

Setup Instructions:

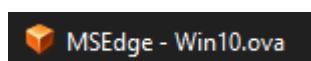
- Installing Windows 10 VM.
- System configuration and downloading attack script.
- Execution of attack script.

Installing VirtualBox

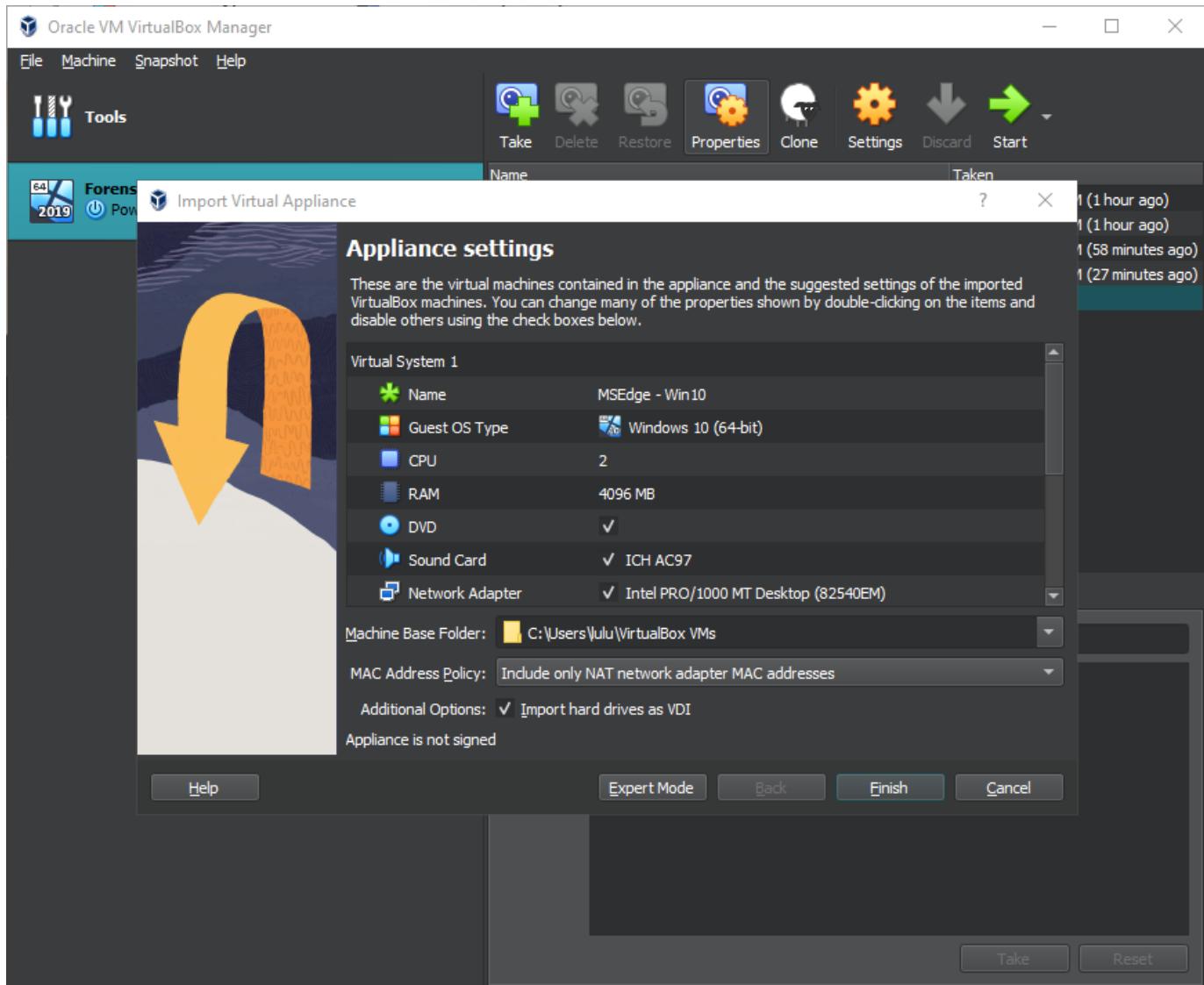
- Link: <https://archive.org/details/msedge.win10.virtualbox>
- You should have:

Name	Date	Type	Size	Tags
_ia_thumb.jpg	2/8/2023 7:50 PM	JPG File	10 KB	
MSEdge.Win10.VirtualBox.zip	2/8/2023 7:50 PM	Compressed (zipp...)	4,462,871 KB	
msedge.win10.virtualbox_meta.sqlite	2/8/2023 7:50 PM	SQlite File	26 KB	
msedge.win10.virtualbox_meta.xml	2/8/2023 7:50 PM	XML Document	2 KB	
screenshot-1.png	2/8/2023 7:50 PM	PNG File	162 KB	
screenshot-1_thumb.jpg	2/8/2023 7:50 PM	JPG File	5 KB	
screenshot-2.png	2/8/2023 7:50 PM	PNG File	247 KB	
screenshot-2_thumb.jpg	2/8/2023 7:50 PM	JPG File	4 KB	
screenshot-3.png	2/8/2023 7:50 PM	PNG File	138 KB	
screenshot-3_thumb.jpg	2/8/2023 7:50 PM	JPG File	6 KB	
screenshot-4.png	2/8/2023 7:50 PM	PNG File	10 KB	
screenshot-4_thumb.jpg	2/8/2023 7:50 PM	JPG File	3 KB	
screenshot-5.png	2/8/2023 7:50 PM	PNG File	360 KB	
screenshot-5_thumb.jpg	2/8/2023 7:50 PM	JPG File	3 KB	

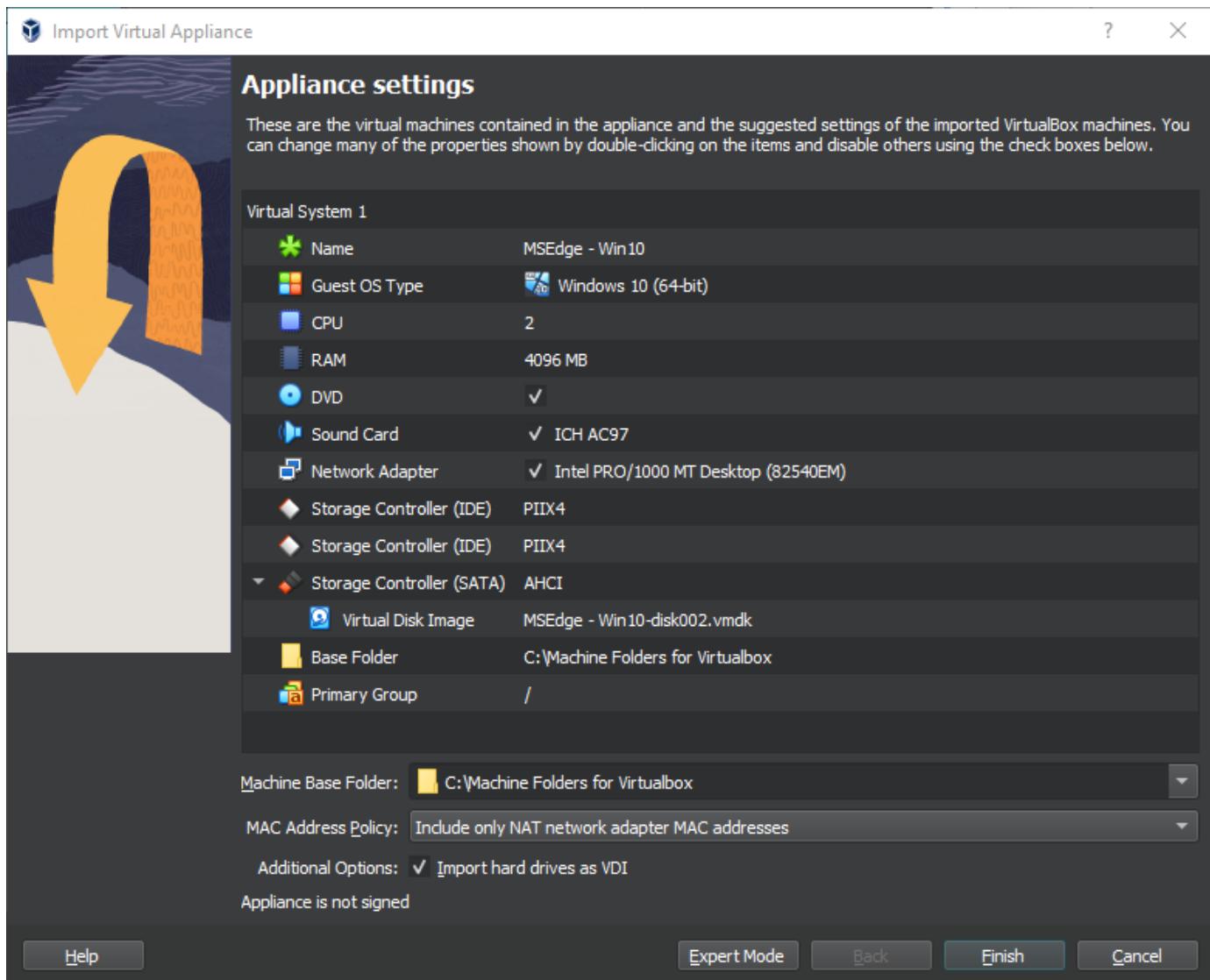
- Enter zip file and extract the .ova file to C:\VMs (in my case):



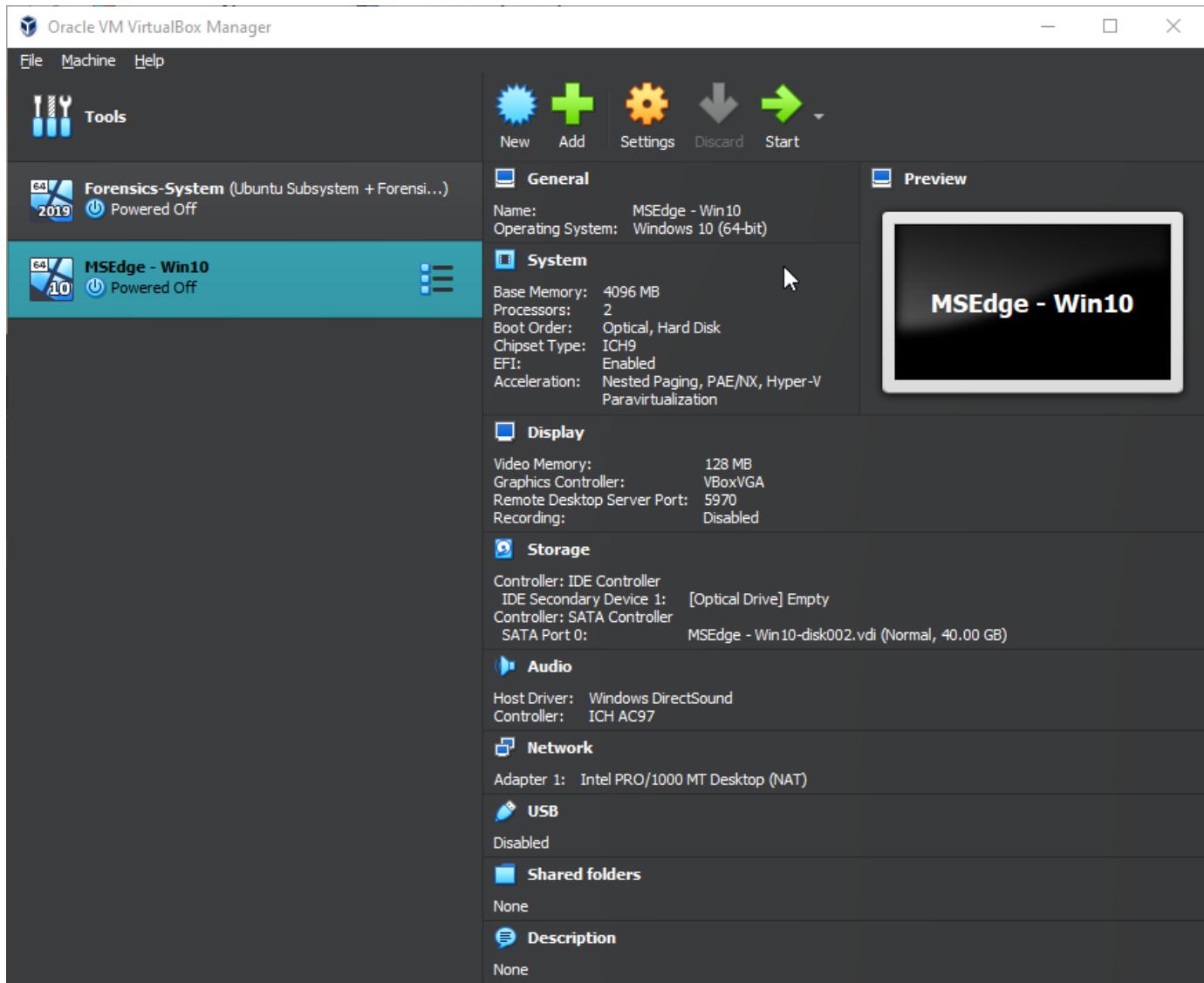
- Double Click on the file:



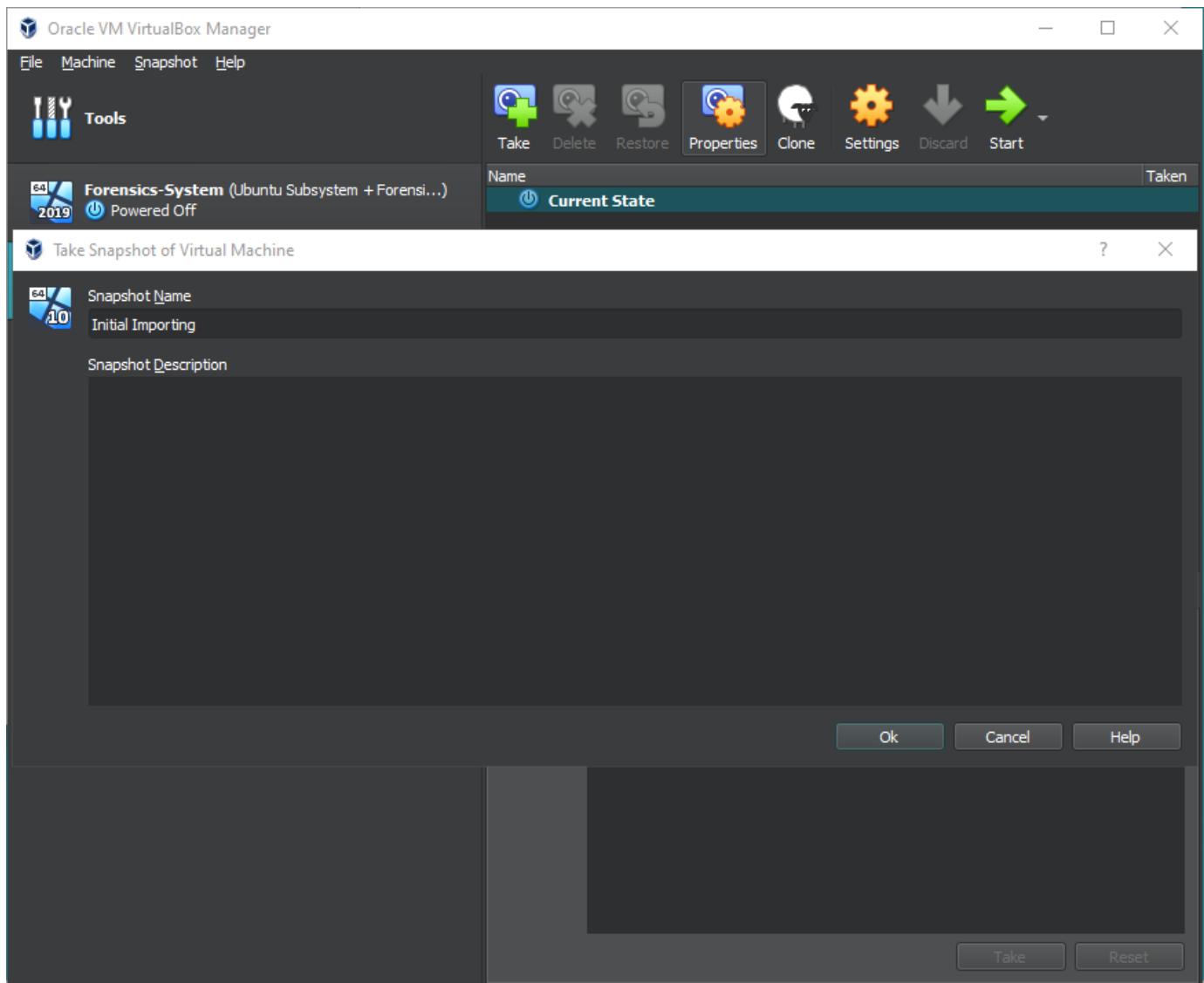
- Change the Machine Base Folder:

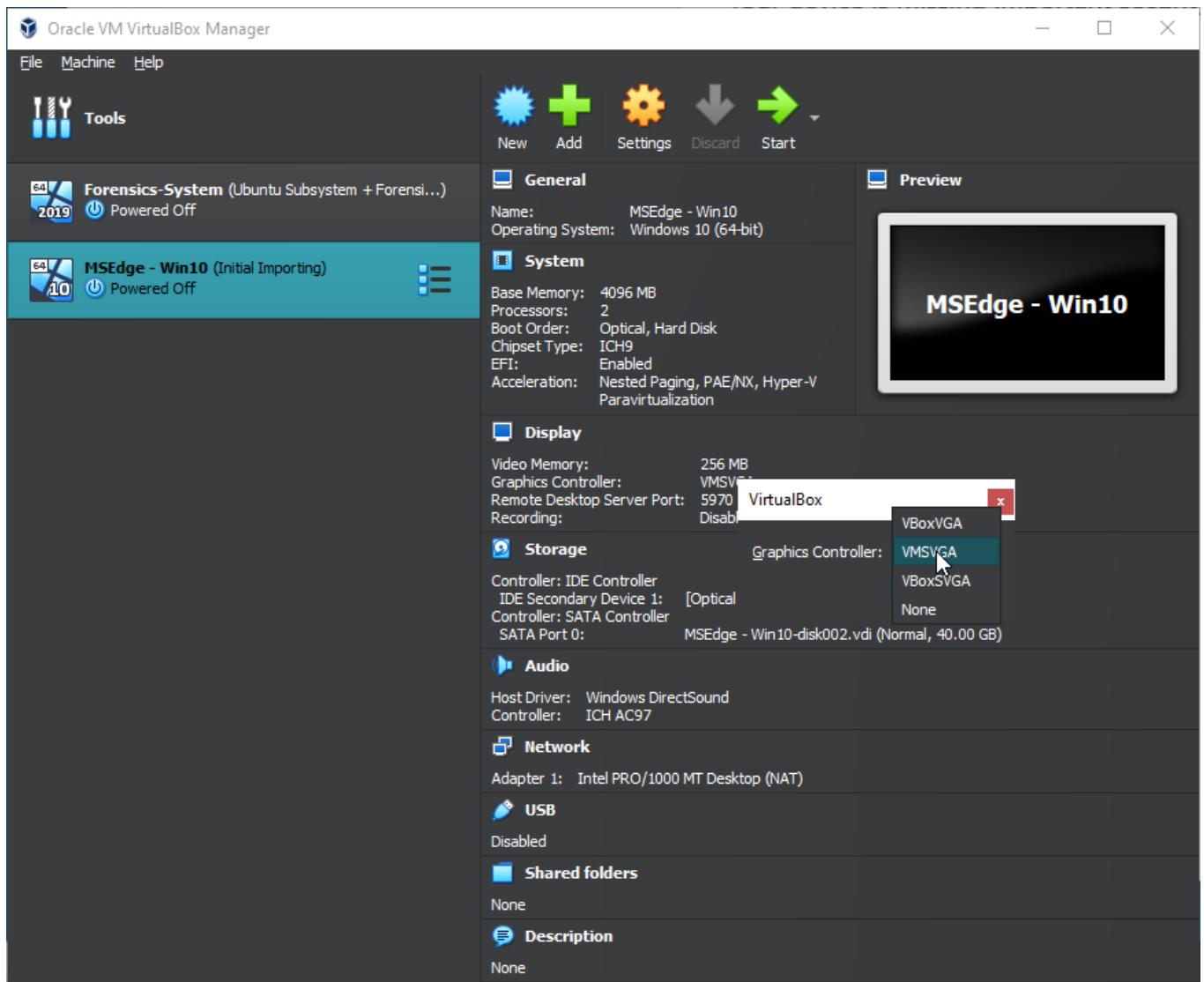


- There should be enough resources on the compromised virtual machine, press finish to finish importing:

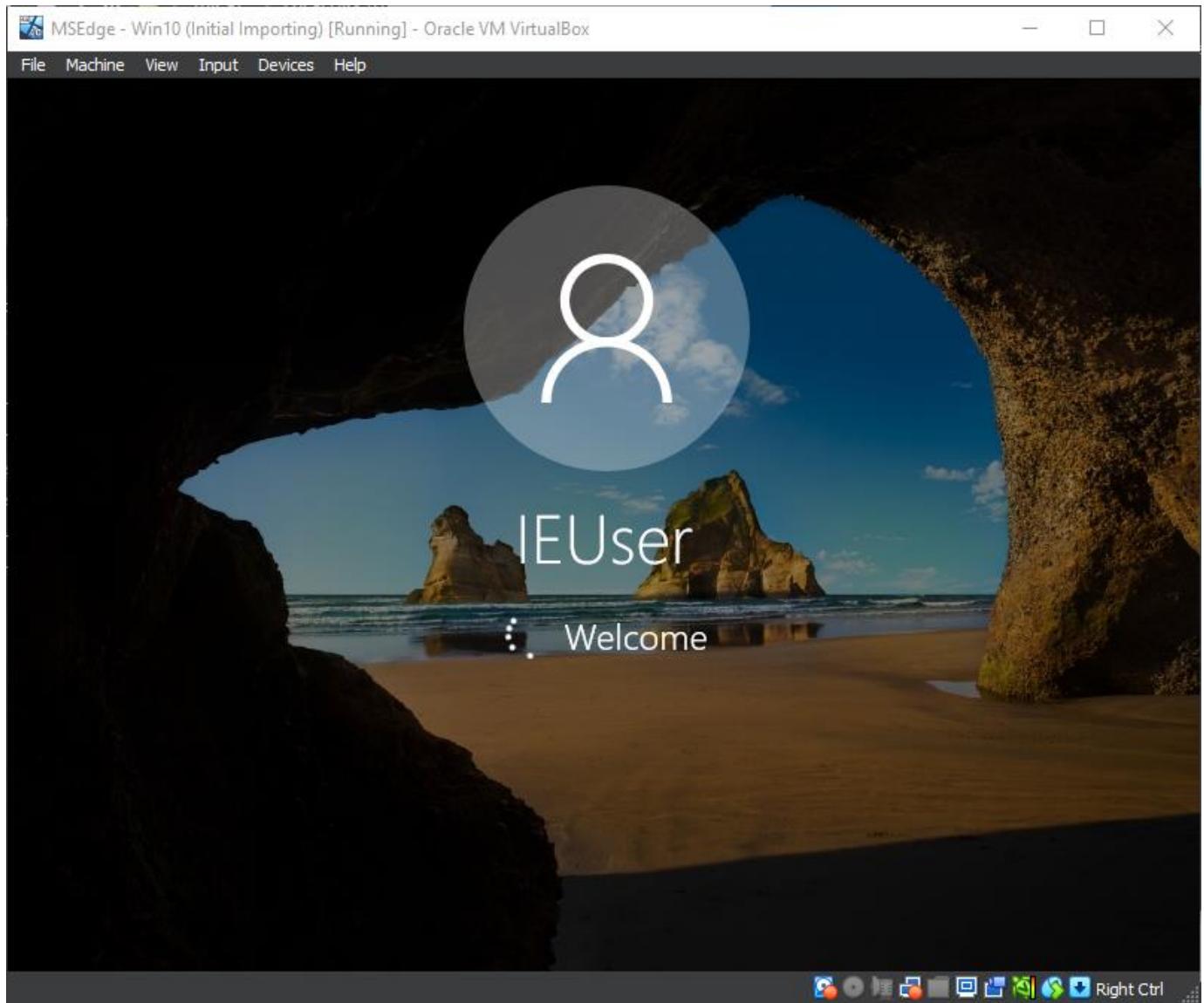


- Take an initial snapshot + Change Graphics Controller to VMSVGA boot, shutdown, then to VBoxVGA, then boot:



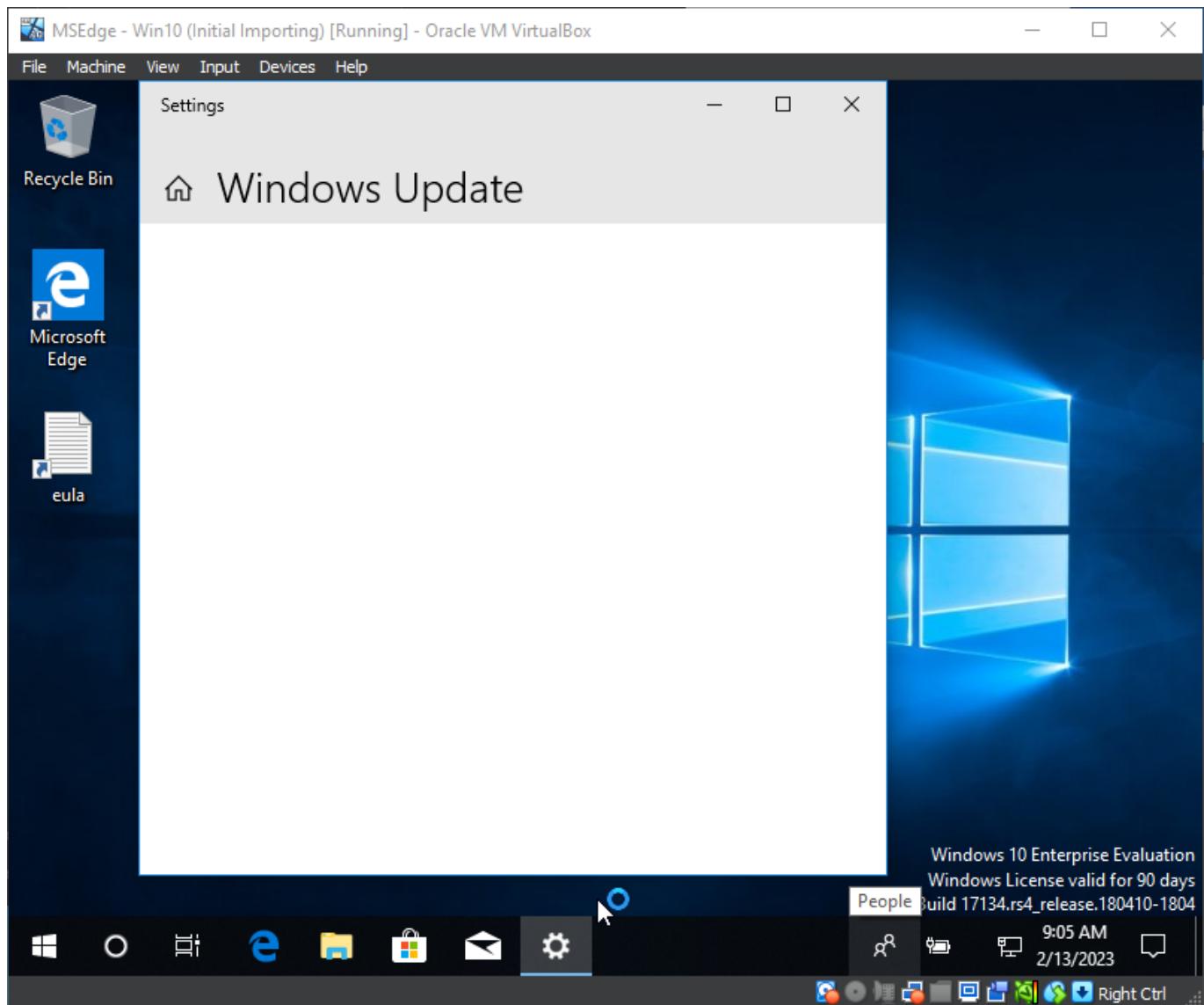


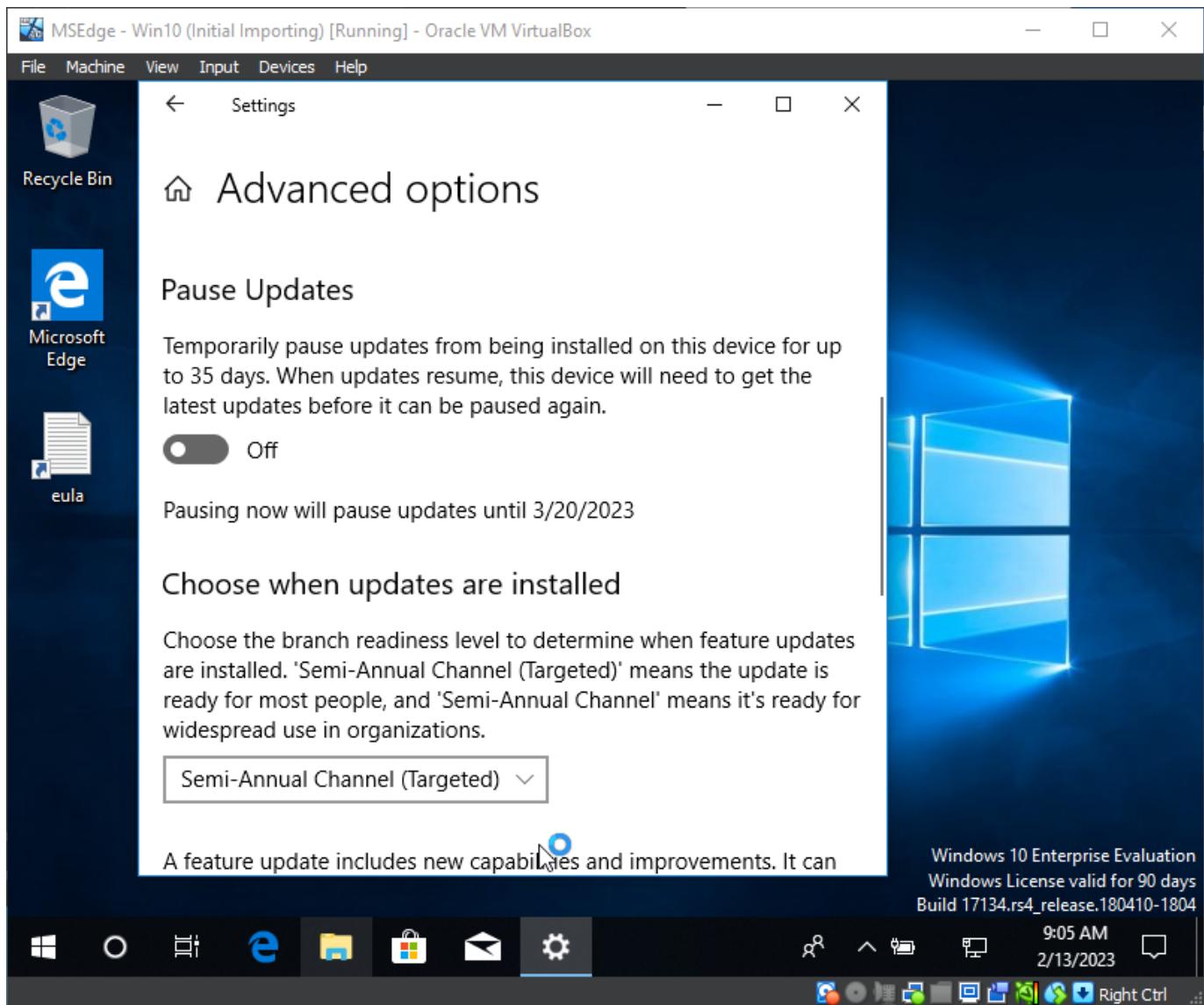
- Start the virtual machine:



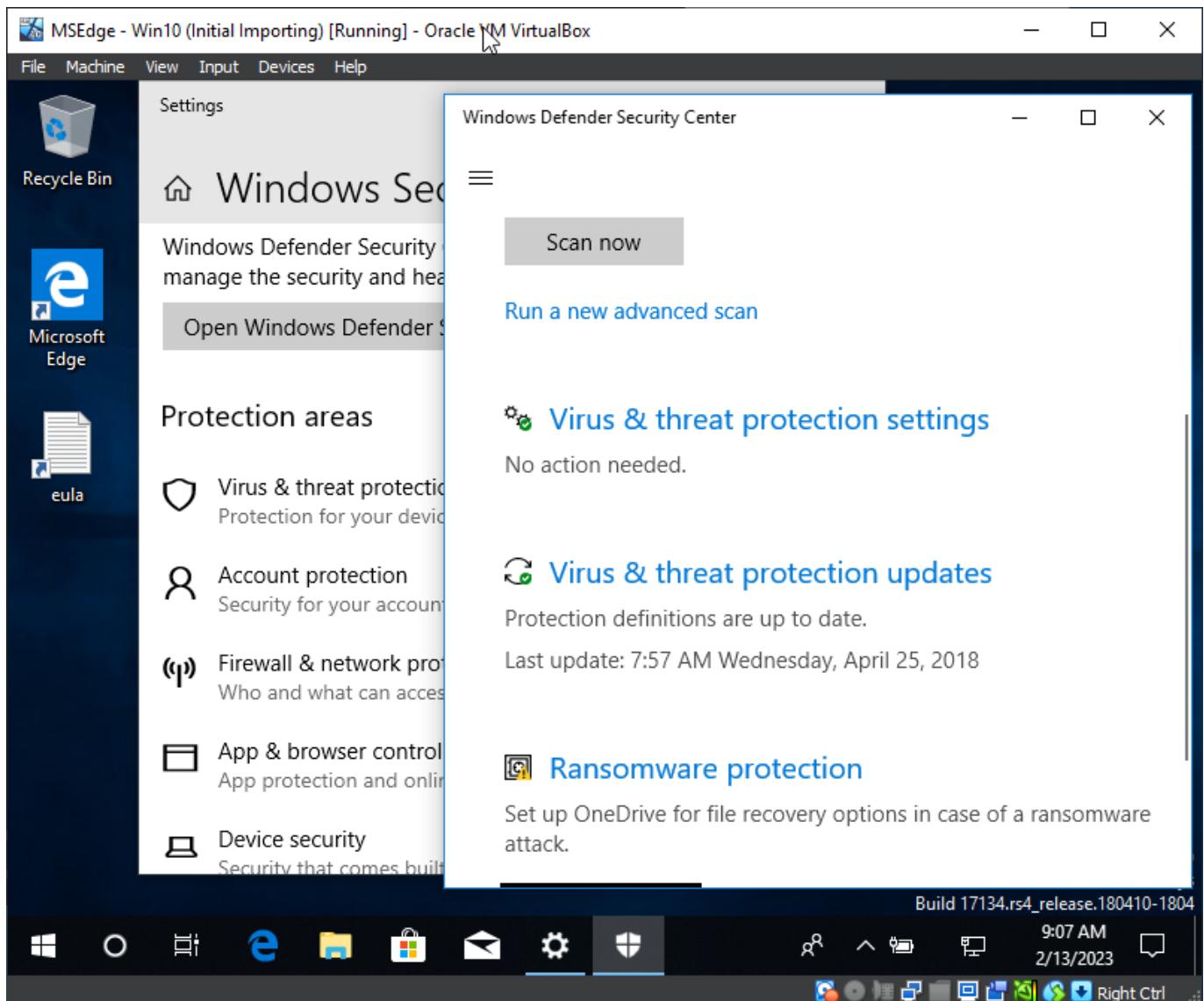
System configuration and downloading attack script

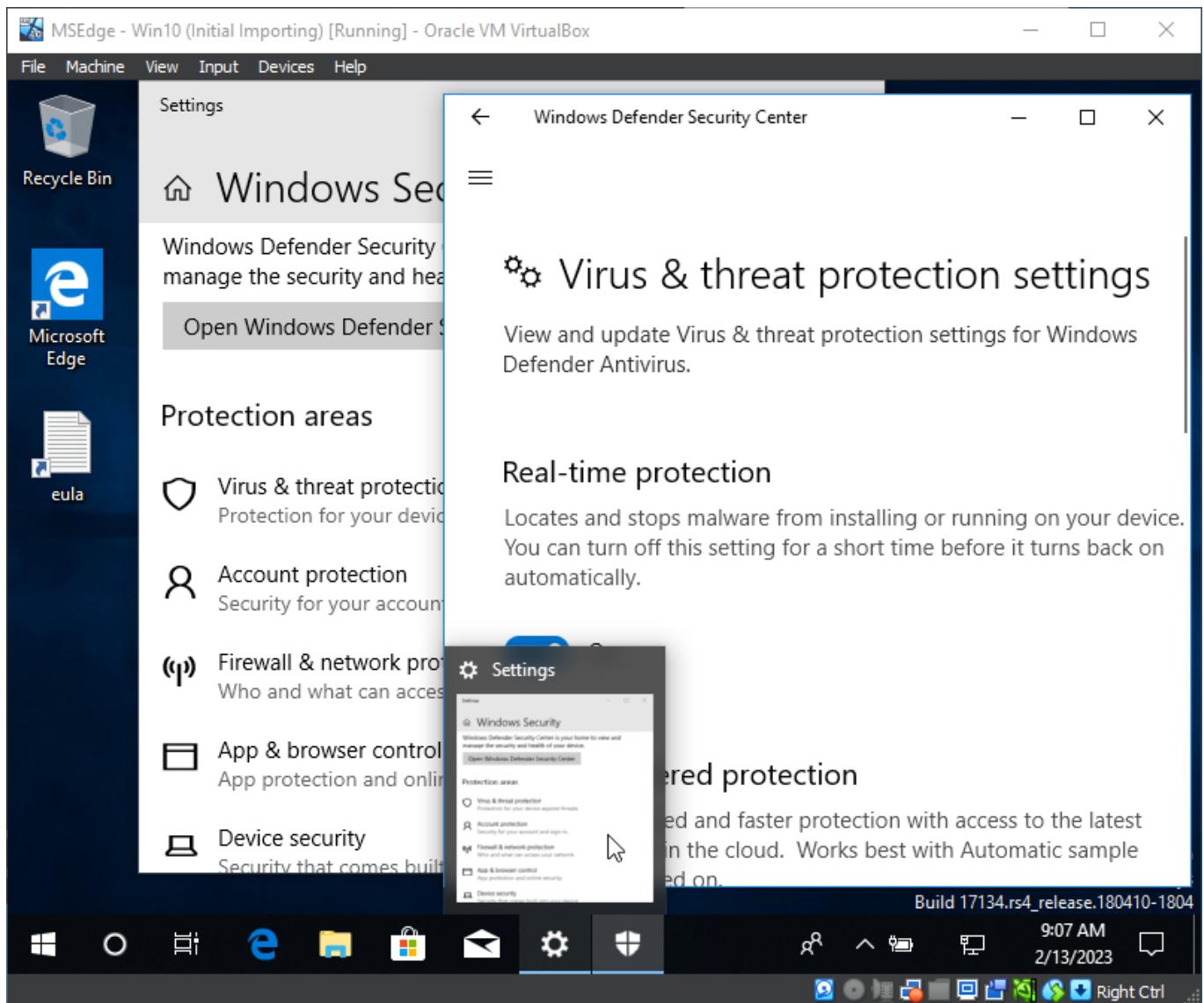
- Pause Windows Updates:





- Disable Defender Settings:





MSEdge - Win10 (Initial Importing) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Recycle Bin

Microsoft Edge

eula

Settings

Windows Security

Windows Defender Security Center

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

✖ Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

⚠ Cloud-delivered protection is off. Your device may be [Dismiss](#) vulnerable.

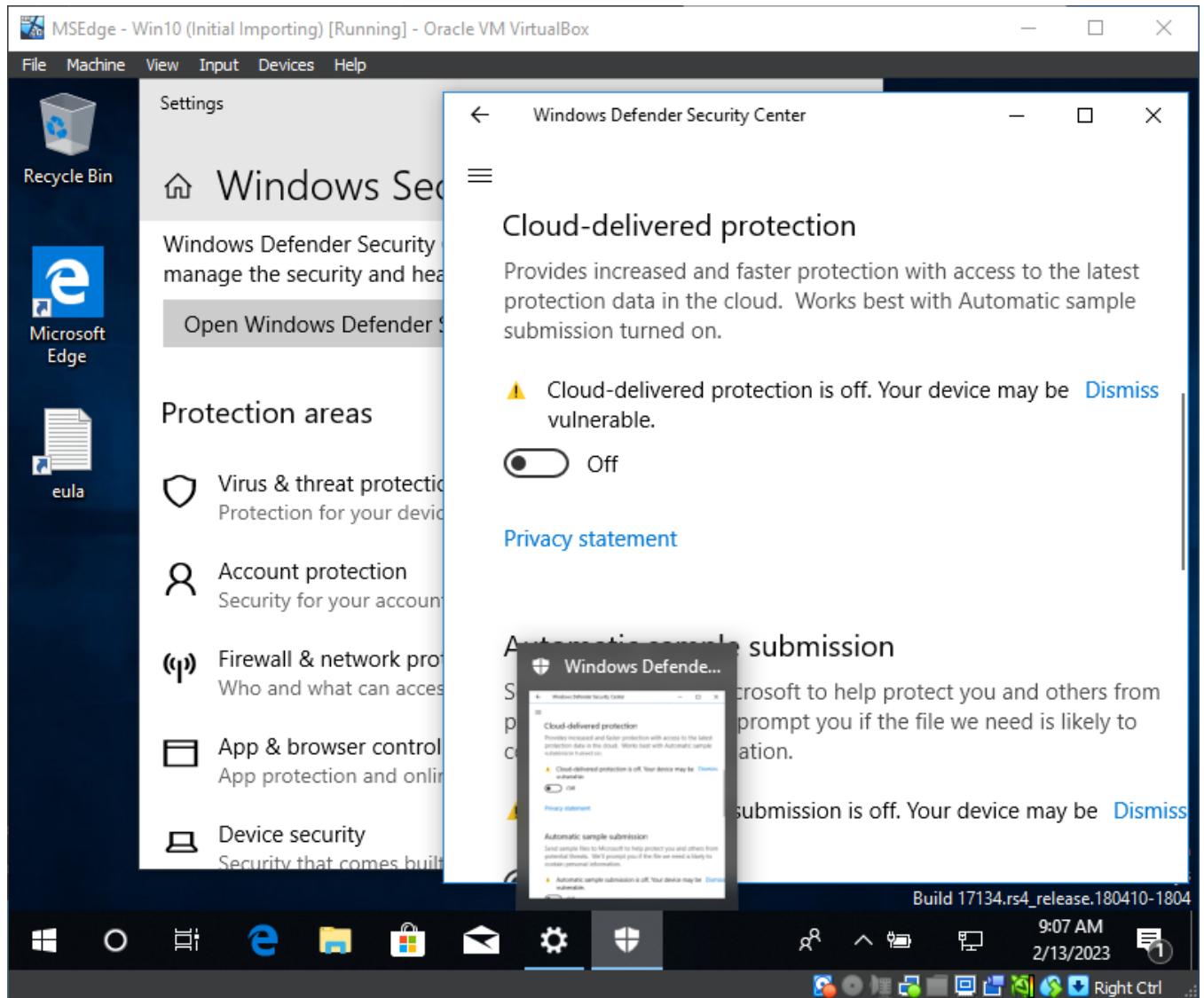
Off

Build 17134.rs4_release.180410-1804

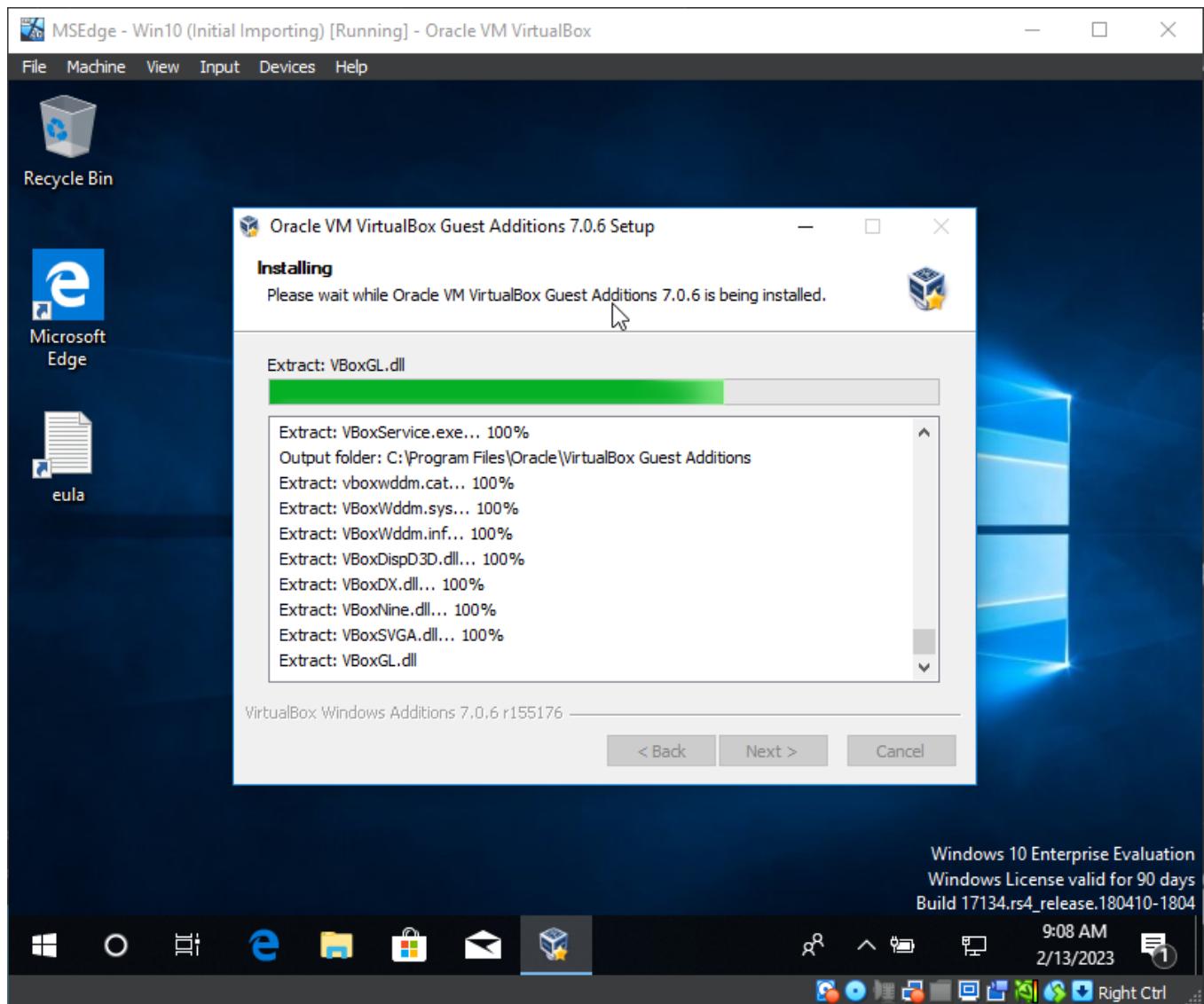
9:07 AM 2/13/2023

Right Ctrl

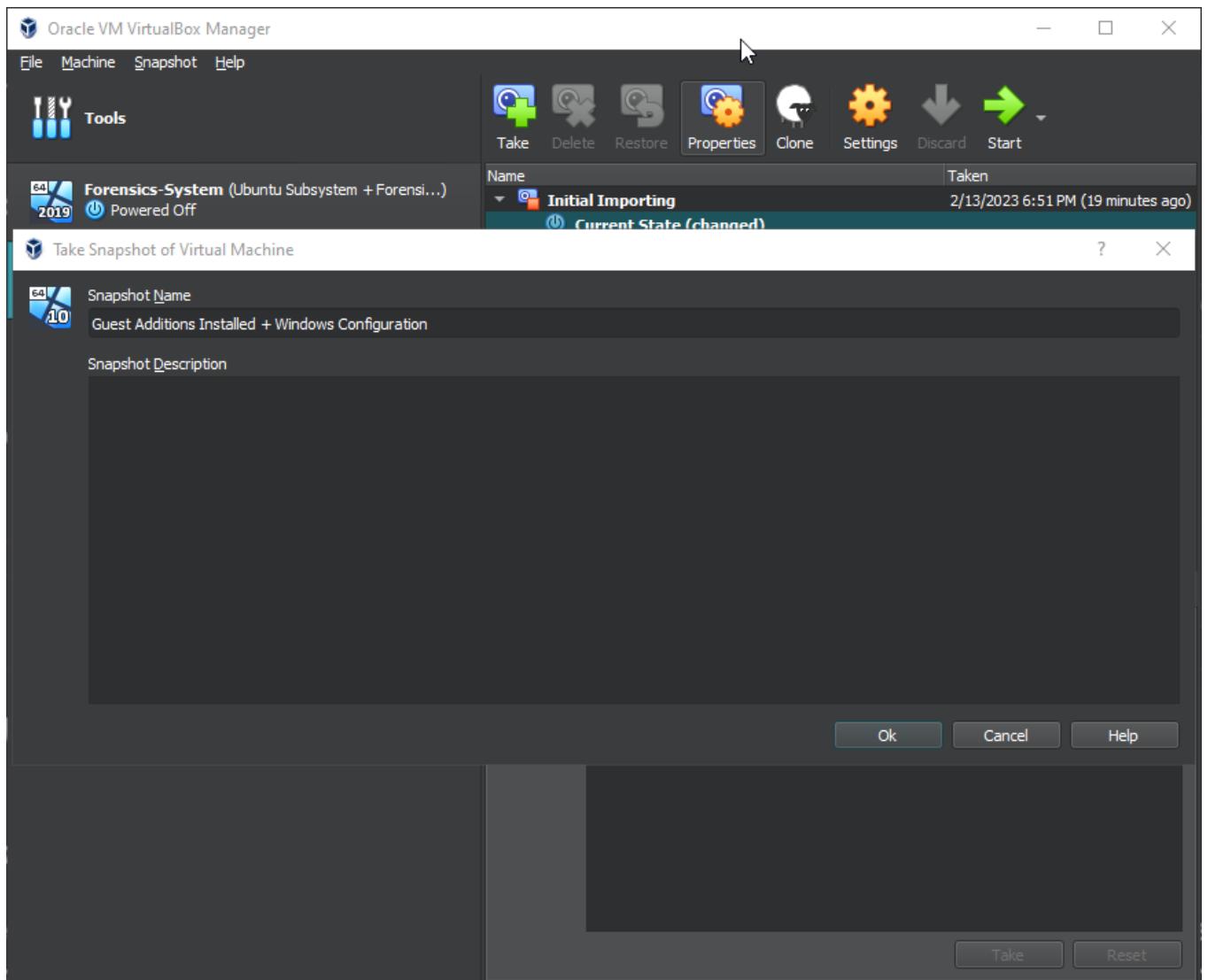
This screenshot shows the Windows Defender Security Center window open in a Microsoft Edge browser. The left sidebar lists icons for Recycle Bin, Microsoft Edge, and eula. The main content area shows the 'Real-time protection' section with a warning message and a toggle switch set to 'Off'. Below it is the 'Cloud-delivered protection' section with a similar warning and a toggle switch also set to 'Off'. The status bar at the bottom indicates the build number as 'Build 17134.rs4_release.180410-1804' and the date and time as '9:07 AM 2/13/2023'. The taskbar at the bottom includes icons for Start, Task View, File Explorer, Microsoft Edge, Settings, and other system icons.



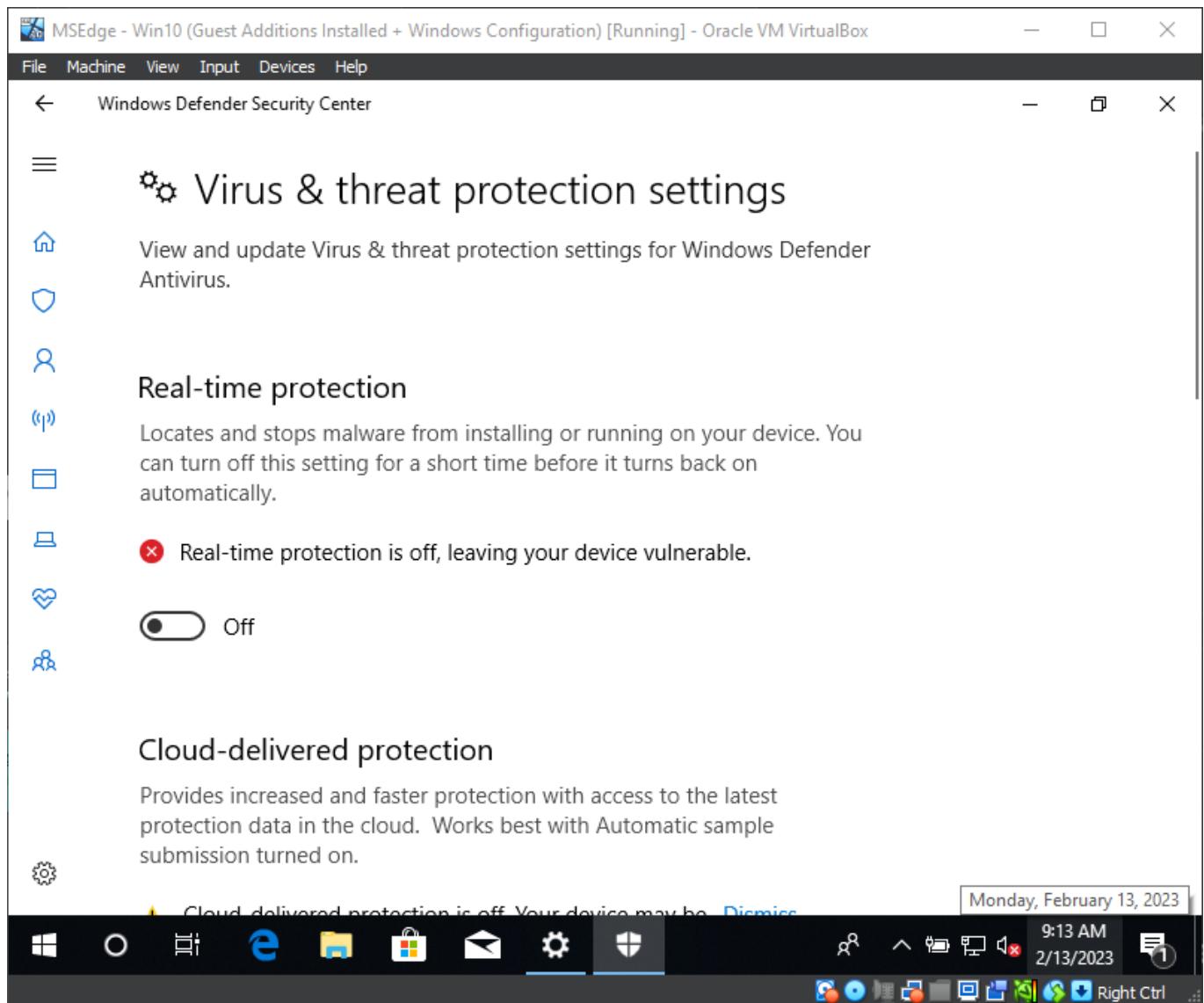
- Optional, install VBOX Guest Additions:



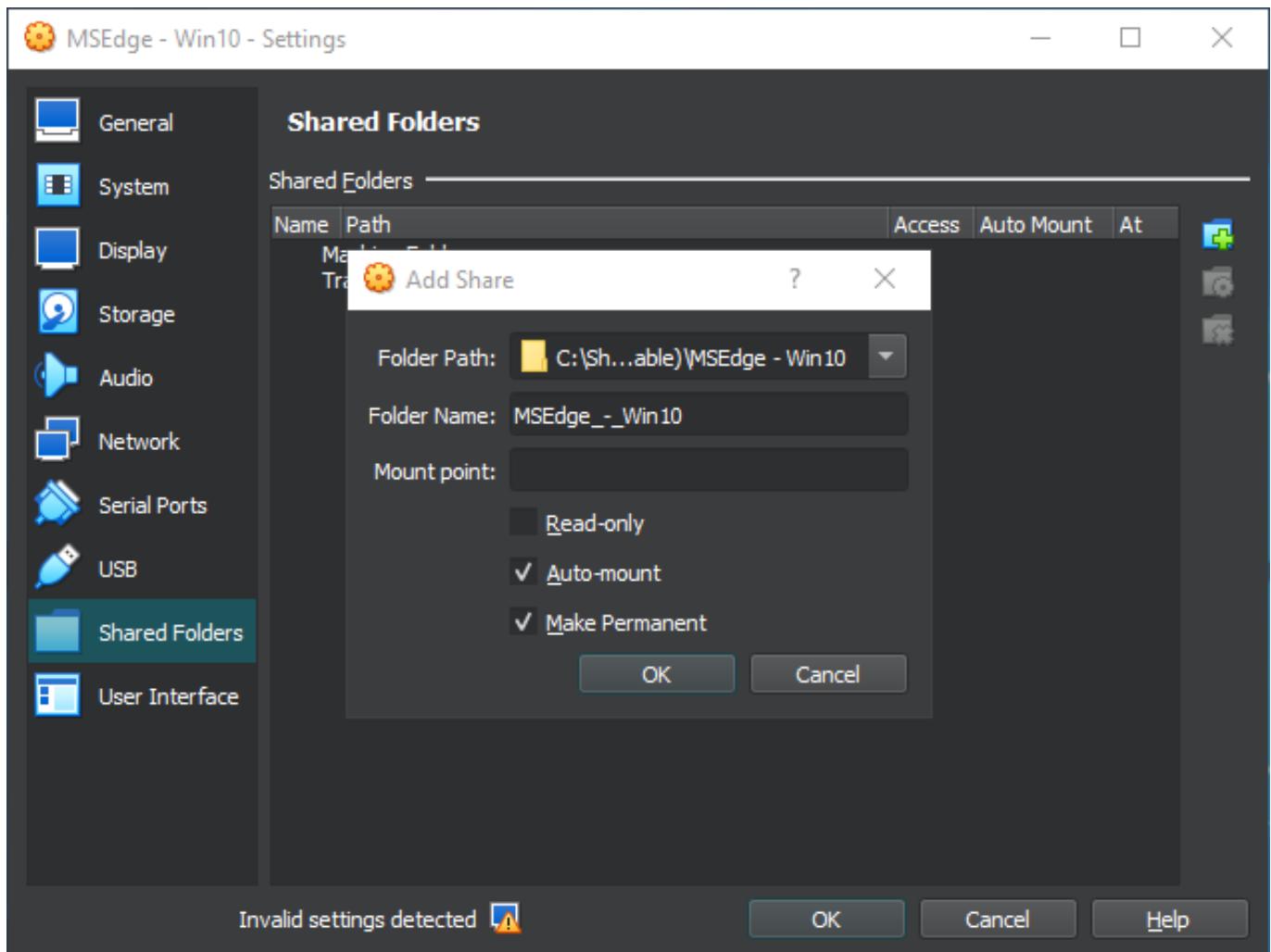
- Reboot, shutdown and take a snapshot:



- Remember, at every shutdown or restart, windows virus real-time protection is set to on automatically, you will need to disable it in order for the script to work:



- Share folder with the virtual machine:



- Go to this github link for the attack script and download the repository as a ZIP file:

<https://github.com/bluecapesecurity/PWF>

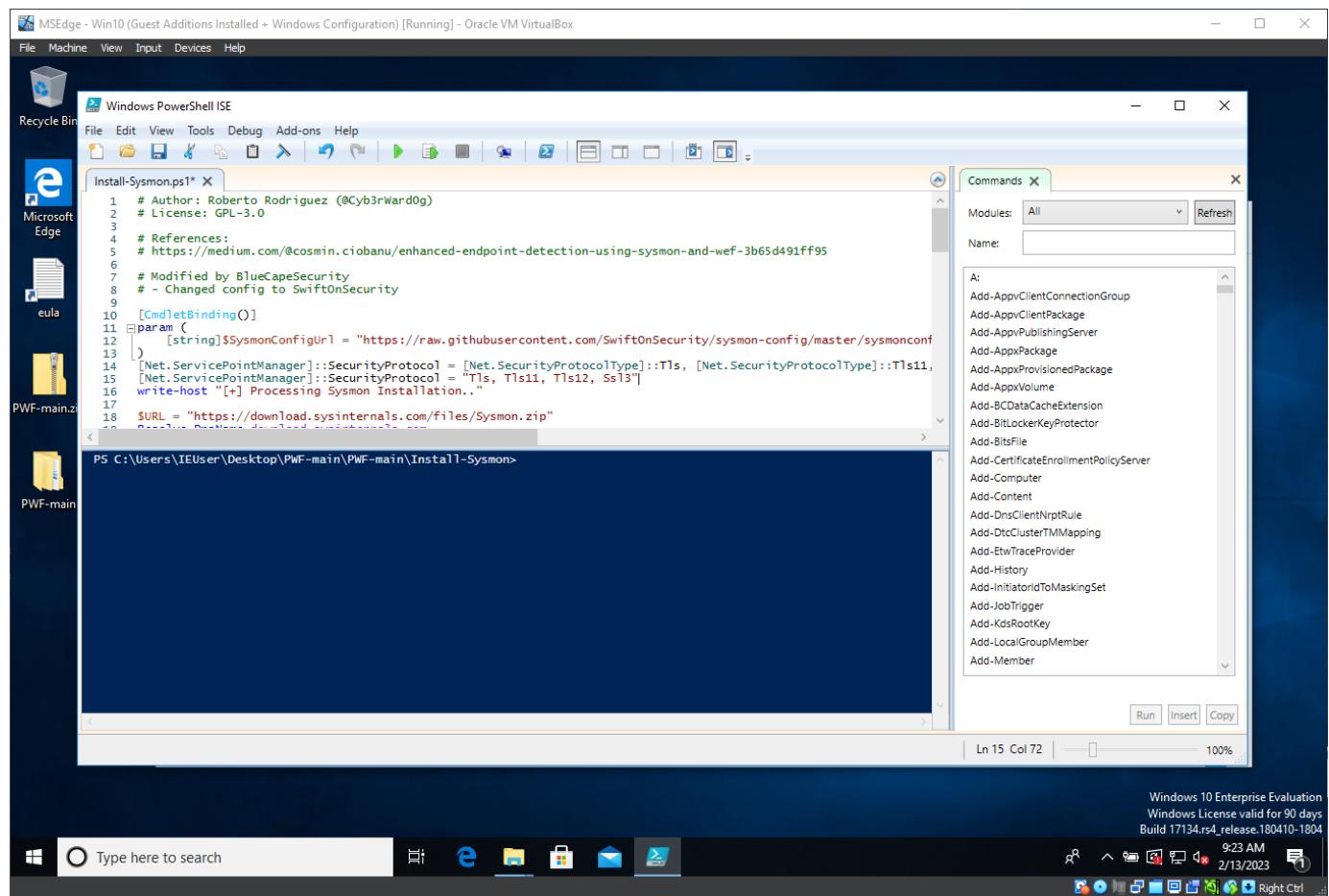
The screenshot shows a GitHub repository page for 'bluecapesecurity / PWF'. The 'Code' tab is active. In the 'Clone' section, there are two tabs: 'Local' and 'Codespaces'. The 'Local' tab is selected. It displays a URL: <https://github.com/blueapesecurity/PWF.git>. Below the URL, there are options to 'Open with GitHub Desktop' or 'Download ZIP'. A red arrow points to the 'Download ZIP' button. To the right of the clone section, there is an 'About' section with the repository's name, a website link (www.blueapesecurity.com), and several tags: forensics, cybersecurity, blueteam, and purpleteam. Below the 'About' section are sections for 'Readme', 'AGPL-3.0 license', '202 stars', '9 watching', and '38 forks'. Further down are sections for 'Releases' (with one entry: T1055.001 and license updates, latest on Jul 12, 2022), 'Packages' (no packages published), and 'Languages'.

- Copy .zip file from the network drive in the virtual machine to the Desktop:

The screenshot shows a Windows 10 desktop environment. A File Explorer window is open, showing a folder structure. The path in the address bar is 'This PC > MSEdge_-_Win10 (\\\VBoxSrv) (Z:)'. Inside this folder, there is a single item named 'PWF-main.zip'. The desktop background is dark blue. On the left, there are icons for 'Recycle Bin', 'Microsoft Edge', 'eula', and 'PWF-main.zip'. The taskbar at the bottom includes icons for Start, Search, Task View, Edge, File Explorer, File Explorer (selected), File Explorer, Mail, and Task View again. The system tray shows the date and time as '2/13/2023 9:19 AM'. The status bar at the bottom right indicates 'Windows 10 Enterprise Evaluation' and 'Windows License valid for 90 days Build 17134.rs4_release.180410-1804'.

- Enter the folder PWF-main and edit all .ps1 files by adding the following code:
-

```
[Net.ServicePointManager]::SecurityProtocol =  
[Net.SecurityProtocolType]::Tls, [Net.SecurityProtocolType]::Tls11,  
[Net.SecurityProtocolType]::Tls12, [Net.SecurityProtocolType]::Ssl3  
  
[Net.ServicePointManager]::SecurityProtocol = "Tls, Tls11, Tls12,  
Ssl3"
```



MSEdge - Win10 (Guest Additions Installed + Windows Configuration) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Recycle Bin

e Microsoft Edge

eula

PWF-main.zip

PWF-main

Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

Install-Sysmon.ps1 ART-attack.ps1 ART-attack-cleanup.ps1

```
1 #TODO - check if ART framework is already installed
2 [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls, [Net.SecurityProtocolType]::Tls11,
3 [Net.ServicePointManager]::SecurityProtocol = "Tls, Tls11, Tls12, Ssl3"
4 #Install Execution Framework and Atomics Folder
5
6 Write-Output "Installing AtomicRedTeam"
7 Write-Output "===="
8 Invoke-WebRequest -Uri 'https://raw.githubusercontent.com/bluecapesecurity/Invoke-AtomicRedTeam/master/install-atomicredteam.ps1' -OutFile Install-AtomicRedTeam -Repository bluecapesecurity
9
10 Write-Output "Installing AtomicsFolder...this might take a few minutes."
11 Invoke-WebRequest -Uri 'https://raw.githubusercontent.com/bluecapesecurity/Invoke-AtomicRedTeam/master/install-atomicsfolder.ps1' -OutFile Install-AtomicsFolder -Force -Branch 724cb3f50dcd34181515d2f34cbf90168017404
12
13 # Starting atomics attack simulation
14
15 Write-Output "Starting ART attack simulation"
16 Write-Output "===="
```

Commands x

Modules: All Refresh

Name:

A:

- Add-AppClientConnectionGroup
- Add-AppClientPackage
- Add-AppPublishingServer
- Add-AppPackage
- Add-AppxProvisionedPackage
- Add-AppVolume
- Add-BCDataCacheExtension
- Add-BitLockerKeyProtector
- Add-BitsFile
- Add-CertificateEnrollmentPolicyServer
- Add-Computer
- Add-Content
- Add-DnsClientNrrRule
- Add-DtcClusterTMMapping
- Add-EtwTraceProvider
- Add-History
- Add-InitiatorIdToMaskingSet
- Add-JobTrigger
- Add-KdsRootKey
- Add-LocalGroupMember
- Add-Member

Run Insert Copy

PS C:\Users\IEUser\Desktop\PWF-main\PWF-main\Install-Sysmon>

Ln 3 Col 72 | 9:23 AM 2/13/2023 100%

Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 17134.rs4_release.180410-1804

Type here to search

Start button

File Explorer

Edge

Task View

PowerShell

Mail

File History

System

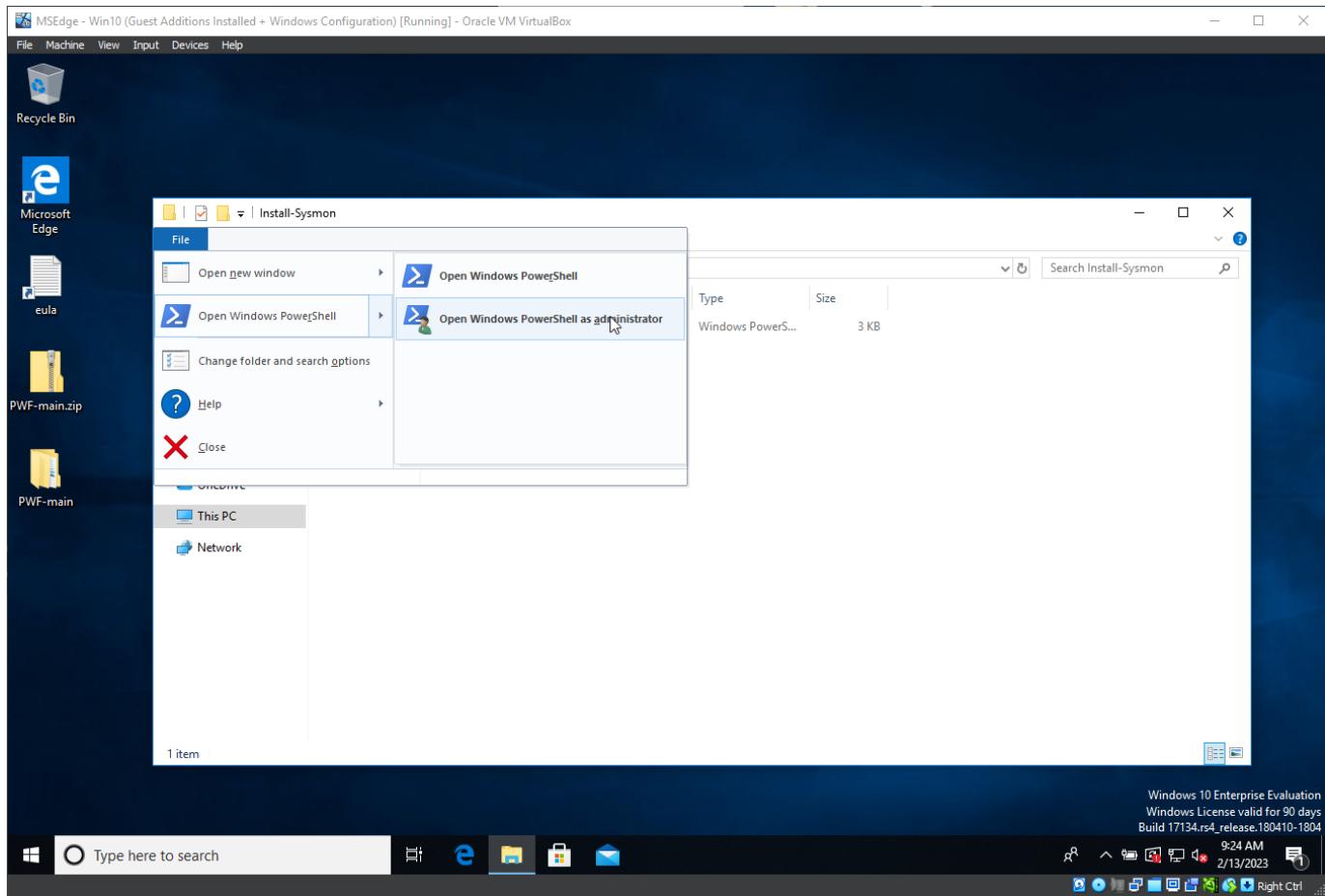
People

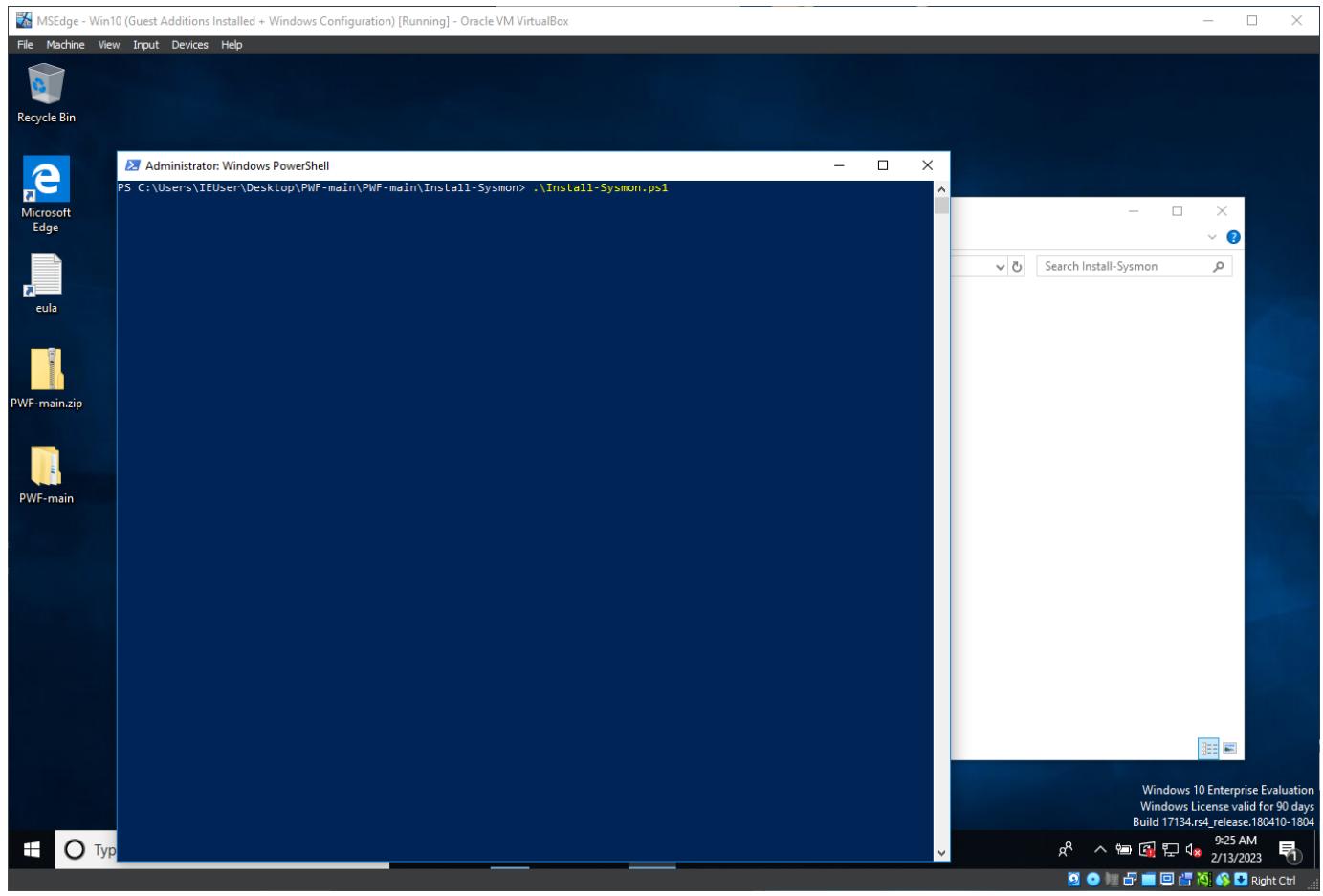
9:23 AM 2/13/2023

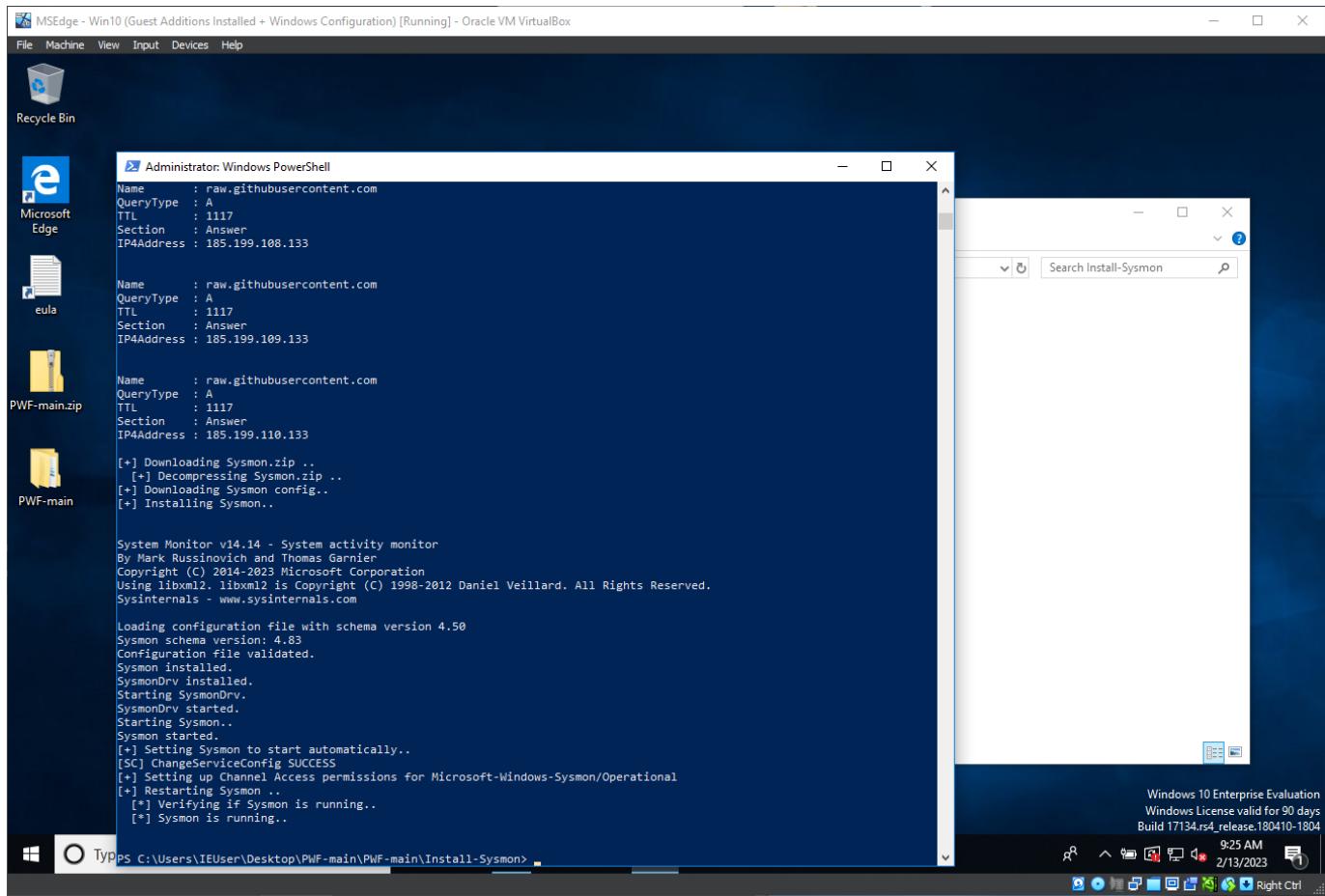
Right Ctrl

The screenshot shows a Windows 10 desktop environment. In the foreground, a Windows PowerShell ISE window is open, displaying a script named `ART-attack.ps1`. The script contains several lines of PowerShell code, including module imports and various commands related to network security and attack simulation. To the right of the script editor is a 'Commands' palette, which lists numerous PowerShell cmdlets starting with 'Add-'. The desktop background is dark blue, and the taskbar at the bottom shows standard icons like File Explorer, Edge, and Mail. A status bar at the bottom right indicates the system is a 'Windows 10 Enterprise Evaluation' build valid for 90 days.

- Install Sysmon:

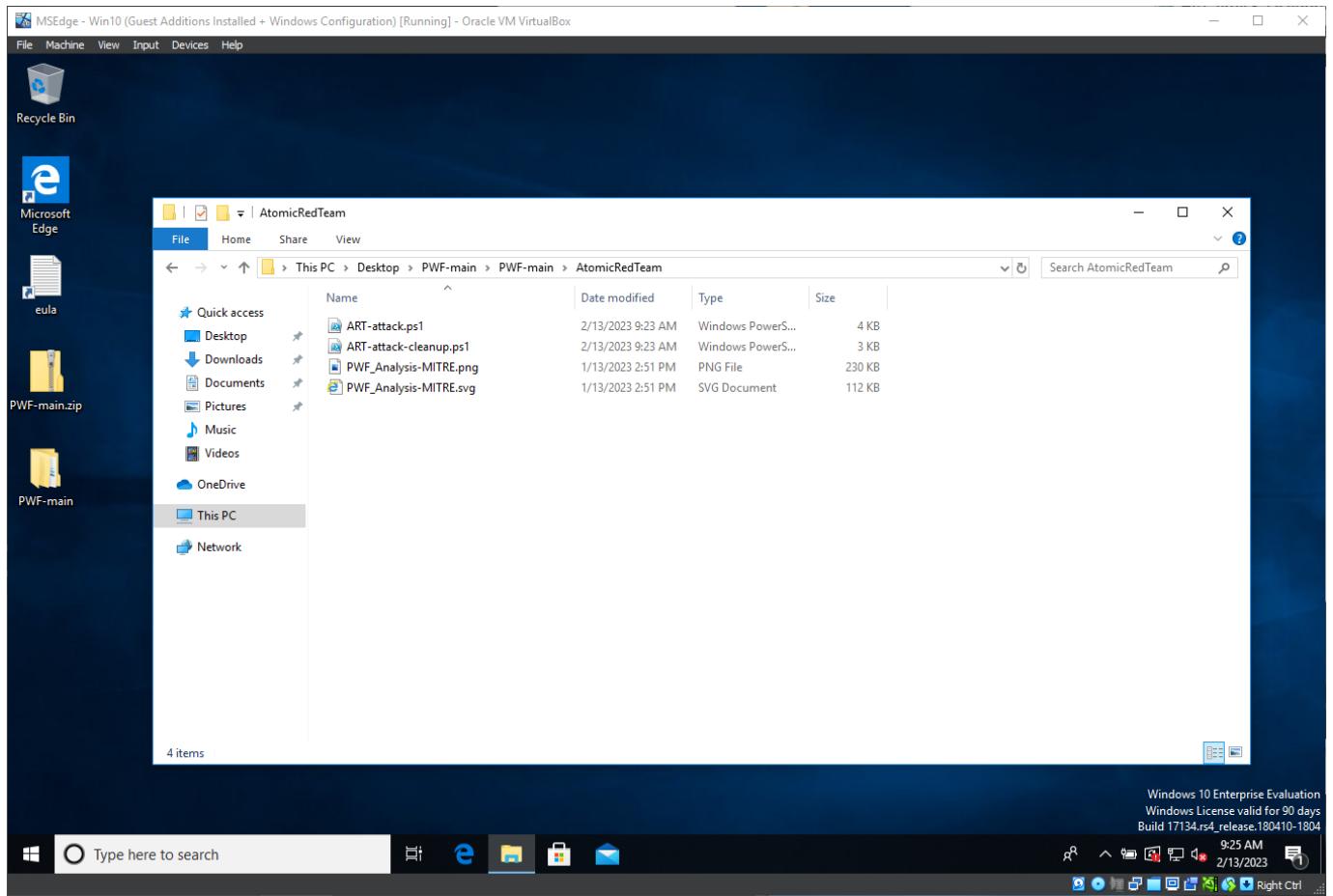


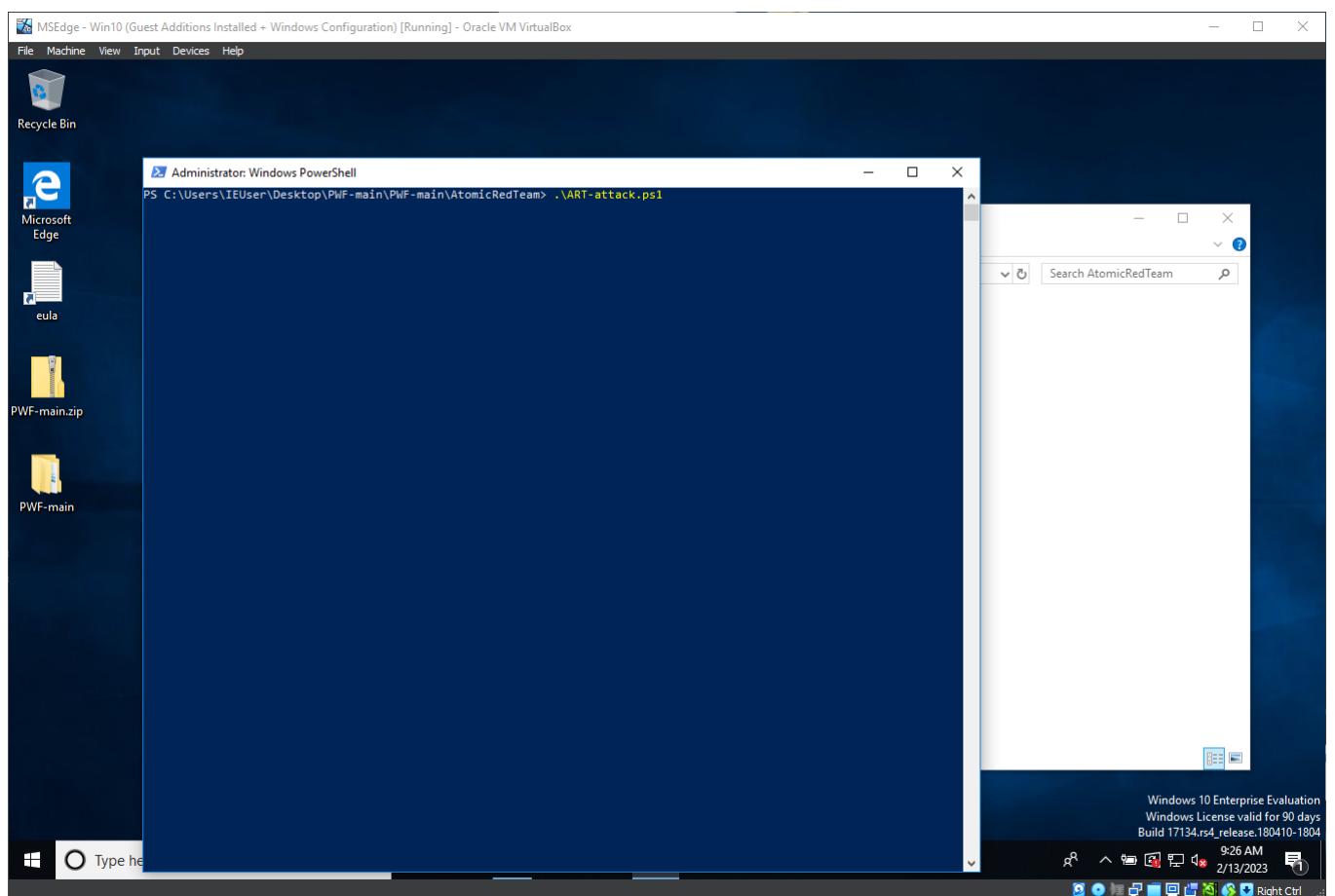
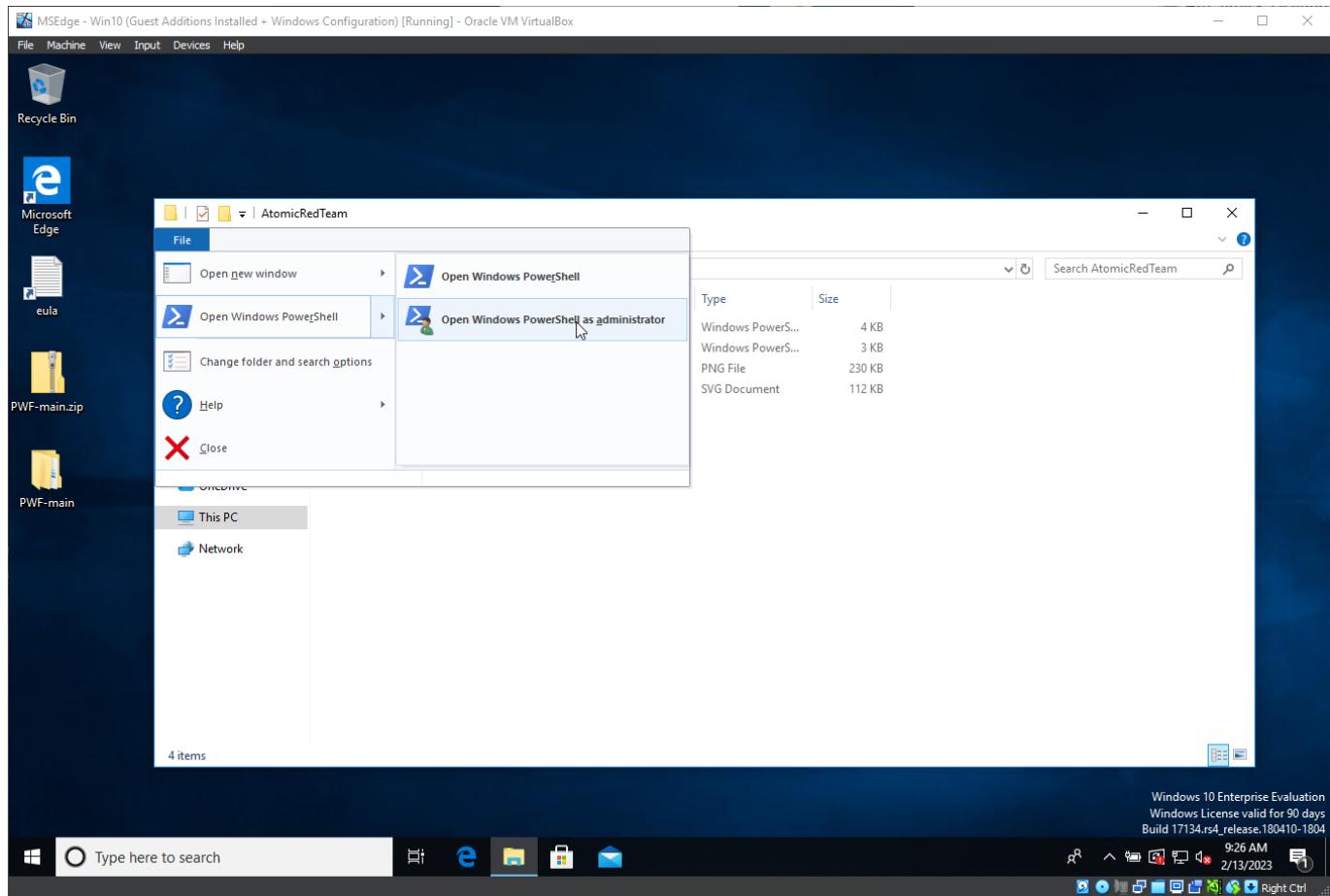


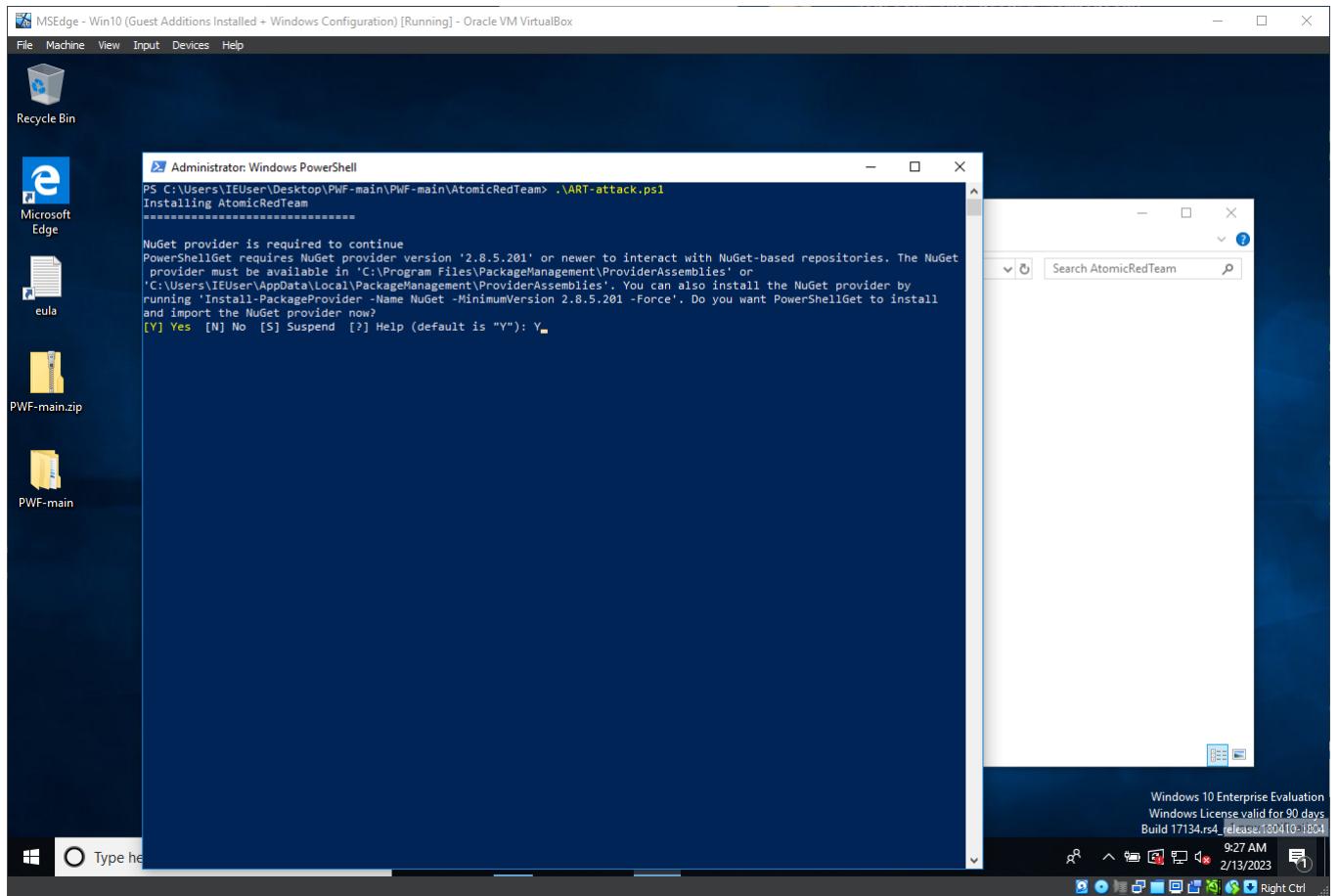


Execution of attack script

- Execute attack script that is based on AtomicRedTeam techniques. The script will download the AtomicRedTeam framework and then will execute some atomic techniques, or atomics to simulate a realistic attack that malicious software or threat actors often execute on windows systems. After the execution I will investigate the attack:







- There are multiple atomic tests being executed:
 - o T1566.001: Phishing: Spearphishing Attachment
 - Tactic: [Initial Access](#)
 - o T1078.003: Valid Accounts: Local Accounts
 - Tactic: [Defense Evasion](#), [Persistence](#), [Privilege Escalation](#), [Initial Access](#)
 - o T1059.001: Command and Scripting Interpreter: PowerShell
 - Tactic: [Execution](#)
 - o T1547.001: Boot or Logon Autostart Execution: Registry Run Keys
 - Tactic: [Persistence](#), [Privilege Escalation](#)
 - o T1547.001: Boot or Logon Autostart Execution: Startup Folder
 - Tactic: [Persistence](#), [Privilege Escalation](#)
 - o T1053.005: Scheduled Task/Job: Scheduled Task

- Tactic: [Execution, Persistence, Privilege Escalation](#)
- T1543.003: Create or Modify System Process: Windows Service
 - Tactic: [Persistence, Privilege Escalation](#)
- T1055.001: Process Injection: Dynamic-link Library Injection
 - Tactic: [Defense Evasion, Privilege Escalation](#)
- T1070.004: Indicator Removal: File Deletion
 - Tactic: [Defense Evasion](#)

- Based on the script that BlueCapeSecurity used:

```

1 #TODO - check if ART framework is already installed
2
3 #Install Execution Framework and Atomics Folder
4
5 Write-Output "Installing AtomicRedTeam"
6 Write-Output "=====
7 IEX (IWR 'https://raw.githubusercontent.com/bluecapesecurity/Invoke-AtomicRedTeam/master/install-atomicredteam.ps1' -UseBasicParsing);
8 Install-AtomicRedTeam -RepoOwner bluecapesecurity
9
10 Write-Output "Installing AtomicsFolder...this might take a few minutes."
11 IEX (IWR 'https://raw.githubusercontent.com/bluecapesecurity/Invoke-AtomicRedTeam/master/install-atomicsfolder.ps1' -UseBasicParsing);
12 Install-AtomicsFolder -Force -Branch 724cb3f50dcdd341815d5d2f34cbf90168017404
13
14 # Starting atomics attack simulation
15
16 Write-Output "Starting ART attack simulation"
17 Write-Output "=====
18
19
20 # initial-access
21 #
22
23 "T1566.001 Atomic Test #1 - Download Macro-Enabled Phishing Attachment"
24 # https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1566.001/T1566.001.md#atomic-test-1---download-macro-enabled-phishing-attachment
25 Invoke-AtomicTest T1566.001 -TestNumbers 1
26
27 Start-Sleep -s 2
28
29 "T1078.003 Atomic Test #1 - Create local account with admin privileges"
30 # https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1078.003/T1078.003.md#atomic-test-3---create-local-account-with-admin-privileges
31 Invoke-AtomicTest T1078.003 -TestNumbers 1
32
33 Start-Sleep -s 2
34
35 # execution
36 #

```

- You can go to: <https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/>, and use another techniques, just for learning purposes, for example for initial-access, execution, persistence, defense-evasion, etc.

- The script used just some techniques. Based on <https://attack.mitre.org/techniques/enterprise/>, techniques represent 'how' an adversary achieves a tactical goal by performing an action. You can see the MITRE ATT&CK Matrix here: <https://attack.mitre.org/matrices/enterprise/>. According to <https://www.blackberry.com/us/en/solutions/endpoint-security/mitre-attack/mitre-attack-vs-cyber-kill-chain>, there is a difference between Cyber Kill Chain framework and Mitre Attack framework:

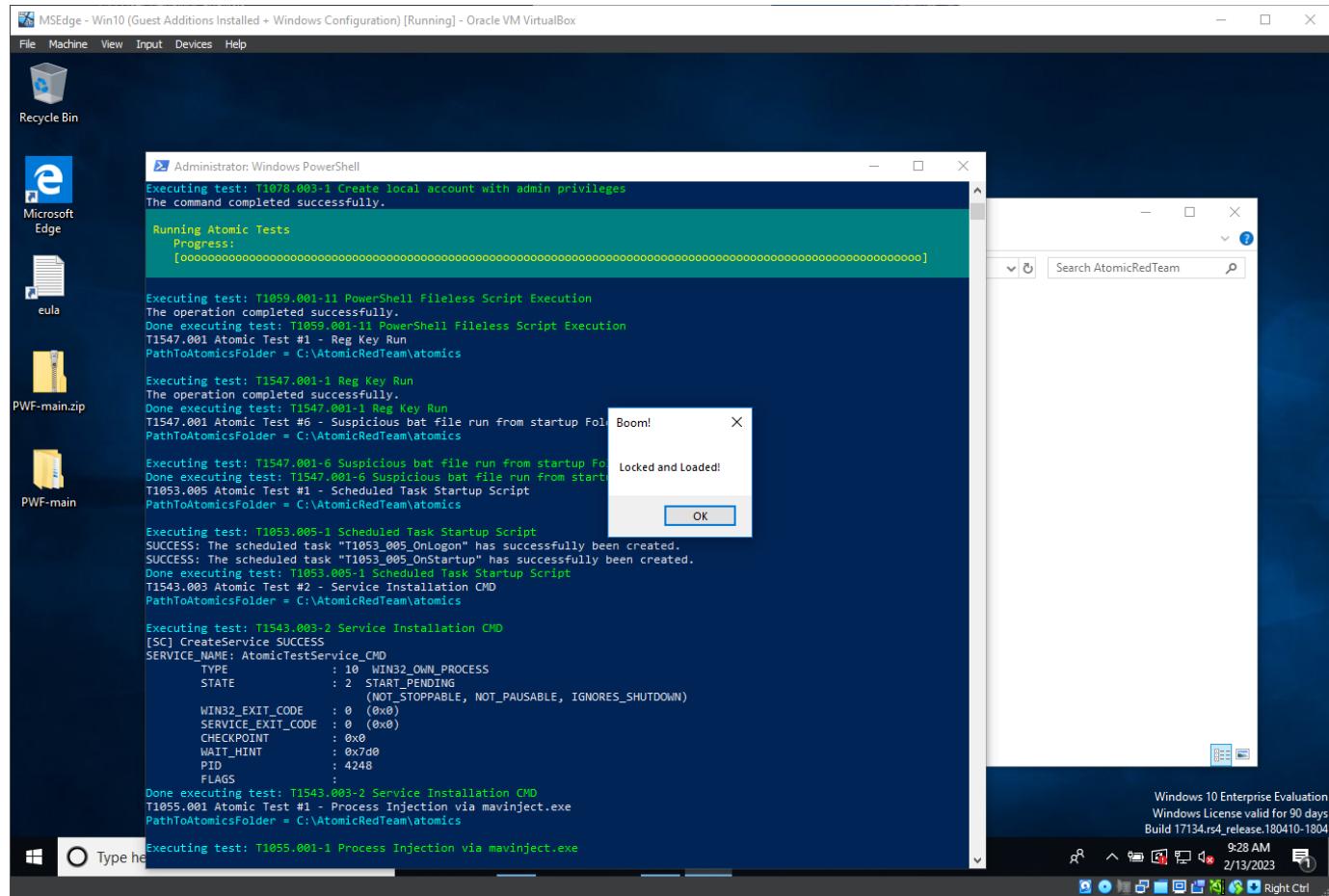
CYBER KILL CHAIN VS. MITRE ATT&CK

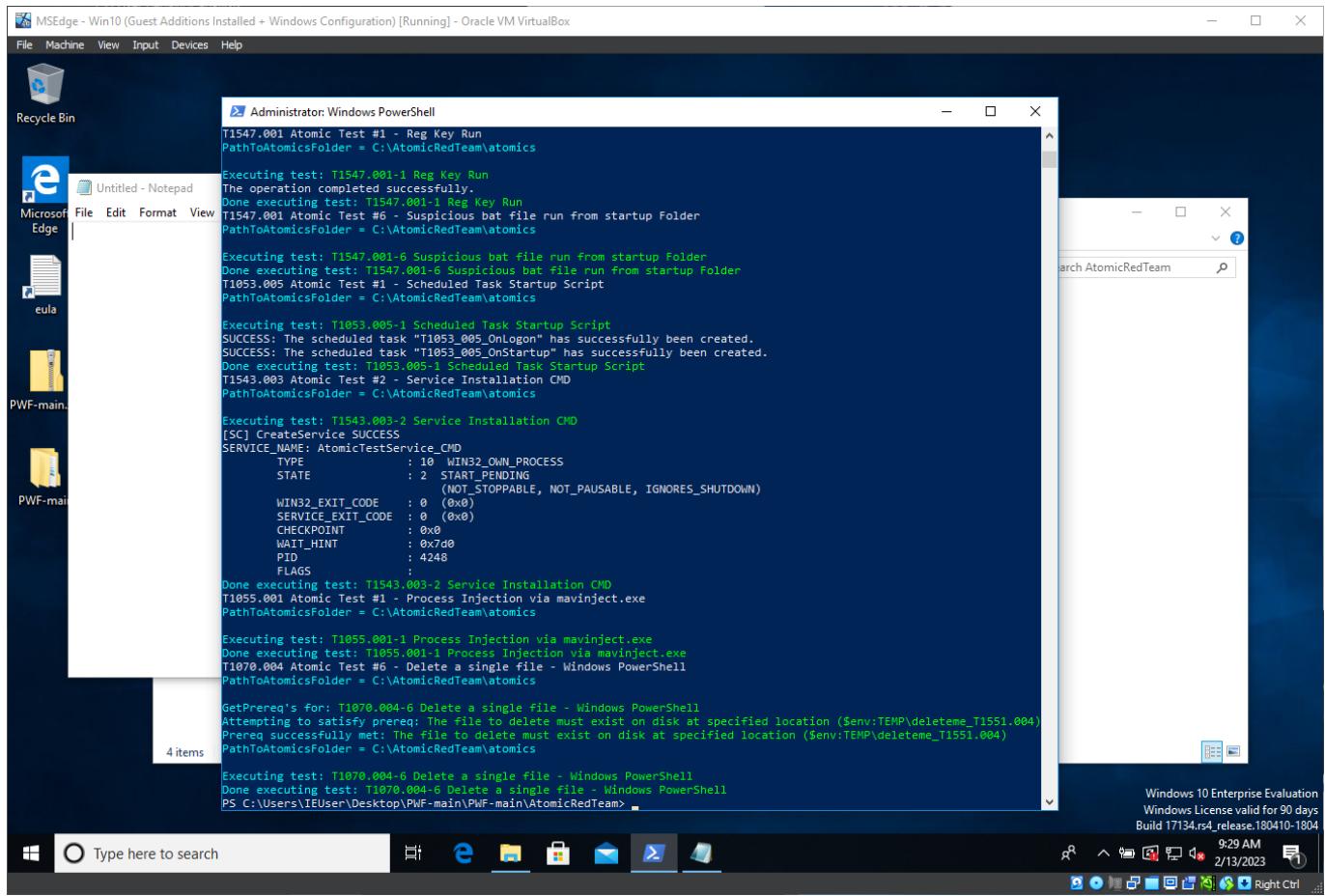


- Both MITRE ATT&CK and Cyber Kill Chain are frameworks to address cyberattacks against an organization. But, Cyber Kill Chain addresses the cyberattack process for a high level point

of view, while MITRE ATT&CK contains a deeper scope of knowledge that includes granular details about cyberattacks, such as attack techniques and procedures.

- Important, do not close notepad, just press ok on the prompt:





- Timeline of the cyber attack:
 - o 9:26-27AM 2/13/2023
 - o 9:29-30AM 2/13/2023

- Pause the virtual machine for further data acquisition:

MSEdge - Win10 (Guest Additions Installed + Windows Configuration) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Recycle Bin

Microsoft Edge

eula

PWF-main.

PWF-main.

4 items

Host+S Host+T Host+N Host+P Host+R Host+H

Administrator: Windows PowerShell

```
mic Test #1 - Reg Key Run
Folder = C:\AtomicRedTeam\atomics
t: T1547.001-1 Reg Key Run
completed successfully.
g t: T1547.001-1 Reg Key Run
g completed successfully.
Host+H mic Test #6 - Suspicious bat file run from startup Folder
PathToAtomicsFolder C:\AtomicRedTeam\atomics

Executing test: T1547.001-6 Suspicious bat file run from startup Folder
Done executing test: T1547.001-6 Suspicious bat file run from startup Folder
T1053.005 Atomic Test #1 - Scheduled Task Startup Script
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1053.005-1 Scheduled Task Startup Script
SUCCESS: The scheduled task "T1053.005_OnLogon" has successfully been created.
SUCCESS: The scheduled task "T1053.005_OnStartup" has successfully been created.
Done executing test: T1053.005-1 Scheduled Task Startup Script
T1053.003 Atomic Test #2 - Service Installation CMD
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1053.003-2 Service Installation CMD
[SC] CreateService SUCCESS
SERVICE_NAME: AtomicTestService_CMD
    TYPE          : 10 WIN32_OWN_PROCESS
    STATE         : 2 START_PENDING
                   (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE : 0 (0x0)
    SERVICE_EXIT_CODE : 0 (0x0)
    CHECKPOINT   : 0x0
    WAIT_HINT    : 0x7d0
    PID          : 4248
    FLAGS        :
Done executing test: T1053.003-2 Service Installation CMD
T1055.001 Atomic Test #1 - Process Injection via mavinject.exe
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1055.001-1 Process Injection via mavinject.exe
Done executing test: T1055.001-1 Process Injection via mavinject.exe
T1070.004 Atomic Test #6 - Delete a single file - Windows PowerShell
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1070.004-6 Delete a single file - Windows PowerShell
Attempting to satisfy prereq: The file to delete must exist on disk at specified location ($env:TEMP\deleteme_T1551.004)
Prereq successfully met: The file to delete must exist on disk at specified location ($env:TEMP\deleteme_T1551.004)
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1070.004-6 Delete a single file - Windows PowerShell
Done executing test: T1070.004-6 Delete a single file - Windows PowerShell
PS C:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam>
```

Type here to search

Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 17134.rs4_release.180410-1804

9:30 AM 2/13/2023 Right Ctrl

MSEdge - Win10 (Guest Additions Installed + Windows Configuration) [Paused] - Oracle VM VirtualBox

File Machine View Input Devices Help

Recycle Bin

Microsoft Edge

eula

PWF-main.

PWF-main.

4 items

Select Administrator: Windows PowerShell

```
T1547.001 Atomic Test #1 - Reg Key Run
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1547.001-1 Reg Key Run
The operation completed successfully.
Done executing test: T1547.001-1 Reg Key Run
T1547.001 Atomic Test #6 - Suspicious bat file run from startup Folder
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1547.001-6 Suspicious bat file run from startup Folder
Done executing test: T1547.001-6 Suspicious bat file run from startup Folder
T1053.005 Atomic Test #1 - Scheduled Task Startup Script
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1053.005-1 Scheduled Task Startup Script
SUCCESS: The scheduled task "T1053.005_OnLogon" has successfully been created.
SUCCESS: The scheduled task "T1053.005_OnStartup" has successfully been created.
Done executing test: T1053.005-1 Scheduled Task Startup Script
T1053.003 Atomic Test #2 - Service Installation CMD
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1053.003-2 Service Installation CMD
[SC] CreateService SUCCESS
SERVICE_NAME: AtomicTestService_CMD
    TYPE          : 10 WIN32_OWN_PROCESS
    STATE         : 2 START_PENDING
                   (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE : 0 (0x0)
    SERVICE_EXIT_CODE : 0 (0x0)
    CHECKPOINT   : 0x0
    WAIT_HINT    : 0x7d0
    PID          : 4248
    FLAGS        :
Done executing test: T1053.003-2 Service Installation CMD
T1055.001 Atomic Test #1 - Process Injection via mavinject.exe
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1055.001-1 Process Injection via mavinject.exe
Done executing test: T1055.001-1 Process Injection via mavinject.exe
T1070.004 Atomic Test #6 - Delete a single file - Windows PowerShell
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1070.004-6 Delete a single file - Windows PowerShell
Attempting to satisfy prereq: The file to delete must exist on disk at specified location ($env:TEMP\deleteme_T1551.004)
Prereq successfully met: The file to delete must exist on disk at specified location ($env:TEMP\deleteme_T1551.004)
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1070.004-6 Delete a single file - Windows PowerShell
Done executing test: T1070.004-6 Delete a single file - Windows PowerShell
PS C:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam>
```

Type here to search

Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 17134.rs4_release.180410-1804

9:30 AM 2/13/2023 Right Ctrl

