

Creating and Maintaining your Detonation Environment

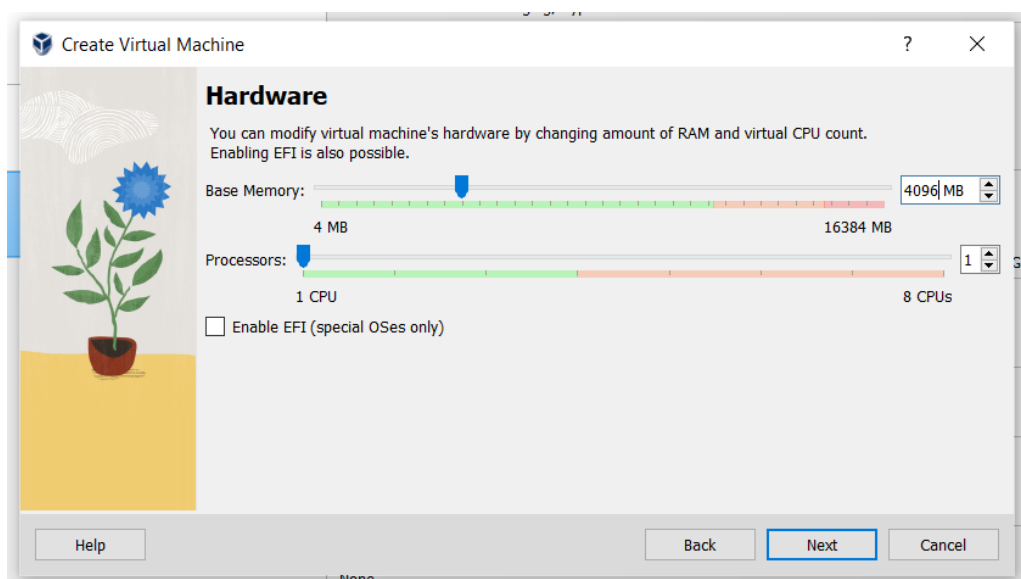
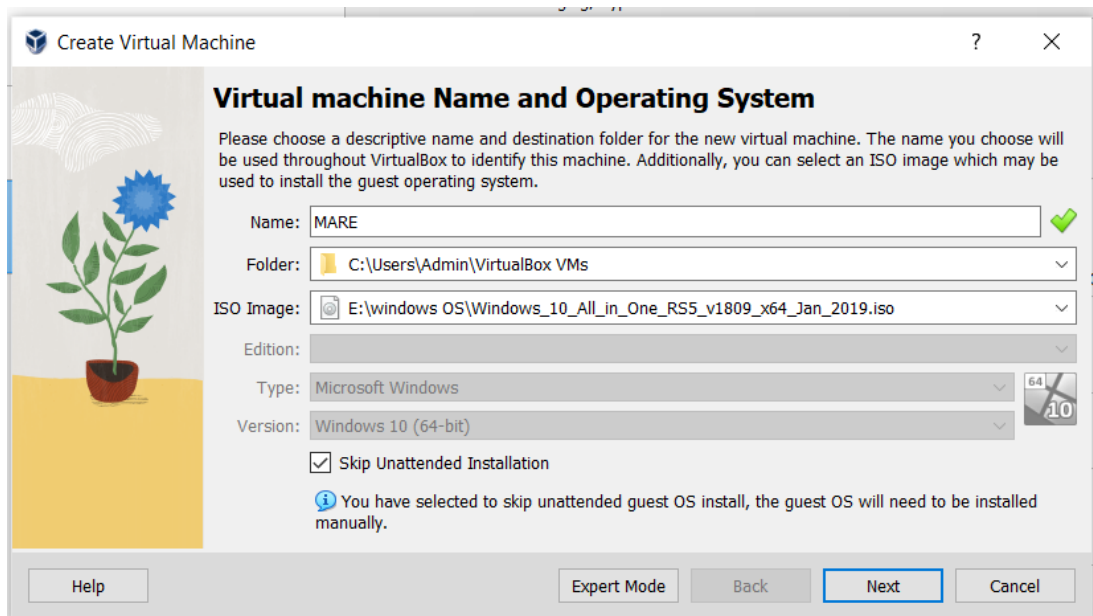
Technical requirements

The following are the requirements for this lab:

- A PC/Mac with at least 8 GB of memory and a quad-core processor
- An internet connection
- FLARE VM GitHub package: <https://github.com/fireeye/flare-vm>
- The latest VirtualBox installer: <https://virtualbox.org/wiki/downloads>
- A Windows 10 ISO and product key

Text book : Malware Analysis Techniques Tricks for the triage of adversarial software Dylan Barker, 2021

Setting up VirtualBox with Windows 10



Create Virtual Machine

Virtual Hard disk

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

☒ Create a Virtual Hard Disk Now

Disk Size:

☐ Pre-allocate Full Size

☐ Use an Existing Virtual Hard Disk File

☐ Do Not Add a Virtual Hard Disk

Help

BackNextCancel

Create Virtual Machine

Summary

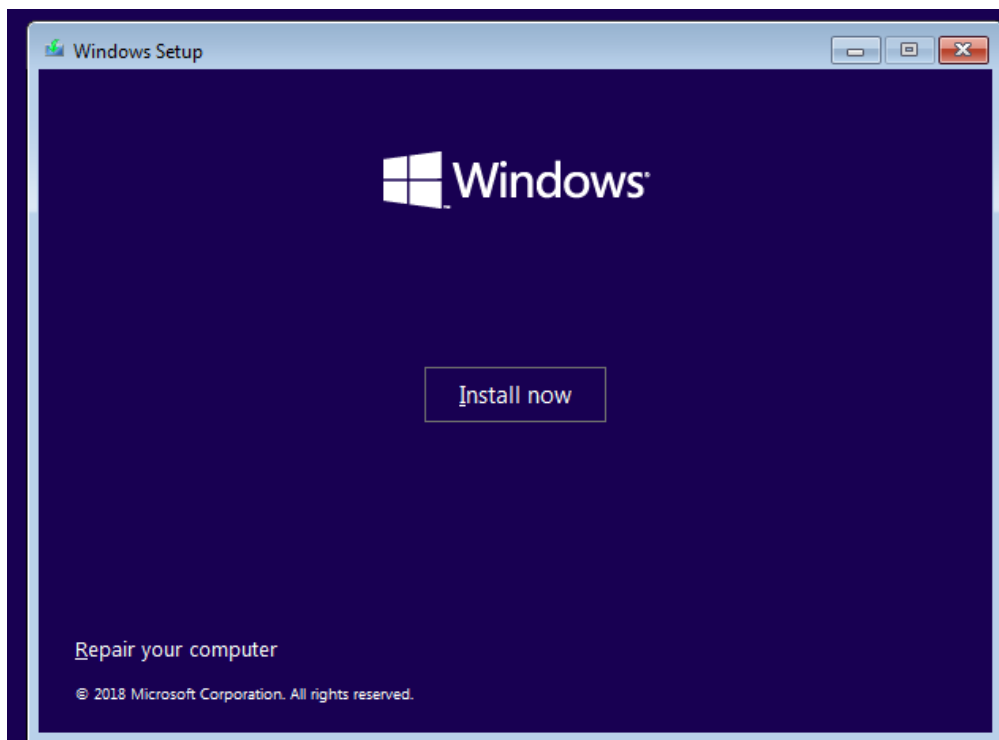
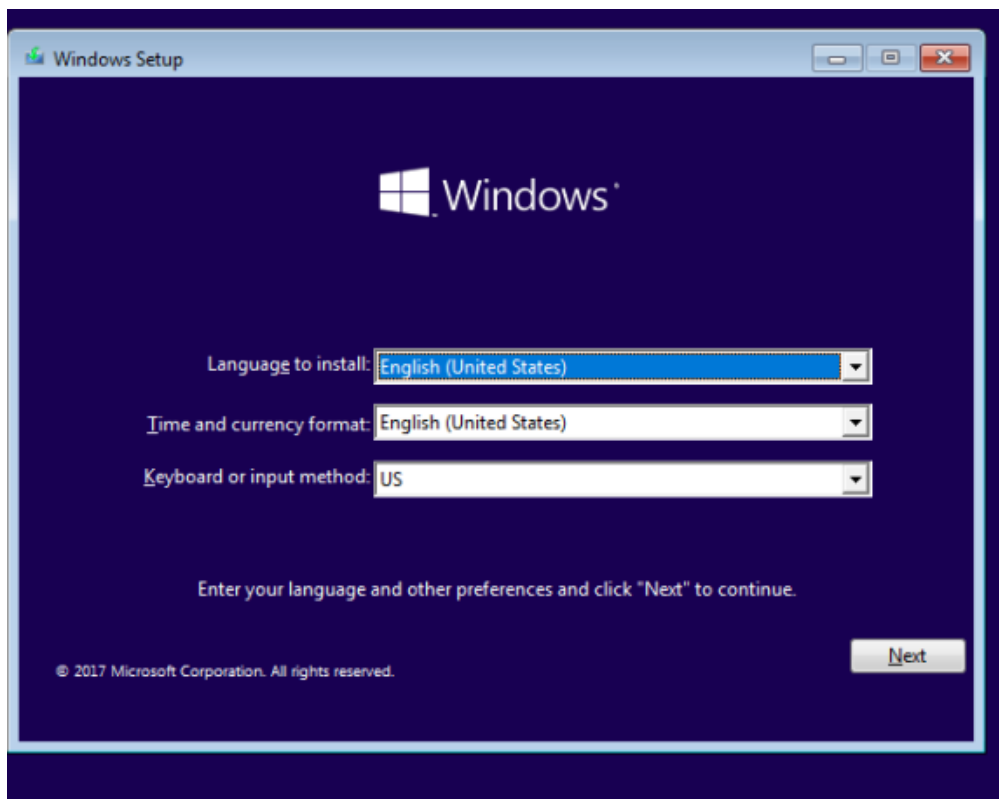
The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

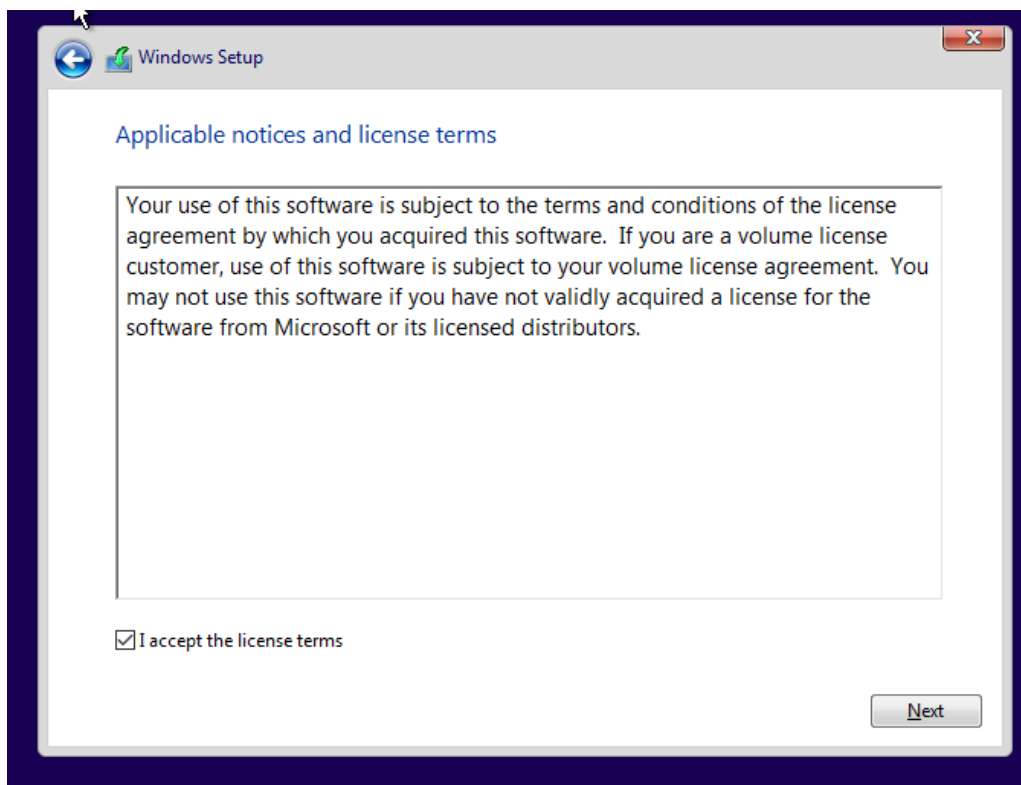
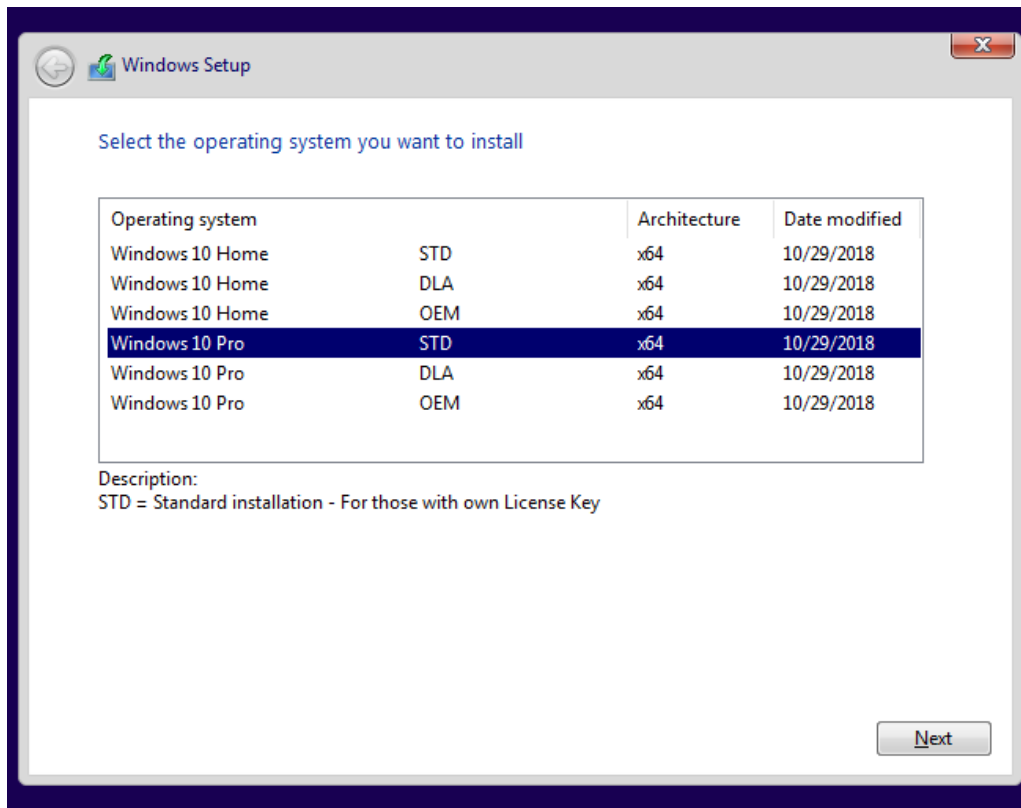
Machine Name and OS Type	
Machine Name	MARE
Machine Folder	G:/VM/MARE
ISO Image	E:/windows OS/Windows_10_All_in_One_RS5_v1809_x64_Jan_2019.iso
Guest OS Type	Windows 10 (64-bit)
Skip Unattended Install	true
Hardware	
Base Memory	4096
Processor(s)	1
EFI Enable	false
Disk	
Disk Size	70.00 GB
Pre-allocate Full Size	false

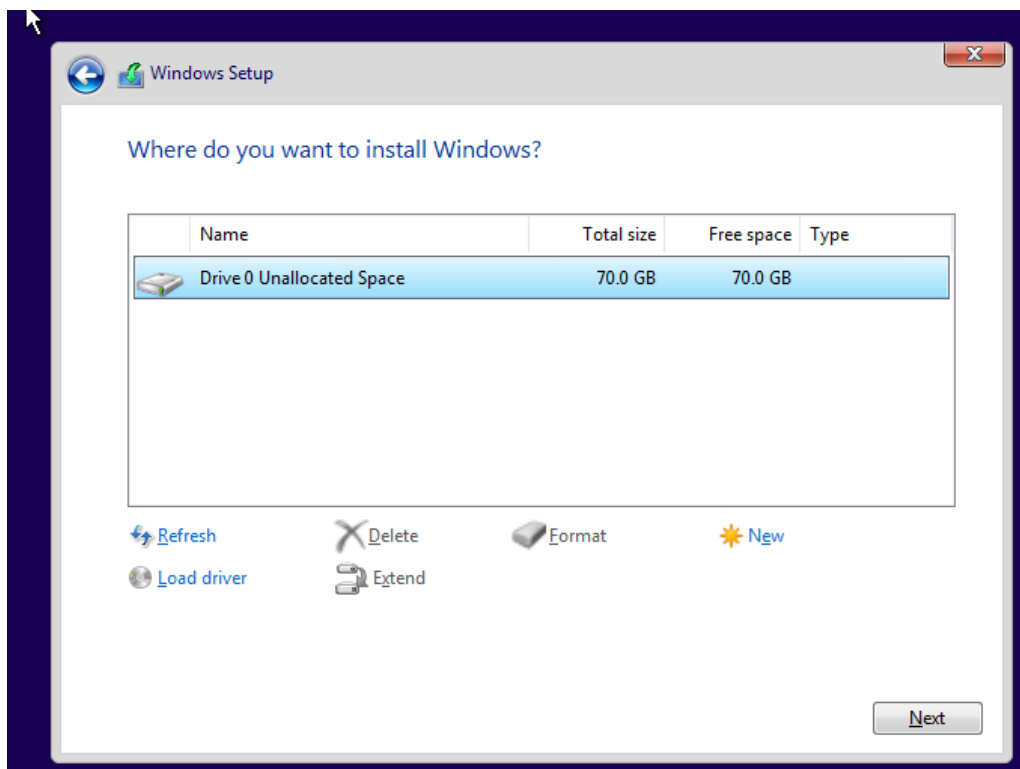
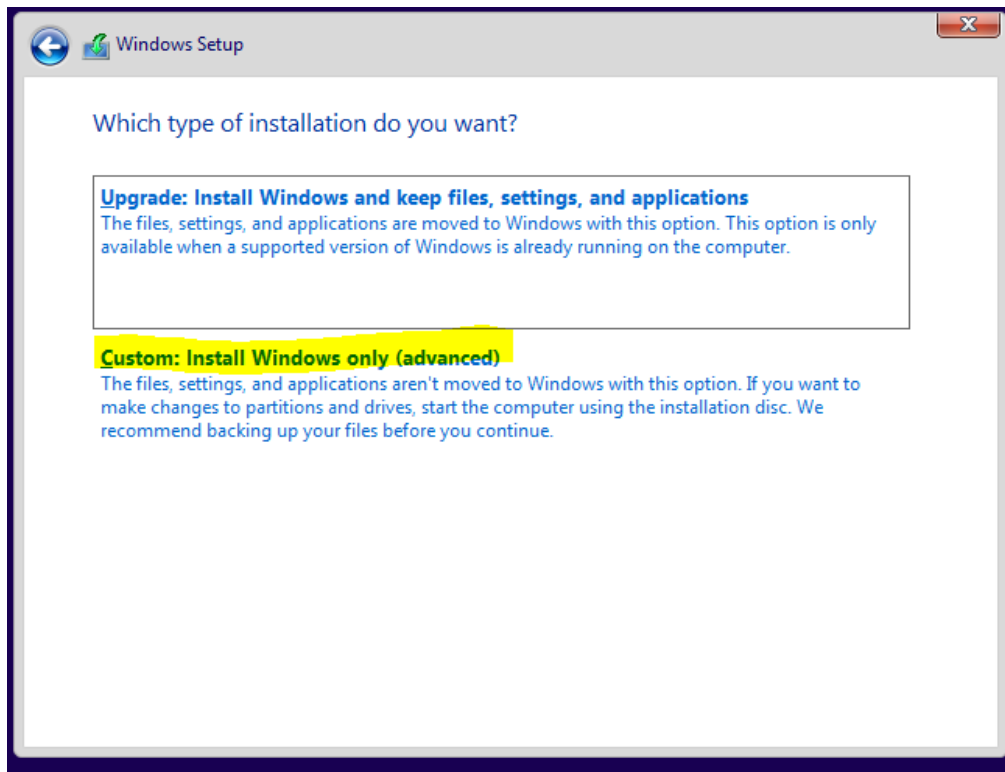
Help

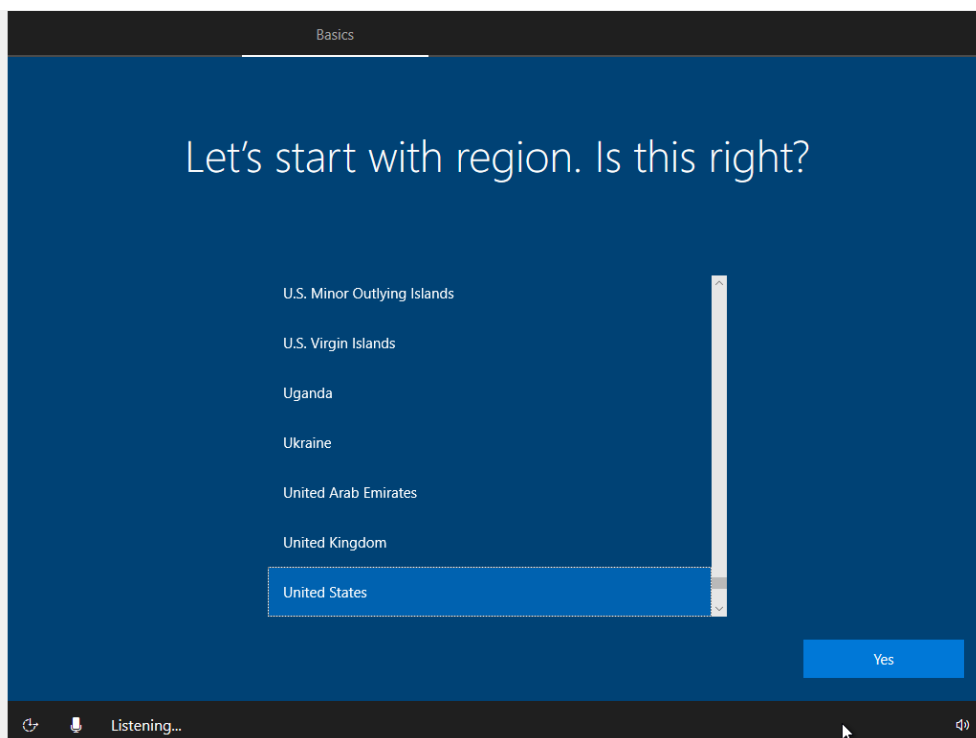
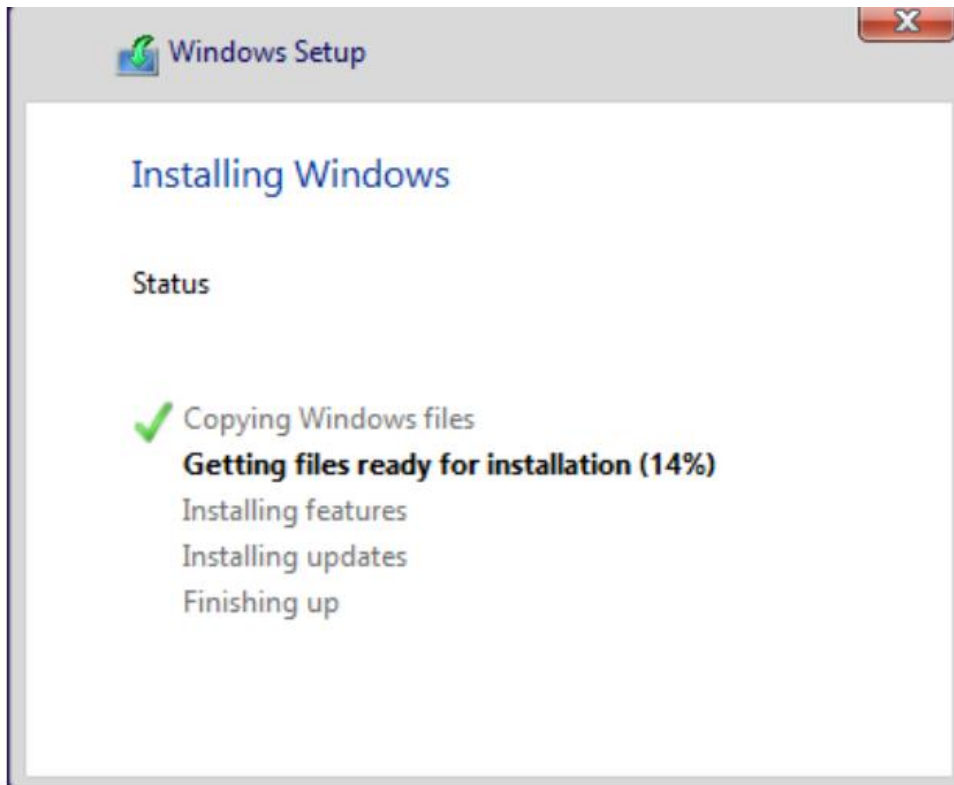
BackFinishCancel

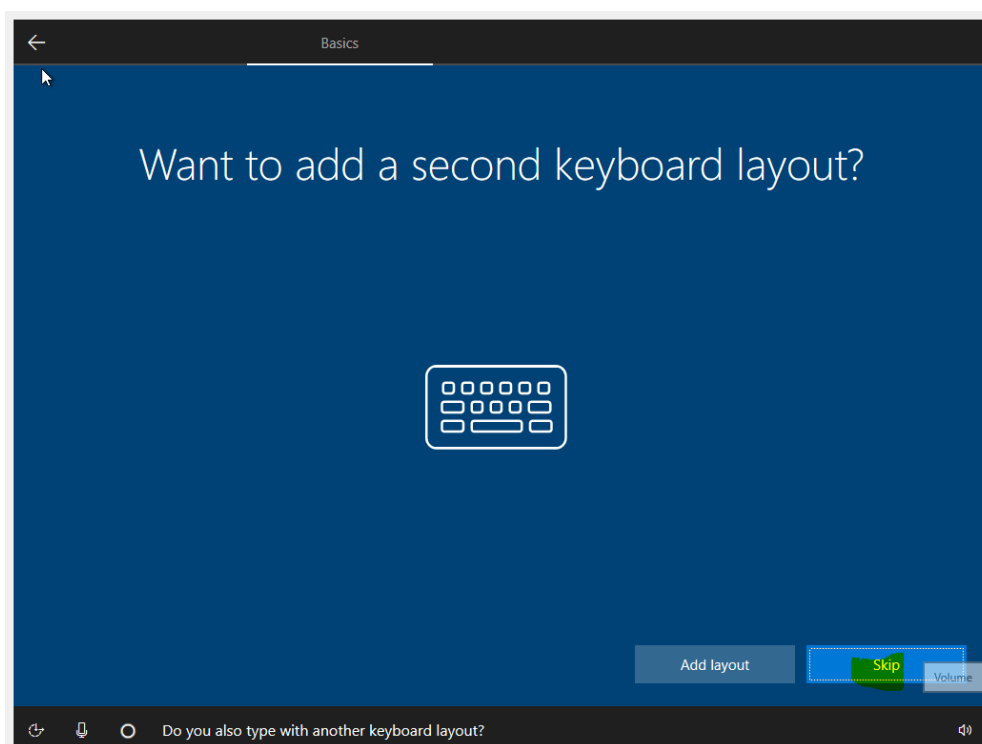
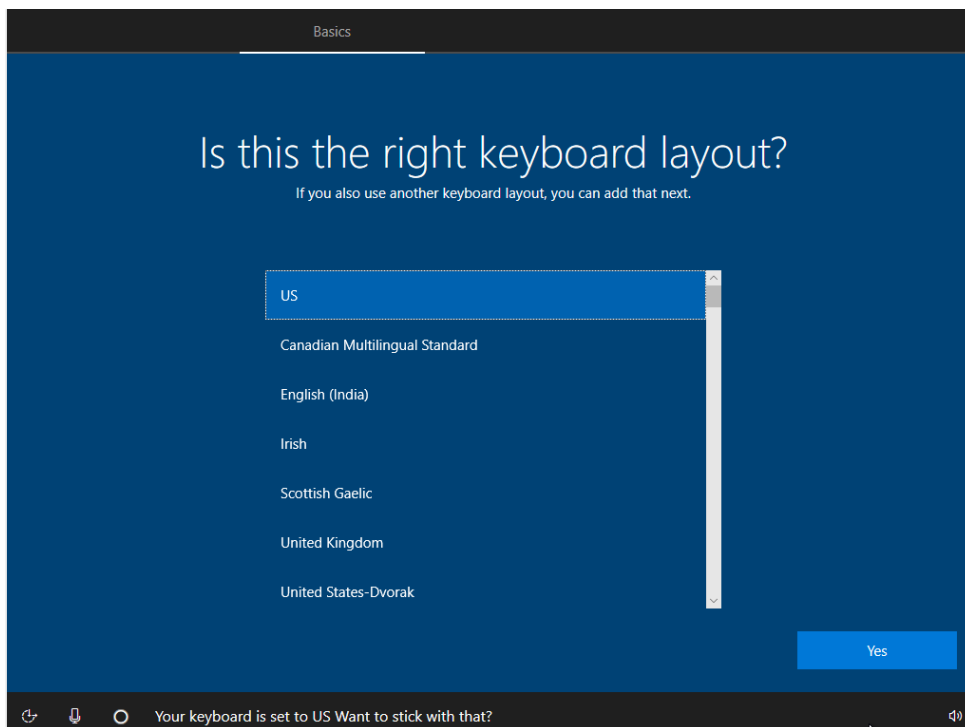
Windows 10 installation












Network


Get the latest from Windows




The newest Windows feature update is ready for you to download and install.
It's about 4 GB, and we'll download it in the background while you continue setting up.

Skip for now

Get it




The newest Windows feature update is ready for you to download and install. Whenever you're ready, say "Get it" and we'll download it in the background while you continue setting up.




Account

How would you like to set up?



Set up for personal use
We'll help you set it up with a personal Microsoft account.
You'll have full control over this device.



Set up for an organization
You'll gain access to your organization's resources like email, network, apps, and services. Your organization will have full control over this device.


Next

←

Account

Let's add your account

One account connects your device across Microsoft apps and services, like Office, OneDrive, Microsoft Edge, and the Microsoft Store.






Create account

Offline account


Privacy & Cookies

Terms of Use

Next



Type your email address or phone number, then follow the instructions to sign in. I'll catch up with you once that's done.




User name and password as per your choice

←

Account

Who's going to use this PC?

What name do you want to use?



Or, even better, use an online account


Next


←

Account

Create a super memorable password




Make sure to pick something you'll absolutely remember.





Or, even better, use an online account

Next





←

Account

Confirm your password




Type your password one last time





Or, even better, use an online account

Next




Question and answer as per your choice

←

Account

Create security questions for this account

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

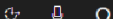


Security question (1 of 3) ▾


Your answer

Or, even better, use an online account

Next




Now you can set up 3 security questions to help you reset your password if you forget it. Choose the first question



Services

Make Cortana your personal assistant?

Hey look, that's me, Cortana!
Can I have permission to use the info I need to do my best work?



To let Cortana provide personalized experiences and relevant suggestions in Microsoft products that offer Cortana experiences, including this device when your device is locked, Microsoft collects and uses information including your location and location history, voice input, speech patterns, contacts, searching history, relationships, calendar details, email, content and communication history from text messages, instant messages and apps, and other information on your device. In Microsoft Edge, Cortana uses your browsing history.

You can always tinker with what Cortana remembers in the Notebook and disable Cortana in Microsoft Edge.


Learn more

Decline

Accept

Services

Do more across devices with activity history



If you want timeline and other Windows features to help you continue what you were doing, even when you switch devices, send Microsoft your activity history, which includes info about websites you browse and how you use apps and services. Select **Learn more** to find out how Microsoft products and services use this data to personalize experiences while respecting your privacy.

[Learn more](#)

No

Yes

Windows can save your spot in apps, files, and websites so you can keep doing what you were doing, even when you switch devices. Just choose Yes to sync your Activities.

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.

Location

Windows and apps can't use your location to provide things like local weather, directions, and Find My Device.

☐ Off

Speech recognition

You can't talk to Cortana or apps from the Store.

☐ Off

Diagnostics

At the basic level, you'll be sending Microsoft less data to help fix errors you encounter.

☐ Basic

Tailored experiences with diagnostic data

The tips you get will be more generic and recommendations may be less relevant to you.

☐ Off

Relevant Ads

The number of ads you see won't change, but they may be less relevant to you.

☐ Off

Select 'Learn more' for info on the above settings, how Windows Defender SmartScreen works, and the related data transfers and uses.

[Learn more](#)

Accept

Recycle Bin

Microsoft Edge

Networks

Network

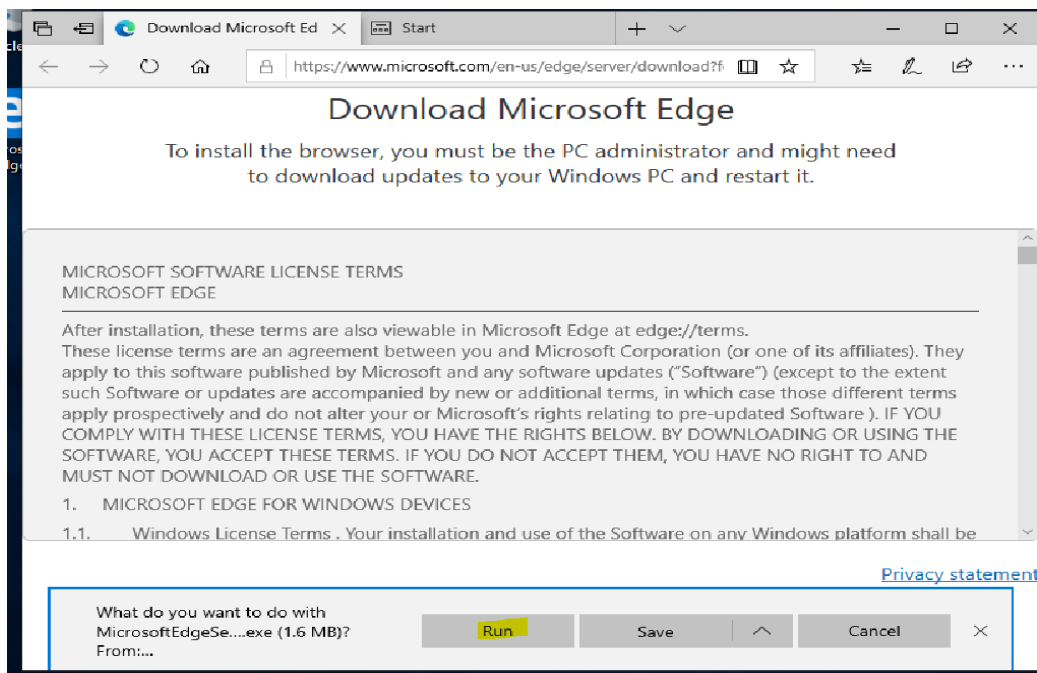
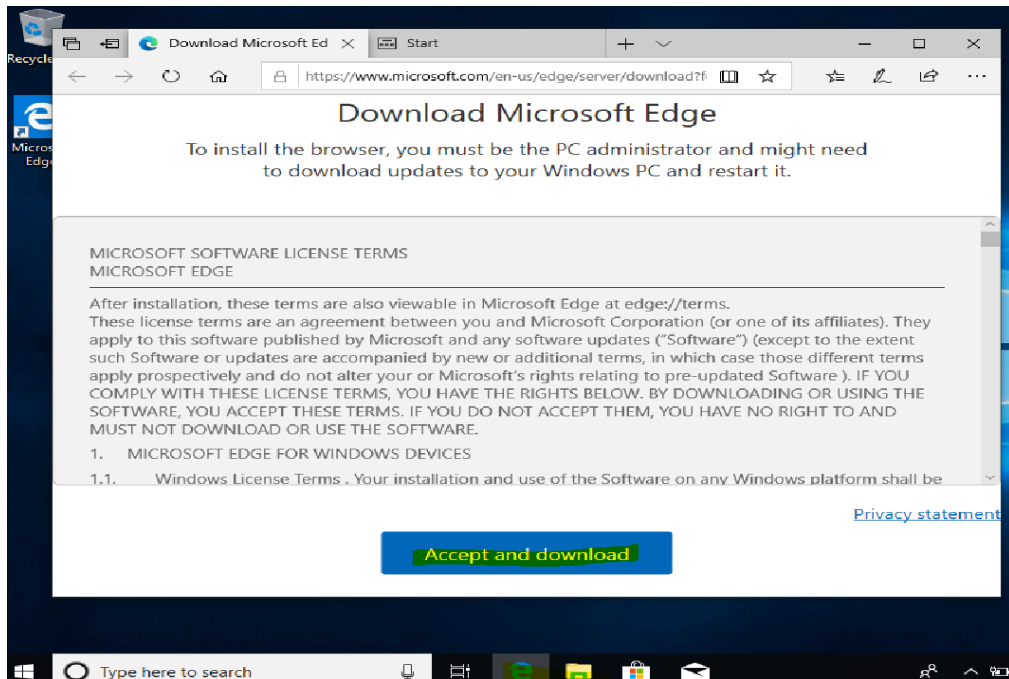
Do you want to allow your PC to be discoverable by other PCs and devices on this network?

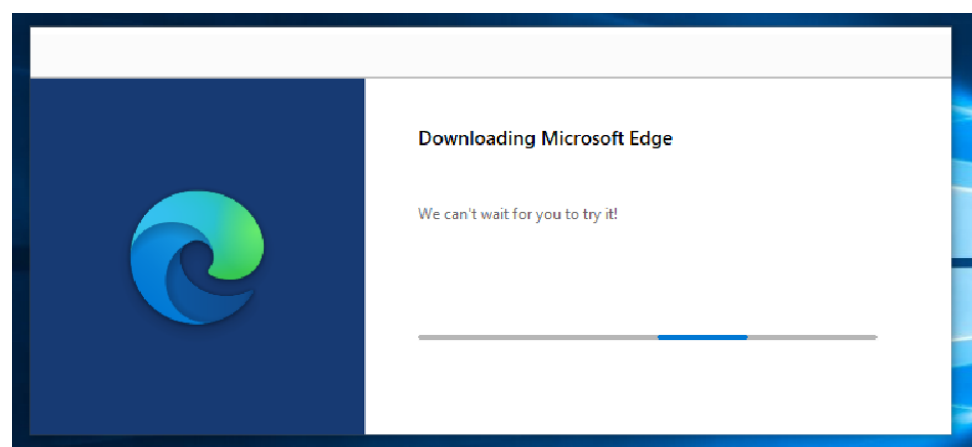
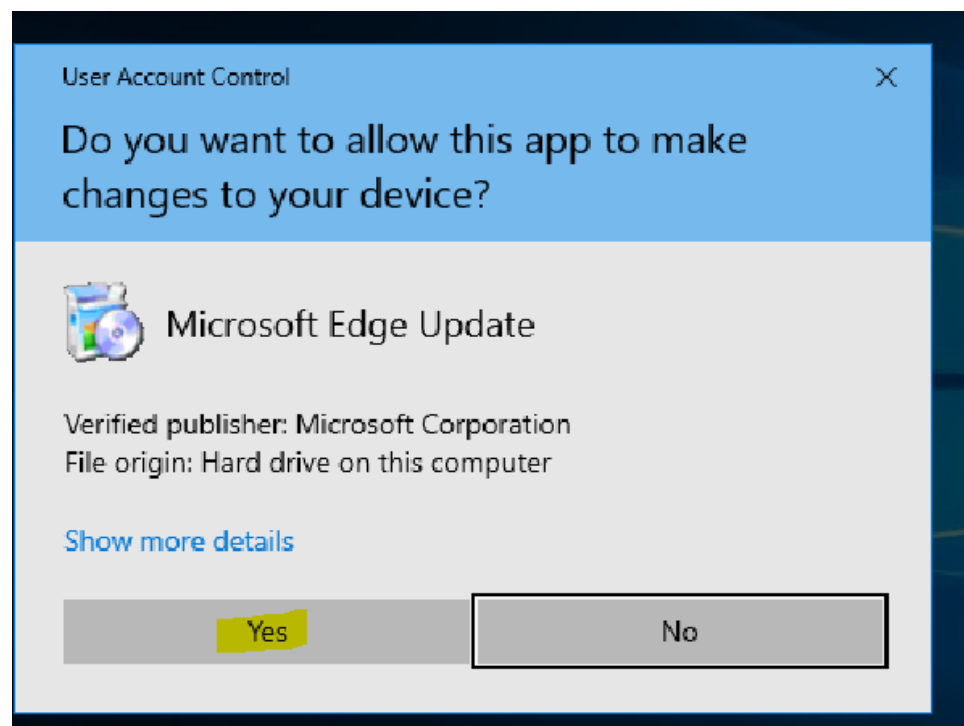
We recommend allowing this on your home and work networks, but not public ones.

Yes

No

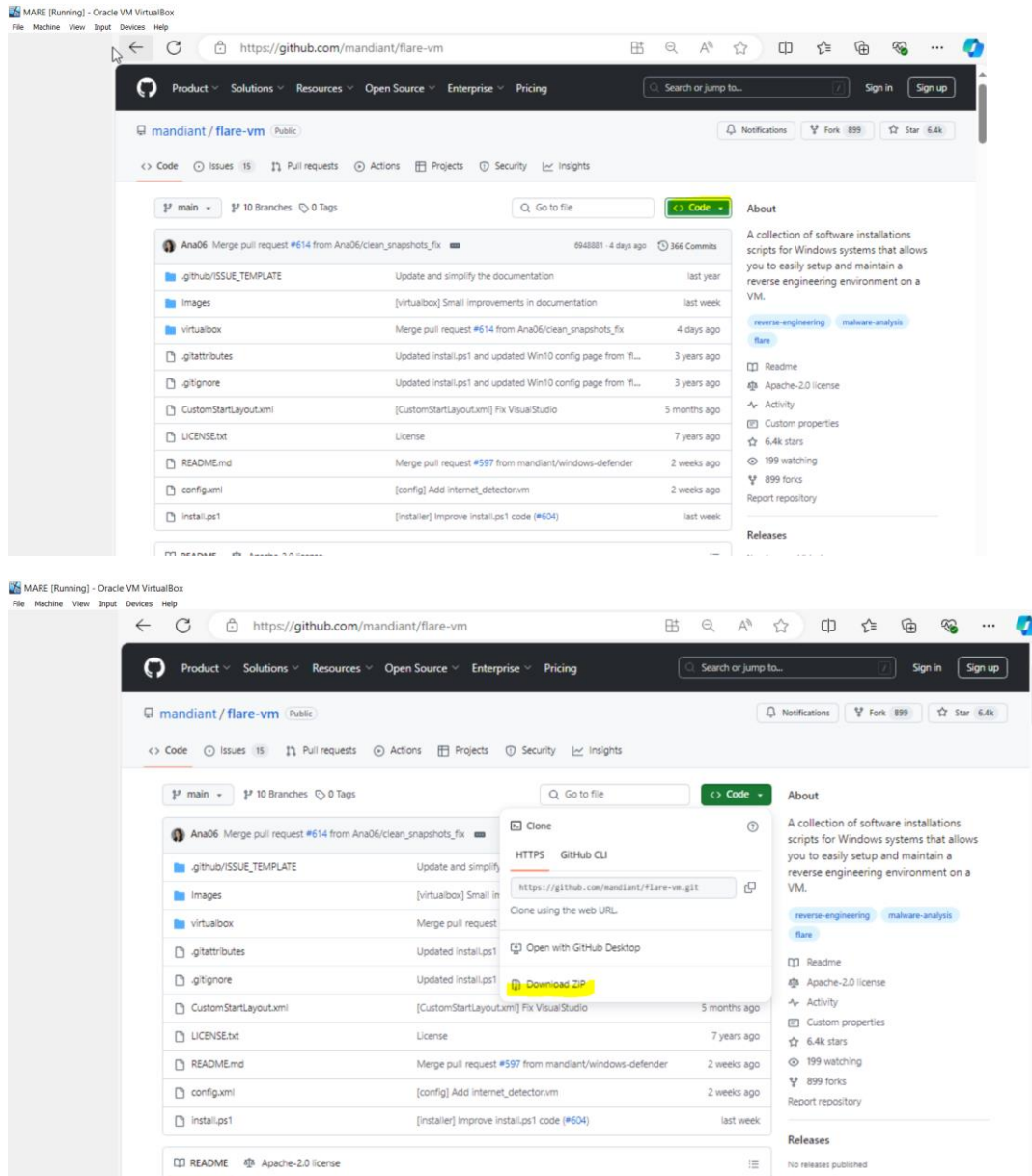
Launch the browser install Microsoft edge





Download the FLARE VM package

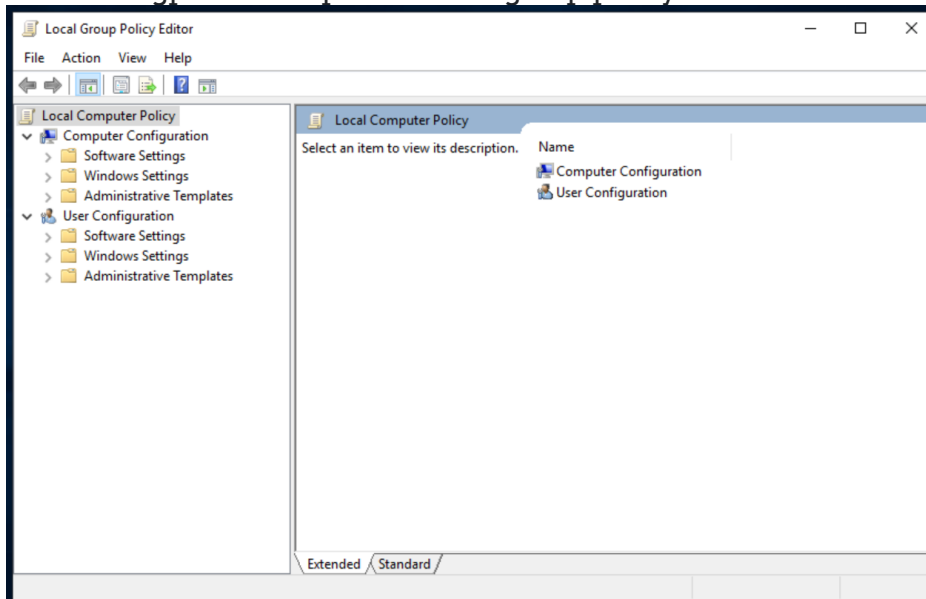
FLARE VM, a PowerShell script that can automatically download and install nearly every tool a malware analyst would need. The script is publicly available on GitHub at the following address: <https://github.com/fireeye/flare-vm>



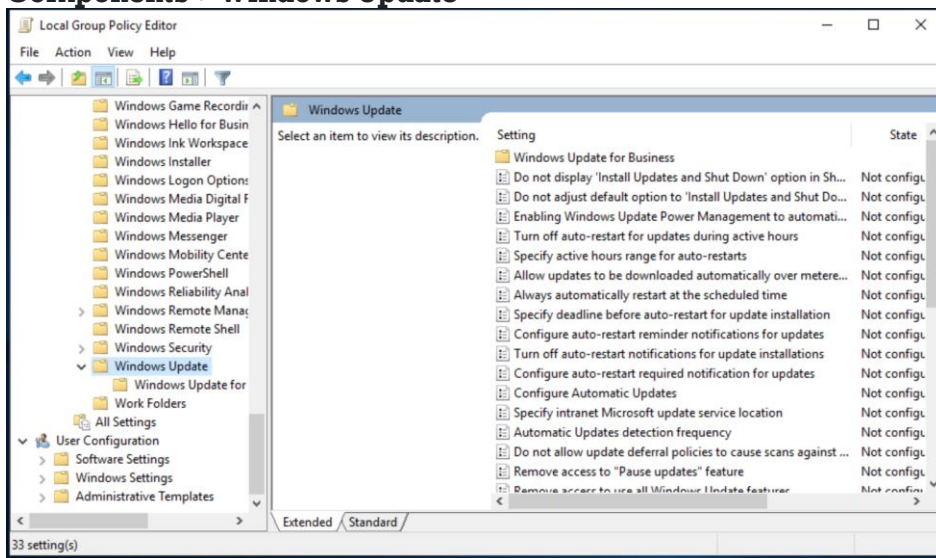
Prerequisite settings

- **Disable Windows Updates (at least until installation is finished)**

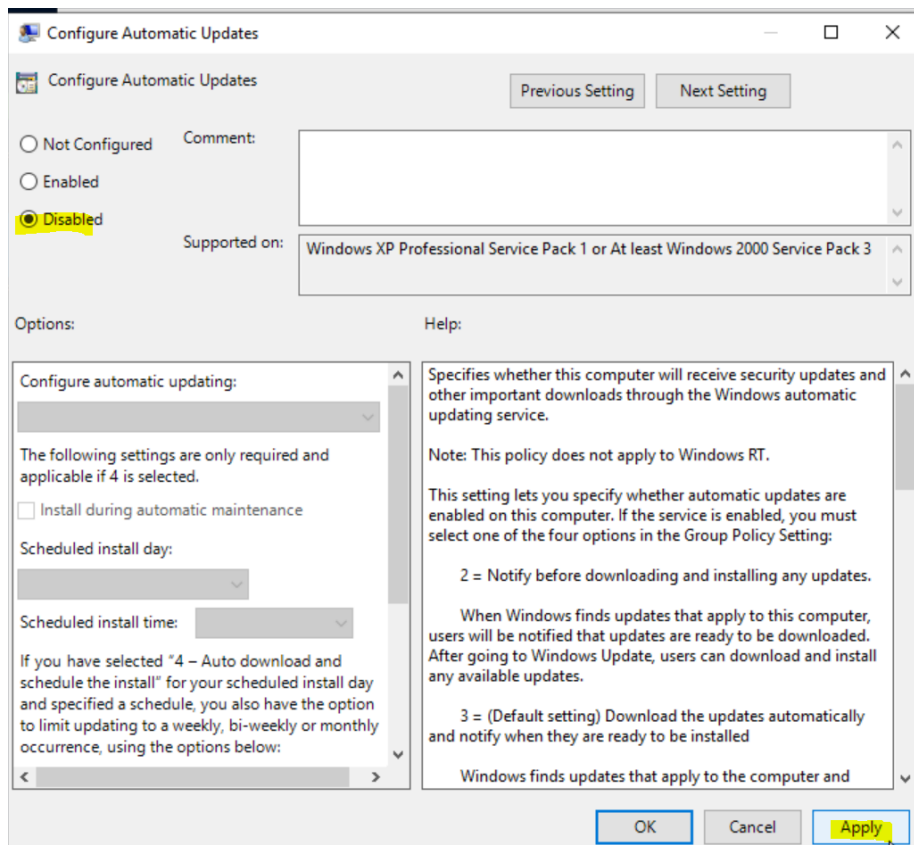
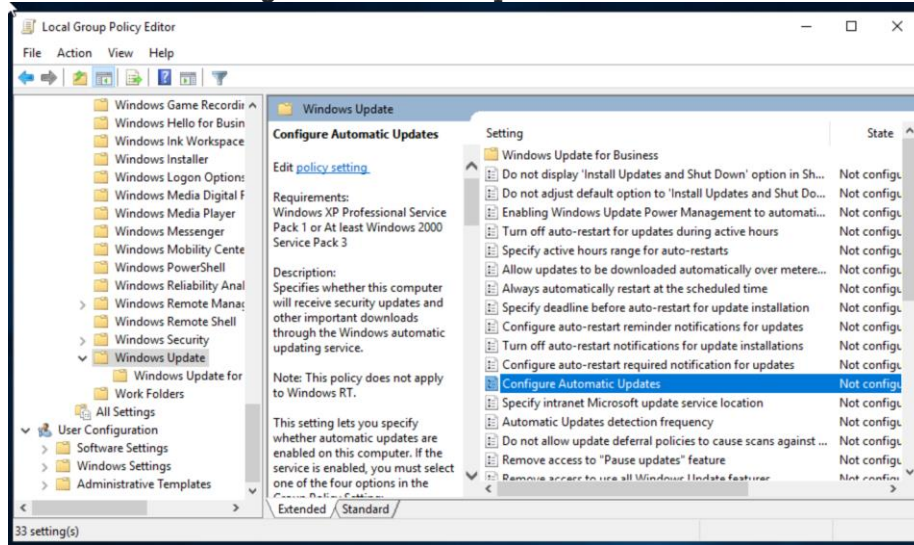
➤ Search for gpedit and open the local group policy editor



➤ Navigate to **computer configuration->Administrative Templates->Windows Components->Windows Update**

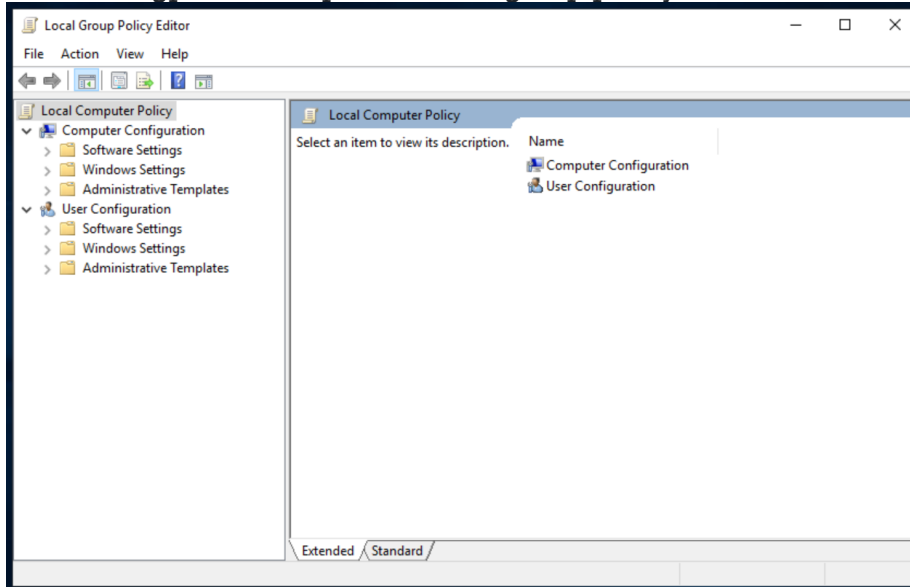


- Double click **Configure Automatic Updates** and disable it.

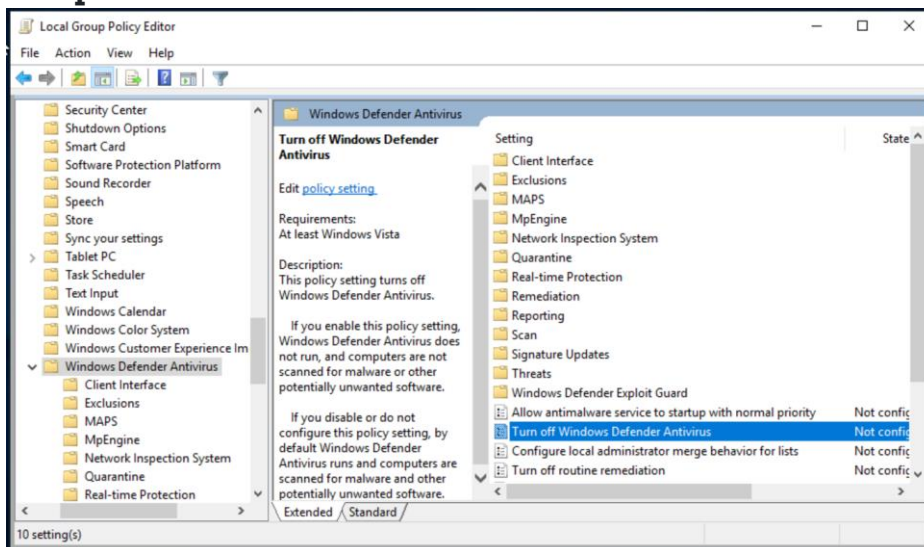


- **Disable Tamper Protection and any Anti-Malware solution (e.g., Windows Defender), preferably via Group Policy.**

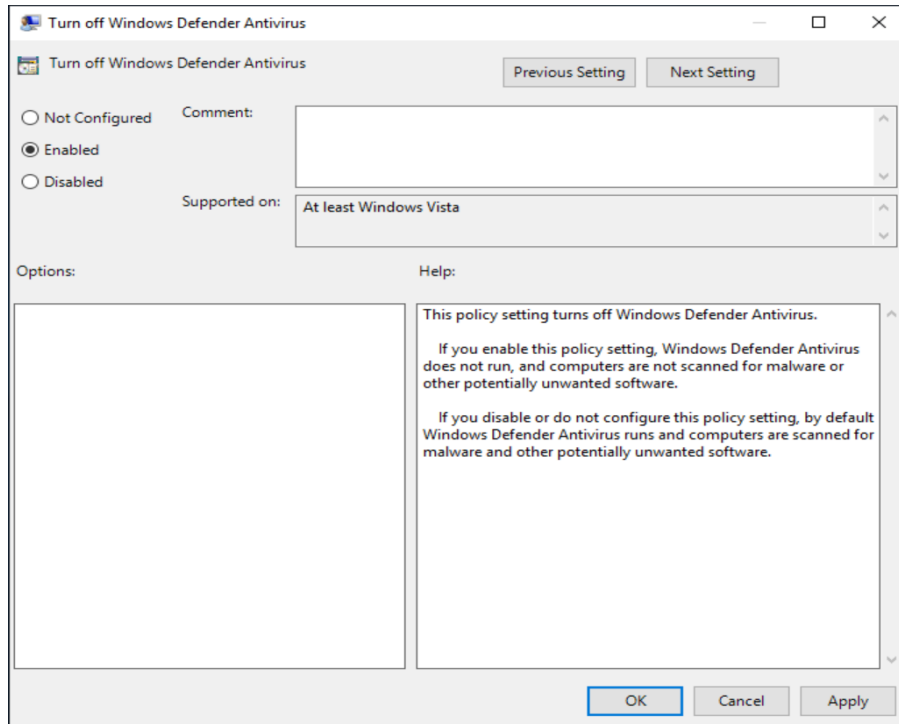
- Search for gpedit and open the local group policy editor



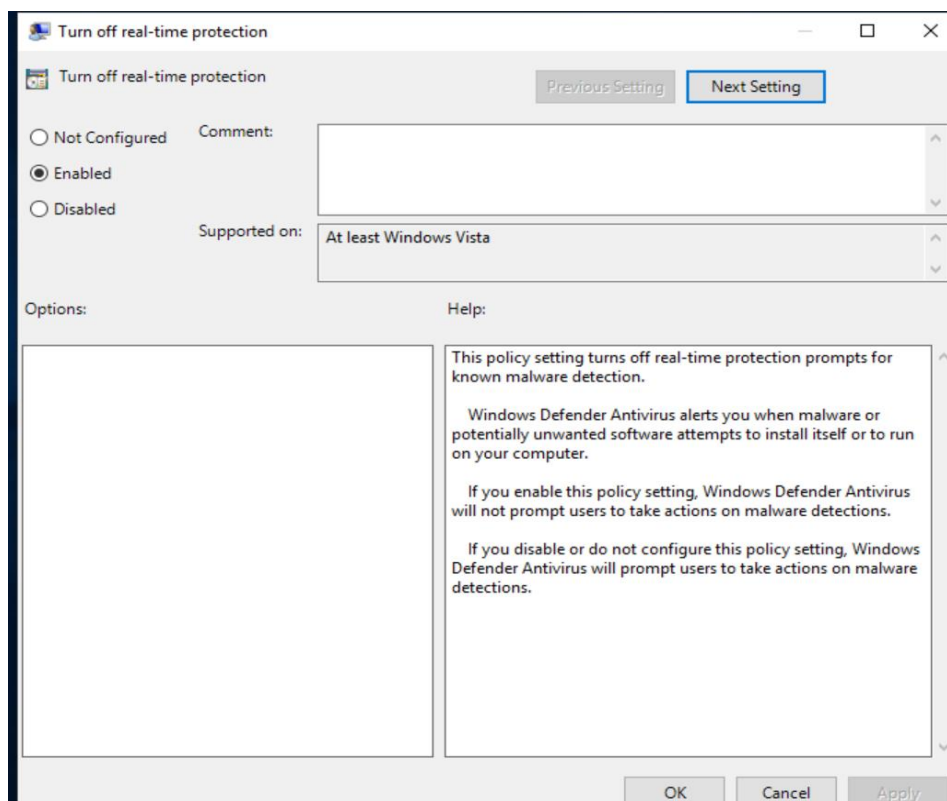
- Navigate to **computer configuration->Administrative Templates->Windows Components->Windows Defender Antivirus**



- Double click on Turn off Windows Defender Antivirus and disable it



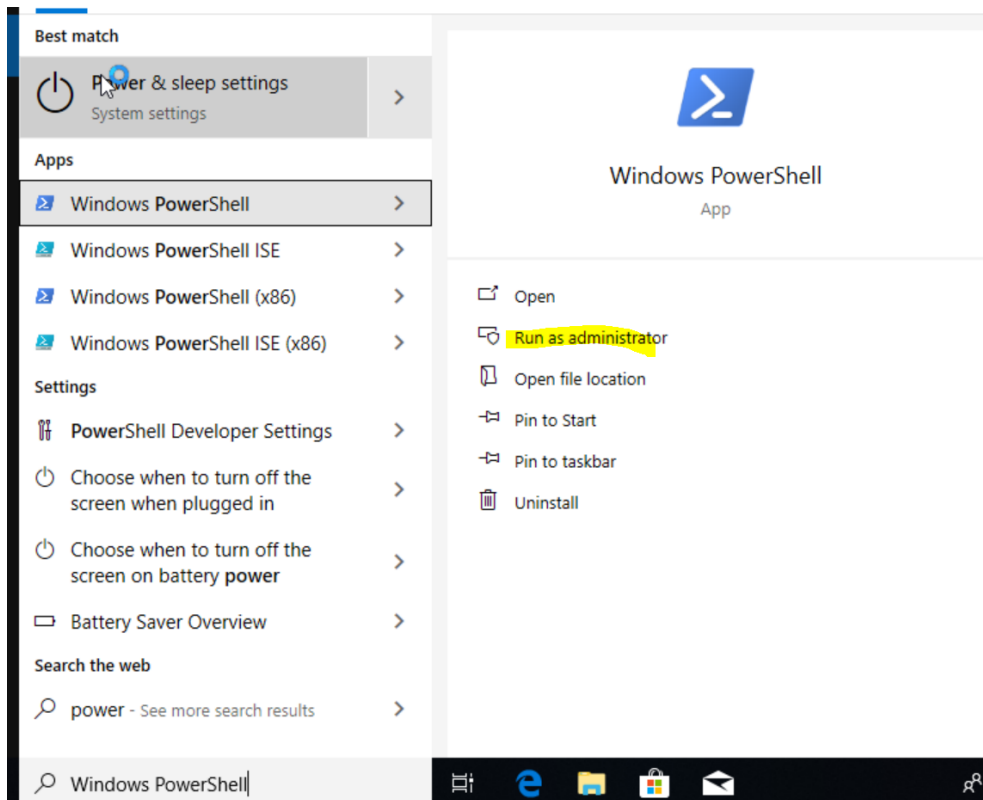
- Navigate to **computer configuration->Administrative Templates->Windows Components->Windows Defender Antivirus->Real-time Protection**
- Double click on Turn off real-time protection



- Install >NET 4.8 framework as well
- Restart the system

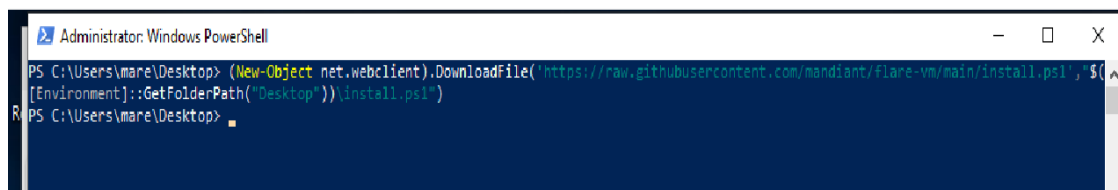
FLARE-VM installation

- Open a PowerShell prompt as administrator



- Download the installation script [installer.ps1](https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1) to your Desktop:
 - `(New-Object net.webclient).DownloadFile('https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1','$([Environment]::GetFolderPath("Desktop"))install.ps1')`

Copy and paste the above in the prompt



```
Administrator: Windows PowerShell
PS C:\Users\mare\Desktop> (New-Object net.webclient).DownloadFile('https://raw.githubusercontent.com/marek-duda/Powercat/master/Powercat.ps1')
[Environment]::GetFolderPath("Desktop")\install.ps1
PS C:\Users\mare\Desktop> dir

Directory: C:\Users\mare\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----          9/13/2024   2:55 AM           46932 install.ps1
-a----          9/13/2024   2:45 AM           2348 Microsoft Edge.lnk

PS C:\Users\mare\Desktop>
```

- Unblock the installation script:
 - Unblock-File .\install.ps1

```
PS C:\Users\mare\Desktop> Unblock-File .\install.ps1
PS C:\Users\mare\Desktop>
```

- Enable script execution:
 - Set-ExecutionPolicy Unrestricted -Force

```
PS C:\Users\mare\Desktop> Set-ExecutionPolicy Unrestricted -Force
PS C:\Users\mare\Desktop>
```

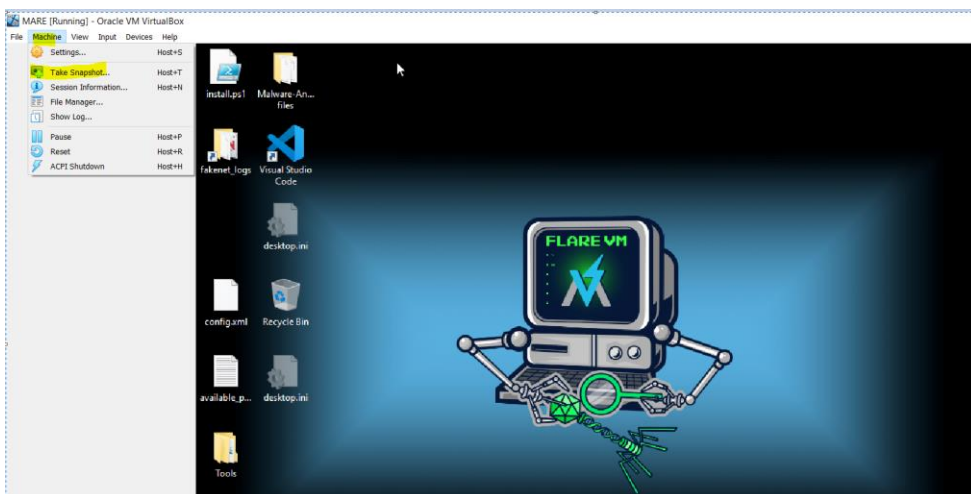
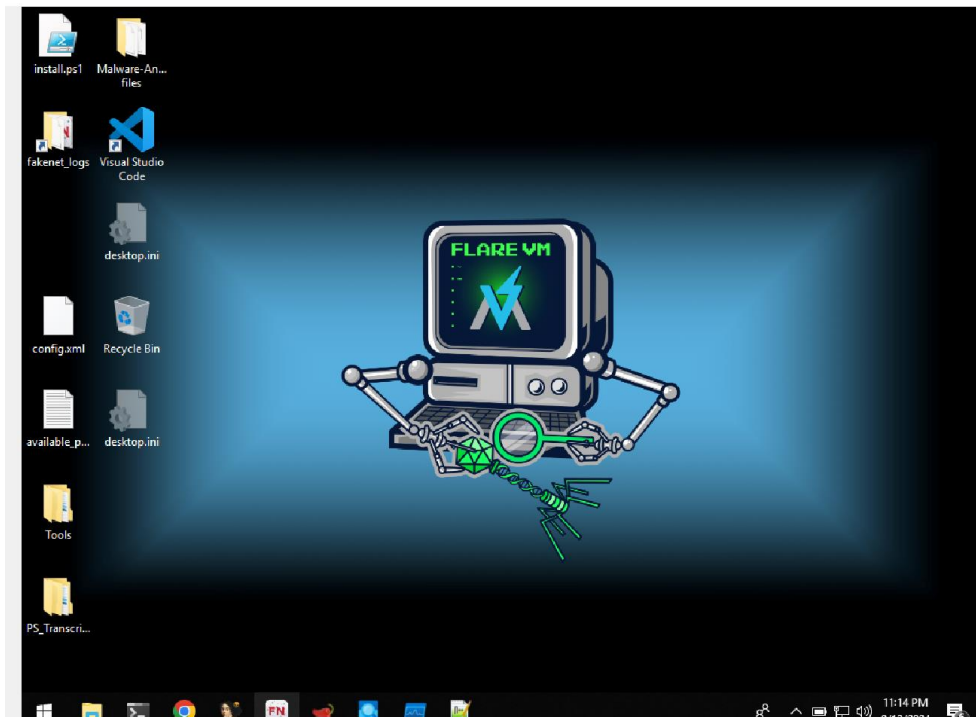
- If you receive an error saying the execution policy is overridden by a policy defined at a more specific scope, you may need to pass a scope in via Set-ExecutionPolicy Unrestricted -Scope CurrentUser -Force. To view execution policies for all scopes, execute Get-ExecutionPolicy -List
- Finally, execute the installer script as follow:
 - .\install.ps1

```
PS C:\Users\mare\Desktop> .\install.ps1
[+] Checking if PowerShell version is compatible...
    [+] Installing with PowerShell version 5.1.17763.134
[+] Checking if script is running as administrator...
    [+] Running as administrator
[+] Checking if execution policy is unrestricted...
    [+] Execution policy is unrestricted
[+] Checking to make sure Operating System is compatible...
    [+] Installing on Windows version 17763
[+] Checking for spaces in the username...
    [+] Username ' ' does not contain any spaces.
[+] Checking if host has enough disk space...
    [+] Disk is larger than 60 GB
[+] Checking for Internet connectivity (google.com)...
    [+] Internet connectivity check for google.com passed
[+] Checking for Internet connectivity (github.com)...
```

```
[+] Network connectivity looks good
[+] Checking if Windows Defender Tamper Protection is disabled...
[+] Tamper Protection is either not enabled or not detected
[-] Do you still wish to proceed? (Y/N): Y
[+] Checking if Windows Defender service is disabled...
[!] Please disable Windows Defender through Group Policy, reboot, and rerun installer
[+] Hint: https://stackoverflow.com/questions/62174426/how-to-permanently-disable-windows-defender-real-time-protection-with-gpo
[+] Hint: https://www.windowscentral.com/how-permanently-disable-windows-defender-windows-10
[+] Hint: https://github.com/jeremybeaume/tools/blob/master/disable-defender.ps1
[+] You are welcome to continue, but may experience errors downloading or installing packages
[-] Do you still wish to proceed? (Y/N): Y
[+] Setting password to never expire to avoid that a password expiration blocks the installation...
[-] Have you taken a VM snapshot to ensure you can revert to pre-installation state? (Y/N): Y
[+] Getting user credentials ...

Windows PowerShell credential request
Enter your credentials.
Password for user mare: *****
```

Take a snapshot with all the tools installed before performing any malware analysis and reverse engineering



Isolating your environment

