Hardening Windows 11

Larry Baldwin · Follow
7 min read · Dec 29, 2023

This article outlines the various steps you can take to harden Windows 11. Lowering the attack surface through hardening makes your Windows 11 more secure.

Tools Used

VirtualBox: https://www.virtualbox.org/

Windows 11 Iso: https://www.microsoft.com/software-download/windows11

Brave Browser: https://brave.com/

Avast Free Antivirus: https://www.avast.com/en-us/index#pc

VeraCrypt: https://www.veracrypt.fr/en/Downloads.html

Common Definitions:

Attack Surface — the number of all possible points, or attack vectors, where an unauthorized user can access a system and extract data.

Hardening — the process of securing a system by reducing its attack surface.

Cross-Site Scripting (XSS) — XSS attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.

Hypervisor — A hypervisor is a type of computer software, firmware or hardware that creates and runs virtual machines.

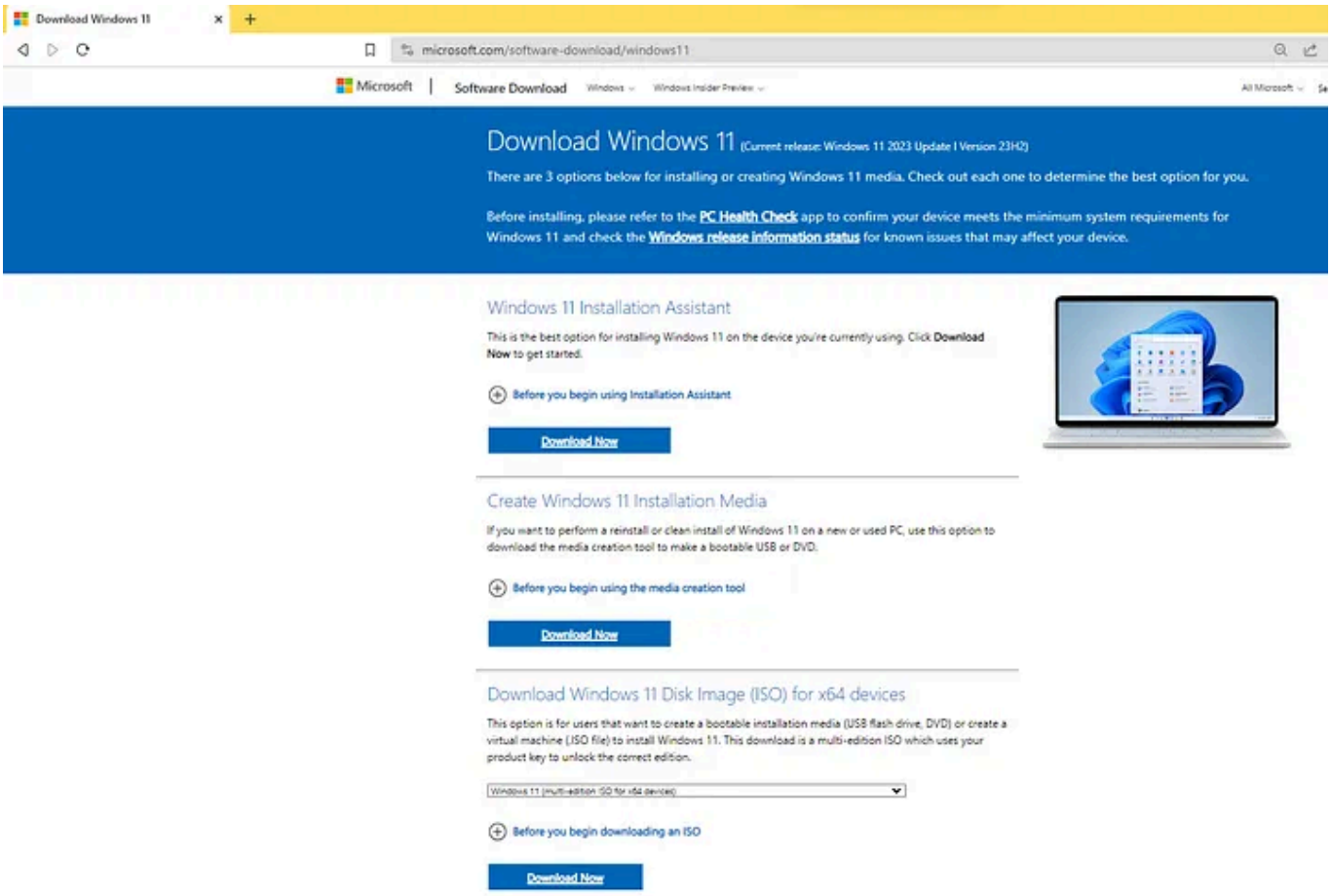
Type-2 Hypervisor — Type-2 hypervisor runs on top of supported operating systems and uses the OS's drivers to communicate with the hardware.

Encryption — encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.

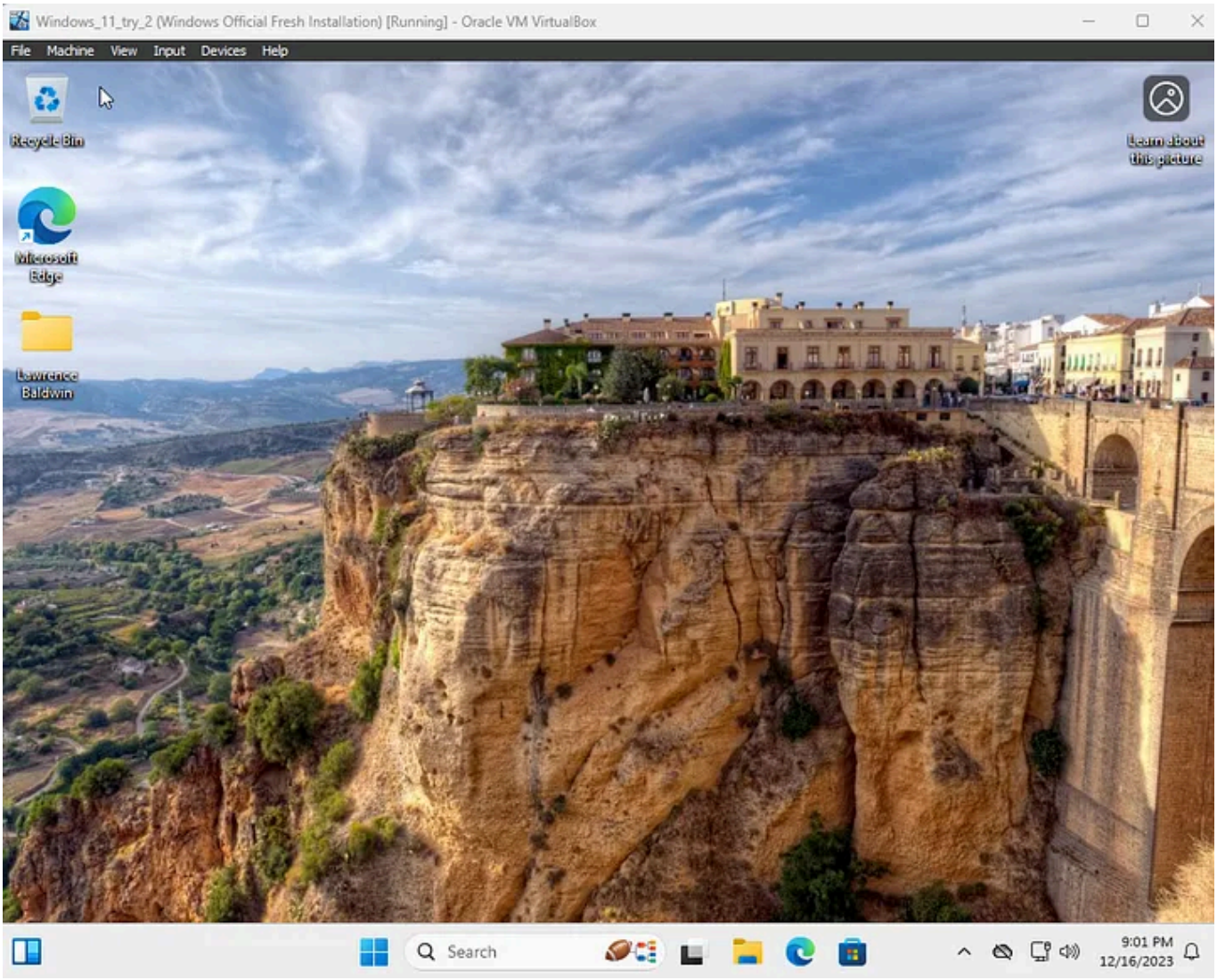
Installation and Setup

In this project, I use VirtualBox, a Type-2 Hypervisor running a fresh windows 11 virtual machine. After downloading VirtualBox, download the Windows 11 Iso file from the official Microsoft website. Next, in VirtualBox click **new**, then import the windows 11 iso file, start the virtual machines installation process, go through the setup, and create your first user with a secure password, name the user **Admin**, and it will be administrator as default.

VirtualBox download



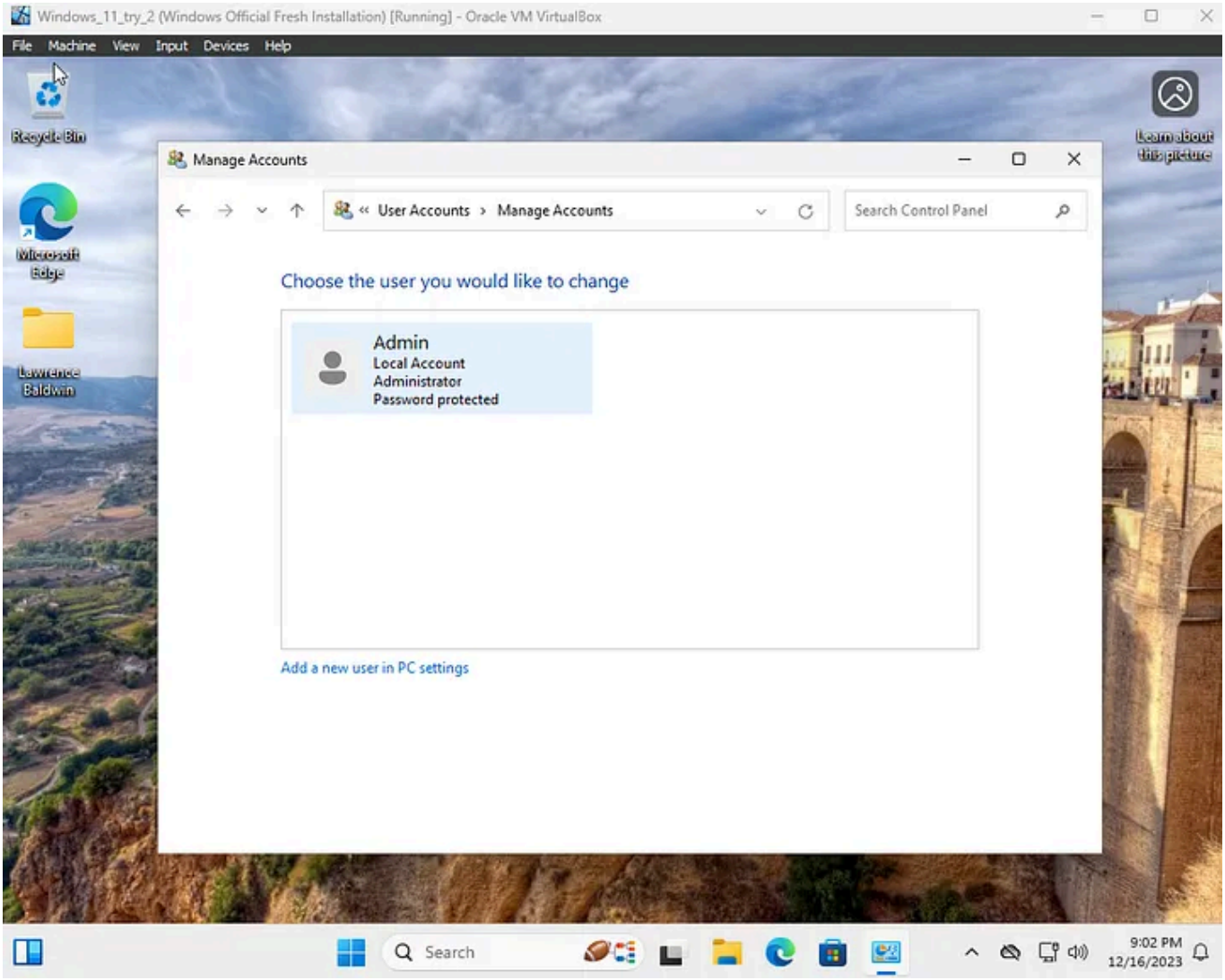
Windows 11 iso download

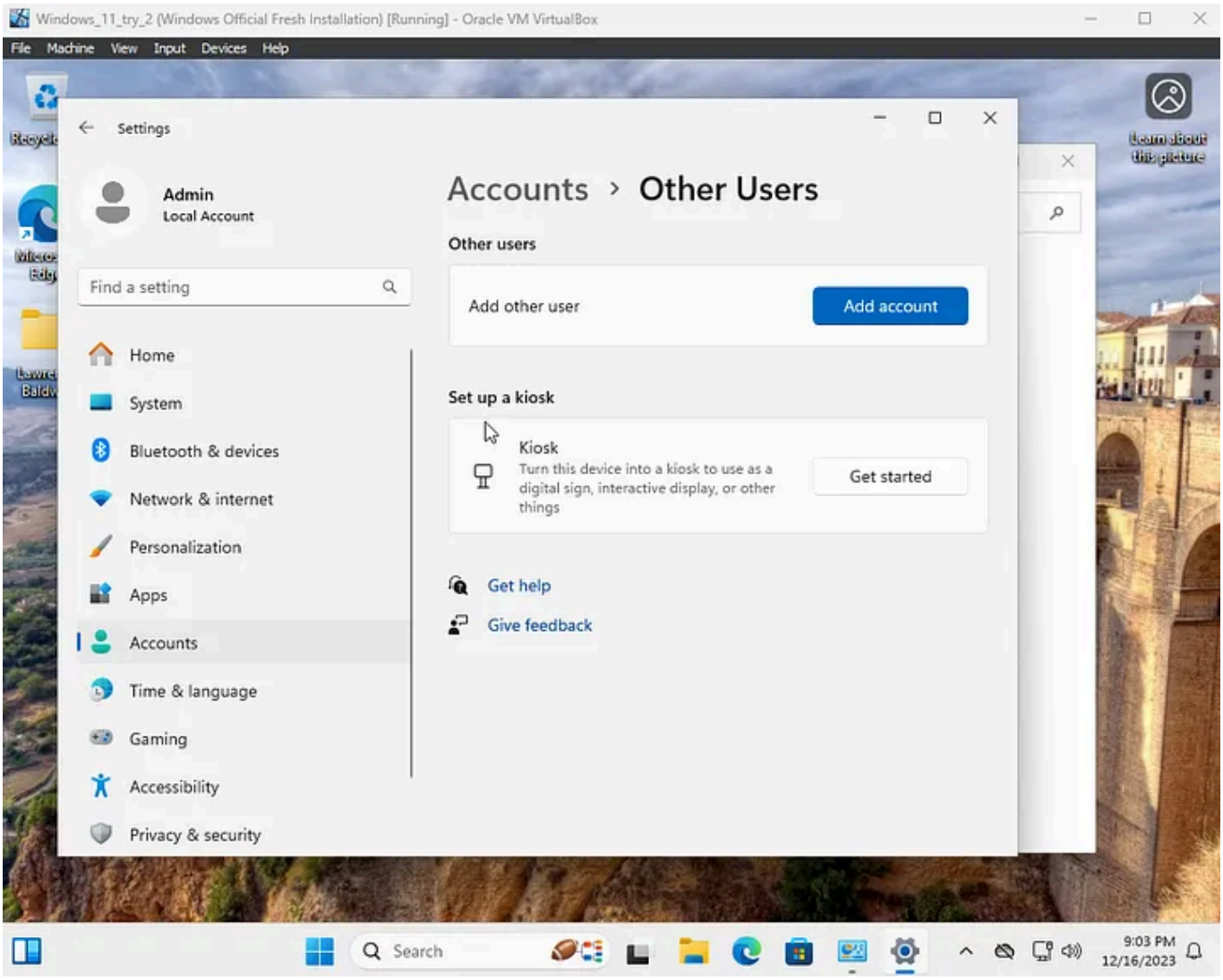


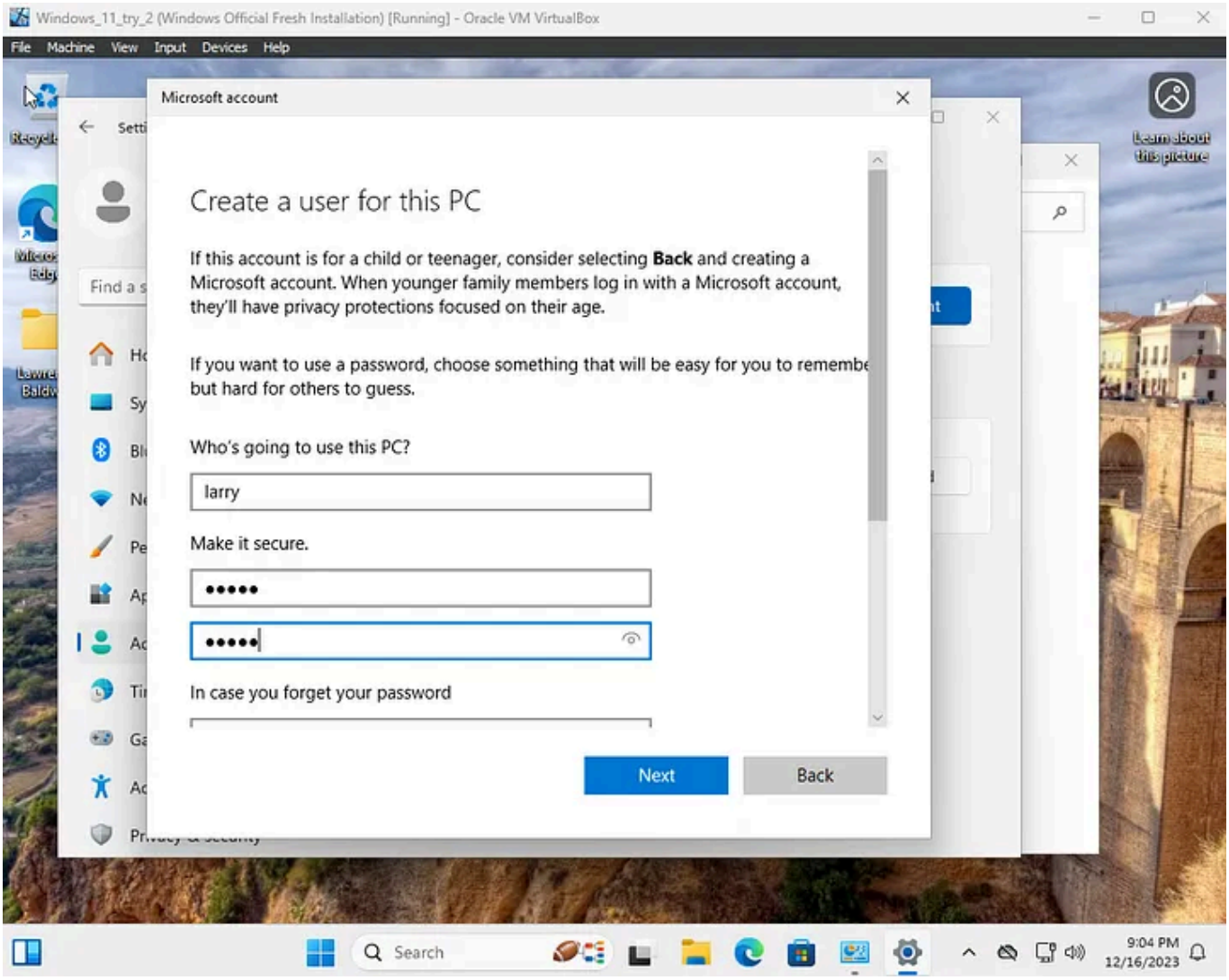
Windows 11 fresh home screen on the Admin account

User Account Control and Setup

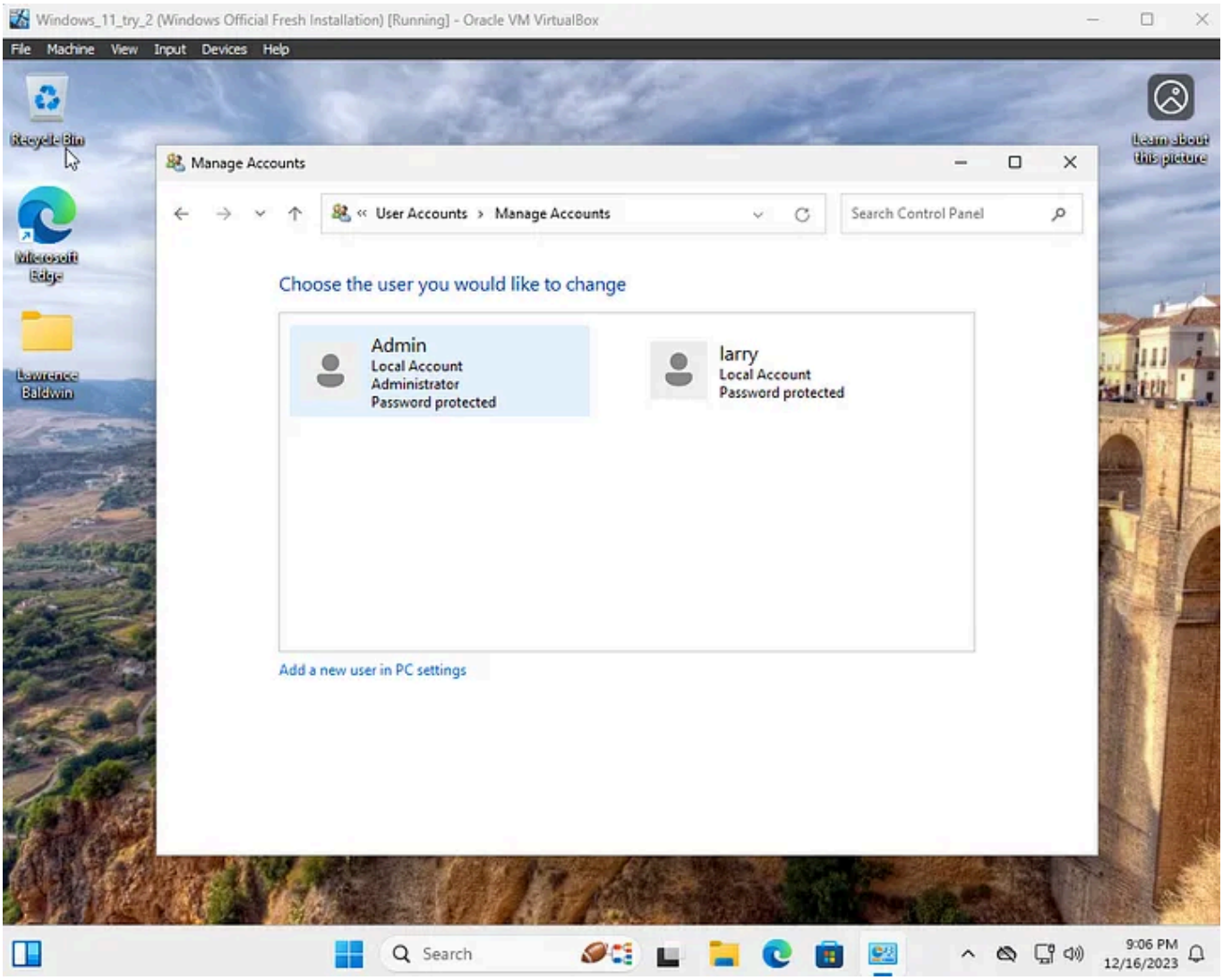
Now on the windows machine the first step is to create a standard user for daily use. This makes your machine more secure for daily use, and before being able to download or make any changes to the pc you must input the administrator password from the admin account. The setting to manage user accounts is **Control Panel** > **User Accounts** > **Manage another account** > **Add a new user in PC settings.** For the last setting search in settings user access control to find it. Then move the User Access Control (UAC) slider to the top to notify you when any changes happen to your computer and sometimes stop unwanted software changes or malicious programs.


Windows_11_try_2 (Windows Official Fresh Installation) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
Lawrence Baldwin
Learn about this picture
Manage Accounts
« User Accounts › Manage Accounts
Search Control Panel
Choose the user you would like to change
Admin
Local Account
Administrator
Password protected
Add a new user in PC settings
Search
9:02 PM
12/16/2023

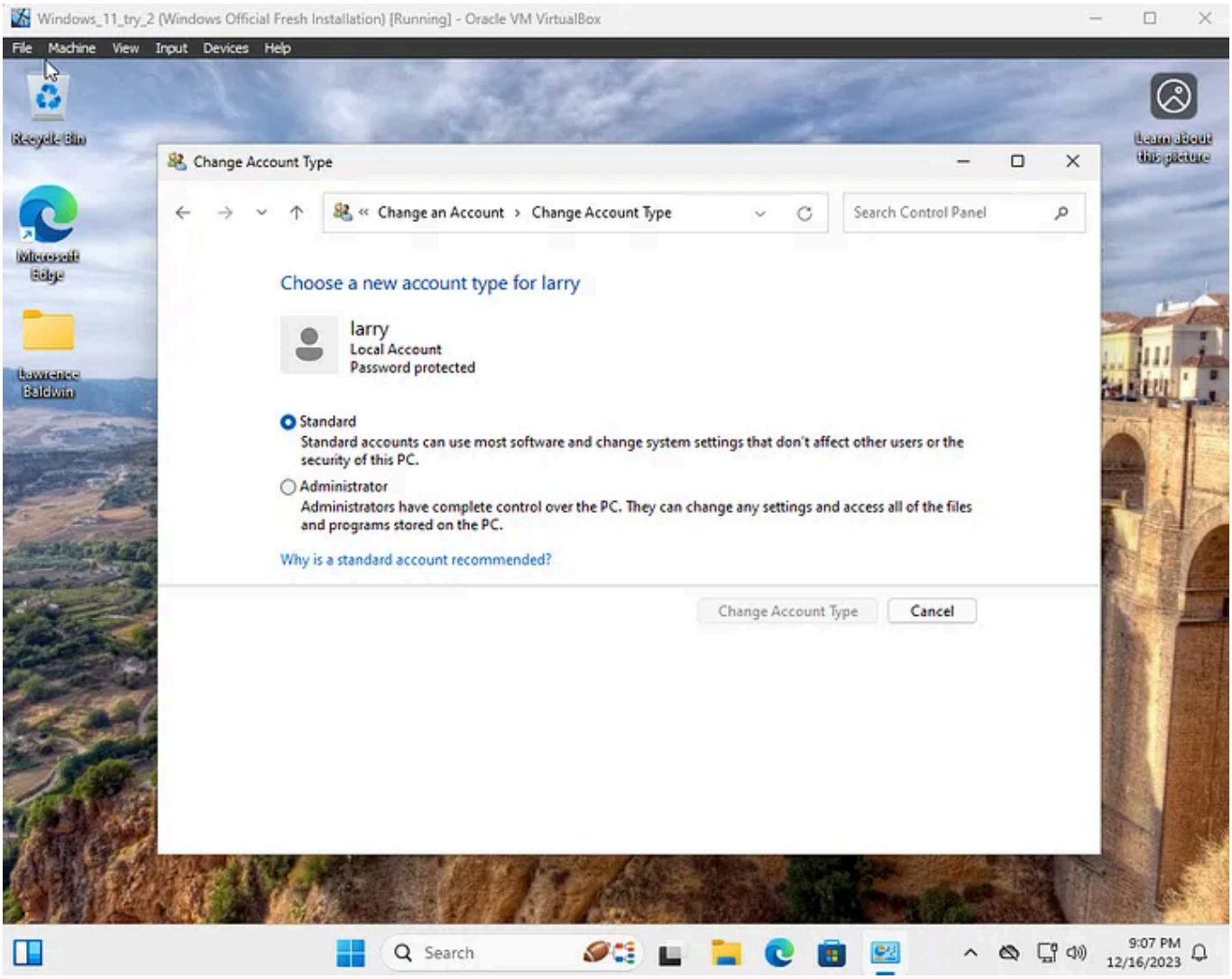

Windows_11_try_2 (Windows Official Fresh Installation) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Settings
Admin
Local Account
Find a setting
Home
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Privacy & security
Accounts › Other Users
Other users
Add other user
Add account
Set up a kiosk
Kiosk
Turn this device into a kiosk to use as a digital sign, interactive display, or other things
Get started
Get help
Give feedback
Learn about this picture
Search
9:03 PM
12/16/2023



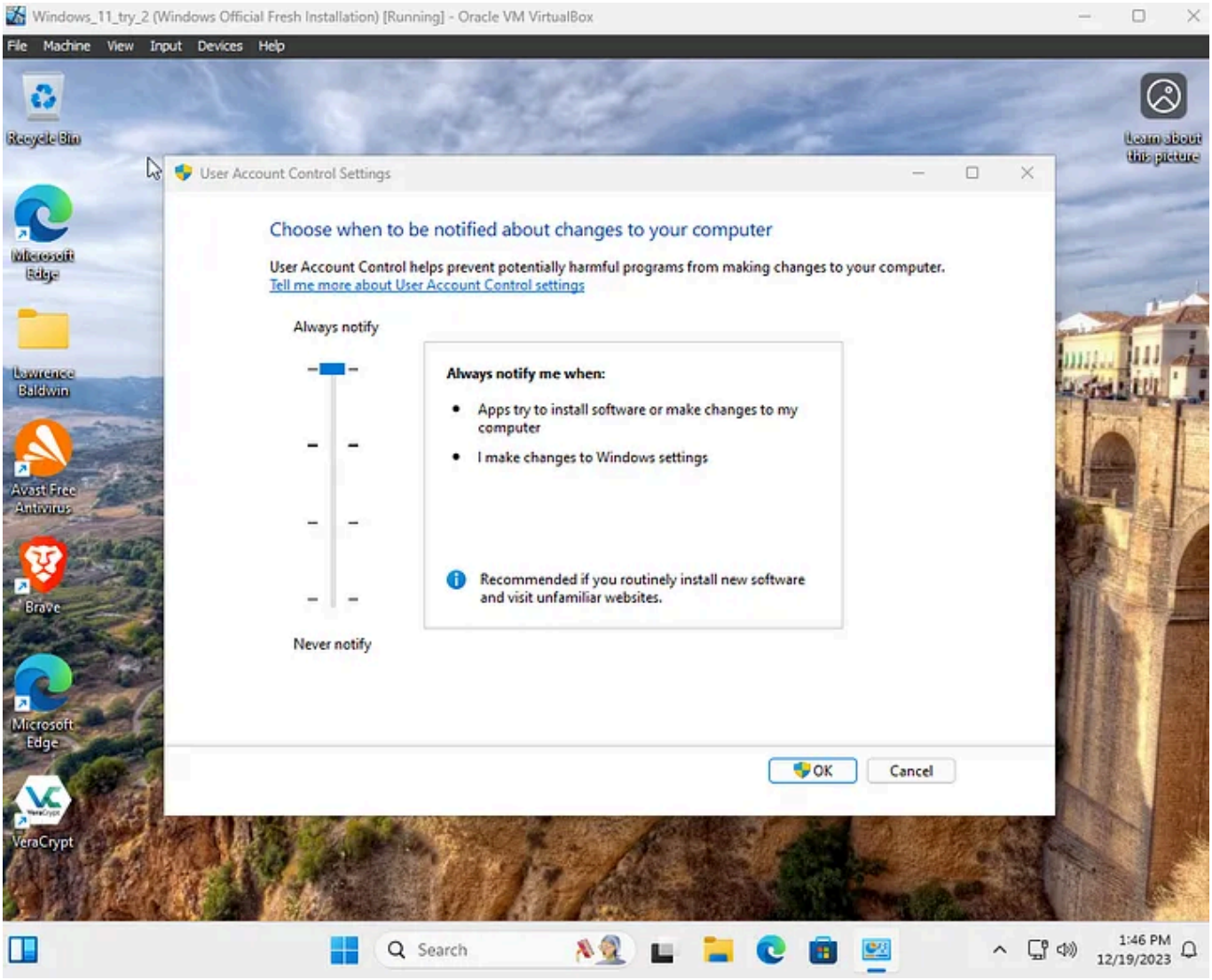
creating new standard user



shows the administrator account on the left, and the new standard user on the right



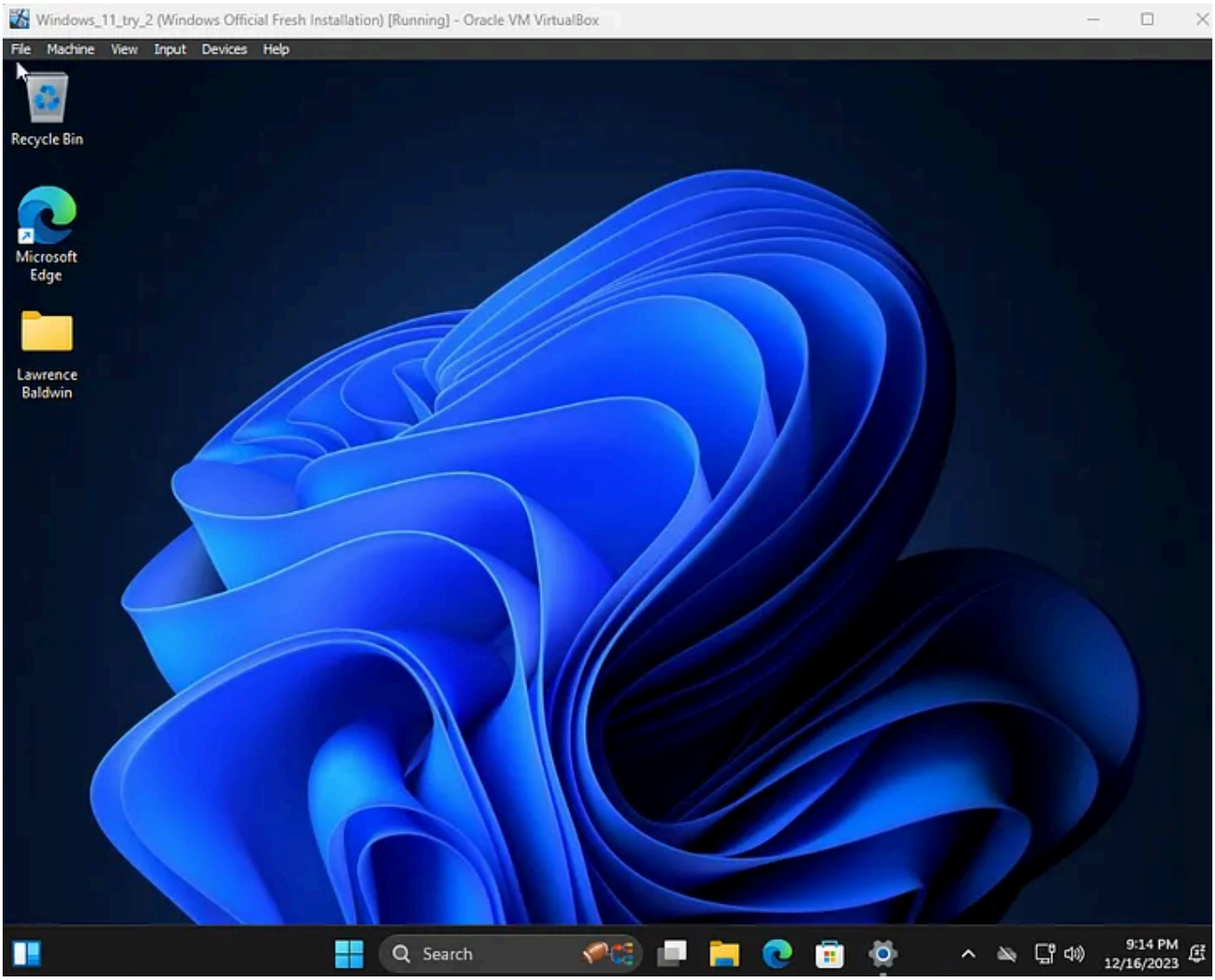
Showing the new standard user account



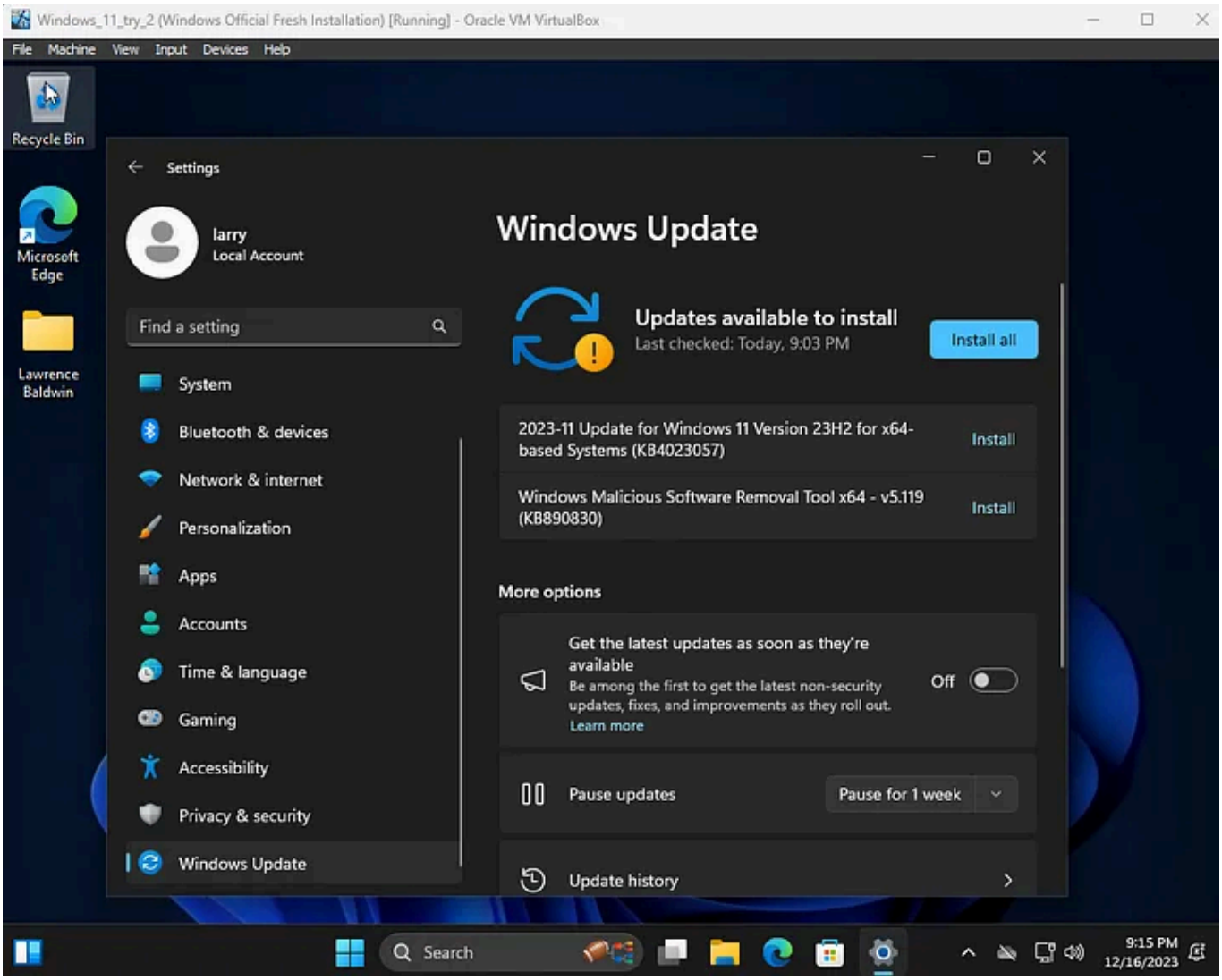
User Access Control (UAC) slider

System Updates

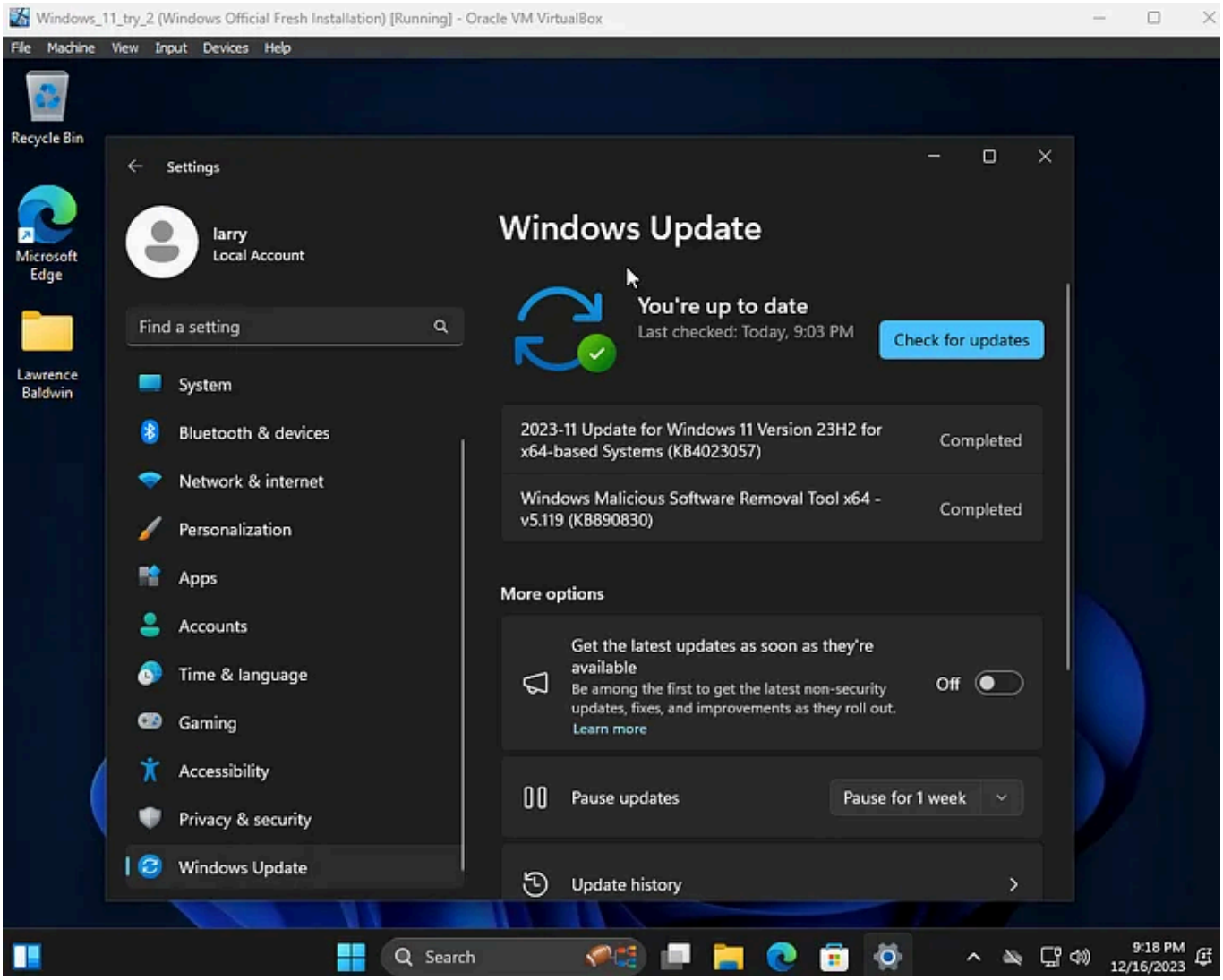
It is important to always keep your operating system up to date to ensure you have the latest security updates. Now on the standard user, go to **Settings** > **Windows Update** and click **Check for updates** or **install all.**



new standard user home screen



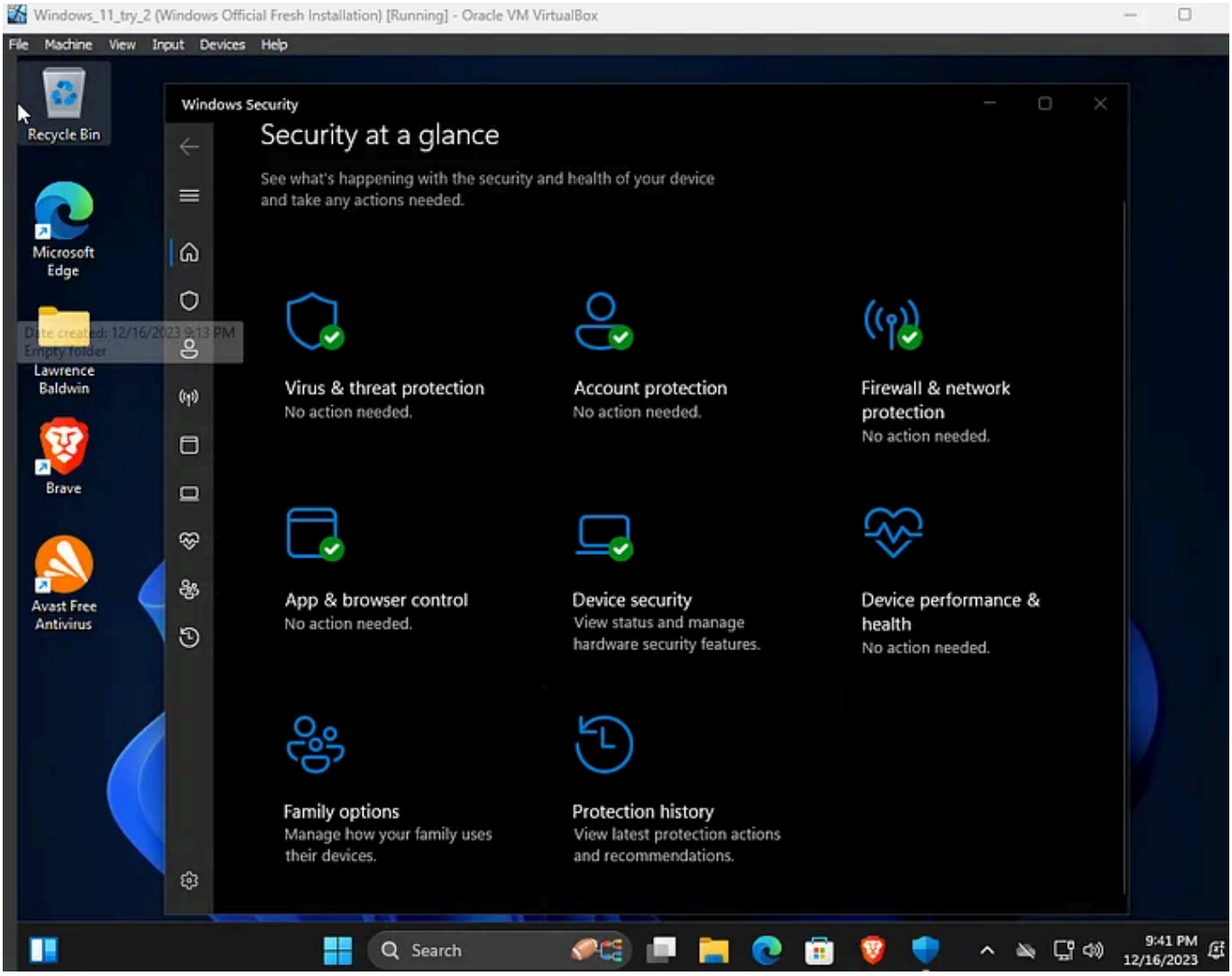
Windows Update screen before updating



Windows Update screen after updating

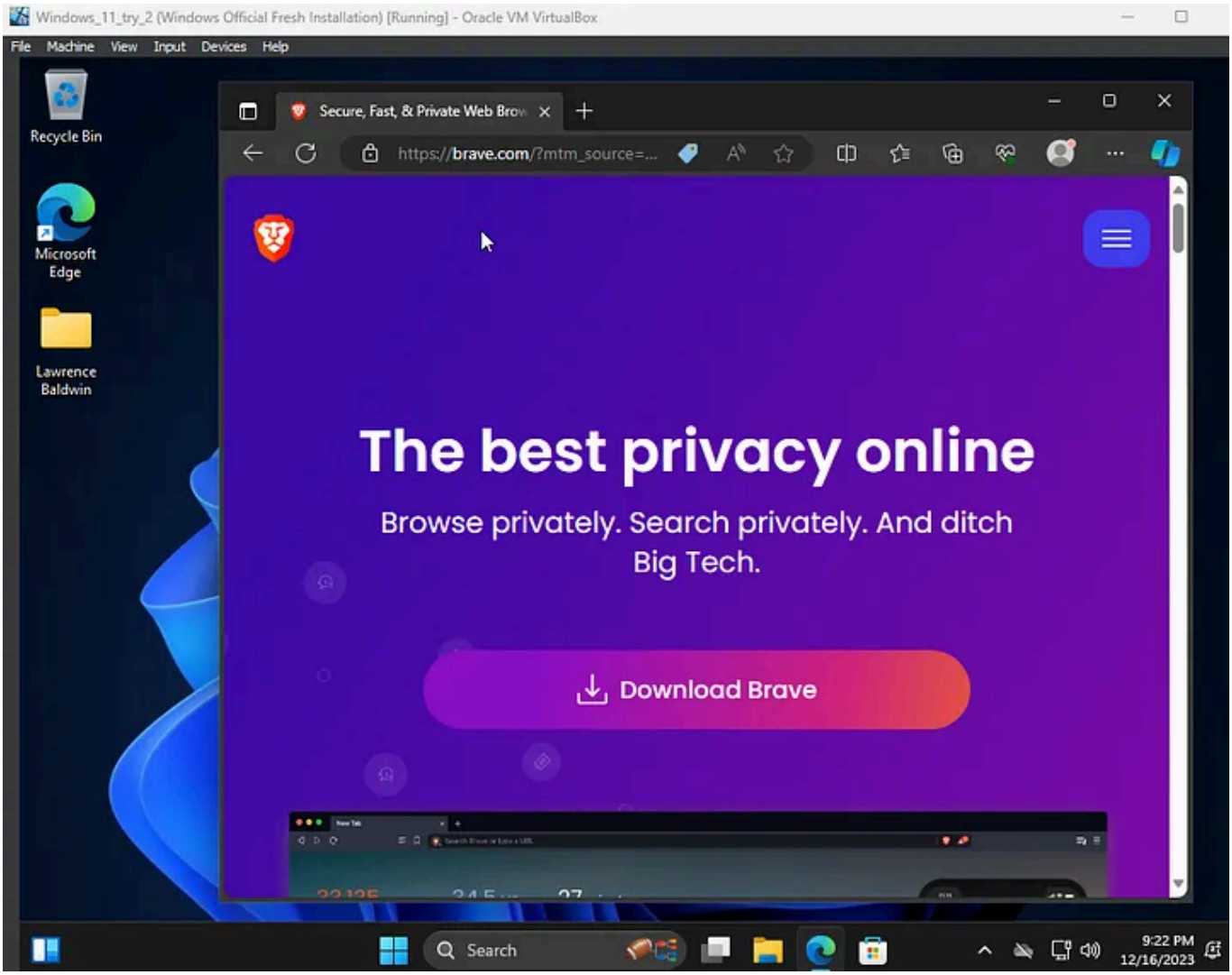
Windows Defender Features

Go to the Windows Security settings to check your security. Make sure everything is on and running with a green check mark. You can click on each section for more information.

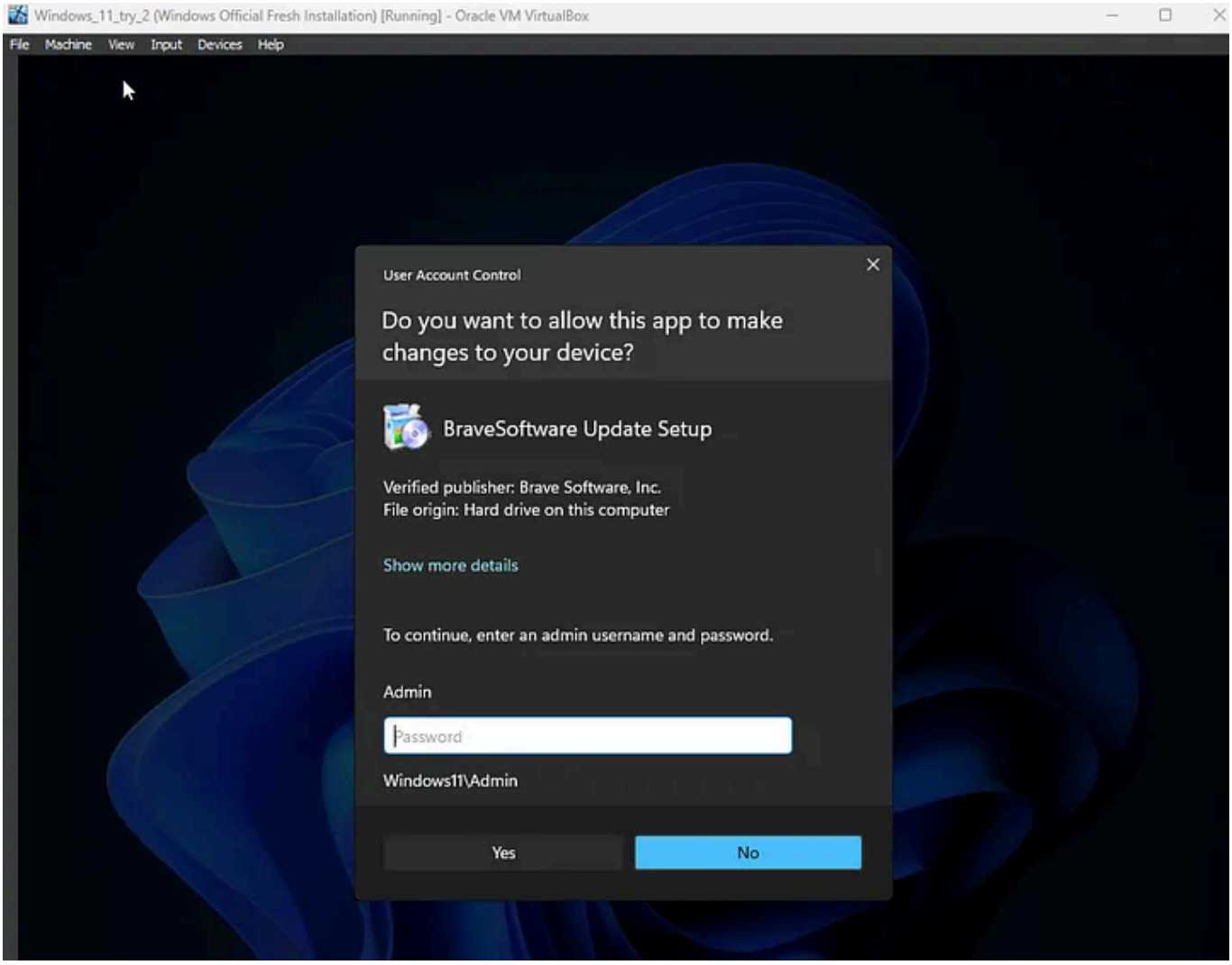


Download and Use a Secure Browser

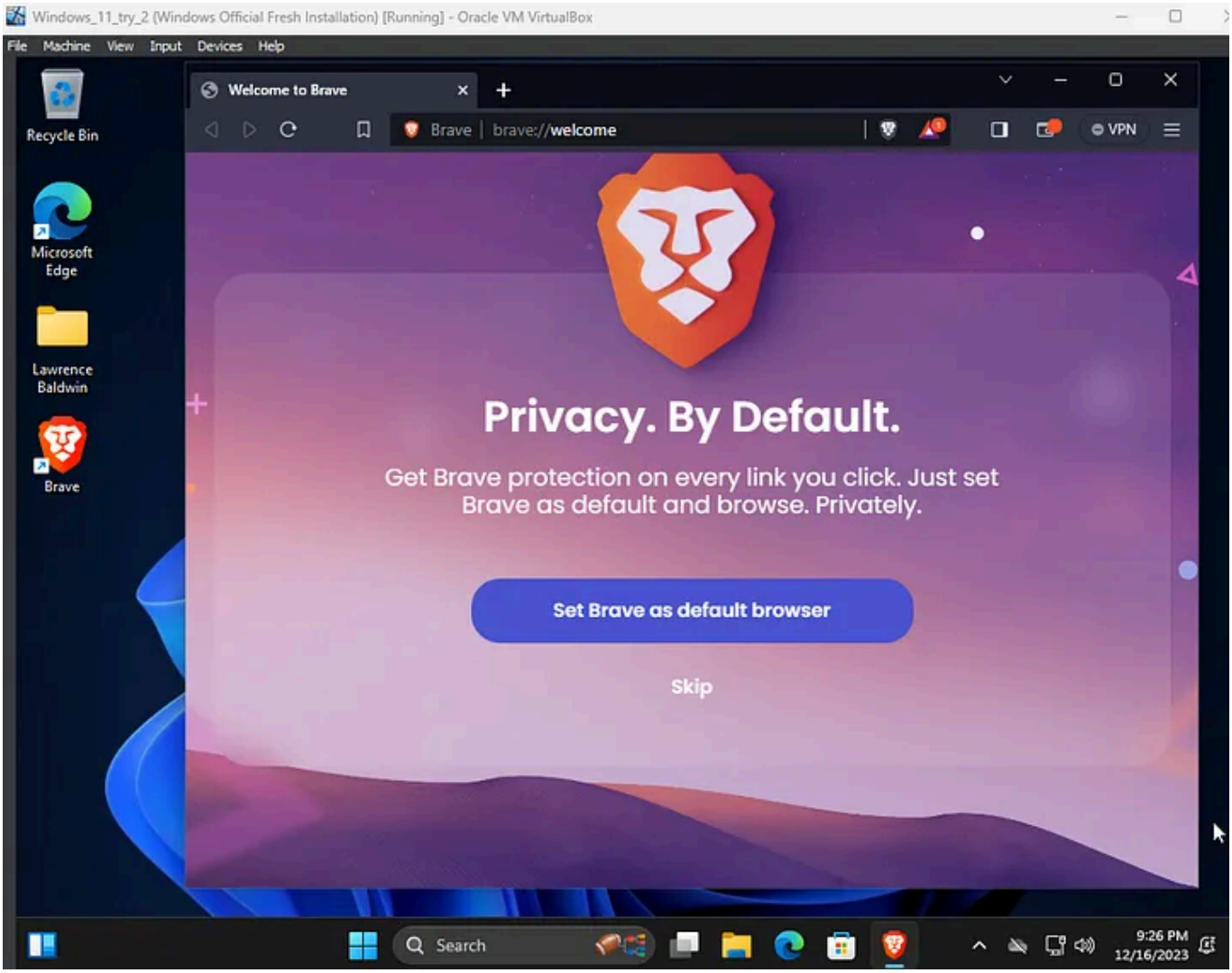
It is always important to use a secure browser. My favorite is Brave Browser, a chromium-based browser which automatically blocks annoying advertisements and popups and has all the same standard security settings as google chrome. I always block third party cookies to stop 3rd parties from tracking my browsing. It is also important to periodically check the site and shield settings in Brave to make sure the shields are on and check if permissions are correct. You may also want to disable JavaScript or only allow it on certain websites if you want enhanced security to avoid XSS type attacks.



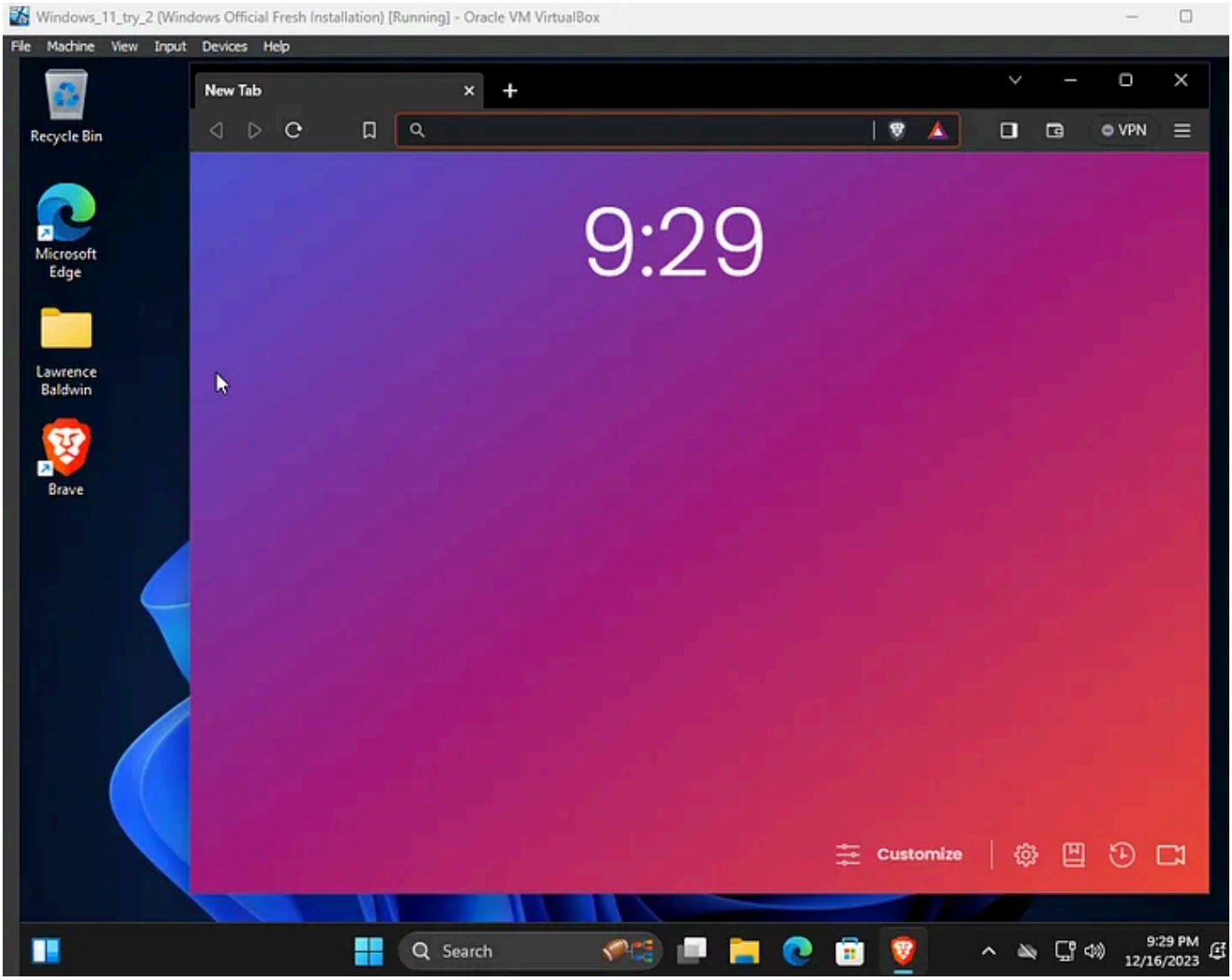
brave download button



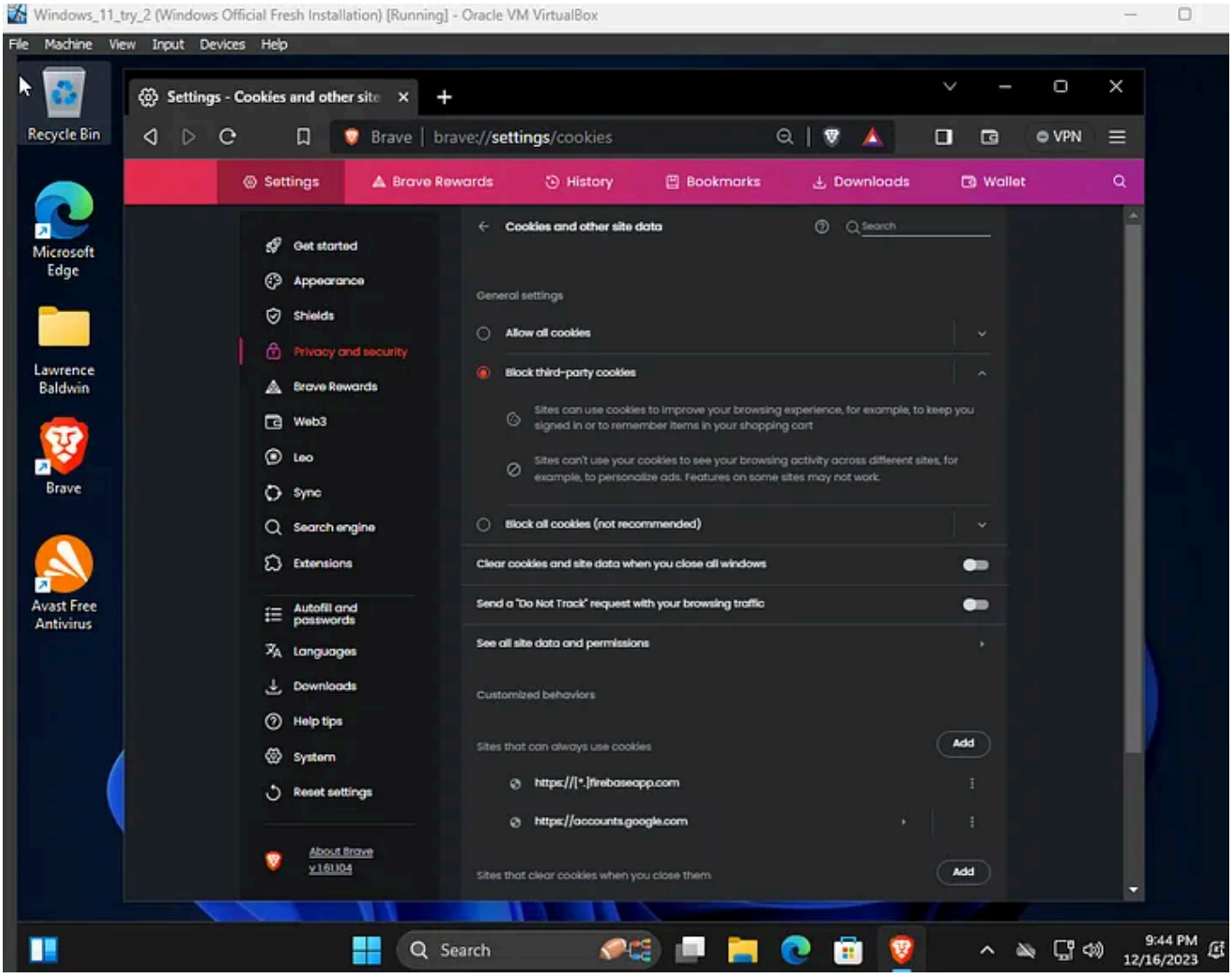
user access control setup



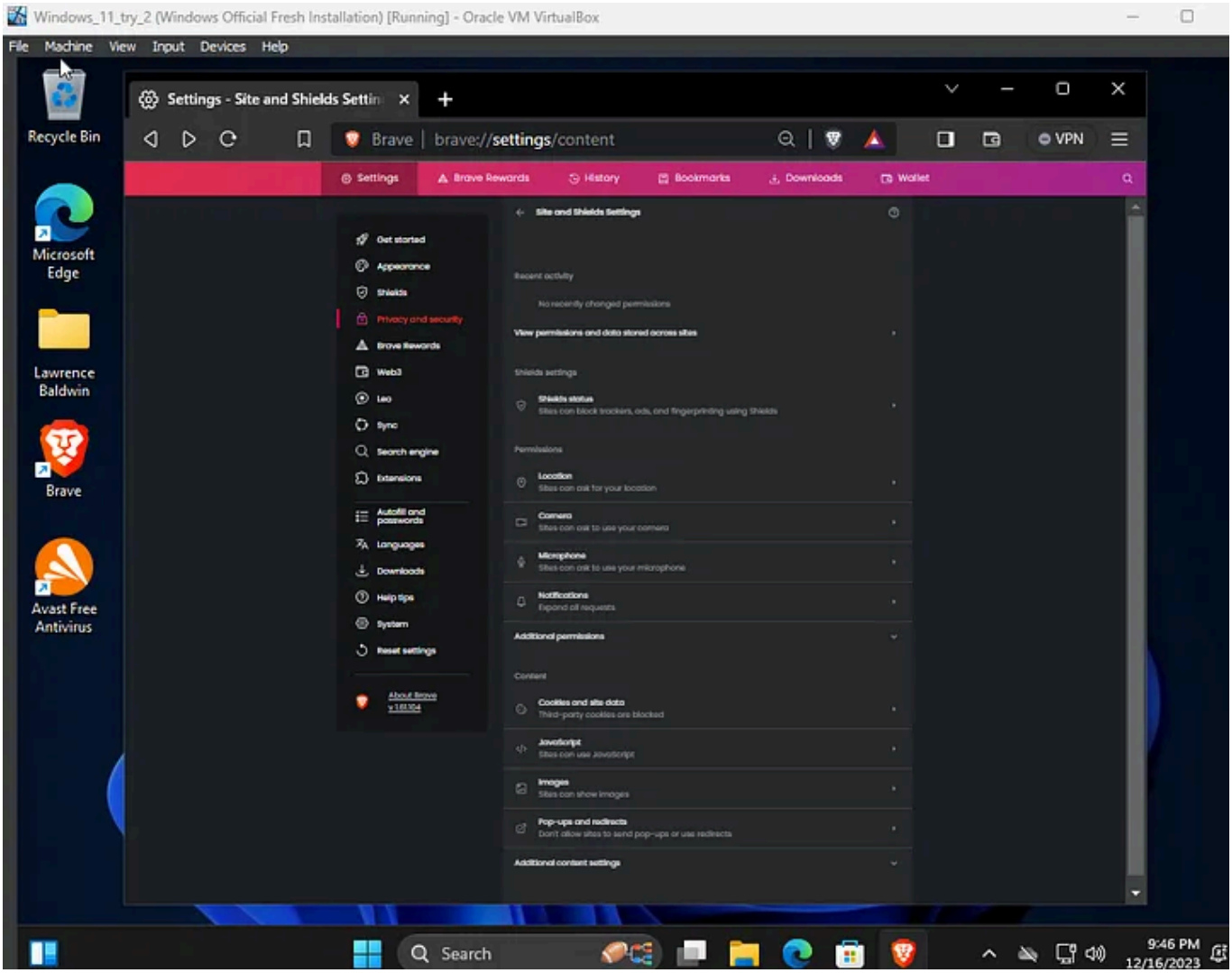
set brave as default browser



brave fresh install screen



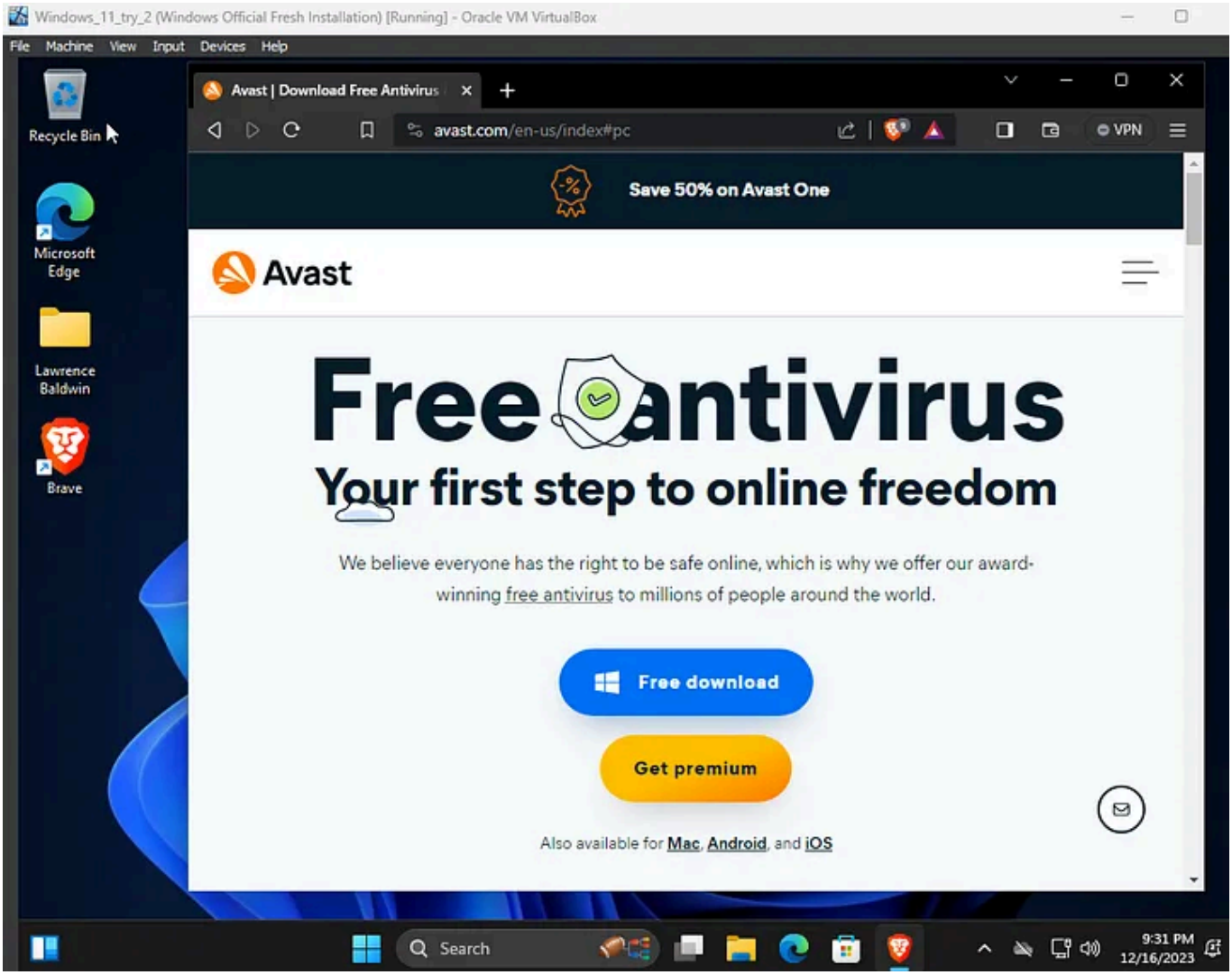
block third-party cookies



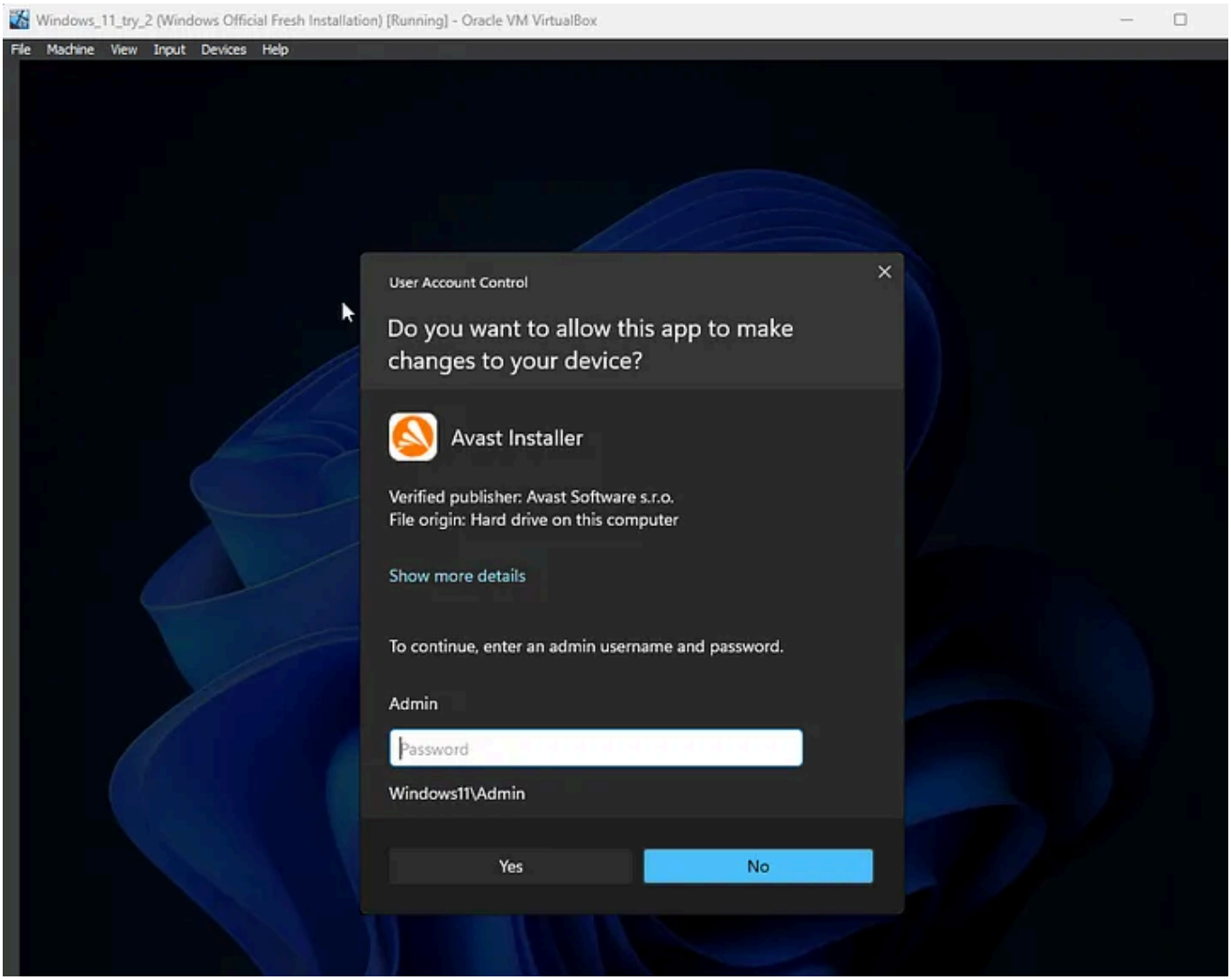
set proper permissions and security settings

Installing Antimalware/Antivirus software

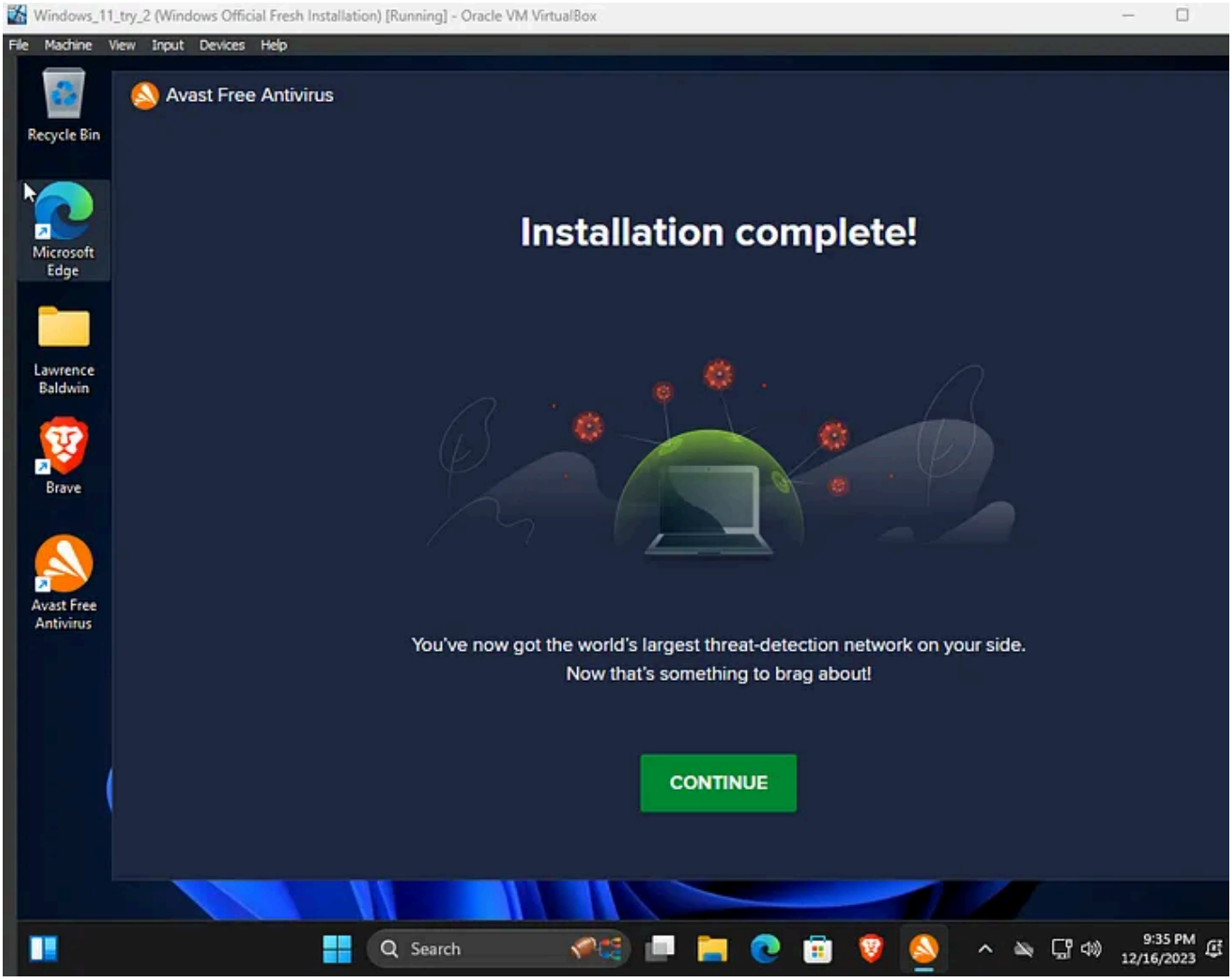
It is advisable to install a host-based antivirus or antimalware application for scanning and blocking malware, and to catch signatures the default windows defender misses. I chose Avast's free antivirus for this project. I downloaded and installed Avast, then clicked scan which detected 2 issues in my system settings, I clicked **Resolve All** to fix the issues, then selected the prompt to schedule a smart scan to run once a month. It is recommended to always turn on periodic scans.

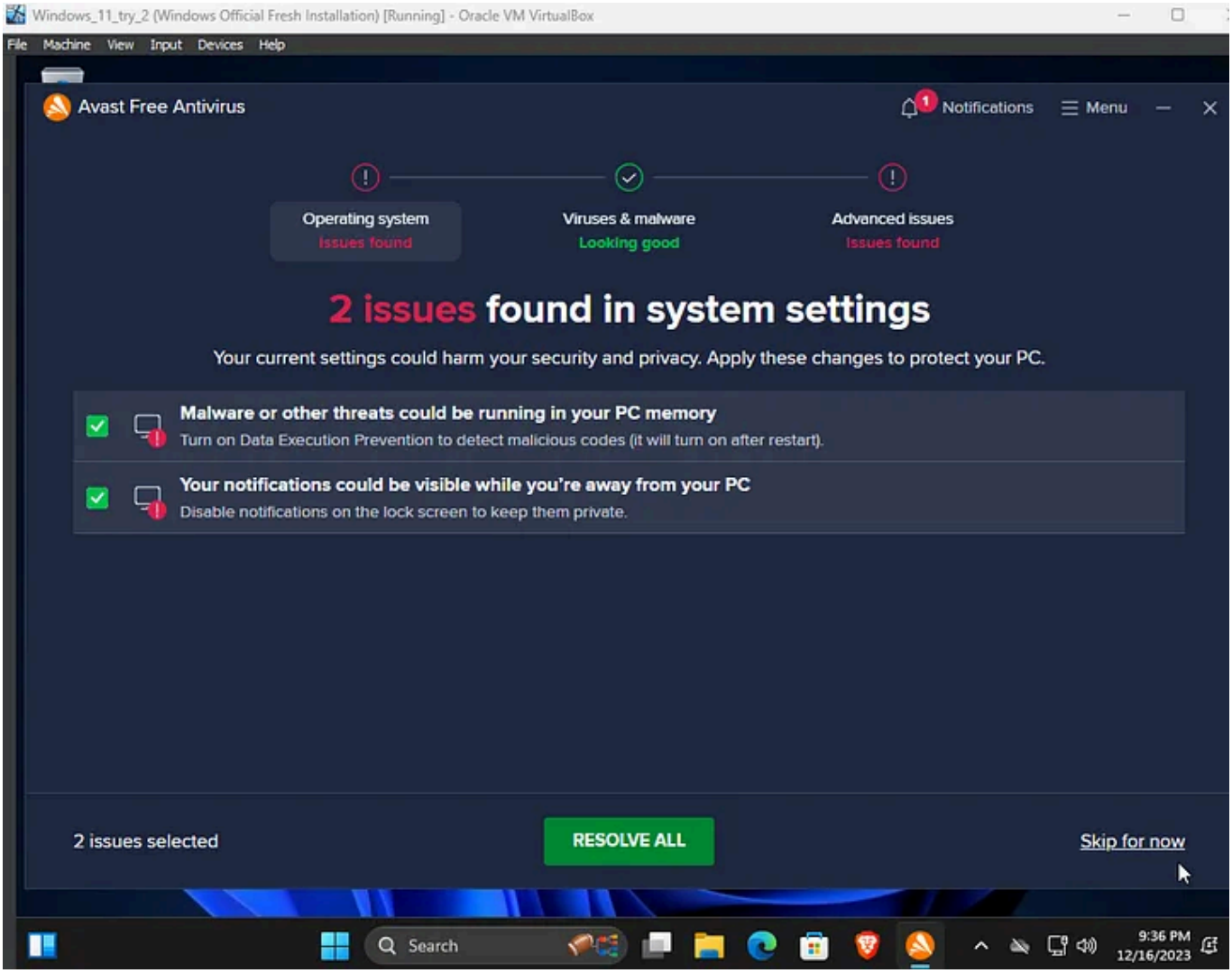


free antivirus download

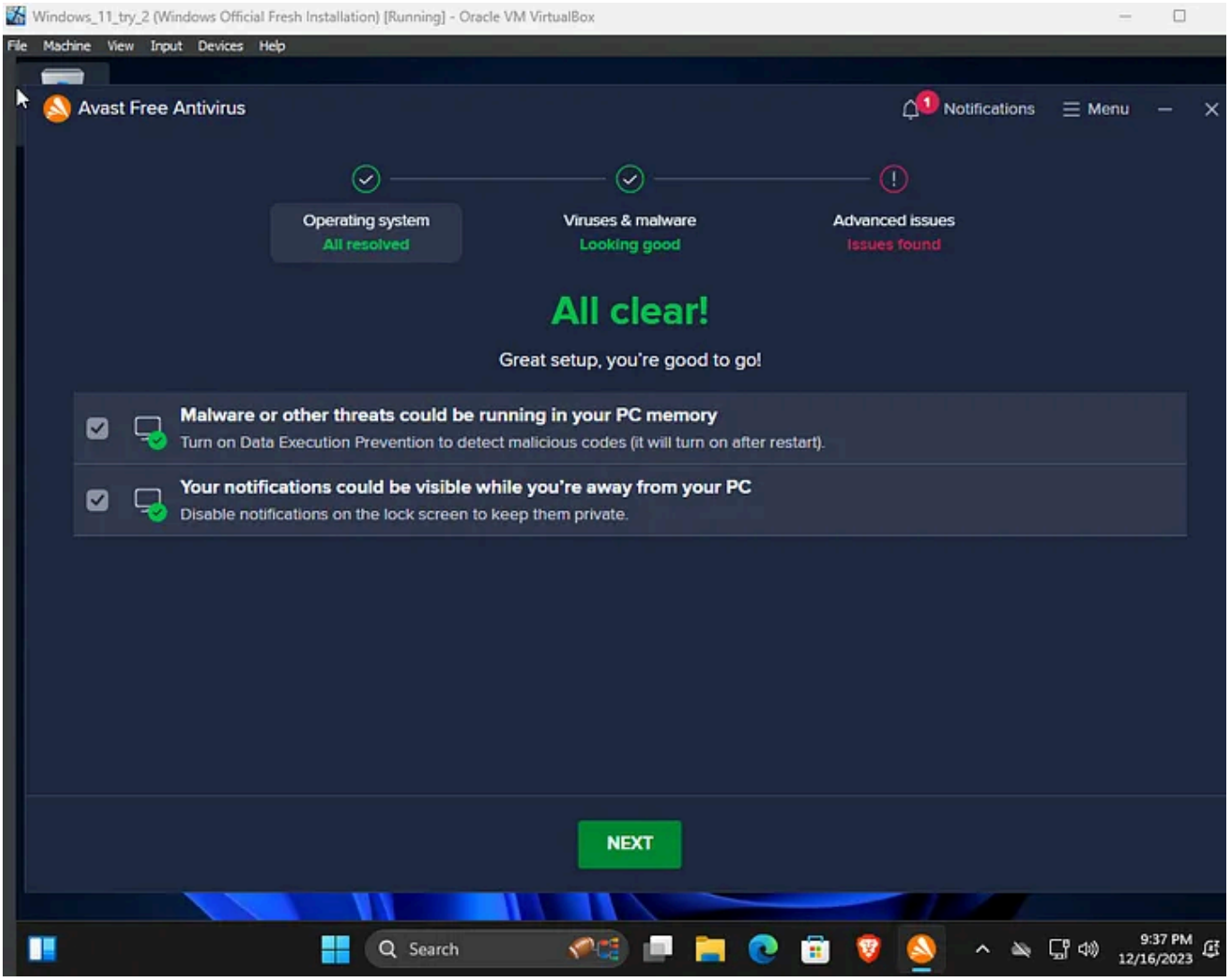


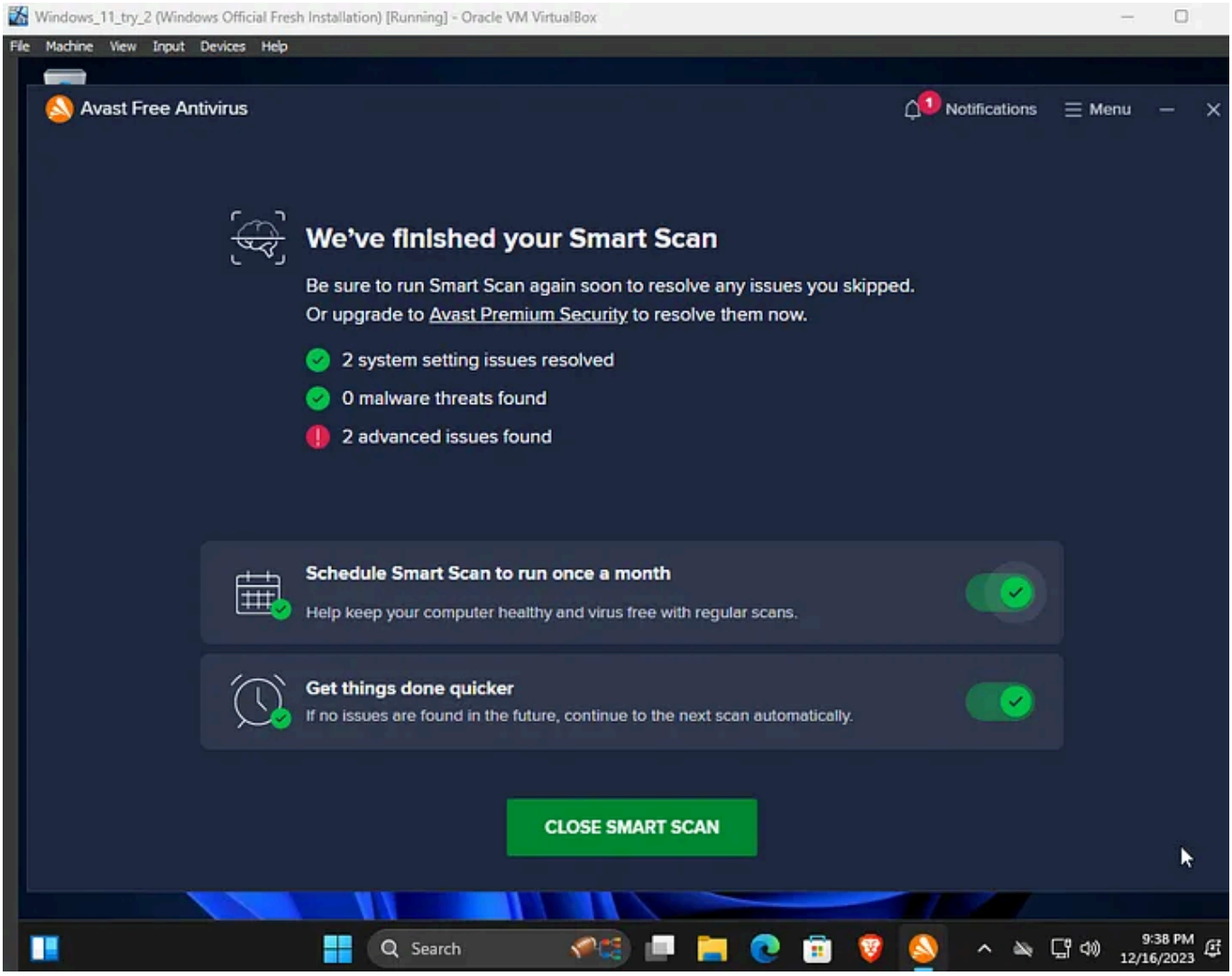
user access control installer


Windows_11_try_2 (Windows Official Fresh Installation) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
Lawrence Baldwin
Brave
Avast Free Antivirus
Avast Free Antivirus
Installation complete!
You've now got the world's largest threat-detection network on your side.
Now that's something to brag about!
CONTINUE
Search
9:35 PM
12/16/2023



resolve any issues


Windows_11_try_2 (Windows Official Fresh Installation) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Avast Free Antivirus
Notifications
Menu
Operating system
All resolved
Viruses & malware
Looking good
Advanced issues
Issues found
All clear!
Great setup, you're good to go!
Malware or other threats could be running in your PC memory
Turn on Data Execution Prevention to detect malicious codes (it will turn on after restart).
Your notifications could be visible while you're away from your PC
Disable notifications on the lock screen to keep them private.
NEXT
Search
9:37 PM
12/16/2023

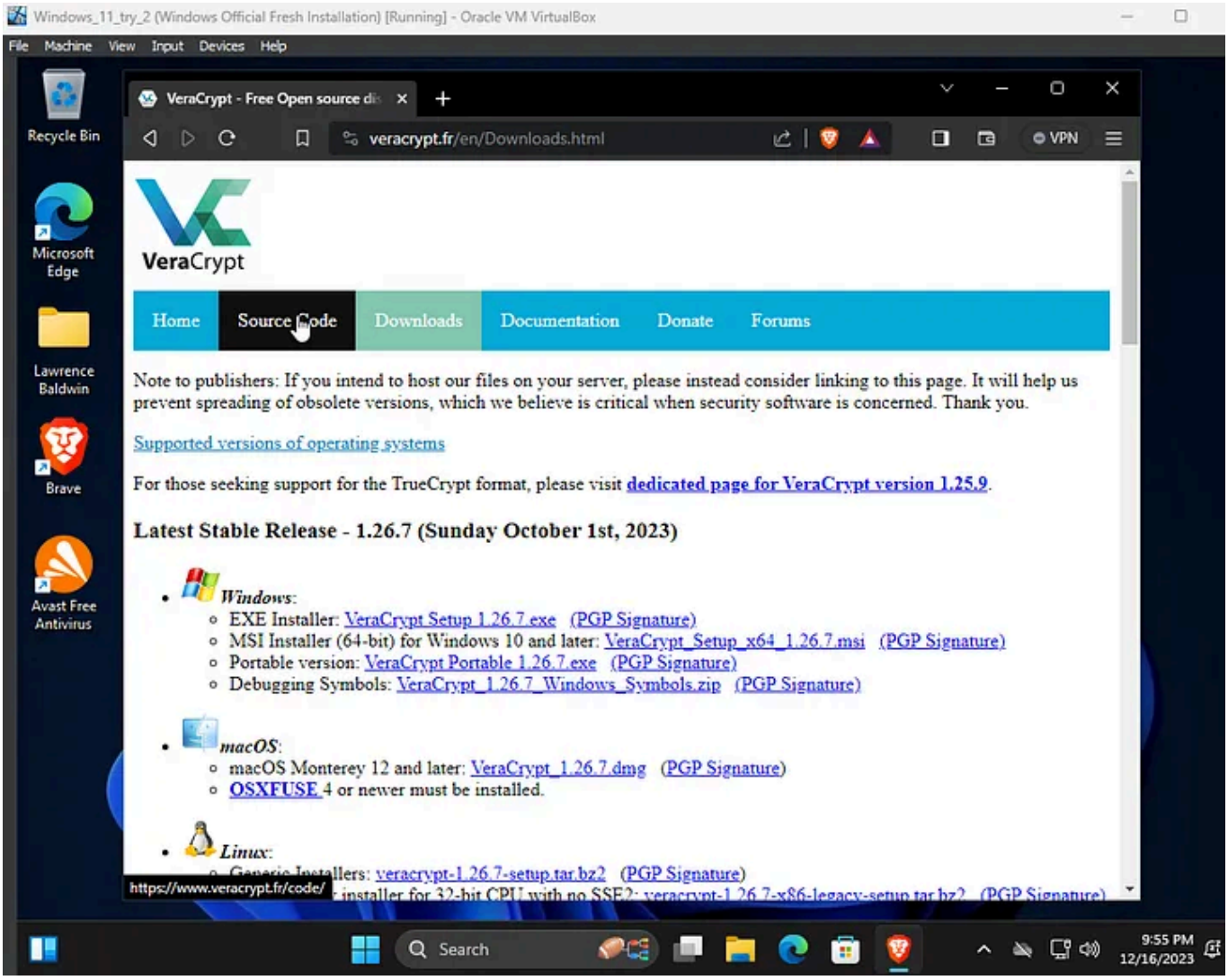


schedule a smart can to run periodically

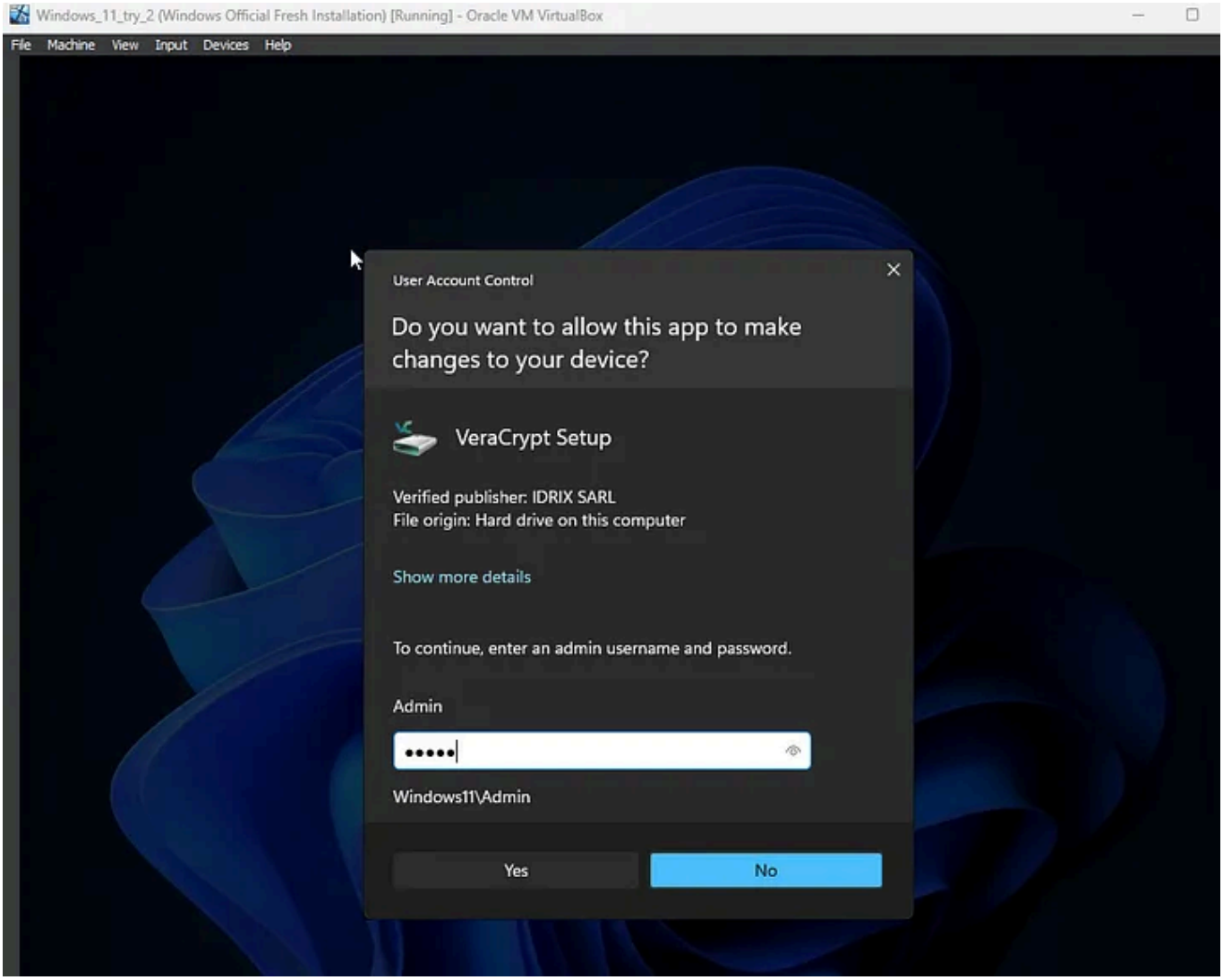
Encryption

Full disk encryption protects your data at rest, securing your entire drive through encryption. This prevents your data from being unauthorized if the machine is physically compromised. For this project I chose VeraCrypt, an open-source encryption tool. First, download and install VeraCrypt, then select **Create Volume** to start the Volume Creation Wizard, choose to encrypt the entire system drive for full disk encryption, or choose the other two options which just encrypt a certain section of the drive. Next, choose **AES**, or another secure encryption algorithm of your choice, and select a secure hashing algorithm, I chose **SHA-512** for this project. Next, input a 20-digit password which will be used to access the disk on startup before the

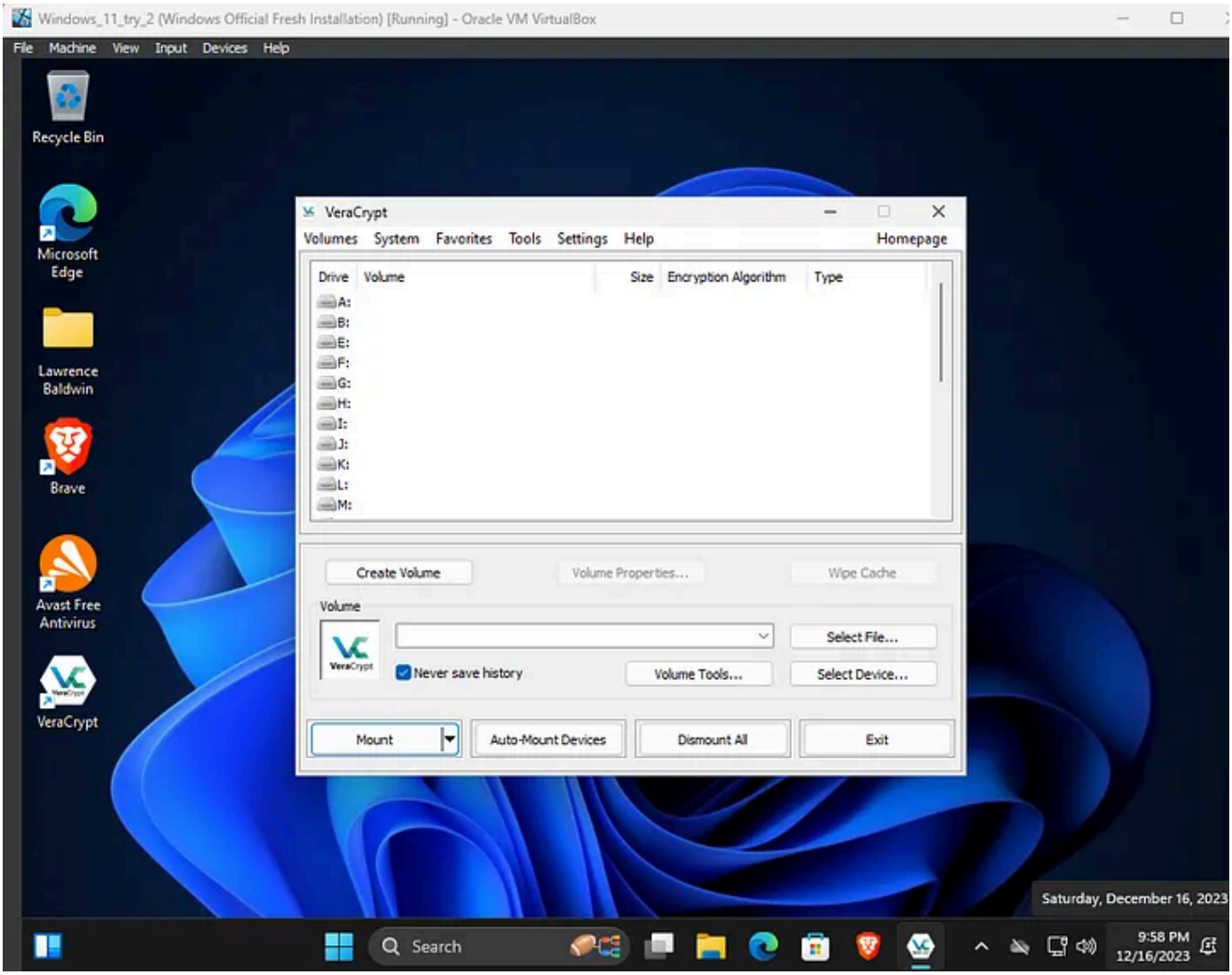
operating system boots. Next, collect the random data by moving your mouse inside the box, then start the pretest. After the pretest finishes, you may click **Encrypt** to start the encryption process!



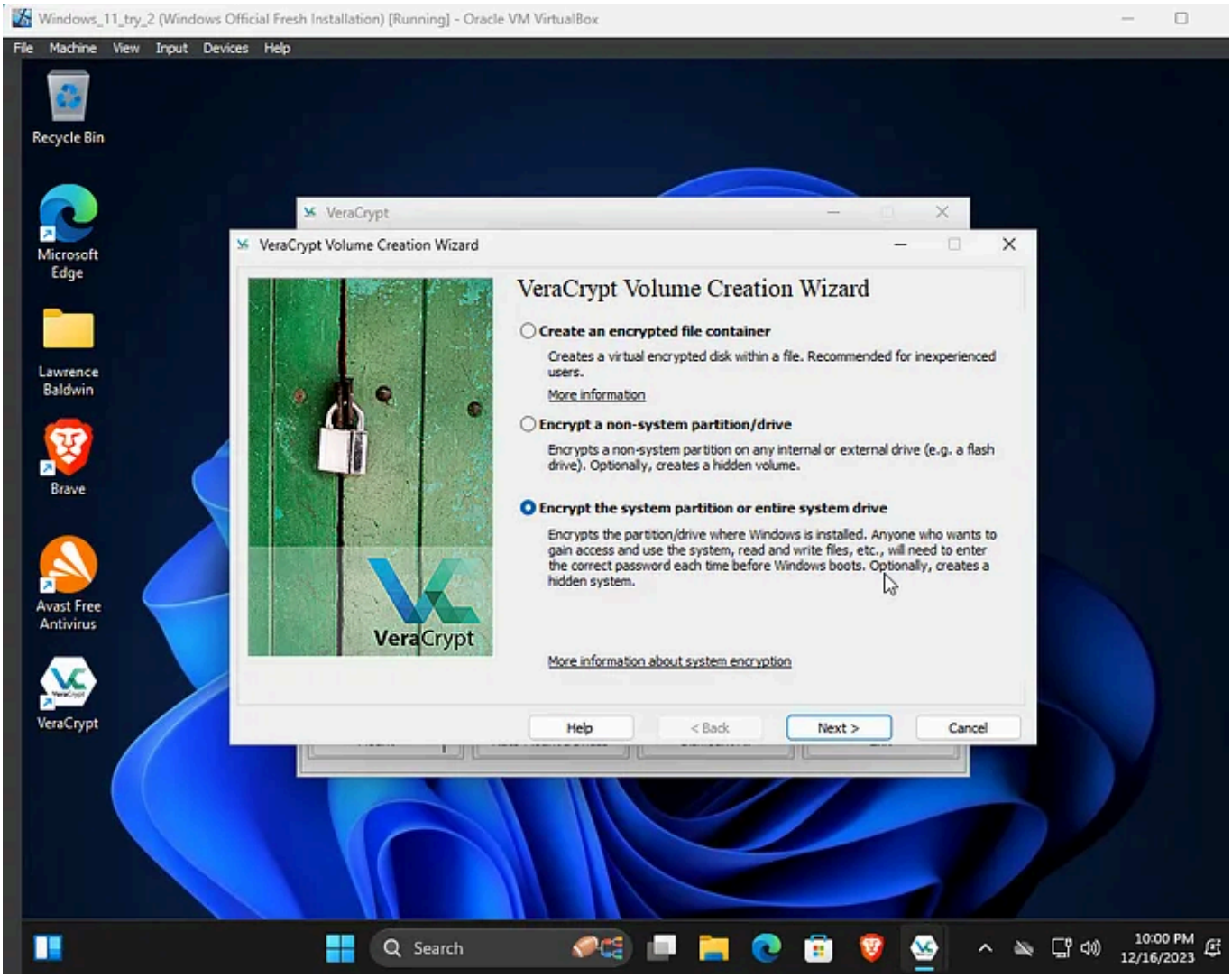
veracrypt download



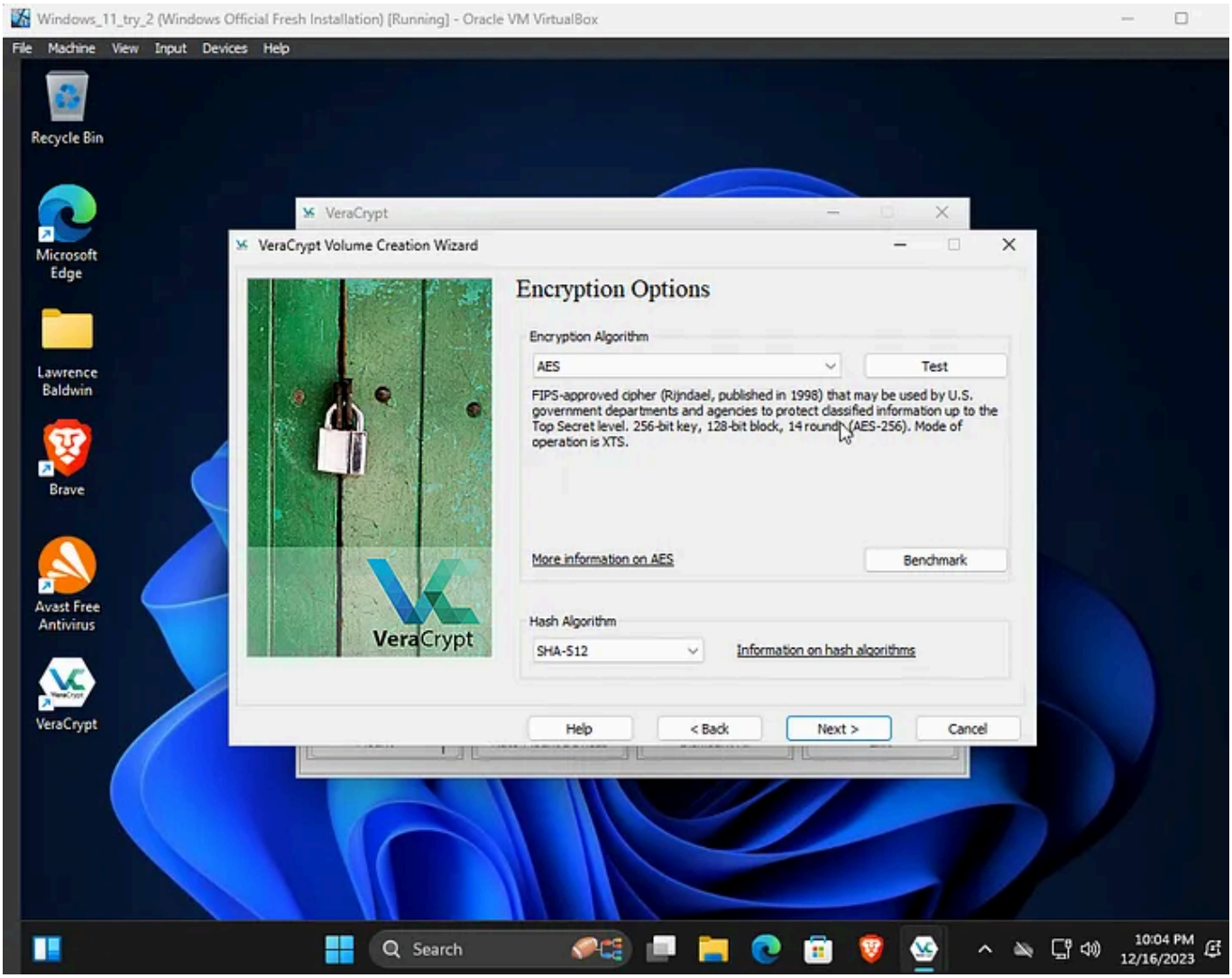
user access control installer

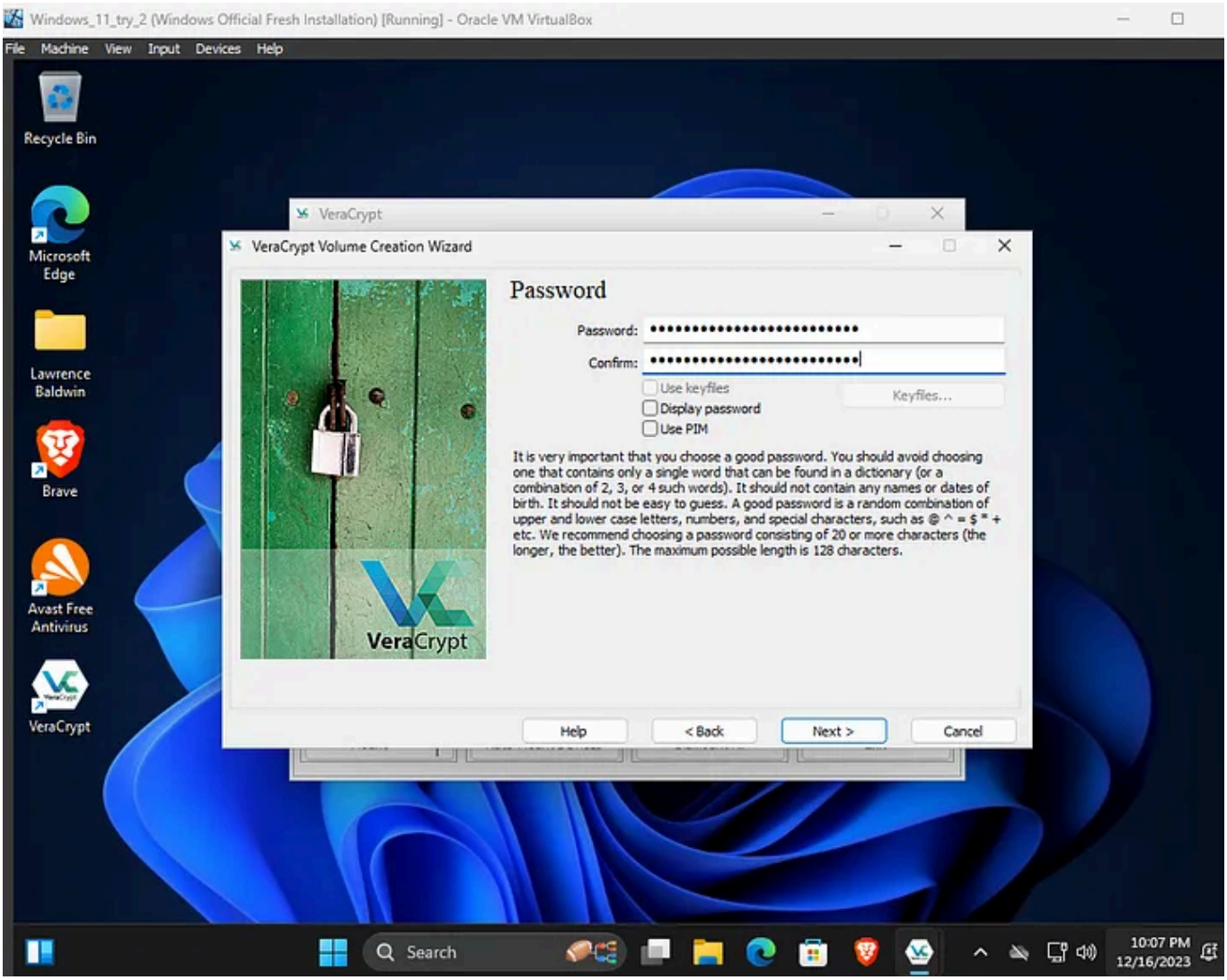


create volume

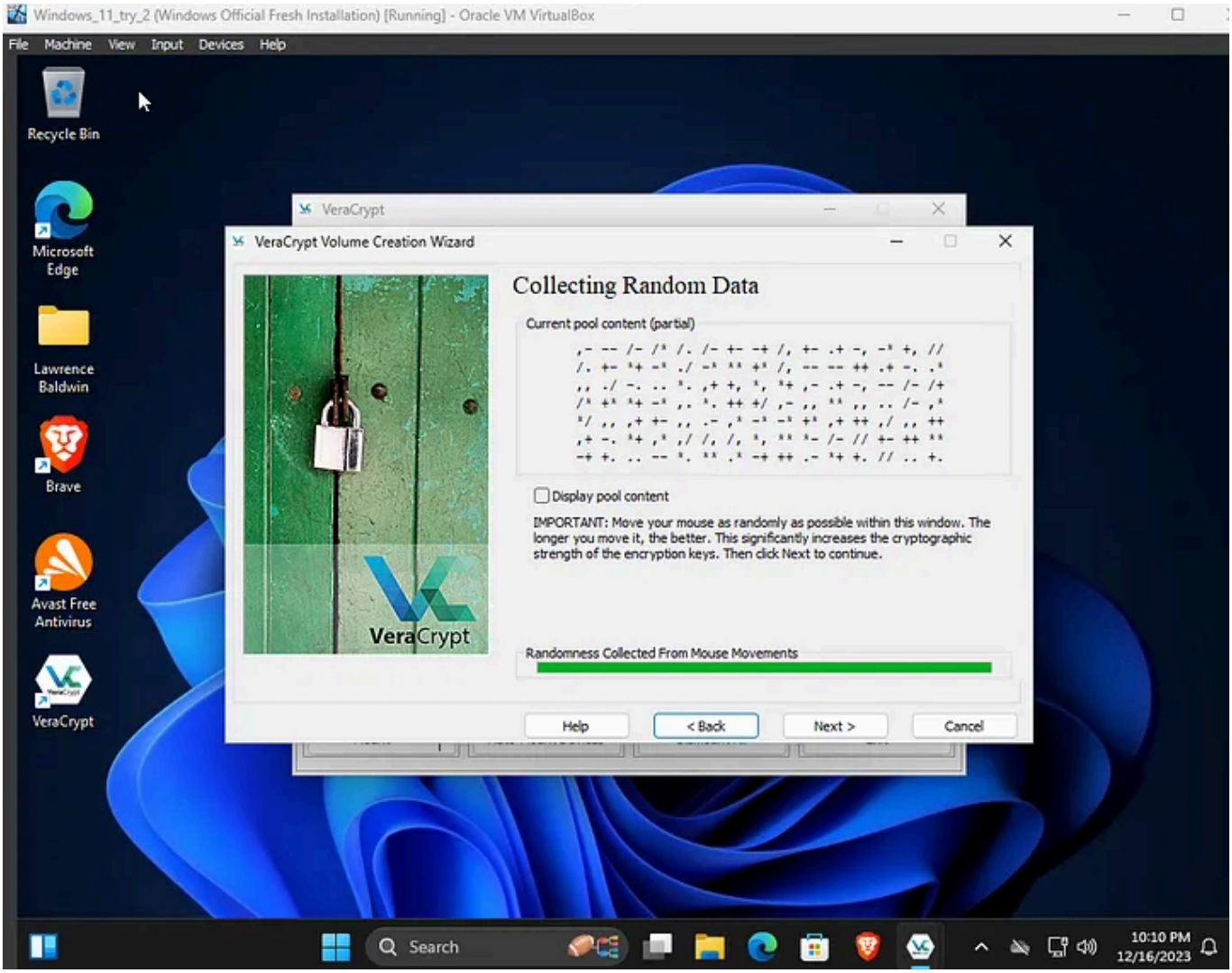


encrypt the whole drive for full disk encryption

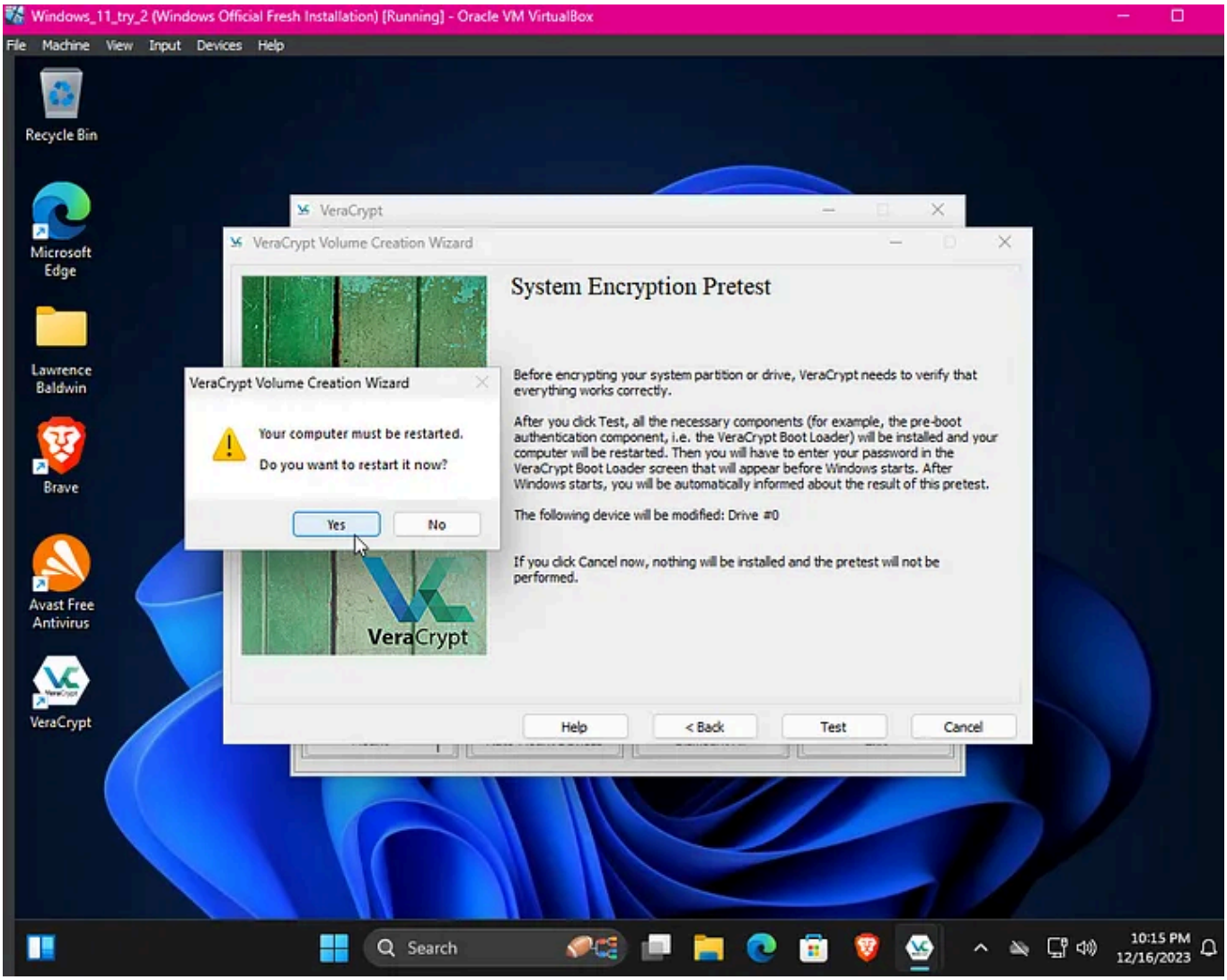




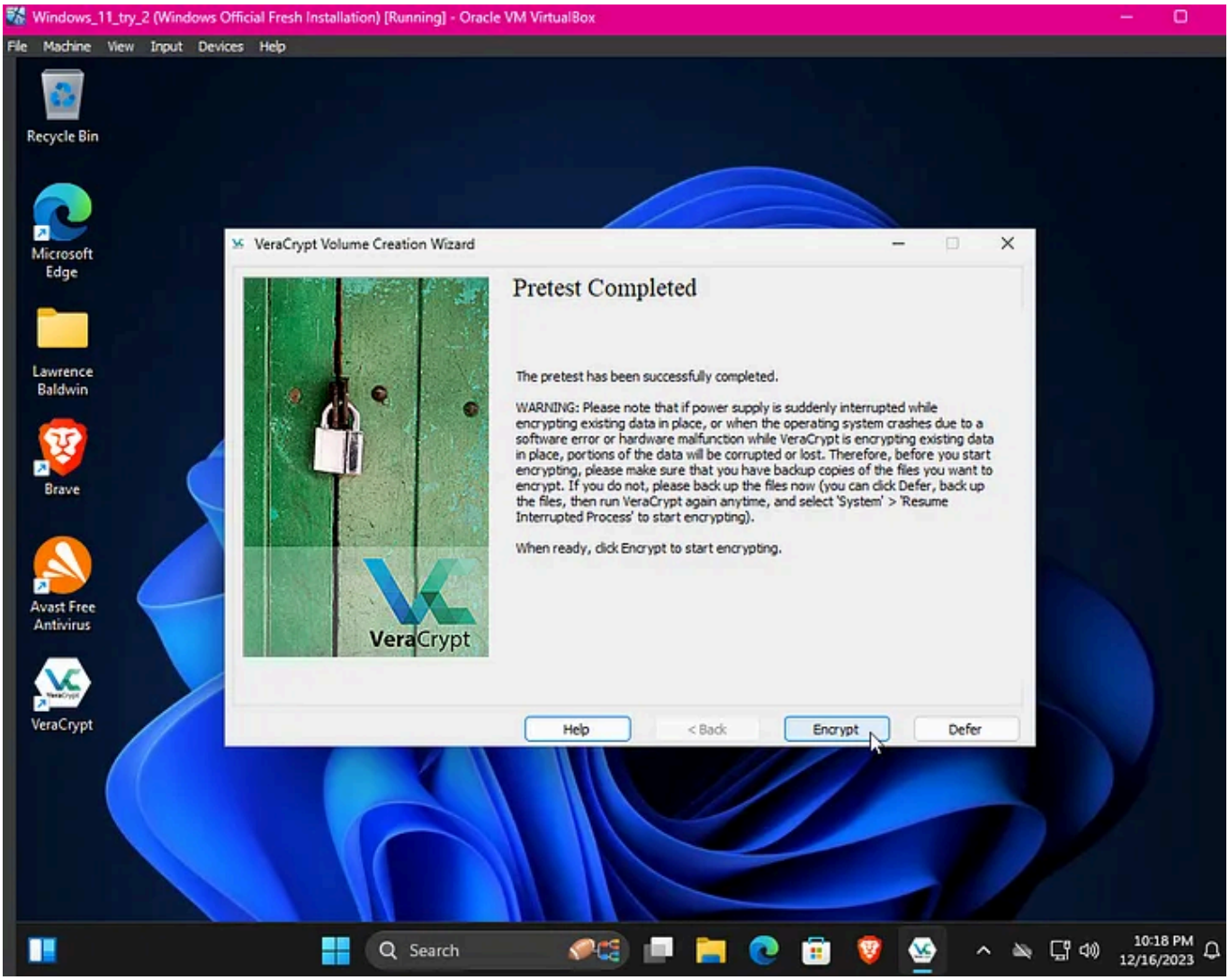
set a 20-digit password



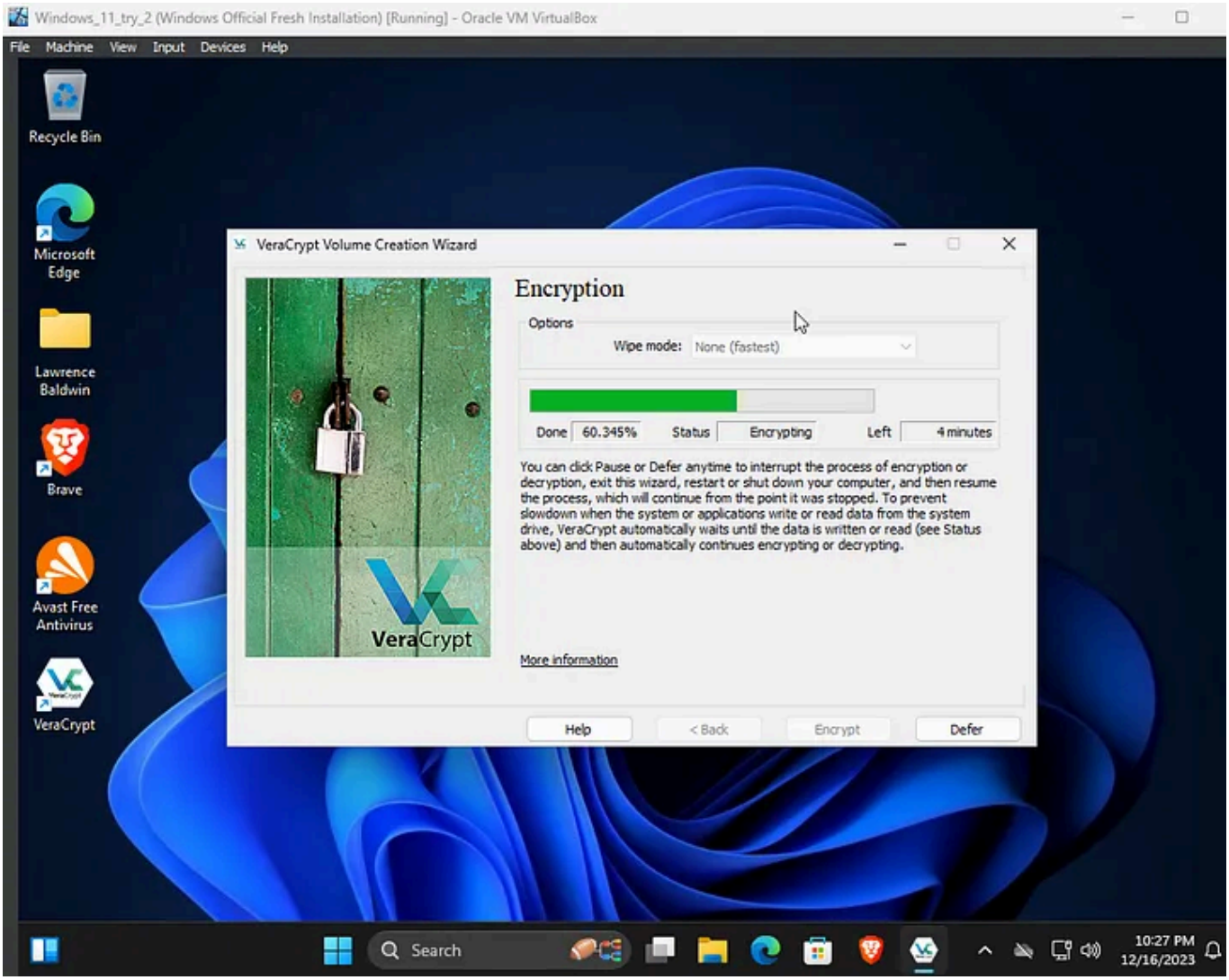
create the encryption keys



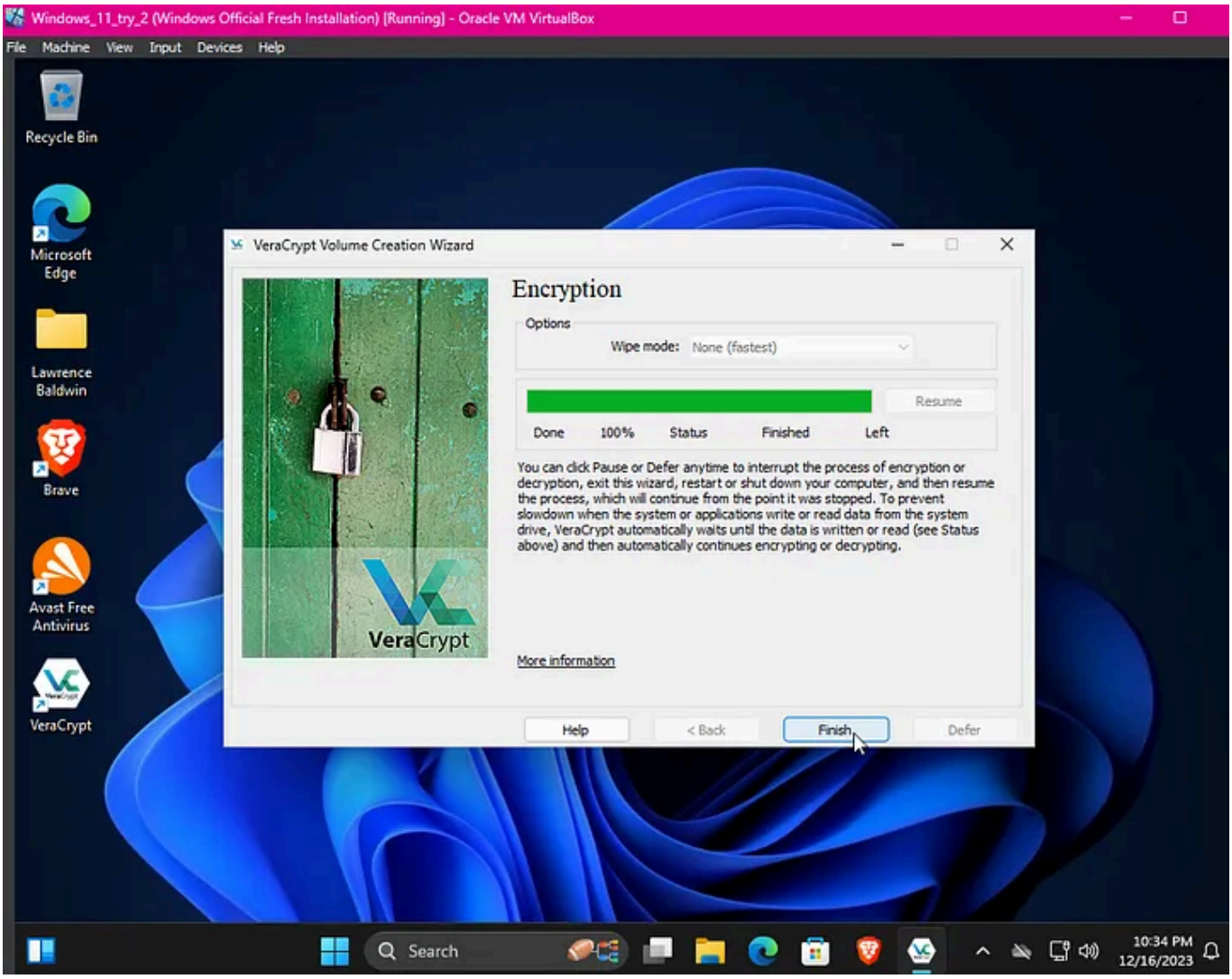
start a pretest



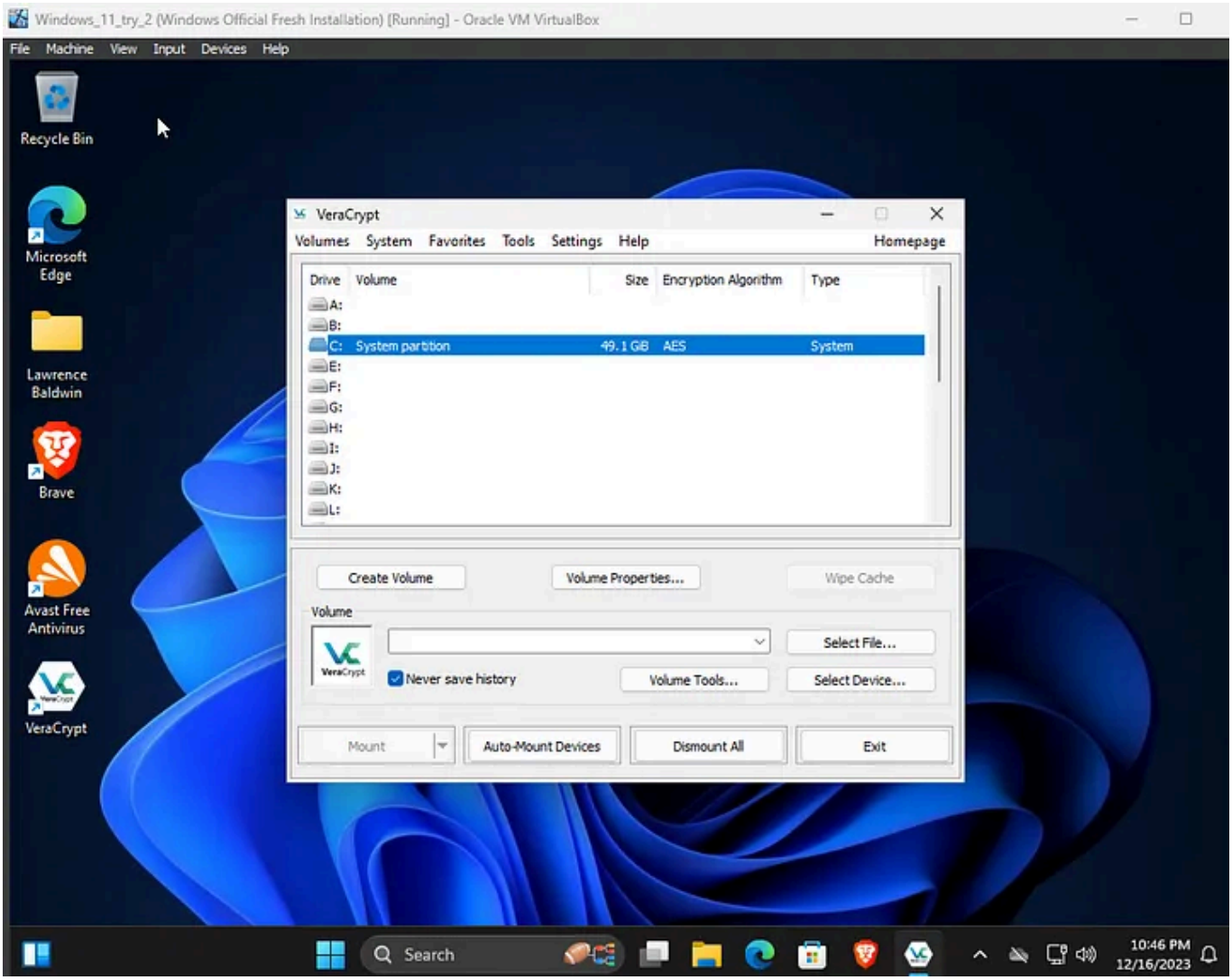
pretest complete


Windows_11_try_2 (Windows Official Fresh Installation) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
Lawrence Baldwin
Brave
Avast Free Antivirus
VeraCrypt
VeraCrypt Volume Creation Wizard
Encryption
Options
Wipe mode: None (fastest)
Done 60.345% Status Encrypting Left 4 minutes
You can click Pause or Defer anytime to interrupt the process of encryption or decryption, exit this wizard, restart or shut down your computer, and then resume the process, which will continue from the point it was stopped. To prevent slowdown when the system or applications write or read data from the system drive, VeraCrypt automatically waits until the data is written or read (see Status above) and then automatically continues encrypting or decrypting.
More information
Help
< Back
Encrypt
Defer
Search
10:27 PM
12/16/2023

encrypting



encryption complete

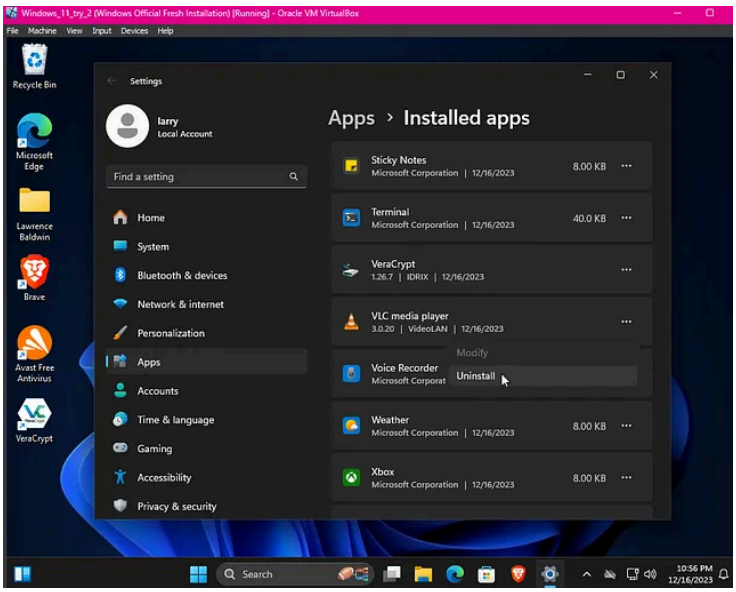


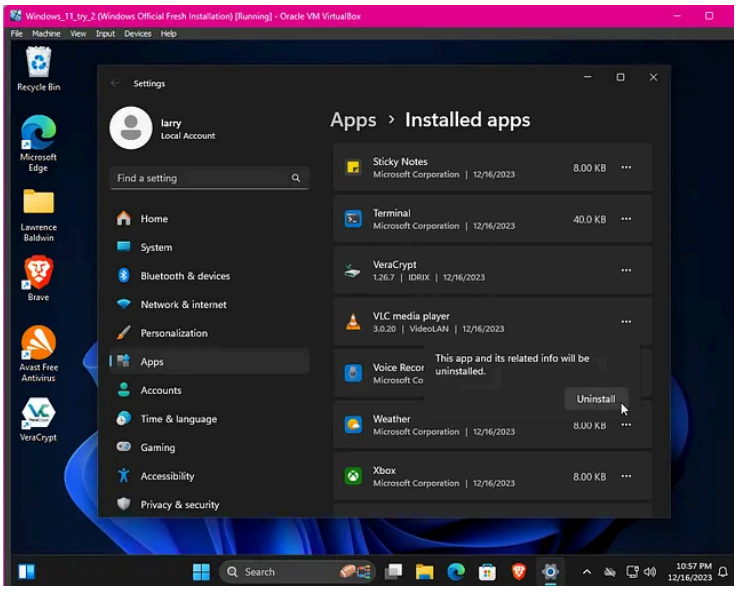
shows the new encrypted volume

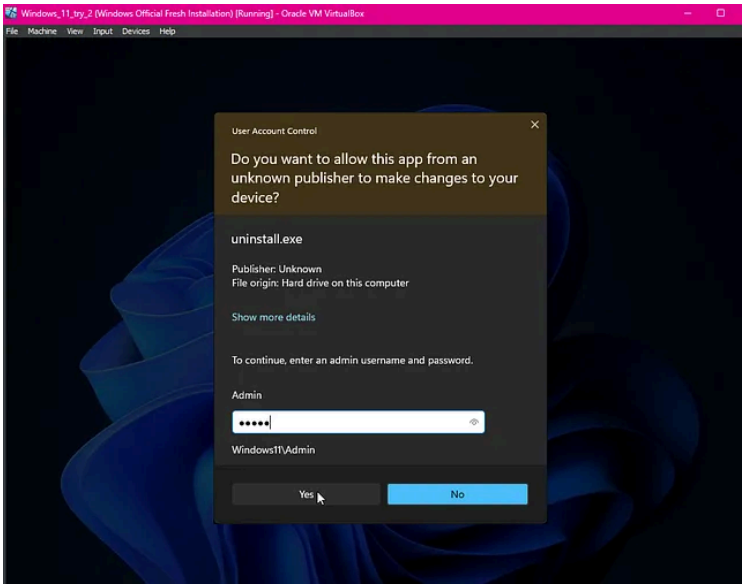
Uninstalling Unnecessary or Unused Applications

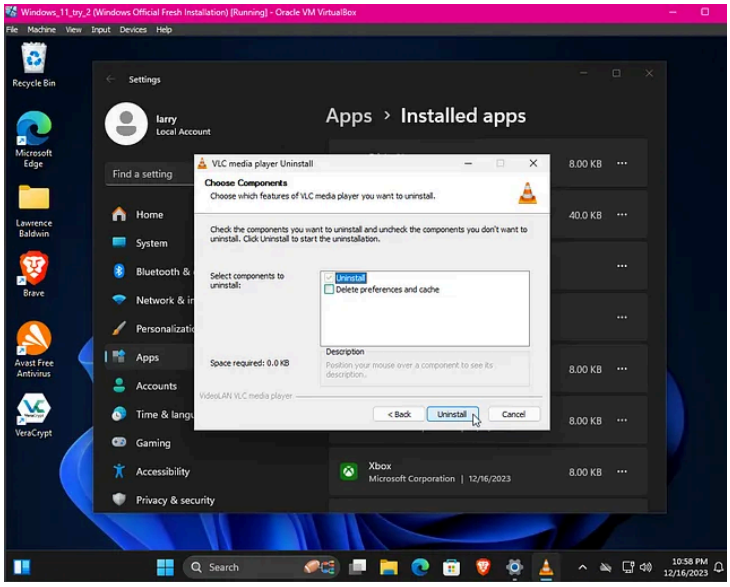
One of the easiest ways to lower your devices attack surface is to remove unnecessary applications. For this project, I chose to uninstall **VLC**, **Notepad++**, and **7zip**. To do this, go to **Apps** > **Installed Apps**, select the 3 dots, select **uninstall**, input the Admin password, click **uninstall** on the app's wizard, and then the application has been removed!

Uninstalling VLC

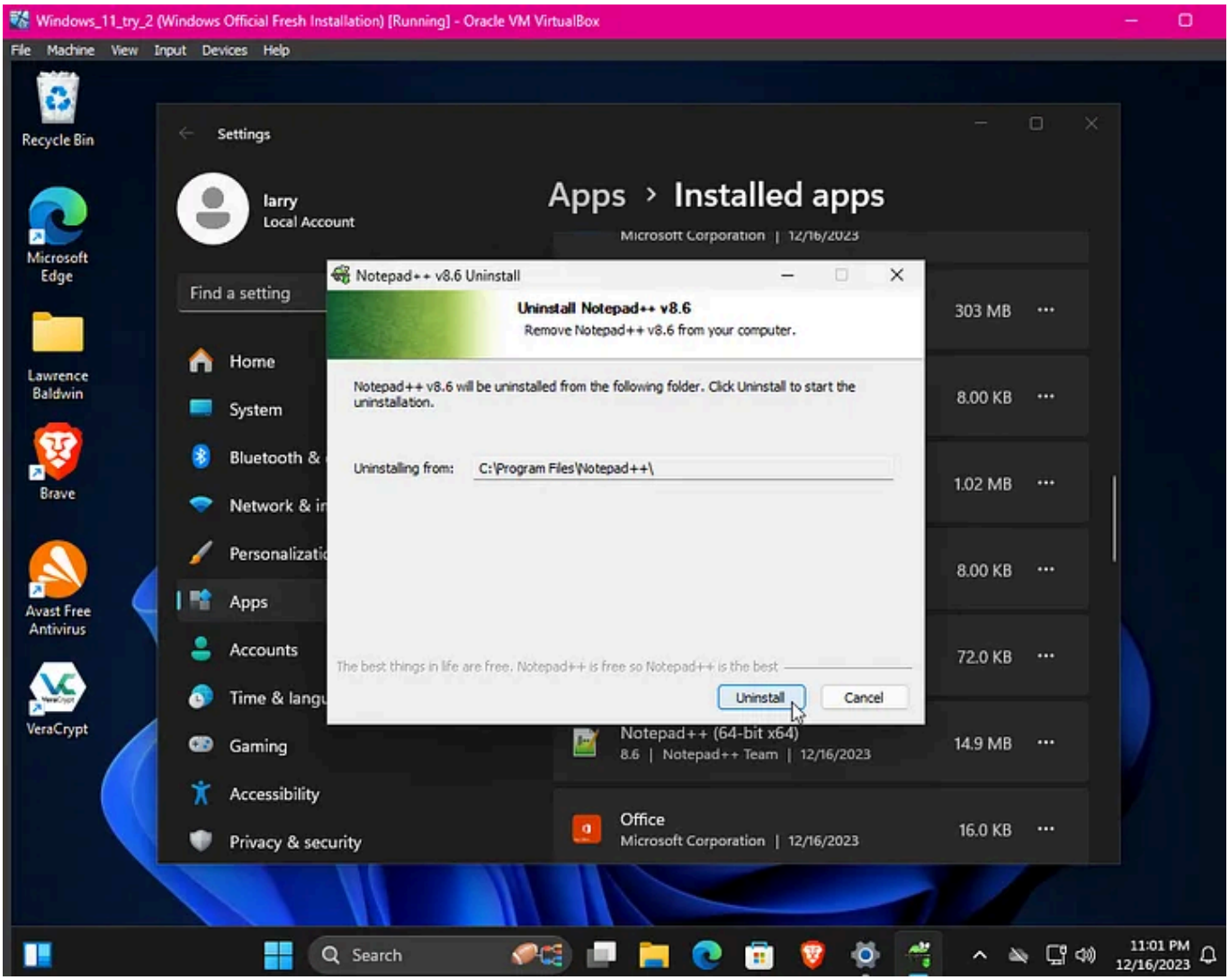




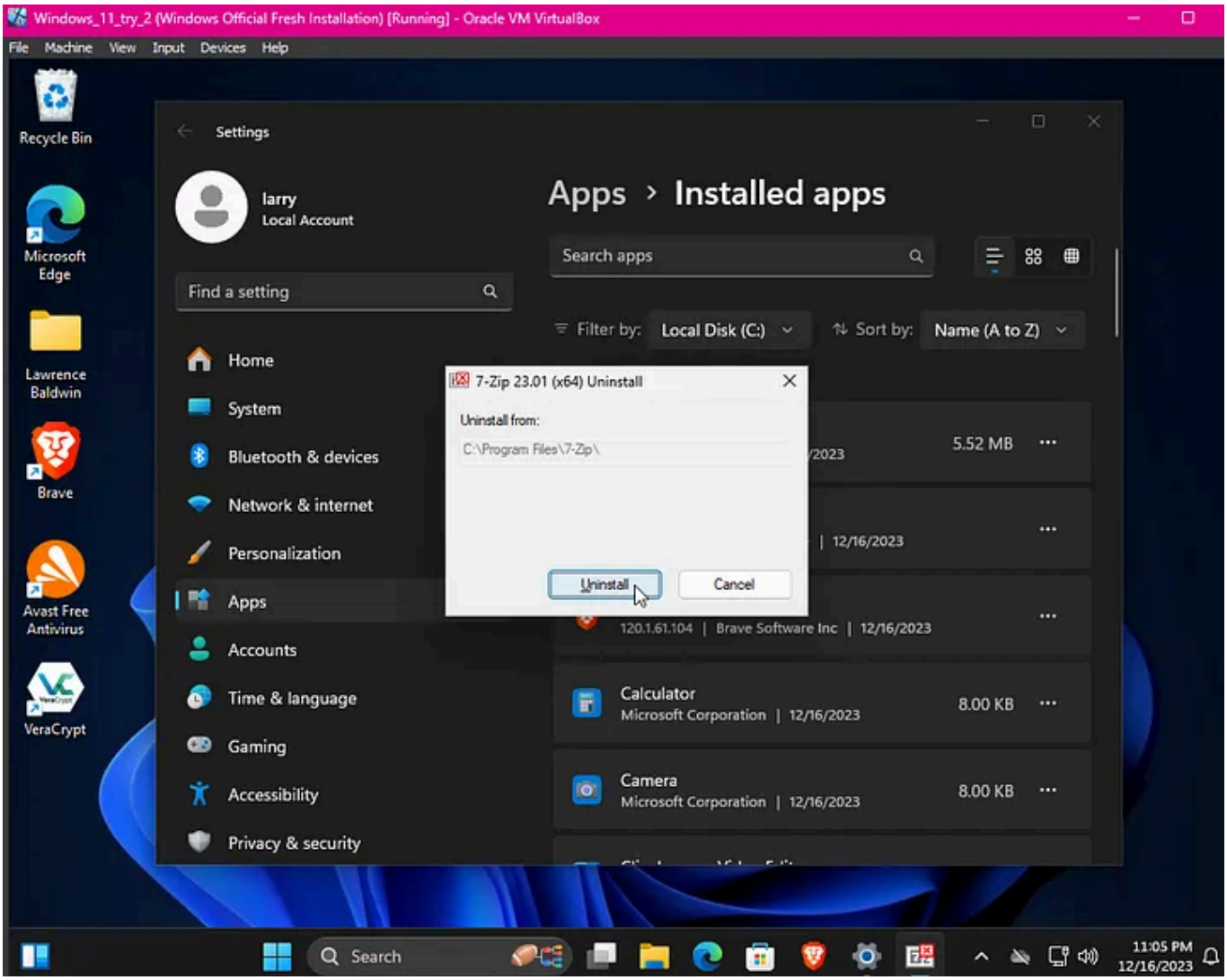




Uninstalling Notepad+



Uninstalling 7zip



December 29, 2023, Larry Baldwin

Cybersecurity Endpoint Security Windows 11

Written by Larry Baldwin

Follow

3 Followers

WGU Alumni | Actively looking for Cyber Position | CySA+ | PenTest+ | Security + | Associate of ISC2

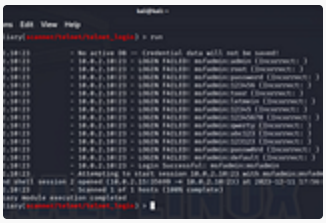
More from Larry Baldwin

Larry Baldwin

Simulated Telnet Penetration Test

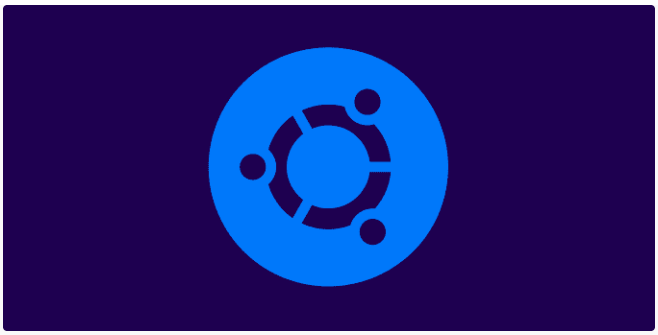
December 28, 2023, Larry Baldwin

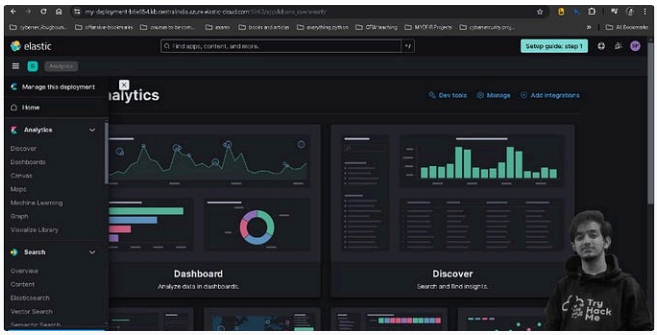
Dec 28, 2023 1



See all from Larry Baldwin

Recommended from Medium





Karthick Dkk in devsecops-community

Step-by-Step Guide: How to Join Ubuntu to Windows Active...

How to Connect Ubuntu/Debian to Windows Active Directory for Centralized...

Oct 21 2

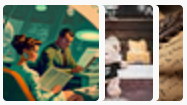
Satyam Pathania in OSINT Team

A Simple yet Powerful Elastic SIEM Lab Project

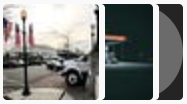
Aug 29 318 5

Lists

Tech & Tools
21 stories · 332 saves



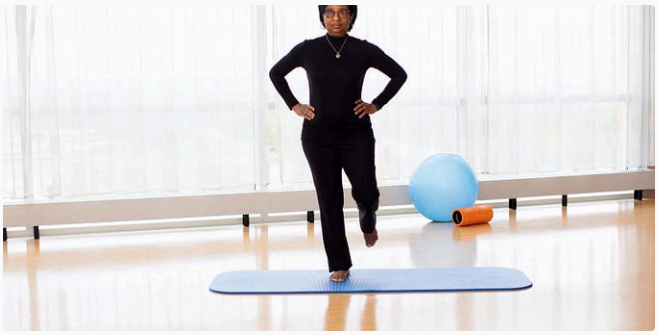
Medium's Huge List of Publications Accepting...
378 stories · 3804 saves



Staff Picks
754 stories · 1413 saves

Natural Language Processing
1782 stories · 1389 saves

Sanskar Kalra



F. Perry Wilson, MD MSCE

Game of Active Directory: Pentesting Strategies for Real-...

Introduction

Aug 16 2 1

How Old Is Your Body? Stand On One Leg and Find Out

According to new research, the time you can stand on one leg is the best marker of...

Oct 23 4.6K 116

RootRouteway

Hacking Active Directory: From Reconnaissance to Exploitation -...

Welcome back! This blog is a continuation of my first Active Directory pentesting article. I...

Jul 4 62

Bell Peterkin in ILLUMINATION

Nine iOS 18.0.1 Features You've Never Used

Put your $799 to work now. The best one is number eight.

Oct 18 782 15

See more recommendations