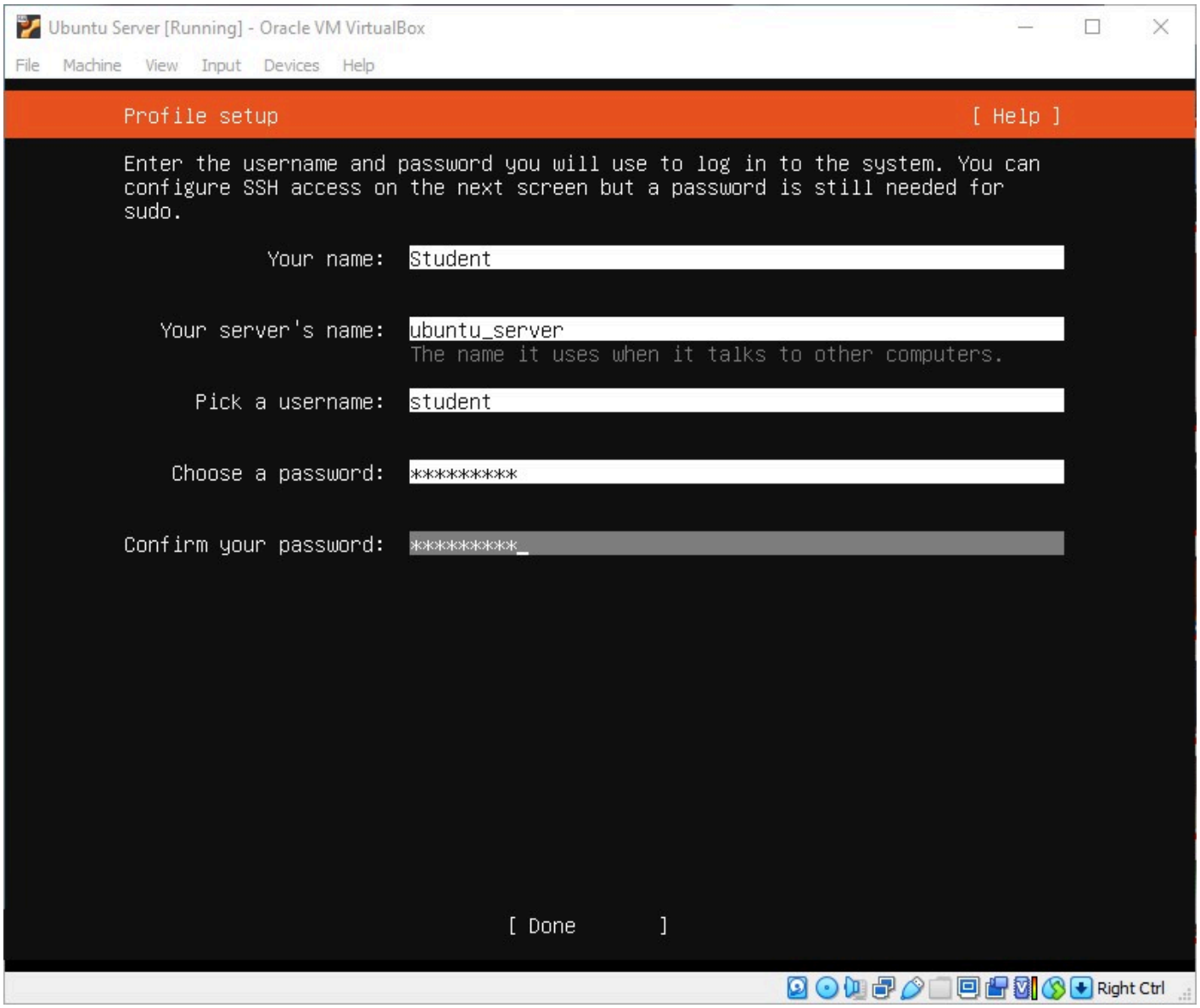


Figure 12 – Enter profile information

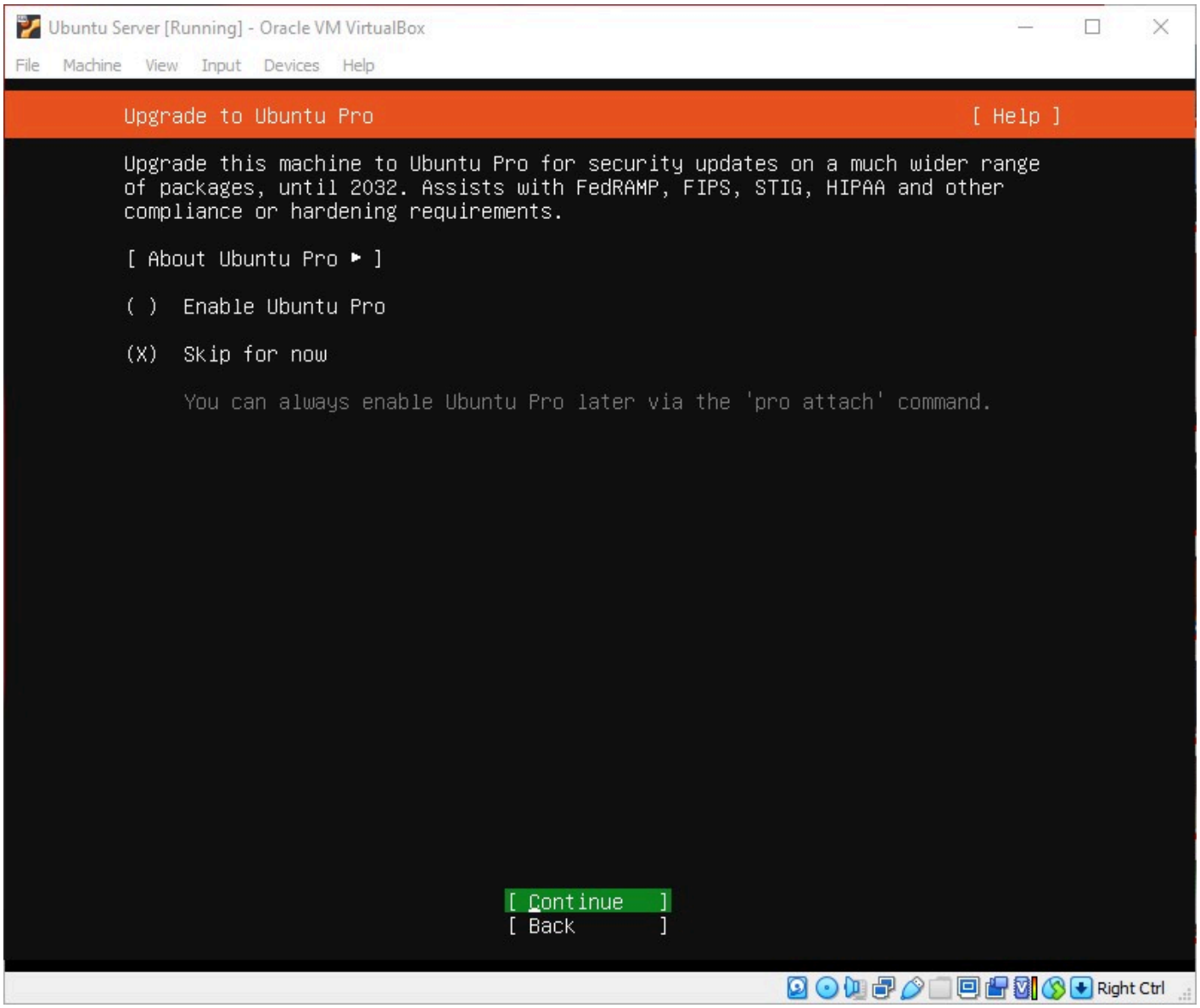


Figure 13 – Skip updating to pro

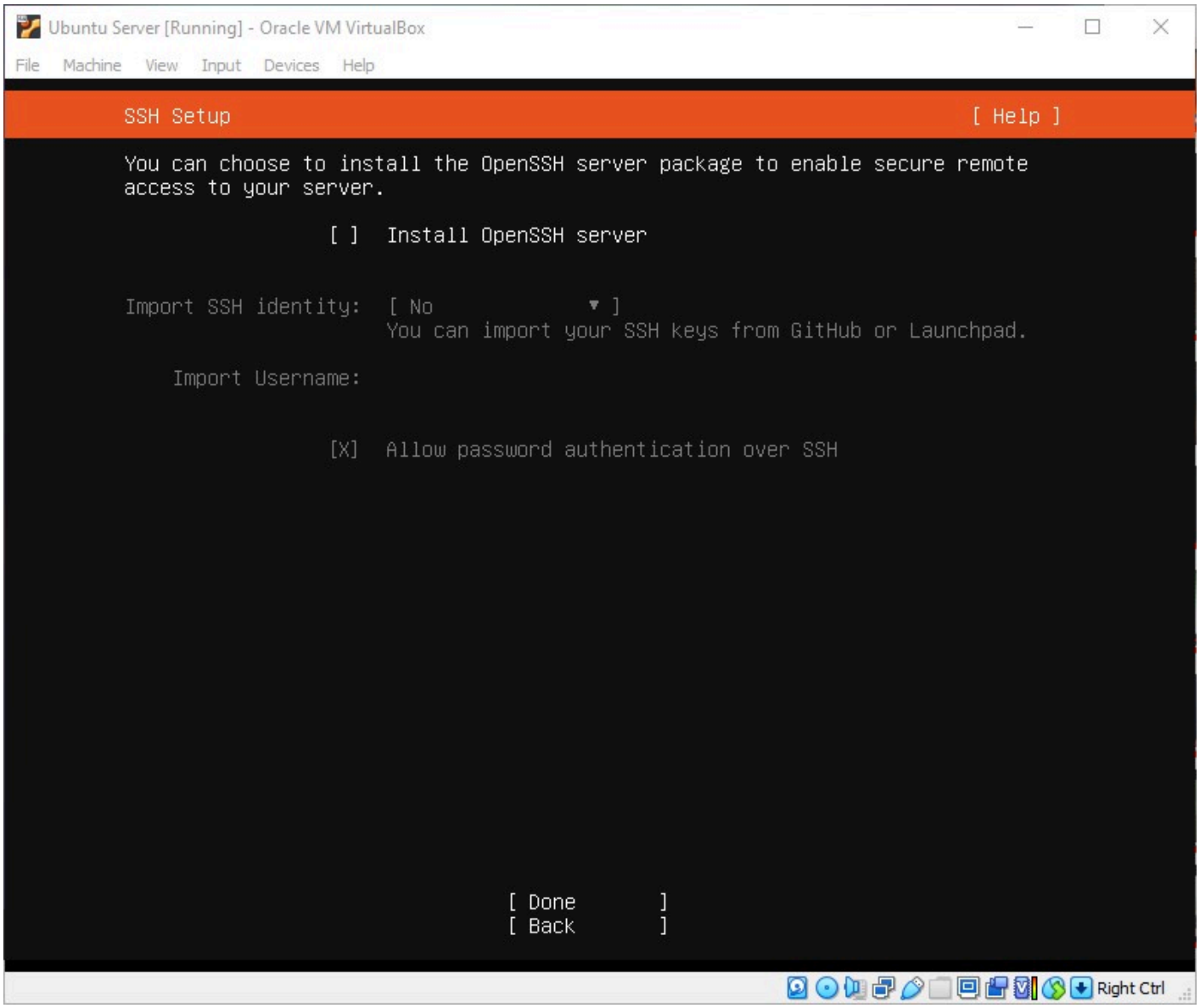


Figure 14 – Install OpenSSH server

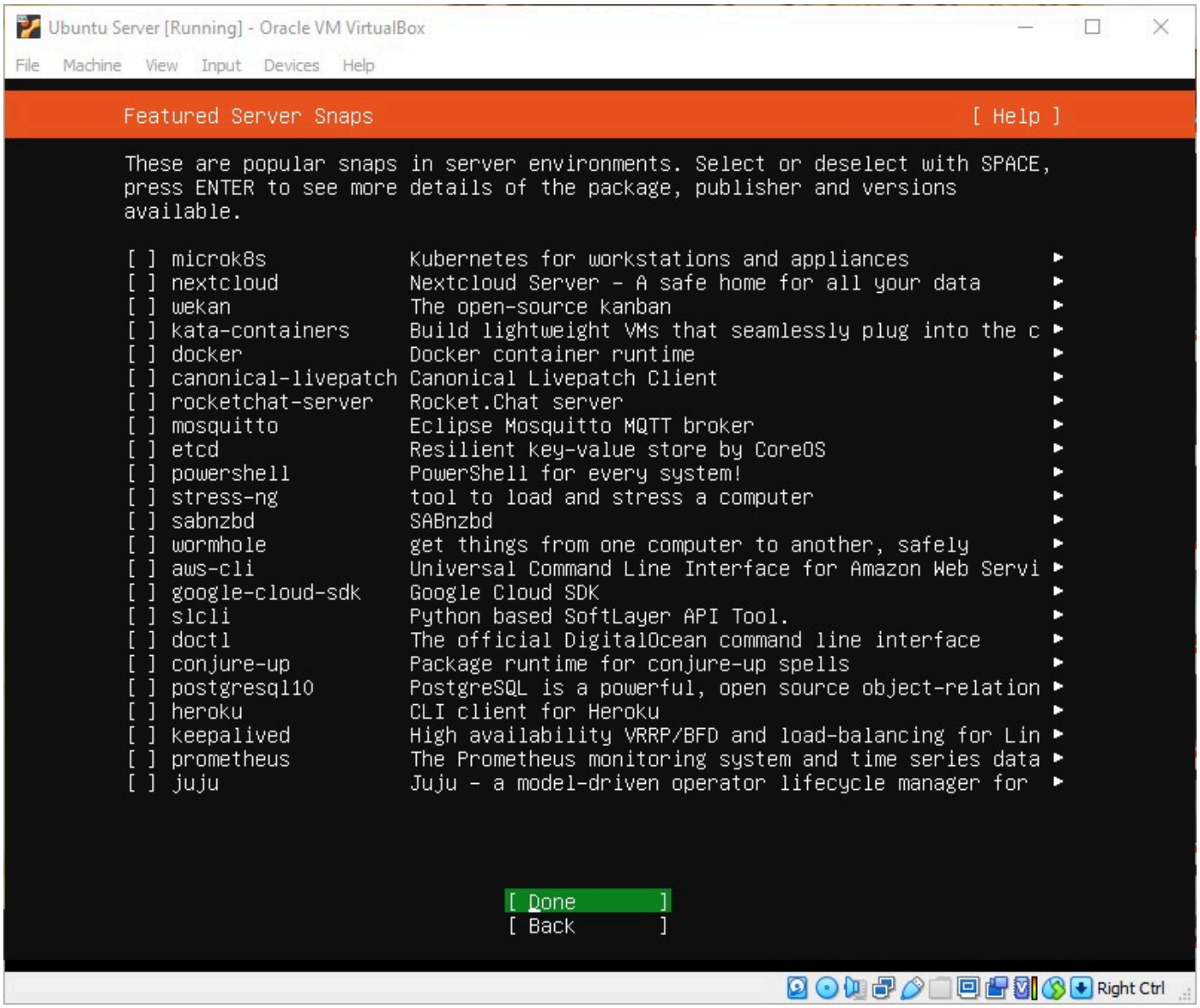


Figure 15 – No snaps needed

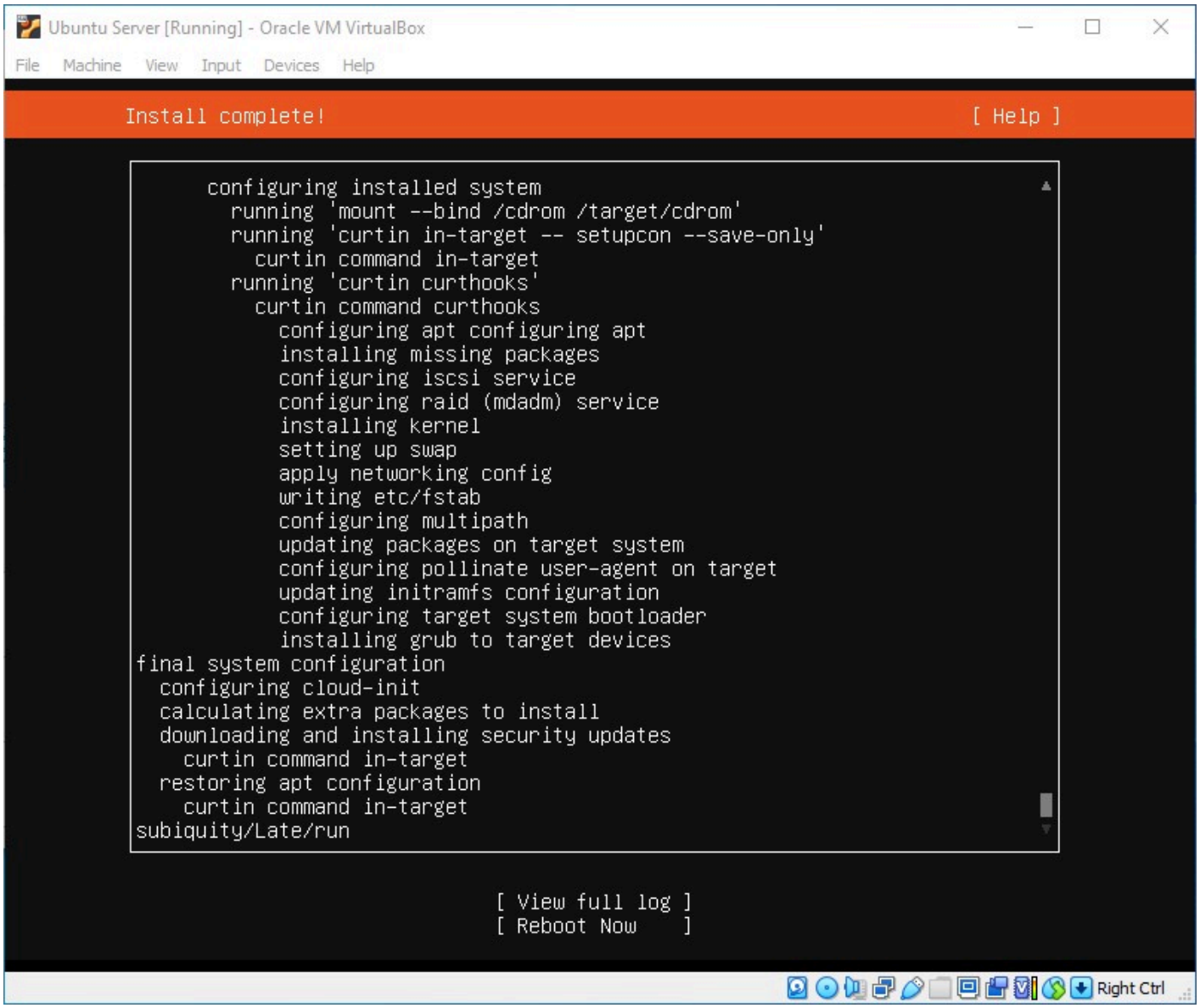


Figure 16 – Reboot now

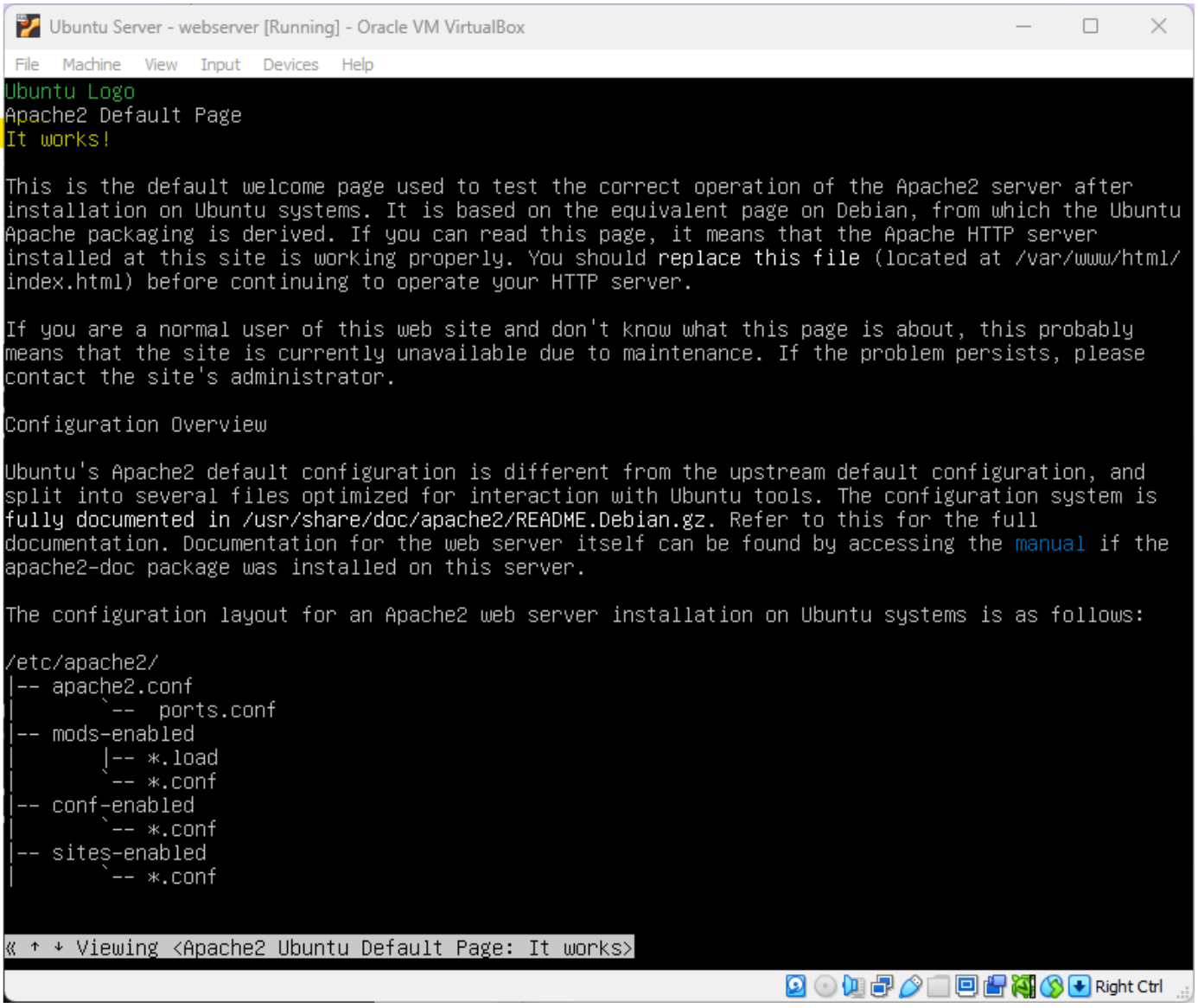


Figure 17 – Apache installed

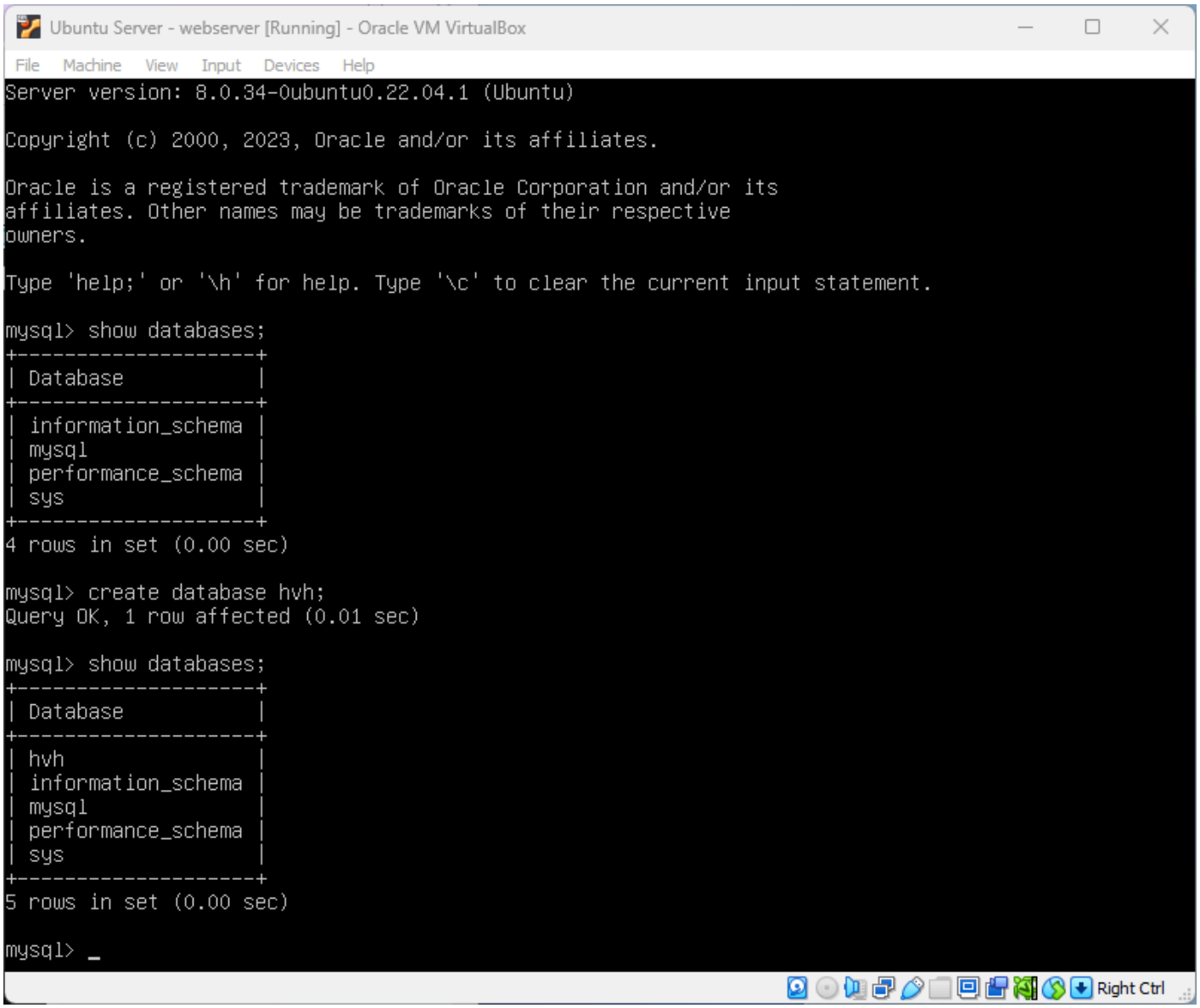


Figure 18 – mySQL is installed

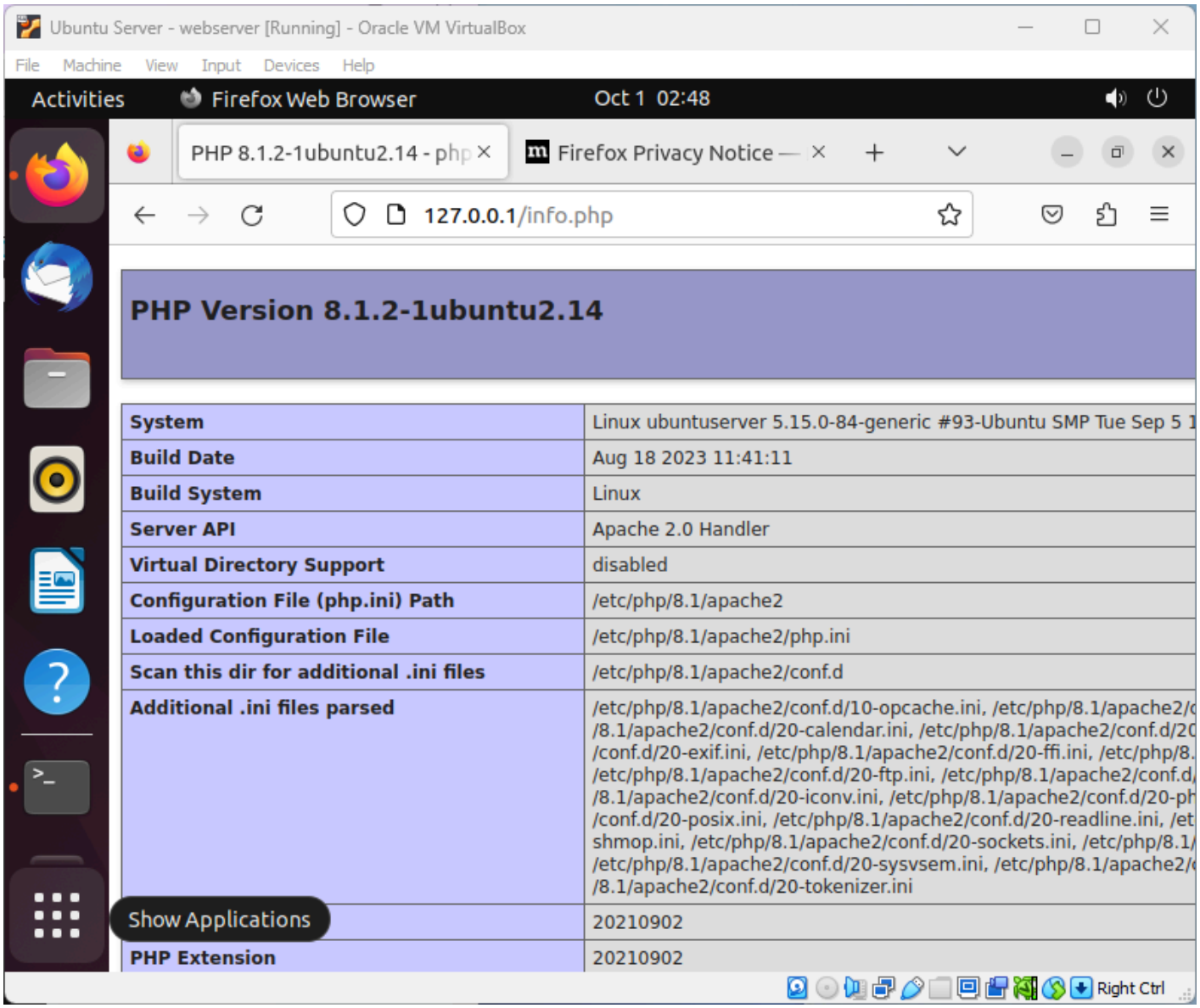


Figure 19 – PHP Test Successful

CHAPTER 8

Create a Windows Server

MATHEW J. HEATH VAN HORN, PHD AND RAECHEL FERGUSON

Windows Server is a popular server that offers many functions for businesses to control their enterprise network. It is not a singular operating system, but rather a group of operating systems that can be used in a variety of ways. This lab's focus is on installing Windows Server for the first time with the most common features.

LEARNING OBJECTIVES

- Using an image of Windows Server, install and configure Windows Server as a virtual machine in the GNS3 workspace

PREREQUISITES

- VirtualBox installed
- GNS3 Workspace Installed

DELIVERABLES

- None – this is a preparatory lab that supports other labs in this book

RESOURCES

- Most students at colleges and high schools can download Windows Server (with a license key) through Azure for Education. Ask your instructor for details or a copy of the Windows Server iso file.
- Some testers have used the Windows Server Evaluation copy available here. If you use an evaluation copy, ignore references to product keys.
- **NOTE: Each source will referenced with its corresponding number in superscript (EX: [1]) at the end of a step**
- 1. MSFT WebCast. "How to Install Windows Server 2019 in VirtualBox (STEP by Step Guide)." YouTube, January 23, 2019. https://www.youtube.com/watch?v=ZjQSuyuN0nA&list=PLUZTRmXEpBy32NP6z_qvVBOTWUzdTZVHt.
- 2. MSFT WebCast. "Basic Configuration Tasks in Windows Server 2019." YouTube, January 25, 2019.

https://www.youtube.com/watch?v=1nxYJSV7-u8&list=PLUZTRmXEpBy32NP6z_qvVBOTWUzdTZVHt&index=3.

- 3. MSFT WebCast. “Setting up Active Directory in Windows Server 2019 (Step by Step Guide).” YouTube, January 28, 2019. https://www.youtube.com/watch?v=h3sxduUt5a8&list=PLUZTRmXEpBy32NP6z_qvVBOTWUzdTZVHt&index=5.

CONTRIBUTORS AND TESTERS

- Julian Romano, Student, ERAU Prescott
- Evan Paddock, Cybersecurity Student, ERAU-Prescott
- Dante Rocca, Cybersecurity Student, ERAU-Prescott

Phase I – Install Windows Server as a VM

Installing Windows Server on a VM has some nuances to be followed in VirtualBox. Please read the instructions carefully.

1. Open Virtual Box Manager

2. Select ***New*** from the top ribbon to open the “Create Virtual Machine” window (Figure 1) [1]

    2.1. Name the VM “Windows Server” [1]

    2.2. Use the ISO Image drop-down box to select the iso image for Windows Server that you have downloaded

    2.3. Click the box that states ***Skip Unattended Installation***

    2.4. Press ***Next***

    2.5. Use the default hardware settings (Figure 2)

    2.6. Press ***Next***

    2.7. Use the default Virtual Hard disk settings (Figure 3)

    2.8. Press ***Next***

    2.9. Review the Summary and press ***Finish*** (Figure 4)

3. Start the Windows Server VM by pressing the big green arrow on VirtualBox Manager to start the setup process

3.1. On the setup screen, use the defaults and press ***Next*** (Figure 5) [1]

3.2. Click ***Install now*** (Figure 6) [1]

3.3. Enter your product key (Figure 7) and press ***next***

3.4. Select the desktop experience (Figure 8) and press ***next***

3.5. Read and accept the license terms (Figure 9) and press ***next*** [1]

3.6. Click on ***Custom Install*** (Figure 10) [1]

3.7. Leave the defaults (Figure 11) and press ***Next***

3.8. Wait for the installation to finish (Figure 12) and restart

3.9. At the Password Screen, set the password to "Security1" and press ***Finish*** (Figure 13) [1]

3.10. If your Host OS reacts to the pressing of ***Ctrl-Alt-Delete*** instead of the VM, press your ***Host Key (right ctrl by default) and delete*** simultaneously to get to the Windows Server login screen on your VM

3.11. Log into the Windows Server using the administrator credentials (Figure 14)

3.12. At the first start-up, you will get two popups (Figure 15)

3.12.1. Server Manager – Click on ***Don't show this message again***

3.12.2. Networks – Click ***Yes***

3.13. This brings you to the Server Manager Dashboard (Figure 16)

Phase II – Install Active Directory

Active Directory (AD) is a collection of processes and services. It is commonly used to assign and enforce security policies for all computers on the network via a Windows Server running Domain Services. The Windows Server with Domain Services running is called a Domain Controller. Most Windows Server services rely on the Domain Controller to function properly.

1. The Server Management Dashboard should open automatically on Windows Server startup (Figure 16)

2. On the left side of the dashboard, click on ***Local Server*** (Figure 17) and give it a couple of seconds to populate the information [3]

3. Click on ***Manage*** in the top right-hand corner of the screen. Once the drop-down appears click on the ***Add Roles and Features*** option shown (Figure 18) [3]

4. An "Add Roles and Features Wizard" box will open

    4.1. Before you begin – Click ***next*** (Figure 19) [3]

    4.2. Installation Type – click the ***Role-Based*** option – click ***next*** (Figure 20) [3]

    4.3. Server Selection – click on your local server (Should be the only option) – click ***next*** (Figure 21) [3]

    4.4. Server Roles – select ***Active Directory Domain Services*** which will automatically open a pop-up window (Figure 22) where you will press the ***Add Features*** button [3]

    4.5. Returns you back to the Select Server Roles (Figure 23) and you can see that the Active Directory Services option now has a checkmark next to it

    4.6. Select ***DNS Server*** from the list of options which will open a pop-up Window (Figure 24) where you will press the ***Add Features*** button [3]

    > **NOTE:** You may get an alert. This is normal because we haven't finished configuring everything. Just press "Continue"

    4.7. Returns you back to the Select Server Roles (Figure 25) and you can see that the DNS Server has a checkmark next to it – Click ***Next*** [3]

    4.8. Features (Figure 26) – Click ***Next*** [3]

    4.9. AD DS (Figure 27) – Click ***Next*** [3]

    4.10. DNS Server (Figure 28) – Click ***Next*** [3]

    4.11. Confirmation (Figure 29) – Click ***Install*** [3]

    4.12. Wait for the installation to complete (Figure 30)

    4.13. Click on the blue text that states, ***Promote this server to a domain controller.*** (Figure 31) and you will get a popup [3]

5. Configure Active Directory Domain Services Wizard

5.1. Deployment Configuration (Figure 32)

5.1.1. Click on ***Add a new forest*** [3]

5.1.2. Root domain name: pick something you would like. For these examples "mycyber.local" was chosen [3]

5.1.3. Click ***Next***

> **NOTE:** Creating a new forest can take a minute or two.

5.2. Domain Controller Options- select a password for the DSRM – we typically use "Security1" in this book (Figure 33) – Click ***Next*** [3]

5.3. DNS Options (Figure 34) – Ignore the alert if there is one and Click ***Next*** (Figure 34) [3]

5.4. Additional Options – It takes a moment to auto-populate with MYCYBER, but if it doesn't type it in. Then Click ***Next*** (Figure 35)

5.5. Paths – Click ***Next*** (Figure 36) [3]

5.6. Review Options – Click ***Next*** (Figure 37) [3]

5.7. Prerequisites Check – (this could take a minute for a green box to appear – Ignore the alerts) Click ***Install*** (Figure 38) [3]

5.8. The Server VM will automatically restart (Figure 39), just wait for it to finish

Phase III – Add to GNS3

Add the newly created Windows Server VM to GNS3.

1. Follow the procedures for adding a VM to GNS3
2. You may want to make some changes to the default settings
   - Change the image to look more like a server instead of a PC
   - Change the network options to ***Allow GNS3 to use any configured VirtualBox adapter***

End of Lab

List of Figures for Printed Version

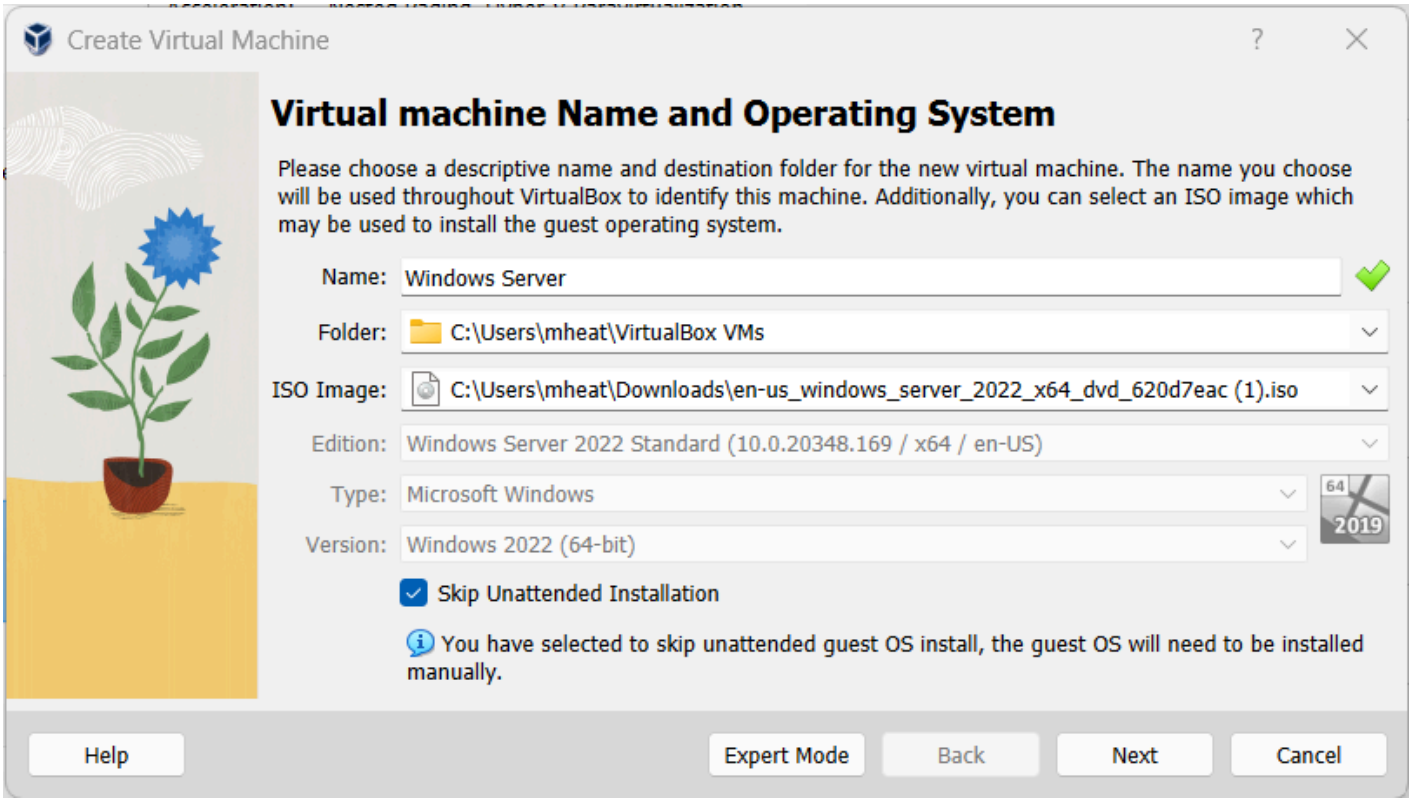


Figure 1 – Create virtual machine

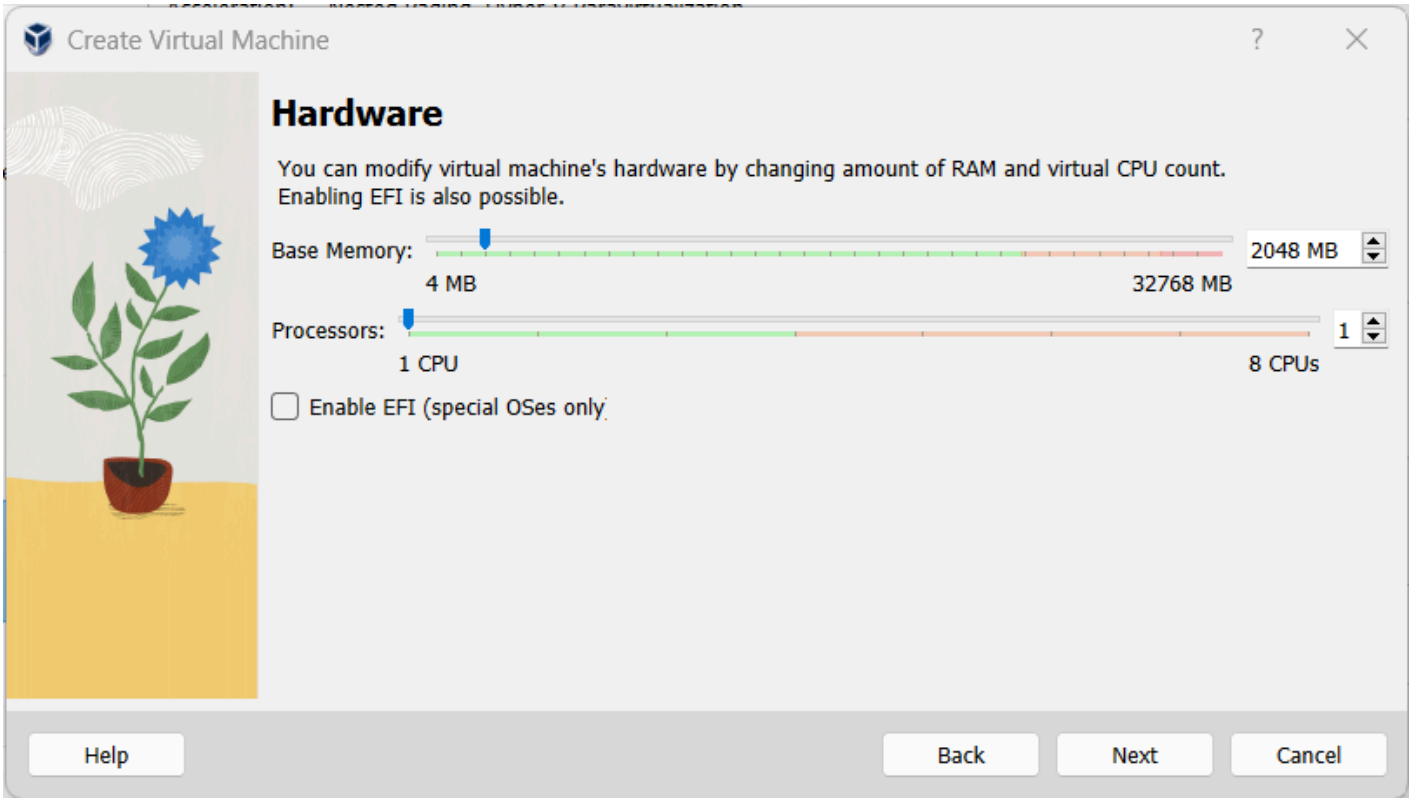


Figure 2 – Hardware settings

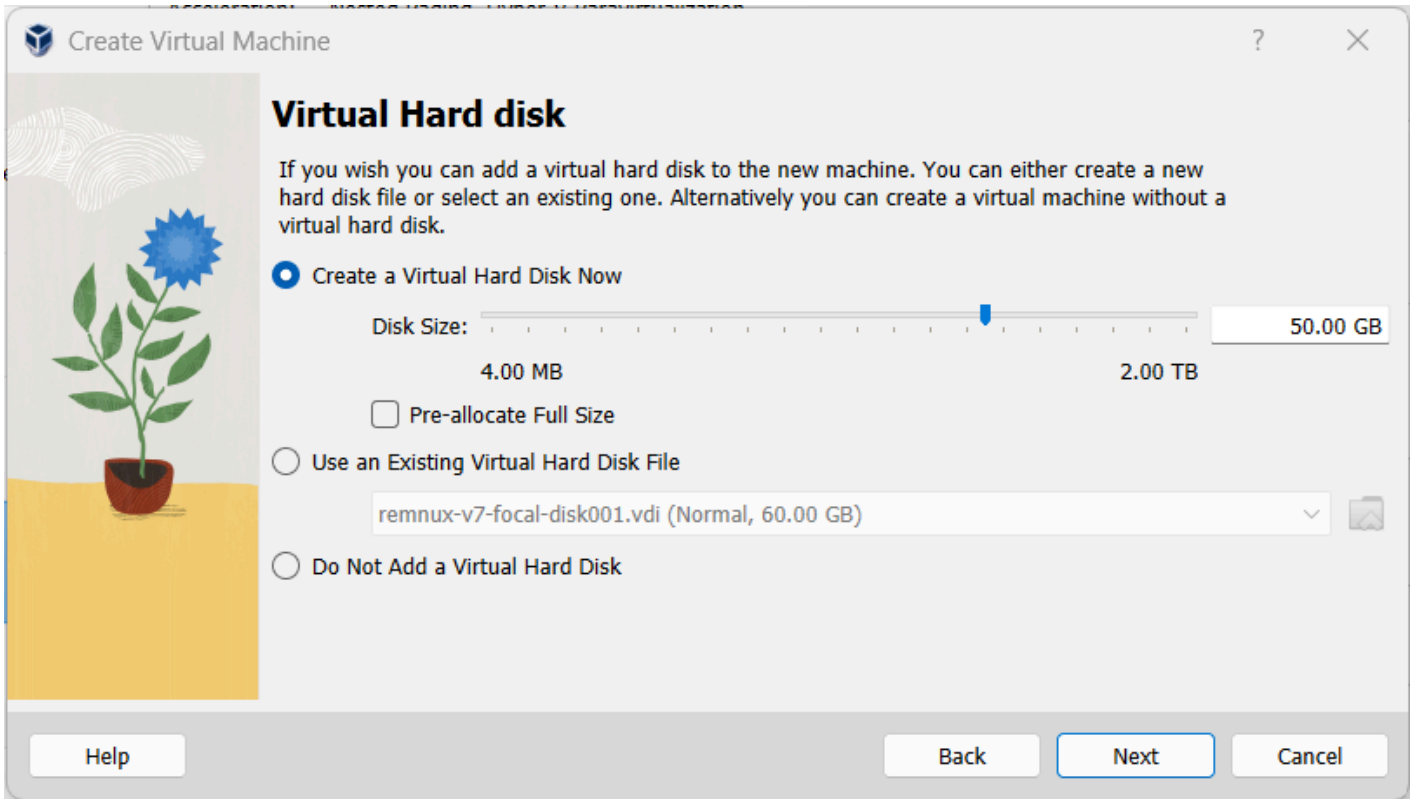


Figure 3 – Virtual hard disk settings

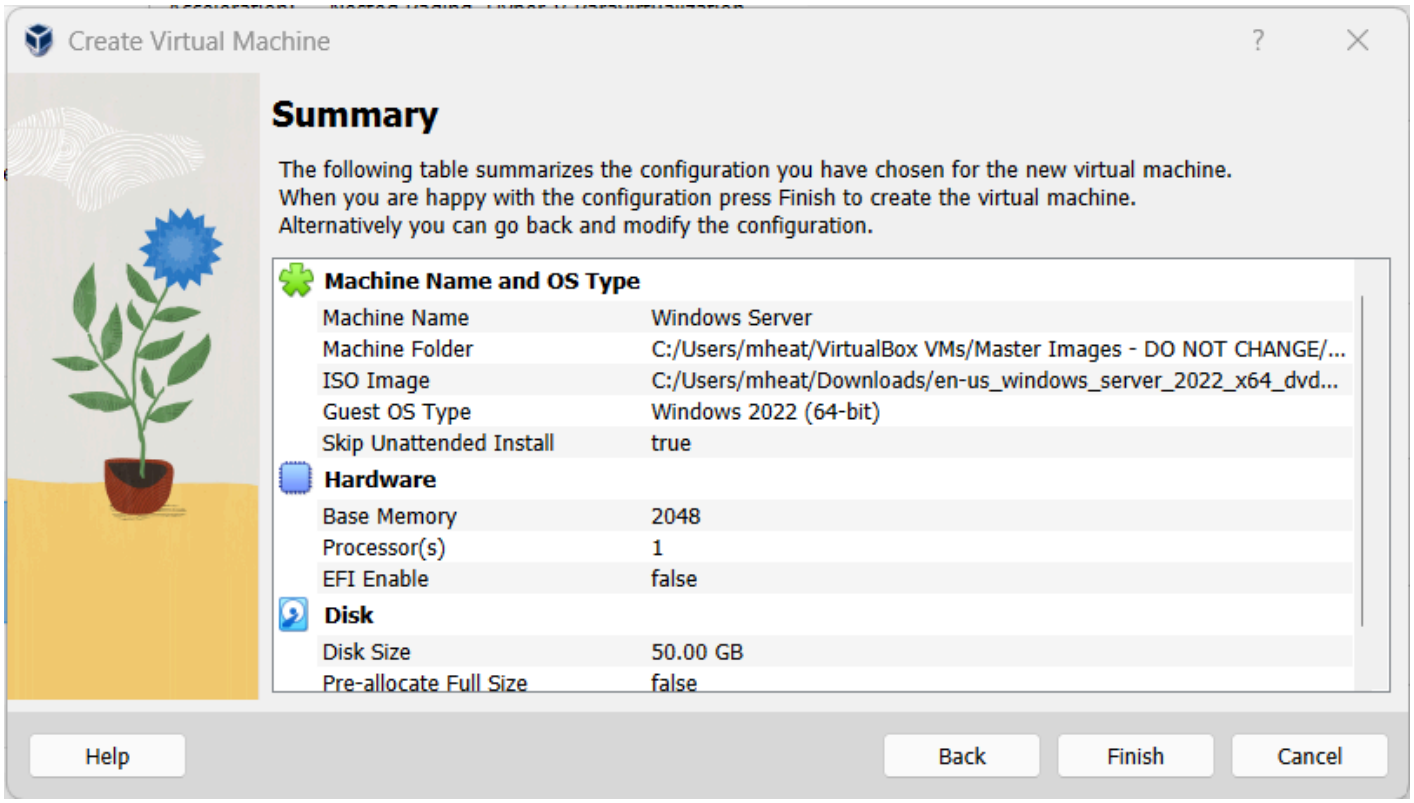


Figure 4 – Review and approve settings

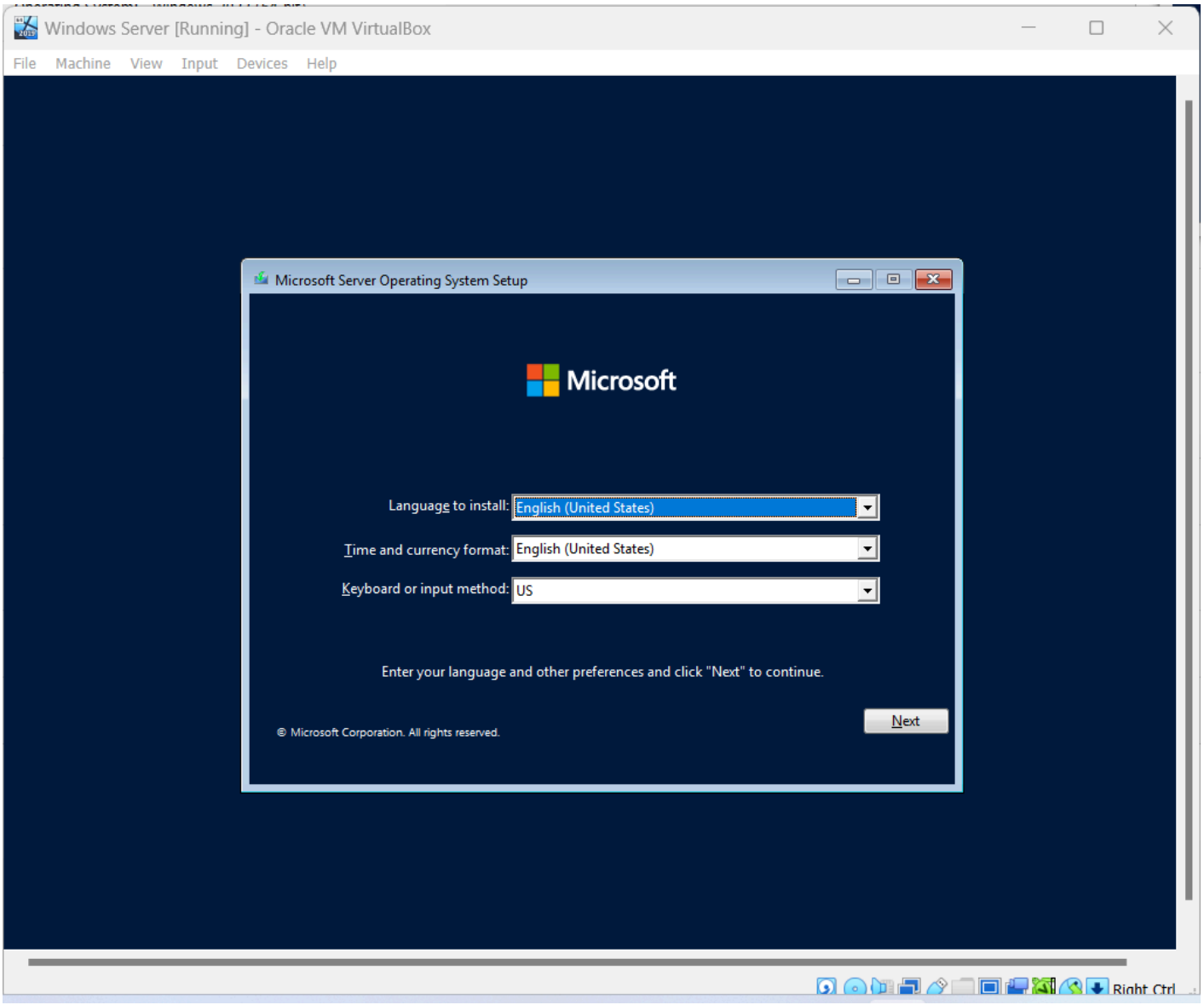


Figure 5 – Windows server default settings

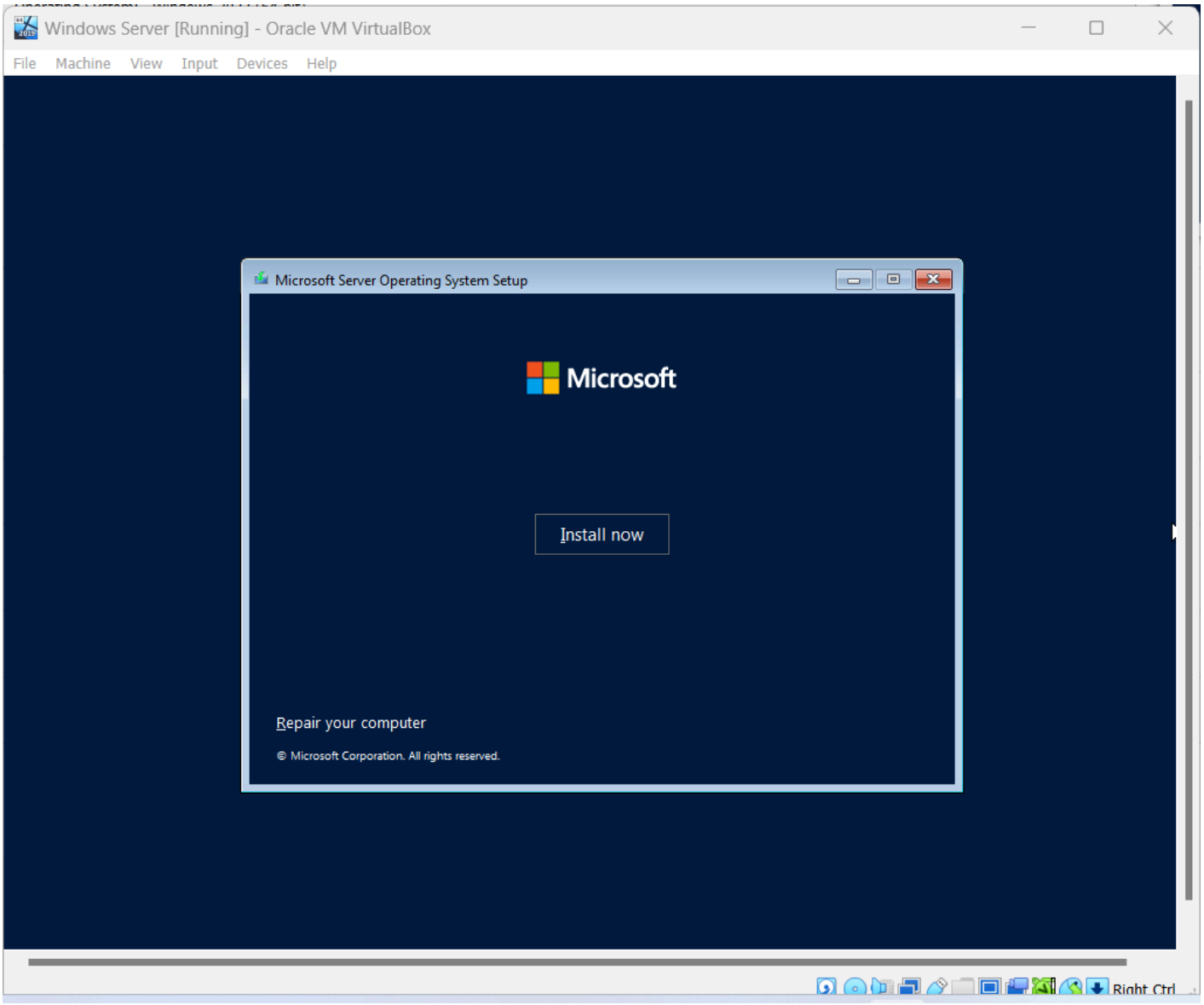


Figure 6 – Install now

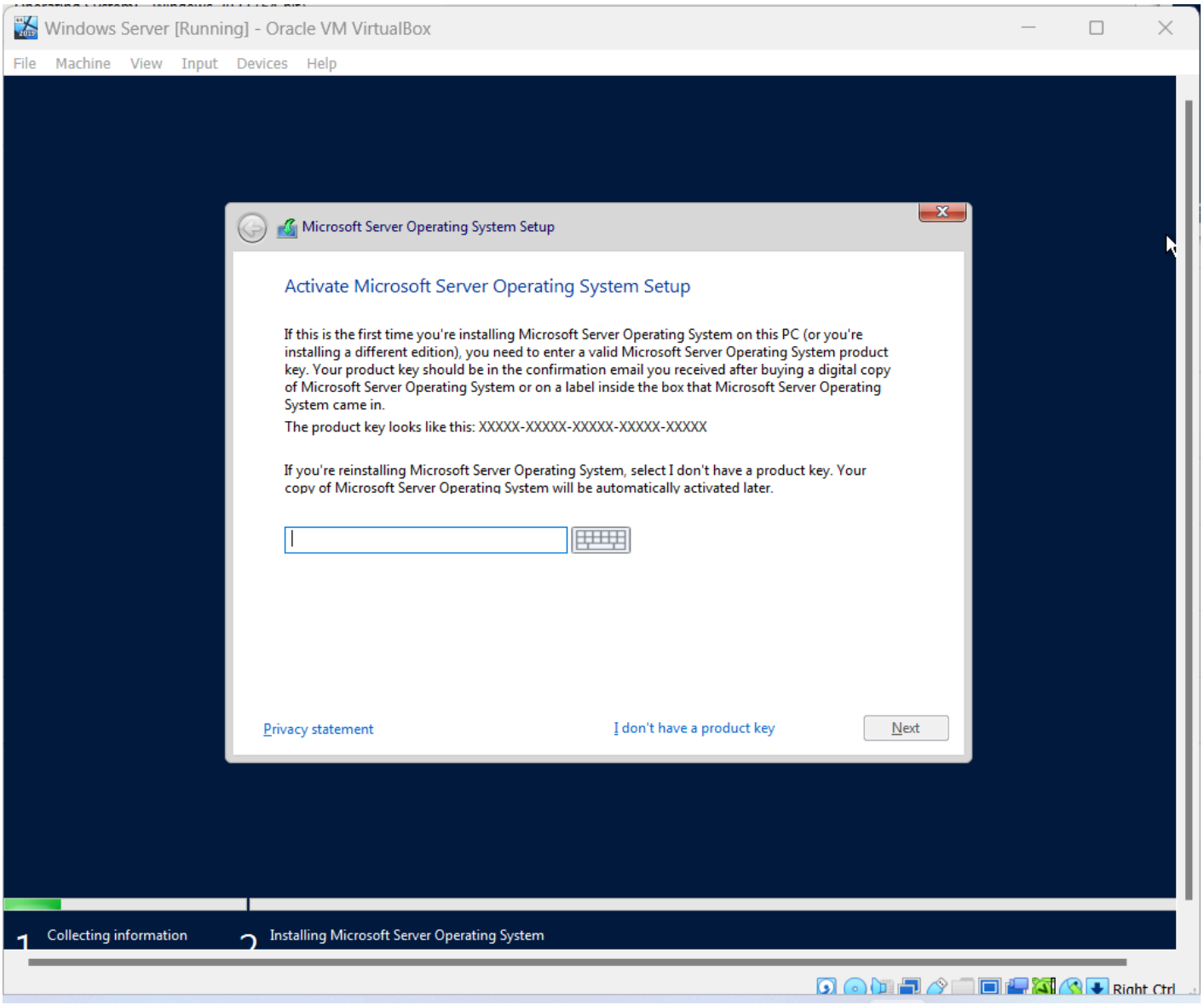


Figure 7 – Product key

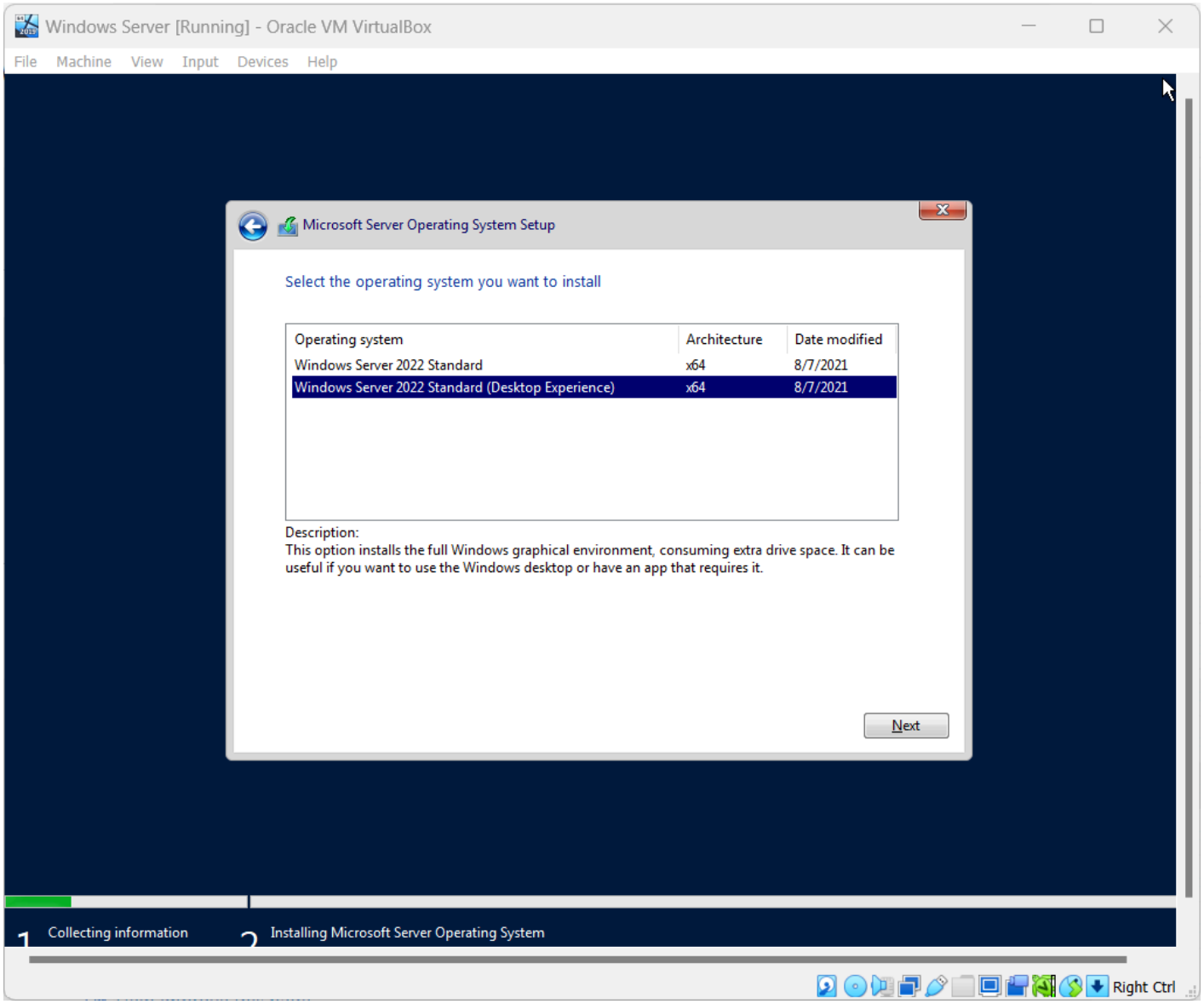


Figure 8 – Desktop Experience

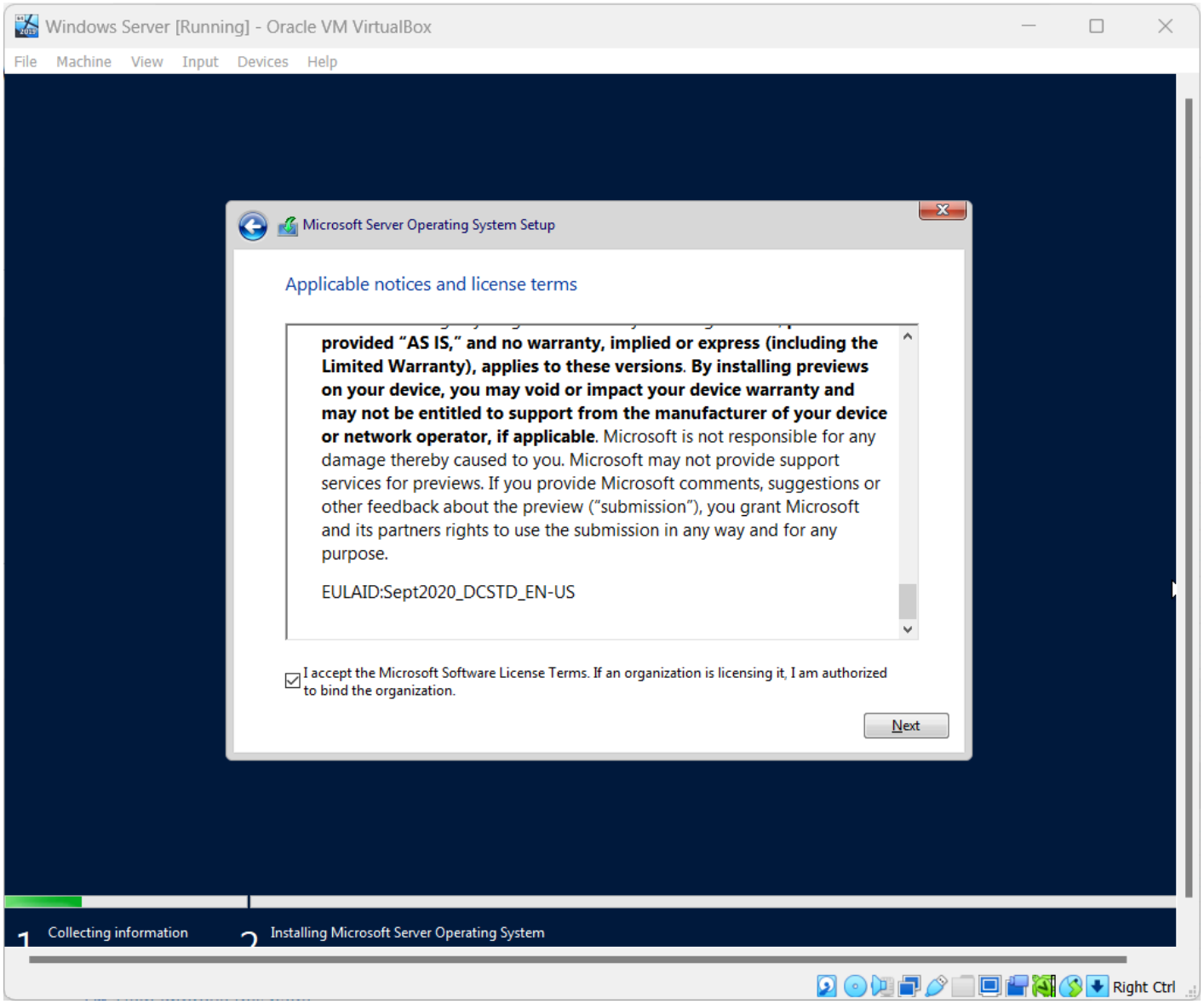


Figure 9 – Accept license terms

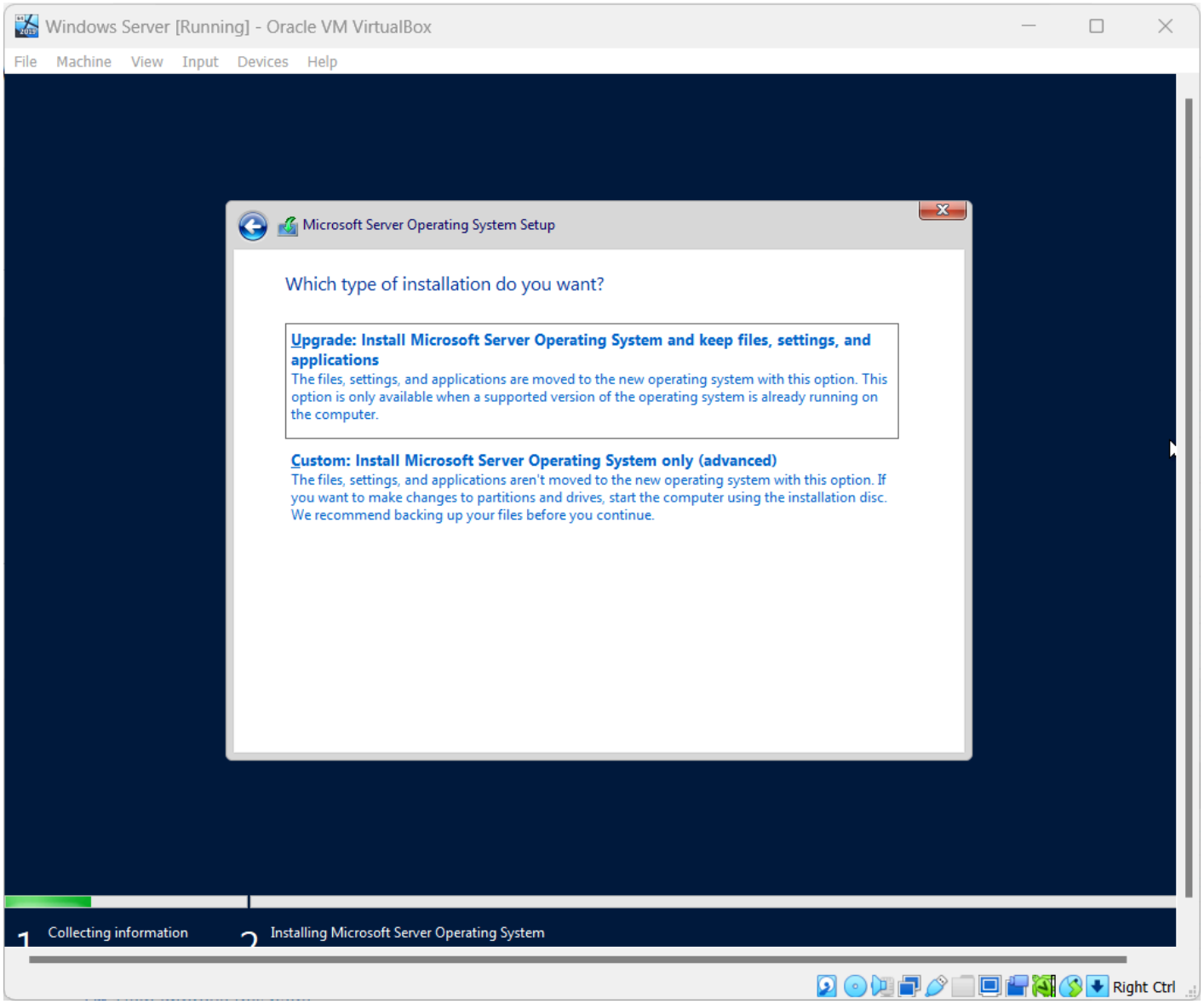


Figure 10 – Custom install

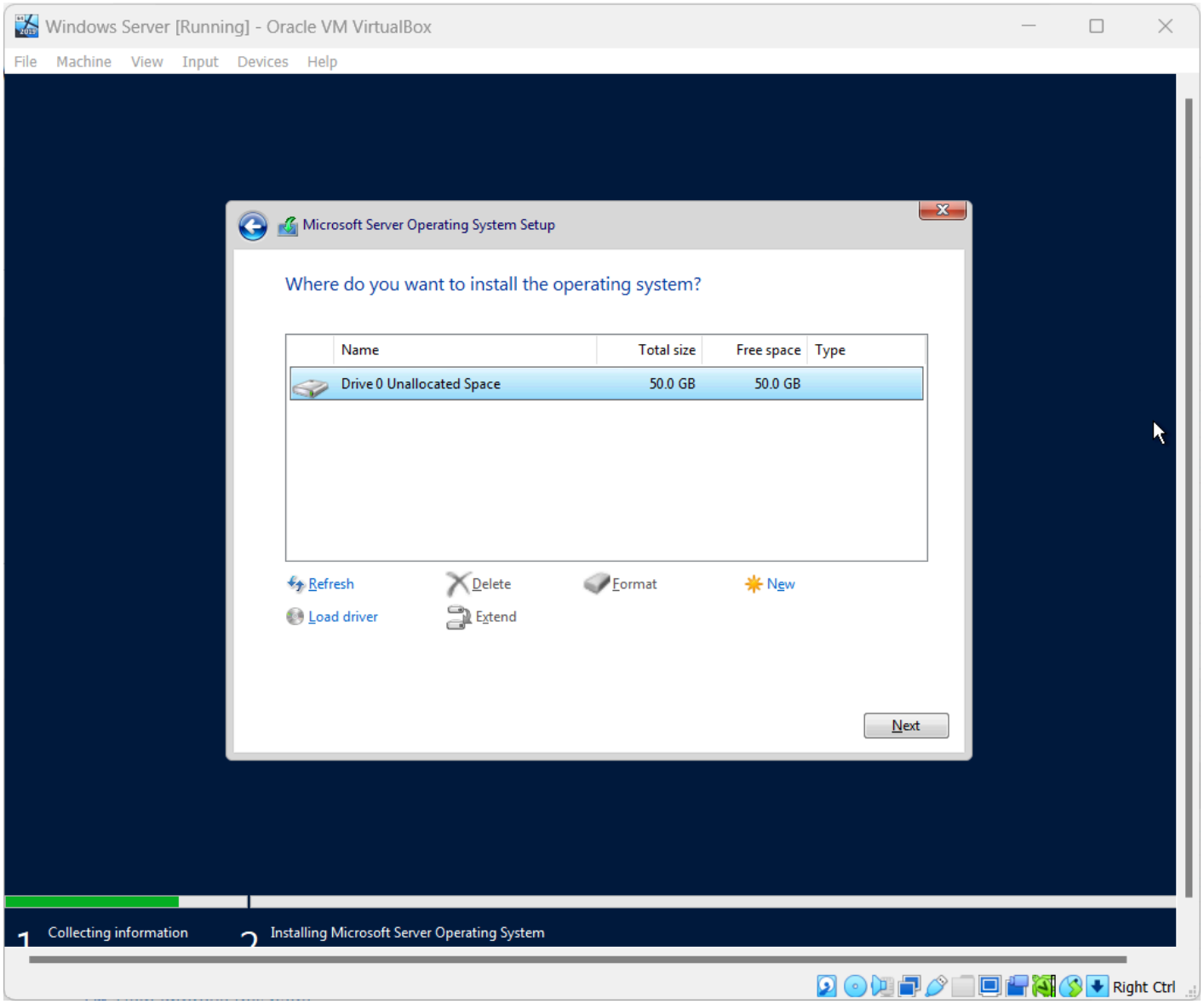


Figure 11 – Use defaults

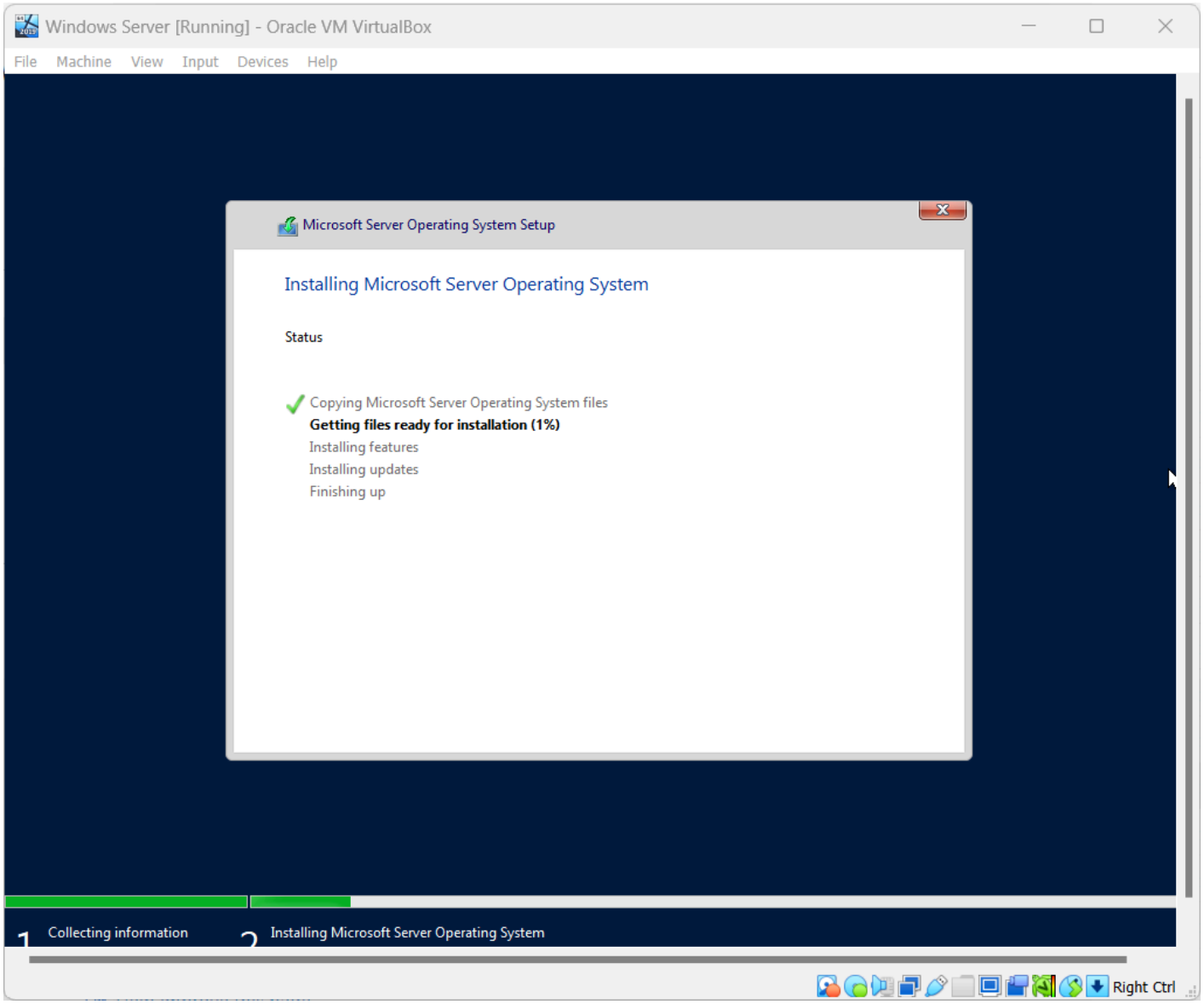


Figure 12 – Waiting for installation to finish

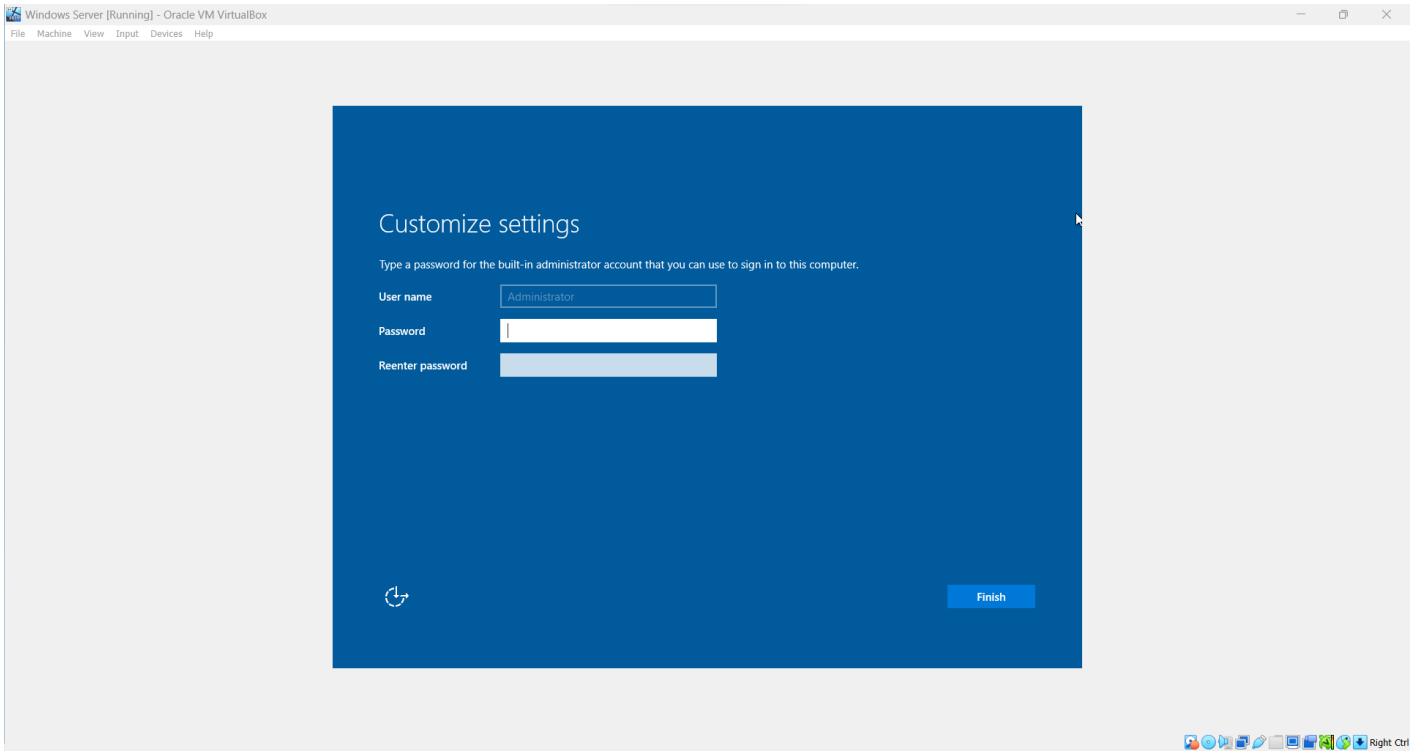


Figure 13 – Set the password

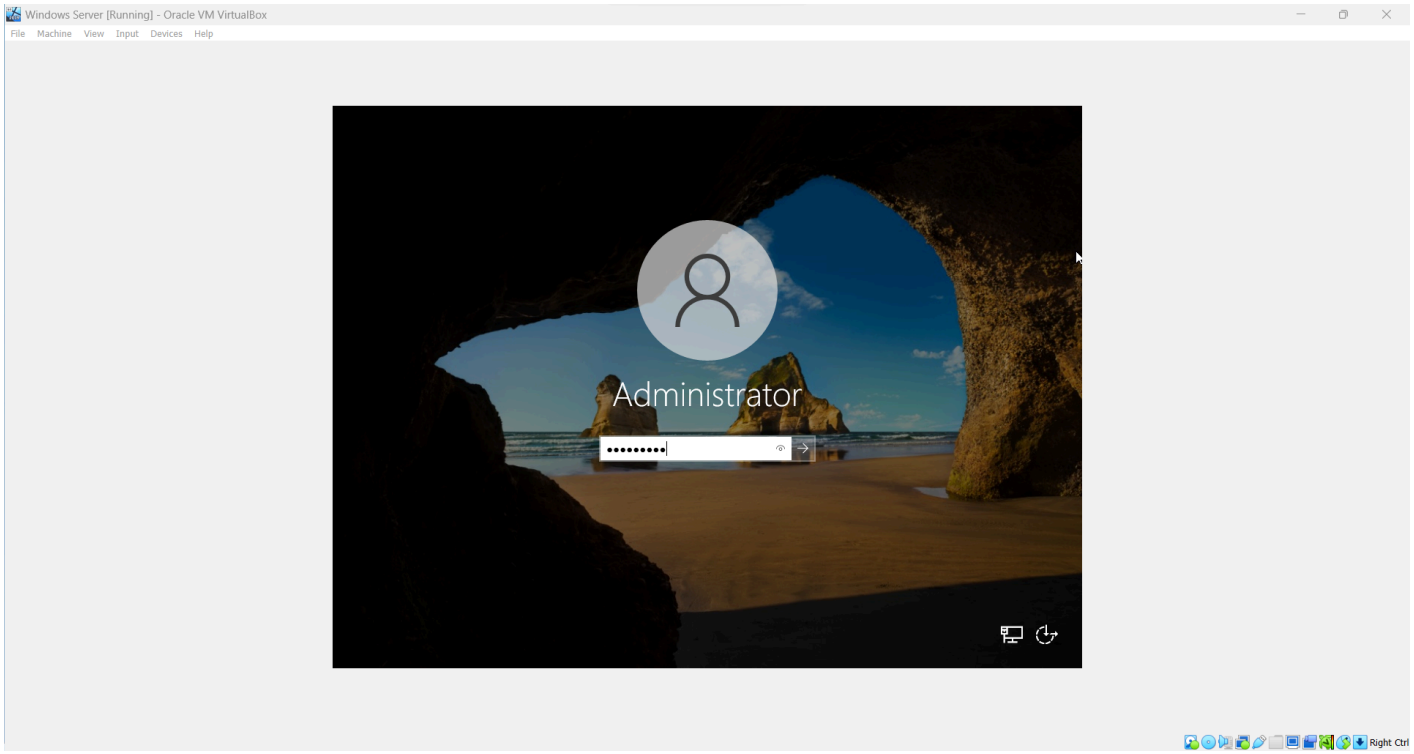


Figure 14 – Login as admin

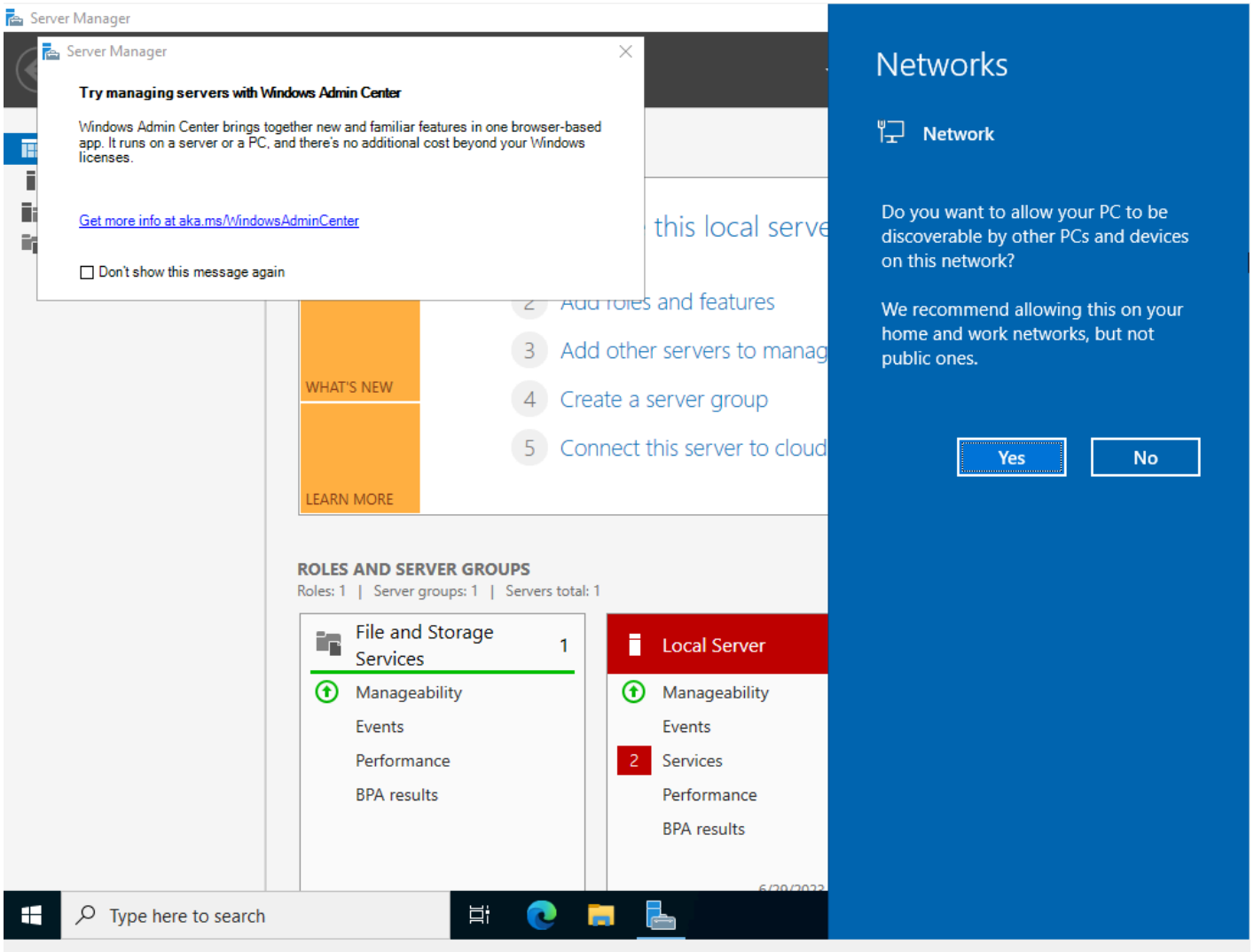


Figure 15 – First start up

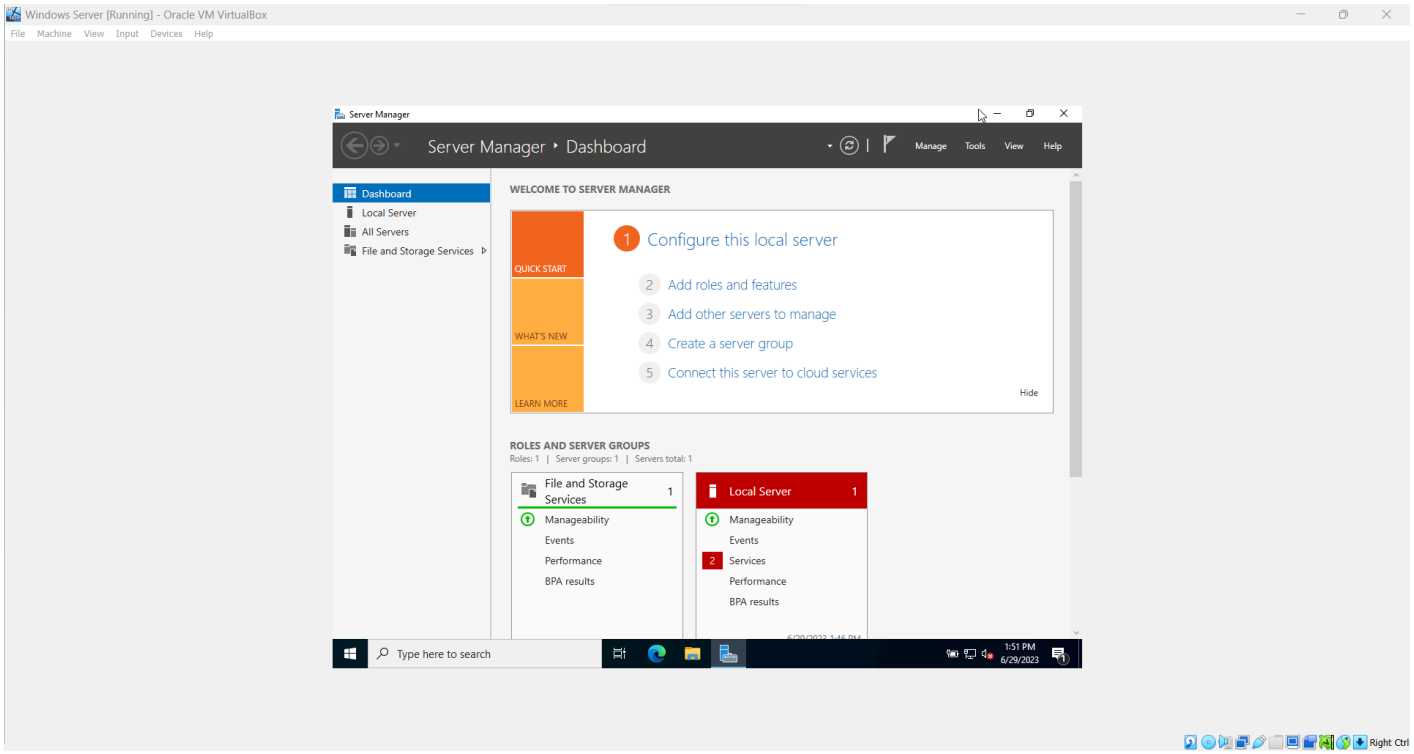


Figure 16 – Server manager dashboard

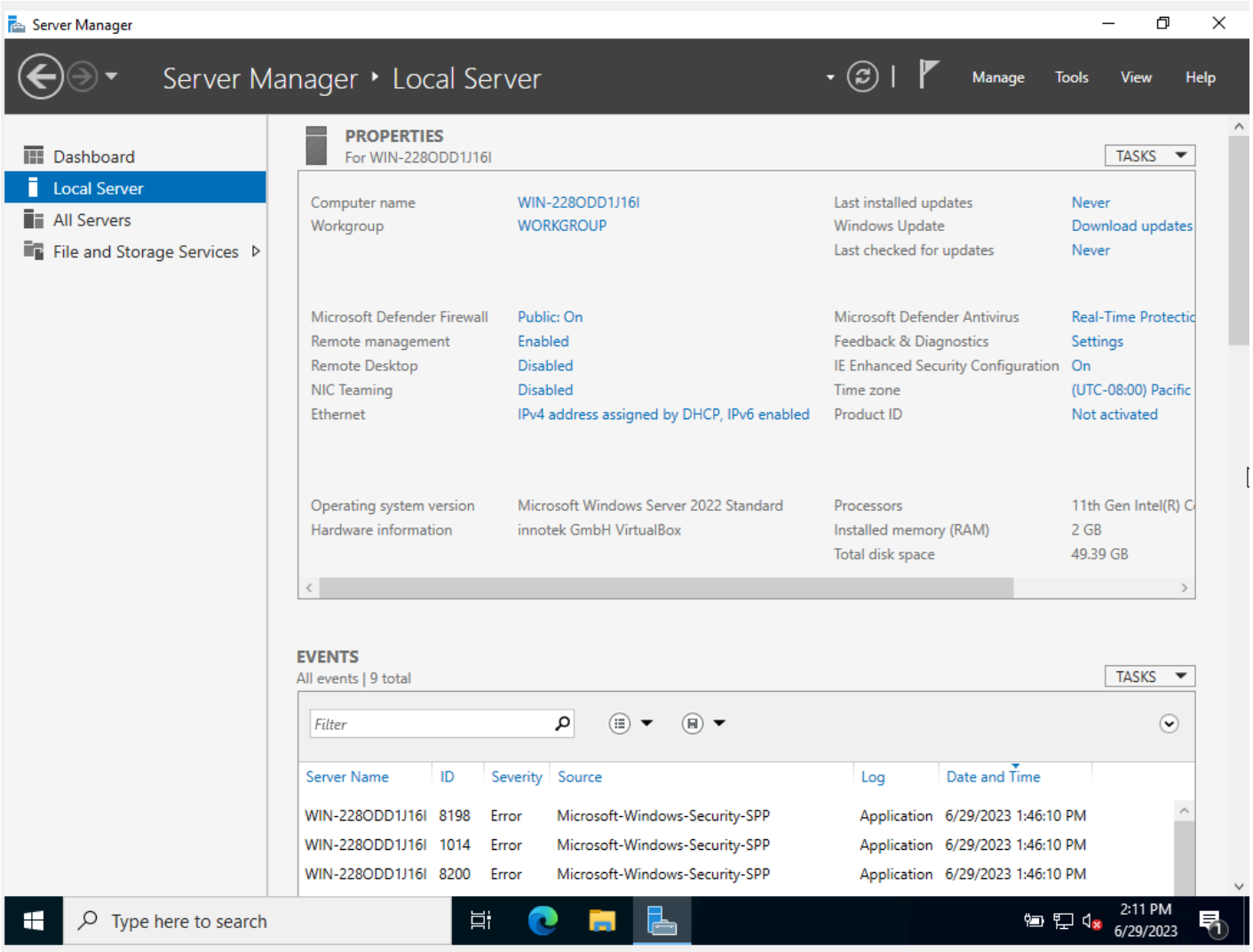


Figure 17 – Local Server

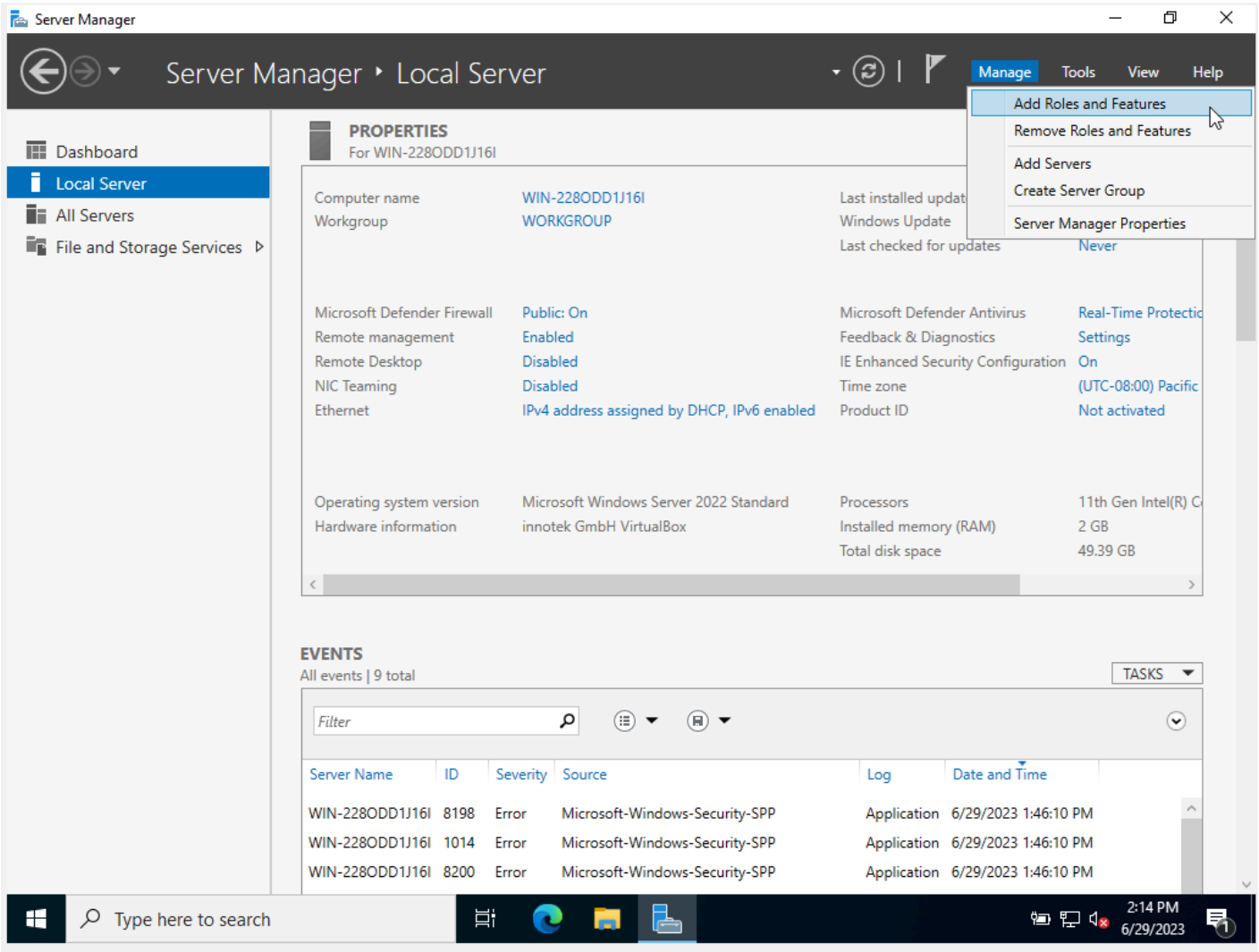


Figure 18 – Add roles and features

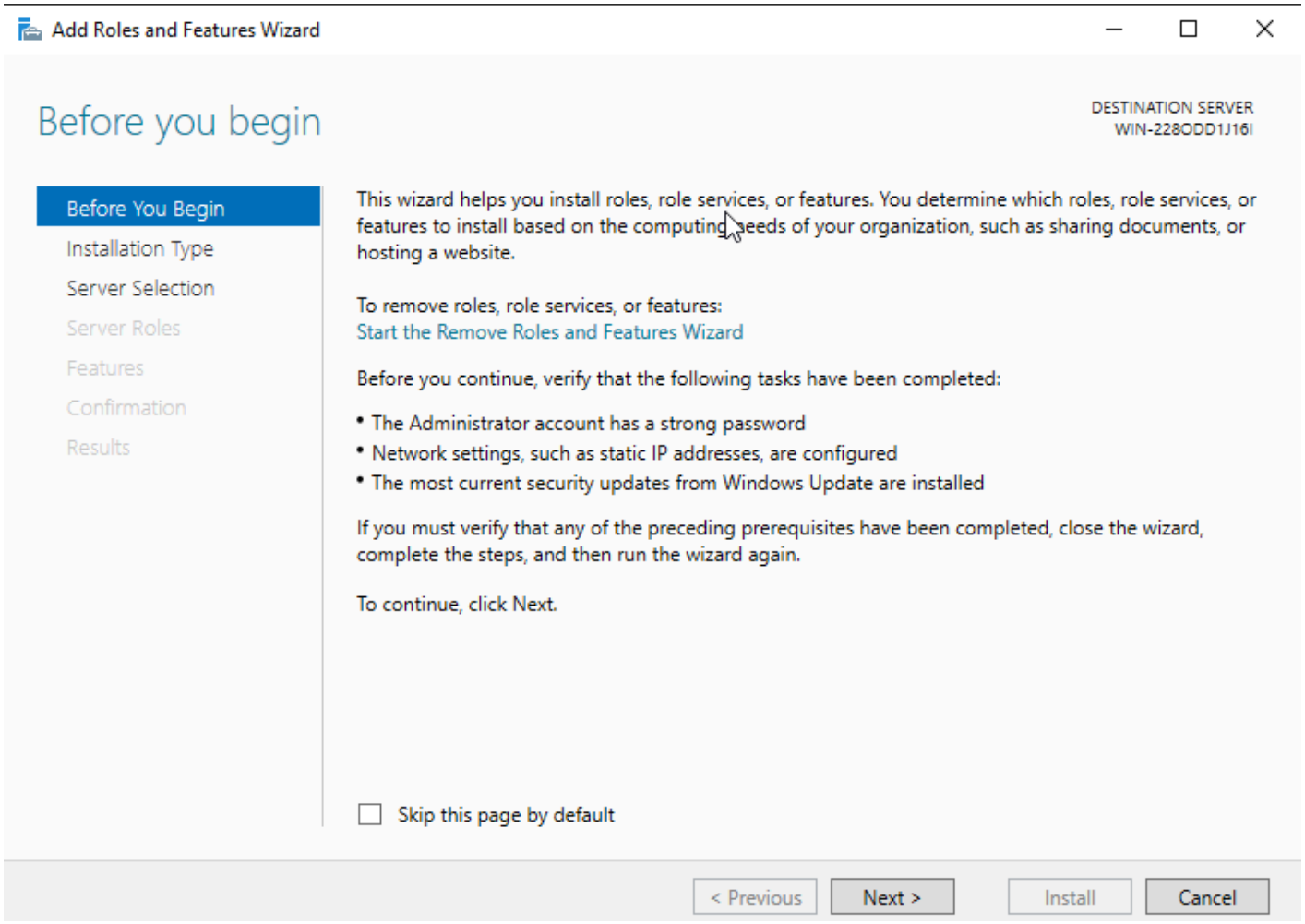


Figure 19 – Click next

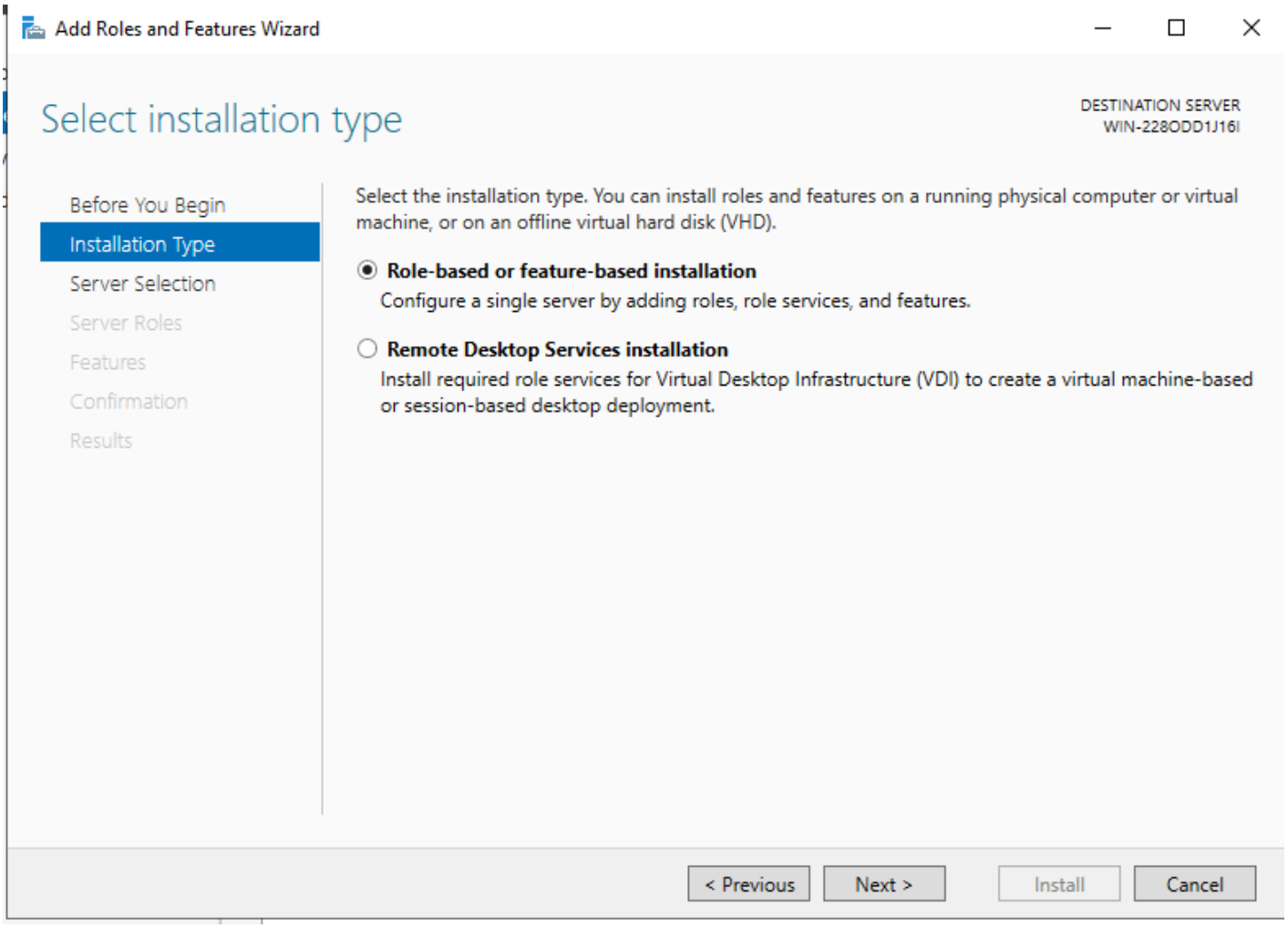


Figure 20 – Installation type, Roll-based

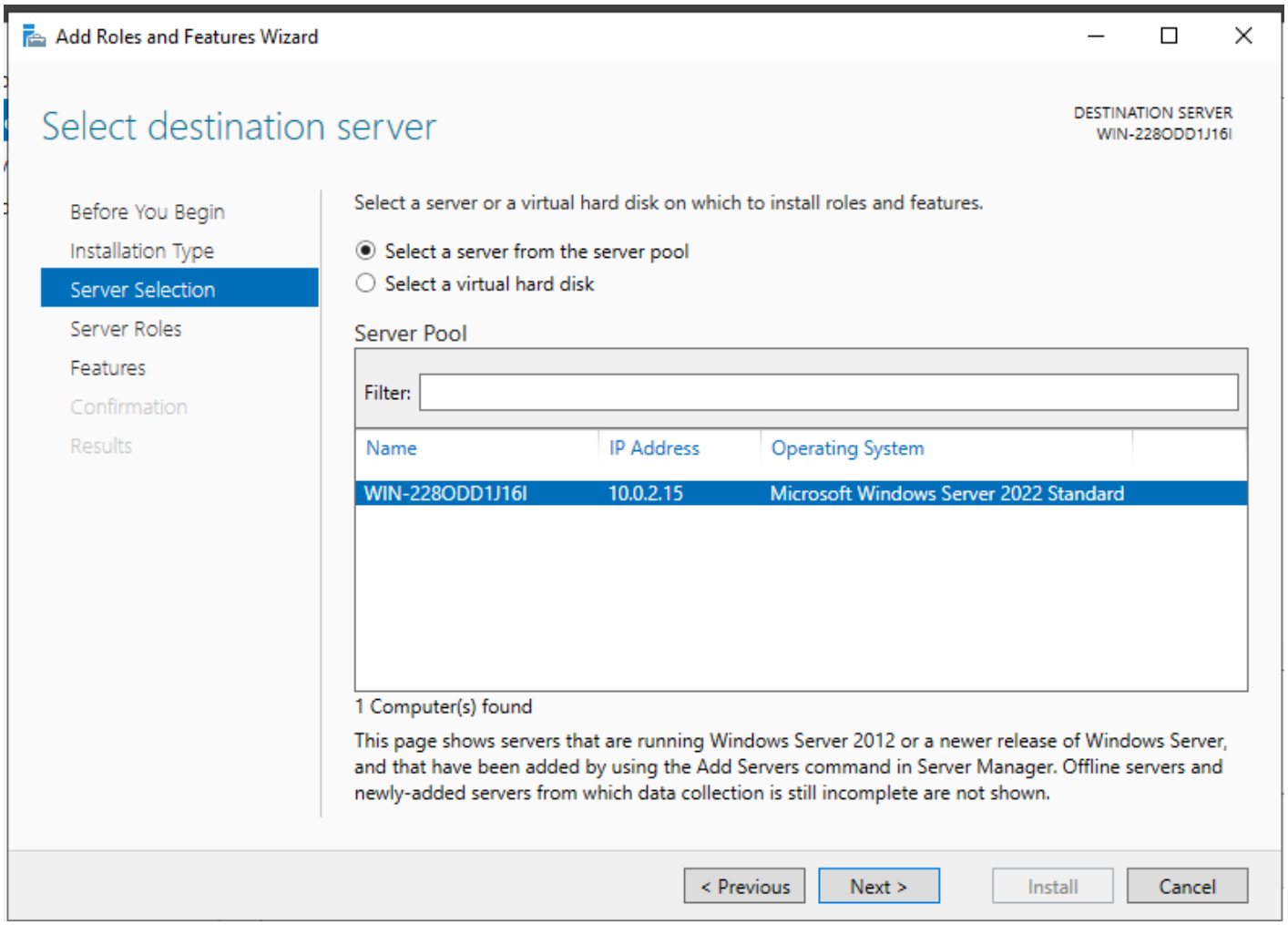


Figure 21 – Select the server

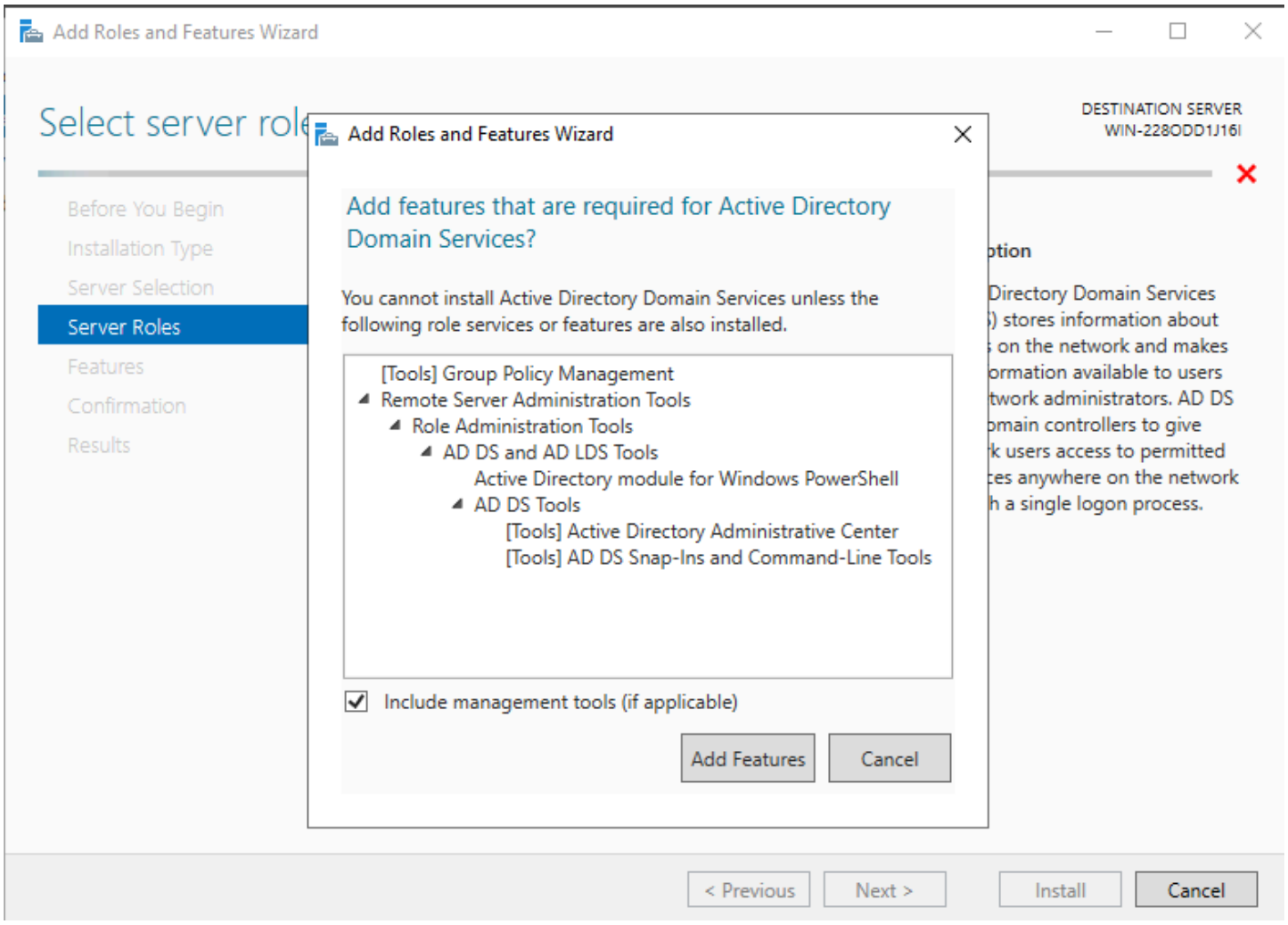


Figure 22 – Add features to active directory

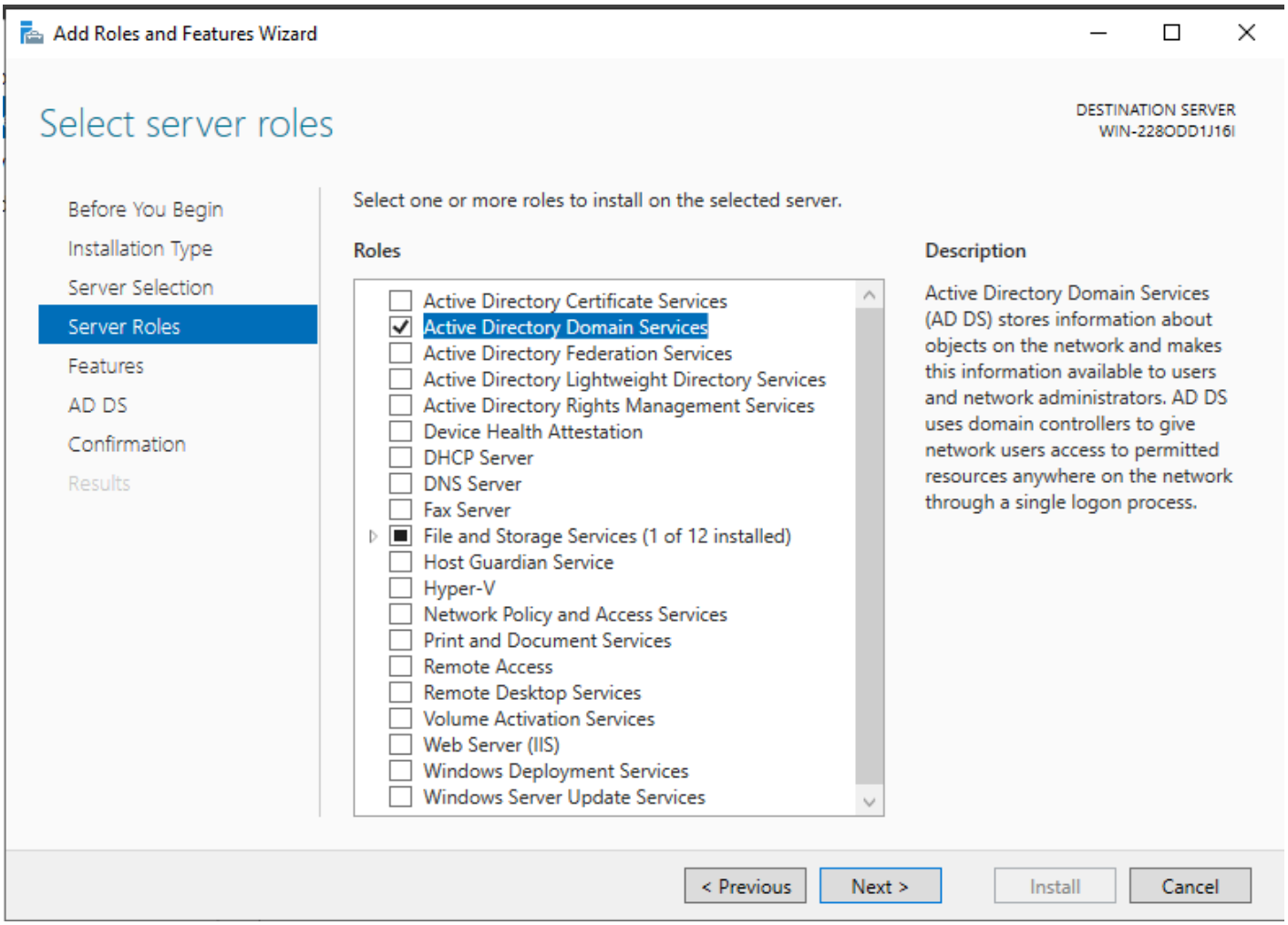


Figure 23 – Select server roles

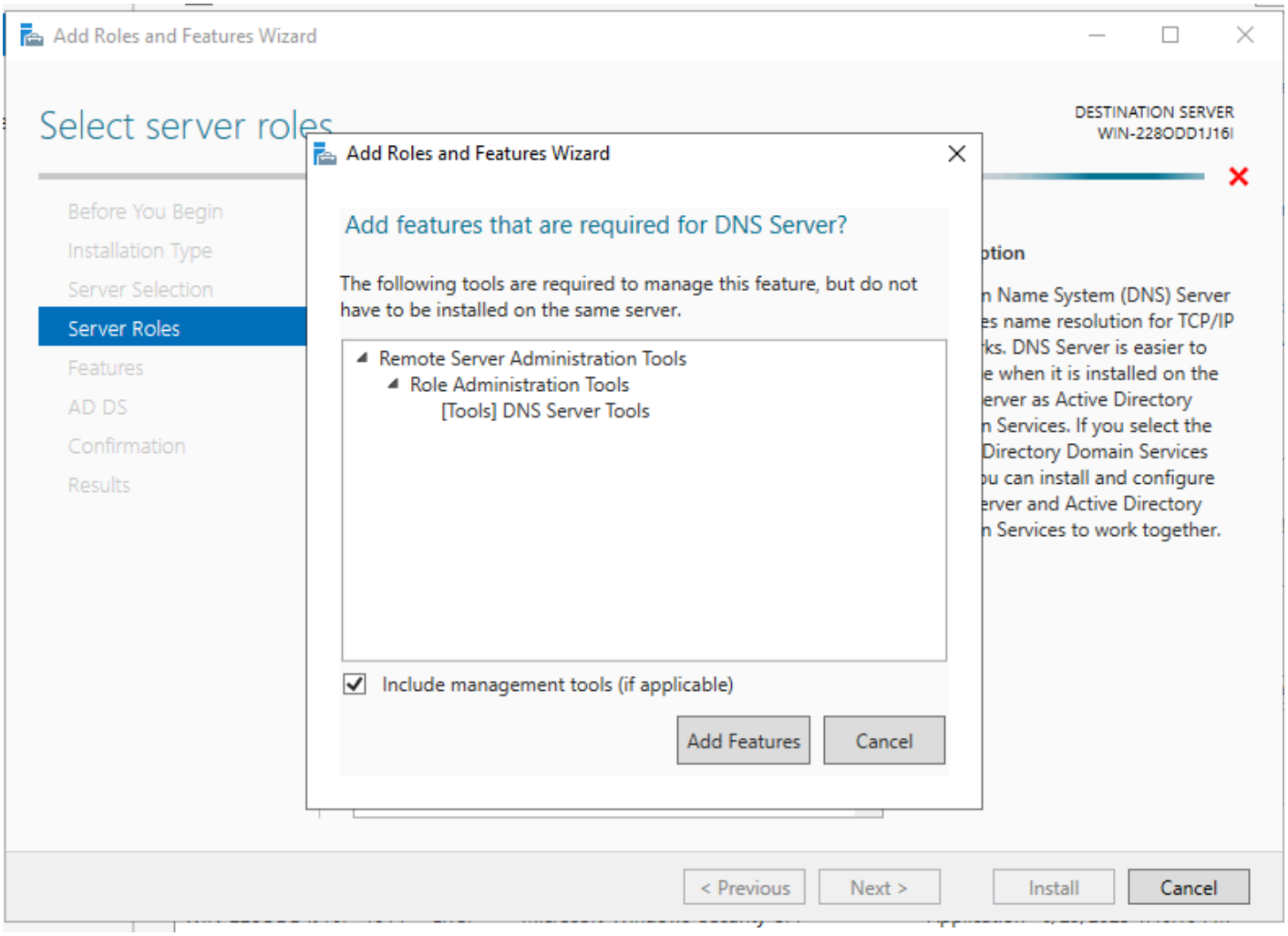


Figure 24 – Add features to DNS

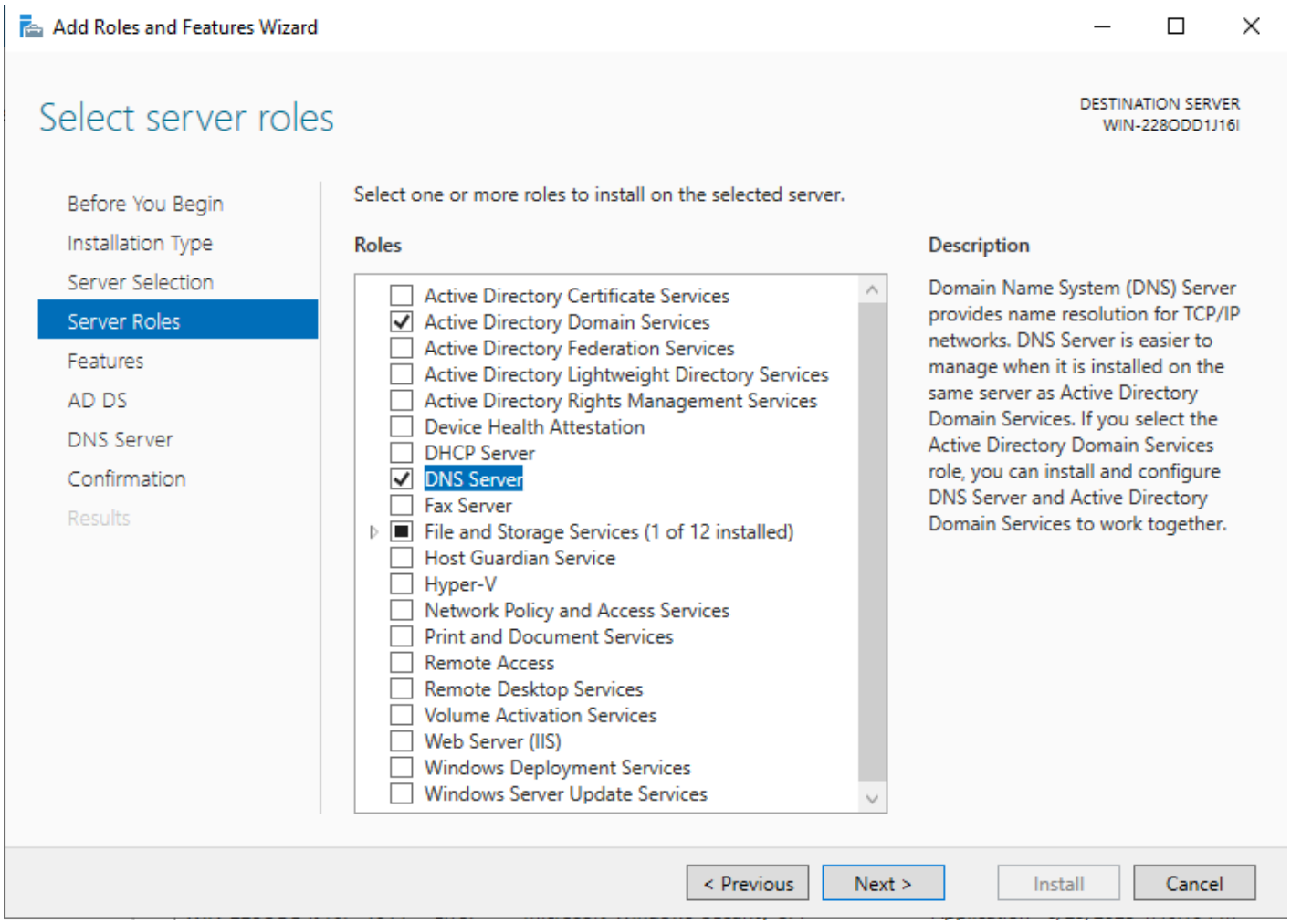


Figure 25 – Verify changes and select next

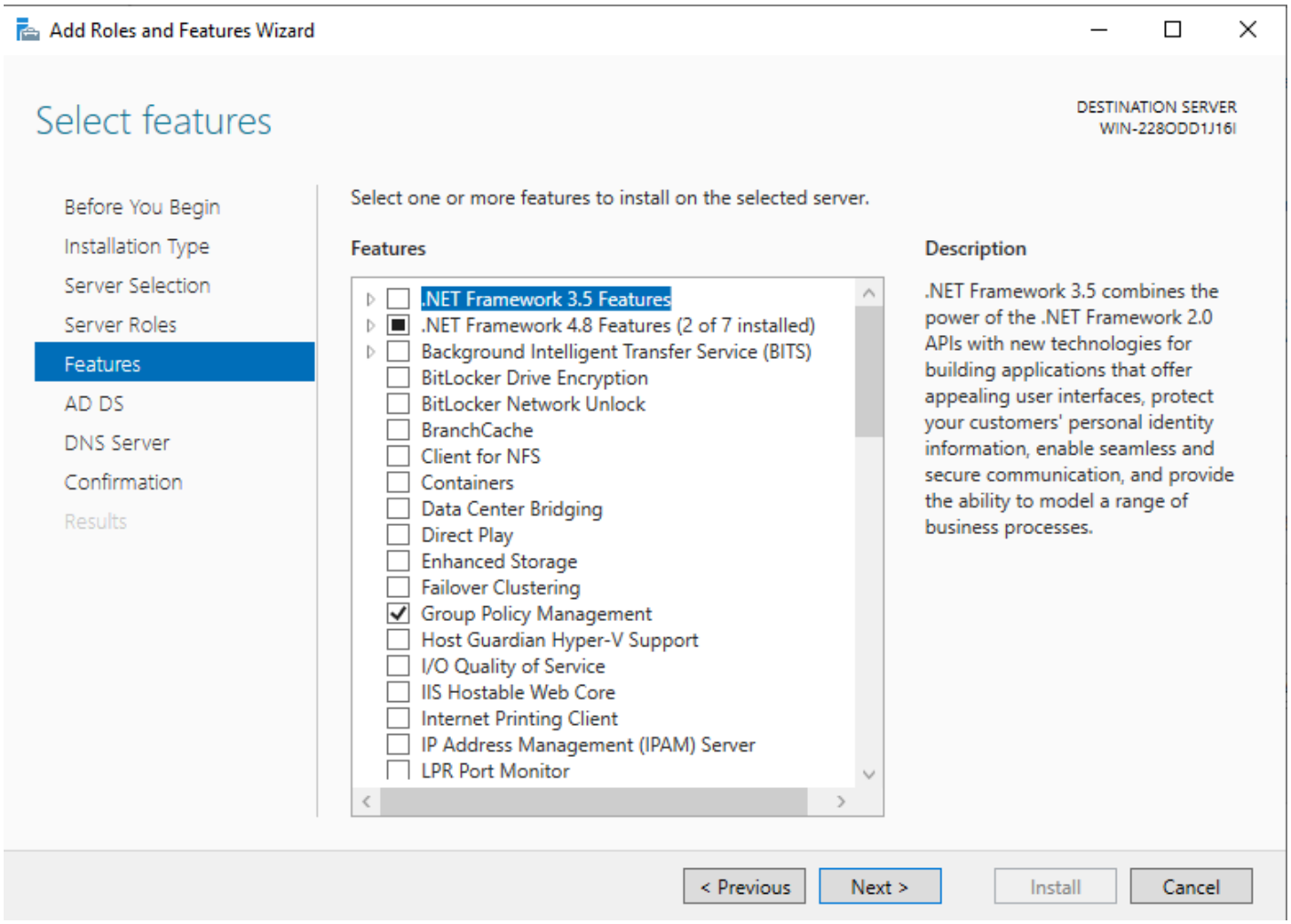


Figure 26 – Confirm Features

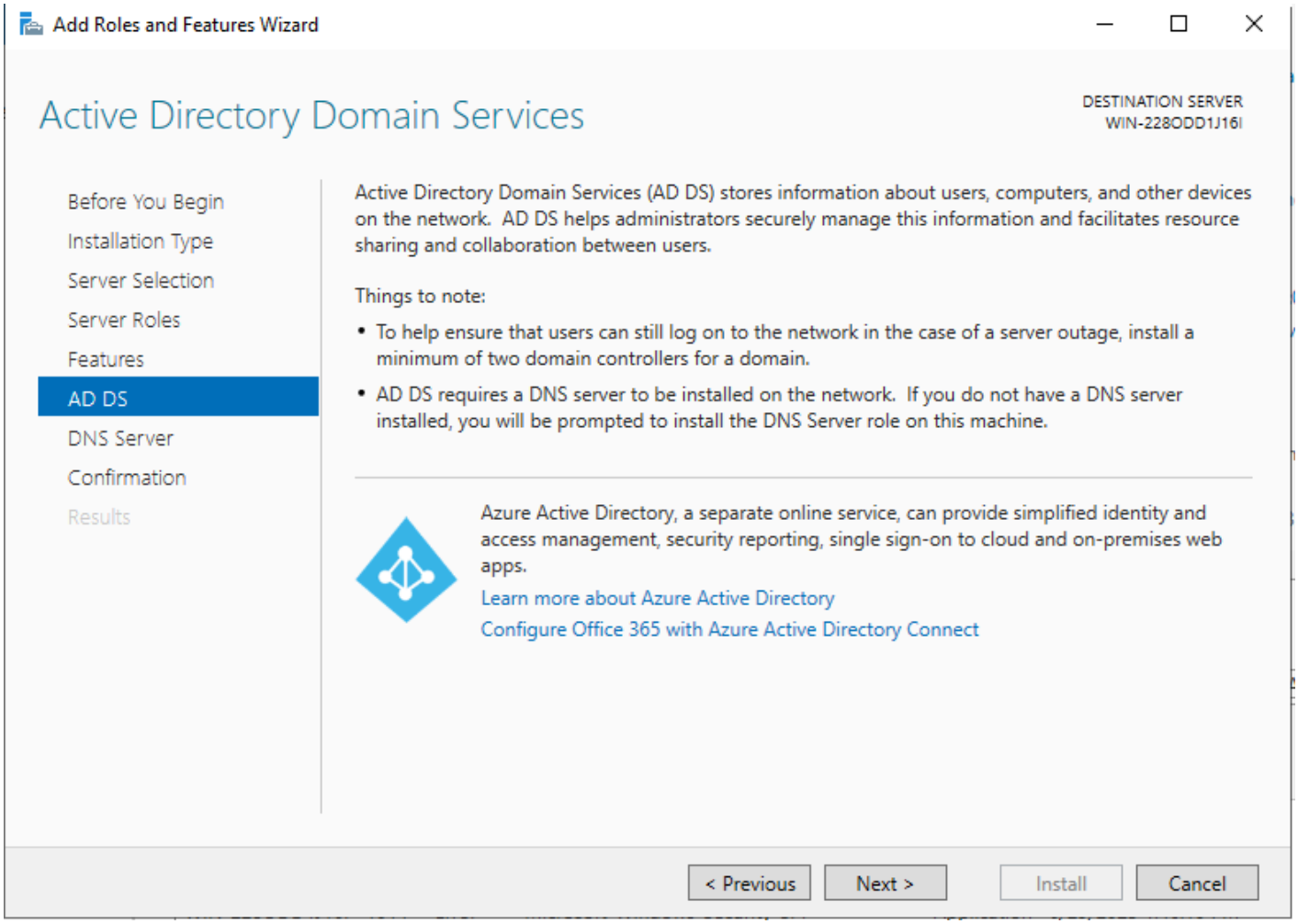


Figure 27 – Confirm AD DS

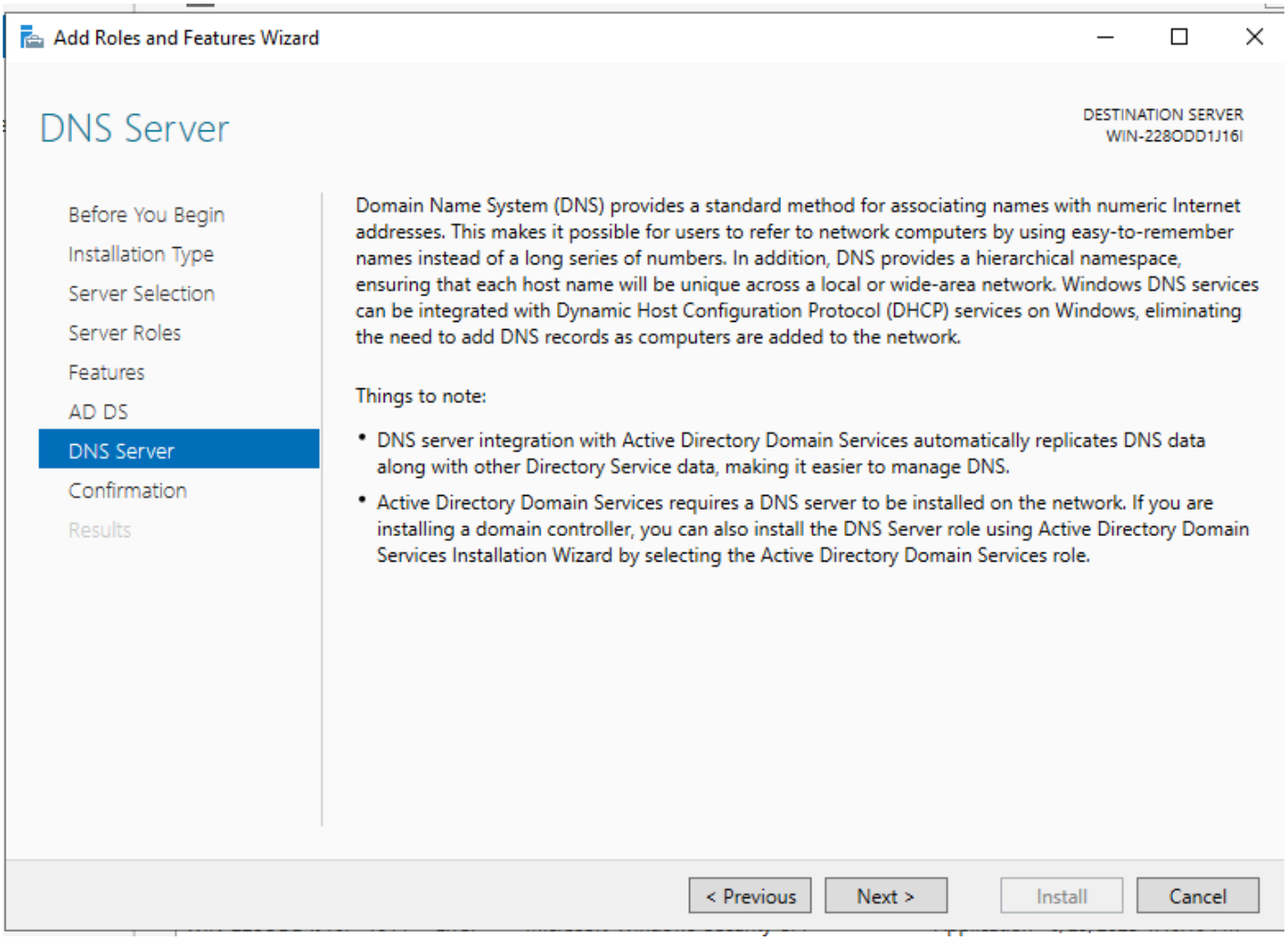


Figure 28 – Confirm DNS

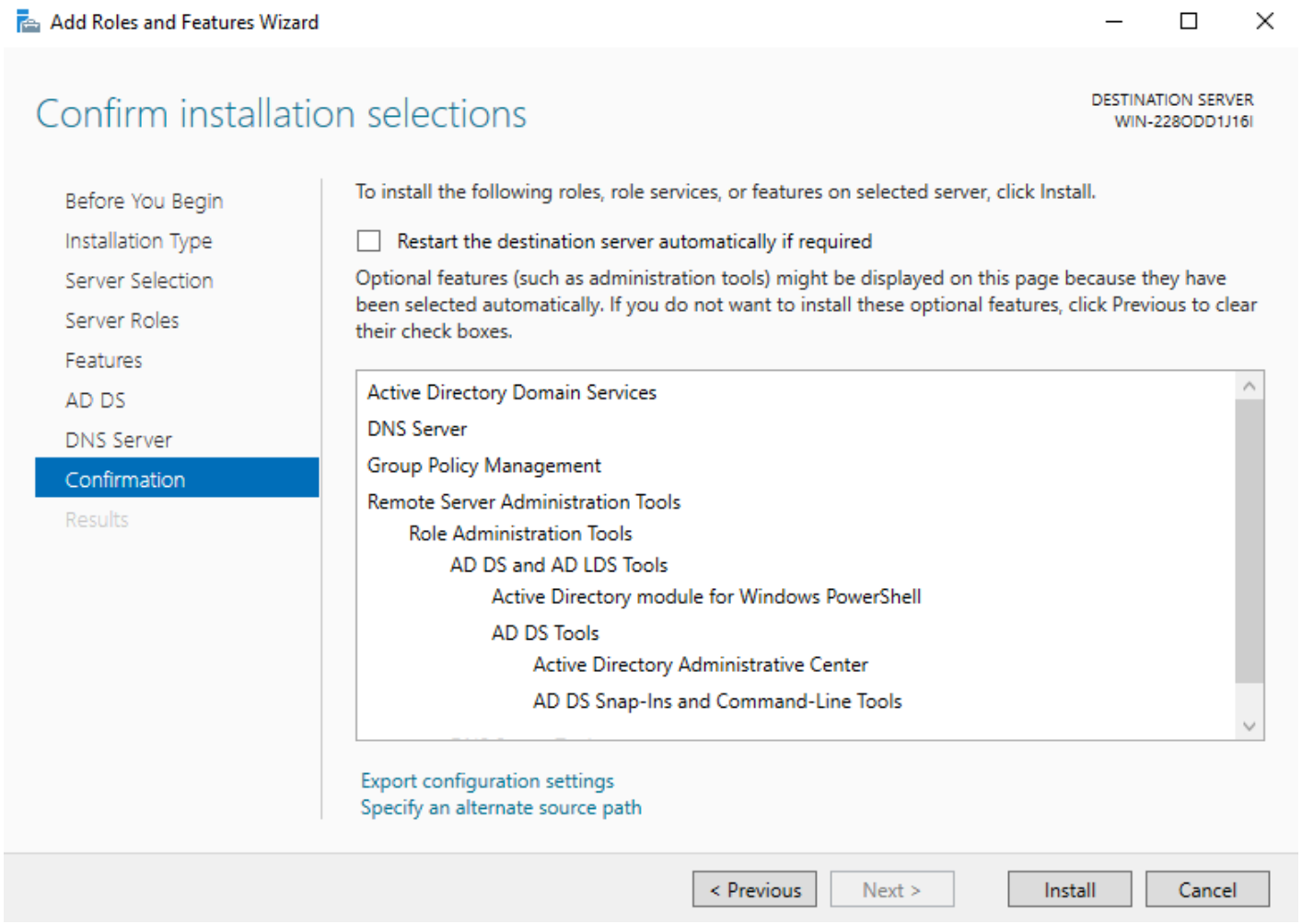


Figure 29 – Confirm settings

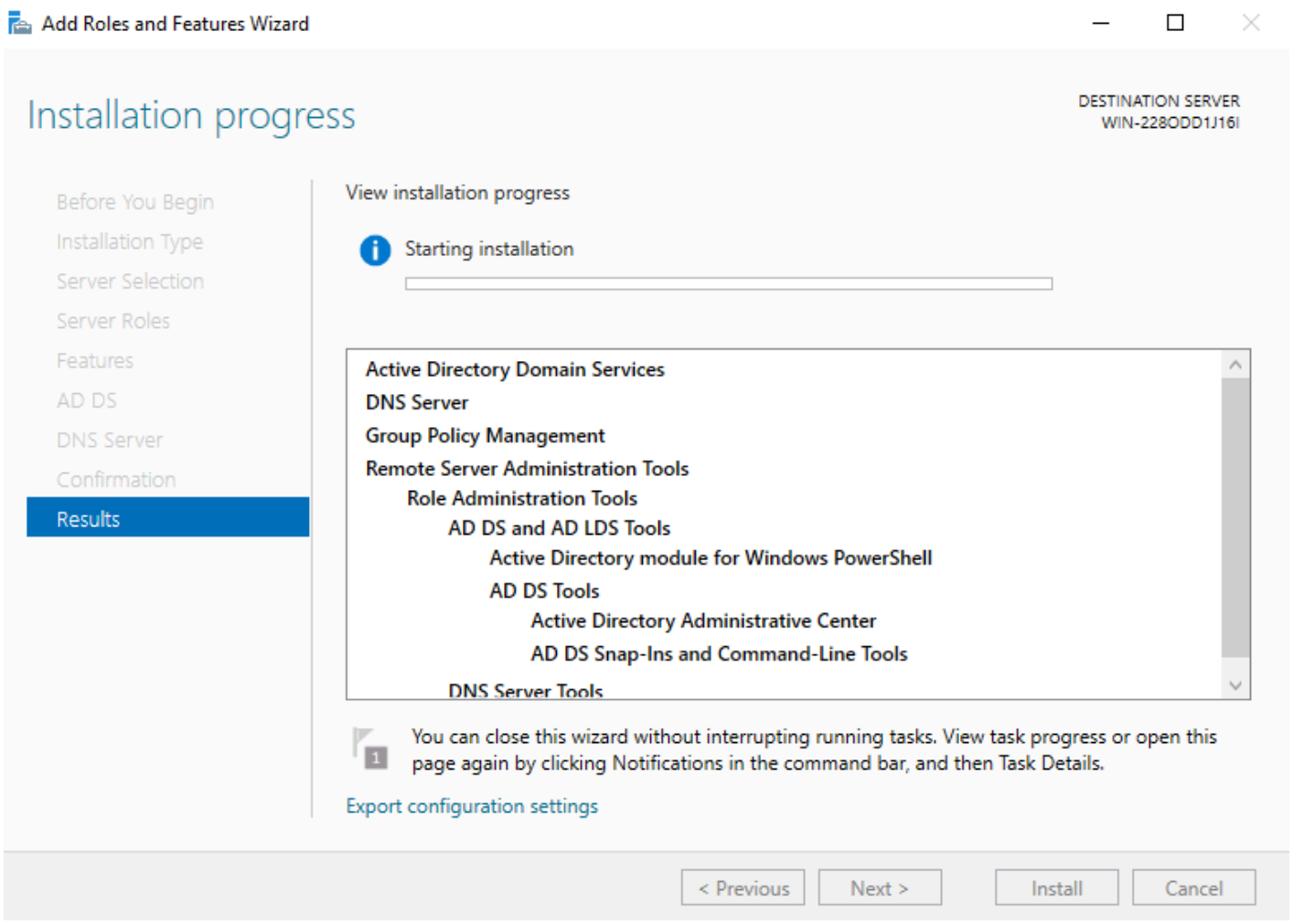


Figure 30 – Wait for installation

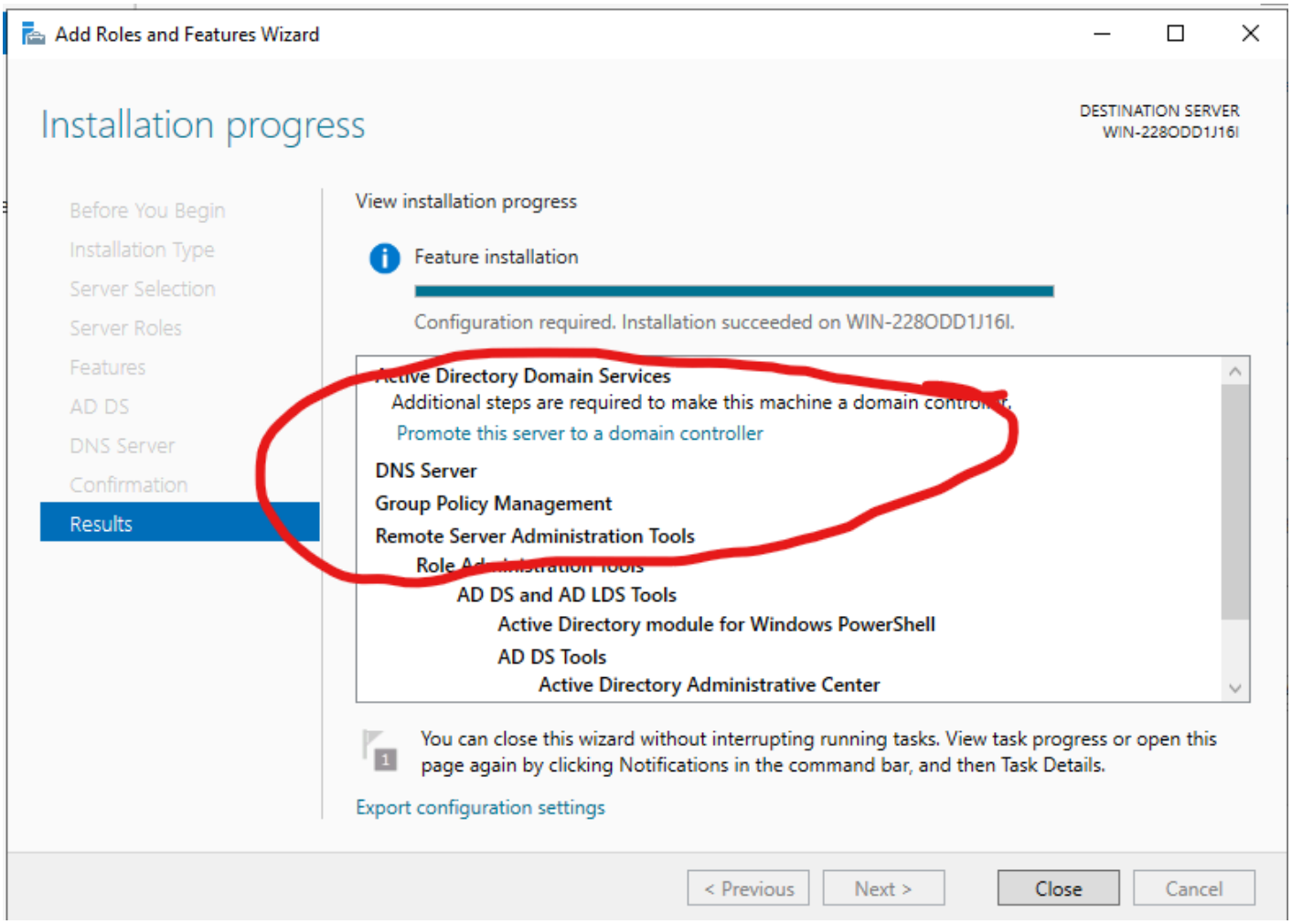


Figure 31 – Promote the server

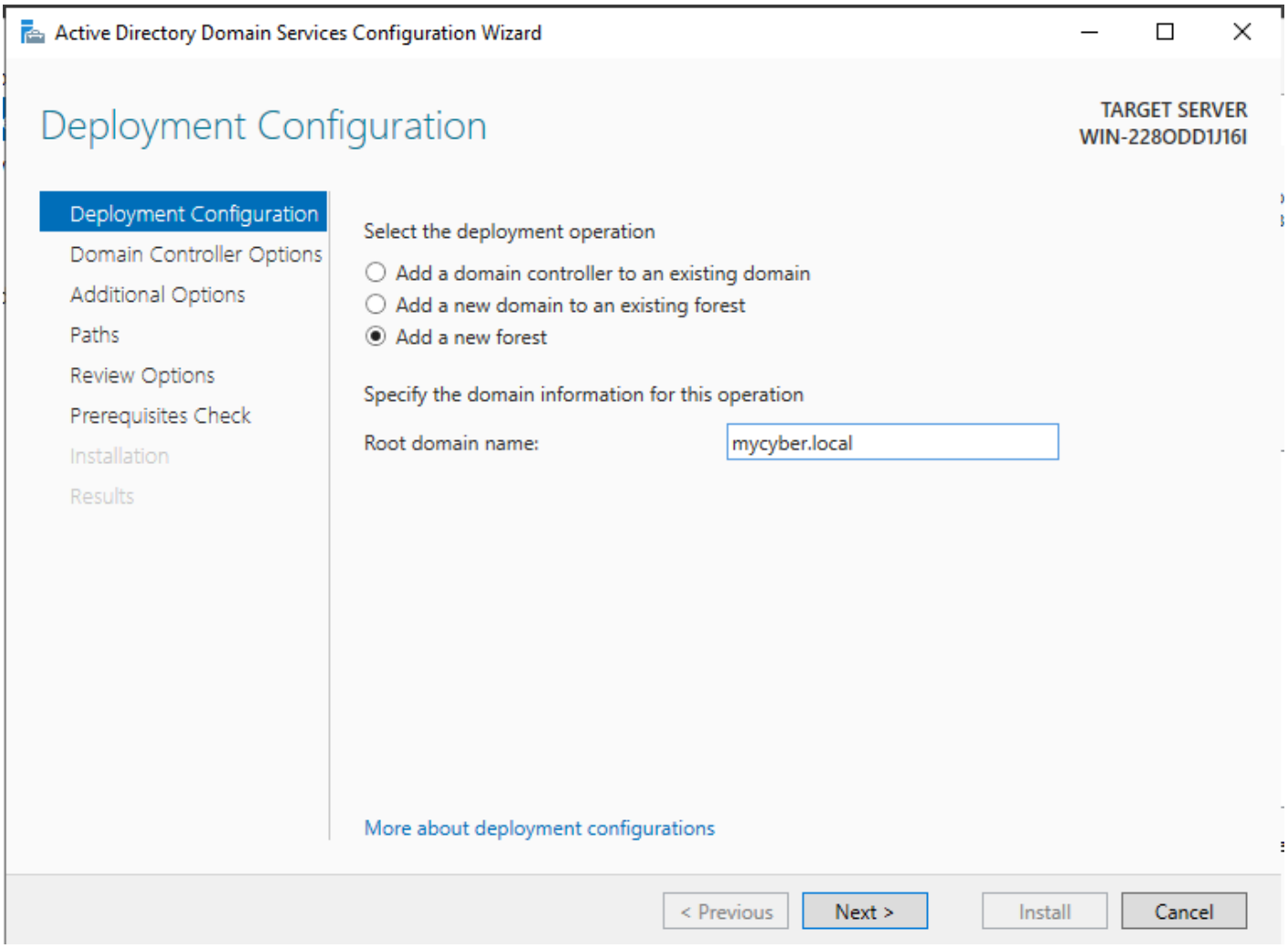


Figure 32 – Active Directory Domain Services Wizard

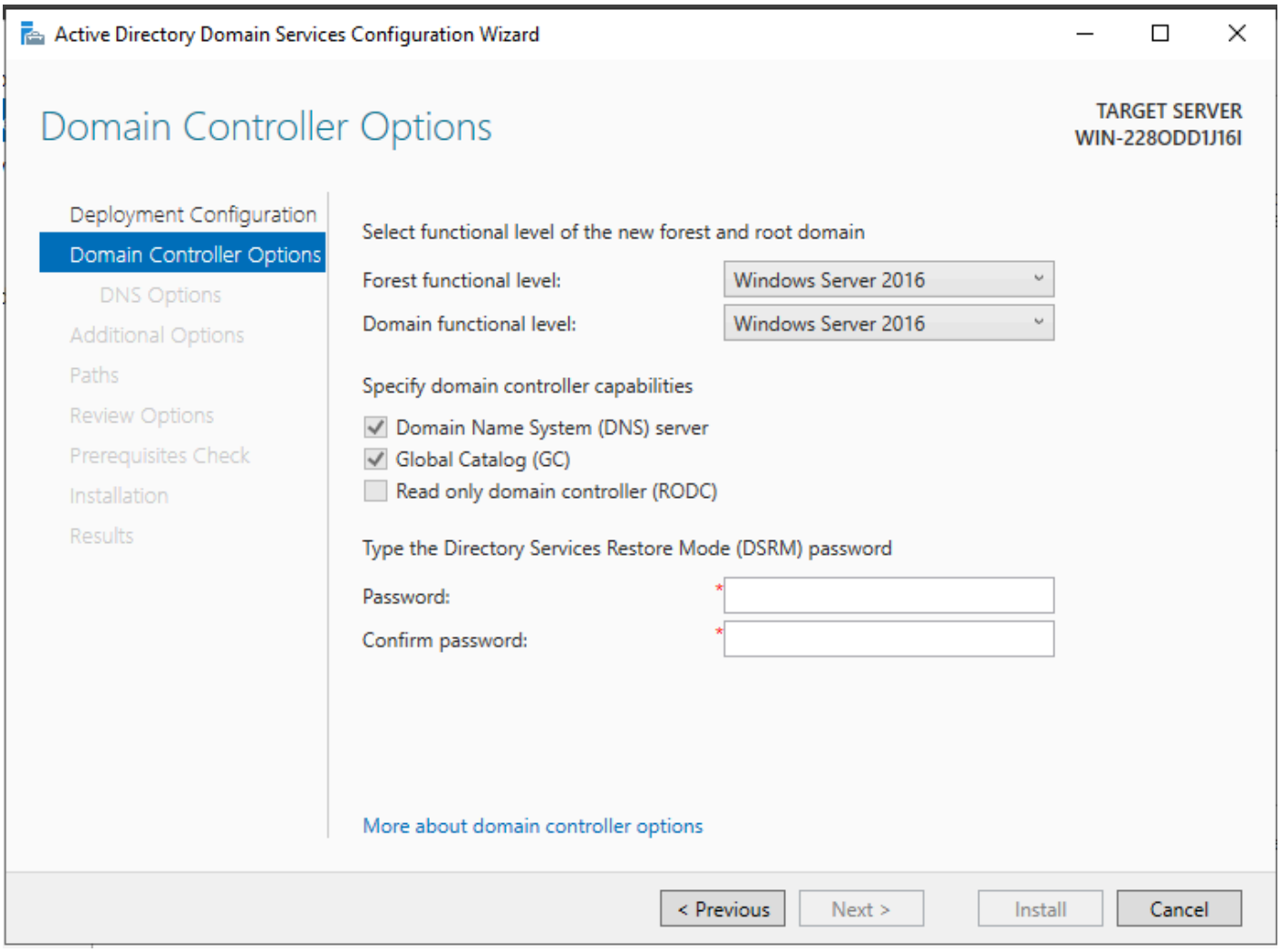


Figure 33 – Set password for DC

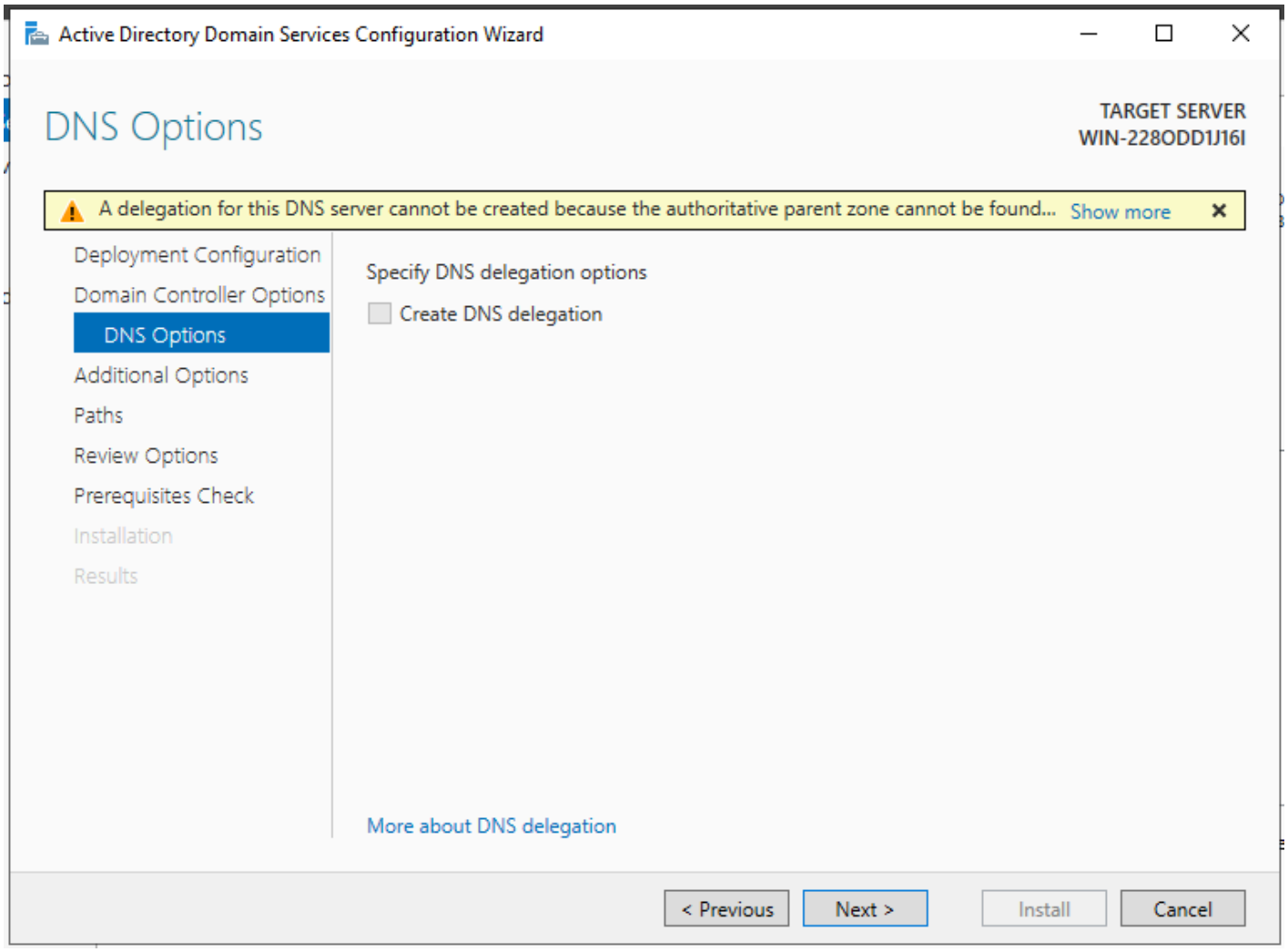


Figure 34 – DNS Options

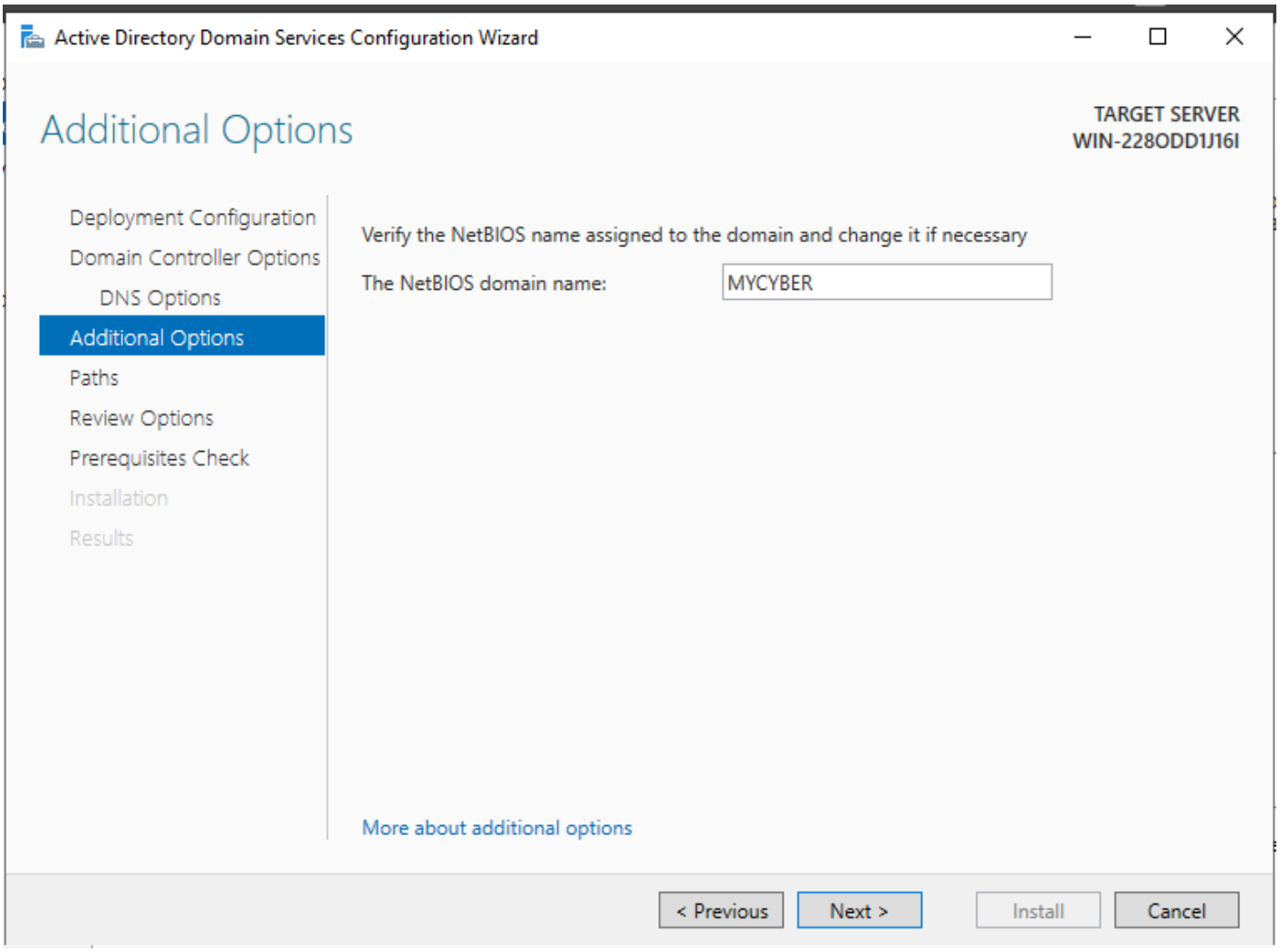


Figure 35 – MyCYBER

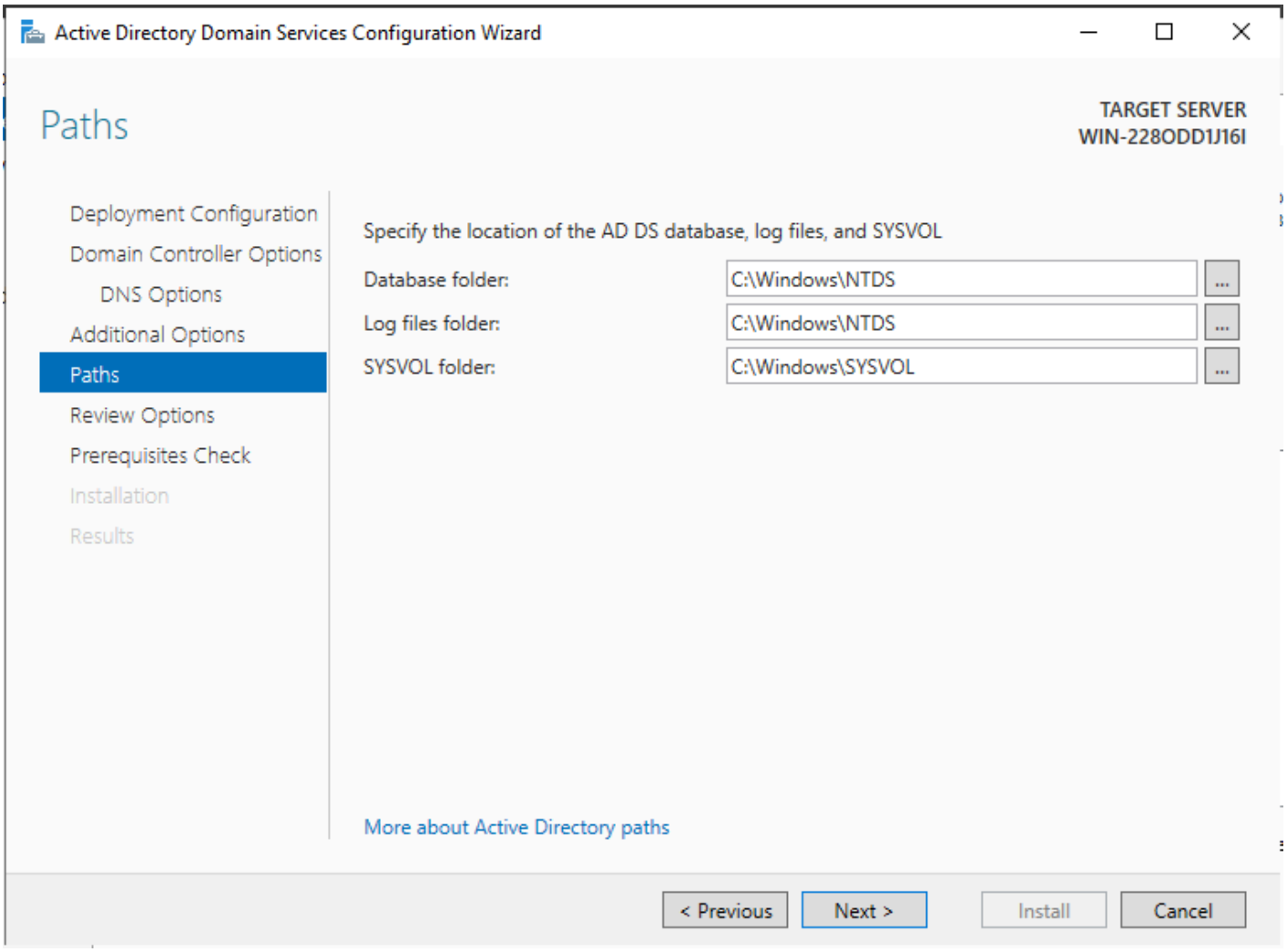


Figure 36 – Confirm paths

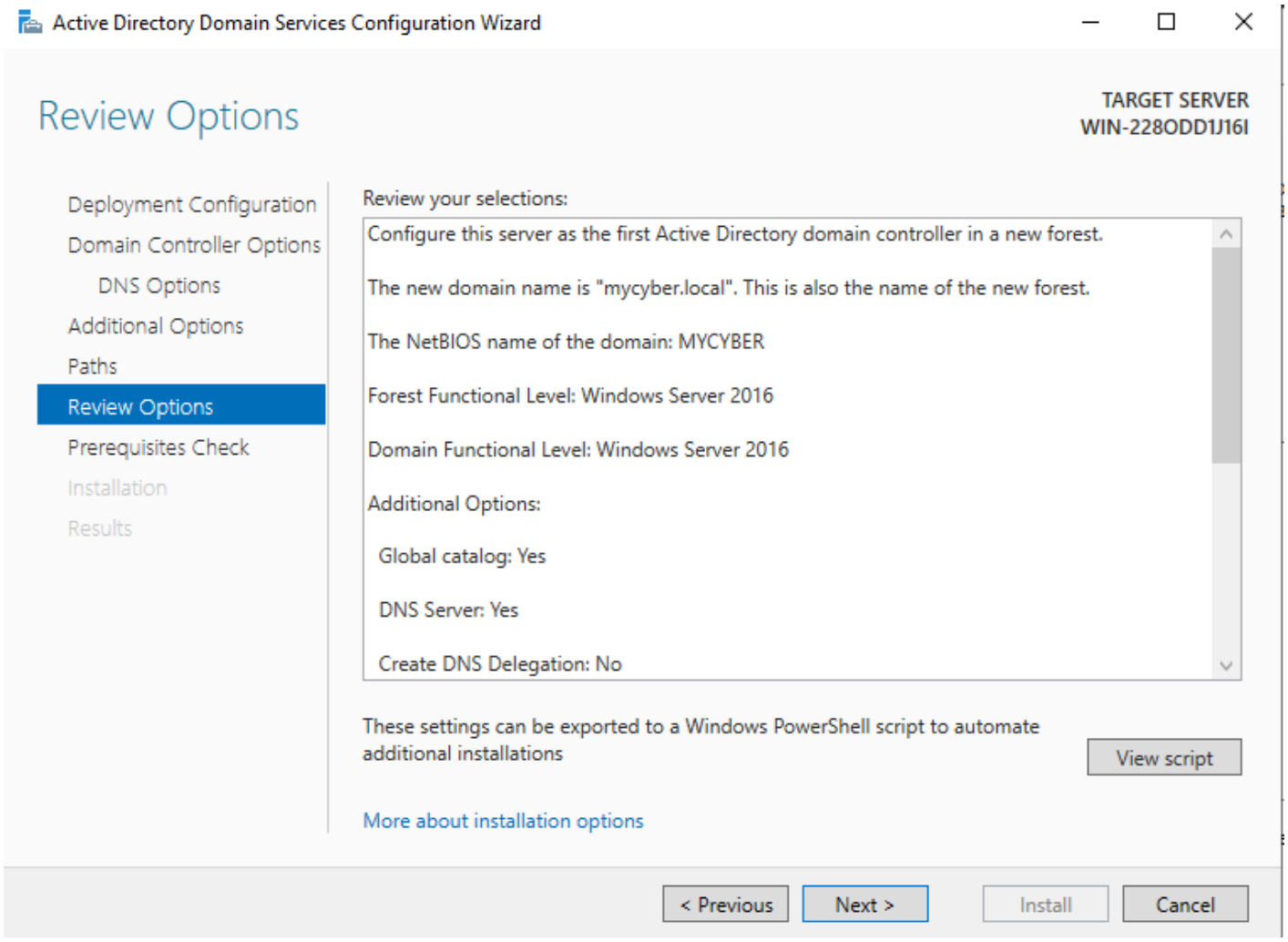


Figure 37 – Review and confirm

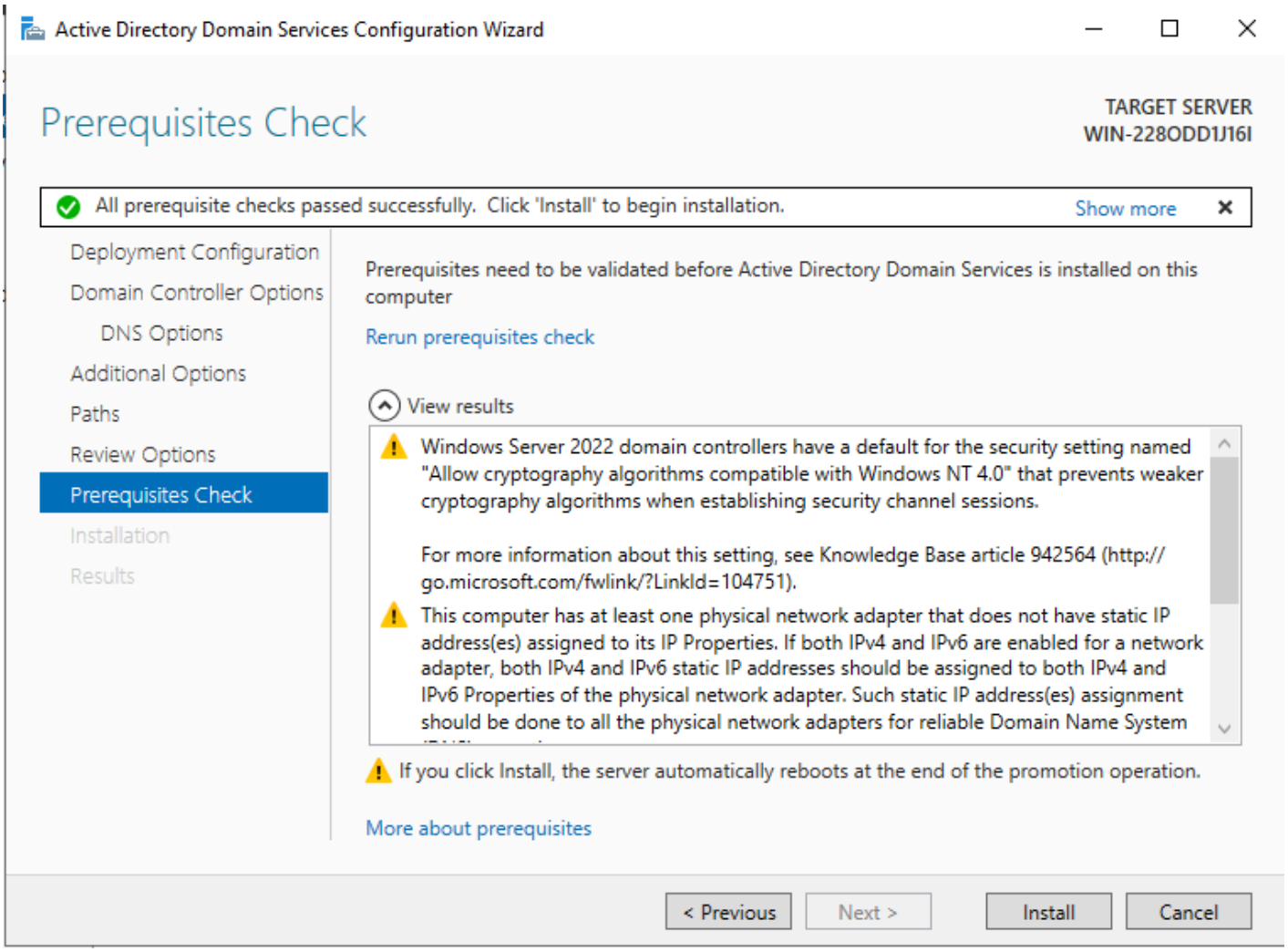


Figure 38 – Wait for green checkmark

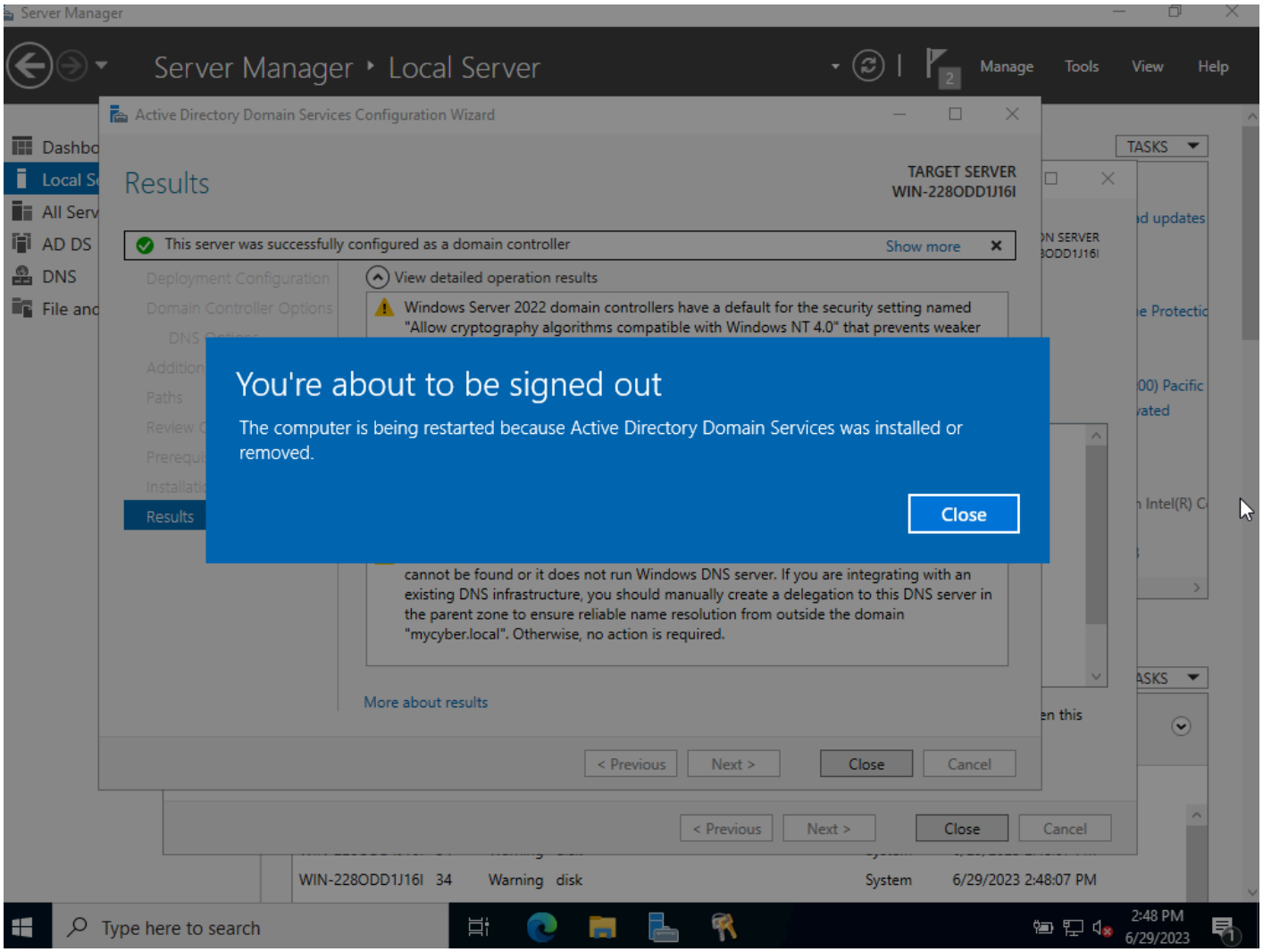


Figure 39 – It will restart automatically

CHAPTER 9

Build a Simple Local Area Network with DHCP

MATHEW J. HEATH VAN HORN, PHD

A Local Area Network (LAN) has many definitions depending on who you speak to. They can be defined by geography, function, or electrical connections. In this book, we typically use the term "LAN" to specify a few end devices connected to the same switch. This is a gross oversimplification of LANs, but simplification is helpful when exploring larger concepts. Consider how we use logs to represent exponential equations or ask veterans in the audience to stand for recognition. Both actions are simplifications of greater meaning.

In this lab, we show you how to make a fundamental LAN with DHCP that won't stress your host machine's resources.

LEARNING CONCEPTS

- Create a functional LAN with:
    - 1 switch
    - 2 PCs
    - 1 DHCP server

PREREQUISITES

- Chapter 2 – Setup a GNS3 environment
- Chapter 5 – Install Tiny Core Linux
- Chapter 6 – Adding a VM to GNS3

DELIVERABLES

- None – this is a preparatory lab for other labs

RESOURCES

- GNS3 Documentation – https://docs.gns3.com/

CONTRIBUTORS AND TESTERS

- Jacob M. Christensen, C.I.S. Student, ERAU-Prescott
- Julian Romano, C.I.S. Student, ERAU-Prescott
- Cody Shinkyu Park, Honeywell Software Engineer, ERAU-Prescott Alumni
- Evan Paddock, Cybersecurity Student, ERAU-Prescott
- Dante Rocca, Cybersecurity Student, ERAU-Prescott
- Sawyer Hansen, Cybersecurity Student, ERAU-Prescott

Phase I – Inital Setup

Initial setup involves creating a workspace, segmenting that workspace, and then labeling the components. By the end of the this chapter, your network should look like the following:

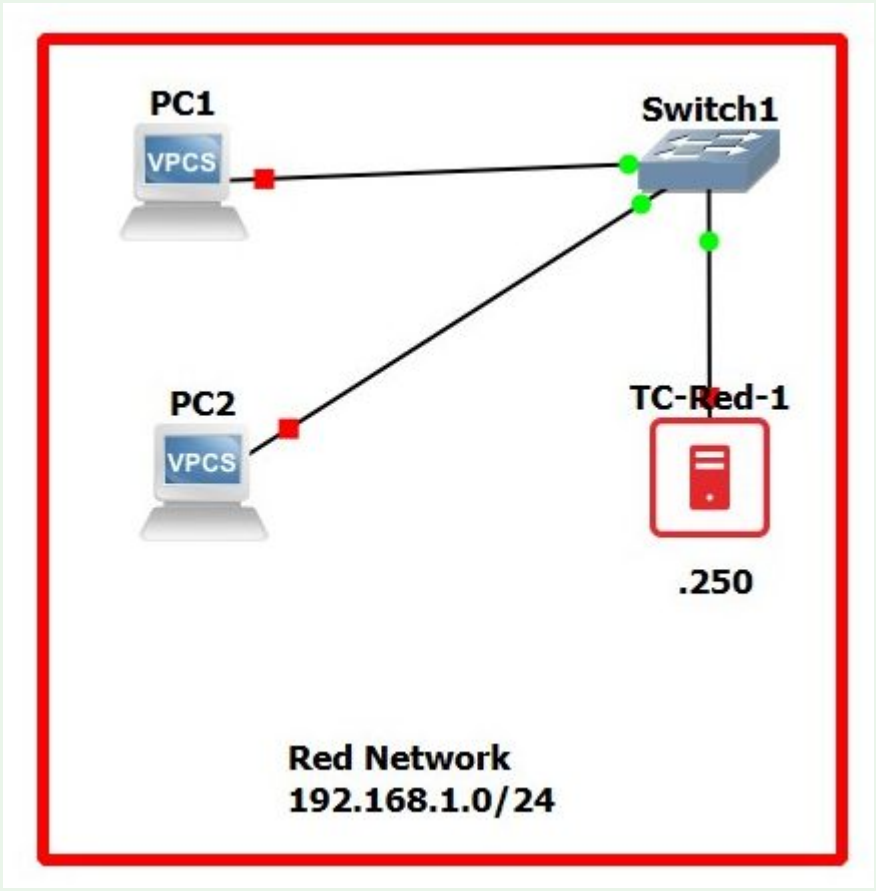


Figure 1 – Final GNS3 network

1. Ensure you have completed the prerequisites before starting the lab
2. Open Oracle VirtualBox Manager

3. Make a full clone of the TinyCoreLinux VM

    3.1. ***Right-click*** on the machine and select ***Clone*** (Figure 2)

    3.2. Rename it to "TC-red" and select the option to generate new MAC addresses (Figure 3), then click ***Next***

    3.3. Select Full Clone, then click ***Finish***

4. **Right-click** on the TC-red VM and click on ***settings*** (Figure 4)

5. Navigate to "Network" and change the ***network adapter 1 settings*** to ***Generic Driver*** and***UDPTunnel,*** then click ***OK*** (Figure 5)

6. Start GNS3 and start a new blank project. Name it anything you like, but for this example, we are calling it ***Simple LAN***

7. Add the TC-red VM to the GNS3 appliances – Change its symbol to a Red Server

8. In the GNS3 toolbar ribbon, click on the ***Draw a Rectangle*** tool and click the workspace to place a rectangle (Figure 6)

9. You can use the mouse to resize the rectangle at any time

10. Change the properties of the rectangle by ***right-clicking*** on the edge and selecting ***Style*** (Figure 7)

    10.1. Some people use a fill color and some don't (Figure 8)

    10.2. Change the border color to a primary color (we are using red)

    10.3. Change the Border width to***6 px***

    10.4. Click ***apply***, then click ***ok***

11. GNS3 uses layers for its graphics. Generally, the shapes are at a higher layer than the connectors. This means that anything you put into the box risks not being seen. So you can change the box's layer now or at any time by *right-clicking* on the shape and selecting ***Lower one layer*** (Figure 9)

12. Place the following inside the red rectangle

    12.1. Ethernet Switch

    12.2. Two (2) VPCS

    12.3. TC-red VM

13. Connect the devices to the switch
14. Use the ***note tool*** – next to the shape tool – to add a new note of "Red Network 192.168.1.0/24"
15. Use the ***note tool*** to add a new note of ".250" next to the TC-Red VM (Figure 10)
16. Start all devices

Phase II – Configure DHCP on TC-red VM

Tiny Core Linux comes with a DHCP service. However, we will have to type quite a bit to make it work. When you are finished with this lab, you may want to use these instructions to create a default TC-DHCP VM that you can clone whenever you need a lightweight DHCP server.

NOTE: Most errors encountered by testers were due to typos. Be careful and everything should work fine.

1. Navigate to the TC-Red VM and open a terminal (Figure 11)
2. Configure the ethernet interface with a static IP address

2.1. Open a new configuration file by typing

```
> sudo vi /opt/eth0.sh
```

2.2. You will see a lot of tildes (~) which means a blank document

2.3. Press*i* to activate insert, and type the following in the file (Figure 12)

```
  # fast storage device may need a delay on boot for the settings to take
# adjust the following sleep statement if needed
sleep .2
  #kill the dhcp client for eth0
sleep 1
if [ -f /var/run/udhcpc.eth0.pid ]; then rm /var/run/udhcpc.eth0.pid;
sleep 0.1
fi
  #configure the interface eth0
ifconfig eth0 192.168.1.250 netmask 255.255.255.0 broadcast 192.168.1.255
up
  #start the DHCP server process once the interface is ready with the IP
add
```

```
sleep .1
sudo udhcpd /etc/udhcpd.conf &
```

2.4. Press ***esc*** to exit the edit mode

2.5. Press the full colon ***:*** followed by ***wq*** (this means write out – old school save file – and quit)

```
  :wq
```

2.6. Now type in the command line

```
  > sudo chmod 777 /opt/eth0.sh
```

2.7. Followed by

```
  > sudo /opt/eth0.sh
```

2.8. You can check if interface eth0 is configured (Figure 13) by typing

```
  > ifconfig
```

3. Create a DHCP configuration file

3.1. Type

```
  > sudo vi /etc/udhcpd.conf
```

3.2. In this new file, press ***i*** to insert and type the following

```
  start 192.168.1.100
end 192.168.1.200
interface eth0
option subnet 255.255.255.0
option router 192.168.1.250
option lease 43200
```

```
option dns 192.168.1.250
option domain local
```

NOTE: These settings mean the following

Statement	Setting	Meaning
Start	192.168.1.100	This is the first possible IP address that can be given out to end devices asking for an IP address
Stop	192.168.1.200	This is the last possible IP address that can be given out to end devices asking for an IP address
interface	eth0	This is the network interface that will be looking for DHCP requests
option subnet	255.255.255.0	The IPv4 subnet mask used for this network (192.168.1.0)
option router	192.168.1.250	This is the IP address of the gateway router to leave the local LAN
option lease	43200	The amount of seconds between lease refresh – this is 12 hours
option dns	192.168.1.250	DNS should use this gateway router
option domain	local	DNS requests will resolve locally first before using the gateway

3.3. When finished typing, (Figure 14) press escape followed by

```
:wq
```

3.4. Then start the DHCP Daemon by typing

```
sudo udhcpd /etc/udhcpd.conf
```

3.5. Verify if the DHCP process is running by typing the following

```
sudo netstat -anp
```

3.6. You should see a listening line like this: udp 0 0 0.0.0.0:67 0.0.0.0:* 1413/udhcpd (Figure 15)

4. Remember, Tiny Core Linux has limited persistence, so we have to add our DHCP configuration file to the list

4.1. Gain change permissions to the bootlocal file by typing

```
  sudo chown root:staff /opt/bootlocal.sh
sudo chmod 775 /opt/bootlocal.sh
```

4.2. Now add the persistence by typing the following

```
  sudo echo 'etc/udhcpd.conf' >> /opt/.filetool.lst
sudo echo 'opt/eth0.sh' >> /opt/.filetool.lst
sudo echo 'opt/eth0.sh &' >> /opt/bootlocal.sh
filetool.sh -b
```

4.3. You should get a confirmation like in (Figure 16)

4.4. Now reboot TC-red to verify the settings were retained by typing the following at the command line

4.4.1. Static IP is configured (Figure 13)

```
  ifconfig
```

4.4.2. DHCP server is running (Figure 15)

```
  sudo netstat -anp
```

Phase III – Verify hosts are getting IP addresses

We can never be certain that our VPCS are getting IP addresses until we try it.

1. Navigate to the GNS3 workspace
2. Right-click on a ***VPCS console*** and type

```
  ip dhcp
```

3. You should get a response of an IP address between 192.168.1.100 – 192.168.1.200 (Figure 17)
4. Note the IP address and use the GNS3 note tool to add the IP address to the Workspace (Figure 18)

NOTE: Most errors encountered by testers were due to typos. Be careful and everything should work fine.

Final Note – you can change the DHCP configuration any time by modifying IP addresses. For instance if our network was 20.20.0.0/16 and we knew our gateway router was 20.20.20.254, we would change are settings to the following:

Purpose	Lab IP Address	Possible Modification
Network ID	192.168.1.0	20.20.0.0
subnet mask	255.255.255.0	255.255.0.0
Static IP (this DHCP Server)	192.168.1.250	20.20.20.1
Option Router (gateway or next-hop)	192.168.1.250	20.20.20.254
start – the first available IP address for DHCP	192.168.1.100	20.20.20.50
stop – the last available IP address for DHCP	192.168.1.200	20.20.20.99
Option DNS (the gateway if DNS cannot be resolved locally)	192.168.1.250	20.20.20.254
lease time (in seconds)	43200 (=12 hours)	21600 (= 6 hours)

End of Lab

List of Figures for Print Copy

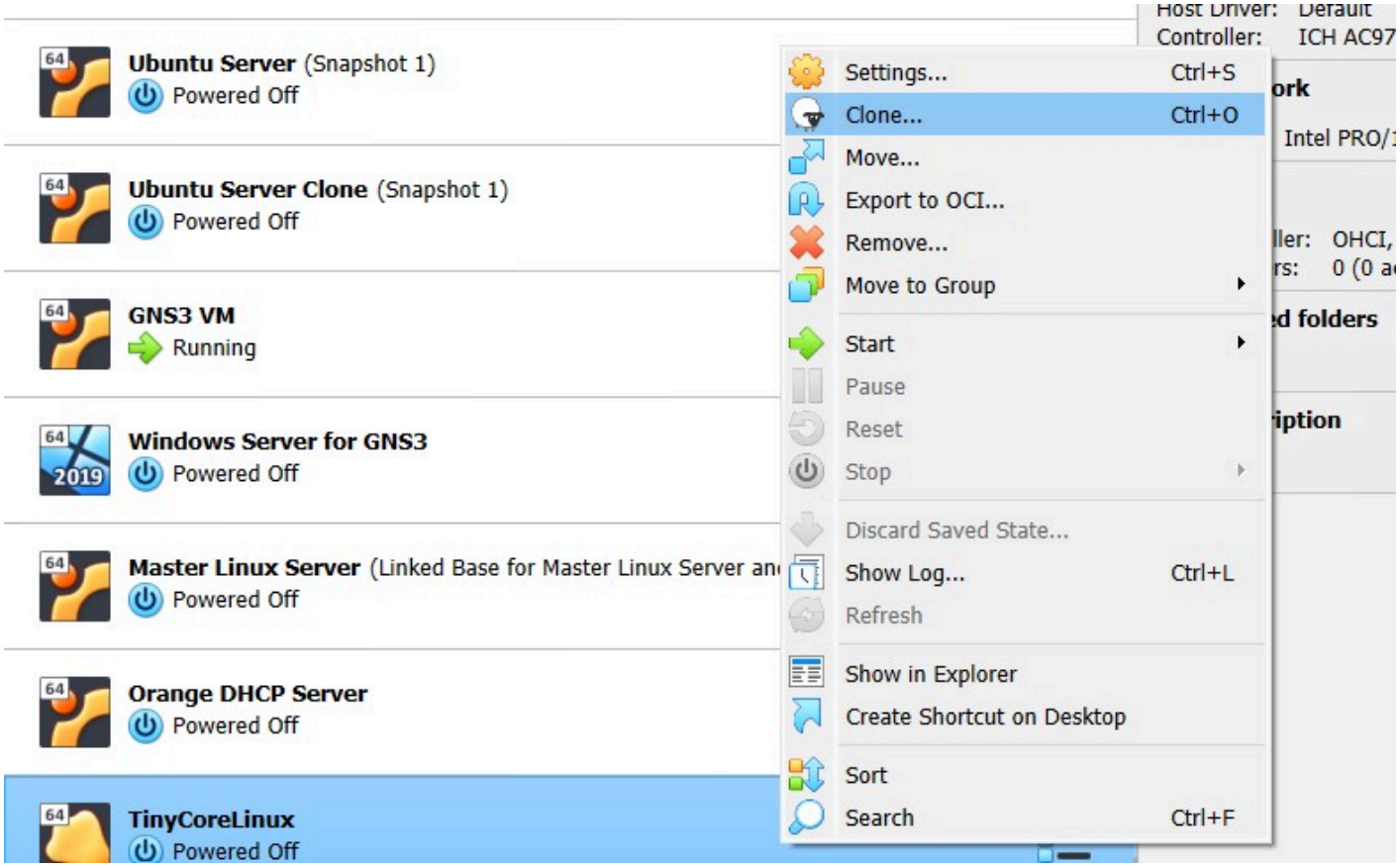


Figure 2 – Cloning a VM

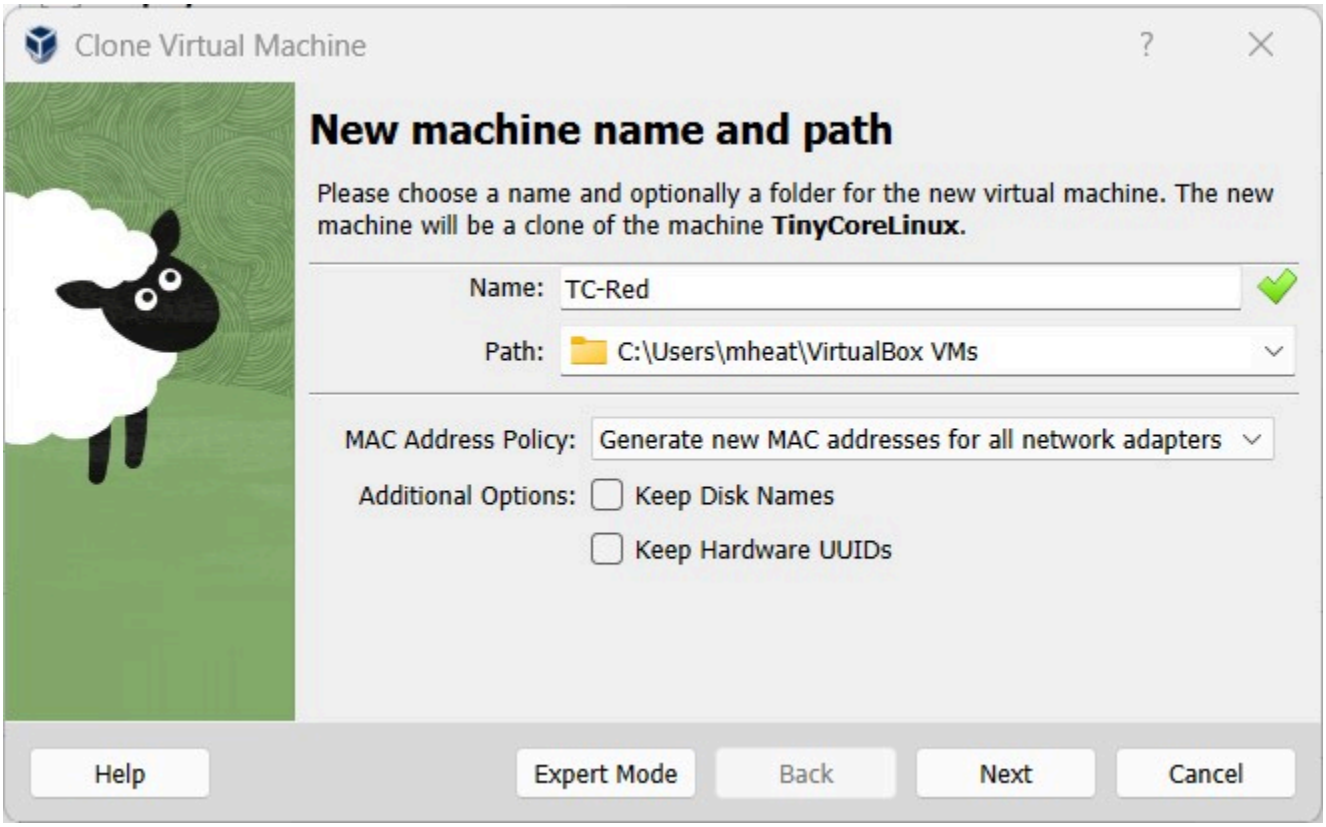


Figure 3 – Renaming and resetting MACs

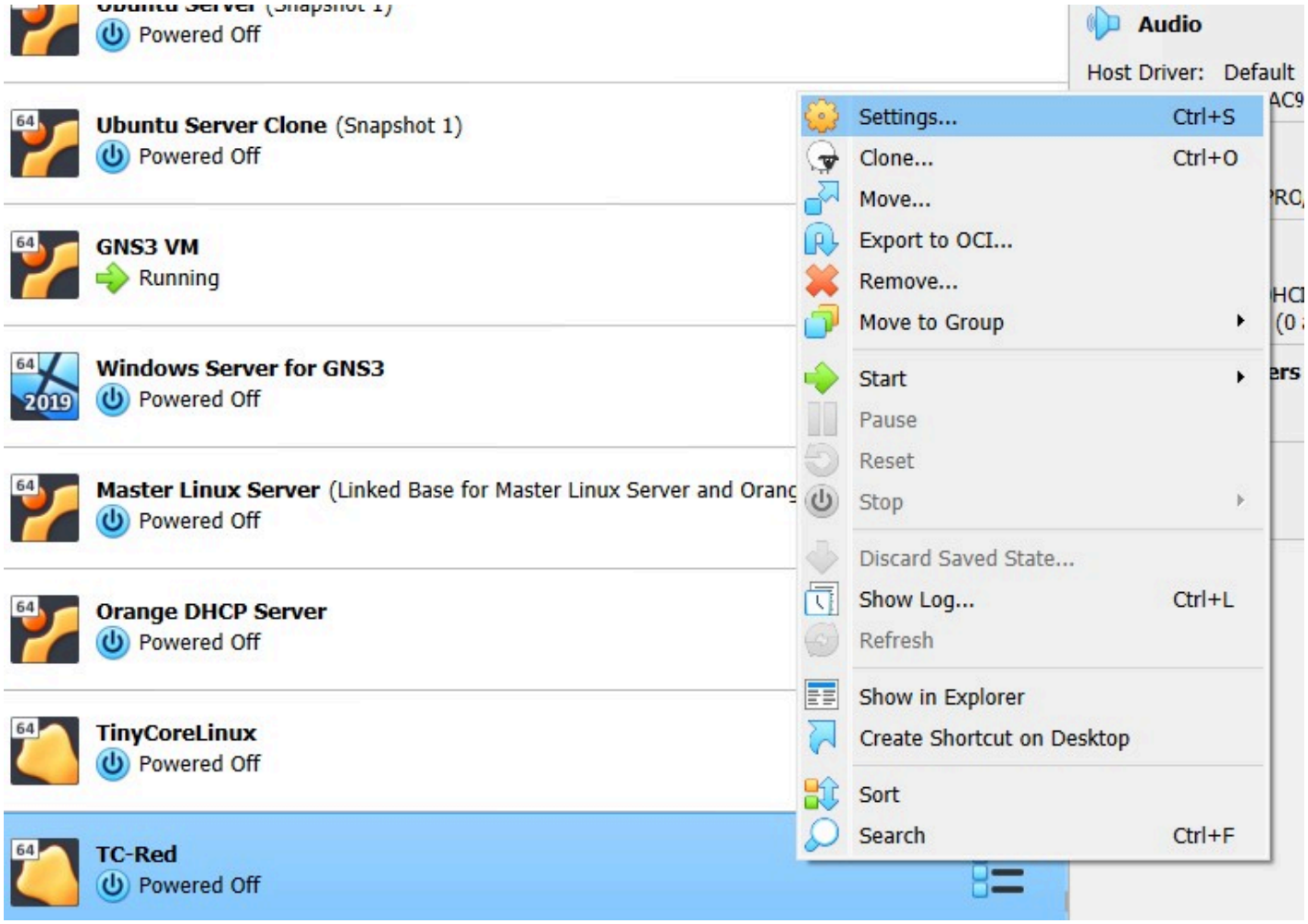


Figure 4 – Adjust settings for TC-Red

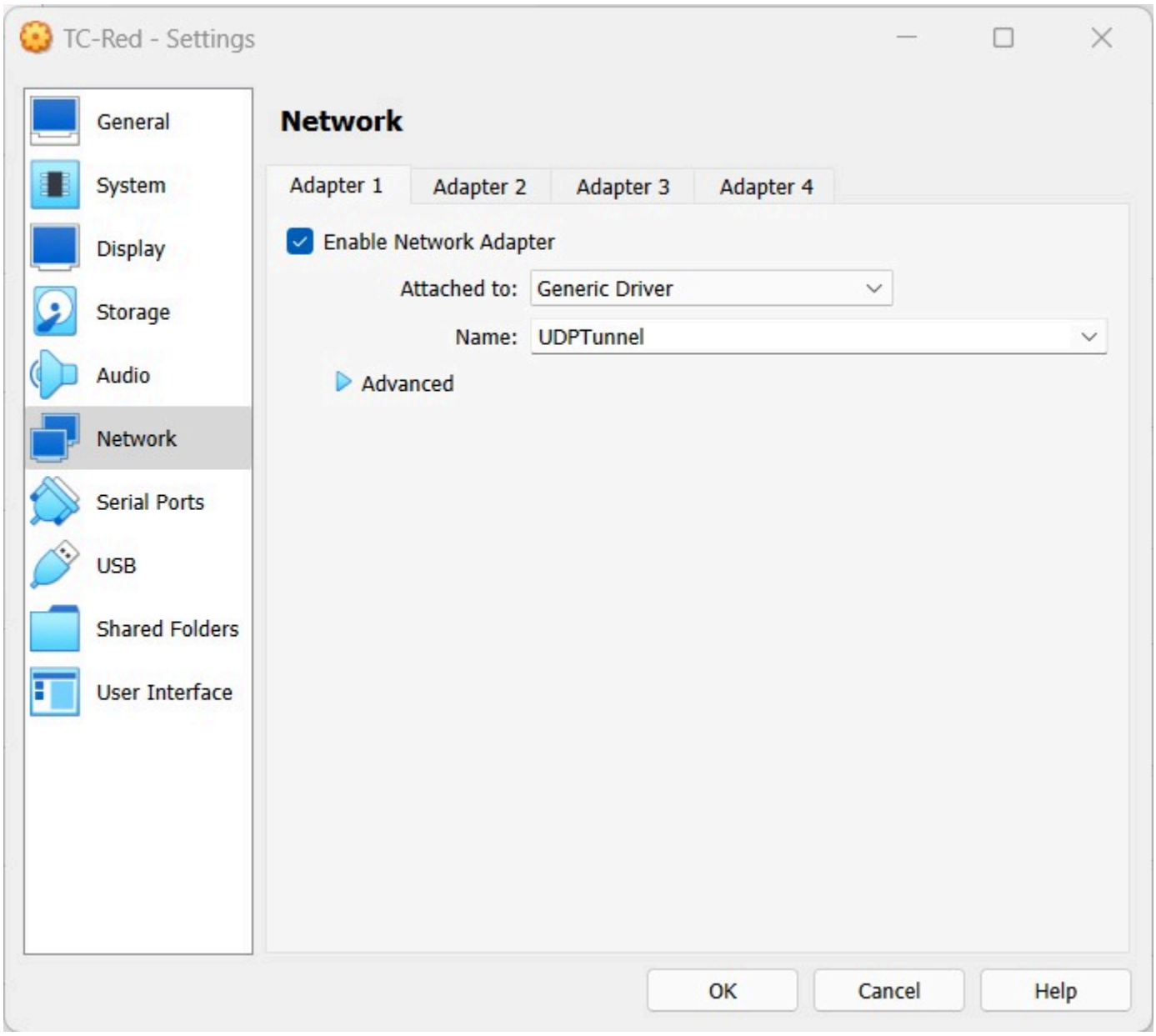


Figure 5 – Adjust NIC to generic

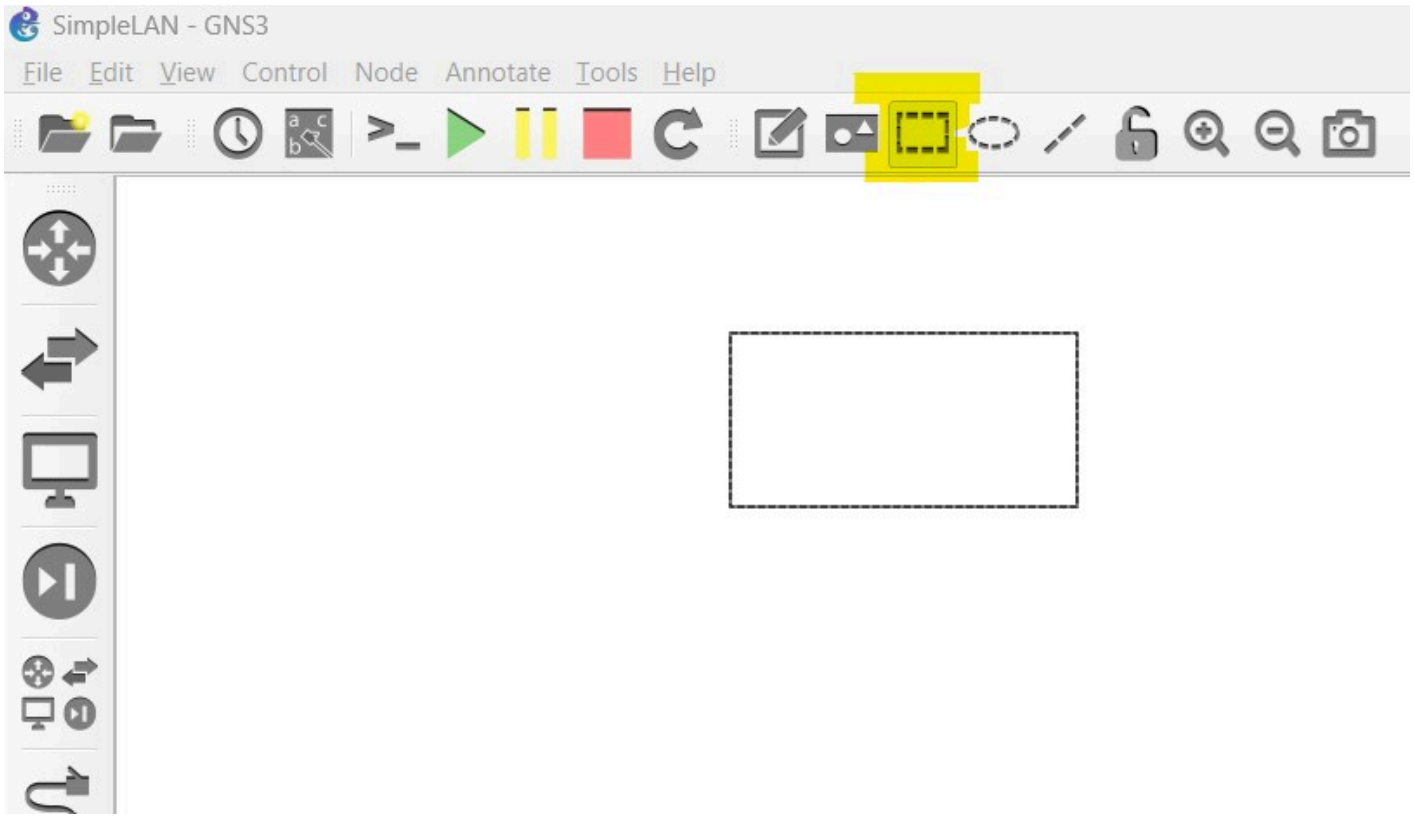


Figure 6 – Drawing a rectangle

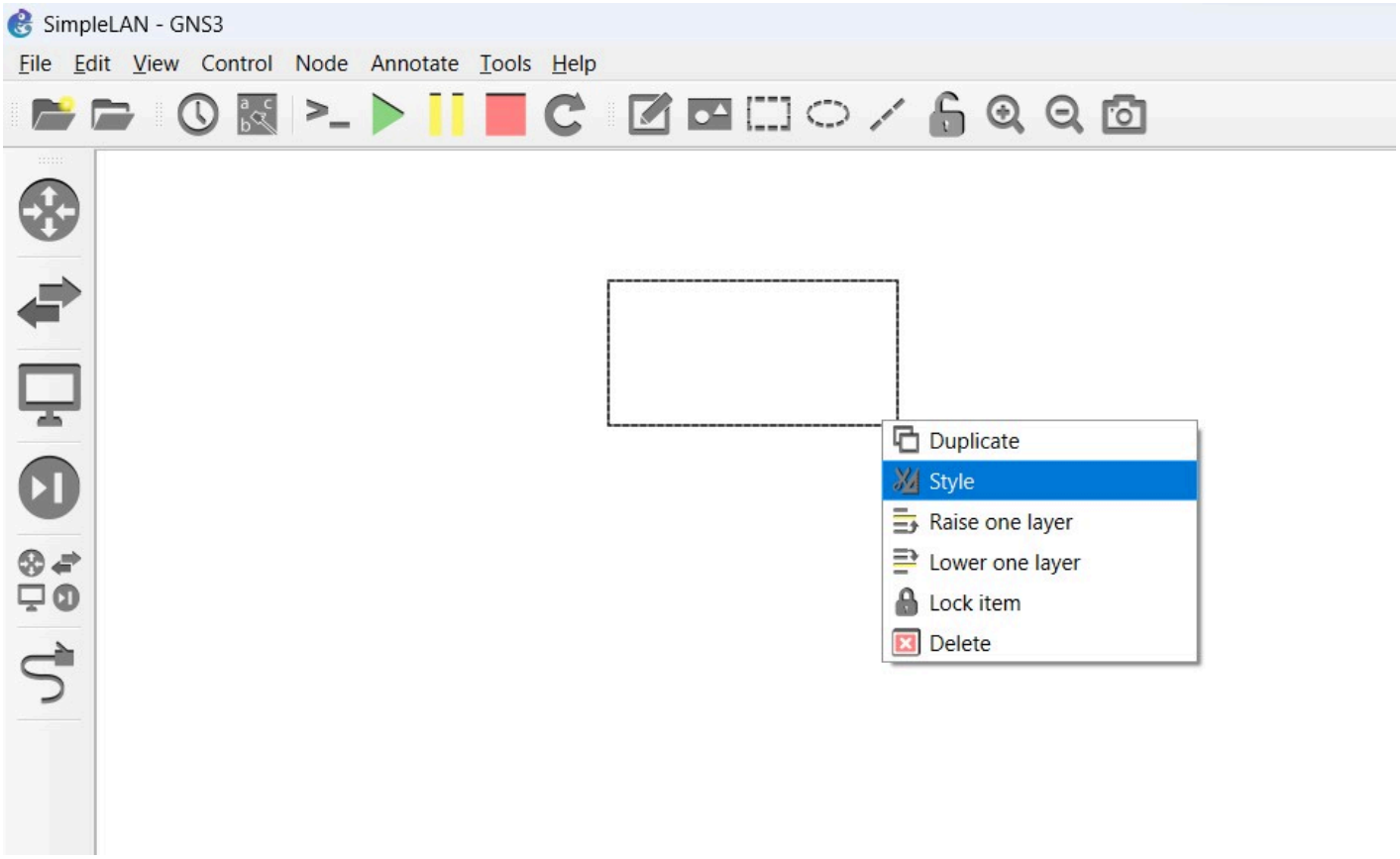


Figure 7 – Changing rectangle style

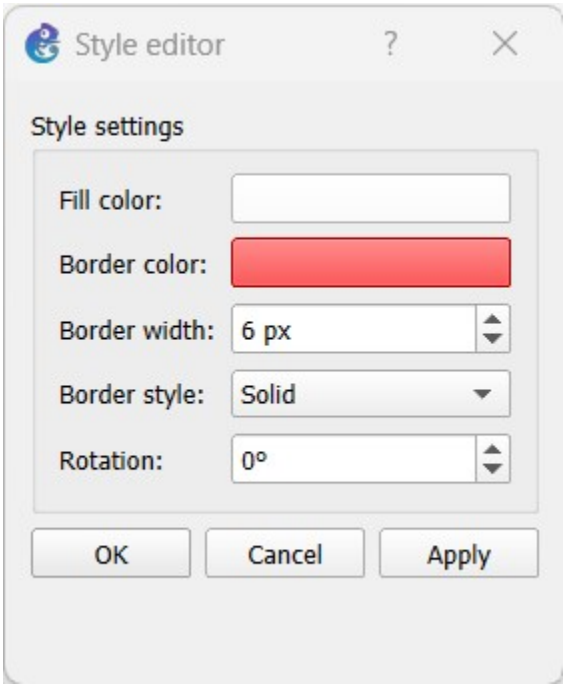


Figure 8 – Changing rectangle color

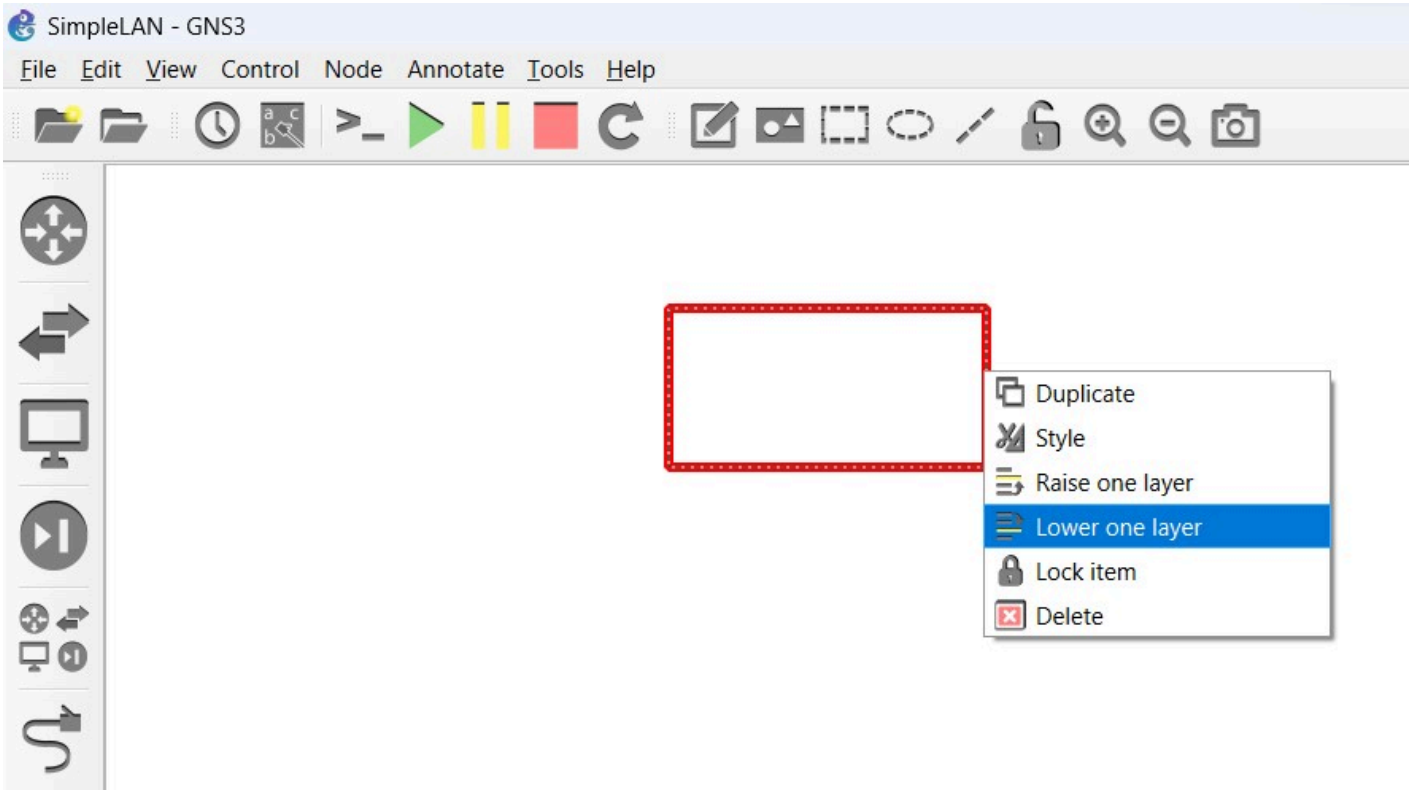


Figure 9 – Send rectangle back a layer

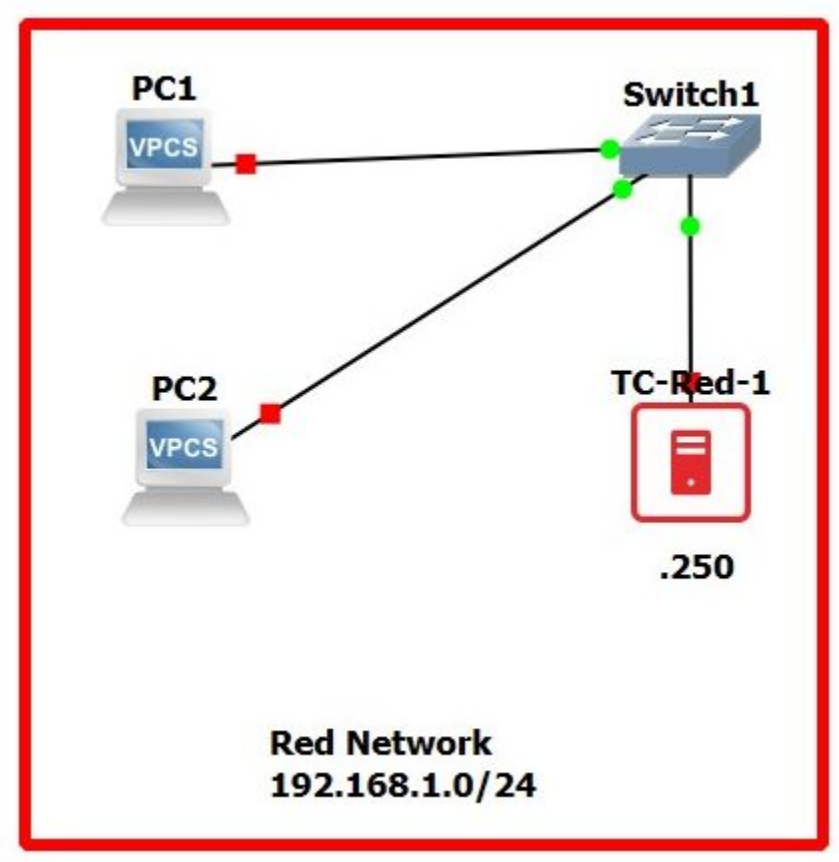


Figure 10 – Add a note

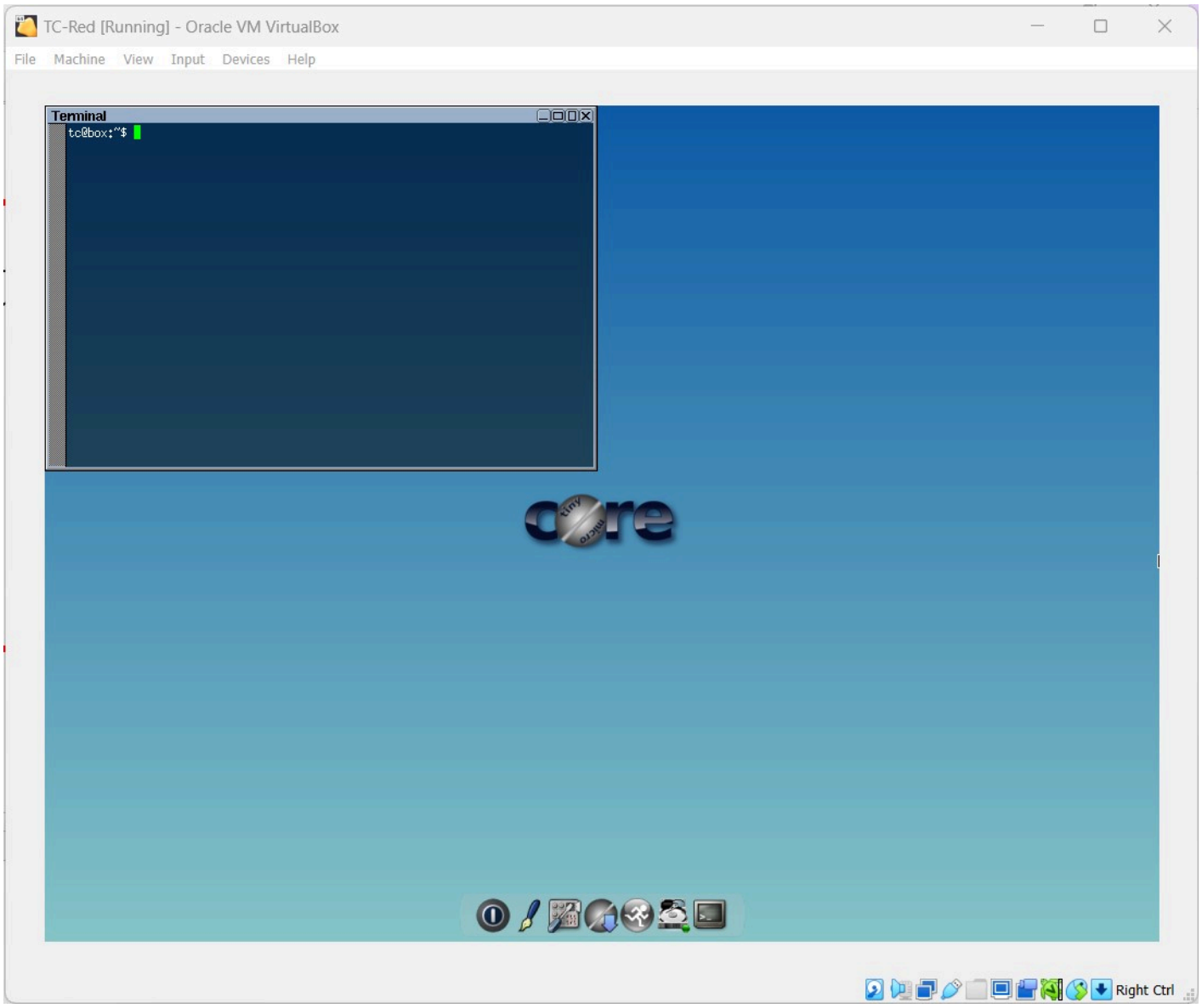


Figure 11 – Open a terminal

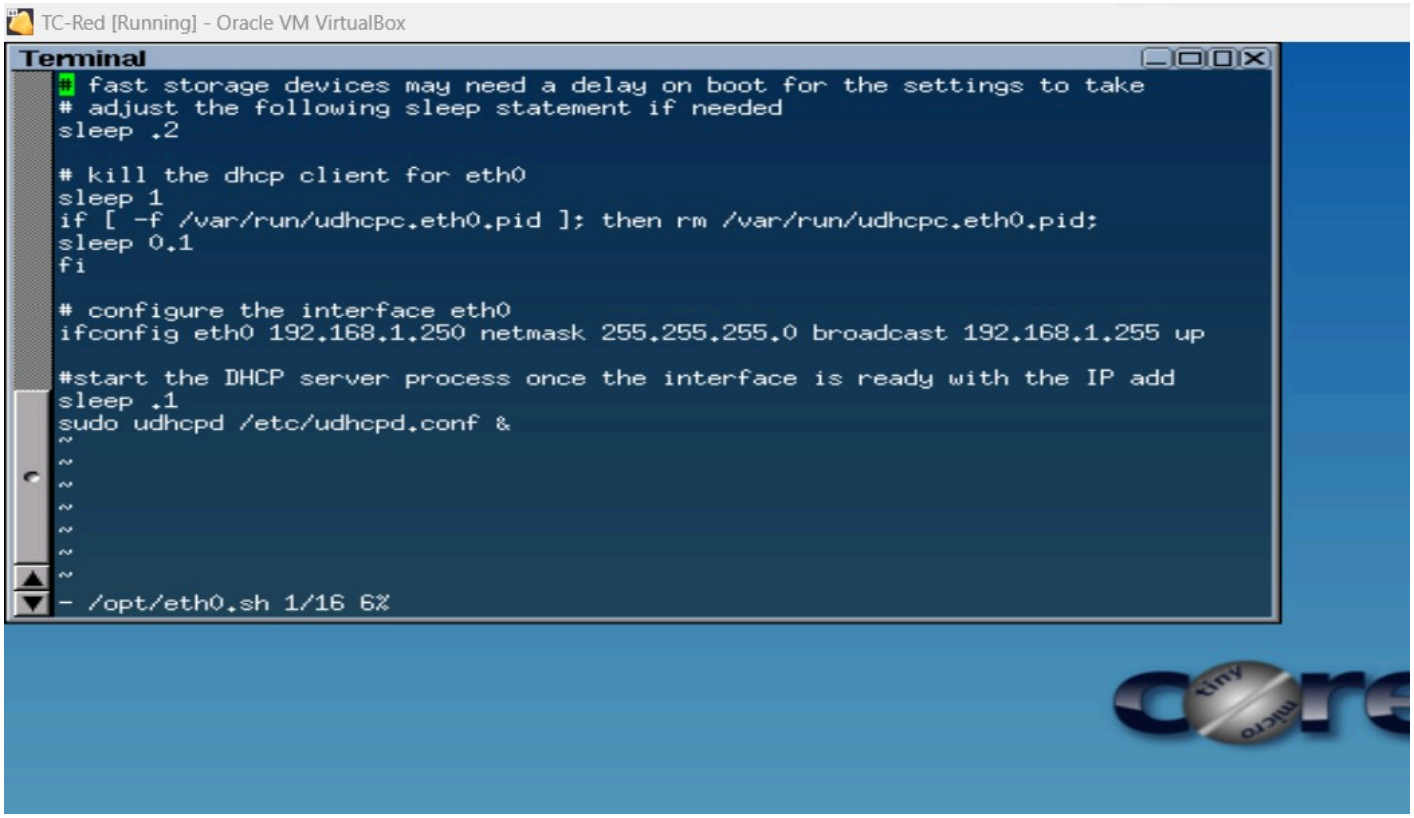


Figure 12 – Create a settings file for the NIC

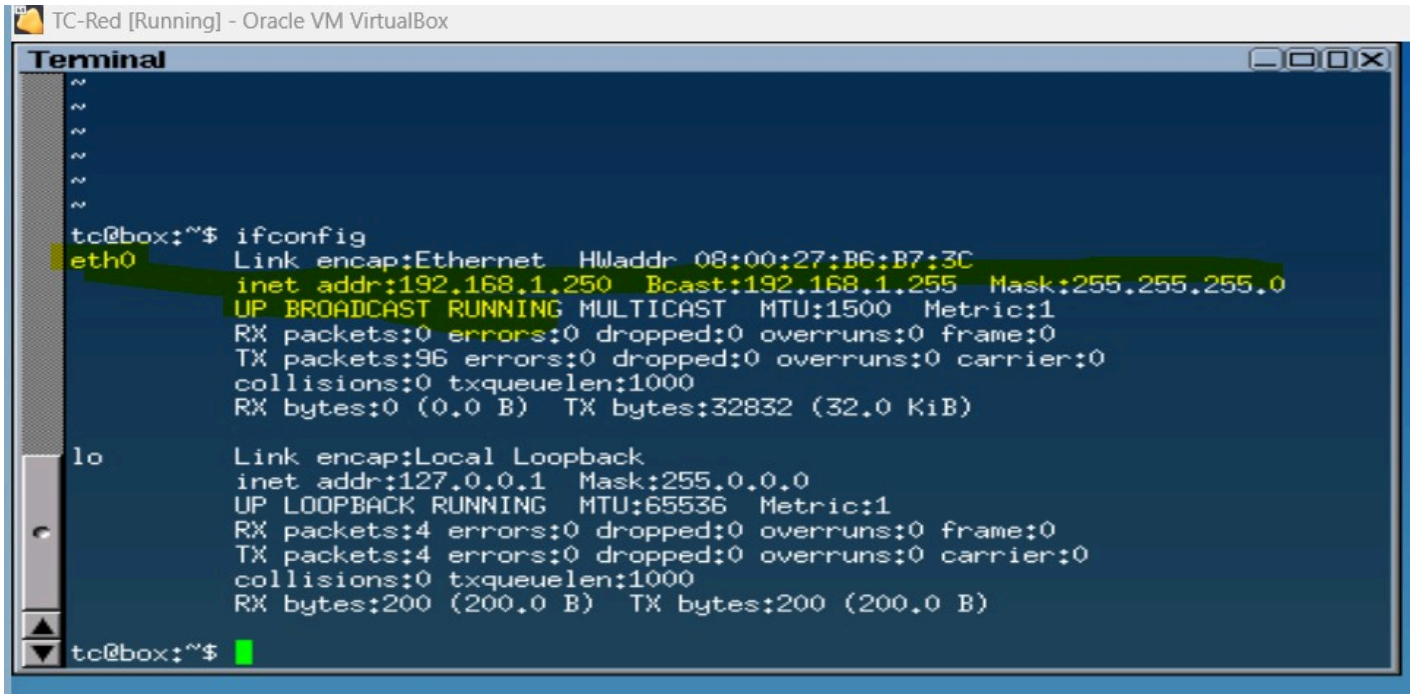


Figure 13 – Verify the NIC configurations are correct

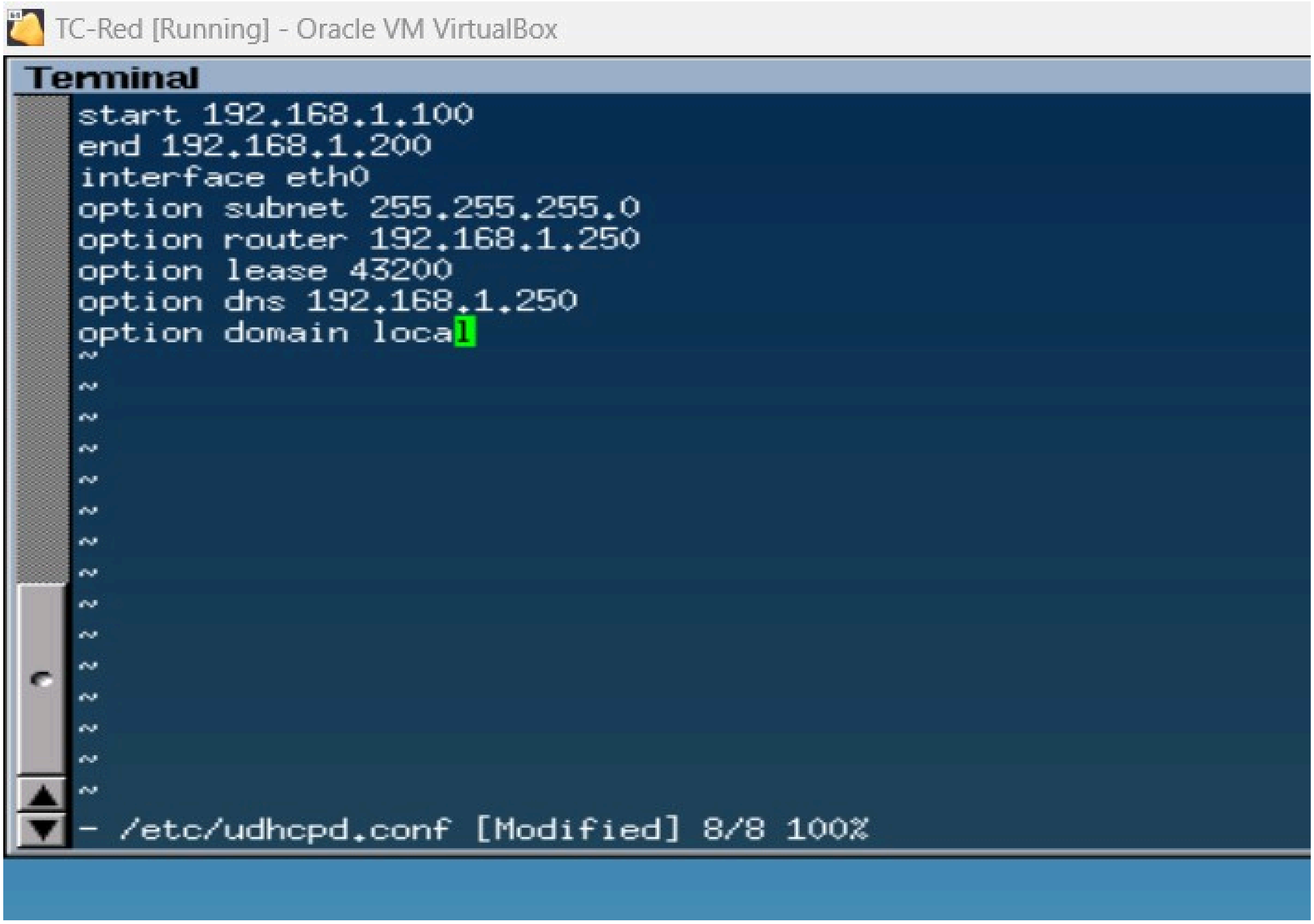


Figure 14 – Configure DHCP

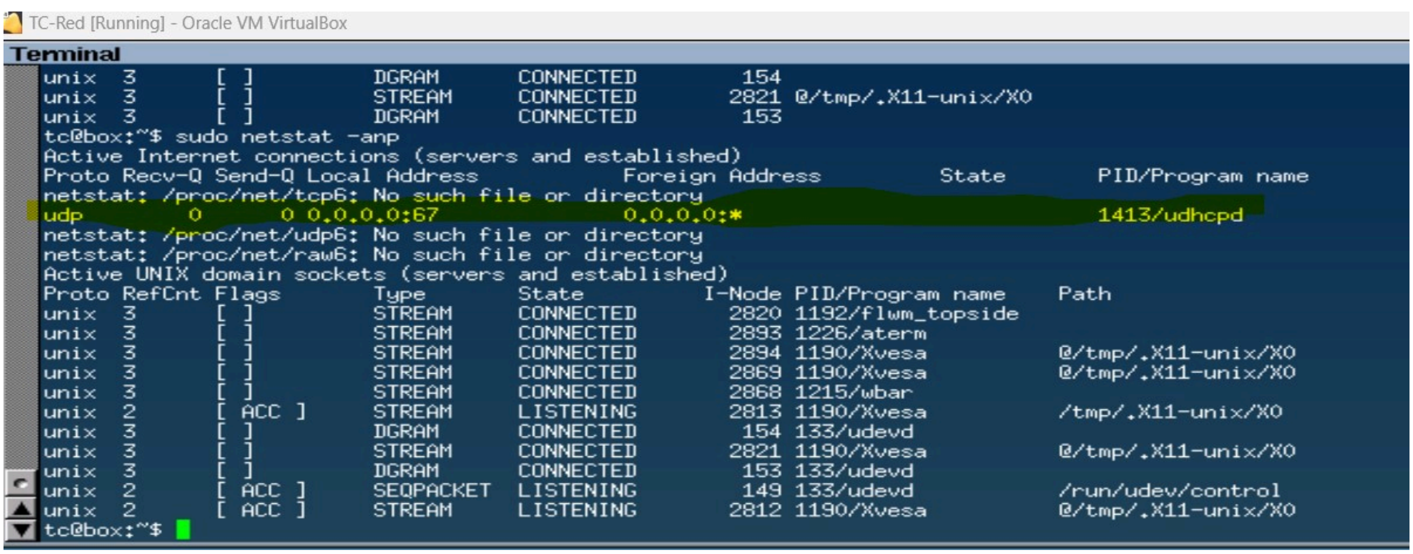


Figure 15 – Perform a netstat check

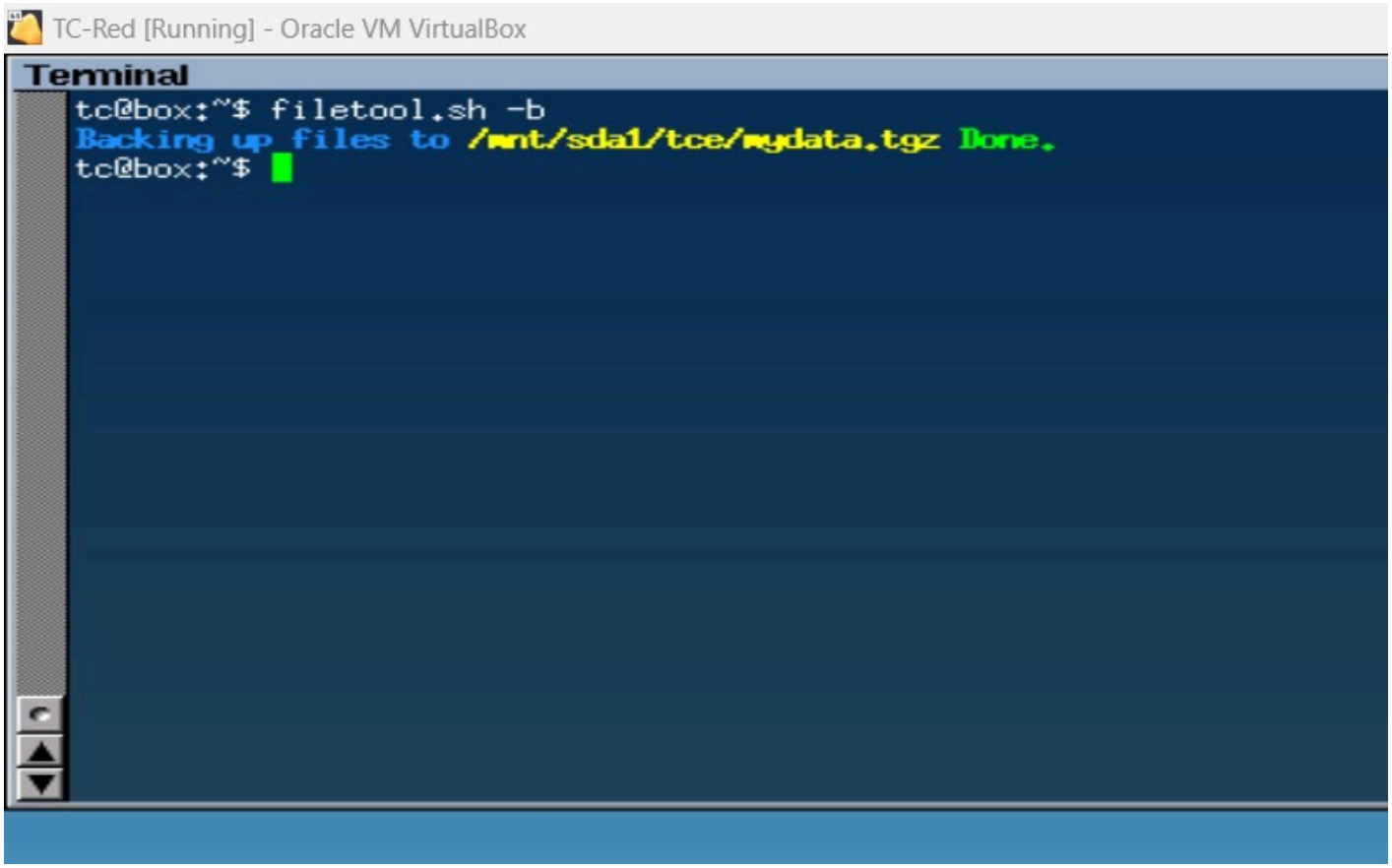


Figure 16 – Add persistance

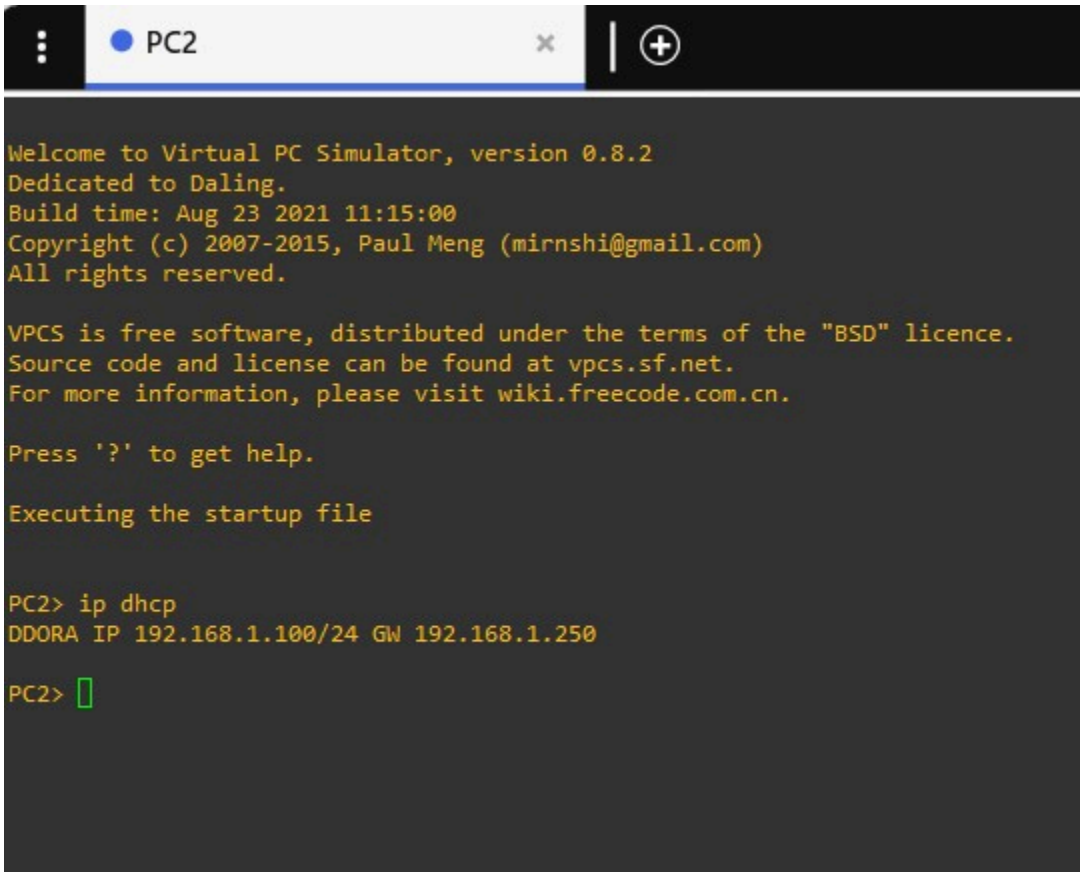


Figure 17 – Ensure devices are getting DHCP

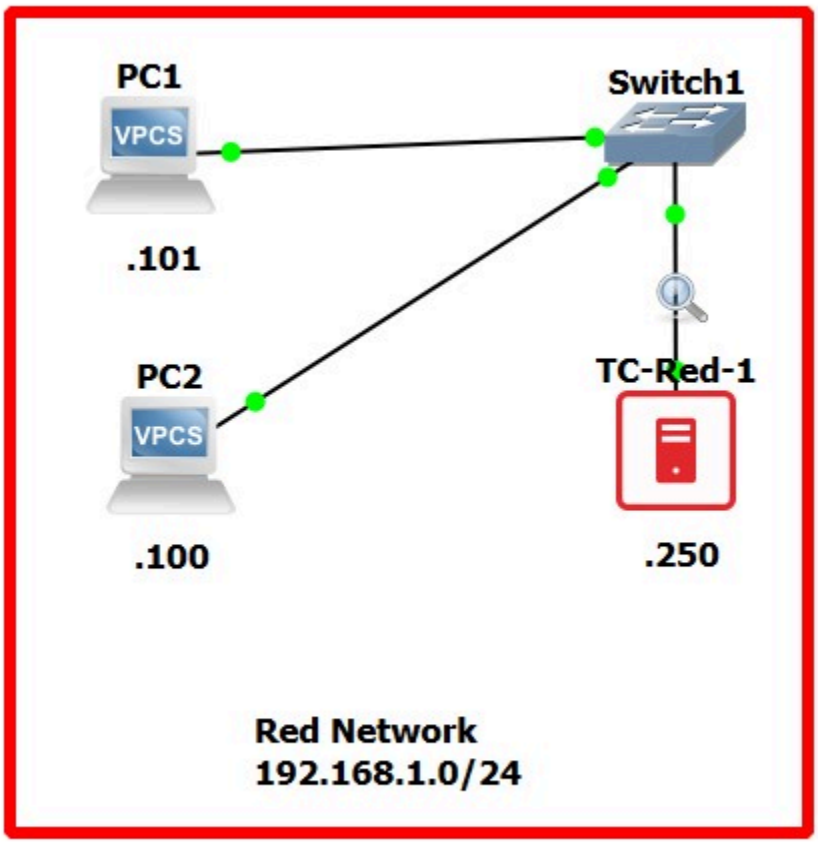


Figure 18 – Add a note to the workspace

CHAPTER 10

Create a pfSense Firewall VM

MATHEW J. HEATH VAN HORN, PHD

The software product pfSense is a popular open-source firewall used by small and mid-sized companies. The software can run on hardware or a virtual machine. It is based on Unix FreeBSD which differs from Linux. This lab leads the learner to create a pfSense VM in VirtualBox.

LEARNING OBJECTIVES

- Successfully download, install, and run pfSense in VirtualBox

PREREQUISITES

- Virtualbox Installed

DELIVERABLES

- None – this is a preparatory lab that supports other labs in this book

RESOURCES

- Download pfSense
- Kingatua, Amos, "How to install pfSense Firewall on Ubuntu and CentOS?", https://geekflare.com/pfsense-installation-guide/

CONTRIBUTORS AND TESTERS

- Jacob M. Christensen, Cybersecurity Student, ERAU-Prescott
- Julian H. Romano, Cybersecurity Student, ERAU-Prescott
- Evan Paddock, Cybersecurity Student, ERAU-Prescott
- Dante Rocca, Cybersecurity Student, ERAU-Prescott

Phase I – Download pfSense

pfSense is an operating system (OS), like Windows, Linux, or MacOS.

1. Download the installer for pfSense Community Edition

> **NOTE:** At the time this was written, Netgate made a surprising update that requires users to register for a new account and give up personal information just to download the Community Edition image of pfSense. For many, this compromise of privacy for the sake of corporate data harvesting is not worth this extra road block for learning. Therefore, we will provide two different methods for downloading pfSense.

1.1. **The "Official" Method:** https://www.pfsense.org/download/

> **NOTE:** It is strongly advised to avoid using to real personally identifiable information (PII) for online accounts you'll only use once. Companies get hacked all the time; the last thing you want is your name, physical address, and phone number leaked just because you wanted to mess around with firewalls! However, you are not restricted from using temporary emails, temporary phone numbers or false addresses when needed.

1.2. **The "Unofficial" Method (Recommended):** https://www.pfsense.app/download/

1.2.1. Select the following options from the associated drop-down menus (Figure 1)

> **NOTE:** This example uses CE version **2.7.2**.

1.2.1.1. Architecture: **AMD64 (64-bit)**

1.2.1.2. Installer: **DVD Image (ISO) Installer**

1.2.2. Click ***Download***

> **NOTE:** At this point, a file named **pfSense-CE-x.x.x-RELEASE-amd64.iso.gz** should be downloaded by your browser. The .gz file extension stands for GNU Zip, which is an application commonly used for file compression.

2. Navigate to the folder where you downloaded the ISO and decompress (unzip) it

2.1. If you're on Windows, use 7zip

2.2. If you're on Linux, use GNU unzip

```
$ gunzip ~/Downloads/file-name.gz
```

3. You should now see a file name **pfSense-CE-x.x.x-RELEASE-amd64.iso** in your Downloads directory

Phase II – Create a pfSense VM

Creating a pfSense VM is a pretty standard exercise.

1. Start the **Oracle VM VirtualBox Manager** application

> **NOTE:** This example uses **VirtualBox GUI Version 6.1.X** in the following steps. While your version may vary in organization and layout, the fundamental process should remain the same.

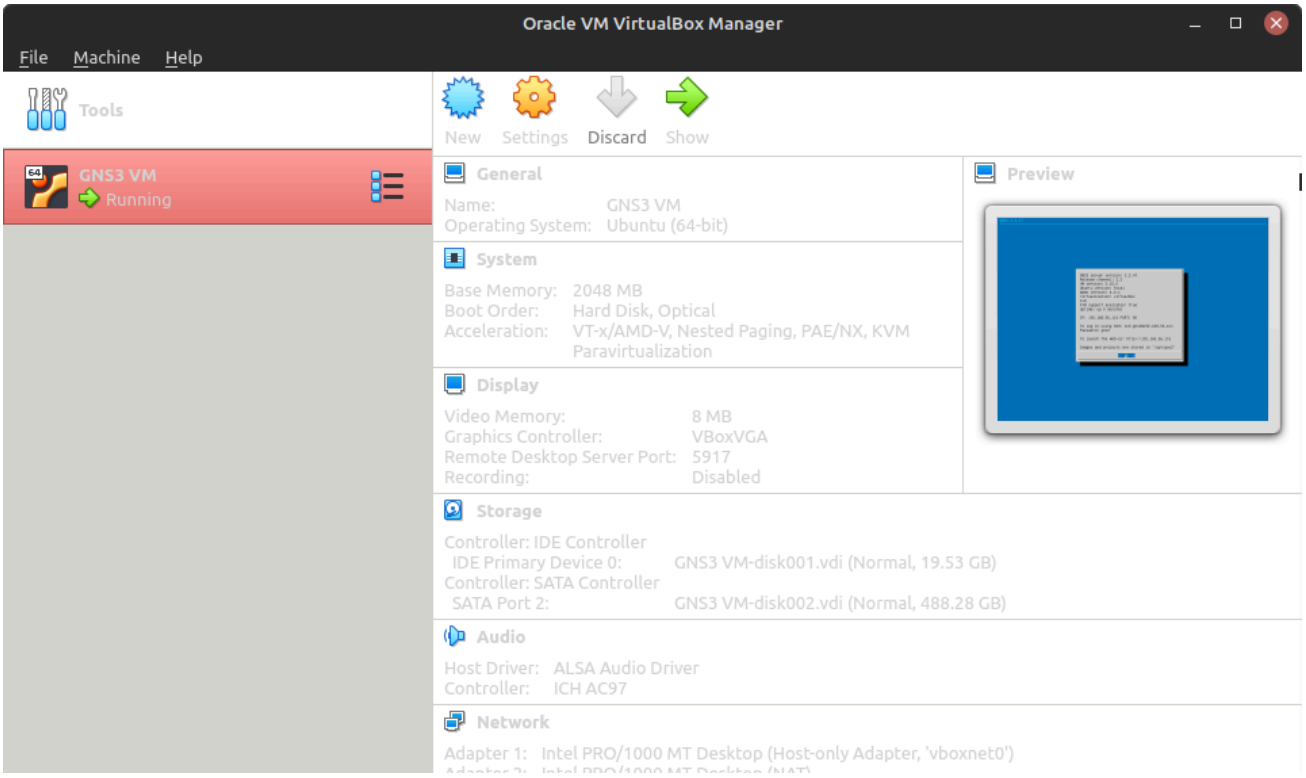


Figure 2 – VirtualBox Manager

2. At the top of the dashboard, select ***New***

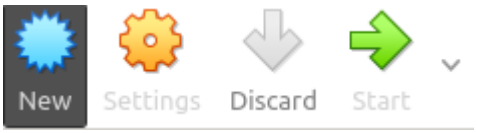


Figure 3 – Create a new VM

3. A new sub-menu called **Create Virtual Machine** should appear (Figure 4)

    3.1. Fill in the following information:

Option	Recommended Value	Description
Name	**pfSense-Firewall**	Custom name of the Virtual Machine. Can be anything, but should probably be somewhat descriptive to differentiate from other VMs.
Machine Folder	**<Leave as default path>**	The directory in which to store all files related to VM creation.
Type	**BSD**	Selects the generic operating system of the VM such as Windows, Linux, or Mac OS.
Version	**FreeBSD (64-bit)**	Specifies the specific sub-category of the selected OS and whether it will use a 32bit or 64bit processor.
Memory size	**1024 MB (1 GB)**	Determines how much RAM to allocate to the VM.
Hard disk	**Create a virtual hard disk now**	Determines whether or not to allocate physical storage to act as a hard disk or to use an existing virtual hard disk file.

    3.2. Select ***Create***

4. A new sub-menu called Create Virtual Hard Disk should appear (Figure 5)

    4.1. Fill in the following information:

Option	Recommended Value	Description
File location	**<Leave as default path>**	The directory in which to save the virtual hard disk. This will often be the same directory as the Machine Folder path.
File size	**8 GB**	Determines the size of the virtual hard disk. The minimum requirements for pfSense is 8 GB.
Hard disk file type	**VDI (VirtualBox Disk Image)**	Selects the type of virtual hard disk to create.
Storage on physical hard disk	**Dynamically allocated**	Selects whether to allocate physical hard disk space as needed (dynamically), or all at once (fixed). Choosing fixed will may result in slightly better performance at the cost of a higher storage footprint that will potentially go unused.

    4.2. Select ***Create***

5. This will create a new virtual machine in your VM list

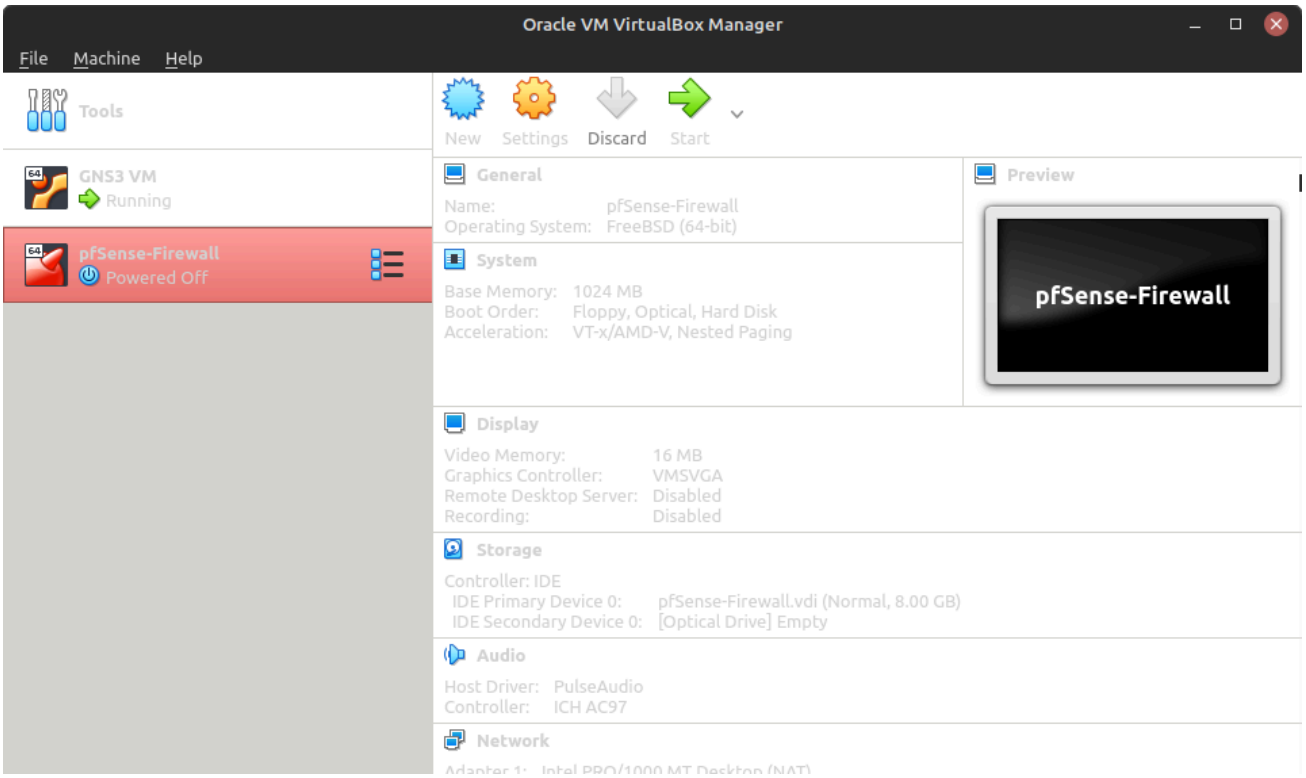


Figure 6 – pfSense created in VM list

Phase III – Configure VM settings for the pfSense Server

Depending on your existing VirtualBox configuration, some configurations may already be applied.

1. Select (highlight) the **pfSense-Firewall** VM and then click *Settings*

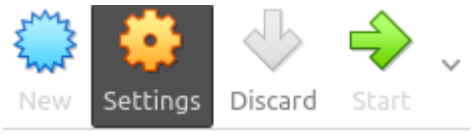


Figure 7 – Modify VM settings

2. A new sub-menu called **pfSense-Firewall – Settings** should appear

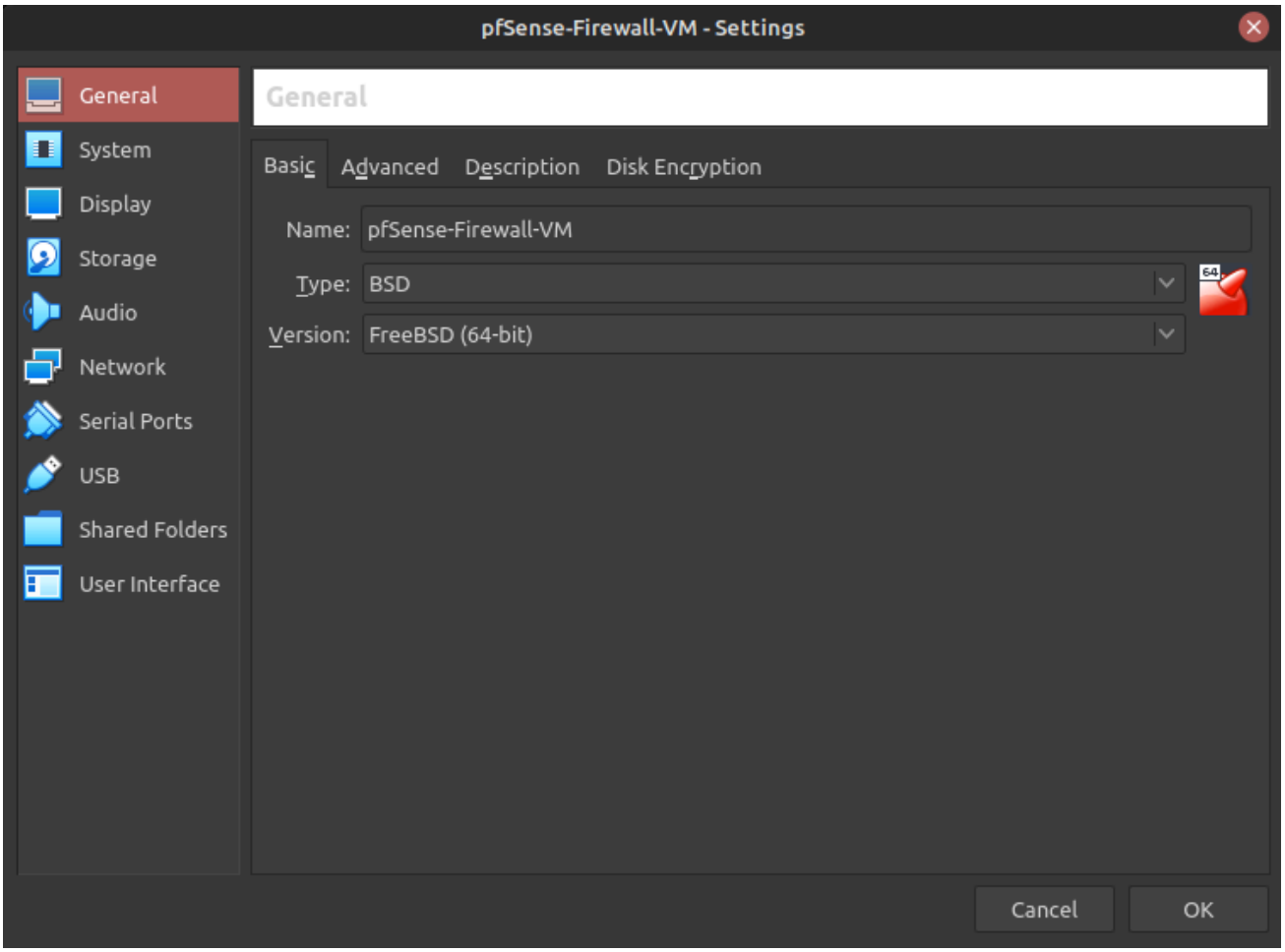


Figure 8 – Settings menu

3. Modify the **System settings** to make booting off the virtual hard disk highest priority (Figure 9)

    3.1. On the left-side menu, select ***System***

    3.2. Under Boot Order, highlight ***Hard Disk*** and click on the UP arrow until it's at the top of the list

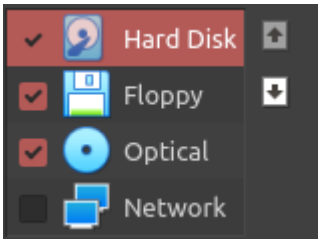


Figure 10 – Boot order menu

4. Modify the **Storage settings** to add the pfSense ISO installer (Figure 11)

4.1. On the left-side menu, select ***Storage***

4.2. Under Storage Devices, select ***Controller: IDE***

4.2.1. Select the small icon labeled ***Add optical drive*** 

4.3. A new sub-menu called **pfSense-Firewall – Optical Disk Selector** should appear (Figure 12)

4.3.1. Select ***Add Disk Image***

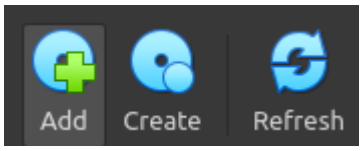


Figure 13 – Add new installation image

4.3.2. Navigate to the location where you unzipped the pfSense ISO installer and click***Open***

4.3.3. Ensure that the .iso file is highlighted and click ***Choose*** (Figure 14)

4.4. You should now see the pfSense installer in the list of Storage Devices

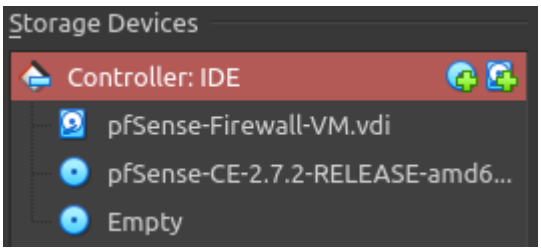


Figure 15 – Storage device list

5. Modify the **Network settings** to give the VM internet connectivity (Figure 16)

5.1. On the left-side menu, select ***Network***

5.2. Click the ***Adapter 1*** tab

5.3. Ensure that ***Enable Network Adapter*** is selected

5.4. Attached to: ***NAT***

6. Click on ***OK*** to save the new configuration settings

Phase IV – Installing the pfSense VM to the Virtual Hard Disk

Launch the pfSense VM like any other virtual machine.

1. Start the pfSense-Firewall virtual machine

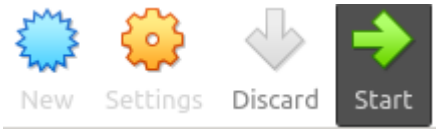


Figure 17 – Start the virtual machine

2. Select the DVD Image files to begin the installation sequence then press ***Start***

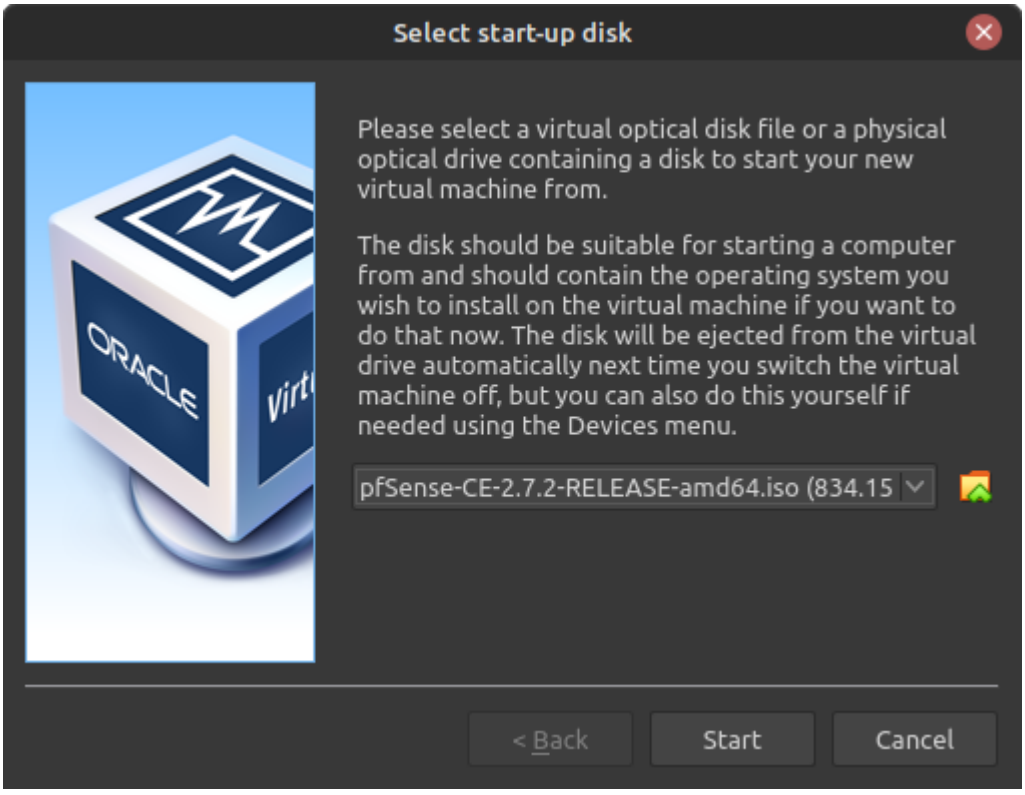


Figure 18 – Choose boot medium

3. Follow the installation guide to install pfSense to the VDI

NOTE: Place your mouse inside the VM and***left-click*** to make the VM active. To navigate out of the VM, press the ***Right-Ctrl*** key on the keyboard.

3.1. Press ***Enter*** to accept the Copyright and distribution notice (Figure 19)

3.2. Use the arrow keys to highlight ***Install*** and then tab to select ***OK*** and press ***Enter*** (Figure 20)

3.3. Use the arrow keys to highlight ***Auto (ZFS)*** and then tab to select ***OK*** and press ***Enter*** (Figure 21)

3.4. Use the arrow keys to highlight >>> ***Install*** and then tab to select ***Select*** and press ***Enter*** (Figure 22)

3.5. Use the arrow keys to highlight ***stripe*** and then tab to select ***OK*** and press ***Enter*** (Figure 23)

3.6. Use the spacebar to select ***ada0*** and then tab to select ***OK*** and press ***Enter*** (Figure 24)

> **NOTE:** You'll know it's selected when you see an asterisk (*) next to the disk name.

3.7. Use the tab key to select ***YES*** to overwrite all data and press ***Enter*** (Figure 25)

4. When installation is finished, use the tab key to select ***Reboot*** and press ***Enter***

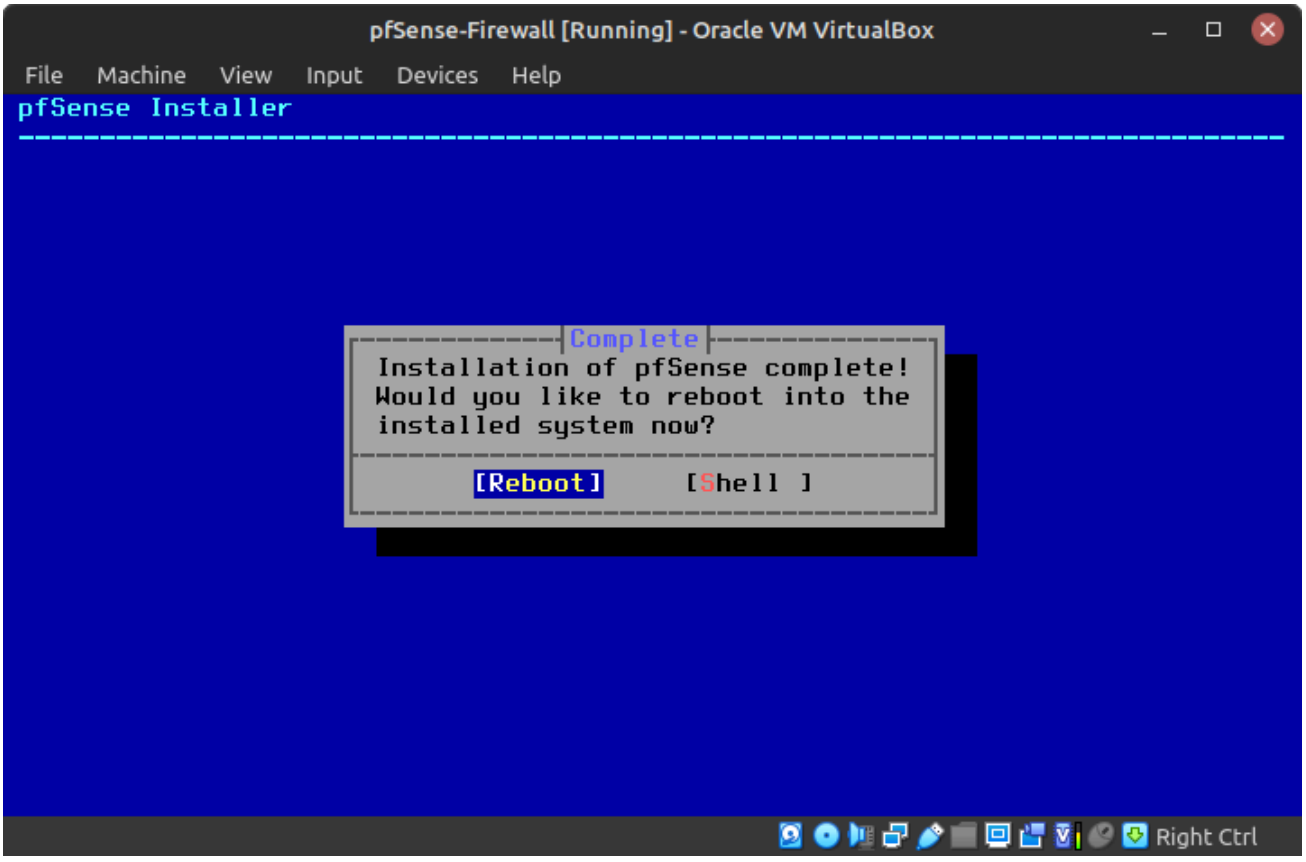


Figure 26 – Reboot after installation

5. Wait a minute for the machine to reboot

Figure Zzzzzz

6. Once the machine has booted from disk, you will be prompted for some post-installation configuration settings

> **NOTE:** You may have to press ***Enter*** for the menu to appear.

```
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 or a):
```

Figure 27 – Interface configuration settings

6.1. When prompted for the WAN interface name type ***em0*** (Figure 28)

6.2. When prompted for the LAN interface name, type nothing (press ***Enter***) (Figure 29)

6.3. Type***y*** when asked to proceed (Figure 30)

7. You should now see the main menu for pfSense!

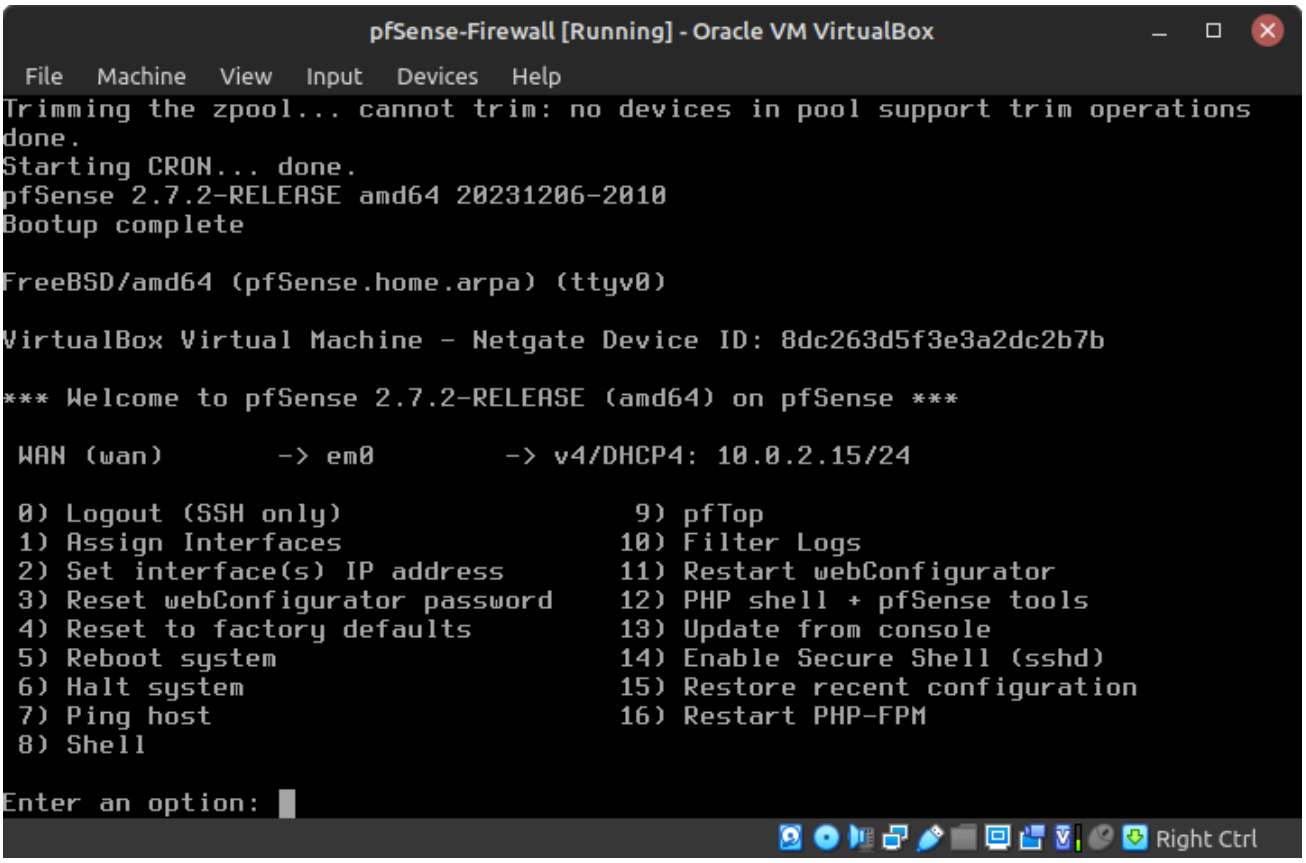


Figure 31 – pfSense console menu

8. Now pfSense is installed, we can remove the DVD installer image from the VM's virtual disk drive

    8.1. Type ***6*** and press ***Enter*** in the pfSense console menu to gracefully shutdown the device

    8.2. Type ***y*** and press ***Enter*** to proceed

    8.3. Navigate back to the VirtualBox dashboard

    8.4. Highlight the VM, click ***Settings***, then ***Storage***

    8.5. Under Storage Devices, select the ISO file (Figure 32)

    8.6. Near the bottom of the window, click ***Remove selected storage attachment*** 

> **NOTE:** Sometimes two copies of the ISO file appear. Remove them both.

    8.7. Click ***OK*** to save your settings

9. Your pfSense firewall VM is now successfully built if it boots again to the main console menu!

End of Lab

List of Figures for Print Copy

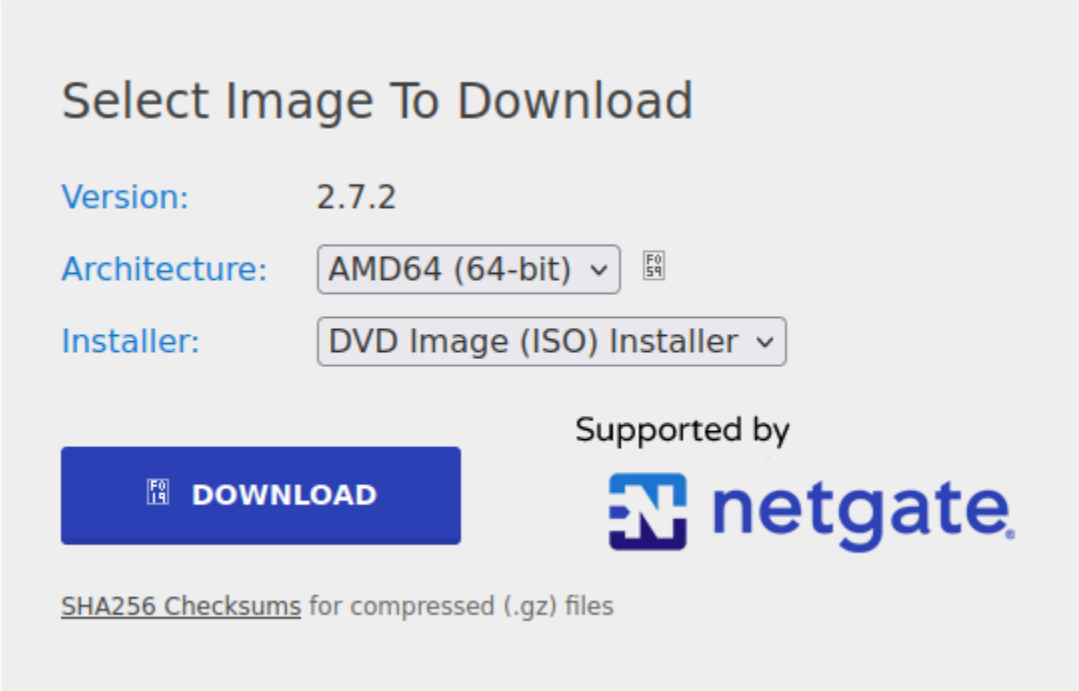


Figure 1 – Download pfSense installer

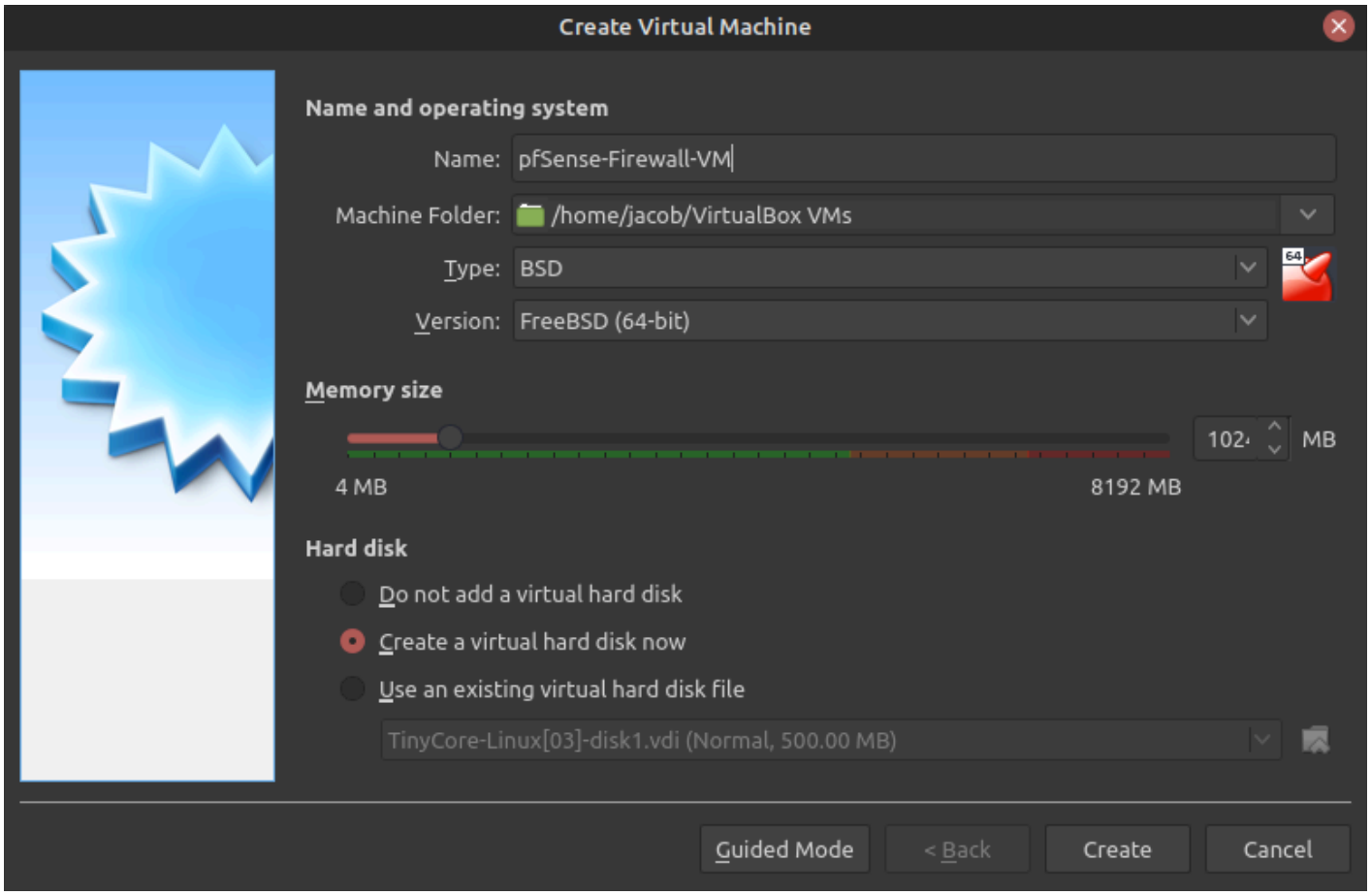


Figure 4 – Create a new virtual machine

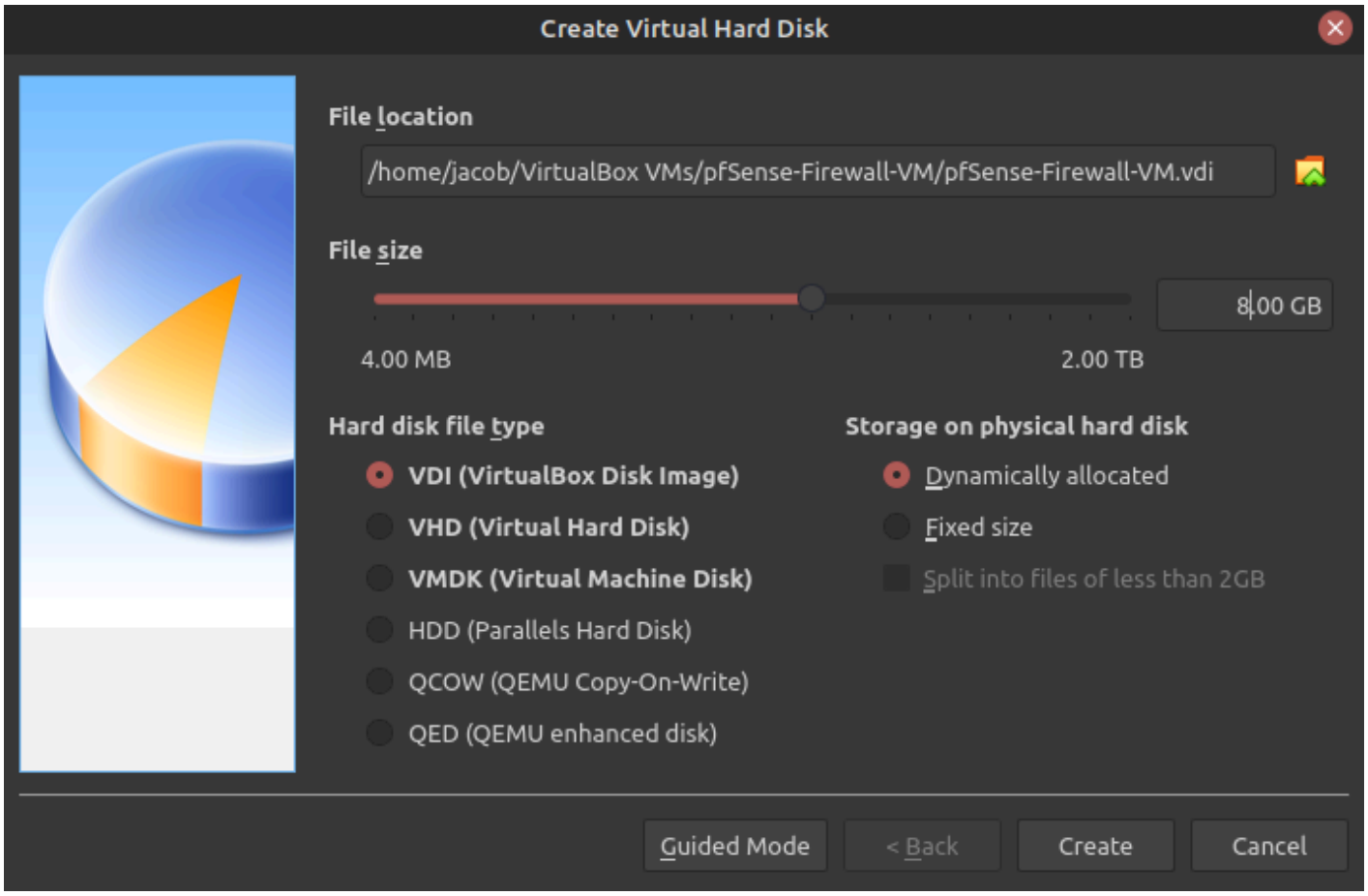


Figure 5 – Create a new virtual hard disk

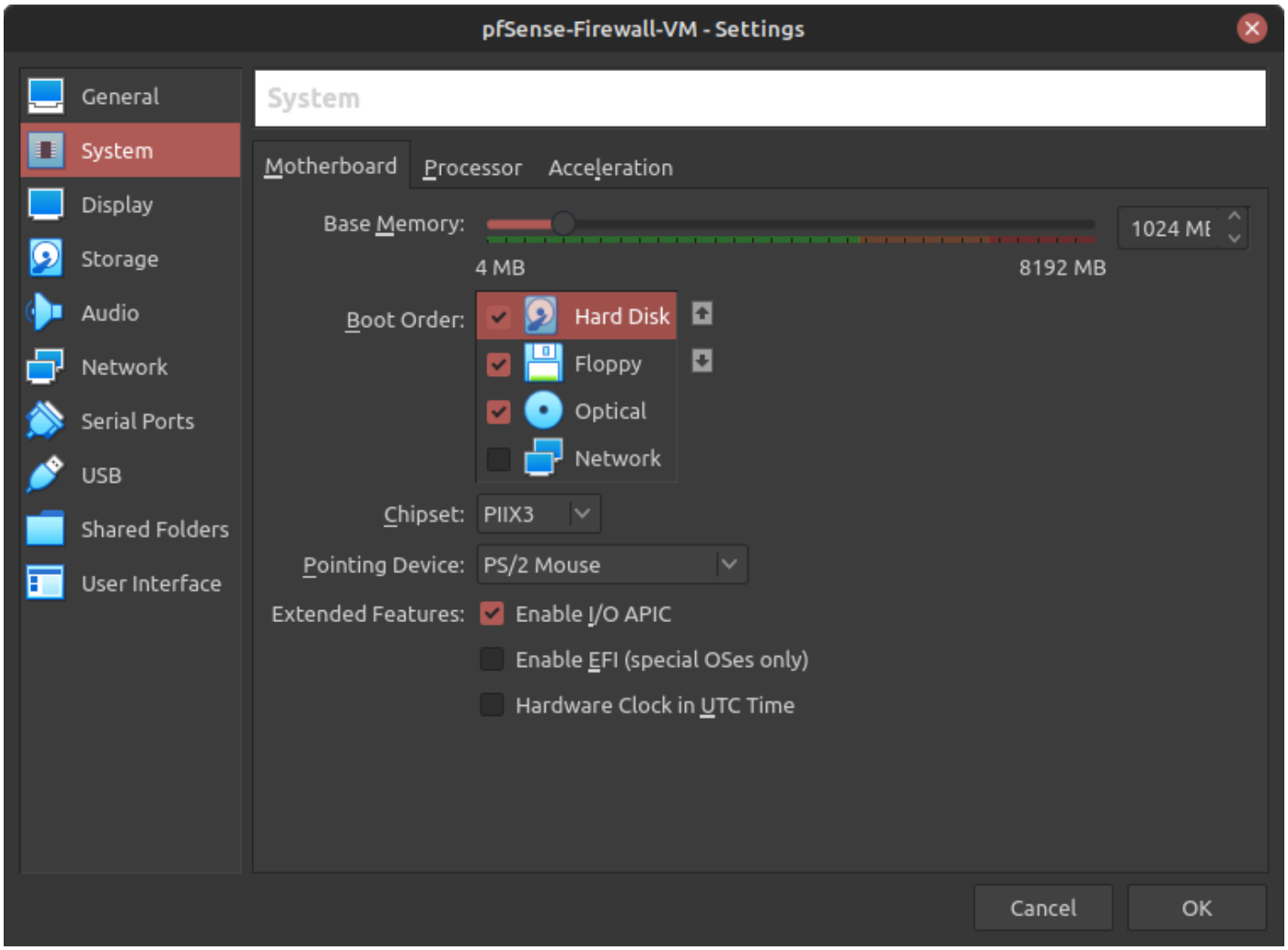


Figure 9 – Configured boot order settings

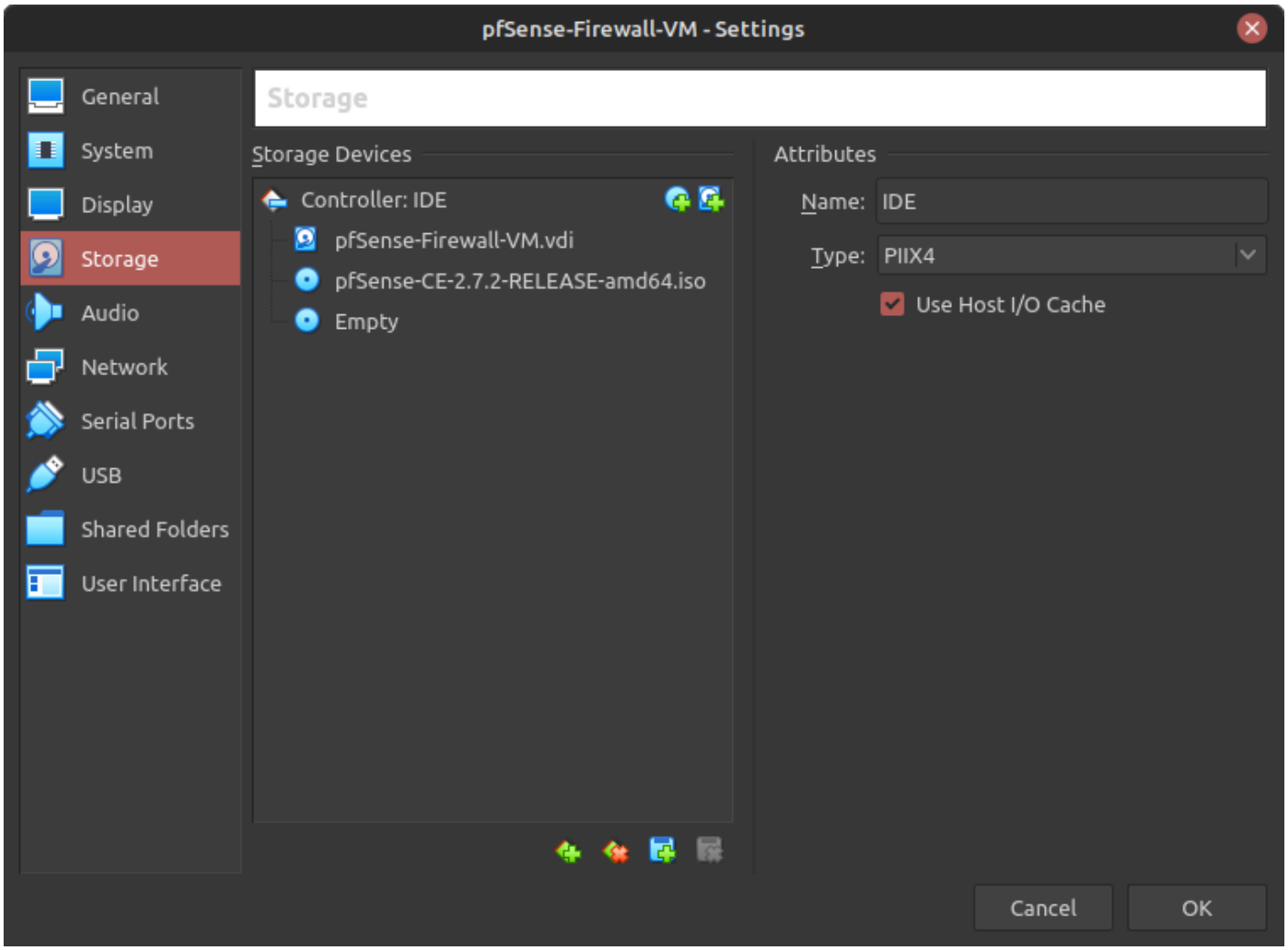


Figure 11 – Configured storage device settings

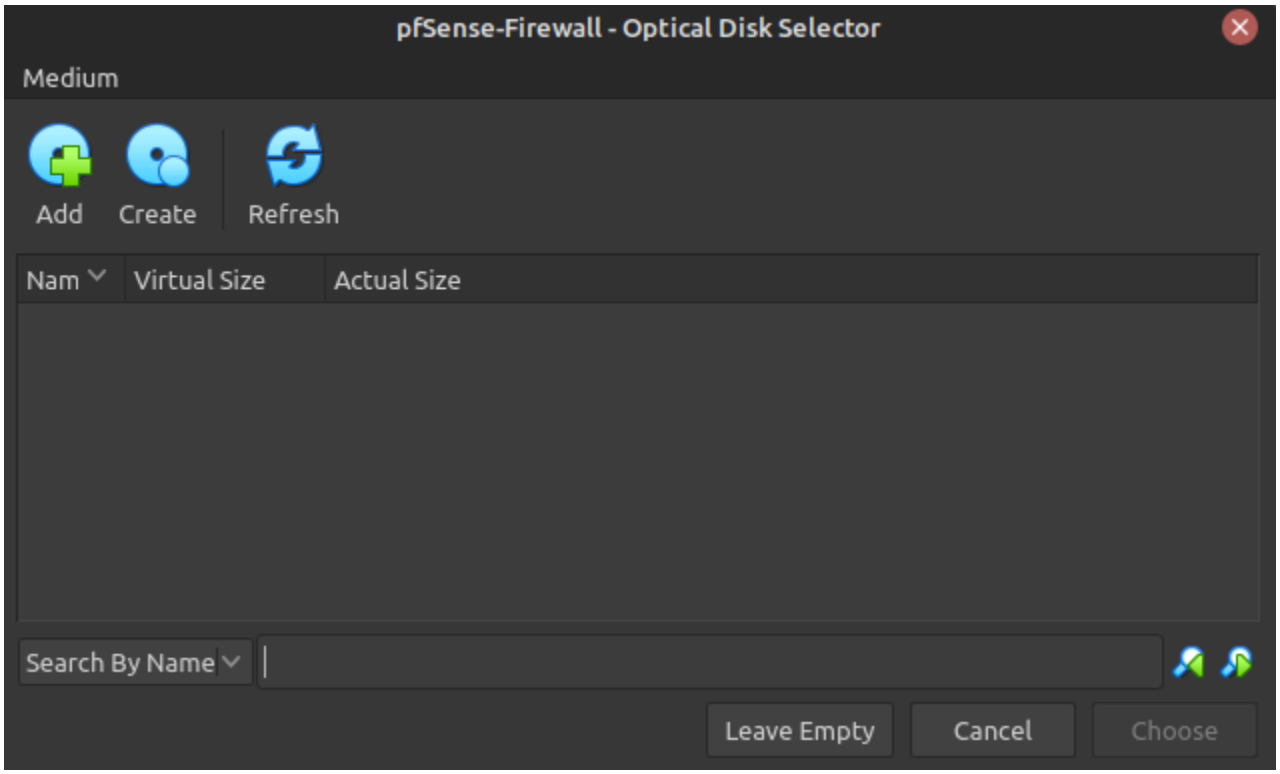


Figure 12 – Optical disk selector

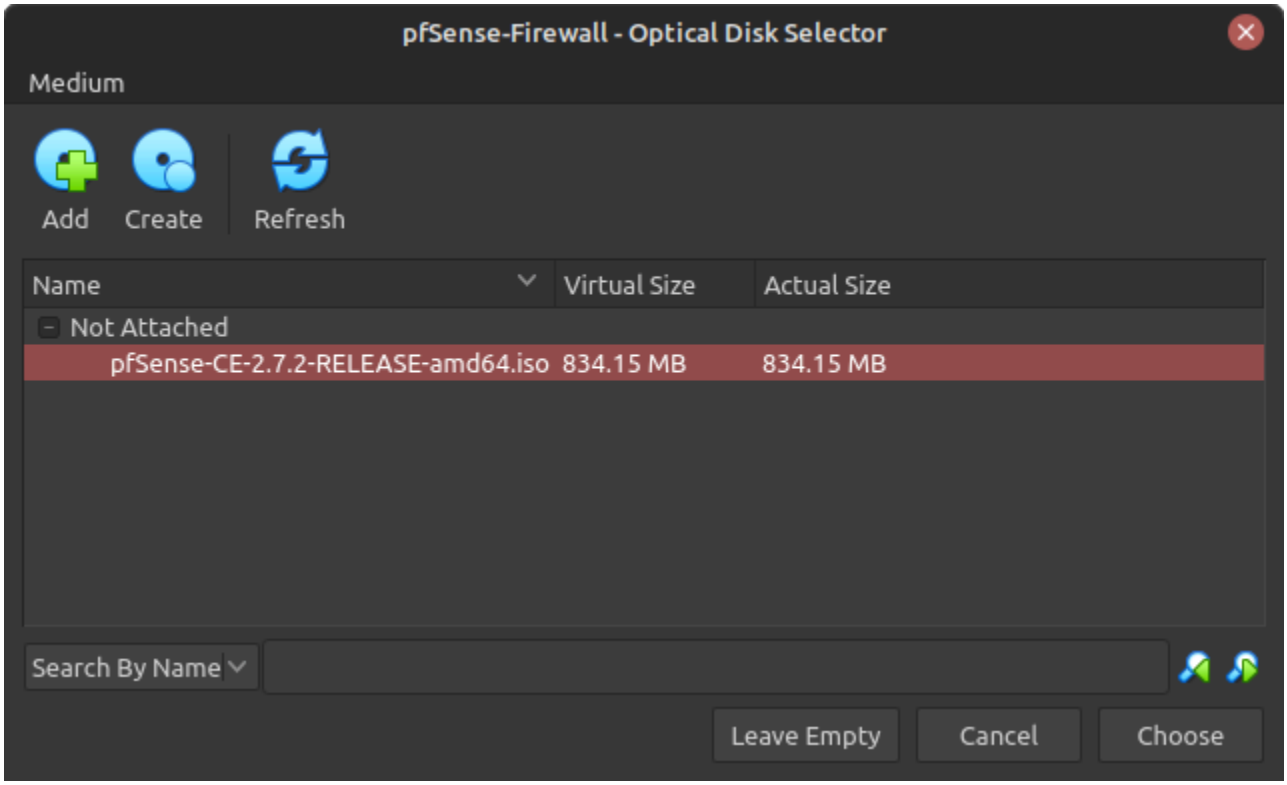


Figure 14 – Add installer to storage devices

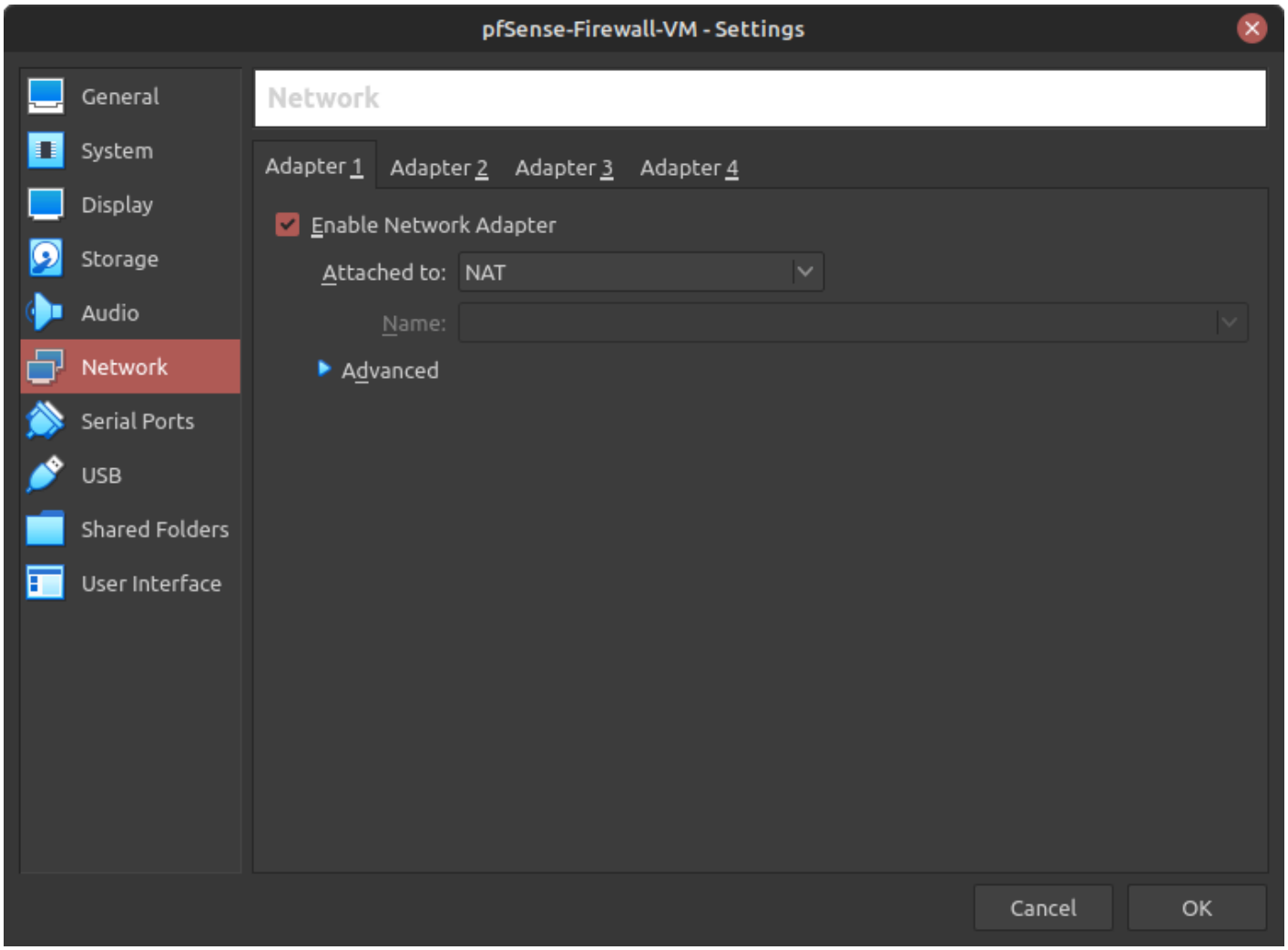


Figure 16 – Configured network settings

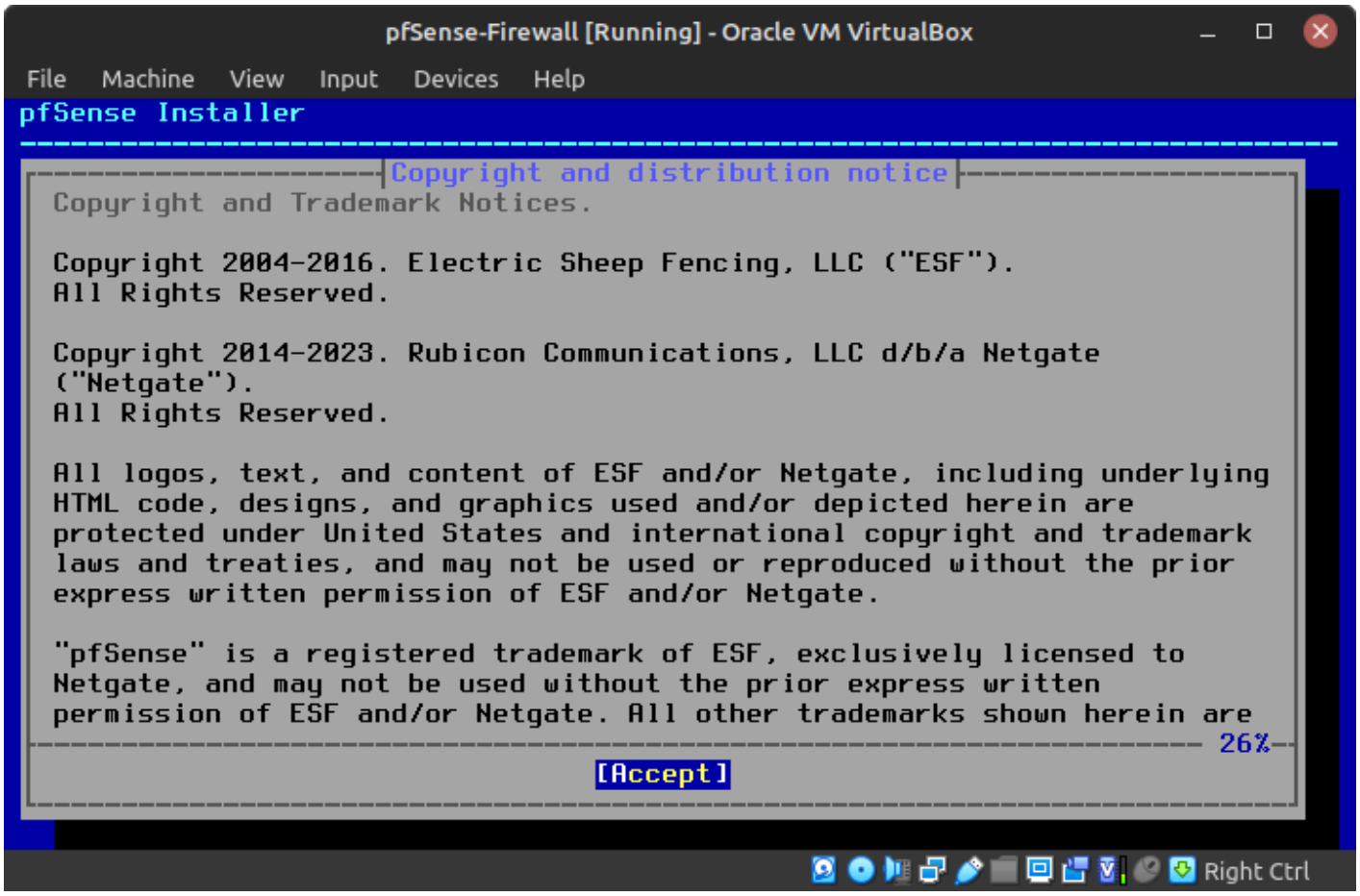


Figure 19 – Copyright and distribution notice

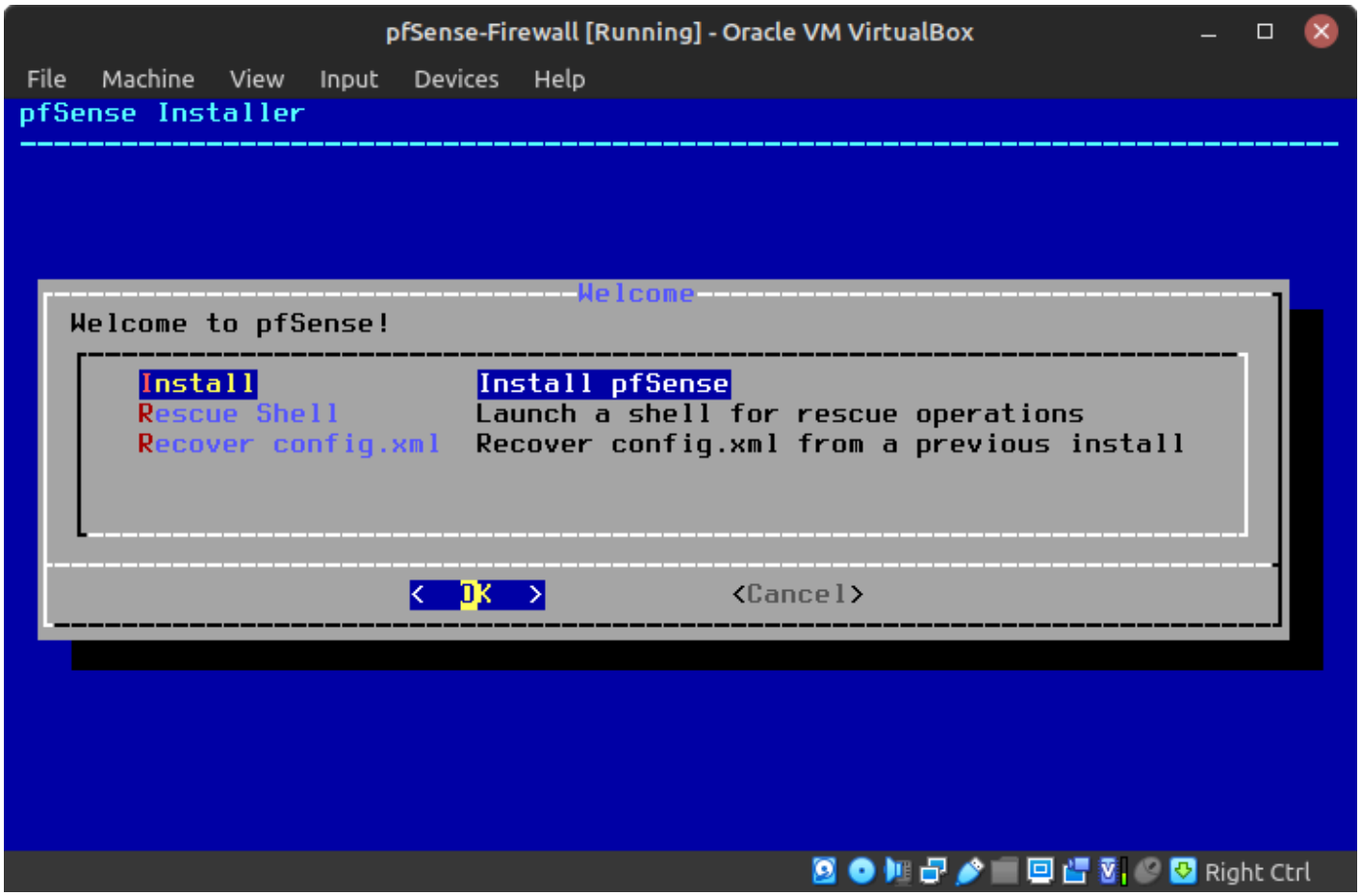


Figure 20 – Begin pfSense installation process

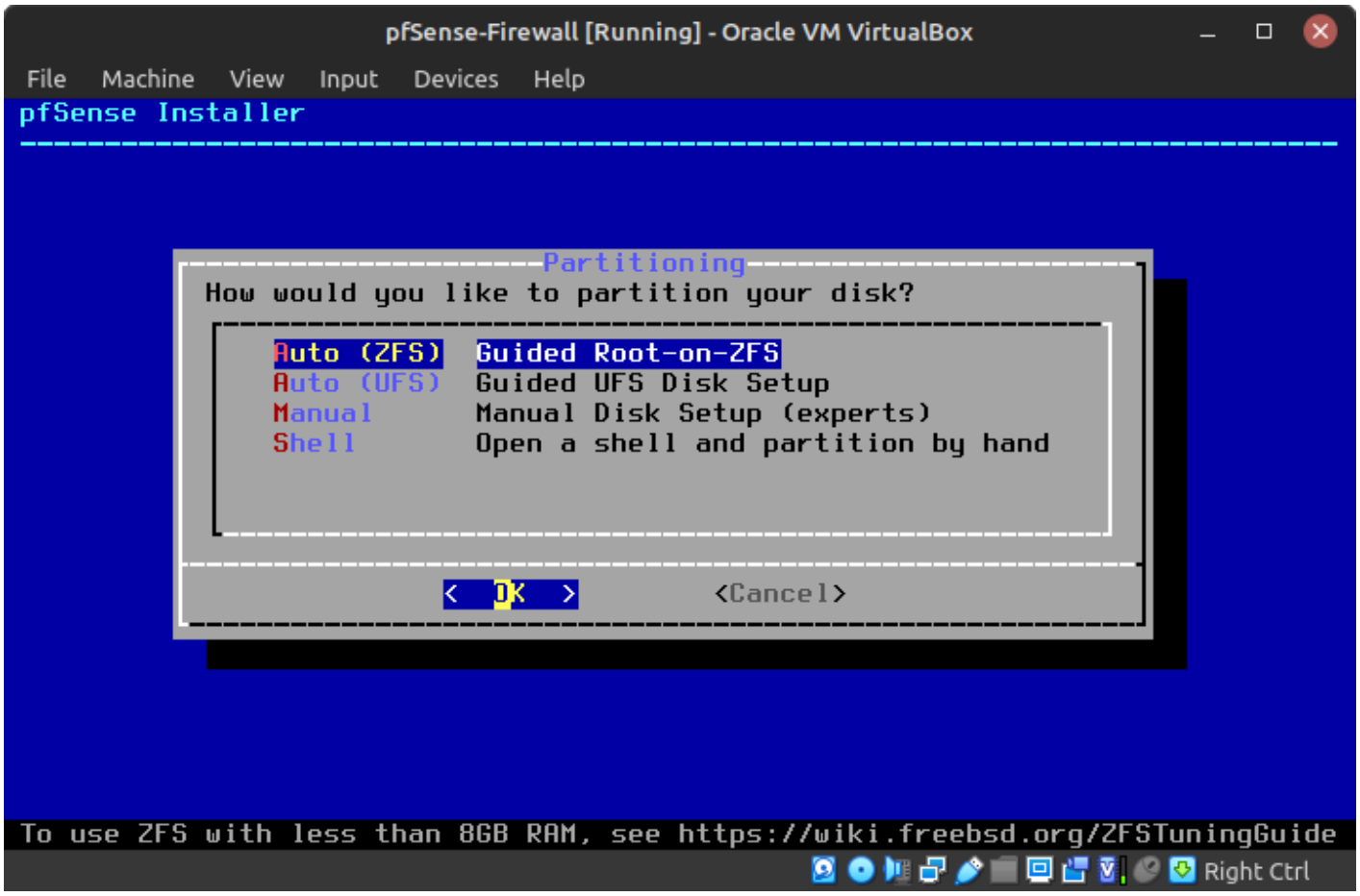


Figure 21 – Disk partitioning

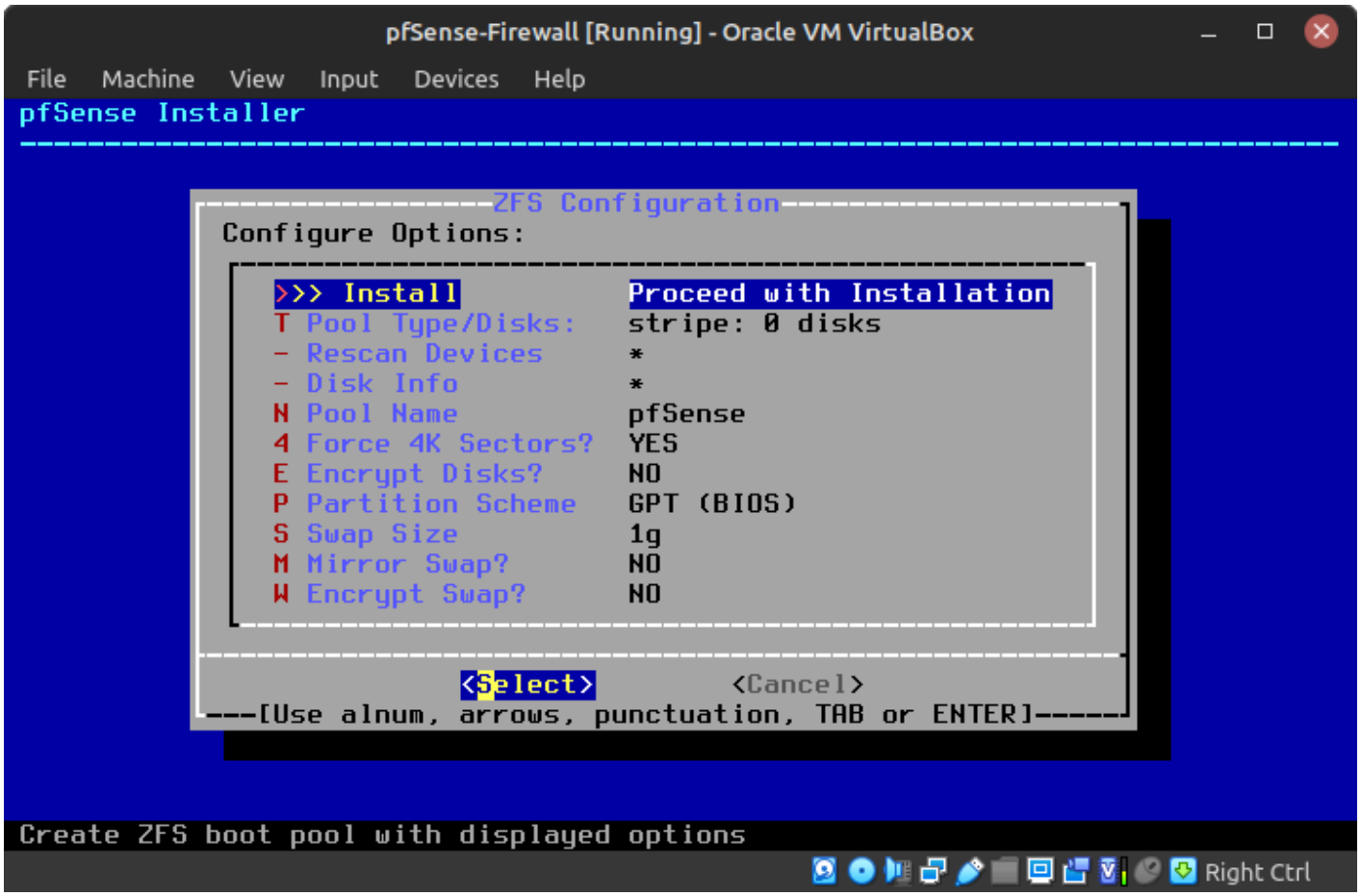


Figure 22 – Proceed with installation

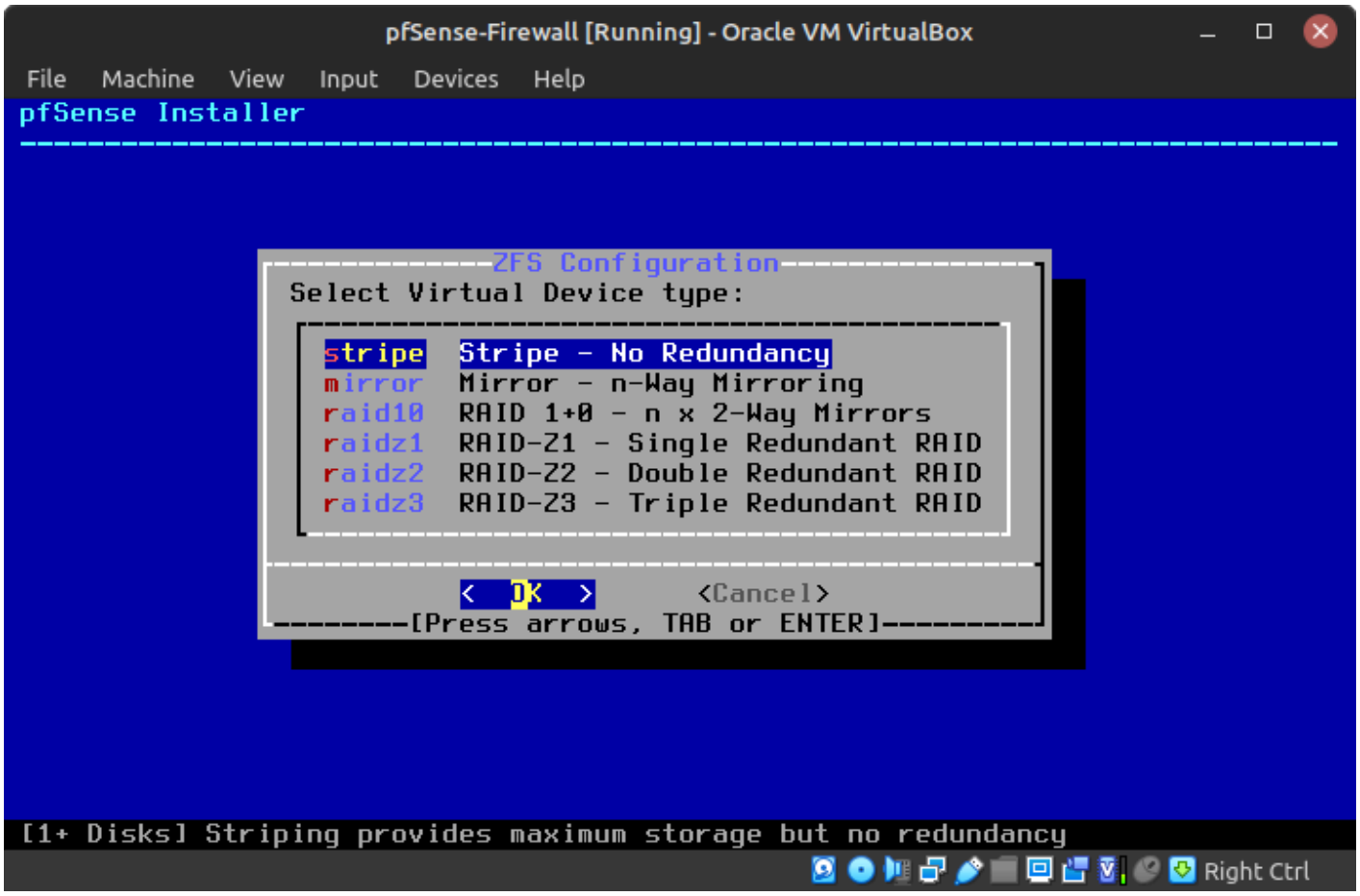


Figure 23 – Redundancy configuration

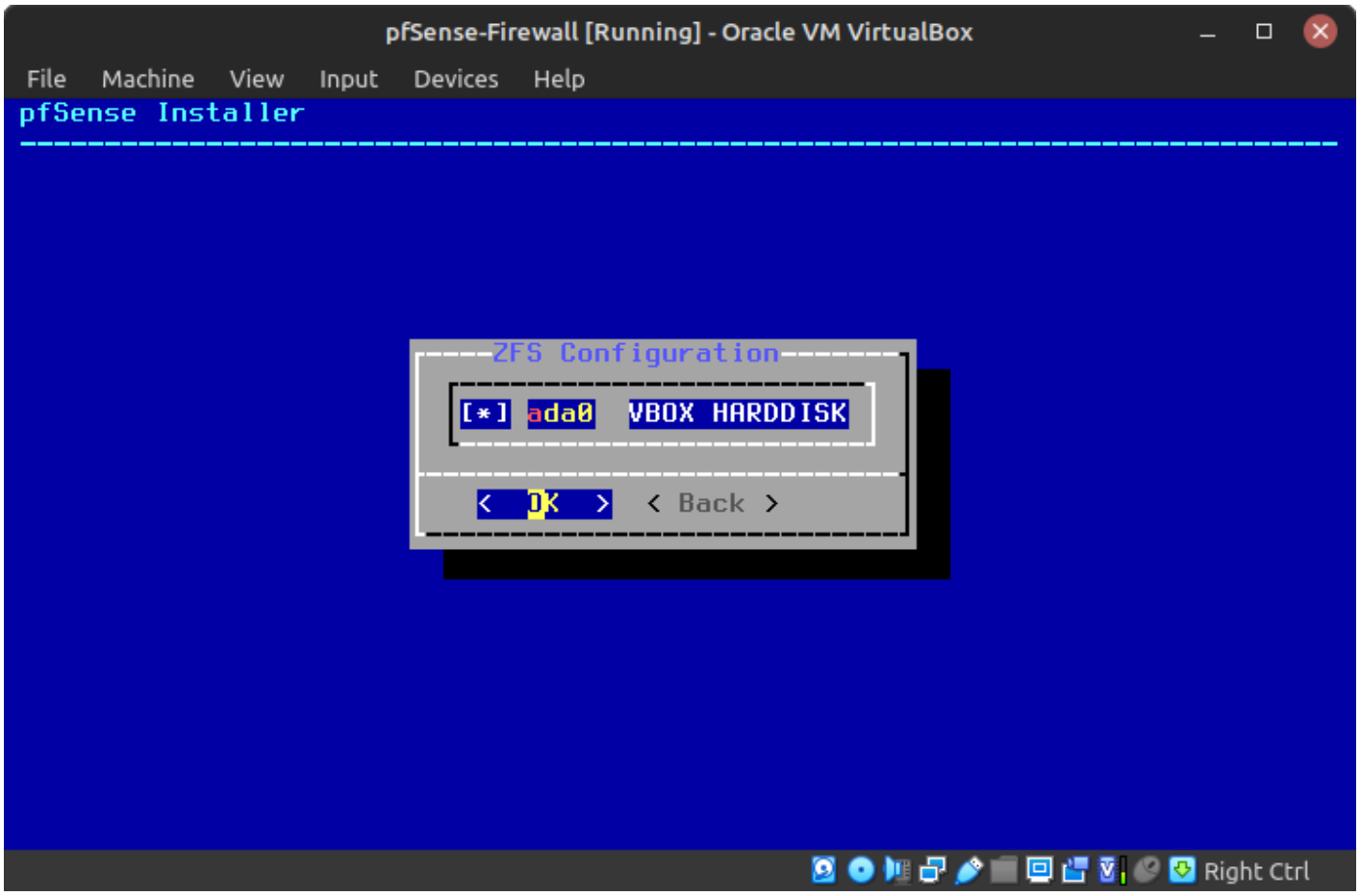


Figure 24 – Select disk to install pfSense

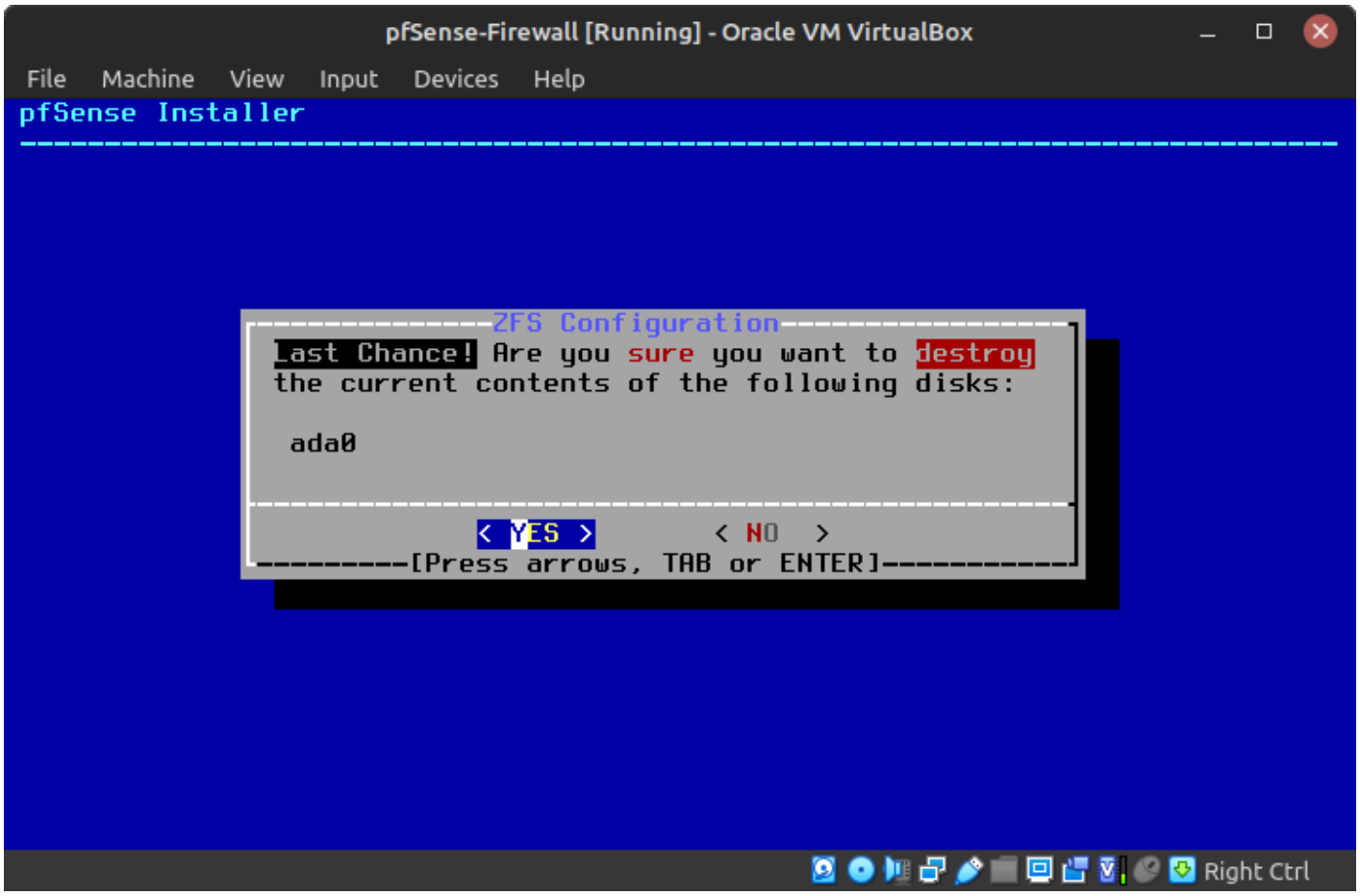


Figure 25 – Overwrite disk

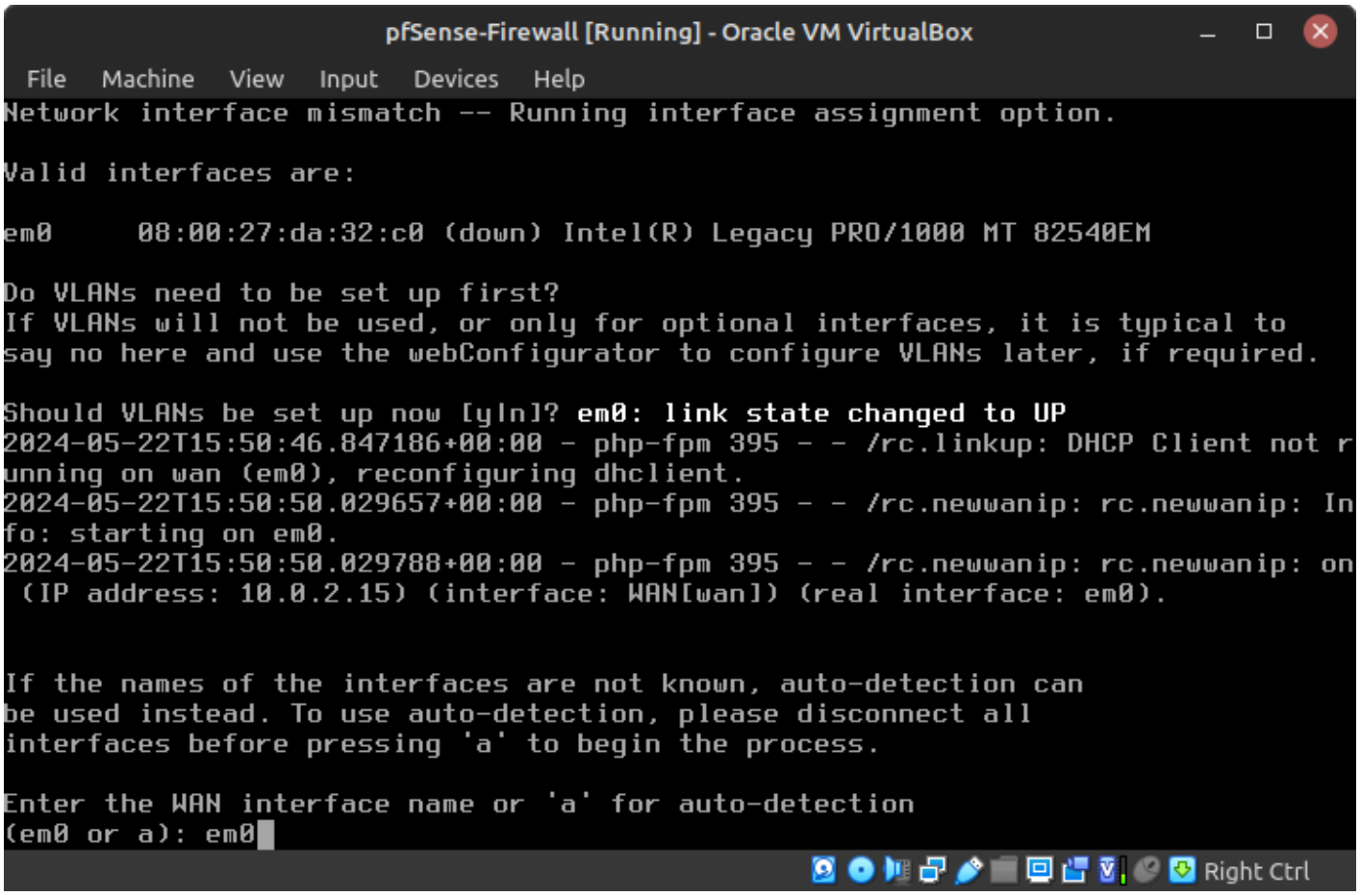


Figure 28 – Configure WAN interface

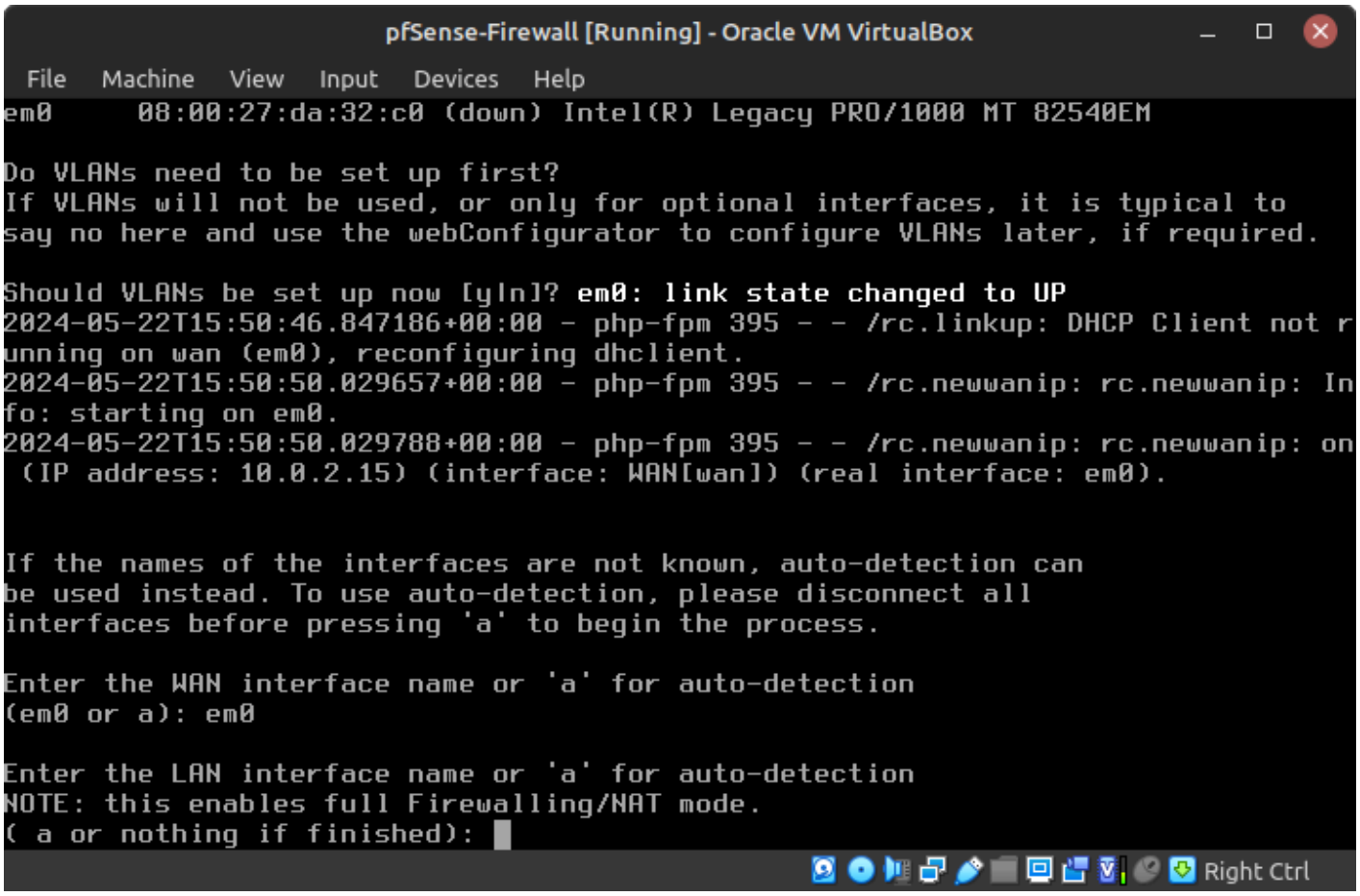


Figure 29 – Configure LAN interface

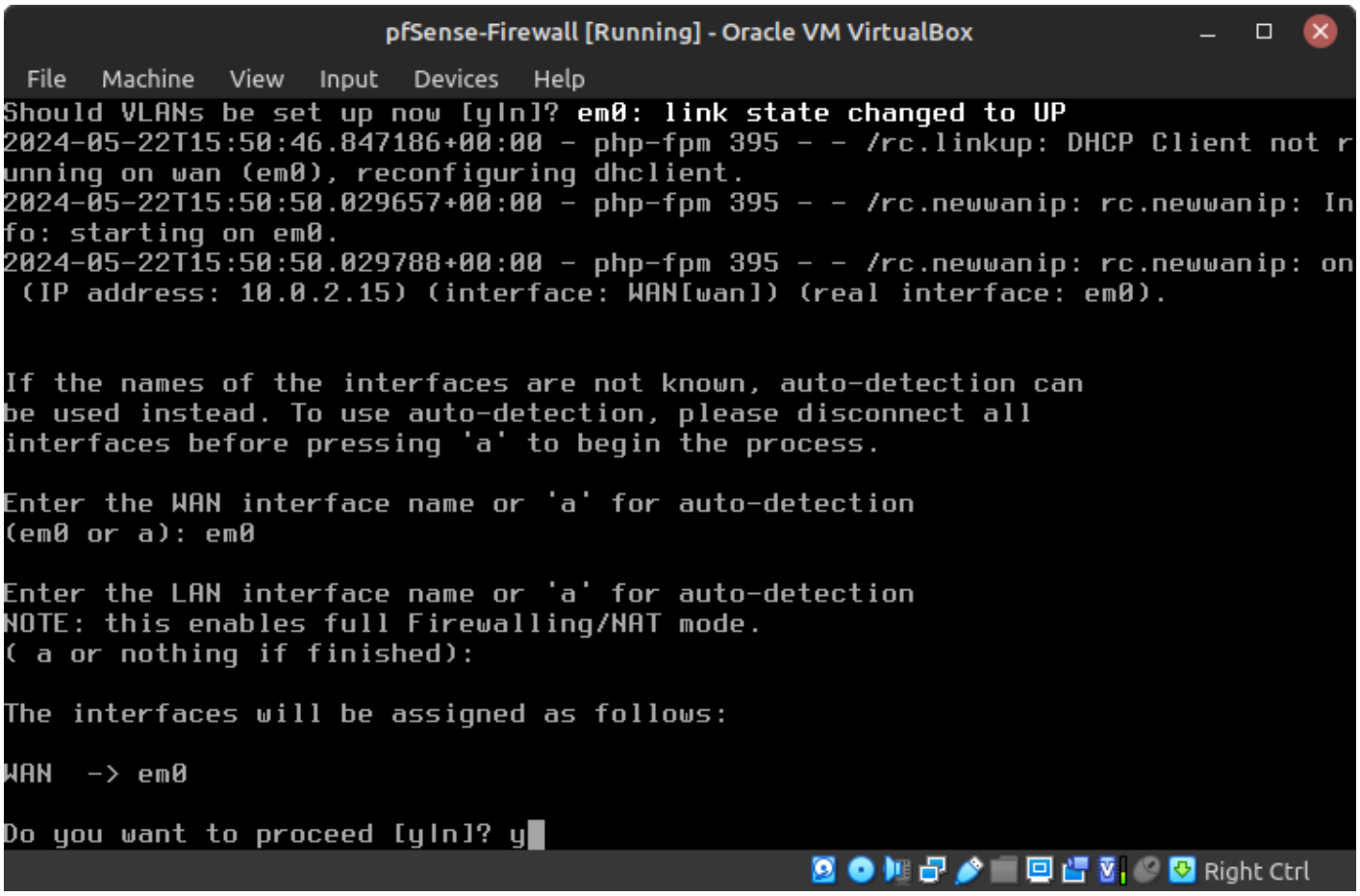


Figure 30 – Confirm settings

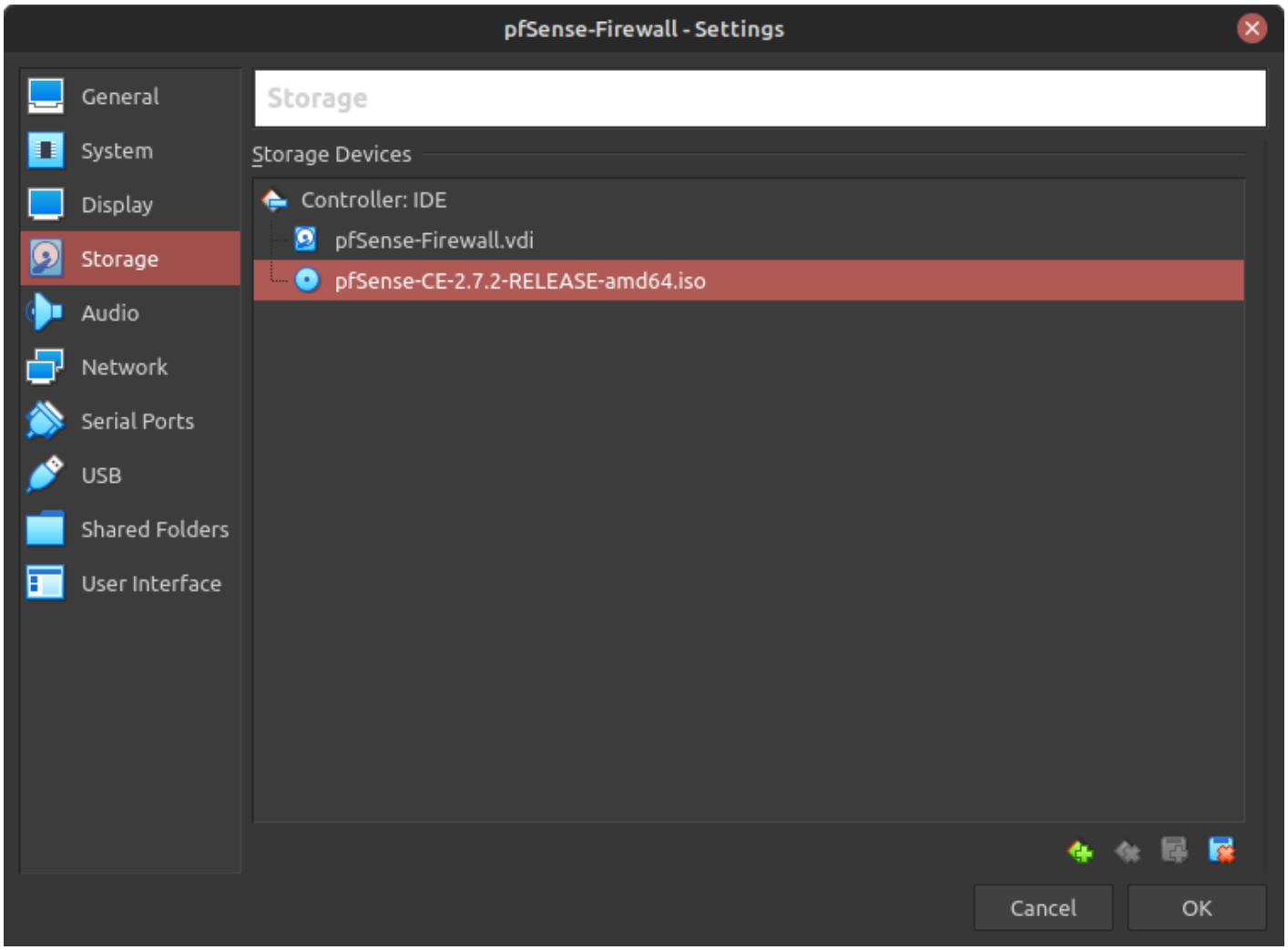


Figure 32 – Select device to remove

CHAPTER 11

Create an Ubuntu Desktop

DANTE ROCCA

Sometimes we need a Linux desktop with more power than Tiny Core Linux. Like other Linux flavors (known as distributions), Ubuntu's primary strength is the command line interface. Ubuntu Desktop has a graphical interface already installed but we will use the terminal for the installation in this lab anyway.

LEARNING OBJECTIVES

- Successfully download, install, and run Ubuntu Desktop in a GNS3 environment

PREREQUISITES

- Virtualbox Installed
- GNS3 Workspace Installed

DELIVERABLES

- None – this is a preparatory lab that supports other labs in this book

RESOURCES

- Download Ubuntu Desktop

CONTRIBUTORS AND TESTERS

- Mathew J. Heath Van Horn, PhD, ERAU-Prescott

Phase I – Download and Installation

Much like the Linux Server, installation is pretty straightforward. Be sure to work through the lab completely as the tools installed later will be used down the line.

1. Download Ubuntu Desktop from here
2. Start Oracle Virtual Box Manager
3. Click on ***New*** (Figure 1)
    3.1. Pick a name, here we will use ***Ubuntu Desktop New***
    3.2. Choose a directory where you want the VM installed. Here we used an external M2 drive
    3.3. Use the dropdown menu to select the***Ubuntu Desktop ISO*** that you downloaded
    3.4. **IMPORTANT!** Click ***Skip Unattended Installation***
    3.5. Click ***Next*** (Figure 2)
    3.6. Change the base memory to 4096 MB and click ***next*** (Figure 3)

> **NOTE**: Ubuntu Desktop requires 4GB of RAM to install. This unfortunately makes it more intense than other machines used in this book. If you need an Ubuntu Desktop that uses less RAM we recommend version 22 instead of version 24. That can be found here.

    3.7. Leave the default Virtual Hard Disk settings and click ***next*** (Figure 4)
    3.8. Review the summary and click ***Finish*** (Figure 5)
4. Start the Ubuntu Desktop VM
5. Hit enter to***try or install Ubuntu*** (Figure 6)
6. When the welcome to Ubuntu window appears select your language and click ***next*** (Figure 7)
7. On the Accessibility screen, select any accessibility settings relevant to you. Once done, hit ***next***
8. Select your keyboard layout and hit ***next*** (Figure 8)
9. On the Internet Connection screen leave the ***Use wired connection*** radio button selected and hit ***next*** (Figure 9)
10. Select ***Install Ubuntu*** and hit ***Next*** (Figure 10)
11. Select ***Interactive Installation*** and hit ***next*** (Figure 11)
12. Select ***Default selection*** and hit ***next*** (Figure 12)

NOTE: If desired you may select Extended selection but it isn't required for the labs present in this book and will take longer to install.

13. Select any proprietary software you desire, none of them will be needed for labs in this book. Hit ***next***

14. Select ***Erase disk and install Ubuntu*** then click ***next*** (Figure 13)

15. Enter a name and the computer and username should be automatically filled out. Like every other machine we will use the name ***student***. Enter a password, as with every other machine, we use ***Security1*** as our password. Click***next*** (Figure 14)

16. Select your time zone and location (Figure 15)

17. Review your choices and click ***Install*** (Figure 16)

18. Once the installation is complete, click ***Restart now*** (Figure 17)

19. Hit ***enter*** when prompted to boot into the machine

Phase II – Installing SSH

Secure Shell (SSH) is a common remote shell and administration tool. It is used to securely remote login and command-line execution. We install it here for later use.

1. Log into the Ubuntu Desktop virtual machine

2. Click the ***Canonical logo*** (show applications) button in the bottom left corner. In the search screen that appears, search for and open the ***terminal*** (Figure 18)

3. In the newly opened terminal, type the following command to install SSH

```
sudo apt install ssh
```

4. Enter ***y*** when prompted

5. Once the install is finished, ssh will successfully be installed (Figure 19)

End of Lab

Figures for Printed Version

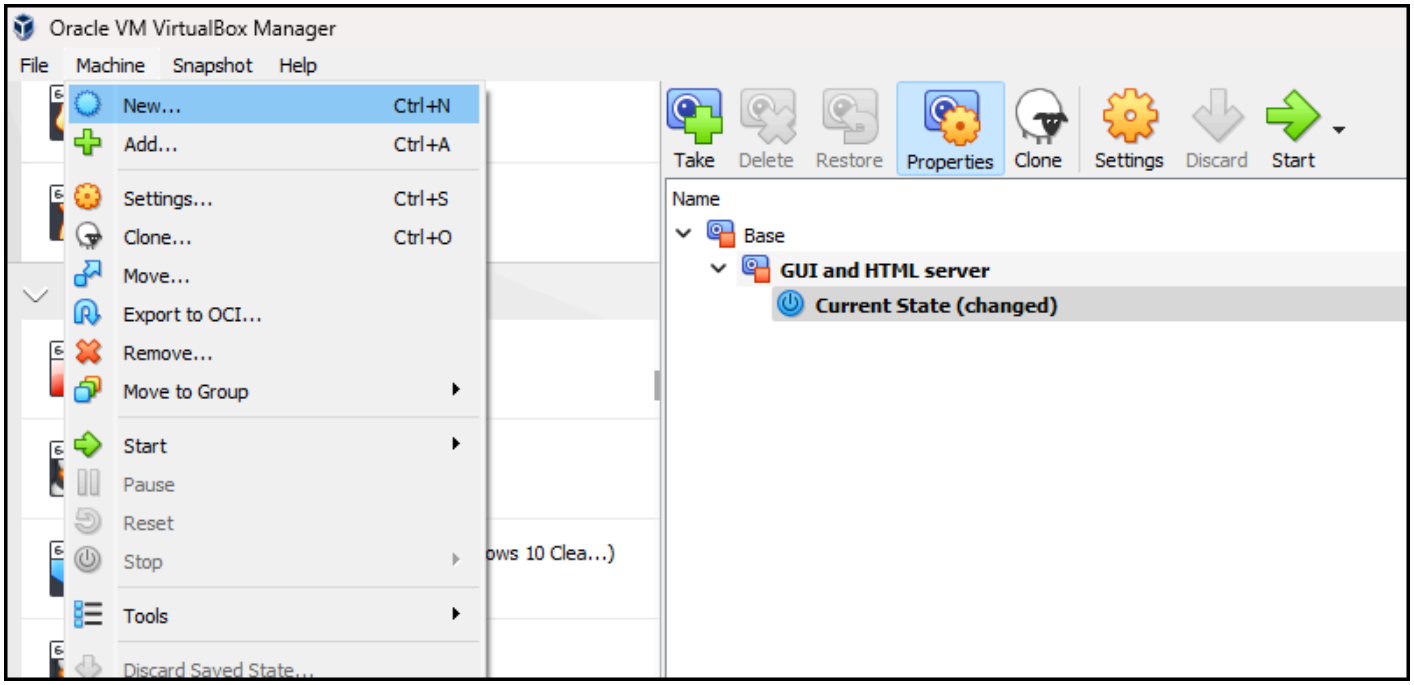


Figure 1 – Creating a new VM

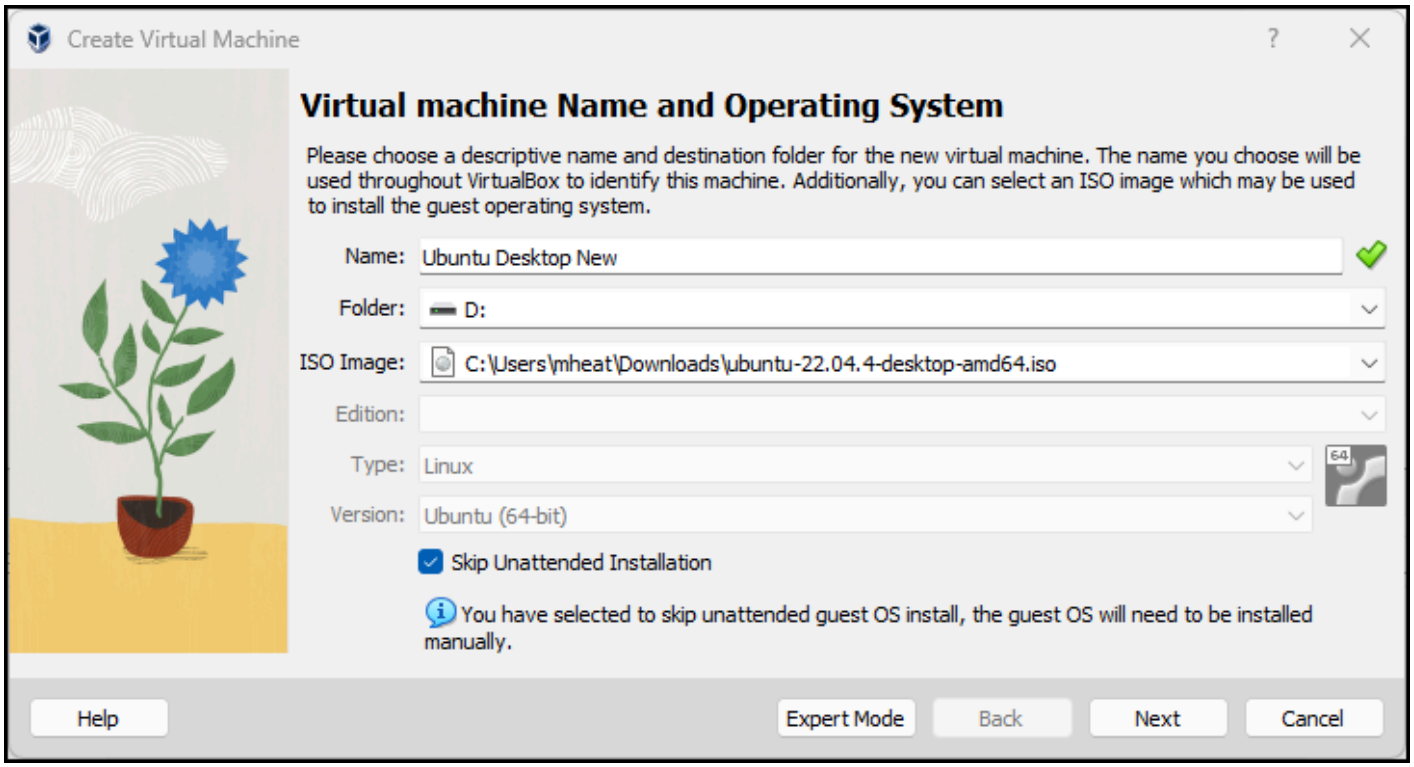


Figure 2 – Creating a new VM

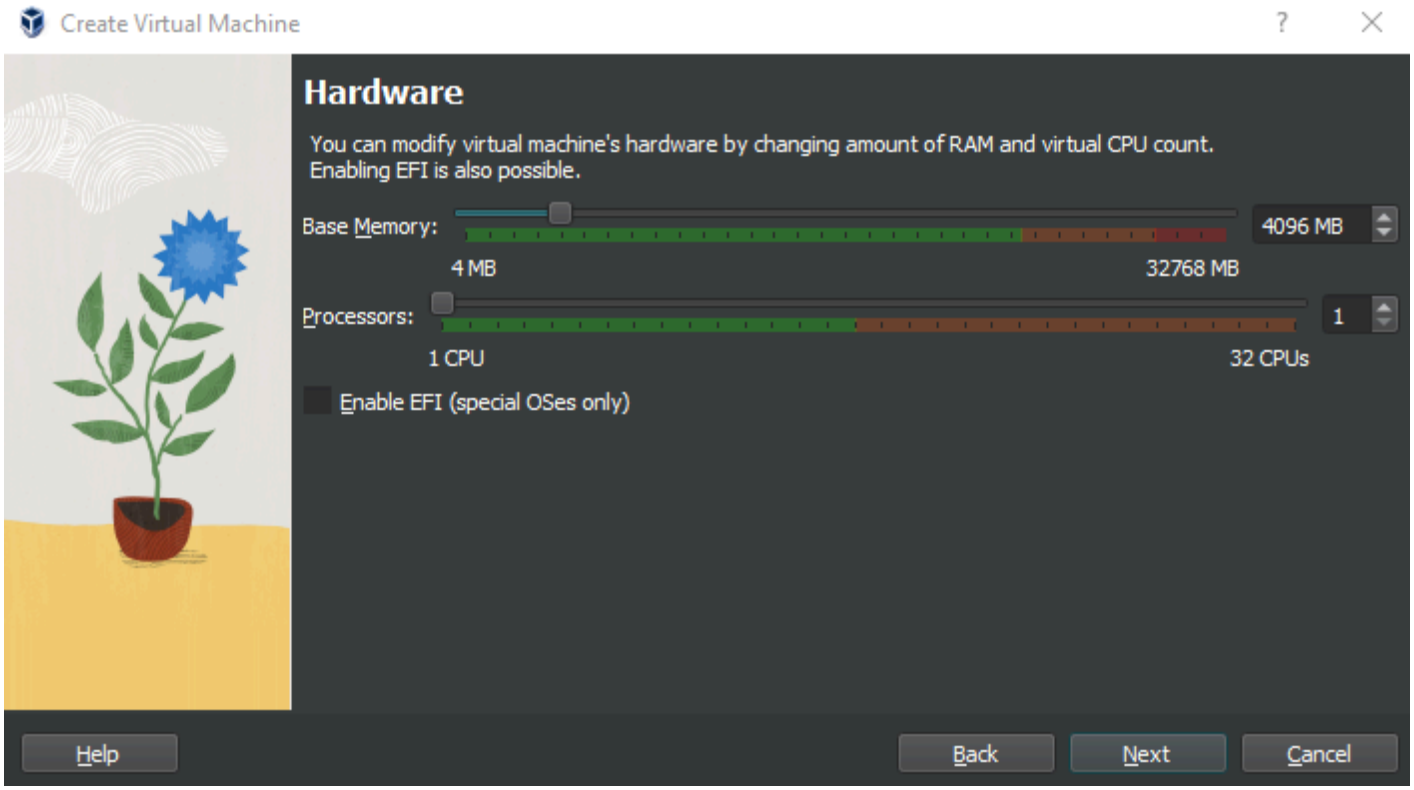


Figure 3 – Screenshot of Hardware Specifications

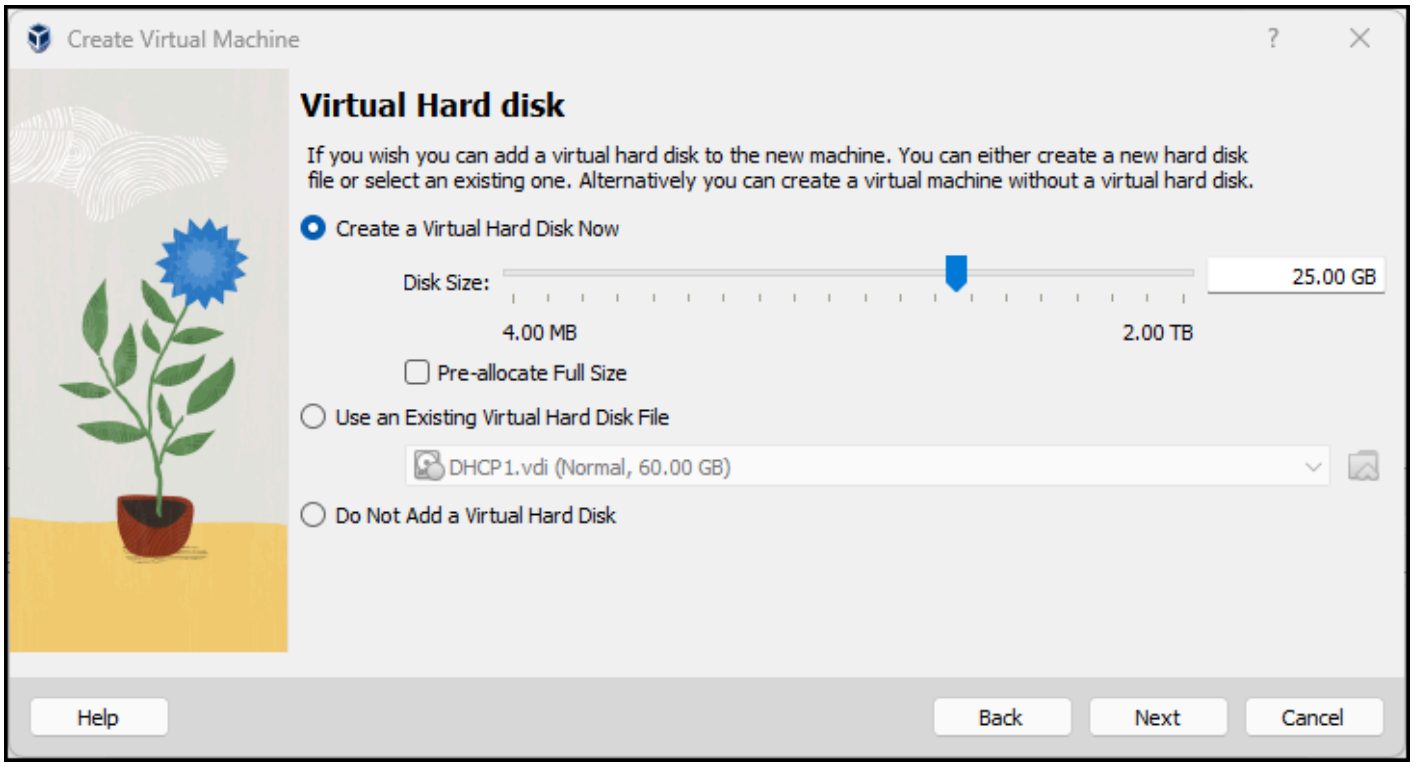


Figure 4 – Creating a new VM

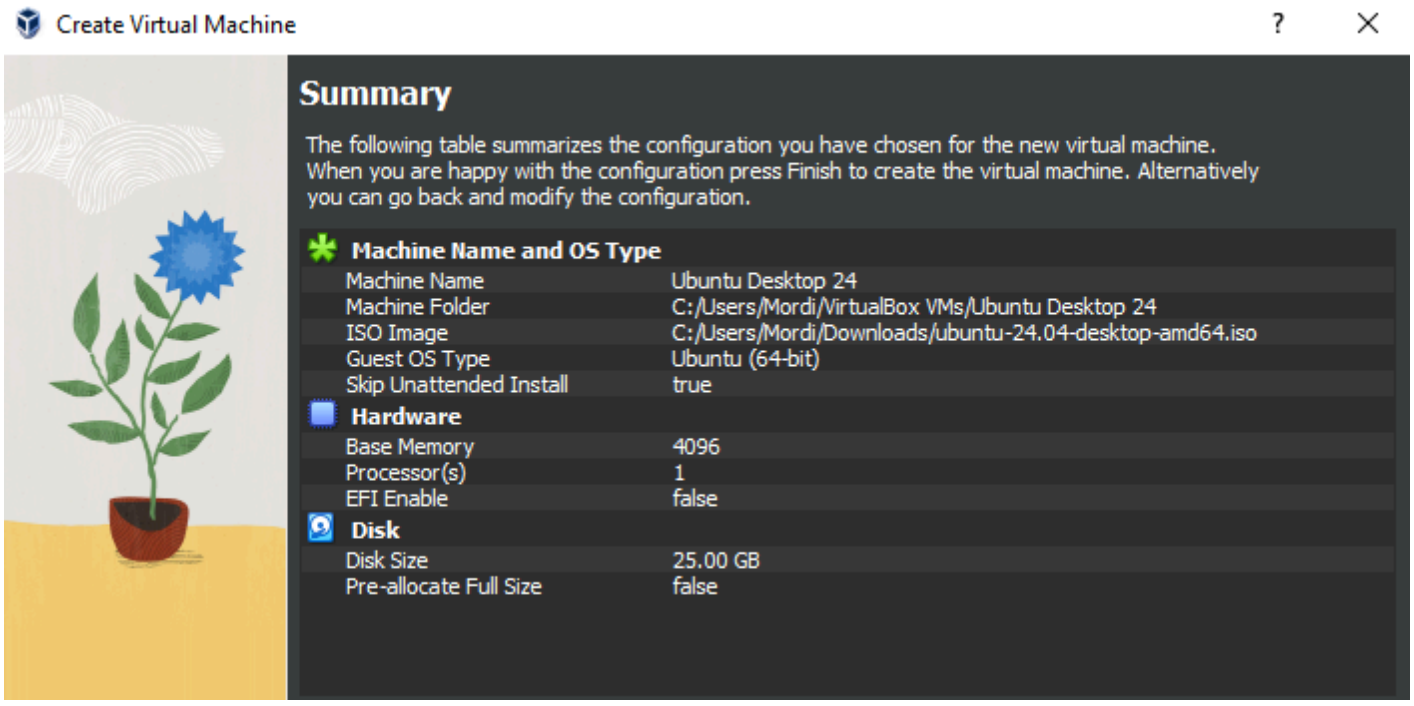


Figure 5 – Screenshot of Summary Page

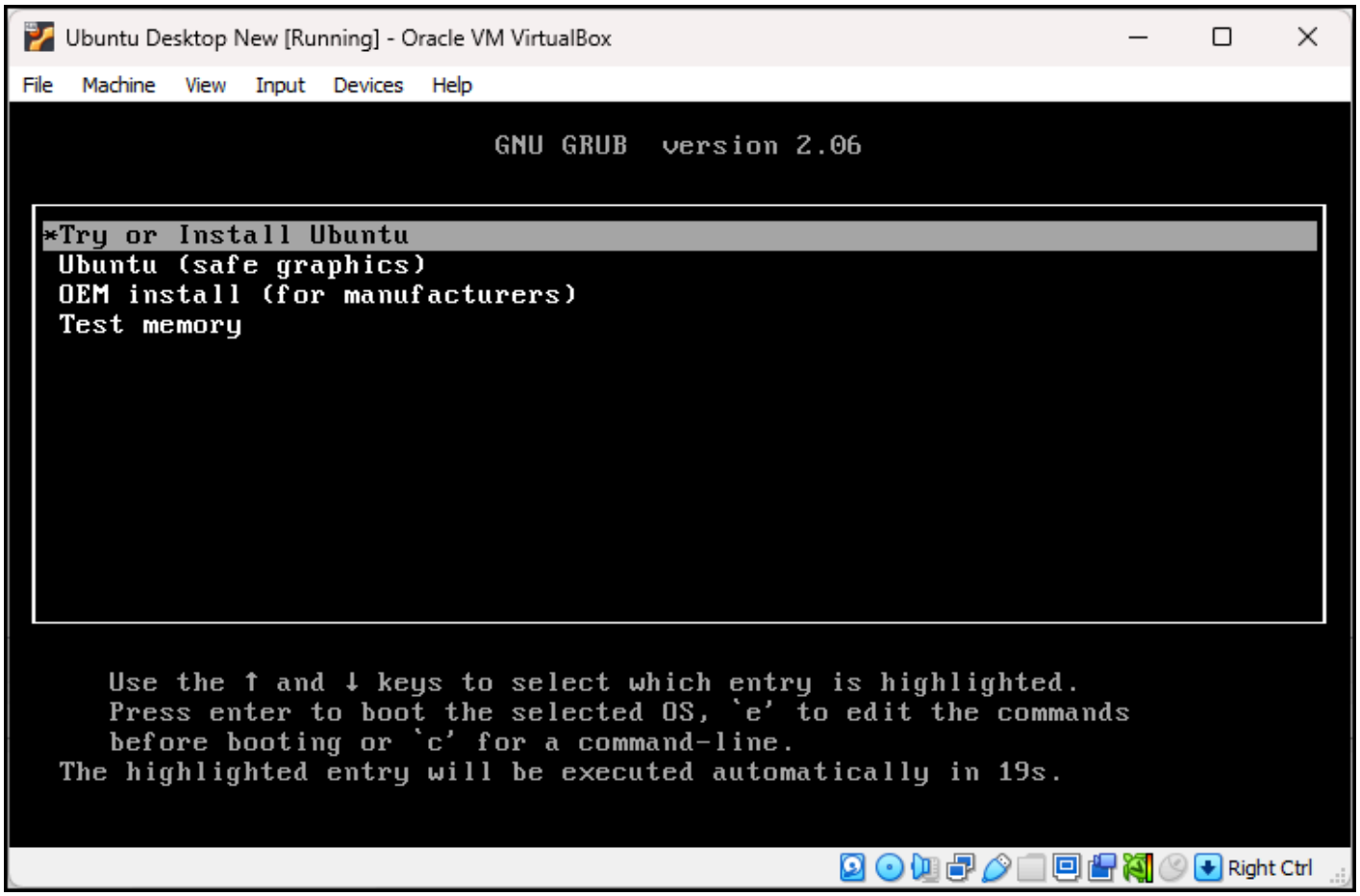


Figure 6 – Installing a Ubuntu Desktop

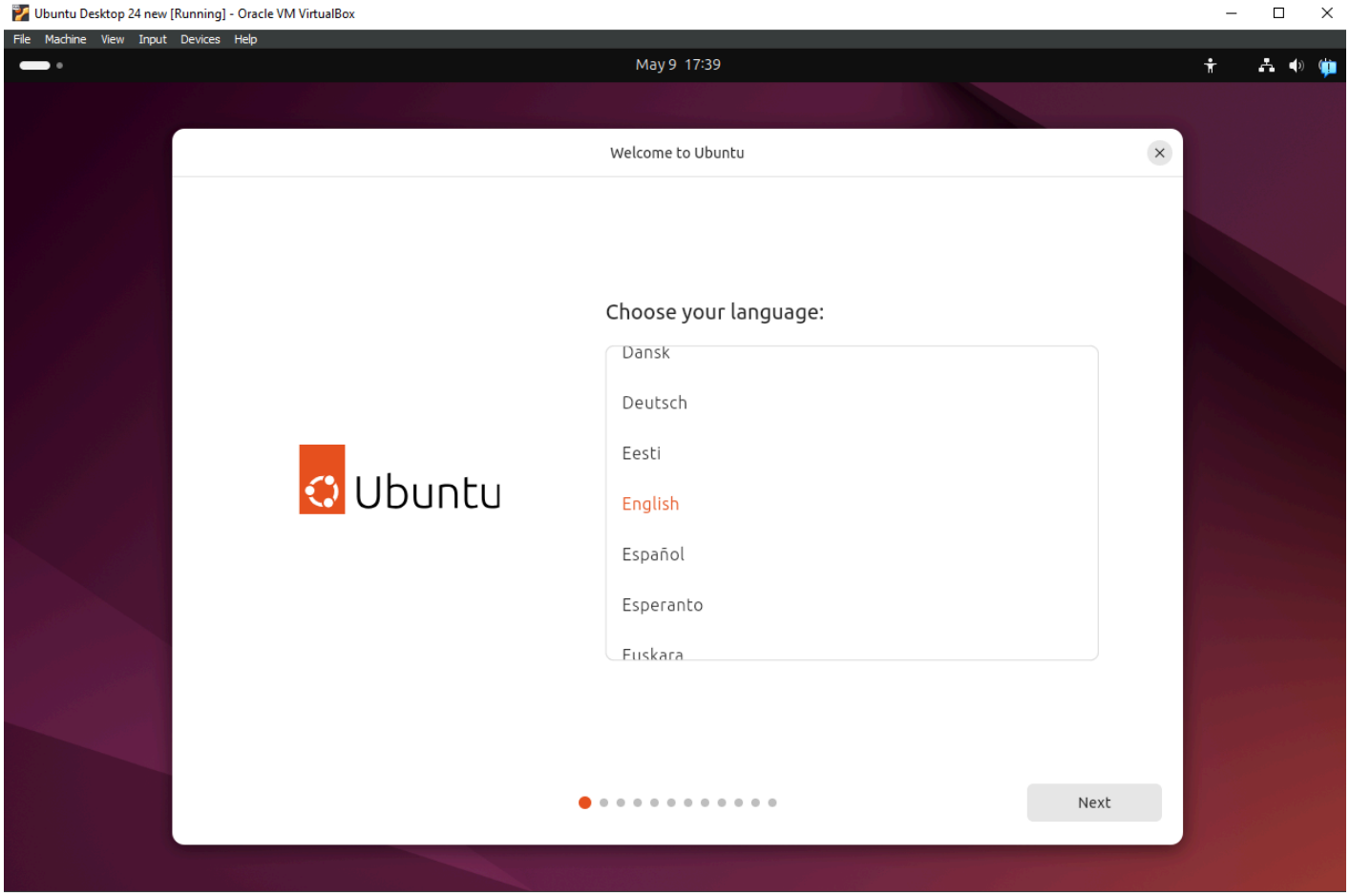


Figure 7 – Language Selection Screen

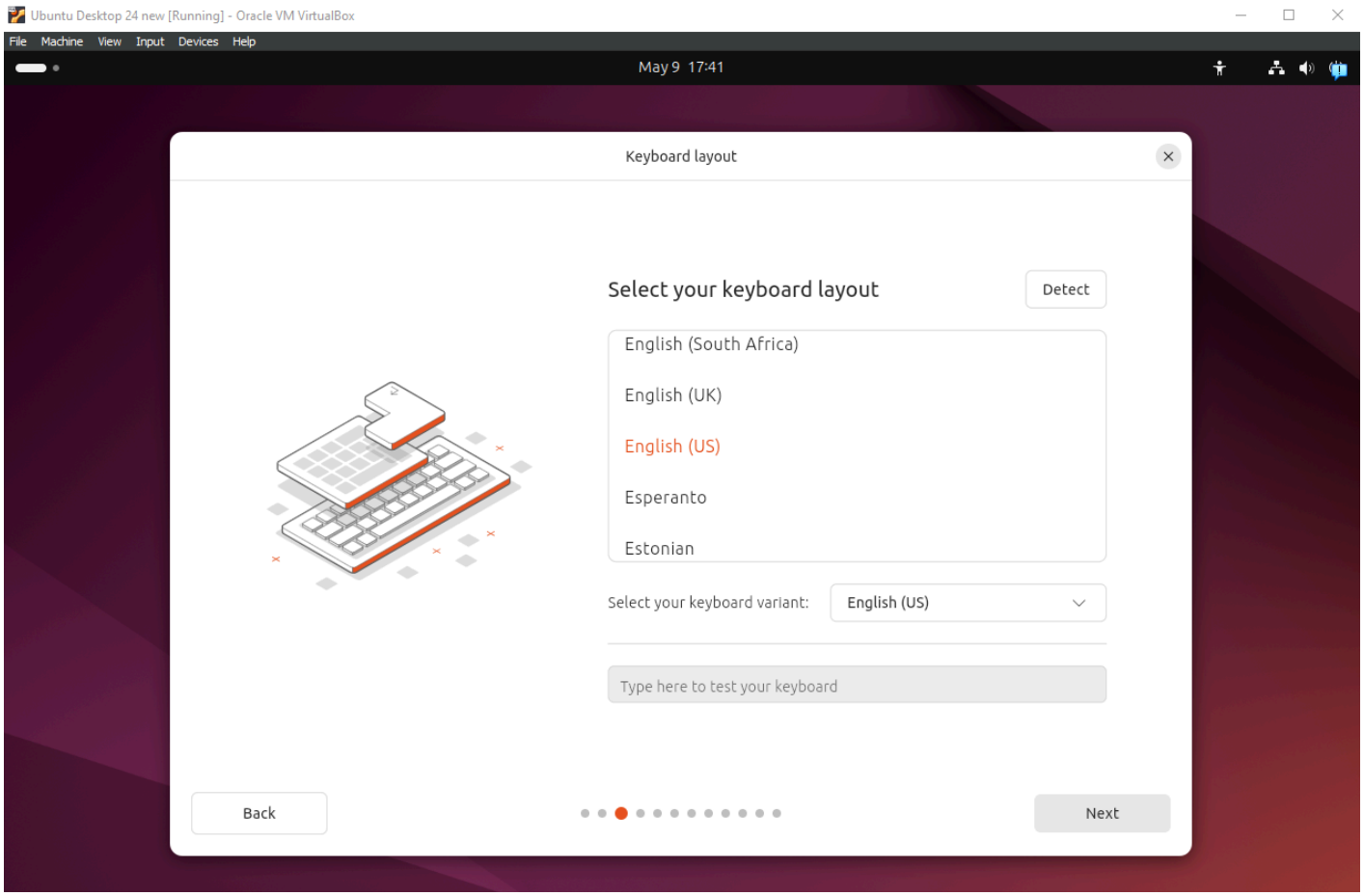


Figure 8 – Keyboard Layout Screen

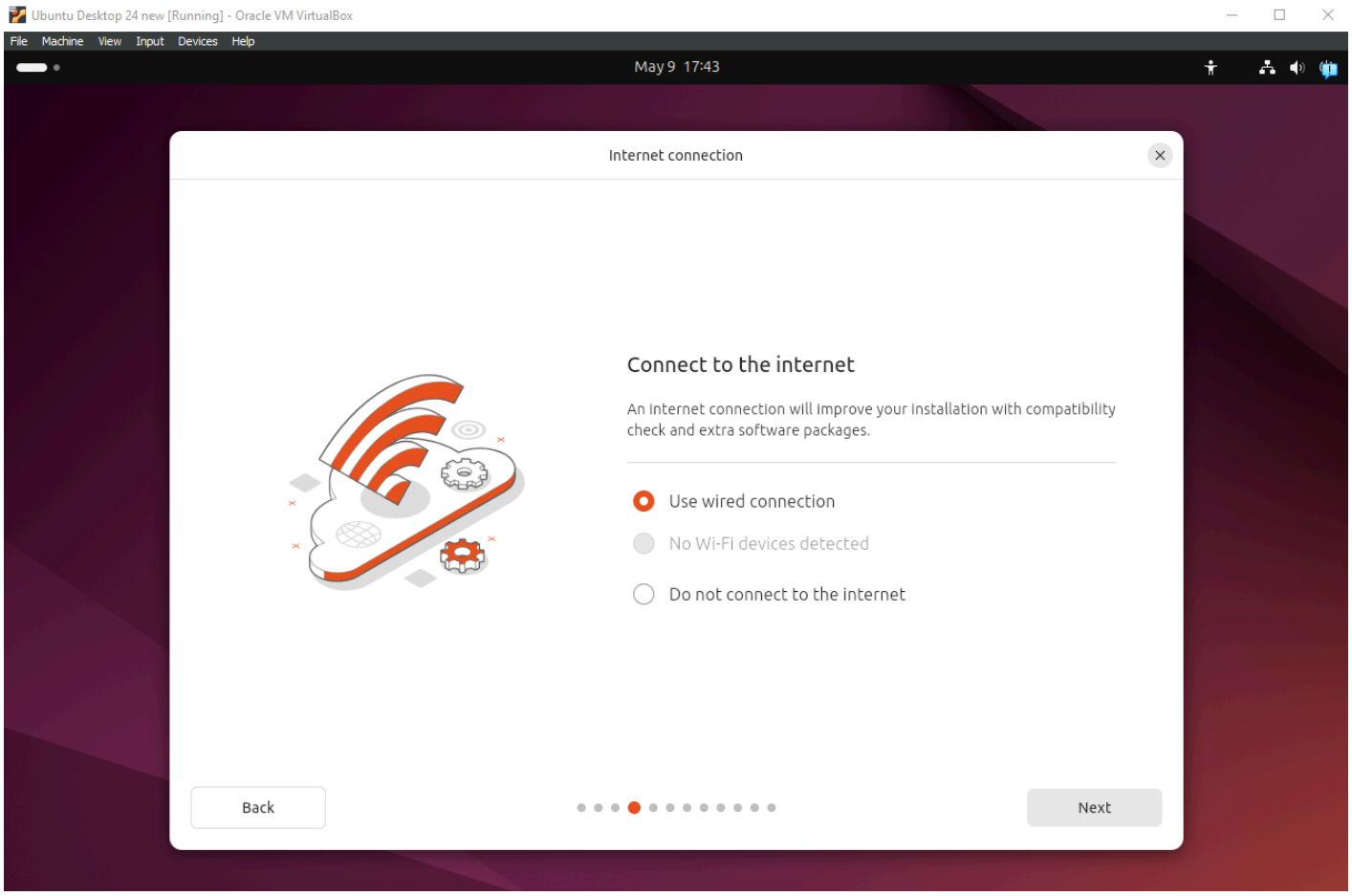


Figure 9 – Internet Connection Screen

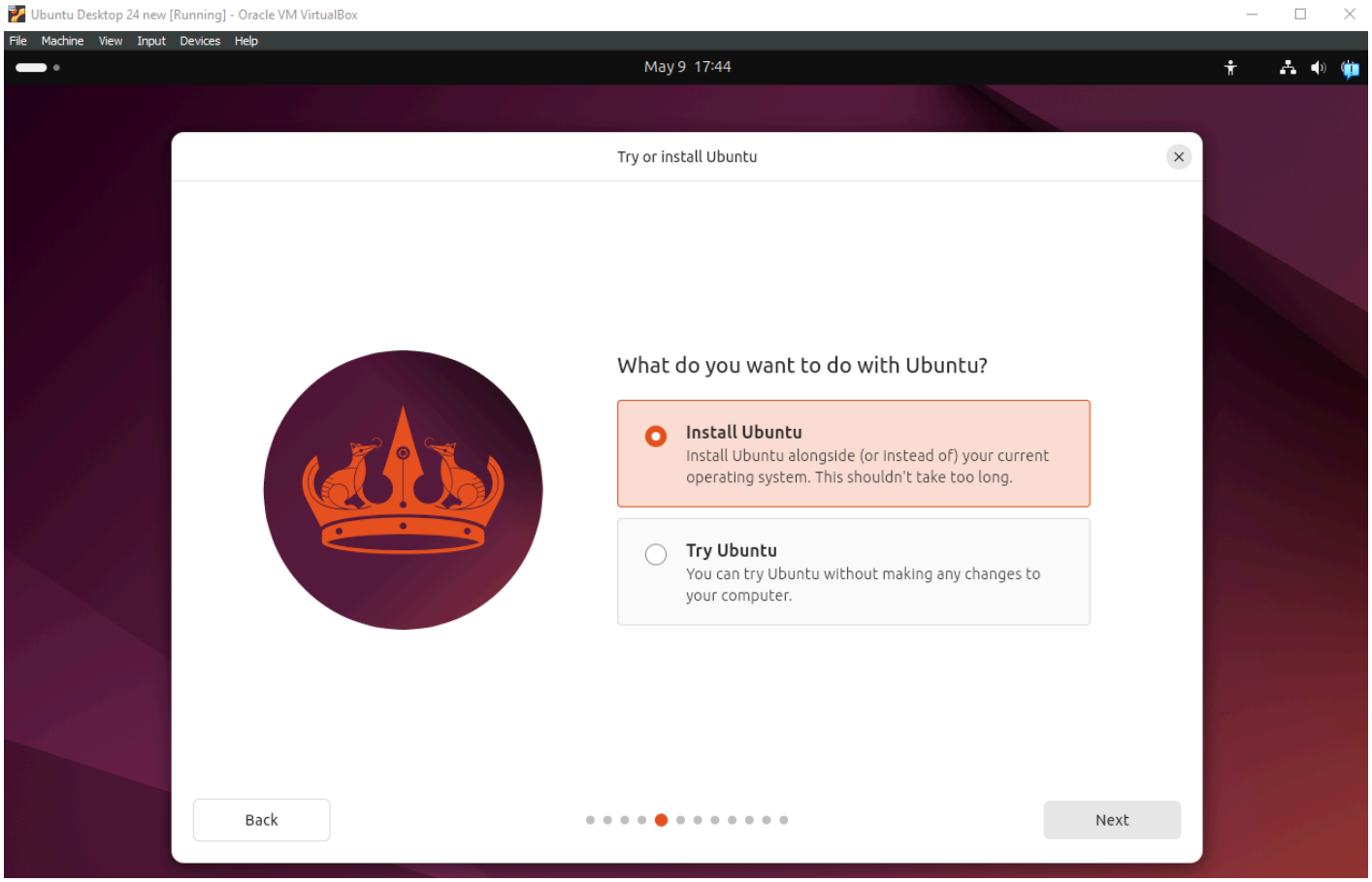


Figure 10 – Try or Install Ubuntu Screen

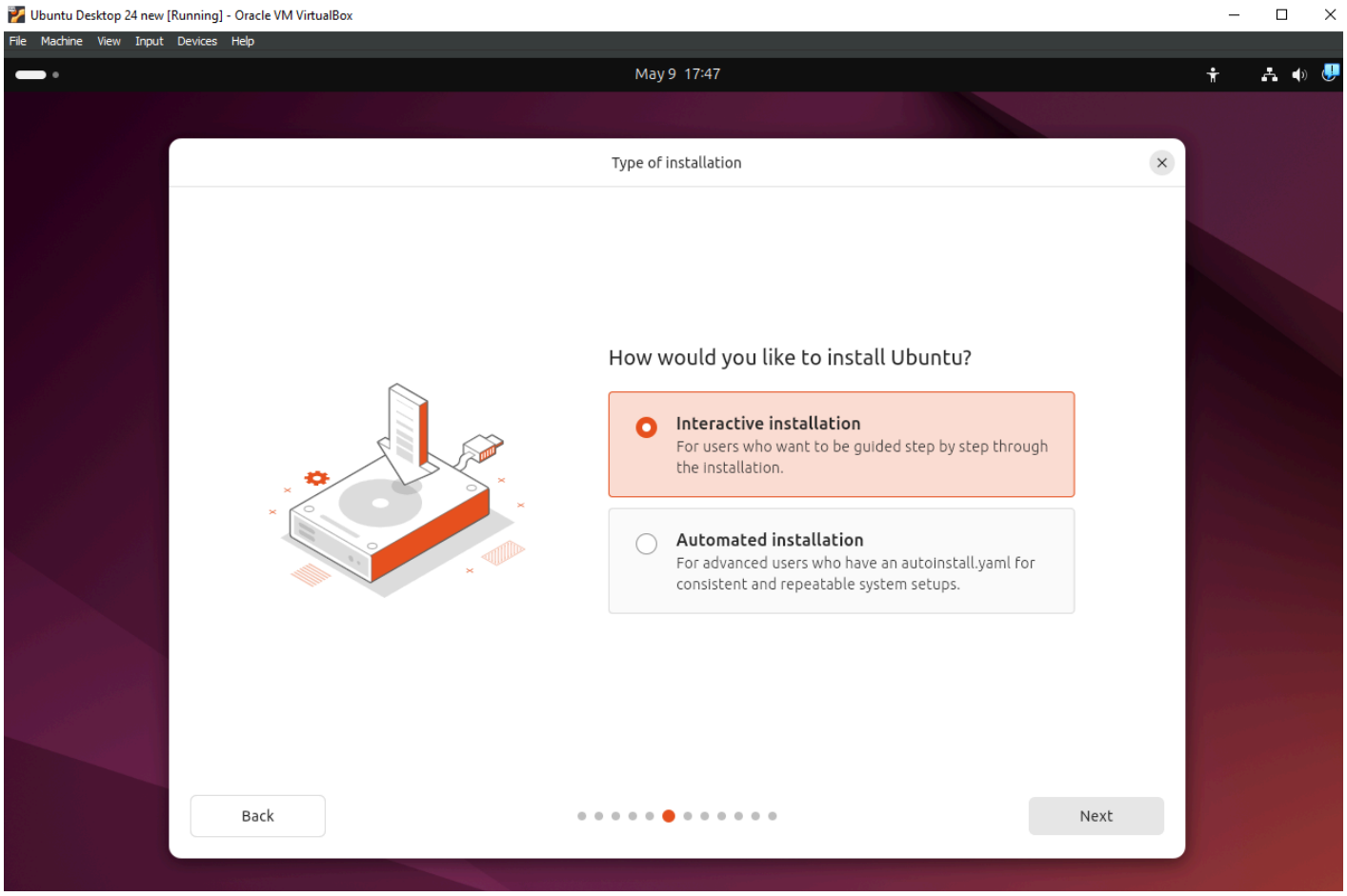


Figure 11 – Type of Installation Screen

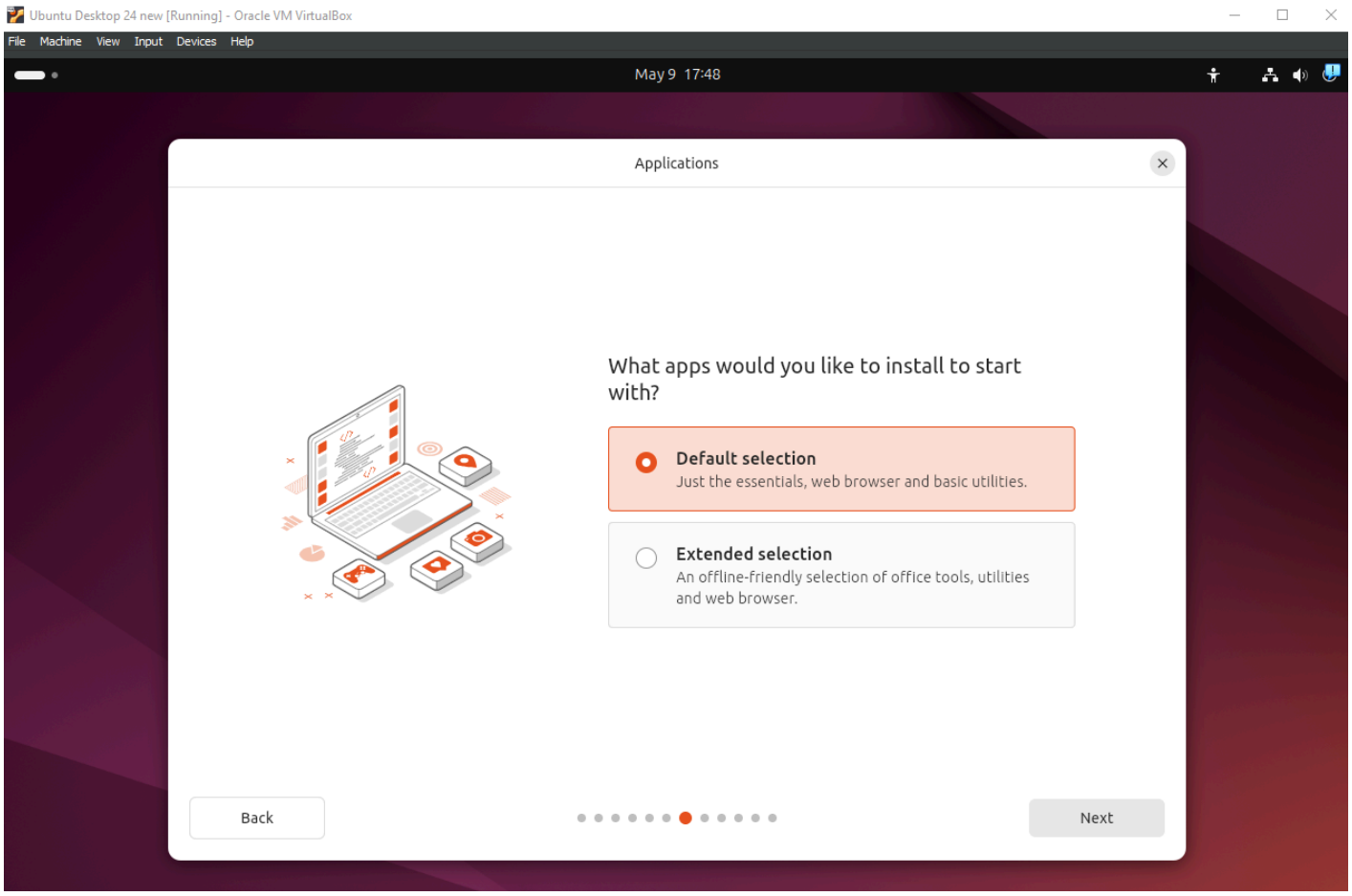


Figure 12 – Applications Screen

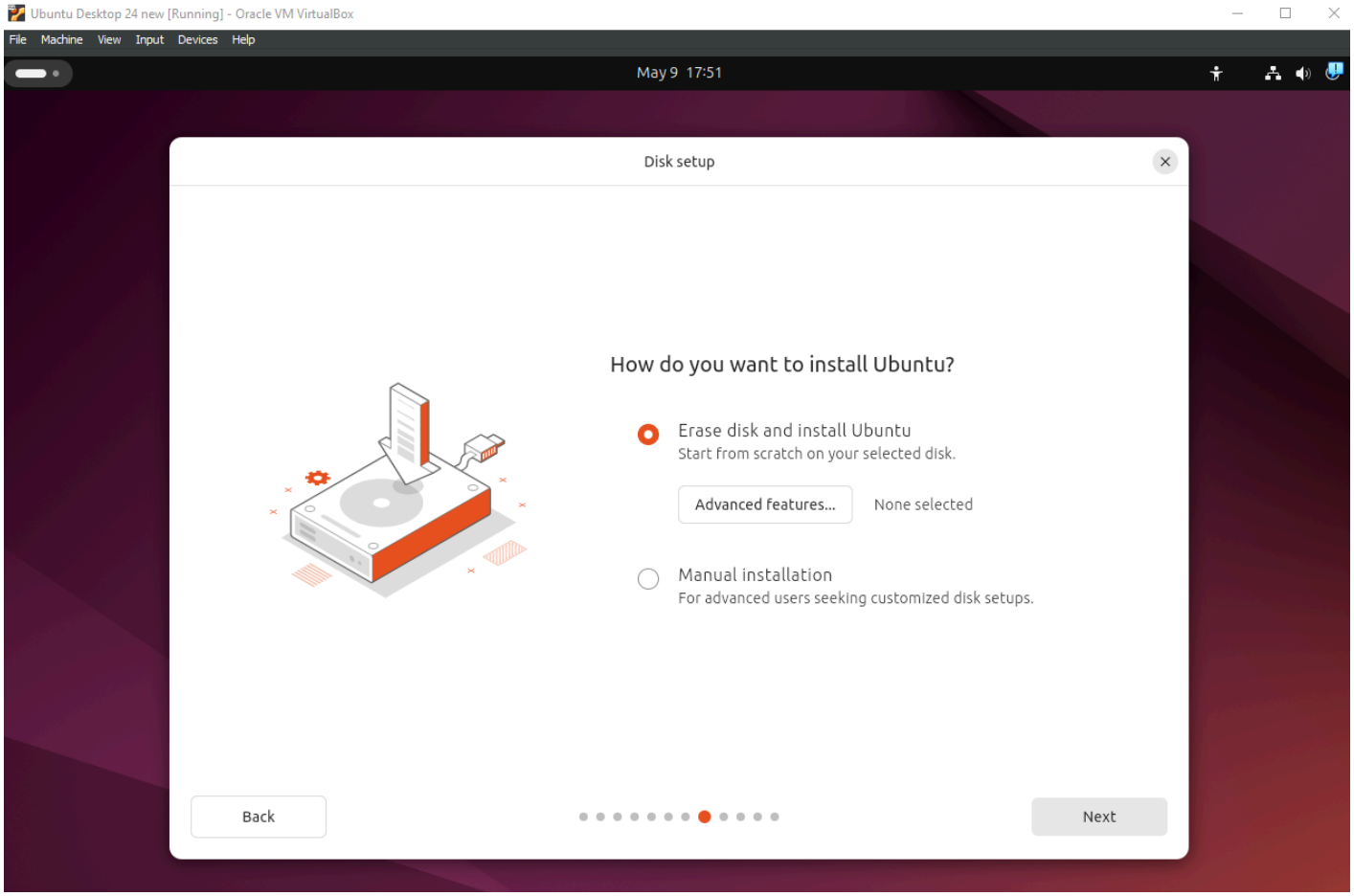


Figure 13 – Disk Setup Screen

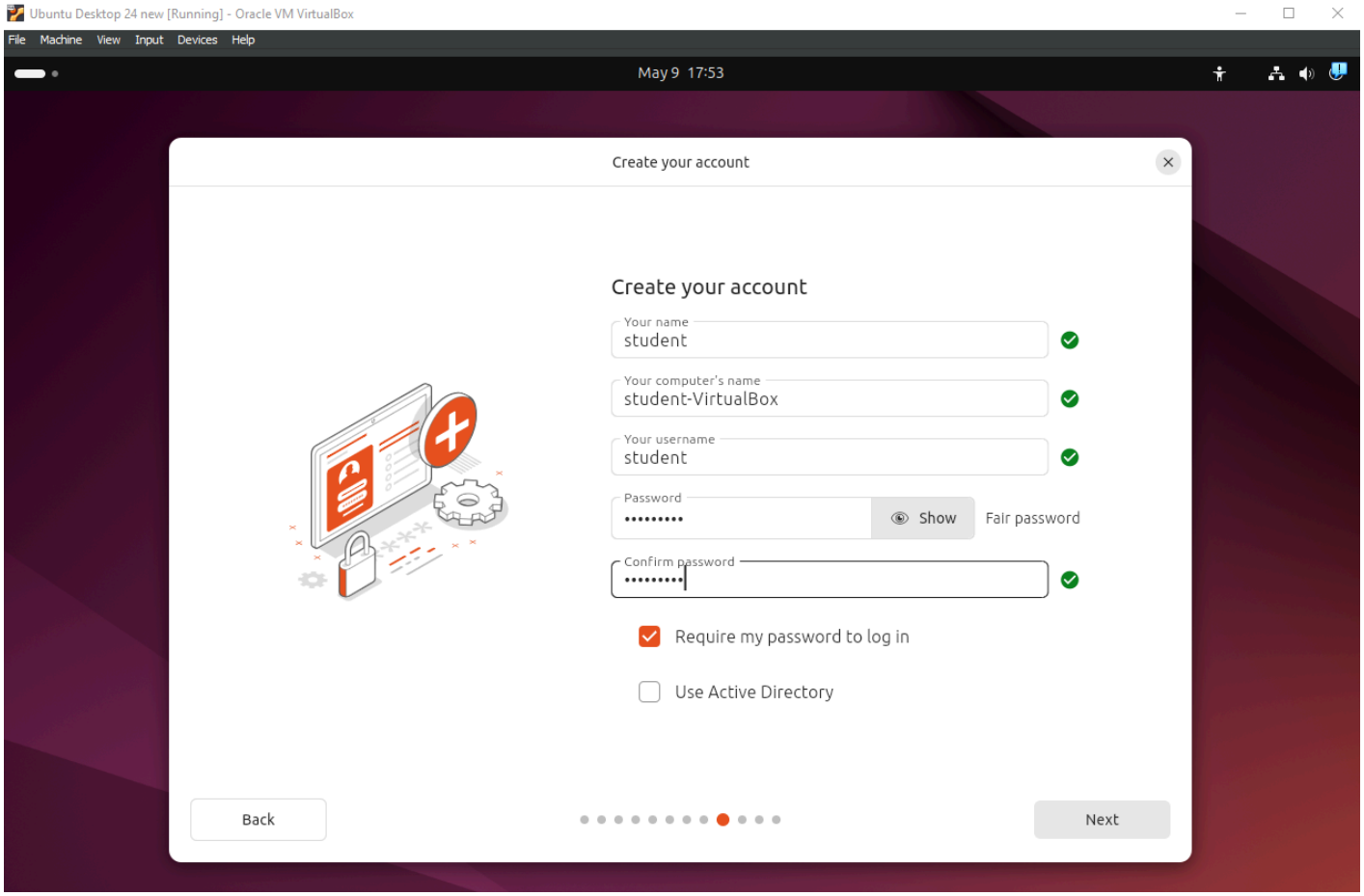


Figure 14 – Create Account Screen

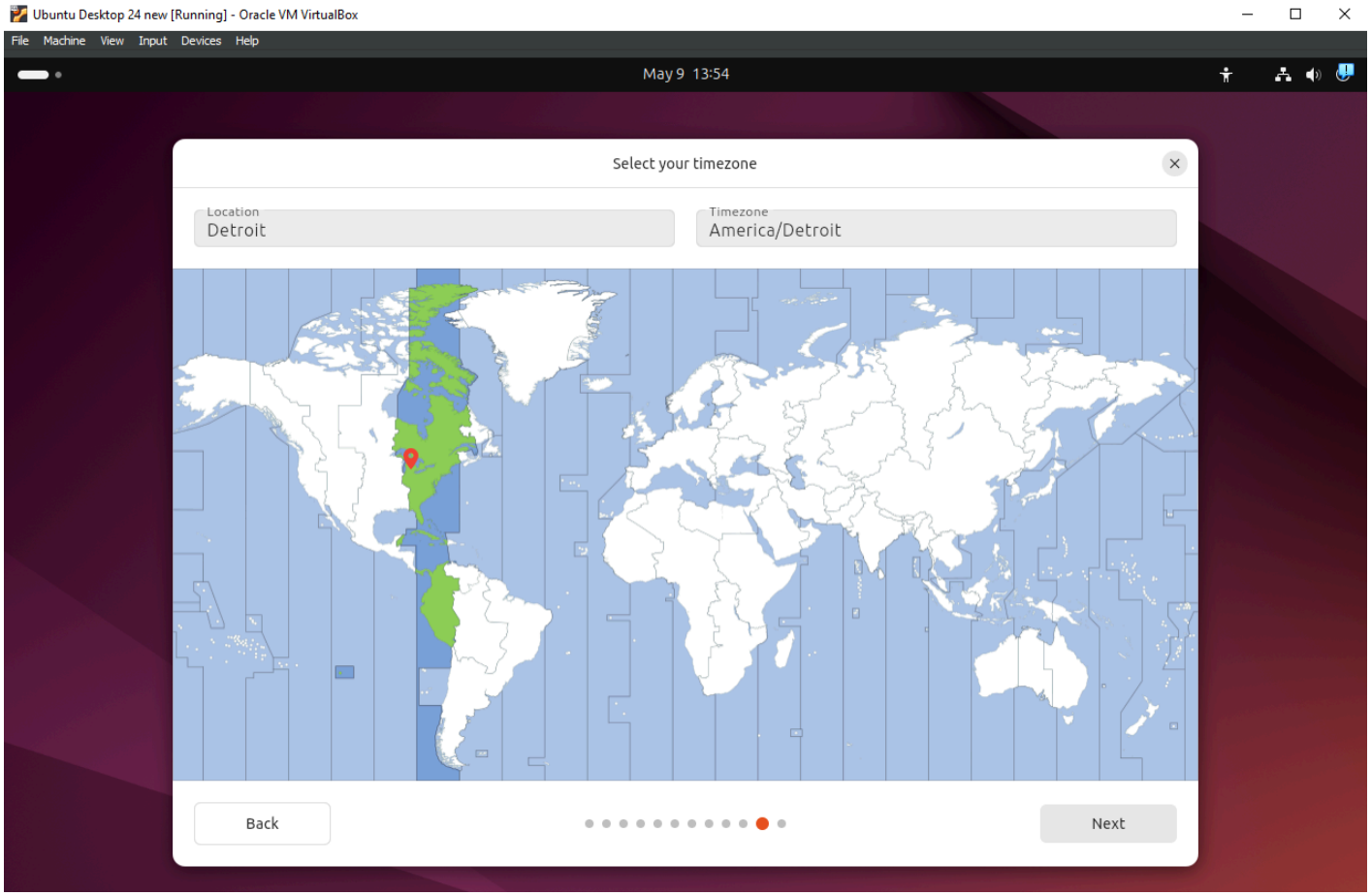


Figure 15 – Select Timezone Screen

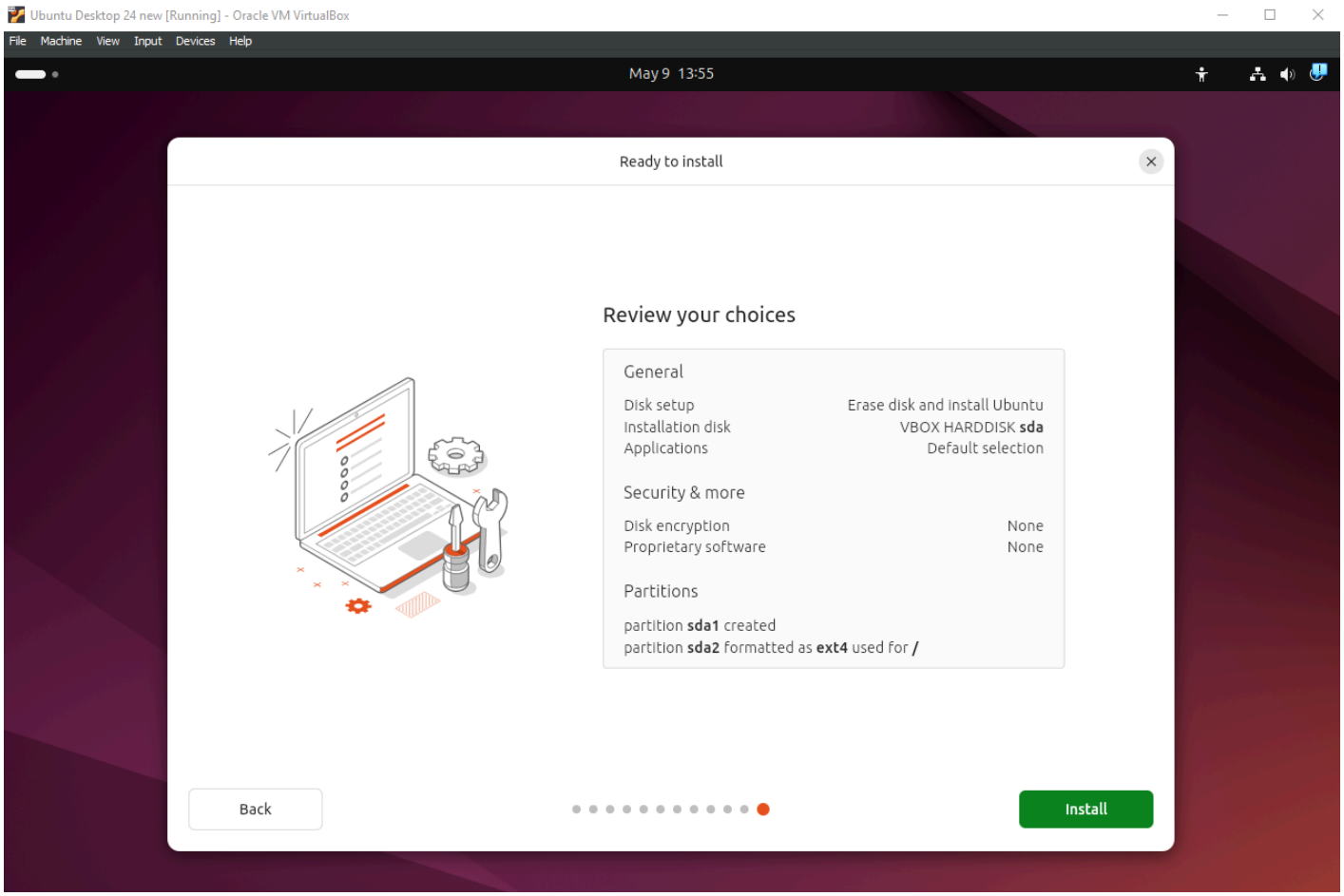


Figure 16 – Ready to Install Screen

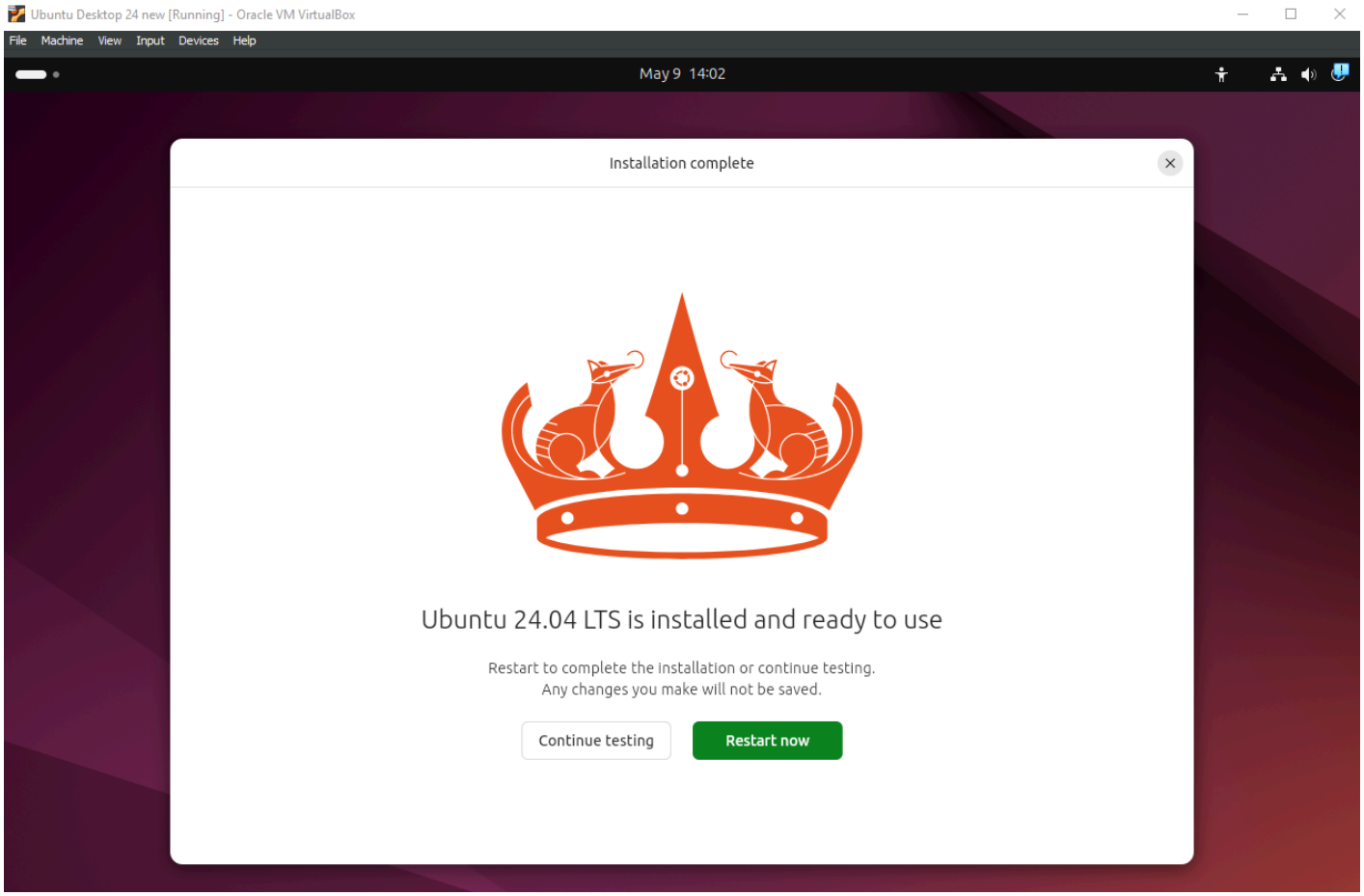


Figure 17 – Installation Complete Screen

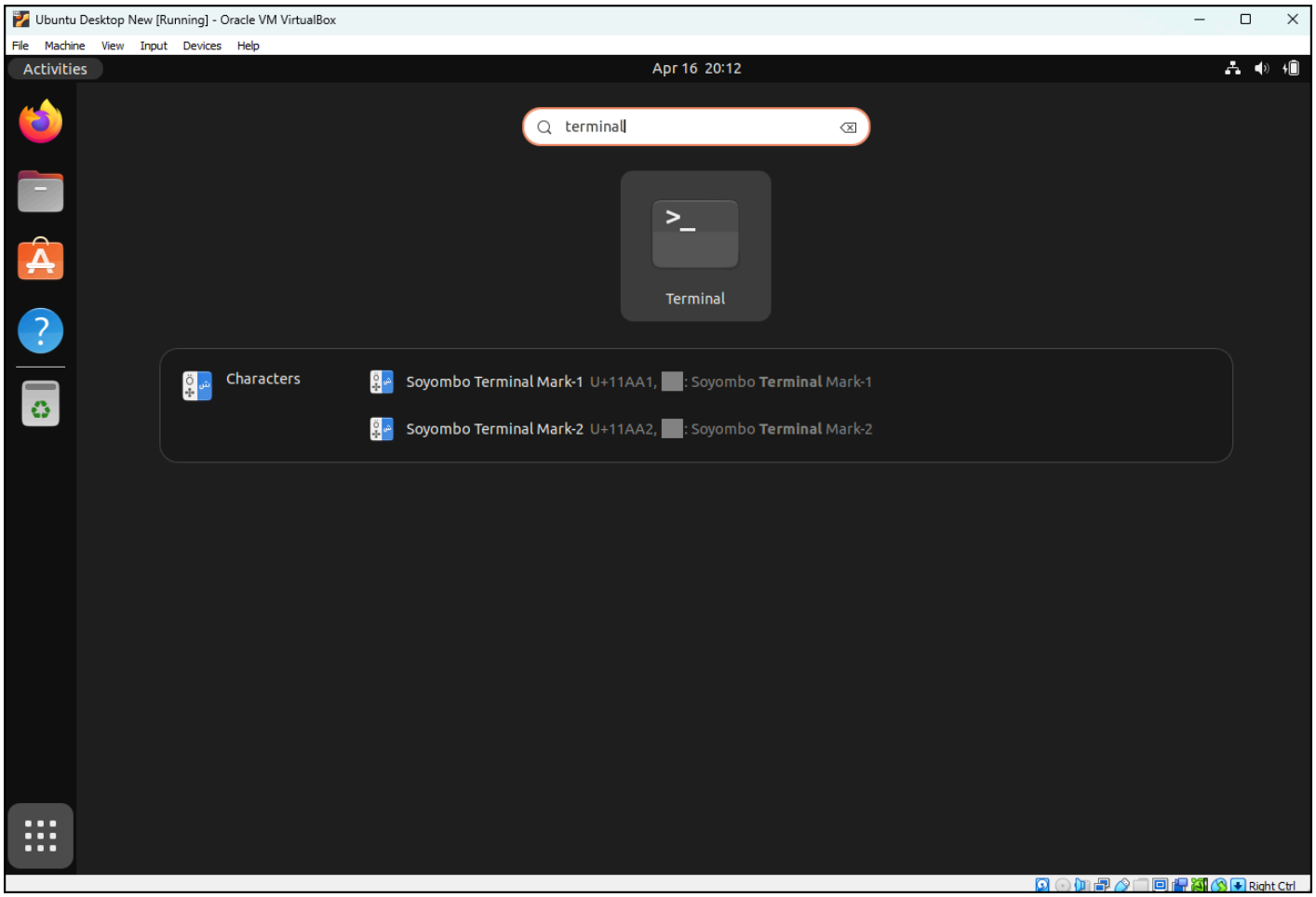


Figure 18 – Find the terminal

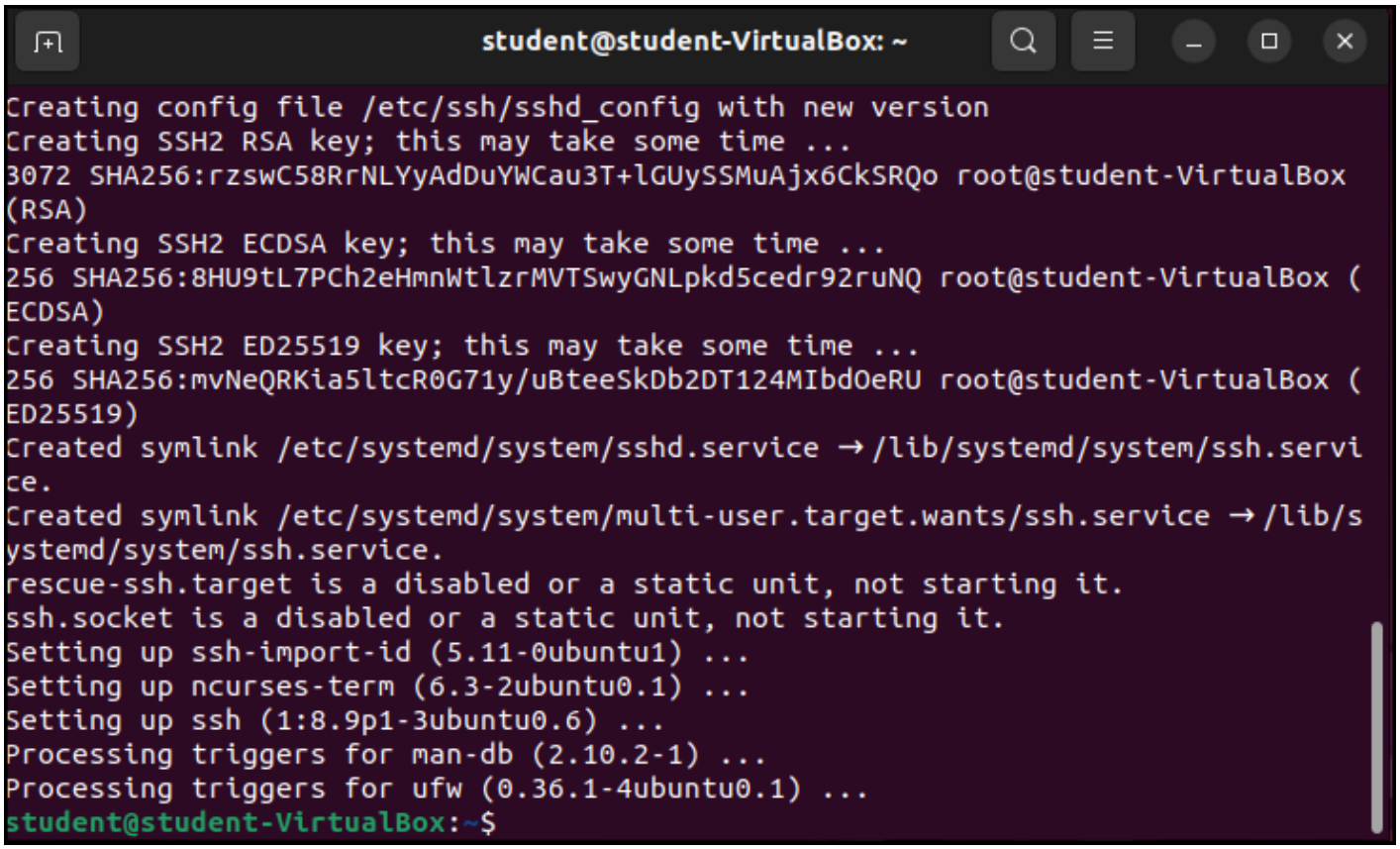


Figure 19 – Install SSH

CHAPTER 12

Create a Kali Linux VM

DANTE ROCCA

Kali Linux is the distribution of choice for attacking a network thanks to the many attack tools it comes bundled with. This lab provides instructions for making a Kali Linux VM.

LEARNING OBJECTIVES

- Successfully download, install, and run Kali Linux in a GNS3 environment

PREREQUISITES

- Chapter 2 – Setting Up a GNS3 Environment

DELIVERABLES

- None – this is a preparatory lab that supports other labs in this book

RESOURCES

- Download Kali Linux
- Download Nessus Essentials for Education

CONTRIBUTORS AND TESTERS

- Mathew J. Heath Van Horn, PhD, ERAU-Prescott

Phase I – Download and Installation

We are going to download and install the Kali Linux VM. We are going to use the .iso image and not the prebuilt VM. Generally, the pre-made VM works fine, but a few testers had problems. When we used the .iso the configuration and compatibility problems resolved themselves.

1. Start by downloading the recommended image file here

> **IMPORTANT:** Make sure you download the Installer Image and not the Virtual Machine image.

2. Select the 64-bit installer image and click the download method you prefer
3. Once the image file has been downloaded, open VirtualBox
4. Click on the ***new*** button (Figure 1)
    4.1. Give the new VM a name
    4.2. Select the folder you want to save the VM
    4.3. Select the ISO image you downloaded earlier
    4.4. Select ***next*** (Figure 2)
5. Leave the defaults for the hardware (Figure 3)
6. Use the defaults for the virtual disk space (Figure 4)
7. Verify the settings and click on***finish*** (Figure 5)
8. Start the Kali VM
9. Hit ***enter*** over the graphical install (Figure 6)
10. Select your language and hit ***continue*** (Figure 7)
11. Select your region and hit ***continue*** (Figure 8)
12. Select your keyboard layout and click ***continue*** (Figure 9)
13. Leave the hostname as default and click ***continue*** (Figure 10). Then leave the domain blank and click ***continue*** (Figure 11)
14. Give the full name as ***student*** and click ***continue*** (Figure 12)
15. Then leave the account name as ***student*** and click ***continue*** (Figure 13)
16. Like other VMs use the password ***Security1*** and click ***continue*** (Figure 14)
17. Select your time zone and click***continue*** (Figure 15)

18. Partition Disk

    18.1. Select option ***guided – use entire disk*** and press ***continue*** (Figure 16)

    18.2. Leave the disk partition as default and click ***continue*** (Figure 17)

    18.3. Select – ***All files in one partition*** and click ***continue*** (Figure 18)

    18.4. Verify your partition information and click ***continue*** (Figure 19)

19. Once the software selection screen pops up, leave the defaults and click ***continue*** (Figure 20)

20. Once the install GRUB boot loader screen pops up, leave the default yes radio button and click ***continue*** (Figure 21)

21. On the next screen select the device, there should be only one, and click **continue** (Figure 22)

22. Once this is done, click ***continue*** one last time

23. Finish the installation by clicking ***continue*** (Figure 23)

24. Once the login screen pops up, login to make sure everything works

Phase II – Necessary Software

While Kali comes with a large toolset, there are two tools we will need later that don't come preinstalled.

1. Open the terminal and run this command to install rainbow crack

```
sudo apt-get install rainbowcrack
```

2. Once the install completes, close the terminal and open Firefox

3. In Firefox, go to this link to download Nessus Essentials for Education. Click on ***try now*** (Figure 24). You will need to provide a business email but none of our testers has reported spam from this

4. Click the ***download*** button that appears. Then leave the defaults on the next screen and click download. At the time of writing the version of Nessus is 10.7.1

5. Open the folder where you downloaded the file. Right-click inside the folder and click open terminal here (Figure 25)

6. Use the following command to install the Nessus Package

```
sudo dpkg -i Nessus-10.7.1-ubuntu1404_amd64.deb
```

7. Use the following command to start the Nessus Scanner. While we won't do much with it right now, we will need to input the activation code from our email

```
/bin/systemctl start nessusd.service
```

8. In the window that pops up enter the user password. Following that, reopen Firefox and go to this link

```
https://kali:8834
```

9. The page will tell you that it is insecure. Click ***advanced*** and then ***Accept the risk and continue*** (Figure 26)

10. Click ***continue*** on the first screen (Figure 27)

11. Select the ***Register for Nessus Essentials*** radio button (Figure 28) and click ***continue***. If you already got the email earlier, then click ***skip*** (Figure 29)

12. Input the activation code from your email and click***continue*** (Figure 30)

13. Make a username and password for your account (Figure 31) and select submit

Figure 32 – This could take a while

14. Nessus will take a while to download and compile plugins so wait for this process to complete before switching the machine off

End of Lab

Figures for Printed Version

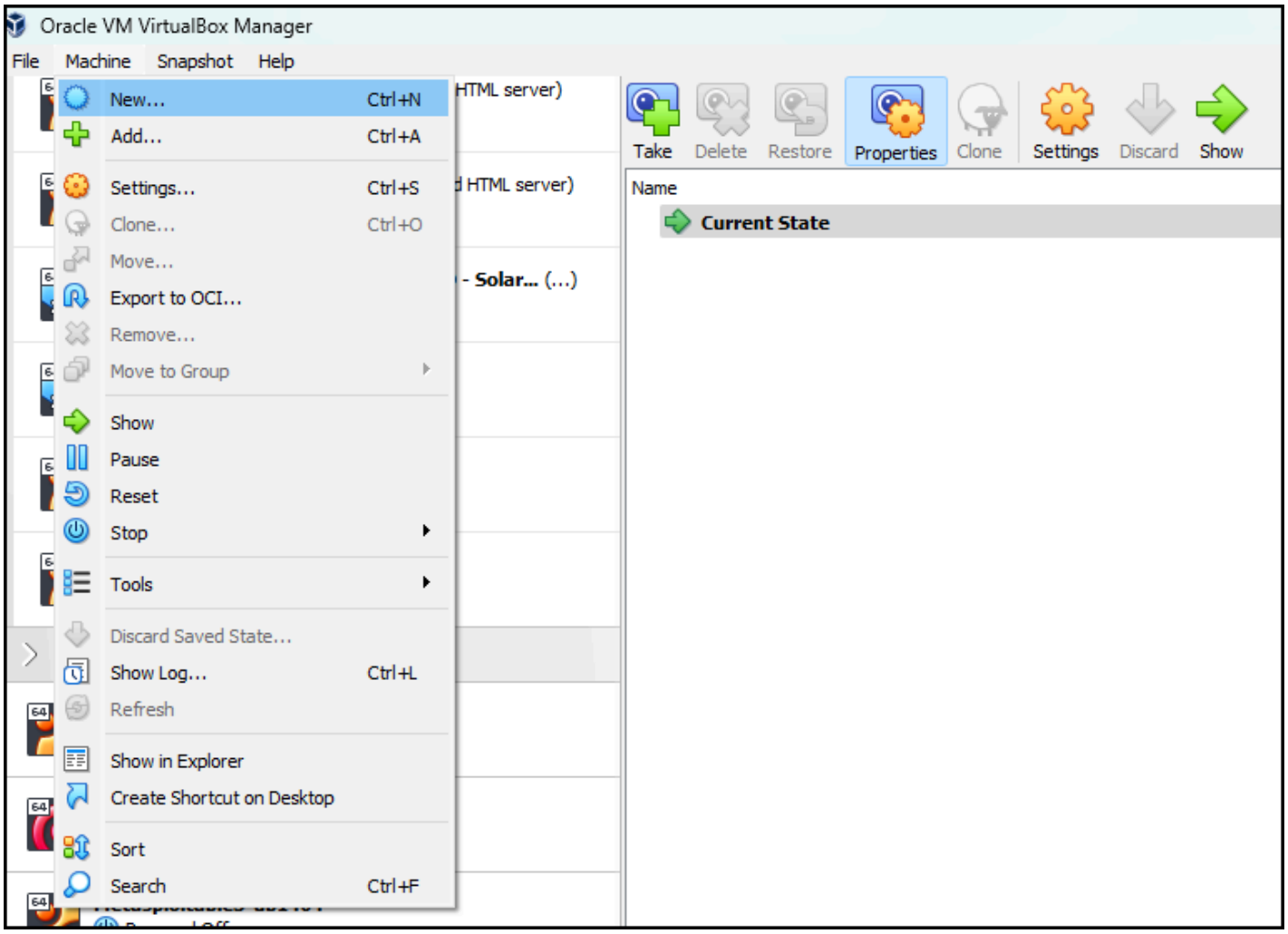


Figure 1 – Create a new VM

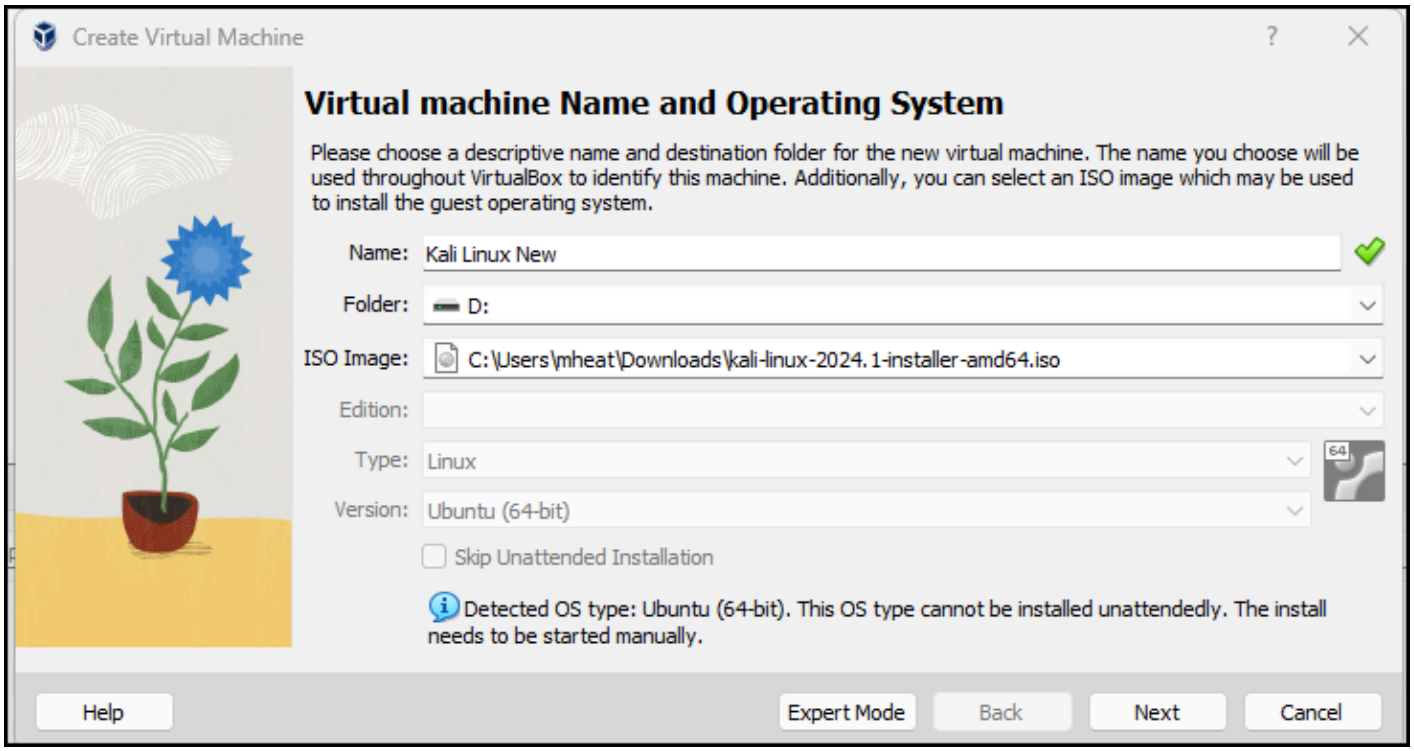


Figure 2 – Create a new Kali VM

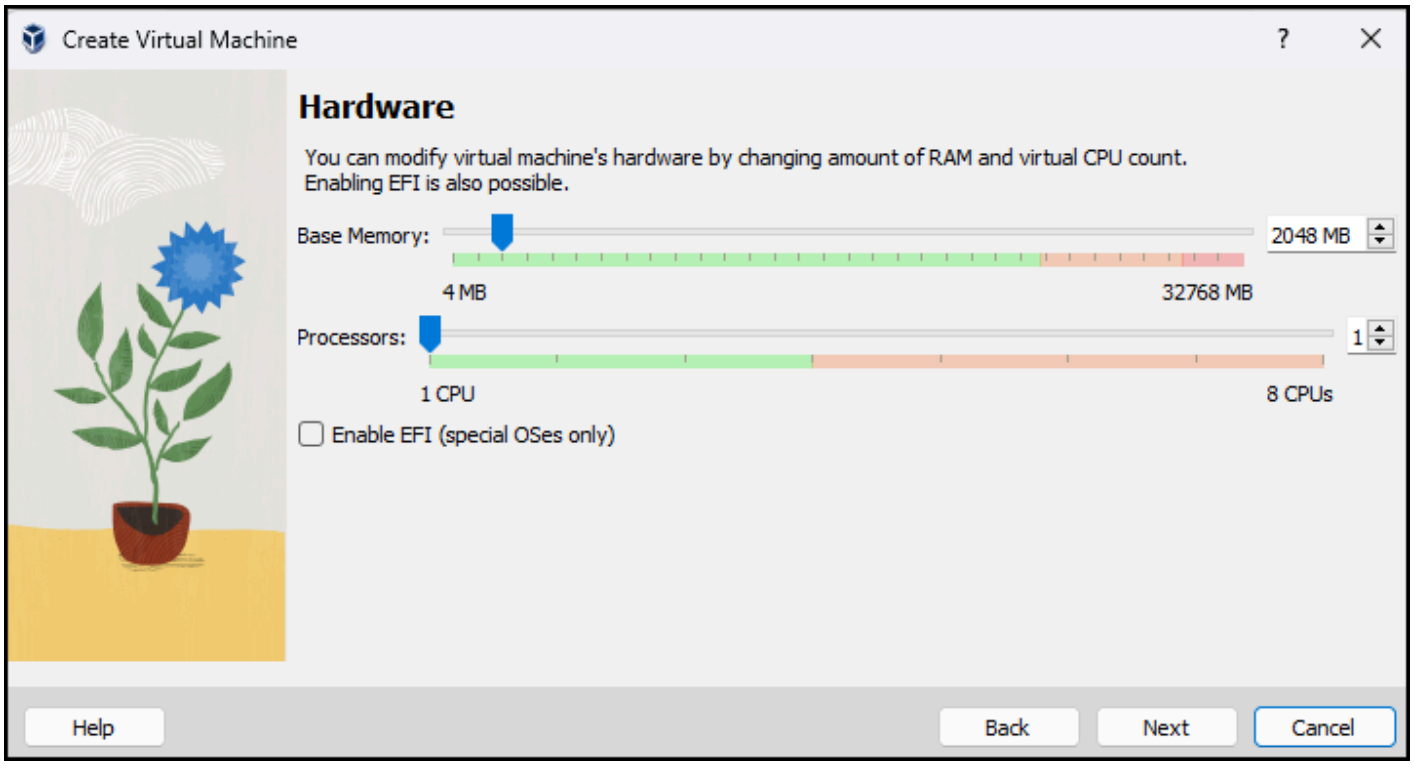


Figure 3 – Set resources for Kali VM

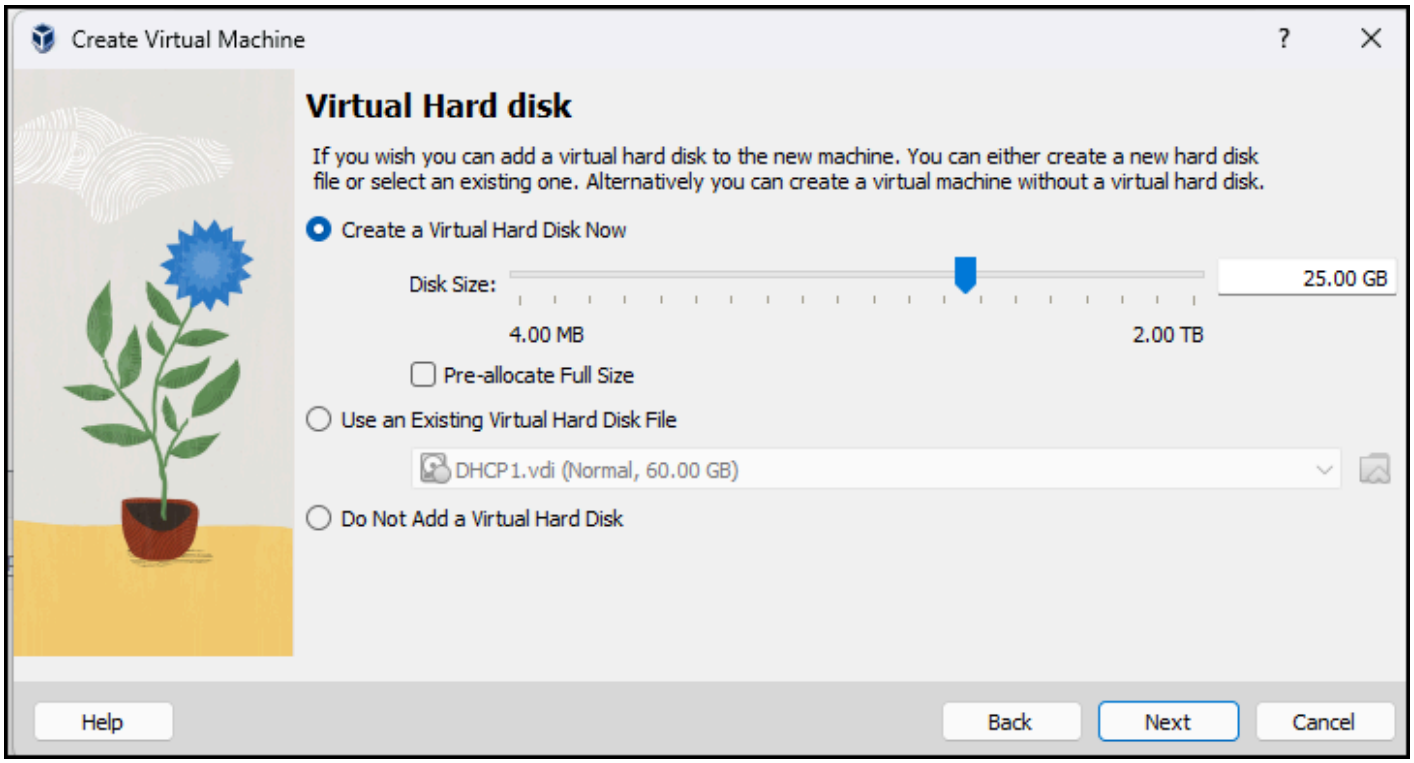


Figure 4 – Set disk space for Kali VM

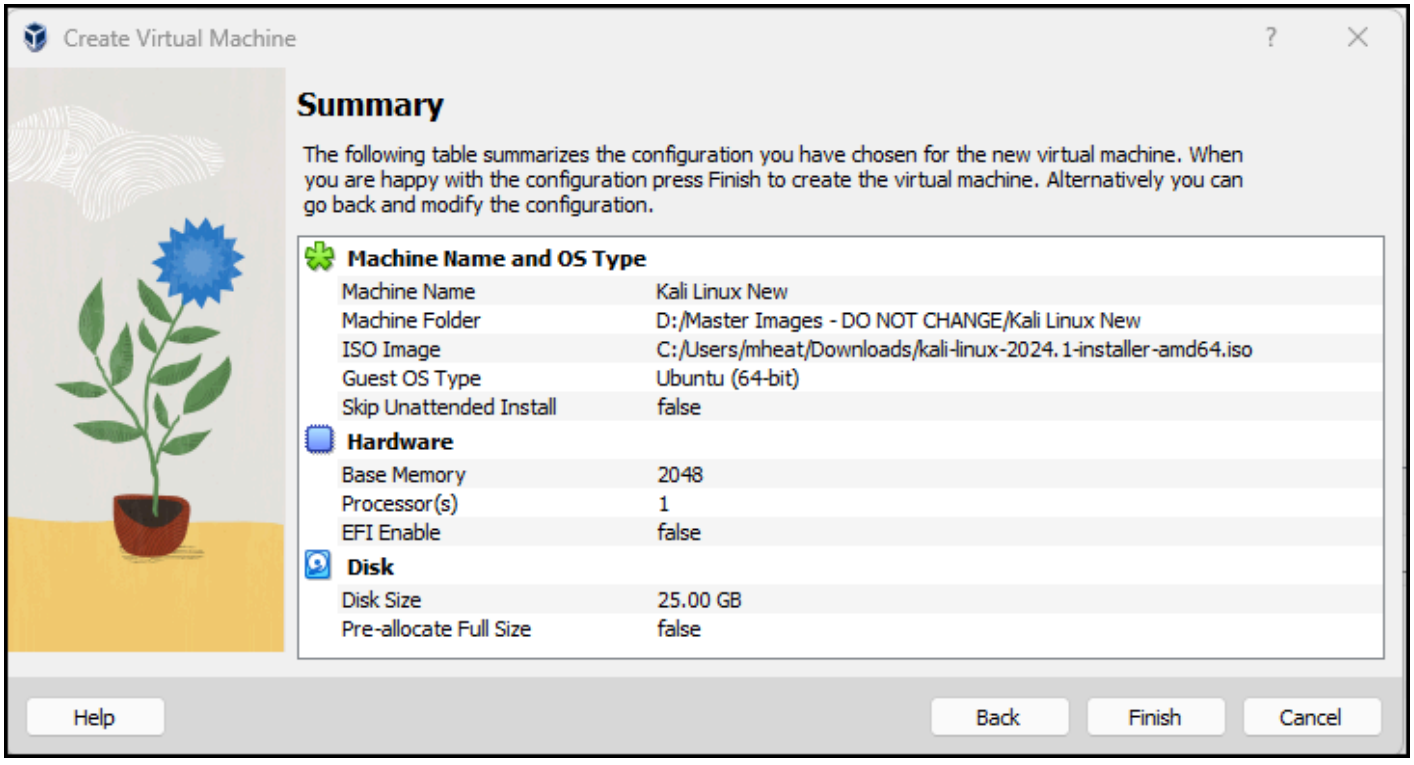


Figure 5 – Verify settings for new Kali VM

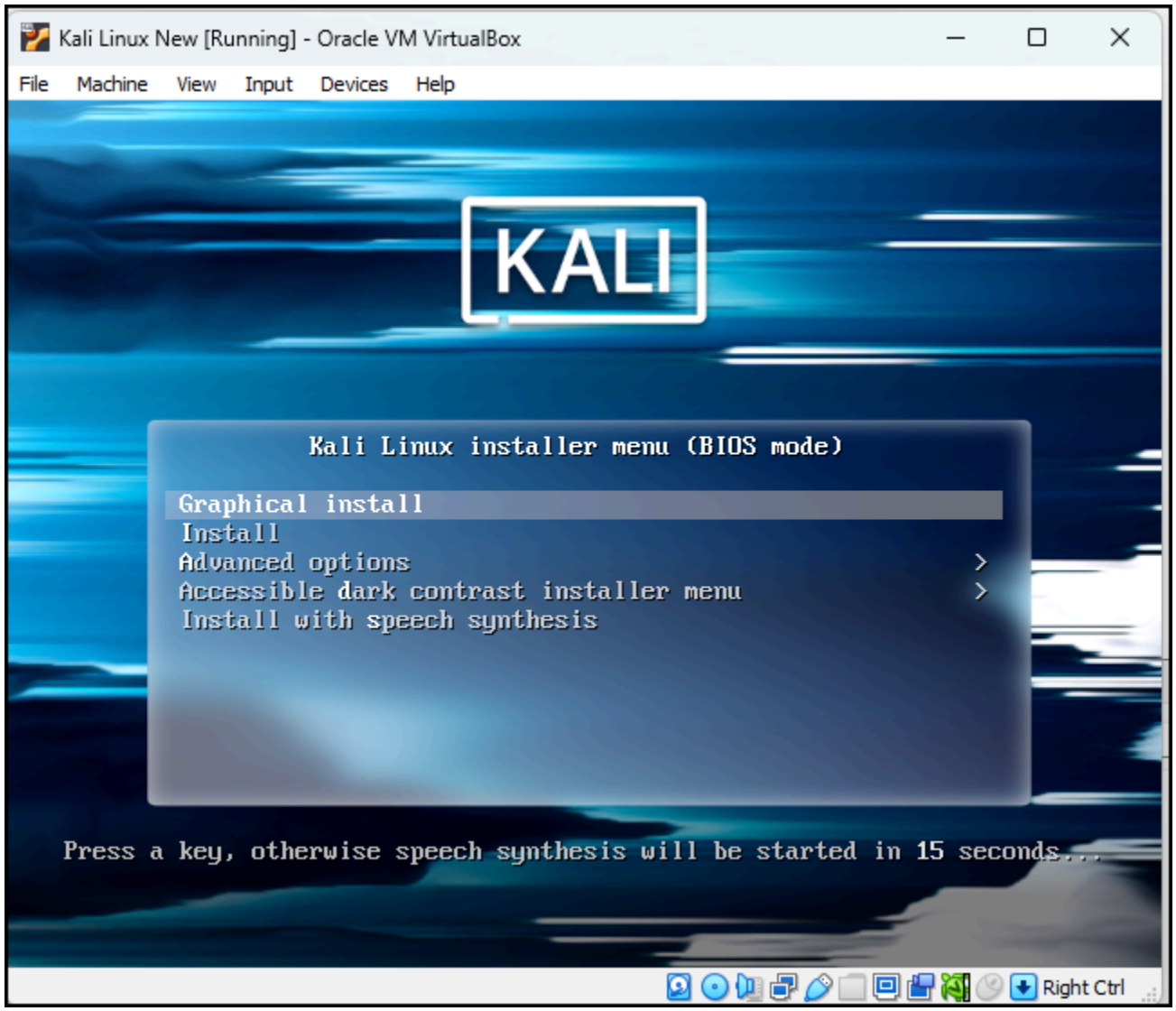


Figure 6 – Start Kali VM

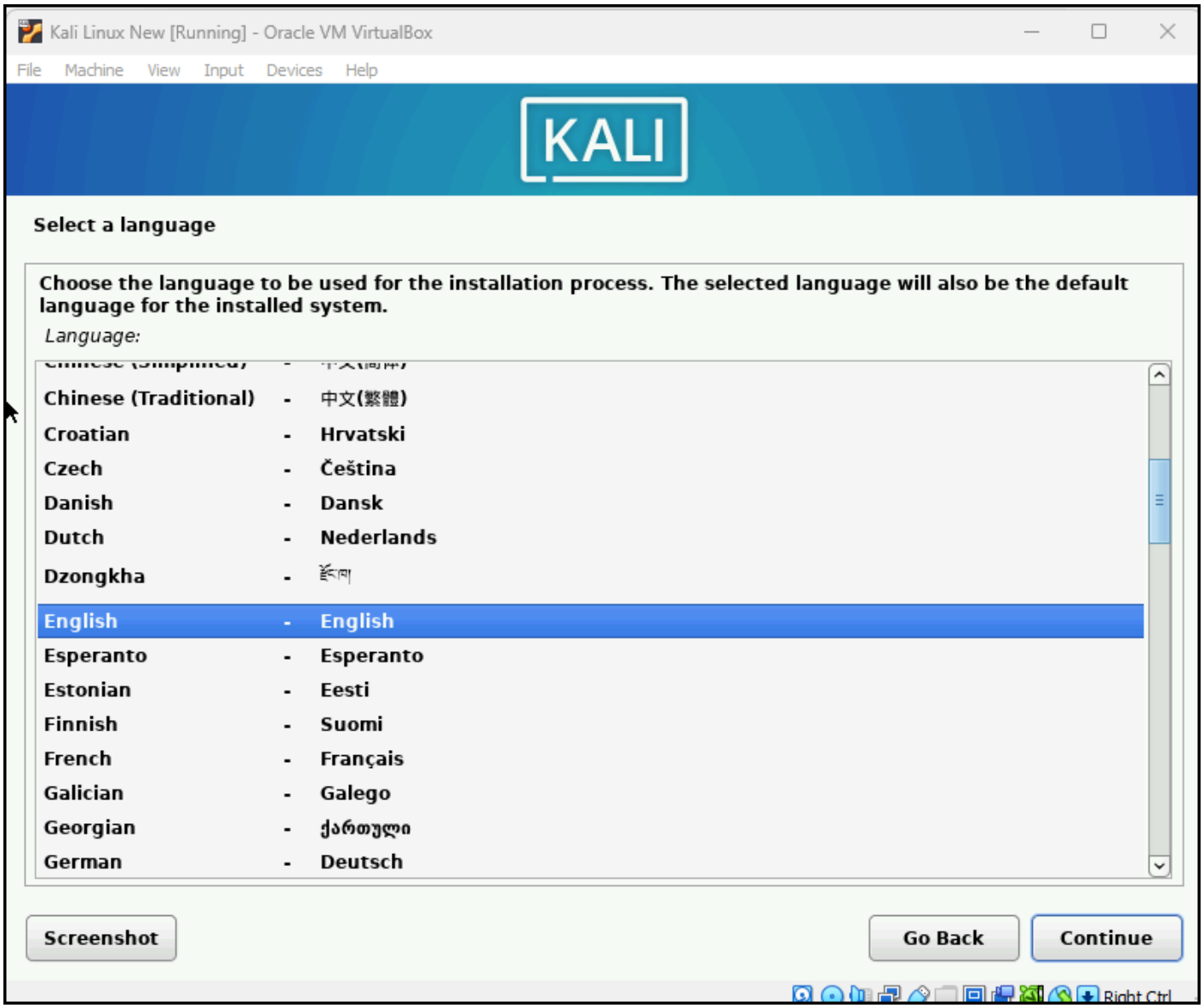


Figure 7 – Set language

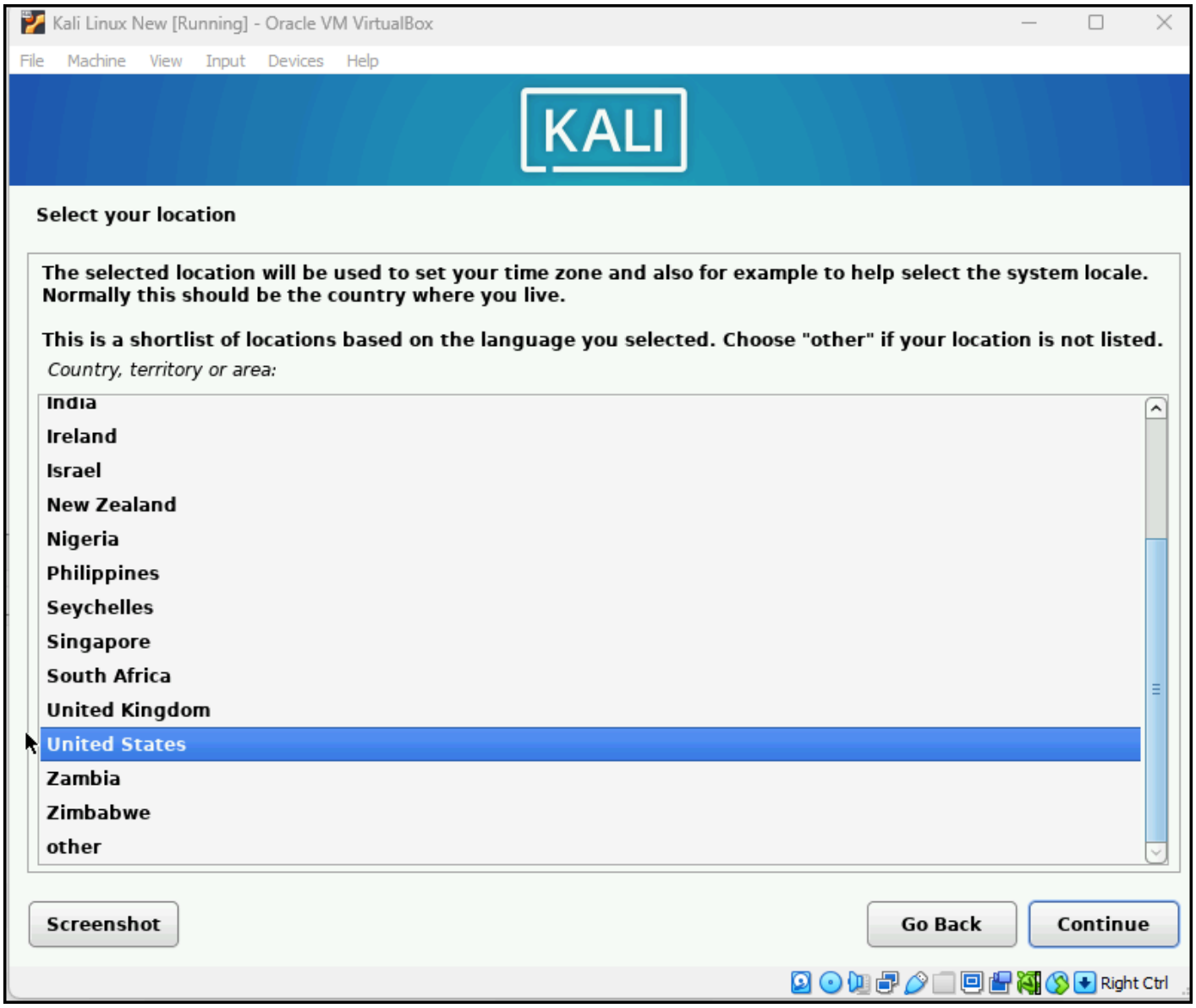


Figure 8 – Set region

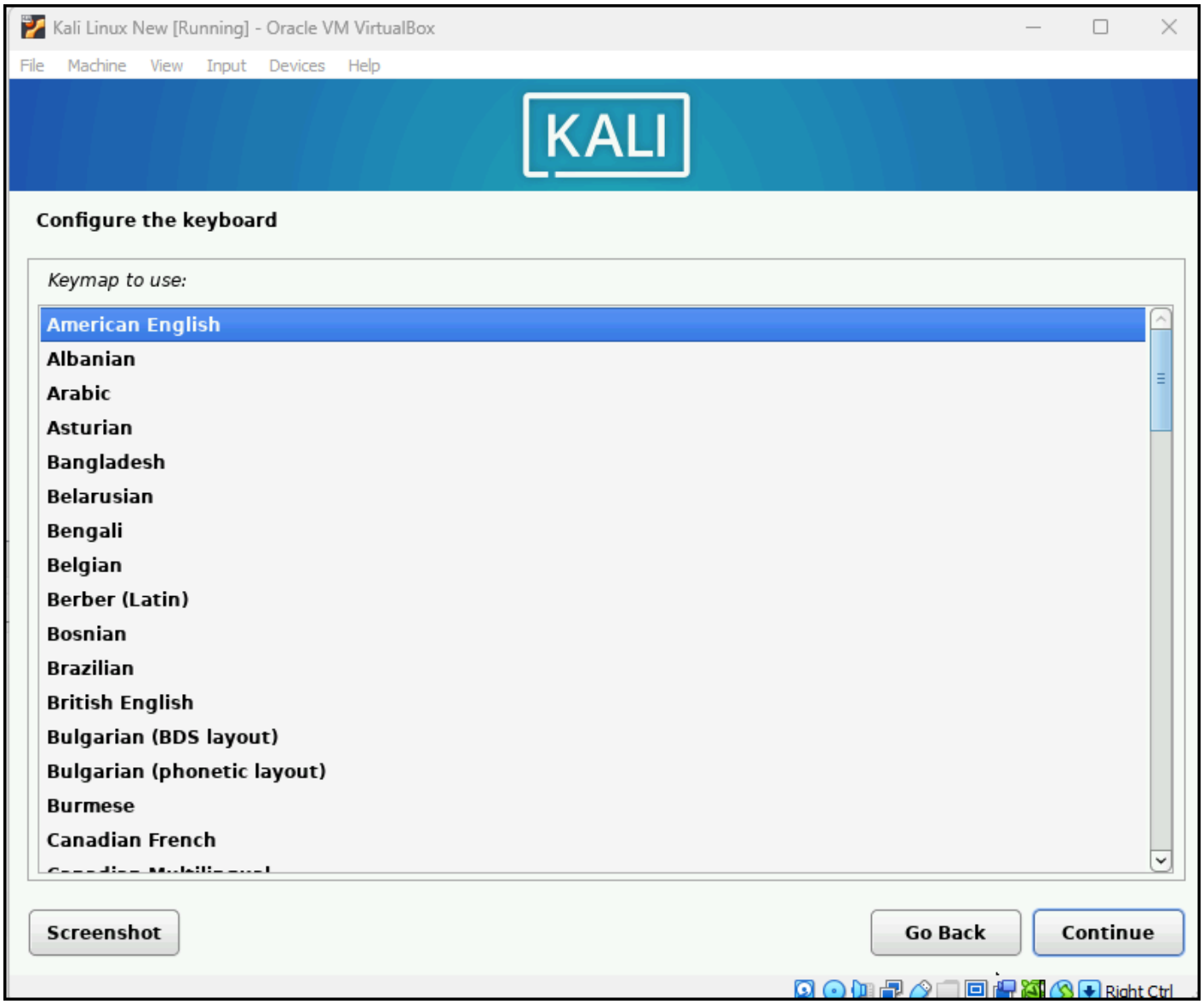


Figure 9 – Set keyboard layout

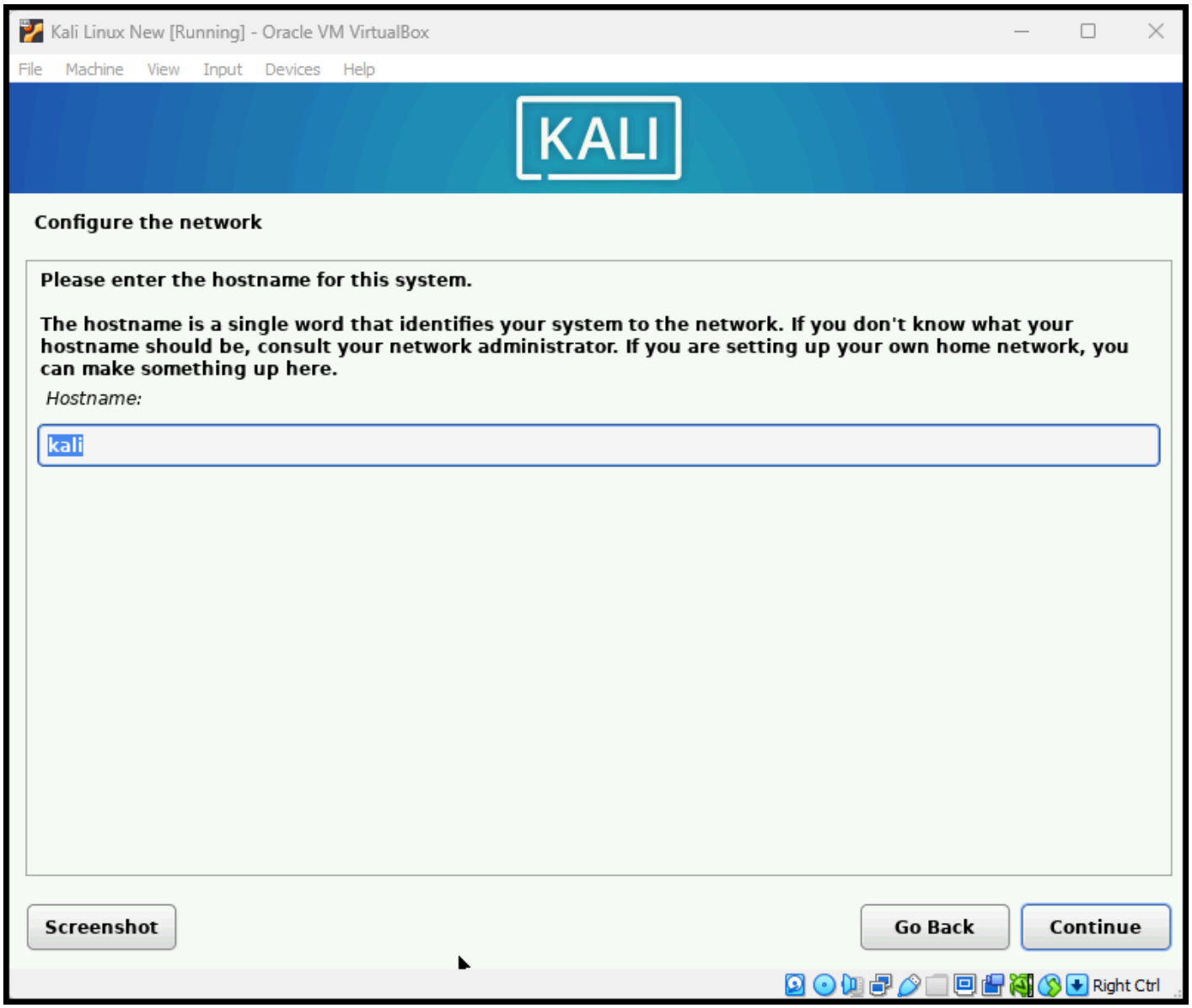


Figure 10 – Set the host name as default

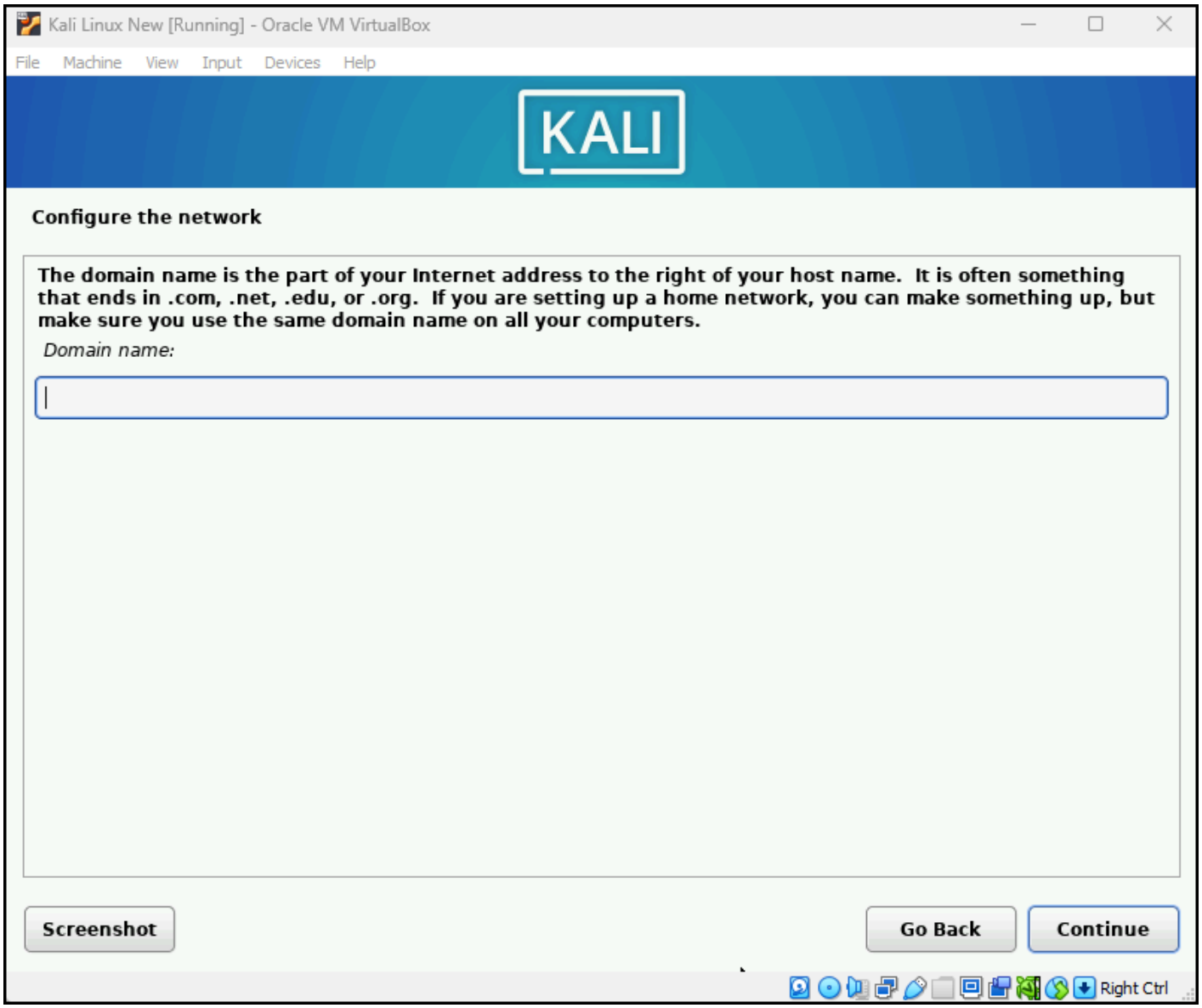


Figure 11 – Leave domain blank

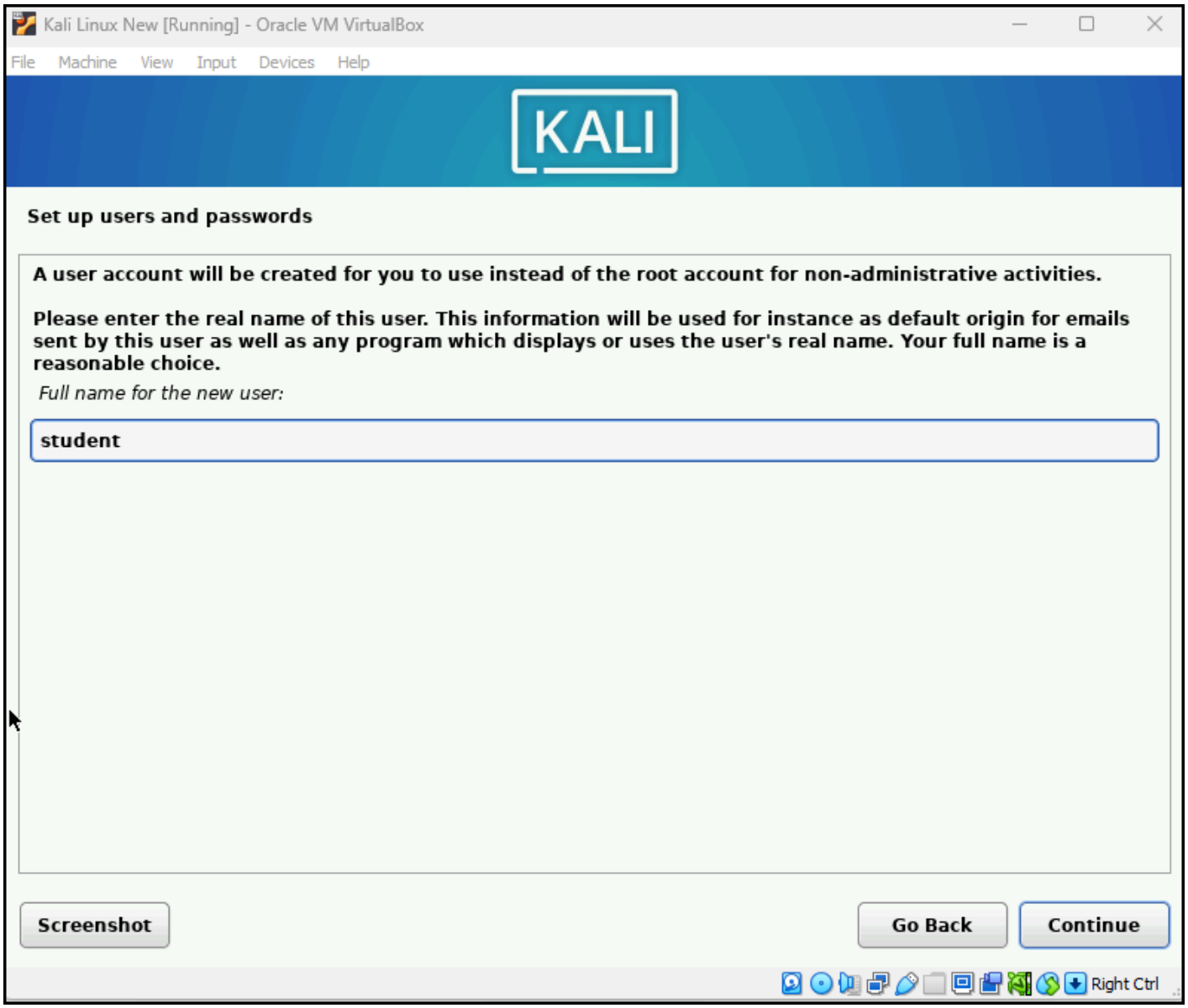


Figure 12 – Set username to student

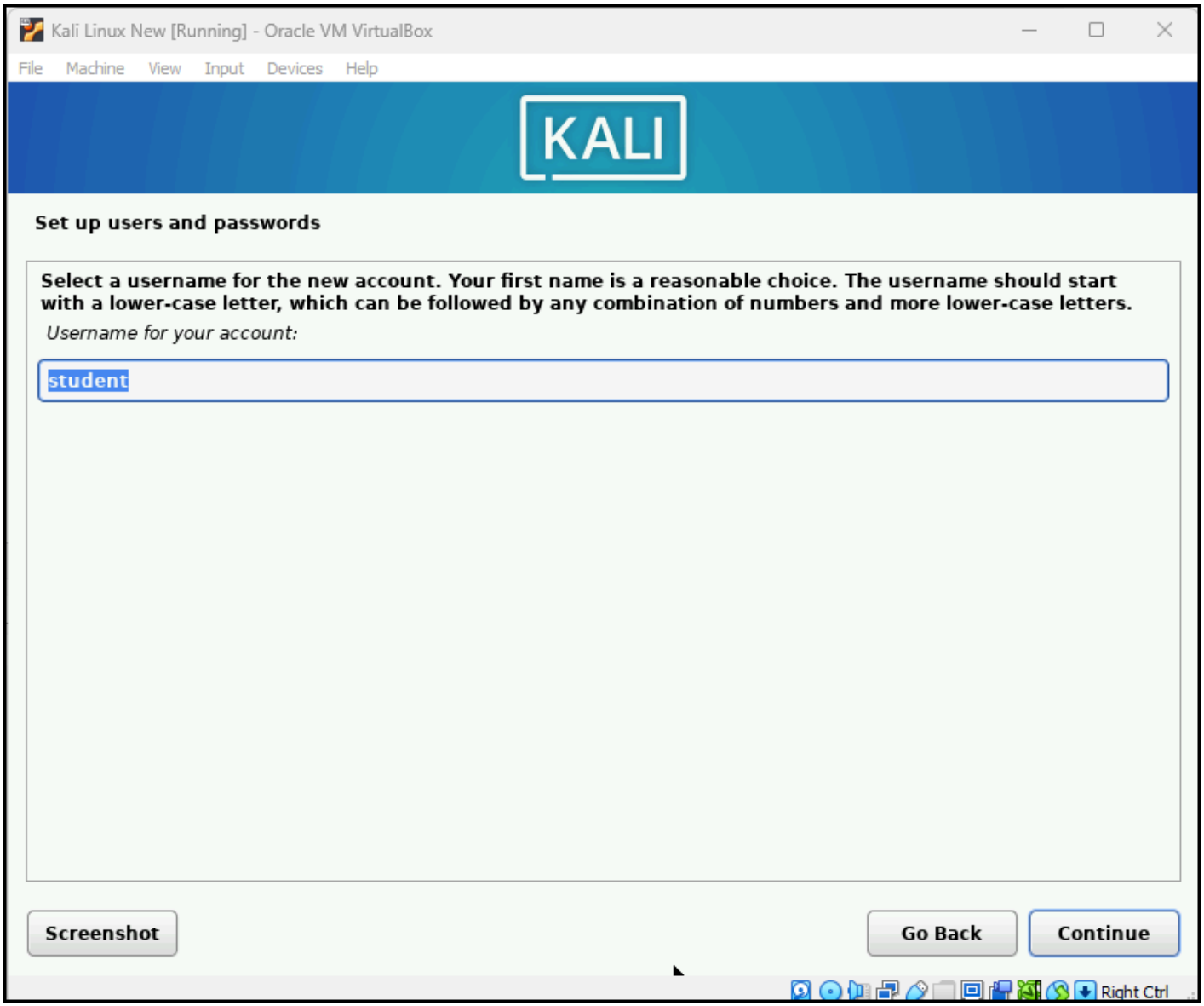


Figure 13 – Set account name to student

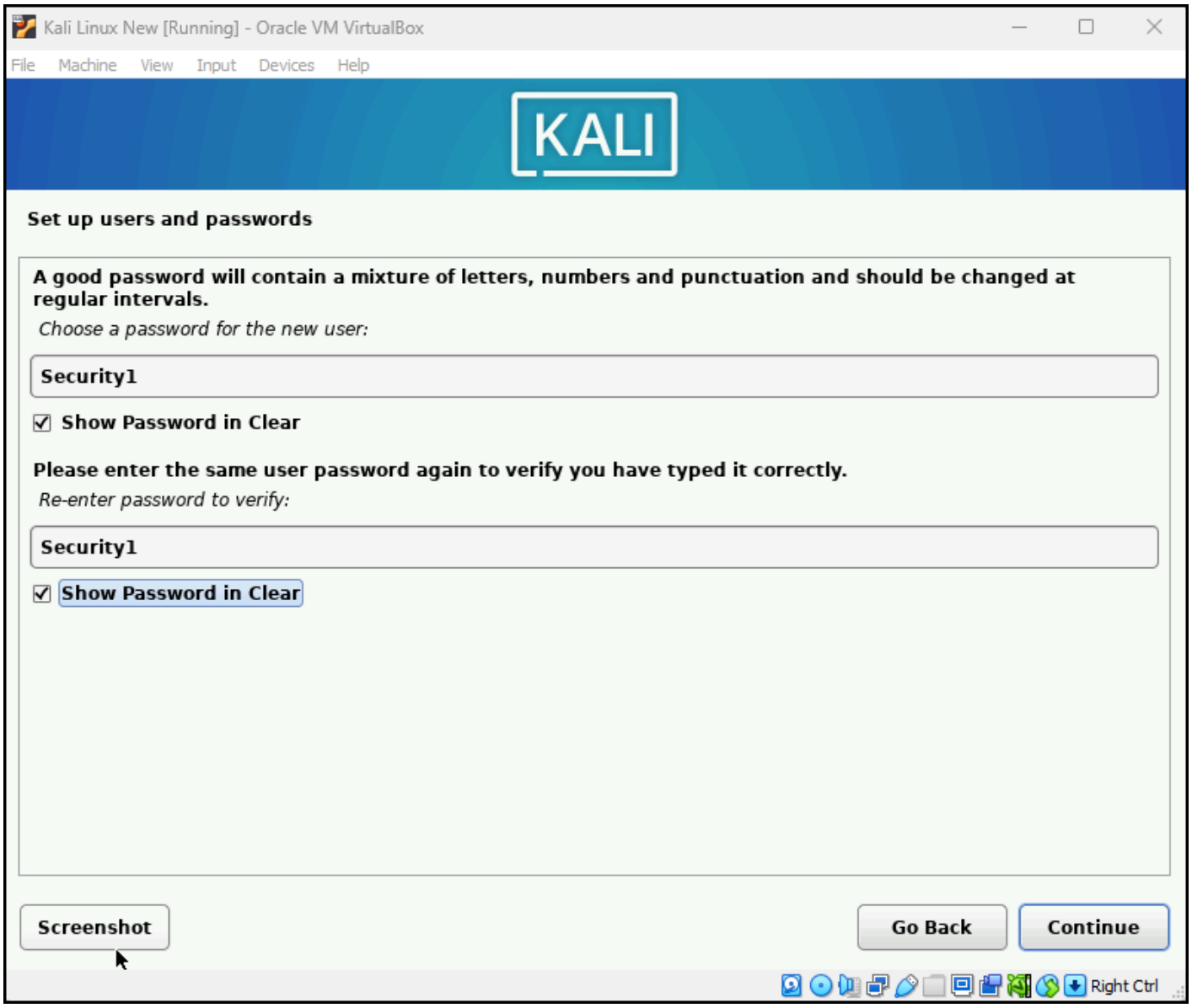


Figure 14 – Set password

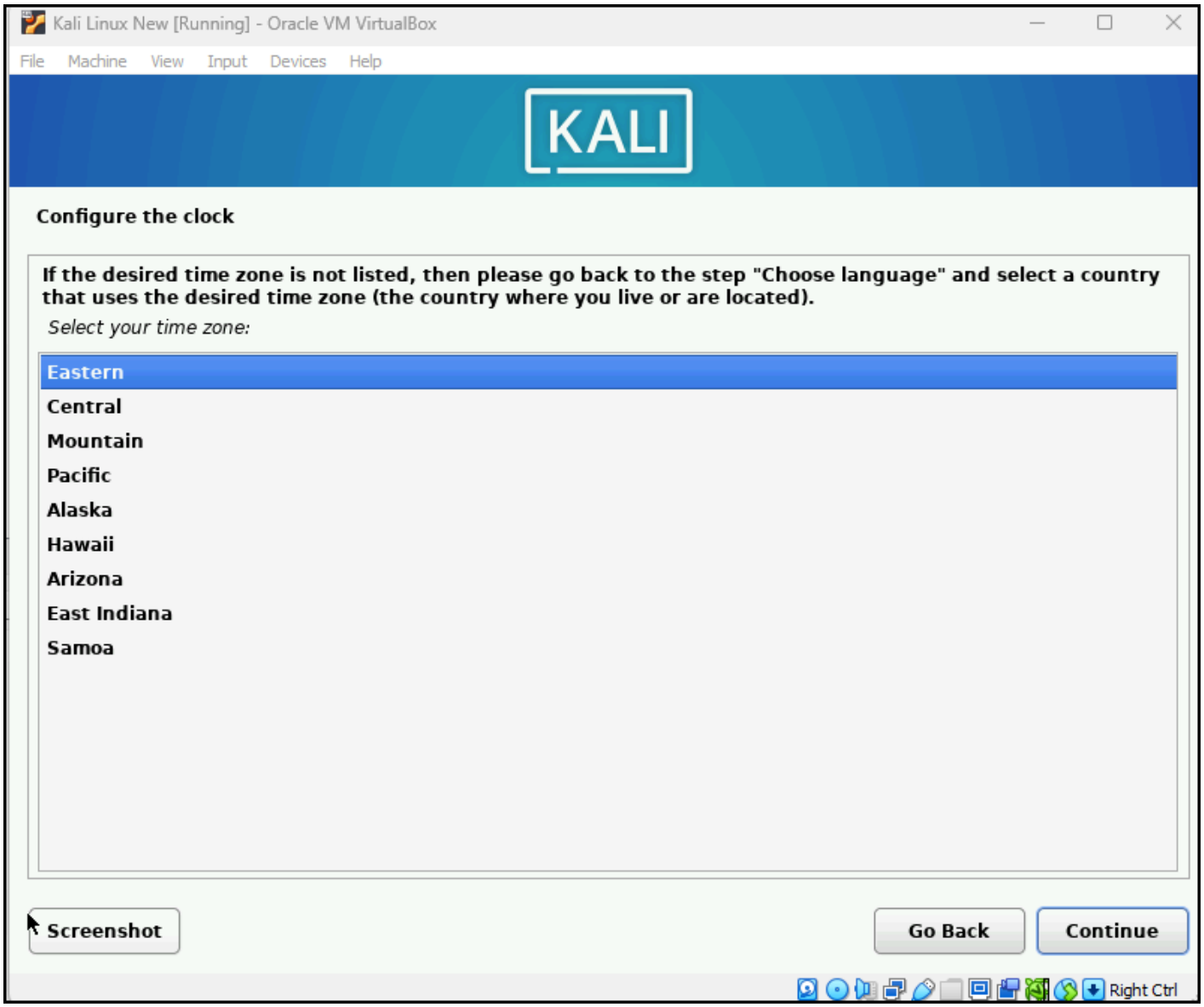


Figure 15 – Select time zone

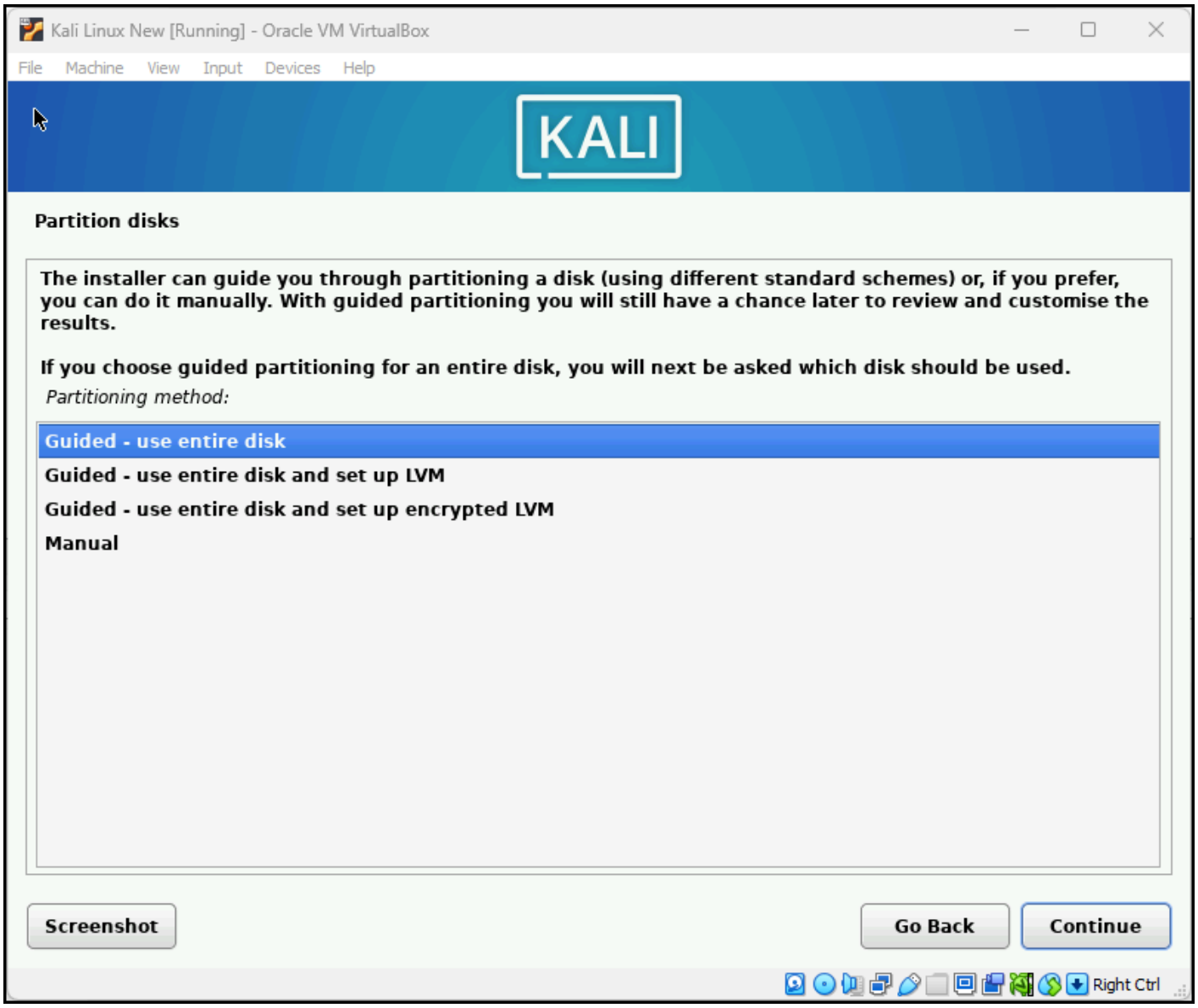


Figure 16 – Use the entire disk

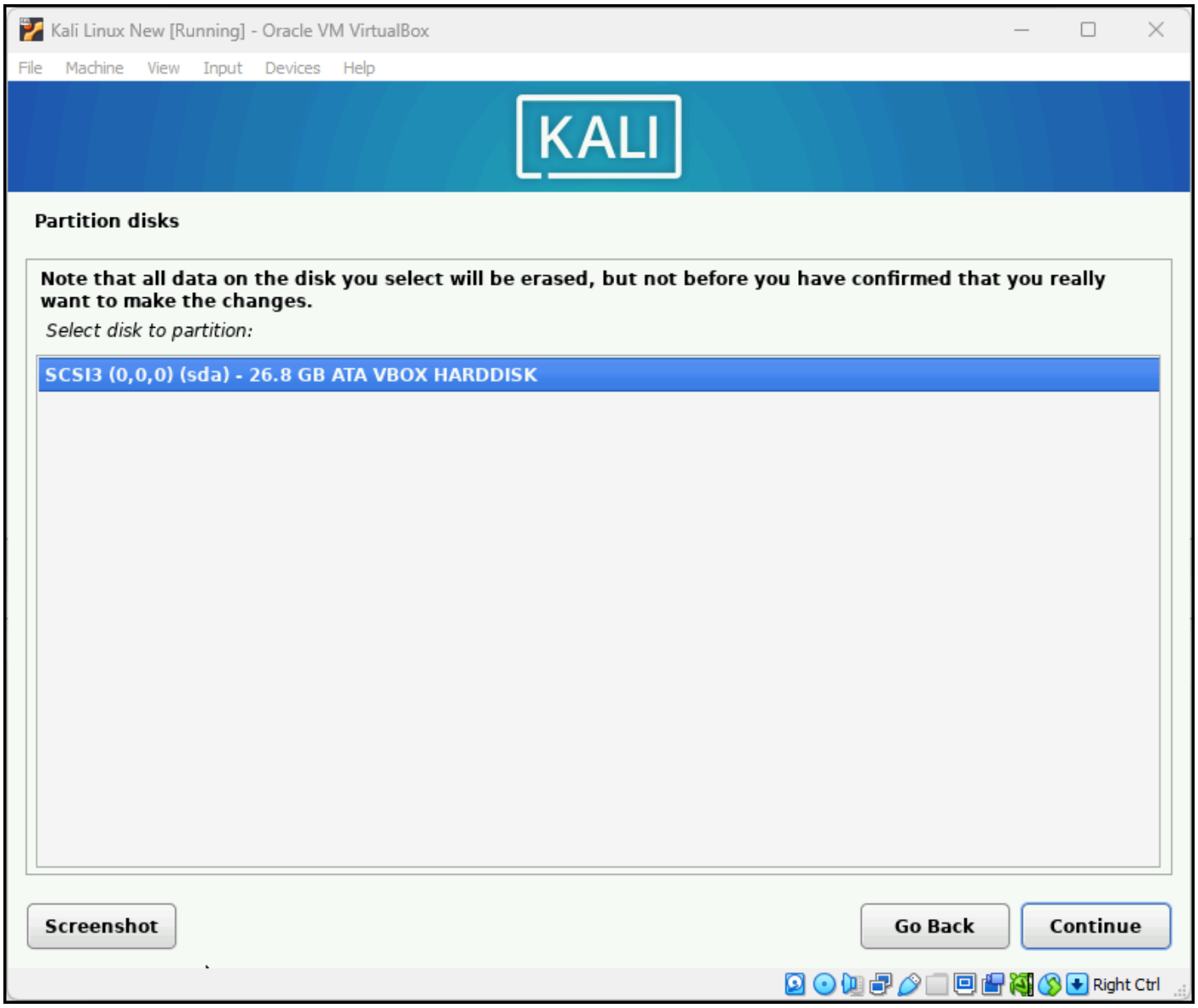


Figure 17 – Use default disk partition

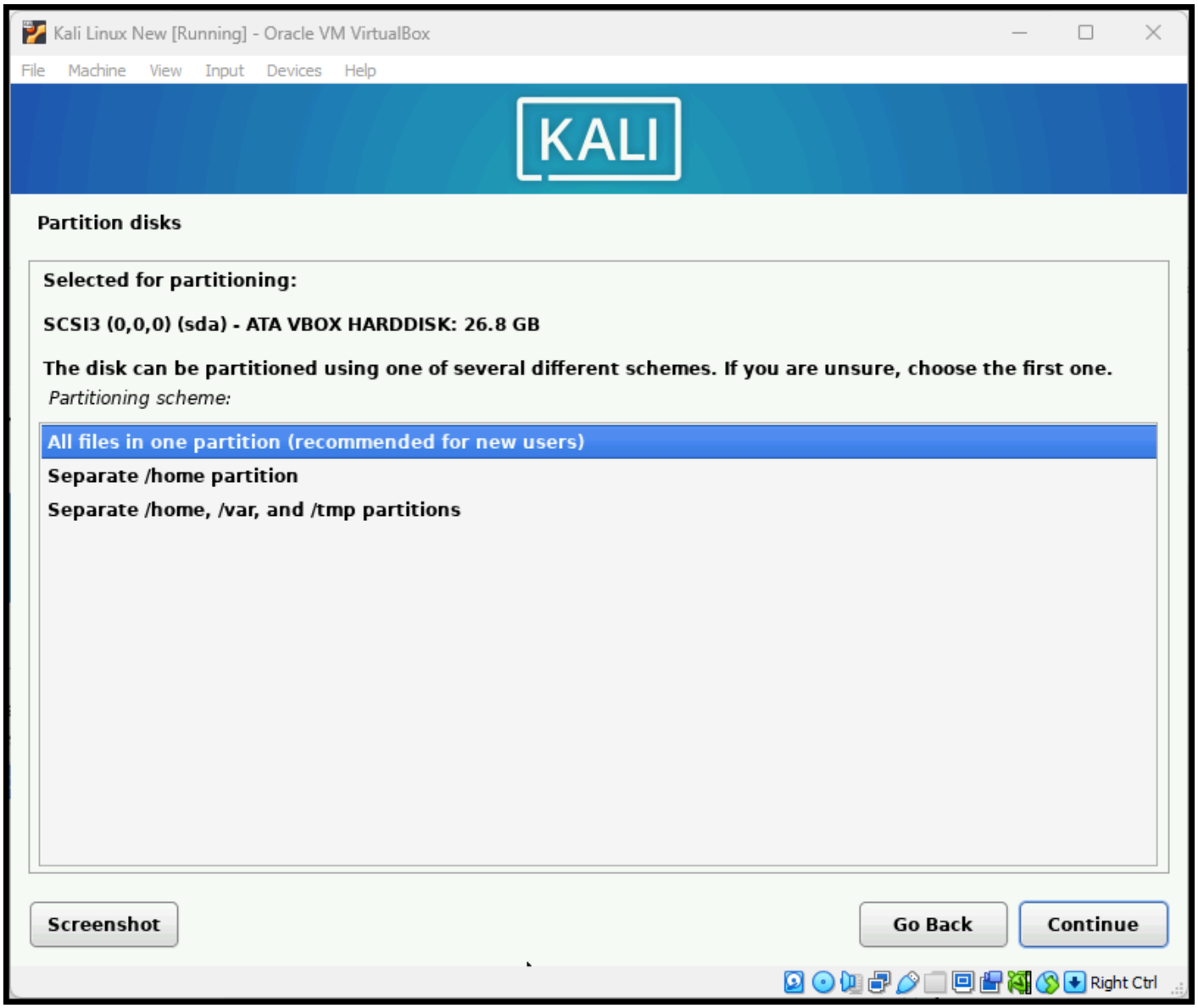


Figure 18 – Use all files in one partition

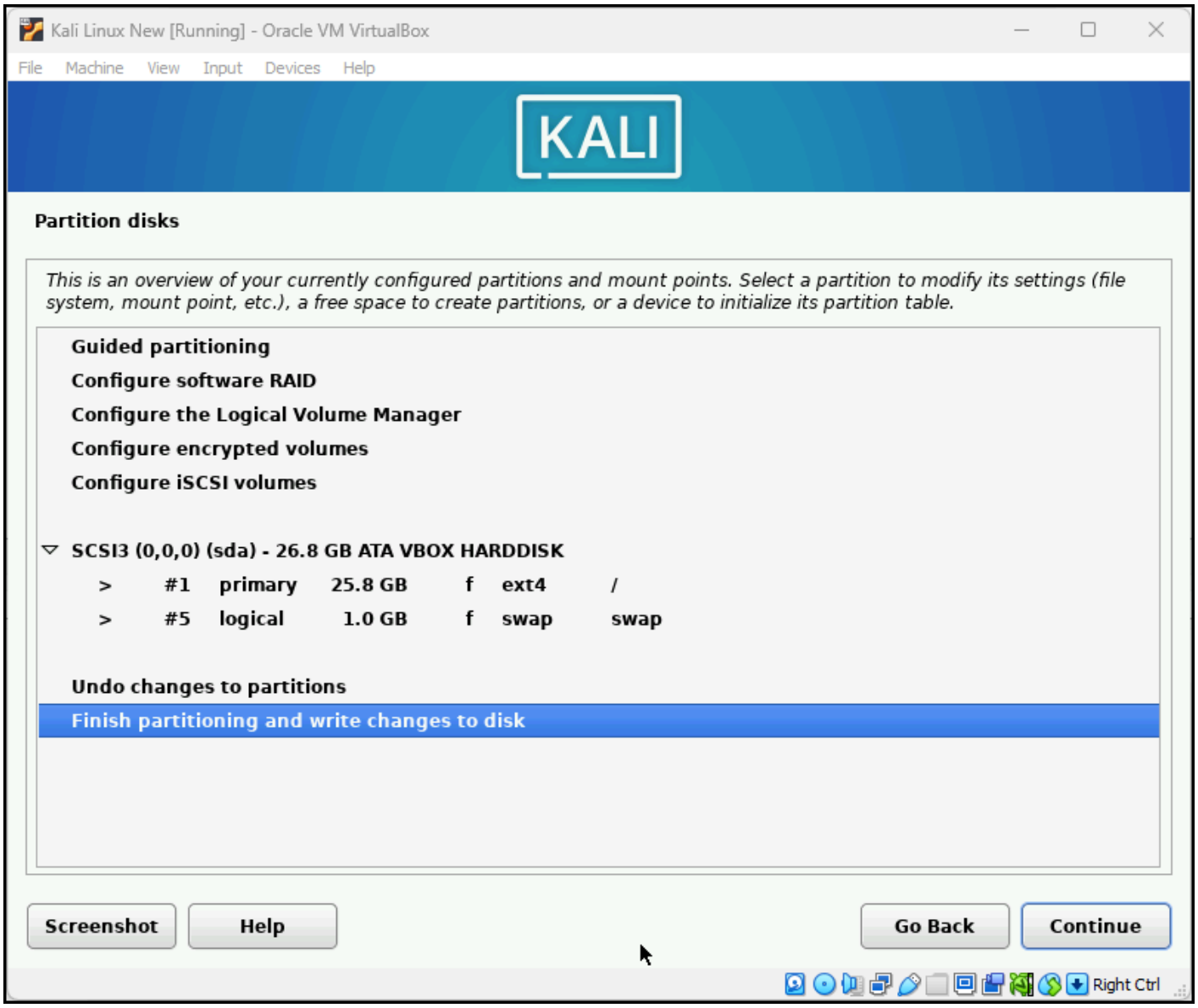


Figure 19 – Verify settings and continue

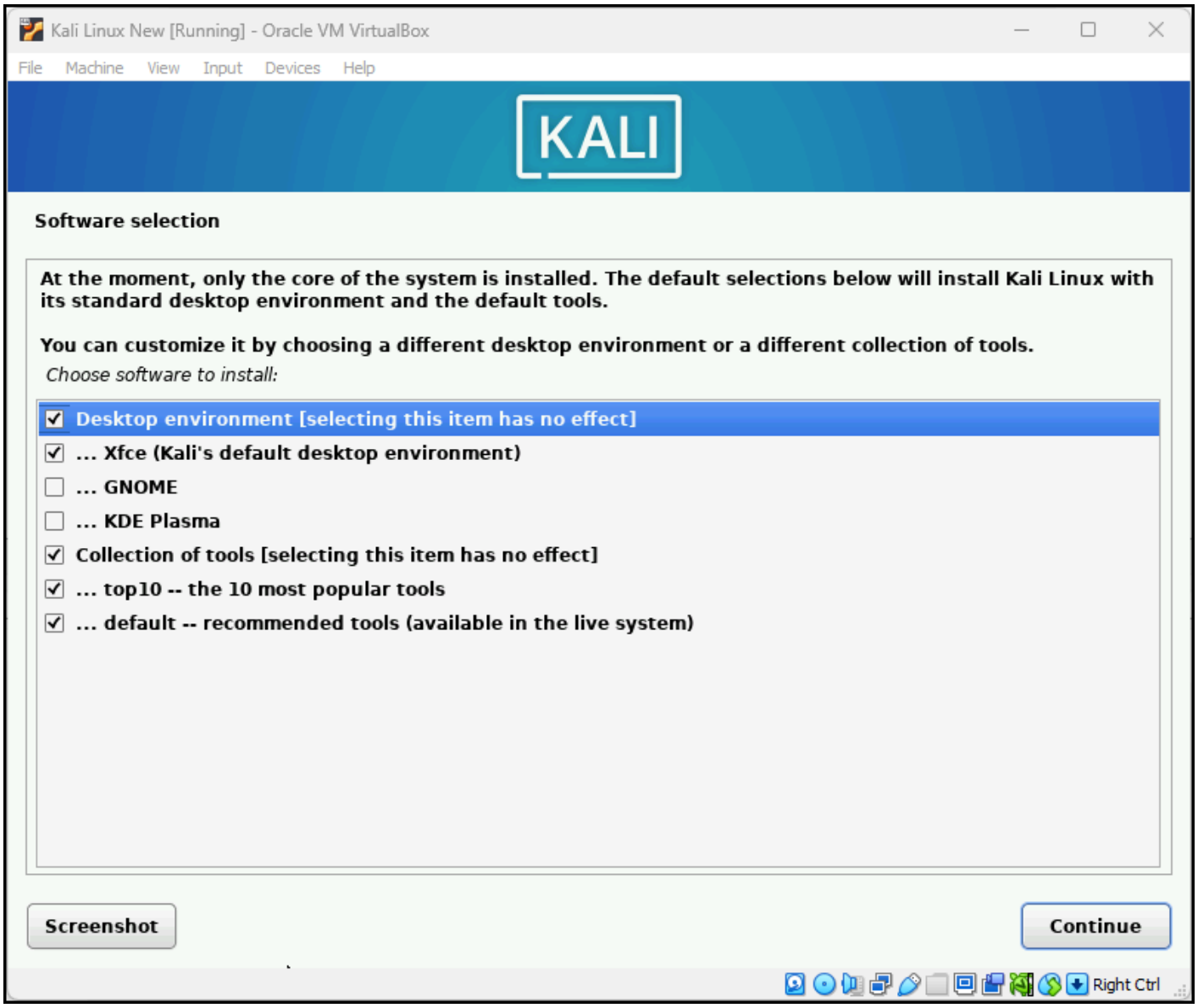


Figure 20 – Software selection is default

Figure 21 – GRUB loader

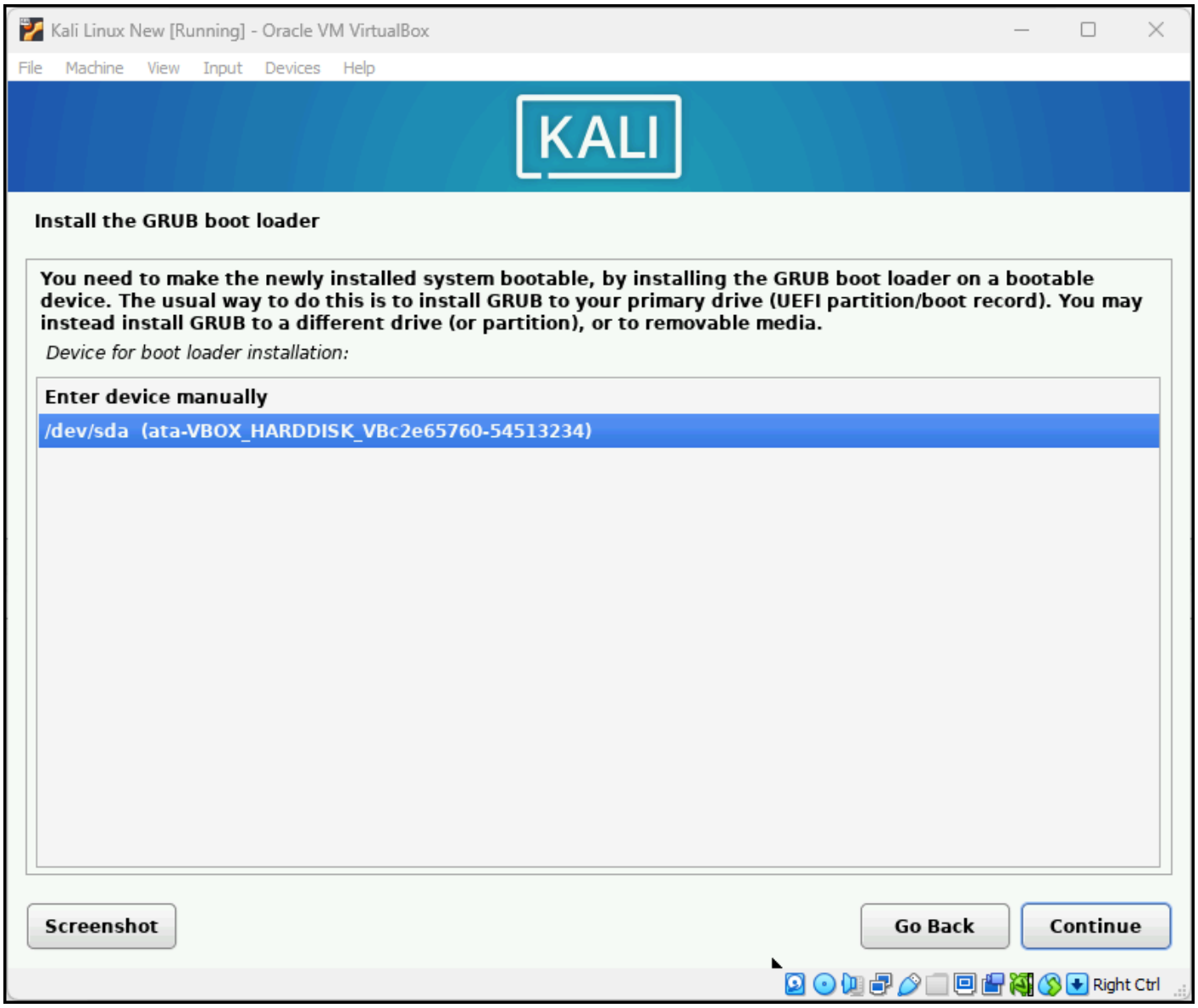


Figure 22 – Select the device

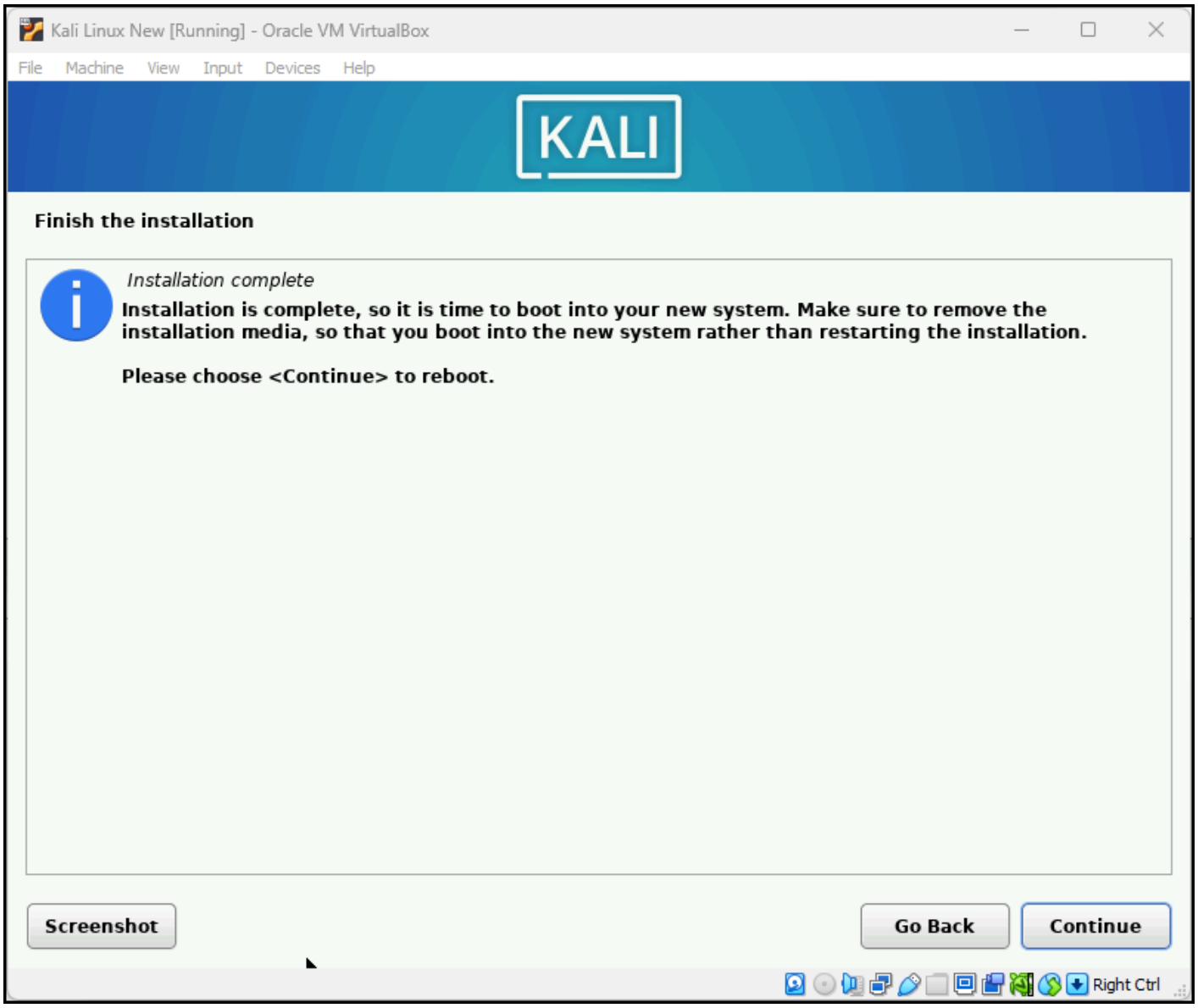


Figure 23 – Finish the installation

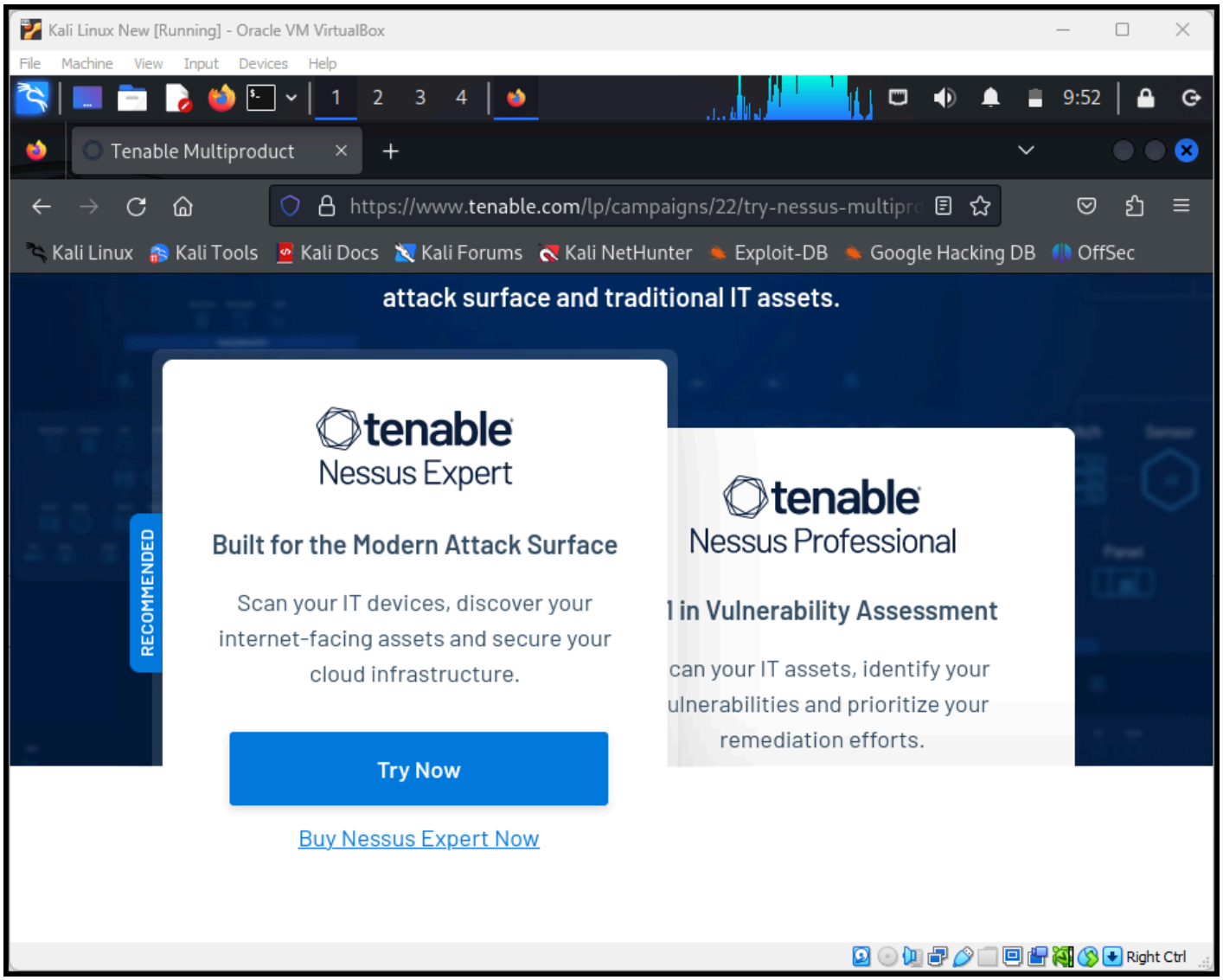


Figure 24 – Install Nessus

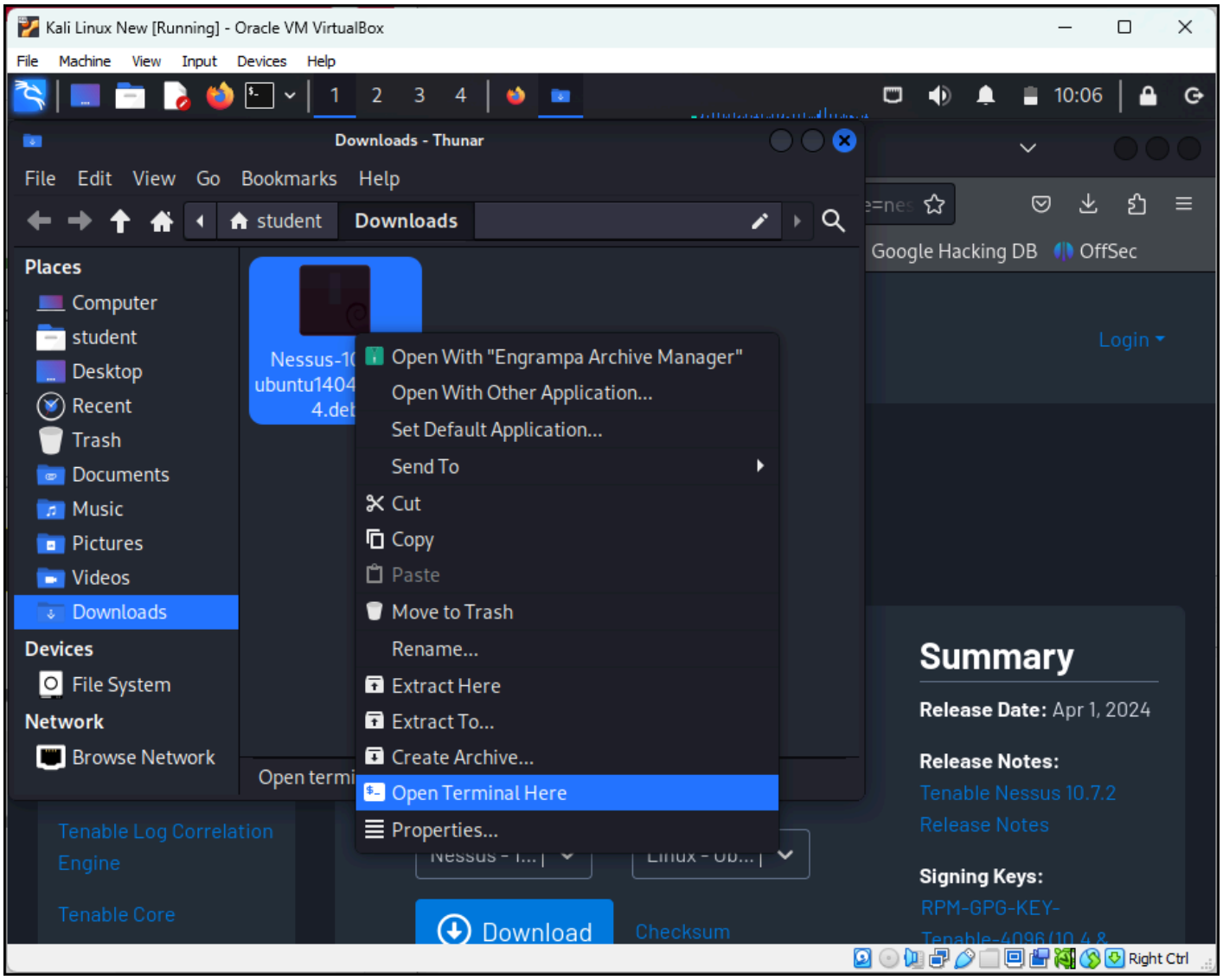


Figure 25 – Open download folder

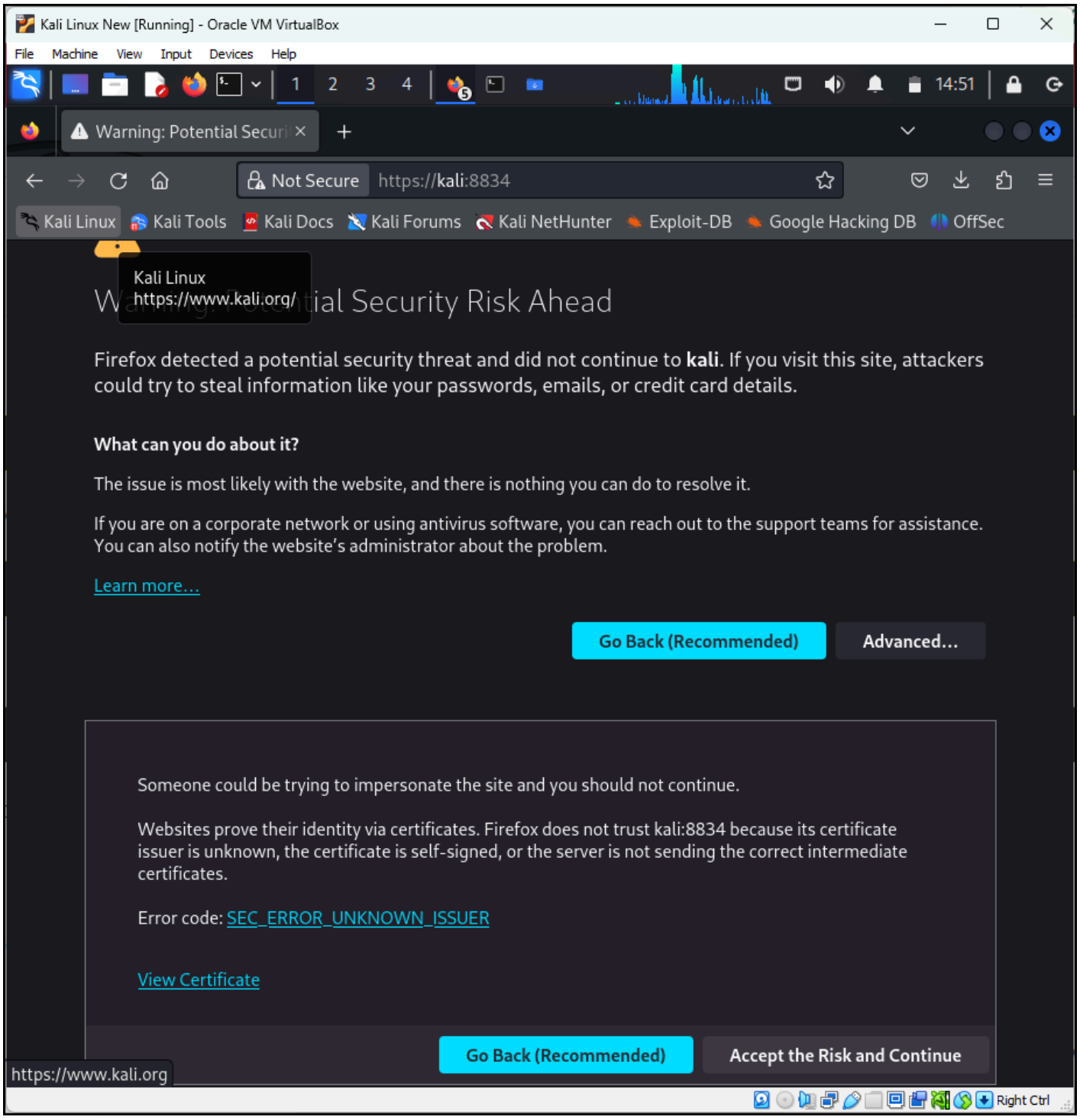


Figure 26 – Using Firefox to navigate Nessus

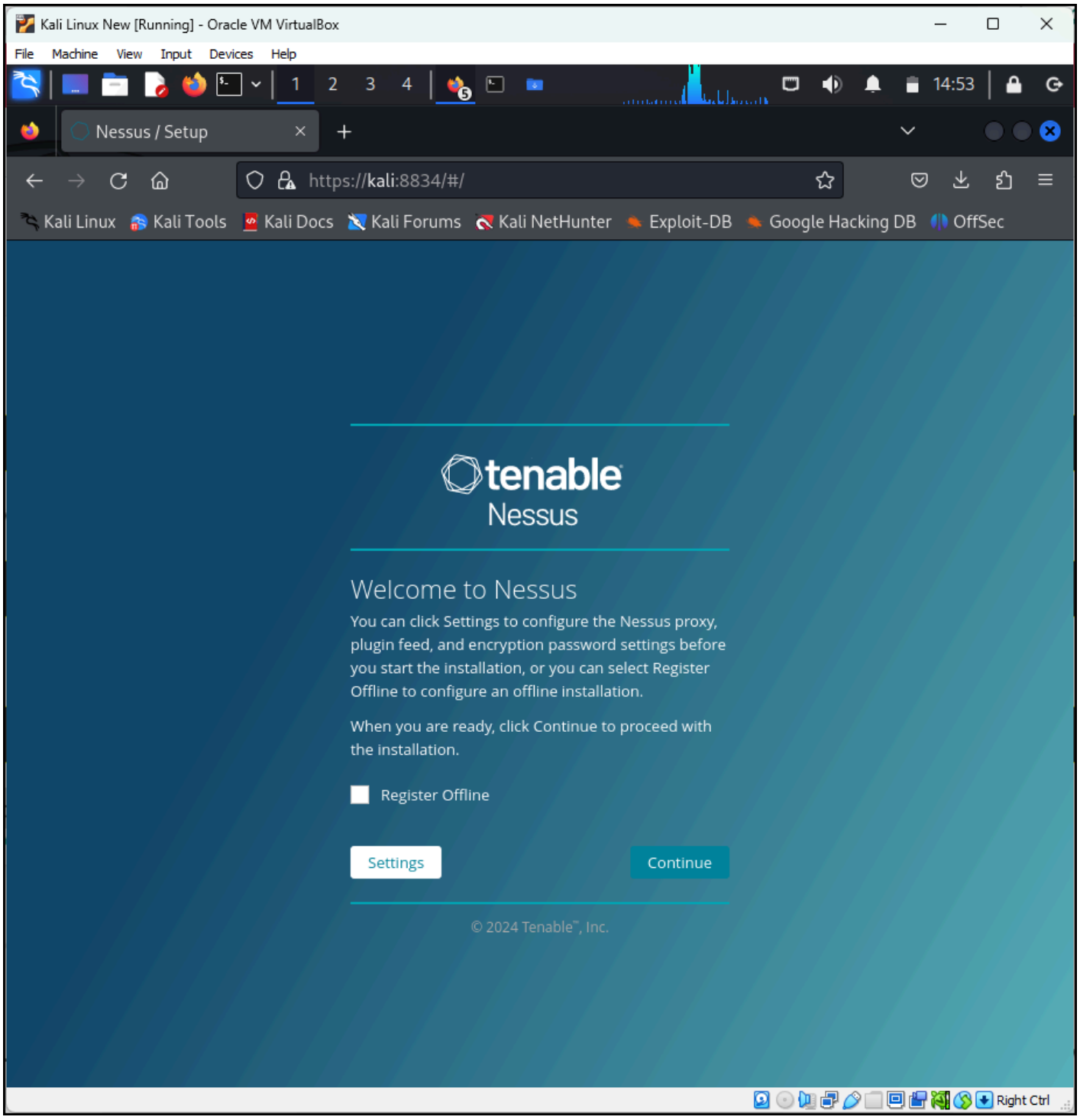


Figure 27 – Continue

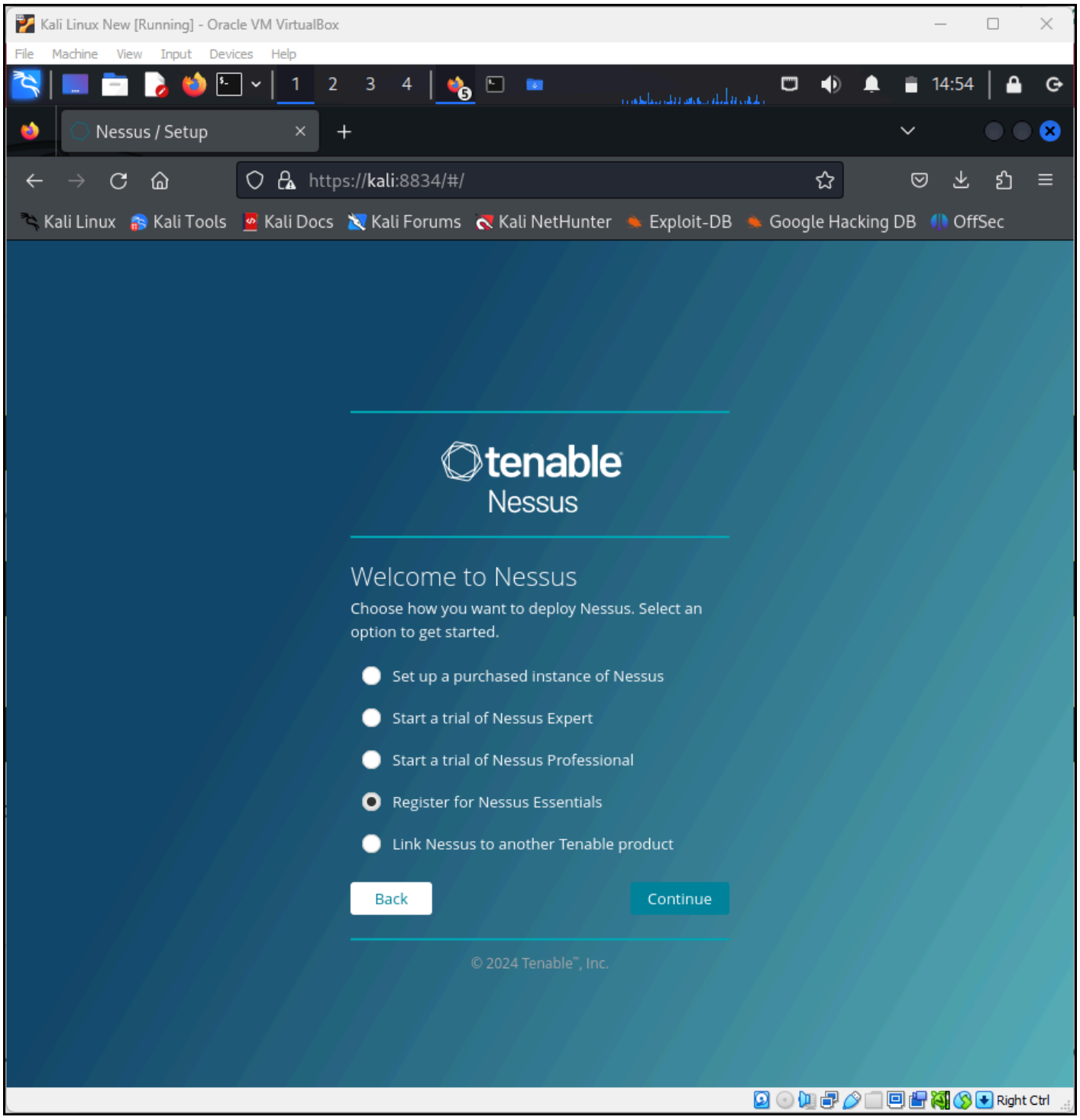


Figure 28 – Register

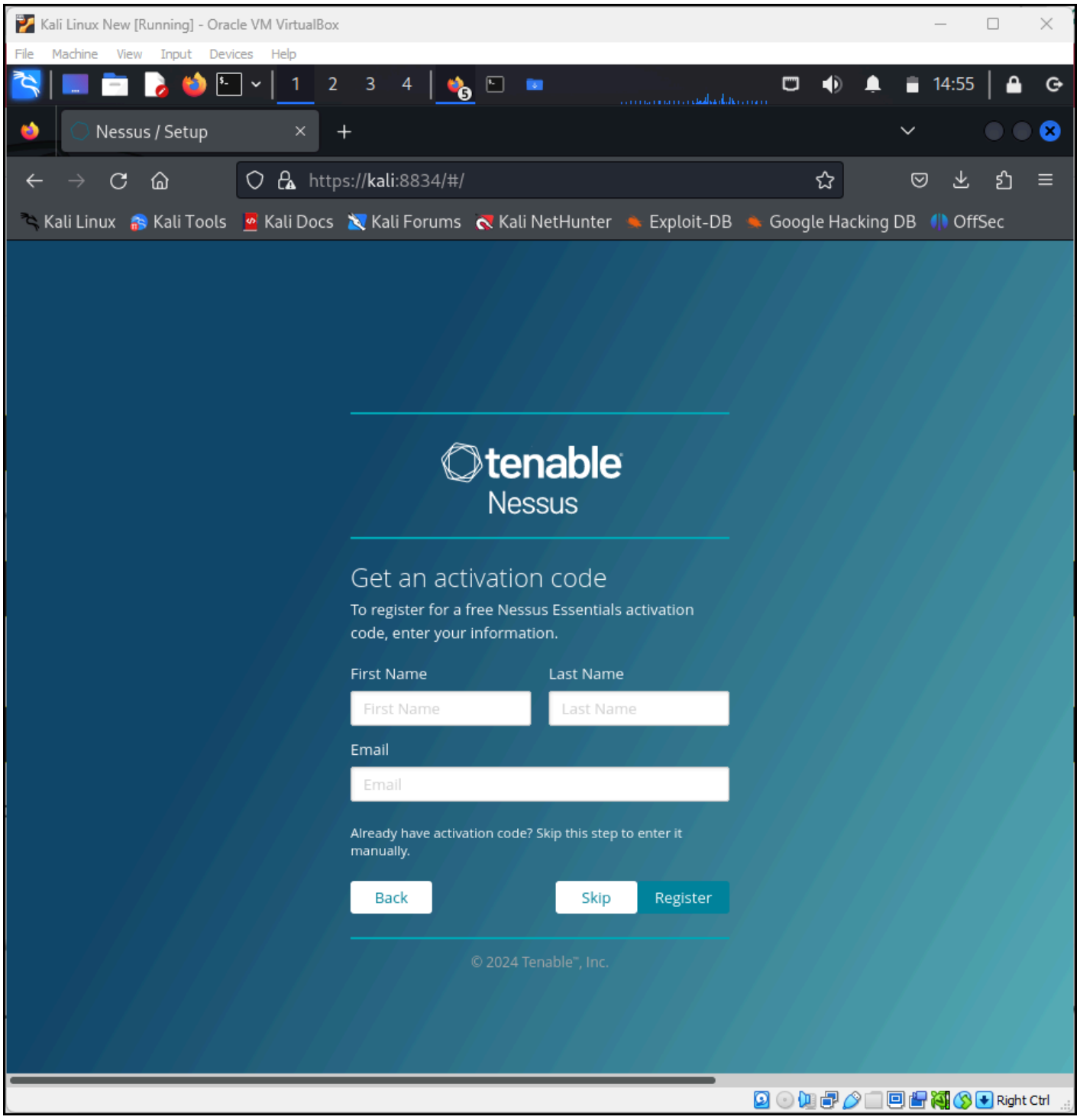


Figure 29 – Skip if already have the code

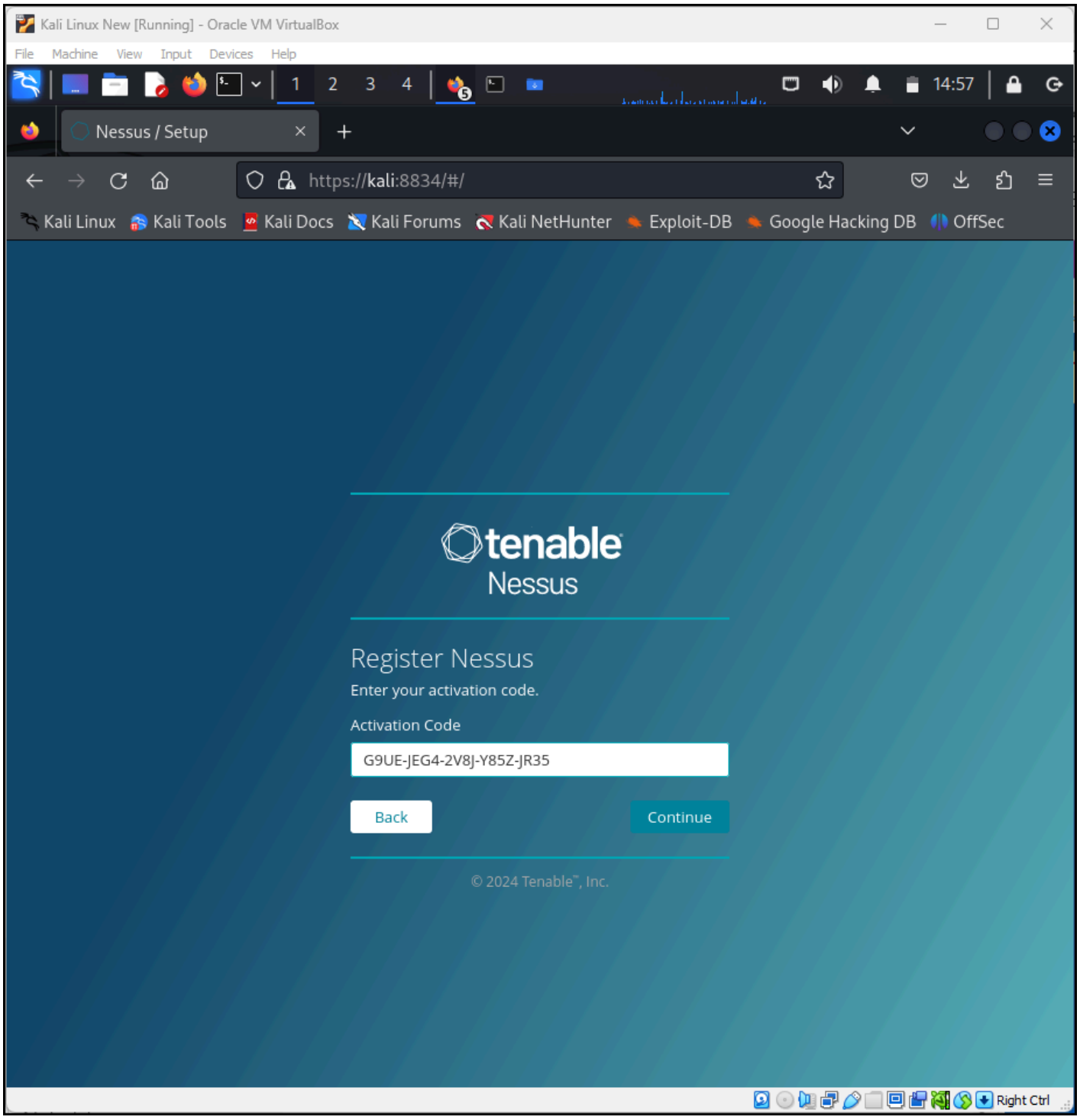


Figure 30 – Input the activation code

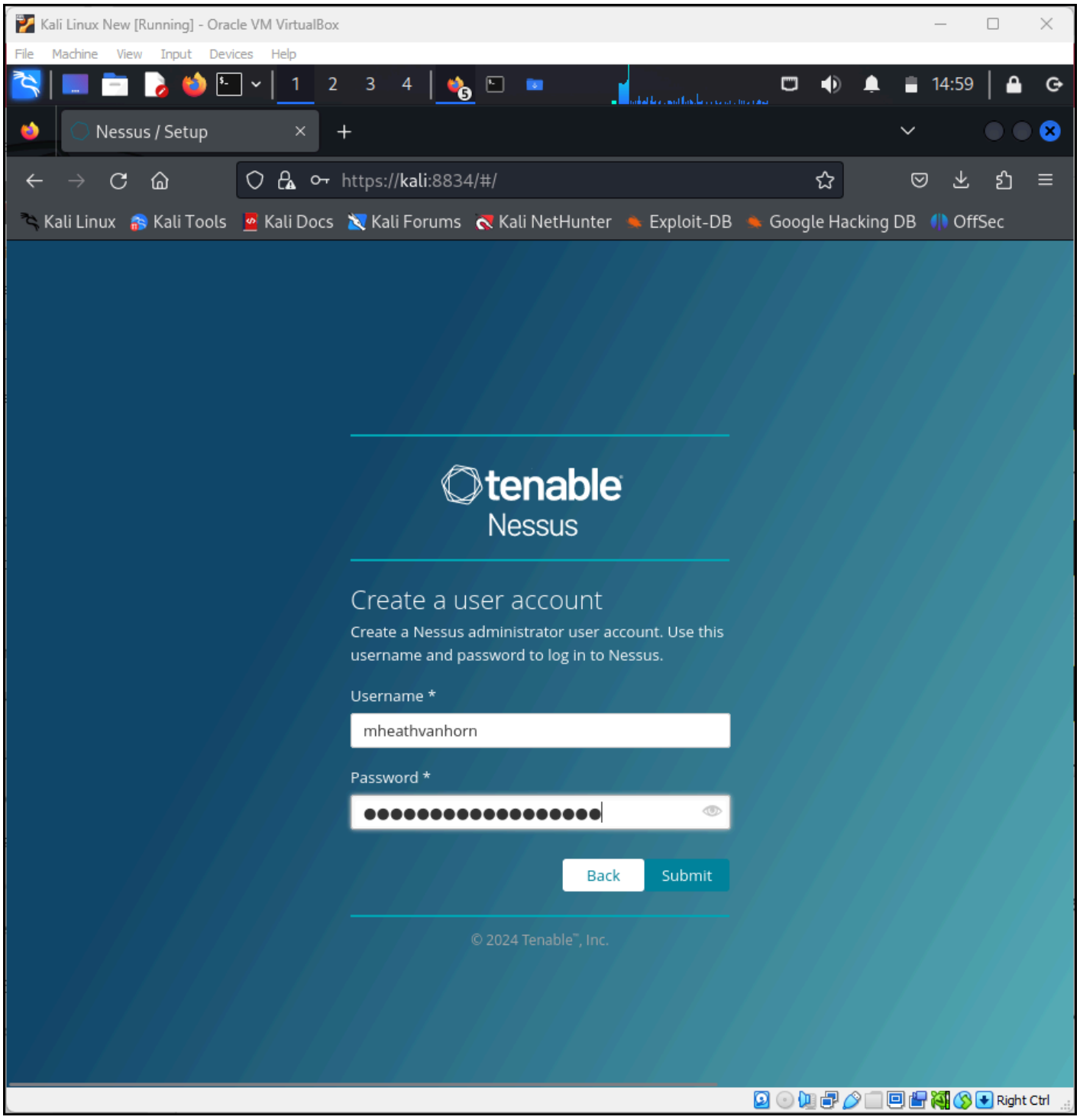


Figure 31 – Create username and password

CHAPTER 13

Create a Vulnerable Desktop VM

MATHEW J. HEATH VAN HORN, PHD

Metasploitable is an intentionally vulnerable virtual machine (VM) that can be used to conduct security training, test security tools, and practice common penetration testing techniques. There are different flavors of Metasploitable (original, 2, and 3) and it offers many features provided by servers and websites except it is completely vulnerable to attacks. Metasploitable 2 is easier to build and based on Linux. However, it's outdated and has been replaced by Metasploitable 3 which is based on Windows Server.

LEARNING OBJECTIVES

- Successfully download, install, and run Metasploitable 2 in VirtualBox and add it to the GNS3 environment.
- Successfully download, build, and run Metasploitable 3 in VirtualBox and add it to the GNS3 environment.

PREREQUISITES

- Chapter 2 – Setting up a GNS3 environment
- Chapter 6 – Adding a Virtual Machine to GNS3

DELIVERABLES

- None – this is a preparatory lab that supports other labs in this book

RESOURCES

- MikroTik Documentation – Getting Started, https://help.mikrotik.com/docs/display/ROS/Getting+started
- Metasploitable Documentation
- RKiLAB, "Metasploitable2 kernal panic – not syncing: IO-APIC error solution (Virtualbox)", https://www.youtube.com/watch?v=aYxfhMrjVhk
- elconak Network & Security, "Lab Setup 1 – Import Metasploitable 2 Linux into Oracle VirtualBox – boot with 'noapic' option", https://www.youtube.com/watch?v=oTSdSIdFbIQ

- Metasploitable 3 Quickstart guide, https://github.com/rapid7/metasploitable3/blob/master/README.md
- Metaspoitable 2 Exploitability Guide, https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/
- Metasploitable 3 Exploitability Guide, https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities

CONTRIBUTORS AND TESTERS

Dante Rocca, Cybersecurity Student, ERAU-Prescott

Phase I – Installing Metasploitable 2 – Sourceforge

This is an easy way to download Metasploitable 2 as a VM. However, it is an older repository.
NEVER expose this VM to an untrusted network. Use NAT or Host-Only modes when using this VM.
Metasploitable 2 is VERY old. It still works as a vulnerable machine, but its usefulness may be limited.

1. Visit SourceForge and download the Metasploitable 2 zip file here

2. Once downloaded unzip the file and note where the file is extracted. In our example, we extracted it to the downloads folder

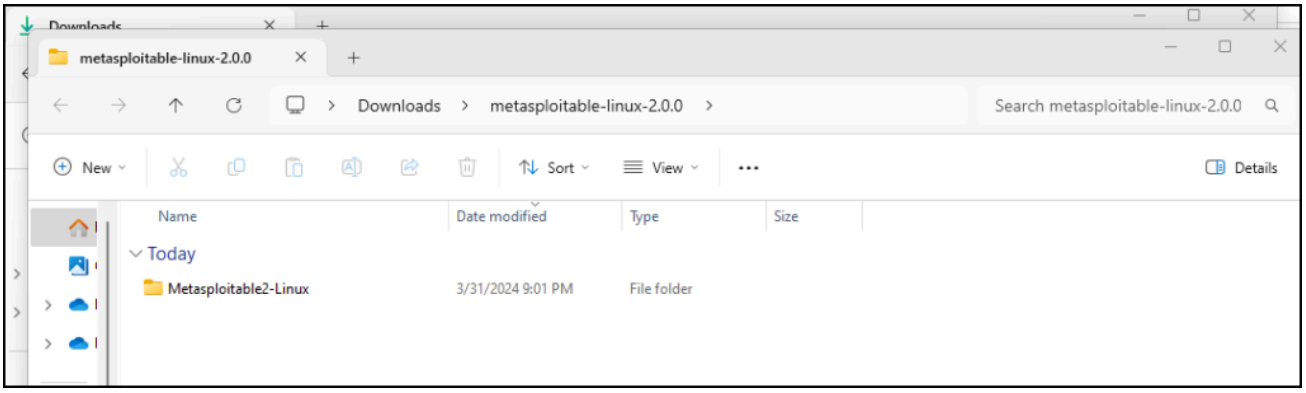


Figure 1 – Metasploitable 2 in Downloads folder

3. Open VirtualBox and create a new virtual machine

    3.1. On the VirtualBox menu click on ***Machine*** then ***New...***

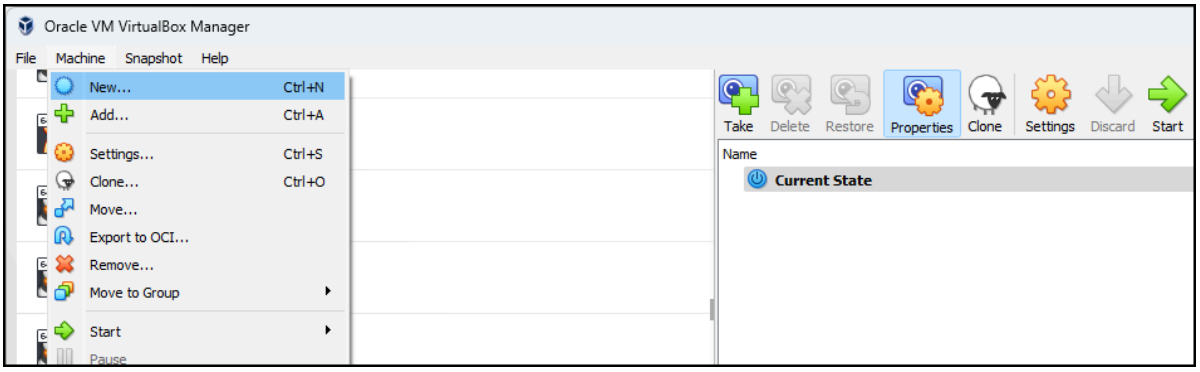


Figure 2 – Create a new VM

3.2. Choose a name for the new Virtual Machine (VM). In this case, we will call it ***Metasploitable 2***

3.3. Select the folder where you want the VM to reside

3.4. Select Type: ***Linux***
Select Version: ***Oracle Linux (64-bit)***

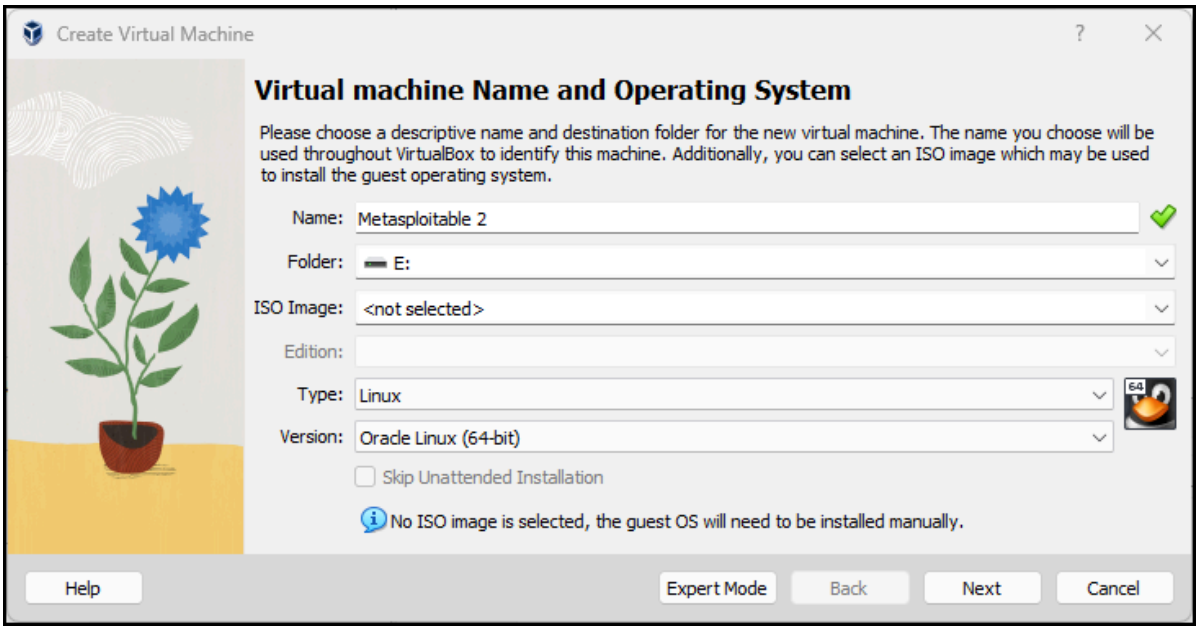


Figure 3 – VM name and operating system selections

3.5. Click ***Next***

3.6. Base memory: ***2048 MB***
Processors: ***2***

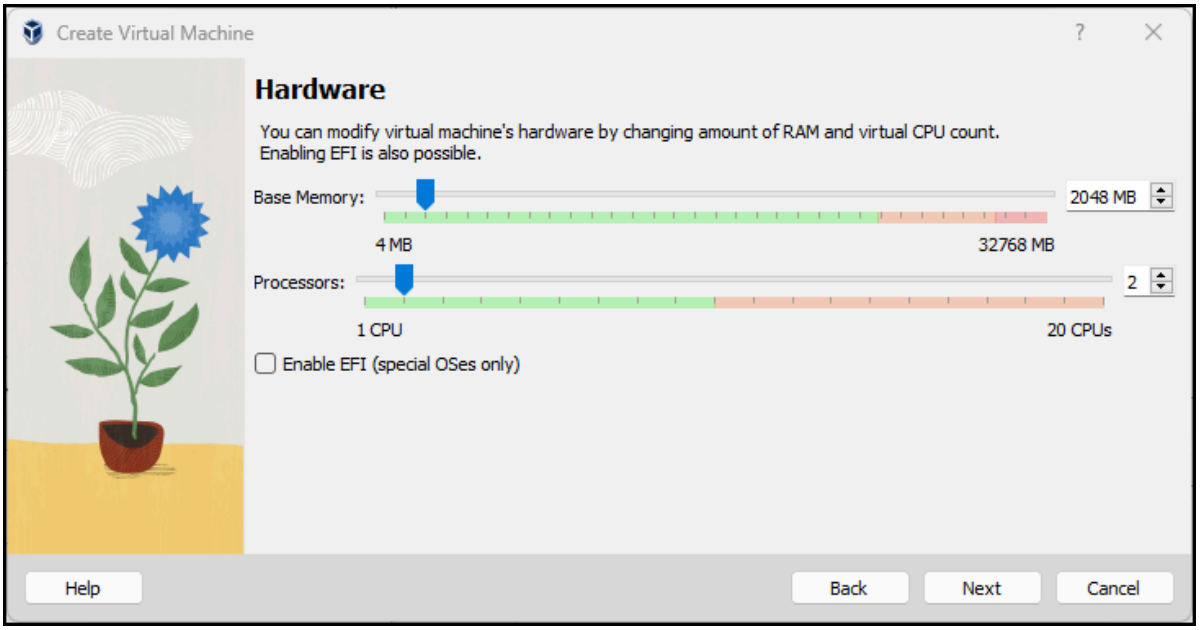


Figure 4 – VM Hardware Selections

3.7. Click ***Next***

3.8. Click on ***Use an existing virtual hard disk file***

3.9. Click on the folder next to the dropdown menu

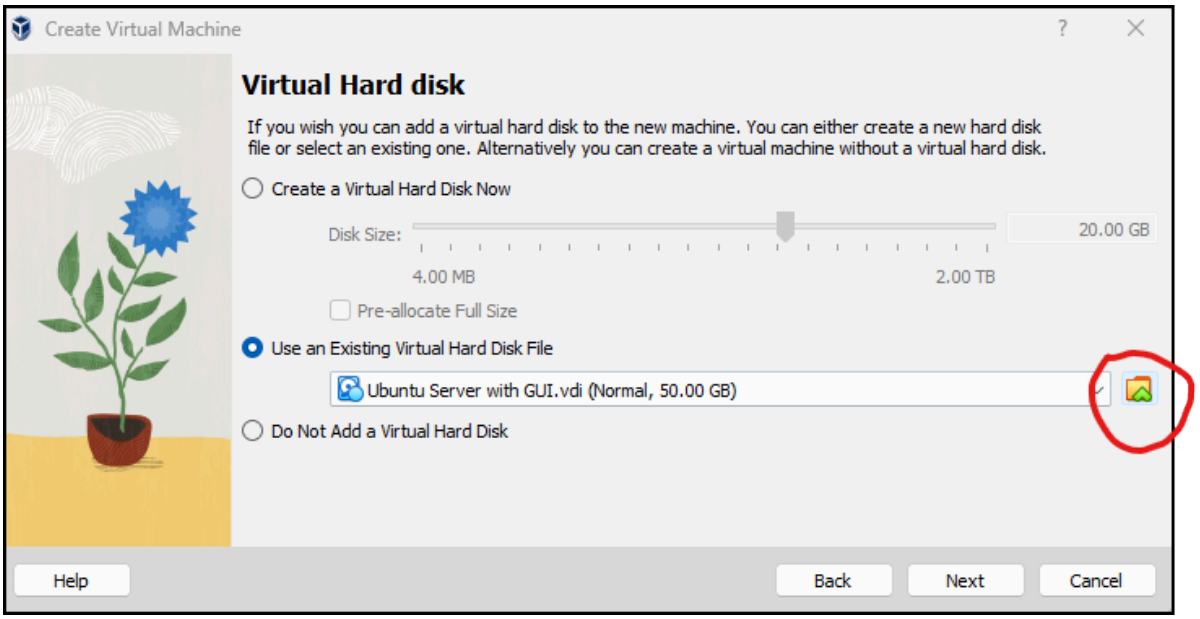


Figure 5 – Use and Existing Virtual Hard Disk

3.10. Click on the ***Add*** button

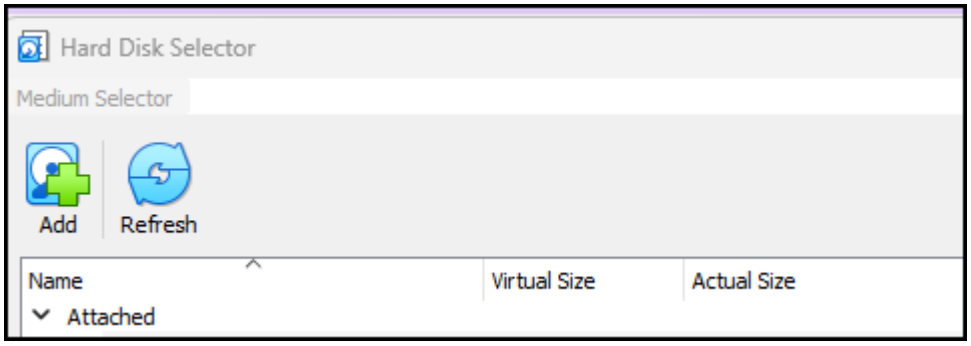


Figure 6 – Virtual Hard Disk Selector

3.11. Navigate to the location of the file you extracted and select it

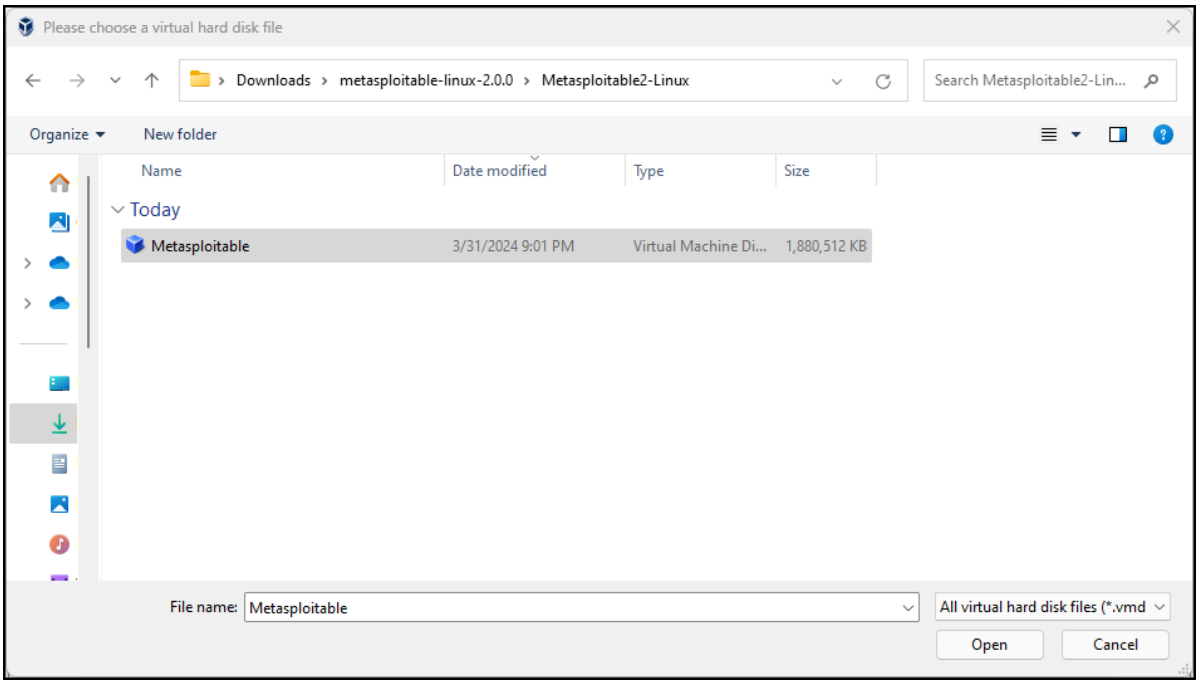


Figure 7 – Add the Metasploitable Virtual Hard Disk File

3.12. Click on ***Open*** and notice it is now in the hard disk selector menu. Keep it selected and click on ***Choose***

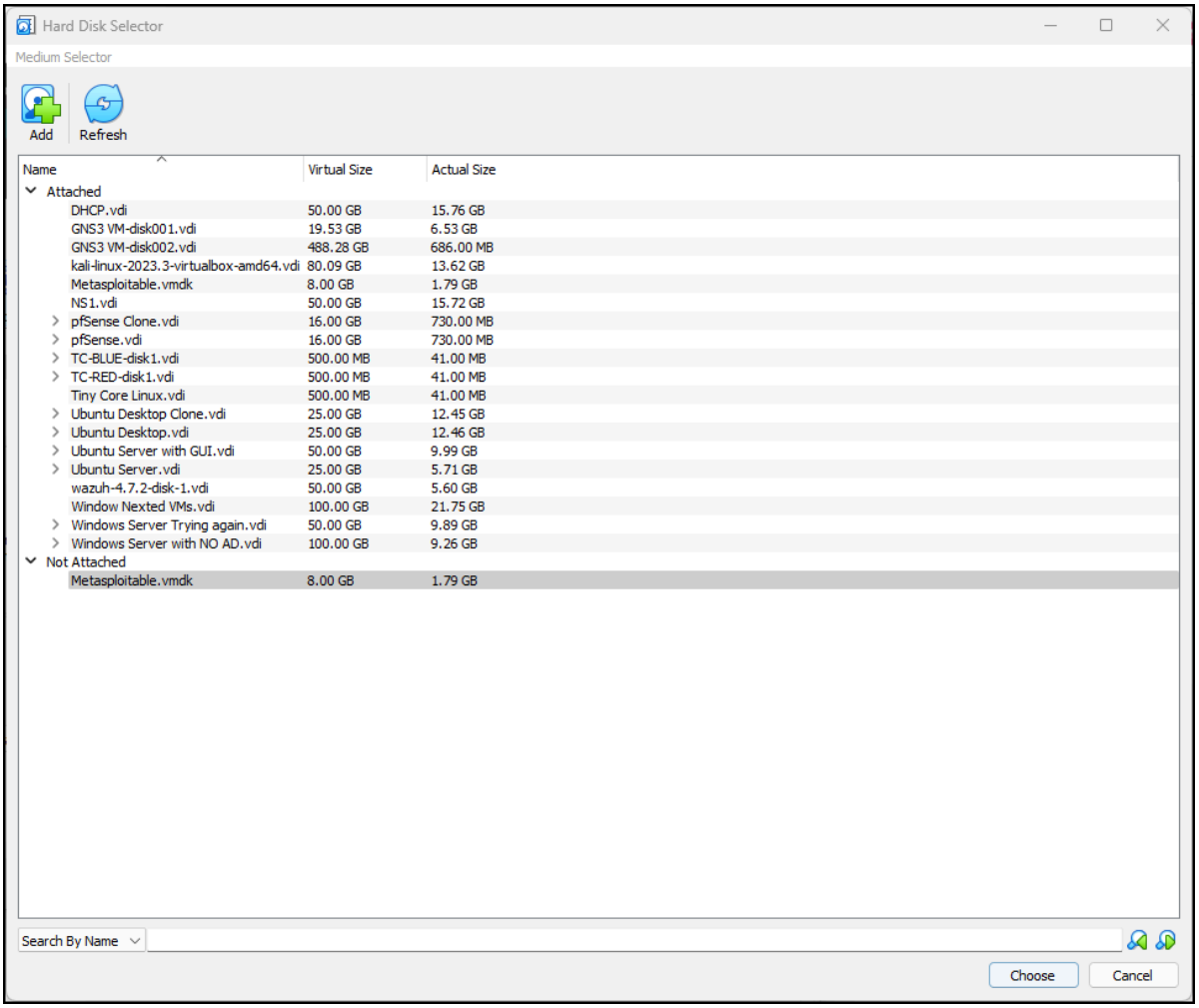


Figure 8 – Select the Metasploitable Virtual Hard Disk File

3.13. It is now selected as our hard disk file, so click ***Next***

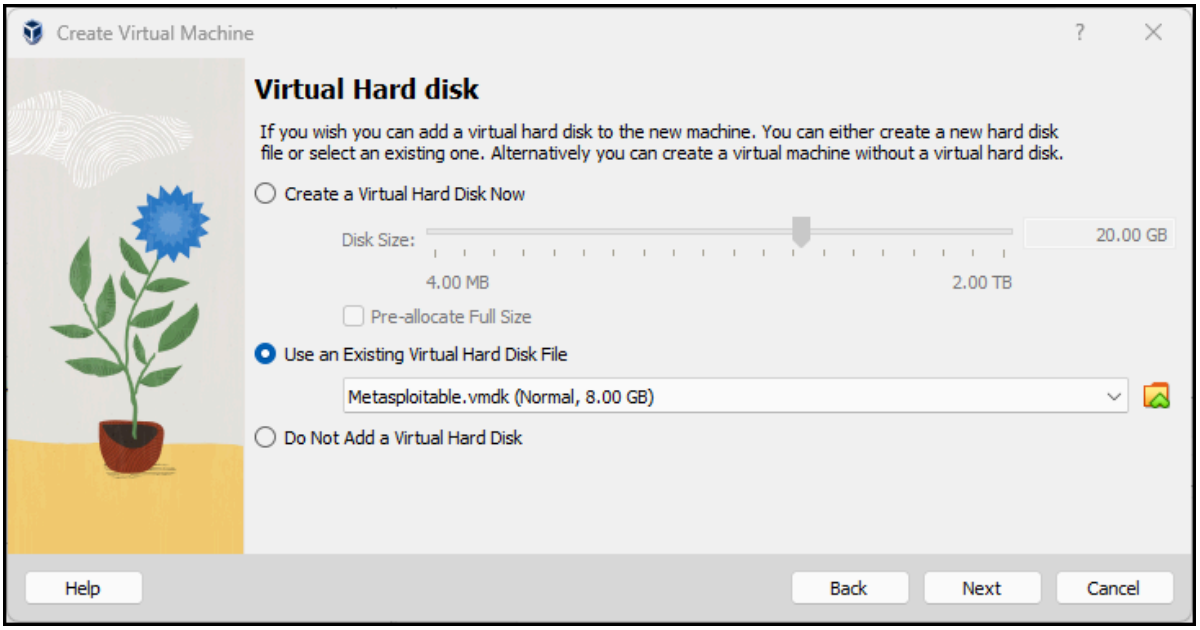


Figure 9 – Use Metasploitable Virtual Hard Disk File

3.14. Click ***Finish*** and you can see it added to the rest of your VMs

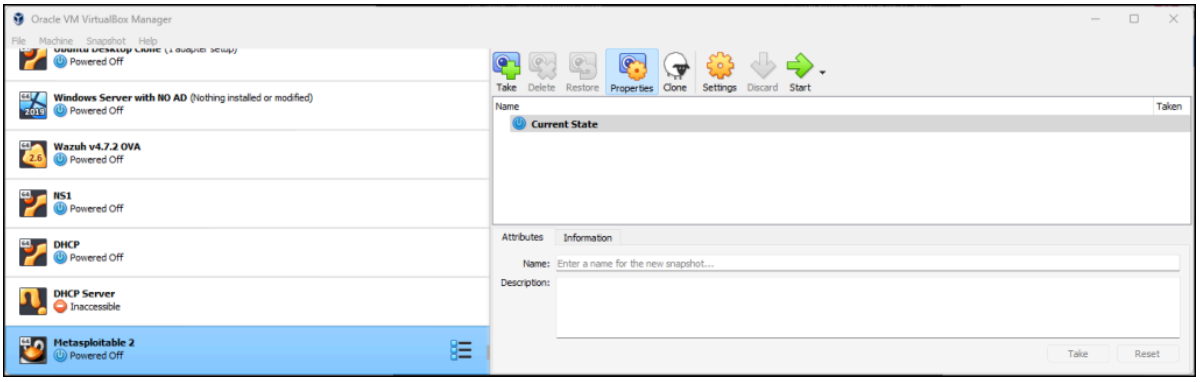


Figure 10 – Metasploitable 2 VM added to Virtual Machines

4. Now you can start it up like any other VM and the login information is
USER: ***msfadmin***
PASSWORD: ***msfadmin***

A note on hardware

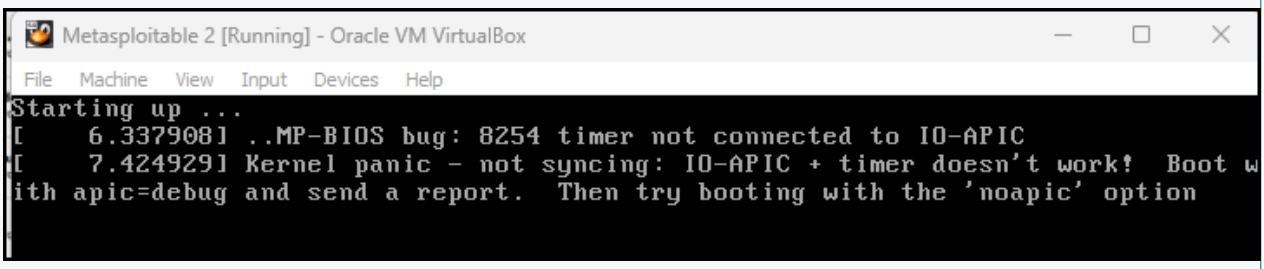


Figure 11 – Metasploitable 2 startup error

Metasploitable2 is very old and hardware and software have changed. If you get an error when you try to start the machine, take the following steps:

4.1. Close the virtual machine

4.2. Open settings, go to the motherboard settings and disable all the extended features

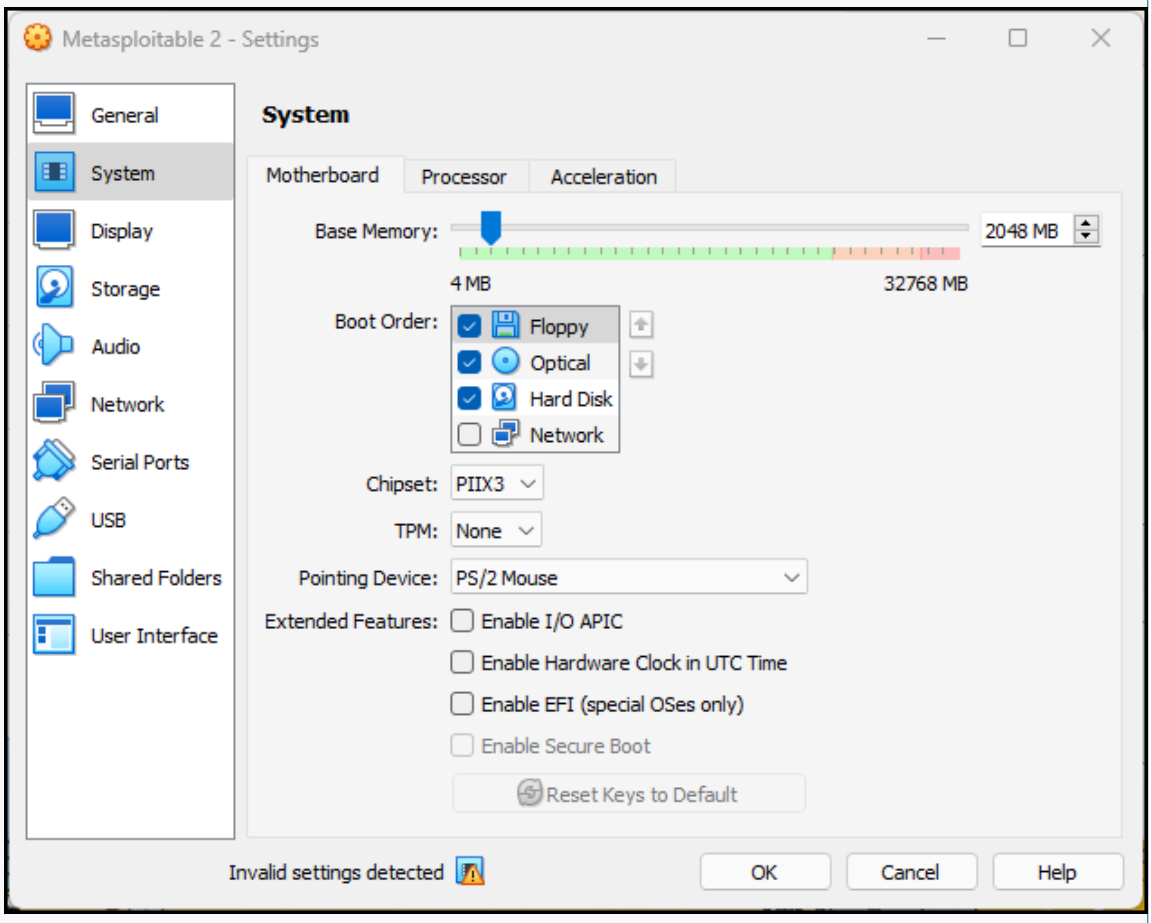


Figure 12 – Disable Extended Features

4.3. Press ***ok***

4.4. Start the virtual machine and get ready to hit the ***Esc*** key as soon as it starts

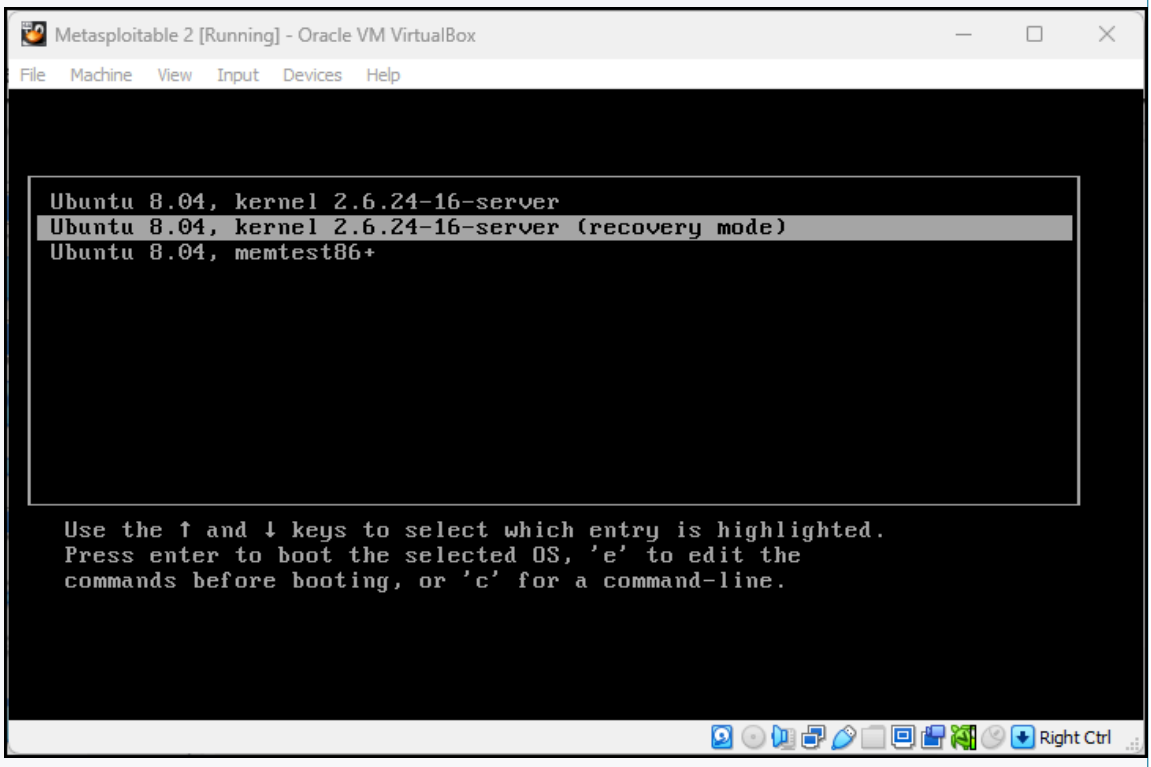


Figure 13 – Start the VM and press the Esc key

4.5. Press ***e*** to edit the boot commands

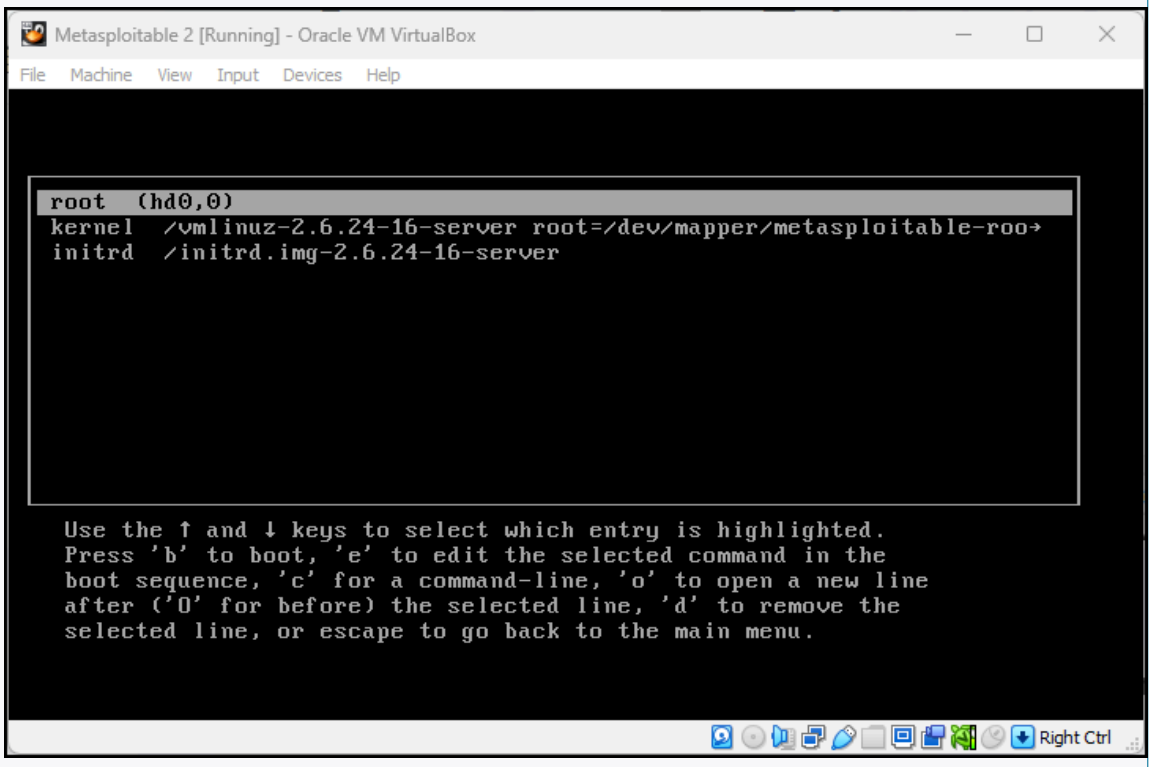


Figure 14 – Edit the boot commands

4.6. Press ***e*** to edit the root command to add

```
noapic
```

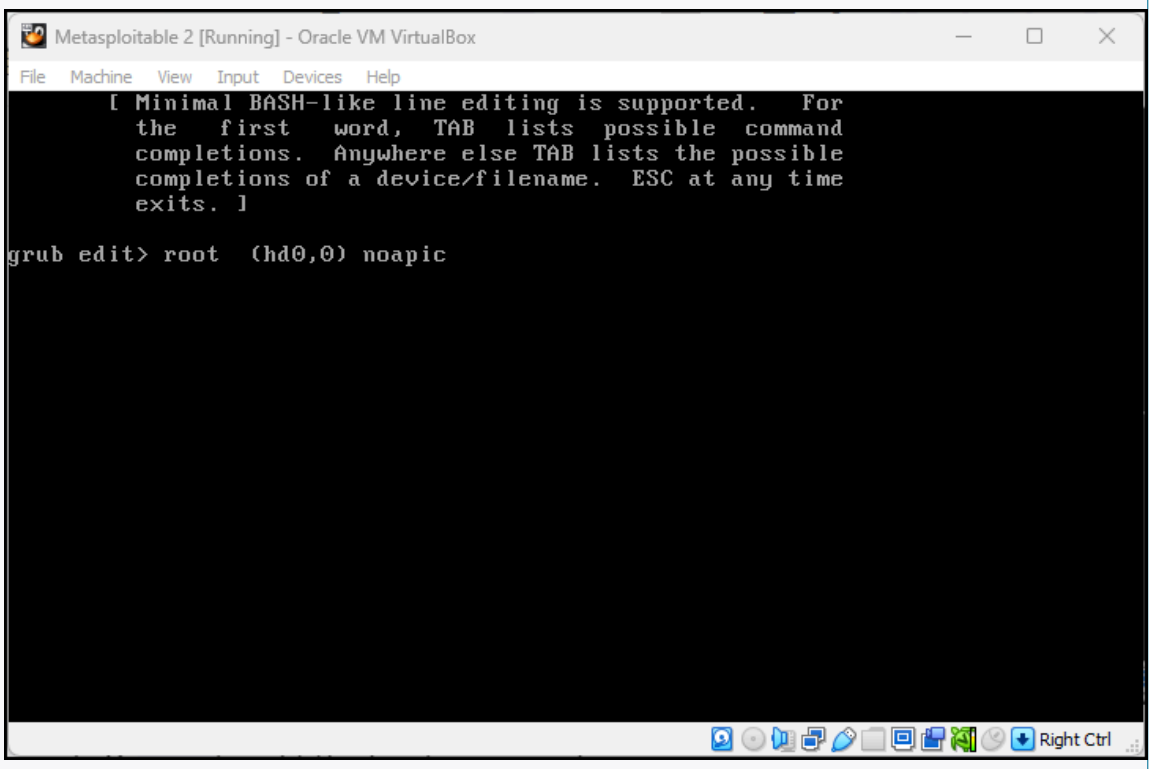


Figure 15 – Add the noapic command

4.7. Repeat for the kernel command and add

```
noapic
```

4.8. Press ***b*** for boot

4.9. This is a temporary solution. But the machine will boot so you can apply a more permanent solution. Log onto the machine using msfadmin msfadmin. Then type

```
sudo nano /boot/grub/menu.lst
```

> **NOTE:** /boot/grub/menu.lst is a lowercase 'L' as in *list*, **NOT** a '1' as in *1st*

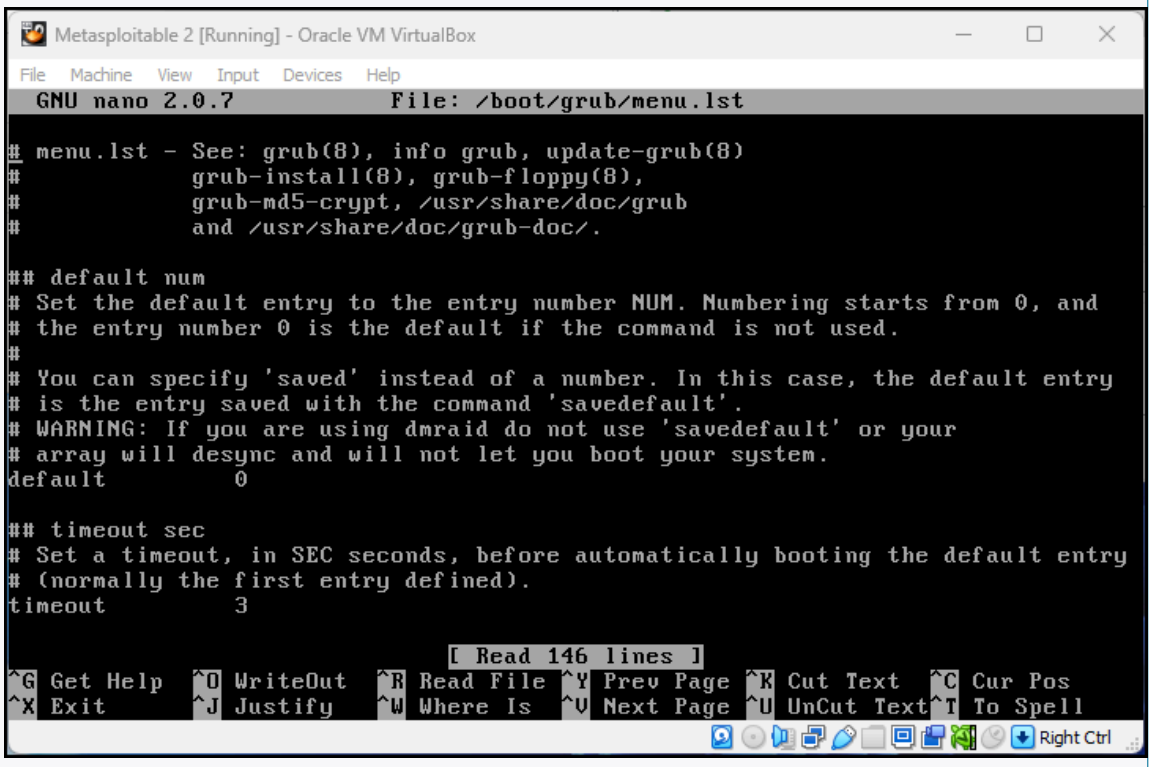


Figure 16 – menu.lst file opened in nano

This will open the grub boot configuration file called menu.lst

4.10. Use the arrow keys to scroll down after the default options and stop at a line called ***kernel*** (highlighted in yellow)

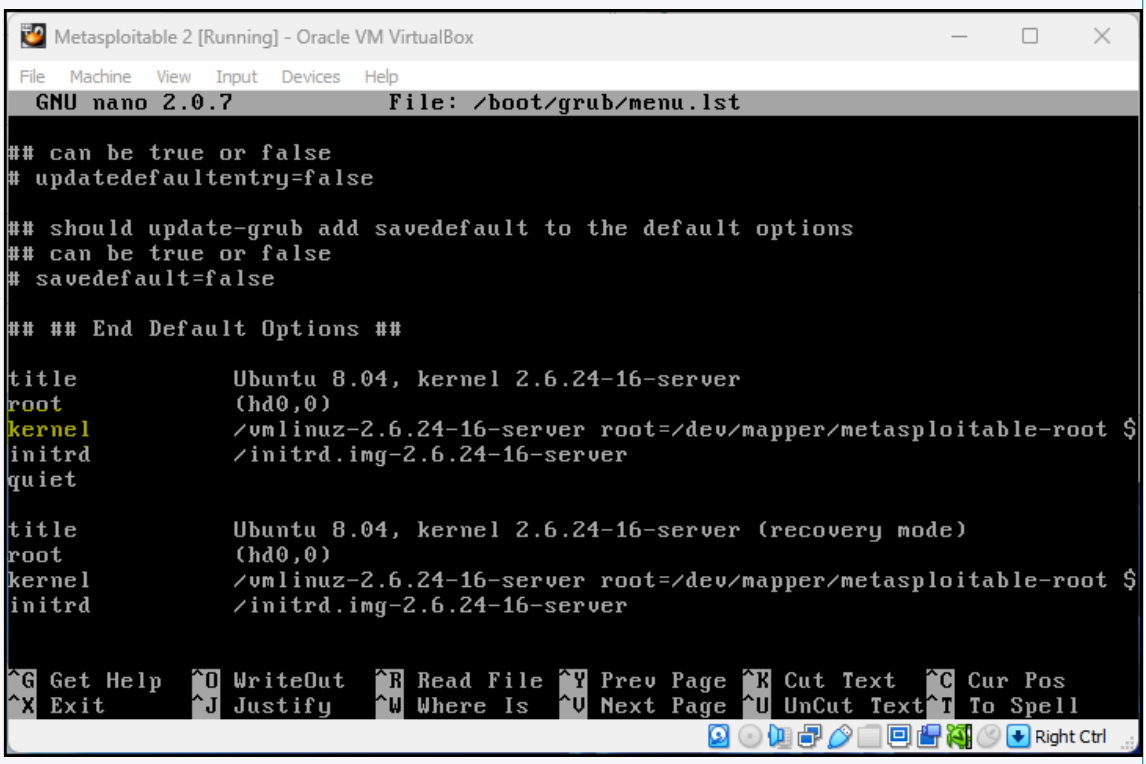


Figure 17 – kernel line in menu.lst file

4.11. Use the right arrow key to go to the end of this line and add –> ***noapic*** (highlighted in yellow) after the word splash

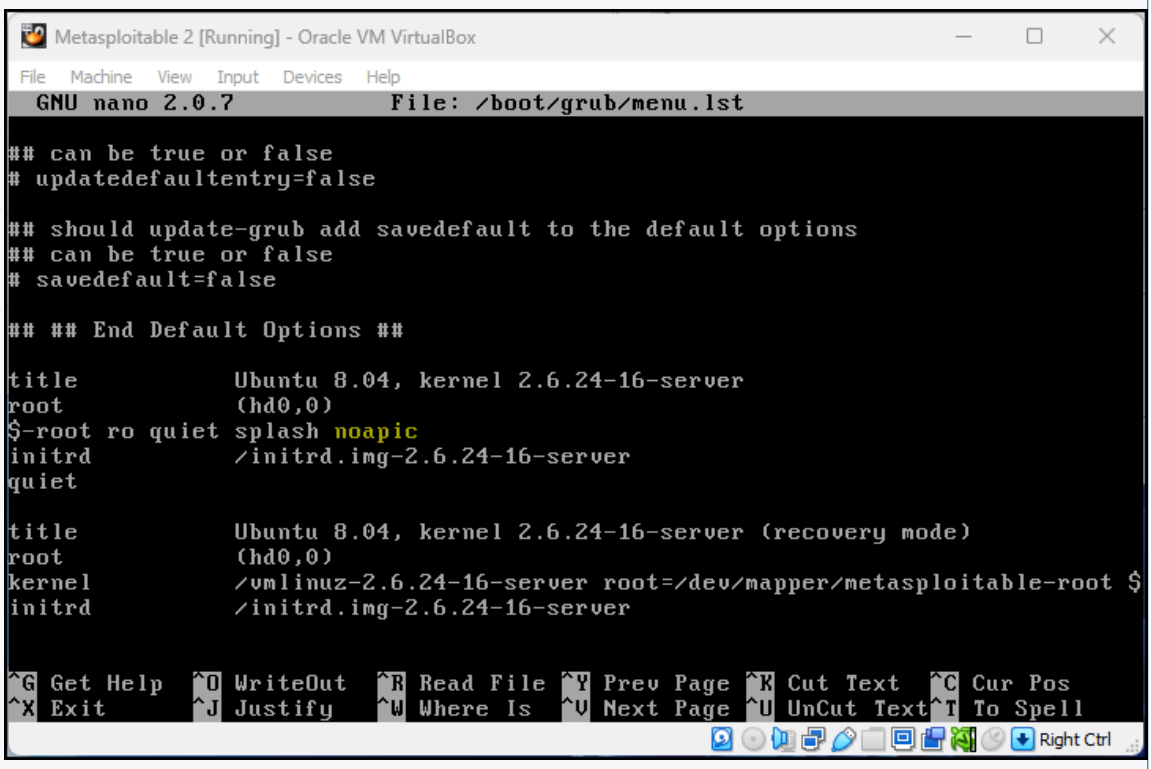


Figure 18 – noapic added to end of kernel line in menu.lst file

4.12. Save your change by pressing ^O Write Out (old school way of saying save)

4.13. Exit nano by pressing ^X Exit

4.14. Reboot the VM and it should boot without having to type noapic twice

Phase II – Installing Metasploitable3

Metasploitable3 comes in two flavors: Windows and Linux. Because of licensing issues, sharing Metasploitable 3 as a Windows VM is prohibitive, but you may build the image without violating any laws.

1. Visit Rapid7's GitHub page for metasploitable3 and read the README file. You will see lots of steps. We are going to follow the steps for building the VM using Windows

2. Install some supporting software

2.1. Install Packer

2.1.1. Download the precompiled binary (AMD64) for Windows 11 here

2.1.2. Once downloaded, extract it from the zip file. We are extracting all the supporting software files to the Downloads folder

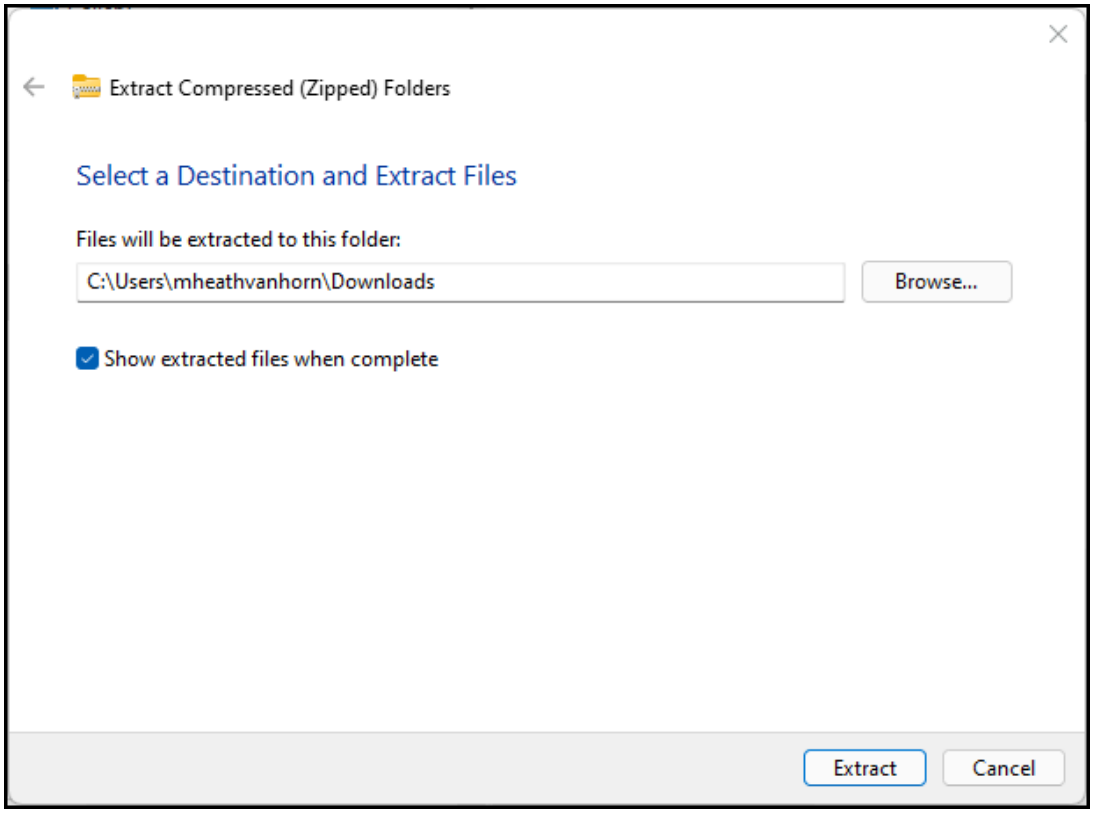


Figure 19 – Extract the downloaded file

2.1.3. In the Windows Start menu type “environment variables” and click on the menu item when it appears

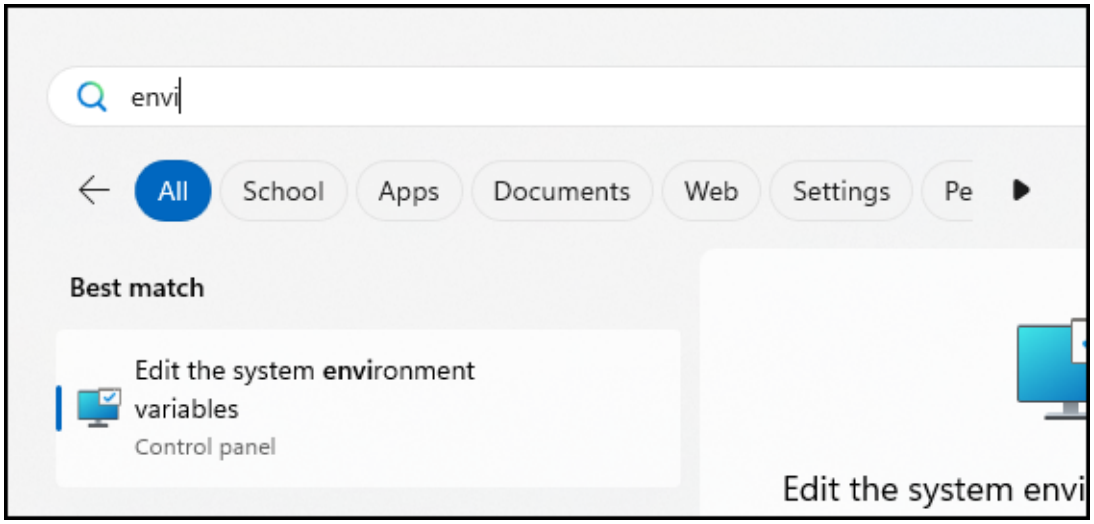


Figure 20 – Search environment variables

2.1.4. Click on the ***Environment Variables*** button

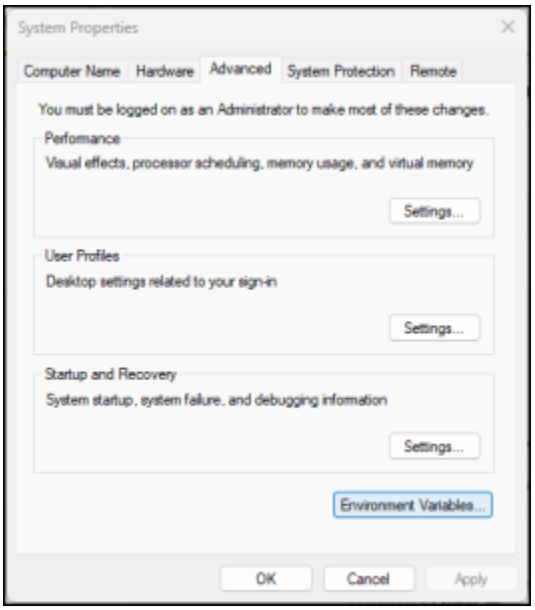


Figure 21 – System Properties Window

2.1.5. Scroll down to Path and click on ***edit***

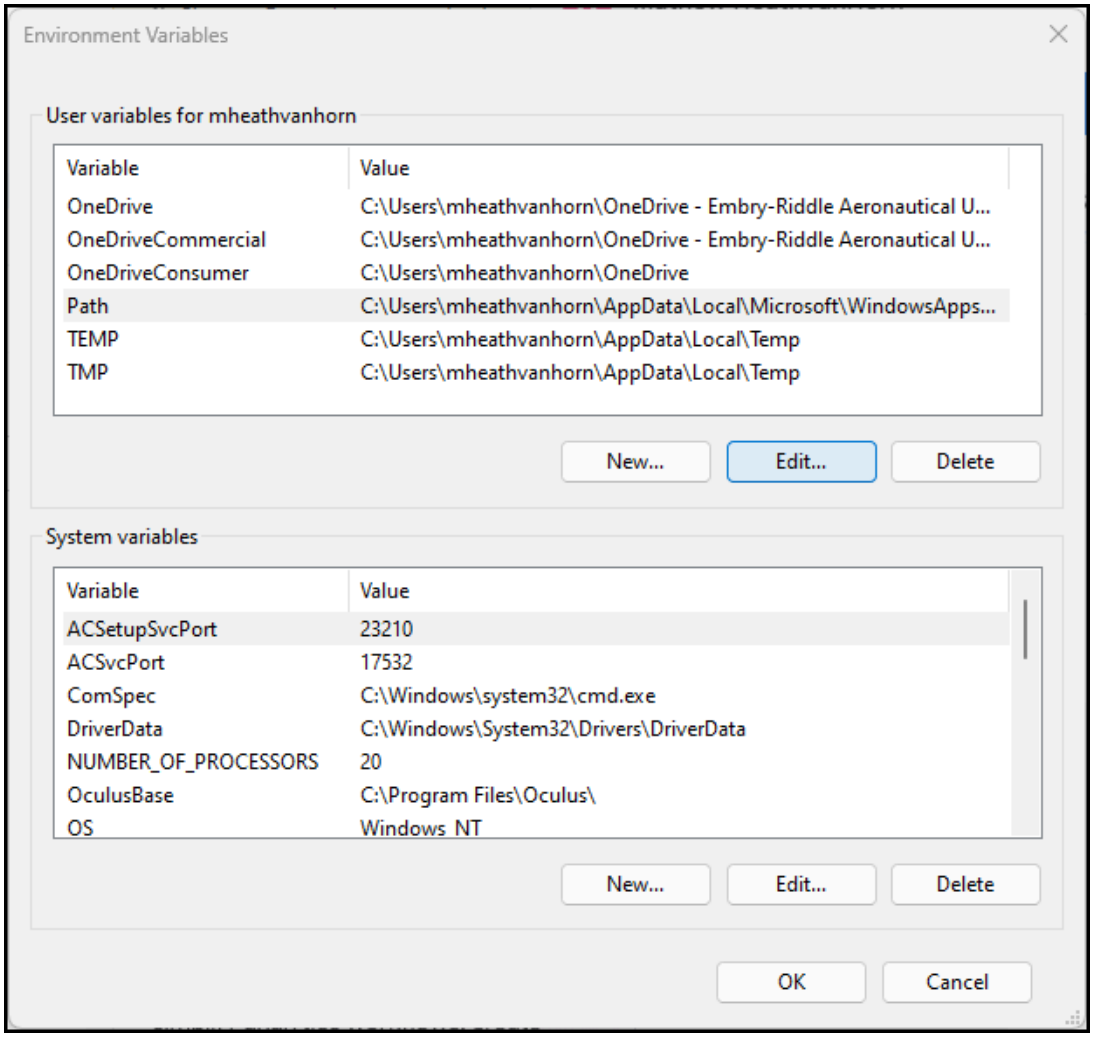


Figure 22 – Environment Variables Window

2.1.6. Click on ***new*** then ***browse*** then click on the downloads folder

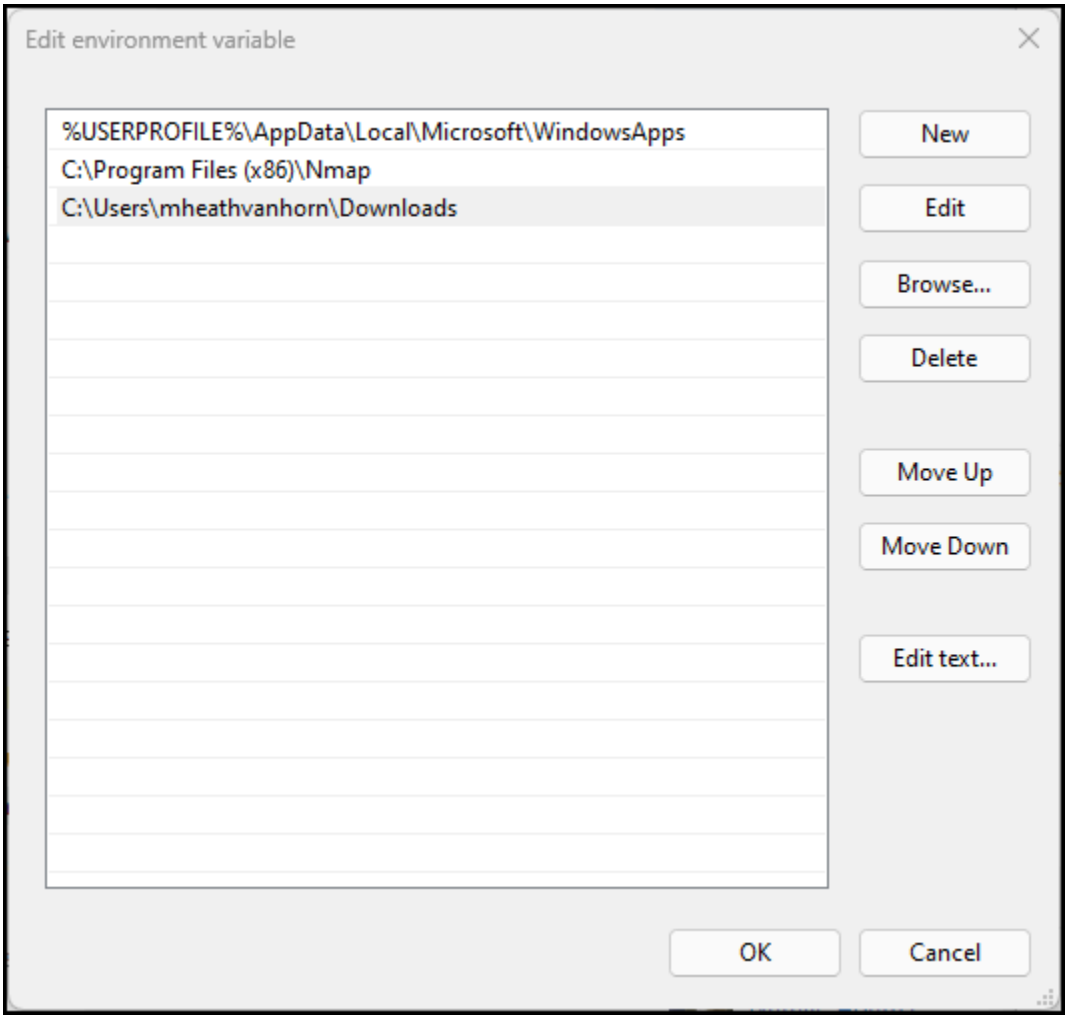


Figure 23 – Adding a folder to the path variable

2.1.7. Click ***ok*** until the system properties menu closes

2.1.8. Open a new PowerShell window for the changes to take effect

2.1.9. Type ***packer*** (highlighted in yellow) and you should get a list of available commands. This means Packer is working

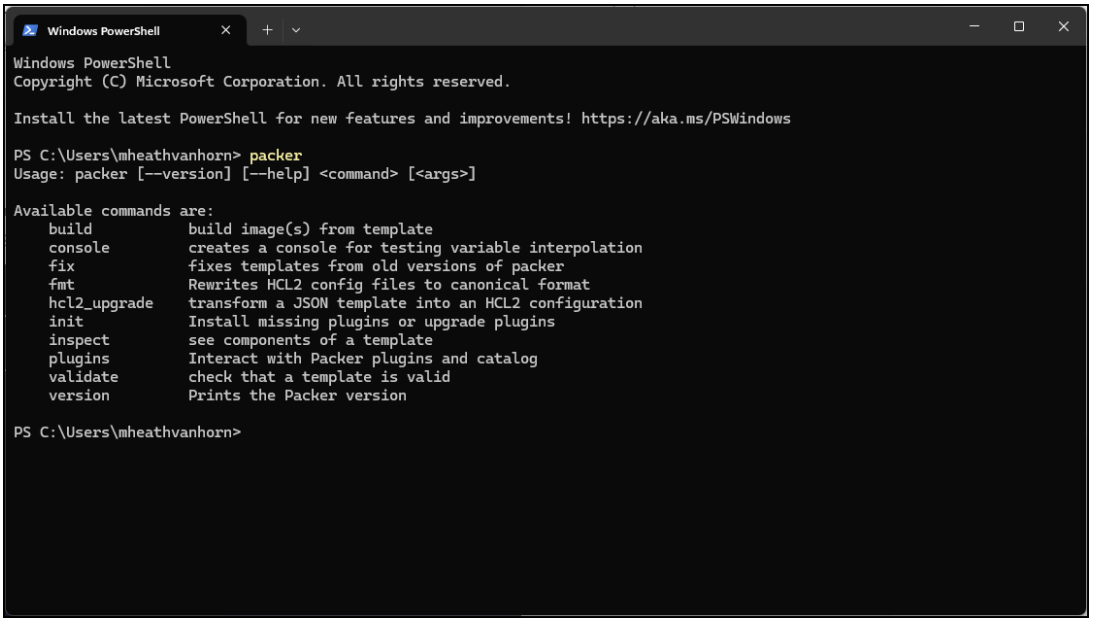


Figure 24 – Image of packer working

2.2. Install Vagrant

2.2.1. Visit the Vagrant downloads page and download the appropriate package

2.2.2. Once downloaded, you can click on the file and install it like any other Windows program

2.2.3. Restart the Computer

2.2.4. Open Windows PowerShell

2.2.5. Type ***vagrant*** to see a menu of commands

2.2.6. Create a new vagrant environment by typing

```
vagrant init
```

2.2.7. Install the vagrant reload plugin that allows the reloading of VMs as they are being created by typing

```
vagrant plugin install vagrant-reload
```

2.2.8. Create a new vagrant box by typing

```
vagrant box add hashicorp/bionic64
```

2.2.9. When asked, choose ***option 2*** for VirtualBox

```
PS C:\Users\mheathvanhorn> vagrant box add hashicorp/bionic64
==> box: Loading metadata for box 'hashicorp/bionic64'
    box: URL: https://vagrantcloud.com/api/v2/vagrant/hashicorp/bionic64
This box can work with multiple providers! The providers that it
can work with are listed below. Please review the list and choose
the provider you will be working with.

1) hyperv
2) virtualbox
3) vmware_desktop

Enter your choice: 2
==> box: Adding box 'hashicorp/bionic64' (v1.0.282) for provider: virtualbox
    box: Downloading: https://vagrantcloud.com/hashicorp/boxes/bionic64/versions/1.0.282/providers/virtual
box/unknown/vagrant.box
    box:
==> box: Successfully added box 'hashicorp/bionic64' (v1.0.282) for 'virtualbox'!
PS C:\Users\mheathvanhorn>
```

Figure 25 – Select option 2 for VirtualBox

2.3. Install both versions of metsasploitable (Windows and Linux) by doing the following:

2.3.1. Create a new directory by typing

```
mkdir metasploitable3-workspace
```

2.3.2. Navigate to the directory by typing

```
cd metasploitable-workspace
```

2.3.3. Extract both versions of metasploitable3 by typing the following (all on one line)

```
Invoke-WebRequest -Uri "https://raw.githubusercontent.com/
rapid7/metasploitable3/master/Vagrantfile" -OutFile "Vagrantfile"
```

2.3.4. Start the building of the VMs by typing

```
vagrant up
```

Figure 26 – This could take awhile

2.4. This will take a while, but when it is finished, you will have two new VMs in VirtualBox. The credentials for both machines is:
USER: ***vagrant***
PASSWORD: ***vagrant***

3. Now add them to the GNS3 environment for future use

End of Lab

PART II

BUILDING AN ENTERPRISE NETWORK

CHAPTER 14

Your First Network

MATHEW J. HEATH VAN HORN, PHD

A user's experience with network devices varies widely. Gamers are probably familiar with port forwarding on their home router, but may not understand why these actions are needed. Others may have never been interested in how the magic network box in their home works.

This exercise helps all users get familiar with using the GNS3 environment. We used a typical home environment because some users have probably encountered this type of setup before. However, our testers found that even the most novice users could follow these instructions to gain an understanding of using GNS3.

We had to take some liberties since many home network devices are all-in-one solutions, but learners should focus on using the tools and not how close it resembles "real life".

Estimated time for completion: 15 minutes

LEARNING OBJECTIVES

- Create a typical home network in the GNS3 network
- Become familiar with labels and symbols in the GNS3 network

PREREQUISITES

- Chapter 2 – Setting Up a GNS3 Environment
- Chapter 4 – Installing an OpenWRT Router
- Chapter 6 – Adding a Virtual Machine to GNS3

DELIVERABLES

- One screenshot of the completed GNS3 Environment

RESOURCES

- N/A

CONTRIBUTORS AND TESTERS

- Jacob M. Christensen, Cybersecurity Student, ERAU-Prescott
- Sawyer Hanson, Cybersecurity Student, ERAU-Prescott
- Julian Romano, Cybersecurity Student, ERAU-Prescott
- Quinton D. Heath Van Horn, 7th Grade
- David Reese, Mathematics Student, SUNY Brockport
- Cody Shinkyu Park, Honeywell Software Engineer, ERAU-Prescott Alumni
- Dante Rocca, Cybersecurity Student, ERAU-Prescott

Phase I – Background Information

This LAB is designed to resemble a typical home network. Some adjustments will need to be made because you are unable to see the device or the wireless signals. So, we will take this opportunity to familiarize you with the setup and then you can add your own devices.

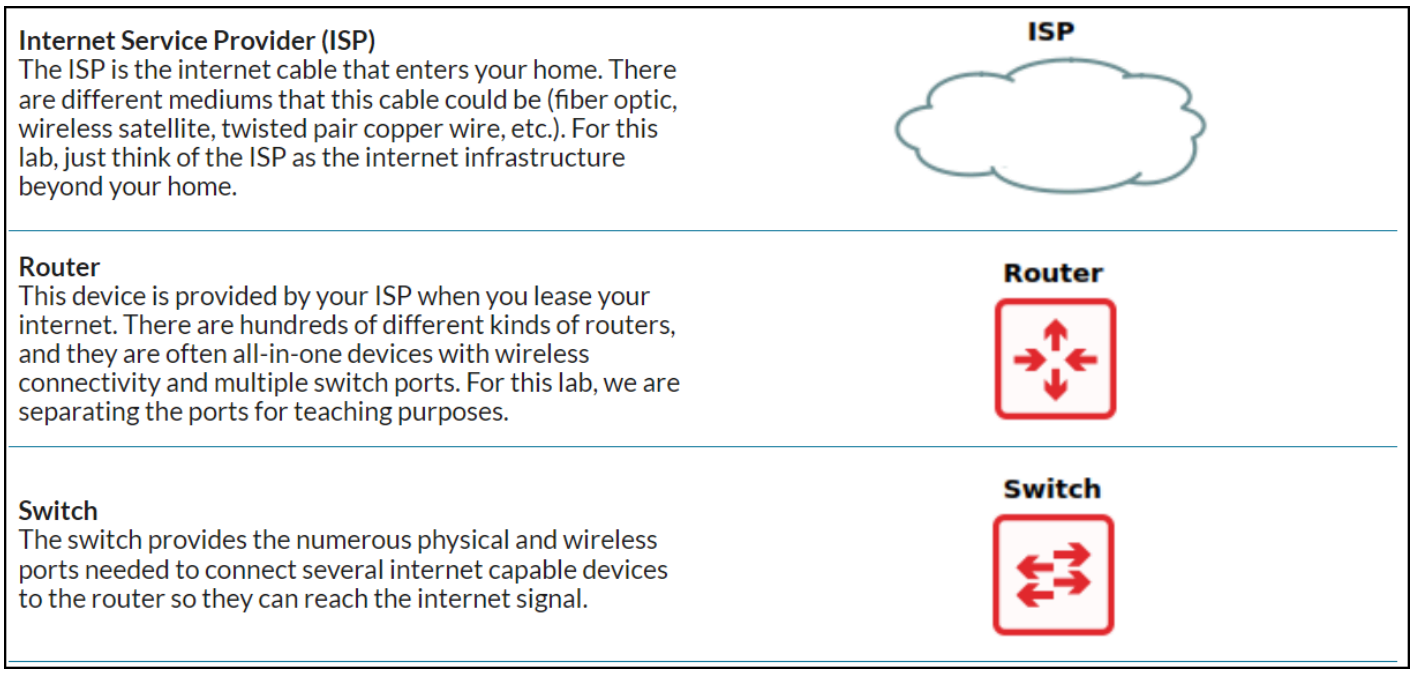


Figure 1 – Explanation of Symbols

In this lab, the typical all-in-one device is split apart for better visualization. Look at the figures below to compare a typical home environment with our lab environment. You can trace the route of the internet from the ISP to the PC in both images.

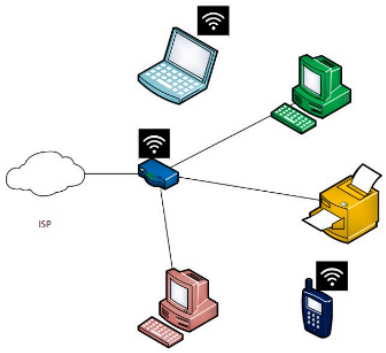
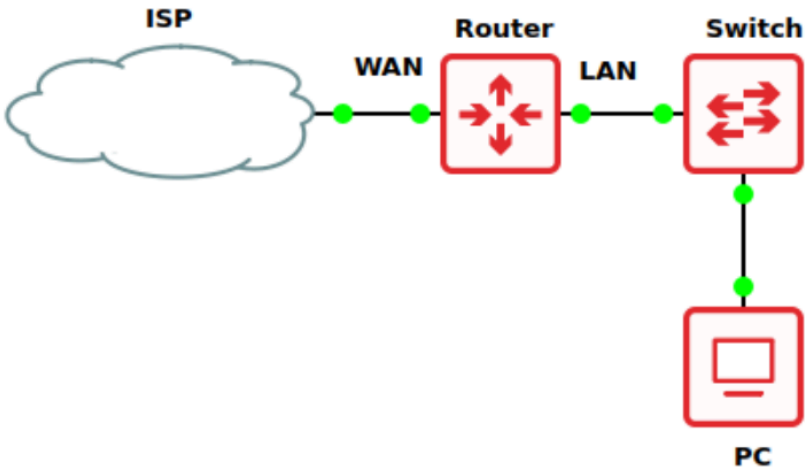
Typical all-in-one device that provides routing and switching for wired and wireless devices.	Our lab environment. The all-in-one device is split into a separate router and switch.
 *Typical home network environment*	 *Simple GNS3 network*

Figure 2 – Picture of final outcome

Phase II – Setup

These steps are necessary to prepare the playing field. There a quite a few of them, but they are simple. Complete them one at a time and you will have a working learning environment in no time.

1. Start the GNS3 application

2. Create a new project

    2.1. Start by clicking *File* > *New Blank Project* on the upper left-hand side

    2.2. For this example, we are using the name **LAB_01**

    2.3. Select *OK*

3. Under the **Servers Summary** section in the bottom-left-hand corner of the workspace, verify that both the host machine and GNS3 VM are connected by looking for the two green lights