EDR Automated Script Documentation

# Introduction

This document provides detailed documentation for the EDR Automated Script. The script is designed to set up   
an endpoint detection and response (EDR) system that works across platforms (Windows, macOS, and Linux).   
The script automates the setup of directory structures, installation of dependencies, and provides monitoring   
features such as process monitoring, file system monitoring, network traffic monitoring, malware scanning,   
and forensic report generation.

# Features

## 1. Cross-Platform Compatibility

The script automatically detects the operating system (Windows, macOS, or Linux) and installs the appropriate   
dependencies. It ensures that the EDR system can run on any platform by adjusting commands accordingly.

## 2. Automated Directory Setup

The script automatically creates the following directories in the user's home directory:  
- PLEXOR: Used to store logs related to terminal multiplexing (if needed).  
- EDR: Stores the EDR system files and configurations.  
- Docx-Reporting: Stores generated forensic reports in .docx format.

## 3. Dependency Installation

The script automatically installs all required Python libraries based on the user's operating system using pip.   
The dependencies include:  
- psutil: For system process monitoring.  
- watchdog: For file system monitoring.  
- scapy: For network traffic monitoring and packet sniffing.  
- python-docx: For generating forensic reports in .docx format.

## 4. System Process Monitoring

The script continuously monitors running system processes on the endpoint. It logs details such as process names,  
CPU usage, and memory usage. This is done using psutil on all supported platforms. On Windows, it runs tasklist;   
on macOS and Linux, it runs ps aux to gather process information.

## 5. File System Monitoring

The script monitors any changes to the file system, such as file creations, modifications, or deletions. It logs   
alerts for any such activity in real-time. This feature is powered by the watchdog library, which works across all platforms.

## 6. Network Traffic Monitoring

The script captures and logs network traffic using the scapy library. It can capture a specified number of packets and   
log packet summaries, including source and destination IP addresses, protocols, and more. On Windows, Npcap must be   
installed to enable network packet sniffing.

## 7. Full Directory Malware Scanning

The script traverses the specified directory (e.g., the home directory or C:\ on Windows) and scans files for known   
malware signatures by calculating the MD5 hash of each file and comparing it against a list of known malware hashes.   
The list can be customized by adding more hash values. The scan results are logged, including any detected malware.

## 8. Forensic Report Generation

At the end of the monitoring period, the script automatically generates a detailed forensic report in .docx format.  
The report includes all logged information such as system processes, file system changes, network traffic, and any   
detected malware. The report is saved in the Docx-Reporting directory.

# How the Script Works

1. The script first installs all necessary dependencies automatically based on the user's operating system.  
2. It sets up the required directory structure (PLEXOR, EDR, Docx-Reporting) in the user's home directory.  
3. The script then starts monitoring system processes, file system changes, and network traffic concurrently using   
 multiple threads.  
4. It also performs a malware scan of the specified directory.  
5. All findings are logged in real-time to a log file.  
6. After a predefined period (e.g., 60 seconds), the script generates a comprehensive forensic report in .docx format.

# Usage Instructions

1. Clone or download the script to your local machine.  
2. Run the script using Python:  
 ```  
 python edr.py  
 ```  
3. The script will install any missing dependencies and begin monitoring your system automatically.  
4. After the monitoring completes, you will find a detailed forensic report in the Docx-Reporting directory.

# Copyright

Copyright © 2024 DarkSpace Software & Security  
Author: Michael James Blenkinsop