Lab - Exploring Processes, Threads, Handles, and Windows Registry

Part 1: Exploring Processes

Step 1: Download Windows SysInternals Suite.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Step 2: Explore an active process.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Изображение выглядит как текст, снимок экрана, Красочность, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

The Web Browser Window immediately have closed right after clicking one of options - “Kill Process”.

Step 3: Start another process.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

During the ping process, we have noticed that a new PING.EXE file appeared here, which was then immediately deleted when the Ping process ended.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

When the cmd.exe process was killed, the child process conhost.exe was also terminated automatically.

Part 2: Exploring Threads and Handles

Step 1: Explore threads.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

The Threads in the Properties window shows information such as: TID, CPU, Cycles Delta, Suspend Count, Start Adress.

Step 2: Explore handles.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

The handles for conhost.exe are pointing to various system resources such as ALPC Ports, directories/system objects, files, keys, sections, threads and so on.