

# Entorno de Pruebas en Ciberseguridad: Diseña tu Propio Laboratorio Virtual

- Miércoles mayo 29 de 2024
- 7 a 10 PM
- Microsoft Teams

## Seo Rodríguez, MBA

CISSP, CISM, CRISC, CISA, CySA+, Pentest+, Security+, M365 Security, ITIL

[Seo@certtoday.com](mailto:Seo@certtoday.com) | CertToday.com | LinkedIn: <https://www.linkedin.com/in/seolito>

En el campo de la ciberseguridad, la práctica y la experimentación son cruciales para desarrollar habilidades robustas y conocimientos profundos. Un laboratorio virtual, especialmente a través de herramientas como VirtualBox, proporciona un entorno seguro y controlado donde los aprendices pueden sumergirse en escenarios reales sin riesgos. Aquí, los estudiantes pueden configurar, probar y desmontar sistemas sin temor a causar daños reales. Esto permite una exploración profunda de vulnerabilidades, técnicas de hacking, y métodos de defensa, haciendo que la teoría cobre vida. Esencialmente, un laboratorio virtual es la piedra angular del aprendizaje en ciberseguridad, donde la teoría se encuentra con la práctica en un escenario dinámico y realista.

## Contenido

Introducción .....	3
Instalación y configuración de VirtualBox.....	3
Introducción a la virtualización.....	3
Configuración de un laboratorio virtual .....	7
Un primer vistazo a VirtualBox .....	8
Instalación de Kali como Virtual Appliance .....	20
Descargar e importar la máquina virtual.....	22
Cambiar el nombre de la máquina virtual .....	23
Cámbialo a Nat Network.....	23
Inicio de la máquina virtual .....	25
Cambiar la resolución.....	25
Instalación de Windows 11 .....	27
Crear medios de instalación de Windows 11 .....	28
Nueva máquina virtual de Windows 11.....	32
Elija la imagen ISO de Windows 11 desde la que arrancar.....	34
Adiciones de invitados .....	57
Instalación de Windows Server 2022 como controlador de dominio .....	58
Creación de una máquina virtual de Windows Server 2022 .....	59
Instalación de Windows Server 2022.....	62
Configurar el servidor.....	66
Convertir en un controlador de dominio .....	76
Agregar Windows 11 como miembro de Dominio .....	88
Herramientas adicionales.....	93
Instalación de Nessus.....	93
WireShark .....	106
Zenmap .....	109
Advanced IP Scanner .....	114

VeraCrypt.....	116
Conclusión.....	127

## Introducción

El objetivo principal de este laboratorio es proporcionar a los estudiantes y profesionales de la ciberseguridad un entorno realista y seguro donde puedan aprender, practicar y perfeccionar habilidades técnicas esenciales.

A través del uso de VirtualBox para crear máquinas virtuales, los participantes pueden simular redes y sistemas informáticos complejos para explorar y contrarrestar diversas amenazas y vulnerabilidades cibernéticas sin el riesgo de afectar infraestructuras reales.

Esto facilita una comprensión profunda de los conceptos de ciberseguridad y promueve el desarrollo de competencias críticas en la detección, respuesta y mitigación de incidentes de seguridad, preparando a los individuos para enfrentar desafíos reales en entornos operativos.

## Instalación y configuración de VirtualBox

### Introducción a la virtualización

La virtualización es una tecnología fundamental que permite la creación de entornos simulados o "virtuales", separados del hardware físico subyacente. Esta capacidad es esencial en numerosos aspectos de la tecnología de la información, desde la gestión de servidores hasta el desarrollo de software y la ciberseguridad. A continuación, se presentan algunos puntos clave sobre la virtualización:

#### ¿Qué es la virtualización?

1. **Definición:** La virtualización implica el uso de software para simular la existencia de hardware y crear un sistema virtual. Esto permite a las organizaciones ejecutar múltiples sistemas operativos y aplicaciones en un solo servidor físico.

2. **Componentes:** Incluye el hipervisor, que es el software que se ejecuta directamente sobre el hardware y que gestiona las máquinas virtuales, asignando recursos como CPU, memoria y almacenamiento según sea necesario.

## Tipos de Virtualización

1. **Virtualización de servidores:** Permite dividir un servidor físico en varios servidores virtuales independientes. Cada servidor virtual puede ejecutar su propio sistema operativo y aplicaciones.
2. **Virtualización de escritorios:** Facilita a los usuarios acceder a sus escritorios personales desde cualquier dispositivo, ya que el escritorio está hospedado en un servidor central.
3. **Virtualización de redes:** Simula hardware de red, permitiendo a las organizaciones dividir, agrupar y simplificar redes físicas en estructuras lógicas.

## Beneficios de la Virtualización

1. **Eficiencia de recursos:** Mejora la utilización de los recursos del hardware al permitir que múltiples entidades comparten un solo recurso físico de manera eficiente.
2. **Reducción de costos:** Disminuye los costos operativos y de capital al reducir la necesidad de hardware físico y el consumo de energía asociado.
3. **Flexibilidad y escalabilidad:** Facilita la administración de cargas de trabajo al permitir el fácil despliegue, clonación y movimiento de entornos virtuales.
4. **Recuperación ante desastres:** Mejora las capacidades de recuperación ante desastres y continuidad del negocio debido a la facilidad de replicación y seguridad de las máquinas virtuales.

## Importancia en Ciberseguridad

1. **Entornos de prueba seguros:** Permite la creación de entornos de prueba y simulación seguros para entrenar en técnicas de ciberseguridad sin poner en riesgo infraestructuras reales.
2. **Aislamiento de amenazas:** Ayuda a aislar software potencialmente malicioso o experimentar con configuraciones de seguridad en un entorno controlado y reversible.

En conclusión, la virtualización es una piedra angular de la tecnología moderna que apoya la innovación y la seguridad, proporcionando plataformas versátiles para el despliegue de soluciones de TI y prácticas de ciberseguridad avanzadas.

**Los hipervisores**, también conocidos como monitores de máquinas virtuales (VMM), son fundamentales para la tecnología de virtualización. Se clasifican en dos tipos principales, conocidos como hipervisor Tipo 1 y Tipo 2, cada uno con características y usos específicos.

## Hipervisores Tipo 1 y Tipo 2

### Hipervisor Tipo 1

1. **Definición y Funcionamiento:** Operan directamente sobre el hardware del host, sin necesidad de un sistema operativo subyacente, lo que los clasifica como hipervisores nativos o de bare-metal.
2. **Ventajas:** Ofrecen alto rendimiento y eficiencia, ideales para entornos empresariales y data centers. Tienen una superficie de ataque menor, aumentando la seguridad.
3. **Ejemplos:** VMware ESXi, Microsoft Hyper-V, Xen.

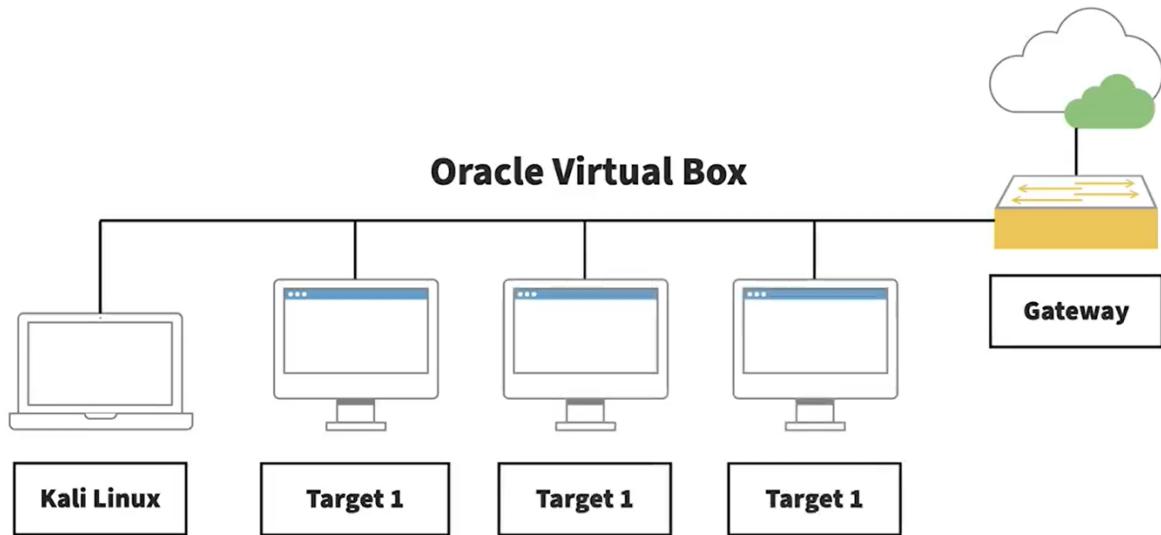
### Hipervisor Tipo 2

1. **Definición y Funcionamiento:** Funcionan como una aplicación dentro de un sistema operativo existente, siendo conocidos como hipervisores alojados.
2. **Ventajas:** Proporcionan flexibilidad y son fáciles de instalar, ideales para uso en desarrollo, pruebas y entornos educativos. Soportan una variedad de sistemas operativos.
3. **Ejemplos:** VMware Workstation, Oracle VirtualBox, Microsoft Virtual PC.

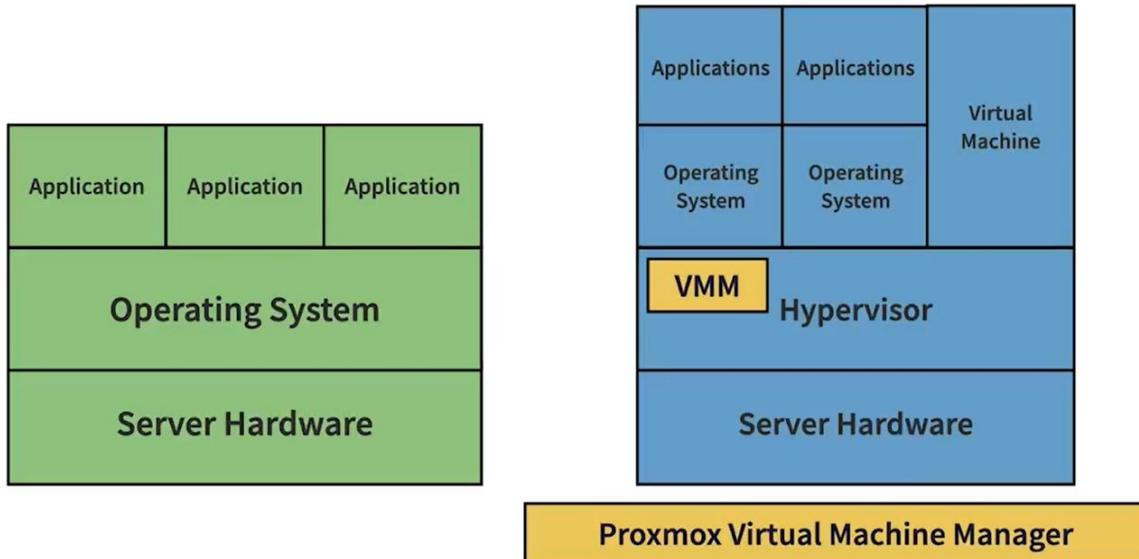
### Selección y Uso

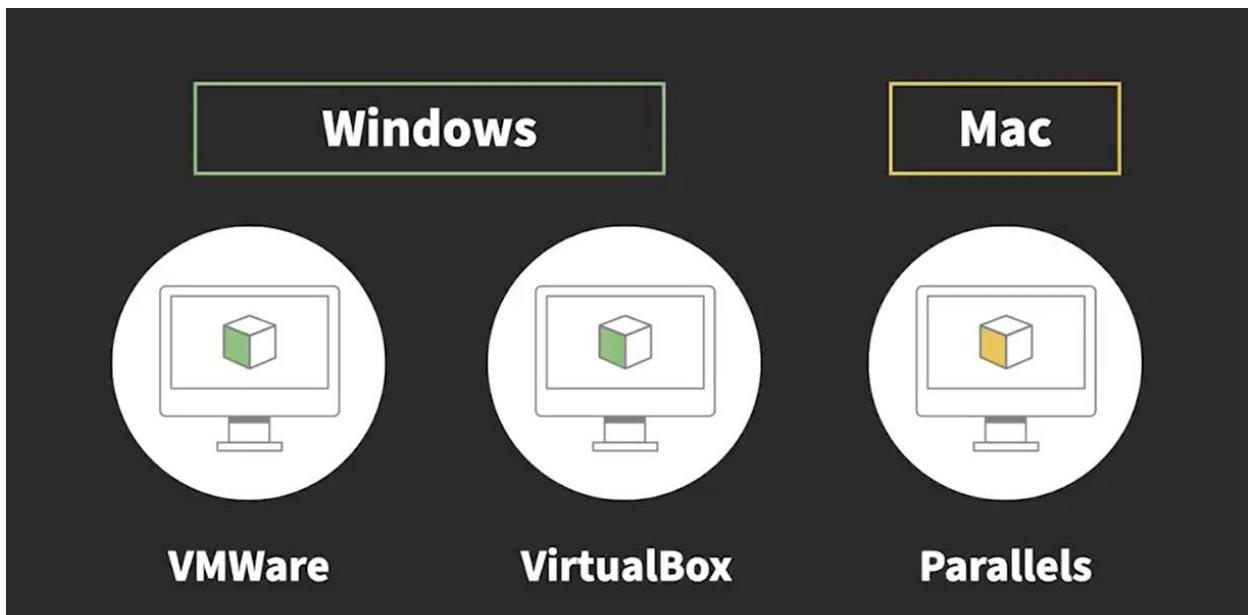
1. **Criterios de Elección:** Los hipervisores Tipo 1 son preferibles en entornos donde se requieren alto rendimiento y seguridad, mientras que los Tipo 2 son más adecuados para pruebas y entornos de desarrollo debido a su flexibilidad y facilidad de uso.
2. **Consideraciones de Seguridad:** Los hipervisores Tipo 1 proporcionan un mejor aislamiento y menor vulnerabilidad a ataques externos, en contraste, los Tipo 2

pueden estar expuestos a vulnerabilidades del sistema operativo anfitrión pero permiten configurar rápidamente entornos seguros para pruebas.



## Hardware Virtualization





# VirtualBox

Start Page

## Welcome to VirtualBox.org!

VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, high performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 3. See "About VirtualBox" for an introduction.

Presently, VirtualBox runs on Windows, Linux, macOS, and Solaris hosts and supports a large number of guest operating systems including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, 7, 8, Windows 10 and Windows 11), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x, 4.x, 5.x and 6.x), Solaris and OpenSolaris, OS/2, OpenBSD, NetBSD and FreeBSD.

VirtualBox is being actively developed with frequent releases and has an ever growing list of features, supported guest operating systems and platforms it runs on. VirtualBox is a community effort backed by a dedicated company: everyone is encouraged to contribute while Oracle ensures the product always meets professional quality criteria.

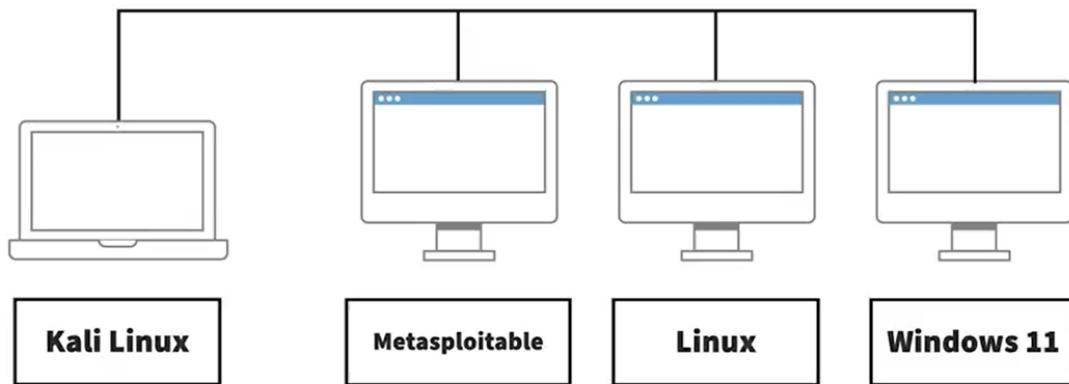
Download  
**VirtualBox 7.0**

**News Flash**

- **New October 17th, 2023**  
VirtualBox 7.0.12 released!  
Oracle today released a 7.0 maintenance release which improves stability and fixes regressions. See the Changelog for details.
- **New October 17th, 2023**  
VirtualBox 6.1.48 released!  
Oracle today released a 6.1 maintenance release which improves stability and fixes regressions. See the Changelog for details.
- **New July 18th, 2023**  
VirtualBox 7.0.10 released!  
Oracle today released a 7.0 maintenance release which improves stability and fixes regressions. See the Changelog for details.
- **New July 18th, 2023**  
VirtualBox 6.1.46 released!  
Oracle today released a 6.1

## Configuración de un laboratorio virtual

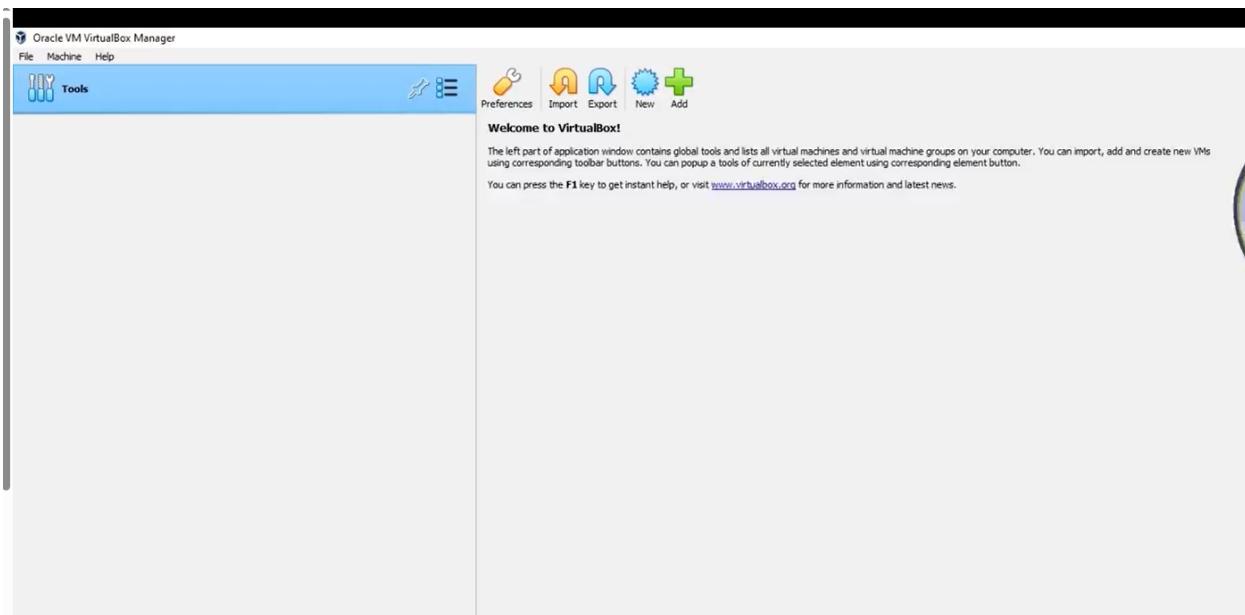
## Virtual Box



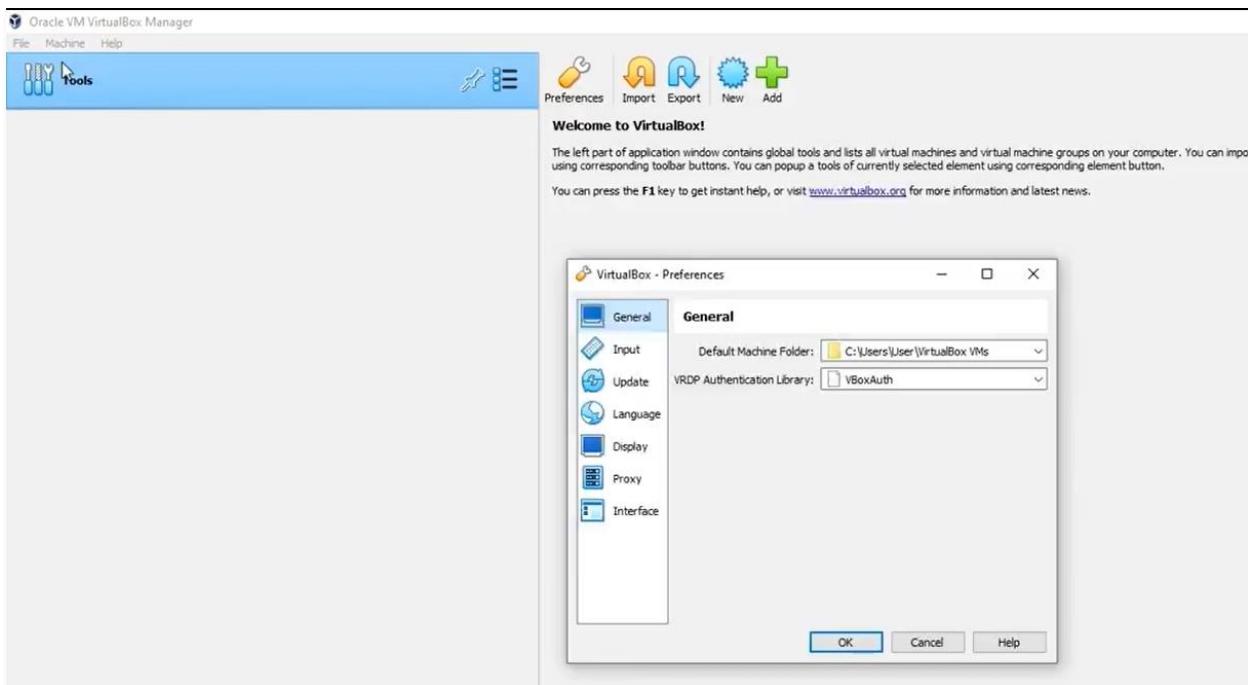
### Instalar VirtualBox y el paquete de extensiones

<https://www.virtualbox.org/wiki/Downloads>

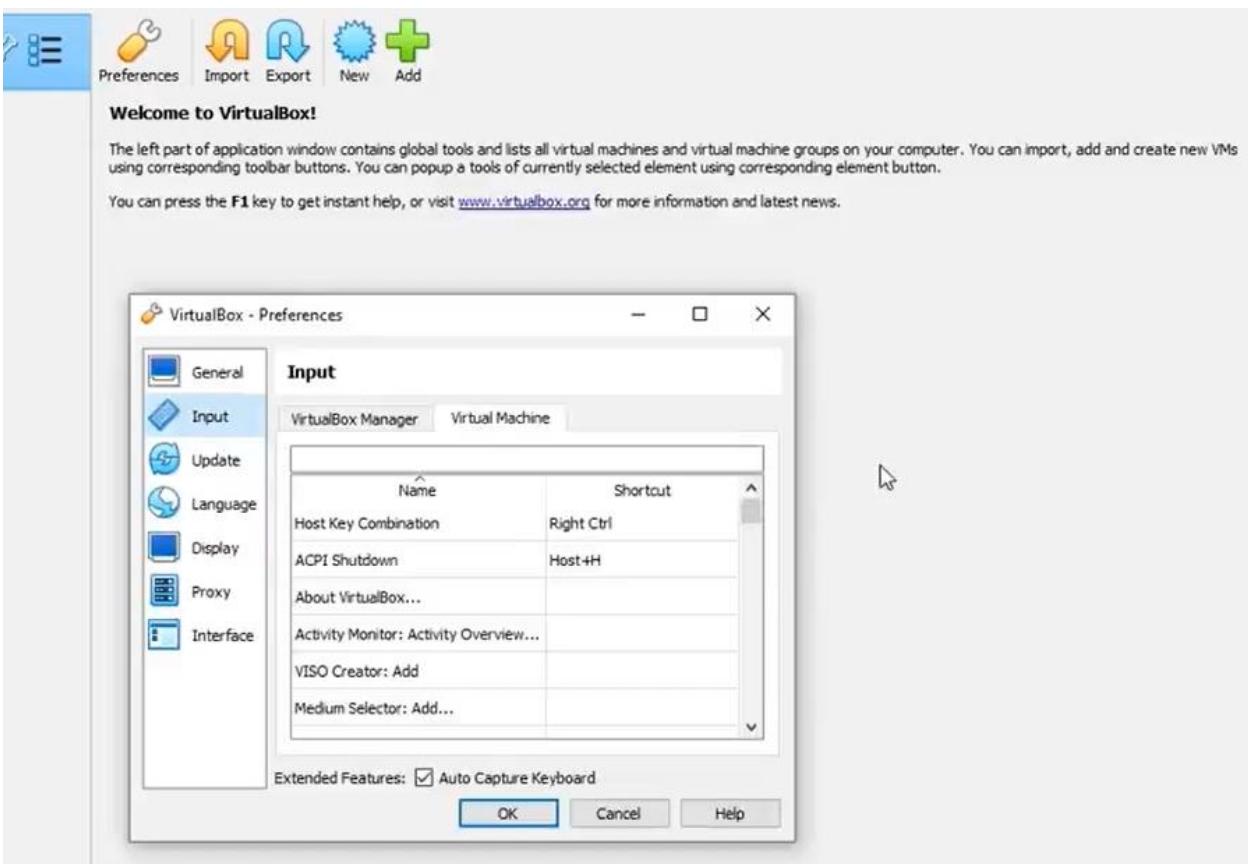
### Un primer vistazo a VirtualBox

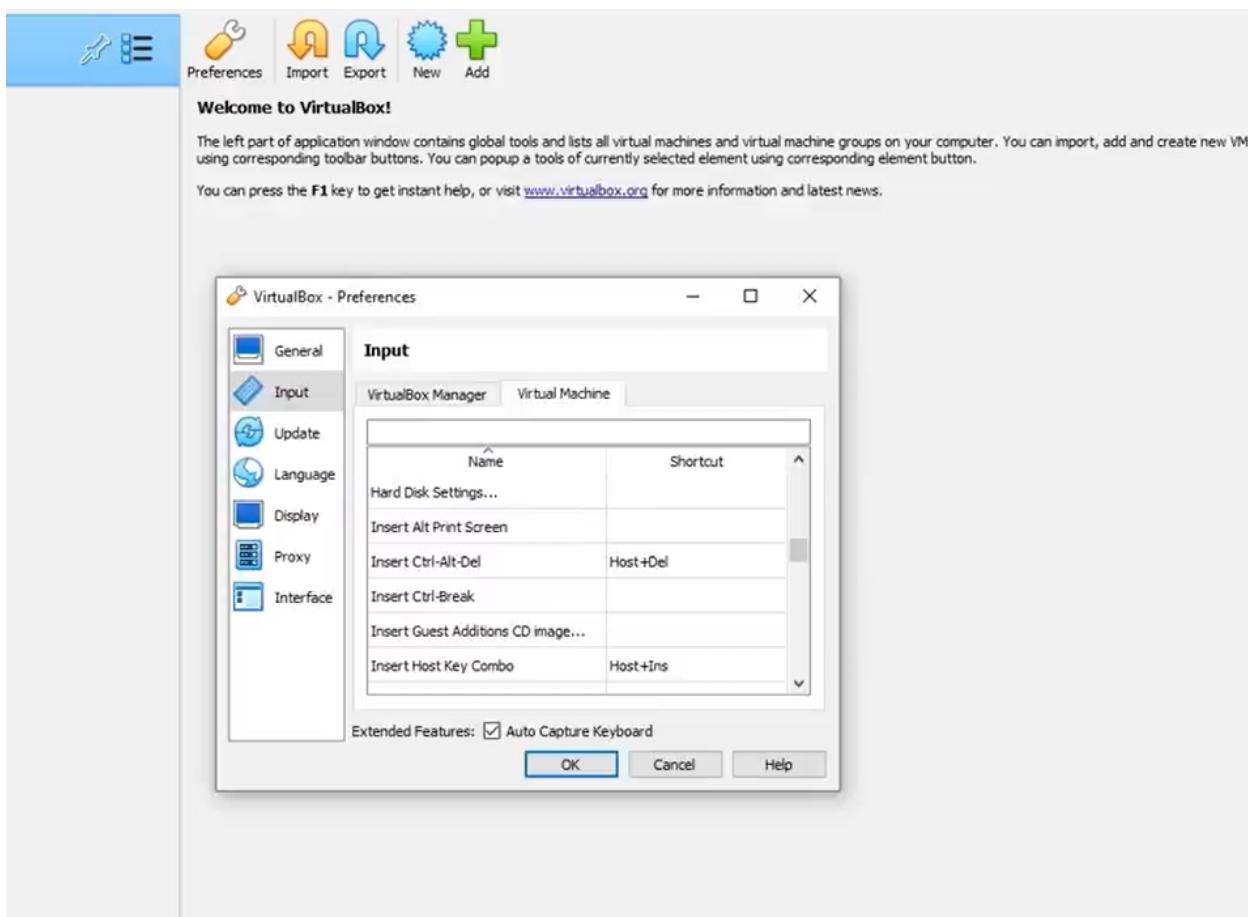


### El archivo | Preferencias

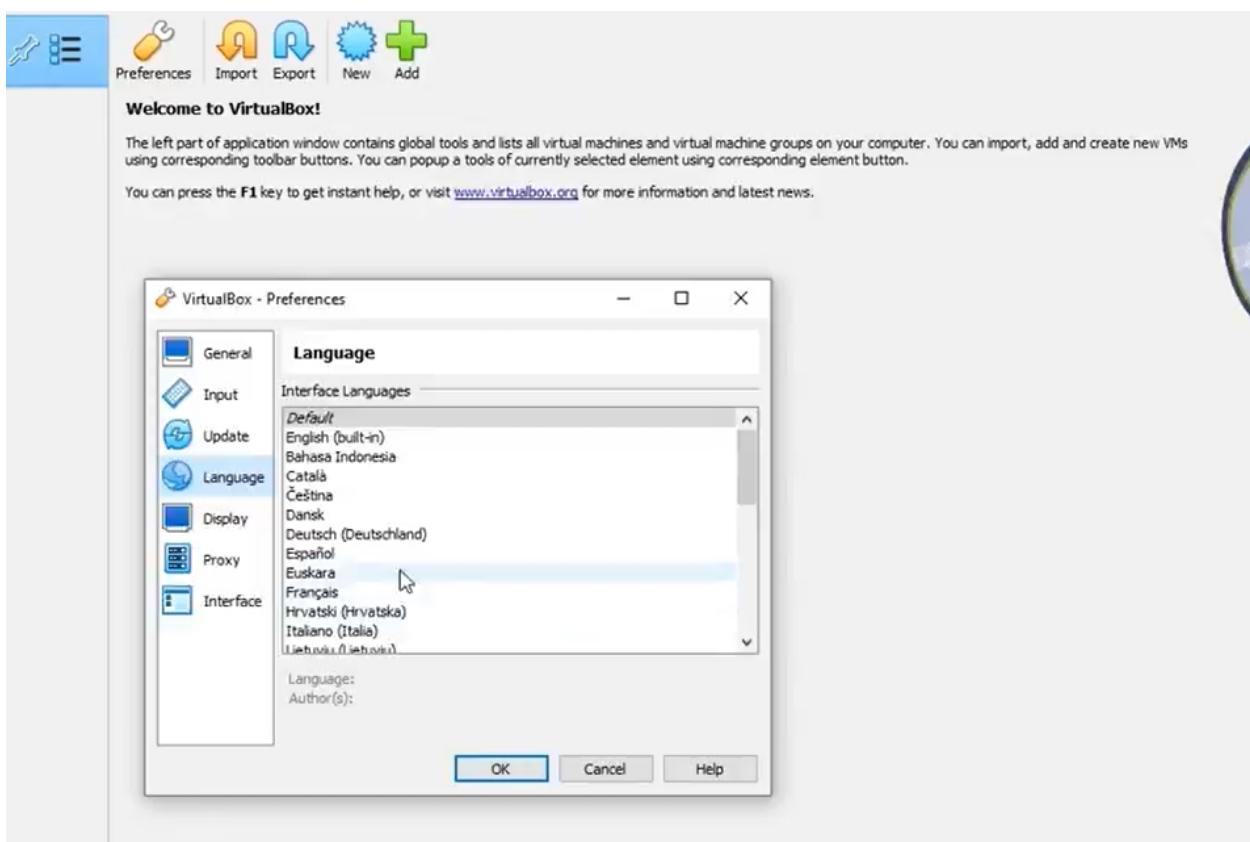
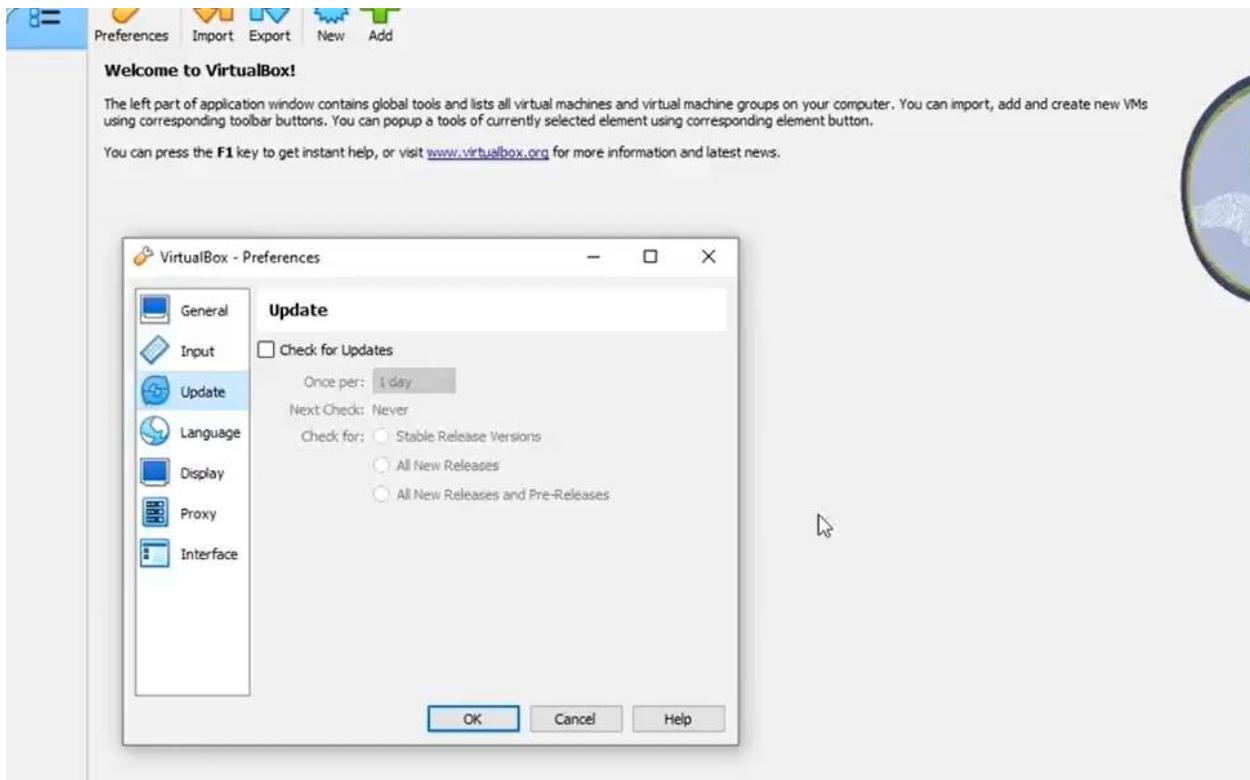


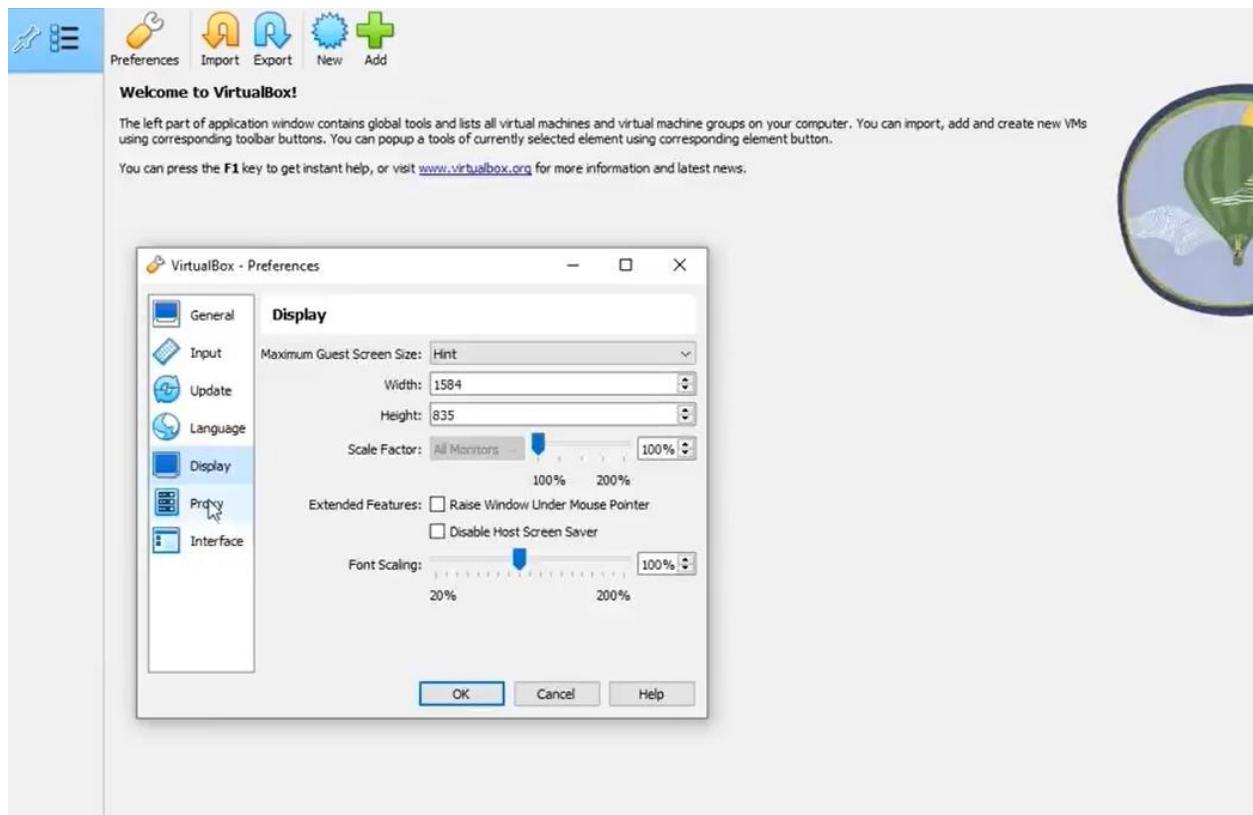
## Entrada

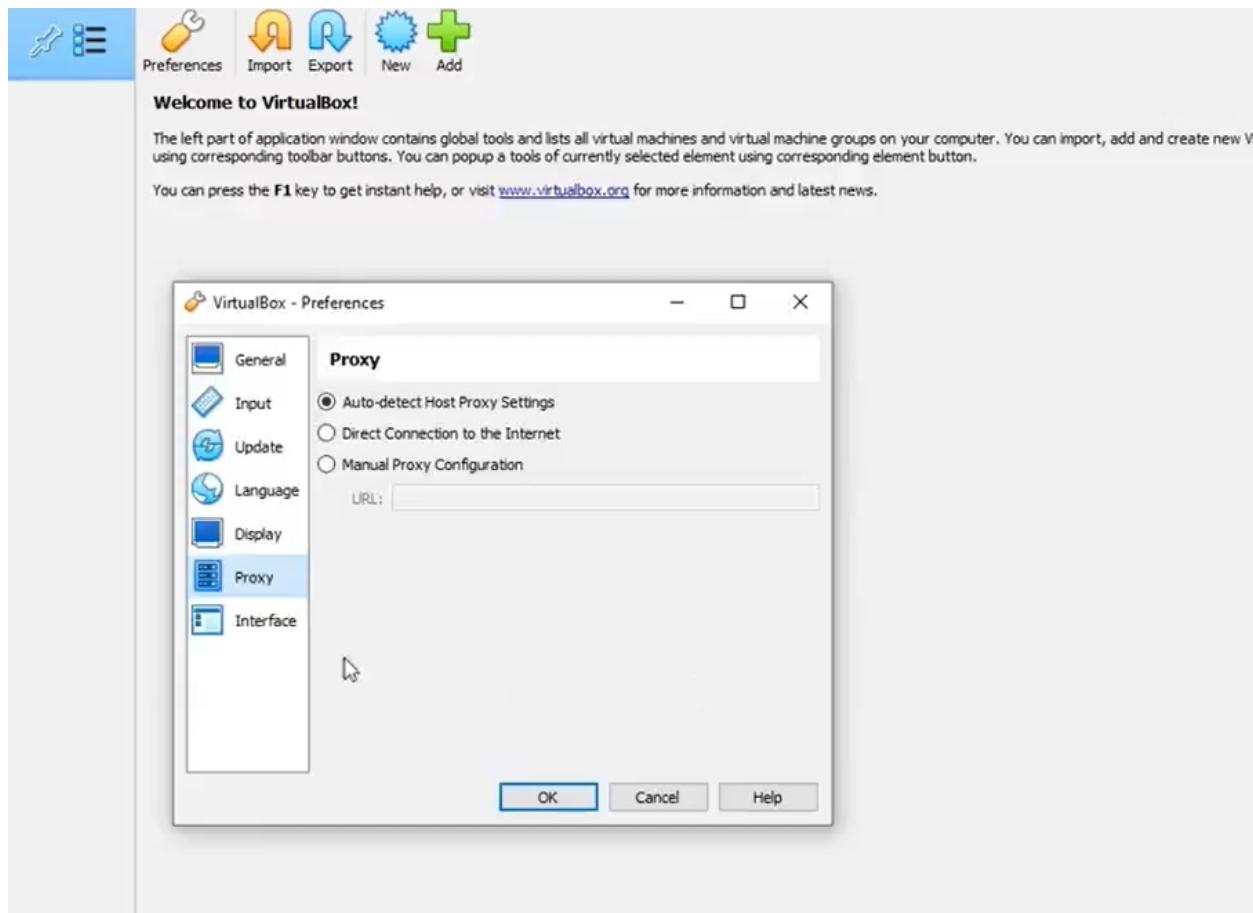


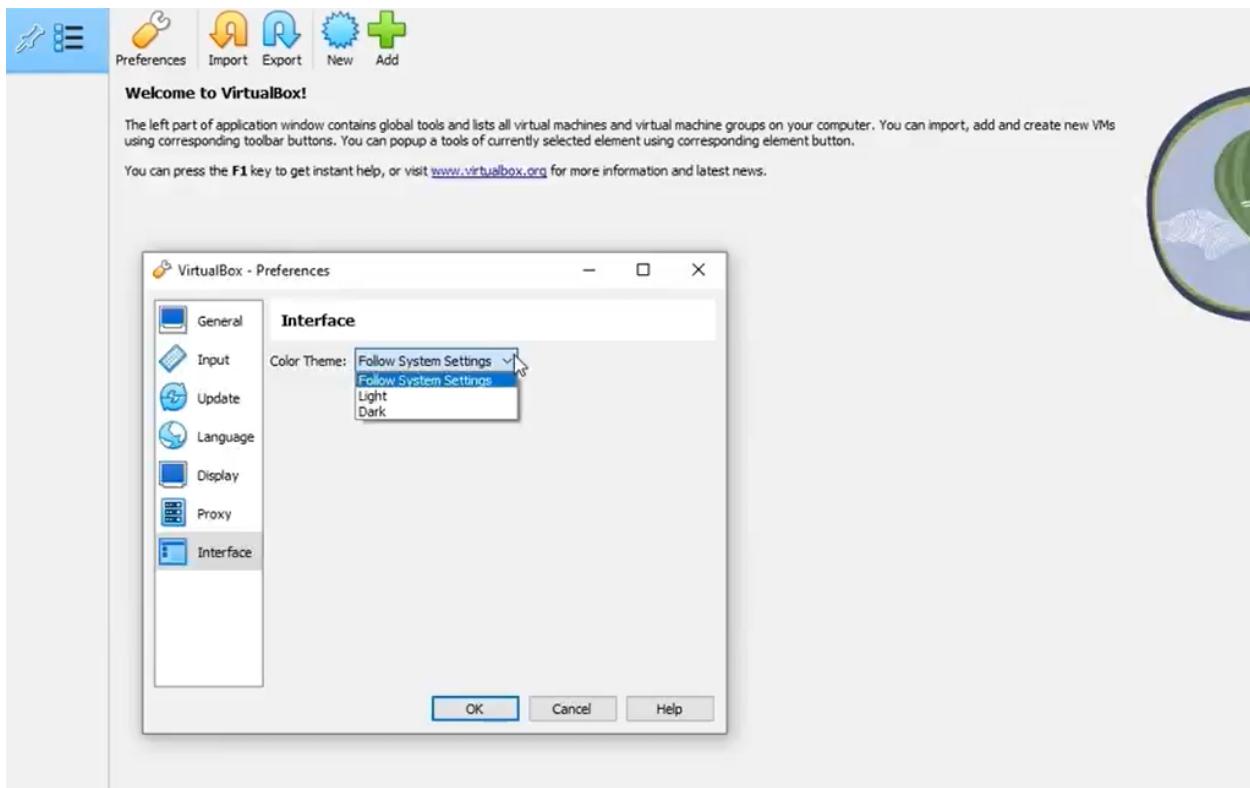


## Actualizar

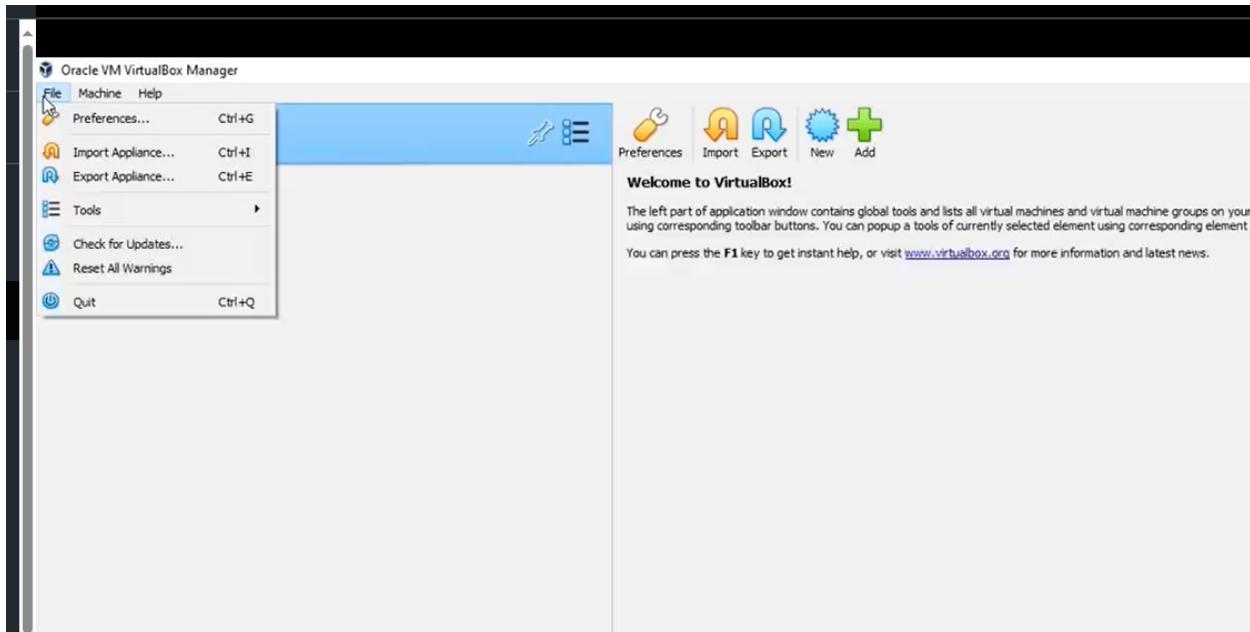




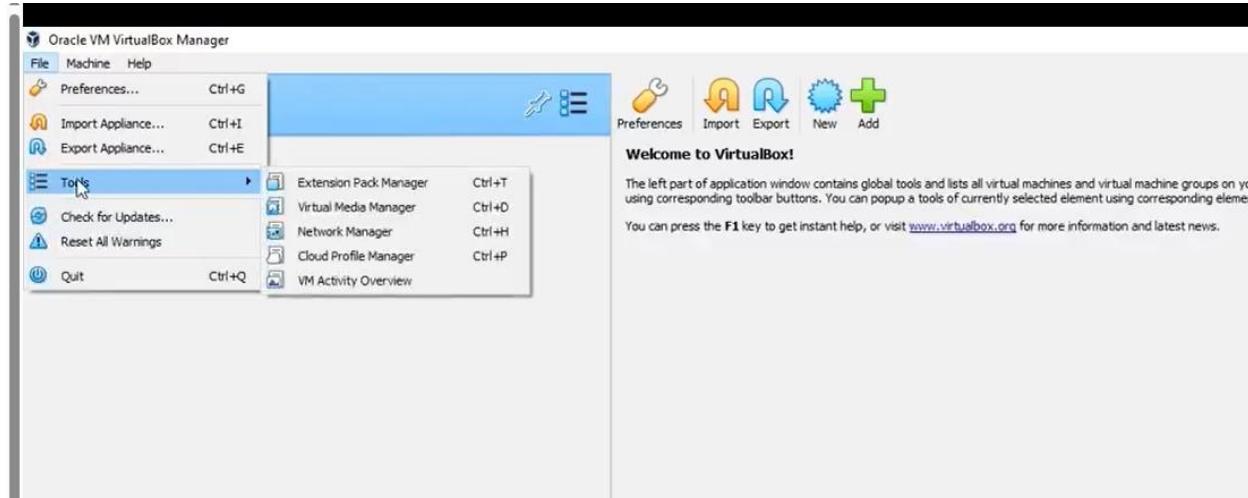




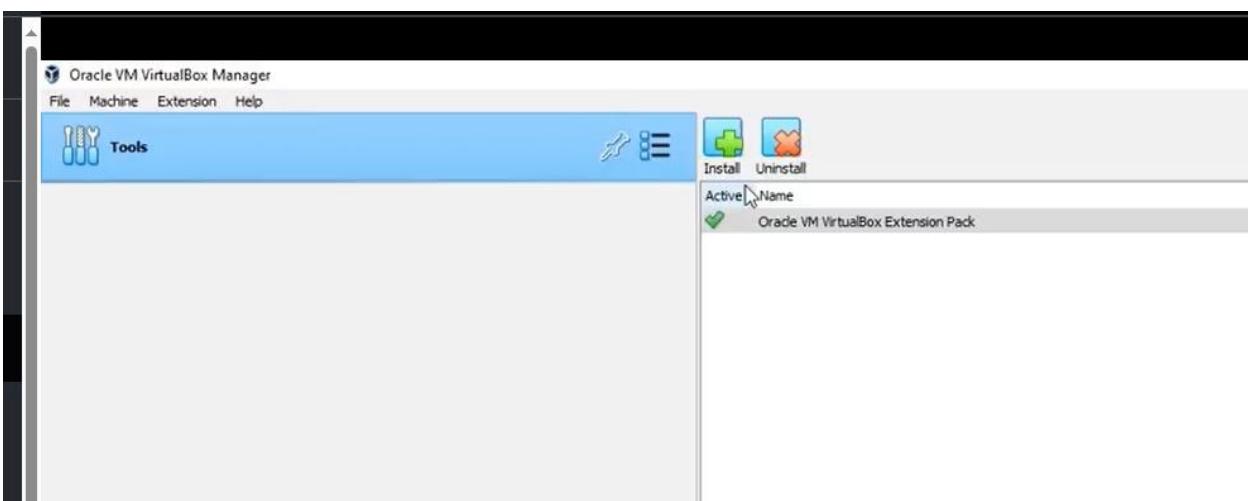
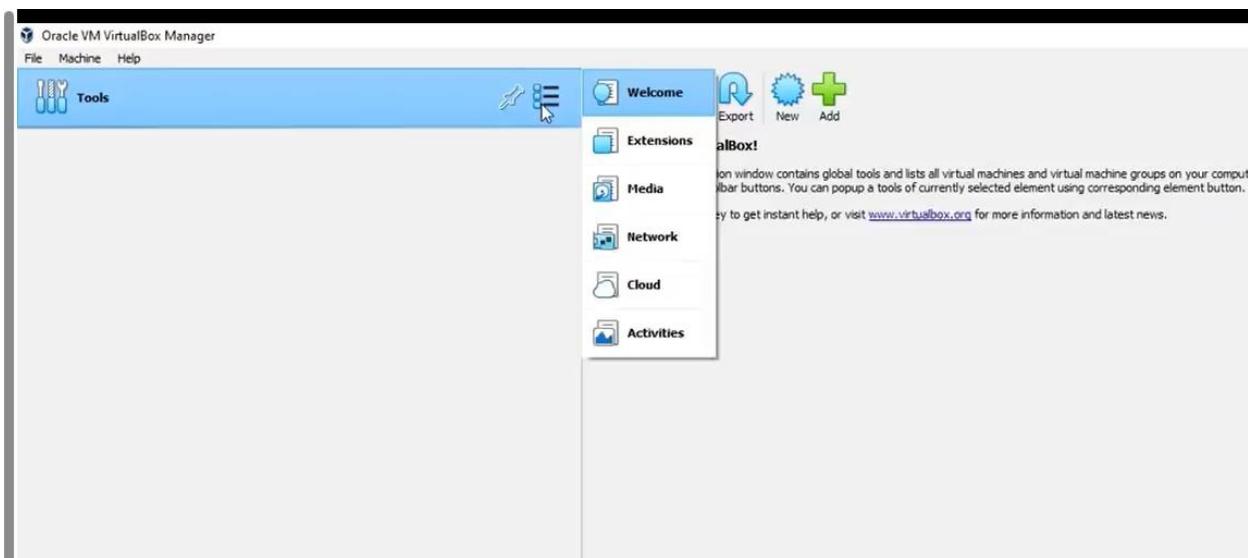
## Archivo | Importar dispositivo



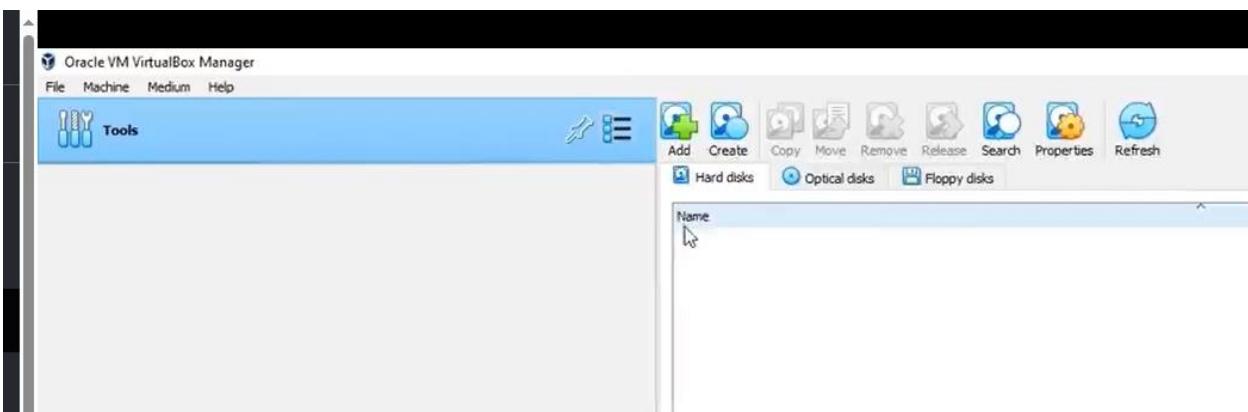
## Archivo | Herramientas



## El menú de opciones

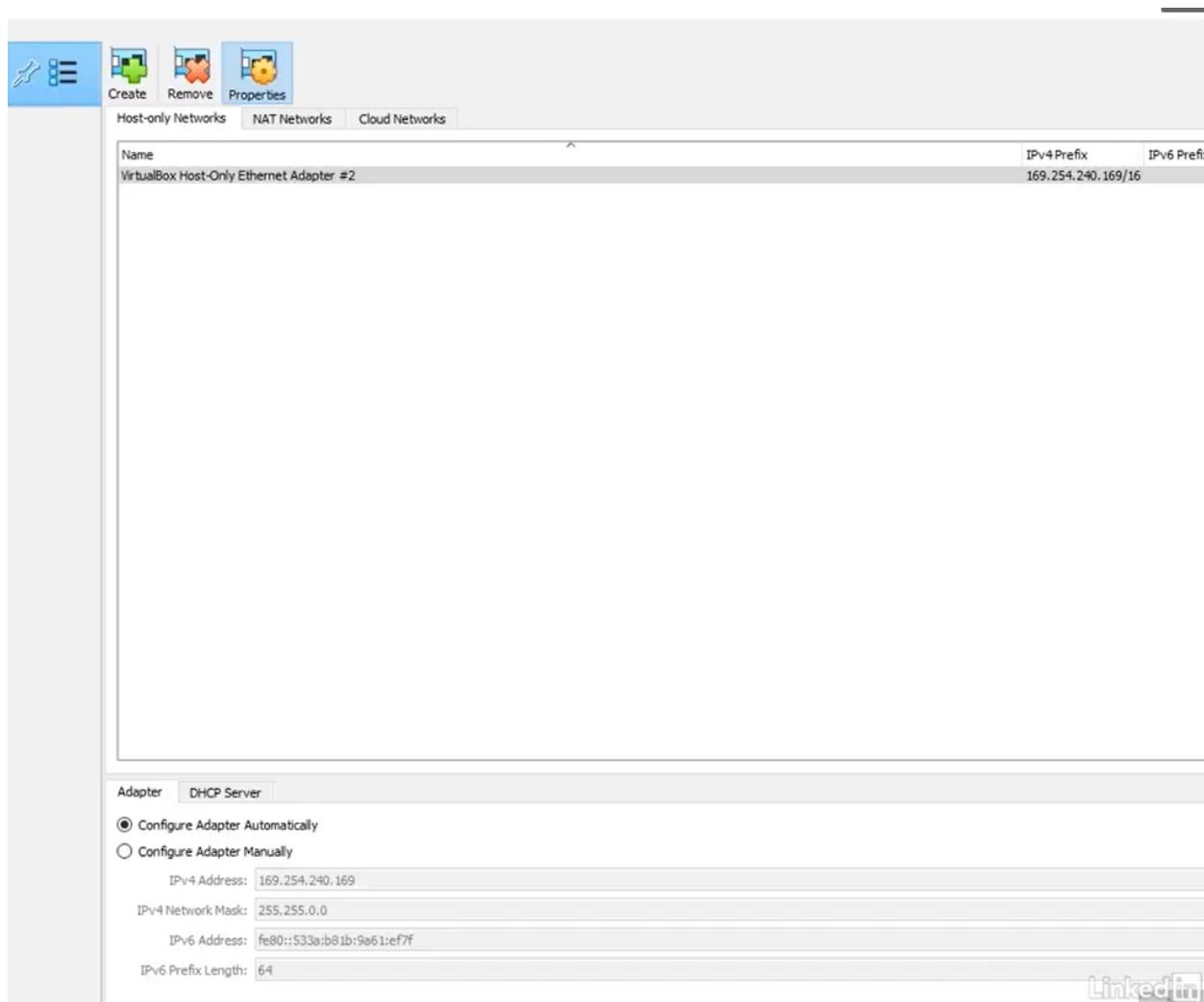


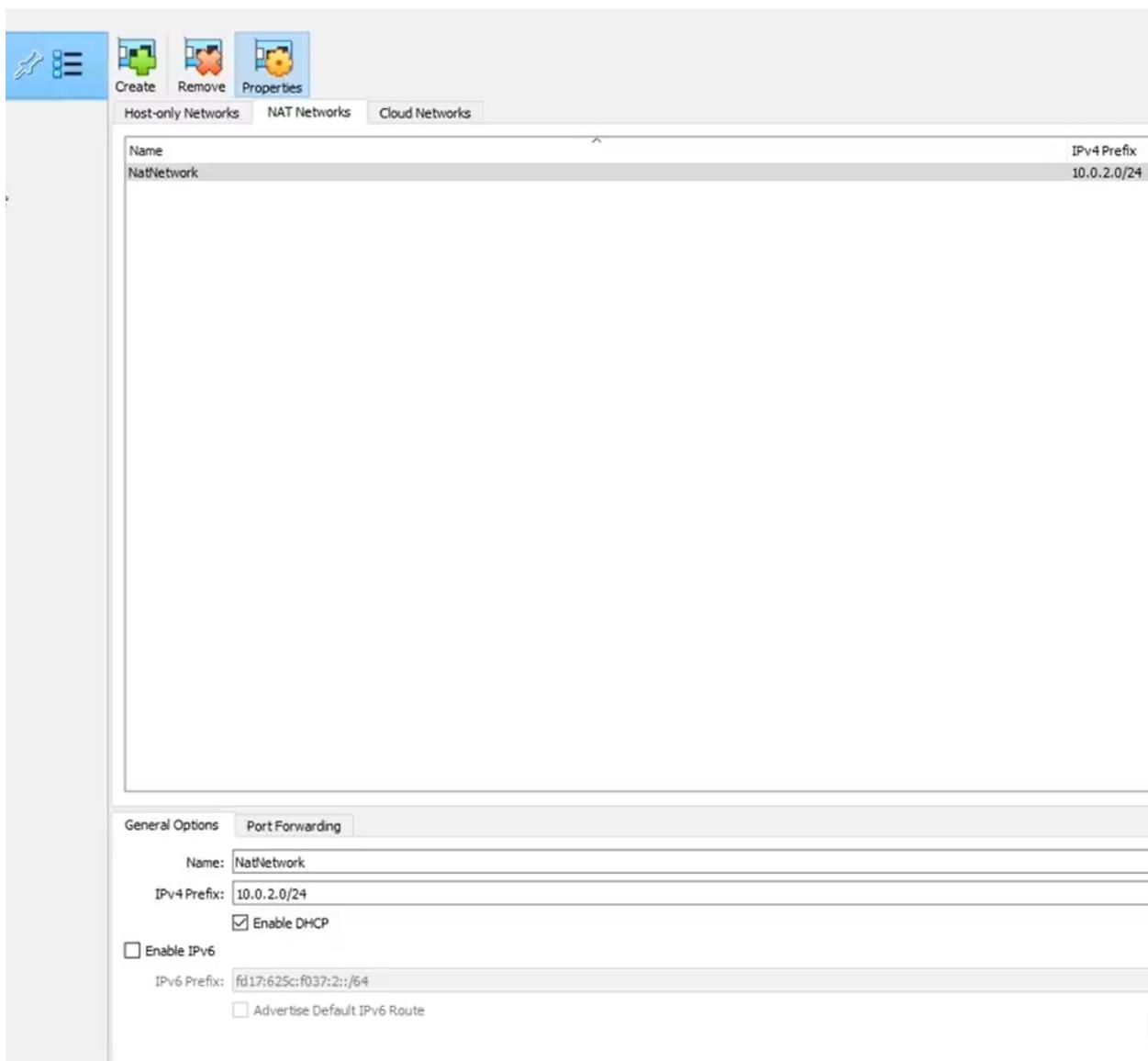
## El submenú Medios

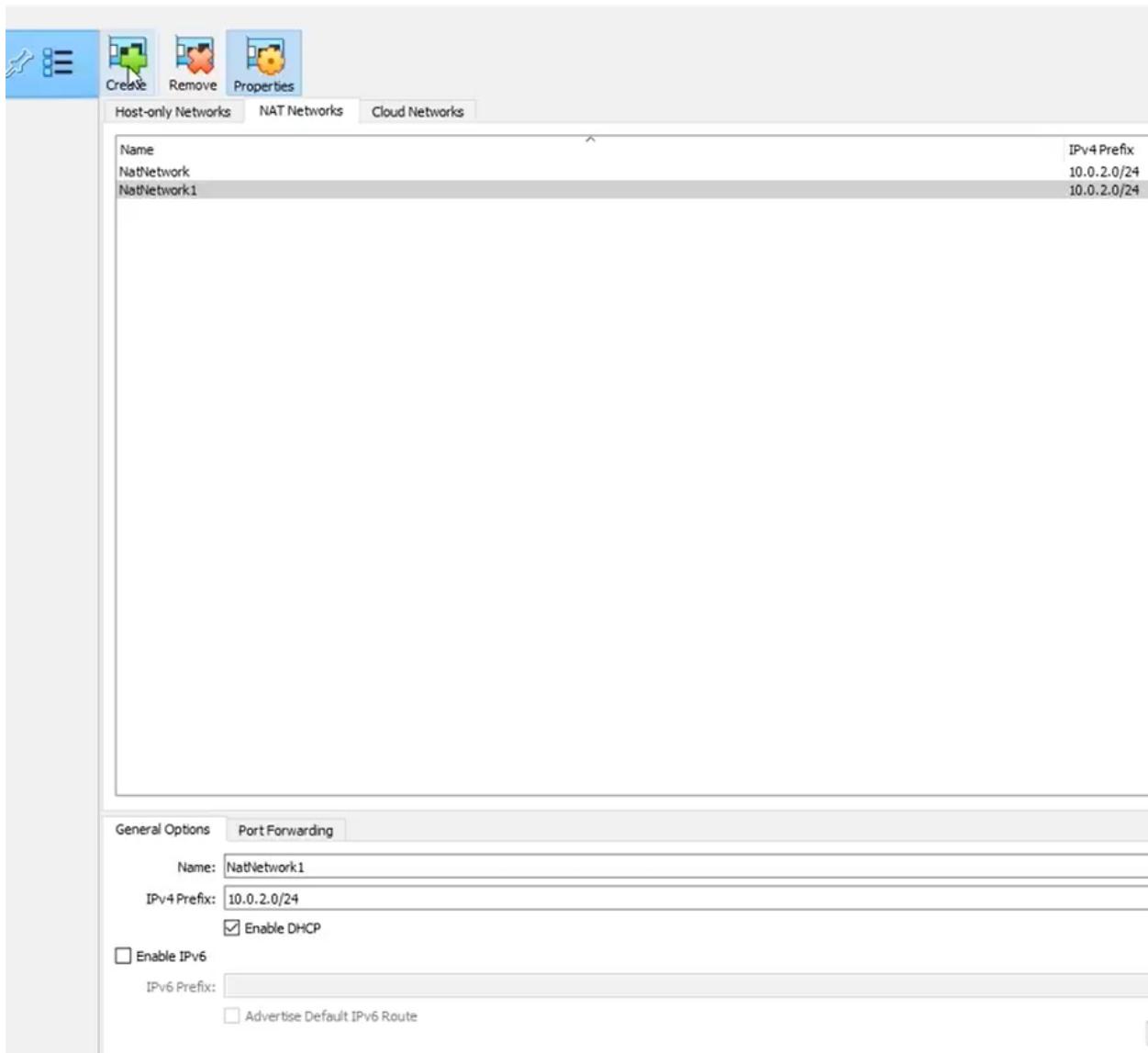


## Red

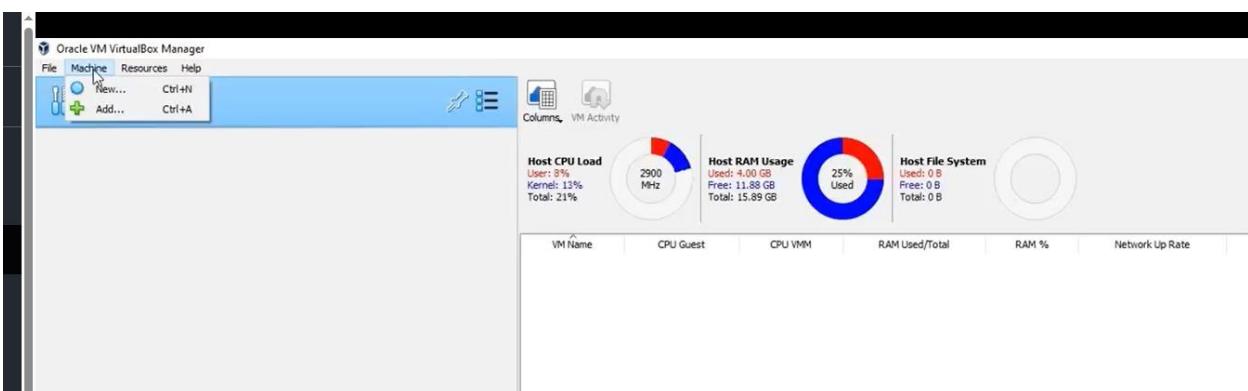
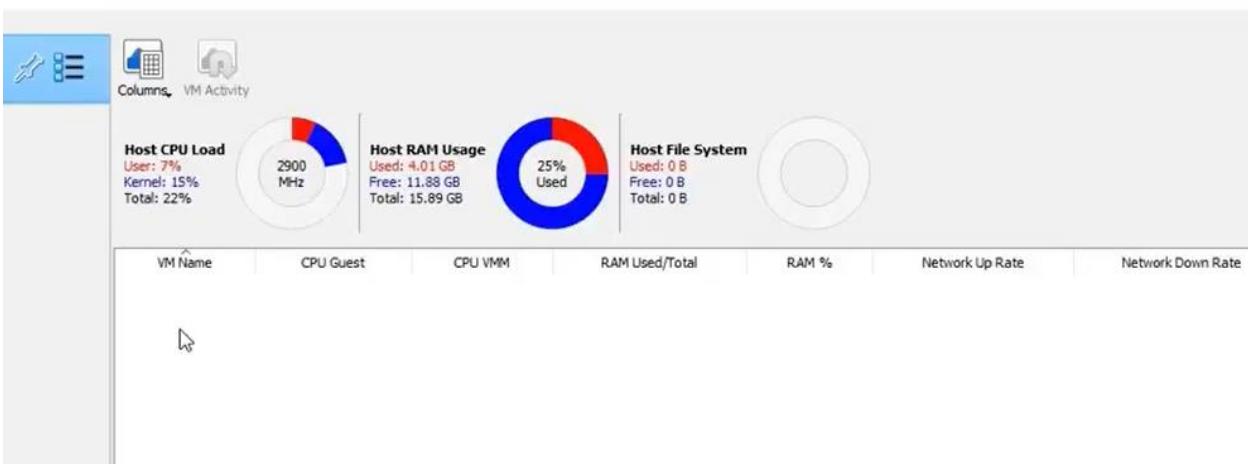
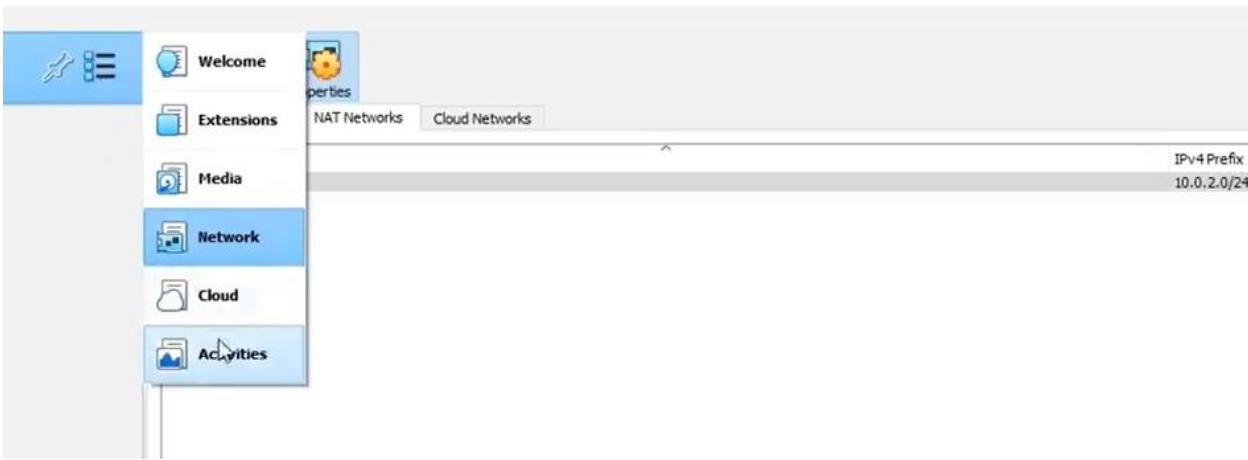
1. Red de solo host
2. Redes NAT
3. Redes en la nube







## Actividades



## Instalación de Kali como Virtual Appliance

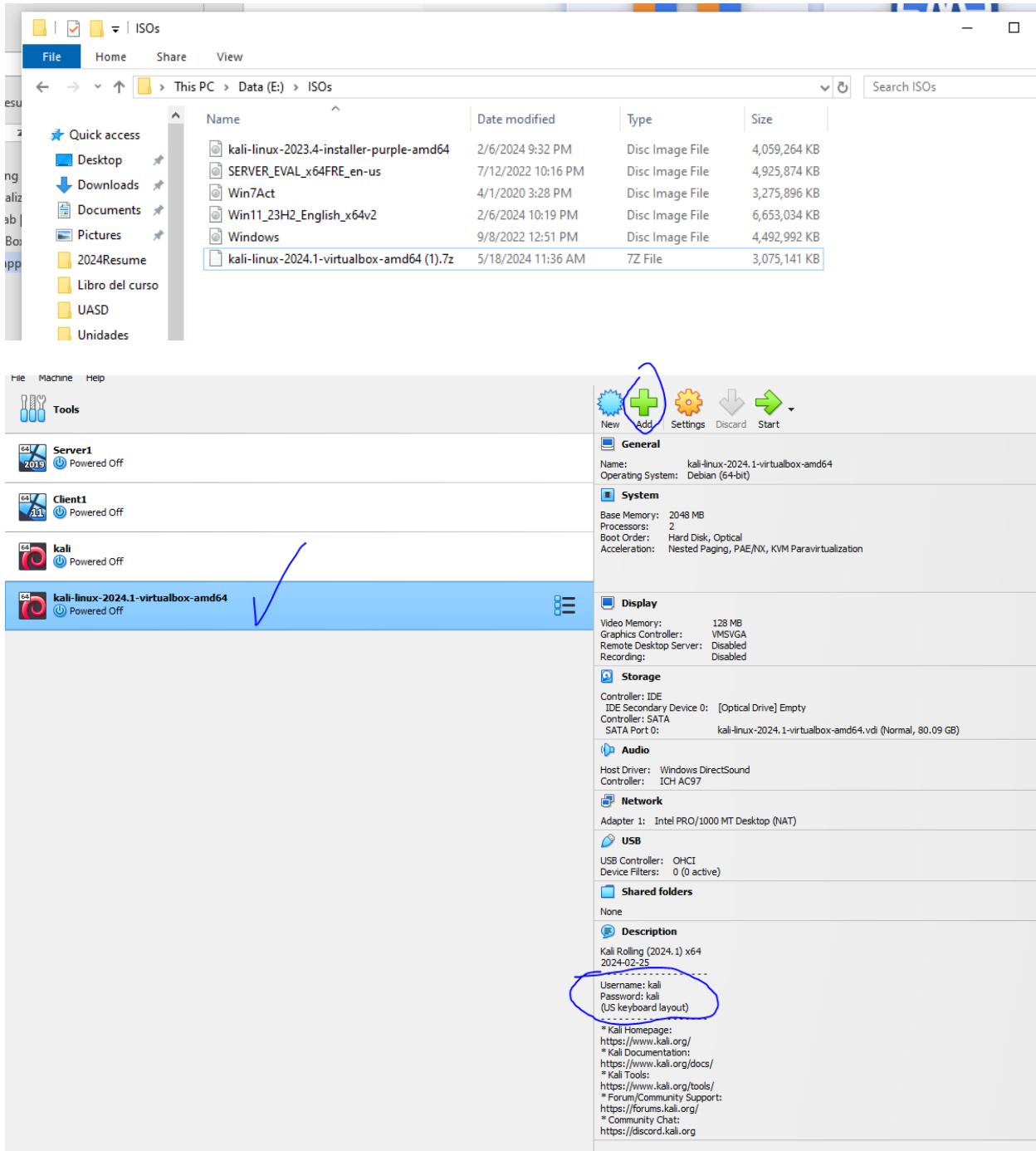
<https://www.kali.org/>



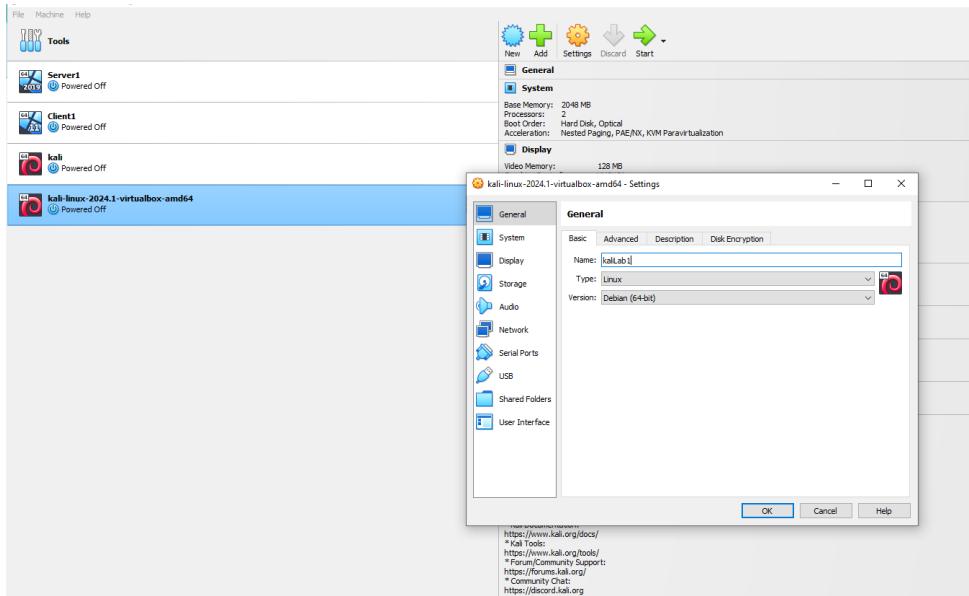
<https://www.kali.org/get-kali/#kali-virtual-machines>

This screenshot shows the 'Pre-built Virtual Machines' section of the Kali Linux website. The URL in the address bar is 'kali.org/get-kali/#kali-virtual-machines'. The page has a navigation bar with links for 'Personal stuff', 'YouTube', 'Cars', 'ChatGPT', 'M365', 'Bard', 'NSCC', 'Learning', 'SeoChannel', 'Cybersecurity Hoy', 'LinkedIn', 'MISC', and 'WhatsApp'. Below the navigation is a horizontal menu with tabs: 'Installer' (selected), 'Pre-built VMs' (underlined), 'ARM', 'Mobile', 'Cloud', 'Containers', 'Live', and 'WSL'. The main content area features a green cube icon and the heading 'Pre-built Virtual Machines'. It states that VMware &amp; VirtualBox images are available for users who prefer or whose specific needs require a virtual machine installation. It notes that these images have default credentials 'kali/kali'. A link to 'Virtual Machines Documentation' is provided. There are four download options for 64-bit systems: 'VMware' (Recommended, orange square icon), 'VirtualBox' (Recommended, blue circle icon), 'Hyper-V' (Recommended, Windows logo icon), and 'QEMU' (Recommended, orange bird logo icon). Each option includes download links for 'torrent', 'docs', and 'sum'.

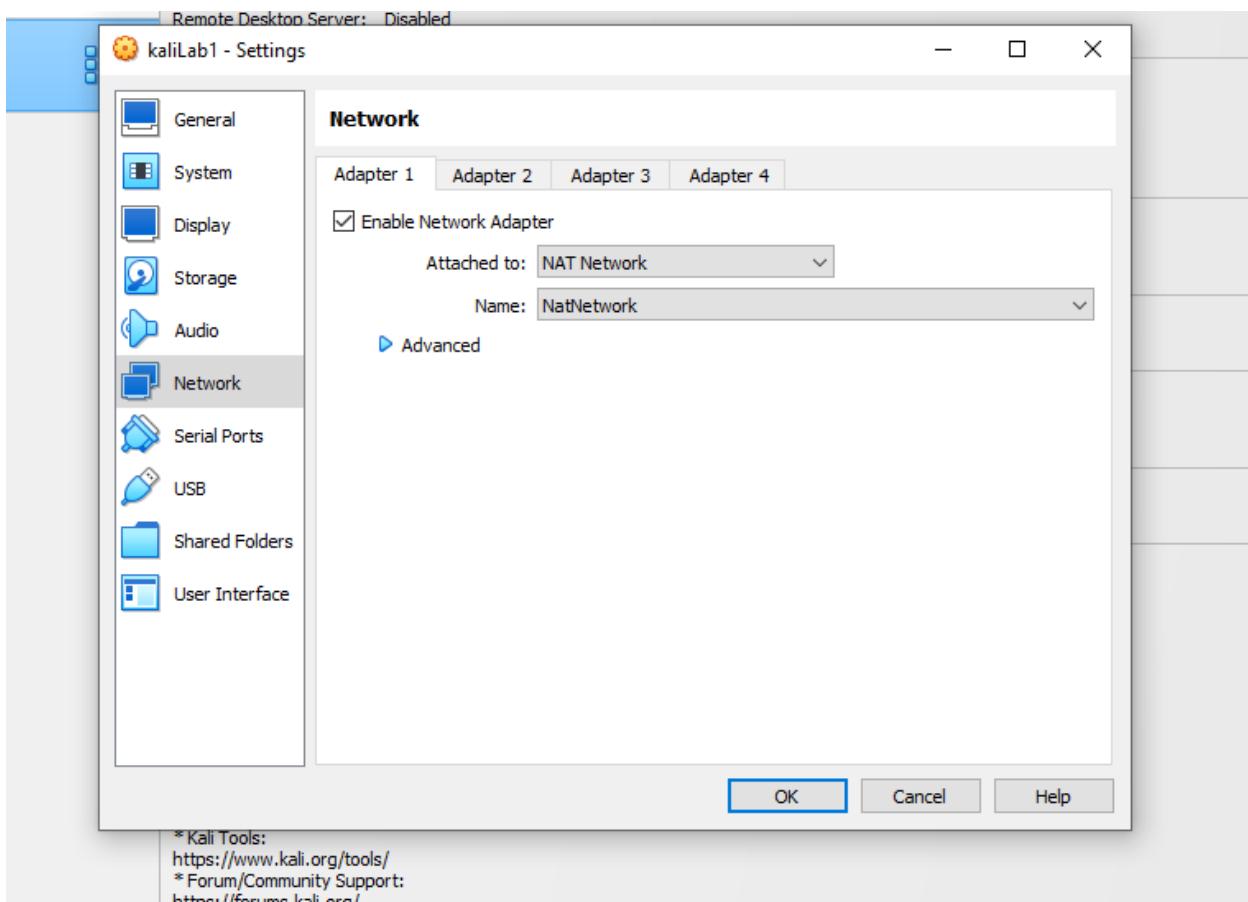
## Descargar e importar la máquina virtual

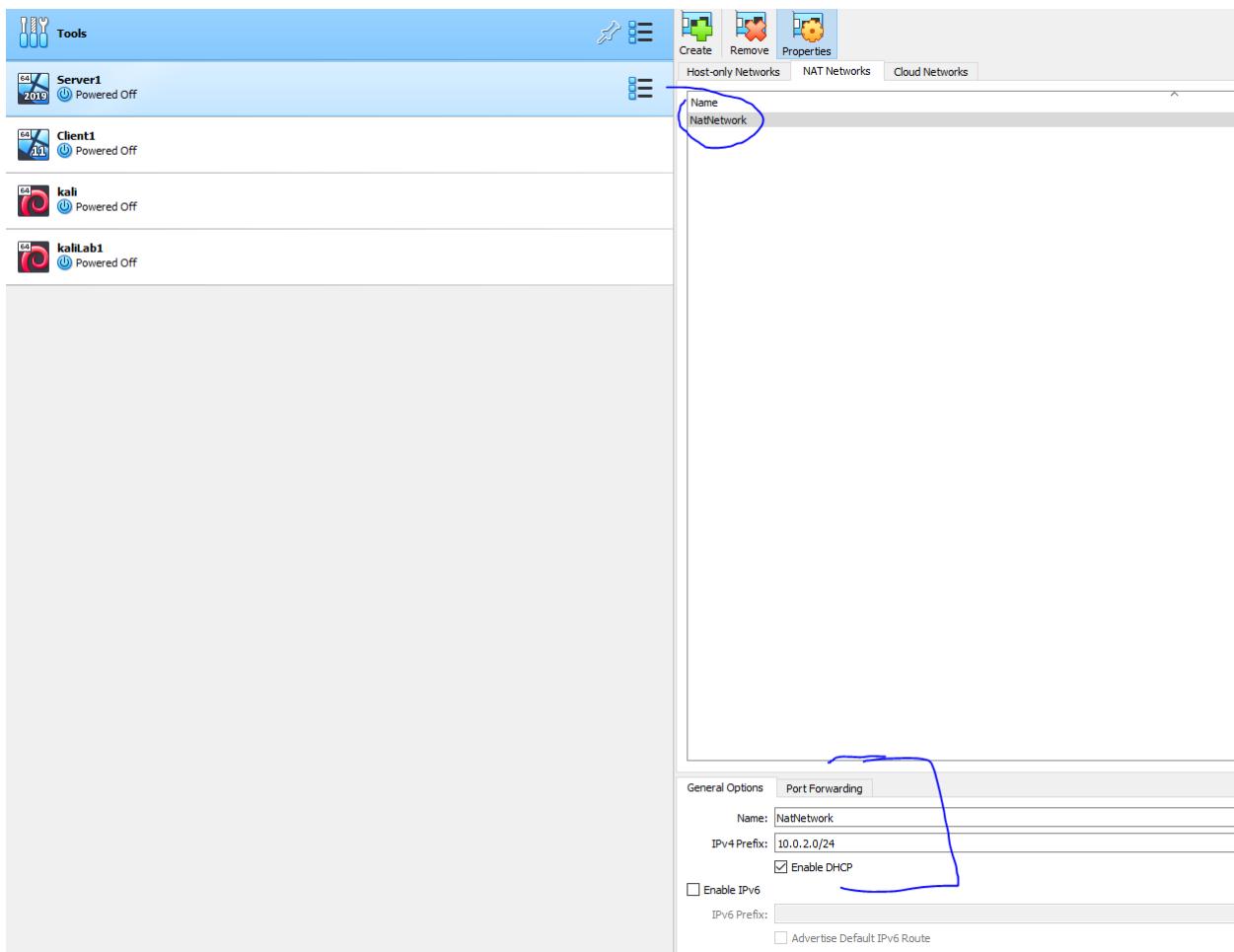


## Cambiar el nombre de la máquina virtual

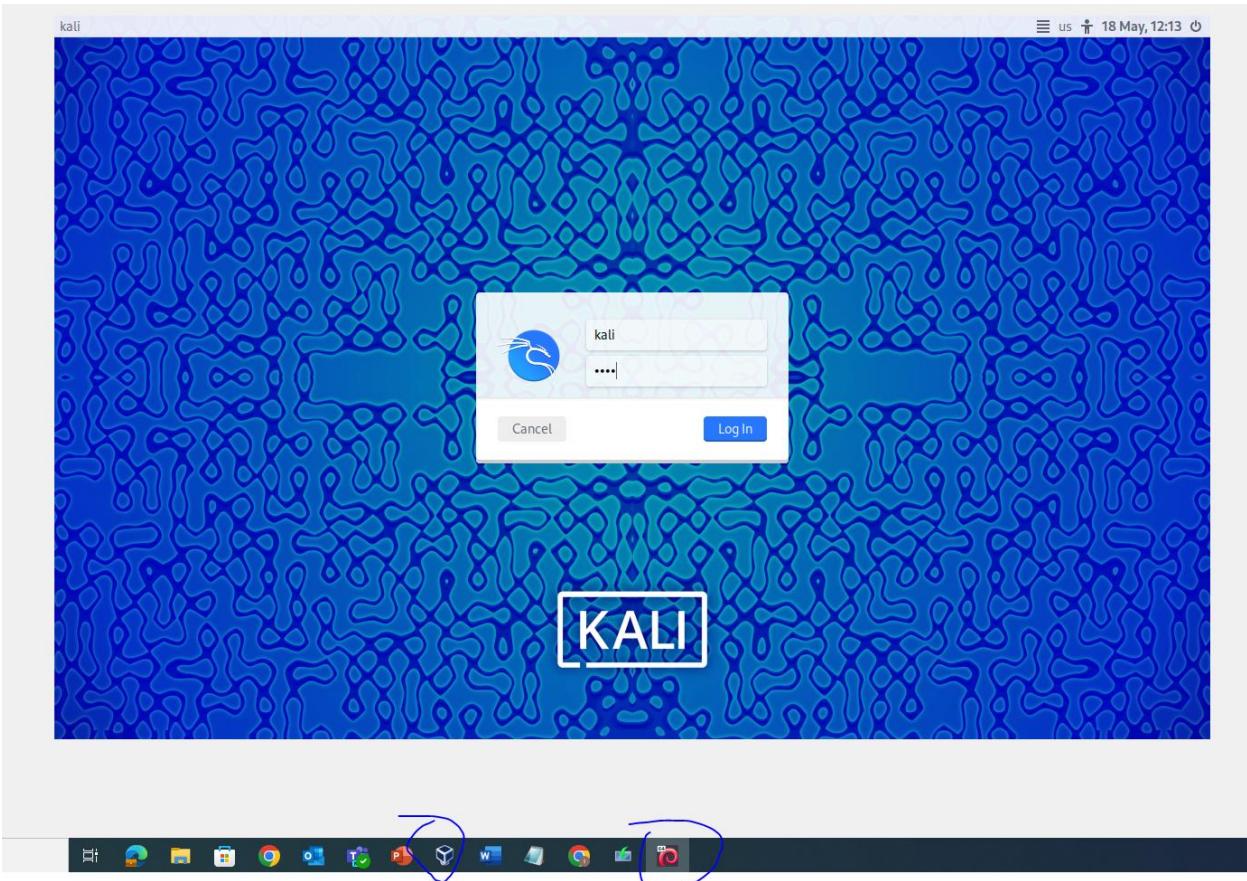


## Cámbialo a Nat Network

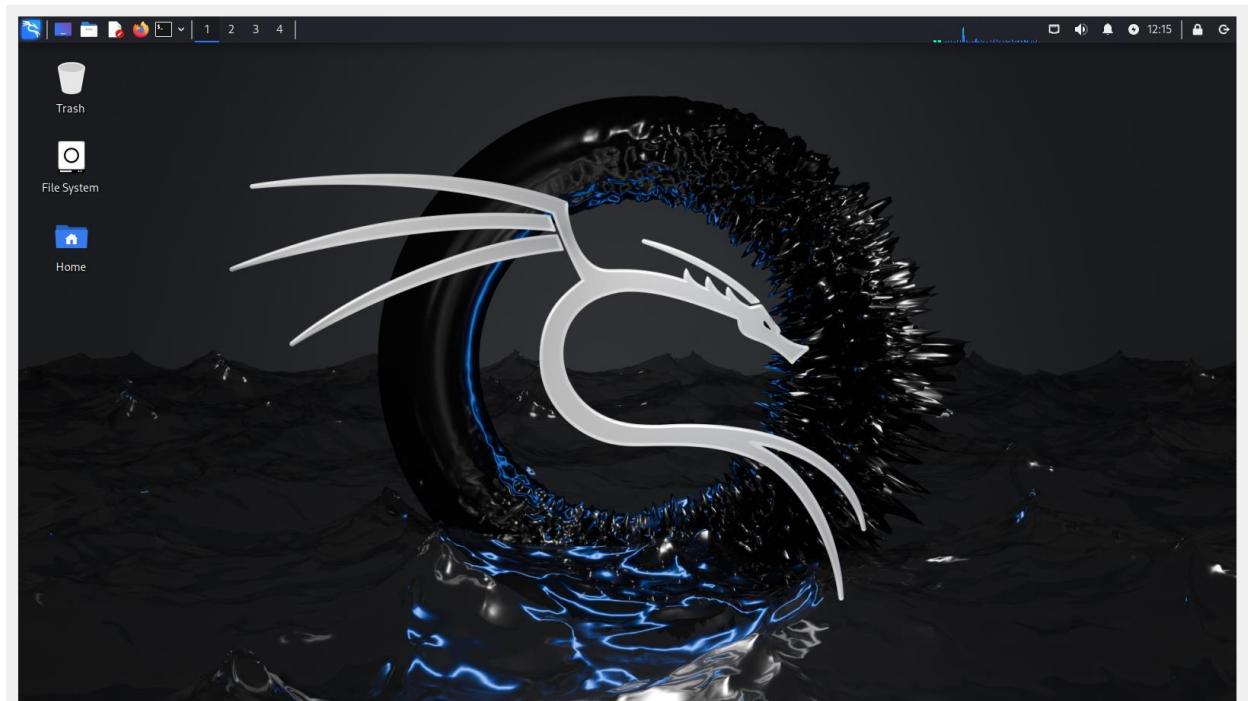
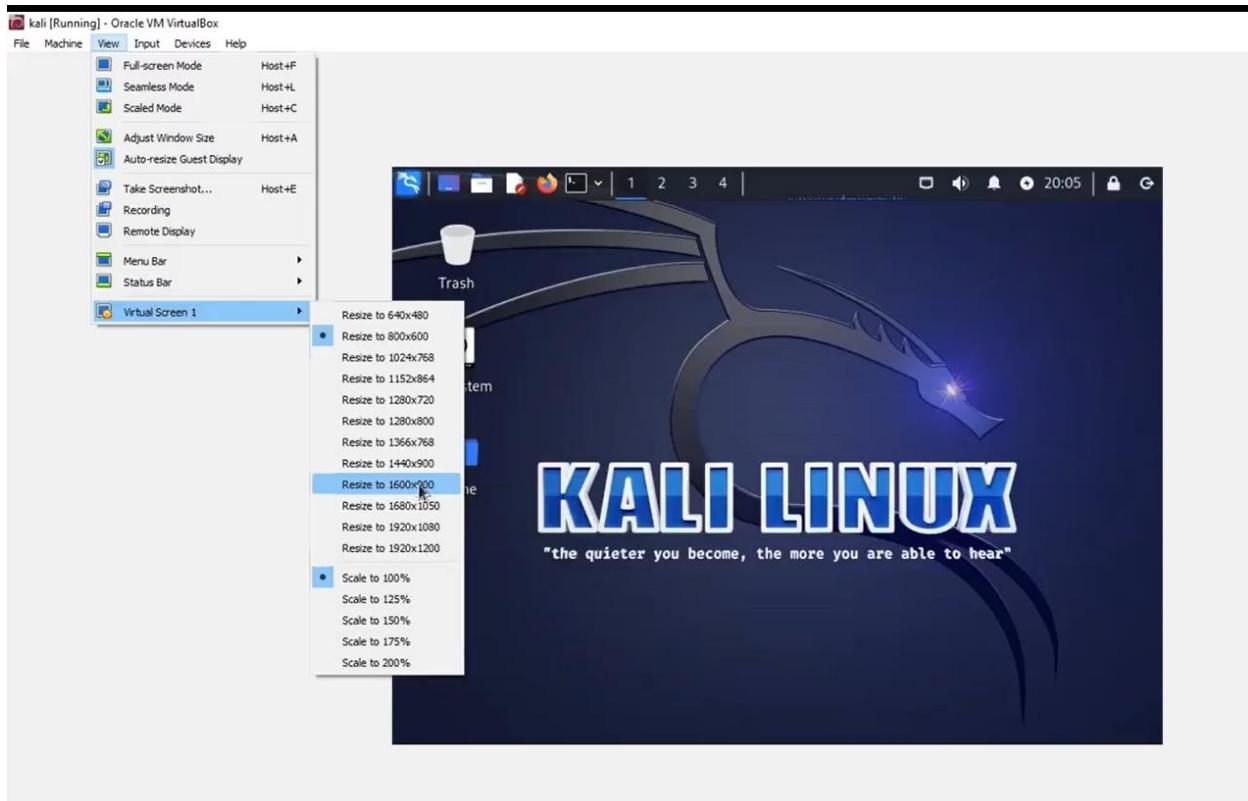




## Inicio de la máquina virtual



Cambiar la resolución



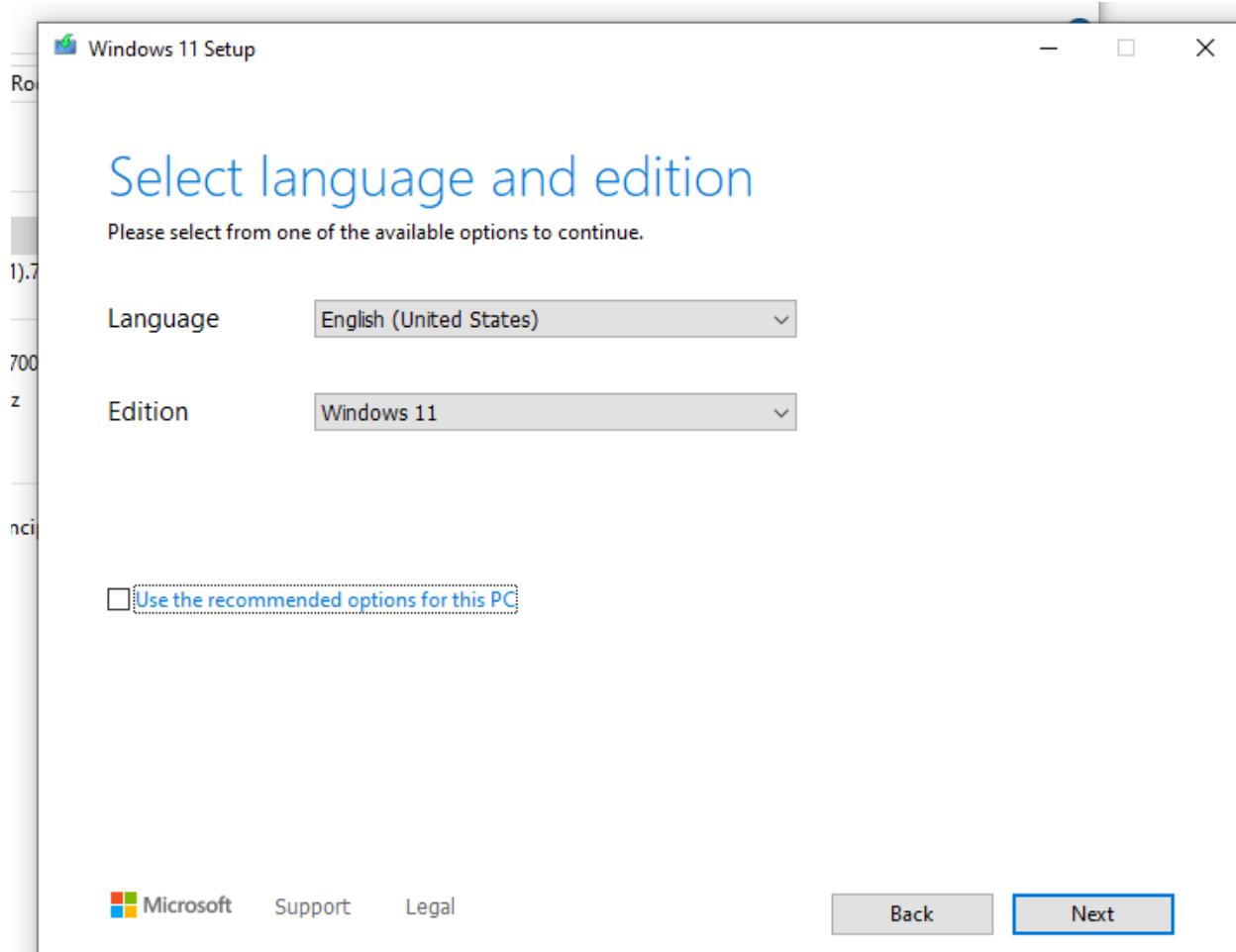
# Instalación de Windows 11

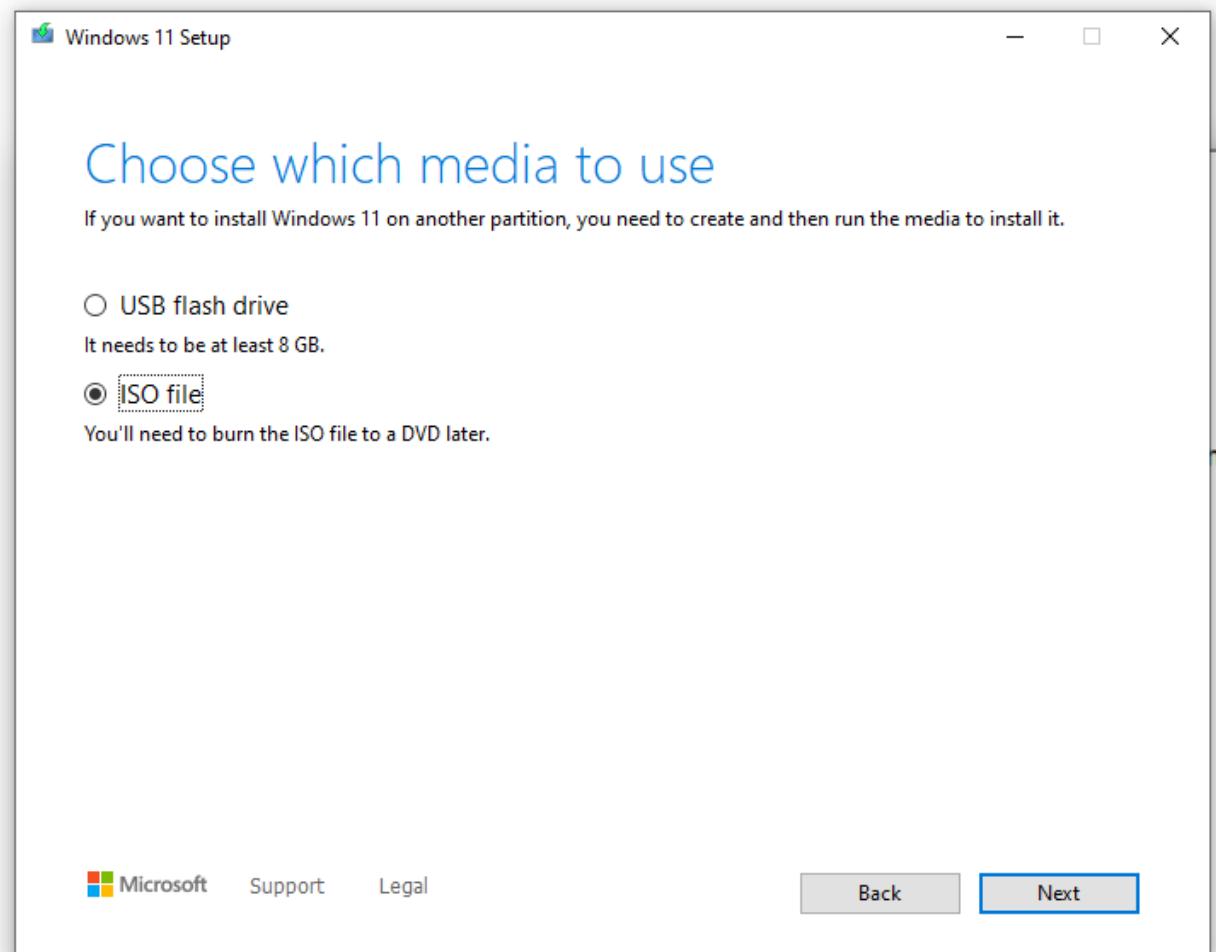
<https://www.microsoft.com/software-download/windows11>

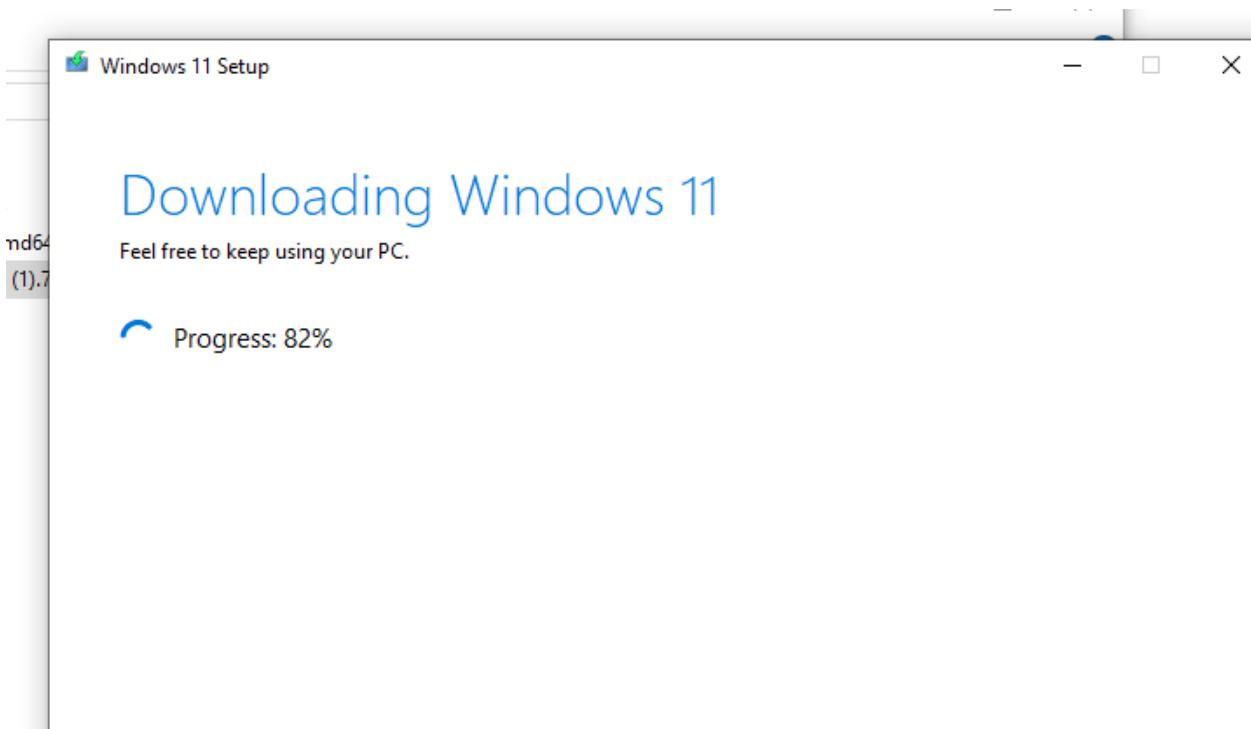
The screenshot shows the Microsoft software download page for Windows 11. It features three main sections:

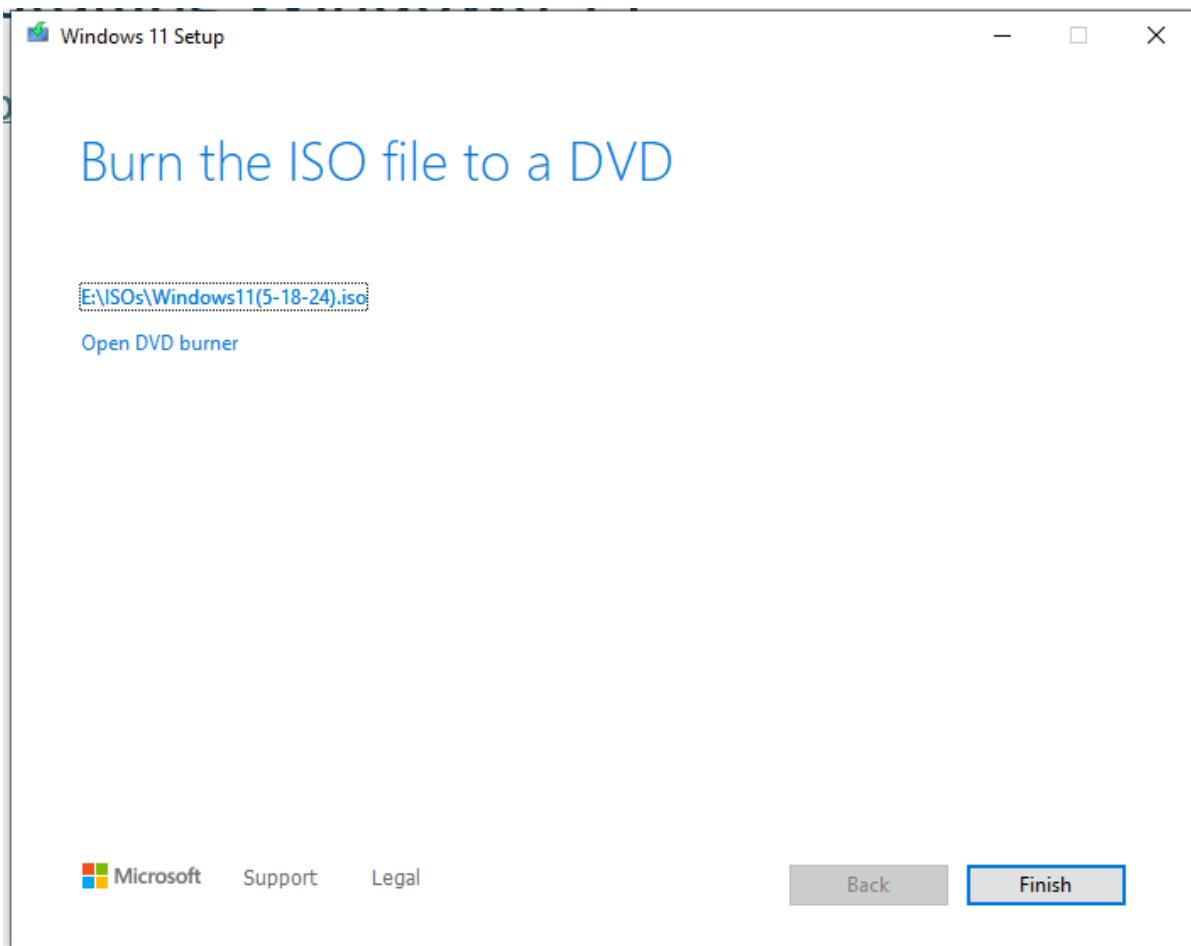
- Windows 11 Installation Assistant**: This section is described as the best option for installing Windows 11 on the current device. It includes a "Before you begin using Installation Assistant" note, a "Download Now" button, and a thumbnail image of a laptop screen displaying a blue rose.
- Create Windows 11 Installation Media**: This section is for performing a reinstall or clean install. It includes a "Before you begin using the media creation tool" note, a "Download Now" button, and a thumbnail image of a laptop screen displaying a blue rose.
- Download Windows 11 Disk Image (ISO) for x64 devices**: This section is for creating bootable media like USB drives or virtual machines. It includes a dropdown menu labeled "Select Download", a "Before you begin downloading an ISO" note, and a "Download Now" button.

## Crear medios de instalación de Windows 11

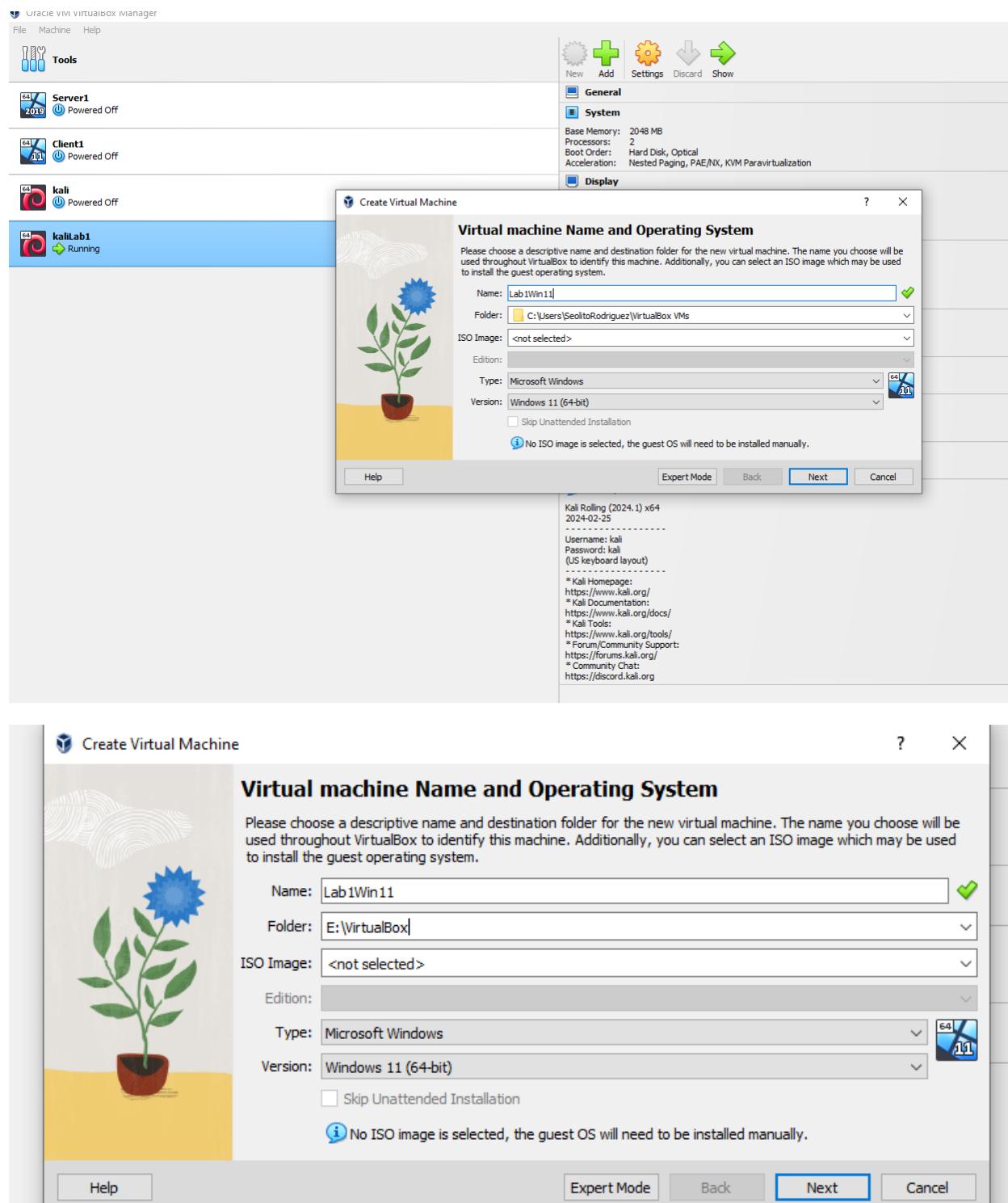


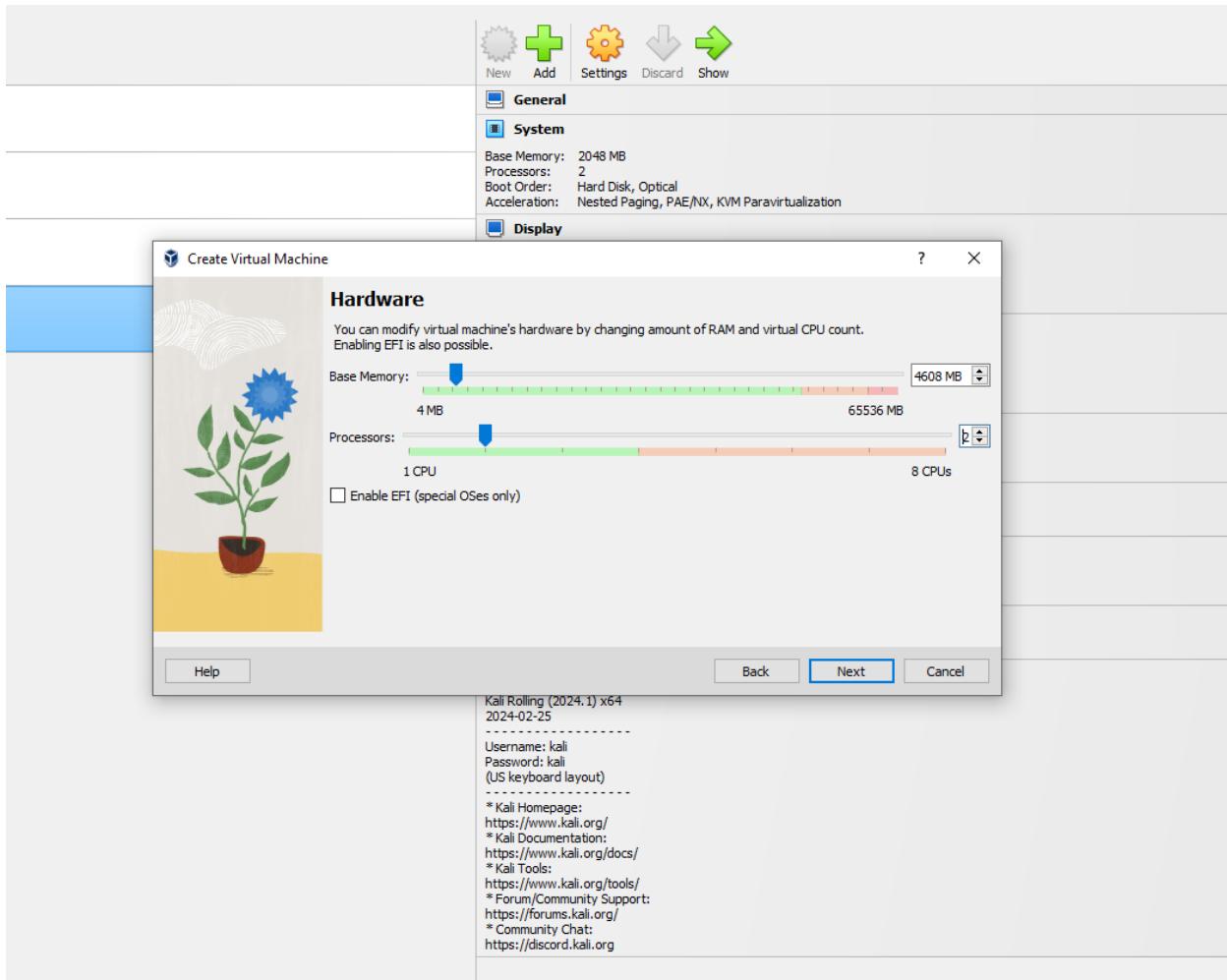


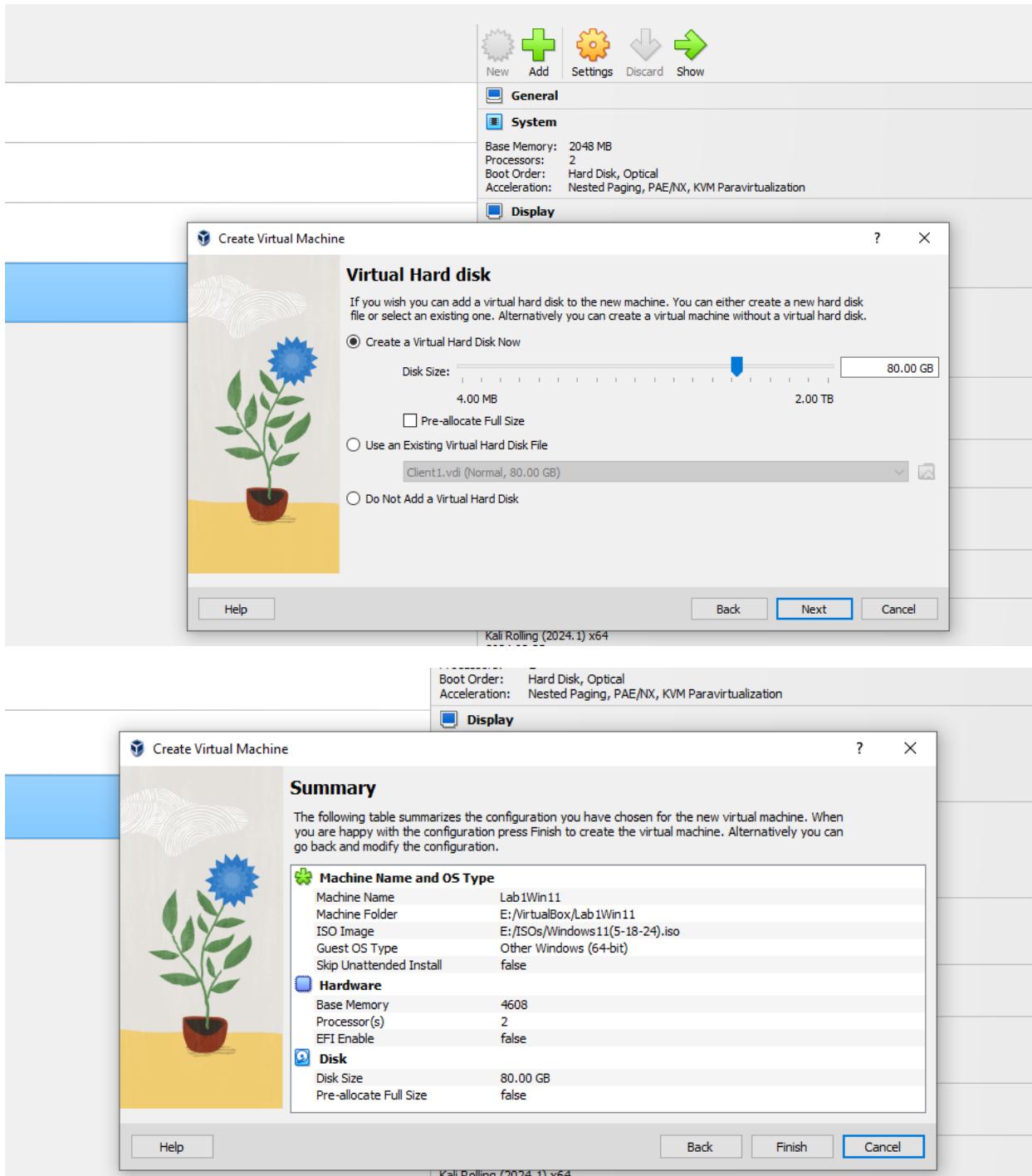




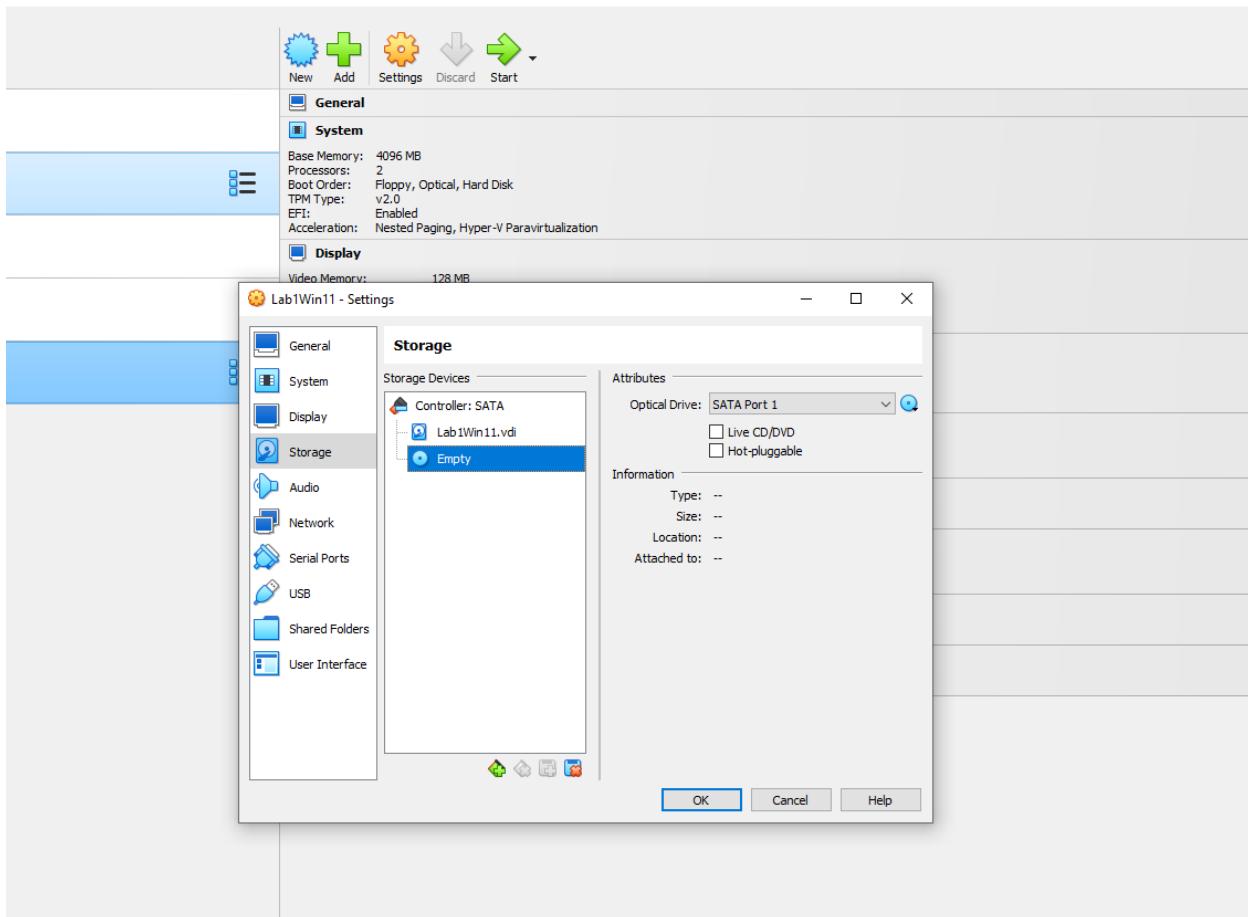
## Nueva máquina virtual de Windows 11

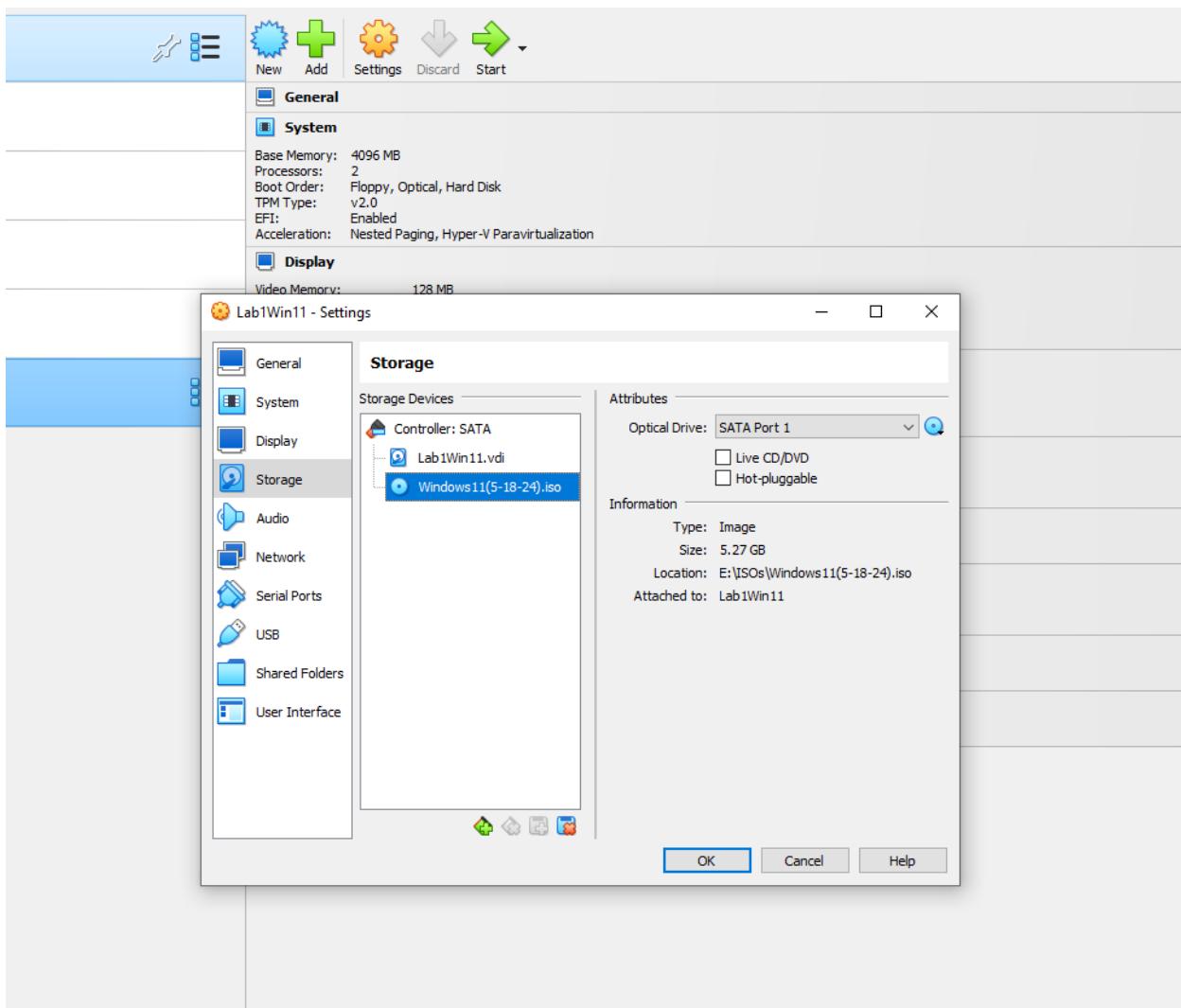


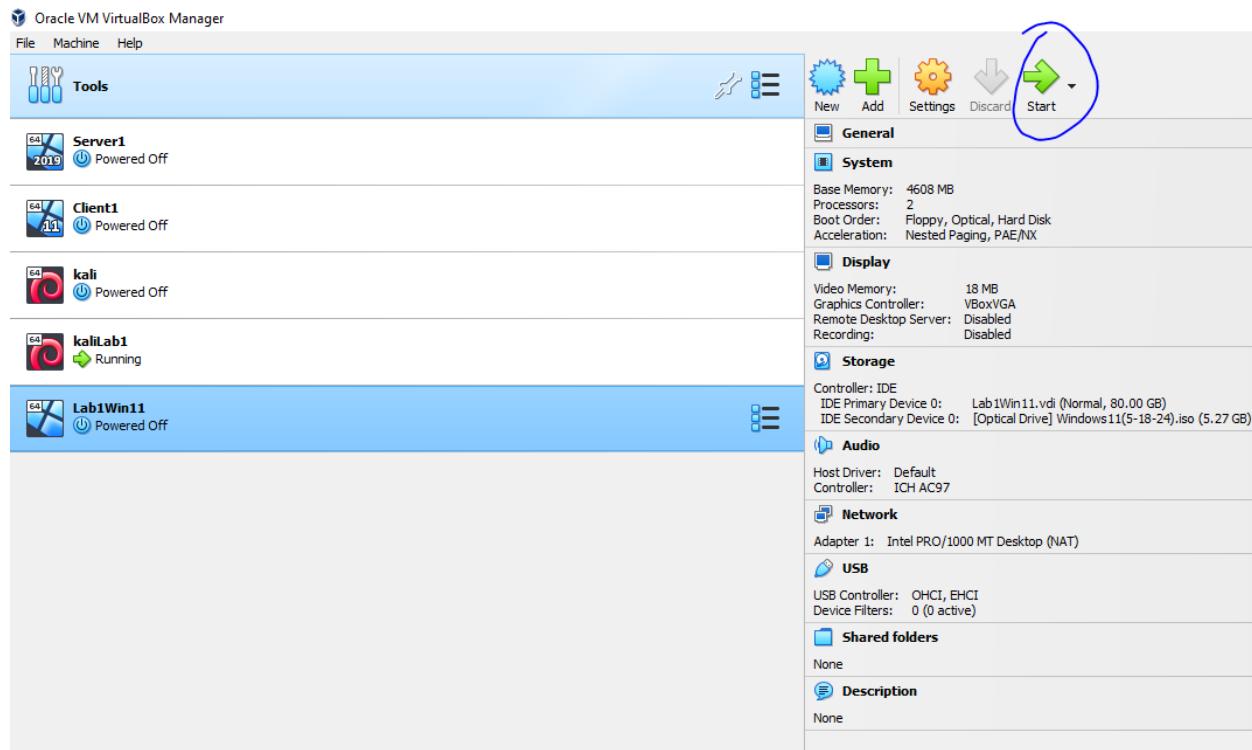


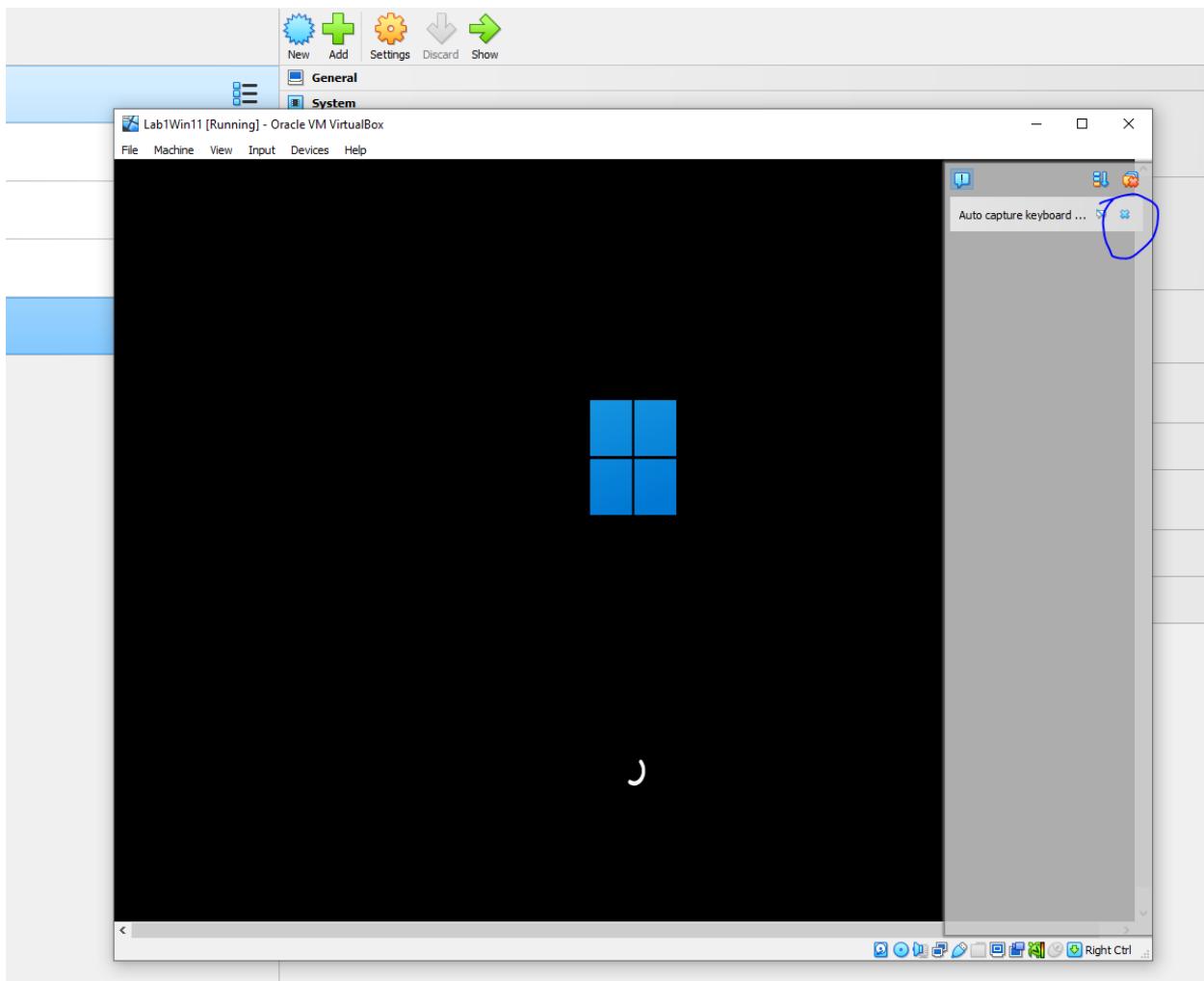


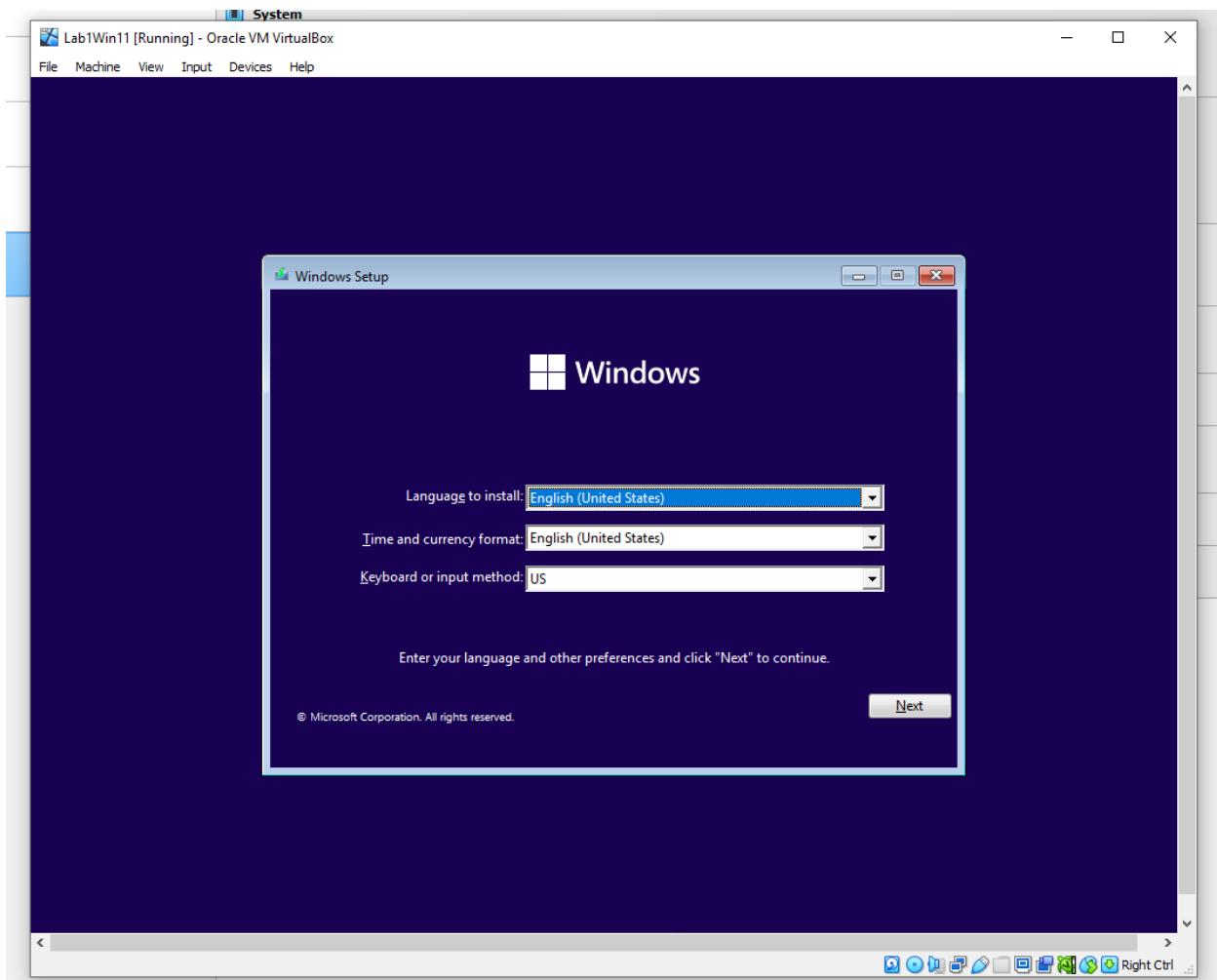
Elija la imagen ISO de Windows 11 desde la que arrancar

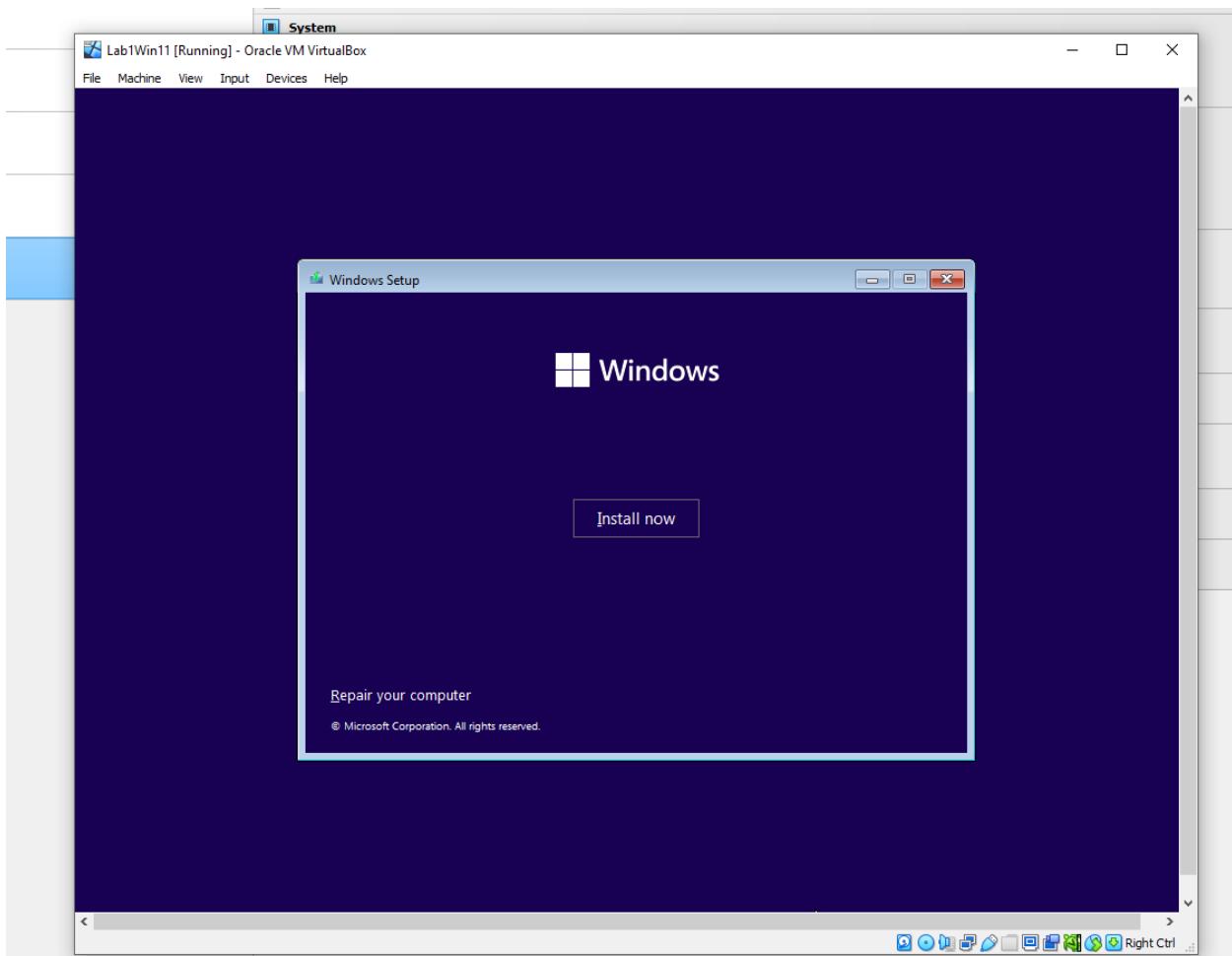


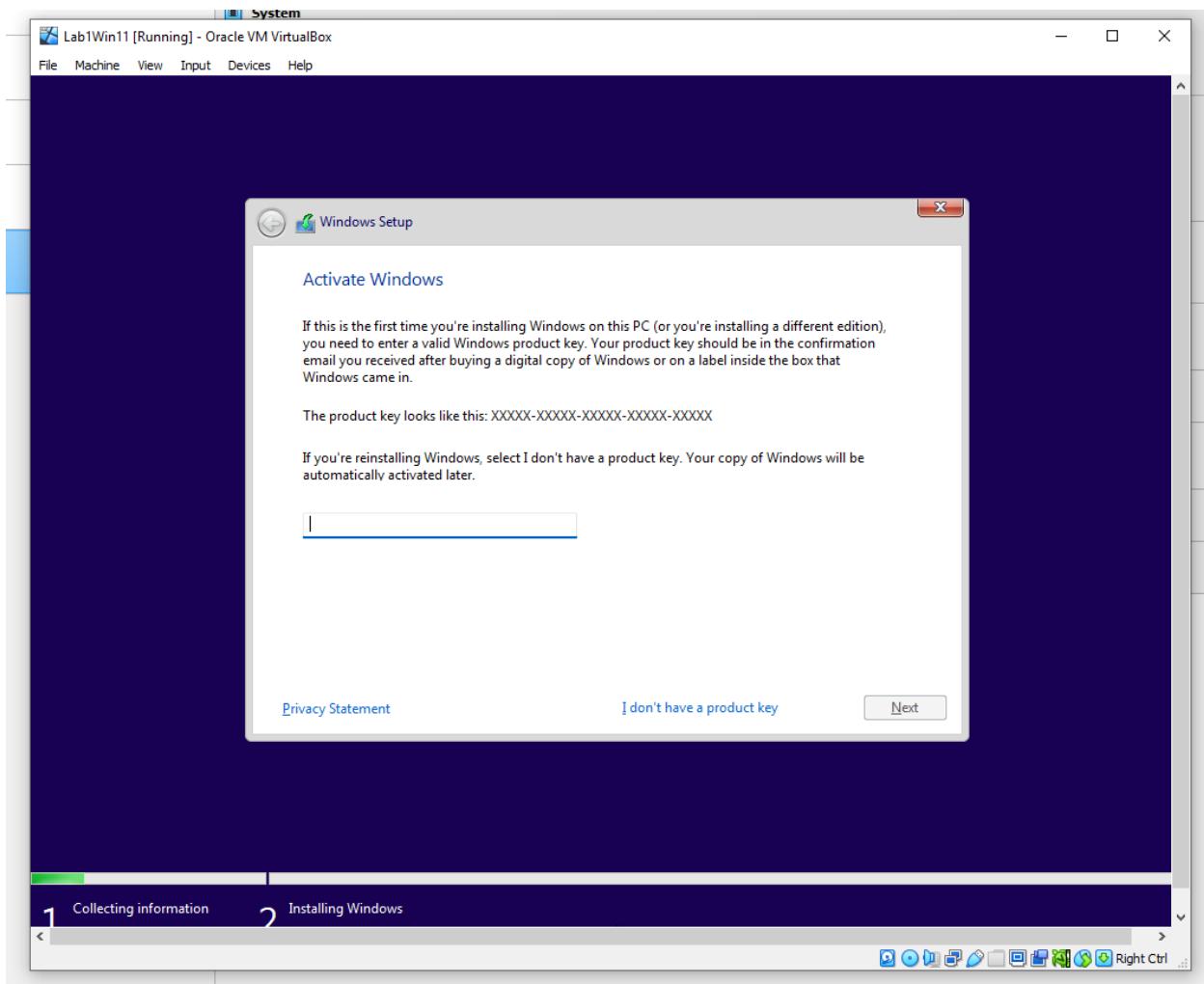


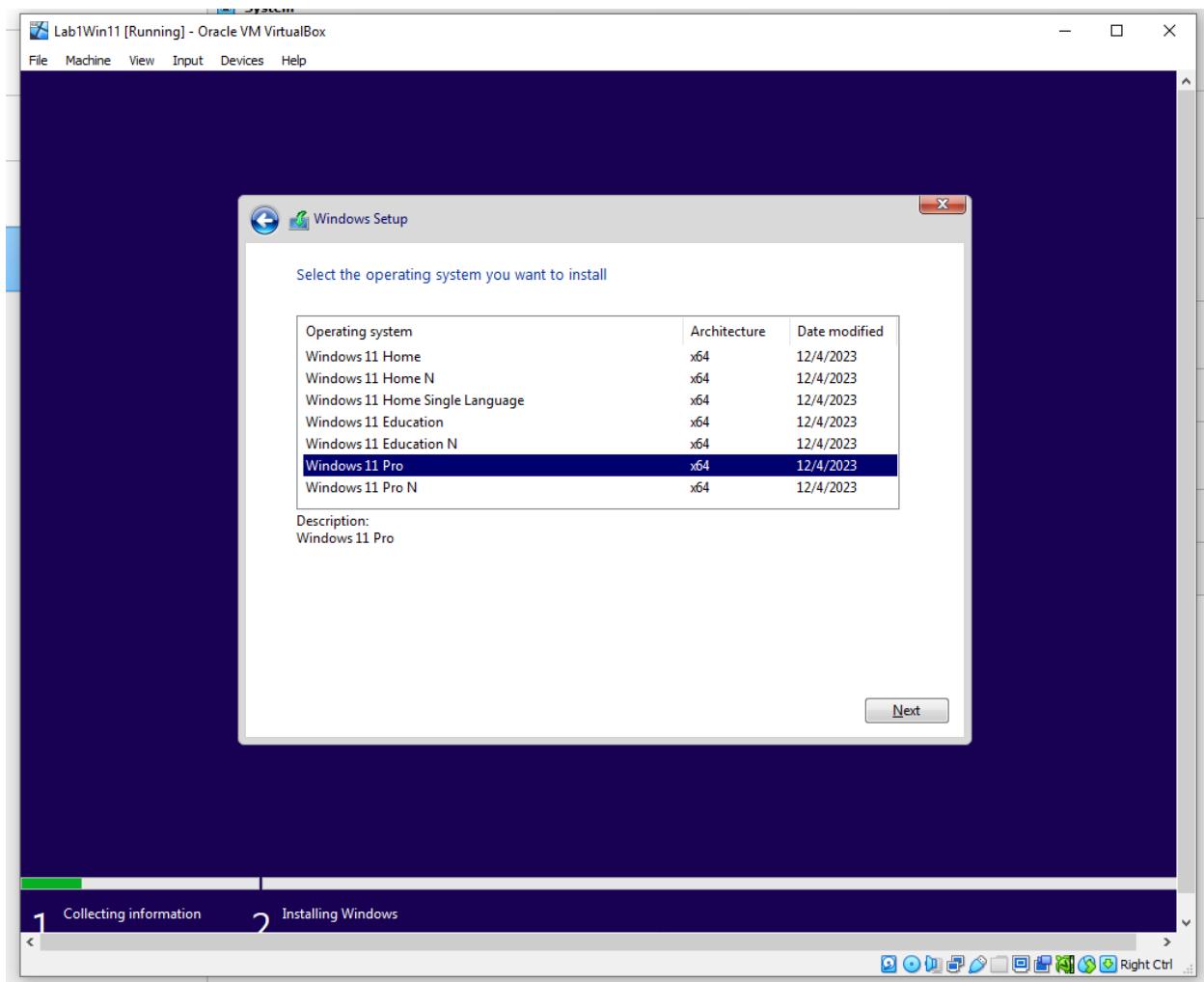


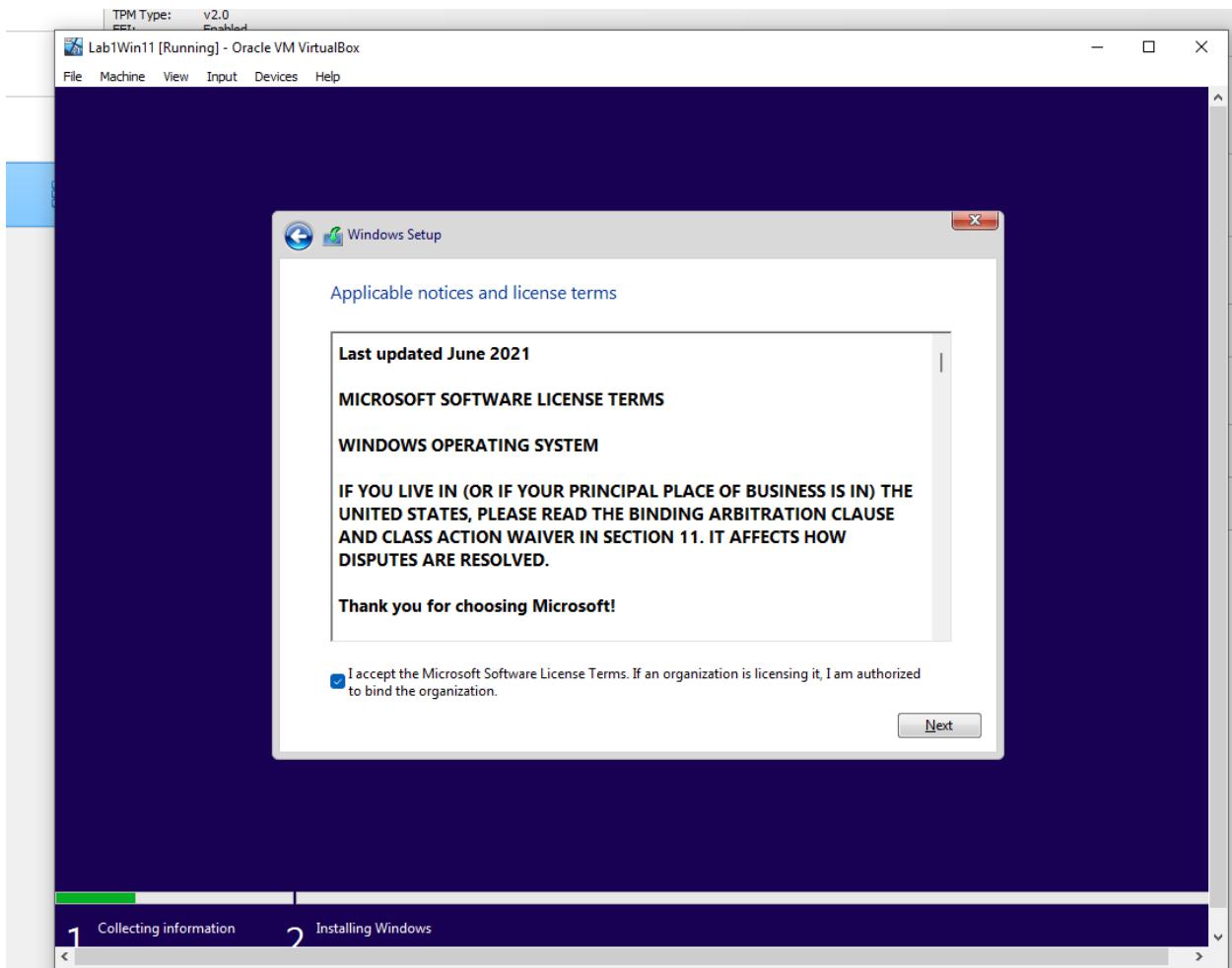


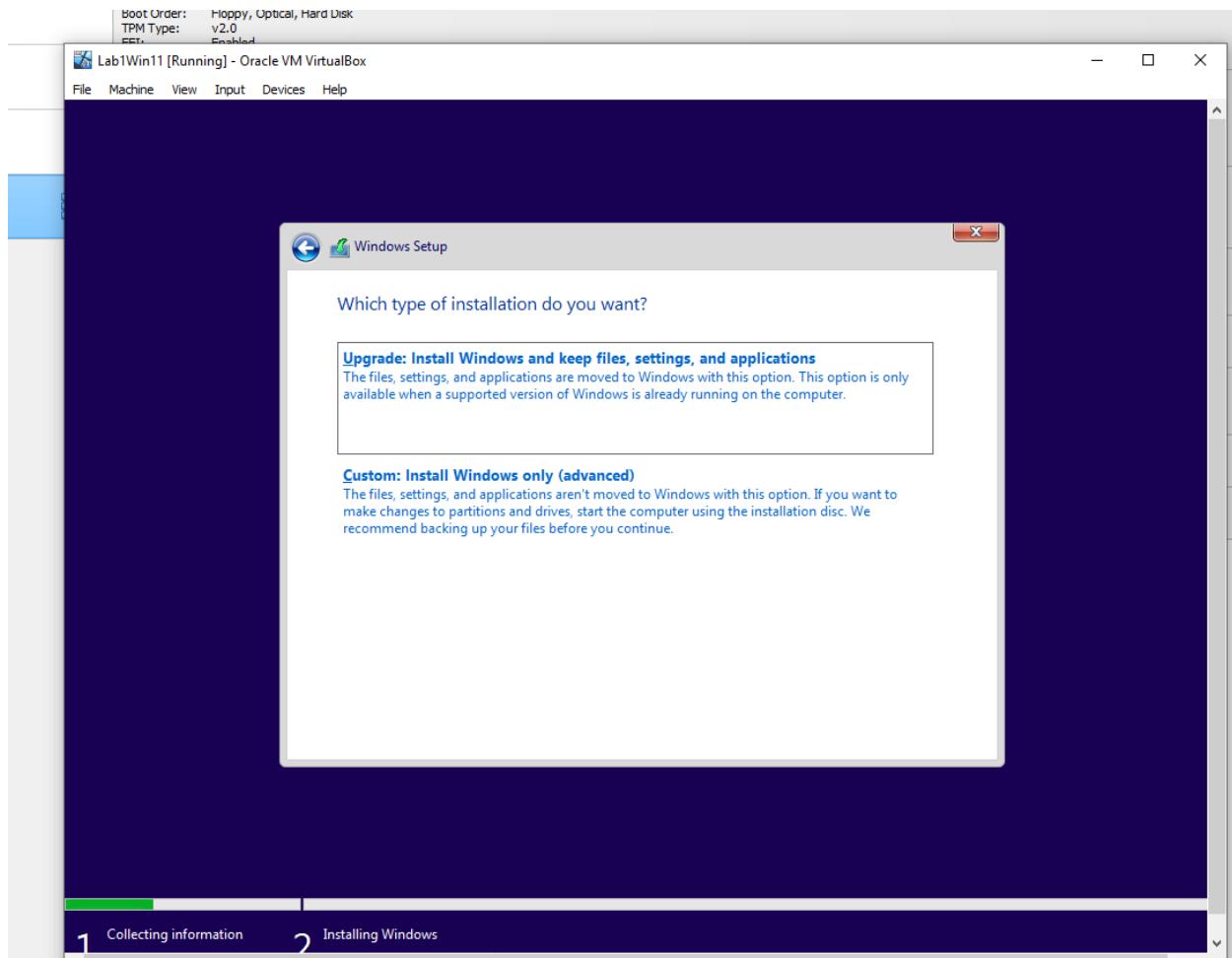


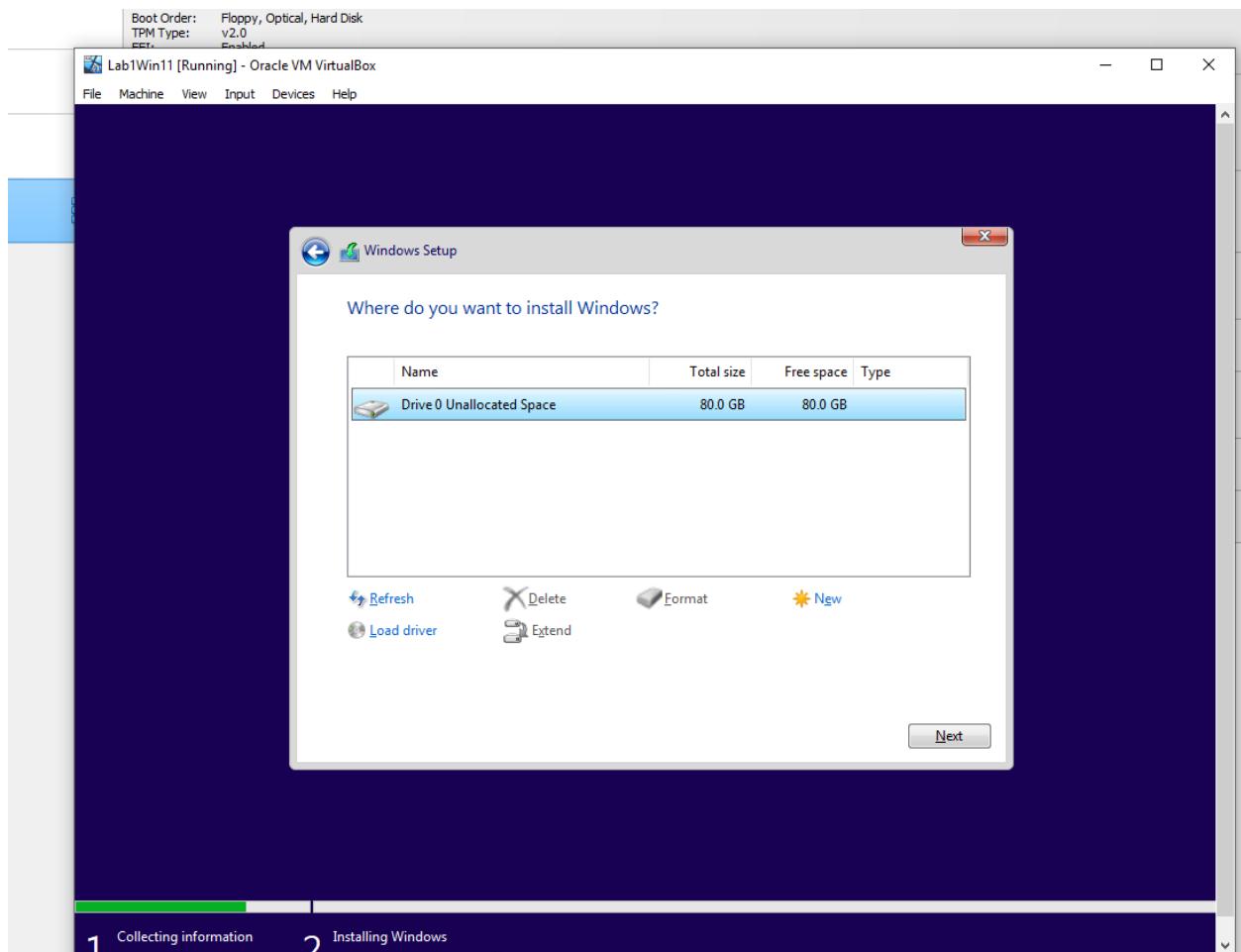


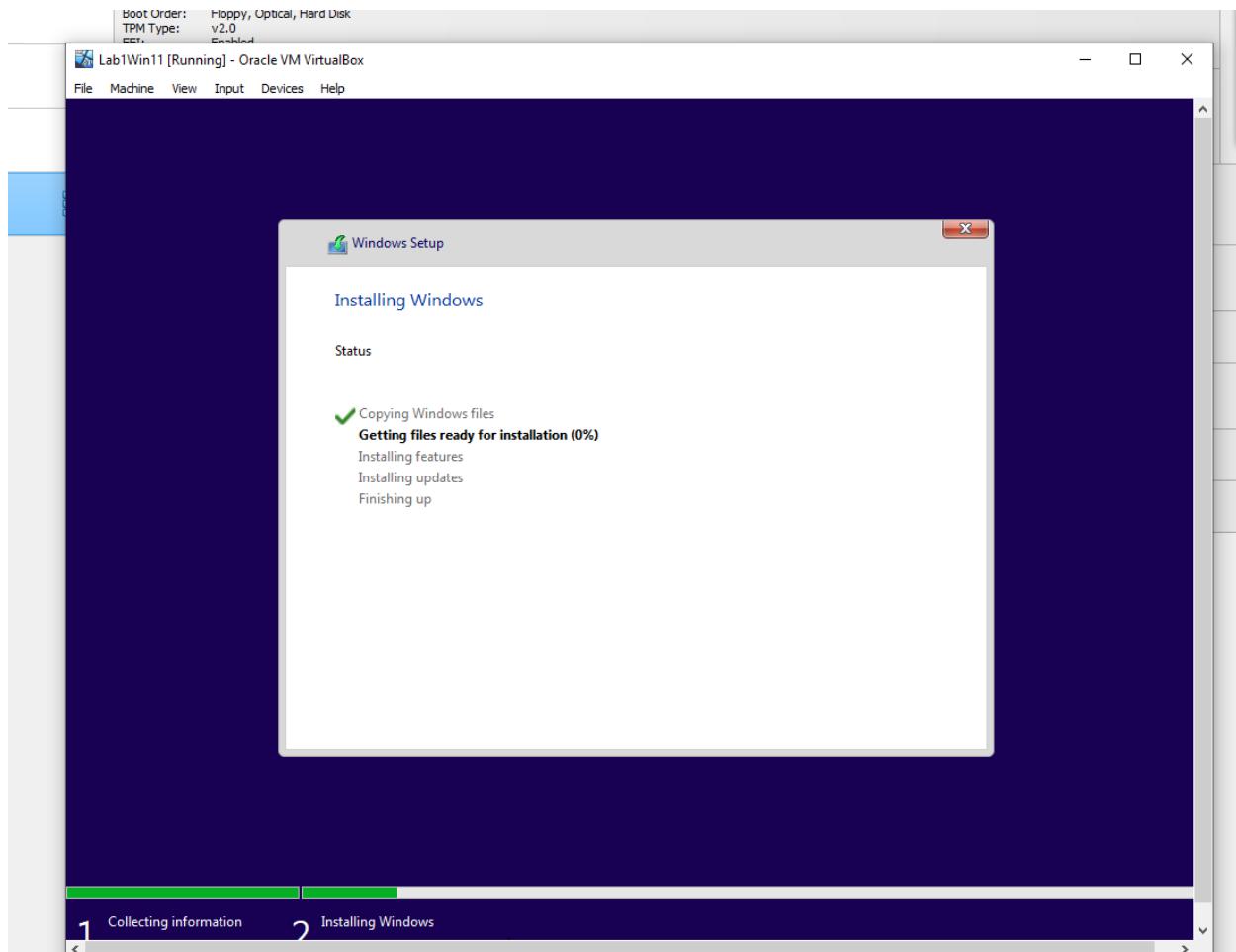


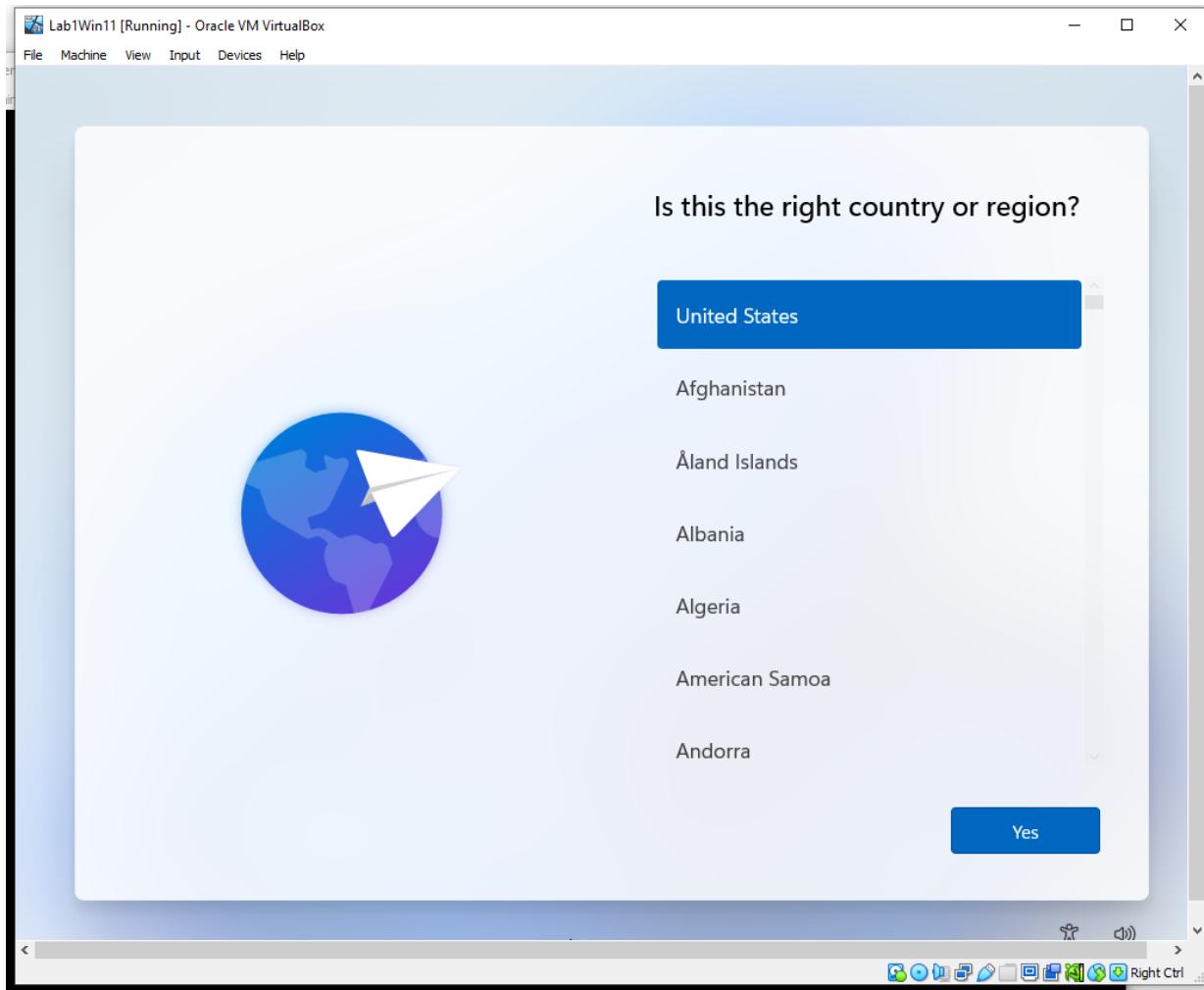


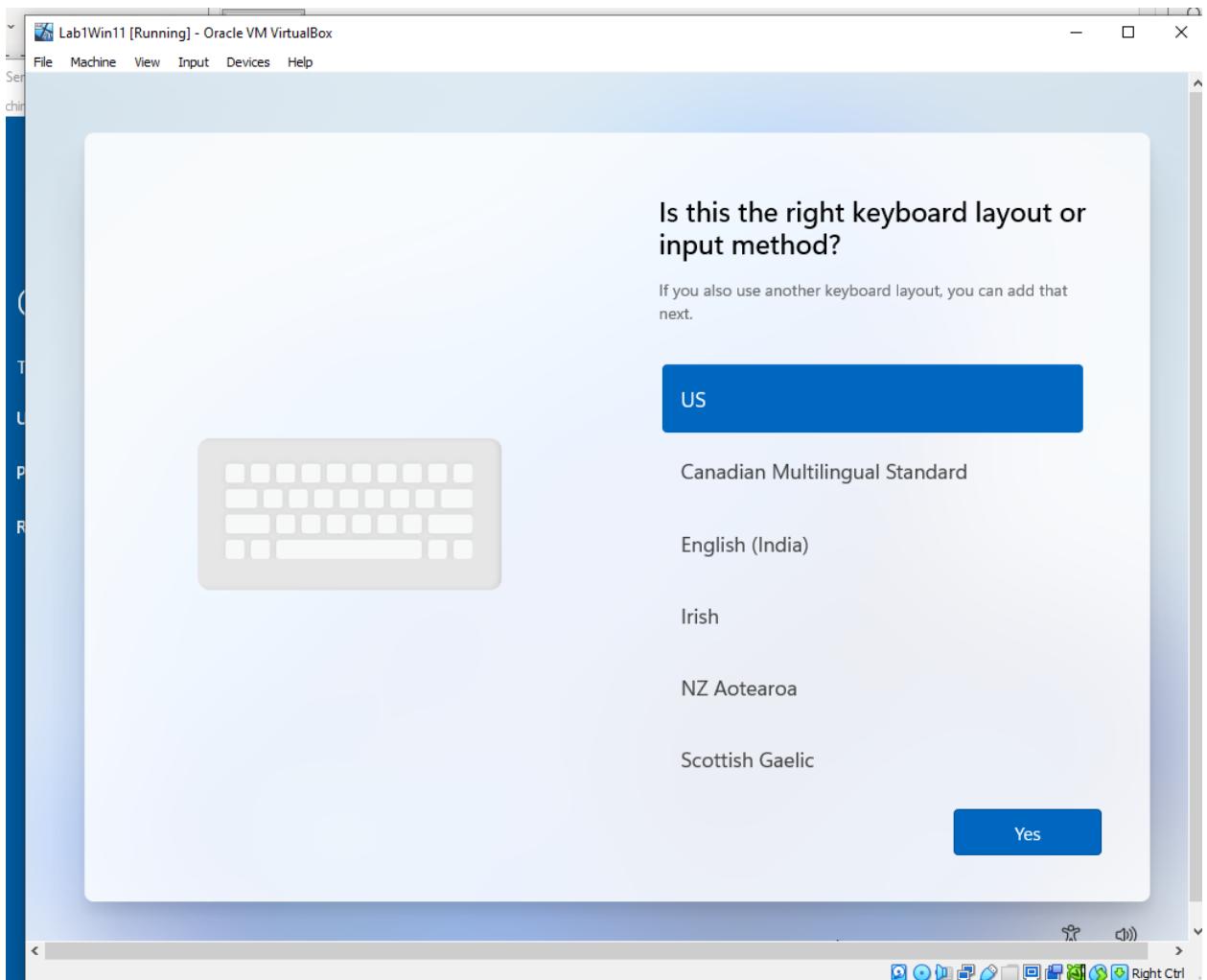


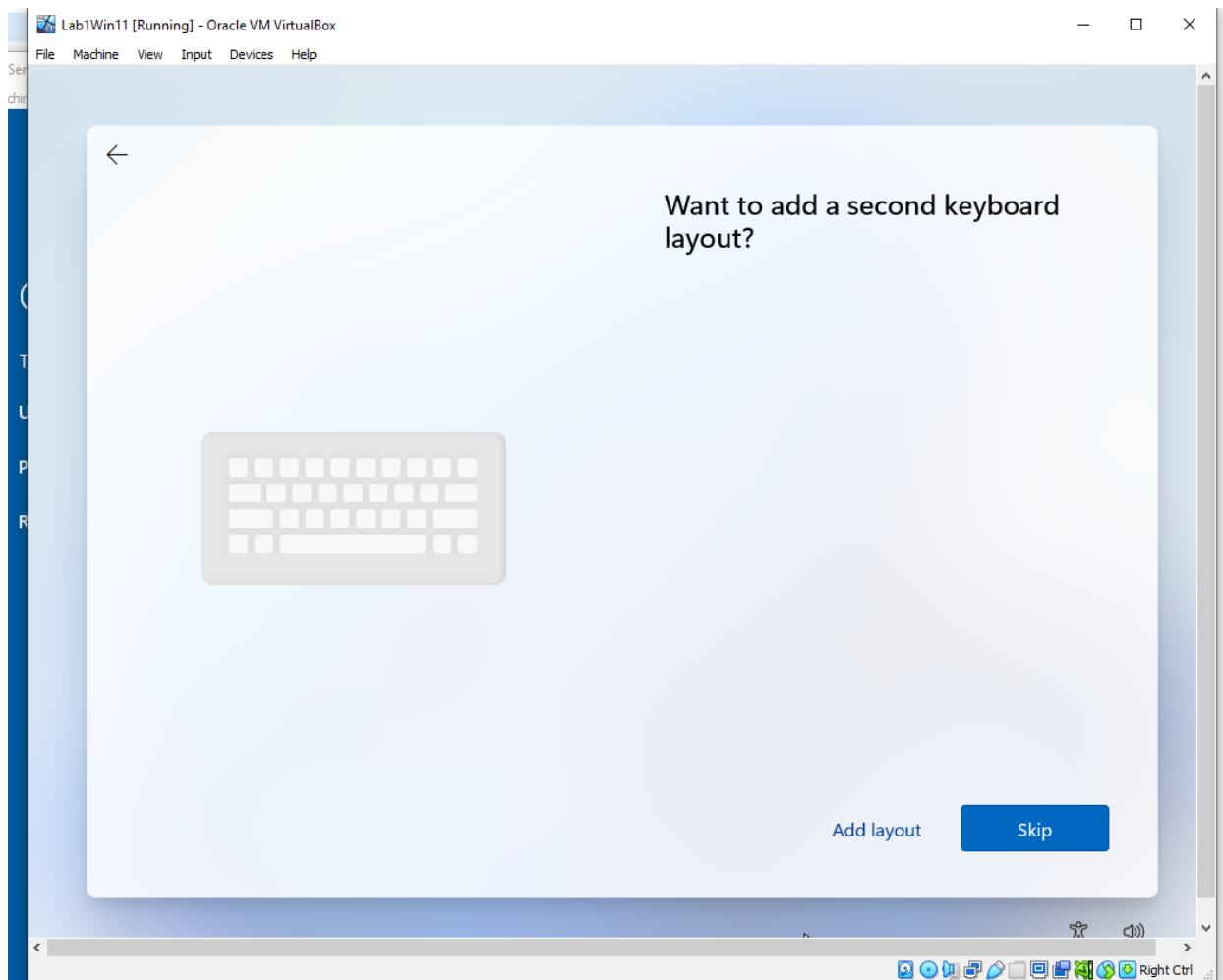






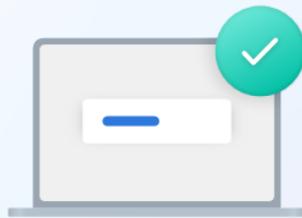






## Let's name your device

Make it yours with a unique name that's easy to recognize when connecting to it from other devices. Your device will restart after you name it.



Lab1Win11

X

Can't contain only numbers  
No more than 15 characters  
No spaces or special characters other than hyphen (-), dashes  
(— and –), and underscore (\_)

Skip for now

Next

How would you like to set up this device?



Set up for personal use

Use a personal Microsoft account to get set up and have full control over this device.



Set up for work or school

Get access to your organization's resources like email, network, apps, and services. Your organization will have full control over this device.

Next





## Let's set things up for your work or school

You'll use this info to sign in to your devices.



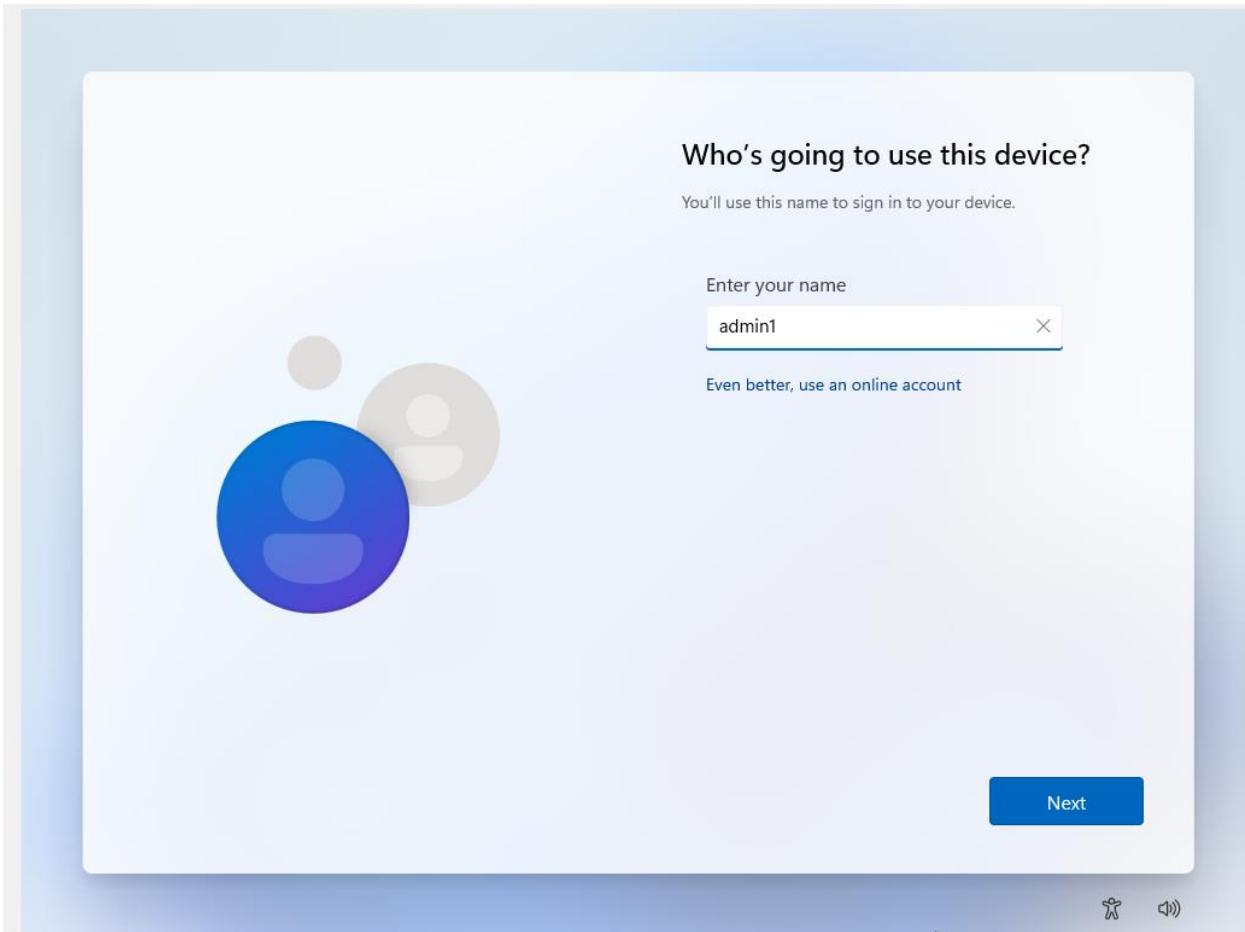
### Sign-in options

Face, fingerprint, PIN or security key  
Use your device to sign in with a passkey.

Domain join instead

[Back](#)







## Now add security questions

Just in case you forget your password, choose 3 security questions. Make sure your answers are unforgettable.

Security question (3 of 3)

What's the name of the first school you

123

Even better, use an online account

Next



## Choose privacy settings for your device

Microsoft puts you in control of your privacy. Choose your settings, then select **Accept** to save them. You can change these settings at any time.

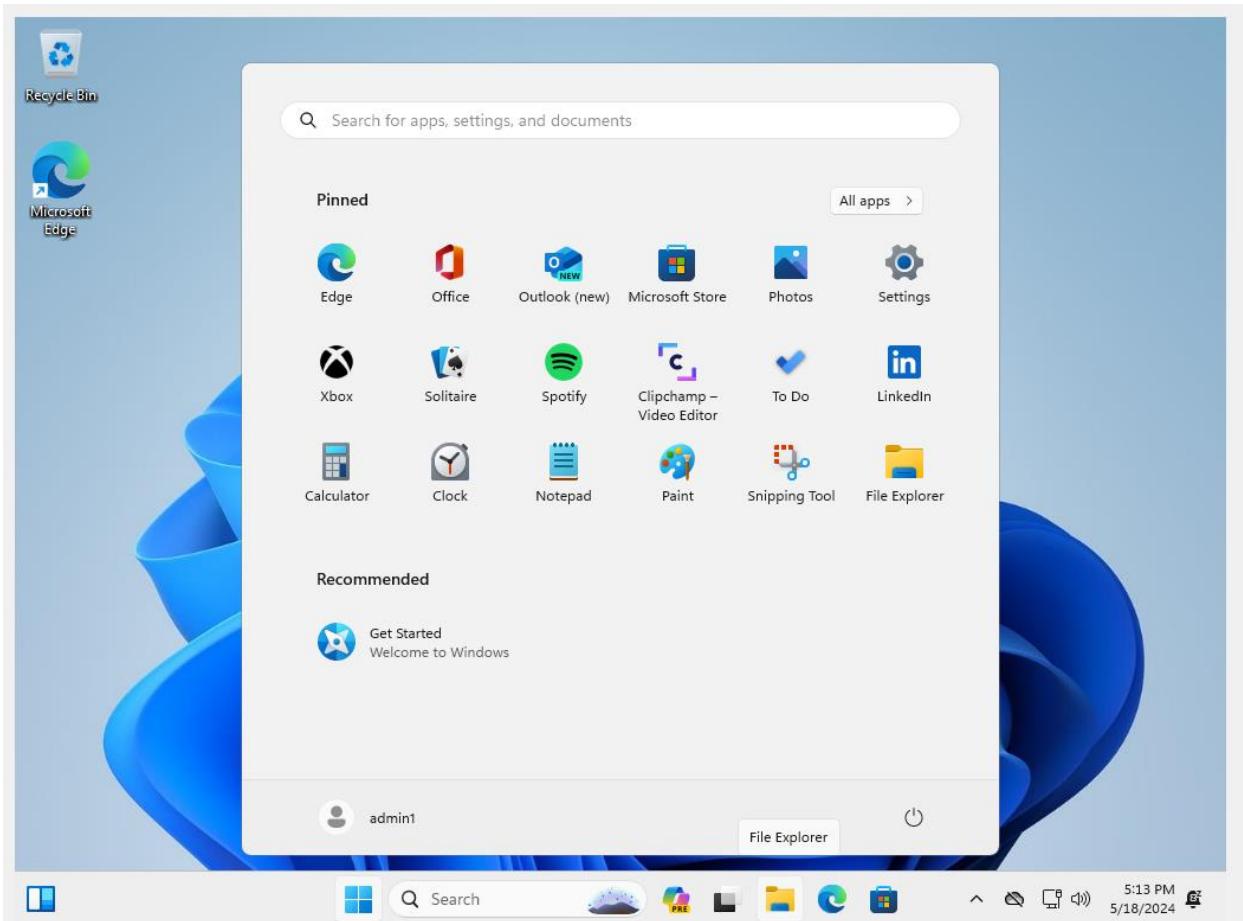
Don't use my diagnostic data to help improve the language recognition and suggestion capabilities of Microsoft apps and services.  
 No

**Tailored experiences**  
The tips, ads, and recommendations you see will be more generic and may be less relevant to you.  
 No

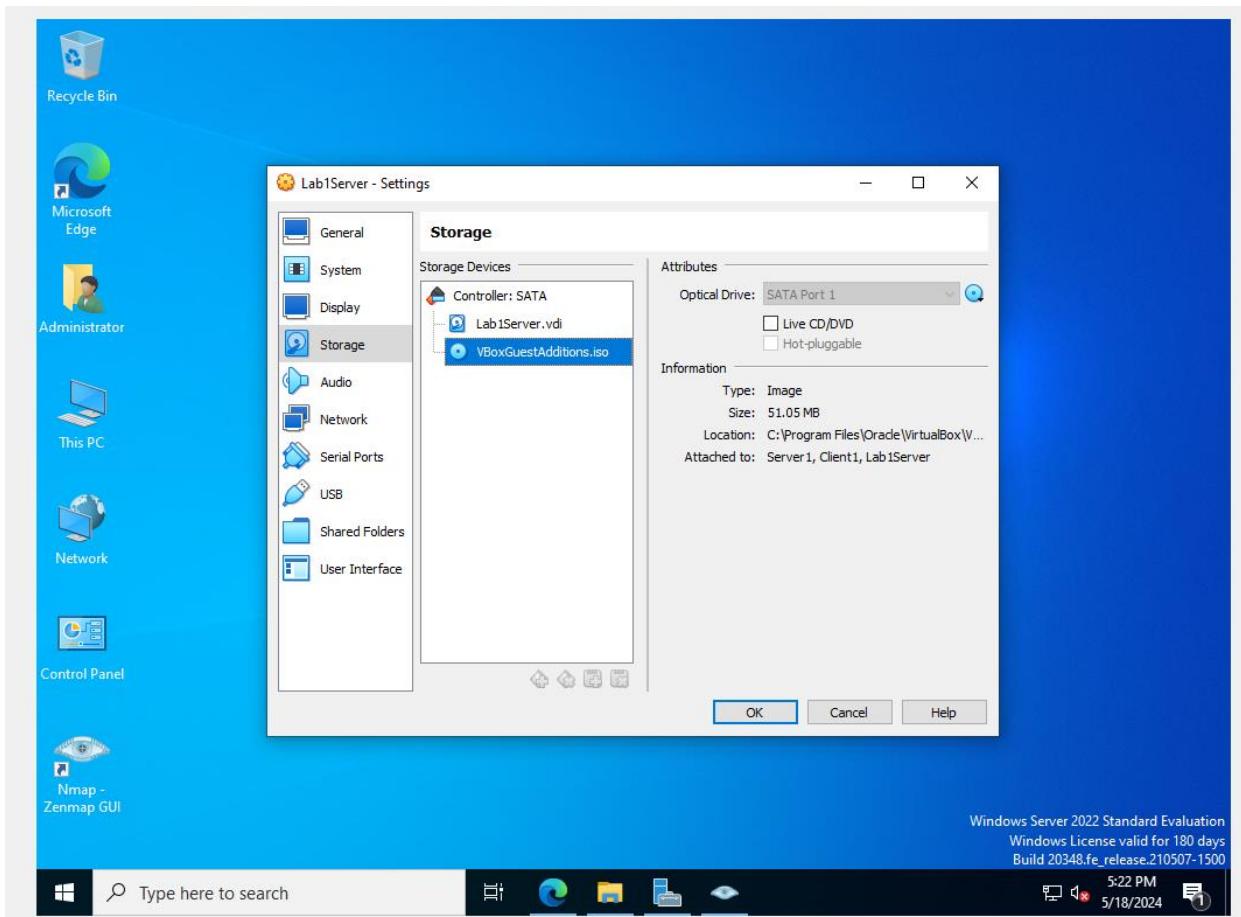
**Advertising ID**  
The number of ads you see won't change, but they may be less relevant to you.  
 No

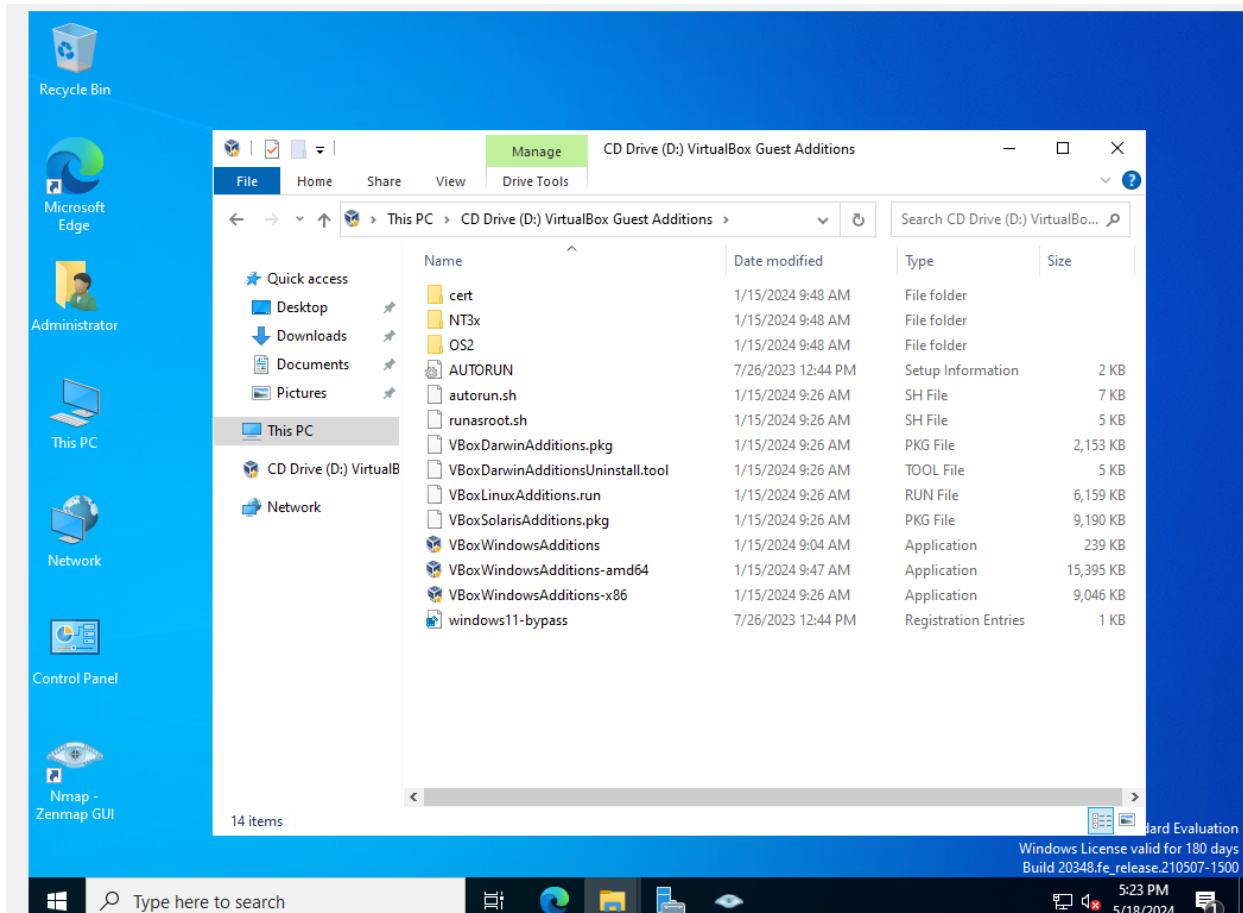
Select **Learn more** for info on the above settings, how Windows helps protect you from unsafe apps and web

[Learn more](#) [Next](#)



## Adiciones de invitados





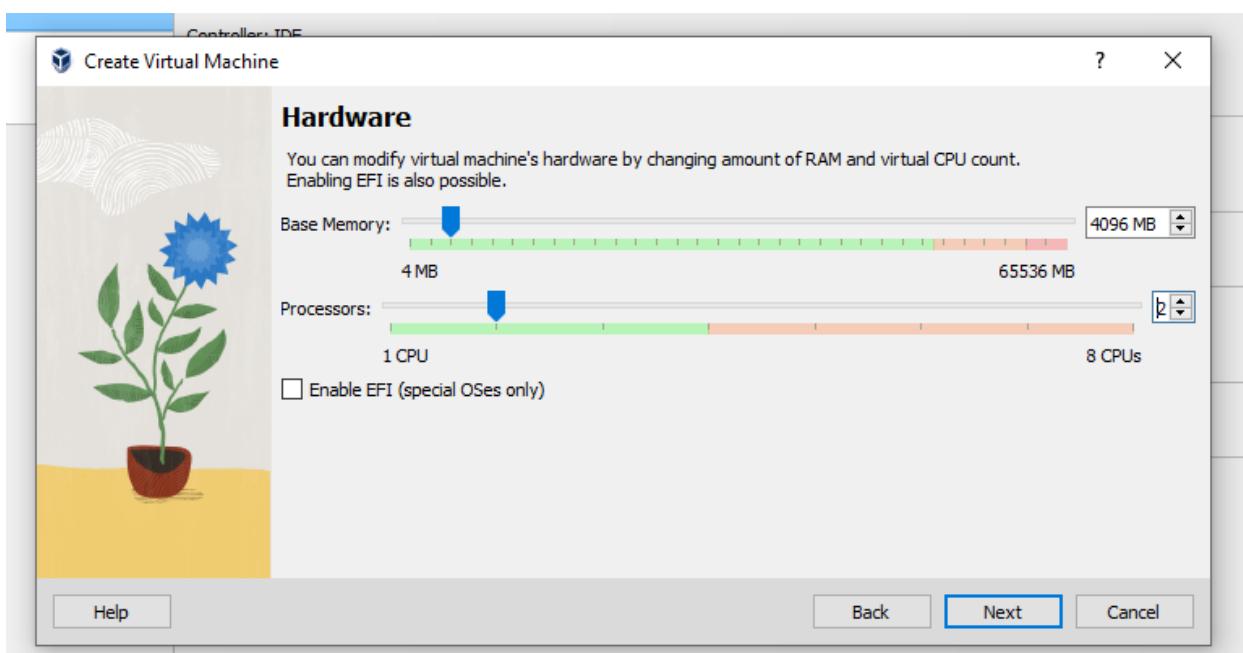
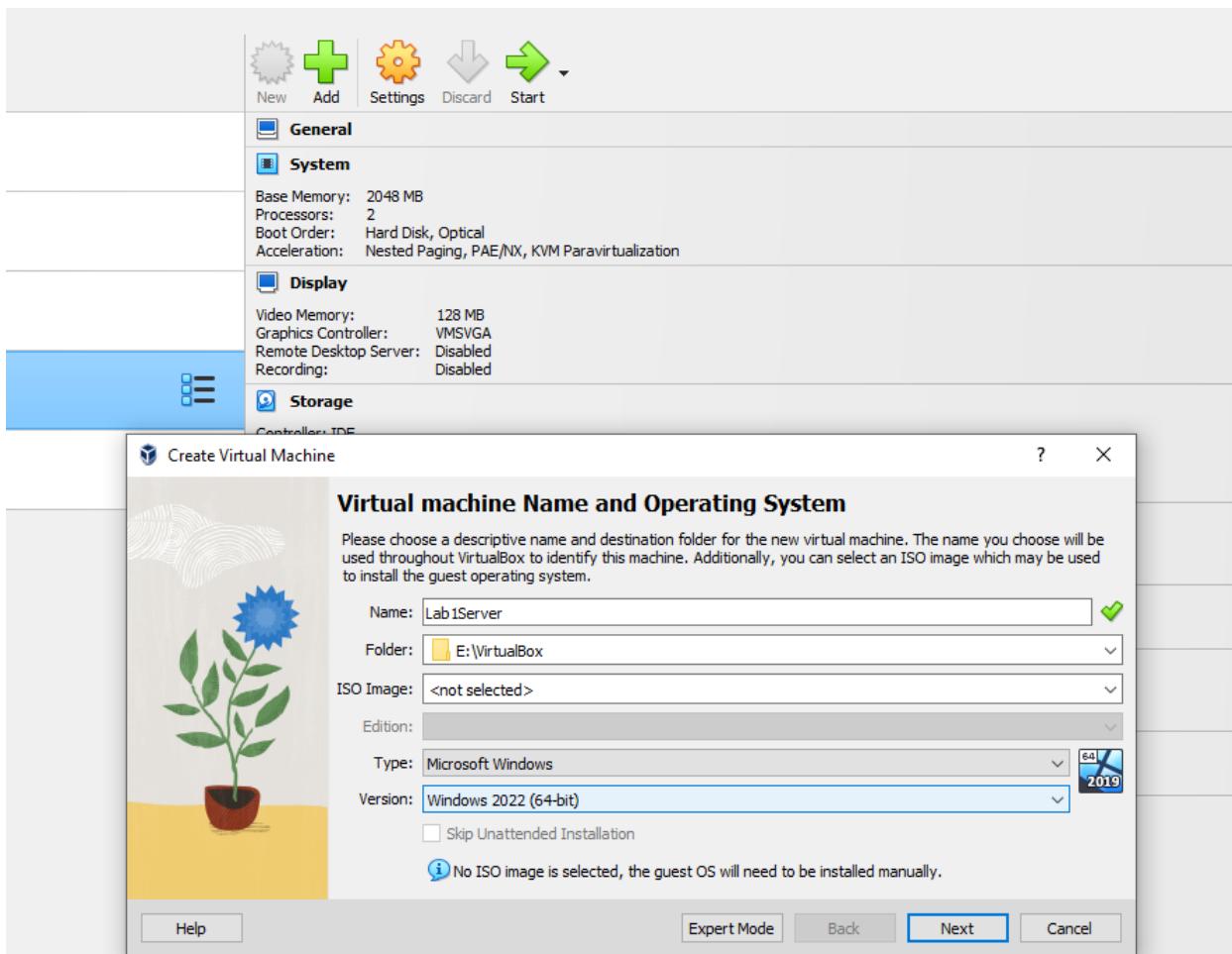
## Instalación de Windows Server 2022 como controlador de dominio

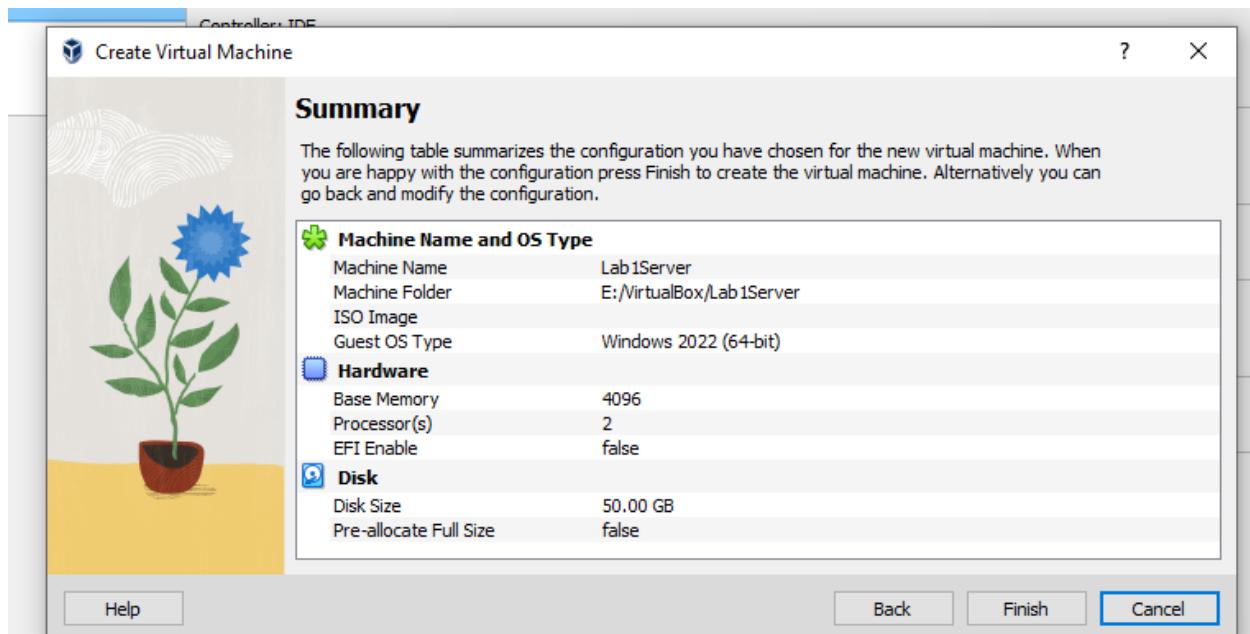
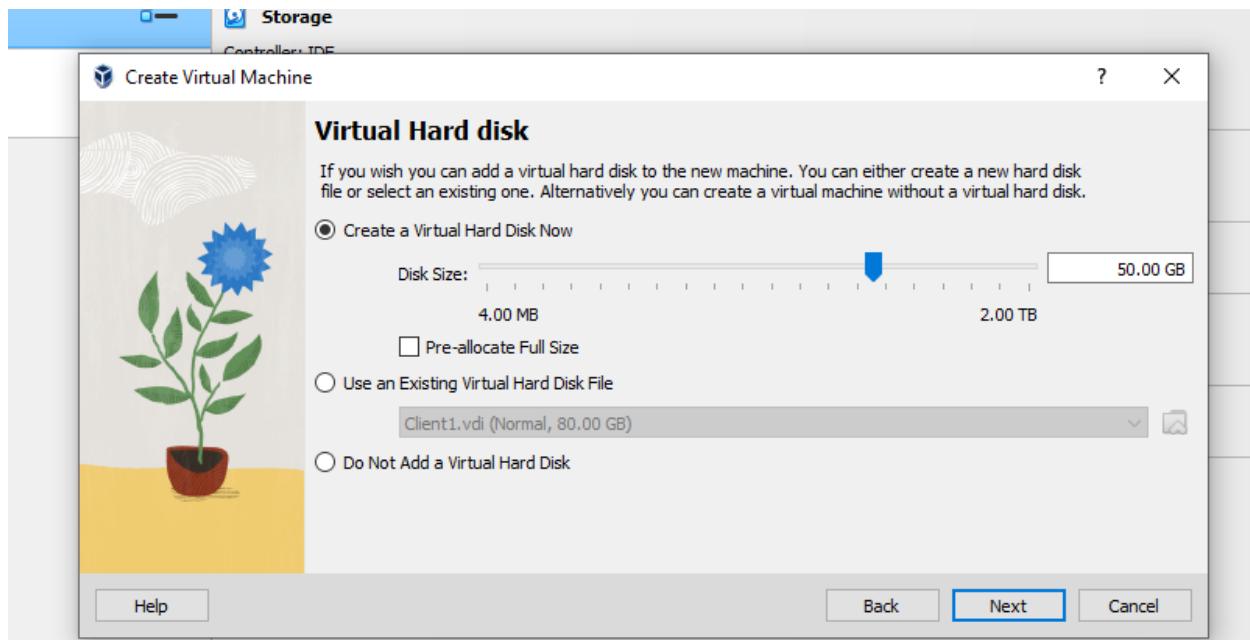
<https://www.microsoft.com/en-us/evalcenter/download-windows-server-2022>

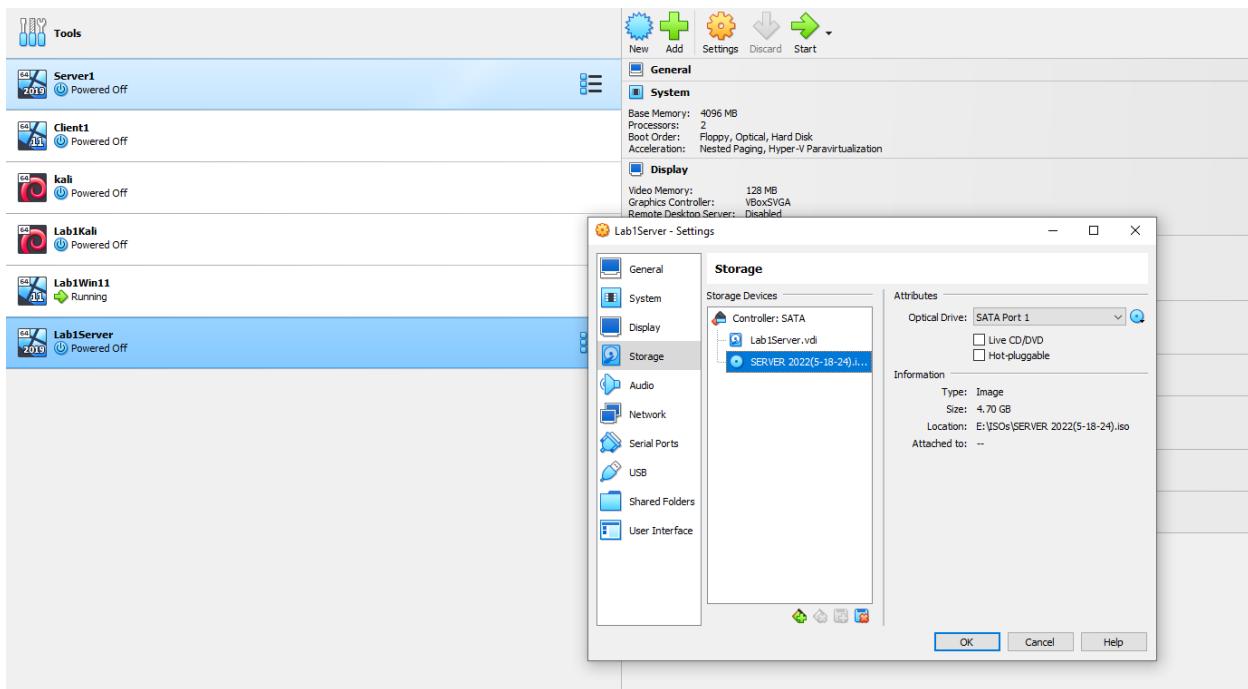
The screenshot shows the Microsoft Evaluation Center page for Windows Server 2022. At the top, there's a navigation bar with links like Personal stuff, YouTube, Cars, ChatGPT, M365, Bard, NSC, Learning, SeoChannel, Cybersecurity Hoy, LinkedIn, MSC, and WhatsApp. Below the navigation bar, there's a main heading: "Please select your Windows Server 2022 download". A horizontal line follows. Below that, there's a table with three rows, each representing a language: English (United States), Chinese (Simplified), and French. Each row contains four columns: "ISO downloads" (with a link to "64-bit edition"), "VHD download" (with a link to "64-bit edition"), "Try on Azure" (with a link to "Learn more >"), and "Create a VM in Azure" (with a link to "Learn more >").

English (United States)	<b>ISO downloads</b> 64-bit edition >	<b>VHD download</b> 64-bit edition >	<b>Try on Azure</b> Learn more >	<b>Create a VM in Azure</b> Learn more >
Chinese (Simplified)	<b>ISO downloads</b> 64-bit edition >			
French	<b>ISO downloads</b> 64-bit edition >			

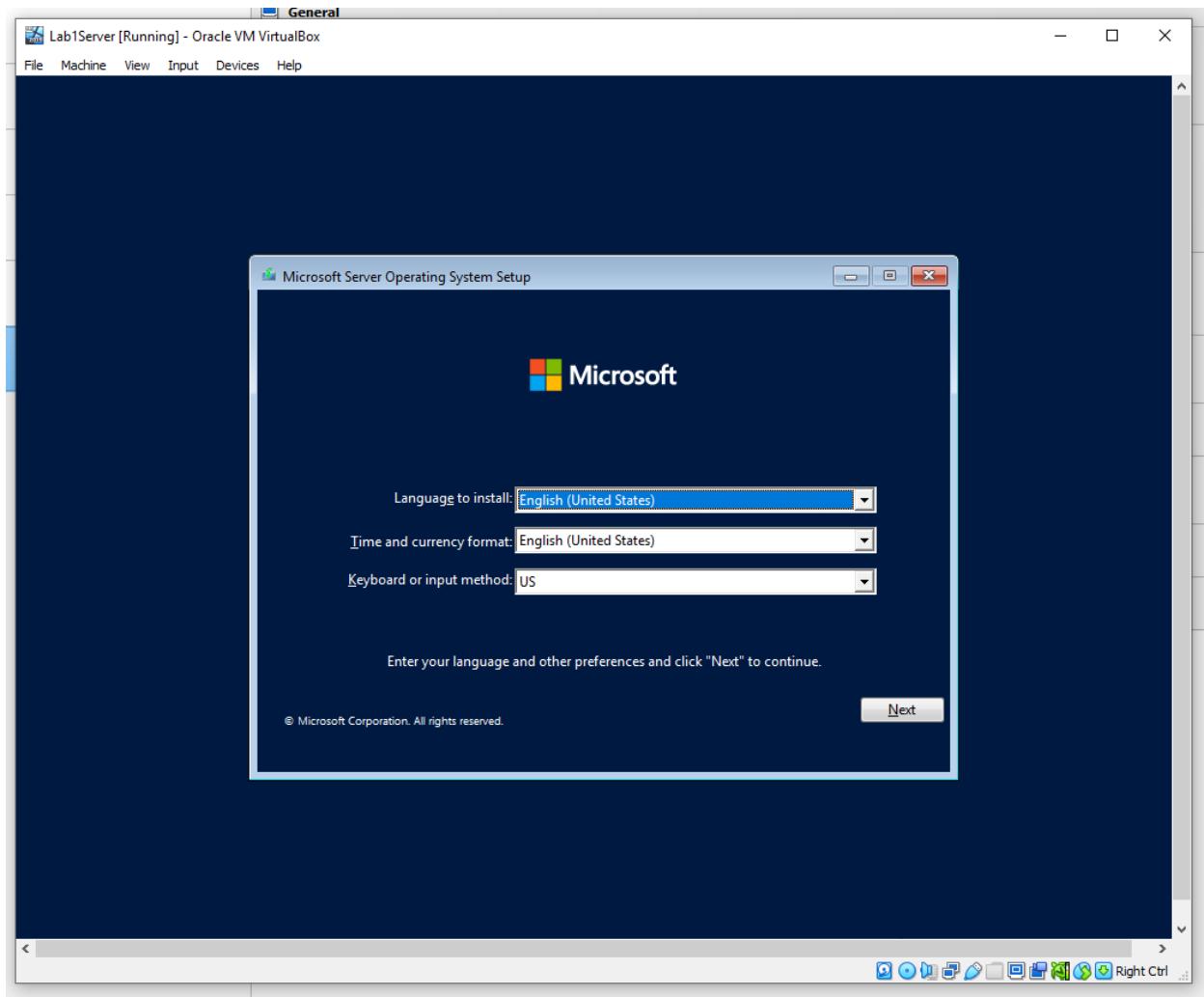
## Creación de una máquina virtual de Windows Server 2022

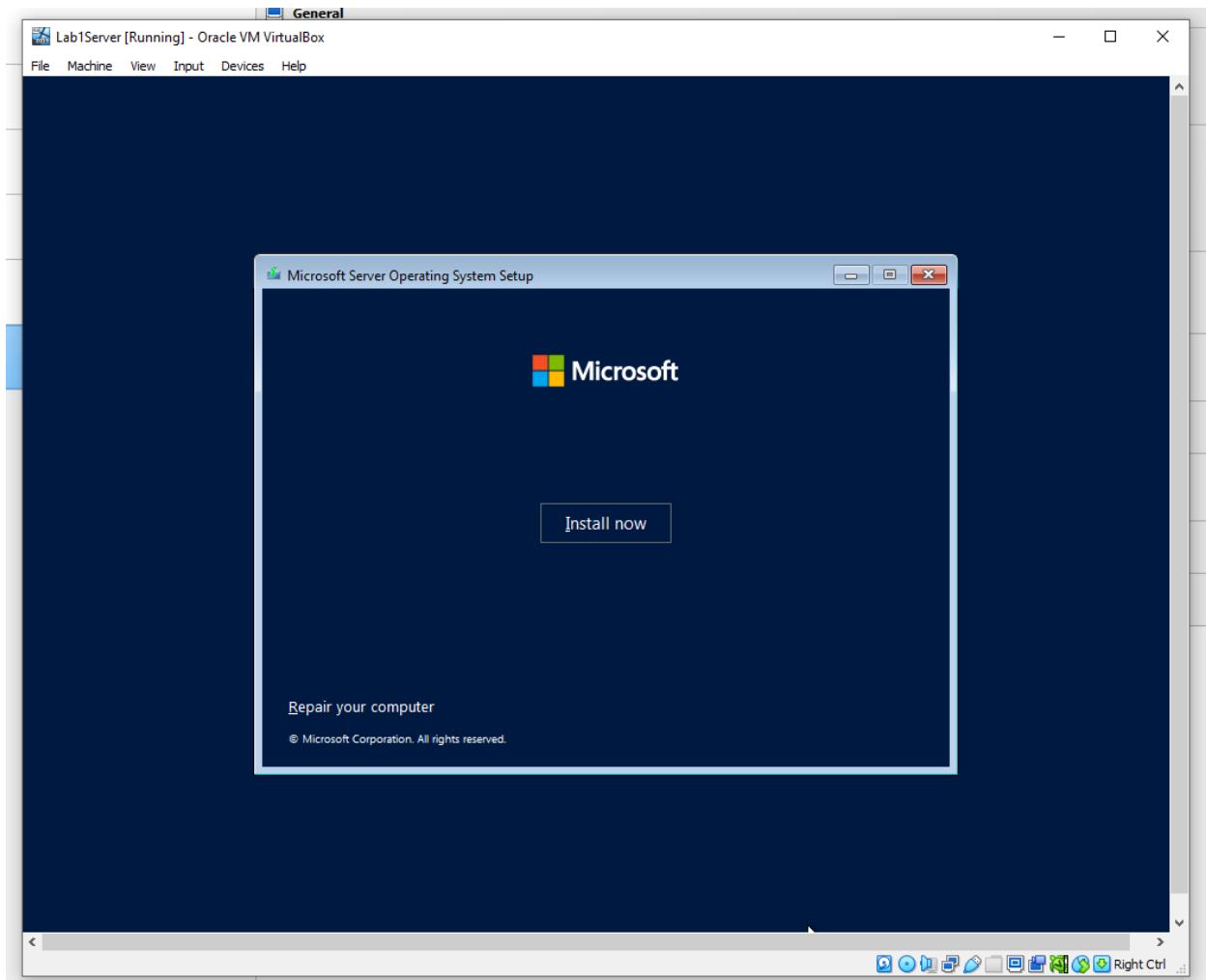


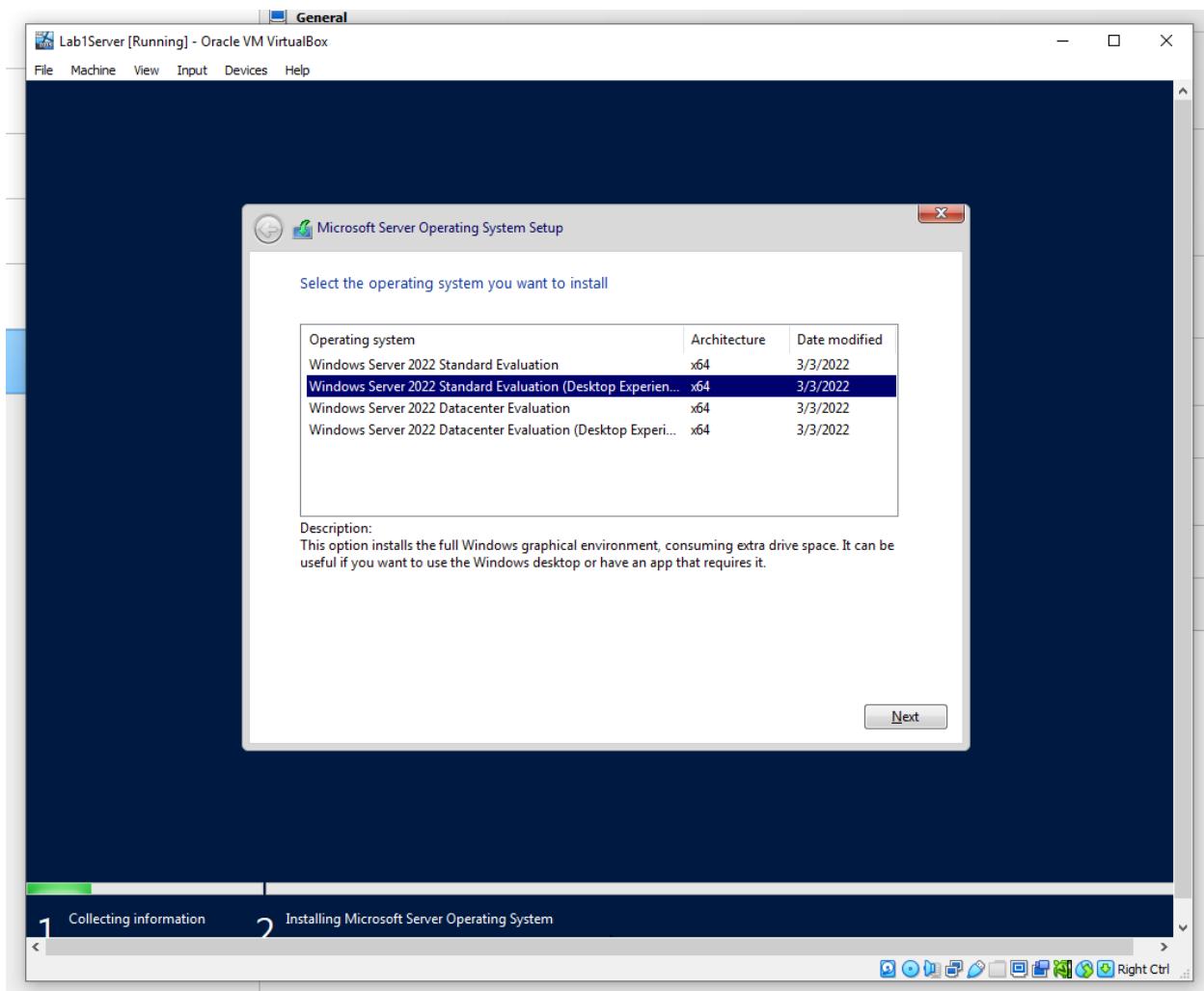


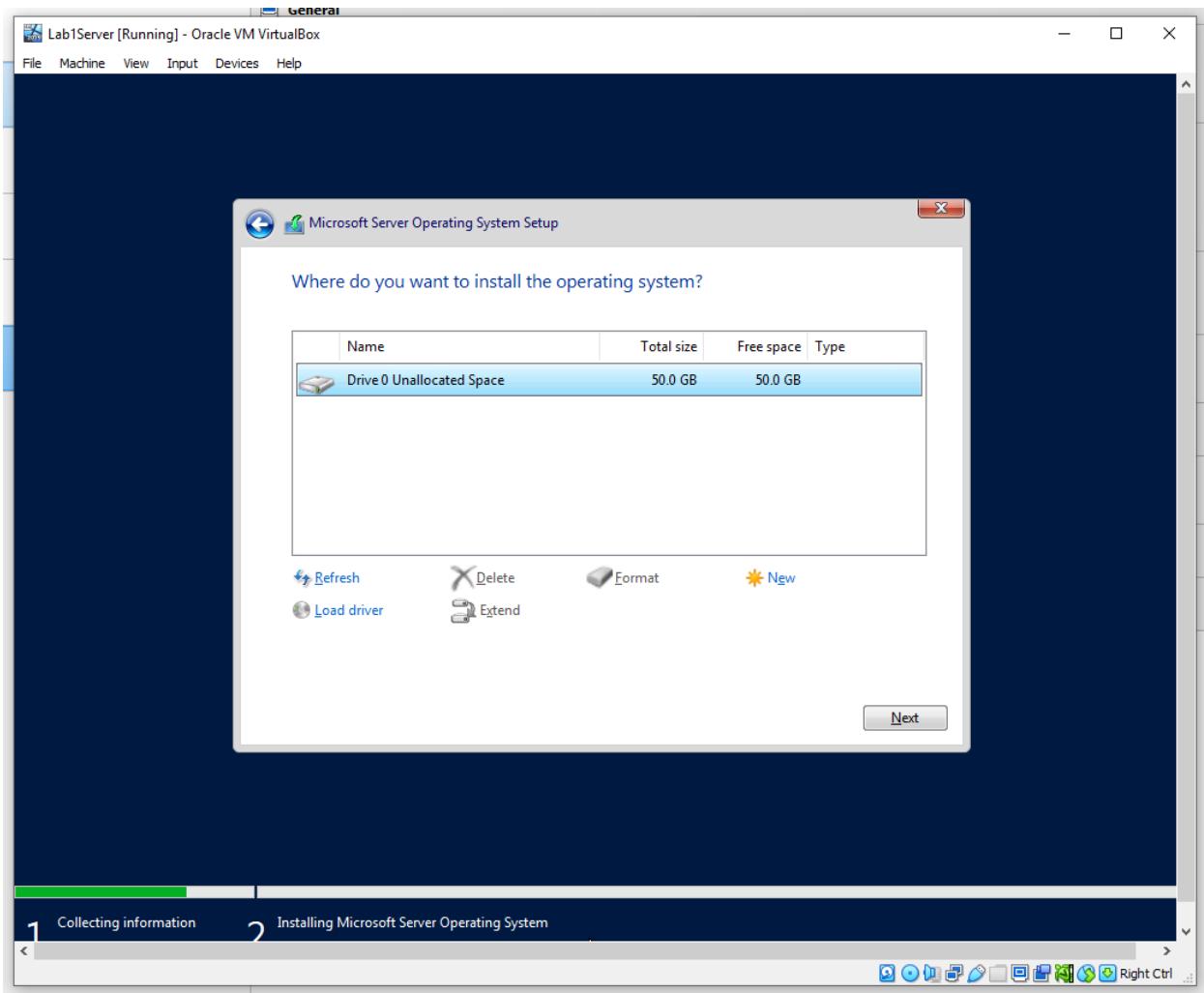


## Instalación de Windows Server 2022

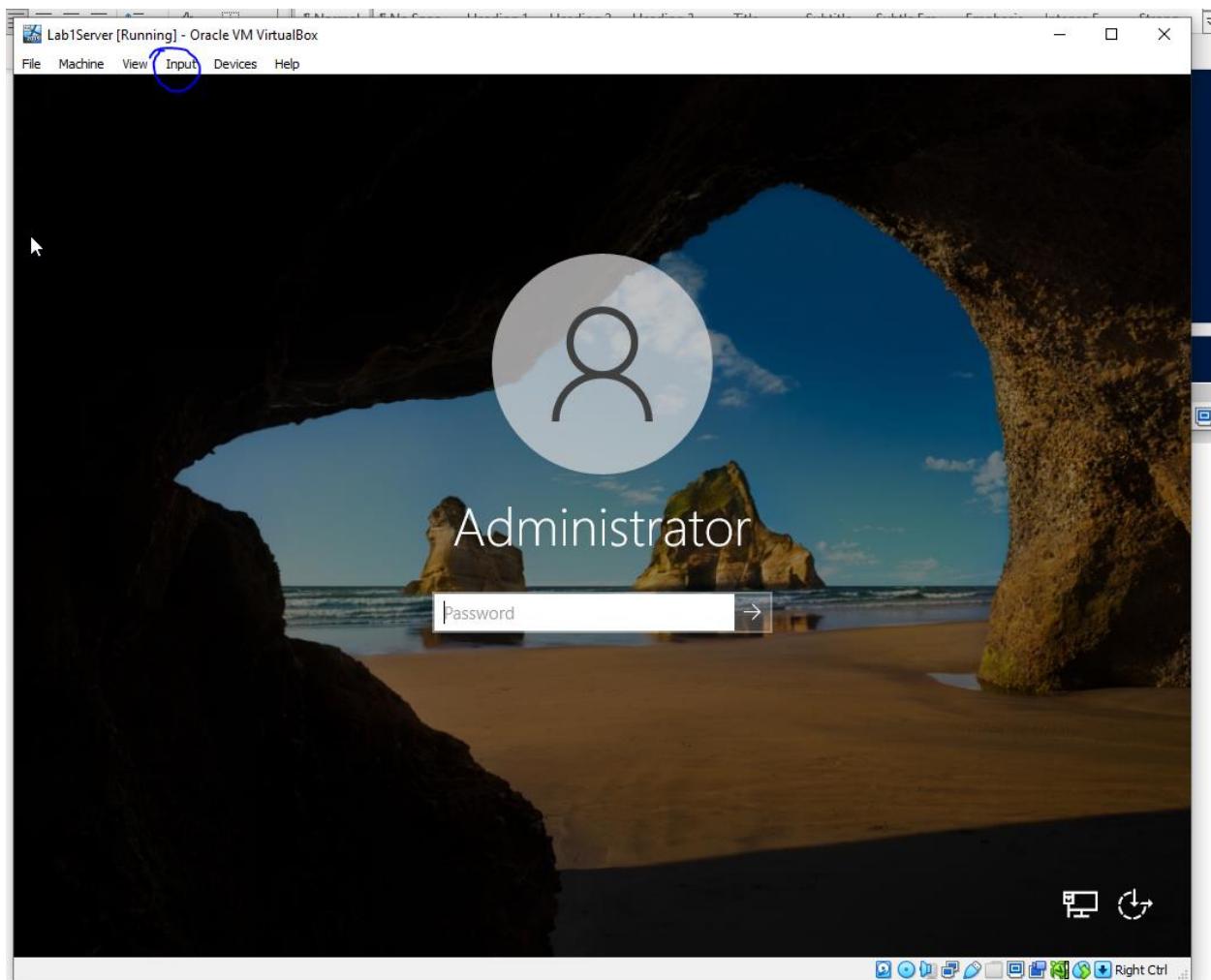


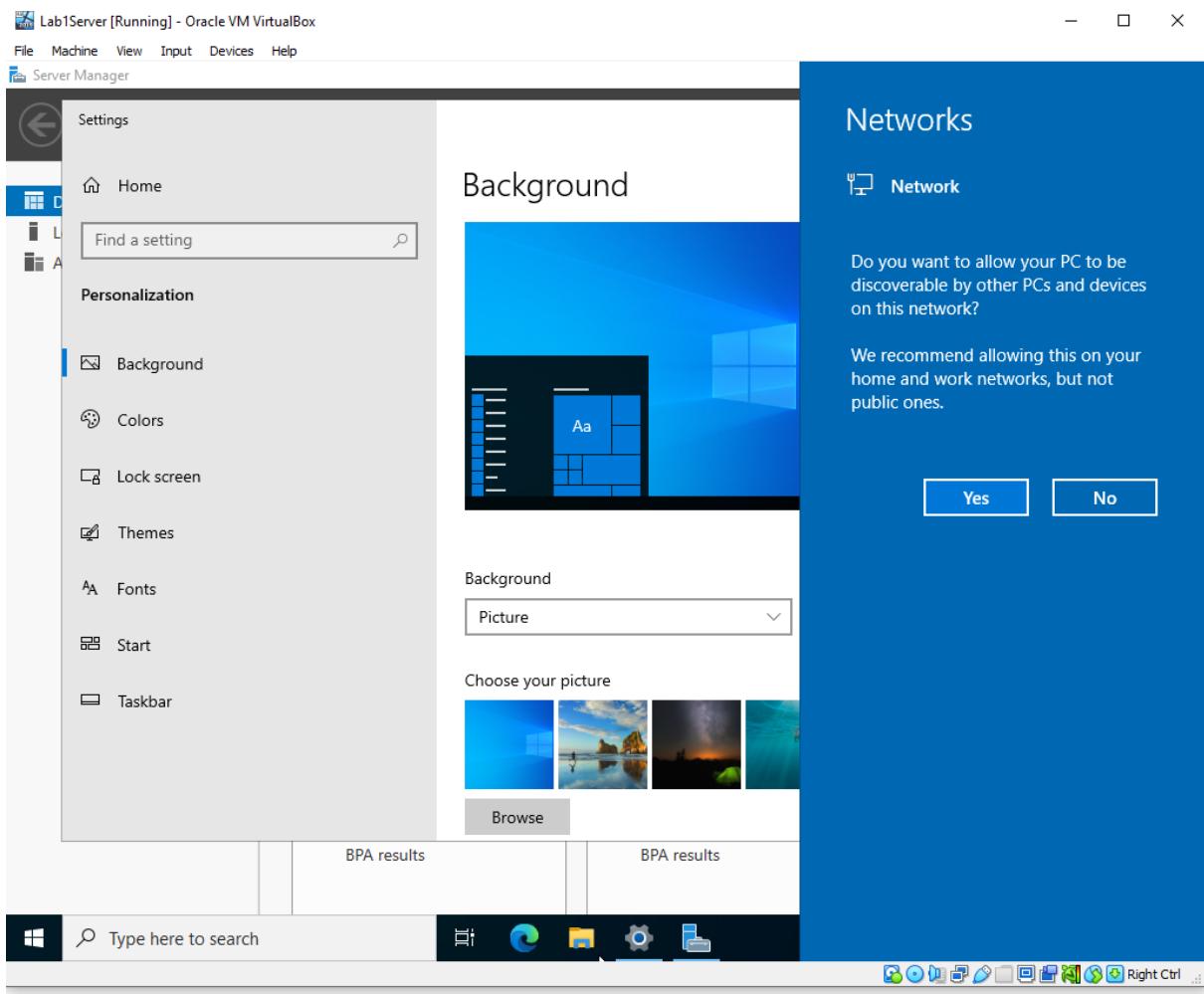






## Configurar el servidor





Server Manager

Server Manager • Local Server

Dashboard Local Server All Servers File and Storage Services

**PROPERTIES**  
For WIN-1JC440BCKKN

Computer name	WIN-1JC440BCKKN	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Download update
		Last checked for updates	Never
Microsoft Defender Firewall	Public: On	Microsoft Defender Antivirus	Real-Time Protection
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific
Network	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00454-40000-01
Operating system version	Microsoft Windows Server 2022 Standard Evaluation	Processors	Intel(R) Core(TM)
Hardware information	Innatek GmbH VirtualBox	Installed memory (RAM)	4 GB
		Total disk space	49.39 GB

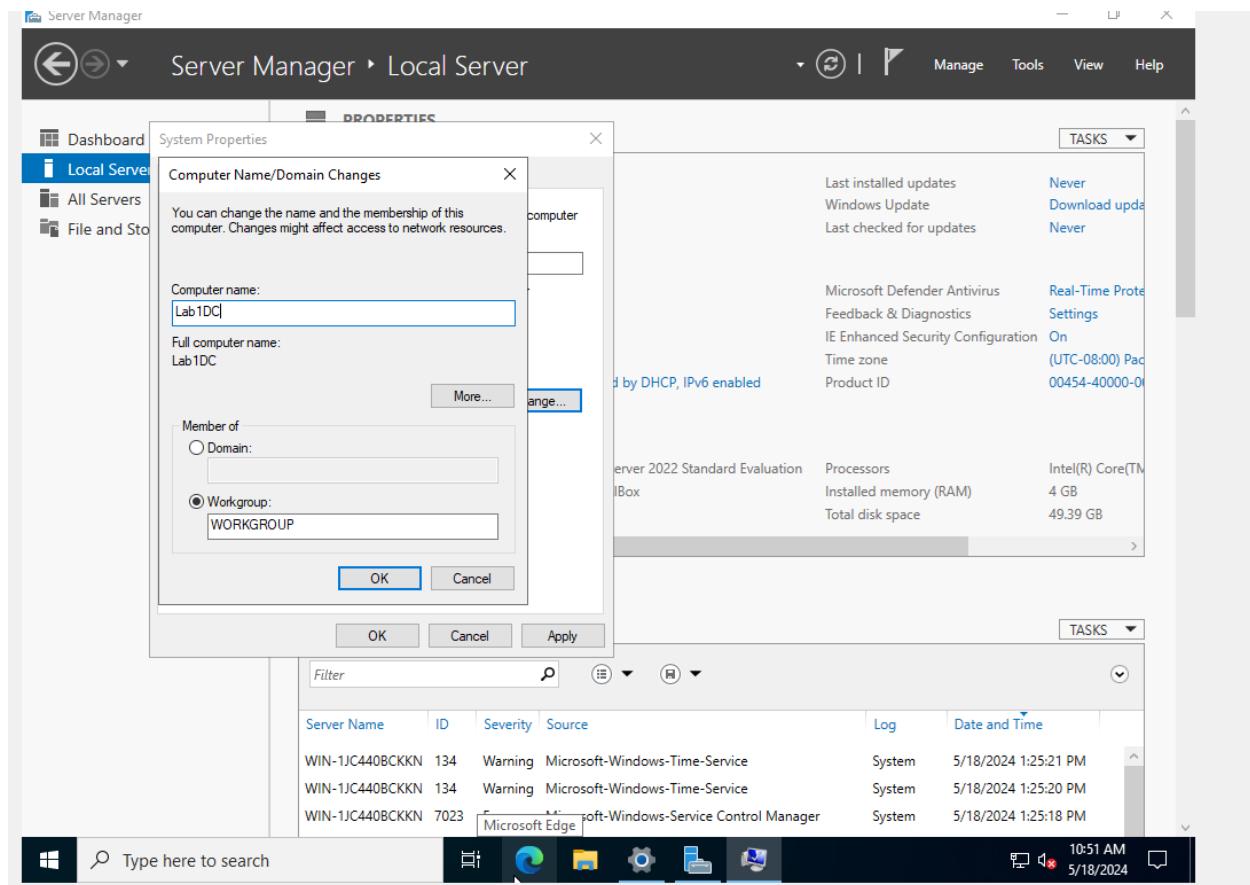
**EVENTS**  
All events | 12 total

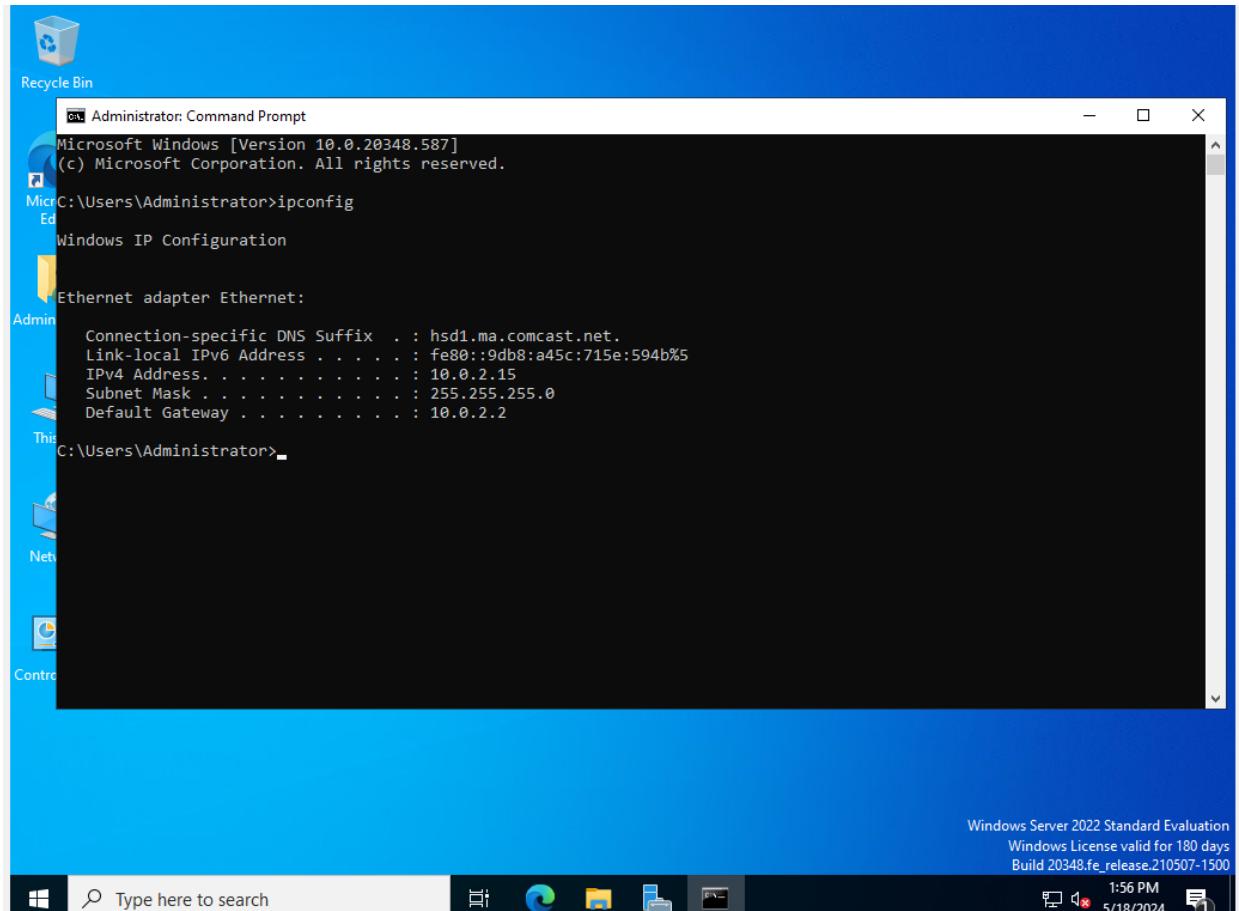
Server Name	ID	Severity	Source	Log	Date and Time
WIN-1JC440BCKKN	134	Warning	Microsoft-Windows-Time-Service	System	5/18/2024 1:25:21 PM
WIN-1JC440BCKKN	134	Warning	Microsoft-Windows-Time-Service	System	5/18/2024 1:25:20 PM
WIN-1JC440BCKKN	7023	Error	Microsoft-Windows-Service Control Manager	System	5/18/2024 1:25:18 PM

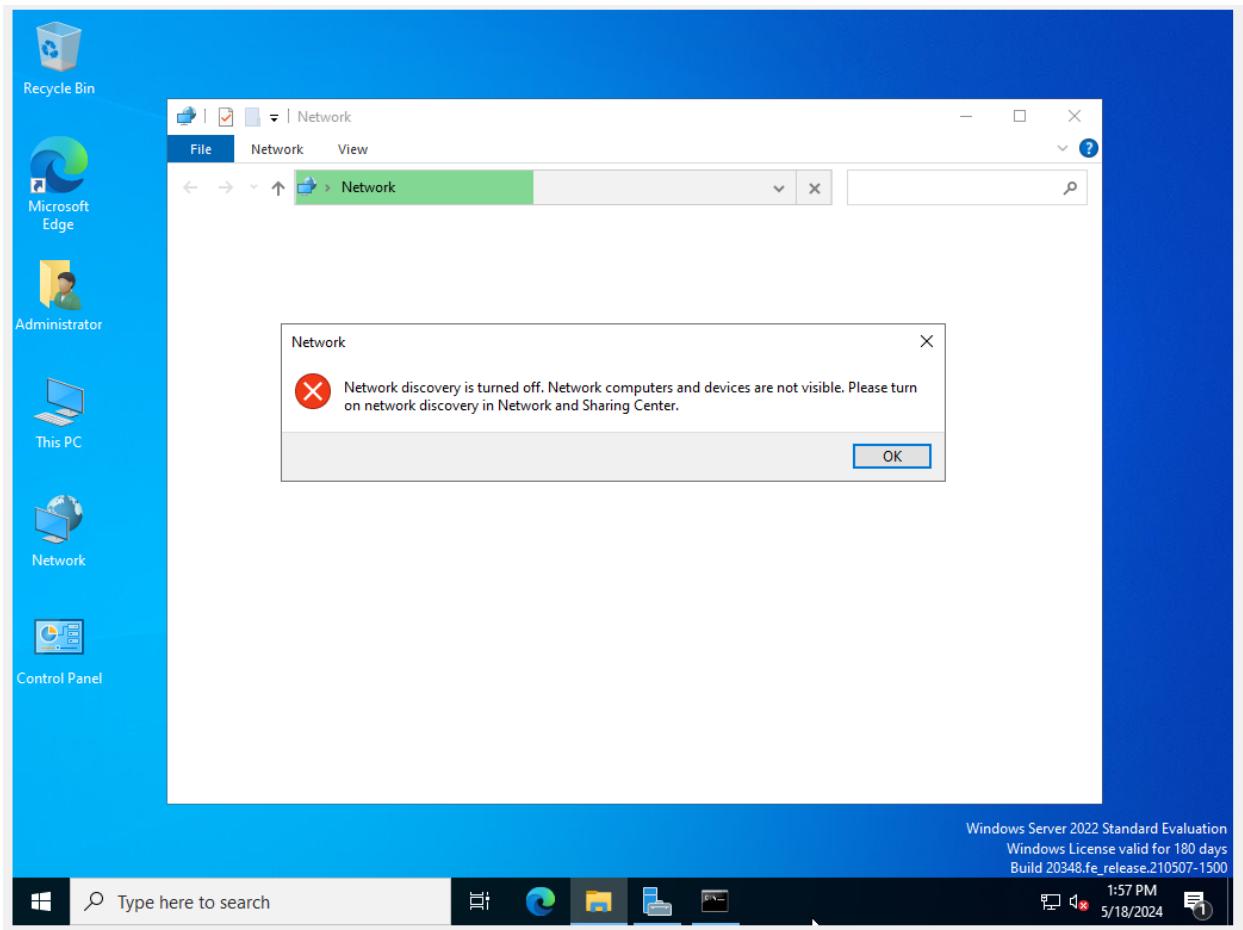
Type here to search

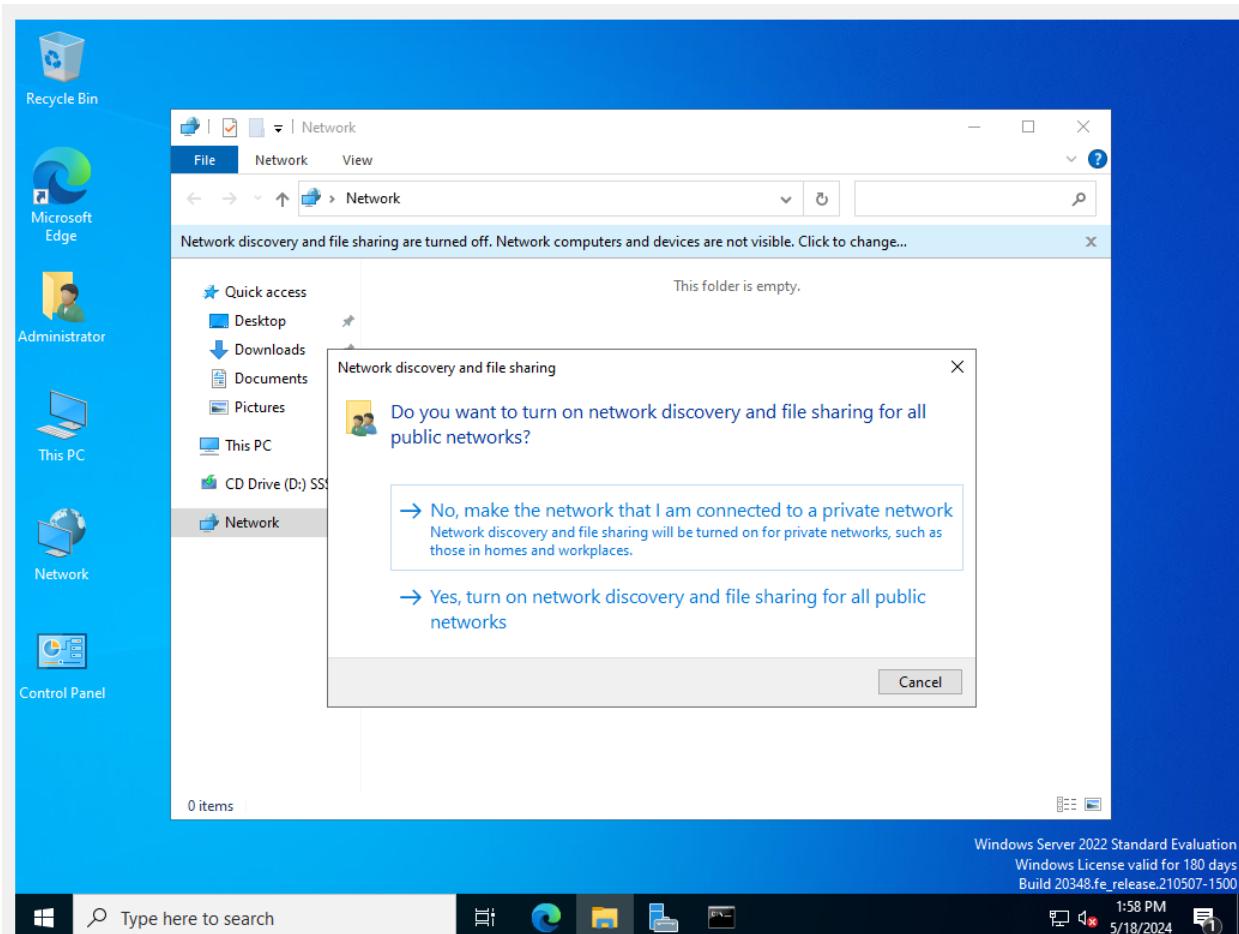
10:50 AM 5/18/2024

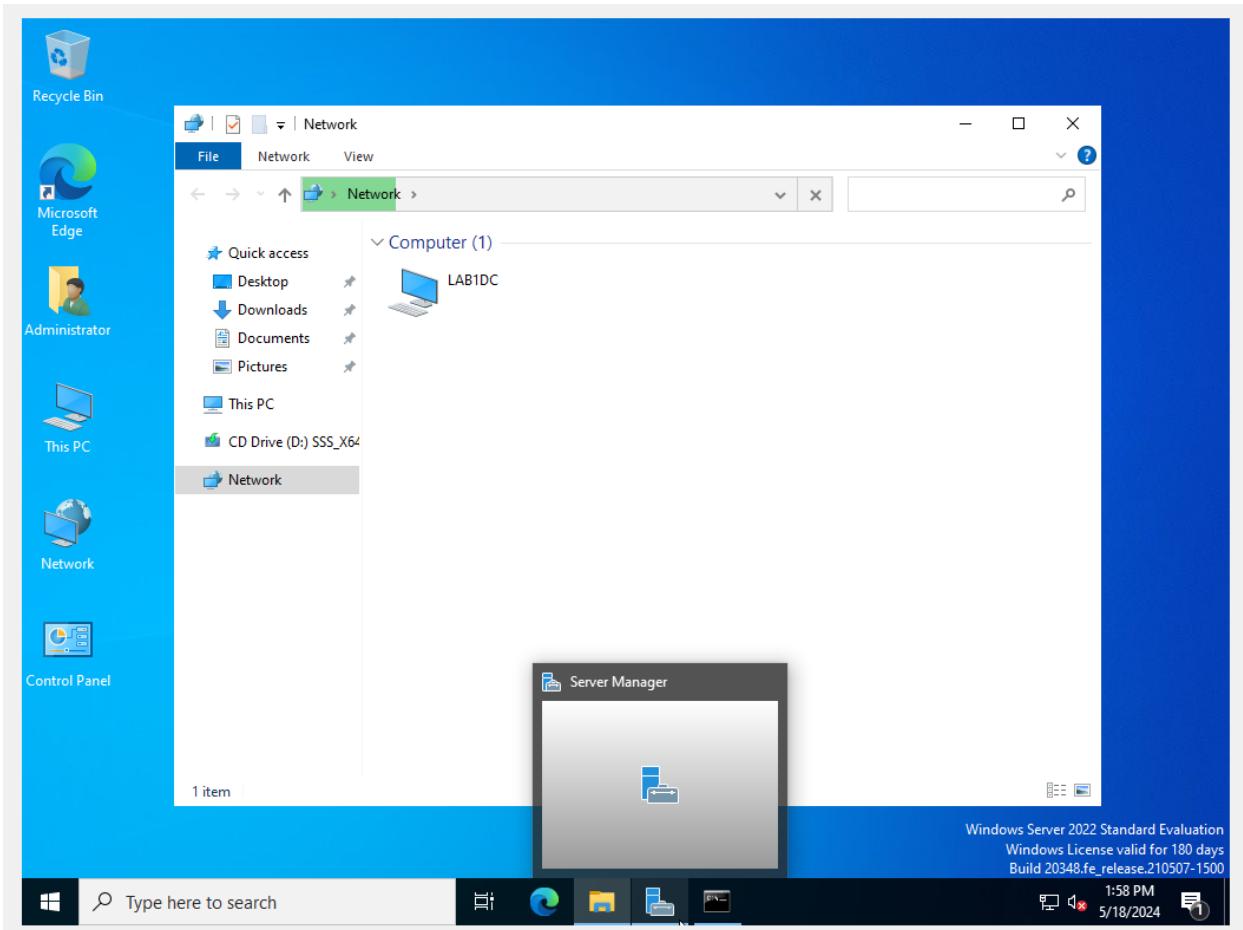
This screenshot shows the Windows Server 2022 Local Server properties and event logs in the Server Manager. The left sidebar shows navigation links: Dashboard, Local Server (which is selected), All Servers, and File and Storage Services. The main area displays the server's properties, including its name (WIN-1JC440BCKKN), workgroup (WORKGROUP), and various system settings like network and security configurations. Below the properties is a table of recent events, showing three entries from the Microsoft-Windows-Time-Service and Microsoft-Windows-Service Control Manager logs. The bottom of the screen features the Windows taskbar with icons for File Explorer, Edge, File History, Settings, Task View, and Start. The system tray shows the date and time (10:50 AM, 5/18/2024).

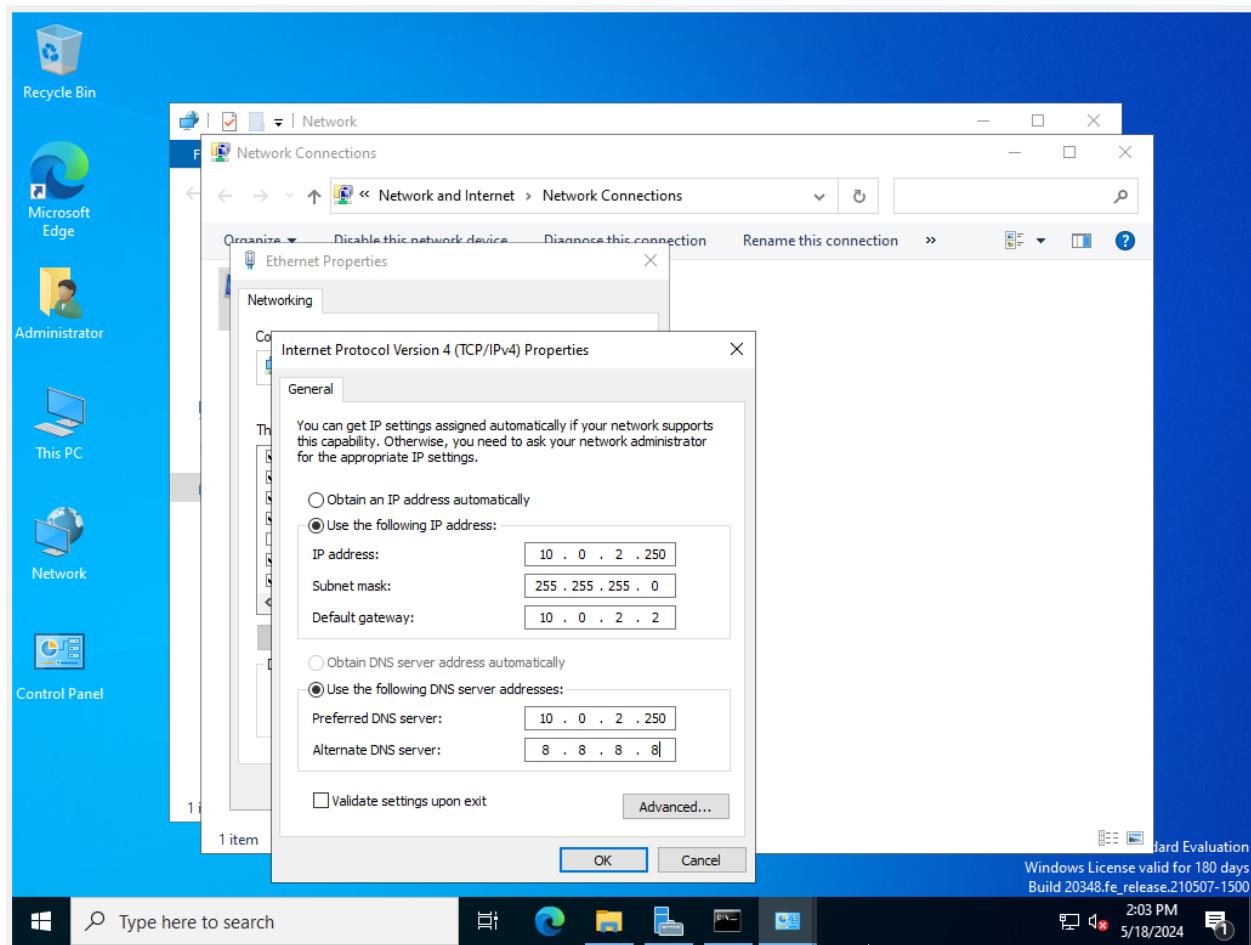




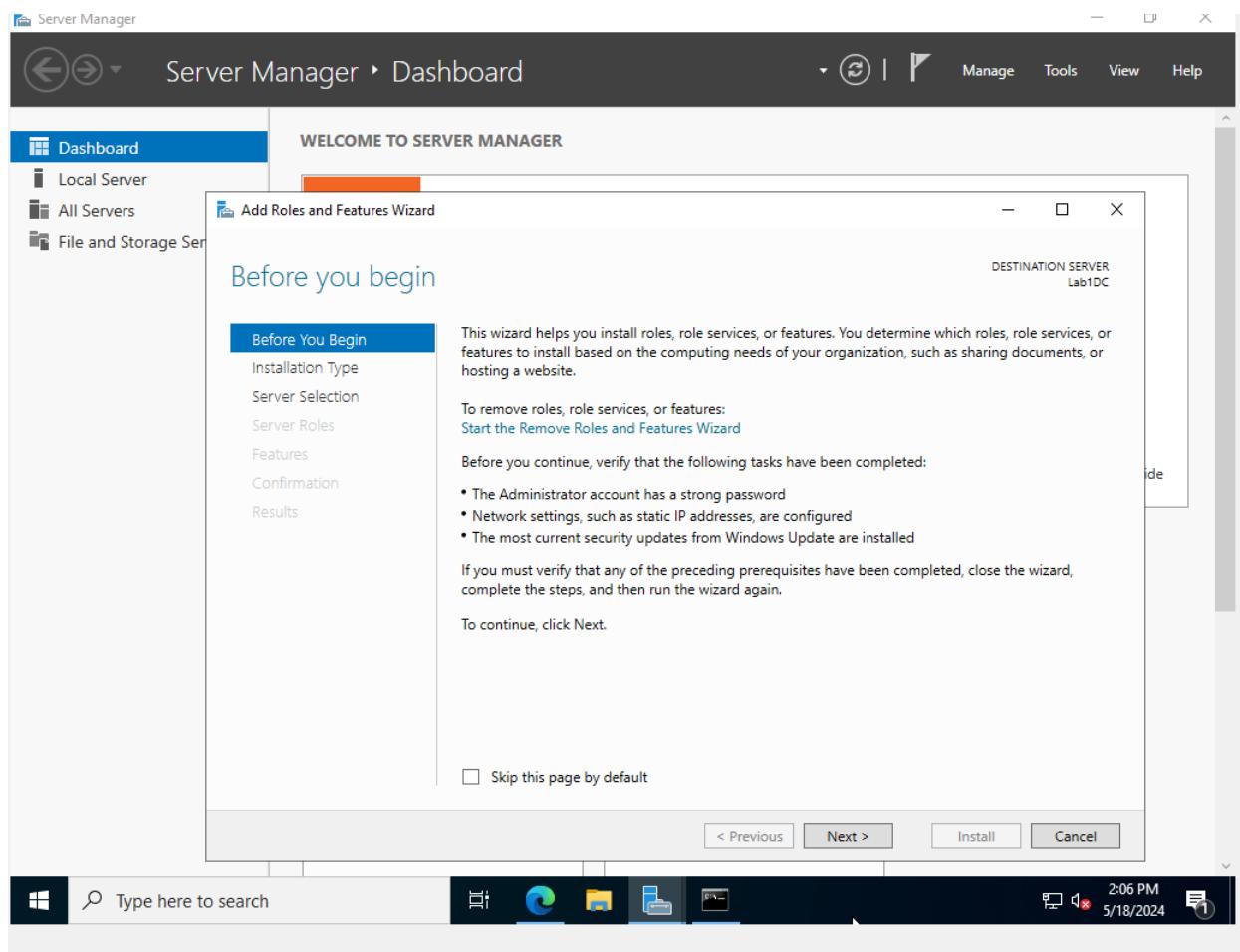


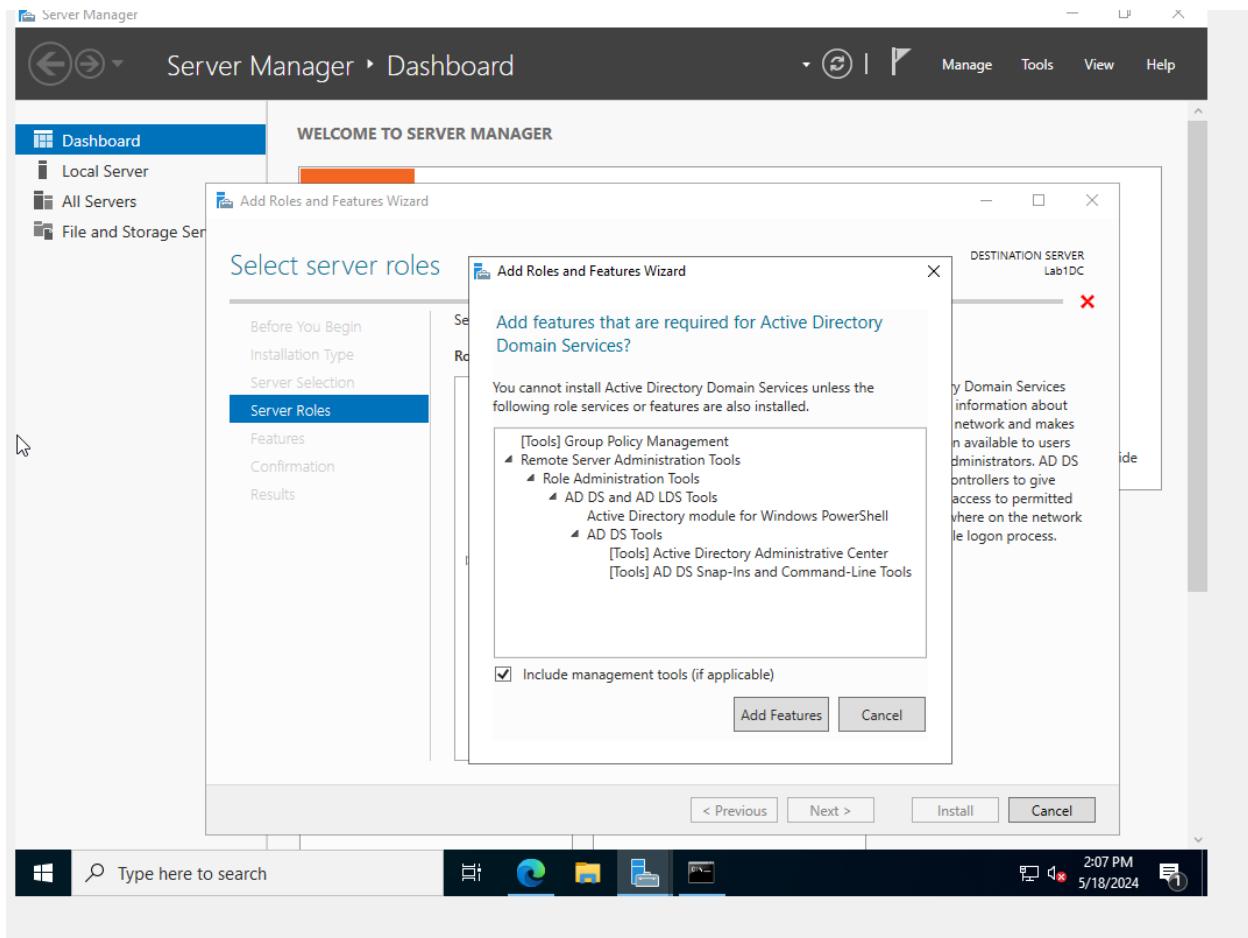


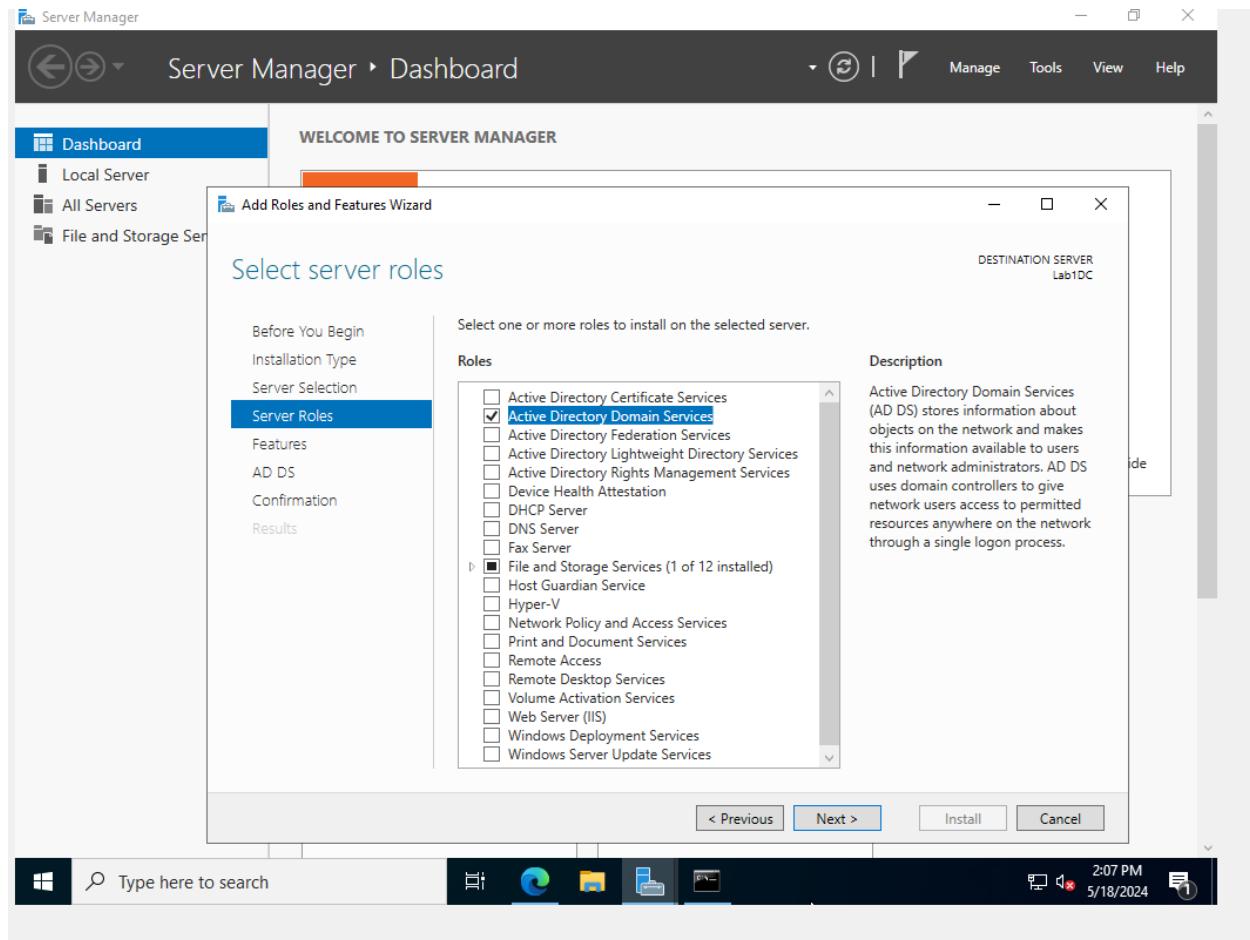


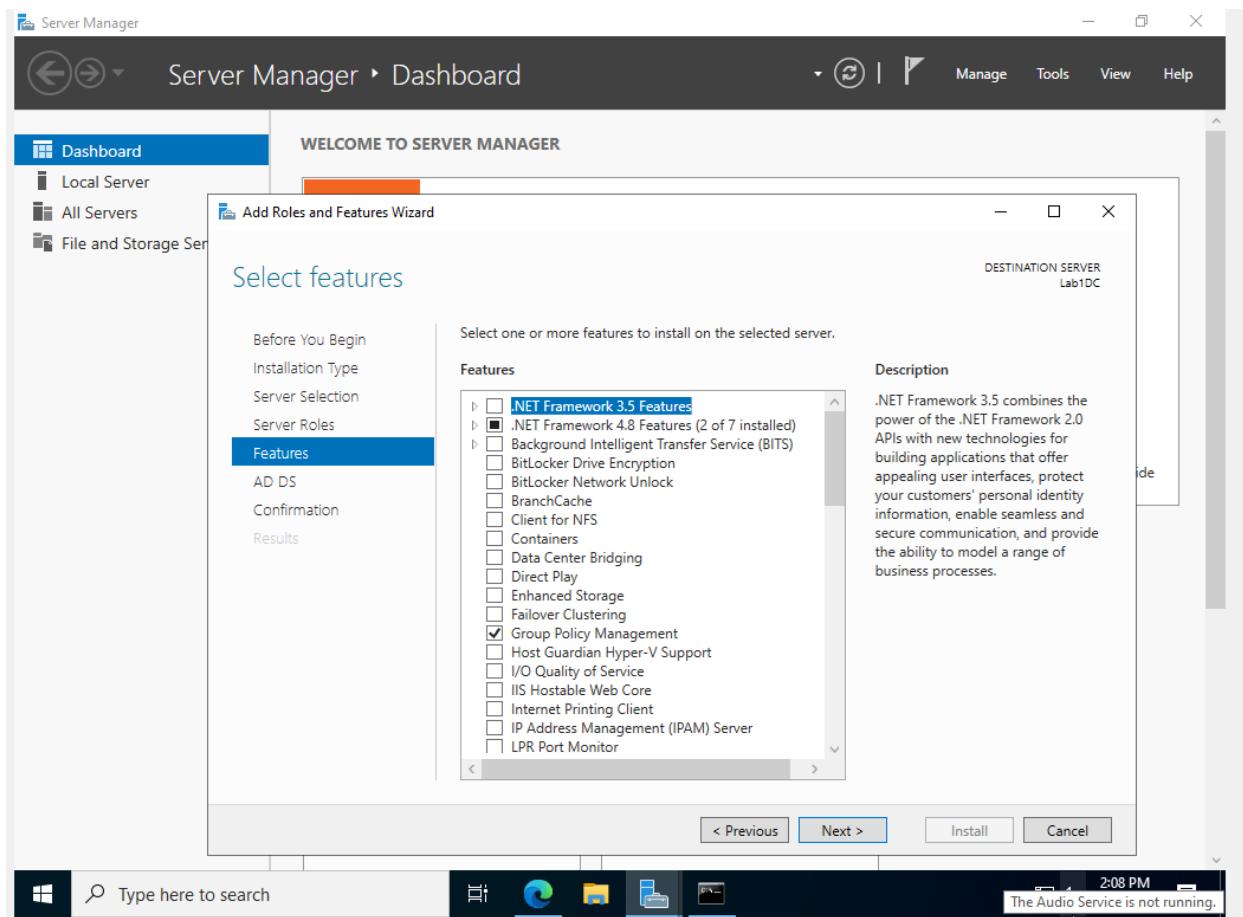


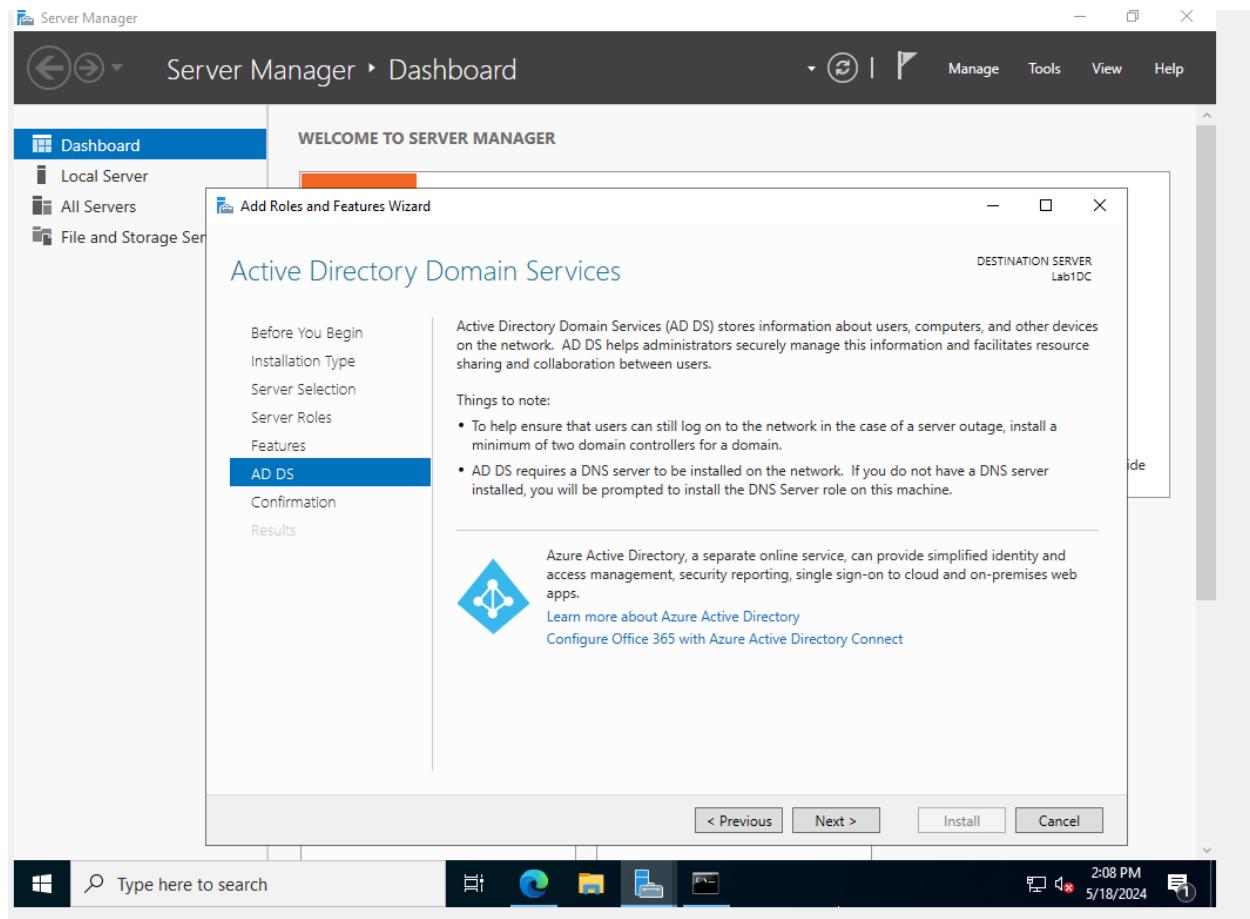
## Convertir en un controlador de dominio

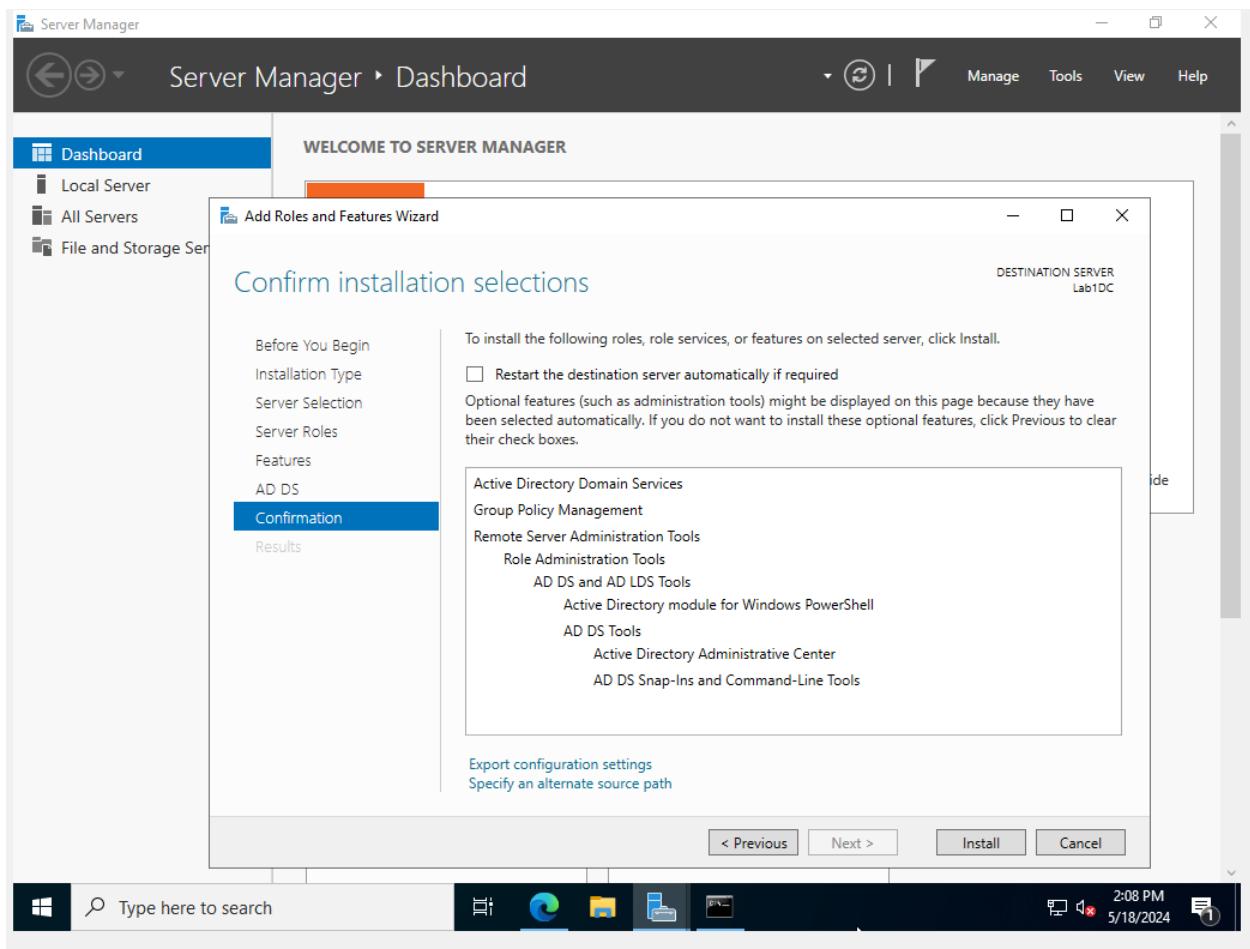


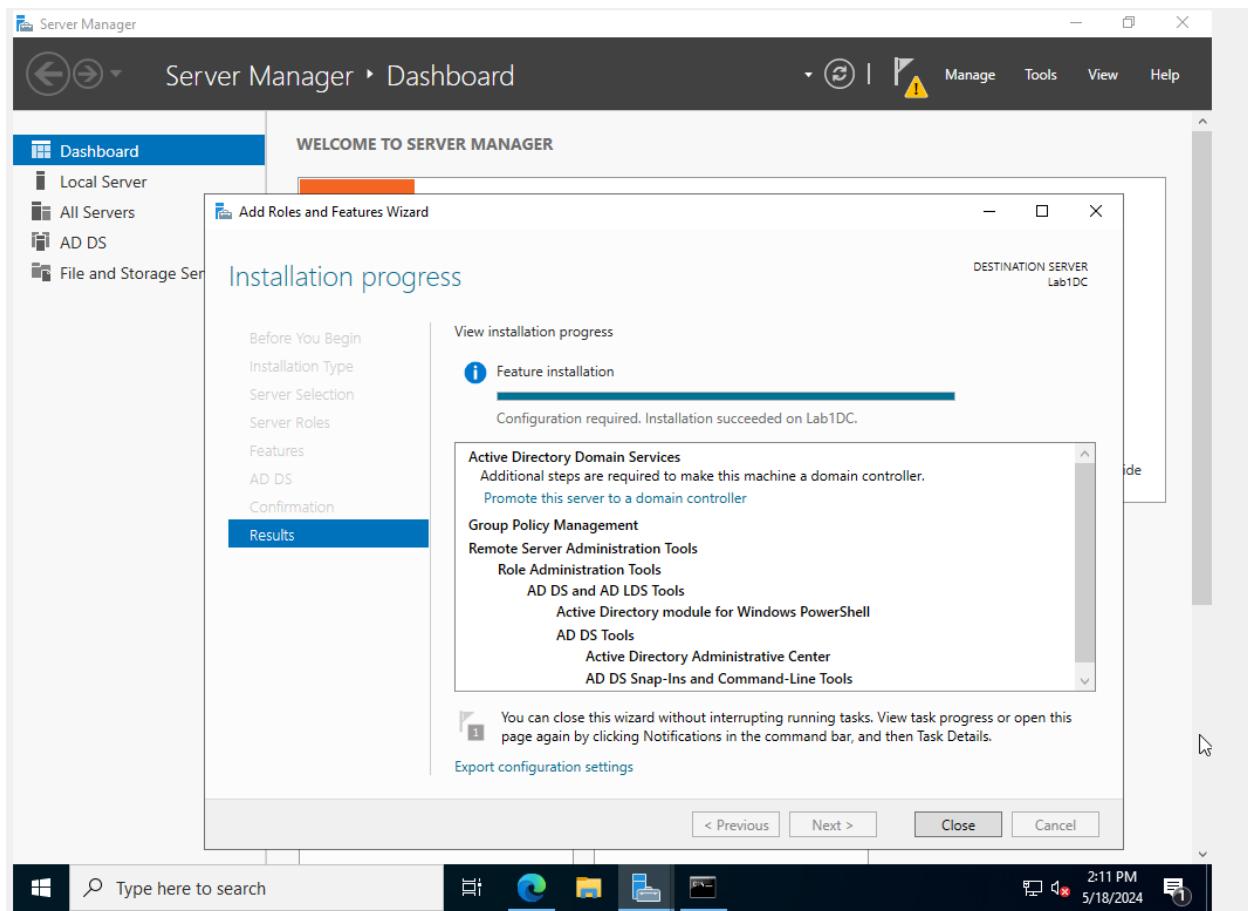


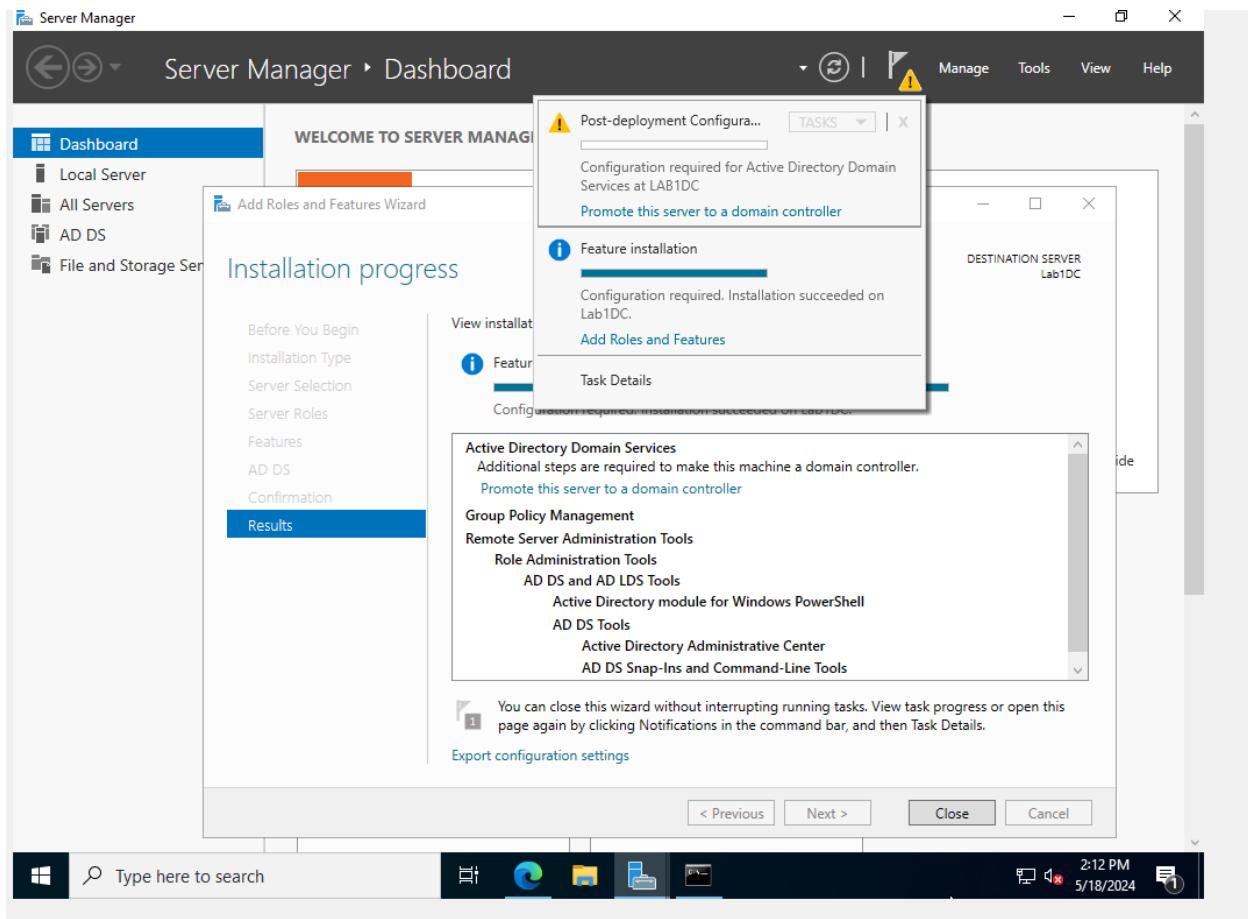


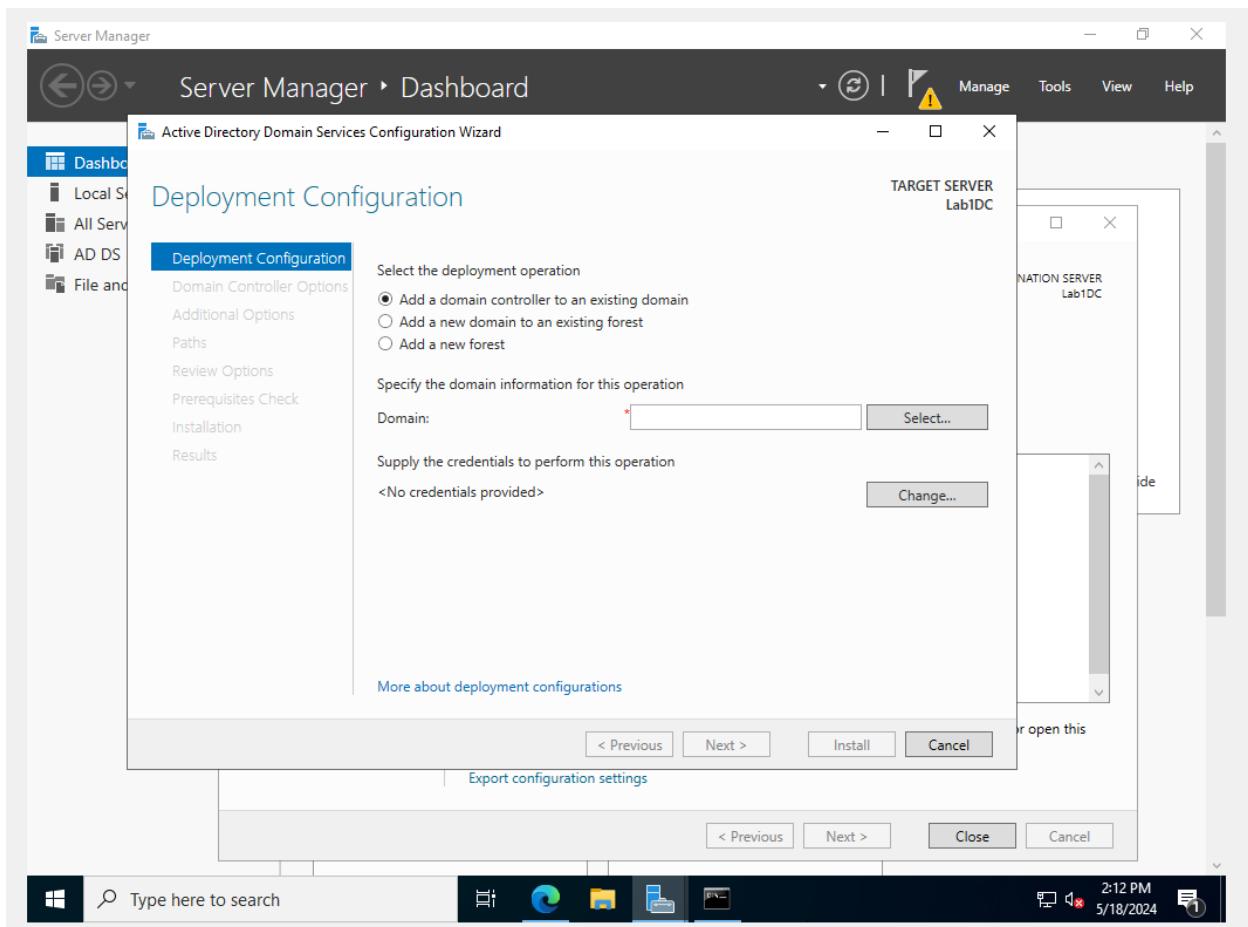


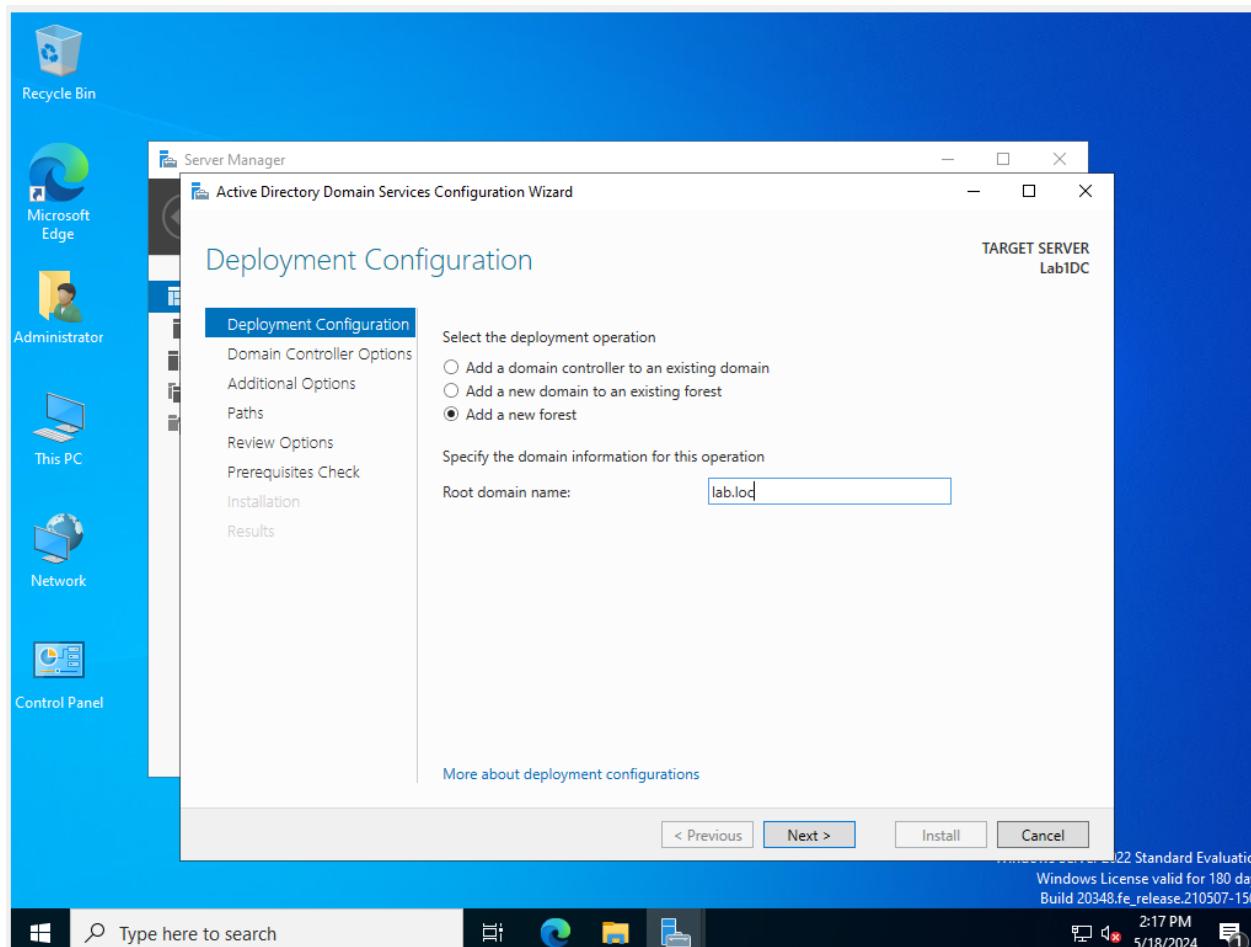


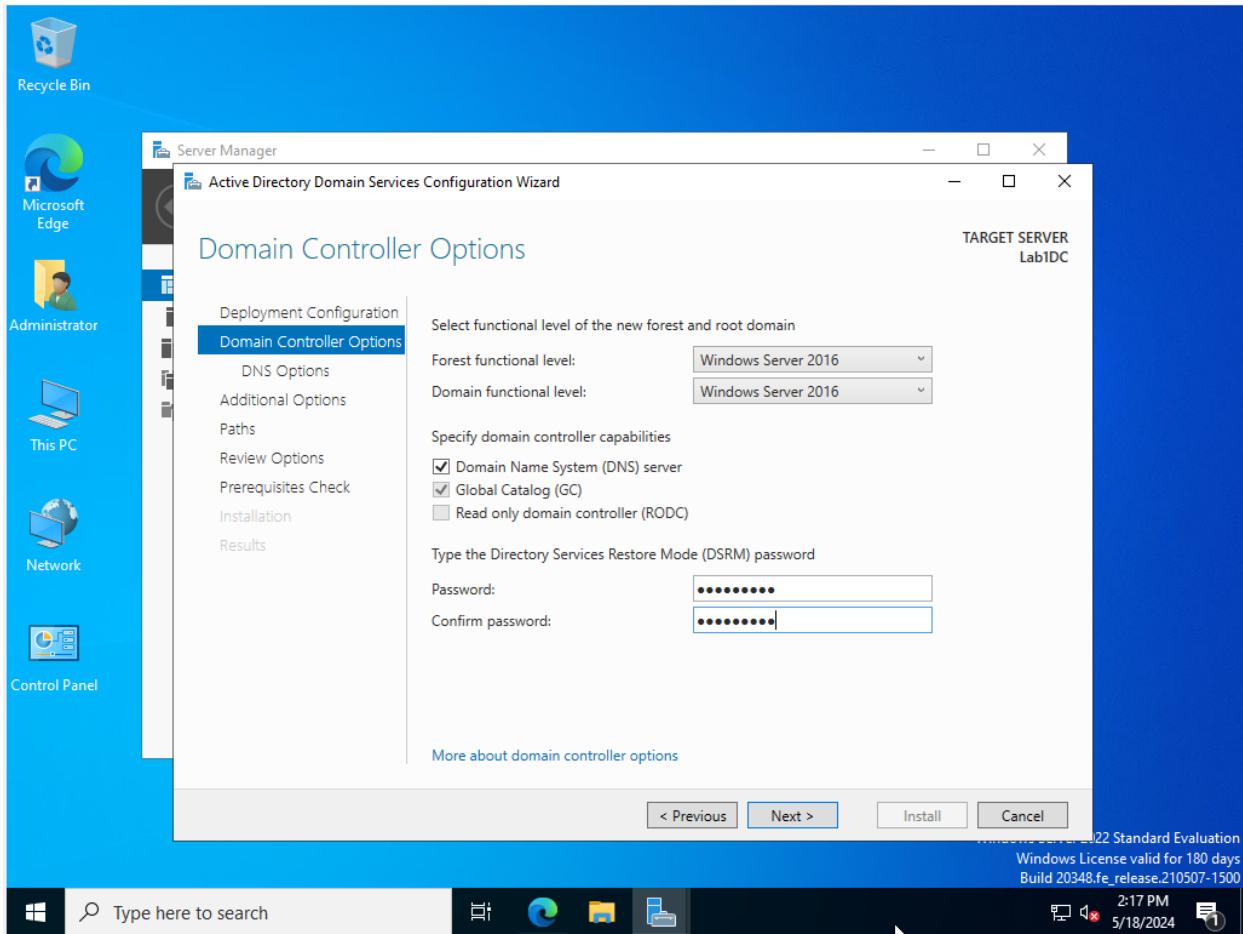


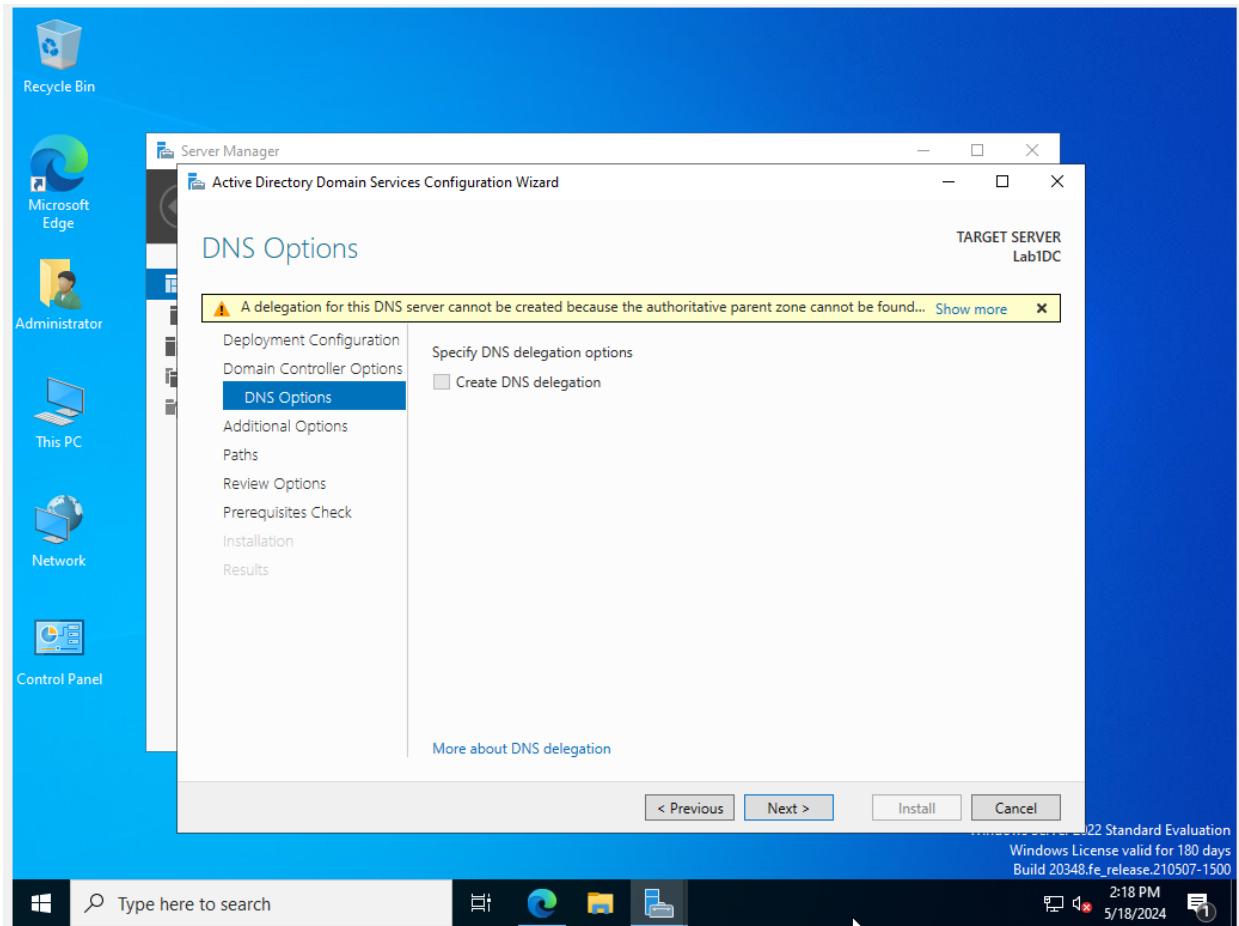










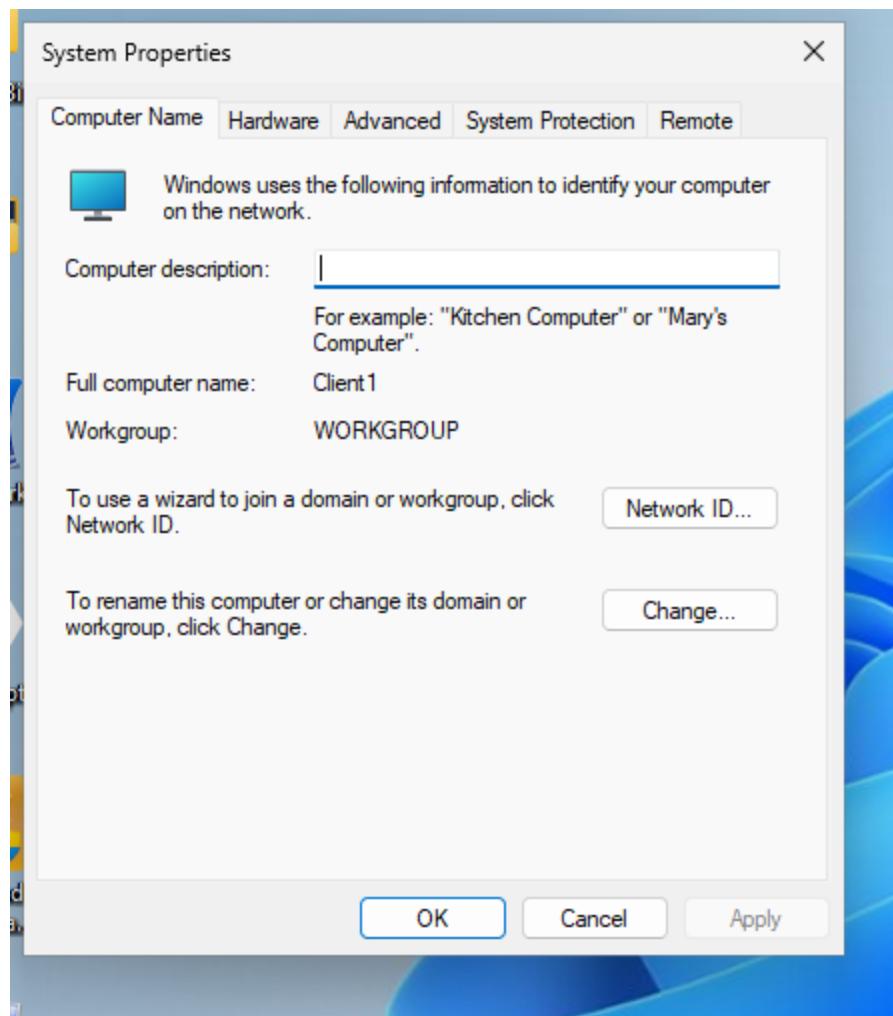


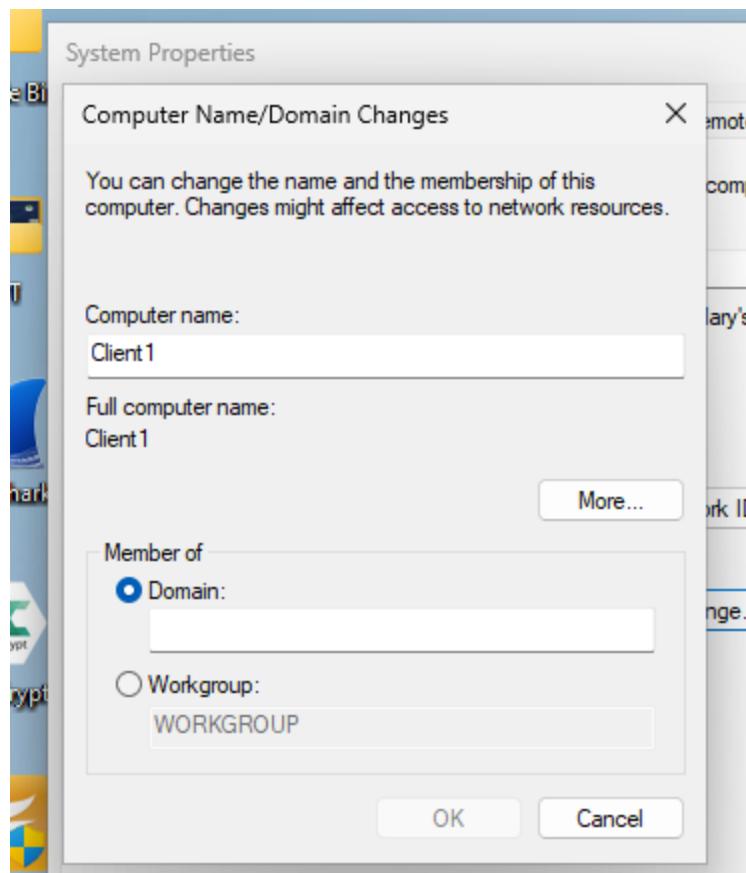
## Agregar Windows 11 como miembro de Dominio

The screenshot shows the Windows Settings application window titled "System > About". On the left sidebar, under the "System" category, the "Windows Update" option is selected. The main content area displays "Device specifications" and "Windows specifications" tables, along with related links like "Domain or workgroup", "System protection", and "Advanced system settings". A "Related" section at the bottom includes links for "Product key and activation", "File Explorer", and "Remote desktop".

Device name	Client1
Processor	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz 3.60 GHz
Installed RAM	7.98 GB
Device ID	72BF2BA4-C6D9-4593-B525-CE16740F23E1
Product ID	00330-80000-00000-AA458
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Edition	Windows 11 Pro
Version	23H2
Installed on	2/6/2024
OS build	22631.3447
Experience	Windows Feature Experience Pack 1000.22688.1000.0

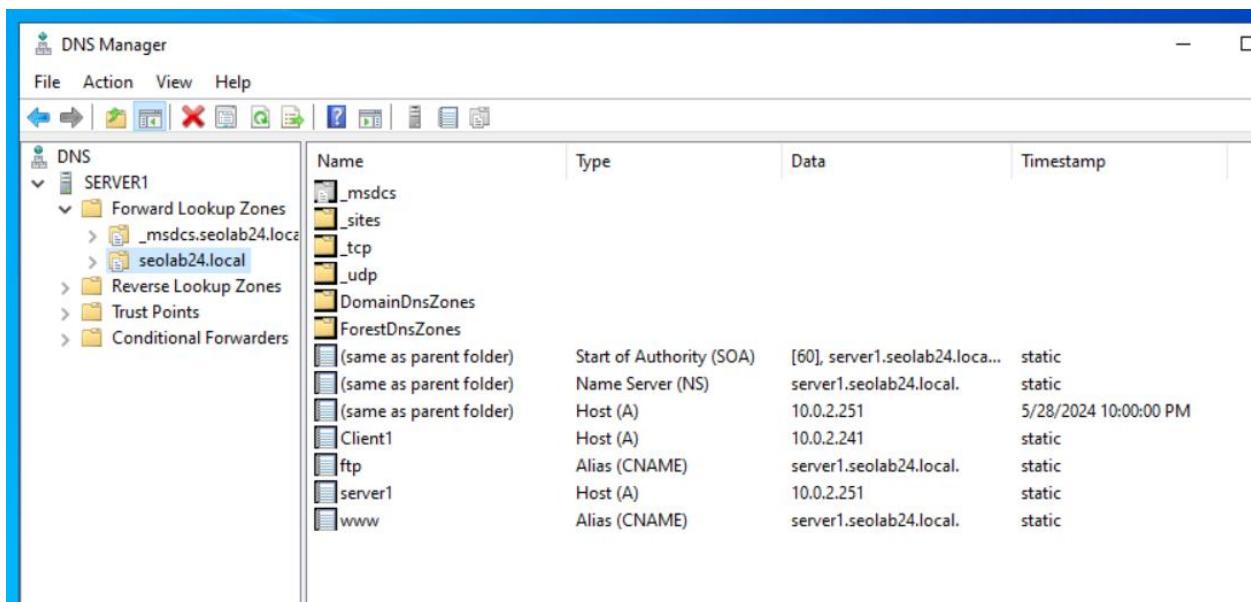




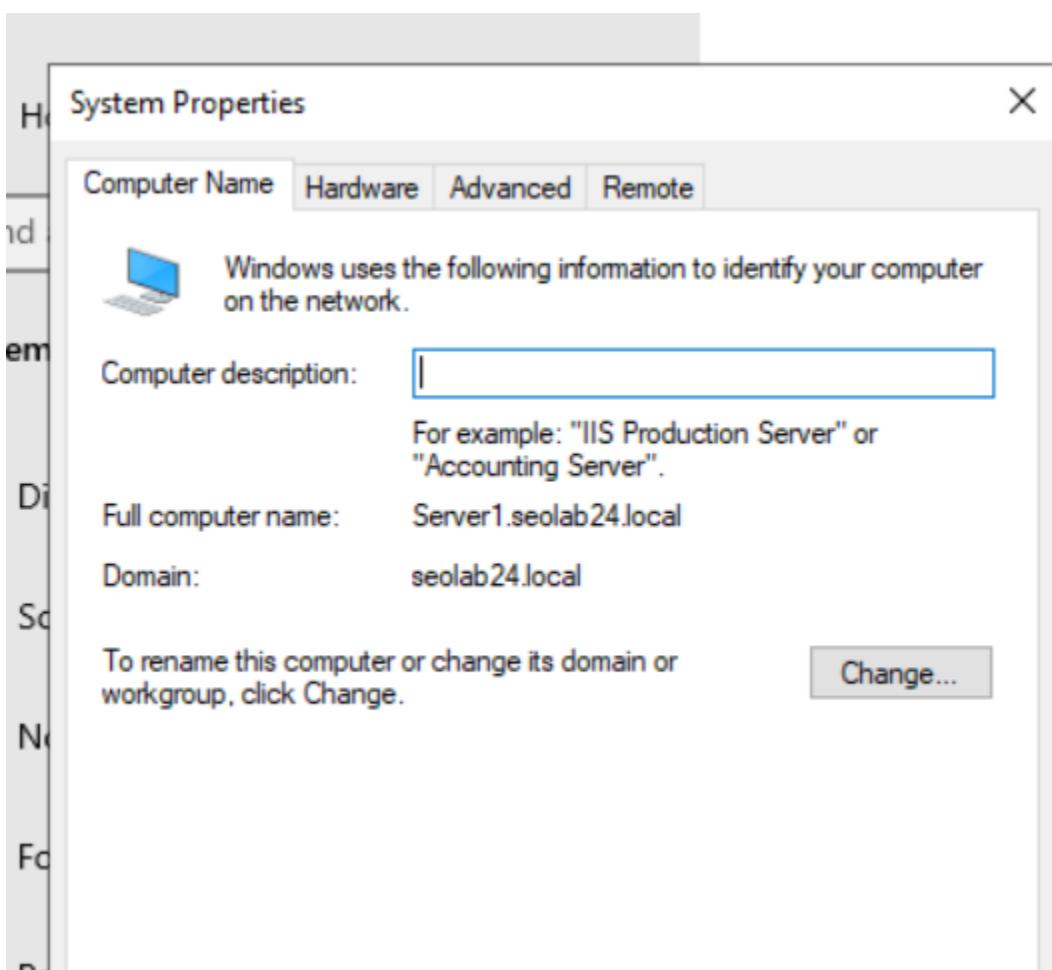
The screenshot shows the Windows Settings application window. The left sidebar lists various settings categories: Home, System, Bluetooth & devices, Network & internet (which is selected and highlighted in blue), Personalization, Apps, Accounts, Time & language, Gaming, Accessibility, Privacy & security, and Windows Update. A search bar at the top says "Find a setting". The main content area is titled "Network & internet > Ethernet". It displays network configuration details for an Ethernet connection, including IP assignment (Manual), IPv4 address (10.0.2.241), IPv4 mask (255.255.255.0), and IPv4 gateway (10.0.2.1). It also shows DNS server assignment (Manual), IPv4 DNS servers (10.0.2.251 (Unencrypted) 8.8.8.8 (Unencrypted)), and link speed (1000/1000 Mbps). The "Metered connection" toggle switch is set to "Off". A note says "Some apps might work differently to reduce data usage when you're connected to this network".

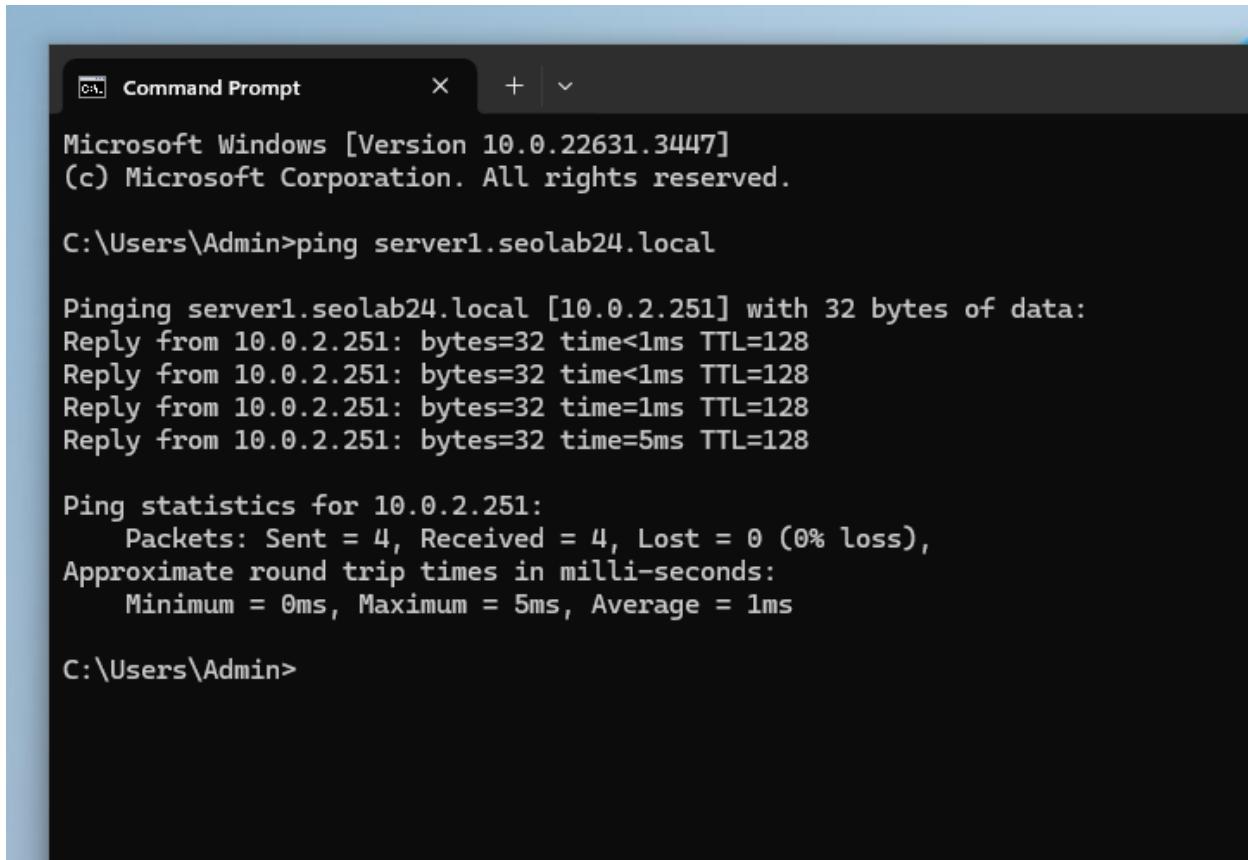
DNS Manager

File Action View Help



	Name	Type	Data	Timestamp
	_msdcs	Start of Authority (SOA)	[60], server1.seolab24.local...	static
	_sites	Name Server (NS)	server1.seolab24.local.	static
	_tcp	Host (A)	10.0.2.251	5/28/2024 10:00:00 PM
	_udp	Host (A)	10.0.2.241	static
	DomainDnsZones	Alias (CNAME)	server1.seolab24.local.	static
	ForestDnsZones	Host (A)	10.0.2.251	static
	(same as parent folder)	Alias (CNAME)	server1.seolab24.local.	static
	(same as parent folder)	Host (A)	10.0.2.251	static
	Client1	Host (A)	10.0.2.241	static
	ftp	Host (A)	10.0.2.251	static
	server1	Host (A)	10.0.2.251	static
	www	Alias (CNAME)	server1.seolab24.local.	static





```
Command Prompt      X + ^ Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping server1.seolab24.local

Pinging server1.seolab24.local [10.0.2.251] with 32 bytes of data:
Reply from 10.0.2.251: bytes=32 time<1ms TTL=128
Reply from 10.0.2.251: bytes=32 time<1ms TTL=128
Reply from 10.0.2.251: bytes=32 time=1ms TTL=128
Reply from 10.0.2.251: bytes=32 time=5ms TTL=128

Ping statistics for 10.0.2.251:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 1ms

C:\Users\Admin>
```

## Herramientas adicionales

### Instalación de Nessus

<https://www.tenable.com/products/nessus/nessus-essentials>



Platform Products Solutions Resources Partners Support Company

Try Buy



## Tenable Nessus® Essentials

As part of the Tenable Nessus family, Tenable Nessus Essentials allows you to scan your environment (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Essentials does not allow you to perform compliance checks or content audits, Live Results or use the Nessus virtual appliance. If you require these additional features, please purchase a [Tenable Nessus Professional](#) subscription.

Using Nessus Essentials for education? Register for Nessus Essentials through the [Tenable for Education](#) program to get started.

Interested in learning how to use Nessus? Our [on-demand course](#) enables the student, through a series of targeted videos, to develop the building blocks for effective use of the Nessus vulnerability assessment solution. From asset discovery to vulnerability assessment to compliance, participants will learn to effectively utilize Nessus in a variety of business use cases. [Learn more](#).



Nessus is the **GOLD STANDARD** for vulnerability assessments

[TRY NESSUS FREE FOR 7 DAYS](#)

TRY NOW

### Register for an Activation Code

First Name Last Name

Business Email

Check to receive updates from Tenable  
Tenable will only process your personal data in accordance with its [Privacy Policy](#).

Get Started



Platform Products Solutions Resources Partners Support Company

Try Buy



## Thank You for Registering for Nessus Essentials!

Check Your Email for the Activation Code

Thank you for registering for Nessus® Essentials. An email containing your activation code has been sent to you at the email address you provided.

### Download Nessus

To download Nessus, visit the Nessus Download page.

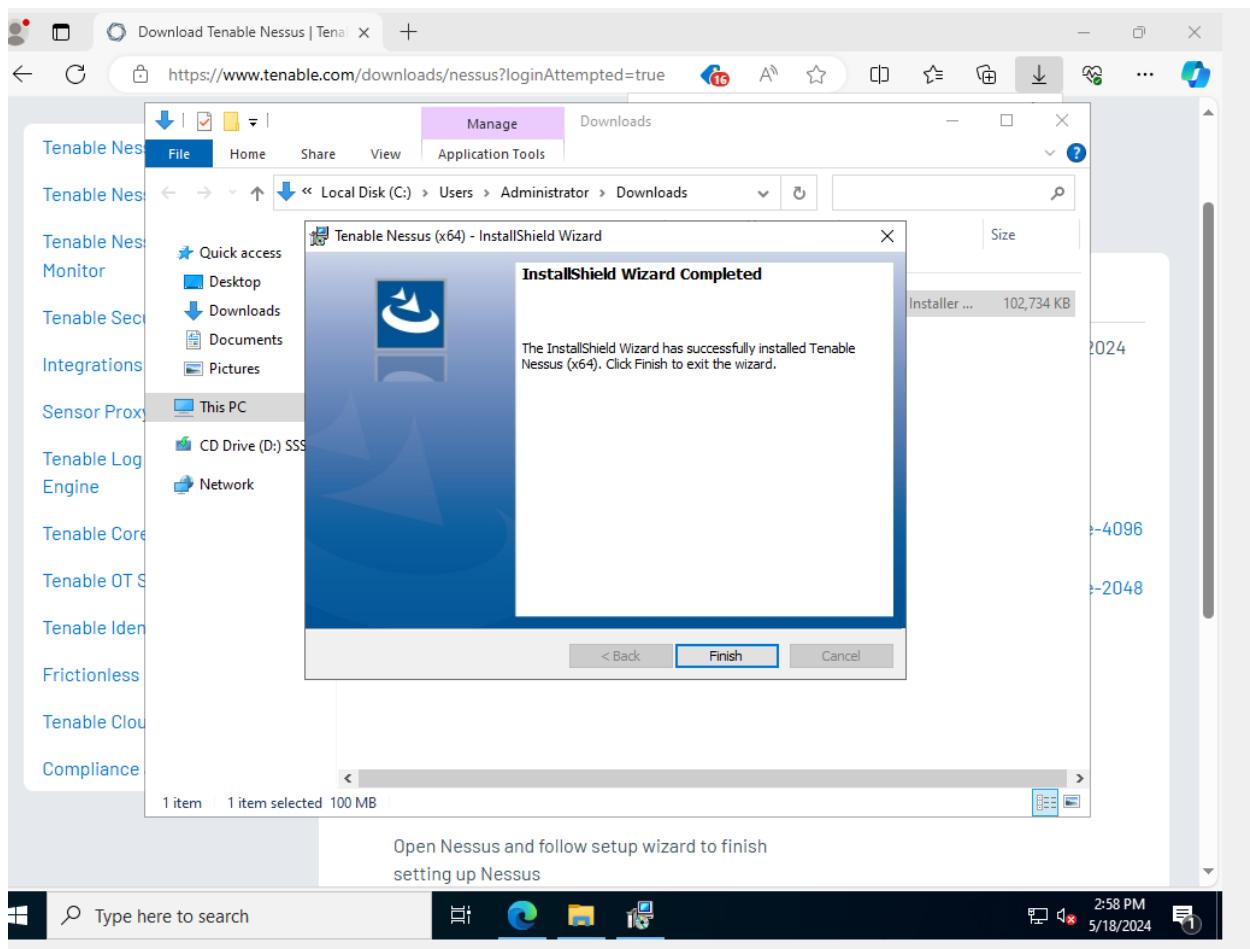
Download

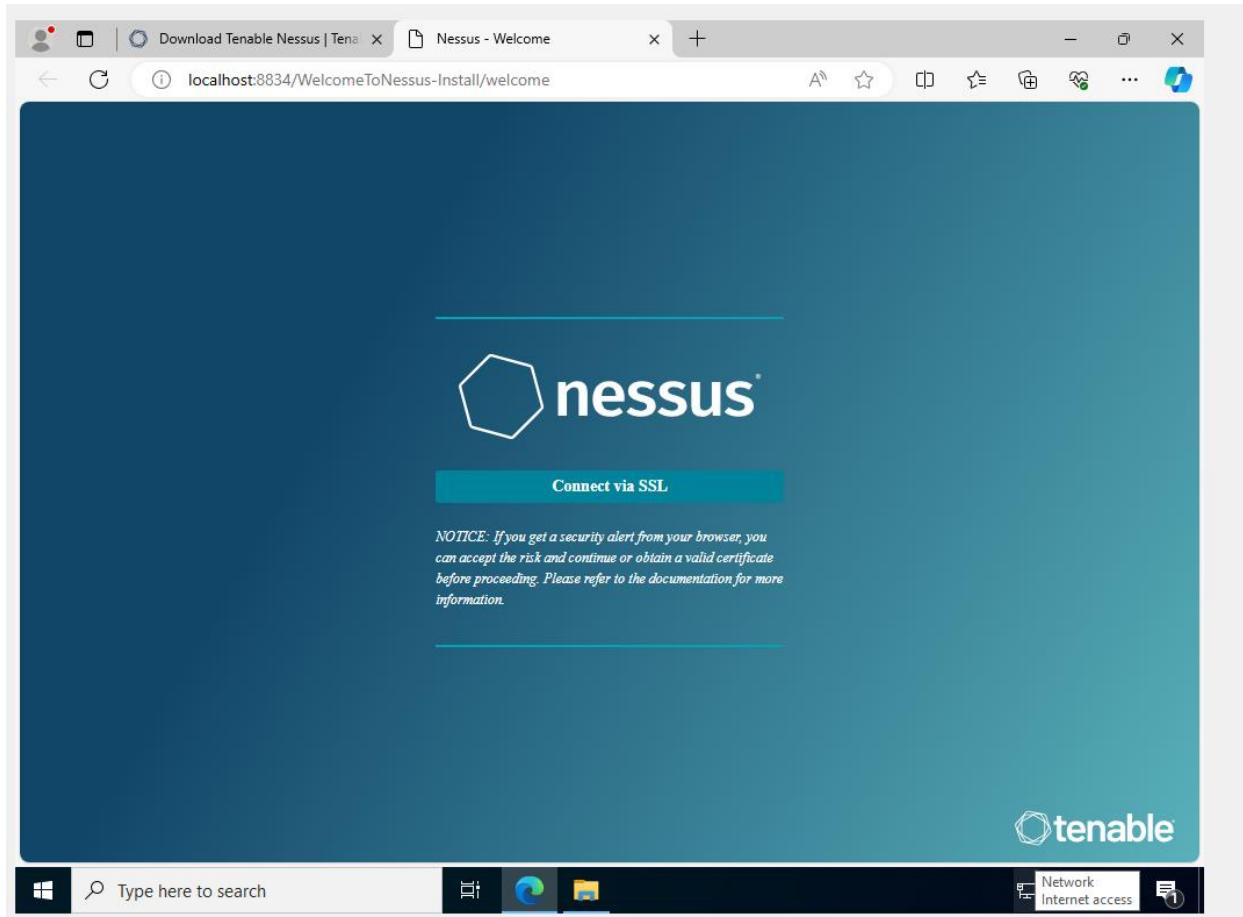
Suggested reading for you

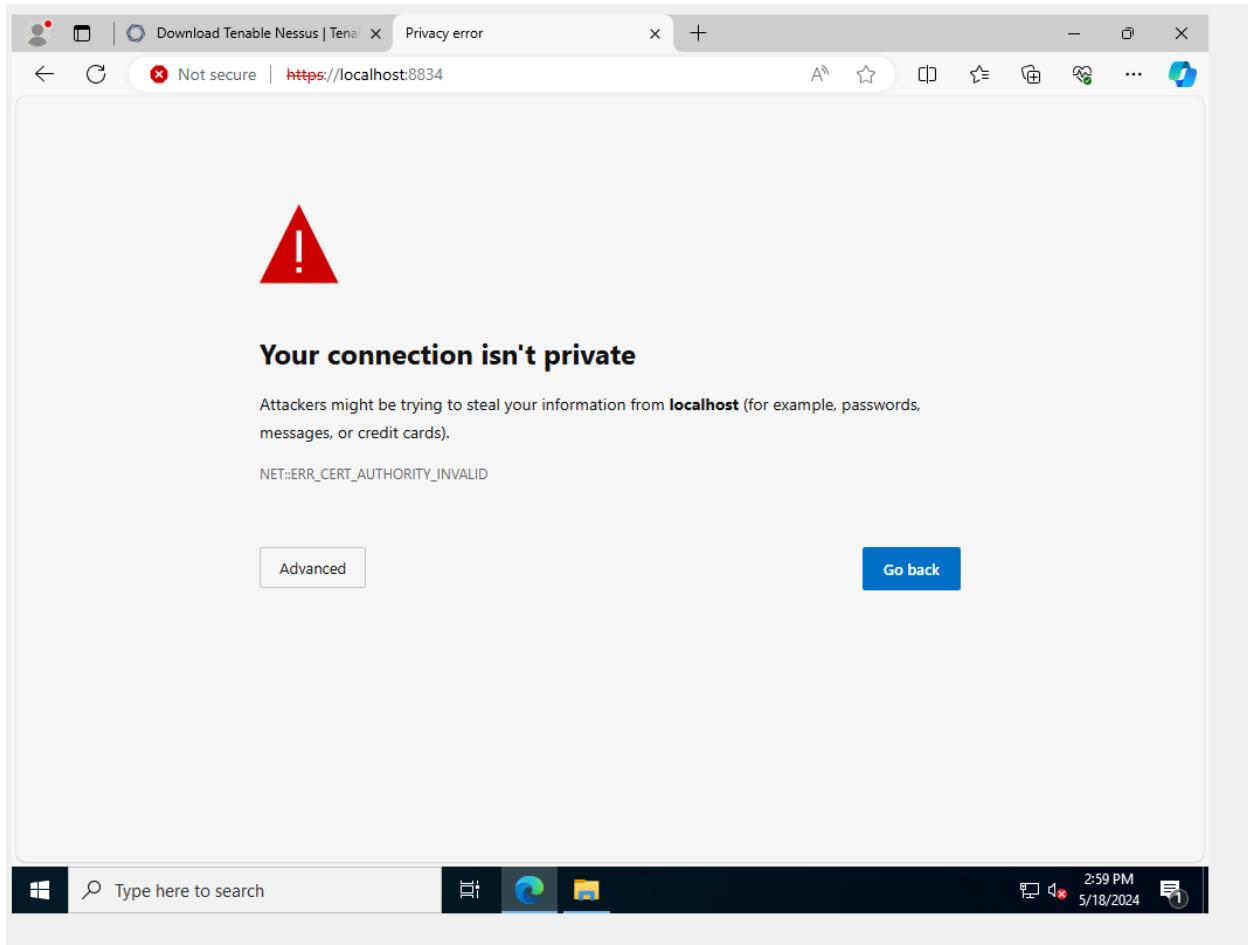


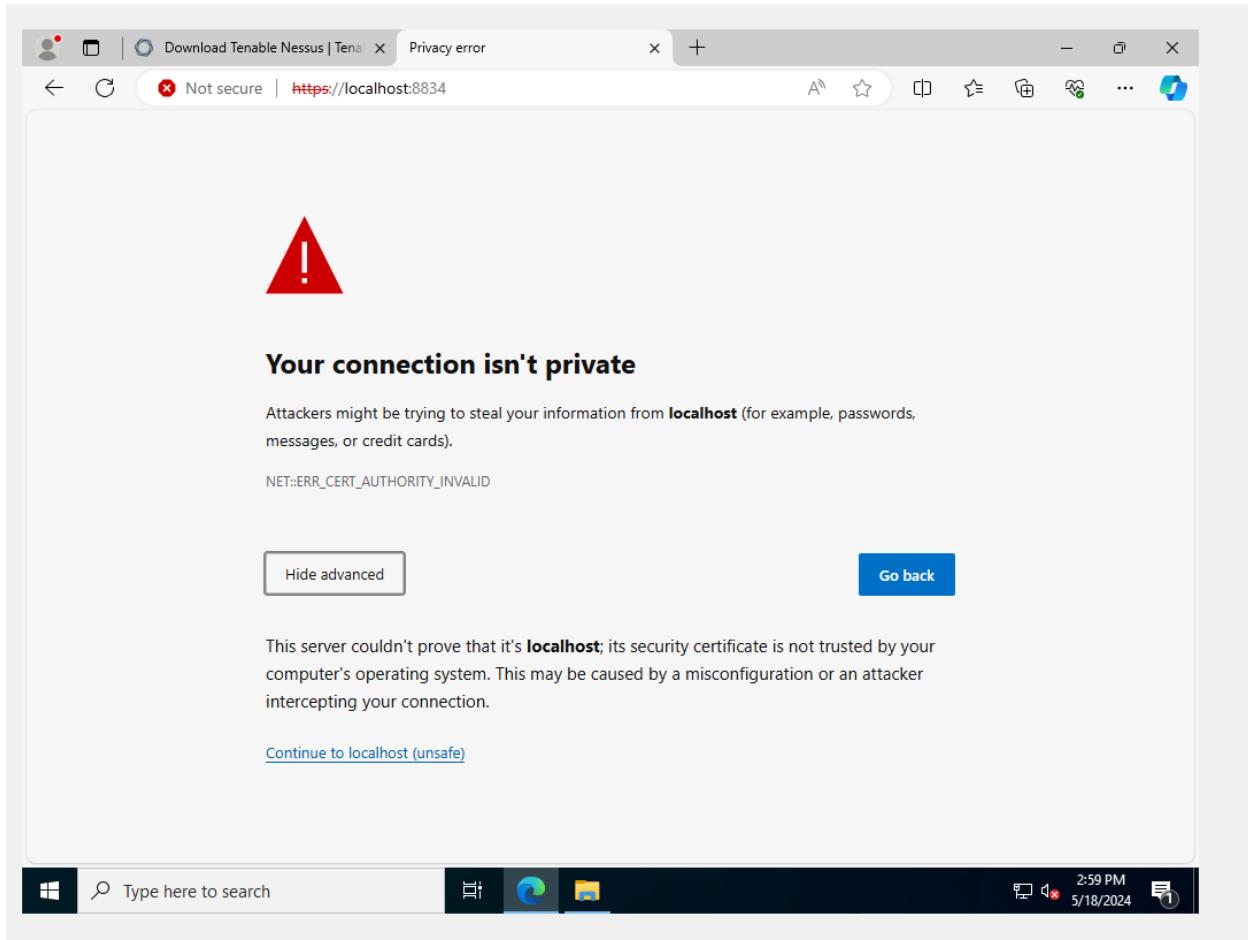
Hey there! our site toc

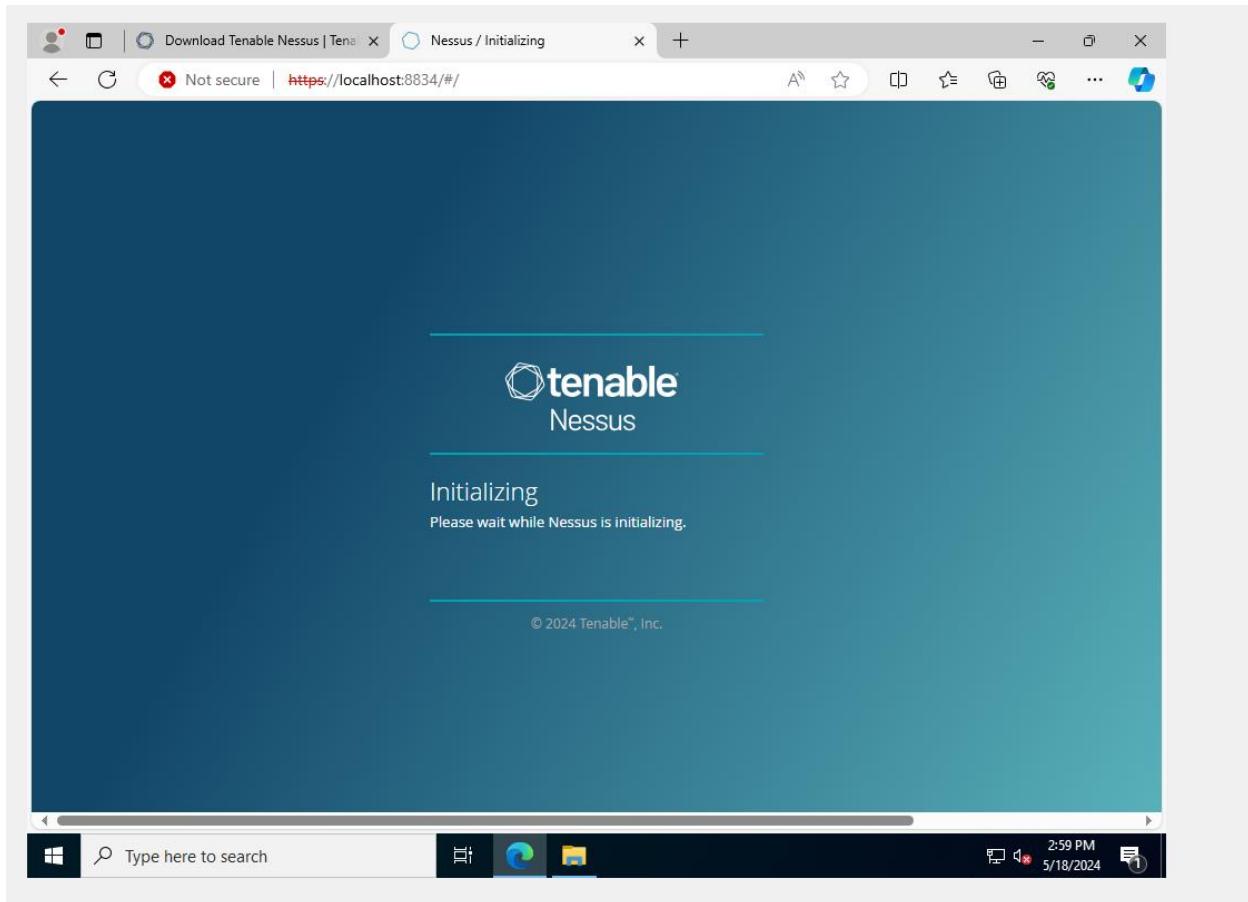
The screenshot shows a web browser window with the URL <https://www.tenable.com/downloads/nessus?loginAttempted=true>. The page is titled "Tenable Nessus" and displays instructions for "Download and Install Nessus". On the left, a sidebar lists various Tenable products: Tenable Nessus, Tenable Nessus Agent, Tenable Nessus Network Monitor, Tenable Security Center, Integrations, Sensor Proxy, Tenable Log Correlation Engine, Tenable Core, Tenable OT Security, Tenable Identity Exposure, Frictionless, Tenable Cloud Security, and Compliance & Audit Files. The main content area has two sections: "Choose Download" (Version: Nessus - 10.7.3, Platform: Windows - x86...) with a "Download" button, and "Start and Setup Nessus" (instructions: Open Nessus and follow setup wizard to finish setting up Nessus). To the right, a "Summary" box provides release details: Release Date: May 15, 2024, Release Notes: Tenable Nessus 10.7.3, Signing Keys: RPM-GPG-KEY-Tenable-4096 (10.4 & above) and RPM-GPG-KEY-Tenable-2048 (10.3 & below). The browser interface includes a search bar at the bottom.

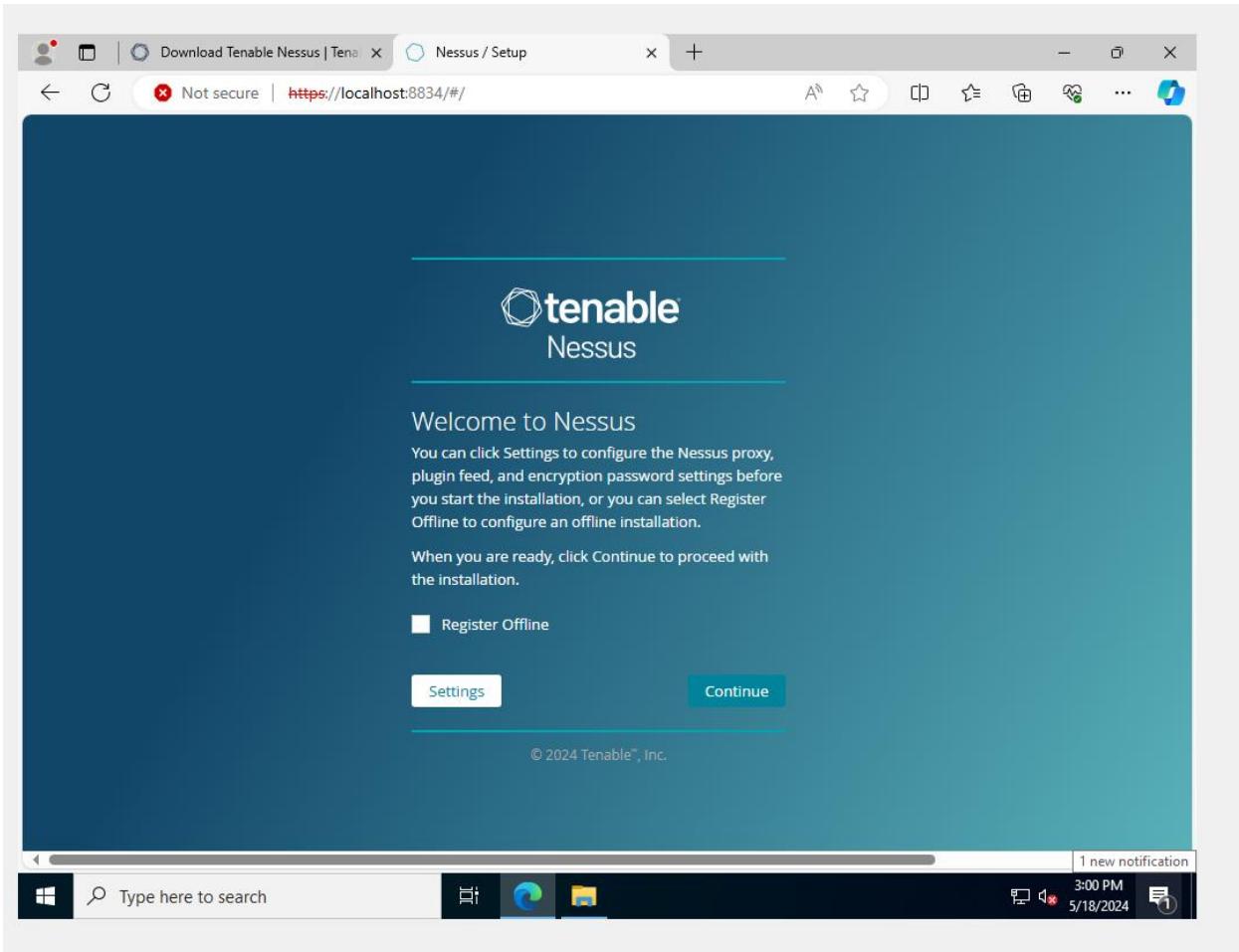


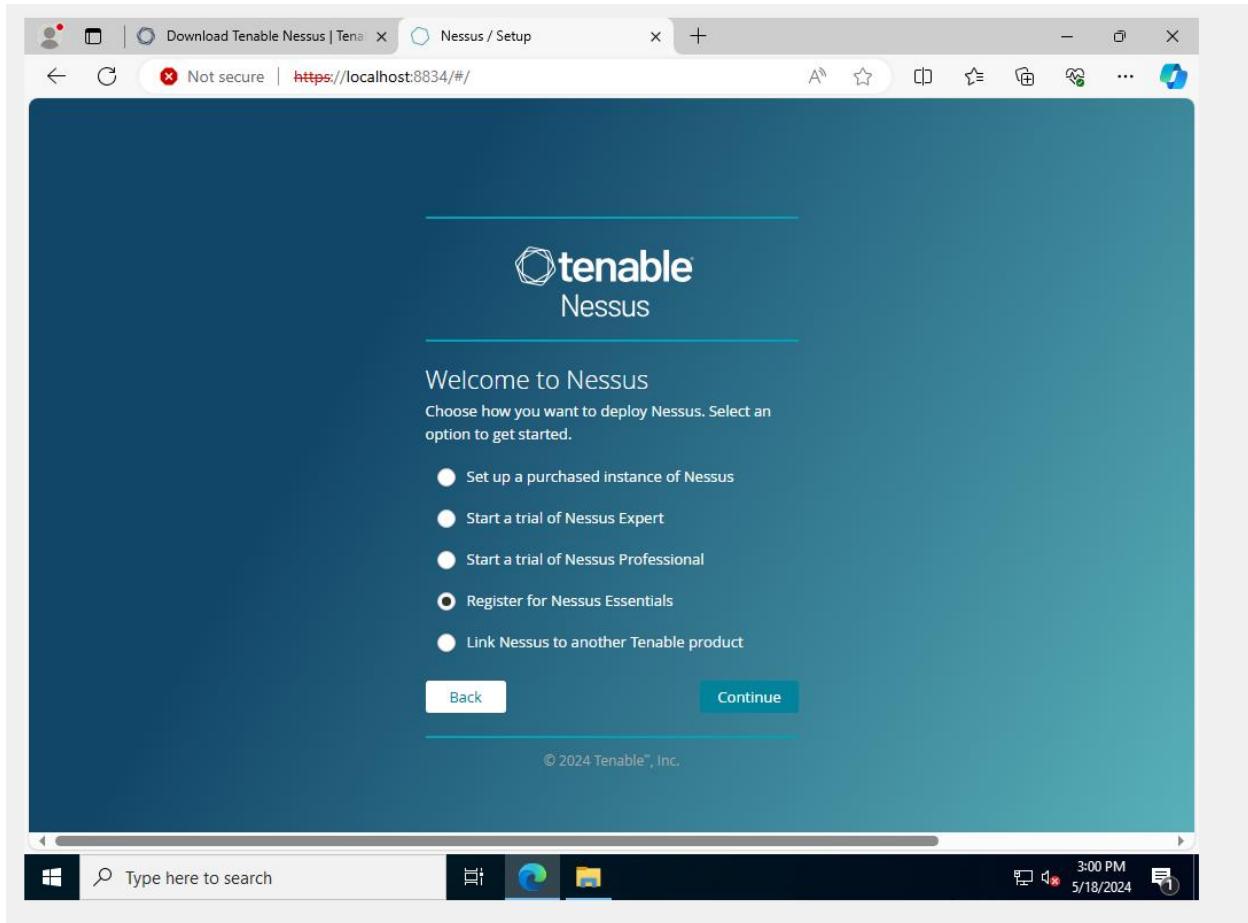


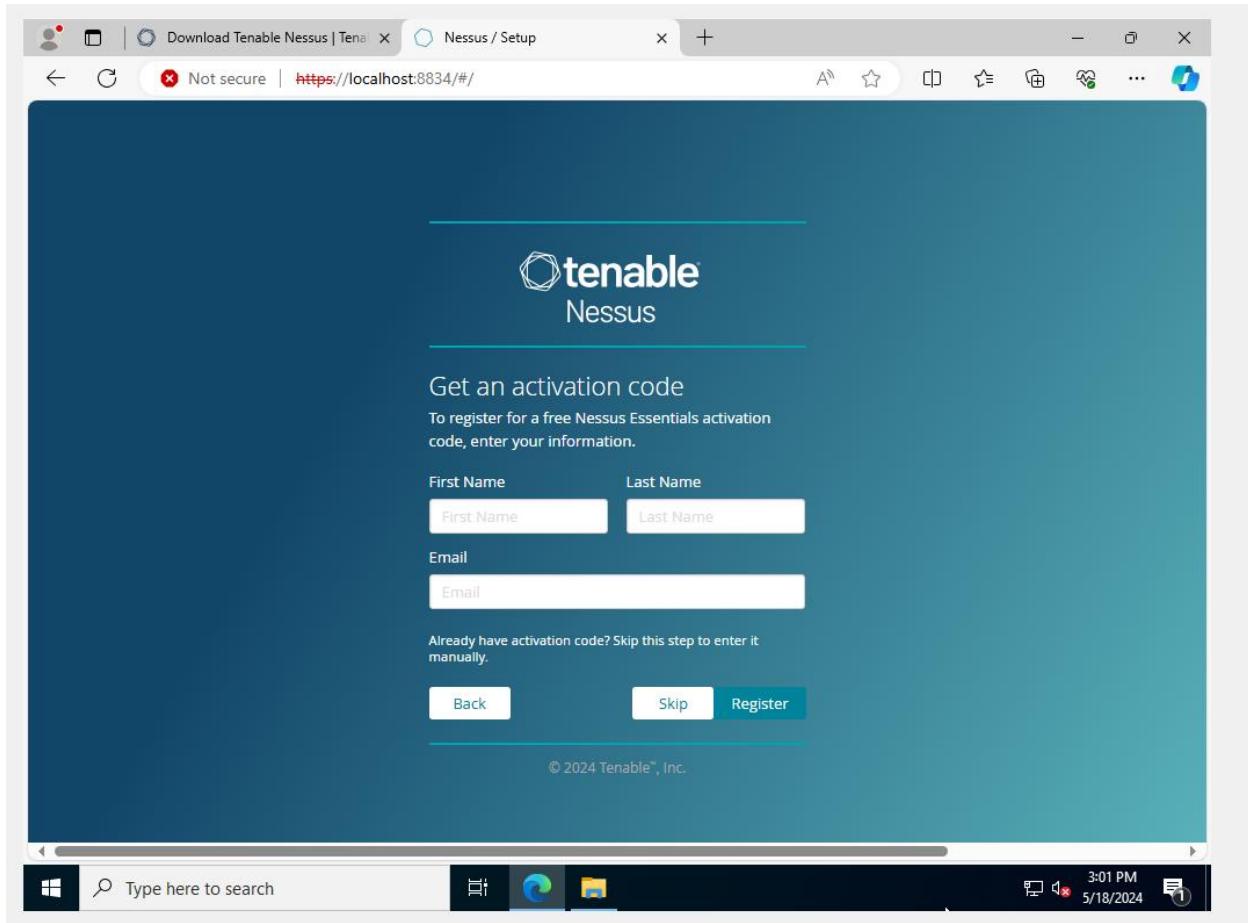


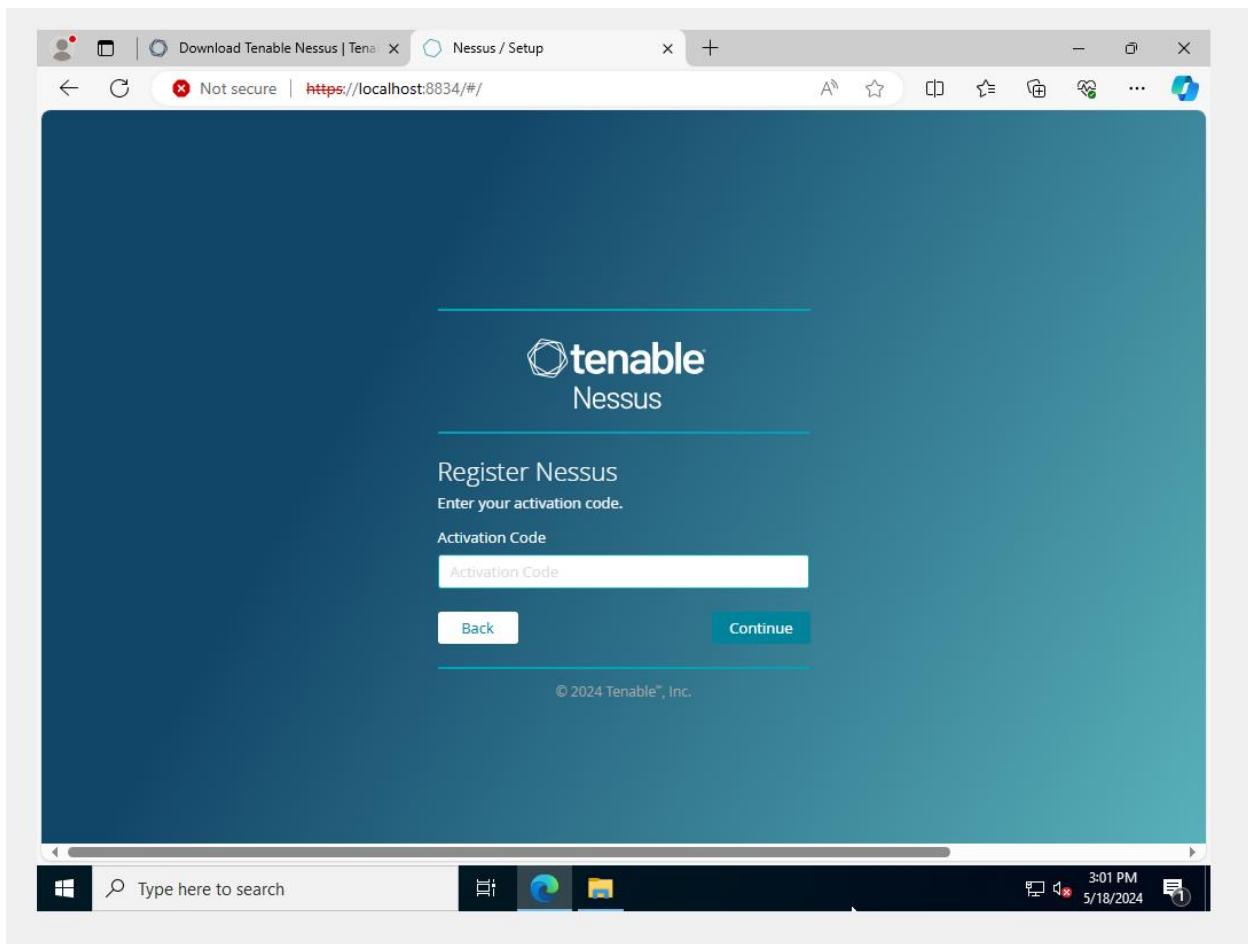


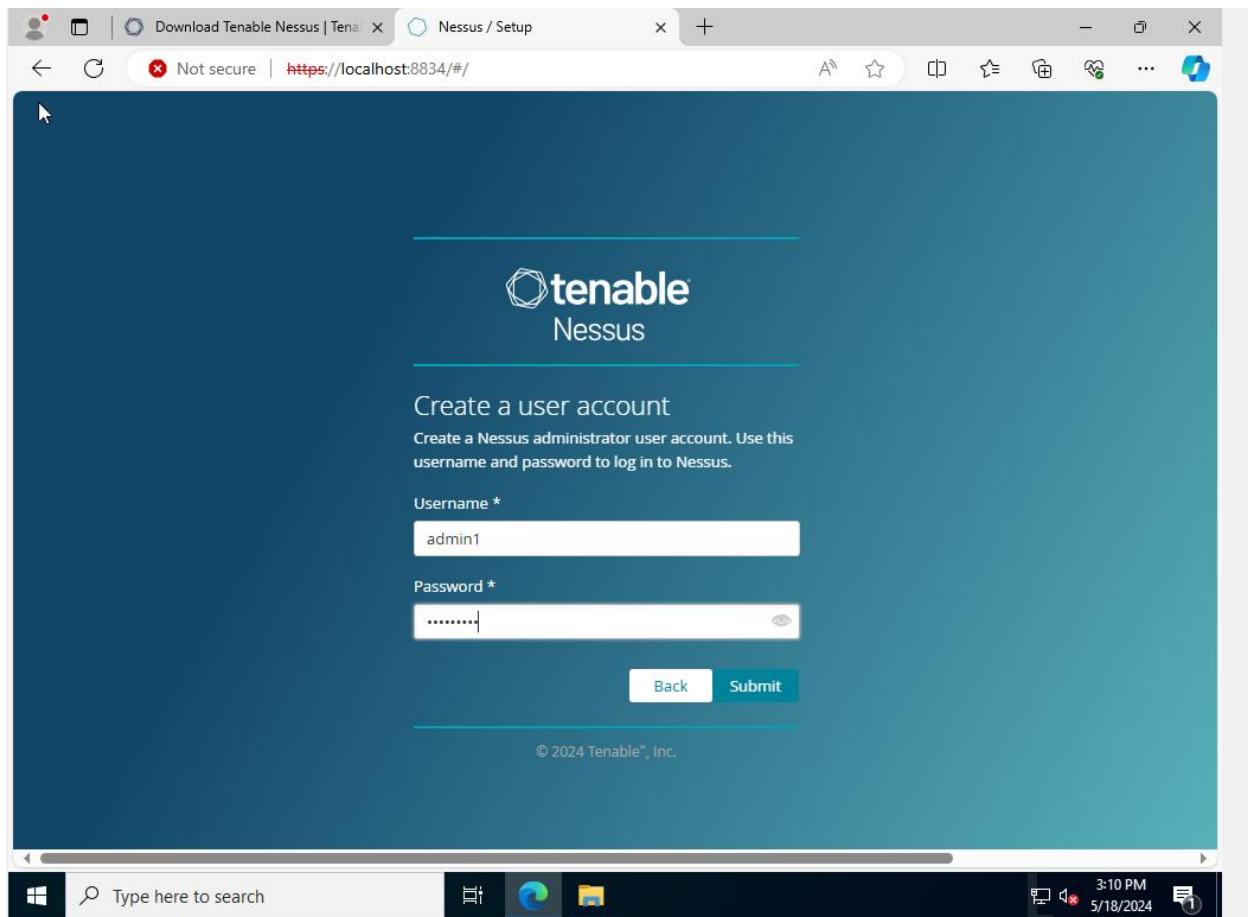


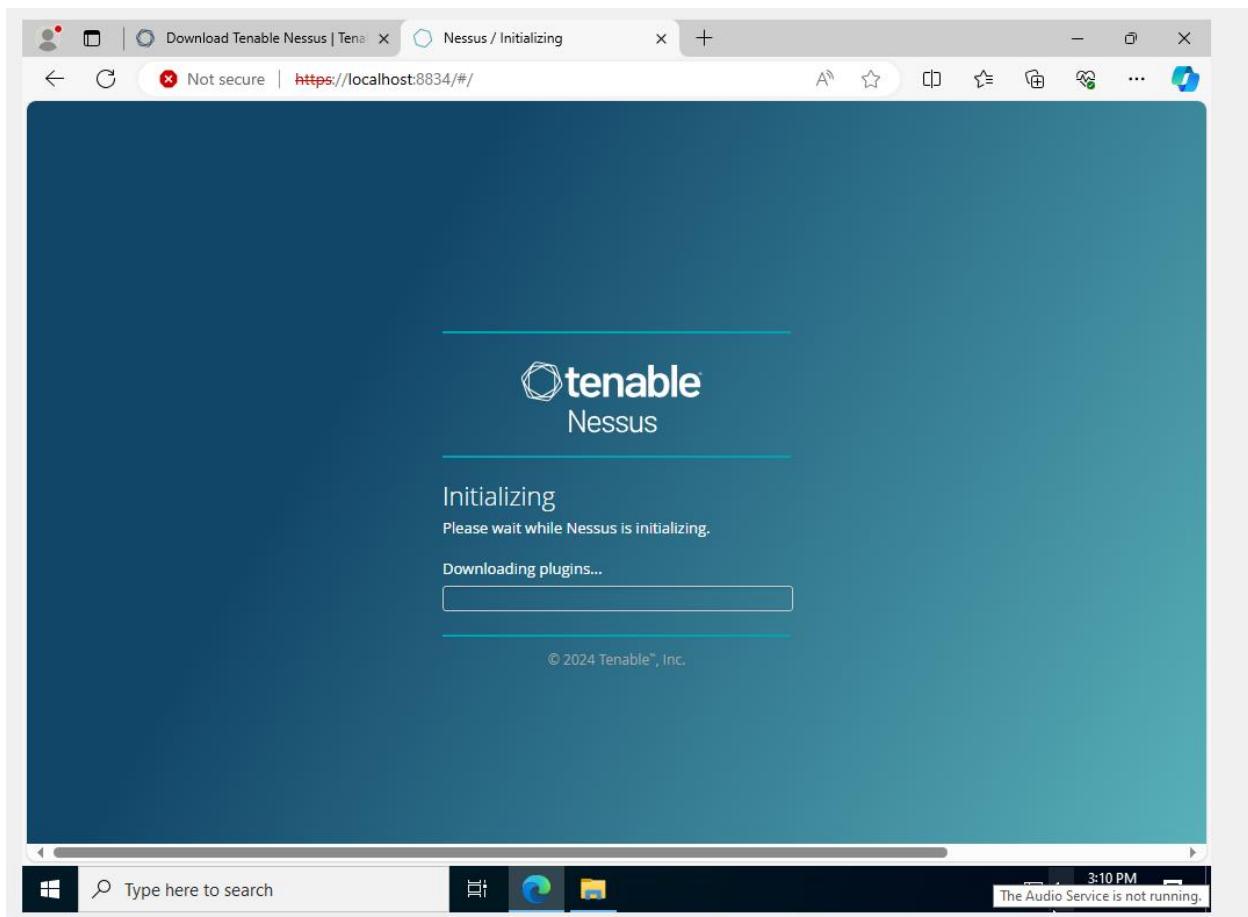












## WireShark

<https://www.wireshark.org/>

### ¿Qué es Wireshark?

1. **Definición:** Wireshark es una herramienta de análisis de red gratuita y de código abierto, utilizada para capturar y analizar el tráfico de red en tiempo real.
2. **Funcionalidad:** Permite a los usuarios ver el tráfico que pasa por una red en un nivel microscópico, siendo útil para la resolución de problemas de red, análisis de seguridad, y desarrollo de software y protocolos.

### Características Clave de Wireshark

1. **Captura y Análisis de Paquetes:** Captura datos de red desde Ethernet, Bluetooth, Wireless (IEEE.802.11), PPP/HDLC, ATM, y muchas otras fuentes.

2. **Filtrado de Datos:** Ofrece potentes capacidades de filtrado para permitir a los usuarios centrarse en los paquetes específicos de interés.
3. **Interfaz Gráfica y Uso de Comandos:** Disponible con una interfaz gráfica de usuario y también como TShark, su versión de línea de comandos.

### Usos Comunes de Wireshark

1. **Diagnóstico de Problemas de Red:** Ayuda a identificar problemas de latencia, pérdida de paquetes y puntos conflictivos en la comunicación de red.
2. **Seguridad Informática:** Utilizado para detectar actividades sospechosas o maliciosas en la red, como flujos de tráfico no autorizados o malformados.
3. **Desarrollo y Análisis de Protocolos:** Permite a los desarrolladores y analistas de red verificar si sus protocolos están funcionando según lo previsto.

### Importancia en la Ciberseguridad

1. **Análisis de Amenazas:** Esencial para los profesionales de seguridad para monitorizar y analizar el tráfico de red en busca de posibles amenazas o brechas de seguridad.
2. **Capacitación y Educación:** Ampliamente utilizado en la formación de profesionales de la ciberseguridad para entender y analizar el comportamiento del tráfico de red.

Wireshark es reconocido por su capacidad para proporcionar una visión detallada y en profundidad del tráfico de red, siendo una herramienta indispensable tanto para profesionales de redes como de seguridad.

Wireshark ofrece una gran variedad de filtros que permiten a los usuarios aislar tráfico específico, facilitando el análisis detallado de los paquetes. Aquí tienes una lista de algunos filtros comunes en Wireshark:

### Filtros de Protocolo

1. **ip:** Filtra todos los paquetes que utilizan el protocolo IP.
2. **tcp:** Selecciona solo los paquetes que usan TCP.
3. **udp:** Filtra los paquetes que utilizan el protocolo UDP.

4. **icmp**: Captura paquetes que utilizan el protocolo ICMP, útil para diagnosticar problemas en la red.

### Filtros de Dirección

1. **ip.addr == 192.168.1.1**: Filtra todos los paquetes donde la dirección IP es 192.168.1.1.
2. **eth.addr == 00:1A:2B:3C:4D:5E**: Filtra paquetes que involucran la dirección MAC especificada.
3. **ip.src == 10.0.0.5**: Filtra por paquetes con la dirección IP de origen específica.
4. **ip.dst == 10.0.0.5**: Filtra por paquetes con la dirección IP de destino específica.

### Filtros de Puerto

1. **tcp.port == 80**: Filtra todos los paquetes que involucran el puerto TCP 80.
2. **udp.port == 53**: Selecciona paquetes que involucran el puerto UDP 53, comúnmente usado por DNS.
3. **tcp.srcport == 443**: Filtra por paquetes cuyo puerto de origen es 443 (HTTPS).
4. **tcp.dstport == 443**: Filtra por paquetes cuyo puerto de destino es 443 (HTTPS).

### Filtros de Conversación

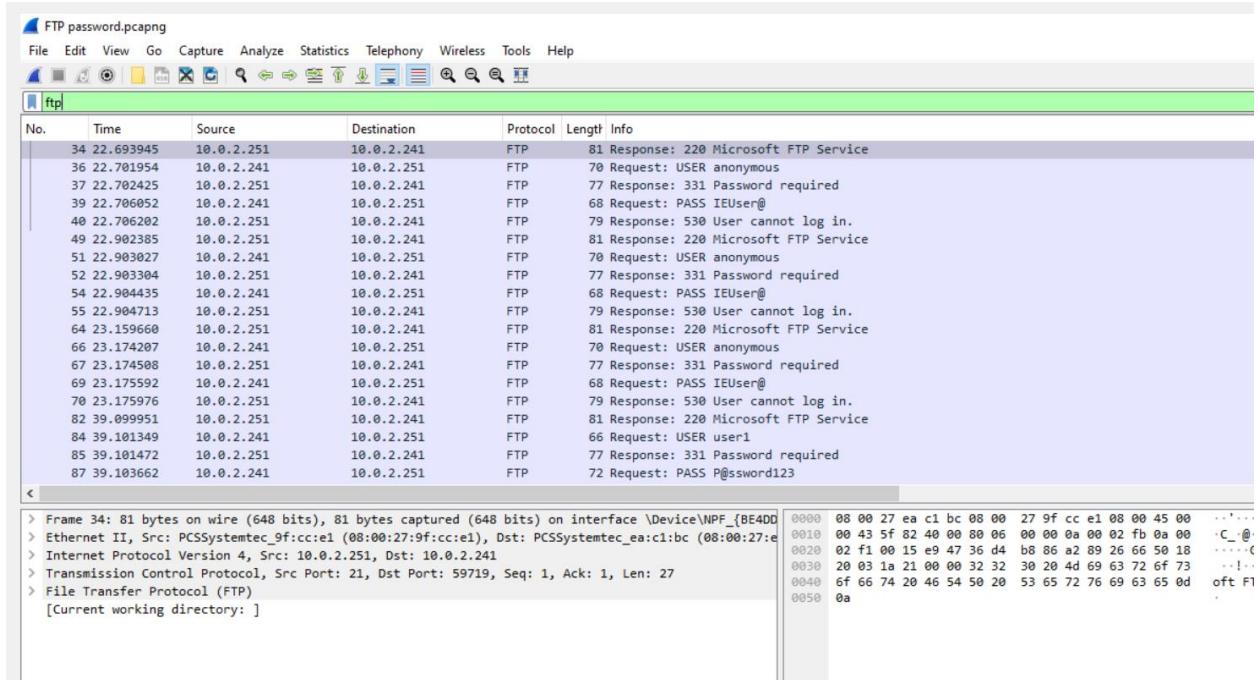
1. **tcp.stream eq 5**: Filtra por una conversación TCP específica, identificada por su número de stream.
2. **ip.conversation filter**: Filtra por todas las tramas pertenecientes a la misma conversación IP.

### Filtros de Contenido

1. **http contains "example.com"**: Busca paquetes HTTP que contengan la cadena "example.com".
2. **frame contains "data"**: Filtra por paquetes que contienen la cadena de texto "data".

Estos filtros pueden ser combinados usando operadores lógicos como and, or, y not para realizar análisis aún más específicos y detallados del tráfico de red.

## Ver la contraseña de un Usuario de FTP



## Zenmap

<https://nmap.org/zenmap/>

### ¿Qué es Zenmap?

1. **Definición:** Zenmap es la interfaz gráfica oficial del escáner de red Nmap, una herramienta ampliamente utilizada por administradores de sistemas y profesionales de la seguridad para descubrir dispositivos en una red, identificar servicios abiertos y obtener configuraciones de seguridad de sistemas remotos.
2. **Propósito:** Facilita el uso de Nmap para usuarios que prefieren una interfaz gráfica en lugar de la línea de comandos, haciendo que las funciones de Nmap sean más accesibles y fáciles de interpretar.

### Características Clave de Zenmap

1. **Interfaz de Usuario Amigable:** Proporciona una forma sencilla y visual de realizar y guardar escaneos de red, gestionar perfiles de escaneo y ver resultados.

2. **Funcionalidad de Mapeo:** Incluye una función de mapeo topológico que ayuda a visualizar la disposición de los hosts en una red, mostrando cómo están conectados.
3. **Compatibilidad:** Es compatible con múltiples sistemas operativos, incluyendo Windows, macOS y Linux.

### Usos Comunes de Zenmap

1. **Descubrimiento de Red:** Ayuda a identificar todos los dispositivos conectados a una red, incluyendo servidores, computadoras, impresoras, switches y routers.
2. **Análisis de Puertos:** Permite a los usuarios verificar qué puertos están abiertos en los dispositivos, lo que es crucial para la evaluación de la seguridad de la red.
3. **Auditoría de Seguridad:** Facilita la realización de comprobaciones de seguridad para identificar configuraciones inseguras y servicios innecesariamente expuestos.

### Importancia en la Ciberseguridad

1. **Evaluación de Vulnerabilidades:** Zenmap es una herramienta esencial para los escaneos preliminares en la evaluación de vulnerabilidades, permitiendo a los profesionales identificar puntos débiles potenciales en la seguridad de la red.
2. **Educación y Formación:** Debido a su interfaz gráfica, es ampliamente utilizado en la enseñanza y formación de nuevos profesionales de la ciberseguridad, proporcionando una plataforma accesible para aprender sobre escaneo de red y análisis de seguridad.

Zenmap simplifica la complejidad de Nmap, ofreciendo una solución poderosa y visual que ayuda a los usuarios a comprender mejor la estructura y seguridad de sus redes.

nmap.org/download.html

Bills Personal stuff YouTube Cars ChatGPT M365 Bard NSCC LLearning SeoChannel Cybersecurity Hoy LinkedIn MISC WhatsApp

Npcap.com SecLists.org Sectools.org Insecure.org

**Downloading Nmap**

Get the latest Nmap for your system:

- Windows
- macOS
- Linux (RPM)
- Any other OS (source code)

Older versions (and sometimes newer test releases) are available from the [Nmap release archive](#) (and really old ones are in [dist-old](#)). For the more security-paranoid (smart) users, GPG detached signatures and SHA-1 hashes for each release are available in the [sig directory](#) ([verification instructions](#)). Before downloading, be sure to read the relevant sections for your platform from the [Nmap Install Guide](#). The most important changes (features, bugfixes, etc) in each Nmap version are described in the [Changelog](#). Using Nmap is covered in the [Reference Guide](#), and don't forget to read the other [available documentation](#), particularly the official book [Nmap Network Scanning!](#)

Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (7 posts in 2015), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join the 128,953 current subscribers (as of September 2017) by submitting your email address here:

(or subscribe with custom options from the [Nmap-hackers list info page](#))

You can also get updates by liking [Nmap on Facebook](#) or following us [@nmap on Twitter](#).

Nmap is distributed with source code under [custom license terms](#) similar to (and derived from) the GNU General Public License, as noted in the [copyright page](#).

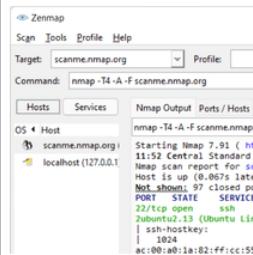
**Microsoft Windows binaries**

Please read the [Windows section](#) of the Install Guide for limitations and installation instructions for the Windows version of Nmap. It's provided as an executable self-installer which includes Nmap's dependencies and the Zenmap GUI. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 R2 and newer. We also maintain a [guide for users who must run Nmap on earlier Windows releases](#).

Latest stable release self-installer: [nmap-7.95-setup.exe](#)

We have written [nmap install usage instructions](#). Please notify us if you encounter any problems or have

## Microsoft Windows binaries



```
nmap -T4 -A -F scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2023-01-11 11:52 Central Standard Time
Nmap scan report for scanme.nmap.org
Host is up (0.00s latency).
Netmiko: 97 closed ports
PORT      STATE      SERVICE
22/tcp    open       ssh
22/tcp    open       ssh
22/tcp    open       ssh
| ssh-hostkey:
|   1024
|   ac:00:a0:1a:02:ff:cc:55
```

## Linux RPM Source and Binaries

Many popular Linux distributions (Redhat, Mandrake, Suse, etc) use the [RPM](#) package management system for quick and easy binary package installation. We have written a detailed [guide to installing our RPM packages](#), though these simple commands usually do the trick:

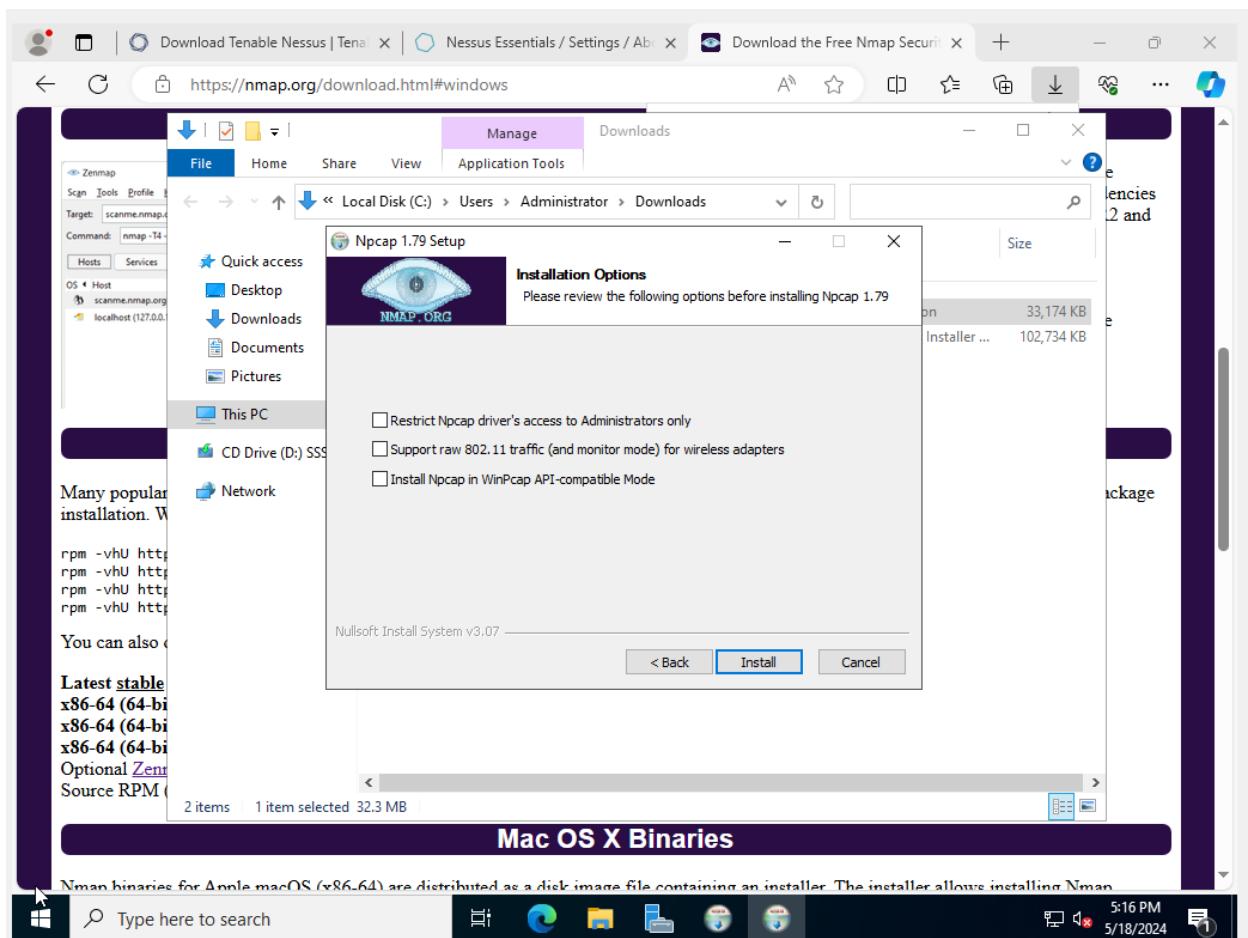
```
rpm -vhU https://nmap.org/dist/nmap-7.95-2.x86_64.rpm
rpm -vhU https://nmap.org/dist/zenmap-7.95-1.noarch.rpm
rpm -vhU https://nmap.org/dist/ncat-7.95-2.x86_64.rpm
rpm -vhU https://nmap.org/dist/nping-0.7.95-2.x86_64.rpm
```

You can also download and install the RPMs yourself:

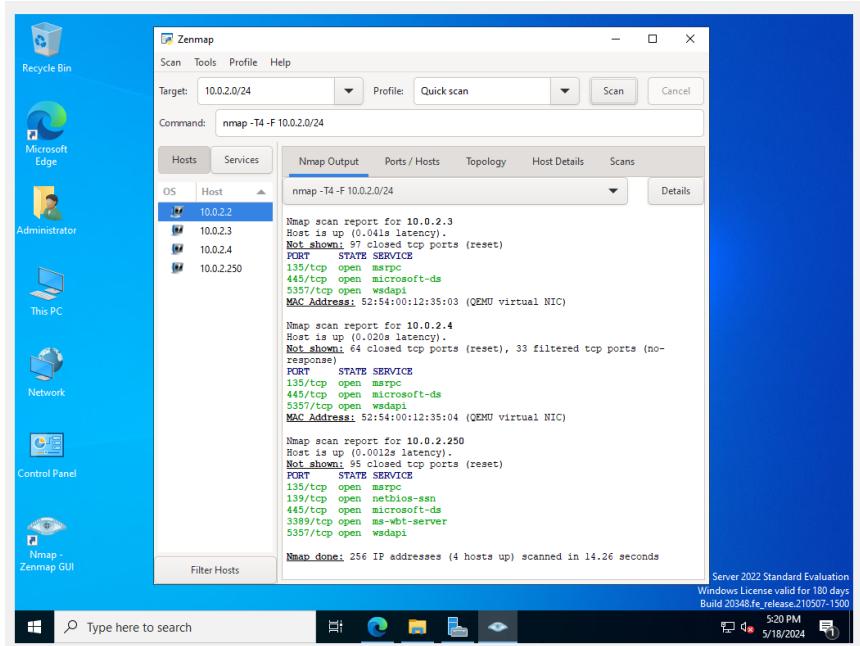
Latest [stable](#) release:  
**x86-64 (64-bit Linux)** [Nmap](#) RPM: [nmap-7.95-2.x86\\_64.rpm](#)  
**x86-64 (64-bit Linux)** [Ncat](#) RPM: [ncat-7.95-2.x86\\_64.rpm](#)  
**x86-64 (64-bit Linux)** [Nping](#) RPM: [nping-0.7.95-2.x86\\_64.rpm](#)  
Optional [Zenmap GUI](#) (all platforms): [zenmap-7.95-1.noarch.rpm](#)  
Source RPM (includes Nmap, Zenmap, Ncat, and Nping): [nmap-7.95-1.src.rpm](#)

## Mac OS X Binaries

Nmap binaries for Apple macOS (x86-64) are distributed as a disk image file containing an installer. The installer allows installing Nmap, Zenmap, Ncat, and Ndif. The programs have been tested on Mac OS X 10.9 and later. See the [Mac OS X Nmap install page](#) for more details.



## Escaneo rápido con Zenmap



## Advanced IP Scanner

<https://www.advanced-ip-scanner.com/>

### ¿Qué es Advanced IP Scanner?

- Definición:** Advanced IP Scanner es una herramienta gratuita y rápida de escaneo de red para Windows que permite a los usuarios identificar rápidamente todos los dispositivos conectados a una red LAN (Local Area Network).
- Funcionalidad:** Ofrece una variedad de funciones como el escaneo de IP, acceso remoto (RDP, SSH), apagado y encendido remoto de equipos, entre otras.

### Características Clave de Advanced IP Scanner

- Escaneo Rápido:** Capaz de escanear cientos de IP en segundos, lo que permite a los administradores obtener rápidamente una visión general de los dispositivos en la red.
- Detección de Dispositivos:** Identifica todos los dispositivos en una red, incluyendo computadoras, routers, y otros dispositivos de red, mostrando sus nombres, direcciones IP y fabricantes.

3. **Control Remoto:** Permite el acceso y control remotos a computadoras, utilizando RDP (Remote Desktop Protocol) y SSH, facilitando la gestión de dispositivos sin necesidad de estar físicamente presente.
4. **Funciones de Red:** Ofrece la capacidad de encender (a través de Wake-on-LAN) y apagar equipos remotamente, lo cual es útil para la gestión de grandes redes.

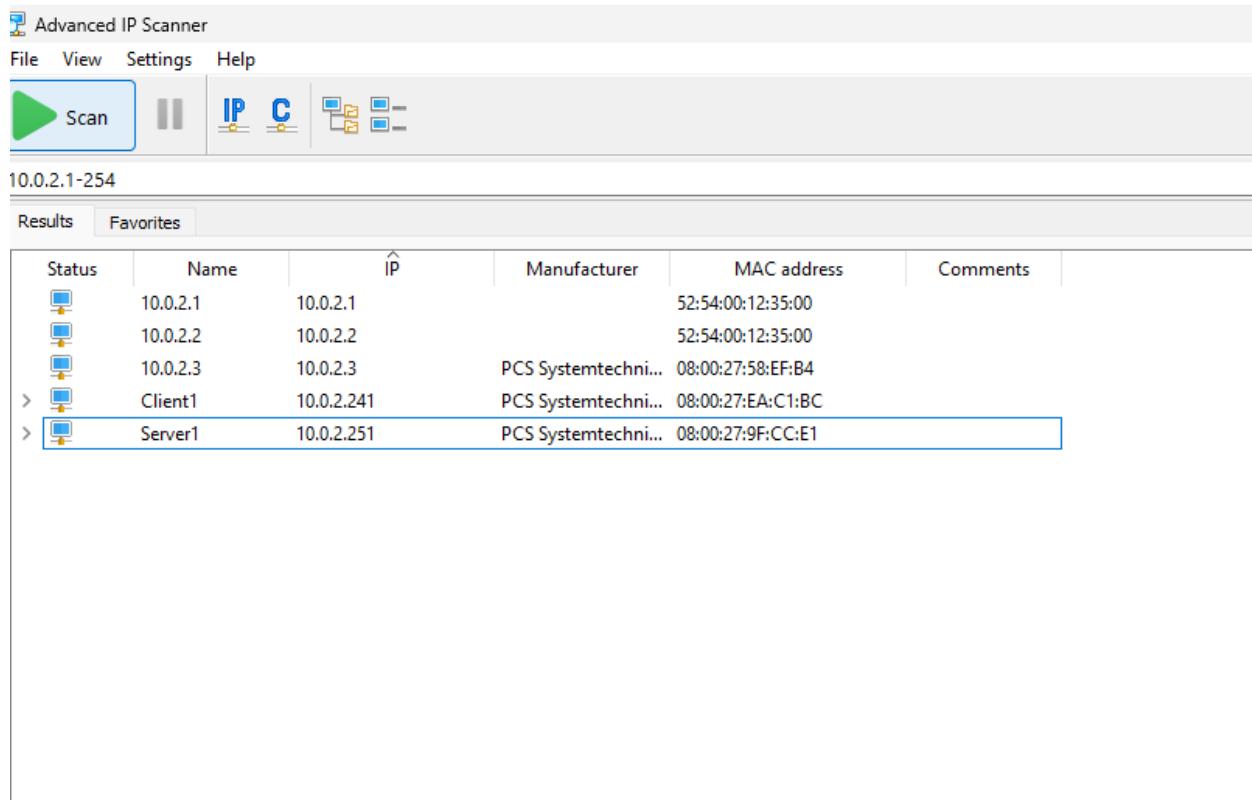
### **Usos Comunes de Advanced IP Scanner**

1. **Administración de Redes:** Ideal para administradores de sistemas que necesitan monitorear y gestionar la red, especialmente en entornos con un gran número de dispositivos conectados.
2. **Soporte Técnico:** Utilizado por equipos de soporte técnico para acceder y controlar rápidamente computadoras de usuarios para diagnóstico y mantenimiento.
3. **Auditorías de Seguridad:** Permite a los profesionales de seguridad realizar auditorías rápidas de la red para identificar dispositivos no autorizados o desconocidos que podrían ser potenciales riesgos de seguridad.

### **Importancia en la Ciberseguridad**

1. **Detección de Anomalías en la Red:** Ayuda a detectar rápidamente dispositivos no autorizados o comportamientos inusuales en la red, lo que es esencial para la prevención de intrusiones y la seguridad cibernética.
2. **Eficiencia Operativa:** Proporciona a los administradores herramientas para gestionar eficientemente la red, optimizando el rendimiento y la seguridad.

Advanced IP Scanner es reconocido por su facilidad de uso y por proporcionar una visión comprensiva de la infraestructura de red, haciendo que sea una herramienta esencial tanto para la gestión de redes como para la ciberseguridad.



## VeraCrypt

<https://www.veracrypt.fr/en/Downloads.html>

### VeraCrypt: Herramienta de Cifrado de Discos

#### ¿Qué es VeraCrypt?

1. **Definición:** VeraCrypt es un software gratuito y de código abierto utilizado para el cifrado de discos, diseñado para mejorar la seguridad de los datos mediante la creación de volúmenes cifrados. Es el sucesor de TrueCrypt, ampliamente conocido por su robustez en el cifrado de datos.

#### Características Clave de VeraCrypt

1. **Cifrado Fuerte:** Utiliza algoritmos de cifrado de alta seguridad como AES, Serpent y Twofish, y combinaciones de estos en modos de cifrado en cascada para ofrecer una protección muy robusta.

2. **Creación de Volúmenes Cifrados:** Permite a los usuarios crear un espacio virtual cifrado en sus dispositivos, que se comporta como una unidad física real una vez montado con la contraseña correcta.
3. **Cifrado de Discos Completos:** Ofrece la capacidad de cifrar una partición entera o un dispositivo de almacenamiento, incluyendo la posibilidad de cifrar el disco de arranque del sistema operativo.
4. **Resistencia a Ataques de Fuerza Bruta:** Implementa complejas estructuras de hash y demoras en la autenticación para contrarrestar ataques de fuerza bruta.

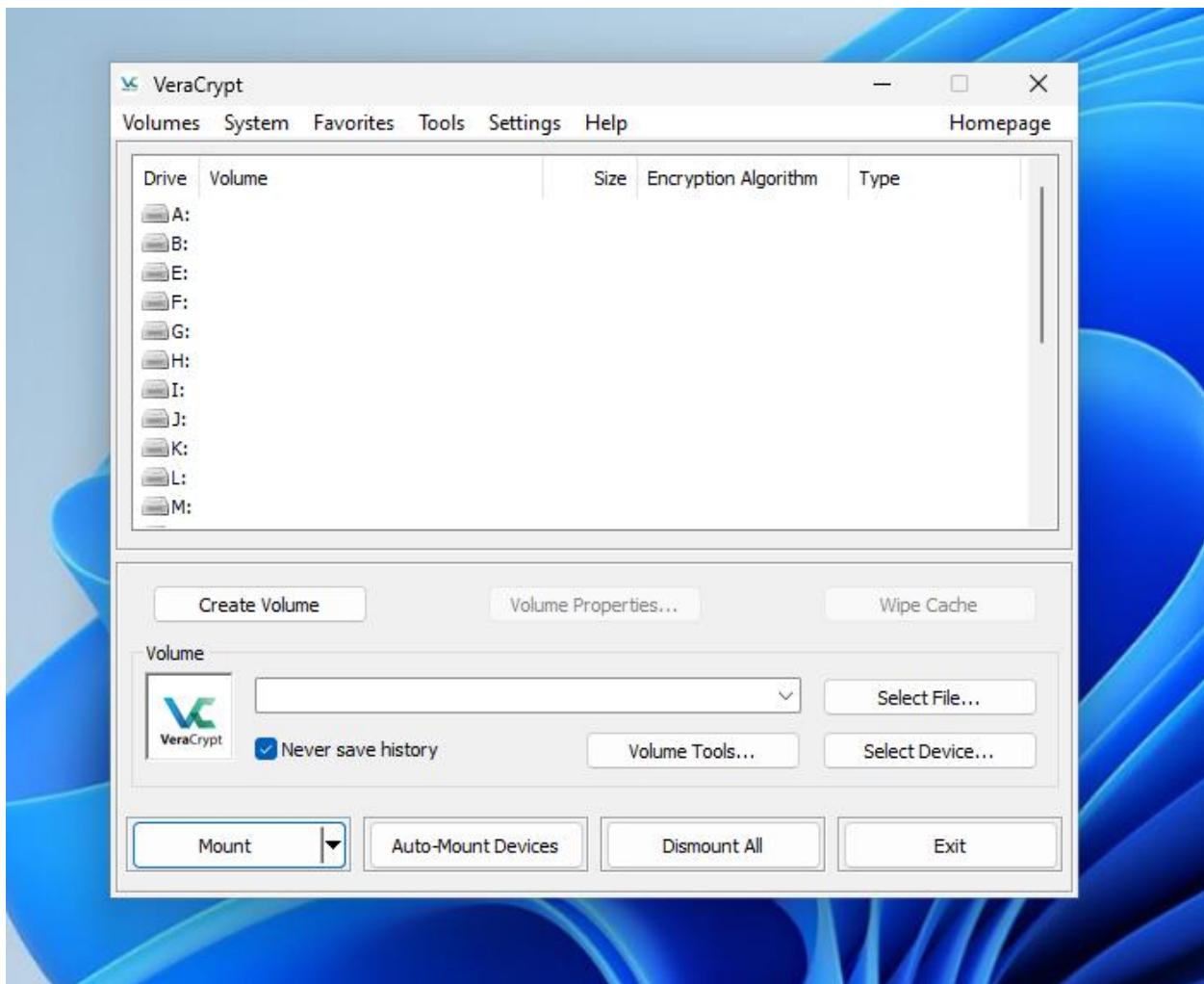
### **Usos Comunes de VeraCrypt**

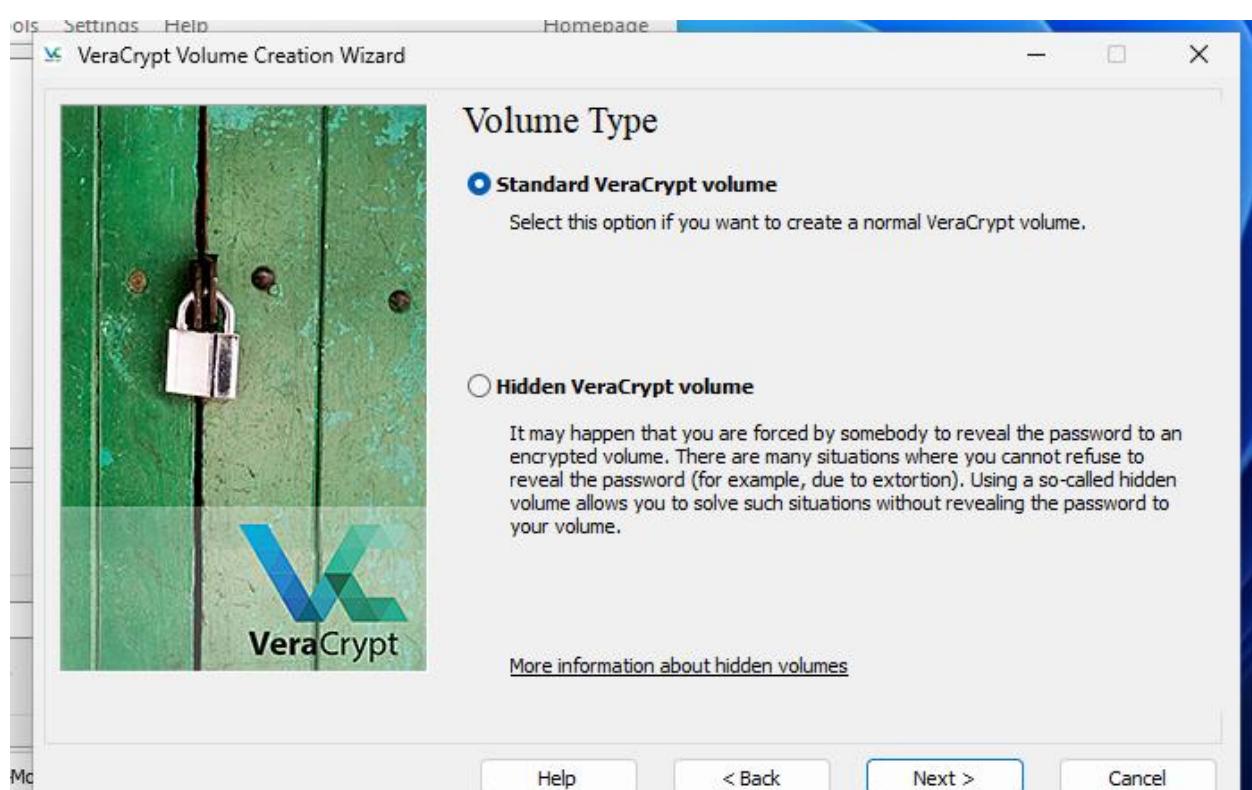
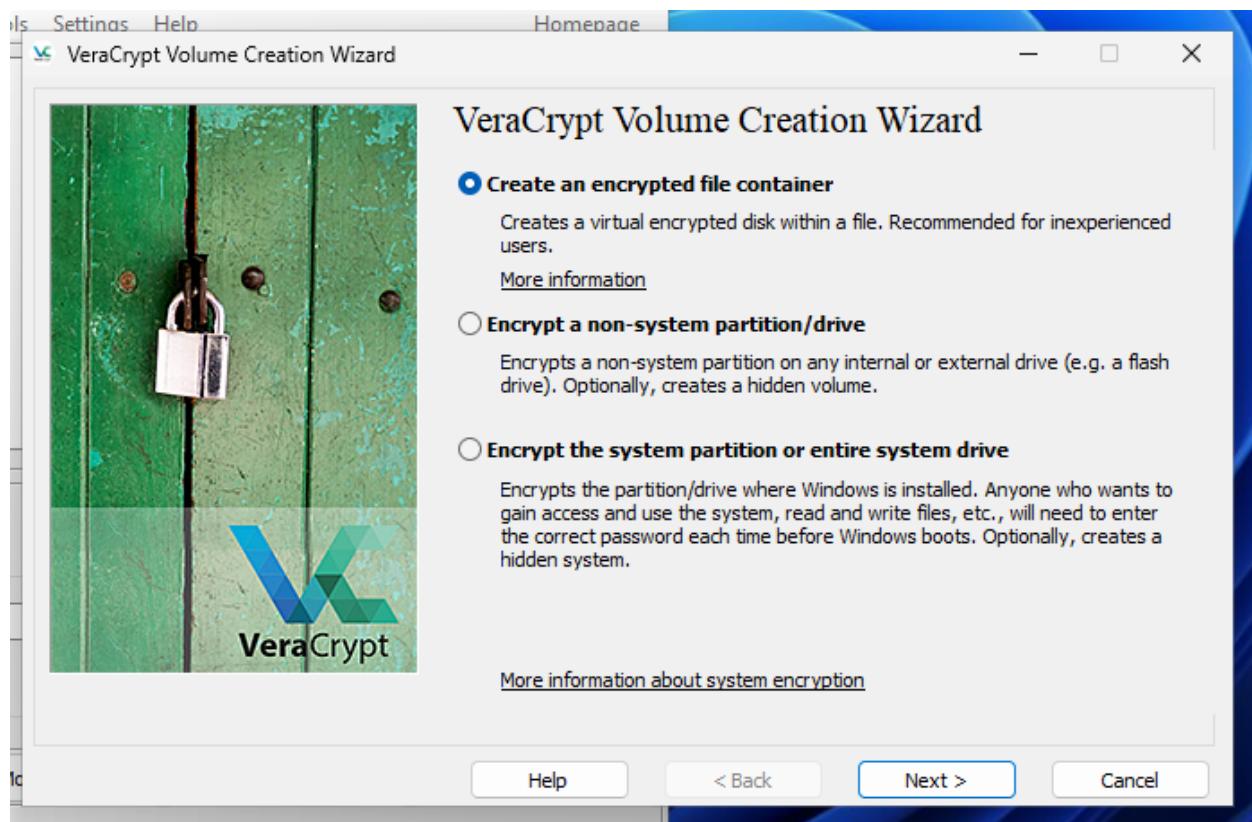
1. **Protección de Datos Sensibles:** Ideal para individuos y empresas que necesitan proteger datos sensibles de accesos no autorizados, especialmente en dispositivos que pueden ser susceptibles a robo o pérdida.
2. **Seguridad en la Nube:** Utilizado para cifrar archivos antes de subirlos a servicios de almacenamiento en la nube, asegurando que los datos permanezcan seguros incluso si el proveedor de la nube es comprometido.
3. **Compliance y Normativas:** Ayuda a las organizaciones a cumplir con regulaciones de privacidad y seguridad de datos, como GDPR, HIPAA, entre otras, que requieren protección de datos personales y sensibles.

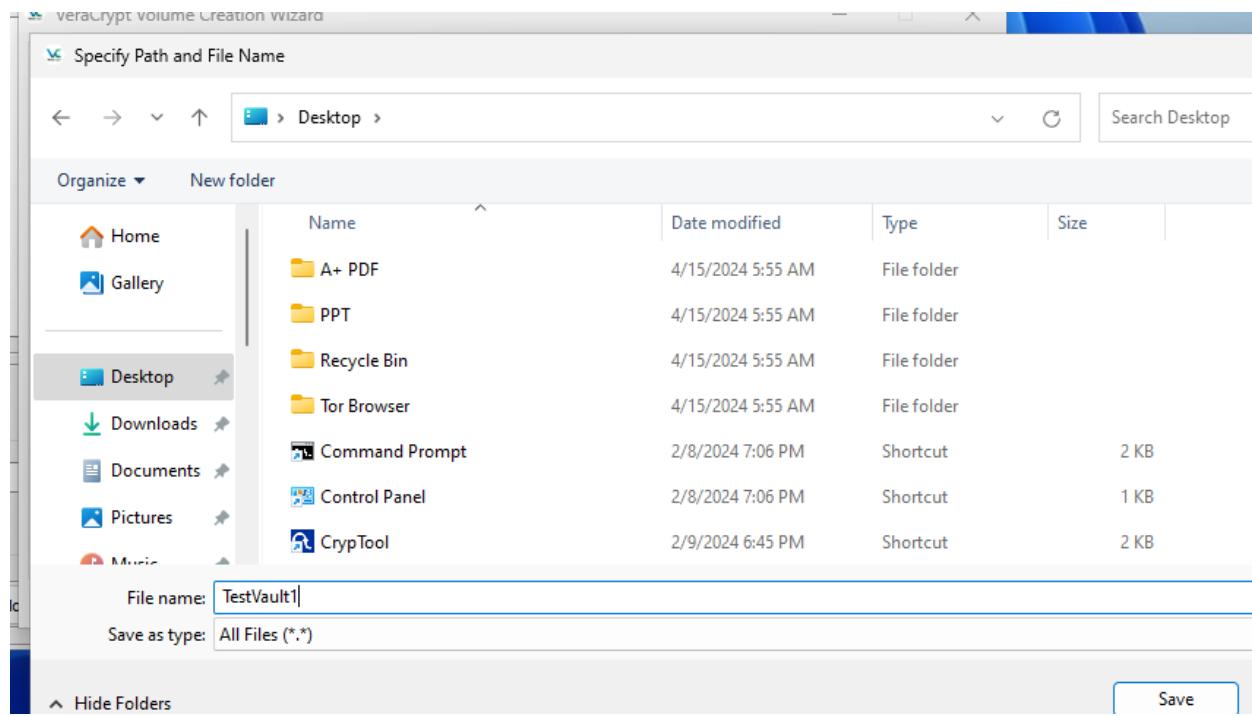
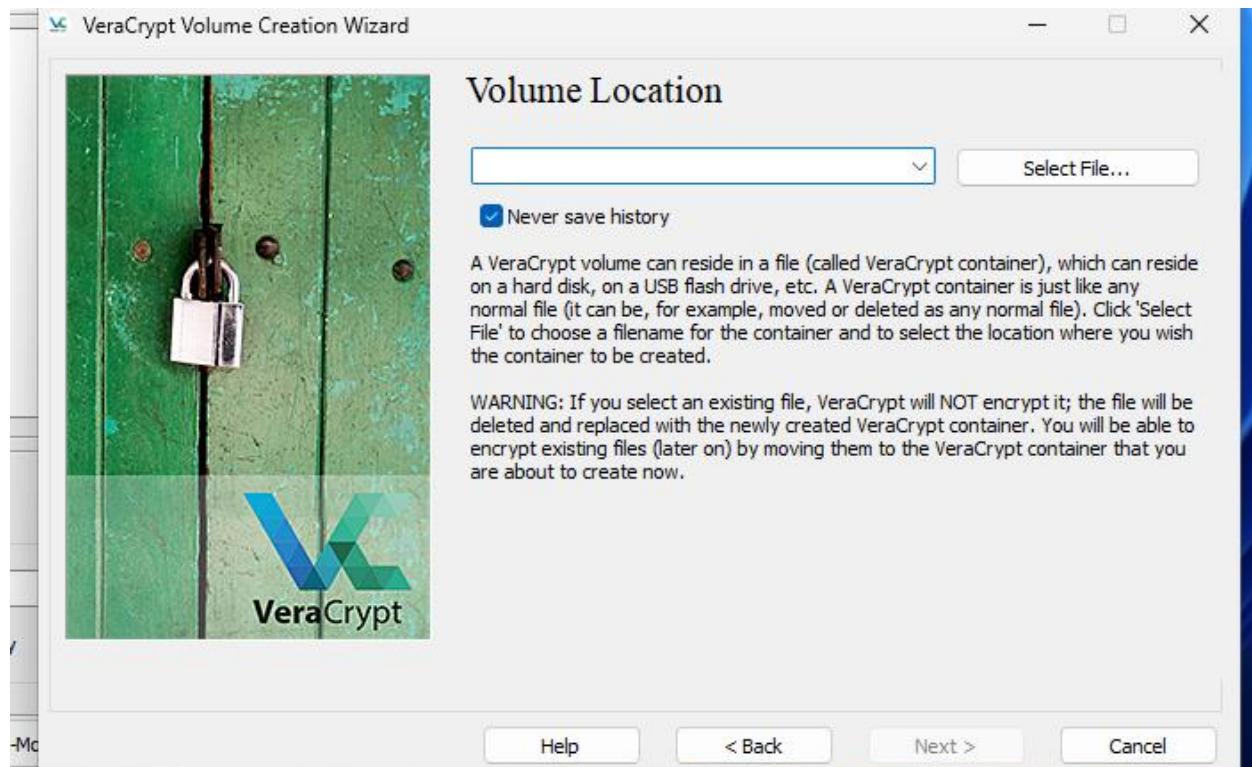
### **Importancia en la Ciberseguridad**

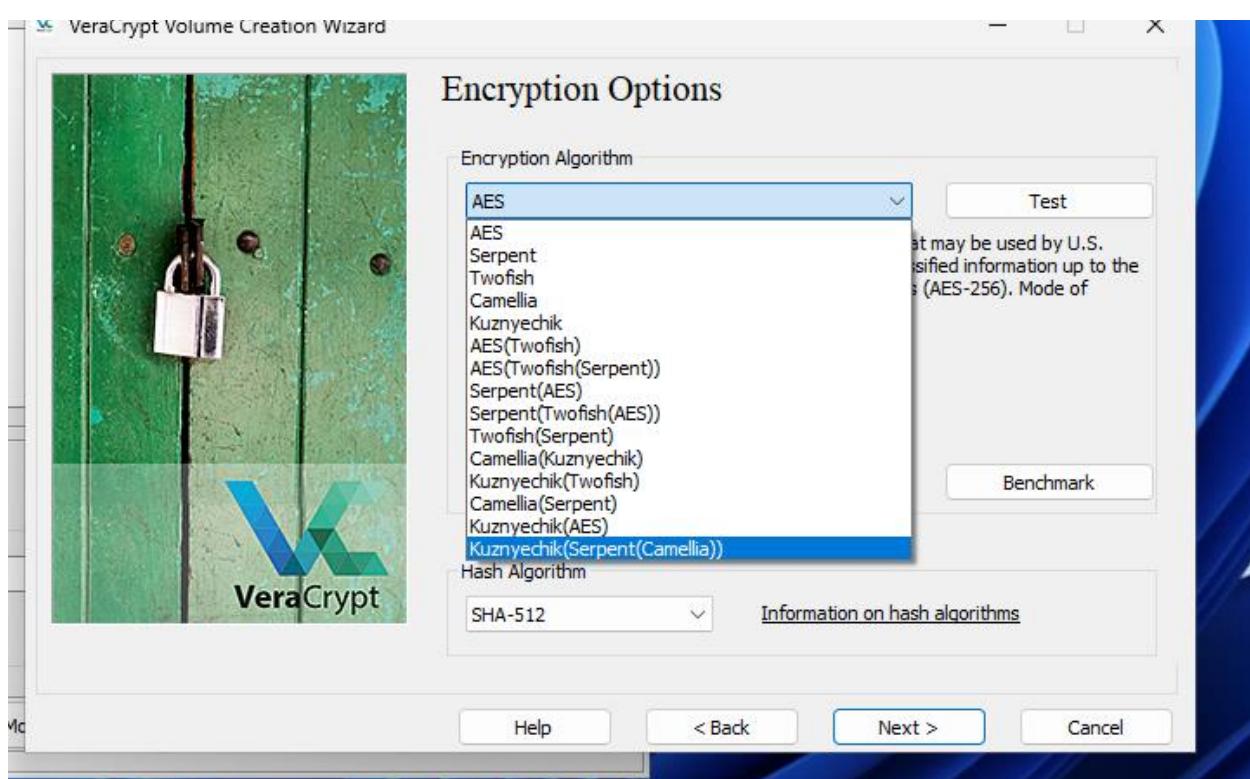
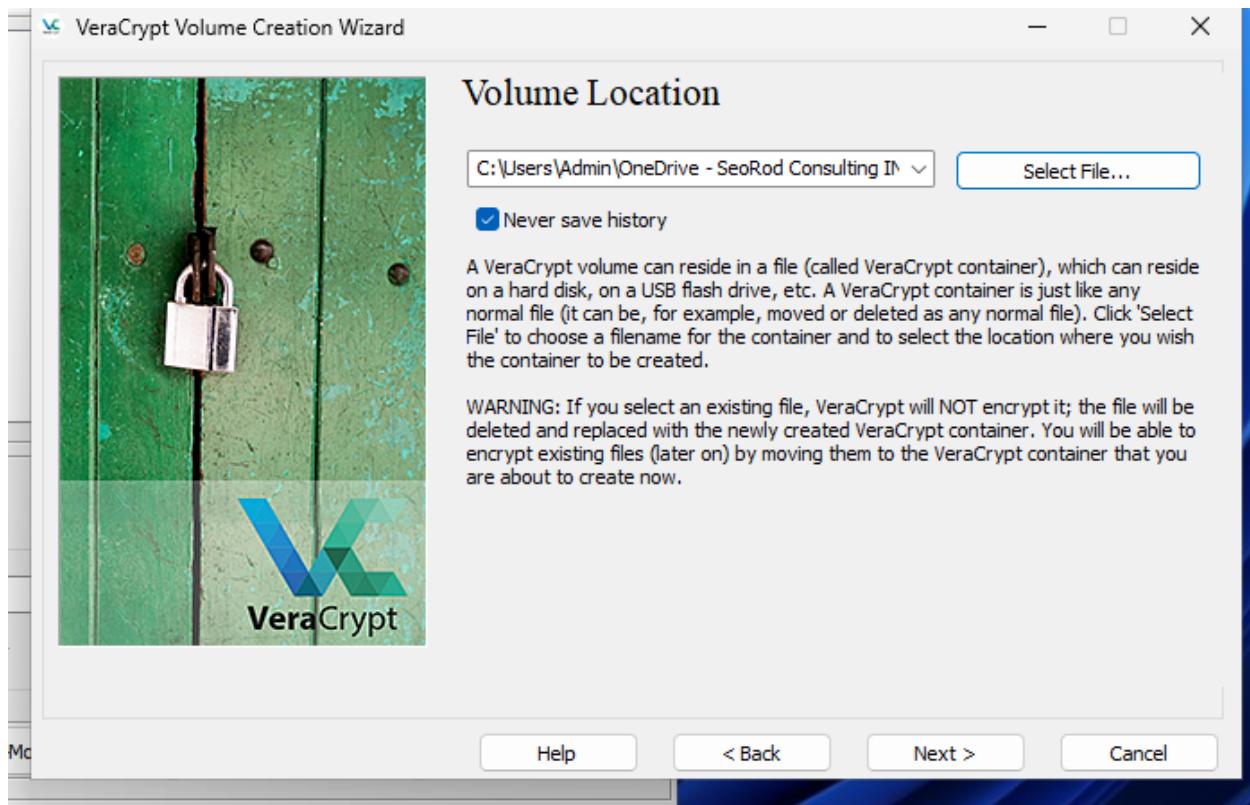
1. **Confidencialidad de los Datos:** Asegura que los datos solo sean accesibles para quienes poseen la clave de cifrado correcta, preservando la confidencialidad.
2. **Integridad del Sistema:** El cifrado del disco de arranque ayuda a proteger contra malware y otros vectores de ataque que podrían comprometer un sistema al inicio.

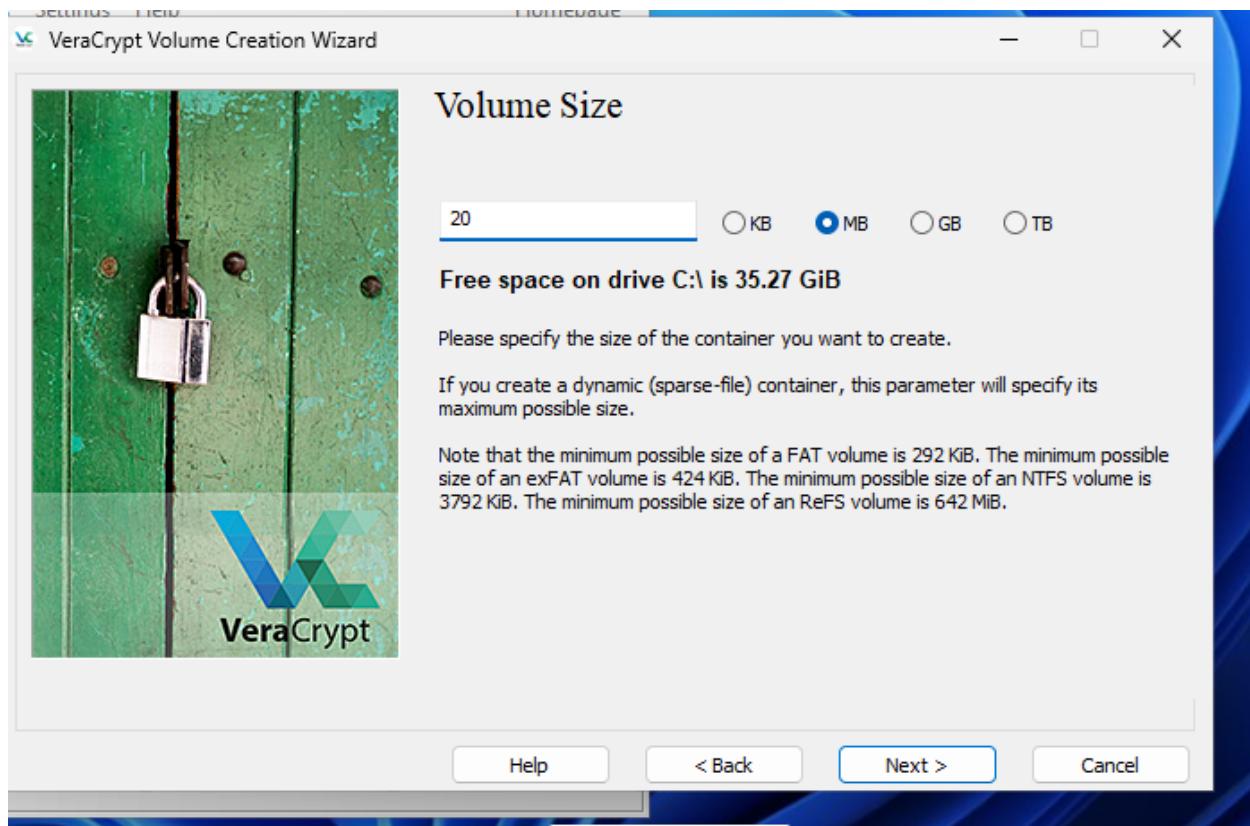
VeraCrypt es altamente valorado en la comunidad de ciberseguridad por proporcionar una solución de cifrado accesible y altamente segura, haciendo que sea una herramienta esencial para cualquier persona o negocio que tome en serio la seguridad de sus datos.







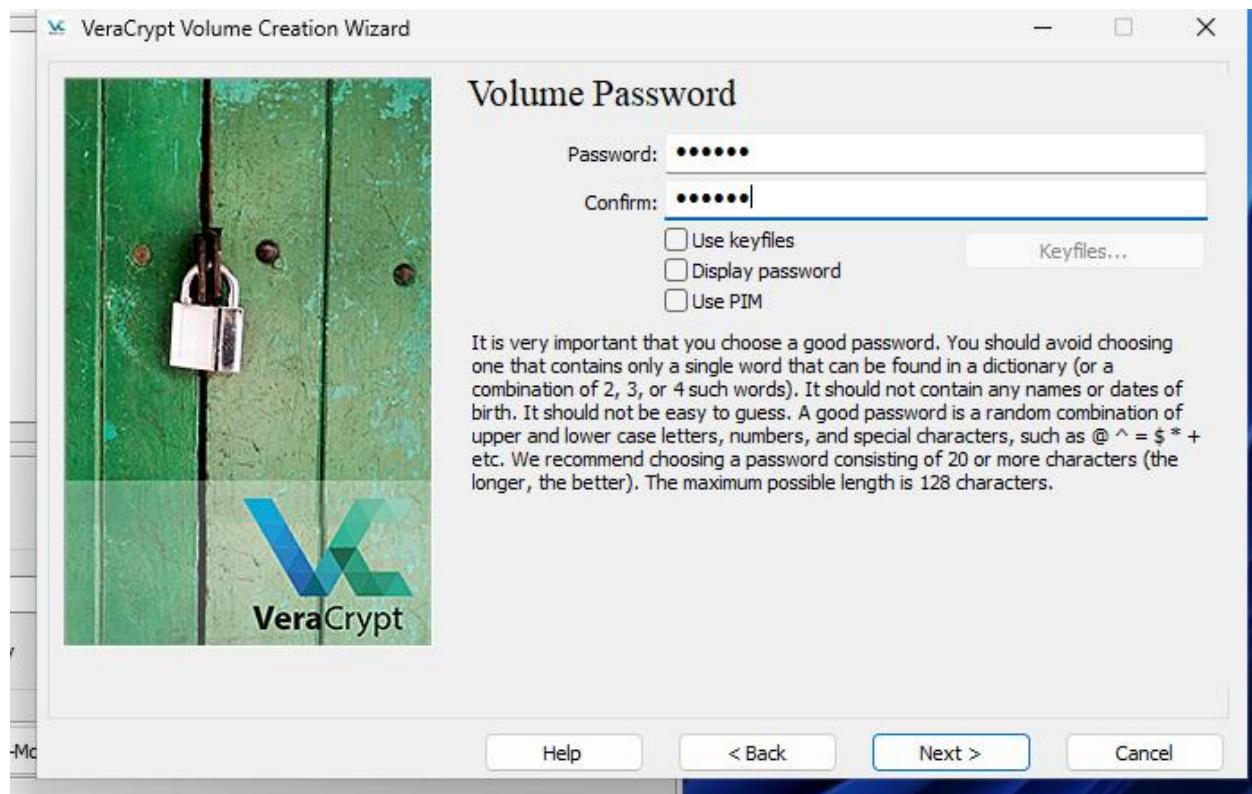


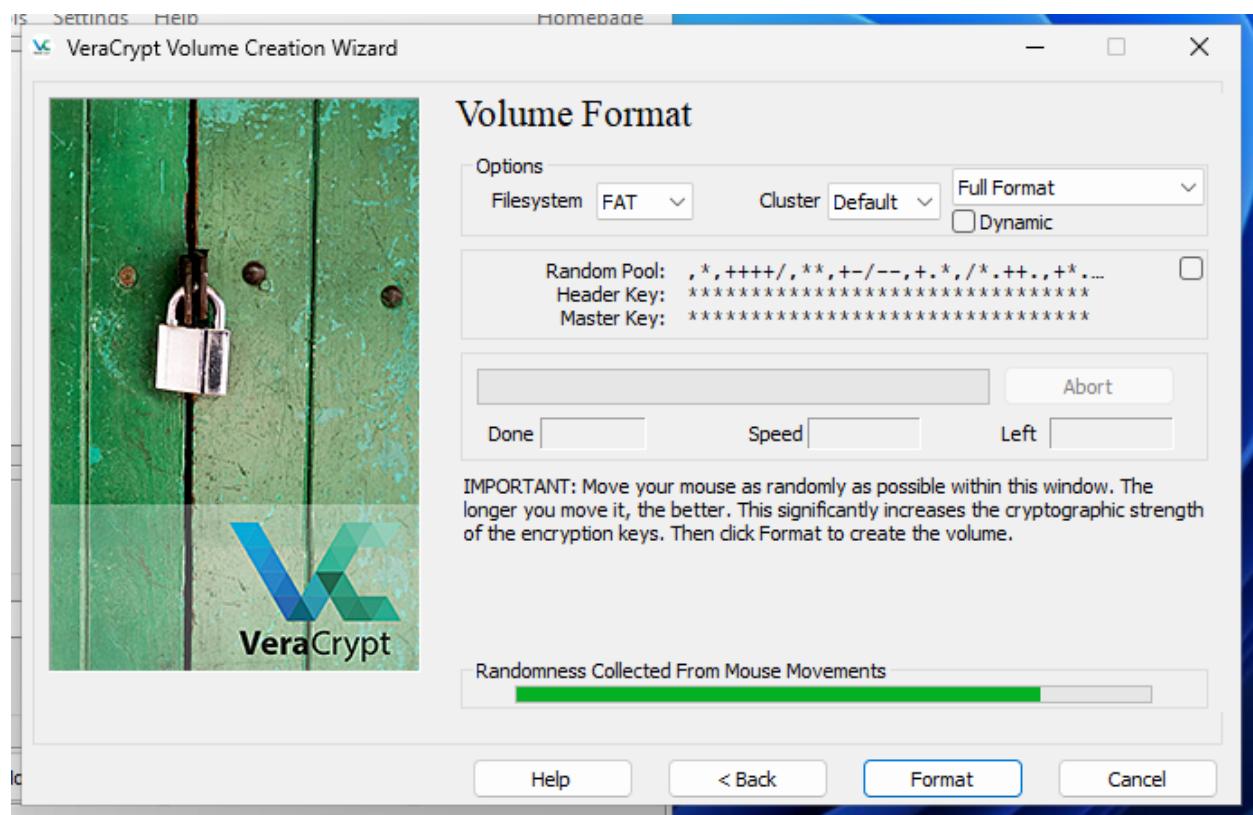


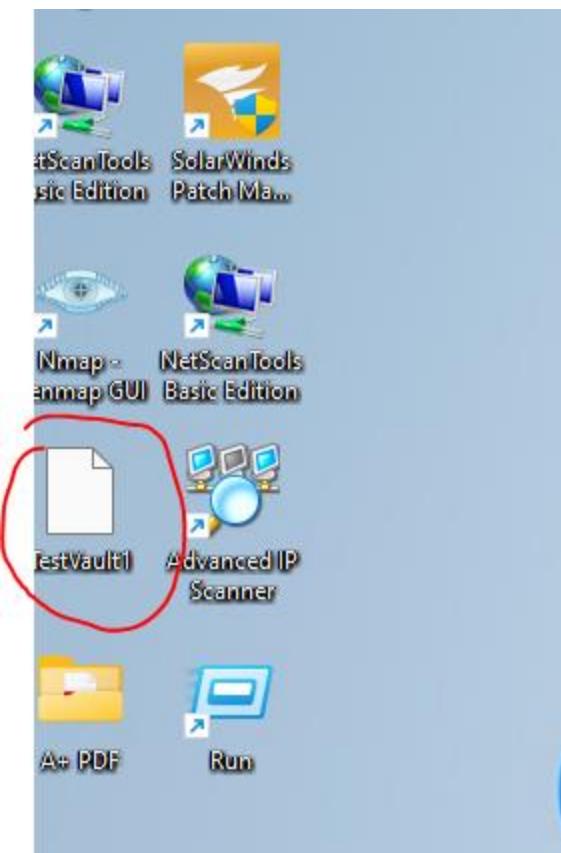
123456

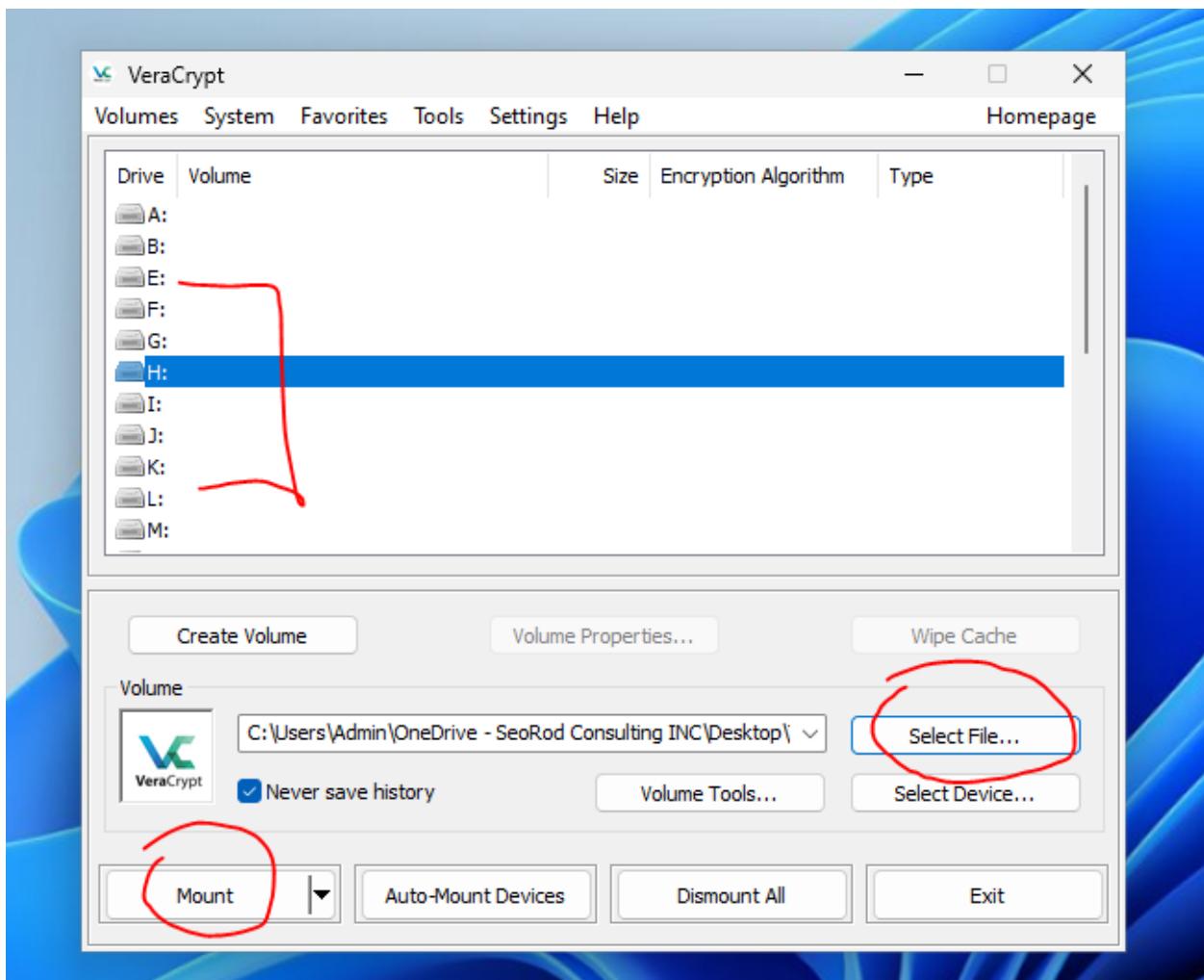
122

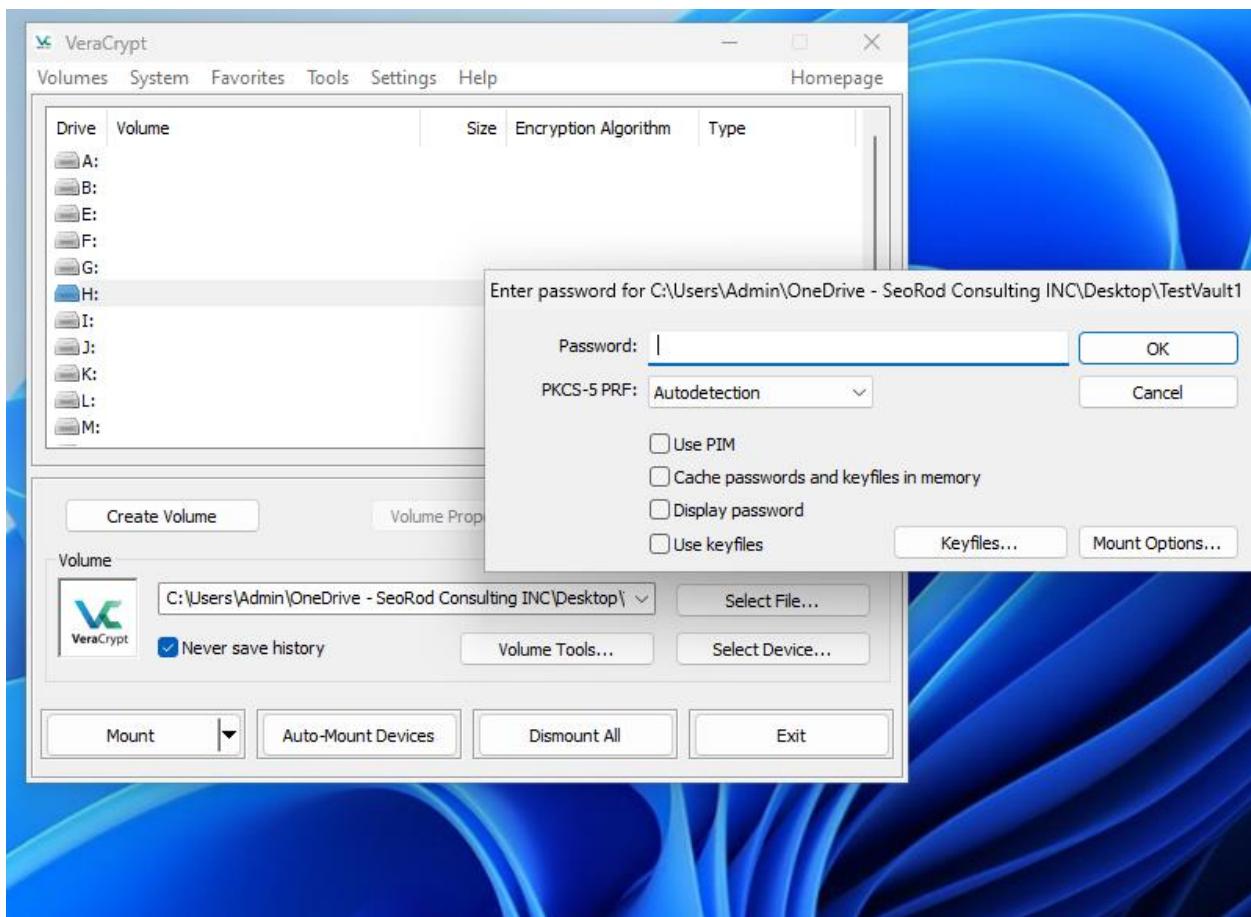
CertToday.com











## Conclusión

Este taller laboratorio ha proporcionado a los participantes una experiencia práctica y comprensiva en la configuración y manejo de una variedad de sistemas operativos y herramientas esenciales para la ciberseguridad. Al instalar y configurar VirtualBox, los estudiantes han establecido un entorno virtual seguro para hospedar sistemas operativos clave como Windows 11 y Windows Server 2022, este último configurado como Domain Controller, además de Kali Linux. La inclusión de herramientas especializadas como Nessus, Wireshark y Zenmap ha enriquecido este entorno, permitiendo a los participantes realizar tareas avanzadas de análisis y auditoría de redes.

**Puntos destacados del aprendizaje incluyen:**

1. **Habilidades Técnicas:** Los estudiantes han adquirido habilidades técnicas en la instalación y configuración de máquinas virtuales, una competencia indispensable en la ciberseguridad para crear y manejar entornos de prueba seguros.
2. **Análisis de Red:** La práctica con Wireshark y Zenmap ha enseñado a los participantes cómo monitorizar y analizar el tráfico de red, identificando posibles vulnerabilidades y amenazas.
3. **Evaluación de Vulnerabilidades:** El uso de Nessus para realizar escaneos de vulnerabilidades ha demostrado la importancia de la evaluación regular para mantener la seguridad de la red.
4. **Defensa y Seguridad:** La configuración de un Domain Controller en Windows Server 2022 ha proporcionado una base sólida en conceptos de gestión de red y políticas de seguridad.

Este taller no solo ha equipado a los participantes con conocimientos teóricos, sino que también ha reforzado estos conceptos con aplicaciones prácticas, asegurando que estén preparados para enfrentar los retos reales en el mundo de la ciberseguridad. Así, los estudiantes salen de este laboratorio con una comprensión profunda y habilidades aplicables que son críticas para su futuro profesional en el campo de la seguridad informática.