Configuration Manual

Enhancing Virtualization Security in Oracle VirtualBox: Investigating VM Escape Vulnerabilities and Mitigations

MSc Research Project
Programme Name

Joshua Chakko Jacob
Student ID: 21124701

School of Computing
National College of Ireland

Supervisor: Joel Aleburu

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Joshua Chakko Jacob

Student ID: 21124701

Programme: MSc Cybersecurity **Year:** 2023

Module: Research Project

Lecturer: ……………………………………………………………………………………………

Submission Due Date: 16-09-2023 ……………………………………………………………………………………………

Project Title: Enhancing Virtualization Security in Oracle VirtualBox: Investigating VM Escape Vulnerabilities and Mitigations

Word Count: 1279 **Page Count:** 8

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……………Joshua Jacob……………………………………………………………………

Date: 14-08-2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	■
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	■
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	■

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

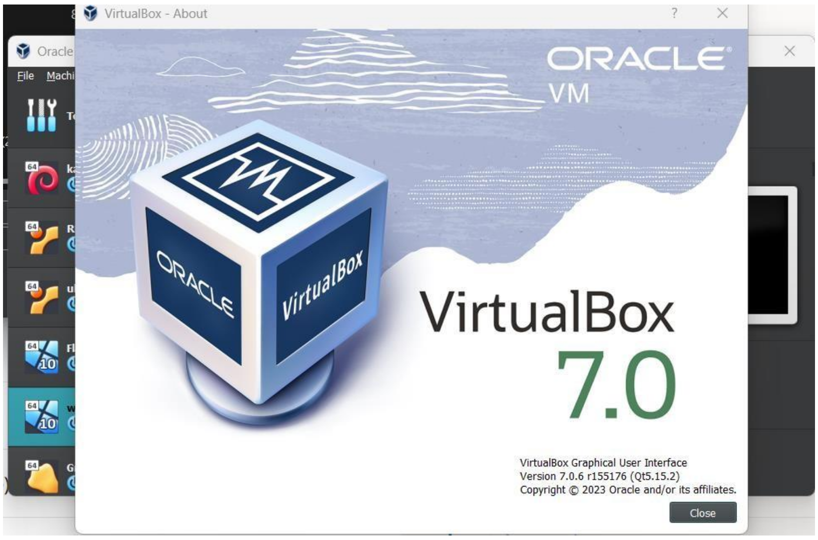
Configuration Manual

Joshua Chakko Jacob
Student ID: 21124701

1 Exploration of the default configuration of the Oracle VirtualBox Hypervisor

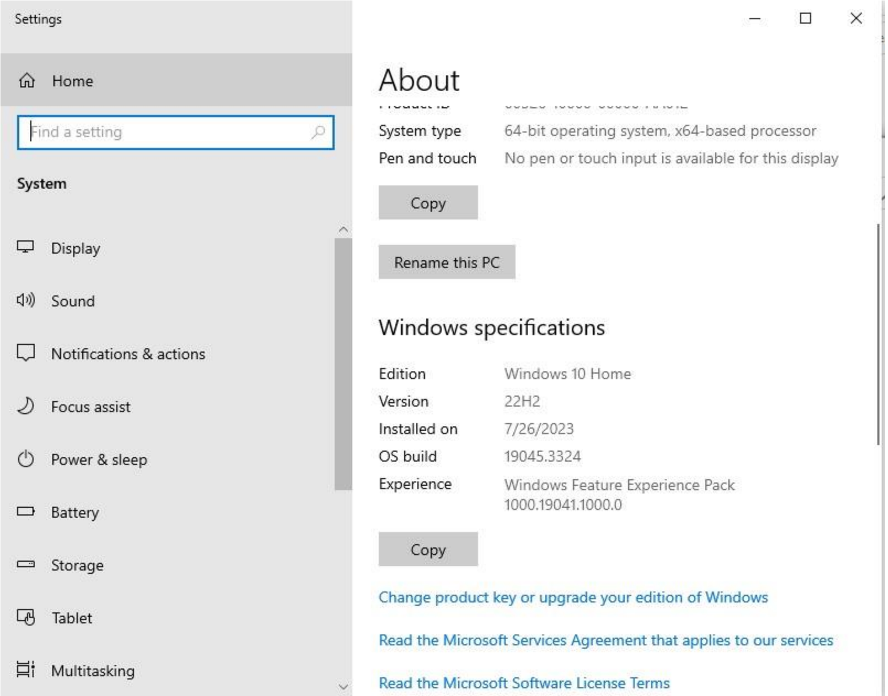
This section focuses on the exploration of the default configuration and the review of the Hypervisor and the Host OS. Default installation of the Oracle VirtualBox with no modification of the path or custom installation was setup.
Versions setup and review details. The Windows 10 Guest VM was setup by downloading the ISO file from the Windows Media Creation Tool for Windows 10.

Software	**Version**	**Configuration Setting**
Oracle VirtualBox	VirtualBox7.0, Version 7.0.6 r155176(*Oracle VM VirtualBox 7.0.10 is now generally available!*, no date)	default
Guest VM – OS - Windows 10 Home	Version 22H2, Build 19045.3324	default
PowerShell	Version 5.1.22621.1778	default
Host OS – Windows 11 Pro	Version 22H2, Build 22621.2070	default



VirtualBox Graphical User Interface
Version 7.0.6 r155176 (Qt5.15.2)
Copyright © 2023 Oracle and/or its affiliates.

Fig.1 Oracle Virtual Box Version



About

System type 64-bit operating system, x64-based processor
Pen and touch No pen or touch input is available for this display

Windows specifications

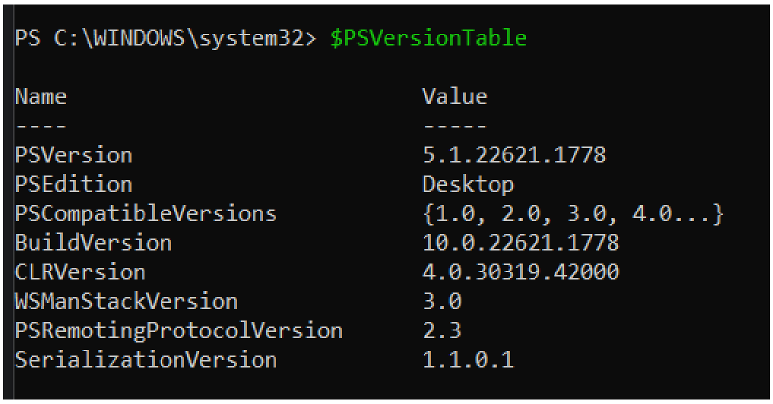
Edition Windows 10 Home
Version 22H2
Installed on 7/26/2023
OS build 19045.3324
Experience Windows Feature Experience Pack 1000.19041.1000.0

Change product key or upgrade your edition of Windows

Read the Microsoft Services Agreement that applies to our services

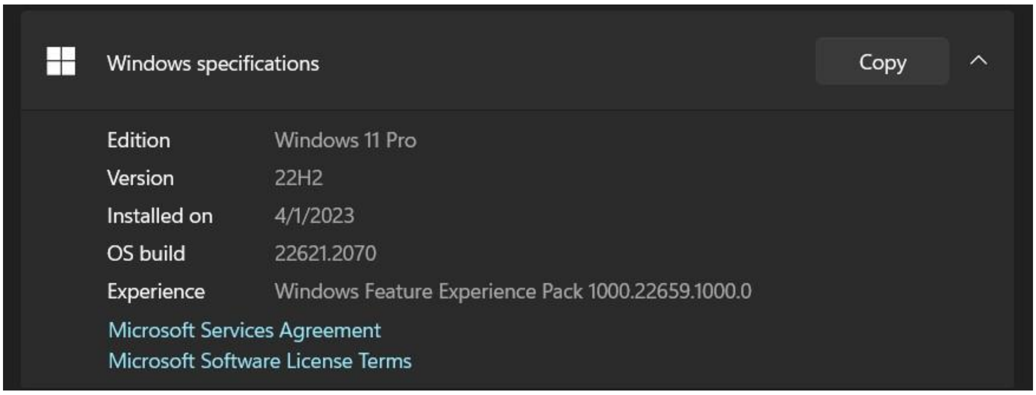
Read the Microsoft Software License Terms

Fig.2 Windows 10 Guest OS Virtual Machine Version Details



```
PS C:\WINDOWS\system32> $PSVersionTable

Name                           Value
----                           -----
PSVersion                      5.1.22621.1778
PSEdition                      Desktop
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.22621.1778
CLRVersion                     4.0.30319.42000
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1
```

Fig.3 PowerShell on Host OS Windows 11



Windows specifications

Edition Windows 11 Pro
Version 22H2
Installed on 4/1/2023
OS build 22621.2070
Experience Windows Feature Experience Pack 1000.22659.1000.0

Microsoft Services Agreement
Microsoft Software License Terms

Fig.4 Host OS – Windows 11 Pro

Whilst exploring, the default method to map the shared folder to the Virtual Machine was

1. Devices>shared folders>shared folder settings

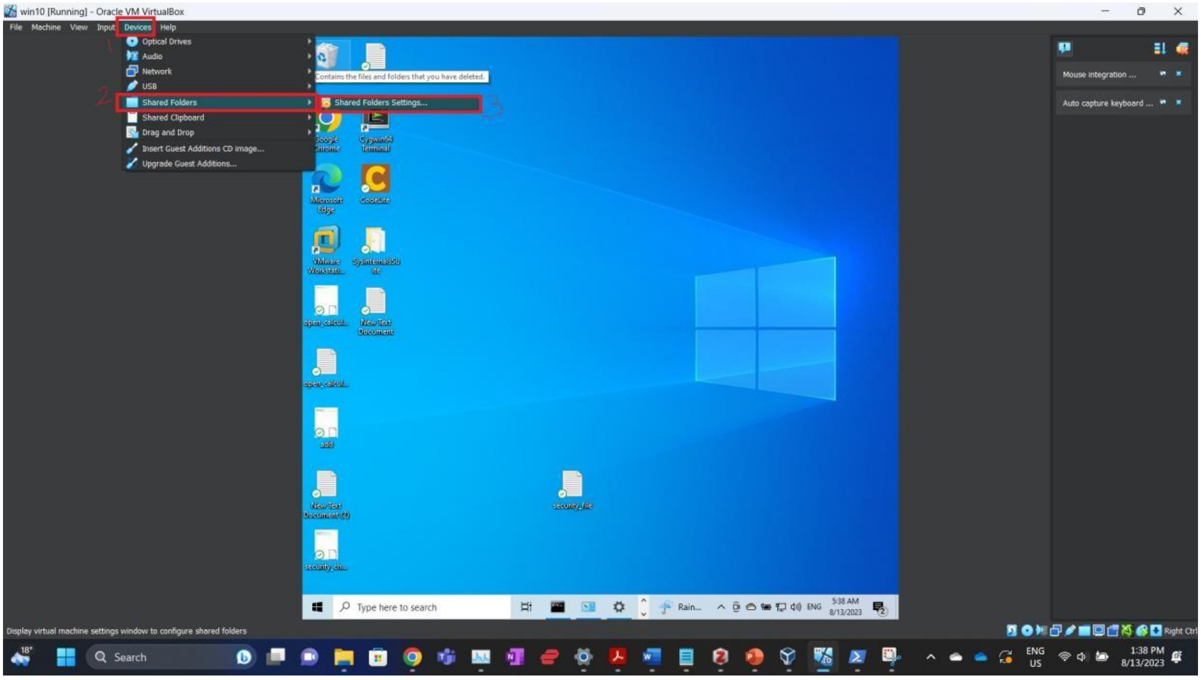
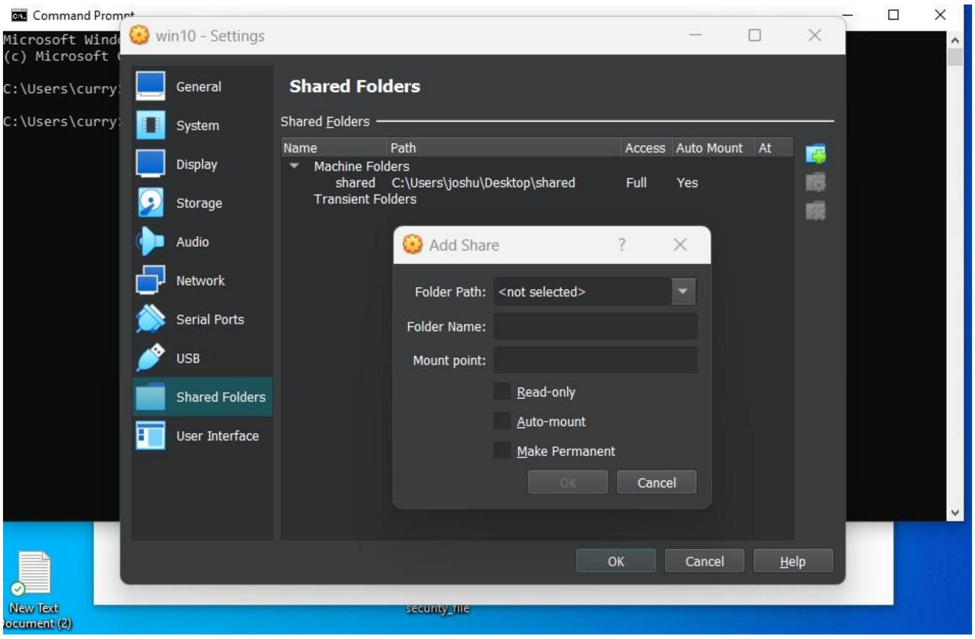

win10 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
1
Optical Drives
Audio
Network
USB
2
Shared Folders
Shared Clipboard
Drag and Drop
Insert Guest Additions CD image...
Upgrade Guest Additions...
Shared Folders Settings...
3
Contains the files and folders that you have deleted.
Mouse integration ...
Auto capture keyboard ...
Type here to search
Display virtual machine settings window to configure shared folders
Search
Right Ctrl

Fig.5 Shared Folder Settings Path on the Guest VM VirtualBox Settings

Once that is opened, the available options to only map the shared folder is available as seen in Fig.6. There is no control to specify the access controls of the file as probably it is not possible to do so as the shared folder is created on the Host OS Desktop, but in reality there should be some level security measures required to ensure that no form of communication should take place via this shared folder. However if we see in Fig.6, it can be seen that there is an option to make it only read only, but when this option is enabled, nothing can be done to access these files, which is redundant in the case of using a shared folder in the first place. This is because the intention for a shared folder is to ensure that there is some form of access between the two Operating systems accessible to the shared folder.



Shared Folders

Shared Folders

Name	Path	Access	Auto Mount	At
Machine Folders				
shared	C:\Users\joshu\Desktop\shared	Full	Yes	
Transient Folders				

Folder Path: <not selected>

Folder Name:

Mount point:

□ Read-only

□ Auto-mount

□ Make Permanent

Fig.6 Shared Folder Setting available option.

2 Project Setup

Upon exploring the default configuration of the hypervisor and identifying the lack of security controls for the shared folder, a shared folder has been created on the HOST OS – Desktop titled as “shared”

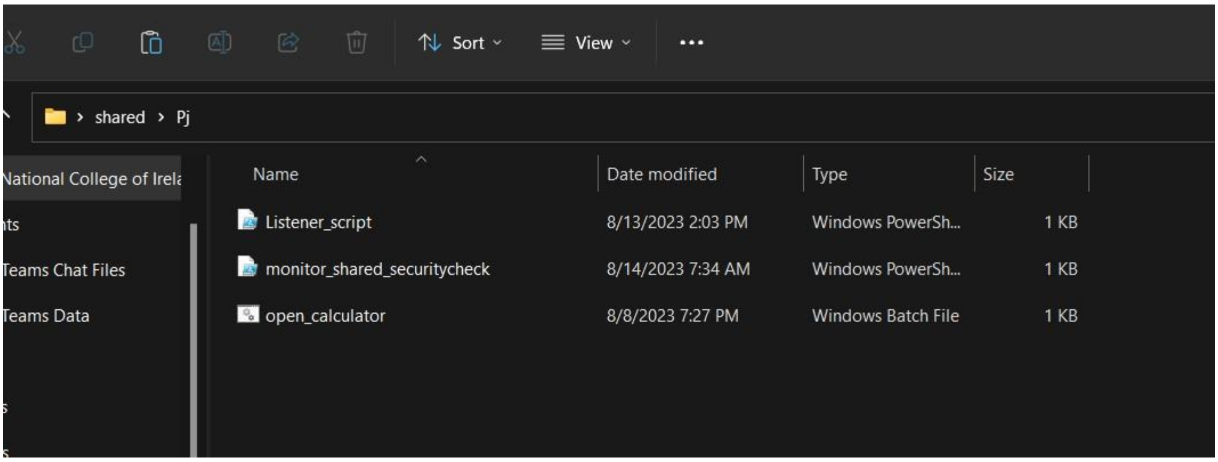
The location of this file as is on the Host OS is - ***C:\Users\joshu\Desktop\shared***

Within this shared folder, another folder was created which is titled as Pj - ***C:\Users\joshu\Desktop\shared\Pj***

Once this has been created, by following the mapping of the shared drive settings as seen in Fig.5 and Fig.6, the “shared” shared folder has been mapped to the specific Windows 10 Guest VM. This can be seen as below from the Guest OS.

On the Gues OS the location of the shared folder is on the Z Drive as seen in Fig.7

Z:\Pj



Name	Date modified	Type	Size
Listener_script	8/13/2023 2:03 PM	Windows PowerSh...	1 KB
monitor_shared_securitycheck	8/14/2023 7:34 AM	Windows PowerSh...	1 KB
open_calculator	8/8/2023 7:27 PM	Windows Batch File	1 KB

Fig.7 Shared folder on Guest OS VM

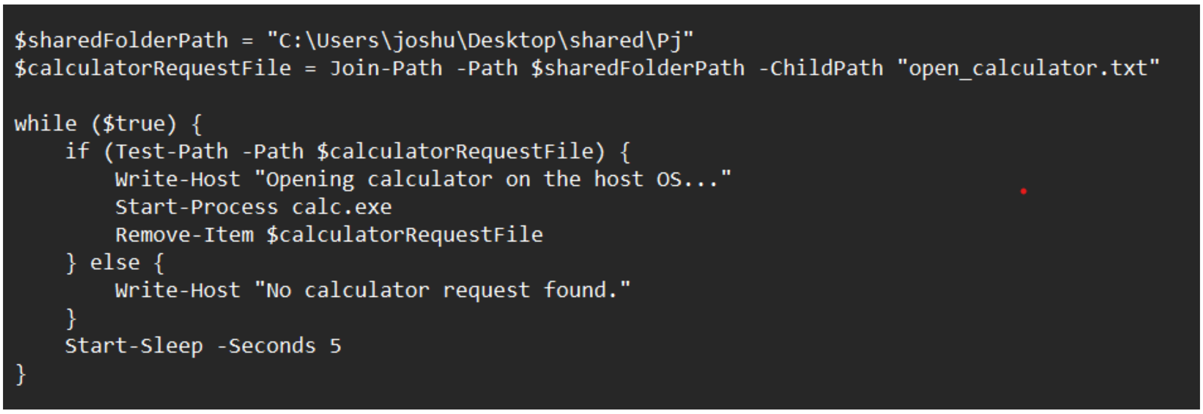
Scripts

Script 1 : Host Side : Listener script

Type of Script : PowerShell

Brief on the actions of the script.

The first script is to just check for the presence of a file, titled as “open_calculator.txt”, this can be considered as the trigger file that is generated by the Guest OS VM Batch script. Once when this file is generated the host listener script checks for the presence of this file and then executes the commands to open the calculator application. The code contents are displayed as shown in Fig.8.



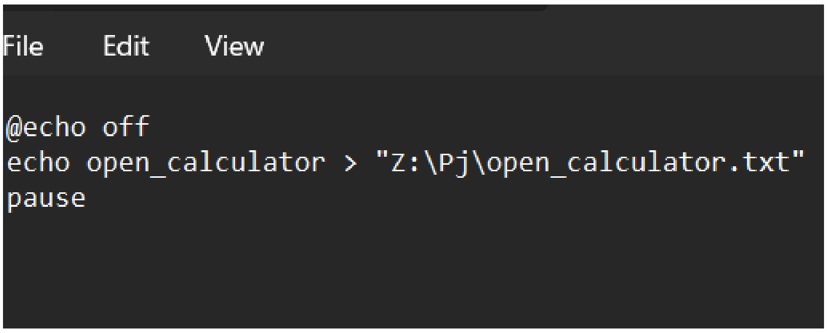
```
$sharedFolderPath = "C:\Users\joshu\Desktop\shared\Pj"
$calculatorRequestFile = Join-Path -Path $sharedFolderPath -ChildPath "open_calculator.txt"

while ($true) {
    if (Test-Path -Path $calculatorRequestFile) {
        Write-Host "Opening calculator on the host OS..."
        Start-Process calc.exe
        Remove-Item $calculatorRequestFile
    } else {
        Write-Host "No calculator request found."
    }
    Start-Sleep -Seconds 5
}
```

Fig.8 PS Script to open the calculator app on the Host OS

As we can see in line 2, the *calculatorrequestfile* is responsible for checking the presence of the calculator request file if at all it is present I the shared folder.

Executing the batch script from the Guest VM

Script 2 : Guest Side : Code Execution Script – Open calculator app on Host OS Script



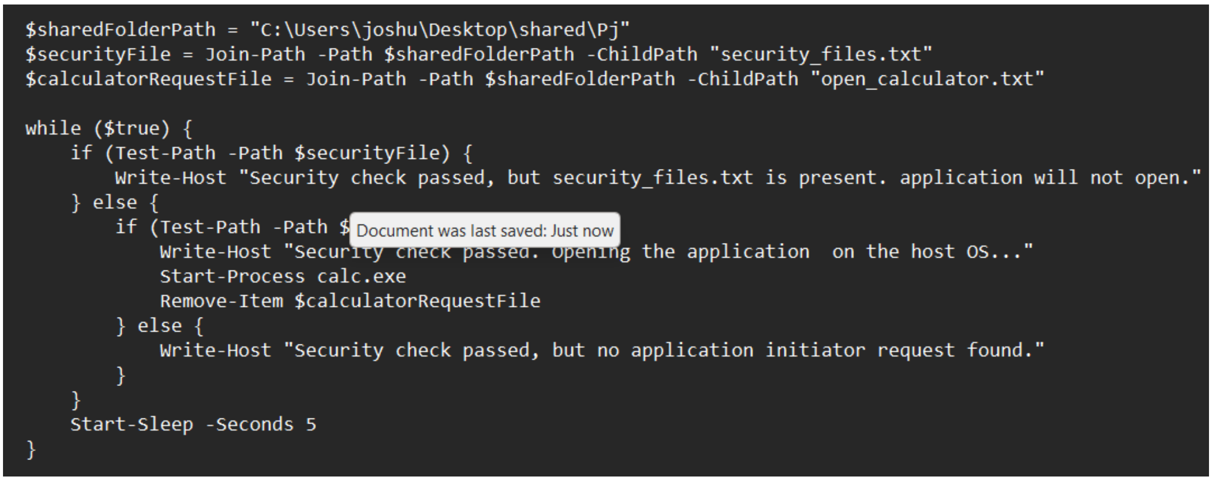
```
@echo off
echo open_calculator > "Z:\Pj\open_calculator.txt"
pause
```

Fig. 9 Contents of the Guest OS batch Script

The batch script to echo the status of open calculator and also to write the creation of the open_calculator.txt file. This is the text file that acts as the trigger to open the calculator application on the HOST OS.

Script 3 : Modified security check Listener script on the Host side

This script is similar ot the Script 1 but with an addition of a logic to include a security check wherein, in the presence of a specific file, in this case “security_files.txt” which in this case is just an empty file, but as we see in the code content below the logic check for this is to check if such a file exists or not. If it does exists, then the code to open the calc.exe should not run, else the code gets through.



```
$sharedFolderPath = "C:\Users\joshu\Desktop\shared\Pj"
$securityFile = Join-Path -Path $sharedFolderPath -ChildPath "security_files.txt"
$calculatorRequestFile = Join-Path -Path $sharedFolderPath -ChildPath "open_calculator.txt"

while ($true) {
    if (Test-Path -Path $securityFile) {
        Write-Host "Security check passed, but security_files.txt is present. application will not open."
    } else {
        if (Test-Path -Path $ Document was last saved: Just now
            Write-Host "Security check passed. Opening the application  on the host OS..."
            Start-Process calc.exe
            Remove-Item $calculatorRequestFile
        } else {
            Write-Host "Security check passed, but no application initiator request found."
        }
    }
    Start-Sleep -Seconds 5
}
```

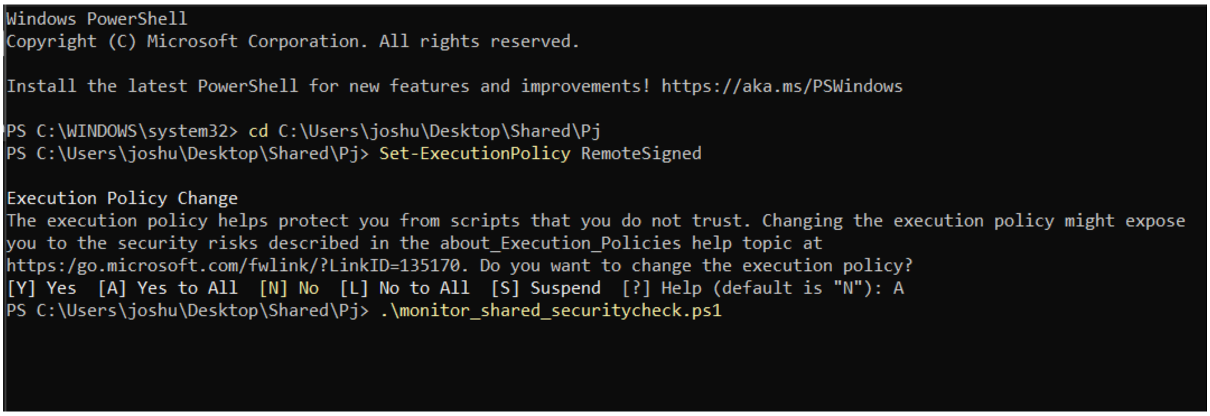
Fig.10 Security embedded listener script

3 Order of Execution

1. The listener_monitor.ps1 script on the host OS should first be executed via the PowerShell cmd. PowerShell has to be executed as an administrator, the directory should be changed to the shared folder on the desktop and by .\listener_monitor.ps1 the PowerShell script now continuously monitors the shared folder.
   Once the "open_calculator.txt" file is detected, the script triggers the execution of the desired application which in this case is the calculator application.

   PowerShell script Execution

   Run PS as administrator > Change the directory location to that of the shared folder > execute this command "Set-Execution Policy RemoteSigned" to execute custom commands via PS. And then we run the scripts as seen below.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> cd C:\Users\joshu\Desktop\Shared\Pj
PS C:\Users\joshu\Desktop\Shared\Pj> Set-ExecutionPolicy RemoteSigned

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): A
PS C:\Users\joshu\Desktop\Shared\Pj> .\monitor_shared_securitycheck.ps1
```

   Fig. 11 Order of Execution in the PS

2. **Execute the Batch Script on the guest OS by double clicking the .bat file:**

   On the guest OS, create a batch script named "generate_request.bat."
   This script is responsible for generating the "open_calculator.txt" file in the shared folder.

Creating the Request:

Within the "generate_request.bat" script, include code to create the "open_calculator.txt" file in the shared folder.

The presence of this file will serve as a request to trigger an action on the host OS. Executing the Request:

Observe the host OS to verify that the specified application (calculator) is launched. This demonstrates the successful interaction between the guest and host OS via the shared folder.

3. The secure_listener_monitor.ps1 script on the host OS should then be executed via the PowerShell cmd. PowerShell has to be executed as an administrator, the directory should be changed to the shared folder on the desktop and by .\secure_listener_monitor.ps1 the PowerShell script now continuously monitors the shared folder, but this time since it has an additional security check to ensure that there is a security_files.txt file and reject the interaction in terms of opening the calculator application.

   This ensures that, by ensuring the presence of a certificate, no communication can take place on the Host OS.

References

Oracle VM VirtualBox 7.0.10 is now generally available! (no date). Available at: https://blogs.oracle.com/virtualization/post/oracle-vm-virtualbox-7010-is-now-available (Accessed: 13 August 2023).