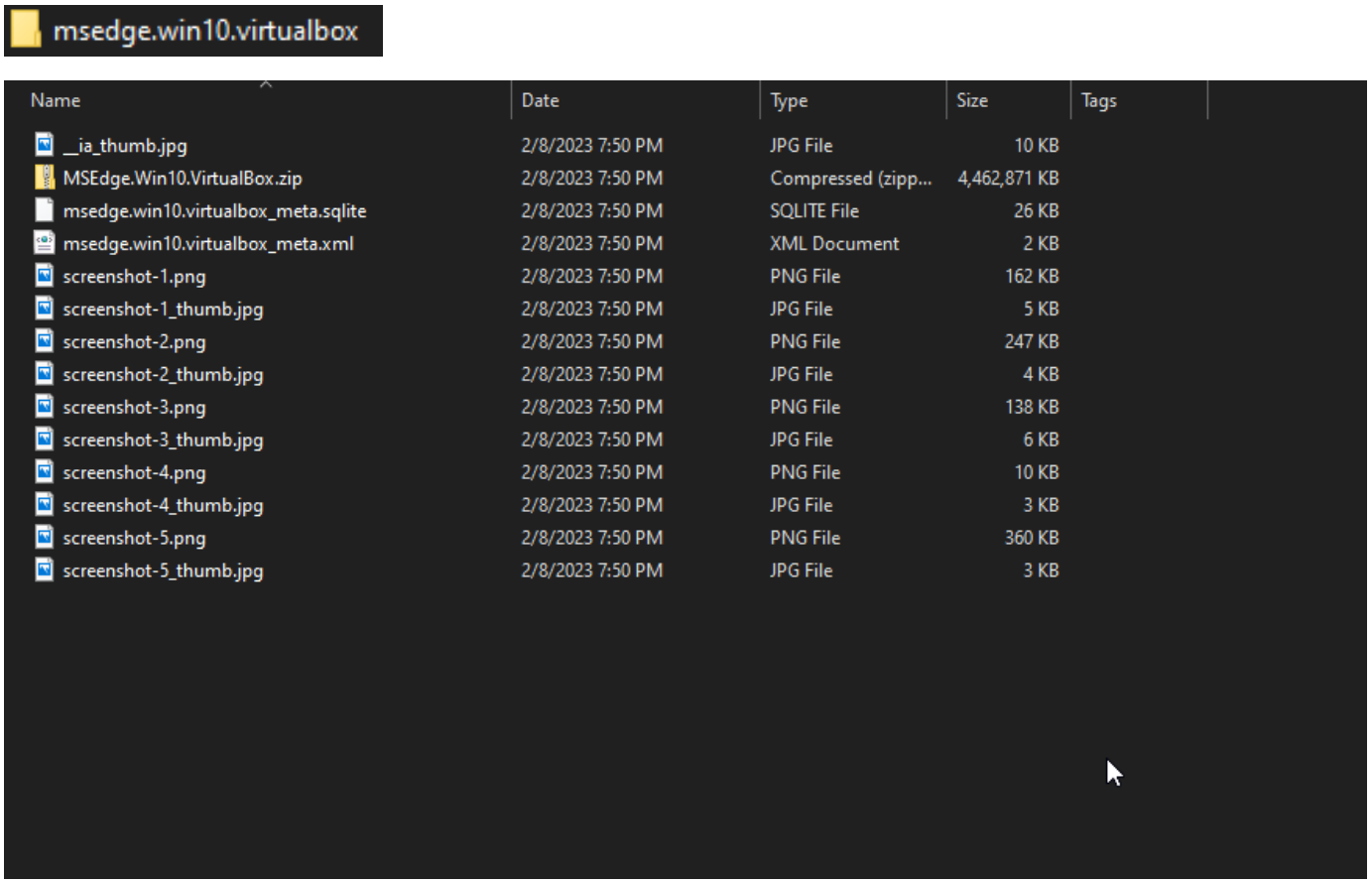
Setup Instructions:

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

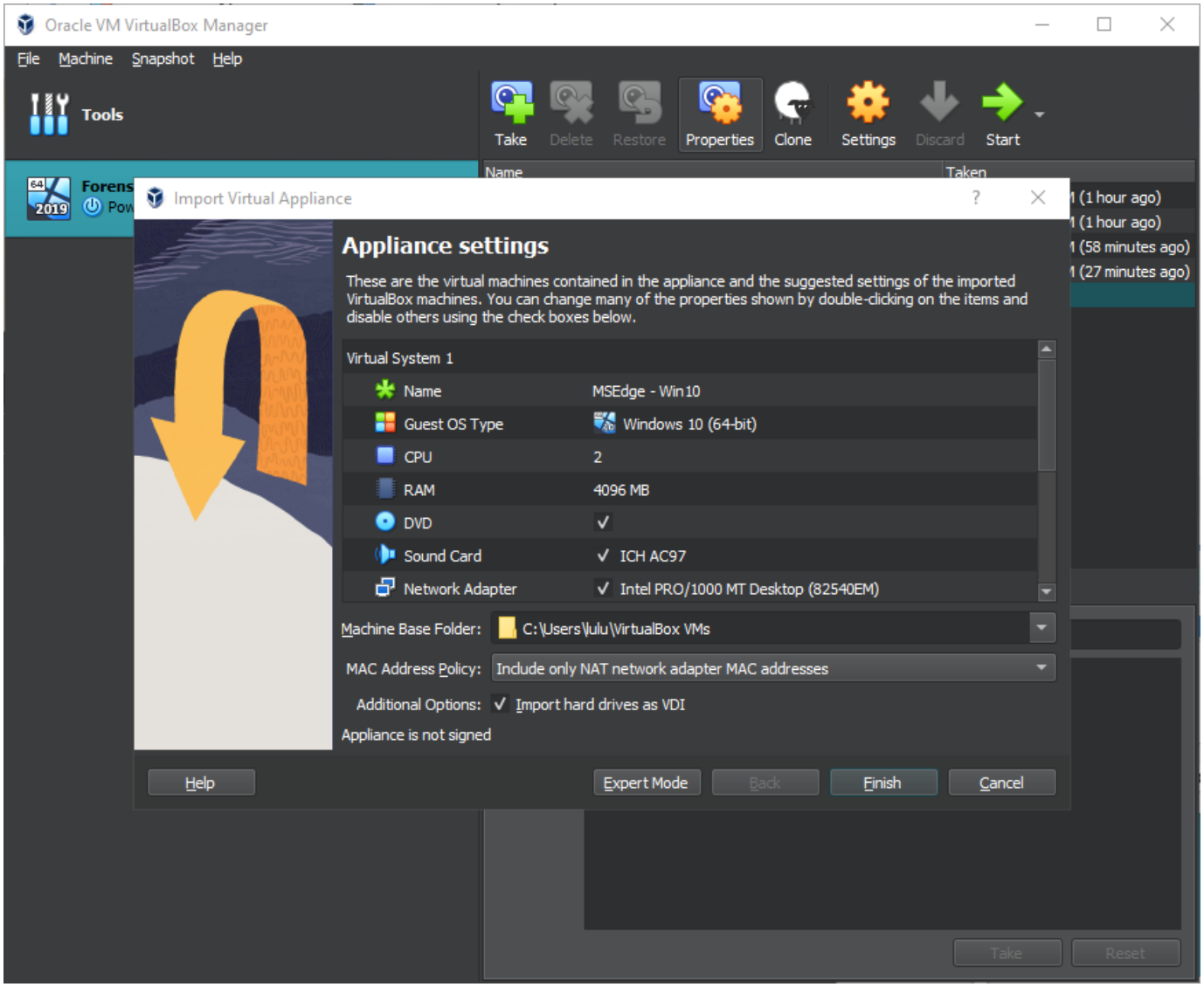
Installing VirtualBox

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

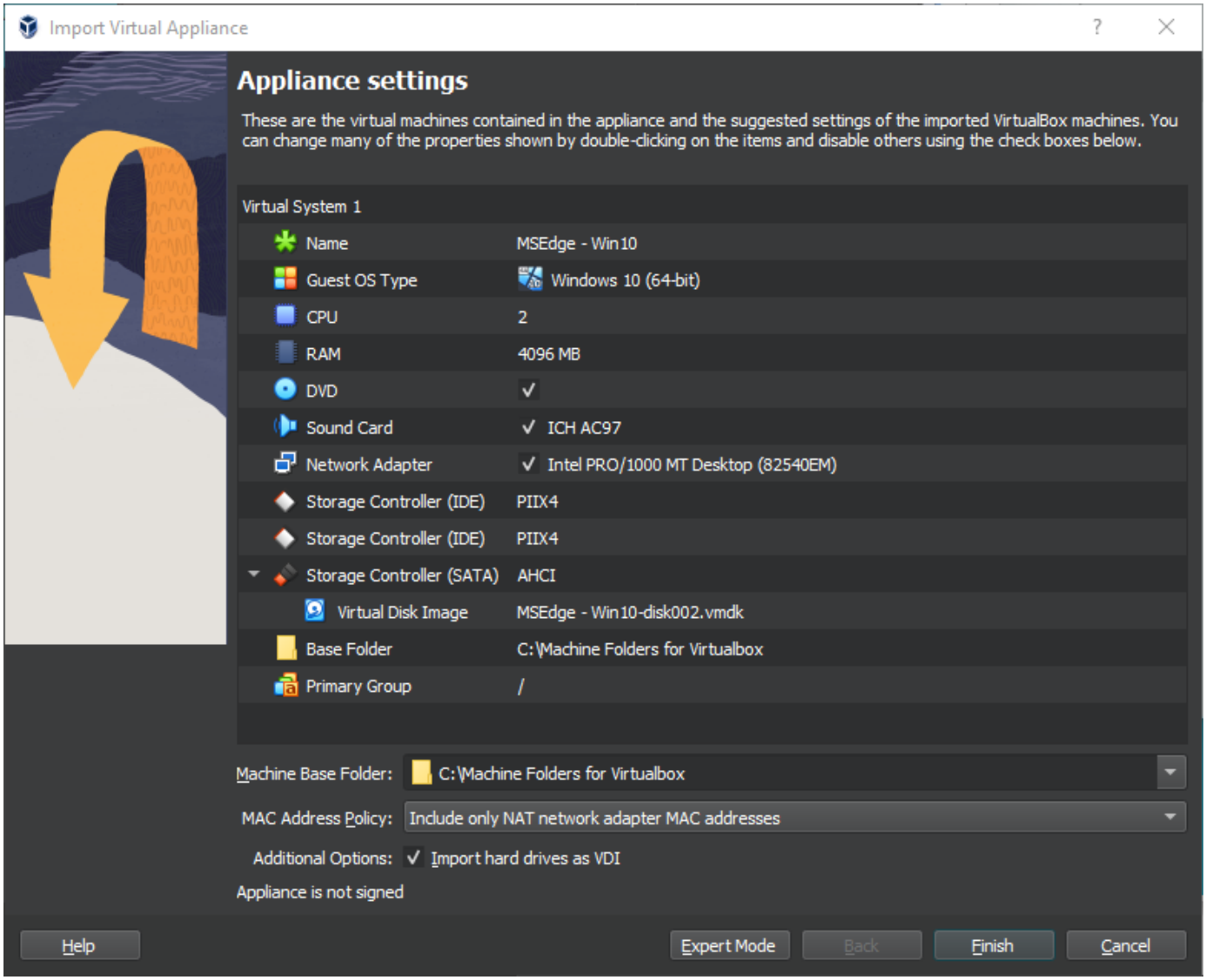


- Enter zip file and extract the .ova file to C:\VMs (in my case):

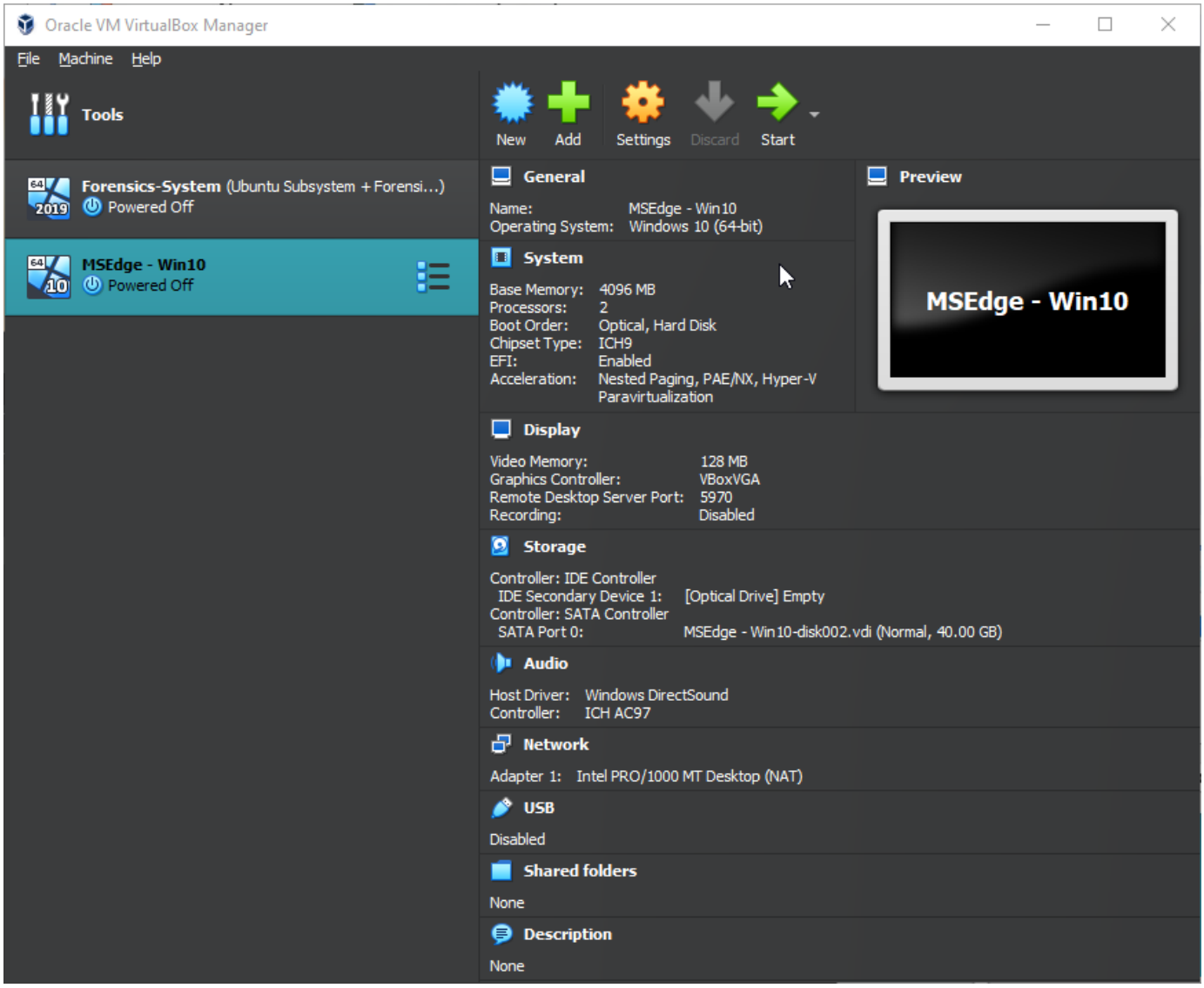
- Double Click on the file:



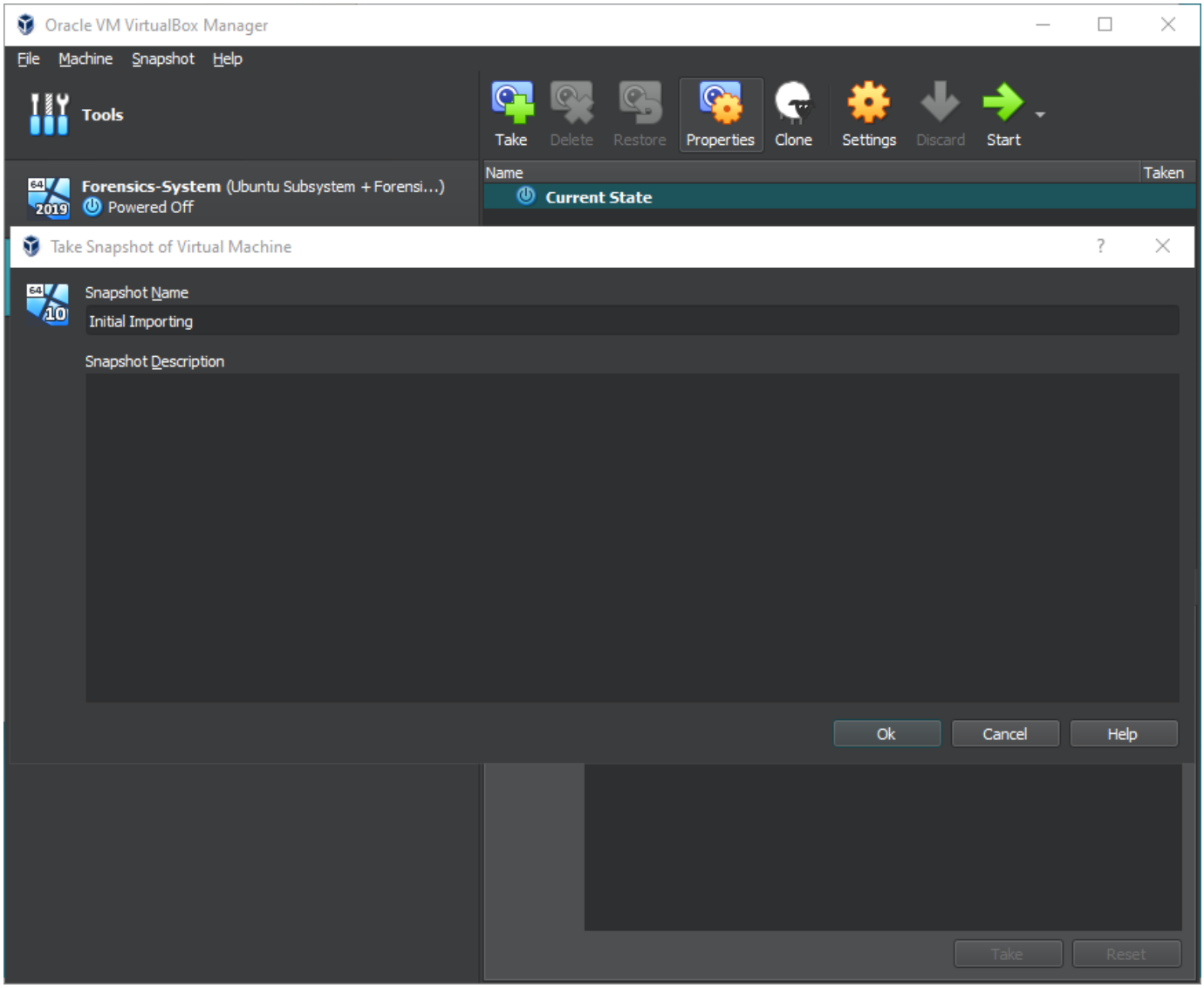
- Change the Machine Base Folder:

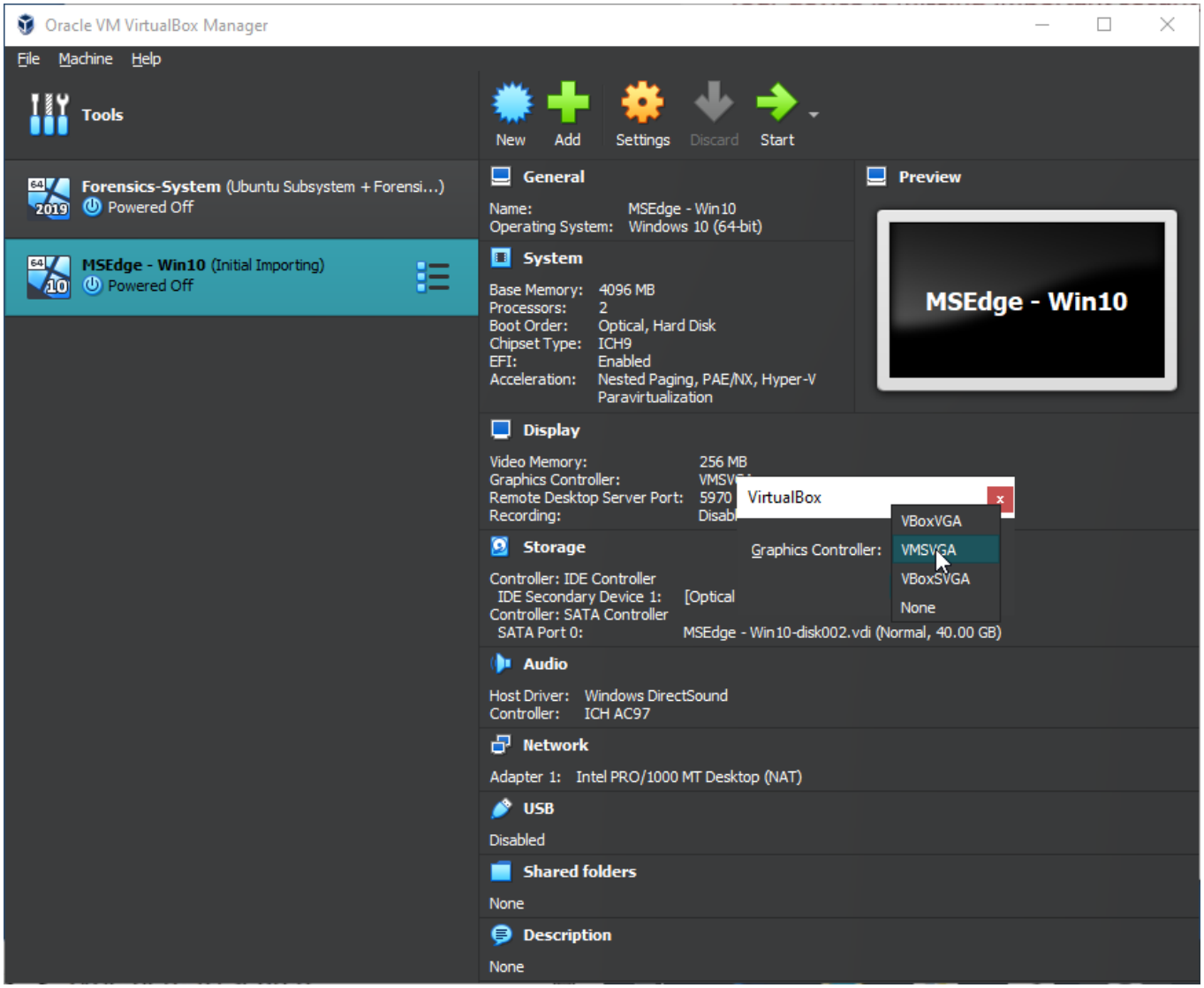


- There should be enough resources on the compromised virtual machine, press finish to finish importing:

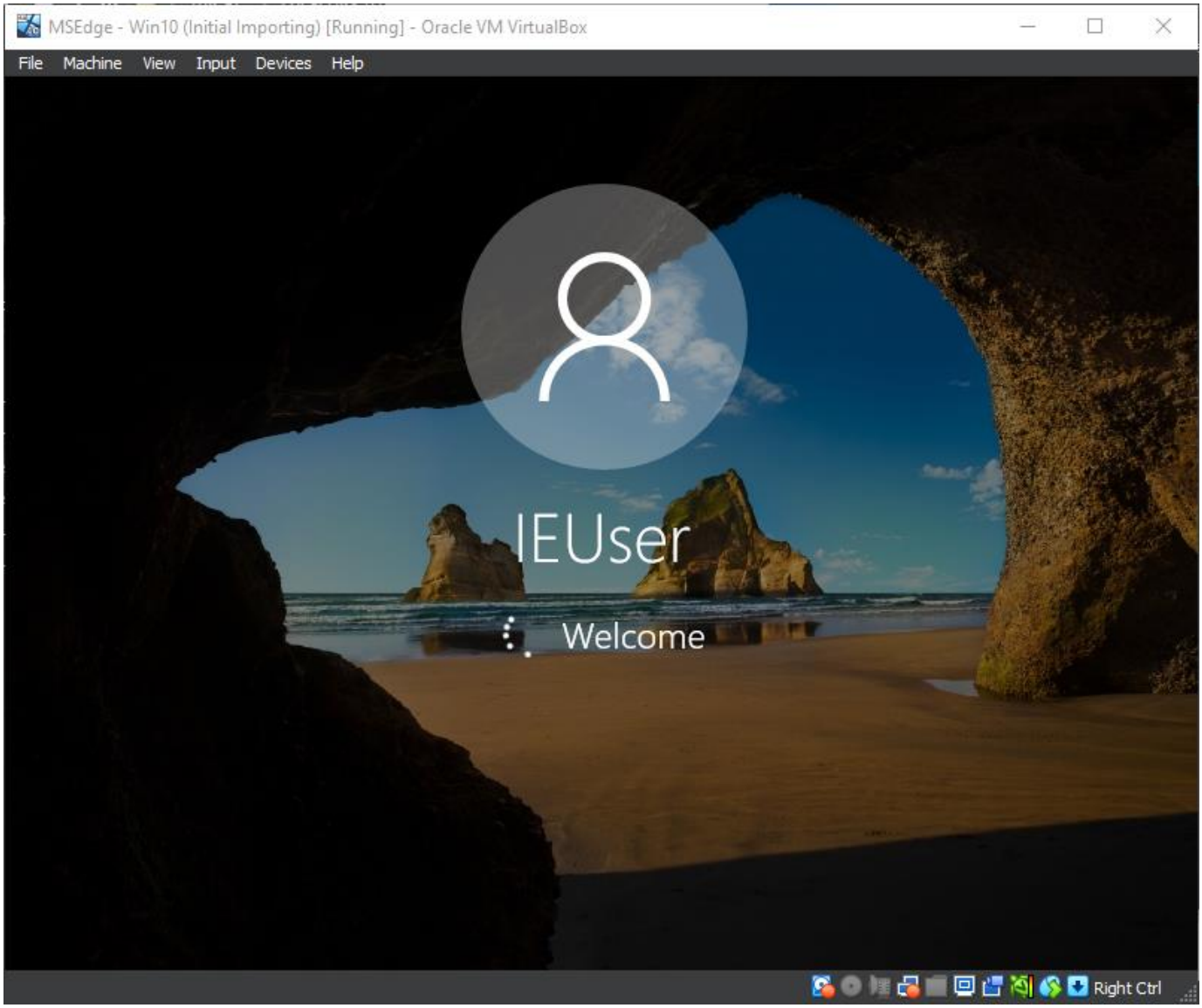


- Take an initial snapshot + Change Graphics Controller to VMSVGA boot, shutdown, then to VBoxVGA, then boot:


Oracle VM VirtualBox Manager
File Machine Snapshot Help
Tools
Take Delete Restore Properties Clone Settings Discard Start
Forensics-System (Ubuntu Subsystem + Forensi...)
Powered Off
Name Taken
Current State
Take Snapshot of Virtual Machine
Snapshot Name
Initial Importing
Snapshot Description
Ok Cancel Help
Take Reset

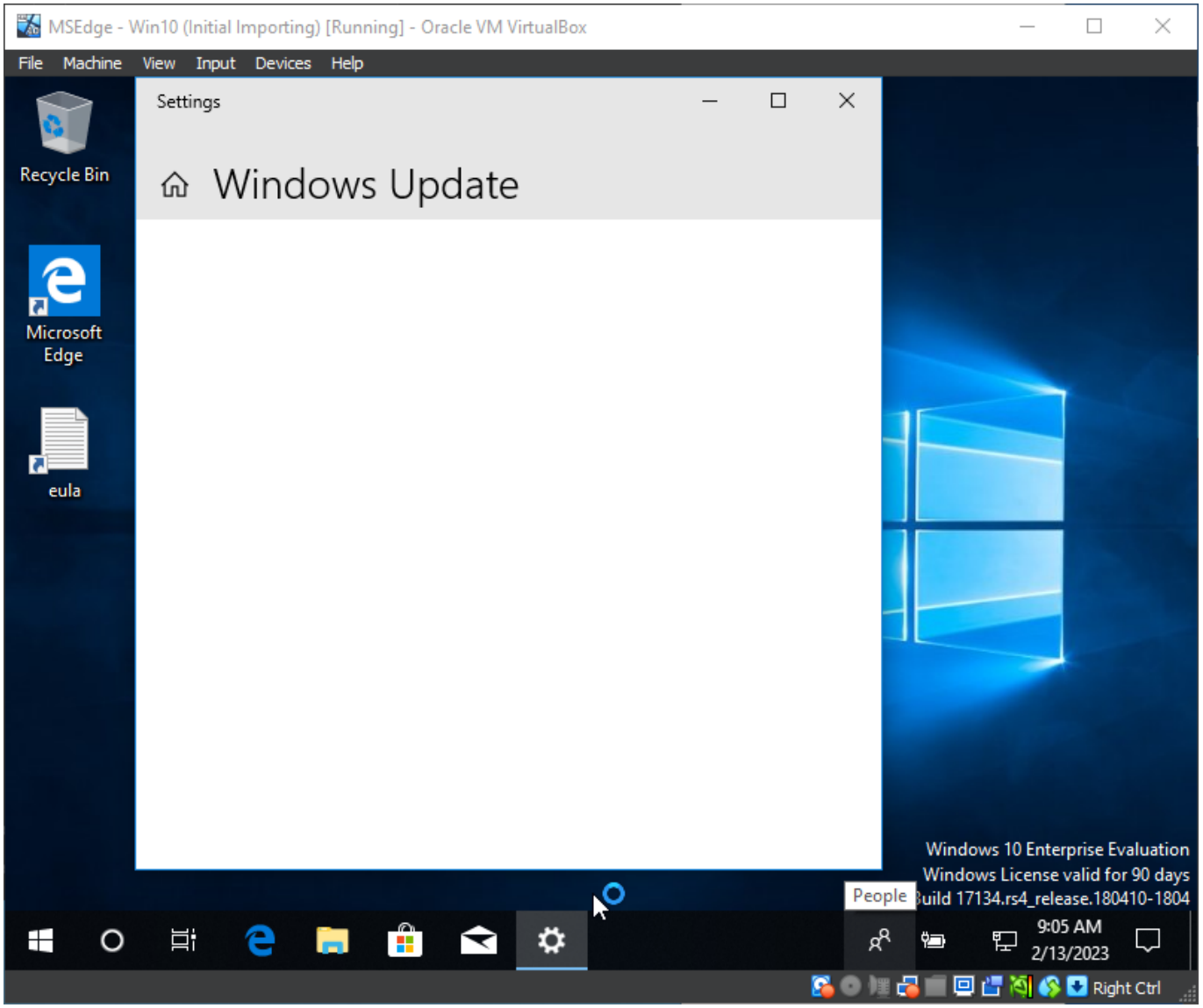


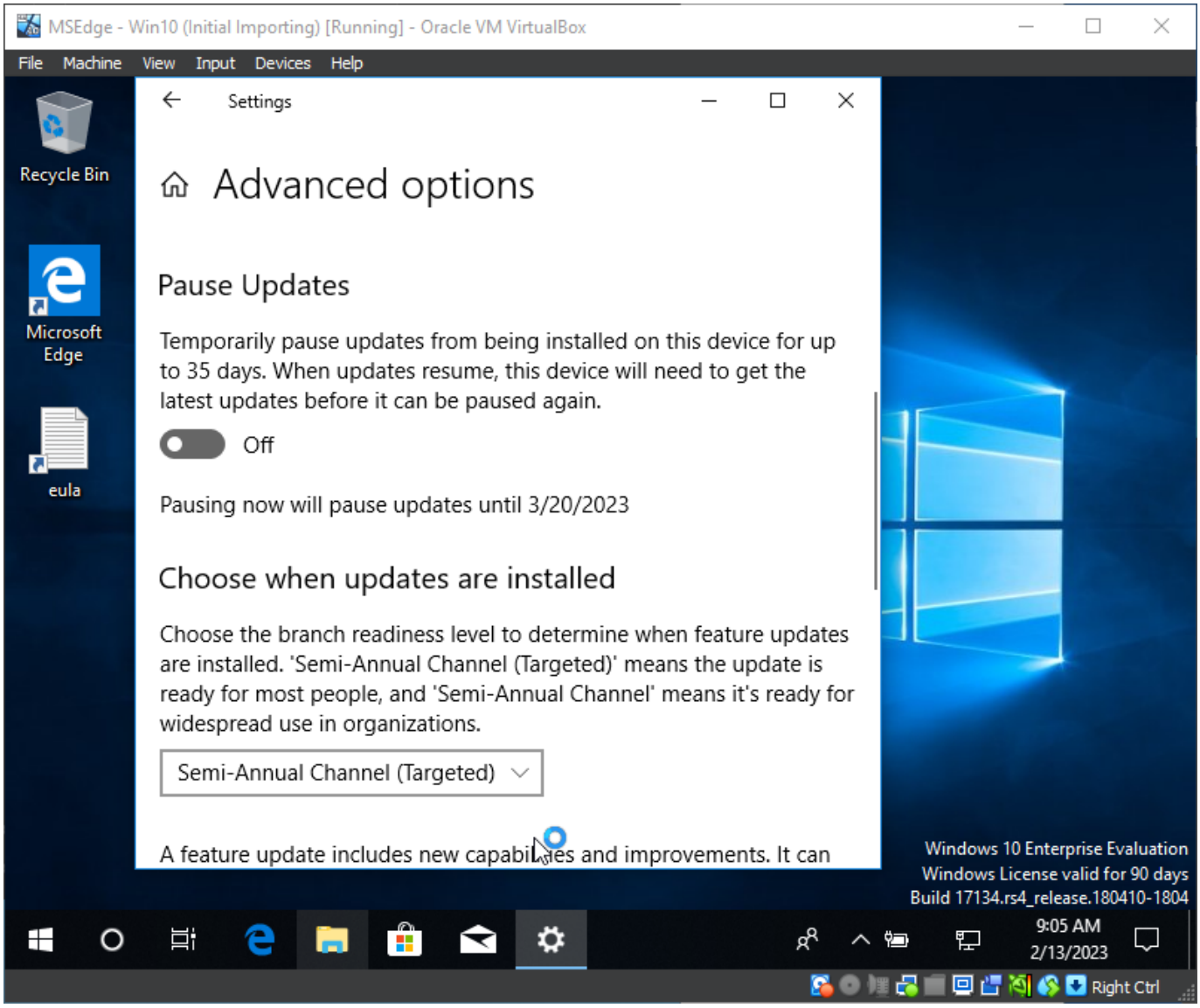
- Start the virtual machine:



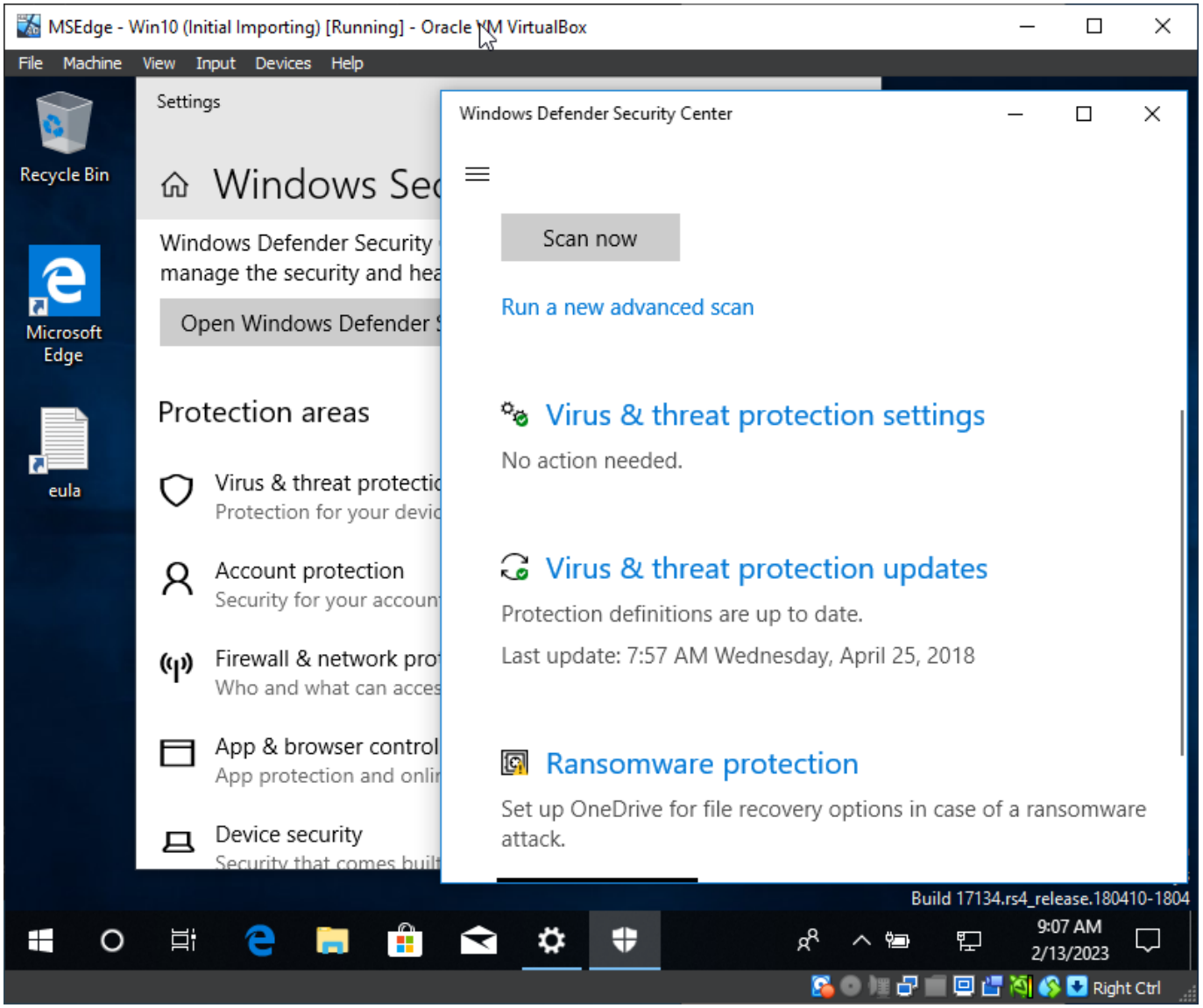
System configuration and downloading attack script

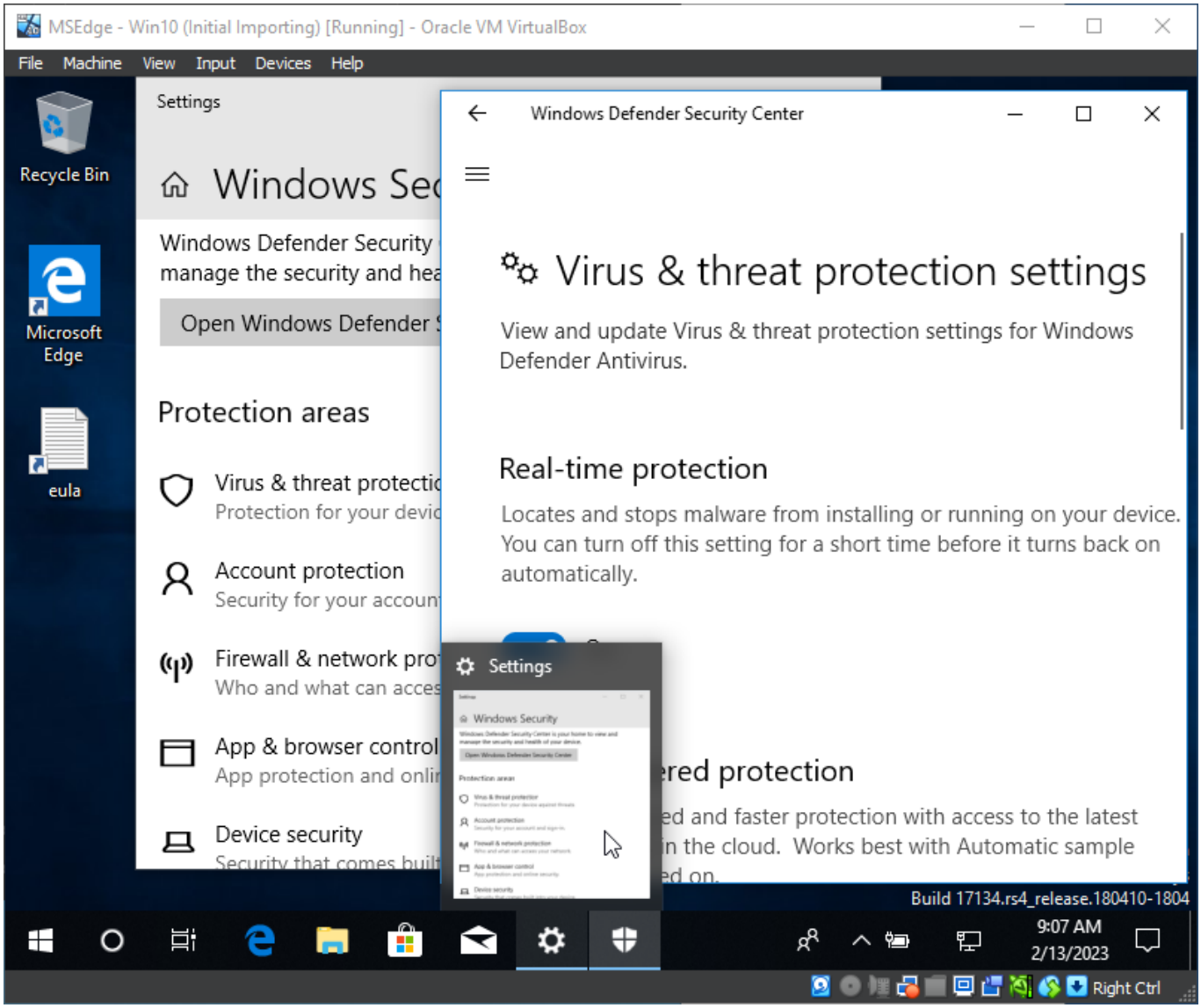
- Pause Windows Updates:

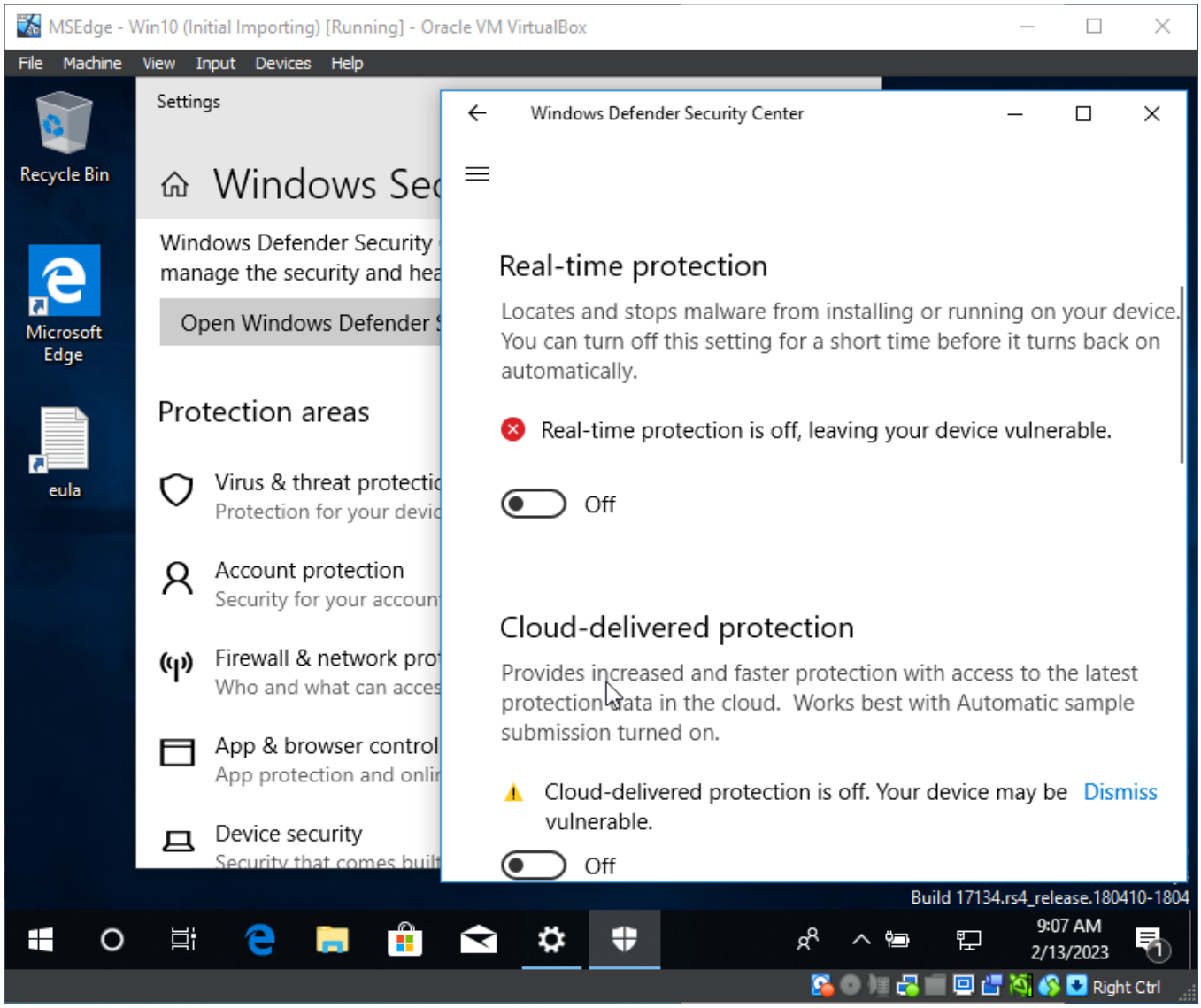

MSEdge - Win10 (Initial Importing) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
Settings
Windows Update
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
uild 17134.rs4_release.180410-1804
People
9:05 AM
2/13/2023
Right Ctrl

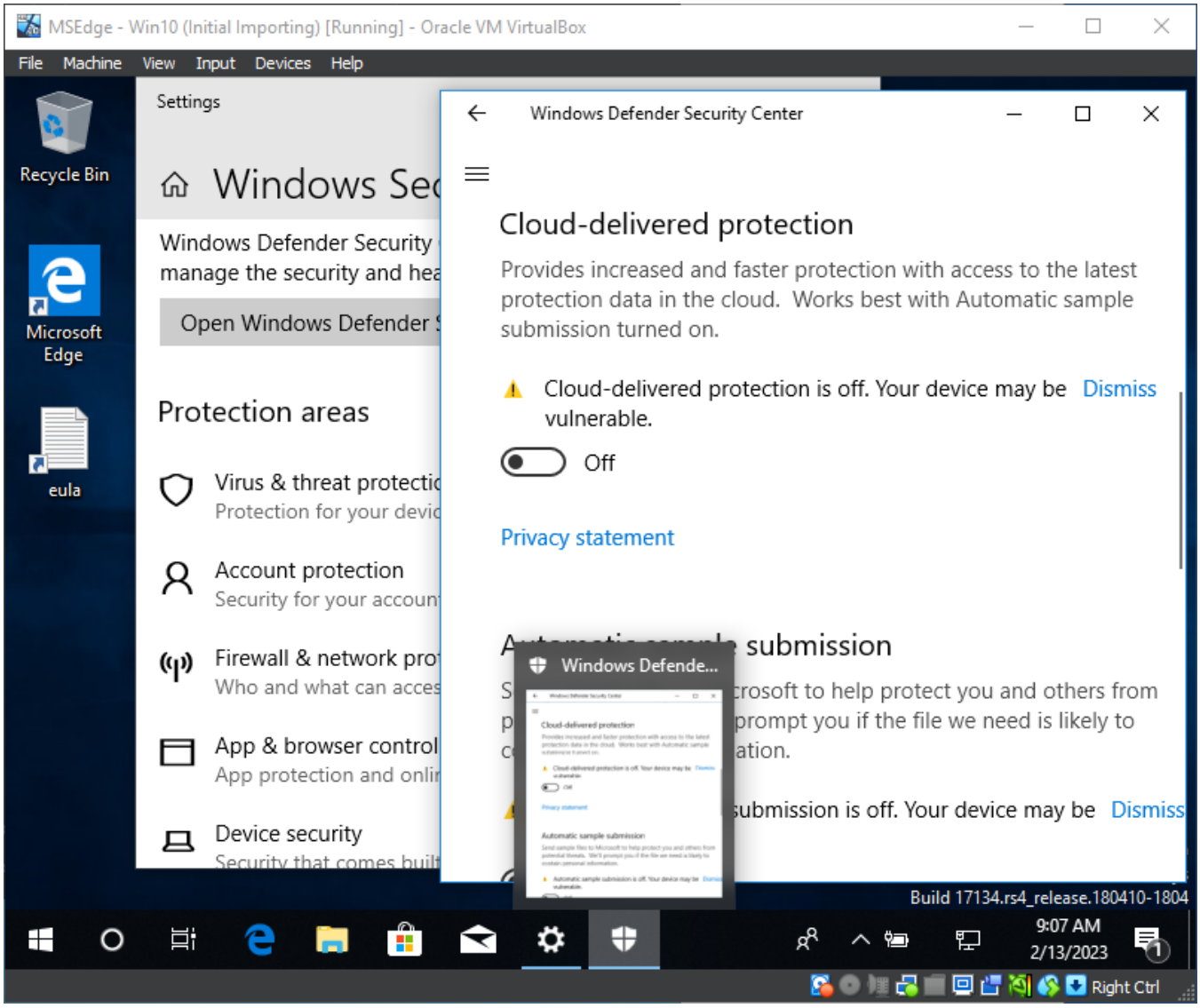


- Disable Defender Settings:

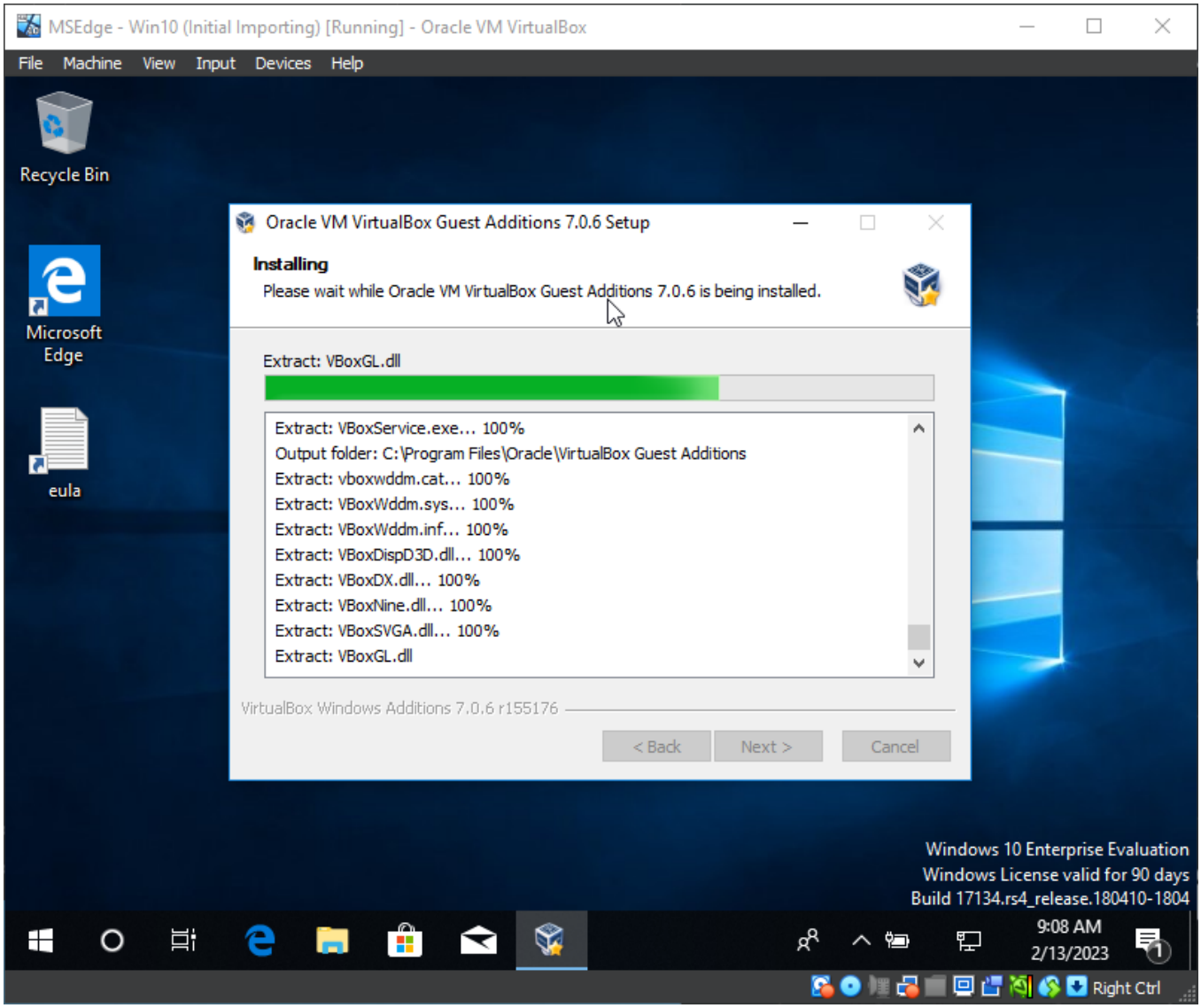

MSEdge - Win10 (Initial Importing) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
Settings
Windows Sec
Windows Defender Security
manage the security and hea
Open Windows Defender
Protection areas
Virus & threat protecti
Protection for your devic
Account protection
Security for your accoun
Firewall & network pro
Who and what can acce
App & browser control
App protection and onli
Device security
Windows Defender Security Center
Scan now
Run a new advanced scan
Virus & threat protection settings
No action needed.
Virus & threat protection updates
Protection definitions are up to date.
Last update: 7:57 AM Wednesday, April 25, 2018
Ransomware protection
Set up OneDrive for file recovery options in case of a ransomware attack.
Build 17134.rs4_release.180410-1804
9:07 AM
2/13/2023
Right Ctrl


MSEdge - Win10 (Initial Importing) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
Settings
Windows Sec
Windows Defender Security
manage the security and hea
Open Windows Defender
Protection areas
Virus & threat protecti
Protection for your devic
Account protection
Security for your accoun
Firewall & network pro
Who and what can acce
App & browser control
App protection and onli
Device security
Windows Defender Security Center
Virus & threat protection settings
View and update Virus & threat protection settings for Windows Defender Antivirus.
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.
Settings
ered protection
ed and faster protection with access to the latest
n the cloud. Works best with Automatic sample
ed on.
Build 17134.rs4_release.180410-1804
9:07 AM
2/13/2023
Right Ctrl

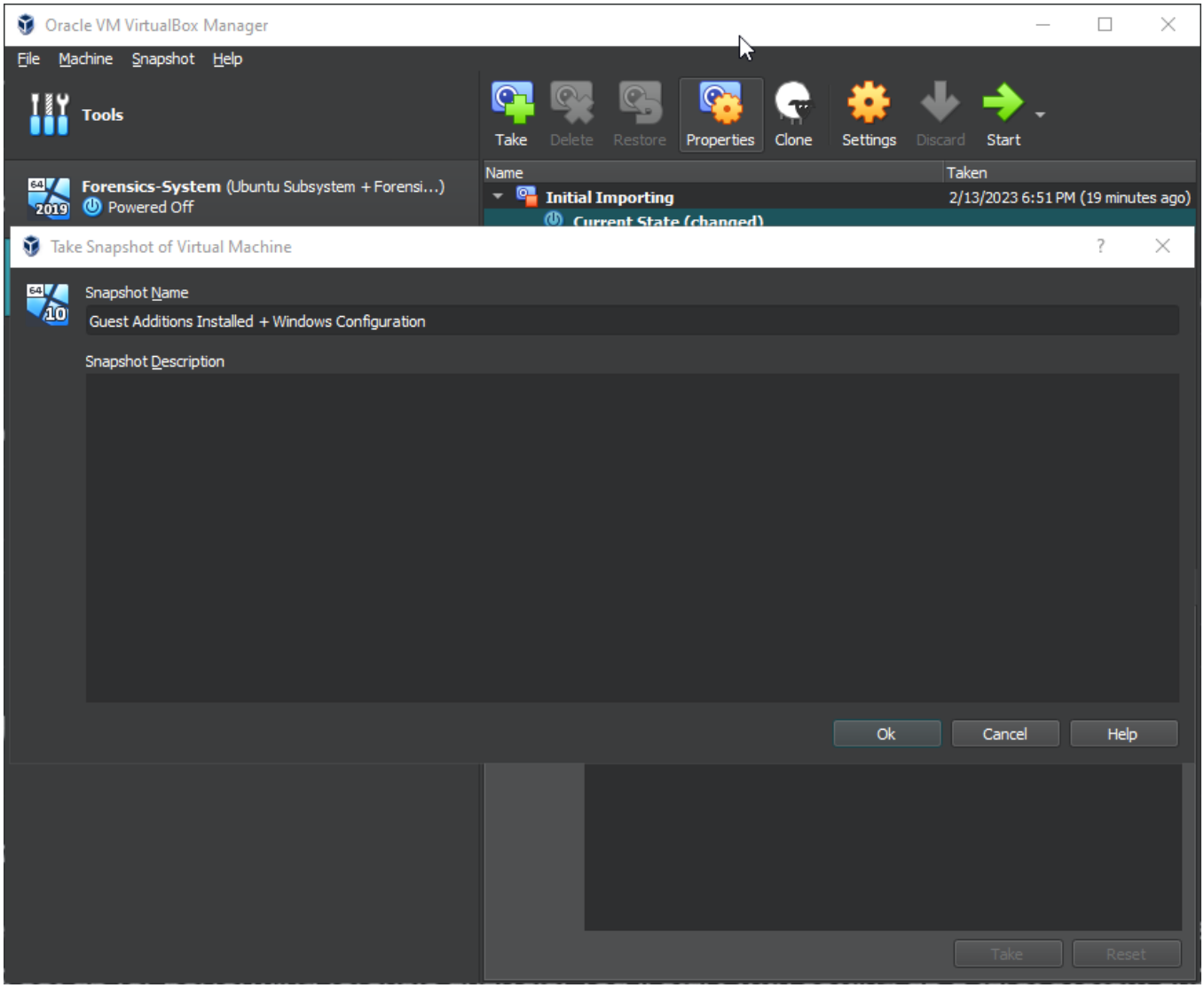

MSEdge - Win10 (Initial Importing) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
Settings
Windows Sec
Windows Defender Security
manage the security and hea
Open Windows Defender
Protection areas
Virus & threat protecti
Protection for your devic
Account protection
Security for your accoun
Firewall & network pro
Who and what can acces
App & browser control
App protection and onli
Device 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 vulnerable.
Dismiss
Off
Build 17134.rs4_release.180410-1804
9:07 AM
2/13/2023
Right Ctrl



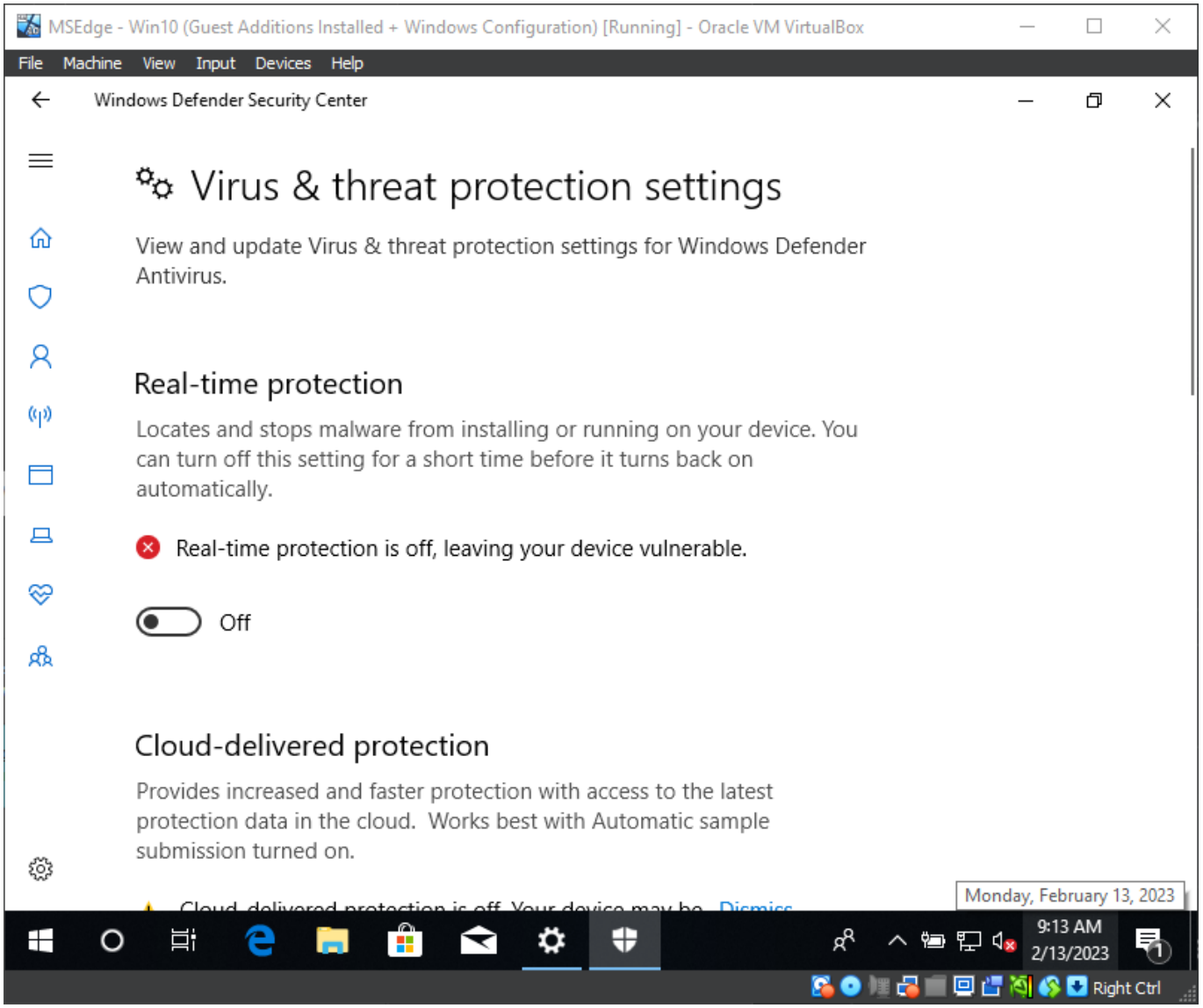
- Optional, install VBOX Guest Additions:



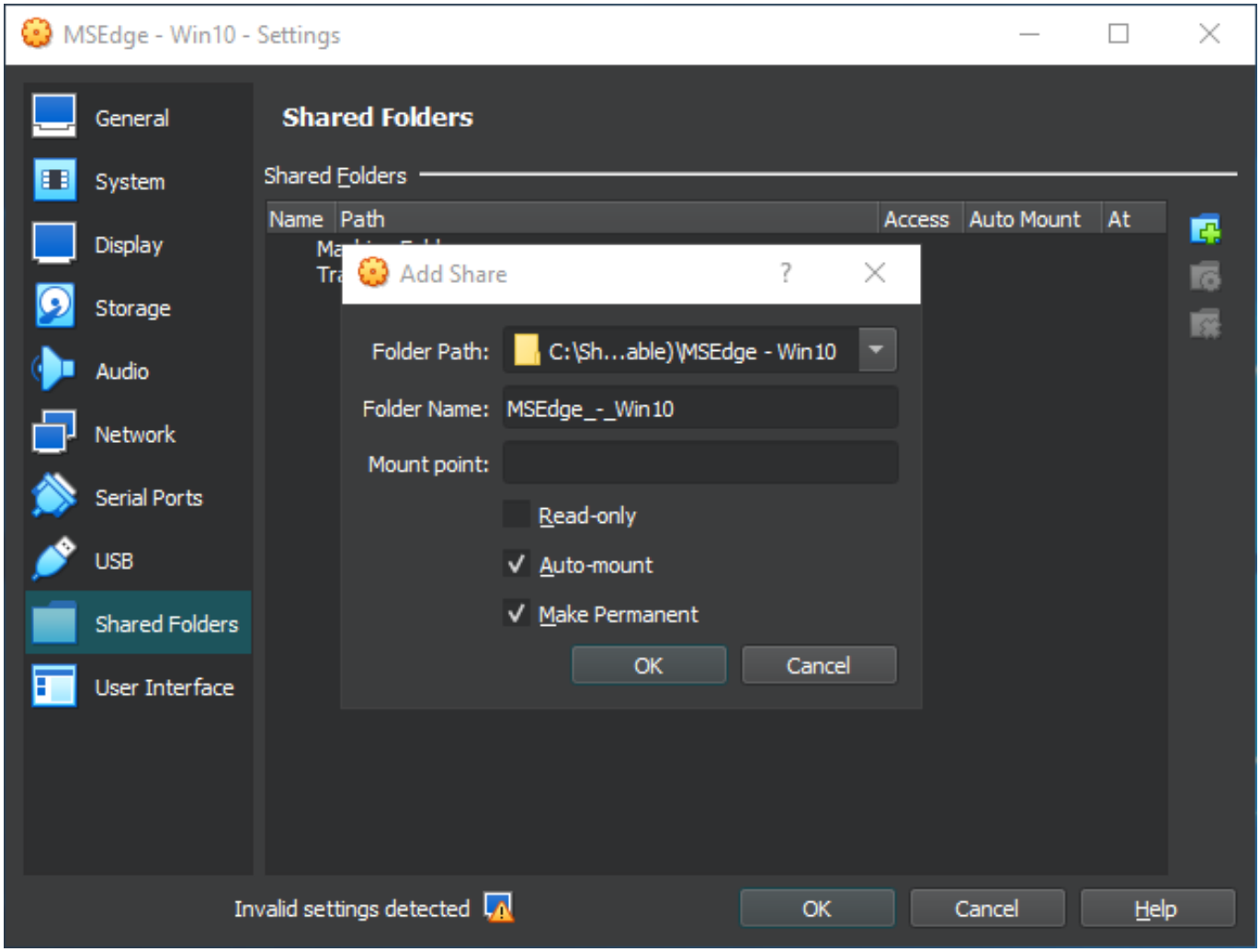
- Reboot, shutdown and take a snapshot:



- 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:



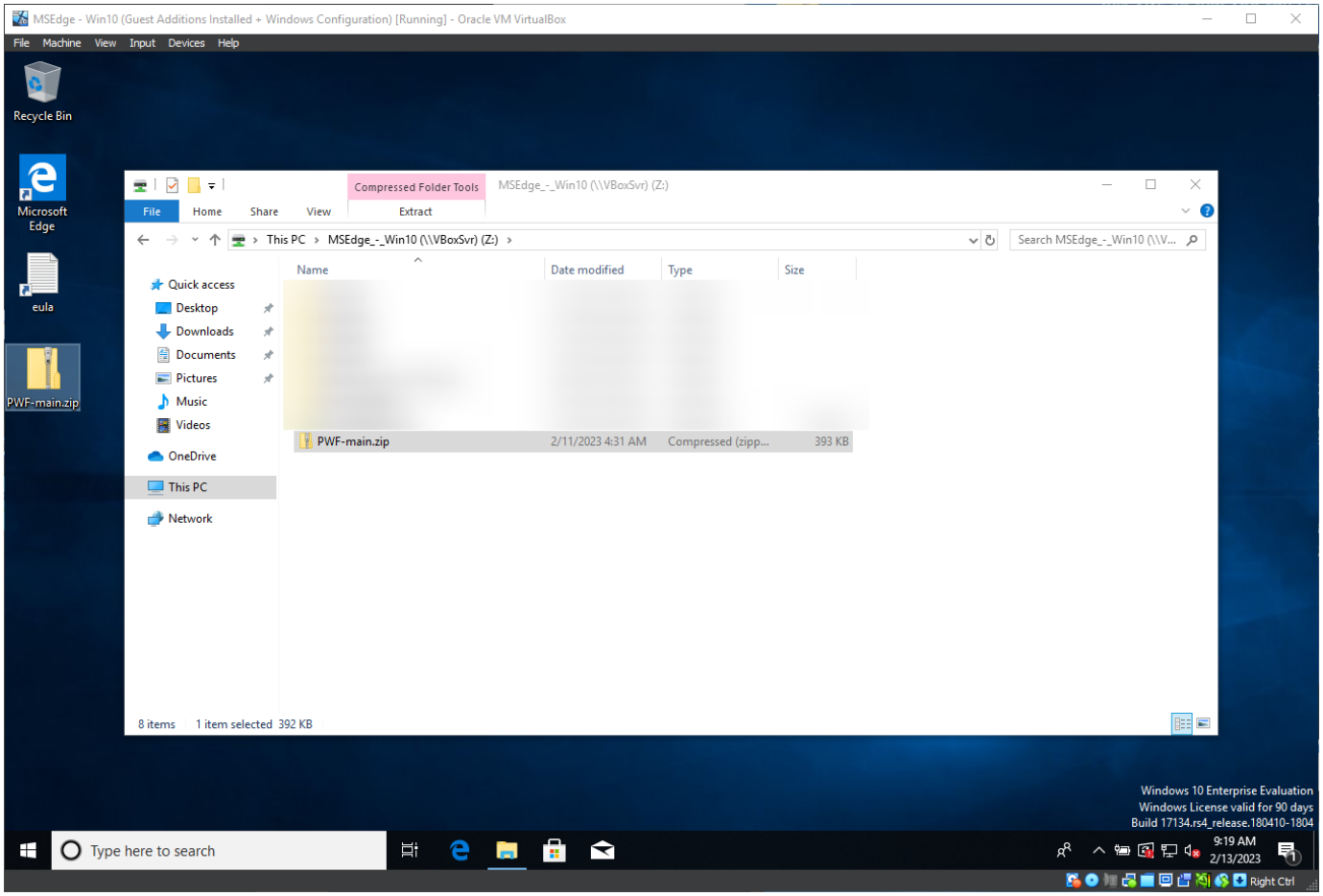
- Share folder with the virtual machine:



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

https://github.com/bluecapesecurity/PWF

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



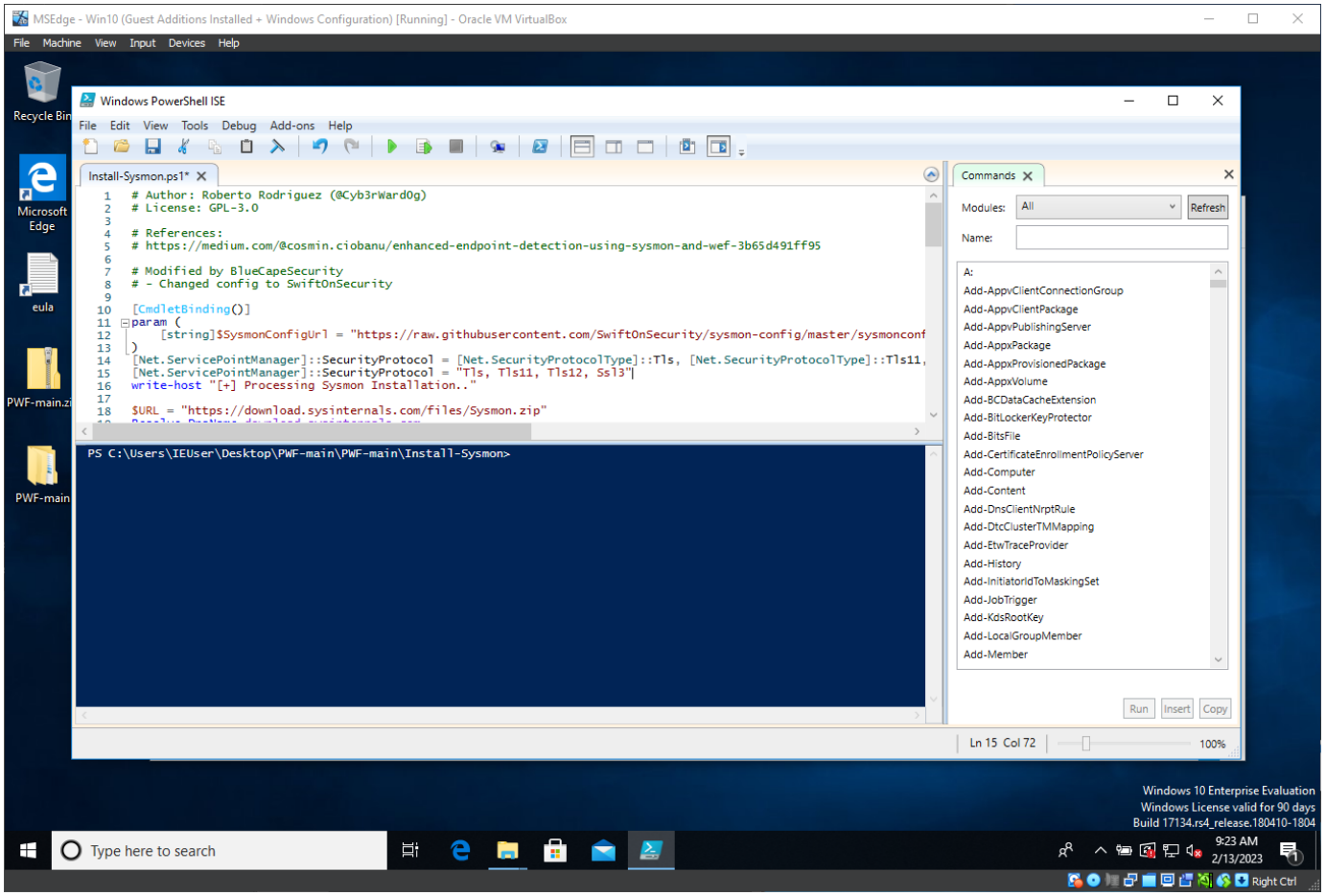
- Enter the folder PWF-main and edit all .ps1 files by adding the following code:

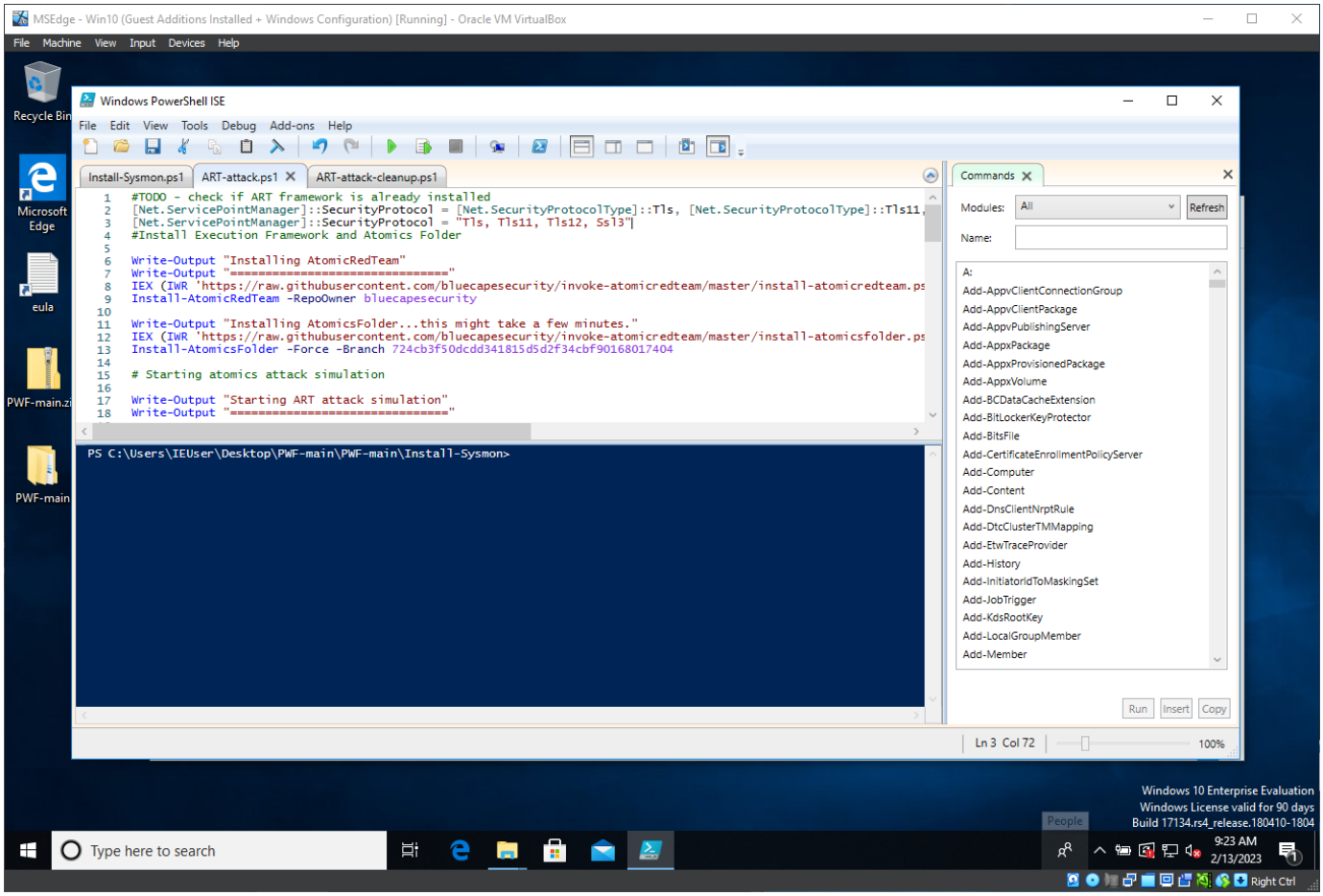
---------- ---------- ---------- ----------

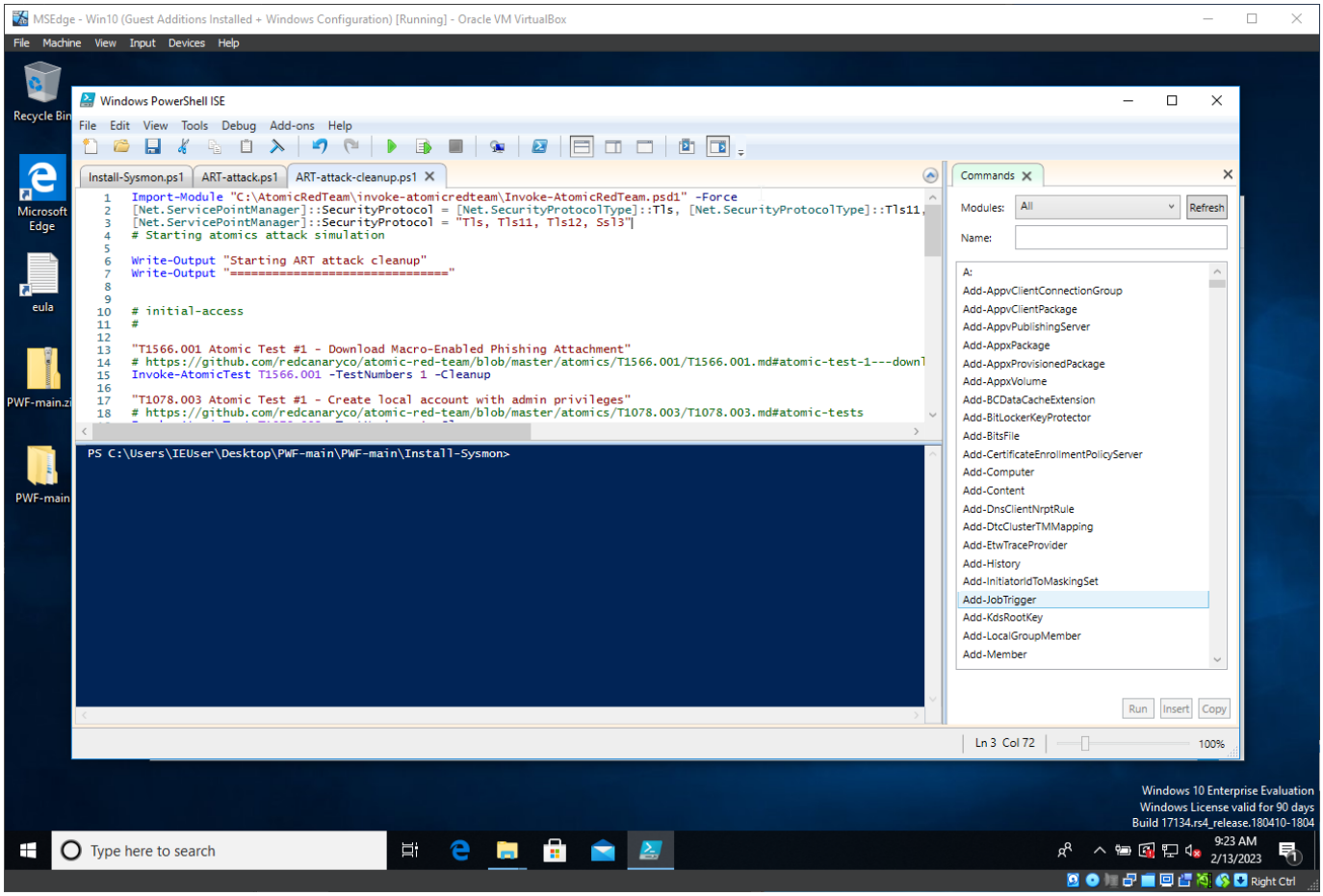
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls, [Net.SecurityProtocolType]::Tls11, [Net.SecurityProtocolType]::Tls12, [Net.SecurityProtocolType]::Ssl3

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

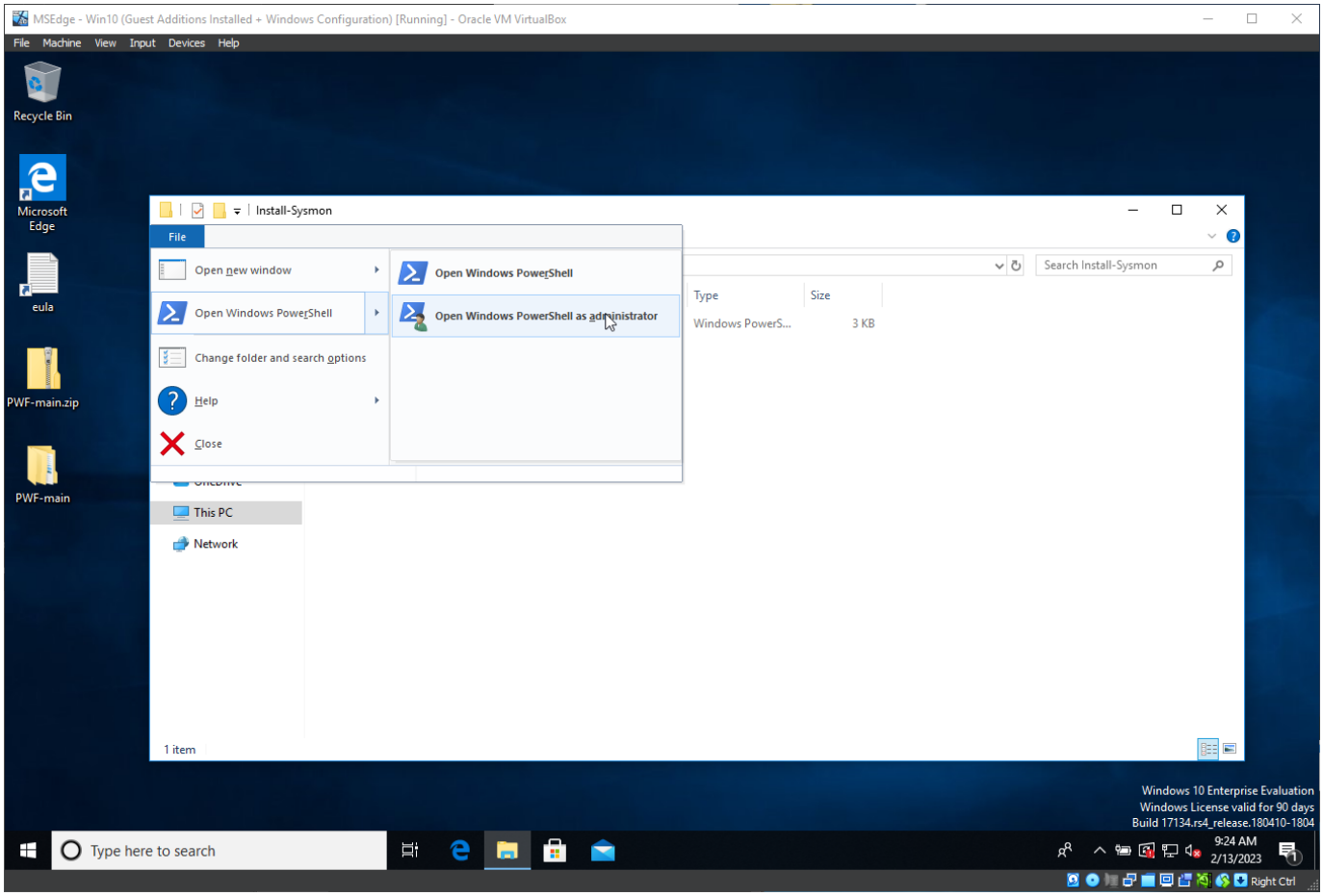
---------- ---------- ---------- ----------

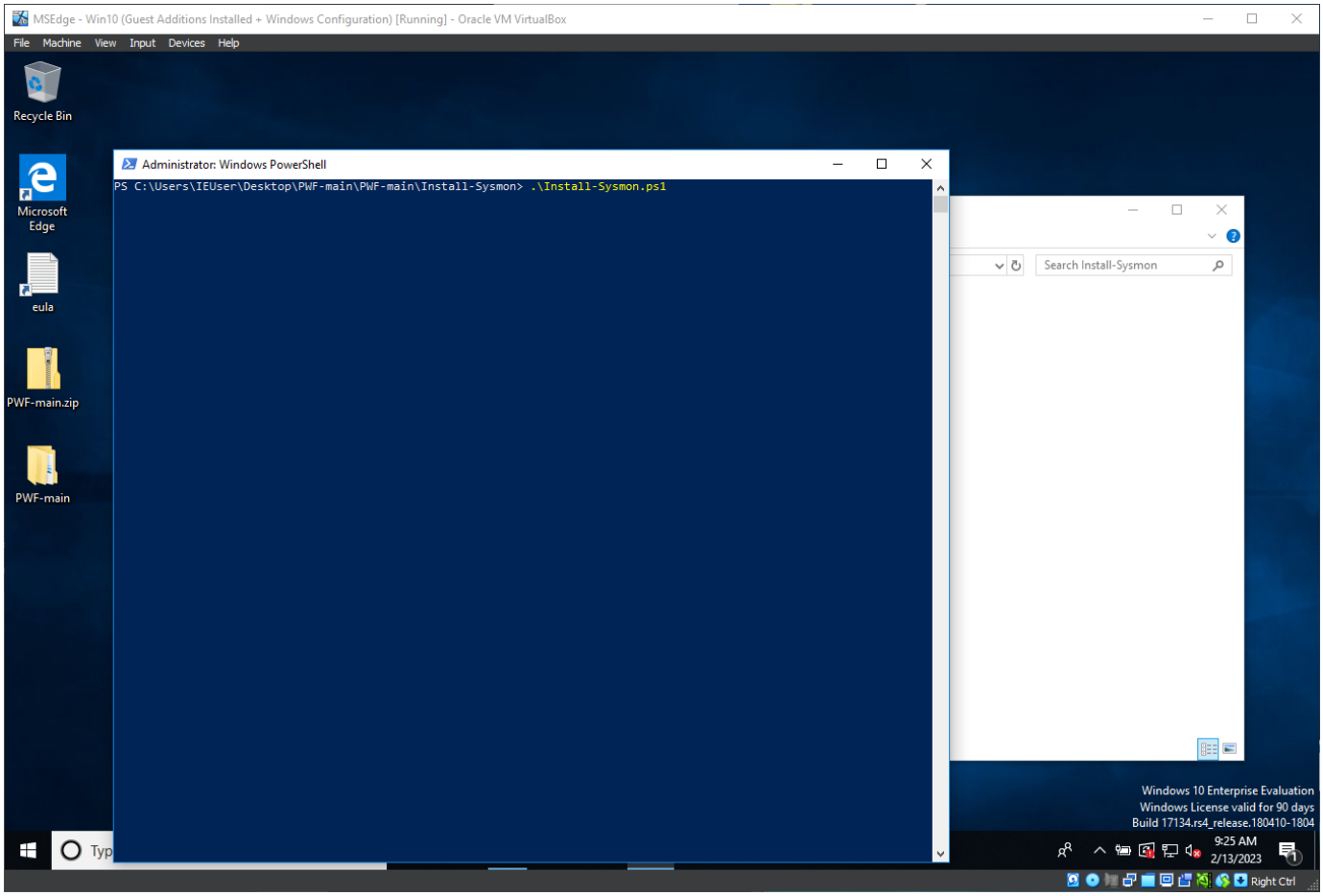

MSEdge - Win10 (Guest Additions Installed + Windows Configuration) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
PWF-main.zip
PWF-main
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Install-Sysmon.ps1*
Author: Roberto Rodriguez (@Cyb3rWard0g)
License: GPL-3.0
References:
https://medium.com/@cosmin.ciobanu/enhanced-endpoint-detection-using-sysmon-and-wef-3b65d491ff95
Modified by BlueCapeSecurity
- Changed config to SwiftOnSecurity
[CmdletBinding()]
param (
[string]$SysmonConfigUrl = "https://raw.githubusercontent.com/SwiftOnSecurity/sysmon-config/master/sysmonconf
)
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls, [Net.SecurityProtocolType]::Tls11,
[Net.ServicePointManager]::SecurityProtocol = "Tls, Tls11, Tls12, Ssl3"
write-host "[+] Processing Sysmon Installation.."
$URL = "https://download.sysinternals.com/files/Sysmon.zip"
PS C:\Users\IEUser\Desktop\PWF-main\PWF-main\Install-Sysmon>
Commands
Modules: All Refresh
Name:
A:
Add-AppvClientConnectionGroup
Add-AppvClientPackage
Add-AppvPublishingServer
Add-AppxPackage
Add-AppxProvisionedPackage
Add-AppxVolume
Add-BCDataCacheExtension
Add-BitLockerKeyProtector
Add-BitsFile
Add-CertificateEnrollmentPolicyServer
Add-Computer
Add-Content
Add-DnsClientNrptRule
Add-DtcClusterTMMapping
Add-EtwTraceProvider
Add-History
Add-InitiatorIdToMaskingSet
Add-JobTrigger
Add-KdsRootKey
Add-LocalGroupMember
Add-Member
Run Insert Copy
Ln 15 Col 72
100%
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 17134.rs4_release.180410-1804
Type here to search
9:23 AM
2/13/2023
Right Ctrl

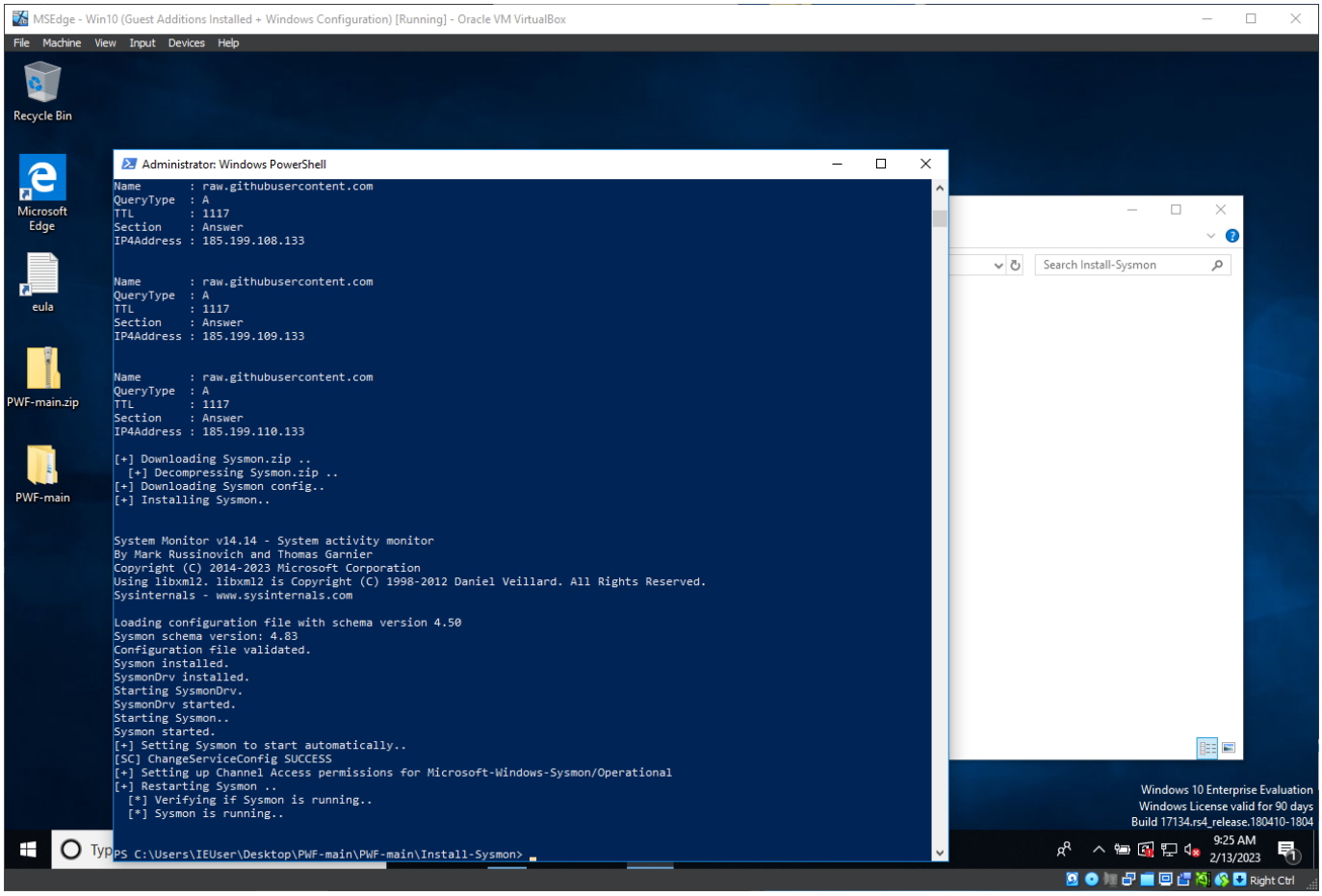

MSEdge - Win10 (Guest Additions Installed + Windows Configuration) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
PWF-main.zip
PWF-main
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Install-Sysmon.ps1
ART-attack.ps1
ART-attack-cleanup.ps1
#TODO - check if ART framework is already installed
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls, [Net.SecurityProtocolType]::Tls11,
[Net.ServicePointManager]::SecurityProtocol = "Tls, Tls11, Tls12, Ssl3"
#Install Execution Framework and Atomics Folder
Write-Output "Installing AtomicRedTeam"
Write-Output "============================="
IEX (IWR 'https://raw.githubusercontent.com/bluecapesecurity/invoke-atomicredteam/master/install-atomicredteam.ps
Install-AtomicRedTeam -RepoOwner bluecapesecurity
Write-Output "Installing AtomicsFolder...this might take a few minutes."
IEX (IWR 'https://raw.githubusercontent.com/bluecapesecurity/invoke-atomicredteam/master/install-atomicsfolder.ps
Install-AtomicsFolder -Force -Branch 724cb3f50dcdd341815d5d2f34cbf90168017404
Starting atomics attack simulation
Write-Output "Starting ART attack simulation"
Write-Output "============================="
PS C:\Users\IEUser\Desktop\PWF-main\PWF-main\Install-Sysmon>
Commands
Modules: All
Refresh
Name:
A:
Add-AppvClientConnectionGroup
Add-AppvClientPackage
Add-AppvPublishingServer
Add-AppxPackage
Add-AppxProvisionedPackage
Add-AppxVolume
Add-BCDataCacheExtension
Add-BitLockerKeyProtector
Add-BitsFile
Add-CertificateEnrollmentPolicyServer
Add-Computer
Add-Content
Add-DnsClientNrptRule
Add-DtcClusterTMMapping
Add-EtwTraceProvider
Add-History
Add-InitiatorIdToMaskingSet
Add-JobTrigger
Add-KdsRootKey
Add-LocalGroupMember
Add-Member
Run Insert Copy
Ln 3 Col 72
100%
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 17134.rs4_release.180410-1804
Type here to search
People
9:23 AM
2/13/2023
Right Ctrl



- Install Sysmon:

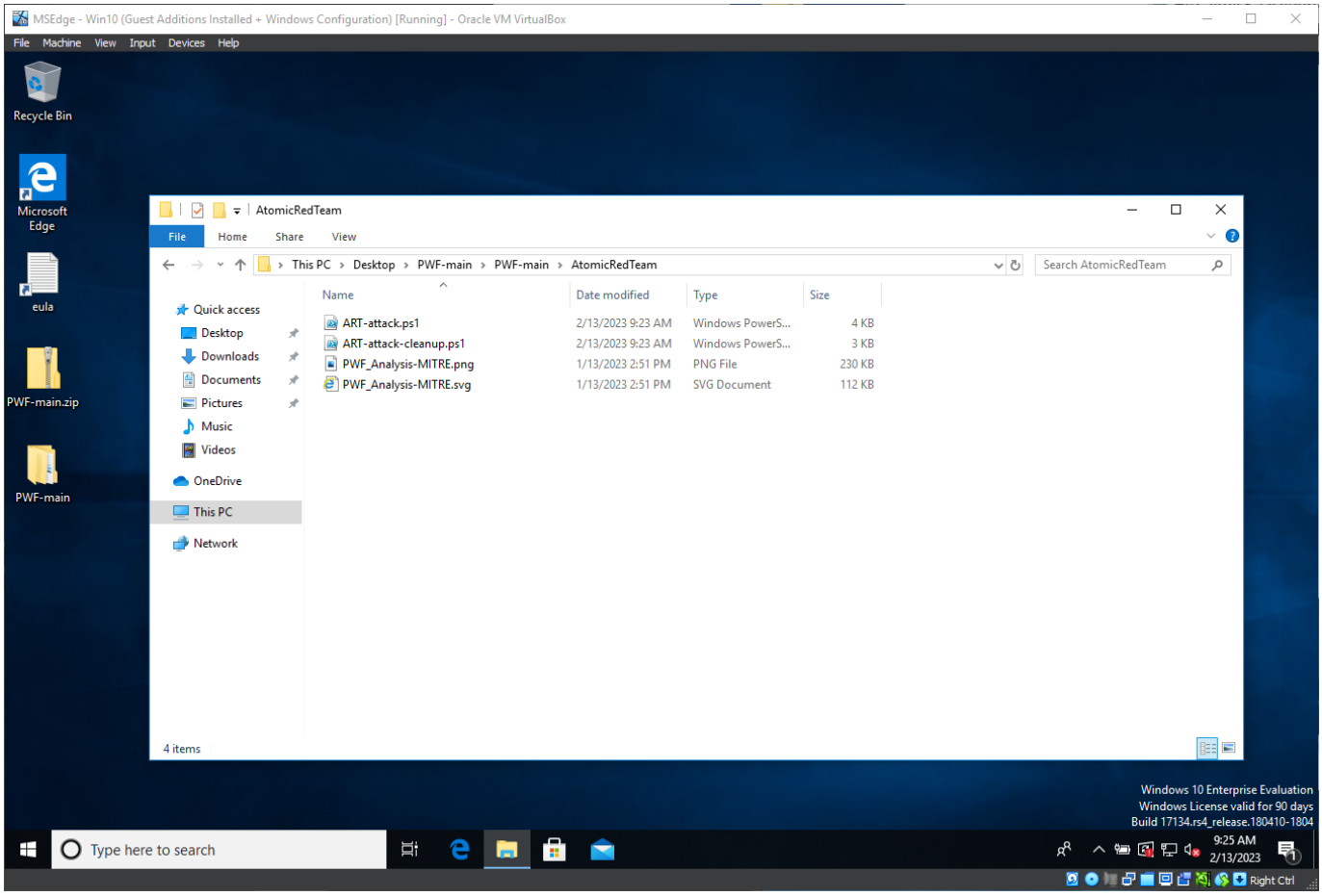

MSEdge - Win10 (Guest Additions Installed + Windows Configuration) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
PWF-main.zip
PWF-main
Install-Sysmon
File
Open new window
Open Windows PowerShell
Change folder and search options
Help
Close
Open Windows PowerShell
Open Windows PowerShell as administrator
Search Install-Sysmon
Type
Size
Windows PowerS...
3 KB
This PC
Network
1 item
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 17134.rs4_release.180410-1804
Type here to search
9:24 AM
2/13/2023
Right Ctrl

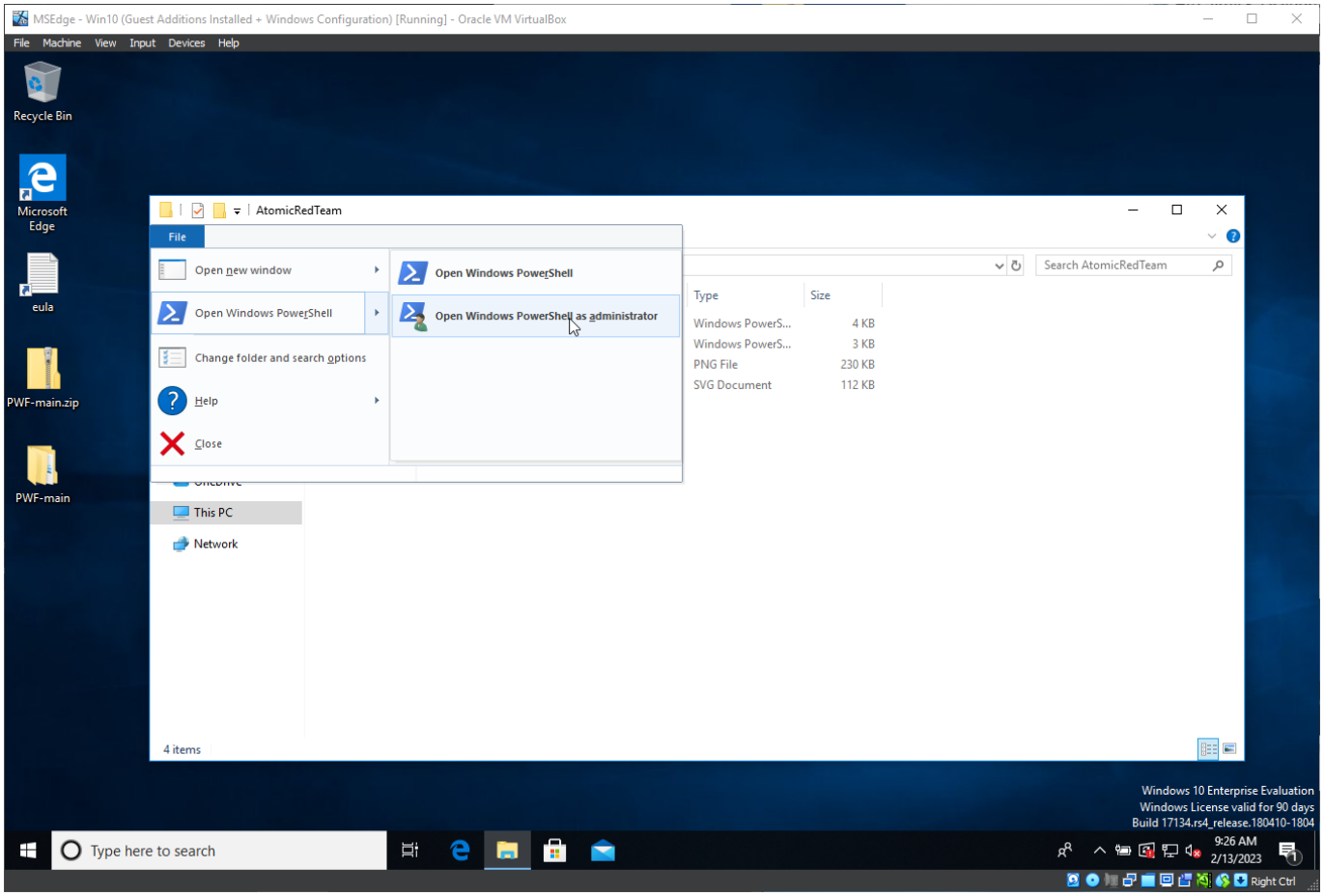

MSEdge - Win10 (Guest Additions Installed + Windows Configuration) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
PWF-main.zip
PWF-main
Administrator: Windows PowerShell
PS C:\Users\IEUser\Desktop\PWF-main\PWF-main\Install-Sysmon> .\Install-Sysmon.ps1
Search Install-Sysmon
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 17134.rs4_release.180410-1804
9:25 AM
2/13/2023
Right Ctrl

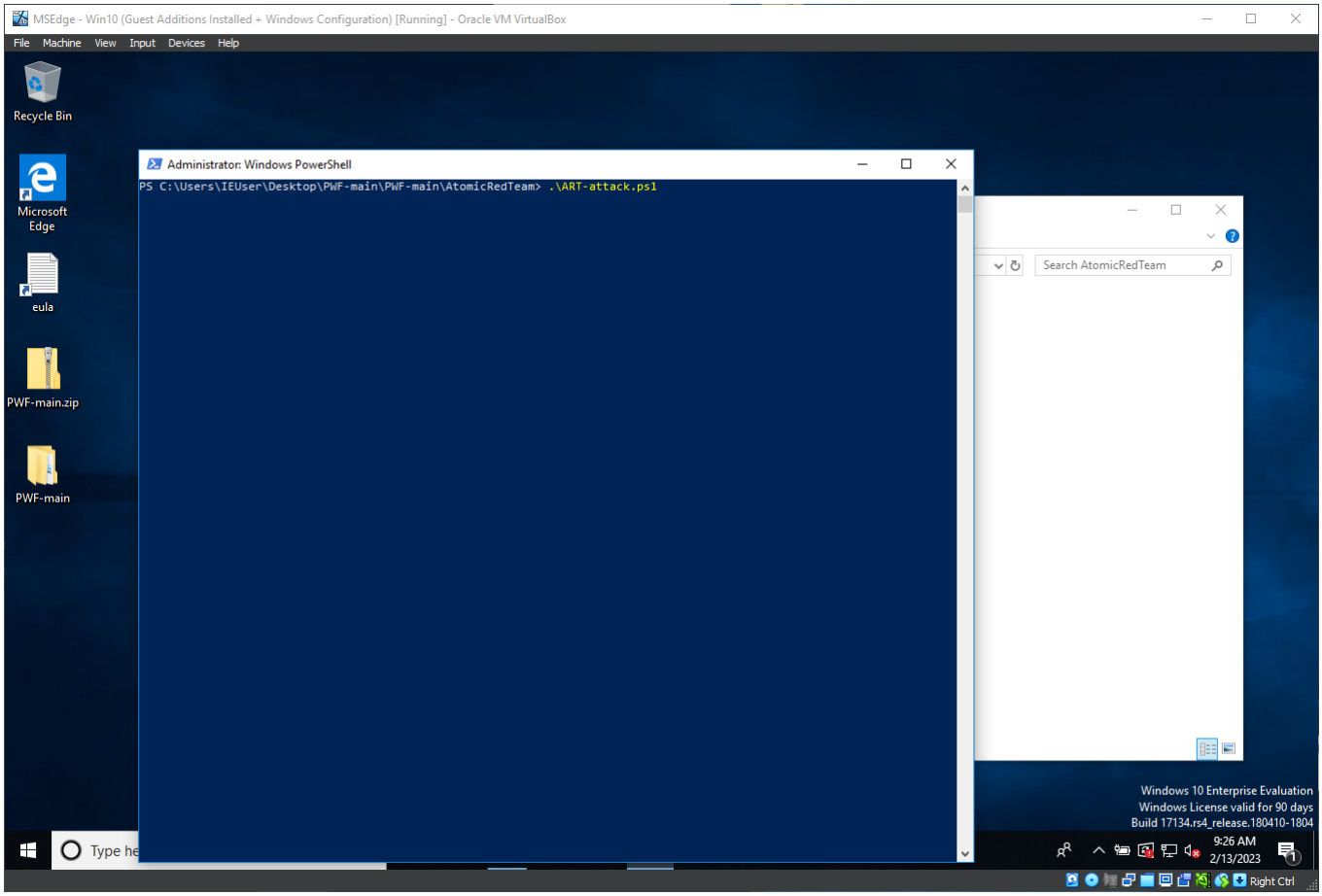


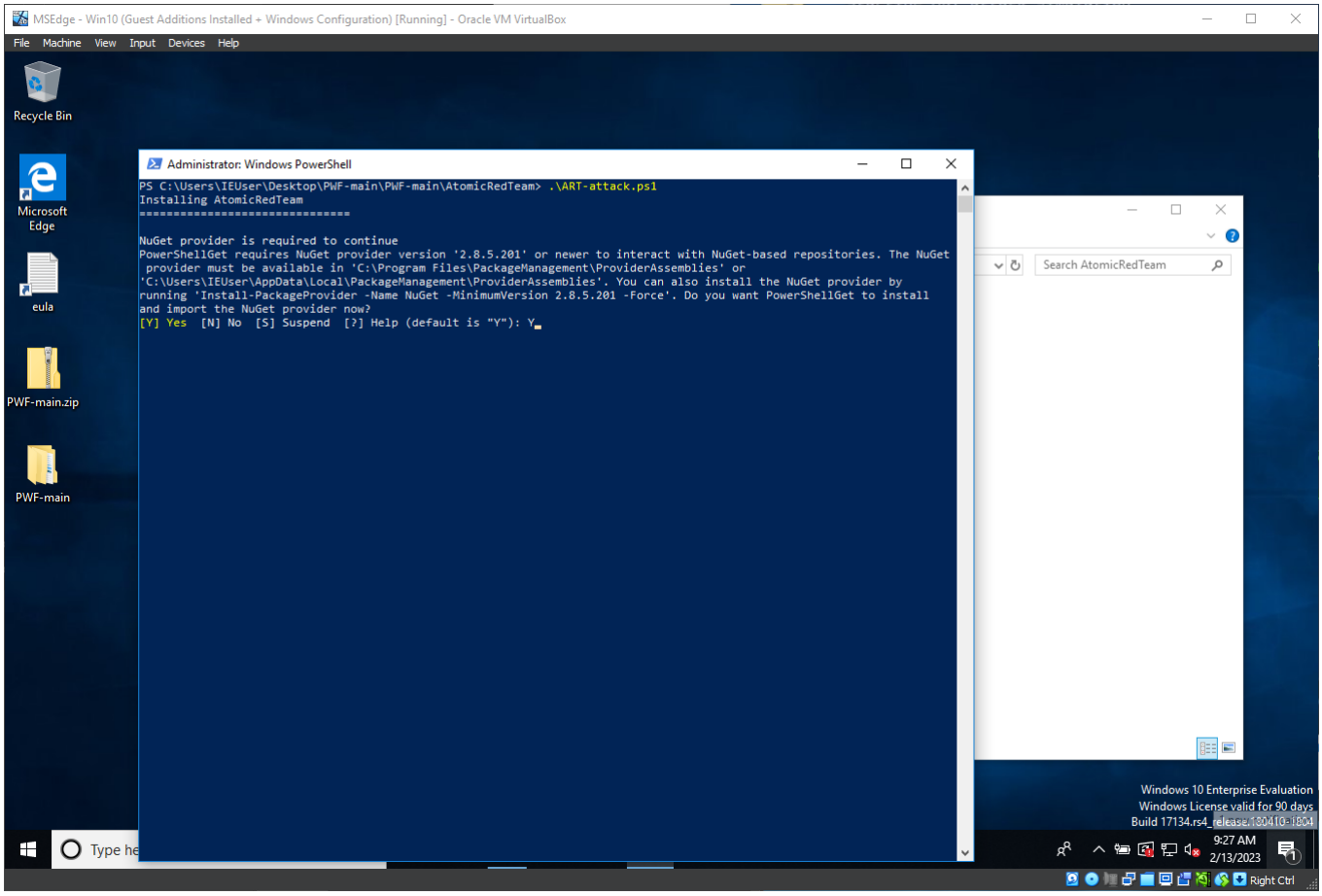
Execution of attack script

- 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:


MSEdge - Win10 (Guest Additions Installed + Windows Configuration) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
PWF-main.zip
PWF-main
AtomicRedTeam
File Home Share View
This PC › Desktop › PWF-main › PWF-main › AtomicRedTeam
Search AtomicRedTeam
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
ART-attack.ps1 2/13/2023 9:23 AM Windows PowerS... 4 KB
ART-attack-cleanup.ps1 2/13/2023 9:23 AM Windows PowerS... 3 KB
PWF_Analysis-MITRE.png 1/13/2023 2:51 PM PNG File 230 KB
PWF_Analysis-MITRE.svg 1/13/2023 2:51 PM SVG Document 112 KB
4 items
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 17134.rs4_release.180410-1804
Type here to search
9:25 AM
2/13/2023
Right Ctrl


MSEdge - Win10 (Guest Additions Installed + Windows Configuration) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
PWF-main.zip
PWF-main
AtomicRedTeam
File
Open new window
Open Windows PowerShell
Change folder and search options
Help
Close
Open Windows PowerShell
Open Windows PowerShell as administrator
Search AtomicRedTeam
Type
Size
Windows PowerS... 4 KB
Windows PowerS... 3 KB
PNG File 230 KB
SVG Document 112 KB
This PC
Network
4 items
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 17134.rs4_release.180410-1804
Type here to search
9:26 AM
2/13/2023
Right Ctrl

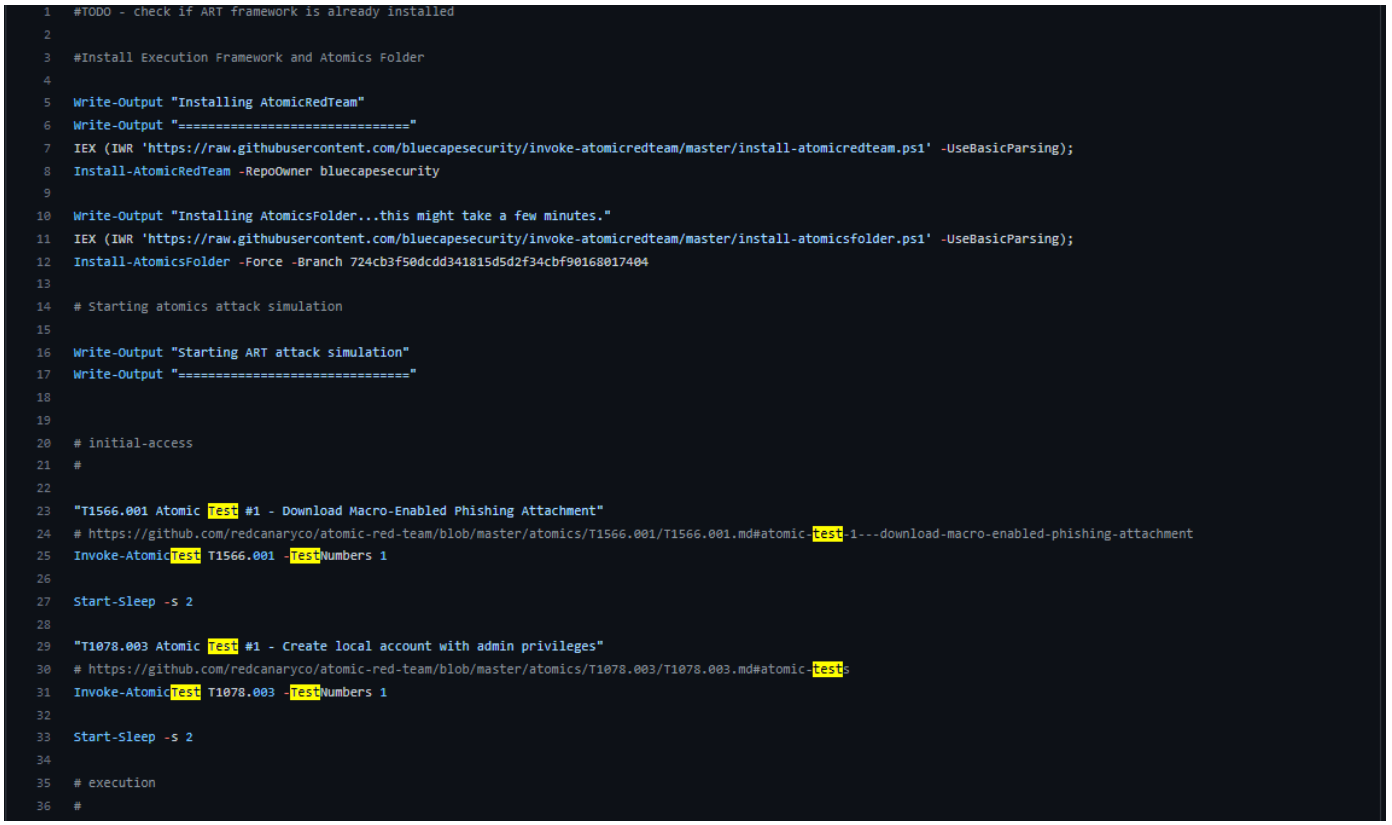

MSEdge - Win10 (Guest Additions Installed + Windows Configuration) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
PWF-main.zip
PWF-main
Administrator: Windows PowerShell
PS C:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam> .\ART-attack.ps1
Search AtomicRedTeam
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 17134.rs4_release.180410-1804
9:26 AM
2/13/2023
Right Ctrl



- There are multiple atomic tests being executed:
  - T1566.001: Phishing: Spearphishing Attachment
    - Tactic: Initial Access
  - T1078.003: Valid Accounts: Local Accounts
    - Tactic: Defense Evasion, Persistence, Privilege Escalation, Initial Access
  - T1059.001: Command and Scripting Interpreter: PowerShell
    - Tactic: Execution
  - T1547.001: Boot or Logon Autostart Execution: Registry Run Keys
    - Tactic: Persistence, Privilege Escalation
  - T1547.001: Boot or Logon Autostart Execution: Startup Folder
    - Tactic: Persistence, Privilege Escalation
  - 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:



```
#TODO - check if ART framework is already installed

#Install Execution Framework and Atomics Folder

Write-Output "Installing AtomicRedTeam"
Write-Output "==============================="
IEX (IWR 'https://raw.githubusercontent.com/bluecapesecurity/invoke-atomicredteam/master/install-atomicredteam.ps1' -UseBasicParsing);
Install-AtomicRedTeam -RepoOwner bluecapesecurity

Write-Output "Installing AtomicsFolder...this might take a few minutes."
IEX (IWR 'https://raw.githubusercontent.com/bluecapesecurity/invoke-atomicredteam/master/install-atomicsfolder.ps1' -UseBasicParsing);
Install-AtomicsFolder -Force -Branch 724cb3f50dcdd341815d5d2f34cbf90168017404

# Starting atomics attack simulation

Write-Output "Starting ART attack simulation"
Write-Output "==============================="


# initial-access
#

"T1566.001 Atomic Test #1 - Download Macro-Enabled Phishing Attachment"
# https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1566.001/T1566.001.md#atomic-test-1---download-macro-enabled-phishing-attachment
Invoke-AtomicTest T1566.001 -TestNumbers 1

Start-Sleep -s 2

"T1078.003 Atomic Test #1 - Create local account with admin privileges"
# https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1078.003/T1078.003.md#atomic-tests
Invoke-AtomicTest T1078.003 -TestNumbers 1

Start-Sleep -s 2

# execution
#
```

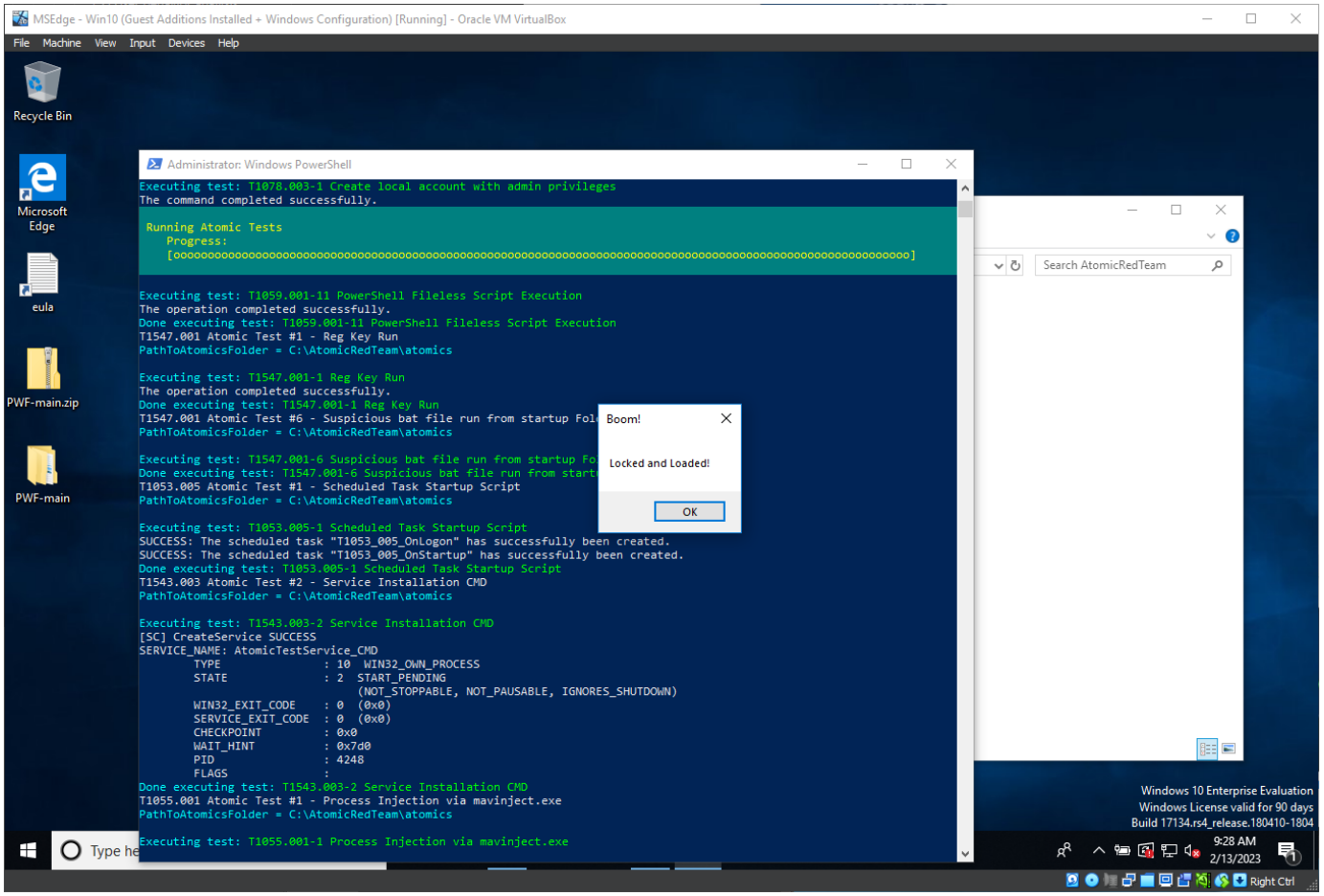
- You can go to: https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/, and use another techniques, just for learning purposes, for example for initial-access, execution, persistence, defense-evasion, etc.

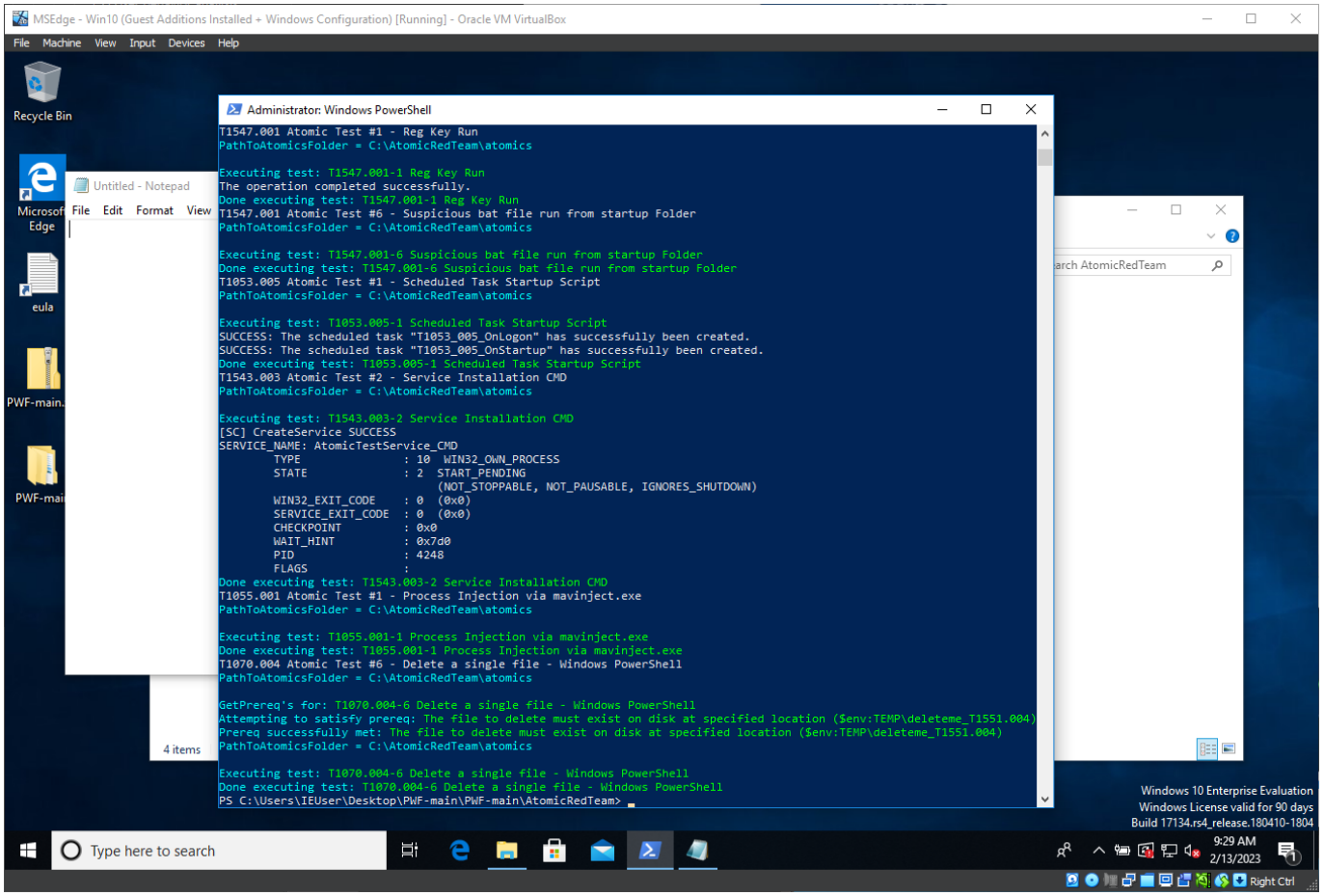
- The script used just some techniques. Based on https://attack.mitre.org/techniques/enterprise/, techniques represent 'how' an adversary achieves a tactical goal by performing an action. You can see the MITRE ATT&CK Matrix here: https://attack.mitre.org/matrices/enterprise/. According to https://www.blackberry.com/us/en/solutions/endpoint-security/mitre-attack/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

- Both MITRE ATT&CK and Cyber Kill Chain are frameworks to address cyberattacks agains 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.

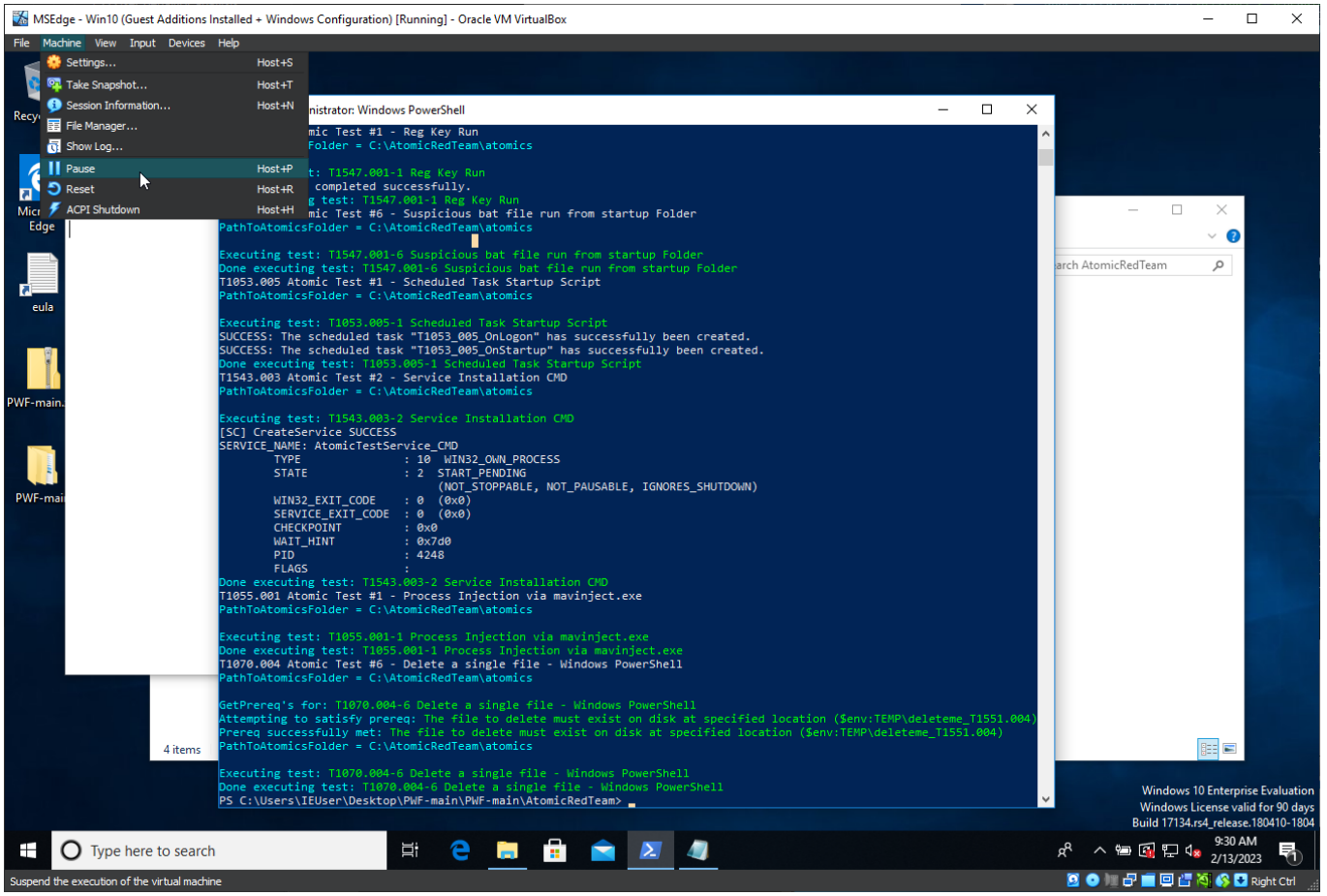
- Important, do not close notepad, just press ok on the prompt:

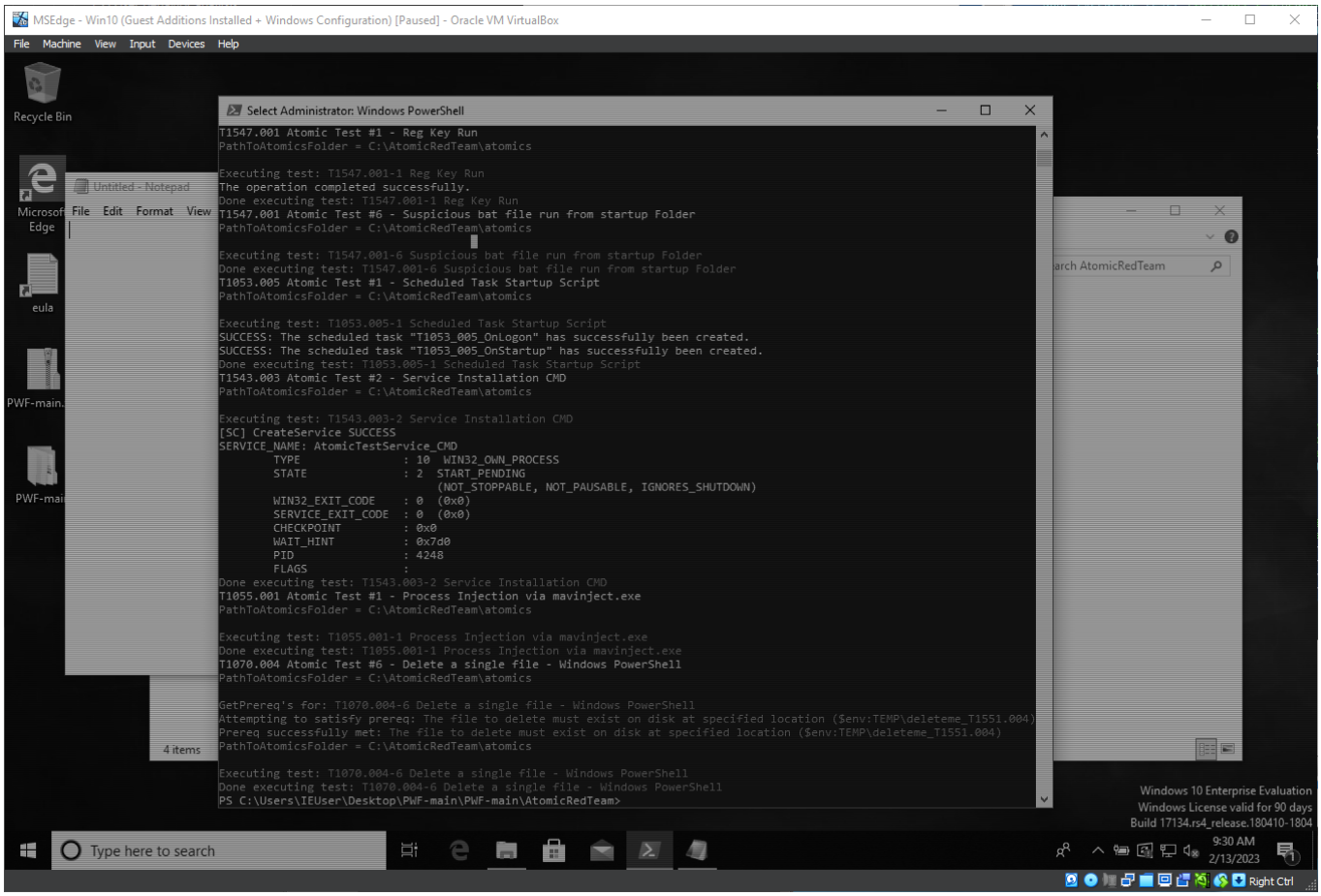




- Timeline of the cyber attack:
  - 9:26-27AM 2/13/2023
  - 9:29-30AM 2/13/2023

- 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
Settings... Host+S
Take Snapshot... Host+T
Session Information... Host+N
File Manager...
Show Log...
Pause Host+P
Reset Host+R
ACPI Shutdown Host+H
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
T1543.003 Atomic Test #2 - Service Installation CMD
PathToAtomicsFolder = C:\AtomicRedTeam\atomics
Executing test: T1543.003-2 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: T1543.003-2 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>
4 items
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 17134.rs4_release.180410-1804
Type here to search
9:30 AM
2/13/2023
Suspend the execution of the virtual machine
Right Ctrl


MSEdge - Win10 (Guest Additions Installed + Windows Configuration) [Paused] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Select Administrator: Windows PowerShell
Untitled - Notepad
File Edit Format View
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
T1543.003 Atomic Test #2 - Service Installation CMD
PathToAtomicsFolder = C:\AtomicRedTeam\atomics
Executing test: T1543.003-2 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: T1543.003-2 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>
4 items
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 17134.rs4_release.180410-1804
Type here to search
9:30 AM
2/13/2023
Right Ctrl