

## SECURE CODING LAB 4

# POWERCFG ENERGY

Microsoft Windows [Version 10.0.19041.804]

(c) 2020 Microsoft Corporation. All rights reserved.

```
C:\Windows\system32>powercfg /energy
```

Enabling tracing for 60 seconds...

Observing system behavior...

Analyzing trace data...

Analysis complete.

Energy efficiency problems were found.

7 Errors

8 Warnings

38 Informational

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

```
C:\Windows\system32>
```

## Power and Attrib Commands

Microsoft Windows [Version 10.0.19041.804]

(c) 2020 Microsoft Corporation. All rights reserved.

```
C:\Users\user>powercfg /?
```

POWERCFG /COMMAND [ARGUMENTS]

Description:

Enables users to control power settings on a local system.

For detailed command and option information, run "POWERCFG /? <COMMAND>"

Command List:

/LIST, /L       Lists all power schemes.

/QUERY, /Q      Displays the contents of a power scheme.

/CHANGE, /X     Modifies a setting value in the current power scheme.

/CHANGENAME     Modifies the name and description of a power scheme.

/DUPLICATEScheme Duplicates a power scheme.

/DELETE, /D      Deletes a power scheme.

/DELETESetting    Deletes a power setting.

/SETACTIVE, /S    Makes a power scheme active on the system.

/GETACTIVEScheme   Retrieves the currently active power scheme.

/SETACVALUEINDEX   Sets the value associated with a power setting  
while the system is powered by AC power.

/SETDCVALUEINDEX   Sets the value associated with a power setting  
while the system is powered by DC power.

/IMPORT            Imports all power settings from a file.

/EXPORT            Exports a power scheme to a file.

/ALIASES          Displays all aliases and their corresponding GUIDs.

/GETSECURITYDESCRIPTOR  
                 Gets a security descriptor associated with a specified  
power setting, power scheme, or action.

/SETSECURITYDESCRIPTOR  
                 Sets a security descriptor associated with a  
power setting, power scheme, or action.

/HIBERNATE, /H    Enables and disables the hibernate feature.

/AVAILABLESLEEPSTATES, /A  
                 Reports the sleep states available on the system.

/DEVICEQUERY      Returns a list of devices that meet specified criteria.

/DEVICEENABLEWAKE   Enables a device to wake the system from a sleep state.

/DEVICEDISABLEWAKE   Disables a device from waking the system from a sleep  
state.

/LASTWAKE          Reports information about what woke the system from the  
last sleep transition.

/WAKETIMERS      Enumerates active wake timers.

/REQUESTS      Enumerates application and driver Power Requests.

/REQUESTSOVERRIDE      Sets a Power Request override for a particular Process, Service, or Driver.

/ENERGY      Analyzes the system for common energy-efficiency and battery life problems.

/BATTERYREPORT      Generates a report of battery usage.

/SLEEPSTUDY      Generates a diagnostic system power transition report.

/SRUMUTIL      Dumps Energy Estimation data from System Resource Usage Monitor (SRUM).

/SYSTEMSLEEPDIAGNOSTICS  
                 Generates a diagnostic report of system sleep transitions.

/SYSTEMPOWERREPORT      Generates a diagnostic system power transition report.

/POWERTHROTTLING      Control power throttling for an application.

```
C:\Users\user>powercfg lastwake
```

```
Wake History Count - 1
```

```
Wake History [0]
```

```
Wake Source Count - 0
```

```
C:\Users\user>cd Desktop
```

```
C:\Users\user\Desktop>dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is A0D4-F368
```

```
Directory of C:\Users\user\Desktop
```

```
25-02-2021  22:20  <DIR>      .
25-02-2021  22:20  <DIR>      ..
25-02-2021  22:20                0 attrib
25-02-2021  22:20                0 cd
25-02-2021  22:20                0 mkdir
```

```

25-02-2021  22:29          5,200 New Text Document.txt
20-02-2021  14:27          1,032 Nmap - Zenmap GUI.lnk
08-01-2021  10:29  <DIR>      Old Firefox Data
27-01-2021  16:38  <DIR>      Secure
25-02-2021  22:10  <DIR>      SecureLab
          5 File(s)      6,232 bytes
          5 Dir(s) 161,523,335,168 bytes free

```

```

C:\Users\user\Desktop>attrib /?
Displays or changes file attributes.

```

```

ATTRIB [+R | -R] [+A | -A] [+S | -S] [+H | -H] [+O | -O] [+I | -I] [+X | -X] [+P | -P] [+U | -U]
[drive:][path][filename] [/S [/D]] [/L]

```

```

+  Sets an attribute.
-  Clears an attribute.
R  Read-only file attribute.
A  Archive file attribute.
S  System file attribute.
H  Hidden file attribute.
O  Offline attribute.
I  Not content indexed file attribute.
X  No scrub file attribute.
V  Integrity attribute.
P  Pinned attribute.
U  Unpinned attribute.
B  SMR Blob attribute.
[drive:][path][filename]
    Specifies a file or files for attrib to process.
/S  Processes matching files in the current folder
    and all subfolders.
/D  Processes folders as well.
/L  Work on the attributes of the Symbolic Link versus
    the target of the Symbolic Link

```

```

C:\Users\user\Desktop>attrib +h +r +s /s /d Old Firefox Data
Parameter format not correct -

```

```

C:\Users\user\Desktop>attrib +h +r +s /s /d Old_Firefox_Data

```

```

C:\Users\user\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is A0D4-F368

```

Directory of C:\Users\user\Desktop

```
03-03-2021 21:50 <DIR>      .
03-03-2021 21:50 <DIR>      ..
25-02-2021 22:20          0 attrib
25-02-2021 22:20          0 cd
25-02-2021 22:20          0 mkdir
25-02-2021 22:29        5,200 New Text Document.txt
20-02-2021 14:27        1,032 Nmap - Zenmap GUI.Ink
27-01-2021 16:38 <DIR>      Secure
25-02-2021 22:10 <DIR>      SecureLab
          5 File(s)      6,232 bytes
          4 Dir(s) 161,521,524,736 bytes free
```

C:\Users\user\Desktop>attrib -h -r -s /s /d Old\_Firefox\_Data

```
C:\Users\user\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is A0D4-F368
```

Directory of C:\Users\user\Desktop

```
03-03-2021 21:50 <DIR>      .
03-03-2021 21:50 <DIR>      ..
25-02-2021 22:20          0 attrib
25-02-2021 22:20          0 cd
25-02-2021 22:20          0 mkdir
25-02-2021 22:29        5,200 New Text Document.txt
20-02-2021 14:27        1,032 Nmap - Zenmap GUI.Ink
08-01-2021 10:29 <DIR>      Old_Firefox_Data
27-01-2021 16:38 <DIR>      Secure
25-02-2021 22:10 <DIR>      SecureLab
          5 File(s)      6,232 bytes
          5 Dir(s) 161,521,442,816 bytes free
```

C:\Users\user\Desktop>

# SCRIPT TO DO JOBS

## 1. Lock Windows PC

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

## 2. Clear Recycle Bin

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