Secure Coding Lab-4

Chekuri.mahesh

18BCN7101 L39+L40

# Mid-Level



## Python script :

print(‘hello world 18BCN7081’)





G:\Secure Coding LABS\lab4>**pyinstaller -F 18BCN7081.py**

|  |  |  |
| --- | --- | --- |
| 401 | INFO: | PyInstaller: 4.2 |
| 401 | INFO: | Python: 3.9.0 |
| 417 | INFO: | Platform: Windows-10-10.0.19041-SP0 |
| 417 | INFO: | wrote G:\Secure Coding LABS\lab4\18BCN7081.spec |
| 417 | INFO: | UPX is not available. |
| 432 | INFO: | Extending PYTHONPATH with paths |

['G:\\Secure Coding LABS\\lab4', 'G:\\Secure Coding LABS\\lab4']

517 INFO: checking Analysis

517 INFO: Building Analysis because Analysis-00.toc is non existent

517 INFO: Initializing module dependency graph...

533 INFO: Caching module graph hooks...

533 WARNING: Several hooks defined for module

'win32ctypes.core'. Please take care they do not conflict.

571 INFO: Analyzing base\_library.zip ...

7244 INFO: Processing pre-find module path hook distutils from

'c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39\

\lib\\site-packages\\PyInstaller\\hooks\\pre\_find\_module\_path\\h ook-distutils.py'.

7245 INFO: distutils: retargeting to non-venv dir

'c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39\

\lib'

13460 INFO: Caching module dependency graph... 13590 INFO: running Analysis Analysis-00.toc

13597 INFO: Adding Microsoft.Windows.Common-Controls to dependent assemblies of final executable

required by

c:\users\javvadi\appdata\local\programs\python\python39\python.e xe

13742 WARNING: lib not found: api-ms-win-core-path-l1-1-0.dll dependency of

c:\users\javvadi\appdata\local\programs\python\python39\python39

.dll

13785 INFO: Analyzing G:\Secure Coding LABS\lab4\18BCN7081.py 13808 INFO: Processing module hooks...

13809 INFO: Loading module hook 'hook-difflib.py' from

'c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39\

\lib\\site-packages\\PyInstaller\\hooks'...

13811 INFO: Excluding import of doctest from module difflib 13812 INFO: Loading module hook 'hook-distutils.py' from

'c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39\

\lib\\site-packages\\PyInstaller\\hooks'...

13815 INFO: Loading module hook 'hook-distutils.util.py' from

'c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39\

\lib\\site-packages\\PyInstaller\\hooks'...

13818 INFO: Excluding import of lib2to3.refactor from module distutils.util

13819 INFO: Loading module hook 'hook-encodings.py' from

'c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39\

\lib\\site-packages\\PyInstaller\\hooks'...

13929 INFO: Loading module hook 'hook-heapq.py' from

'c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39\

\lib\\site-packages\\PyInstaller\\hooks'...

13933 INFO: Excluding import of doctest from module heapq 13933 INFO: Loading module hook 'hook-lib2to3.py' from

'c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39\

\lib\\site-packages\\PyInstaller\\hooks'...

13994 INFO: Loading module hook 'hook-multiprocessing.util.py' from

'c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39\

\lib\\site-packages\\PyInstaller\\hooks'...

13997 INFO: Excluding import of test.support from module multiprocessing.util

13998 INFO: Excluding import of test from module multiprocessing.util

14000 INFO: Loading module hook 'hook-pickle.py' from

'c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39\

\lib\\site-packages\\PyInstaller\\hooks'...

14002 INFO: Excluding import of argparse from module pickle 14002 INFO: Loading module hook 'hook-sysconfig.py' from

'c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39\

\lib\\site-packages\\PyInstaller\\hooks'...

14066 INFO: Loading module hook 'hook-xml.etree.cElementTree.py' from

'c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39\

\lib\\site-packages\\PyInstaller\\hooks'...

14069 INFO: Loading module hook 'hook-xml.py' from

'c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39\

\lib\\site-packages\\PyInstaller\\hooks'...

14290 INFO: Loading module hook 'hook-\_tkinter.py' from

'c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39\

\lib\\site-packages\\PyInstaller\\hooks'...

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 14562 | INFO: | checking | Tree |  | | | |
| 14562 | INFO: | Building | Tree | because Tree-00.toc | is | non | existent |
| 14564 | INFO: | Building | Tree | Tree-00.toc |  |  |  |
| 14658 | INFO: | checking | Tree |  |  |  |  |
| 14659 | INFO: | Building | Tree | because Tree-01.toc | is | non | existent |
| 14662 | INFO: | Building | Tree | Tree-01.toc |  |  |  |
| 14775 | INFO: | checking | Tree |  |  |  |  |
| 14775 | INFO: | Building | Tree | because Tree-02.toc | is | non | existent |
| 14779 | INFO: | Building | Tree | Tree-02.toc |  |  |  |
| 14816 | INFO: | Looking for ctypes DLLs | | | | | |
| 14849 | INFO: | Analyzing run-time hooks ... | | | | | |

14852 INFO: Including run-time hook

'c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39\

\lib\\site-packages\\PyInstaller\\hooks\\rthooks\\pyi\_rth\_multip rocessing.py'

14876 INFO: Looking for dynamic libraries 15221 INFO: Looking for eggs

15221 INFO: Using Python library

c:\users\javvadi\appdata\local\programs\python\python39\python39

.dll

15224 INFO: Found binding redirects:

[]

15229 INFO: Warnings written to G:\Secure Coding LABS\lab4\build\18BCN7081\warn-18BCN7081.txt

15299 INFO: Graph cross-reference written to G:\Secure Coding LABS\lab4\build\18BCN7081\xref-18BCN7081.html

15359 INFO: checking PYZ

15359 INFO: Building PYZ because PYZ-00.toc is non existent 15361 INFO: Building PYZ (ZlibArchive) G:\Secure Coding

LABS\lab4\build\18BCN7081\PYZ-00.pyz

15898 INFO: Building PYZ (ZlibArchive) G:\Secure Coding

LABS\lab4\build\18BCN7081\PYZ-00.pyz completed successfully. 15930 INFO: checking PKG

15930 INFO: Building PKG because PKG-00.toc is non existent 15931 INFO: Building PKG (CArchive) PKG-00.pkg

18229 INFO: Building PKG (CArchive) PKG-00.pkg completed successfully.

18232 INFO: Bootloader

c:\users\javvadi\appdata\local\programs\python\python39\lib\site

-packages\PyInstaller\bootloader\Windows-64bit\run.exe 18233 INFO: checking EXE

18235 INFO: Building EXE because EXE-00.toc is non existent 18235 INFO: Building EXE from EXE-00.toc

18368 INFO: Copying icons from

['c:\\users\\javvadi\\appdata\\local\\programs\\python\\python39

\\lib\\site-packages\\PyInstaller\\bootloader\\images\\icon-cons ole.ico']

18442 INFO: Writing RT\_GROUP\_ICON 0 resource with 104 bytes

18443 INFO: Writing RT\_ICON 1 resource with 3752 bytes

18445 INFO: Writing RT\_ICON 2 resource with 2216 bytes

18447 INFO: Writing RT\_ICON 3 resource with 1384 bytes

18447 INFO: Writing RT\_ICON 4 resource with 37019 bytes

18448 INFO: Writing RT\_ICON 5 resource with 9640 bytes

18449 INFO: Writing RT\_ICON 6 resource with 4264 bytes

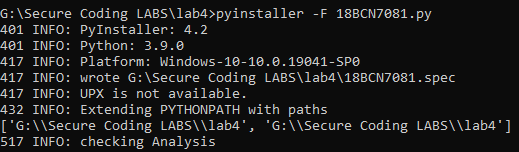
18449 INFO: Writing RT\_ICON 7 resource with 1128 bytes 18463 INFO: Updating manifest in G:\Secure Coding

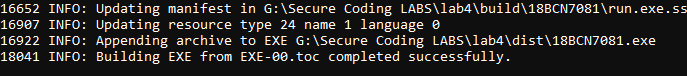
LABS\lab4\build\18BCN7081\run.exe.rawka8ta

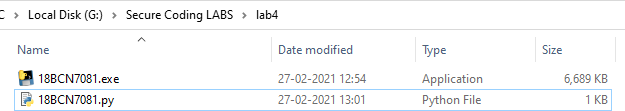
18528 INFO: Updating resource type 24 name 1 language 0 18533 INFO: Appending archive to EXE G:\Secure Coding

LABS\lab4\dist\18BCN7081.exe

18633 INFO: Building EXE from EXE-00.toc completed successfully.



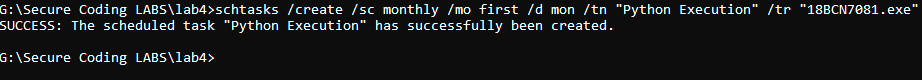




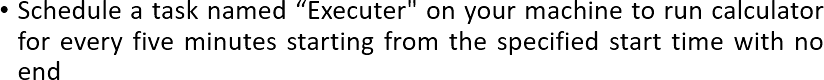


G:\Secure Coding LABS\lab4>schtasks /create /sc monthly /mo first /d mon /tn "Python Execution" /tr "18BCN7081.exe"

SUCCESS: The scheduled task "Python Execution" has successfully been created.

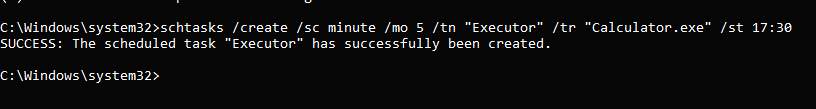


# Intermediate



C:\Windows\system32>schtasks /create /sc minute /mo 5 /tn "Executor" /tr "Calculator.exe" /st 17:30

SUCCESS: The scheduled task "Executor" has successfully been created.

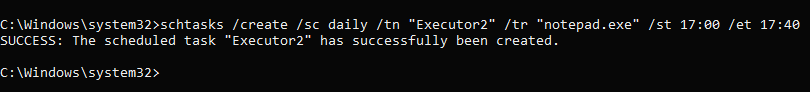




C:\Windows\system32>schtasks /create /sc daily /tn "Executor2"

/tr "notepad.exe" /st 17:00 /et 17:40

SUCCESS: The scheduled task "Executor2" has successfully been created.

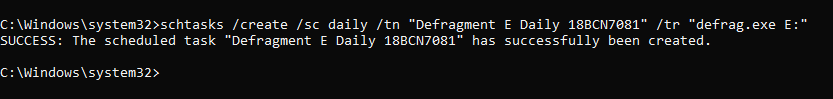


# Advanced



C:\Windows\system32>schtasks /create /sc daily /tn "Defragment E Daily 18BCN7081" /tr "defrag.exe E:"

SUCCESS: The scheduled task "Defragment E Daily 18BCN7081" has successfully been created.



# Attrib Commands

+r = This assigns the read-only ﬁle attribute to the ﬁle or directory.

-r = This removes the read-only attribute.

+s = This assigns the system ﬁle attribute to the ﬁle or directory.

-s = This removes the system attribute.

+h = This assigns the hidden ﬁle attribute to the ﬁle or directory.

-h = This removes the hidden attribute.

+c = This assigns the compressed ﬁle attribute to the ﬁle or directory.

-c = This removes the compressed attribute.

|  |  |  |  |
| --- | --- | --- | --- |
| C:',>azzrib | | | |
| A | SHR |  | C:',boozmgr |
| A | SH |  | C:',BCC MX |
| A | SH |  | C :',DumpSzac<.log.amp |
| A | SH | I | C :',hiberfil.sys |
| A | SH |  | C : ,pagefile.sys |
| A | SH |  | C: ,snapfile.sys |



E: ,>azzrib

E : \*,18BC fJ7081. exe E : \*,18BC f J7 081. pdf E : \*,18BCIJ7081. axe

E:',>a-crib -r -h 18BCM7081.exe

E:',>azznib -s 18BCM7081.pdf

E:',>azzrib

A HR

S

E : \*,18BC fJ7081. exe E : \*,18BC fJ7081. pdf E : \*,18BC fJ7081. axe

E : , ›a zz rib - r - h 18BCIJ7081. exe

E:',>azzrib -s 18BCM7081.pdf E: ,>azzrib

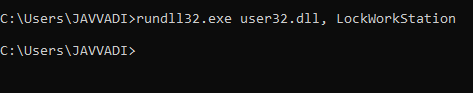
E: \18BCM7081.exe E: \18BCM7081.pdf E:',18BCM7081.zxz





## CMD Script:

rundll32.exe user32.dll, LockWorkStation

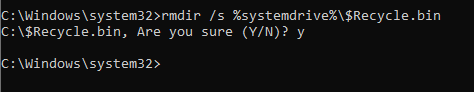






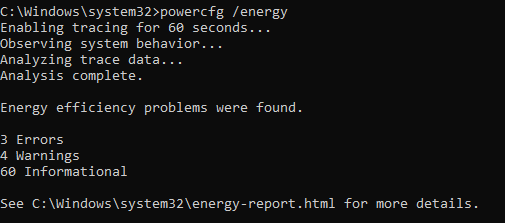
## CMD Script:

rmdir /s %systemdrive%\$Recycle.bin

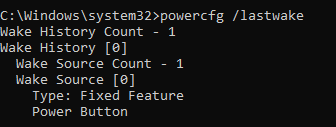


# Powercfg

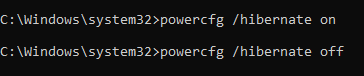
Powercfg is a very powerful command for managing and tracking how your computer uses energy



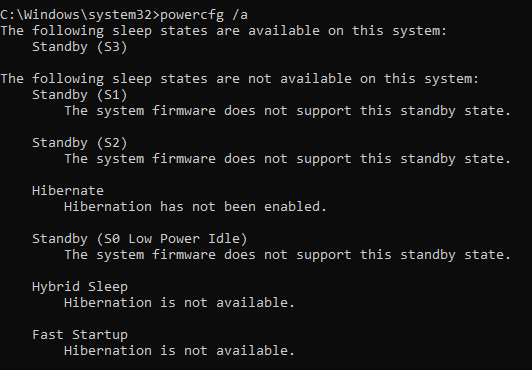
Examines the system for common energy-efficiency and battery life problems.



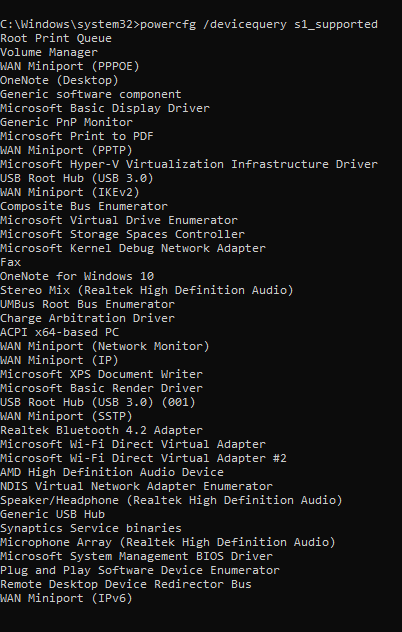
shows the information about what woke the system from the last sleep transition.



Will turn hibernate feature on and off.



shows the sleep states in available system



To list the devices that supports waking PC from S1 state