**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.

**Part 3: Exploring Windows Registry**

Изображение выглядит как текст, снимок экрана, Шрифт, Цвет электрик

Содержимое, созданное искусственным интеллектом, может быть неверным.

0x00000000 (0)

Nothing, bc we have downloaded it with Microsoft Store, what have probably saved the EulaAccepted as 1 forever and we can not change it by hands.

* 1. **Create User Accounts**

f) A local account (no Microsoft account). By default it is a Standard user.

h) User1, Administrators, and SYSTEM have Full control. Creator Owner has special permissions.

No. Access is denied for a normal user. Only the folder owner, Administrators, and SYSTEM can read or change that profile folder as I did understand

1. Administrators and SYSTEM have Full control. So Regular Users have only Read & execute and List folder contents.

## Part 2: Reviewing User Account Properties

d) Users

e) Amdinistrators. (It may also list Users, but the key one is Administrators.)

**Part 3: Modifying Local User Accounts**

Step 1 Administrators and Users.

Step 2 Settings → Accounts → Family & other users → select the account → Remove.

Reflection — 1)  
Strong passwords stop unauthorized access and reduce the chance of account theft. They protect personal data and system settings and make brute-force attacks harder.

Reflection — 2)  
A Standard user follows the “only what is needed” idea. It lowers the risk of accidental changes and malware installing system-level software. Admin rights are used only when really needed. Also I did not pin any screenshots, because I see how it is easy to do. Any way, that kind of knowledge is going to be in my memory for a while, so I do not see the meaning of such kind of process there. Have a good day!