SETTING UP A PERSONALIZED MALWARE ANALYSIS LAB

Utilizing Diverse Cybersecurity Tools on Microsoft Windows and Linux Operating System on Oracle VirtualBox

DOCUMENT CONTROL

Change Record

Date	Author	Version	Change Reference
13-Aug-2024	Adeyinka Freeman	Draft 1a	
19-Aug-2024	Adeyinka Freeman	Draft 1b	Draft 1a

Reviewers

Name	Contact
N/A	N/A

Repository

Copy No.	Name	Location	URL
1	Document Repository	GitHUB	https://github.com/kayfreeman/MyGRC-Journey/

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

This document provides a comprehensive guide for setting up a personalized malware analysis lab using Oracle VirtualBox. It outlines the configuration and utilization of various cybersecurity tools on both Microsoft Windows and Linux operating systems.

The goal is to create a robust environment for conducting in-depth malware analysis, facilitating the identification and mitigation of potential threats. By leveraging on the use of Oracle VirtualBox, this setup allows for isolated and secure testing, ensuring that the host system I would be using remains unaffected by malicious activities.

This document serves as a valuable resource for cybersecurity professionals and enthusiasts seeking to enhance their skills and capabilities in malware analysis.

1.1.1 BACKGROUND

With the technological landscape evolving rapidly it is critical that cybersecurity experts have a platform for them to analyze and understand malware as it spreads and causes significant risk to the business objectives of any organization. Malware or malicious systems are tools used in compromising the system integrity of an organization. As cybercriminals develop increasingly sophisticated malware, the demand for skilled analysts who can dissect and neutralize these threats has grown.

The need for a malware analysis lab provides a controlled environment where analysts can safely examine and reverse-engineer malicious code. Such a lab typically includes multiple virtual machines (VMs) running different operating systems, enabling analysts to observe how malware behaves across various platforms.

This document therefore guides the reader through the process of setting up a malware analysis lab using Oracle VirtualBox. It covers the installation and configuration of necessary software, the deployment of VMs, and the integration of essential cybersecurity tools.

1.1.2 TOOL USED

Tools used for the setup and implementation of the malware lab includes: -

- Microsoft Office 365 (Provided by RMIT University)
- Oracle VirtualBox (from Oracle).
- Parrot OS
- Kali Linux OS/Suite
- Microsoft OS Ver 10.
- Browser of choice deployed/setup – Tor, Brave, Google Chrome and Internet Explorer/Edge
- Mandiant Flare VM

2 VIRTUALIZATION AND CONTAINERS

2.1.1 Virtualization and Virtualization Servers

Virtualization is a technology that allows multiple virtual instances or environments to run on a single physical hardware system. This approach maximizes hardware utilization, enhances resource efficiency, and provides greater flexibility in managing IT infrastructure. Virtualization is fundamental in setting up a personalized malware analysis lab as it enables the creation of isolated environments for safe testing and analysis of malicious software.

2.1.1.1 Concept of Virtualization

Virtualization abstracts physical hardware resources to create multiple virtual machines (VMs) that operate as if they were independent physical systems. This abstraction layer allows for:

- **Resource Optimization:** Multiple VMs can run on a single physical server, sharing CPU, memory, and storage resources, thus reducing hardware costs.
- **Isolation:** Each VM operates independently, which is crucial for safely analysing malware without risk to the host system.
- **Flexibility and Scalability:** VMs can be easily created, modified, or deleted, allowing rapid deployment and adjustment of testing environments.

2.1.1.2 Types of Virtualizations

Virtualization is a technique that allows you to create and manage virtual instances of resources or systems, rather than relying solely on physical hardware. There are several types of virtualizations, each serving different purposes and using various techniques. Here’s a breakdown of the main types:

2.1.1.2.1 Hardware Virtualization

- **Type 1 Hypervisor (Bare metal):**

Description: Runs directly on the host's hardware, without an underlying operating system. It manages guest virtual machines (VMs) directly.

Examples: VMware ESXi, Microsoft Hyper-V, Xen.

Use Case: Enterprise environments where high performance and security are critical.

- **Type 2 Hypervisor (Hosted):**

Description: Runs on top of a conventional operating system. It relies on the host OS to manage hardware resources.

Examples: Oracle VirtualBox, VMware Workstation, Parallels Desktop.

Use Case: Development, testing, and desktop virtualization.

2.1.1.2.2 Operating System Virtualization

- **Containers:**

Description: Virtualizes the operating system to run isolated user-space instances (containers) on a single OS kernel. Containers share the host OS but run applications in isolated environments.

Examples: Docker, LXC (Linux Containers), Kubernetes (for orchestration).

Use Case: Microservices architecture, lightweight application isolation, and deployment.

2.1.1.2.3 Network Virtualization

- **Network Functions Virtualization (NFV)**:

Description: Virtualizes network services that traditionally ran on dedicated hardware appliances (like firewalls and load balancers) to run as virtual instances on standard servers.

Examples: Virtualized Network Functions (VNFs), OpenStack Neutron.

Use Case: Modernizing network infrastructure and improving scalability and flexibility.

- **Software-Defined Networking (SDN):**

Description: Abstracts the network control plane from the data plane, allowing for centralized management and programmability of network behaviour.

Examples: OpenFlow, Cisco ACI.

Use Case: Dynamic network management, improved network automation.

2.1.1.2.4 Storage Virtualization

Description: Abstracts and pools physical storage resources into a virtualized storage pool, making it easier to manage and allocate storage resources.

Examples: Storage Area Networks (SANs), Network-Attached Storage (NAS) with virtualization capabilities, software-defined storage solutions.

Use Case: Efficient storage management, consolidation, and increased flexibility.

2.1.1.2.5 Desktop Virtualization

- **Virtual Desktop Infrastructure (VDI):**

Description: Hosts desktop environments on a central server and delivers them to users' devices over a network.

Examples: VMware Horizon, Citrix Virtual Apps and Desktops.

Use Case: Centralized desktop management, remote access to desktops.

2.1.1.2.6 Application Virtualization

Description: Abstracts applications from the underlying operating system, allowing applications to run in isolated environments or be delivered over the network.

Examples: Microsoft App-V, VMware ThinApp.

Use Case: Simplified application deployment, compatibility with different OS versions.

Each type of virtualization provides unique benefits and is suited for different scenarios, depending on the needs of the organization or individual.

For our malware lab to be setup and configured, the Virtual machine to be used is: -

- Oracle VirtualBox which is a type 2 hosted hypervisor hardware virtualization

2.1.1.3 Benefits of the Tools we used for the Malware Analysis Lab

- **Oracle VirtualBox**

1. Cost-Effective:

- Oracle VirtualBox is a free and open-source virtualization solution, making it accessible for both individual and enterprise users without incurring additional costs.

2. Cross-Platform Compatibility:

- VirtualBox supports multiple hosts operating systems, including Windows, macOS, Linux, and Solaris, providing flexibility in choosing the environment for your malware analysis lab.

3. Robust Feature Set:

- It offers a comprehensive set of features, including snapshots, seamless mode, shared folders, and hardware virtualization support, which are essential for creating and managing isolated virtual environments efficiently.

4. Community and Support:

- Being widely used, VirtualBox has an active community and extensive documentation, making it easier to troubleshoot issues and get support when needed.
- **Kali Linux**

1. Pre-Installed Security Tools:

- Kali Linux comes with a vast array of pre-installed security tools specifically designed for penetration testing, forensics, and malware analysis, saving time and effort in tool installation and configuration.

2. Customizability:

- It allows users to customize the environment according to their specific needs, making it highly versatile for various cybersecurity tasks.

3. Community and Documentation:

- Kali Linux is well-documented and supported by an active community, providing a wealth of resources for learning and troubleshooting.

4. Regular Updates:

- Maintained by Offensive Security, Kali Linux receives regular updates and new tool integrations, ensuring that users have access to the latest security tools and features.
- **Windows VM**

1. Realistic Environment:

- Since a significant amount of malware targets Windows systems, having a Windows VM in the lab provides a realistic environment to analyse malware behaviour and its impact on widely used operating systems.

2. Software Compatibility:

- Many malware analysis tools and applications are designed to run on Windows, making it essential to have a Windows VM for comprehensive analysis.

3. Diverse Threat Landscape:

- The Windows operating system encounters a wide variety of threats, allowing analysts to study different types of malwares, from ransomware to trojans and beyond.

- **FLARE VM**

1. Specialized Malware Analysis Tools:

- FLARE VM is a Windows-based distribution specifically designed for malware analysis, reverse engineering, and incident response. It comes pre-configured with tools like IDA Pro, OllyDbg, and Ghidra, which are essential for deep malware analysis.

2. Comprehensive Analysis Environment:

- By combining a variety of tools in one environment, FLARE VM provides a comprehensive platform for performing static and dynamic analysis, unpacking, debugging, and reverse engineering of malware.

3. Community and Updates:

- Maintained by FireEye's FLARE team, FLARE VM is regularly updated with new tools and features, ensuring that analysts have access to the latest resources for effective malware analysis.
- **Compelling Reason**

  By using Oracle VirtualBox to set up a malware analysis lab with Kali Linux, Windows, and FLARE VM, we create a versatile, cost-effective, and comprehensive environment tailored for in-depth malware analysis. VirtualBox provides the necessary isolation and resource management, while Kali Linux offers a rich set of pre-installed security tools. The Windows VM, complemented by FLARE VM, ensures a realistic and specialized environment for analysing malware in the most targeted operating system. This setup not only maximizes our analytical capabilities but also ensures we are equipped to handle a wide range of malware threats effectively.

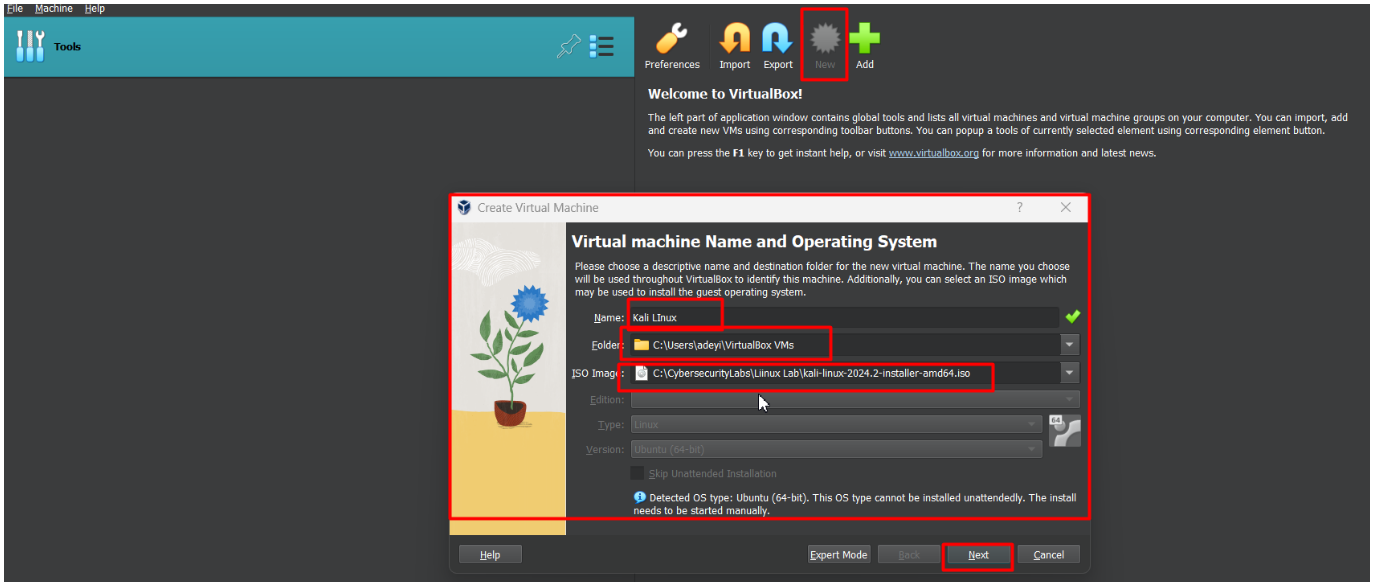
In conclusion, our proposed Laboratory will play a pivotal role in creating a secure and flexible environment for malware analysis. By leveraging these technologies, we can conduct thorough investigations and develop effective defences against emerging threats.

3 SETTING UP KALI LINUX

3.1. Setting Up Kali Linux Using Command Line Interface

To setup Kali Linux OS using the command line interface, we take the following steps displayed below.

- We first create the folder name, the file path and ISO file.



Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

Create Virtual Machine

Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: Kali LInux

Folder: C:\Users\adeyi\VirtualBox VMs

ISO Image: C:\CybersecurityLabs\Liinux Lab\kali-linux-2024.2-installer-amd64.iso

Edition:

Type: Linux

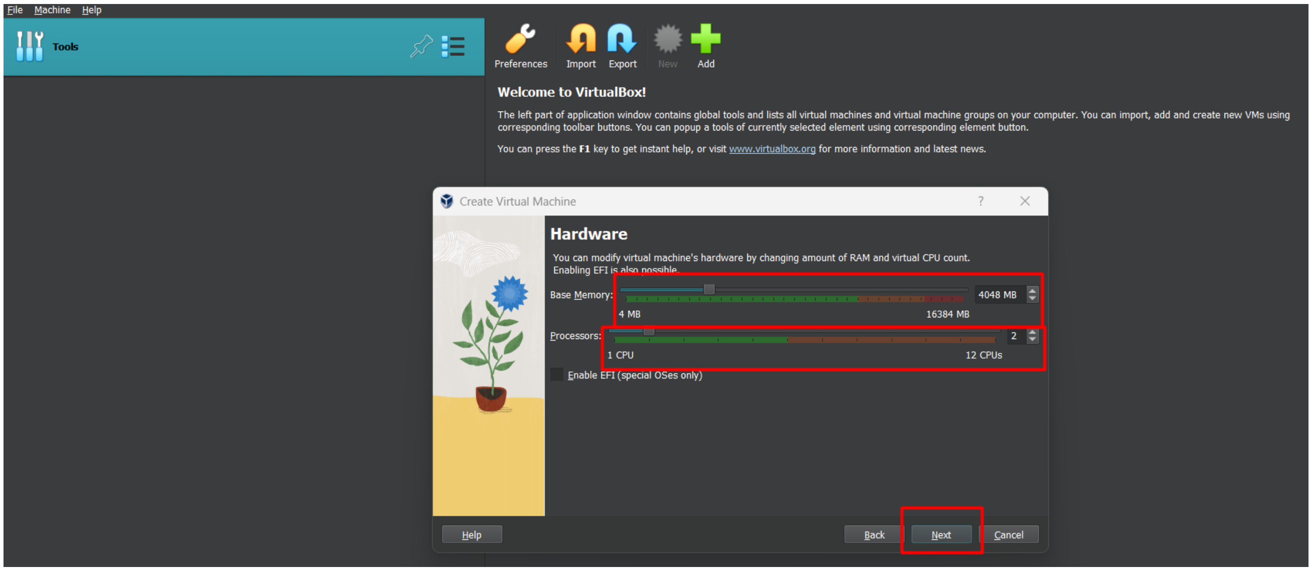
Version: Ubuntu (64-bit)

☐ Skip Unattended Installation

Detected OS type: Ubuntu (64-bit). This OS type cannot be installed unattendedly. The install needs to be started manually.

Figure 1: - Defining Kali Linux OS on Oracle Virtual Box - CLI

- We specify the ideal RAM memory (4048MB), the processor (2 CPU), and the “Next” option



Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

Create Virtual Machine

Hardware

You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

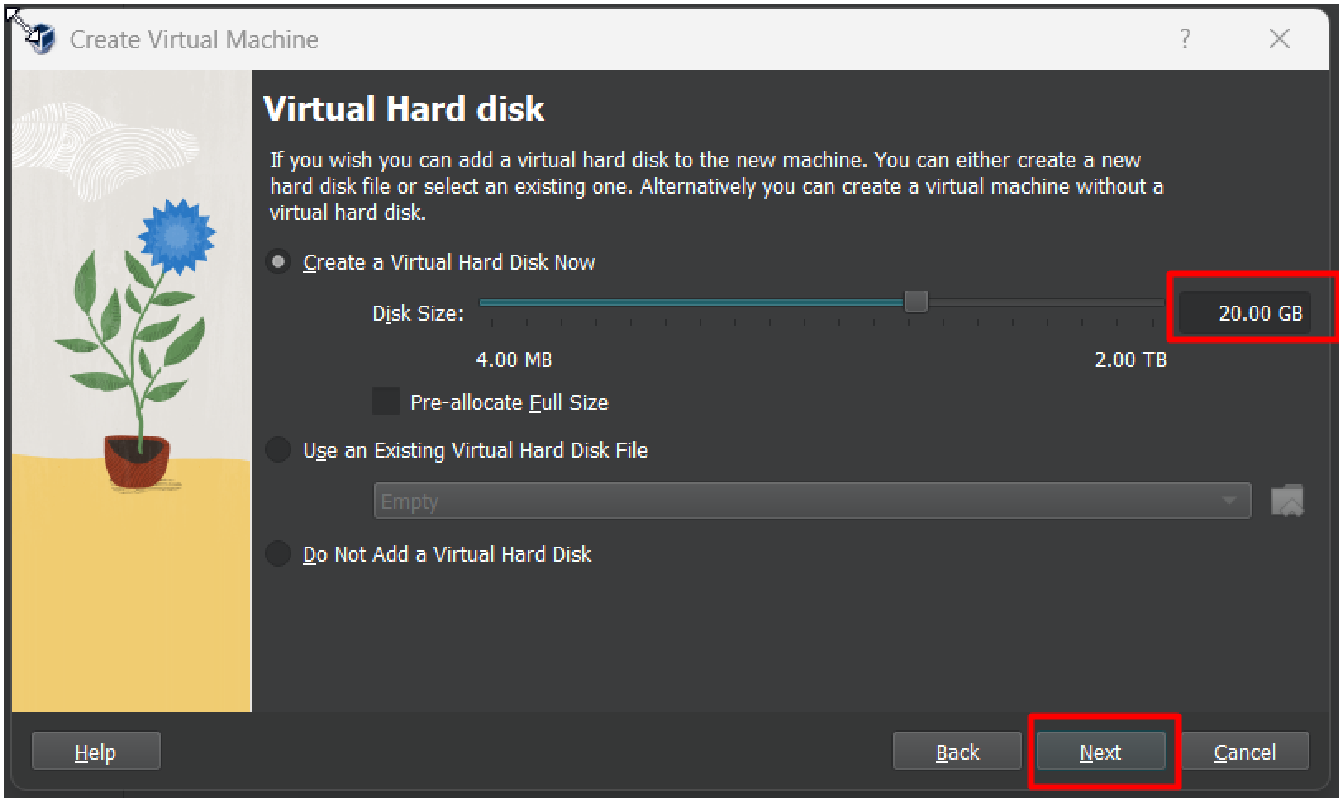
Base Memory: 4048 MB (4 MB – 16384 MB)

Processors: 2 (1 CPU – 12 CPUs)

☐ Enable EFI (special OSes only)

Figure 2: Defining Kali Linux base memory and processor on Oracle Virtual Box - CLI

- We define our virtual hard disk space (20GB) and complete the setup by clicking on the "Next" option



Create Virtual Machine

Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

● Create a Virtual Hard Disk Now

Disk Size: 20.00 GB

4.00 MB 2.00 TB

□ Pre-allocate Full Size

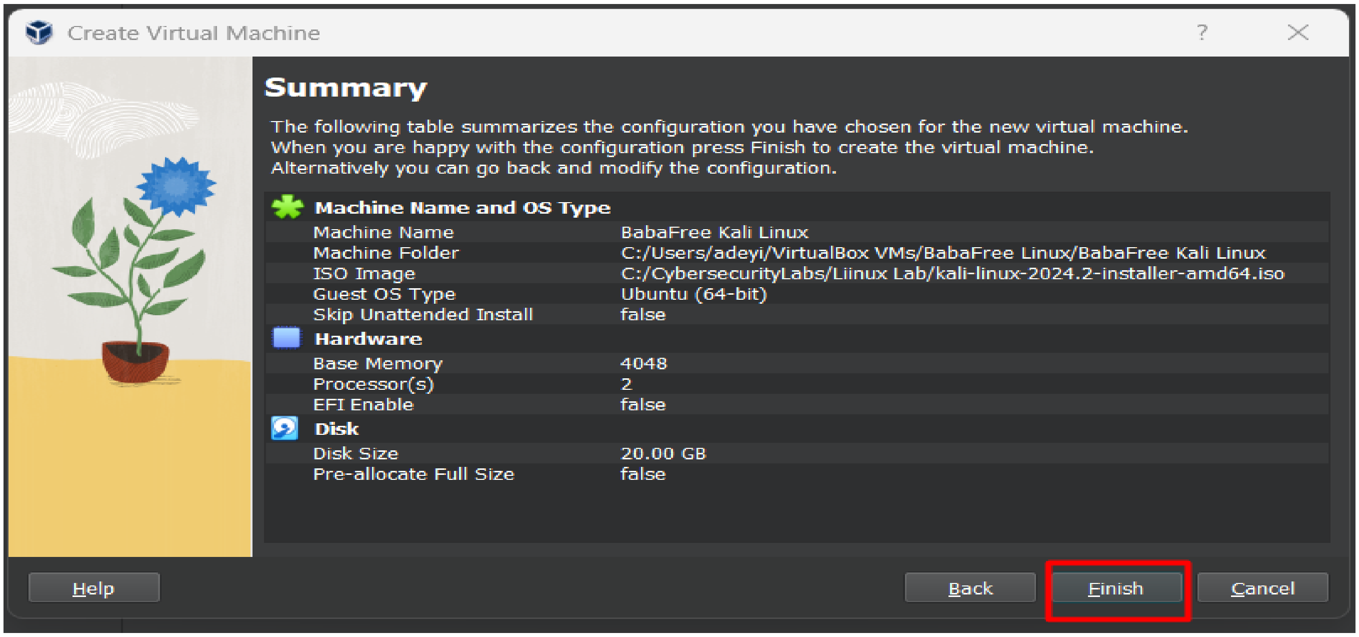
○ Use an Existing Virtual Hard Disk File

Empty

○ Do Not Add a Virtual Hard Disk

Figure 3: - Defining Kali Linux Virtual Hard disk on Oracle Virtual Box – CLI

- The finish button completes the setup and provides us with a Kali Linux platform on Oracle VirtualBox



Create Virtual Machine

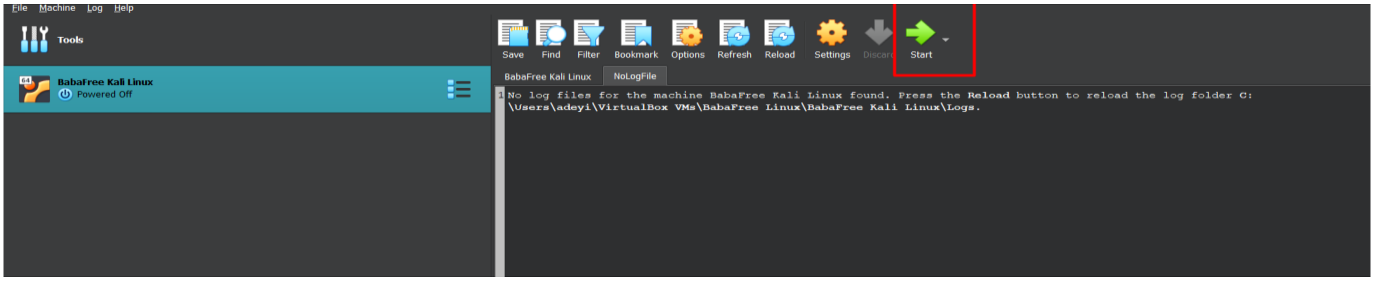
Summary

The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

Machine Name and OS Type	
Machine Name	BabaFree Kali Linux
Machine Folder	C:/Users/adeyi/VirtualBox VMs/BabaFree Linux/BabaFree Kali Linux
ISO Image	C:/CybersecurityLabs/Liinux Lab/kali-linux-2024.2-installer-amd64.iso
Guest OS Type	Ubuntu (64-bit)
Skip Unattended Install	false
Hardware	
Base Memory	4048
Processor(s)	2
EFI Enable	false
Disk	
Disk Size	20.00 GB
Pre-allocate Full Size	false

Figure 4: - Reviewing Kali Linux's Summary Setup on Oracle Virtual Box – CLI

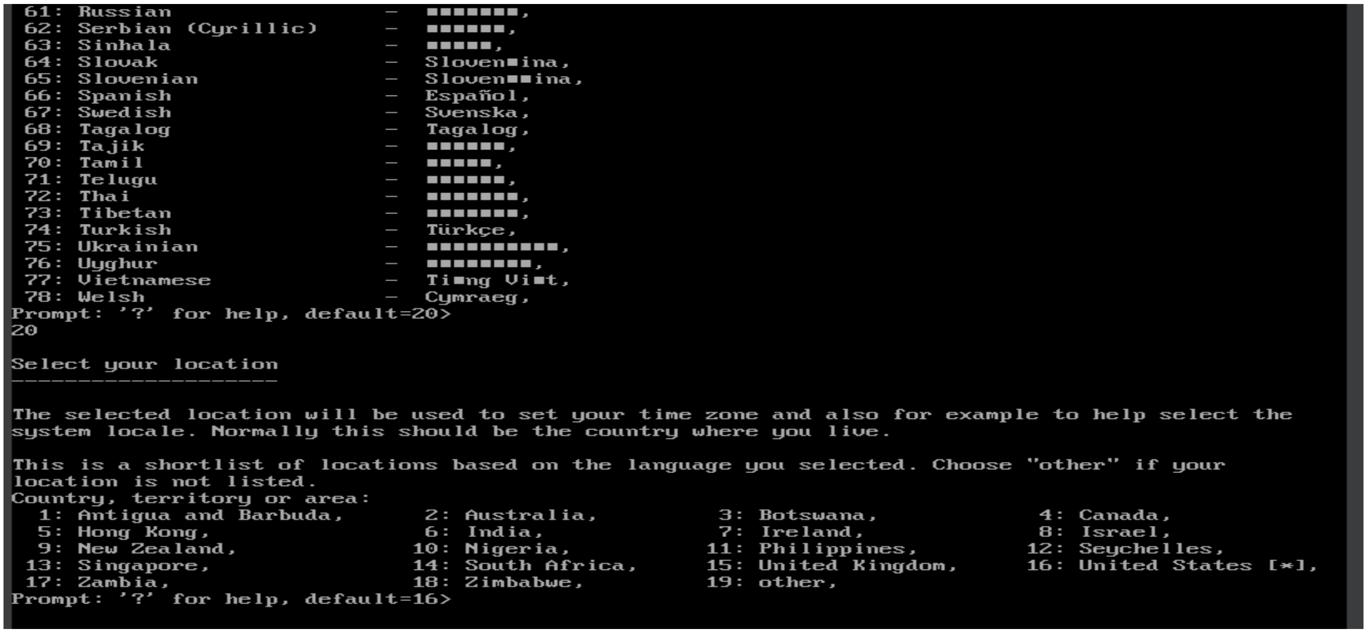
- The “Start” button initiates Kali Linux



```
No log files for the machine BabaFree Kali Linux found. Press the Reload button to reload the log folder C:
\Users\adeyi\VirtualBox VMs\BabaFree Linux\BabaFree Kali Linux\Logs.
```

Figure 5: - Launching Kali Linux setup on Oracle Virtual Box – CLI

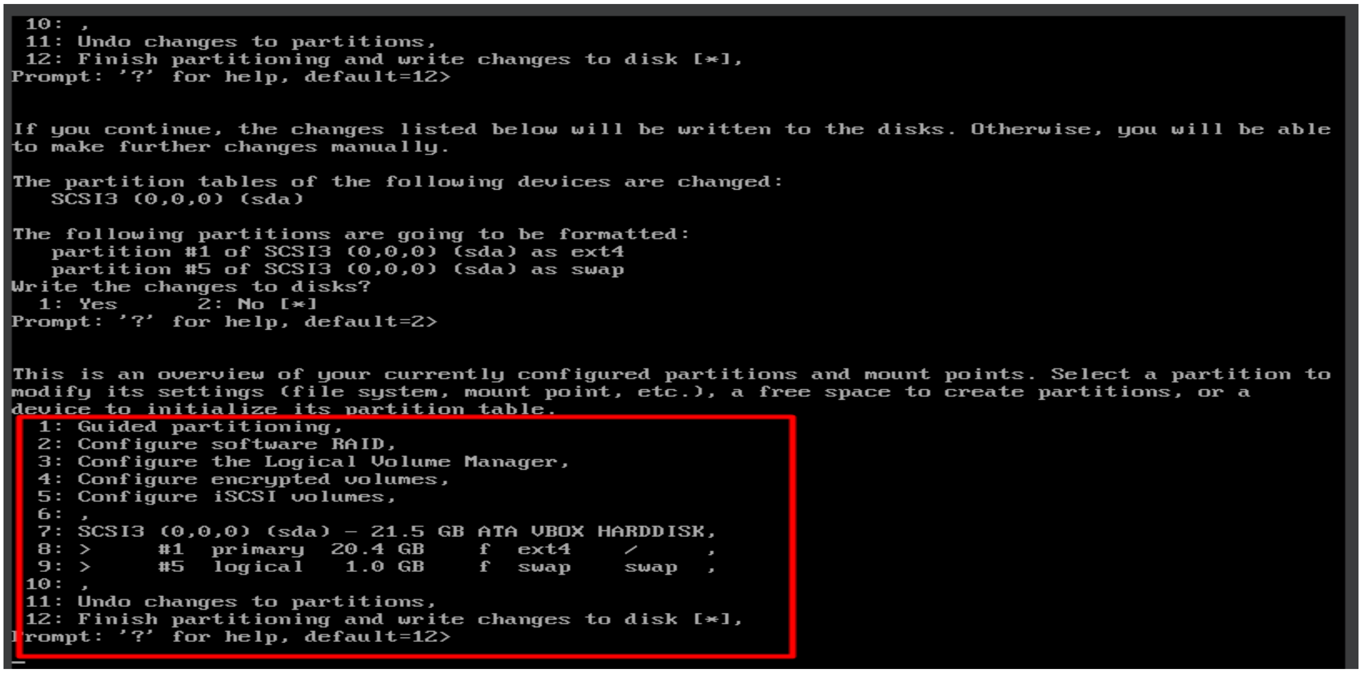
- We setup our Linux environment by configuring our preferred language, keyboard type, username, password and location



```
  61: Russian                  -  ■■■■■■■■,
  62: Serbian (Cyrillic)       -  ■■■■■■■,
  63: Sinhala                  -  ■■■■■,
  64: Slovak                   -  Sloven■ina,
  65: Slovenian                -  Sloven■■ina,
  66: Spanish                  -  Español,
  67: Swedish                  -  Svenska,
  68: Tagalog                  -  Tagalog,
  69: Tajik                    -  ■■■■■■■,
  70: Tamil                    -  ■■■■■,
  71: Telugu                   -  ■■■■■■■,
  72: Thai                     -  ■■■■■■■■,
  73: Tibetan                  -  ■■■■■■■■,
  74: Turkish                  -  Türkçe,
  75: Ukrainian                -  ■■■■■■■■■■■,
  76: Uyghur                   -  ■■■■■■■■■,
  77: Vietnamese               -  Ti■ng Vi■t,
  78: Welsh                    -  Cymraeg,
Prompt: '?' for help, default=20>
20

Select your location
--------------------

The selected location will be used to set your time zone and also for example to help select the
system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if your
location is not listed.
Country, territory or area:
   1: Antigua and Barbuda,      2: Australia,          3: Botswana,           4: Canada,
   5: Hong Kong,                6: India,              7: Ireland,            8: Israel,
   9: New Zealand,             10: Nigeria,           11: Philippines,       12: Seychelles,
  13: Singapore,               14: South Africa,      15: United Kingdom,    16: United States [*],
  17: Zambia,                  18: Zimbabwe,          19: other,
Prompt: '?' for help, default=16>
```

Figure 6: - Configuring our Kali Linux setup on Oracle Virtual Box – CLI - 1

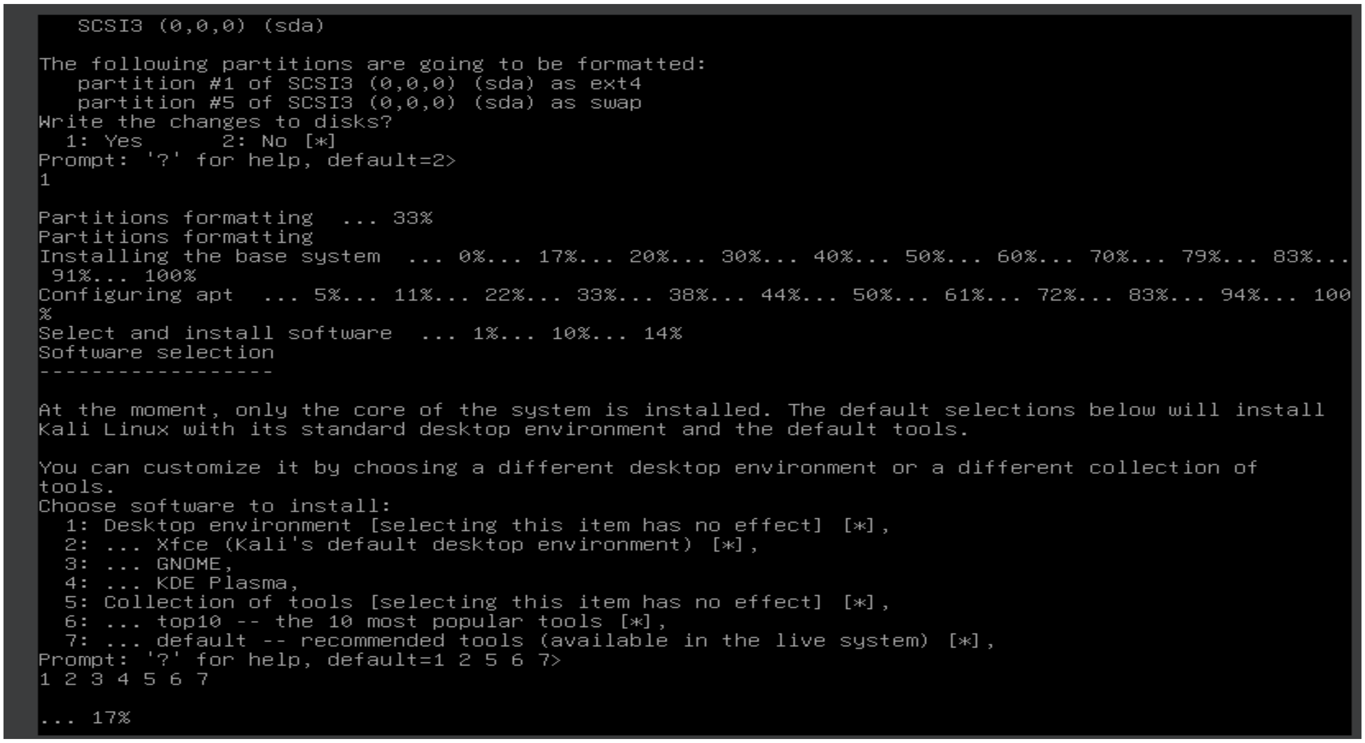
- Complete partition to disk or any preferred configuration of choice



```
 10: ,
 11: Undo changes to partitions,
 12: Finish partitioning and write changes to disk [*],
Prompt: '?' for help, default=12>


If you continue, the changes listed below will be written to the disks. Otherwise, you will be able
to make further changes manually.

The partition tables of the following devices are changed:
   SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:
   partition #1 of SCSI3 (0,0,0) (sda) as ext4
   partition #5 of SCSI3 (0,0,0) (sda) as swap
Write the changes to disks?
  1: Yes       2: No [*]
Prompt: '?' for help, default=2>


This is an overview of your currently configured partitions and mount points. Select a partition to
modify its settings (file system, mount point, etc.), a free space to create partitions, or a
device to initialize its partition table.
  1: Guided partitioning,
  2: Configure software RAID,
  3: Configure the Logical Volume Manager,
  4: Configure encrypted volumes,
  5: Configure iSCSI volumes,
  6: ,
  7: SCSI3 (0,0,0) (sda) - 21.5 GB ATA VBOX HARDDISK,
  8: >     #1  primary  20.4 GB     f  ext4     /      ,
  9: >     #5  logical   1.0 GB     f  swap     swap   ,
 10: ,
 11: Undo changes to partitions,
 12: Finish partitioning and write changes to disk [*],
Prompt: '?' for help, default=12>
_
```

Figure 7:- Configuring our Kali Linux setup on Oracle Virtual Box – CLI – 2

- We select the software options we intend to install.



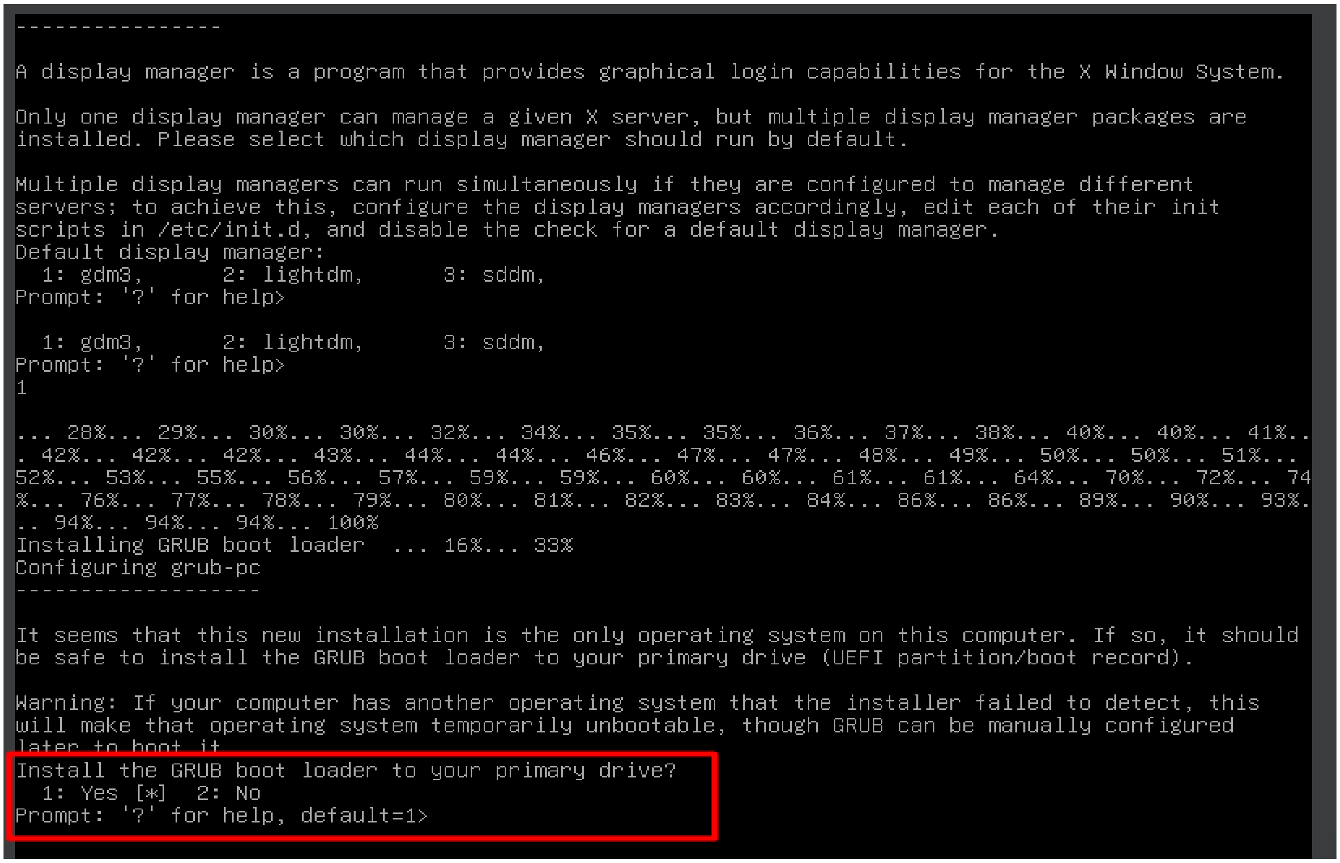
```
   SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:
   partition #1 of SCSI3 (0,0,0) (sda) as ext4
   partition #5 of SCSI3 (0,0,0) (sda) as swap
Write the changes to disks?
  1: Yes       2: No [*]
Prompt: '?' for help, default=2>
1

Partitions formatting  ... 33%
Partitions formatting
Installing the base system  ... 0%... 17%... 20%... 30%... 40%... 50%... 60%... 70%... 79%... 83%...
 91%... 100%
Configuring apt  ... 5%... 11%... 22%... 33%... 38%... 44%... 50%... 61%... 72%... 83%... 94%... 100
%
Select and install software  ... 1%... 10%... 14%
Software selection
------------------

At the moment, only the core of the system is installed. The default selections below will install
Kali Linux with its standard desktop environment and the default tools.

You can customize it by choosing a different desktop environment or a different collection of
tools.
Choose software to install:
  1: Desktop environment [selecting this item has no effect] [*],
  2: ... Xfce (Kali's default desktop environment) [*],
  3: ... GNOME,
  4: ... KDE Plasma,
  5: Collection of tools [selecting this item has no effect] [*],
  6: ... top10 -- the 10 most popular tools [*],
  7: ... default -- recommended tools (available in the live system) [*],
Prompt: '?' for help, default=1 2 5 6 7>
1 2 3 4 5 6 7

... 17%
```

Figure 8: - Configuring our Kali Linux setup on Oracle Virtual Box – CLI - 3

For display, we select option 1 GDM3 (GNOME Display Manager) which is the default display manager for GNOME-based Linux distributions. It provides a polished and user-friendly interface with support for accessibility features, custom theming, and integration with the GNOME desktop environment. We also have the LightDM which is a lightweight, cross-desktop display manager that is simple to configure and has a small footprint. It is a good choice for users who prioritize system performance and minimalism over extensive customization options.

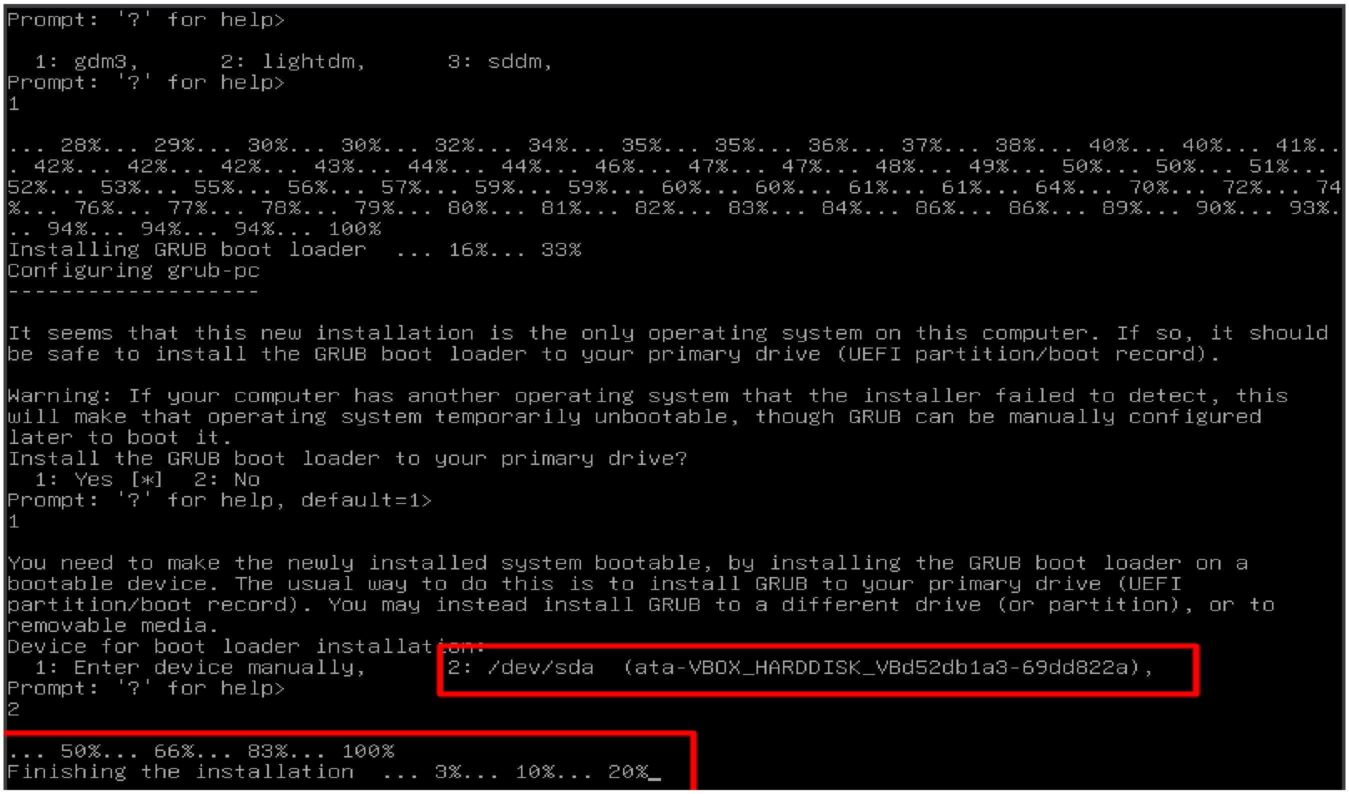
SDDM (Simple Desktop Display Manager) is the default display manager for KDE Plasma-based distributions. It offers a modern, Qt-based interface with support for themes and user customization. SDDM is well-integrated with the KDE desktop environment.

In summary, GDM3 is best suited for GNOME users, LightDM is a good choice for users who value simplicity and performance, and SDDM is the preferred option for KDE Plasma users. The "better" display manager depends on the user's desktop environment, desired features, and system resource requirements.



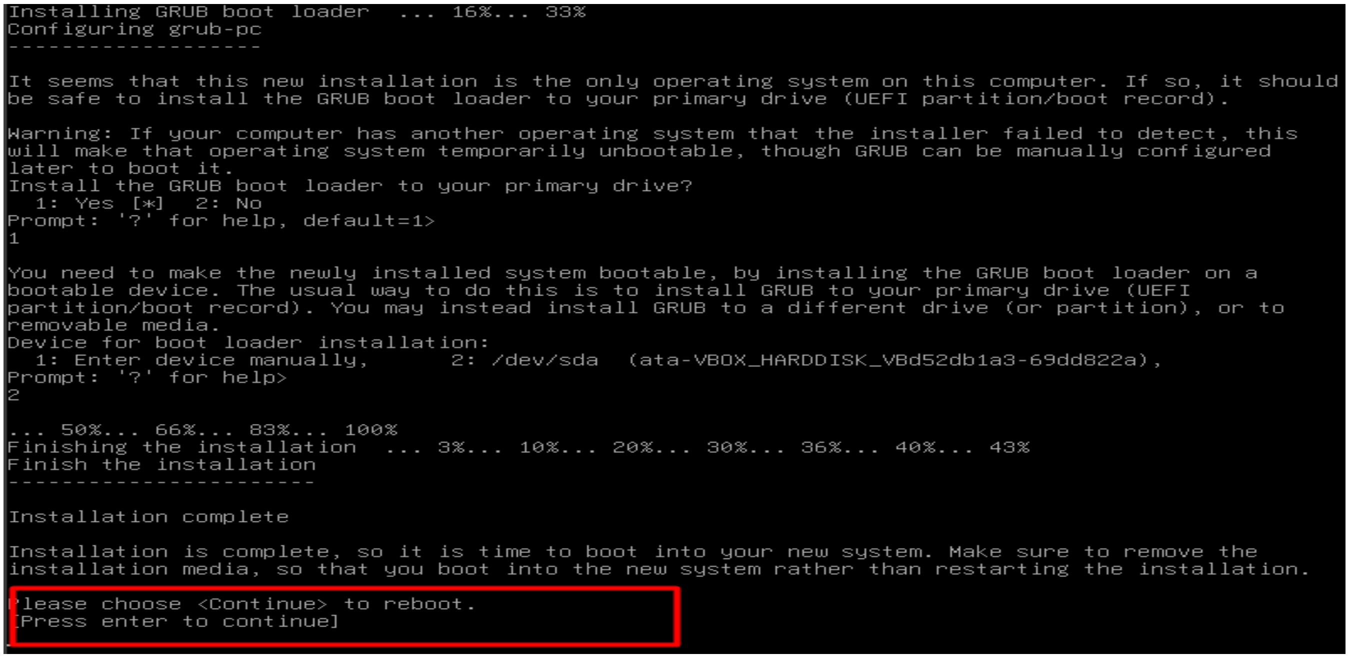
```
----------------

A display manager is a program that provides graphical login capabilities for the X Window System.

Only one display manager can manage a given X server, but multiple display manager packages are
installed. Please select which display manager should run by default.

Multiple display managers can run simultaneously if they are configured to manage different
servers; to achieve this, configure the display managers accordingly, edit each of their init
scripts in /etc/init.d, and disable the check for a default display manager.
Default display manager:
  1: gdm3,      2: lightdm,      3: sddm,
Prompt: '?' for help>

  1: gdm3,      2: lightdm,      3: sddm,
Prompt: '?' for help>
1

... 28%... 29%... 30%... 30%... 32%... 34%... 35%... 35%... 36%... 37%... 38%... 40%... 40%... 41%..
. 42%... 42%... 42%... 43%... 44%... 44%... 46%... 47%... 47%... 48%... 49%... 50%... 50%... 51%...
52%... 53%... 55%... 56%... 57%... 59%... 59%... 60%... 60%... 61%... 61%... 64%... 70%... 72%... 74
%... 76%... 77%... 78%... 79%... 80%... 81%... 82%... 83%... 84%... 86%... 86%... 89%... 90%... 93%.
.. 94%... 94%... 94%... 100%
Installing GRUB boot loader  ... 16%... 33%
Configuring grub-pc
-------------------

It seems that this new installation is the only operating system on this computer. If so, it should
be safe to install the GRUB boot loader to your primary drive (UEFI partition/boot record).

Warning: If your computer has another operating system that the installer failed to detect, this
will make that operating system temporarily unbootable, though GRUB can be manually configured
later to boot it.
Install the GRUB boot loader to your primary drive?
  1: Yes [*]  2: No
Prompt: '?' for help, default=1>
```

Figure 9: - Configuring our Kali Linux setup on Oracle Virtual Box – CLI - 4



```
Prompt: '?' for help>

  1: gdm3,       2: lightdm,       3: sddm,
Prompt: '?' for help>
1

... 28%... 29%... 30%... 30%... 32%... 34%... 35%... 35%... 36%... 37%... 38%... 40%... 40%... 41%..
. 42%... 42%... 42%... 43%... 44%... 44%... 46%... 47%... 47%... 48%... 49%... 50%... 50%... 51%...
52%... 53%... 55%... 56%... 57%... 59%... 59%... 60%... 60%... 61%... 61%... 64%... 70%... 72%... 74
%... 76%... 77%... 78%... 79%... 80%... 81%... 82%... 83%... 84%... 86%... 86%... 89%... 90%... 93%.
.. 94%... 94%... 94%... 100%
Installing GRUB boot loader  ... 16%... 33%
Configuring grub-pc
-------------------

It seems that this new installation is the only operating system on this computer. If so, it should
be safe to install the GRUB boot loader to your primary drive (UEFI partition/boot record).

Warning: If your computer has another operating system that the installer failed to detect, this
will make that operating system temporarily unbootable, though GRUB can be manually configured
later to boot it.
Install the GRUB boot loader to your primary drive?
  1: Yes [*]  2: No
Prompt: '?' for help, default=1>
1

You need to make the newly installed system bootable, by installing the GRUB boot loader on a
bootable device. The usual way to do this is to install GRUB to your primary drive (UEFI
partition/boot record). You may instead install GRUB to a different drive (or partition), or to
removable media.
Device for boot loader installation:
  1: Enter device manually,      2: /dev/sda  (ata-VBOX_HARDDISK_VBd52db1a3-69dd822a),
Prompt: '?' for help>
2

... 50%... 66%... 83%... 100%
Finishing the installation  ... 3%... 10%... 20%_
```

Figure 10: - Configuring our Kali Linux setup on Oracle Virtual Box – CLI – 5



```
Installing GRUB boot loader  ... 16%... 33%
Configuring grub-pc
-------------------

It seems that this new installation is the only operating system on this computer. If so, it should
be safe to install the GRUB boot loader to your primary drive (UEFI partition/boot record).

Warning: If your computer has another operating system that the installer failed to detect, this
will make that operating system temporarily unbootable, though GRUB can be manually configured
later to boot it.
Install the GRUB boot loader to your primary drive?
  1: Yes [*]  2: No
Prompt: '?' for help, default=1>
1

You need to make the newly installed system bootable, by installing the GRUB boot loader on a
bootable device. The usual way to do this is to install GRUB to your primary drive (UEFI
partition/boot record). You may instead install GRUB to a different drive (or partition), or to
removable media.
Device for boot loader installation:
  1: Enter device manually,      2: /dev/sda  (ata-VBOX_HARDDISK_VBd52db1a3-69dd822a),
Prompt: '?' for help>
2

... 50%... 66%... 83%... 100%
Finishing the installation  ... 3%... 10%... 20%... 30%... 36%... 40%... 43%
Finish the installation
-----------------------

Installation complete

Installation is complete, so it is time to boot into your new system. Make sure to remove the
installation media, so that you boot into the new system rather than restarting the installation.

Please choose <Continue> to reboot.
[Press enter to continue]
```

Figure 11: - Configuring our Kali Linux setup on Oracle Virtual Box – CLI - 6

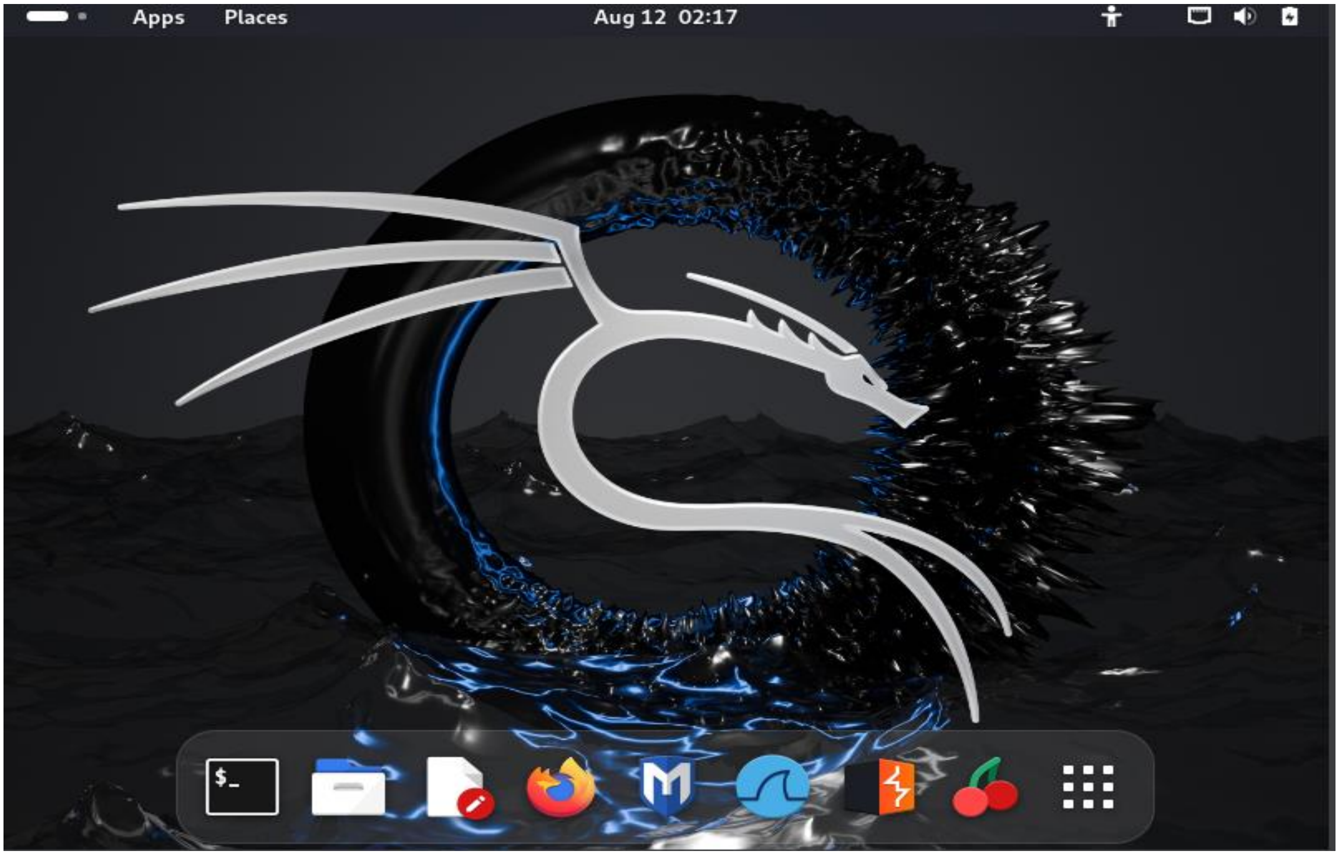


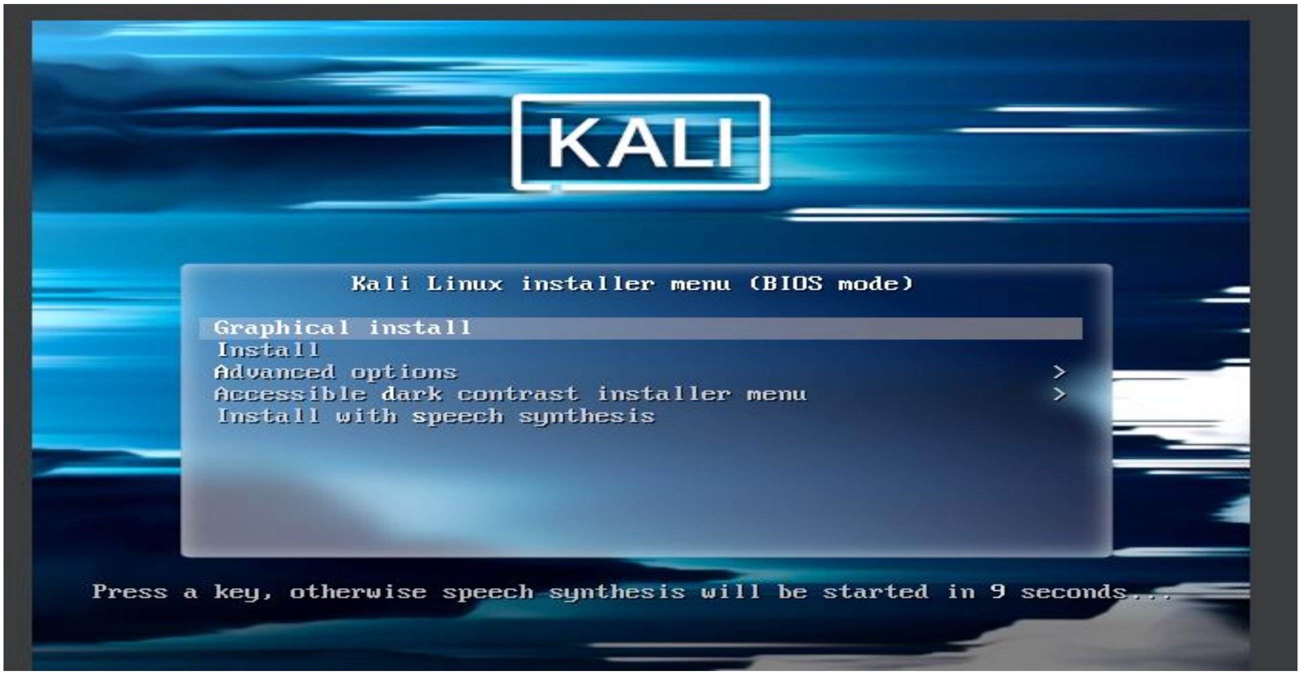
Figure 12: - Configuring our Kali Linux setup on Oracle Virtual Box – CLI - 7

3.2. Setting Up Kali Linux Using Graphical User Interface

Kali Linux is a widely recognized and powerful distribution tailored for penetration testing and cybersecurity research. Its rich suite of pre-installed tools makes it an ideal choice for a personalized malware analysis lab. While Kali Linux can be set up using various methods, employing the Graphical User Interface (GUI) provides a user-friendly approach that simplifies the installation process, particularly for those who prefer visual guidance over command-line interactions.

This section will guide you through the process of installing Kali Linux using its graphical installer, which streamlines the setup with intuitive prompts and options. By leveraging the GUI, users can more easily configure system settings, select package options, and manage disk partitions. The goal is to ensure that the installation is as straightforward and efficient as possible, setting up a robust environment for malware analysis and other cybersecurity tasks.

- We launch the Kali Linux platform on Oracle Virtual Box and select the “graphical install” option.



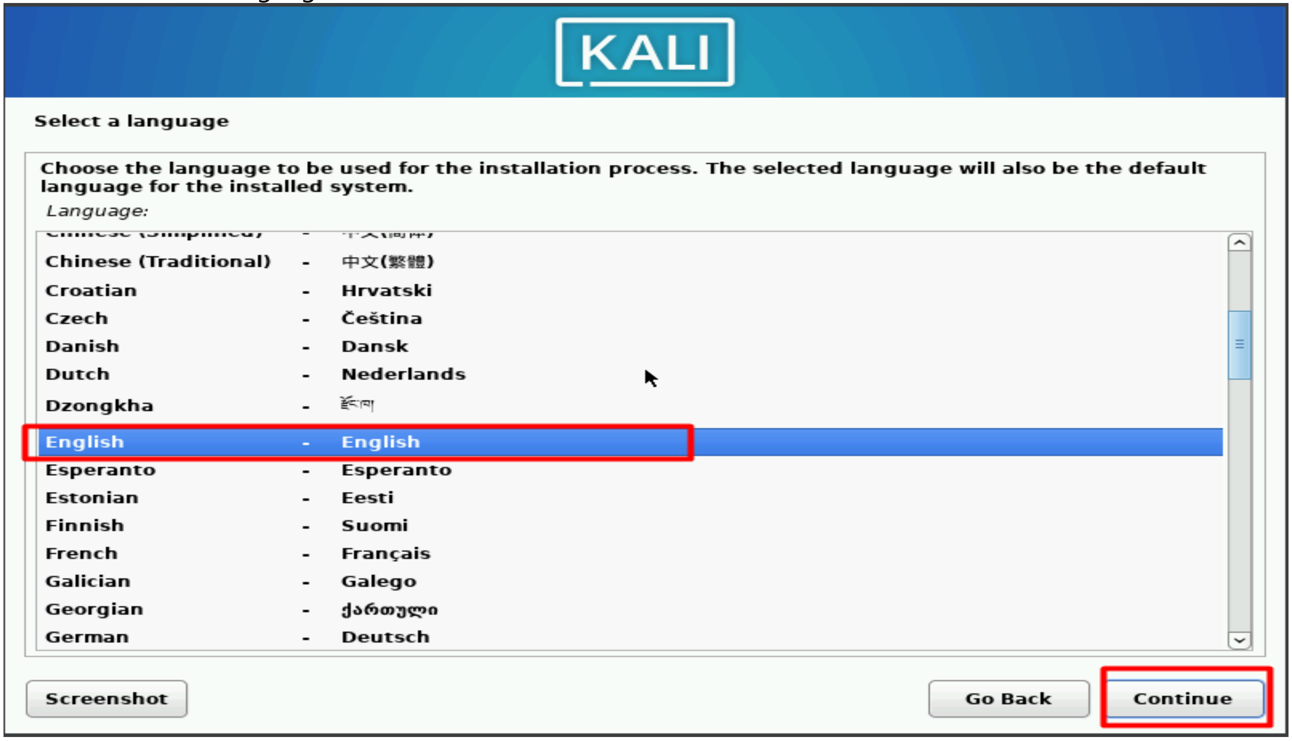
Kali Linux installer menu (BIOS mode)

KALI
Graphical install
Install
Advanced options >
Accessible dark contrast installer menu >
Install with speech synthesis

Press a key, otherwise speech synthesis will be started in 9 seconds...

Figure 13: - Setting up Kali Linux using the GUI

- Select the language of choice, and define the username



Select a language

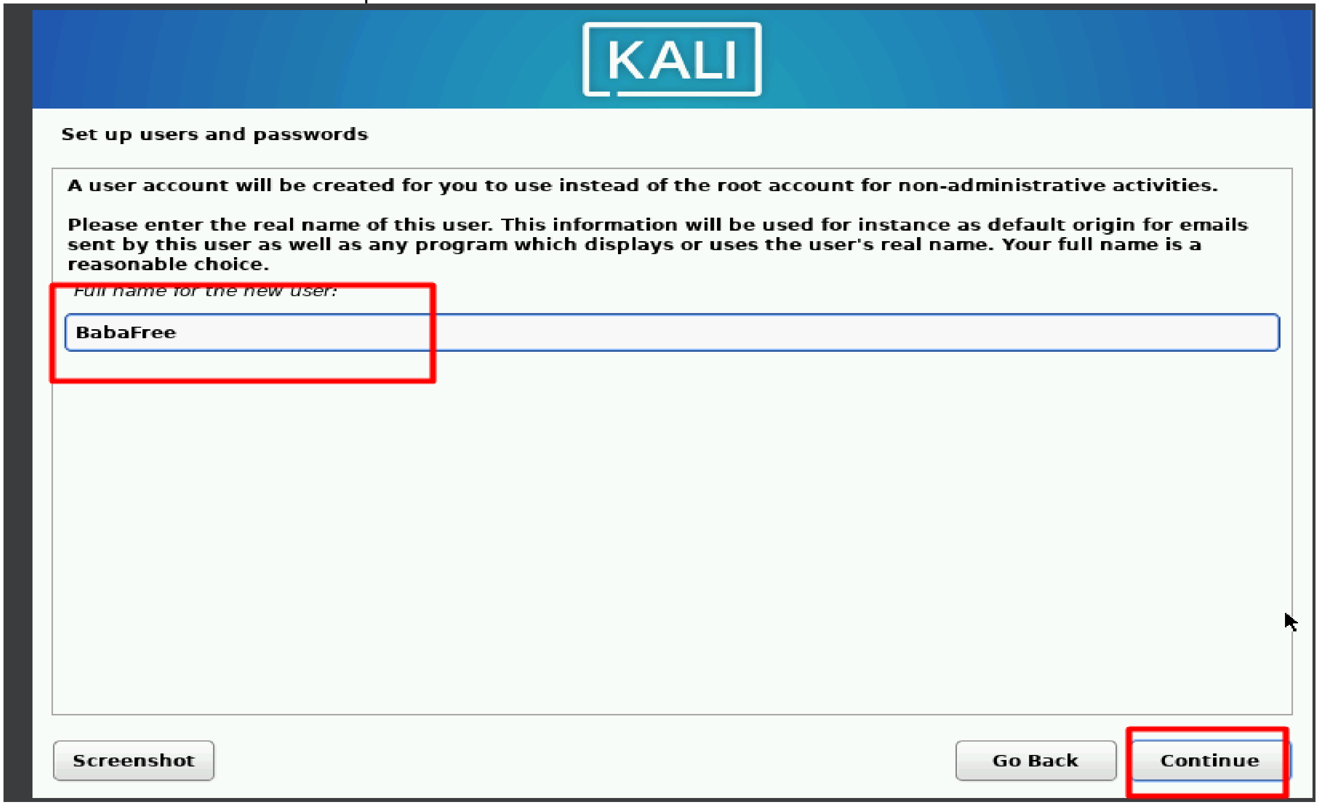
Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Chinese (Simplified)	-	中文(简体)
Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
Dzongkha	-	ཇོང་ཁ
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
Georgian	-	ქართული
German	-	Deutsch

Figure 14: - Selecting language of choice

- Set the username and password of choice



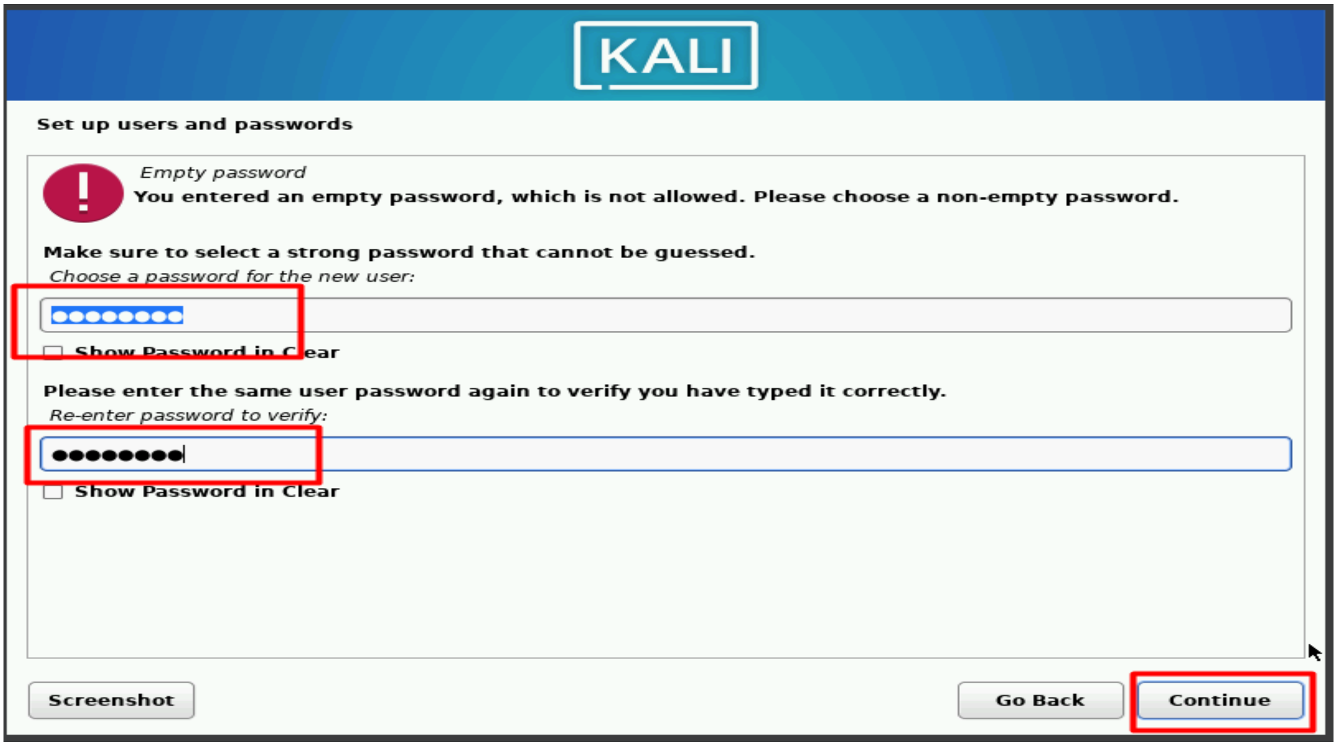
Set up users and passwords

A user account will be created for you to use instead of the root account for non-administrative activities.

Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.

Full name for the new user:

BabaFree



Set up users and passwords

Empty password

You entered an empty password, which is not allowed. Please choose a non-empty password.

Make sure to select a strong password that cannot be guessed.

Choose a password for the new user:

●●●●●●●●●

□ Show Password in Clear

Please enter the same user password again to verify you have typed it correctly.

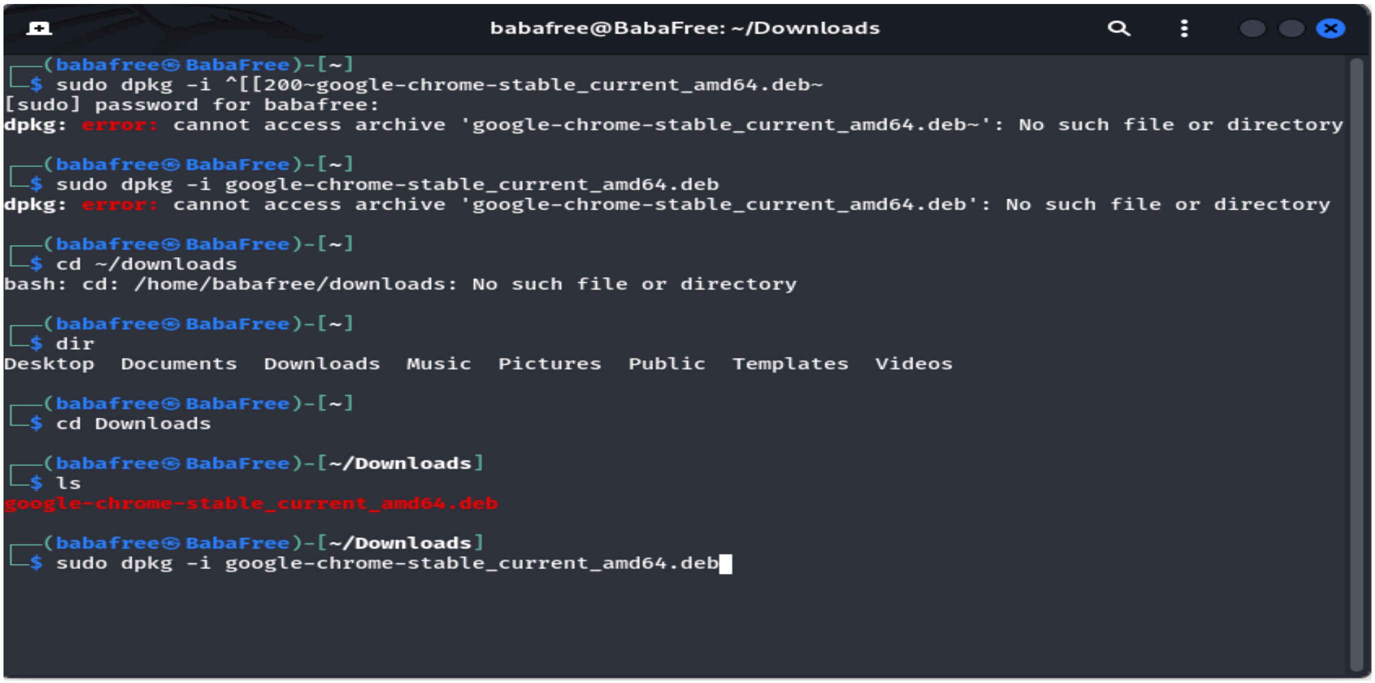
Re-enter password to verify:

●●●●●●●●●

□ Show Password in Clear

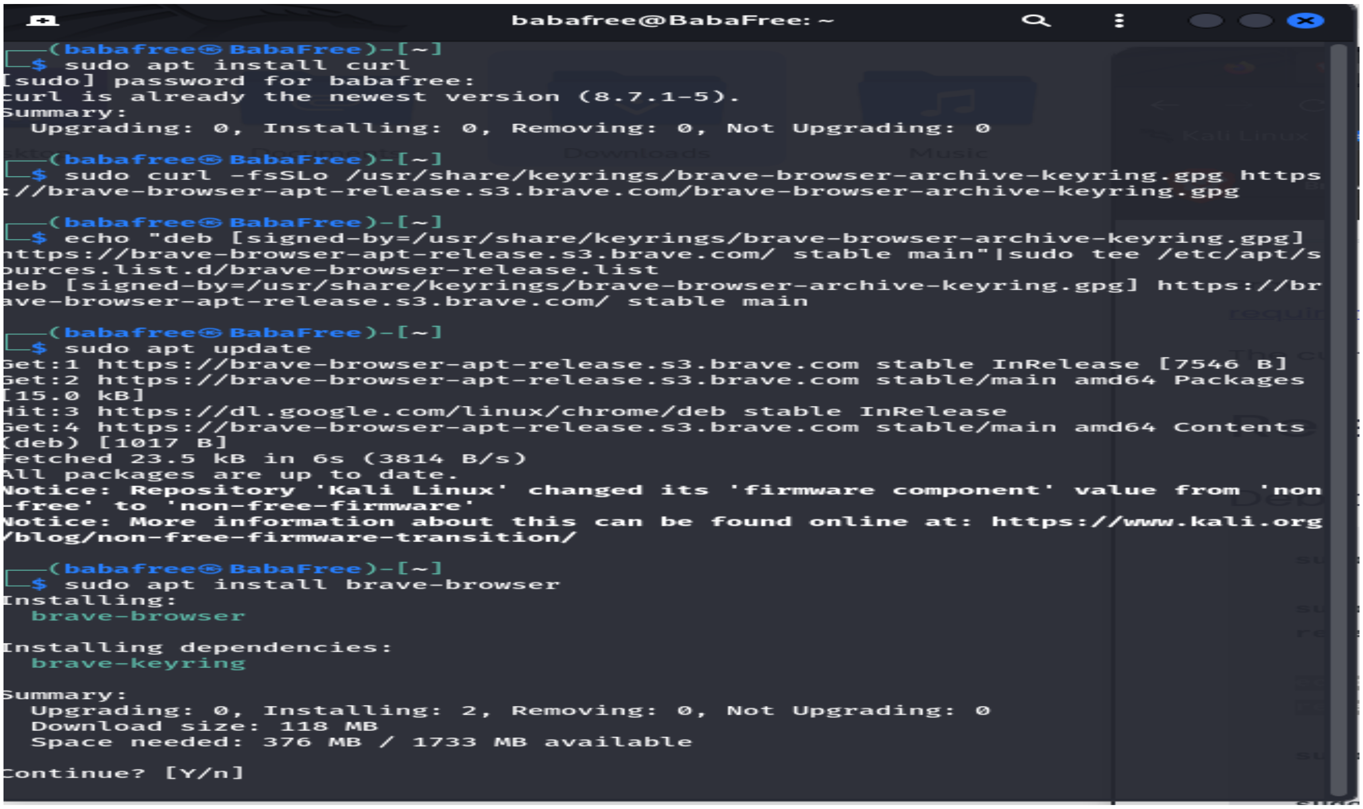
Figure 15: - Username and password

- Setup browser of Choice



```
┌──(babafree㉿BabaFree)-[~]
└─$ sudo dpkg -i ^[[200~google-chrome-stable_current_amd64.deb~
[sudo] password for babafree:
dpkg: error: cannot access archive 'google-chrome-stable_current_amd64.deb~': No such file or directory

┌──(babafree㉿BabaFree)-[~]
└─$ sudo dpkg -i google-chrome-stable_current_amd64.deb
dpkg: error: cannot access archive 'google-chrome-stable_current_amd64.deb': No such file or directory

┌──(babafree㉿BabaFree)-[~]
└─$ cd ~/downloads
bash: cd: /home/babafree/downloads: No such file or directory

┌──(babafree㉿BabaFree)-[~]
└─$ dir
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(babafree㉿BabaFree)-[~]
└─$ cd Downloads

┌──(babafree㉿BabaFree)-[~/Downloads]
└─$ ls
google-chrome-stable_current_amd64.deb

┌──(babafree㉿BabaFree)-[~/Downloads]
└─$ sudo dpkg -i google-chrome-stable_current_amd64.deb
```

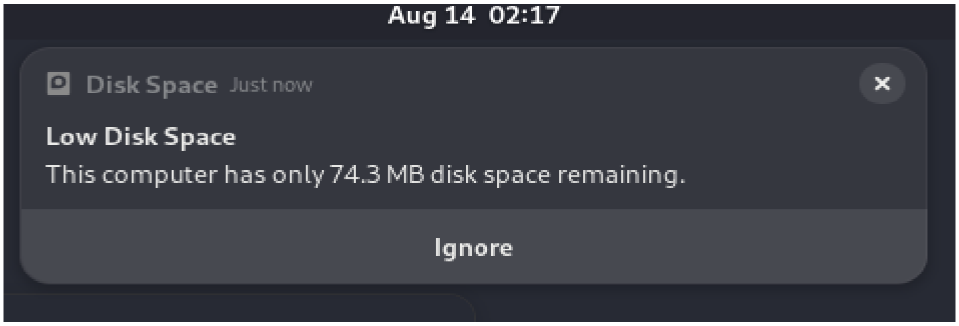
Figure 16: - Setting up Google Browser on Kali Linux



```
┌──(babafree㉿BabaFree)-[~]
└─$ sudo apt install curl
[sudo] password for babafree:
curl is already the newest version (8.7.1-5).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

┌──(babafree㉿BabaFree)-[~]
└─$ sudo curl -fsSLo /usr/share/keyrings/brave-browser-archive-keyring.gpg https
://brave-browser-apt-release.s3.brave.com/brave-browser-archive-keyring.gpg

┌──(babafree㉿BabaFree)-[~]
└─$ echo "deb [signed-by=/usr/share/keyrings/brave-browser-archive-keyring.gpg]
https://brave-browser-apt-release.s3.brave.com/ stable main"|sudo tee /etc/apt/s
ources.list.d/brave-browser-release.list
deb [signed-by=/usr/share/keyrings/brave-browser-archive-keyring.gpg] https://br
ave-browser-apt-release.s3.brave.com/ stable main

┌──(babafree㉿BabaFree)-[~]
└─$ sudo apt update
Get:1 https://brave-browser-apt-release.s3.brave.com stable InRelease [7546 B]
Get:2 https://brave-browser-apt-release.s3.brave.com stable/main amd64 Packages
[15.0 kB]
Hit:3 https://dl.google.com/linux/chrome/deb stable InRelease
Get:4 https://brave-browser-apt-release.s3.brave.com stable/main amd64 Contents
(deb) [1017 B]
Fetched 23.5 kB in 6s (3814 B/s)
All packages are up to date.
Notice: Repository 'Kali Linux' changed its 'firmware component' value from 'non
-free' to 'non-free-firmware'
Notice: More information about this can be found online at: https://www.kali.org
/blog/non-free-firmware-transition/

┌──(babafree㉿BabaFree)-[~]
└─$ sudo apt install brave-browser
Installing:
  brave-browser

Installing dependencies:
  brave-keyring

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 0
  Download size: 118 MB
  Space needed: 376 MB / 1733 MB available

Continue? [Y/n]
```

Figure 17: - Setting up Brave Browser on Kali Linux

To address space management in Kali Linux



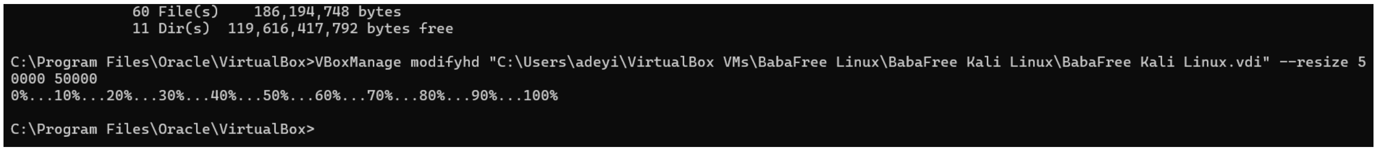
Aug 14 02:17

Disk Space Just now

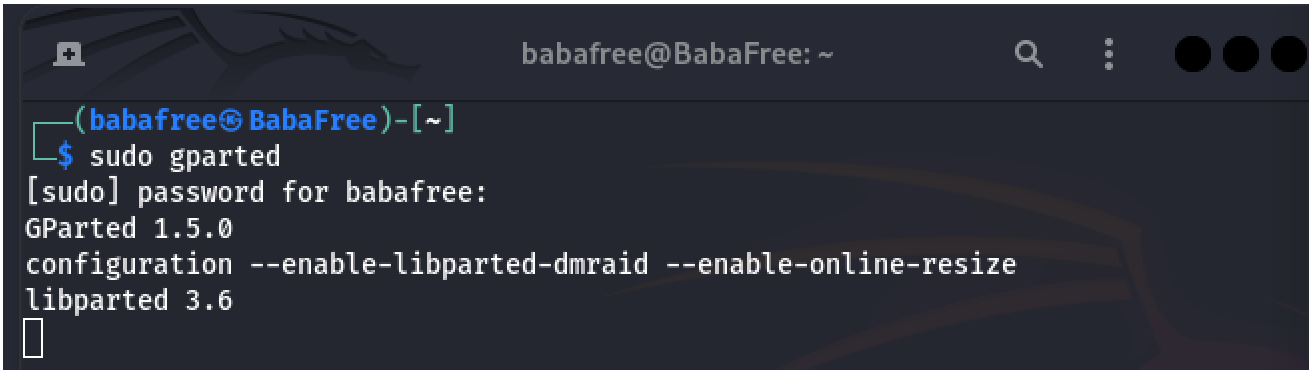
Low Disk Space

This computer has only 74.3 MB disk space remaining.

- We use the following approach. We launch the Terminal CLI

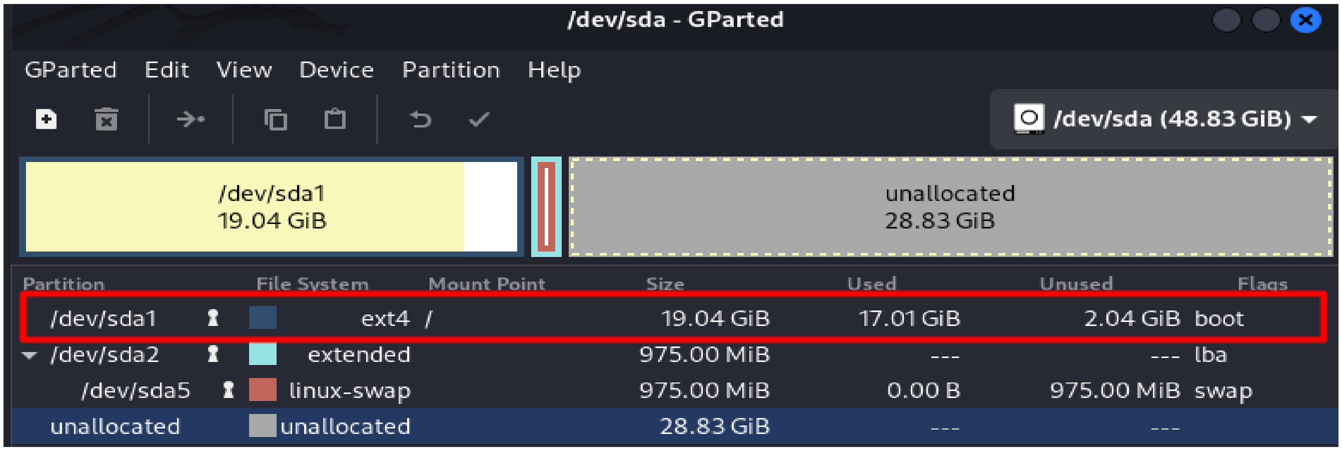


```
               60 File(s)    186,194,748 bytes
               11 Dir(s)  119,616,417,792 bytes free

C:\Program Files\Oracle\VirtualBox>VBoxManage modifyhd "C:\Users\adeyi\VirtualBox VMs\BabaFree Linux\BabaFree Kali Linux\BabaFree Kali Linux.vdi" --resize 5
0000 50000
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%

C:\Program Files\Oracle\VirtualBox>
```



babafree@BabaFree: ~

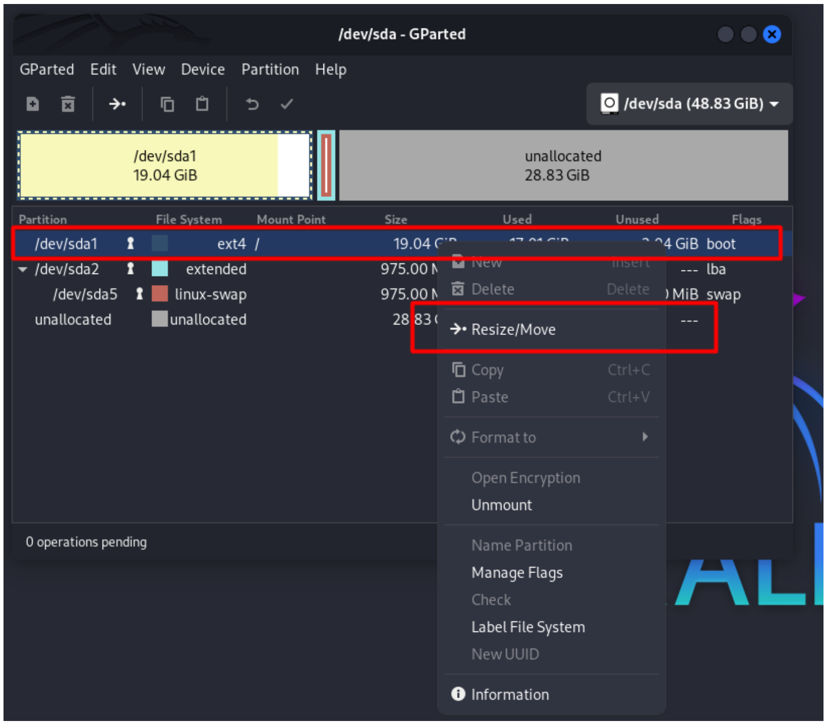
```
┌──(babafree㉿BabaFree)-[~]
└─$ sudo gparted
[sudo] password for babafree:
GParted 1.5.0
configuration --enable-libparted-dmraid --enable-online-resize
libparted 3.6
```



/dev/sda - GParted

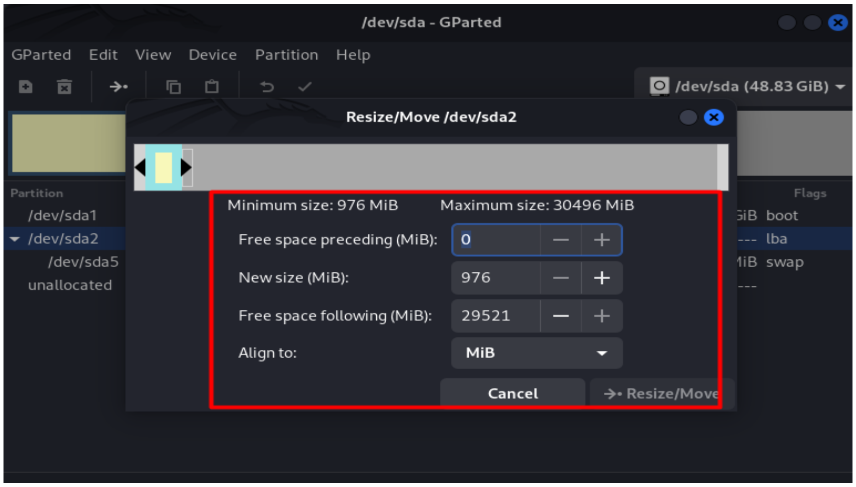
Partition	File System	Mount Point	Size	Used	Unused	Flags
/dev/sda1	ext4	/	19.04 GiB	17.01 GiB	2.04 GiB	boot
/dev/sda2	extended		975.00 MiB	---	---	lba
/dev/sda5	linux-swap		975.00 MiB	0.00 B	975.00 MiB	swap
unallocated	unallocated		28.83 GiB	---	---	

Figure 18: - File storage resizing on Kali Linux



Partition	File System	Mount Point	Size	Used	Unused	Flags
/dev/sda1	ext4	/	19.04 G	17.01 G	2.04 GiB	boot
/dev/sda2	extended		975.00 M		---	lba
/dev/sda5	linux-swap		975.00 M		MiB	swap
unallocated	unallocated		28.83		---	

- **Option 1: Navigate Directly to the VirtualBox Directory**
- **Find the VirtualBox Installation Path:**
  - Typically, VirtualBox is installed in C:\Program Files\Oracle\VirtualBox.
- **Navigate to the Directory:**
  - Open **Command Prompt**.
  - Change the directory to where VirtualBox is installed:



Minimum size: 976 MiB   Maximum size: 30496 MiB

Free space preceding (MiB): 0

New size (MiB): 976

Free space following (MiB): 29521

Align to: MiB

cd "C:\Program Files\Oracle\VirtualBox"

- **Run the VBoxManage Command:**
  - Now, try running the VBoxManage command again:
- VBoxManage modifyhd "path_to_your_vdi_file.vdi" --resize size_in_MB

- **Option 2: Add VirtualBox to the System PATH (Recommended)**
- **Find the VirtualBox Installation Path:**
  - As mentioned earlier, it's typically in C:\Program Files\Oracle\VirtualBox.
- **Add VirtualBox to the PATH Environment Variable:**

  - Right-click on **This PC** or **Computer** on your desktop or in File Explorer.
  - Select **Properties** > **Advanced system settings** > **Environment Variables**.
  - In the **System variables** section, scroll down and find the **Path** variable, then click **Edit**.
  - Click **New** and add the path to your VirtualBox installation (e.g., C:\Program Files\Oracle\VirtualBox).
  - Click **OK** to close all dialogs.

- **Restart Command Prompt:**
  - Close and reopen Command Prompt so that the new PATH variable is recognized.

- **Run the VBoxManage Command:**
  - Now, you should be able to run the VBoxManage command from any directory:
  - VBoxManage modifyhd "path_to_your_vdi_file.vdi" --resize size_in_MB

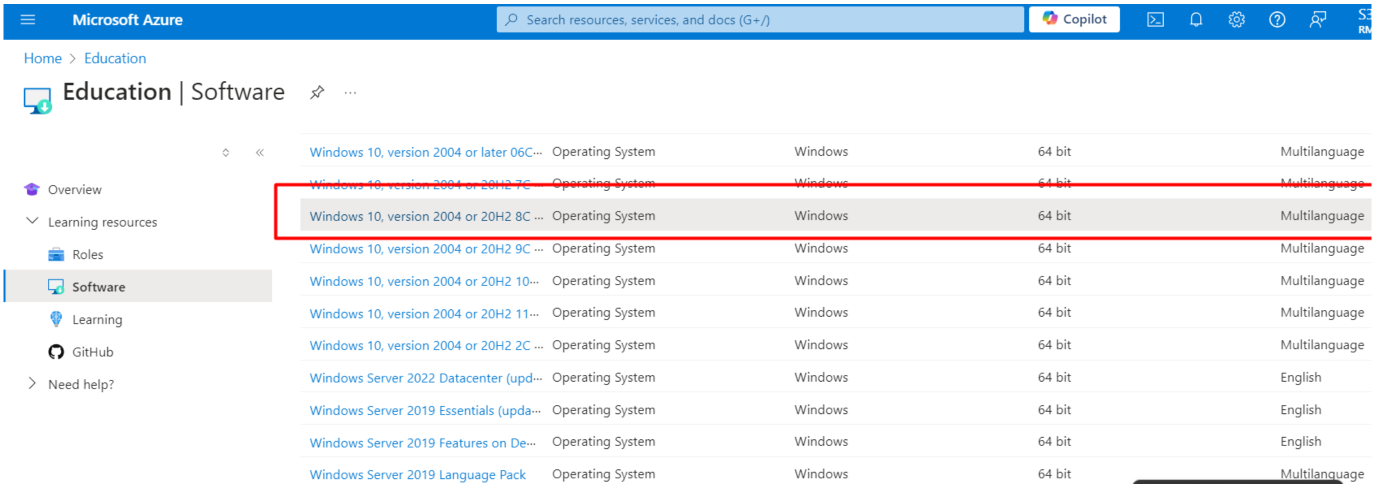
- **Final Steps**

  After adding the space to the virtual disk, proceed with resizing the partition in Kali Linux as previously described.

4 SETTING UP MICROSOFT OPERATING SYSTEM

4.1. Setting Up - Microsoft Operating System

We commence by setting up the Microsoft Operating System. We select Windows Operating system from Version 10 and above.



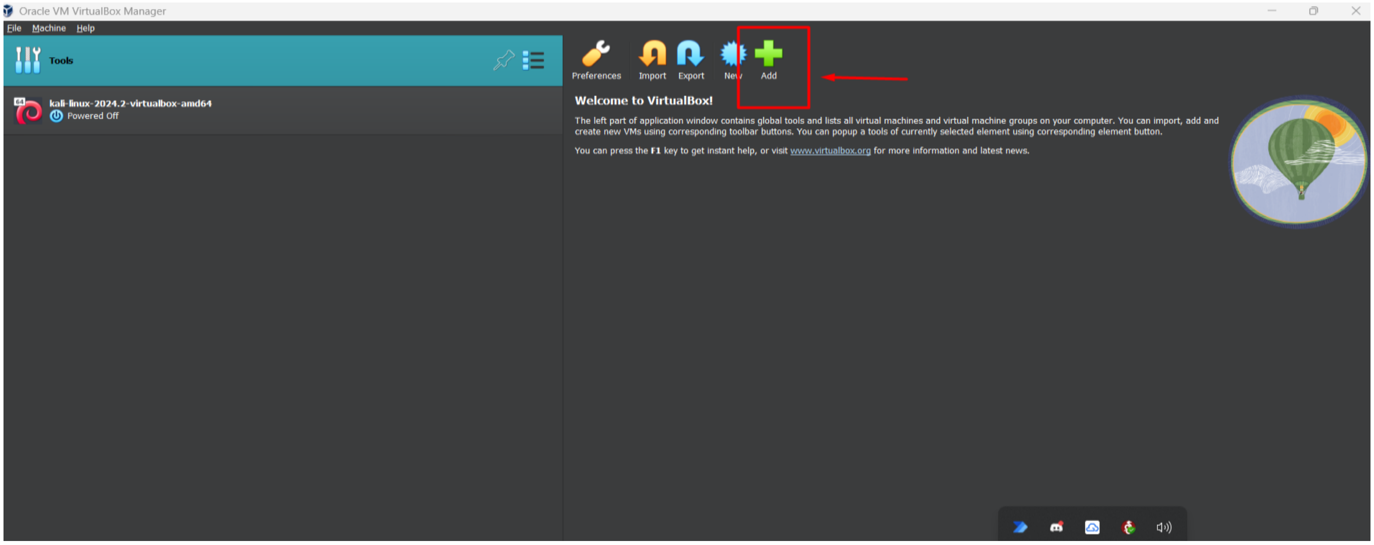
Education | Software

Windows 10, version 2004 or later 06C…	Operating System	Windows	64 bit	Multilanguage
Windows 10, version 2004 or 20H2 7C…	Operating System	Windows	64 bit	Multilanguage
Windows 10, version 2004 or 20H2 8C …	Operating System	Windows	64 bit	Multilanguage
Windows 10, version 2004 or 20H2 9C …	Operating System	Windows	64 bit	Multilanguage
Windows 10, version 2004 or 20H2 10…	Operating System	Windows	64 bit	Multilanguage
Windows 10, version 2004 or 20H2 11…	Operating System	Windows	64 bit	Multilanguage
Windows 10, version 2004 or 20H2 2C …	Operating System	Windows	64 bit	Multilanguage
Windows Server 2022 Datacenter (upd…	Operating System	Windows	64 bit	English
Windows Server 2019 Essentials (upda…	Operating System	Windows	64 bit	English
Windows Server 2019 Features on De…	Operating System	Windows	64 bit	English
Windows Server 2019 Language Pack	Operating System	Windows	64 bit	Multilanguage

Figure 19:- Microsoft Windows 10 Version 2004 (64 bit)

4.2. Setting up Microsoft Operating System on Oracle VirtualBox

- We select the “Add” button



kali-linux-2024.2-virtualbox-amd64
Powered Off

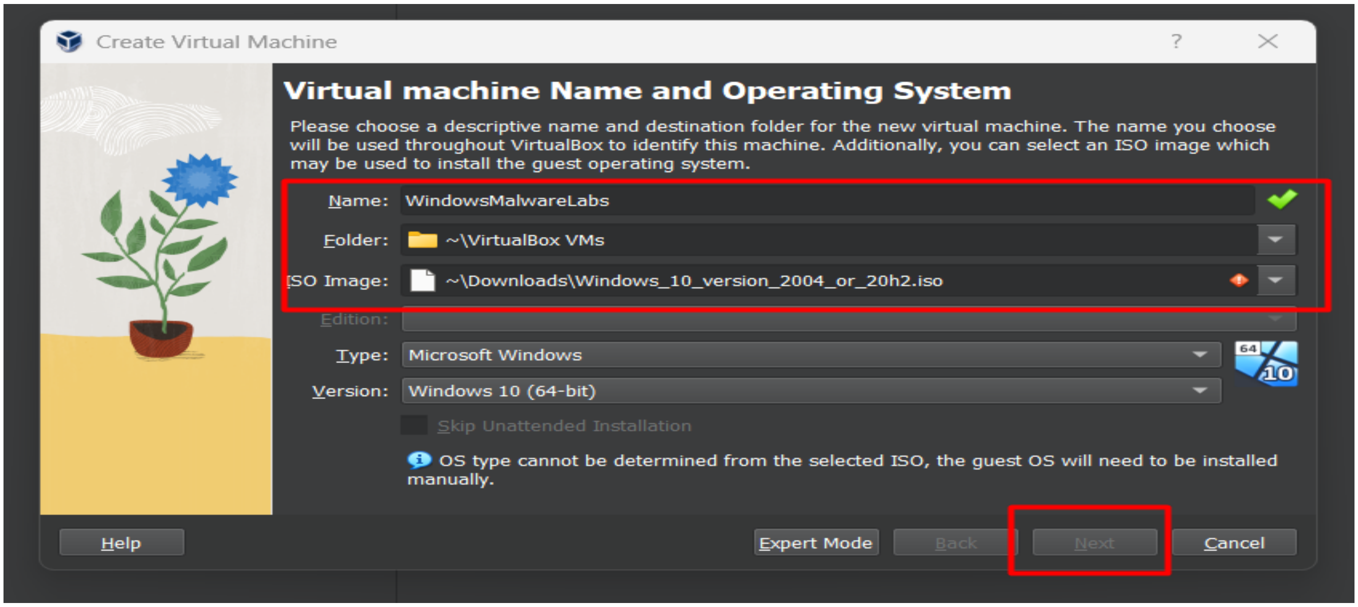
Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the F1 key to get instant help, or visit www.virtualbox.org for more information and latest news.

Figure 20: - Setting up Microsoft Windows 10 Ver. 2004 (64-bit) on Oracle VirtualBox

We define the name of our Lab - “**WindowsMalwareLabs**”, We specify the folder pathway: - “**C:\~\VirtualBox VMs**” and the ISO Image - Windows 10 Version 2004. Once we do this, we select the “**Next**” button to commence the setup



Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: WindowsMalwareLabs

Folder: ~\VirtualBox VMs

ISO Image: ~\Downloads\Windows_10_version_2004_or_20h2.iso

Edition:

Type: Microsoft Windows

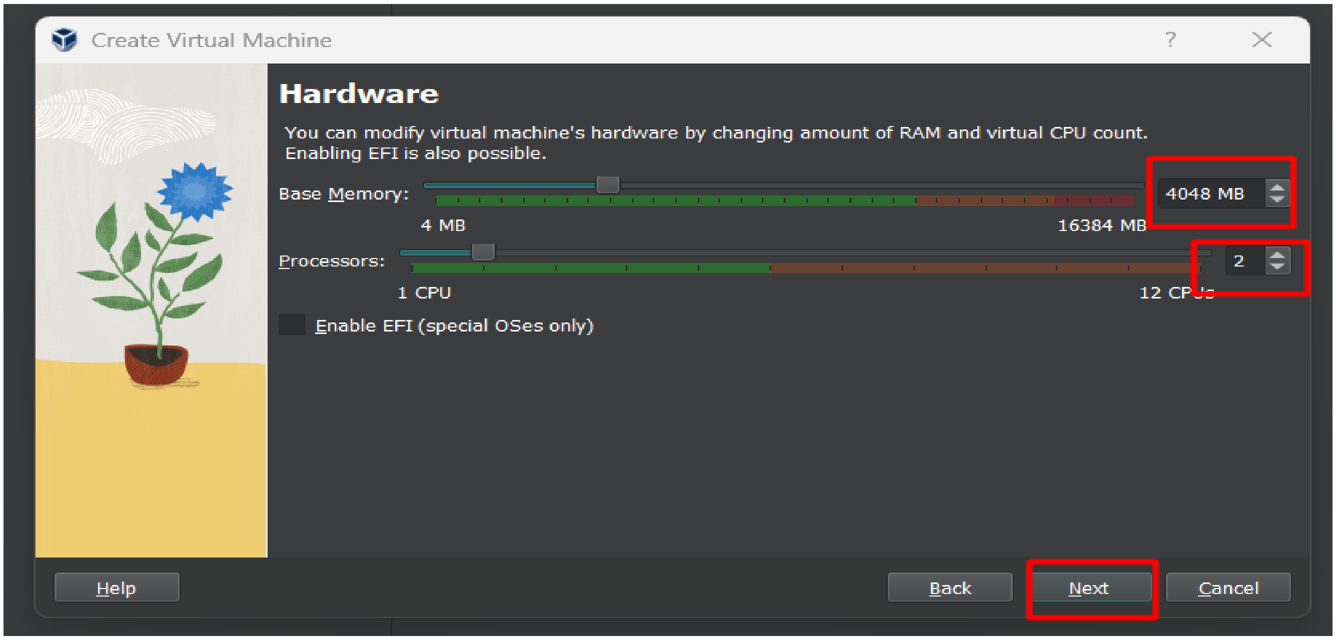
Version: Windows 10 (64-bit)

□ Skip Unattended Installation

OS type cannot be determined from the selected ISO, the guest OS will need to be installed manually.

Figure 21: - Configuring Microsoft Windows 10 Ver. 2004 (64-bit) on Oracle VirtualBox

- We specify the based memory increasing it to “**4048MB”** and processor to **“2CPU”** We use this as our preferred configuration requirement.



Hardware

You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

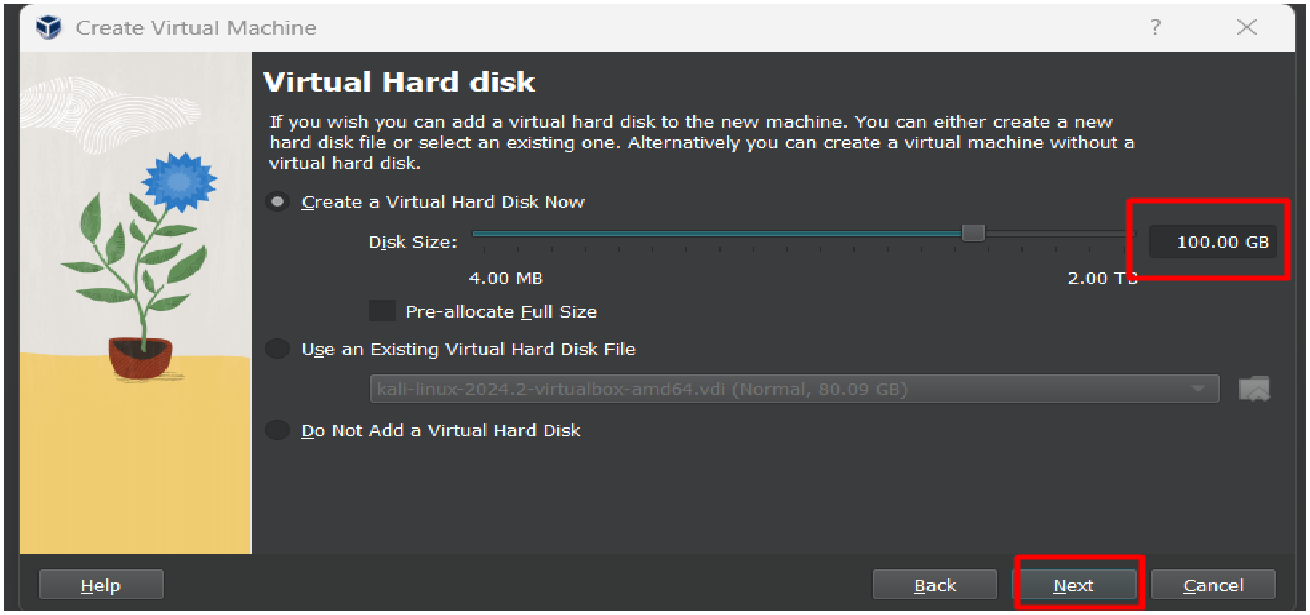
Base Memory: 4048 MB

Processors: 2

□ Enable EFI (special OSes only)

Figure 22: - Configuring Hardware requirements -Microsoft Windows 10 Ver. 2004 (64-bit) on Oracle VirtualBox

- We also specify our recommended configuration for virtual hard disk space to be “**100 GB**”.



Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

● Create a Virtual Hard Disk Now

Disk Size: 100.00 GB (4.00 MB – 2.00 TB)

□ Pre-allocate Full Size

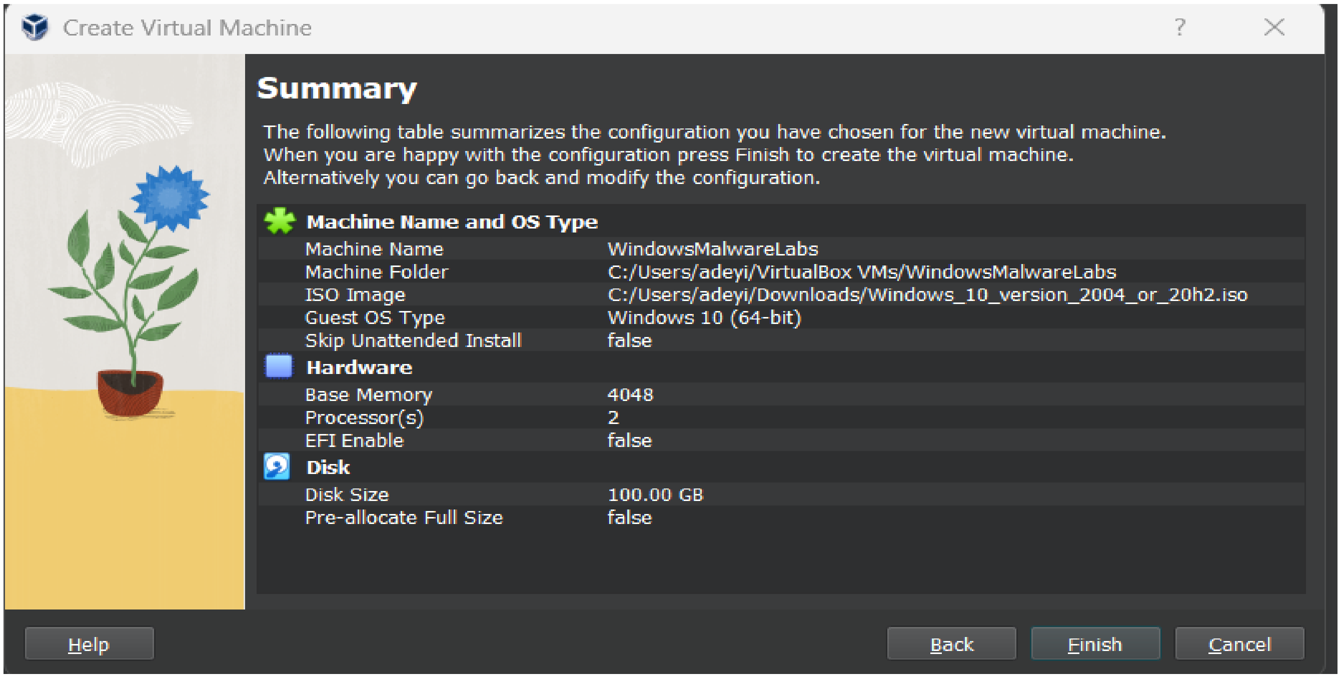
○ Use an Existing Virtual Hard Disk File

kali-linux-2024.2-virtualbox-amd64.vdi (Normal, 80.09 GB)

○ Do Not Add a Virtual Hard Disk

Figure 23: - Configuring Hardware requirements -Microsoft Windows 10 Ver. 2004 (64-bit) on Oracle VirtualBox (ii)

- Our summary configuration is displayed below: -



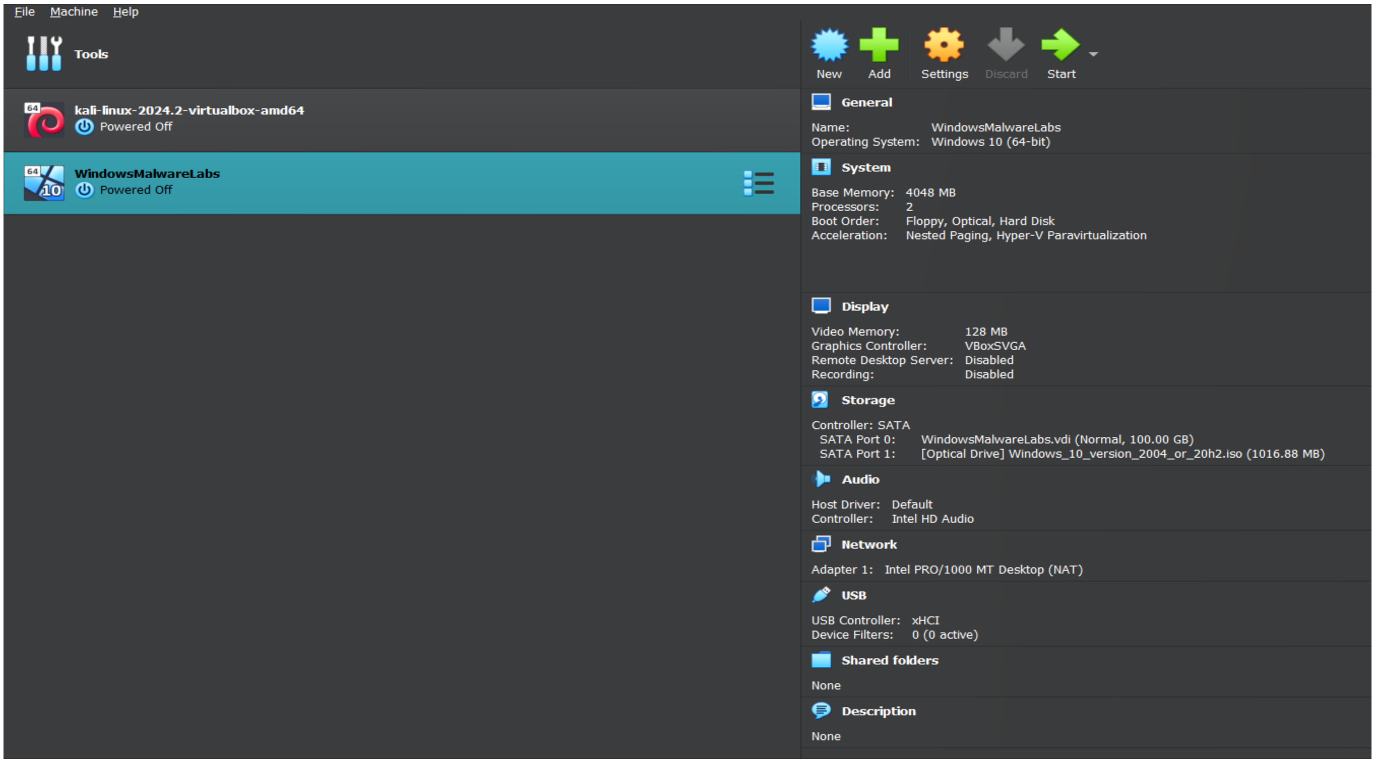
Summary

The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

Machine Name and OS Type	
Machine Name	WindowsMalwareLabs
Machine Folder	C:/Users/adeyi/VirtualBox VMs/WindowsMalwareLabs
ISO Image	C:/Users/adeyi/Downloads/Windows_10_version_2004_or_20h2.iso
Guest OS Type	Windows 10 (64-bit)
Skip Unattended Install	false
Hardware	
Base Memory	4048
Processor(s)	2
EFI Enable	false
Disk	
Disk Size	100.00 GB
Pre-allocate Full Size	false

Figure 24: - Reviewing requirement setup on Oracle VirtualBox

- Selecting the “Finish” button displays a summary of our setup



kali-linux-2024.2-virtualbox-amd64
Powered Off

WindowsMalwareLabs
Powered Off

General

Name: WindowsMalwareLabs
Operating System: Windows 10 (64-bit)

System

Base Memory: 4048 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: WindowsMalwareLabs.vdi (Normal, 100.00 GB)
SATA Port 1: [Optical Drive] Windows_10_version_2004_or_20h2.iso (1016.88 MB)

Audio

Host Driver: Default
Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: xHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

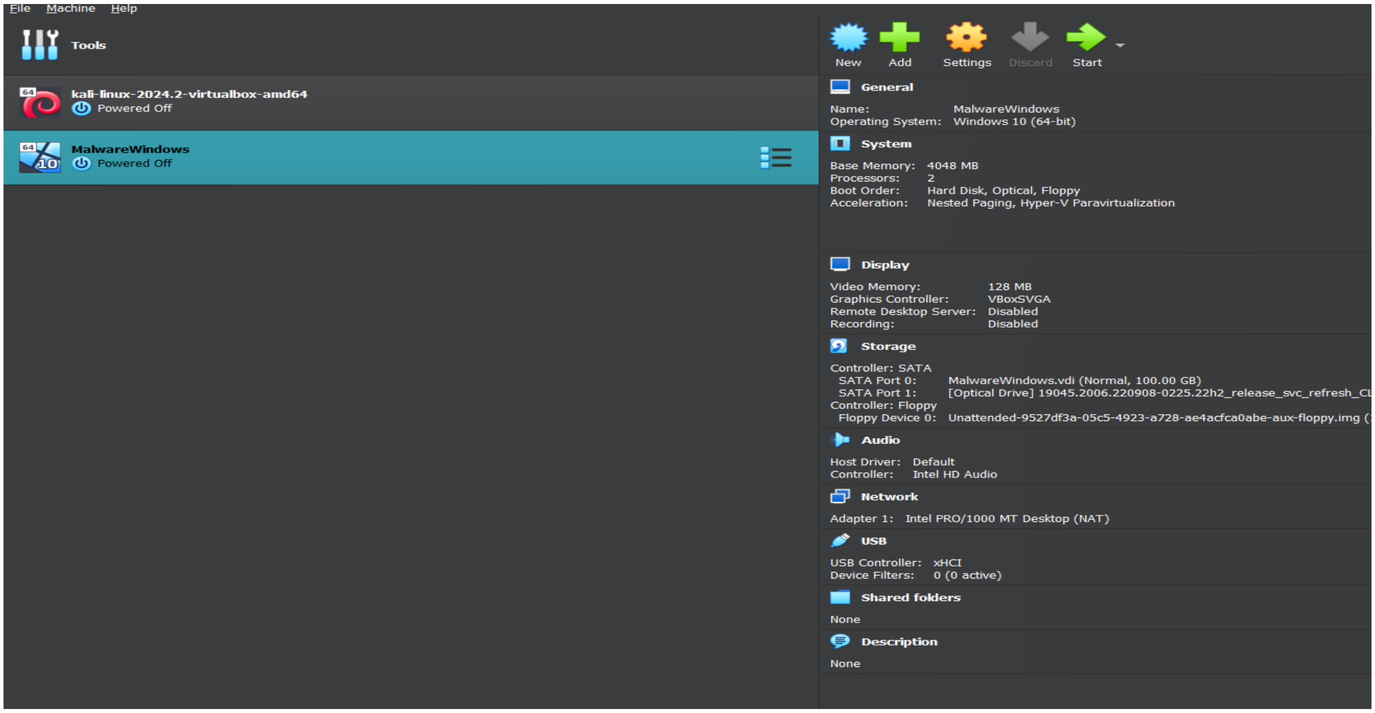
None

Figure 25: - Reviewing requirement setup and configuration on Oracle VirtualBox

4.3. Configuring Windows 10 VM

To setup and configure Windows 10 VM, we confirm that our bootable ISO image is properly loaded by checking to confirm we selected the virtual machine in VirtualBox carrying the following steps: -

- Click on "Settings".
- Go to "Storage".
- Under "Controller: IDE" (or SATA), click the empty CD/DVD drive icon.
- Click on the CD/DVD icon next to "Optical Drive" and select "Choose a disk file".
- Locate and select your bootable ISO image file.
- Ensure that the ISO is correctly selected and attached.



```
General

Name:               MalwareWindows
Operating System:   Windows 10 (64-bit)

System

Base Memory:   4048 MB
Processors:    2
Boot Order:    Hard Disk, Optical, Floppy
Acceleration:  Nested Paging, Hyper-V Paravirtualization

Display

Video Memory:            128 MB
Graphics Controller:     VBoxSVGA
Remote Desktop Server:   Disabled
Recording:               Disabled

Storage

Controller: SATA
  SATA Port 0:      MalwareWindows.vdi (Normal, 100.00 GB)
  SATA Port 1:      [Optical Drive] 19045.2006.220908-0225.22h2_release_svc_refresh_CL
Controller: Floppy
  Floppy Device 0:  Unattended-9527df3a-05c5-4923-a728-ae4acfca0abe-aux-floppy.img (

Audio

Host Driver:  Default
Controller:   Intel HD Audio

Network

Adapter 1:  Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller:  xHCI
Device Filters:  0 (0 active)

Shared folders

None

Description

None
```

Figure 26: - Reviewing requirement setup and configuration on Oracle VirtualBox

4.4. Running Windows on Oracle VirtualBox

We installed browser of choice - Brave and Google Chrome.

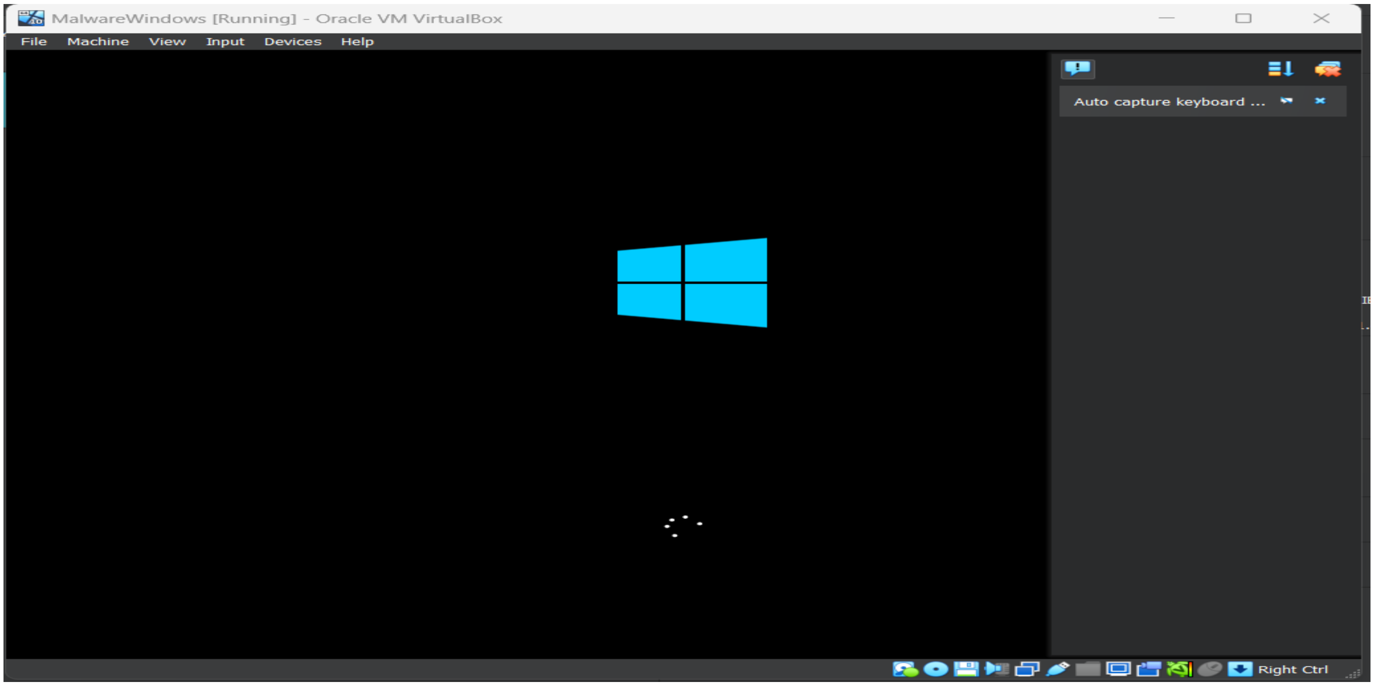

MalwareWindows [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Auto capture keyboard ...
Right Ctrl

Figure 27: - Launching Windows on Oracle VirtualBox

- Install preferred browsers – Chrome, Brave, Firefox, etc. for Compatibility Testing

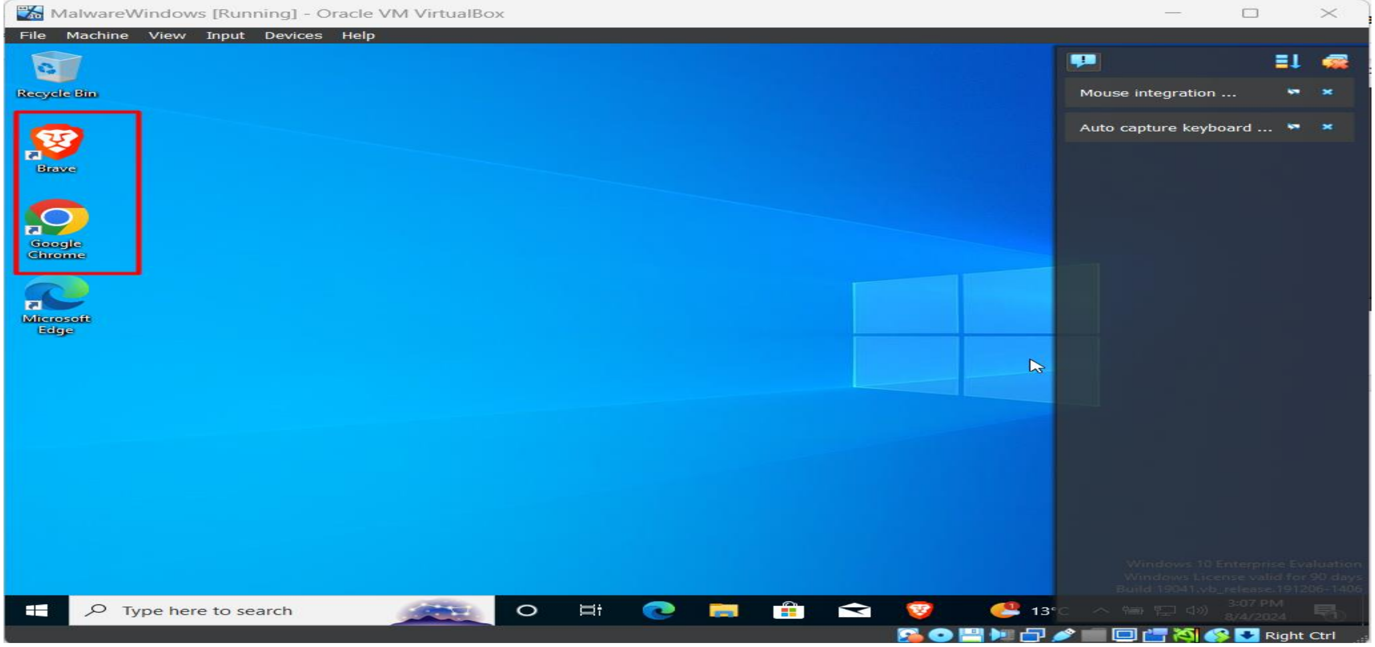
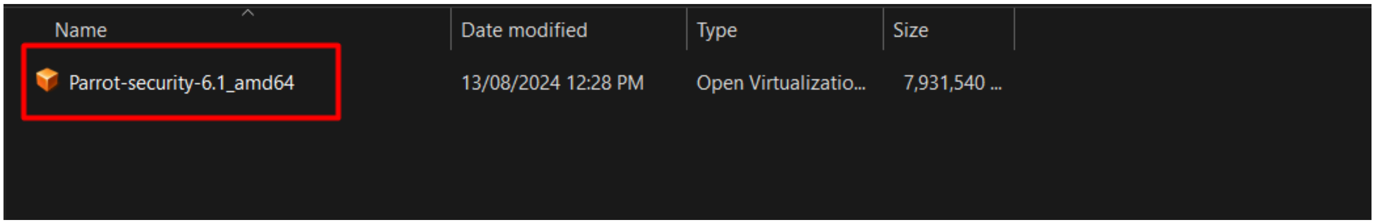

MalwareWindows [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Recycle Bin
Brave
Google Chrome
Microsoft Edge
Mouse integration ...
Auto capture keyboard ...
Type here to search
13°C
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 19041.vb_release.191206-1406
3:07 PM
8/4/2024
Right Ctrl

Figure 28: - Installing browser of our choice

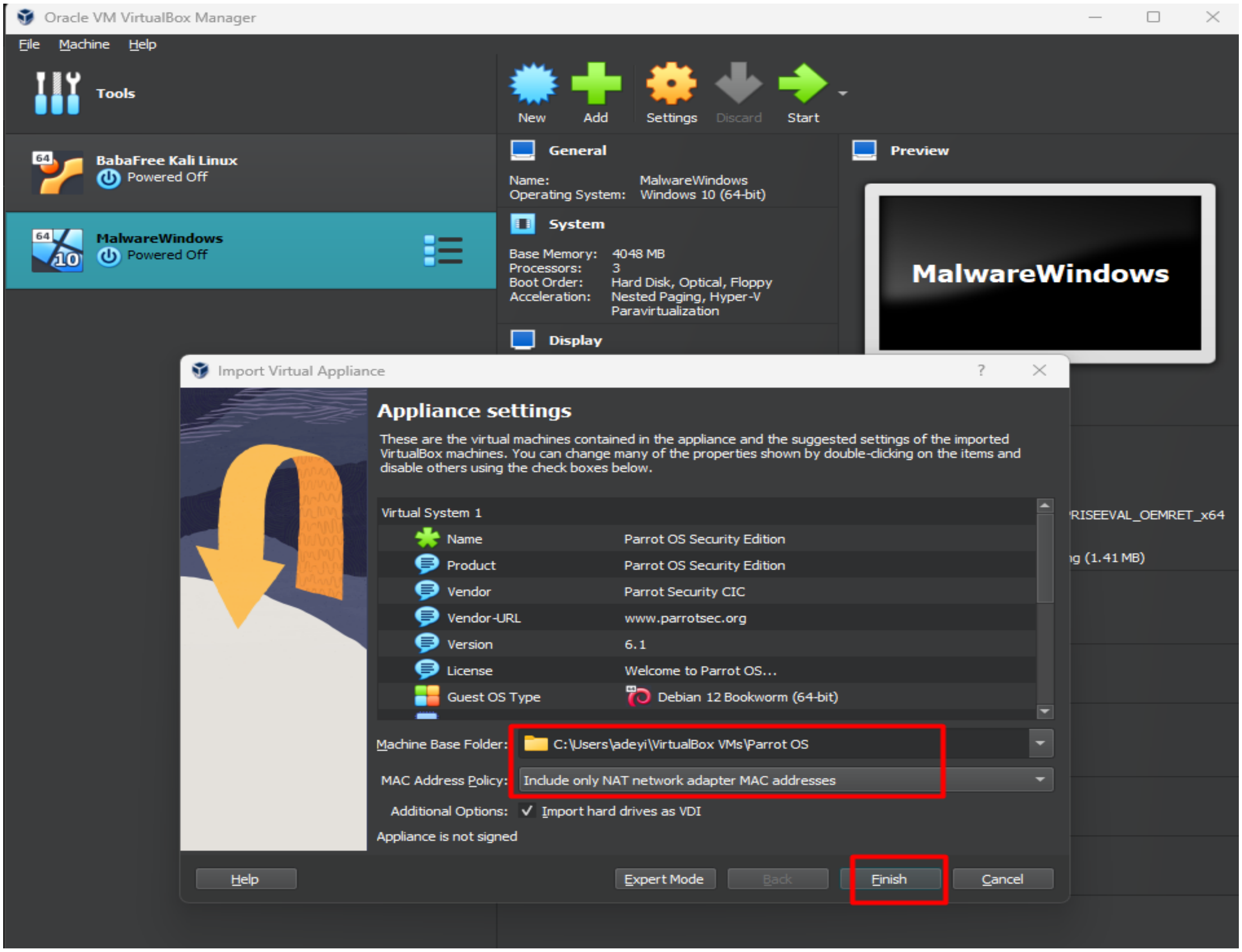
4.5. Setting up Parrot OS

To setup Parrot OS, we download the Parrot OS,



Name	Date modified	Type	Size
Parrot-security-6.1_amd64	13/08/2024 12:28 PM	Open Virtualizatio...	7,931,540 ...

Figure 29: - Installing Parrot OS from the downloaded folder



Name: MalwareWindows
Operating System: Windows 10 (64-bit)

Base Memory: 4048 MB
Processors: 3
Boot Order: Hard Disk, Optical, Floppy
Acceleration: Nested Paging, Hyper-V Paravirtualization

RISEEVAL_OEMRET_x64

ıg (1.41 MB)

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1	
Name	Parrot OS Security Edition
Product	Parrot OS Security Edition
Vendor	Parrot Security CIC
Vendor-URL	www.parrotsec.org
Version	6.1
License	Welcome to Parrot OS...
Guest OS Type	Debian 12 Bookworm (64-bit)

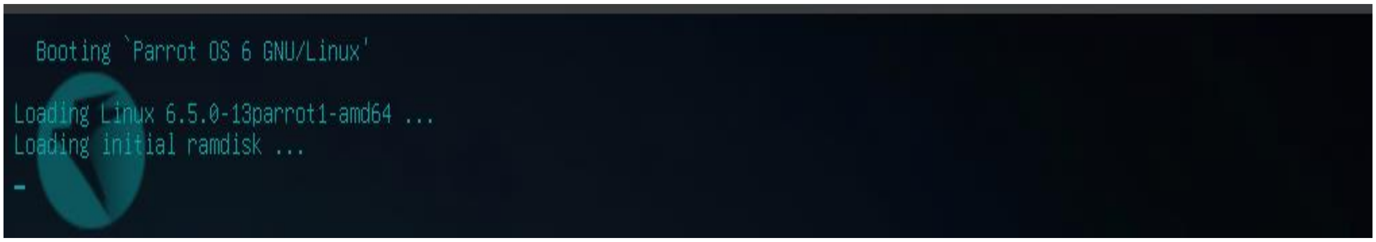
Machine Base Folder: C:\Users\adeyi\VirtualBox VMs\Parrot OS

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: ✓ Import hard drives as VDI

Appliance is not signed

Figure 30: - Installing Parrot OS



```
  Booting `Parrot OS 6 GNU/Linux'

Loading Linux 6.5.0-13parrot1-amd64 ...
Loading initial ramdisk ...
_
```

Figure 31: - Installing Parrot OS

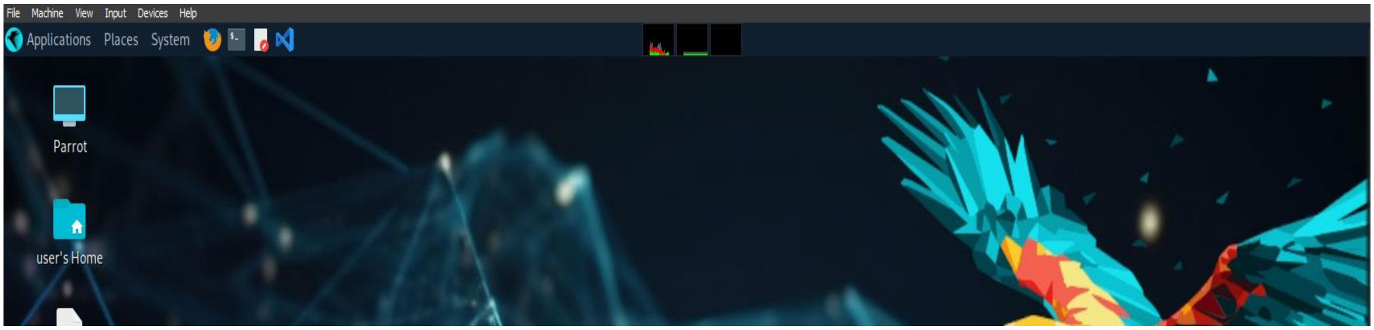


Figure 32: - Installing Parrot OS

5. SETTING UP MALWARE DETECTION AND ANALYTICS TOOLS

Kali Linux is packed with a wide range of tools specifically designed for various cybersecurity tasks. Here's a broad overview of some of the categories and notable tools available in Kali Linux:

5.1. Information Gathering

- Nmap: Network exploration and security auditing tool.
- Wireshark: Network protocol analyser.
- Maltego: Interactive data mining tool.
- Recon-ng: Web reconnaissance framework.

5.2. Vulnerability Analysis

- OpenVAS: Vulnerability scanning and management tool.
- Nikto: Web server scanner.
- Lynis: Security auditing and hardening tool.

5.3. Web Application Analysis

- Burp Suite: Web vulnerability scanner.
- OWASP ZAP: Web application security scanner.
- SQLmap: Automated SQL injection tool.
- Nikto: Web server scanner.

5.4. Database Assessment

- sqlmap: Automatic SQL injection and database takeover tool.
- jSQL: SQL injection tool.

5.5. Password Attacks

- John the Ripper: Password cracking tool.
- Hashcat: Advanced password recovery tool.
- Hydra: Fast and flexible network login cracker.
- CeWL: Custom wordlist generator.

5.6. Wireless Attacks

- Aircrack-ng: Suite of tools to assess Wi-Fi network security.
- Kismet: Wireless network detector and intrusion detection system.
- Reaver: WPS attack tool.
- Fern WiFi Cracker: Wireless security auditing and attack tool.

5.7. ExploitationTools

- Metasploit Framework: Exploitation framework.
- Armitage: GUI for Metasploit.
- BeEF: Browser Exploitation Framework.

5.8. Sniffing and spoofing

- Ettercap: Comprehensive suite for man-in-the-middle attacks.
- Bettercap: Network monitoring and attack tool.
- Responder: LLMNR, NBT-NS, and MDNS poisoner.

5.9. Post Exploitation

- Empire: Post-exploitation framework.
- Metasploit: Also used for post-exploitation activities.
- PowerSploit: PowerShell post-exploitation framework.

5.10. Forensics

- Autopsy: Digital forensics platform and graphical interface.
- Sleuth Kit: Command line tools for digital forensics.
- Binwalk: Firmware analysis tool.
- Volatility: Advanced memory forensics framework.

5.11. Reverse Engineering

- Ghidra: Software reverse engineering framework.
- Radare2: Open-source software for reverse engineering.
- OllyDbg: 32-bit assembler-level analyzing debugger.

5.12. Social Engineering

- Social Engineering Toolkit (SET): Framework for social engineering.
- Creepy: Geolocation tool for social engineering.

5.13. Stress Testing

- Slowloris: Denial of Service (DoS) attack tool.
- T50: Multi-protocol packet injector.

5.14. Hardware Hacking

- Arduino: Integrated development environment for Arduino.
- RFIDiot: RFID exploration and hacking toolkit.

5.15. Reporting Tools

- Dradis: Collaboration framework for reporting and sharing information.
- MagicTree: Penetration tester productivity tool.

5.16. Miscellaneous

- Netcat: Network utility for reading from and writing to network connections.
- P0f: Passive OS fingerprinting tool.

Kali Linux regularly updates and adds new tools to its repository, making it a comprehensive platform for penetration testing, ethical hacking, and cybersecurity research. We setup alternatives like REMnux Malware Analysis toolkit.

5.17. Setting up REMnux Malware Analysis Toolkit

REMnux is a specialized Linux distribution designed for reverse engineering and malware analysis. It provides a collection of free tools that are specifically tailored for analysing malicious software, investigating suspicious files, and dissecting malware-related artifacts. REMnux is particularly useful for cybersecurity professionals, malware analysts, and incident responders who need a dedicated environment for examining malicious code and its behaviours.

5.17.1. Key Features of REMnux:

- **Pre-installed Tools**: REMnux comes with a wide array of tools for various aspects of malware analysis, including:
- **Static analysis**: Tools to inspect the contents of files without executing them.
- **Dynamic analysis**: Tools to observe the behaviour of malware during execution.
- **Memory forensics**: Tools to analyse memory dumps and investigate in-memory artifacts.
- **Network analysis**: Tools to inspect network traffic and detect malicious activities.
- **File forensics**: Tools to investigate files, including document metadata and embedded objects.
- **Malware Analysis Environment**: The distribution is set up to minimize the risk of accidental infection during analysis, providing a safer environment to work with potentially harmful software.
- **Ease of Use**: REMnux includes various helper scripts and utilities that simplify complex tasks, such as unpacking and analysing obfuscated malware.
- **Community Support**: REMnux is supported by a community of cybersecurity professionals, and it is continuously updated to include the latest tools and techniques for malware analysis.
- **Lightweight**: Unlike full-fledged distributions like Kali Linux, REMnux is lightweight and focused purely on malware analysis, making it easier to maintain and use.

5.17.2. Use Cases:

- **Malware Analysis**: Dissect and understand malware to develop defences against it.
- **Incident Response**: Investigate and respond to security incidents involving malicious software.
- **Threat Intelligence**: Gather and analyse information on emerging threats.
- **Security Research**: Conduct research on malicious code and its effects.

5.17.3. Installation:

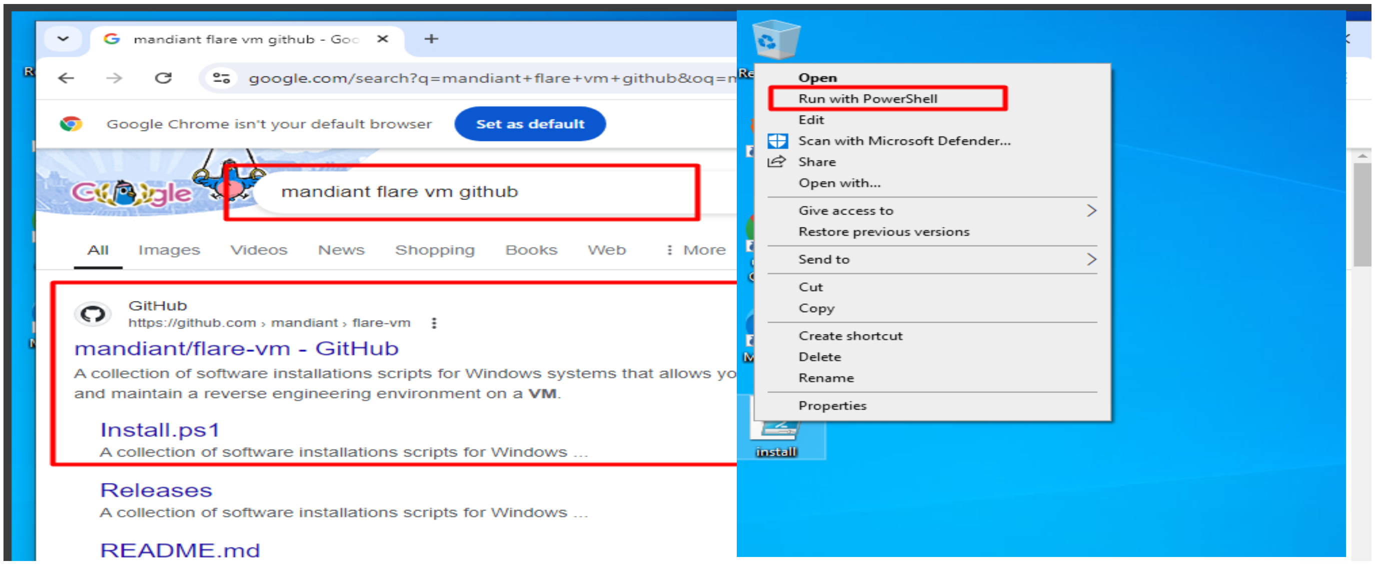
REMnux can be installed as a standalone operating system, or you can add its tools to an existing Ubuntu-based system. It's also available as a virtual machine, which can be particularly convenient for setting up a contained analysis environment.

In summary, REMnux is a highly specialized toolkit that is invaluable for anyone involved in malware analysis and reverse engineering, providing a robust platform to safely and effectively investigate malicious software.

To install Mandiant Flare VM, we search for the location of our file in its github location via our preferred browser

5.18. Setting up Mandiant Flare WM

To install the Mandiant Flare VM, we search for the location of our file in its github location via our preferred browser



google.com/search?q=mandiant+flare+vm+github&oq=n

Google Chrome isn't your default browser

GitHub
https://github.com › mandiant › flare-vm

mandiant/flare-vm - GitHub

A collection of software installations scripts for Windows systems that allows yo and maintain a reverse engineering environment on a VM.

Install.ps1

A collection of software installations scripts for Windows ...

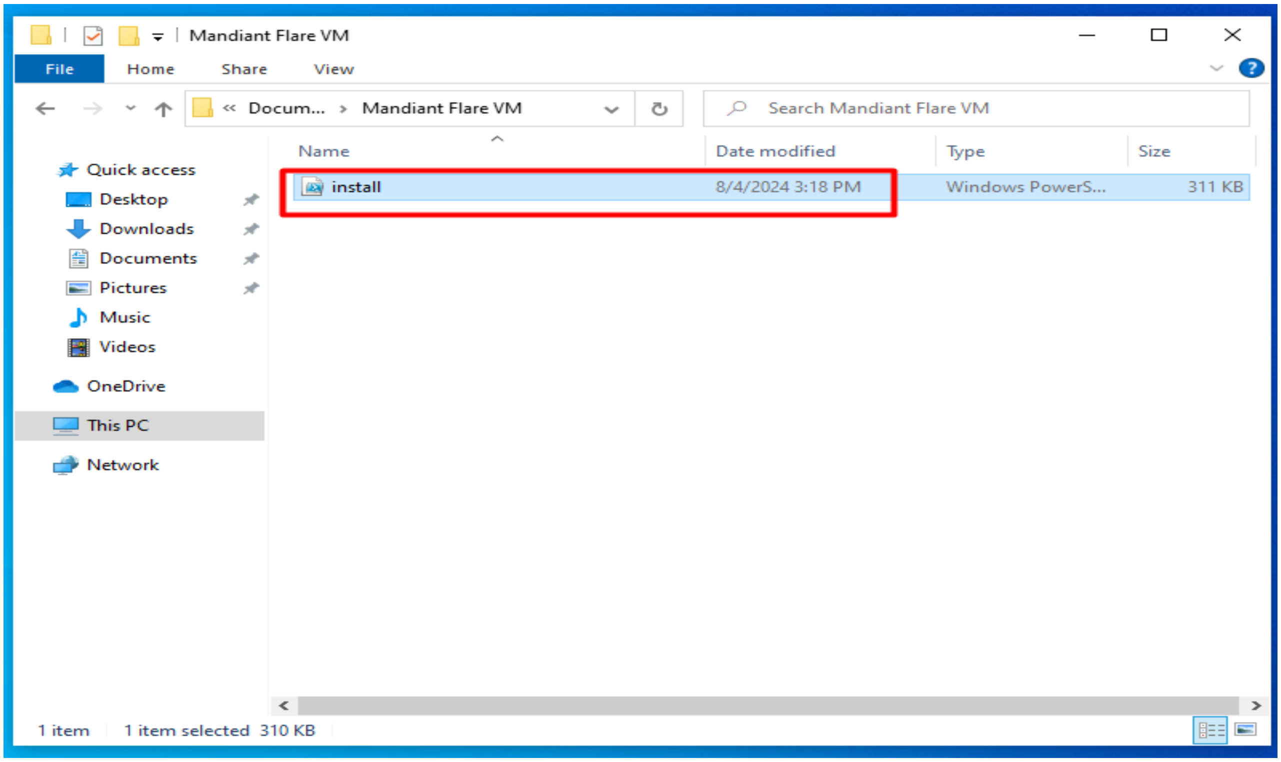
Releases

A collection of software installations scripts for Windows ...

README.md

Figure 33: - Mandiant Flare VM on Oracle VirtualBox

- Download the “install.ps1” file and run in Microsoft PowerShell. Or, Downloaded to a folder



Name	Date modified	Type	Size
install	8/4/2024 3:18 PM	Windows PowerS...	311 KB

1 item 1 item selected 310 KB

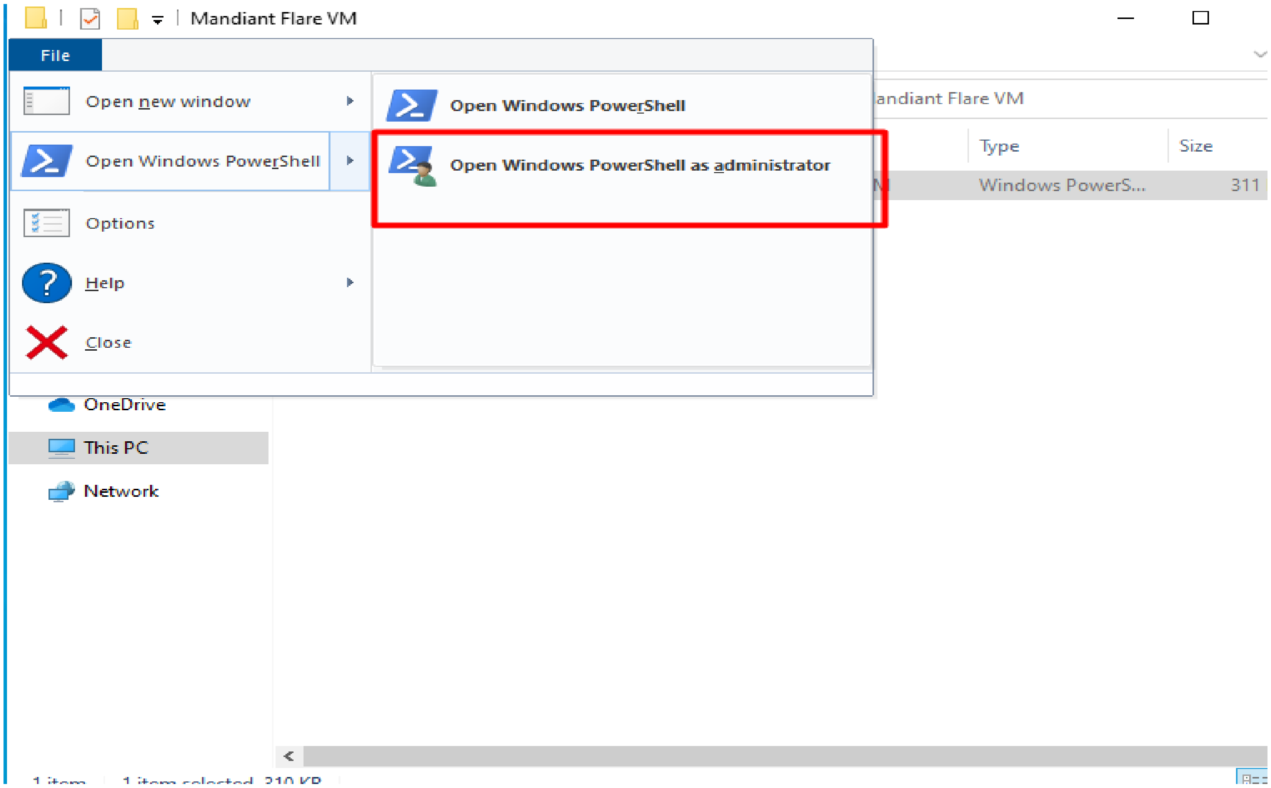
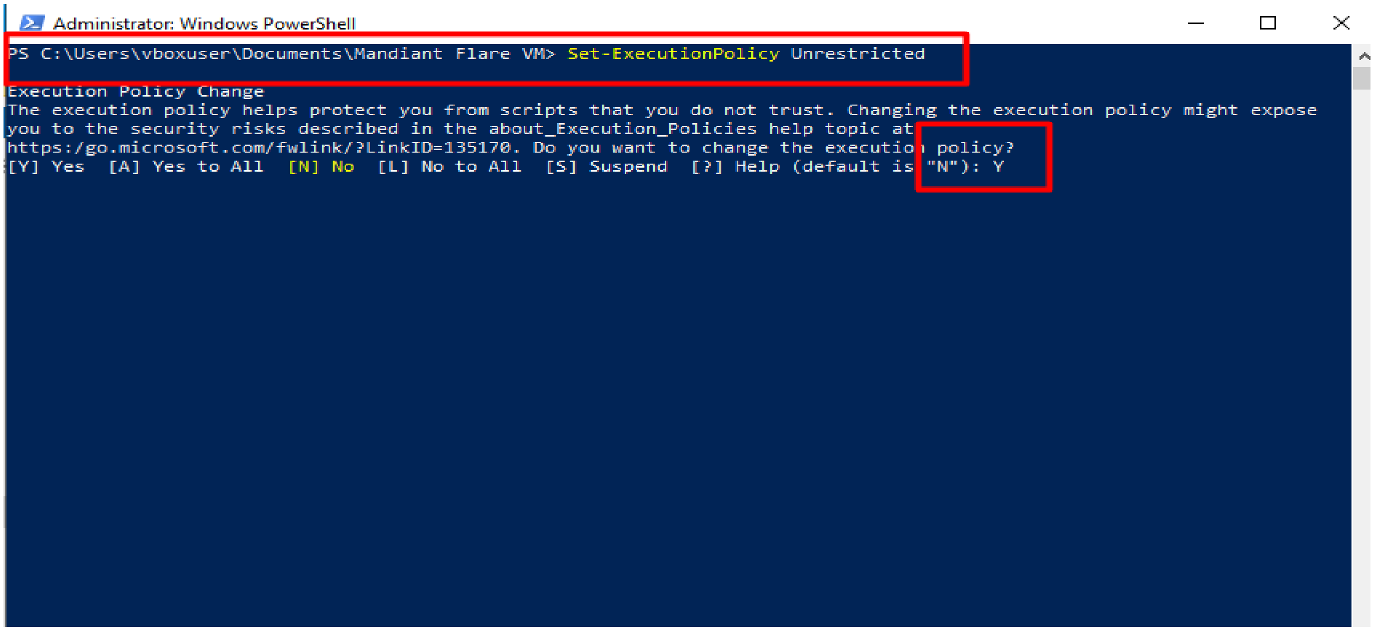


Figure 34:- Installing via Powershell

We block our script using the Unblock file command in powershell and set restriction policy



```
PS C:\Users\vboxuser\Documents\Mandiant Flare VM> Set-ExecutionPolicy Unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): Y
```

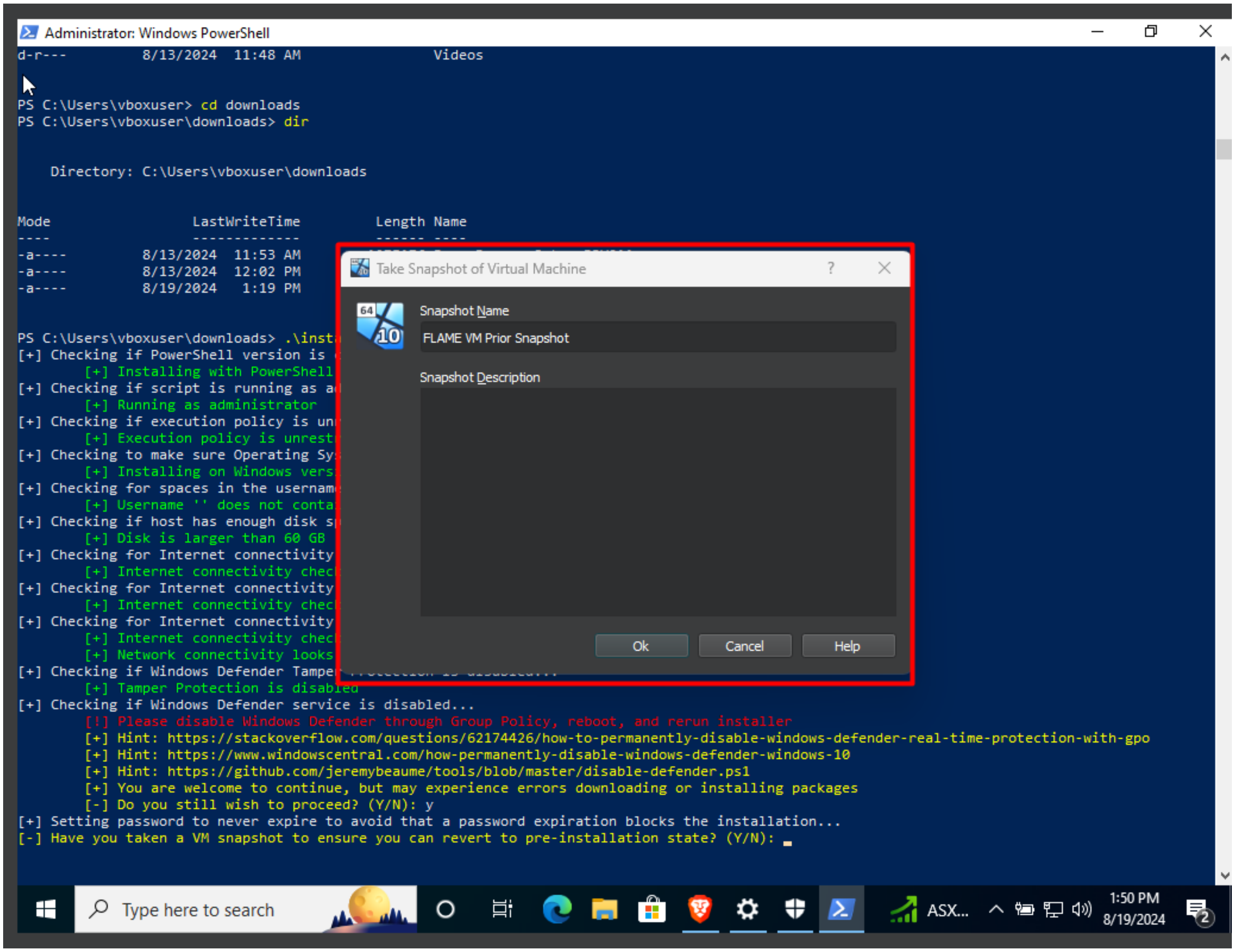
Figure 35:- Confirmation of policies and installation requirements for Mandiant Flare VM via PowerShell

If an error message saying the execution policy is overridden by a policy defined at a more specific scope, we may need to pass a scope in via "Set-ExecutionPolicy Unrestricted -Scope CurrentUser -Force" command. To view execution policies for all scopes, we execute the "Get-ExecutionPolicy -List" command

We finally, execute the installer script as follow: ".\install.ps1" Command in PowerShell

We may carry out the following activities: -

- To pass our password as an argument: .\install.ps1 -password <password>
- To use the CLI-only mode with minimal user interaction: .\install.ps1 -password <password> -noWait -noGui
- To use the CLI-only mode with minimal user interaction and a custom config file: .\install.ps1 -customConfig <config.xml> -password <password> -noWait -noGui



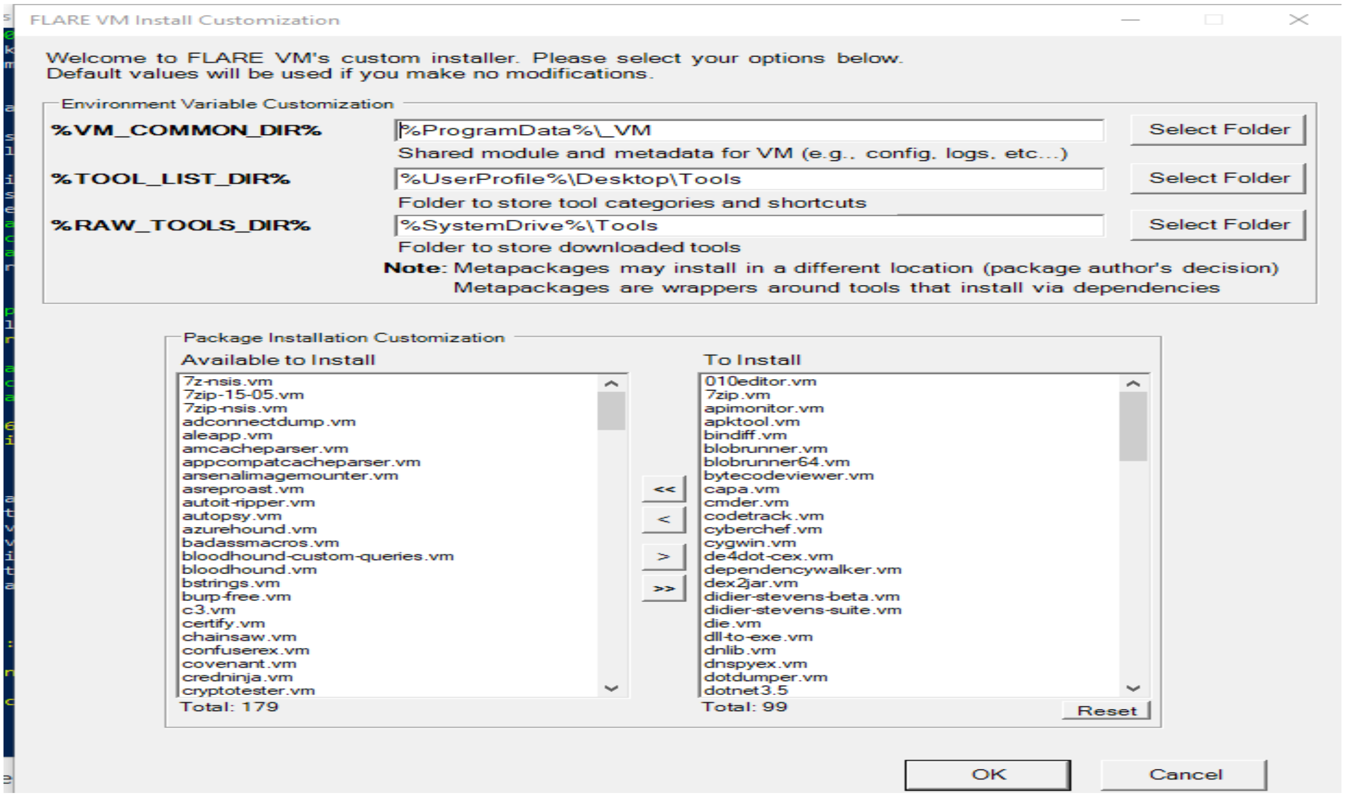
```
d-r---        8/13/2024  11:48 AM                Videos


PS C:\Users\vboxuser> cd downloads
PS C:\Users\vboxuser\downloads> dir


    Directory: C:\Users\vboxuser\downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        8/13/2024  11:53 AM
-a----        8/13/2024  12:02 PM
-a----        8/19/2024   1:19 PM


PS C:\Users\vboxuser\downloads> .\inst
[+] Checking if PowerShell version is
        [+] Installing with PowerShell
[+] Checking if script is running as a
        [+] Running as administrator
[+] Checking if execution policy is un
        [+] Execution policy is unrest
[+] Checking to make sure Operating Sy
        [+] Installing on Windows vers
[+] Checking for spaces in the usernam
        [+] Username '' does not conta
[+] Checking if host has enough disk s
        [+] Disk is larger than 60 GB
[+] Checking for Internet connectivity
        [+] Internet connectivity chec
[+] Checking for Internet connectivity
        [+] Internet connectivity chec
[+] Checking for Internet connectivity
        [+] Internet connectivity chec
        [+] Network connectivity looks
[+] Checking if Windows Defender Tampe
        [+] Tamper Protection is disabled
[+] Checking if Windows Defender service is disabled...
        [!] Please disable Windows Defender through Group Policy, reboot, and rerun installer
        [+] Hint: https://stackoverflow.com/questions/62174426/how-to-permanently-disable-windows-defender-real-time-protection-with-gpo
        [+] Hint: https://www.windowscentral.com/how-permanently-disable-windows-defender-windows-10
        [+] Hint: https://github.com/jeremybeaume/tools/blob/master/disable-defender.ps1
        [+] You are welcome to continue, but may experience errors downloading or installing packages
        [-] Do you still wish to proceed? (Y/N): y
[+] Setting password to never expire to avoid that a password expiration blocks the installation...
[-] Have you taken a VM snapshot to ensure you can revert to pre-installation state? (Y/N):
```

Snapshot Name: FLAME VM Prior Snapshot

Snapshot Description:

Figure 36: - VM snapshot before Mandiant Installation via PowerShell

We install the tools we want the “Available to Install” modal window.



Welcome to FLARE VM's custom installer. Please select your options below.
Default values will be used if you make no modifications.

Environment Variable Customization

%VM_COMMON_DIR%: %ProgramData%_VM
Shared module and metadata for VM (e.g., config, logs, etc...)

%TOOL_LIST_DIR%: %UserProfile%\Desktop\Tools
Folder to store tool categories and shortcuts

%RAW_TOOLS_DIR%: %SystemDrive%\Tools
Folder to store downloaded tools

Note: Metapackages may install in a different location (package author's decision)
Metapackages are wrappers around tools that install via dependencies

Package Installation Customization

Available to Install

```
7z-nsis.vm
7zip-15-05.vm
7zip-nsis.vm
adconnectdump.vm
aleapp.vm
amcacheparser.vm
appcompatcacheparser.vm
arsenalimagemounter.vm
asreproast.vm
autoit-ripper.vm
autopsy.vm
azurehound.vm
badassmacros.vm
bloodhound-custom-queries.vm
bloodhound.vm
bstrings.vm
burp-free.vm
c3.vm
certify.vm
chainsaw.vm
confuserex.vm
covenant.vm
credninja.vm
cryptotester.vm
```

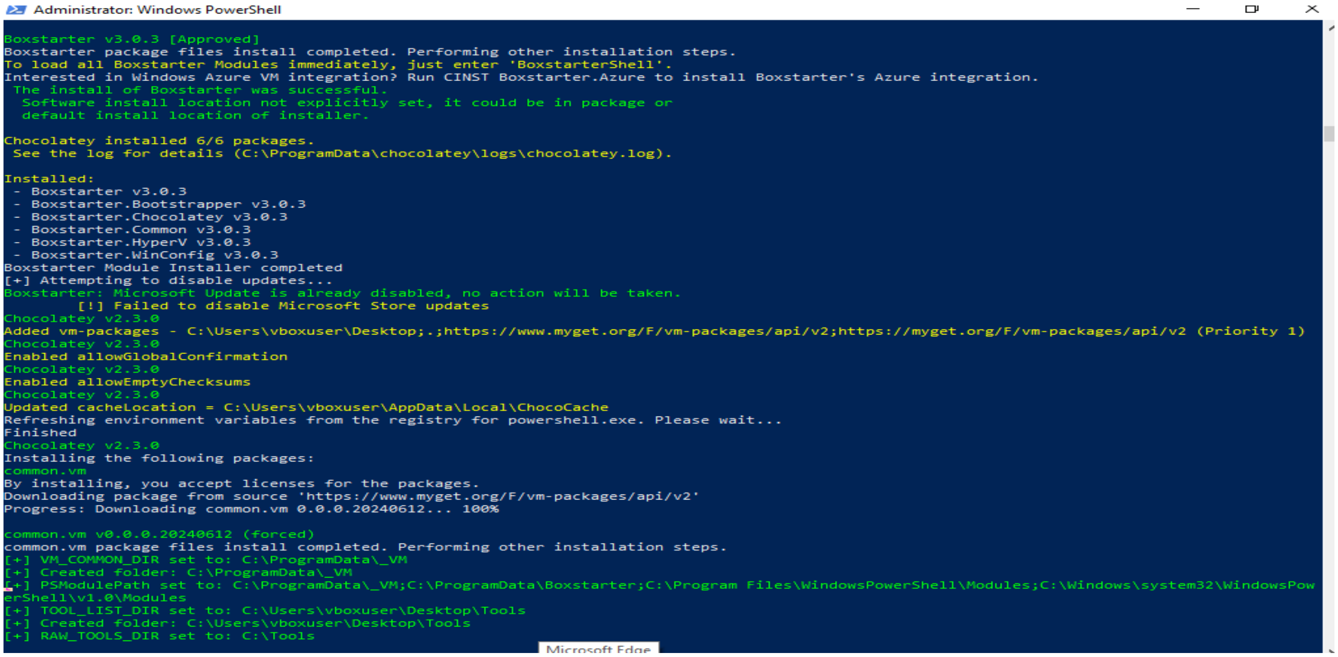
Total: 179

To Install

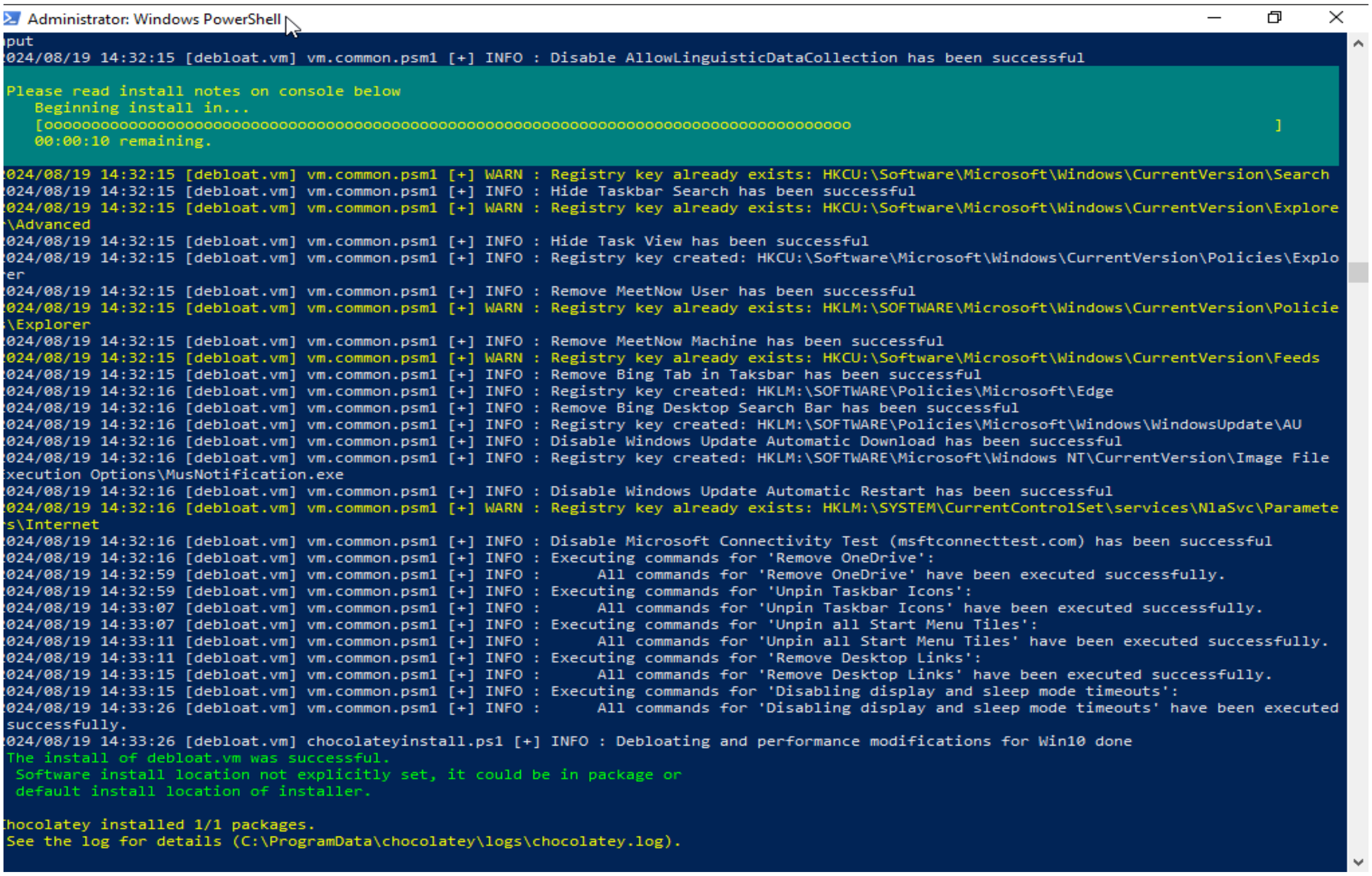
```
010editor.vm
7zip.vm
apimonitor.vm
apktool.vm
bindiff.vm
blobrunner.vm
blobrunner64.vm
bytecodeviewer.vm
capa.vm
cmder.vm
codetrack.vm
cyberchef.vm
cygwin.vm
de4dot-cex.vm
dependencywalker.vm
dex2jar.vm
didier-stevens-beta.vm
didier-stevens-suite.vm
die.vm
dll-to-exe.vm
dnlib.vm
dnspyex.vm
dotdumper.vm
dotnet3.5
```

Total: 99

Figure 37: - Custom Install on Flare VM



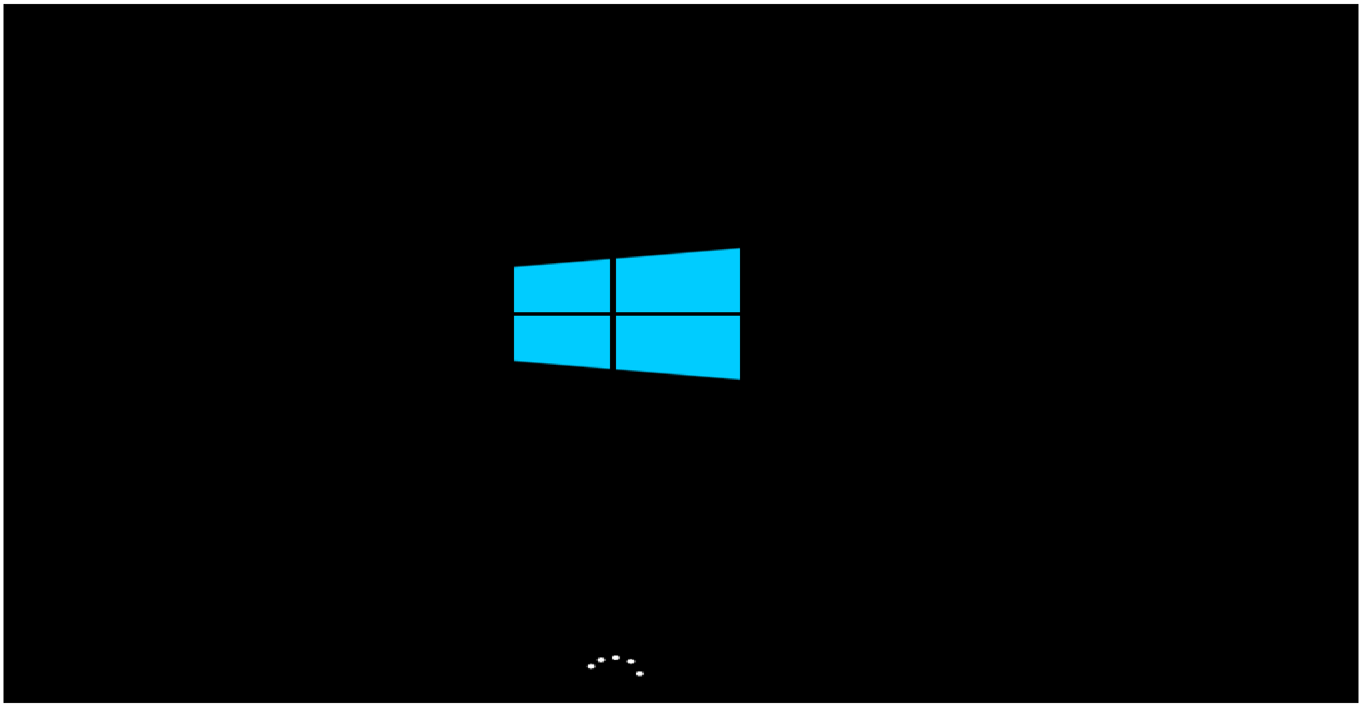
```
Boxstarter v3.0.3 [Approved]
Boxstarter package files install completed. Performing other installation steps.
To load all Boxstarter Modules immediately, just enter 'BoxstarterShell'.
Interested in Windows Azure VM integration? Run CINST Boxstarter.Azure to install Boxstarter's Azure integration.
 The install of Boxstarter was successful.
  Software install location not explicitly set, it could be in package or
  default install location of installer.

Chocolatey installed 6/6 packages.
 See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).

Installed:
 - Boxstarter v3.0.3
 - Boxstarter.Bootstrapper v3.0.3
 - Boxstarter.Chocolatey v3.0.3
 - Boxstarter.Common v3.0.3
 - Boxstarter.HyperV v3.0.3
 - Boxstarter.WinConfig v3.0.3
Boxstarter Module Installer completed
[+] Attempting to disable updates...
Boxstarter: Microsoft Update is already disabled, no action will be taken.
        [!] Failed to disable Microsoft Store updates
Chocolatey v2.3.0
Added vm-packages - C:\Users\vboxuser\Desktop;.;https://www.myget.org/F/vm-packages/api/v2;https://myget.org/F/vm-packages/api/v2 (Priority 1)
Chocolatey v2.3.0
Enabled allowGlobalConfirmation
Chocolatey v2.3.0
Enabled allowEmptyChecksums
Chocolatey v2.3.0
Updated cacheLocation = C:\Users\vboxuser\AppData\Local\ChocoCache
Refreshing environment variables from the registry for powershell.exe. Please wait...
Finished
Chocolatey v2.3.0
Installing the following packages:
common.vm
By installing, you accept licenses for the packages.
Downloading package from source 'https://www.myget.org/F/vm-packages/api/v2'
Progress: Downloading common.vm 0.0.0.20240612... 100%

common.vm v0.0.0.20240612 (forced)
common.vm package files install completed. Performing other installation steps.
[+] VM_COMMON_DIR set to: C:\ProgramData\_VM
[+] Created folder: C:\ProgramData\_VM
[+] PSModulePath set to: C:\ProgramData\_VM;C:\ProgramData\Boxstarter;C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPow
erShell\v1.0\Modules
[+] TOOL_LIST_DIR set to: C:\Users\vboxuser\Desktop\Tools
[+] Created folder: C:\Users\vboxuser\Desktop\Tools
[+] RAW_TOOLS_DIR set to: C:\Tools
```

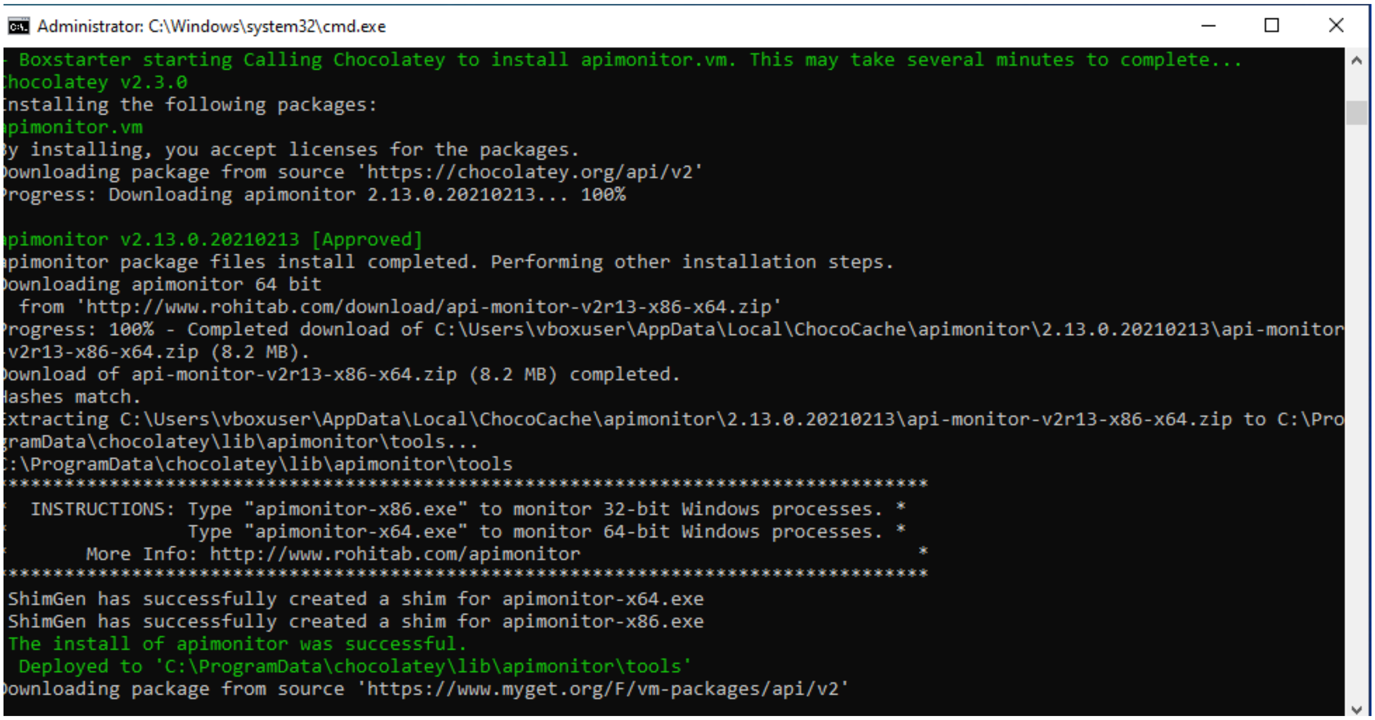


```
put
024/08/19 14:32:15 [debloat.vm] vm.common.psm1 [+] INFO : Disable AllowLinguisticDataCollection has been successful

 Please read install notes on console below
    Beginning install in...
    [oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo                                             ]
    00:00:10 remaining.

024/08/19 14:32:15 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\Windows\CurrentVersion\Search
024/08/19 14:32:15 [debloat.vm] vm.common.psm1 [+] INFO : Hide Taskbar Search has been successful
024/08/19 14:32:15 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\Windows\CurrentVersion\Explore
\Advanced
024/08/19 14:32:15 [debloat.vm] vm.common.psm1 [+] INFO : Hide Task View has been successful
024/08/19 14:32:15 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKCU:\Software\Microsoft\Windows\CurrentVersion\Policies\Explo
er
024/08/19 14:32:15 [debloat.vm] vm.common.psm1 [+] INFO : Remove MeetNow User has been successful
024/08/19 14:32:15 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policie
\Explorer
024/08/19 14:32:15 [debloat.vm] vm.common.psm1 [+] INFO : Remove MeetNow Machine has been successful
024/08/19 14:32:15 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\Windows\CurrentVersion\Feeds
024/08/19 14:32:15 [debloat.vm] vm.common.psm1 [+] INFO : Remove Bing Tab in Taksbar has been successful
024/08/19 14:32:16 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Policies\Microsoft\Edge
024/08/19 14:32:16 [debloat.vm] vm.common.psm1 [+] INFO : Remove Bing Desktop Search Bar has been successful
024/08/19 14:32:16 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
024/08/19 14:32:16 [debloat.vm] vm.common.psm1 [+] INFO : Disable Windows Update Automatic Download has been successful
024/08/19 14:32:16 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
xecution Options\MusNotification.exe
024/08/19 14:32:16 [debloat.vm] vm.common.psm1 [+] INFO : Disable Windows Update Automatic Restart has been successful
024/08/19 14:32:16 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKLM:\SYSTEM\CurrentControlSet\services\NlaSvc\Paramete
s\Internet
024/08/19 14:32:16 [debloat.vm] vm.common.psm1 [+] INFO : Disable Microsoft Connectivity Test (msftconnecttest.com) has been successful
024/08/19 14:32:16 [debloat.vm] vm.common.psm1 [+] INFO : Executing commands for 'Remove OneDrive':
024/08/19 14:32:59 [debloat.vm] vm.common.psm1 [+] INFO :      All commands for 'Remove OneDrive' have been executed successfully.
024/08/19 14:32:59 [debloat.vm] vm.common.psm1 [+] INFO : Executing commands for 'Unpin Taskbar Icons':
024/08/19 14:33:07 [debloat.vm] vm.common.psm1 [+] INFO :      All commands for 'Unpin Taskbar Icons' have been executed successfully.
024/08/19 14:33:07 [debloat.vm] vm.common.psm1 [+] INFO : Executing commands for 'Unpin all Start Menu Tiles':
024/08/19 14:33:11 [debloat.vm] vm.common.psm1 [+] INFO :      All commands for 'Unpin all Start Menu Tiles' have been executed successfully.
024/08/19 14:33:11 [debloat.vm] vm.common.psm1 [+] INFO : Executing commands for 'Remove Desktop Links':
024/08/19 14:33:15 [debloat.vm] vm.common.psm1 [+] INFO :      All commands for 'Remove Desktop Links' have been executed successfully.
024/08/19 14:33:15 [debloat.vm] vm.common.psm1 [+] INFO : Executing commands for 'Disabling display and sleep mode timeouts':
024/08/19 14:33:26 [debloat.vm] vm.common.psm1 [+] INFO :      All commands for 'Disabling display and sleep mode timeouts' have been executed
successfully.
024/08/19 14:33:26 [debloat.vm] chocolateyinstall.ps1 [+] INFO : Debloating and performance modifications for Win10 done
 The install of debloat.vm was successful.
  Software install location not explicitly set, it could be in package or
  default install location of installer.

hocolatey installed 1/1 packages.
 See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).
```

Figure 38: - Run the Flare VM installation

- The application will continue to restart and continue with the installation





Administrator: C:\Windows\system32\cmd.exe

```
- Boxstarter starting Calling Chocolatey to install apimonitor.vm. This may take several minutes to complete...
hocolatey v2.3.0
nstalling the following packages:
pimonitor.vm
y installing, you accept licenses for the packages.
ownloading package from source 'https://chocolatey.org/api/v2'
rogress: Downloading apimonitor 2.13.0.20210213... 100%

pimonitor v2.13.0.20210213 [Approved]
pimonitor package files install completed. Performing other installation steps.
ownloading apimonitor 64 bit
  from 'http://www.rohitab.com/download/api-monitor-v2r13-x86-x64.zip'
rogress: 100% - Completed download of C:\Users\vboxuser\AppData\Local\ChocoCache\apimonitor\2.13.0.20210213\api-monitor
-v2r13-x86-x64.zip (8.2 MB).
ownload of api-monitor-v2r13-x86-x64.zip (8.2 MB) completed.
ashes match.
xtracting C:\Users\vboxuser\AppData\Local\ChocoCache\apimonitor\2.13.0.20210213\api-monitor-v2r13-x86-x64.zip to C:\Pro
gramData\chocolatey\lib\apimonitor\tools...
:\ProgramData\chocolatey\lib\apimonitor\tools
*********************************************************************************
*  INSTRUCTIONS: Type "apimonitor-x86.exe" to monitor 32-bit Windows processes. *
*                Type "apimonitor-x64.exe" to monitor 64-bit Windows processes. *
*       More Info: http://www.rohitab.com/apimonitor                             *
*********************************************************************************
 ShimGen has successfully created a shim for apimonitor-x64.exe
 ShimGen has successfully created a shim for apimonitor-x86.exe
 The install of apimonitor was successful.
  Deployed to 'C:\ProgramData\chocolatey\lib\apimonitor\tools'
ownloading package from source 'https://www.myget.org/F/vm-packages/api/v2'
```

- Once download is completed, save the log file

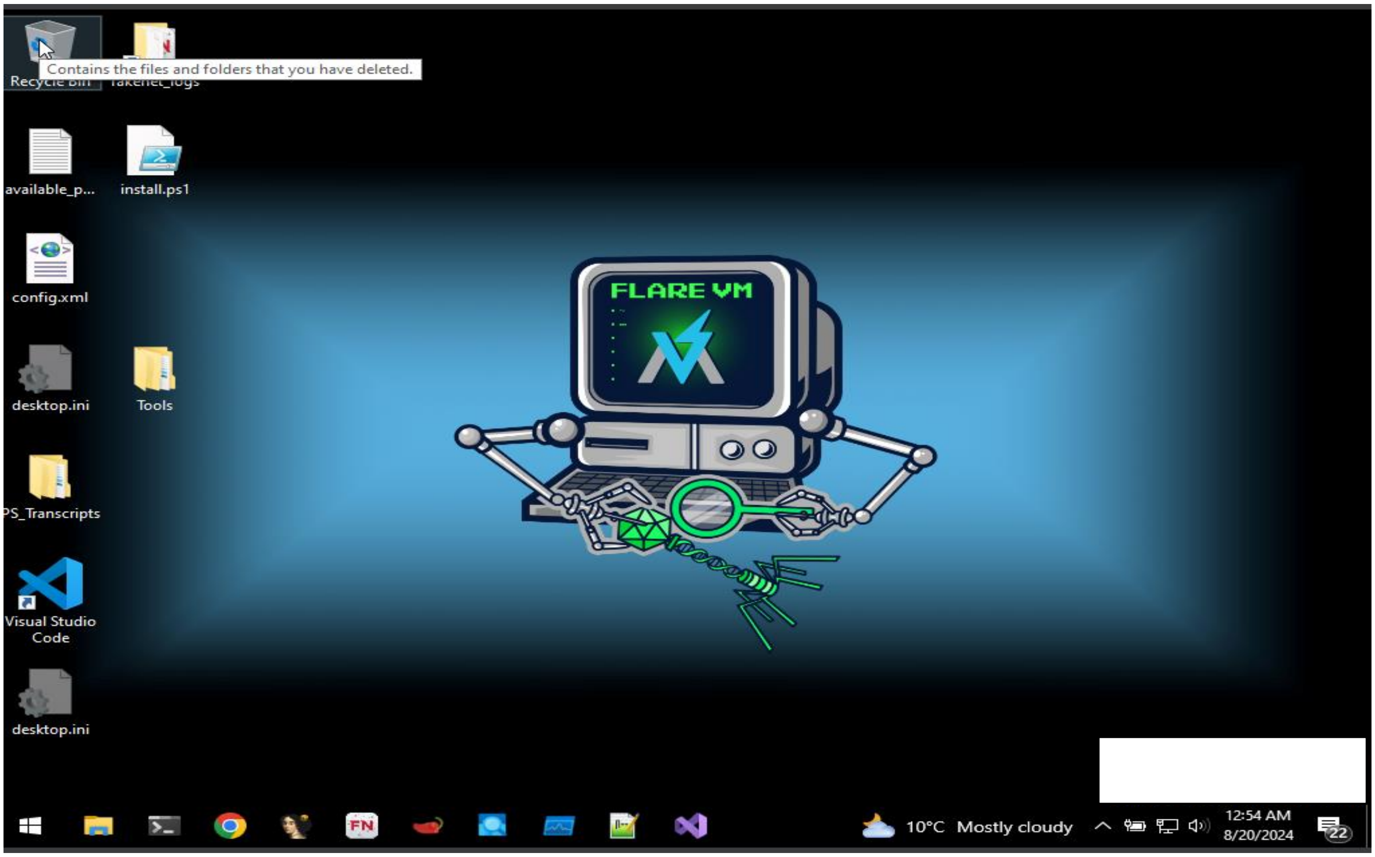
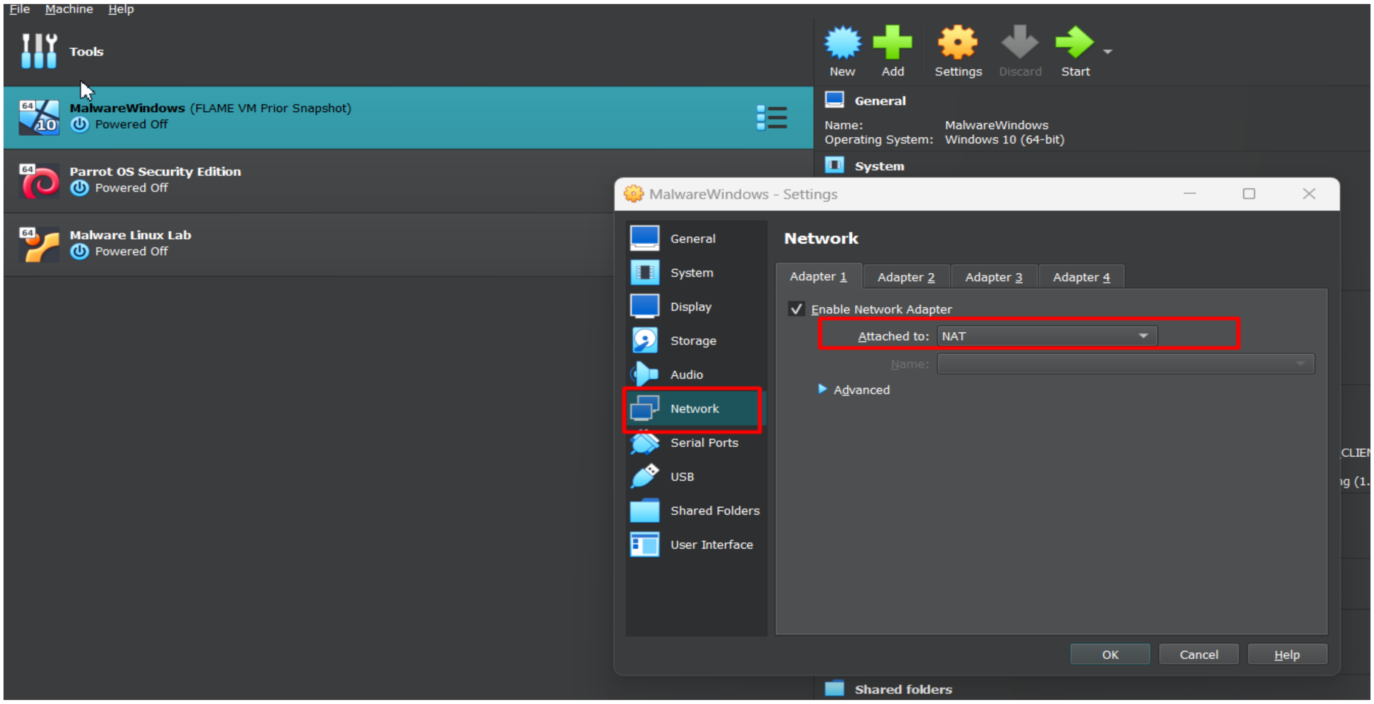


Figure 39: - Completed Installation - Flare VM

5.19. Protecting our Environment

To keep your Virtual Machine (VM) isolated from your main network and prevent any accidental spread of malware, you can configure VirtualBox's network settings to use a private network or a host-only adapter. Here are the steps to achieve this:

- **Configuring a Host-Only Adapter in VirtualBox**
- **Open VirtualBox:**
    - Start VirtualBox on your host machine.
- **Select Your VM:**
    - Click on the VM (e.g., FLARE VM) you want to configure.
- **Open VM Settings:**
    - Click on the "Settings" button.
- **Navigate to Network Settings:**
    - In the Settings window, go to the "Network" section.
- **Enable Network Adapter:**
    - Ensure that "Adapter 1" (or another adapter) is enabled by checking the "Enable Network Adapter" box.



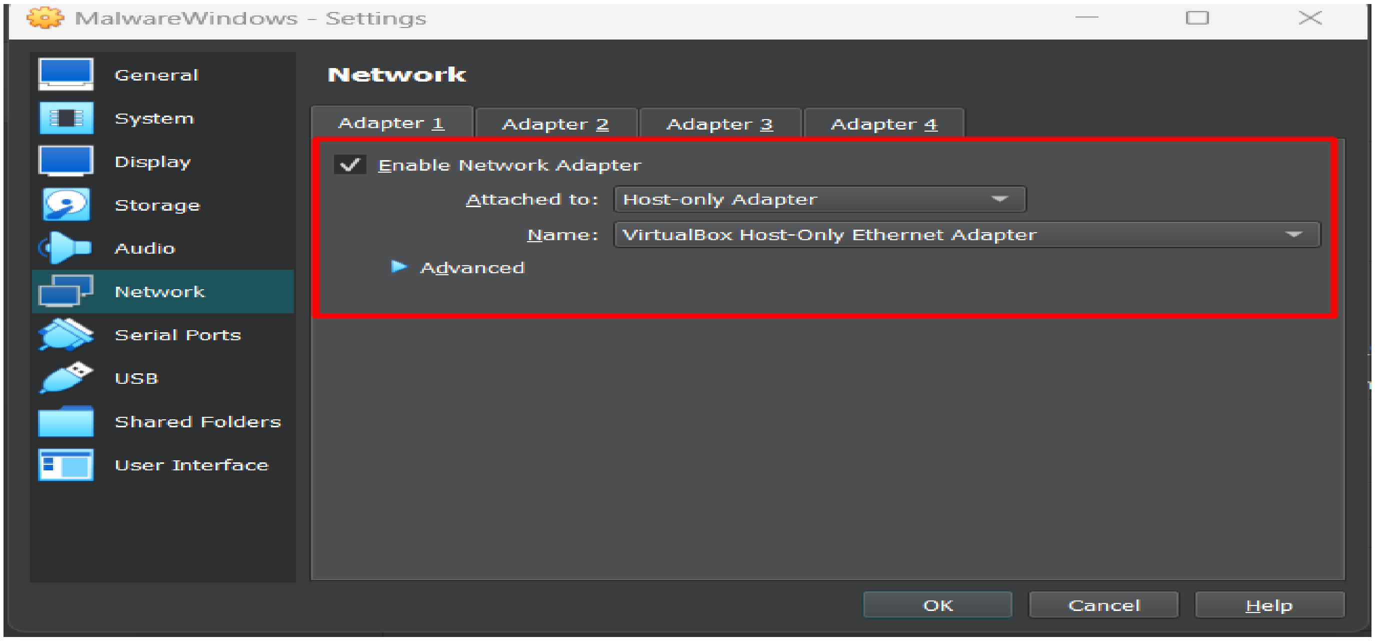
Name: MalwareWindows
Operating System: Windows 10 (64-bit)

☑ Enable Network Adapter
Attached to: NAT
Name:

Figure 40: - Hardening virtual environment

- **Select Adapter Type:**
    - In the "Attached to" dropdown menu, select "Host-only Adapter."

- **Choose Host-Only Network:**
    - In the "Name" dropdown menu, select the host-only network you want to use. If no host-only network is available, you may need to create one.



MalwareWindows - Settings

Network

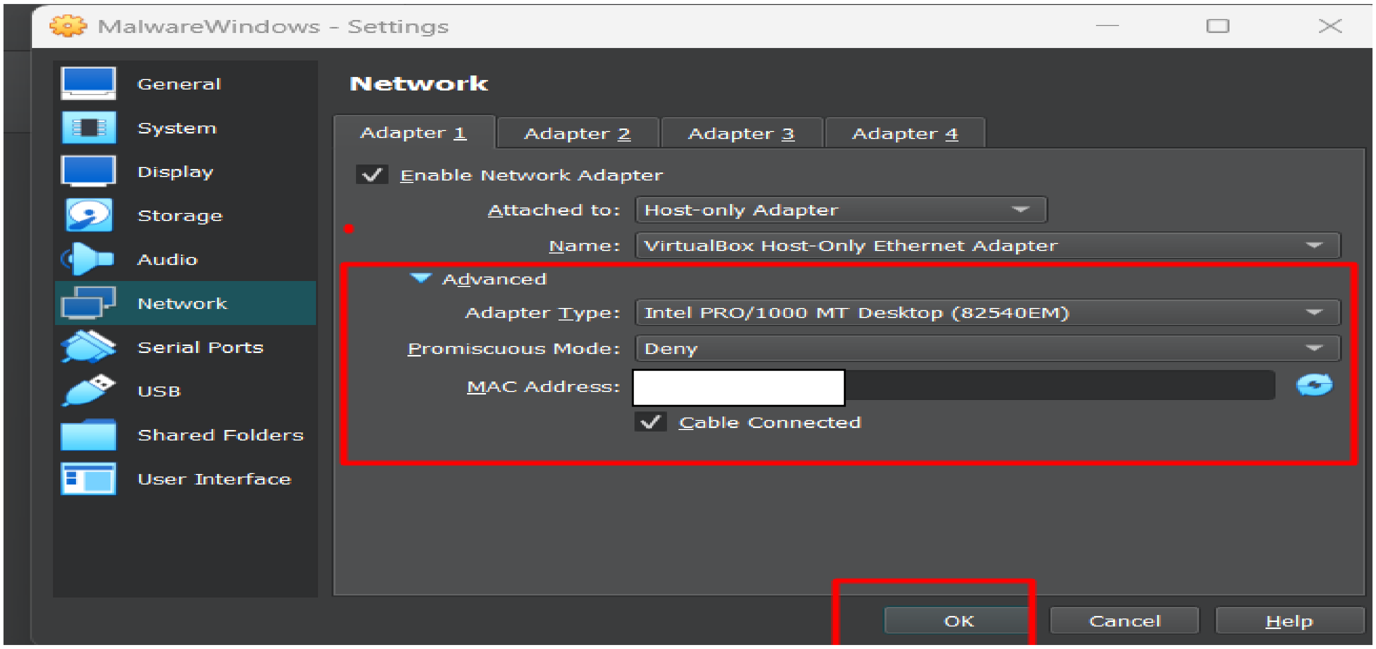
☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

▶ Advanced

Figure 41: - Confirming network adapter setup



MalwareWindows - Settings

Network

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

▼ Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address:

☑ Cable Connected

- **Creating a Host-Only Network**

If you need to create a new host-only network, follow these steps:

- **Open VirtualBox Preferences:**
    - Go to "File" > "Host Network Manager."

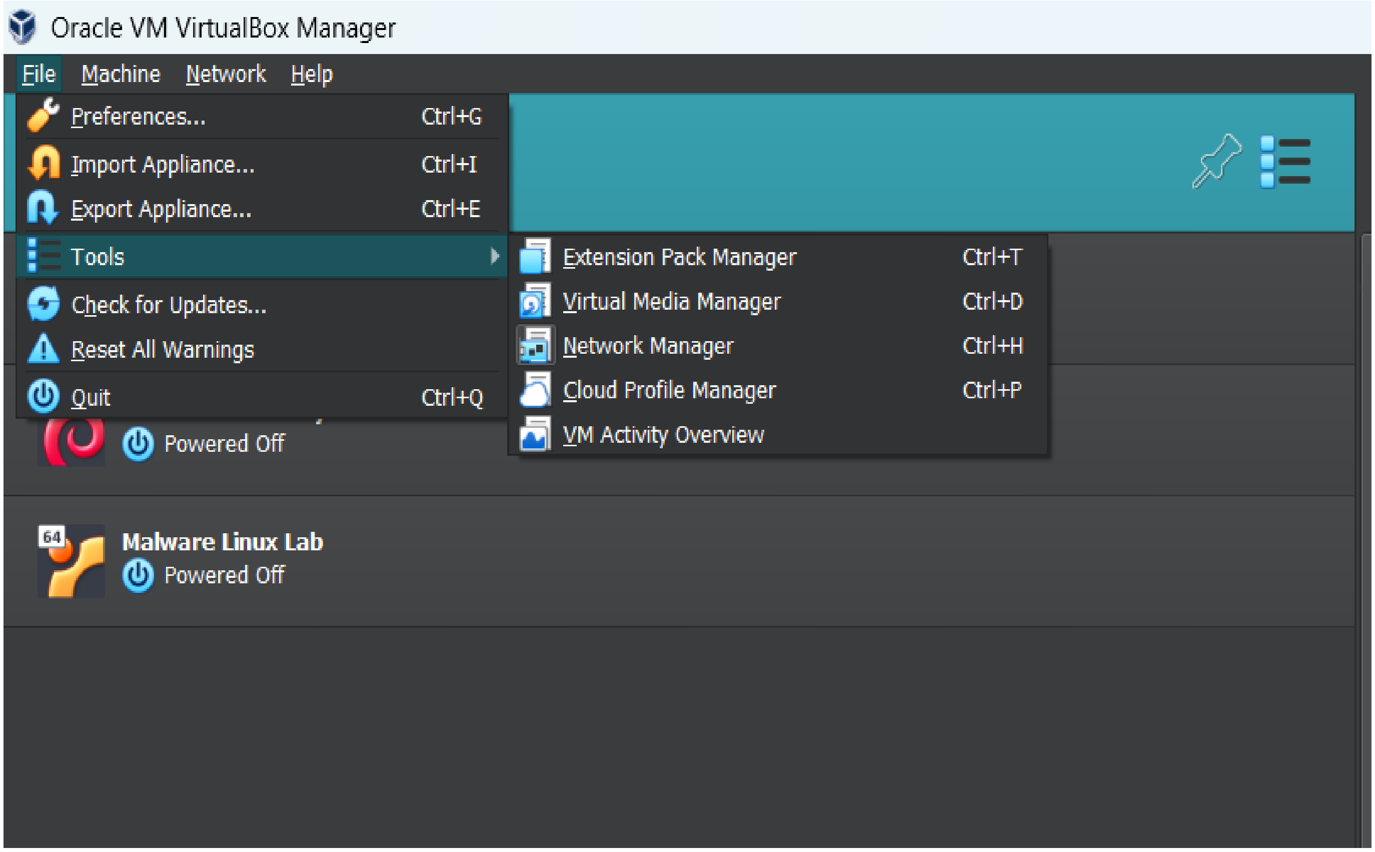
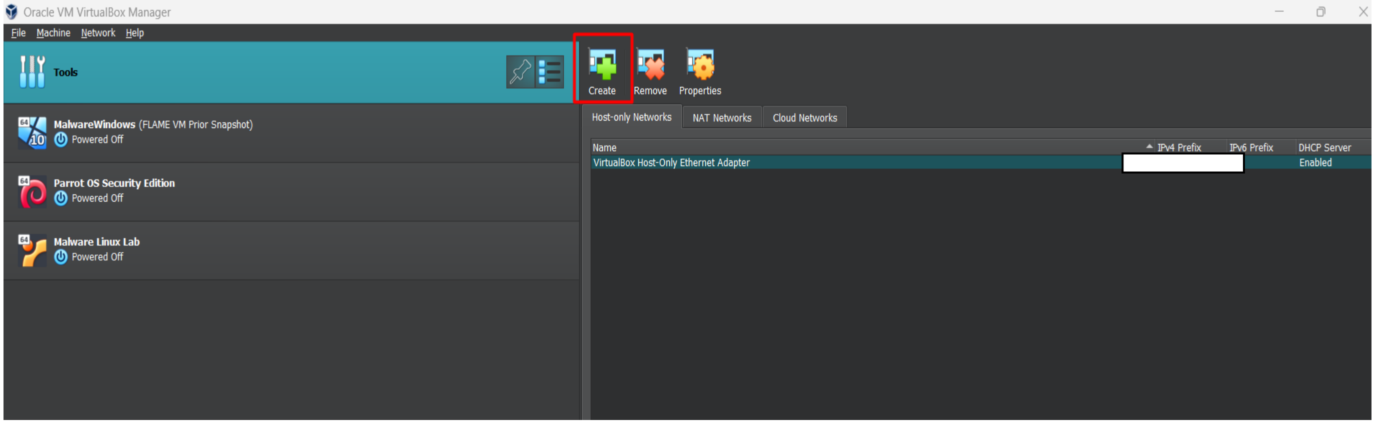

Oracle VM VirtualBox Manager
File Machine Network Help
Preferences... Ctrl+G
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
Tools
Check for Updates...
Reset All Warnings
Quit Ctrl+Q
Extension Pack Manager Ctrl+T
Virtual Media Manager Ctrl+D
Network Manager Ctrl+H
Cloud Profile Manager Ctrl+P
VM Activity Overview
Powered Off
Malware Linux Lab
Powered Off

Figure 42: - Configuring Tools to manage Network adapter - Hardening

- **Create a New Network:**
    - Click on the "Create" button to add a new host-only network.



Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
VirtualBox Host-Only Ethernet Adapter	[redacted]		Enabled

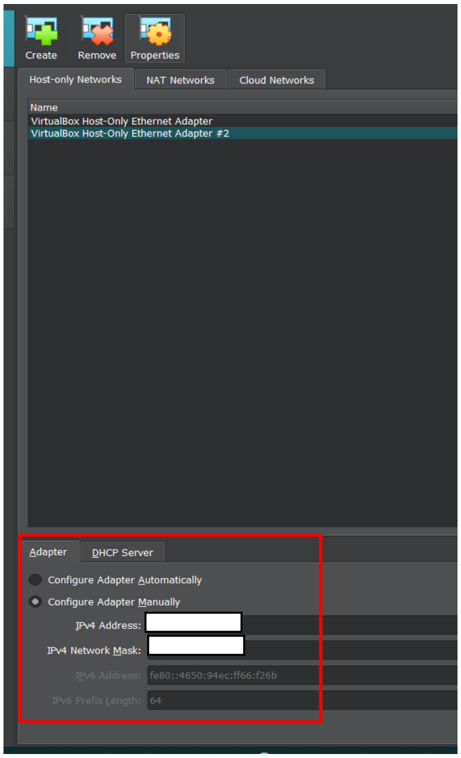
Figure 43: - Configuring Tools to manage Network adapter - Hardening 2

- **Configure the Network:**

  - You can configure the network settings such as IP address range, DHCP server, etc., if necessary. The default settings usually suffice for isolation purposes.

- **Apply Settings:**
  - Click "OK" to apply the settings and close the Host Network Manager.
- **Verify Network Isolation**

After setting up the host-only adapter, verify that your VM is isolated:



Name
VirtualBox Host-Only Ethernet Adapter
VirtualBox Host-Only Ethernet Adapter #2

○ Configure Adapter Automatically
● Configure Adapter Manually
IPv4 Address: [redacted]
IPv4 Network Mask: [redacted]
IPv6 Address: fe80::4650:94ec:ff66:f26b
IPv6 Prefix Length: 64

Figure 44:- Configuring Tools to manage Network adapter - Hardening 3

1. **Start the VM:**
   - Boot up the VM and log in.
2. **Check Network Connectivity:**
   - Ensure that the VM can communicate with the host machine and other VMs on the host-only network, but not with the internet or other devices on your main network.
3. **Test Isolation:**
   - Try pinging external IP addresses (e.g., 8.8.8.8) or domain names (e.g., google.com) from the VM. The ping should fail, indicating that the VM is isolated from the internet.

- **Additional Security Measures**
- **Snapshots:**
  - Take a snapshot of your VM before performing any malware analysis. This allows you to revert to a clean state if needed.
- **Firewall Rules:**
  - Configure your host machine's firewall to restrict network traffic from the VM if additional isolation is required.
- **Limited Shared Folders:**
  - Use shared folders sparingly and with caution. Ensure that shared folders have appropriate permissions to prevent unauthorized access.

By following these steps, you can ensure that your malware analysis VM is isolated from your main network, reducing the risk of accidental malware spread.

Steps to Test Isolation

- **Open Command Prompt:**
  - On your Windows VM, press Win + R to open the Run dialog.
  - Type “cmd” and press Enter to open the Command Prompt.

- **Ping an External IP Address:**
    - In the Command Prompt window, type the following command and press Enter:
    - ping 8.8.8.8
    - This will attempt to ping Google's public DNS server.
- **Ping an External Domain Name:**
    - In the Command Prompt window, type the following command and press Enter:
    - ping google.com
    - This will attempt to ping the Google website.

Expected Results

- If your VM is properly isolated from the internet, you should see output like the following for both commands:

Troubleshooting

If the ping does not fail (i.e., if you receive replies), the VM is not properly isolated. You should:

1. **Check Network Settings:**
    - Ensure that the network adapter in VirtualBox is set to "Host-only Adapter."
    - Verify that you selected the correct host-only network.
2. **Reconfigure Network:**
    - If necessary, recreate the host-only network in VirtualBox and reassign it to the VM.
3. **Restart the VM:**
    - Sometimes changes to network settings may require restarting the VM for them to take effect.

6. REFERENCES

Amazon (2024). *What is Virtualization? - Cloud Computing Virtualization - AWS*. [online] Amazon Web Services, Inc. Available at: https://aws.amazon.com/what-is/virtualization/#:~:text=Virtualization%20is%20technology%20that%20you.

Oracle.com. (2020). *Oracle VM VirtualBox*. [online] Available at: https://www.oracle.com/au/virtualization/virtualbox/.