Secure Coding Lab – 4

Fareena Sk

18BCE7094

Slot: L39+40

Finding Files

```
C:\>where /R C: \ PDFReaderSetup.exe
C:\Btech pdf\SecureCoding_Lab\Lab2\PDFReaderSetup.exe
```

Scheduled tasks

```
C:\Btech pdf\SecureCoding_Lab\Lab3>schtasks

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Adobe Flash Player NPAPI Notifier        06-Mar-21 6:02:00 AM   Ready
App Explorer                             N/A                    Running
LenovoUtility Task                       N/A                    Ready
McAfeeLogon                              N/A                    Ready
NvDriverUpdateCheckDaily_{B2FE1952-0186- 04-Mar-21 12:25:57 PM  Ready
NVIDIA GeForce Experience SelfUpdate_{B2 N/A                    Ready
NvNodeLauncher_{B2FE1952-0186-46C3-BAEC- N/A                    Ready
NvProfileUpdaterDaily_{B2FE1952-0186-46C 04-Mar-21 12:25:56 PM  Ready
NvProfileUpdaterOnLogon_{B2FE1952-0186-4 N/A                    Ready
NvTmMon_{B2FE1952-0186-46C3-BAEC-A80AA35 N/A                    Ready
NvTmRepOnLogon_{B2FE1952-0186-46C3-BAEC- N/A                    Ready
NvTmRep_{B2FE1952-0186-46C3-BAEC-A80AA35 04-Mar-21 12:25:57 PM  Ready
OneDrive Standalone Update Task-S-1-5-21 04-Mar-21 5:38:33 PM   Ready
RtHDVBg_Dolby                            N/A                    Running
RtHDVBg_LENOVO_DOLBYDRAGON               N/A                    Running
RTKCPL                                   N/A                    Ready
User_Feed_Synchronization-{CDE355A9-06C4 04-Mar-21 4:35:13 AM   Ready

Folder: \Agent Activation Runtime
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
S-1-5-21-2120435217-1201098145-243260754 N/A                    Ready

Folder: \Lenovo
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Lenovo\ImController
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Lenovo\Lenovo Service Bridge
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
S-1-5-21-2120435217-1201098145-243260754 N/A                    Ready
```

```
Folder: \Lenovo\Vantage
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Office
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Office Automatic Updates 2.0             04-Mar-21 8:42:33 AM   Ready
Office ClickToRun Service Monitor        04-Mar-21 6:08:15 AM   Ready
Office Feature Updates                   04-Mar-21 10:08:02 AM  Ready
Office Feature Updates Logon             N/A                    Ready

Folder: \Microsoft\OneCore
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\VisualStudio
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\VisualStudio\Updates
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
BackgroundDownload                       N/A                    Ready

Folder: \Microsoft\Windows
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows\.NET Framework
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
```

```
========================================= ====================== ===============
.NET Framework NGEN v4.0.30319           N/A                    Ready
.NET Framework NGEN v4.0.30319 64        N/A                    Ready
.NET Framework NGEN v4.0.30319 64 Critic N/A                    Disabled
.NET Framework NGEN v4.0.30319 Critical  N/A                    Disabled

Folder: \Microsoft\Windows\Active Directory Rights Management Services Client
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
AD RMS Rights Policy Template Management N/A                    Disabled
AD RMS Rights Policy Template Management N/A                    Ready

Folder: \Microsoft\Windows\AppID
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
PolicyConverter                          N/A                    Disabled
VerifiedPublisherCertStoreCheck          N/A                    Disabled

Folder: \Microsoft\Windows\Application Experience
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Microsoft Compatibility Appraiser        04-Mar-21 3:17:30 AM   Ready
PcaPatchDbTask                           04-Mar-21 3:49:43 AM   Ready
ProgramDataUpdater                       N/A                    Ready
StartupAppTask                           N/A                    Ready

Folder: \Microsoft\Windows\ApplicationData
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
appuriverifierdaily                      N/A                    Ready
appuriverifierinstall                    N/A                    Ready
CleanupTemporaryState                    N/A                    Ready
DsSvcCleanup                             N/A                    Ready

Folder: \Microsoft\Windows\AppxDeploymentClient
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Pre-staged app cleanup                   N/A                    Disabled
```

```
Folder: \Microsoft\Windows\Autochk
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Proxy                                    N/A                    Ready

Folder: \Microsoft\Windows\BitLocker
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
BitLocker Encrypt All Drives             N/A                    Ready
BitLocker MDM policy Refresh             N/A                    Ready

Folder: \Microsoft\Windows\Bluetooth
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
UninstallDeviceTask                      N/A                    Ready

Folder: \Microsoft\Windows\BrokerInfrastructure
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
BgTaskRegistrationMaintenanceTask        N/A                    Ready

Folder: \Microsoft\Windows\CertificateServicesClient
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
UserTask                                 N/A                    Ready
UserTask-Roam                            N/A                    Ready

Folder: \Microsoft\Windows\Chkdsk
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
ProactiveScan                            N/A                    Ready
SyspartRepair                            N/A                    Ready

Folder: \Microsoft\Windows\CloudExperienceHost
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
CreateObjectTask                         N/A                    Ready

Folder: \Microsoft\Windows\Customer Experience Improvement Program
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Consolidator                             04-Mar-21 6:00:00 AM   Ready
UsbCeip                                  N/A                    Ready
```

```
Folder: \Microsoft\Windows\Device Information
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Device                                   04-Mar-21 4:11:53 AM   Ready
Device User                              N/A                    Ready

Folder: \Microsoft\Windows\Diagnosis
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
RecommendedTroubleshootingScanner        N/A                    Ready
Scheduled                                N/A                    Ready

Folder: \Microsoft\Windows\DirectX
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
DirectXDatabaseUpdater                   N/A                    Ready
DXGIAdapterCache                         N/A                    Ready

Folder: \Microsoft\Windows\DiskCleanup
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
SilentCleanup                            N/A                    Ready

Folder: \Microsoft\Windows\DiskDiagnostic
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Microsoft-Windows-DiskDiagnosticDataColl N/A                    Disabled
Microsoft-Windows-DiskDiagnosticResolver N/A                    Disabled

Folder: \Microsoft\Windows\DiskFootprint
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Diagnostics                              N/A                    Ready
StorageSense                             N/A                    Ready

Folder: \Microsoft\Windows\DUSM
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
dusmtask                                 N/A                    Ready
```

```
Folder: \Microsoft\Windows\EDP
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
EDP App Launch Task                      N/A                    Ready
EDP Auth Task                            N/A                    Ready
EDP Inaccessible Credentials Task        N/A                    Ready
StorageCardEncryption Task               N/A                    Ready

Folder: \Microsoft\Windows\ExploitGuard
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
ExploitGuard MDM policy Refresh          N/A                    Ready

Folder: \Microsoft\Windows\Feedback
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows\Feedback\Siuf
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
DmClient                                 N/A                    Ready
DmClientOnScenarioDownload               N/A                    Ready

Folder: \Microsoft\Windows\FileHistory
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
File History (maintenance mode)          N/A                    Ready

Folder: \Microsoft\Windows\Flighting
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows\Flighting\FeatureConfig
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
ReconcileFeatures                        N/A                    Ready
UsageDataFlushing                        N/A                    Ready
UsageDataReporting                       N/A                    Ready
```

Advanced

```
C:\Btech pdf\SecureCoding_Lab\Lab3>SCHTASKS /Create /SC DAILY /TN "Internet_Logger" /TR "netstat -n
SUCCESS: The scheduled task "Internet_Logger" has successfully been created.
```

```
C:\Btech pdf\SecureCoding_Lab\Lab3>SCHTASKS /DELETE /TN "Internet_Logger"
WARNING: Are you sure you want to remove the task "Internet_Logger" (Y/N)? y
SUCCESS: The scheduled task "Internet_Logger" was successfully deleted.
```

To lock your PC

(Win + L)

```
 import ctypes ctypes.windll.user32.LockWorkStation()
```

To clear your recycle bin

```
import os

import subprocess

import winshell from random

import randint from time

import sleep

def main():

file_size = os.path.getsize('C:')

print("{} kb of data will be removed".format(file_size))

 del_dir = r'

c:\windows\temp'

# Could this just be os.rmdir(del_dir)???

process = subprocess.Popen('rmdir /S /Q {}'.format(del_dir), shell=True,
stdout=subprocess.PIPE, stderr=subprocess.PIPE) _ = process.communicate()

return_code = process.returncode

if return_code == 0:

 print('Success: Cleaned Windows Temp Folder')

else:

 print('Fail: Unable to Clean Windows Temp Folder')

winshell.recycle_bin().empty(confirm=False, show_progress=False, sound=False)

# Is this important?

# sleep(randint(4, 6))

 input("Press any key to continue")
```

```
 if __name__ == '__main__':
main()
Rundll32.exe user32.dll,LockWorkStation
powercfg /SETACVALUEINDEX SCHEME_CURRENT SUB_VIDEO VIDEOCONLOCK 1500
 C:\WINDOWS\system32>rd /q /s c:\$Recycle.Bin
 C:\WINDOWS\system32>rd /q /s e:\$Recycle.Bin
```