PowerShell EZ Admin Menu - Manual

This document explains the functionality and usage of the provided PowerShell script.

Some options say “MUST BE ADMIN” but it may be best to be an administrator for all options.

Main Menu

The script presents a main menu with the following options:

```
===Powershell EZ Admin Menu===
1. File Hashes
2. Get, Kill, Start Processes
3. Account Creation, Removal, Information, Modifications
4. Policy Editor
5. Baseline Information
6. Networking
7. CPU, Memory, Disk Information
   Quit (q)
```

Usage

1. Run the PowerShell script.
2. Enter the number corresponding to the desired option.
3. Follow the prompts within the selected submenu.
4. Enter q to quit the application.

1) File Hashes

This option allows you to calculate and view various cryptographic hashes of a specified file.

Submenu

```
===File Hash Menu===
1: View SHA1
2: View SHA256
3: View SHA384
4: View SHA512
```

5: View MD5
6: View RIPEMD160
7: View MACTripleDES
Back To Main Menu (b)
```

**Usage**

1. Select a hash algorithm (1-7).
2. Enter the full file path when prompted.
3. The hash value will be displayed.
4. Enter b to return to the main menu.

## 2) Get, Kill, Start Processes

This option provides tools for managing processes.

**Submenu**

```
===Get, Kill, Start Processes===
1: Get Processes
2: Kill Processes
3: Start Processes
Back to Main Menu (b)
```

2.1) Get Processes Submenu

```
===Get Process Menu===
1: Get All Processes
2: Get Process Filepath
3: Get Process Username (!!!MUST BE ADMIN!!!)
4: Get Process Via PID
Back to Main Menu (b)
```

Usage

- **1: Get All Processes:** Displays a list of all running processes.
- **2: Get Process Filepath:** Displays the file path of a specified process.
- **3: Get Process Username:** Displays the username associated with a specified process.
- **4: Get Process Via PID:** Displays information about a process using its Process
```

ID (PID).

2.2) Kill Processes Submenu

```
===Kill Processes Menu===
1: Stop Process By Name
2: Stop Process By PID
3: Stop Process not owned by current user (!!!MUST BE ADMIN!!!)
Back to Main Menu (b)
```

Usage

- **1: Stop Process By Name:** Stops a process by its name.
- **2: Stop Process By PID:** Stops a process by its PID.
- **3: Stop Process not owned by current user:** Stops a process owned by another user.

2.3) Start Processes Submenu

```
===Start Processes Menu===
1: Start Process Via File Name
2: Start Process As Administrator
Back to Main Menu (b)
```

Usage

- **1: Start Process Via File Name:** Starts a process using its executable file name.
- **2: Start Process As Administrator:** Starts a process with administrator privileges.

3) Account Creation, Removal, Information, Modifications

This option provides tools for managing local user accounts.

Submenu

```
===Account Creation, Removal, Information, Modification Menu===
```

1. Account Creation
2. Account Removal
3. Account Information
4. Account Modification

b) Back To Main Menu
```

### 3.1) Account Creation

- Prompts for username, password, full name, description, and group.
- Creates a new local user and adds it to the specified group.

### 3.2) Account Removal

- Prompts for the username of the account to delete.
- Deletes the specified local user account.

### 3.3) Account Information Submenu

```
===Account Information===
1. Get All Local Accounts
2. Get Specific User Account
3. Get User SID
4. Get User account via SID
b) Back to Account Creation, Removal, Information, Modification Menu
```

Usage

- **1) Get All Local Accounts:** Displays a list of all local user accounts.
- **2) Get Specific User Account:** Displays information about a specified user account.
- **3) Get User SID:** Displays the Security Identifier (SID) of a specified user.
- **4) Get User account via SID:** Displays information about a user account using the user SID.

3.4) Account Modification

- This option is a placeholder and currently displays "test1".

4) Policy Editor

This option allows you to configure local security policies.

Submenu

```
===Policy Editor===
1. Password Policy Reconfiguration
```
```

2. Net Account Monitor
3. Policy Update with .INF File (!!!MUST BE ADMIN!!!)
   b) Back to Main Menu
   ```

**Usage**

- **1) Password Policy Reconfiguration:** Prompts for password policy settings (length, age, lockout) and applies them.
- **2) Net Account Monitor:** Monitors changes to the password policy and displays alerts.
- **3) Policy Update with .INF File:** Applies security settings from a specified .INF file.

## 5) Baseline Information

This option allows you to compare local users with a CSV file.

**Submenu**

```
===Baseline Information===
1. Compare Users with CSV
   b) Back to Main Menu
   ```

Usage

- **1) Compare Users with CSV:** Prompts for a CSV file path. If the file is not found, it provides the option to create a CSV of current local users. Then, it compares the users in the CSV with the local users and displays the differences.

6) Networking

This option provides tools for viewing and managing network connections.

Submenu

```
===Networking===
1. View Active Connections
2. Close Active Connection
```
```

3. Initiate Connections
   b) Back to Main Menu
   ```

**Usage**

- **1) View Active Connections:** Displays a list of active network connections using netstat -ano.
- **2) Close Active Connection:** Prompts for a PID and terminates the corresponding connection.
- **3) Initiate Connections Submenu**

**6.3) Initiate Connections Submenu**

```
===Initiate Connection===
1. Invoke Web Request
2. SSH Connection
   b) Back to Main Menu
   ```

Usage

- **1) Invoke Web Request:** Prompts for a URL or IP address and sends a web request.
- **2) SSH Connection:** Prompts for an IP address and initiates an SSH connection.

7) CPU, Memory, Disk Information

This option displays system information related to CPU, memory, and disk usage.

Usage

- Displays CPU load, total/used/free memory, disk usage for each logical disk, physical disk info, and disk IO information.
- Pauses after displaying the information.

Quit (q)

- Exits the PowerShell script.
   ```