| | | |
|---|---|---|
| **Kingdom of Saudi Arabia**<br>**Ministry of Education**<br>**University of Jeddah**<br>**College of Science and Computer Engineering** | | **المملكة العربية السعودية**<br>**وزارة التعليم**<br>**جامعة جدّة**<br>**كلية علوم و هندسة الحاسب** |

**CCCY432 – Reverse Engineering and Malware Analysis**

**Lab 1 – Creating and Maintaining your REM Lab Environment (CLO 2.3 / PLO S4)**


Lara Sami Alofi

2110886

Y


**Due Date: 1 Sep 2024 11:00 PM**

## Objective

The purpose of this lab is to set up a secure and isolated Reverse Engineering and Malware Analysis (REM) lab environment. This includes creating and configuring a Windows 10 virtual machine (VM) and a REMnux VM, disabling unnecessary services, installing essential analysis tools, and ensuring both VMs are isolated from the internet while maintaining network connectivity between them.

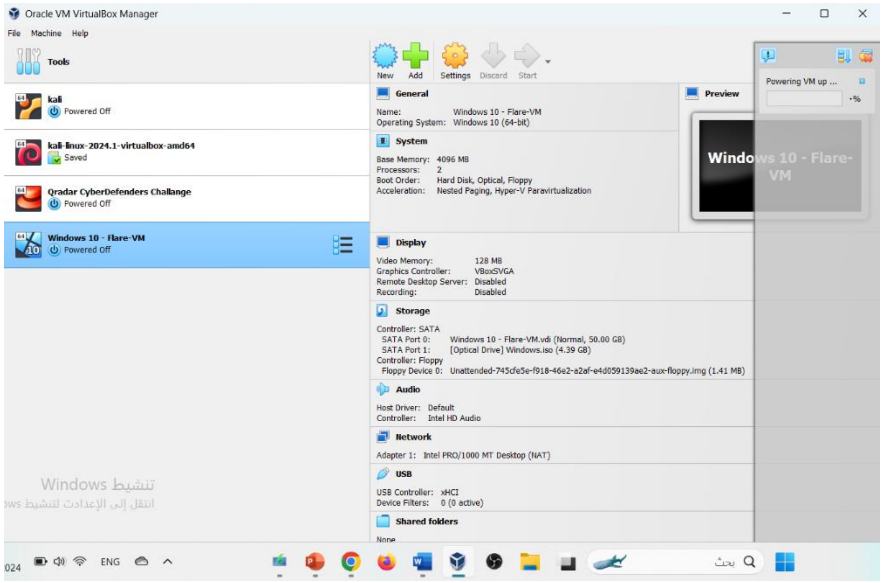
## Lab Environment Setup

### Step 1: Download and Import Windows 10

1. **Downloading Windows 10:**
    - I began by downloading the Windows 10 ISO file from the official Microsoft website: from https://www.microsoft.com/ar-sa/software-download/windows10
    - 

2. **Importing Windows 10 into VirtualBox:**

   - I imported the downloaded Windows 10 ISO file into Oracle VirtualBox to create a new VM. During this process, I configured the VM with the recommended settings: 2 GB of RAM, 2 CPUs, and a 50 GB virtual hard disk.

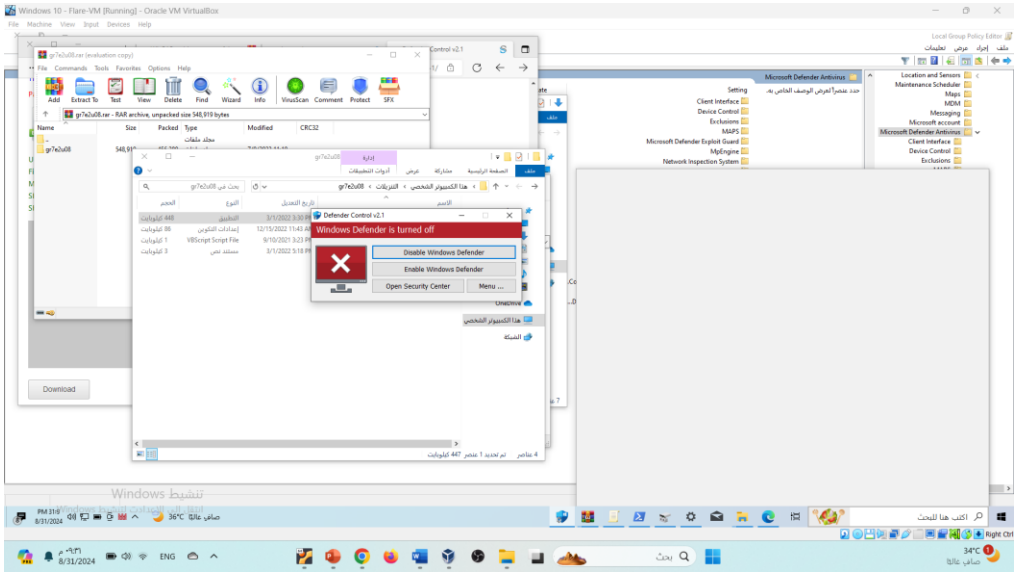



## Step 2: Disable Windows Defender and Windows Update

1. **Disabling Windows Defender:**

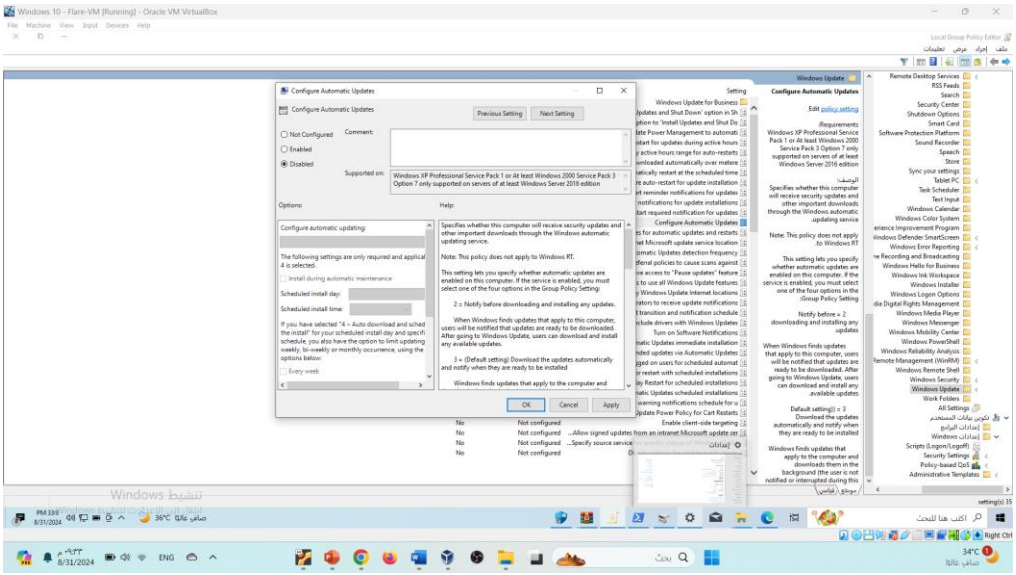
   - To prevent Windows Defender from interfering with malware analysis, I used Defender Control v2.1, which is a third-party tool that simplifies the process of disabling Microsoft Defender.

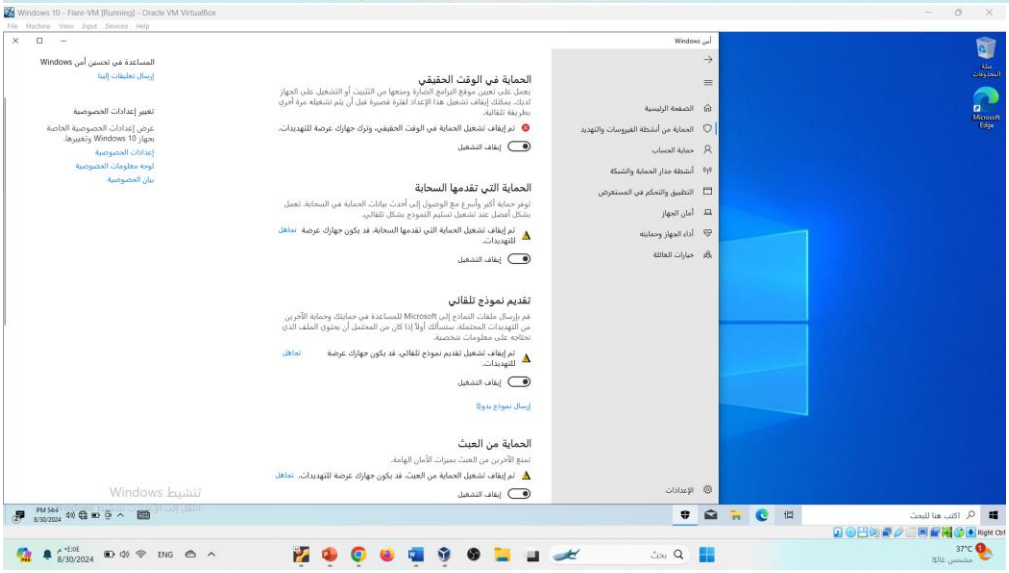
   - I downloaded the tool from [Sordum.org](Sordum.org) and ran it to disable Windows Defender.



## Disabling Windows Update & virus:

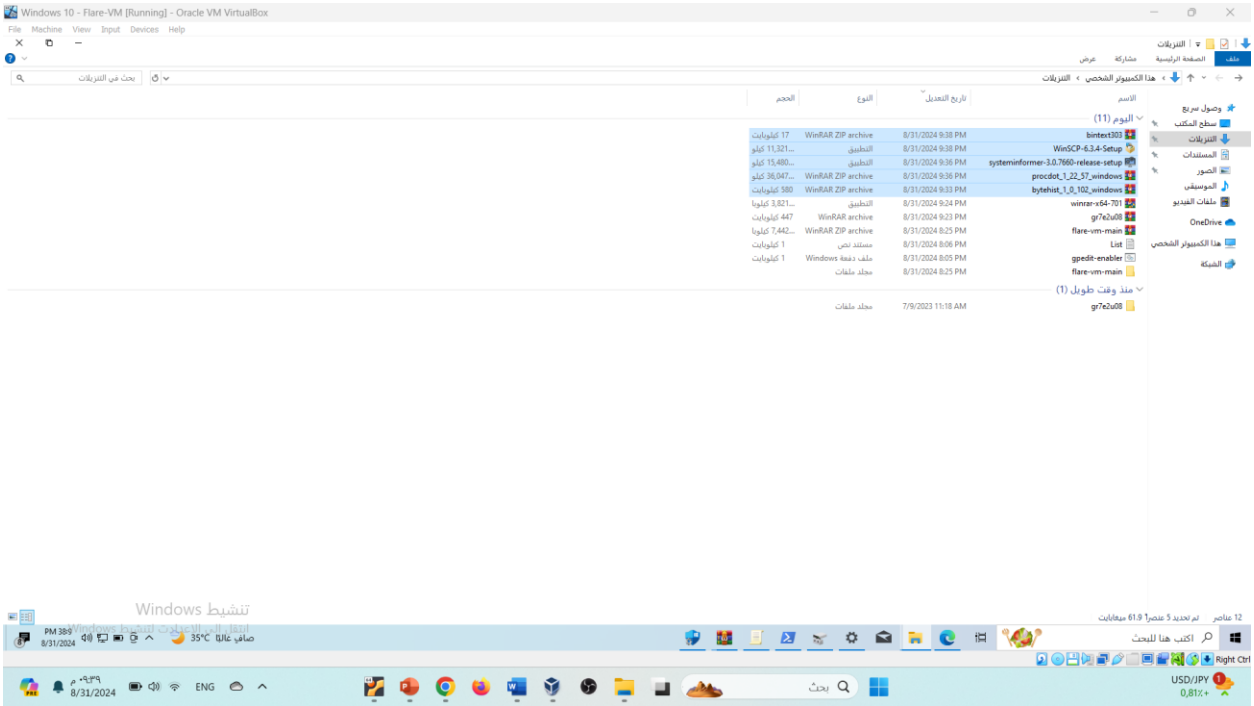
- To prevent automatic updates that might disrupt the lab environment, I disabled Windows Update through the Group Policy Editor.
- Steps followed:
    1. Pressed Win + R and typed gpedit.msc to open the Group Policy Editor.
    2. Navigated to Computer Configuration > Administrative Templates > Windows Components > Windows Update.
    3. Double-clicked on Configure Automatic Updates, selected the Disabled option, and applied the changes.





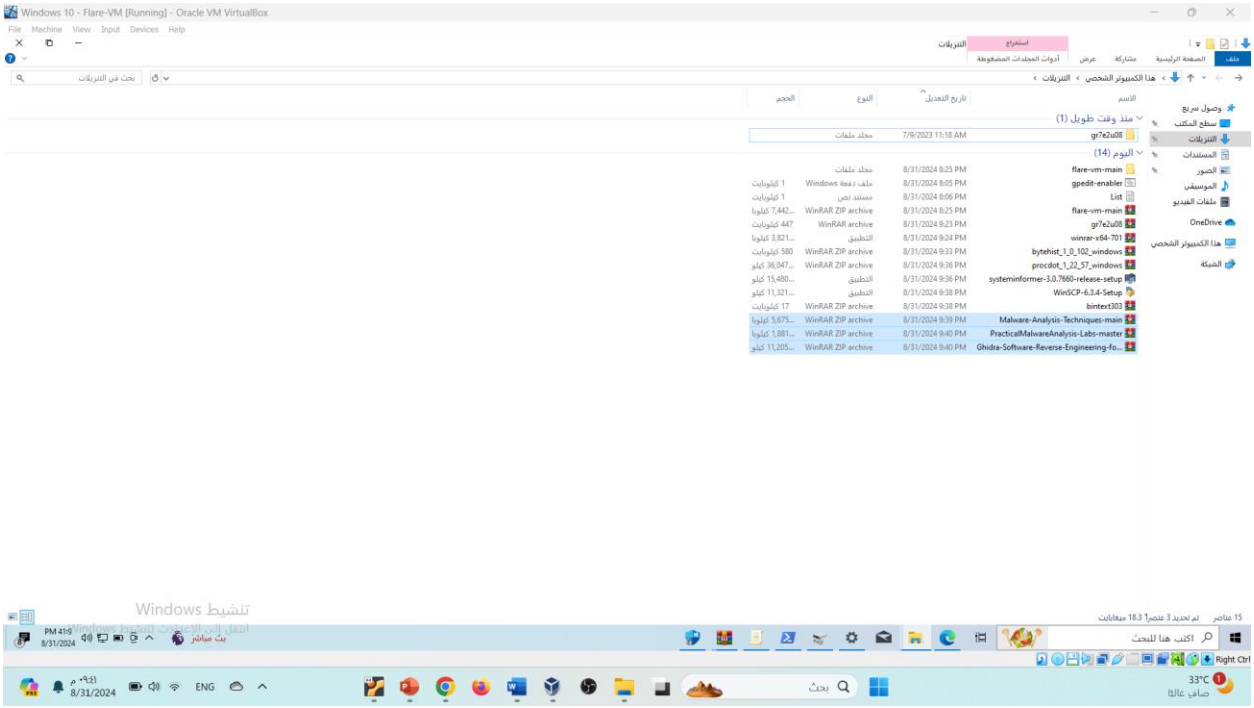
Step 3: Download and Install Essential Analysis Tools

1. Tools Installation:
    - I downloaded and installed the following tools, which are essential for malware analysis:
        - Bytehist: A tool for byte histogram analysis. Download Link
        - ProcDot: A tool that visualizes the events of processes running on a Windows system. Download Link
        - Process Hacker: A powerful tool for process analysis. Download Link
        - WinSCP: A secure file transfer client. Download Link
        - BinText: A text extractor utility. https://files1.majorgeeks.com/10afebdbffcd4742c81a3cb0f6ce4092156b4375/office/bintext303.zip



Step 4: Download and extract following samples into the desktop:

1. Downloading Malware Samples:
    - I downloaded various malware samples from the following repositories:
        - [Malware Analysis Techniques]
        - [Practical Malware Analysis Labs]
        - [Ghidra Software Reverse Engineering for Beginners]
    - The samples were extracted to the desktop for easy access during analysis.



## Step 5: Prepare PowerShell for Script Execution

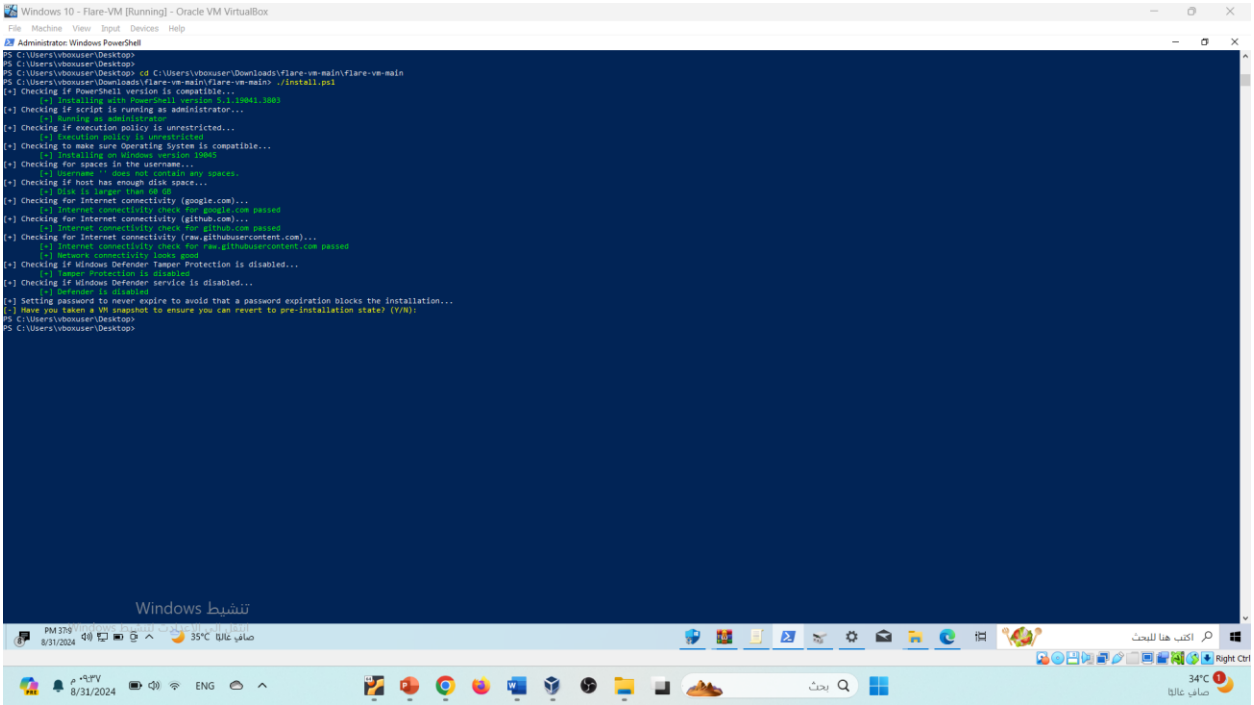
1. Configuring PowerShell:
    - I opened PowerShell as an administrator and set the execution policy to unrestricted, allowing the execution of scripts that might be necessary during malware analysis.
    - Commands executed:

Set-ExecutionPolicy Unrestricted -Force

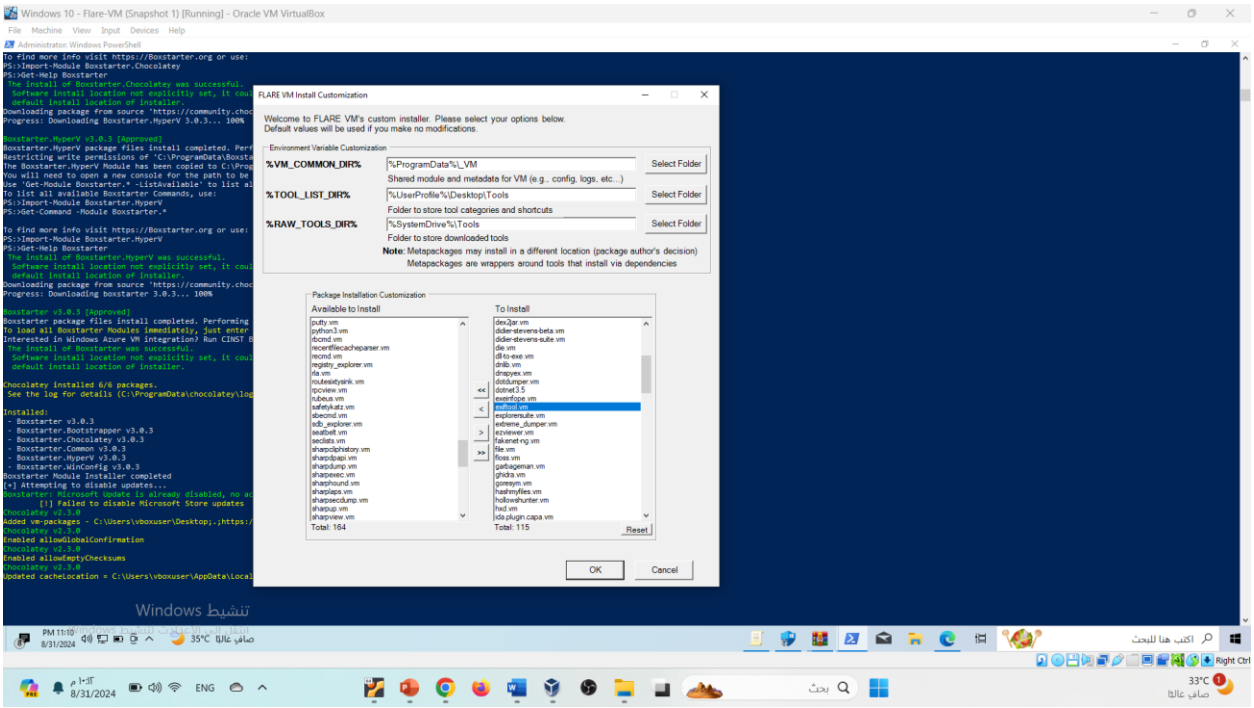
Set-ExecutionPolicy Unrestricted -Scope CurrentUser -Force

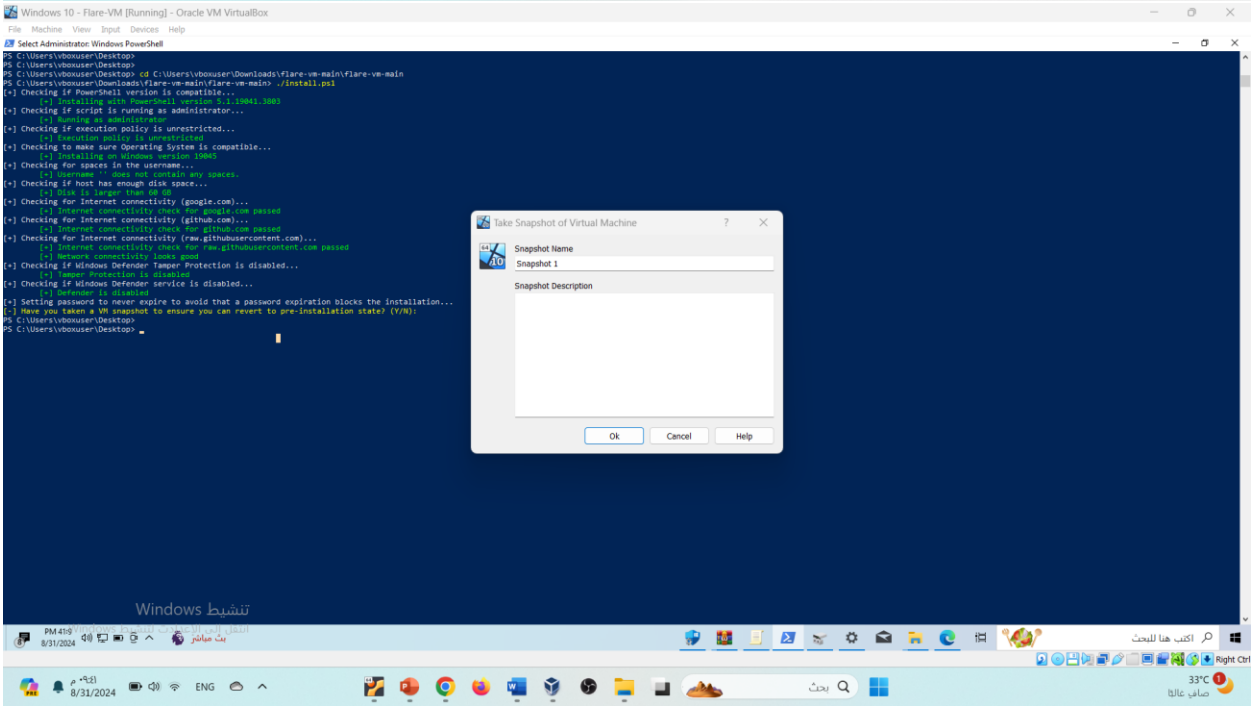
## Step 6: Install FLARE-VM Packages

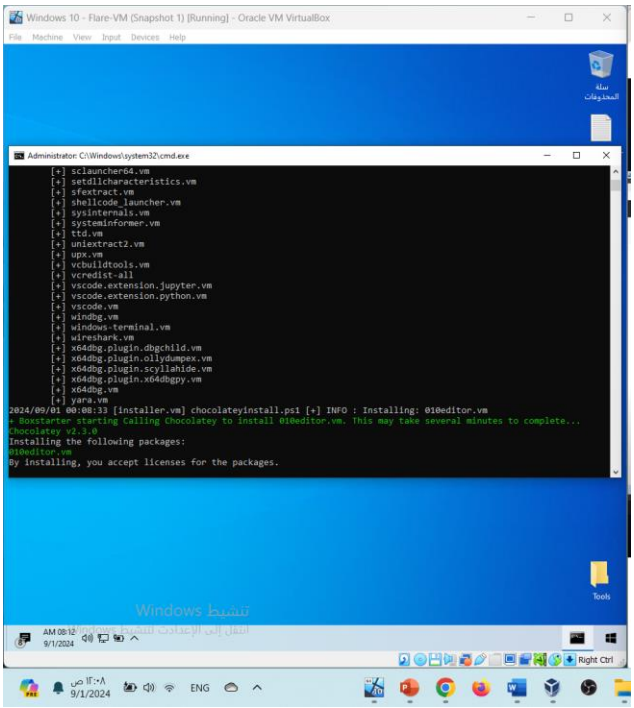
1. Installing FLARE-VM:
    - I downloaded the FLARE-VM setup package from GitHub and unblocked the install script using the command Unblock-File .\install.ps1.

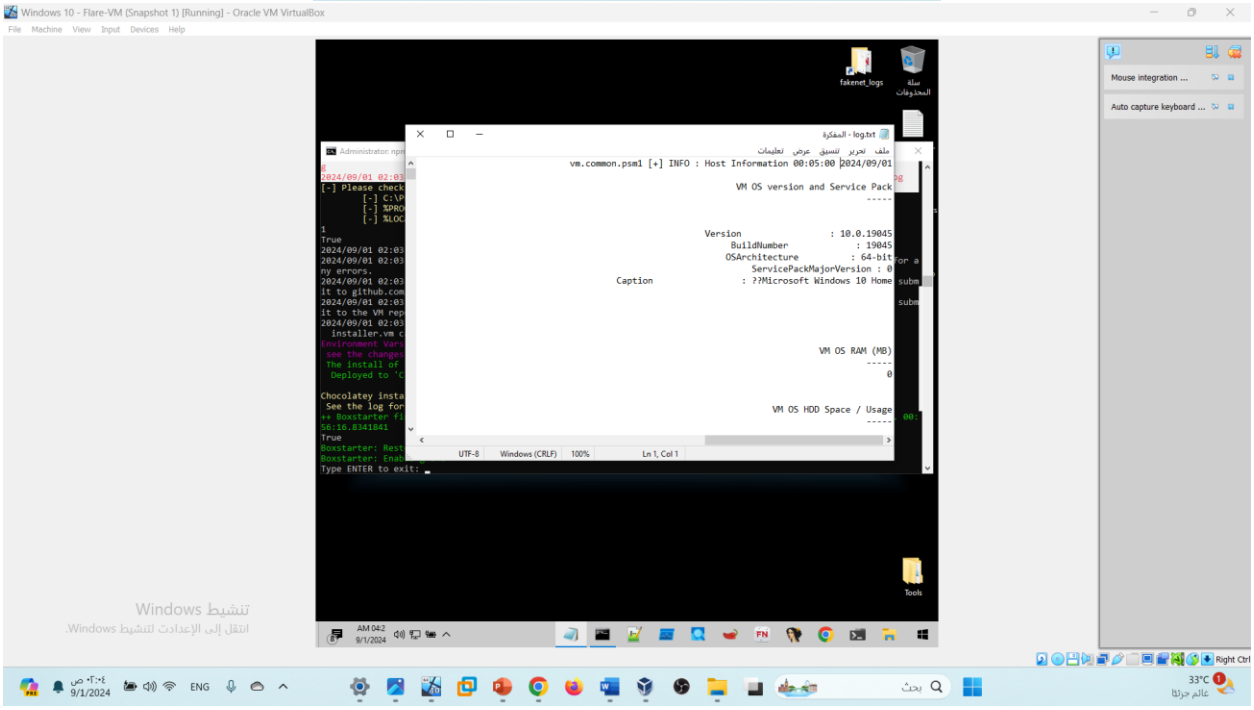



    - then executed the script to begin the installation.
    - During the installation, I selected the following packages:
        - exeinfope.vm
        - exiftool.vm
        - Ollydbg2
        - Ollydbg2.oyyldumpex.vm
        - Ollydbg2.scyllahide.vm
        - Setdllcharacteristics.vm


Windows 10 - Flare-VM (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
FLARE VM Install Customization
Welcome to FLARE VM's custom installer. Please select your options below.
Default values will be used if you make no modifications.
Environment Variable Customization
%VM_COMMON_DIR%
%ProgramData%_VM
Shared module and metadata for VM (e.g., config, logs, etc...)
Select Folder
%TOOL_LIST_DIR%
%UserProfile%\Desktop\Tools
Folder to store tool categories and shortcuts
%RAW_TOOLS_DIR%
%SystemDrive%\Tools
Folder to store downloaded tools
Note: Metapackages may install in a different location (package author's decision)
Metapackages are wrappers around tools that install via dependencies
Package Installation Customization
Available to Install
To Install
Total: 164
Total: 115
Reset
OK
Cancel


Windows 10 - Flare-VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Select Administrator: Windows PowerShell
Take Snapshot of Virtual Machine
Snapshot Name
Snapshot 1
Snapshot Description
Ok
Cancel
Help

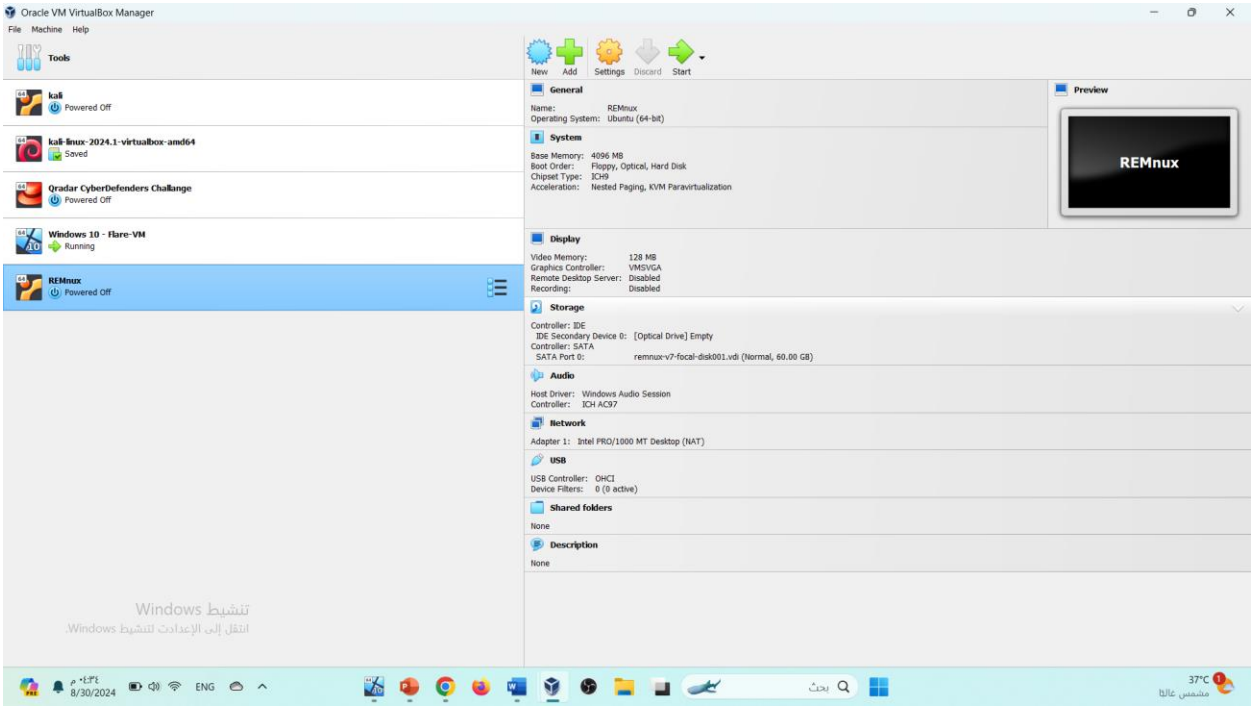

Windows 10 - Flare-VM (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
سلة المحذوفات
Administrator: C:\Windows\system32\cmd.exe
[+] sclauncher64.vm
[+] setdllcharacteristics.vm
[+] sfextract.vm
[+] shellcode_launcher.vm
[+] sysinternals.vm
[+] systeminformer.vm
[+] ttd.vm
[+] uniextract2.vm
[+] upx.vm
[+] vcbuildtools.vm
[+] vcredist-all
[+] vscode.extension.jupyter.vm
[+] vscode.extension.python.vm
[+] vscode.vm
[+] windbg.vm
[+] windows-terminal.vm
[+] wireshark.vm
[+] x64dbg.plugin.dbgchild.vm
[+] x64dbg.plugin.ollydumpex.vm
[+] x64dbg.plugin.scylladbide.vm
[+] x64dbg.plugin.x64dbgpy.vm
[+] x64dbg.vm
[+] yara.vm
2024/09/01 00:08:33 [installer.vm] chocolateyinstall.ps1 [+] INFO : Installing: 010editor.vm
+ Boxstarter starting Calling Chocolatey to install 010editor.vm. This may take several minutes to complete...
Chocolatey v2.3.0
Installing the following packages:
010editor.vm
By installing, you accept licenses for the packages.
Tools
Right Ctrl
ENG


Windows 10 - Flare-VM (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
fakenet_logs
سلة المحذوفات
log.txt - المفكرة
ملف تحرير تنسيق عرض تعليمات
vm.common.psm1 [+] INFO : Host Information 00:05:00 2024/09/01
VM OS version and Service Pack
Version : 10.0.19045
BuildNumber : 19045
OSArchitecture : 64-bit
ServicePackMajorVersion : 0
Caption : ??Microsoft Windows 10 Home
VM OS RAM (MB)
0
VM OS HDD Space / Usage
UTF-8 Windows (CRLF) 100% Ln 1, Col 1
Type ENTER to exit:
Tools
Mouse integration ...
Auto capture keyboard ...
Right Ctrl
ENG

## Part B: REMnux VM

### Step 7: Download and Import REMnux VM

1. Downloading REMnux:
    - I downloaded the REMnux OVA file from the official documentation page: [REMnux Download](REMnux Download).
2. Importing REMnux into VirtualBox:
    - I imported the OVA file into VirtualBox, creating a new REMnux VM.
    - Screenshot: [Insert Screenshot of REMnux VM After Import]

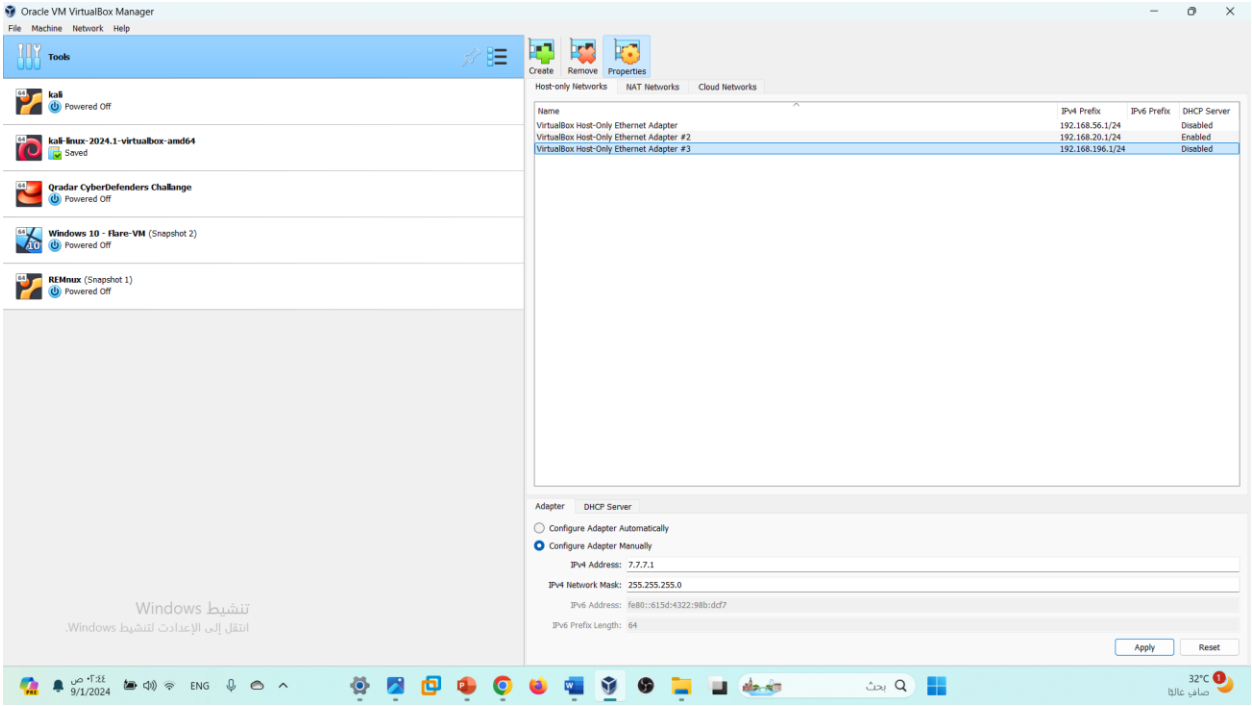



## Part C: Network Configuration

### Step 8: Configure an Isolated Virtual Network

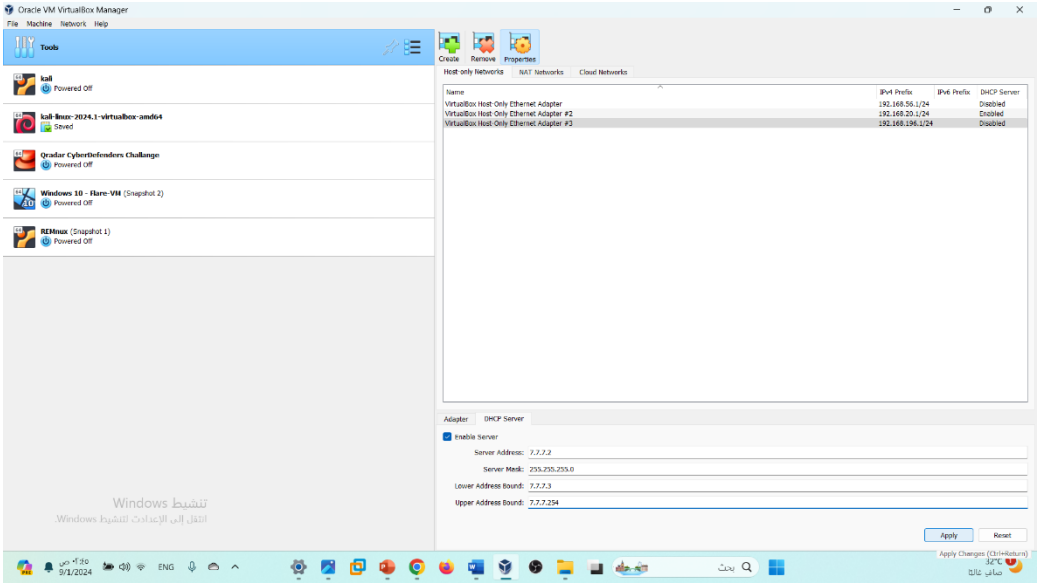
1. Creating a Host-Only Network:
    - In VirtualBox, I created a new host-only network adapter named VirtualBox Host-Only Ethernet Adapter #3 and manually configured the adapter with the following settings:
        - IPv4 Address: 7.7.7.1
        - IPv4 Network Mask: 255.255.255.0
    - The DHCP server was configured as follows:
        - Server Address: 7.7.7.2
        - Server Mask: 255.255.255.0

        - Lower Address Bound: 7.7.7.3
        - Upper Address Bound: 7.7.7.254
    - Screenshot: [Screenshot of Host-Only Network Configuration]




Configuring Network Interfaces:

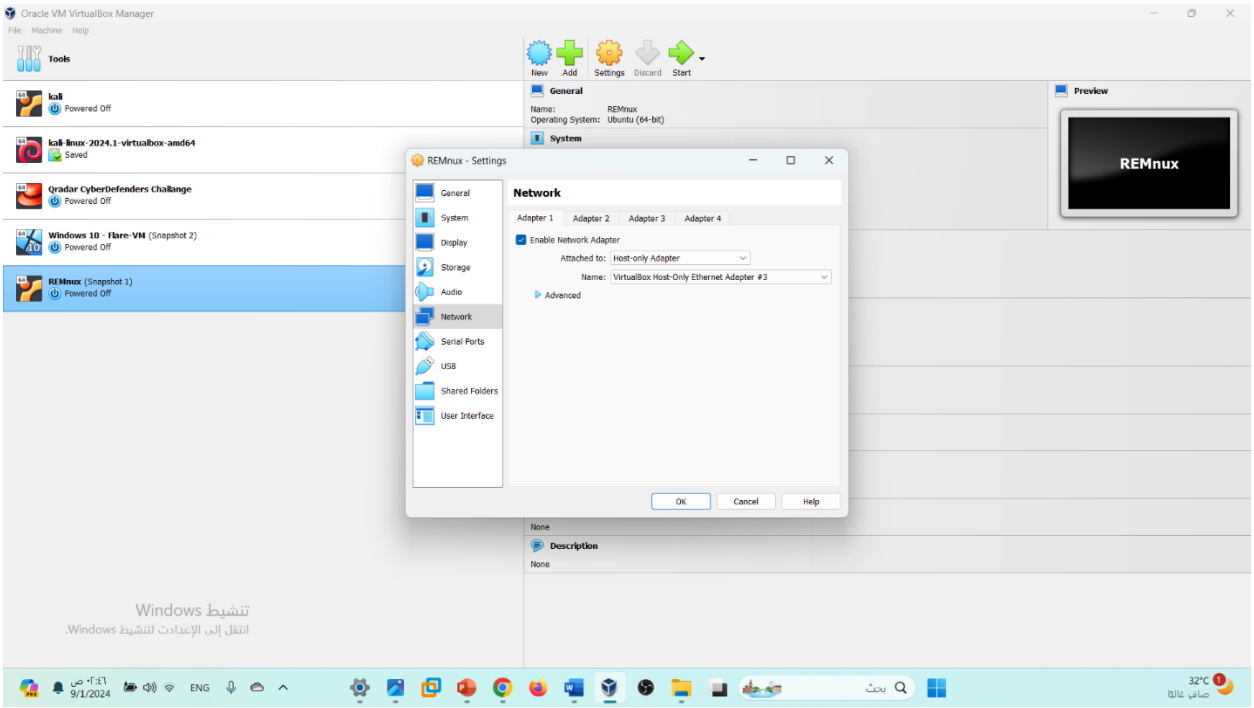
- REMnux Network Interface: Configured to use the newly created host-only network.
- Windows Network Interface:
    - Set the IP address to 7.7.7.4.
    - Set the network mask to 255.255.255.0.
    - Set the DNS server to 7.7.7.7.
- Screenshot: [Screenshot of Windows Network Settings]

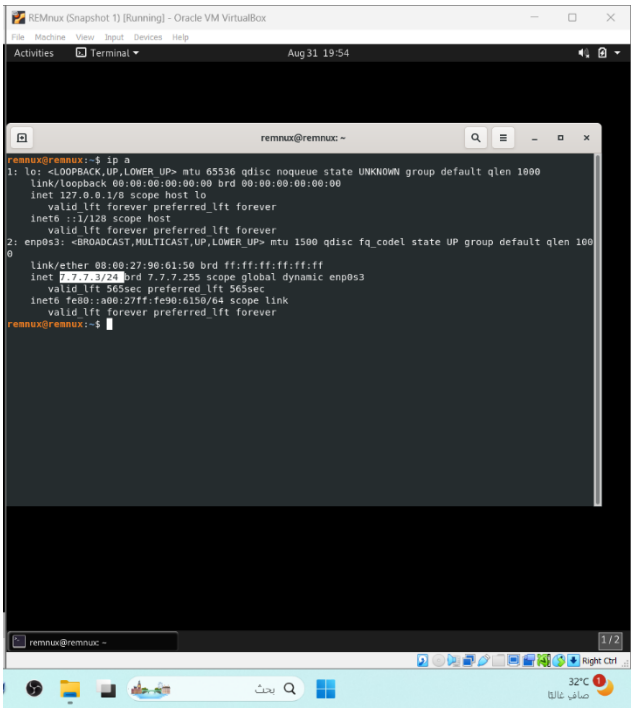


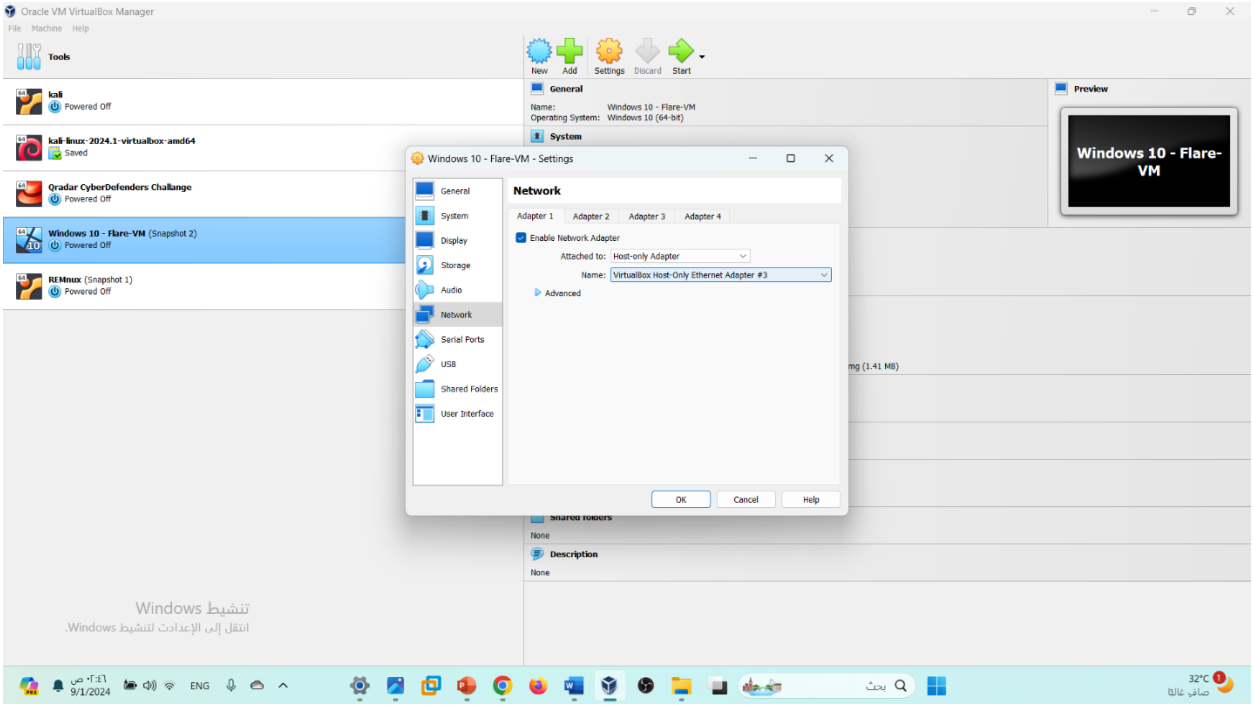

## Configuring REMnux and Windows Network Interfaces

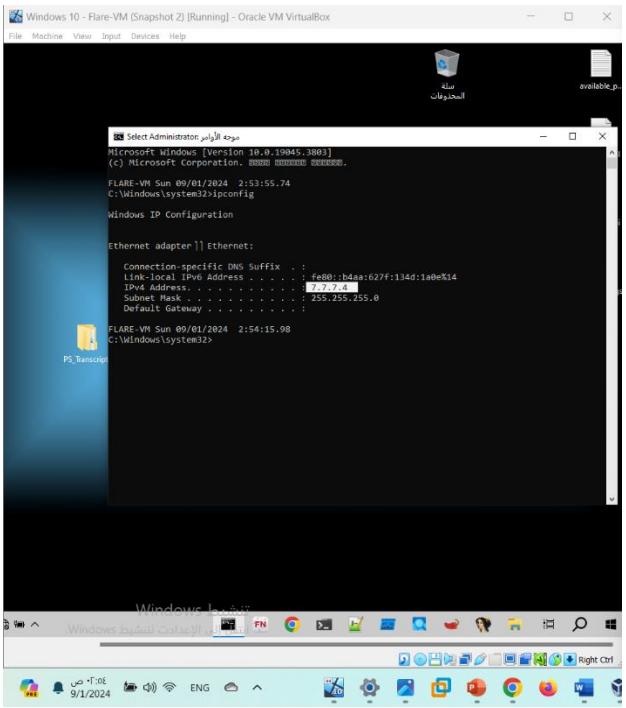
1. Configure REMnux Network Interface:

- In VirtualBox, open the settings for the REMnux VM and navigate to the "Network" tab.
- Select "Adapter 1" and ensure it is attached to the "Host-only Adapter" that you previously configured (e.g., VirtualBox Host-Only Ethernet Adapter #3).
- Click "OK" to apply the changes.



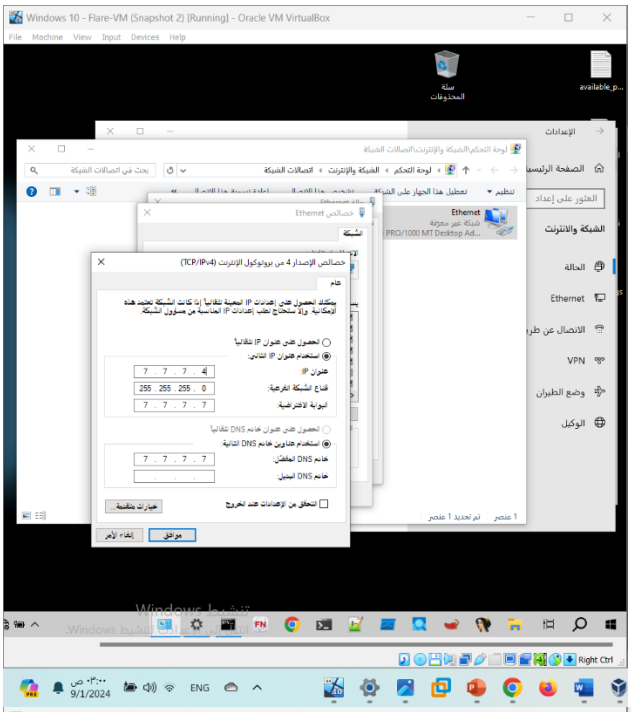

REMnux (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Aug 31 19:54
remnux@remnux: ~
remnux@remnux:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:90:61:50 brd ff:ff:ff:ff:ff:ff
inet 7.7.7.3/24 brd 7.7.7.255 scope global dynamic enp0s3
valid_lft 565sec preferred_lft 565sec
inet6 fe80::a00:27ff:fe90:6150/64 scope link
valid_lft forever preferred_lft forever
remnux@remnux:~$
remnux@remnux: ~
1/2
Right Ctrl
32°C
صافي غالبًا

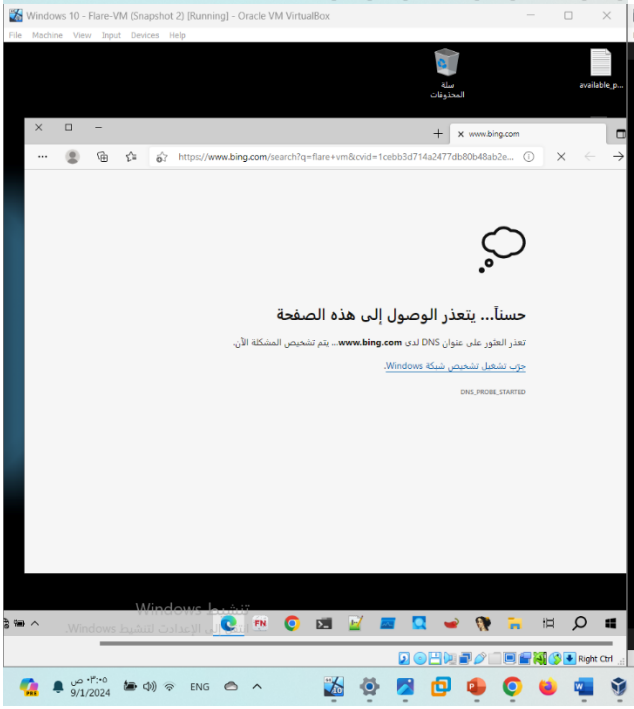

Oracle VM VirtualBox Manager
File Machine Help
Tools
kali
Powered Off
kali-linux-2024.1-virtualbox-amd64
Saved
Qradar CyberDefenders Challange
Powered Off
Windows 10 - Flare-VM (Snapshot 2)
Powered Off
REMnux (Snapshot 1)
Powered Off
New
Add
Settings
Discard
Start
General
Name: Windows 10 - Flare-VM
Operating System: Windows 10 (64-bit)
System
Preview
Windows 10 - Flare-VM
Windows 10 - Flare-VM - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Host-only Adapter
Name: VirtualBox Host-Only Ethernet Adapter #3
Advanced
OK
Cancel
Help
Shared folders
None
Description
None
تنشيط Windows
انتقل إلى الإعدادات لتنشيط Windows.
ENG
9/1/2024
32°C
صافي غالبًا

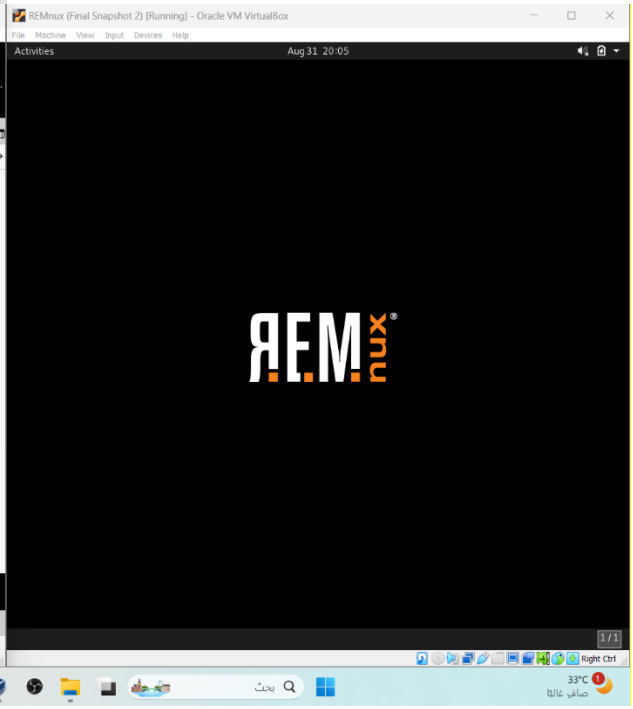



Configure Windows Network Interface:

- Open the VirtualBox settings for the Windows 10 VM and go to the "Network" tab.
- Similar to REMnux, ensure that the network adapter is attached to the "Host-only Adapter" (VirtualBox Host-Only Ethernet Adapter #3).
- After booting into Windows 10, manually configure the network settings:
    - Go to Control Panel > Network and Sharing Center > Change adapter settings.
    - Right-click on the network adapter associated with the host-only network and select Properties.
    - Select Internet Protocol Version 4 (TCP/IPv4) and click Properties.
    - Set the IP address to 7.7.7.4.
    - Set the subnet mask to 255.255.255.0.
    - Set the DNS server to 7.7.7.7.
    - Click "OK" to save the configuration.


Windows 10 - Flare-VM (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
سلة المحذوفات
available_p...
الإعدادات
الصفحة الرئيسية
العثور على إعداد
الشبكة والانترنت
الحالة
Ethernet
الاتصال عن طريق
VPN
وضع الطيران
الوكيل
لوحة التحكم\الشبكة والإنترنت\اتصالات الشبكة
لوحة التحكم › الشبكة والإنترنت › اتصالات الشبكة
تعطيل هذا الجهاز على الشبكة
تنظيم
Ethernet
شبكة غير معرفة
PRO/1000 MT Desktop Ad...
خصائص Ethernet
الشبكة
خصائص الإصدار 4 من بروتوكول الإنترنت (TCP/IPv4)
عام
يمكنك الحصول على إعدادات IP المعينة تلقائياً إذا كانت الشبكة تدعم هذه الإمكانية. وإلا، ستحتاج لطلب إعدادات IP المناسبة من مسؤول الشبكة.
الحصول على عنوان IP تلقائياً
استخدام عنوان IP التالي:
عنوان IP:
قناع الشبكة الفرعية:
البوابة الافتراضية:
الحصول على عنوان خادم DNS تلقائياً
استخدام عناوين خادم DNS التالية:
خادم DNS المفضل:
خادم DNS البديل:
تحقق من الإعدادات عند الخروج
خيارات متقدمة
موافق
إلغاء الأمر
1 عنصر
تم تحديد 1 عنصر
Right Ctrl
ENG
9/1/2024


Windows 10 - Flare-VM (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
سلة المحذوفات
available_p...
www.bing.com
https://www.bing.com/search?q=flare+vm&cvid=1cebb3d714a2477db80b48ab2e...
حسناً... يتعذر الوصول إلى هذه الصفحة
تعذر العثور على عنوان DNS لدى www.bing.com... يتم تشخيص المشكلة الآن.
جرّب تشغيل تشخيص شبكة Windows.
DNS_PROBE_STARTED
Right Ctrl
ENG
9/1/2024


REMnux (Final Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Aug 31 20:05
REMnux
1/1
Right Ctrl
بحث
33°C
صافي غالبًا

In remnux:

```
remnux@remnux:~$ sudo nano /etc/netplan/01-netcfg.yaml
```

```
  GNU nano 4.8                    /etc/netplan/01-netcfg.yaml
# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    ens33:
      dhcp4: no
      addresses:
      - 7.7.7.7/24
```

## Ensure Connectivity Between Windows and REMnux:

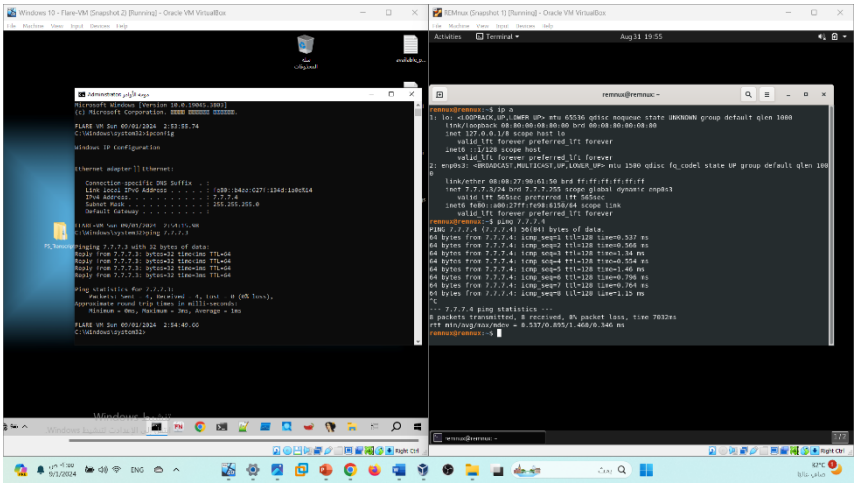
- To verify that the network configuration is correct and that both VMs can communicate, perform the following tests:

### Ping from Windows to REMnux:

  - Open a Command Prompt in Windows (cmd.exe).
  - Run the command: ping 7.7.7.3.
  - A successful ping will indicate that the Windows VM can reach the REMnux VM.

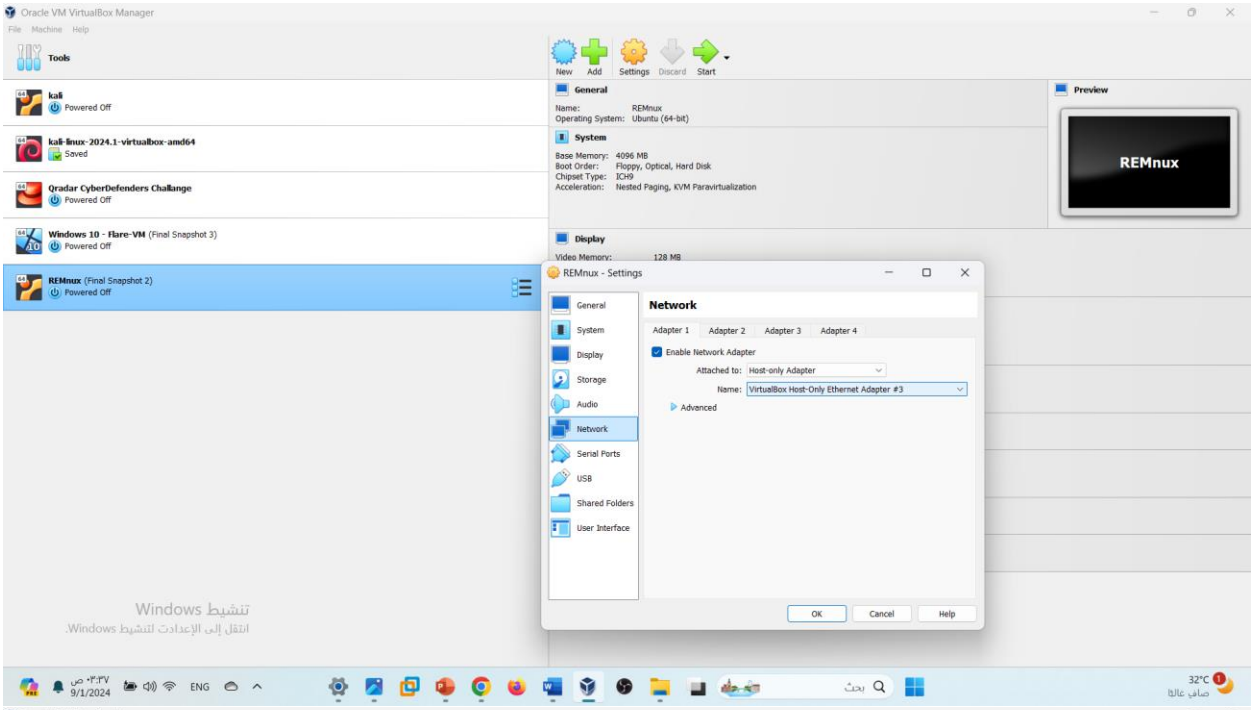
### Ping from REMnux to Windows:

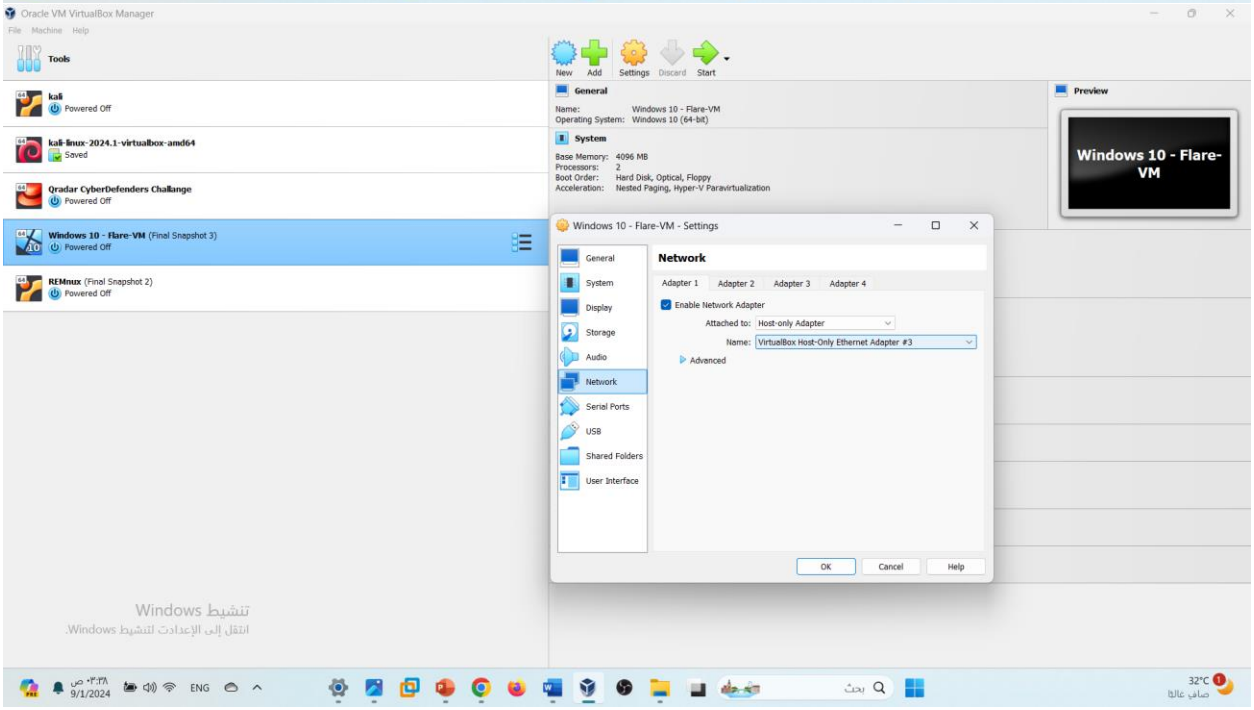
  - Open a terminal in REMnux.
  - Run the command: ping 7.7.7.4.
  - A successful ping will indicate that the REMnux VM can reach the Windows VM.



4. Ensure Network Isolation:

- To maintain the security of the REM lab environment, it is crucial to ensure that neither the Windows nor the REMnux VM has access to the internet.
- Confirm that the network settings in VirtualBox for both VMs are configured to use the host-only network, without any additional network adapters that provide external connectivity.



References:

1. Disabling MS-Defender:

- https://www.sordum.org/9480/defender-control-v2-1/

2. YouTube tutorial:

- https://www.youtube.com/watch?v=mhM6jfdDbso