SALMAC

Security Audit System

Rewrite Version 0.0.1

By

Mohammad Zakaria Alam

M00838940

And

Nikhil Bhat

M00845976

As part of

CST 4550 Penetration Testing and Digital Forensic

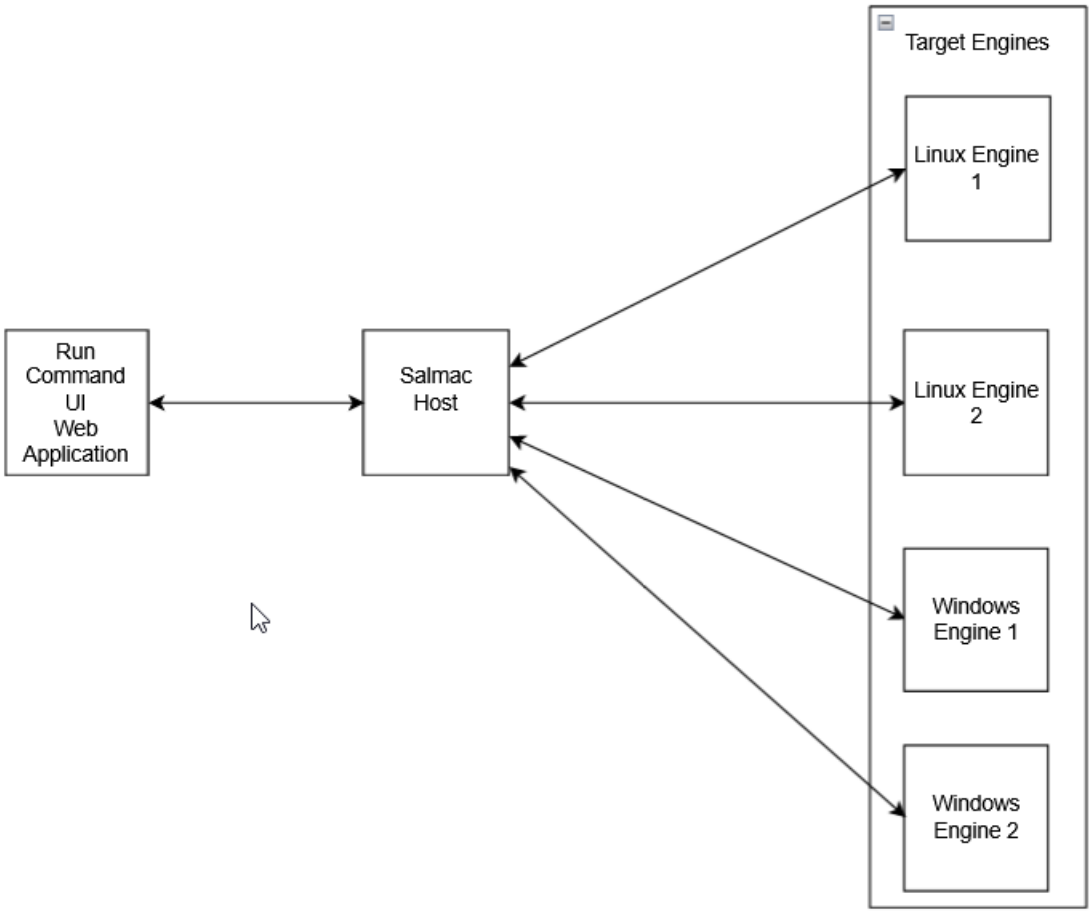
Under the supervision of

Dr Mahdi Aiash

School of Science and Technology

Middlesex University London

The Architecture:



So, we have basically Three stakeholders in our current Salmac.

1. Host Application: developed in Java
2. Target Engine Application: developed in Java
3. UI application: developed in ReactJS

UI web app communicate with Host application for everything.

When a Target Engine application gets alive it connected automatically with Host Application.

Target engines are orchestrated by the Host machine.

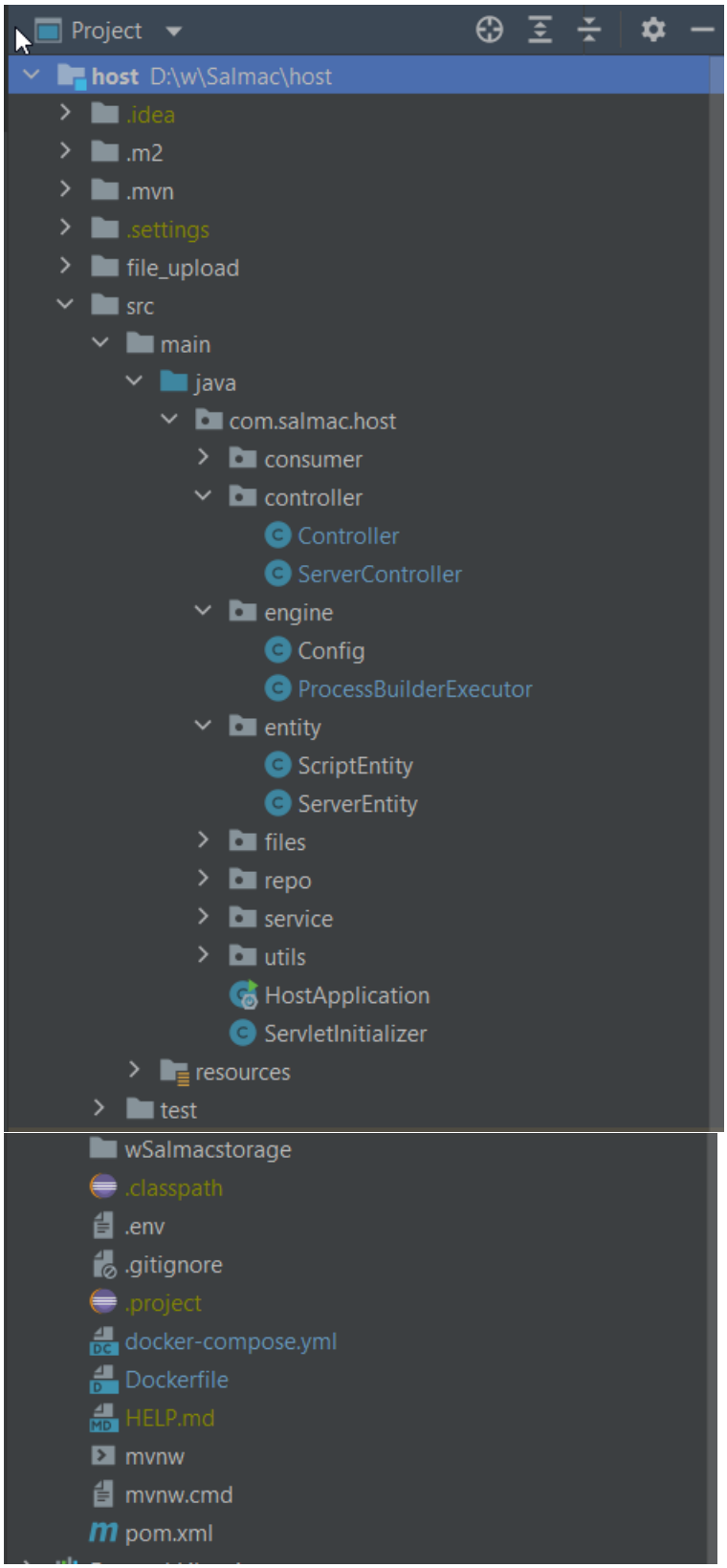
So, if we send any command for a Target Engines from the UI, it first goes to Host machine then Host machine send that to expected Target Engine. So, we are safeguarding our target engines from the UI with is accessible from world wide web.

Containerization has been implemented using Docker

Two script files have been attached too for test purpose.

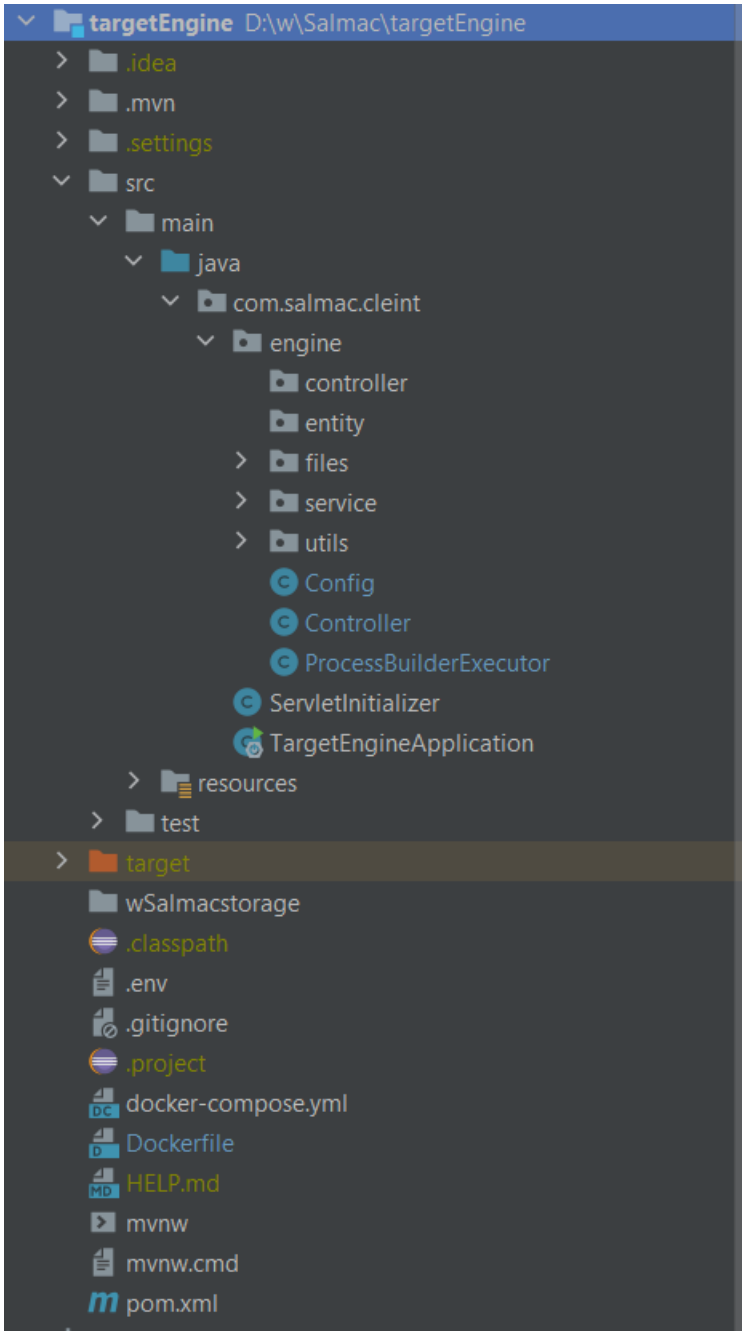
Project Structure of Host application:

Developed in Spring Boot. So, this is the standard project structure.



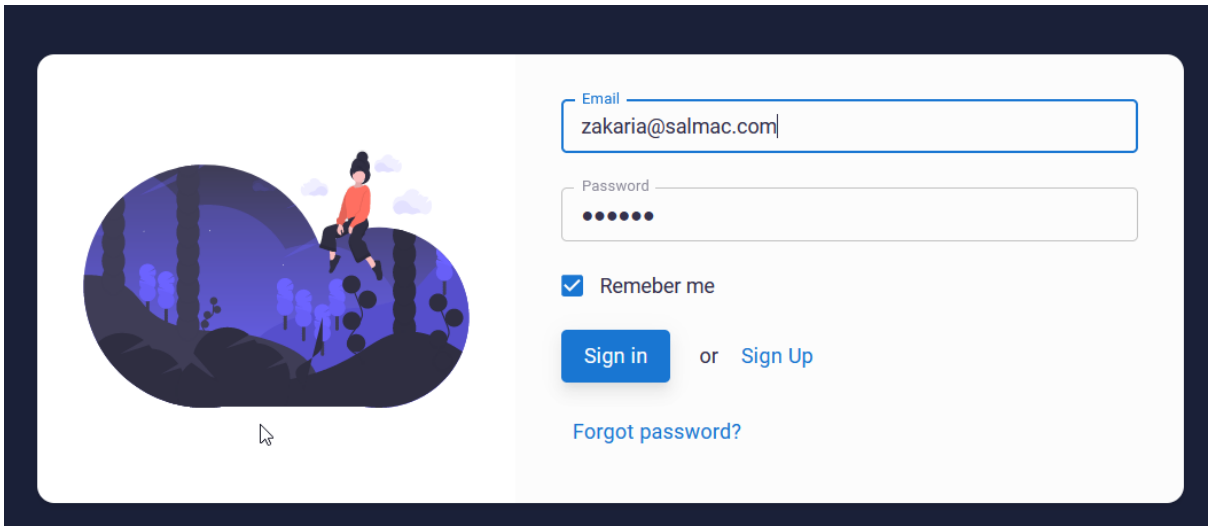
Project Structure for Target Engine:

Developed in Spring Boot. So, this is the standard project structure.

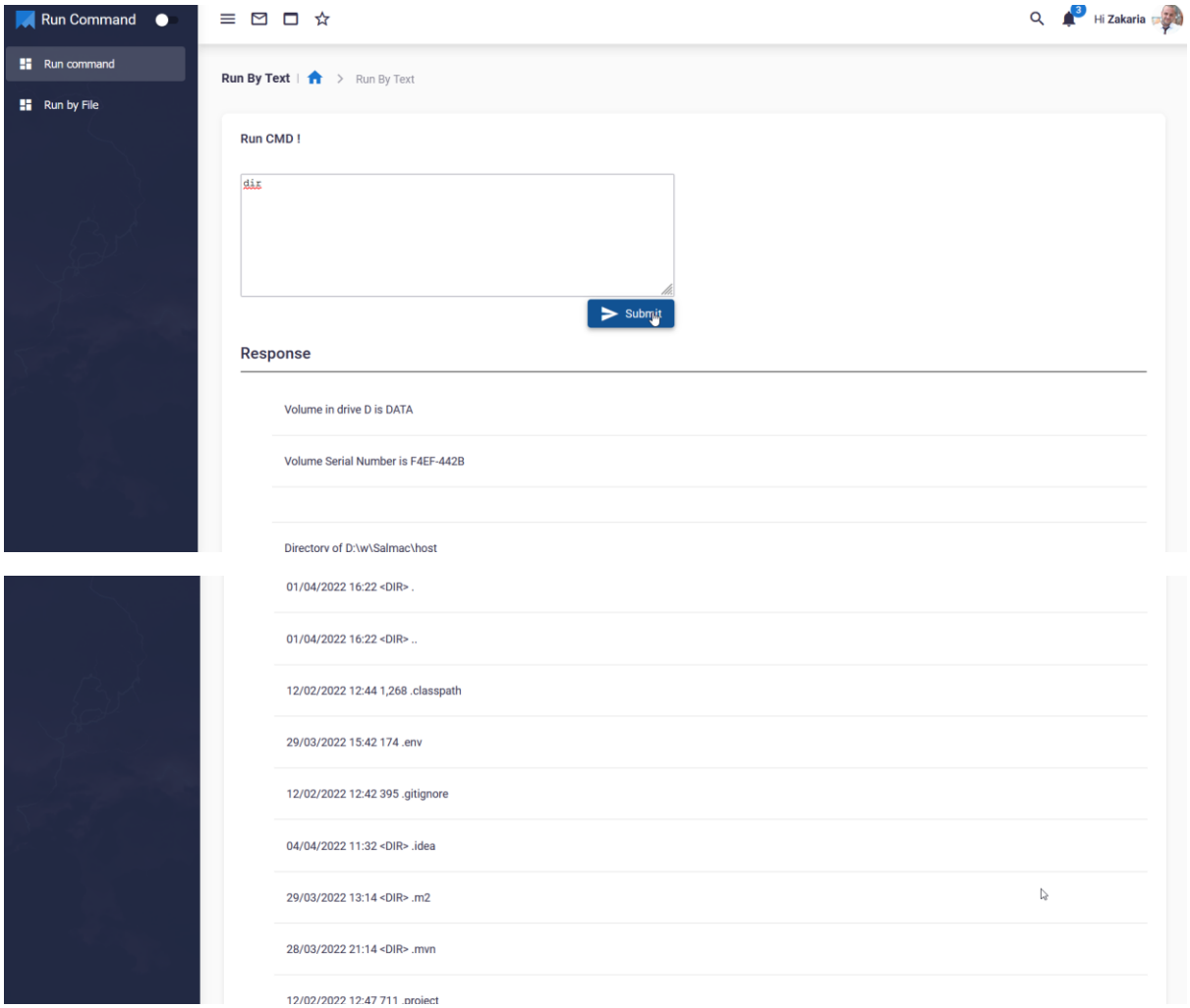


Current UI:

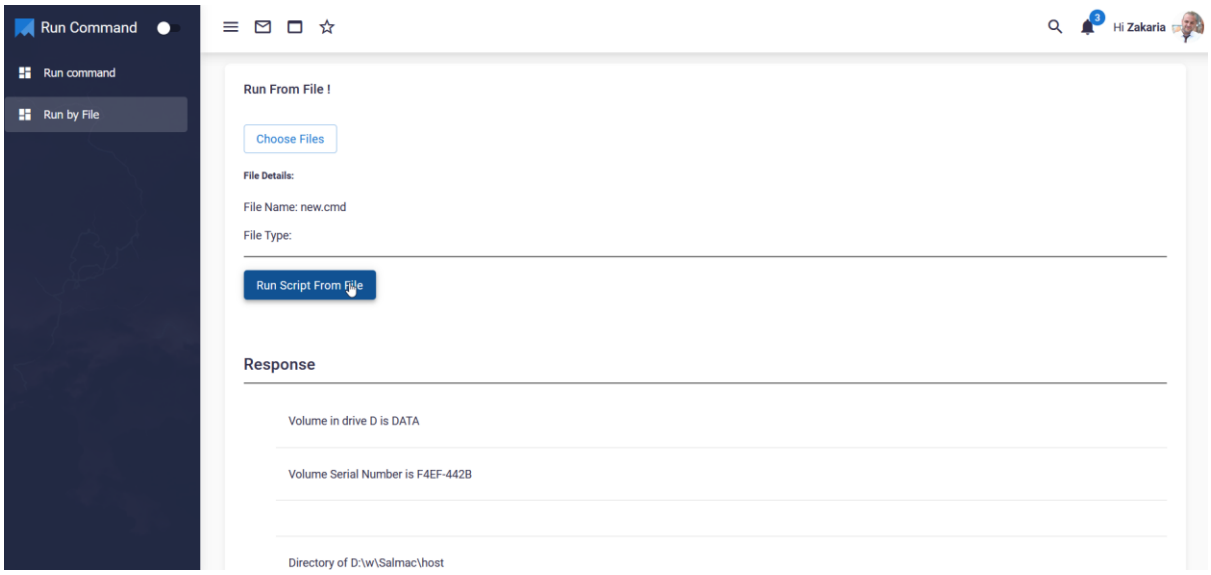
Login



Run command similar to Terminal or Command Promt



Run a script file:



Scripts for Test:

Firewall.cmd

```
:: ECHO OFF
@echo off
SETLOCAL
:: CALLING Firewall function
CALL :Firewall %~1
EXIT /B %ERRORLEVEL%

:: Firewall function definition
:Firewall

:: Initializing Variables
SET /A show = 2
SET /A on = 1
SET /A off = 0


:: Setting messages before actions
if %show%==%~1 echo " FIREWALL SCRIPT: SHOWING ALL PROFILES "
if %on%==%~1 echo " FIREWALL SCRIPT: TURNING ALL PROFILES ON "
if %off%==%~1 echo " FIREWALL SCRIPT: TURNING ALL PROFILES OFF "

:: Action performing
if %show%==%~1 netsh advfirewall show allprofiles
if %on%==%~1 netsh advfirewall set allprofiles state on
if %off%==%~1 netsh advfirewall set allprofiles state off

:: holding output
SET /p wait = "PRESS ANY KEY TO EXIT"

EXIT /B 0
```

This batch script is written in PowerShell to check the status of the firewall for the desired system and to enable and disable it whenever required.

This is implemented with the help of UI using few constant values given as input to perform specific action on the firewall of the system. These inputs are:

2 **show all firewall profiles**
0 **turn off all firewall profiles**
1 **turn on all firewall profiles**

We have function were based on the input from UI (0,1,2) respective message will be printed showing the status of the firewall. We have used netsh commands to perform the action based on the input received.

Why netsh?

Network shell (netsh) is a command-line utility that allows you to configure and display the status of various network communications server roles and components after they are installed on computers running Windows Server. Netsh commands can be run by typing commands at the netsh prompt and they can be used in batch files or scripts. Remote computers and the local computer can be configured by using netsh commands.

Below mentioned are the netsh commands used to handle the firewall in the windows:

- netsh advfirewall show allprofiles
- netsh advfirewall set allprofiles state on
- netsh advfirewall set allprofiles state off

Screenshot showing the steps to disable or enable the firewalls in windows system.

1. Option 2, shows status of all the firewall profiles in the system.

```
Administrator: Command Prompt - firewall.cmd 2
Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>f:

F:\>cd test

F:\test>firewall.cmd 2
" FIREWALL SCRIPT: SHOWING ALL PROFILES "

Domain Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096


Private Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096
```

```
Public Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Ok.
```

2. Option 0, Disable's all the profiles of the firewall, to check and confirm we can re-enter option 2 in cmd to check whether the profiles have been disabled or not.

```
Administrator: Command Prompt - firewall.cmd 2
F:\test>firewall.cmd 0
" FIREWALL SCRIPT: TURNING ALL PROFILES OFF "
Ok.

PRESS CLICK ENTER KEY

F:\test>firewall.cmd 2
" FIREWALL SCRIPT: SHOWING ALL PROFILES "

Domain Profile Settings:
----------------------------------------------------------------------
State                                 OFF
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Private Profile Settings:
----------------------------------------------------------------------
State                                 OFF
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Public Profile Settings:
----------------------------------------------------------------------
State                                 OFF
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Ok.
```

3. Option 1 , enables all the firewalls , which can be confirmed using option 2.

```
Administrator: Command Prompt - firewall.cmd 2
F:\test>firewall.cmd 1
" FIREWALL SCRIPT: TURNING ALL PROFILES ON "
Ok.

PRESS CLICK ENTER KEY

F:\test>firewall.cmd 2
" FIREWALL SCRIPT: SHOWING ALL PROFILES "

Domain Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Private Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096
```

```
Public Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Ok.
```

Screenshot for Private profile

```
@echo off



SETLOCAL
:: CALLING Firewall function
CALL :Firewall %~1
EXIT /B %ERRORLEVEL%

:: Firewall function definition
:Firewall

:: Initializing Variables
SET /A show = 2
SET /A currentOn=3
Set /A currentOff=4

:: Setting messages before actions
if %show%==%~1 echo " FIREWALL SCRIPT: SHOWING STATUS OF PRIVATE PROFILES "
if %currentOn%==%~1 echo " FIREWALL SCRIPT: TURNING PRIVATE PROFILES ON "
if %currentOff%==%~1 echo " FIREWALL SCRIPT: TURNING PRIVATE PROFILES OFF "

:: Action performing
if %show%==%~1 netsh advfirewall show currentprofile
if %currentOn%==%~1 netsh advfirewall set currentprofile state on
if %currentOff%==%~1 netsh advfirewall set currentprofile state off

:: holding output
SET /p wait = "PRESS or CLICK ENTER KEY"

EXIT /B 0
```

4. If we need to only change/update status of private/current firewall if required then we have implanted another scripts using netsh commands, which will enable, disable and show the status.

```
Administrator: Command Prompt - firewall_Additional.cmd currentOn - firewall_Additional.cmd currentOn - firewall_Additional.cmd currentOn - firewall
F:\test>PrivateFirewall_Script.cmd 2
" FIREWALL SCRIPT: SHOWING STATUS OF PRIVATE PROFILES "

Private Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Ok.
```

```
Administrator: Command Prompt - firewall_Additional.cmd currentOn - firewall_Additional.cmd currentOn - firewall_Additional.cmd cur
F:\test>PrivateFirewall_Script.cmd 4
" FIREWALL SCRIPT: TURNING PRIVATE PROFILES OFF "
Ok.

PRESS or CLICK ENTER KEY

F:\test>PrivateFirewall_Script.cmd 2
" FIREWALL SCRIPT: SHOWING STATUS OF PRIVATE PROFILES "

Private Profile Settings:
----------------------------------------------------------------------
State                                 OFF
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Ok.
```

```
Administrator: Command Prompt - firewall_Additional.cmd currentOn - firewall_Additional.cmd currentOn - firewall_Additional.cmd currentO
F:\test>PrivateFirewall_Script.cmd 3
" FIREWALL SCRIPT: TURNING PRIVATE PROFILES ON "
Ok.

PRESS or CLICK ENTER KEY

F:\test>PrivateFirewall_Script.cmd 2
" FIREWALL SCRIPT: SHOWING STATUS OF PRIVATE PROFILES "

Private Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Ok.

PRESS or CLICK ENTER KEY
```