

Ex.No: 4
Date: 17-02-2021

Name: Ganga Suresh Kumar Nair
Reg.No: 18BCN7014

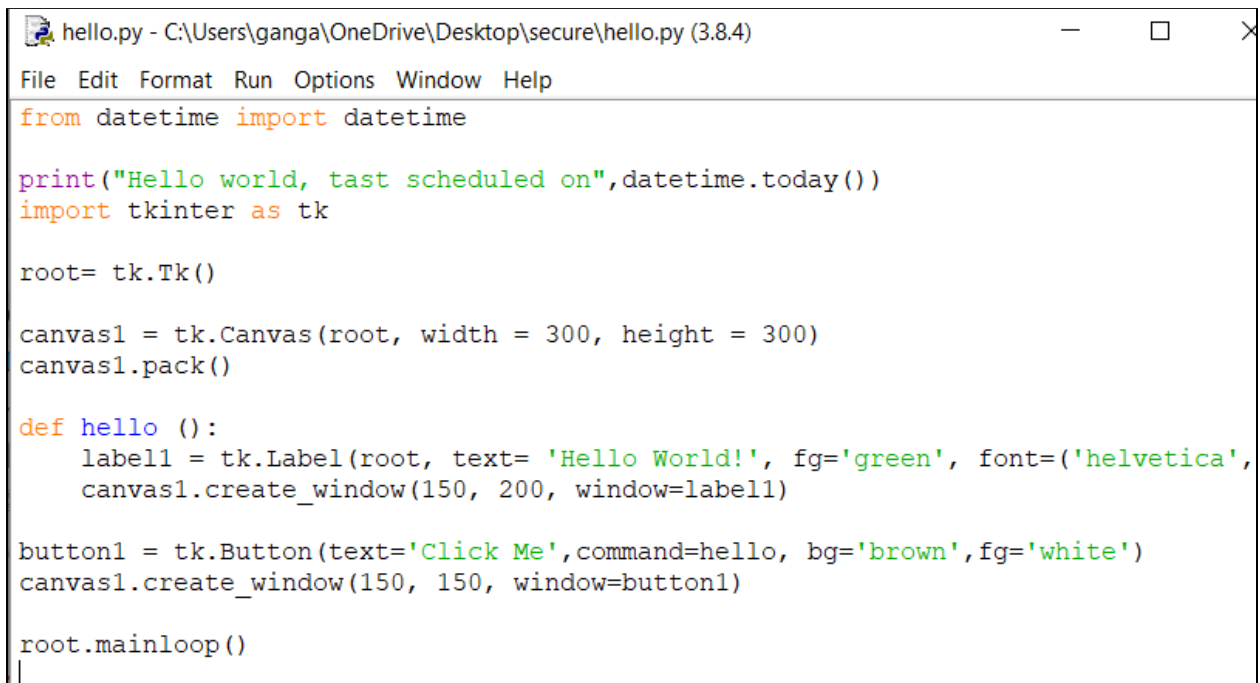
Secure Coding

1.

Mid-level

- Write a python script to print hello world.
- Convert the script into executable (use pyinstaller or py2exe – any of your choice).
- Schedule a task named “Python execution” to run the above executable on the first Monday of every month.

Python file



```
from datetime import datetime

print("Hello world, task scheduled on",datetime.today())
import tkinter as tk

root= tk.Tk()

canvas1 = tk.Canvas(root, width = 300, height = 300)
canvas1.pack()

def hello ():
    label1 = tk.Label(root, text= 'Hello World!', fg='green', font=('helvetica',
    canvas1.create_window(150, 200, window=label1)

button1 = tk.Button(text='Click Me',command=hello, bg='brown',fg='white')
canvas1.create_window(150, 150, window=button1)

root.mainloop()
```

Convert the script into executable

```

C:\Users\ganga\OneDrive\Desktop\secure>pyinstaller --onefile hello.py
80 INFO: PyInstaller: 4.2
81 INFO: Python: 3.8.4
83 INFO: Platform: Windows-10-10.0.18362-SP0
84 INFO: wrote C:\Users\ganga\OneDrive\Desktop\secure\hello.spec
88 INFO: UPX is not available.
96 INFO: Extending PYTHONPATH with paths
['C:\\Users\\ganga\\OneDrive\\Desktop\\secure',
 'C:\\Users\\ganga\\OneDrive\\Desktop\\secure']
104 INFO: checking Analysis
104 INFO: Building Analysis because Analysis-00.toc is non existent
105 INFO: Initializing module dependency graph...
110 INFO: Caching module graph hooks...
119 WARNING: Several hooks defined for module 'win32ctypes.core'. Please take care they do not conflict.

```

Scheduling task

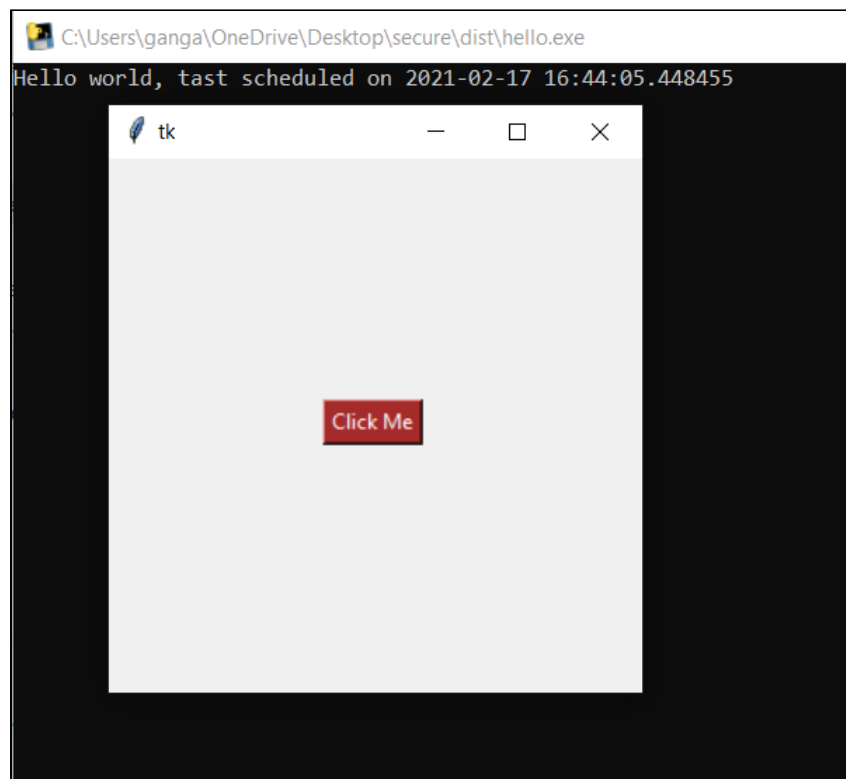
```

C:\Users\ganga\OneDrive\Desktop\secure>SCHEDTASKS/Create /SC MONTHLY /MO first /D MON /TN "Python execution" /TR "C:\Users\ganga\OneDrive\Desktop\secure\dist\hello.exe"
SUCCESS: The scheduled task "Python execution" has successfully been created.

```

OneDrive Standalone Update Task-S-1-5-21	18/02/2021	12:53:37	Ready
Python execution	01/03/2021	16:50:00	Ready

Output



2.

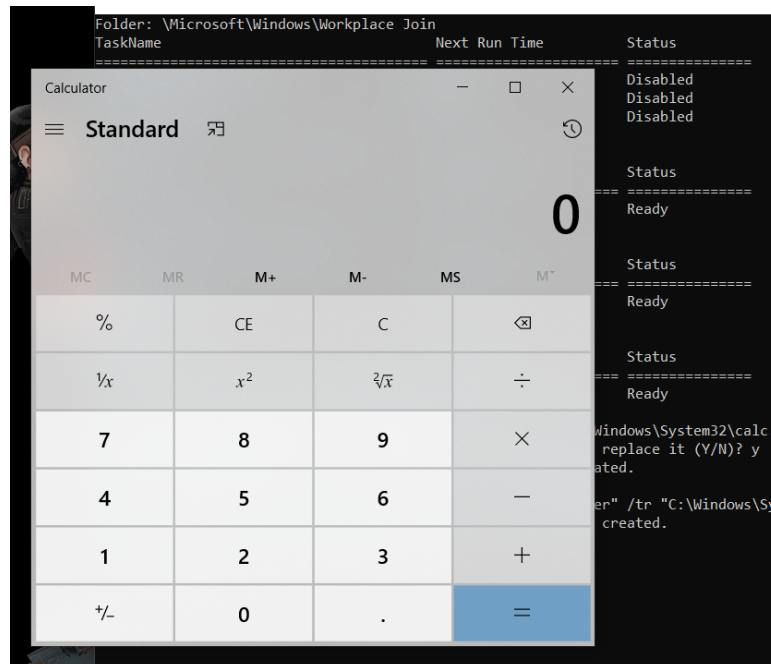
Intermediate

- Schedule a task named "Executer" on your machine to run calculator for every five minutes starting from the specified start time with no end
- Schedule a task named "Executer2" to run notepad starting at 5:00PM and automatically terminating at 5:40PM hours every day

To run Calculator

```
C:\Users\ganga>schtasks /create /sc minute /mo 5 /tn "Executer" /tr "C:\Windows\System32\calc.exe" /st 17:19  
SUCCESS: The scheduled task "Executer" has successfully been created.
```

Folder: \	TaskName	Next Run Time	Status
BlueStacksHelper		17/02/2021 22:59:30	Ready
Executer		17/02/2021 17:24:00	Ready



To run Notepad

```
C:\Users\ganga>schtasks /create /sc daily /tn "Executer2" /tr "C:\Windows\System32\notepad.exe" /st 17:00 /et 17:40  
SUCCESS: The scheduled task "Executer2" has successfully been created.
```

Folder: \	TaskName	Next Run Time	Status
=====	=====	=====	=====
	BlueStacksHelper	17/02/2021 22:59:30	Ready
	Executer	17/02/2021 17:34:00	Ready
	Executer2	17/02/2021 17:40:00	Ready

3.

Advanced

- Schedule a task named "Logger" to log your internet explorer activity to a separate text file.

Install sysmon

```
C:\Users\ganga\OneDrive\Desktop\Sysmon>Sysmon.exe -i -h md5 -l -n  
  
System Monitor v13.01 - System activity monitor  
Copyright (C) 2014-2021 Mark Russinovich and Thomas Garnier  
Sysinternals - www.sysinternals.com  
  
Sysmon installed.  
SysmonDrv installed.  
Starting SysmonDrv.  
SysmonDrv started.  
Starting Sysmon..  
Sysmon started.
```

Check on the event viewer, it logs processes, network activities etc.

Operational Number of events: 121 (0) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	23/02/2021 16:46:03	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	23/02/2021 16:45:59	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	23/02/2021 16:45:59	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	23/02/2021 16:45:57	Sysmon	1	Process Create (rule: ProcessCreate)
Information	23/02/2021 16:45:56	Sysmon	1	Process Create (rule: ProcessCreate)
Information	23/02/2021 16:45:55	Sysmon	5	Process terminated (rule: ProcessTermination)
Information	23/02/2021 16:45:54	Sysmon	5	Process terminated (rule: ProcessTermination)
Information	23/02/2021 16:45:53	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	23/02/2021 16:45:53	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	23/02/2021 16:45:51	Sysmon	1	Process Create (rule: ProcessCreate)
Information	23/02/2021 16:45:51	Sysmon	1	Process Create (rule: ProcessCreate)

Event 3, Sysmon

General Details

ProcessGUID: {70afb326-e3cc-6034-f704-000000008400}
 ProcessId: 8536
 Image: C:\Windows\Sysmon.exe
 User: NT AUTHORITY\SYSTEM
 Protocol: tcp
 Initiated: true
 SourceIpV6: false
 SourceIp: 192.168.1.108
 SourceHostname: LAPTOP-OREUD2V6.dlinkrouter
 SourcePort: 52326
 SourcePortName: -
 DestinationIpV6: false
 DestinationIp: 23.15.155.27
 DestinationHostname: -
 DestinationPort: 80
 DestinationPortName: http

Log Name: Microsoft-Windows-Sysmon/Operational
 Source: Sysmon
 Event ID: 3
 Level: Information
 User: SYSTEM
 OpCode: Info
 More Information: [Event Log Online Help](#)

Logged: 23/02/2021 16:45:53
 Task Category: Network connection detected (rule: NetworkConnect)
 Keywords:
 Computer: LAPTOP-OREUD2V6

Configure it to your specific needs

Administrator: Command Prompt

```
activity from early in the boot that the service will write to the event log when it starts.
On Vista and higher, events are stored in "Applications and Services Logs/Microsoft/Windows/Sysmon/Operational". On older systems, events are stored in the event log.
Use the '-? config' command for configuration file documentation on the Sysinternals website.
Specify -accepteula to automatically accept the EULA on installation. Sysmon will not be installed interactively prompted to accept it.
Neither install nor uninstall requires a reboot.
C:\Users\ganga\OneDrive\Desktop\Sysmon>sysmon -c config.xml

System Monitor v13.01 - System activity monitor
Copyright (C) 2014-2021 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 13.01
Sysmon schema version: 4.50
Configuration file validated.
Configuration updated.
```

config - Notepad

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Sysmon schemaversion="13.01">
  <HashAlgorithms>md5,sha256</HashAlgorithms>
  <EventFiltering>
    <NetworkConnect onmatch="exclude"/>
    <CreateRemoteThread onmatch="include">
      <TargetImage condition="image">explorer.exe</TargetImage>
      <TargetImage condition="image">lsass.exe</TargetImage>
      <TargetImage condition="image">services.exe</TargetImage>
      <TargetImage condition="image">svchost.exe</TargetImage>
      <TargetImage condition="image">winlogon.exe</TargetImage>
    </CreateRemoteThread>
    <RawAccessRead onmatch="exclude">
      <Image condition="image">C:\Users\ganga\OneDrive\Desktop\Sysmon\config.xml</Image>
      <Image condition="image">System</Image>
    </RawAccessRead>
  </EventFiltering>
</Sysmon>
```

OUTPUT

Operational Number of events: 1,851 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	23/02/2021 17:35:25	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	23/02/2021 17:35:26	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	23/02/2021 17:35:26	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	23/02/2021 17:35:26	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	23/02/2021 17:35:26	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	23/02/2021 17:35:26	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	23/02/2021 17:35:26	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	23/02/2021 17:35:27	Sysmon	3	Network connection detected (rule: NetworkConnect)
Information	23/02/2021 17:35:41	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	23/02/2021 17:35:41	Sysmon	1	Process Create (rule: ProcessCreate)

Event 3, Sysmon

General Details

☒ Friendly View ☐ XML View

Image C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
User LAPTOP-OREUD2V6\ganga
Protocol tcp
Initiated true
SourceIsIpv6 false
SourceIp 192.168.1.108
SourceHostname LAPTOP-OREUD2V6.dlinkrouter
SourcePort 53147
SourcePortName -
DestinationIsIpv6 false
DestinationIp 40.90.189.152
DestinationHostname -
DestinationPort 443
DestinationPortName https

4.

Advanced

- Schedule a task to defragment any of your local disk daily at 10AM

Python script to defrag

```
diskdefrag.py - C:\Users\ganga\OneDrive\Desktop\secure\diskdefrag.py (3.8.4)
File Edit Format Run Options Window Help
import win32com.shell.shell as shell
commands = 'defrag.exe D:'
shell.ShellExecuteEx(lpVerb='runas', lpFile='cmd.exe', lpParameters='/c '+commands)
```

Scheduling a task to run this script everyday at 10 am

```
C:\Users\ganga\OneDrive\Desktop\secure>schtasks /create /sc daily /tn "fragDiskDaily" /tr "C:\Users\ganga\OneDrive\Desktop\secure\diskdefrag.exe" /st 10:00
SUCCESS: The scheduled task "fragDiskDaily" has successfully been created.
```





5.

Attrib command

```
C:\Users\ganga>attrib -h -r -s /s /d C:\*.*
Access denied - C:\$Recycle.Bin\S-1-5-18
Access denied - C:\$Recycle.Bin\S-1-5-21-304216329-2939352978-3859065660-1000
Access denied - C:\$Recycle.Bin\S-1-5-21-304216329-2939352978-3859065660-1002
Access denied - C:\$Recycle.Bin\S-1-5-21-304216329-2939352978-3859065660-1003
Access denied - C:\$SysReset\Scratch\csrss.exe
Access denied - C:\OneDriveTemp\S-1-5-21-304216329-2939352978-3859065660-1002
Access denied - C:\Program Files\Android\Android Studio\bin\clang\win\clang-tidy.exe
Access denied - C:\Program Files\Android\Android Studio\bin\clang\win\clangd.exe
Access denied - C:\Program Files\Android\Android Studio\bin\clang\win\libgcc_s_seh-1.dll
Access denied - C:\Program Files\Android\Android Studio\bin\clang\win\libssp-0.dll
```







Set attribute to read-only and to hide the file and system file.

```
C:\Users\ganga\OneDrive\Desktop\secure>attrib +h +r +s /s /d build
C:\Users\ganga\OneDrive\Desktop\secure>
```

	__pycache__		20/02/2021 06:47 PM	File folder
	dist		20/02/2021 06:47 PM	File folder

Reverse to get back the file

```
C:\Users\ganga\OneDrive\Desktop\secure>attrib -h -r -s /s /d build
```

	__pycache__		20/02/2021 06:47 PM	File folder
	build		20/02/2021 06:47 PM	File folder
	dist		20/02/2021 06:47 PM	File folder

6.

Powercfg

- Powercfg is a very powerful command for managing and tracking how your computer uses energy.
- >powercfg /energy
- > Powercfg /lastwake
- >powercfg /hibernate on
- > powercfg /hibernate off
- > powercfg /a
- powercfg /devicequery s1_supported

```
C:\WINDOWS\system32>powercfg /energy
Enabling tracing for 60 seconds...
Observing system behavior...
Analyzing trace data...
Analysis complete.

Energy efficiency problems were found.

8 Errors
11 Warnings
67 Informational

See C:\WINDOWS\system32\energy-report.html for more details.
```

```
C:\WINDOWS\system32>powercfg /lastwake
Wake History Count - 1
Wake History [0]
Wake Source Count - 1
Wake Source [0]
Type: Fixed Feature
Power Button
```



```
C:\WINDOWS\system32>powercfg /hibernate on  
C:\WINDOWS\system32>powercfg /hibernate off
```

```
C:\WINDOWS\system32>powercfg /a  
The following sleep states are available on this system:  
Standby (S3)  
  
The following sleep states are not available on this system:  
Standby (S1)  
    The system firmware does not support this standby state.  
  
Standby (S2)  
    The system firmware does not support this standby state.  
  
Hibernate  
    Hibernation has not been enabled.  
  
Standby (S0 Low Power Idle)  
    The system firmware does not support this standby state.  
  
Hybrid Sleep  
    Hibernation is not available.  
  
Fast Startup  
    Hibernation is not available.
```

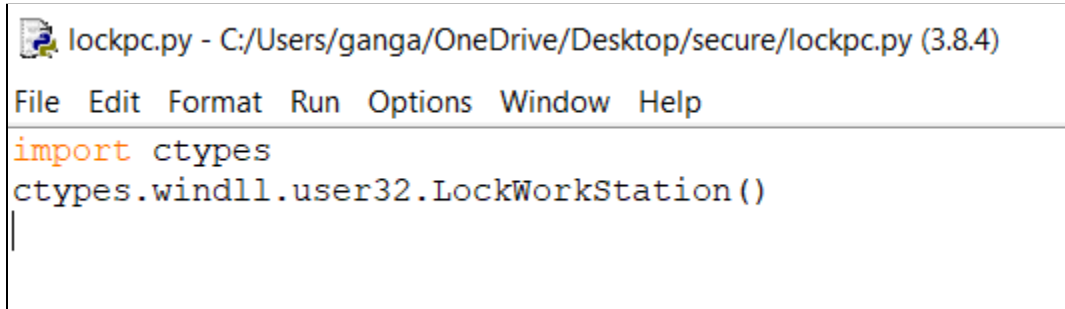
```
C:\WINDOWS\system32>powercfg /devicequery s1_supported  
HID-compliant device  
Root Print Queue  
Volume Manager  
Fax  
Microphone Array (Realtek High Definition Audio)
```

7.

Write a script to perform the following jobs

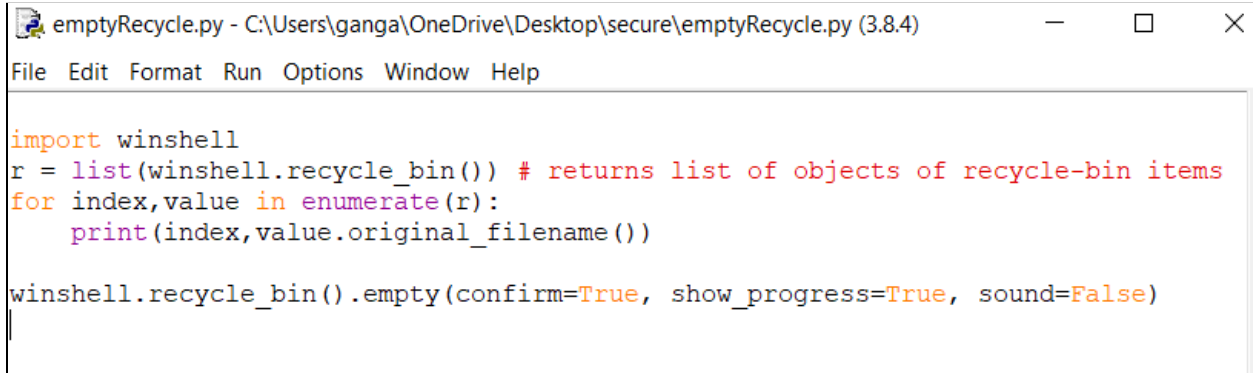
- To lock your PC(Win + L)
- To clear your recycle bin

Script to lock your PC



```
lockpc.py - C:/Users/ganga/OneDrive/Desktop/secure/lockpc.py (3.8.4)
File Edit Format Run Options Window Help
import ctypes
ctypes.windll.user32.LockWorkStation()
|
```

Script to clear recycle bin



```
emptyRecycle.py - C:\Users\ganga\OneDrive\Desktop\secure\emptyRecycle.py (3.8.4)
File Edit Format Run Options Window Help
import winshell
r = list(winshell.recycle_bin()) # returns list of objects of recycle-bin items
for index,value in enumerate(r):
    print(index,value.original_filename())

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

