Documentation – Manual to run the script

Prerequisites: These requirements are specific to Windows system. It requires Python 3.x and various python modules those are mentioned below. These modules can be installed using pip, the Python package installer.

Usage: To use the Windows Tool, navigate to the directory where the Python script is located and run the mainscript.py using command prompt or any external code editor.

Modules: Following are the python modules you need to have installed before running this script. You can also run requirement.txt command which will give you the details whether all requirements have been satisfied or not. To install following modules use the command *pip install modulename*

1. Wmi: This library provides a Python interface to the Windows Management Instrumentation (WMI) API, which allows you to query information about the system, such as hardware configuration, operating system details, and performance metrics.
2. psutil: This library provides an easy-to-use interface for retrieving information about running processes and system utilization on a variety of platforms, including Windows.
3. socket: This library provides low-level access to networking primitives, such as sockets, which can be used to implement network clients and servers.
4. uuid: This library provides a Python interface for generating universally unique identifiers (UUIDs), which are used to uniquely identify objects in distributed systems.
5. re: This library provides support for regular expressions, which can be used to search, replace, and manipulate text.
6. dns: This library provides a Python interface for performing DNS lookups and other DNS-related operations.
7. platform: This library provides an interface to system-specific configuration and information, such as the operating system version and hardware architecture.
8. Os: This library provides a Python interface to various operating system features, such as file I/O, process management, and environment variables.
9. nmap3: This library provides a Python interface to the Nmap network scanning tool, which can be used to identify hosts and services on a network.
10. Nmap: This library is a wrapper around the Nmap command-line utility, providing a Python interface for performing network scans.
11. Datetime: This library provides a Python interface for working with dates and times.

12. Pwnedpasswords: This library provides an interface to the Have I Been Pwned? (HIBP) service, which allows you to check whether a given password has been compromised in a data breach.
13. Codecs: This library provides support for character encoding and decoding, including common encodings like UTF-8 and ASCII.
14. Sys: This library provides access to various system-specific parameters and functions, such as the command line arguments and the Python interpreter.
15. Time: This library provides a Python interface for working with time, including sleep and timing functions.
16. Traceback: This library provides functions for working with Python traceback objects, which contain information about errors and exceptions in Python code.
17. win32con: This library provides constants and functions for working with Windows system services.
18. win32evtlog: This library provides an interface for working with the Windows Event Log.
19. win32evtlogutil: This library provides utility functions for working with the Windows Event Log.
20. Winerror: This library provides constants for Windows error codes.
21. Threading: This library provides support for threading and parallelism in Python code.
22. Scapy: This library provides a Python interface for capturing, manipulating, and sending network packets.
23. win32net: This library provides an interface for working with the Windows networking API, including functions for managing users, groups, and shares.
24. win32api: This library provides an interface to various Windows system services and functions, including file I/O, process management, and window creation.

Features: Following are the features provided by this tool.

1. General Information: This provides information about the system, such as the manufacturer, model, processor name, number of processors, Timezone, IP address, MAC Addresses, devices connected on ethernet.
2. Network Information: This option provides information about the network details such as IP Address, MAC address, DNS details, Hostname. It also scans for all open ports and saves the output in *openports.xls* file.It also does the network analysis which will

capture all TCP ,UDP and other kind of packets and save their details in *Networkanalysis.txt*

3. Process Analysis: This gives you details regarding all kinds of services and processes running in the system. You can see the details of running processes in *Process.xls* file. You can see the details of running services in *Services.xls* file. You can see the details of stopped services in *Stopped Services.xls* file. You can also see the list of MRU(Most Recently Used) files in *MRUList.xls* file.
4. Memory Analysis: These provides information related to the memory present in the system, You'll get the details related to Virtual Memory, Disk Usage, Disk Partition, CPU usage and RAM usage.
5. File and Folder Analysis: This provides you with the option to search for any kind of file type. User just needs to enter the file extension details, the tool will fetch all files present with that extension in the system.
6. Account Activities: This option displays information about the user accounts and groups present in the system. This information includes the user name, SSID, RID, group description, user specific to each group, login time details, number of logins and password age details.
7. External Devices analysis: This provides details regarding the external devices being connected to the system with their names and last connection time.
8. Check Password Pwned or not: This tells you whether the password you enter on the terminal has been pawned or not.
9. Save windows logs: This option allows you to save windows logs in a specified location.